XenMobile Server : Version actuelle

Contents

Notes de publication pour les versions Rolling Patch

January 10, 2022

Cette section contient les notes de publication pour les versions Rolling Patch récentes de XenMobile Server. Cliquez sur un lien ci-dessous pour afficher les problèmes connus et résolus, les modifications de fonctionnalités et les actions nécessaires.

La dernière version Rolling Patch contient tous les correctifs des versions Rolling Patch précédentes pour la même publication.

Notes de publication pour les correctifs de la version actuelle	Date de publication
10.14 Rolling Patch 3	Dec 22, 2021
10.14 Rolling Patch 2	Dec 15, 2021
10.14 Rolling Patch 1	Nov 19, 2021

Notes de publication pour les correctifs des versions antérieures	Date de publication
10.13 Rolling Patch 6	Dec 21, 2021
10.13 Rolling Patch 5	Dec 15, 2021
10.13 Rolling Patch 4	Aug 11, 2021
10.13 Rolling Patch 3	May 13, 2021
10.13 Rolling Patch 2	Feb 25, 2021
10.13 Rolling Patch 1	Jan 8, 2021
10.12 Rolling Patch 11	Dec 21, 2021
10.12 Rolling Patch 10	Dec 16, 2021
10.12 Rolling Patch 9	Oct 8, 2021
10.12 Rolling Patch 8	Jun 2, 2021
10.12 Rolling Patch 7	Mar 29, 2021
10.12 Rolling Patch 6	Jan 26, 2021
10.11 Rolling Patch 7	Nov 18, 2020
10.10 Rolling Patch 6	Jul 22, 2020

Notes de publication pour XenMobile Server 10.14 Rolling Patch 3

January 10, 2022

Ces notes de publication décrivent les améliorations et les problèmes connus et résolus pour XenMobile Server 10.14 Rolling Patch 3.

Cette version inclut des corrections de bogues.

Pour plus d'informations sur les rolling patches précédents pour XenMobile Server 10.14.0, consultez Notes de publication pour les versions Rolling Patch.

Notes de publication pour la version XenMobile Server 10.13 Rolling Patch 6

January 10, 2022

Ces notes de publication décrivent les améliorations et les problèmes connus et résolus pour XenMobile Server 10.13 Rolling Patch 6.

Cette version inclut des corrections de bogues.

Pour plus d'informations sur les rolling patches précédents pour XenMobile Server 10.13.0, consultez Notes de publication pour les versions Rolling Patch.

Notes de publication pour XenMobile Server 10.12 Rolling Patch 11

January 10, 2022

Ces notes de publication décrivent les améliorations et les problèmes connus et résolus pour XenMobile Server 10.12 Rolling Patch 11.

Cette version inclut des corrections de bogues.

Pour plus d'informations sur les rolling patches précédents pour XenMobile Server 10.12.0, consultez Notes de publication pour les versions Rolling Patch.

Notes de publication pour XenMobile Server 10.12 Rolling Patch 10

January 10, 2022

Ces notes de publication décrivent les améliorations et les problèmes connus et résolus pour XenMobile Server 10.12 Rolling Patch 10.

Cette version inclut des corrections de bogues.

Pour plus d'informations sur les rolling patches précédents pour XenMobile Server 10.12.0, consultez Notes de publication pour les versions Rolling Patch.

Notes de publication pour XenMobile Server 10.14 Rolling Patch 2

January 10, 2022

Ces notes de publication décrivent les améliorations et les problèmes connus et résolus pour XenMobile Server 10.14 Rolling Patch 2.

Pour plus d'informations sur les rolling patches précédents pour XenMobile Server 10.14.0, consultez Notes de publication pour les versions Rolling Patch.

Problème résolu

Sur XenMobile Server, vous constatez une utilisation élevée du processeur sur les nœuds de serveur aux heures de pointe. [CXM-102568]

Notes de publication pour la version XenMobile Server 10.13 Rolling Patch 5

January 10, 2022

Ces notes de publication décrivent les améliorations et les problèmes connus et résolus pour XenMobile Server 10.13 Rolling Patch 5.

Nouveautés

- **Prise en charge des appareils Windows 11.** Vous pouvez désormais utiliser XenMobile Server pour gérer les appareils Windows 11. Pour de plus amples informations, consultez la liste des systèmes d'exploitation pris en charge. [CXM-99998]
- **Configuration du mode de connexion et de la priorité réseau pour macOS.** Dans la stratégie Wi-Fi, activez le paramètre **Mode de connexion** pour les appareils macOS afin de choisir la manière dont les utilisateurs rejoignent le réseau. L'appareil peut utiliser les informations

d'identification système ou les informations d'identification saisies dans la fenêtre de connexion pour authentifier l'utilisateur. Si vous disposez de plusieurs réseaux, tapez un numéro dans le champ **Priorité** pour définir la priorité de la connexion réseau. L'appareil choisit le réseau avec le numéro le plus bas. Pour plus d'informations, reportez-vous aux paramètres macOS dans la section Stratégie Wi-Fi. [CXM-100533]

- XenMobile Server ne pourra pas synchroniser les licences de groupe avec Google, en raison de l'abandon de la prise en charge des licences de groupe par Google sur les appareils Android Enterprise. Pour plus d'informations, consultez cet article. [CXM-101309]

Pour plus d'informations sur les rolling patches précédents pour XenMobile Server 10.13.0, consultez Notes de publication pour les versions Rolling Patch.

Problèmes résolus

- Après l'inscription d'appareils iOS 15 ou macOS 12, le profil de configuration MDM affiche la mention « Non vérifié ». [CXM-99380]
- Les applications d'achat en volume Apple installées sur les appareils se mettent automatiquement à jour vers la dernière version lorsque le paramètre **Actualisation auto des apps** est désactivé. [CXM-99723]
- Sur la console XenMobile Server, lorsque vous modifiez les paramètres d'une application pour effacer toutes les plateformes et que vous enregistrez, l'application n'est pas répertoriée dans **Configurer > Applications**. [CXM-99850]
- Sur certains appareils Android Enterprise, les groupes de mise à disposition et les stratégies ou applications attribuées ne sont pas appliquées par intermittence. [CXM-101554]
- Sur XenMobile Server, vous constatez une utilisation élevée du processeur sur les nœuds de serveur aux heures de pointe. [CXM-102450]
- Sur les appareils iOS inscrits en mode MDM uniquement, vous ne pouvez pas ajouter d'applications via les navigateurs ouverts par Secure Hub à partir de l'App Store. L'erreur suivante s'affiche : **Votre session a expiré. Reconnectez-vous pour continuer.** [CXM-102604]
- Sur XenMobile Server version 10.13, vous ne pouvez pas vous connecter et configurer le StorageZone Controller avec des connecteurs StorageZone uniquement. [CXM-102655]
- Sur les versions 10.13 RP1 et ultérieures de XenMobile Server, l'interruption de connectivité entre nœuds XenMobile de la surveillance SNMP ne fonctionne pas. [CXM-102788]

Notes de publication pour XenMobile Server 10.14 Rolling Patch 1

January 10, 2022

Ces notes de publication décrivent les améliorations et les problèmes connus et résolus pour XenMobile Server 10.14 Rolling Patch 1.

Nouveautés

- **Prise en charge des appareils Windows 11.** Vous pouvez désormais utiliser XenMobile pour gérer des appareils Windows 11. Pour de plus amples informations, consultez la liste des systèmes d'exploitation pris en charge. [CXM-99999]
- **Configuration du mode de connexion et de la priorité réseau pour macOS.** Dans la stratégie Wi-Fi, activez le paramètre **Mode de connexion** pour les appareils macOS afin de choisir la manière dont les utilisateurs rejoignent le réseau. L'appareil peut utiliser les informations d'identification système ou les informations d'identification saisies dans la fenêtre de connexion pour authentifier l'utilisateur. Si vous disposez de plusieurs réseaux, tapez un numéro dans le champ **Priorité** pour définir la priorité de la connexion réseau. L'appareil choisit le réseau avec le numéro le plus bas. Pour plus d'informations, reportez-vous aux paramètres macOS dans la section Stratégie Wi-Fi. [CXM-100879]
- XenMobile Server ne pourra pas synchroniser les licences de groupe avec Google, en raison de l'abandon de la prise en charge des licences de groupe par Google sur les appareils Android Enterprise. Pour plus d'informations, consultez cet article. [CXM-101209]

Problèmes connus

Les appareils inscrits mis à niveau de macOS 11 ou version antérieure vers macOS 12, ou les appareils récemment inscrits sur macOS12, peuvent s'afficher comme « Non vérifié » sous **Préférences système > Profils** sur l'appareil. Pour plus d'informations et une solution au problème, consultez cet article d'assistance.[CXM-101843]

Problèmes résolus

- Après l'inscription d'un appareil iOS 15 ou macOS 12, le profil de configuration MDM affiche la mention **Non vérifié**. [CXM-99379]
- Sur la console XenMobile Server, lorsque vous modifiez les paramètres d'une application pour effacer toutes les plateformes et que vous enregistrez, l'application n'est pas répertoriée dans **Configurer > Applications**. [CXM-99851]
- Vous ne pouvez pas quitter Citrix Launcher sur la plate-forme Android Enterprise. L'erreur suivante s'affiche : **Mot de passe incorrect**. [CXM-100975]
- Sur la version 10.14 de XenMobile Server, vous ne pouvez pas modifier la stratégie Importer le profil iOS et macOS. [CXM-102393]

Notes de publication pour XenMobile Server 10.12 Rolling Patch 9

January 10, 2022

Ces notes de publication décrivent les améliorations et les problèmes connus et résolus pour XenMobile Server 10.12 Rolling Patch 9.

Nouveautés

Prise en charge de Android 12. XenMobile Server prend désormais en charge Android 12 sur les appareils Android Enterprise. Pour obtenir un résumé des avantages en matière de sécurité et de confidentialité, consultez la documentation de Google pour Android. [CXM-97765]

Prise en charge des appareils Windows 11. Vous pouvez désormais utiliser XenMobile Server pour gérer les appareils Windows 11. Pour de plus amples informations, consultez la liste des systèmes d'exploitation pris en charge. [CXM-99995]

Problèmes résolus

Les applications d'achat en volume Apple installées sur les appareils se mettent automatiquement à jour vers la dernière version lorsque le paramètre **Actualisation auto des apps** est désactivé. [CXM-95985]

Sur XenMobile Server version 10.12, une erreur s'affiche lors de l'accès aux **détails de l'appareil**. Cette erreur se produit lorsque la propriété de l'appareil a une valeur dans **”“**. [CXM-97953]

Sur la console XenMobile Server, lorsque vous modifiez les paramètres d'une application pour désélectionner toutes les plateformes et que vous enregistrez, l'application n'est pas répertoriée dans **Configurer > Applications**. [CXM-99708]

Notes de publication pour la version XenMobile Server 10.13 Rolling Patch 4

September 22, 2021

Ces notes de publication décrivent les améliorations et les problèmes connus et résolus pour XenMobile Server 10.13 Rolling Patch 4.

Nouveautés

Prise en charge de Android 12. XenMobile Server prend désormais en charge les mises à jour d'appareils Android Enterprise vers Android 12. Pour obtenir un résumé des avantages en matière de sécurité et de confidentialité, consultez la documentation Android.

Pour plus d'informations sur les rolling patches précédents pour XenMobile Server 10.13.0, consultez Notes de publication pour les versions Rolling Patch.

Problèmes résolus

- La propriété du serveur `ios.mdm.apns.connectionPoolSize` est masquée lorsque vous passez à l'API HTTP/2 pour APNs. [CXM-95479]
- Sur XenMobile Server version 10.12, vous ne pouvez pas modifier les propriétés VPP sur certaines applications. [CXM-96854]
- L'installation automatique des applications Web requises échoue sur les appareils MDM uniquement. [CXM-97477]
- Sur XenMobile Server version 10.13, lorsque vous configurez le serveur proxy à l'aide de l'**interface de ligne de commande**, vous ne pouvez pas envoyer de notifications à Secure Hub exécuté sur des appareils iOS. [CXM-97807]
- Sur XenMobile Server version 10.13, une erreur s'affiche lors de l'accès aux **détails de l'appareil**. Cette erreur se produit lorsque la propriété de l'appareil a une valeur dans **”“**. [CXM-97951]

Notes de publication pour XenMobile Server 10.12 Rolling Patch 8

June 11, 2021

Ces notes de publication décrivent les améliorations et les problèmes connus et résolus pour XenMobile Server 10.12 Rolling Patch 8.

Nouveautés

Renouvellement du certificat APNs du Secure Hub. Le certificat APNs (Apple Push Notification Service) de Secure Hub pour XenMobile Server 10.12 expire le 17 juin 2021. Cette mise à jour renouvelle le certificat APNs de Secure Hub, qui expire le 7 mai 2022. [CXM-94513]

Problèmes résolus

- Juste après l'inscription d'un appareil exécutant macOS 10.14+, les propriétés de l'appareil ne sont pas toujours renseignées dans la console XenMobile Server. Après le redémarrage de

l'appareil, les propriétés de l'appareil apparaissent comme prévu. [CXM-94221]

- Sur XenMobile Server 10.12, ShareFile échoue par intermittence à établir une connexion. [CXM-95419]

Notes de publication pour la version XenMobile Server 10.13 Rolling Patch 3

May 21, 2021

Ces notes de publication décrivent les améliorations et les problèmes connus et résolus pour XenMobile Server 10.13 Rolling Patch 3.

Nouveautés

Renouvellement du certificat APNs du Secure Hub. Le certificat APNs (Apple Push Notification Service) de Secure Hub pour XenMobile Server 10.13 expire le 17 juin 2021. Cette mise à jour renouvelle le certificat APNs de Secure Hub, qui expire le 7 mai 2022. [CXM-94070]

Port secondaire pour les notifications APNs. XenMobile Server prend désormais en charge l'utilisation du port 2197 comme port secondaire (au lieu du port 443). Vous utilisez le port 2197 pour envoyer des notifications APNs et recevoir des commentaires de `api.push.apple.com`. Le port utilise l'API du fournisseur APNs basé sur HTTP/2. La valeur par défaut de la propriété serveur `apns.http2.alternate.port.enabled` est **`false`**. Pour utiliser le port secondaire, mettez à jour la propriété serveur, puis redémarrez le serveur. [CXM-93911]

Problèmes résolus

Juste après l'inscription d'un appareil exécutant macOS 10.14+, les propriétés de l'appareil ne sont pas toujours renseignées dans la console XenMobile Server. Après le redémarrage de l'appareil, les propriétés de l'appareil apparaissent comme prévu. [CXM-94150]

Si vous activez les paramètres **Activer les applications système** et **Désactiver les applications** pour la même application dans la stratégie Restrictions, l'application apparaît dans le profil de travail. [CXM-94097]

Lorsque vous ajoutez des utilisateurs SNMP à la console XenMobile Server, les utilisateurs n'apparaissent pas dans la liste **Utilisateurs de surveillance SNMP** ou les agents SNMP deviennent inactifs. [CXM-93199]

Sur XenMobile Server, les tests de connectivité NetScaler Gateway n'affichent pas de résultat. [CXM-93134]

Sur la console XenMobile Server, la date d'expiration correcte du certificat racine n'est pas affichée. [CXM-93133]

Nouveautés dans XenMobile Server 10.14

January 10, 2022

Prise en charge continue des stratégies classiques obsolètes de Citrix ADC

Citrix a récemment annoncé la fin de la prise en charge de certaines fonctionnalités basées sur des stratégies classiques à partir de Citrix ADC 12.0 build 56.20. Les avis de fin de prise en charge Citrix ADC n'ont aucun impact sur les intégrations XenMobile Server existantes avec Citrix Gateway. XenMobile Server continue de prendre en charge les stratégies classiques et aucune action n'est donc nécessaire.

XenMobile Migration Service

Si vous utilisez une installation locale de XenMobile Server, notre service de migration de XenMobile (XenMobile Migration Service) gratuit peut vous aider à démarrer avec Endpoint Management. La migration de XenMobile Server vers Citrix Endpoint Management ne nécessite pas de réinscrire les appareils.

Pour démarrer la migration, contactez votre représentant ou partenaire Citrix local. Consultez XenMobile Migration Service.

Annonces de fin de prise en charge

Pour plus d'informations sur les fonctionnalités Citrix XenMobile qui vont disparaître, consultez la section Fin de prise en charge.

Avant de mettre à niveau les terminaux vers iOS 14.5

Avant de mettre à niveau un point de terminaison vers iOS 14.5, Citrix recommande d'effectuer les actions suivantes pour atténuer les plantages d'applications :

- Mettez à niveau Citrix Secure Mail et Secure Web vers la version 21.2.X ou supérieure. Consultez Mettre à niveau les applications MDX ou Enterprise.
- Si vous utilisez MDX Toolkit, encapsulez toutes les applications iOS tierces avec MDX Toolkit 21.3.X ou version ultérieure. Consultez la page de téléchargement du MDX Toolkit pour obtenir la dernière version.

Avant la mise à niveau d'une instance Citrix ADC locale

La mise à niveau d'un Citrix ADC local vers certaines versions peut entraîner une erreur d'authentification unique. L'authentification unique à Citrix Files ou à l'URL du domaine ShareFile dans un navigateur avec l'option **Connexion employés** entraîne une erreur. L'utilisateur ne peut pas se connecter.

Pour contourner ce problème : si vous n'avez pas encore exécuté la commande suivante à partir de l'interface de ligne de commande ADC sur Citrix Gateway, exécutez-la pour activer l'authentification unique (SSO) globale :

```
`set vpn parameter SSO ON`
`bind vpn vs <vsName> -portalTheme X1`
```

Pour plus d'informations, consultez :

- Version Citrix ADC (Feature Phase) 13.0 Build 67.39/67.43
- Configurations SSO affectées

Après avoir terminé ces étapes, les utilisateurs peuvent utiliser l'authentification unique (SSO) avec Citrix Files ou l'URL du domaine ShareFile dans un navigateur avec l'option Connexion employés. [CXM-88400]

Avant de procéder à la mise à niveau vers XenMobile 10.14 (sur site)

Certaines configurations système requises ont été modifiées. Pour plus d'informations, consultez la section Configuration système requise et compatibilité et Compatibilité XenMobile.

1. Si la machine virtuelle exécutant XenMobile Server à mettre à niveau dispose de moins de 8 Go de RAM, nous vous recommandons d'augmenter la mémoire vive à 8 Go au minimum.
2. Mettez à jour votre serveur de licences Citrix vers la version 11.16 ou version ultérieure avant la mise à jour vers la dernière version de XenMobile Server 10.14.

   La dernière version de XenMobile requiert le serveur de licences Citrix 11.16 (version minimale).

   > **Remarque :**
   >
   > La date Customer Success Services (anciennement la date Subscription Advantage) dans XenMobile 10.14 est le 15 septembre 2021. La date Customer Success Services sur votre licence Citrix doit être postérieure à cette date.
   >
   > Vous pouvez visualiser la date en regard de la licence dans le serveur de licences. Si vous connectez la dernière version de XenMobile à un environnement de serveur de licences plus ancien, la vérification de la connectivité échoue et vous ne pouvez pas configurer le serveur de licences.

Pour renouveler la date sur votre licence, téléchargez le dernier fichier de licence à partir du portail Citrix, puis téléchargez-le sur le serveur de licences. Consultez Customer Success Services (Forfait réussite client).

3. Pour un environnement en cluster, la configuration requise pour les déploiements de stratégies et d'applications iOS sur des appareils exécutant iOS 11 ou version ultérieure est la suivante. Si Citrix Gateway est configuré pour la persistance SSL, vous devez ouvrir le port 80 sur tous les nœuds de XenMobile Server.
4. Avant d'installer une mise à jour XenMobile, utilisez les fonctions de votre machine virtuelle pour prendre un instantané de votre système. Sauvegardez aussi la base de données de configuration de votre système. Si vous rencontrez des problèmes durant une mise à niveau, des copies de sauvegarde complètes vous permettent de récupérer.

Pour effectuer la mise à niveau

Avec cette version, XenMobile prend en charge VMware ESXi 7.0. Assurez-vous de mettre à niveau vers la version 10.14 avant d'installer ou de mettre à niveau ESXi 7.0.

Vous pouvez effectuer une mise à niveau directement vers XenMobile 10.14 depuis XenMobile 10.13.x ou 10.12.x. Pour effectuer la mise à niveau, téléchargez le dernier fichier binaire disponible en accédant à https://www.citrix.com/downloads. Accédez à **Citrix Endpoint Management (XenMobile) > XenMobile Server > Produit logiciel > XenMobile Server 10**. Sur la vignette du logiciel XenMobile Server de votre hyperviseur, cliquez sur **Télécharger le fichier**.

Pour télécharger la mise à niveau, utilisez la page **Gestion des versions** dans la console XenMobile. Consultez Pour mettre à niveau depuis la page Gestion des versions.

Après la mise à niveau

Si une fonctionnalité utilisant des connexions sortantes cesse de fonctionner alors que vous n'avez pas changé la configuration de vos connexions, vérifiez dans le journal de XenMobile Server s'il existe des erreurs telle que la suivante : « Impossible de se connecter au serveur VPP : le nom d'hôte 192.0.2.0 ne correspond pas au sujet du certificat fourni par l'homologue ».

- L'erreur de validation de certificat signifie que vous devez désactiver la vérification du nom d'hôte sur XenMobile Server.
- Par défaut, la vérification de nom d'hôte est activée sur les connexions sortantes à l'exception du serveur PKI de Microsoft.
- Si la vérification de nom d'hôte interrompt votre déploiement, définissez la propriété de serveur `disable.hostname.verification` sur **`true`**. La valeur par défaut de cette propriété est **`false`**.

Mises à jour de prise en charge de plate-forme

- **iOS 15 :** XenMobile Server et les applications de productivité Citrix Mobile sont compatibles avec iOS 15, mais ne prennent actuellement en charge aucune nouvelle fonctionnalité iOS 15.
- **Android 12 :** XenMobile Server prend en charge Android 12. Consultez Migrer de l'administration des appareils vers Android Enterprise pour plus d'informations sur la façon dont la fin de prise en charge des API d'administration des appareils Google affecte les appareils exécutant Android 10. Consultez également ce blog Citrix.

Stratégies d'appareil

- Nous avons ajouté deux paramètres à tous les modes d'inscription Android Enterprise afin d'obtenir une correspondance plus étroite avec les paramètres Google et de simplifier la configuration.
  - **Autoriser le partage Bluetooth :** si cette option est désactivée, les utilisateurs ne peuvent pas établir de partage Bluetooth sortant sur leurs appareils.
  - **Autoriser désinstallation d'applications :** permet aux utilisateurs de désinstaller des applications depuis le Google Play Store d'entreprise.

  En outre, nous avons déplacé le paramètre **Autoriser mise à jour par réseau cellulaire** de la stratégie de restrictions vers la stratégie de mise à jour d'OS.

  Pour plus d'informations sur ces modifications, consultez Stratégie de restrictions et Stratégie de mise à jour d'OS.
- Les paramètres de restriction pour Android Enterprise ont été réorganisés pour plus de clarté. Dans certains cas, des modifications mineures ont été apportées aux noms des paramètres. Pour plus d'informations sur la réorganisation, consultez Paramètres Android Enterprise.
- Vous pouvez désormais mettre à jour automatiquement les applications gérées sur les appareils Android Enterprise. Pour plus d'informations, consultez la section Stratégie de mise à jour automatique des applications gérées.
- Vous pouvez configurer une liste des types de fichiers qui peuvent être chargés à l'aide de la stratégie Fichiers. Les types de fichiers suivants ne peuvent pas être chargés même si vous les ajoutez à cette liste d'autorisation :
  - .cab
  - .appx
  - .ipa
  - .apk
  - .xap
  - .mdx

  - .exe

  Pour plus d'informations, consultez Propriétés du serveur.

Inscription des appareils

- Vous pouvez maintenant créer différents profils d'inscription pour les appareils iOS et Android. XenMobile Server prend en charge un certain nombre de profils d'inscription comportant différents types d'inscription. Pour plus d'informations, voir Profils d'inscription.
- Les appareils Android 11+ entièrement gérés sont inscrits en mode profil de travail sur appareils appartenant à l'entreprise. Le nouveau mode sépare davantage les profils personnels et de travail sur un appareil. Cette modification offre à l'organisation un plus grand contrôle sur le profil géré et offre aux utilisateurs plus de confidentialité sur leur profil personnel. Pour plus d'informations, consultez Android Enterprise et Propriétés du serveur.
- Vous pouvez désormais spécifier d'autres écrans de configuration à ignorer lorsque les utilisateurs configurent des appareils iOS ou macOS.
  - iOS
    - **Restauration terminée :** empêche les utilisateurs de voir si une restauration est terminée pendant l'installation. Pour iOS 14.0 et versions ultérieures.
    - **Mise à jour terminée :** empêche les utilisateurs de voir si une mise à jour logicielle est terminée pendant l'installation. Pour iOS 14.0 et versions ultérieures.
  - macOS
    - **Accessibilité :** empêche les utilisateurs d'entendre la fonctionnalité VoiceOver automatiquement. Disponible uniquement si l'appareil est connecté à Ethernet. Pour macOS 11 et versions ultérieures.
    - **Biométrie :** empêche l'utilisateur de configurer Touch ID et Face ID. Pour macOS 10.12.4 et versions ultérieures.
    - **True Tone :** empêche les utilisateurs de configurer des capteurs à quatre canaux pour régler dynamiquement la balance des blancs de l'affichage. Pour macOS 10.13.6 et versions ultérieures.
    - **Apple Pay :** empêche les utilisateurs de configurer Apple Pay. Si ce paramètre est désactivé, les utilisateurs doivent configurer Touch ID et Apple ID. Assurez-vous que les paramètres **Apple ID** et **Biométrie** sont effacés. Pour macOS 10.12.4 et versions ultérieures.
    - **Screen Time :** empêche les utilisateurs d'activer la fonction Screen Time. Pour macOS 10.15 et versions ultérieures.

  Pour plus d'informations sur la configuration des options de configuration, consultez la section Déployer des appareils via le programme de déploiement d'Apple.

Afficher les fichiers journaux de mise à jour

Une nouvelle option appelée **Afficher les fichiers journaux de mise à jour** est disponible dans l'interface de ligne de commande **Journaux** du menu **Dépannage**. Cette option vous permet d'afficher une liste du contenu du journal de mise à jour et d'augmenter l'efficacité du dépannage. Pour plus d'informations sur les outils d'interface de ligne de commande, consultez la section Options d'interface de ligne de commande.

Fichier journal des erreurs

Lorsque vous affichez les journaux dans **Dépannage et support > Journaux**, vous pouvez maintenant afficher un journal qui affiche les erreurs filtrées à partir du journal de débogage. Pour plus d'informations, consultez la section Afficher les fichiers journaux dans XenMobile.

Propriétés du serveur

- Vous pouvez décider si les applications Android d'ancienne génération sont mises à disposition sur les applications Android Enterprise en configurant la propriété de serveur `afw.allow.legacy.apps`. Pour plus d'informations, consultez Propriétés du serveur.
- XenMobile Server prend désormais en charge l'utilisation du port 2197 comme port secondaire (au lieu du port 443). Vous utilisez le port 2197 pour envoyer et recevoir des notifications APNs de `api.push.apple.com`. Le port utilise l'API du fournisseur APNs basé sur HTTP/2. La valeur par défaut de la propriété de serveur `apns.http2.alternate.port.enabled` est **`false`**. Pour utiliser le port 2197, mettez à jour la propriété de serveur, puis redémarrez le serveur.
- La validation du mot de passe empêche l'ajout d'utilisateurs possédant des mots de passe faibles. Lorsque la propriété `enable.password.strength.validation` est définie sur **`true`**, vous ne pouvez pas créer d'utilisateurs locaux s'ils utilisent des mots de passe faibles.

Amélioration de la liste de serveurs virtuels VPN

Si le nom du serveur VPN n'inclut pas `_XM_XenMobileGetway`, XenMobile Server sélectionne le premier serveur virtuel VPN disponible dans la liste.

Prise en charge de Citrix Launcher

XenMobile Server prend en charge Citrix Launcher sur les appareils Android Enterprise. Pour plus d'informations, consultez la section Stratégie de configuration du Launcher.

Revamping des couleurs de XenMobile Server

XenMobile Server est conforme aux mises à jour des couleurs de la marque Citrix.

Nouveautés dans XenMobile Server 10.13

January 10, 2022

XenMobile Server 10.13 (PDF)

Prise en charge continue des stratégies classiques obsolètes de Citrix ADC

Citrix a récemment annoncé la fin de la prise en charge de certaines fonctionnalités basées sur des stratégies classiques à partir de Citrix ADC 12.0 build 56.20. Les avis de fin de prise en charge Citrix ADC n'ont aucun impact sur les intégrations XenMobile Server existantes avec Citrix Gateway. XenMobile Server continue de prendre en charge les stratégies classiques et aucune action n'est donc nécessaire.

XenMobile Migration Service

Si vous utilisez une installation locale de XenMobile Server, notre service de migration de XenMobile (XenMobile Migration Service) gratuit peut vous aider à démarrer avec Endpoint Management. La migration de XenMobile Server vers Citrix Endpoint Management ne nécessite pas de réinscrire les appareils.

Pour démarrer la migration, contactez votre représentant ou partenaire Citrix local. Consultez XenMobile Migration Service.

Annonces de fin de prise en charge

Pour plus d'informations sur les fonctionnalités Citrix XenMobile qui vont disparaître, consultez la section Fin de prise en charge.

Avant de mettre à niveau les terminaux vers iOS 14.5

Avant de mettre à niveau un point de terminaison vers iOS 14.5, Citrix recommande d'effectuer les actions suivantes pour atténuer les plantages d'applications :

- Mettez à niveau Citrix Secure Mail et Secure Web vers la version 21.2.X ou supérieure. Consultez Mettre à niveau les applications MDX ou Enterprise.

- Si vous utilisez MDX Toolkit, encapsulez toutes les applications iOS tierces avec MDX Toolkit 21.3.X ou version ultérieure. Consultez la page de téléchargement du MDX Toolkit pour obtenir la dernière version.

Avant la mise à niveau d'une instance Citrix ADC locale

La mise à niveau d'un Citrix ADC local vers certaines versions peut entraîner une erreur d'authentification unique. L'authentification unique à Citrix Files ou à l'URL du domaine ShareFile dans un navigateur avec l'option **Connexion employés** entraîne une erreur. L'utilisateur ne peut pas se connecter.

Pour contourner ce problème : si vous n'avez pas encore exécuté la commande suivante à partir de l'interface de ligne de commande ADC sur Citrix Gateway, exécutez-la pour activer l'authentification unique (SSO) globale :

```
1 `set vpn parameter SSO ON`
2 `bind vpn vs <vsName> -portalTheme X1`
```

Pour plus d'informations, consultez :

- Version Citrix ADC (Feature Phase) 13.0 Build 67.39/67.43
- Configurations SSO affectées

Après avoir terminé ces étapes, les utilisateurs peuvent utiliser l'authentification unique (SSO) avec Citrix Files ou l'URL du domaine ShareFile dans un navigateur avec l'option Connexion employés. [CXM-88400]

Avant de procéder à la mise à niveau vers XenMobile 10.13 (sur site)

Certaines configurations système requises ont été modifiées. Pour plus d'informations, consultez la section Configuration système requise et compatibilité et Compatibilité XenMobile.

1. Si la machine virtuelle exécutant XenMobile Server à mettre à niveau dispose de moins de 8 Go de RAM, nous vous recommandons d'augmenter la mémoire vive à 8 Go au minimum.
2. Mettez à jour votre serveur de licences Citrix vers la version 11.16 ou version ultérieure avant la mise à jour vers la dernière version de XenMobile Server 10.13.

   La dernière version de XenMobile requiert le serveur de licences Citrix 11.16 (version minimale).

   > **Remarque :**
   >
   > la date Customer Success Services (anciennement la date Subscription Advantage) dans XenMobile 10.13 est le 29 septembre 2020. La date Customer Success Services sur votre licence Citrix doit être postérieure à cette date.
   >
   > Vous pouvez visualiser la date en regard de la licence dans le serveur de licences. Si vous

> connectez la dernière version de XenMobile à un environnement de serveur de licences plus ancien, la vérification de la connectivité échoue et vous ne pouvez pas configurer le serveur de licences.

Pour renouveler la date sur votre licence, téléchargez le dernier fichier de licence à partir du portail Citrix, puis téléchargez-le sur le serveur de licences. Consultez Customer Success Services (Forfait réussite client).

3. Pour un environnement en cluster, la configuration requise pour les déploiements de stratégies et d'applications iOS sur des appareils exécutant iOS 11 ou version ultérieure est la suivante. Si Citrix Gateway est configuré pour la persistance SSL, vous devez ouvrir le port 80 sur tous les nœuds de XenMobile Server.
4. Avant d'installer une mise à jour XenMobile, utilisez les fonctions de votre machine virtuelle pour prendre un instantané de votre système. Sauvegardez aussi la base de données de configuration de votre système. Si vous rencontrez des problèmes durant une mise à niveau, des copies de sauvegarde complètes vous permettent de récupérer.

Pour effectuer la mise à niveau

Avec cette version, XenMobile prend en charge VMware ESXi 7.0. Assurez-vous de mettre à niveau vers la version 10.13 avant d'installer ou de mettre à niveau ESXi 7.0.

Vous pouvez effectuer une mise à niveau directement vers XenMobile 10.13 depuis XenMobile 10.12.x ou 10.11.x. Pour effectuer la mise à niveau, téléchargez le dernier fichier binaire disponible en accédant à https://www.citrix.com/downloads. Accédez à **Citrix Endpoint Management (XenMobile) > XenMobile Server > Produit logiciel > XenMobile Server 10**. Sur la vignette du logiciel XenMobile Server de votre hyperviseur, cliquez sur **Télécharger le fichier**.

Pour télécharger la mise à niveau, utilisez la page **Gestion des versions** dans la console XenMobile. Consultez Pour mettre à niveau depuis la page Gestion des versions.

Après la mise à niveau

Si une fonctionnalité utilisant des connexions sortantes cesse de fonctionner alors que vous n'avez pas changé la configuration de vos connexions, vérifiez dans le journal de XenMobile Server s'il existe des erreurs telle que la suivante : « Impossible de se connecter au serveur VPP : le nom d'hôte 192.0.2.0 ne correspond pas au sujet du certificat fourni par l'homologue. »

- L'erreur de validation de certificat signifie que vous devez désactiver la vérification du nom d'hôte sur XenMobile Server.
- Par défaut, la vérification de nom d'hôte est activée sur les connexions sortantes à l'exception du serveur PKI de Microsoft.

- Si la vérification de nom d'hôte interrompt votre déploiement, définissez la propriété de serveur `disable.hostname.verification` sur **`true`**. La valeur par défaut de cette propriété est **`false`**.

Mises à jour de prise en charge de plate-forme

- **iOS 14 :** XenMobile Server et les applications de productivité Citrix Mobile sont compatibles avec iOS 14, mais ne prennent actuellement en charge aucune nouvelle fonctionnalité iOS 14. Utilisez le MDX Toolkit 20.8.5 ou une version ultérieure ou préparez les applications à l'aide du SDK MAM.
- **Android 11 :** XenMobile Server prend en charge Android 11. Consultez Migrer de l'administration des appareils vers Android Enterprise pour plus d'informations sur la façon dont la fin de prise en charge des API d'administration des appareils Google affecte les appareils exécutant Android 10. Consultez également ce blog Citrix.

Configurer plusieurs modes de gestion d'appareils et d'applications dans un environnement unique

Vous pouvez maintenant configurer un seul site XenMobile pour prendre en charge plusieurs configurations d'inscription. Le rôle des profils d'inscription a été élargi pour inclure les paramètres d'inscription pour la gestion des appareils et des applications.

Vous pouvez utiliser des profils d'inscription pour combiner plusieurs cas d'utilisation et chemins de migration d'appareils au sein d'une seule console XenMobile. Parmi les cas d'utilisation :

- Gestion des appareils mobiles (MDM exclusif)
- MDM+Gestion des applications mobiles (MAM)
- MAM exclusif
- Inscriptions d'appareils appartenant à l'entreprise
- Inscriptions BYOD (possibilité de se désinscrire de MDM)
- Migration des inscriptions Android Device Administrator vers les inscriptions Android Enterprise (appareil entièrement géré, profil de travail, dédié)

Les profils d'inscription remplacent la propriété de serveur `xms.server.mode`, qui est désormais obsolète. Cette modification n'affecte pas vos groupes de mise à disposition existants ni vos appareils inscrits.

Si vous n'avez pas besoin d'inscrire des appareils dédiés, vous pouvez désactiver cette fonctionnalité en définissant la propriété de serveur `enable.multimode.xms` sur **`false`**. Consultez Propriétés du serveur.

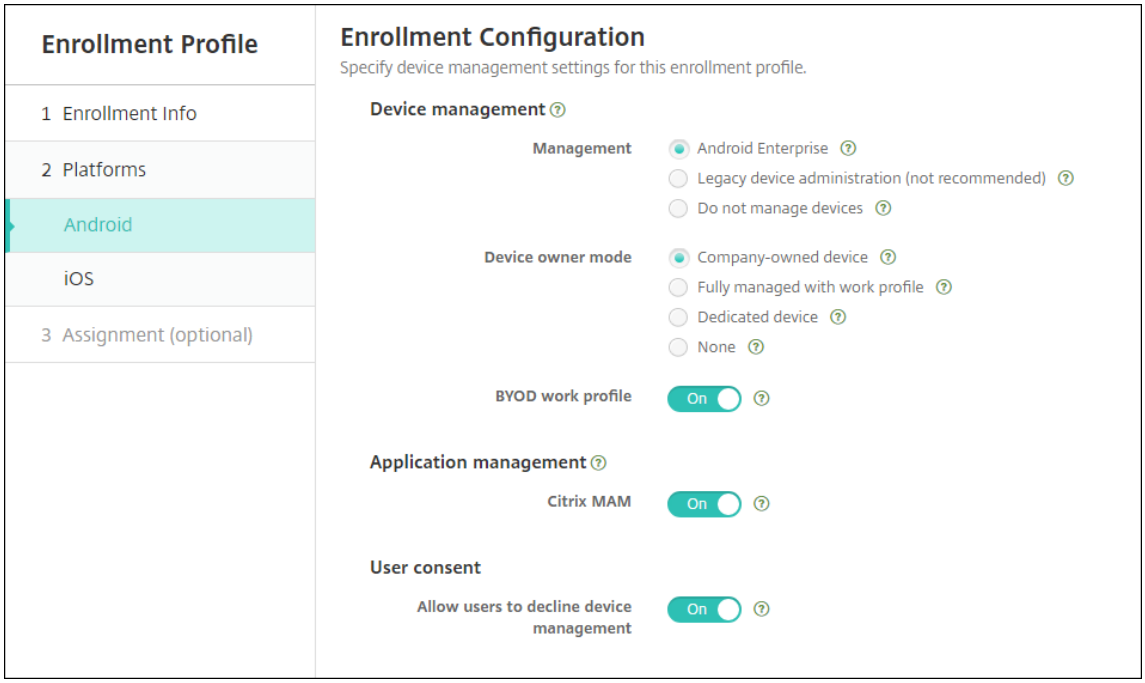
Le tableau suivant présente le chemin de migration automatisée du mode de propriété de serveur existant vers la nouvelle fonctionnalité de profil d'inscription :

Propriété de serveur existante	Nouveau mode de gestion
Mode ENT (iOS)	Inscription d'appareil Apple avec Citrix MAM
Mode ENT (Android)	Administrateur des anciens appareils avec Citrix MAM
Mode ENT (Android Enterprise)	Profil de travail sur appareils entièrement gérés (anciennement COPE), avec Citrix MAM
Mode MAM (iOS et Android)	Citrix MAM
Mode MDM (iOS)	Inscription d'appareils Apple
Mode MDM (Android)	Administration des anciens appareils
Mode MDM (Android Enterprise)	Profil de travail sur appareils entièrement gérés

Lorsque vous créez un groupe de mise à disposition, vous pouvez attacher un profil d'inscription au groupe. Si vous ne joignez pas de profil d'inscription, XenMobile attache le profil d'inscription Global.

Les profils d'inscription fournissent les fonctionnalités de gestion d'appareils suivantes :

- **Migration plus facile du mode Administrateur d'appareils (DA) Android vers Android Enterprise.** Pour les appareils Android Enterprise, les paramètres incluent un mode propriétaire d'appareil tel que : appareil entièrement géré, profil de travail sur appareil entièrement géré ou appareil dédié. Consultez Android Enterprise.



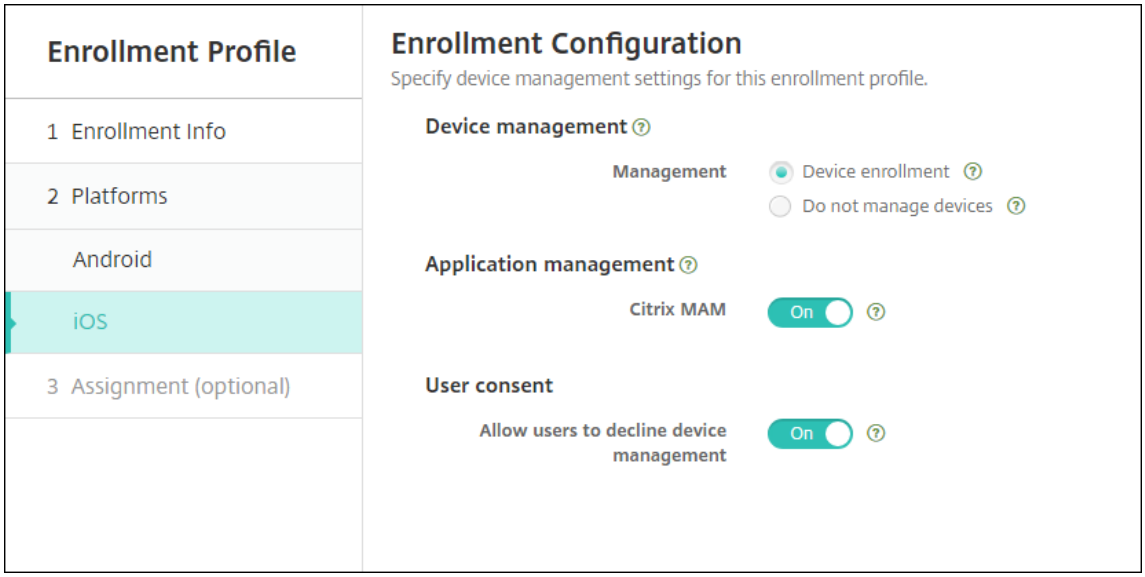
Pour cette mise à niveau, vos configurations actuelles de XenMobile pour le mode serveur et **Paramètres > Android Enterprise** sont associées aux nouveaux paramètres de profil d'inscription comme suit.

Configuration actuelle	Paramètre de gestion	Paramètre du mode propriétaire de l'appareil	Paramètre MAM Citrix
MDM Google Play géré (Android Enterprise)	Android Entreprise	Profil de travail sur appareils entièrement gérés	Désactivé
MDM ; G Suite (Administration anciens appareils)	Administration anciens appareils	non applicable	Désactivé
MAM	Ne pas gérer les appareils	non applicable	Activé
MDM+MAM Google Play géré (Android Enterprise)	Android Enterprise*	Profil de travail sur appareils entièrement gérés	Activé
MDM+MAM ; G Suite (Administration anciens appareils)	Administration des anciens appareils*	non applicable	Activé

* Si l'inscription est requise, **Autoriser les utilisateurs à décliner la gestion des appareils** est **Désactivé**.

Après la mise à niveau, vos profils d'inscription actuels reflètent ces mappages. Déterminez si vous souhaitez créer d'autres profils d'inscription pour gérer les nouveaux cas d'utilisation lorsque vous migrez depuis le mode Administration des anciens appareils.

- **Gestion iOS plus facile.** Pour les appareils iOS, vous pouvez choisir entre l'inscription d'appareils en tant qu'appareils gérés ou non gérés.



Pour cette mise à niveau, vos configurations antérieures sont associées aux nouveaux paramètres de profil d'inscription comme suit.

Mode du serveur	Paramètre de gestion	Paramètre MAM Citrix
MDM	Inscription des appareils	Désactivé
MAM	Ne pas gérer les appareils	Activé
MDM+MAM	Inscription des appareils	Activé

Si l'inscription est requise, **Autoriser les utilisateurs à décliner la gestion des appareils** est **Désactivé**.

Les limitations suivantes existent pour les profils d'inscription améliorés :

- La fonctionnalité de profil d'inscription amélioré n'est pas disponible pour les invitations à l'inscription avec code confidentiel unique ou authentification à deux facteurs.

Consultez Profils d'inscription.

Prise en charge de la dernière API du fournisseur APNs basée sur HTTP/2

La prise en charge par Apple du protocole binaire hérité du service Apple Push Notification prend fin le 31 mars 2021. Apple recommande d'utiliser à la place l'API du fournisseur APNs basé sur HTTP/2. XenMobile Server prend désormais en charge l'API basée sur HTTP/2. Pour plus d'informations, consultez « Apple Push Notification Service Update » dans https://developer.apple.com/. Pour obtenir de l'aide sur la vérification de la connectivité à APNs, consultez la section Tests de connectivité.

Les versions suivantes de XenMobile Server permettent la prise en charge de l'API basée sur HTTP/2 par défaut :

- XenMobile Server 10.13
- XenMobile Server 10.12 Rolling Patch 5 et versions ultérieures

Si vous utilisez les versions suivantes de XenMobile Server, vous devez ajouter la propriété de serveur **apple.apns.http2** pour activer la prise en charge :

- XenMobile Server 10.12 Rolling Patches 2-4 et versions ultérieures
- XenMobile Server 10.11 Rolling Patch 5 et versions ultérieures

XenMobile Server 10.11 n'est plus pris en charge. Nous vous recommandons de mettre à niveau vers la dernière version.

Utiliser un VPN IPsec basé sur un certificat d'appareil avec de nombreux appareils iOS

Au lieu de configurer une stratégie VPN et une stratégie d'informations d'identification pour chaque appareil iOS nécessitant un VPN IPsec basé sur un certificat d'appareil, automatisez le processus.

1. Configurez une stratégie VPN iOS avec le type de connexion **Toujours sur IKEv2**.
2. Sélectionnez **Certificat d'appareil basé sur l'identité de l'appareil** comme méthode d'authentification d'appareil.
3. Sélectionnez le **type d'identité de l'appareil** à utiliser.
4. Importez de façon groupée vos certificats d'appareil à l'aide de l'API REST.

Pour plus d'informations sur la configuration de la stratégie VPN, consultez la section Stratégie VPN. Pour plus d'informations sur l'importation groupée de certificats, consultez la section Effectuer un chargement groupé de certificats avec l'API REST.

Mises à jour automatiques pour les applications d'achat en volume d'Apple

Lorsque vous ajoutez un compte d'achat en volume (**Paramètres > Paramètres iOS**), vous pouvez activer les mises à jour automatiques pour toutes les applications iOS. Consultez le paramètre **Actualisation auto des apps** dans la section Achats en volume d'Apple.

Exigences relatives au mot de passe pour un compte d'utilisateur local

Lorsque vous ajoutez ou modifiez un compte d'utilisateur local dans la console XenMobile, assurez-vous de respecter les exigences les plus récentes en matière de mot de passe.

Pour plus d 'informations, consultez la section Pour ajouter un compte d'utilisateur local.

- **Exigences relatives au mot de passe :** lorsque vous ajoutez ou modifiez un compte d'utilisateur local dans la console XenMobile Server, suivez les dernières exigences relatives au mot de passe. Consultez Pour ajouter un compte d'utilisateur local.

- **Local user account locking :** si un utilisateur atteint le nombre maximal de tentatives de connexion non valides consécutives, le compte d'utilisateur local se verrouille pendant 30 minutes. Le système refuse toutes les tentatives d'authentification supplémentaires jusqu'à l'expiration de la période de verrouillage. Pour déverrouiller le compte dans la console XenMobile Server, accédez à **Gérer > Utilisateurs**, sélectionnez le compte d'utilisateur, puis cliquez sur **Déverrouiller utilisateur local**. Consultez Pour déverrouiller un compte d'utilisateur local.

Stratégies d'appareil

De nouvelles stratégies et de nouveaux paramètres de stratégie ont été ajoutés pour les appareils Android Enterprise

Masquer l'icône de zone de notification sur les appareils Android Enterprise

Vous pouvez désormais indiquer si l'icône de zone de notification est masquée ou visible pour les appareils Android Enterprise. Consultez Stratégie d'options XenMobile.

Ajout de fonctionnalités de gestion des certificats pour les appareils Android Enterprise en mode Profil de travail ou en mode entièrement géré

Outre l'installation des autorités de certification dans le keystore géré, vous pouvez désormais gérer les fonctionnalités suivantes.

- **Configurer les certificats utilisés par des applications gérées spécifiques.** La stratégie d'informations d'identification pour Android Enterprise inclut désormais le paramètre **Applications qui utilisent les certificats**. Vous pouvez spécifier les applications qui utilisent les certificats utilisateur émis par le fournisseur d'identités sélectionné dans cette stratégie. Les applications bénéficient d'un accès aux certificats en mode silencieux pendant l'exécution. Pour utiliser les certificats pour toutes les applications, laissez la liste des applications vide. Consultez Stratégie d'informations d'identification.
- **Supprimer en mode silencieux les certificats du keystore géré ou désinstaller tous les certificats CA non système.** Consultez Stratégie d'informations d'identification.
- **Empêcher les utilisateurs de modifier les informations d'identification stockées dans le keystore géré.** La stratégie de restrictions pour Android Enterprise inclut désormais le paramètre **Autoriser l'utilisateur à configurer les informations d'identification**. Par défaut, ce paramètre est **Activé**. consultez la section Stratégie de restrictions.

Utilisation plus facile de l'alias de certificat dans les configurations gérées par Android Enterprise

Utilisez le nouveau paramètre **Alias de certificat** dans la stratégie **Informations d'identification** avec la stratégie **Configurations gérées par Android Enterprise**. Cela permet aux applications de s'authentifier sur le VPN sans intervention de l'utilisateur. Au lieu de trouver l'alias d'informations d'identification dans les journaux de l'application, vous créez l'alias d'informations d'identification. Créez l'alias en le tapant dans le champ **Alias de certificat** de la stratégie **Configurations gérées par Android Enterprise**. Vous tapez ensuite le même alias de certificat dans le paramètre **Alias de certificat** dans la stratégie **Informations d'identification**. Consultez Stratégie Configurations gérées par Android Entreprise et Stratégie d'informations d'identification.

Contrôle du paramètre Utiliser une seule méthode de verrouillage sur les appareils Android Enterprise

Le nouveau paramètre **Activer le code secret unifié** de la stratégie de **code secret** vous permet de contrôler si un appareil nécessite un code secret distinct pour l'appareil et le profil de travail. Avant la création de ce paramètre, les utilisateurs contrôlaient ce comportement à l'aide du paramètre **Utiliser une seule méthode de verrouillage** sur l'appareil. Lorsque le paramètre **Activer le code secret unifié** est défini sur **Activé**, les utilisateurs peuvent utiliser le même code secret pour l'appareil et le profil de travail. Si le paramètre **Activer le code secret unifié** est défini sur **Désactivé**, les utilisateurs ne peuvent pas utiliser le même code secret pour l'appareil et le profil de travail. La valeur par défaut est **Désactivé**. Le paramètre **Activer le code secret unifié** est disponible pour les appareils Android Enterprise exécutant Android 9.0 ou version ultérieure. consultez la section Stratégie de code secret.

Afficher des applications et des raccourcis sur les appareils Android Enterprise qui ne sont pas conformes

La stratégie Code secret pour Android Enterprise a un nouveau paramètre, **Afficher les applications et les raccourcis bien que le code d'accès ne soit pas conforme**. Activez le paramètre pour que les applications et les raccourcis restent visibles lorsque le code secret de l'appareil n'est plus conforme. Citrix vous recommande de créer une action automatisée pour marquer l'appareil comme non conforme lorsque le code d'accès n'est pas conforme. consultez la section Stratégie de code secret.

Désactivation de l'impression sur les appareils avec profil de travail Android Enterprise ou les appareils entièrement gérés

Dans la stratégie de restrictions, le paramètre **Interdire l'impression** vous permet de spécifier si les utilisateurs peuvent imprimer sur n'importe quelle imprimante accessible à partir de l'appareil Android Enterprise. Consultez Paramètres Android Enterprise.

Autoriser les applications sur des appareils dédiés en ajoutant leur nom de package dans la stratégie kiosque

Vous pouvez maintenant entrer le nom du package que vous souhaitez autoriser sur la plateforme Android Enterprise. Consultez Paramètres Android Enterprise.

Gérer les fonctionnalités de keyguard pour le profil de travail Android Enterprise et les appareils entièrement gérés

Le keyguard Android gère l'appareil et les challenges d'écran de verrouillage des profils professionnels. Utilisez la stratégie d'appareil Gestion du keyguard pour contrôler :

- Gestion du keyguard sur les appareils avec profil de travail. Vous pouvez spécifier les fonctionnalités disponibles pour les utilisateurs avant qu'ils déverrouillent le keyguard de l'appareil et le keyguard de challenge professionnel. Par exemple, par défaut, les utilisateurs peuvent utiliser le déverrouillage par empreinte digitale et afficher les notifications non censurées sur l'écran de verrouillage. Vous pouvez également utiliser la stratégie Gestion du keyguard pour désactiver toute authentification biométrique pour les appareils exécutant Android 9.0 et versions ultérieures.
- Gestion du keyguard sur des appareils entièrement gérés et dédiés. Vous pouvez spécifier les fonctionnalités disponibles, telles que les agents de confiance et la caméra sécurisée, avant qu'ils déverrouillent l'écran du keyguard. Ou, vous pouvez choisir de désactiver toutes les fonctionnalités du keyguard.

Consultez Stratégie Gestion du keyguard.

Publier des applications d'entreprise pour Android Enterprise dans la console XenMobile

Vous n'avez plus besoin de vous inscrire à un compte développeur Google Play lorsque vous ajoutez une application privée Android Enterprise. La console XenMobile ouvre une interface utilisateur Google Play Store d'entreprise pour que vous puissiez charger et publier le fichier APK. Pour de plus amples informations, consultez la section Ajouter une application d'entreprise.

Publier des applications Web pour Android Enterprise dans la console XenMobile

Vous n'avez plus besoin d'accéder à Google Play d'entreprise ou au portail Google Developer pour publier des applications Web Android Enterprise pour XenMobile. Lorsque vous cliquez sur **Charger** dans **Configurer > Applications > Lien Web**, une interface utilisateur Google Play Store d'entreprise s'ouvre pour que vous puissiez charger et enregistrer le fichier. L'approbation et la publication des applications prennent environ 10 minutes. Pour plus d'informations, consultez Ajouter un lien Web.

Effectuer un chargement groupé de certificats sur des appareils iOS avec l'API REST de XenMobile Server

Si le chargement de certificats un par un n'est pas pratique, utilisez l'API REST de XenMobile Server pour charger les certificats sur des appareils iOS de façon groupée.

1. Configurez une stratégie VPN iOS avec le type de connexion **Toujours sur IKEv2**.
2. Sélectionnez **Certificat d'appareil basé sur l'identité de l'appareil** comme méthode d'authentification d'appareil.
3. Sélectionnez le **type d'identité de l'appareil** à utiliser.
4. Importez de façon groupée vos certificats d'appareil à l'aide de l'API REST.

Pour plus d'informations sur la configuration de la stratégie VPN, consultez la section Stratégie VPN. Pour plus d'informations sur l'importation groupée de certificats, consultez la section Effectuer un chargement groupé de certificats sur des appareils iOS avec l'API REST.

Actualiser les clés de cryptage

L'option **Actualiser les clés de cryptage** a été ajoutée dans les paramètres avancés de l'interface de ligne de commande XenMobile. Vous pouvez utiliser cette option pour actualiser les clés de cryptage un nœud à la fois. Consultez la section Options système.

Prise en charge d'ESXi 7.0

Avec cette version, XenMobile prend en charge VMware ESXi 7.0. Assurez-vous de mettre à niveau vers la version 10.13 avant d'installer ou de mettre à niveau ESXi 7.0.

Nouvelles propriétés de serveur

Les propriétés de serveur suivantes sont désormais disponibles :

- **Allow hostnames for iOS App Store links :** pour ajouter des applications de magasin d'applications publiques pour iOS à l'aide des API publiques plutôt que de la console, configurez une liste de noms d'hôtes autorisés si vous le souhaitez.
- **Local user account lockout limit :** configurez le nombre de tentatives de connexion d'un utilisateur local avant que son compte ne soit verrouillé.
- **Local user account lockout time :** configurez combien de temps un utilisateur local est verrouillé après trop de tentatives de connexion échouées.
- **Maximum size of file upload restriction enabled :** activez la restriction de la taille maximale de fichier pour les fichiers chargés.
- **Maximum size of file upload allowed :** définissez la taille maximale de fichier pour les fichiers chargés.

Pour plus d'informations sur ces propriétés, consultez la section Propriétés du serveur.

Nettoyage de disque en libre-service

Une nouvelle option d'interface de ligne de commande appelée **Utilisation du disque** est disponible dans le **menu Dépannage**. Cette option vous permet de voir une liste des fichiers d'image mémoire et des fichiers de pack de support. Après avoir consulté la liste, vous pouvez choisir de supprimer tous ces fichiers via la ligne de commande. Pour plus d'informations sur les outils d'interface de ligne de commande, consultez la section Options d'interface de ligne de commande.

Nouveautés dans XenMobile Server 10.12

January 10, 2022

XenMobile Server 10.12 (PDF)

XenMobile Migration Service

Si vous utilisez une installation locale de XenMobile Server, notre service de migration de XenMobile (XenMobile Migration Service) gratuit peut vous aider à démarrer avec Endpoint Management. La migration de XenMobile Server vers Citrix Endpoint Management ne nécessite pas de réinscrire les appareils.

Pour démarrer la migration, contactez votre représentant ou partenaire Citrix local. Pour plus d'informations, consultez la section XenMobile Migration Service.

Annonces de fin de prise en charge

Pour plus d'informations sur les fonctionnalités Citrix XenMobile qui vont disparaître, consultez la section Fin de prise en charge.

Préparer vos appareils Android pour les changements à venir

Ces annonces de fin de prise en charge communiquées précédemment ont un impact sur vos appareils Android et Android Enterprise :

- Inscriptions d'administrateur d'appareils pour Android 10 :
  - **31 juillet 2020 :** Citrix cesse de prendre en charge les nouvelles inscriptions pour le mode d'administration des appareils Android d'ancienne génération.

  - **1er novembre 2020 :** Google cesse de prendre en charge l'API d'administration des appareils d'ancienne génération. Les appareils Android 10 fonctionnant en mode d'administration des appareils d'ancienne génération ne fonctionneront plus.
- Cryptage MDX :
  - **1er août 2020 :** Citrix commence à appliquer la migration du cryptage MDX vers le cryptage de plate-forme pour les applications de productivité mobiles Citrix et les applications MDX tierces.
  - **1er septembre 2020 :** le cryptage MDX atteint sa fin de vie.

Pour les appareils inscrits au mode d'administration d'ancienne génération

- Si vous n'utilisez pas le cryptage MDX, aucune action n'est requise.
- Si vous utilisez le cryptage MDX, migrez les appareils Android vers Android Enterprise avant le 31 juillet 2020. Les appareils exécutant Android 10 doivent s'inscrire ou se réinscrire à l'aide d'Android Enterprise. Cette exigence inclut les appareils Android en mode MAM uniquement. Consultez la section Migrer de l'administration des appareils vers Android Enterprise.

Pour les appareils déjà inscrits à Android Enterprise le 31 juillet

- Si vous avez publié les applications à l'aide de la plate-forme Android Enterprise, le cryptage est déjà géré via Android Enterprise. Aucune action requise.
- Si vous avez publié les applications à l'aide de l'ancienne plate-forme Android, republiez-les à l'aide d'Android Enterprise avant le 31 juillet 2020.

Avant de procéder à la mise à niveau vers XenMobile 10.12 (sur site)

Certaines configurations système requises ont été modifiées. Pour plus d'informations, consultez la section Configuration système requise et compatibilité et Compatibilité XenMobile.

1. Mettez à jour votre serveur de licences Citrix vers la version 11.16 ou version ultérieure avant la mise à jour vers la dernière version de XenMobile Server 10.12.

   La dernière version de XenMobile requiert le serveur de licences Citrix 11.16 (version minimale).

   > **Remarque :**
   >
   > Si vous souhaitez utiliser votre propre licence pour la version préliminaire, sachez que la date Customer Success Services (anciennement la date Subscription Advantage) dans XenMobile 10.12 est le 20 janvier 2020. La date Customer Success Services sur votre licence Citrix doit être postérieure à cette date.
   >
   > Vous pouvez visualiser la date en regard de la licence dans le serveur de licences. Si vous connectez la dernière version de XenMobile à un environnement de serveur de licences

> plus ancien, la vérification de la connectivité échoue et vous ne pouvez pas configurer le serveur de licences.

Pour renouveler la date sur votre licence, téléchargez le dernier fichier de licence à partir du portail Citrix, puis téléchargez-le sur le serveur de licences. Pour plus d'informations, consultez Customer Success Services.

2. Pour un environnement en cluster, la configuration requise pour les déploiements de stratégies et d'applications iOS sur des appareils exécutant iOS 11 ou version ultérieure est la suivante. Si Citrix Gateway est configuré pour la persistance SSL, vous devez ouvrir le port 80 sur tous les nœuds de XenMobile Server.
3. Si la machine virtuelle exécutant le serveur XenMobile à mettre à niveau a moins de 4 Go de RAM, augmentez la mémoire vive à 4 Go au minimum. Veuillez noter que la mémoire RAM minimum recommandée est 8 Go pour les environnements de production.
4. Avant d'installer une mise à jour XenMobile, utilisez les fonctions de votre machine virtuelle pour prendre un instantané de votre système. Sauvegardez aussi la base de données de configuration de votre système. Si vous rencontrez des problèmes durant une mise à niveau, des copies de sauvegarde complètes vous permettent de récupérer.

Pour effectuer la mise à niveau

Vous pouvez effectuer une mise à niveau directement vers XenMobile 10.12 depuis XenMobile 10.11.x ou 10.10.x. Pour effectuer la mise à niveau, téléchargez le dernier fichier binaire disponible en accédant à https://www.citrix.com/downloads. Accédez à **Citrix Endpoint Management (XenMobile) > XenMobile Server > Produit logiciel > XenMobile Server 10**. Sur la vignette du logiciel XenMobile Server de votre hyperviseur, cliquez sur **Télécharger le fichier**.

Pour télécharger la mise à niveau, utilisez la page **Gestion des versions** dans la console XenMobile. Pour plus d'informations, consultez Pour mettre à niveau depuis la page Gestion des versions.

Après la mise à niveau

Après la mise à niveau vers XenMobile 10.12 (sur site)

Si une fonctionnalité utilisant des connexions sortantes cesse de fonctionner alors que vous n'avez pas changé la configuration de vos connexions, vérifiez dans le journal de XenMobile Server s'il existe des erreurs telle que la suivante : « Impossible de se connecter au serveur VPP : le nom d'hôte 192.0.2.0 ne correspond pas au sujet du certificat fourni par l'homologue. »

L'erreur de validation du certificat indique que vous devez désactiver la vérification de nom d'hôte sur XenMobile Server. Par défaut, la vérification de nom d'hôte est activée sur les connexions sortantes à l'exception du serveur PKI de Microsoft. Si la vérification de nom d'hôte interrompt votre

déploiement, définissez la propriété de serveur `disable.hostname.verification` sur **`true`**. La valeur par défaut de cette propriété est **`false`**.

Prise en charge supplémentaire pour iOS 13

XenMobile Server prend en charge les appareils mis à niveau vers iOS 13. La mise à niveau affecte vos utilisateurs comme suit :

- Pendant l'inscription, de nouveaux écrans Option de l'assistant d'installation iOS apparaissent. Apple a ajouté de nouveaux écrans Options de l'assistant d'installation iOS à iOS 13. Les nouvelles options sont incluses dans la page **Paramètres > Programme d'inscription des appareils (DEP) Apple** de cette version. Vous pouvez configurer XenMobile Server pour ignorer ces écrans. Ces pages apparaissent pour les utilisateurs sur les appareils iOS 13.
- Certains paramètres de stratégie de restrictions qui étaient disponibles sur les appareils supervisés ou non supervisés pour les versions précédentes d'iOS ne sont disponibles que sur les appareils supervisés pour iOS 13+. Les info-bulles actuelles de la console XenMobile Server n'indiquent pas encore que ces paramètres s'appliquent uniquement aux appareils supervisés pour iOS 13+.
  - Autoriser le contrôle du matériel :
    - FaceTime
    - Installation d'applications
  - Autoriser les applications :
    - iTunes Store
    - Safari
    - Safari > Remplissage automatique
  - Réseau - Autoriser les actions iCloud :
    - Documents et données iCloud
  - Paramètres supervisés uniquement - Autoriser :
    - Game Center > Ajouter des amis
    - Game Center > Jeux multijoueurs
  - Contenu multimédia - Autoriser :
    - Musique, podcasts et cours iTunes U explicites

Ces restrictions s'appliquent comme suit :

- Si un appareil iOS 12 (ou version antérieure) est déjà inscrit dans XenMobile Server, puis passe à iOS 13, les restrictions précédentes s'appliquent aux appareils non supervisés et supervisés.
- Si un appareil iOS 13 ou version supérieure non supervisé est inscrit dans XenMobile Server, les restrictions précédentes s'appliquent uniquement aux appareils supervisés.
- Si un appareil iOS13 ou version supérieure supervisé est inscrit dans XenMobile Server, les restrictions précédentes s'appliquent uniquement aux appareils supervisés.

Migration du programme d'achat en volume d'Apple vers Apple Business Manager (ABM) et Apple School Manager (ASM)

Les entreprises et les institutions qui utilisent le Programme d'achat en volume (VPP) d'Apple doivent migrer vers les applications et les livres d'Apple Business Manager ou d'Apple School Manager avant le 1er décembre 2019.

Avant de migrer des comptes VPP dans XenMobile, consultez cet article de l'assistance Apple.

Si votre organisation ou votre établissement utilise uniquement le programme d'achat en volume (VPP), vous pouvez vous inscrire à ABM/ASM, puis inviter les acheteurs VPP existants à accéder à votre nouveau compte ABM/ASM. Pour ASM, accédez à https://school.apple.com. Pour ABM, accédez à https://business.apple.com.

Pour mettre à jour votre compte VPP sur XenMobile :

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Paramètres iOS**. La page de configuration **Programme d'achat en volume** s'affiche.
3. Assurez-vous que votre compte ABM ou ASM présente la même configuration d'applications que votre compte VPP précédent.
4. Dans le portail ABM ou ASM, téléchargez un jeton mis à jour.
5. Dans la console XenMobile, procédez comme suit :
    a) Modifiez le compte d'achat en volume existant avec les informations du jeton mis à jour pour cet emplacement.
    b) Modifiez vos informations d'identification ABM ou ASM. Ne modifiez pas le suffixe.
    c) Cliquez deux fois sur **Enregistrer**.

Pour plus d'informations, consultez :

- Programme de déploiement d'Apple
- Inscription en bloc d'appareils Apple

Prise en charge des appareils Android Enterprise COPE

XenMobile Server prend en charge les appareils Android Enterprise entièrement gérés avec profil de travail, anciennement appelés appareils COPE (propriété de l'entreprise avec accès privé). Ces appareils sont un type d'appareils Android Enterprise entièrement gérés qui ont également un profil de travail. Vous pouvez appliquer des paramètres de stratégie distincts à l'appareil et au profil de travail. Pour cette version :

- Vous pouvez appliquer des paramètres distincts à l'appareil et au profil de travail à l'aide des stratégies suivantes : Informations d'identification, Code secret et Restrictions.
- Vous pouvez appliquer le paramètre de mode de localisation de la stratégie d'emplacement à l'appareil COPE lui-même, mais pas au profil de travail de l'appareil COPE. Les autres paramètres de la stratégie d'emplacement ne sont pas disponibles pour les appareils COPE.
- Vous pouvez appliquer l'action de sécurisation Verrouiller séparément à l'appareil ou au profil de travail.

Stratégies d'appareil

Pour les appareils Android Enterprise entièrement gérés avec profil de travail (appareils COPE), vous pouvez utiliser certaines stratégies pour appliquer des paramètres distincts à l'ensemble de l'appareil et au profil de travail. Dans la console XenMobile Server, certaines stratégies vous permettent d'appliquer des paramètres distincts. Vous pouvez utiliser d'autres stratégies pour appliquer des paramètres uniquement à l'ensemble de l'appareil ou uniquement au profil de travail des appareils entièrement gérés avec profil de travail.

Actions de sécurisation

Pour les appareils Android Enterprise entièrement gérés avec profil de travail (appareils COPE), vous pouvez appliquer :

- l'action de sécurisation Verrouiller séparément à l'appareil ou au profil de travail ;
- toutes les autres actions de sécurité sur l'appareil.

Les profils d'inscription contrôlent les options d'inscription pour les appareils Android

Les profils d'inscription contrôlent désormais la façon dont les appareils Android sont inscrits si Android Entreprise est activé pour votre déploiement XenMobile. Les profils d'inscription déterminent si les appareils Android sont inscrits en mode Android Entreprise par défaut (profil entièrement géré ou professionnel) ou en mode d'ancienne génération (administrateur de l'appareil).

Par défaut, le profil d'inscription global inscrit les nouveaux appareils Android Entreprise et les appareils soumis à une réinitialisation d'usine en tant qu'appareils entièrement gérés et les appareils Android Entreprise BYOD en tant qu'appareils avec profil de travail. Pour plus d'informations, consultez la section Android Enterprise.

Préparation d'appareils Android d'ancienne génération pour Android Entreprise dans le cadre d'une inscription par défaut

Google va mettre fin à la prise en charge du mode Administrateur de l'appareil et encourage les clients à gérer tous les appareils Android en mode Propriétaire de l'appareil ou Propriétaire du profil. (Voir

Fin de prise en charge du mode Administrateur de l'appareil dans les guides du développeur Google Android Entreprise.) Pour prendre en charge cette modification, Android Entreprise est maintenant l'option d'inscription par défaut pour les appareils Android.

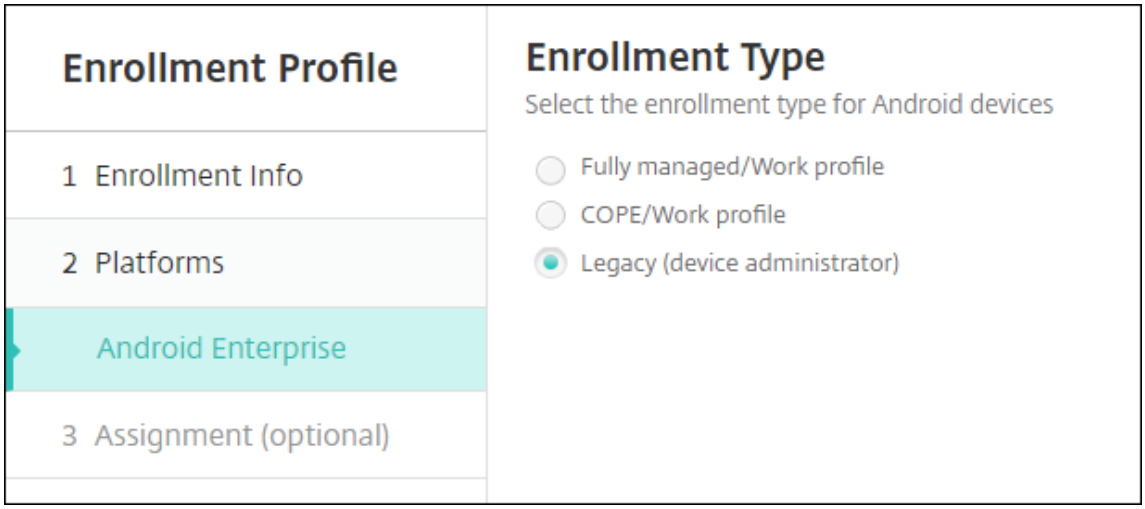
Cette modification signifie que si Android Entreprise est activé pour votre déploiement XenMobile, tous les appareils Android nouvellement inscrits ou réinscrits le sont en tant qu'appareils Android Entreprise.

Pour préparer cette modification, XenMobile vous permet désormais de créer des profils d'inscription qui contrôlent la façon dont les appareils Android sont inscrits.

Votre organisation n'est peut-être pas prête à gérer les appareils Android d'ancienne génération en mode Propriétaire de l'appareil ou Propriétaire du profil. Dans ce cas, vous pouvez continuer à les gérer en mode Administrateur de l'appareil. Créez un profil d'inscription pour les appareils d'ancienne génération et réinscrivez tous les appareils d'ancienne génération inscrits.

Pour créer un profil d'inscription pour les appareils d'ancienne génération :

1. Dans la console XenMobile, accédez à **Configurer > Profils d'inscription**.
2. Pour ajouter un profil d'inscription, cliquez sur **Ajouter**. Sur la page Infos d'inscription, entrez un nom pour le profil d'inscription.
3. Cliquez sur **Suivant** ou sélectionnez **Android Enterprise** sous **Plates-formes**. La page Configuration de l'inscription s'affiche.
4. Définissez **Gestion** sur **Administration des appareils d'ancienne génération**. Cliquez sur **Suivant** ou sélectionnez **Attribution (facultatif)**. L'écran Attribution de groupes de mise à disposition s'affiche.



5. Choisissez le(s) groupe(s) de mise à disposition contenant les administrateurs qui inscrivent les appareils dédiés. Cliquez ensuite sur **Enregistrer**.

Pour continuer à gérer les appareils d'ancienne génération en mode Administrateur de l'appareil, inscrivez-les ou réinscrivez-les à l'aide de ce profil. Inscrivez les appareils en mode Administrateur de l'appareil de la même manière que les appareils en mode Profil de travail, en demandant aux utilisateurs de télécharger Secure Hub et en fournissant une URL de serveur d'inscription.

Pour plus d'informations sur la prise en charge de Endpoint Management pour la transition vers Android Enterprise, consultez le blog Android Enterprise par défaut pour le service Citrix Endpoint Management.

Gestion simplifiée des applications pour Android Enterprise

Vous n'avez plus besoin d'accéder à Google Play d'entreprise ou au portail Google Developer pour approuver ou publier des applications pour XenMobile Server. Par conséquent, l'approbation et la publication des applications prennent environ 10 minutes plutôt que des heures.

Approuver les applications Android Enterprise pour le magasin d'applications public dans la console XenMobile Server. Vous pouvez désormais approuver les applications Google Play Store d'entreprise sans quitter la console XenMobile Server. Après avoir entré un nom d'application dans le champ de recherche, l'interface utilisateur Google Play Store d'entreprise s'ouvre avec les instructions pour approuver et enregistrer l'application. Votre application renseigne ensuite les résultats, ce qui vous permet de configurer les détails. Voir Ajouter une application d'un magasin d'applications public.

Ajouter des applications MDX pour Android Enterprise. La console XenMobile Server prend désormais en charge Android Enterprise en tant que plate-forme pour le déploiement d'applications MDX. Consultez la section Ajouter une application MDX.

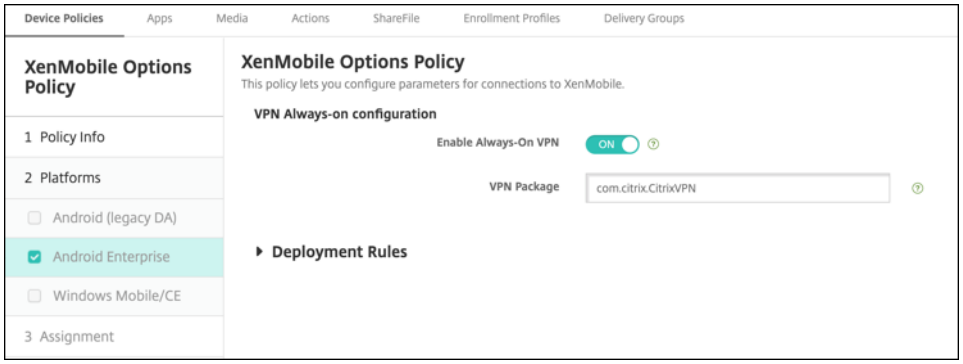
Approuver les applications MDX pour Android Enterprise dans la console XenMobile Server. Vous pouvez désormais approuver les applications Google Play Store d'entreprise pour Android Enterprise sans quitter la console XenMobile Server. Une fois un fichier MDX chargé, l'interface utilisateur Google Play Store d'entreprise s'ouvre avec les instructions vous permettant d'approuver et d'enregistrer l'application. Voir Ajouter une application MDX.

Prise en charge de VPN Always On pour Android Enterprise

La stratégie d'options XenMobile Server vous permet désormais d'activer le paramètre VPN Always On pour Android Enterprise.

Lorsque vous configurez des profils VPN pour Android Enterprise, entrez le nom du profil VPN dans le champ **Profil VPN par défaut**. XenMobile utilise ce profil lorsque les utilisateurs touchent le bouton de connexion dans l'interface utilisateur de l'application Citrix SSO au lieu de toucher un profil spécifique. Si ce champ est vide, le profil principal est utilisé pour la connexion. Si un seul profil est

configuré, il est marqué comme profil par défaut. Pour un VPN Always On, ce champ doit être défini sur le nom du profil VPN à utiliser pour établir un VPN Always On.



Configurez le suivi du produit pour vos applications Android Entreprise

Lors de l'ajout d'une application de magasin public ou d'une application MDX pour Android Entreprise, configurez le suivi du produit que vous souhaitez transférer sur les appareils utilisateur. Par exemple, si vous avez un suivi conçu pour les tests, vous pouvez le sélectionner et l'affecter à un groupe de mise à disposition spécifique. Pour en savoir plus sur le déploiement de votre version, consultez le Centre d'aide Google Play. Pour de plus amples informations sur la configuration du suivi du produit, consultez la section Ajouter une application MDX ou Ajouter une application d'un magasin d'applications public.

Forcer une réinitialisation du code secret pour les utilisateurs de macOS

Lorsqu'un appareil macOS reçoit un profil de configuration avec une stratégie de code secret, les utilisateurs doivent fournir un code secret conforme aux paramètres de stratégie. Vous pouvez désormais forcer la réinitialisation du code secret la prochaine fois qu'un utilisateur s'authentifie. Dans la stratégie de code secret pour macOS (10.13 et versions ultérieures), activez le nouveau paramètre **Forcer la réinitialisation du code d'accès**. Pour plus d'informations sur la stratégie, consultez Stratégie de code secret.

Nouveautés dans XenMobile Server 10.11

January 10, 2022

XenMobile Server 10.11 (PDF)

XenMobile Migration Service

Si vous utilisez une installation locale de XenMobile Server, notre service de migration de XenMobile (XenMobile Migration Service) gratuit peut vous aider à démarrer avec Endpoint Management. La migration de XenMobile Server vers Citrix Endpoint Management ne nécessite pas de réinscrire les appareils.

Pour démarrer la migration, contactez votre représentant ou partenaire Citrix local. Pour plus d'informations, consultez la section XenMobile Migration Service.

Migration du programme d'achat en volume d'Apple vers Apple Business Manager (ABM) et Apple School Manager (ASM)

Les entreprises et les institutions qui utilisent le Programme d'achat en volume (VPP) d'Apple doivent migrer vers les applications et les livres d'Apple Business Manager ou d'Apple School Manager avant le 1er décembre 2019.

Avant de migrer des comptes VPP dans XenMobile, consultez cet article de l'assistance Apple.

Si votre organisation ou votre établissement utilise uniquement le programme d'achat en volume (VPP), vous pouvez vous inscrire à ABM/ASM, puis inviter les acheteurs VPP existants à accéder à votre nouveau compte ABM/ASM. Pour ASM, accédez à https://school.apple.com. Pour ABM, accédez à https://business.apple.com.

Pour mettre à jour votre compte d'achat en volume (anciennement VPP) sur XenMobile :

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Achat en volume**. La page de configuration de **l'achat en volume** s'affiche.
3. Assurez-vous que votre compte ABM ou ASM présente la même configuration d'applications que votre compte VPP précédent.
4. Dans le portail ABM ou ASM, téléchargez un jeton mis à jour.
5. Dans la console XenMobile, procédez comme suit :
    a) Modifiez le compte d'achat en volume existant avec les informations du jeton mis à jour pour cet emplacement.
    b) Modifiez vos informations d'identification ABM ou ASM. Ne modifiez pas le suffixe.
    c) Cliquez deux fois sur **Enregistrer**.

Prise en charge supplémentaire pour iOS 13

> **Important :**
>
> Pour préparer les mises à niveau des appareils vers iOS 12+ : le type de connexion VPN Citrix dans la stratégie VPN pour iOS ne prend pas en charge iOS 12+. Supprimez votre stratégie VPN et créez une nouvelle stratégie VPN avec le type de connexion Citrix SSO.
>
> La connexion VPN Citrix continue de fonctionner sur les appareils précédemment déployés après la suppression de la stratégie VPN. Votre nouvelle configuration de stratégie VPN prend effet dans XenMobile Server 10.11 lors de l'inscription de l'utilisateur.

XenMobile Server prend en charge les appareils mis à niveau vers iOS 13. La mise à niveau affecte vos utilisateurs comme suit :

- Pendant l'inscription, de nouveaux écrans Option de l'assistant d'installation iOS apparaissent. Apple a ajouté de nouveaux écrans Options de l'assistant d'installation iOS à iOS 13. Les nouvelles options ne sont pas incluses dans la page **Paramètres > Programme d'inscription des appareils (DEP) Apple** de cette version. Par conséquent, vous ne pouvez pas configurer XenMobile Server pour ignorer ces écrans. Ces pages apparaissent pour les utilisateurs sur les appareils iOS 13.
- Certains paramètres de stratégie de restrictions qui étaient disponibles sur les appareils supervisés ou non supervisés pour les versions précédentes d'iOS ne sont disponibles que sur les appareils supervisés pour iOS 13+. Les info-bulles actuelles de la console XenMobile Server n'indiquent pas encore que ces paramètres s'appliquent uniquement aux appareils supervisés pour iOS 13+.
  - Autoriser le contrôle du matériel :
    - FaceTime
    - Installation d'applications
  - Autoriser les applications :
    - iTunes Store
    - Safari
    - Safari > Remplissage automatique
  - Réseau - Autoriser les actions iCloud :
    - Documents et données iCloud
  - Paramètres supervisés uniquement - Autoriser :
    - Game Center > Ajouter des amis
    - Game Center > Jeux multijoueurs
  - Contenu multimédia - Autoriser :
    - Musique, podcasts et cours iTunes U explicites

Ces restrictions s'appliquent comme suit :

- Si un appareil iOS 12 (ou version antérieure) est déjà inscrit dans XenMobile Server, puis passe à iOS 13, les restrictions précédentes s'appliquent aux appareils non supervisés et supervisés.

- Si un appareil iOS 13 ou version supérieure non supervisé est inscrit dans XenMobile Server, les restrictions précédentes s'appliquent uniquement aux appareils supervisés.
- Si un appareil iOS13 ou version supérieure supervisé est inscrit dans XenMobile Server, les restrictions précédentes s'appliquent uniquement aux appareils supervisés.

Configuration requise pour les certificats de confiance dans iOS 13 et macOS 15

Apple a introduit de nouvelles exigences pour les certificats de serveur TLS. Vérifiez que tous les certificats respectent les nouvelles exigences d'Apple. Consultez la publication Apple, https://support.apple.com/en-us/HT210176. Pour obtenir de l'aide sur la gestion des certificats, consultez la section Chargement de certificats dans XenMobile.

Mise à niveau de GCM vers FCM

Depuis le 10 avril 2018, Google ne prend plus en charge Google Cloud Messaging (GCM). Google a supprimé les API client et serveur GCM le 29 mai 2019.

> **Exigences importantes :**
>
> - Mettez à niveau vers la version la plus récente de XenMobile Server.
> - Mettez à niveau vers la version la plus récente de Secure Hub.

Google recommande la mise à niveau immédiate vers Firebase Cloud Messaging (FCM) pour commencer à profiter des nouvelles fonctionnalités disponibles dans FCM. Pour plus d'informations sur Google, consultez https://developers.google.com/cloud-messaging/faq et https://firebase.googleblog.com/2018/04/time-to-upgrade-from-gcm-to-fcm.html.

Pour continuer à prendre en charge les notifications push sur vos appareils Android : si vous utilisez GCM avec XenMobile Server, migrez vers FCM. Ensuite, mettez à jour XenMobile Server avec la nouvelle clé FCM disponible depuis la console Firebase Cloud Messaging.

Les étapes suivantes reflètent le workflow d'inscription lorsque vous utilisez des certificats de confiance.

Étapes de mise à niveau :

1. Suivez les informations fournies par Google pour passer de GCM à FCM.
2. Dans la console Firebase Cloud Messaging, copiez votre nouvelle clé FCM. Vous en aurez besoin pour l'étape suivante.
3. Dans la console XenMobile Server, accédez à **Paramètres > Firebase Cloud Messaging** et configurez vos paramètres.

Les appareils passent à FCM la prochaine fois qu'ils se connectent avec XenMobile Server et actualisent la stratégie. Pour forcer Secure Hub à actualiser les stratégies : dans Secure Hub, accédez

à **Préférences > Informations sur l'appareil**, puis appuyez sur **Actualiser la stratégie**.
Pour plus d'informations sur la configuration de FCM, consultez Firebase Cloud Messaging.

XenMobile Migration Service

Si vous utilisez une installation locale de XenMobile Server, notre service de migration de XenMobile (XenMobile Migration Service) peut vous aider à démarrer avec Endpoint Management. La migration de XenMobile Server vers Citrix Endpoint Management ne nécessite pas de réinscrire les appareils.

Pour plus d'informations, contactez votre représentant Citrix, votre ingénieur système ou votre partenaire Citrix local. Ces blogs traitent du service de migration de XenMobile :

Nouveau service de migration de XenMobile

Avantages de XenMobile dans le Cloud

Avant de mettre à niveau vers XenMobile 10.11 (sur site)

Certaines configurations système requises ont été modifiées. Pour plus d'informations, consultez la section Configuration système requise et compatibilité et Compatibilité XenMobile.

1. Mettez à jour votre serveur de licences Citrix vers la version 11.15 ou version ultérieure avant la mise à jour vers la dernière version de XenMobile Server 10.11.

   La dernière version de XenMobile requiert le serveur de licences Citrix 11.15 (version minimale).

   > **Remarque :**
   >
   > Si vous souhaitez utiliser votre propre licence pour la version préliminaire, sachez que la date Customer Success Services (anciennement la date Subscription Advantage) dans XenMobile 10.11 est le 9 avril 2019. La date Customer Success Services sur votre licence Citrix doit être postérieure à cette date.
   >
   > Vous pouvez visualiser la date en regard de la licence dans le serveur de licences. Si vous connectez la dernière version de XenMobile à un environnement de serveur de licences plus ancien, la vérification de la connectivité échoue et vous ne pouvez pas configurer le serveur de licences.

   Pour renouveler la date sur votre licence, téléchargez le dernier fichier de licence à partir du portail Citrix, puis téléchargez-le sur le serveur de licences. Pour plus d'informations, consultez Customer Success Services.

2. Pour un environnement en cluster, la configuration requise pour les déploiements de stratégies et d'applications iOS sur des appareils exécutant iOS 11 ou version ultérieure est la suivante. Si Citrix Gateway est configuré pour la persistance SSL, vous devez ouvrir le port 80 sur tous les nœuds de XenMobile Server.

3. Si la machine virtuelle exécutant le serveur XenMobile à mettre à niveau a moins de 4 Go de RAM, augmentez la mémoire vive à 4 Go au minimum. Veuillez noter que la mémoire RAM minimum recommandée est 8 Go pour les environnements de production.
4. Avant d'installer une mise à jour XenMobile, utilisez les fonctions de votre machine virtuelle pour prendre un instantané de votre système. Sauvegardez aussi la base de données de configuration de votre système. Si vous rencontrez des problèmes durant une mise à niveau, des copies de sauvegarde complètes vous permettent de récupérer.

Pour effectuer la mise à niveau

Vous pouvez effectuer une mise à niveau directement vers XenMobile 10.11 depuis XenMobile 10.10.x ou 10.9.x. Pour effectuer la mise à niveau, téléchargez le dernier fichier binaire disponible en accédant à https://www.citrix.com/downloads. Accédez à **Citrix Endpoint Management (et Citrix XenMobile Server) > XenMobile Server (local) > Logiciel produit > XenMobile Server 10**. Sur la vignette du logiciel XenMobile Server de votre hyperviseur, cliquez sur **Télécharger le fichier**.

Pour télécharger la mise à niveau, utilisez la page **Gestion des versions** dans la console XenMobile. Pour plus d'informations, consultez Pour mettre à niveau depuis la page Gestion des versions.

Après la mise à niveau

Après la mise à niveau vers XenMobile 10.11 (sur site)

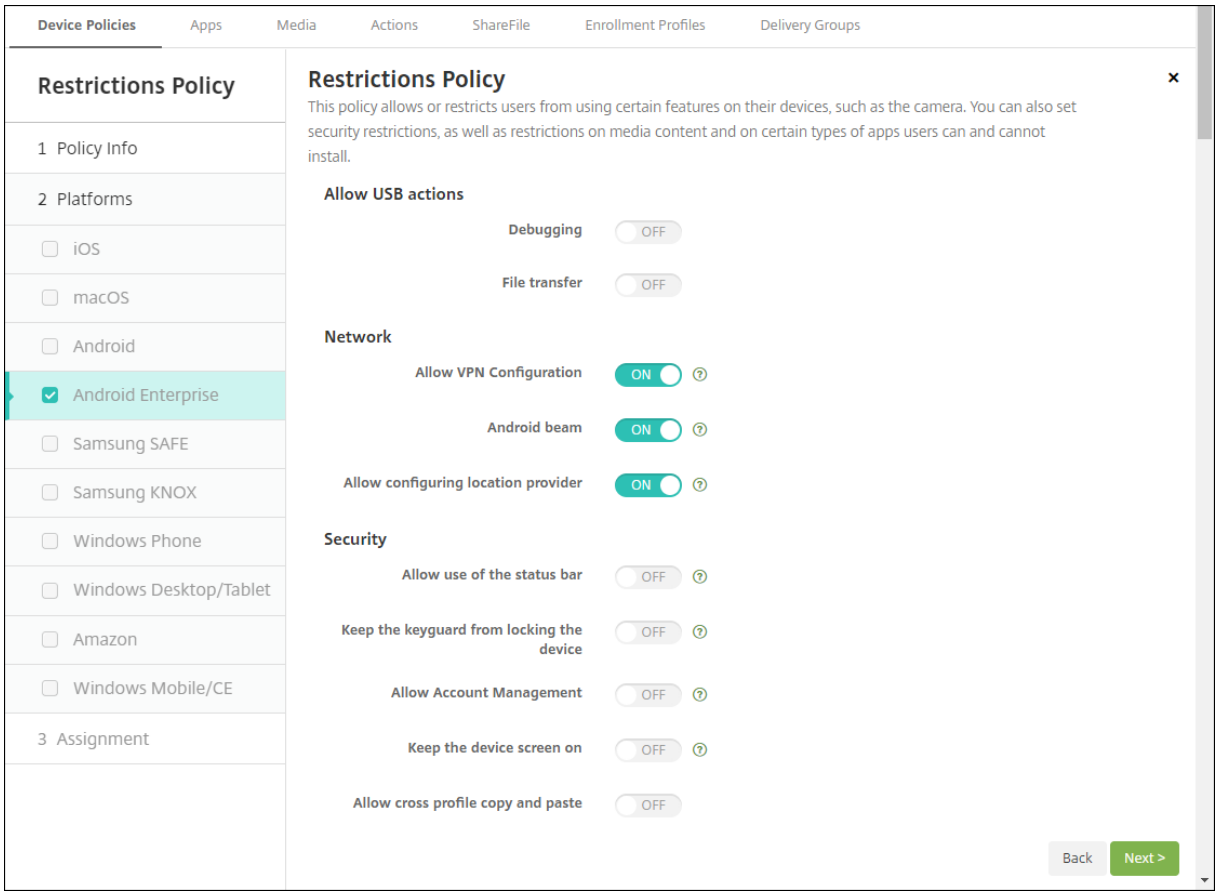
Si une fonctionnalité utilisant des connexions sortantes cesse de fonctionner alors que vous n'avez pas changé la configuration de vos connexions, vérifiez dans le journal de XenMobile Server s'il existe des erreurs telle que la suivante : « Impossible de se connecter au serveur VPP : le nom d'hôte 192.0.2.0 ne correspond pas au sujet du certificat fourni par l'homologue. »

L'erreur de validation du certificat indique que vous devez désactiver la vérification de nom d'hôte sur XenMobile Server. Par défaut, la vérification de nom d'hôte est activée sur les connexions sortantes à l'exception du serveur PKI de Microsoft. Si la vérification de nom d'hôte interrompt votre déploiement, définissez la propriété de serveur `disable.hostname.verification` sur **`true`**. La valeur par défaut de cette propriété est **`false`**.

Nouveaux paramètres de stratégie et paramètres de stratégie mis à jour pour les appareils Android Enterprise

Unification des stratégies Samsung Knox et Android Enterprise : pour les appareils Android Enterprise exécutant Samsung Knox 3.0 ou version ultérieure et Android 8.0 ou version ultérieure, Knox et Android Enterprise sont combinés en une solution unifiée de gestion des appareils et des profils. Configurez les paramètres Knox sur la page Android Enterprise des stratégies d'appareil suivantes :

- **Stratégie de mise à jour d'OS.** Inclut les paramètres pour les mises à jour de Samsung Enterprise FOTA.
- **Stratégie de code secret.**
- **Stratégie de clé de licence MDM Samsung.** Configure la clé de licence Knox.
- **Paramètres de stratégie Restrictions.**

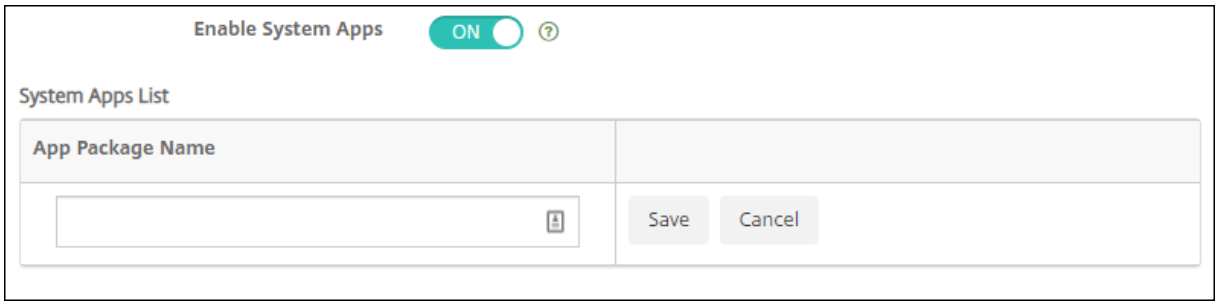


Stratégie d'inventaire des applications pour Android Enterprise : vous pouvez désormais établir un inventaire des applications Android Enterprise sur les appareils gérés. Consultez la section Stratégie d'inventaire des applications.

Accéder à toutes les applications Google Play dans Google Play Store d'entreprise. La propriété de serveur **Accéder à toutes les applications dans Google Play Store d'entreprise** rend toutes les applications du Google Play Store public accessibles depuis Google Play Store d'entreprise. La définition de cette propriété sur **true** autorise les applications du Google Play Store public pour tous les utilisateurs d'Android Enterprise. Les administrateurs peuvent ensuite utiliser la stratégie Restrictions pour contrôler l'accès à ces applications.

Activer les applications système sur les appareils Android Enterprise. pour permettre aux utilisateurs d'exécuter des applications système préinstallées en mode Profil de travail Android Enterprise ou en mode entièrement géré, configurez la stratégie Restrictions. Cette configuration permet à l'utilisateur d'accéder aux applications de l'appareil par défaut, telles que l'appareil photo, la galerie,

etc. Pour restreindre l'accès à une application particulière, définissez les autorisations d'application à l'aide de la stratégie Autorisations applicatives Android Entreprise.



Prise en charge des appareils Android Enterprise dédiés. XenMobile prend désormais en charge la gestion des appareils dédiés, anciennement appelés appareils d'entreprise à usage unique (COSU).

Les appareils Android Enterprise dédiés sont des appareils entièrement gérés qui ne remplissent qu'une seule fonction. En effet, vous limitez ces appareils à une application ou à un petit ensemble d'applications nécessaires pour effectuer les tâches propres à une fonction. Vous pouvez également empêcher les utilisateurs d'activer d'autres applications ou d'effectuer d'autres actions sur l'appareil.

Pour plus d'informations sur le provisionnement d'appareils Android Enterprise, consultez Provisionner des appareils Android Enterprise dédiés.

Stratégie renommée : pour s'aligner sur la terminologie Google, la stratégie de restriction d'application Android Enterprise est désormais appelée Configurations gérées par Android Enterprise. Consultez Stratégie Configurations gérées par Android Entreprise.

Verrouiller et réinitialiser le mot de passe pour Android Enterprise

XenMobile prend désormais en charge l'action de sécurisation Verrouiller et réinitialiser le mot de passe pour les appareils Android Enterprise. Ces appareils doivent être inscrits en mode Profil de travail exécutant Android 8.0 et versions ultérieures.

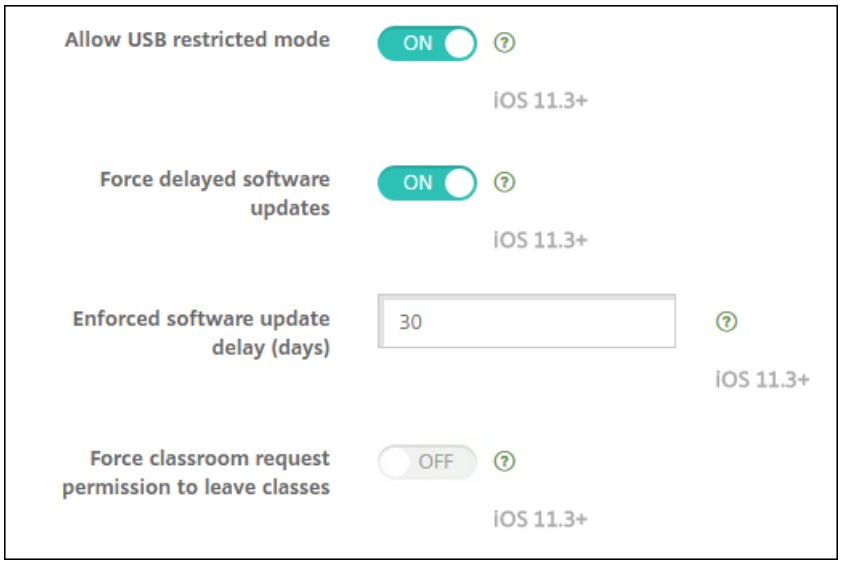
- Le code secret envoyé verrouille le profil de travail. L'appareil n'est pas verrouillé.
- Si aucun code secret n'est envoyé ou si le code secret envoyé ne répond pas aux exigences de code secret :
  - Et si aucun code secret n'est déjà défini sur le profil de travail, l'appareil est verrouillé.
  - Et si un code secret est déjà défini sur le profil de travail, le profil travail est verrouillé, mais l'appareil ne l'est pas.

Pour plus d'informations sur les actions de sécurité de verrouillage et de réinitialisation du mot de passe, consultez la section Actions de sécurité.

Nouveaux paramètres de stratégie Restrictions pour iOS ou macOS

- **Les applications non gérées lisent des contacts gérés :** option facultative. Disponible uniquement si l'option **Documents provenant d'applications gérées dans les applications non gérées** est désactivée. Si cette stratégie est activée, des applications non gérées peuvent lire les données des contacts des comptes gérés. La valeur par défaut est **Désactivé**. Disponible à partir d'iOS 12.
- **Les applications gérées écrivent des contacts non gérés :** option facultative. Si cette option est activée, des applications gérées peuvent écrire des contacts dans les contacts des comptes non gérés. Si l'option **Documents provenant d'applications gérées dans les applications non gérées** est activée, cette restriction n'a aucun effet. La valeur par défaut est **Désactivé**. Disponible à partir d'iOS 12.
- **Remplissage automatique du mot de passe :** option facultative. Si cette option est désactivée, les utilisateurs ne peuvent pas utiliser les fonctionnalités de remplissage automatique de mot de passe ou de mot de passe fort automatique. La valeur par défaut est **Activé**. Disponible à partir d'iOS 12 et macOS 10.14.
- **Requêtes de proximité de mot de passe :** option facultative. Si cette option est désactivée, les appareils des utilisateurs ne demandent pas de mots de passe aux appareils à proximité. La valeur par défaut est **Activé**. Disponible à partir d'iOS 12 et macOS 10.14.
- **Partage de mot de passe :** option facultative. Si cette option est désactivée, les utilisateurs ne peuvent pas partager leurs mots de passe à l'aide de la fonctionnalité Mots de passe AirDrop. La valeur par défaut est **Activé**. Disponible à partir d'iOS 12 et macOS 10.14.
- **Forcer réglage automatique de la date et l'heure :** Supervisé. Si cette option est activée, les utilisateurs ne peuvent pas désactiver l'option **Général > Date et heure > Définir automatiquement**. La valeur par défaut est **Désactivé**. Disponible à partir d'iOS 12.
- **Autoriser le mode restreint USB :** disponible uniquement pour les appareils supervisés. Si cette option est désactivée, l'appareil peut toujours se connecter aux accessoires USB lorsqu'il est verrouillé. La valeur par défaut est **Activé**. Disponible à partir de iOS 11.3.
- **Retarder les mises à jour logicielles :** disponible uniquement pour les appareils supervisés. Si cette option est définie sur **Activé**, elle diffère la visibilité des mises à jour logicielles par les utilisateurs Avec cette restriction en place, l'utilisateur ne voit pas de mise à jour logicielle avant le nombre de jours spécifié après la date de publication de la mise à jour logicielle. La valeur par défaut est **Désactivé**. Disponible à partir d'iOS 11.3 et macOS 10.13.4.
- **Délai imposé pour les mises à jour logicielles (jours) :** disponible uniquement pour les appareils supervisés. Cette restriction permet à l'administrateur de définir le délai pendant lequel retarder une mise à jour logicielle sur l'appareil. La valeur maximale est 90 jours et la valeur par défaut est **30**. Disponible à partir d'iOS 11.3 et macOS 10.13.4.
- **Exiger la permission de En classe pour quitter les classes :** disponible uniquement pour les appareils supervisés. Si cette option est définie sur **Activé**, un élève inscrit à un cours non géré avec En classe doit demander la permission à l'enseignant pour quitter le cours. La valeur par

défaut est **Désactivé**. Disponible à partir de iOS 11.3.



consultez la section Stratégie de restrictions.

Mises à jour de la stratégie Exchange pour iOS ou macOS

Davantage de paramètres de signature et de cryptage S/MIME Exchange sont disponibles à partir d'iOS 12. La stratégie Exchange inclut désormais des paramètres permettant de configurer la signature et le cryptage S/MIME.

Pour la signature S/MIME :

- **Informations d'identification de l'identité de signature :** choisissez les informations d'identification de signature à utiliser.
- **Signature S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer et désactiver la signature S/MIME dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**.
- **UUID du certificat de signature S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent sélectionner les informations d'identification de signature à utiliser dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**.

Pour le cryptage S/MIME :

- **Informations d'identification de l'identité de chiffrement :** dans la liste, sélectionnez les informations d'identification de chiffrement à utiliser.
- **Activer commutateur de chiffrement S/MIME par message :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer ou désactiver le chiffrement S/MIME pour chaque message composé. La valeur par défaut est **Désactivé**.
- **Chiffrement S/MIME par défaut remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent choisir si S/MIME est activé par défaut dans les paramètres de

leurs appareils. La valeur par défaut est **Désactivé**.

- **UUID du certificat de chiffrement S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer et désactiver l'identité de chiffrement S/MIME dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**.

Paramètres OAuth Exchange à partir d'iOS 12. Vous pouvez maintenant configurer la connexion avec Exchange pour utiliser OAuth pour l'authentification.

Paramètres Exchange OAuth à partir de macOS 10.14. Vous pouvez maintenant configurer la connexion avec Exchange pour utiliser OAuth pour l'authentification. Pour l'authentification à l'aide d'OAuth, vous pouvez spécifier l'URL de connexion pour une installation qui n'utilise pas la détection automatique.

Consultez la section Stratégie Exchange.

Mises à jour de la stratégie de messagerie pour iOS

Davantage de paramètres de signature et de cryptage S/MIME Exchange sont disponibles à partir d'iOS 12. La stratégie de messagerie inclut davantage de paramètres permettant de configurer la signature et le cryptage S/MIME.

Pour la signature S/MIME :

- **Activer signature S/MIME :** indiquez si ce compte prend en charge la signature S/MIME. La valeur par défaut est **Activé**. Lorsque la valeur est définie sur **Activé**, les champs suivants apparaissent.
  - **Signature S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer et désactiver la signature S/MIME dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
  - **UUID du certificat de signature S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent sélectionner les informations d'identification de signature à utiliser dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.

Pour le cryptage S/MIME :

- **Activer chiffrement S/MIME :** sélectionnez cette option si vous souhaitez que ce compte prenne en charge le chiffrement S/MIME. La valeur par défaut est **Désactivé**. Lorsque la valeur est définie sur **Activé**, les champs suivants apparaissent.
  - **Activer commutateur de chiffrement S/MIME par message :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer ou désactiver le chiffrement S/MIME pour chaque message composé. La valeur par défaut est **Désactivé**.

- **Chiffrement S/MIME par défaut remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent choisir si S/MIME est activé par défaut dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
- **UUID du certificat de chiffrement S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer et désactiver l'identité de chiffrement S/MIME dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.

Consultez la section Stratégie de messagerie.

Mises à jour de la stratégie Notifications d'applications pour iOS

Les paramètres Notifications d'application suivants sont disponibles à partir d'iOS 12.

- **Afficher dans CarPlay :** sélectionnez **Activé** pour afficher les notifications dans Apple CarPlay. La valeur par défaut est **Activé**.
- **Activer alerte critique :** sélectionnez **Activé** pour autoriser une application à marquer une notification comme critique qui ignore les paramètres Ne pas déranger et Sonnerie. La valeur par défaut est **Désactivé**.

Consultez Stratégie Notifications d'applications.

Prise en charge des iPads partagés utilisés avec Apple Éducation

L'intégration de XenMobile avec les fonctionnalités Apple Éducation prend désormais en charge les iPad partagés. Plusieurs élèves d'une salle de classe peuvent partager un iPad pour différentes matières enseignées par un ou plusieurs instructeurs.

Vous ou les instructeurs inscrivez les iPad partagés, puis déployez des stratégies, des applications et des médias sur ces appareils. Ensuite, les étudiants fournissent leurs informations d'identification Apple gérées pour se connecter à un iPad partagé. Si vous avez déjà déployé une stratégie Configuration de l'éducation pour les étudiants, ils ne se connectent plus en tant que « Autre utilisateur » pour partager les appareils.

Conditions préalables pour iPads partagés :

- iPad Pro, iPad 5ème génération, iPad Air 2 ou ultérieur et iPad mini 4 ou ultérieur
- Au moins 32 Go de stockage
- Supervisé

Pour de plus amples informations, consultez la section Configurer les iPads partagés.

Modification des autorisations de contrôle d'accès basé sur des rôles (RBAC)

L'autorisation RBAC Ajouter/Supprimer des utilisateurs locaux est maintenant divisée en deux autorisations : Ajouter des utilisateurs locaux et Supprimer des utilisateurs locaux.

Pour plus d'informations, veuillez consulter la section Configurer des rôles avec RBAC.

Avis de tiers

January 10, 2022

Cette version de XenMobile peut inclure un logiciel tiers distribué sous une licence selon les conditions définies dans les documents suivants :

Avis de tiers XenMobile

Fin de prise en charge

January 10, 2022

Les annonces de cet article visent à vous avertir à l'avance des fonctionnalités de XenMobile Server qui vont disparaître. Nous fournissons ces informations afin que vous puissiez prendre des décisions appropriées. Citrix surveille l'utilisation des clients et leurs commentaires pour déterminer quand les retirer. Les annonces peuvent être modifiées dans les versions ultérieures et peuvent ne pas contenir chaque fonctionnalité amenée à disparaître. Pour obtenir des informations sur la prise en charge du cycle de vie d'un produit, consultez l'article Politique de prise en charge du cycle de vie d'un produit.

Fins de prise en charge et retraits

La liste suivante présente les fonctionnalités de XenMobile Server qui sont obsolètes ou ont été retirées.

Les éléments *obsolètes* ne sont pas retirés immédiatement. Citrix continue de prendre en charge les éléments obsolètes jusqu'à leur suppression dans une version ultérieure.

Les éléments *retirés* sont retirés, ou ne sont plus pris en charge, dans XenMobile Server.

Pour plus d'informations sur les applications de productivité mobiles ayant atteint la fin du cycle de vie, consultez la section Applications en fin de vie et obsolètes.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Inscription Knox Mobile Enrollment (ancien mode DA)	Fin de prise en charge de Knox Mobile Enrollment (KME) dans l'ancien mode Administrateur d'appareils (DA) sur toutes les versions Android.	4 mai 2021	Date prévue : 30 juin 2021	Utilisez KME pour l'inscription au mode Android Enterprise. Android 8, 9, 10, 11 prend en charge Android Enterprise.
Applications de mobilité Citrix et applications Workspace pour Android 7.x et iOS 12.x	Fin de prise en charge des versions Android 7.x et iOS 12.x de Secure Hub, Secure Mail, Secure Web et de l'application Citrix Workspace.	Avril 2021	Date prévue : juin 2021	Utilisez, au minimum, la version actuelle et une version antérieure des principales plates-formes de système d'exploitation. Les appareils plus anciens restent inscrits. Toutefois, Citrix ne teste ni ne prend en charge les appareils d'ancienne génération.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Informations d'identification dérivées	Fin de la prise en charge des informations d'identification dérivées et de l'application Citrix Derived Credential Manager.	25 mars 2021	Objectif : T2 2021	Pour obtenir la liste des types d'authentification pris en charge pour iOS, consultez iOS.
Internet Explorer 11	Fin de prise en charge de l'utilisation d'Internet Explorer avec la console XenMobile Server	Janvier 2021	Janvier 2021	Utilisez la dernière version de ces navigateurs Web : Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari
Prise en charge des jetons logiciels RSA pour Android	Fin de prise en charge de l'importation directe des jetons logiciels RSA dans Secure Hub pour Android.	Janvier 2021	Février 2021	Vous pouvez importer le jeton logiciel RSA dans l'application RSA Secure ID disponible dans Google Play. Vous pouvez ensuite utiliser le jeton pour l'authentification Citrix Gateway.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Android - Sony	Fin de la prise en charge des appareils Android Sony et des stratégies spécifiques à Sony.	Janvier 2021	Février 2021	Utiliser Android Enterprise
Android - HTC	Fin de la prise en charge des appareils Android HTC et des stratégies spécifiques à HTC.	Janvier 2021	Février 2021	Utiliser Android Enterprise
Composant tiers du tableau de bord XenMobile	Nous allons déclasser un composant tiers utilisé dans le tableau de bord XenMobile.	Décembre 2020	Janvier 2021	Pour continuer à utiliser le tableau de bord, mettez à niveau vers XenMobile 10.12 ou une version ultérieure

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Applications publiées pour le mode Administrateur de l'appareil (DA) hérité sur les appareils Android Enterprise	Nous ne fournissons plus d'applications publiées pour la plate-forme en mode DA hérité aux appareils inscrits dans Android Enterprise.	Octobre 2020	Novembre 2020	Pour les appareils Android Enterprise, publiez des applications pour la plate-forme Android Enterprise. Pour continuer à publier des applications en mode DA hérité sur des appareils en mode DA, créez un groupe de mise à disposition distinct pour ces applications.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Ports sortants APNs	La prise en charge par Apple du protocole binaire hérité du service Apple Push Notification prend fin le 31 mars 2021. Apple recommande d'utiliser à la place l'API du fournisseur APNs basé sur HTTP/2. Dans le cadre de ce changement, les ports 2195 et 2196, utilisés pour envoyer des notifications APNs à `*.push.apple.com` sont dépréciés.	Octobre 2020	Date prévue : avril 2021	Utilisez plutôt le port 443 ou 2197. Consultez Ouvrir des ports XenMobile pour gérer des appareils.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Conteneur Samsung SEAMS	Fin de la prise en charge du conteneur Samsung SEAMS.	Juin 2020	Août 2020	Utilisez l'application Samsung Knox Service Plugin (KSP) pour Android Enterprise. Consultez Ajouter l'application de plug-in de service Knox.
Certificats SSL (Secure Sockets Layer) auto-signés	Fin de la prise en charge des certificats SSL auto-signés pour toutes les plates-formes d'appareil.	Mai 2020		Remplacez votre certificat auto-signé existant par un certificat SSL approuvé d'une autorité de certification connue.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Algorithmes de signature d'authentification basés sur des certificats (non-FIPS et chiffrements faibles)	Fin de prise en charge des algorithmes de signature suivants : SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA SHA1withDSA, RIPEMD160withRS RIPEMD128withRS RIPEMD256withRS	Mai 2020	Janvier 2021	Lorsque vous créez un CSR pour un fournisseur d'informations d'identification dans la console XenMobile (**Paramètres > Fournisseurs d'identités > Demande de signature de certificat**), choisissez un chiffrement plus puissant.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Serveurs de base de données	Abandon de la prise en charge de Microsoft SQL Server 2014 et versions antérieures.	Octobre 2021	Août 2022	Effectuez une mise à jour du système vers l'une des versions prises en charge suivantes : Microsoft SQL Server 2016 SP2, Microsoft SQL Server 2017 CU 13 ou Microsoft SQL Server 2019 CTP 3.2. Consultez la liste des serveurs pris en charge dans Configuration système requise et compatibilité.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Hyperviseurs	Fin de prise en charge de Citrix XenServer 6.5.x et versions antérieures, de VMware ESXi 5.5 Update 3 et versions antérieures et de Hyper-V 2012.	Mai 2020	Août 2020	Effectuez une mise à jour du système vers l'une des versions prises en charge suivantes : Citrix Hypervisor 8.0 et versions ultérieures, Citrix XenServer 7.0 et versions ultérieures, VMware (ESXi 6.0, ESXi 6.5.0 Update 3, ESXi 6.7 Update 2 correctif 10 ou ESXi 7.0) ou Hyper-V (Windows Server 2016 ou Windows Server 2019).
Citrix Launcher	Fin de la prise en charge de l'application Citrix Launcher.	Mai 2020	Août 2020 (suppression de l'application du magasin d'applications)	Provisionner des appareils kiosques (appareils dédiés). Pour plus d'informations, consultez Remplacement de Citrix Launcher.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Applications de mobilité Citrix et applications Workspace pour Android 6.x et iOS 11.x	Fin de prise en charge des versions Android 6.x et iOS 11.x de Secure Hub, Secure Mail, Secure Web et Citrix Workspace.	Avril 2020	Juin 2020	Utilisez, au minimum, la version actuelle et une version antérieure des principales plates-formes de système d'exploitation.
MDX Toolkit et service MDX	Fin de prise en charge de MDX Toolkit et de MDX Service en faveur du SDK MAM (Gestion d'applications mobiles). Pendant la période de transition, vous pouvez utiliser à la fois des applications encapsulées avec MDX et des applications développées par le SDK MAM.	Mars 2020	Objectif : mars 2022 (pour MDX Toolkit) et septembre 2021 (pour MDX Service)	Pour continuer à gérer vos applications d'entreprise, utilisez le SDK MAM.
MDX : Autre serveur de passerelle	Fin de prise en charge de l'authentification renforcée pour les appareils iOS et Android.	Mars 2020	Objectif : septembre 2021	Pas de solution alternative

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
MDX : Micro VPN (mode tunnel complet)	Fin de prise en charge du tunnel VPN complet pour les appareils iOS et Android.	Mars 2020	Objectif : septembre 2021	Utilisez le mode SSO Web du SDK MAM ou créez une stratégie Per App VPN avec le type de connexion Citrix SSO.
MDX : prise en charge des fichiers PAC	Fin de prise en charge d'un fichier PAC (Proxy Automatic Configuration) avec un déploiement de tunnel VPN complet pour les appareils iOS.	Mars 2020	Objectif : septembre 2021	Utilisez Citrix Gateway pour vous connecter via un serveur proxy pour accéder aux réseaux internes.
Prise en charge des appareils partagés MDX	Fin de prise en charge des appareils partagés pour les applications MDX.	Mars 2020	Objectif : septembre 2021	Pour Android Enterprise, utilisez la prise en charge d'appareils partagés pour MDM. Pour iOS, utilisez Apple School Manager ou GroundControl.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Nouvelles inscriptions d'administrateur d'appareils pour Android 10	Prise en charge obsolète des nouvelles inscriptions ou réinscriptions en mode Administrateur d'appareils (DA) hérité sur les appareils Android 10. Les appareils déjà inscrits continuent de fonctionner.	Février 2020	Septembre 2020	Inscrivez les nouveaux appareils Android 10+ dans Android Enterprise.
Mode Administrateur d'appareils (DA) hérité pour les appareils Android 10.	Google a mis fin à la prise en charge de certaines API d'administrateur d'appareils Citrix ne prend pas en charge les appareils Android 10 inscrits en mode Administrateur d'appareils après la mise à niveau de Citrix Secure Hub qui cible l'API Android niveau 29.	Février 2020	Novembre 2020	Migrez les appareils Android 10 vers Android Enterprise.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Cryptage MDX	Fin de prise en charge de la fonctionnalité de cryptage MDX dans la console XenMobile.	Octobre 2019	Septembre 2020	Activez le cryptage de plate-forme iOS ou Android à l'aide de notre fonctionnalité de gestion du cryptage avec contrôle de la conformité. Assurez-vous d'avoir testé et planifié la migration depuis le cryptage MDX d'ici juillet 2020.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Stratégie de code secret : paramètre **Aucune restriction** pour Android Enterprise	Les appareils Android Enterprise exécutant Android 7 ou version ultérieure prennent uniquement en charge un code d'accès créé avec restrictions de caractère. Si vous avez précédemment défini **Caractères requis** sur **Aucune restriction**, cette mise à jour change la valeur vers **Chiffres uniquement**.	Février 2019	April 2019	Cette modification n'affecte pas l'expérience de connexion utilisateur actuelle.
Assistance à distance	Dépréciation du client Assistance à distance pour les déploiements de XenMobile Server locaux en cluster.	Janvier 2019	Août 2020	Pas de solution alternative

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Extensions réseau Secure Hub pour iOS	Fin de prise en charge de l'infrastructure d'extension réseau qui permet de personnaliser les fonctionnalités de mise en réseau pour les appareils iOS, à compter de Secure Hub version 20.3.0.	Octobre 2018	Mars 2020	Pas de solution alternative
TLS versions 1.0 et 1.1	Pour améliorer la sécurité de XenMobile, Citrix bloque désormais toute communication via TLS (Transport Layer Security) 1.0 et 1.1. En raison de leur faible niveau de sécurité, TLS 1.0 et TLS 1.1 ont été déclaré obsolètes par le PCI Council.	Juin 2018	Mars 2019	Mise à niveau vers TLS 1.2.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Alternative
Windows Mobile/CE	Fin de la prise en charge des périphériques Windows Mobile/CE.	Avril 2018	Septembre 2020	Utilisez Windows 10 Desktop et Laptop.
Android TouchDown	DigiCert a cessé de prendre en charge Android TouchDown. Citrix supprimera la page de la plate-forme Android TouchDown de la stratégie Exchange.	Juillet 2018	2021	Recommandation : Utiliser Citrix Secure Mail.

Problèmes résolus

September 22, 2021

Les problèmes suivants ont été résolus dans XenMobile 10.14.

- Lors de la mise à niveau vers XMS 10.12, il existe des problèmes avec la vue du tableau de bord sur la console XenMobile Server. [CXM-88918]
- L'inscription aux programmes de déploiement Apple (anciennement DEP) échoue sur les appareils Apple lorsque l'entité PKI générique est configurée. [CXM-89978]
- Des autorisations supplémentaires sont requises pour modifier les profils d'inscription lorsque vous vous connectez avec le contrôle d'accès basé sur rôle (RBAC). [CXM-89985]
- Sur la console XenMobile Server, vous ne pouvez pas modifier la stratégie **Configurations gérées par Android Entreprise** pour l'application Chrome. [CXM-89986]
- Sur la plate-forme iOS, lorsque vous modifiez une stratégie VPN dont le type de connexion est **Double configuration AlwaysOn IKEv2**, une erreur s'affiche. [CXM-90010]

- L'inscription d'appareils Android Enterprise avec **SamAccountName** échoue et l'erreur suivante s'affiche : « Work profile deleted, wiping profile » (Profil de travail supprimé, effacement du profil). [CXM-90049]
- La base de données n'accepte pas les noms d'utilisateur commençant par un « U » en minuscules. [CXM-90722]
- La console XenMobile Server affiche l'ICCID (Integrated Card ID) pour les appareils sans carte SIM insérée. [CXM-90845]
- L'inscription au programme d'inscription d'appareils Apple (DEP) échoue sur les appareils exécutant iOS 14. [CXM-91697]
- Sur la console XenMobile Server, la date d'expiration correcte du certificat racine n'est pas affichée. [CXM-91961]
- Sur XenMobile Server, les tests de connectivité NetScaler Gateway n'affichent pas de résultat. [CXM-93129]
- Lorsque vous ajoutez des utilisateurs SNMP à la console XenMobile Server, les utilisateurs n'apparaissent pas dans la liste *Utilisateurs de surveillance SNMP* ou les agents SNMP deviennent inactifs. [CXM-93197]
- Si vous activez les paramètres **Activer les applications système** et **Désactiver les applications** pour la même application dans la stratégie de restrictions, l'application apparaît dans le profil de travail. [CXM-93671]
- La propriété du serveur `ios.mdm.apns.connectionPoolSize` est masquée lorsque vous passez à l'API HTTP/2 pour APNs. [CXM-95478]
- Sur XenMobile Server version 10.12, vous ne pouvez pas modifier les propriétés VPP sur certaines applications. [CXM-96796]
- Les applications d'achat en volume Apple installées sur les appareils se mettent automatiquement à jour vers la dernière version lorsque le paramètre **Actualisation auto des apps** est désactivé. [CXM-96855]
- Sur XenMobile Server version 10.13, lorsque vous configurez le serveur proxy à l'aide de l'**interface de ligne de commande**, vous ne pouvez pas envoyer de notifications à Secure Hub exécuté sur des appareils iOS. [CXM-97609]
- Sur XenMobile Server version 10.13, une erreur s'affiche lors de l'accès aux **détails de l'appareil**. Cette erreur se produit lorsque la propriété de l'appareil a une valeur dans **”“**. [CXM-97952]
- Pour plus d'informations sur les problèmes résolus dans la version 10.13.0 Rolling Patch, consultez :
  - XenMobile Server 10.13.0 Rolling Patch 4
  - XenMobile Server 10.13.0 Rolling Patch 3

  - XenMobile Server 10.13.0 Rolling Patch 2

Informations connexes

- Centre de connaissances XenMobile

Mises à jour de prise en charge de plate-forme

Problèmes connus

January 10, 2022

Le problème suivant est connu dans XenMobile 10.14 :

- Après avoir importé l'image XenMobile Server 10.8 ou 10.9 dans VMware ESXi 6.7 ou 6.5 Mise à jour 2 : après le redémarrage de la VM, l'application de configuration ne démarre pas, XenMobile Server passe en mode de récupération et les paramètres IP sont effacés. Pour résoudre ce problème, créez une nouvelle VM avec une carte d'interface réseau VMXNET3, puis associez cette VM à la base de données de la VM qui est passée en mode de récupération. [CXM-54581]
- Après l'inscription d'un appareil iOS 15 ou macOS 12, le profil de configuration MDM affiche la mention « Non vérifié ». [CXM-98525]
- Après la mise à niveau vers Android 12, les terminaux réinscrits en mode profil de travail apparaissent deux fois dans le tableau de gestion des appareils. [CXM-99712]
- Après l'envoi d'une commande de localisation à un appareil inscrit auprès de MDM exécutant Android 12, les utilisateurs obtiennent un écran blanc qui se charge indéfiniment lors du lancement de Secure Hub. [CXM-99878]
- Pour les problèmes connus liés aux applications de productivité mobile, consultez Secure Hub, Secure Mail et Secure Web.
- Pour plus d'informations sur les problèmes connus dans la dernière version 10.13.0 Rolling Patch, consultez :
  - Notes de publication pour la version XenMobile Server 10.13 Rolling Patch 4

Informations connexes

- Centre de connaissances XenMobile

Architecture

January 10, 2022

Les besoins en matière de gestion des applications ou appareils de votre organisation déterminent les composants XenMobile de votre architecture XenMobile. Les composants XenMobile sont modulaires et complémentaires. Par exemple, votre déploiement inclut Citrix Gateway :

- Citrix Gateway permet aux utilisateurs d'accéder à distance à des applications mobiles et effectue le suivi des types d'appareils des utilisateurs.
- XenMobile est là où vous gérez ces applications et appareils.

Déploiement des composants XenMobile : vous pouvez déployer XenMobile afin de permettre aux utilisateurs de se connecter à des ressources sur votre réseau interne de l'une des façons suivantes :

- Connexions au réseau interne. Si vos utilisateurs sont distants, ils peuvent se connecter à l'aide d'un VPN ou d'une connexion micro VPN via Citrix Gateway. Cette connexion permet d'accéder aux applications et bureaux dans le réseau interne.
- Inscription d'appareils. Les utilisateurs peuvent inscrire des appareils mobiles dans XenMobile de façon à ce que vous puissiez gérer les appareils qui se connectent aux ressources du réseau dans la console XenMobile.
- Application Web, SaaS et mobiles. Les utilisateurs peuvent accéder à leurs applications Web, SaaS, mobiles à partir de XenMobile via Secure Hub.
- Applications et bureaux virtuels Windows. Les utilisateurs peuvent se connecter par le biais de Citrix Receiver ou un navigateur Web pour accéder à des applications et des bureaux virtuels Windows à partir de StoreFront ou l'Interface Web.

Pour utiliser une de ces fonctionnalités sur un serveur XenMobile sur site, Citrix vous recommande de déployer les composants XenMobile dans l'ordre suivant :

- Citrix Gateway. Vous pouvez configurer les paramètres dans Citrix Gateway afin de faciliter la communication avec XenMobile, StoreFront ou l'Interface Web à l'aide de l'assistant de configuration rapide. Avant d'utiliser l'assistant de configuration rapide dans Citrix Gateway, vous devez installer un des composants suivants pour configurer les communications : XenMobile, StoreFront ou Interface Web.
- XenMobile. Après avoir installé XenMobile, vous pouvez configurer les stratégies et les paramètres qui permettent aux utilisateurs d'inscrire leurs appareils mobiles dans la console XenMobile. Vous pouvez également configurer des applications mobiles, Web et SaaS. Les applications mobiles peuvent inclure des applications provenant de l'App Store ou de Google Play. Les utilisateurs peuvent également se connecter à des applications mobiles que vous encapsulez avec le MDX Toolkit et que vous chargez sur la console.
- SDK MAM ou MDX Toolkit La technologie d'encapsulation MDX devrait atteindre la fin de son

cycle de vie en mars 2022. Pour continuer à gérer vos applications d'entreprise, vous devez incorporer le SDK MAM.

Le SDK MAM (Mobile Application Management) fournit des fonctionnalités MDX qui ne sont pas couvertes par les plates-formes iOS et Android. Vous pouvez activer MDX pour les applications iOS ou Android et les sécuriser. Vous rendez ces applications disponibles dans un magasin interne ou dans des magasins d'applications publics. Consultez SDK de l'application MDX.

- StoreFront (facultatif). Vous pouvez fournir l'accès à des applications et des bureaux virtuels Windows à partir de StoreFront via des connexions avec Receiver.
- Citrix Files (facultatif). Si vous déployez Citrix Files, vous pouvez activer l'intégration de l'annuaire d'entreprise via XenMobile, qui agit en tant que fournisseur d'identité SAML (Security Assertion Markup Language). Pour plus d'informations sur la configuration des fournisseurs d'identité pour Citrix Content Collaboration, consultez le site de support Content Collaboration.

XenMobile fournit une gestion des appareils et des applications via la console XenMobile. Cette section décrit l'architecture de référence du déploiement XenMobile.

Dans un environnement de production, Citrix vous recommande de déployer la solution XenMobile dans une configuration en cluster à des fins de montée en charge et de redondance. Par ailleurs, l'utilisation de la capacité de déchargement SSL de Citrix ADC peut réduire la charge sur XenMobile Server et augmenter le débit. Pour de plus amples informations sur la configuration de la mise en cluster pour XenMobile en configurant deux adresses IP virtuelles d'équilibrage de charge sur Citrix ADC, consultez la section Mise en cluster.

Pour plus d'informations sur la configuration de XenMobile pour un déploiement de récupération d'urgence, consultez l'article Récupération d'urgence du manuel de déploiement. Cet article contient un diagramme d'architecture.

Les sections suivantes décrivent différentes architectures de référence pour le déploiement XenMobile. Vous trouverez des diagrammes d'architecture de référence dans les articles du manuel de déploiement XenMobile, Architecture de référence pour les déploiements sur site et Architecture. Pour obtenir une liste complète des ports, consultez les sections Configuration requise pour les ports (sur site) et Configuration requise pour les ports (cloud).

Mode de gestion d'appareils mobiles (MDM)

> **Important :**
>
> Si vous configurez le mode MDM et passez ensuite au mode ENT, veillez à utiliser la même authentification (Active Directory). XenMobile ne prend pas en charge la modification du mode

> d'authentification après l'inscription de l'utilisateur. Pour plus amples informations, consultez la section Mise à niveau de XenMobile MDM Edition vers Enterprise Edition.

XenMobile MDM Edition fournit une gestion des appareils mobiles. Pour connaître les plates-formes prises en charge, consultez la section Systèmes d'exploitation d'appareils pris en charge. Vous déployez XenMobile en mode MDM si vous projetez d'utiliser uniquement les fonctionnalités MDM de XenMobile. Par exemple, si vous souhaitez procédez comme suit.

- Déployer des applications et des stratégies d'appareil
- Récupérer des inventaires logiciels
- Effectuer des actions sur les appareils, telles que l'effacement

Dans le modèle recommandé, le serveur XenMobile Server est positionné dans la zone démilitarisée (DMZ) avec une instance Citrix ADC au premier plan (facultatif), ce qui offre une protection renforcée pour XenMobile.

Mode de gestion d'applications mobiles (MAM)

MAM, également appelé mode MAM exclusif, fournit la gestion des applications mobiles. Pour connaître les plates-formes prises en charge, consultez la section Systèmes d'exploitation d'appareils pris en charge. Si vous projetez d'utiliser uniquement les fonctionnalités MAM de XenMobile sans inscrire d'appareils auprès de MDM, vous devez déployer XenMobile en mode MAM. Par exemple, si vous souhaitez procédez comme suit.

- Sécuriser les applications et données sur les appareils mobiles BYO
- Mettre à disposition des applications mobiles d'entreprise
- Verrouiller les applications et effacer leurs données

Les appareils ne peuvent pas être inscrits auprès de MDM.

Dans ce modèle de déploiement, le serveur XenMobile Server est positionné avec une instance Citrix Gateway au premier plan, ce qui offre une protection renforcée pour XenMobile.

Mode MDM+MAM

L'utilisation conjointe des modes MAM et MDM permet de gérer les données et les applications mobiles ainsi que les appareils mobiles. Pour connaître les plates-formes prises en charge, consultez la section Systèmes d'exploitation d'appareils pris en charge. Vous déployez XenMobile en mode ENT (enterprise) si vous prévoyez d'utiliser les fonctionnalités MDM+MAM de XenMobile. Par exemple, si vous souhaitez :

- Gérer un appareil fourni par l'entreprise via MDM
- Déployer des applications et des stratégies d'appareil
- Récupérer un inventaire logiciel

- Effacer des appareils
- Mettre à disposition des applications mobiles d'entreprise
- Verrouiller des applications et effacer les données sur les appareils

Dans le modèle de déploiement recommandé, le serveur XenMobile Server est positionné dans la zone démilitarisée (DMZ) avec une instance Citrix Gateway au premier plan, ce qui offre une protection renforcée pour XenMobile.

XenMobile dans le réseau interne : une autre option de déploiement consiste à positionner un serveur XenMobile sur site dans le réseau interne, plutôt que dans la DMZ. Ce type de déploiement est utilisé si votre stratégie de sécurité autorise uniquement le positionnement d'appliances réseau dans la DMZ. Dans ce déploiement, le serveur XenMobile n'est pas dans la DMZ. Par conséquent, vous n'avez pas besoin d'ouvrir de ports sur le pare-feu interne pour autoriser l'accès à SQL Server et aux serveurs PKI depuis la DMZ.

Configuration système requise et compatibilité

January 10, 2022

> **Remarque :**
>
> Cet article traite de la configuration système requise et de la compatibilité pour XenMobile Server 10.14. Pour plus d'informations sur la configuration système requise pour Endpoint Management, consultez la section Configuration système requise.

Pour de plus amples informations sur la configuration requise et la compatibilité, consultez les articles suivants :

- Compatibilité XenMobile
- Systèmes d'exploitation d'appareils pris en charge
- Configuration requise pour les ports
- Capacité à monter en charge
- Gestion des licences
- Conformité FIPS 140-2
- Langues prises en charge

Pour exécuter XenMobile 10.14, vous avez besoin de la configuration système minimale suivante :

- Un des composants suivants :
  - Citrix Hypervisor 8.1 ou 8.0 ou Citrix XenServer (versions prises en charge : 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1, 8.2) ; pour plus d'information, consultez XenServer.
  - VMware (versions prises en charge : ESXi 6.0, ESXi 6.5.0 Mise à jour 3 ou ESXi 6.7 Mise à jour 2 Correctif 10, ESXi 7.0 Mise à jour 2a) ; pour plus d'information, consultez Solution de

contournement ESXi 6.7 et VMware.
  - Hyper-V (versions prises en charge : Windows Server 2016 et Windows Server 2019) ; pour plus d'informations, consultez Hyper-V.
- Endpoint Management Connector pour Exchange ActiveSync 10.1.10 ou Citrix Gateway Connector pour Exchange ActiveSync 8.5.3.19
- Processeur double cœur
- Quatre processeurs virtuels
- 8 Go de RAM pour les environnements de production ; 4 Go de RAM pour les environnements d'évaluation et de test
- 50 Go d'espace disque
- Serveur de licences Citrix 11.16.

  Mettez à jour votre serveur de licences avant de mettre à niveau XenMobile Server.

Solution de contournement ESXi 6.7

Pour le bon fonctionnement de ESXi 6.7, vous devez exécuter la solution suivante.

1. À l'aide de l'outil OVF fourni par VMware, extrayez le fichier OVA téléchargé à partir de citrix.com. Obtenez l'outil OVF à partir de la page de VMware (https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491).
2. À partir des trois fichiers extraits, téléchargez le fichier .vmdk dans votre magasin de données.
3. Créez une machine virtuelle.
   a) Nommez la machine virtuelle et sélectionnez **ESX/ESXi 4.x virtual machine** comme option de compatibilité.
   b) Sous Guest OS Family, sélectionnez **Linux**.
   c) Sous Guest OS Version, sélectionnez **Other 2.6.x Linux (64-bit)**.
   d) Sous Data Store, sélectionnez **Default**.
   e) Lors de la personnalisation, supprimez le disque dur, le contrôleur USB et le lecteur de CD/DVD par défaut.
   f) Sous Network, sélectionnez **VMXNET3** comme type d'adaptateur.
   g) Sur ESXi, si vos disques sont locaux, sélectionnez **SCSI Controller** et **LSI Logic Parallel**. Si vous utilisez un disque partagé, sélectionnez **VMware Paravirtual**.
   h) Cliquez sur Next pour terminer la création de la VM.
4. Accédez à votre magasin de données et copiez le fichier .vmdk que vous avez téléchargé précédemment. Copiez-le dans le répertoire de la VM que vous avez créé pour XenMobile.
5. Dans l'interface Web ESXi, sélectionnez la VM et modifiez les paramètres.
6. Cliquez sur **Add Hard disk**.
7. Sélectionnez le fichier .vmdk copié précédemment et attachez-le à la VM.

8. Cliquez sur **Enregistrer**.
9. Mettez la VM sous tension.

Configuration requise pour Citrix Gateway

Pour exécuter Citrix Gateway avec XenMobile 10.14, vous avez besoin de la configuration système minimale suivante.

- Citrix Gateway (local). Versions prises en charge : 12.1 ou supérieures
- Vous devez également être en mesure de communiquer avec Active Directory, ce qui nécessite un compte de service. Vous avez uniquement besoin d'un accès de requête/lecture.

Configuration requise pour la base de données XenMobile 10.14

XenMobile nécessite l'une des bases de données suivantes :

- Microsoft SQL Server

  XenMobile prend en charge une base de données Microsoft SQL Server exécutée sur l'une des versions prises en charge suivantes. Pour plus d'informations sur les bases de données Microsoft SQL Server et leur configuration matérielle requise, consultez la documentation Microsoft.

  - Microsoft SQL Server 2014 SP3
  - Microsoft SQL Server 2016 SP2
  - Microsoft SQL Server 2017 CU 25
  - Microsoft SQL Server 2019 CU 12

  Les exigences de votre base de données Microsoft SQL Server dépendent également de la taille de votre déploiement. Pour plus d'informations sur les exigences de base de données Microsoft SQL Server en fonction de votre taille de déploiement, consultez la section Capacité à monter en charge.

  XenMobile prend en charge les groupes de disponibilité de base SQL (groupes de disponibilité AlwaysOn) ainsi que la mise en cluster SQL pour assurer une haute disponibilité de la base de données.

  Citrix vous recommande d'utiliser Microsoft SQL à distance.

  Pour plus d'informations sur la mise à niveau de Microsoft SQL, consultez l'article Microsoft Mise à niveau de SQL Server.

- PostgreSQL (pour les environnements de test uniquement). PostgreSQL est inclus avec XenMobile. Vous pouvez l'utiliser localement ou à distance dans des environnements de test. La migration de la base de données n'est pas prise en charge. Vous ne pouvez pas déplacer les bases de données créées dans un environnement de test dans un environnement de production.

Toutes les éditions de XenMobile prennent en charge Remote PostgreSQL 9.5.1 et 9.5.11 pour Windows avec les limitations suivantes : non recommandé pour les environnements de production. Jusqu'à 300 appareils pris en charge. Utilisez SQL Server localement pour plus de 300 appareils. Mise en cluster non prise en charge

Configuration requise pour le compte de service SQL Server

Vérifiez que le compte de service du serveur SQL à utiliser avec XenMobile dispose de l'autorisation de rôle `DBcreator`. Enregistrez le mot de passe du compte du serveur SQL que vous spécifiez lors de l'installation de XenMobile Server. Ce mot de passe est requis si vous devez cloner la base de données XenMobile lors de la récupération de XenMobile Server.

Sécurisez vos bases de données SQL Server à l'aide du chiffrement transparent des données (TDE). N'autorisez pas l'accès externe aux ports SQL Server, comme indiqué dans l'architecture de référence dans Architecture de référence pour les déploiements sur site.

Pour plus d'informations sur les comptes de service SQL Server, consultez les pages suivantes sur le site de documentation Microsoft. Ces liens pointent vers des informations concernant SQL Server 2014. Si vous utilisez une version différente, sélectionnez la version de votre serveur dans la liste **Autres versions** :

- Configurer les comptes de service Windows et les autorisations
- Rôles de niveau serveur

Compatibilité avec Virtual Apps and Desktops

- Virtual Apps and Desktops 7.15 LTSR CU3
- Virtual Apps and Desktops 7.1811
- Virtual Apps and Desktops 7 1906
- Virtual Apps and Desktops 7 1909
- Virtual Apps and Desktops 7 2006

Compatibilité StoreFront

- StoreFront 3.12.2
- StoreFront 7 1811
- StoreFront 7 1906
- StoreFront 7 1909
- StoreFront 7 2006

Autre compatibilité

- Endpoint Management Connector pour Exchange ActiveSync 10.1.10
  - Les anciennes versions ne sont pas testées.
- Citrix Gateway Connector pour Exchange ActiveSync 8.5.3.19
  - Les anciennes versions ne sont pas testées.

Compatibilité XenMobile

January 10, 2022

> **Remarque :**
>
> Cet article traite de la compatibilité pour XenMobile Server. Pour les composants testés avec Endpoint Management, consultez la section Compatibilité Endpoint Management.

Pour utiliser les nouvelles fonctionnalités, des correctifs et des mises à jour de stratégie, Citrix vous recommande d'installer la dernière version des éléments suivants :

- Citrix vous recommande d'intégrer le SDK MAM (Mobile Application Management) aux applications iOS et Android d'entreprise afin d'appliquer les fonctionnalités MDX aux applications.

  Le MDX Toolkit devrait atteindre la fin de son cycle de vie en mars 2022. Pour continuer à gérer vos applications d'entreprise, vous devez incorporer le SDK MAM.

Cet article décrit les versions des composants XenMobile pris en charge que vous pouvez intégrer.

Chemins de compatibilité et de mise à niveau

Les dernières versions de Secure Hub, du MDX Toolkit et des applications de productivité mobiles sont compatibles avec la dernière version et la version précédente de XenMobile Server.

La dernière version des applications de productivité mobiles requiert la dernière version de Secure Hub. Les deux versions précédentes des applications sont compatibles avec la dernière version de Secure Hub. Consultez le tableau des produits Citrix pour plus d'informations.

Citrix prend en charge la distribution des applications de productivité XenMobile uniquement à partir d'un magasin d'applications public.

XenMobile Server (sur site)

- Citrix prend en charge les mises à niveau à partir des deux dernières versions de XenMobile Server.
- Dernière version de XenMobile Server : XenMobile Server 10.14

- Mise à niveau à partir de :
  - XenMobile Server 10.13.x
  - XenMobile Server 10.12.x

Applications de productivité mobiles

Les utilisateurs ont accès aux applications de productivité mobiles à partir des magasins d'applications publics. La dernière version des applications de productivité mobiles requiert la dernière version de Secure Hub. Les deux versions précédentes des applications sont compatibles avec la dernière version de Secure Hub.

Pour plus d'informations sur la cadence de publication de deux semaines des applications de productivité mobiles, consultez la section Calendrier de publication. Pour plus d'informations, consultez la section Prise en charge des applications de productivité mobiles.

SDK MAM

Le SDK MAM fournit des fonctionnalités MDX qui ne sont pas couvertes par les plates-formes iOS et Android. Vous rendez ces applications disponibles dans un magasin interne ou dans des magasins d'applications publics. Consultez SDK de l'application MDX.

MDX Toolkit

La technologie d'encapsulation MDX devrait atteindre la fin de son cycle de vie en septembre 2021. Pour continuer à gérer vos applications d'entreprise, vous devez incorporer le SDK MAM.

Citrix prend en charge les trois dernières versions (nnn) de MDX Toolkit. Consultez Nouveautés dans le MDX Toolkit.

Prise en charge des navigateurs

La console XenMobile Server nécessite l'un des navigateurs Web pris en charge suivants :

- Dernière version de Google Chrome
- Dernière version de Mozilla Firefox
- Dernière version de Microsoft Edge
- Dernière version de Apple Safari

Systèmes d'exploitation d'appareils pris en charge

January 10, 2022

> **Remarque :**
>
> Cet article couvre les systèmes d'exploitation des appareils pris en charge pour XenMobile Server 10.13. Pour les systèmes d'exploitation pris en charge par Endpoint Management, consultez la section Systèmes d'exploitation d'appareils pris en charge.

XenMobile prend en charge les appareils exécutant les plates-formes et les systèmes d'exploitation suivants pour la gestion de la mobilité d'entreprise, y compris la gestion d'applications et d'appareils. En raison de restrictions spécifiques à la plate-forme et de fonctionnalités de sécurité, XenMobile ne prend pas en charge toutes les fonctionnalités sur toutes les plates-formes.

Les informations relatives aux plates-formes d'appareil prises en charge dans cet article s'appliquent également à XenMobile Connector pour Exchange ActiveSync et Citrix Gateway Connector pour Exchange ActiveSync.

Pour obtenir les dernières versions des applications de productivité mobiles, ainsi que les appareils pris en charge pour le cryptage MDX, consultez la section Prise en charge des applications de productivité mobiles.

> **Remarque :**
>
> Citrix prend en charge, au minimum, la version actuelle et une version antérieure des principales plates-formes de système d'exploitation. Les fonctionnalités de la nouvelle version de Endpoint Management ne fonctionnent pas sur toutes sur les anciennes versions de plates-formes.
>
> Pour les annonces de fin de prise en charge, consultez la section Fin de prise en charge.

Liste des systèmes d'exploitation pris en charge

Citrix XenMobile prend en charge les systèmes d'exploitation suivants :

> **Remarque :**
>
> La prise en charge des versions Android 7.x et iOS 12.x de Secure Hub, Secure Mail, Secure Web et de l'application Citrix Workspace a pris fin en avril 2021.

- **Android :** 8.x, 9.x, 10.x, 11.x, 12.x

  Pour plus d'informations sur Android 10, consultez la section Considérations relatives à Android.

- **iOS :** 13.x, 14.x, 15.x

  XenMobile et les applications mobiles Citrix sont compatibles avec iOS 14.x, mais ne prennent pas actuellement en charge les nouvelles fonctionnalités iOS 14.x. Pour encapsuler des applications d'entreprise internes pour iOS 14.x, utilisez le MDX Toolkit 21.8.5 ou version ultérieure ou préparez les applications à l'aide du SDK MAM.

- **iPadOS :** 13.x, 14.x, 15.x

  XenMobile et les applications mobiles Citrix sont compatibles avec iPadOS 14.x, mais ne prennent pas actuellement en charge les nouvelles fonctionnalités iPadOS 14.x.

- **macOS :** 10.13x, 10.14x, 10.15x, 11.x

  XenMobile et les applications mobiles Citrix sont compatibles avec macOS 11, mais ne prennent pas actuellement en charge les nouvelles fonctionnalités macOS 11.

- **Bureaux et tablettes Windows :** (MDM uniquement). Windows 10 et Windows 11
- **Windows Phone :** (MDM exclusif). Windows Phone 8.1, Windows Phone 10, Windows 10 RS4 et RS5
- **Windows Mobile/CE :** (MDM exclusif). À compter du deuxième trimestre de 2018, la prise en charge des appareils Windows Mobile/CE n'est plus disponible.
- **Samsung SAFE et Knox :** sur les appareils Samsung compatibles, XenMobile prend en charge et étend les stratégies Samsung Knox et Samsung for Enterprise (SAFE). XenMobile nécessite l'activation d'API SAFE avant le déploiement de stratégies et de restrictions SAFE. Pour ce faire, déployez la clé Samsung Enterprise License Management (ELM) intégrée sur un appareil. Consultez la section Stratégie de clé de licence MDM Samsung.

Considérations relatives à Android

Avant de mettre à niveau vers Android 10 ou version ultérieure : consultez Migrer de l'administration des appareils vers Android Enterprise pour plus d'informations sur la façon dont la fin de prise en charge des API d'administration des appareils Google affecte les appareils exécutant Android 10.

- Citrix vous recommande d'éviter d'inscrire les appareils Android 10 en mode d'administration des appareils d'ancienne génération. Google est en train de mettre fin à la prise en charge des API d'administration des appareils, ce qui a un impact sur les appareils fonctionnant sous Android 10+. Une fois les API obsolètes, l'inscription des appareils Android 10+ en mode d'administration des appareils d'ancienne génération échouera. Citrix ne prend pas en charge l'inscription d'appareils Android 11 en mode d'administration des appareils.
- Citrix recommande d'utiliser Android Entreprise pour les appareils Android 10. Pour plus d'informations, consultez la section Migrer de l'administration des appareils vers Android Enterprise.
- La modification de l'API Google n'affecte pas les appareils inscrits en mode MAM-uniquement.

Avant la mise à niveau :

- Assurez-vous que votre infrastructure de serveurs est conforme aux certificats de sécurité ayant un nom d'hôte correspondant dans l'extension SAN (autre nom de l'objet).

- Pour vérifier un nom d'hôte, le serveur doit présenter un certificat avec un SAN correspondant. Citrix approuve les certificats uniquement s'ils contiennent un SAN correspondant au nom d'hôte.

Configuration requise pour les ports

January 10, 2022

Pour autoriser des appareils et des applications à communiquer avec XenMobile, vous devez ouvrir des ports spécifiques dans vos pare-feu. Les tableaux suivants répertorient les ports qui doivent être ouverts.

Ouvrir des ports pour Citrix Gateway et XenMobile afin de gérer des applications

Ouvrez les ports suivants pour autoriser les connexions utilisateur à partir de Citrix Secure Hub, Citrix Receiver et Citrix Gateway Plug-in via Citrix Gateway pour les composants suivants :

- XenMobile
- StoreFront
- Citrix Virtual Apps and Desktops
- Citrix Gateway Connector pour Exchange ActiveSync
- Autres ressources du réseau interne telles que les sites Web intranet

Pour activer le trafic vers Launch Darkly depuis Citrix ADC, vous pouvez utiliser les adresses IP indiquées dans cet article du centre de connaissances.

Pour plus d'informations sur Citrix Gateway, consultez la documentation relative à Citrix Gateway. Cette documentation contient des informations sur les adresses IP de Citrix ADC (NSIP), du serveur virtuel (VIP) et de sous-réseau (SNIP).

Port TCP	Description	Source	Destination
21 ou 22	Utilisé pour envoyer des packs d'assistance à un serveur FTP ou SCP	XenMobile	Serveur FTP ou SCP
53 (TCP et UDP)	Utilisé pour les connexions DNS.	Citrix Gateway, XenMobile	Serveur DNS

Port TCP	Description	Source	Destination
80	Citrix Gateway transmet la connexion VPN à la ressource du réseau interne via le second pare-feu. Cette situation se produit généralement si les utilisateurs ouvrent une session à l'aide de Citrix Gateway Plug-in.	Citrix Gateway	Sites Web intranet
80 ou 8080 ; 443	Port XML et Secure Ticket Authority (STA) utilisé pour l'énumération, la fonctionnalité de ticket et l'authentification. Citrix recommande d'utiliser le port 443.	Trafic réseau XML de StoreFront et l'Interface Web ; STA Citrix Gateway	Virtual Apps ou Desktops
123 (TCP et UDP)	Utilisé pour les services NTP (Network Time Protocol).	Citrix Gateway ; XenMobile	Serveur NTP
389	Utilisé pour les connexions LDAP non sécurisées	Citrix Gateway ; XenMobile	Serveur d'authentification LDAP ou Microsoft Active Directory
443	Utilisé pour les connexions à StoreFront à partir de Citrix Receiver ou Receiver pour Web vers Virtual Apps and Desktops.	Internet	Citrix Gateway

Port TCP	Description	Source	Destination
443	Utilisé pour les connexions à XenMobile pour la mise à disposition d'applications Web, mobiles et SaaS.	Internet	Citrix Gateway
443	Utilisé pour la communication des appareils avec XenMobile Server	XenMobile	XenMobile
443	Utilisé pour les connexions à partir d'appareils mobiles à XenMobile pour l'inscription.	Internet	XenMobile
443	Utilisé pour les connexions de XenMobile vers Citrix Gateway Connector pour Exchange ActiveSync.	XenMobile	Citrix Gateway Connector pour Exchange ActiveSync
443	Utilisé pour les connexions de Citrix Gateway Connector pour Exchange ActiveSync vers XenMobile.	Citrix Gateway Connector pour Exchange ActiveSync	XenMobile
443	Utilisé pour les URL de rappel dans les déploiements sans authentification par certificat.	XenMobile	Citrix Gateway
514	Utilisé pour les connexions entre XenMobile et un serveur syslog.	XenMobile	Serveur Syslog

Port TCP	Description	Source	Destination
636	Utilisé pour les connexions LDAP sécurisées.	Citrix Gateway ; XenMobile	Serveur d'authentification LDAP ou Active Directory
1494	Utilisé pour les connexions ICA à des applications Windows dans le réseau interne. Citrix recommande de conserver ce port ouvert.	Citrix Gateway	Virtual Apps ou Desktops
1812	Utilisé pour les connexions RADIUS.	Citrix Gateway	Serveur d'authentification RADIUS
2598	Utilisé pour les connexions aux applications Windows dans le réseau interne à l'aide de la fiabilité de session. Citrix recommande de conserver ce port ouvert.	Citrix Gateway	Virtual Apps ou Desktops
3268	Utilisé pour les connexions LDAP non sécurisées au Microsoft Global Catalog.	Citrix Gateway ; XenMobile	Serveur d'authentification LDAP ou Active Directory
3269	Utilisé pour les connexions LDAP sécurisées au Microsoft Global Catalog.	Citrix Gateway ; XenMobile	Serveur d'authentification LDAP ou Active Directory

Port TCP	Description	Source	Destination
9080	Utilisé pour le trafic HTTP entre Citrix ADC et Citrix Gateway Connector pour Exchange ActiveSync.	Citrix ADC	Citrix Gateway Connector pour Exchange ActiveSync
30001	API de gestion pour la gestion intermédiaire du service HTTPS	Réseau local interne	XenMobile Server
9443	Utilisé pour le trafic HTTPS entre Citrix ADC et Citrix Gateway Connector pour Exchange ActiveSync.	Citrix ADC	Citrix Gateway Connector pour Exchange ActiveSync
45000 ; 80	Utilisé pour la communication entre deux VM XenMobile lors du déploiement dans un cluster. Le port 80 est utilisé pour la communication entre les nœuds et le déchargement SSL.	XenMobile	XenMobile
8443	Utilisé pour l'inscription, XenMobile Store et la gestion des applications mobiles (MAM).	XenMobile ; Citrix Gateway ; Appareils ; Internet	XenMobile

Port TCP	Description	Source	Destination
4443	Utilisé pour l'accès à la console XenMobile par un administrateur via le navigateur. Également utilisé pour le téléchargement des journaux et des packs d'assistance pour tous les nœuds de cluster XenMobile à partir d'un seul nœud.	Point d'accès (navigateur) ; XenMobile	XenMobile
27000	Port par défaut utilisé pour l'accès au serveur de licences Citrix externe.	XenMobile	Serveur de licences Citrix
7279	Port par défaut utilisé pour la libération et l'obtention de licences Citrix.	XenMobile	Démon vendeur Citrix
161	Utilisé pour le trafic SNMP à l'aide du protocole UDP.	Gestionnaire SNMP	XenMobile
162	Utilisé pour l'envoi d'alertes d'interruption SNMP vers le gestionnaire SNMP à partir de XenMobile. La source est XenMobile et la destination est le gestionnaire SNMP.	XenMobile	Gestionnaire SNMP

Ouvrir des ports XenMobile pour gérer des appareils

Ouvrez les ports suivants pour autoriser XenMobile à communiquer dans votre réseau.

Port TCP	Description	Source	Destination
25	Port SMTP par défaut du service de notification XenMobile. Si votre serveur SMTP utilise un port différent, assurez-vous que votre pare-feu ne bloque pas ce port.	XenMobile	Serveur SMTP
80 et 443	Connexion de l'App Store d'entreprise à Apple iTunes App Store, Google Play (doit utiliser 80) ou Windows Phone Store. Utilisé pour l'achat en volume Apple. Utilisé pour la publication d'applications à partir des magasins d'application via iOS, Secure Hub pour Android, ou Secure Hub pour Windows Phone.	XenMobile	`ax.apps.apple.com` et `*.mzstatic.com`; `vpp.itunes.apple.com`; `login.live.com`; `*.notify.windows.com`; `play.google.com`, `android.clients.google.com`, `android.l.google.com`
80 ou 443	Utilisé pour les connexions sortantes entre XenMobile et Nexmo SMS Notification Relay.	XenMobile	Serveur Nexmo SMS Relay

Port TCP	Description	Source	Destination
389	Utilisé pour les connexions LDAP non sécurisées.	XenMobile	Serveur d'authentification LDAP ou Active Directory
443	Utilisé pour l'inscription et l'installation de l'agent pour Android et Windows Mobile.	Internet	XenMobile
443	Utilisé pour l'inscription et l'installation de l'agent pour appareils Android et Windows, ainsi que le client d'assistance à distance MDM.	Réseau local Internet et Wi-Fi	XenMobile
1433	Utilisé par défaut pour les connexions à un serveur de base de données distant (facultatif).	XenMobile	SQL Server
443 ou 2197	Utilisé pour envoyer des notifications APNs à `*.push.apple.com`	XenMobile	Internet (hôtes APNs utilisant l'adresse IP publique 17.0.0.0/8)
5223	Utilisé pour les connexions sortantes APNs à partir d'appareils iOS sur `*.push.apple.com`.	Appareils iOS	Internet (hôtes APNs utilisant l'adresse IP publique 17.0.0.0/8)

Port TCP	Description	Source	Destination
8081	Utilisé pour les tunnels applicatifs depuis le client d'assistance à distance MDM (facultatif). La valeur par défaut est 8081.	Client d'assistance à distance	XenMobile
8443	Utilisé pour l'inscription d'appareils iOS et Windows Phone.	Internet ; Réseau local et Wi-Fi	XenMobile

Exigences en matière de port pour la connectivité au service de détection automatique

La configuration de ce port permet de s'assurer que les appareils Android qui se connectent à partir de Secure Hub pour Android peuvent accéder au service de détection automatique (ADS) de Citrix depuis le réseau interne. Vous devez accéder à ADS pour télécharger les mises à jour de sécurité mises à disposition via ADS.

> **Remarque :**
>
> Les connexions ADS peuvent ne pas prendre en charge votre serveur proxy. Dans ce scénario, autorisez la connexion ADS à contourner le serveur proxy.

Si vous souhaitez autoriser le certificate pinning, procédez comme suit :

- **Collecter les certificats de XenMobile Server et de Citrix ADC.** Les certificats doivent être au format PEM et doivent être des certificats de clé publique et non de clé privée.
- **Contacter l'assistance Citrix et demander l'activation du certificate pinning.** Lors de cette opération, vous êtes invité à fournir vos certificats.

Le certificate pinning nécessite que les appareils se connectent à ADS avant l'inscription de l'appareil. Cela garantit que Secure Hub dispose des dernières informations de sécurité. Pour que Secure Hub puisse inscrire un appareil, l'appareil doit contacter le service ADS. Par conséquent, il est primordial d'autoriser l'accès à ADS dans le réseau interne pour permettre aux appareils de s'inscrire.

Pour autoriser l'accès à ADS pour Secure Hub pour Android, ouvrez le port 443 pour les adresses IP et les noms de domaine complets suivants :

FQDN	Adresse IP	Port	Utilisation adresse IP et port
ads.xm.cloud.com	34.194.83.188	443	Secure Hub - Communication ADS
ads.xm.cloud.com	34.193.202.23	443	Secure Hub - Communication ADS

> **Remarque :**
>
> Pour les versions de Secure Hub antérieures à 10.6.15, le nom de domaine complet est discovery.mdm.zenprise.com. Ouvrez le port 443 pour les adresses IP 52.5.138.94 et 52.1.30.122.

Configuration réseau requise pour Android Enterprise

Pour plus d'informations sur les connexions sortantes à prendre en compte lors de la configuration d'environnements réseau pour Android Enterprise, consultez l'article de support Google Android Enterprise Network Requirements.

Exigences en matière de port requises par XenMobile

Les hôtes de destination suivants doivent être accessibles à partir du réseau pour créer une instance Google Play d'entreprise et accéder à Managed Google Play iFrame. Google a mis le composant Managed Play iFrame à la disposition des développeurs EMM afin de simplifier la recherche et l'approbation des applications. Pour pouvoir utiliser Managed Play iFrame, le navigateur à partir duquel vous accédez à la console XenMobile doit avoir accès à Google Play.

Hôte de destination	**Port**	**Description**
play.google.com	TCP/443	Utilisé pour l'inscription à Google Play Store et Play Enterprise
*.googleapis.com	TCP/443	Utilisé pour la gestion des appareils mobiles Google, les API Google et les API Google Play Store
accounts.youtube.com, accounts.google.com	TCP/443	Utilisé pour l'authentification du compte

Hôte de destination	Port	Description
apis.google.com	TCP/443	Utilisé pour GCM et autres services Web Google
ogs.google.com	TCP/443	Utilisé pour les éléments de l'interface utilisateur iFrame
notifications.google.com	TCP/443	Utilisé pour les notifications de bureaux et d'appareils mobiles
fonts.googleapis.com, *.gstatic.com, *.googleusercontent.com	TCP/443	Utilisé pour le contenu généré par l'utilisateur Google Fonts, par exemple, les icônes de l'application dans le magasin
cri.pki.goog, ocsp.pki.goog	TCP/443	Utilisé pour la validation du certificat

Capacité à monter en charge et performances

January 10, 2022

Comprendre l'échelle de votre infrastructure XenMobile joue un rôle significatif dans la façon dont vous décidez de déployer et de configurer XenMobile. Cet article contient des données provenant de tests de capacité à monter en charge ainsi que des instructions permettant de déterminer les exigences en matière de performance et de capacité à monter en charge des déploiements d'entreprise XenMobile sur site à petite ou grande échelle.

La capacité à monter en charge se définit ici comme la capacité des appareils déjà inscrits dans le déploiement à se reconnecter au déploiement en même temps.

- La *capacité à monter en charge* se définit comme le nombre maximal d'appareils inscrits dans le déploiement.
- Le *taux de connexion* représente la vitesse maximale à laquelle les appareils existants peuvent se reconnecter au déploiement.

Les données de cet article sont tirées de tests effectués dans des déploiements allant de 10 000 à 75 000 appareils. Pour les besoins des tests, des appareils mobiles avec des charges de travail connues ont été utilisés.

Tous les tests ont été effectués sur XenMobile Enterprise Edition.

Les tests ont été effectués à l'aide de Citrix Gateway 8200. Une appliance Citrix ADC dotée d'une capacité identique ou supérieure est censée produire des performances de capacité à monter en charge identiques ou supérieures.

Un résumé des résultats des tests de la capacité à monter en charge est présenté ci-après.

Résumé des résultats des tests de la capacité à monter en charge pour les déploiements allant jusqu'à 75 000 appareils

Taux de connexion (taux de reconnexion des utilisateurs existants) - Jusqu'à 9 375 appareils par heure

Configuration utilisée :

- Citrix Gateway
- MPX 8200
- XenMobile Enterprise Edition
- Cluster à 7 nœuds XenMobile Server
- Base de données : base de données externe Microsoft SQL Server

Résultats des tests en fonction du nombre d'appareils et de la configuration matérielle

Nombre d'appareils	12 500	30 000	60 000	75 000
Taux de reconnexion d'appareils existants par heure	1 250	3 750	7 500	9 375
XenMobile Server – mode	Autonome	Cluster :	Cluster :	Cluster :
XenMobile Server – cluster	S.O.	3	5	7
XenMobile Server – Appliance virtuelle	Mémoire = 8 Go de RAM ; vCPUs = 4	Mémoire = 16 Go de RAM ; vCPU = 6	Mémoire = 24 Go de RAM ; vCPUs = 8	Mémoire = 24 Go de RAM ; vCPUs = 8
Active Directory	Mémoire = 4 Go de RAM ; vCPUs = 2	Mémoire = 8 Go de RAM ; vCPUs = 4	Mémoire = 16 Go de RAM ; vCPUs = 4	Mémoire = 16 Go de RAM ; vCPUs = 4

Nombre d'appareils	12 500	30 000	60 000	75 000
Base de données externe Microsoft SQL Server	Mémoire = 8 Go de RAM ; vCPUs = 4	Mémoire = 16 Go de RAM ; vCPUs = 8	Mémoire = 24 Go de RAM ; vCPU = 16	Mémoire = 24 Go de RAM ; vCPU = 16

Profil de capacité à monter en charge

Configuration d'Active Directory	Profil utilisé
Utilisateurs	100 000
Groupes	200 000
Niveaux d'imbrication	5

Configuration de XenMobile Server	Total :	Par utilisateur
Stratégies	20	20
Applications	270	50
Publique	200	0
MDX	50	30
Web et SaaS	20	20
Actions	50	
Groupes de mise à disposition	20	
Groupes Active Directory par groupe de mise à disposition	10	
SQL		
Nombre de bases de données	1	

Connexions des appareils et activités applicatives

Ces tests de capacité à monter en charge ont collecté des données sur la capacité des appareils inscrits dans un déploiement à se reconnecter au cours d'une période de 8 heures.

Les tests simulaient un intervalle de reconnexion au cours duquel les appareils se reconnectant obtiennent toutes les stratégies de sécurité autorisées, soumettant les nœuds XenMobile Server à des charges supérieures à la normale. Durant les reconnexions, seules les nouvelles stratégies ou les stratégies modifiées sont déployées sur les appareils iOS, ce qui réduit la charge sur les nœuds XenMobile Server.

Ces tests utilisaient une combinaison de 50 % d'appareils iOS et 50 % d'appareils Android.

Ces tests supposent que les appareils Android qui se reconnectent ont préalablement reçu des notifications GCM.

Durant la durée du test (8 heures), les activités suivantes liées aux applications se sont produites :

- Secure Hub a été ouvert une fois pour énumérer les applications autorisées
- 2 applications Web SAML ont été ouvertes
- 4 applications MAM ont été téléchargées
- 1 STA a été générée pour être utilisée par Secure Mail
- 240 validations de ticket STA, une pour chaque événement de reconnexion à Secure Mail via un micro VPN, ont été effectuées.

Architecture de référence

Pour accéder à l'architecture de référence des déploiements utilisés dans ces tests de capacité à monter en charge, consultez la section « Architecture de référence principale pour le mode MAM+MDM » de l'article Architecture de référence pour les déploiements sur site.

Restrictions et limitations

Tenez compte de ce qui suit lorsque vous consultez les résultats des tests de capacité à monter en charge dans cet article :

- La plate-forme Windows n'a pas été testée.
- La transmission de stratégies a été testée sur les appareils iOS et Android.
- Chaque nœud XenMobile Server prend en charge un maximum de 12 000 appareils simultanément.

Gestion des licences

January 10, 2022

> **Important :**
>
> le processus de renvoi et de modification des licences Citrix a changé le 4 novembre 2020. Pour plus d'informations sur les modifications apportées au portail « Gérer des licences » sur Citrix.com et à « My Licensing Tools » sur Partner Central, consultez l'article de support Citrix, https://support.citrix.com/article/CTX285157.

XenMobile utilise le système de licences Citrix pour gérer les licences. XenMobile Server et Citrix Gateway requièrent des licences.

Pour plus d'informations sur le système de licences Citrix Gateway, consultez la documentation relative à Citrix Gateway. Pour plus d'informations sur le système de licences Citrix, consultez la section Système de licences Citrix.

Lorsque vous achetez XenMobile Server, vous recevez un e-mail de confirmation de commande contenant des instructions pour activer vos licences. Les nouveaux clients doivent s'inscrire à un programme de licence avant de passer commande. Pour plus d'informations sur les modèles de licence et programmes XenMobile, consultez la section Système de licences XenMobile.

Exigences

- Mettez à jour votre serveur de licences Citrix vers la version 11.16.x ou version ultérieure avant la mise à jour vers la dernière version de XenMobile Server. Les versions antérieures du serveur de licences ne prennent pas en charge la dernière version de XenMobile.
- Vous devez installer le système de licences Citrix avant de télécharger vos licences XenMobile. Le nom du serveur sur lequel vous avez installé le système de licences Citrix est requis pour générer le fichier de licences. Lorsque vous installez XenMobile, le système de licences Citrix est installé sur le serveur par défaut. Éventuellement, vous pouvez utiliser un déploiement de serveur de licences Citrix existant pour gérer vos licences XenMobile. Pour plus d'informations sur l'installation, le déploiement et la gestion du système de licences Citrix, consultez la section Obtenir une licence pour votre produit.
- si vous envisagez de mettre en cluster des nœuds ou instances de XenMobile, vous devez utiliser le système de licences Citrix sur un serveur distant.
- Citrix vous recommande de conserver des copies locales de tous les fichiers de licences que vous recevez. Lorsque vous enregistrez une copie de sauvegarde du fichier de configuration, elle inclut tous les fichiers de licences. Toutefois, si vous réinstallez XenMobile sans sauvegarder le fichier de configuration, vous aurez besoin des fichiers de licences d'origine.

Considérations sur les licences de XenMobile

En l'absence d'une licence, XenMobile reste pleinement fonctionnel en mode d'évaluation pendant une période de grâce de 30 jours. Ce mode d'évaluation ne peut être utilisé qu'une seule fois, et la

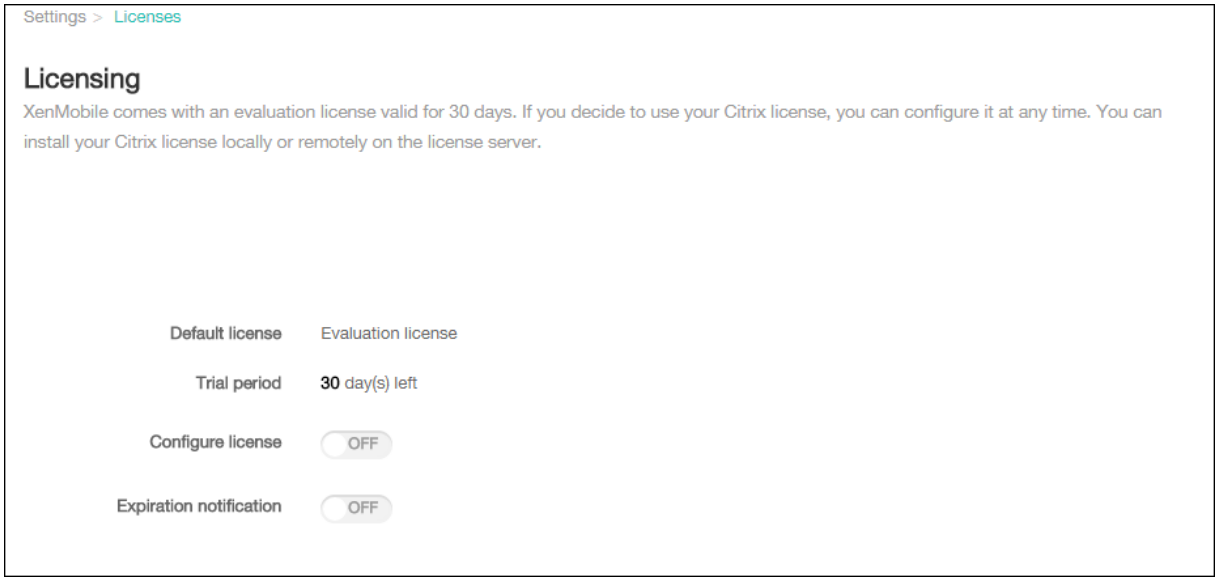
période de 30 jours commence à l'installation de XenMobile. L'accès à la console Web XenMobile n'est jamais bloqué, qu'une licence XenMobile valide soit disponible ou non. Dans la console XenMobile, vous pouvez voir combien de jours restent pour votre période d'évaluation.

Bien que XenMobile vous permette de charger plusieurs licences, seule une licence peut être activée à la fois.

Lorsqu'une licence XenMobile expire, vous ne pouvez plus exécuter les fonctions de gestion de l'appareil. Par exemple, de nouveaux utilisateurs ou de nouveaux appareils ne peuvent pas être inscrits et les applications et les configurations déployées sur les appareils inscrits ne peuvent pas être mises à jour. Pour plus d'informations sur les modèles de licence et programmes XenMobile, consultez la section Système de licences XenMobile.

Pour trouver la page Licences sur la console XenMobile

Lorsque la page **Licences** s'affiche pour la première fois après l'installation de XenMobile, la licence est définie par défaut pour le mode d'évaluation de 30 jours et n'est pas encore configurée. Vous pouvez ajouter et configurer des licences sur cette page.



1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Licences**. La page **Licences** s'ouvre.

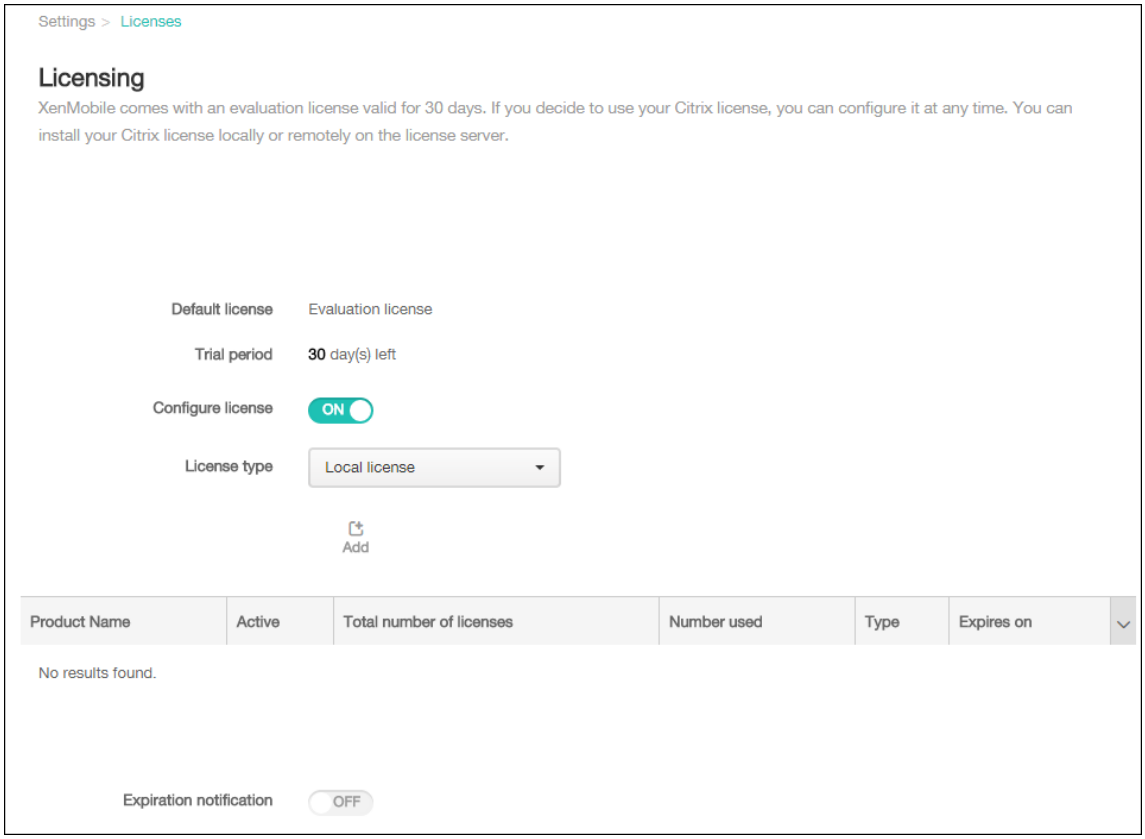
Pour ajouter une licence locale

Lors de l'ajout de nouvelles licences, celles-ci apparaissent dans le tableau. La première licence ajoutée est automatiquement activée. Si vous ajoutez plusieurs licences de la même catégorie, par exemple, Entreprise et du même type, ces licences sont affichées dans une seule ligne sur le tableau.

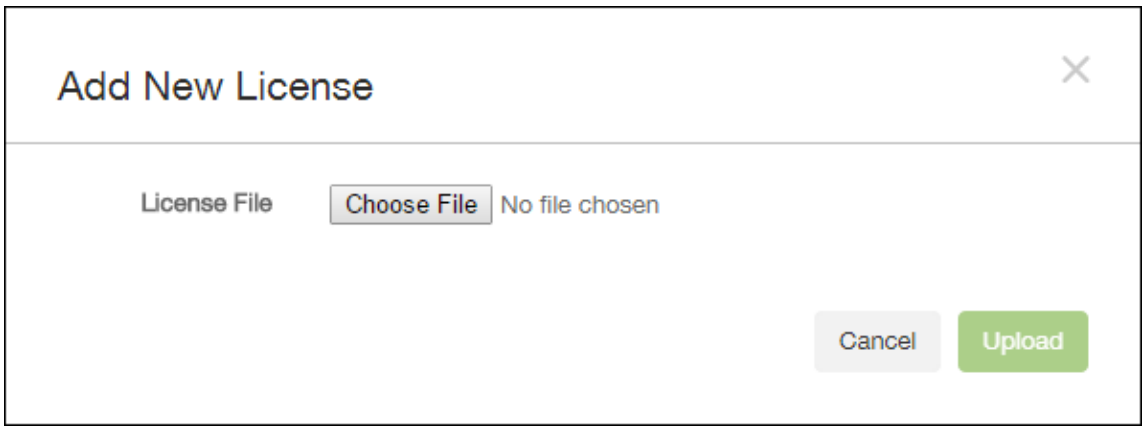
Dans ces cas de figure, **Nombre total de licences** et **Nombre utilisé** reflètent le montant cumulé des licences courantes. La date **Expire le** affiche la date d'expiration des licences courantes.

Vous pouvez gérer toutes les licences locales via la console XenMobile.

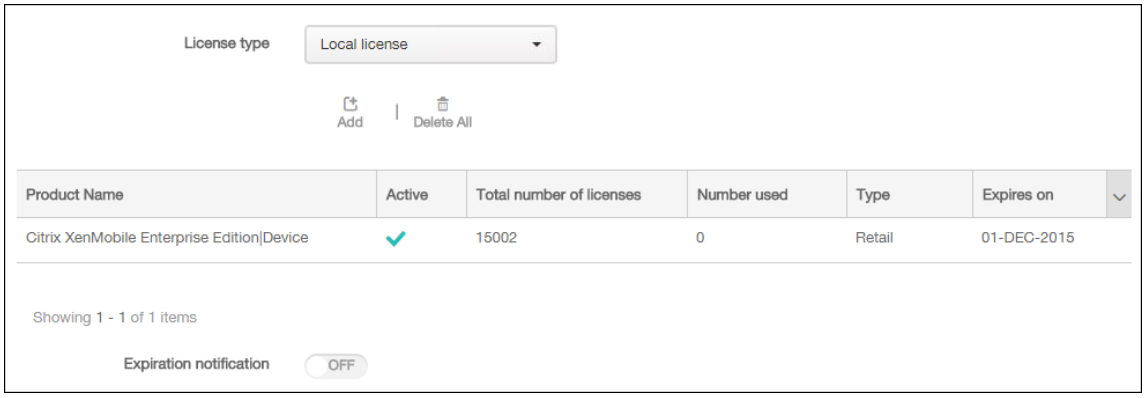
1. Obtenez un fichier de licences à l'aide de Simple License Service, au travers de la console License Administration Console, ou directement à partir de votre compte sur Citrix.com. Consultez la documentation relative au système de licences Citrix pour plus d'informations.
2. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
3. Cliquez sur **Licences**. La page **Licences** s'ouvre.
4. Définissez **Configurer licence** sur **Activé**. La liste **Type de licence**, le bouton **Ajouter** et le tableau **Licences** apparaissent. Le tableau **Licence** contient les licences que vous avez utilisées avec XenMobile. Si vous n'avez pas encore ajouté de licence Citrix, le tableau est vide.



5. Vérifiez que **Type de licence** est défini sur **Licence locale**, puis cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle licence** apparaît.



6. Dans la boîte de dialogue **Ajouter une nouvelle licence**, cliquez sur **Choisir un fichier**, puis recherchez l'emplacement de votre fichier de licence.
7. Cliquez sur **Charger**. Les licences sont chargées localement et s'affichent dans le tableau.



8. Lorsque la licence s'affiche dans le tableau sur la page **Licences**, activez-la. S'il s'agit de la première licence dans le tableau, la licence est activée automatiquement.

Pour ajouter une licence à distance

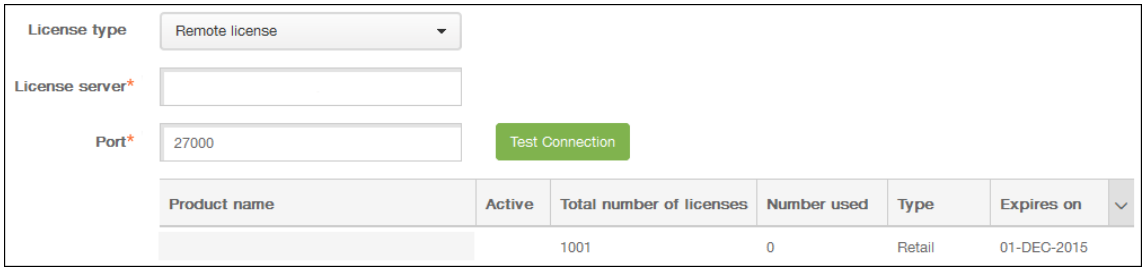
Si vous utilisez le serveur de licences Citrix à distance, utilisez le serveur de licences Citrix pour gérer *toutes* les activités liées aux licences. Pour plus d'informations, consultez la section Obtenir une licence pour votre produit.

1. Importez le certificat de serveur de licences dans XenMobile Server (**Paramètres > Certificats**).
2. Par défaut, la vérification de nom d'hôte est activée sur les connexions sortantes à l'exception du serveur PKI de Microsoft. Si la vérification de nom d'hôte interrompt votre déploiement, définissez la propriété de serveur **disable.hostname.verification** sur **true**. La valeur par défaut de cette propriété est **false**.

   Lorsque la vérification du nom d'hôte échoue, le journal du serveur contient des erreurs telles que : « Impossible de se connecter au serveur d'achat en volume : le nom d'hôte '192.0.2.0' ne

correspond pas à l'objet du certificat fourni par l'homologue ».

3. Sur la page **Licences**, définissez **Configurer licence** sur **Activé**. La liste **Type de licence**, le bouton **Ajouter** et le tableau **Licences** apparaissent. Le tableau **Licence** contient les licences que vous avez utilisées avec XenMobile. Si vous n'avez pas encore ajouté de licence Citrix, le tableau est vide.
4. Définissez **Type de licence** sur **Licence distante**. Le bouton **Ajouter** est remplacé par les champs **Serveur de licences** et **Port**, et le bouton **Tester la connexion**.

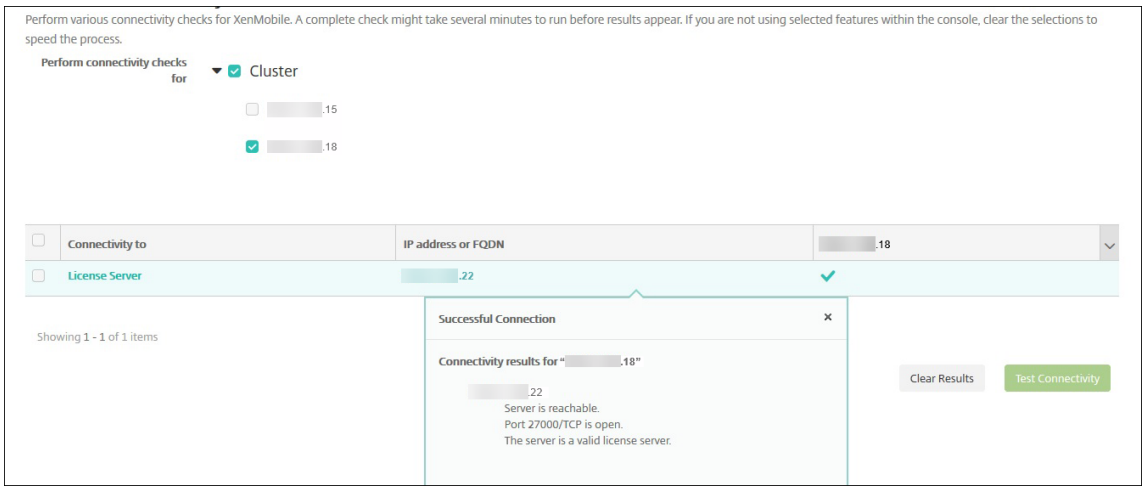


5. Pour configurer ces paramètres :
   - **Serveur de licences :** entrez l'adresse IP ou le nom de domaine complet (FQDN) de votre serveur de licences distant.
   - **Port :** acceptez le port par défaut ou saisissez le numéro de port utilisé pour communiquer avec le serveur de licences.
6. Cliquez sur **Tester la connexion**. Si la connexion est établie, XenMobile se connecte au serveur de licences et le tableau des licences est renseigné avec les licences disponibles. s'il n'existe qu'une seule licence, elle est activée automatiquement.

   Lorsque vous cliquez sur **Tester la connexion**, XenMobile vérifie les points suivants :

   - XenMobile peut communiquer avec le serveur de licences.
   - Les licences sur le serveur de licences sont valides.
   - Le serveur de licences est compatible avec XenMobile.

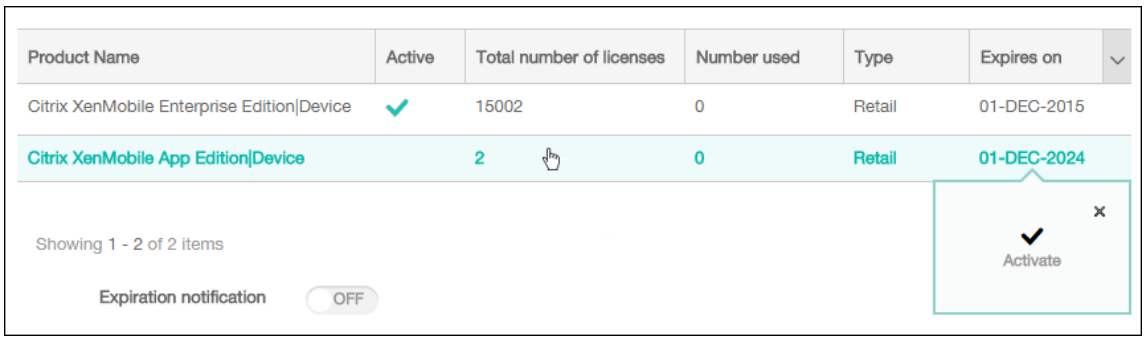
   Si la connexion échoue, consultez le message d'erreur affiché, apportez les corrections nécessaires, puis cliquez sur **Tester la connexion**.



Pour activer une autre licence

Si vous disposez de plusieurs licences, vous pouvez choisir la licence que vous souhaitez activer. Vous ne pouvez disposer que d'une seule licence active à la fois.

1. Sur la page **Licences**, dans le **tableau des licences**, cliquez sur la ligne de la licence que vous souhaitez activer. La boîte de dialogue de confirmation **Activer** apparaît à côté de la ligne.



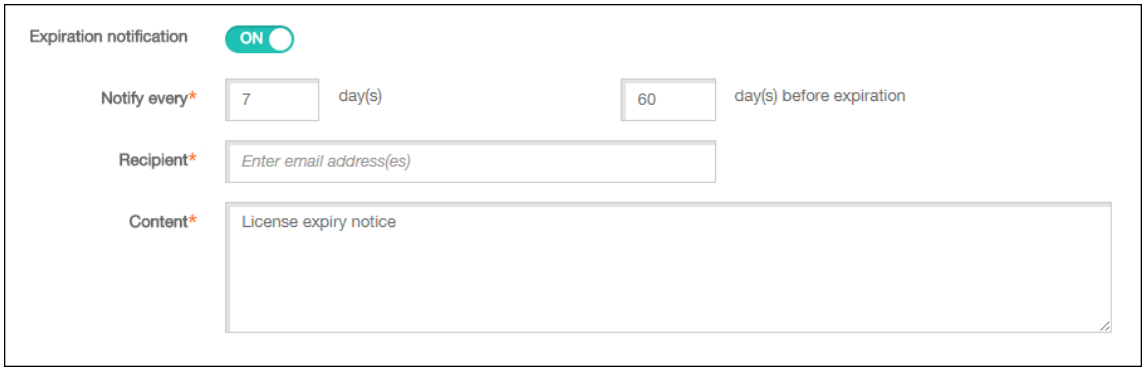
2. Cliquez sur **Activer**. La boîte de dialogue **Activer** s'affiche.
3. Cliquez sur **Activer**. La licence sélectionnée est activée.

> **Important :**
>
> si vous activez la licence sélectionnée, la licence actuellement active est désactivée.

Pour automatiser une notification d'expiration

Après avoir activé des licences distantes ou locales, vous pouvez configurer XenMobile pour qu'il vous informe (ou une personne que vous avez désignée) lorsque la date d'expiration de la licence approche.

1. Sur la page **Licences**, définissez **Notification d'expiration** sur **Activé**. Des nouveaux champs liés à la notification apparaissent.



2. Pour configurer ces paramètres :
    - **Notifier chaque :** entrez :
    - la fréquence à laquelle les notifications sont envoyées, telle que tous les **7** jours.
    - La date à laquelle commencer à envoyer la notification, telle que 60 jours avant l'expiration de la licence.
    - **Destinataire :** entrez votre adresse e-mail ou l'adresse e-mail de la personne responsable de la licence.
    - **Contenu :** entrez un message de notification d'expiration à l'attention du destinataire.
3. Cliquez sur **Enregistrer**. En fonction de vos paramètres, XenMobile commence à envoyer des messages contenant le texte que vous avez fourni dans **Contenu** aux destinataires que vous avez spécifiés dans **Destinataire**. Les notifications sont envoyées en fonction de la fréquence que vous avez définie.

Conformité FIPS 140-2

January 10, 2022

La norme FIPS (Federal Information Processing Standard) est publiée par le US National Institute of Standards and Technologies (NIST). FIPS spécifie les exigences de sécurité des modules cryptographiques utilisés dans les systèmes de sécurité. FIPS 140-2 est la seconde version de ce standard. Pour plus d'informations sur les modules FIPS 140 validés par NIST, consultez la page NIST Computer Security Resource Center.

> **Important :**
>
> - vous pouvez activer le mode XenMobile FIPS uniquement lors de l'installation initiale.
> - La gestion d'appareils mobiles XenMobile, la gestion d'applications mobiles XenMobile et la gestion MDM+MAM XenMobile sont conformes à la norme FIPS tant qu'aucune application HDX n'est utilisée.

Toutes les opérations de chiffrement de données au repos et données en transit sur iOS utilisent des modules de chiffrement certifiés FIPS fournis par Citrix et Apple. Sur Android, toutes les opérations de chiffrement de données au repos utilisent des modules de chiffrement certifiés FIPS fournis par les modules de chiffrement de la plate-forme fournis par le fabricant de l'appareil. Contactez votre représentant Citrix pour plus d'informations sur les modules des fabricants d'appareils.

Toutes les opérations de chiffrement de données au repos et données en transit pour Mobile Device Management (MDM) sur les appareils Windows pris en charge utilisent des modules de chiffrement certifiés FIPS.

Toutes les opérations de chiffrement de données au repos et de données en transit dans XenMobile MDM utilisent des modules cryptographiques certifiés FIPS. Toutes les données au repos et en transit pour les flux MDM utilisent des modules cryptographiques conformes à la norme FIPS de bout en bout. Cette sécurité inclut les opérations cryptographiques décrites ci-dessus pour les appareils mobiles, ainsi que les opérations cryptographiques entre les appareils mobiles et Citrix Gateway.

Le MDX Vault chiffre les applications MDX encapsulées et les données au repos associées sur les appareils iOS et Android à l'aide des modules cryptographiques validés FIPS.

Langues prises en charge

November 11, 2020

Les applications de productivité mobiles et la console XenMobile sont conçues pour être utilisées dans des langues autres que l'anglais. La prise en charge inclut les caractères étendus ainsi que les claviers non anglais même lorsque l'application n'est pas traduite dans la langue préférée d'un utilisateur. Pour de plus amples informations sur les différents niveaux d'internationalisation de tous les produits Citrix, consultez l'article https://support.citrix.com/article/CTX119253.

Cet article dresse la liste des langues prises en charge dans la dernière version de XenMobile.

Console XenMobile et portail en libre-service

- Français
- Allemand
- Espagnol
- Japonais
- Coréen
- Portugais
- Chinois simplifié

Applications de productivité mobiles

Un X indique que l'application est disponible dans cette langue.

iOS et Android

Langue	Secure Hub	Secure Mail	Secure Web	QuickEdit
Japonais	X	X	X	X
Chinois simplifié	X	X	X	X
Chinois traditionnel	X	X	X	X
Français	X	X	X	X
Allemand	X	X	X	X
Espagnol	X	X	X	X
Coréen	X	X	X	X
Portugais	X	X	X	X
Néerlandais	X	X	X	X
Italien	X	X	X	X
Danois	X	X	X	X
Suédois	X	X	X	X
Hébreu	X	X	X	iOS uniquement
Arabe	X	X	X	X
Russe	X	X	X	X
Turc	X	X	Android uniquement	-
Polonais	X	X	X	-

Windows

Langue	Secure Hub	Secure Mail	Secure Web
Français	X	X	X
Allemand	X	X	X
Espagnol	X	X	X

Langue	Secure Hub	Secure Mail	Secure Web
Italien	X	X	X
Danois	X	X	X
Suédois	X	X	X

Prise en charge des langues de droite à gauche

Le tableau suivant dresse la liste des langues du Moyen-Orient qui sont prises en charge pour chaque application. Un X indique que la fonctionnalité est disponible pour cette plate-forme. La prise en charge des langues de droite à gauche n'est pas disponible pour les appareils Windows.

Application	iOS	Android
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X
QuickEdit	X	X

Installer et configurer

January 10, 2022

Avant de commencer

Vous pouvez utiliser la check-list suivante qui dresse la liste des conditions préalables et des paramètres nécessaires à l'installation de XenMobile sur site. Chaque tâche ou note contient une colonne indiquant la fonction ou le composant pour lesquels la condition s'applique.

De nombreuses considérations sont à prendre en compte lors de la planification d'un déploiement XenMobile. Pour obtenir des conseils, accéder aux questions fréquemment posées et à des cas d'utilisation relatifs à votre environnement XenMobile complet, consultez le manuel de déploiement de XenMobile.

Vous trouverez la procédure d'installation dans la section Installer XenMobile plus loin dans cet article.

Checklist de pré-installation

Connectivité réseau de base

Voici les paramètres réseau dont vous avez besoin pour la solution XenMobile.

Prérequis ou paramètre	Composant ou fonction	Prendre note du paramètre
———————–	———–	——-
Notez le nom de domaine complet (FQDN) auquel les utilisateurs distants se connectent.	XenMobile et Citrix Gateway	
Notez l'adresse IP publique et locale.		
Vous avez besoin de ces adresses IP pour configurer le pare-feu afin de configurer la traduction d'adresses réseau (NAT).	XenMobile et Citrix Gateway	
Notez le masque de sous-réseau.	XenMobile et Citrix Gateway	
Notez les adresses IP DNS.	XenMobile et Citrix Gateway	
Notez les adresses IP du serveur WINS (le cas échéant).	Citrix Gateway	
Identifiez et notez le nom d'hôte Citrix Gateway.	Citrix Gateway	Cet élément n'est pas le nom de domaine complet. Le nom de domaine complet est contenu dans le certificat de serveur signé qui est lié au serveur virtuel et auquel les utilisateurs se connectent. Vous pouvez configurer le nom d'hôte à l'aide de l'assistant d'installation dans Citrix Gateway.	Citrix Gateway	
Notez l'adresse IP de XenMobile. Réservez une adresse IP si vous installez une instance de XenMobile. Si vous configurez un cluster, notez toutes les adresses IP dont vous avez besoin.	XenMobile	
Une adresse IP publique configurée sur Citrix Gateway	Citrix Gateway	
Une entrée DNS externe pour Citrix Gateway	Citrix Gateway	
Notez l'adresse IP du serveur proxy Web, le port, la liste des hôtes proxy, ainsi que le nom d'utilisateur et le mot de passe de l'administrateur. Ces paramètres sont facultatifs si vous déployez un serveur proxy sur votre réseau (le cas échéant).	Citrix Gateway	Vous pouvez utiliser sAMAccountName ou le nom d'utilisateur principal (UPN) lors de la configuration du nom d'utilisateur pour le proxy Web.	XenMobile et Citrix Gateway	
Notez l'adresse IP de la passerelle par défaut.	XenMobile et Citrix Gateway	
Notez l'adresse IP du système (NSIP) et le masque de sous-réseau.	Citrix Gateway	
Notez l'adresse IP du sous-réseau (SNIP) et le masque de sous-réseau.	Citrix Gateway	
Notez l'adresse IP du serveur virtuel Citrix Gateway et le nom de domaine complet du certificat. Pour configurer plusieurs serveurs virtuels, notez toutes les adresses IP virtuelles et les noms de domaine complets des certificats.	Citrix Gateway	
Notez les réseaux internes auxquels les utilisateurs peuvent accéder via Citrix Gateway. Exemple : 10.10.0.0/24 Entrez tous les réseaux internes et les segments de réseau auxquels les utilisateurs ont besoin d'accéder dans les cas suivants : lorsque les utilisateurs se connectent avec Secure Hub ou le plug-in Citrix Gateway lorsque le split tunneling est défini sur Activé.	Citrix Gateway	
Vérifiez que XenMobile Server, Citrix Gateway, le serveur Microsoft SQL externe et le serveur DNS peuvent communiquer entre eux.	XenMobile et Citrix Gateway	

Gestion des licences

XenMobile nécessite que vous achetiez des options de licences pour Citrix Gateway et XenMobile. Pour plus d'informations sur le système de licences Citrix, consultez la section Système de licences Citrix.

Conditions préalables	Composant	Noter l'emplacement
Obtenez des licences Universal à partir du site Web de Citrix. Pour plus d'informations, consultez la section Système de licences dans la documentation relative à Citrix Gateway.	Citrix Gateway, XenMobile et serveur de licences Citrix	

Certificats

XenMobile et Citrix Gateway nécessitent des certificats pour autoriser les connexions avec d'autres produits et applications Citrix et à partir de machines utilisateur. Pour de plus amples informations, consultez la section Certificats et authentification dans la documentation XenMobile.

Conditions préalables	Composant	Remarques
Obtenez et installez les certificats requis.	XenMobile et Citrix Gateway	

Ports

Ouvrez les ports pour autoriser la communication avec les composants XenMobile.

Conditions préalables	Composant	Remarques
Ouvrez les ports pour XenMobile	XenMobile et Citrix Gateway	

Base de données

XenMobile nécessite une configuration pour la connexion à la base de données. Le référentiel XenMobile nécessite une base de données Microsoft SQL Server exécutée sur l'une des versions prises en charge indiquées dans la section Configuration système requise et compatibilité. Citrix vous recommande d'utiliser Microsoft SQL à distance. PostgreSQL est inclus avec XenMobile. Utilisez PostgreSQL localement ou à distance *seulement* dans des environnements de test.

Par défaut, XenMobile utilise le pilote de la base de données jTDS. Pour utiliser le pilote Microsoft JDBC pour les installations locales de XenMobile Server, consultez la page Pilotes SQL Server.

Conditions préalables	Composant	Remarques
Adresse IP et port du serveur Microsoft SQL. Vérifiez que le compte de service du serveur SQL à utiliser sur XenMobile dispose de l'autorisation de rôle DBcreator.	XenMobile	

Paramètres Active Directory

Conditions préalables	Composant	Remarques
———	———	———
Notez l'adresse IP et le port Active Directory pour les serveurs principaux et secondaires. Si vous utilisez le port 636, installez un certificat racine à partir d'une autorité de certification sur XenMobile, puis modifiez l'option Utiliser des connexions sécurisées sur Oui.	XenMobile et Citrix Gateway	
Notez le nom de domaine Active Directory.	XenMobile et Citrix Gateway	
Notez le compte de service Active Directory qui requiert un ID utilisateur, un mot de passe et un alias de domaine.		
Le compte de service Active Directory est le compte utilisé par XenMobile pour interroger Active Directory.	XenMobile et Citrix Gateway	
Notez le nom unique de base de l'utilisateur, qui correspond au niveau d'arborescence sous lequel se trouvent les utilisateurs. Par exemple : `cn=users,dc=ace,dc=com`. Citrix Gateway et XenMobile utilisent le nom unique de base de l'utilisateur pour interroger Active Directory.	XenMobile et Citrix Gateway	
Notez le nom unique de base du groupe, qui correspond au niveau d'arborescence sous lequel se trouvent les groupes. Citrix Gateway et XenMobile utilisent ce nom unique pour interroger Active Directory.	XenMobile et Citrix Gateway	

Connexions entre XenMobile et Citrix Gateway

Conditions préalables	Composant	Prendre note du paramètre
Notez le nom d'hôte XenMobile.	XenMobile	

Conditions préalables	Composant	Prendre note du paramètre
Notez l'adresse IP ou le nom de domaine complet de XenMobile.	XenMobile	
Identifiez les applications auxquelles les utilisateurs peuvent accéder.	Citrix Gateway	
Notez l'URL de rappel.	XenMobile	

Connexions utilisateur : accès à Citrix Virtual Apps and Desktops et Citrix Secure Hub

Citrix vous recommande d'utiliser l'assistant de configuration rapide dans Citrix ADC pour configurer les paramètres de connexion entre XenMobile et Citrix Gateway et entre XenMobile et Secure Hub. Vous créez un deuxième serveur virtuel pour activer les connexions utilisateur à partir de Citrix Receiver et des navigateurs Web. Ces connexions sont effectuées vers des applications et des bureaux virtuels Windows dans Virtual Apps and Desktops. Citrix vous recommande d'utiliser l'assistant de configuration rapide dans Citrix ADC pour configurer ces paramètres.

Conditions préalables	Composant	Prendre note du paramètre
Notez le nom d'hôte de Citrix Gateway et l'URL externe. L'URL externe est l'adresse Web à laquelle les utilisateurs se connectent.	XenMobile	
Notez l'URL de rappel de Citrix Gateway.	XenMobile	
Notez les adresses IP et les masques de sous-réseau du serveur virtuel.	Citrix Gateway	
Notez le chemin d'accès à l'Agent Program Neighborhood ou à un site Virtual Apps and Desktops.	Citrix Gateway et XenMobile	

Conditions préalables	Composant	Prendre note du paramètre
Notez le nom de domaine complet ou l'adresse IP du serveur Citrix Virtual Apps and Desktops exécutant Secure Ticket Authority (STA) (pour les connexions ICA uniquement).	Citrix Gateway	
Notez le nom de domaine complet public de XenMobile.	Citrix Gateway	
Notez le nom de domaine complet public de Secure Hub.	Citrix Gateway	

Organigramme pour le déploiement de XenMobile

Vous pouvez utiliser cet organigramme pour vous guider dans les étapes principales du déploiement XenMobile. Vous trouverez des liens vers des rubriques liées à chaque étape après la figure.

1: Configuration système requise et compatibilité

2: Installer et configurer

3 et 4 : Checklist de pré-installation (cet article)

5 : Configurer XenMobile dans la fenêtre d'invite de commande (cet article)

6 : Configurer XenMobile dans un navigateur Web (cet article)

7: Configuration des paramètres de votre environnement XenMobile

8: Configuration requise pour les ports

Installer XenMobile

La machine virtuelle XenMobile (VM) fonctionne sur Citrix XenServer, VMware ESXi ou Microsoft Hyper-V. Vous pouvez utiliser les consoles de gestion XenCenter ou vSphere pour installer XenMobile.

> **Remarque :**
>
> Assurez-vous que l'hyperviseur est configuré avec l'heure correcte, à l'aide d'un serveur NTP ou d'une configuration manuelle, car XenMobile utilise cette heure. Si vous rencontrez des problèmes de fuseau horaire lors de la synchronisation de l'heure XenMobile avec un hyperviseur,

> vous pouvez éviter ces problèmes en pointant XenMobile sur un serveur NTP. Pour ce faire, utilisez l'interface de ligne de commande XenMobile, comme décrit dans la section Options d'interface de ligne de commande.

Prérequis XenServer ou VMware ESXi. Avant d'installer XenMobile sur XenServer ou VMware ESXi, vous devez effectuer les opérations suivantes. Pour de plus amples informations, consultez votre documentation XenServer ou VMware.

- Installez XenServer ou VMware ESXi sur un ordinateur doté des ressources matérielles appropriées.
- Installez XenCenter ou vSphere sur un autre ordinateur. L'ordinateur qui héberge XenCenter ou vSphere se connecte à l'hôte XenServer ou VMware ESXi via le réseau.

Prérequis Hyper-V. Avant d'installer XenMobile sur Hyper-V, vous devez effectuer les opérations suivantes. Pour plus d'informations, consultez votre documentation Hyper-V.

- Installez Windows Server 2008 R2, Windows Server 2012 ou Windows Server 2012 R2 avec le rôle Hyper-V activé, sur un ordinateur disposant des ressources système appropriées. Lors de l'installation du rôle Hyper-V, assurez-vous de spécifier les cartes d'interface réseau sur le serveur qui sera utilisé par Hyper-V pour créer les réseaux virtuels. Vous pouvez réserver certaines cartes d'interface réseau pour l'hôte.
- Supprimez le fichier Virtual Machines/<*UUID spécifique à la version*>.xml.
- Déplacez le fichier Legacy/<*UUID spécifique à la version*>.exp dans Virtual Machines.

Si vous installez Windows Server 2008 R2 ou Windows Server 2012, effectuez les opérations suivantes :

Ces étapes sont nécessaires, car il y existe deux versions différentes du fichier manifeste Hyper-V représentant la configuration d'une machine virtuelle (.exp et .xml). Les versions Windows Server 2008 R2 et Windows Server 2012 prennent en charge uniquement les fichiers .exp. Pour ces versions, vous devez uniquement disposer du fichier de manifeste .exp avant l'installation.

Windows Server 2012 R2 ne requiert pas ces étapes supplémentaires.

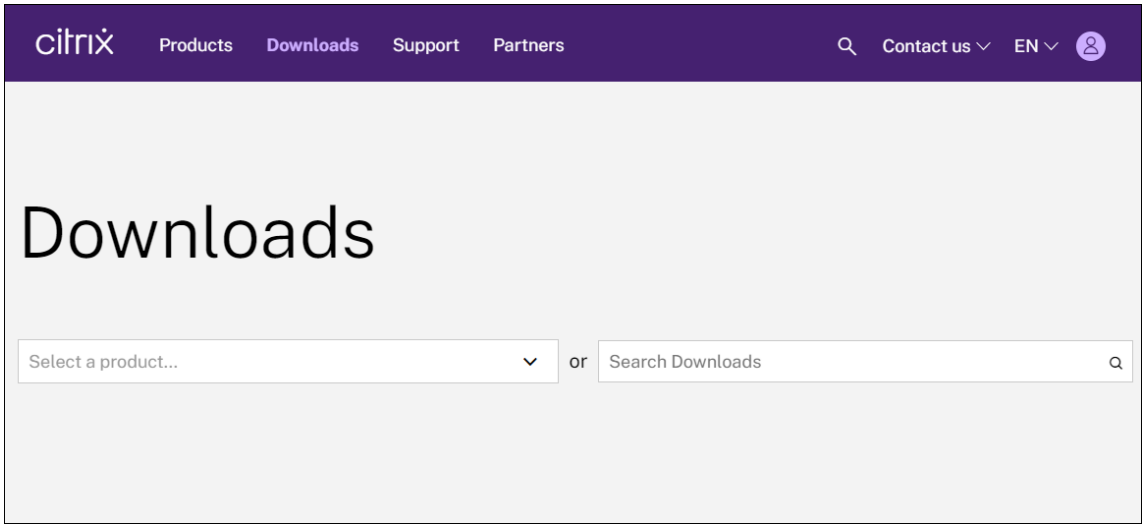
Mode FIPS 140-2. Pour installer XenMobile Server en mode FIPS, vous devez remplir un certain nombre de conditions préalables, comme abordé dans la section Configuration de FIPS avec XenMobile.

Télécharger le logiciel XenMobile

Vous pouvez télécharger le logiciel à partir du site Web de Citrix. Ouvrez une session sur le site, puis utilisez le lien Téléchargements pour accéder à la page contenant le logiciel que vous souhaitez télécharger.

Pour télécharger le logiciel pour XenMobile

1. Accédez au site Web Citrix.
2. À côté de la zone de recherche, cliquez sur **Log On** (Connexion), puis connectez-vous à votre compte.
3. Cliquez sur l'onglet **Downloads** (Téléchargements).
4. Sur la page Téléchargements, dans la liste **Sélectionner un produit**, cliquez sur **Citrix Endpoint Management (and Citrix XenMobile Server)**. La page Citrix Endpoint Management (and Citrix XenMobile Server) s'affiche automatiquement.



5. Développez **XenMobile Server (on-premises)**.
6. Développez **Product Software** (Logiciels produit).
7. Cliquez sur **XenMobile Server 10**.
8. Cliquez sur le menu **Jump to Download** et choisissez l'image virtuelle appropriée à utiliser pour installer XenMobile. Vous pouvez également faire défiler vers le bas de la page pour localiser le bouton **Download File** pour l'image que vous souhaitez installer.
9. Suivez les instructions à l'écran pour télécharger le logiciel.

Pour télécharger le logiciel pour Citrix Gateway

Vous pouvez utiliser cette procédure pour télécharger l'appliance virtuelle Citrix Gateway ou les mises à niveau logicielles de votre appliance Citrix Gateway existante.

1. Accédez au site Web Citrix.
2. Si vous n'êtes pas déjà connecté au site Web Citrix, à côté de la zone de recherche, cliquez sur **Log On** (Connexion), puis connectez-vous à votre compte.
3. Cliquez sur l'onglet **Downloads** (Téléchargements).

4. Sur la page Downloads (Téléchargements), à partir de la liste des produits, cliquez sur **Citrix Gateway**.
5. Cliquez sur **OK**. La page Citrix Gateway s'affiche.
6. Sur la page Citrix Gateway, développez la version de Citrix Gateway que vous exécutez.
7. Sous **Firmware**, cliquez sur la version du logiciel de l'appliance que vous souhaitez télécharger.

   > **Remarque :**
   >
   > Vous pouvez également cliquer sur **Virtual Appliances** pour télécharger Citrix ADC VPX. Lorsque vous sélectionnez cette option, vous recevez une liste des logiciels pour la machine virtuelle pour chaque hyperviseur.

8. Cliquez sur la version du logiciel de l'appliance que vous souhaitez télécharger.
9. Sur la page du logiciel d'appliance que vous voulez télécharger, sélectionnez l'appliance virtuelle et cliquez sur **Download** (Télécharger).
10. Suivez les instructions à l'écran pour télécharger le logiciel.

Configuration initiale de XenMobile

1. Pour configurez l'adresse IP et le masque de sous-réseau, la passerelle par défaut, les serveurs DNS et d'autres paramètres pour XenMobile, utilisez la console de ligne de commande de XenCenter ou de vSphere.

   > **Remarque :**
   >
   > Lorsque vous utilisez un client Web vSphere, nous vous recommandons de ne pas configurer les propriétés du réseau pendant que vous déployez le modèle OVF sur la page **Customize template**. Dans une configuration à haute disponibilité : vous évitez un problème qui se produit avec l'adresse IP lorsque vous clonez, puis redémarrez la seconde machine virtuelle XenMobile.

2. Accédez à la console de gestion XenMobile uniquement via le nom de domaine complet du serveur XenMobile ou les adresses IP du nœud.
3. Ouvrez une session et suivez les étapes des écrans d'ouverture de session.

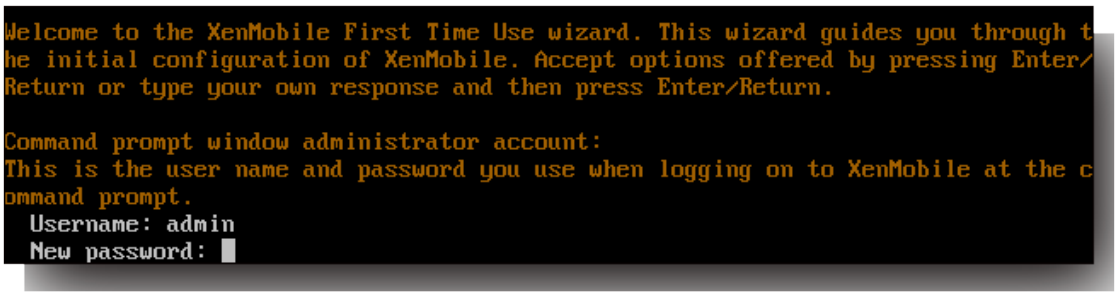
Configurer XenMobile dans la fenêtre d'invite de commande

1. Importez la machine virtuelle XenMobile dans Citrix XenServer, Microsoft Hyper-V ou VMware ESXi. Pour de plus amples informations, consultez votre documentation XenServer, Hyper-V ou VMware.

2. Dans votre hyperviseur, sélectionnez la machine virtuelle XenMobile importée et démarrez l'invite de commande. Pour de plus amples informations, consultez la documentation de votre hyperviseur.
3. À partir de la page de la console de l'hyperviseur, créez un compte d'administrateur pour XenMobile dans la fenêtre d'invite de commande en tapant le nom d'utilisateur et le mot de passe d'administrateur.

   Lorsque vous créez ou modifiez des mots de passe pour le compte d'administrateur dans l'invite de commande, des certificats de serveur PKI et FIPS, XenMobile applique les règles suivantes pour tous les utilisateurs, à l'exception des utilisateurs Active Directory dont les mots de passe sont gérés en dehors de XenMobile.

   - Le mot de passe doit contenir au moins huit caractères.
   - Le mot de passe doit respecter au moins trois des critères de complexité suivants :
     - Majuscules (de A à Z)
     - Minuscules (a à z)
     - Chiffres (de 0 à 9)
     - Caractères spéciaux (par exemple, ! ## $ %)

   Aucun caractère, par exemple un astérisque, ne s'affiche lorsque vous entrez le nouveau mot de passe.
4. Fournissez les informations réseau suivantes, puis tapez **y** pour valider les paramètres :

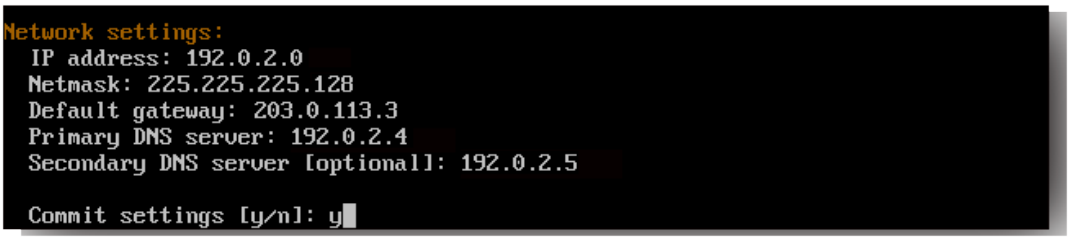
   a) Adresse IP du serveur XenMobile

   b) Masque réseau

   c) Passerelle par défaut qui correspond à l'adresse IP de la passerelle par défaut dans la DMZ

   d) Serveur DNS principal qui correspond à l'adresse IP du serveur DNS

   e) Serveur DNS secondaire (facultatif)



> **Remarque :**
>
> Les adresses indiquées dans cette image et les suivantes ne fonctionnent pas et sont fournies à titre d'exemple uniquement.

5. Tapez **y** pour renforcer la sécurité en générant une phrase secrète de cryptage aléatoire ou **n** pour fournir votre propre phrase secrète. Citrix recommande de taper **y** pour générer une phrase secrète aléatoire.

   La phrase secrète est utilisée dans le cadre de la protection des clés de chiffrement utilisées pour sécuriser vos données confidentielles. Un hachage de la phrase secrète, stocké dans le système de fichiers du serveur, est utilisé pour récupérer les clés durant le chiffrement et déchiffrement des données. La phrase secrète ne peut pas être affichée.

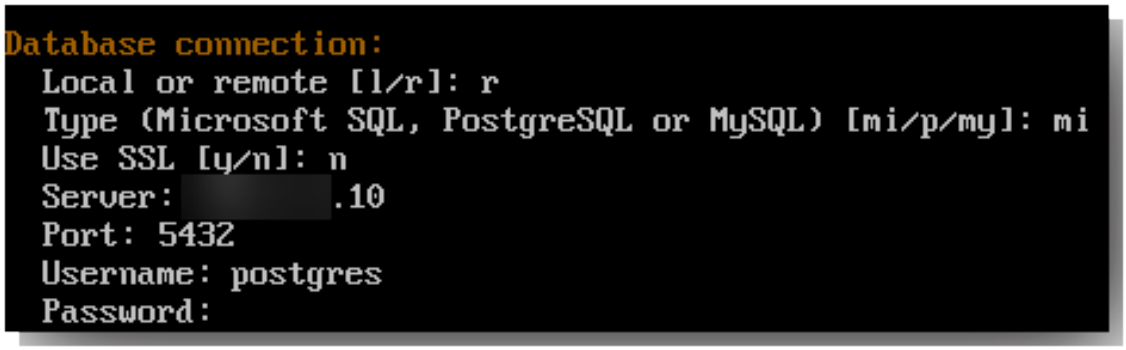
   > **Remarque :**
   >
   > Si vous souhaitez étendre votre environnement et configurer des serveurs supplémentaires, fournissez votre propre phrase secrète. Si vous sélectionnez une phrase secrète aléatoire, vous ne pouvez pas l'afficher.

6. Activez éventuellement FIPS (Federal Information Processing Standard). Pour plus de détails sur la norme FIPS, consultez la section FIPS. Vous devez également vous assurer que certaines conditions sont respectées, comme abordé dans la section Configurer FIPS avec XenMobile.

7. Fournissez les informations suivantes pour configurer la connexion à la base de données.



- Votre base de données peut être locale ou distante. Tapez **l** pour une base de données locale ou **r** pour une base de données distante.
- Sélectionnez le type de base de données. Tapez **mi** pour Microsoft SQL ou tapez **p** pour PostgreSQL.

  > **Important :**
  >
  > – Citrix vous recommande d'utiliser Microsoft SQL à distance. PostgreSQL est inclus avec XenMobile. Utilisez PostgreSQL localement ou à distance *seulement* dans des environnements de test.
  > – La migration de la base de données n'est pas prise en charge. Les bases de données créées dans un environnement de test ne peuvent pas être déplacées dans un environnement de production.

- Tapez éventuellement **y** pour utiliser l'authentification SSL pour votre base de données.
- Indiquez le nom de domaine complet (FQDN) du serveur hébergeant XenMobile. Ce serveur hôte fournit à la fois des services de gestion d'appareils et de gestion d'applications.
- Tapez le numéro de port de votre base de données s'il est différent du numéro de port par défaut. Le port par défaut pour Microsoft SQL est 1433 et le port par défaut pour PostgreSQL est 5432.
- Tapez le nom d'utilisateur d'administrateur de votre base de données.
- Tapez le mot de passe d'administrateur de votre base de données.
- Tapez le nom de la base de données.
- Appuyez sur **Entrée** pour valider les paramètres de la base de données.

8. Tapez éventuellement **y** pour activer la mise en cluster des nœuds ou instances XenMobile.

   > **Important :**
   >
   > Si vous activez un cluster XenMobile, une fois la configuration du système terminée, ouvrez

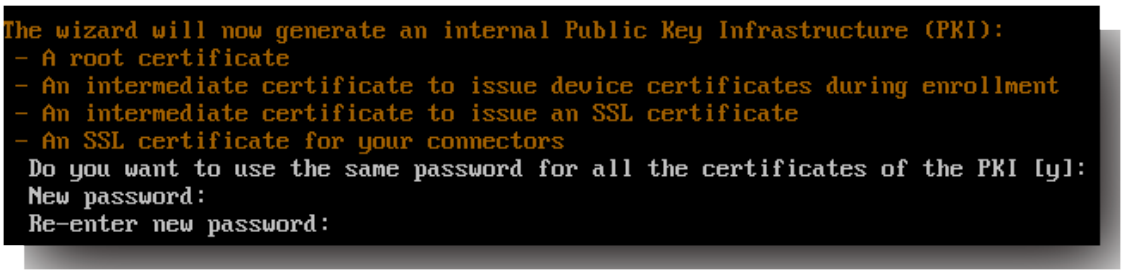
> le port 80 pour activer les communications en temps réel entre les membres du cluster. Terminez cette installation sur tous les nœuds de cluster.

9. Tapez le nom de domaine complet (FQDN) de XenMobile Server.

10. Appuyez sur **Entrée** pour valider les paramètres.
11. Identifiez les ports de communication. Pour de plus amples informations sur les ports et leurs utilisations, consultez la section Configuration requise pour les ports.

> **Remarque :**
>
> Acceptez les ports par défaut en appuyant sur **Entrée** (ou Retour sur un Mac).

12. Ignorez la question suivante sur la mise à niveau à partir d'une version précédente de XenMobile, car vous installez XenMobile pour la première fois.
13. Tapez **y** si vous souhaitez utiliser le même mot de passe pour chaque certificat PKI. Pour plus d'informations sur la fonctionnalité PKI de XenMobile, consultez la section Chargement de certificats.



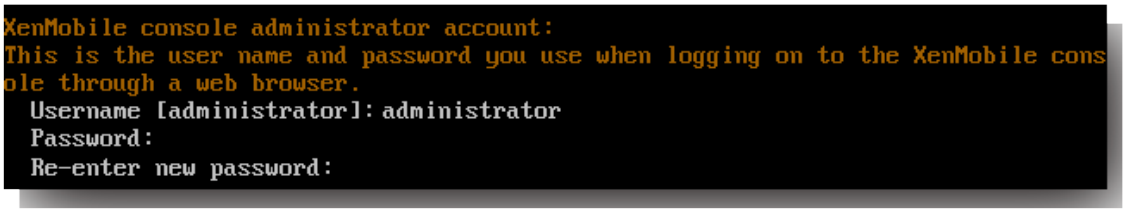
> **Important :**
>
> Si vous envisagez de mettre en cluster des nœuds ou instances de XenMobile, fournissez les mêmes mots de passe pour chaque nœud.

14. Tapez le nouveau mot de passe, puis retapez-le pour le confirmer.

    Aucun caractère, par exemple un astérisque, ne s'affiche lorsque vous entrez le nouveau mot de passe.

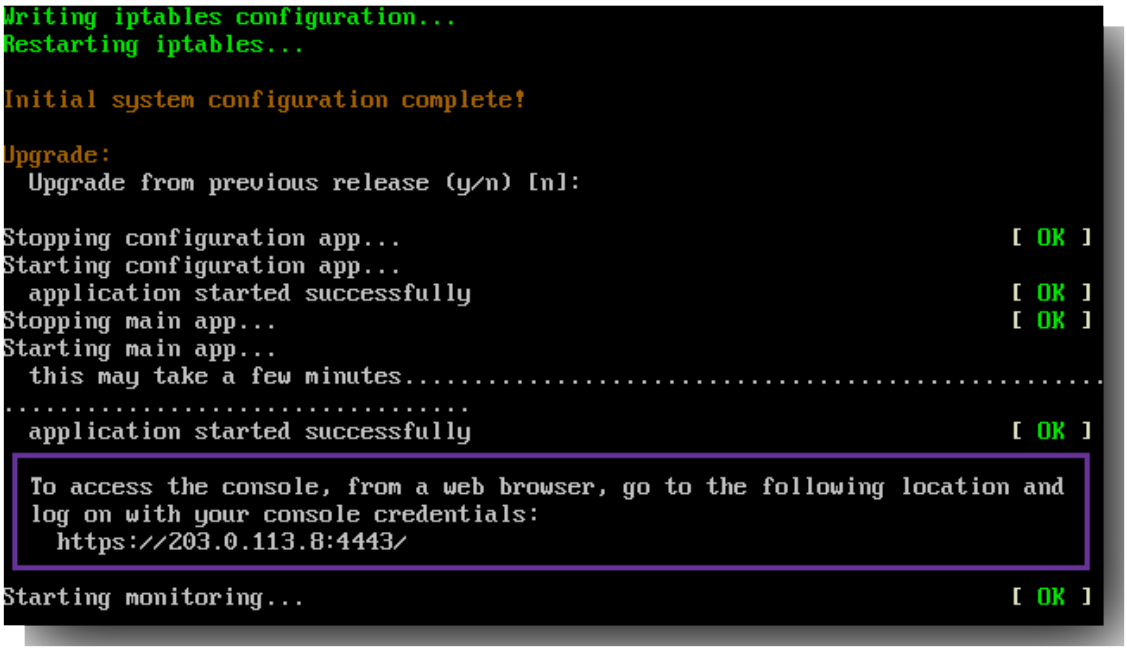
15. Appuyez sur **Entrée** pour valider les paramètres.

16. Créez un compte d'administrateur pour la connexion à la console XenMobile avec un navigateur Web. Veillez à enregistrer ces informations d'identification pour une utilisation ultérieure.



> **Remarque :**
>
> Aucun caractère, par exemple un astérisque, ne s'affiche lorsque vous entrez le nouveau mot de passe.

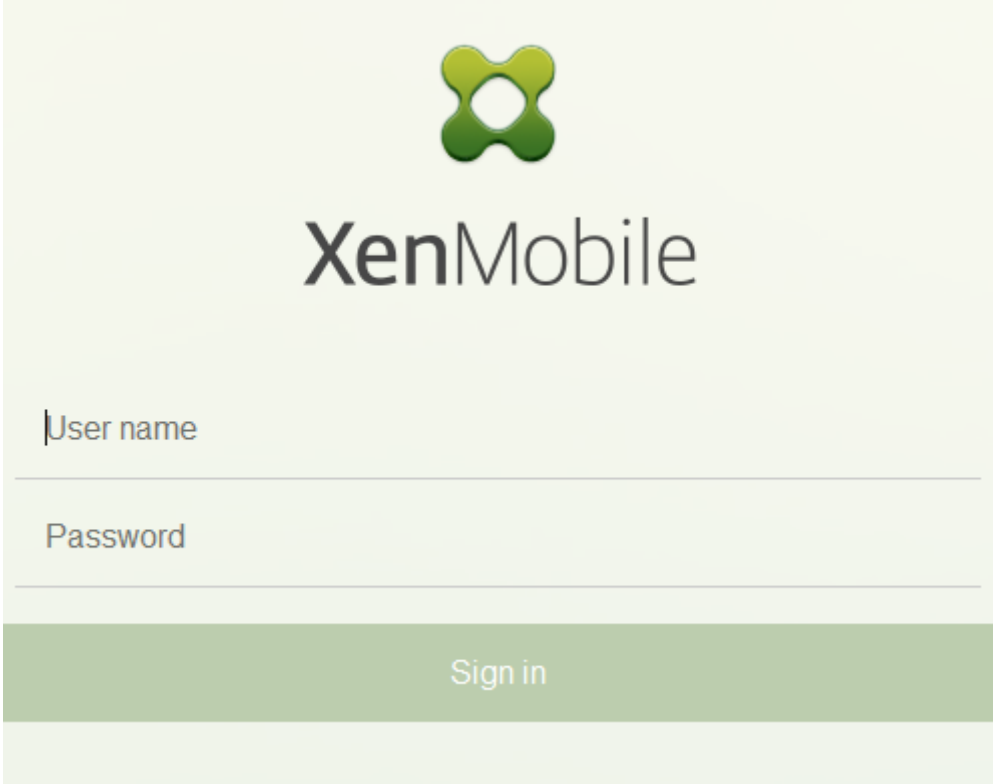
17. Appuyez sur **Entrée** pour valider les paramètres. La configuration du système est enregistrée.
18. Lorsque vous êtes invité à indiquer si vous procédez à une mise à niveau, tapez **n** car il s'agit d'une nouvelle installation.
19. Copiez l'URL complète qui s'affiche sur l'écran et continuez la configuration initiale de XenMobile dans votre navigateur Web.



Configurer XenMobile dans un navigateur Web

Une fois la première partie de la configuration de XenMobile terminée dans la fenêtre d'invite de commandes de votre hyperviseur, continuez le processus dans votre navigateur Web.

1. Dans votre navigateur Web, accédez à l'emplacement fourni à la fin de la fenêtre d'invite de commandes.
2. Entrez le nom d'utilisateur et le mot de passe du compte administrateur de la console XenMobile console que vous avez créés dans la fenêtre d'invite de commandes.



3. Dans la page Mise en route, cliquez sur **Démarrer**. La page **Licences** s'ouvre.
4. Configurez la licence. Si vous ne chargez pas de licence, une licence d'évaluation valide pendant 30 jours sera utilisée. Pour plus d'informations sur l'ajout et la configuration de licences et la configuration de notifications d'expiration, consultez la section Gestion des licences.

> **Important :**
>
> Si vous envisagez d'utiliser la mise en cluster XenMobile en ajoutant des nœuds ou instances de XenMobile, vous devez utiliser le système de licences Citrix sur un serveur distant.

5. Sur la page **Certificats**, cliquez sur **Importer**. La boîte de dialogue Importer apparaît.
6. Importez vos certificats APNs et SSL Listener. La gestion des appareils iOS nécessite un certificat APNs. Pour de plus amples informations sur l'utilisation de certificats, consultez la section Certificats.

> **Remarque :**
>
> Cette étape nécessite le redémarrage du serveur.

7. Si cela est approprié pour l'environnement, configurez Citrix Gateway. Pour de plus amples informations sur la configuration de Citrix Gateway, consultez les sections Citrix Gateway et XenMobile et Configuration des paramètres de votre environnement XenMobile.

   > **Remarque :**
   >
   > - Vous pouvez déployer Citrix Gateway sur le périmètre de votre réseau interne (ou intranet). Ce déploiement fournit un point d'accès unique sécurisé aux serveurs, applications et autres ressources réseau résidant sur le réseau interne. Dans ce déploiement, tous les utilisateurs distants doivent se connecter à Citrix Gateway pour pouvoir accéder aux ressources du réseau interne.
   > - Bien que Citrix Gateway soit un paramètre facultatif, après la saisie de données sur la page, vous devez effacer ou compléter les champs obligatoires avant de quitter la page.

8. Terminez la configuration LDAP pour accéder aux utilisateurs et groupes à partir d'Active Directory. Pour de plus amples informations sur la configuration de la connexion LDAP, consultez la section Configuration LDAP.
9. Configurez le serveur de notification de manière à pouvoir envoyer des messages aux utilisateurs. Pour de plus amples informations sur la configuration du serveur de notification, consultez la section Notifications.

Post-requis : redémarrez XenMobile Server pour activer vos certificats.

Configurer FIPS avec XenMobile

January 10, 2022

Le mode FIPS (Federal Information Processing Standards) dans XenMobile prend en charge les clients du gouvernement fédéral américain en utilisant uniquement des annuaires certifiés FIPS 140-2 pour toutes les opérations de cryptage. L'installation de XenMobile Server avec le mode FIPS garantit que toutes les données pour le client et le serveur XenMobile sont entièrement conformes à la norme FIPS 140-2. Cette conformité s'applique aux données au repos et aux données en transit.

Avant d'installer XenMobile Server en mode FIPS, vous devez remplir les conditions préalables suivantes.

- Utilisez un SQL Server 2014 externe pour la base de données XenMobile. Le SQL Server doit également être configuré pour sécuriser les communications avec SSL. Pour obtenir des instruc-

tions sur la configuration de la communication SSL sécurisée avec SQL Server, consultez Activer les connexions chiffrées dans le moteur de base de données (Gestionnaire de configuration SQL Server).

- La communication SSL sécurisée nécessite l'installation d'un certificat SSL approuvé provenant d'une autorité de certification bien connue sur votre SQL Server. Veuillez noter que SQL Server 2014 n'accepte pas les certificats génériques. Citrix vous recommande par conséquent de demander un certificat SSL avec le nom de domaine complet du SQL Server.

Configuration du mode FIPS

Vous pouvez activer le mode FIPS uniquement lors de l'installation initiale de XenMobile Server. Il n'est pas possible d'activer le mode FIPS une fois l'installation terminée. Par conséquent, si vous envisagez d'utiliser le mode FIPS, vous devez installer XenMobile Server avec le mode FIPS dès le début. En outre, pour les clusters XenMobile, FIPS doit être activé pour tous les nœuds de cluster. Vous ne pouvez pas avoir un mélange de serveurs XenMobile FIPS et non-FIPS dans le même cluster.

L'option **Toggle FIPS mode** dans l'interface de ligne de commande XenMobile n'est pas destinée à une utilisation en production. Cette option est conçue pour les environnements de non production, à des fins de diagnostic et n'est pas prise en charge sur un serveur XenMobile de production.

1. Durant l'installation initiale, activez **FIPS mode**.
2. Chargez le certificat d'autorité de certification racine pour votre SQL Server.
3. Spécifiez le nom et le port du serveur de votre SQL Server, les informations d'identification permettant de se connecter à SQL Server, et le nom de la base de données à créer pour XenMobile.

   > **Remarque :**
   >
   > Vous pouvez utiliser au choix une ouverture de session SQL ou un compte Active Directory pour accéder à SQL Server, mais l'ouverture de session que vous utilisez doit avoir le rôle DBcreator.

4. Pour utiliser un compte Active Directory, entrez les informations d'identification au format domaine\nomutilisateur.
5. Une fois ces étapes terminées, procédez à l'installation initiale de XenMobile.

Pour confirmer que le mode FIPS est opérationnel, ouvrez une session sur l'interface de ligne de commande XenMobile. La phrase **In FIPS Compliant Mode** apparaît dans la bannière d'ouverture de session.

Importation de certificats

La procédure suivante décrit comment configurer FIPS sur XenMobile en important le certificat, ce qui est requis lorsque vous utilisez un hyperviseur VMware.

Configuration SQL requise

1. La connexion à l'instance SQL à partir de XenMobile doit être sécurisée et doit être SQL Server version 2012 ou SQL Server 2014. Pour sécuriser la connexion, consultez la page Comment activer le chiffrement SSL pour une instance de SQL Server à l'aide de la console MMC.
2. Si le service ne redémarre pas correctement, vérifiez ce qui suit : ouvrez **Services.msc**.
   a) Copiez les informations du compte d'ouverture de session utilisées pour le service SQL Server.
   b) Ouvrez MMC.exe sur le SQL Server.
   c) Accédez à **Fichier > Ajouter/Supprimer un composant logiciel enfichable** et double-cliquez sur les certificats pour ajouter le composant logiciel enfichable Certificats. Sélectionnez le compte d'ordinateur et l'ordinateur local dans les deux pages de l'assistant.
   d) Cliquez sur **OK**.
   e) Développez **Certificats (ordinateur local) > Personnel > Certificats** et localisez le certificat SSL importé.
   f) Cliquez avec le bouton droit sur le certificat importé (sélectionné dans le Gestionnaire de configuration SQL Server) et cliquez sur **Toutes les tâches > Gérer les clés privées**.
   g) Sous **Noms de groupe ou d'utilisateur**, cliquez sur **Ajouter**.
   h) Entrez le nom de compte du service SQL que vous avez copié dans l'étape précédente.
   i) Décochez l'option **Autoriser Contrôle total**. Par défaut, les autorisations Contrôle totale et Lecture seront accordées au compte de service, toutefois il a seulement besoin de pouvoir lire la clé privée.
   j) Fermez **MMC** et démarrez le service SQL.
3. Assurez-vous que le service SQL est démarré correctement.

Conditions requises par les services Internet (IIS)

1. Téléchargez le certificat racine (base 64).
2. Copiez le certificat racine sur le site par défaut sur le serveur IIS, C:\inetpub\wwwroot.
3. Cochez la case **Authentification** du site par défaut.
4. Définissez **Anonyme** sur **Activé**.
5. Sélectionnez la case à cocher des règles **Échec de la demande de suivi**.
6. Assurez-vous que .cer n'est pas bloqué.

7. Accédez à l'emplacement du .cer dans un navigateur Web à partir du serveur local, `https://localhost/certname.cer`. Le texte du certificat racine apparaît dans le navigateur.
8. Si le certificat racine ne s'affiche pas dans votre navigateur Web, assurez-vous que ASP est activé sur le serveur IIS comme suit.
   a) Ouvrez le gestionnaire de serveur.
   b) Accédez à l'assistant sous **Gérer > Ajouter des rôles et fonctionnalités**.
   c) Dans les rôles de serveur, développez **Serveur Web (IIS)**, développez **Serveur Web**, développez **Développement d'applications** et sélectionnez **ASP**.
   d) Cliquez sur **Suivant** jusqu'à ce que l'installation soit terminée.
9. Accédez à `https://localhost/cert.cer`.

   Pour plus d'informations, consultez la section Serveur Web (IIS).

   > **Remarque :**
   >
   > Vous pouvez utiliser l'instance IIS de l'autorité de certification pour cette procédure.

Importation du certificat racine durant la configuration initiale de FIPS

Lorsque vous configurez XenMobile pour la première fois dans la console de ligne de commande, vous devez définir les paramètres suivants pour importer le certificat racine. Pour plus de détails sur les étapes d'installation, consultez la section Installer XenMobile.

- Enable FIPS : Yes
- Upload Root Certificate : Yes
- Copy(c) or Import(i) : i
- Entrez l'URL HTTP à importer : `https://<FQDN of IIS server>/cert.cer`
- Server : *Nom de domaine complet de SQL Server*
- Port : 1433
- User name : compte de service qui peut créer la base de données (`domain\username`)
- Password : mot de passe du compte de service.
- Database Name : un nom de votre choix.

Activer le mode FIPS sur des appareils mobiles

Par défaut, le mode FIPS est désactivé sur les appareils mobiles. Pour activer le mode FIPS, accédez à **Paramètres > Propriétés du client**, modifiez la propriété **Activer le mode FIPS** et définissez la valeur sur **true**. Pour de plus amples informations, consultez la section Propriétés du client.

Configurer la mise en cluster

January 10, 2022

Pour configurer la mise en cluster, configurez les deux adresses IP virtuelles d'équilibrage de charge suivantes sur Citrix ADC.

- **Adresse IP virtuelle d'équilibrage de charge MDM :** une adresse IP virtuelle d'équilibrage de charge MDM est requise pour communiquer avec les nœuds XenMobile qui sont configurés dans un cluster. L'équilibrage de charge est effectué en mode pont SSL.
- **Adresse IP virtuelle d'équilibrage de charge MAM :** des adresses IP virtuelles d'équilibrage de charge MAM sont requises pour que Citrix Gateway communique avec les nœuds XenMobile qui sont configurés dans un cluster. Dans XenMobile, par défaut, tout le trafic provenant de Citrix Gateway est acheminé vers l'adresse IP virtuelle d'équilibrage de charge sur le port 8443.

Les procédures décrites dans cet article expliquent comment créer une nouvelle machine virtuelle (VM) XenMobile et associer la nouvelle VM à une VM existante. Ces étapes créent une configuration de cluster.

Conditions préalables

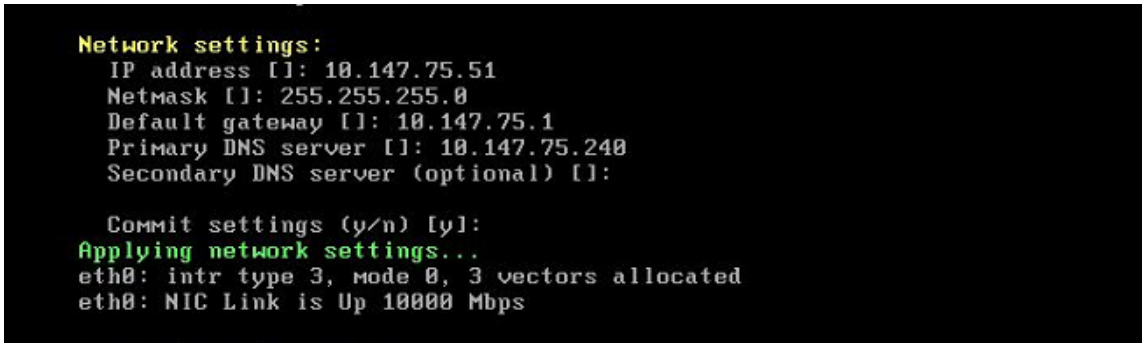
- Vous avez entièrement configuré le nœud XenMobile requis.
- Configurez NTP sur tous les nœuds de cluster et la base de données XenMobile. La mise en cluster ne fonctionne que si tous ces serveurs sont réglés sur la même heure.
- Une adresse IP publique pour l'équilibrage de charge MDM et une adresse IP privée pour MAM.
- Des certificats de serveur.
- Une adresse IP disponible pour l'adresse IP virtuelle de Citrix Gateway.
- Lorsque XenMobile est déployé dans un cluster et en mode MDM exclusif ou entreprise (MDM+MAM) : modifiez votre configuration d'équilibrage de charge Citrix ADC pour utiliser la **persistance de l'adresse IP Source** pour tous les équilibrages de charge MDM Citrix ADC, c'est-à-dire les serveurs virtuels configurés pour les ports 8443 et 443. Effectuez cette configuration avant la mise à niveau des machines utilisateur vers iOS 11. Pour plus d'informations, consultez cet article dans le centre de connaissances Citrix : https://support.citrix.com/article/CTX227406.
- Pour installer des applications depuis XenMobile Store sur les appareils iOS 11, vous devez activer le port 80 sur XenMobile Server.

Pour consulter des diagrammes d'architecture de référence XenMobile 10.x dans des configurations en cluster, consultez la section Architecture.

Installation des nœuds de cluster XenMobile

En fonction du nombre de nœuds requis, vous pouvez créer des VM XenMobile. Pointez la nouvelle VM vers la même base de données et fournissez les mêmes mots de passe de certificat PKI.

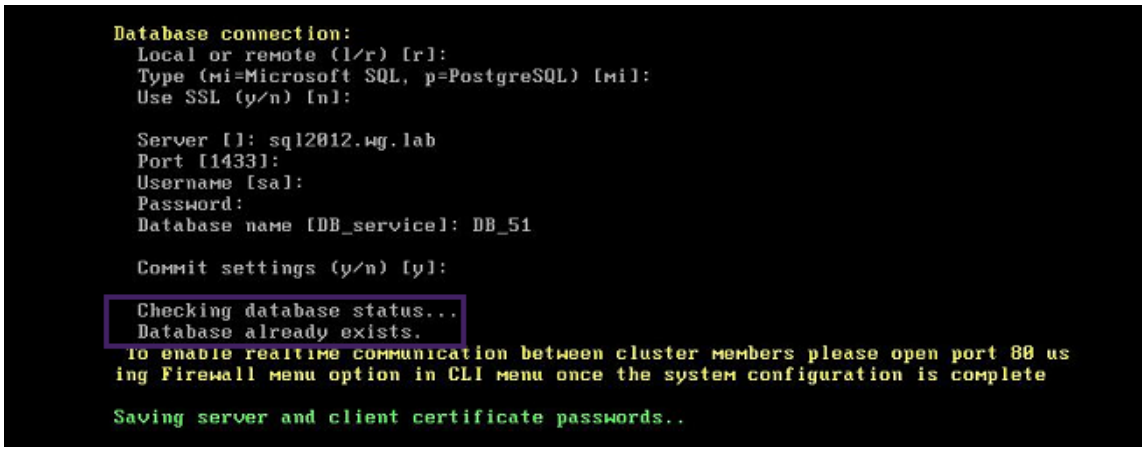
1. Ouvrez la console de ligne de commande de la nouvelle VM et entrez le nouveau mot de passe du compte administrateur.
2. Fournissez les détails de la configuration du réseau, comme indiqué dans la figure suivante.



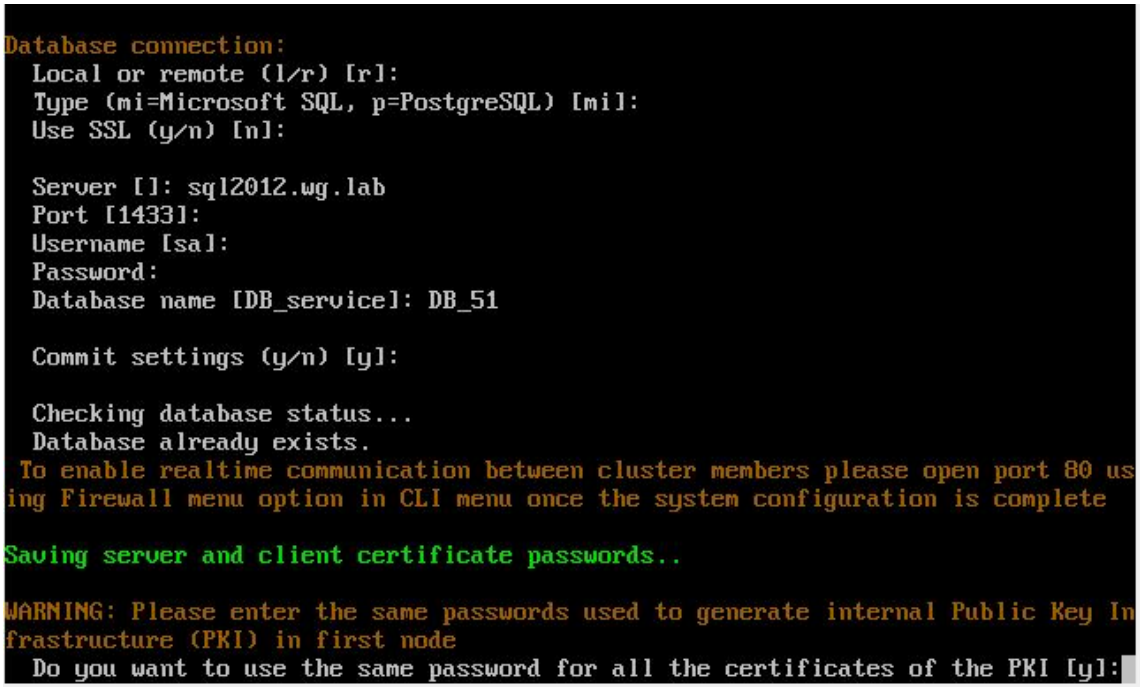
3. Si vous souhaitez utiliser le mot de passe par défaut pour la protection des données, tapez **y** ou tapez **n** et entrez le nouveau mot de passe.

4. Si vous souhaitez utiliser FIPS, tapez **y**. Sinon, tapez **n**.

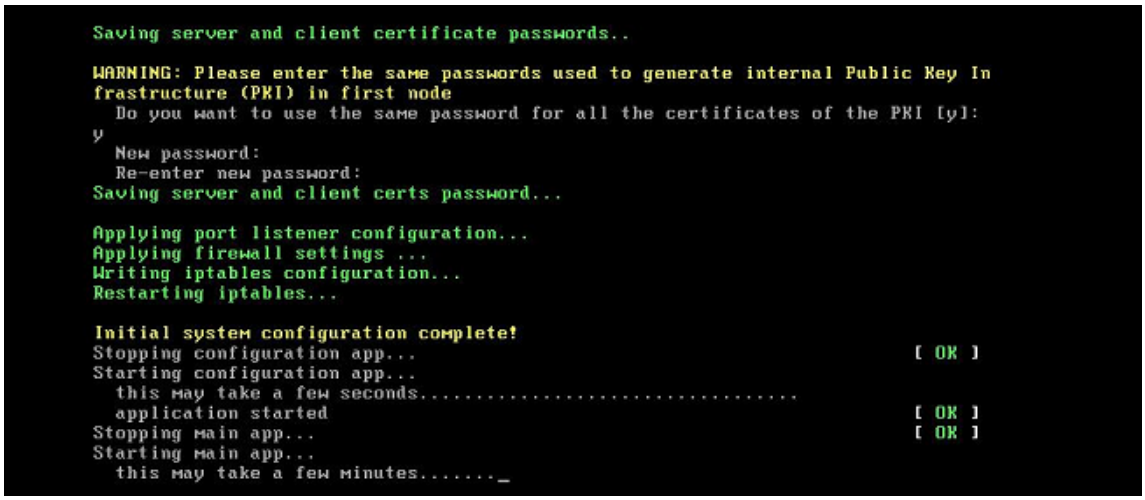
5. Configurez la base de données pour pointer sur la même base de données que la VM entièrement configurée précédemment. Le message suivant s'affiche : « La base de données existe déjà ».



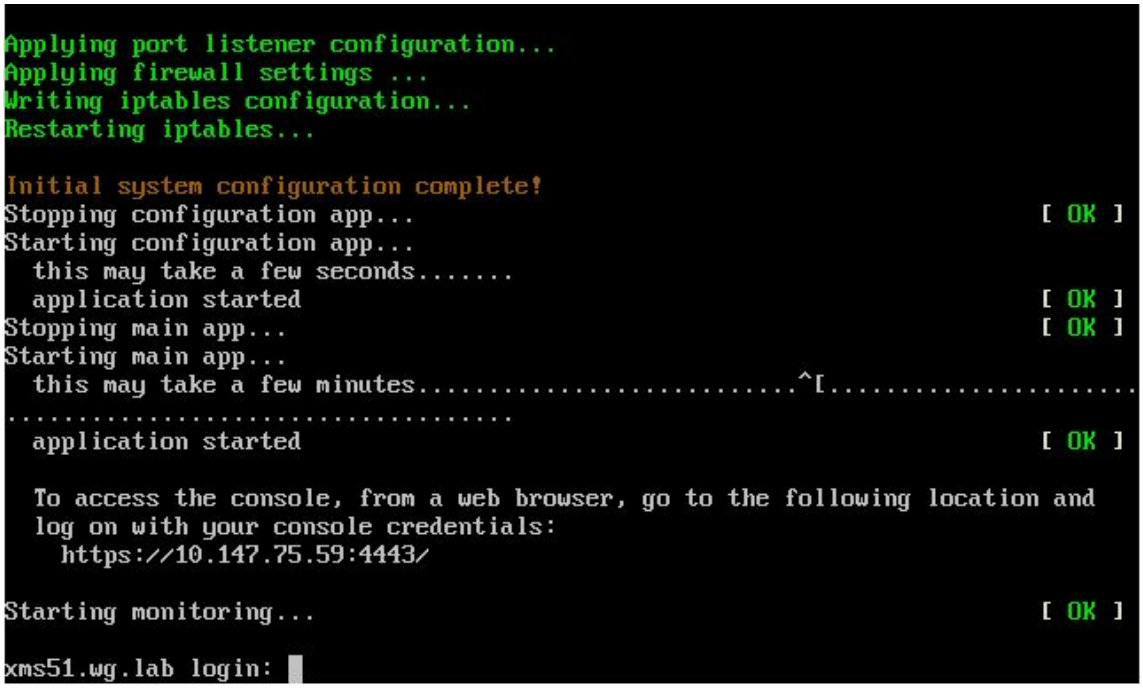
6. Entrez les mêmes mots de passe pour les certificats que vous avez fournis pour la première VM.



Une fois que vous avez entré le mot de passe, la configuration initiale sur le second nœud se termine.



7. Une fois la configuration terminée, le serveur redémarre et la boîte de dialogue d'ouverture de session apparaît.

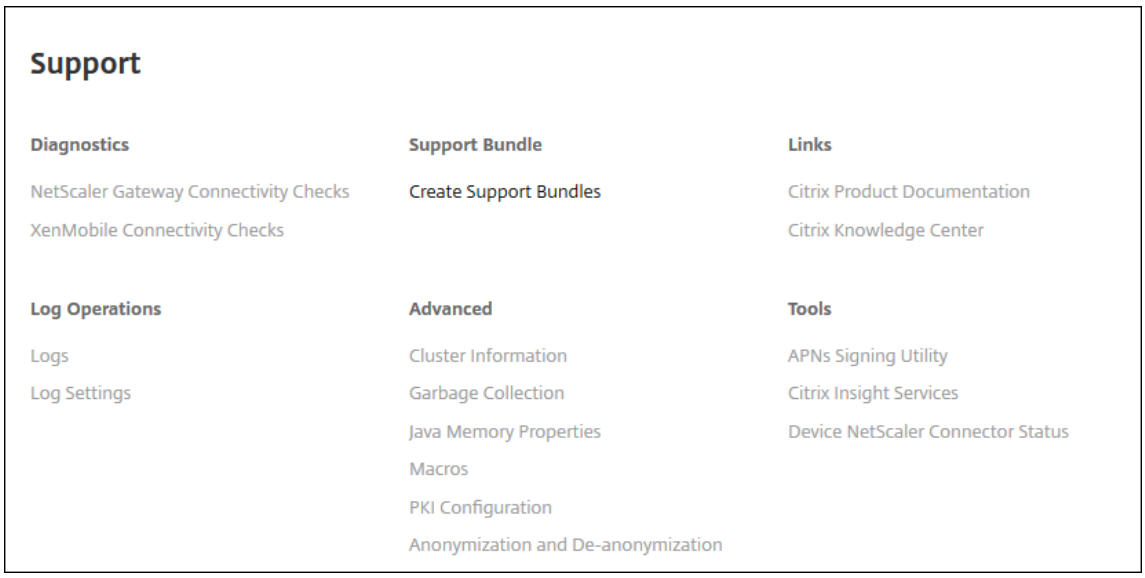


> **Remarque :**
>
> La boîte de dialogue d'ouverture de session est identique à la boîte de dialogue d'ouverture de session de la première VM. Cette correspondance vous permet de vérifier que les deux VM utilisent le même serveur de base de données.

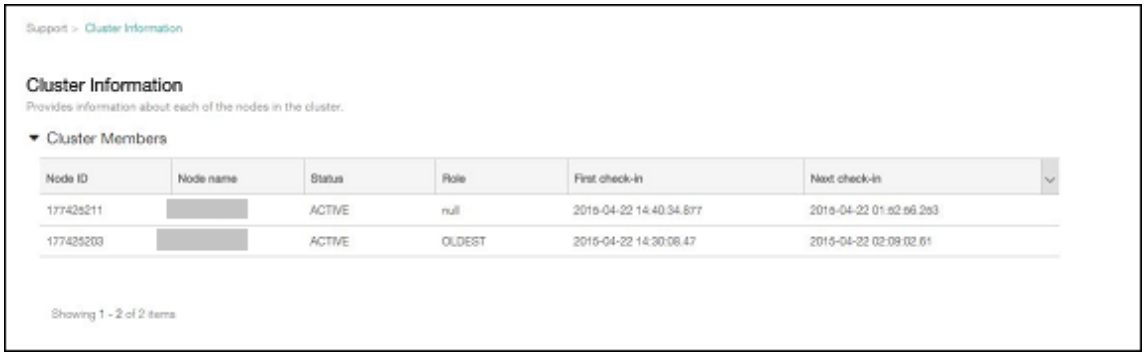
8. Utilisez le nom de domaine complet de XenMobile pour ouvrir la console XenMobile dans un navigateur Web.
9. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit.

La page **Support** s'ouvre.

10. Sous **Avancé**, cliquez sur **Informations de cluster**.



Toutes les informations sur le cluster, y compris les membres du cluster, les informations de connexion, les tâches, etc., s'affichent. Le nouveau nœud est maintenant membre du cluster.

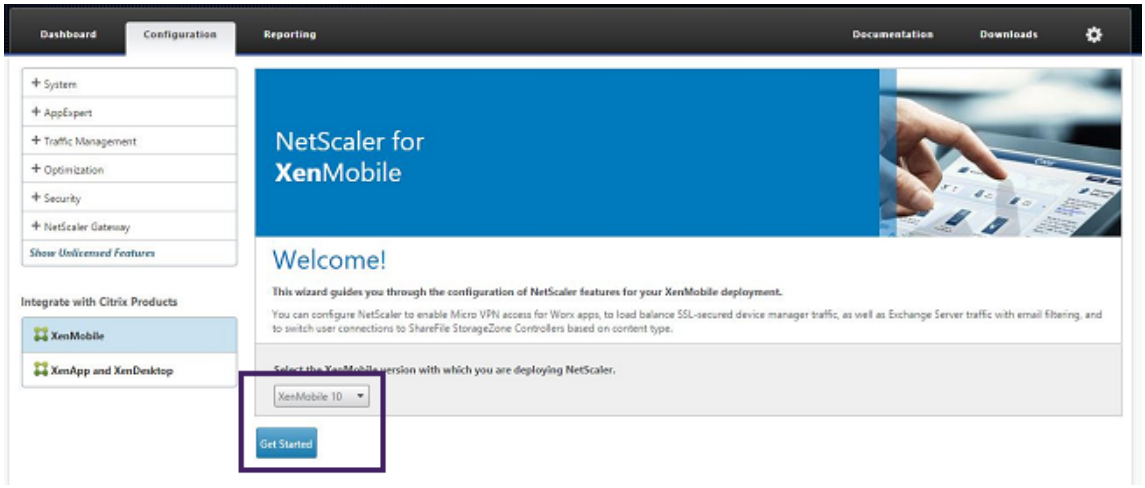


Vous pouvez ajouter d'autres nœuds en suivant les étapes suivantes. Le premier nœud ajouté au cluster détient un rôle **Plus ancien**. Les nœuds ajoutés après afficheront un rôle **Aucun** ou **null**.

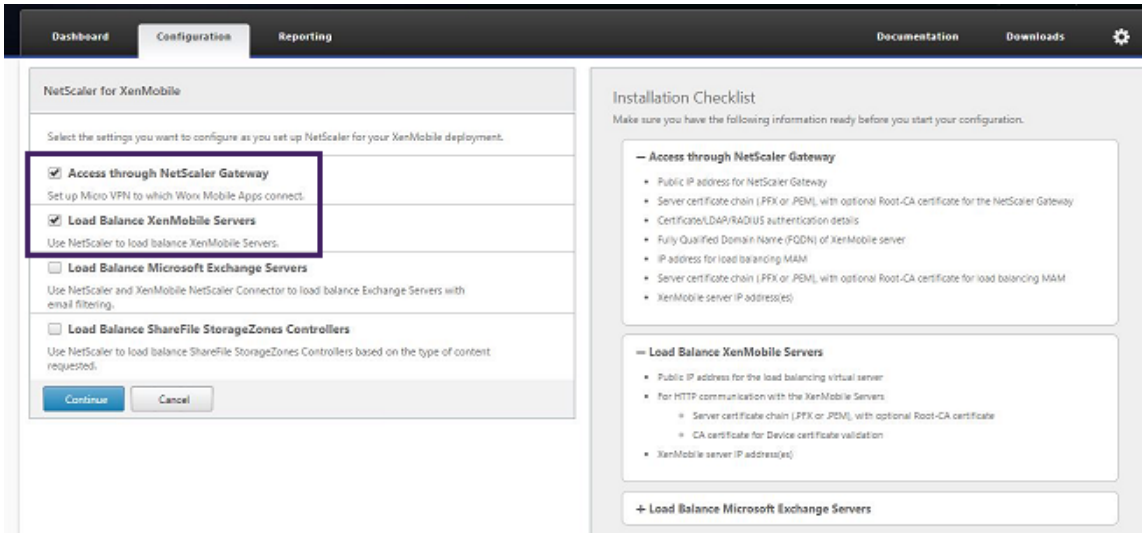
Pour configurer l'équilibrage de charge pour le cluster XenMobile dans Citrix ADC

Après avoir ajouté des nœuds en tant que membres du cluster XenMobile, équilibrez la charge des nœuds pour être en mesure d'accéder aux clusters. L'équilibrage de charge est réalisé en exécutant l'assistant XenMobile disponible dans Citrix ADC. Les étapes suivantes décrivent comment effectuer l'équilibrage de charge de XenMobile en exécutant l'assistant.

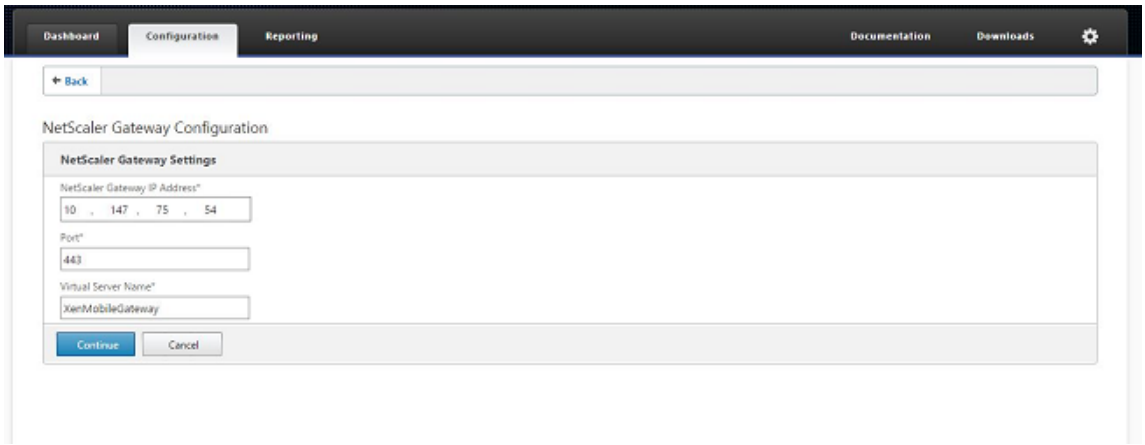
1. Connectez-vous à Citrix ADC.
2. Sur l'onglet Configuration, cliquez sur **XenMobile**, puis sur **Get Started**.



3. Cochez les cases **Access through Citrix Gateway** et **Load Balance XenMobile Servers**, puis cliquez sur **Continue**.



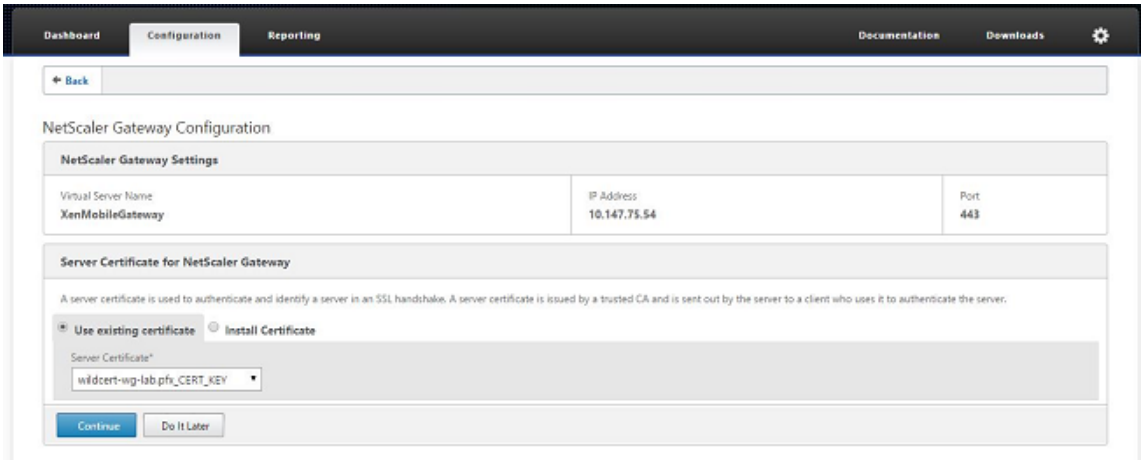
4. Entrez l'adresse IP de Citrix Gateway et cliquez sur **Continue**.



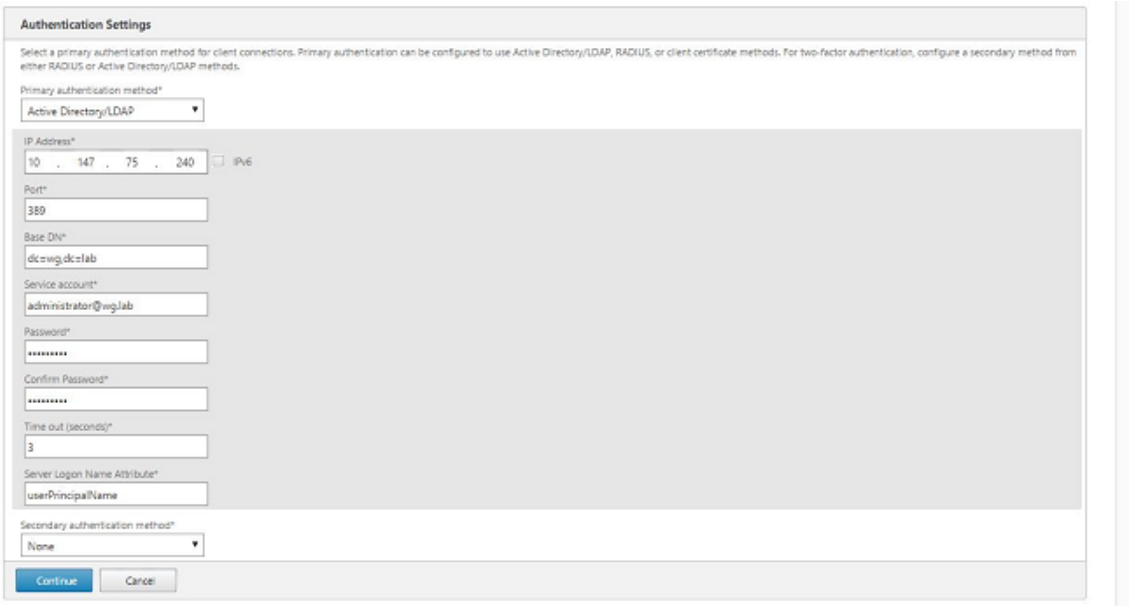
5. Liez le certificat de serveur à l'adresse IP virtuelle Citrix Gateway en effectuant l'une des opéra-

tions suivantes, puis cliquez sur **Continue**.

- Dans **Use existing certificate**, choisissez le certificat de serveur dans la liste.
- Cliquez sur l'onglet **Install Certificate** pour télécharger un nouveau certificat de serveur.

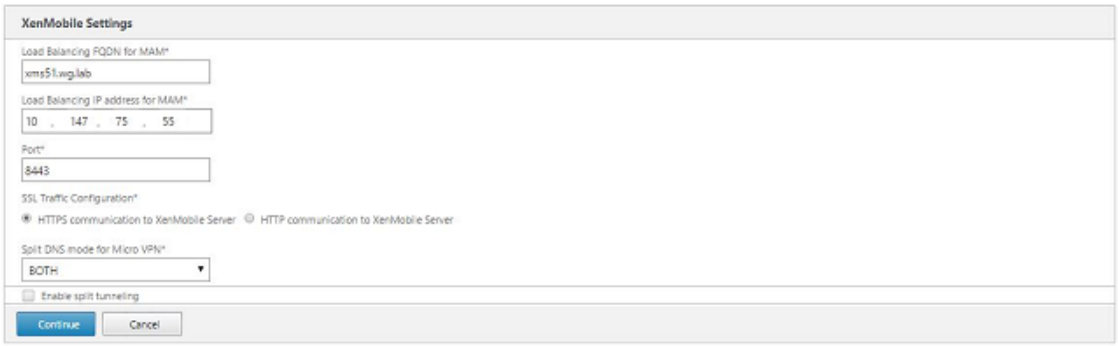


6. Entrez les détails du serveur d'authentification, puis cliquez sur **Continue**.



> **Remarque :**
>
> Assurez-vous que l'attribut Server Logon Name Attribute correspond à celui que vous avez fourni dans la configuration LDAP de XenMobile.

7. Sous XenMobile settings, entrez une valeur pour Load Balancing FQDN for MAM, puis cliquez sur **Continue**.

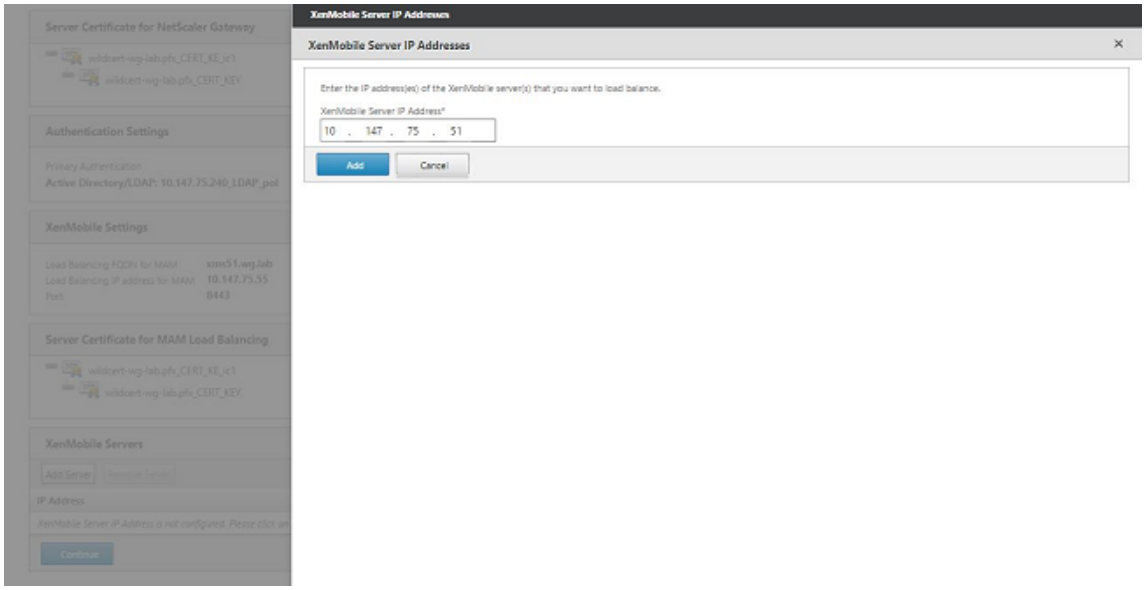


> **Remarque :**
>
> Assurez-vous que le nom de domaine complet de l'adresse IP virtuelle d'équilibrage de charge MAM et le nom de domaine complet de XenMobile sont les mêmes.

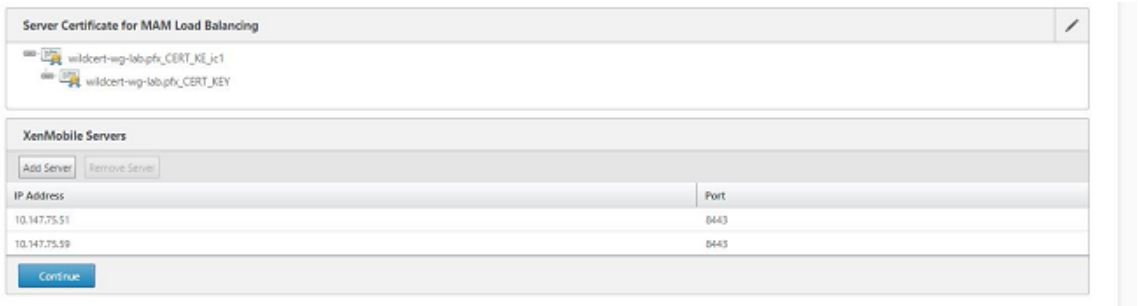
8. Si vous souhaitez utiliser le mode pont SSL (HTTPS), sélectionnez **HTTPS communication to XenMobile Server**. Toutefois, si vous souhaitez utiliser le déchargement SSL, sélectionnez **HTTP communication to XenMobile Server**, comme indiqué dans la figure précédente. Pour les besoins de cet article, l'option choisie est le mode pont SSL (HTTPS).
9. Liez le certificat de serveur pour l'adresse IP virtuelle d'équilibrage de charge MAM, puis cliquez sur Continue.

10. Sous XenMobile Servers, cliquez sur **Add Server** pour ajouter les nœuds XenMobile.

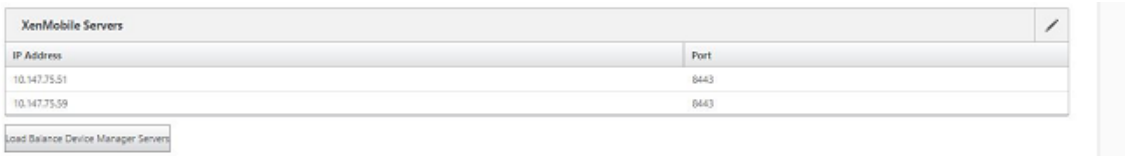
11. Entrez l'adresse IP du nœud XenMobile, puis cliquez sur Add.



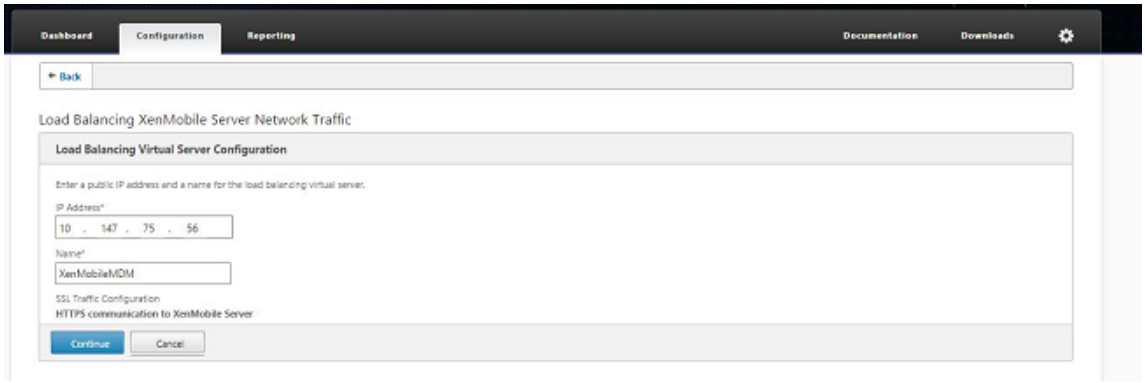
12. Répétez les étapes 10 et 11 pour ajouter d'autres nœuds XenMobile qui font partie du cluster XenMobile. Vous pouvez afficher tous les nœuds XenMobile que vous avez ajoutés. Cliquez sur Continuer.



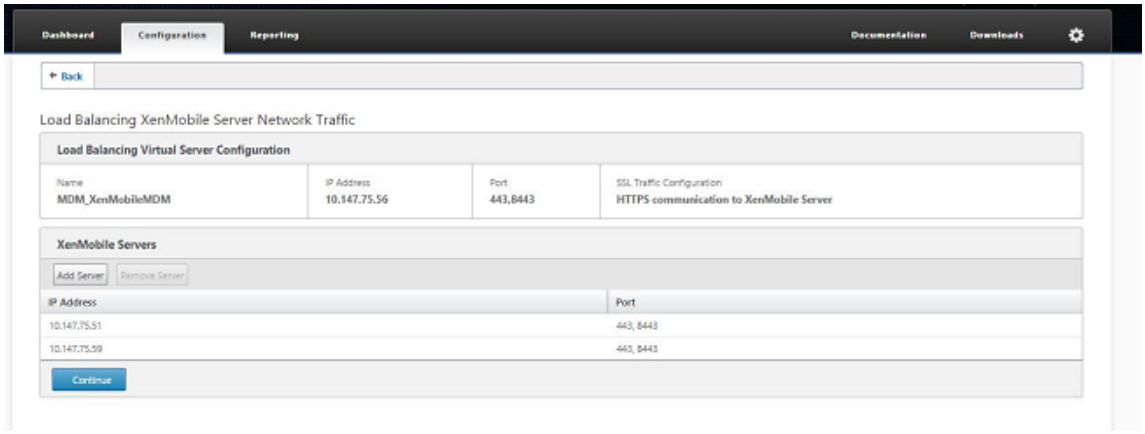
13. Cliquez sur **Load Balance Device Manager Servers** pour poursuivre la configuration d'équilibrage de charge MDM.



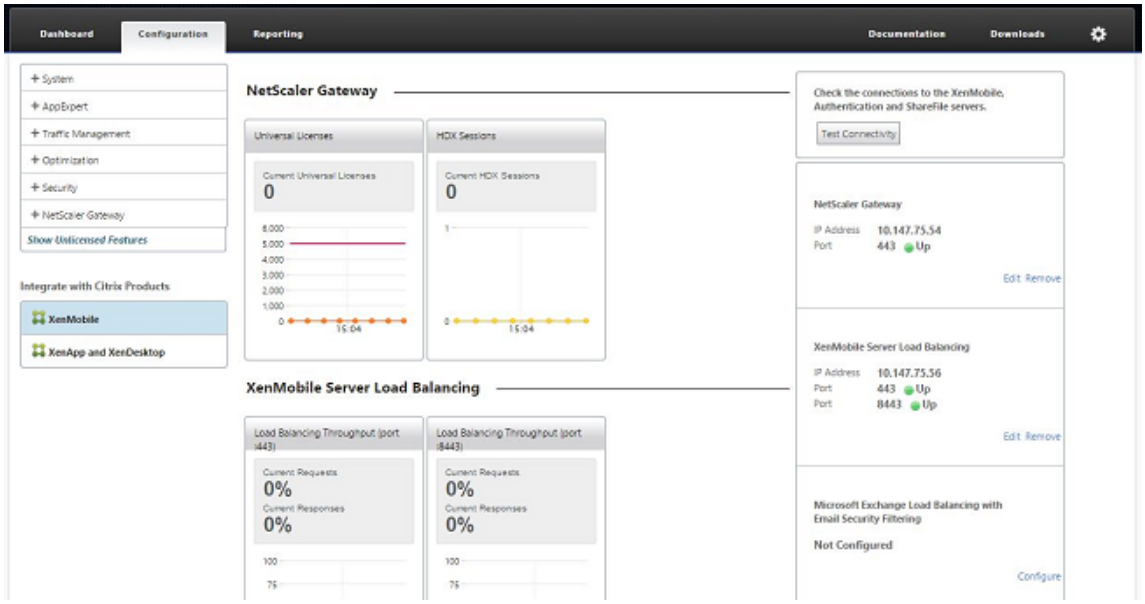
14. Entrez l'adresse IP à utiliser pour l'adresse IP d'équilibrage de charge MDM, puis cliquez sur **Continue**.



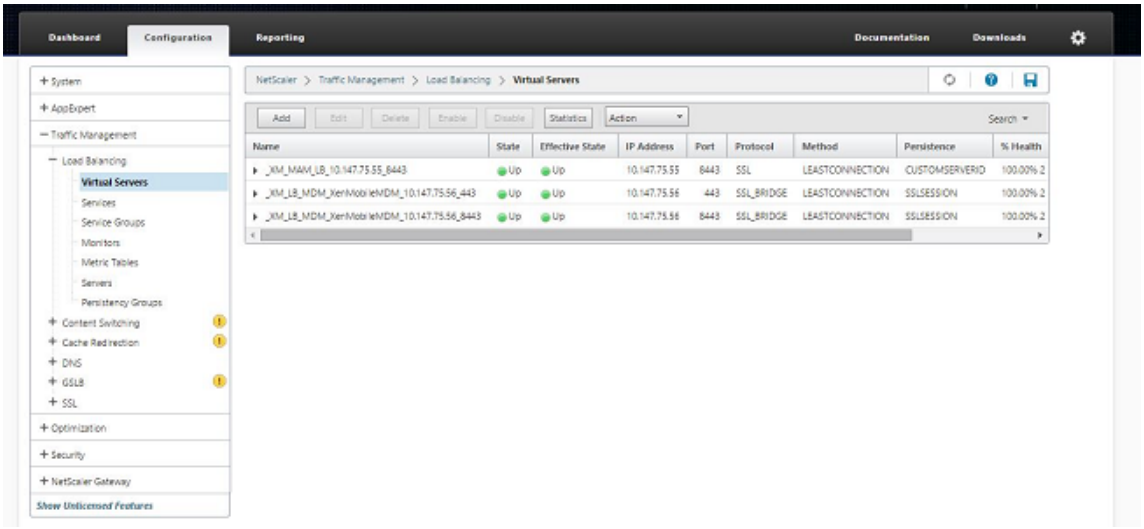
15. Lorsque les nœuds XenMobile sont affichés dans la liste, cliquez sur **Continue**, puis cliquez sur Done pour terminer le processus.



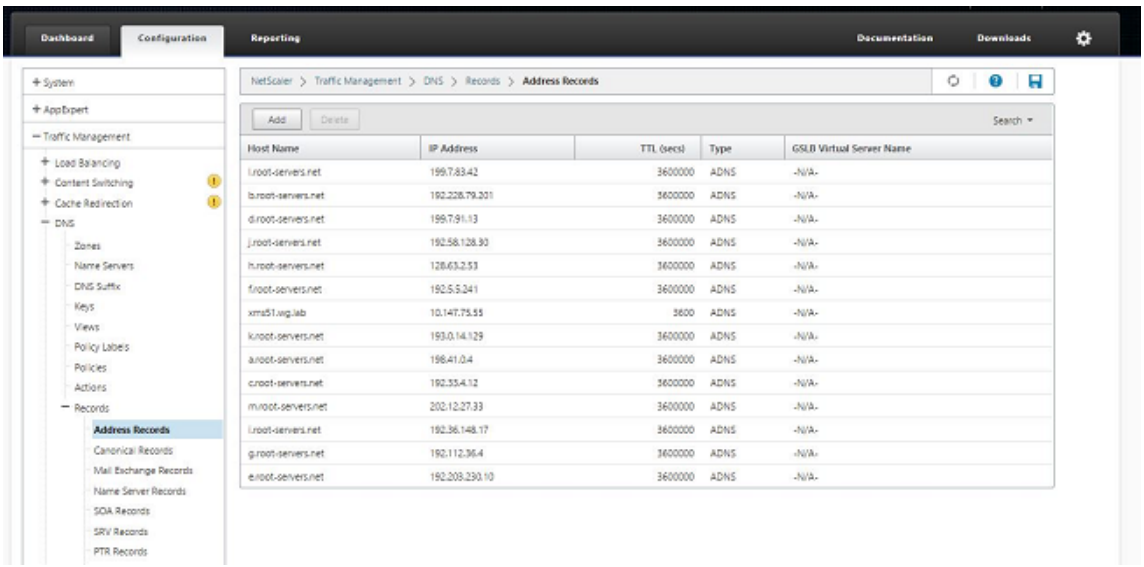
Vous verrez l'état de l'adresse IP virtuelle sur la page XenMobile.



16. Pour vérifier que les adresses IP virtuelles sont opérationnelles, cliquez sur l'onglet Configuration, puis accédez à **Traffic Management > Load Balancing > Virtual Servers**.



Vous verrez également que l'entrée DNS dans Citrix ADC pointe vers l'adresse IP virtuelle d'équilibrage de charge MAM.



Guide de récupération d'urgence

January 10, 2022

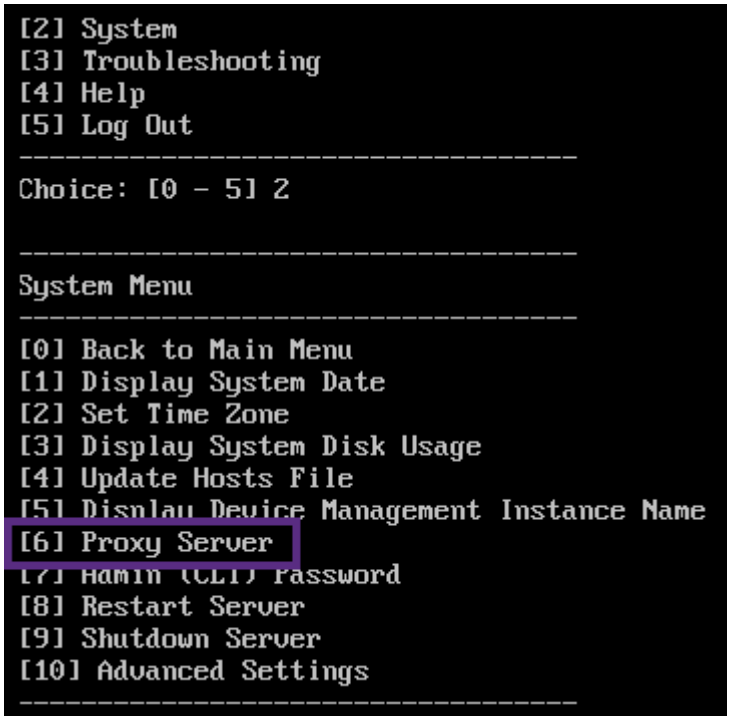
Vous pouvez concevoir et configurer des déploiements XenMobile comprenant plusieurs sites pour la récupération d'urgence à l'aide d'une stratégie de basculement active-passive. Pour plus d'informations, consultez l'article Récupération d'urgence du manuel de déploiement XenMobile.

Activer les serveurs proxy

January 10, 2022

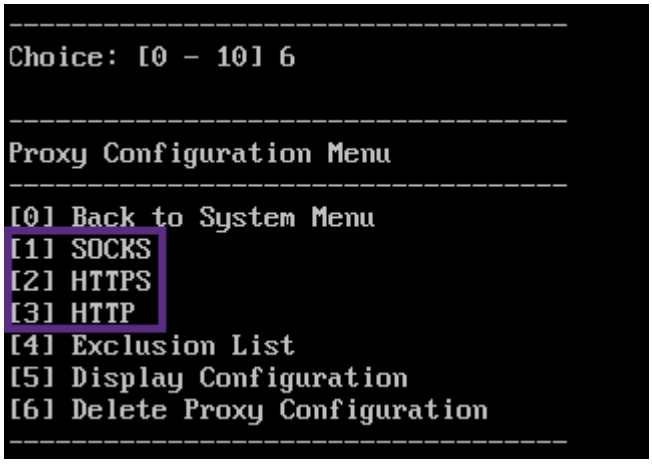
Pour contrôler le trafic Internet sortant, vous pouvez configurer un serveur proxy dans XenMobile pour acheminer ce trafic. Vous configurez le serveur proxy par le biais de l'interface de ligne de commande (CLI). La configuration du serveur proxy requiert le redémarrage de votre système.

1. Dans le menu principal de la ligne de commande XenMobile, tapez **2** pour sélectionner le menu système.
2. Dans le menu système, tapez **6** pour sélectionner le menu Serveur proxy.



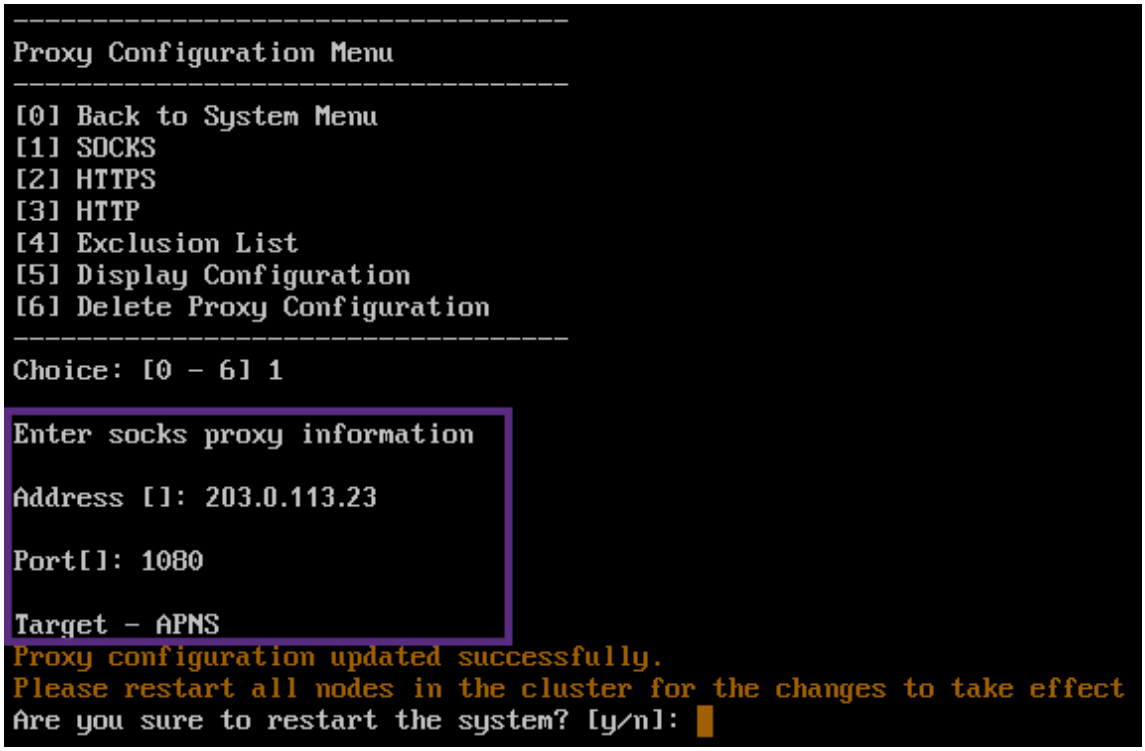
3. Dans le menu Configuration du proxy, tapez **1** pour sélectionnez SOCKS.

   Avant d'enregistrer cette configuration, vous devez également configurer HTTPS. Le proxy ne fonctionne que si vous enregistrez les paramètres SOCKS et HTTPS dans la même configuration.

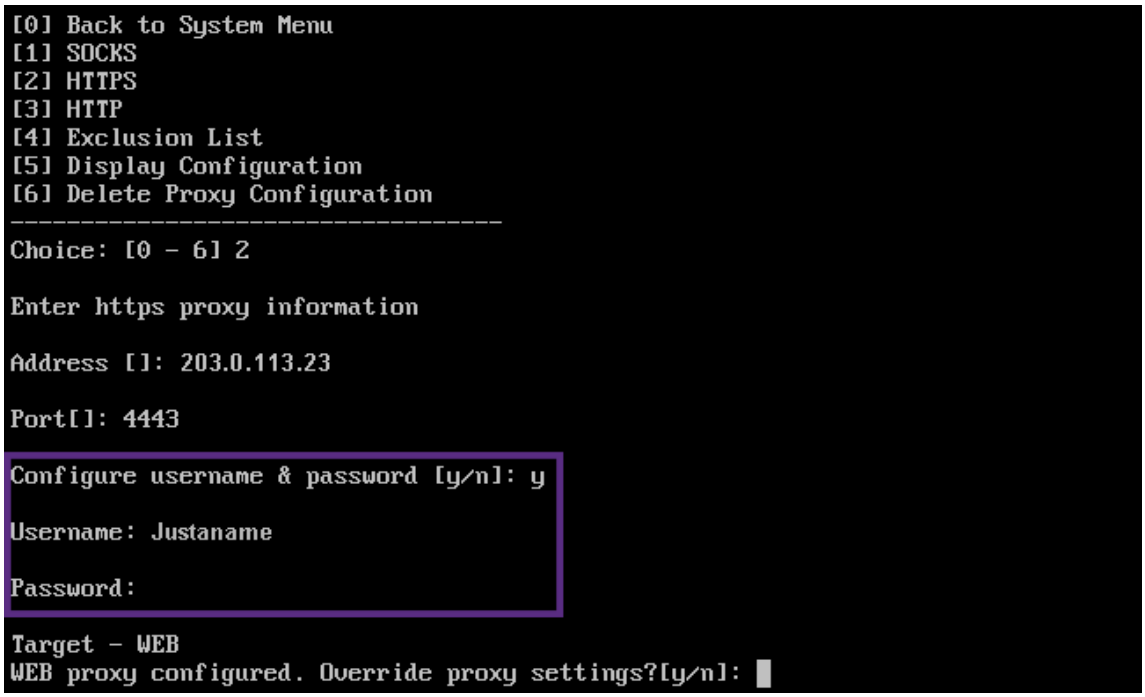


4. Entrez l'adresse IP de votre serveur proxy, le numéro de port et une cible. Reportez-vous au tableau suivant pour consulter la liste des types de cibles prises en charge pour chaque type de serveur proxy.

Type de proxy	Cibles prises en charge
SOCKS	APNS
HTTP	APNS, Web, PKI
HTTPS	Web, PKI
HTTP avec authentification	Web, PKI
HTTPS avec authentification	Web, PKI



5. Tapez **n**, tapez **2** pour sélectionner HTTPS, puis saisissez l'adresse IP de votre serveur proxy, le numéro de port et une cible.
6. Si vous choisissez de configurer un nom d'utilisateur et un mot de passe pour l'authentification sur votre serveur proxy, tapez **y**, puis entrez le nom d'utilisateur et le mot de passe.



7. Tapez **y** pour enregistrer la configuration.

Configurer SQL Server

January 10, 2022

Pour les connexions à SQL Server à partir d'une instance locale de XenMobile Server, vous pouvez utiliser l'un des pilotes suivants :

- Pilote par défaut
- JTD
- Pilote JDBC (Microsoft Java Database Connectivity)

Le pilote jTDS est le pilote par défaut dans les cas suivants :

- Vous installez XenMobile Server sur site.
- Vous mettez à niveau à partir de XenMobile Server configuré pour utiliser le pilote jTDS.

Pour les deux pilotes, XenMobile prend en charge l'authentification SQL Server ou l'authentification Windows. Pour les combinaisons d'authentification et de pilote, SSL peut être activé ou désactivé.

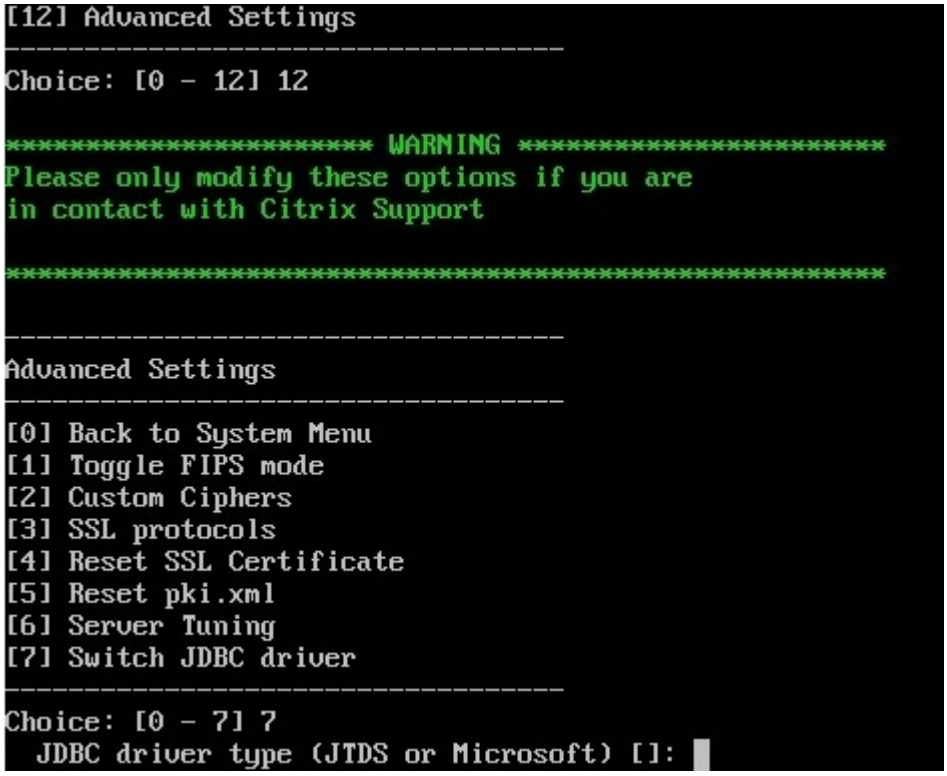
Lorsque vous utilisez l'authentification Windows avec le pilote JDBC de Microsoft, le pilote utilise l'authentification intégrée avec Kerberos. XenMobile contacte Kerberos pour obtenir les détails du Centre de distribution de clés Kerberos (KDC). Si les informations requises ne sont pas disponibles, la CLI XenMobile vous invite à entrer l'adresse IP du serveur Active Directory.

Pour passer du pilote jTDS au pilote JDBC, envoyez une commande SSH à tous vos nœuds XenMobile Server et utilisez la CLI XenMobile pour la configuration. Les étapes varient en fonction de la configuration actuelle du pilote jTDS, comme suit.

Basculer vers Microsoft JDBC (Authentification SQL Server)

Pour effectuer ces étapes, vous avez besoin du nom d'utilisateur et du mot de passe SQL Server.

1. Envoyez une commande SSH à tous les nœuds XenMobile Server.
2. Dans le menu principal de la ligne de commande XenMobile, tapez **2** pour sélectionner le **menu système**.
3. Entrez **12** pour sélectionner Paramètres avancés.
4. Entrez **7** pour sélectionner le basculement de pilote JDBC, puis entrez **m** pour Microsoft.



5. Lorsque vous y êtes invité, entrez **y** pour sélectionner l'authentification SQL, puis entrez le nom d'utilisateur et le mot de passe SQL Server.
6. Répétez les étapes pour chaque nœud XenMobile Server.
7. Redémarrez chaque nœud XenMobile Server.

Basculer vers Microsoft JDBC (SSL est désactivé ; authentification Windows)

Pour effectuer ces étapes, vous avez besoin du nom d'utilisateur et du mot de passe Active Directory, du domaine Kerberos KDC et du nom d'utilisateur KDC.

1. Envoyez une commande SSH à tous les nœuds XenMobile Server.
2. Dans le menu principal de la ligne de commande XenMobile, tapez **2** pour sélectionner le **menu système**.
3. Entrez **12** pour sélectionner Paramètres avancés.
4. Entrez **7** pour sélectionner le basculement de pilote JDBC, puis entrez **m**.
5. Lorsque vous êtes invité à utiliser l'authentification SQL Server, tapez **n**.
6. Lorsque vous y êtes invité, entrez le nom d'utilisateur et le mot de passe Active Directory configurés pour SQL Server.
7. Si XenMobile ne détecte pas automatiquement le domaine Kerberos KDC, vous êtes invité à entrer les détails du KDC, y compris le nom de domaine complet de SQL Server.

8. Lorsque vous êtes invité à utiliser SSL, tapez **n**. XenMobile enregistre la configuration. Si XenMobile ne peut pas enregistrer la configuration à cause d'erreurs, un message d'erreur et les détails que vous avez entrés s'affichent.
9. Répétez les étapes pour chaque nœud XenMobile Server.
10. Redémarrez chaque nœud XenMobile Server.

Pour modifier le mot de passe de la base de données XenMobile

Suivez ces instructions pour modifier le mot de passe de la base de données XenMobile, par exemple lorsque le support technique de Citrix vous demande de le modifier.

Si SQL Server utilise l'authentification Windows, modifiez le mot de passe de la base de données dans Windows Active Directory. Puis actualisez le compte administrateur de base de données sur le serveur de base de données pour synchroniser la modification du mot de passe. Vous pouvez ensuite modifier le mot de passe dans XenMobile, comme suit.

> **Important :**
>
> - Planifiez une fenêtre de maintenance pour modifier le mot de passe de la base de données dans XenMobile. Une modification de mot de passe doit avoir lieu pendant le temps d'arrêt du système.
> - Lorsque vous modifiez le mot de passe, assurez-vous que tous les nœuds XenMobile sont connectés au réseau. Après avoir modifié le mot de passe, redémarrez XenMobile.
>
>   If you don't restart XenMobile after a password change, XenMobile goes into recovery mode. In that case, revert to the old password in SQL server, restart XenMobile, and change the password again.

1. Vérifiez que tous les nœuds de XenMobile Server sont en cours d'exécution. Pour un environnement en cluster, affichez tous les nœuds.
2. Bloquez le trafic des appareils entrant vers XenMobile via l'équilibreur de charge Citrix ADC en désactivant les serveurs virtuels.
3. Pour modifier le mot de passe de la base de données sur SQL Server : ouvrez une session dans la CLI XenMobile, accédez à **Configuration > Base de données** et entrez le mot de passe modifié lorsque vous y êtes invité :

```
Server []: <ipAddress>
Port [1433]: 1433
Username [sa]: <userName>
Password: <****>
<!--NeedCopy-->
```


4. Sélectionnez **Y** pour redémarrer le serveur.
5. Répétez les étapes 3 et 4 pour tous les autres nœuds du cluster.
6. Débloquez le trafic des appareils entrant en activant les serveurs virtuels sur l'équilibreur de charge Citrix ADC.

Propriétés du serveur

January 10, 2022

XenMobile dispose de nombreuses propriétés qui s'appliquent aux opérations du serveur. Cet article décrit un grand nombre des propriétés de serveur et décrit en détail comment ajouter, modifier ou supprimer des propriétés de serveur.

Certaines propriétés sont des clés personnalisées. Pour ajouter une clé personnalisée, cliquez sur **Ajouter** puis, dans **Clé**, choisissez **Clé personnalisée**.

Pour de plus amples informations sur les propriétés généralement configurées, consultez la section Propriétés du serveur dans le manuel virtuel XenMobile.

Définitions des propriétés du serveur

Add Device Always

- Si ce paramètre est défini sur **true**, XenMobile ajoute un appareil à la console XenMobile, même si son inscription échoue, afin que vous puissiez voir les appareils qui ont tenté de s'inscrire. La valeur par défaut est **false**.

AG Client Cert Issuing Throttling Interval

- Période de grâce entre la génération de certificats. Cet intervalle empêche XenMobile de générer de multiples certificats pour un appareil pendant une courte période de temps. Citrix vous recommande de ne pas modifier cette valeur. La valeur par défaut est de **30** minutes.

Heure d'exécution du nettoyage du journal d'audit

- Heure de début du nettoyage du journal d'audit, au format HH:MM AM/PM. Exemple : 04:00 AM. La valeur par défaut est **02:00 AM**.

Intervalle de nettoyage du journal d'audit (en jours)

- Nombre de jours pendant lequel XenMobile conserve le journal d'audit. La valeur par défaut est **1**.

Enregistreur d'audit

- Si la valeur est **False**, les événements d'interface utilisateur ne sont pas journalisés. La valeur par défaut est **False**.

Rétention du journal d'audit (en jours)

- Nombre de jours pendant lequel XenMobile conserve le journal d'audit. La valeur par défaut est **7**.

auth.ldap.connect.timeout and auth.ldap.read.timeout

- Pour compenser les réponses LDAP lentes, Citrix recommande d'ajouter des propriétés de serveur pour les clés personnalisées suivantes.
  - Clé : **Clé personnalisée**
  - Clé : **auth.ldap.connect.timeout**
  - Valeur : **60000**
  - Nom d'affichage : **auth.ldap.connect.timeout**
  - Description : **Délai d'expiration de la connexion LDAP**
  - Clé : **Clé personnalisée**
  - Clé : **auth.ldap.read.timeout**
  - Valeur : **60000**
  - Nom d'affichage : **auth.ldap.read.timeout**
  - Description : **Délai d'expiration de la lecture LDAP**

Certificate Renewal in Seconds

- Nombre de secondes avant qu'un certificat expire après lequel XenMobile commence à renouveler les certificats. Par exemple, si un certificat expire le 30 décembre et que cette propriété est définie sur 30 jours : si l'appareil se connecte entre le 1er décembre et le 30 décembre, XenMobile tente de renouveler le certificat. La valeur par défaut est **2592000** secondes (30 jours).

Connection Timeout

- Délai d'inactivité de session, en minutes, après lequel XenMobile ferme la connexion TCP à un appareil. La session est toujours ouverte. S'applique aux appareils Android et Windows CE et à l'assistance à distance. La valeur par défaut est **5** minutes.

Délai d'expiration de la connexion au serveur de certification Microsoft

- Nombre de secondes pendant lequel XenMobile attend une réponse du serveur de certificats. Si le serveur de certificats est lent et que le trafic est élevé, vous pouvez augmenter ce nombre à 60 secondes ou plus. Un serveur de certificats qui ne répond pas après 120 secondes doit être contrôlé. La valeur par défaut est **15000** millisecondes (15 secondes).

Default deployment channel

- Détermine la manière dont XenMobile déploie une ressource à une machine : au niveau de l'utilisateur (**DEFAULT_TO_USER**) ou au niveau de l'appareil. La valeur par défaut est **DEFAULT_TO_DEVICE**.

Nettoyage du journal de déploiement (en jours)

- Nombre de jours pendant lequel le serveur XenMobile doit conserver le journal de déploiement. La valeur par défaut est **7**.

Désactiver la vérification du nom d'hôte

- Par défaut, la vérification de nom d'hôte est activée sur les connexions sortantes à l'exception du serveur PKI de Microsoft. Lorsque la vérification du nom d'hôte échoue, le journal du serveur contient des erreurs telles que : « Impossible de se connecter au serveur d'achat en volume : le nom d'hôte '192.0.2.0' ne correspond pas à l'objet du certificat fourni par l'homologue ». Si la vérification du nom d'hôte interrompt votre déploiement, définissez cette propriété sur **true**. La valeur par défaut est **false**.

Désactiver la vérification de serveur SSL

- Si **True**, elle désactive la validation du certificat de serveur SSL lorsque toutes les conditions suivantes sont remplies :
  - Vous avez activé l'authentification par certificats sur XenMobile Server.
  - Le serveur Microsoft CA est l'émetteur du certificat.
  - Une autorité de certification interne, dont la racine n'est pas approuvée par XenMobile Server, a signé votre certificat.

La valeur par défaut est **True**.

Enable Console

- Si la valeur est **true**, les utilisateurs peuvent accéder au portail en libre-service. La valeur par défaut est **true**.

Enable Crash Reporting

- Si le paramètre est réglé sur **true**, Citrix collecte les rapports d'incident et les diagnostics pour aider à résoudre les problèmes avec Secure Hub pour iOS et Android. Si ce paramètre est défini sur **false**, aucune donnée n'est collectée. La valeur par défaut est **true**.

Activer/désactiver la journalisation des statistiques de mise en veille prolongée pour le diagnostic

- Si la valeur est **True**, permet la journalisation des statistiques de veille prolongée pour faciliter la résolution des problèmes de performances des applications. Veille prolongée est un composant utilisé pour les connexions de XenMobile avec Microsoft SQL Server. Par défaut, la journalisation est désactivée car elle affecte la performance des applications. N'activez la journalisation que pour une courte durée pour éviter la création d'un énorme fichier journal. XenMobile enregistre les journaux sur /opt/sas/logs/hibernate_stats.log. La valeur par défaut est **False**.

Enable macOS OTAE

- Si le paramètre est réglé sur **false**, empêche l'utilisation d'un lien d'inscription pour les appareils macOS, ce qui signifie que les utilisateurs de macOS peuvent s'inscrire uniquement à l'aide d'une invitation d'inscription. La valeur par défaut est **true**.

Enable Notification Trigger

- Active ou désactive les notifications du client Secure Hub. La valeur **true** active les notifications. La valeur par défaut est **true**.

force.server.push.required.apps

- Permet le déploiement forcé des applications requises sur les appareils Android et iOS dans des situations telles que les suivantes :
  - Vous chargez une nouvelle application et la marquez comme requise.
  - Vous marquez une application existante comme requise.

- Un utilisateur supprime une application requise.
- Une mise à jour de Secure Hub est disponible.

Le déploiement forcé des applications requises est réglé sur **false** par défaut. Créez la clé personnalisée et définissez **Valeur** sur **true** pour activer le déploiement forcé. Au cours du déploiement forcé, les applications MDX requises, y compris les applications d'entreprise et les applications de magasin d'applications publiques, sont immédiatement mises à niveau. La mise à niveau se produit même si vous configurez une stratégie MDX pour une période de grâce de mise à jour d'application et que l'utilisateur choisit de mettre à niveau l'application ultérieurement.

- Clé : **Clé personnalisée**
- Clé : **force.server.push.required.apps**
- Valeur : **false**
- Nom d'affichage : **force.server.push.required.apps**
- Description : **Forcer le déploiement des applications requises**

Full Pull of ActiveSync Allowed and Denied Users

- L'intervalle (en secondes) pendant lequel XenMobile extrait une liste complète (référence) des utilisateurs autorisés et refusés par ActiveSync. Le délai par défaut est **28800** secondes.

hibernate.c3p0.idle_test_period

- Cette propriété XenMobile Server, une clé personnalisée, détermine le temps d'inactivité en secondes avant qu'une connexion soit automatiquement validée. Configurez la clé comme suit. La valeur par défaut est **30**.
- Clé : **Clé personnalisée**
- Clé : **hibernate.c3p0. idle_test_period**
- Valeur : **30**
- Nom d'affichage : **hibernate.c3p0. idle_test_period =*nnn***
- Description : **Période d'inactivité prolongée de test**

hibernate.c3p0.max_size

- Cette clé personnalisée détermine le nombre maximal de connexions que XenMobile peut ouvrir pour la base de données SQL Server. XenMobile utilise la valeur que vous spécifiez pour cette clé personnalisée en tant qu'une limite supérieure. Les connexions s'ouvrent uniquement si vous en avez besoin. Basez vos paramètres sur la capacité de votre serveur de base de données. Pour plus d'informations, consultez la section Optimisation des opérations XenMobile. Configurez la clé comme suit. La valeur par défaut est **1000**.

- Clé : **hibernate.c3p0.max_size**
- Valeur : **1000**
- Nom d'affichage : **hibernate.c3p0.max_size**
- Description : **Connexions de base de données à SQL**

hibernate.c3p0.min_size

- Cette clé personnalisée détermine le nombre minimal de connexions que XenMobile ouvre pour la base de données SQL Server. Configurez la clé comme suit. La valeur par défaut est **100**.
- Clé : **hibernate.c3p0.min_size**
- Valeur : **100**
- Nom d'affichage : **hibernate.c3p0.min_size**
- Description : **Connexions de base de données à SQL**

hibernate.c3p0.timeout

- Cette clé personnalisée détermine le délai d'inactivité en secondes. La valeur par défaut est **120**.
- Clé : **Clé personnalisée**
- Clé : **hibernate.c3p0.timeout**
- Valeur : **120**
- Nom d'affichage : **hibernate.c3p0.timeout**
- Description: **Délai d'inactivité de la base de données**

Identifie si la télémétrie est activée ou non

- Identifie si la télémétrie (Programme d'amélioration de l'expérience utilisateur, ou CEIP) est activée. Vous pouvez choisir de participer au programme CEIP lorsque vous installez ou mettez à niveau XenMobile. La télémétrie est désactivée après 15 tentatives de chargement infructueuses consécutives. La valeur par défaut est **false**.

Délai d'inactivité en minutes

- Si la propriété de serveur **WebServices timeout type** est **INACTIVITY_TIMEOUT** : cette propriété définit le nombre de minutes après lequel XenMobile ferme la session d'un administrateur inactif qui a fait ce qui suit :

- Utilisé l'API publique XenMobile pour les services REST pour accéder à la console XenMobile
- Utilisé l'API publique XenMobile pour les Services REST pour accéder à une application tierce. Un délai d'expiration de **0** signifie qu'un utilisateur inactif reste connecté.

La valeur par défaut est **5**.

iOS Device Management Enrollment Auto-Install Enabled

- Si la valeur est définie sur true, cette propriété réduit les interactions des utilisateurs lors de l'inscription d'appareils. Les utilisateurs doivent cliquer sur **Root CA install** (si nécessaire) et **MDM Profile install**.

iOS Device Management Enrollment First Step Delayed

- Après qu'un utilisateur entre ses informations d'identification lors de l'inscription d'un appareil, cette valeur spécifie la durée d'attente avant d'afficher une invite pour l'autorité de certification racine. Citrix vous recommande de modifier cette propriété uniquement si vous observez des problèmes de latence réseau ou de vitesse. Dans ce cas, ne définissez pas la valeur au-delà de 5 000 millisecondes (5 secondes). La valeur par défaut est **1000** millisecondes (1 seconde).

iOS Device Management Enrollment Last Step Delayed

- Lors de l'inscription d'un appareil, cette valeur de propriété spécifie la durée d'attente entre installation du profil MDM et le démarrage de l'agent sur l'appareil. Citrix vous recommande de modifier cette propriété uniquement si vous observez des problèmes de latence réseau ou de vitesse. Dans ce cas, ne définissez pas la valeur au-delà de 5 000 millisecondes (5 secondes). La valeur par défaut est **1000** millisecondes (1 seconde).

iOS Device Management Identity Delivery Mode

- Spécifie si XenMobile distribue le certificat MDM aux appareils utilisant **SCEP** (recommandé pour des raisons de sécurité) ou **PKCS12**. En mode PKCS12, la paire de clés est générée sur le serveur et aucune négociation n'est effectuée. La valeur par défaut est **SCEP**.

iOS Device Management Identity Key Size

- Définit la taille des clés privées pour les identités MDM, le service de profils iOS et les identités d'agent XenMobile. La valeur par défaut est **1024**.

iOS Device Management Identity Renewal Days

- Spécifie le nombre de jours avant qu'un certificat n'expire après lequel XenMobile commence à renouveler les certificats. Par exemple, si un certificat expire dans 10 jours et que cette propriété est **10** jours, lorsqu'un appareil se connecte 9 jours avant l'expiration, XenMobile émet un nouveau certificat. La valeur par défaut est **30** jours.

iOS MDM APNS Private Key Password

- Cette propriété contient le mot de passe APNS requis par XenMobile pour les notifications push aux serveurs Apple.

Length of Inactivity Before Device Is Disconnected

- Spécifie la durée pendant laquelle un appareil peut rester inactif, y compris la dernière authentification, avant que XenMobile le déconnecte. La valeur par défaut est **7** jours.

MAM Only Device Max

- Cette clé personnalisée limite le nombre d'appareils en mode MAM exclusif que chaque utilisateur peut inscrire. Configurez la clé comme suit. Une **valeur** de **0** permet un nombre illimité d'inscriptions d'appareils.
- Clé = **number.of.mam.devices.per.user**
- Valeur = **5**
- Nom d'affichage = **MAM Only Device Max**
- Description = **Limite le nombre d'appareils MAM que chaque utilisateur peut inscrire.**

MaxNumberOfWorker

- Nombre de threads utilisé lors de l'importation d'un grand nombre de licences d'achat en volume. La valeur par défaut est **3**. Si vous avez besoin d'une plus grande optimisation, vous pouvez augmenter le nombre de threads. Toutefois, avec un nombre important de threads (6, par exemple), une importation d'achat en volume entraîne une forte utilisation de l'UC.

Citrix ADC Single Sign-On

- Si la valeur est **False**, elle désactive la fonctionnalité de rappel de XenMobile durant le Single Sign-On depuis Citrix ADC vers XenMobile. Si la configuration de Citrix Gateway comprend une adresse URL de rappel, XenMobile utilise la fonctionnalité de rappel pour vérifier l'ID de session Citrix Gateway. La valeur par défaut est **False**.

Number of consecutive failed uploads

- Affiche le nombre d'échecs consécutifs durant les chargements du programme CEIP. XenMobile incrémente la valeur lorsqu'un chargement échoue. Après 15 échecs de chargement, XenMobile désactive le programme CEIP, également appelé télémétrie. Pour plus d'informations, consultez la section de la propriété de serveur **Identifies if telemetry is enabled or not**. XenMobile réinitialise la valeur sur **0** lorsqu'un chargement réussit.

Number of Users Per Device

- Nombre maximal d'utilisateurs qui peuvent inscrire le même appareil en mode MDM. La valeur **0** signifie qu'un nombre illimité d'utilisateurs peut inscrire le même appareil. La valeur par défaut est **0**.

Pull of Incremental Change of Allowed and Denied Users

- Nombre de secondes pendant lesquelles XenMobile attend une réponse du domaine lors de l'exécution d'une commande PowerShell pour obtenir un delta des appareils ActiveSync. Le délai par défaut est **60** secondes.

Read Timeout to Microsoft Certification Server

- Nombre de secondes pendant lesquelles XenMobile attend une réponse du serveur de certificats lors d'une opération de lecture. Si le serveur de certificats est lent et que le trafic est élevé, vous pouvez augmenter ce nombre à 60 secondes ou plus. Un serveur de certificats qui ne répond pas après 120 secondes doit être contrôlé. La valeur par défaut est **15000** millisecondes (15 secondes).

REST Web Services

- Permet d'activer le service Web REST. La valeur par défaut est **true**.

Récupère les informations sur les appareils par blocs de taille spécifiée

- Cette valeur est utilisée en interne pour le multi-threading lors de l'exportation de l'appareil. Si la valeur est plus élevée, un seul thread analyse davantage d'appareils. Si la valeur est moins élevée, plus de threads récupèrent les appareils. La réduction de la valeur peut augmenter les performances des exportations et les récupérations de liste d'appareils, mais peut réduire la mémoire disponible. La valeur par défaut est **1000**.

Nettoyage du journal de sessions (en jours)

- Nombre de jours pendant lequel XenMobile conserve le journal de session. La valeur par défaut est **7**.

Mode de serveur

- Détermine si XenMobile est exécuté en mode MAM, MDM ou ENT (Enterprise), qui correspond à la gestion des applications, la gestion des appareils ou la gestion des appareils et des applications. Définissez la propriété du mode de serveur en fonction de la façon dont vous voulez que les appareils s'inscrivent, comme indiqué dans le tableau ci-dessous. Le mode de serveur par défaut est **ENT**, quel que soit le type de licence.

Si vous disposez d'une licence XenMobile MDM Edition, le mode de serveur efficace est toujours MDM, quel que soit le mode de serveur que vous avez défini dans les propriétés du serveur. Si vous disposez d'une licence MDM Edition, vous ne pouvez pas activer la gestion des applications en définissant le mode du serveur sur MAM ou ENT.

Vos licences sont cette Édition	Vous voulez que les appareils s'inscrivent dans ce mode	Définissez la propriété du mode de serveur sur
Enterprise / Advanced	Mode MDM	MDM
Enterprise / Advanced	Mode MDM+MAM	ENT
MDM	Mode MDM	MDM

Le mode de serveur efficace est la combinaison du type de licence et du mode de serveur. Pour une licence MDM, le mode de serveur efficace est toujours MDM, quel que soit le paramètre de mode du serveur. Pour les licences Enterprise et Advanced, le mode de serveur efficace correspond au mode du serveur, si le mode de serveur est **ENT** ou **MDM**. Si le mode de serveur est **MAM**, le mode de serveur efficace est ENT.

XenMobile ajoute le mode de serveur au journal du serveur pour chacune de ces activités : une licence est activée, une licence est supprimée et vous modifiez le mode du serveur dans les propriétés du serveur. Pour plus d'informations sur la création et l'affichage des fichiers journaux, consultez les sections Journaux et Visualiser et analyser les fichiers journaux dans XenMobile.

Type de configuration Content Collaboration

- Spécifie le type de stockage Citrix Files. **ENTERPRISE** active le mode Citrix Files Enterprise. **CONNECTORS** permet d'accéder uniquement aux connecteurs StorageZone que vous créez via la console XenMobile. La valeur par défaut est **NONE**, qui affiche la vue initiale de l'écran **Configurer > ShareFile** dans lequel vous avez le choix entre Citrix Files Enterprise et Connecteurs. La valeur par défaut est **NONE**.

Static Timeout in Minutes

- Si la propriété de serveur **WebServices timeout type** est **STATIC_TIMEOUT :** cette propriété définit le nombre de minutes après lequel XenMobile ferme la session d'un administrateur qui a fait ce qui suit :
  - Utilisé l'API publique XenMobile pour les services REST pour accéder à la console XenMobile
  - Utilisé l'API publique XenMobile pour les services REST pour accéder une application tierce

Le délai par défaut est **60**.

Trigger Agent Message Suppression

- Active ou désactive la messagerie du client Secure Hub. La valeur **false** active la messagerie. La valeur par défaut est **true**.

Trigger Agent Sound Suppression

- Active ou désactive les sons du client Secure Hub. La valeur **false** active les sons. La valeur par défaut est **true**.

Téléchargement d'applications non authentifiées pour les appareils Android

- Si la valeur est **True**, vous pouvez télécharger des applications auto-hébergées sur des appareils Android exécutant Android Enterprise. XenMobile a besoin de cette propriété si l'option Android Enterprise permettant de fournir une adresse URL de téléchargement statique dans Google Play Store est activée. Dans ce cas, les adresses URL de téléchargement ne peuvent pas inclure de ticket à usage unique (défini par la propriété du serveur **Ticket à usage unique XAM**) qui possède le jeton d'authentification. La valeur par défaut est **False**.

Téléchargement d'applications non authentifiées pour les appareils Windows

- Utilisé uniquement pour les anciennes versions de Secure Hub qui ne valident pas les tickets à usage unique. Si la valeur est **False**, vous pouvez télécharger des applications non authentifiées

depuis XenMobile sur des appareils Windows. La valeur par défaut est **False**.

Utiliser l'ID ActiveSync pour réinitialiser un appareil ActiveSync

- Si la valeur est définie sur **true**, Endpoint Management Connector pour Exchange ActiveSync utilise l'identificateur ActiveSync en tant qu'argument pour la méthode asWipeDevice. La valeur par défaut est **false**.

Propriétés N d'appareil définies par l'utilisateur

- Utilisé pour les appareils Windows CE uniquement. Cette clé personnalisée vous permet d'obtenir les propriétés que vous créez dans le Registre des appareils Windows CE. Une fois que ces propriétés sont dans la base de données de XenMobile, vous pouvez créer des règles de déploiement basées sur la valeur des propriétés.
- Clé : **Clé personnalisée**
- Clé : **device.properties.userDefinedN**
- Valeur : *administrator-defined*
- Nom d'affichage : *administrator-defined*
- Description : *administrator-defined*

Users only from Exchange

- Si la valeur est **true**, désactive l'authentification utilisateur pour les utilisateurs ActiveSync Exchange. La valeur par défaut est **false**.

Intervalle de ligne de base VP

- Intervalle minimum après lequel XenMobile ré-importe les licences d'achat en volume depuis Apple. L'actualisation des informations de licence permet de s'assurer que XenMobile reflète toutes les modifications, par exemple en cas de suppression manuelle d'une application importée à partir de l'achat en volume. Par défaut, XenMobile actualise la ligne de base de licence d'achat en volume toutes les **720** minutes au minimum.

Si de nombreuses licences d'achat en volume sont installées (plus de 50 000, par exemple), Citrix vous recommande d'augmenter l'intervalle de ligne de base pour réduire la fréquence et la charge de l'importation de licences. Si vous prévoyez des modifications fréquentes de licence d'achat en volume depuis Apple, Citrix vous recommande de réduire la valeur pour que XenMobile reste à jour. L'intervalle minimal entre deux lignes de base est de 60 minutes. En outre, XenMobile effectue une

importation delta toutes les 60 minutes, pour capturer les modifications depuis la dernière importation. Par conséquent, si l'intervalle de ligne de base d'achat en volume est de 60 minutes, l'intervalle entre les lignes de base peut être retardé, jusqu'à 119 minutes.

Type de délai d'expiration des WebServices

- Indique comment faire expirer un jeton d'authentification récupéré depuis l'API publique. Si **STATIC_TIMEOUT** est sélectionné, XenMobile considère qu'un jeton d'authentification a expiré après expiration de la valeur spécifiée dans la propriété de serveur **Static Timeout in Minutes**.

Si **INACTIVITY_TIMEOUT** est sélectionné, XenMobile considère qu'un jeton d'authentification a expiré si ce dernier reste inactif pendant la valeur spécifiée dans la propriété de serveur **Inactivity Timeout in Minutes**. La valeur par défaut est **STATIC_TIMEOUT**.

Windows Phone MDM Certificate Extended Validity (5y)

- Période de validité du certificat émis par MDM pour Windows Phone et Tablet. Les appareils utilisent un certificat d'appareil pour s'authentifier auprès du serveur MDM lors de la gestion des appareils. Si la valeur est **true**, la période de validité est de cinq ans. Si la valeur est **false**, la période de validité est de deux ans. La valeur par défaut est **true**.

Windows WNS Channel - Number of Days Before Renewal

- Fréquence de renouvellement de ChannelURI. La valeur par défaut est **10** jours.

Windows WNS Heartbeat Interval

- Durée pendant laquelle XenMobile attend avant de se connecter à un appareil après s'y être connecté 5 fois toutes les 3 minutes. La valeur par défaut est **6** heures.

Ticket XAM à usage unique

- Nombre de millisecondes pendant lequel un jeton d'authentification à usage unique (OTT) est valide pour le téléchargement d'une application. Cette propriété fonctionne avec les propriétés **Téléchargement d'applications non authentifiées pour Android** et **Téléchargement d'applications non authentifiées pour Windows**. Ces propriétés indiquent si les téléchargements d'applications non authentifiées sont autorisés. La valeur par défaut est **3600000**.

Intervalle maximale d'inactivité (minutes) du portail en libre-service de XenMobile MDM

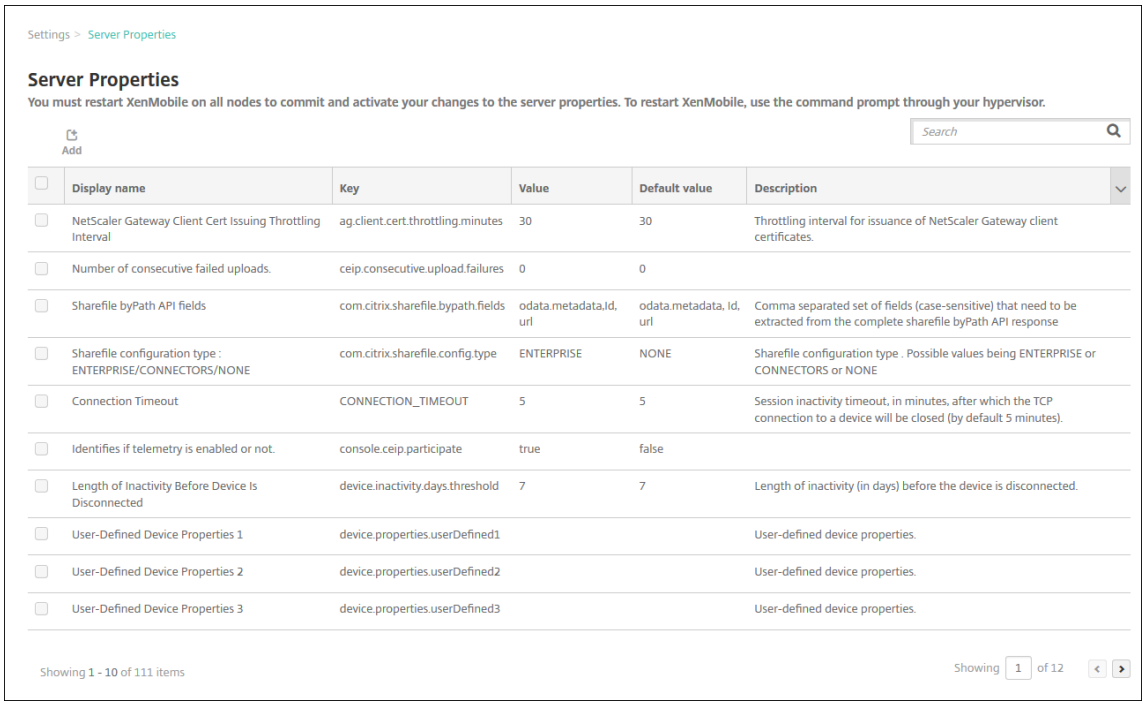
- Nombre de minutes après lesquelles XenMobile ferme la session d'un utilisateur inactif sur le portail en libre-service de XenMobile. Un délai d'expiration de **0** signifie qu'un utilisateur inactif reste connecté. La valeur par défaut est **30**.

Ajout, modification ou suppression de propriétés de serveur

Dans XenMobile, vous pouvez appliquer des propriétés au serveur. Après avoir effectué des modifications, vous devez redémarrer XenMobile sur tous les nœuds pour valider et activer les modifications.

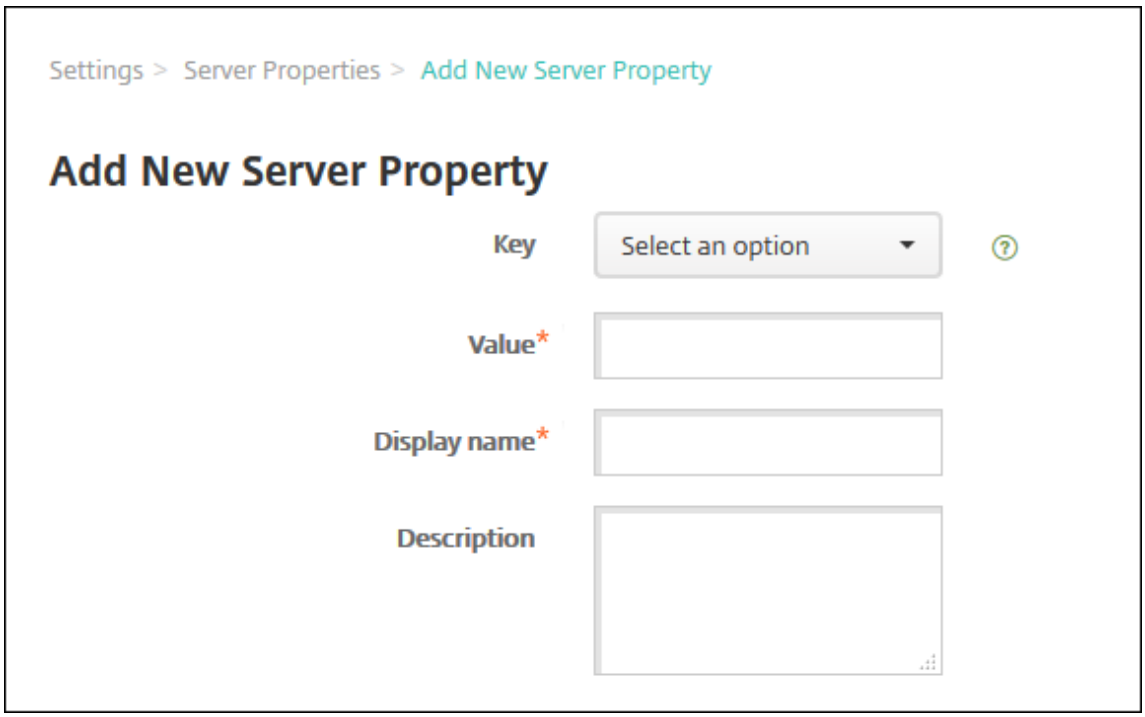
> **Remarque :**
>
> Pour redémarrer XenMobile, utilisez l'invite de commande par le biais de votre hyperviseur.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Serveur**, cliquez sur **Propriétés du serveur**. La page **Propriétés du serveur** s'affiche. Vous pouvez ajouter, modifier ou supprimer des propriétés de serveur à partir de cette page.



Pour ajouter une propriété de serveur

1. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle propriété de serveur** s'affiche.

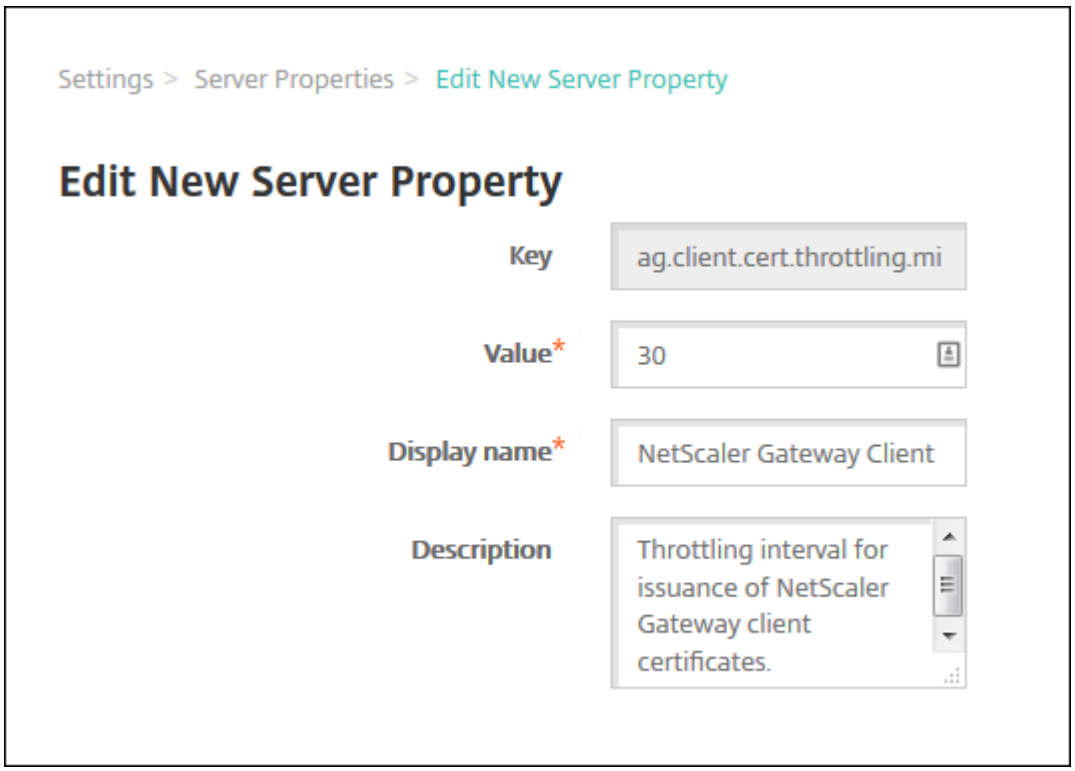


2. Pour configurer ces paramètres :
   - Clé : dans la liste, sélectionnez la clé appropriée. Les clés sont sensibles à la casse. Contactez le Support Citrix avant de modifier les valeurs de propriété ou pour demander une clé spéciale.
   - Valeur : entrez une valeur, en fonction de la clé que vous avez sélectionnée.
   - Nom d'affichage : entrez un nom pour la nouvelle valeur de propriété qui s'affiche dans le tableau **Propriétés du serveur**.
   - Description : entrez une description pour la nouvelle propriété de serveur (facultatif).
3. Cliquez sur **Enregistrer**.

Pour modifier une propriété de serveur

1. Dans le tableau **Propriétés du serveur**, sélectionnez la propriété de serveur que vous voulez modifier.

   Lorsque vous sélectionnez la case à cocher en regard d'une propriété de serveur, le menu d'options s'affiche au-dessus de la liste des propriétés de serveur. Cliquez dans la liste pour ouvrir le menu d'options sur le côté droit de la liste.
2. Cliquez sur **Modifier**. La page **Modifier une nouvelle propriété de serveur** s'affiche.



3. Modifiez les informations suivantes le cas échéant :
   - Clé : vous ne pouvez pas modifier ce champ.
   - Valeur : valeur de la propriété.
   - Nom d'affichage : nom de la propriété.
   - Description : description de la propriété.
4. Cliquez sur **Enregistrer** pour enregistrer vos modifications ou sur **Annuler** pour laisser la propriété inchangée.

Pour supprimer une propriété de serveur

1. Dans le tableau **Propriétés du serveur**, sélectionnez la propriété de serveur que vous voulez supprimer.

   Vous pouvez sélectionner plusieurs propriétés à supprimer en sélectionnant la case à cocher en regard de chaque propriété.
2. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer**.

Options d'interface de ligne de commande

January 10, 2022

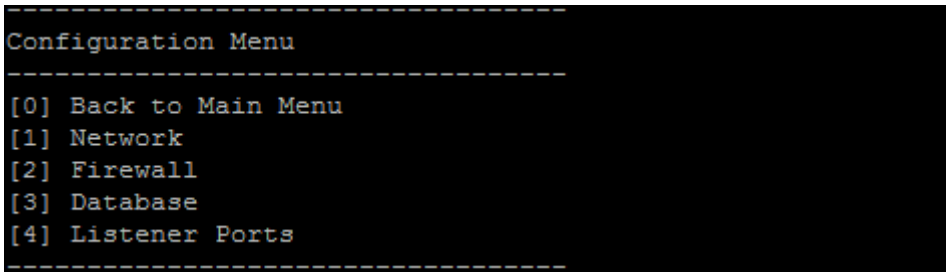
Pour une installation locale de XenMobile Server, vous pouvez accéder aux options de ligne de commande comme suit :

- **Depuis l'hyperviseur sur lequel vous avez installé XenMobile :** dans votre hyperviseur, sélectionnez la machine virtuelle XenMobile importée, démarrez l'invite de commande et connectez-vous à votre compte d'administrateur pour XenMobile. Pour de plus amples informations, consultez la documentation de votre hyperviseur.
- **Si SSH est activé sur votre pare-feu, à l'aide de SSH :** connectez-vous à votre compte administrateur pour XenMobile.

L'interface de ligne de commande vous permet d'effectuer un grand nombre de tâches de configuration et de dépannage. La figure suivante montre le menu de niveau supérieur de l'interface de ligne de commande.

Options de configuration

Exemples du **menu de configuration** et des paramètres affichés pour chaque option :



[1] Réseau

```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  IP address [10.207.87.75]:10.200.87.75
  Netmask [255.255.254.0]:255.255.254.0
  Default gateway [10.207.86.1]:10.200.86.1
  Primary DNS server [10.207.86.50]:10.200.86.50
  Secondary DNS server (optional) []:

Applying network settings...

Are you sure to restart the system? [y/n]:
```

[2] Pare-feu

```
Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:
 - comma separated list of hosts or networks
 - e.g. 10.20.5.3, 10.20.6.0/24
 - an empty value means no access restriction
 - enter c as value to clear list

  HTTP service
    Port: 80
    Enable access (y/n) [y]: y
    Access white list []:

  Management HTTPS service
    Port: 4443
    Enable access (y/n) [y]:
    Access white list []:

  SSH service
    Port [22]:
    Enable access (y/n) [y]:
    Access white list []:

  Management API (for initial staging) HTTPS service
    Port [30001]:
    Enable access (y/n) [n]:

  Remote support tunnel
    Port [8081]:
    Enable access (y/n) [n]:

Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
```


[3] Base de données

```
  Type: [mi]
  Use SSL (y/n) [n]:
  Server [10.207.86.64]:
  Port [1433]:
  Username [sa]:
  Password:
  Database name [RC]:

 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]:
```

[4] Ports d'écoute

```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  HTTP [80]:
  HTTPS with certificate authentication [443]:
  HTTPS with no certificate authentication [8443]:
  HTTPS for management [4443]:
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
Are you sure to restart the system? [y/n]:
```

Options de mise en cluster

Exemples du **menu de mise en cluster** et des paramètres affichés pour chaque option :

```
---------------------------------
Clustering Menu
---------------------------------
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
---------------------------------
```

[1] Afficher l'état du cluster

```
Current Node ID: 181360459

Cluster Members:
node: 10.207.87.75  status: ACTIVE  role: OLDEST
node: 10.207.87.77  status: ACTIVE  role: NONE
node: 10.207.87.88  status: ACTIVE  role: NONE
```


[2] Activer/désactiver le cluster

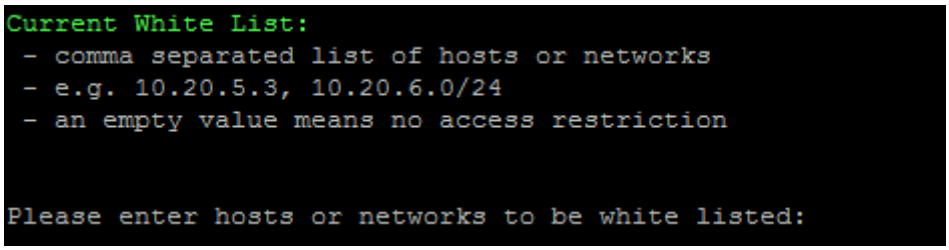
Lorsque vous choisissez d'activer la mise en cluster, le message suivant s'affiche :

```
To enable real-time communication between cluster members, please open port
 80 using the Firewall menu option in CLI menu. Also configure Access white
 list under Firewall settings for restricted access.
```

Lorsque vous choisissez de désactiver la mise en cluster, le message suivant s'affiche :

```
You have chosen to disable clustering. Access to port 80 is not needed.
Please disable it.
```

[3] Liste blanche des membres du cluster



[4] Activer ou désactiver le déchargement SSL

Si vous choisissez d'activer ou de désactiver le déchargement SSL, le message suivant s'affiche :

```
Enabling SSL offload opens port 80 for everyone. Please configure Access
white list under Firewall settings for restricted access.
```

[5] Afficher le cluster Hazelcast

Lorsque vous sélectionnez d'afficher le cluster Hazelcast, les options suivantes s'affichent :

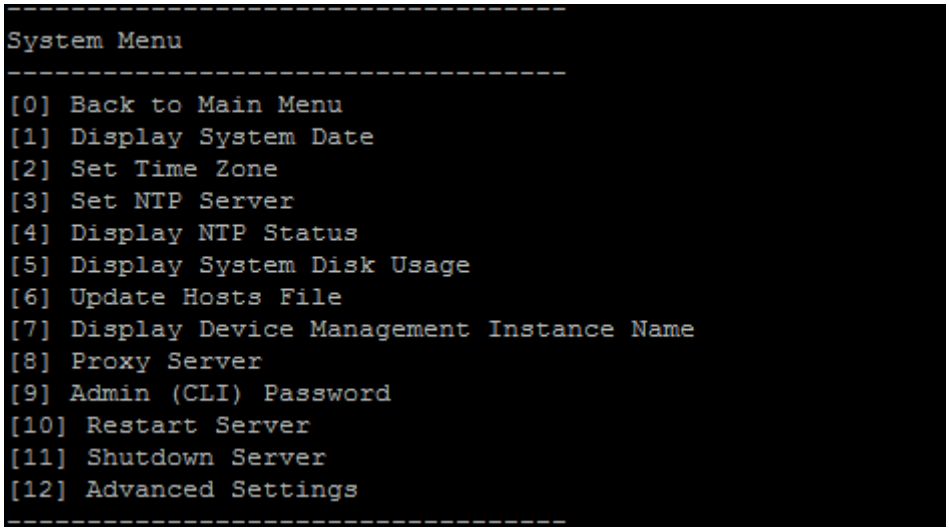
Membres du cluster Hazelcast :

[Adresses IP répertoriées]

> **Remarque :**
>
> Si un nœud configuré ne fait pas partie du cluster, redémarrez ce nœud.

Options système

À partir du **menu système**, vous pouvez afficher ou définir des informations de niveau du système, redémarrer ou arrêter le serveur ou accéder aux **Paramètres avancés**.



La définition du serveur NTP vous permet de spécifier les informations du serveur NTP. Si vous rencontrez des problèmes de fuseau horaire lors de la synchronisation de l'heure XenMobile avec un hyperviseur, vous pouvez éviter ces problèmes en pointant XenMobile sur un serveur NTP. Après avoir modifié cette option, redémarrez tous les serveurs en cluster.

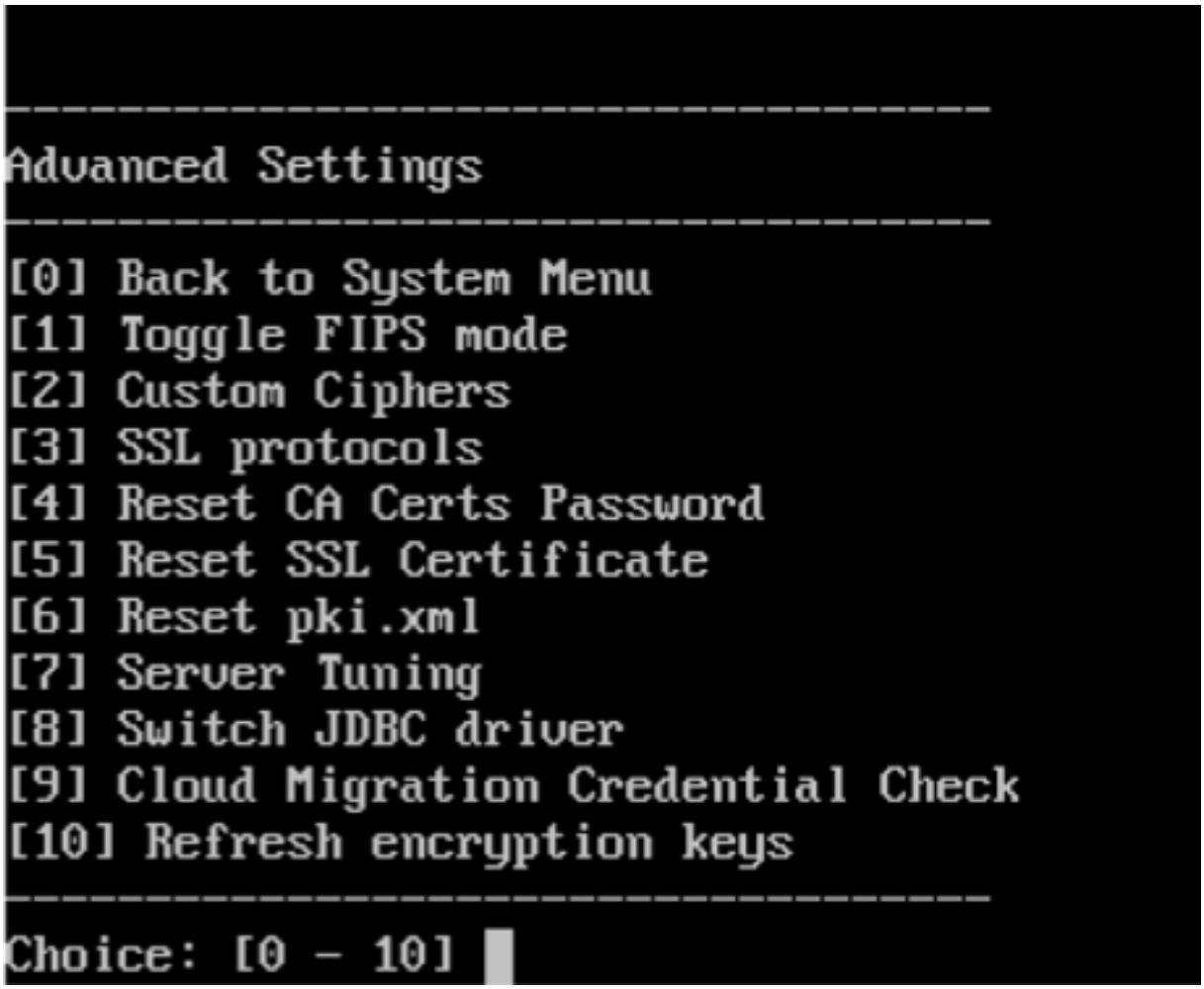
Vous pouvez également vérifier l'espace disque en affichant l'option de menu **[5]Afficher l'utilisation du disque système**.

À propos de l'arrêt des nœuds de serveur

Lorsque vous arrêtez un nœud de serveur unique dans un cluster, d'autres nœuds peuvent généralement gérer la charge de travail s'ils répondent aux exigences décrites dans la section Capacité à monter en charge et performances. L'impact peut varier en fonction du nombre de nœuds arrêtés en même temps, du nombre total d'utilisateurs et de la durée d'arrêt des nœuds.

- Les utilisateurs peuvent toujours accéder à Secure Hub et au magasin.
- Les utilisateurs peuvent toujours accéder aux applications gérées déployées et les lancer, si un nœud disponible peut gérer le nombre d'utilisateurs. Les connexions peuvent être plus lentes, ce qui entraîne des archivages plus lents des appareils.
- Les stratégies d'appareil continuent de fonctionner sauf si tous les nœuds sont arrêtés. Selon les ressources et le nombre d'appareils, les stratégies peuvent être déployées plus lentement.

[12] Paramètres avancés



L'option **Protocoles SSL** est réglée sur tous les protocoles autorisés par défaut. Après l'invite **New SSL protocols to enable**, entrez les protocoles que vous souhaitez activer. XenMobile désactive les protocoles que vous n'avez pas inclus dans votre réponse. Par exemple : pour désactiver TLSv1, tapez `TLSv1.2,TLSv1.1` et tapez **y** pour redémarrer le serveur XenMobile.

Les options de **réglage du serveur** incluent un délai d'expiration de la connexion au serveur, un nombre maximal de connexions (par port) et un nombre maximal de threads (par port).

Les options de **basculement de pilote JDBC** sont **jTDS** et **Microsoft**. Le pilote par défaut est jTDS. Pour plus d'informations sur le basculement vers le pilote JDBC de Microsoft, consultez la section Pilotes SQL Server.

Options de dépannage

Exemples du **menu de dépannage** et des paramètres affichés pour chaque option :


```
-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
-----------------------------------
Choice: [0 - 4] 4
```

[1] Utilitaires de réseau

```
---------------------------------
Network Menu
---------------------------------
[0] Back to Troubleshooting Menu
[1] Network Information
[2] Show Routing Table
[3] Show Address Resolution Protocol (ARP) Table
[4] PING
[5] Traceroute
[6] DNS Lookup
[7] Network Trace
---------------------------------
```

[2] Journaux

```
-------------------------------------
Logs Menu
-------------------------------------
[0] Back to Troubleshooting Menu
[1] Display debug log file
[2] Display update log file
```


[3] Packs d'assistance

```
-----------------------------------
Support Bundle Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Upload Support Bundle by Using SCP
[3] Upload Support Bundle by Using FTP
-----------------------------------
```

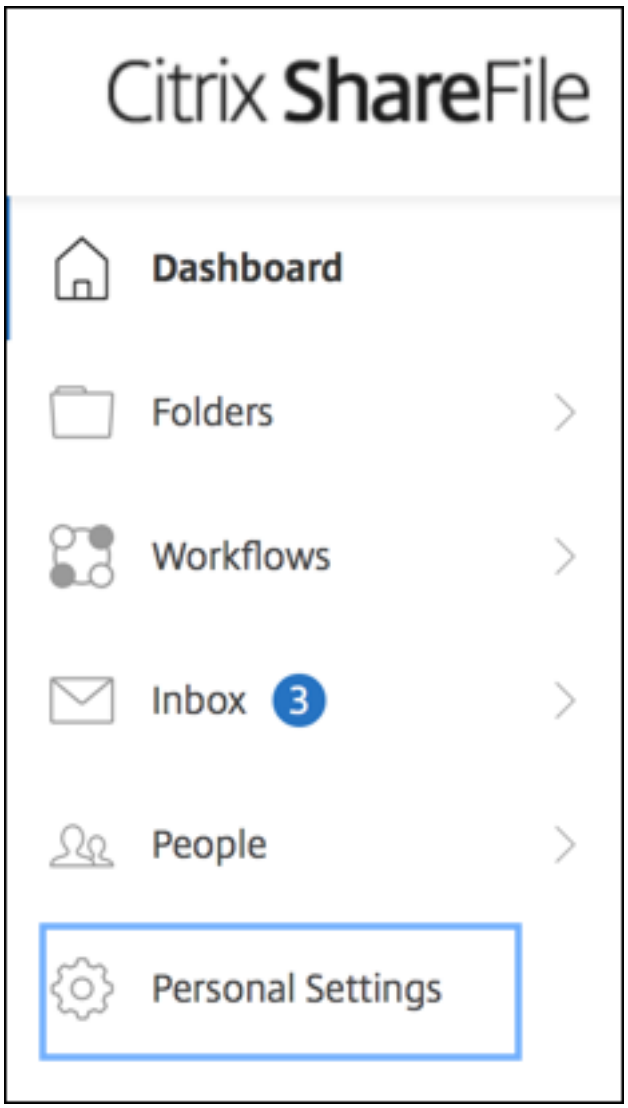
[4] Utilisation du disque

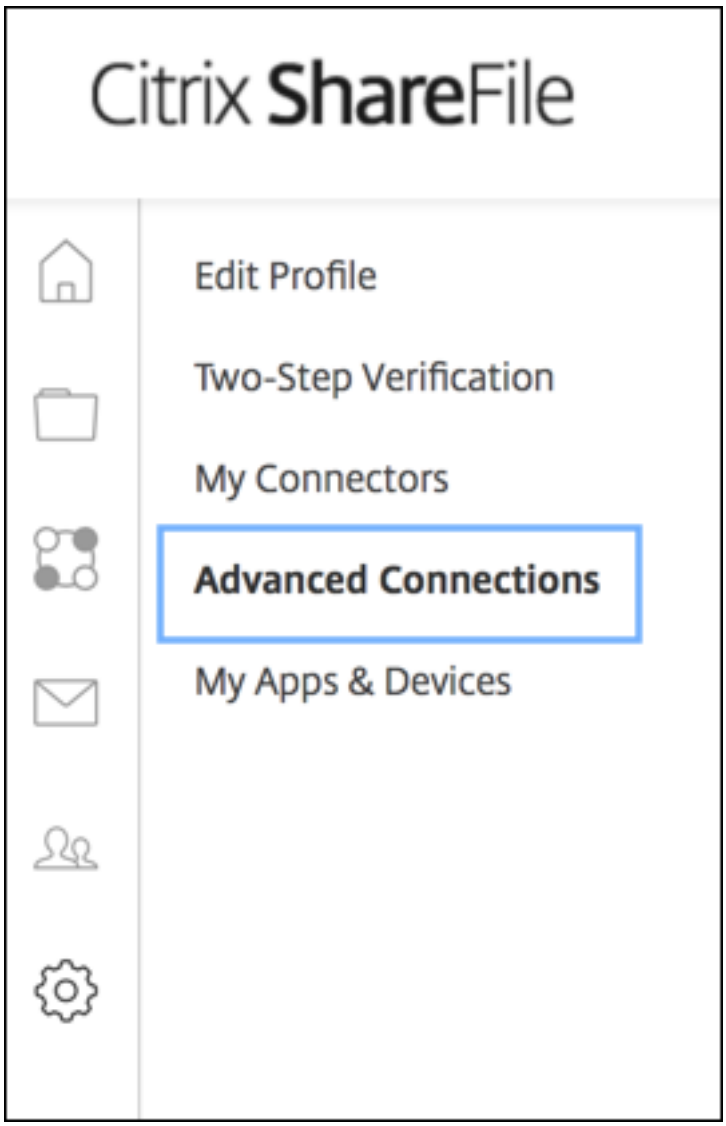
```
-------------------------------------

Troubleshooting Menu
-------------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
-------------------------------------
Choice: [0 - 4] 4
```

Pour télécharger un bundle de support via le site FTP Citrix Files

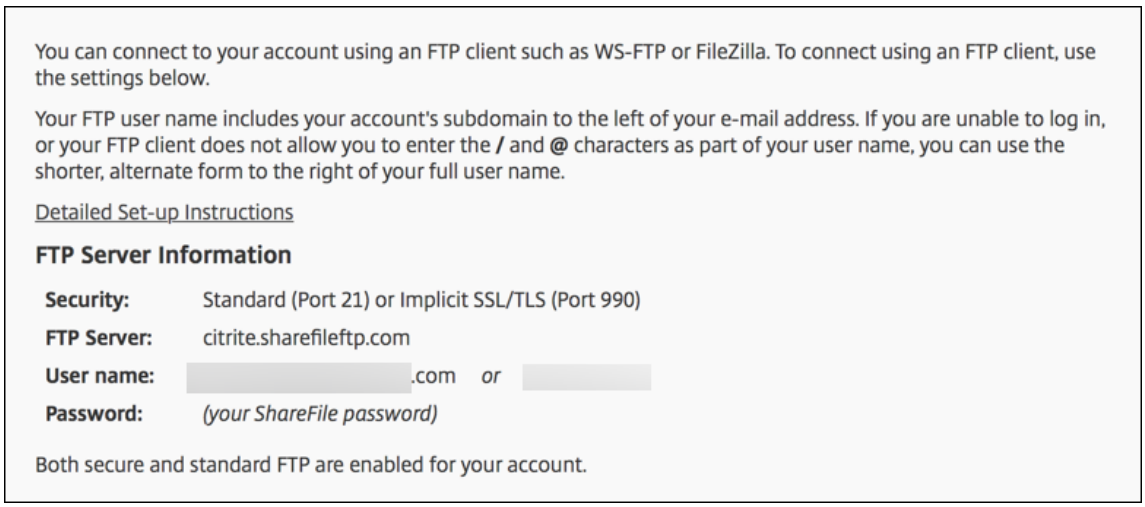
Avant de commencer le téléchargement d'un bundle de support, configurez les prérequis suivants sur Citrix Files :

1. Vérifiez les détails d'ouverture de session FTP.
   a. Dans un navigateur Web, ouvrez https://citrix.sharefile.com.
   b. Cliquez sur **Paramètres personnels**, puis sur **Connexions avancées**.





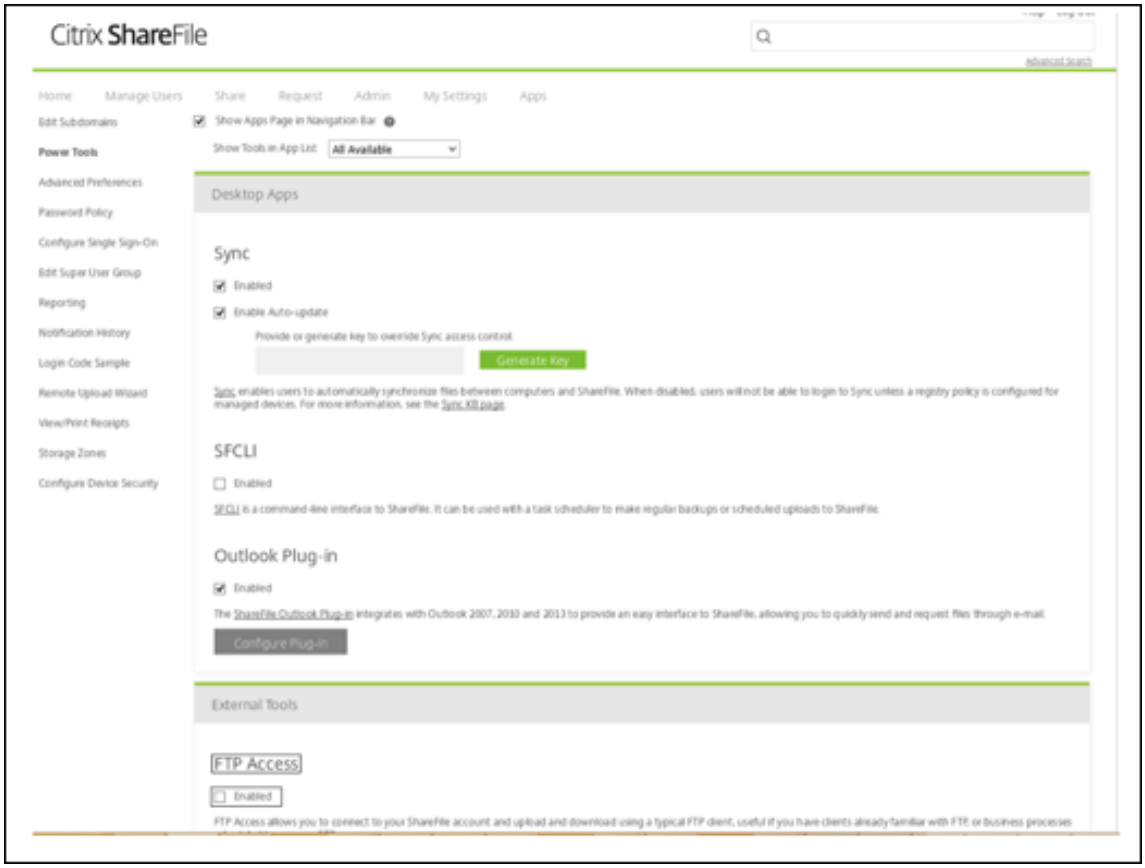
c. Dans les informations sur le serveur FTP, vérifiez que le nom d'utilisateur contient un ID utilisateur alphanumérique et des informations de sous-domaine/de nom d'utilisateur par défaut.



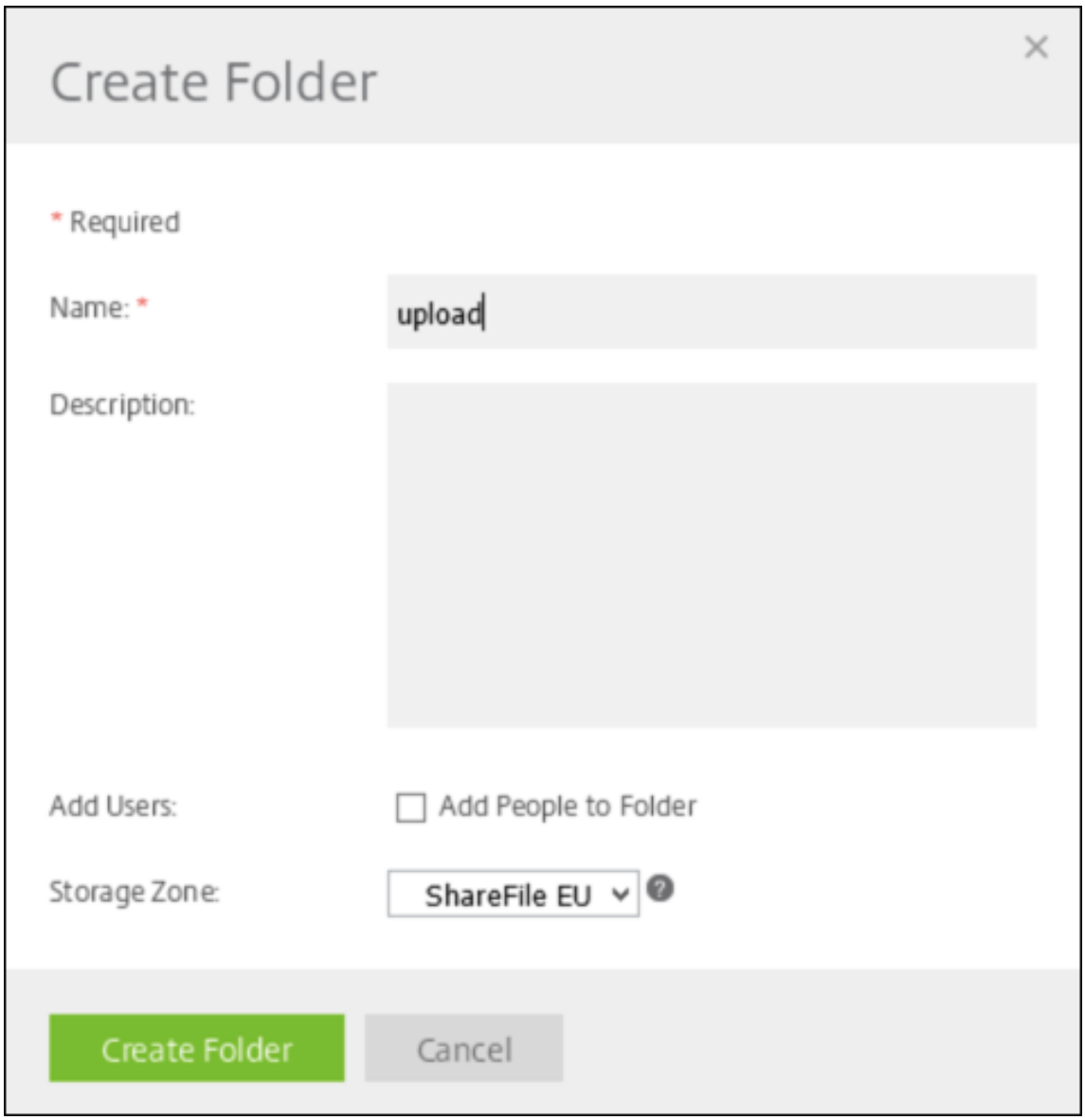
> **Remarques :**
>
> - Le fichier que vous téléchargez à partir de XenMobile est un client FTP basé sur une interface de ligne de commande Linux. Par conséquent, la barre oblique inverse (\) et l'arobase (@) ne sont pas autorisées dans votre nom d'utilisateur.
> - Si vous ne voyez pas l'ID utilisateur alphanumérique, vous pouvez l'obtenir auprès de l'administrateur ou du support Content Collaboration.

2. Vérifiez que les communications FTP et FTPS sont activées pour le serveur Citrix Files. Dans l'idéal, les administrateurs Content Collaboration autorisent l'ouverture d'un compte utilisateur pour la communication FTP. Toutefois, seule la communication FTPS est parfois autorisée.

   Un utilisateur possédant les droits d'administrateur peut vérifier et activer ce paramètre en cliquant sur **Paramètres**, **Paramètres d'administration**, **Préférences avancées** et **Activer outils ShareFile**. Dans **Applications externes** > **Accès FTP**, la case à cocher **Activer** est sélectionnée.



3. Créez un dossier partagé pour le client FTP à utiliser comme répertoire de téléchargement de fichiers. Cliquez sur **Accueil**, **Dossiers**, puis **Dossiers personnels**.
4. À l'extrême droite, cliquez sur l'icône (+) et sur **Créer un dossier**, puis entrez le nom du dossier.



5. Dans le **menu principal** de l'interface de ligne de commande XenMobile Server, sélectionnez **Troubleshooting > Support Bundle**. Dans le **menu Support Bundle**, sélectionnez **Generate Support Bundle**.

> **Remarque :**
>
> Si un bundle de support existe, saisissez **y** pour remplacer le bundle lorsque vous y êtes invité.

6. Téléchargez le bundle de support vers le serveur FTP :

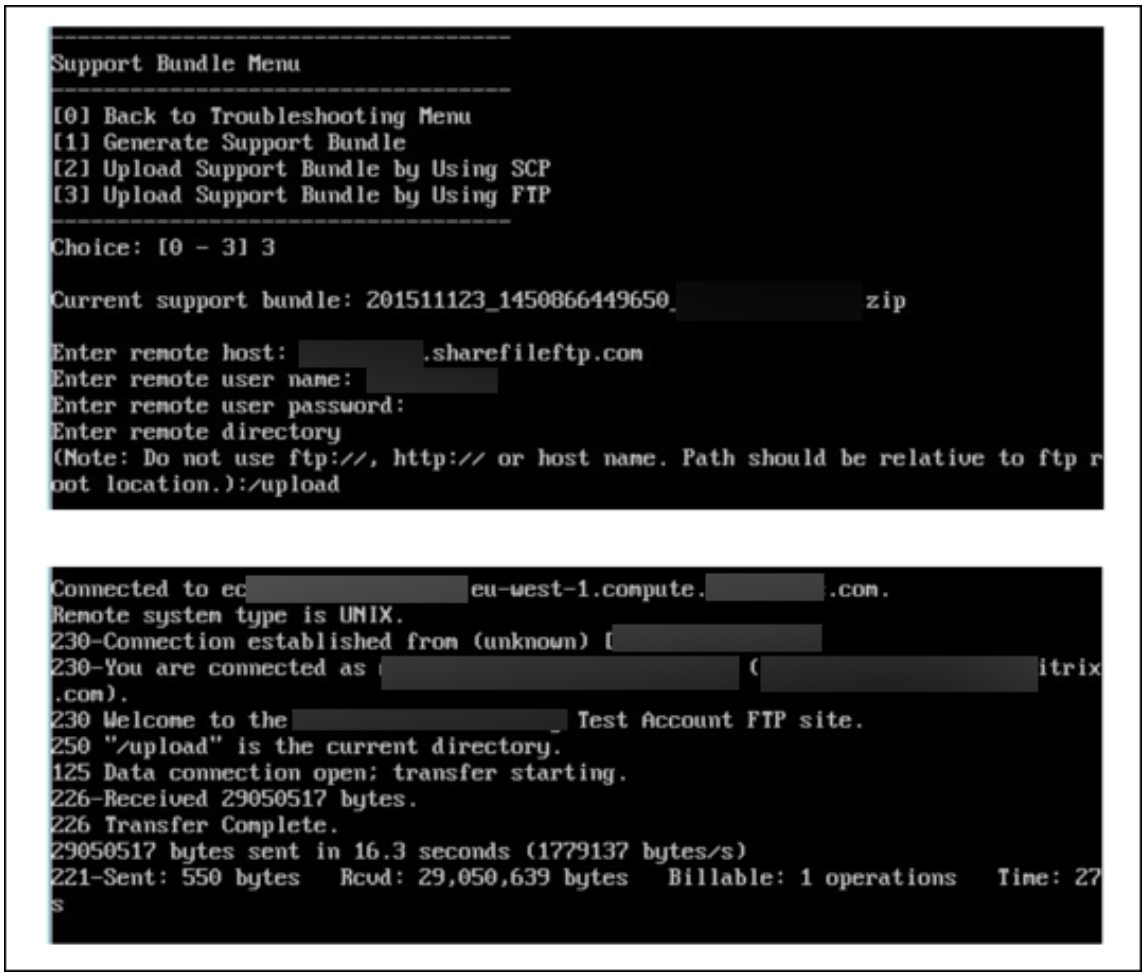
   a. Sélectionnez **Upload Support Bundle by using FTP**.

   b. **Enter remote host :** lorsque vous êtes invité à saisir l'hôte distant, saisissez le nom de votre serveur FTP. Lorsque Citrix Files est utilisé comme serveur FTP, saisissez le nom de l'entreprise, suivi du nom du site FTP Citrix Files. Par exemple, citrix.sharefileftp.com.

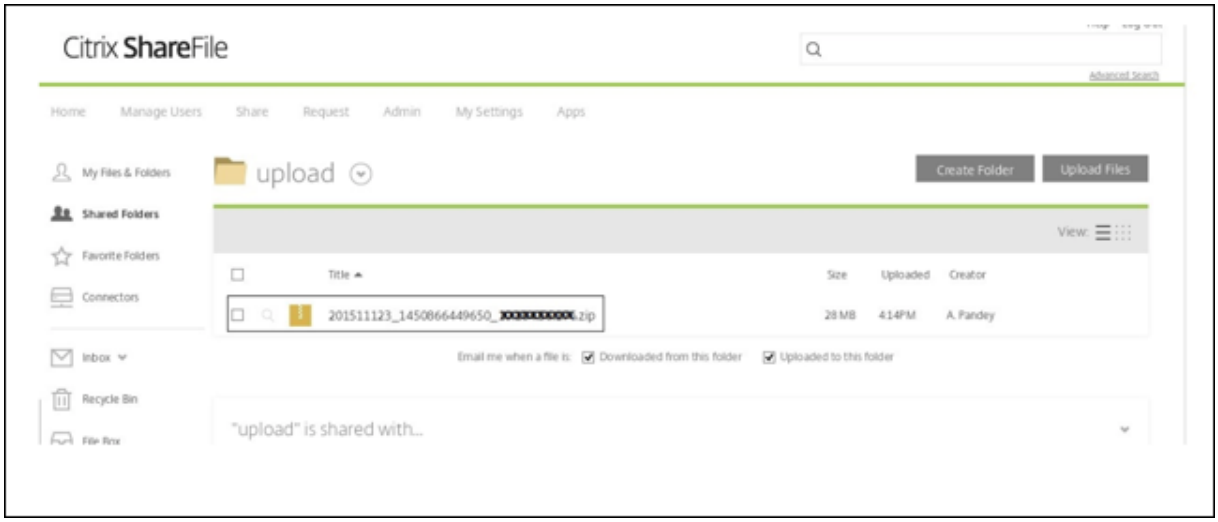
c. **Enter remote user name :** lorsque vous êtes invité à saisir le nom d'utilisateur distant, saisissez l'ID utilisateur alphanumérique.

d. **Enter remote user password :** lorsque vous êtes invité à saisir le mot de passe utilisateur distant, saisissez votre mot de passe.

e. **Enter remote directory :** lorsque vous êtes invité à saisir le répertoire distant, entrez le nom de dossier partagé créé dans Citrix Files et appuyez sur **Entrée**.



Vous pouvez afficher le bundle de support téléchargé dans le dossier partagé créé dans Citrix Files.



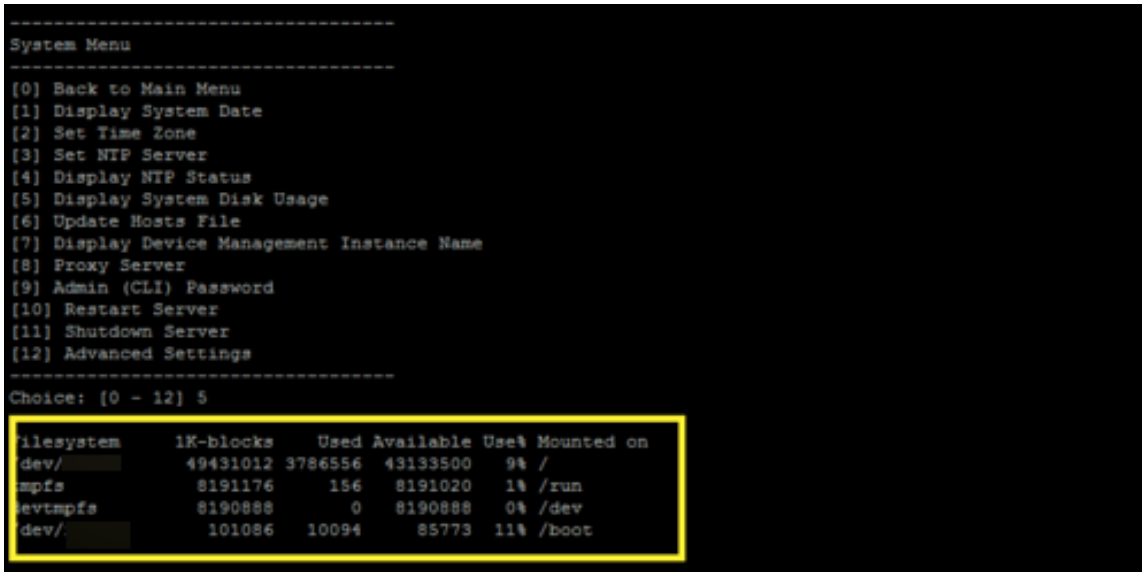
Pour plus d'informations sur Capacité à monter en charge et performances FTP, consultez cet article du centre de connaissances du support Citrix.

Pour vérifier l'espace disque

Vous pouvez vérifier l'espace disque système dans l'interface de ligne de commande comme suit :

1. Dans le menu principal, sélectionnez le menu **Système**.
2. Dans le menu **Système**, sélectionnez l'option **Afficher l'utilisation du disque système**.

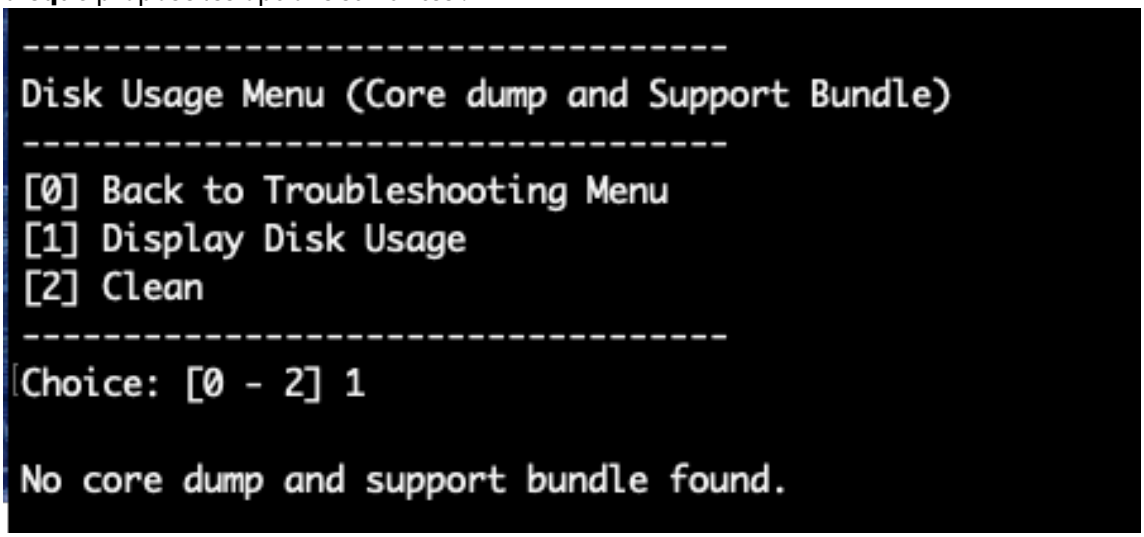
   Les informations du système de fichiers s'affichent.



Pour effectuer un nettoyage de disque en libre-service

Vous pouvez nettoyer le disque dans l'interface de ligne de commande comme suit :

1. Dans le **menu Dépannage**, sélectionnez **Utilisation du disque**. Le **menu Utilisation du disque** propose les options suivantes :



2. Tapez 1 pour répertorier les types de fichiers d'image mémoire et de pack de support. S'il n'y a pas de fichiers, le message suivant s'affiche : **No core dump and support bundles found.**
3. Tapez 2 pour nettoyer le fichier d'image mémoire analysé et le fichier de pack de support.

Présentation des workflows pour la console XenMobile

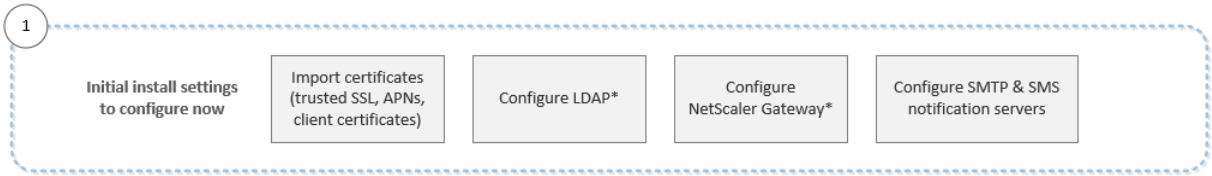
January 10, 2022

La console XenMobile est l'outil de gestion unifiée dans XenMobile. Cet article suppose que vous avez installé XenMobile et que vous êtes prêt à travailler dans la console. Si vous devez encore installer XenMobile, consultez la section Installer XenMobile. Pour plus de détails sur les navigateurs pris en charge pour la console XenMobile, consultez la section Prise en charge des navigateurs dans l'article Compatibilité XenMobile.

Workflow des paramètres initiaux

Après avoir terminé la configuration de XenMobile dans la console de ligne de commande puis dans la console XenMobile, le tableau de bord s'ouvre. Vous ne pouvez pas revenir aux écrans de configuration initiale. Si vous n'avez pas effectué certaines configurations de l'installation, vous pouvez configurer les paramètres suivants dans la console. Avant de commencer à ajouter des utilisateurs, des applications et des appareils, il est préférable d'avoir complété ces paramètres d'installation. Pour commencer, cliquez sur l'icône d'engrenage dans le coin supérieur droit.

> **Remarque :**
>
> Les éléments marqués d'un astérisque sont facultatifs.



Pour plus d'informations sur chaque paramètre, ainsi que les procédures détaillées, consultez les sections et articles suivants de la documentation des produits Citrix :

- Authentification
- Citrix Gateway et XenMobile
- Notifications

Pour prendre en charge les plates-formes Windows, iOS et Android, vous devez configurer votre compte comme suit.

Android

- Créer les informations d'identification Google Play. Pour de plus amples informations, consultez Launch dans Google Play.
- Créer un compte d'administrateur Android Enterprise. Pour de plus amples informations, consultez la section Android Enterprise.
- Vérifier votre nom de domaine avec Google. Pour plus de détails, voir Vérifier votre domaine pour Google Workspace.
- Activer les API et créer un compte de service pour Android Enterprise. Pour de plus amples informations, consultez la section Aide Android Enterprise.

iOS

- Créer un compte Apple ID et de développeur. Pour de plus amples informations, consultez le site Web Apple Developer Program.
- Créer un certificat APNS (Apple Push Notification Service). Si vous envisagez de gérer des appareils iOS avec votre déploiement XenMobile Server, vous avez besoin d'un certificat APNS d'Apple. Si vous utilisez la notification push pour votre déploiement Secure Mail, vous avez aussi besoin d'un certificat APNs d'Apple. Pour de plus amples informations, consultez le portail Apple Push Certificates Portal. Pour plus d'informations sur XenMobile et APNS, consultez Certificats APNs et Notifications push pour Secure Mail pour iOS.
- Créez un jeton d'entreprise d'achat en volume. Pour de plus amples informations, consultez la section Programme d'achat en volume d'Apple.

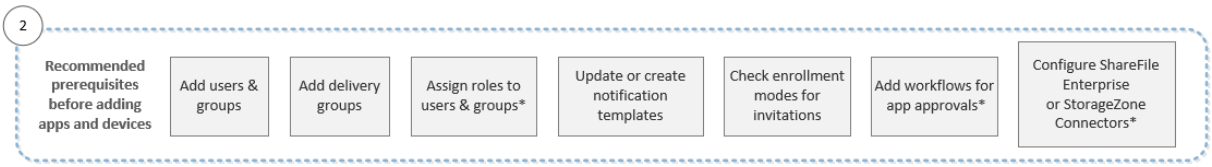
Windows

- Créer un compte de développeur Microsoft Windows Store. Pour plus d'informations, consultez la page Types de compte, emplacements et frais.
- Obtenir un ID Microsoft Windows Store Publisher. Pour plus d'informations, consultez la page Gérer les paramètres de compte et les informations de profil.
- Obtenir un certificat d'entreprise de DigiCert. Pour plus d'informations, consultez la page Company app distribution for Windows Phone.
- Si vous souhaitez utiliser le service de détection automatique de XenMobile pour l'inscription de votre Windows Phone, assurez-vous que vous disposez d'un certificat SSL public. Pour de plus amples informations, consultez la section XenMobile AutoDiscovery Service.
- Créer un jeton d'inscription d'application (AET). Pour plus d'informations, consultez la page How to generate an application enrollment token for Windows Phone.

Workflow de la configuration requise pour la console

Ce workflow affiche les prérequis que vous devez configurer avant d'ajouter des applications et des appareils.

> **Remarque :**
>
> Les éléments marqués d'un astérisque sont facultatifs.



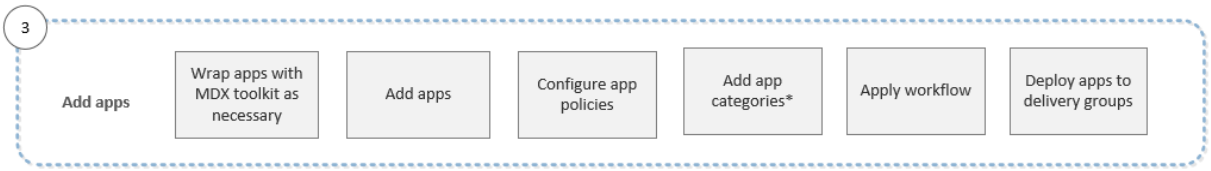
Pour plus d'informations sur chaque paramètre, ainsi que les procédures détaillées, consultez les sections et articles suivants de la documentation des produits Citrix :

- Comptes utilisateur, rôles et inscription
- Déployer des ressources
- Configurer des rôles avec RBAC
- Notifications
- Appliquer les workflows
- Utiliser Citrix Content Collaboration avec XenMobile

Workflow d'ajout d'applications

Ce workflow affiche un ordre recommandé à suivre lors de l'ajout d'applications à XenMobile.

> **Remarque :**
>
> Les éléments marqués d'un astérisque sont facultatifs.



Pour plus d'informations sur chaque paramètre, ainsi que les procédures détaillées, consultez les sections et articles suivants de la documentation des produits Citrix :

- À propos du MDX Toolkit
- Ajouter des applications
- Synopsis des stratégies MDX
- Appliquer les workflows
- Déployer des ressources

Workflow d'ajout d'appareils

Ce workflow affiche un ordre recommandé à suivre lors de l'ajout et de l'enregistrement d'appareils dans XenMobile.

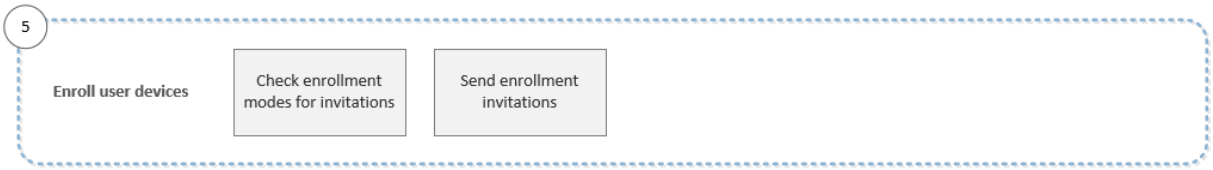
> **Remarque :**
>
> Les éléments marqués d'un astérisque sont facultatifs.

Pour plus d'informations sur chaque paramètre, ainsi que les procédures détaillées, consultez les sections et articles suivants de la documentation des produits Citrix :

- Périphériques
- Systèmes d'exploitation d'appareils pris en charge
- Déployer des ressources
- Surveillance et support
- Actions automatisées

Workflow d'inscription d'appareils utilisateur

Ce workflow affiche un ordre recommandé à suivre lors de l'inscription d'appareils utilisateur dans XenMobile.



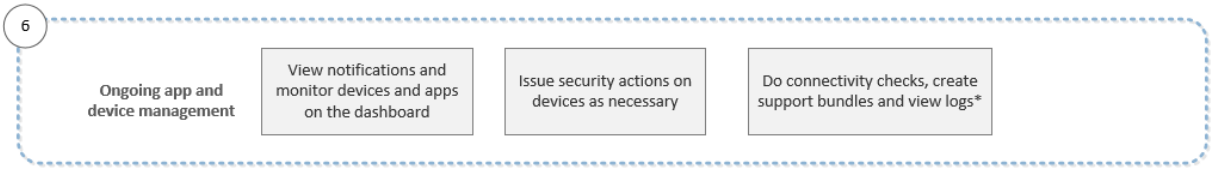
Pour plus d'informations sur chaque paramètre, ainsi que les procédures détaillées, consultez les articles suivants de la documentation des produits Citrix :

- Comptes utilisateur, rôles et inscription
- Notifications

Workflow de gestion des applications et appareils

Ce workflow affiche les activités de gestion des applications et des appareils que vous pouvez effectuer dans la console.

> **Remarque :**
>
> Les éléments marqués d'un astérisque sont facultatifs.



Pour de plus amples informations sur les options de support disponibles à partir de l'icône de clé dans le coin supérieur droit de la console, consultez la section Surveillance et support.

Certificats et authentification

January 10, 2022

Plusieurs composants jouent un rôle dans le processus d'authentification lors des opérations XenMobile :

- **XenMobile Server :** XenMobile Server vous permet de définir la sécurité liée à l'inscription ainsi que l'expérience d'inscription. Les options d'intégration des utilisateurs comprennent :
  - Inscription ouverte à tous ou sur invitation seulement.
  - Authentification à deux facteurs ou à trois facteurs obligatoire. Dans les propriétés du client XenMobile, vous pouvez activer l'authentification par code PIN Citrix et configurer la complexité et le délai d'expiration du code PIN.

- **Citrix ADC :** Citrix ADC fournit une expiration pour les sessions SSL micro VPN. Citrix ADC assure aussi la sécurité en transit sur le réseau et vous permet de définir l'expérience d'authentification utilisée chaque fois qu'un utilisateur accède à une application.
- **Secure Hub :** Secure Hub fonctionne avec XenMobile Server au cours des opérations d'inscription. Secure Hub est l'entité basée sur un appareil qui communique avec Citrix ADC : lorsqu'une session expire, Secure Hub obtient un ticket d'authentification de Citrix ADC et transmet le ticket aux applications MDX. Citrix vous recommande le certificate pinning, qui empêche les attaques « man-in-the-middle ». Pour de plus amples informations, consultez cette section dans l'article Secure Hub : Certificate pinning.

  Secure Hub gère également le conteneur de sécurité MDX : Secure Hub force les stratégies, crée une session avec Citrix ADC lors de l'expiration d'une application et définit le délai d'expiration MDX et l'authentification. Secure Hub est également responsable de la détection des appareils jailbreakés, des contrôles de géolocalisation et de toute autre stratégie que vous appliquez.
- **Stratégies MDX :** les stratégies MDX créent l'espace de stockage sécurisé sur l'appareil. Les stratégies MDX redirigent les connexions micro VPN vers Citrix ADC et appliquent les restrictions du mode déconnecté ainsi que les stratégies de client, telles que les délais d'expiration.

Pour de plus amples informations sur la configuration de l'authentification, y compris une vue d'ensemble des méthodes d'authentification à un et deux facteurs, veuillez consulter l'article Authentification du manuel de déploiement.

Dans XenMobile, les certificats permettent d'établir des connexions sécurisées et d'authentifier les utilisateurs. Le reste de cet article décrit les certificats. Pour plus d'informations sur la configuration, consultez les articles suivants :

- Authentification domaine ou domaine + jeton de sécurité
- Authentification certificat client ou certificat + domaine
- Entités PKI
- Fournisseurs d'informations d'identification
- Certificats APNs
- SAML pour l'authentification unique avec Citrix Files
- Paramètres du serveur Microsoft Azure Active Directory
- Pour envoyer un certificat aux appareils pour l'authentification auprès du serveur Wi-Fi : Stratégie Wi-Fi
- Pour envoyer un certificat unique non utilisé pour l'authentification, tel qu'un certificat d'autorité de certification racine interne ou une stratégie spécifique : Stratégie d'informations d'identification

Certificats

XenMobile génère un certificat SSL auto-signé lors de l'installation afin de sécuriser les communications sur le serveur. Vous devez remplacer le certificat SSL avec un certificat SSL approuvé provenant d'une autorité de certification (CA) reconnue.

XenMobile utilise également son propre service d'infrastructure de clé publique (PKI) ou obtient les certificats de l'autorité de certification pour les certificats clients. Tous les produits Citrix prennent en charge les caractères génériques et les certificats SAN. Pour la plupart des déploiements, vous n'aurez besoin que deux caractères génériques ou certificats SAN.

L'authentification du certificat client offre une couche de sécurité supplémentaire pour les applications mobiles et permet aux utilisateurs d'accéder de manière transparente aux applications HDX. Lorsque l'authentification du certificat client est configurée, les utilisateurs entrent leur code PIN Citrix pour accéder en Single Sign-On aux applications XenMobile. Le code secret Citrix simplifie également l'expérience utilisateur pour l'authentification. Le code PIN Citrix est utilisé pour sécuriser un certificat client ou enregistrement des informations d'identification Active Directory localement sur leur appareil.

Pour inscrire et gérer des appareils iOS avec XenMobile, configurez et créez un certificat Apple Push Notification Service (APNS). Ces étapes sont décrites sous Certificats APNS.

Le tableau suivant illustre le format et le type du certificat pour chaque composant de XenMobile :

Composant XenMobile	Format du certificat	Type de certificat requis
Citrix Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Root (Citrix Gateway convertit automatiquement un fichier PFX vers PEM.)
XenMobile Server	.p12 (.pfx sur les ordinateurs Windows)	SSL, SAML, APN (XenMobile génère également une PKI complète au cours du processus d'installation.) Important : XenMobile Server ne prend pas en charge les certificats avec une extension .pem. Pour utiliser un certificat .pem, divisez le fichier .pem en un certificat et une clé et importez-les dans XenMobile Server.
StoreFront	PFX (PKCS #12)	SSL, racine

XenMobile prend en charge les certificats d'écoute SSL et les certificats clients de 4096, 2048 et 1024 bits. Les certificats 1024 bits sont facilement compromis.

Pour Citrix Gateway et XenMobile Server, Citrix recommande d'obtenir les certificats de serveur à partir d'une autorité de certification publique, comme Verisign, Thawte ou DigiCert. Vous pouvez créer une demande de signature de certificat (CSR) à partir de Citrix Gateway ou de l'utilitaire de configuration XenMobile. Lorsque vous créez la CSR, envoyez-la à l'autorité de certification pour signature. Lorsque l'autorité de certification renvoie le certificat signé, vous pouvez l'installer sur Citrix Gateway ou XenMobile.

> **Important : conditions requises pour les certificats de confiance dans iOS, iPadOS et macOS**
>
> Apple a introduit de nouvelles exigences pour les certificats de serveur TLS. Vérifiez que tous les certificats respectent les nouvelles exigences d'Apple. Consultez la publication Apple, https://support.apple.com/en-us/HT210176.
>
> Apple réduit la durée de vie maximale autorisée des certificats de serveur TLS. Cette modification concerne uniquement les certificats de serveur émis après septembre 2020. Consultez la publication Apple, https://support.apple.com/en-us/HT211025.

Chargement de certificats dans XenMobile

Chaque certificat que vous chargez est représenté par une entrée dans le tableau Certificats, qui résume son contenu. Lorsque vous configurez des composants d'intégration PKI qui nécessitent un certificat, vous choisissez un certificat de serveur répondant à des critères spécifiques au contexte. Par exemple, il se peut que vous souhaitiez configurer XenMobile pour s'intégrer à votre autorité de certification Microsoft. La connexion à Microsoft CA doit être authentifiée à l'aide d'un certificat client.

Cette section explique comment charger des certificats. Pour de plus amples informations sur la création, le chargement et la configuration de certificats clients, consultez la section Authentification certificat client ou certificat + domaine.

Configuration requise pour la clé privée

XenMobile peut posséder ou pas la clé privée d'un certificat donné. De même, XenMobile peut nécessiter ou non une clé privée pour les certificats chargés.

Chargement de certificats

Vous disposez de deux options pour charger des certificats :

- Chargez les certificats individuellement sur la console.
- Effectuez un chargement groupé de certificats sur des appareils iOS avec l'API REST.

Vous avez le choix entre deux options principales pour charger des certificats sur la console :

- Cliquez pour importer un keystore. Vous identifiez ensuite l'entrée dans le référentiel de keystore dans lequel vous souhaitez l'installer, sauf si vous chargez un format PKCS #12.
- Cliquez pour importer un certificat.

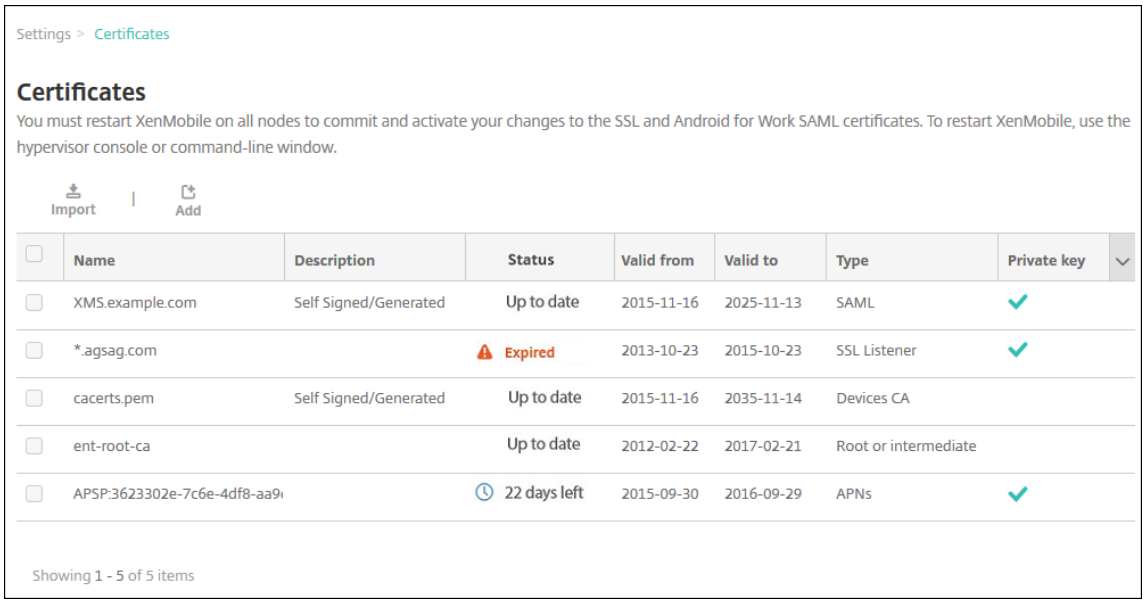
Vous pouvez charger le certificat d'autorité de certification (sans clé privée) que l'autorité de certification utilise pour signer les demandes. Vous pouvez également charger un certificat de client SSL (avec clé privée) pour l'authentification du client.

Lors de la configuration de l'entité Microsoft CA, vous spécifiez le certificat d'autorité de certification. Vous sélectionnez le certificat d'autorité de certification dans une liste de tous les certificats de serveur qui sont des certificats d'autorité de certification. De même, lorsque vous configurez l'authentification de client, vous pouvez faire votre choix dans une liste de tous les certificats de serveur pour lesquels XenMobile possède la clé privée.

Pour importer un keystore

À dessein, les keystores, qui sont des référentiels de certificats de sécurité, peuvent comporter plusieurs entrées. Par conséquent, lors du chargement à partir d'un keystore, vous êtes invité à indiquer l'alias d'entrée qui identifie l'entrée à charger. Si vous ne spécifiez pas d'alias, la première entrée du magasin est chargée. Étant donné que les fichiers PKCS #12 ne contiennent généralement qu'une seule entrée, le champ d'alias ne s'affiche pas lorsque vous sélectionnez PKCS #12 en tant que type de keystore.

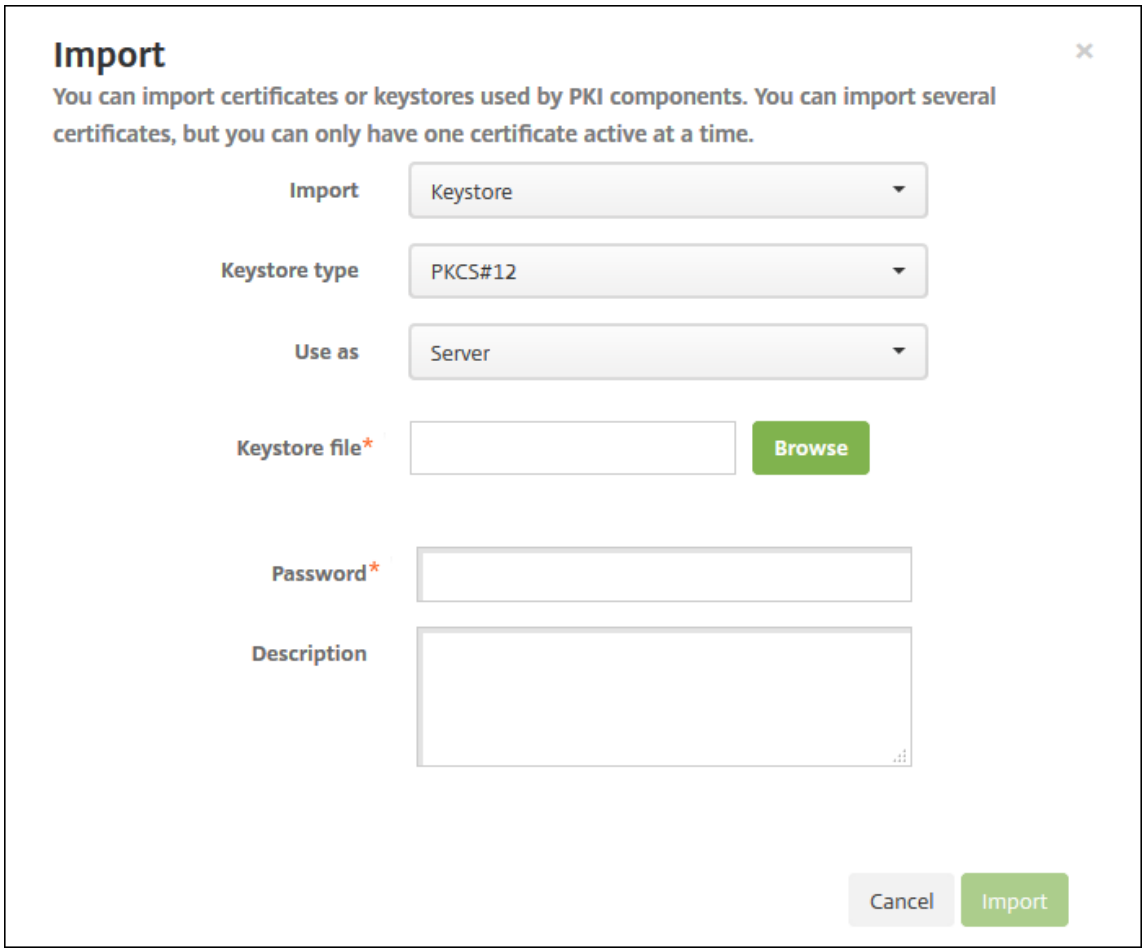
1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Certificats**. La page **Certificats** s'affiche.



3. Cliquez sur **Importer**. La boîte de dialogue **Importer** apparaît.

4. Pour configurer ces paramètres :

   - **Importer :** dans la liste, cliquez sur **Keystore**. La boîte de dialogue **Importer** change pour refléter les options de keystore disponibles.



   - **Type de keystore :** dans la liste, cliquez sur **PKCS #12**.
   - **Utiliser en tant que :** dans la liste, cliquez pour spécifier la manière dont vous prévoyez d'utiliser le certificat. Les options disponibles sont :
     - **Serveur**. Les certificats de serveur sont des certificats utilisés par XenMobile Server qui sont chargés sur la console Web XenMobile. Ils comprennent des certificats d'autorité de certification, des certificats d'autorité d'inscription et des certificats pour l'authentification des clients avec d'autres composants de votre infrastructure. En outre, vous pouvez utiliser les certificats de serveur en tant que stockage pour les certificats que vous voulez déployer vers des appareils. Cette utilisation s'applique particulièrement aux autorités de certification utilisées pour établir une relation de confiance sur l'appareil.
     - **SAML**. La certification SAML vous permet de fournir une authentification unique (SSO) aux serveurs, sites Web et applications.
     - **APNS**. Les certificats APNS d'Apple permettent de gérer les appareils mobiles via le

réseau Apple Push Network.
  - **Écouteur SSL**. L'écouteur SSL notifie XenMobile de l'activité cryptographique SSL.
- **Fichier de keystore :** recherchez le keystore de type de fichier .p12 que vous souhaitez importer (ou .pfx sur les ordinateurs Windows).
- **Mot de passe :** entrez le mot de passe affecté au certificat.
- **Description :** entrez une description vous permettant de distinguer le keystore de vos autres keystores (facultatif).

5. Cliquez sur **Importer**. Le keystore est ajouté au tableau Certificats.

Pour importer un certificat

Lors de l'importation d'un certificat, soit à partir d'un fichier, soit depuis une entrée de keystore, XenMobile tente de construire une chaîne de certificats à partir de l'entrée. XenMobile importe tous les certificats de cette chaîne pour créer une entrée de certificat de serveur pour chacun d'eux. Cette opération fonctionne uniquement si les certificats du fichier ou l'entrée keystore forment réellement une chaîne. Par exemple, si chaque certificat suivant de la chaîne est l'émetteur du certificat précédent.

Vous pouvez ajouter une description facultative pour le certificat importé. La description est uniquement attachée au premier certificat dans la chaîne. Vous pouvez mettre à jour la description des certificats restants plus tard.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Certificats**.
2. Sur la page **Certificats**, cliquez sur **Importer**. La boîte de dialogue **Importer** apparaît.
3. Dans la boîte de dialogue **Importer**, dans **Importer**, s'il n'est pas déjà sélectionné, cliquez sur **Certificat**.
4. La boîte de dialogue **Importer** change pour refléter les options de certificat disponibles. Dans **Utiliser en tant que**, sélectionnez comment vous prévoyez d'utiliser le keystore. Les options disponibles sont :
   - **Serveur**. Les certificats de serveur sont des certificats utilisés par XenMobile Server qui sont chargés sur la console Web XenMobile. Ils comprennent des certificats d'autorité de certification, des certificats d'autorité d'inscription et des certificats pour l'authentification des clients avec d'autres composants de votre infrastructure. En outre, vous pouvez utiliser les certificats de serveur en tant que stockage pour les certificats que vous voulez déployer vers des appareils. Cette option s'applique particulièrement aux autorités de certification utilisées pour établir une relation de confiance sur l'appareil.
   - **SAML**. La certification SAML vous permet de fournir une authentification unique (SSO) aux serveurs, sites Web et applications.

- **Écouteur SSL**. L'écouteur SSL notifie XenMobile de l'activité cryptographique SSL.

5. Recherchez le keystore de type de fichier .p12 que vous souhaitez importer (ou .pfx sur les ordinateurs Windows).
6. Parcourez pour rechercher un fichier de clé privée facultatif pour le certificat. La clé privée est utilisée pour le chiffrement et le déchiffrement en conjonction avec le certificat.
7. Entrez une description pour le certificat (facultatif) pour vous aider à le distinguer de vos autres certificats.
8. Cliquez sur **Importer**. Le certificat est ajouté au tableau Certificats.

Effectuer un chargement groupé de certificats sur des appareils iOS avec l'API REST

Si le chargement de certificats un par un n'est pas pratique, vous pouvez les charger de façon groupée sur des appareils iOS à l'aide de l'API REST. Cette méthode prend en charge les certificats au format .p12. Pour plus d'informations sur l'API REST, reportez-vous à la section API REST.

1. Renommez chacun des fichiers de certificat au format `device_identity_value.p12`. `device_identity_value` peut être l'IMEI, le numéro de série ou le MEID de chaque appareil.

   Par exemple, vous choisissez d'utiliser les numéros de série comme méthode d'identification. Le numéro de série de l'appareil est `A12BC3D4EFGH`, donc nommez le fichier de certificat que vous prévoyez d'installer sur cet appareil de la façon suivante : `A12BC3D4EFGH.p12`.

2. Créez un fichier texte pour stocker les mots de passe pour les certificats .p12. Dans ce fichier, tapez l'identifiant et le mot de passe de chaque appareil sur une nouvelle ligne. Utilisez le format `device_identity_value=password`. Procédez comme suit :

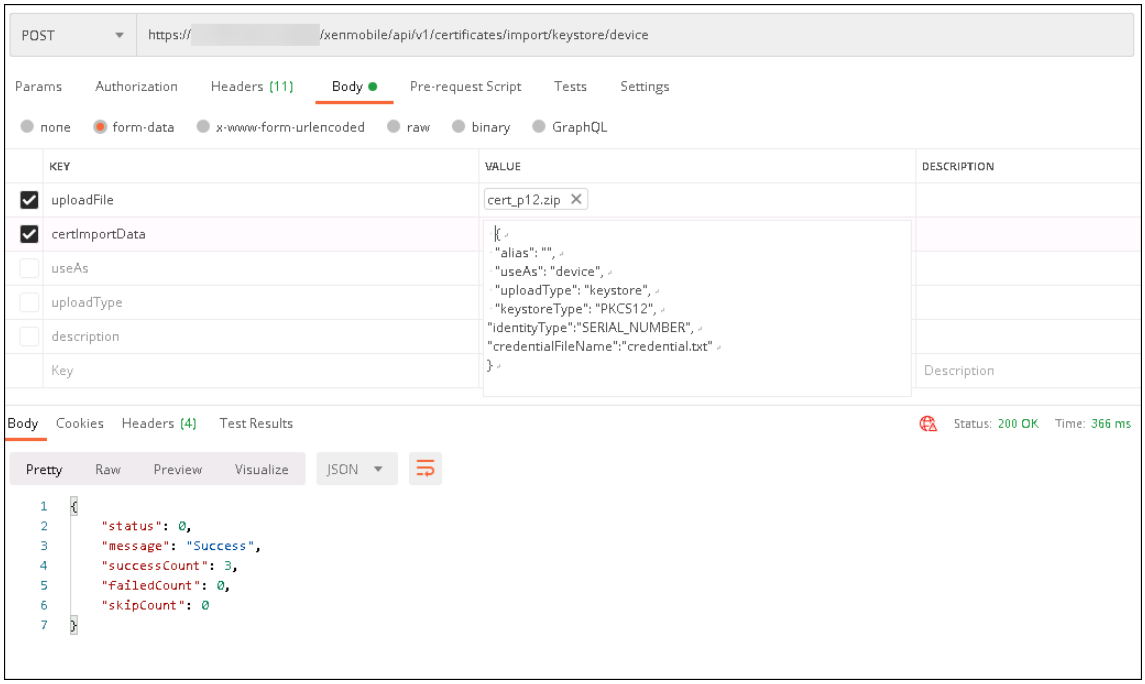
```
A12BC3D4EFGH.p12=password1!
A12BC3D4EFIJ.p12=password2@
A12BC3D4EFKL.p12=password3#
<!--NeedCopy-->
```

3. Compressez tous les certificats et le fichier texte que vous avez créé dans un fichier .zip.
4. Lancez votre client d'API REST, connectez-vous à XenMobile et obtenez un jeton d'authentification.
5. Importez vos certificats, en vous assurant de placer les éléments suivants dans le corps du message :

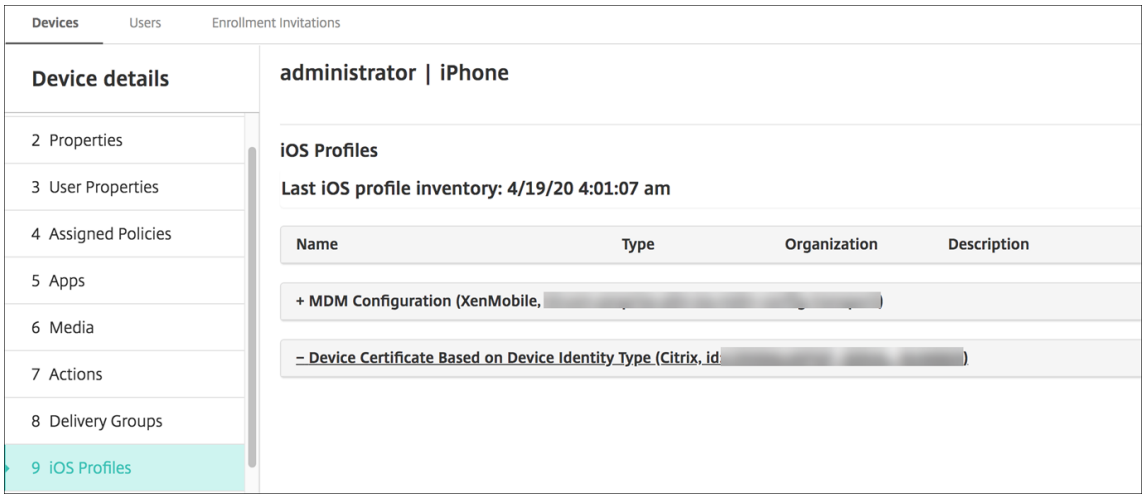
```
{

    "alias": "",
    "useAs": "device",
    "uploadType": "keystore",
    "keystoreType": "PKCS12",
```



```
    "identityType":"SERIAL_NUMBER",          # identity type can be
        "SERIAL_NUMBER","IMEI","MEID"
    "credentialFileName":"credential.txt"    # The credential file
        name in .zip
}

<!--NeedCopy-->
```

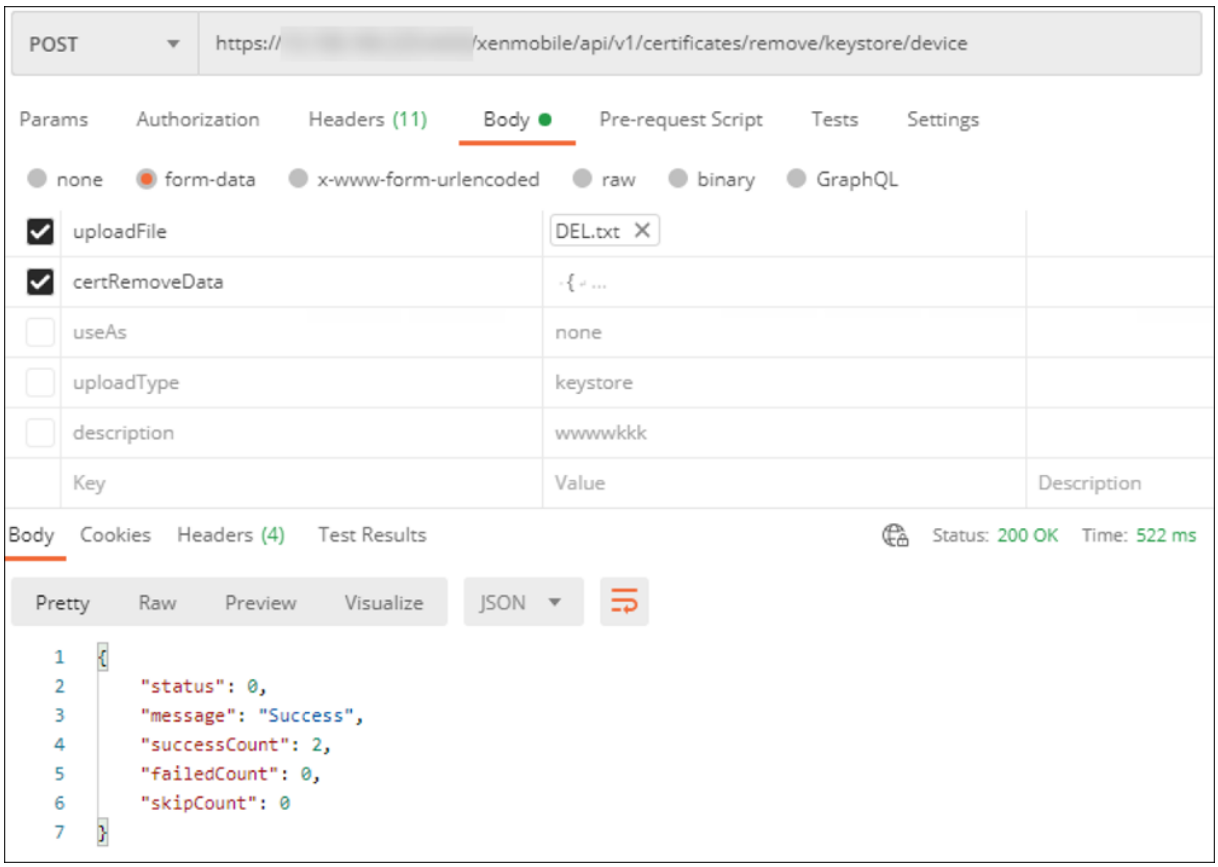


6. Créez une stratégie VPN avec le type d'informations d'identification **Always on IKEv2** (Toujours sur IKEv2) et la méthode d'authentification d'appareil **Certificat d'appareil basé sur l'identité de l'appareil**. Sélectionnez le **Type d'identité de l'appareil** que vous avez utilisé dans vos noms de fichiers de certificat. Consultez la section Stratégie VPN.
7. Inscrivez un appareil iOS et attendez le déploiement de la stratégie VPN. Confirmez l'installation du certificat en vérifiant la configuration MDM sur l'appareil. Vous pouvez également vérifier les détails de l'appareil dans la console XenMobile.



Vous pouvez également supprimer des certificats de façon groupée en créant un fichier texte avec la valeur `device_identity_value` répertoriée pour chaque certificat à supprimer. Dans l'API REST, appelez l'API delete et utilisez la requête suivante, en remplaçant `device_identity_value` par l'identifiant approprié :

```
1 ```
2 {
3
4     "identityType"="device_identity_value"
5  }
6
7 <!--NeedCopy--> ```
```

Mise à jour d'un certificat

XenMobile n'autorise l'existence que d'un seul certificat par clé publique dans le système à tout moment. Si vous essayez d'importer un certificat pour la même paire de clés qu'un certificat déjà importé, vous pouvez remplacer l'entrée existante ou la supprimer.

Pour mettre à jour vos certificats de la façon la plus efficace, dans la console XenMobile, procédez comme suit. Cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console pour ouvrir la page **Paramètres**, puis cliquez sur **Certificats**. Dans la boîte de dialogue **Importer**, importez le nouveau certificat.

Lorsque vous mettez un certificat de serveur à jour, les composants qui utilisaient le certificat précédent utilisent automatiquement le nouveau certificat. De même, si vous avez déployé le certificat de serveur sur les appareils, il sera automatiquement mis à jour lors du prochain déploiement.

Renouvellement d'un certificat

XenMobile Server utilise les autorités de certification suivantes en interne pour l'infrastructure de clé publique (PKI) : autorité de certification racine, autorité de certification d'appareil et autorité de certification de serveur. Ces autorités de certification sont classées en tant que groupe logique et reçoivent

un nom de groupe. Lorsqu'une nouvelle instance de XenMobile Server est provisionnée, les trois autorités de certification sont générées et se voient attribuer le nom de groupe « default ».

Vous pouvez renouveler les autorités de certification pour les appareils iOS, macOS et Android pris en charge à l'aide de la console XenMobile Server ou de l'API REST publique. Pour les appareils Windows inscrits, les utilisateurs doivent réinscrire leurs appareils pour recevoir une nouvelle autorité de certification d'appareil.

Les API suivantes sont disponibles pour le renouvellement ou la régénération des autorités de certification PKI internes dans XenMobile Server et le renouvellement des certificats d'appareils émis par ces autorités de certification.

- Créer des autorités de certification de groupe.
- Activer de nouvelles autorités de certification et désactiver les anciennes.
- Renouveler le certificat de l'appareil sur une liste configurée d'appareils. Les appareils déjà inscrits continuent de fonctionner sans interruption. Un certificat d'appareil est émis lorsqu'un appareil se reconnecte au serveur.
- Renvoyer une liste d'appareils qui utilisent l'ancienne autorité de certification.
- Supprimer l'ancienne autorité de certification une fois que tous les appareils ont la nouvelle autorité de certification.

Pour de plus amples informations, consultez les sections suivantes du PDF Public API for REST Services :

- Section 3.16.58, Renouveler le certificat d'appareil
- Section 3.23, Groupes internes d'autorisation de certificat PKI

La console **Gérer les appareils** inclut l'action de sécurité, **Renouvellement de certificat**, utilisée pour renouveler le certificat d'inscription sur un appareil.

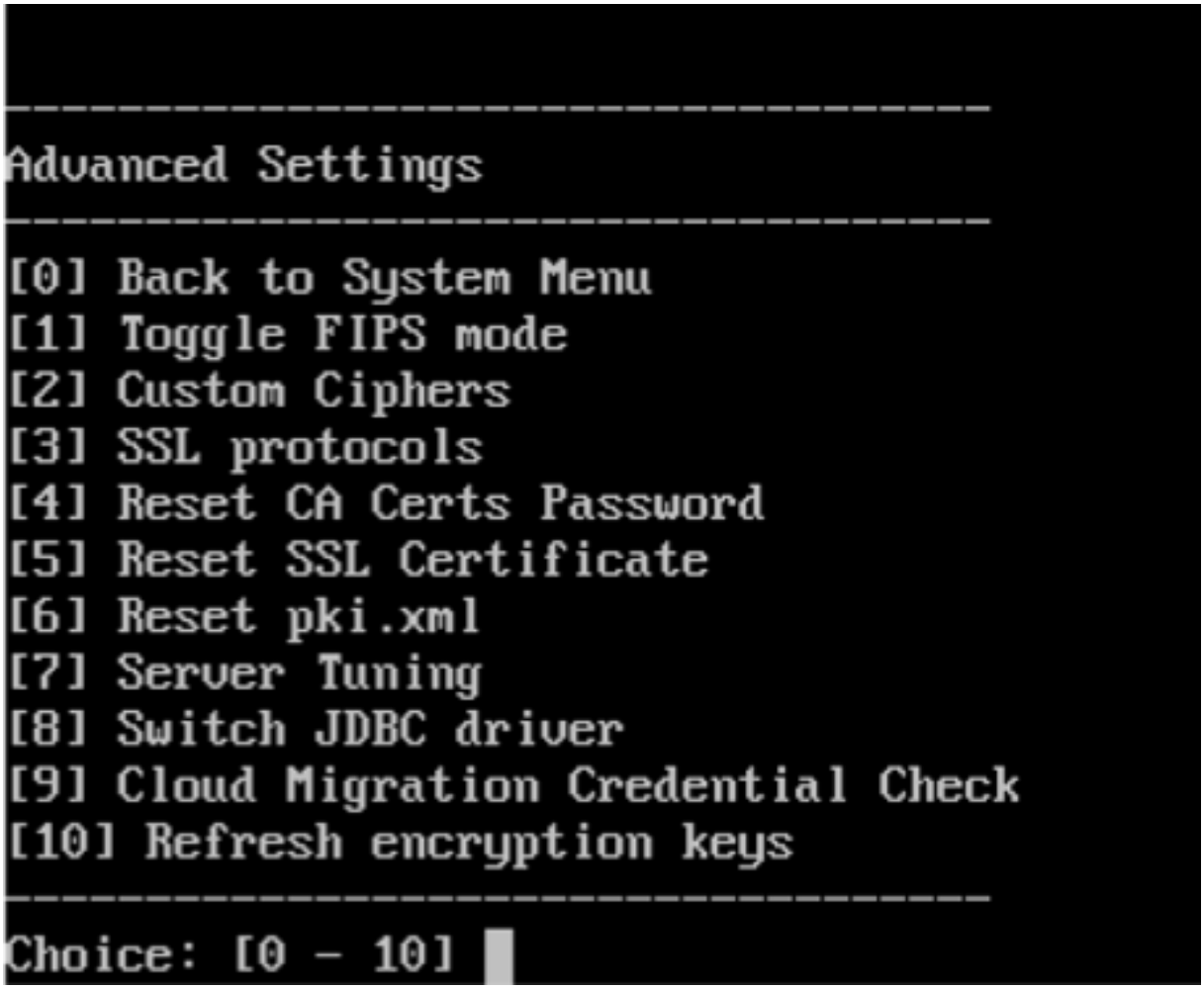
Conditions préalables

- Par défaut, cette fonctionnalité d'actualisation de certificat est désactivée. Pour activer les fonctionnalités d'actualisation de certificat, définissez la valeur de la propriété du serveur **refresh.internal.ca** sur **True**.

> **Important :**
>
> Si Citrix ADC est configuré pour la décharge SSL, lorsque vous générez un nouveau certificat, assurez-vous de mettre à jour l'équilibrage de charge avec le nouveau certificat cacert.perm. Pour plus d'informations sur la configuration de Citrix Gateway, consultez Pour utiliser le mode de déchargement SSL pour les VIP Citrix ADC.

Option CLI pour réinitialiser le mot de passe du certificat de l'autorité de certification du serveur pour les nœuds de cluster

Une fois que vous avez généré un certificat d'autorité de certification de serveur sur un nœud XenMobile Server, utilisez la CLI XenMobile pour réinitialiser le mot de passe du certificat sur les autres nœuds de cluster. Dans le menu principal de la CLI, sélectionnez **Système > Paramètres avancés > Réinitialiser le mot de passe du certificat CA**. Si vous réinitialisez le mot de passe alors qu'il n'y a pas de nouveau certificat CA, XenMobile ne réinitialise pas le mot de passe.



Gestion des certificats XenMobile

Nous vous recommandons de répertorier les certificats que vous utilisez dans votre déploiement XenMobile, plus particulièrement leurs dates d'expiration et les mots de passe associés. Cette section vise à vous aider à faciliter la gestion des certificats dans XenMobile.

Votre environnement peut inclure certains ou tous les certificats suivants :

- XenMobile Server
  - Certificat SSL pour nom de domaine complet MDM
  - Certificat SAML (pour Citrix Files)

  - Certificats d'autorité de certification racine et intermédiaire pour les certificats ci-dessus et toute autre ressource interne (StoreFront/Proxy, etc)
  - Certificat APN pour la gestion des appareils iOS
  - Certificat APNS interne pour les notifications Secure Hub de XenMobile Server
  - Certificat utilisateur PKI pour la connectivité à PKI

- MDX Toolkit

  - Certificat Apple Developer
  - Profil de provisioning Apple (par application)
  - Certificat APNs Apple (pour utilisation avec Citrix Secure Mail)
  - Fichier de keystore Android
  - Windows Phone – Certificat DigiCert

  Le SDK MAM n'encapsulant pas les applications, il ne nécessite donc pas de certificat.

- Citrix ADC

  - Certificat SSL pour nom de domaine complet MDM
  - Certificat SSL pour nom de domaine complet Gateway
  - Certificat SSL pour nom de domaine complet ShareFile SZC
  - Certificat SSL pour l'équilibrage de charge Exchange (configuration de déchargement)
  - Certificat SSL pour l'équilibrage de charge StoreFront
  - Certificats d'autorité de certification racine et intermédiaire pour les certificats ci-dessus

Stratégie d'expiration de certificat XenMobile

Si vous autorisez un certificat à expirer, le certificat n'est plus valide. Vous ne pouvez plus exécuter de transactions sécurisées dans votre environnement et vous ne pouvez pas accéder aux ressources XenMobile.

> **Remarque :**
>
> L'autorité de certification (CA) vous invite à renouveler votre certificat SSL avant la date d'expiration.

Certificat APNS pour Citrix Secure Mail

Certificats Apple Push Notification Service (APNs) Veillez à créer un certificat SSL APNs et à le mettre à jour dans le portail Citrix avant l'expiration du certificat. Si le certificat expire, les utilisateurs rencontrent des problèmes avec les notifications push Secure Mail. De plus, vous ne pouvez plus envoyer de notifications push pour vos applications.

Certificat APNS pour la gestion des appareils iOS

Pour inscrire et gérer des appareils iOS avec XenMobile, configurez et créez un certificat APNS Apple. Si le certificat expire, les utilisateurs ne peuvent pas s'inscrire dans XenMobile et vous ne pouvez pas gérer leurs appareils iOS. Pour plus d'informations, consultez la section Certificats APNS.

Vous pouvez afficher l'état et la date d'expiration du certificat APNs en ouvrant une session sur le portail de certificats push Apple. Veillez à ouvrir une session avec les informations de l'utilisateur qui a créé le certificat.

Vous recevez également une notification par e-mail d'Apple 30 et 10 jours avant la date d'expiration. La notification inclut les informations suivantes :

```
1 The following Apple Push Notification Service certificate, created for
     Apple ID CustomerID will expire on Date. Revoking or allowing this
     certificate to expire will require existing devices to be re-
     enrolled with a new push certificate.
2
3 Please contact your vendor to generate a new request (a signed CSR),
     then visit https://identity.apple.com/pushcert to renew your Apple
     Push Notification Service certificate.
4
5 Thank You,
6
7 Apple Push Notification Service
8 <!--NeedCopy-->
```

MDX Toolkit (certificat de distribution iOS)

Toute application exécutée sur un appareil iOS physique (autres que des applications dans l'App Store d'Apple) présente les exigences de signature suivantes :

- Signer l'application avec un profil de provisioning.
- Signer l'application avec un certificat de distribution correspondant.

Pour vérifier que vous disposez d'un certificat de distribution iOS valide, procédez comme suit :

1. À partir du portail Apple Enterprise Developer, créez un ID d'application explicite pour chaque application que vous voulez encapsuler avec le MDX Toolkit. Exemple d'ID d'application acceptable : `com.CompanyName.ProductName`.
2. À partir du portail Apple Enterprise Developer, accédez à **Provisioning Profiles > Distribution** et créez un profil de provisioning interne. Répétez cette étape pour chaque ID d'application créé à l'étape précédente.
3. Téléchargez tous les profils de provisioning. Pour plus d'informations, consultez la section Encapsulation des applications mobiles iOS.

Pour vérifier si tous les certificats de XenMobile Server sont valides, procédez comme suit :

1. Dans la console XenMobile, cliquez sur **Paramètres > Certificats**.
2. Assurez-vous que tous les certificats y compris les certificats APNs, d'écoute SSL, racine et intermédiaire sont valides.

Keystore Android

Le keystore est un fichier qui contient les certificats utilisés pour signer votre application Android. Lorsque la période de validité de votre clé expire, les utilisateurs ne peuvent plus mettre à niveau vers les nouvelles versions de votre application.

Certificat d'entreprise de DigiCert pour Windows Phone

DigiCert est le fournisseur exclusif de certificats de signature de code du service Microsoft App Hub. Les développeurs et éditeurs de logiciels rejoignent le hub d'applications pour distribuer des applications Windows Phone et Xbox 360 à télécharger à l'aide de Windows Marketplace. Pour de plus amples informations, consultez la section DigiCert Code Signing Certificates for Windows Phone dans la documentation DigiCert.

Si le certificat expire, les utilisateurs de Windows Phone ne peuvent pas s'inscrire. Les utilisateurs ne peuvent pas installer une application publiée et signée par l'entreprise ou démarrer une application d'entreprise qui a été installée sur le téléphone.

Citrix ADC

Pour plus d'informations sur la gestion de l'expiration de certificat pour Citrix ADC, consultez la section How to handle certificate expiry on NetScaler dans le centre de connaissances Citrix.

Un certificat Citrix ADC ayant expiré empêche les utilisateurs de s'inscrire et d'accéder au magasin. Le certificat expiré empêche également les utilisateurs de se connecter à Exchange Server lors de l'utilisation de Secure Mail. En outre, les utilisateurs ne peuvent pas énumérer ni ouvrir les applications HDX (en fonction de quel certificat a expiré).

Le Moniteur d'expiration et Command Center peuvent vous aider à effectuer le suivi de vos certificats Citrix ADC. Le Command Center vous informe de l'expiration du certificat. Ces outils permettent de surveiller les certificats Citrix ADC suivants :

- Certificat SSL pour nom de domaine complet MDM
- Certificat SSL pour nom de domaine complet Gateway
- Certificat SSL pour nom de domaine complet ShareFile SZC
- Certificat SSL pour l'équilibrage de charge Exchange (configuration de déchargement)
- Certificat SSL pour l'équilibrage de charge StoreFront

- Certificats d'autorité de certification racine et intermédiaire pour les certificats ci-dessus

Citrix Gateway et XenMobile

January 10, 2022

Lorsque vous configurez Citrix Gateway à l'aide de XenMobile, vous établissez le mécanisme d'authentification utilisé par les appareils distants pour accéder au réseau interne. Cette fonctionnalité permet aux applications sur un appareil mobile d'accéder à des serveurs d'entreprise situés dans l'intranet. XenMobile crée un micro VPN depuis les applications vers Citrix Gateway sur l'appareil.

Vous configurez Citrix Gateway pour une utilisation avec XenMobile en exportant un script depuis XenMobile que vous exécutez sur Citrix Gateway.

Conditions préalables à l'utilisation du script de configuration de Citrix Gateway

Configuration requise pour Citrix ADC :

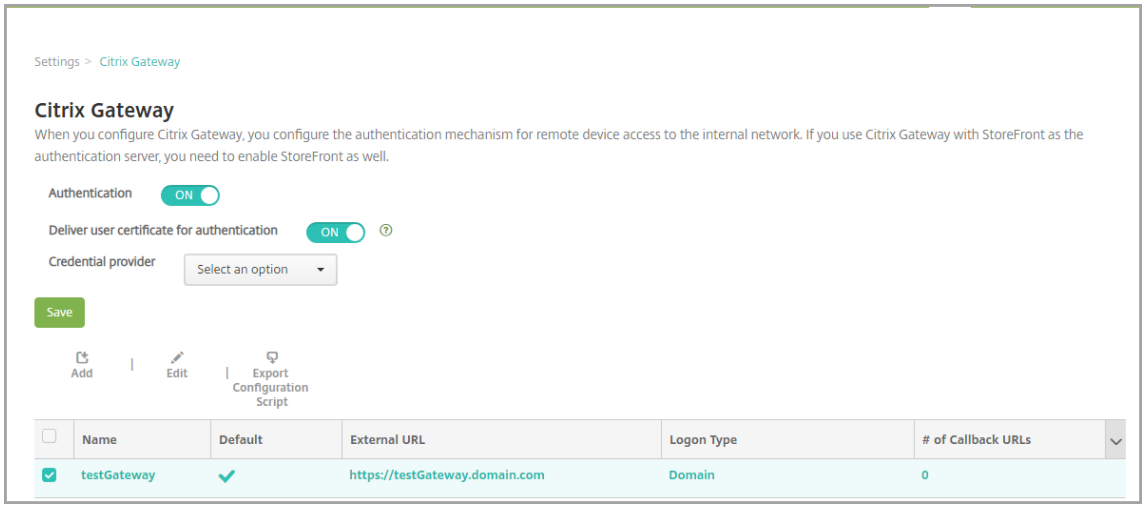
- Citrix ADC (version minimale 11.0, Build 70.12).
- L'adresse IP Citrix ADC est configurée et peut se connecter au serveur LDAP, à moins d'un équilibrage de charge de LDAP.
- L'adresse IP de sous-réseau de Citrix ADC (SNIP) est configurée, peut se connecter aux serveurs back-end nécessaires et dispose d'un accès réseau public sur le port 8443/TCP.
- DNS peut résoudre les domaines publics.
- Citrix ADC est utilisé sous licence Platform/Universal ou d'évaluation. Pour de plus amples informations, consultez https://support.citrix.com/article/CTX126049.
- Un certificat SSL de Citrix Gateway est téléchargé et installé sur Citrix ADC. Pour plus d'informations, veuillez consulter la section https://support.citrix.com/article/CTX136023.

Configuration requise pour XenMobile :

- XenMobile Server (version minimum 10.6).
- Serveur LDAP configuré.

Configurer l'authentification pour un accès à distance au réseau interne

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Serveur**, cliquez sur **Citrix Gateway**. La page **Citrix Gateway** s'affiche. Dans l'exemple suivant, il existe une instance Citrix Gateway.

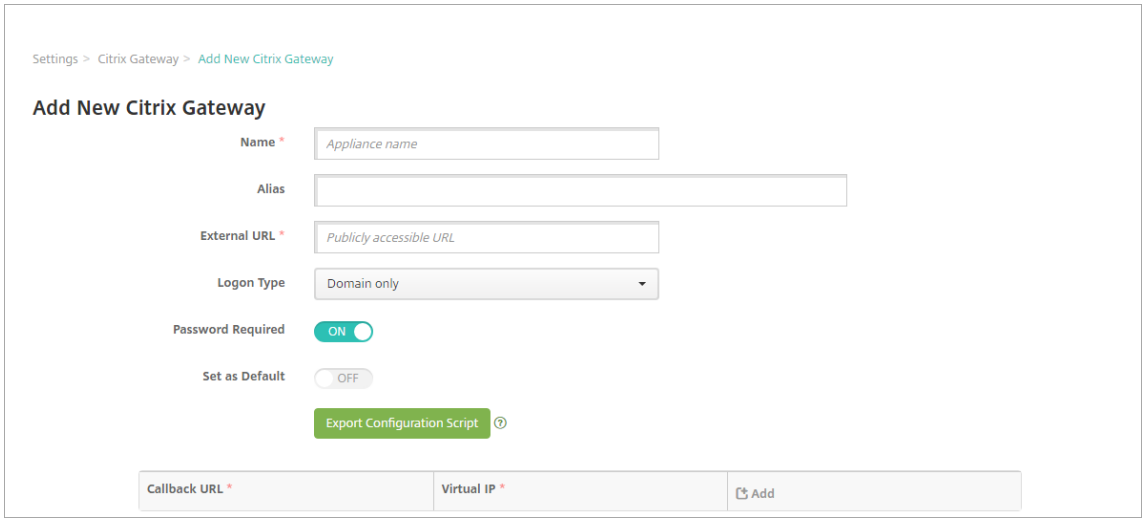


3. Pour configurer ces paramètres :
   - **Authentification :** sélectionnez cette option pour activer l'authentification. La valeur par défaut est **Activé**.
   - **Délivrer un certificat utilisateur pour l'authentification :** indiquez si vous voulez que XenMobile partage le certificat d'authentification avec Secure Hub afin que Citrix Gateway gère l'authentification du certificat client. La valeur par défaut est **Désactivé.**
   - **Fournisseur d'identités :** dans la liste, cliquez sur le fournisseur d'identités. Pour de plus amples informations, consultez la section Fournisseurs d'identités.
4. Cliquez sur **Enregistrer**.

Ajouter une instance Citrix Gateway

Après avoir enregistré les paramètres d'authentification, vous ajoutez une instance Citrix Gateway à XenMobile.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'ouvre.
2. Sous **Serveur**, cliquez sur **Citrix Gateway**. La page **Citrix Gateway** s'affiche.
3. Cliquez sur **Ajouter**. La page **Ajouter Citrix Gateway** apparaît.



4. Pour configurer ces paramètres :

   - **Nom :** entrez un nom pour l'instance Citrix Gateway.
   - **Alias :** si vous le souhaitez, vous pouvez inclure un alias pour Citrix Gateway.
   - **URL externe :** entrez l'adresse URL publiquement accessible de Citrix Gateway. Par exemple, `https://receiver.com`.
   - **Type d'ouverture de session :** choisissez un type d'ouverture de session. Les types disponibles sont les suivants : **Domaine uniquement**, **Jeton de sécurité uniquement**, **Domaine et jeton de sécurité**, **Certificat**, **Certificat et domaine** et **Certificat et jeton de sécurité**. La valeur par défaut pour le champ **Mot de passe requis** change selon le **Type d'ouverture de session** sélectionné. La valeur par défaut est **Domaine uniquement**.

   Si vous disposez de plusieurs domaines, utilisez **Certificat et domaine**. Pour plus d'informations sur la configuration de l'authentification multi-domaines avec XenMobile et Citrix Gateway, consultez la section Configuration de l'authentification multi-domaines.

   Si vous utilisez **Certificat et jeton de sécurité**, une configuration supplémentaire est requise sur Citrix Gateway pour la prise en charge de Secure Hub. Pour de plus amples informations, consultez la section Configuration de XenMobile pour l'authentification par certificat et jeton de sécurité.

   Pour plus d'informations, consultez la section Authentification dans le manuel de déploiement.

   - **Mot de passe requis :** indiquez si vous souhaitez demander l'authentification par mot de passe. La valeur par défaut varie selon le **Type d'ouverture de session** choisi.
   - **Définir par défaut :** indiquez si cette passerelle Citrix Gateway doit être utilisée par défaut. La valeur par défaut est **Désactivé.**
   - **Exporter le script de configuration :** cliquez sur le bouton pour exporter un bundle de configuration que vous chargerez sur Citrix Gateway pour le configurer avec les paramètres de XenMobile. Pour plus d'informations, consultez « Configurer une instance

Citrix Gateway locale à utiliser avec XenMobile Server » après cette procédure.

- **URL de rappel** et **Adresse IP virtuelle :** enregistrez vos paramètres avant d'ajouter ces champs. Pour plus d'informations, consultez la section Ajouter une URL de rappel et une adresse IP virtuelle de VPN Citrix Gateway dans cet article.

5. Cliquez sur **Enregistrer**.

   La nouvelle passerelle Citrix Gateway est ajoutée et s'affiche dans le tableau. Pour modifier ou supprimer une instance, cliquez sur le nom dans la liste.

Configurer une instance Citrix Gateway à utiliser avec XenMobile Server

Pour configurer une instance Citrix Gateway locale pour une utilisation avec XenMobile, vous devez effectuer les étapes générales suivantes, détaillées dans cet article :

1. Téléchargez un script et les fichiers associés depuis XenMobile Server. Pour plus d'informations, consultez le fichier Lisez-moi accompagnant le script pour accéder aux instructions détaillées les plus récentes.
2. Vérifiez que votre environnement répond à la configuration requise.
3. Mettez à jour le script pour votre environnement.
4. Exécutez le script sur Citrix ADC.
5. Testez la configuration.

Le script configure les paramètres Citrix Gateway suivants requis par XenMobile :

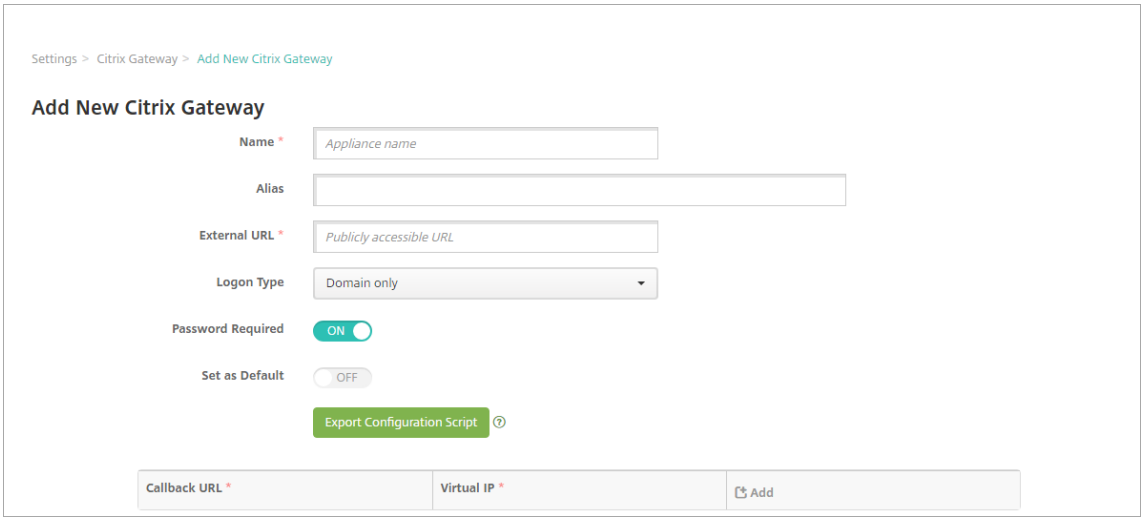
- Serveurs virtuels Citrix Gateway requis pour le mode MDM et MAM
- Stratégies de session pour les serveurs virtuels Citrix Gateway
- Détails XenMobile Server
- Stratégies d'authentification et Actions pour le serveur virtuel Citrix Gateway. Le script décrit les paramètres de configuration LDAP.
- Actions et stratégies de trafic pour le serveur proxy
- Profil d'accès sans client
- Enregistrement DNS local statique sur Citrix ADC
- Autres liaisons : stratégie de service, certificat d'autorité de certification

Le script ne prend pas en charge la configuration suivante :

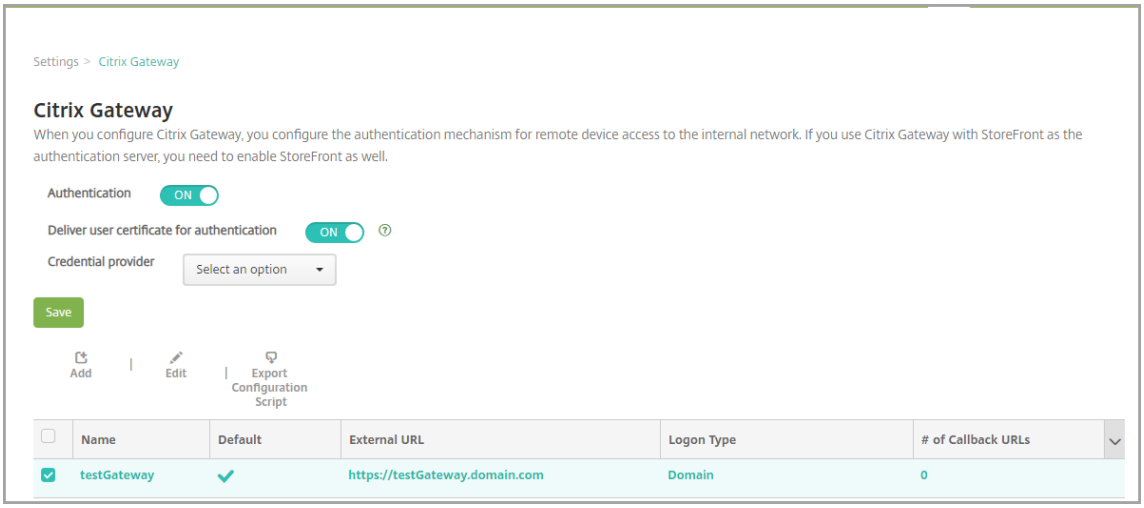
- Équilibrage de charge Exchange
- Equilibrage de charge Citrix Files
- Configuration du proxy ICA
- Déchargement SSL

Pour télécharger, mettre à jour et exécuter le script

1. Si vous ajoutez Citrix Gateway, cliquez sur **Exporter le script de configuration** sur la page **Ajouter nouveau Citrix Gateway**.



Ou, si vous ajoutez une instance Citrix Gateway et cliquez sur **Enregistrer** avant d'exporter le script : revenez à **Paramètres > Citrix Gateway**, sélectionnez Citrix ADC, cliquez sur **Exporter le script de configuration**, puis cliquez sur **Télécharger**.

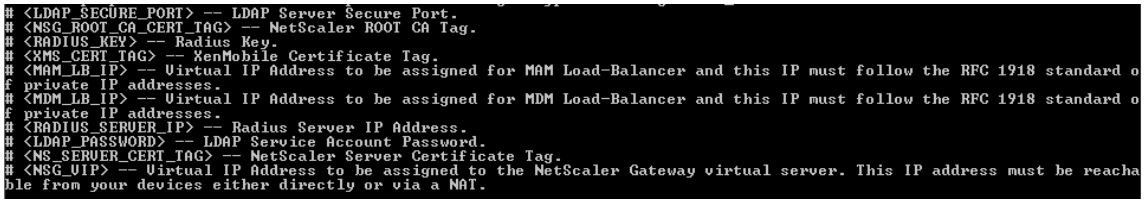


Après avoir cliqué sur **Exporter le script de configuration**, XenMobile crée un bundle de script tar.gz. Le bundle de script inclut les éléments suivants :

- Fichier Lisez-moi avec instructions détaillées
- Script contenant les commandes d'interface de ligne de commande Citrix ADC permettant de configurer les composants requis dans Citrix ADC
- Certificat d'autorité de certification racine public et certificat d'autorité de certification intermédiaire de XenMobile Server (ces certificats, pour le déchargement SSL, ne sont pas nécessaires pour la version actuelle)

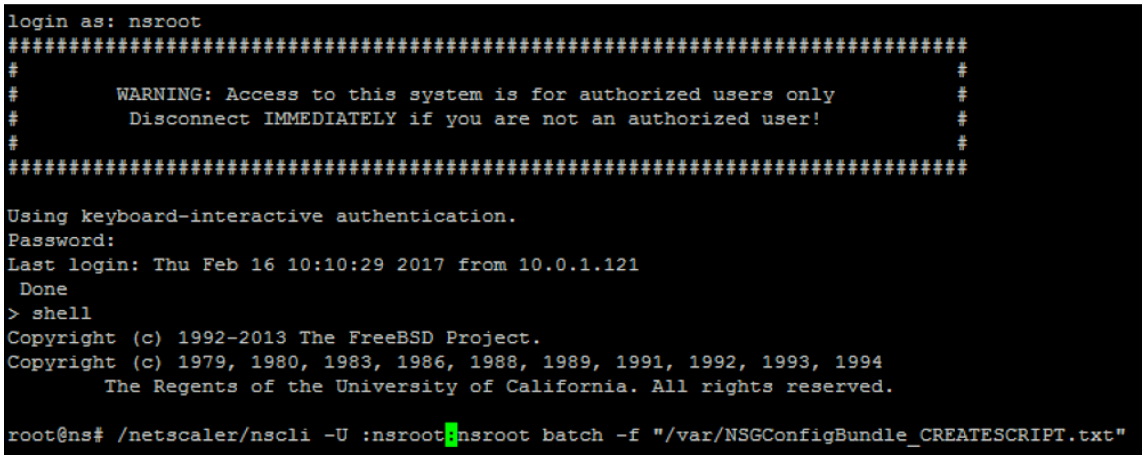
- Script contenant les commandes d'interface de ligne de commande Citrix ADC permettant de supprimer la configuration de Citrix ADC

2. Modifiez le script (NSGConfigBundle_CREATESCRIPT.txt) en remplaçant tous les espaces réservés avec les détails de votre environnement.

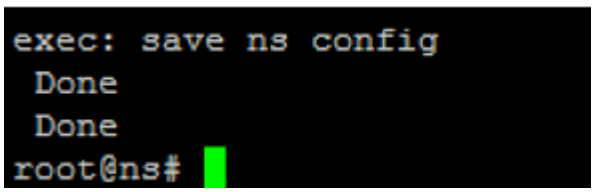


3. Exécutez le script modifié dans le shell bash Citrix ADC, comme décrit dans le fichier Lisez-moi accompagnant le bundle de script. Par exemple :

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management
 Password> batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

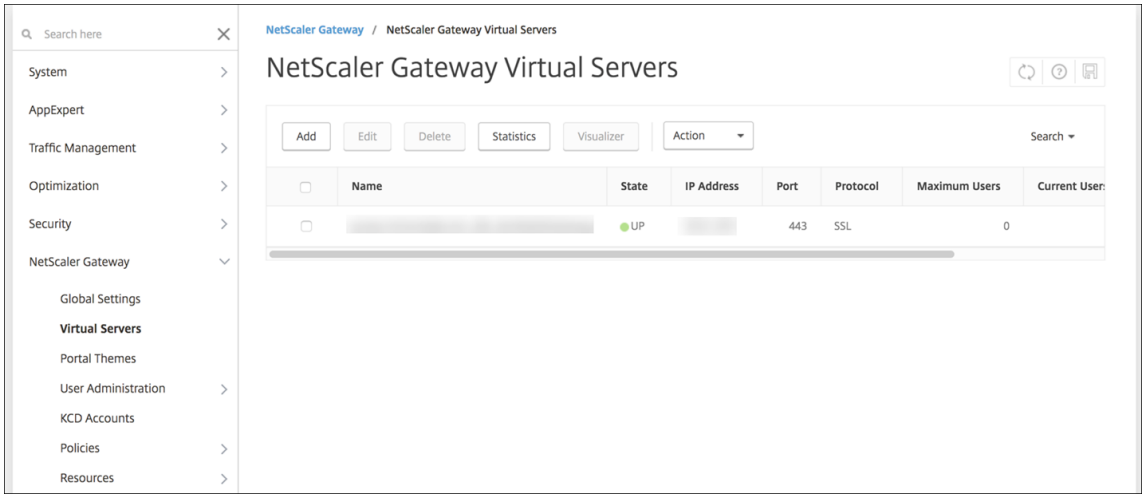


Lorsque le script prend fin, les lignes suivantes s'affichent.

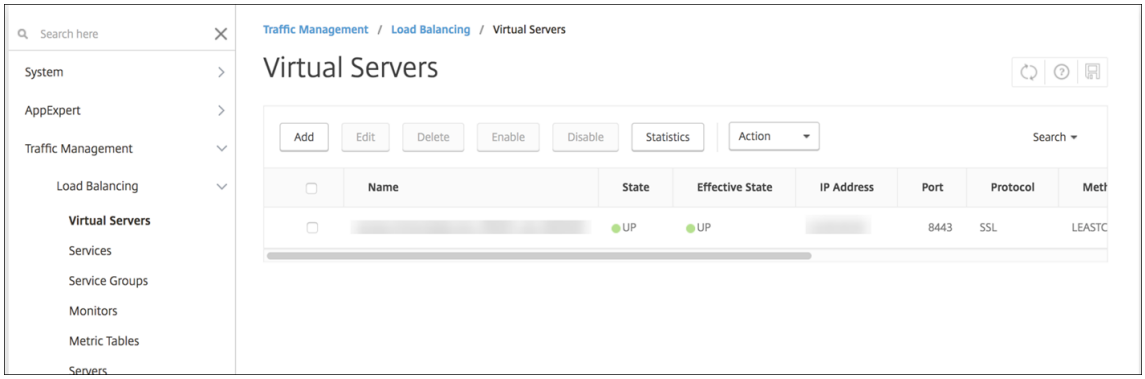


Tester la configuration

1. Vérifiez que le serveur virtuel Citrix Gateway affiche un état **Actif**.



2. Vérifiez que le serveur virtuel d'équilibrage de charge du proxy indique un état **Actif**.



3. Ouvrez un navigateur Web, connectez-vous à l'adresse URL de Citrix Gateway et essayez de vous authentifier. Si l'authentification échoue, ce message s'affiche : État HTTP 404 - introuvable
4. Inscrivez un appareil et assurez-vous qu'il est inscrit auprès de MDM et MAM.

Ajouter une URL de rappel et une adresse IP virtuelle de VPN Citrix Gateway

Après avoir ajouté l'instance Citrix Gateway, vous pouvez ajouter une adresse URL de rappel et spécifier l'adresse IP virtuelle d'une appliance Citrix Gateway. Ces paramètres sont facultatifs, mais peut être configurée pour plus de sécurité, plus particulièrement lorsque XenMobile Server est dans la DMZ.

1. Dans **Paramètres > Citrix Gateway**, sélectionnez l'instance NetScaler Gateway et cliquez sur **Modifier**.
2. Dans le tableau, cliquez sur **Ajouter**.
3. Pour **URL de rappel**, entrez le nom de domaine complet. L'URL de rappel vérifie que la demande provient de Citrix Gateway.

   Assurez-vous que l'URL de rappel devient une adresse IP qui est accessible à partir de XenMobile Server. L'URL de rappel peut être une URL Citrix Gateway externe ou d'autres URL.

4. Entrez l'**adresse IP virtuelle** Citrix Gateway et cliquez sur **Enregistrer**.

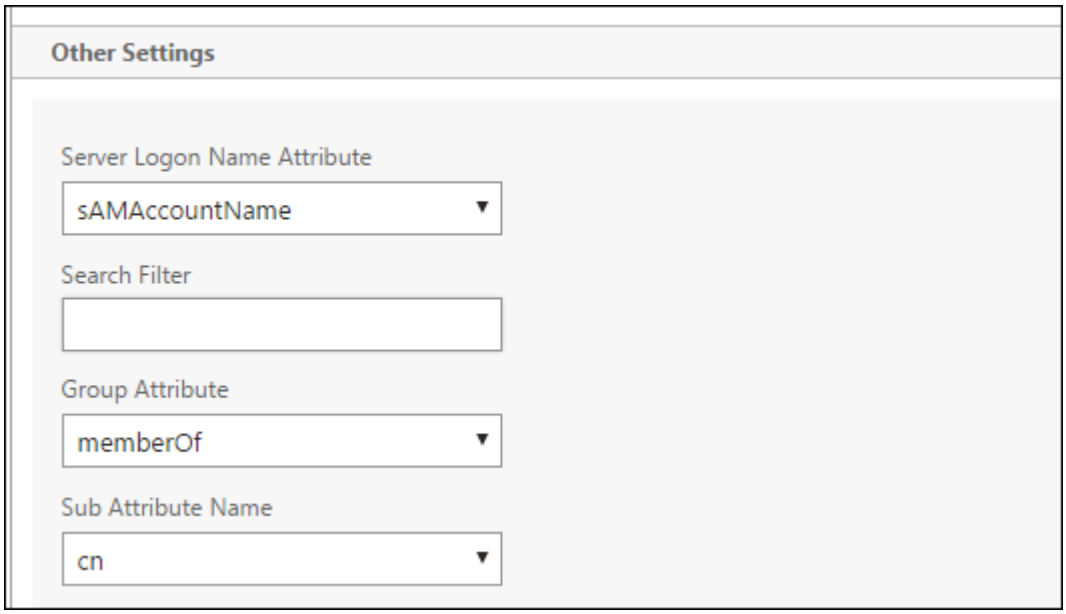
Configuration de l'authentification multi-domaines

Si vous disposez de plusieurs instances XenMobile Server, telles que les environnements de test, de développement et de production, configurez manuellement Citrix Gateway pour les environnements supplémentaires. (Vous ne pouvez exécuter l'assistant Citrix ADC for XenMobile qu'une seule fois.)

Configuration de Citrix Gateway

Pour configurer les stratégies d'authentification Citrix Gateway et une stratégie de session pour un environnement multi-domaine :

1. Dans l'onglet **Configuration** de l'outil de configuration Citrix Gateway, développez **Citrix Gateway > Policies > Authentication**.
2. Dans le panneau de navigation, cliquez sur **LDAP**.
3. Cliquez pour modifier le profil LDAP. Définissez **Server Logon Name Attribute** sur **userPrincipalName** ou sur l'attribut que vous souhaitez utiliser pour vos recherches. Prenez note de l'attribut que vous spécifiez pour en disposer lors de la configuration des paramètres LDAP dans la console XenMobile.

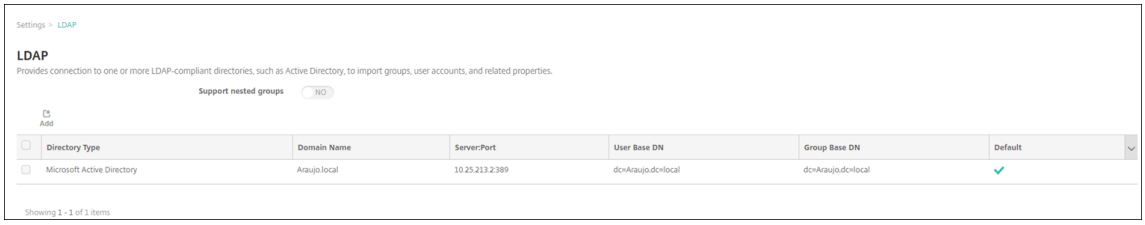


4. Répétez ces étapes pour chaque stratégie LDAP. Une stratégie LDAP distincte est requise pour chaque domaine.
5. Dans la stratégie de session liée au serveur virtuel Citrix Gateway, accédez à **Edit session profile > Published Applications**. Assurez-vous que le champ **Single Sign-On Domain** est vide.

Configuration de XenMobile Server

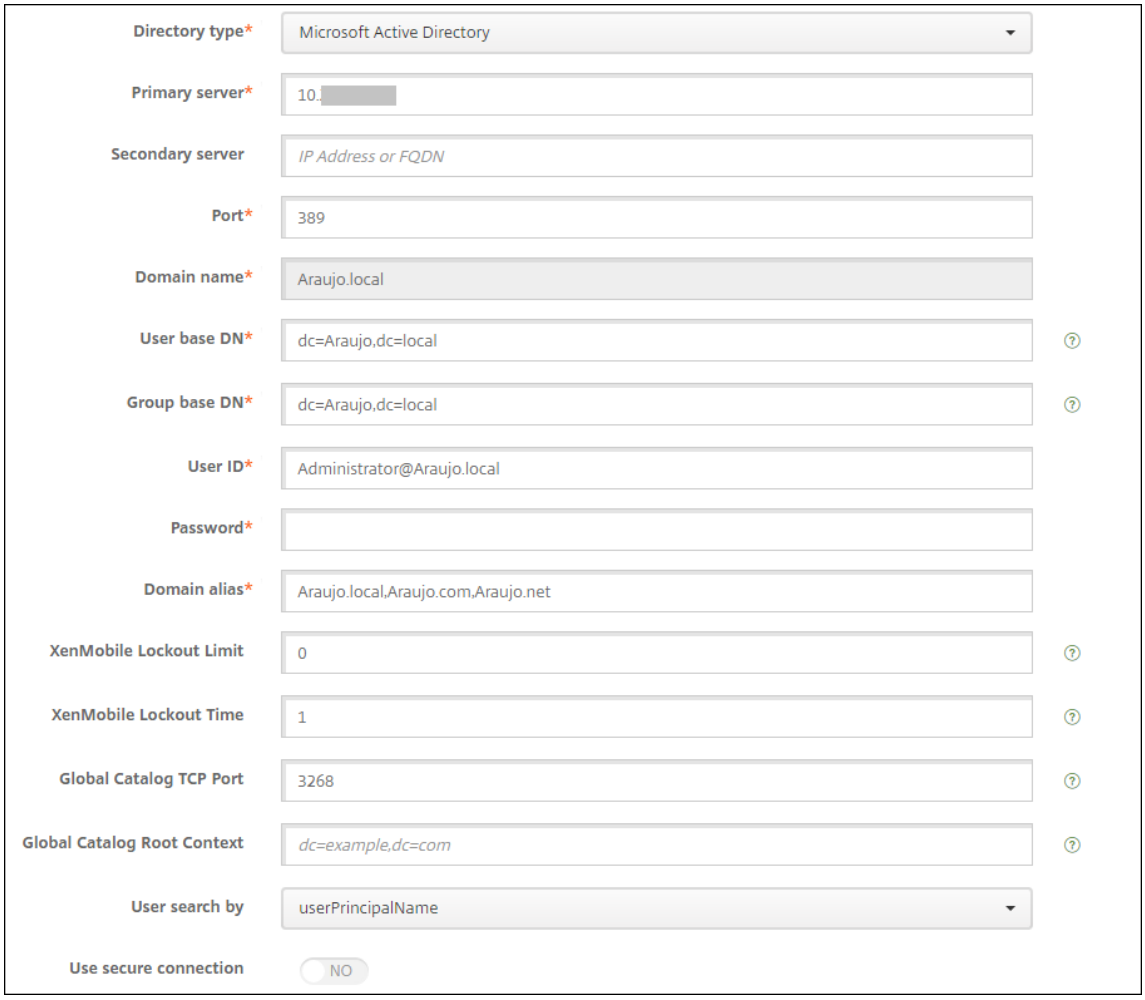
Pour configurer LDAP pour un environnement XenMobile multi-domaine :

1. Dans la console XenMobile, accédez à **Settings > LDAP** et ajoutez ou modifiez un répertoire.



2. Entrez les informations.

   - Sous **Alias de domaine**, spécifiez chaque domaine à utiliser pour l'authentification utilisateur. Séparez les domaines avec une virgule et n'insérez pas d'espaces entre les domaines. Pa exemple : `domain1.com,domain2.com,domain3.com`
   - Assurez-vous que le champ **User search by** correspond à l'attribut **Server Logon Name Attribute** spécifié dans la stratégie LDAP Citrix Gateway.



Supprimer les demandes de connexion entrante vers des adresses URL spécifiques

Dans votre environnement, si Citrix Gateway est configuré pour le déchargement SSL, vous pouvez souhaiter que la passerelle supprime les demandes de connexion entrante pour des adresses URL spécifiques.

Si vous souhaitez ajouter cette sécurité supplémentaire, configurez les deux serveurs virtuels d'équilibrage de charge MDM (un pour le port 443 et un pour le port 8443) sur Citrix Gateway. Utilisez les informations suivantes comme modèle pour vos paramètres.

> **Important :**
>
> Les mises à jour suivantes concernent uniquement une instance Citrix Gateway configurée pour le déchargement SSL.

1. Créez une séquence de modèles et nommez-la `XMS_DropURLs`.

```
add policy patset XMS_DropURLs
<!--NeedCopy-->
```

2. Ajoutez les adresses URL suivantes à la nouvelle séquence de modèles. Personnalisez cette liste si nécessaire.

```
bind policy patset XMS_DropURLs /zdm/shp/console -index 6

bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5

bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4

bind policy patset XMS_DropURLs /zdm/log.jsp -index 3

bind policy patset XMS_DropURLs /zdm/login.jsp -index 2

bind policy patset XMS_DropURLs /zdm/console -index 1
<!--NeedCopy-->
```

3. Créez une stratégie pour supprimer tout le trafic vers ces adresses URL, sauf si la demande de connexion provient du sous-réseau spécifié.

```
add responder policy XMS_DROP_pol  “CLIENT.IP.SRC.IN_SUBNET
    (192.168.0.0/24).NOT &&
HTTP.REQ.URL.CONTAINS_ANY(” XMS_DropURLs” )”  DROP -comment "Allow
     only subnet 192.168.0.0/24 to access these URLs. All other
    connections are DROPed"
<!--NeedCopy-->
```


4. Liez la nouvelle stratégie aux deux serveurs virtuels d'équilibrage de charge MDM (ports 443 et 8443).

```
1 bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName
    XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
    REQUEST
2
3 bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName
    XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
    REQUEST
4 <!--NeedCopy-->
```

Authentification domaine ou domaine + jeton de sécurité

March 2, 2021

XenMobile prend en charge l'authentification basée sur domaine auprès d'un ou plusieurs annuaires, qui sont compatibles avec le protocole LDAP (Lightweight Directory Access Protocol). Dans XenMobile, vous pouvez configurer une connexion à un ou plusieurs annuaires, puis utiliser la configuration LDAP pour importer des groupes, des comptes utilisateur et les propriétés correspondantes.

LDAP est un protocole applicatif indépendant open source qui permet d'accéder et de gérer les services d'informations d'annuaire distribués sur un réseau IP (Internet Protocol). Les services d'informations d'annuaire sont utilisés pour partager des informations sur les utilisateurs, les systèmes, les réseaux, les services et les applications disponibles sur le réseau.

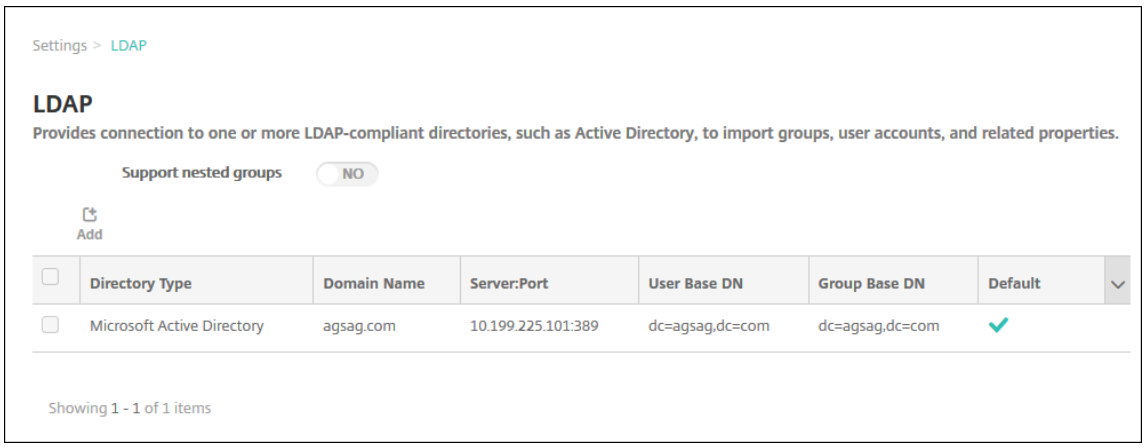
LDAP est couramment utilisé pour fournir une authentification unique (SSO) aux utilisateurs, avec laquelle un seul mot de passe (par utilisateur) est partagé entre plusieurs services. L'authentification unique permet à un utilisateur de se connecter une seule fois au site Web d'une entreprise, pour un accès authentifié à l'intranet de l'entreprise.

Un client démarre une session LDAP en se connectant à un serveur LDAP, appelé DSA (Agent système d'annuaire). Le client envoie une demande d'opération au serveur et le serveur répond avec l'authentification appropriée.

> **Important :**
>
> XenMobile ne prend pas en charge le passage du mode d'authentification, de l'authentification de domaine à un autre mode d'authentification, après que les utilisateurs ont inscrit des appareils dans XenMobile.

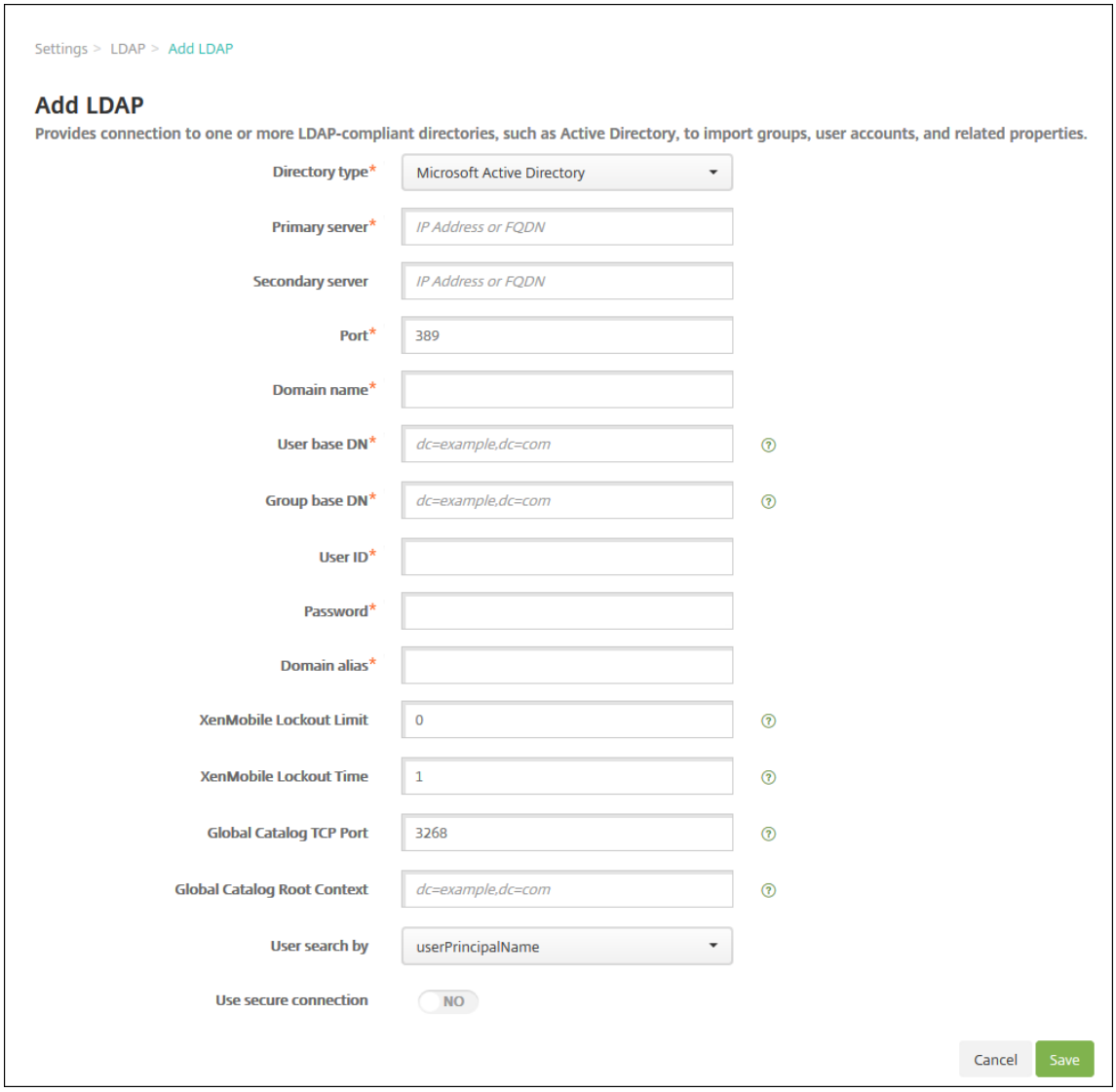
Pour ajouter des connexions LDAP dans XenMobile

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Serveur**, cliquez sur **LDAP**. La page **LDAP** s'affiche. Vous pouvez ajouter, modifier ou supprimer des annuaires compatibles LDAP comme décrit dans cet article.



Pour ajouter un annuaire compatible LDAP

1. Sur la page **LDAP**, cliquez sur **Ajouter**. La page **Ajouter LDAP** s'affiche.



2. Pour configurer ces paramètres :

   - **Type d'annuaire :** dans la liste, cliquez sur le type d'annuaire approprié. La valeur par défaut est **Microsoft Active Directory**.
   - **Serveur principal :** entrez le serveur principal utilisé pour LDAP ; vous pouvez entrer l'adresse IP ou le nom de domaine complet (FQDN).
   - **Serveur secondaire :** éventuellement, si un serveur secondaire a été configuré, entrez l'adresse IP ou le nom de domaine complet du serveur secondaire. Ce serveur est un serveur de basculement utilisé au cas où le serveur principal ne peut pas être contacté.
   - **Port :** entrez le numéro du port utilisé par le serveur LDAP. Par défaut, le numéro de port est défini sur **389** pour les connexions LDAP non sécurisées. Utilisez le numéro de port **636** pour les connexions LDAP sécurisées, **3268** pour les connexions LDAP non sécurisées Microsoft, ou **3269** pour les connexions LDAP sécurisées Microsoft.
   - **Nom de domaine :** entrez le nom du domaine.

- **Nom unique de l'utilisateur de base :** entrez l'emplacement des utilisateurs dans Active Directory à l'aide d'un identificateur unique. Exemples de syntaxe : `ou=users`, `dc=example` ou `dc=com`.
- **Nom unique du groupe de base :** entrez l'emplacement des groupes dans Active Directory. Par exemple, `cn=users, dc=domain, dc=net` où `cn=users` représente le nom de conteneur des groupes et `dc` représente le composant de domaine d'Active Directory.
- **ID utilisateur :** entrez l'ID de l'utilisateur associé au compte Active Directory.
- **Mot de passe :** entrez le mot de passe associé à l'utilisateur.
- **Alias de domaine :** entrez un alias pour le nom de domaine. Si vous modifiez le paramètre **Alias de domaine** après l'inscription, les utilisateurs doivent s'inscrire à nouveau.
- **Limite de verrouillage de XenMobile :** entrez un nombre compris entre **0** et **999** pour le nombre d'échecs de tentatives d'ouverture de session. Si ce champ est défini sur **0**, XenMobile ne verrouillera jamais l'utilisateur quel que soit le nombre de tentatives d'ouverture de session infructueuses.
- **Durée de verrouillage de XenMobile :** entrez un nombre compris entre **0** et **99 999** représentant le nombre de minutes pendant lesquelles un utilisateur doit patienter après avoir dépassé la limite de verrouillage. Une valeur de **0** signifie que l'utilisateur n'est pas forcé d'attendre après un verrouillage.
- **Port TCP du catalogue global :** entrez le numéro de port TCP du serveur du catalogue global. Par défaut, le numéro de port TCP est défini sur **3268** ; pour les connexions SSL, utilisez le numéro de port **3269**.
- **Base de recherche du catalogue global :** si vous le souhaitez, entrez la valeur de base de recherche globale utilisée pour activer une recherche du catalogue global dans Active Directory. Cette recherche est en supplément de la recherche LDAP standard, dans tout domaine sans avoir à spécifier le nom de domaine.
- **Recherche utilisateur par :** dans la liste, cliquez sur **userPrincipalName** ou **sAMAccountName**. La valeur par défaut est **userPrincipalName**. Si vous modifiez le paramètre **Rechercher utilisateurs par** après l'inscription, les utilisateurs doivent s'inscrire à nouveau.
- **Utiliser une connexion sécurisée :** indiquez si des connexions sécurisées doivent être utilisées. La valeur par défaut est **Non**.

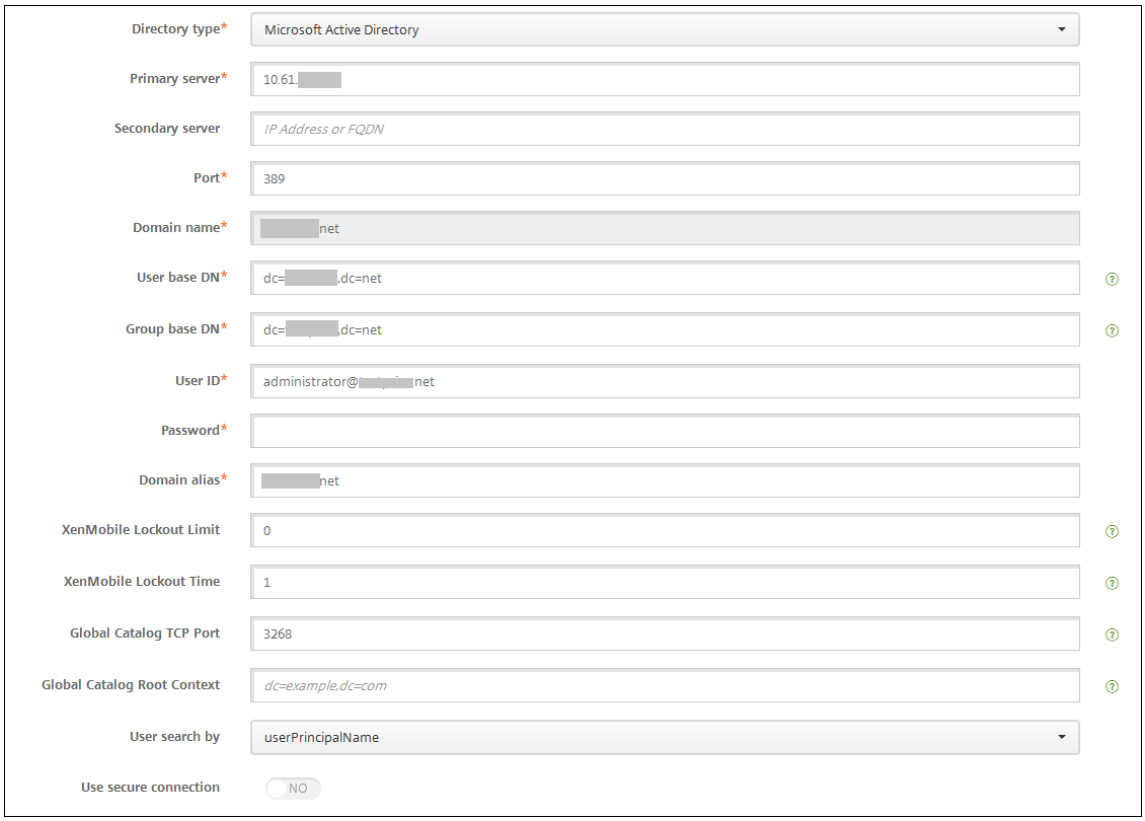
3. Cliquez sur **Enregistrer**.

Pour modifier un annuaire compatible LDAP

1. Dans le tableau **LDAP**, sélectionnez l'annuaire que vous souhaitez modifier.

   Lorsque vous sélectionnez la case à cocher en regard d'un annuaire, le menu d'options s'affiche au-dessus de la liste LDAP. Cliquez dans la liste et le menu d'options s'affiche sur le côté droit de la liste.

2. Cliquez sur **Modifier**. La page **Modifier LDAP** s'affiche.



3. Modifiez les informations suivantes le cas échéant :

   - **Type d'annuaire :** dans la liste, cliquez sur le type d'annuaire approprié.
   - **Serveur principal :** entrez le serveur principal utilisé pour LDAP ; vous pouvez entrer l'adresse IP ou le nom de domaine complet (FQDN).
   - **Serveur secondaire :** entrez l'adresse IP ou le nom de domaine complet du serveur secondaire (facultatif), si un tel serveur a été configuré.
   - **Port :** entrez le numéro du port utilisé par le serveur LDAP. Par défaut, le numéro de port est défini sur **389** pour les connexions LDAP non sécurisées. Utilisez le numéro de port **636** pour les connexions LDAP sécurisées, **3268** pour les connexions LDAP non sécurisées Microsoft, ou **3269** pour les connexions LDAP sécurisées Microsoft.
   - **Nom de domaine :** vous ne pouvez pas modifier ce champ.
   - **Nom unique de l'utilisateur de base :** entrez l'emplacement des utilisateurs dans Active Directory à l'aide d'un identificateur unique. Exemples de syntaxe : `ou=users`, `dc=example` ou `dc=com`.
   - **Nom unique du groupe de base :** entrez le nom unique du groupe de base spécifié comme `cn=groupname`. Par exemple, `cn=users, dc=servername, dc=net` où `cn=users` est le nom du groupe. `DN` et `servername` représentent le nom du serveur exécutant Active Directory.
   - **ID utilisateur :** entrez l'ID de l'utilisateur associé au compte Active Directory.

- **Mot de passe :** entrez le mot de passe associé à l'utilisateur.
- **Alias de domaine :** entrez un alias pour le nom de domaine. Si vous modifiez le paramètre **Alias de domaine** après l'inscription, les utilisateurs doivent s'inscrire à nouveau.
- **Limite de verrouillage de XenMobile :** entrez un nombre compris entre **0** et **999** pour le nombre d'échecs de tentatives d'ouverture de session. Si ce champ est défini sur **0**, XenMobile ne verrouillera jamais l'utilisateur quel que soit le nombre de tentatives d'ouverture de session infructueuses.
- **Durée de verrouillage de XenMobile :** entrez un nombre compris entre **0** et **99 999** représentant le nombre de minutes pendant lesquelles un utilisateur doit patienter après avoir dépassé la limite de verrouillage. Une valeur de **0** signifie que l'utilisateur n'est pas forcé d'attendre après un verrouillage.
- **Port TCP du catalogue global :** entrez le numéro de port TCP du serveur du catalogue global. Par défaut, le numéro de port TCP est défini sur **3268** ; pour les connexions SSL, utilisez le numéro de port **3269**.
- **Base de recherche du catalogue global :** si vous le souhaitez, entrez la valeur de base de recherche globale utilisée pour activer une recherche du catalogue global dans Active Directory. Cette recherche est en supplément de la recherche LDAP standard, dans tout domaine sans avoir à spécifier le nom de domaine.
- **Recherche utilisateur par :** dans la liste, cliquez sur **userPrincipalName** ou **sAMAccountName**. Si vous modifiez le paramètre **Rechercher utilisateurs par** après l'inscription, les utilisateurs doivent s'inscrire à nouveau.
- **Utiliser une connexion sécurisée :** indiquez si des connexions sécurisées doivent être utilisées.

4. Cliquez sur **Enregistrer** pour enregistrer vos modifications ou sur **Annuler** pour laisser la propriété inchangée.

Pour supprimer un annuaire compatible LDAP

1. Dans le tableau **LDAP**, sélectionnez l'annuaire que vous souhaitez supprimer.

   Vous pouvez sélectionner plusieurs propriétés à supprimer en sélectionnant la case à cocher en regard de chaque propriété.

2. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer**.

Configuration de l'authentification multi-domaines

Pour configurer XenMobile Server pour utiliser plusieurs suffixes de domaine dans une configuration LDAP, consultez la procédure dans la documentation Citrix Endpoint Management Configuration de

l'authentification multi-domaines. Les étapes sont les mêmes dans la version locale de XenMobile Server et dans la version cloud Endpoint Management.

Configurer l'authentification domaine + jeton de sécurité

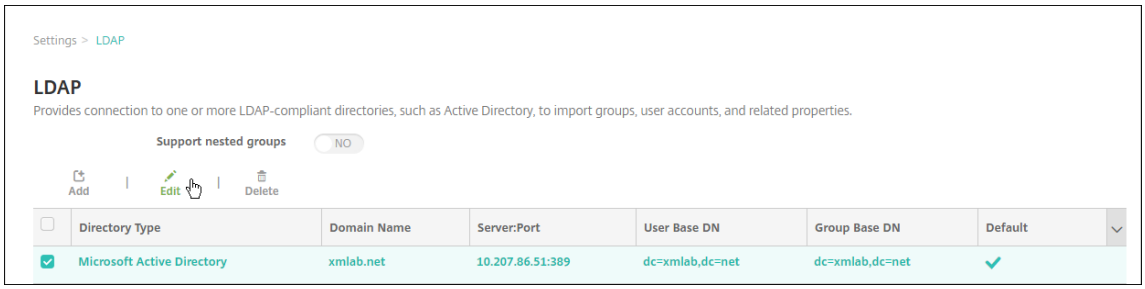
Vous pouvez configurer XenMobile de manière à obliger les utilisateurs à s'authentifier avec leurs informations d'identification LDAP plus un mot de passe à usage unique, à l'aide du protocole RADIUS.

Pour une utilisabilité optimale, vous pouvez combiner cette configuration avec le code PIN Citrix et la mise en cache du mot de passe Active Directory. Avec cette configuration, les utilisateurs n'ont pas à entrer leurs noms d'utilisateur et mots de passe LDAP à plusieurs reprises. Les utilisateurs doivent entrer leurs noms et mots de passe lors de l'inscription, de l'expiration du mot de passe et du verrouillage du compte.

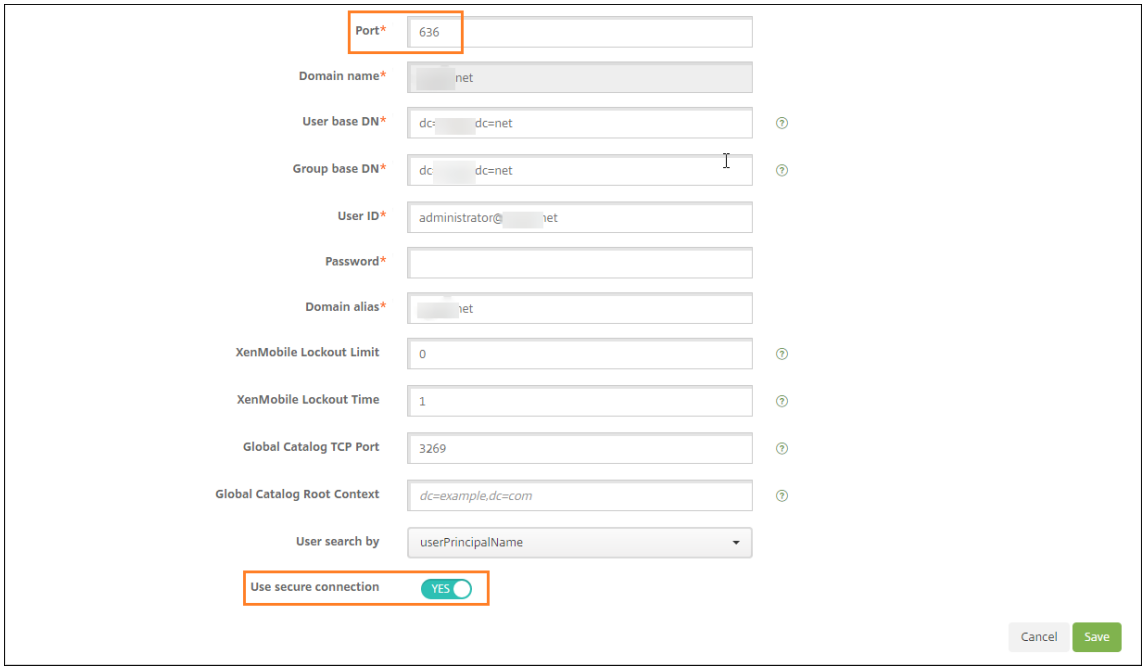
Configurer les paramètres LDAP

L'utilisation de LDAP pour l'authentification nécessite que vous installiez un certificat SSL d'une autorité de certification sur XenMobile. Pour de plus amples informations, consultez la section Chargement de certificats dans XenMobile.

1. Dans **Paramètres**, cliquez sur **LDAP**.
2. Sélectionnez **Microsoft Active Directory** et cliquez sur **Modifier**.



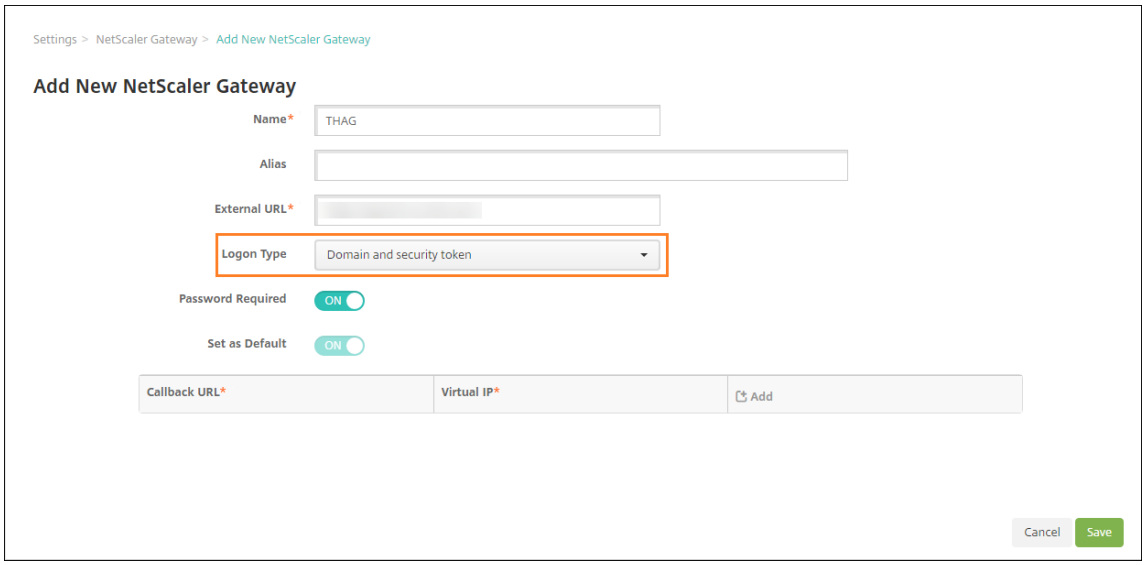
3. Vérifiez que le port Port est **636** pour les connexions LDAP sécurisées ou **3269** pour les connexions LDAP sécurisées Microsoft.
4. Changez **Utiliser une connexion sécurisée** sur **Oui**.



Configurer les paramètres de Citrix Gateway

Les étapes suivantes supposent que vous avez déjà ajouté une instance Citrix Gateway à XenMobile. Pour ajouter une instance Citrix Gateway, consultez la section Ajouter une instance Citrix Gateway.

1. Dans **Paramètres**, cliquez sur **Citrix Gateway**.
2. Sélectionnez **Citrix Gateway**, puis cliquez sur **Modifier**.
3. Depuis **Type d'ouverture de session**, sélectionnez **Domaine et jeton de sécurité**.



Activer le code PIN Citrix et la mise en cache du mot de passe de l'utilisateur

Pour activer le code PIN Citrix et la mise en cache du mot de passe de l'utilisateur, accédez à **Paramètres > Propriétés du client** et sélectionnez ces cases : **Activer l'authentification par code PIN Citrix** et **Activer la mise en cache du mot de passe de l'utilisateur**. Pour de plus amples informations, consultez la section Propriétés du client.

Configurer Citrix Gateway pour l'authentification par jeton de sécurité et domaine

Configurez des profils de sessions Citrix Gateway et des stratégies pour les serveurs virtuels que vous utilisez avec XenMobile. Pour plus d'informations, consultez la documentation Citrix Gateway.

Authentification certificat client ou certificat + domaine

January 10, 2022

La configuration par défaut pour XenMobile est l'authentification par nom d'utilisateur et mot de passe. Pour ajouter une autre couche de sécurité pour l'inscription et l'accès à l'environnement XenMobile, vous pouvez utiliser l'authentification basée sur certificats. Dans l'environnement XenMobile, cette configuration est la meilleure combinaison de sécurité et d'expérience utilisateur. L'authentification par certificat plus domaine offre les meilleures possibilités d'authentification unique associées à la sécurité fournie par l'authentification à deux facteurs sur Citrix ADC.

Pour une utilisabilité optimale, vous pouvez combiner l'authentification par certificat plus domaine avec le code PIN Citrix et la mise en cache du mot de passe Active Directory. Dans ce cas, les utilisateurs n'ont pas à entrer leurs noms d'utilisateur et mots de passe LDAP à plusieurs reprises. Les utilisateurs doivent entrer leurs noms et mots de passe lors de l'inscription, de l'expiration du mot de passe et du verrouillage du compte.

> **Important :**
>
> XenMobile ne prend pas en charge le passage du mode d'authentification, de l'authentification de domaine à un autre mode d'authentification, après que les utilisateurs ont inscrit des appareils dans XenMobile.

Si vous n'autorisez pas LDAP et utilisez des cartes à puce ou méthodes similaires, la configuration des certificats vous permet de représenter une carte à puce auprès de XenMobile. Les utilisateurs s'inscrivent alors à l'aide d'un code PIN unique généré par XenMobile. Une fois qu'un utilisateur a accès, XenMobile crée et déploie le certificat utilisé ensuite pour s'authentifier auprès de l'environnement XenMobile.

Vous pouvez utiliser l'assistant Citrix ADC for XenMobile pour procéder à la configuration requise pour

XenMobile lors de l'utilisation de l'authentification par certificat Citrix ADC ou certificat + domaine. Vous ne pouvez exécuter l'assistant Citrix ADC for XenMobile qu'une seule fois.

Dans les environnements hautement sécurisés, l'utilisation d'informations d'identification LDAP en dehors d'une organisation dans des réseaux publics ou non sécurisés est considérée comme une menace de sécurité majeure pour l'entreprise. Pour les environnements hautement sécurisés, il est possible d'opter pour l'authentification à deux facteurs à l'aide d'un certificat client et d'un jeton de sécurité. Pour de plus amples informations, consultez la section Configuration de XenMobile pour l'authentification par certificat et jeton de sécurité.

L'authentification du certificat client est disponible pour le mode XenMobile MAM (MAM exclusif) et le mode ENT (lorsque les utilisateurs s'inscrivent dans MDM). L'authentification du certificat client n'est pas disponible pour le mode XenMobile ENT lorsque les utilisateurs s'inscrivent dans l'ancien mode MAM. Pour utiliser l'authentification du certificat client dans les modes XenMobile ENT et MAM, vous devez configurer le serveur Microsoft, XenMobile Server et Citrix Gateway. Suivez ces étapes générales, décrites dans cet article.

Sur le serveur Microsoft :

1. Ajoutez un composant logiciel enfichable pour les certificats dans la console Microsoft Management Console.
2. Ajoutez le modèle à l'autorité de certification (CA).
3. Créez un certificat PFX depuis le serveur CA.

Sur XenMobile Server :

1. Chargez le certificat sur XenMobile.
2. Créez l'entité PKI pour l'authentification par certificat.
3. Configurez les fournisseurs d'informations d'identification.
4. Configurez Citrix Gateway afin de fournir un certificat utilisateur pour l'authentification.

Pour plus d'informations sur la configuration de Citrix Gateway, consultez ces articles dans la documentation de Citrix ADC :

- Authentification client
- Infrastructure de profils SSL
- Configuration et liaison d'une stratégie d'authentification de certificat client

Conditions préalables

- Lorsque vous créez un modèle d'entité Services de certificats Microsoft, évitez les problèmes d'authentification possibles avec des appareils inscrits, en n'utilisant pas de caractères spéciaux. Par exemple, n'utilisez pas ces caractères dans le nom du modèle : `: ! $ ()## % + * ~ ? | { } []`

- Pour les appareils Windows Phone 8.1 utilisant l'authentification du certificat et le déchargement SSL, désactivez la réutilisation de session SSL pour le port 443 sur les serveurs virtuels d'équilibrage de charge dans Citrix ADC. Pour ce faire, exécutez la commande suivante sur les serveurs virtuels pour le port 443 :

  ```
  set ssl vserver <ssl lb vserver> sessReuse DISABLE
  ```

  La désactivation de la réutilisation de la session SSL désactive certaines des optimisations fournies par Citrix ADC, ce qui peut entraîner une diminution des performances sur Citrix ADC.

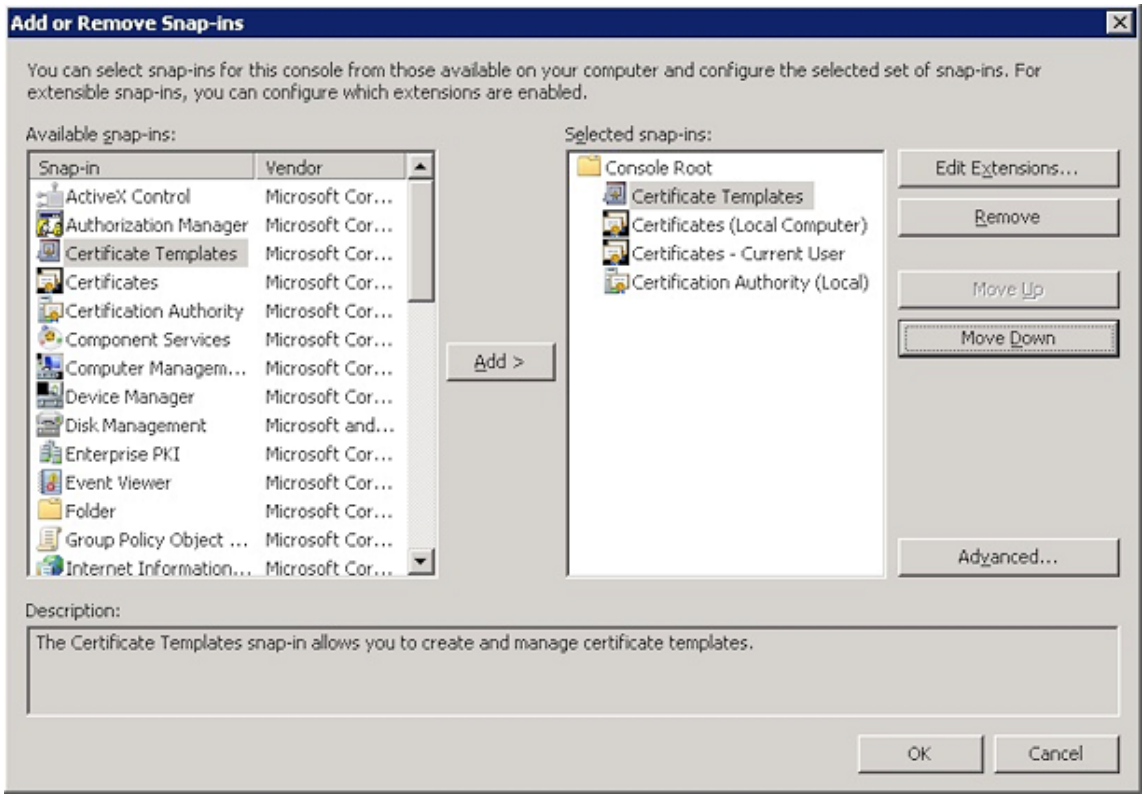
- Pour configurer l'authentification basée sur certificat pour Exchange ActiveSync, consultez le blog de Microsoft. Configurez le site de serveur d'autorité de certification (CA) pour Exchange ActiveSync pour exiger des certificats clients.

- Si vous utilisez des certificats de serveur privé pour sécuriser le trafic ActiveSync avec le serveur Exchange, assurez-vous que tous les certificats racine et intermédiaires nécessaires ont été installés sur les appareils mobiles. Sinon, l'authentification basée sur certificat échoue lors de la configuration de la boîte aux lettres dans Secure Mail. Dans la console Exchange IIS, vous devez :

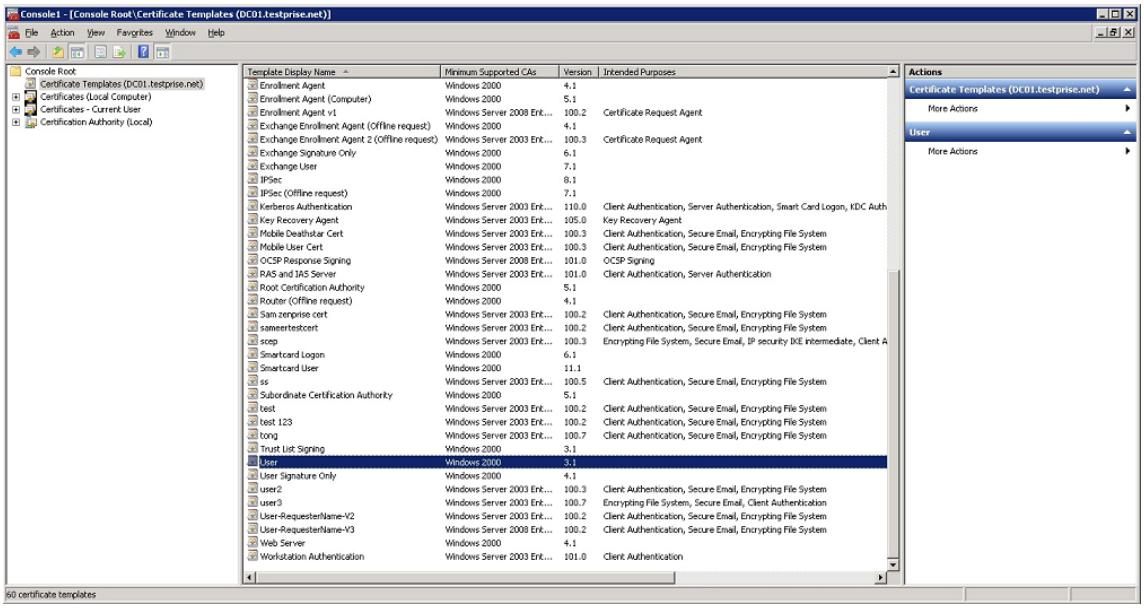
  - Ajouter un site Web à utiliser par XenMobile avec Exchange et lier le certificat de serveur Web.
  - Utiliser le port 9443.
  - Pour ce site Web, vous devez ajouter deux applications, une pour « Microsoft-Server-ActiveSync » et une pour « EWS ». Pour ces deux applications, sous **Paramètres SSL**, sélectionnez **Exiger SSL**.

Ajoutez un composant logiciel enfichable pour les certificats dans la console Microsoft Management Console

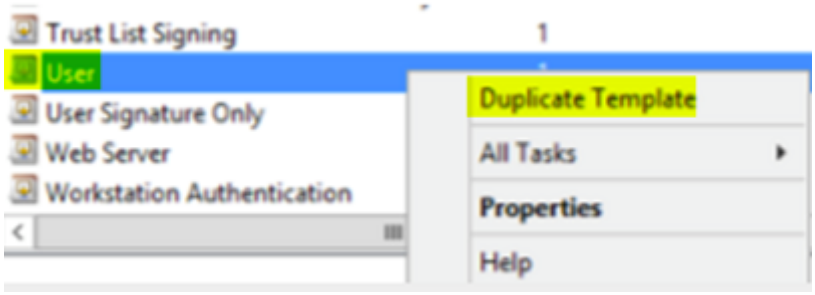
1. Ouvrez la console et cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
2. Ajoutez les composants logiciels enfichables suivants :
   - Modèles de certificats
   - Certificats (ordinateur local)
   - Certificats - Utilisateur actuel
   - Autorité de certification (locale)



3. Développez **Modèles de certificats**.



4. Sélectionnez le modèle **Utilisateur** et **Dupliquer le modèle**.

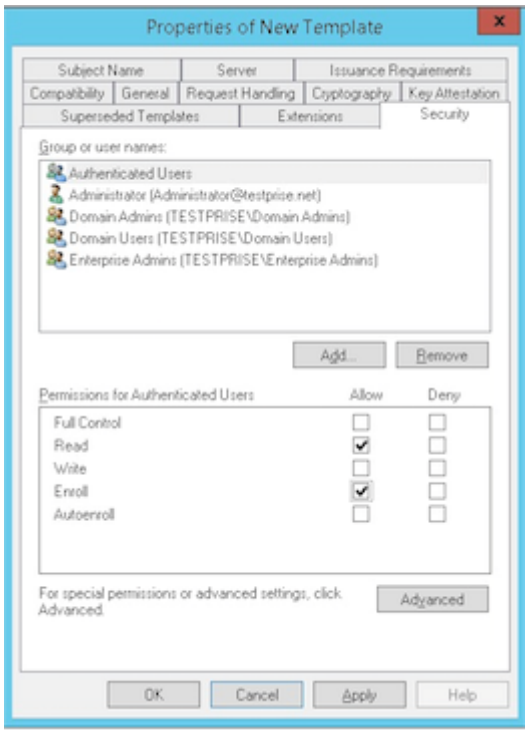


5. Fournissez le nom du modèle.

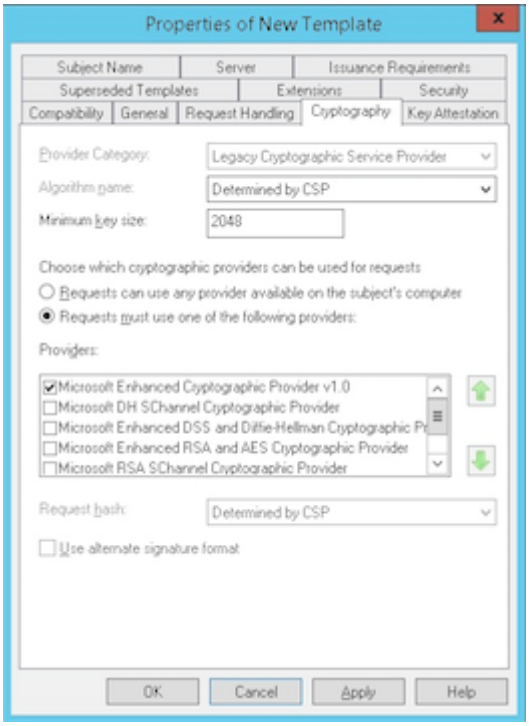
> **Important :**
>
> Sélectionnez la case **Publier le certificat dans Active Directory** uniquement si nécessaire. Si cette option est sélectionnée, tous les certificats client utilisateur sont créés dans Active Directory, ce qui pourrait encombrer votre base de données Active Directory.

6. Sélectionnez **Windows 2003 Server** comme type de modèle. Dans Windows 2012 R2 Server, sous **Compatibilité**, sélectionnez **Autorité de certification** et définissez le destinataire en tant que **Windows 2003**.

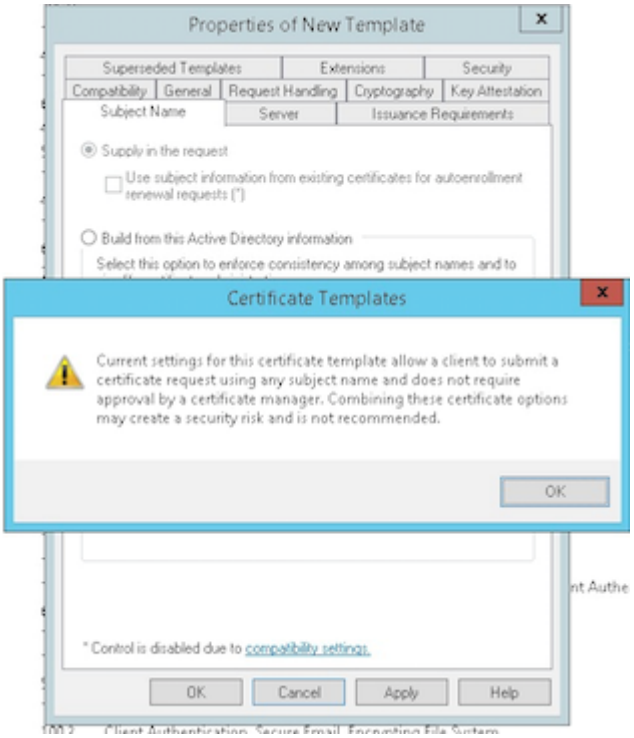
7. Sous **Sécurité**, sélectionnez l'option **Inscrire** dans la colonne **Autoriser** pour les utilisateurs authentifiés.



8. Sous **Cryptographie**, assurez-vous de fournir la taille de la clé. Vous entrerez plus tard la taille de la clé lors de la configuration de XenMobile.

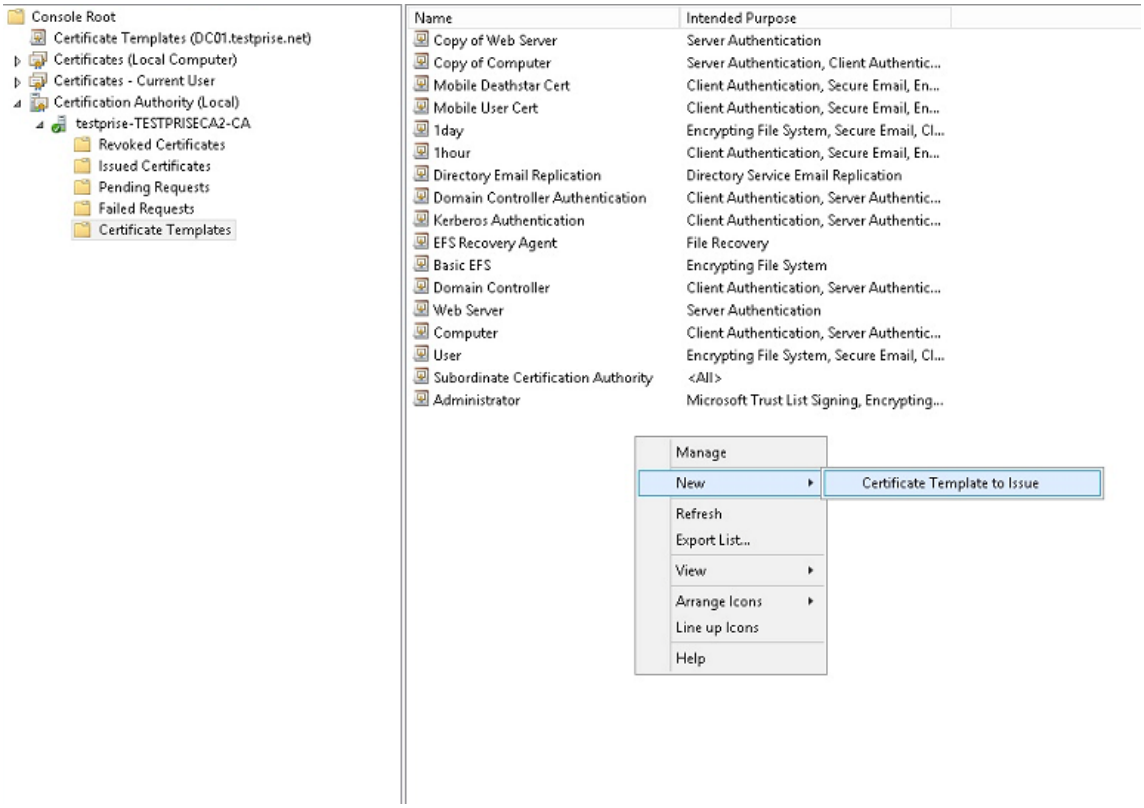


9. Sous **Nom du sujet**, sélectionnez **Fournir dans la demande**. Appliquez les modifications et enregistrez.

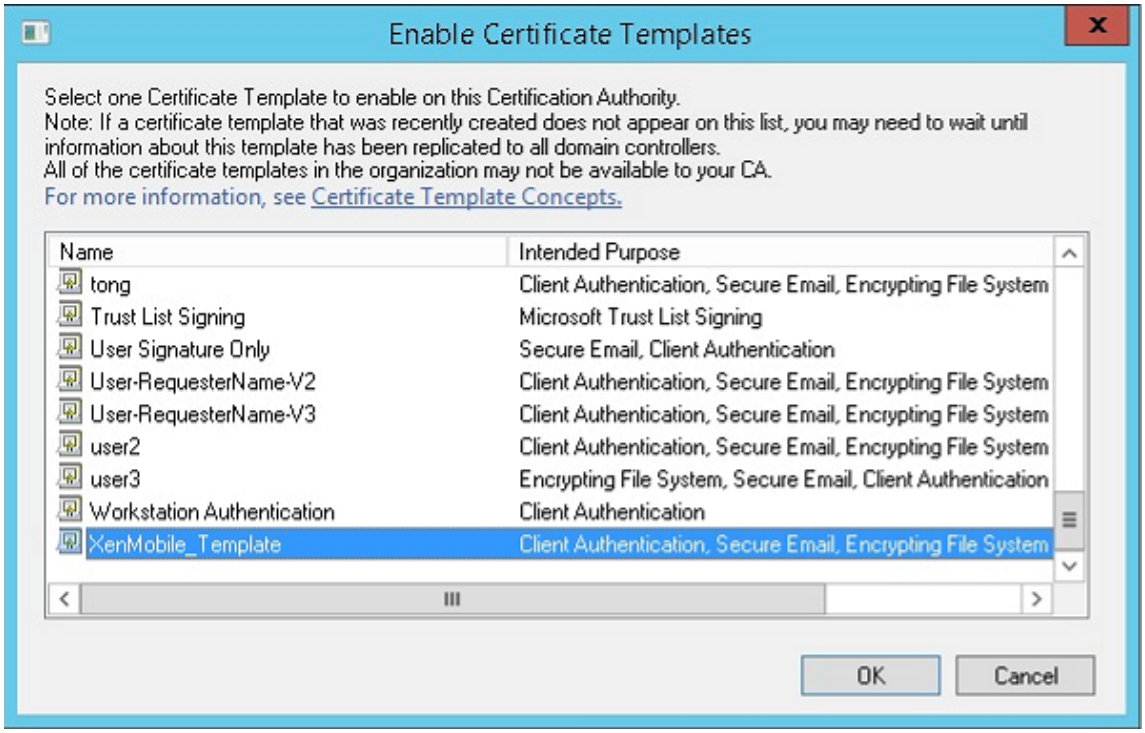


Ajout du modèle à l'autorité de certification (CA)

1. Accédez à **Autorité de certification** et sélectionnez **Modèles de certificats**.
2. Cliquez avec le bouton droit dans le panneau de droite et sélectionnez **Nouveau > Modèle de certificat à délivrer**.

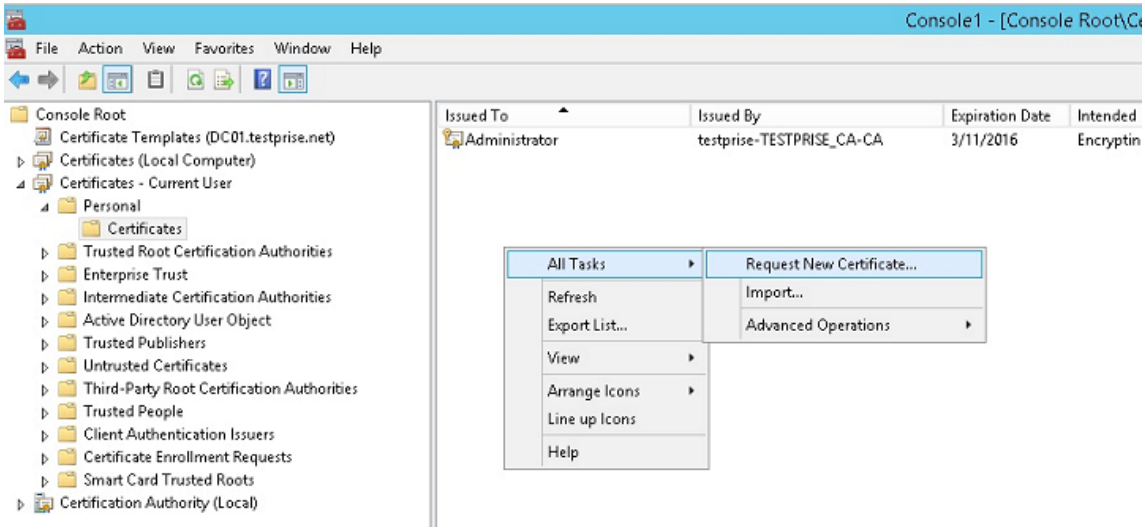


3. Sélectionnez le modèle que vous avez créé à l'étape précédente et cliquez sur **OK** pour l'ajouter à l'**autorité de certification**.

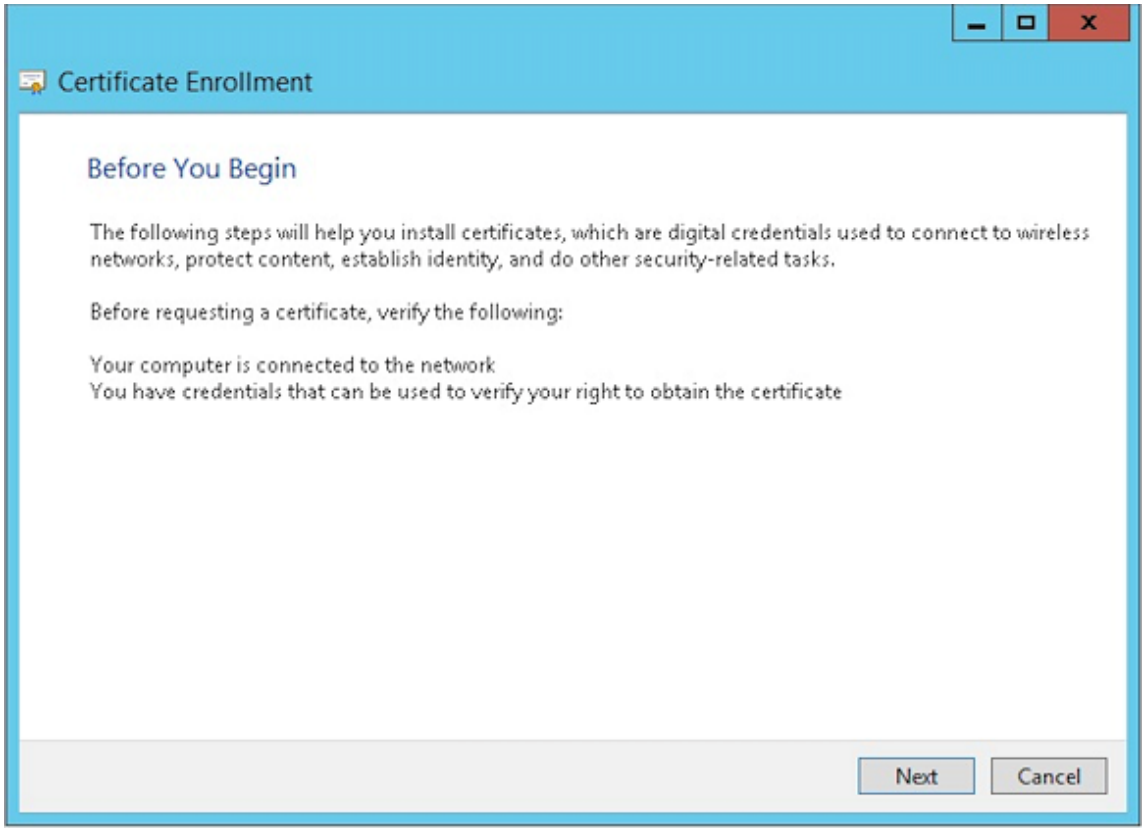


Création d'un certificat PFX depuis le serveur CA

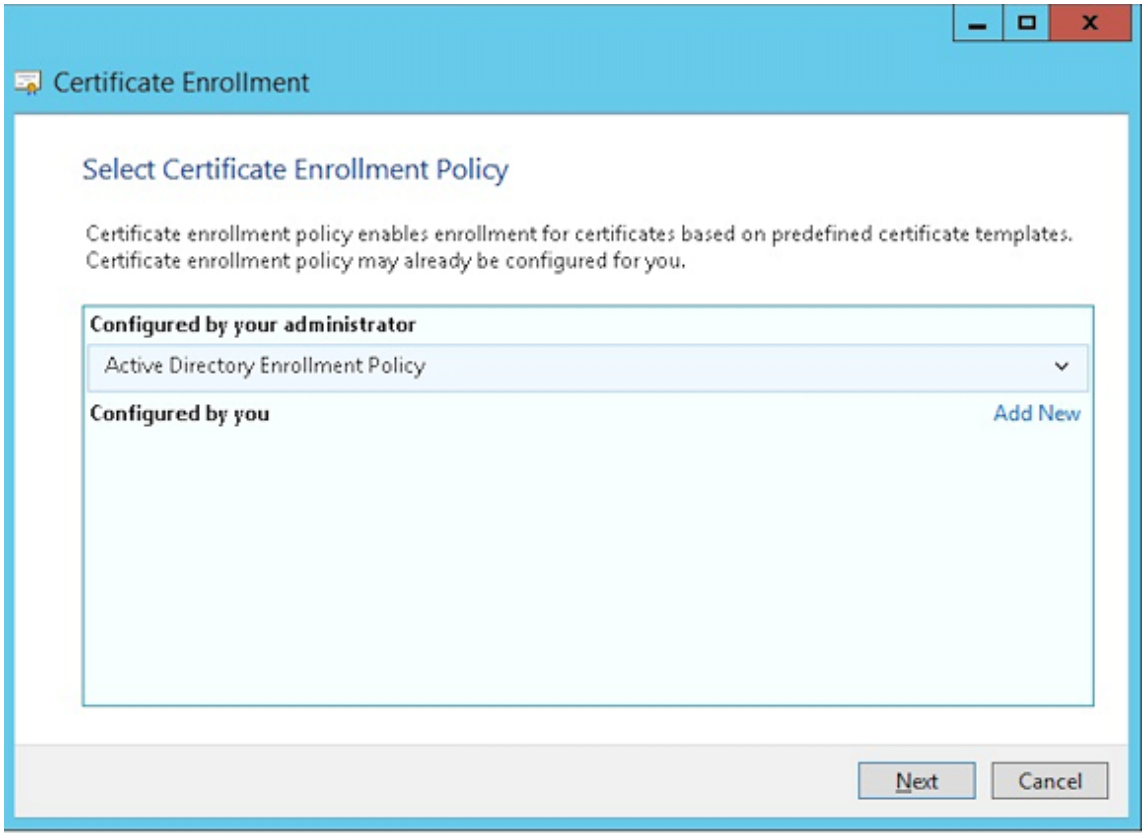
1. Créez un certificat utilisateur .pfx à l'aide du compte de service avec lequel vous vous êtes connecté. Ce fichier .pfx est chargé dans XenMobile, qui demande ensuite un certificat utilisateur de la part des utilisateurs qui inscrivent leurs appareils.
2. Sous **Utilisateur actuel**, développez **Certificats**.
3. Cliquez avec le bouton droit dans le panneau de droite et cliquez sur **Demander un nouveau certificat**.



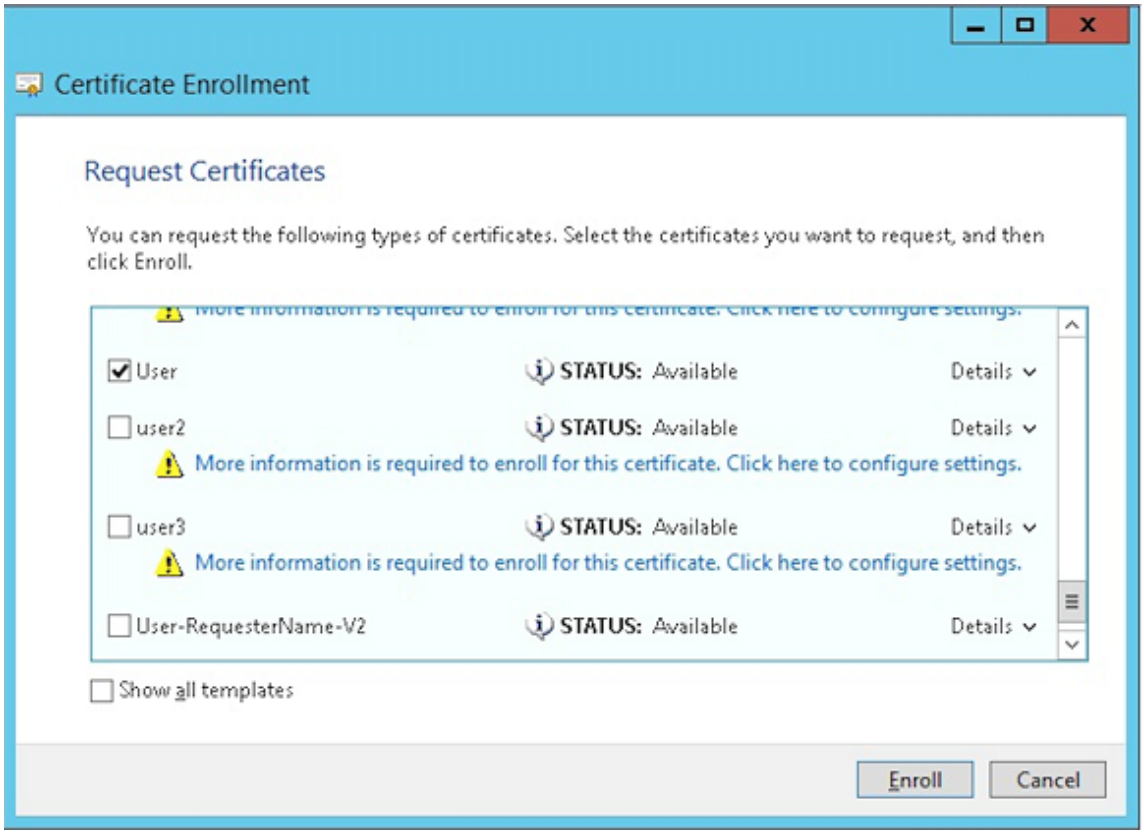
4. L'écran **Inscription de certificats** s'affiche. Cliquez sur **Suivant**.



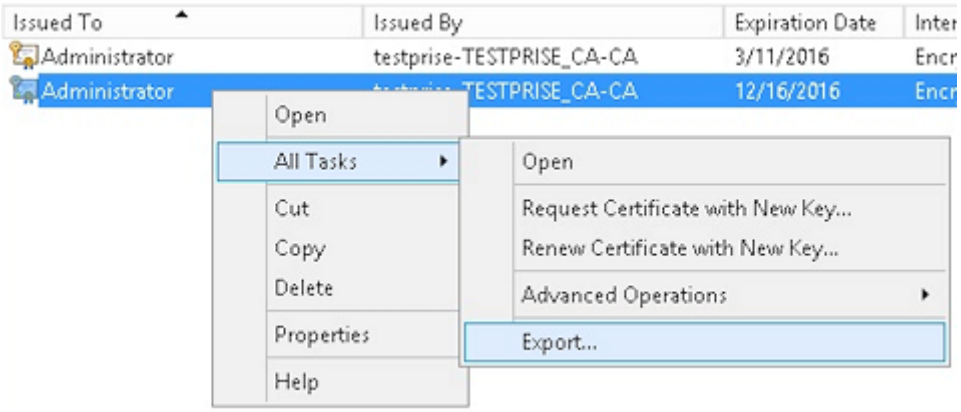
5. Sélectionnez **Stratégie d'inscription à Active Directory** et cliquez sur **Suivant**.



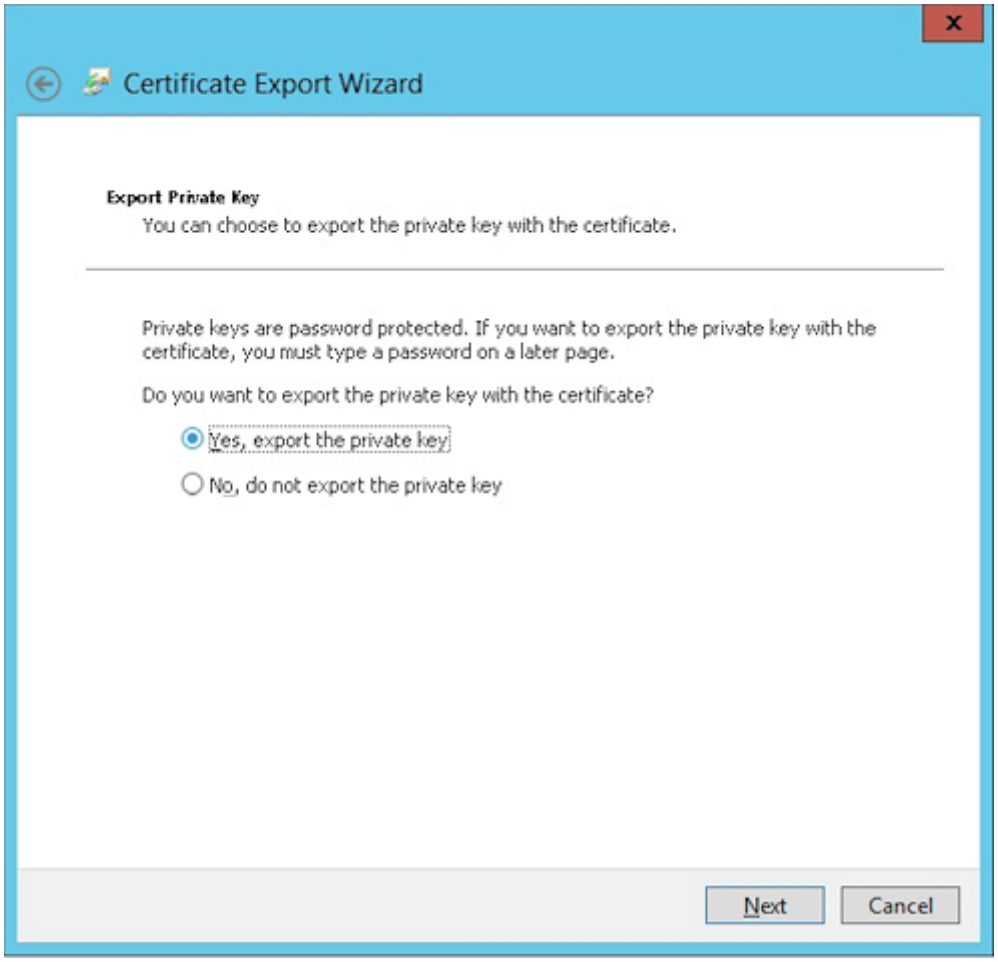
6. Sélectionnez le modèle **Utilisateur** et cliquez sur **Inscrire**.



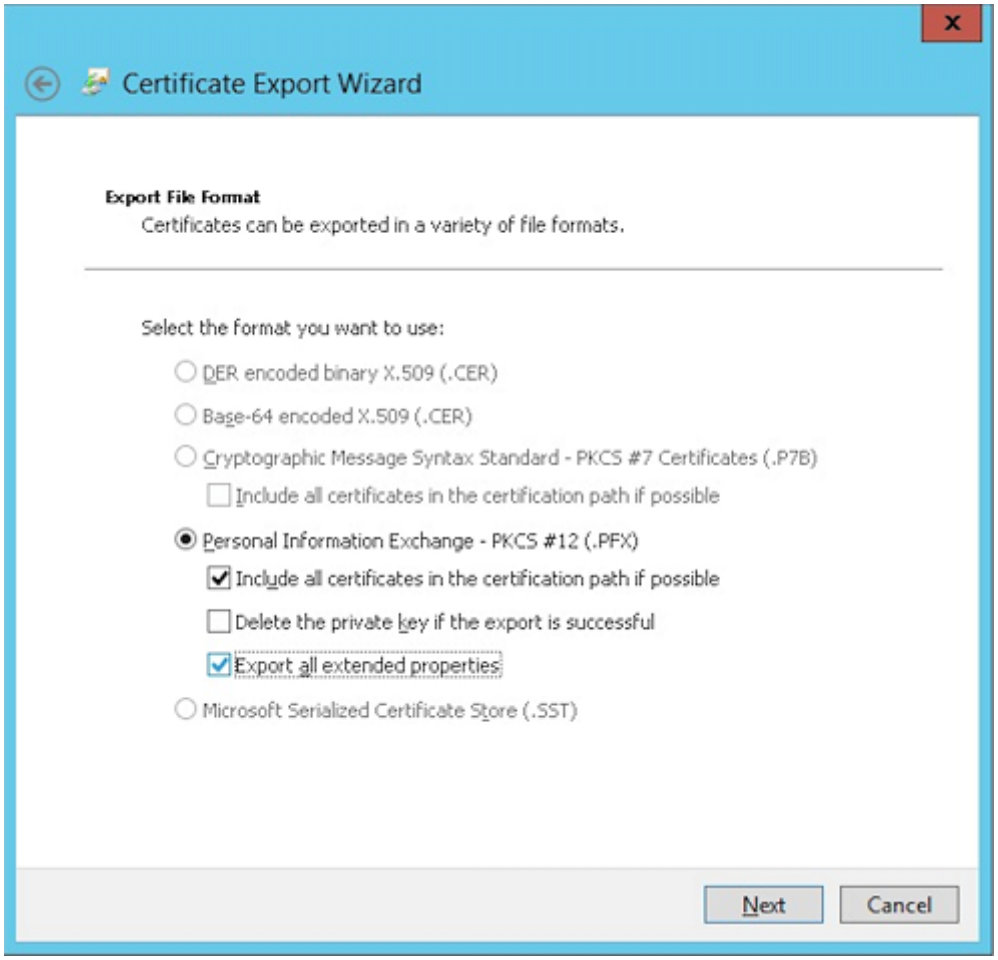
7. Exportez le fichier .pfx que vous avez créé à l'étape précédente.



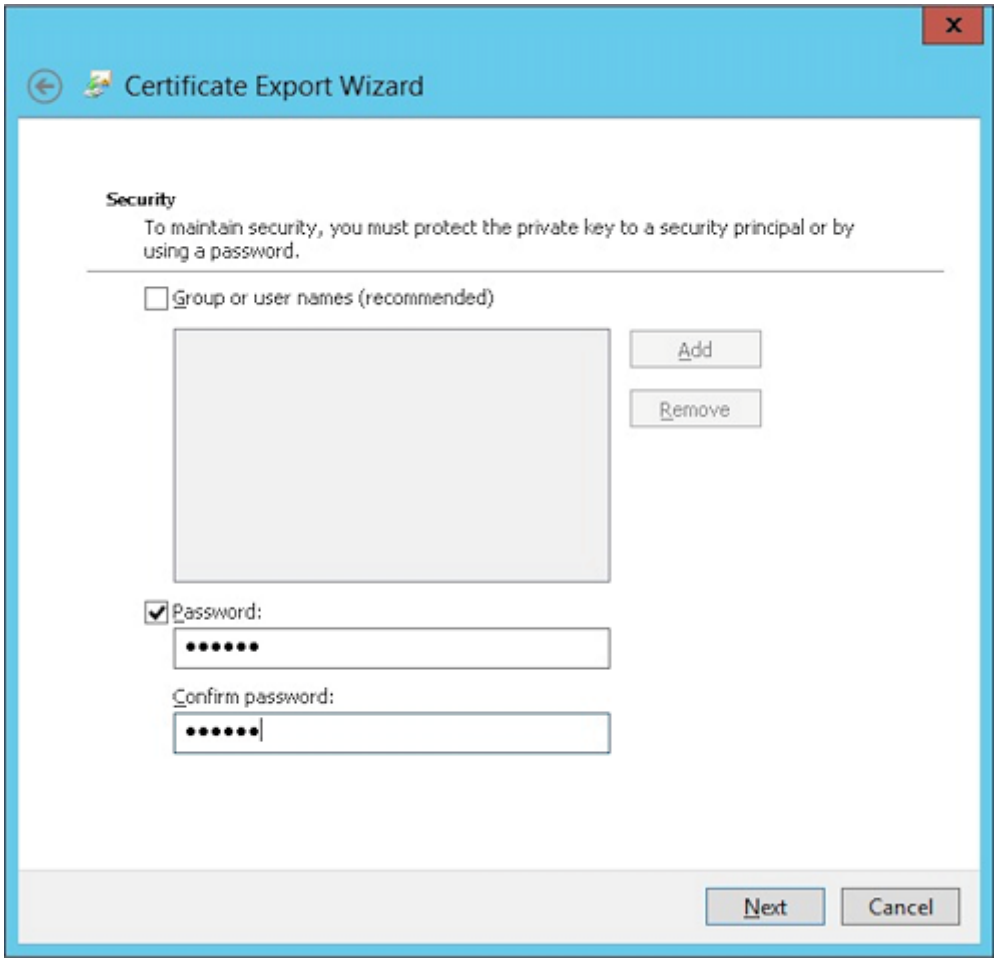
8. Cliquez sur **Oui, exporter la clé privée**.



9. Sélectionnez **Si possible inclure tous les certificats dans le chemin d'accès de certification si possible** et la case **Exporter toutes les propriétés étendues**.



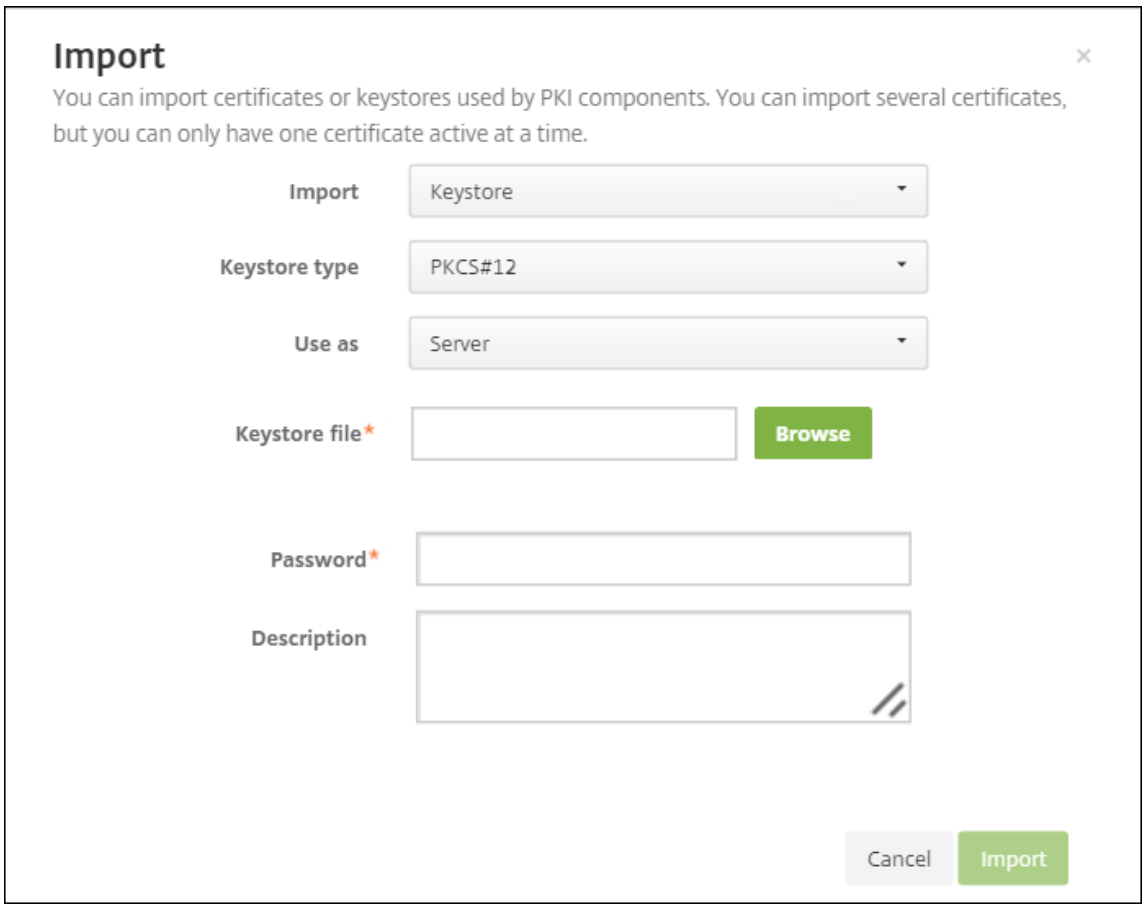
10. Définissez un mot de passe que vous utiliserez lors du chargement de ce certificat dans XenMobile.



11. Enregistrez le certificat sur votre disque dur.

Chargement du certificat sur XenMobile

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. L'écran **Paramètres** s'affiche.
2. Cliquez sur **Certificats** et sur **Importer**.
3. Entrez les paramètres suivants :
   - **Importer :** Keystore
   - **Type de keystore :** PKCS # 12
   - **Utiliser en tant que :** Serveur
   - **Fichier de keystore :** cliquez sur **Parcourir** pour sélectionner le certificat `.pfx` que vous avez créé.
   - **Mot de passe :** entrez le mot de passe que vous avez créé pour ce certificat.

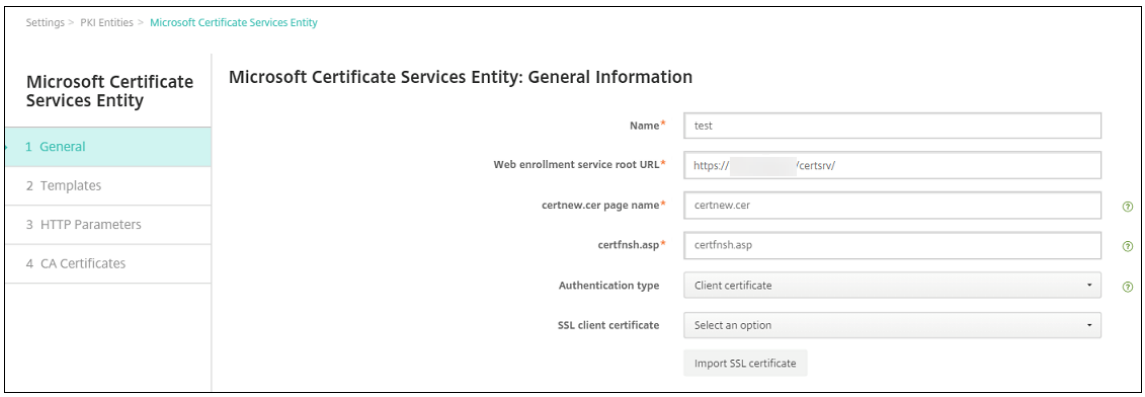


4. Cliquez sur **Importer**.
5. Vérifiez que le certificat a été installé correctement. Un certificat correctement installé s'affiche en tant que certificat utilisateur.

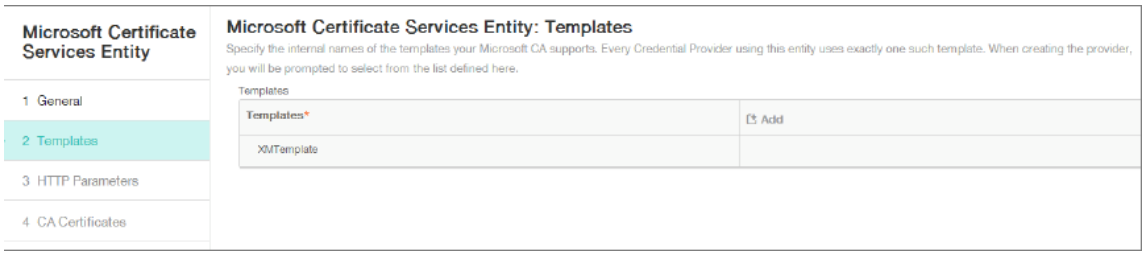
Création de l'entité PKI pour l'authentification par certificat

1. Dans **Paramètres**, accédez à **Plus > Gestion des certificats > Entités PKI**.
2. Cliquez sur **Ajouter** et sur **Entité Services de certificats Microsoft**. L'écran **Entité Services de certificats Microsoft : informations générales** s'affiche.
3. Entrez les paramètres suivants :
   - **Nom :** entrez un nom quelconque.
   - **URL racine du service d'inscription Web :** `https://RootCA-URL/certsrv/` (N'oubliez pas d'ajouter la dernière barre oblique (/) dans l'URL.)
   - **Nom de page certnew.cer :** certnew.cer (valeur par défaut)
   - **certfnsh.asp :** certfnsh.asp (valeur par défaut)
   - **Type d'authentification :** certificat client

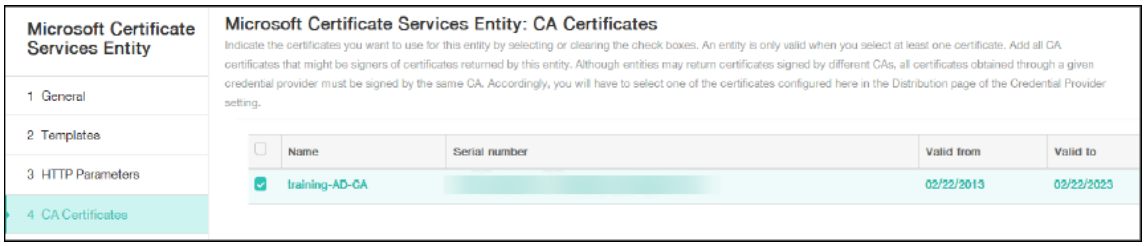
- **Certificat SSL :** sélectionnez le certificat utilisateur à utiliser pour émettre le certificat client XenMobile.



4. Sous **Modèles**, ajoutez le modèle que vous avez créé lors de la configuration du certificat Microsoft. N'ajoutez pas d'espaces.



5. Ignorez les paramètres HTTP et cliquez sur **Certificats CA**.
6. Sélectionnez le nom de l'autorité de certification racine qui correspond à votre environnement. L'autorité de certification racine fait partie de la chaîne importée depuis le certificat client XenMobile.

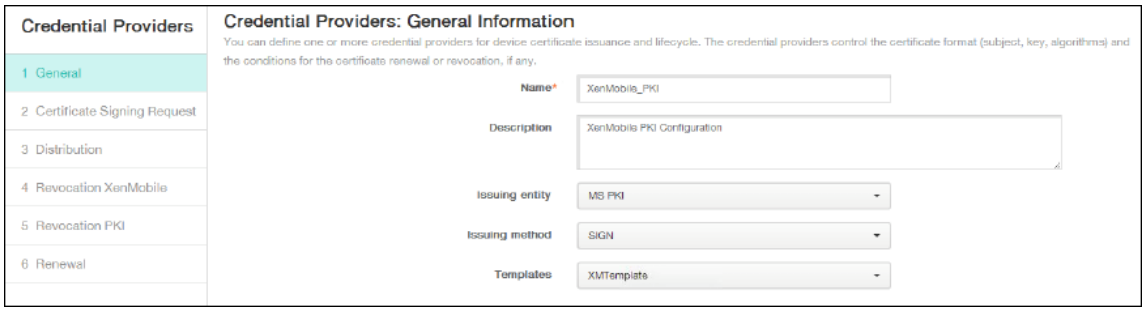


7. Cliquez sur **Enregistrer**.

Configuration des Fournisseurs d'informations d'identification

1. Dans **Paramètres**, accédez à **Plus > Gestion des certificats > Fournisseurs d'informations d'identification**.
2. Cliquez sur **Ajouter**.
3. Sous **Général**, entrez les paramètres suivants :

- **Nom :** entrez un nom quelconque.
- **Description :** entrez une description quelconque.
- **Entité émettrice :** sélectionnez l'entité PKI créée précédemment.
- **Méthode d'émission :** SIGNER
- **Modèles :** sélectionnez le modèle ajouté sous l'entité PKI.

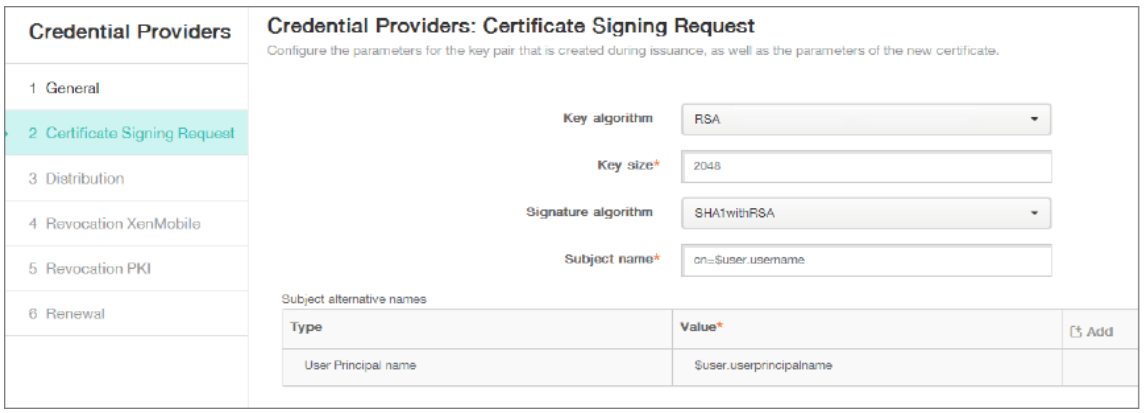


4. Cliquez sur **Demande de signature de certificat** et entrez les paramètres suivants :

   - **Algorithme de clé :** RSA
   - **Taille de la clé :** 2048
   - **Algorithme de signature :** SHA256withRSA
   - **Nom du sujet :** `cn=$user.username`

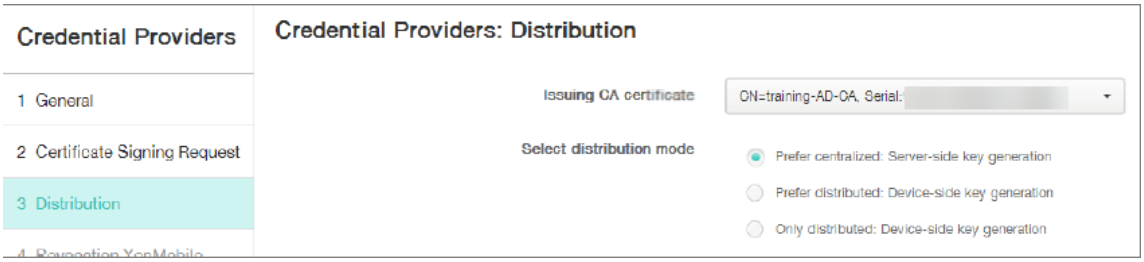
   Pour **Noms de sujet alternatifs**, cliquez sur **Ajouter** et entrez les paramètres suivants :

   - **Type :** nom principal de l'utilisateur
   - **Valeur :** `$user.userprincipalname`

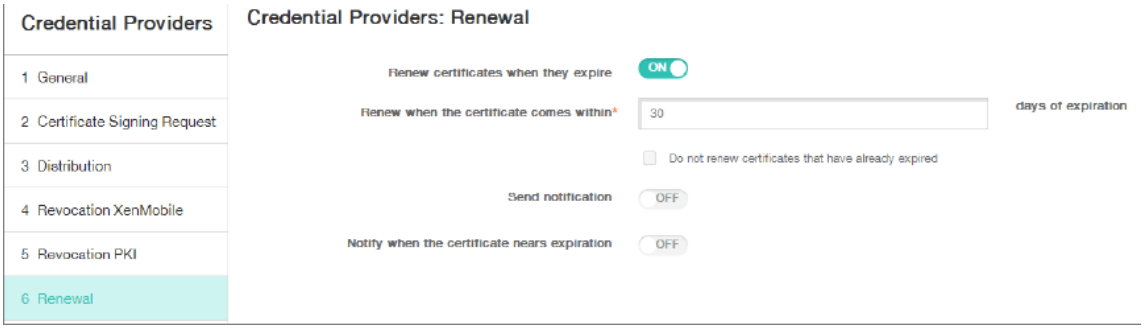


5. Cliquez sur **Distribution** et entrez les paramètres suivants :

   - **Certificat émis par l'autorité de certification :** sélectionnez l'autorité de certification émettrice qui a signé le certificat client XenMobile.
   - **Sélectionner le mode de distribution :** sélectionnez **Préférer mode centralisé : génération de la clé sur le serveur**.



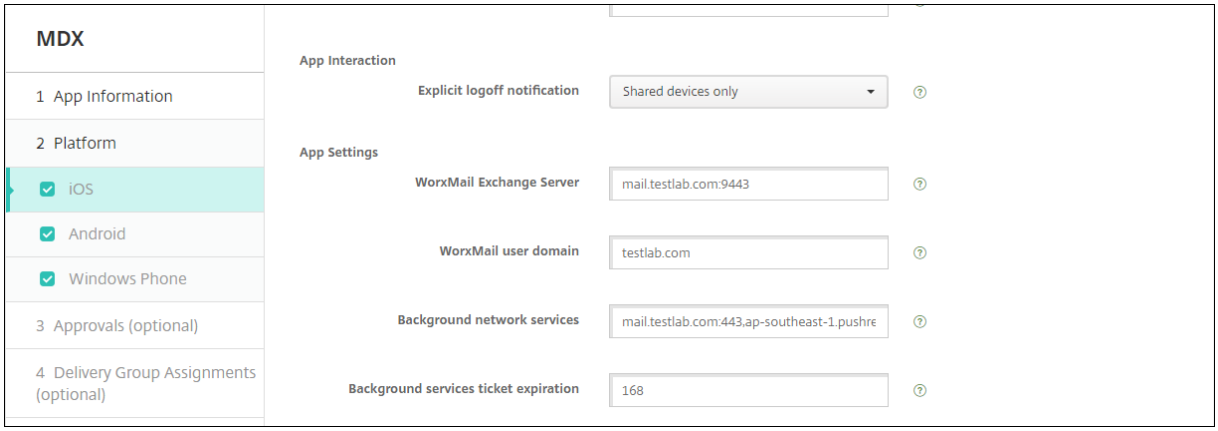
6. Pour les deux prochaines sections – **Révocation XenMobile** et **Révocation PKI** – définissez les paramètres comme vous le souhaitez. Dans cet exemple, les deux options sont ignorées.
7. Cliquez sur **Renouvellement**.
8. Pour **Renouveler les certificats lorsqu'ils expirent**, sélectionnez **Activé**.
9. Laissez tous les autres paramètres par défaut ou modifiez-les comme vous le souhaitez.



10. Cliquez sur **Enregistrer**.

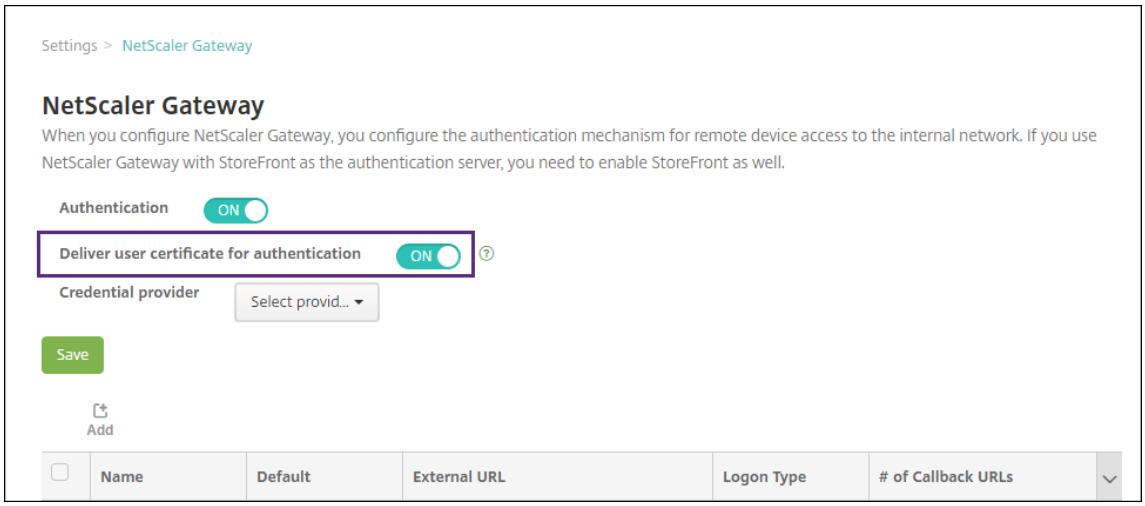
Configuration de Secure Mail pour utiliser l'authentification basée sur certificat

Lorsque vous ajoutez Secure Mail à XenMobile, n'oubliez pas de configurer les paramètres Exchange sous **Paramètres applicatifs**.

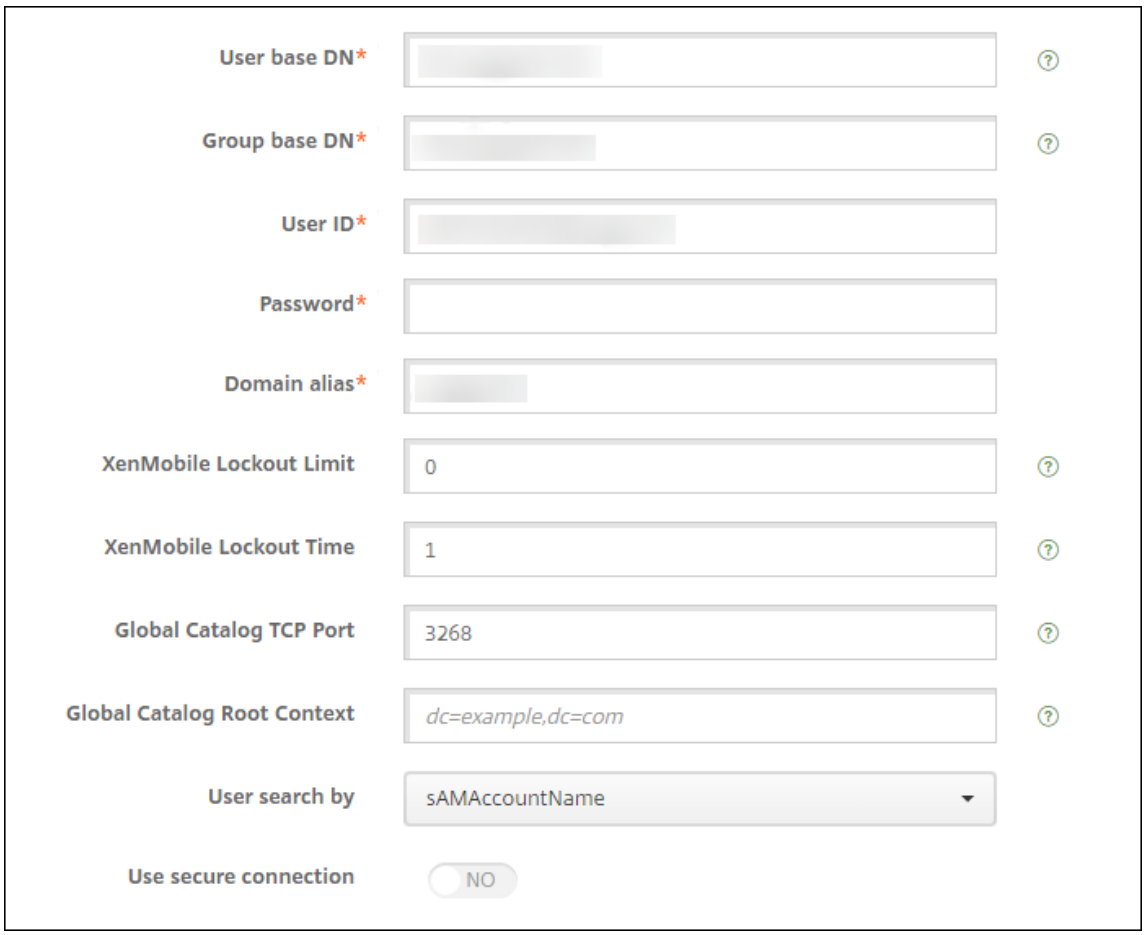


Configuration de la remise de certificats Citrix ADC dans XenMobile

1. Connectez-vous à la console XenMobile et cliquez sur l'icône d'engrenage dans le coin supérieur droit. L'écran **Paramètres** s'affiche.
2. Sous **Serveur**, cliquez sur **Citrix Gateway**.
3. Si Citrix Gateway n'est pas déjà ajouté, cliquez sur **Ajouter** et spécifiez les paramètres :
   - **URL externe :** `https://YourCitrixGatewayURL`
   - **Type d'ouverture de session :** Certificat et domaine
   - **Mot de passe requis :** DÉSACTIVÉ
   - **Définir par défaut :** ACTIVÉ
4. Pour **Délivrer un certificat utilisateur pour l'authentification**, sélectionnez **Activé**.



5. Pour **Fournisseur d'identités**, sélectionnez un fournisseur et cliquez sur **Enregistrer**.
6. Pour utiliser des attributs sAMAccount dans les certificats utilisateur comme une alternative au nom d'utilisateur principal (UPN), configurez le connecteur LDAP dans XenMobile comme suit : accédez à **Paramètres > LDAP**, sélectionnez le répertoire et cliquez sur **Modifier**, puis sélectionnez **sAMAccountName** dans **Recherche utilisateur par**.



Activer le code PIN Citrix et la mise en cache du mot de passe de l'utilisateur

Pour activer le code PIN Citrix et la mise en cache du mot de passe de l'utilisateur, accédez à **Paramètres > Propriétés du client** et sélectionnez ces cases : **Activer l'authentification par code PIN Citrix** et **Activer la mise en cache du mot de passe de l'utilisateur**. Pour de plus amples informations, consultez la section Propriétés du client.

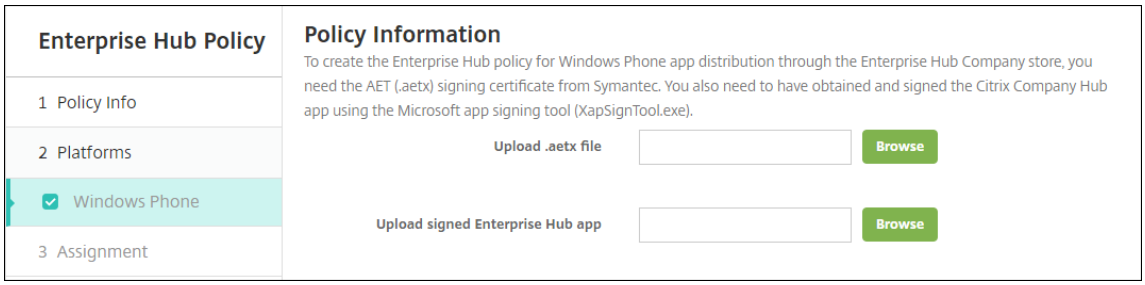
Création d'une stratégie d'hub d'entreprise pour Windows Phone

Pour les appareils Windows Phone, vous devez créer une stratégie d'hub d'entreprise pour délivrer le fichier AETX et le client Secure Hub.

> **Remarque :**
>
> Assurez-vous que les fichiers AETX et Secure Hub utilisent tous les deux :
>
> - le même certificat d'entreprise du fournisseur de certificat
> - le même ID d'éditeur depuis le compte développeur Windows Store

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**.

2. Cliquez sur **Ajouter**, puis, sous **Plus > Agent XenMobile**, cliquez sur **Hub d'entreprise**.
3. Après avoir attribué un nom à la stratégie, sélectionnez le fichier `.AETX` correct et l'application Secure Hub signée pour le hub d'entreprise.



4. Attribuez la stratégie à des groupes de mise à disposition et enregistrez-la.

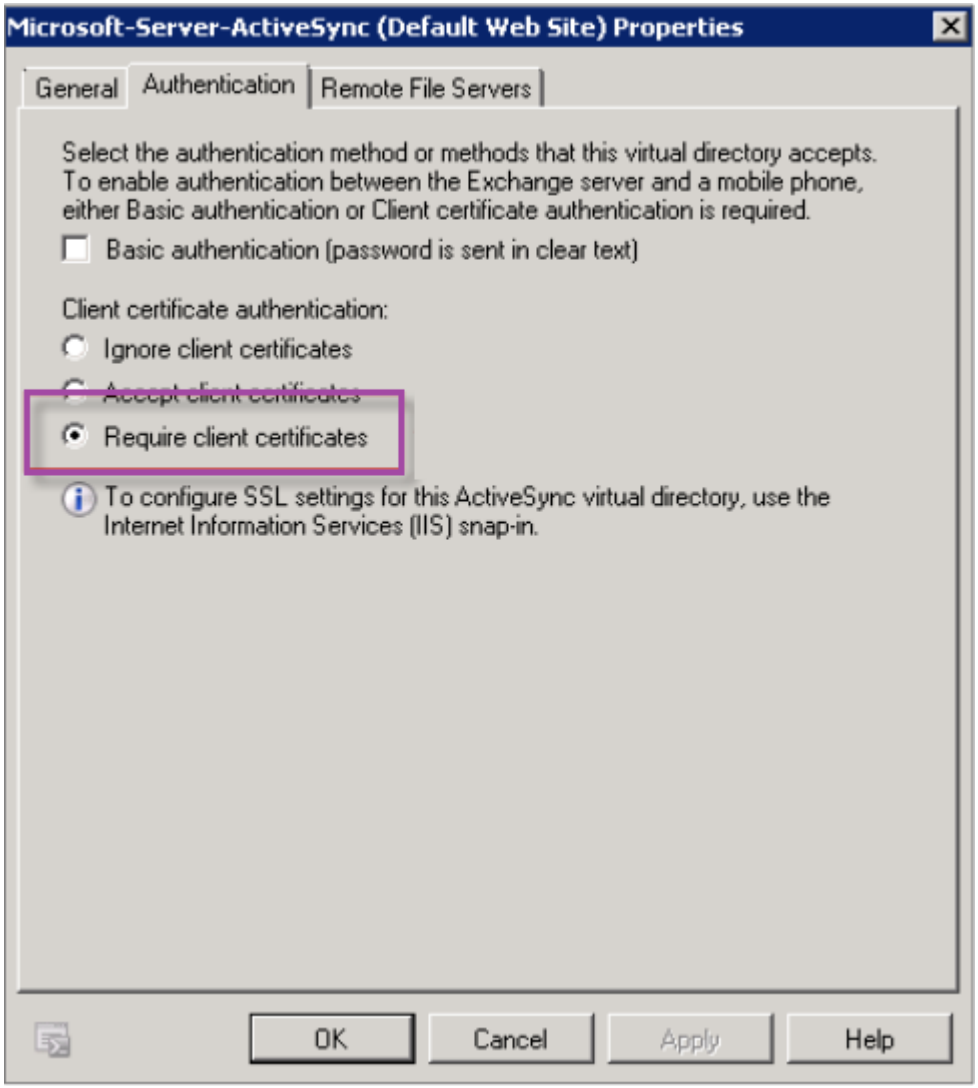
Résolution des problèmes de configuration du certificat client

Une fois la configuration précédente et la configuration Citrix Gateway effectuées, le workflow de l'utilisateur est le suivant :

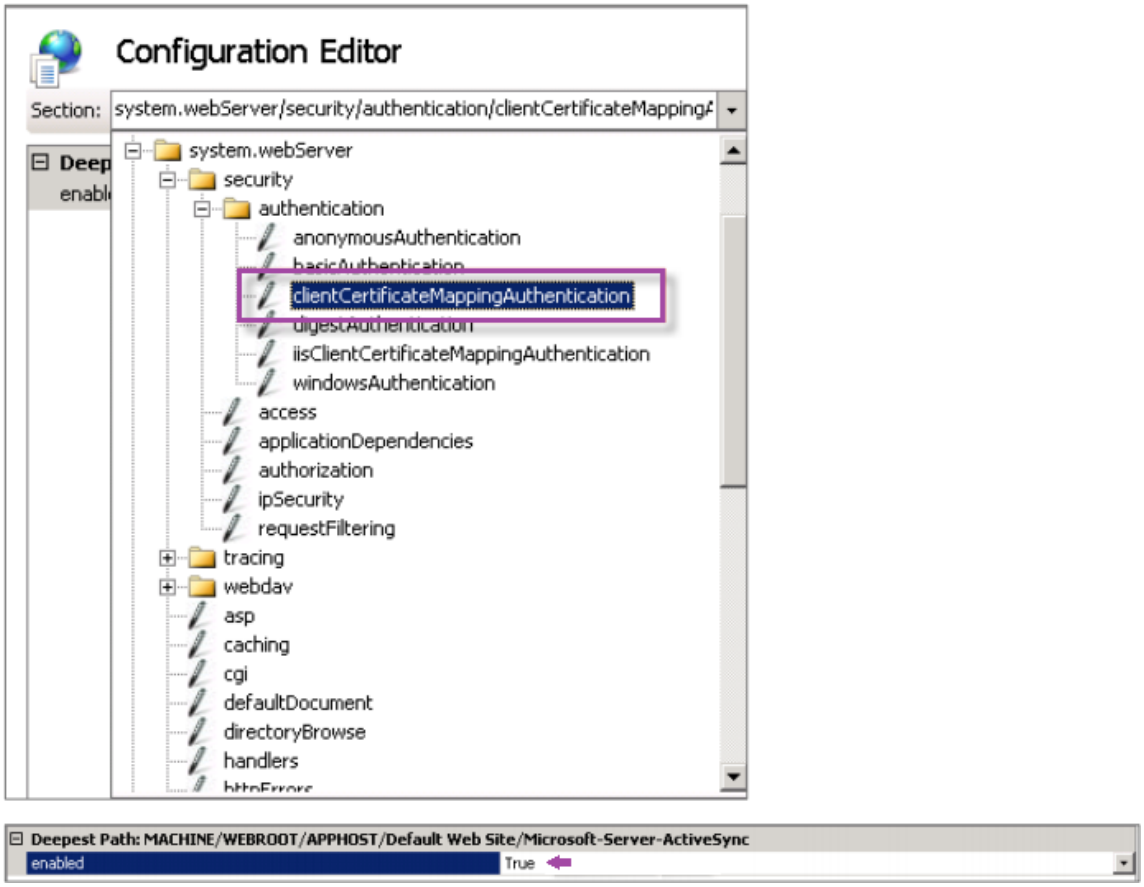
1. Les utilisateurs inscrivent leurs appareils mobiles.
2. XenMobile invite les utilisateurs à créer un code PIN Citrix.
3. Les utilisateurs sont redirigés vers XenMobile Store.
4. Lorsque les utilisateurs démarrent Secure Mail, XenMobile ne les invite pas à entrer d'informations d'identification afin de configurer leurs boîtes aux lettres. Au lieu de cela, Secure Mail demande le certificat client de Secure Hub et l'envoie à Microsoft Exchange Server pour authentification. Si XenMobile invite les utilisateurs à entrer des informations d'identification lorsqu'ils démarrent Secure Mail, vérifiez votre configuration.

Si les utilisateurs peuvent télécharger et installer Secure Mail, mais que Secure Mail ne termine pas la configuration durant la configuration de la boîte aux lettres :

1. Si Microsoft Exchange Server ActiveSync utilise des certificats de serveur SSL privé pour sécuriser le trafic, vérifiez que les certificats racine/intermédiaire sont installés sur l'appareil mobile.
2. Vérifiez que le type d'authentification sélectionné pour ActiveSync est **Exiger les certificats clients**.



3. Sur Microsoft Exchange Server, sélectionnez le site **Microsoft-Server-ActiveSync** pour vérifier que l'authentification par mappage de certificat client est activée. Par défaut, l'authentification par mappage de certificat client est désactivée. L'option figure sous **Éditeur de configuration > Sécurité > Authentification**.



Après avoir sélectionné **Vrai**, cliquez sur **Appliquer** pour que les modifications prennent effet.

4. Vérifiez les paramètres de Citrix Gateway dans la console XenMobile : assurez-vous que **Délivrer un certificat utilisateur pour l'authentification** est réglé sur **ACTIVÉ**, que le profil correct est sélectionné pour **Fournisseur d'identités**.

Pour déterminer si le certificat client a été délivré à un appareil mobile

1. Dans la console XenMobile, accédez à **Gérer > Appareils** et sélectionnez l'appareil.
2. Cliquez sur **Modifier** ou **Afficher plus**.
3. Accédez à la section **Groupes de mise à disposition** et recherchez cette entrée :

   Informations d'identification Citrix Gateway : Requested credential, CertId=

Pour vérifier si la négociation du certificat client est activée

1. Exécutez cette commande `netsh` pour afficher la configuration du certificat SSL qui est liée sur le site Web IIS :

   ```
   netsh http show sslcert
   ```


2. Si la valeur **Négocier le certificat client** est **désactivée**, exécutez la commande suivante pour l'activer :

```
netsh http delete sslcert ipport=0.0.0.0:443
```

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={
 app_id } certstorename=store_name verifyclientcertrevocation=Enable
 VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable
clientcertnegotiation=Enable
```

Par exemple :

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c54
 appid={ 4dc3e181-e14b-4a21-b022-59fc669b0914 } certstorename=ExampleCertStoreNam
 verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly
=Disable UsageCheck=Enable clientcertnegotiation=Enable
```

Si vous ne pouvez pas délivrer de certificats racine/intermédiaire à un appareil Windows Phone 8.1 via XenMobile :

- Envoyez des fichiers de certificats racine/intermédiaire (.cer) par e-mail à l'appareil Windows Phone 8.1 et installez-les directement.

Si Secure Mail n'est pas installé correctement sur Windows Phone 8.1, vérifiez les points suivants :

- Le fichier de jeton d'inscription d'application (.AETX) est délivré via XenMobile à l'aide de la stratégie d'hub d'entreprise.
- Le jeton d'inscription d'application a été créé à l'aide du même certificat d'entreprise que celui du fournisseur de certificats utilisé pour encapsuler Secure Mail et signer les applications Secure Hub.
- Le même ID d'éditeur est utilisé pour signer et encapsuler Secure Hub, Secure Mail et le jeton d'inscription d'application.

Entités PKI

January 10, 2022

Une configuration d'entité d'infrastructure de clé publique (PKI) XenMobile représente un composant réalisant des opérations PKI réelles (émission, révocation et informations d'état). Ces composants sont internes ou externes à XenMobile. Les composants internes sont appelés discrétionnaire. Les composants externes font partie de votre infrastructure d'entreprise.

XenMobile prend en charge les types d'entités PKI suivantes :

- PKI génériques (GPKI)

La prise en charge de protocoles PKI génériques par XenMobile Server inclut DigiCert Managed PKI.

- Services de certificats Microsoft
- Autorités de certification discrétionnaires (CA)

XenMobile prend en charge les serveurs d'autorité de certification suivants :

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Concepts de PKI communs

Quel que soit son type, chaque entité PKI possède un sous-ensemble des fonctionnalités suivantes :

- **Signer :** émission d'un nouveau certificat, basé sur une demande de signature de certificat (CSR).
- **Récupérer :** récupération d'un certificat existant et d'une paire de clés.
- **Révoquer :** révocation d'un certificat client.

À propos des certificats CA

Lorsque vous configurez une entité PKI, informez XenMobile de la nature du certificat d'autorité de certification qui est le signataire des certificats émis par (ou récupérés depuis) cette entité. Cette entité PKI peut renvoyer des certificats signés (récupérés ou nouvellement signés) par un certain nombre d'autorités de certification différentes.

Fournissez le certificat de chacune de ces autorités de certification dans le cadre de la configuration de l'entité PKI. Pour ce faire, chargez les certificats sur XenMobile puis référencez-les dans l'entité PKI. Pour les autorités de certification discrétionnaires, le certificat est implicitement le certificat de l'autorité de certification signataire. Pour les entités externes, vous devez spécifier le certificat manuellement.

> **Important :**
>
> Lorsque vous créez un modèle d'entité Services de certificats Microsoft, évitez les problèmes d'authentification possibles avec des appareils inscrits ; n'utilisez pas de caractères spéciaux dans le nom du modèle. Par exemple, n'utilisez pas : `! : $ ( )## % + * ~ ? | { } [ ]`

PKI générique

Le protocole PKI générique (GPKI) est un protocole XenMobile propriétaire exécuté sur une couche du service Web SOAP qui permet un interfaçage avec différentes solutions PKI. Le protocole GPKI définit

les trois opérations PKI fondamentales suivantes :

- **Signer :** la carte peut prendre des demandes de signature de certificat (CSR), les transmettre à la PKI et retourner des certificats nouvellement signés.
- **Récupérer :** la carte peut récupérer des certificats existants et des paires de clés (selon les paramètres d'entrée) depuis la PKI.
- **Révoquer :** la carte peut entraîner la révocation d'un certificat donné par la PKI.

La carte GPKI se trouve en bout du protocole GPKI. La carte convertit les opérations fondamentales pour le type de PKI spécifique pour lequel elle a été créée. Par exemple, il existe des cartes GPKI pour RSA et Entrust.

La carte GPKI, en tant que point de terminaison des services Web SOAP, publie une définition WSDL auto-descriptive. La création d'une entité GPKI PKI équivaut à fournir cette définition WSDL à XenMobile, soit par le biais d'une adresse URL soit en chargeant le fichier lui-même.

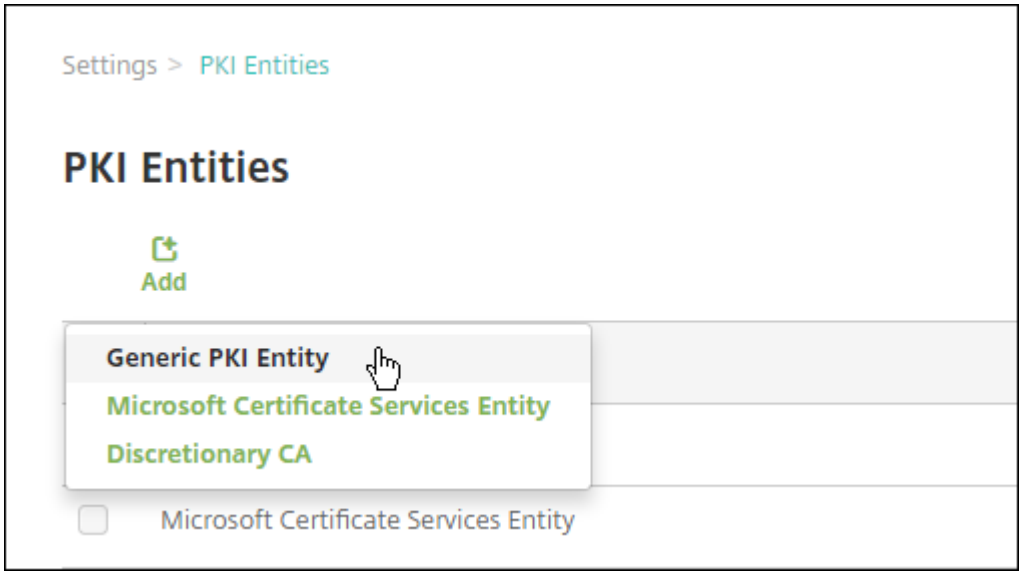
La prise en charge de chaque opération PKI dans une carte est facultative. Si une carte prend en charge une opération donnée, on considère qu'elle dispose de la capacité correspondante (signature, récupération ou révocation). Chacune de ces fonctionnalités peut être associée à un ensemble de paramètres utilisateur.

Les paramètres utilisateur sont des paramètres que la carte GPKI définit pour une opération spécifique et pour lesquels vous devez fournir des valeurs à XenMobile. XenMobile analyse le fichier WSDL pour déterminer les opérations prises en charge par la carte et les paramètres requis par la carte pour chacune des opérations. Si vous le souhaitez, utilisez l'authentification de client SSL pour sécuriser la connexion entre XenMobile et la carte GPKI.

Pour ajouter une PKI générique

1. Dans la console Web XenMobile, cliquez sur **Paramètres > Entités PKI**.
2. Sur la page **Entités PKI**, cliquez sur **Ajouter**.

   Un menu des types d'entité PKI s'affiche.



3. Cliquez sur **Entité PKI générique**.

   La page Entité PKI générique : informations générales s'affiche.

4. Sur la page **Entité PKI générique : informations générales**, procédez comme suit :

   - **Nom :** entrez un nom descriptif pour l'entité PKI.
   - **URL du WSDL :** entrez l'emplacement du WSDL décrivant la carte.
   - **Type d'authentification :** cliquez sur la méthode d'authentification à utiliser.
   - **Aucune**
   - **HTTP basique :** fournissez le nom d'utilisateur et mot de passe requis pour se connecter à la carte.
   - **Certificat client :** sélectionnez le certificat client SSL correct.

5. Cliquez sur **Suivant**.

   La page Entité PKI générique : capacité de l'adaptateur s'affiche.

6. Sur la page **Entité PKI générique : capacité de l'adaptateur**, passez en revue les capacités et les paramètres associés à votre carte et cliquez sur **Suivant**.

   La page **Entité PKI générique : émission de certificats CA** s'affiche.

7. Sur la page Entité PKI générique : émission de certificats CA, sélectionnez les certificats que vous voulez utiliser pour l'entité.

   Bien que les entités puissent retourner des certificats signés par des autorités de certification différentes, la même autorité de certification doit signer tous les certificats obtenus via un fournisseur de certificats donné. Par conséquent, lorsque vous configurez le paramètre **Fournisseur d'identités**, sur la page **Distribution**, sélectionnez l'un des certificats configuré ici.

8. Cliquez sur **Enregistrer**.

   L'entité s'affiche sur le tableau Entités PKI.

DigiCert Managed PKI

La prise en charge de protocoles PKI génériques par XenMobile Server inclut DigiCert Managed PKI, également connu sous le nom MPKI. Cette section décrit comment configurer Windows Server et XenMobile Server pour DigiCert Managed PKI.

Conditions préalables

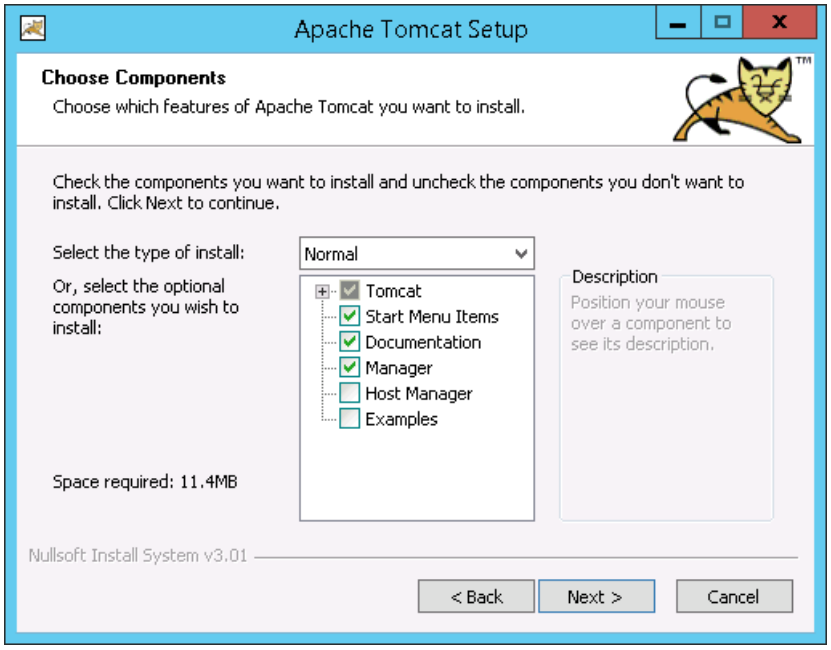
- Accès à l'infrastructure de DigiCert Managed PKI
- Un serveur Windows Server 2012 R2 avec les composants suivants, comme décrit dans cet article :
  - Java
  - Apache Tomcat
  - DigiCert PKI Client
  - Portecle
- Accès au site de téléchargement XenMobile

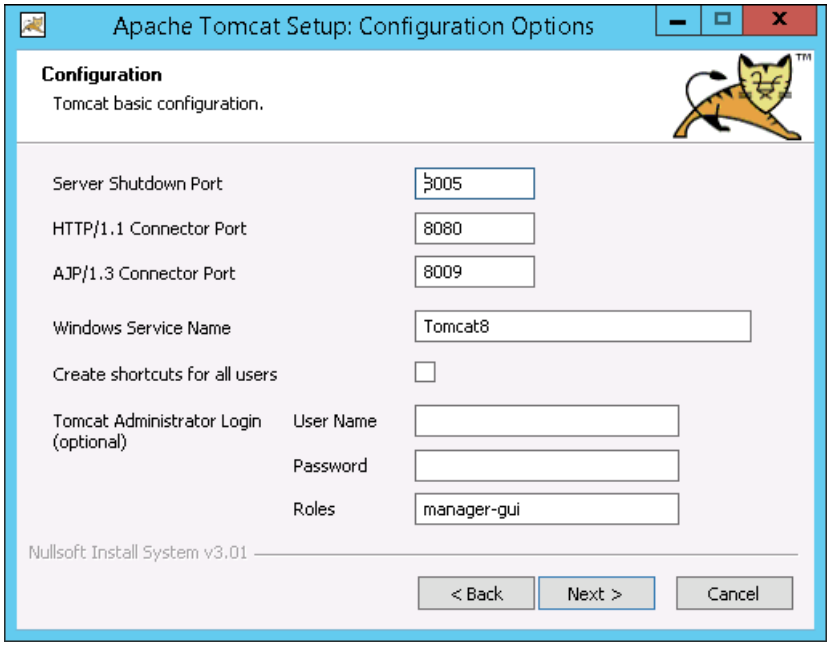
Installer Java sur Windows Server

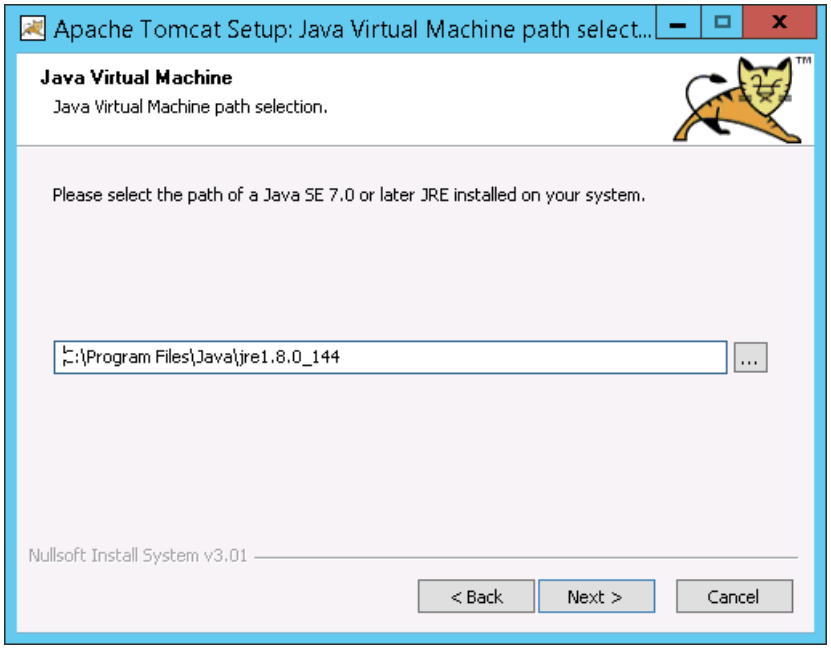
Téléchargez Java à partir de https://java.com/en/download/faq/java_win64bit.xml, puis installez le programme. Dans la boîte de dialogue Avertissement de sécurité, cliquez sur **Exécuter**.

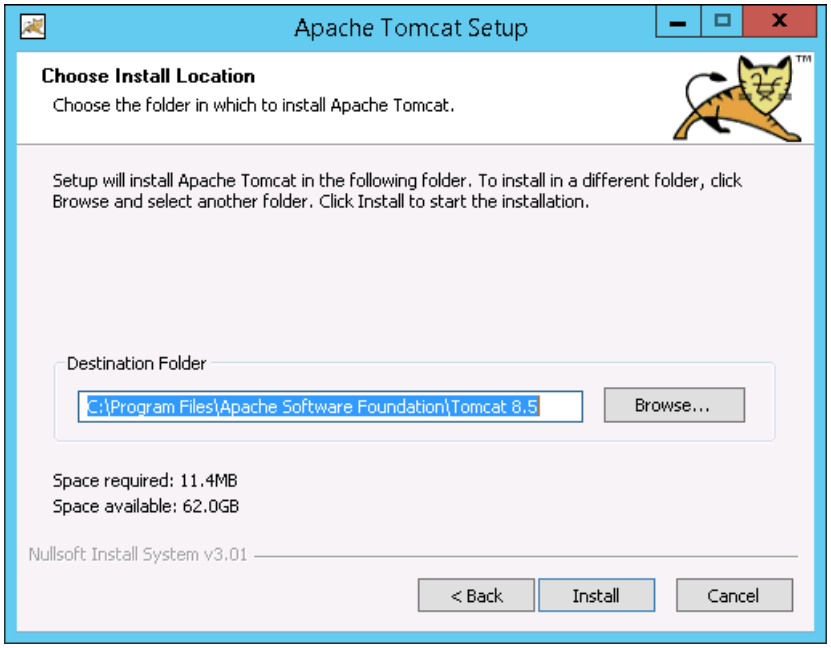
Installer Apache Tomcat sur Windows Server

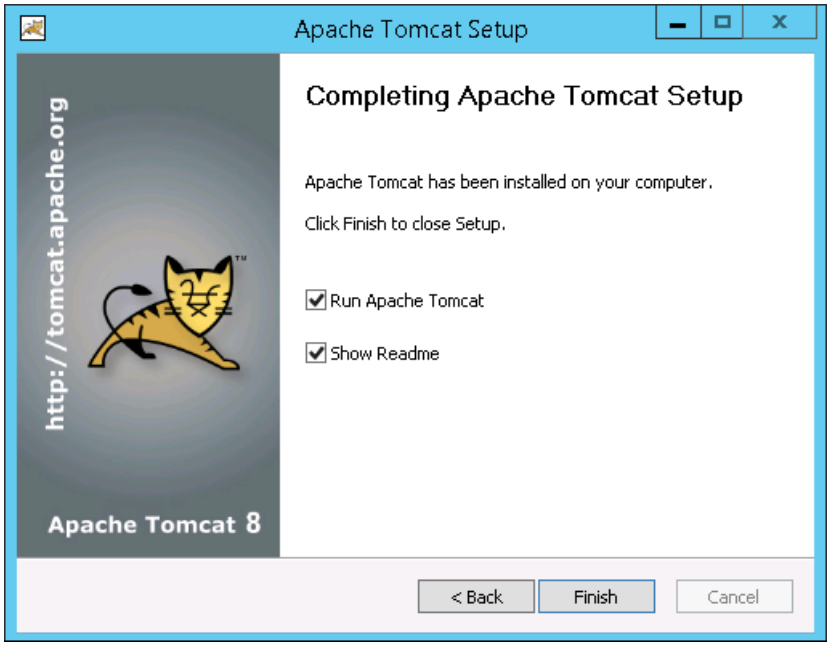
Téléchargez le programme d'installation du Service Windows 32 bits/64 bits d'Apache Tomcat à partir de https://tomcat.apache.org/download-80.cgi et installez. Dans la boîte de dialogue Avertissement de sécurité, cliquez sur **Exécuter**. Effectuez la configuration d'Apache Tomcat, en utilisant les exemples suivants comme guide.



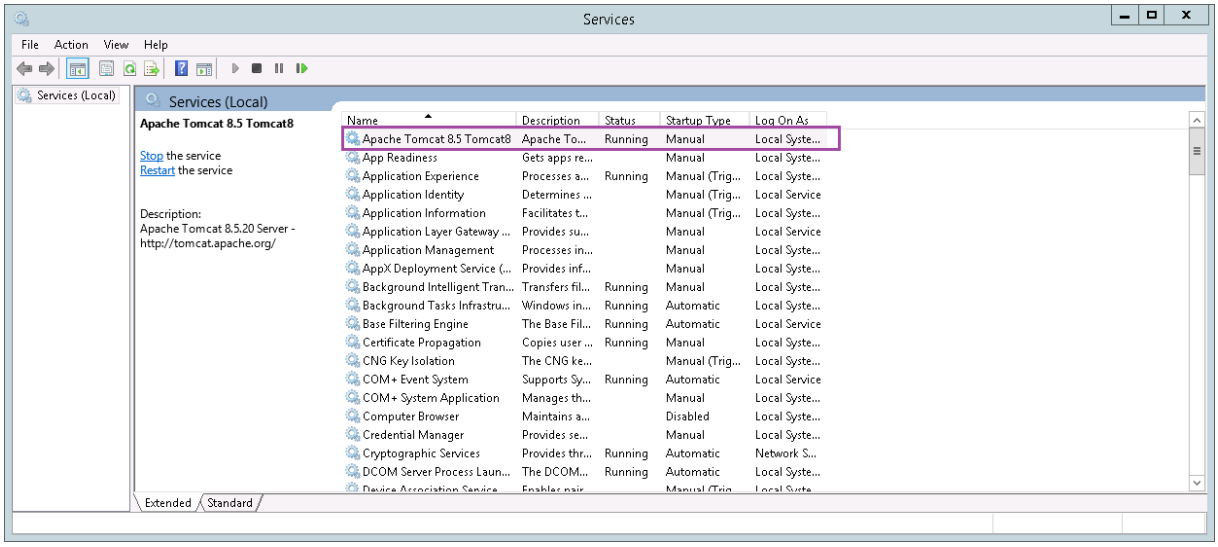


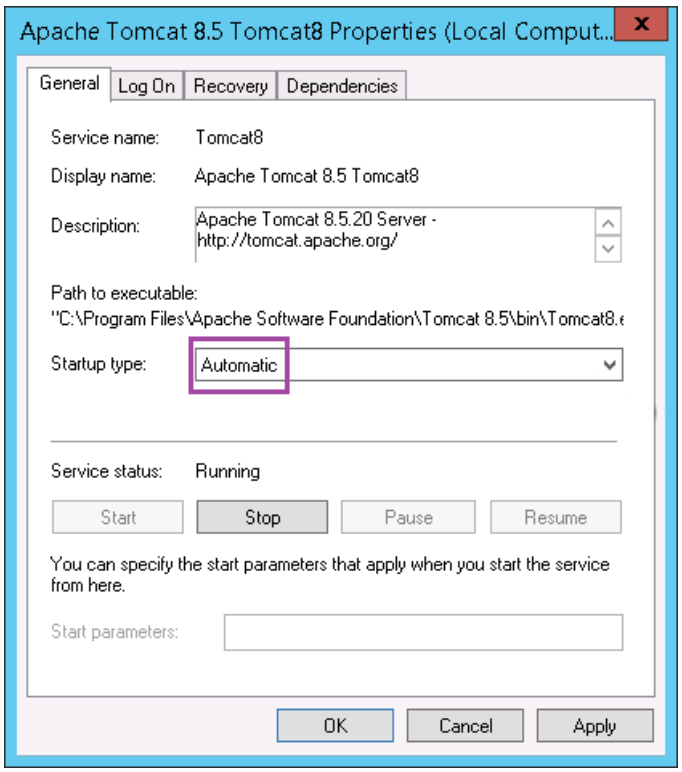






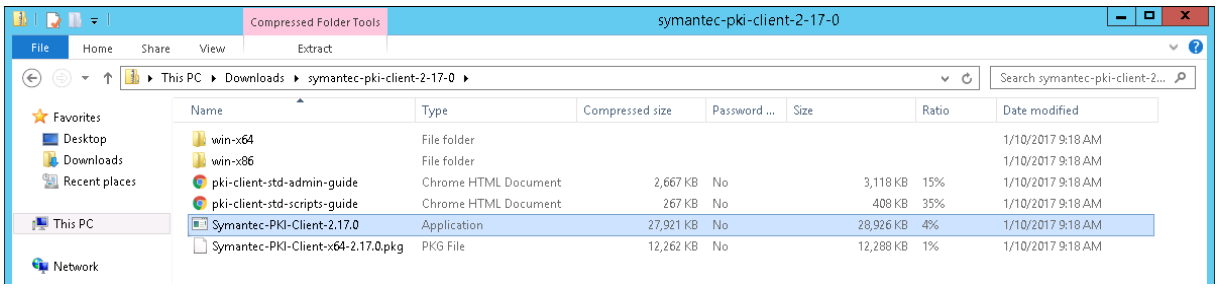
Ensuite, accédez à Services Windows et modifiez **Type de démarrage**, de **Manuel** à **Automatique**.

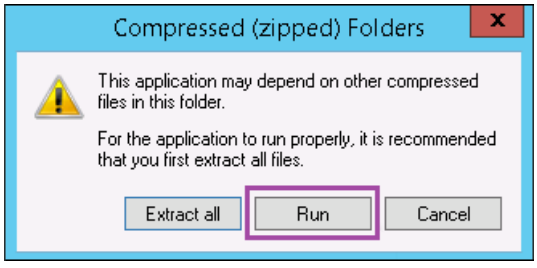




Installer DigiCert PKI Client sur Windows Server

Téléchargez le programme d'installation à partir de la console PKI Manager. Si vous n'avez pas accès à cette console, téléchargez le programme d'installation à partir de la page de support de DigiCert, Comment télécharger DigiCert PKI Client. Décompressez et exécutez le programme d'installation.





Dans la boîte de dialogue Avertissement de sécurité, cliquez sur **Exécuter**. Suivez les instructions du programme d'installation pour effectuer l'installation. Lorsque le programme d'installation est

terminé, il vous invite à redémarrer.

Installer Portecle sur Windows Server

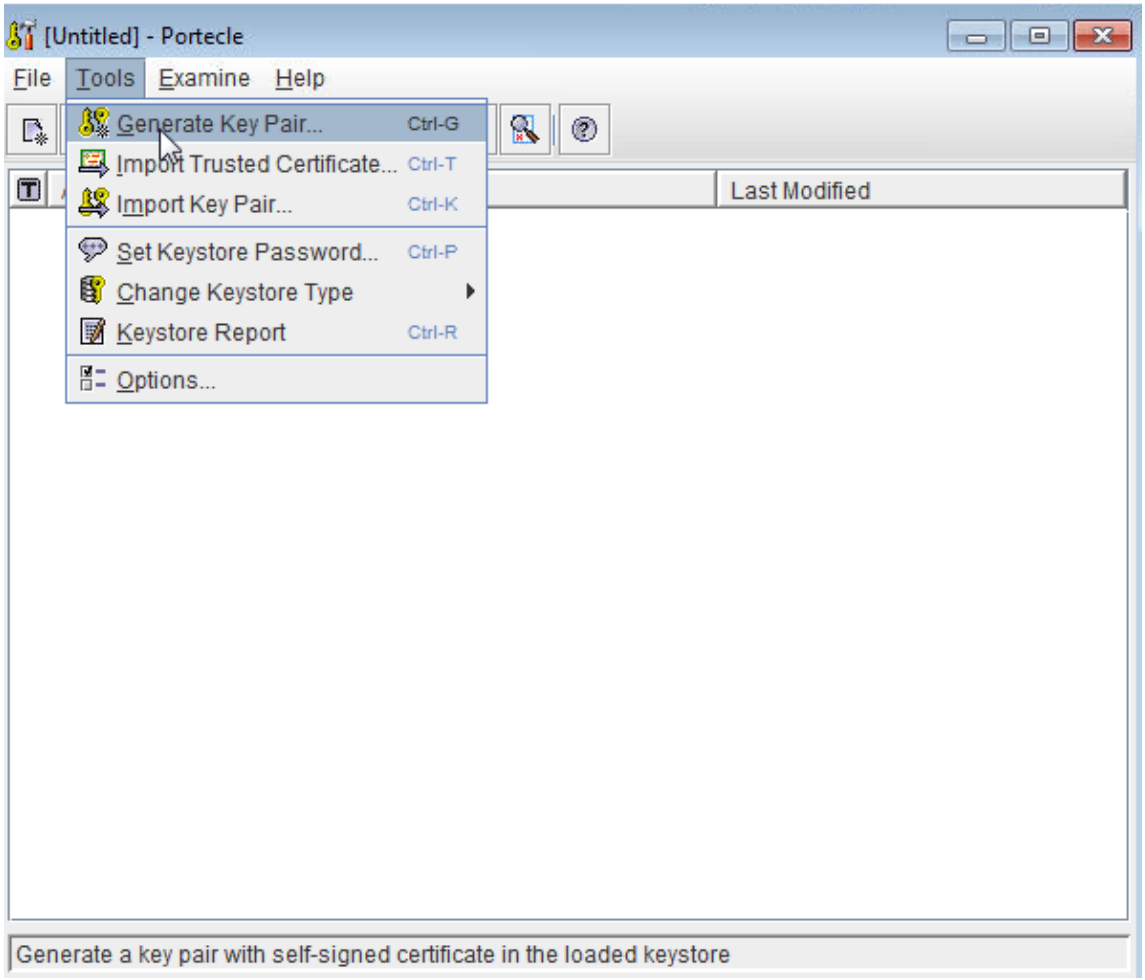
Téléchargez le programme d'installation à partir de https://sourceforge.net/projects/portecleinstall/files/, puis décompressez et exécutez le programme d'installation.

Générer le certificat d'autorité d'inscription (RA) pour DigiCert Managed PKI

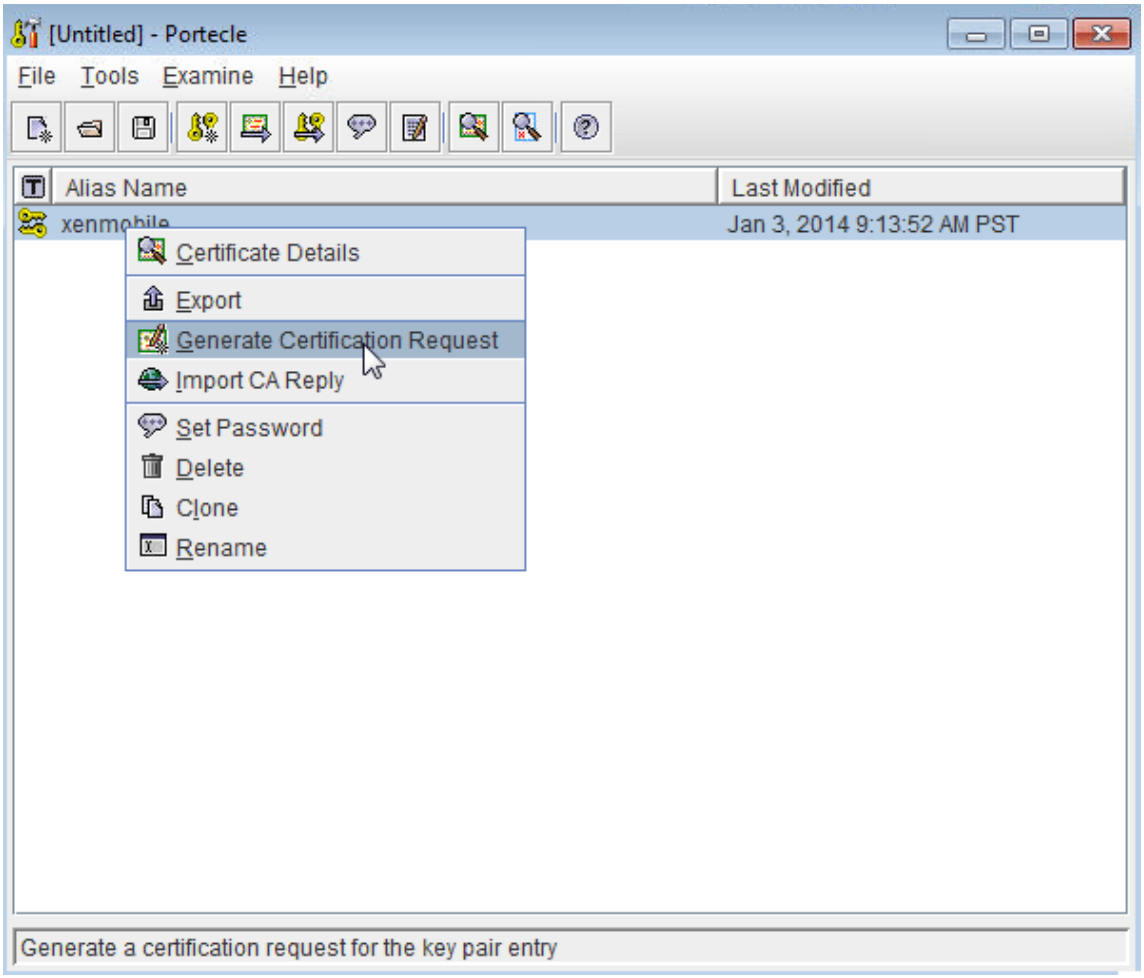
Le magasin de clés pour l'authentification du certificat client est contenu dans un certificat d'autorité d'inscription (RA), appelé RA.jks. Les étapes suivantes décrivent comment générer le certificat à l'aide de Portecle. Vous pouvez également générer le certificat RA à l'aide de la ligne de commande Java.

Cet article explique également comment télécharger les certificats RA et publics.

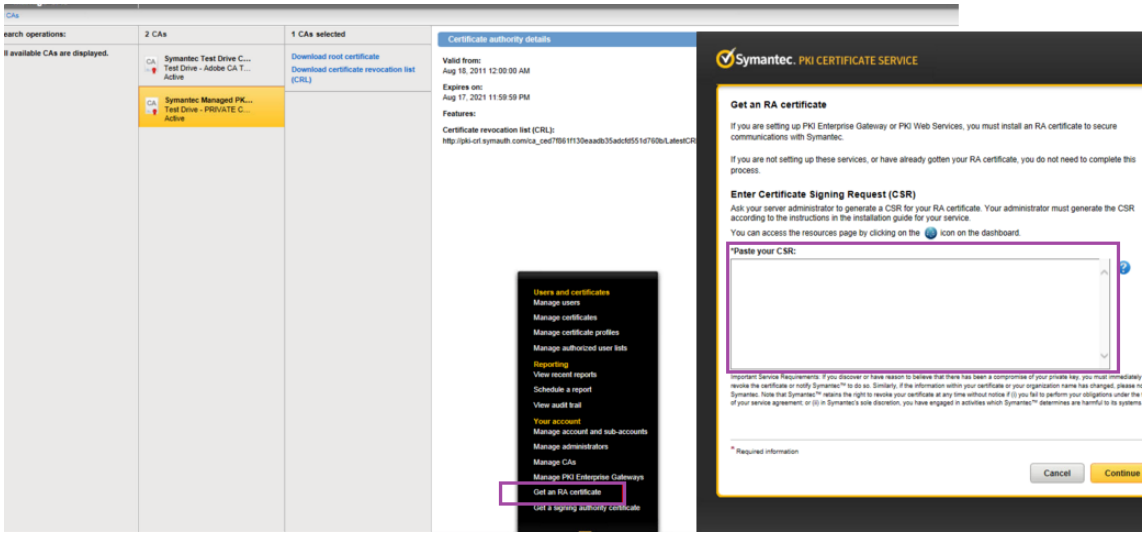
1. Dans Portecle, accédez à **Tools > Generate Key Pair**, fournissez les informations requises et générez la paire de clés.



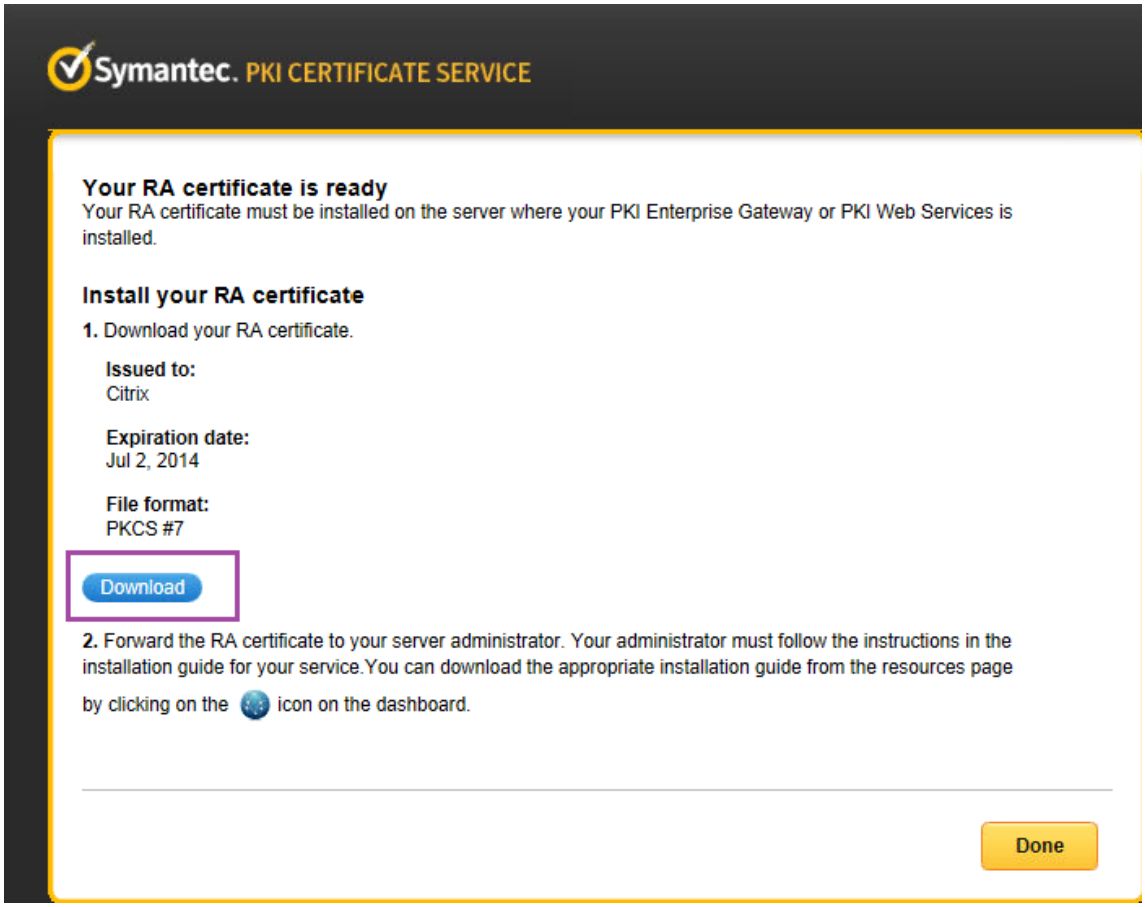
2. Cliquez avec le bouton droit de la souris sur la paire de clés, puis cliquez sur **Generate Certification Request**.



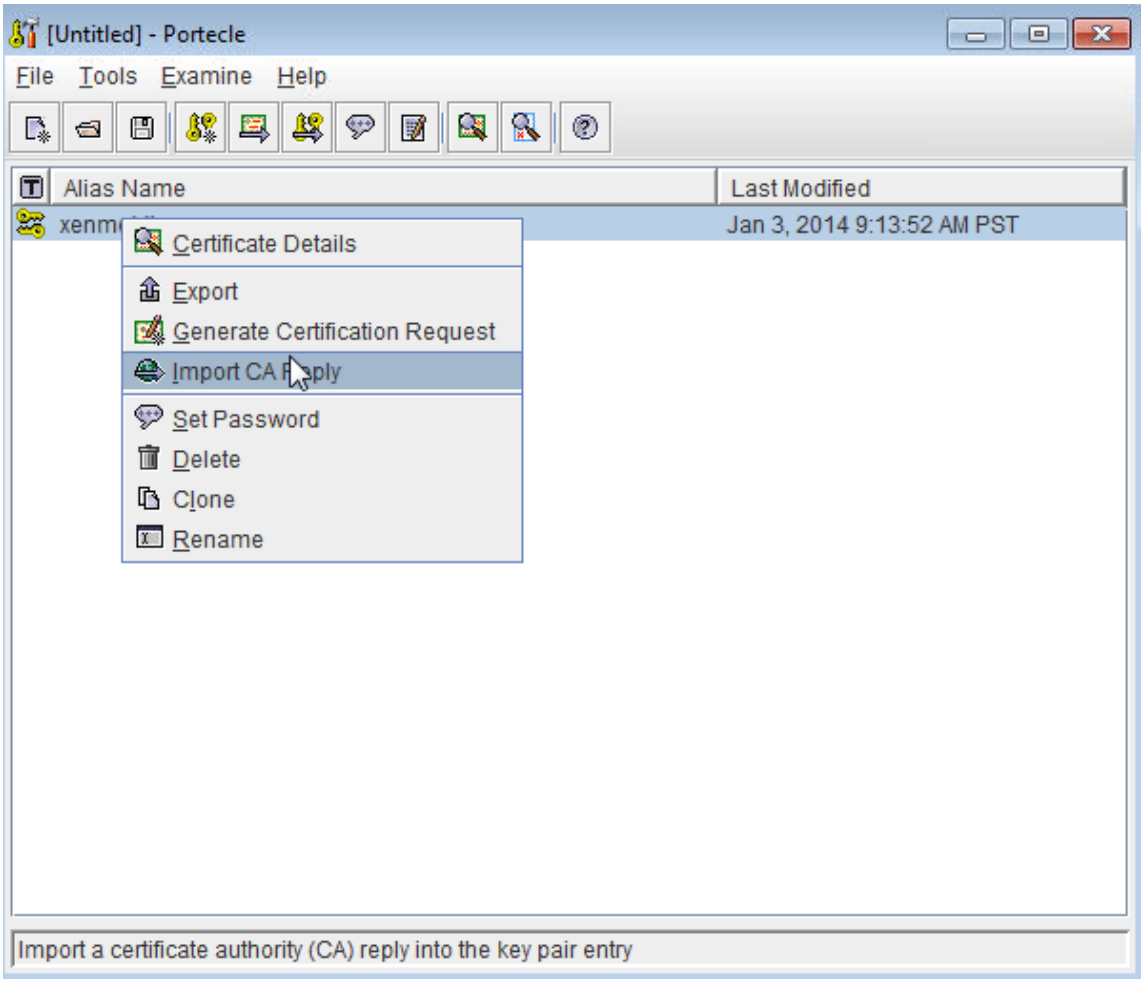
3. Copiez la requête de signature de certificat (CSR).
4. Dans DigiCert PKI Manager, générez un certificat RA : cliquez sur **Settings**, puis sur **Get a RA Certificate**, collez le fichier CSR, puis cliquez sur **Continue**.



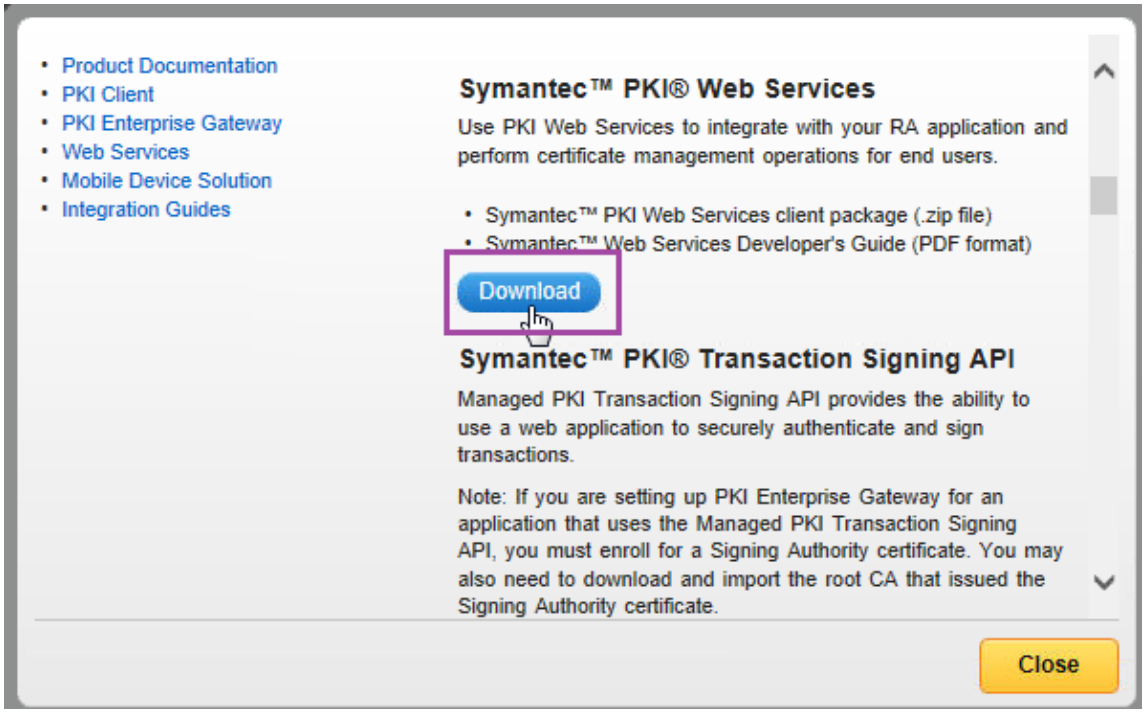
5. Cliquez sur **Download** pour télécharger le certificat RA généré.



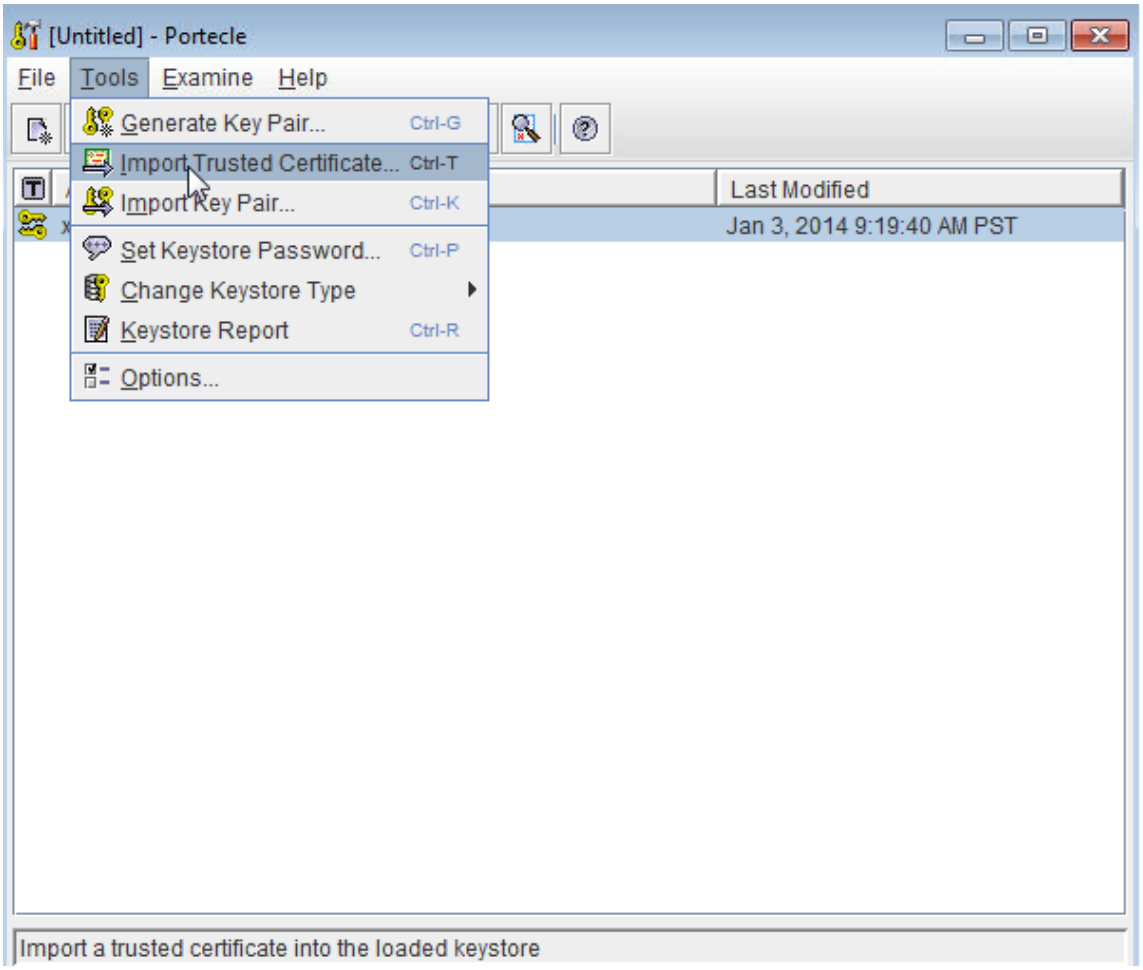
6. Dans Portecle, importez le certificat RA : cliquez avec le bouton droit de la souris sur la paire de clés, puis cliquez sur **Import CA Reply**.



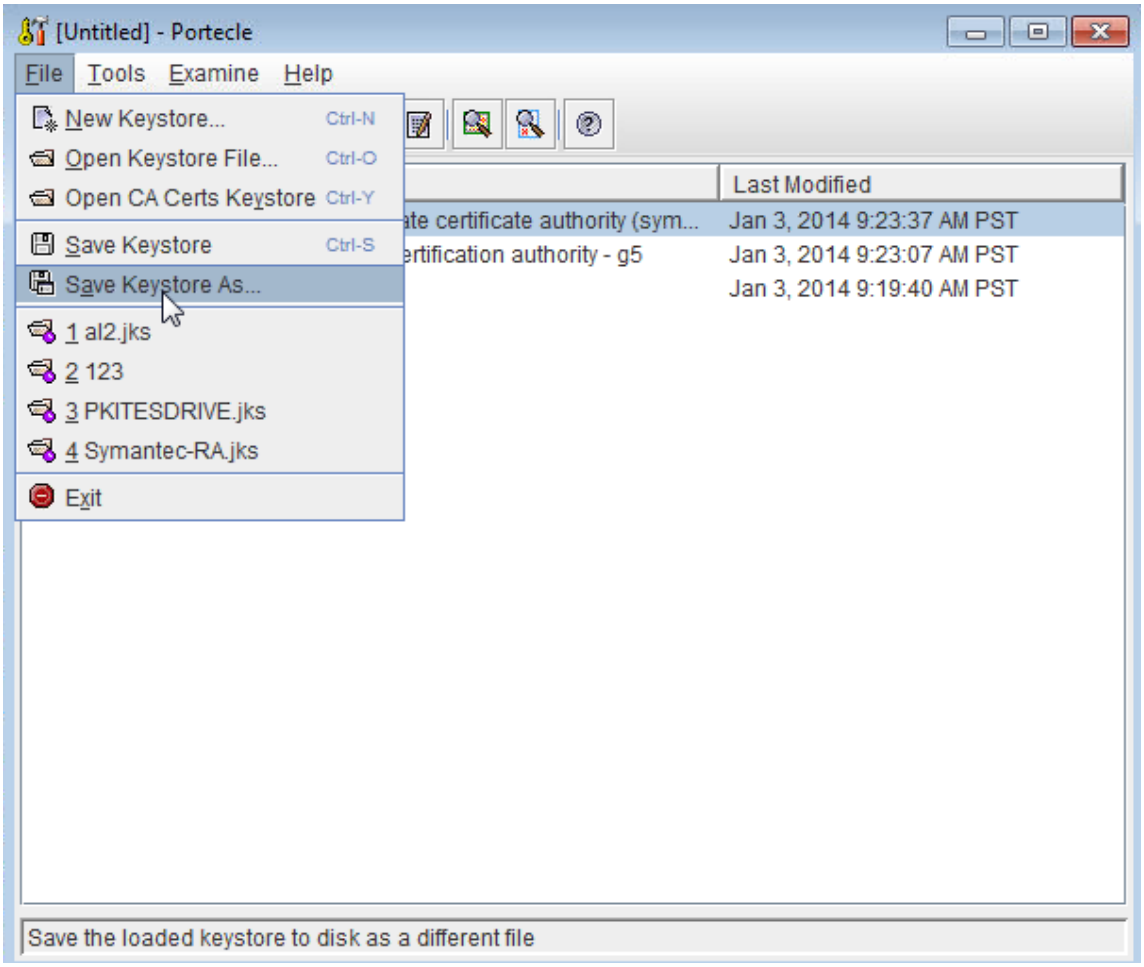
7. Dans DigiCert PKI Manager : accédez à **Resources > Web Services** et téléchargez les certificats d'autorité de certification.



8. Dans Portecle, importez les certificats racine et intermédiaire RA dans le magasin de clés : **Tools > Import Trusted Certificates**.



9. Après avoir importé les autorités de certification, enregistrez le magasin de clés en tant que RA.jks dans le dossier C:\DigiCert sur le serveur Windows.



Configurer la carte DigiCert PKI sur Windows Server

1. Connectez-vous à Windows Server en tant qu'administrateur.
2. Chargez le fichier RA.jks que vous avez généré dans la section précédente. Chargez également les certificats publics (cacerts.jks) pour votre serveur Symantec MPKI.
3. Téléchargez le fichier de la carte PKI Symantec :
   a) Accédez à https://www.citrix.com/downloads.
   b) Accédez à **Citrix Endpoint Management (et Citrix XenMobile Server) > XenMobile Server (local) > Logiciel produit > XenMobile Server 10 > Outils**.
   c) Sur la vignette **Symantec PKI Adapter**, cliquez sur **Download File**.
   d) Décompressez le fichier et copiez ces fichiers sur le lecteur C: du serveur Windows :
      - custom_gpki_adapter.properties
      - Symantec.war

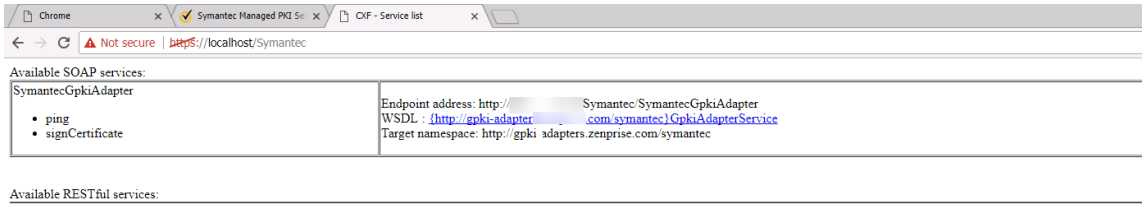
4. Ouvrez custom_gpki_adapter.properties dans Bloc-notes et modifiez les valeurs suivantes :

```
Gpki.CaSvc.Url=https://<managed PKI URL>

# keystore for client-cert auth

keyStore=C:\Symantec\RA.jks

# truststore for server with self-signed root CA

trustStore=C:\Symantec\cacerts.jks
<!--NeedCopy-->
```

5. Copiez Symantec.war sous le dossier <tomcat dir>\webapps, puis démarrez Tomcat.
6. Vérifiez que l'application est déployée : ouvrez un navigateur web et accédez à https://localhost/Symantec.
7. Accédez au dossier <tomcat dir>\webapps\Symantec\WEB-INF\classes et modifiez gpki_adapter.properties. Modifiez la propriété **CustomProperties** pour la faire pointer vers le fichier custom_gpki_adapter sous le dossier C:\Symantec :

   CustomProperties=C:\\Symantec\\custom_gpki_adapter.properties

8. Redémarrez Tomcat, accédez à https://localhost/Symantec, puis copiez l'adresse du point de terminaison. Dans la section suivante, vous collez cette adresse lors de la configuration de la carte PKI.

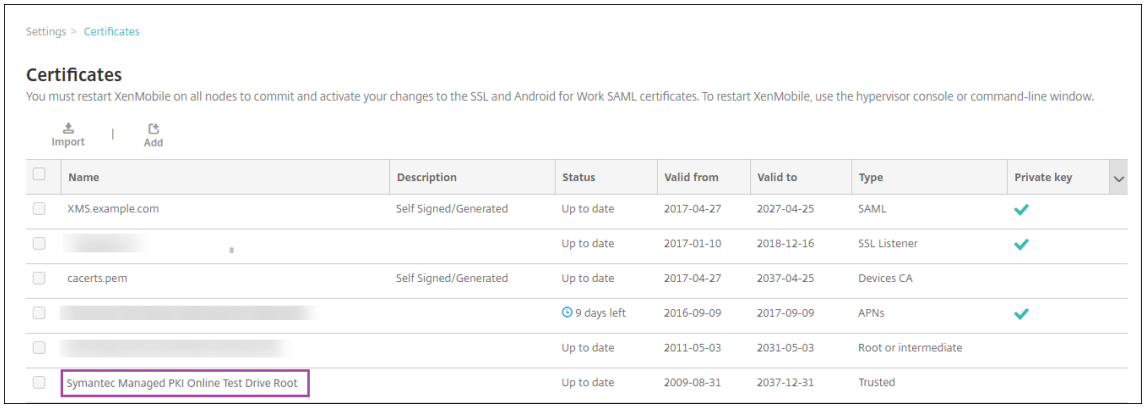


Configurer XenMobile Server pour DigiCert Managed PKI

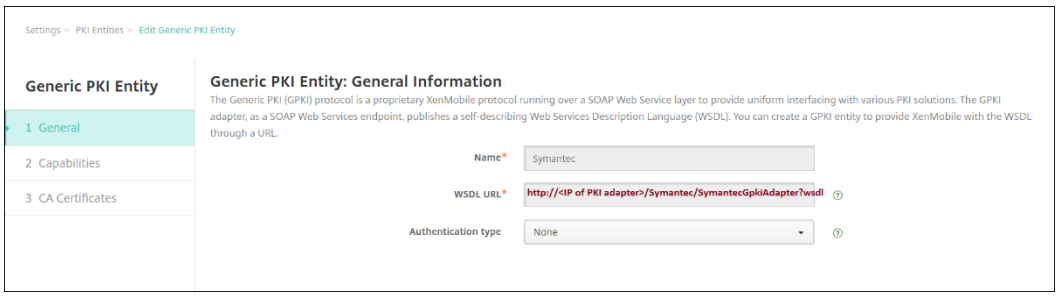
Effectuez l'installation de Windows Server avant d'effectuer la configuration XenMobile Server suivante.

Pour importer les certificats d'autorité de certification de DigiCert et configurer l'entité PKI

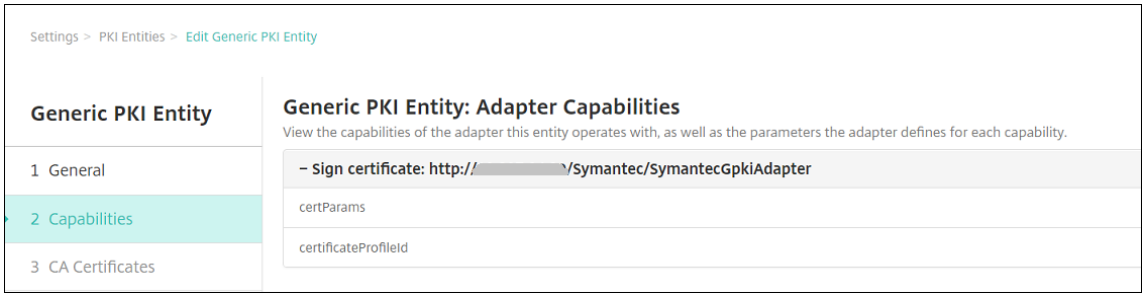
1. Importez les certificats d'autorité de certification DigiCert qui émettent le certificat de l'utilisateur final : dans la console XenMobile Server, accédez à **Paramètres > Certificats** et cliquez sur **Importer**.



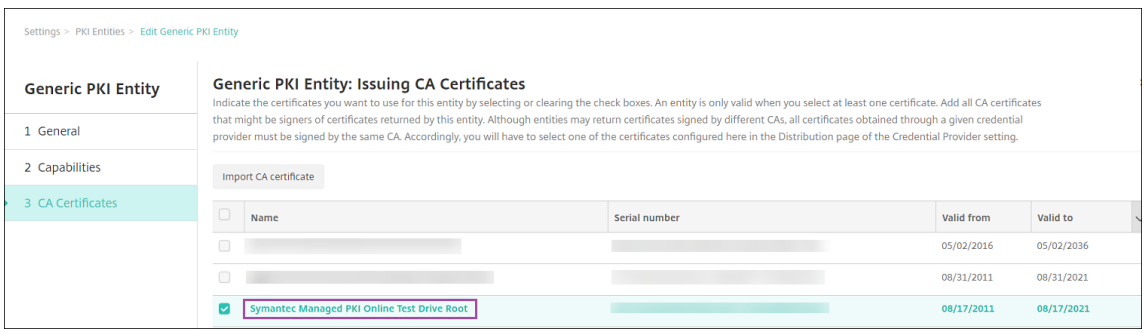
2. Ajoutez et configurez l'entité PKI : accédez à **Paramètres > Entités PKI**, cliquez sur **Ajouter**, puis choisissez **Entité PKI générique**. Dans **URL du WSDL**, collez l'adresse de point de terminaison que vous avez copiée lors de la configuration de la carte PKI dans la section précédente, puis ajoutez `?wsdl` comme illustré ci-dessous.



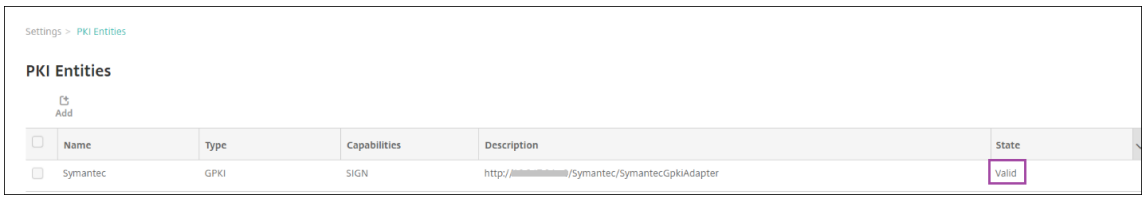
3. Cliquez sur **Suivant**. XenMobile renseigne les noms des paramètres depuis le WSDL.



4. Cliquez sur **Suivant**, sélectionnez le certificat CA correct, puis cliquez sur **Enregistrer**.

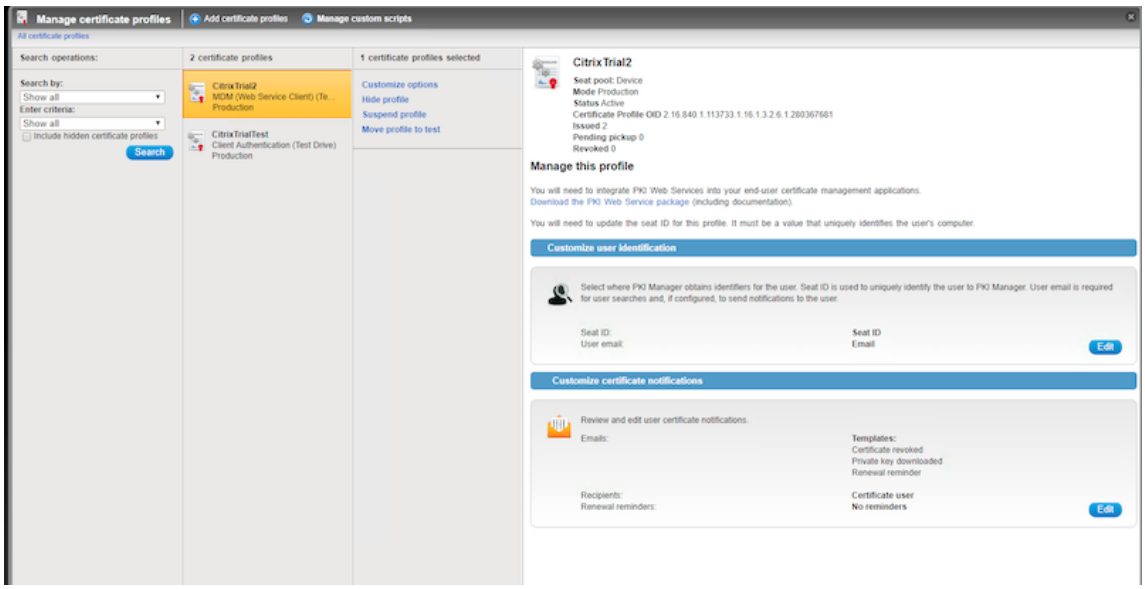


5. Sur la page **Paramètres > Entités PKI**, vérifiez que l'**état** de l'entité PKI que vous avez ajoutée est défini sur **valide**.



Pour créer le fournisseur d'informations d'identification pour DigiCert Managed PKI

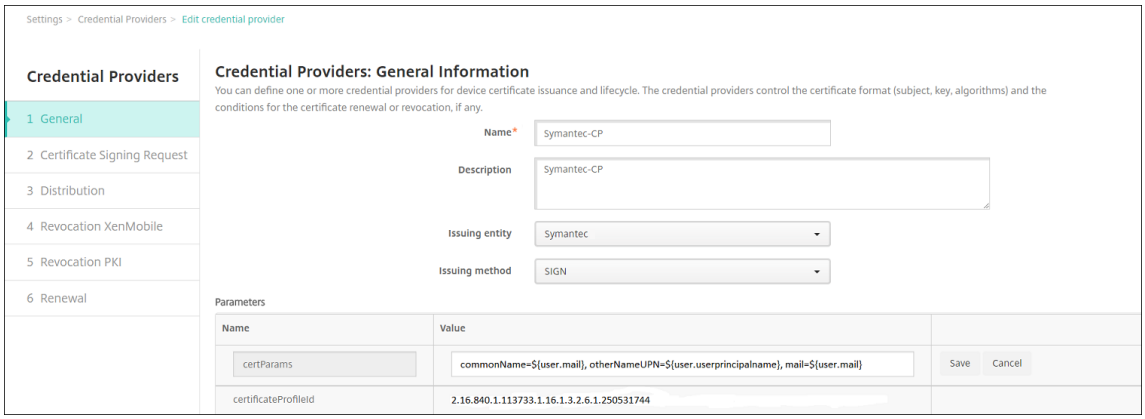
1. Dans la console DigiCert PKI Manager, copiez le **Certificate Profile OID** à partir du modèle de certificat.



2. Dans la console de XenMobile Server, accédez à **Paramètres > Fournisseurs d'identités**, cliquez sur **Ajouter**, puis configurez les paramètres comme suit.

   - **Nom :** entrez un nom unique pour la nouvelle configuration du fournisseur. Ce nom sera utilisé pour faire référence à la configuration dans d'autres parties de la console XenMobile.
   - **Description :** décrivez le fournisseur d'identités. Bien que ce champ soit facultatif, une description peut être utile pour vous fournir des détails sur le fournisseur d'identités.
   - **Entité émettrice :** choisissez l'entité qui émet le certificat.
   - **Méthode d'émission :** choisissez **Signer** comme méthode que le système utilise pour obtenir des certificats client auprès de l'entité configurée.
   - **certParams :** ajoutez la valeur suivante : **commonName=${user.mail},otherNameUPN=${user.userp**

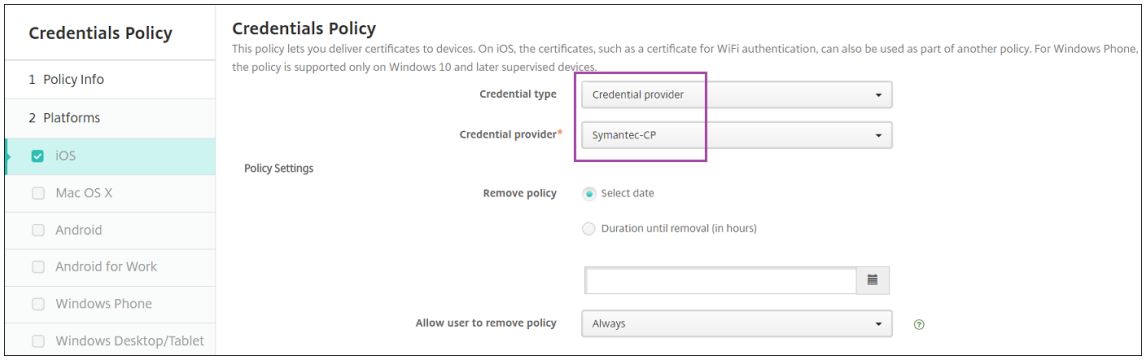
- **certificateProfileid :** collez l'entrée Certificate Profile OID que vous avez copiée à l'étape 1.



3. Cliquez sur **Suivant**. Sur chacune des pages restantes (Demande de signature de certificat jusqu'à Renouvellement), acceptez les paramètres par défaut. Lorsque vous avez terminé, cliquez sur **Enregistrer**.

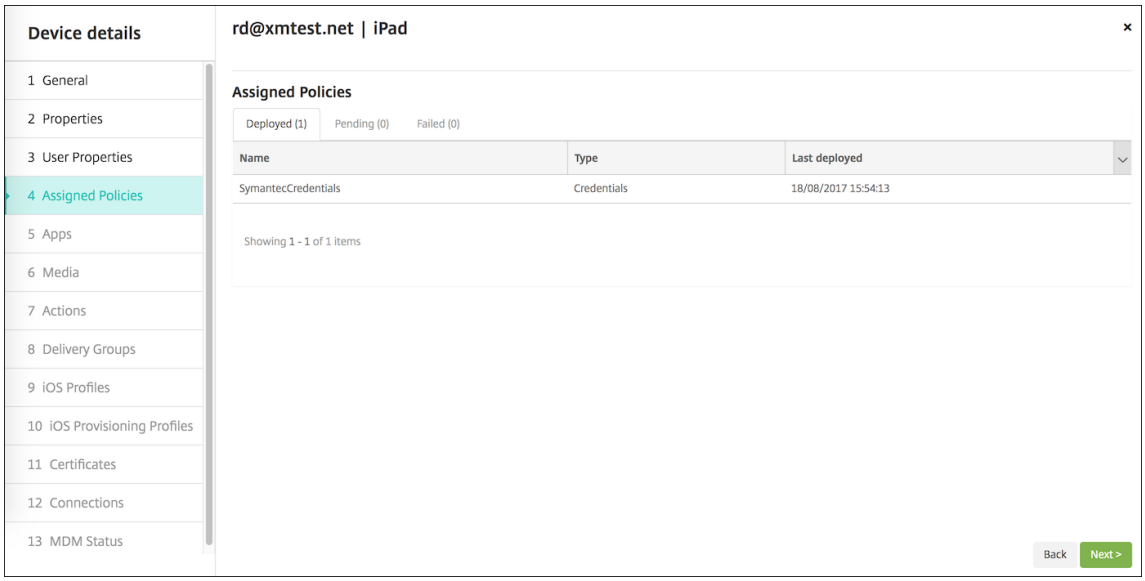
Pour tester et résoudre les problèmes de configuration

1. Créez une stratégie Informations d'identification : accédez à **Configurer > Stratégies d'appareil**, cliquez sur **Ajouter**, commencez à taper **Informations d'identification**, puis cliquez sur **Informations d'identification**.
2. Spécifiez un **nom de stratégie**.
3. Configurez les paramètres de plate-forme comme suit :
   - **Type de certificat :** choisissez **Fournisseur d'identités**.
   - **Fournisseur d'informations d'identification :** choisissez le fournisseur DigiCert.

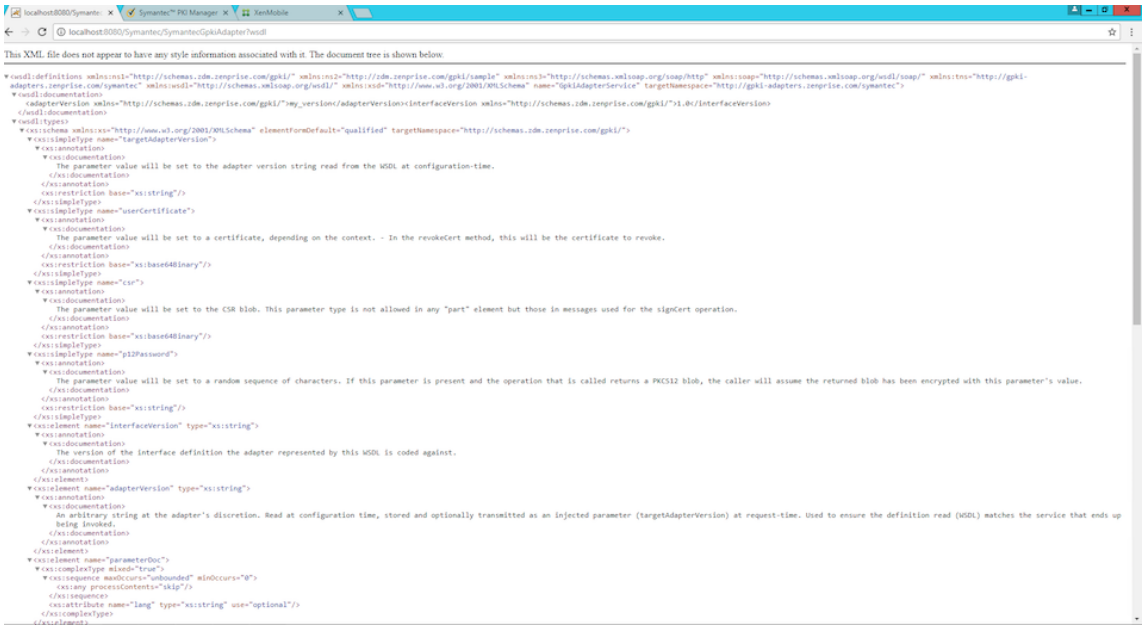


4. Après avoir terminé la configuration de la plate-forme, passez à la page **Attribution**, attribuez la stratégie à des groupes de mise à disposition, puis cliquez sur **Enregistrer**.
5. Pour vérifier si la stratégie est déployée sur l'appareil, accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Modifier** et cliquez sur **Stratégies attribuées**. L'exemple suivant illustre

un déploiement réussi de stratégie.



Si la stratégie n'a pas été déployée, connectez-vous à Windows Server et vérifiez si le WSDL est chargé correctement.



Pour obtenir des informations de dépannage supplémentaires, vérifiez les journaux Tomcat dans <tomcat dir>\logs\catalina.<current date>.

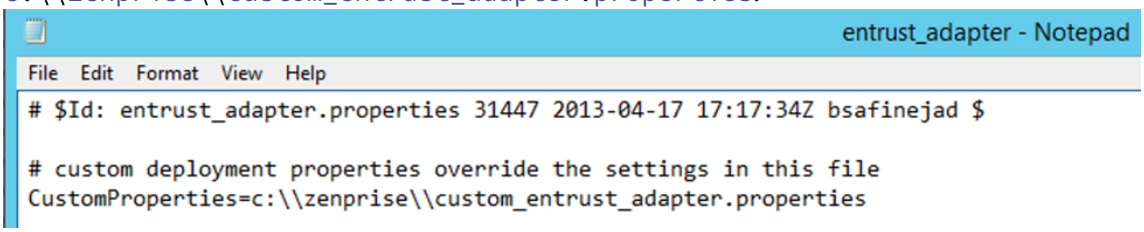
Carte Entrust PKI

Au lieu d'utiliser DigiCert Managed PKI, vous pouvez installer la carte Entrust PKI. Avant d'installer la carte, reportez-vous aux étapes d'installation de Java et de Apache Tomcat sur Windows Server dans

la section DigiCert Managed PKI de cet article.

Installer la carte Entrust PKI

1. Téléchargez le fichier de la carte PKI Entrust :
   a) Accédez à https://www.citrix.com/downloads.
   b) Accédez à **Citrix Endpoint Management (et Citrix XenMobile Server) > XenMobile Server > Logiciel produit > XenMobile Server 10 > Outils**.
   c) Sur la vignette **Entrust PKI Adapter**, cliquez sur **Download File**.
   d) Extrayez le fichier entrust.war du fichier .zip téléchargé et placez-le dans le répertoire C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps.
2. Dans C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps\Entrust\WEB-INF\classes, modifiez le fichier entrust_adapter.properties et définissez CustomProperties sur `c:\\zenprise\\custom_entrust_adapter.properties`.



3. Dans votre lecteur C, créez un répertoire zenprise et un nouveau fichier appelé custom_entrust_adapter.properties.
4. Modifiez le fichier avec le contenu suivant en veillant à remplacer les fichiers Entrust.MdmSvc.URL, AdminUserId et and AdminPassword de manière appropriée.

   ~

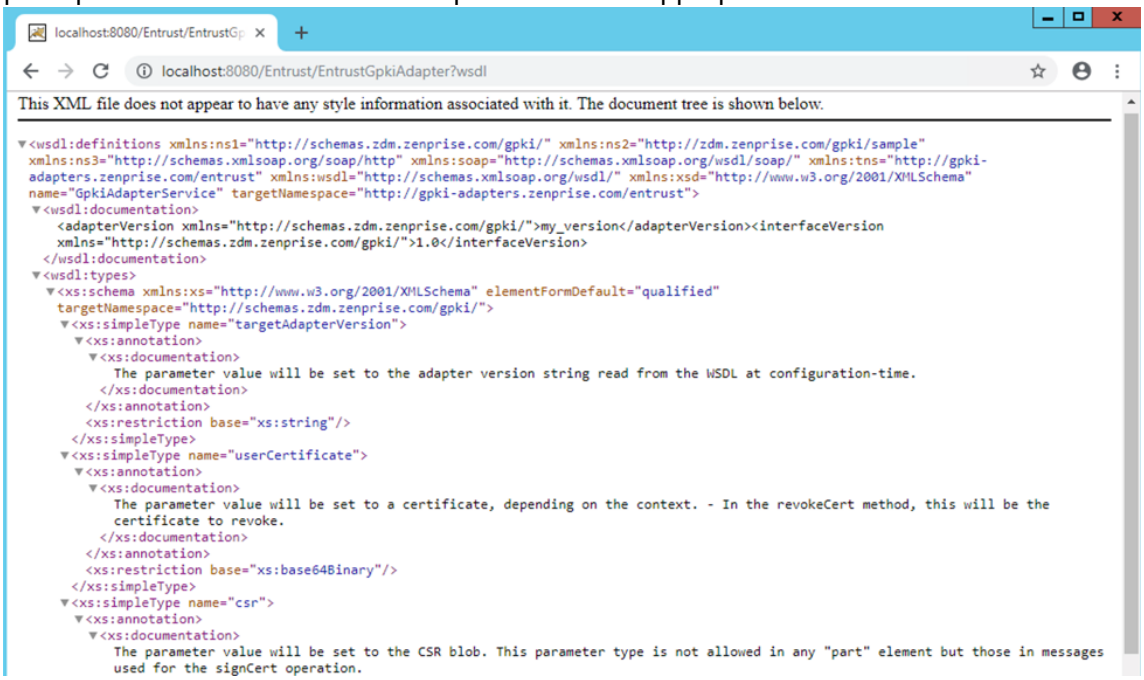
   # Définissez les lignes suivantes sur l'URL appropriée pour AS/IG
   Entrust.MdmSvc.Url=`https://pki.yourcorp.com:19443/mdmws/services/AdminServiceV8`

```
# set to 1 or true to force user creation from passed user and
    group parameters if using IG and user does not exist
CreateUser=

# set the credentials for the endpoint
AdminUserId=`[User ID]`
AdminPassword=`[password]`


# keystore for client-cert auth
#keyStore=
#keyStorePassword=
```



```
12 #keyStoreType: JKS, JCEKS and PKCS12  -- not needed for .p12 and .
      jks files
13
14 # truststore for server with self-signed root CA
15 #trustStore=
16 #trustStorePassword=
17 #trustStoreType: JKS, JCEKS and PKCS12  -- not needed for .p12 and
       .jks files
18 ~
```

5. Redémarrez le service Tomcat. Accédez à C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\logs et ouvrez Catalina_201x-MM-DD.log. -Vérifiez qu'il n'y a pas d'erreurs et que la ligne suivante s'affiche :
   `13-Nov-2018 09:02:35.319 INFO [localhost-startStop-1] org.apache.cxf.endpoint.ServerImpl.initDestination Setting the server's publish address to be /EntrustGpkiAdapter`
6. Accédez à `http://localhost:8080/Entrust/EntrustGpkiAdapter?wsdl` ou à l'URL publique de votre serveur et vérifiez que le code XML approprié s'affiche.



Configurer XenMobile pour la carte Entrust PKI

1. Connectez-vous à la console XenMobile et accédez à **Paramètres > Entités PKI**. Cliquez sur **Ajouter > Entité PKI générique**.
2. Entrez les informations suivantes :
   - **Nom :** saisissez un nom pour l'entité PKI.

- **URL WSDL :** entrez l'URL publique de votre serveur.
- **Type d'authentification :** choisissez la méthode d'authentification à utiliser.
  - **Aucune**
  - **HTTP basique :** entrez le nom d'utilisateur et mot de passe requis pour se connecter.
  - **Certificat client :** sélectionnez le certificat client SSL correct.
- **Emplacement des ressources :** sélectionnez **Emplacement de mes ressources**.
- **Chemins relatifs autorisés :** saisissez /`Entrust/*`.

3. Une fois la configuration de l'entité PKI terminée, revenez à la page **Paramètres** et ajoutez un **fournisseur d'identités**.
4. Dans l'onglet **Général**, sélectionnez votre entité Entrust comme **Entité émettrice** et **SIGNER** comme **Méthode d'émission**.
5. Dans l'onglet **Demande de signature de certificat**, configurez les paramètres suivants :
   - **Algorithme de clé : RSA**
   - **Taille de la clé :** 2048
   - **Algorithme de signature : SHA256withRSA**
   - **Nom du sujet :** cd=$user.username
   - **Noms de sujet alternatifs :** facultatif. Nous recommandons les paramètres suivants :
     - **Type : nom d'utilisateur principal**
     - **Valeur :** $user.userprincipalname

     > **Remarque :**
     > Si vous modifiez des paramètres de la carte, procédez comme suit pour reconfigurer le fournisseur d'informations d'identification.
6. Une fois le fournisseur d'informations d'identification configuré, accédez à **Configurer > Stratégies d'appareil** et ajoutez une stratégie d'informations d'identification.
7. Configurez la stratégie pour les systèmes d'exploitation que vous prévoyez d'utiliser. Sur chaque page de configuration du système d'exploitation, pour **Type de certificat**, sélectionnez **Fournisseur d'identités**. Dans le menu **Fournisseur d'identités**, sélectionnez le fournisseur d'informations d'identification que vous avez configuré précédemment.

Services de certificats Microsoft

XenMobile se connecte avec Microsoft Certificate Services Web par le biais de son interface d'inscription Web. XenMobile prend uniquement en charge l'émission de nouveaux certificats via cette interface (l'équivalent de la fonctionnalité de signature GPKI). Si l'autorité de certification Microsoft génère un certificat d'utilisateur Citrix Gateway, Citrix Gateway prend en charge le renouvellement et la révocation de ces certificats.

Pour créer une entité PKI Microsoft CA dans XenMobile, vous devez spécifier l'adresse URL de base de l'interface Web des services de certificats. Si vous le souhaitez, utilisez l'authentification de client SSL pour sécuriser la connexion entre XenMobile et l'interface Web des services de certificats.

Ajouter une entité Services de certificats Microsoft

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Entités PKI**.
2. Sur la page **Entités PKI**, cliquez sur **Ajouter**.

   Un menu des types d'entité PKI s'affiche.
3. Cliquez sur **Entité Services de certificats Microsoft**.

   La page **Entité Services de certificats Microsoft : informations générales** s'affiche.
4. Sur la page **Entité Services de certificats Microsoft : informations générales**, configurez ces paramètres :

   - **Nom :** entrez un nom pour votre nouvelle entité, qui sera utilisé plus tard pour faire référence à cette entité. Les noms de l'entité doivent être uniques.
   - **URL racine du service d'inscription Web :** entrez l'adresse URL de votre service d'inscription Web d'autorité de certification Microsoft ; par exemple, `https://192.0.2.13/certsrv/`. L'adresse URL peut utiliser un format HTTP ou HTTP-over-SSL.
   - **Nom de page certnew.cer :** nom de la page certnew.cer. Utilisez le nom par défaut sauf si vous l'avez renommé pour une raison quelconque.
   - **certfnsh.asp :** nom de la page certfnsh.asp. Utilisez le nom par défaut sauf si vous l'avez renommé pour une raison quelconque.
   - **Type d'authentification :** choisissez la méthode d'authentification à utiliser.
     - **Aucune**
     - **HTTP basique :** entrez le nom d'utilisateur et mot de passe requis pour se connecter.
     - **Certificat client :** sélectionnez le certificat client SSL correct.
5. Cliquez sur **Tester la connexion** pour vous assurer que le serveur est accessible. S'il n'est pas accessible, un message s'affiche, indiquant que la connexion a échoué. Vérifiez vos paramètres de configuration.
6. Cliquez sur **Suivant**.

   La page **Entité Services de certificats Microsoft : modèles** s'affiche. Sur cette page, spécifiez le nom interne des modèles pris en charge par votre autorité de certification Microsoft. Lors de la création de Fournisseurs d'informations d'identification, vous devez sélectionner un modèle dans la liste définie ici. Chaque fournisseur d'identités utilisant cette entité utilise un seul modèle de ce type.

   Pour connaître la configuration requise pour les modèles Services de certificats Microsoft, veuillez consulter la documentation Microsoft relative à votre version de serveur Microsoft. XenMobile ne requiert pas de configuration particulière pour les certificats qu'il distribue autre que les formats de certificat indiqués dans Certificats.

7. Sur la page **Entité Services de certificats Microsoft : modèles**, cliquez sur **Ajouter**, entrez le nom du modèle et cliquez sur **Enregistrer**. Répétez cette étape pour chaque modèle à ajouter.
8. Cliquez sur **Suivant**.

   La page **Entité Services de certificats Microsoft : paramètres HTTP** s'affiche. Sur cette page, spécifiez des paramètres personnalisés que XenMobile doit ajouter à la requête HTTP auprès de l'interface d'inscription Web de Microsoft. Les paramètres personnalisés ne sont utiles que pour les scripts personnalisés exécutés sur l'autorité de certification.
9. Sur la page **Entité Services de certificats Microsoft : paramètres HTTP**, cliquez sur **Ajouter**, entrez le nom et la valeur des paramètres HTTP que vous souhaitez ajouter, puis cliquez sur **Suivant**.

   La page **Entité Services de certificats Microsoft : certificats CA** s'affiche. Sur cette page, vous devez informer XenMobile des signataires des certificats que le système obtient par le biais de cette entité. Lorsque votre certificat CA est renouvelé, mettez-le à jour dans XenMobile. XenMobile applique le changement à l'entité de manière transparente.
10. Sur la page **Entité Services de certificats Microsoft : certificats CA**, sélectionnez les certificats que vous voulez utiliser pour cette entité.
11. Cliquez sur **Enregistrer**.

    L'entité s'affiche sur le tableau Entités PKI.

Liste de révocation de certificats (CRL) Citrix ADC

XenMobile prend en charge la liste de révocation de certificats (CRL) uniquement pour une autorité de certification tierce. Si vous disposez d'une autorité de certification Microsoft configurée, XenMobile utilise Citrix ADC pour gérer la révocation.

Lorsque vous configurez l'authentification basée sur un certificat client, vous devez décider si vous souhaitez configurer le paramètre Liste de révocation de certificats (CRL) Citrix ADC, **Enable CRL Auto Refresh**. Cette étape garantit que l'utilisateur d'un appareil en mode MAM exclusif ne peut pas s'authentifier à l'aide d'un certificat existant sur l'appareil.

XenMobile émet un nouveau certificat, car il n'interdit pas à un utilisateur de générer un certificat utilisateur si un certificat est révoqué. Ce paramètre renforce la sécurité des entités PKI lorsque la CRL vérifie la présence d'entités PKI expirées.

Autorités de certification discrétionnaires

Une autorité de certification discrétionnaire est créée lorsque vous fournissez un certificat d'autorité de certification et la clé privée qui lui est associée à XenMobile. XenMobile gère l'émission, la révocation et les informations d'état en interne des certificats, selon les paramètres que vous spécifiez.

Lorsque vous configurez une autorité de certification discrétionnaire, vous pouvez activer la prise en charge du protocole OCSP pour cette autorité de certification. Si, et uniquement si vous activez la prise en charge du protocole OCSP, l'autorité de certification ajoute une extension `id-pe-authorityInfoAccess` aux certificats qu'elle émet. L'extension pointe vers le répondeur OCSP interne de XenMobile à l'emplacement suivant :

```
https://<server>/<instance>/ocsp
```

Lors de la configuration du service OCSP, spécifiez un certificat de signature OCSP pour l'entité discrétionnaire en question. Vous pouvez utiliser le certificat d'autorité de certification lui-même en tant que signataire. Pour éviter la divulgation inutile de la clé privée de votre autorité de certification (recommandé), créez un certificat de signature OCSP délégué, signé par le certificat d'autorité de certification et incluez l'extension suivante : `id-kp-OCSPSigning extendedKeyUsage`.

Le service du répondeur OCSP de XenMobile prend en charge les réponses OCSP de base et les algorithmes de hash suivants utilisés dans les requêtes :

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Les réponses sont signées avec SHA-256 et l'algorithme de clé du certificat de signature (DSA, RSA ou ECDSA).

Ajouter des autorités de certification discrétionnaires

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Plus > Entités PKI**.
2. Sur la page **Entités PKI**, cliquez sur **Ajouter**.

   Un menu des types d'entité PKI s'affiche.
3. Cliquez sur **CA discrétionnaire**.

   La page **CA discrétionnaire : informations générales** s'affiche.
4. Sur la page **CA discrétionnaire : informations générales**, procédez comme suit :
   - **Nom :** entrez un nom descriptif pour la CA discrétionnaire.
   - **Certificat CA utilisé pour signer les demandes de certificat :** cliquez sur un certificat pour la CA discrétionnaire à utiliser pour signer les demandes de certificats.

     Cette liste de certificats est générée à partir des certificats CA avec des clés privées que vous avez chargées sur XenMobile dans **Configure > Paramètres > Certificats**.

5. Cliquez sur **Suivant**.

   La page **CA discrétionnaire : paramètres** s'affiche.

6. Sur la page **CA discrétionnaire : paramètres**, procédez comme suit :

   - **Générateur de numéro de série :** la CA discrétionnaire génère des numéros de série pour les certificats qu'elle émet. Dans cette liste, cliquez sur **Séquentiel** ou **Non-séquentiel** pour déterminer comment les numéros sont générés.
   - **Numéro de série suivant :** entrez une valeur pour déterminer le numéro suivant émis.
   - **Certificat valide pour :** entrez le nombre de jours pendant lesquels le certificat est valide.
   - **Utilisation de la clé :** identifiez la fonction des certificats émis par l'autorité de certification discrétionnaire en définissant les clés appropriées sur **Activé**. Une fois cette option définie, l'autorité de certification peut uniquement émettre des certificats aux fins susmentionnées.
   - **Utilisation de clé étendue :** pour ajouter d'autres paramètres, cliquez sur **Ajouter**, entrez le nom de clé, puis cliquez sur **Enregistrer**.

7. Cliquez sur **Suivant**.

   La page **CA discrétionnaire : distribution** s'affiche.

8. Sur la page **CA discrétionnaire : distribution**, sélectionnez un mode de distribution :

   - **Centralisé : génération de la clé sur le serveur**. Citrix recommande l'option centralisée. Les clés privées sont générées et stockées sur le serveur et distribuées sur les appareils des utilisateurs.
   - **Distribué : génération de la clé sur l'appareil**. Les clés privées sont générées sur les appareils des utilisateurs. Ce mode distribué utilise SCEP et requiert un certificat de chiffrement RA avec l'extension `keyUsage keyEncryption` et un certificat de signature RA avec l'extension `keyUsage digitalSignature`. Le même certificat peut être utilisé pour le chiffrement et la signature.

9. Cliquez sur **Suivant**.

   La page **CA discrétionnaire : protocole OCSP** s'affiche.

   Sur la page **CA discrétionnaire : protocole OCSP**, procédez comme suit :

   - Si vous souhaitez ajouter une extension `AuthorityInfoAccess` (RFC2459) pour les certificats signés par cette autorité de certification, définissez **Activer le support d'OCSP pour cette CA** sur **Activé**. Cette extension pointe vers le répondeur OCSP de l'autorité de certification sur `https://<server>/<instance>/ocsp`.
   - Si vous avez activé la prise en charge du protocole OCSP, sélectionnez un certificat d'autorité de certification de signature OSCP. Cette liste de certificats est générée à partir des certificats d'autorité de certification que vous avez chargés sur XenMobile.

10. Cliquez sur **Enregistrer**.

    L'autorité de certification discrétionnaire s'affiche sur le tableau Entités PKI.

Fournisseurs d'informations d'identification

January 10, 2022

Les fournisseurs d'identités sont les configurations de certificat réelles que vous utilisez dans différentes parties du système XenMobile. Les fournisseurs d'informations d'identification définissent les sources, les paramètres et les cycles de vie de vos certificats. Ces opérations se produisent que les certificats fassent partie des configurations de l'appareil ou soient autonomes (c'est-à-dire, envoyés tels quels sur l'appareil).

L'inscription d'appareil limite le cycle de vie du certificat. En effet, XenMobile ne délivre pas de certificats avant l'inscription, bien qu'il puisse en émettre certains dans le cadre de l'inscription. En outre, les certificats émis par la PKI interne dans le cadre d'une inscription sont révoqués lorsque l'inscription est révoquée. Après la fin de la relation de gestion, aucun certificat valide n'est conservé.

Une configuration de fournisseur d'identités peut être utilisée à plusieurs endroits, par conséquent une configuration peut régir un grand nombre de certificats simultanément. L'unité existe alors sur la ressource de déploiement et le déploiement. Par exemple, si le fournisseur d'identités P est déployé sur l'appareil D dans le cadre de la configuration C : les paramètres d'émission pour P déterminent le certificat qui est déployé sur D. De même, les paramètres de renouvellement pour D s'appliquent lorsque C est mis à jour. Les paramètres de révocation pour D s'appliquent également lorsque C est supprimé ou que D est révoqué.

Selon ces règles, la configuration du fournisseur d'identités détermine ce qui suit dans XenMobile :

- La source des certificats.
- La méthode grâce à laquelle les certificats sont obtenus : signature d'un nouveau certificat ou récupération d'un certificat existant et d'une paire de clés.
- Les paramètres d'émission ou de récupération. Par exemple, les paramètres de demande de signature de certificat (CSR), tels que la taille de la clé, l'algorithme de clé et les extensions de certificat.
- La façon dont les certificats sont mis à disposition sur l'appareil.
- Les conditions de révocation. Bien que tous les certificats soient révoqués dans XenMobile lorsque la relation de gestion est rompue, la configuration peut spécifier une révocation antérieure. Par exemple, la configuration peut spécifier de révoquer un certificat lorsque la configuration d'appareil associée est supprimée. En outre, dans certaines conditions, il se peut que la révocation du certificat associé dans XenMobile puisse être envoyée à l'infrastructure interne

à clé publique (PKI) principale. Autrement dit, la révocation de certificats dans XenMobile peut entraîner la révocation de certificats sur la PKI.
- Les paramètres de renouvellement. Les certificats obtenus via un fournisseur d'informations d'identification donné peuvent être automatiquement renouvelés lorsqu'ils arrivent à expiration. Ou, des notifications peuvent être émises lorsque cette expiration approche.

La disponibilité des options de configuration dépend principalement du type d'entité PKI et de la méthode d'émission que vous sélectionnez pour un fournisseur d'identités.

Méthodes d'émission de certificats

Vous pouvez obtenir un certificat, désigné comme méthodes d'émission de deux manières différentes :

- **Signer :** avec cette méthode, l'émission implique la création d'une nouvelle clé privée, la création d'une demande de signature de certificat (CSR) et la soumission de la demande de signature de certificat à une autorité de certification (CA) pour signature. XenMobile prend en charge la méthode de signature des trois entités PKI (Entité Services de certificats Microsoft, PKI générique et CA discrétionnaire).
- **Récupérer :** dans le cadre de XenMobile, cette méthode implique la récupération d'une paire de clés. XenMobile prend en charge la méthode de récupération uniquement pour l'entité PKI générique.

Un fournisseur d'identités utilise l'une ou l'autre de ces deux méthodes d'émission. La méthode sélectionnée affecte les options de configuration disponibles. Notamment, la configuration CSR et la mise à disposition distribuée sont uniquement disponibles si la méthode d'émission est la signature. Un certificat de récupération est toujours envoyé à l'appareil au format PKCS #12, ce qui correspond à une méthode de mise à disposition centralisée pour la méthode de signature.

Mise à disposition de certificats

Deux modes de mise à disposition de certificats sont disponibles dans XenMobile : centralisée et distribuée. Le mode Distribué utilise le protocole d'inscription du certificat simple (SCEP) et est uniquement disponible dans les situations dans lesquelles le client prend en charge le protocole (iOS uniquement). Le mode distribué est obligatoire dans certains cas.

Pour qu'un fournisseur d'identités prenne en charge la mise à disposition (assisté par SCEP) distribuée, une étape de configuration spéciale est nécessaire : configuration des certificats de l'autorité d'inscription (RA). Les certificats RA sont requis, car lors de l'utilisation du protocole SCEP, XenMobile agit comme un délégué (registre) pour l'autorité de certification réelle. XenMobile doit prouver au client qu'il dispose de l'autorité d'agir en tant que tel. Cette autorité est établie par le chargement vers XenMobile des certificats mentionnés plus haut.

Deux rôles de certificat distincts sont requis (bien qu'un seul certificat puisse remplir les deux rôles) : la signature RA et le chiffrement RA. Les contraintes pour ces rôles sont les suivantes :

- Le certificat de signature RA doit posséder une signature numérique d'utilisation de clé X.509.
- Le certificat de chiffrement RA doit posséder un chiffrement de clé d'utilisation de clé X.509.

Pour configurer les certificats RA du fournisseur d'identités, vous devez charger les certificats sur XenMobile, puis les associer au fournisseur d'identités.

Un fournisseur d'identités est considéré comme pouvant uniquement prendre en charge une mise à disposition distribuée s'il possède un certificat configuré pour les rôles de certificat. Vous pouvez configurer chaque fournisseur d'identités pour privilégier au choix le mode centralisé, le mode distribué ou pour requérir le mode distribué. Le résultat réel dépend du contexte : si le contexte ne prend pas en charge le mode distribué, mais que le fournisseur d'identités requiert ce mode, le déploiement échoue. De même, si le contexte requiert le mode distribué, mais que le fournisseur d'identités ne le prend pas en charge, le déploiement échoue. Dans tous les autres cas, le paramètre préféré est appliqué.

Le tableau suivant présente la distribution SCEP au travers de XenMobile :

Contexte	SCEP pris en charge	SCEP requis
Service de profil iOS	Oui	Oui
Inscription à la gestion des appareils mobiles iOS	Oui	Non
Profils de configuration iOS	Oui	Non
Inscription SHTP	Non	Non
Configuration de SHTP	Non	Non
Inscription de Windows Phone et Tablet	Non	Non
Configuration de Windows Phone et Tablet	Non, à l'exception de la stratégie Wi-Fi qui est prise en charge pour Windows Phone 8.1, Windows 10 et Windows 11	Non

Révocation de certificats

Il existe trois types de révocation.

- **Révocation interne :** la révocation interne du certificat affecte le statut du certificat géré par

XenMobile. XenMobile vérifie ce statut lors de l'évaluation d'un certificat présenté ou lors de la fourniture d'informations de statut OCSP pour un certificat. La configuration du fournisseur d'identités détermine la manière dont le statut est affecté par plusieurs conditions. Par exemple, le fournisseur d'identités peut spécifier que les certificats soient marqués comme révoqués lorsqu'ils ont été supprimés de l'appareil.

- **Révocation propagée en externe :** également appelée révocation XenMobile, ce type de révocation s'applique aux certificats obtenus à partir d'une PKI externe. Le certificat est révoqué sur la PKI lorsque le certificat est révoqué en interne par XenMobile, sous les conditions définies par la configuration du fournisseur d'identités. La demande de révocation requiert une entité GPKI disposant d'une capacité de révocation.
- **Révocation induite en interne :** également appelée PKI de révocation, ce type de révocation s'applique uniquement aux certificats obtenus à partir d'une PKI externe. Chaque fois que XenMobile évalue le statut d'un certificat donné, XenMobile interroge la PKI afin de déterminer ce statut. Si le certificat est révoqué, XenMobile révoque le certificat en interne. Ce mécanisme utilise le protocole OCSP.

Ces trois types ne sont pas exclusifs, mais s'appliquent ensemble. Une révocation externe ou une observation indépendante peut entraîner une révocation interne. Une révocation interne affecte potentiellement une révocation externe.

Renouvellement de certificat

Un renouvellement du certificat est la combinaison de révocation d'un certificat existant et de l'émission d'un autre certificat.

XenMobile tente tout d'abord d'obtenir le nouveau certificat avant de révoquer le certificat précédent, afin d'éviter une discontinuité du service lorsque l'émission échoue. Pour la mise à disposition distribuée (prise en charge par SCEP), la révocation ne se produit également qu'une fois le certificat installé sur l'appareil. Sinon, la révocation a lieu avant que le nouveau certificat soit envoyé à l'appareil. Cette révocation est indépendante du succès ou de l'échec de l'installation du certificat.

La configuration de la révocation nécessite que vous spécifiiez une certaine durée (en jours). Lorsque l'appareil se connecte, le serveur vérifie que la date du certificat `NotAfter` est postérieure à la date actuelle, moins la durée spécifiée. Si le certificat remplit cette condition, XenMobile tente de renouveler le certificat.

Créer un fournisseur d'identités

La configuration d'un fournisseur d'identités varie principalement en fonction de l'entité d'émission et de la méthode d'émission sélectionnées pour le fournisseur d'identités. Vous pouvez faire la distinction entre les fournisseurs d'identités qui utilisent une entité interne ou une entité externe :

- Une entité discrétionnaire, qui est interne à XenMobile, est une entité interne. La méthode d'émission pour une entité discrétionnaire est toujours la signature. La signature signifie qu'avec chaque opération d'émission, XenMobile signe une nouvelle paire de clés avec le certificat d'autorité de certification sélectionné pour l'entité. L'emplacement où la paire de clés est générée (l'appareil où le serveur) dépend de la méthode de distribution sélectionnée.
- Une entité externe, qui fait partie de votre infrastructure d'entreprise, inclut une autorité de certification Microsoft ou une GPKI.

Pour obtenir des informations détaillées sur la configuration de DigiCert Managed PKI, y compris la création du fournisseur d'informations d'identification, consultez la section « DigiCert Managed PKI » dans Entités PKI.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit, puis cliquez sur **Paramètres > Fournisseurs d'identités**.
2. Sur la page **Fournisseurs d'informations d'identification**, cliquez sur **Ajouter**.

   La page **Fournisseurs d'informations d'identification : informations générales** s'affiche.
3. Sur la page **Fournisseurs d'informations d'identification : informations générales**, procédez comme suit :

   - **Nom :** entrez un nom unique pour la nouvelle configuration du fournisseur. Ce nom sera utilisé par la suite pour faire référence à la configuration dans d'autres parties de la console XenMobile.
   - **Description :** décrivez le fournisseur d'identités. Bien que ce champ soit facultatif, une description peut être utile pour vous fournir des détails sur ce fournisseur d'identités.
   - **Entité émettrice :** cliquez sur l'entité qui émet le certificat.
   - **Méthode d'émission :** cliquez sur **Signer** ou **Récupérer** pour choisir la méthode que le système utilise pour obtenir des certificats auprès de l'entité configurée. Pour l'authentification de certificat client, utilisez **Signer**.
   - Si la liste **Modèle** est disponible, sélectionnez le modèle que vous avez ajouté sous l'entité PKI pour le fournisseur d'identités.

     Ces modèles deviennent disponibles lorsque les entités Services de certificats Microsoft sont ajoutées sur **Paramètres > Entités PKI**.
4. Cliquez sur **Suivant**.

   La page **Fournisseur d'identités : demande de signature de certificat** s'affiche.
5. Sur la page **Fournisseurs d'identités : demande de signature de certificat**, configurez les éléments suivants en fonction de votre configuration de certificat :

- **Algorithme de clé :** choisissez l'algorithme de clé pour la nouvelle paire de clés. Les valeurs disponibles sont **RSA**, **DSA** et **ECDSA**.
- **Taille de la clé :** entrez la taille en octets de la paire de clés. Ce champ est obligatoire.

  Les valeurs autorisées dépendent du type de clé. Par exemple, la taille maximale des clés DSA est de 1024 bits. Pour éviter de faux résultats négatifs, qui dépendent du matériel ou du logiciel sous-jacent, XenMobile n'exige pas l'utilisation d'une taille de clé particulière. Vous devez toujours tester les configurations de fournisseur d'identités dans un environnement de test avant de les activer dans un environnement de production.
- **Algorithme de signature :** cliquez sur une valeur pour le nouveau certificat. Les valeurs dépendent de l'algorithme de clé.
- **Nom du sujet :** obligatoire. Tapez le nom unique (DN) du sujet du nouveau certificat. Pa exemple : `CN=${ user.username } , OU=${ user.department } , O=${ user .companyname } ,C=${ user.c } \endquotation`

  Par exemple, pour l'authentification du certificat client, utilisez ces paramètres :

  - **Algorithme de clé :** RSA
  - **Taille de la clé :** 2048
  - **Algorithme de signature :** SHA256withRSA
  - **Nom du sujet :** `cn=$user.username`
- Pour ajouter une entrée à la table **Noms de sujet alternatifs**, cliquez sur **Ajouter**. Sélectionnez le type de nom alternatif, puis tapez une valeur dans la deuxième colonne.

  Pour l'authentification du certificat client, spécifiez :

  - **Type :** nom principal de l'utilisateur
  - **Valeur :** `$user.userprincipalname`

    Comme avec le nom du sujet, vous pouvez utiliser les macros XenMobile dans le champ de valeur.

6. Cliquez sur **Suivant**.

   La page **Fournisseurs d'informations d'identification : distribution** s'affiche.

7. Sur la page **Fournisseurs d'informations d'identification : distribution**, procédez comme suit :

   - Dans la liste **Certificat émis par l'autorité de certification**, cliquez sur le certificat d'autorité de certification proposé. Étant donné que le fournisseur d'identités utilise une entité d'autorité de certification discrétionnaire, le certificat d'autorité de certification du fournisseur d'identités sera toujours le certificat d'autorité de certification configuré sur l'entité elle-même. Le certificat d'autorité de certification est présenté ici pour des raisons de cohérence avec les configurations utilisant des entités externes.

- Dans **Sélectionner le mode de distribution**, sélectionnez l'une des méthodes de génération et de distribution de clés :
  - **Préférer mode centralisé : génération de la clé sur le serveur :** Citrix recommande cette option centralisée. Ce mode prend en charge toutes les plates-formes prises en charge par XenMobile et est requis lors de l'utilisation de l'authentification Citrix Gateway. Les clés privées sont générées et stockées sur le serveur et distribuées sur les appareils des utilisateurs.
  - **Préférer mode distribué : génération de la clé sur l'appareil.** Les clés privées sont générées et stockées sur les appareils des utilisateurs. Ce mode distribué utilise SCEP et requiert un certificat de chiffrement RA avec le keyUsage keyEncryption et un certificat de signature RA avec le KeyUsage digitalSignature. Le même certificat peut être utilisé pour le chiffrement et la signature.
  - **Distribué uniquement : génération de la clé sur l'appareil :** cette option fonctionne de la même façon que Préférer mode distribué : génération de la clé sur l'appareil, sauf qu'étant « Uniquement » au lieu de « Préférer », aucune option n'est disponible si la génération de la clé sur l'appareil échoue.

Si vous avez sélectionné **Préférer mode distribué : génération de la clé sur l'appareil** ou **Distribué uniquement : génération de la clé sur l'appareil**, cliquez sur le certificat de signature RA et le certificat de chiffrement RA. Le même certificat peut être utilisé pour les deux modes. De nouveaux champs apparaissent pour ces certificats.

8. Cliquez sur **Suivant**.

   La page **Fournisseurs d'identités : révocation XenMobile** s'affiche. Sur cette page, vous configurez les conditions dans lesquelles XenMobile marque (en interne) comme révoqué les certificats émis au travers de cette configuration de fournisseur.

9. Sur la page **Fournisseurs d'identités : révocation XenMobile**, procédez comme suit :

   - Dans **Révoquer les certificats émis**, sélectionnez l'une des options qui indique quand les certificats doivent être révoqués.
   - Si vous voulez que XenMobile envoie une notification lorsque le certificat est révoqué, définissez la valeur de **Envoyer une notification** sur **Activé** et choisissez un modèle de notification.
   - Si vous souhaitez révoquer le certificat sur la PKI lorsque le certificat est révoqué de XenMobile, définissez **Révoquer le certificat** auprès de la PKI sur **Activé** et cliquez sur un modèle dans la liste **Entité**. La liste Entité répertorie toutes les entités GPKI disponibles avec des capacités de révocation. Lorsque le certificat est révoqué de XenMobile, une demande de révocation est envoyée à la PKI sélectionnée à partir de la liste Entité.

10. Cliquez sur **Suivant**.

La page **Fournisseurs d'informations d'identification : révocation PKI** s'affiche. Sur cette page, identifiez les actions à effectuer sur la PKI si le certificat est révoqué. Vous avez aussi la possibilité de créer un message de notification.

11. Sur la page **Fournisseurs d'informations d'identification : révocation PKI**, procédez comme suit si vous souhaitez révoquer les certificats de la PKI :

    - Modifiez le paramètre **Activer les vérifications de révocation externe** sur **Activé**. Des champs supplémentaires liés à la PKI de révocation apparaissent.
    - Dans la liste **Certificat CA du répondeur OCSP**, cliquez sur le nom unique (DN) du sujet du certificat.

      Vous pouvez utiliser les macros XenMobile pour les valeurs de champ de nom unique. Pa exemple : `CN=${ user.username } , OU=${ user.department } , O=${ user .companyname } , C=${ user.c } \endquotation`
    - Dans la liste **Lorsque le certificat est révoqué**, cliquez sur l'une des actions suivantes à entreprendre sur l'entité PKI lorsque le certificat est révoqué :
      - Ne rien faire.
      - Renouveler le certificat.
      - Révoquer et de réinitialiser l'appareil.
    - Si vous voulez que XenMobile envoie une notification lorsque le certificat est révoqué, définissez la valeur de **Envoyer une notification** sur **Activé**.

      Vous avez le choix entre deux options de notification :
    - Si vous sélectionnez **Sélectionner un modèle de notification**, vous pouvez sélectionner un message de notification pré-rempli que vous pouvez personnaliser. Ces modèles figurent dans la liste Modèle de notification.
    - Si vous sélectionnez **Entrer les détails de notification**, vous pouvez créer votre propre message de notification. En plus de fournir l'adresse e-mail du destinataire et le message, vous pouvez définir la fréquence à laquelle la notification est envoyée.

12. Cliquez sur **Suivant**.

    La page **Fournisseurs d'informations d'identification : renouvellement** s'affiche. Sur cette page, vous pouvez configurer XenMobile pour effectuer les opérations suivantes :

    - Renouveler le certificat. Vous pouvez envoyer (facultatif) une notification lors du renouvellement et exclure (facultatif) les certificats déjà expirés de l'opération.
    - Émettre une notification pour les certificats dont l'expiration approche (avant le renouvellement).

13. Sur la page **Fournisseurs d'informations d'identification : renouvellement**, procédez comme suit si vous souhaitez renouveler les certificats lorsqu'ils expirent :

Réglez **Renouveler les certificats lorsqu'ils expirent** sur **Activé**. Des champs supplémentaires apparaissent.

- Dans le champ **Renouveler lorsque le certificat expire dans**, entrez quand le renouvellement doit être effectué, en nombre de jours avant l'expiration.
- Si vous le souhaitez, sélectionnez **Ne pas renouveler les certificats expirés**. Dans ce cas, « expiré » signifie que la date `NotAfter` (fin de validité) est dans le passé, et non pas qu'il a été révoqué. XenMobile ne renouvelle pas les certificats après leur révocation interne.

Si vous voulez que XenMobile envoie une notification lorsque le certificat a été renouvelé, définissez **Envoyer une notification** sur **Activé**. Si vous voulez que XenMobile envoie une notification lorsque la certification arrive à échéance, définissez **Notifier quand un certificat va expirer** sur **Activé**.
Dans tous les cas, vous avez le choix entre deux options de notification :

- **Sélectionner un modèle de notification :** sélectionnez un message de notification prérempli que vous pouvez personnaliser. Ces modèles figurent dans la liste Modèle de notification.
- **Entrer les détails de notification :** créez votre propre message de notification. Indiquez l'adresse e-mail du destinataire, un message et la fréquence d'envoi de la notification.

Dans le champ **Notifier lorsque le certificat expire dans**, entrez le nombre de jours avant expiration du certificat après lequel la notification doit être envoyée.

14. Cliquez sur **Enregistrer**.

    Le fournisseur d'identités apparaît dans la table Fournisseur d'identités.

Certificats APNs

January 10, 2022

> **Important :**
>
> La prise en charge par Apple du protocole binaire hérité du service Apple Push Notification prend fin le 31 mars 2021. Apple recommande d'utiliser à la place l'API du fournisseur APNs basé sur HTTP/2. À partir de la version 10.13.0, XenMobile Server prend en charge l'API basée sur HTTP/2. Pour plus d'informations, consultez « Apple Push Notification Service Update » dans https://developer.apple.com/. Pour obtenir de l'aide sur la vérification de la connectivité à APNs, consultez la section Tests de connectivité.

Pour inscrire et gérer des appareils iOS et macOS dans XenMobile, vous devez configurer un certificat Apple Push Notification Service (APNS).

Résumé du workflow :

- **Étape 1 :** Créer une demande de signature de certificat (CSR) en utilisant l'une des méthodes suivantes :
  - Créer une demande de signature de certificat à l'aide de l'application Trousseau d'accès sur macOS (recommandé par Citrix)
  - Créer une demande de signature de certificat à l'aide de Microsoft IIS
  - Créer une demande de signature de certificat avec OpenSSL
- **Étape 2 :** Signer la CSR dans XenMobile Tools
- **Étape 3 :** Envoyer la CSR signée à Apple pour obtenir le certificat APNs
- **Étape 4 :** En utilisant le même ordinateur que celui utilisé pour l'étape 1, remplir la CSR et exportez un fichier PKCS #12 :
  - Créer un fichier PKCS #12 à l'aide de l'application Trousseau d'accès sur macOS
  - Créer un fichier PKCS #12 à l'aide de Microsoft IIS
  - Créer un fichier PKCS #12 avec OpenSSL
- **Étape 5 :** Importer un certificat APNS dans XenMobile
- **Étape 6 :** Renouveler un certificat APNs

Créer une demande de signature de certificat

Nous vous recommandons de créer une demande de signature de certificat (CSR) à l'aide de l'application Trousseau d'accès sur macOS. Vous pouvez également créer une demande de signature de certificat à l'aide de Microsoft IIS ou OpenSSL.

> **Important :**
>
> - Pour l'identifiant Apple ID utilisé pour créer le certificat :
>   - The Apple ID must be a corporate ID and not a personal ID.
>   - Record the Apple ID that you use to create the certificate.
>   - To renew your certificate, use the same organization name and Apple ID. Using a different Apple ID to renew the certificate require device reenrollment.
> - Si vous avez délibérément ou accidentellement révoqué le certificat, vous perdrez la possibilité de gérer vos appareils.
> - Si vous avez utilisé iOS Developer Enterprise Program pour créer un certificat push de gestion des appareils mobiles, vous devez gérer les actions concernant les certificats migrés dans le portail Apple Push Certificates Portal.

Créer une demande de signature de certificat à l'aide de l'application Trousseau d'accès sur macOS

1. Sur un ordinateur exécutant macOS, sous **Applications > Utilitaires**, démarrez l'application Trousseau d'accès.
2. Ouvrez le menu **Trousseaux d'accès** et cliquez sur **Assistant de certification > Demander un certificat à une autorité de certification**.
3. L'Assistant de certification vous invite à entrer les informations suivantes :
    - **Adresse e-mail :** adresse de messagerie de la personne ou du compte de rôle qui est responsable de la gestion du certificat.
    - **Nom commun :** nom commun de la personne ou compte de rôle qui est responsable de la gestion du certificat.
    - **Adresse e-mail de l'AC :** adresse de messagerie de l'autorité de certification.
4. Sélectionnez **Enregistrée sur le disque** et **Me laisser indiquer les informations sur la bi-clé** et cliquez sur **Continuer**.
5. Entrez un nom pour le fichier CSR, enregistrez le fichier sur votre ordinateur, puis cliquez sur **Enregistrer**.
6. Spécifiez les informations de bi-clé en sélectionnant la **Dimension de clé** de 2048 bits et **Algorithme RSA**, puis cliquez sur **Continuer**. Le fichier CSR est prêt à être chargé dans le cadre du processus de certificat APNS.
7. Cliquez sur **Terminé** lorsque l'Assistant de certification termine le processus de demande de signature de certificat.
8. Pour continuer, signez la CSR.

Créer une demande de signature de certificat à l'aide de Microsoft IIS

La première étape de génération d'une demande de certificat APNS consiste à créer une demande de signature de certificat (CSR). Pour Windows, générez une CSR à l'aide de Microsoft IIS.

1. Ouvrez Microsoft IIS.
2. Double-cliquez sur l'icône Certificats de serveur pour IIS.
3. Dans la fenêtre **Certificats de serveur**, cliquez sur **Créer une demande de certificat**.
4. Tapez les informations de nom unique (DN) appropriées, puis cliquez sur **Suivant**.
5. Sélectionnez le **Fournisseur de services de chiffrement Microsoft RSA SChannel** pour le fournisseur de services de chiffrement et **2048** pour la longueur en bits, puis cliquez sur **Suivant**.
6. Entrez un nom de fichier et spécifiez un emplacement pour enregistrer la CSR, puis cliquez sur **Terminer**.
7. Pour continuer, signez la CSR.

Créer une demande de signature de certificat avec OpenSSL

Si vous ne pouvez pas utiliser un appareil macOS ou Microsoft IIS pour générer une demande de signature de certificat, utilisez OpenSSL. Vous pouvez télécharger et installer OpenSSL à partir du site Web OpenSSL.

1. Sur l'ordinateur sur lequel vous avez installé OpenSSL, exécutez la commande suivante à partir d'une invite de commandes ou de shell.

   ```
   openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.
   csr -newkey rsa:2048
   ```

2. Le message suivant s'affiche pour les informations de nom du certificat. Entrez les informations demandées.

   ```
   1  You are about to be asked to enter information that will be
          incorporated into your certificate request.
   2  What you are about to enter is what is called a Distinguished Name
           or a DN.
   3  There are quite a few fields but you can leave some blank
   4  For some fields there will be a default value,
   5  If you enter '.', the field will be left blank.
   6  -----
   7  Country Name (2 letter code) [AU]:US
   8  State or Province Name (full name) [Some-State]:CA
   9  Locality Name (eg, city) []:RWC
   10 Organization Name (eg, company) [Internet Widgits Pty Ltd]:
          Customer
   11 Organizational Unit Name (eg, section) [:Marketing
   12 Common Name (eg, YOUR name) []:John Doe
   13 Email Address []:john.doe@customer.com
   14 <!--NeedCopy-->
   ```

3. Dans le message suivant, entrez un mot de passe pour la clé privée de la demande de signature de certificat.

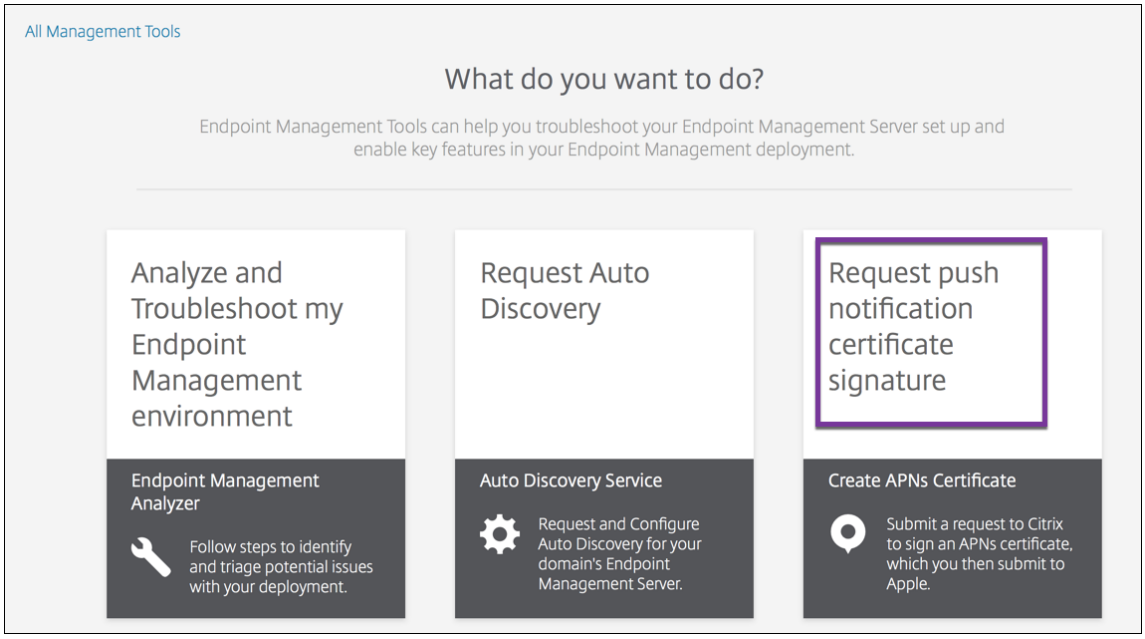
   ```
   1  Please enter the following 'extra' attributes
   2  to be sent with your certificate request
   3  A challenge password []:
   4  An optional company name []:
   5  <!--NeedCopy-->
   ```

4. Pour continuer, signez la demande de signature de certificat comme décrit dans la section suivante.

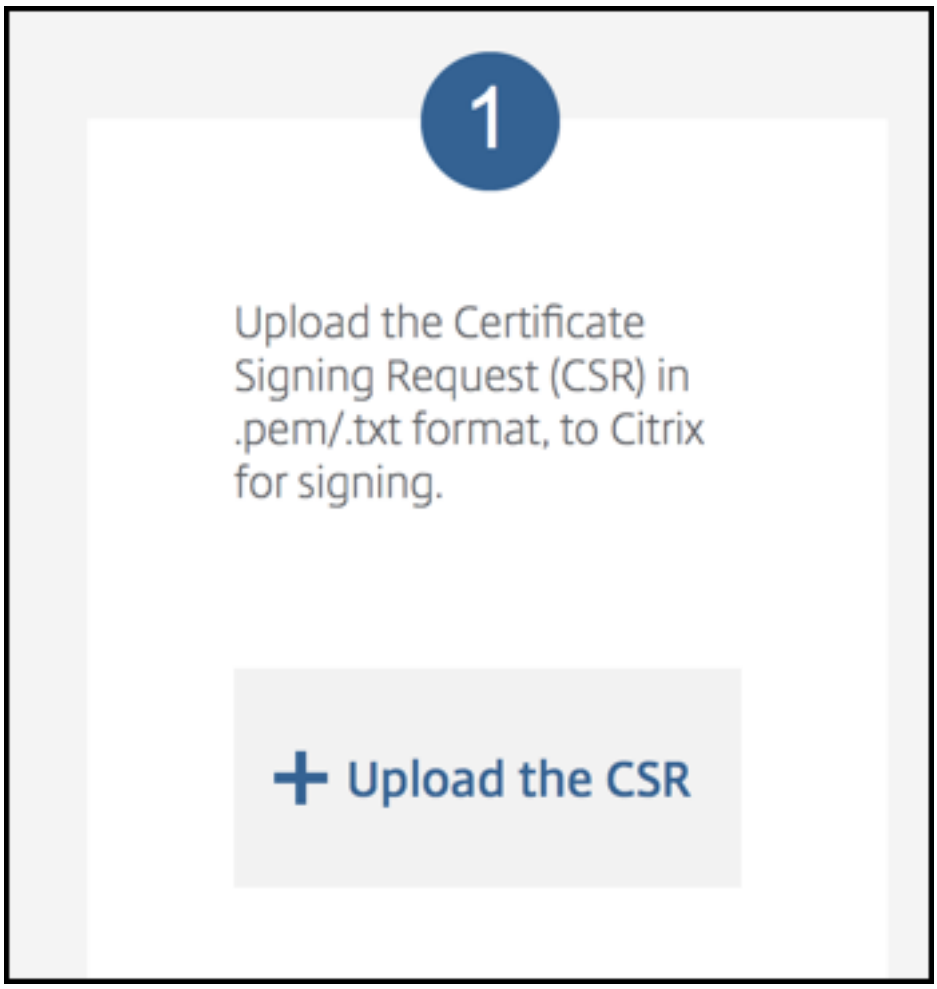
Signer la demande de signature de certificat

Pour utiliser un certificat avec XenMobile, soumettez-le à Citrix pour signature. Citrix signe la demande de signature de certificat (CSR) à l'aide de son certificat de signature de gestion d'appareils mobiles et renvoie le fichier signé au format `.plist`.

1. Dans votre navigateur, accédez au site Web Endpoint Management Tools, puis cliquez sur **Request push notification certificate signature**.



2. Sur la page **Creating a new certificate**, cliquez sur **Upload the CSR**.



3. Localisez et sélectionnez le certificat.

   Le certificat doit être au format .pem/txt.

4. Sur la page **Endpoint Management APNs CSR Signing**, cliquez sur **Sign**. La demande de signature de certificat est signée et automatiquement enregistrée sur votre dossier de téléchargement configuré.
5. Pour continuer, soumettez la demande de signature de certificat signée comme décrit dans la section suivante.

Soumettre la demande de signature de certificat à Apple afin d'obtenir le certificat APNS

Après la réception de votre demande de signature de certificat (CSR) signée de Citrix, envoyez-la à Apple pour obtenir le certificat APNS nécessaire à l'importation dans XenMobile.

> **Remarque :**
>
> Certains utilisateurs ont signalé des problèmes lors de la connexion au portail Apple Push Portal. Vous pouvez également vous connecter au portail Apple Developer Portal, puis suivez ces étapes.

1. Dans un navigateur, accédez au portail Apple Push Certificates Portal.
2. Cliquez sur **Create a Certificate**.
3. La première fois que vous créez un certificat avec Apple, sélectionnez la case **I have read and agree to these terms and conditions** et cliquez sur **Accept**.
4. Cliquez sur **Choose File** pour charger votre demande de signature de certificat signée, accédez à la demande sur votre ordinateur, puis cliquez sur **Upload**. Un message de confirmation indique que le chargement a réussi.
5. Cliquez sur **Download** pour récupérer le certificat .pem.
6. Pour continuer, remplissez la demande de signature de certificat et exportez un fichier PKCS #12 comme décrit dans la section suivante.

Terminer la demande de signature de certificat et exporter un fichier PKCS #12

Après la réception de votre certificat APNS d'Apple, revenez à l'application Trousseau d'accès, Microsoft IIS ou OpenSSL pour exporter le certificat dans un fichier PCKS #12.

Un fichier PKCS #12 contient le fichier de certificat APNS, ainsi que votre clé privée. Les fichiers PFX ont généralement l'extension .pfx ou .p12. Vous pouvez utiliser les fichiers .pfx et .p12 de manière interchangeable.

> **Important :**
>
> Citrix vous recommande d'enregistrer ou d'exporter les clés personnelles et publiques du système local. Vous avez besoin des clés pour accéder aux certificats APNS à réutiliser. Sans ces clés, votre certificat n'est pas valide et vous devez répéter l'intégralité du processus de demande de signature de certificat et le processus APNS.

Créer un fichier PKCS #12 à l'aide de l'application Trousseau d'accès sur macOS

> **Important :**
>
> Utilisez le même appareil macOS pour cette tâche que vous avez utilisé pour générer la demande de signature de certificat.

1. Sur l'appareil, recherchez le certificat d'identité de produit (.pem) d'Apple.
2. Démarrez l'application Trousseaux d'accès et accédez à l'onglet **Connexion > Mes certificats**. Faites glisser et déposez le certificat d'identité de produit dans la fenêtre ouverte.

3. Cliquez sur le certificat et développez la flèche gauche pour vérifier que le certificat inclut une clé privée associée.
4. Pour commencer l'exportation du certificat dans un certificat PCKS #12 (.pfx), choisissez le certificat et la clé privée, cliquez avec le bouton droit de la souris, puis sélectionnez **Exporter 2 éléments**.
5. Donnez au fichier de certificat un nom unique à utiliser avec XenMobile. N'insérez pas d'espace dans le nom. Ensuite, choisissez un emplacement de dossier pour le certificat enregistré, sélectionnez le format du fichier .pfx, puis cliquez sur **Enregistrer**.
6. Entrez un mot de passe pour l'exportation du certificat. Citrix vous recommande d'utiliser un mot de passe fort et unique. Par ailleurs, conservez le certificat et le mot de passe de manière sécurisée à des fins d'utilisation ultérieure et de référence.
7. L'application Trousseau d'accès vous invite à saisir le mot de passe ou le trousseau sélectionné. Tapez le mot de passe, puis cliquez sur **OK**. Le certificat enregistré est maintenant prêt à être utilisé avec XenMobile server.
8. Pour continuer, consultez Importer un certificat APNs dans XenMobile.

Créer un fichier PKCS #12 à l'aide de Microsoft IIS

> **Important :**
>
> Utilisez le même serveur IIS pour cette tâche que vous avez utilisé pour générer la demande de signature de certificat.

1. Ouvrez Microsoft IIS.
2. Cliquez sur l'icône **Certificats de serveur**.
3. Dans la fenêtre **Certificats de serveur**, cliquez sur **Terminer la demande de certificat**.
4. Accédez au fichier Certificate.pem d'Apple. Tapez ensuite un nom convivial ou le nom du certificat, puis cliquez sur **OK**. N'insérez pas d'espace dans le nom.
5. Sélectionnez le certificat que vous avez identifié dans l'étape 4, puis cliquez sur **Exporter**.
6. Spécifiez un emplacement et un nom de fichier pour le certificat .pfx ainsi qu'un mot de passe, puis cliquez sur **OK**.

   Vous devez fournir le mot de passe du certificat pour l'importer dans XenMobile.
7. Copiez le certificat .pfx sur le serveur sur lequel XenMobile sera installé.
8. Pour continuer, consultez Importer un certificat APNs dans XenMobile.

Créer un fichier PKCS #12 avec OpenSSL

Si vous utilisez OpenSSL pour créer une demande de signature de certificat, vous pouvez également utiliser OpenSSL pour créer un certificat APNS .pfx.

1. À l'invite de commandes ou shell, exécutez la commande suivante. `Customer.privatekey.pem` est la clé privée de votre demande de signature de certificat et `APNs_Certificate.pem` le certificat que vous venez de recevoir d'Apple.

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey
   .pem -out apns_identity.pfx
   ```

2. Entrez un mot de passe pour le fichier de certificat .pfx. Mémorisez ce mot de passe car vous devez l'utiliser pour charger le certificat sur XenMobile.
3. Notez l'emplacement du fichier de certificat .pfx. Copiez ensuite le fichier sur le serveur XenMobile, de façon à pouvoir utiliser la console pour charger le fichier.
4. Pour continuer, importez un certificat APNS dans XenMobile comme décrit dans la section suivante.

Importer un certificat APNS dans XenMobile

Une fois que vous avez reçu un nouveau certificat APNS, vous devez l'importer dans XenMobile pour ajouter le certificat (pour la première fois) ou remplacer un certificat.

1. Dans la console XenMobile, accédez à **Paramètres > Certificats**.
2. Cliquez sur **Importer > Keystore**.
3. Dans **Utiliser en tant que**, choisissez **APNS**.
4. Accédez au fichier .pfx ou .p12 sur votre ordinateur.
5. Entrez un mot de passe, puis cliquez sur **Importer**.

Pour de plus amples informations sur les certificats dans XenMobile, consultez la section Certificats et authentification.

Renouveler un certificat APNS

> **Important :**
>
> Si vous utilisez un identifiant Apple ID différent pour le processus de renouvellement, vous devez réinscrire les appareils utilisateur.

Pour renouveler un certificat APNs, procédez comme suit pour créer un certificat, puis accédez au portail Apple Push Certificates Portal. Utilisez ce portail pour charger le nouveau certificat. Une fois

la session ouverte, votre certificat existant ou un certificat importé à partir de votre ancien compte Apple Developers apparaît.

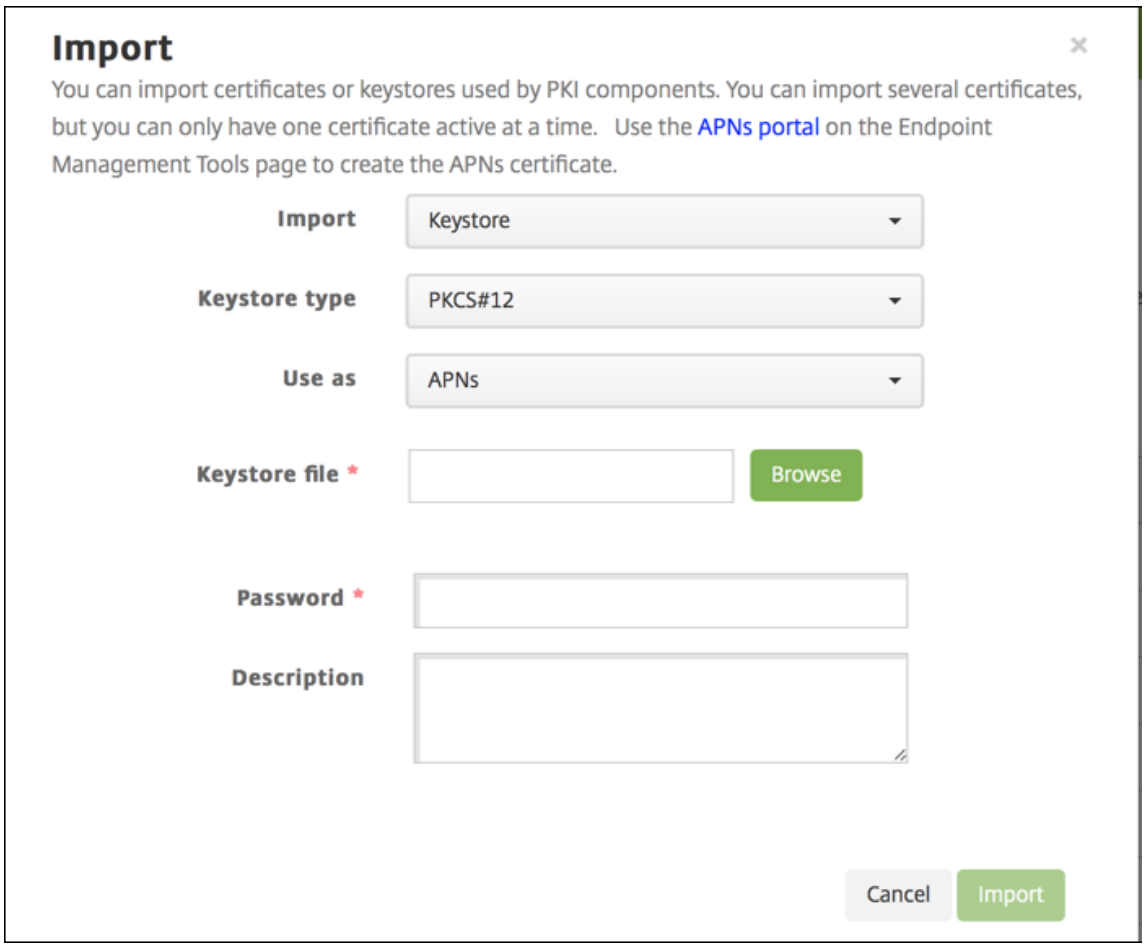
Sur la page Certificats Portal, la seule différence lors du renouvellement du certificat est que vous cliquez sur **Renew**. Vous devez avoir un compte de développeur auprès du Certificates Portal pour accéder au site. Pour renouveler votre certificat, utilisez le même nom d'organisation et le même identifiant Apple ID.

Pour déterminer la date à laquelle votre certificat APNS expire, dans la console XenMobile, accédez à **Paramètres > Certificats**. Si le certificat expire, ne le révoquez pas.

1. Générez une demande de signature de certificat à l'aide de Microsoft IIS, l'application Trousseau d'accès (macOS) ou OpenSSL. Pour plus d'informations sur la génération d'une CSR, consultez Créer une demande de signature de certificat.
2. Dans votre navigateur, accédez à XenMobile Tools. Cliquez ensuite sur **Request push notification certificate signature**.
3. Cliquez sur **+Upload the CSR**.
4. Dans la boîte de dialogue, accédez à la CSR, cliquez sur **Open**, puis sur **Sign**.
5. Lorsque vous recevez un fichier `.plist`, enregistrez-le.
6. Dans le titre de l'étape 3, cliquez sur **Apple Push Certificates Portal** et connectez-vous.
7. Sélectionnez le certificat que vous souhaitez renouveler et cliquez sur **Renew**.
8. Chargez le fichier `.plist`. Vous devriez recevoir un fichier .pem en sortie. Enregistrez le fichier .pem.
9. À l'aide du fichier .pem, complétez la CSR (en fonction de la méthode utilisée pour créer la CSR à l'étape 1).
10. Exportez le certificat en tant que fichier .pfx.

Dans la console XenMobile, importez le fichier .pfx et procédez à la configuration comme suit :

1. Accédez à **Paramètres > Certificats > Importer**.
2. Depuis le menu **Importer**, sélectionnez **Keystore**.
3. Dans le menu **Type de keystore**, choisissez **PKCS #12**.
4. Dans **Utiliser en tant que**, choisissez **APNS**.



5. Sous **Fichier de keystore**, cliquez sur **Parcourir** et accédez au fichier.
6. Sous **Mot de passe**, entrez le mot de passe du certificat.
7. Entrez une **Description** (facultatif).
8. Cliquez sur **Importer**.

XenMobile vous redirige vers la page **Certificats**. Les champs **Nom**, **État**, **Valide du** et **Valide jusqu'au** sont mis à jour.

SAML pour l'authentification unique avec Citrix Files

January 10, 2022

Vous pouvez configurer XenMobile et Content Collaboration pour une utilisation avec SAML (Security Assertion Markup Language) afin de fournir l'accès SSO aux applications mobiles Citrix Files. Cette fonctionnalité comprend les éléments suivants :

- Applications Citrix Files pour lesquelles le SDK MAM est activé ou qui sont encapsulées à l'aide de MDX Toolkit
- Clients Citrix Files non encapsulés, tels que le site Web, Outlook Plug-in ou les clients de synchronisation
- **Pour les applications Citrix Files encapsulées**. Les utilisateurs qui ouvrent une session sur Citrix Files via l'application mobile Citrix Files sont redirigés vers Secure Hub pour l'authentification utilisateur et pour acquérir un jeton SAML. Une fois l'authentification réussie, l'application mobile Citrix Files envoie le jeton SAML à Content Collaboration. Après la première ouverture de session, les utilisateurs peuvent accéder à l'application mobile Citrix Files via l'authentification unique. Ils peuvent également joindre des documents de Content Collaboration aux e-mails Secure Mail sans se connecter à chaque fois.
- **Pour les clients Citrix Files non encapsulés**. Les utilisateurs qui se connectent à Citrix Files à l'aide d'un navigateur Web ou d'un autre client Citrix Files sont redirigés vers XenMobile. XenMobile authentifie les utilisateurs, qui acquièrent ensuite un jeton SAML envoyé à Content Collaboration. Après la première ouverture de session, les utilisateurs peuvent accéder aux clients Citrix Files via l'authentification unique sans se connecter à chaque fois.

Pour utiliser XenMobile en tant que fournisseur d'identité SAML pour Content Collaboration, vous devez configurer XenMobile pour l'utilisation de comptes Enterprise, comme décrit dans cet article. Vous pouvez également configurer XenMobile pour fonctionner uniquement avec des connecteurs StorageZone. Pour de plus amples informations, consultez la section Utiliser Citrix Content Collaboration avec XenMobile.

Pour un diagramme d'architecture de référence détaillé, voir Architecture.

Conditions préalables

Vous devez remplir les conditions suivantes pour pouvoir configurer l'authentification unique avec les applications XenMobile et Citrix Files :

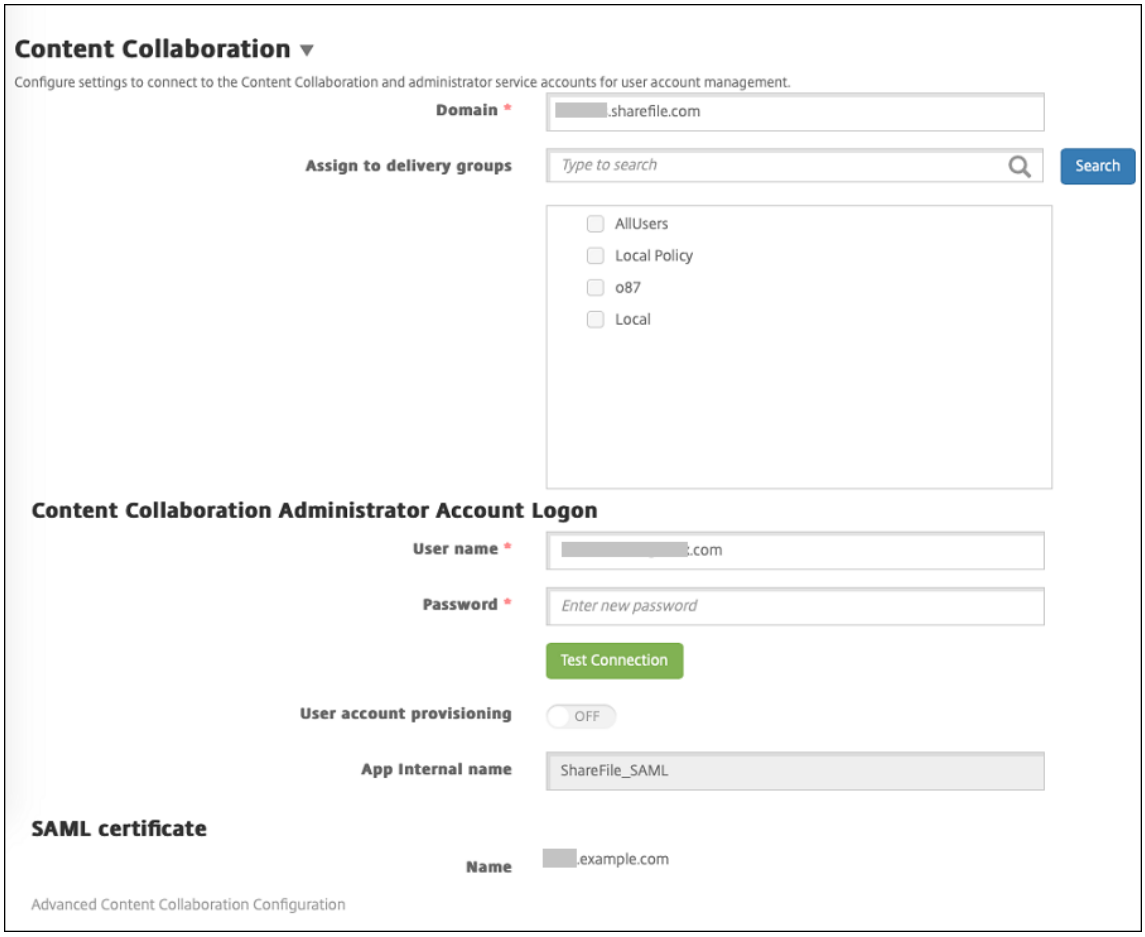
- SDK MAM ou une version compatible de l'outil MDX Toolkit (pour les applications mobiles Citrix Files)

  Pour de plus amples informations, consultez la section Compatibilité XenMobile.
- Version compatible de Secure Hub et des applications mobiles Citrix Files
- Compte administrateur Content Collaboration
- Connectivité vérifiée entre XenMobile et Content Collaboration

Configurer l'accès à Content Collaboration

Avant de configurer SAML pour Content Collaboration, fournissez les informations d'accès à Content Collaboration comme suit :

1. Dans la console Web XenMobile, cliquez sur **Configurer > ShareFile**. La page de configuration de **ShareFile** s'affiche. Votre console peut afficher le terme Content Collaboration au lieu de ShareFile.



2. Pour configurer ces paramètres :
   - **Domaine :** entrez le nom de votre sous-domaine Content Collaboration. Par exemple : `example.sharefile.com`.
   - **Attribuer aux groupes de mise à disposition :** sélectionnez ou recherchez les groupes de mise à disposition que vous souhaitez autoriser à utiliser l'authentification unique avec Content Collaboration.
   - **Connexion au compte administrateur ShareFile**
   - **Nom d'utilisateur :** entrez le nom d'utilisateur de l'administrateur Content Collaboration. Cet utilisateur doit disposer des privilèges d'administrateur.
   - **Mot de passe :** entrez le mot de passe administrateur de Content Collaboration.

- **Provisioning du compte utilisateur :** laissez ce paramètre désactivé. Utilisez l'outil de gestion des utilisateurs Content Collaboration pour le provisioning des utilisateurs. Voir Provisionner des comptes d'utilisateurs et des groupes de distribution.

3. Cliquez sur **Tester la connexion** pour vérifier que le nom d'utilisateur et le mot de passe du compte administrateur Content Collaboration permettent de s'authentifier auprès du compte Content Collaboration spécifié.
4. Cliquez sur **Enregistrer**.
   - XenMobile se synchronise avec Content Collaboration et met à jour les paramètres Content Collaboration **ID d'émetteur/d'entité ShareFile** et **URL de connexion**.
   - La page **Configurer > ShareFile** affiche le champ **Nom interne de l'application**. Vous avez besoin de ce nom pour effectuer les étapes décrites plus loin dans Modifier les paramètres d'authentification unique de Citrix Files.com.

Configurer SAML pour les applications Citrix Files MDX encapsulées

Vous n'avez pas besoin d'utiliser Citrix Gateway pour la configuration de l'authentification unique avec les applications MDX Citrix Files encapsulées. Pour configurer l'accès aux clients Citrix Files non encapsulés, tels que le site Web, Outlook Plug-in ou les clients de synchronisation, consultez Configurer Citrix Gateway pour d'autres clients Citrix Files.

Les étapes suivantes s'appliquent aux applications et appareils iOS et Android. Pour configurer SAML pour les applications MDX Citrix Files encapsulées :

1. À l'aide du MDX Toolkit, encapsulez l'application mobile Citrix Files. Pour de plus amples informations sur l'encapsulation d'applications avec le MDX Toolkit, consultez la section Encapsulation des applications avec le MDX Toolkit.
2. Dans la console XenMobile, chargez l'application mobile Citrix Files encapsulée. Pour plus d'informations sur le chargement des applications MDX, consultez la section Pour ajouter une application MDX à XenMobile.
3. Vérifiez les paramètres SAML : ouvrez une session Content Collaboration avec le nom d'utilisateur et le mot de passe administrateur que vous avez configurés auparavant.
4. Vérifiez que Content Collaboration et XenMobile sont configurés pour le même fuseau horaire. Assurez-vous que XenMobile indique l'heure appropriée par rapport au fuseau horaire configuré. Sinon, l'authentification unique peut échouer.

Valider l'application mobile Citrix Files

1. Sur la machine utilisateur, installez et configurez Secure Hub.

2. À partir de XenMobile Store, téléchargez et installez l'application mobile Citrix Files.
3. Démarrez l'application mobile Citrix Files. Citrix Files démarre sans vous inviter à saisir un nom d'utilisateur ou un mot de passe.

Valider avec Secure Mail

1. Sur la machine utilisateur, si cela n'a pas déjà été fait, installez et configurez Secure Hub.
2. À partir de XenMobile Store, téléchargez, installez et configurez Secure Mail.
3. Ouvrez un nouveau formulaire électronique et appuyez sur **Joindre à partir de Citrix Files**. Les fichiers pouvant être joints à l'e-mail sont affichés sans vous inviter à saisir un nom d'utilisateur ou un mot de passe.

Configurer Citrix Gateway pour d'autres clients Citrix Files

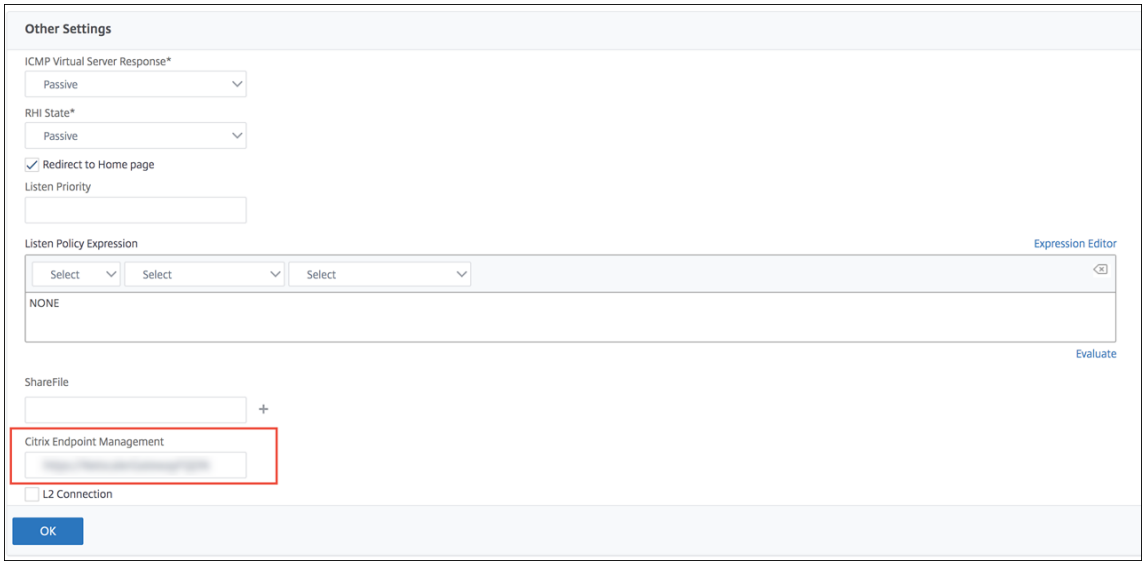
Pour configurer l'accès des clients Citrix Files non encapsulés, tels que le site Web, le plug-in Outlook ou les clients de synchronisation, vous devez configurer Citrix Gateway pour prendre en charge l'utilisation de XenMobile en tant que fournisseur d'identité SAML de la manière suivante.

- Désactivez la redirection vers la page d'accueil.
- Créez une stratégie et un profil de session Citrix Files.
- Configurez des stratégies sur le serveur virtuel Citrix Gateway.

Désactiver la redirection vers la page d'accueil

Désactivez le comportement par défaut pour les demandes qui passent par le chemin / cginfra. Cette action permet aux utilisateurs de voir l'URL interne demandée à la place de la page d'accueil configurée.

1. Modifiez les paramètres du serveur virtuel Citrix Gateway qui est utilisé pour les ouvertures de session XenMobile. Dans Citrix ADC, cliquez sur **Other Settings**, puis désactivez la case à cocher intitulée **Redirect to Home Page**.



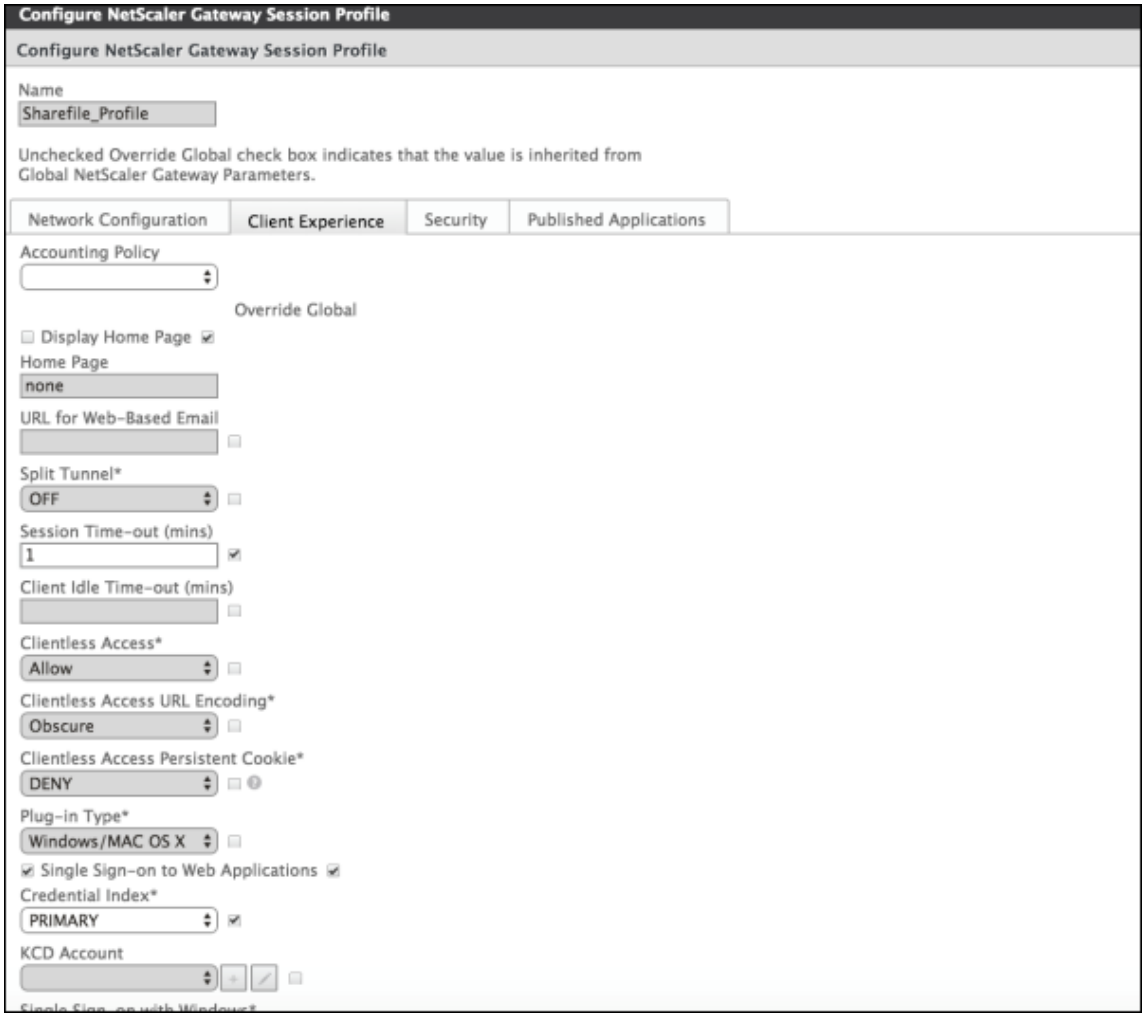
2. Sous **ShareFile** (à présent renommé Content Collaboration), entrez le nom et le numéro de port de votre serveur interne XenMobile.
3. Sous **Citrix Endpoint Management**, tapez votre URL XenMobile. Votre version de Citrix Gateway peut faire référence à l'ancien nom de produit **AppController**.

   Cette configuration autorise les demandes pour l'URL indiquée via le chemin d'accès /cginfra.

Créez une stratégie et un profil de demande de session Citrix Files

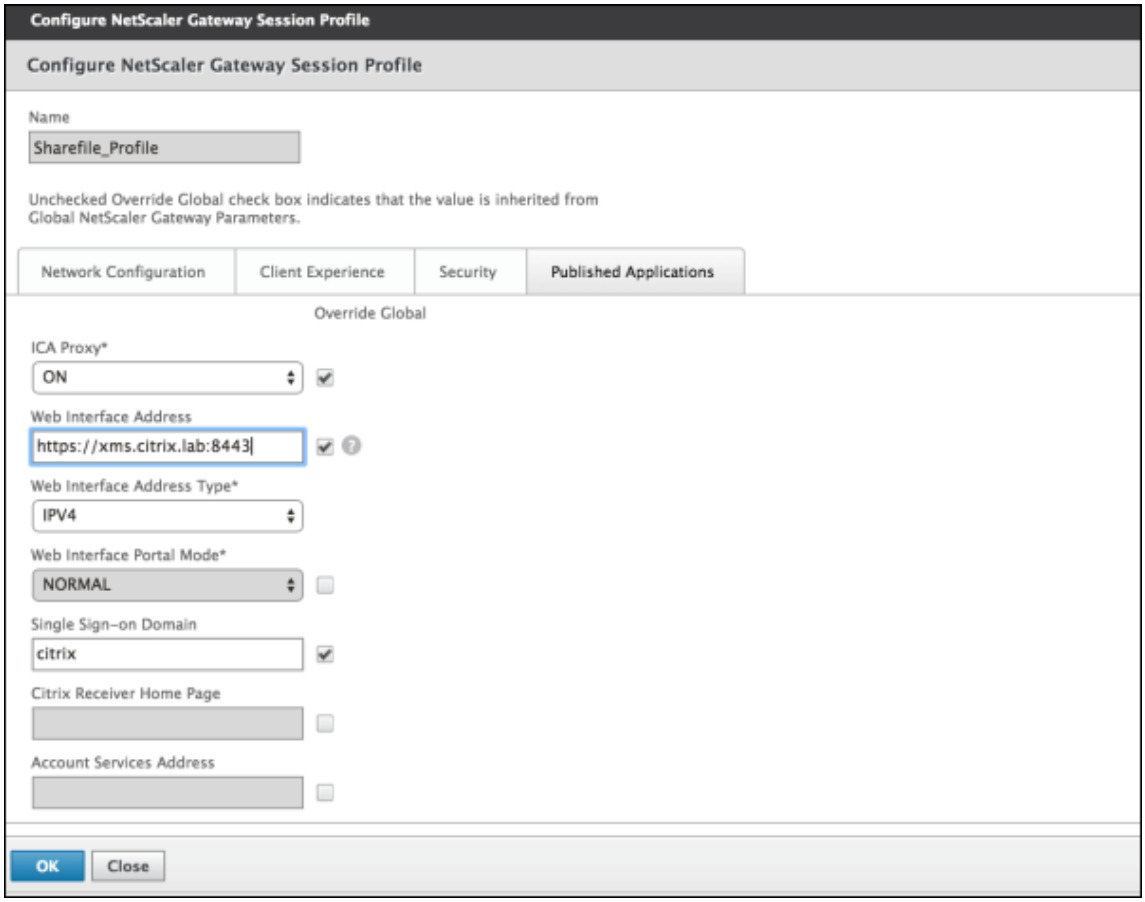
Configurez ces paramètres pour créer une stratégie et un profil de demande de session Citrix Files :

1. Dans l'utilitaire de configuration de Citrix Gateway, dans le volet de navigation de gauche, cliquez sur **Citrix Gateway > Policies > Session**.
2. Créez une stratégie de session. Dans l'onglet **Policies**, cliquez sur **Add**.
3. Dans le champ **Name**, tapez **ShareFile_Policy**.
4. Créez une action en cliquant sur le bouton **+**. La page **Create Session Profile** s'affiche.



Pour configurer ces paramètres :

- **Name :** tapez **ShareFile_Profile**.
- Cliquez sur l'onglet **Client Experience**, puis configurez les paramètres suivants :
  - **Home Page :** tapez **none**.
  - **Session Time-out (mins) :** tapez **1**.
  - **Single Sign-on to Web Applications :** sélectionnez ce paramètre.
  - **Credential Index :** dans la liste, cliquez sur **PRIMARY**.
- Cliquez sur l'onglet **Published Applications**.

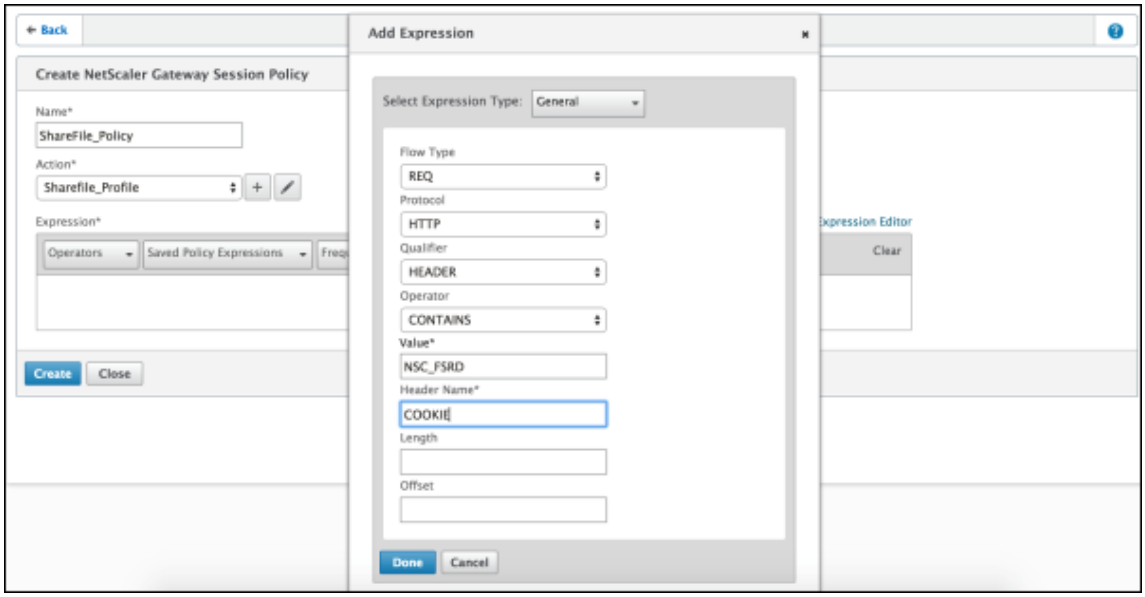


Pour configurer ces paramètres :

- **Proxy ICA :** dans la liste, cliquez sur **ON**.
- **Web Interface Address :** entrez l'URL de votre serveur XenMobile.
- **Single Sign-on Domain :** tapez votre nom de domaine Active Directory.

  Lors de la configuration du profil de session de Citrix Gateway, le suffixe de domaine pour **Single Sign-on Domain** doit correspondre à l'alias de domaine XenMobile défini dans LDAP.

5. Cliquez sur **Create** pour définir le profil de session.
6. Cliquez sur **Expression Editor**.



Pour configurer ces paramètres :

- **Value :** tapez **NSC_FSRD**.
- **Header Name :** tapez **COOKIE**.

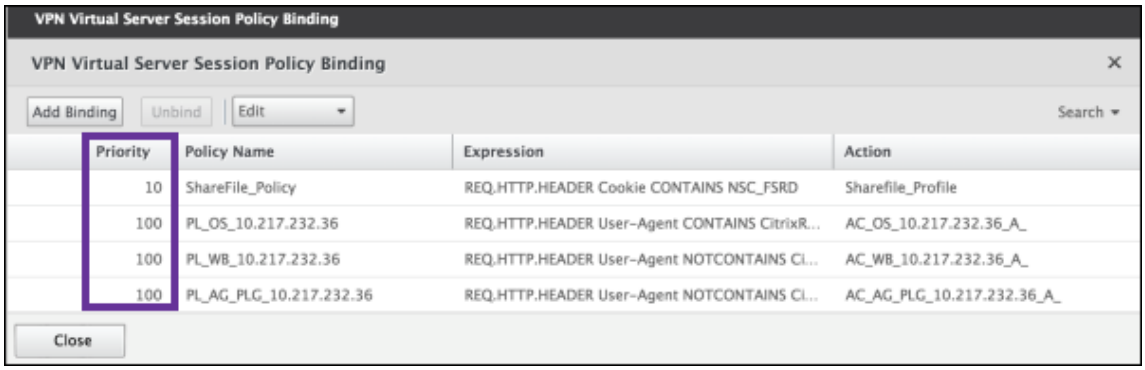
7. Cliquez sur **Create**, puis cliquez sur **Close**.

Configurer des stratégies sur le serveur virtuel Citrix Gateway

Configurez les paramètres suivants sur le serveur virtuel Citrix Gateway.

1. Dans l'utilitaire de configuration de Citrix Gateway, dans le volet de navigation de gauche, cliquez sur **Citrix Gateway > Virtual Servers**.
2. Dans le panneau **Details**, cliquez sur votre serveur virtuel Citrix Gateway.
3. Cliquez sur **Modifier**.
4. Cliquez sur **Configured policies > Session policies**, puis sur **Add binding**.

5. Sélectionnez **ShareFile_Policy**.
6. Modifiez le numéro de **priorité** (Priority) généré automatiquement pour la stratégie sélectionnée de manière à lui attribuer la priorité la plus élevée (le plus petit nombre) par rapport aux autres stratégies indiquées. Par exemple :



7. Cliquez sur **Done**, puis enregistrez la configuration Citrix ADC actuelle.

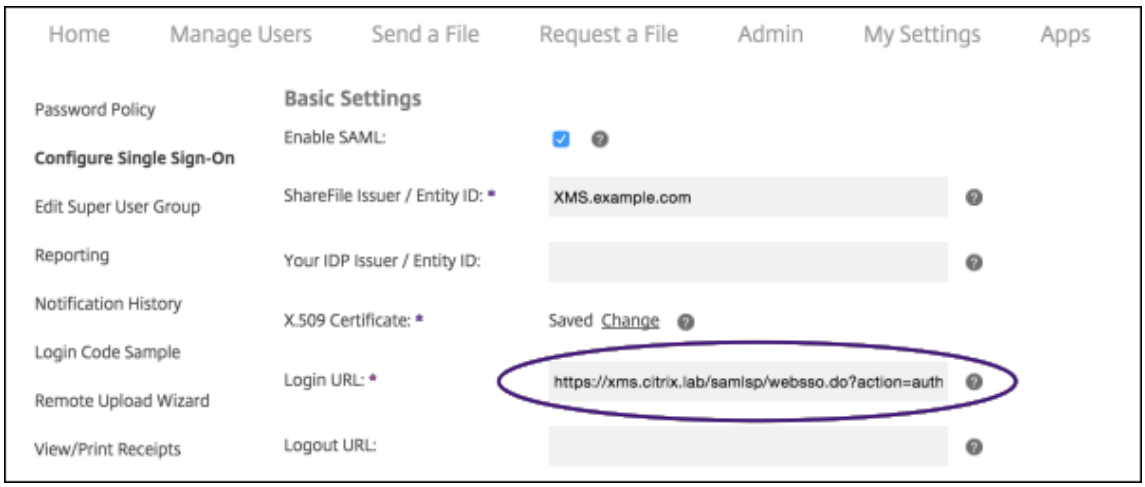
Modifier les paramètres d'authentification unique de Citrix Files.com

Apportez les modifications suivantes pour les applications MDX et non-MDX Citrix Files.

> **Important :**
>
> Un nouveau numéro est ajouté au nom de l'application interne :
>
> - Chaque fois que vous modifiez ou recréez l'application Citrix Files
> - Chaque fois que vous modifiez les paramètres de Content Collaboration dans XenMobile
>
> Par conséquent, vous devez également mettre à jour l'URL de connexion dans le site Web Citrix Files pour refléter le nom d'application mis à jour.

1. Connectez-vous à votre compte Content Collaboration (`https://<subdomain>.sharefile.com`) en tant qu'administrateur Content Collaboration.
2. Dans l'interface Web Content Collaboration, cliquez sur **Admin**, puis sélectionnez **Configurer le Single Sign-On**.
3. Modifiez l'**URL de connexion** comme suit :

   Voici un exemple d'**URL de connexion** avant les modifications : `https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`.



- Insérez le nom de domaine complet (FQDN) externe du serveur virtuel de Citrix Gateway et **/cginfra/https/** devant le nom de domaine complet de XenMobile Server, puis ajoutez **8443** après le nom de domaine complet de XenMobile.

  Voici un exemple d'URL modifiée: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=SHareFile_SAML_SP&reqtype=1`

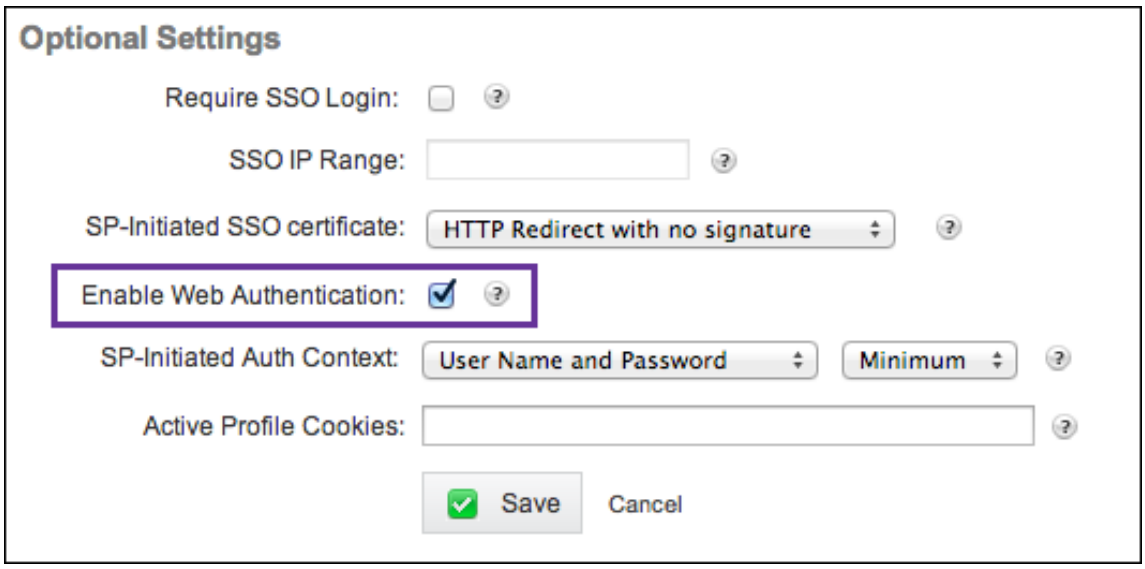
- Remplacez le paramètre &app=ShareFile_SAML_SP par le nom de l'application Citrix Files interne. Le nom interne est ShareFile_SAML par défaut. Toutefois, chaque fois que vous modifiez votre configuration, un numéro est ajouté au nom interne (ShareFile_SAML_2, ShareFile_SAML_3, etc.). Vous pouvez rechercher le **nom interne de l'application** sur la page **Configurer > ShareFile**.

  Voici un exemple d'URL modifiée: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- Ajoutez &nssso=**true** à la fin de l'URL.

  Voici un exemple de l'URL finale : `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`.

4. Sous **Paramètres facultatifs**, sélectionnez la case à cocher **Activer l'authentification Web**.



Valider la configuration

Procédez comme suit pour valider la configuration.

1. Pointez votre navigateur sur `https://<subdomain>sharefile.com/saml/login`.

   Vous êtes redirigé vers l'écran d'ouverture de session de Citrix Gateway. Si vous n'êtes pas redirigé, vérifiez les paramètres de configuration précédents.

2. Entrez le nom d'utilisateur et le mot de passe pour l'environnement Citrix Gateway et XenMobile que vous avez configuré.

   Vos dossiers Citrix Files à l'adresse `<subdomain>.sharefile.com` s'affichent. Si vos dossiers Citrix Files n'apparaissent pas, assurez-vous que les informations d'identification saisies pour l'ouverture de session sont correctes.

Azure Active Directory en tant que fournisseur d'identité (IdP)

January 10, 2022

La configuration d'Azure Active Directory (AAD) en tant que fournisseur d'identité (IdP) permet aux utilisateurs de s'inscrire auprès de XenMobile à l'aide de leurs informations d'identification Azure.

Les appareils iOS, Android, Windows 10 et Windows 11 sont pris en charge. Les appareils iOS et Android s'inscrivent via Secure Hub. Cette méthode d'authentification est disponible uniquement pour les utilisateurs qui s'inscrivent à MDM via l'application Citrix Secure Hub. Les appareils inscrits à MAM ne peuvent pas s'authentifier à l'aide des informations d'identification AAD. Pour utiliser Secure Hub

avec MDM+MAM, configurez XenMobile pour utiliser Citrix Gateway pour l'inscription MAM. Pour de plus amples informations, consultez Citrix Gateway et XenMobile.

Vous configurez Azure en tant que IdP sous **Paramètres > Authentification > IDP**. La page **IDP** a été ajoutée dans cette version de XenMobile. Dans les versions précédentes de XenMobile, vous configuriez Azure sous **Paramètres > Microsoft Azure**.

Exigences

- Versions et licences
  - Pour inscrire des appareils iOS ou Android, vous devez utiliser Secure Hub 10.5.5.
  - Pour inscrire des appareils Windows 10 et Windows 11, vous devez utiliser les licences Microsoft Azure Premium.
- Services Directory et authentification
  - XenMobile Server doit être configuré pour l'authentification basée sur certificat.
  - Si vous utilisez Citrix ADC pour l'authentification, Citrix ADC doit être configuré pour l'authentification basée sur les certificats.
  - L'authentification Secure Hub utilise Azure AD et respecte le mode d'authentification défini sur Azure AD.
  - XenMobile Server doit se connecter à Windows Active Directory (AD) à l'aide de LDAP. Configurez votre serveur LDAP local pour le synchroniser avec Azure AD.

Flux d'authentification

Lors de l'inscription de l'appareil via Secure Hub, si XenMobile est configuré pour utiliser Azure en tant que fournisseur d'identité (IdP) :

1. Les utilisateurs entrent leur nom d'utilisateur et mot de passe sur leur appareil, dans l'écran d'ouverture de session d'Azure AD affiché dans Secure Hub.
2. Azure Active Directory valide l'utilisateur et envoie un jeton d'ID.
3. Secure Hub partage le jeton d'ID avec XenMobile Server.
4. XenMobile valide le jeton d'ID et les informations utilisateur inclues dans le jeton d'ID. XenMobile renvoie un ID de session.

Configuration du compte Azure

Pour utiliser Azure Active Directory en tant que IdP, connectez-vous à votre compte Azure et effectuez ces modifications :

1. Enregistrez votre domaine personnalisé et vérifiez le domaine. Pour plus d'informations, consultez la page Ajouter votre nom de domaine personnalisé à l'aide du Portail Azure Active Directory.
2. Étendez votre annuaire local à Azure Active Directory à l'aide des outils d'intégration d'annuaire. Pour plus d'informations, consultez la page [Intégration d'annuaire](https://docs.microsoft.com/en-us/previous-versions/azure/azure-services/jj573653(v=azure.100).

Pour utiliser Azure Active Directory pour inscrire des appareils Windows 10 et Windows 11, apportez les modifications suivantes à votre compte Azure :

1. Faites du MDM une partie de confiance de Azure Active Directory. Pour ce faire, cliquez sur **Azure Active Directory > Applications**, puis sur **Ajouter**.
2. Sélectionnez **Ajouter une application** à partir de la galerie. Accédez à **Gestion des appareils mobiles**, puis sélectionnez **Paramètres d'application GPM locale**. Enregistrez les paramètres.

   Vous choisissez l'application locale même si vous êtes abonné à Citrix XenMobile Cloud. Selon la terminologie Microsoft, toute application non multi-locataire est une application MDM locale.
3. Dans l'application, configurez la détection de XenMobile Server, les points de terminaison des conditions d'utilisation et l'URI d'ID de l'application :
   - **URL de détection GAM :** `https://<FQDN>:8443/<instanceName>/wpe`
   - **URL des conditions d'utilisation de GAM :** `https://<FQDN>:8443/<instanceName>/wpe/tou`
   - **URI ID d'application :** `https://<FQDN>:8443/`
4. Sélectionnez l'application MDM locale que vous avez créée à l'étape 2. Activez l'option **Gérer les appareils pour ces utilisateurs** pour activer la gestion MDM pour tous les utilisateurs ou un groupe d'utilisateurs spécifique.

   Pour plus d'informations sur l'utilisation de Azure AD pour les appareils Windows 10 et Windows 11, consultez l'article Microsoft Azure Active Directory integration with MDM.

Configurer Azure AD en tant que fournisseur d'identité (IdP)

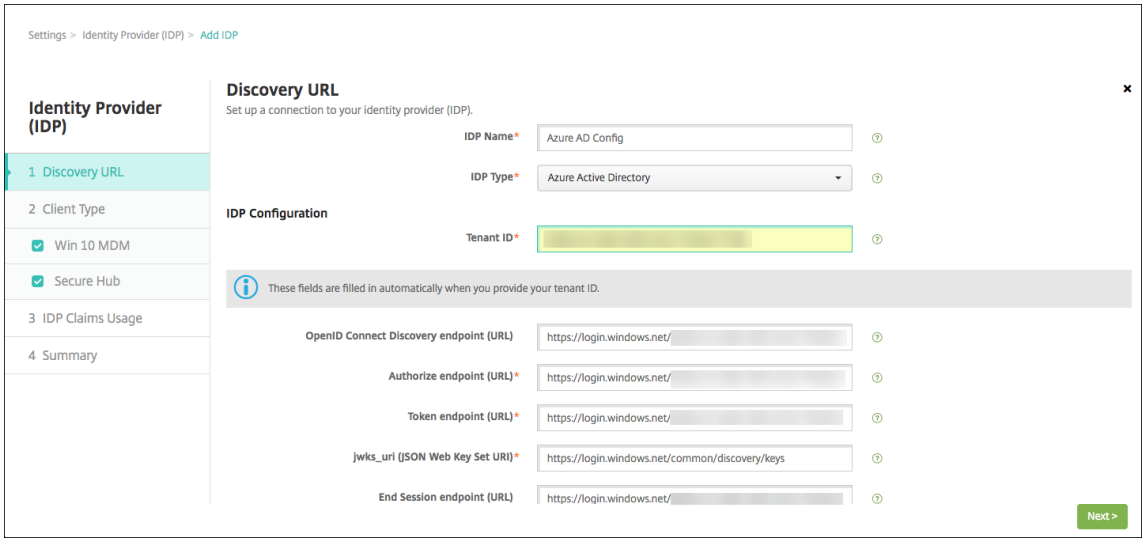
1. Recherchez ou prenez note des informations dont vous avez besoin sur votre compte Azure :
   - ID du locataire à partir de la page des paramètres d'application Azure.
   - Si vous souhaitez utiliser Azure Active Directory pour inscrire des appareils Windows 10 et Windows 11, vous avez aussi besoin des éléments suivants :
     - **URI ID d'application :** adresse URL du serveur exécutant XenMobile.
     - **ID client :** identificateur unique pour votre application depuis la page de configuration Azure.
     - **Clé :** dans la page des paramètres d'application Azure.

2. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
3. Sous **Authentification**, cliquez sur **Fournisseur d'identité (IDP)**. La page **Fournisseur d'identité** s'affiche.

4. Cliquez sur **Ajouter**. La page **Configuration IdP** s'affiche.
5. Configurez les informations suivantes sur votre IdP :

   - **Nom IdP :** entrez un nom pour la connexion de fournisseur d'identité que vous créez.
   - **Type d'IdP :** choisissez Azure Active Directory comme type de fournisseur d'identité.
   - **ID du locataire :** copiez cette valeur à partir de la page des paramètres d'application Azure. Dans la barre d'adresse du navigateur, copiez la section composée de chiffres et de lettres.

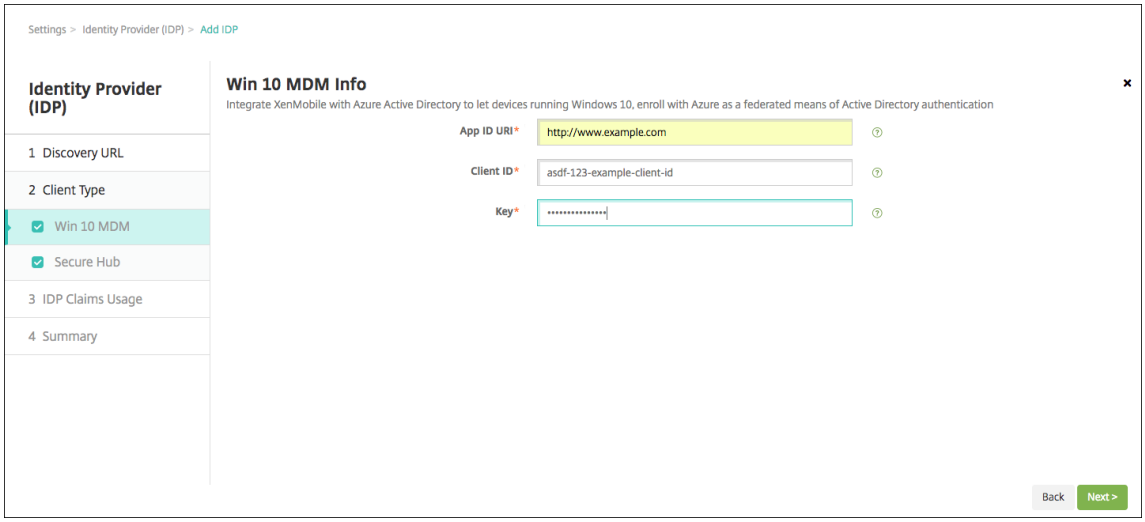
   Par exemple, dans `https://manage.windowszaure.com/acmew.onmicrosoft.com##workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...`, l'ID du locataire est `abc123-abc123-abc123`.



6. Les autres champs se remplissent automatiquement. Lorsqu'ils sont remplis, cliquez sur **Suivant**.

7. Pour configurer XenMobile pour inscrire des appareils Windows 10 et Windows 11 à l'aide de Azure AD pour l'inscription MDM, configurez les paramètres suivants. Pour ignorer cette étape facultative, désactivez **Windows MDM**.

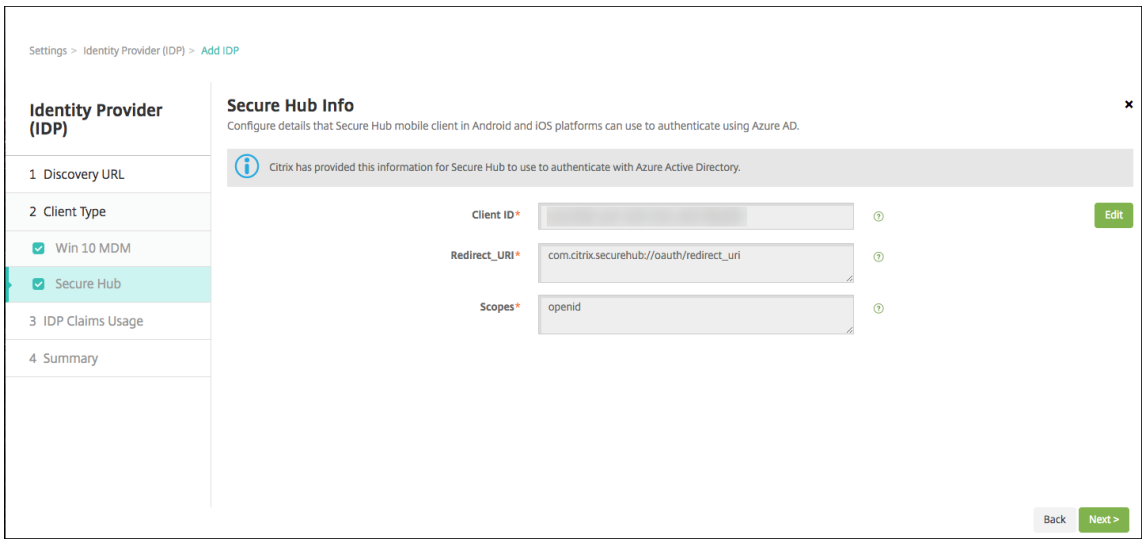
   - **URI ID application :** entrez l'adresse URL de l'instance XenMobile Server que vous avez entrée lorsque vous avez configuré vos paramètres Azure.
   - **ID du client :** copiez et collez cette valeur depuis la page de configuration Azure. L'ID du client est l'identificateur unique pour votre application.
   - **Clé :** copiez cette valeur à partir de la page des paramètres d'application Azure. Sous Clés, sélectionnez une durée dans la liste puis enregistrez le paramètre. Vous pouvez copier la clé et la coller dans ce champ. Une clé est requise lorsque les applications doivent lire et écrire des données dans Microsoft Azure Active Directory.



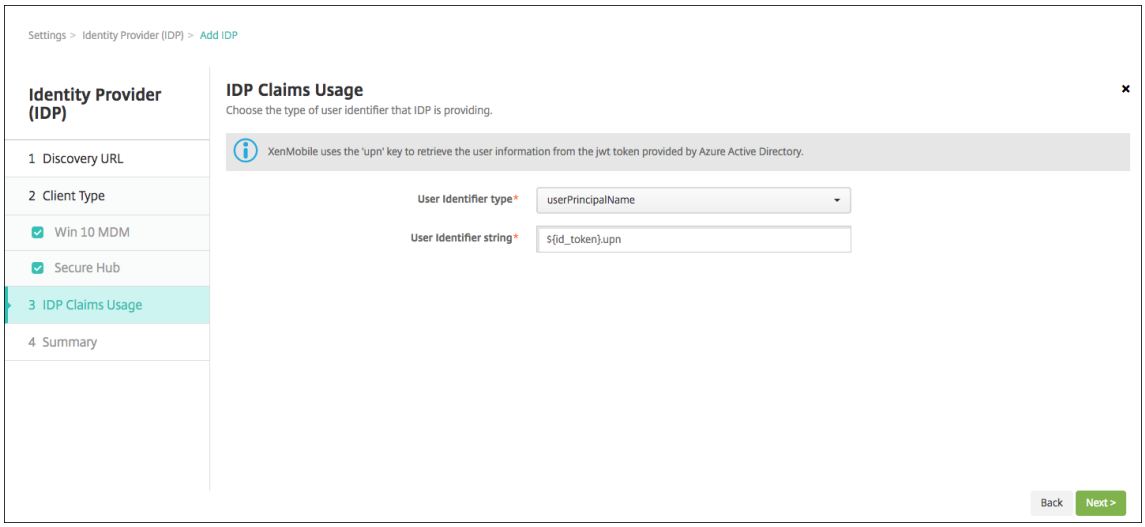
8. Cliquez sur **Suivant**.

   Citrix a enregistré Secure Hub avec Microsoft Azure et conserve les informations. Cet écran affiche les détails utilisés par Secure Hub pour communiquer avec Azure Active Directory. Cette page sera utilisée si certaines informations ont besoin d'être modifiées à l'avenir. Modifiez cette page uniquement si Citrix vous y invite.

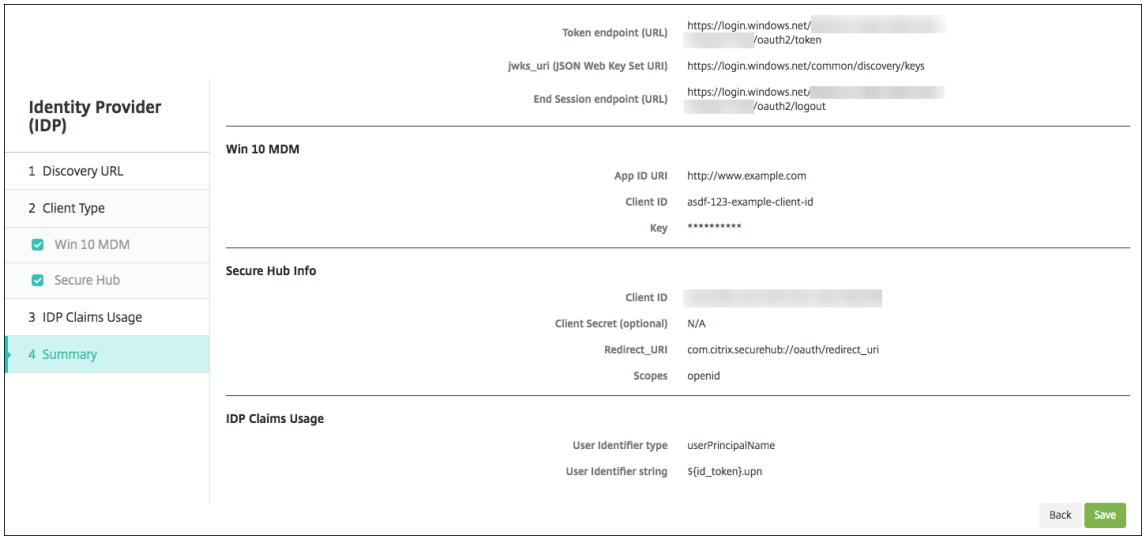
9. Cliquez sur **Suivant**.



10. Configurez le type d'identificateur d'utilisateur fourni par le fournisseur d'identité :
    - **Type d'identificateur d'utilisateur :** choisissez **userPrincipalName** dans la liste déroulante.
    - **Chaîne d'identificateur d'utilisateur :** ce champ est renseigné automatiquement.
11. Cliquez sur **Suivant**.

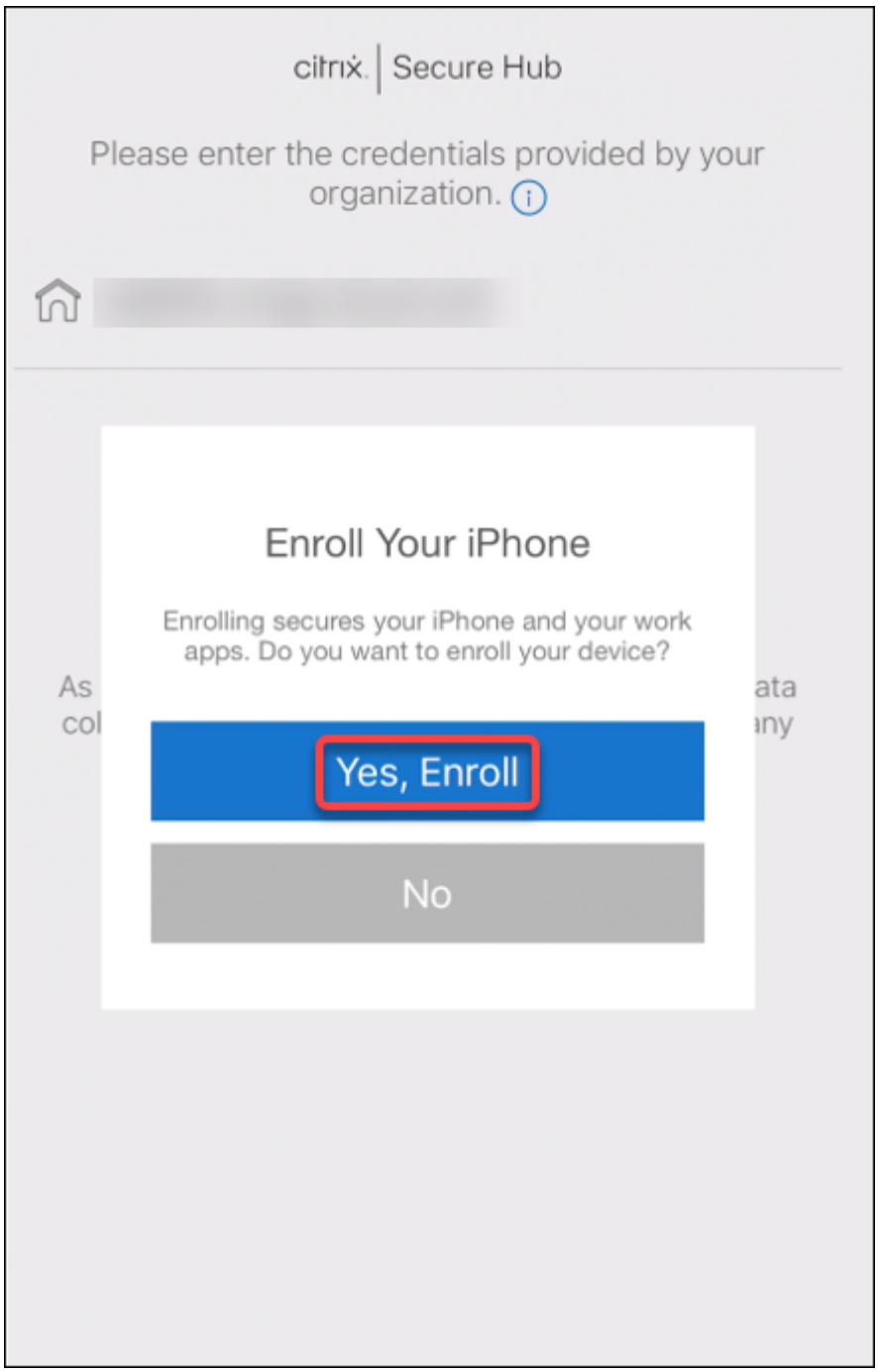


12. Vérifiez la page **Récapitulatif** et cliquez sur **Enregistrer**.

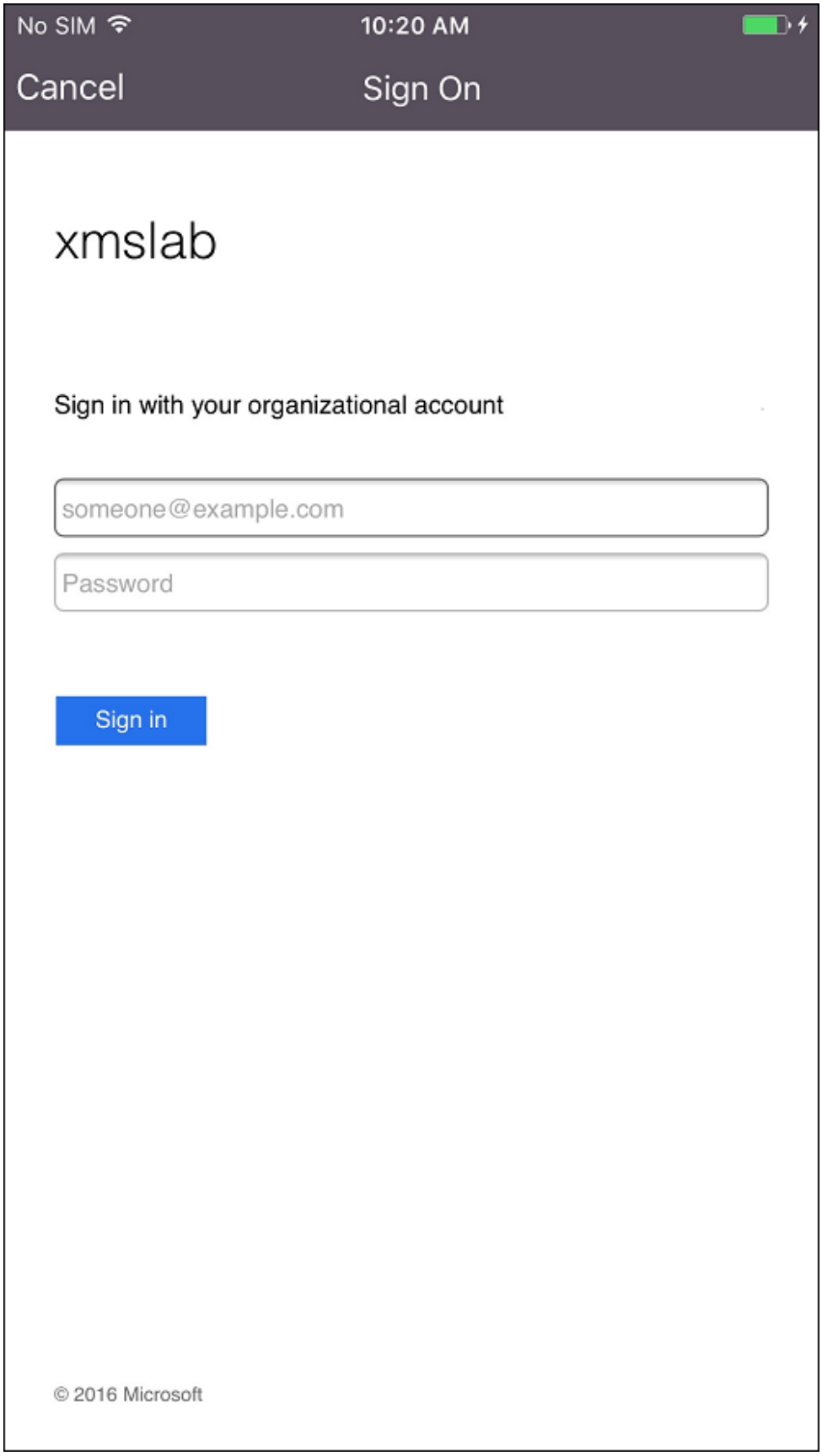


Expérience de l'utilisateur

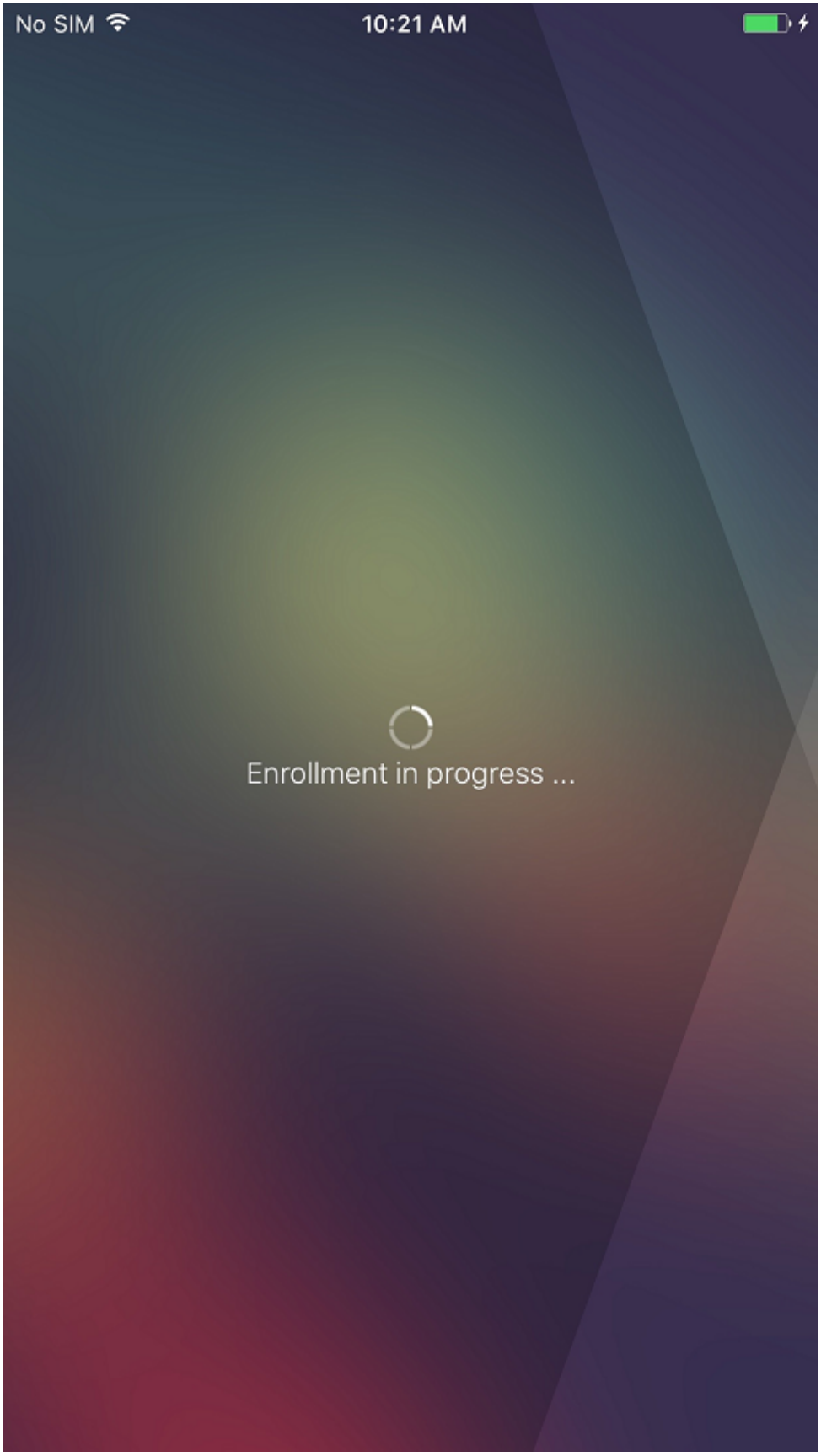
1. L'utilisateur démarre Secure Hub. Les utilisateurs entrent ensuite le nom de domaine complet de XenMobile Server, un nom de domaine principal d'utilisateur (UPN) ou une adresse e-mail.

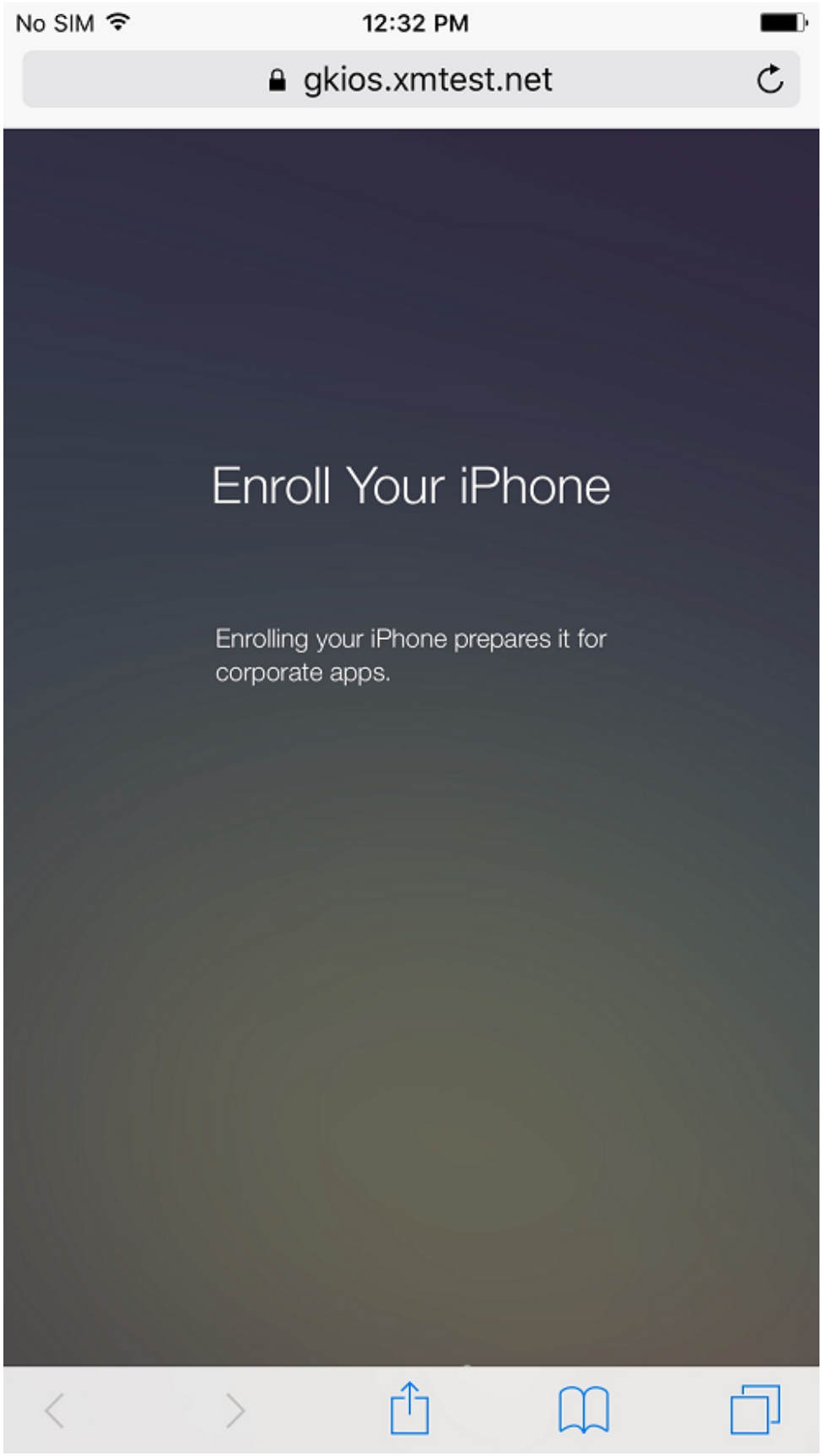


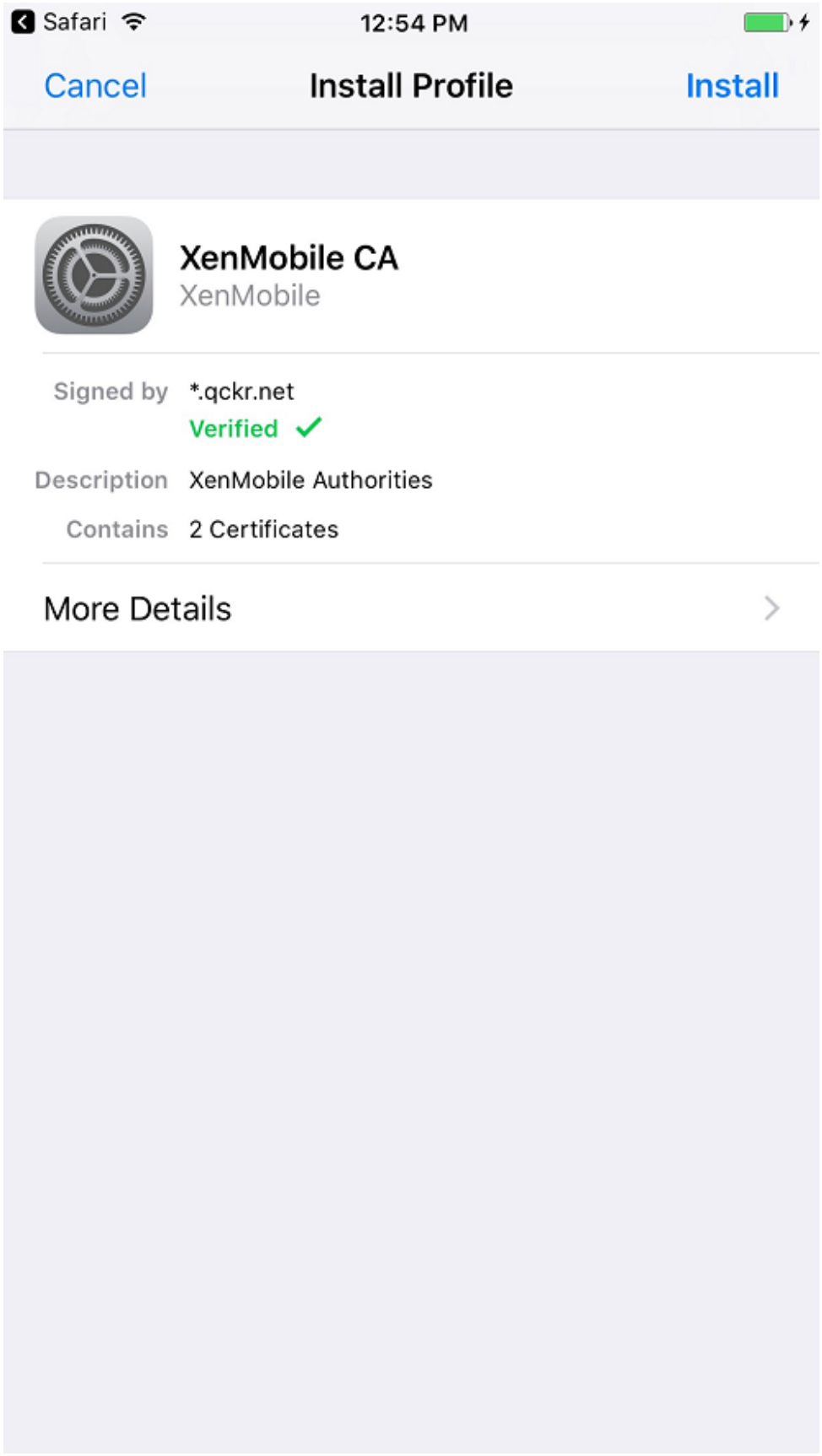
2. Les utilisateurs cliquent sur **Oui, inscrire**.



3. Les utilisateurs se connectent à l'aide de leurs informations d'identification Azure AD.







4. Les utilisateurs effectuent les étapes d'inscription de la même façon que toute autre inscription via Secure Hub.

> **Remarque :**
>
> XenMobile ne prend pas en charge l'authentification par Azure AD pour les invitations d'inscription. Si vous envoyez une invitation d'inscription contenant une adresse URL d'inscription aux utilisateurs, les utilisateurs s'authentifient via LDAP au lieu d'Azure AD.

Informations d'identification dérivées

January 10, 2022

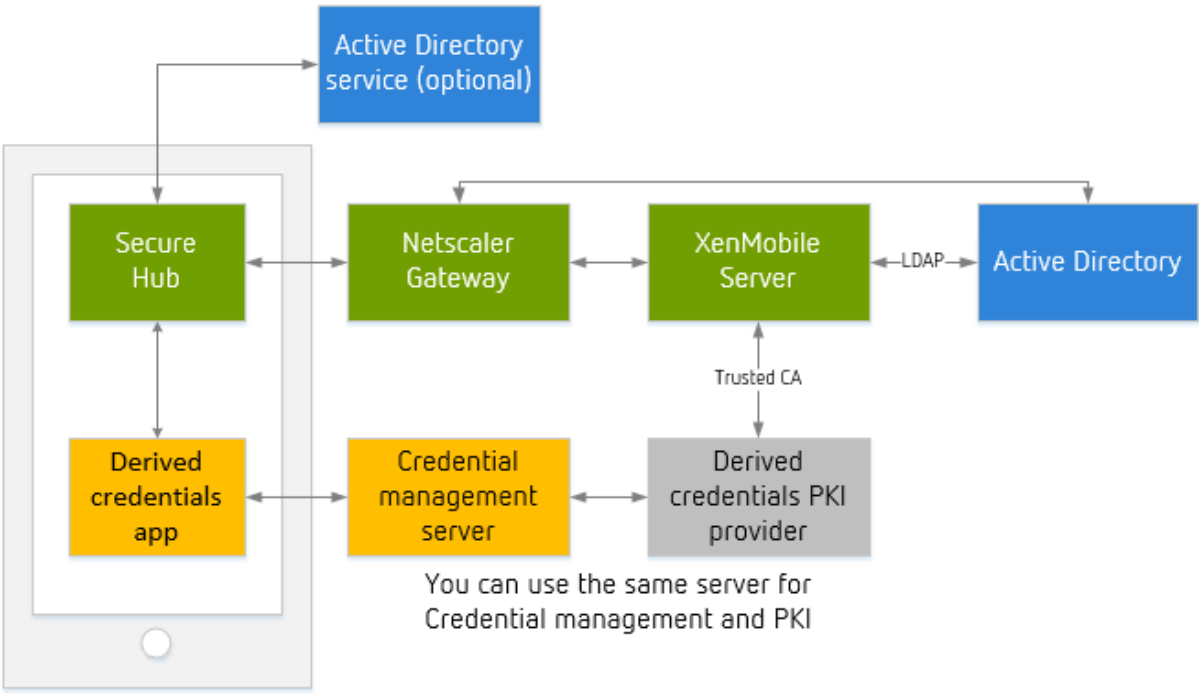
Les informations d'identification dérivées fournissent une authentification forte pour les appareils mobiles. Une carte à puce fournit les informations d'identification, qui résident dans un appareil mobile plutôt que sur la carte. La carte à puce est une carte Personal Identity Verification (PIV).

Les informations d'identification dérivées sont un certificat d'inscription qui contient l'identifiant de l'utilisateur, tel qu'un UPN (nom d'utilisateur principal). XenMobile enregistre les informations d'identification obtenues à partir du fournisseur d'informations d'identification dans un coffre sécurisé sur l'appareil.

XenMobile peut utiliser les informations d'identification dérivées pour l'inscription et l'authentification d'appareils. S'il est configuré pour des informations d'identification dérivées, XenMobile ne prend pas en charge les invitations d'inscription ou les autres modes d'inscription sécurisée. Citrix prend en charge l'utilisation d'une application d'informations d'identification dérivées lors de l'inscription d'iOS.

Architecture

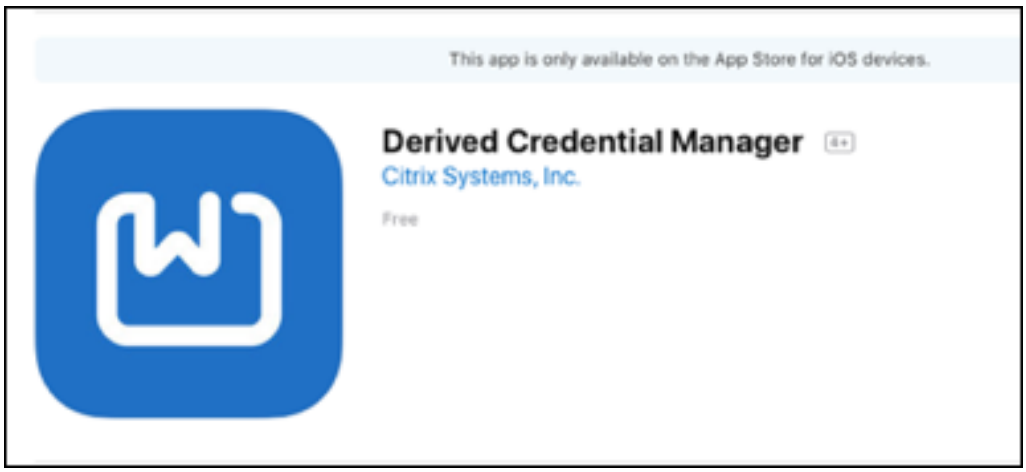
Pour l'inscription, XenMobile Server se connecte aux composants, comme illustré dans le diagramme suivant.



- Lors de l'inscription d'appareil, Secure Hub obtient les certificats à partir de l'application des informations d'identification dérivées.
- L'application des informations d'identification dérivées communique avec le serveur de gestion d'informations d'identification lors de l'inscription.
- Vous pouvez utiliser le même serveur ou un autre serveur comme serveur de gestion d'informations d'identification et un fournisseur PKI tiers.
- XenMobile Server se connecte à votre serveur PKI tiers pour obtenir les certificats.

Exigences

- Téléchargez et installez Citrix Secure Hub.
- En fonction de votre solution d'identifications dérivées, téléchargez et configurez l'application :
  - **Pour Entrust Datacard :**
    * Téléchargez et installez l'application Citrix Derived Credential Manager sur vos appareils *avant* de vous inscrire à XenMobile. Derived Credentials Manager est l'application de fournisseur d'identités de Citrix. Le logo de cette application est affiché ci-dessous.



  * L'application Citrix Derived Credential Manager prend en charge les nouvelles inscriptions uniquement. Les utilisateurs d'appareil doivent se réinscrire.
    · XenMobile Server version 10.8 ou ultérieure.
    · Nécessite l'inscription d'appareil dans MDM+MAM.
- **Autres fournisseurs d'informations d'identification dérivées :** S'il est probable que la plupart des autres solutions d'informations d'identification soient compatibles avec XenMobile, testez leur intégration avant de les déployer en production.

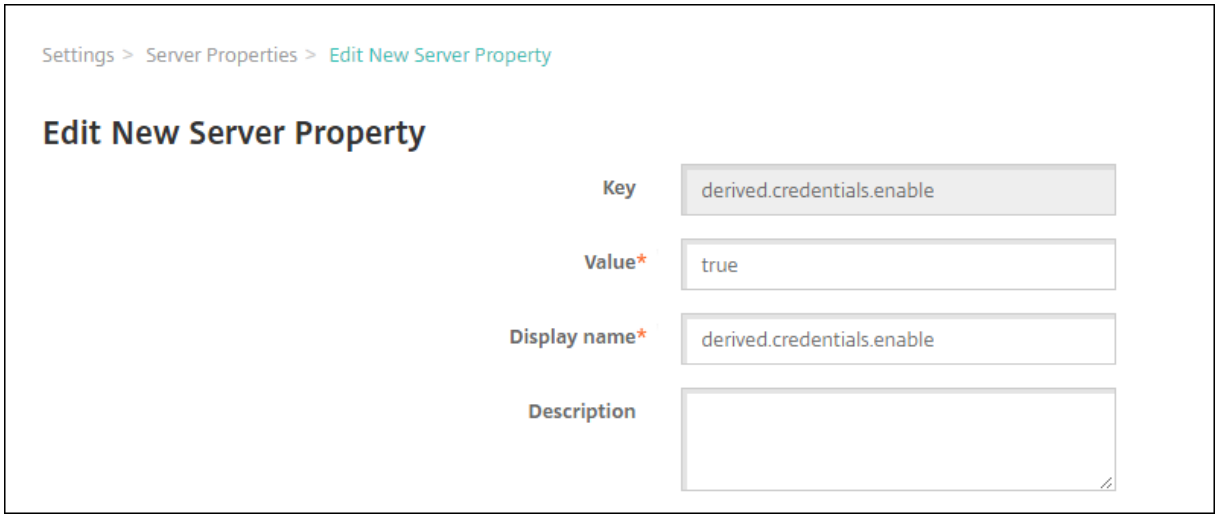
- Doit avoir le certificat racine de l'autorité de certification qui émet des certificats sur le serveur du fournisseur d'informations d'identification. Cette configuration permet à XenMobile d'accepter les certificats signés numériquement lors de l'inscription. Pour de plus amples informations sur l'ajout de certificats, consultez la section Certificats et authentification.
  - Si le domaine de messagerie utilisateur diffère du domaine LDAP, ajoutez le domaine de messagerie dans le paramètre **Alias de domaine** sous **Paramètres > LDAP**. Par exemple, si le domaine pour les adresses e-mail est `citrix.com` et le nom de domaine LDAP est `sample.com`, définissez **Alias de domaine** sur **`sample.com, citrix.com`**.
  - XenMobile ne prend pas en charge l'utilisation d'informations d'identification dérivées avec les appareils partagés.
- Certificats d'identité utilisateur :
  - Le nom d'utilisateur dans le champ Autre nom de l'objet doit être formaté en tant que champ otherName, rfc822Name ou dNSName de l'extension SubjectAltName. Les autres champs ne sont pas pris en charge. Pour plus d'informations sur Autre nom de l'objet, veuillez consulter le RFC, https://www.ietf.org/rfc/rfc5280.txt.
  - L'identité utilisateur dans le champ Objet pour E-mail ou CN n'est pas prise en charge.
- Citrix Gateway configuré pour l'authentification par certificat ou l'authentification par certificat + jeton de sécurité

Activer les informations d'identification dérivées

Par défaut, la console XenMobile n'inclut pas la page **Paramètres > Informations d'identification dérivées**.

Pour activer l'interface pour les informations d'identification dérivées :

- Accédez à **Paramètres > Propriétés du serveur**, ajoutez **derived.credentials.enable** comme propriété de serveur et définissez la valeur de la propriété sur **true**.

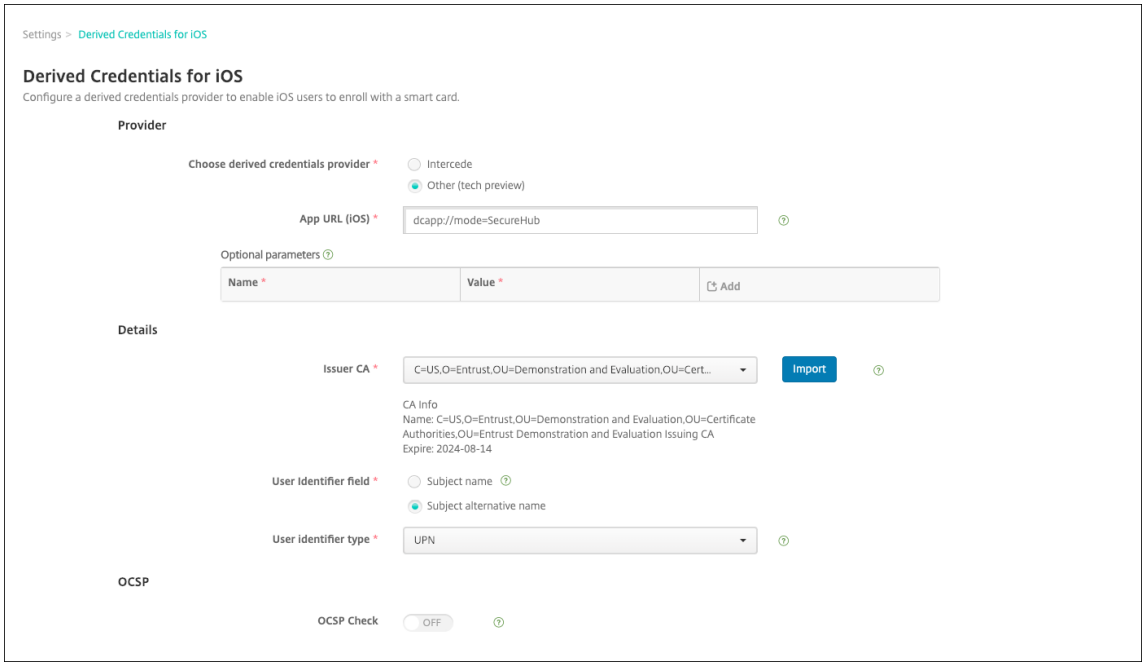


Configurer les informations d'identification dérivées

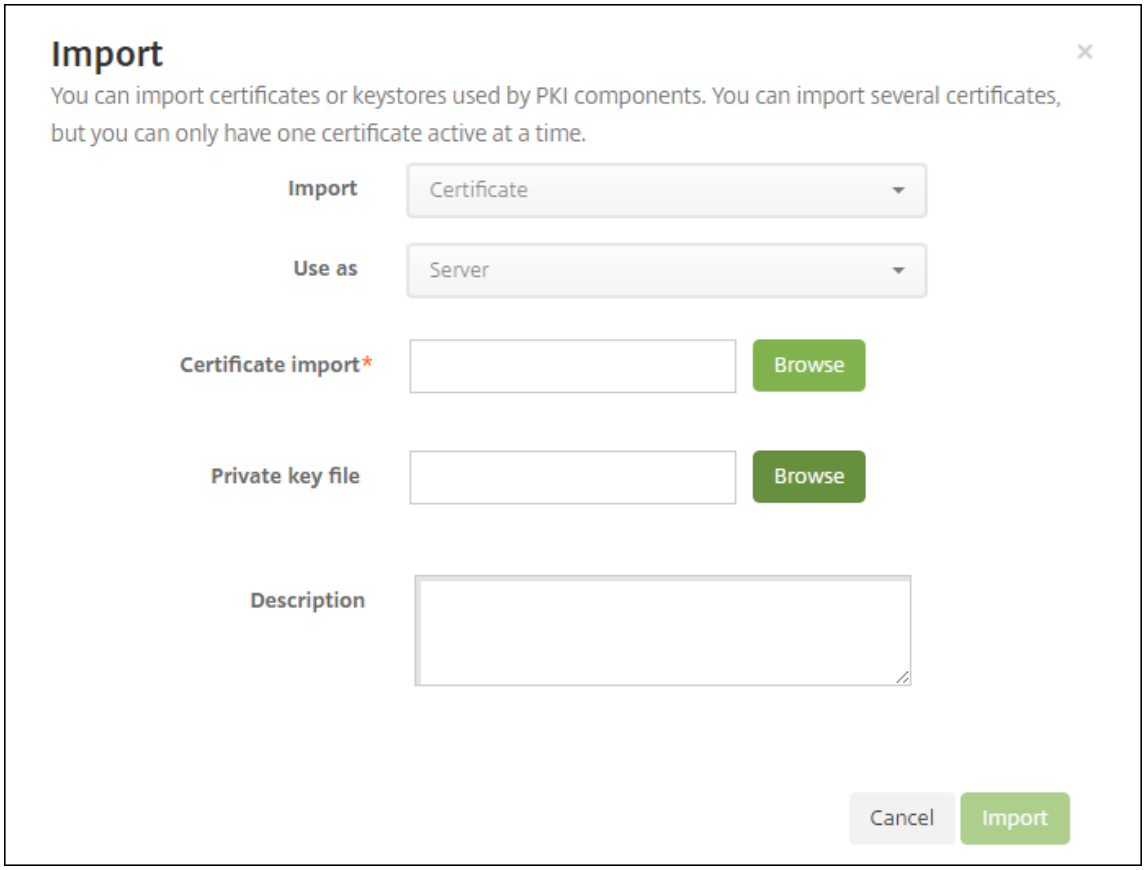
Nous supposons que vous disposez d'une configuration qui fonctionne pour le fournisseur d'informations d'identification dérivées que vous prévoyez d'intégrer à XenMobile. Vous pouvez configurer XenMobile pour communiquer avec ce serveur. Vous pouvez également choisir un certificat d'autorité de certification d'informations d'identification dérivées déjà ajouté à XenMobile ou importer le certificat.

Vous pouvez activer la prise en charge du protocole OCSP pour ce certificat d'autorité de certification. Pour plus d'informations sur le protocole OCSP, consultez la section « Autorités de certification discrétionnaire » dans Entités PKI.

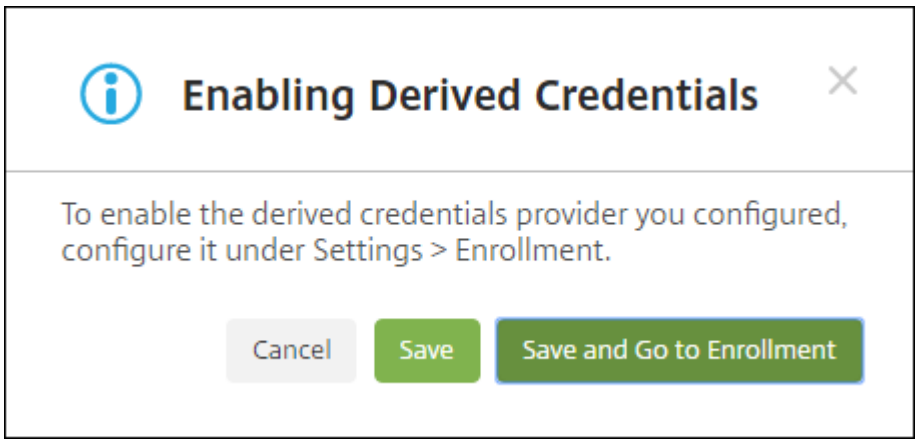
1. Dans la console XenMobile, accédez à **Paramètres > Informations d'identification dérivées pour iOS**.
2. Sous **Choisir un fournisseur d'informations d'identification dérivées**, sélectionnez **Autre** pour Entrust Datacard. Saisissez `dcapp://mode=SecureHub` dans le champ **URL de l'application (iOS)**.



3. **Paramètres facultatifs :** certains fournisseurs d'informations d'identification dérivées exigent que des paramètres soient spécifiés pour la connexion. Par exemple, un fournisseur peut nécessiter que les adresses URL d'un serveur back-end soient spécifiées. Cliquez sur **Ajouter** pour fournir des paramètres.
4. Spécifiez un certificat pour les informations d'identification dérivées : si le certificat est déjà chargé sur XenMobile, choisissez ce certificat depuis **AC émettrice**. Sinon, cliquez sur **Importer** pour ajouter un certificat. La boîte de dialogue **Importer le certificat** apparaît.
5. Dans la boîte de dialogue **Importer le certificat**, cliquez sur **Parcourir** pour accéder à l'emplacement du certificat. Cliquez sur **Parcourir** pour accéder au fichier de clé privée.

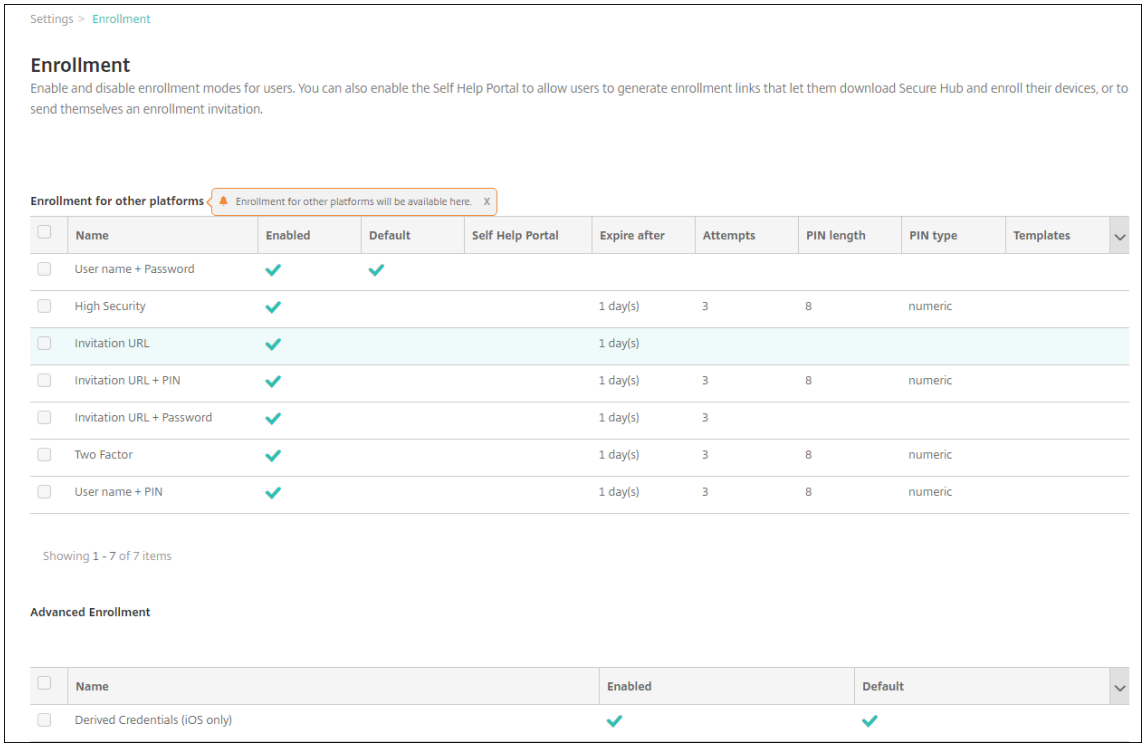


6. Configurez les paramètres.
    - Pour une application Citrix Derived Credential Manager : définissez **Champ d'identificateur d'utilisateur** sur **Autre nom de l'objet** et **Type d'identificateur d'utilisateur** sur **userPrincipalName**.
    - Contactez les autres fournisseurs d'informations d'identification dérivées pour obtenir leurs informations.
7. Vous pouvez également utiliser un répondeur OCSP pour la vérification de révocation de certificat. Citrix recommande d'utiliser un répondeur OCSP pour des raisons de sécurité. Par défaut, la vérification OSP est définie sur **Désactivée**.
    - Si vous activez la prise en charge OCSP pour le certificat d'autorité de certification, sélectionnez une option pour **Utiliser URL OCSP personnalisée**. Par défaut, XenMobile récupère l'adresse URL du protocole OCSP depuis le certificat (l'option **Utiliser définition du certificat pour la révocation**). Pour spécifier une adresse URL de réponse, cliquez sur **Utiliser URL personnalisée** et entrez l'adresse URL.
    - **AC répondeur :** dans **AC répondeur**, choisissez un certificat. Ou, cliquez sur **Importer**, puis utilisez la boîte de dialogue **Importer le certificat** pour localiser le certificat.
8. Cliquez sur **Enregistrer**. La boîte de dialogue **Informations d'identification dérivées** s'affiche.

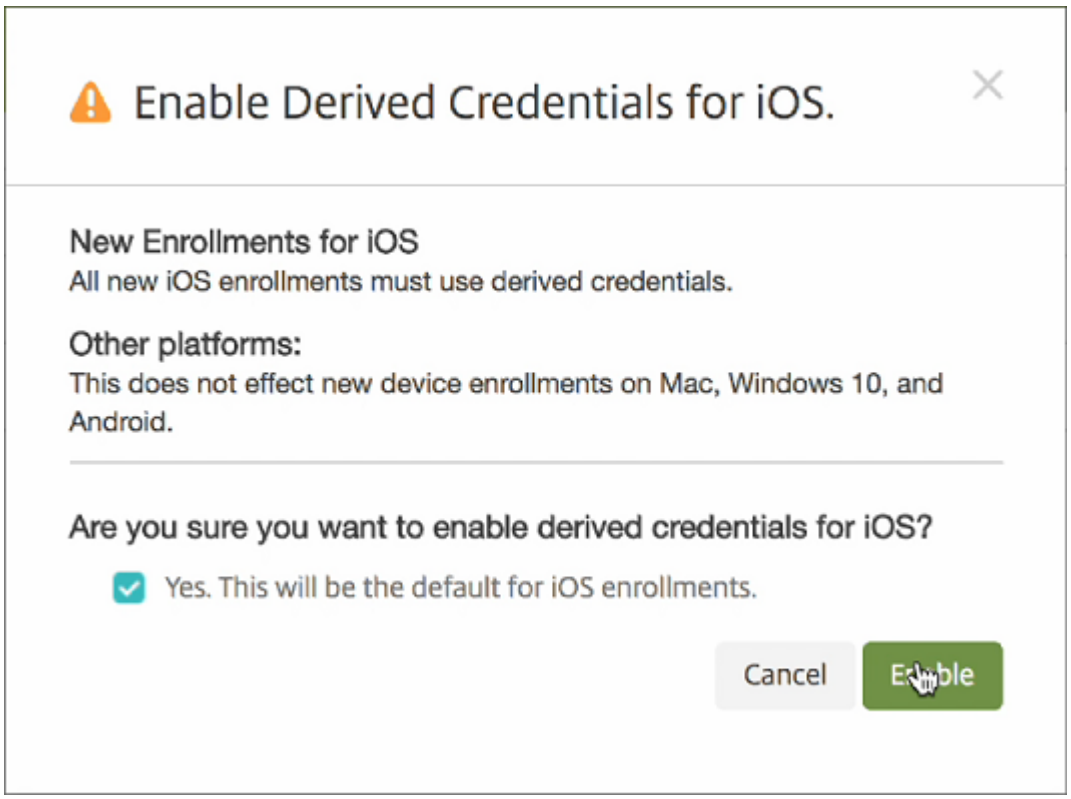


- Pour activer la configuration des informations d'identification dérivées, cliquez sur **Enregistrer**. Pour utiliser les informations d'identification dérivées, vous devez également configurer les paramètres d'inscription.
- Pour activer la configuration des informations d'identification dérivées, puis accéder immédiatement à **Paramètres > Inscription**, cliquez sur **Enregistrer et aller à Inscription**.

9. Pour activer les informations d'identification dérivées pour l'inscription : sur la page **Paramètres > Inscription** sous **Inscription avancée**, sélectionnez **Informations d'identification dérivées (iOS uniquement)**, puis cliquez sur **Activer**.



10. Une boîte de dialogue de confirmation s'affiche. Pour activer les informations d'identification dérivées, sélectionnez la case à cocher et cliquez sur **Activer**.



11. Pour modifier les options des informations d'identification dérivées pour l'inscription, accédez à la page **Paramètres > Inscription**, sélectionnez **Informations d'identification dérivées (iOS uniquement)**, puis cliquez sur **Modifier**.

Après avoir activé les informations d'identification dérivées : dans le rapport **Inscription d'appareils**, la colonne **Mode d'inscription** affiche **derived_credentials**.

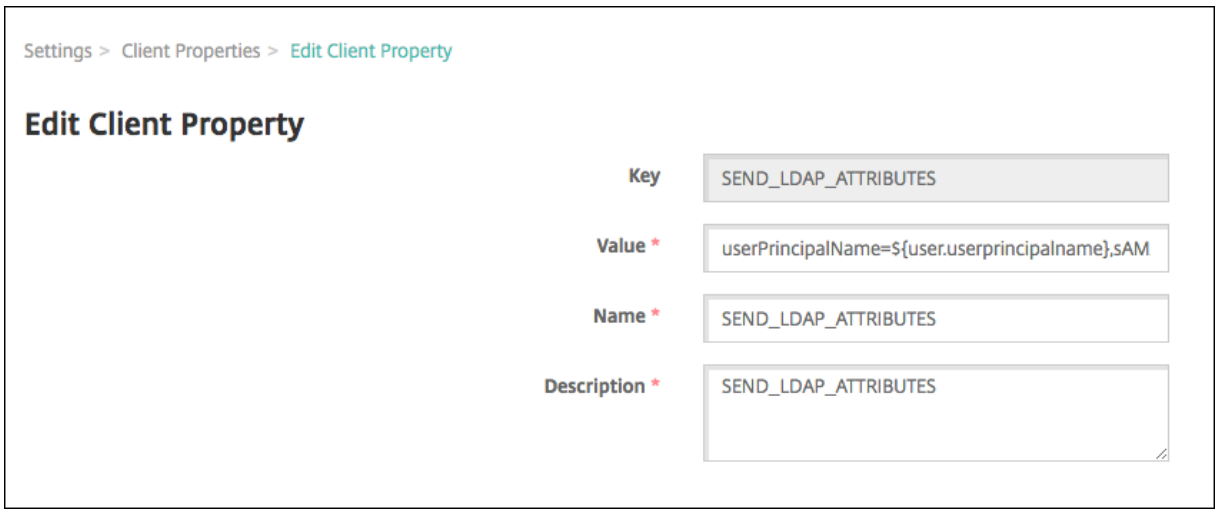
> **Important :**
>
> Après avoir ajouté le fournisseur d'informations d'identification dérivées, redémarrez XenMobile Server.

Configurer XenMobile Server pour Secure Mail

Pour permettre à Secure Mail de fonctionner avec des informations d'identification dérivées, ajoutez la propriété client `SEND_LDAP_ATTRIBUTES`. Pour plus d'informations sur l'ajout d'une propriété de client, voir Propriétés du client.

Utilisez les informations suivantes pour la propriété de client :

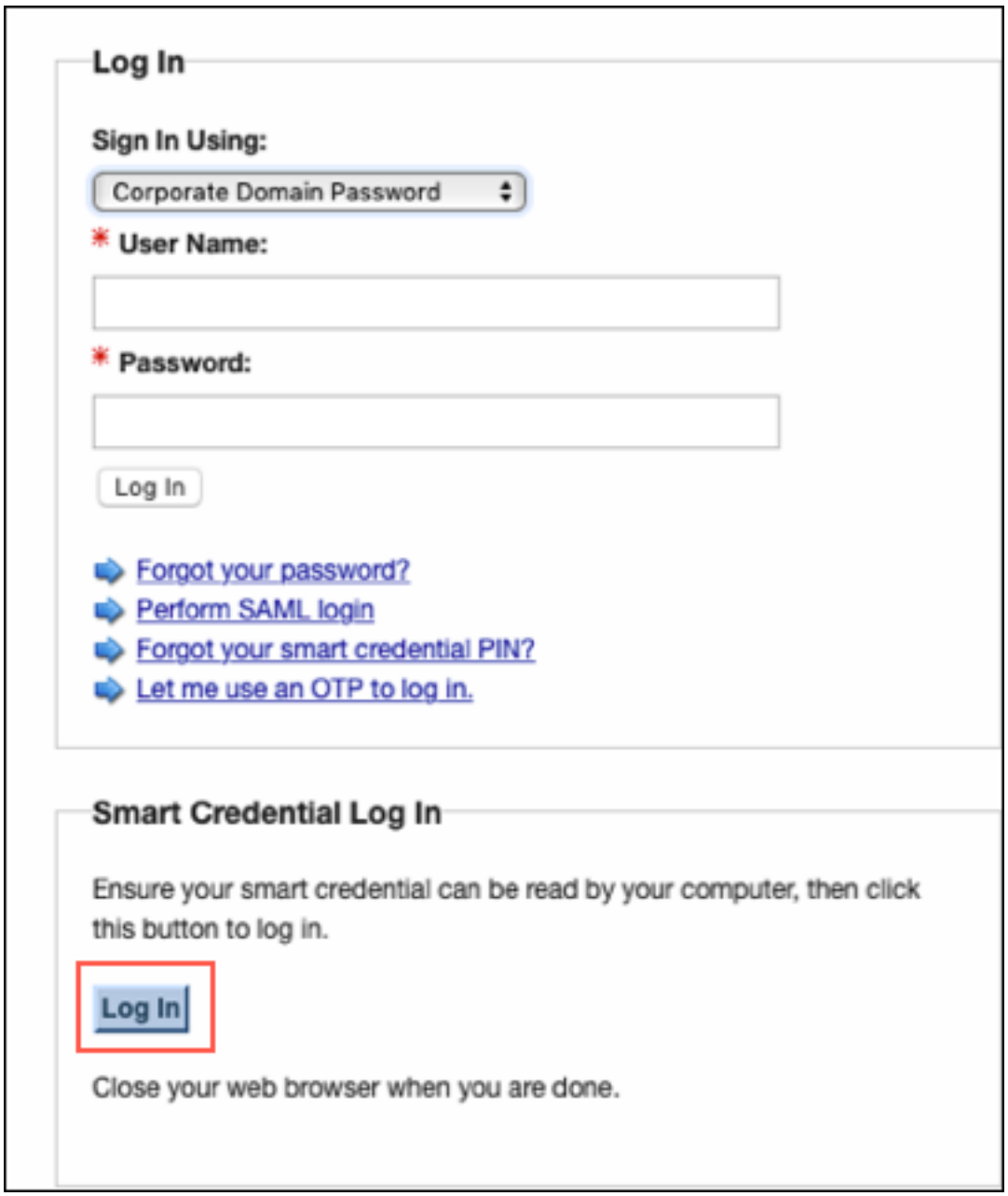
- **Key :** `SEND_LDAP_ATTRIBUTES`
- **Valeur :** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`



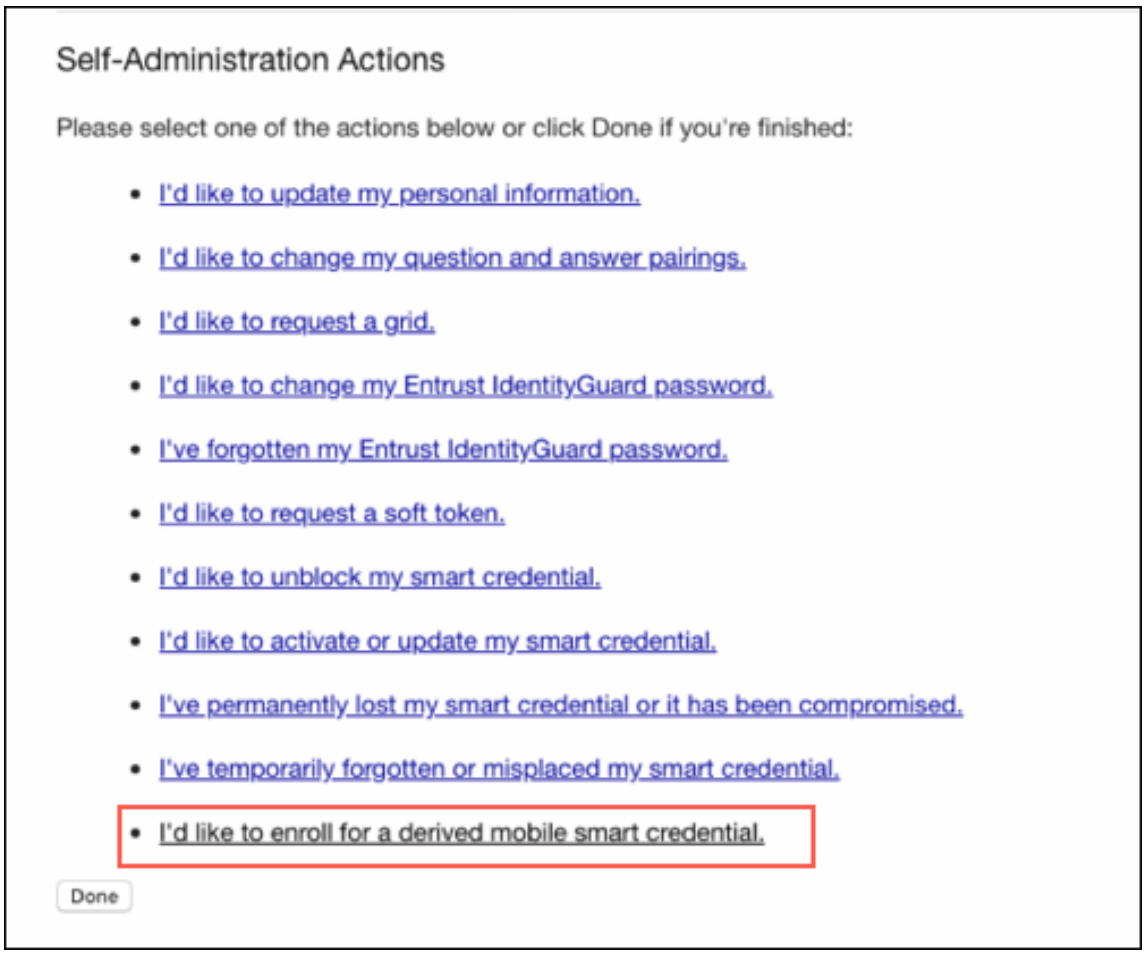
Activation des informations d'identification dérivées d'Entrust Datacard sur les appareils iOS

> **Remarque :**
>
> lors de l'utilisation du site Web Entrust, effacez le cache du navigateur lors du changement de carte PIV.

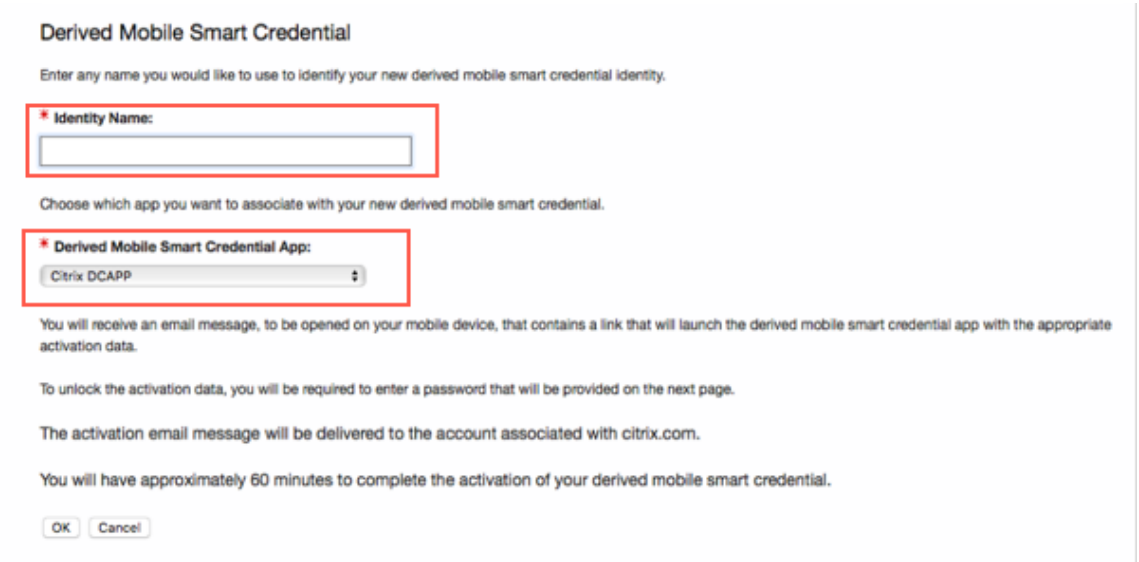
1. Pour demander de nouvelles informations d'identification intelligentes, utilisez un bureau ou un appareil pour vous connecter au site Entrust. Connectez-vous à l'aide du bouton **Smart Credential Log In** au bas de la page. Les utilisateurs insèrent leur carte à puce dans un lecteur relié à leur bureau.



2. Dans **Self-Administration Actions**, sélectionnez **I'd like to enroll for a derived mobile smart credential** et cliquez sur **Done**.



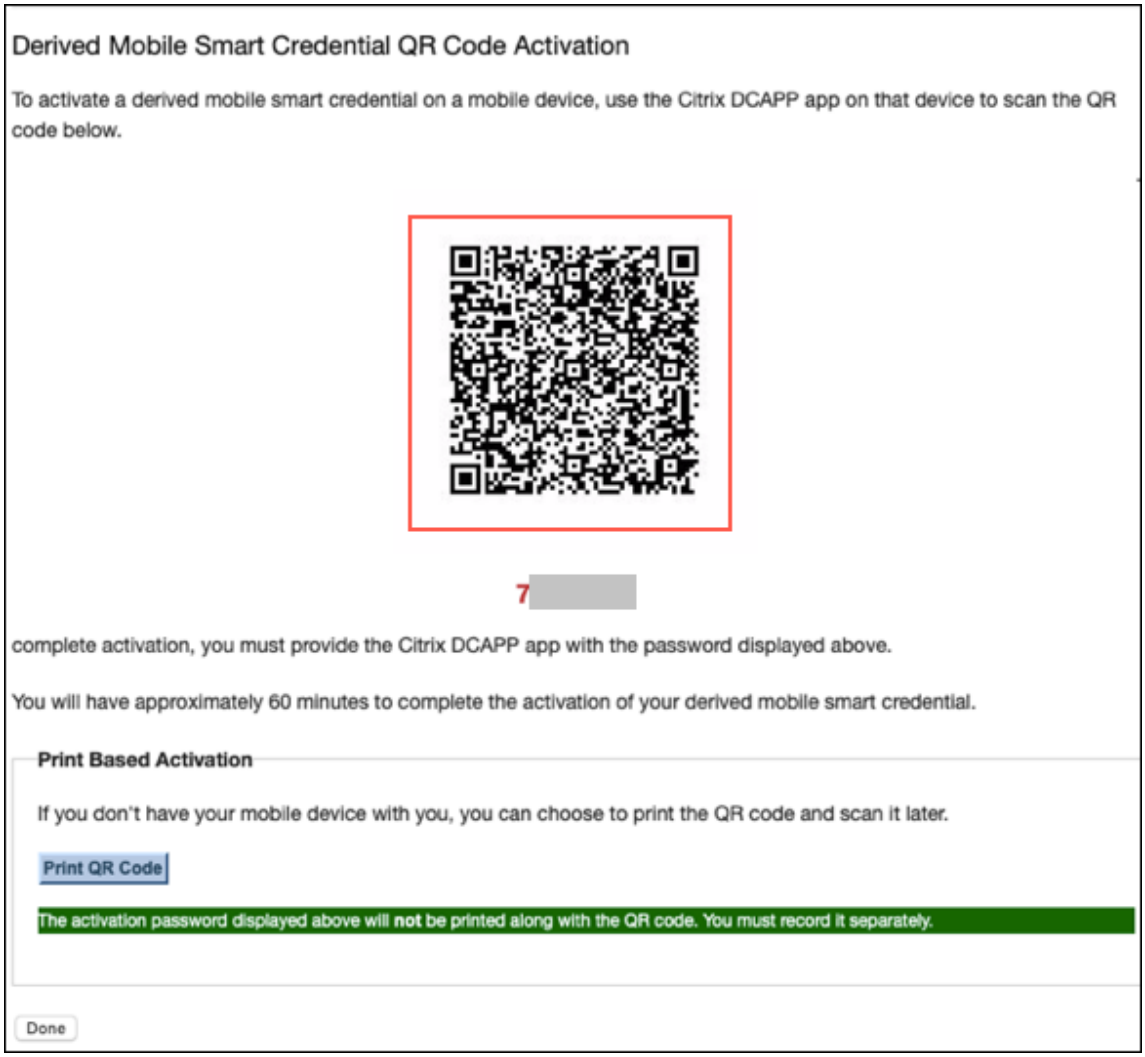
3. Dans l'écran **Derived Mobile Smart Credential**, indiquez le nom d'identité, **Identity Name**. L'utilisateur peut choisir un nom unique tel qu'un nom d'utilisateur ou des numéros d'identification.
4. Sélectionnez **Citrix DCAPP** dans le menu de l'application des informations d'identification dérivées, puis cliquez sur **OK**.



Un écran d'activation de code QR s'affiche et invite l'utilisateur à scanner le code avec son appareil mobile.

> **Remarque :**
>
> Par défaut, le code QR d'informations identification dérivées expire au bout de 3 minutes.

5. Scannez le code QR à l'aide de l'application **Derived Credential Manager** sur l'appareil pour terminer l'activation.

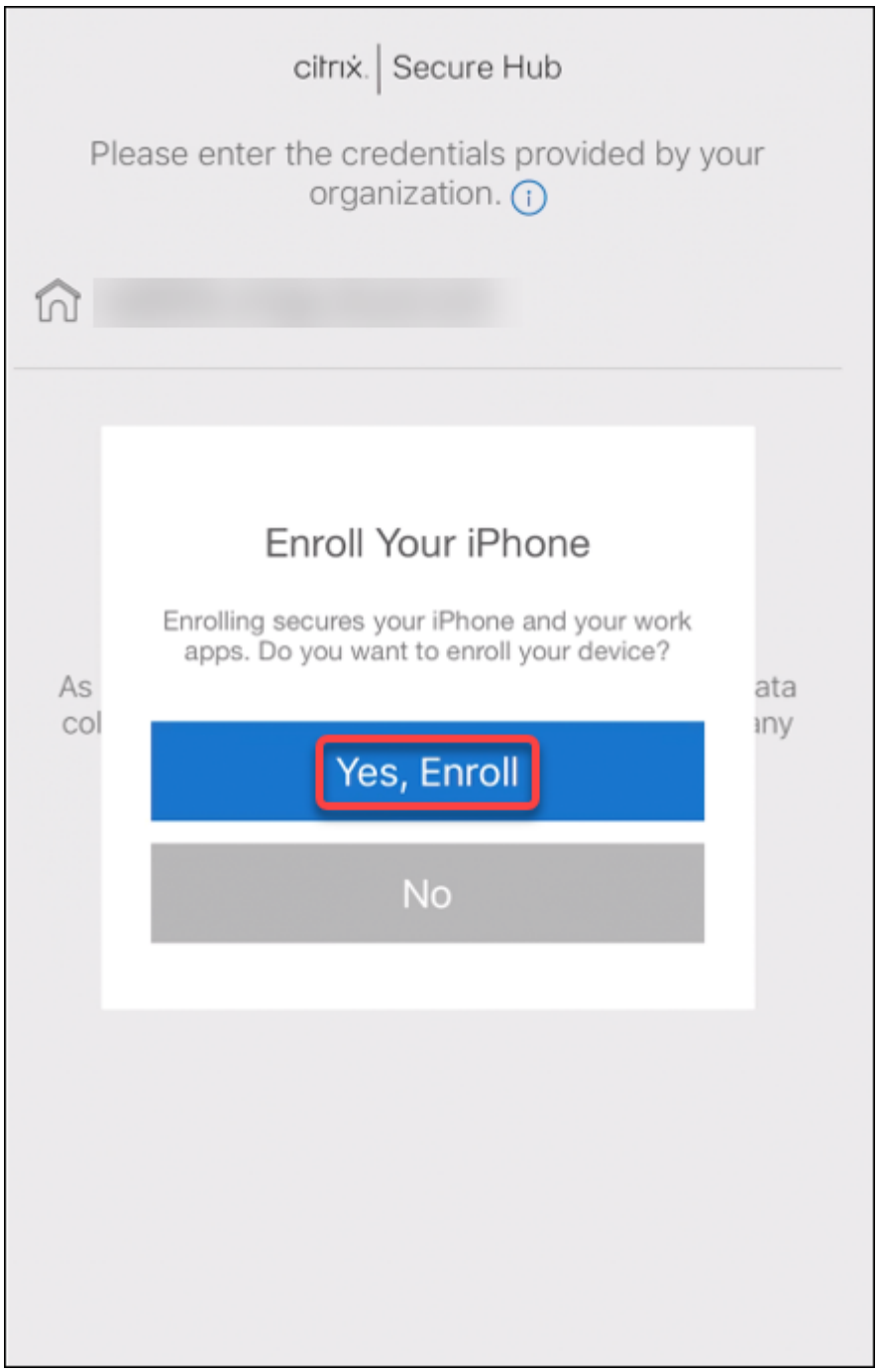


Inscription des appareils

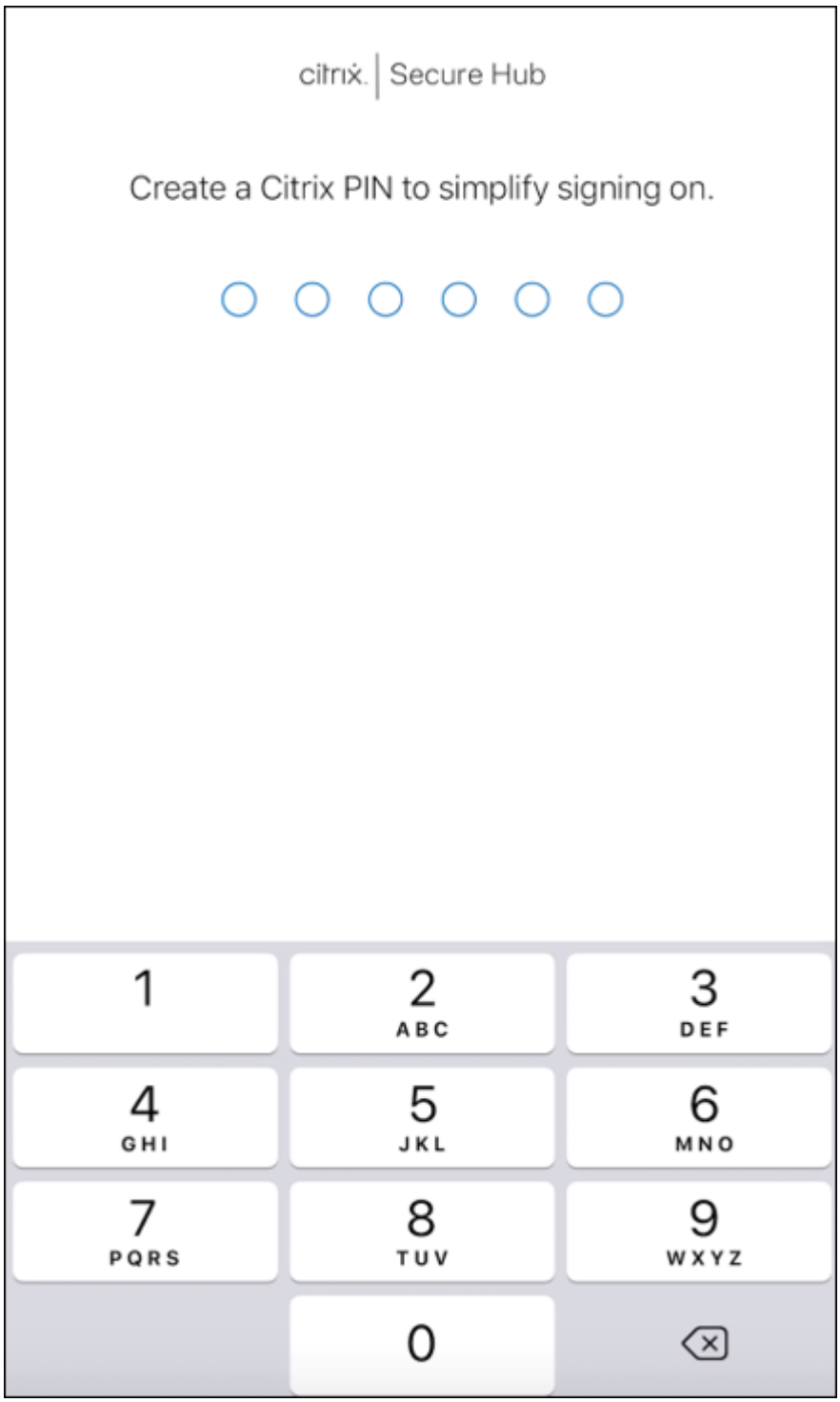
Après avoir terminé la configuration décrite plus haut dans cet article, les utilisateurs peuvent inscrire leurs appareils à l'aide des informations d'identification dérivées.

> **Remarque :**
>
> Les captures d'écran de cette section utilisent Entrust Datacard comme exemple.

1. Touchez pour ouvrir **Secure Hub**. Lorsque vous y êtes invité, saisissez le nom de domaine complet de XenMobile Server, puis cliquez sur **Suivant**.
2. Cliquez sur **Oui, inscrire**. L'inscription de l'appareil dans Secure Hub démarre.

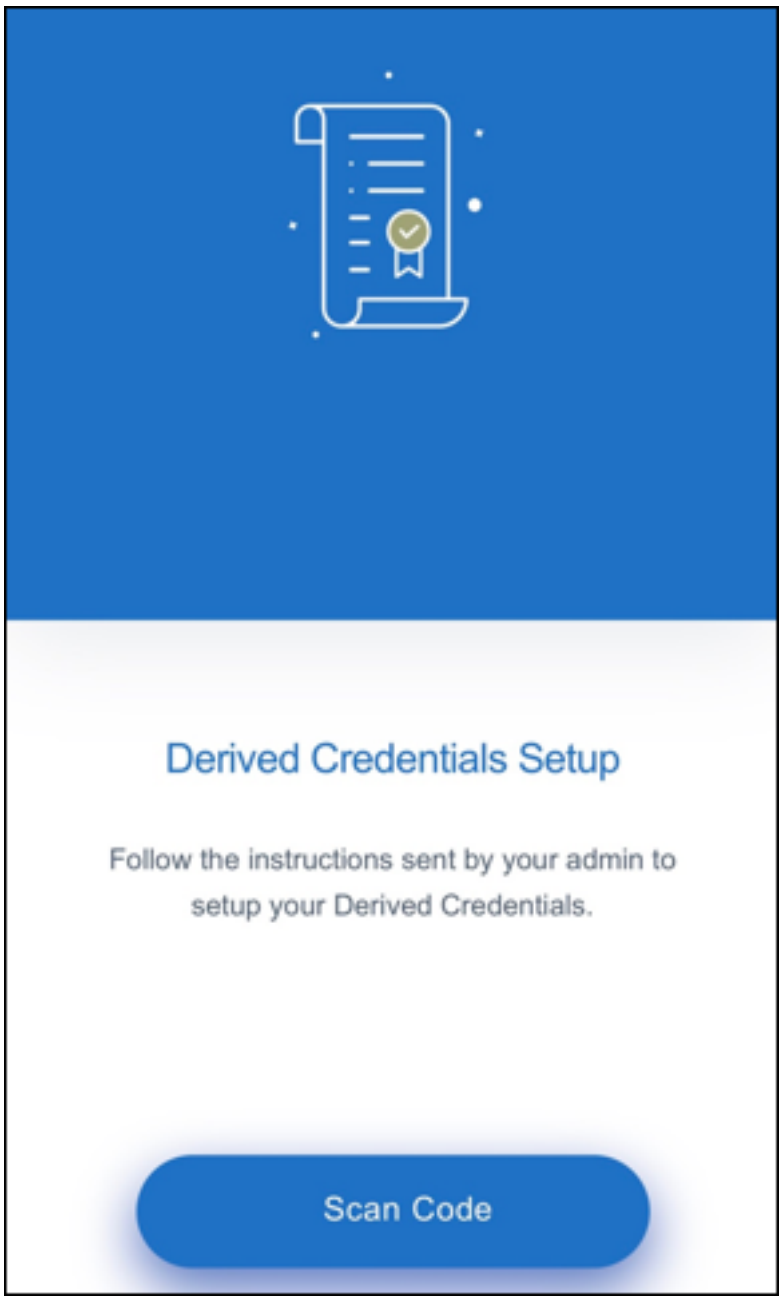


Si XenMobile Server prend en charge les informations d'identification dérivées, Secure Hub invite l'utilisateur à créer et à confirmer un code PIN Citrix.



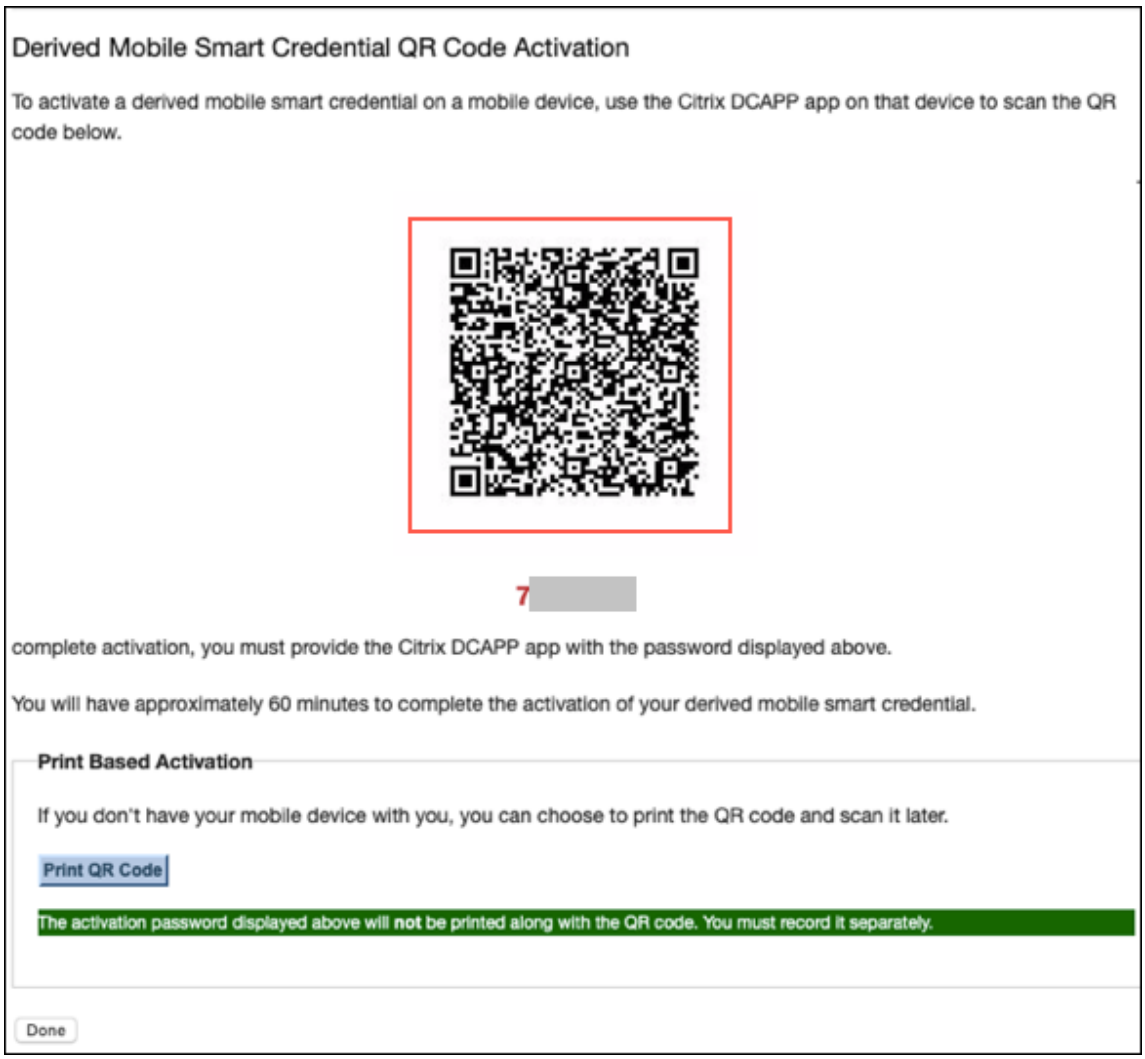
Une fois que vous avez confirmé le code PIN Citrix, l'écran de démarrage d'installation des informations d'identification dérivées s'affiche. Suivez les instructions pour activer les informations d'identification intelligentes.

3. Appuyez sur **Scanner le code**. La caméra du téléphone mobile s'active.

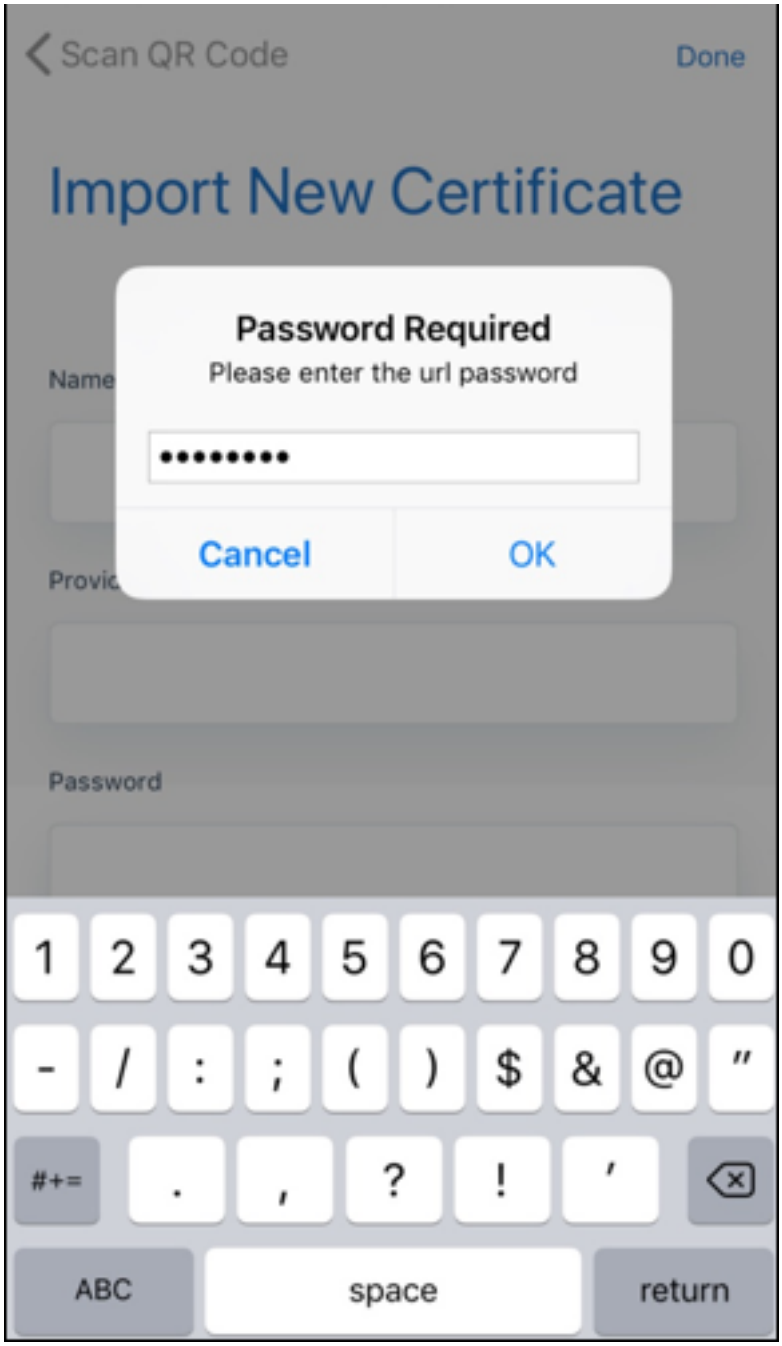


> **Remarque :**
>
> Pour numériser le code QR, assurez-vous que votre appareil photo et votre microphone sont activés et qu'ils ont les autorisations d'accès requises.

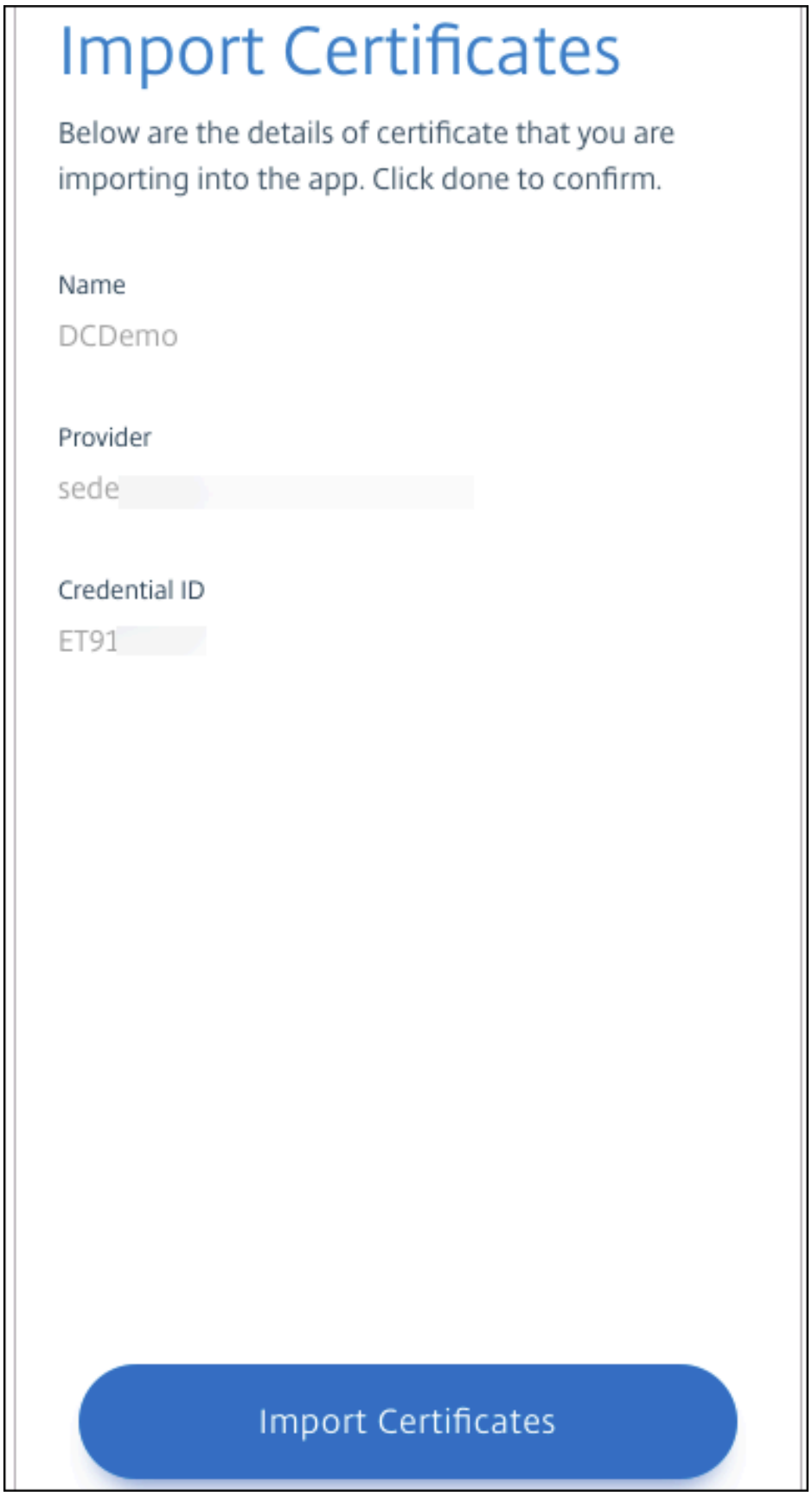
4. Dans l'application d'informations d'identification dérivées, scannez le code QR créé lors des étapes précédentes.



5. Une fois que le code QR a été scanné, dans l'écran **Importer un nouveau certificat**, un mot de passe s'affiche, entrez le mot de passe et cliquez sur **OK**.



L'écran **Importer un nouveau certificat** s'affiche avec les champs remplis automatiquement.



6. Une fois les certificats ajoutés correctement, dans l'écran **Informations d'identification dérivées**, cliquez sur **Continuer vers Secure Hub**.

7. Dans Secure Hub, entrez un nouveau code PIN lorsque vous y êtes invité.

   Après l'authentification du code PIN, Secure Hub télécharge les certificats. Suivez les invites pour terminer l'inscription.

Pour afficher des informations sur l'appareil dans la console XenMobile :

- Accédez à **Gérer** > **Appareils**, puis sélectionnez un appareil pour afficher une zone de commande. Cliquez sur **Afficher plus**.
- Accédez à **Analyser** > **Tableau de bord**.

Mise à niveau

September 22, 2021

> **Conseil : XenMobile Migration Service**
>
> Si vous utilisez une installation locale de XenMobile Server, notre service de migration de XenMobile (XenMobile Migration Service) gratuit peut vous aider à démarrer avec Endpoint Management. La migration de XenMobile Server vers Citrix Endpoint Management ne nécessite pas de réinscrire les appareils.
>
> Pour plus d'informations, contactez votre représentant Citrix, votre ingénieur système ou votre partenaire Citrix local. Ces blogs traitent du service de migration de XenMobile :
>
> Nouveau service de migration de XenMobile
>
> Avantages de XenMobile dans le Cloud

Avant de mettre à niveau vers XenMobile 10.14

1. Mettez à jour votre serveur de licences Citrix vers la version 11.16 ou version ultérieure avant la mise à jour vers la dernière version de XenMobile Server 10.14.

   La dernière version de XenMobile requiert le serveur de licences Citrix 11.16 (version minimale).

   La date Customer Success Services (anciennement la date Subscription Advantage) dans XenMobile 10.14 est le 15 septembre 2021. La date Customer Success Services sur votre licence Citrix doit être postérieure à cette date. Vous pouvez visualiser la date en regard de la licence dans le serveur de licences. Si vous connectez la dernière version de XenMobile à un environnement de serveur de licences plus ancien, la vérification de la connectivité échoue et vous ne pouvez pas configurer le serveur de licences.

   Pour renouveler la date sur votre licence, téléchargez le dernier fichier de licence à partir du portail Citrix, puis téléchargez-le sur le serveur de licences. Pour plus d'informations, consultez

Customer Success Services.

2. Pour un environnement en cluster, la configuration requise pour les déploiements de stratégies et d'applications iOS sur des appareils exécutant iOS 11 ou version ultérieure est la suivante. Si Citrix Gateway est configuré pour la persistance SSL, vous devez ouvrir le port 80 sur tous les nœuds de XenMobile Server.
3. Si la machine virtuelle exécutant XenMobile Server à mettre à niveau dispose de moins de 8 Go de RAM, nous vous recommandons d'augmenter la mémoire vive à 8 Go au minimum.
4. Avant d'installer une mise à jour XenMobile, utilisez les fonctions de votre machine virtuelle pour prendre un instantané de votre système. Sauvegardez aussi la base de données de configuration de votre système. Si vous rencontrez des problèmes durant une mise à niveau, des copies de sauvegarde complètes vous permettent de récupérer.

Pour effectuer la mise à niveau

Vous pouvez effectuer une mise à niveau directement vers XenMobile 10.14 depuis XenMobile 10.13.x ou 10.12.x. Pour effectuer la mise à niveau, téléchargez le dernier fichier binaire disponible en accédant à https://www.citrix.com/downloads. Accédez à **Citrix Endpoint Management (XenMobile) > XenMobile Server > Produit logiciel > XenMobile Server 10**. Sur la vignette du logiciel XenMobile Server de votre hyperviseur, cliquez sur **Télécharger le fichier**. Pour télécharger la mise à niveau, utilisez la page **Gestion des versions** dans la console XenMobile.

Pour mettre à niveau depuis la page Gestion des versions

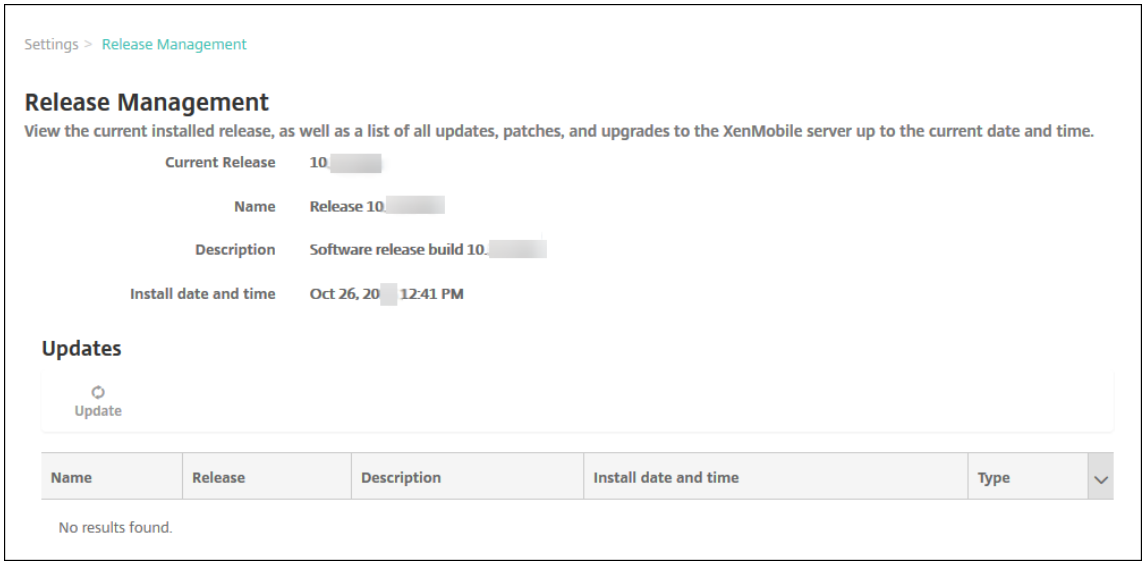
Utilisez la page **Gestion des versions** pour mettre à niveau vers la dernière version de XenMobile Server.

Pré-requis :

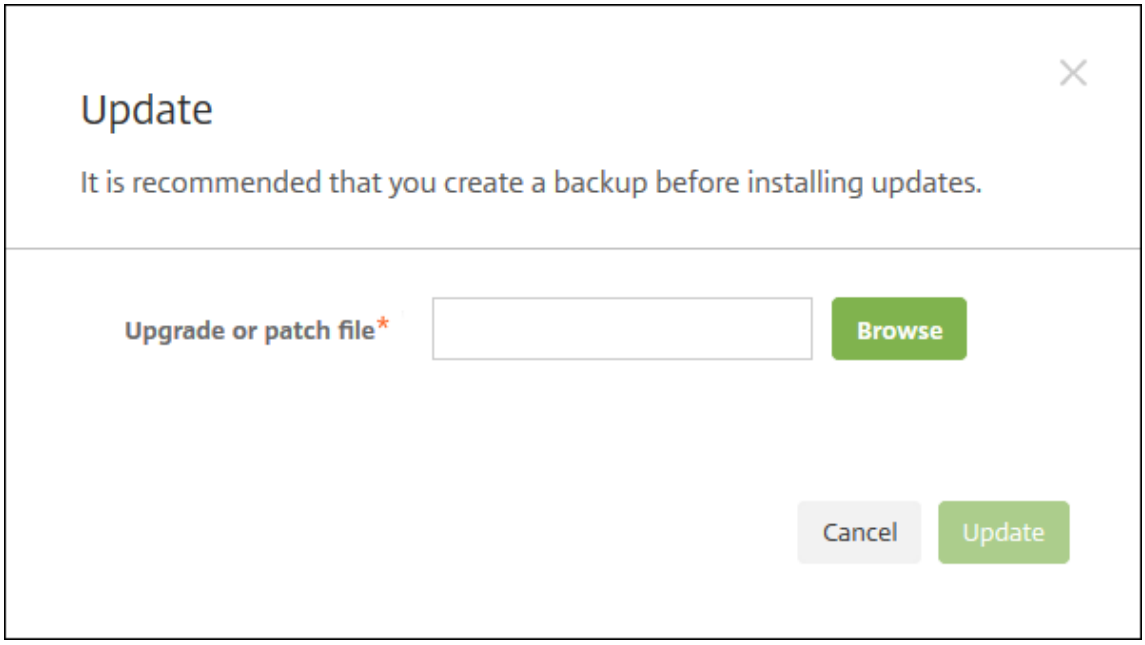
- Vérifiez la configuration système requise.

Si vous disposez d'un déploiement en cluster, reportez-vous aux instructions à la fin de cet article.

1. Téléchargez le dernier fichier binaire disponible en accédant à https://www.citrix.com/downloads. Accédez à **Citrix Endpoint Management (et Citrix XenMobile Server) > XenMobile Server (local) > Logiciel produit > XenMobile Server 10**. Sur la vignette du logiciel XenMobile Server de votre hyperviseur, cliquez sur **Télécharger le fichier**.
2. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
3. Cliquez sur **Gestion des versions**. La page **Gestion des versions** s'affiche.



4. Sous **Mises à jour**, cliquez sur **Mettre à jour**. La boîte de dialogue **Mettre à jour** s'affiche.



5. Sélectionnez le fichier de mise à niveau de XenMobile que vous avez téléchargé à partir de Citrix.com en cliquant sur **Parcourir** pour accéder à l'emplacement du fichier.
6. Cliquez sur **Mettre à jour**, et si vous y êtes invité, redémarrez XenMobile.

   Si pour une raison quelconque la mise à jour ne peut pas être effectuée, un message d'erreur s'affiche indiquant le problème. L'état dans lequel votre système était avant la tentative de mise à jour est restauré.

Après la mise à niveau

Après une mise à niveau, XenMobile nécessite un redémarrage. Utilisez la CLI XenMobile pour redémarrer le serveur XenMobile. Il est important d'effacer le cache de votre navigateur après le redémarrage du système.

Si une fonctionnalité utilisant des connexions sortantes cesse de fonctionner alors que vous n'avez pas changé la configuration de vos connexions, vérifiez dans le journal de XenMobile Server s'il existe des erreurs telle que la suivante : « Impossible de se connecter au serveur VPP : le nom d'hôte 192.0.2.0 ne correspond pas au sujet du certificat fourni par l'homologue. »

L'erreur de validation du certificat indique que vous devez désactiver la vérification de nom d'hôte sur XenMobile Server. Par défaut, la vérification de nom d'hôte est activée sur les connexions sortantes à l'exception du serveur PKI de Microsoft. Si la vérification de nom d'hôte interrompt votre déploiement, définissez la propriété de serveur **disable.hostname.verification** sur **true**. La valeur par défaut de cette propriété est **false**.

Citrix publie les nouvelles versions ou les mises à jour importantes de XenMobile sur Citrix.com. Dans ce cas, une notification est envoyée au contact de chaque client.

Pour mettre à niveau des déploiements XenMobile en cluster

> **Important :**
>
> Avant d'installer une mise à jour XenMobile, utilisez les fonctions de votre machine virtuelle (VM) pour prendre un instantané de votre système. Sauvegardez aussi la base de données de configuration de votre système. Si vous rencontrez des problèmes durant une mise à niveau, des copies de sauvegarde complètes vous permettent de récupérer.

Si votre système est configuré en mode cluster, suivez les étapes suivantes pour mettre à jour chaque nœud d'une version de XenMobile 10 :

1. Chargez le fichier .bin sur tous les nœuds depuis **Paramètres > Gestion des versions**.
2. Fermez tous les nœuds depuis le **menu Système** dans l'interface de ligne de commande.
3. Affichez un nœud, depuis le **menu Système** dans l'interface de ligne de commande, et vérifiez que le service est en cours d'exécution.
4. Affichez les autres nœuds les uns après les autres.

   Si XenMobile ne peut pas effectuer la mise à jour, un message d'erreur expliquant le problème s'affiche. XenMobile rétablit alors l'état du système à l'état qui était le sien avant la tentative de mise à jour.

Mise à niveau de XenMobile MDM Edition vers Enterprise Edition

Vous pouvez mettre à niveau XenMobile MDM Edition vers XenMobile Enterprise Edition pour les appareils iOS et Android.

Conditions préalables

- Une licence Enterprise correcte
- L'instance Citrix Gateway configurée

Pour effectuer la mise à niveau

1. Accédez à **Paramètres > Système de licences** et vérifiez que le type de licence Enterprise Edition correct est chargé.
2. Accédez à **Paramètres > Propriétés du serveur** et modifiez la propriété **Mode de serveur** de **MDM** vers **ENT**.
3. Accédez à **Paramètres > Citrix Gateway** et configurez les détails de Citrix Gateway. Définissez le mode d'authentification sur le même mode que MDM Edition, c'est-à-dire l'authentification de domaine (Active Directory). XenMobile ne prend pas en charge la modification du mode d'authentification après l'inscription de l'utilisateur.
4. Facultatif : accédez à **Paramètres > Propriétés du Client** et activez l'authentification par code PIN Citrix.

Après avoir effectué ces étapes, les utilisateurs doivent effectuer les étapes suivantes pour faire basculer un appareil en mode Enterprise.

Utilisateurs iOS

1. Fermer Secure Hub : appuyez deux fois (rapidement) sur le bouton d'accueil de l'appareil et faites glisser l'application Secure Hub vers le haut.
2. Ouvrez Secure Hub.

Utilisateurs Android

1. Ouvrez Secure Hub.
2. Accédez à **Préférences > Informations sur l'appareil**.
3. Cliquez sur **Actualiser la stratégie**.

Si vous avez activé l'authentification par code PIN Citrix, Secure Hub invite les utilisateurs à créer un code PIN. Lorsqu'un utilisateur crée un code PIN, XenMobile configure l'appareil en mode Enterprise. Dans la console XenMobile, la page **Gérer> Appareils** affiche alors MDM et MAM comme actifs pour l'appareil.

Comptes utilisateur, rôles et inscription

September 22, 2021

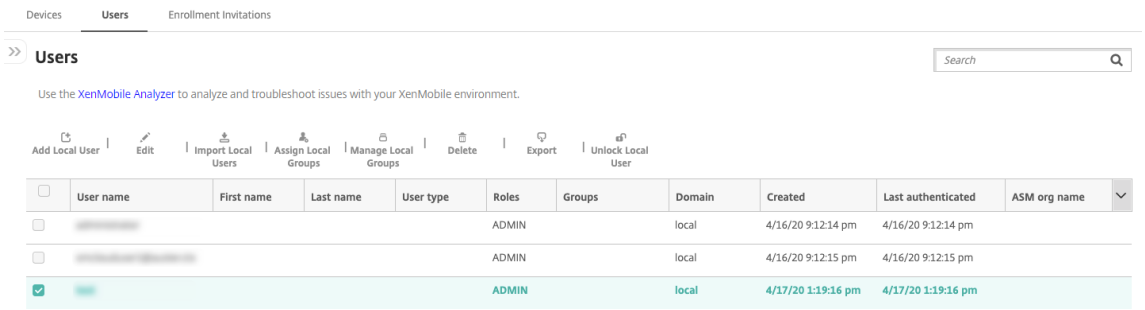
Vous configurez les comptes utilisateur, les rôles et les inscriptions dans la console XenMobile, sur l'onglet **Gérer** et la page **Paramètres**. Sauf indication contraire, les étapes des tâches suivantes sont fournies dans cet article.

- Groupes et comptes utilisateur :
  - Depuis **Gérer > Utilisateurs**, ajoutez des comptes utilisateur manuellement ou utilisez un fichier de provisioning .csv pour importer des comptes et gérer des groupes locaux.
  - Depuis **Paramètres > Workflows**, appliquez des workflows pour gérer la création et la suppression des comptes d'utilisateur.
- Rôles des groupes et comptes utilisateur
  - Depuis **Paramètres > Contrôle d'accès basé sur rôle**, attribuez des rôles prédéfinis ou des ensembles d'autorisations aux utilisateurs et aux groupes. Ces autorisations contrôlent le niveau d'accès des utilisateurs aux fonctions du système. Pour plus d'informations, veuillez consulter la section Configurer des rôles avec RBAC.
  - Depuis **Paramètres > Modèles de notification**, créez ou mettez à jour des modèles de notification dans XenMobile à utiliser dans les actions automatisées, l'inscription, et les messages de notifications standard envoyés aux utilisateurs. Vous configurez les modèles de notification pour l'envoi de messages sur trois canaux différents : Secure Hub, SMTP ou SMS. Pour plus d'informations, consultez la section Créer et mettre à jour des modèles de notification.
- Mode et invitations d'inscription sécurisée
  - Depuis **Paramètres > Inscription**, configurez jusqu'à sept modes d'inscription sécurisée et envoyez des invitations d'inscription. Chaque mode d'inscription sécurisée dispose de son propre niveau de sécurité et d'étapes que les utilisateurs doivent suivre pour inscrire leurs appareils.
  - Activer AutoDiscovery pour l'inscription utilisateur dans XenMobile

Pour ajouter, modifier, verrouiller ou supprimer des comptes utilisateur locaux

Vous pouvez ajouter des comptes d'utilisateur locaux à XenMobile manuellement ou vous pouvez utiliser un fichier de provisioning pour importer les comptes. Pour savoir comment importer des comptes utilisateur à l'aide d'un fichier de provisioning, consultez Importer comptes utilisateur.

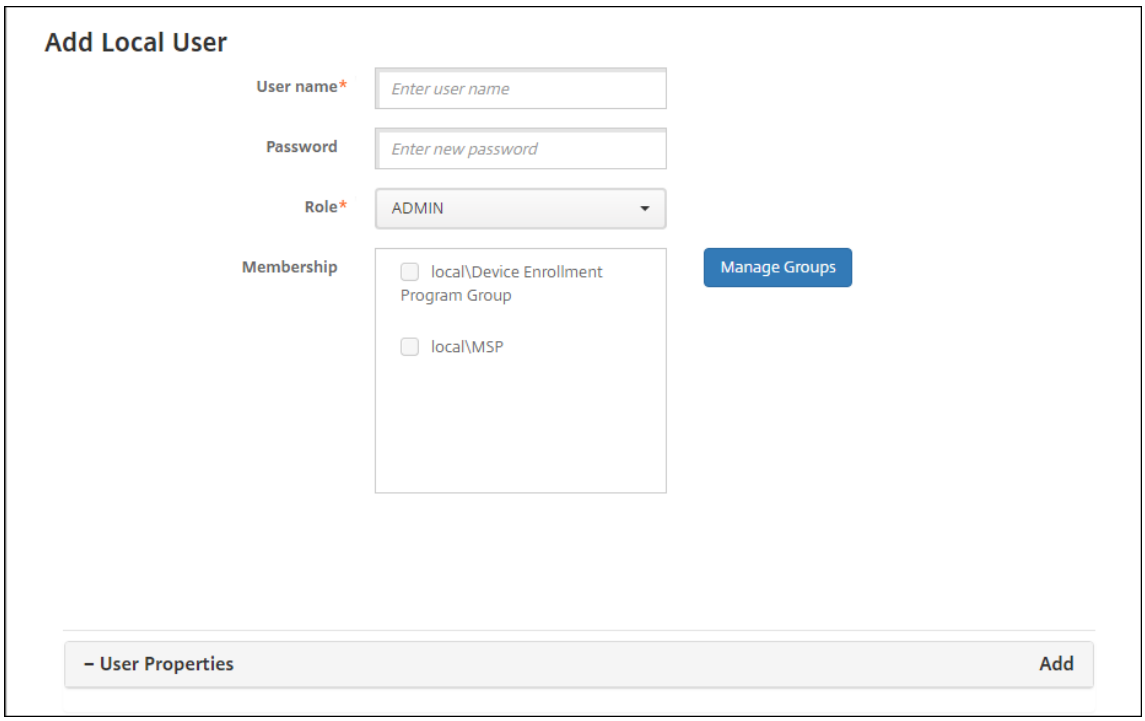
1. Dans la console XenMobile, cliquez sur **Gérer > Utilisateurs**. La page **Utilisateurs** s'affiche.



2. Cliquez sur **Afficher le filtre** pour filtrer la liste.

Pour ajouter un compte d'utilisateur local

1. Sur la page **Utilisateurs**, cliquez sur **Ajouter un utilisateur local**. La page **Ajouter un utilisateur local** s'affiche.



2. Pour configurer ces paramètres :

   - **Nom d'utilisateur :** entrez le nom (champ obligatoire). Le nom peut contenir des espaces ainsi que des majuscules et des minuscules.
   - **Mot de passe :** entrez un mot de passe utilisateur (facultatif). Le mot de passe doit comporter au moins 14 caractères et répondre à tous les critères suivants :
     - Inclure au moins deux chiffres
     - Inclure au moins une lettre majuscule et une lettre minuscule
     - Inclure au moins un caractère spécial

  - N'incluez pas de mots du dictionnaire ou de mots restreints tels que votre nom d'utilisateur ou adresse e-mail Citrix.
  - N'incluez pas plus de trois caractères séquentiels (dans l'alphabet et sur le clavier) et répétitifs, tels que 1111, 1234 ou asdf
- **Rôle :** dans la liste, cliquez sur le rôle utilisateur. Pour plus d'informations concernant les rôles, consultez la section Configurer des rôles avec RBAC. Les options possibles sont les suivantes :
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT
  - USER
- **Adhésion :** dans la liste, cliquez sur le groupe ou les groupes auxquels ajouter l'utilisateur.
- **Propriétés utilisateur :** ajoutez des propriétés utilisateur (facultatif). Pour chaque propriété d'utilisateur que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Propriétés utilisateur :** dans la liste, cliquez sur une propriété, puis entrez l'attribut de la propriété utilisateur dans le champ en regard de la propriété.
  - Cliquez sur **Terminé** pour enregistrer la propriété utilisateur ou cliquez sur **Annuler**.

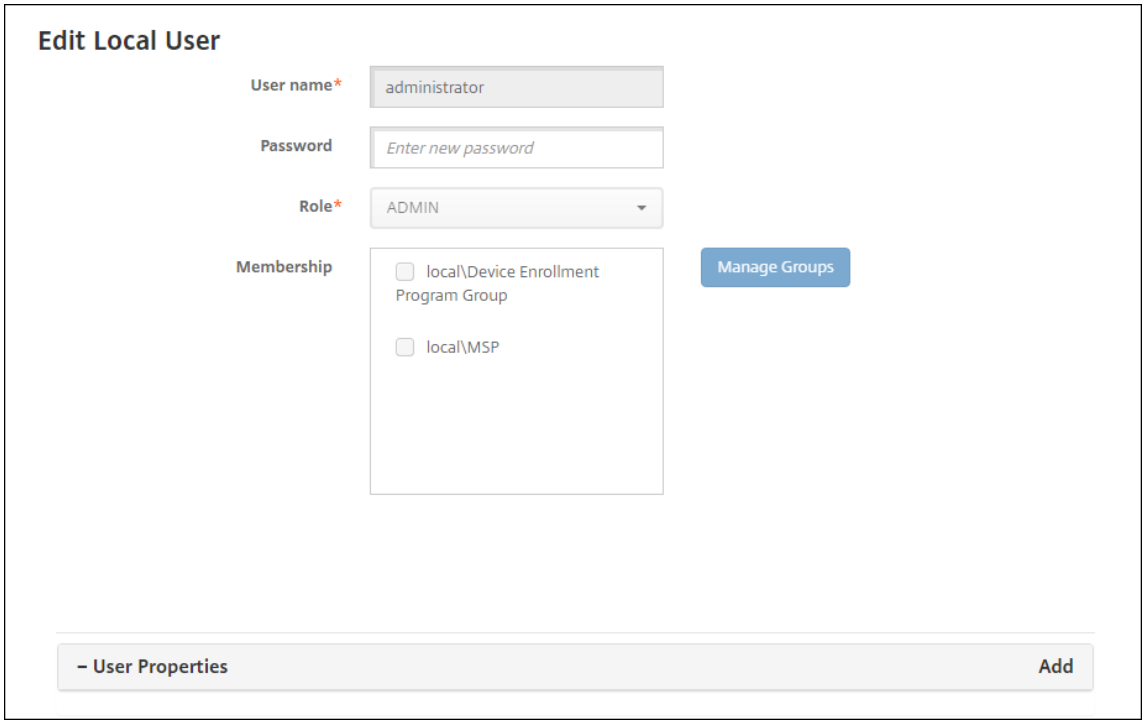
Pour supprimer une propriété utilisateur existante, placez le curseur sur la ligne contenant la propriété et cliquez sur le X sur le côté droit. La propriété est immédiatement supprimée.

Pour modifier une propriété utilisateur, cliquez sur la propriété et effectuez les modifications. Cliquez sur **Terminé** pour enregistrer les modifications ou sur **Annuler** pour laisser la propriété inchangée.

3. Cliquez sur **Enregistrer**.

Pour modifier un compte d'utilisateur local

1. Sur la page **Utilisateurs**, dans la liste des utilisateurs, cliquez pour sélectionner un utilisateur, puis cliquez sur **Modifier**. La page **Modifier un utilisateur local** apparaît.



2. Modifiez les informations suivantes le cas échéant :
   - **Nom d'utilisateur :** vous ne pouvez pas modifier le nom d'utilisateur.
   - **Mot de passe :** modifiez ou ajoutez un mot de passe utilisateur.
   - **Rôle :** dans la liste, cliquez sur le rôle utilisateur.
   - **Adhésion :** dans la liste, cliquez sur le groupe ou les groupes pour lesquels ajouter ou modifier le compte utilisateur. Pour supprimer le compte utilisateur d'un groupe, désactivez la case à cocher en regard du nom du groupe.
   - **Propriétés utilisateur :** effectuez l'une des opérations suivantes :
     - Pour chaque propriété utilisateur que vous voulez modifier, cliquez sur la propriété et effectuez des modifications. Cliquez sur **Terminé** pour enregistrer les modifications ou sur **Annuler** pour laisser la propriété inchangée.
     - Pour chaque propriété d'utilisateur que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
       * **Propriétés utilisateur :** dans la liste, cliquez sur une propriété, puis entrez l'attribut de la propriété utilisateur dans le champ en regard de la propriété.
       * Cliquez sur **Terminé** pour enregistrer la propriété utilisateur ou cliquez sur **Annuler**.
     - Pour chaque propriété utilisateur que vous souhaitez supprimer, placez le curseur sur la ligne contenant la propriété, puis cliquez sur le **X** sur le côté droit. La propriété est immédiatement supprimée.
3. Cliquez sur **Enregistrer** pour enregistrer vos modifications ou sur **Annuler** pour laisser l'utilisateur inchangé.

Pour déverrouiller un compte d'utilisateur local

1. Sur la page **Utilisateurs**, dans la liste des comptes utilisateur, cliquez pour sélectionner un compte utilisateur.
2. Cliquez sur **Déverrouiller utilisateur local**. Une boîte de dialogue de confirmation s'affiche.
3. Cliquez sur **Déverrouiller** pour déverrouiller le compte utilisateur ou cliquez sur **Annuler** pour laisser l'utilisateur inchangé.

Pour supprimer un compte d'utilisateur local

1. Sur la page **Utilisateurs**, dans la liste des comptes utilisateur, cliquez pour sélectionner un compte utilisateur.

Vous pouvez sélectionner plusieurs comptes utilisateur à supprimer en sélectionnant la case à cocher en regard de chaque compte utilisateur.

1. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche.
2. Cliquez sur **Supprimer** pour supprimer le compte utilisateur ou cliquez sur **Annuler**.

Pour supprimer des utilisateurs Active Directory

Pour supprimer un ou plusieurs utilisateurs Active Directory à la fois, sélectionnez les utilisateurs et cliquez sur **Supprimer**.

Si un utilisateur que vous supprimez dispose d'appareils inscrits et que vous souhaitez ré-inscrire ces appareils, supprimez les appareils avant la réinscription. Pour supprimer un appareil, accédez à **Gérer > Appareils**, sélectionnez l'appareil et cliquez sur **Supprimer**.

Importer des comptes utilisateur

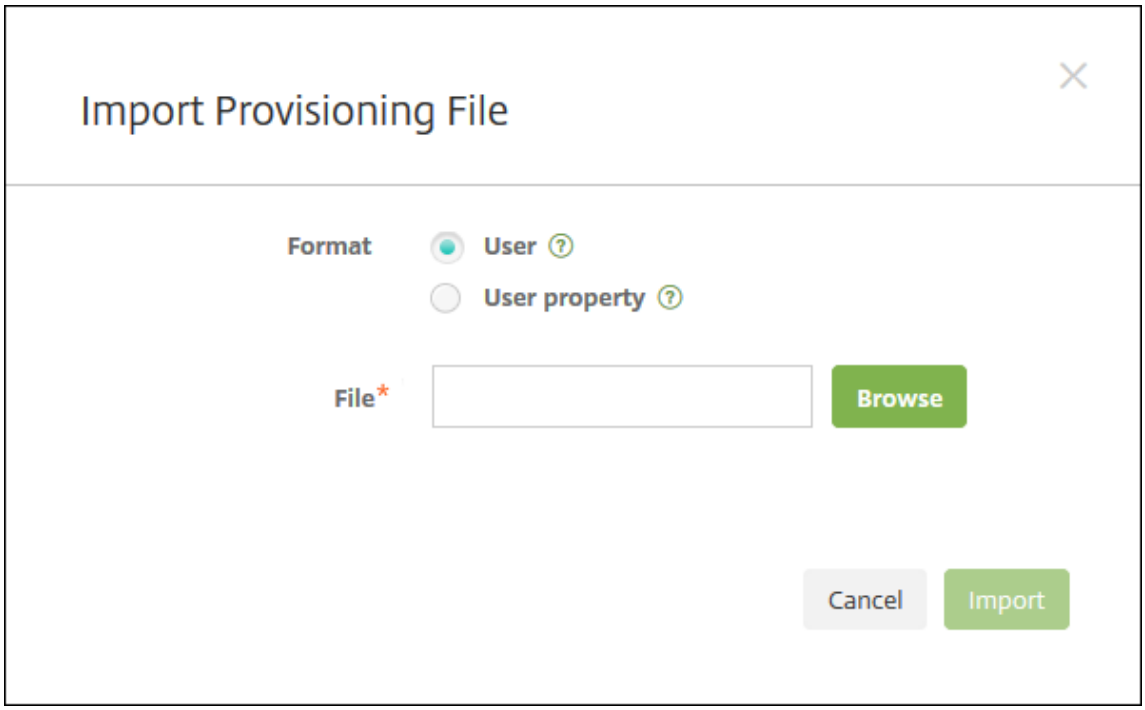
Vous pouvez importer des comptes utilisateur locaux et des propriétés à partir d'un fichier .csv appelé fichier de provisioning, que vous pouvez créer manuellement. Pour de plus amples informations sur la mise en forme des fichiers de provisioning, consultez Formats des fichiers de provisioning.

> **Remarque :**
>
> - Pour les utilisateurs locaux, utilisez le nom de domaine ainsi que le nom d'utilisateur du fichier d'importation. Par exemple, spécifiez nomutilisateur@domaine. Si l'utilisateur local que vous créez ou importez est destiné à un domaine géré dans XenMobile, l'utilisateur ne peut pas s'inscrire en utilisant les informations d'identification LDAP correspondantes.
> - Si vous importez des comptes utilisateur sur l'annuaire utilisateur interne XenMobile, désactivez le domaine par défaut pour accélérer le processus d'importation. N'oubliez pas que

> la désactivation du domaine affecte les inscriptions, c'est la raison pour laquelle vous devez réactiver le domaine par défaut une fois que l'importation des utilisateurs internes est terminée.
> - Les utilisateurs locaux peuvent être au format UPN (nom d'utilisateur principal). Toutefois, Citrix vous recommande de ne pas utiliser le domaine géré. Par exemple, si exemple.com est géré, ne créez pas d'utilisateur local au format UPN : utilisateur@exemple.com.

Lorsque vous préparez un fichier de provisioning, suivez ces étapes pour importer le fichier sur XenMobile.

1. Dans la console XenMobile, cliquez sur **Gérer > Utilisateurs**. La page **Utilisateurs** s'affiche.
2. Cliquez sur **Importer des utilisateurs locaux**. La boîte de dialogue **Importer le fichier de provisioning** apparaît.



3. Sélectionnez **Utilisateur** ou **Propriété** pour le format du fichier de provisioning que vous importez.
4. Sélectionnez le fichier de provisioning à utiliser en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
5. Cliquez sur **Importer**.

Formats des fichiers de provisioning

Vous pouvez créer manuellement un fichier de provisioning pour importer des comptes d'utilisateur et des propriétés dans XenMobile. Les formats valides sont les suivants :

- **Champs des fichiers de provisioning utilisateur :** `user;password;role;group1;group2`
- **Champs des fichiers de provisioning des attributs utilisateur :** `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

> **Remarque :**
>
> - Séparez les champs dans le fichier de provisioning par un point-virgule (;). Si une partie d'un champ contient un point-virgule, elle doit être précédée d'une barre oblique inverse (\). Par exemple, saisissez la propriété `propertyV;test;1;2` en tant que `propertyV\\;test\\;1\\;2` dans le fichier de provisioning.
> - Les valeurs valides pour **Rôle** sont les rôles prédéfinis USER, ADMIN, SUPPORT et DEVICE_PROVISIONING, ainsi que tout autre rôle que vous avez défini.
> - Utilisez le caractère point (.) en tant que séparateur pour créer une hiérarchie de groupe. N'utilisez pas de point dans les noms de groupe.
> - Utilisez des minuscules pour les attributs de propriété dans les fichiers de provisioning d'attribut. La base de données est sensible à la casse.

Exemple de contenu de provisioning utilisateur

L'entrée `user01;pwd\\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` signifie :

- **Utilisateur :** `user01`
- **Mot de passe :** `pwd;01`
- **Rôle :** `USER`
- **Groupes :**
  - `myGroup.users01`
  - `myGroup.users02`
  - `myGroup.users.users.users01`

Dans cet autre exemple, `AUser0;1.password;USER;ActiveDirectory.test.net` signifie :

- **Utilisateur :** `AUser0`
- **Mot de passe :** `1.password`
- **Rôle :** `USER`
- **Groupe :** `ActiveDirectory.test.net`

Exemple de contenu de provisioning d'attribut utilisateur

L'entrée `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` signifie :

- **Utilisateur :** `user01`
- **Propriété 1**
  - **nom :** `propertyN`

    - **valeur :** `propertyV;test;1;2`
- **Propriété 2 :**
    - **nom :** `prop 2`
    - **valeur :** `prop2 value`

Configurer les modes d'inscription sécurisée

Vous configurez un mode d'inscription sécurisée pour l'appareil pour spécifier un niveau de sécurité et un modèle de notification pour l'inscription d'appareil dans XenMobile.

XenMobile offre sept modes d'inscription sécurisée, chacun doté de son propre niveau de sécurité et de ses propres étapes que les utilisateurs doivent suivre pour inscrire leurs appareils. Vous configurez les modes d'inscription sécurisée dans la console XenMobile Server sur la page **Paramètres > Inscription**.

Vous pouvez mettre à disposition certains modes sur le portail utilisateur. À partir du portail, les utilisateurs génèrent des liens d'inscription qui leur permettent d'inscrire leurs appareils. Les utilisateurs d'appareils iOS, iPadOS, macOS, Android Enterprise et d'appareils Android d'ancienne génération peuvent choisir d'envoyer eux-mêmes une invitation d'inscription à partir du portail. Les invitations d'inscription ne sont pas disponibles pour les appareils Windows.

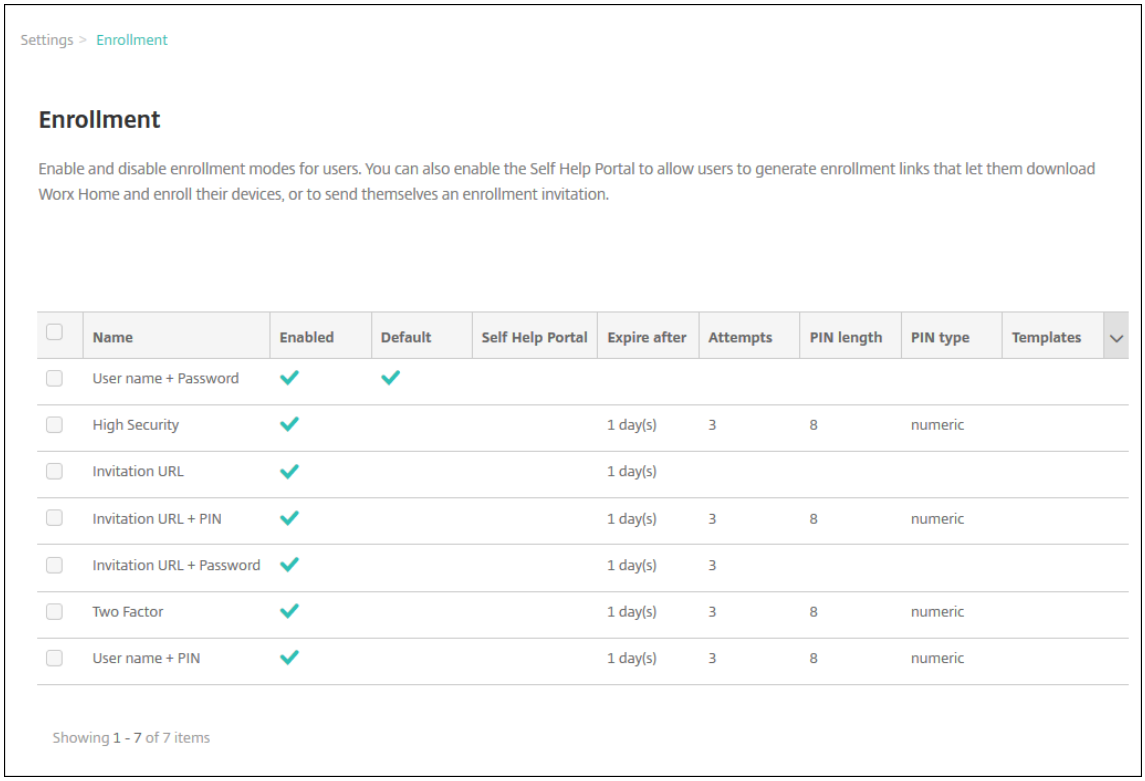
Vous envoyez des invitations d'inscription depuis la page **Gérer > Invitations d'inscription**. Pour de plus amples informations, consultez la section Envoyer une invitation d'inscription.

> **Remarque :**
>
> Si vous prévoyez d'utiliser des modèles de notification personnalisés, vous devez définir les modèles avant de configurer des modes de sécurité d'inscription. Pour de plus amples informations sur les modèles de notification, consultez la section Création et mise à jour de modèles de notification.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Inscription**. La page **Inscription** s'affiche. Elle contient un tableau de tous les modes d'inscription sécurisée disponibles. Par défaut, tous les modes d'inscription sécurisée sont activés.
3. Sélectionnez un mode d'inscription sécurisée à modifier dans la liste. Définissez ensuite le mode comme le mode par défaut, désactivez le mode ou autorisez l'accès des utilisateurs via le portail utilisateur.

    > **Remarque :**
    >
    > Lorsque vous sélectionnez la case à cocher en regard d'un mode d'inscription sécurisée, le menu d'options s'affiche au-dessus de la liste des modes d'inscription sécurisée. Lorsque

> vous cliquez dans la liste, le menu d'options s'affiche sur le côté droit de la liste.



Choisissez parmi les modes d'inscription sécurisée :

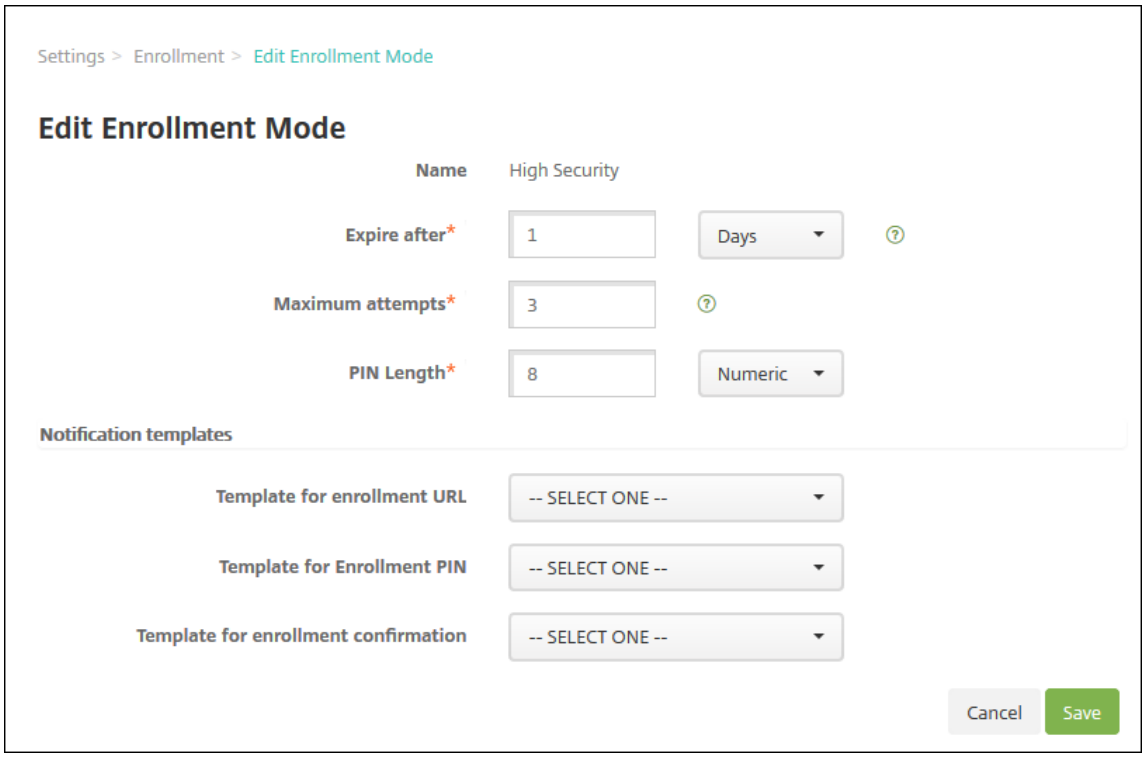
- Nom d'utilisateur + mot de passe
- Haute sécurité
- URL d'invitation
- URL d'invitation + PIN
- URL d'invitation + mot de passe
- Authentification à deux facteurs
- Nom d'utilisateur + PIN

Vous pouvez utiliser des invitations d'inscription pour restreindre l'inscription aux utilisateurs avec une invitation uniquement. Pour envoyer des invitations d'inscription, vous pouvez uniquement utiliser les modes d'inscription sécurisée **URL d'invitation**, **URL d'invitation + PIN** ou **URL d'invitation + mot de passe**. Pour les appareils qui sont inscrits avec **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + PIN**, les utilisateurs doivent entrer manuellement leurs informations d'identification dans Secure Hub.

Vous pouvez utiliser des invitations d'inscription avec code PIN à usage unique (OTP) comme solution d'authentification à deux facteurs. Les invitations d'inscription OTP contrôlent le nombre d'appareils qu'un utilisateur peut inscrire. Les invitations OTP ne sont pas disponibles pour les appareils Windows.

Pour modifier un mode d'inscription sécurisée

1. Dans la liste **Inscription**, sélectionnez un mode d'inscription sécurisée, puis cliquez sur **Modifier**. La page **Modifier le mode d'inscription** apparaît. Le mode que vous sélectionnez détermine les options affichées.



2. Modifiez les informations suivantes le cas échéant :

   - **Expire après :** entrez un délai d'expiration au-delà duquel les utilisateurs ne peuvent pas inscrire leurs appareils. Cette valeur s'affiche dans les pages de configuration des invitations d'inscription des utilisateurs et des groupes.

     Tapez **0** pour éviter que l'invitation n'expire.

   - **Jours :** dans la liste, cliquez sur **Jours** ou **Heures** afin qu'ils correspondent au délai d'expiration que vous avez entré dans **Expire après**.

   - **Nbre max de tentatives :** entrez le nombre de tentatives d'inscription qu'un utilisateur peut effectuer avant qu'il ne soit verrouillé du processus d'inscription. Cette valeur s'affiche dans les pages de configuration des invitations d'inscription des utilisateurs et des groupes.

     Tapez **0** pour autoriser un nombre illimité de tentatives.

   - **Longueur du code PIN :** entrez un chiffre pour définir la longueur du code PIN généré.

   - **Numérique :** dans la liste, cliquez sur **Numérique** ou **Alphanumérique** pour le type de code PIN.

- **Modèles de notification :**
  - **Modèle pour l'URL d'inscription :** sélectionnez un modèle à utiliser pour l'adresse URL d'inscription. Par exemple, le modèle d'invitation d'inscription envoie aux utilisateurs un e-mail ou un SMS. La méthode dépend de la manière dont vous avez configuré le modèle qui leur permet d'inscrire leurs appareils dans XenMobile. Pour plus d'informations sur les modèles de notification, consultez la section Créer et mettre à jour des modèles de notification.
  - **Modèle pour le PIN d'inscription :** dans la liste, sélectionnez un modèle à utiliser pour le PIN d'inscription.
  - **Modèle pour la confirmation d'inscription :** dans la liste, sélectionnez un modèle à utiliser pour informer un utilisateur que l'inscription a réussi.

3. Cliquez sur **Enregistrer**.

Pour définir un mode d'inscription sécurisée comme mode par défaut

Lorsque vous définissez un mode d'inscription sécurisée en tant que mode par défaut, le mode est utilisé pour toutes les demandes d'inscription d'appareil, sauf si vous sélectionnez un autre mode d'inscription. Si aucun mode d'inscription sécurisée n'est défini par défaut, vous devez créer une demande d'inscription pour chaque inscription d'appareil.

> **Remarque :**
>
> Les seuls modes d'inscription sécurisée que vous pouvez utiliser par défaut sont **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + code PIN**.

1. Sélectionnez le mode d'inscription sécurisée par défaut : **Nom d'utilisateur + mots de passe**, **Deux facteurs** ou **Nom d'utilisateur + PIN**.

   Pour utiliser un mode comme mode par défaut, vous devez tout d'abord l'activer.

2. Cliquez sur **Défaut**. Le mode sélectionné est maintenant le mode par défaut. Si un autre mode d'inscription sécurisée a été défini comme mode par défaut, le mode n'est plus le mode par défaut.

Pour désactiver un mode d'inscription sécurisée

La désactivation d'un mode d'inscription sécurisée rend ce dernier inutilisable, à la fois pour les invitations d'inscription de groupe et sur le portail en libre-service. Vous pouvez modifier la façon dont les utilisateurs peuvent inscrire leurs appareils en désactivant un mode d'inscription sécurisée et en activant un autre.

1. Sélectionnez un mode d'inscription sécurisée.

Vous ne pouvez pas désactiver le mode d'inscription sécurisée par défaut. Pour désactiver le mode d'inscription sécurisée par défaut, vous devez d'abord lui retirer son état de mode par défaut.

2. Cliquez sur **Désactiver**. Le mode d'inscription sécurisée n'est plus activé.

Pour activer un mode d'inscription sécurisée sur le portail en libre-service

L'activation d'un mode d'inscription sécurisée sur le portail en libre-service permet aux utilisateurs d'inscrire leurs appareils dans XenMobile individuellement.

> **Remarque :**
>
> - Le mode d'inscription sécurisée doit être activé et lié à des modèles de notification pour être disponible sur le portail en libre-service.
> - Vous ne pouvez activer qu'un seul mode d'inscription sécurisée à la fois sur le portail utilisateur.

1. Sélectionnez un mode d'inscription sécurisée.
2. Cliquez sur **Portail en libre-service**. Le mode d'inscription sécurisée que vous avez sélectionné est maintenant mis à la disposition des utilisateurs sur le portail en libre-service. Tout mode déjà activé sur le portail en libre-service n'est plus disponible.

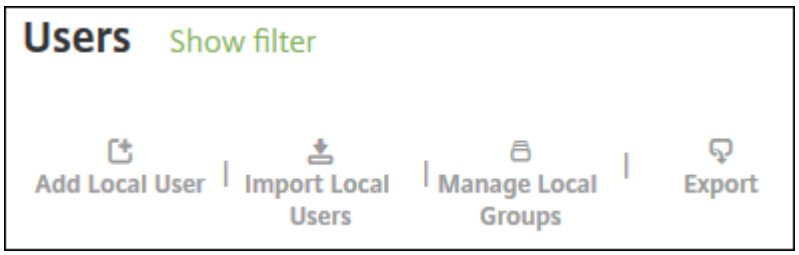
Ajout ou suppression de groupes

Vous gérez les groupes dans la boîte de dialogue **Gérer les groupes** dans la console XenMobile sur ces pages : **Utilisateurs**, **Ajouter un utilisateur local** ou **Modifier un utilisateur local**. Aucune commande ne permet de modifier un groupe.

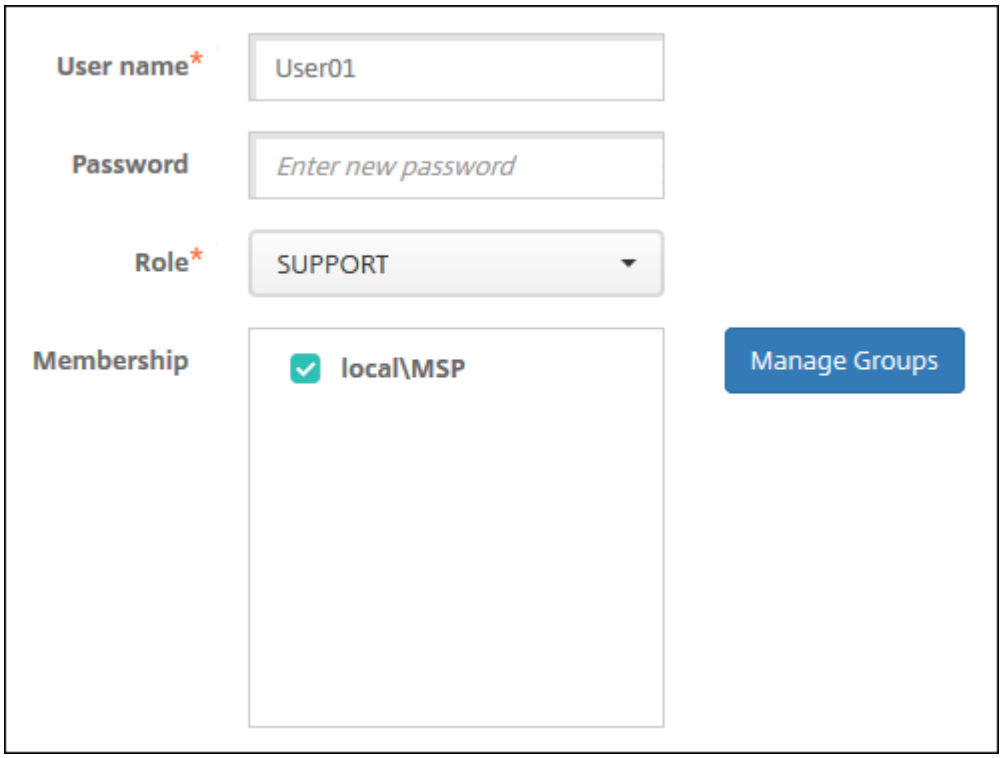
Si vous supprimez un groupe, n'oubliez pas que la suppression du groupe n'a aucun effet sur les comptes d'utilisateur. La suppression d'un groupe supprime simplement l'association des utilisateurs avec ce groupe. Les utilisateurs perdent également l'accès aux applications ou profils fournis par les groupes de mise à disposition qui sont associés à ce groupe ; toutes les autres associations de groupe restent toutefois intactes. Si les utilisateurs ne sont associés à aucun autre groupe local, ils sont associés au niveau supérieur.

Pour ajouter un groupe local

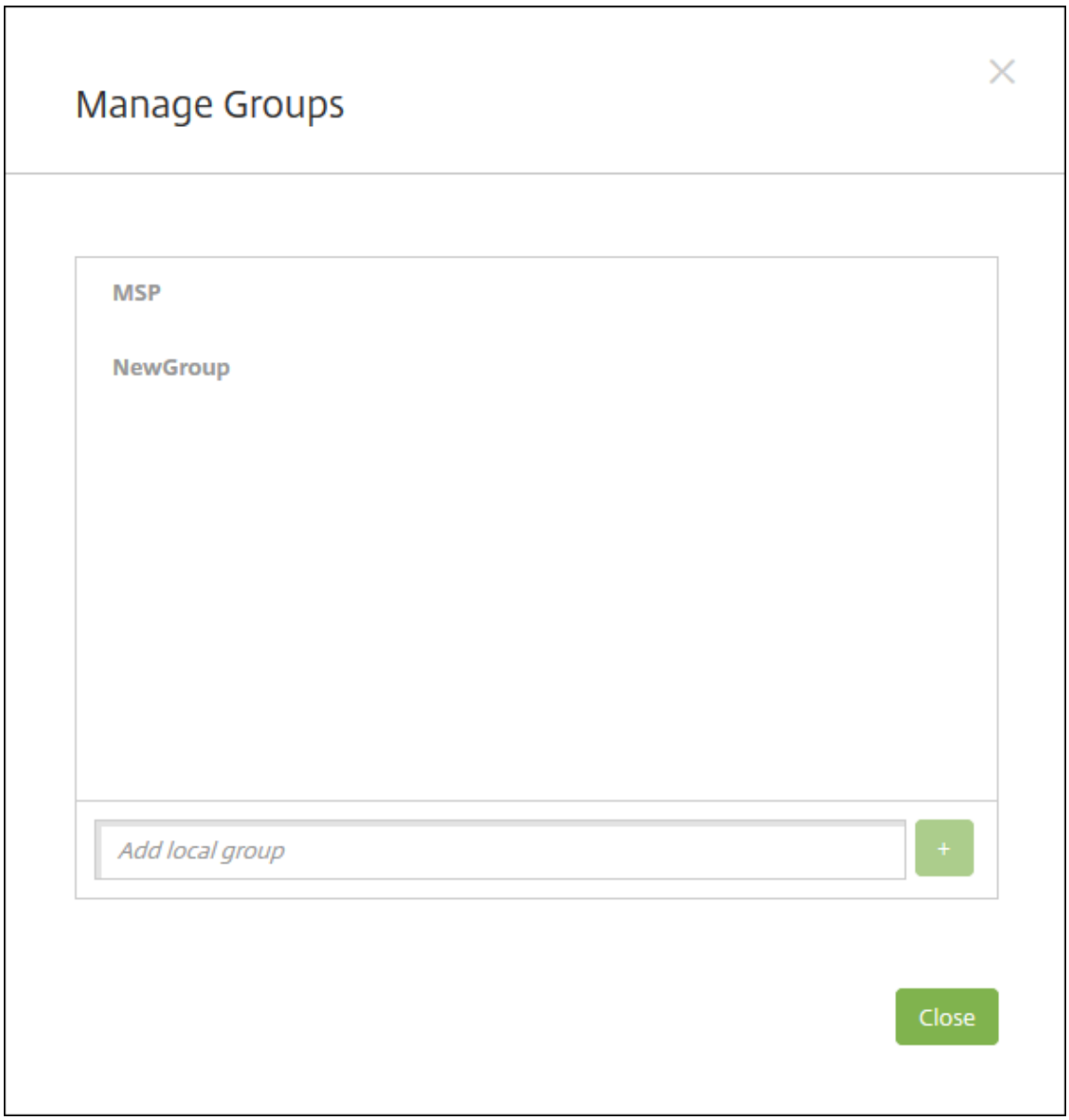
1. Procédez comme suit :
    - Sur la page **Utilisateurs**, cliquez sur **Gérer les groupes locaux**.



- Sur la page **Ajouter un utilisateur local** ou la page **Modifier un utilisateur local**, cliquez sur **Gérer les groupes**.



La boîte de dialogue **Gérer les groupes** s'affiche.



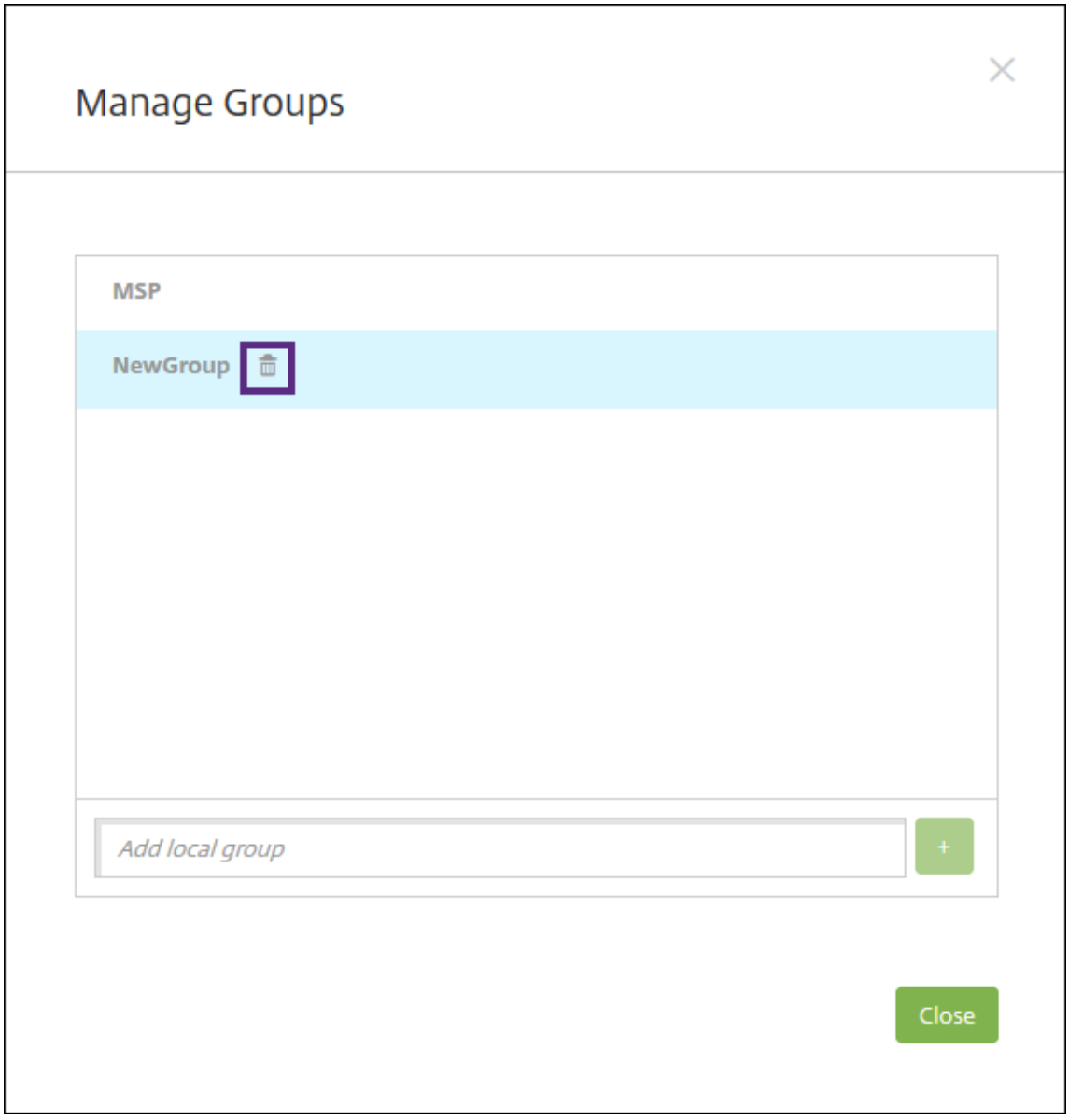
2. Sous les listes de groupes, entrez un nouveau nom de groupe, puis cliquez sur le signe plus (**+**). Le groupe d'utilisateurs est ajouté à la liste.
3. Cliquez sur **Fermer**.

Pour supprimer un groupe

La suppression d'un groupe n'a aucun effet sur les comptes d'utilisateur. La suppression d'un groupe supprime simplement l'association des utilisateurs avec ce groupe. Les utilisateurs perdent également l'accès aux applications ou profils fournis par les groupes de mise à disposition qui sont associés à ce groupe. Les autres associations de groupe restent toutefois intactes. Si les utilisateurs ne sont associés à aucun autre groupe local, ils sont associés au niveau supérieur.

1. Procédez comme suit :
   - Sur la page **Utilisateurs**, cliquez sur **Gérer les groupes locaux**.
   - Sur la page **Ajouter un utilisateur local** ou la page **Modifier un utilisateur local**, cliquez sur **Gérer les groupes**.

   La boîte de dialogue **Gérer les groupes** s'affiche.



2. Dans la boîte de dialogue **Gérer les groupes**, sélectionnez le groupe que vous souhaitez supprimer.
3. Cliquez sur l'icône de la corbeille à droite du nom de groupe. Une boîte de dialogue de confirmation s'affiche.
4. Cliquez sur **Supprimer** pour confirmer l'opération et supprimer le groupe.

> **Important :**
>
> vous ne pouvez pas annuler cette opération.

5. Dans la boîte de dialogue **Gérer les groupes**, cliquez sur **Fermer**.

Créer et gérer des workflows

Vous pouvez appliquer des workflows pour gérer la création et la suppression des comptes utilisateur. Avant de pouvoir utiliser un workflow, vous devez identifier les personnes de votre organisation chargées d'approuver les demandes d'ouverture de comptes d'utilisateur. Vous pouvez ensuite utiliser le modèle de workflow pour créer et approuver les demandes.

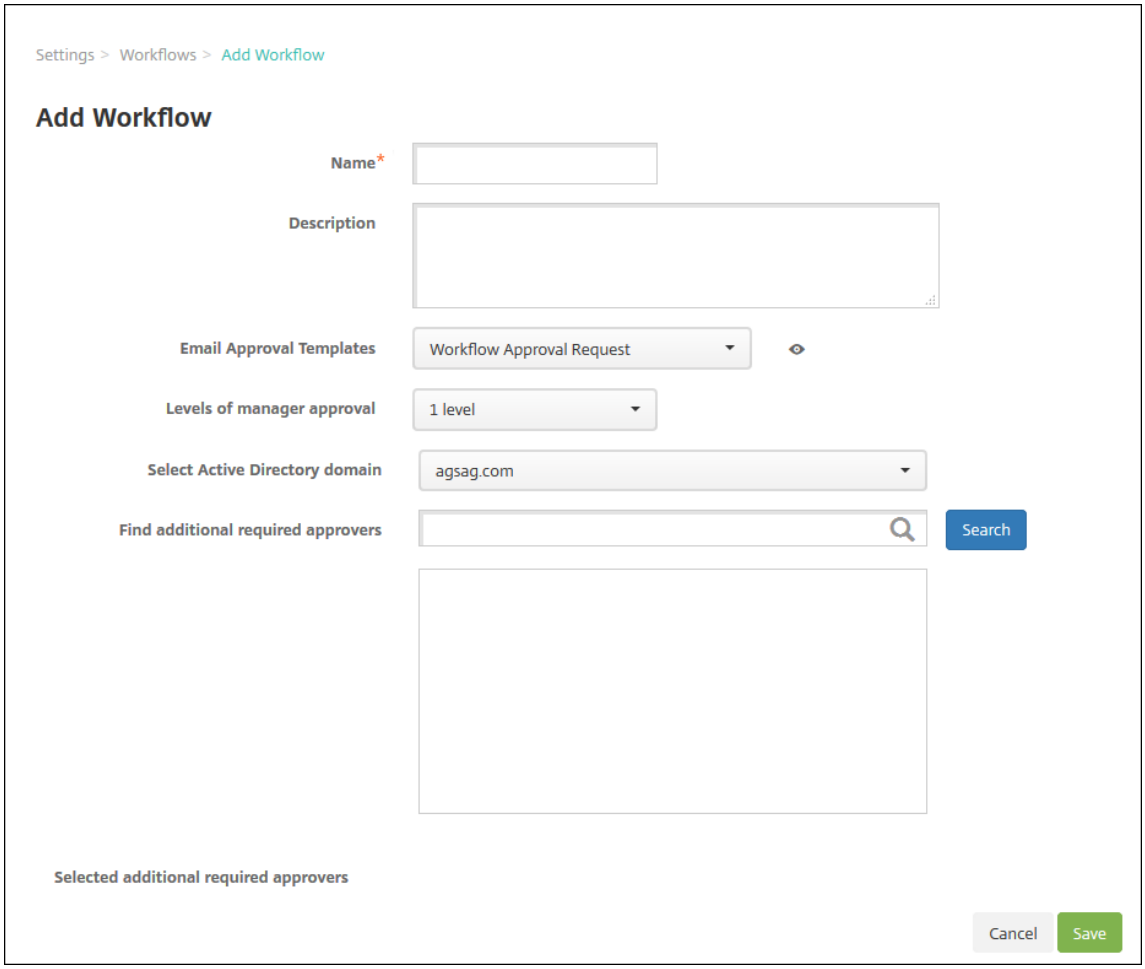
Lorsque vous configurez XenMobile pour la première fois, vous configurez les paramètres d'e-mail de workflow, qui doivent être définis avant que vous puissiez utiliser des workflows. Vous pouvez modifier les paramètres de messagerie de workflow à tout moment. Ces paramètres incluent le serveur de messagerie, le port, l'adresse e-mail et si la demande de création du compte utilisateur requiert une approbation.

Vous pouvez configurer des workflows à deux emplacements dans XenMobile :

- Sur la page **Workflows** sur la console XenMobile. Sur la page **Workflows**, vous pouvez configurer plusieurs workflows à utiliser pour la configuration d'applications. Lorsque vous configurez des workflows sur la page Workflows, vous pouvez sélectionner le workflow lors de la configuration de l'application.
- Lorsque vous configurez un connecteur d'application, dans l'application, vous devez fournir un nom de workflow, puis configurer les personnes qui peuvent approuver la demande de compte utilisateur. Consultez la section Ajout d'applications à XenMobile.

Vous pouvez désigner jusqu'à trois niveaux pour l'approbation du responsable des comptes d'utilisateur. Si vous voulez faire approuver le compte utilisateur par d'autres personnes, vous pouvez les rechercher et les sélectionner en utilisant leur nom ou adresse e-mail. Lorsque XenMobile trouve la personne concernée, vous pouvez l'ajouter au workflow. Toutes les personnes figurant dans le workflow reçoivent un e-mail afin d'approuver ou de refuser l'ouverture du nouveau compte d'utilisateur.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Workflows**. La page **Workflows** s'affiche.
3. Cliquez sur **Ajouter**. La page **Ajouter un workflow** s'affiche.



4. Pour configurer ces paramètres :

   - **Nom :** entrez un nom unique pour le workflow.
   - **Description :** entrez une description pour le workflow (facultatif).
   - **Modèles d'approbation d'e-mail :** dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Vous créez des modèles d'e-mail dans la section **Modèles de notification** sous **Paramètres** dans la console XenMobile. Lorsque vous cliquez sur l'icône d'œil à droite de ce champ, vous voyez un aperçu du modèle que vous êtes en train de configurer.
   - **Niveaux d'approbation par un responsable :** dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est **1 niveau**. Les options possibles sont les suivantes :
     - Pas nécessaire
     - 1 niveau
     - 2 niveaux
     - 3 niveaux
   - **Sélectionner un domaine Active Directory :** dans la liste, sélectionnez le domaine Active

Directory à utiliser pour le workflow.

- **Rechercher des approbateurs supplémentaires requis :** tapez un nom dans le champ de recherche et cliquez sur **Rechercher**. Les noms proviennent d'Active Directory.
- Lorsque le nom s'affiche dans le champ, sélectionnez la case à cocher en regard du nom. Le nom et l'adresse e-mail s'affichent dans la liste **Approbateurs supplémentaires requis sélectionnés**.
  - Pour supprimer un nom de la liste, effectuez l'une des opérations suivantes :
    * Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.
    * Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats de la recherche.
    * Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

5. Cliquez sur **Enregistrer**. Le workflow créé s'affiche sur la page **Workflows**.

Après avoir créé le workflow, vous pouvez afficher les détails du workflow, voir les applications associées au workflow ou supprimer le workflow. Vous ne pouvez pas modifier un workflow après sa création. Si vous avez besoin d'un workflow avec différents niveaux d'approbation ou approbateurs, créez un autre workflow.

Pour afficher les détails d'un workflow et le supprimer

1. Sur la page **Workflows**, dans la liste des workflows, sélectionnez un workflow. Pour ce faire, cliquez sur la ligne dans le tableau ou sélectionnez la case à cocher en regard du workflow.
2. Pour supprimer un workflow, cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer**.

> **Important :**
>
> vous ne pouvez pas annuler cette opération.

Profils d'inscription

January 10, 2022

Un profil d'inscription permet de spécifier les éléments suivants :

- Options d'inscription associées à la gestion d'appareils pour les appareils Android et iOS Pour Android, les options d'inscription disponibles pour le mode serveur MDM+MAM (ENT) diffèrent

des options du mode MDM.
- Options d'inscription associées à la gestion d'applications pour les appareils Android et iOS
- Autres options d'inscription :
  - Indique s'il faut limiter le nombre d'appareils qu'un utilisateur peut inscrire. Si le nombre maximal d'appareils est atteint, un message d'erreur informe l'utilisateur qu'il a dépassé la limite d'enregistrement d'appareils.
  - Indique s'il faut autoriser un utilisateur à refuser la gestion d'appareils.

Vous pouvez utiliser des profils d'inscription pour combiner plusieurs cas d'utilisation et chemins de migration d'appareils au sein d'une seule console XenMobile Server. Parmi les cas d'utilisation :

- Gestion des appareils mobiles (MDM exclusif)
- MDM+Gestion des applications mobiles (MAM)
- MAM exclusif
- Inscriptions d'appareils appartenant à l'entreprise
- Inscriptions BYOD (possibilité de se désinscrire de MDM)
- Migration des inscriptions Administrateur d'appareil Android vers les inscriptions Android Enterprise (appareil entièrement géré, profil de travail, dédié)

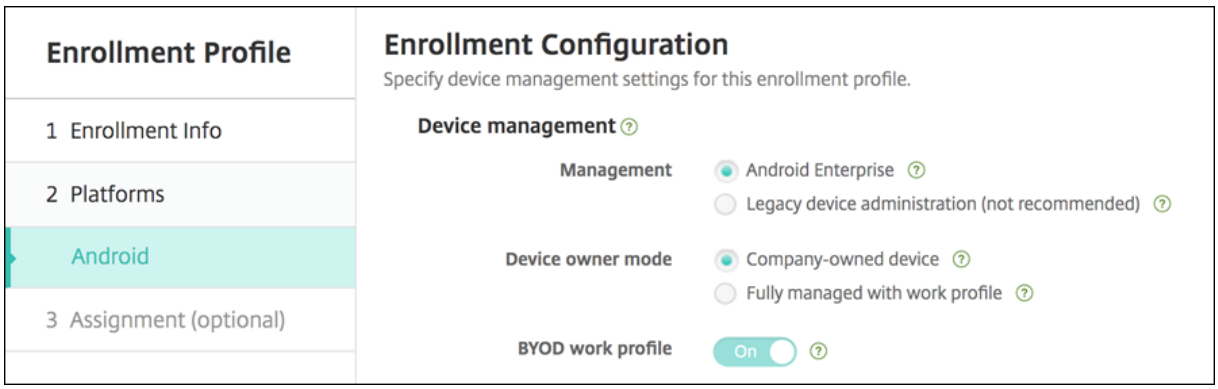
Lorsque vous créez un groupe de mise à disposition, vous pouvez utiliser le profil d'inscription par défaut nommé Global ou spécifier un profil d'inscription différent.

Les caractéristiques du profil d'inscription par plateforme sont les suivantes.

- **Pour les appareils Android :** vous spécifiez le mode propriétaire de l'appareil. Par exemple : entièrement géré, entièrement géré avec profil de travail et profil de travail BYOD. L'option **Appareil dédié** s'affiche uniquement lorsque vous disposez d'une licence Enterprise ou Advanced pour XenMobile. Par défaut, les nouveaux appareils sont inscrits dans Android Enterprise et la gestion des applications. Les modes d'inscription sécurisée **Nom d'utilisateur + PIN**, **URL d'invitation**, **URL d'invitation + PIN** et **URL d'invitation + mot de passe** ne sont pas disponibles pour Android Enterprise.
- **Pour les appareils iOS :** vous spécifiez le type d'inscription de l'appareil : Inscription d'appareils ou aucune gestion. Les paramètres iOS apparaissent uniquement lorsque vous disposez d'une licence Enterprise ou Advanced pour XenMobile. Par défaut, les nouveaux appareils sont inscrits dans la gestion des appareils Apple et la gestion des applications.

Si vous n'avez pas besoin d'inscrire des appareils dédiés pour les appareils Android ou l'inscription MAM exclusif pour les appareils Android ou iOS, vous pouvez désactiver la propriété de serveur `enable.multimode.xms`. Toutefois, si cette propriété est activée, vous n'avez besoin que d'un seul serveur XenMobile Server pour gérer tous les types de profils d'inscription. Consultez Propriétés du serveur.

Lorsque vous désactivez `enable.multimode.xms`, seuls les paramètres de cette capture d'écran sont disponibles :

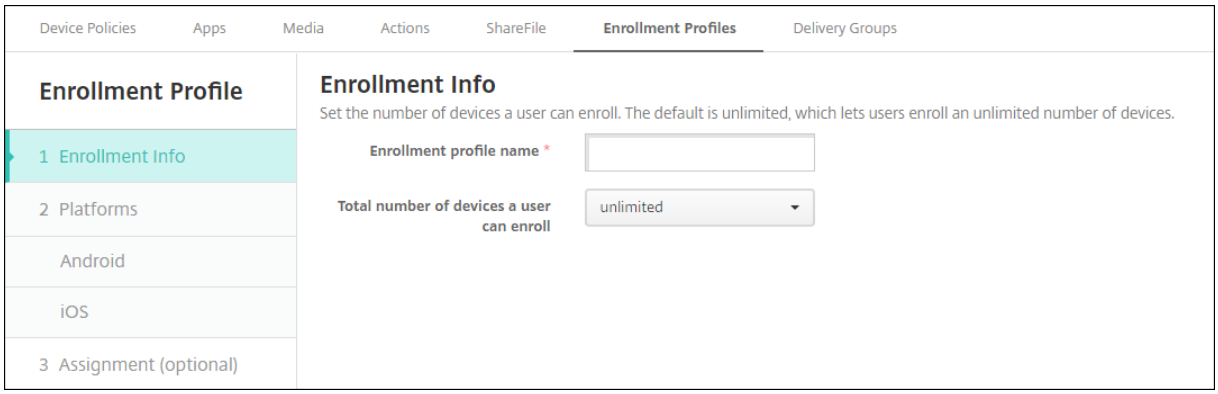


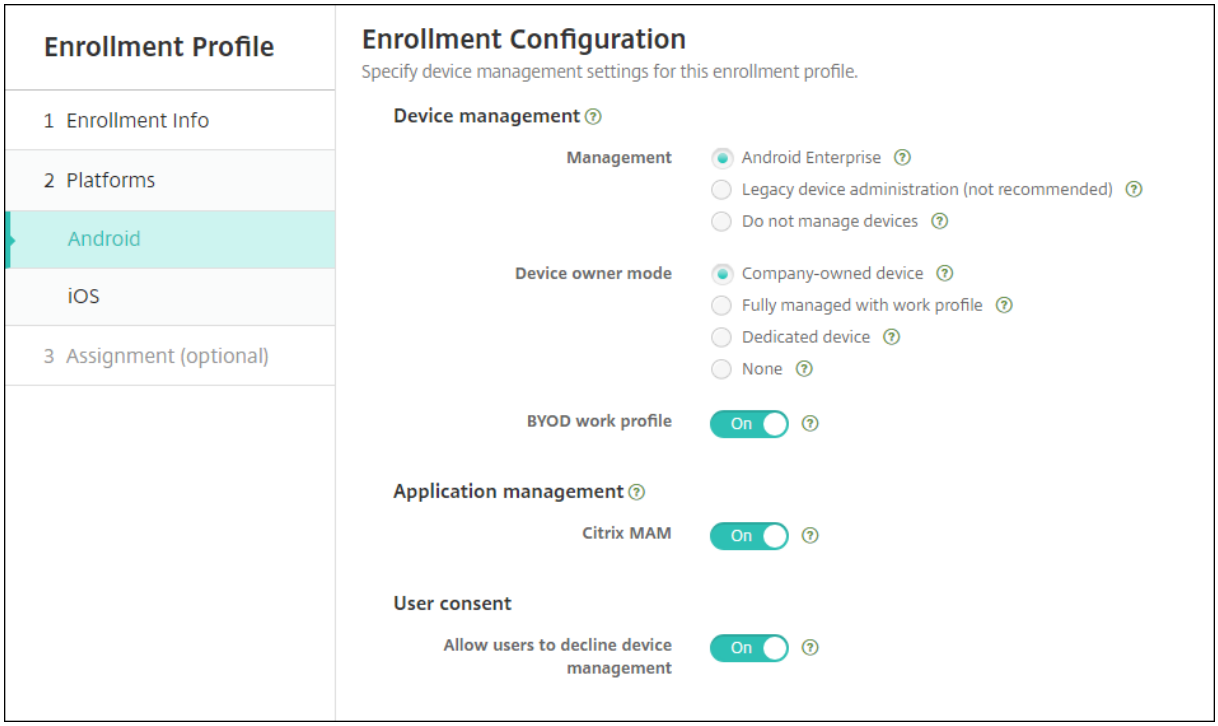
Pour plus d'informations sur ces paramètres, consultez Android Enterprise.

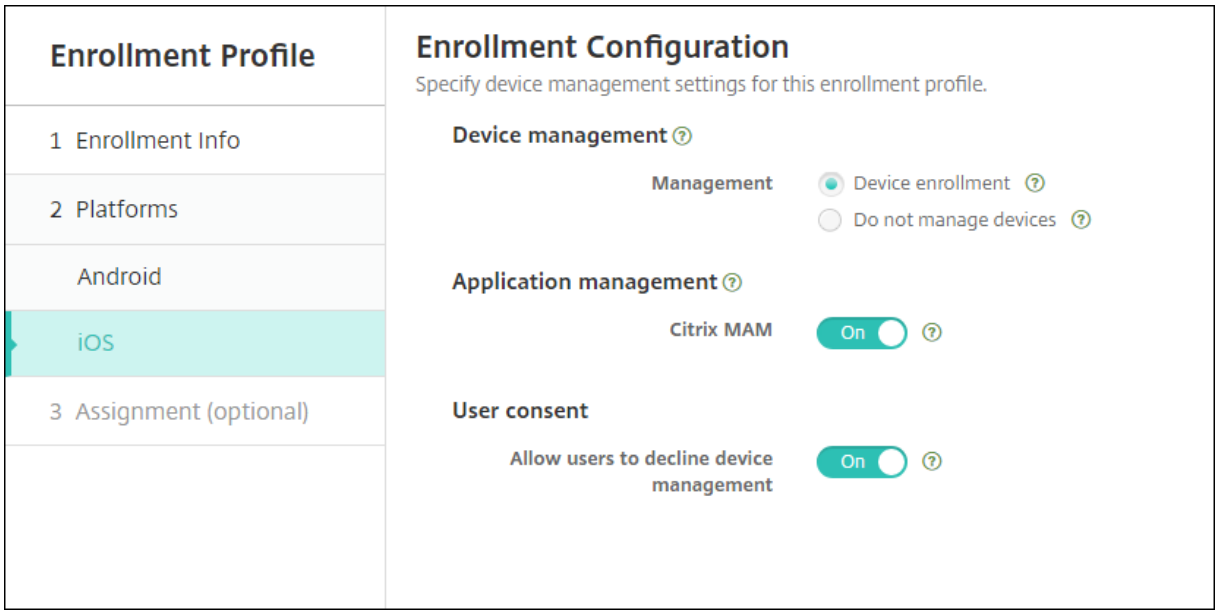
Profil d'inscription Global

Le profil d'inscription par défaut est appelé Global. Le profil Global est utile pour effectuer des tests jusqu'à ce que vous ayez la possibilité de créer des profils d'inscription.

Les captures d'écran suivantes affichent les paramètres par défaut du profil d'inscription Global.







Profils d'inscription, groupes de mise à disposition et inscription

Les profils d'inscription et les groupes de mise à disposition interagissent comme suit :

- Vous pouvez joindre un profil d'inscription à un ou plusieurs groupes de mise à disposition.
- Si un utilisateur appartient à plusieurs groupes de mise à disposition qui ont des profils d'inscription différents, le nom du groupe de mise à disposition détermine le profil d'inscription utilisé. XenMobile Server sélectionne le groupe de mise à disposition qui apparaît en dernier

dans une liste alphabétique des groupes de mise à disposition. Par exemple, supposons que vous disposez des éléments suivants :

- Deux profils d'inscription, nommés « EP1 » et « EP2 ».
- Deux groupes de mise à disposition, nommés « DG1 » et « DG2 ».
- « DG1 » est associé à « EP1 ».
- « DG2 » est associé à « EP2 ».

Si l'utilisateur inscrit fait partie des groupes de mise à disposition « DG1 » et « DG2 », XenMobile Server utilise le profil d'inscription « EP2 » pour déterminer le type d'inscription pour l'utilisateur.

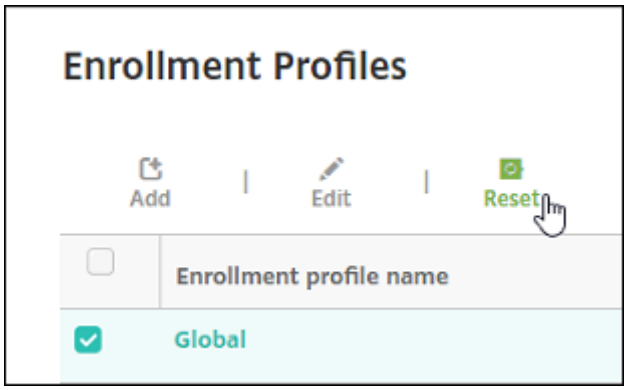
- L'ordre de déploiement s'applique uniquement aux appareils d'un groupe de mise à disposition dont le profil d'inscription est configuré pour la gestion des appareils (MDM).
- Après l'inscription d'un appareil, certaines modifications apportées à un profil d'inscription nécessitent une réinscription :
  - Ajout de MAM à un profil d'inscription configuré pour MDM.
  - Déplacement d'un appareil inscrit à MDM vers un groupe de mise à disposition configuré pour MDM+MAM. Cette modification n'affecte que les inscriptions de nouveaux appareils. Les inscriptions d'appareils existantes ne sont pas affectées.
  - Ajout de MDM à un profil d'inscription configuré pour MAM.
- Le passage à un profil d'inscription différent n'affecte pas les appareils inscrits existants. Toutefois, les utilisateurs doivent désinscrire, puis réinscrire ces appareils pour que les modifications prennent effet.

Pour créer un profil d'inscription

1. Dans la console XenMobile Server, accédez à **Configurer > Profils d'inscription**.
2. Dans la page **Infos d'inscription**, tapez un nom descriptif pour le profil. Par défaut, un utilisateur peut inscrire un nombre illimité d'appareils. Sélectionnez une valeur pour limiter le nombre d'appareils par utilisateur. La limite s'applique à la somme des appareils Android et iOS gérés par MAM ou MDM qu'un utilisateur inscrit.
3. Renseignez les pages de plates-formes. Pour plus d'informations sur les paramètres d'inscription spécifiques aux plates-formes, voir :
   - Android Entreprise
   - iOS : Méthodes d'inscription prises en charge
4. Sur la page **Attribution**, attachez un ou plusieurs groupes de mise à disposition au profil d'inscription.

Un utilisateur peut appartenir à plusieurs groupes de mise à disposition ayant des profils d'inscription différents. Dans ce cas, le nom du groupe de mise à disposition détermine le profil d'inscription utilisé. XenMobile sélectionne le groupe de mise à disposition qui apparaît en dernier dans une liste alphabétique des groupes de mise à disposition. Pour créer des groupes de mise à disposition, accédez à **Configurer > Groupes de mise à disposition**.

La liste de vos profils d'inscription apparaît sur la page **Configurer > Profils d'inscription**. Pour modifier le profil Global ou le réinitialiser sur les valeurs par défaut d'origine, sélectionnez la ligne correspondant au profil Global et cliquez sur **Réinitialiser**. Vous ne pouvez pas supprimer le profil Global.



Configurer des rôles avec RBAC

January 10, 2022

Chaque rôle RBAC prédéfini dispose de certains accès et de certaines autorisations associés. Cet article explique chacune de ces autorisations. Pour obtenir une liste complète des autorisations par défaut pour chaque rôle intégré, téléchargez le PDF Role-Based Access Control Defaults.

Lorsque vous *appliquez des autorisations*, vous définissez les groupes d'utilisateurs que le rôle RBAC est autorisé à gérer. L'administrateur par défaut ne peut pas modifier les paramètres d'autorisation appliqués. Par défaut, les autorisations appliquées s'appliquent à tous les groupes d'utilisateurs.

Lorsque vous procédez à une *attribution*, vous attribuez le rôle RBAC à un groupe, afin que le groupe d'utilisateurs disposent des droits d'administrateur RBAC.

> **Important :**
>
> Sous l'autorisation Paramètres, l'autorisation RBAC donne aux utilisateurs Admin un accès complet, y compris la possibilité d'attribuer leurs propres autorisations. Accordez cet accès uniquement aux utilisateurs auxquels vous avez l'intention de donner la possibilité de manipuler tout ce qui se trouve dans le système Endpoint Management.

Cet article comporte les sections suivantes :

Rôle d'administrateur

Les utilisateurs avec le rôle administrateur prédéfini ont accès ou n'ont pas accès aux fonctionnalités suivantes dans XenMobile. Par défaut, **Accès autorisé** (sauf Portail en libre-service), **Fonctionnalités de la console** et **Appliquer des autorisations** sont activés.

Accès autorisé

Accès à la console d'admin	Les administrateurs ont accès à toutes les fonctions de la console XenMobile.
Accès au portail en libre-service	Les administrateurs n'ont pas accès au portail en libre-service.
Assistant d'inscription d'appareils partagés	Les administrateurs n'ont pas accès à l'assistant d'inscription d'appareils partagés. Cette fonctionnalité est conçue pour les utilisateurs qui ont besoin d'inscrire des appareils partagés.
Accès à l'assistance à distance	Les administrateurs ont accès à l'Assistance à distance.*
Accès à l'API publique	Les administrateurs ont accès à l'API publique pour réaliser via un programme des actions qui sont disponibles sur la console XenMobile. Ces actions comprennent l'administration des certificats, des applications, des appareils, des groupes de mise à disposition et des utilisateurs locaux.

Inscription d'appareils COSU	Permet aux administrateurs d'inscrire des appareils Android Enterprise dédiés (également appelés appareils COSU) si cette fonctionnalité n'est pas configurée à l'aide d'un profil d'inscription.

* L'Assistance à distance permet aux représentants du service d'assistance de contrôler à distance des appareils mobiles Windows CE et Android gérés. La capture d'écran est uniquement prise en charge sur les appareils Samsung Knox. L'Assistance à distance n'est pas disponible pour les déploiements de XenMobile Server locaux en cluster. L'Assistance à distance n'est plus disponible pour les nouveaux clients à compter du 1er janvier 2019. Les clients existants peuvent continuer à utiliser le produit, mais Citrix ne fournit pas d'améliorations ou de correctifs.

Fonctionnalités de la console

Les administrateurs ont un accès illimité à la console XenMobile.

Tableau de bord	Le **tableau de bord** est la première page que les administrateurs voient s'afficher après une ouverture de session sur la console XenMobile. Le **tableau de bord** contient des informations de base sur les notifications et les appareils.
Rapports	La page **Analyser > Rapports** propose des rapports prédéfinis qui vous permettent d'analyser les déploiements d'applications et d'appareils.
Périphériques	La page **Gérer > Appareils** vous permet de gérer les appareils des utilisateurs. Vous pouvez ajouter des appareils un par un sur la page, ou importer un fichier de provisioning pour ajouter plusieurs appareils à la fois.
Utilisateurs et groupes locaux	La page **Gérer > Utilisateurs** vous permet d'ajouter, de modifier ou de supprimer des utilisateurs locaux et des groupes d'utilisateurs locaux.
Inscription	La page **Gérer > Invitations d'inscription** vous permet de gérer la manière dont les utilisateurs sont invités à inscrire leurs appareils dans XenMobile.
Stratégies	La page **Configurer > Stratégies d'appareil** est la page à partir de laquelle vous gérez les stratégies telles que VPN et Wi-Fi.
Applications	La page **Configurer > Applications** vous permet de gérer les applications que les utilisateurs peuvent installer sur leurs appareils.
Média	La page **Configurer > Média** vous permet de gérer le contenu multimédia que les utilisateurs peuvent installer sur leurs appareils.

Action	La page **Configurer > Actions** vous permet de gérer les réponses pour déclencher des événements.
Profils d'inscription	La page **Configurer > Profils d'inscription** vous permet de configurer des profils d'inscription (modes) pour permettre aux utilisateurs d'inscrire leurs appareils.
Groupes de mise à disposition	La page **Configurer > Groupes de mise à disposition** vous permet de gérer les groupes de mise à disposition et les ressources associées.
Paramètres	La page **Paramètres** vous permet de gérer les paramètres du système, tels que les propriétés client et serveur, les certificats et les fournisseurs d'identités. **Important :** ces paramètres incluent l'autorisation RBAC. L'autorisation RBAC donne aux administrateurs un accès complet, y compris la possibilité d'attribuer leurs propres autorisations. Accordez cet accès uniquement aux utilisateurs auxquels vous avez l'intention de donner la possibilité de manipuler tout ce qui se trouve dans le système Endpoint Management.	
Support	La page **Dépannage et support** vous permet de réaliser des tâches de résolution des problèmes telles que l'exécution de diagnostics et la génération de journaux.

Périphériques

Les administrateurs accèdent aux fonctionnalités des appareils depuis la console par la définition de restrictions d'appareil, la configuration et l'envoi de notifications aux appareils, l'administration des applications sur les appareils, et ainsi de suite.

Effacer un appareil	Permet d'effacer toutes les données et applications d'un appareil, y compris des cartes mémoire si l'appareil en est doté.
Effacer la restriction	Permet de supprimer une ou plusieurs restrictions.
Effacer les données d'entreprise d'un appareil	Permet d'effacer toutes les données et applications d'entreprise d'un appareil, sans toucher aux données et applications personnelles.
Afficher la localisation	Permet d'afficher l'emplacement géographique et définir des restrictions sur un appareil. Inclut : Localiser un appareil, Voir l'emplacement d'un appareil, Suivre un appareil, Suivre l'emplacement d'un appareil au fil du temps.

Lock device	Permet de verrouiller à distance un appareil de façon à ce que les utilisateurs ne puissent pas utiliser l'appareil.
Unlock device	Permet de déverrouiller à distance un appareil de façon à ce que les utilisateurs puissent utiliser l'appareil.
Verrouiller le conteneur	Permet de verrouiller à distance le conteneur d'entreprise sur un appareil.
Déverrouiller le conteneur	Permet de déverrouiller à distance le conteneur d'entreprise sur un appareil.
Réinitialiser le mot de passe du conteneur	Permet de réinitialiser le mot de passe du conteneur d'entreprise.
Activer contournement du verrouillage d'activation DEP ASM	Stocke un code de contournement sur un appareil iOS supervisé lorsque le verrouillage d'activation est activé. Si vous avez besoin d'effacer l'appareil, utilisez ce code pour annuler automatiquement le verrouillage d'activation.
Appeler l'appareil	Permet d'appeler à distance un appareil Windows à plein volume pendant 5 minutes.
Redémarrer l'appareil	Permet de redémarrer les appareils Windows à partir de la console XenMobile.
Déployer vers un appareil	Permet d'envoyer des applications, des notifications, des restrictions, et ainsi de suite à un appareil.
Modifier un appareil	Permet de modifier les paramètres sur l'appareil.
Notification vers un appareil	Permet d'envoyer une notification à un appareil.
Ajouter/Supprimer un appareil	Permet d'ajouter ou de supprimer des appareils dans XenMobile.
Importer des appareils	Permet d'importer un groupe d'appareils depuis un fichier vers XenMobile.

Exporter la liste des appareils	Permet de collecter des informations sur les appareils à partir de la page Appareil et de les exporter vers un fichier .csv.
Révoquer un appareil	Permet d'empêcher un appareil de se connecter à XenMobile.
Mode kiosque	Permet de refuser l'accès à toutes les applications sur un appareil. Sur Android, les utilisateurs ne peuvent pas se connecter à XenMobile. Sur iOS, les utilisateurs peuvent se connecter, mais ils ne peuvent pas accéder aux applications.
Effacement des applications	Sur Android, cette action supprime le compte XenMobile de l'utilisateur. Sur iOS, cette action supprime les clés de cryptage dont les utilisateurs ont besoin d'accéder aux fonctionnalités de XenMobile.
Voir l'inventaire logiciel	Permet de voir quels logiciels sont installés sur un appareil.
Demander la mise en miroir AirPlay	Permet de démarrer le streaming AirPlay.
Arrêter la mise en miroir AirPlay	Permet d'arrêter le streaming AirPlay.
Activer le mode perdu	Sous **Gérer > Appareils**, vous pouvez placer un appareil supervisé en mode perdu pour le bloquer sur l'écran de verrouillage. Le mode perdu vous permet également de localiser l'appareil en cas de perte ou de vol.
Désactiver le mode perdu	Sous **Gérer > Appareils**, vous pouvez désactiver le mode perdu pour un appareil.
Mise à jour de l'OS de l'appareil	Vous pouvez déployer une stratégie Contrôler mise à jour d'OS sur les appareils.
Arrêter l'appareil	Permet d'arrêter les appareils iOS à partir de la console XenMobile.
Redémarrer l'appareil	Permet de redémarrer les appareils iOS à partir de la console XenMobile.

Utilisateurs et groupes locaux

Les administrateurs gèrent les utilisateurs locaux et les groupes d'utilisateurs locaux sur la page **Gérer > Utilisateurs** dans XenMobile.

Ajouter des utilisateurs locaux
Supprimer des utilisateurs locaux
Modifier un utilisateur local
Importer des utilisateurs locaux
Exporter un utilisateur local
Groupes d'utilisateurs locaux
Obtenir l'ID de verrouillage de l'utilisateur local
Supprimer verrouillage de l'utilisateur local

Inscription

Les administrateurs peuvent ajouter et supprimer des invitations d'inscription, envoyer des notifications aux utilisateurs et exporter la table d'inscription vers un fichier .csv.

Ajouter/supprimer inscription	Permet d'ajouter ou de supprimer une invitation d'inscription à un utilisateur ou un groupe d'utilisateurs.
Notifier un utilisateur	Permet d'envoyer une invitation d'inscription à un utilisateur ou un groupe d'utilisateurs.
Exporter la table d'invitation d'inscription	Permet de collecter des informations d'inscription à partir de la page Inscription et de les exporter vers un fichier .csv.

Stratégies

Ajouter/Supprimer une stratégie	Permet d'ajouter ou de supprimer une stratégie d'appareil ou d'application.
Modifier une stratégie	Permet de modifier une stratégie d'appareil ou d'application.
Charger la stratégie	Permet de charger une stratégie d'appareil ou d'application.
Cloner la stratégie	Permet de copier une stratégie d'appareil ou d'application.
Désactiver la stratégie	Permet de désactiver une stratégie d'application existante.
Exporter la stratégie	Permet de collecter des informations sur une stratégie à partir de la page Stratégies d'appareil et de les exporter vers un fichier .csv.
Attribuer la stratégie	Permet d'attribuer une stratégie d'appareil à un ou plusieurs groupes de mise à disposition.

Application

Les administrateurs gèrent plusieurs applications sur la page **Configurer > Applications** dans XenMobile.

Ajouter/supprimer un magasin d'applications ou une application d'entreprise	Permet d'ajouter ou de supprimer une application de magasin d'applications public ou une application d'entreprise (non compatible avec MDX).
Modifier un magasin d'applications ou une application d'entreprise	Permet de modifier une application de magasin d'applications publiques ou une application d'entreprise (non MDX).
Ajouter/supprimer une application MDX, Web et SaaS	Permet d'ajouter ou de supprimer une application MDX, une application de votre réseau interne (application Web) ou une application d'un réseau public (SaaS) à XenMobile.

Modifier une application MDX, Web et SaaS	Permet de modifier une application MDX, une application de votre réseau interne (application Web) ou une application d'un réseau public (SaaS) à XenMobile.
Ajouter/supprimer une catégorie	Permet d'ajouter ou de supprimer une catégorie dans laquelle les applications peuvent s'afficher dans le XenMobile Store.
Attribuer une application publique/d'entreprise à un groupe de mise à disposition	Permet d'attribuer une application de magasin d'applications public ou une application MDX à un groupe de mise à disposition pour le déploiement.
Attribuer une application MDX/WebLink/SaaS à un groupe de mise à disposition	Permet d'attribuer à un groupe de mise à disposition une application MDX, ne nécessitant pas d'authentification unique (WebLink) ou provenant d'un réseau public (SaaS).
Exporter la liste des applications	Permet de collecter des informations sur les applications à partir de la page Application et de les exporter vers un fichier .csv.

Média

Permet de gérer le contenu multimédia obtenu à partir d'un magasin d'applications public ou via une licence d'achat en volume.

Ajouter/supprimer livres App Store ou d'entreprise
Attribuer des livres publics/d'entreprise à un groupe de mise à disposition
Modifier livres App Store ou d'entreprise

Action

Ajouter/supprimer une action	Permet d'ajouter ou de supprimer une action qui est définie par un déclencheur (événement, appareil ou propriété utilisateur, ou nom de l'application installée) et la réponse associée.
Modifier action	Permet de modifier une action qui est définie par un déclencheur (événement, appareil ou propriété utilisateur, ou nom de l'application installée) et la réponse associée.
Attribuer une action à un groupe de mise à disposition	Permet d'attribuer une action à un groupe de mise à disposition pour le déploiement vers les appareils d'utilisateurs.
Exporter action	Permet de collecter des informations sur une action à partir de la page Actions et de les exporter vers un fichier .csv.

Groupe de mise à disposition

Les administrateurs gèrent les groupes de mise à disposition à partir de la page **Configurer > Groupes de mise à disposition**.

Ajouter/supprimer un groupe de mise à disposition	Permet de créer ou de supprimer un groupe de mise à disposition, ce qui ajoute les utilisateurs spécifiés et les stratégies, les applications et les actions facultatives.
Modifier un groupe de mise à disposition	Permet de modifier un groupe de mise à disposition, ce qui modifie les utilisateurs et les stratégies, les applications et les actions facultatives.
Déployer un groupe de mise à disposition	Permet de distribuer un groupe de mise à disposition.
Exporter un groupe de mise à disposition	Permet de collecter des informations sur un groupe de mise à disposition à partir de la page Groupe de mise à disposition et de les exporter vers un fichier .csv.

Profil d'inscription

Permet de gérer les profils d'inscription.

Ajouter/supprimer profil d'inscription
Modifier le profil d'inscription
Attribuer profil d'inscription à un groupe de mise à disposition

Paramètres

Les administrateurs configurent divers paramètres sur les pages **Paramètres**.

RBAC	Attribution d'un rôle RBAC, Attribuer des rôles. **Important :** cette autorisation donne aux administrateurs un accès complet, y compris la possibilité d'attribuer leurs propres autorisations. Accordez cet accès uniquement aux utilisateurs auxquels vous avez l'intention de donner la possibilité de manipuler tout ce qui se trouve dans le système Endpoint Management.
LDAP	Permet de gérer un ou plusieurs annuaires compatibles LDAP, tels que Active Directory, pour importer des groupes, comptes d'utilisateurs et propriétés associées.
Licence	Pour XenMobile Server sur site. Permet de gérer vos licences Citrix.
Inscription	Permet d'activer des modes d'inscription sécurisée pour les utilisateurs ainsi que le portail en libre-service.
Gestion des versions	Permet d'afficher la version installée. Inclut : Mise à jour de la gestion des versions
Certificats	Modifier le certificat APNS, Certificats d'écoute SSL

Modèles de notification	Permet de créer des modèles de notification à utiliser dans les actions automatisées, l'inscription et la remise de messages de notification standard aux utilisateurs.
Workflows	Permet de gérer la création, l'approbation et la suppression des comptes d'utilisateur à utiliser avec les configurations d'application.
Fournisseurs d'informations d'identification	Permet d'ajouter un ou plusieurs fournisseurs d'informations d'identification autorisés à émettre des certificats d'appareil. Les fournisseurs d'informations d'identification contrôlent le format du certificat et les conditions de renouvellement ou de révocation du certificat.
Entités PKI	Permet de gérer les entités d'infrastructure de clé publique (générique, Services de certificats Microsoft ou autorité de certification discrétionnaire).
Tester la connexion PKI	Permet d'utiliser le bouton Tester la connexion sur la page **Paramètres > Entités PKI** pour vous assurer que le serveur est accessible.
Propriétés du client	Permet de gérer les différentes propriétés sur les appareils d'utilisateur, telles que le type de code secret, le niveau de sécurité ou la date d'expiration.
Support client	Permet de définir la méthode utilisée par les utilisateurs pour contacter votre service d'assistance (messagerie, téléphone ou ticket d'assistance).
Personnalisation du client	Personnalisez le nom du magasin et les vues de magasin par défaut du XenMobile Store. Permet d'ajouter un logo personnalisé qui s'affiche sur XenMobile Store ou Secure Hub.

Passerelle SMS opérateur	Permet de configurer des passerelles SMS d'opérateur pour configurer les notifications que XenMobile envoie via les passerelles SMS d'opérateur.
Serveur de notification	Permet de définir un serveur de passerelle SMTP pour envoyer des e-mails aux utilisateurs.
ActiveSync Gateway	Permet de gérer l'accès des utilisateurs à des utilisateurs et à des appareils à l'aide de règles et de propriétés.
Programme de déploiement d'Apple	Ajoutez un compte de programme de déploiement Apple à XenMobile.
Inscription d'appareils dans Apple Configurator	Permet de configurer les paramètres d'Apple Configurator dans XenMobile.
Paramètres d'achat en volume/iOS	Permet d'ajouter des comptes d'achat en volume d'Apple.
Fournisseur de services mobiles	Permet d'utiliser l'interface du fournisseur de services mobiles pour interroger des appareils BlackBerry et d'autres appareils Exchange ActiveSync et d'effectuer des opérations d'émission.
Citrix Gateway	Pour XenMobile Server sur site. Ajoutez une instance Citrix Gateway. Choisissez si vous souhaitez activer l'authentification et si vous souhaitez distribuer le certificat utilisateur pour l'authentification. Choisissez un fournisseur d'identités.
Contrôle d'accès réseau	Permet de définir les conditions qui déterminent si un appareil est non compatible et par conséquent s'il n'a pas accès au réseau.
Samsung Knox	Permet d'activer ou de désactiver l'interrogation par XenMobile des API REST du serveur d'attestation Samsung Knox.

Propriétés du serveur	Permet d'ajouter ou de modifier des propriétés de serveur. Requiert le redémarrage de XenMobile sur tous les nœuds.
Syslog	Pour XenMobile Server sur site. Permet d'envoyer des fichiers journaux à un serveur syslog à l'aide du nom d'hôte ou de l'adresse IP du serveur.
XenApp et XenDesktop	Autorise les utilisateurs à ajouter Virtual Apps and Desktops via Secure Hub.
Citrix Files	Lors de l'utilisation de XenMobile avec des comptes Enterprise : configurez les paramètres pour la connexion au compte Content Collaboration et au compte de service d'administrateur afin de gérer les comptes utilisateur. Requiert des informations d'identification d'administrateur et de domaine Citrix Files. Lors de l'utilisation de XenMobile avec des connecteurs StorageZone : permet de configurer XenMobile pour pointer vers les partages réseau et les emplacements SharePoint définis dans les connecteurs StorageZones.
Programme d'amélioration de l'expérience	Pour XenMobile Server sur site. Permet de participer ou non à l'envoi d'informations d'utilisation et de statistiques anonymes à Citrix.
Microsoft Azure	Pour XenMobile Server sur site. Intégrez XenMobile avec Microsoft Azure.
Android Entreprise	Permet de configurer les paramètres de serveur Android Enterprise.
Fournisseur d'identité (IdP)	Permet de configurer un fournisseur d'identité.
XenMobile Tools	Permet d'accéder à la page XenMobile Tools.

Configuration de SNMP	Activez SNMP pour les nœuds de XenMobile Server. Modifiez ou ajoutez des utilisateurs de surveillance, configurez le gestionnaire SNMP sur lequel les notifications trap s'affichent et configurez des seuils et des intervalles de trap.

Support

Les administrateurs peuvent effectuer diverses tâches de support.

Test de la connectivité Citrix Gateway	Permet de tester la connectivité de Citrix Gateway par adresse IP. Requiert un nom d'utilisateur et un mot de passe.
Contrôles de connectivité dans XenMobile	Permet de tester la connectivité de certaines fonctionnalités XenMobile, telles que la base de données, DNS ou Google Plan.
Créer des packs d'assistance	Pour XenMobile Server sur site. Créez un fichier à envoyer à l'assistance Citrix pour la résolution des problèmes. Contient les informations système, les journaux, les informations de base de données, les informations principales, les fichiers de trace et les dernières informations de configuration de XenMobile ou Citrix Gateway.
Documentation Produit Citrix	Permet d'accéder au site de documentation Citrix XenMobile public.
Centre de connaissances de Citrix	Permet d'accéder au site d'assistance de Citrix pour rechercher des articles de la base de connaissances.
Journaux	Permet d'afficher et d'analyser les informations des fichiers journaux de débogage, d'audit administrateur et d'audit utilisateur.

Informations de cluster	Pour XenMobile Server sur site. Permet d'accéder à des informations sur chaque nœud dans un environnement en cluster.
Nettoyage de la mémoire	Pour XenMobile Server sur site. Permet d'accéder à des informations sur les objets de la mémoire inutilisés.
Propriétés de la mémoire Java	Pour XenMobile Server sur site. Permet d'accéder à un résumé de l'utilisation de la mémoire Java, des détails de la mémoire et des détails du pool de mémoires.
Macros	Permet de remplir les données de propriété d'appareil ou d'utilisateur dans le champ textuel d'un profil, d'une stratégie, d'une notification ou d'un modèle d'inscription. Configurez une stratégie et déployez-la auprès d'un grand nombre d'utilisateurs et de manière à ce que des valeurs spécifiques à l'utilisateur s'affichent pour chaque utilisateur ciblé.
Configuration PKI	Permet d'importer et d'exporter des informations de configuration d'infrastructure de clé publique (PKI).
Utilitaire de signature APNs	Permet d'envoyer une demande de certificats APNS ou de télécharger un certificat APNS Secure Mail pour iOS.
Citrix Insight Services	Permet de charger des journaux sur Citrix Insight Services (CIS) pour obtenir de l'aide avec divers problèmes.
État d'un appareil envoyé à Citrix Gateway Connector pour Exchange ActiveSync	Permet d'effectuer une requête auprès de XenMobile pour connaître l'état d'un appareil tel qu'envoyé à Citrix Gateway Connector pour Exchange ActiveSync en fonction de l'ID ActiveSync de l'appareil.

Anonymisation et réidentification	Pour XenMobile Server sur site. Lorsque vous créez des packs d'assistance dans XenMobile, les données sensibles liées aux utilisateurs, serveurs et réseaux sont rendues anonymes par défaut. Vous pouvez modifier ce comportement dans **Support > Anonymisation et réidentification** sous **Avancé**.
Paramètres du journal	Personnalisez le niveau de journalisation ou ajoutez un enregistreur d'événements.

Restreindre l'accès aux groupes

Les utilisateurs de niveau administrateur peuvent appliquer des autorisations à tous les groupes d'utilisateurs.

Rôle de provisioning d'appareils

> **Important :**
>
> Le rôle Provisioning d'appareils s'applique uniquement aux appareils Windows CE.

Les utilisateurs disposant du rôle Provisioning d'appareils prédéfini ont un accès limité aux fonctionnalités de la console. Par défaut, leur autorisation est définie pour tous les groupes d'utilisateurs et ils ne peuvent pas modifier ce paramètre.

Fonctionnalités de la console

Les utilisateurs avec le rôle Provisioning d'appareils ont l'accès limité suivant à la console XenMobile. Par défaut, les fonctionnalités suivantes sont activées.

Périphériques

Modifier un appareil	Permet de modifier les paramètres sur l'appareil.

Ajouter/Supprimer un appareil	Permet d'ajouter ou de supprimer des appareils dans XenMobile.

Paramètres

Les utilisateurs du provisioning d'appareils peuvent accéder à la page **Paramètres**, mais ils ne sont pas autorisés à configurer les fonctionnalités.

Rôle Support

Les utilisateurs disposant du rôle Support ont accès au support à distance. Leurs autorisations s'appliquent à tous les utilisateurs par défaut et ils ne peuvent pas modifier ce paramètre.

Rôle Utilisateur

Les utilisateurs avec le rôle Utilisateur disposent de l'accès limité suivant à XenMobile.

Accès autorisé

Portail en libre-service	Les utilisateurs ont seulement accès à la console du portail d'assistance (en libre-service) dans XenMobile.

Fonctionnalités de la console

Les utilisateurs ont l'accès limité suivant à la console XenMobile.

Périphériques

Effacer un appareil	Permet d'effacer toutes les données et applications d'un appareil, y compris des cartes mémoire si l'appareil en est doté.

Effacer les données d'entreprise d'un appareil	Permet d'effacer toutes les données et applications d'entreprise d'un appareil, sans toucher aux données et applications personnelles.
Afficher la localisation	Permet d'afficher l'emplacement géographique et définir des restrictions sur un appareil. Inclut : Localiser un appareil, Voir l'emplacement d'un appareil, Suivre un appareil, Suivre l'emplacement d'un appareil au fil du temps.
Lock device	Permet de verrouiller à distance un appareil de façon à ce qu'il ne puisse pas être utilisé.
Unlock device	Permet de déverrouiller à distance un appareil de façon à ce qu'il puisse être utilisé.
Verrouiller le conteneur	Permet de verrouiller à distance le conteneur d'entreprise sur un appareil.
Déverrouiller le conteneur	Permet de déverrouiller à distance le conteneur d'entreprise sur un appareil.
Réinitialiser le mot de passe du conteneur	Permet de réinitialiser le mot de passe du conteneur d'entreprise.
Activer contournement du verrouillage d'activation DEP ASM	Stocke un code de contournement sur un appareil iOS supervisé lorsque le verrouillage d'activation est activé. Si vous avez besoin d'effacer l'appareil, utilisez ce code pour annuler automatiquement le verrouillage d'activation.
Appeler l'appareil	Permet d'appeler à distance un appareil Windows à plein volume pendant 5 minutes.
Redémarrer l'appareil	Permet de redémarrer un appareil Windows.
Voir l'inventaire logiciel	Permet de voir quels logiciels sont installés sur un appareil.

Inscription

Ajouter/supprimer inscription	Permet d'ajouter ou de supprimer une invitation d'inscription à un utilisateur ou un groupe d'utilisateurs.
Notifier un utilisateur	Permet d'envoyer une invitation d'inscription à un utilisateur ou un groupe d'utilisateurs.

Restreindre l'accès aux groupes

Pour les quatre rôles par défaut, cette autorisation est définie par défaut et peut être appliquée à tous les groupes d'utilisateurs. Vous ne pouvez pas modifier le rôle.

Configurer des rôles avec RBAC

La fonctionnalité de contrôle d'accès basé sur rôle (RBAC) de XenMobile vous permet d'attribuer des rôles prédéfinis ou un ensemble d'autorisations aux utilisateurs et aux groupes. Ces autorisations contrôlent le niveau d'accès des utilisateurs aux fonctions du système.

XenMobile implémente quatre rôles utilisateur par défaut de façon à séparer logiquement l'accès aux fonctions système :

- **Administrateur :** accorde un accès complet au système.
- **Provisioning d'appareils :** accorde un accès à l'administration de base des appareils pour les appareils Windows CE.
- **Assistance :** accorde l'accès à l'assistance à distance.
- **Utilisateur :** utilisé par les utilisateurs autorisés à inscrire des appareils et à accéder au portail en libre-service.

Vous pouvez également utiliser les rôles par défaut en tant que modèles que vous personnalisez pour créer des rôles utilisateur. Vous pouvez attribuer les autorisations de rôles pour un accès à des fonctions système spécifiques au-delà des fonctions définies par les rôles par défaut.

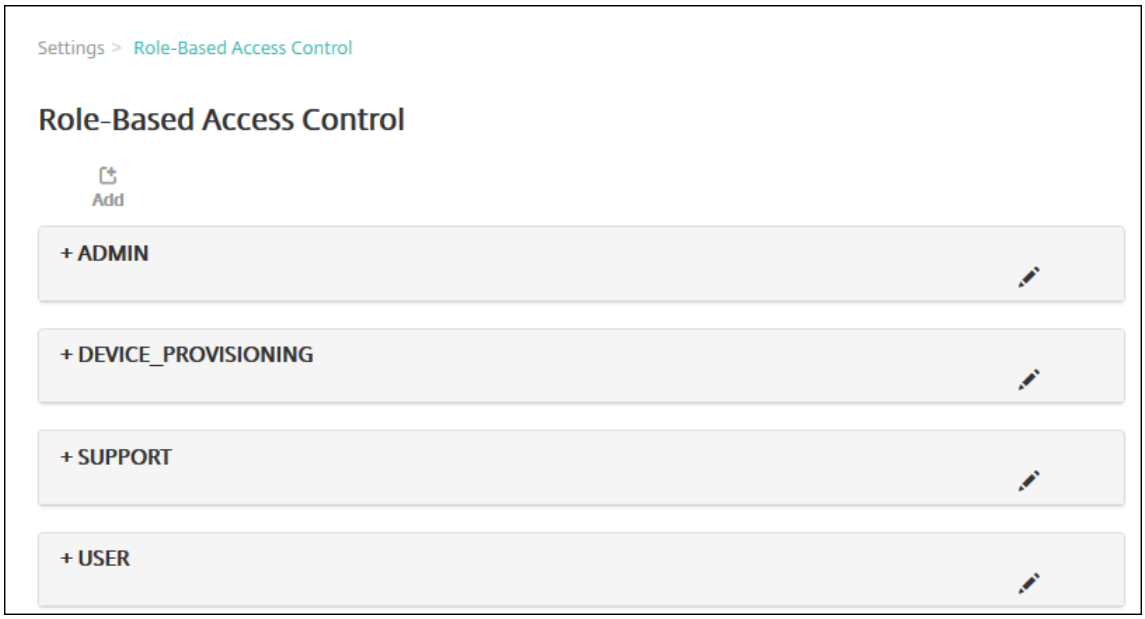
Les rôles peuvent être attribués à des utilisateurs locaux (au niveau de l'utilisateur) ou à des groupes Active Directory (tous les utilisateurs de ce groupe ont les mêmes autorisations). Si un utilisateur appartient à plusieurs groupes Active Directory, les autorisations sont fusionnées pour définir les autorisations de cet utilisateur. Par exemple, supposons que les utilisateurs d'ADGroupA puissent localiser les appareils des responsables et que les utilisateurs d'ADGroupB puissent effacer les appareils des employés. Dans ce cas, un utilisateur appartenant aux deux groupes peut localiser et effacer les appareils des responsables et des employés.

> **Remarque :**
>
> Un seul rôle peut être attribué aux utilisateurs locaux.

Vous pouvez utiliser la fonctionnalité RBAC dans XenMobile pour effectuer les opérations suivantes :

- Créer un rôle.
- Ajouter des groupes à un rôle.
- Associer des utilisateurs locaux aux rôles.

1. Dans la console XenMobile, accédez à **Paramètres > Contrôle d'accès basé sur rôle**. La page **Contrôle d'accès basé sur rôle** qui apparaît affiche les quatre rôles utilisateur par défaut, ainsi que tout rôle que vous avez déjà ajouté.



   si vous cliquez sur le signe plus (+) à côté d'un rôle, celui-ci se développe pour afficher toutes les autorisations pour ce rôle, comme illustré dans la figure suivante.

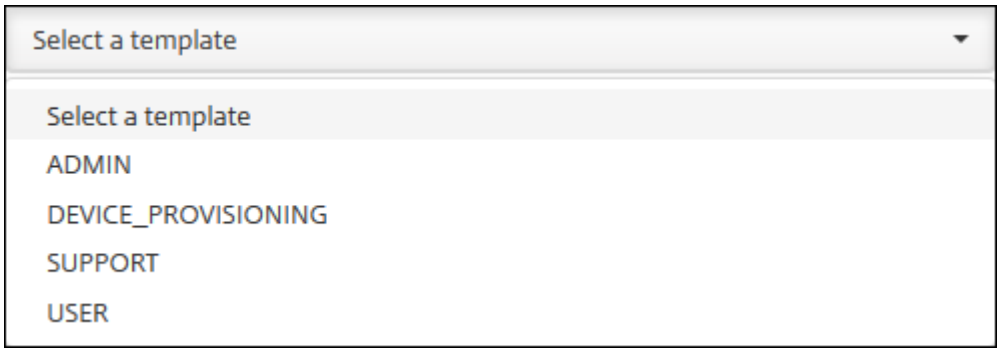
2. Cliquez sur **Ajouter** pour ajouter un nouveau rôle d'utilisateur. Cliquez sur l'icône de crayon à droite d'un rôle existant pour modifier le rôle. Pour supprimer le rôle, cliquez sur l'icône de la corbeille située à droite d'un rôle. Vous ne pouvez pas supprimer les rôles utilisateur par défaut.

- Lorsque vous cliquez sur **Ajouter** ou l'icône de crayon, la page **Ajouter un rôle** ou **Modifier le rôle** s'affiche.
- Lorsque vous cliquez sur l'icône de corbeille, une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer le rôle sélectionné.

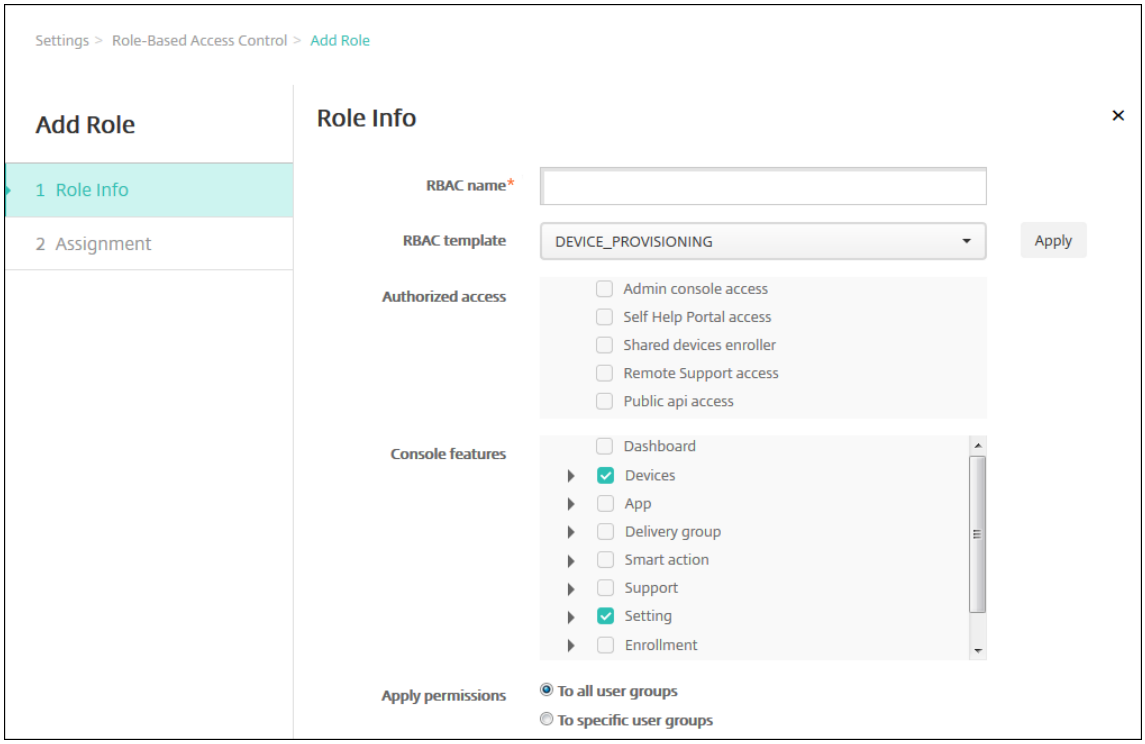
3. Entrez les informations suivantes pour créer modifier un rôle utilisateur :

   - **Nom RBAC :** entrez un nom descriptif pour le nouveau rôle utilisateur. Vous ne pouvez pas modifier le nom d'un rôle existant.
   - **Modèle RBAC :** si vous le souhaitez, cliquez sur un modèle en tant que point de départ pour le nouveau rôle. Vous ne pouvez pas sélectionner de modèle si vous modifiez un rôle existant.

   Les modèles RBAC sont les rôles utilisateur par défaut. Ils définissent l'accès aux fonctions système dont disposent les utilisateurs associés à ce rôle. Lorsque vous sélectionnez un modèle RBAC, vous pouvez voir toutes les autorisations associées à ce rôle dans les champs **Accès autorisé** et **Fonctionnalités de la console**. L'utilisation d'un modèle est facultative. Vous pouvez sélectionner les options que vous voulez attribuer à un rôle directement dans les champs **Accès autorisé** et **Fonctionnalités de la console**.

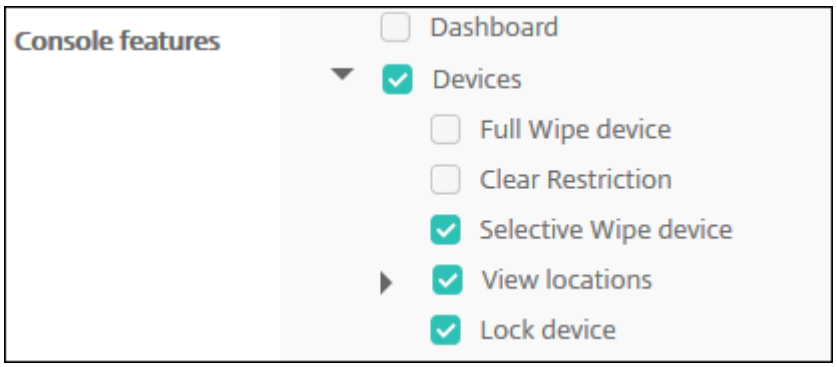


4. Cliquez sur **Appliquer** près du champ **Modèle RBAC** sélectionné pour renseigner **Accès autorisé** et **Fonctionnalités de la console** avec les autorisations d'accès prédéfinies.



5. Sélectionnez et décochez les cases à cocher appropriées dans **Accès autorisé** et **Fonctionnalités de la console** pour personnaliser le rôle.

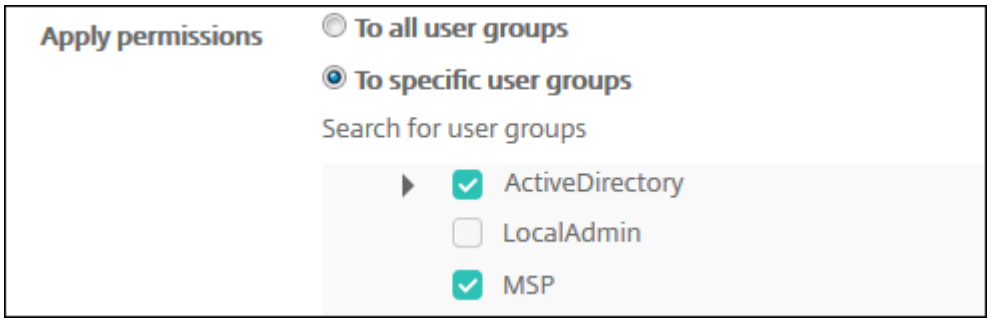
   si vous cliquez sur le triangle à côté de Fonctionnalités de la console, les autorisations spécifiques à cette fonctionnalité s'affichent de façon à ce que vous puissiez les sélectionner ou les désélectionner. Si vous cliquez sur la case à cocher de niveau supérieur, cela interdit l'accès à cette zone de la console. Sélectionnez les options individuelles sous le niveau supérieur pour activer ces options. Par exemple, dans la figure suivante, les options **Effacer un appareil** et **Effacer les restrictions** ne s'affichent pas pour les utilisateurs associés au rôle. Les options cochées apparaissent.



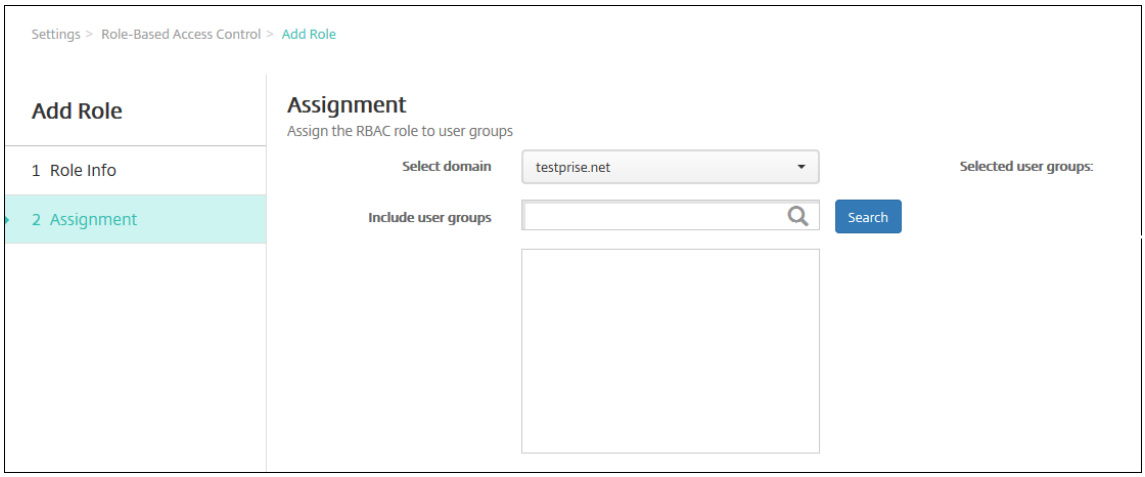
6. **Appliquer les autorisations :** sélectionnez un ou plusieurs groupes d'utilisateurs pour limiter les groupes que l'administrateur peut gérer. Si vous cliquez sur **À des groupes d'utilisateurs spécifiques**, une liste des groupes s'affiche à partir de laquelle vous pouvez sélectionner un ou plusieurs groupes.

Par exemple, si un administrateur RBAC dispose d'autorisations sur les groupes d'utilisateurs ActiveDirectory et MSP :

- L'administrateur ne peut accéder aux informations que pour les utilisateurs qui font partie du groupe ActiveDirectory, du groupe MSP ou des deux groupes.
- L'administrateur ne peut afficher aucun autre utilisateur local ou AD. L'administrateur peut afficher les utilisateurs qui sont membres de groupes enfants de l'un ou l'autre de ces groupes.
- L'administrateur peut envoyer des invitations :
  - aux groupes d'autorisations et à leurs groupes enfants
  - aux utilisateurs qui sont membres des groupes d'autorisations et de leurs groupes enfants



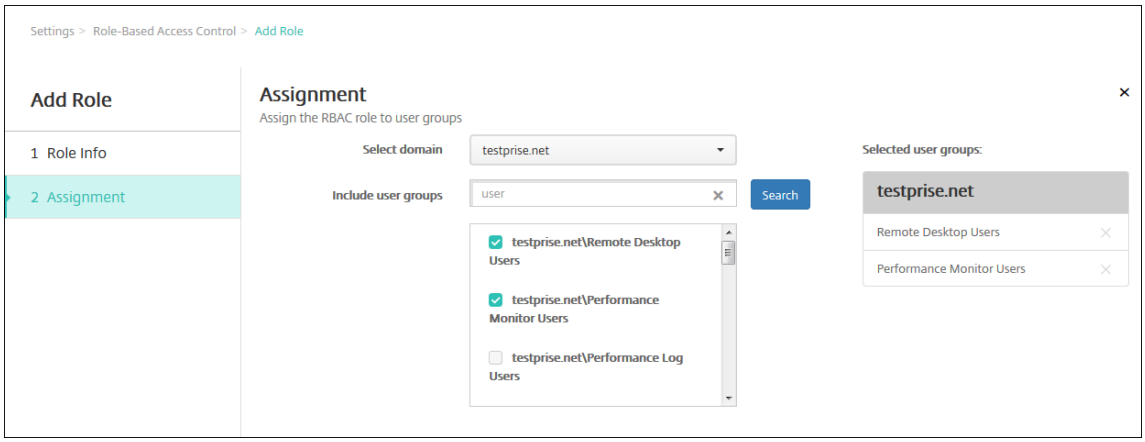
7. Cliquez sur **Suivant**. La page **Attribution** s'affiche.



8. Entrez les informations suivantes pour attribuer le rôle à des groupes d'utilisateurs.

   - **Sélectionner un domaine :** cliquez sur un domaine dans la liste.
   - **Inclure des groupes d'utilisateurs :** cliquez sur Rechercher pour afficher une liste de tous les groupes disponibles, ou tapez un nom de groupe complet ou partiel pour limiter la liste aux groupes portant ce nom.
   - Dans la liste qui s'affiche, sélectionnez les groupes d'utilisateurs auxquels vous souhaitez attribuer le rôle. Lorsque vous sélectionnez un groupe d'utilisateurs, le groupe apparaît

dans la liste **Groupes d'utilisateurs sélectionnés**.



> **Remarque :**
>
> Pour supprimer un groupe d'utilisateurs de la liste **Groupes d'utilisateurs sélectionnés**, cliquez sur le X en regard du nom du groupe d'utilisateurs.

9. Cliquez sur **Enregistrer**.

Notifications

January 10, 2022

Vous pouvez utiliser les notifications dans XenMobile aux fins suivantes :

- Pour communiquer avec des groupes d'utilisateurs sélectionnés à propos d'un certain nombre de fonctions liées au système. Vous pouvez également cibler ces notifications pour certains utilisateurs. Par exemple, tous les utilisateurs équipés d'appareils iOS, les utilisateurs dont les appareils ne sont pas conformes, les utilisateurs équipés d'appareils leur appartenant, etc.
- Pour inscrire les utilisateurs et leurs appareils.
- Pour notifier automatiquement les utilisateurs (via des actions automatisées) lorsque certaines conditions sont remplies. Par exemple :
  - Lorsqu'un appareil utilisateur est sur le point d'être bloqué du domaine d'entreprise en raison d'un problème de conformité.
  - Lorsqu'un appareil a été jailbreaké ou rooté.

Pour de plus amples informations sur les actions automatisées, consultez la section Actions automatisées.

Pour envoyer des notifications avec XenMobile, vous devez configurer une passerelle et un serveur de notification. Vous pouvez configurer un serveur de notification dans XenMobile pour configurer des serveurs de passerelle SMTP et SMS de façon à pouvoir envoyer des notifications sous forme d'e-mails

et de messages texte (SMS) aux utilisateurs. Vous pouvez utiliser les notifications pour envoyer des messages sur deux canaux : SMTP ou SMS.

- SMTP est un protocole basé sur texte orienté connexion, dans lequel un expéditeur communique avec un récepteur de courrier en émettant des chaînes de commande et en fournissant les données nécessaires, généralement via une connexion TCP. Les sessions SMTP se composent de commandes émanant d'un client SMTP (la personne qui envoie le message) et des réponses correspondantes à partir du serveur SMTP.
- SMS est un composant du service de messagerie texte du téléphone, du Web ou de systèmes de communication mobiles. SMS utilise des protocoles de communication standard pour permettre à des téléphones portables ou fixes d'échanger des messages texte courts.

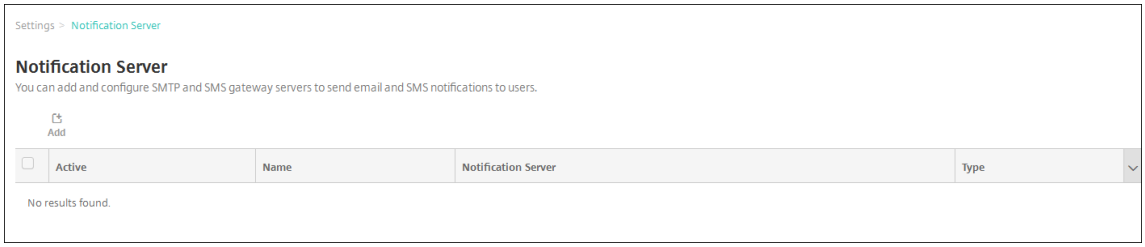
Vous pouvez également définir une passerelle SMS d'opérateur dans XenMobile pour configurer les notifications envoyées via la passerelle SMS d'un opérateur. Les opérateurs utilisent les passerelles SMS pour envoyer ou recevoir des transmissions SMS vers ou à partir d'un réseau de télécommunications. Ces messages texte utilisent des protocoles de communication standard pour permettre à des téléphones portables ou fixes d'échanger des messages texte courts.

Conditions préalables

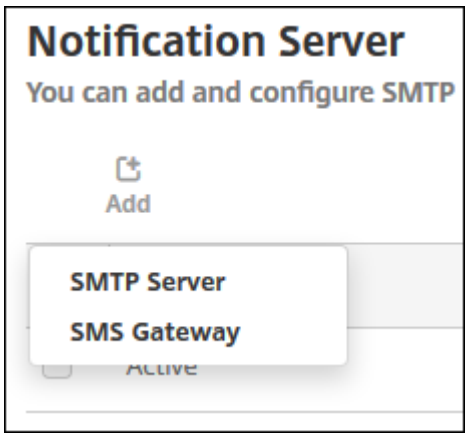
- Avant de configurer la passerelle SMS, consultez votre administrateur système pour déterminer les informations de serveur. Il est important de savoir si le serveur SMS est hébergé sur un réseau d'entreprise interne, ou s'il fait partie d'un service de messagerie hébergé. Dans ce cas, vous aurez besoin des informations du site Web du fournisseur de services.
- Configurez le serveur de notifications SMTP pour envoyer des messages aux utilisateurs. Si le serveur est hébergé sur un serveur interne, contactez votre administrateur système pour obtenir les informations de configuration. Si le serveur est un service de messagerie hébergé, recherchez les informations de configuration appropriées sur le site Web du fournisseur de services.
- Vous pouvez utiliser simultanément un serveur SMTP actif et un serveur SMS actif. Ces deux canaux de communication permettent une configuration active.
- Ouvrez le port 25 depuis XenMobile dans la zone démilitarisée (DMZ) de votre réseau afin de pointer vers le serveur SMTP sur votre réseau interne. Cela permet à XenMobile d'envoyer des notifications avec succès.

Configurer un serveur SMTP et une passerelle SMS

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Notifications**, cliquez sur **Serveur de notification**. La page **Serveur de notification** s'affiche.

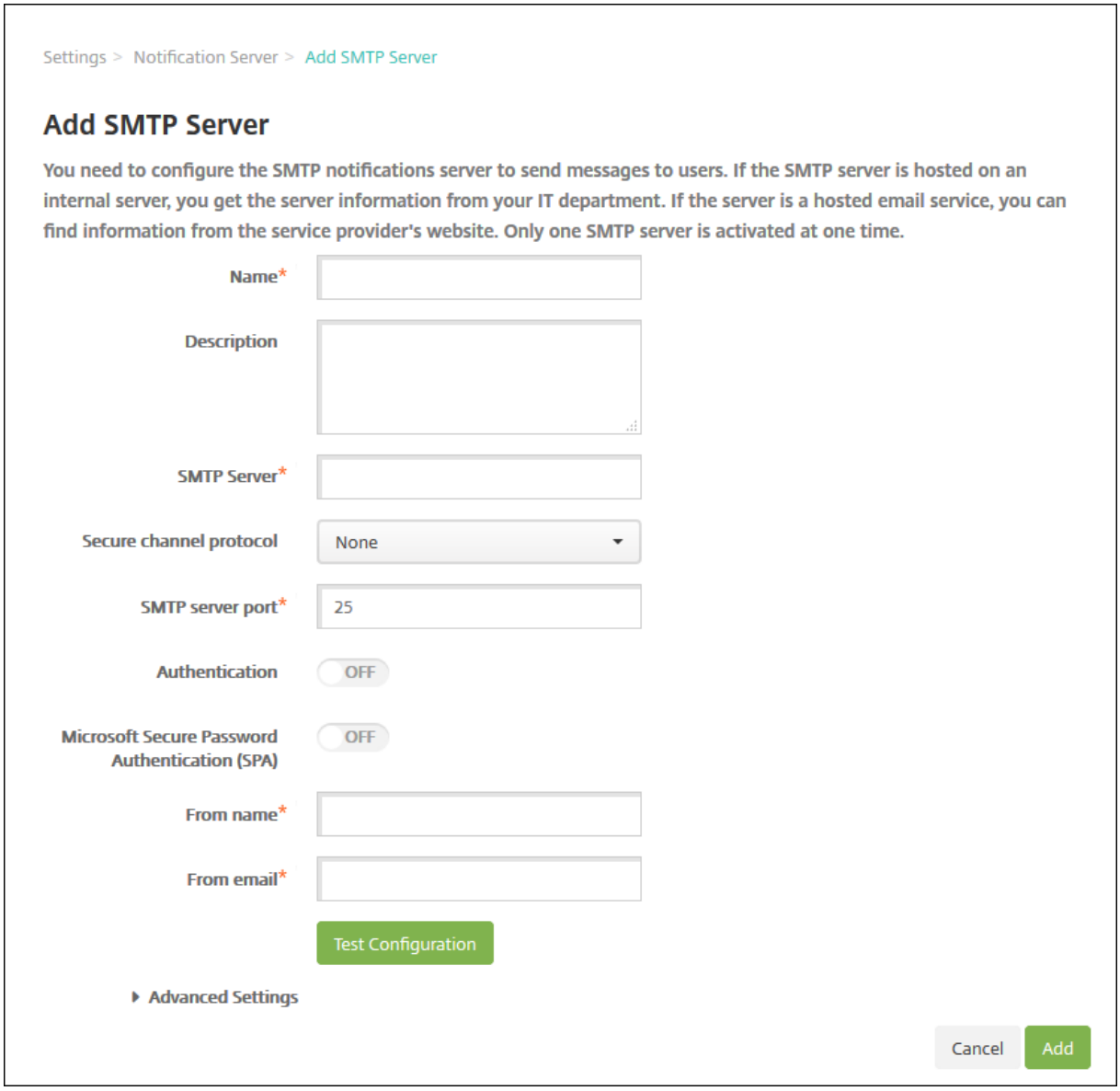


3. Cliquez sur **Ajouter**. Un menu s'affiche avec des options pour configurer un serveur SMTP ou une passerelle SMS.



   - Pour ajouter un serveur SMTP, cliquez sur **Serveur SMTP**, puis consultez la section Pour ajouter un serveur SMTP pour connaître les étapes suivantes.
   - Pour ajouter une passerelle SMS, cliquez sur **Passerelle SMS**, puis consultez la section Pour ajouter une passerelle SMS pour connaître les étapes suivantes.

Ajouter un serveur SMTP



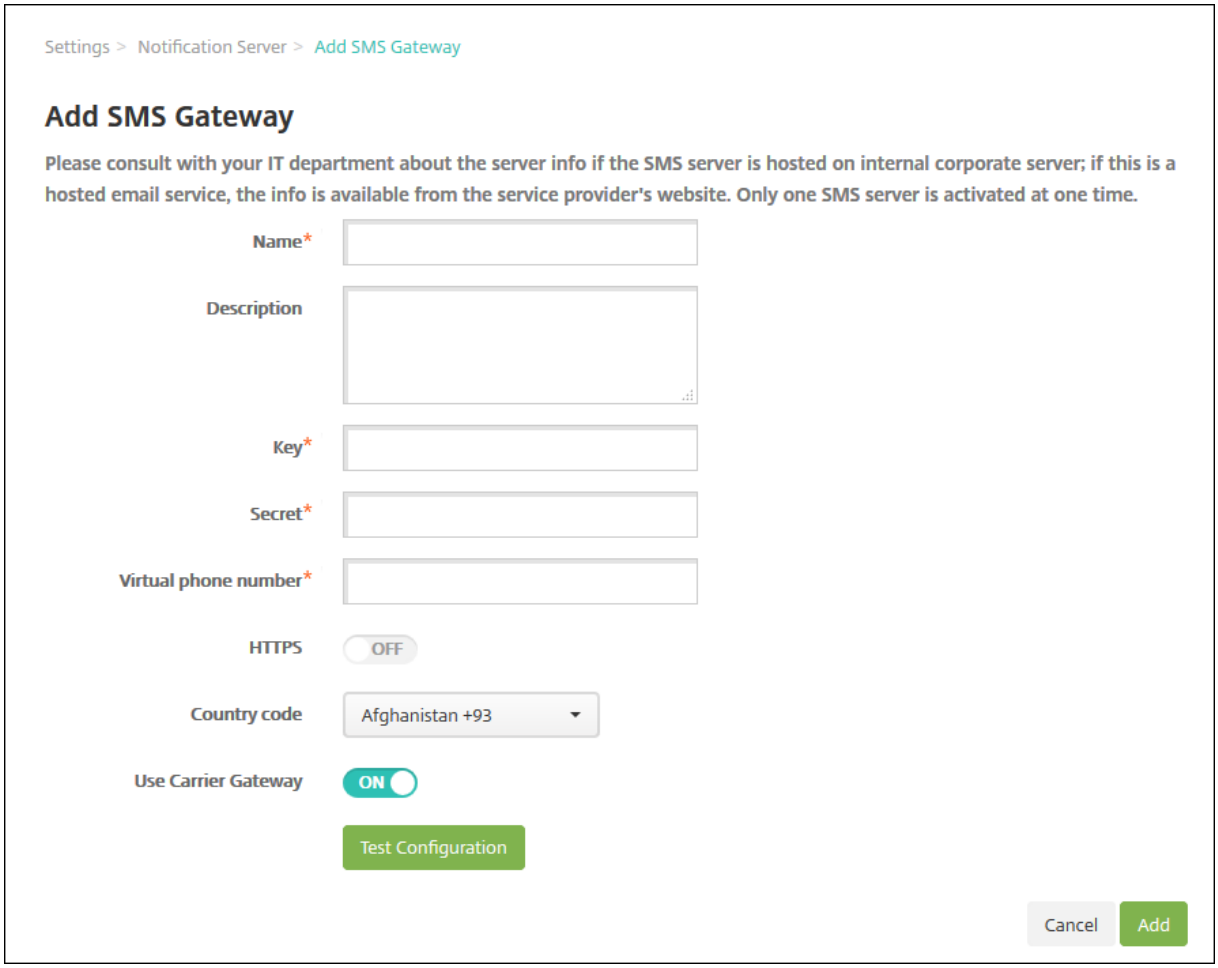
1. Pour configurer ces paramètres :

   - **Nom :** entrez le nom associé à ce compte de serveur SMTP.
   - **Description :** entrez une description pour le serveur (facultatif).
   - **Serveur SMTP :** entrez le nom d'hôte du serveur. Le nom d'hôte peut être un nom de domaine complet (FQDN) ou une adresse IP.
   - **Secure Channel Protocol :** dans la liste, cliquez sur le protocole de canal sécurisé approprié utilisé par le serveur (si le serveur est configuré pour utiliser une authentification sécurisée) : **SSL**, **TLS** ou **Aucun**. La valeur par défaut est **Aucun**.
   - **Port du serveur SMTP :** entrez le port utilisé par le serveur SMTP. Par défaut, le port est défini sur 25 ; si les connexions SMTP utilisent le protocole de canal sécurisé SSL, le port

est défini sur 465.
- **Authentification :** sélectionnez **Activé** ou **Désactivé**. La valeur par défaut est **Désactivé.**
- Si vous avez activé **Authentification**, configurez les paramètres suivants :
  - **Nom d'utilisateur :** entrez un nom d'utilisateur à utiliser pour l'authentification.
  - **Mot de passe :** entrez le mot de passe de l'utilisateur à utiliser pour l'authentification.
- **Authentification par mot de passe sécurisé (SPA) Microsoft :** si le serveur SMTP utilise la SPA, cliquez sur **Activé**. La valeur par défaut est **Désactivé.**
- **Nom expéditeur :** entrez le nom affiché dans la case **De** lorsqu'un client reçoit une notification par e-mail à partir de ce serveur. Par exemple, Département Informatique.
- **E-mail expéditeur :** entrez l'adresse e-mail utilisée si le destinataire d'un e-mail répond à la notification envoyée par le serveur SMTP.

2. Cliquez sur **Tester la configuration** pour envoyer une notification par e-mail test.
3. Développez **Paramètres avancés** et configurez les paramètres suivants :
   - **Nombre d'essais SMTP :** entrez le nombre de tentatives d'envoi d'un message dont l'envoi a échoué à partir du serveur SMTP. La valeur par défaut est 5.
   - **Délai d'attente SMTP :** entrez la durée d'attente (en secondes) lors de l'envoi d'une demande SMTP. Augmentez cette valeur si l'envoi de messages échoue continuellement en raison de l'expiration des délais. Soyez prudent lorsque vous diminuez cette valeur ; cela pourrait augmenter les échecs dus à l'expiration des délais ainsi que le nombre de messages non remis. La durée par défaut est de 30 secondes.
   - **Nombre max de destinataires SMTP :** entrez le nombre maximal de destinataires par message envoyés par le serveur SMTP. La valeur par défaut est 100.
4. Cliquez sur **Ajouter**.

Ajouter une passerelle SMS



Remarque :

XenMobile prend uniquement en charge la messagerie Nexmo SMS. Si vous ne possédez pas de compte pour utiliser la messagerie Nexmo, visitez leur site Web pour en créer un.

1. Configurez les paramètres suivants :
   - **Nom :** entrez un nom pour la configuration de la passerelle SMS. Ce champ est obligatoire.
   - **Description :** entrez une description pour la configuration (facultatif).
   - **Clé :** entrez l'identificateur numérique fourni par l'administrateur système lors de l'activation du compte. Ce champ est obligatoire.
   - **Secret :** entrez un secret fourni par l'administrateur système qui est utilisé pour accéder à votre compte dans le cas où un mot de passe est perdu ou volé. Ce champ est obligatoire.
   - **Numéro de téléphone virtuel :** ce champ est utilisé lors de l'envoi à des numéros de téléphone d'Amérique du Nord (avec le préfixe +1). Vous devez entrer un numéro de téléphone virtuel Nexmo et seuls des chiffres peuvent être utilisés dans ce champ. Vous pouvez acheter des numéros de téléphone virtuels sur le site Web Nexmo.

- **HTTPS :** indiquez si vous souhaitez utiliser le protocole HTTPS pour transmettre des requêtes SMS à Nexmo. La valeur par défaut est **Désactivé.**

> **Important :**
>
> Laissez HTTPS défini sur **Activé** sauf si l'assistance Citrix vous demande de désactiver l'option (**Désactivé**).

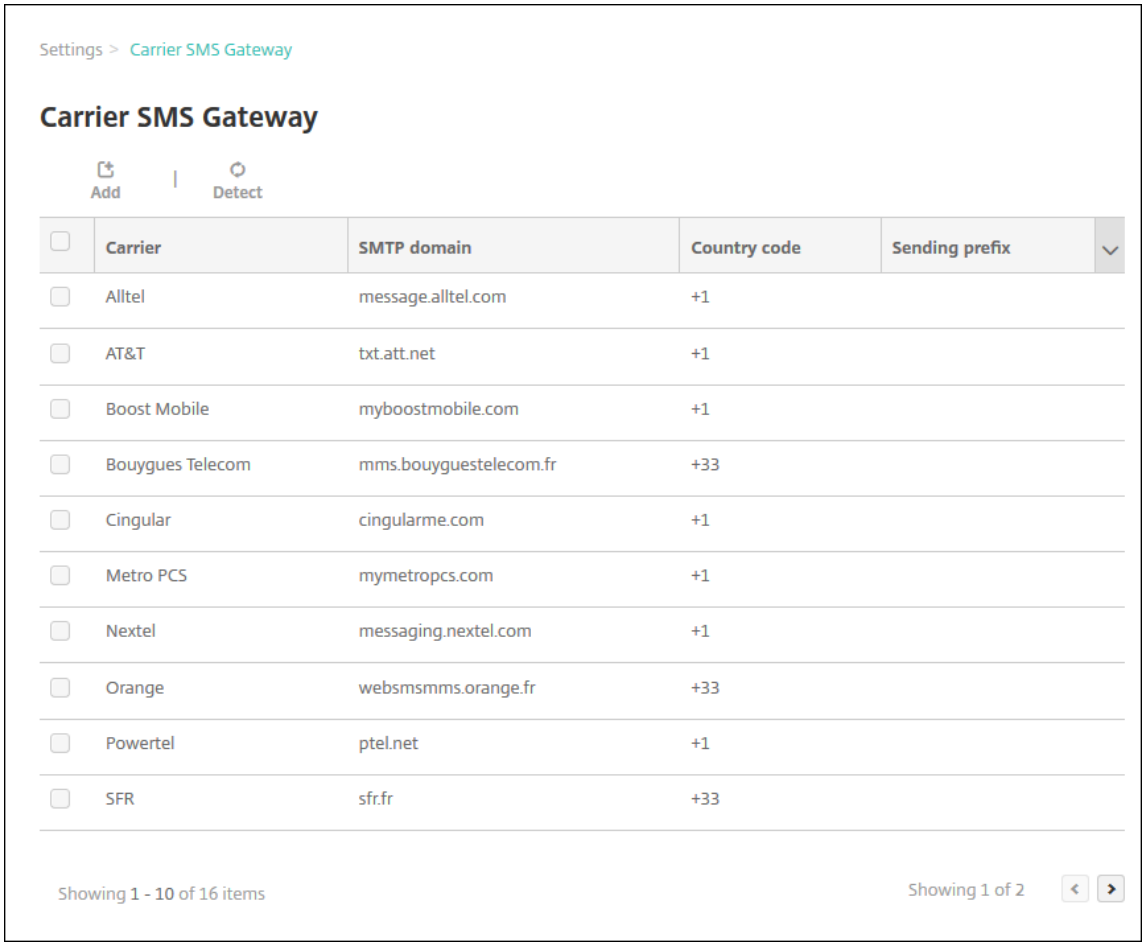
- **Indicatif du pays :** dans la liste, cliquez sur le préfixe d'indicatif du pays SMS par défaut pour les destinataires dans votre organisation. Ce champ commence toujours par un symbole +. La valeur par défaut est **Afghanistan +93**.

2. Cliquez sur **Tester la configuration** pour envoyer un message test à l'aide de la configuration actuelle. Les erreurs de connexion, telles que les erreurs de numéro de téléphone d'authentification ou virtuels, sont détectées et apparaissent immédiatement. Les messages sont reçus dans les mêmes délais que ceux envoyés entre téléphones portables.
3. Cliquez sur **Ajouter**.

Ajouter la passerelle SMS d'un opérateur

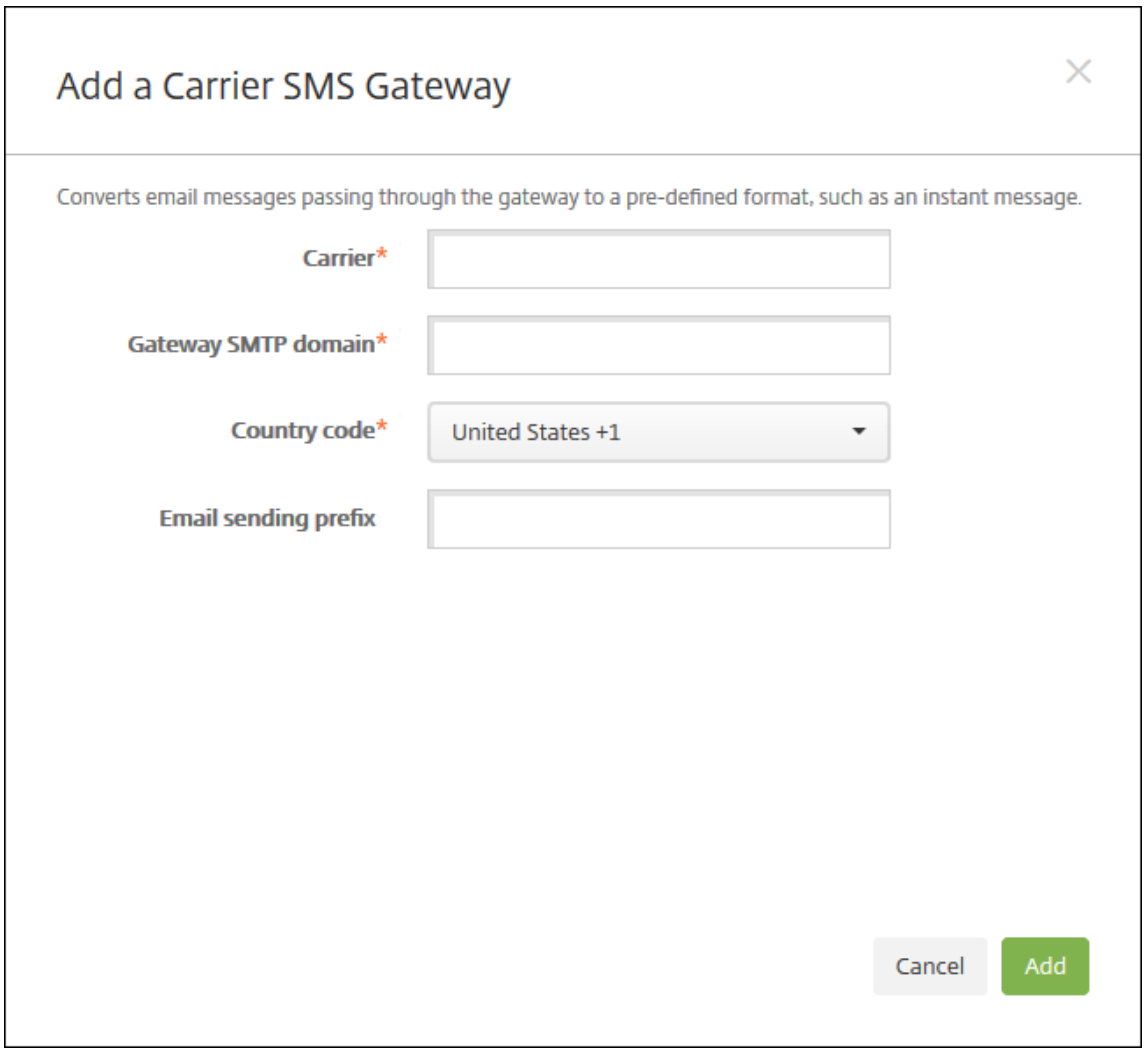
Vous pouvez configurer une passerelle SMS d'opérateur dans XenMobile pour configurer les notifications qui sont envoyées via la passerelle SMS d'un opérateur. Les opérateurs utilisent les passerelles SMS pour envoyer ou recevoir des transmissions SMS vers ou à partir d'un réseau de télécommunications. Ces messages texte utilisent des protocoles de communication standard pour permettre à des téléphones portables ou fixes d'échanger des messages texte courts.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Notifications**, cliquez sur **Passerelle SMS de l'opérateur**. La page **Passerelle SMS de l'opérateur** s'ouvre.



3. Procédez comme suit :

   - Cliquez sur le bouton **Détecter** pour découvrir automatiquement une passerelle. Une boîte de dialogue s'affiche indiquant qu'aucun nouvel opérateur n'a été détecté ou répertoriant les nouveaux opérateurs détectés parmi les appareils inscrits.
   - Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter la passerelle SMS d'un opérateur** apparaît.



> **Remarque :**
>
> XenMobile prend uniquement en charge la messagerie Nexmo SMS. Si vous ne possédez pas de compte pour utiliser la messagerie Nexmo, visitez leur site Web pour en créer un.

4. Pour configurer ces paramètres :
   - **Opérateur :** entrez le nom de l'opérateur.
   - **Domaine SMTP de la passerelle :** entrez le domaine associé à la passerelle SMTP.
   - **Indicatif du pays :** dans la liste, cliquez sur l'indicatif de pays pour l'opérateur.
   - **Préfixe d'envoi d'e-mail :** si vous le souhaitez, vous pouvez spécifier un préfixe pour l'envoi d'e-mail.
5. Cliquez sur **Ajouter** pour ajouter le nouvel opérateur ou cliquez sur **Annuler** pour ne pas ajouter le nouvel opérateur.

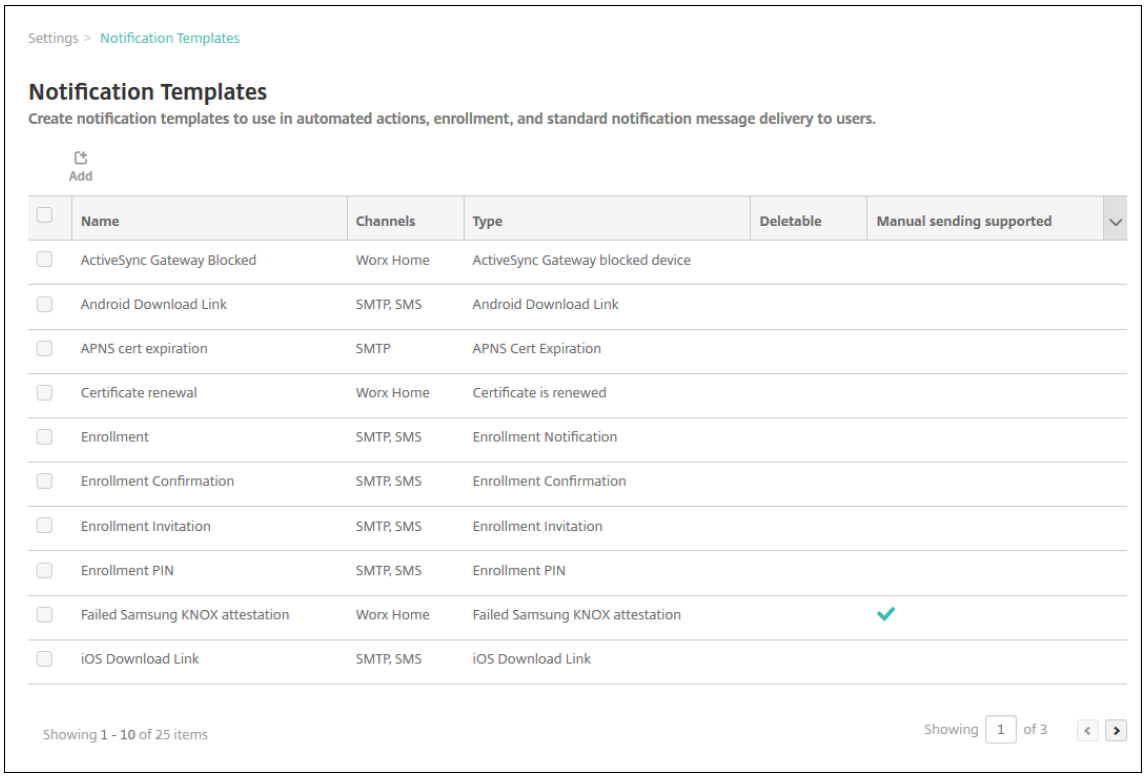
Créer et mettre à jour des modèles de notification

Vous pouvez créer ou mettre à jour des modèles de notification dans XenMobile à utiliser dans les actions automatisées, l'inscription, et les messages de notifications standard envoyés aux utilisateurs. Vous configurez les modèles de notification pour l'envoi de messages sur trois canaux différents : Secure Hub, SMTP ou SMS.

XenMobile comprend plusieurs modèles de notification prédéfinis qui reflètent les différents types d'événements auxquels XenMobile répond automatiquement pour chaque appareil dans le système.

> **Remarque :**
>
> Si vous prévoyez d'utiliser les canaux SMTP ou SMS pour envoyer des notifications aux utilisateurs, vous devez définir les canaux avant de pouvoir les activer. XenMobile vous invite à configurer les canaux lorsque vous ajoutez des modèles de notification s'ils ne sont pas déjà configurés.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Modèles de notification**. La page **Modèles de notification** s'affiche.



Ajouter un modèle de notification

1. Cliquez sur **Ajouter**. Si aucune passerelle SMS ou aucun serveur SMTP n'a été défini, un message s'affiche relatif à l'utilisation des notifications SMS et SMTP. Vous pouvez choisir de configurer

le serveur SMTP ou la passerelle SMS maintenant ou les configurer les plus tard.

Si vous choisissez de configurer les paramètres de passerelle SMS ou de serveur SMTP maintenant, vous serez redirigé vers la page **Serveur de notification** sur la page **Paramètres**. Après avoir configuré les canaux que vous souhaitez utiliser, vous pouvez retourner sur la page **Modèle de notification** pour continuer à ajouter ou modifier des modèles de notification.

> **Important :**
>
> si vous choisissez de configurer les paramètres de passerelle SMS ou de serveur SMTP ultérieurement, vous ne pourrez pas activer ces canaux lorsque vous ajoutez ou modifiez un modèle de notification, ce qui signifie que ces canaux ne seront pas disponibles pour l'envoi de notifications aux utilisateurs.

2. Pour configurer ces paramètres :

   - **Nom :** entrez un nom descriptif pour le modèle.
   - **Description :** entrez une description pour le modèle.
   - **Type :** dans la liste, cliquez sur le type de notification. Seuls les canaux pris en charge pour le type sélectionné s'affichent. seul un modèle de type Expiration du certificat APNS est autorisé, qui est un modèle prédéfini. Cela signifie que vous ne pouvez pas ajouter un nouveau modèle de ce type.

   > **Remarque :**
   >
   > Pour certains types de modèle, la phrase Envoi manuel pris en charge s'affiche en dessous du type. Cela signifie que le modèle est disponible dans la liste **Notifications** sur le **tableau de bord** et sur la page **Appareils** et que vous pouvez envoyer manuellement la notification aux utilisateurs. L'envoi manuel n'est disponible dans aucun des modèles qui utilisent les macros suivantes dans le champ Sujet ou Message d'un canal :

   - ${outofcompliance.reason(whitelist_blacklist_apps_name)}

     > **Remarque :**
     >
     > La console XenMobile Server utilise les termes « liste noire » et « liste blanche ». Ces termes seront modifiés dans une prochaine version et les termes « liste de blocage » et « liste d'autorisation » les remplaceront.

   - ${outofcompliance.reason(smg_block)}

3. Sous **Canaux**, configurez les informations pour chaque canal à utiliser avec cette notification. Vous pouvez choisir un ou tous les canaux. Le canal que vous choisissez dépend de la façon dont vous souhaitez envoyer des notifications :

   - Si vous choisissez **Secure Hub**, seuls les appareils iOS et Android reçoivent des notifications ; elles apparaissent dans la barre de notification de l'appareil.

- Si vous choisissez **SMTP**, la plupart des utilisateurs recevront le message, car ils se sont inscrits avec leurs adresses e-mail.
- Si vous choisissez **SMS**, seuls les utilisateurs d'appareils équipés d'une carte SIM reçoivent la notification.

Secure Hub :

- **Activer :** cliquez pour activer le canal de notification.
- **Message :** entrez le message à envoyer à l'utilisateur. Ce champ est obligatoire si vous utilisez Secure Hub. Pour de plus amples informations sur l'utilisation de macros dans un message, veuillez consulter la section Macros.
- **Fichier son :** dans la liste, cliquez sur le son de notification que l'utilisateur entend lorsque la notification est reçue.

SMTP :

- **Activer :** cliquez pour activer le canal de notification.

  Vous ne pouvez activer la notification SMTP qu'après avoir configuré le serveur SMTP.

- **Expéditeur :** entrez un expéditeur (facultatif) pour la notification, qui peut être un nom, une adresse e-mail, ou les deux.

- **Destinataire :** ce champ contient une macro préconfigurée pour toutes les notifications sauf les notifications Ad-Hoc pour garantir l'envoi des notifications à l'adresse de destinataire SMTP correcte. Citrix vous recommande de ne pas modifier les macros dans les modèles. Vous pouvez également ajouter des destinataires (par exemple, l'administrateur d'entreprise), en plus de l'utilisateur en ajoutant leurs adresses séparées par un point-virgule (;). Pour envoyer des notifications ad hoc, vous pouvez entrer des destinataires spécifiques sur cette page, ou vous pouvez sélectionner des appareils à partir de la page **Gérer > Appareils** et envoyer des notifications à partir de cet emplacement. Pour plus de détails, voir Appareils.

- **Sujet :** entrez un sujet pour la notification. Ce champ est obligatoire.

- **Message :** entrez le message à envoyer à l'utilisateur. Pour de plus amples informations sur l'utilisation de macros dans un message, veuillez consulter la section Macros.

SMS :

- **Activer :** cliquez pour activer le canal de notification.

  Vous ne pouvez activer la notification SMTP qu'après avoir configuré le serveur SMTP.

- **Destinataire :** ce champ contient une macro préconfigurée pour toutes les notifications sauf les notifications Ad-Hoc pour garantir l'envoi des notifications à l'adresse de destinataire SMS correcte. Citrix vous recommande de ne pas modifier les macros dans les

modèles. Pour envoyer des notifications ad hoc, vous pouvez entrer des destinataires spécifiques, ou vous pouvez sélectionner des appareils à partir de la page **Gérer > Appareils**.

- **Message :** entrez le message à envoyer à l'utilisateur. Ce champ est obligatoire. Pour de plus amples informations sur l'utilisation de macros dans un message, veuillez consulter la section Macros.

4. Cliquez sur **Ajouter**. Lorsque tous les canaux sont correctement configurés, ils apparaissent dans cet ordre sur la page **Modèles de notification** : SMTP, SMS et Secure Hub. Tout canal qui n'est pas correctement configuré apparaît après les canaux correctement configurés.

Modifier un modèle de notification

1. Sélectionnez un modèle de notification. La page de modification spécifique à ce modèle apparaît dans lequel vous pouvez apporter des modifications à tous les champs sauf **Type**, ainsi qu'activer ou désactiver l'utilisation de canaux.
2. Cliquez sur **Enregistrer**.

Supprimer un modèle de notification

Vous pouvez uniquement supprimer les modèles de notification que vous avez ajoutés. Vous ne pouvez pas supprimer les modèles de notification prédéfinis.

1. Sélectionnez un modèle de notification existant.
2. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche.
3. Cliquez sur **Supprimer** pour supprimer le modèle de notification, ou cliquez sur **Annuler** pour annuler la suppression du modèle de notification.

Périphériques

January 10, 2022

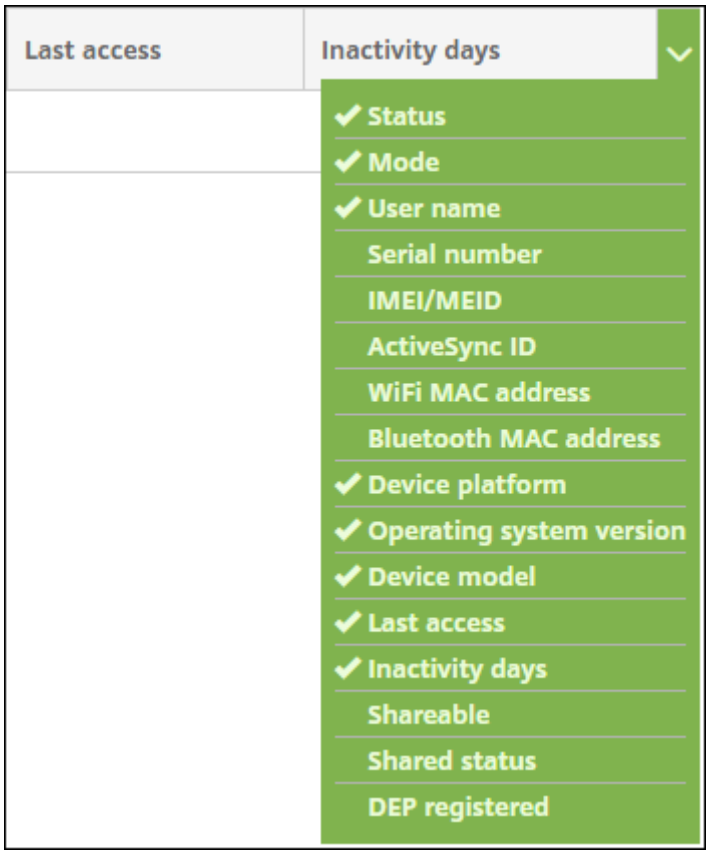
Citrix XenMobile peut provisionner, gérer, sécuriser et inventorier un large éventail de types d'appareils au sein d'une console de gestion unique.

La base de données du serveur XenMobile stocke une liste des appareils mobiles. Un numéro de série unique ou un numéro IMEI (identité internationale d'équipement mobile)/MEID (identifiant de l'équipement mobile) identifie chaque appareil mobile de manière unique. Pour renseigner la console XenMobile avec vos appareils, vous pouvez ajouter les appareils manuellement ou importer une liste d'appareils à partir d'un fichier. Consultez la section Formats des fichiers de provisioning pour de plus amples informations sur les formats de fichier de provisioning.

La page **Appareils** de la console XenMobile répertorie chaque appareil et les informations suivantes :

- **État :** les icônes indiquent si l'appareil est jailbreaké, géré, si Active Sync Gateway est disponible et l'état du déploiement.
- **Mode :** indique le mode de l'appareil, à savoir MDM, MAM ou les deux.
- D'autres informations sur l'appareil : **Nom d'utilisateur**, **Plate-forme de l'appareil**, **Version du système d'exploitation**, **Modèle d'appareil**, **Dernier accès** et **Jours d'inactivité**. Ces en-têtes sont les en-têtes par défaut affichés.

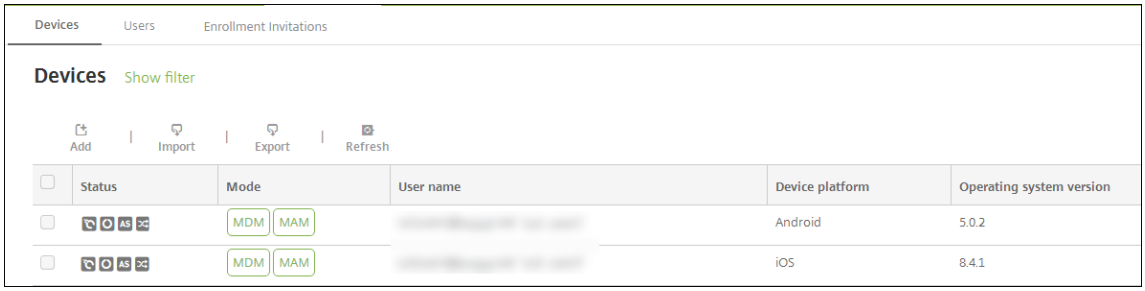
Pour personnaliser le tableau **Appareils**, cliquez sur la flèche vers le bas sur le dernier en-tête. Ensuite, sélectionnez les en-têtes supplémentaires que vous voulez voir dans le tableau ou désactivez les en-têtes à supprimer.



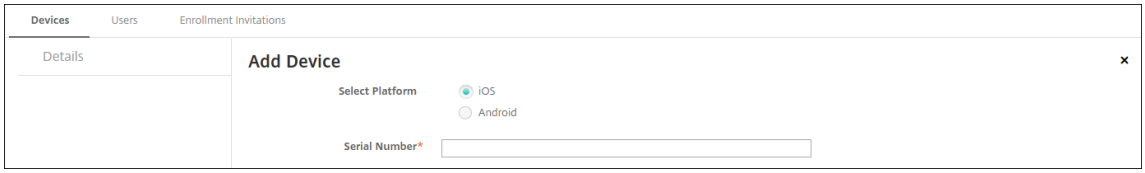
Vous pouvez ajouter des appareils manuellement, importer des appareils à partir d'un fichier de provisioning, modifier les détails de l'appareil, exécuter des actions de sécurité et envoyer des notifications aux appareils. Vous pouvez également exporter toutes les données de tableau d'un appareil dans un fichier .csv pour créer un rapport personnalisé. Le serveur exporte tous les attributs de l'appareil. Si vous appliquez des filtres, XenMobile les utilise lors de la création du fichier .csv.

Ajouter un appareil manuellement

1. Dans la console XenMobile, cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.



2. Cliquez sur **Ajouter**. La page **Ajouter un appareil** s'affiche.



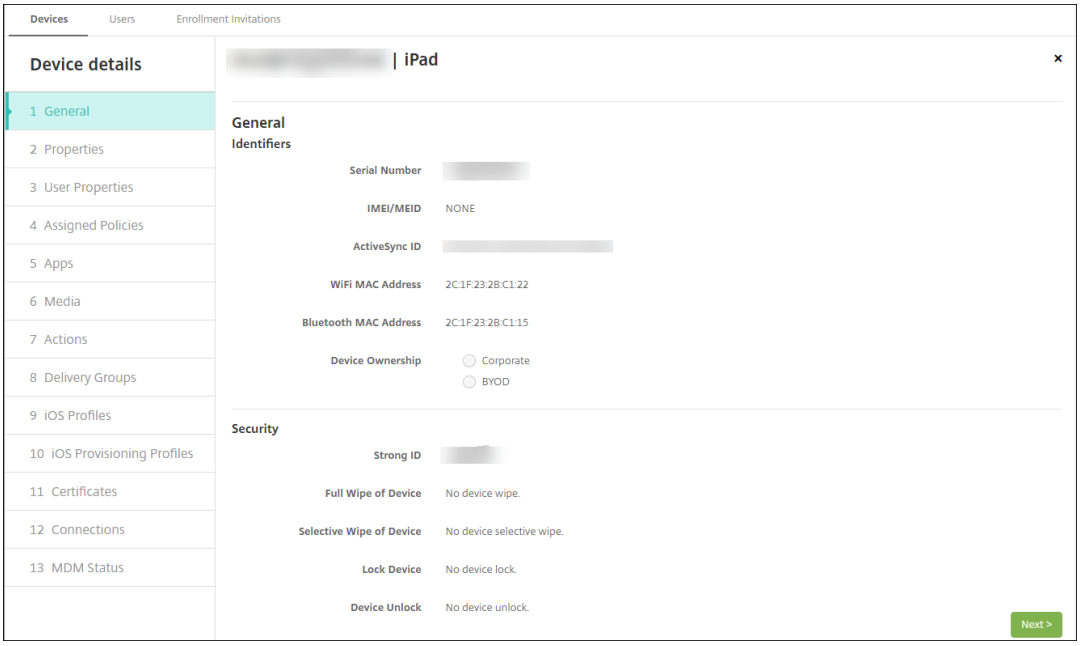
3. Pour configurer ces paramètres :

   - **Sélectionner une plate-forme :** cliquez sur **iOS** ou **Android**.
   - **Numéro de série :** entrez le numéro de série de l'appareil.
   - **IMEI/MEID :** pour les appareils Android uniquement, entrez les informations IMEi/MEID de l'appareil (facultatif).

4. Cliquez sur **Ajouter**. Le tableau **Appareils** s'affiche avec l'appareil ajouté en bas de la liste. Sélectionnez l'appareil que vous avez ajouté, puis dans le menu qui s'affiche, cliquez sur **Modifier** pour afficher et confirmer les détails de l'appareil.

> **Remarque :**
>
> Lorsque vous sélectionnez la case à cocher en regard d'un appareil, le menu d'options s'affiche au-dessus de la liste des appareils. Lorsque vous cliquez dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

- XenMobile Server configuré en mode Enterprise (XME) ou MDM
- LDAP configuré
- Si vous utilisez des groupes locaux et utilisateurs locaux :
  - Un ou plusieurs groupes locaux.
  - Utilisateurs locaux attribués à des groupes locaux.
  - Des groupes de mise à disposition sont associés à des groupes locaux.
- Utilisation d'Active Directory :
  - Des groupes de mise à disposition sont associés à des groupes Active Directory.



5. La page **Général** dresse la liste des **identificateurs**, tels que le numéro de série, l'ID ActiveSync et d'autres informations relatives au type de plate-forme. Pour **Propriétaire**, sélectionnez **Entreprise** ou **BYOD**.

   La page **Général** dresse également la liste des propriétés de **sécurité**, telles que ID fort, Verrouiller l'appareil, Contourner le verrouillage d'activation et d'autres informations relatives au type de plate-forme. Le champ **Effacement complet de l'appareil** inclut le code PIN de l'utilisateur. L'utilisateur doit entrer ce code une fois que l'appareil est effacé. Si l'utilisateur oublie le code, vous pouvez le rechercher ici.

6. La page **Propriétés** dresse la liste des propriétés d'appareil que XenMobile va provisionner. Cette liste affiche toutes les propriétés d'appareil incluses dans le fichier de provisioning utilisé pour ajouter l'appareil. Pour ajouter une propriété, cliquez sur **Ajouter**, puis sélectionnez une propriété dans la liste. Pour connaître les valeurs valides pour chaque propriété, consultez le PDF Valeurs et noms des propriétés d'appareil.

   Lorsque vous ajoutez une propriété, elle s'affiche initialement sous la catégorie dans laquelle vous l'avez ajoutée. Après avoir cliqué sur **Suivant** et être revenu sur la page **Propriétés**, la propriété s'affiche dans la liste appropriée.

   Pour supprimer une propriété, placez le curseur dessus et cliquez sur le **X** sur le côté droit. XenMobile supprime l'élément immédiatement.

7. Les sections **Détails de l'appareil** restantes contiennent des informations sommaires sur l'appareil.

   - **Propriétés utilisateur :** affiche les rôles RBAC, les appartenances aux groupes, les comptes d'achat en volume et les propriétés de l'utilisateur. Vous pouvez retirer un

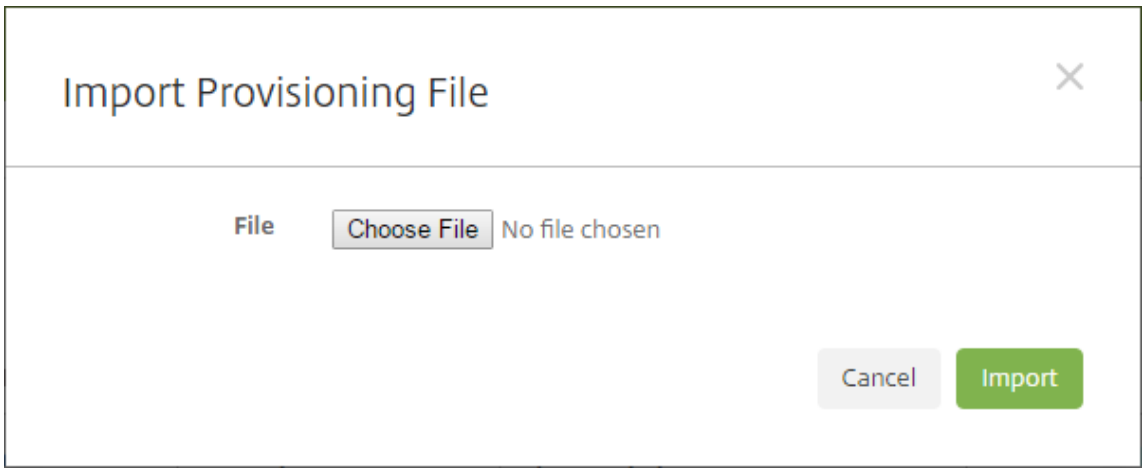
compte d'achat en volume à partir de cette page.

- **Stratégies attribuées :** affiche le nombre de stratégies attribuées, y compris le nombre de stratégies déployées, en attente ou ayant échoué. Fournit les informations relatives au nom, au type et à la dernière date de déploiement pour chaque stratégie.
- **Applications :** affiche, pour le dernier inventaire, le nombre de déploiements d'applications installés, en attente et ayant échoué. Fournit le nom de l'application, l'identificateur, le type et d'autres informations.
- **Média :** affiche, pour le dernier inventaire, le nombre de déploiements de médias installés, en attente et ayant échoué.
- **Actions :** affiche le nombre d'actions déployées, en attente et qui ont échoué. Fournit le nom de l'action et l'heure du dernier déploiement.
- **Groupes de mise à disposition :** affiche le nombre de groupes de mise à disposition ayant réussi, en attente et qui ont échoué. Pour chaque déploiement, fournit le nom du groupe mise à disposition et l'heure déploiement. Sélectionnez un groupe de mise à disposition pour afficher des informations plus détaillées, y compris l'état, l'action, le canal ou l'utilisateur.
- **Profils iOS :** affiche le dernier inventaire de profil iOS, y compris le nom, le type, l'organisation et une description.
- **Profils de provisioning iOS :** affiche les informations du profil de provisioning de distribution d'entreprise, telles que l'UUID, la date d'expiration, et si les profils sont gérés ou non gérés.
- **Certificats :** affiche pour les certificats valides, révoqués ou ayant expiré, des informations telles que le type, le fournisseur, l'émetteur, le numéro de série et le nombre de jours restants avant l'expiration.
- **Connexions :** affiche l'état de la première connexion et de la dernière connexion. Fournit pour chaque connexion, le nom d'utilisateur, l'heure de l'avant-dernière authentification et l'heure de la dernière authentification.
- **État du MDM :** affiche des informations telles que l'état du MDM, l'heure de la dernière notification push et l'heure de la dernière réponse de l'appareil.

Importer des appareils à partir d'un fichier de provisioning

Vous pouvez importer un fichier fourni par les opérateurs mobiles ou les fabricants de l'appareil, ou vous pouvez créer votre propre fichier de provisioning. Pour plus d'informations, consultez la section Formats des fichiers de provisioning dans cet article.

1. Accédez à **Gérer > Appareils** et cliquez sur **Importer**. La boîte de dialogue **Importer le fichier de provisioning** apparaît.

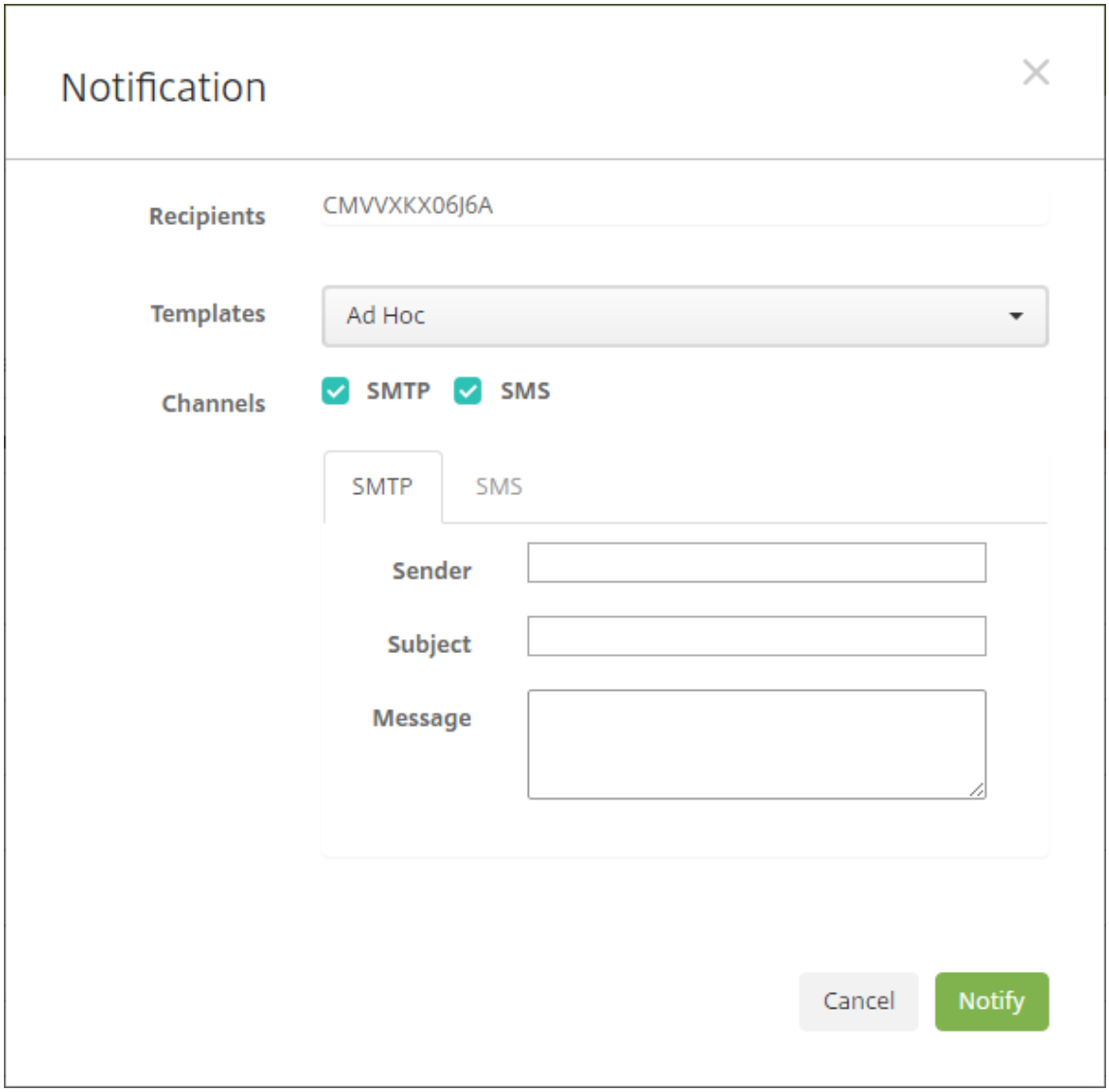


2. Cliquez sur **Choisir un fichier** et accédez au fichier que vous souhaitez importer.
3. Cliquez sur **Importer**. Le tableau **Appareils** répertorie le fichier importé.
4. Pour modifier les informations sur l'appareil, sélectionnez-le, puis cliquez sur **Modifier**. Pour plus d'informations sur les pages **Détails de l'appareil**, consultez la section Ajouter un appareil manuellement.

Envoyer une notification aux appareils

Vous pouvez envoyer des notifications aux appareils à partir de la page Appareils. Pour plus d'informations sur les notifications, veuillez consulter la section Notifications.

1. Sur la page **Gérer > Appareils** sélectionnez l'appareil ou les appareils auxquels vous souhaitez envoyer une notification.
2. Cliquez sur **Notifier**. La boîte de dialogue **Notification** s'affiche. Le champ **Destinataires** répertorie tous les appareils sélectionnés pour recevoir pour la notification.



3. Pour configurer ces paramètres :
   - **Modèles :** dans la liste, cliquez sur le type de notification que vous souhaitez envoyer. Pour chaque modèle excepté le modèle **Ad Hoc**, les champs **Sujet** et **Message** sont renseignés avec le texte configuré pour le modèle que vous avez choisi.
   - **Canaux :** sélectionnez la méthode à utiliser pour envoyer le message. La valeur par défaut est **SMTP** et **SMS**. Cliquez sur les onglets pour afficher le format du message pour chaque canal.
   - **Expéditeur :** entrez un expéditeur (facultatif).
   - **Sujet :** entrez un sujet pour un message **ad hoc**.
   - **Message :** entrez le message pour un message **ad hoc**.
4. Cliquez sur **Notifier**.

Exporter le tableau Appareils

1. Filtrez le tableau **Appareil** en fonction de ce que vous souhaitez voir apparaître dans le fichier d'exportation.
2. Cliquez sur le bouton **Exporter** au-dessus du tableau **Appareils**. XenMobile extrait les informations du tableau **Appareils** filtré et les convertit en fichier .csv.
3. Ouvrez ou enregistrez le fichier .csv lorsque vous y êtes invité.

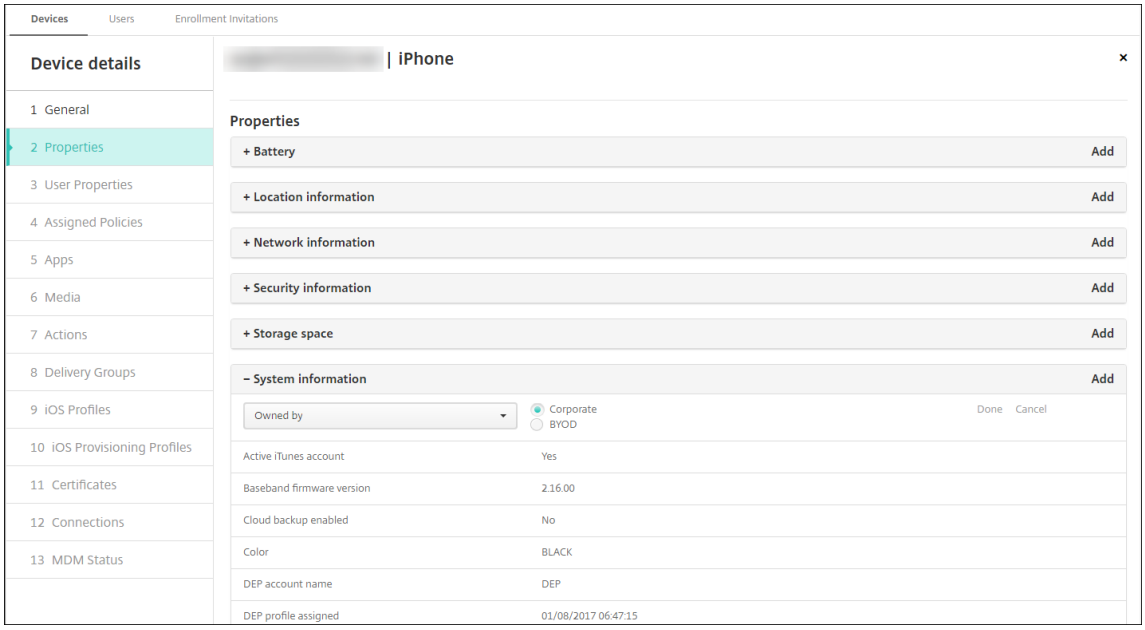
Identifier les appareils utilisateur manuellement

Vous pouvez manuellement identifier un appareil dans XenMobile de l'une des façons suivantes :

- Durant le processus d'inscription basé sur invitation
- Durant le processus d'inscription via le portail en libre-service.
- En ajoutant le propriétaire de l'appareil en tant que propriété d'appareil

Vous avez la possibilité d'identifier l'appareil comme appartenant à la société ou à un employé. Lors de l'utilisation de l'aide du portail d'aide en libre-service pour inscrire un appareil, vous pouvez identifier l'appareil comme appartenant à la société ou à un employé. Vous pouvez également identifier un appareil manuellement, comme suit.

1. Ajoutez une propriété à l'appareil à partir de l'onglet **Appareils** dans la console XenMobile.
2. Ajoutez la propriété appelée **Appartient à** et choisissez **Entreprise** ou **BYOD** (appartenant à un employé).



Formats des fichiers de provisioning

De nombreux opérateurs mobiles ou fournisseurs d'appareils fournissent des listes d'appareils mobiles autorisés. Vous pouvez utiliser ces listes pour éviter d'avoir à entrer manuellement une longue liste d'appareils mobiles. XenMobile prend en charge un format de fichier d'importation commun aux trois types d'appareils pris en charge : Android, iOS et Windows.

Un fichier de provisioning que vous créez manuellement et utilisez pour l'importation d'appareils sur XenMobile doit être au format suivant :

SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2; … propertyNameN;propertyValueN

Gardez à l'esprit les considérations suivantes :

- Pour connaître les valeurs valides pour chaque propriété, consultez le PDF Valeurs et noms des propriétés d'appareil.
- Utilisez le jeu de caractères UTF-8.
- Utilisez un point-virgule (;) pour séparer les champs dans le fichier de provisioning. Si une partie d'un champ contient un point-virgule, elle doit être précédée d'une barre oblique inverse (\).

  Par exemple, pour cette propriété :

  ```
  propertyV;test;1;2
  ```

  utilisez une barre oblique inverse comme caractère d'échappement :

  ```
  propertyV\;test\;1\;2
  ```

- Le numéro de série est requis pour les appareils iOS car le numéro de série est l'identifiant de l'appareil iOS.
- Pour les autres plates-formes, vous devez inclure le numéro de série ou le numéro IMEI.
- Les valeurs valides pour **OperatingSystemFamily** sont **WINDOWS**, **ANDROID** ou **iOS**.

Exemple de fichier de provisioning d'appareil

```
`1050BF3F5173010816100655105903911524201625379901;WINDOWS;propertyN;
   propertyV\;test\;1\;2;prop 2
2050BF3F5173010816100655105903922524201625379902;ANDROID;propertyN;
   propertyV$*&&éééétest
3050BF3F5173010816100655105903933524201625379903;iOS;test;
4050BF3F517301081610065510590393;;iOS;test;
;55244201625379903;ANDROID;test.testé;value;`
```

Chaque ligne du fichier décrit un appareil. La première entrée dans l'exemple ci-dessus signifie :

- SerialNumber: 1050BF3F5173010816100655105903911

- IMEI: `15244201625379901`
- OperatingSystemFamily: `WINDOWS`
- PropertyName : `propertyN`
- PropertyValue: `propertyV\;test\;1\;2;prop 2`

ActiveSync Gateway

January 10, 2022

ActiveSync est un protocole de synchronisation des données mobiles développé par Microsoft. ActiveSync synchronise les données avec les périphériques portables et ordinateurs de bureau (ou portables).

Vous pouvez configurer des règles ActiveSync Gateway dans XenMobile. Basé sur ces règles, vous pouvez autoriser ou non les appareils à accéder aux données ActiveSync. Par exemple, si vous activez la règle Applications requises manquantes, XenMobile vérifie la stratégie d'accès aux applications requises et refuse l'accès aux données ActiveSync si les applications requises sont manquantes. Pour chaque règle, vous avez le choix entre **Autoriser** ou **Refuser**. Le paramètre par défaut est **Autoriser**.

Pour plus d'informations sur la stratégie d'accès aux applications, consultez la section Stratégies d'accès aux applications.

XenMobile prend en charge les règles suivantes :

Appareils anonymes : vérifie si un appareil est en mode anonyme. Cette vérification est disponible si XenMobile ne parvient pas à authentifier à nouveau l'utilisateur lorsqu'un appareil tente de se reconnecter.

Échec de l'attestation Samsung KNOX : vérifie si un appareil n'est pas parvenu à répondre à une requête du serveur d'attestation Samsung KNOX.

Applications sur liste noire : vérifie si un appareil dispose d'applications interdites, telles que définies dans une stratégie d'accès aux applications.

Autorisation et refus implicites : cette action est la valeur par défaut pour ActiveSync Gateway. La passerelle crée une liste d'appareils de tous les appareils qui ne répondent pas à tous les critères de règle de filtre et autorise ou refuse les connexions en se basant sur cette liste. Si aucune règle ne correspond, la valeur par défaut est Autorisation implicite.

Appareils inactifs : vérifie si un appareil est inactif, tel que cela est défini par le paramètre Nombre de jours maximum d'inactivité dans la boîte de dialogue Propriétés du serveur.

Applications requises manquantes : vérifie si des applications nécessaires sont manquantes sur un appareil, tel que cela est défini dans une stratégie d'accès aux applications.

Applications non suggérées : vérifie si un appareil dispose d'applications non suggérées, telles que définies dans une stratégie d'accès aux applications.

Mot de passe non conforme : vérifie si le mot de passe utilisateur est conforme. Sur les appareils iOS et Android, XenMobile peut déterminer si le mot de passe actuel de l'appareil est conforme à la stratégie de code secret envoyée à l'appareil. Par exemple, sur iOS, l'utilisateur dispose de 60 minutes pour définir un mot de passe si XenMobile envoie une stratégie de code secret à l'appareil. Avant qu'un mot de passe ne soit défini par l'utilisateur, le code secret peut ne pas être conforme.

Appareils non conformes : vérifie si un appareil n'est pas conforme, en fonction de la propriété de l'appareil Non conforme. Cette propriété est généralement modifiée par les actions automatisées ou un tiers tirant parti des API XenMobile.

État révoqué : vérifie si le certificat de l'appareil a été révoqué. Un appareil révoqué ne peut pas se réinscrire tant qu'il n'a pas été à nouveau autorisé.

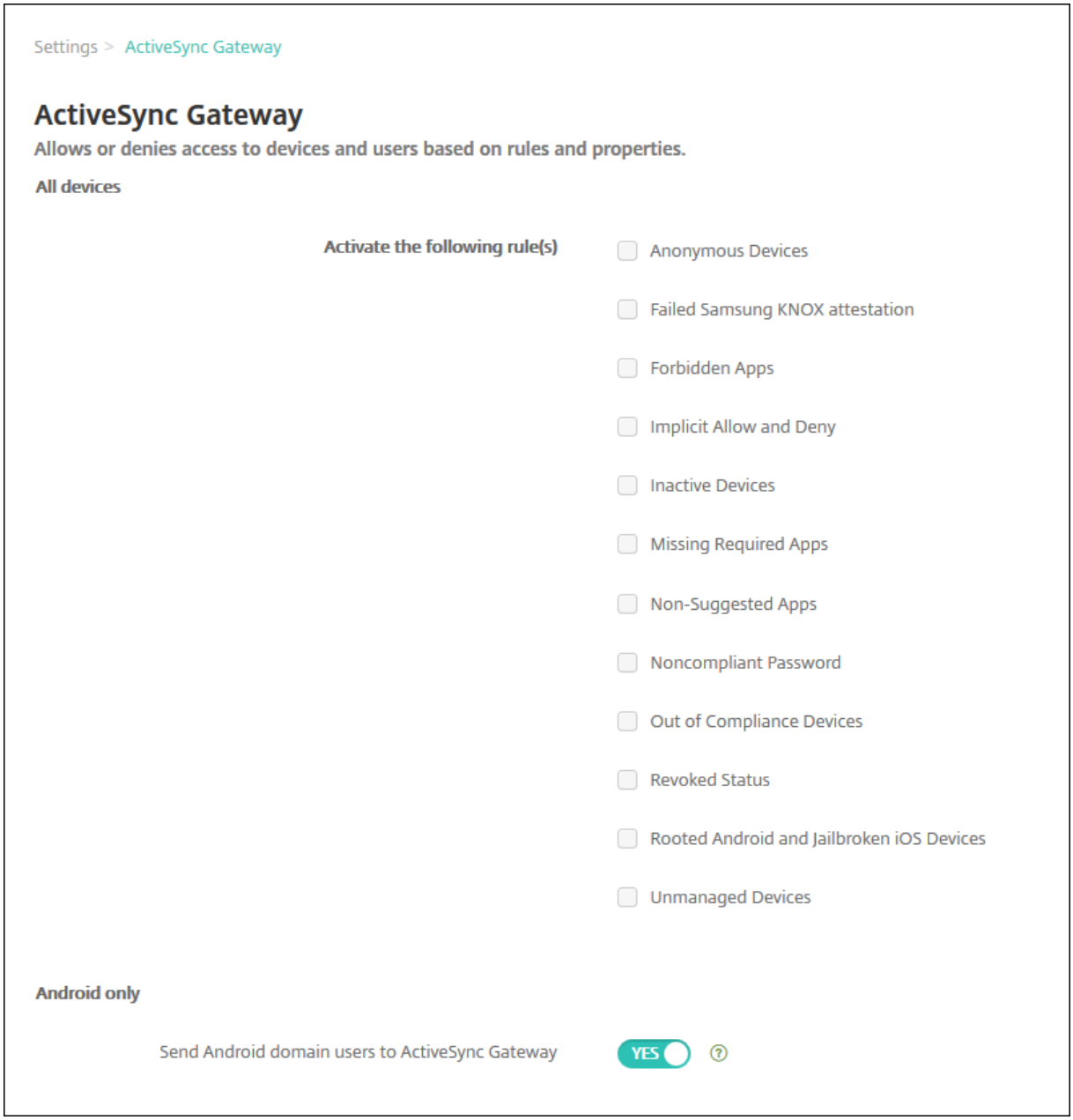
Appareils Android rootés et iOS jailbreakés : vérifie si un appareil Android ou iOS est rooté ou jailbreaké.

Appareils non gérés : vérifie si un appareil est toujours dans un état géré, sous le contrôle de XenMobile. Par exemple, un appareil inscrit au MAM ou un appareil non inscrit n'est pas géré.

Envoyer les utilisateurs Android à ActiveSync Gateway : cliquez sur **OUI** pour vous assurer que XenMobile envoie des informations de l'appareil Android à ActiveSync Gateway.

Pour configurer les paramètres ActiveSync Gateway

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Serveur**, cliquez sur **ActiveSync Gateway**. La page **ActiveSync Gateway** s'affiche.



1. Dans **Activer la ou les règles suivantes**, sélectionnez une ou plusieurs règles à activer.
2. Dans **Android uniquement**, sous **Envoyer les utilisateurs Android à ActiveSync Gateway**, cliquez sur **OUI** pour vous assurer que XenMobile envoie les informations de l'appareil Android à ActiveSync Gateway.
3. Cliquez sur **Enregistrer**.

Migrer de l'administration des appareils vers Android Enterprise

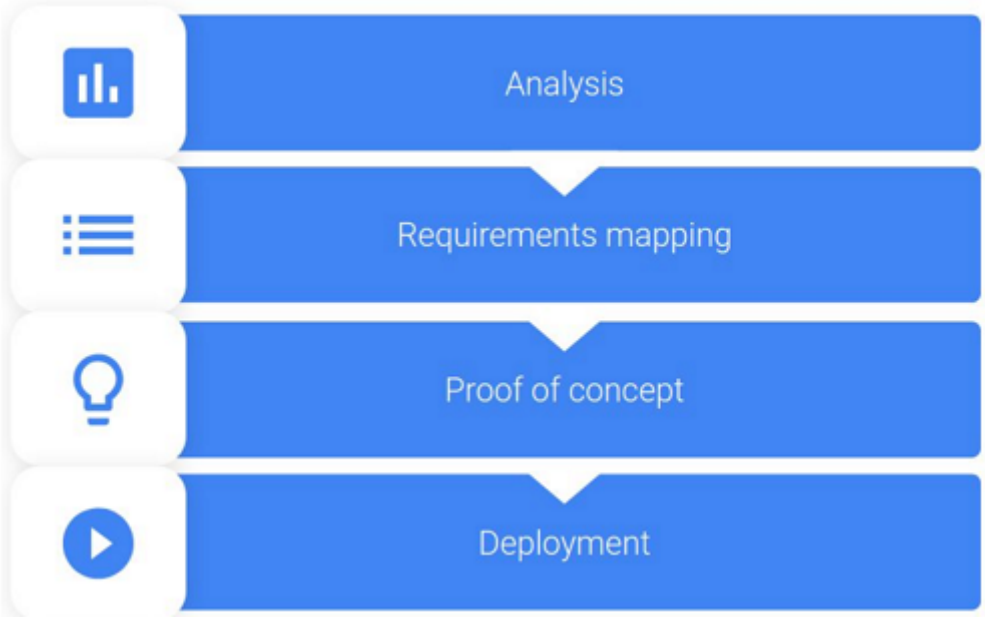
January 10, 2022

Cet article traite des considérations et des recommandations relatives à la migration de l'administration des appareils Android d'ancienne génération vers Android Enterprise. Google est en train de mettre en place la fin de la prise en charge de l'API d'administration des appareils Android (Android Device Administration API). Cette API prend en charge les applications d'entreprise sur les appareils Android. Android Entreprise est la solution de gestion moderne recommandée par Google et Citrix.

XenMobile passe à Android Enterprise comme méthode d'inscription par défaut pour les appareils Android. Une fois que Google a terminé la prise en charge des API, l'inscription échouera pour les appareils Android Q en mode d'administration de l'appareil.

Android Enterprise inclut la prise en charge des modes d'appareils entièrement gérés et d'appareils avec profil de travail. La publication Google, Android Enterprise Migration Bluebook, explique en détail comment l'administration des appareils d'ancienne génération et des appareils Android Enterprise diffèrent. Nous vous recommandons de lire les informations de migration publiées par Google.

Cette publication décrit également les quatre phases de la migration de l'administration des appareils et comprend le diagramme suivant. Cet article contient des recommandations spécifiques à XenMobile pour les phases de migration.



> Schéma tiré du Bluebook
> sur la migration Android Enterprise.
> Reproduit avec l'autorisation de Google.

Impact de la fin de prise en charge de l'administration des appareils

Google va mettre fin à la prise en charge des API d'administration des appareils suivantes. Ces API ne fonctionneront pas sur les appareils exécutant Android Q après la mise à niveau de Secure Hub pour cibler le niveau d'API Android Q :

- Désactivation de la caméra : contrôle l'accès aux caméras de l'appareil.
- Expiration du mot de passe : force les utilisateurs à modifier leur mot de passe après une période configurable.
- Limitation du mot de passe : définit des exigences restrictives en matière de mot de passe

Les API obsolètes n'ont aucun impact sur les appareils inscrits en mode Citrix MAM exclusif.

Recommandations

Les recommandations suivantes s'appliquent aux appareils déjà inscrits en mode d'administration des appareils Android d'ancienne génération, aux appareils non-inscrits et aux appareils inscrits en mode Citrix MAM exclusif.

État de l'inscription d'appareil	Action recommandée
L'appareil existant est inscrit en mode d'administration des appareils et peut être mis à niveau vers Android Q.	Avant de mettre à niveau l'appareil vers Android Q, migrez du mode d'administration des appareils vers Android Entreprise.
L'appareil existant est inscrit en mode d'administration des appareils. L'appareil ne peut pas être mis à niveau vers Android Q.	L'appareil peut rester en mode d'administration des appareils. Toutefois, prévoyez de déplacer l'appareil vers Android Entreprise lors de l'actualisation de l'appareil.
L'appareil existant est inscrit en mode d'administration des appareils et il est mis à niveau vers Android Q.	Migrez du mode d'administration des appareils vers Android Enterprise avant que Google ne mette fin à la prise en charge des API. Un message d'avertissement pour ces appareils s'affiche dans la console XenMobile.
Nouvel appareil mis à disposition avec Android Q et inscrit en mode d'administration des appareils.	Migrez du mode d'administration des appareils vers Android Enterprise avant que Google ne mette fin à la prise en charge des API. Un message d'avertissement pour ces appareils s'affiche dans la console XenMobile.
Nouvel appareil mis à disposition avec Android Q ou pouvant être mis à niveau vers Android Q. L'appareil n'est pas inscrit.	Utilisez Android Entreprise pour tous les nouveaux appareils.

État de l'inscription d'appareil	Action recommandée
Un nouvel appareil ou un appareil existant mis à disposition avec Android Q est inscrit en mode d'administration des appareils après que Google mette fin à la prise en charge des API.	Pour éviter l'impact lié aux API Google obsolètes, Citrix recommande de migrer vers Android Enterprise avant que Google ne mette fin à la prise en charge des API. Après cette date, l'inscription de ces appareils échouera.
Nouvel appareil ou appareil existant inscrit en mode Citrix MAM exclusif.	Aucune action n'est nécessaire. Les API Google obsolètes n'ont aucun impact sur les appareils inscrits en mode MAM exclusif.

Analyse

La phase d'analyse de la migration comprend les étapes suivantes :

- Comprendre votre configuration Android d'ancienne génération
- Documenter votre configuration d'ancienne génération afin de pouvoir mapper les fonctionnalités d'ancienne génération aux fonctionnalités Android Enterprise

Analyse recommandée

1. Évaluez Android Enterprise sur XenMobile : entièrement géré, entièrement géré avec profil de travail, appareil dédié, profil de travail (BYOD).
2. Analysez les fonctionnalités actuelles d'administration de vos appareils par rapport à Android Entreprise.
3. Documentez les cas d'utilisation de l'administration de votre appareil.

Pour documenter les cas d'utilisation de l'administration de votre appareil, procédez comme suit :

1. Créez une feuille de calcul et répertoriez les groupes de stratégies actuels dans votre console XenMobile.
2. Créez des cas d'utilisation distincts en fonction des groupes de stratégies existants.
3. Pour chaque cas d'utilisation, répertoriez les éléments suivants :
    - Nom
    - Chef d'entreprise
    - Modèle d'identité utilisateur
    - Configuration requise par l'appareil
        - Sécurité
        - Direction

    - Utilisation
  - Inventaire des appareils
    - Marque et modèle
    - Version d'OS
  - Applications
4. Pour chaque application, répertoriez les éléments suivants :
   - Nom de l'application
   - Nom du package
   - Méthode d'hébergement
   - Si l'application est publique ou privée
   - Si l'application est obligatoire (vrai/faux)

Mappage des exigences

En vous basant sur l'analyse terminée, déterminez vos exigences en matière de fonctionnalités Android Enterprise.

Mappage des exigences recommandé

1. Déterminez le mode de gestion et la méthode d'inscription :
   - Profil de travail (BYOD) : nécessite une réinscription. Aucune réinitialisation d'usine n'est nécessaire.
   - Entièrement géré : nécessite une réinitialisation d'usine. Inscrivez les appareils à l'aide du code QR, du partage NFC, de l'identifiant du DPC ou de l'inscription sans contact.
2. Créez une stratégie de migration d'application.
3. Mappez les exigences du cas d'utilisation aux fonctionnalités Android Enterprise. Documentez la fonctionnalité pour chaque exigence de l'appareil qui correspond le mieux à l'exigence Android et sa version correspondante.
4. Déterminez le système d'exploitation Android minimum en fonction de la configuration requise (7.0, 8.0, 9.0).
5. Choisissez un modèle d'identité :
   - Modèle recommandé : Compte Google Play d'entreprise
   - Utilisez les comptes Google G-Suite uniquement si vous êtes un client Google Cloud Identity
6. Créez une stratégie d'appareil :
   - Aucune action : si les appareils répondent au niveau minimum du système d'exploitation.

- Mise à niveau : si les appareils peuvent être mis à jour vers le système d'exploitation pris en charge.
- Remplacement : si les appareils ne peuvent pas être mis à jour vers le niveau du système d'exploitation pris en charge.

Stratégie de migration d'application recommandée

Une fois la correspondance des exigences effectuée, déplacez les applications de la plate-forme Android vers la plate-forme Android Enterprise. Pour plus d'informations sur la publication d'applications, consultez la section Ajouter des applications.

- Applications de magasin public
  1. Sélectionnez les applications à migrer, puis modifiez les applications en effaçant le paramètre Google Play et en sélectionnant **Android Enterprise** comme plate-forme.
  2. Sélectionnez le groupe de mise à disposition. Si une application est obligatoire, déplacez l'application vers la liste **Applications requises** dans le groupe de mise à disposition.

  Une fois l'application enregistrée, elle apparaît dans Google Play Store. Si vous avez un profil de travail, les applications apparaissent dans Google Play Store dans le profil de travail.
- Applications (d'entreprise) privées

  Les applications privées sont développées en interne ou par un développeur tiers. Nous vous recommandons de publier les applications privées à l'aide de Google Play.
  1. Sélectionnez les applications à migrer, puis modifiez les applications en sélectionnant **Android Enterprise** comme plate-forme.
  2. Chargez le fichier APK, puis configurez les paramètres de l'application.
  3. Publiez l'application dans le groupe de mise à disposition requis.
- Applications MDX
  1. Sélectionnez les applications à migrer, puis modifiez les applications en sélectionnant **Android Enterprise** comme plate-forme.
  2. Chargez le fichier MDX. Procédez au processus d'approbation de l'application.
  3. Sélectionnez les stratégies MDX.

  Pour les applications MDX d'entreprise, nous vous recommandons de les remplacer par des applications encapsulées en mode SDK MDX :
  - Option 1 : hébergez l'APK dans Google Play avec un compte de développeur attribué à titre privé à votre organisation. Publiez le fichier MDX dans XenMobile.

- Option 2 : publiez l'application depuis XenMobile en tant qu'application d'entreprise. Publiez l'APK dans XenMobile et sélectionnez la plate-forme **Android Enterprise** pour le fichier MDX.

Migration de stratégie d'appareil Citrix

Pour les stratégies disponibles pour les plates-formes Android et Android Enterprise, modifiez la stratégie et sélectionnez la plate-forme **Android Enterprise**.

Pour Android Enterprise, considérez l'utilisation du mode d'inscription. Certaines options de stratégie sont disponibles uniquement pour les appareils en mode Profil de travail ou en mode entièrement géré.

Preuve de concept

Après avoir migré des applications vers Android Entreprise, vous pouvez configurer un test de migration pour vérifier que les fonctionnalités fonctionnent comme prévu.

Configuration de l'évaluation recommandée

1. Configurez l'infrastructure de déploiement :
   - Créez un groupe de mise à disposition pour votre évaluation Android Enterprise.
   - Configurez Android Enterprise dans XenMobile.
2. Configurez les applications utilisateur.
3. Configurez les fonctionnalités Android Enterprise.
4. Attribuez des stratégies au groupe de mise à disposition Android Enterprise.
5. Testez et confirmez les fonctionnalités.
6. Effectuez une procédure détaillée de la configuration de l'appareil pour chaque cas d'utilisation.
7. Documentez les étapes de configuration de l'utilisateur.

Déploiement

Vous pouvez désormais déployer votre configuration Android Entreprise et préparer vos utilisateurs à la migration.

Stratégie de déploiement recommandée

La stratégie de déploiement recommandée par Citrix consiste à tester tous vos systèmes de production pour Android Enterprise, puis à terminer la migration d'appareils ultérieurement.

- Dans ce scénario, les utilisateurs continuent à utiliser des appareils d'ancienne génération avec leur configuration actuelle. Vous configurez de nouveaux appareils pour la gestion Android Entreprise.
- Migrez les appareils existants uniquement lorsqu'une mise à niveau ou un remplacement est nécessaire.
- Migrez les appareils existants vers la gestion Android Entreprise à la fin de leur cycle de vie habituel. Vous pouvez également migrer ces appareils lorsqu'ils ont besoin d'être remplacés en raison de perte ou d'endommagement.

Android Entreprise

January 10, 2022

Android Enterprise est un ensemble d'outils et de services fournis par Google en tant que solution de gestion d'entreprise pour les appareils Android. Avec Android Enterprise :

- Vous utilisez XenMobile pour gérer les appareils Android appartenant à l'entreprise et vos appareils Android BYOD (programme « Apportez votre propre appareil »).
- Vous pouvez gérer l'ensemble de l'appareil ou un profil distinct sur l'appareil. Le profil distinct permet d'isoler les comptes, applications et données d'entreprise des comptes, applications et données personnels.
- Vous pouvez également gérer des appareils dédiés à un usage unique, tels que la gestion de l'inventaire. Pour obtenir une vue d'ensemble des fonctionnalités d'Android Enterprise de Google, consultez la section Gestion d'Android Enterprise.

Ressources :

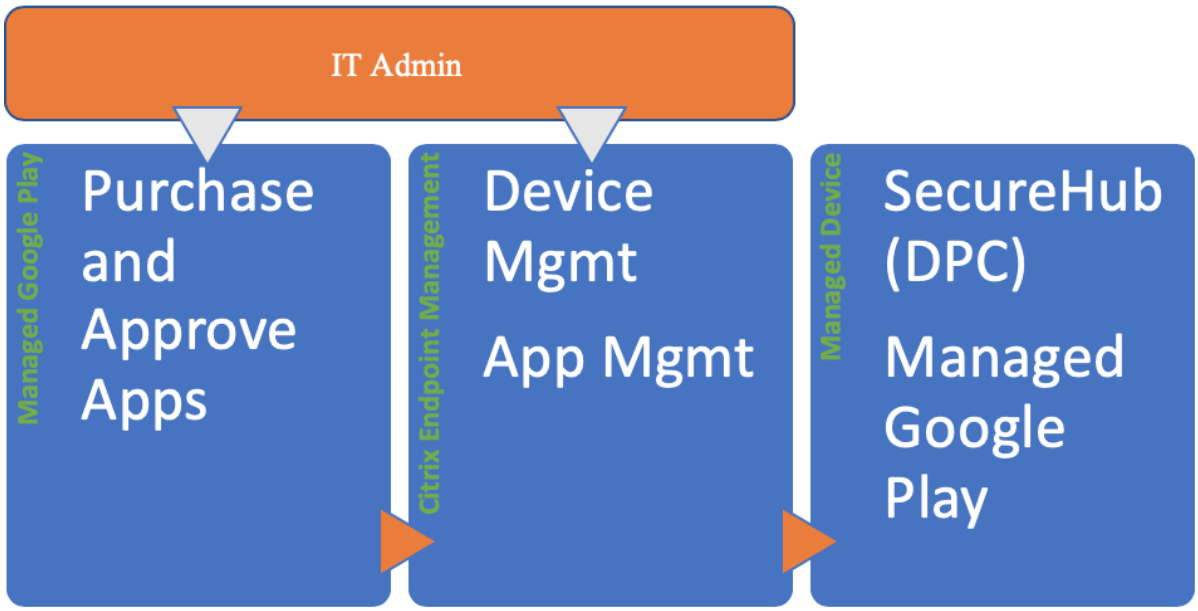
- Pour obtenir la liste des termes et définitions liés à Android Enterprise, consultez la section Terminologie Android Enterprise du guide des développeurs Google Android Enterprise. Google met fréquemment à jour ces termes.
- Pour les systèmes d'exploitation Android pris en charge pour XenMobile, consultez Systèmes d'exploitation d'appareils pris en charge.
- Pour plus d'informations sur les connexions sortantes à prendre en compte lors de la configuration d'environnements réseau pour Android Enterprise, consultez l'article de support Google Android Enterprise Network Requirements.

Lorsque vous intégrez XenMobile à Google Play d'entreprise pour utiliser Android Enterprise, vous créez une entreprise. Google définit une entreprise comme une liaison entre l'organisation et votre solution de gestion mobile d'entreprise (EMM). Tous les utilisateurs et appareils que l'organisation gère via votre solution appartiennent à son entreprise.

Une entreprise pour Android Enterprise comprend trois composants : une solution EMM, une application DPC (Device Policy Controller) et une plate-forme d'application Google Enterprise. Lorsque vous intégrez XenMobile à Android Enterprise, la solution complète comporte les composants suivants :

- **XenMobile :** la solution EMM Citrix. XenMobile est une solution de gestion unifiée qui permet un espace de travail numérique sécurisé. XenMobile fournit aux administrateurs informatiques les moyens de gérer les appareils et les applications de leurs organisations.
- **Citrix Secure Hub :** l'application DPC Citrix. Secure Hub représente la rampe de lancement de XenMobile. Secure Hub applique des stratégies sur l'appareil.
- **Google Play d'entreprise :** plate-forme d'application d'entreprise Google qui s'intègre avec XenMobile. L'API EMM de Google Play définit les stratégies d'application et distribue l'application.

Cette illustration montre comment les administrateurs interagissent avec ces composants et comment les composants interagissent les uns avec les autres :



Utilisation de Google Play d'entreprise avec XenMobile

> **Remarque :**
>
> Vous pouvez utiliser Google Play d'entreprise ou Google Workspace pour enregistrer Citrix en tant que fournisseur de gestion de la mobilité d'entreprise (EMM). Cet article traite de

> l'utilisation d'Android Enterprise avec Google Play d'entreprise. Si votre organisation utilise Google Workspace pour fournir un accès aux applications, vous pouvez l'utiliser avec Android Enterprise. Consultez Ancienne version d'Android Enterprise pour clients Google Workspace (anciennement G Suite).

Lorsque vous utilisez Google Play d'entreprise, vous provisionnez des comptes Google Play d'entreprise pour les appareils et les utilisateurs finaux. Les comptes Google Play d'entreprise permettent d'accéder à Google Play d'entreprise, ce qui permet aux utilisateurs d'installer et d'utiliser les applications que vous mettez à leur disposition. Si votre organisation utilise un service d'identité tiers, vous pouvez lier des comptes Google Play d'entreprise à vos comptes d'identité existants.

Comme ce type d'entreprise n'est pas lié à un domaine, vous pouvez créer plusieurs entreprises pour une seule organisation. Par exemple, chaque département ou région d'une organisation peut s'inscrire en tant qu'entreprise différente pour gérer des ensembles distincts d'appareils et d'applications.

Pour les administrateurs XenMobile, Google Play d'entreprise combine l'expérience utilisateur et les fonctionnalités du magasin d'applications de Google Play avec un ensemble de fonctionnalités de gestion conçues pour les entreprises. Vous utilisez Google Play d'entreprise pour ajouter, acheter et approuver des applications en vue de les déployer sur l'espace Android Enterprise d'un appareil. Vous pouvez utiliser Google Play pour déployer des applications publiques, privées, et tierces.

Pour les utilisateurs d'appareils gérés, Google Play d'entreprise correspond au magasin d'applications d'entreprise. Les utilisateurs peuvent parcourir les applications, afficher les détails des applications et les installer. Contrairement à la version publique de Google Play, les utilisateurs peuvent uniquement installer des applications à partir de Google Play d'entreprise que vous leur mettez à disposition.

Scénarios de déploiement d'appareils et modes de fonctionnement

Le scénario de déploiement d'appareils permet de savoir à qui appartient les appareils que vous déployez et désigne la façon dont vous les gérez. Les profils d'appareils font référence à la façon dont DPC gère et applique les stratégies sur les appareils.

Le profil de travail permet d'isoler les comptes, applications et données d'entreprise des comptes, applications et données personnels. Pour plus d'informations sur les profils de travail (ou profils professionnels), consultez la rubrique d'aide Qu'est-ce qu'un profil professionnel ? de Google Android Enterprise.

> **Important :**
>
> Lorsque les appareils Android Enterprise sont mis à jour vers Android 11, Google migre les appareils « entièrement gérés avec profil de travail » vers une nouvelle expérience de profil de tra-

> vail optimisée pour la sécurité. Pour plus d'informations, consultez Changes ahead for Android Enterprise's Fully Managed with Work Profile.

Gestion des appareils	Cas d'utilisation	Profil de travail	Profil personnel	Remarques
Appareils appartenant à l'entreprise (entièrement gérés)	Appareils appartenant à l'entreprise destinés uniquement à un usage professionnel	Non	Oui. DPC peut effectuer des actions à l'échelle de l'appareil, telles que la configuration de la connectivité sur l'appareil, la configuration des paramètres globaux et la réinitialisation d'usine.	Pour les appareils neufs ou réinitialisés en usine uniquement.
Entièrement géré avec profil de travail	Appareils appartenant à l'entreprise destinés à un usage professionnel et personnel	Oui	Oui. Deux copies du DPC s'exécutent sur ces appareils : l'une qui gère l'appareil en mode propriétaire de l'appareil et l'autre qui gère le profil de travail en mode propriétaire du profil. Vous pouvez appliquer des stratégies distinctes à l'appareil et au profil de travail.	Anciennement connus sous le nom d'appareils COPE.

Gestion des appareils	Cas d'utilisation	Profil de travail	Profil personnel	Remarques
Appareils dédiés*	Appareils appartenant à l'entreprise configurés pour un seul cas d'utilisation, tels que l'affichage numérique ou l'impression de billets	Non	Oui. Vous ne fournissez que les applications requises et empêchez les utilisateurs d'ajouter d'autres applications.	Anciennement connus sous le nom d'appareils d'entreprise à usage unique (appareils COSU).
Profil de travail BYOD**	Appareils personnels inscrits en mode profil professionnel (également appelée mode propriétaire du profil)	Oui	Oui. DPC gère uniquement le profil de travail, pas l'ensemble de l'appareil.	Ces appareils n'ont pas besoin d'être neufs ou réinitialisés en usine.

* Les utilisateurs peuvent partager un appareil dédié. Lorsqu'un utilisateur se connecte à une application sur un appareil dédié, l'état de son travail est celui de l'application, et non celui de l'appareil.

**XenMobile ne prend pas en charge les appareils Zebra en mode profil professionnel BYOD. XenMobile prend en charge les appareils Zebra en tant qu'appareils entièrement gérés et en mode d'appareil d'ancienne génération (également appelé mode d'administration des appareils).

Pour plus d'informations sur la migration du mode d'ancienne génération vers le mode Propriétaire de l'appareil ou Propriétaire du profil, consultez la section Migrer de l'administration des appareils vers Android Enterprise.

Méthodes d'authentification

Les profils d'inscription déterminent si les appareils Android s'inscrivent en mode MAM, MDM ou MDM+MAM, avec la possibilité pour les utilisateurs de se désinscrire de MDM.

Pour plus d'informations sur la spécification du niveau de sécurité et les étapes d'inscription requises, consultez la section Configurer les modes d'inscription sécurisée.

XenMobile prend en charge les types d'authentification suivants pour les appareils Android inscrits dans MDM+MAM. Pour de plus amples informations, consultez la section Certificats et authentification.

- Domaine
- Domaine et jeton de sécurité
- Certificat client
- Certificat client et domaine
- Fournisseurs d'identité :
  - Azure Active Directory
  - Fournisseur d'identité Citrix

Une autre méthode d'authentification rarement utilisée est le certificat client et le jeton de sécurité. Pour de plus amples informations, consultez https://support.citrix.com/article/CTX215200.

Exigences

Avant de commencer à utiliser Android Enterprise, vous devez disposer des éléments suivants :

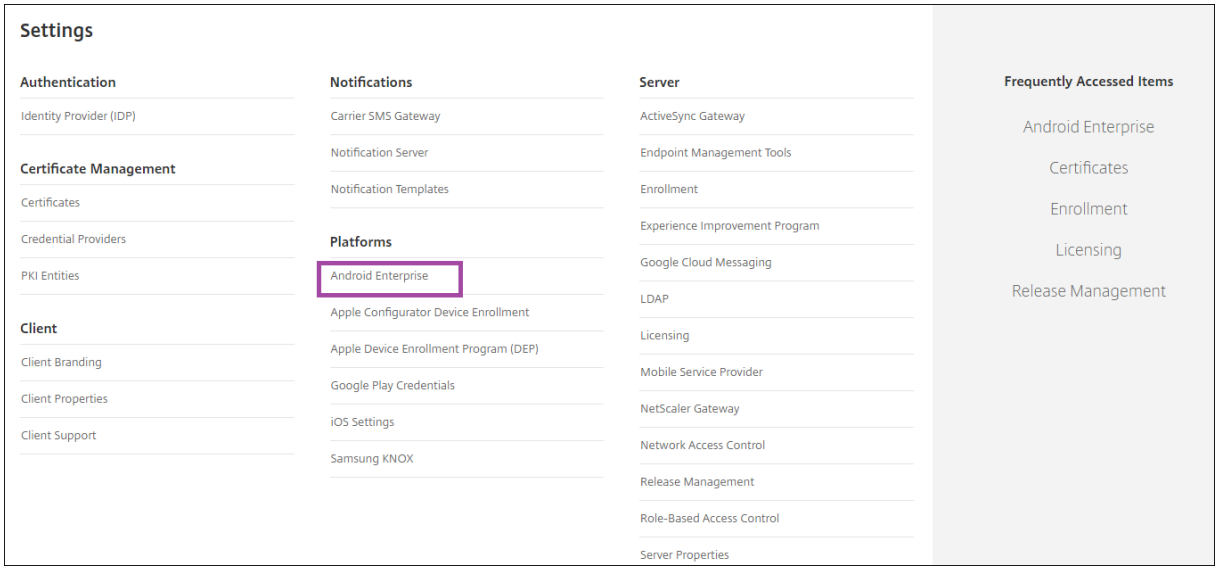
- Comptes et informations d'identification :
  - Pour configurer Android Enterprise avec Google Play d'entreprise, un compte Google d'entreprise
  - Pour télécharger les derniers fichiers MDX, un compte client Citrix
  - Pour déployer des applications privées (facultatif), un compte Google Developer
- Firebase Cloud Messaging (FCM) configuré pour XenMobile. Consultez Firebase Cloud Messaging pour obtenir des instructions.
- Pour l'inscription Samsung Knox Mobile Enrollment (facultatif), des licences Knox Premium

Connecter XenMobile à Google Play

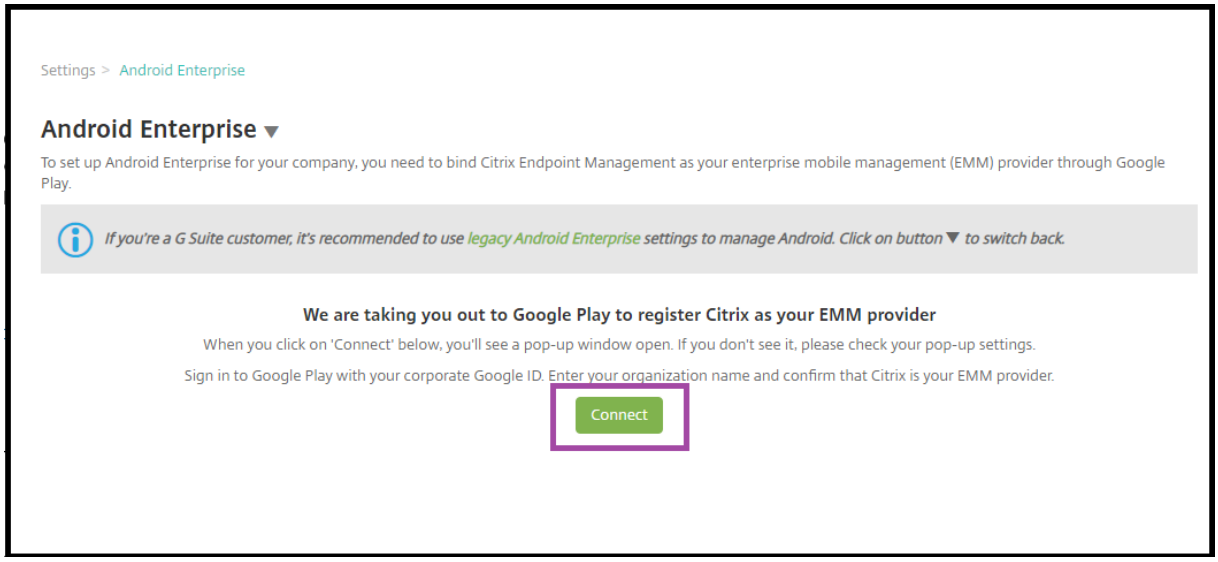
Pour configurer Android Enterprise pour votre organisation, enregistrez Citrix en tant que fournisseur de gestion de la mobilité d'entreprise (EMM) via Google Play d'entreprise. Cette configuration permet de connecter Google Play d'entreprise à XenMobile et de créer une entreprise pour Android Enterprise dans XenMobile.

Vous avez besoin d'un compte Google d'entreprise pour vous connecter à Google Play.

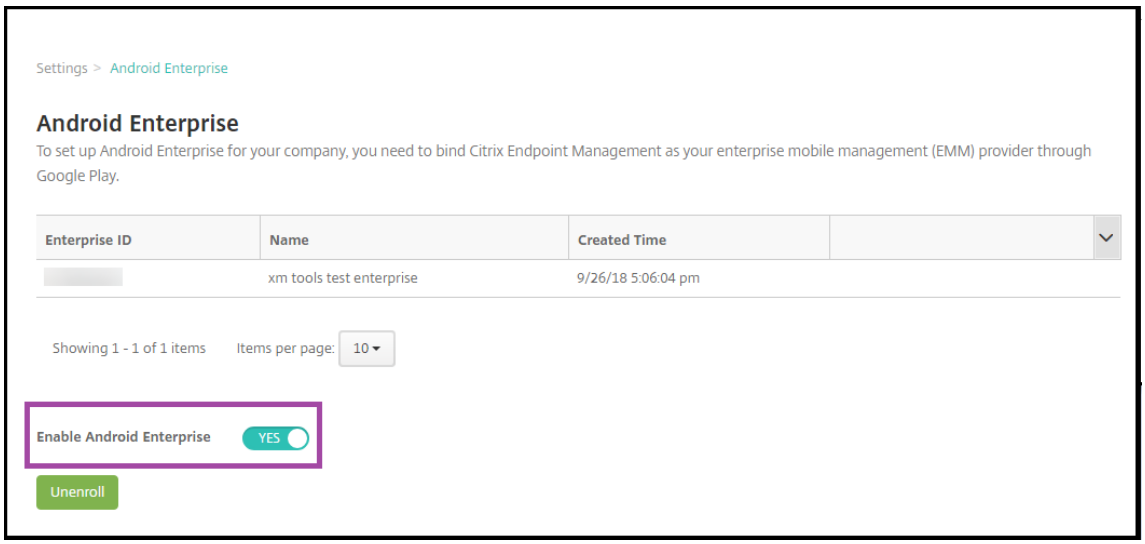
1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Accédez à **Paramètres > Android Enterprise**.



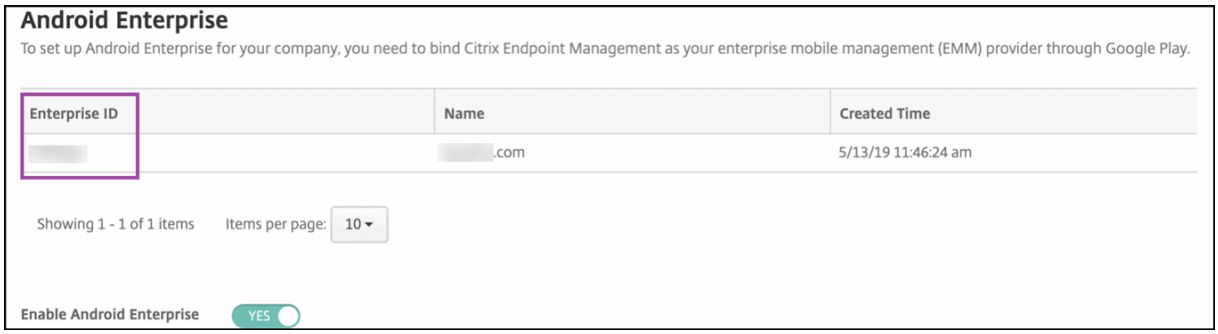
1. Cliquez sur **Connect**. Google Play s'ouvre.



1. Connectez-vous à Google Play avec les informations d'identification de votre compte Google d'entreprise. Entrez le nom de votre organisation et confirmez que Citrix est votre fournisseur EMM.
2. Un ID d'entreprise est ajouté pour Android Enterprise. Pour activer Android Enterprise, faites glisser **Activer Android Enterprise** vers **Oui**.



Votre ID d'entreprise apparaît dans la console XenMobile.



Votre environnement est connecté à Google et est prêt à gérer les appareils. Vous pouvez désormais mettre des applications à la disposition des utilisateurs.

XenMobile peut être utilisé pour mettre à la disposition des utilisateurs des applications de productivité mobiles Citrix, des applications MDX, des applications de magasin d'applications public, des applications Web et SaaS, des applications d'entreprise et des liens Web. Pour plus d'informations sur ces types d'applications et sur leur mise à disposition des utilisateurs, consultez la section Ajouter des applications.

La section suivante explique comment mettre à disposition des applications de productivité mobiles.

Mettre à disposition des applications de productivité mobiles Citrix aux utilisateurs d'Android Enterprise

Afin de mettre à disposition des applications de productivité mobiles Citrix aux utilisateurs d'Android Enterprise, effectuez les étapes suivantes.

1. Publiez les applications en tant qu'applications MDX. Consultez Configurer des applications en tant qu'applications MDX.

2. Configurez les règles pour la question de sécurité que vos utilisateurs utilisent pour accéder aux profils de travail sur leurs appareils. Consultez Configurer la stratégie de la question de sécurité.

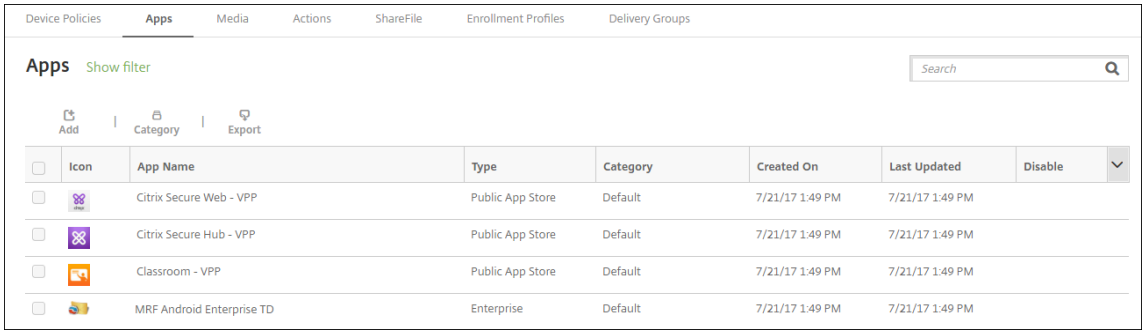
Les applications que vous publiez sont disponibles pour les appareils inscrits dans votre entreprise Android Enterprise.

> **Remarque :**
>
> Lorsque vous déployez une application du magasin d'applications public Android Enterprise sur un utilisateur Android, cet utilisateur est automatiquement inscrit dans Android Enterprise.

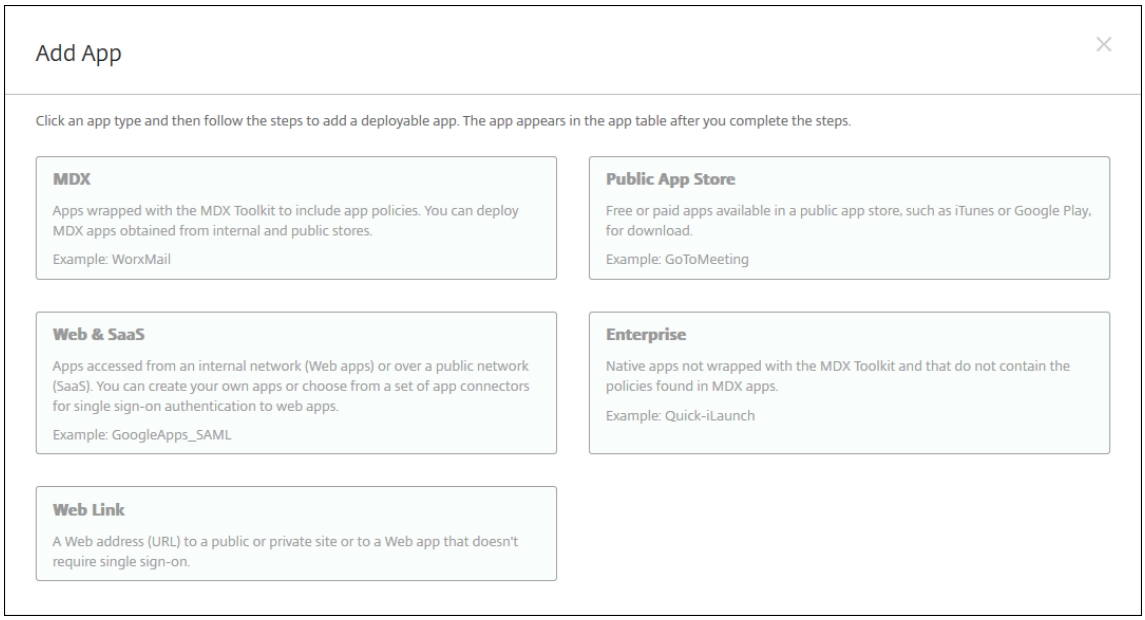
Configurer des applications en tant qu'applications MDX

Pour configurer une application de productivité Citrix en tant qu'application MDX pour Android Enterprise :

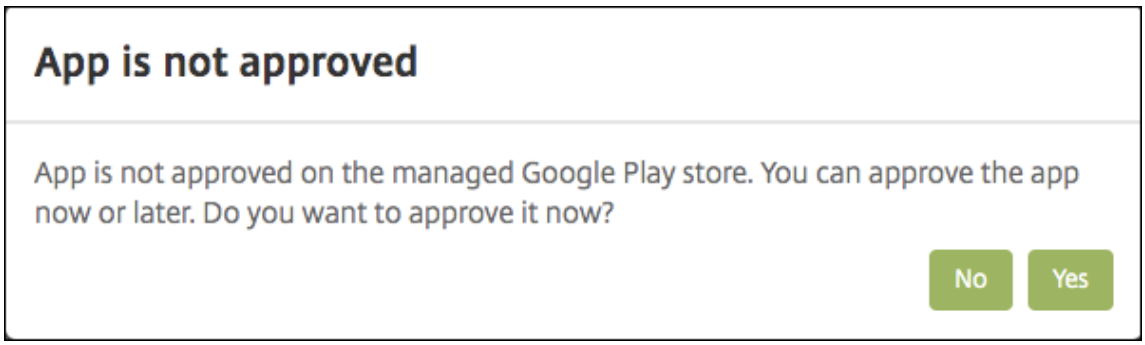
1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'affiche.



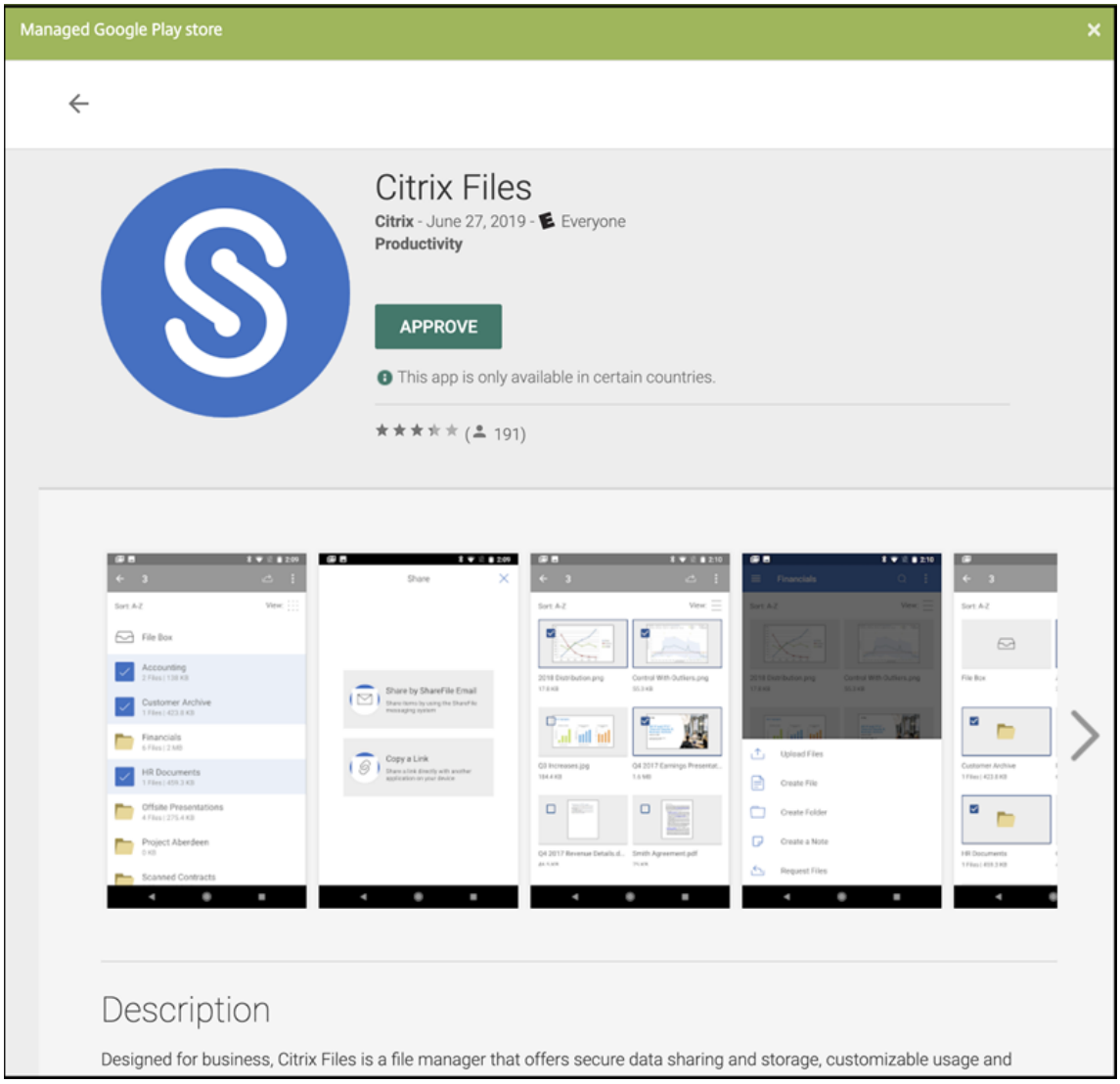
2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



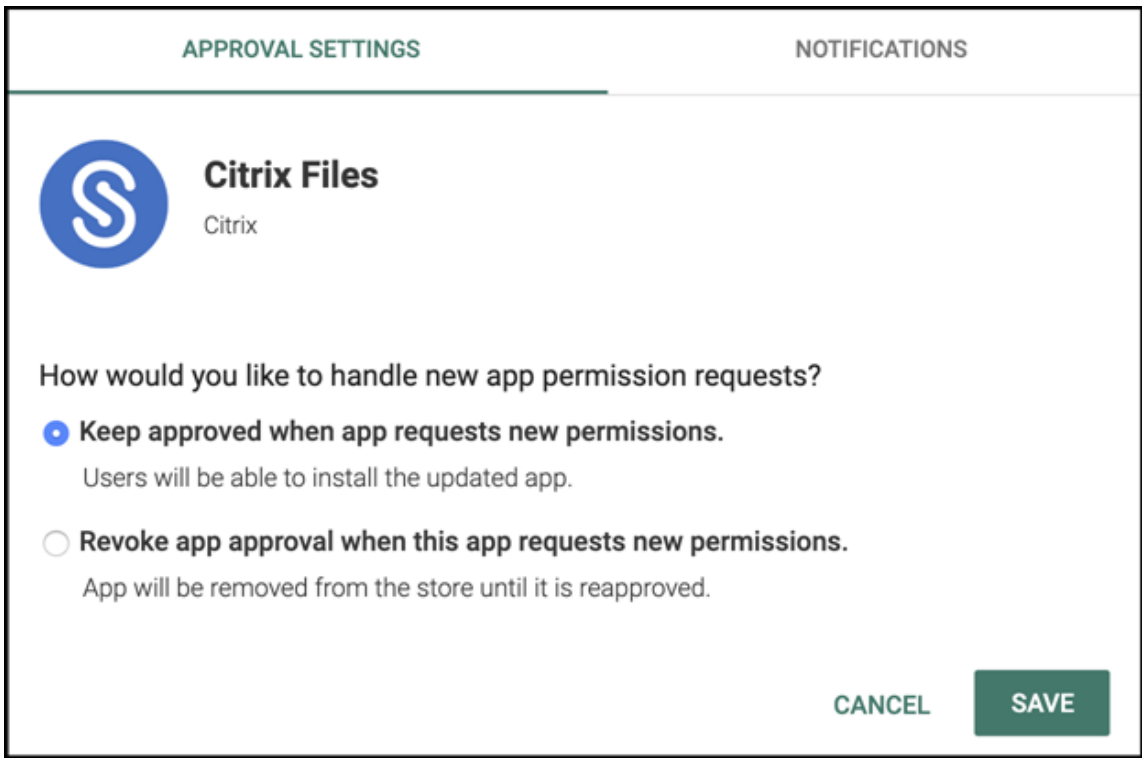
3. Cliquez sur **MDX**. La page **Informations sur l'application** s'affiche.
4. À gauche de la page, sélectionnez **Android Enterprise** comme plate-forme.
5. Sur la page **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous **Nom de l'application** dans le tableau **Applications**.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.
6. Cliquez sur **Suivant**. La page **Android Enterprise MDX App** s'affiche.
7. Cliquez sur **Charger** et accédez à l'emplacement des fichiers .mdx pour l'application. Sélectionnez le fichier et cliquez sur **Ouvrir**.
8. L'interface utilisateur vous avertit si l'application jointe nécessite l'approbation du Google Play Store d'entreprise. Pour approuver l'application sans quitter la console XenMobile, cliquez sur **Oui**.



9. Lorsque la page Google Play Store d'entreprise s'ouvre, cliquez sur **Approuver**.

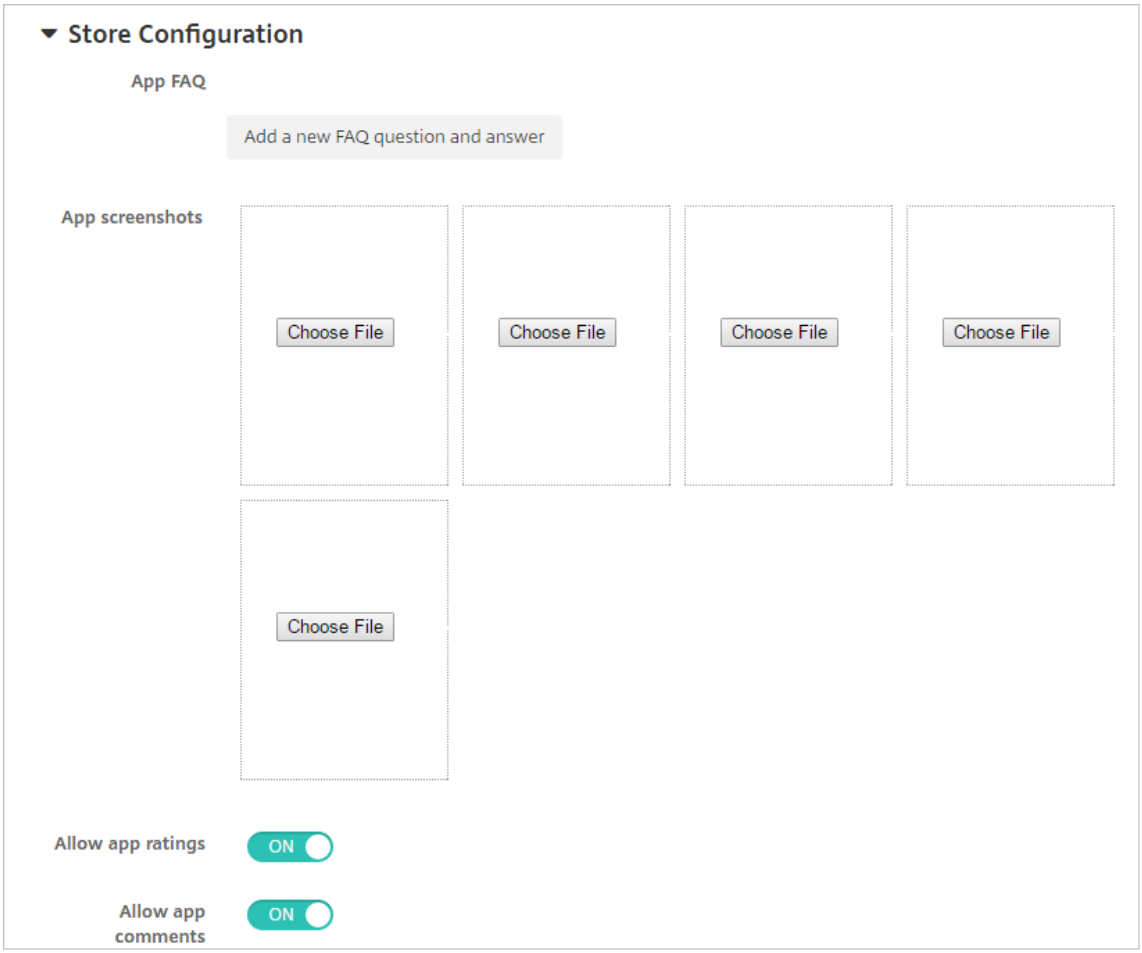


10. Cliquez à nouveau sur **Approuver**.
11. Sélectionnez **Maintenir l'état approuvé de cette application lorsqu'elle demande d'autres autorisations**. Cliquez sur **Enregistrer**.



12. Lorsque l'application est approuvée et enregistrée, d'autres paramètres apparaissent sur la page. Pour configurer ces paramètres :
    - **Nom du fichier :** entrez le nom du fichier associé à l'application.
    - **Description de l'application :** entrez une description pour l'application.
    - **Suivi du produit :** spécifiez le suivi du produit que vous souhaitez transférer aux appareils utilisateur. Si vous avez un suivi conçu à des fins de test, vous pouvez le sélectionner et l'affecter à vos utilisateurs. La valeur par défaut est Production.
    - **Version de l'application :** si vous le souhaitez, entrez le numéro de version de l'application.
    - **ID de package :** URL de l'application dans le Google Play Store.
    - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
    - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
    - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.
13. Configurez les **stratégies MDX**. Pour de plus amples informations sur les stratégies d'application pour applications MDX, veuillez consulter la section Synopsis des stratégies MDX et Présentation du SDK MAM.
14. Configurez les règles de déploiement. Pour de plus amples informations, consultez la section Déployer des ressources.

15. Développez **Configuration du magasin**. Ce paramètre ne s'applique pas aux applications Android Enterprise, qui s'affichent uniquement dans Google Play d'entreprise.

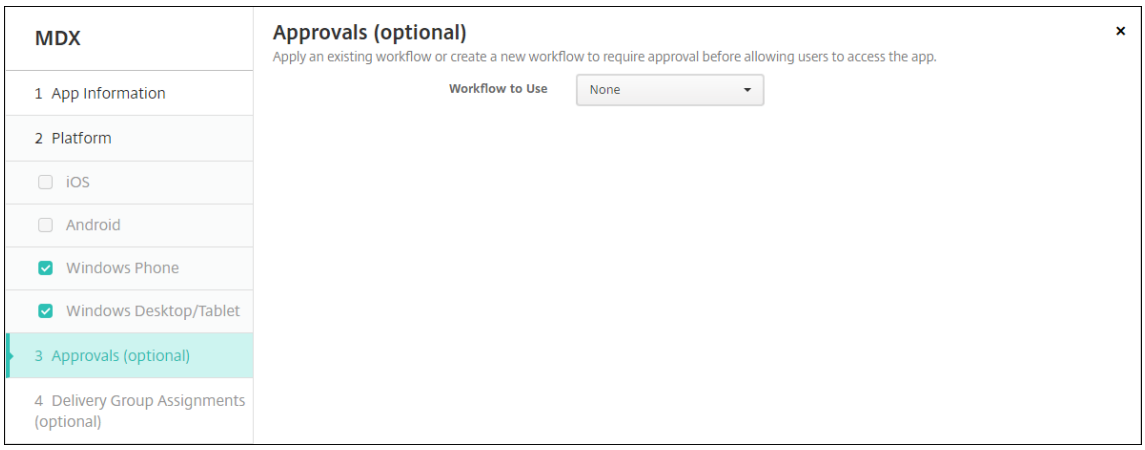


Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le magasin d'applications. Vous pouvez également indiquer si les utilisateurs peuvent évaluer ou ajouter des commentaires sur l'application.

- Pour configurer ces paramètres :
  - **FAQ sur les applications :** ajoutez des questions et réponses pour l'application.
  - **Copies d'écran des applications :** ajoutez des captures d'écran pour faciliter le classement de l'application dans le magasin d'applications. L'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.
  - **Autoriser notation des applications :** indiquez si un utilisateur peut évaluer l'application. La valeur par défaut est **Activé**.

    Autoriser commentaires sur les applications : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée. La valeur par défaut est **Activé**.

16. Cliquez sur **Suivant**. La page **Approbations** s'affiche.



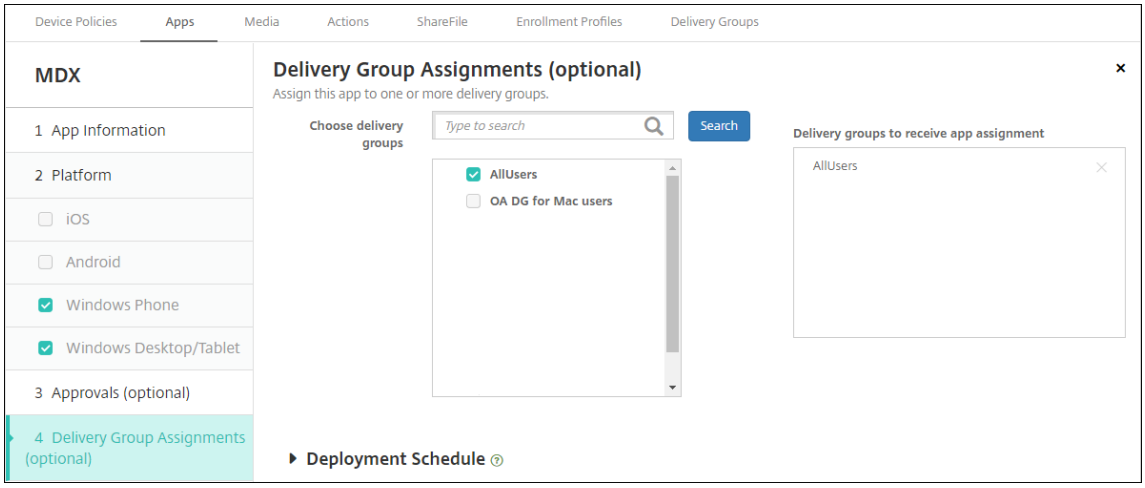
Vous utilisez des workflows lorsque vous avez besoin d'une approbation pour créer des comptes d'utilisateur. Si vous ne souhaitez pas configurer des workflows d'approbation, vous pouvez passer à l'étape 15.

Configurez ces paramètres pour attribuer ou créer un workflow :

- **Workflow à utiliser :** dans la liste, cliquez sur un workflow existant ou cliquez sur **Créer un nouveau workflow**. La valeur par défaut est **Aucun**.
- Si vous sélectionnez **Créer un nouveau workflow**, configurez les paramètres suivants. Pour plus d'informations, voir Appliquer des workflows.
- **Nom :** entrez un nom unique pour le workflow.
- **Description :** entrez une description pour le workflow (facultatif).
- **Modèles d'approbation d'e-mail :** dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Lorsque vous cliquez sur l'icône d'œil à droite du champ, une boîte de dialogue s'affiche dans laquelle vous pouvez afficher un aperçu du modèle.
- **Niveaux d'approbation par un responsable :** dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est 1 niveau. Les options possibles sont les suivantes :
  - Pas nécessaire
  - 1 niveau
  - 2 niveaux
  - 3 niveaux
- **Sélectionner un domaine Active Directory :** dans la liste, sélectionnez le domaine Active Directory à utiliser pour le workflow.
- **Rechercher des approbateurs supplémentaires requis :** tapez le nom de la personne dans le champ de recherche et cliquez sur **Rechercher**. Les noms proviennent d'Active Directory.
- Lorsque le nom s'affiche dans le champ, sélectionnez la case à cocher en regard du nom. Le nom et l'adresse e-mail s'affichent dans la liste **Approbateurs supplémentaires requis sélectionnés**.

- Pour supprimer une personne de la liste **Approbateurs supplémentaires requis sélectionnés**, procédez comme suit :
  * Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.
  * Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats de la recherche.
  * Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

17. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.



18. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.
19. Développez **Calendrier de déploiement** et configurez les paramètres suivants :
    - En regard de **Déployer**, cliquez sur **Activé** pour planifier le déploiement ou cliquez sur **Désactivé** pour empêcher le déploiement. L'option par défaut est **Activé**.
    - En regard de Calendrier de déploiement, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
    - Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    - En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
    - En regard de **Déployer pour les connexions permanentes**, assurez-vous que **Désactivé**

est sélectionné. L'option par défaut est **Désactivé**. Les connexions toujours actives ne sont pas disponibles pour Android Enterprise si vous avez commencé à utiliser XenMobile avec la version 10.18.19 ou ultérieure. Nous ne recommandons pas ces connexions pour les clients qui ont commencé à utiliser XenMobile avant la version 10.18.19.

Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

20. Cliquez sur **Enregistrer**.

Répétez les étapes pour configurer une application MDX pour chaque application de productivité mobile.

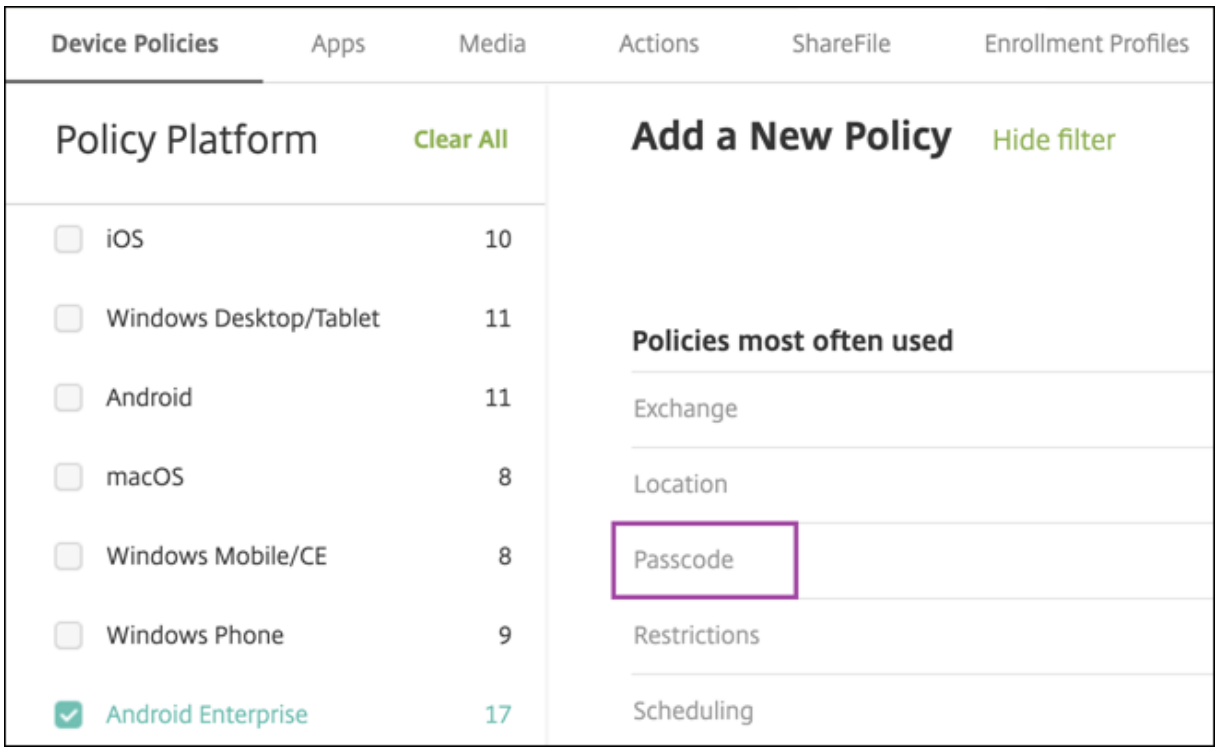
Configurer la stratégie de la question de sécurité

La stratégie de code secret XenMobile configure l'ensemble de règles associées aux questions de sécurité que les utilisateurs utilisent pour accéder à leurs appareils ou aux profils de travail Android Enterprise sur leurs appareils. Une question de sécurité peut être définie avec un mot de passe ou une reconnaissance biométrique. Pour plus d'informations sur la stratégie de code secret, consultez Stratégie de code secret.

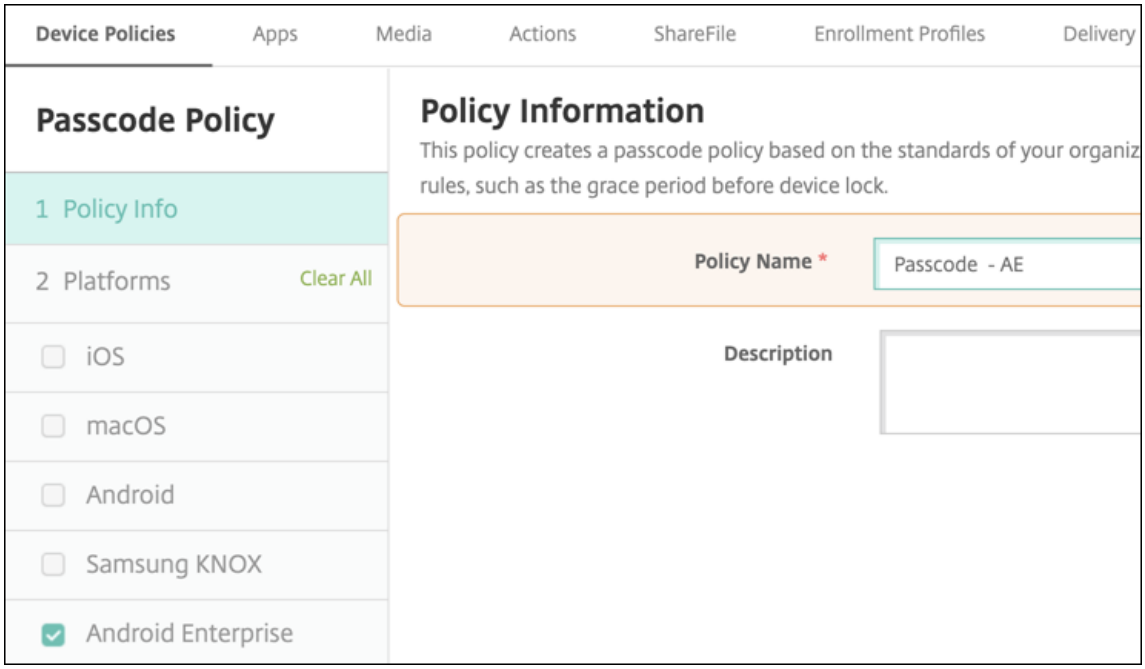
- Si votre déploiement Android Enterprise inclut des appareils BYOD, configurez la stratégie de code secret pour le profil de travail.
- Si votre déploiement inclut des appareils entièrement gérés appartenant à l'entreprise, configurez la stratégie de code secret pour l'appareil lui-même.
- Si votre déploiement inclut les deux types d'appareils, configurez les deux types de stratégie de code secret.

Pour configurer la stratégie de code secret, procédez comme suit :

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**.
2. Cliquez sur **Ajouter**.
3. Cliquez sur **Afficher le filtre** pour afficher le panneau **Stratégie par plate-forme**. Dans le panneau **Stratégie par plate-forme**, sélectionnez **Android Enterprise**.
4. Cliquez sur **Code secret** dans le panneau droit.



1. Entrez un **nom de stratégie**. Cliquez sur **Suivant**.



2. Configurez les paramètres de la stratégie de code secret.
   - Définissez l'option **Code secret de l'appareil requis** sur **Activé** pour afficher les paramètres disponibles pour les questions de sécurité de l'appareil.
   - Définissez l'option **Question de sécurité du profil de travail requise** sur **Activé** pour af-

ficher les paramètres disponibles pour les questions de sécurité du profil de travail.

3. Cliquez sur **Suivant**.
4. Attribuez la stratégie à un ou plusieurs groupes de mise à disposition.
5. Cliquez sur **Enregistrer**.

Création de profils d'inscription

Les profils d'inscription contrôlent la façon dont les appareils Android sont inscrits si Android Enterprise est activé pour votre déploiement XenMobile. Lorsque vous créez un profil d'inscription pour inscrire des appareils Android Enterprise, vous pouvez configurer le profil d'inscription pour inscrire de nouveaux appareils et des appareils réinitialisés en usine comme suit :

- Appareils entièrement gérés
- Appareils dédiés (appareils COSU)
- Appareils entièrement gérés avec profil de travail (appareils COPE)

Vous pouvez également configurer chacun de ces profils d'inscription Android Enterprise pour inscrire les appareils Android BYOD en tant qu'appareils avec profil de travail.

Si Android Enterprise est activé pour votre déploiement XenMobile, tous les appareils Android nouvellement inscrits ou réinscrits le sont en tant qu'appareils Android Enterprise. Par défaut, le profil d'inscription global inscrit les nouveaux appareils Android et les appareils soumis à une réinitialisation d'usine en tant qu'appareils entièrement gérés et les appareils Android BYOD en tant qu'appareils avec profil de travail.

Lorsque vous créez des profils d'inscription, vous leur attribuez des groupes de mise à disposition. Si un utilisateur appartient à plusieurs groupes de mise à disposition qui ont des profils d'inscription différents, le nom du groupe de mise à disposition détermine le profil d'inscription utilisé. XenMobile sélectionne le groupe de mise à disposition qui apparaît en dernier dans une liste alphabétique des groupes de mise à disposition. Pour plus d'informations, voir Profils d'inscription.

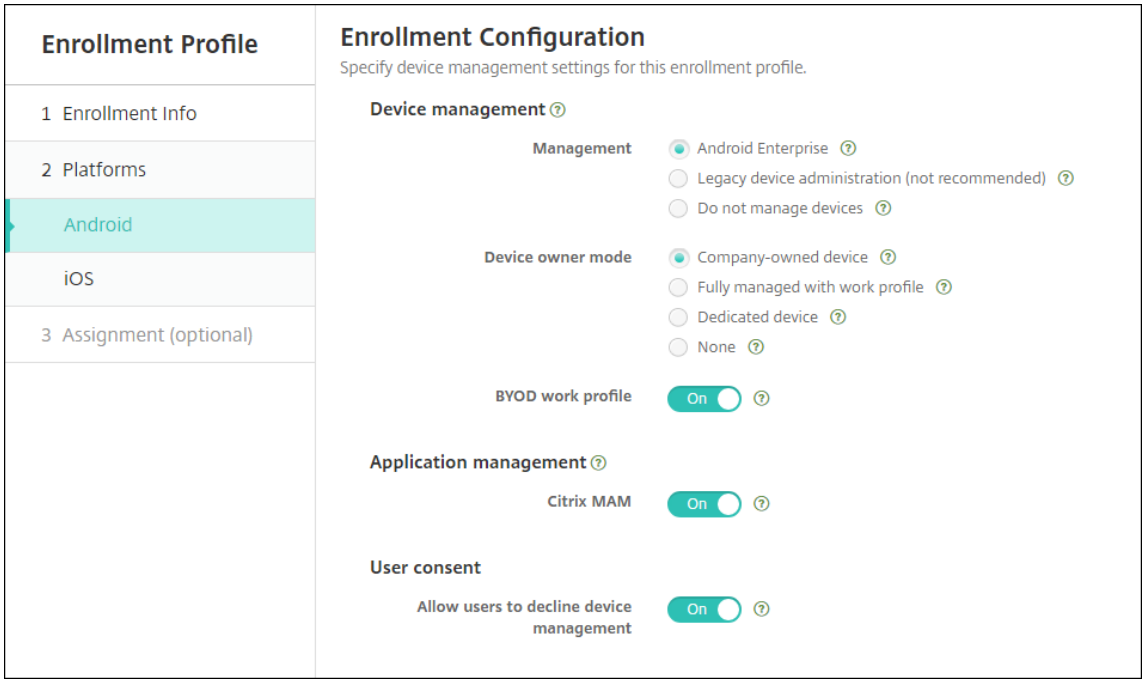
Vous pouvez utiliser des profils d'inscription pour combiner plusieurs cas d'utilisation tels que MDM exclusif, MDM+MAM et MAM exclusif. Le type de licence de XenMobile Server, indiqué dans la propriété du serveur `xms.server.mode`, détermine les paramètres disponibles dans **Configurer > Profils d'inscription**.

Ajouter un profil d'inscription pour les appareils entièrement gérés

Le profil d'inscription global inscrit les appareils entièrement gérés par défaut, mais vous pouvez créer d'autres profils d'inscription pour inscrire les appareils entièrement gérés.

1. Dans la console XenMobile, accédez à **Configurer > Profils d'inscription**.

2. Pour ajouter un profil d'inscription, cliquez sur **Ajouter**. Sur la page Infos d'inscription, entrez un nom pour le profil d'inscription.
3. Définissez le nombre d'appareils que les membres disposant de ce profil peuvent inscrire.
4. Sélectionnez **Android** sous **Plates-formes** ou cliquez sur **Suivant**. La page Configuration de l'inscription s'affiche.
5. Définissez **Gestion** sur **Android Enterprise**.
6. Définissez **Mode propriétaire de l'appareil** sur **Appareil appartenant à l'entreprise**.



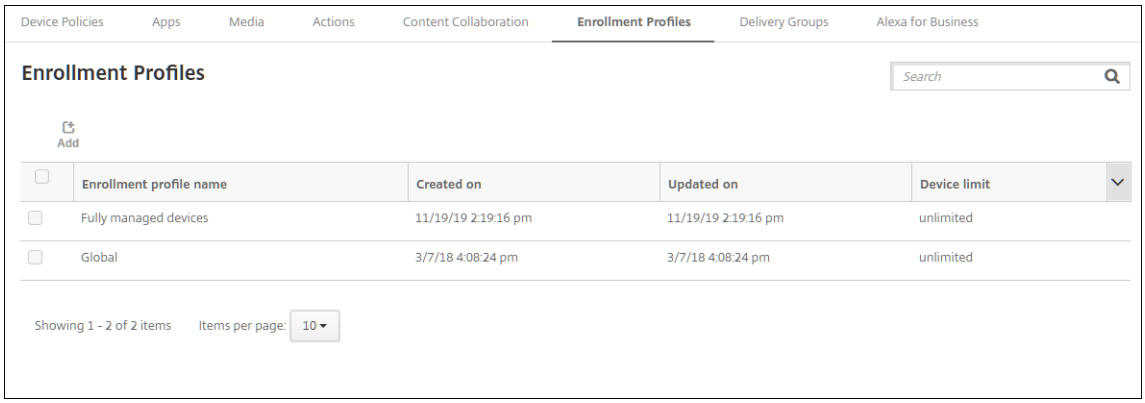
7. Le **profil de travail BYOD** vous permet de configurer le profil d'inscription pour inscrire les appareils BYOD en tant qu'appareils avec profil de travail. Les nouveaux appareils et les appareils avec réinitialisation d'usine sont inscrits en tant qu'appareils entièrement gérés.
   - Définissez le **profil de travail BYOD** sur **Activé** pour autoriser l'inscription d'appareils BYOD en tant qu'appareils avec profil de travail. La valeur par défaut est **Activé**.
   - Définissez le **profil de travail BYOD** sur **Désactivé** pour limiter l'inscription aux appareils entièrement gérés.
8. Indiquez si vous souhaitez inscrire des appareils dans Citrix MAM.
9. Si vous définissez le **profil de travail BYOD** sur **Activé**, configurez le consentement de l'utilisateur. Pour autoriser les utilisateurs d'appareils avec profil de travail BYOD à refuser la gestion des appareils lorsqu'ils inscrivent leurs appareils, définissez **Autoriser les utilisateurs à décliner la gestion des appareils** sur **Activé**.

   Si le **profil de travail BYOD** est défini sur **Activé**, la valeur par défaut pour **Autoriser les utilisateurs à décliner la gestion des appareils** est **Activé**. Si le **profil de travail BYOD** est défini

sur **Désactivé**, l'option **Autoriser les utilisateurs à décliner la gestion des appareils** est désactivée.

10. Sélectionnez **Attribution (facultatif)**. L'écran Attribution de groupes de mise à disposition s'affiche.
11. Choisissez le(s) groupe(s) de mise à disposition contenant les administrateurs qui inscrivent les appareils entièrement gérés. Cliquez ensuite sur **Enregistrer**.

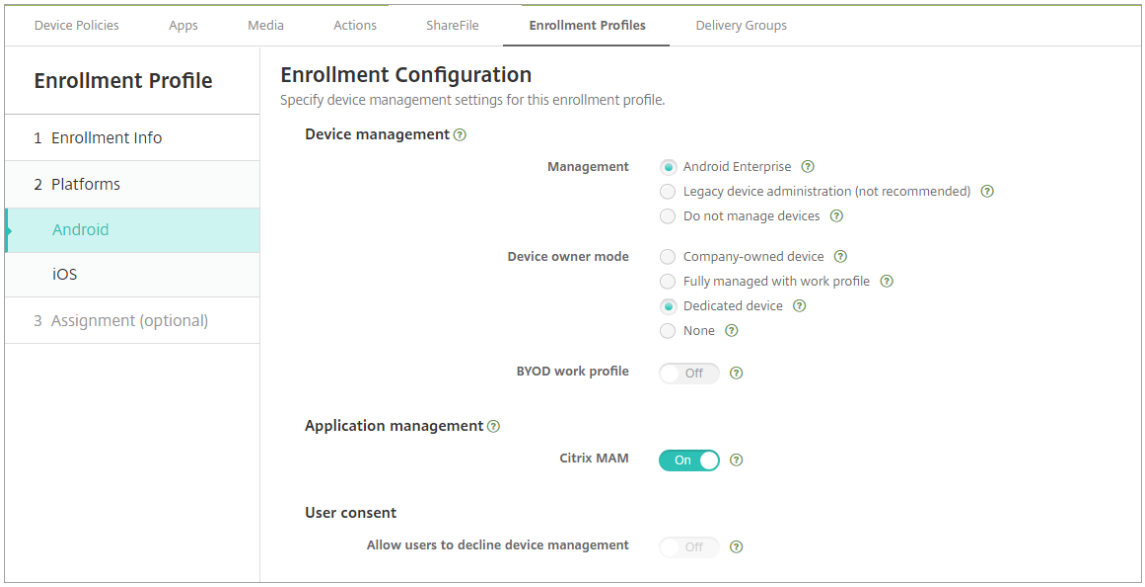
    La page Profil d'inscription apparaît avec le profil que vous avez ajouté.



Ajouter un profil d'inscription d'appareil dédié

Lorsque votre déploiement XenMobile inclut des appareils dédiés, un seul administrateur ou un groupe restreint d'administrateurs XenMobile peut inscrire de nombreux appareils dédiés. Pour vous assurer que ces administrateurs peuvent inscrire tous les appareils requis, créez un profil d'inscription pour eux avec un nombre illimité d'appareils autorisés par utilisateur.

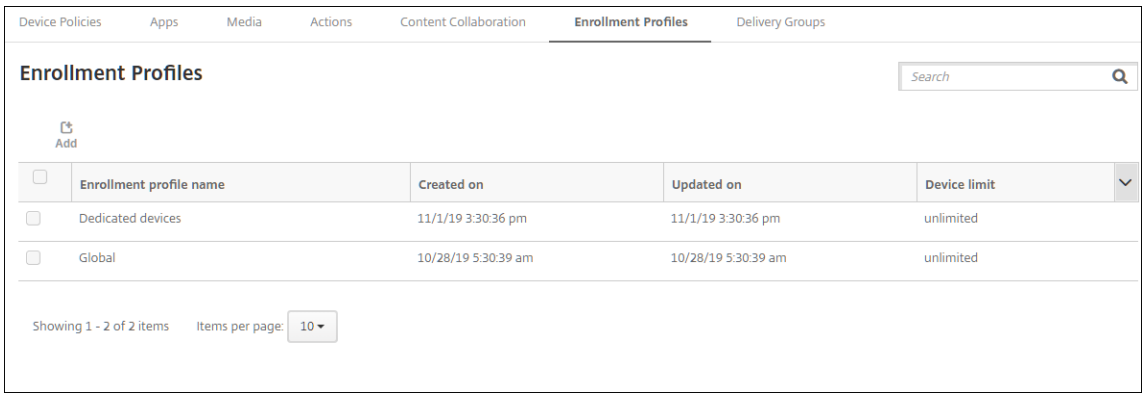
1. Dans la console XenMobile, accédez à **Configurer > Profils d'inscription**.
2. Pour ajouter un profil d'inscription, cliquez sur **Ajouter**. Sur la page Infos d'inscription, entrez un nom pour le profil d'inscription. Assurez-vous que le nombre d'appareils que les membres avec ce profil peuvent inscrire est défini sur illimité.
3. Sélectionnez **Android** sous **Plates-formes** ou cliquez sur **Suivant**. La page Configuration de l'inscription s'affiche.
4. Définissez **Gestion** sur **Android Enterprise**.
5. Définissez **Mode propriétaire de l'appareil** sur **Appareil dédié**.



6. Le **profil de travail BYOD** vous permet de configurer le profil d'inscription pour inscrire les appareils BYOD en tant qu'appareils avec profil de travail. Les nouveaux appareils et les appareils avec réinitialisation d'usine sont inscrits en tant qu'appareils dédiés. Définissez le **profil de travail BYOD** sur **Activé** pour autoriser l'inscription d'appareils BYOD en tant qu'appareils avec profil de travail. Définissez le **profil de travail BYOD** sur **Désactivé** pour limiter l'inscription aux appareils appartenant à l'entreprise. La valeur par défaut est **Activé**.
7. Indiquez si vous souhaitez inscrire des appareils dans Citrix MAM.
8. Si vous définissez le **profil de travail BYOD** sur **Activé**, configurez le consentement de l'utilisateur. Pour autoriser les utilisateurs d'appareils avec profil de travail BYOD à refuser la gestion des appareils lorsqu'ils inscrivent leurs appareils, définissez **Autoriser les utilisateurs à décliner la gestion des appareils** sur **Activé**.

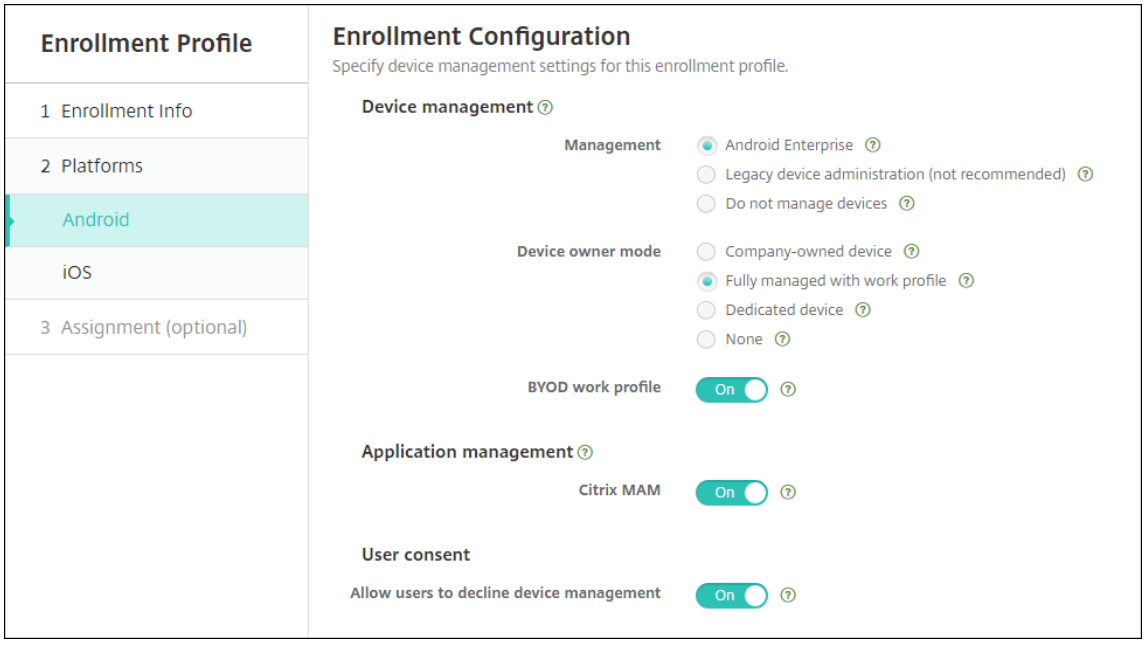
   Si le **profil de travail BYOD** est défini sur **Activé**, la valeur par défaut pour **Autoriser les utilisateurs à décliner la gestion des appareils** est **Activé**. Si le **profil de travail BYOD** est défini sur **Désactivé**, l'option **Autoriser les utilisateurs à décliner la gestion des appareils** est désactivée.
9. Sélectionnez **Attribution (facultatif)**. L'écran Attribution de groupes de mise à disposition s'affiche.
10. Choisissez le(s) groupe(s) de mise à disposition contenant les administrateurs qui inscrivent les appareils dédiés. Cliquez ensuite sur **Enregistrer**.

    La page Profil d'inscription apparaît avec le profil que vous avez ajouté.



Ajouter un profil d'inscription pour les appareils entièrement gérés avec profil de travail

1. Dans la console XenMobile, accédez à **Configurer > Profils d'inscription**.
2. Pour ajouter un profil d'inscription, cliquez sur **Ajouter**. Sur la page Infos d'inscription, entrez un nom pour le profil d'inscription.
3. Définissez le nombre d'appareils que les membres disposant de ce profil peuvent inscrire.
4. Sélectionnez **Android** sous **Plates-formes** ou cliquez sur **Suivant**. La page Configuration de l'inscription s'affiche.
5. Définissez **Gestion** sur **Android Enterprise**. Définissez **Mode propriétaire de l'appareil** sur **Entièrement géré avec profil de travail**.



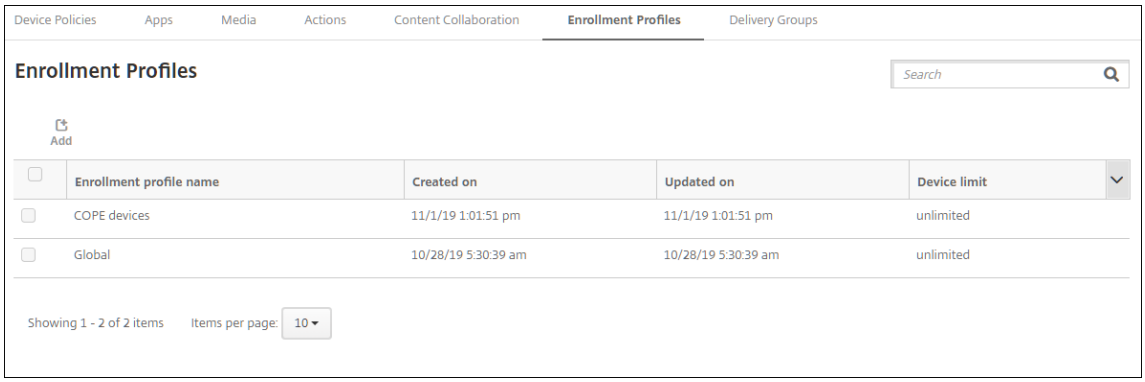
6. Le **profil de travail BYOD** vous permet de configurer le profil d'inscription pour inscrire les appareils BYOD en tant qu'appareils avec profil de travail. Les nouveaux appareils et les appareils avec réinitialisation d'usine sont inscrits en tant qu'appareils entièrement gérés avec profil de

travail. Définissez le **profil de travail BYOD** sur **Activé** pour autoriser l'inscription d'appareils BYOD en tant qu'appareils avec profil de travail. Définissez le **profil de travail BYOD** sur **Désactivé** pour limiter l'inscription aux appareils dédiés. La valeur par défaut est **Désactivé**.

7. Indiquez si vous souhaitez inscrire des appareils dans Citrix MAM.
8. Si vous définissez le **profil de travail BYOD** sur **Activé**, configurez le consentement de l'utilisateur. Pour autoriser les utilisateurs d'appareils avec profil de travail BYOD à refuser la gestion des appareils lorsqu'ils inscrivent leurs appareils, définissez **Autoriser les utilisateurs à décliner la gestion des appareils** sur **Activé**.

   Si le **profil de travail BYOD** est défini sur **Activé**, la valeur par défaut pour **Autoriser les utilisateurs à décliner la gestion des appareils** est **Activé**. Si le **profil de travail BYOD** est défini sur **Désactivé**, l'option **Autoriser les utilisateurs à décliner la gestion des appareils** est désactivée.
9. Sélectionnez **Attribution (facultatif)**. L'écran Attribution de groupes de mise à disposition s'affiche.
10. Choisissez le(s) groupe(s) de mise à disposition contenant les administrateurs qui inscrivent les appareils entièrement gérés avec un profil de travail. Cliquez ensuite sur **Enregistrer**.

    La page Profil d'inscription apparaît avec le profil que vous avez ajouté.



Ajout d'un profil d'inscription pour les appareils d'ancienne génération

Google ne va plus prendre en charge le mode administrateur de l'appareil pour la gestion des appareils. Google encourage les clients à gérer tous les appareils Android en mode propriétaire de l'appareil ou propriétaire de profil. (Consultez la section Device admin deprecation dans les guides des développeurs Google Android Enterprise.)

Pour prendre en charge ce changement :

- Citrix définit Android Enterprise comme option d'inscription par défaut pour les appareils Android.

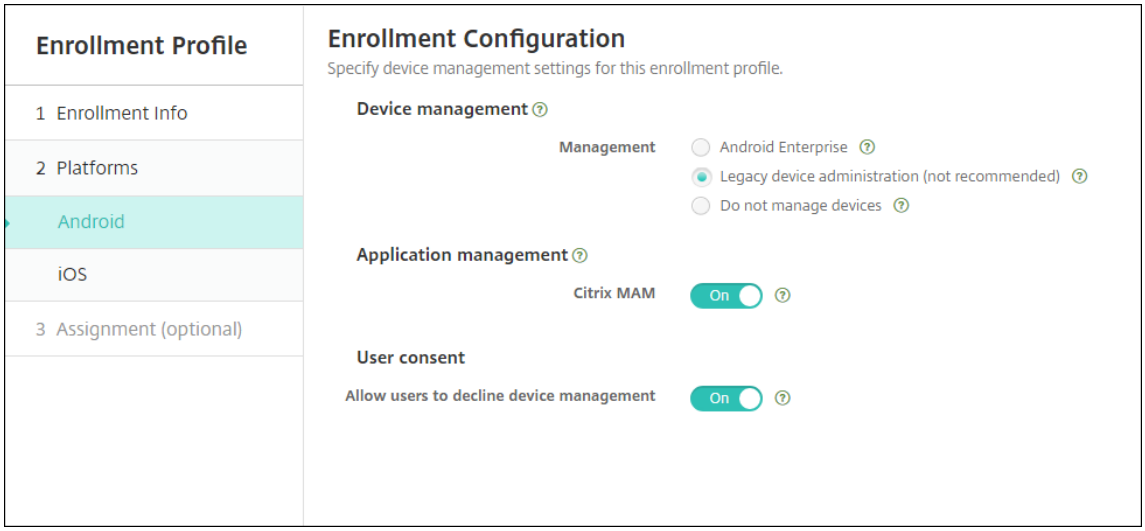
- Si Android Enterprise est activé pour votre déploiement XenMobile, tous les appareils Android nouvellement inscrits ou réinscrits le sont en tant qu'appareils Android Enterprise.

Votre organisation n'est peut-être pas prête à gérer les appareils Android d'ancienne génération à l'aide d'Android Enterprise. Dans ce cas, vous pouvez continuer à les gérer en mode Administrateur de l'appareil. Si des appareils sont déjà inscrits en mode administrateur d'appareil, XenMobile continue de les gérer en mode administrateur d'appareil.

Créez un profil d'inscription pour les appareils hérités afin de permettre aux inscriptions de nouveaux appareils Android d'utiliser le mode administrateur d'appareil.

Pour créer un profil d'inscription pour les appareils d'ancienne génération :

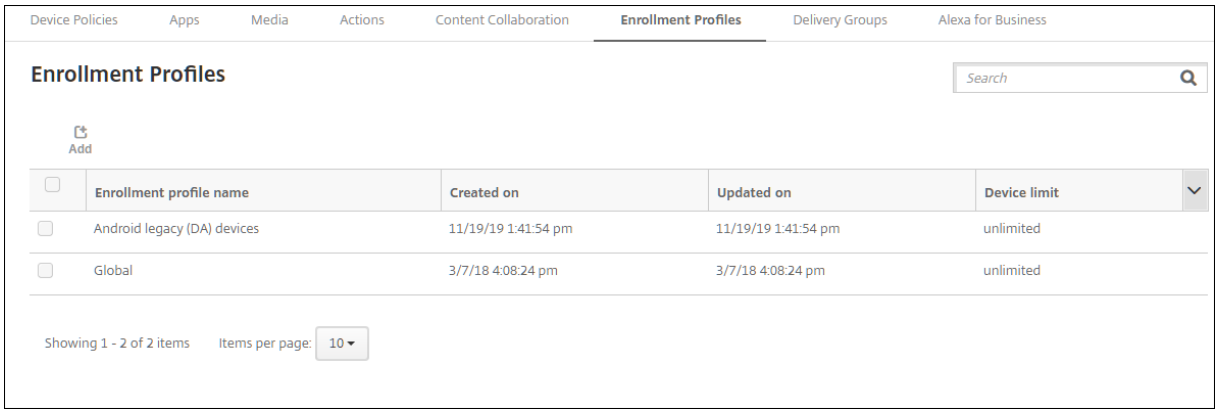
1. Dans la console XenMobile, accédez à **Configurer > Profils d'inscription**.
2. Pour ajouter un profil d'inscription, cliquez sur **Ajouter**. Sur la page Infos d'inscription, entrez un nom pour le profil d'inscription.
3. Définissez le nombre d'appareils que les membres disposant de ce profil peuvent inscrire.
4. Sélectionnez **Android** sous **Plates-formes** ou cliquez sur **Suivant**. La page Configuration de l'inscription s'affiche.
5. Définissez **Gestion** sur **Administration des appareils d'ancienne génération (non recommandé)**. Cliquez sur **Suivant**.



6. Indiquez si vous souhaitez inscrire des appareils dans Citrix MAM.
7. Pour autoriser les utilisateurs à refuser la gestion des appareils lorsqu'ils inscrivent leurs appareils, définissez **Autoriser les utilisateurs à décliner la gestion des appareils** sur **Activé**. La valeur par défaut est **Activé**.
8. Sélectionnez **Attribution (facultatif)**. L'écran Attribution de groupes de mise à disposition s'affiche.

9. Choisissez le(s) groupe(s) de mise à disposition contenant les administrateurs qui inscrivent les appareils dédiés. Cliquez ensuite sur **Enregistrer**.

La page Profil d'inscription apparaît avec le profil que vous avez ajouté.



Pour continuer à gérer les appareils d'ancienne génération en mode Administrateur de l'appareil, inscrivez-les ou réinscrivez-les à l'aide de ce profil. Inscrivez les appareils en mode Administrateur de l'appareil de la même manière que les appareils en mode Profil de travail, en demandant aux utilisateurs de télécharger Secure Hub et en fournissant une URL de serveur d'inscription.

Provisioning d'appareils Android Enterprise avec profil de travail

Les appareils Android Enterprise avec profil de travail sont inscrits en mode Propriétaire du profil. Ces appareils n'ont pas besoin d'être neufs ou réinitialisés en usine. Les appareils BYOD sont inscrits en tant qu'appareils avec profil de travail. L'expérience d'inscription est similaire à l'inscription Android dans XenMobile. Les utilisateurs téléchargent Secure Hub depuis Google Play et inscrivent leurs appareils.

Par défaut, les paramètres **Débogage USB et Sources inconnues** sont désactivés sur un appareil lorsqu'il est inscrit en mode Profil de travail dans Android Enterprise.

Lors de l'inscription d'appareils dans Android Enterprise en tant qu'appareils avec profil de travail, accédez toujours à Google Play. De là, activez l'affichage de Secure Hub dans le profil personnel de l'utilisateur.

Provisionner des appareils Android Enterprise entièrement gérés

Vous pouvez inscrire des appareils entièrement gérés dans le déploiement que vous avez configuré dans les sections précédentes. Les appareils entièrement gérés sont des appareils appartenant à l'entreprise et sont inscrits en mode Propriétaire de l'appareil. Seuls les appareils neufs ou qui ont fait l'objet d'une réinitialisation d'usine peuvent être inscrits en mode Propriétaire de l'appareil.

Vous pouvez inscrire des appareils en mode Propriétaire de l'appareil à l'aide de l'une des méthodes d'inscription suivantes :

- **Jeton d'identification DPC :** cette méthode d'inscription permet aux utilisateurs de saisir les caractères `afw##xenmobile` lors de la configuration de l'appareil. `afw##xenmobile` représente le jeton d'identification DPC Citrix. Ce jeton identifie l'appareil comme étant géré par XenMobile et télécharge Secure Hub depuis Google Play Store. Consultez Inscription d'appareils à l'aide du jeton d'identificateur DPC Citrix.
- **Partage de données à l'aide de NFC :** la méthode d'inscription à l'aide du partage NFC permet de transférer des données entre deux appareils en utilisant une communication en champ proche. Bluetooth, Wi-Fi et les autres modes de communication sont désactivés sur un nouvel appareil ou un appareil dont les paramètres d'usine ont été réinitialisés. NFC est le seul protocole de communication que l'appareil peut utiliser dans cet état. Consultez Inscription d'appareils à l'aide du partage NFC.
- **Code QR :** l'inscription à l'aide d'un code QR permet d'inscrire une flotte distribuée d'appareils qui ne prennent pas en charge la technologie NFC, tels que les tablettes. La méthode d'inscription à l'aide d'un code QR permet de configurer le mode Profil de l'appareil en scannant un code QR depuis l'assistant d'installation. Consultez Inscription d'appareils à l'aide d'un code QR.
- **Inscription sans contact :** l'inscription sans contact vous permet de configurer les appareils pour qu'ils s'inscrivent automatiquement lorsqu'ils sont mis sous tension pour la première fois. L'inscription sans contact est prise en charge sur certains appareils Android exécutant Android 8.0 ou version ultérieure. Consultez Inscription sans contact.
- **Comptes Google :** les utilisateurs saisissent leurs informations d'identification de compte Google pour lancer le processus de provisioning. Cette option est destinée aux entreprises utilisant Google Workspace.

Inscription d'appareils à l'aide du jeton d'identificateur DPC Citrix

Les utilisateurs entrent `afw##xenmobile` lorsqu'ils sont invités à entrer un compte Google après avoir mis sous tension un nouvel appareil ou un appareil ayant fait l'objet d'une réinitialisation d'usine lors de la configuration initiale. Cette action télécharge et installe Secure Hub. Les utilisateurs suivent les invites de configuration de Secure Hub pour terminer l'inscription.

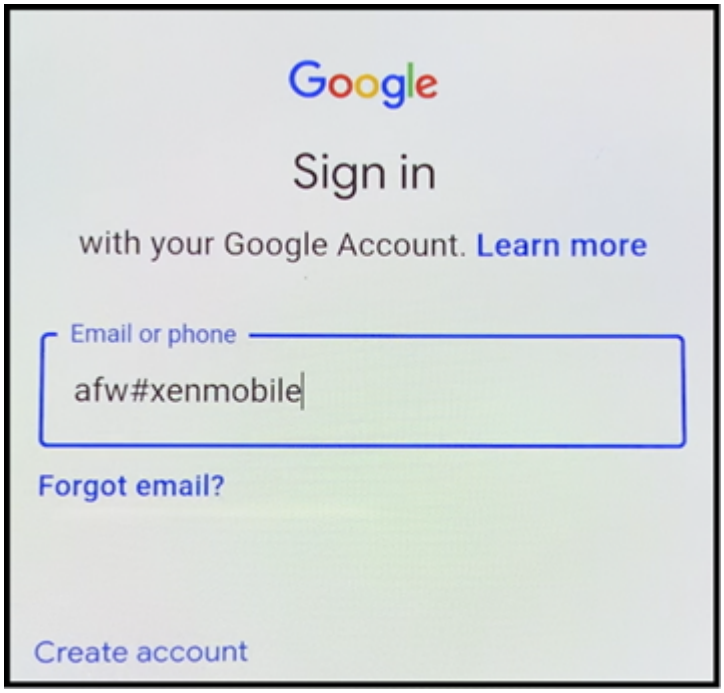
Cette méthode d'inscription est recommandée pour la plupart des clients car la dernière version de Secure Hub est téléchargée à partir de Google Play Store. Contrairement aux autres méthodes d'inscription, vous ne pouvez pas télécharger Secure Hub depuis XenMobile Server.

Configuration système requise

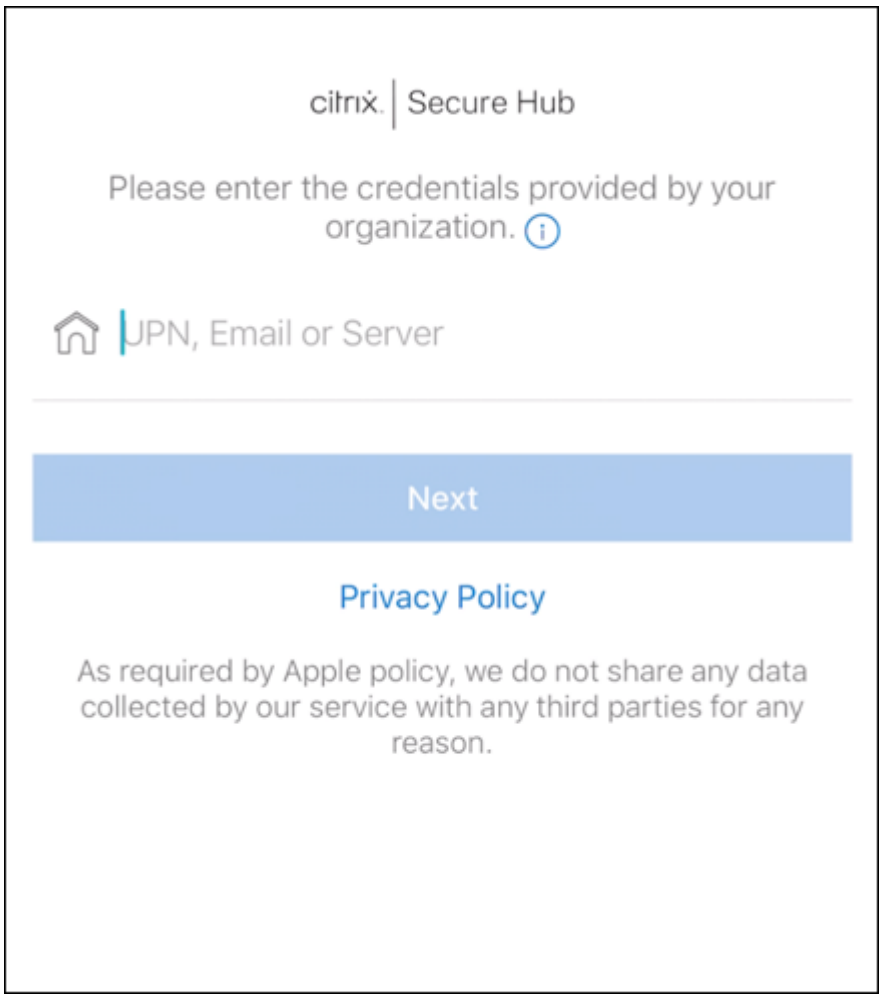
- Pris en charge sur tous les appareils Android exécutant Android OS.

Pour inscrire l'appareil

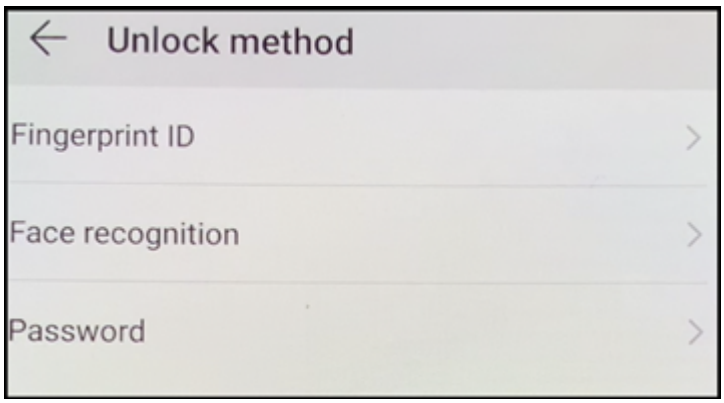
1. Mettez sous tension un nouvel appareil ou un appareil ayant fait l'objet d'une réinitialisation d'usine.
2. La configuration initiale de l'appareil s'affiche et vous invite à créer un compte Google. Si l'appareil affiche l'écran d'accueil, vérifiez dans la barre de notification une notification indiquant **Terminer la configuration**.
3. Entrez `afw##xenmobile` dans le champ **Adresse e-mail ou numéro de téléphone**.



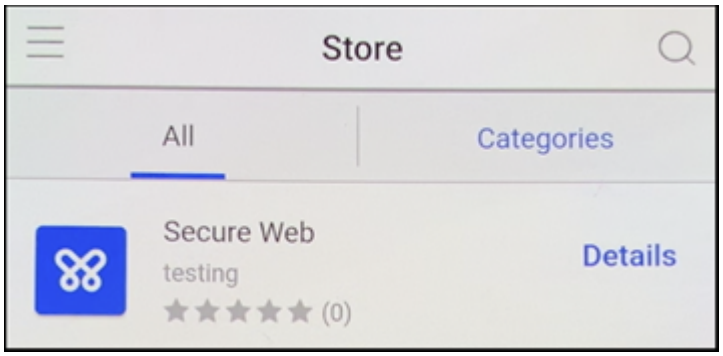
4. Touchez **Installer** sur l'écran Android Enterprise vous invitant à installer Secure Hub.
5. Touchez **Installer** sur l'écran du programme d'installation de Secure Hub.
6. Touchez **Autoriser** pour toutes les demandes d'autorisation d'application.
7. Touchez **Accepter et continuer** pour installer Secure Hub et lui permettre de gérer l'appareil.
8. Secure Hub est maintenant installé et s'affiche sur l'écran d'inscription par défaut. Dans cet exemple, la détection automatique n'est pas configurée. Si c'est le cas, lorsque l'utilisateur entre son nom d'utilisateur et son adresse e-mail, un serveur est automatiquement identifié. Entrez plutôt l'URL d'inscription de l'environnement et touchez **Suivant**.



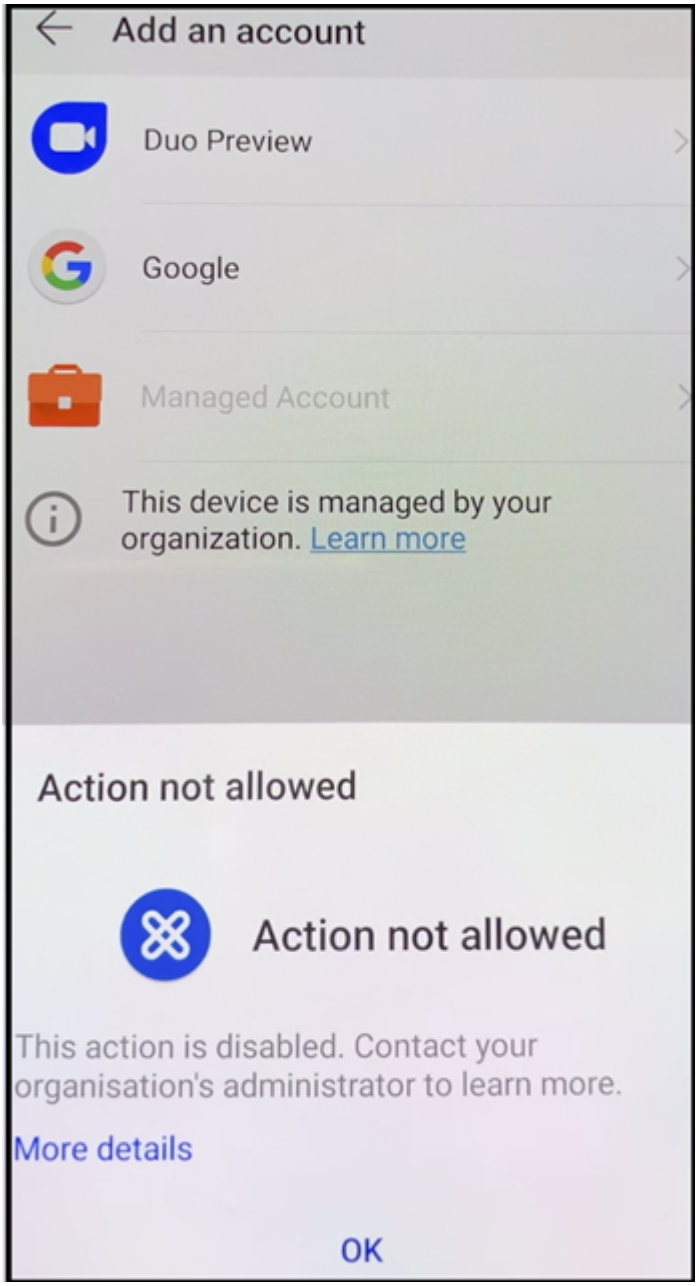
9. La configuration par défaut de XenMobile permet aux utilisateurs de choisir s'ils utilisent MAM ou MDM+MAM. Si vous y êtes invité, touchez **Oui, inscrire** pour choisir MDM+MAM.
10. Entrez le nom d'utilisateur et le mot de passe, puis touchez **Suivant**.
11. L'utilisateur est invité à configurer un code secret pour l'appareil. Touchez **Définir** et saisissez un code secret.
12. L'utilisateur est invité à configurer une méthode de déverrouillage pour le profil de travail. Pour cet exemple, touchez **Mot de passe**, **Code PIN** et saisissez un code PIN.



13. L'appareil se trouve maintenant sur l'écran d'accueil **Mes applications** de Secure Hub. Touchez **Ajouter des applications depuis le magasin**.
14. Pour ajouter Secure Web, touchez **Secure Web**.



15. Touchez **Ajouter**.
16. Secure Hub dirige l'utilisateur vers Google Play Store pour installer Secure Web. Touchez **Installer**.
17. Après l'installation de Secure Web, touchez **Ouvrir**. Entrez une URL d'un site interne dans la barre d'adresse et vérifiez que la page se charge.
18. Accédez à **Paramètres > Comptes** sur l'appareil. Notez que le **compte géré** ne peut pas être modifié. Les options destinées aux développeurs, telles que le partage d'écran ou le débogage à distance, sont également bloquées.



Inscription d'appareils à l'aide du partage NFC

Pour inscrire un appareil en tant qu'appareil entièrement géré à l'aide du partage NFC, deux appareils sont requis : un dont les paramètres d'usine ont été rétablis et un exécutant l'application XenMobile Provisioning Tool.

Configuration système requise et conditions préalables

- Appareils Android pris en charge

- Un nouvel appareil ou un appareil dont les paramètres d'usine ont été rétablis, provisionné pour Android Enterprise en tant qu'appareil entièrement géré. Les étapes à suivre pour satisfaire ces conditions préalables sont disponibles plus loin dans cet article.
- Un autre appareil avec capacité NFC, exécutant l'application Provisioning Tool configurée. Provisioning Tool est disponible dans Secure Hub ou sur la page des téléchargements de Citrix.

Chaque appareil ne peut avoir qu'un seul profil Android Enterprise, géré par Secure Hub. Un seul profil est autorisé sur chaque appareil. La tentative d'ajout d'une deuxième application DPC supprime le Secure Hub installé.

Données transférées via le partage NFC

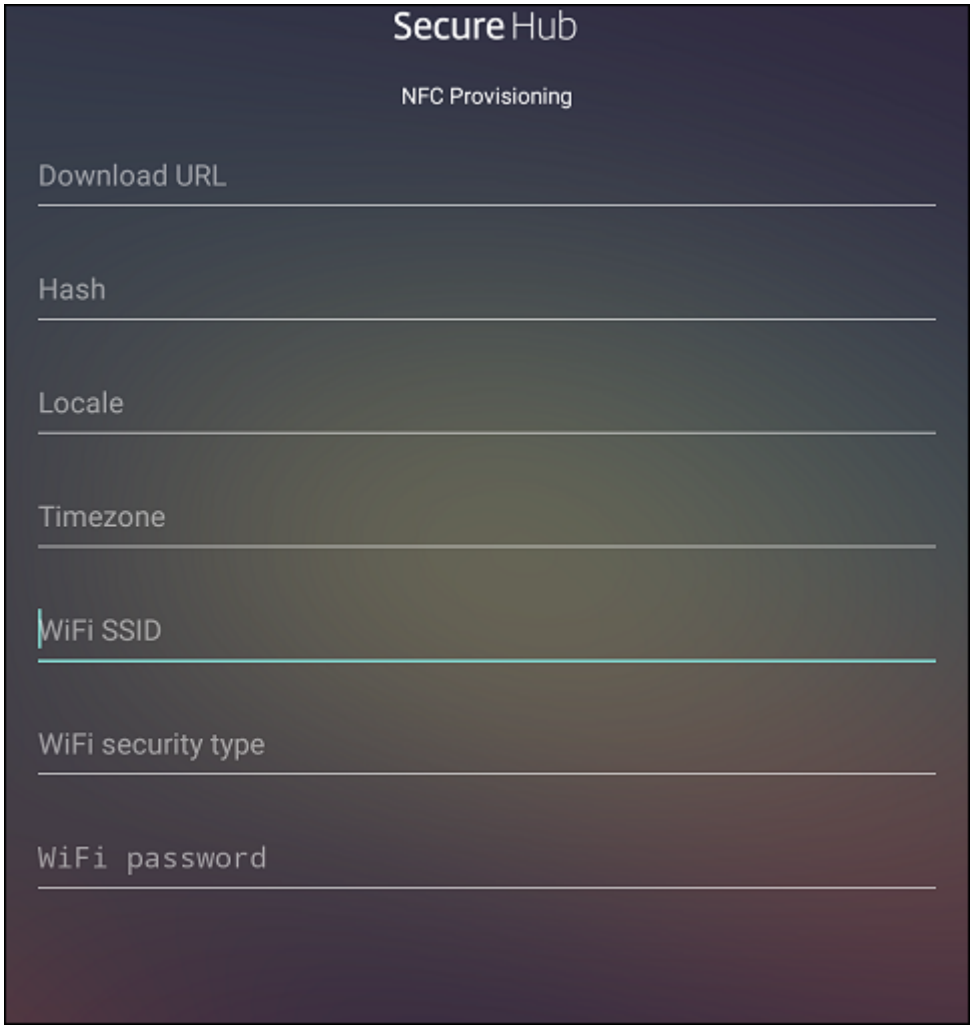
Le provisioning d'un appareil dont les paramètres d'usine ont été rétablis requiert l'envoi des données suivantes via NFC pour initialiser Android Enterprise :

- Nom du package de l'application DPC qui fait office de propriétaire de l'appareil (dans ce cas, Secure Hub).
- Emplacement intranet/Internet à partir duquel l'appareil peut télécharger l'application DPC.
- Hachage SHA1 de l'application DPC pour vérifier que le téléchargement a réussi.
- Détails de la connexion Wi-Fi de façon à ce qu'un appareil dont les paramètres d'usine ont été réinitialisés puisse se connecter et télécharger l'application DPC. Remarque : Android ne prend pas charge 802.1x Wi-Fi pour cette étape.
- Fuseau horaire de l'appareil (facultatif).
- Emplacement géographique de l'appareil (facultatif).

Lorsque les deux appareils sont « cognés », les données de Provisioning Tool sont envoyées à l'appareil dont les paramètres d'usine ont été réinitialisés. Ces données sont ensuite utilisées pour télécharger Secure Hub avec des paramètres d'administrateur. Si vous ne précisez pas le fuseau horaire ni l'emplacement, Android les configure automatiquement sur le nouvel appareil.

Configuration de XenMobile Provisioning Tool

Avant de partager des données avec NFC, vous devez configurer Provisioning Tool. Cette configuration est ensuite transférée à l'appareil dont les paramètres d'usine ont été réinitialisés durant le partage des données avec NFC.



Vous pouvez entrer des données dans les champs requis ou les renseigner via un fichier texte. Les étapes de la procédure suivante décrivent comment configurer le fichier texte et contiennent des descriptions pour chaque champ. L'application n'enregistre pas les informations après qu'elles soient entrées, il peut donc s'avérer utile de créer un fichier texte afin de conserver les informations pour une utilisation ultérieure.

Pour configurer le Provisioning Tool à l'aide d'un fichier texte

Appelez le fichier nfcprovisioning.txt et placez-le dans le dossier `/sdcard/` sur la carte SD de l'appareil. Cela permet à l'application de lire le fichier texte et renseigner les valeurs.

Le fichier texte doit contenir les données suivantes :

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

Il s'agit de l'emplacement intranet/Internet de l'application EMM du fournisseur. Après que l'appareil dont les paramètres d'usine ont été réinitialisés se soit connecté au Wi-Fi suite au partage NFC, il doit

avoir accès à cet emplacement pour le téléchargement. L'adresse URL est une adresse URL standard qui ne requiert aucun formatage spécial.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>
```

Il s'agit de la somme de contrôle de l'application EMM du fournisseur. Elle est utilisée pour vérifier que le téléchargement a réussi. Les étapes à suivre pour obtenir la somme de contrôle sont abordées plus loin dans cet article.

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

Cette ligne est le SSID Wi-Fi connecté de l'appareil sur lequel Provisioning Tool est exécuté.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

Les valeurs prises en charge sont WEP et WPA2. Si le Wi-Fi n'est pas protégé, ce champ doit être vide.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

Si le Wi-Fi n'est pas protégé, ce champ doit être vide.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

Entrez un code de langue et de pays. Les codes de langue sont des codes ISO de deux lettres minuscules (tels que fr) comme défini dans l'ISO 639-1. Les codes de pays sont des codes ISO de deux lettres majuscules (tels que FR) comme défini dans l'ISO 3166-1. À titre d'exemple, entrez fr_FR pour la langue française parlée en France. Si vous n'entrez aucun code, la langue et le pays sont automatiquement renseignés.

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

Fuseau horaire dans lequel l'appareil est exécuté. Entrez un nom basé sur la base de données Olson au format zone/emplacement. Par exemple, Europe/Paris pour l'heure de l'Europe occidentale. Si vous n'entrez rien, le fuseau horaire est automatiquement renseigné.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

Ces données ne pas requises car la valeur est codée en dur dans l'application Secure Hub. Il n'est mentionné ici que par souci de complétude.

Si un accès protégé Wi-Fi WPA2 est utilisé, un fichier nfcprovisioning.txt peut ressembler à ce qui suit :

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
```



```
android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Si un accès non protégé Wi-Fi est utilisé, un fichier nfcprovisioning.txt peut ressembler à ce qui suit :

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Pour obtenir la somme de contrôle de Citrix Secure Hub

La somme de contrôle de Secure Hub est une valeur constante : `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT`
`-yKM`. Pour télécharger un fichier APK pour Secure Hub, utilisez le lien suivant de Google Play Store :
`https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

Pour obtenir une somme de contrôle d'application

Pré-requis :

- L'outil **apksigner** de l'Android SDK Build Tools
- Ligne de commande OpenSSL

Pour obtenir la somme de contrôle d'une application, procédez comme suit :

1. Téléchargez le fichier APK de l'application depuis le Google Play Store.
2. Dans la ligne de commande OpenSSL, accédez à l'outil **apksigner** : `android-sdk/build-tools/<version>/apksigner` et tapez ce qui suit :

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if
   m{
 (?<=SHA-256 digest:) .* }
 '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
<!--NeedCopy-->
```

   La commande renvoie une somme de contrôle valide.

3. Pour générer le code QR, saisissez la somme de contrôle dans le champ `PROVISIONING_DEVICE_ADMIN_SI`
   . Par exemple :


```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.
     zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"
     qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.
     PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://
     play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"
    }

 }

<!--NeedCopy-->
```

Bibliothèques utilisées

Provisioning Tool utilise les bibliothèques suivantes dans son code source :

- Bibliothèque v7 `appcompat`, bibliothèque Design Support et bibliothèque v7 Palette par Google sous licence Apache 2.0

  Pour plus d'informations, consultez le Guide des fonctionnalités de la bibliothèque de support.

- Butter Knife par Jake Wharton sous licence Apache 2.0

Inscription d'appareils à l'aide d'un code QR

Pour inscrire un appareil entièrement géré à l'aide d'un code QR, générez un code QR en créant un fichier JSON et en convertissant le fichier JSON en un code QR. Le code QR est scanné par l'appareil photo de l'appareil pour inscrire l'appareil.

Configuration système requise

- Pris en charge sur tous les appareils Android exécutant Android 8.0 et supérieur.

Créer un code QR à partir d'un JSON

Créez un JSON avec les champs suivants.

Ces champs sont obligatoires :

Clé : android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

Valeur : com.zenprise/com.zenprise.configuration.AdminFunction

Clé : android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

Valeur : qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Clé : android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

Valeur : `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

Ces champs sont facultatifs :

- **android.app.extra.PROVISIONING_LOCALE :** entrez un code de langue et de pays.

  Les codes de langue sont des codes ISO de deux lettres minuscules (tels que fr) comme défini dans l'ISO 639-1. Les codes de pays sont des codes ISO de deux lettres majuscules (tels que FR) comme défini dans l'ISO 3166-1. À titre d'exemple, entrez fr_FR pour la langue française parlée en France.

- **android.app.extra.PROVISIONING_TIME_ZONE :** fuseau horaire dans lequel l'appareil est exécuté.

  Entrez un nom basé sur la base de données Olson au format zone/emplacement. Par exemple, Europe/Paris pour l'heure de l'Europe occidentale. Si vous n'entrez rien, le fuseau horaire est automatiquement renseigné.

- **android.app.extra.PROVISIONING_LOCAL_TIME :** durée en millisecondes depuis l'heure Unix.

  L'heure Unix (également appelée heure POSIX ou Unix timestamp) est le nombre de secondes écoulées depuis le 1er janvier 1970 (minuit UTC/GMT). L'heure n'inclut pas les secondes intercalaires (dans ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION :** définissez cette option sur **true** pour ignorer le cryptage lors de la création du profil. Définissez cette option sur **false** pour forcer le cryptage lors de la création du profil.

Un fichier JSON typique ressemble à ce qui suit :

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

Validez le fichier JSON créé à l'aide de n'importe quel outil de validation JSON, tel que https://jsonlint.com. Convertissez cette chaîne JSON en un code QR à l'aide de n'importe quel générateur de code QR, tel que https://www.qr-code-generator.com.

Ce code QR est scanné par un appareil dont les paramètres d'usine ont été réinitialisés pour inscrire l'appareil en tant qu'appareil entièrement géré.

Pour inscrire l'appareil

Après la mise sous tension d'un nouvel appareil ou d'un appareil ayant fait l'objet d'une réinitialisation d'usine, procédez comme suit :

1. Touchez l'écran 6 fois sur l'écran d'accueil pour lancer le flux d'inscription du code QR.
2. Lorsque vous y êtes invité, connectez-vous au Wi-Fi. L'emplacement de téléchargement de Secure Hub dans le code QR (codé dans le JSON) est accessible sur ce réseau Wi-Fi.

   Une fois que l'appareil se connecte au Wi-Fi, il télécharge un lecteur de code QR à partir de Google et lance l'appareil photo.
3. Pointez l'appareil photo sur le code QR pour scanner le code.

   Android télécharge Secure Hub à partir de l'emplacement de téléchargement dans le code QR, valide la signature du certificat de signature, installe Secure Hub et le définit comme propriétaire de l'appareil.

Pour plus d'informations, consultez ce guide Google destiné aux développeurs Android EMM : https://developers.google.com/android/work/prov-devices#qr_code_method.

Inscription sans contact

L'inscription sans contact vous permet de configurer les appareils pour qu'ils soient provisionnés en tant qu'appareils entièrement gérés lorsqu'ils sont mis sous tension pour la première fois.

Votre revendeur d'appareils vous crée un compte sur le portail d'inscription sans contact Android, un outil en ligne qui vous permet d'appliquer des configurations aux appareils. À l'aide du portail d'inscription sans contact Android, vous créez une ou plusieurs configurations d'inscription sans contact et appliquez les configurations aux appareils attribués à votre compte. Lorsque vos utilisateurs mettent ces appareils sous tension, ils sont automatiquement inscrits dans XenMobile. La configuration attribuée à l'appareil définit son processus d'inscription automatique.

Configuration système requise

- La prise en charge de l'inscription sans contact est disponible à partir de Android 8.0.

Appareils et informations de compte provenant de votre revendeur

- Les appareils pouvant bénéficier de l'inscription sans contact sont achetés auprès d'un revendeur d'entreprise ou d'un partenaire Google. Pour obtenir la liste des partenaires Android Enterprise prenant en charge l'inscription sans contact, consultez le site Web Android.
- Un compte provenant du portail d'inscription sans contact Android Enterprise, créé par votre revendeur.
- Des informations de connexion au compte du portail d'inscription sans contact Android Enterprise, fournies par votre revendeur.

Créer une configuration sans contact

Lorsque vous créez une configuration sans contact, incluez un fichier JSON personnalisé pour spécifier les détails de la configuration.

Utilisez ce fichier JSON pour configurer l'appareil à inscrire sur XenMobile Server que vous spécifiez. Remplacez l'URL de votre serveur par « URL » dans cet exemple.

```
1        {
2
3            "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6                "serverURL":"URL",
7            }
8
9         }
10
11 <!--NeedCopy-->
```

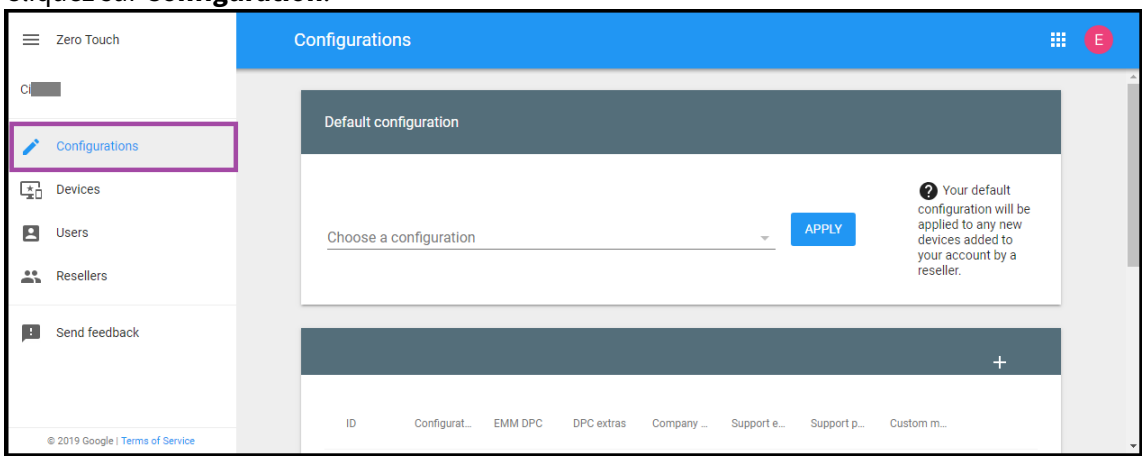
Vous pouvez utiliser un fichier JSON facultatif avec plus de paramètres pour personnaliser davantage votre configuration. Cet exemple spécifie XenMobile Server, ainsi que le nom d'utilisateur et le mot de passe que les appareils configurés utilisent pour ouvrir une session sur le serveur.

```
1       {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4            {
5
6                "serverURL":"URL",
7                "xm_username":"username",
8                "xm_password":"password"
9             }
10
11              }
```

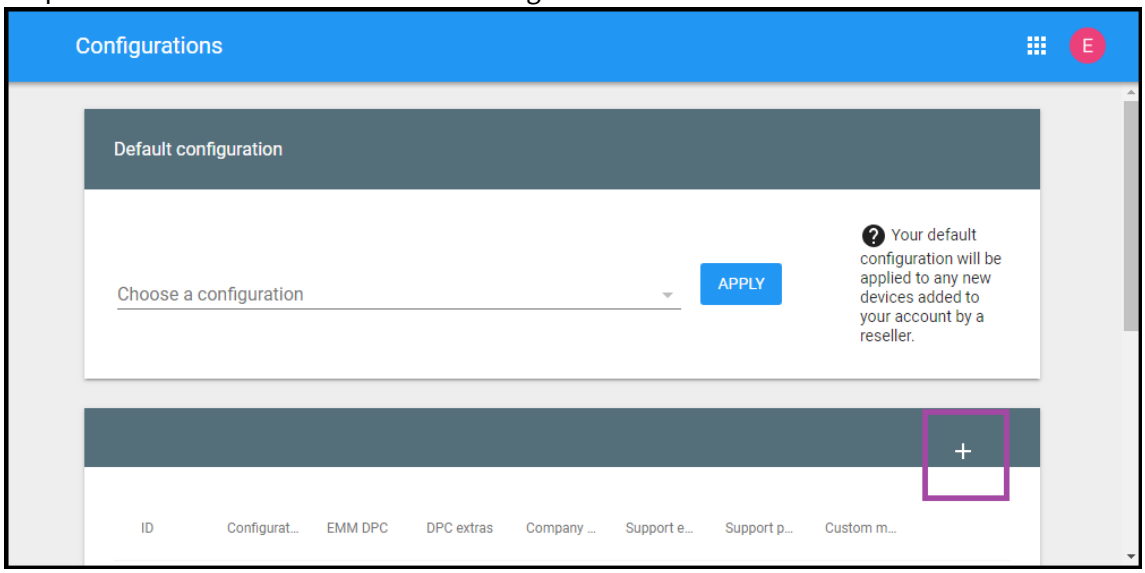


```
12
13    <!--NeedCopy-->
```

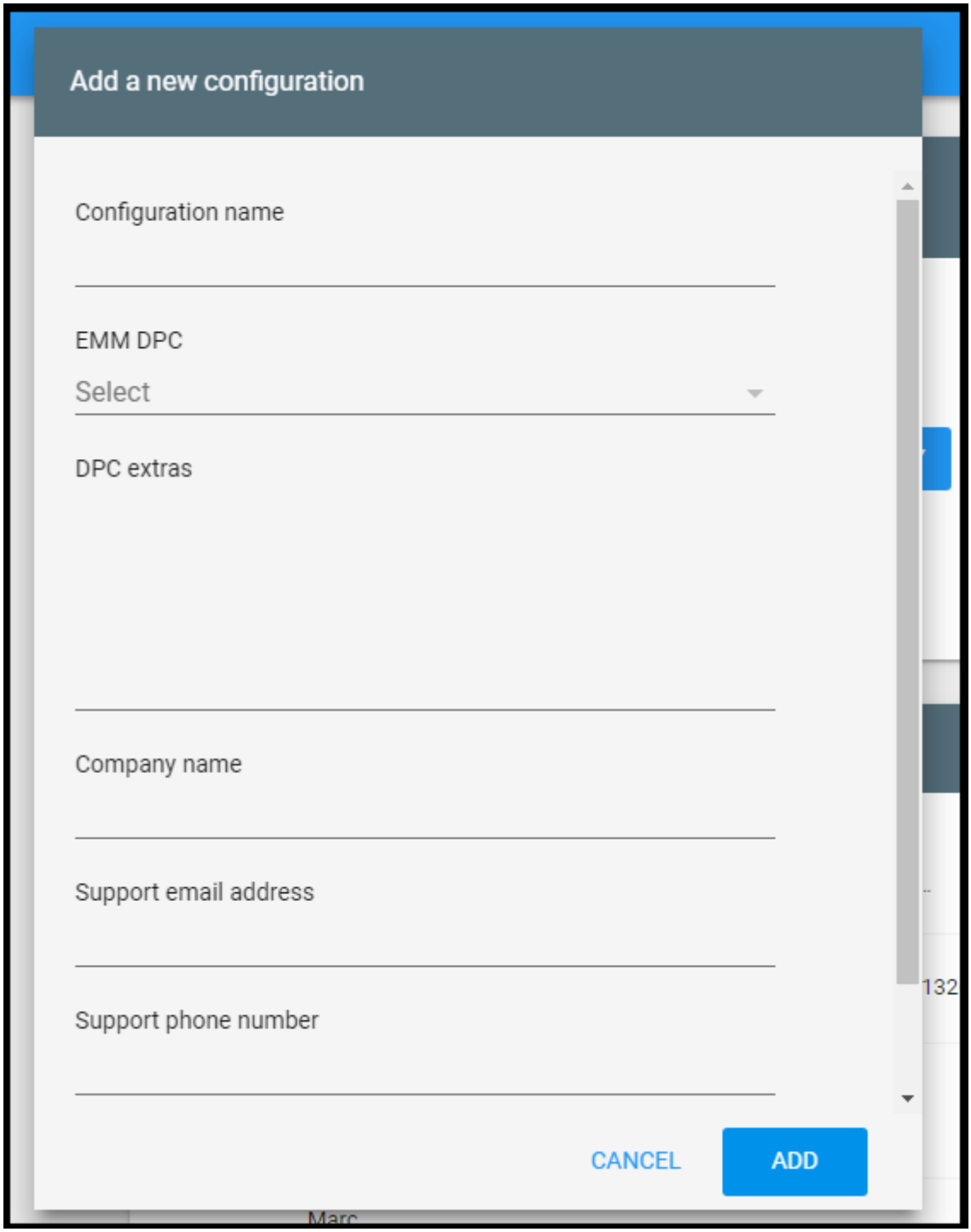
1. Accédez au portail d'inscription sans contact Android à l'adresse https://partner.android.com/zerotouch. Connectez-vous avec les informations de compte provenant de votre revendeur d'appareils sans contact.
2. Cliquez sur **Configuration**.



3. Cliquez sur **+** au-dessus du tableau de configuration.



4. Entrez vos informations de configuration dans la fenêtre de configuration qui s'affiche.

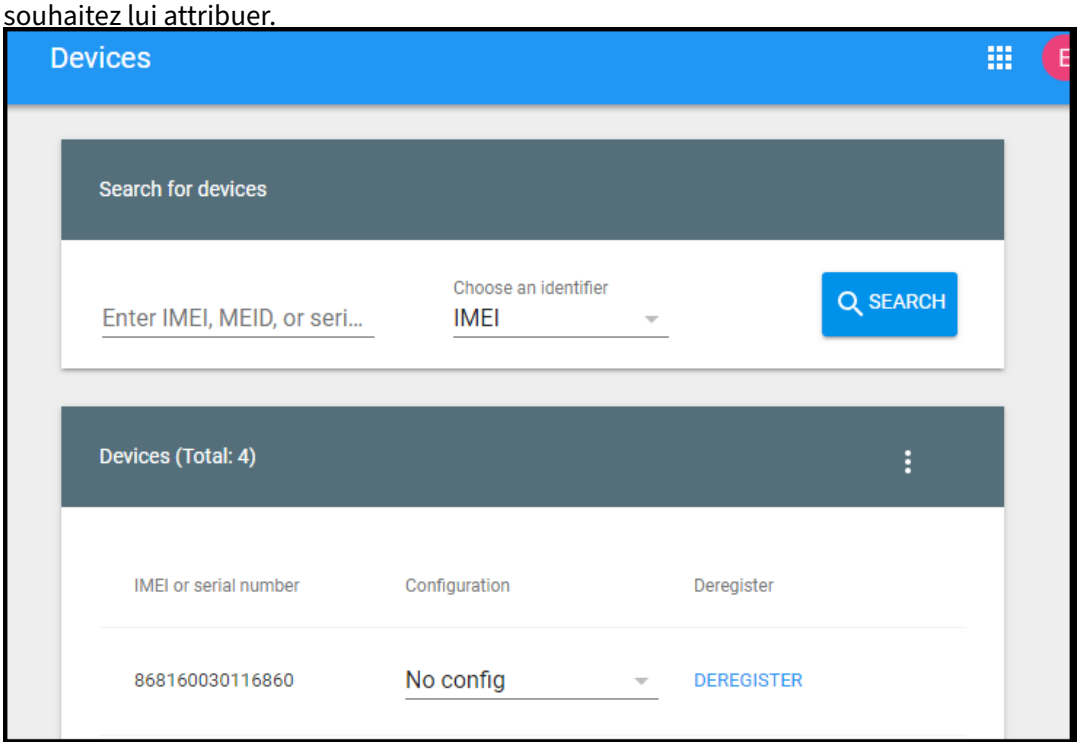


- **Configuration name :** saisissez le nom que vous avez choisi pour cette configuration.
- **EMM DPC :** choisissez **Citrix Secure Hub**.
- **DPC extras :** collez votre texte JSON personnalisé dans ce champ.
- **Company name :** saisissez le nom que vous souhaitez afficher sur vos appareils sans contact Android Enterprise pendant le provisioning de l'appareil.
- **Support email address :** saisissez une adresse e-mail que vos utilisateurs peuvent con-

tacter pour obtenir de l'aide. Cette adresse apparaît sur vos appareils sans contact Android Enterprise avant le provisioning de l'appareil.

- **Support phone number :** saisissez un numéro de téléphone que vos utilisateurs peuvent contacter pour obtenir de l'aide. Ce numéro de téléphone apparaît sur vos appareils sans contact Android Enterprise avant le provisioning de l'appareil.
- **Custom Message :** si vous le souhaitez, ajoutez une ou deux phrases pour aider vos utilisateurs à vous contacter ou leur donner plus de détails sur l'état de leur appareil. Ce message personnalisé apparaît sur vos appareils sans contact Android Enterprise avant le provisioning de l'appareil.

5. Cliquez sur **Ajouter**.
6. Pour créer des configurations supplémentaires, répétez les étapes 2 à 4.
7. Pour appliquer une configuration à un appareil, procédez comme suit :
   a) Dans le portail d'inscription sans contact Android, cliquez sur **Devices**.
   b) Recherchez l'appareil dans la liste des appareils et choisissez la configuration que vous souhaitez lui attribuer.



   c) Cliquez sur **Update**.

Vous pouvez appliquer une configuration à de nombreux appareils à l'aide d'un fichier CSV.

Pour plus d'informations sur l'application d'une configuration à de nombreux appareils, consultez la rubrique d'aide Android Enterprise Inscription sans contact pour les administrateurs informatiques. Cette rubrique d'aide d'Android Enterprise contient plus d'informations sur la façon de gérer les con-

figurations et de les appliquer aux appareils.

Provisionner des appareils Android Enterprise dédiés

Les appareils Android Enterprise dédiés sont des appareils entièrement gérés qui ne remplissent qu'une seule fonction. Les appareils dédiés sont également connus sous le nom d'appareils d'entreprise à usage unique (appareils COSU). En effet, vous limitez ces appareils à une application ou à un petit ensemble d'applications nécessaires pour effectuer les tâches propres à une fonction. Vous pouvez également empêcher les utilisateurs d'activer d'autres applications ou d'effectuer d'autres actions sur l'appareil.

Inscrivez les appareils dédiés à l'aide de l'une des méthodes d'inscription utilisées pour d'autres appareils entièrement gérés, comme décrit dans la section Provisionner des appareils Android Enterprise entièrement gérés. Le provisioning d'appareils dédiés nécessite une configuration supplémentaire avant l'inscription.

Pour provisionner des appareils dédiés, procédez comme suit :

- Ajoutez un profil d'inscription pour les administrateurs XenMobile que vous autorisez à inscrire des appareils dédiés dans votre déploiement XenMobile. Consultez Création de profils d'inscription.
- Autorisez les applications auxquelles vous souhaitez que l'appareil dédié accède.
- Vous pouvez également activer le mode de verrouillage des tâches pour l'application autorisée. Lorsqu'une application est en mode de verrouillage des tâches, elle est épinglée sur l'écran de l'appareil lorsque l'utilisateur l'ouvre. Aucun bouton d'accueil n'apparaît et le bouton Retour est désactivé. L'utilisateur quitte l'application à l'aide d'une action programmée dans l'application, comme la déconnexion.
- Inscrivez chaque appareil dans le profil d'inscription que vous avez ajouté.

Configuration système requise

- L'inscription des appareils dédiés est prise en charge à partir de Android 6.0.

Autoriser les applications et définir le mode de verrouillage des tâches

La stratégie Kiosque vous permet d'autoriser les applications et de définir le mode de verrouillage des tâches. Par défaut, les services Secure Hub et Google Play sont autorisés.

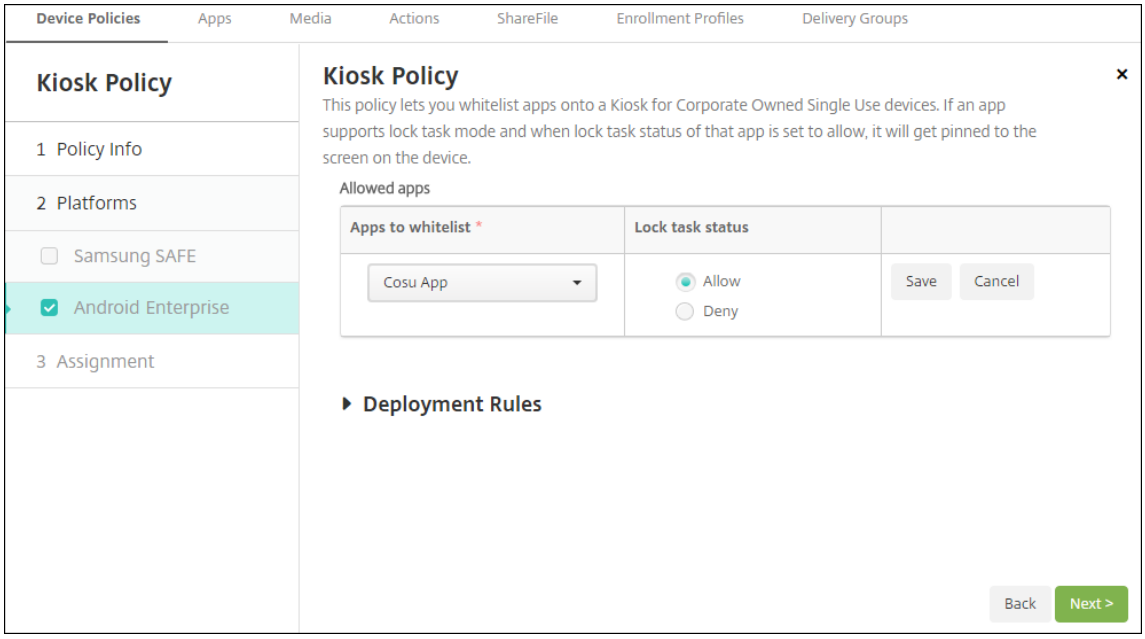
Pour ajouter la stratégie Kiosque :

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.
2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus** puis, sous Sécurité, cliquez sur **Kiosque**. La page **Stratégie kiosque** s'affiche.
4. Sous Plates-formes, sélectionnez **Android Enterprise**. Supprimez les autres plates-formes.
5. Dans le volet Informations sur la stratégie, tapez le **nom de la stratégie** et une **description** facultative.
6. Cliquez sur **Suivant**, puis sur **Ajouter**.
7. Pour autoriser une application, et autoriser ou refuser le mode de verrouillage des tâches pour cette application, procédez comme suit :

   Sélectionnez dans la liste l'application que vous souhaitez autoriser.

   Choisissez **Autoriser** pour que l'application soit épinglée sur l'écran de l'appareil lorsque l'utilisateur démarre l'application. Choisissez **Refuser** pour que l'application ne soit pas épinglée. La valeur par défaut est **Autoriser**.

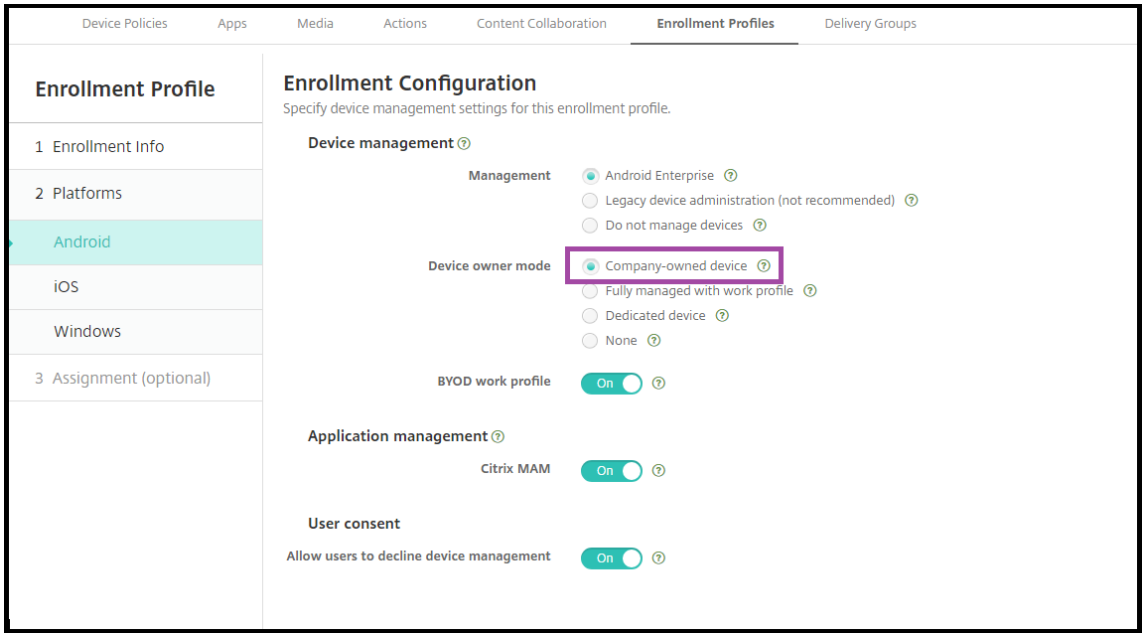


8. Cliquez sur **Enregistrer**.
9. Pour autoriser une application, et autoriser ou refuser le mode de verrouillage des tâches pour cette application, cliquez sur **Ajouter**.
10. Configurez les règles de déploiement et choisissez des groupes de mise à disposition. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Pour inscrire l'appareil

1. Cliquez sur **Suivant** ou sélectionnez **Android** sous **Plates-formes**. La page Configuration de l'inscription s'affiche.

2. Définissez **Gestion** sur **Android Enterprise**.
3. Définissez **Mode propriétaire de l'appareil** sur **Appareil appartenant à l'entreprise**.



4. Sélectionnez **Attribution (facultatif)**. L'écran Attribution de groupes de mise à disposition s'affiche.
5. Choisissez le(s) groupe(s) de mise à disposition contenant les administrateurs qui inscrivent les appareils dédiés. Cliquez ensuite sur **Enregistrer**.

Si vous avez activé le **profil de travail BYOD** dans le profil d'inscription, les appareils qui ne sont pas nouveaux ou réinitialisés en usine sont inscrits en tant qu'appareils avec profil de travail. Consultez Provisioning d'appareils Android Enterprise avec profil de travail.

Provisionner des appareils Android Enterprise entièrement gérés avec profil de travail (appareils COPE)

Les appareils entièrement gérés avec profil de travail, anciennement appelés appareils COPE, sont des appareils appartenant à l'entreprise qui sont utilisés à des fins professionnelles et personnelles. Votre organisation gère l'ensemble des appareils. Vous pouvez appliquer un ensemble de stratégies à l'appareil et un ensemble distinct de stratégies au profil de travail.

Dans la console XenMobile, les appareils entièrement gérés avec profil de travail apparaissent avec les termes suivants :

- La propriété de l'appareil est « Corporate » (Entreprise).
- Le type d'installation de l'appareil Android Enterprise est « Corporate Owner Personally Enabled » (COPE).

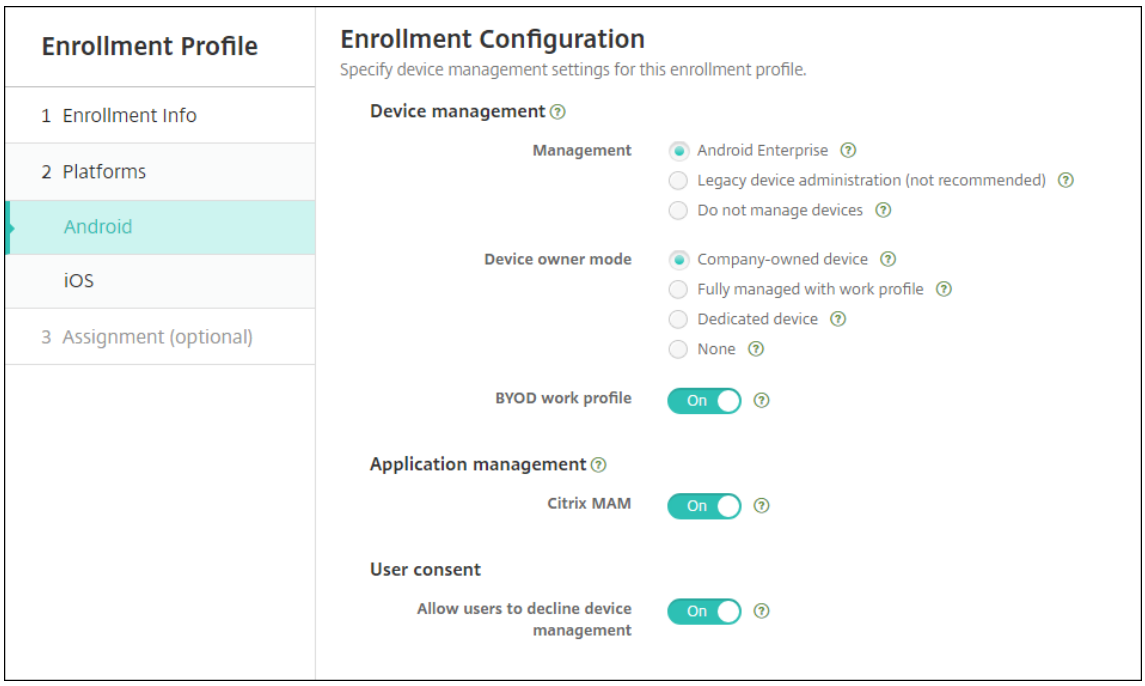
Configuration système requise

- La prise en charge de l'inscription d'appareils entièrement gérés avec profil de travail commence avec Android 8.0 jusqu'à Android 10.x.

Ajouter un profil d'inscription pour les appareils entièrement gérés avec profil de travail

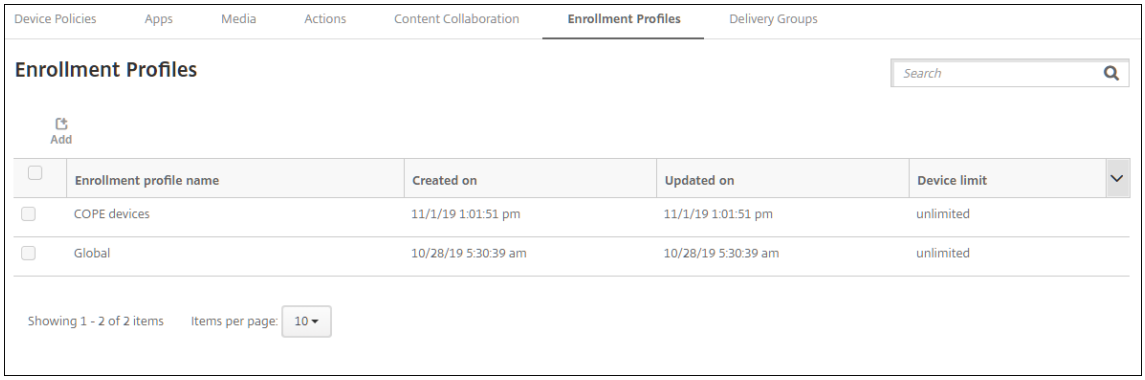
Créez un profil d'inscription pour inscrire les appareils entièrement gérés avec profil de travail. Les administrateurs des groupes de mise à disposition auxquels ce profil d'inscription est attribué peuvent inscrire des appareils entièrement gérés avec profil de travail. Pour vous assurer que ces administrateurs peuvent inscrire tous les appareils requis, créez un profil d'inscription pour eux avec un nombre illimité d'appareils autorisés par utilisateur. Attribuez ce profil à un groupe de mise à disposition contenant les administrateurs qui inscrivent des appareils entièrement gérés avec profil de travail.

1. Dans la console XenMobile, accédez à **Configurer > Profils d'inscription**.
2. Pour ajouter un profil d'inscription, cliquez sur **Ajouter**. Sur la page Infos d'inscription, entrez un nom pour le profil d'inscription. Assurez-vous que le nombre d'appareils que les membres avec ce profil peuvent inscrire est défini sur illimité.
3. Cliquez sur **Suivant** ou sélectionnez **Android Enterprise** sous **Plates-formes**. La page Configuration de l'inscription s'affiche.
4. Définissez **Type d'inscription** sur l'une des options suivantes :
    - **Profil de travail/entièrement géré :** les nouveaux appareils ou les appareils qui ont fait l'objet d'une réinitialisation d'usine sont inscrits en tant qu'appareils entièrement gérés. Les appareils BYOD sont inscrits uniquement avec un profil de travail que vous gérez.
    - **Profil de travail/COPE :** les nouveaux appareils ou les appareils qui ont fait l'objet d'une réinitialisation d'usine sont inscrits en tant qu'appareils entièrement gérés avec profil de travail. Les appareils BYOD sont inscrits uniquement avec un profil de travail que vous gérez.



5. Sélectionnez **Attribution (facultatif)** ou cliquez sur **Suivant**. L'écran Attribution de groupes de mise à disposition s'affiche.
6. Choisissez le(s) groupe(s) de mise à disposition contenant les administrateurs qui inscrivent les appareils dédiés. Cliquez ensuite sur **Enregistrer**.

   La page Profil d'inscription apparaît avec le profil que vous avez ajouté.



Si un utilisateur appartient à plusieurs groupes de mise à disposition qui ont des profils d'inscription différents, le nom du groupe de mise à disposition détermine le profil d'inscription utilisé. XenMobile sélectionne le groupe de mise à disposition qui apparaît en dernier dans une liste alphabétique des groupes de mise à disposition.

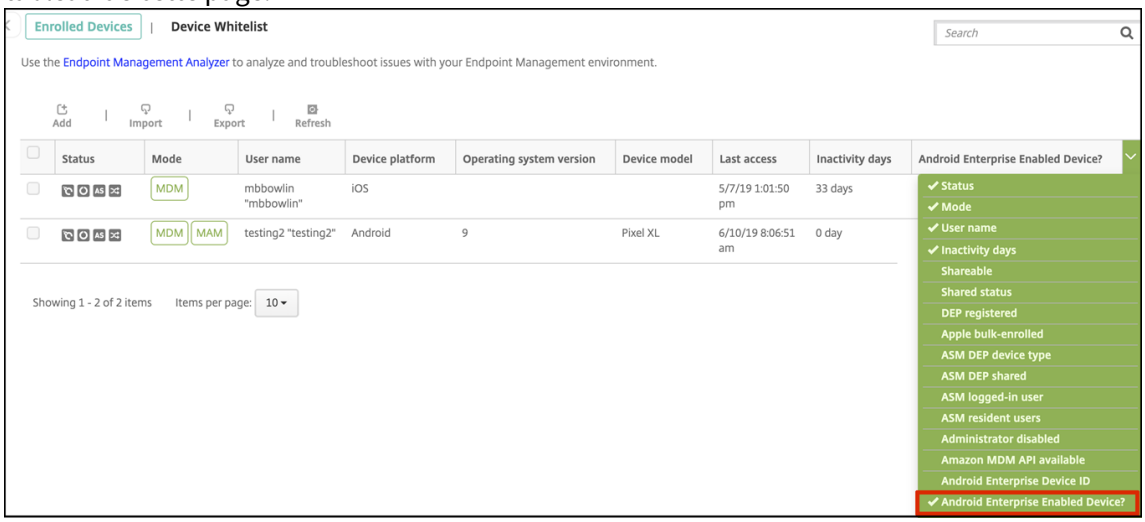
Pour inscrire l'appareil

Les nouveaux appareils et les appareils qui ont fait l'objet d'une réinitialisation d'usine sont inscrits en tant qu'appareils entièrement gérés avec profil de travail à l'aide du jeton d'identificateur DPC, du partage NFC (Near Field Communication) ou des méthodes de code QC. Consultez Inscription d'appareils à l'aide du jeton d'identification DPC Citrix, Inscription d'appareils à l'aide du partage NFCou Enrôlement d'appareils à l'aide d'un code QR.

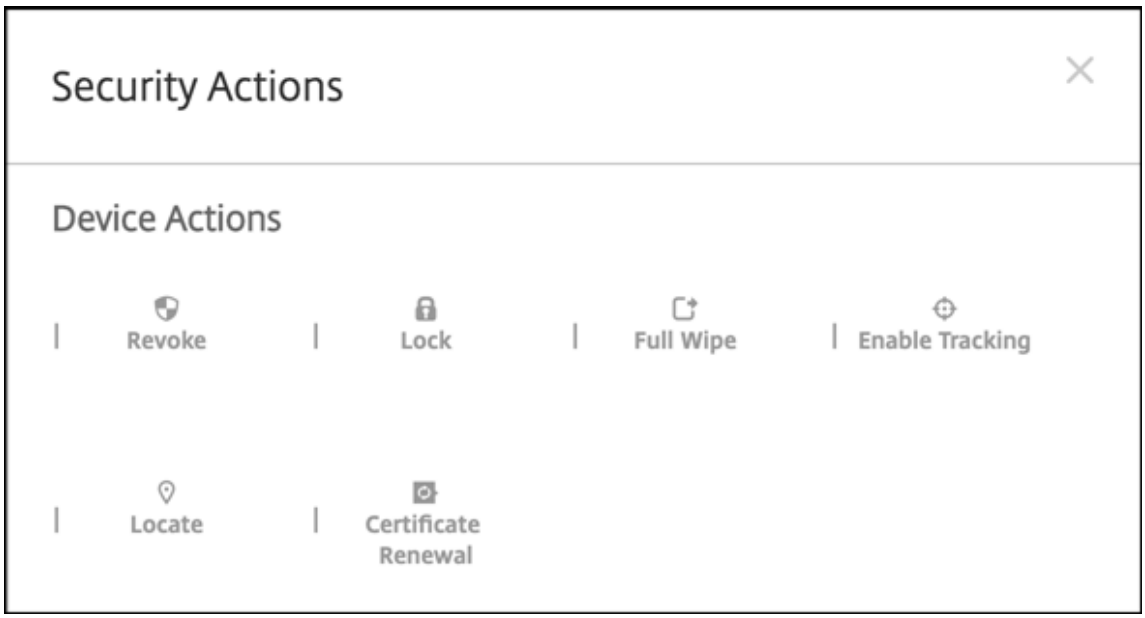
Les appareils qui ne sont pas nouveaux ou réinitialisés en usine sont inscrits en tant qu'appareils avec profil de travail, comme décrit à la section Provisioning d'appareils Android Enterprise avec profil de travail.

Affichage des appareils Android Enterprise dans la console XenMobile

1. Dans la console XenMobile, accédez à **Gérer > Appareils**.
2. Ajouter la colonne **Appareil Android Enterprise activé ?** en cliquant sur le menu à droite du tableau de cette page.



3. Pour afficher les actions de sécurité disponibles, sélectionnez un appareil entièrement géré et cliquez sur **Sécurisé**. Lorsque l'appareil est entièrement géré, l'action **Effacer** est disponible, mais l'opération **Effacer les données d'entreprise** ne l'est pas. Cela est dû au fait que l'appareil n'autorise que les applications de Google Play Store d'entreprise. L'utilisateur ne peut donc pas installer des applications à partir du magasin public. Votre organisation gère tout le contenu de l'appareil.



Configurer les stratégies d'appareil et d'application Android Enterprise

Pour obtenir une vue d'ensemble des stratégies contrôlées au niveau de l'appareil et de l'application, consultez Stratégies d'appareil et stratégies MDX Android Entreprise prises en charge.

Informations clés sur les stratégies :

- **Protection contre la perte de données :** la technologie de conteneur MAM XenMobile sécurise les applications grâce au cryptage et à d'autres technologies mobiles de protection contre la perte de données (DLP). Utilisez le SDK MAM ou le MDX Toolkit de Citrix pour activer MDX sur les applications.
- **Restrictions sur l'appareil :** des dizaines de restrictions sur l'appareil vous permettent de contrôler des fonctionnalités telles que :
  - Utilisation de l'appareil photo de l'appareil
  - Utilisation du copier-coller entre les profils de travail et les profils personnels
- **Per App VPN :** utilisez la stratégie Configurations gérées pour configurer les profils VPN pour Android Enterprise.
- **Stratégie de messagerie :** nous vous recommandons d'utiliser la stratégie Configurations gérées pour configurer les applications.

Ce tableau répertorie toutes les stratégies d'appareils disponibles pour les appareils Android Enterprise.

> **Important :**
>
> Pour les appareils qui sont inscrits dans Android Enterprise et utilisent des applications MDX : vous pouvez contrôler certains paramètres via MDX et Android Enterprise. Utilisez les paramètres de stratégie les moins restrictifs pour MDX et contrôlez la stratégie via Android Enterprise.

Autorisation de l'application Android Entreprise	Configurations gérées par Android Enterprise	Inventaire des applications
Désinstallation des applications	Mise à jour automatique des applications gérées	Contrôler mise à jour d'OS
Informations d'identification	XML personnalisé	Exchange
Fichiers	Gestion du keyguard	Kiosque
Emplacement	Code secret	Restrictions
Clé de licence MDM Samsung	Planification	Wi-Fi
Options XenMobile		

Stratégies pour appareils entièrement gérés avec profil de travail (appareils COPE)

Pour les appareils entièrement gérés avec profil de travail (appareils COPE), vous pouvez utiliser certaines stratégies pour appliquer des paramètres distincts à l'ensemble de l'appareil et au profil de travail. Vous pouvez utiliser d'autres stratégies pour appliquer des paramètres uniquement à l'ensemble de l'appareil ou uniquement au profil de travail des appareils entièrement gérés avec profil de travail.

Stratégie	S'applique à
Autorisation de l'application Android Entreprise	Profil de travail
Configurations gérées par Android Enterprise	Profil de travail
Inventaire des applications	Profil de travail
Désinstallation des applications	Profil de travail
Mise à jour automatique des applications gérées	Profil de travail
Contrôler mise à jour d'OS	S.O.
Informations d'identification	Profil de travail

Stratégie	S'applique à
XML personnalisé	S.O.
Exchange	S.O.
Fichiers	Profil de travail
Gestion du keyguard	Appareil et profil de travail
Kiosque	S.O.
Emplacement	Appareil (mode de localisation uniquement)
Code secret	Appareil et profil de travail
Restrictions	Appareil et profil de travail (créez des stratégies distinctes pour l'appareil et le profil de travail)
Clé de licence MDM Samsung	S.O.
Planification	Profil de travail
Wi-Fi	Appareil
Options XenMobile	Profil de travail

Consultez également Stratégies d'appareil et stratégies MDX Android Entreprise prises en charge et Présentation du SDK MAM.

Actions de sécurisation

Android Enterprise prend en charge les actions de sécurisation suivantes. Pour obtenir une description de chaque action, consultez la section Actions de sécurisation.

Action de sécurisation	Profil de travail	Entièrement géré
Renouvellement de certificat	Oui	Oui
Effacement complet	Non	Oui
Localiser	Oui	Oui
Verrouiller	Oui	Oui
Verrouiller et réinitialiser un mot de passe	Non	Oui
Notifier (sonnerie)	Oui	Oui
Révoquer	Oui	Oui

Action de sécurisation	Profil de travail	Entièrement géré
Effacer les données d'entreprise	Oui	Non

Notes sur les actions de sécurisation

- L'action de sécurisation Localiser échoue à moins que la stratégie d'appareil Localisation n'ait défini le mode de localisation de l'appareil sur **Haute précision** ou **Économie de batterie**. Voir Stratégie d'emplacement.
- Sur les appareils avec profil de travail qui exécutent des versions Android antérieures à Android 8.0 :
  - L'action de verrouillage et de réinitialisation du mot de passe n'est pas prise en charge.
- Sur les appareils avec profil de travail qui exécutent Android 8.0 ou supérieur :
  - Le code secret envoyé verrouille le profil de travail. L'appareil lui-même n'est pas verrouillé.
  - Si aucun code d'accès n'est défini sur le profil de travail :
    - Si aucun code secret n'est envoyé ou si le code secret envoyé ne répond pas aux exigences de code secret : l'appareil est verrouillé.
  - Si un code d'accès est défini sur le profil de travail :
    - Si aucun code secret n'est envoyé ou si le code secret envoyé ne répond pas aux exigences en matière de code secret : le profil de travail est verrouillé mais l'appareil lui-même ne l'est pas.
- Sur les appareils entièrement gérés avec profils de travail (appareils COPE) :
  - Vous pouvez appliquer l'action de sécurisation Verrouiller séparément à l'appareil ou au profil de travail.

Désinscription d'une entreprise Android Enterprise

Si vous ne souhaitez plus utiliser votre entreprise Android Enterprise, vous pouvez annuler l'inscription de l'entreprise.

> **Avertissement :**
>
> une fois que vous avez désinscrit une entreprise, l'état par défaut des applications Android Enterprise sur les appareils déjà inscrits est rétabli. Google ne gère plus les appareils. Si vous inscrivez un appareil sur une nouvelle entreprise Android Enterprise, vous devez approuver les applications de la nouvelle organisation à partir de Google Play d'entreprise. Vous pouvez ensuite

> mettre à jour les applications à partir de la console XenMobile.

Une fois l'entreprise Android Enterprise désinscrite :

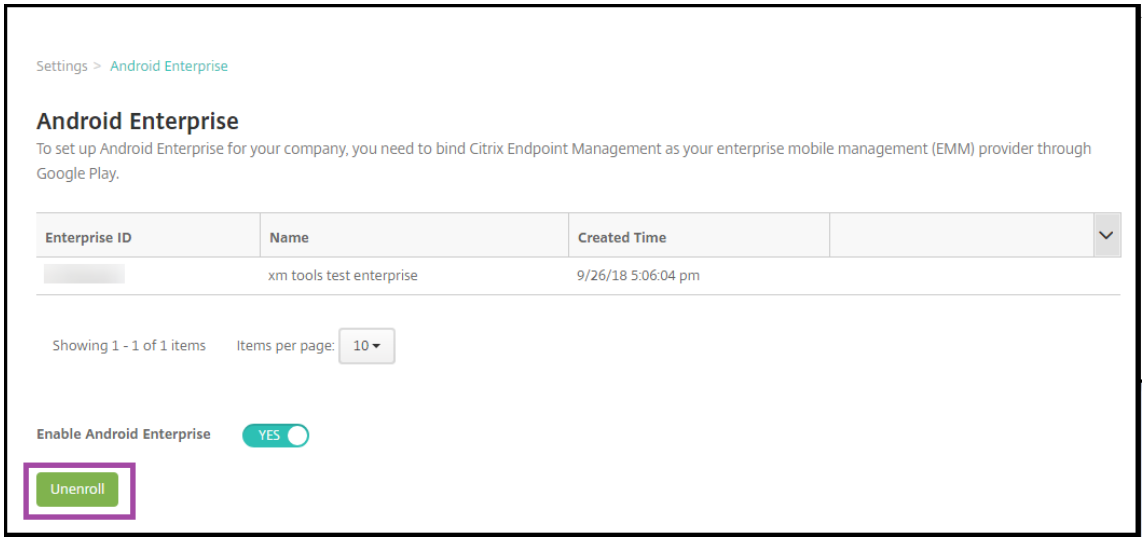
- Les applications Android Enterprise des appareils et des utilisateurs inscrits dans l'entreprise sont réinitialisées à leur état par défaut. Les stratégies Configurations gérées par Android Enterprise appliquées précédemment n'affectent plus les opérations.
- XenMobile gère les appareils inscrits dans l'entreprise. Du point de vue de Google, ces appareils ne sont pas gérés. Vous ne pouvez pas ajouter de nouvelles applications Android Enterprise. Vous ne pouvez pas appliquer les stratégies Configurations gérées par Android Enterprise. Vous pouvez appliquer d'autres stratégies, telles que Planification, Mot de passe et Restrictions, à ces appareils.
- Si vous tentez d'inscrire des appareils dans Android Enterprise, ils sont inscrits comme appareils Android et non comme appareils Android Enterprise.

Désinscrivez une entreprise Android Enterprise à l'aide de la console XenMobile Server et des outils XenMobile Tools.

Lorsque vous effectuez cette tâche, XenMobile ouvre une fenêtre contextuelle XenMobile Tools. Avant de commencer, assurez-vous que XenMobile est autorisé à ouvrir des fenêtres contextuelles dans le navigateur que vous utilisez. Certains navigateurs, tels que Google Chrome, vous obligent à désactiver le blocage des fenêtres contextuelles et à ajouter l'adresse du site XenMobile à la liste d'autorisation des fenêtres contextuelles bloquées.

Désinscription d'une entreprise Android Enterprise :

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page Paramètres s'affiche.
2. Sur la page Paramètres, cliquez sur **Android Enterprise**.
3. Cliquez sur **Désinscrire**.



Distribuer des applications Android Enterprise

January 10, 2022

XenMobile gère les applications déployées sur les appareils. Vous pouvez organiser et déployer les types d'applications Android Enterprise suivants.

- **Applications gérées du magasin d'applications :** ces applications incluent des applications gratuites ou payantes disponibles dans le Google Play Store d'entreprise. Par exemple : GoToMeeting.
- **MDX :** applications préparées avec le SDK MAM ou encapsulées avec MDX Toolkit. Ces applications incluent des stratégies MDX. Vous obtenez des applications MDX à partir de sources internes et de magasins publics. Déployez des applications de productivité mobiles Citrix en tant qu'applications MDX.
- **Entreprise :** applications privées que vous développez ou obtenez à partir d'une autre source. Vous fournissez ces applications à vos utilisateurs via le Google Play Store d'entreprise. Le Google Play Store d'entreprise est le magasin d'applications d'entreprise Google.
- **Applications privées compatibles MDX :** applications d'entreprise préparées avec le SDK MAM ou encapsulées avec MDX Toolkit.

Vous pouvez ajouter des applications d'entreprise et des applications privées compatibles MDX de deux manières différentes.

- Ajoutez les applications à la console XenMobile en tant qu'applications d'entreprise, comme décrit dans les sections Applications d'entreprise et Applications privées compatibles MDX de cet article.
- Publiez les applications directement sur le Google Play Store d'entreprise à l'aide de votre compte Google Developer. Ajoutez ensuite les applications à la console XenMobile en tant qu'applications gérées du magasin d'applications. Voir Applications gérées du magasin d'applications.

Si vous publiez des applications à l'aide de votre compte Google Developer, puis passez à l'utilisation de la console XenMobile, l'appartenance des applications diffère. Vous devez gérer vos applications dans les deux emplacements, dans ce cas. Citrix vous recommande d'ajouter vos applications à l'aide d'une méthode ou d'une autre.

Si vous devez supprimer des applications autogérées du Google Play Store d'entreprise, ouvrez un ticket avec Google. Les développeurs peuvent désactiver, mais pas supprimer, les applications du Google Play Store géré.

Les sections suivantes fournissent des informations plus détaillées sur la configuration des applications Android Enterprise. Pour plus d'informations sur la distribution d'applications, consultez la section Ajouter des applications. Cet article contient les informations suivantes :

- Workflows généraux pour l'ajout d'applications Web et SaaS ou de liens Web
- Workflow des applications requises pour les applications d'entreprise et de magasin public
- Mise à disposition des applications d'entreprise à partir du réseau CDN Citrix pour applications d'entreprise

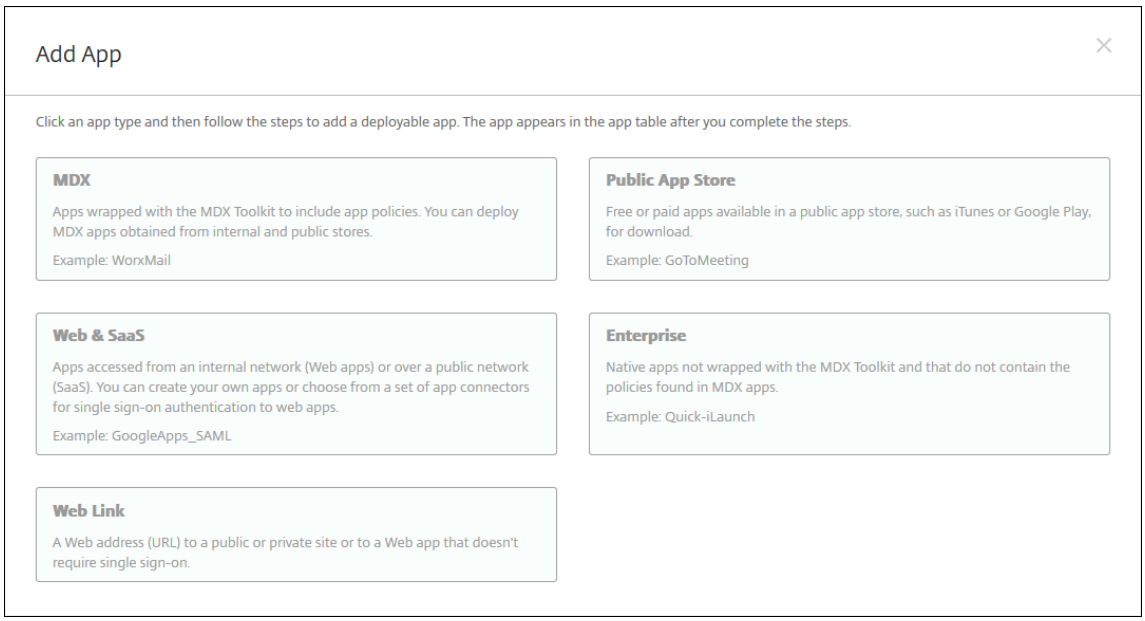
Applications gérées du magasin d'applications

Vous pouvez ajouter des applications gratuites et payantes disponibles sur le Google Play Store d'entreprise à XenMobile.

> **Remarque** pour rendre toutes les applications du Google Play Store accessibles depuis le Google Play d'entreprise, utilisez la propriété de serveur **Accéder à toutes les applications du Google Play Store d'entreprise**. Consultez Propriétés du serveur. La définition de cette propriété sur **true** autorise tous les utilisateurs d'Android Enterprise d'accéder aux applications du Google Play Store public. Vous pouvez ensuite utiliser la stratégie Restrictions pour contrôler l'accès à ces applications.

Étape 1 : Ajouter et configurer des applications

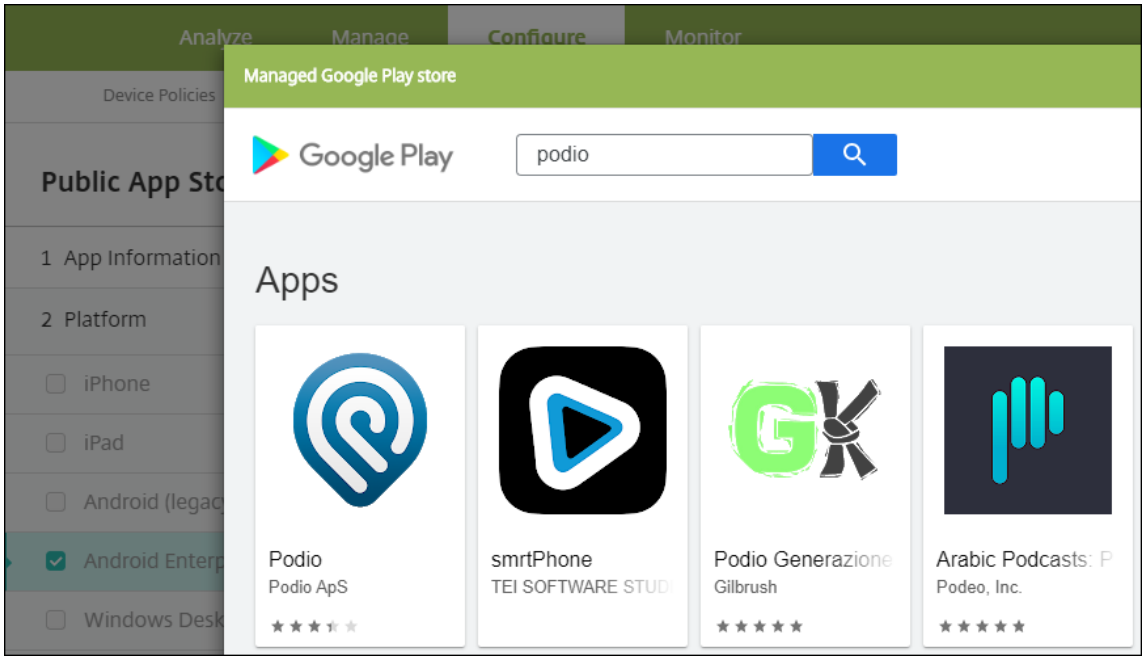
1. Dans la console XenMobile, accédez à **Configurer > Applications**. Cliquez sur **Ajouter**.
2. Cliquez sur **Magasin d'applications public**.



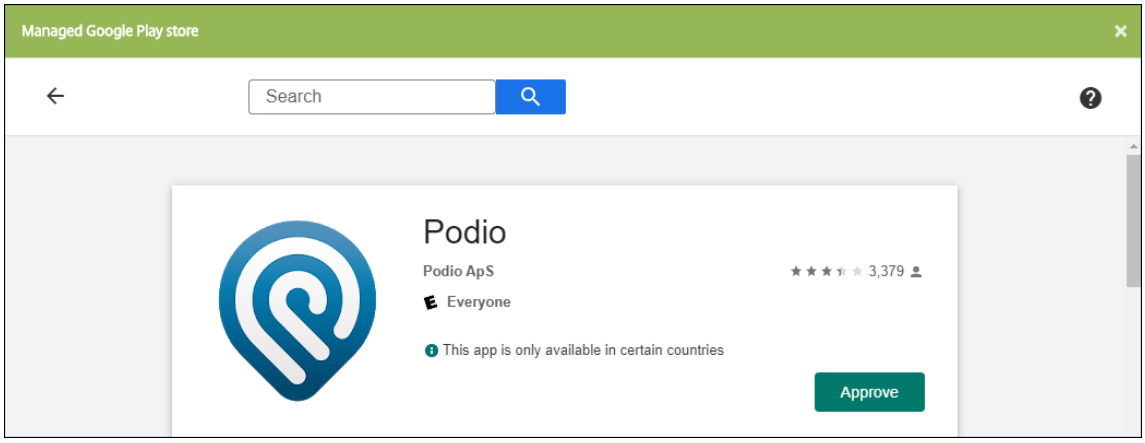
3. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous **Nom de l'application** dans le tableau **Applications**.
   - **Description :** entrez une description pour l'application (facultatif).

- **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.

4. Sélectionnez **Android Enterprise** comme plate-forme.
5. Entrez le nom de l'application ou l'ID de package dans la zone de recherche et cliquez sur **Rechercher**. Vous pouvez trouver l'ID de package dans Google Play Store. L'ID se trouve dans l'URL de l'application. Par exemple, `com.Slack` est l'ID de package de `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`.

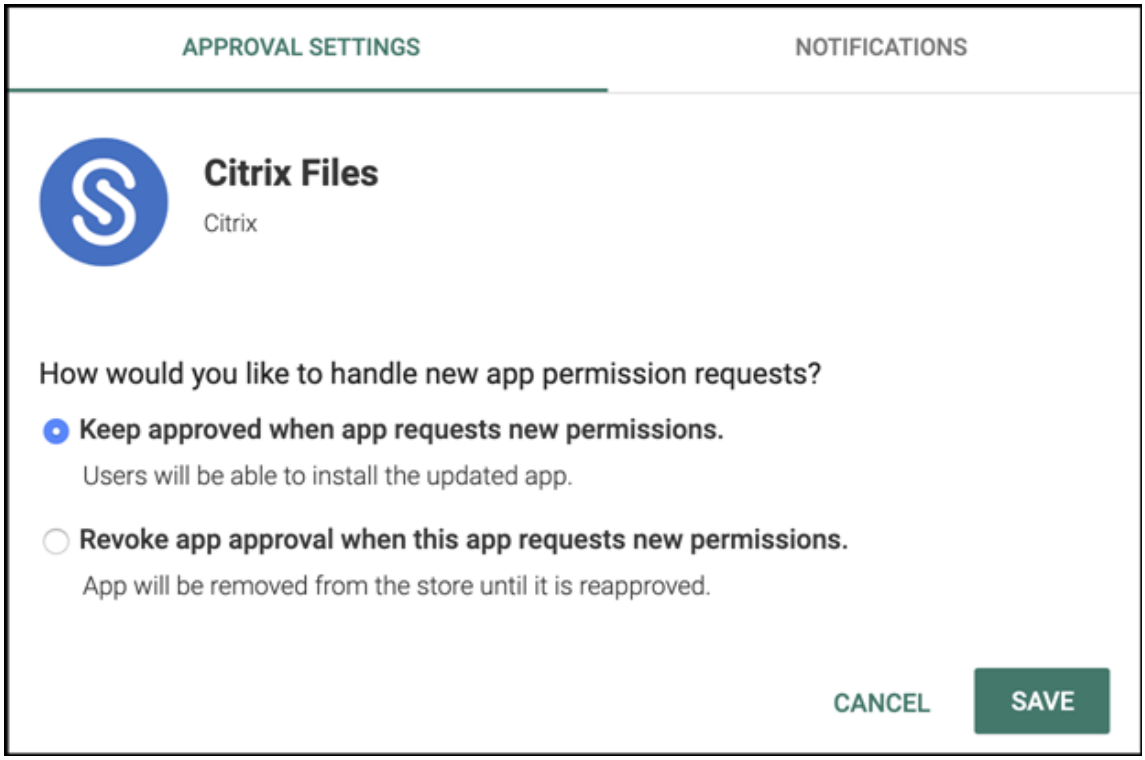


6. Les applications correspondant aux critères de recherche s'affichent. Cliquez sur l'application souhaitée, puis cliquez sur **Approuver**.

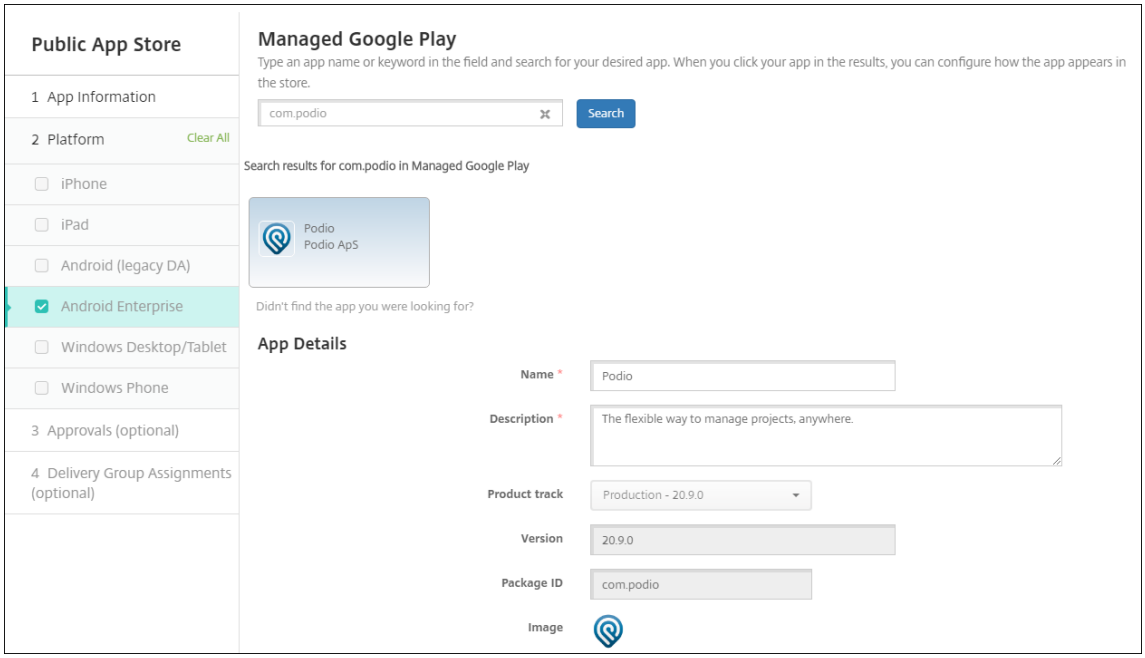


7. Cliquez à nouveau sur **Approuver**.

8. Sélectionnez **Maintenir l'état approuvé de cette application lorsqu'elle demande d'autres autorisations**. Cliquez sur **Enregistrer**.



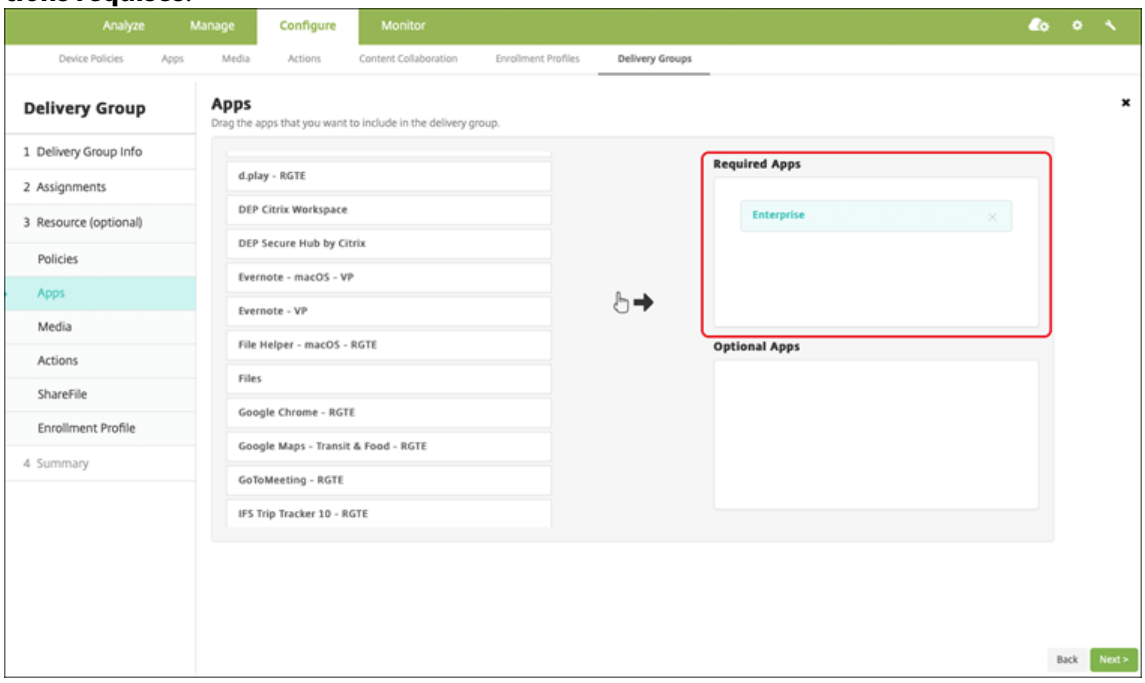
9. Cliquez sur l'icône de l'application et configurez le **nom** et la **description** de l'application.



10. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**. Pour de plus amples informations, consultez la section Déployer des ressources.

Étape 2 : Configurer le déploiement de l'application

1. Accédez à **Configurer > Groupes de mise à disposition** et sélectionnez le groupe de mise à disposition que vous avez configuré. Cliquez sur **Modifier**.
2. Dans la section **Applications**, faites glisser les applications souhaitées vers la zone **Applications requises**.



3. Sur la page **Résumé**, cliquez sur **Enregistrer**.
4. Sur la page **Groupes de mise à disposition**, sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.

Applications MDX

Ajoutez des fichiers MDX à XenMobile et configurez les détails de l'application et les paramètres de stratégie. Pour configurer les applications de productivité mobiles Citrix pour Android Enterprise, ajoutez-les en tant qu'applications MDX. Pour plus d'informations sur les stratégies applicatives disponibles pour chaque type de plate-forme, consultez :

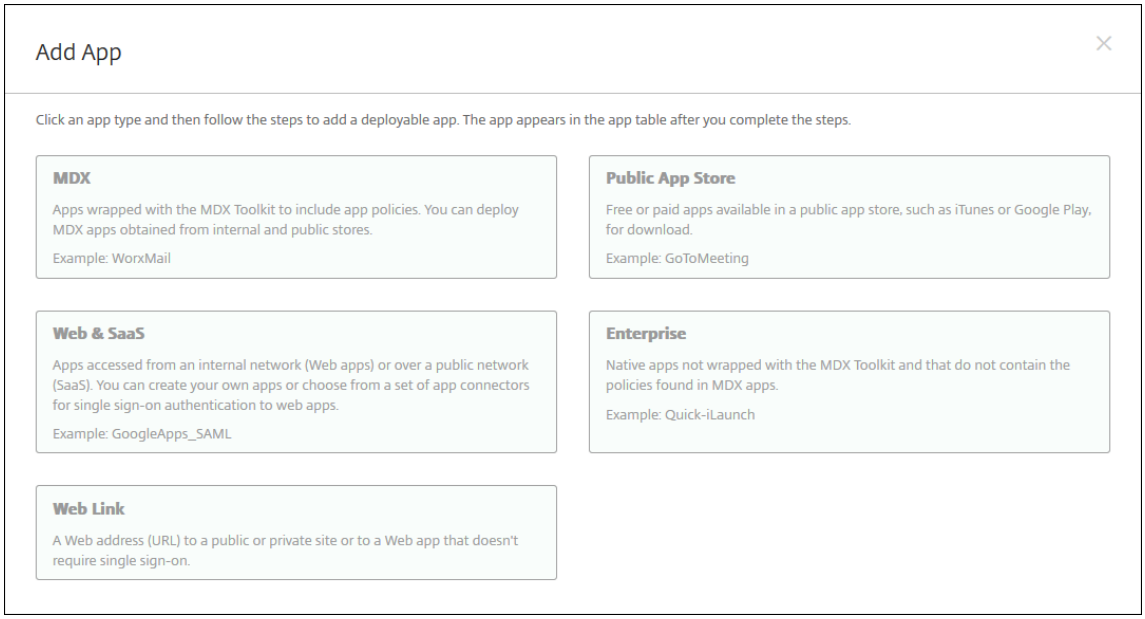
- Présentation du SDK MAM
- Synopsis des stratégies MDX

Étape 1 : Ajouter et configurer des applications

1. Pour les applications de productivité mobiles Citrix, téléchargez les fichiers MDX du magasin public : accédez à https://www.citrix.com/downloads. Accédez à **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.

Pour les autres types d'applications MDX, obtenez le fichier MDX.

2. Dans la console XenMobile, cliquez sur **Configurer > Applications**. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



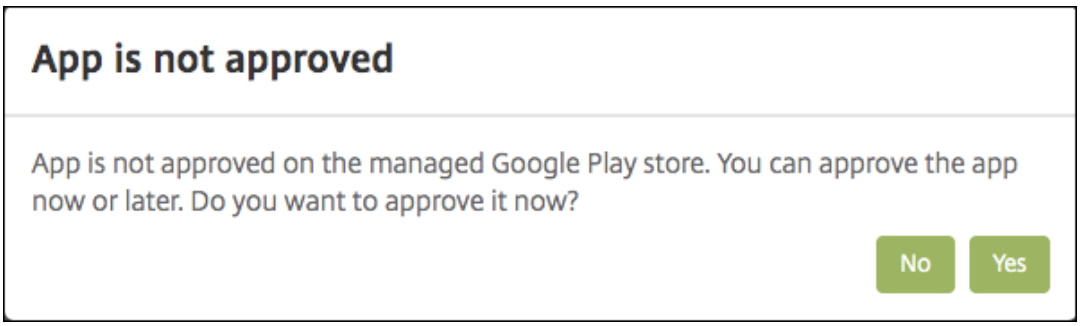
3. Cliquez sur **MDX**. La page **Informations sur l'application MDX** s'affiche. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :

   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous **Nom de l'application** dans le tableau **Applications**.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.

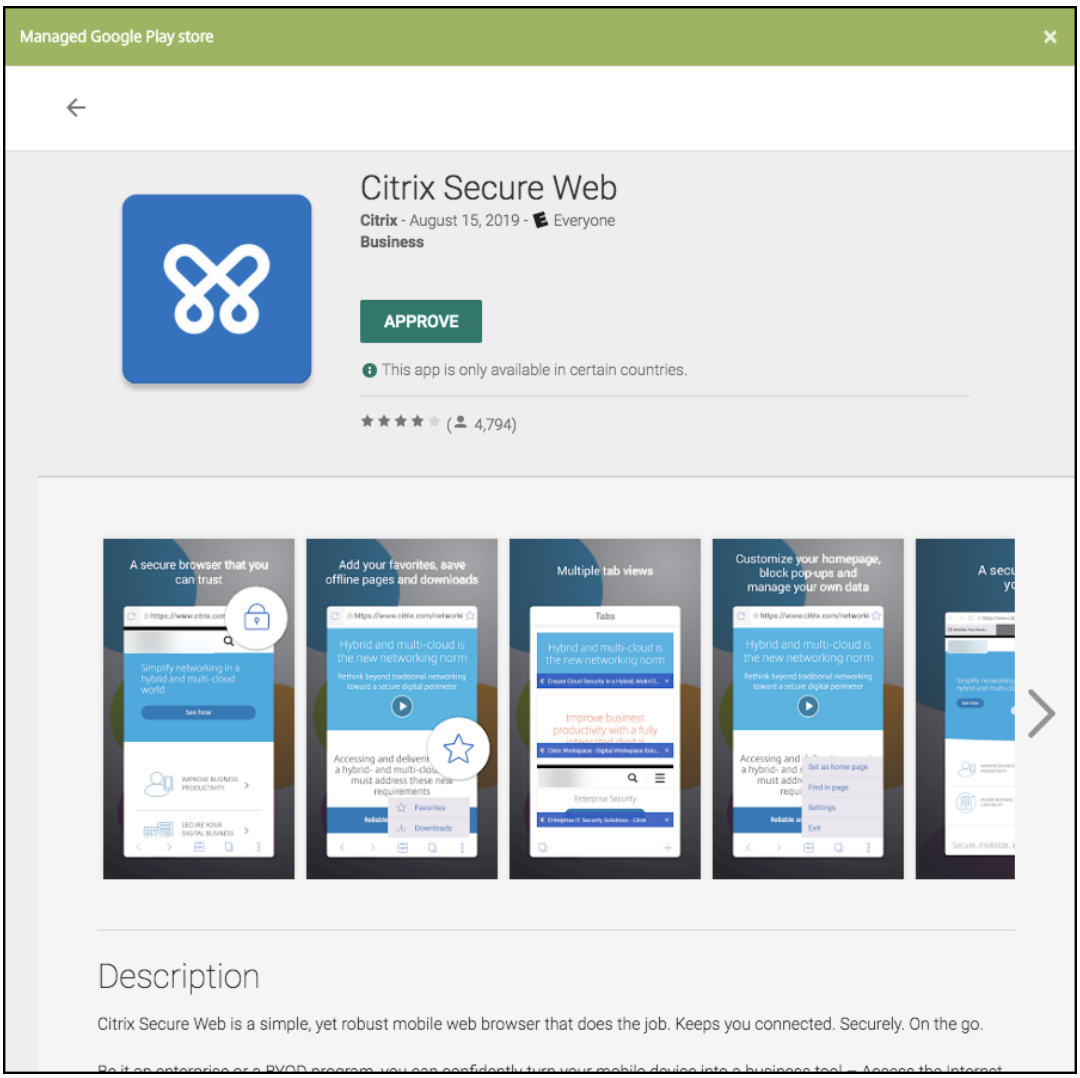
4. Sélectionnez **Android Enterprise** comme plate-forme.

5. Cliquez sur **Charger** et accédez au fichier MDX. Android Enterprise prend uniquement en charge les applications encapsulées avec le SDK MAM ou MDX Toolkit.

   - L'interface utilisateur vous avertit si l'application jointe nécessite l'approbation du Google Play Store d'entreprise. Pour approuver l'application sans quitter la console XenMobile, cliquez sur **Oui**.



Après l'ouverture du Google Play Store d'entreprise, suivez les instructions pour approuver et enregistrer l'application.



Lorsque vous ajoutez l'application, la page de **Détails sur l'application** apparaît.

6. Pour configurer ces paramètres :

   - **Nom du fichier :** entrez le nom du fichier associé à l'application.

- **Description de l'application :** entrez une description pour l'application.
- **Version de l'application :** si vous le souhaitez, entrez le numéro de version de l'application.
- **ID de package :** entrez l'ID du package de l'application, obtenu à partir du Google Play Store d'entreprise.
- **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
- **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
- **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.

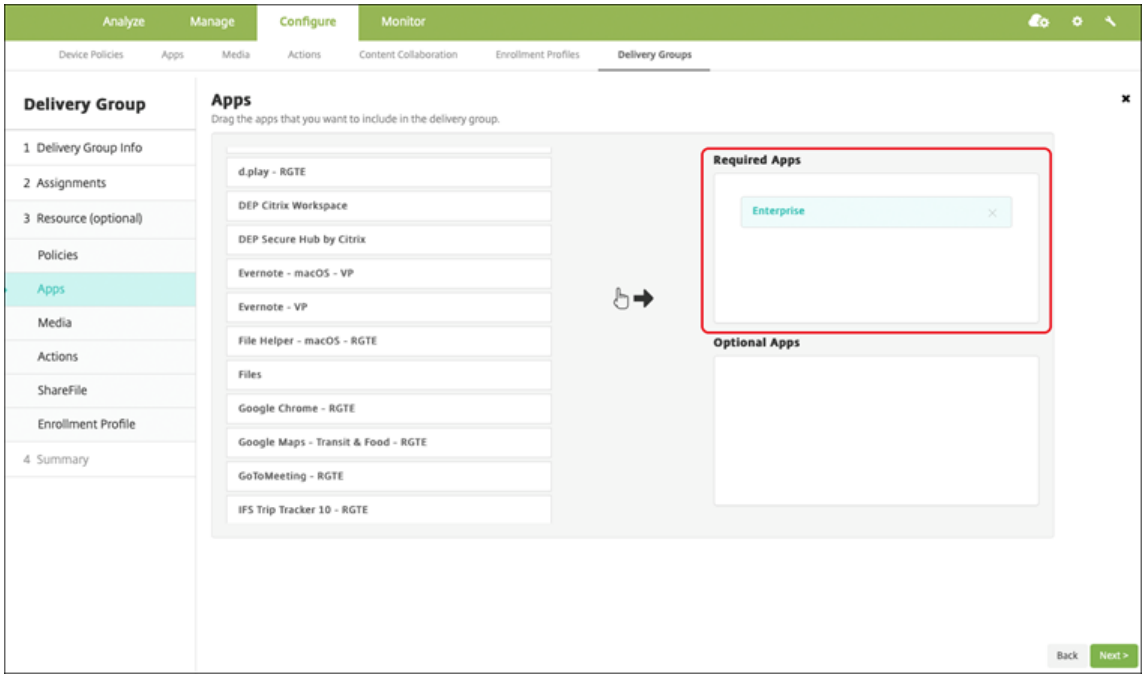
7. Configurez les **stratégies MDX**. Les stratégies MDX varient selon la plate-forme et incluent des options dans des domaines de stratégie tels que l'authentification, la sécurité de l'appareil et les restrictions applicatives. Dans la console, les stratégies ont une info-bulle qui décrit chacune d'entre elles. Pour plus d'informations sur les stratégies applicatives disponibles pour chaque type de plate-forme, consultez :

   - Présentation du SDK MAM
   - Synopsis des stratégies MDX

8. Configurez les règles de déploiement et la configuration du magasin.
9. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**. Pour de plus amples informations, consultez la section Déployer des ressources.

Étape 2 : Configurer le déploiement de l'application

1. Accédez à **Configurer > Groupes de mise à disposition** et sélectionnez le groupe de mise à disposition que vous avez configuré. Cliquez sur **Modifier**.
2. Dans la section **Applications**, faites glisser les applications souhaitées vers la zone **Applications requises**.



3. Sur la page **Résumé**, cliquez sur **Enregistrer**.
4. Sur la page **Groupes de mise à disposition**, sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.

Applications d'entreprise

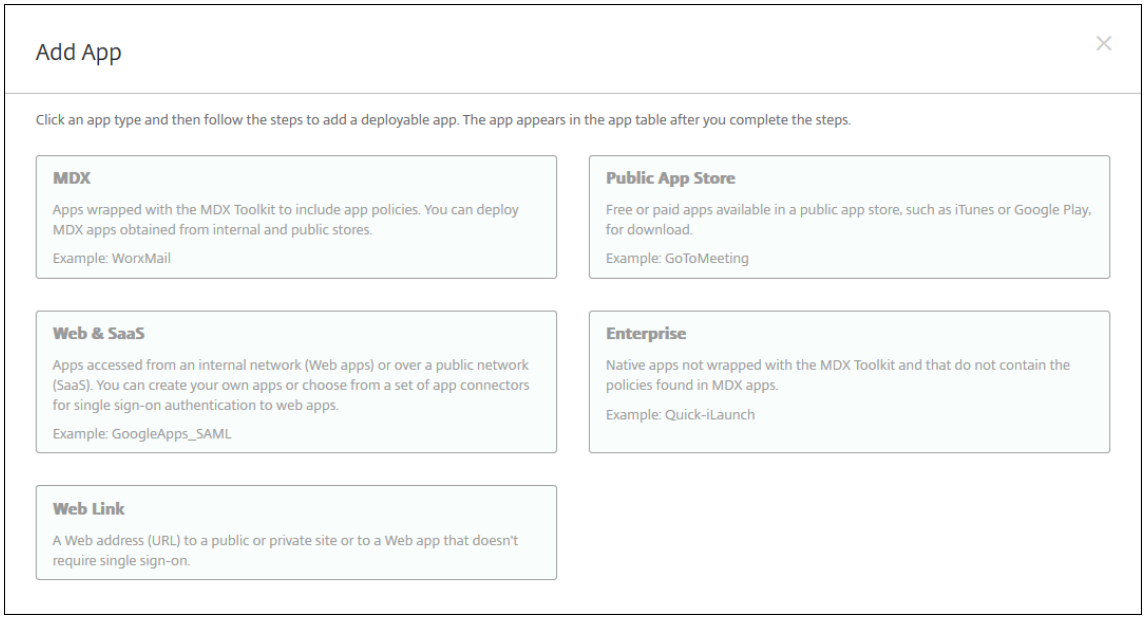
Les applications d'entreprise représentent des applications privées qui ne sont pas préparées avec le SDK MAM ou MDX Toolkit. Vous développez ces applications vous-même ou les obtenez directement à partir d'autres sources. Pour ajouter une application d'entreprise, vous avez besoin du fichier APK associé à l'application. Assurez-vous de suivre l'article Google Bonnes pratiques pour les applications privées.

Étape 1 : Ajouter et configurer des applications

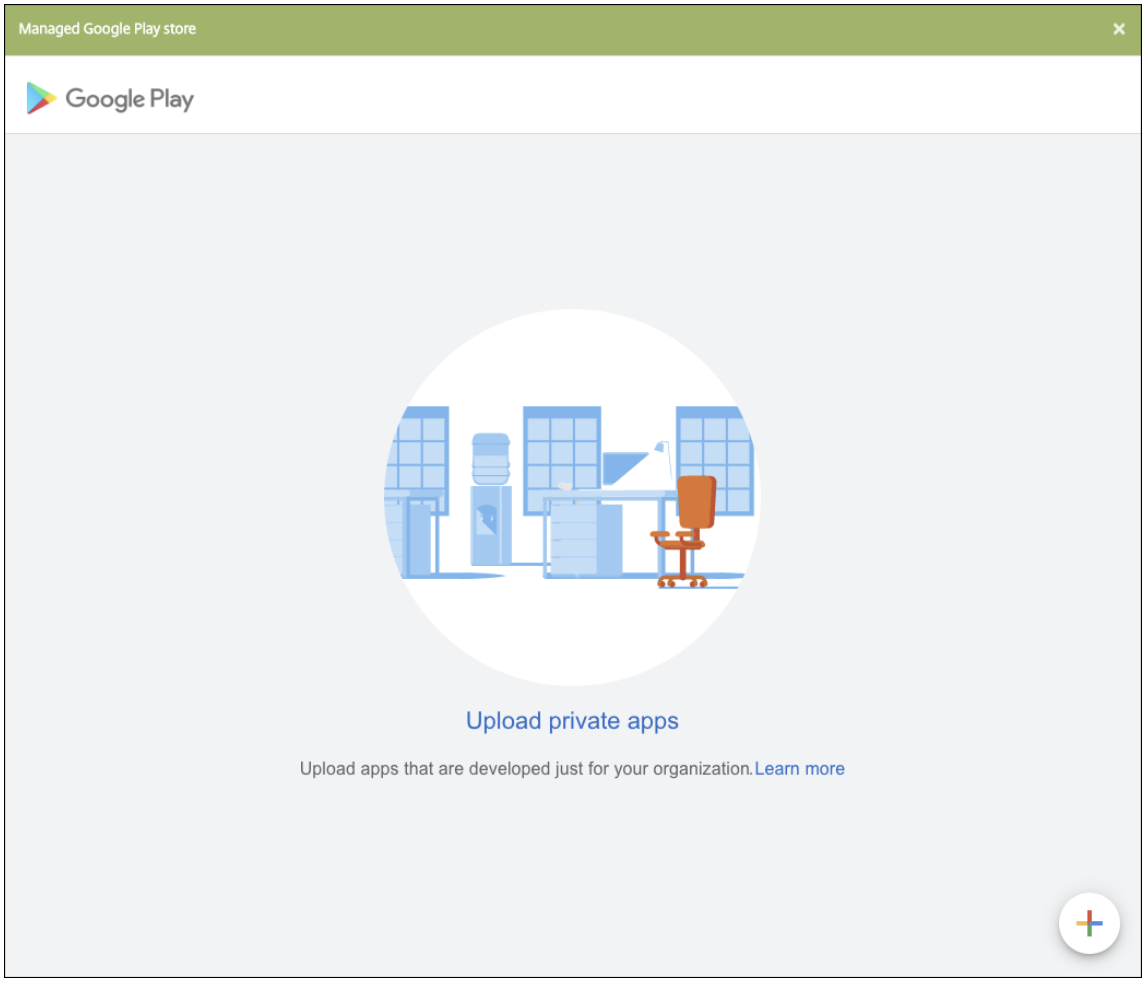
Ajoutez l'application à l'aide d'une des deux façons suivantes :

- Publiez l'application directement sur le Google Play Store d'entreprise et ajoutez-la à la console XenMobile en tant qu'application Play Store d'entreprise. Suivez la procédure Publier des applications privées de la documentation Google, puis suivez les étapes décrites dans la section Applications gérées du magasin d'applications.
- Ajoutez l'application à la console XenMobile en tant qu'application d'entreprise. Effectuez les opérations suivantes :

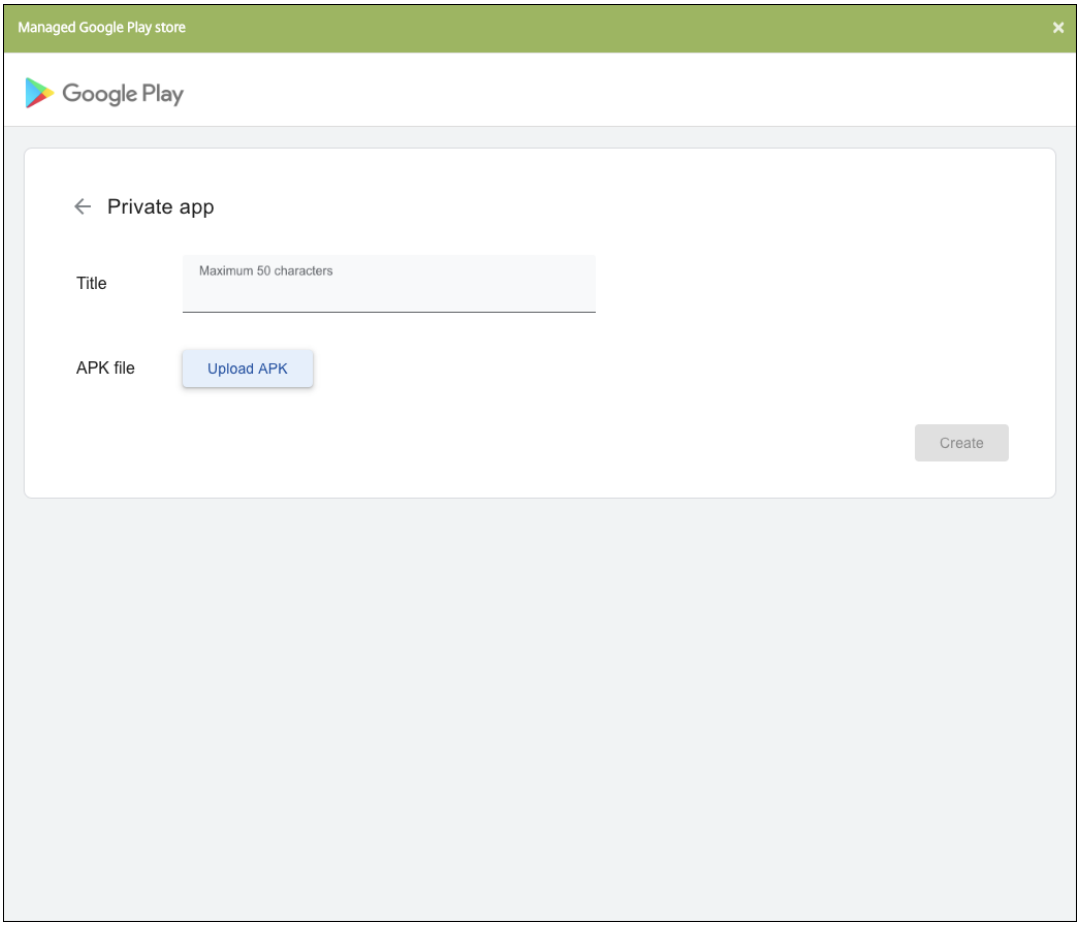
1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



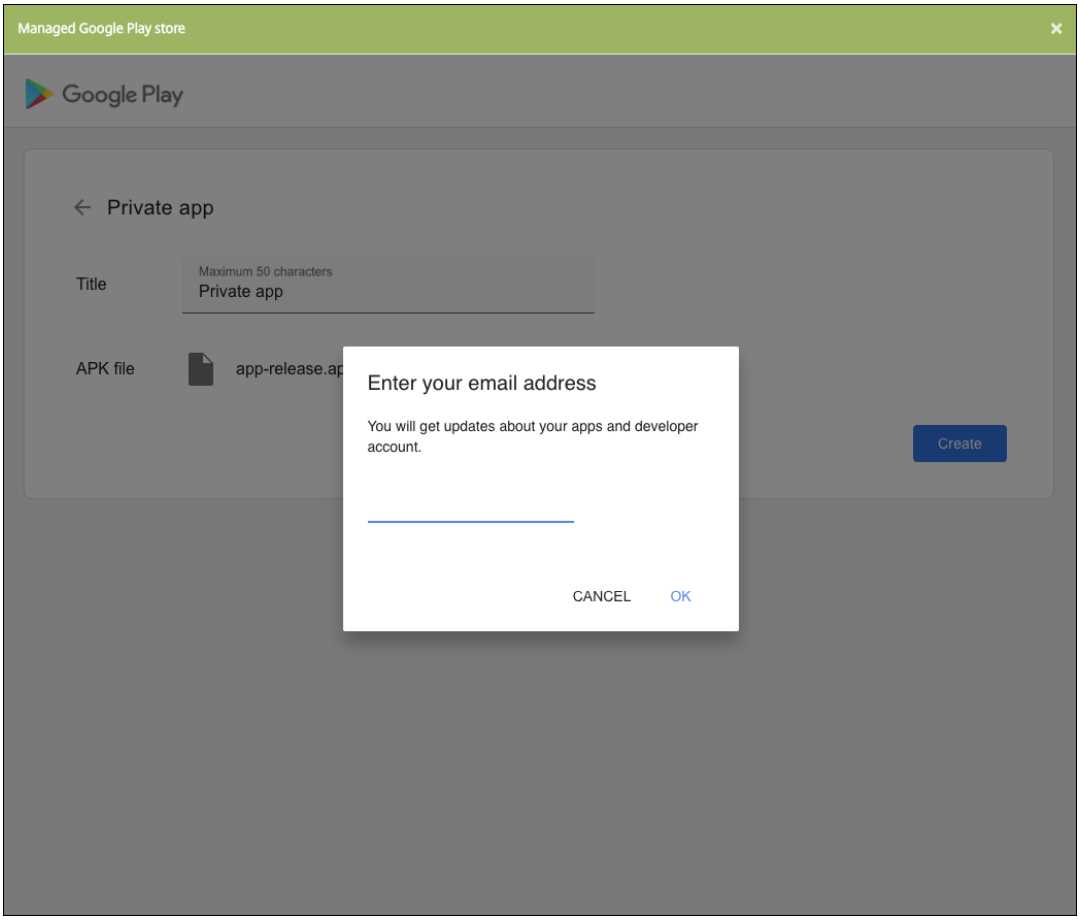
2. Cliquez sur **Entreprise**. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Il apparaît sous Nom de l'application dans le tableau Applications.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.
3. Sélectionnez **Android Enterprise** comme plate-forme.
4. Le bouton **Charger** ouvre le Google Play Store d'entreprise. Vous n'avez pas besoin de vous inscrire pour créer un compte de développeur et publier une application privée. Cliquez sur l'icône **Plus** dans le coin inférieur droit pour continuer.



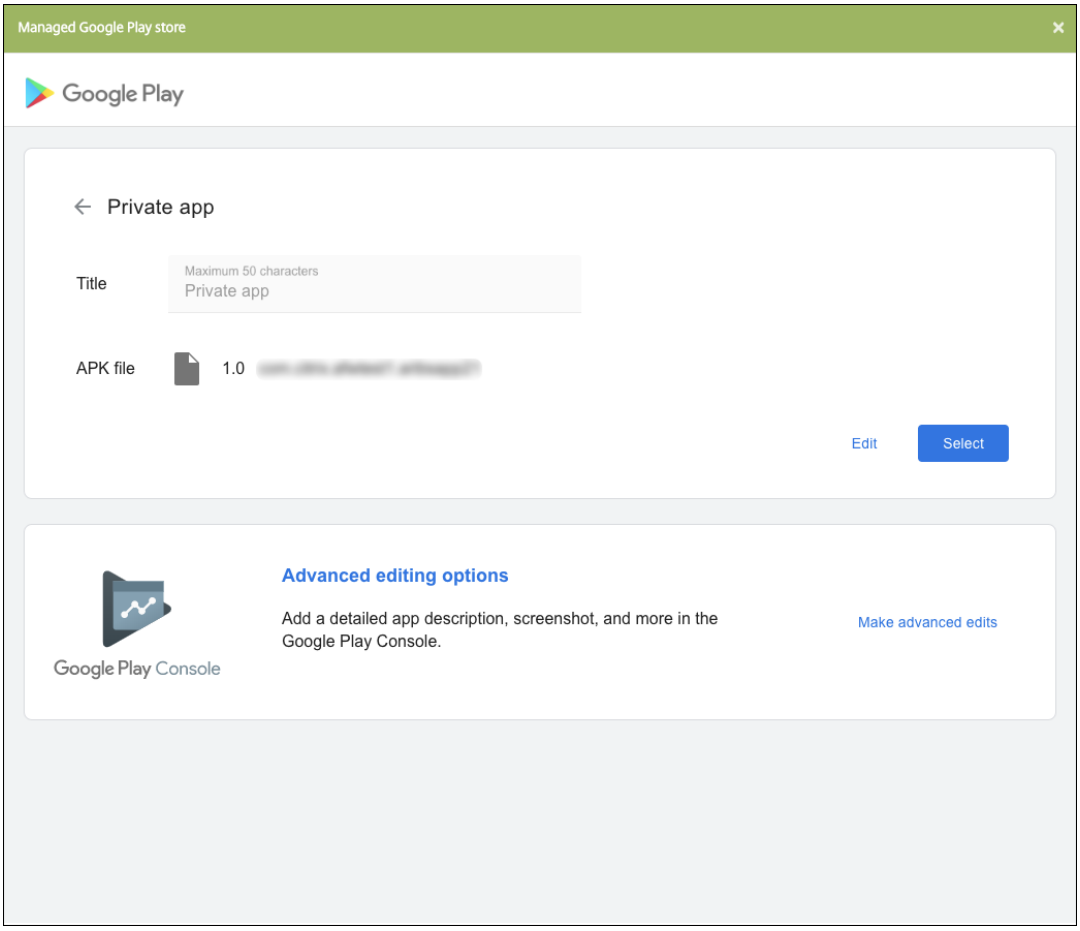
a) Tapez le nom de votre application et chargez le fichier .apk. Lorsque vous avez terminé, cliquez sur **Créer**. La publication de votre application privée peut prendre jusqu'à 10 minutes.



b) Entrez une adresse e-mail pour obtenir des mises à jour sur vos applications.



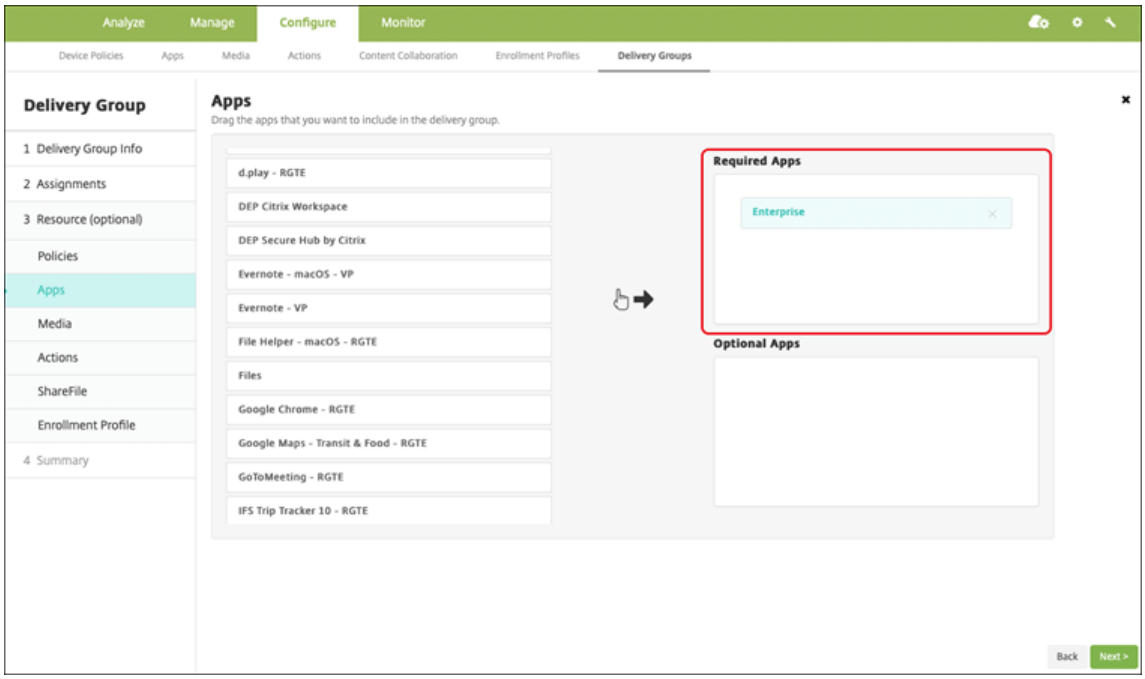
c) Une fois votre application publiée, cliquez sur l'icône correspondant à l'application privée. Si vous souhaitez ajouter une description pour l'application, modifier l'icône de l'application et effectuer d'autres actions, cliquez sur **Apporter des modifications avancées**. Sinon, cliquez sur **Sélectionner** pour ouvrir la page d'informations sur l'application.



5. Cliquez sur **Suivant**. La page d'informations sur l'application pour la plate-forme s'affiche.
6. Configurez les paramètres pour le type de plate-forme, notamment :
   - **Nom du fichier :** entrez un nouveau nom pour l'application (facultatif).
   - **Description de l'application :** entrez une nouvelle description pour l'application (facultatif).
   - **Version de l'application :** vous ne pouvez pas modifier ce champ.
   - **ID de package :** identifiant unique de votre application.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
   - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.
7. Configurez les règles de déploiement et la configuration du magasin.
8. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**. Pour de plus amples informations, consultez la section Déployer des ressources.

Étape 2 : Configurer le déploiement de l'application

1. Accédez à **Configurer > Groupes de mise à disposition** et sélectionnez le groupe de mise à disposition que vous avez configuré. Cliquez sur **Modifier**.
2. Dans la section **Applications**, faites glisser les applications souhaitées vers la zone **Applications requises**.



3. Sur la page **Résumé**, cliquez sur **Enregistrer**.
4. Sur la page **Groupes de mise à disposition**, sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.

Applications privées compatibles MDX

Pour ajouter des applications Android Enterprise en tant qu'applications d'entreprise compatibles MDX :

1. Créez une application Android Enterprise privée et activez MDX sur l'application.
2. Ajoutez l'application à la console XenMobile.
   - Hébergez et publiez l'application sur le Google Play Store d'entreprise.
   - Ajoutez l'application à la console XenMobile en tant qu'application d'entreprise.
3. Ajoutez le fichier MDX à XenMobile.

Si vous décidez d'héberger et de publier des applications via le Google Play Store, n'optez pas pour la signature de certificat Google. Signez l'application avec le même certificat que celui utilisé pour activer l'application avec MDX. Pour plus d'informations sur la publication d'applications, consultez

la documentation Google sur Publier votre application et Signer votre application. Le SDK MAM n'encapsulant pas les applications, il ne nécessite donc pas de certificat autre que celui utilisé pour développer l'application.

Pour plus d'informations sur la publication d'applications privées via la console Google Play, consultez la documentation Google sur la procédure à suivre pour Publier des applications privées depuis la Play Console.

Pour publier une application via XenMobile, consultez les sections suivantes.

Préparer une application Android Enterprise privée

Lorsque vous créez une application Android Enterprise privée, assurez-vous de suivre l'article Bonnes pratiques pour les applications privées de Google.

Après avoir créé une application Android Enterprise privée, intégrez le SDK MAM à l'application ou encapsulez l'application à l'aide de MDX Toolkit. Ensuite, ajoutez les fichiers résultants à XenMobile.

Vous pouvez mettre à jour l'application en téléchargeant un fichier .apk mis à jour. Les étapes suivantes décrivent l'encapsulation de l'application avec MDX Toolkit.

1. Créez votre application Android Enterprise privée et générez un fichier .apk signé.
2. L'exemple de fichier suivant contient toutes les stratégies connues, dont certaines peuvent ne pas être applicables à votre environnement. Tous les paramètres inutilisables sont ignorés. Créez un fichier XML avec les paramètres suivants :

```
<?xml version="1.0" encoding="UTF-8"?>
<MobileAppPolicies>
    <PolicySchemaVersion>
        1.0
    </PolicySchemaVersion>
    <Policies>
        <DevicePasscode>false</DevicePasscode>
        <AppPasscode>false</AppPasscode>
        <MaxOfflinePeriod>72</MaxOfflinePeriod>
        <StepupAuthAddress/>
        <RequireUserEntropy>false</RequireUserEntropy>
        <BlockRootedDevices>true</BlockRootedDevices>
        <BlockDebuggerAccess>false</BlockDebuggerAccess>
        <RequireDeviceLock>false</RequireDeviceLock>
        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
           NonCompliantDeviceBehavior>
        <WifiOnly>false</WifiOnly>
        <RequireInternalNetwork>false</RequireInternalNetwork>
        <InternalWifiNetworks/>
```



```
19          <AllowedWifiNetworks/>
20          <UpgradeGracePeriod>168</UpgradeGracePeriod>
21          <WipeDataOnAppLock>false</WipeDataOnAppLock>
22          <ActivePollPeriod>60</ActivePollPeriod>
23          <PublicFileAccessLimitsList/>
24          <CutAndCopy>Unrestricted</CutAndCopy>
25          <Paste>Unrestricted</Paste>
26          <DocumentExchange>Unrestricted</DocumentExchange>
27          <OpenInExclusionList/>
28          <InboundDocumentExchange>Unrestricted</
                InboundDocumentExchange>
29          <InboundDocumentExchangeWhitelist/>
30          <connectionSecurityLevel>TLS</connectionSecurityLevel>
31          <DisableCamera>false</DisableCamera>
32          <DisableGallery>false</DisableGallery>
33          <DisableMicrophone>false</DisableMicrophone>
34          <DisableLocation>false</DisableLocation>
35          <DisableSms>false</DisableSms>
36          <DisableScreenCapture>false</DisableScreenCapture>
37          <DisableSensor>false</DisableSensor>
38          <DisableNFC>false</DisableNFC>
39          <BlockLogs>false</BlockLogs>
40          <DisablePrinting>false</DisablePrinting>
41          <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
                MvpnNetworkAccess>
42          <MvpnSessionRequired>False</MvpnSessionRequired>
43          <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>
44          <DisableLocalhostConnections>false</
                DisableLocalhostConnections>
45          <CertificateLabel/>
46          <DefaultLoggerOutput>file,console</DefaultLoggerOutput>
47          <DefaultLoggerLevel>15</DefaultLoggerLevel>
48          <MaxLogFiles>2</MaxLogFiles>
49          <MaxLogFileSize>2</MaxLogFileSize>
50          <RedirectSystemLogs>false</RedirectSystemLogs>
51          <EncryptLogs>false</EncryptLogs>
52          <GeofenceLongitude>0</GeofenceLongitude>
53          <GeofenceLatitude>0</GeofenceLatitude>
54          <GeofenceRadius>0</GeofenceRadius>
55          <EnableGoogleAnalytics>false</EnableGoogleAnalytics>
56          <Authentication>OfflineAccessOnly</Authentication>
57          <ReauthenticationPeriod>480</ReauthenticationPeriod>
58          <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
59      </Policies>
60  </MobileAppPolicies>
```



```
61 <!--NeedCopy-->
```

3. Encapsulez l'application à l'aide de l'outil MDX Toolkit. Pour de plus amples informations sur l'utilisation de l'outil MDX Toolkit, consultez la section Encapsulation d'applications mobiles Android.

   Définissez le paramètre **apptype** sur **Premium**. Utilisez le fichier XML de l'étape précédente dans la commande décrite ci-dessous.

   Si vous connaissez l'URL de magasin de l'application, définissez le paramètre **storeURL** sur l'URL du magasin. Les utilisateurs téléchargent l'application à partir de l'URL du magasin après la publication de l'application.

   Voici un exemple de commande MDX Toolkit utilisée pour encapsuler une application appelée SampleAEapp :

```
1  ```
2   java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -
       Duser.variant
3   -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
4   -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
5   -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
6   -MinPlatform 5.0
7   -keystore /MyKeystore
8   -storepass mystorepwd123
9   -keyalias key0
10  -keypass mykeypwd123
11  -storeURL "https://play.google.com/store/apps/details?id=
       SampleAEappPackage"
12  -appType Premium
13  -premiumMdxPolicies <Path to Premium policy XML>
14 <!--NeedCopy--> ```
```

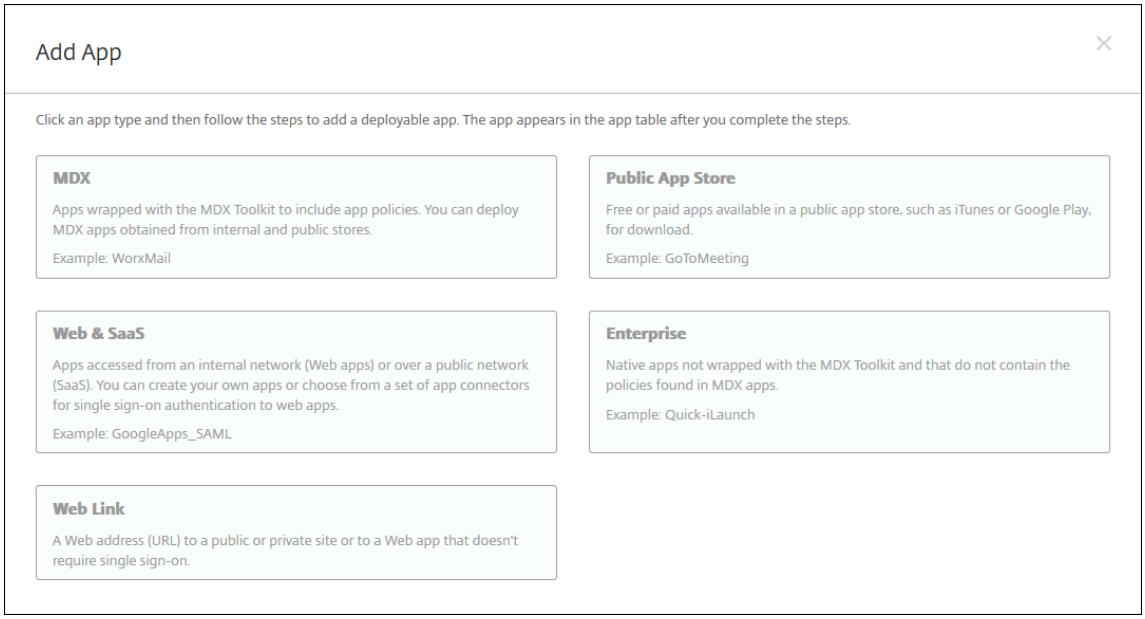
   L'encapsulation de l'application génère un fichier .apk encapsulé et un fichier .mdx.

Ajouter le fichier .apk encapsulé

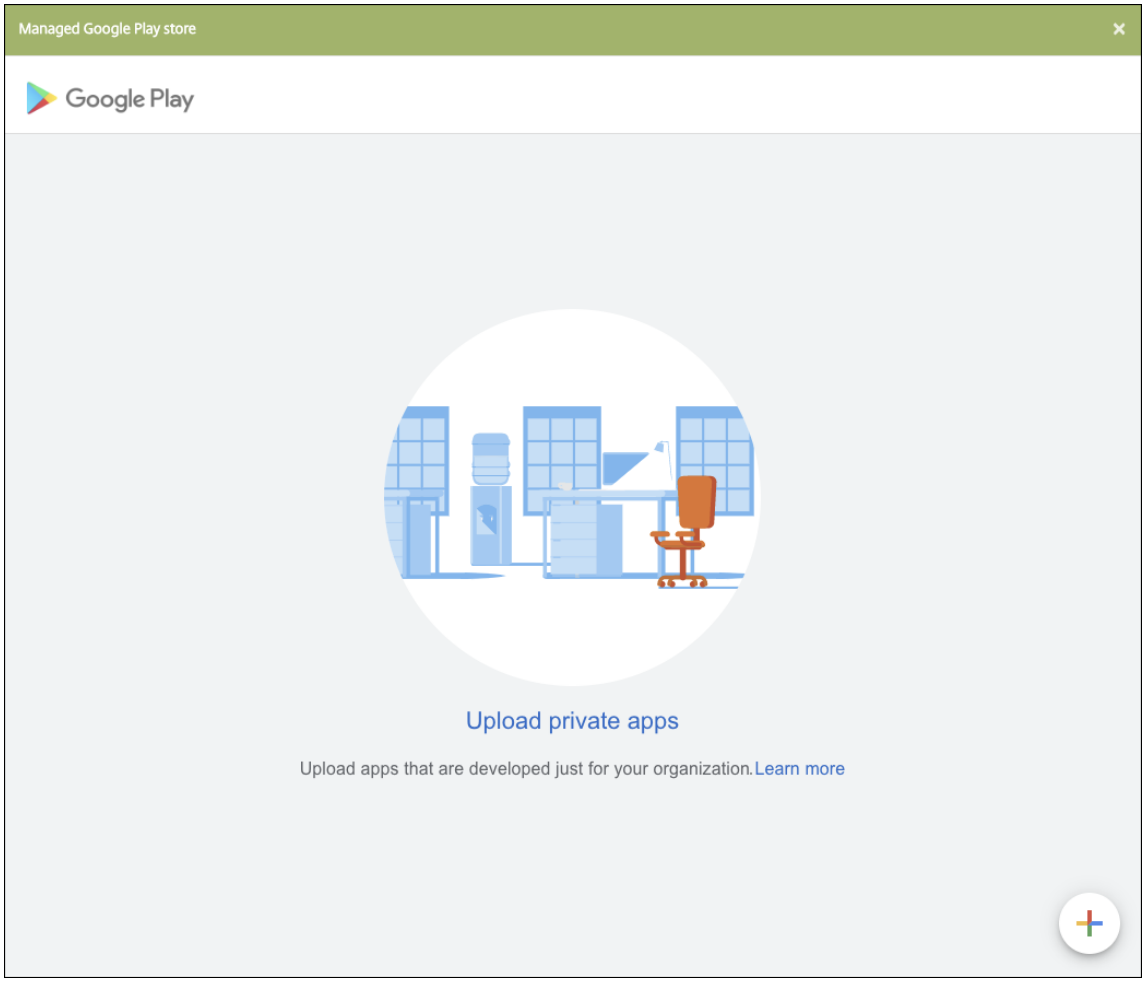
Ajoutez l'application à l'aide d'une des deux façons suivantes :

- Publiez l'application directement sur le Google Play Store d'entreprise et ajoutez-la à la console XenMobile en tant qu'application Play Store d'entreprise. Suivez la procédure Publier des applications privées de la documentation Google, puis suivez les étapes décrites dans la section Applications gérées du magasin d'applications.
- Ajoutez l'application à la console XenMobile en tant qu'application d'entreprise. Effectuez les opérations suivantes :

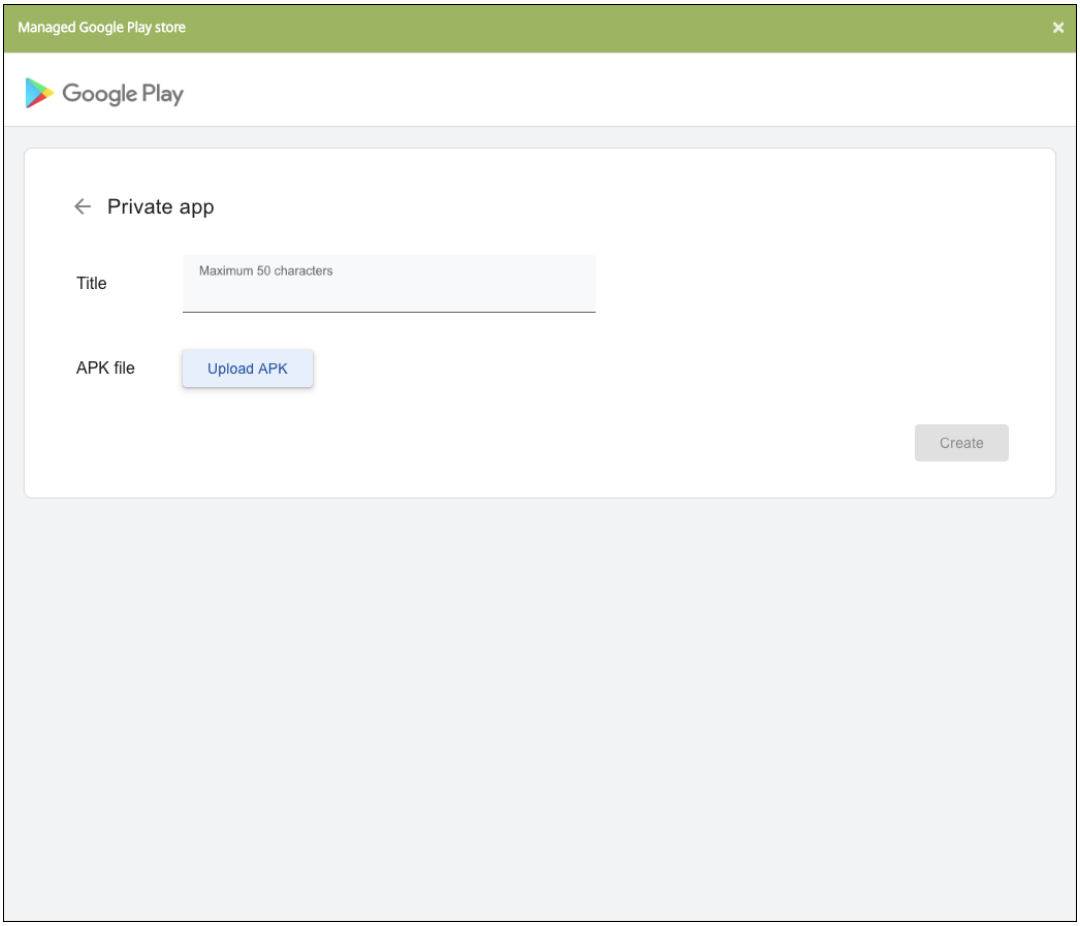
1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'ouvre.
2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



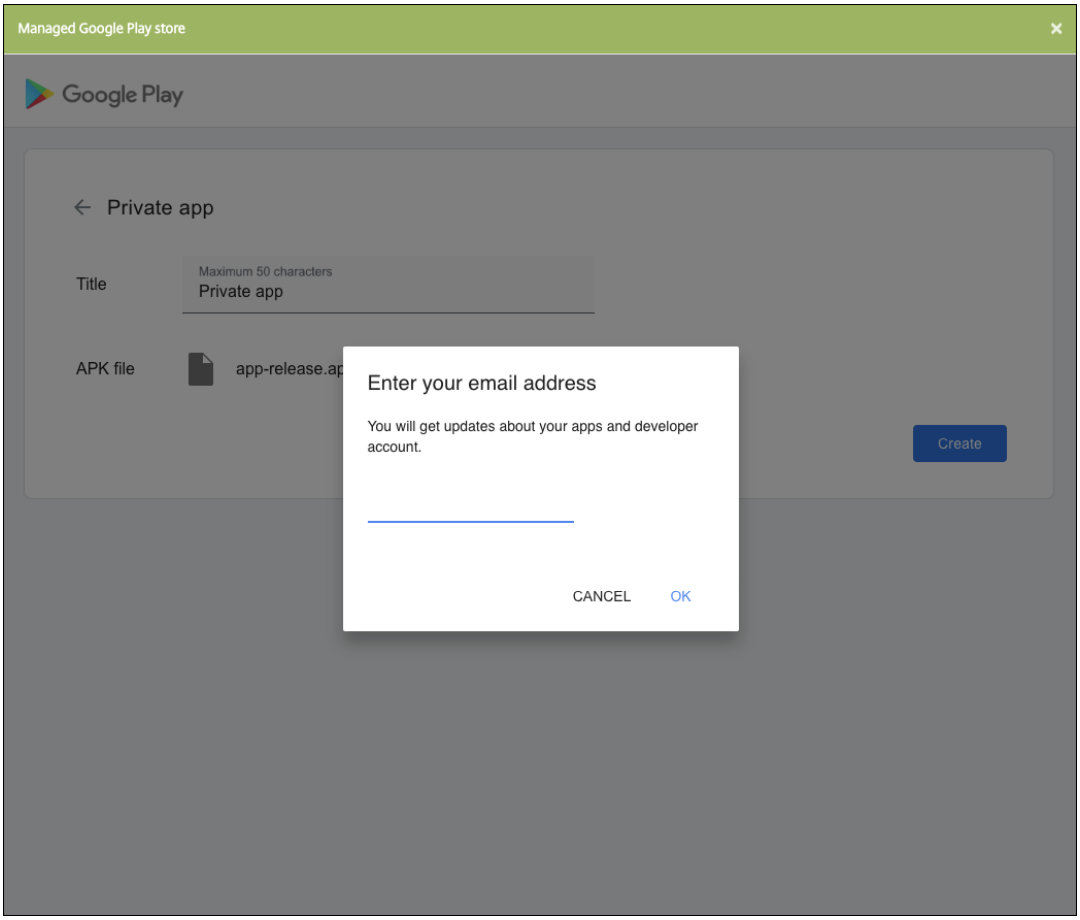
3. Cliquez sur **Entreprise**. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Il apparaît sous Nom de l'application dans le tableau Applications.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.
4. Sélectionnez **Android Enterprise** comme plate-forme.
5. Le bouton **Charger** ouvre le Google Play Store d'entreprise. Vous n'avez pas besoin de vous inscrire pour créer un compte de développeur et publier une application privée. Cliquez sur l'icône **Plus** dans le coin inférieur droit pour continuer.



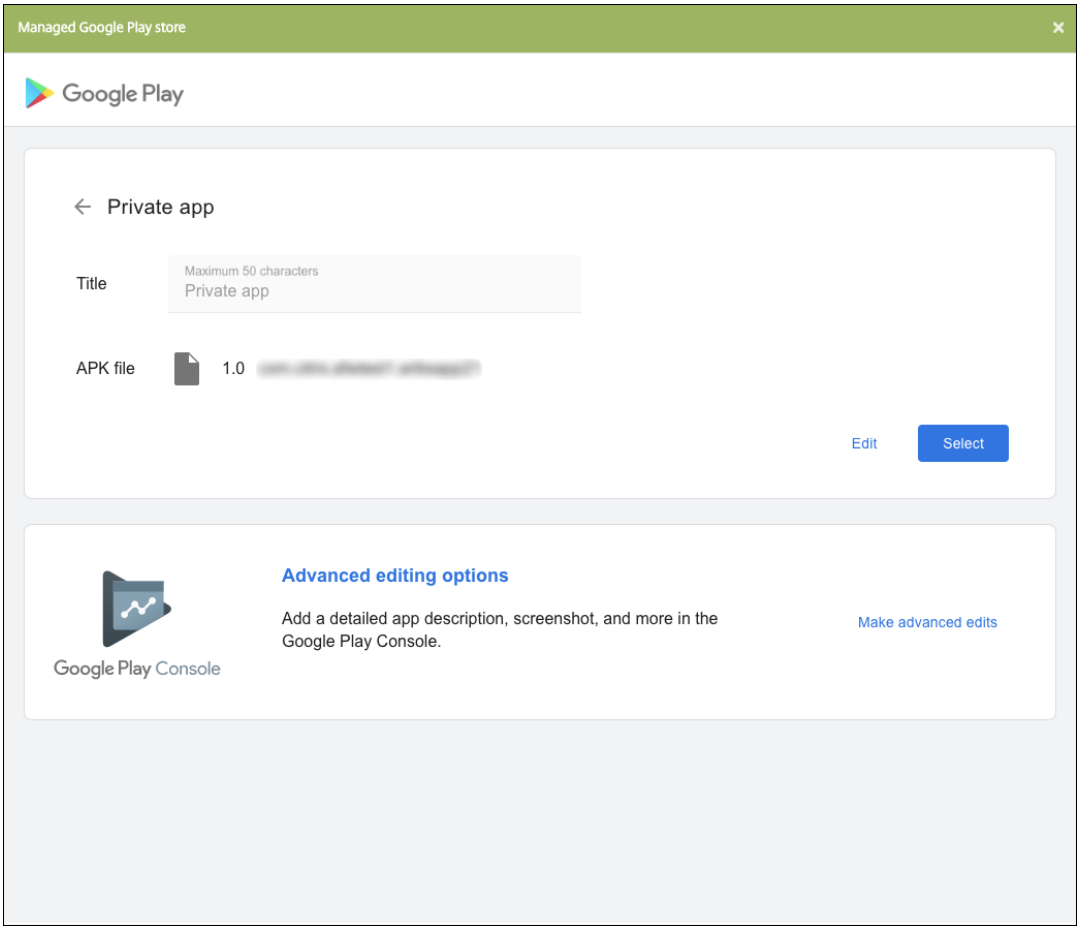
a) Tapez le nom de votre application et chargez le fichier .apk. Lorsque vous avez terminé, cliquez sur **Créer**. La publication de votre application privée peut prendre jusqu'à 10 minutes.



b) Entrez une adresse e-mail pour obtenir des mises à jour sur vos applications.



c) Une fois votre application publiée, cliquez sur l'icône d'une application privée, puis sur **Sélectionner** pour ouvrir la page d'informations de l'application.



6. Cliquez sur **Suivant**. La page d'informations sur l'application pour la plate-forme s'affiche.
7. Configurez les paramètres pour le type de plate-forme, notamment :
   - **Nom du fichier :** entrez un nouveau nom pour l'application (facultatif).
   - **Description de l'application :** entrez une nouvelle description pour l'application (facultatif).
   - **Version de l'application :** vous ne pouvez pas modifier ce champ.
   - **ID de package :** identifiant unique de votre application.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
   - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.
8. Configurez les règles de déploiement et la configuration du magasin.
9. Sur la page **Android Enterprise App**, cliquez sur **Suivant**. La page **Approbations** s'affiche.

   Pour utiliser des workflows afin d'exiger une approbation avant d'autoriser les utilisateurs à

accéder à l'application, consultez la section Appliquer les workflows. Si vous n'avez pas besoin de workflows d'approbation, vous pouvez passer à l'étape 13.

10. Cliquez sur **Suivant**.
11. La page **Attribution de groupes de mise à disposition** s'affiche. Aucune action n'est nécessaire sur cette page. Vous configurez les groupes de mise à disposition et le calendrier de déploiement pour cette application lorsque vous ajoutez le fichier .mdx. Cliquez sur **Enregistrer**.

Facultatif : ajouter ou modifier l'URL du magasin

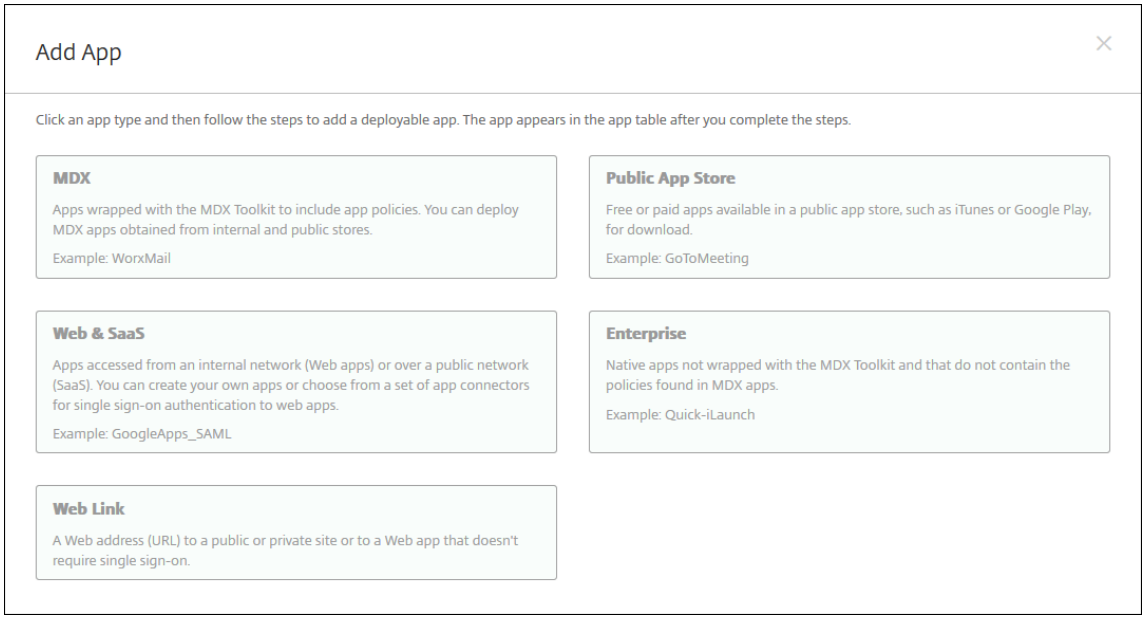
Si vous ne connaissiez pas l'URL du magasin lorsque vous avez encapsulé l'application, ajoutez l'URL du magasin maintenant.

1. Affichez l'application dans le Google Play Store d'entreprise. Lorsque vous sélectionnez l'application, l'URL du magasin apparaît dans la barre d'adresse de votre navigateur. Copiez le nom du package de l'application à partir du formulaire URL. Par exemple : `https://play.google.com/store/apps/details?id=SampleAEappPackage`. L'URL que vous copiez peut commencer par `https://play.google.com/work/`. Assurez-vous de remplacer `work` par `store`.
2. Utilisez le MDX Toolkit pour ajouter l'URL du magasin au fichier .mdx :

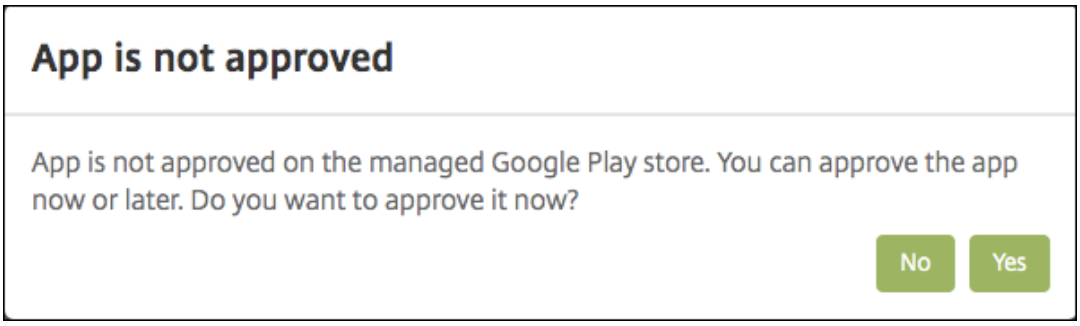
```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \
setinfo \
-in ~/Desktop/SampleApps/Sample.mdx \
-out ~/Desktop/SampleApps/wrapped/Sample.mdx \
-storeURL "https://play.google.com/store/apps/details?id=
   SampleAEappPackage"
<!--NeedCopy-->
```

Ajouter le fichier .mdx

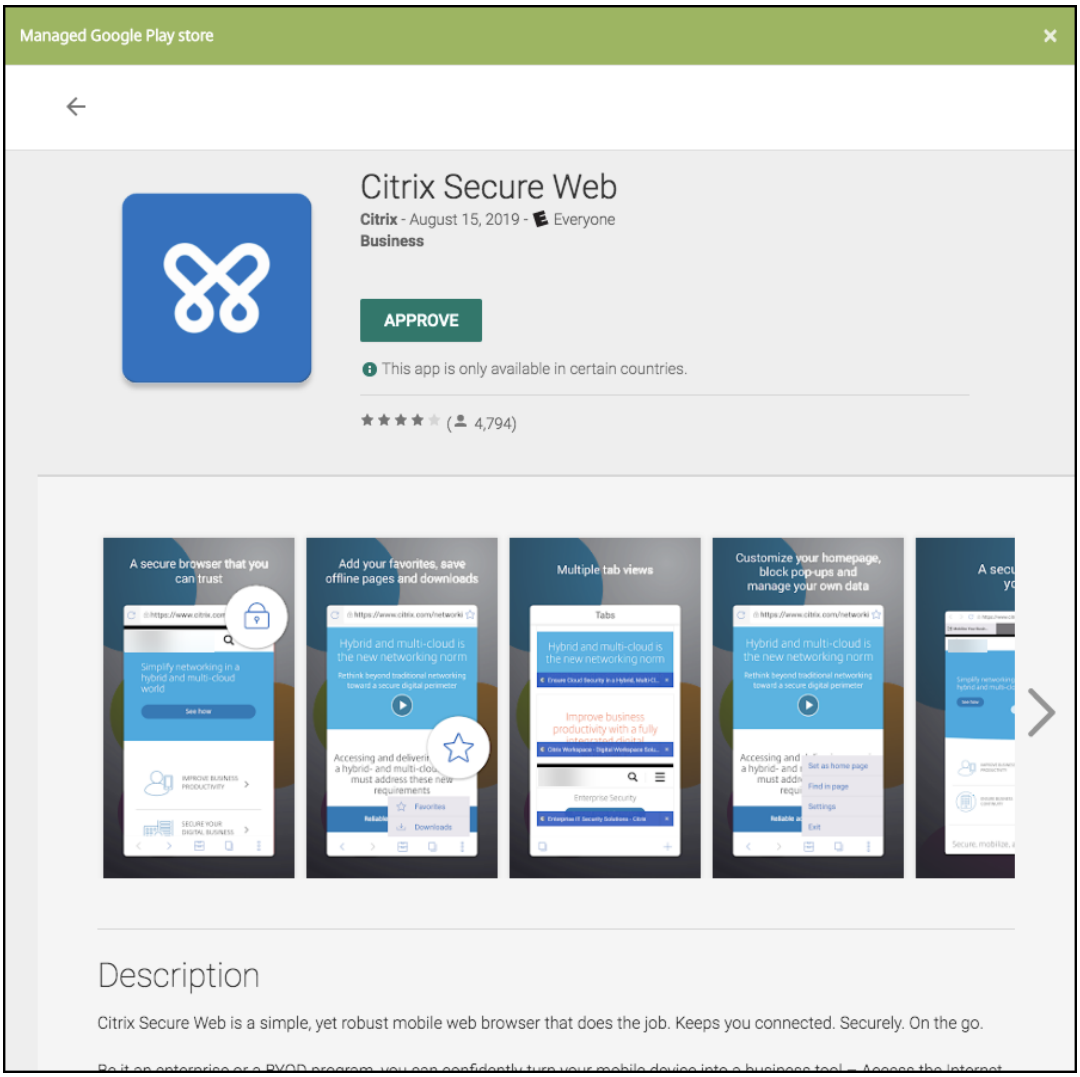
1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



2. Cliquez sur **MDX**. La page **Informations sur l'application MDX** s'affiche. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous **Nom de l'application** dans le tableau **Applications**.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.
3. Sélectionnez **Android Enterprise** comme plate-forme.
4. Cliquez sur **Charger** et accédez au fichier MDX. Android Enterprise prend uniquement en charge les applications encapsulées avec MDX Toolkit.
   - L'interface utilisateur vous avertit si l'application jointe nécessite l'approbation du Google Play Store d'entreprise. Pour approuver l'application sans quitter la console XenMobile, cliquez sur **Oui**.



Après l'ouverture du Google Play Store d'entreprise, suivez les instructions pour approuver et enregistrer l'application.



Lorsque vous ajoutez l'application, la page de **Détails sur l'application** apparaît.

5. Pour configurer ces paramètres :

   - **Nom du fichier :** entrez le nom du fichier associé à l'application.
   - **Description de l'application :** entrez une description pour l'application.
   - **Version de l'application :** si vous le souhaitez, entrez le numéro de version de l'application.
   - **ID de package :** entrez l'ID du package de l'application, obtenu à partir du Google Play Store d'entreprise.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système

d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
- **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.

6. Configurez les **stratégies MDX**. Les stratégies MDX varient selon la plate-forme et incluent des options dans des domaines de stratégie tels que l'authentification, la sécurité de l'appareil et les restrictions applicatives. Dans la console, les stratégies ont une info-bulle qui décrit chacune d'entre elles. Pour plus d'informations sur les stratégies applicatives disponibles pour chaque type de plate-forme, consultez :
   - Présentation du SDK MAM
   - Synopsis des stratégies applicatives tierces MDX
7. Configurez les règles de déploiement et la configuration du magasin.

   L'option **Déployer pour les connexions permanentes** s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

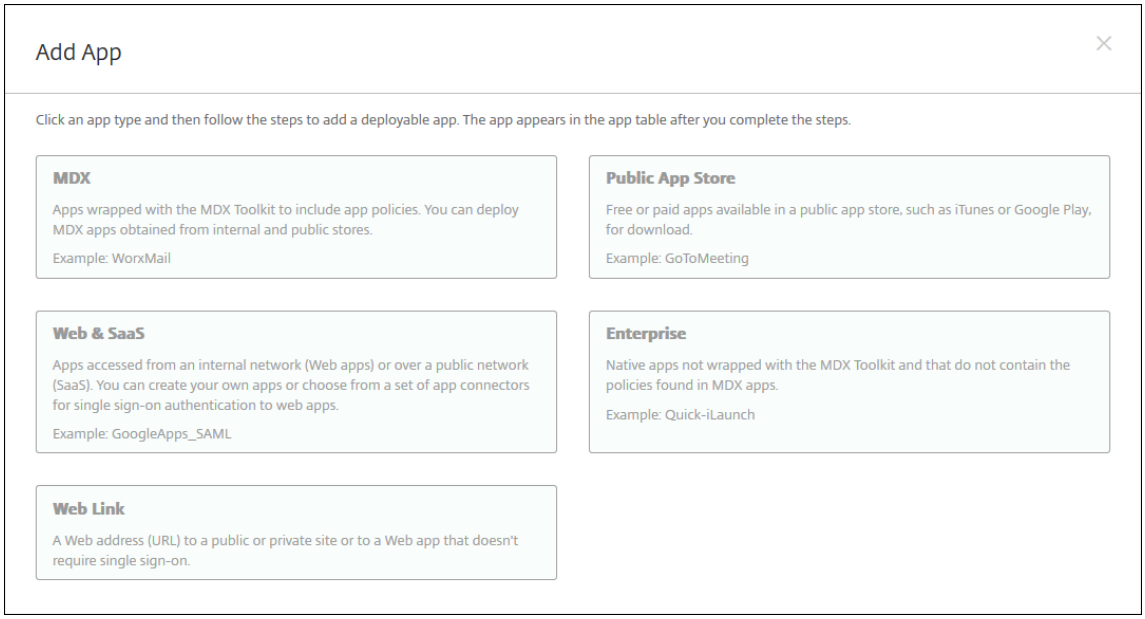
   L'option de connexion permanente :
   - N'est pas disponible pour les clients Android Enterprise ayant commencé à utiliser Endpoint Management avec la version 10.18.19 ou ultérieure.
   - N'est pas recommandée pour les clients Android Enterprise ayant commencé à utiliser Endpoint Management avec une version antérieure à la version 10.18.19.

   Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.
8. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**. Pour de plus amples informations, consultez la section Déployer des ressources.

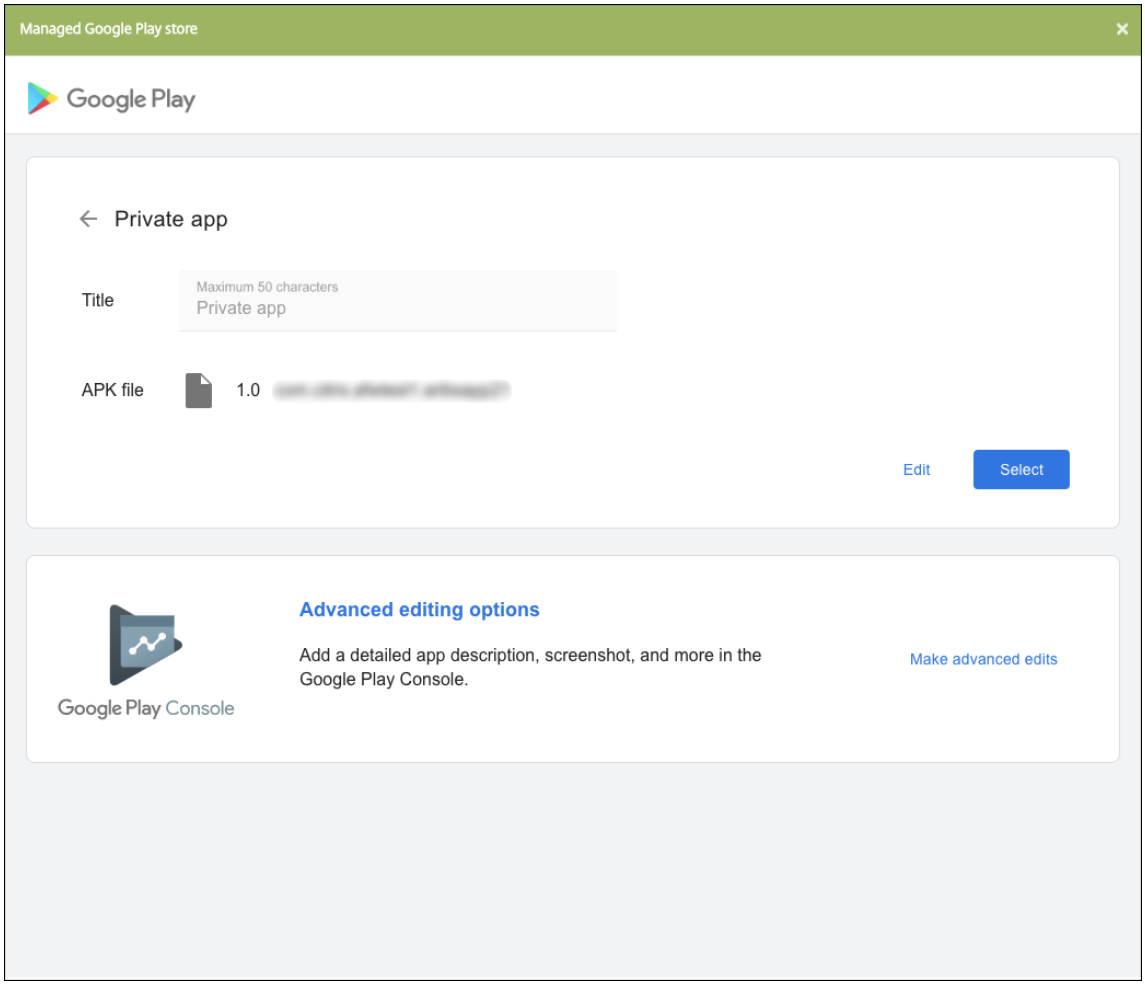
Mettre à jour l'application

Pour mettre à jour l'application Android Enterprise, encapsulez et téléchargez un fichier .apk mis à jour :

1. Encapsulez le fichier .apk de l'application mise à jour à l'aide du SDL MAM ou de MDX Toolkit.
2. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'ouvre.



3. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.
4. Cliquez sur **Entreprise**. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Il apparaît sous Nom de l'application dans le tableau Applications.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.
5. Sélectionnez **Android Enterprise** comme plate-forme.
6. Cliquez sur **Suivant**. La page **Android Enterprise Enterprise App** s'affiche.
7. Cliquez sur **Charger**.
8. Sur la page Google Play Store d'entreprise, sélectionnez l'application que vous souhaitez mettre à jour.
9. Sur la page d'informations sur l'application, cliquez sur **Modifier** en regard du nom du fichier .apk.



10. Accédez au nouveau fichier .apk et chargez-le.
11. Sur la page Google Play Store d'entreprise, cliquez sur **Enregistrer**.

Ancienne version d'Android Enterprise pour clients Google Workspace (anciennement G Suite)

August 18, 2021

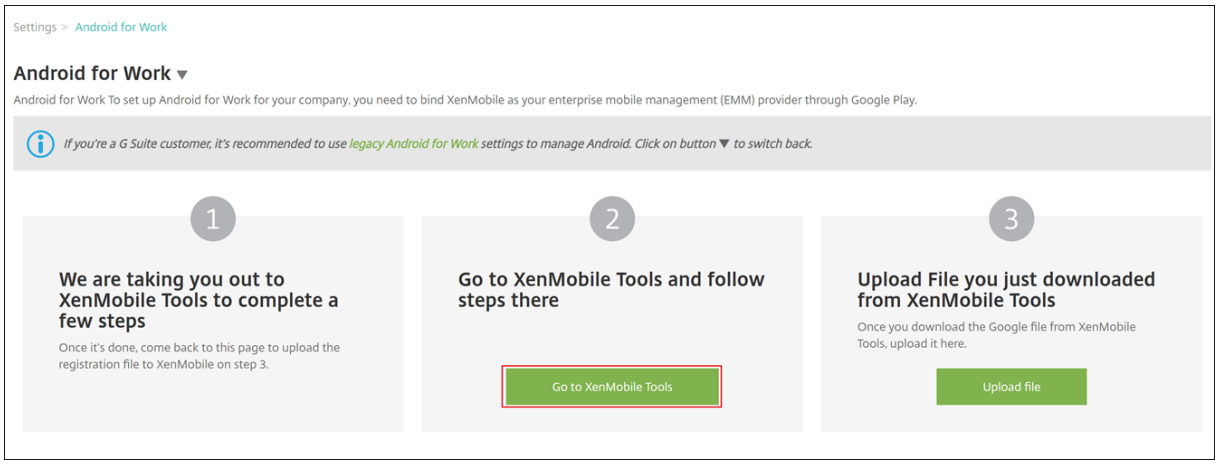
Les clients Google Workspace (anciennement G Suite) doivent utiliser les paramètres de l'ancienne version d'Android Entreprise pour configurer une ancienne version d'Android Entreprise.

Configuration requise pour l'ancienne version d'Android Entreprise :

- Un domaine publiquement accessible
- Un compte d'administrateur Google
- Les appareils qui prennent en charge les profils gérés et qui exécutent Android 5.0+ Lollipop

- Un compte Google sur lequel Google Play est installé
- Un profil de travail configuré sur l'appareil.

Pour démarrer la configuration de l'ancienne version d'Android Entreprise, cliquez sur **Ancienne version de Android Entreprise** dans la page **Android Entreprise** des paramètres XenMobile.



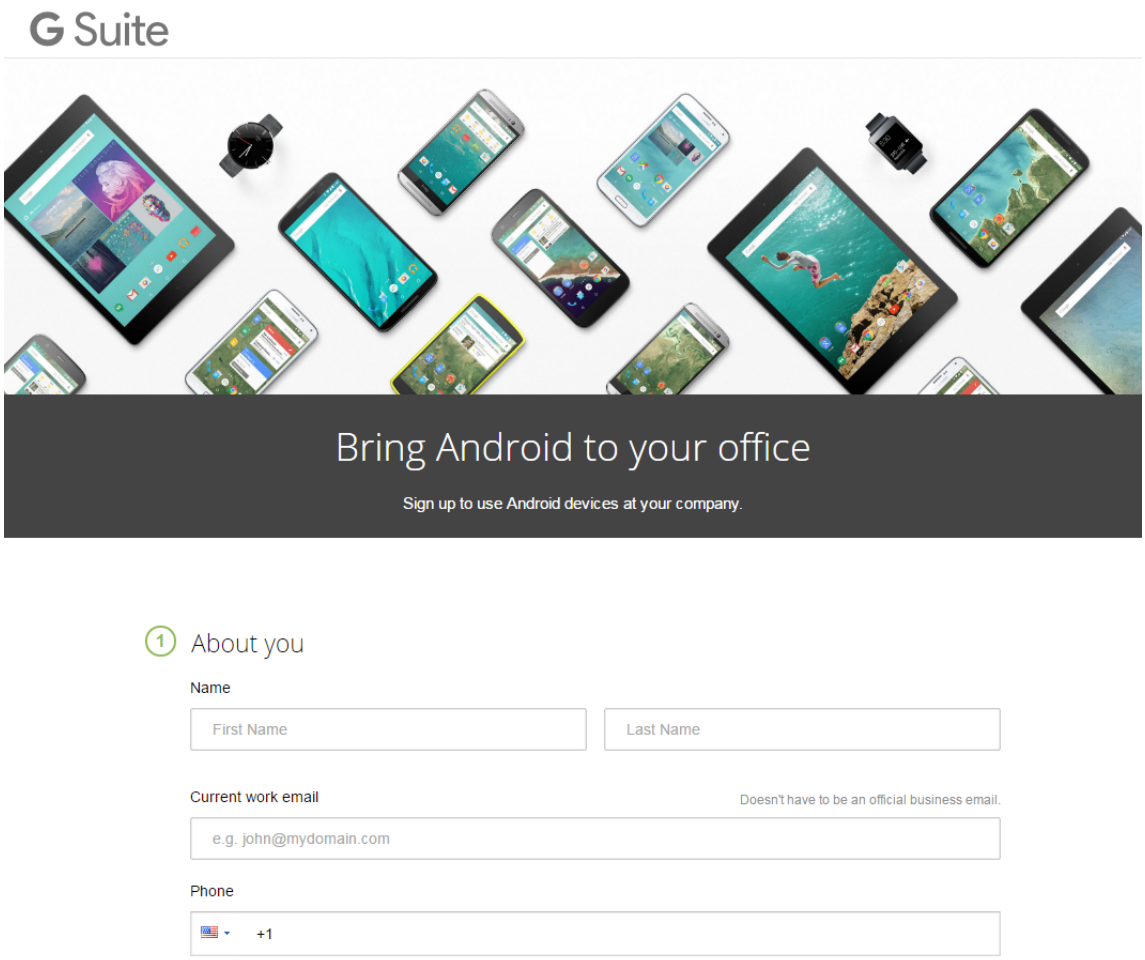
Créer un compte Android Entreprise

Pour pouvoir configurer un compte Android Entreprise, vous devez vérifier votre nom de domaine auprès de Google.

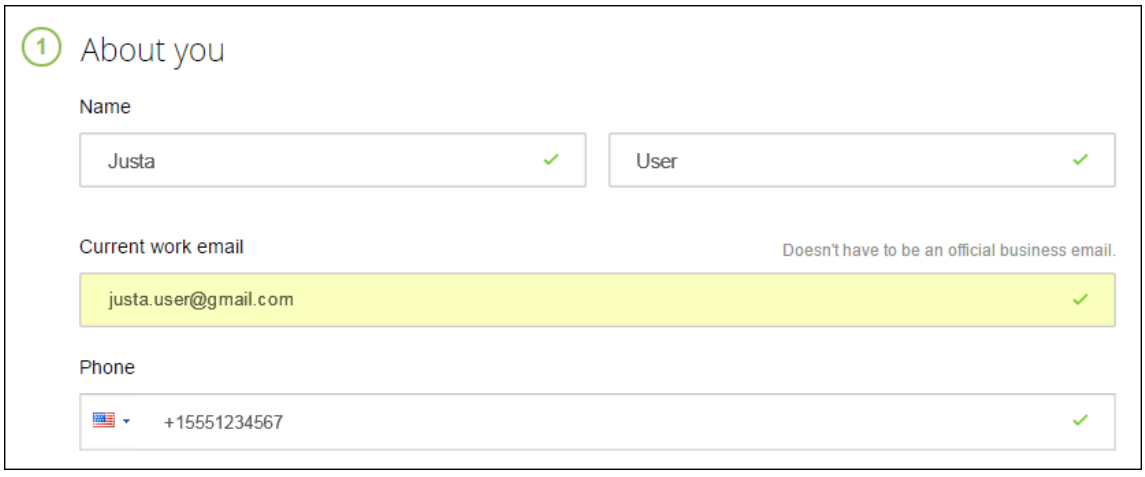
Si vous avez déjà vérifié votre nom de domaine auprès de Google, vous pouvez passer à cette étape : Configurer un compte de service Android Entreprise et télécharger un certificat Android Entreprise.

1. Accédez à https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

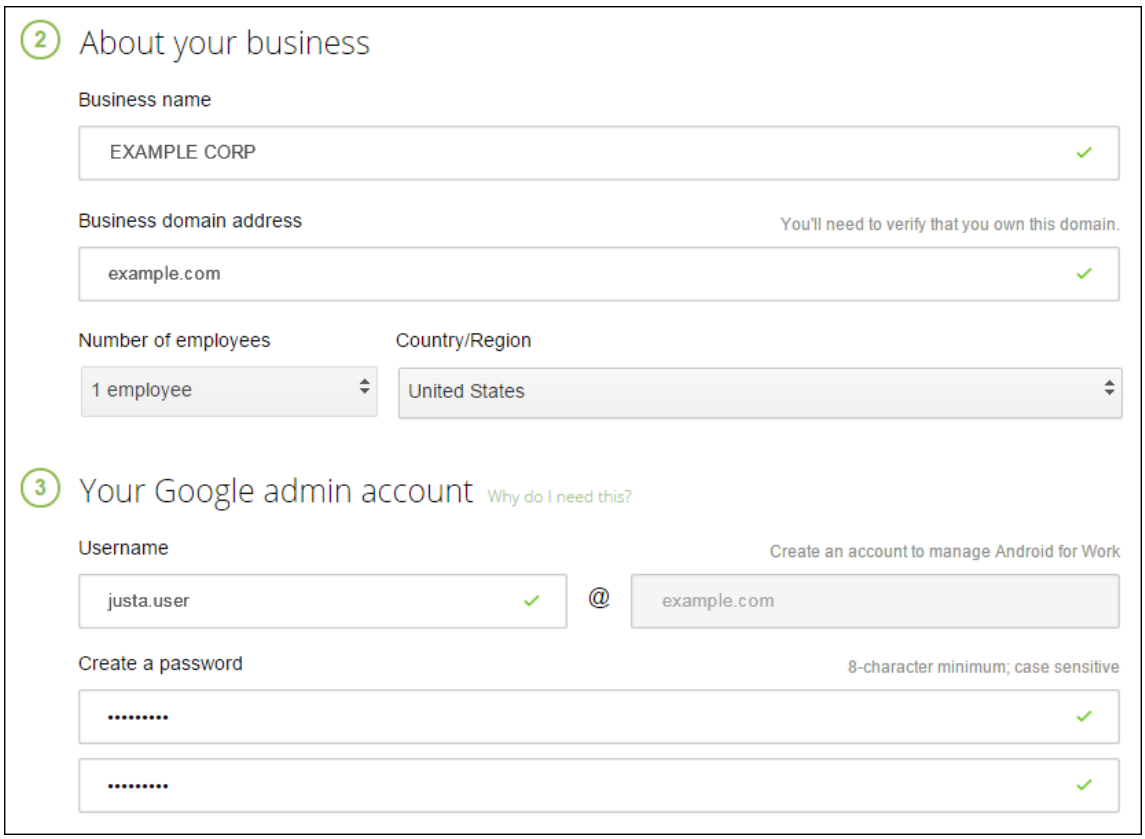
   La page suivante s'affiche où vous entrez vos informations d'administrateur et les informations sur l'entreprise.



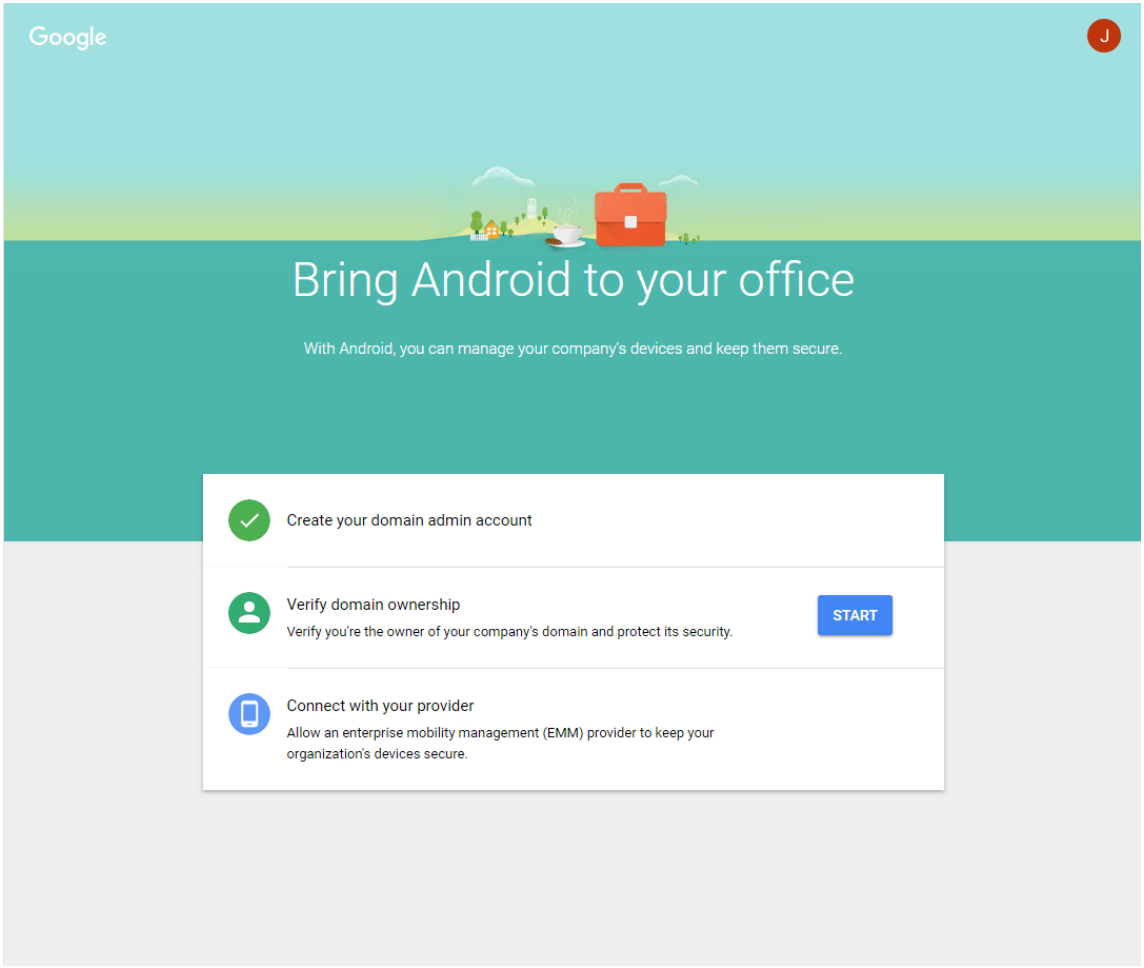
2. Entrez vos informations d'utilisateur administrateur.



3. Entrez vos informations d'entreprise, en plus de vos informations de compte d'administrateur.



La première étape de ce processus est terminée et la page suivante s’affiche.



Vérifier le propriétaire du domaine

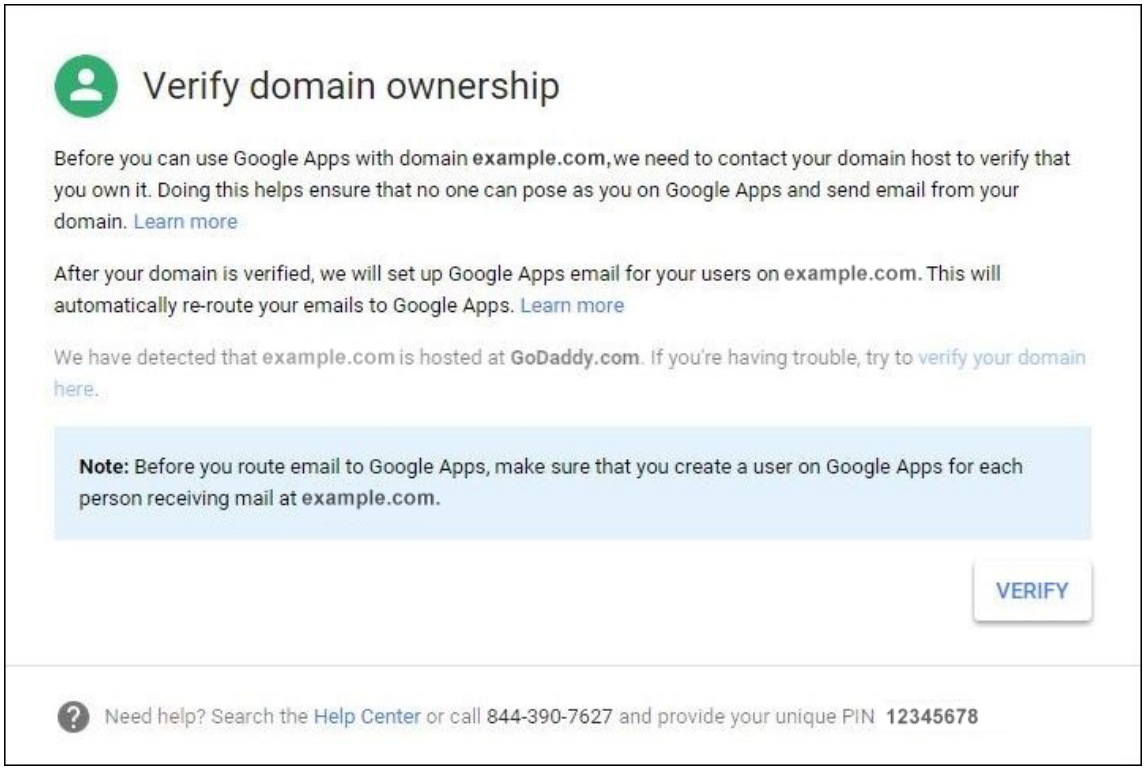
Autorisez Google à vérifier votre domaine de l'une des manières suivantes :

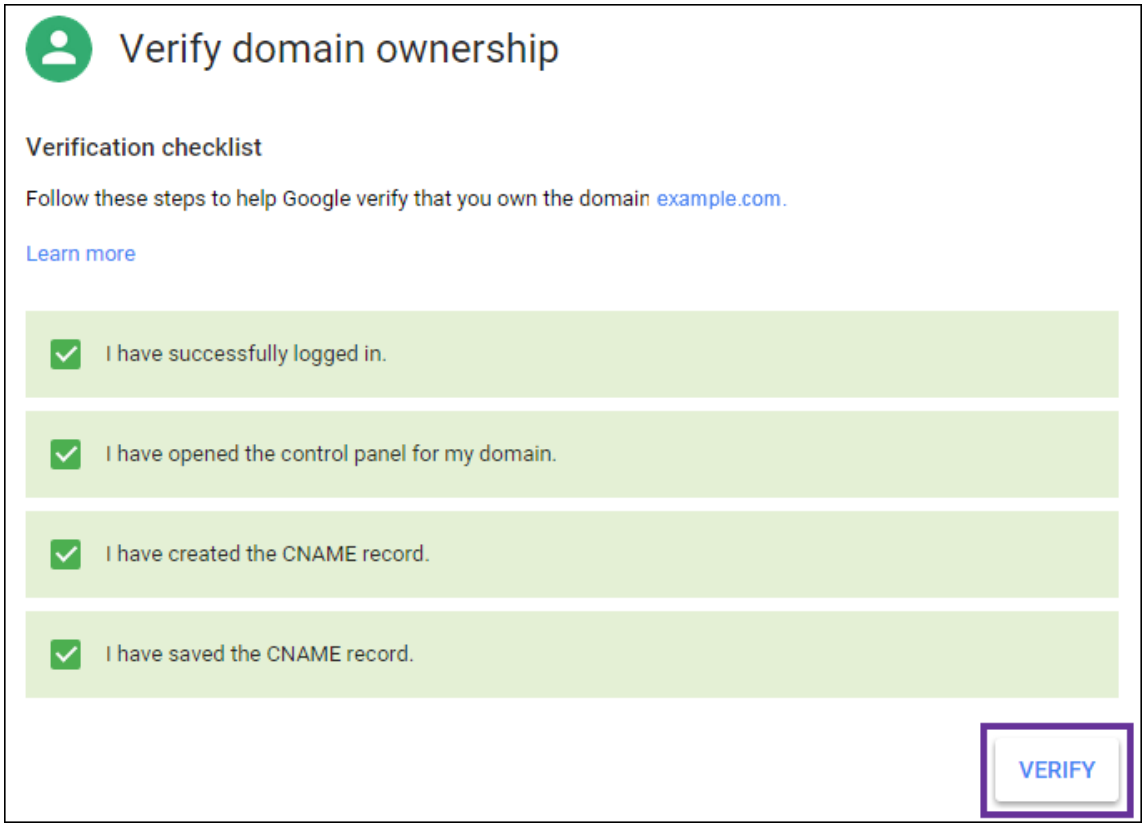
- Ajoutez un enregistrement TXT ou CNAME au site Web de votre hôte de domaine.
- Chargez un fichier HTML sur le serveur Web de votre domaine.
- Ajoutez une balise `<meta>` à votre page d'accueil. Google recommande la première méthode. Cet article ne couvre pas les étapes permettant de vérifier que votre domaine vous appartient, mais vous pouvez trouver les informations dont vous avez besoin sur : https://support.google.com/a/answer/6248925/.

1. Cliquez sur **Démarrer** pour commencer la vérification de votre domaine.

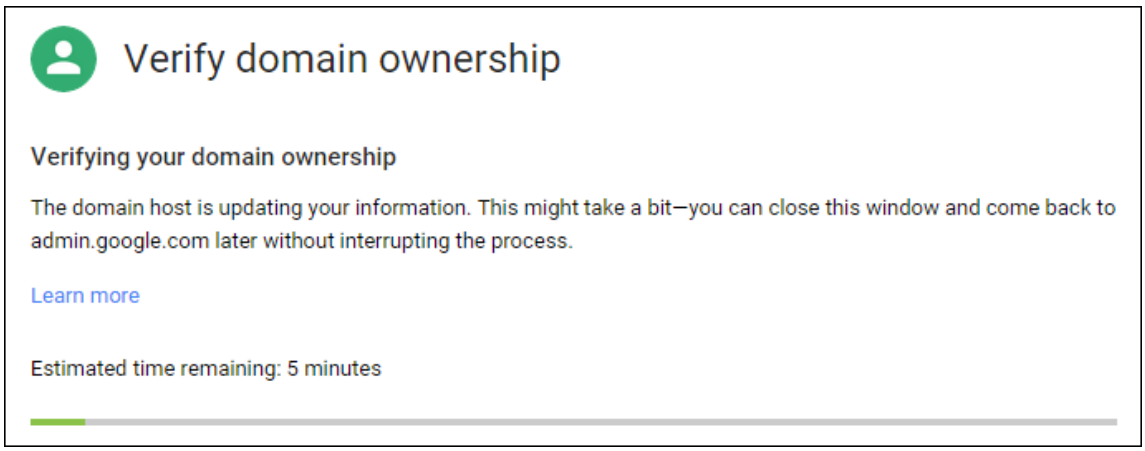
   La page **Valider la propriété du domaine** s'affiche. Suivez les instructions sur la page pour vérifier votre domaine.

2. Cliquez sur **Vérifier**.

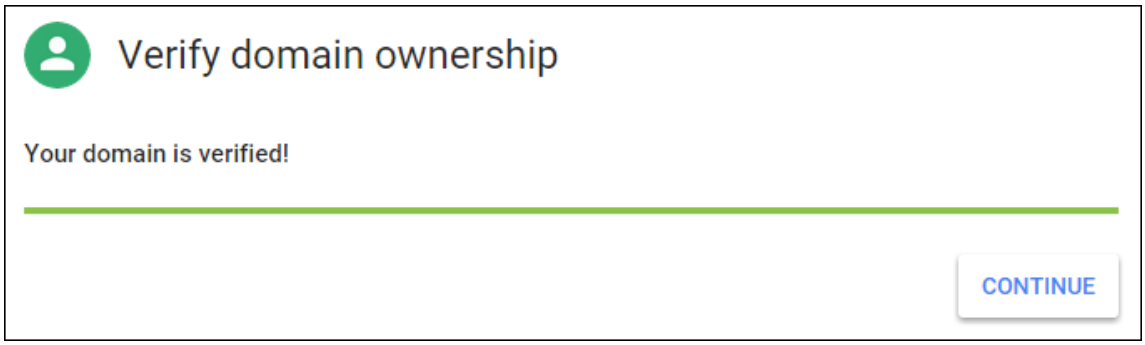




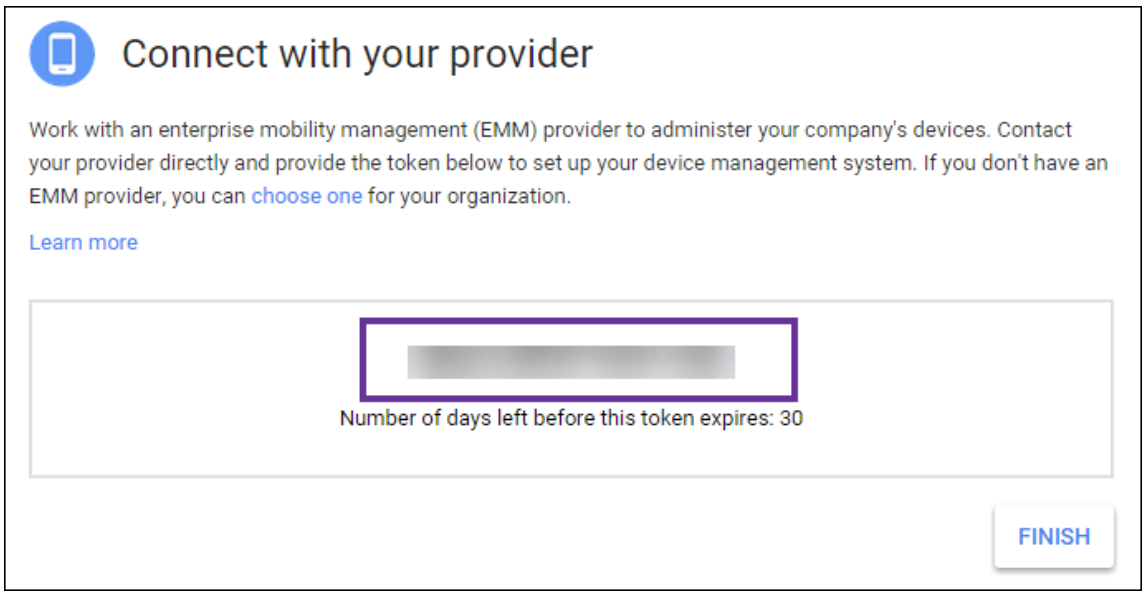
3. Google vérifie que vous êtes le propriétaire du domaine.



4. La page suivante s'affiche si la vérification réussit. Cliquez sur **Continuer**.



5. Google crée un jeton de liaison EMM que vous fournissez à Citrix lorsque vous configurez les paramètres d'Android Entreprise. Copiez et enregistrez le jeton ; vous en aurez besoin plus tard lors de la configuration.



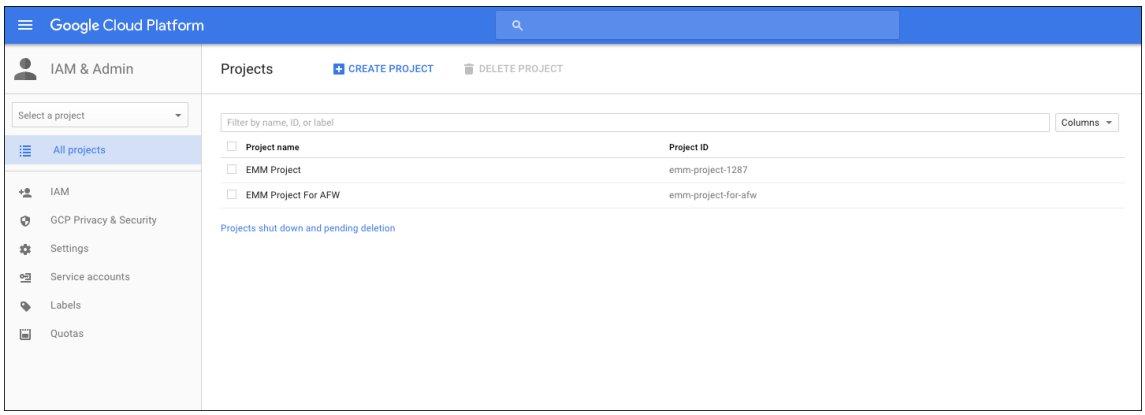
6. Cliquez sur **Terminer** pour terminer la configuration d'Android Entreprise. Une page s'affiche indiquant que vous avez vérifié avec succès votre domaine.

Une fois que vous avez créé un compte de service Android Entreprise, vous pouvez ouvrir une session sur la console d'administration Google pour gérer vos paramètres de gestion de la mobilité.

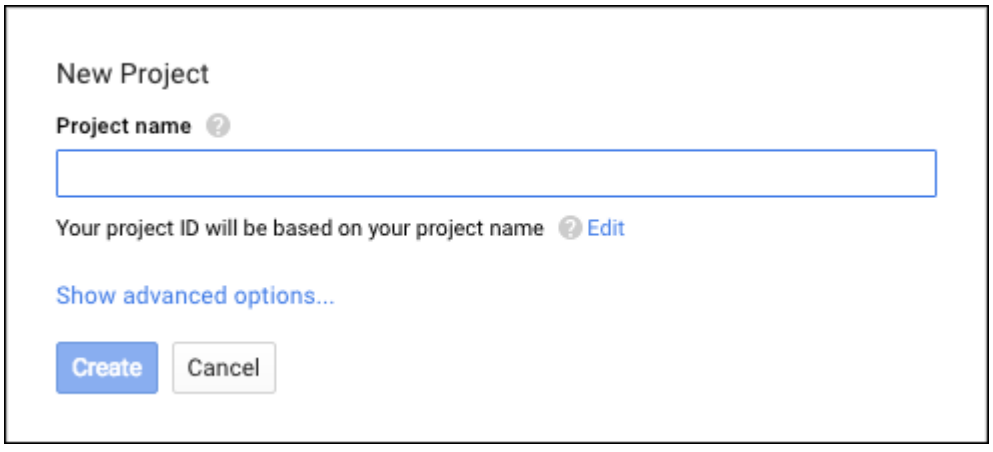
Définir un compte de service Android Entreprise et télécharger un certificat Android Entreprise

Pour autoriser XenMobile à contacter les services Google Play et Directory, vous devez créer un compte de service à l'aide du portail Project de Google destiné aux développeurs. Ce compte de service est utilisé pour permettre les communications entre serveurs entre XenMobile et les services Google pour Android. Pour plus d'informations sur le protocole d'authentification utilisé, accédez à https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

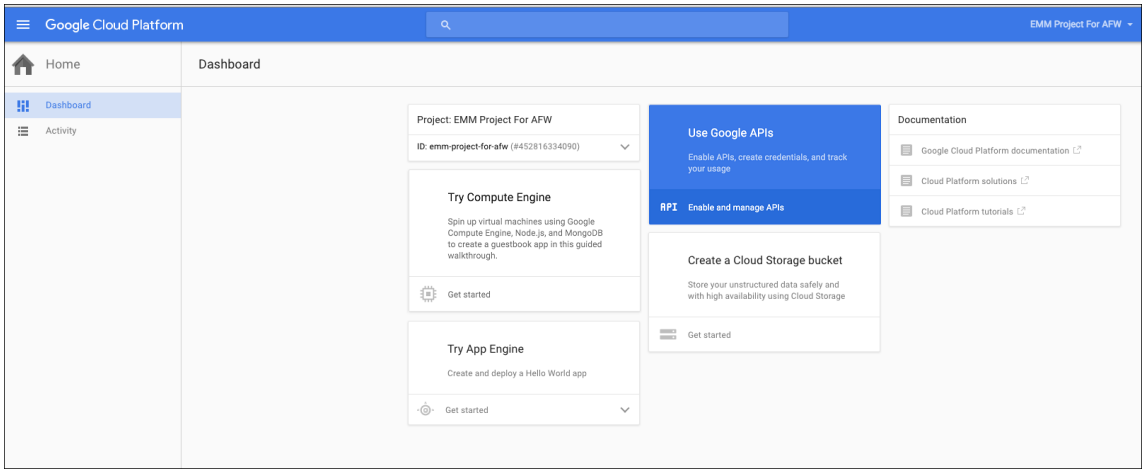
1. Dans un navigateur Web, accédez à https://console.cloud.google.com/project et ouvrez une session à l'aide de vos informations d'identification d'administrateur Google.
2. Dans la liste **Projets**, cliquez sur **Créer un projet**.



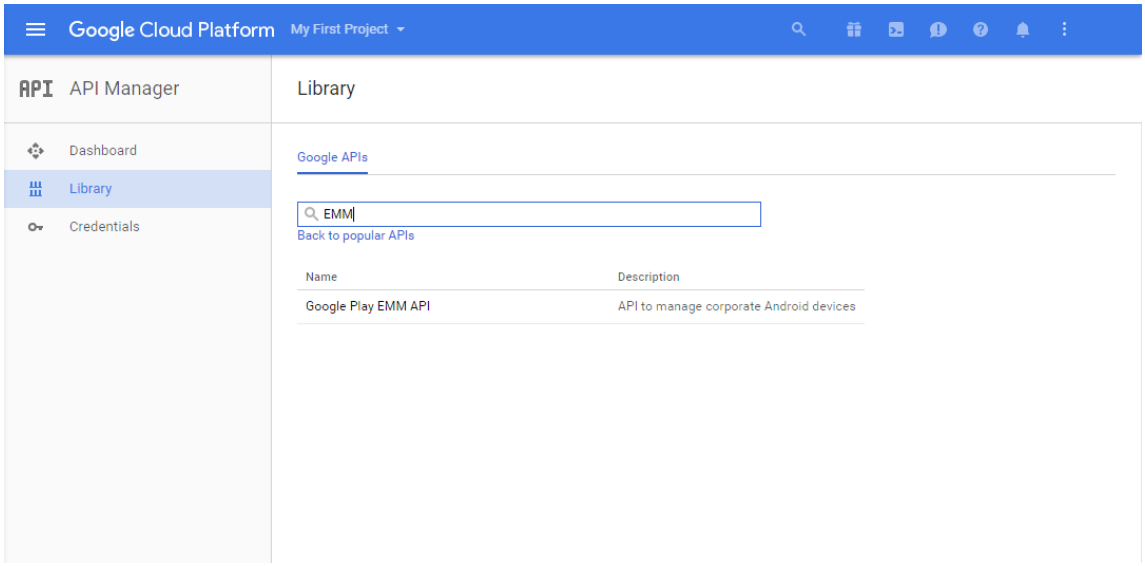
3. Dans **Nom du projet**, entrez un nom pour le projet.



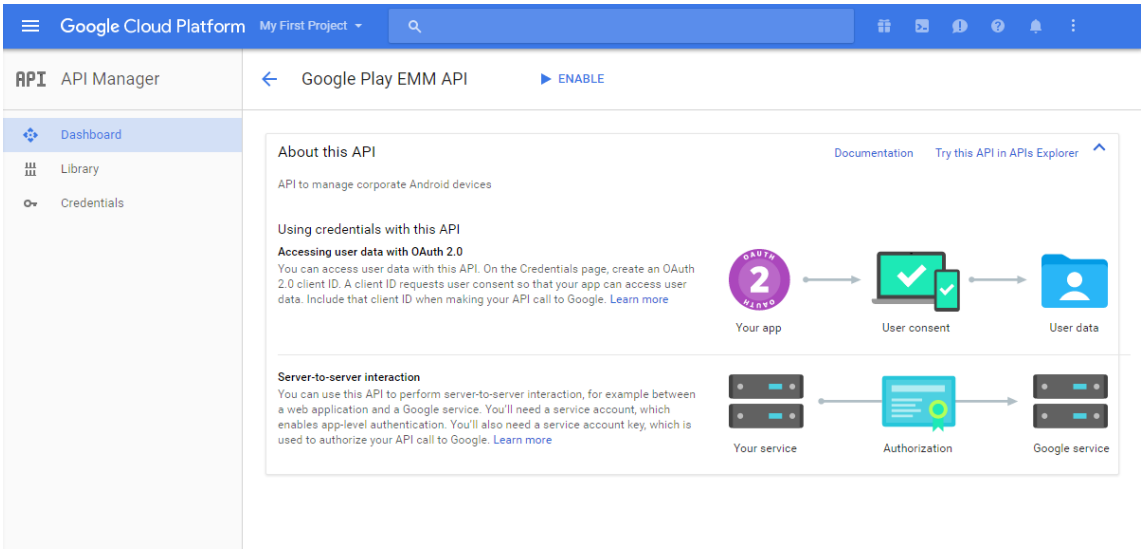
4. Sur le tableau de bord, cliquez sur **Utiliser les API de Google**.



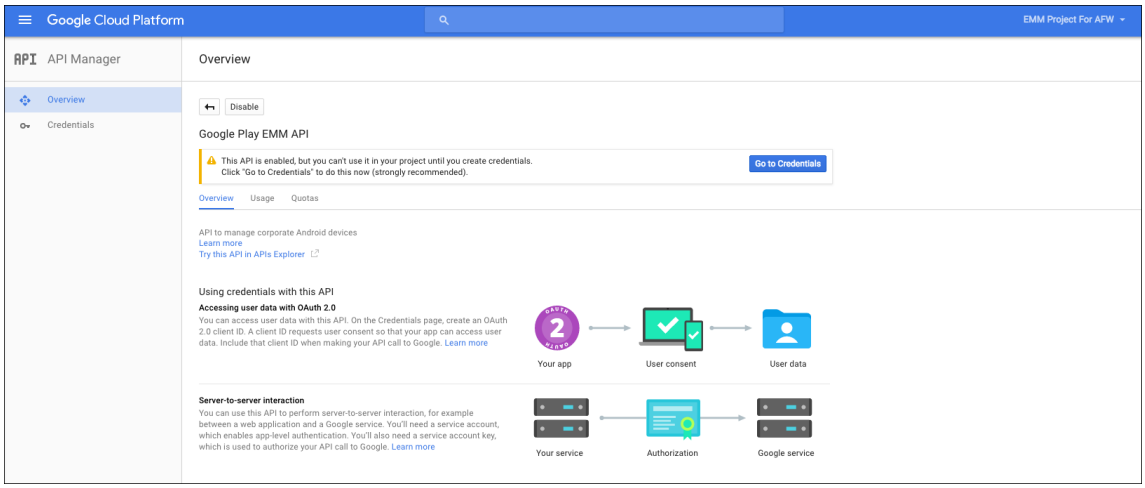
5. Cliquez sur **Bibliothèque** et dans **Rechercher**, entrez **EMM**, puis cliquez sur le résultat de la recherche.



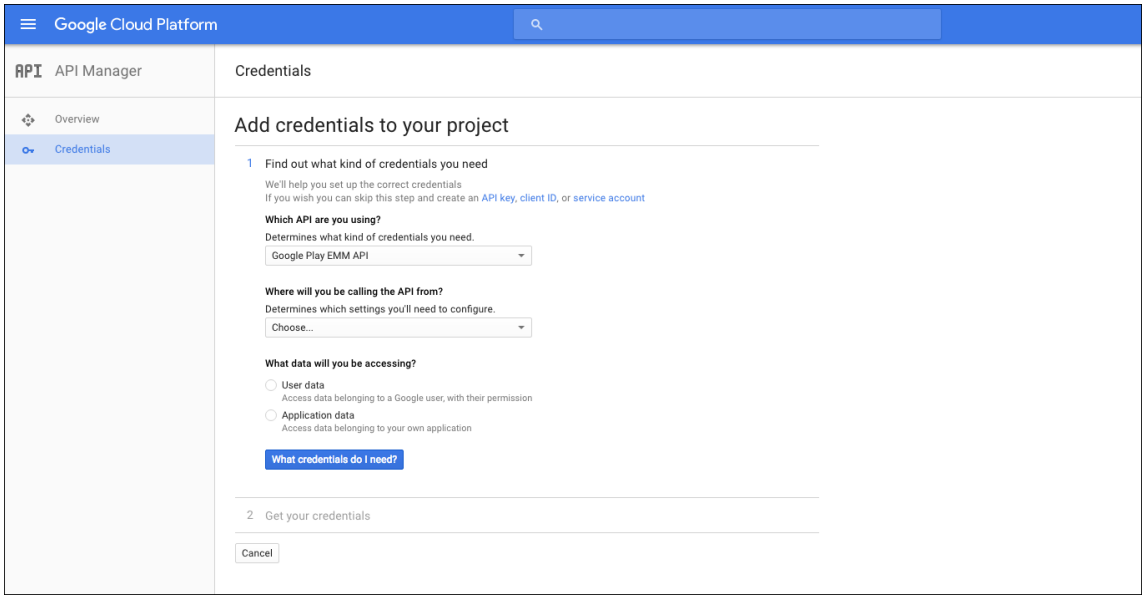
6. Sur la page de **présentation**, cliquez sur **Activer**.



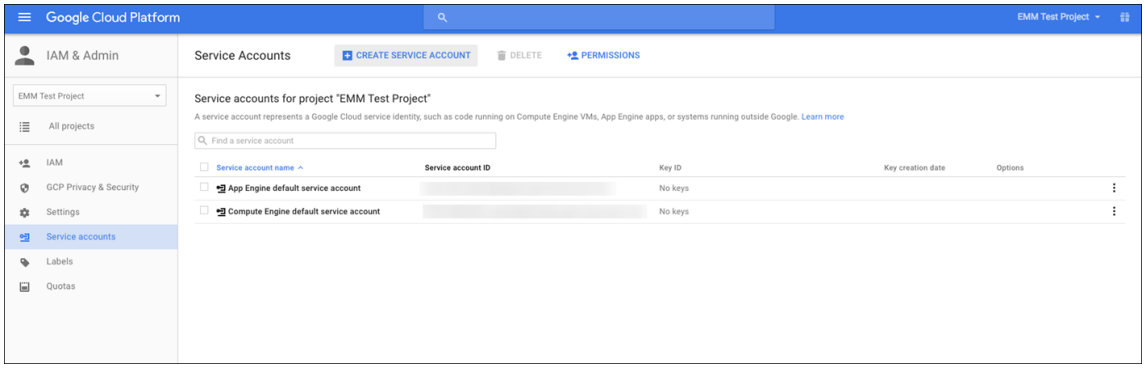
7. En regard de **Google Play EMM API**, cliquez sur **Accéder aux identifiants**.



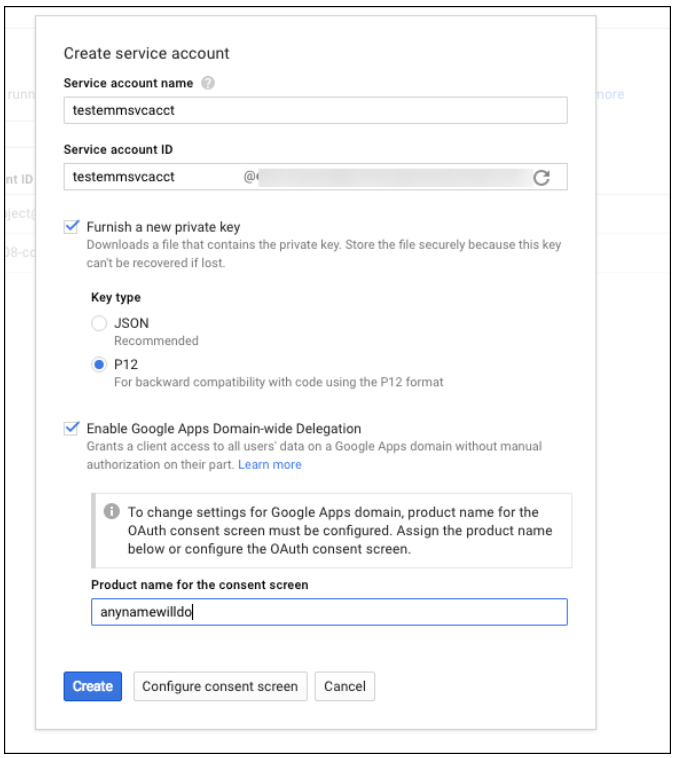
8. Dans la liste **Add credentials to our project**, dans l'étape 1, cliquez sur **service account**.



9. Sur la page **Comptes de service**, cliquez sur **Créer un compte de service**.

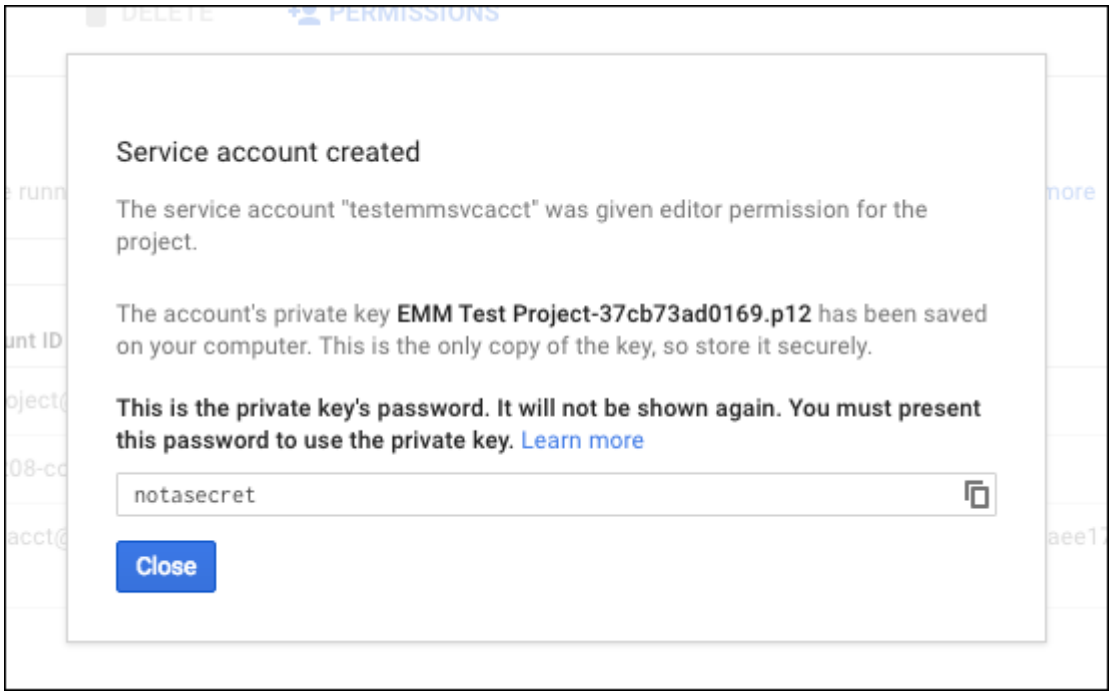


10. Dans **Créer un compte de service**, nommez le compte et sélectionnez la case **Indiquer une nouvelle clé privée**. Cliquez sur **P12**, sélectionnez la case à cocher **Activer la délégation Google Apps au niveau du domaine**, puis cliquez sur **Créer**.

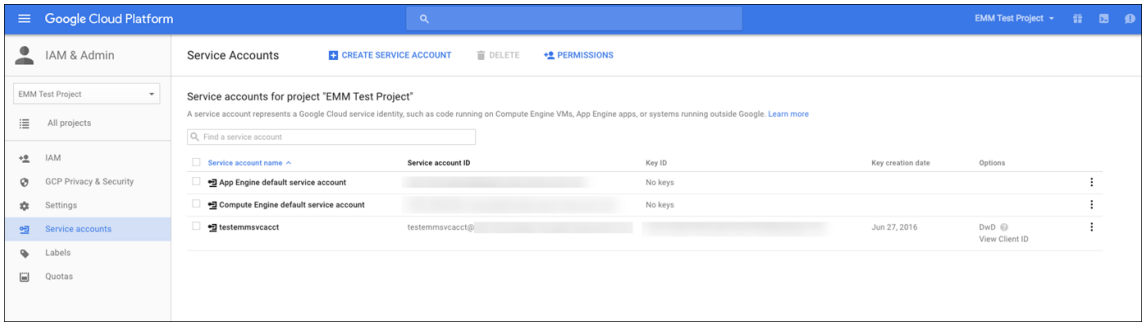


Le certificat (fichier P12) est téléchargé sur votre ordinateur. Veillez à enregistrer le certificat dans un emplacement sécurisé.

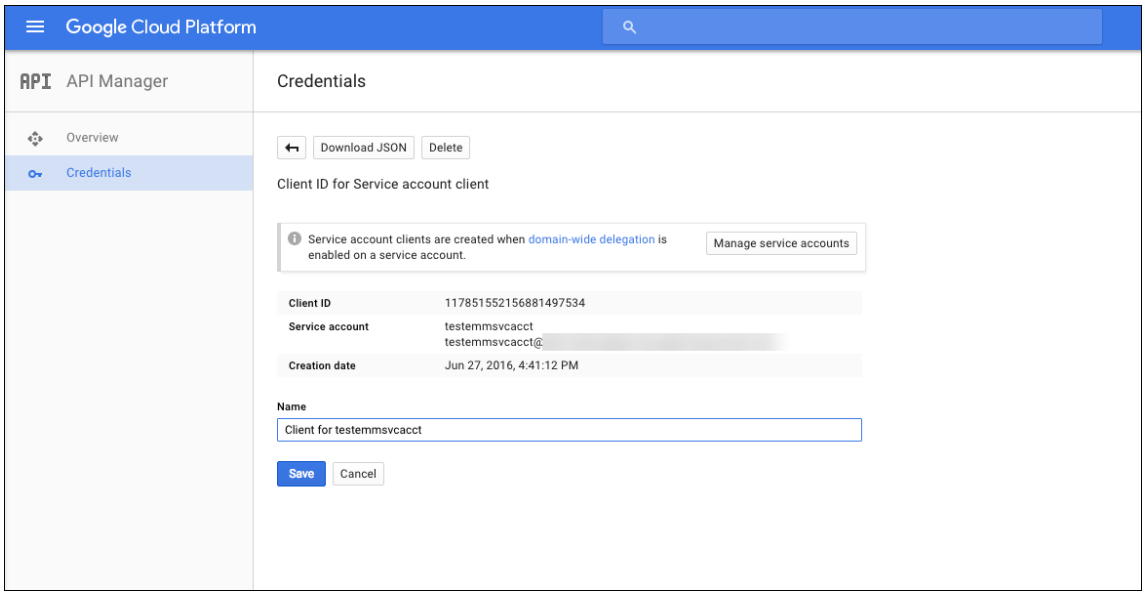
11. Sur l'écran **Compte de service créé**, cliquez sur **Fermer**.



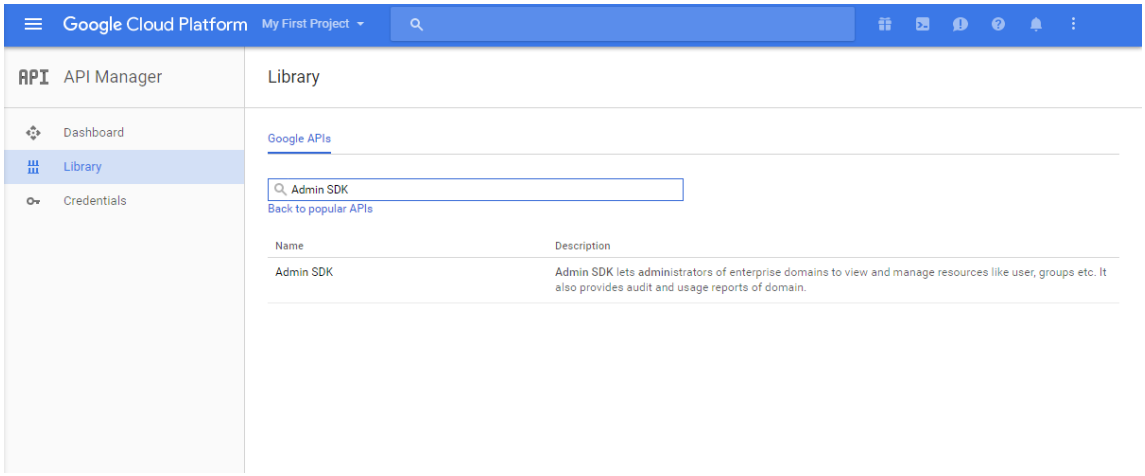
12. Dans **Autorisations**, cliquez sur **Comptes de service**, puis sous **Options** pour votre compte de service, cliquez sur **Afficher l'ID client**.



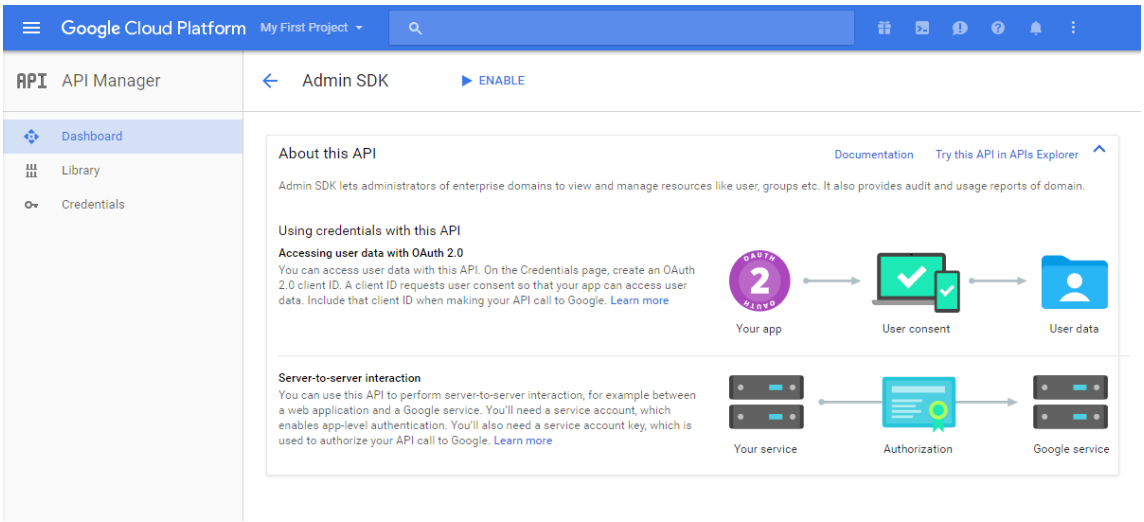
13. Les détails requis pour l'autorisation du compte sur la console d'administration Google s'affichent. Copiez les valeurs des champs **Client ID** et **Service account ID** sur un emplacement où vous pourrez récupérer les informations ultérieurement. Vous avez besoin de ces informations, ainsi que du nom de domaine pour les envoyer à l'assistance Citrix afin qu'ils puissent être autorisés.



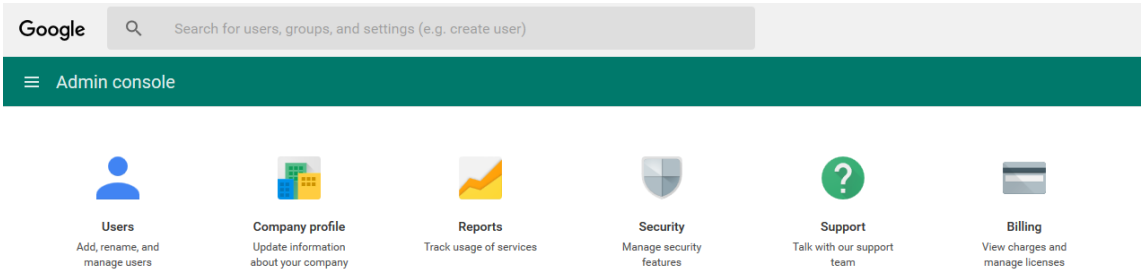
14. Sur la page **Bibliothèque**, recherchez **Admin SDK** et cliquez sur le résultat de la recherche.



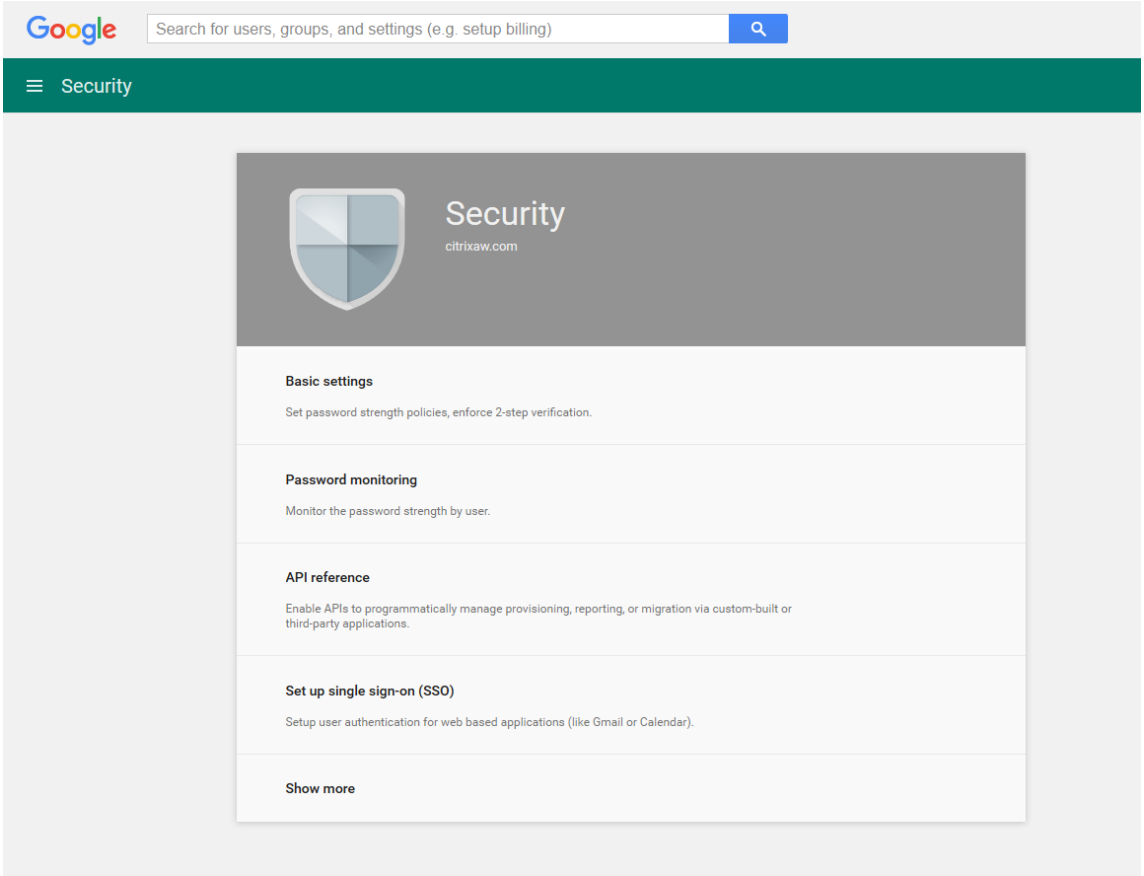
15. Sur la page de **présentation**, cliquez sur **Activer**.

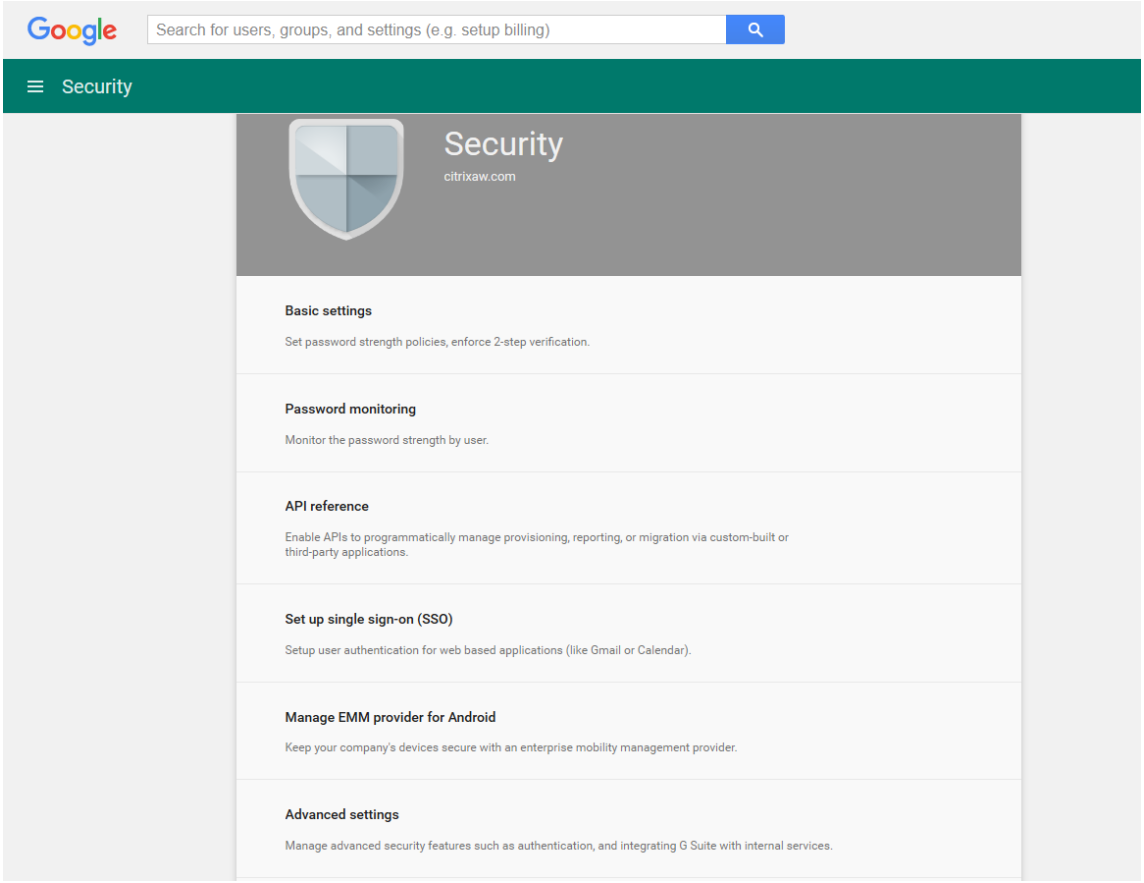


16. Ouvrez la console d'administration Google pour votre domaine et cliquez sur **Sécurité**.

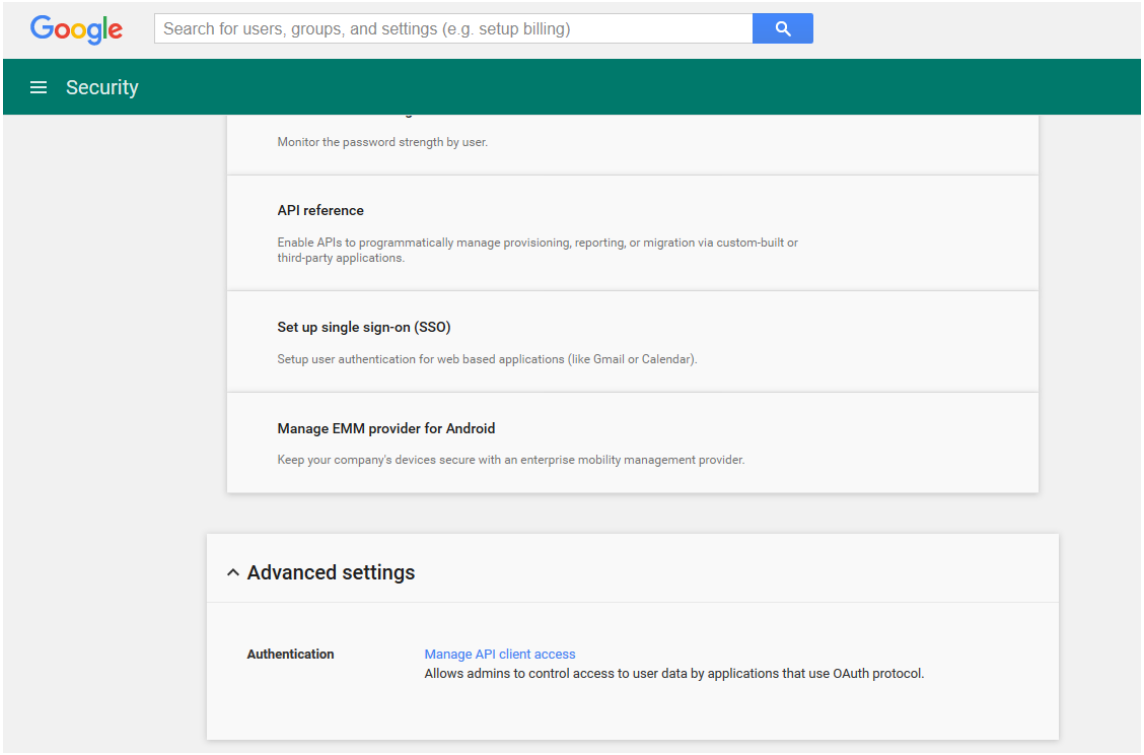


17. Sur la page **Paramètres**, cliquez sur **Afficher plus**, puis cliquez sur **Paramètres avancés**.

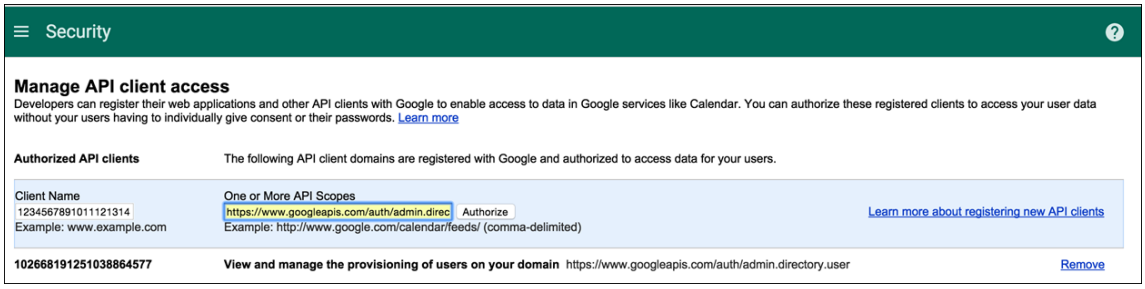




18. Cliquez sur **Gérer l'accès au client d'API**.



19. Dans **Nom du client**, entrez l'ID de client que vous avez enregistré précédemment, dans **Une ou plusieurs étendues d'API**, entrez `https://www.googleapis.com/auth/admin.directory.user` puis cliquez sur **Autoriser**.



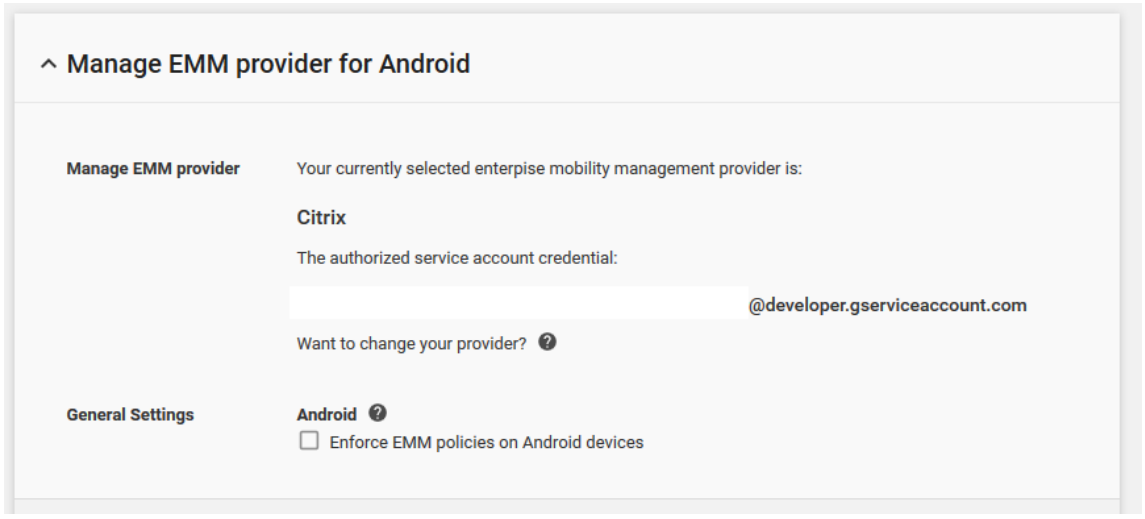
Liaison à EMM

Avant de pouvoir utiliser XenMobile pour gérer vos appareils Android, vous devez contacter l'assistance technique de Citrix et fournir votre nom de domaine, compte de service et jeton de liaison. Citrix lie le jeton à XenMobile en tant que fournisseur de gestion de la mobilité d'entreprise (EMM). Pour accéder aux coordonnées du support technique Citrix, consultez la section Support technique Citrix.

1. Pour confirmer la liaison, ouvrez une session sur le portail de la console d'administration Google et cliquez sur **Sécurité**.
2. Cliquez sur **Gérer le fournisseur EMM pour Android**.

   Votre compte Google Android Entreprise est maintenant lié à Citrix en tant que fournisseur EMM.

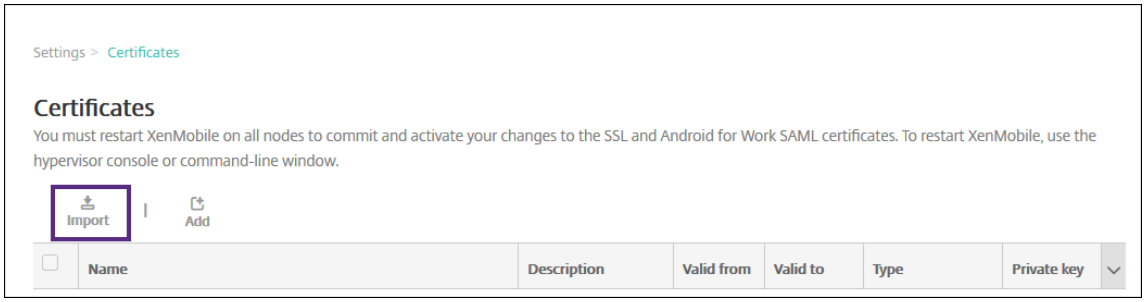
   Après avoir confirmé la liaison du jeton, vous pouvez commencer à utiliser la console XenMobile pour gérer vos appareils Android. Importez le certificat P12 que vous avez généré à l'étape 14. Configurez les paramètres du serveur Android Entreprise, activez l'authentification unique SAML et définissez au moins une stratégie d'appareil Android Entreprise.



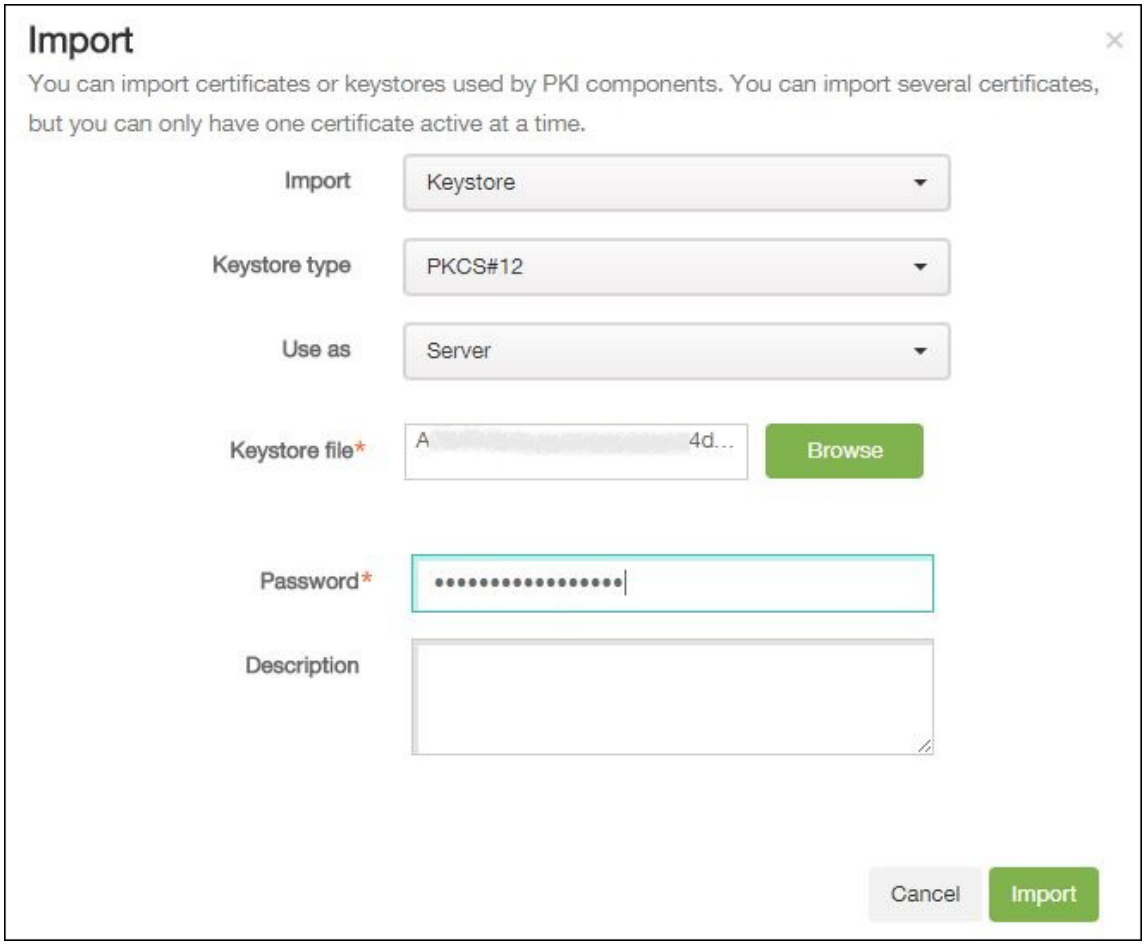
Importer le certificat P12

Suivez ces étapes pour importer votre certificat P12 Android Entreprise :

1. Connectez-vous à la console XenMobile.
2. Cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console pour ouvrir la page **Paramètres**, puis cliquez sur **Certificats**. La page **Certificats** s'affiche.



3. Cliquez sur **Importer**. La boîte de dialogue **Importer** apparaît.



Configurez les paramètres suivants :

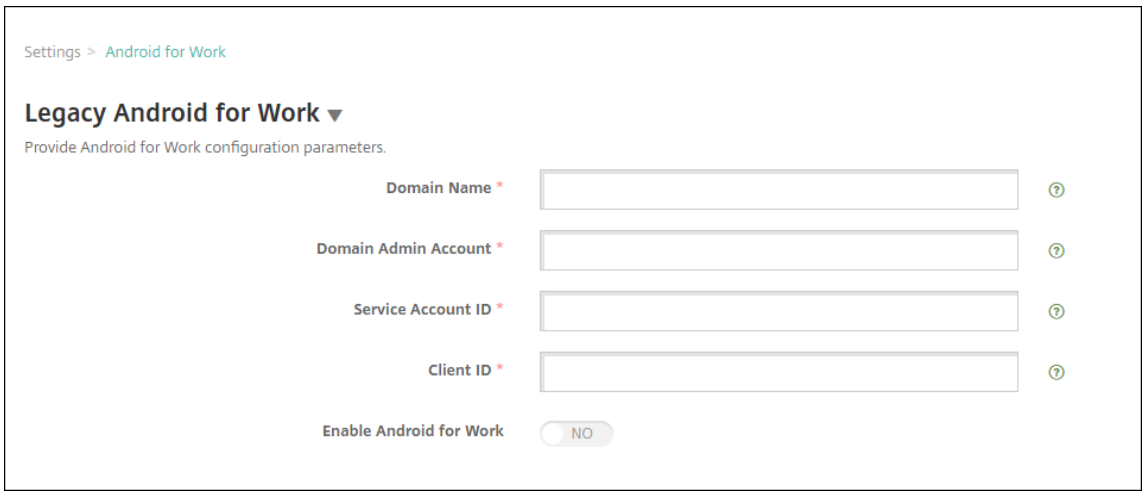
- **Importer :** dans la liste, cliquez sur **Keystore**.

- **Type de keystore :** dans la liste, cliquez sur **PKCS#12**.
- **Utiliser en tant que :** dans la liste, cliquez sur **Serveur**.
- **Fichier de keystore :** cliquez sur **Parcourir** et accédez au certificat P12.
- **Mot de passe :** entrez le mot de passe du keystore.
- **Description :** entrez une description pour le certificat.

4. Cliquez sur **Importer**.

Configurer les paramètres du serveur Android Entreprise

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Serveur**, cliquez sur **Android Entreprise**. La page **Android Entreprise** s'affiche.



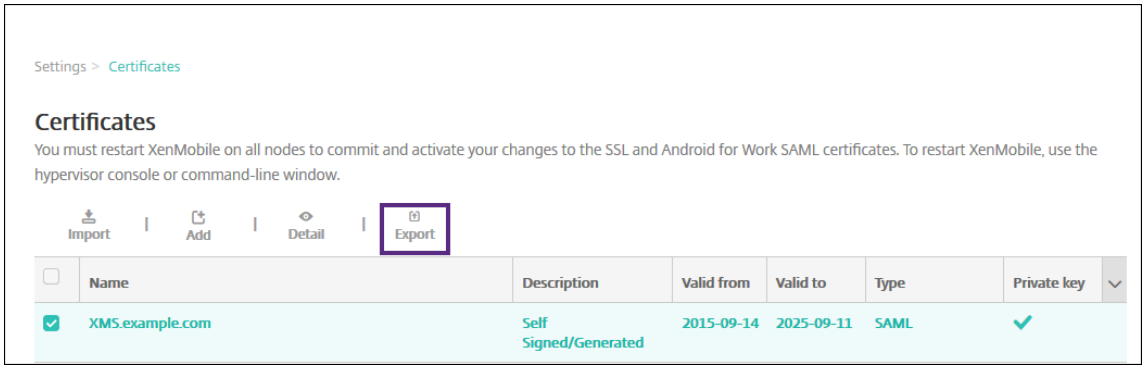
Configurez ces paramètres, puis cliquez sur **Enregistrer**.

- **Nom de domaine :** entrez votre nom de domaine Android Entreprise ; par exemple, domaine.com.
- **Compte d'administrateur de domaine :** entrez le nom d'utilisateur de l'administrateur de domaine ; par exemple, le compte de messagerie utilisé pour le portail Google Developer.
- **ID du compte de service :** entrez votre ID de compte de service, par exemple, l'adresse e-mail associée au compte de service Google (`serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com`).
- **ID client :** entrez l'ID client numérique de votre compte de service Google.
- **Activer Android Entreprise :** activez ou désactivez Android Entreprise.

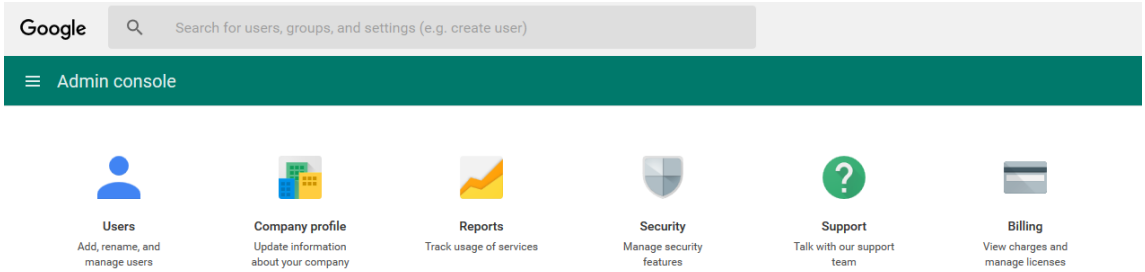
Activer l'authentification unique SAML

1. Connectez-vous à la console XenMobile.

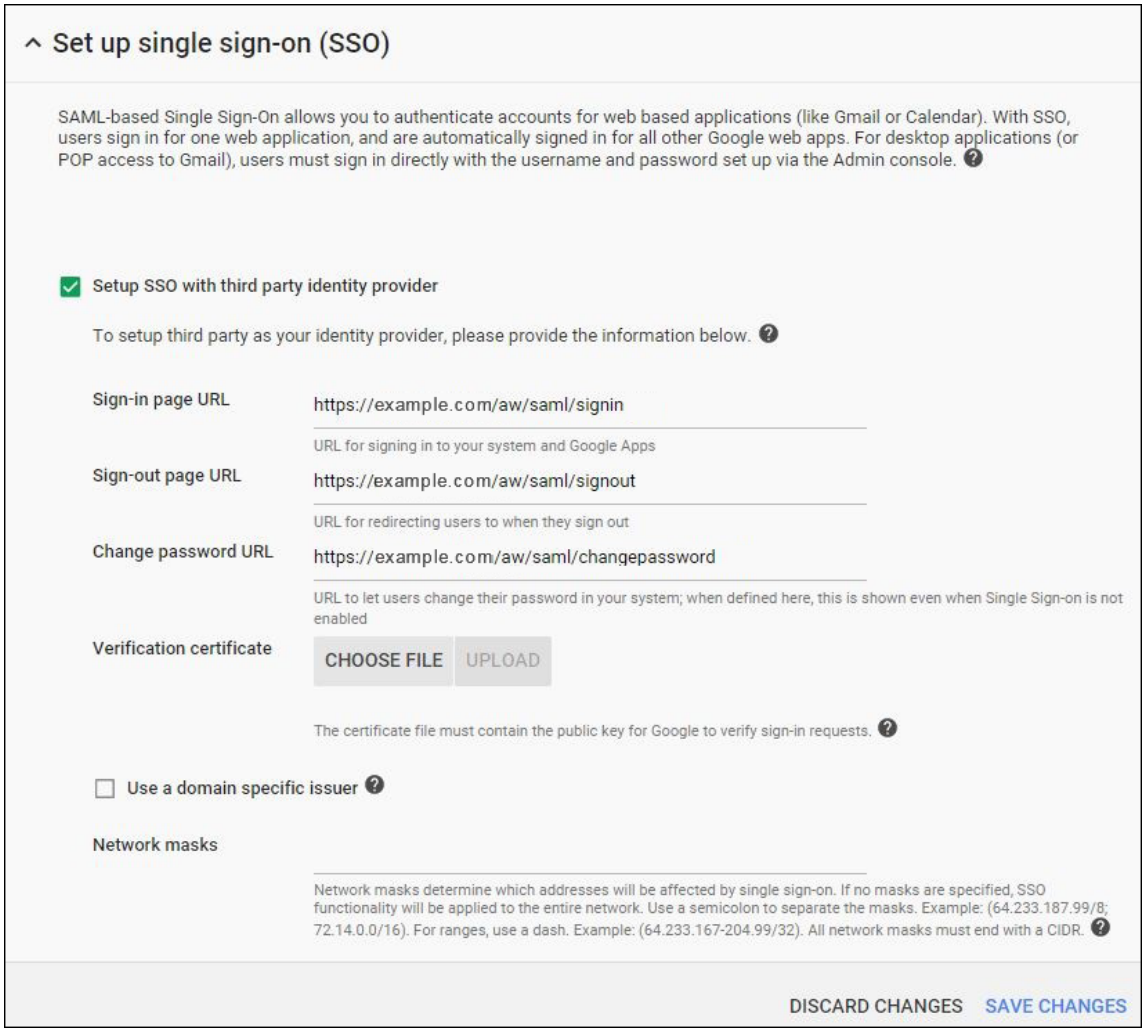
2. Cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console. La page **Paramètres** s'affiche.
3. Cliquez sur **Certificats**. La page **Certificats** s'affiche.



4. Dans la liste des certificats, cliquez sur le certificat SAML.
5. Cliquez sur **Exporter** et enregistrez le certificat sur votre ordinateur.
6. Connectez-vous au portail de la console d'administration Google à l'aide de vos informations d'identification d'administrateur Android Entreprise. Pour accéder au portail, veuillez consulter la section Console d'administration Google.
7. Cliquez sur **Sécurité**.



8. Dans **Sécurité**, cliquez sur **Configurer l'authentification unique (SSO)** et configurez les paramètres suivants :

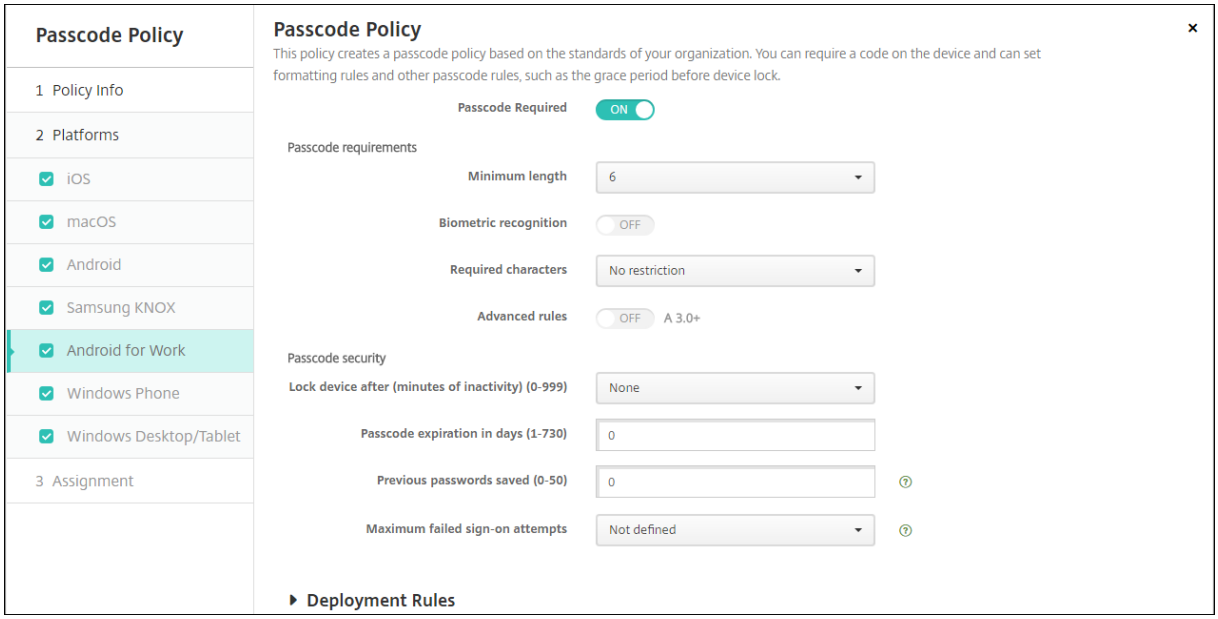


- **URL de la page de connexion :** entrez l'adresse URL pour les utilisateurs qui se connectent à votre système et Google Apps. Par exemple : `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **URL de la page de déconnexion :** entrez l'adresse URL vers laquelle les utilisateurs sont redirigés lorsqu'ils se déconnectent. Par exemple : `https://<Xenmobile-FQDN>/aw/saml/signout`.
- **URL de la page de modification du mot de passe :** entrez l'adresse URL pour permettre aux utilisateurs de modifier leur mot de passe dans votre système. Par exemple : `https://<Xenmobile-FQDN>/aw/saml/changepassword`. Si ce champ est défini, cette invite s'affiche même lorsque l'authentification unique (SSO) n'est pas disponible.
- **Certificat de vérification :** cliquez sur **CHOISIR FICHIER** et accédez à l'emplacement du certificat SAML exporté depuis XenMobile.

9. Cliquez sur **ENREGISTRER LES MODIFICATIONS**.

Configurer une stratégie d'appareil Android Entreprise

Configurez une stratégie de code secret afin d'obliger les utilisateurs à créer un code secret sur leurs appareils la première fois qu'ils s'inscrivent.



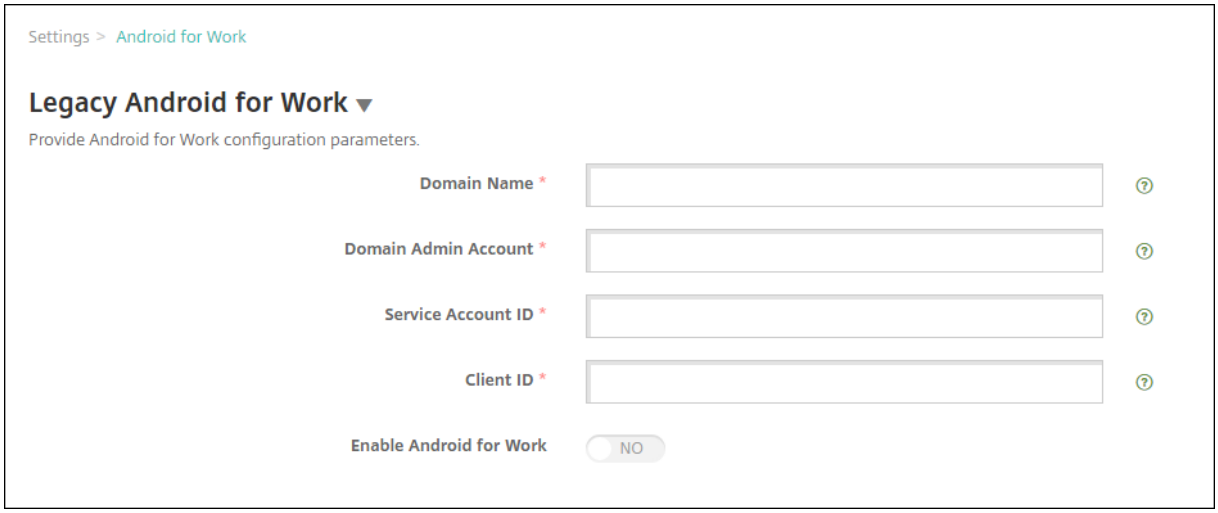
Les étapes de base pour configurer une stratégie sont les suivantes.

1. Connectez-vous à la console XenMobile.
2. Cliquez sur **Configurer** et sur **Stratégies d'appareil**.
3. Cliquez sur **Ajouter**, puis sélectionnez la stratégie que vous souhaitez ajouter à partir de la boîte de dialogue **Ajouter une nouvelle stratégie**. Dans cet exemple, vous cliquez sur **Code secret**.
4. Remplissez la page **Informations sur la stratégie**.
5. Cliquez sur **Android Entreprise** et configurez les paramètres pour la stratégie.
6. Attribuez la stratégie à un groupe de mise à disposition.

Configurer les paramètres de compte Android Entreprise

Avant de démarrer la gestion des applications et des stratégies Android sur les appareils, vous devez définir les informations de domaine et de compte Android Enterprise dans XenMobile. Commencez par effectuer les tâches de configuration Android Entreprise sur Google pour configurer un administrateur de domaine et obtenir un ID de compte de service et un jeton de liaison.

1. Dans la console Web de XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'ouvre.
2. Sous **Serveur**, cliquez sur **Android Entreprise**. La page de configuration **Android Entreprise** s'affiche.



1. Sur la page **Android Entreprise**, configurez les paramètres suivants :
   - **Nom de domaine :** entrez le nom du domaine.
   - **Compte d'administrateur de domaine :** entrez le nom d'utilisateur de l'administrateur de domaine.
   - **ID du compte de service :** entrez votre ID du compte de service Google.
   - **ID client :** entrez l'ID client de votre compte de service Google.
   - **Activer Android Entreprise :** activez ou désactivez Android Entreprise.
2. Cliquez sur **Enregistrer**.

Configurer l'accès partenaire Google Workspace pour XenMobile

Certaines fonctionnalités de gestion des points de terminaison pour Chrome utilisent des API partenaires de Google pour la communication entre XenMobile et votre domaine Google Workspace. Par exemple, XenMobile requiert les API pour les stratégies qui gèrent les fonctionnalités de Chrome, telles que le mode de navigation privée et le mode Invité.

Pour activer les API partenaires, vous devez configurer votre domaine Google Workspace dans la console XenMobile, puis configurer votre compte Google Workspace.

Configurer votre domaine Google Workspace (anciennement G Suite) dans XenMobile

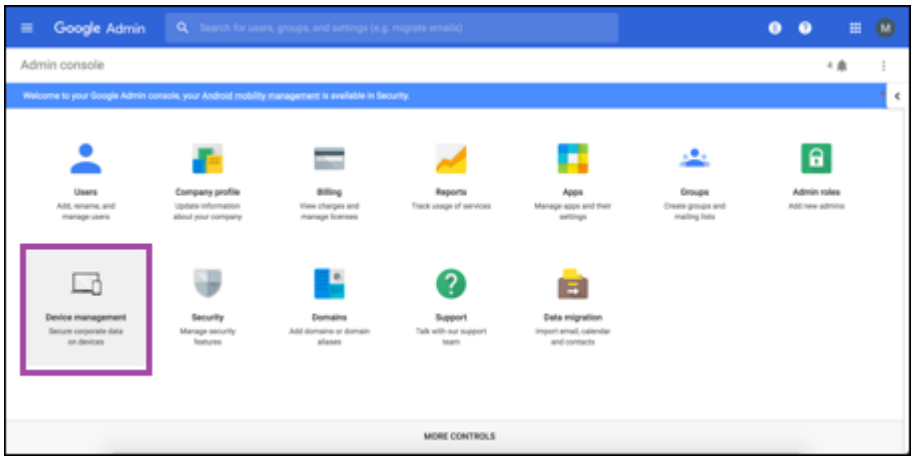
Pour permettre à XenMobile de communiquer avec les API de votre domaine Google Workspace, accédez à **Paramètres > Configuration de Google Chrome** et configurez les paramètres.

- **Domaine G Suite :** domaine Google Workspace hébergeant les API requises par XenMobile.
- **Compte d'administrateur G Suite :** compte administrateur de votre domaine G Suite.
- **ID client G Suite :** identifiant client pour Citrix. Utilisez cette valeur pour configurer l'accès partenaire pour le domaine Google Workspace.

- **Identifiant d'entreprise G Suite :** identifiant d'entreprise de votre compte, renseigné à partir de votre compte d'entreprise Google.

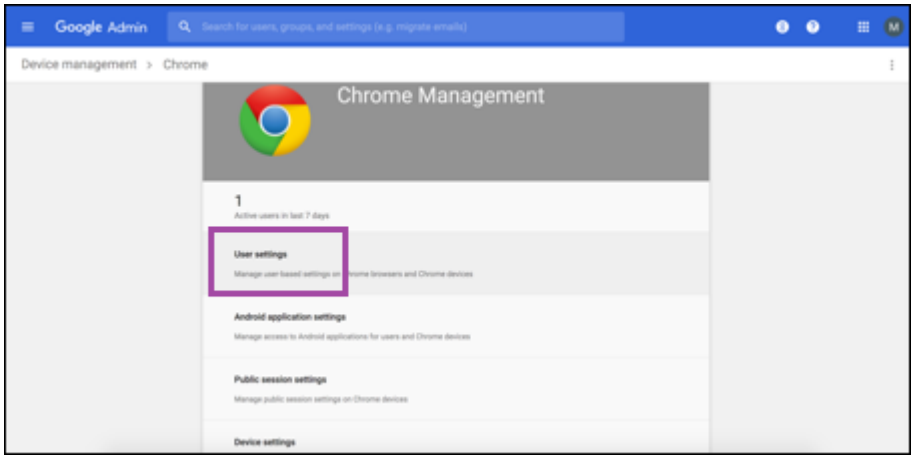
Activer l'accès partenaire pour les appareils et les utilisateurs de votre domaine Google Workspace

1. Connectez-vous à la console d'administration Google https://admin.google.com.
2. Cliquez sur **Gestion des appareils**.



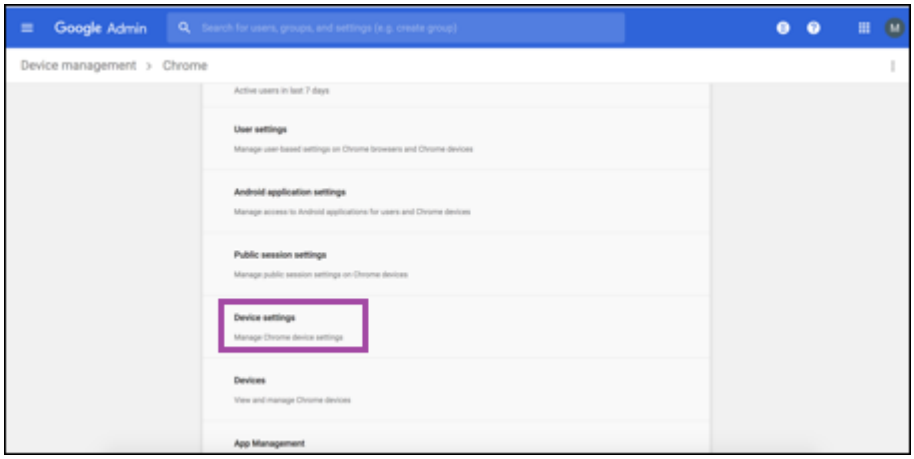
3. Cliquez sur **Gestion de Chrome**.

4. Cliquez sur **Paramètres utilisateur**.



5. Recherchez **Gestion de Chrome - Accès Partenaire**.

6. Activez la case à cocher **Activer la gestion de Chrome - Accès Partenaire**.
7. Confirmez que vous comprenez et que vous souhaitez activer l'accès partenaire. Cliquez sur **Enregistrer**.
8. Sur la page Gestion de Chrome, cliquez sur **Paramètres utilisateur**.



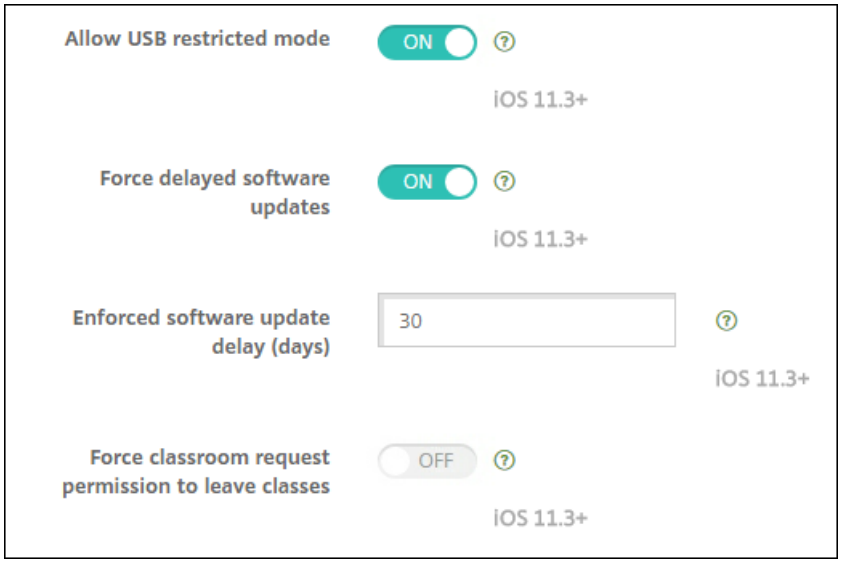
9. Recherchez **Gestion de Chrome - Accès Partenaire**.

10. Activez la case à cocher **Activer la gestion de Chrome - Accès Partenaire**.
11. Confirmez que vous comprenez et que vous souhaitez activer l'accès partenaire. Cliquez sur **Enregistrer**.
12. Accédez à la page **Sécurité**, puis cliquez sur **Paramètres avancés**.

13. Cliquez sur **Gérer l'accès au client d'API**.
14. Dans la console XenMobile, accédez à **Paramètres > Configuration de Google Chrome** et copiez la valeur de l'ID client Google Workspace. Retournez ensuite à la page **Gérer l'accès au client d'API** et collez la valeur copiée dans le champ **Nom du client**.
15. Dans **Un ou plusieurs champs d'application d'API**, ajoutez l'URL : `https://www.googleapis.com/auth/chromedevicemanagementapi`

16. Cliquez sur **Autoriser**.

    Le message « Vos paramètres ont été sauvegardés » apparaît.



Inscription d'appareils Android Entreprise

Si le processus d'inscription de votre appareil nécessite que les utilisateurs saisissent un nom d'utilisateur ou un ID utilisateur, le format accepté dépend de la configuration du serveur XenMobile pour la recherche des utilisateurs par nom principal d'utilisateur (UPN) ou nom de compte SAM.

Si le serveur XenMobile est configuré pour la recherche des utilisateurs par UPN, les utilisateurs doivent entrer un nom UPN au format :

- *nom d'utilisateur@domaine*

Si le serveur XenMobile est configuré pour la recherche des utilisateurs par SAM, les utilisateurs doivent entrer un nom SAM à l'un des formats suivants :

- *nom d'utilisateur@domaine*
- *domaine\nom d'utilisateur*

Pour déterminer le type de nom d'utilisateur pour lequel votre serveur XenMobile est configuré :

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **LDAP** pour afficher la configuration de la connexion LDAP.
3. Dans la partie inférieure de la page, affichez le champ **Recherche utilisateur par** :
    - Si l'option est définie sur **userPrincipalName**, le serveur XenMobile est défini pour UPN.
    - Si l'option est définie sur **sAMAccountName**, le serveur XenMobile est défini pour SAM.

Désinscription d'une entreprise Android Entreprise

Vous pouvez désinscrire une entreprise Android Enterprise à l'aide de la console XenMobile Server et des outils XenMobile Tools.

Lorsque vous effectuez cette tâche, XenMobile Server ouvre une fenêtre contextuelle XenMobile Tools. Avant de commencer, assurez-vous que XenMobile Server est autorisé à ouvrir des fenêtres contextuelles dans le navigateur que vous utilisez. Certains navigateurs, tels que Google Chrome, vous obligent à désactiver le blocage des fenêtres contextuelles et à ajouter l'adresse du site XenMobile à la liste d'autorisation des fenêtres contextuelles bloquées.

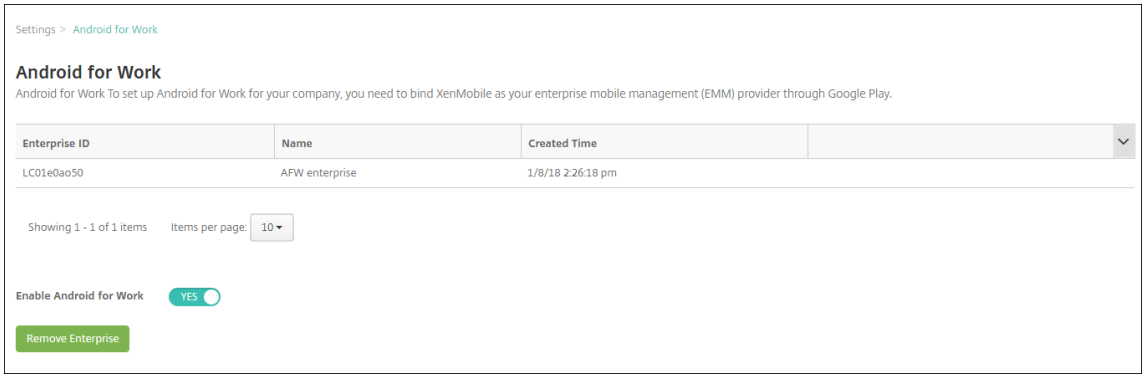
> **Avertissement :**
>
> une fois l'entreprise désinscrite, l'état par défaut des applications Android Entreprise sur les appareils déjà inscrits est rétabli. Les appareils ne sont plus gérés par Google. Leur réinscription dans une entreprise Android Entreprise peut nécessiter une configuration supplémentaire pour restaurer les fonctionnalités précédentes.

Une fois l'entreprise Android Enterprise désinscrite :

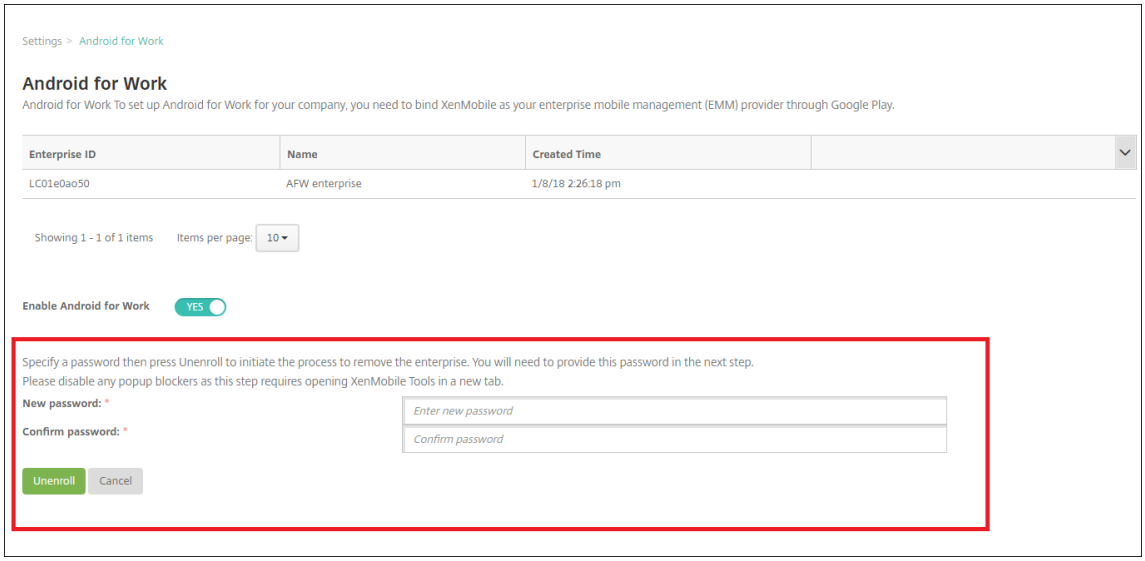
- Les applications Android Enterprise des appareils et des utilisateurs inscrits dans l'entreprise sont réinitialisées à leur état par défaut. Les autorisations d'applications Android Entreprise et les restrictions d'applications Android Entreprise appliquées précédemment n'ont plus d'effet.
- Les appareils inscrits via l'entreprise sont gérés par XenMobile mais ne sont pas gérés du point de vue de Google. Aucune nouvelle application Android Entreprise ne peut être ajoutée. Vous ne pouvez pas appliquer les autorisations d'applications Android Entreprise ou les stratégies de restrictions d'applications Android Entreprise. D'autres stratégies, telles que Planification, Mot de passe et Restrictions, peuvent encore être appliquées à ces appareils.
- Si vous tentez d'inscrire des appareils dans Android Enterprise, ils sont inscrits comme appareils Android et non comme appareils Android Enterprise.

Désinscription d'une entreprise Android Enterprise :

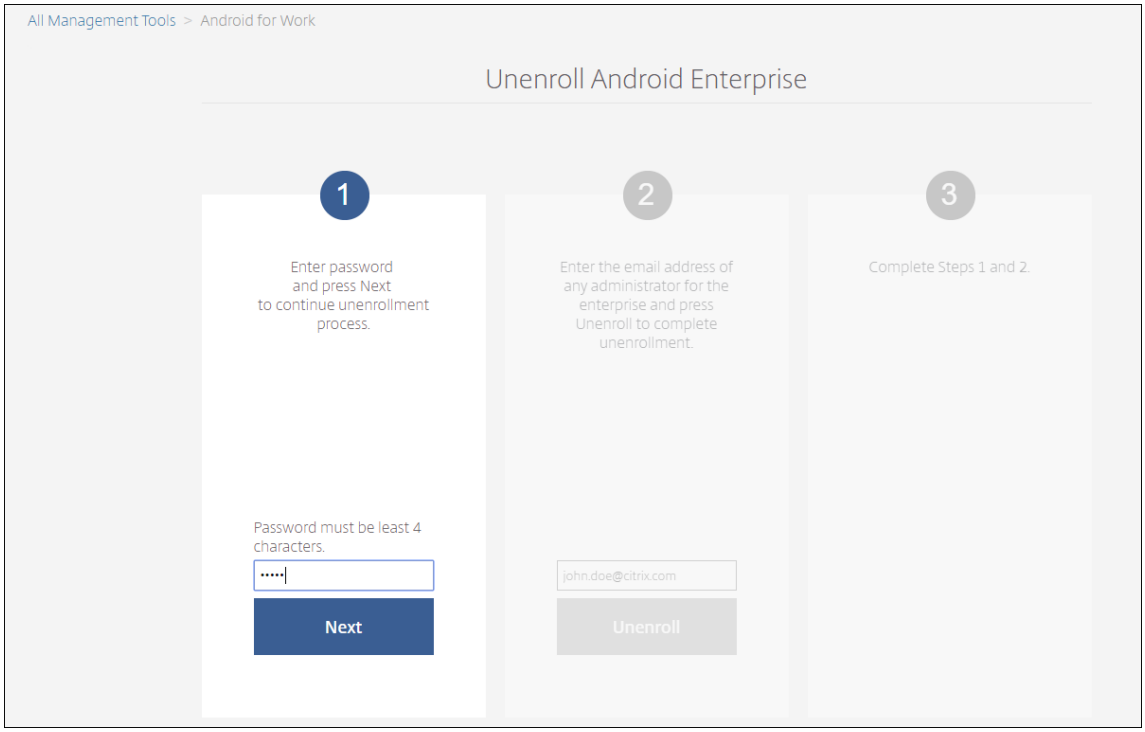
1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page Paramètres s'affiche.
2. Sur la page Paramètres, cliquez sur **Android Enterprise**.
3. Cliquez sur **Supprimer l'entreprise**.



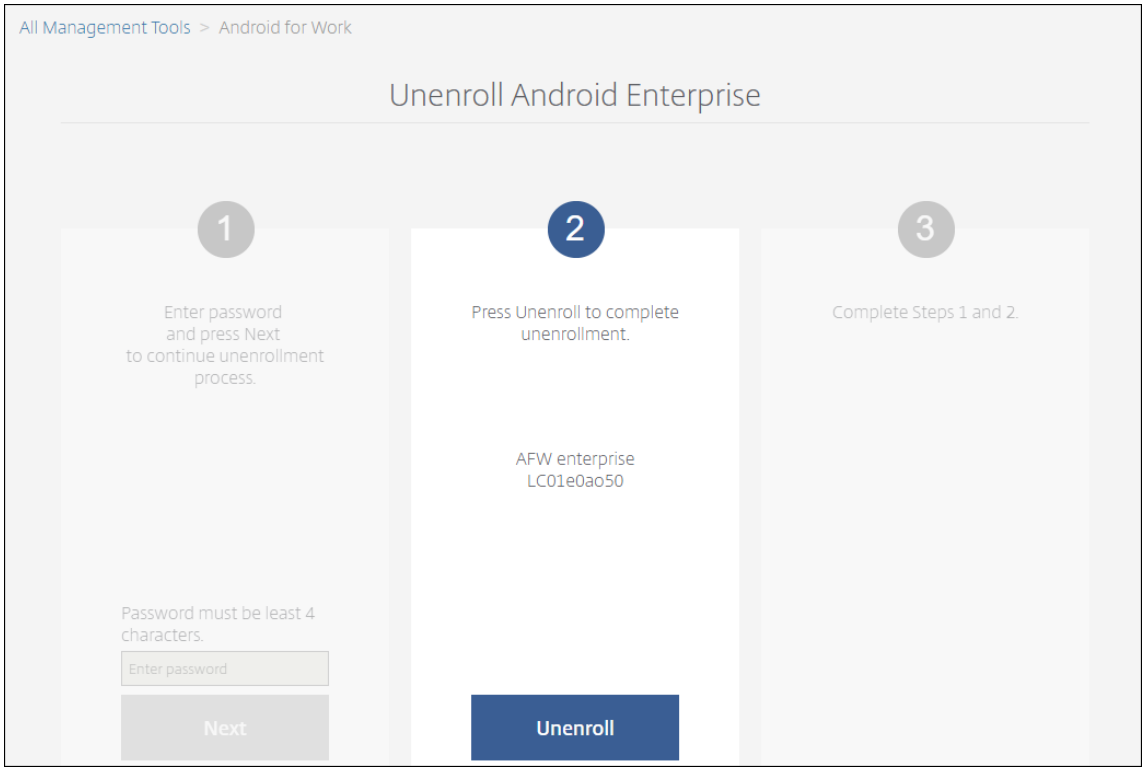
4. Spécifiez un mot de passe. Vous en aurez besoin à l'étape suivante pour terminer la désinscription. Cliquez ensuite sur **Désinscrire**.



5. Lorsque la page XenMobile Tools s'ouvre, entrez le mot de passe que vous avez créé à l'étape précédente.



6. Cliquez sur **Désinscrire**.



Provisionnement d'appareils entièrement gérés dans Android Enterprise

Seuls les appareils appartenant à l'entreprise peuvent être des appareils entièrement gérés pour Android Enterprise. Sur les appareils entièrement gérés, l'ensemble de l'appareil, et pas seulement le profil de travail, est contrôlé par l'entreprise ou l'organisation. Les appareils entièrement gérés sont également appelés appareils gérés de travail.

XenMobile prend en charge ces méthodes d'inscription pour les appareils entièrement gérés :

- **afw#xenmobile :** avec cette méthode d'inscription, l'utilisateur entre les caractères « afw#xenmobile » lors de la configuration de l'appareil. Ce jeton identifie l'appareil comme étant géré par XenMobile et télécharge Secure Hub.
- **Code QR :** le provisioning de code QR est un moyen simple de configurer une flotte distribuée d'appareils qui ne prennent pas en charge la technologie NFC, tels que les tablettes. La méthode d'inscription avec le code QR peut être utilisée sur des appareils de la flotte qui ont été réinitialisés à leurs paramètres d'usine. La méthode d'inscription avec le code QR permet de configurer les appareils entièrement gérés en scannant un code QR depuis l'assistant d'installation.
- **Partage de données à l'aide de NFC :** la méthode d'inscription avec le partage NFC peut être utilisée sur des appareils de la flotte qui ont été réinitialisés à leurs paramètres d'usine. Un partage NFC permet de transférer des données entre deux appareils en utilisant une communication en champ proche. Bluetooth, Wi-Fi et les autres modes de communication sont désactivés sur un appareil dont les paramètres d'usine ont été réinitialisés. NFC est le seul protocole de communication que l'appareil peut utiliser dans cet état.

afw#xenmobile

La méthode d'inscription est utilisée après la mise sous tension d'un nouvel appareil ou d'un appareil réinitialisé à ses paramètres d'usine lors de la configuration initiale. Les utilisateurs entrent « afw#xenmobile » lorsqu'ils sont invités à entrer un compte Google. Cette action télécharge et installe Secure Hub. Les utilisateurs suivent les invites de configuration de Secure Hub pour terminer l'inscription.

Cette méthode d'inscription est recommandée pour la plupart des clients car la dernière version de Secure Hub est téléchargée à partir de Google Play Store. Contrairement aux autres méthodes d'inscription, vous ne pouvez pas télécharger Secure Hub depuis XenMobile Server.

Pré-requis :

- Pris en charge sur tous les appareils Android exécutant Android 5.0 et supérieur.

Code QR

Pour inscrire un appareil en mode Propriétaire d'appareil à l'aide d'un code QR, générez un code QR en créant un JSON et en convertissant le JSON en un code QR. Le code QR est scanné par l'appareil

photo de l'appareil pour inscrire l'appareil.

Pré-requis :

- Pris en charge sur tous les appareils Android exécutant Android 7.0 et supérieur.

Créer un code QR à partir d'un JSON

Créez un JSON avec les champs suivants.

Ces champs sont obligatoires :

Clé : android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

Valeur : com.zenprise/com.zenprise.configuration.AdminFunction

Clé : android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

Valeur : qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Clé : android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

Valeur : `https://path/to/securehub.apk`

> **Remarque :**
>
> si Secure Hub est chargé sur le serveur Citrix XenMobile en tant qu'une application d'entreprise, il peut être téléchargé à partir de `https://<fqdn>:4443/*instanceName*/worxhome.apk`. Le chemin d'accès à Secure Hub APK doit être accessible via la connexion Wi-Fi à laquelle l'appareil se connecte lors du provisioning.

Ces champs sont facultatifs :

- **android.app.extra.PROVISIONING_LOCALE :** entrez un code de langue et de pays.

  Les codes de langue sont des codes ISO de deux lettres minuscules (tels que fr) comme défini dans l'ISO 639-1. Les codes de pays sont des codes ISO de deux lettres majuscules (tels que FR) comme défini dans l'ISO 3166-1. À titre d'exemple, entrez fr_FR pour la langue française parlée en France.

- **android.app.extra.PROVISIONING_TIME_ZONE :** fuseau horaire dans lequel l'appareil est exécuté.

  Entrez un nom basé sur la base de données Olson au format zone/emplacement. Par exemple, Europe/Paris pour l'heure de l'Europe occidentale. Si vous n'entrez rien, le fuseau horaire est automatiquement renseigné.

- **android.app.extra.PROVISIONING_LOCAL_TIME :** durée en millisecondes depuis l'heure Unix.

L'heure Unix (également appelée heure POSIX ou Unix timestamp) est le nombre de secondes écoulées depuis le 1er janvier 1970 (minuit UTC/GMT). L'heure n'inclut pas les secondes intercalaires (dans ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION :** définissez cette option sur **true** pour ignorer le cryptage lors de la création du profil. Définissez cette option sur **false** pour forcer le cryptage lors de la création du profil.

Un fichier JSON typique ressemble à ce qui suit :

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

Validez le fichier JSON créé à l'aide de n'importe quel outil de validation JSON, tel que https://jsonlint.com. Convertissez cette chaîne JSON en un code QR à l'aide de n'importe quel générateur de code QR, tel que https://goqr.me.

Ce code QR est scanné par un appareil dont les paramètres d'usine ont été réinitialisés pour inscrire l'appareil dans le mode Appareil géré de travail.

Pour inscrire l'appareil

Pour inscrire un appareil en tant qu'appareil entièrement géré, les paramètres d'usine de l'appareil doivent être réinitialisés.

1. Touchez l'écran 6 fois sur l'écran d'accueil pour lancer le flux d'inscription du code QR.
2. Lorsque vous y êtes invité, connectez-vous au Wi-Fi. L'emplacement de téléchargement de Secure Hub dans le code QR (codé dans le JSON) est accessible sur ce réseau Wi-Fi.

   Une fois que l'appareil se connecte au Wi-Fi, il télécharge un lecteur de code QR à partir de Google et lance l'appareil photo.
3. Pointez l'appareil photo sur le code QR pour scanner le code.

   Android télécharge Secure Hub à partir de l'emplacement de téléchargement dans le code QR, valide la signature du certificat de signature, installe Secure Hub et le définit comme propriétaire de l'appareil.

Pour plus d'informations, consultez ce guide Google destiné aux développeurs Android EMM : https://developers.google.com/android/work/prov-devices#qr_code_method.

Partage de données avec NFC

Pour inscrire un appareil en tant qu'appareil entièrement géré à l'aide du partage NFC, deux appareils sont requis : un dont les paramètres d'usine ont été rétablis et un exécutant l'application XenMobile Provisioning Tool.

Pré-requis :

- Pris en charge sur tous les appareils Android exécutant Android 5.0, Android 5.1, Android 6.0 et supérieur.
- Version 10.4 de XenMobile Server activée pour Android Enterprise.
- Un nouvel appareil ou un appareil dont les paramètres d'usine ont été rétablis, provisionné pour Android Enterprise en tant qu'appareil entièrement géré. Les étapes à suivre pour satisfaire ces conditions préalables sont disponibles plus loin dans cet article.
- Un autre appareil avec capacité NFC, exécutant l'application Provisioning Tool configurée. Provisioning Tool est disponible dans Secure Hub 10.4 où sur la page des téléchargements de Citrix.

Chaque appareil ne peut disposer que d'un profil Android Enterprise, géré par une application de gestion de la mobilité d'entreprise (EMM). Dans XenMobile, Secure Hub est l'application EMM. Un seul profil est autorisé sur chaque appareil. Si vous essayez d'ajouter une deuxième application EMM, la première application EMM sera supprimée.

Données transférées via le partage NFC

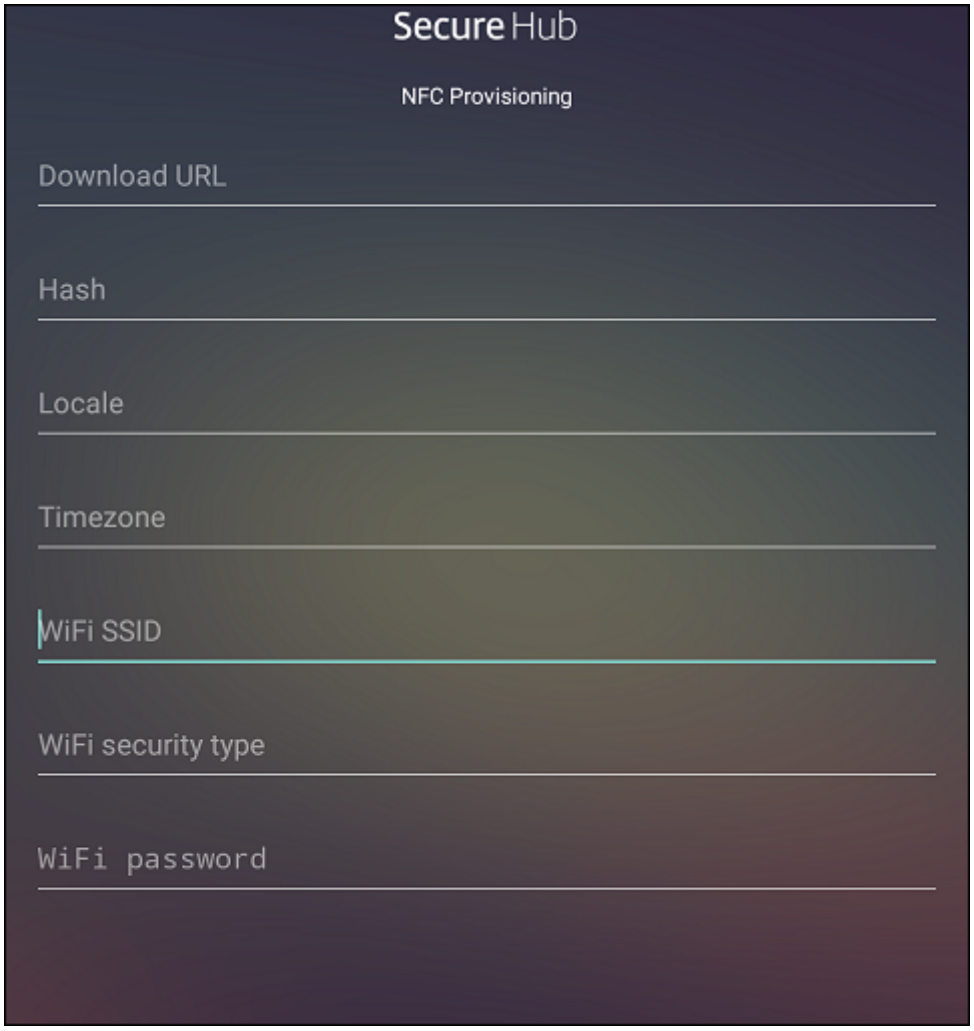
Le provisioning d'un appareil dont les paramètres d'usine ont été rétablis requiert l'envoi des données suivantes via NFC pour initialiser Android Enterprise :

- Nom du package de l'application EMM du fournisseur qui fait office de propriétaire de l'appareil (dans ce cas, Secure Hub).
- Emplacement intranet/Internet à partir duquel l'appareil peut télécharger l'application EMM du fournisseur.
- Hachage SHA1 de l'application EMM du fournisseur pour vérifier que le téléchargement a réussi.
- Détails de la connexion Wi-Fi de façon à ce qu'un appareil dont les paramètres d'usine ont été réinitialisés puisse se connecter et télécharger l'application EMM du fournisseur. Remarque : Android ne prend pas charge 802.1x Wi-Fi pour cette étape.
- Fuseau horaire de l'appareil (facultatif).
- Emplacement géographique de l'appareil (facultatif).

Lorsque les deux appareils sont « cognés », les données de Provisioning Tool sont envoyées à l'appareil dont les paramètres d'usine ont été réinitialisés. Ces données sont ensuite utilisées pour télécharger Secure Hub avec des paramètres d'administrateur. Si vous ne précisez pas le fuseau horaire ni l'emplacement, Android les configure automatiquement sur le nouvel appareil.

Configuration de XenMobile Provisioning Tool

Avant de partager des données avec NFC, vous devez configurer Provisioning Tool. Cette configuration est ensuite transférée à l'appareil dont les paramètres d'usine ont été réinitialisés durant le partage des données avec NFC.



Vous pouvez entrer des données dans les champs requis ou les renseigner via un fichier texte. Les étapes de la procédure suivante décrivent comment configurer le fichier texte et contiennent des descriptions pour chaque champ. L'application n'enregistre pas les informations après qu'elles soient entrées, il peut donc s'avérer utile de créer un fichier texte afin de conserver les informations pour une utilisation ultérieure.

Pour configurer le Provisioning Tool à l'aide d'un fichier texte

Nommez le fichier nfcprovisioning.txt et placez-le dans le dossier /sdcard/ sur la carte SD de l'appareil. Cela permet à l'application de lire le fichier texte et renseigner les valeurs.

Le fichier texte doit contenir les données suivantes :

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>

Il s'agit de l'emplacement intranet/Internet de l'application EMM du fournisseur. Après que l'appareil dont les paramètres d'usine ont été réinitialisés se soit connecté au Wi-Fi suite au partage NFC, il doit avoir accès à cet emplacement pour le téléchargement. L'adresse URL est une adresse URL standard qui ne requiert aucun formatage spécial.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>

Il s'agit de la somme de contrôle de l'application EMM du fournisseur. Elle est utilisée pour vérifier que le téléchargement a réussi. Les étapes à suivre pour obtenir la somme de contrôle sont abordées plus loin dans cet article.

android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>

Cette ligne est le SSID Wi-Fi connecté de l'appareil sur lequel Provisioning Tool est exécuté.

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>

Les valeurs prises en charge sont WEP et WPA2. Si le Wi-Fi n'est pas protégé, ce champ doit être vide.

android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>

Si le Wi-Fi n'est pas protégé, ce champ doit être vide.

android.app.extra.PROVISIONING_LOCALE=<locale>

Entrez un code de langue et de pays. Les codes de langue sont des codes ISO de deux lettres minuscules (tels que fr) comme défini dans l'ISO 639-1. Les codes de pays sont des codes ISO de deux lettres majuscules (tels que FR) comme défini dans l'ISO 3166-1. À titre d'exemple, entrez fr_FR pour la langue française parlée en France. Si vous n'entrez aucun code, la langue et le pays sont automatiquement renseignés.

android.app.extra.PROVISIONING_TIME_ZONE=<timezone>

Fuseau horaire dans lequel l'appareil est exécuté. Entrez un nom basé sur la base de données Olson au format zone/emplacement. Par exemple, Europe/Paris pour l'heure de l'Europe occidentale. Si vous n'entrez rien, le fuseau horaire est automatiquement renseigné.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<**package** name>

Ces données ne pas requises car la valeur est codée en dur dans l'application Secure Hub. Il n'est mentionné ici que par souci de complétude.

Si un accès protégé Wi-Fi WPA2 est utilisé, un fichier nfcprovisioning.txt peut ressembler à ce qui suit :

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb\u003d


```
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Si un accès non protégé Wi-Fi est utilisé, un fichier nfcprovisioning.txt peut ressembler à ce qui suit :

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Pour obtenir la somme de contrôle de Secure Hub

Pour obtenir la somme de contrôle d'une application, ajoutez l'application en tant qu'application d'entreprise.

1. Dans la console XenMobile, accédez à **Configurer > Applications** et sur **Ajouter**.

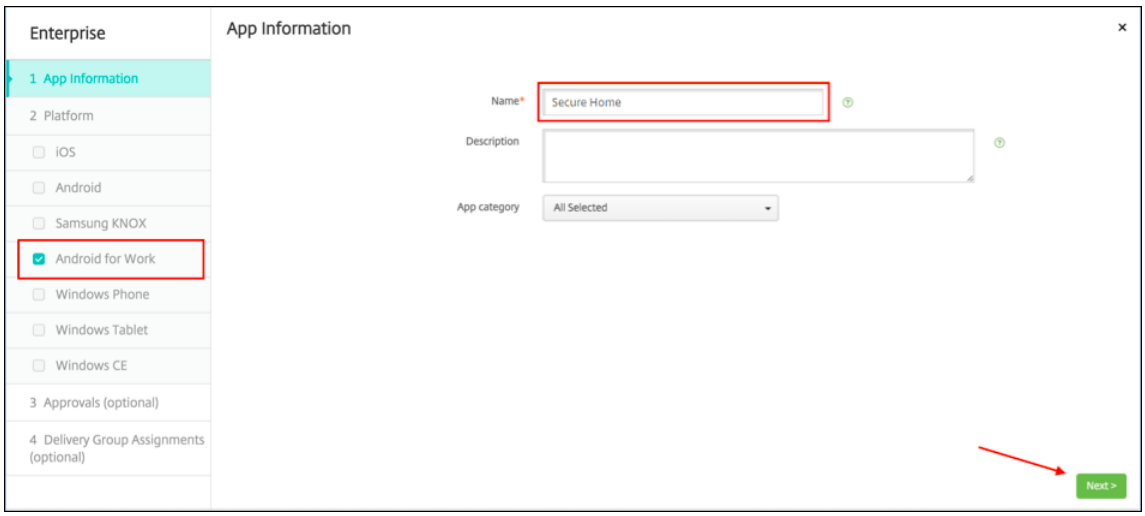
   La fenêtre **Ajouter une application** s'affiche.

2. Cliquez sur **Entreprise**.

   La page **Informations sur l'application** s'affiche.

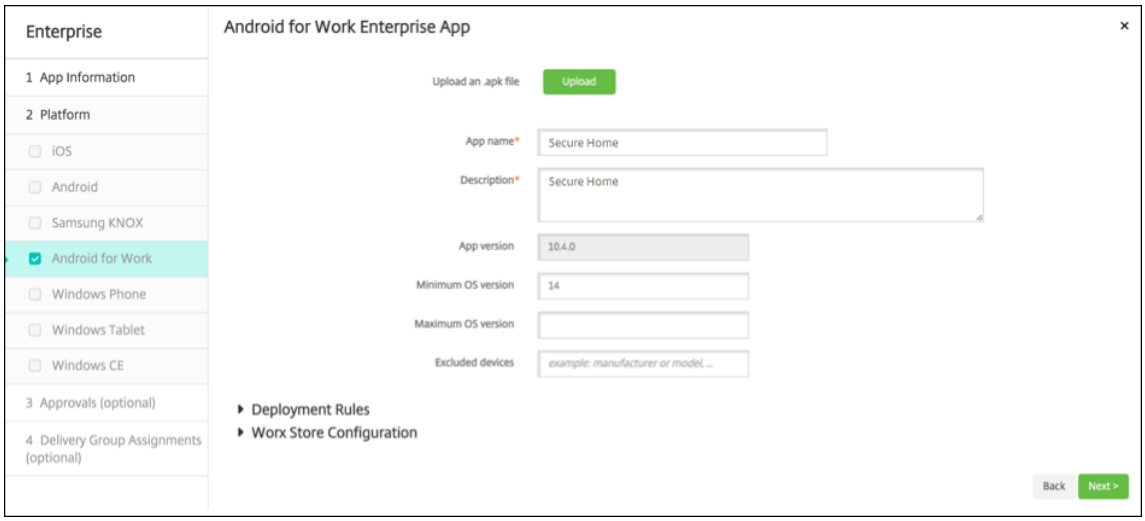
3. Sélectionnez la configuration suivante et cliquez sur **Suivant**.

   La page **Android Enterprise Enterprise App** s'affiche.



4. Fournissez le chemin d'accès au fichier .apk et cliquez sur **Suivant** pour charger le fichier.

   Une fois le chargement terminé, vous verrez les détails du package chargé.



5. Cliquez sur **Suivant** pour ouvrir une page permettant de télécharger le fichier JSON, que vous pouvez ensuite utiliser pour le chargement sur Google Play. Pour Secure Hub, le chargement sur Google Play n'est pas requis, mais vous avez besoin du fichier JSON pour lire la valeur SHA1.

   Un fichier JSON typique ressemble à ce qui suit :

6. Copiez la valeur de **file_sha1_base64** et utilisez-la dans le champ **Hash** de Provisioning Tool.

   > **Remarque :**
   >
   > L'URL du hachage doit être sécurisée.

   - Convertissez tous les symboles **+** en **-**
   - Convertissez tous les symboles **/** en **_**
   - Remplacez **\u003d** à la fin de la valeur par **=**

Si vous stockez le hachage dans le fichier nfcprovisioning.txt de la carte SD de l'appareil, l'application procède à la conversion de sécurité. Toutefois, si vous décidez d'entrer le hachage manuellement, il est de votre responsabilité de vous assurer que l'URL est sécurisée.

Bibliothèques utilisées

Provisioning Tool utilise les bibliothèques suivantes dans son code source :

- Bibliothèque v7 appcompat, bibliothèque Design Support et bibliothèque v7 Palette par Google sous licence Apache 2.0

  Pour plus d'informations, consultez le Guide des fonctionnalités de la bibliothèque de support.

- Butter Knife par Jake Wharton sous licence Apache 2.0

Provisionner des appareils avec profil de travail dans Android Entreprise

Sur les appareils avec profil de travail dans Android Enterprise, vous séparez en toute sécurité les espaces professionnels et personnels de l'appareil. Par exemple, les appareils BYOD peuvent être des appareils avec profil de travail. L'expérience d'inscription des appareils en mode Profil de travail est similaire à l'inscription Android dans XenMobile. Les utilisateurs téléchargent Secure Hub depuis Google Play et inscrivent leurs appareils.

Par défaut, les paramètres Débogage USB et Sources inconnues sont désactivés sur un appareil lorsqu'il est inscrit en mode Profil de travail dans Android Enterprise.

> **Conseil :**
>
> Lors de l'inscription d'appareils dans Android Enterprise en tant qu'appareils avec profil de travail, accédez toujours à Google Play. De là, activez l'affichage de Secure Hub dans le profil personnel de l'utilisateur.

iOS

January 10, 2022

Pour gérer des appareils iOS dans XenMobile Server, vous devez configurer un certificat Apple Push Notification Service (APNS). Pour de plus amples informations, consultez la section Certificats APNs.

Les profils d'inscription déterminent si les appareils iOS s'inscrivent en mode MDM+MAM, avec la possibilité pour les utilisateurs de se désinscrire de MDM. XenMobile Server prend en charge les types d'authentification suivants pour les appareils iOS en mode MDM+MAM. Pour de plus amples informations, consultez la section Certificats et authentification.

- Domaine
- Domaine et jeton de sécurité
- Certificat client
- Certificat client et domaine

> **Exigences pour les certificats de confiance dans iOS 13 :**
>
> Apple a introduit de nouvelles exigences pour les certificats de serveur TLS. Vérifiez que tous les certificats respectent les nouvelles exigences d'Apple. Consultez la publication Apple, https://support.apple.com/en-us/HT210176. Pour obtenir de l'aide sur la gestion des certificats, consultez la section Chargement de certificats dans XenMobile Server.

Pour les systèmes d'exploitation pris en charge, consultez la section Systèmes d'exploitation d'appareils pris en charge.

Compatibilité iOS 14

XenMobile Server et les applications mobiles Citrix sont compatibles avec iOS 14, mais ne prennent pas actuellement en charge les nouvelles fonctionnalités iOS 14.

Pour les appareils iOS supervisés, vous pouvez retarder les mises à niveau logicielles jusqu'à 90 jours. Dans la stratégie Restrictions pour iOS, utilisez les paramètres suivants :

- **Retarder les mises à jour logicielles**
- **Délai imposé pour les mises à jour logicielles**

Consultez la section Paramètres iOS. Ces paramètres ne sont pas disponibles pour les appareils en mode d'inscription utilisateur ou non supervisé (MDM complet).

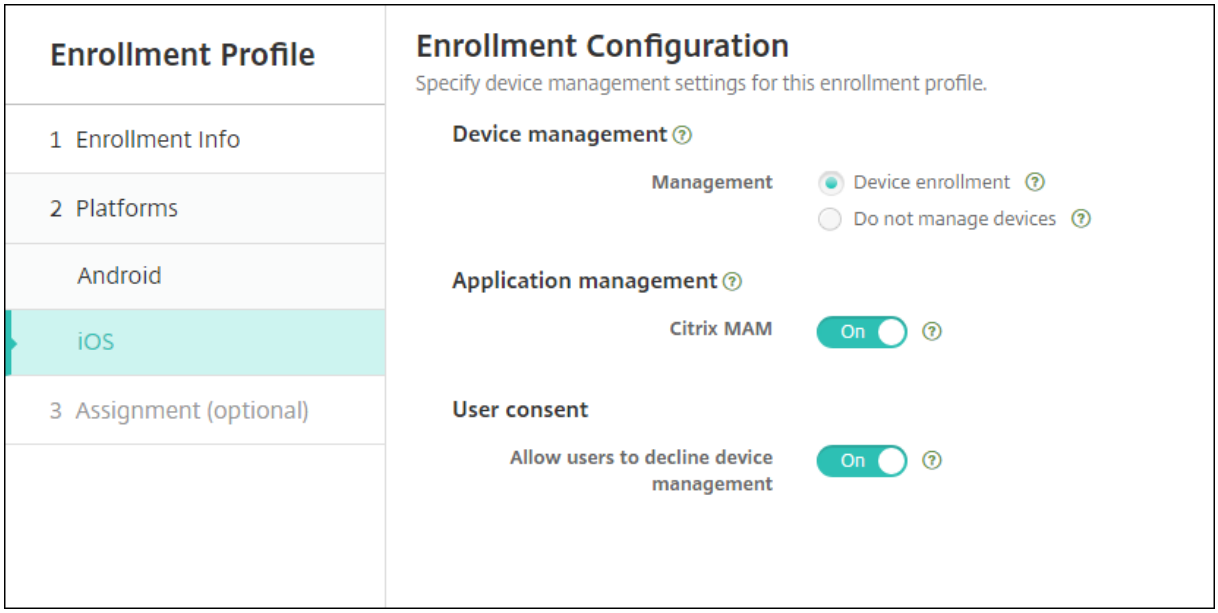
Noms d'hôtes Apple qui doivent rester ouverts

Certains noms d'hôtes Apple doivent rester ouverts pour assurer le bon fonctionnement d'iOS, de macOS et de l'Apple App Store. Le blocage de ces noms d'hôtes peut affecter l'installation, la mise à jour et le bon fonctionnement d'iOS, des applications iOS et de MDM et l'inscription des appareils et des applications. Pour plus d'informations, consultez https://support.apple.com/en-us/HT201999.

Méthodes d'inscription prises en charge

Vous spécifiez comment gérer les appareils iOS dans les profils d'inscription. Vous pouvez choisir l'inscription d'appareils ou pas d'inscription MDM.

Pour configurer les paramètres d'inscription pour les appareils iOS, accédez à **Configurer > Profils d'inscription > iOS**.



Le tableau suivant indique les méthodes d'inscription prises en charge par XenMobile Server pour les appareils iOS :

Méthode	Prise en charge
Programme de déploiement d'Apple	Oui
Apple School Manager	Oui
Apple Configurator	Oui
Inscription manuelle	Oui
Invitations d'inscription	Oui

Apple propose des programmes d'inscription d'appareil pour les comptes d'entreprise et éducation. Pour les comptes d'entreprise, vous devez vous inscrire au Programme de déploiement d'Apple pour utiliser le programme Apple Device Enrollment Program (DEP) afin de gérer et inscrire des appareils dans XenMobile Server. Ce programme est pour les appareils iOS et macOS. Voir Déployer des appareils via le programme de déploiement d'Apple.

Pour les comptes éducation, vous devez créer un compte Apple School Manager. Apple School Manager unifie le programme de déploiement et l'achat en volume. Apple School Manager est un type de programme de déploiement Apple Éducation. Consultez la section Intégration avec les fonctionnalités Apple Éducation.

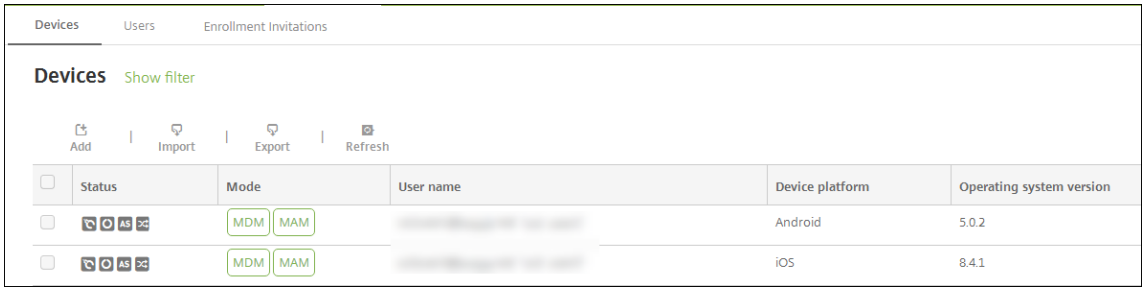
Vous pouvez utiliser le programme de déploiement d'Apple pour inscrire en bloc des appareils iOS et macOS. Vous pouvez acheter ces appareils directement auprès d'Apple, d'un revendeur agréé Apple ou d'un opérateur. Vous pouvez aussi utiliser Apple Configurator pour inscrire des appareils iOS

qu'ils aient été achetés ou non directement auprès d'Apple. Consultez la section Inscription en bloc d'appareils Apple.

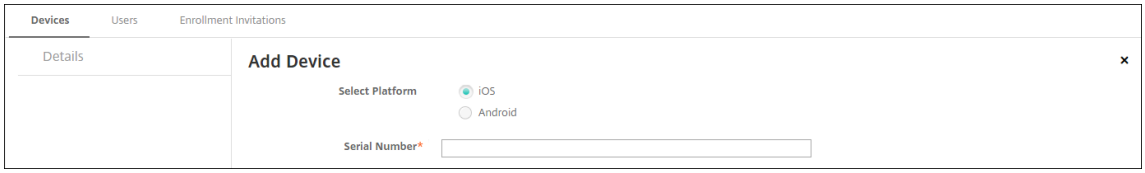
Ajouter un appareil iOS manuellement

Si vous souhaitez ajouter manuellement un appareil iOS, par exemple à des fins de test, procédez comme suit.

1. Dans la console XenMobile Server, cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.



2. Cliquez sur **Ajouter**. La page **Ajouter un appareil** s'affiche.

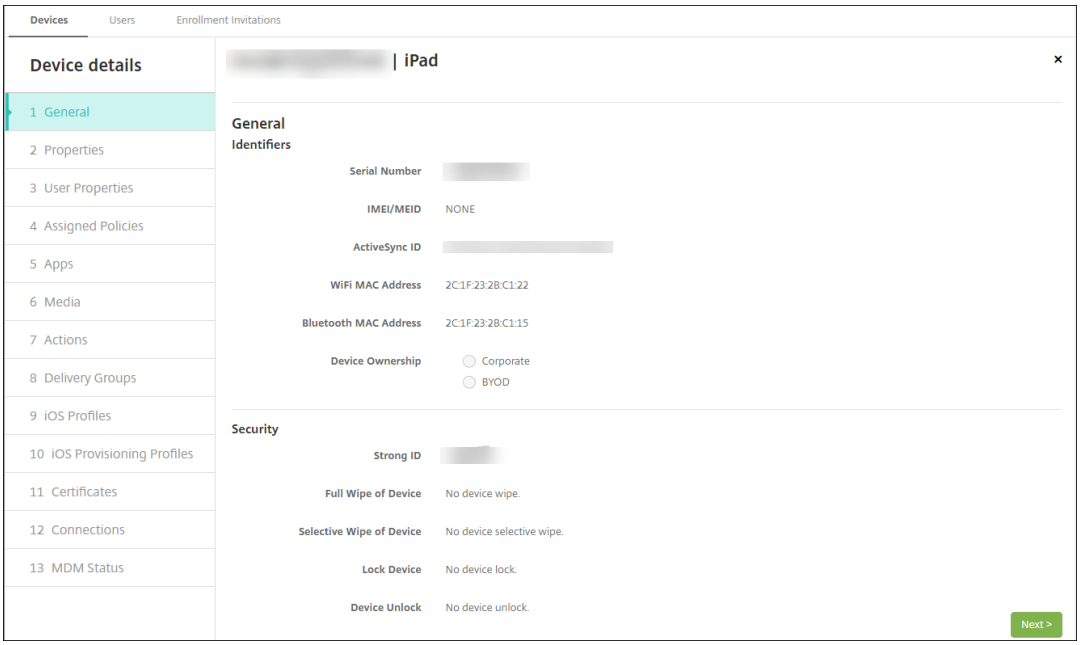


3. Pour configurer ces paramètres :
   - **Sélectionner une plate-forme :** cliquez sur **iOS**.
   - **Numéro de série :** entrez le numéro de série de l'appareil.
4. Cliquez sur **Ajouter**. Le tableau **Appareils** s'affiche avec l'appareil ajouté en bas de la liste. Pour afficher et confirmer les détails de l'appareil, sélectionnez l'appareil que vous avez ajouté, puis dans le menu qui s'affiche, cliquez sur **Modifier**.

> **Remarque :**
>
> Lorsque vous sélectionnez la case à cocher en regard d'un appareil, le menu d'options s'affiche au-dessus de la liste des appareils. Lorsque vous cliquez dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

   - LDAP configuré
   - Si vous utilisez des groupes locaux et utilisateurs locaux :
     - Un ou plusieurs groupes locaux.
     - Utilisateurs locaux attribués à des groupes locaux.
     - Des groupes de mise à disposition sont associés à des groupes locaux.

- Utilisation d'Active Directory :
  - Des groupes de mise à disposition sont associés à des groupes Active Directory.



5. La page **Général** dresse la liste des **identificateurs**, tels que le numéro de série et d'autres informations relatives au type de plate-forme. Pour **Propriétaire**, sélectionnez **Entreprise** ou **BYOD**.

   La page **Général** dresse également la liste des propriétés de **sécurité**, telles que ID fort, Verrouiller l'appareil, Contourner le verrouillage d'activation et d'autres informations relatives au type de plate-forme. Le champ **Effacement complet de l'appareil** inclut le code PIN de l'utilisateur. L'utilisateur doit entrer ce code une fois que l'appareil est effacé. Si l'utilisateur oublie le code, vous pouvez le rechercher ici.

6. La page **Propriétés** dresse la liste des propriétés d'appareil que XenMobile Server va provisionner. Cette liste affiche toutes les propriétés d'appareil incluses dans le fichier de provisioning utilisé pour ajouter l'appareil. Pour ajouter une propriété, cliquez sur **Ajouter**, puis sélectionnez une propriété dans la liste. Pour connaître les valeurs valides pour chaque propriété, consultez le PDF Valeurs et noms des propriétés d'appareil.

   Lorsque vous ajoutez une propriété, elle s'affiche initialement sous la catégorie dans laquelle vous l'avez ajoutée. Après avoir cliqué sur **Suivant** et être revenu sur la page **Propriétés**, la propriété s'affiche dans la liste appropriée.

   Pour supprimer une propriété, placez le curseur dessus et cliquez sur le **X** sur le côté droit. XenMobile Server supprime l'élément immédiatement.

7. Les sections **Détails de l'appareil** restantes contiennent des informations sommaires sur l'appareil.

- **Propriétés utilisateur :** affiche les rôles RBAC, les appartenances aux groupes, les comptes d'achat en volume et les propriétés de l'utilisateur. Vous pouvez retirer un compte d'achat en volume à partir de cette page.
- **Stratégies attribuées :** affiche le nombre de stratégies attribuées, y compris le nombre de stratégies déployées, en attente ou ayant échoué. Fournit les informations relatives au nom, au type et à la dernière date de déploiement pour chaque stratégie.
- **Applications :** affiche, pour le dernier inventaire, le nombre de déploiements d'applications installés, en attente et ayant échoué. Fournit le nom de l'application, l'identificateur, le type et d'autres informations. Pour une description des clés d'inventaire iOS et macOS, telles que **HasUpdateAvailable**, voir Protocole de gestion des appareils mobiles (MDM).
- **Média :** affiche, pour le dernier inventaire, le nombre de déploiements de médias installés, en attente et ayant échoué.
- **Actions :** affiche le nombre d'actions déployées, en attente et qui ont échoué. Fournit le nom de l'action et l'heure du dernier déploiement.
- **Groupes de mise à disposition :** affiche le nombre de groupes de mise à disposition ayant réussi, en attente et qui ont échoué. Pour chaque déploiement, fournit le nom du groupe mise à disposition et l'heure déploiement. Sélectionnez un groupe de mise à disposition pour afficher des informations plus détaillées, y compris l'état, l'action, le canal ou l'utilisateur.
- **Profils iOS :** affiche le dernier inventaire de profil iOS, y compris le nom, le type, l'organisation et une description.
- **Profils de provisioning iOS :** affiche les informations du profil de provisioning de distribution d'entreprise, telles que l'UUID, la date d'expiration, et si les profils sont gérés ou non gérés.
- **Certificats :** affiche pour les certificats valides, révoqués ou ayant expiré, des informations telles que le type, le fournisseur, l'émetteur, le numéro de série et le nombre de jours restants avant l'expiration.
- **Connexions :** affiche l'état de la première connexion et de la dernière connexion. Fournit pour chaque connexion, le nom d'utilisateur, l'heure de l'avant-dernière authentification et l'heure de la dernière authentification.
- **État du MDM :** affiche des informations telles que l'état du MDM, l'heure de la dernière notification push et l'heure de la dernière réponse de l'appareil.

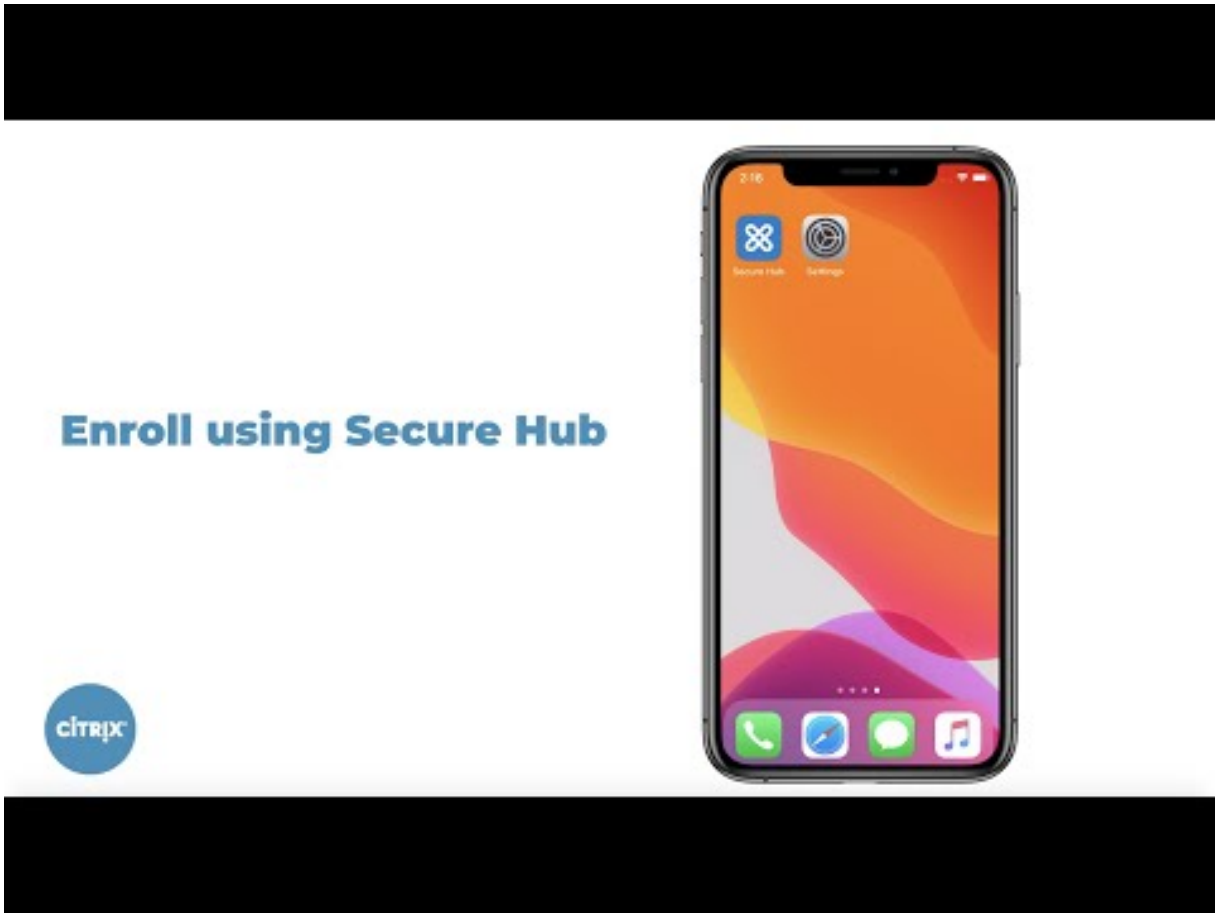
Configurer les stratégies d'appareil iOS

Utilisez ces stratégies pour configurer l'interaction entre XenMobile Server et les appareils exécutant iOS. Ce tableau répertorie toutes les stratégies d'appareils disponibles pour les appareils iOS.

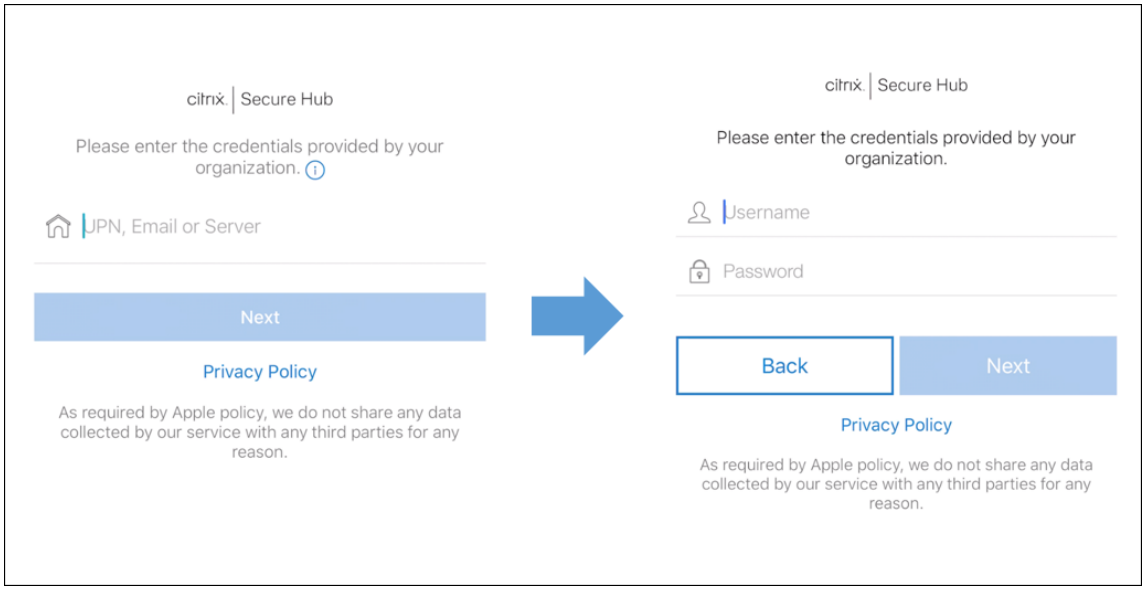
Mise en miroir AirPlay	AirPrint	APN
Accès aux applications	Attributs d'application	Configuration d'applications
Inventaire des applications	Mode kiosque	Utilisation réseau des applications
Désinstallation des applications	Notifications d'applications	Calendrier (CalDav)
Cellulaire	Contacts (CardDAV)	Contrôler mise à jour d'OS
Informations d'identification	Nom de l'appareil	Configuration de l'éducation
Exchange	Police	Disposition de l'écran d'accueil
Importer le profil iOS et macOS	LDAP	Emplacement
Messagerie	Domaines gérés	Options MDM
Infos organisation	Code secret	Personal Hotspot
Suppression de profil	Profil de provisioning	Suppression du profil de provisioning
Proxy	Restrictions	Itinérant
SCEP	iPad partagé - Nombre maximum d'utilisateurs résidents	iPad partagé - Période de grâce de verrouillage par code secret
Compte SSO	Magasin	Abonnements calendriers
Termes et conditions	VPN	Fond d'écran
Filtre de contenu Web	Clip Web	Wi-Fi

Inscrire des appareils iOS

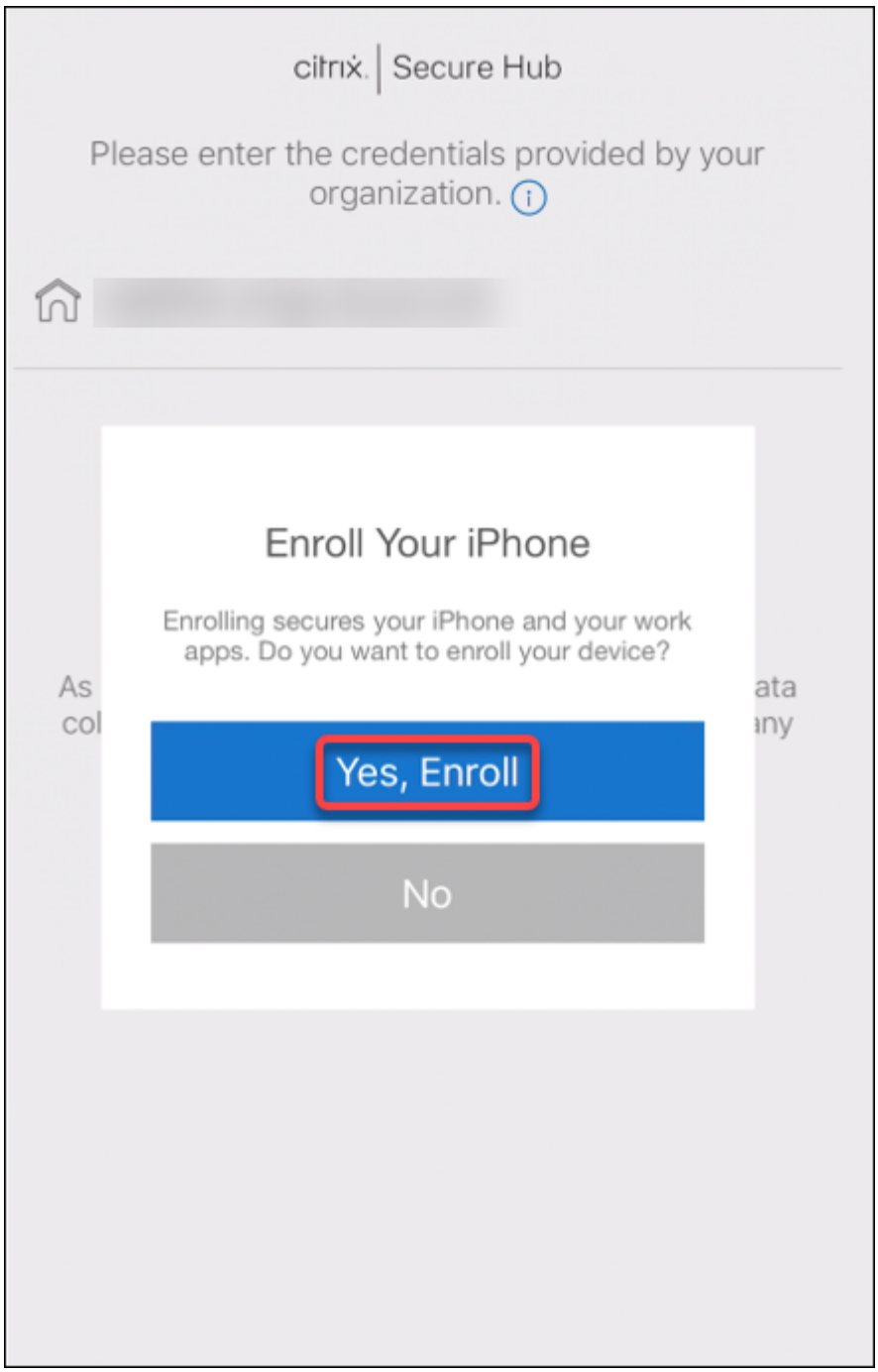
Cette section explique comment les utilisateurs inscrivent des appareils iOS (12.2 ou version ultérieure) dans XenMobile Server. Pour plus d'informations sur l'inscription iOS, ouvrez la vidéo suivante :



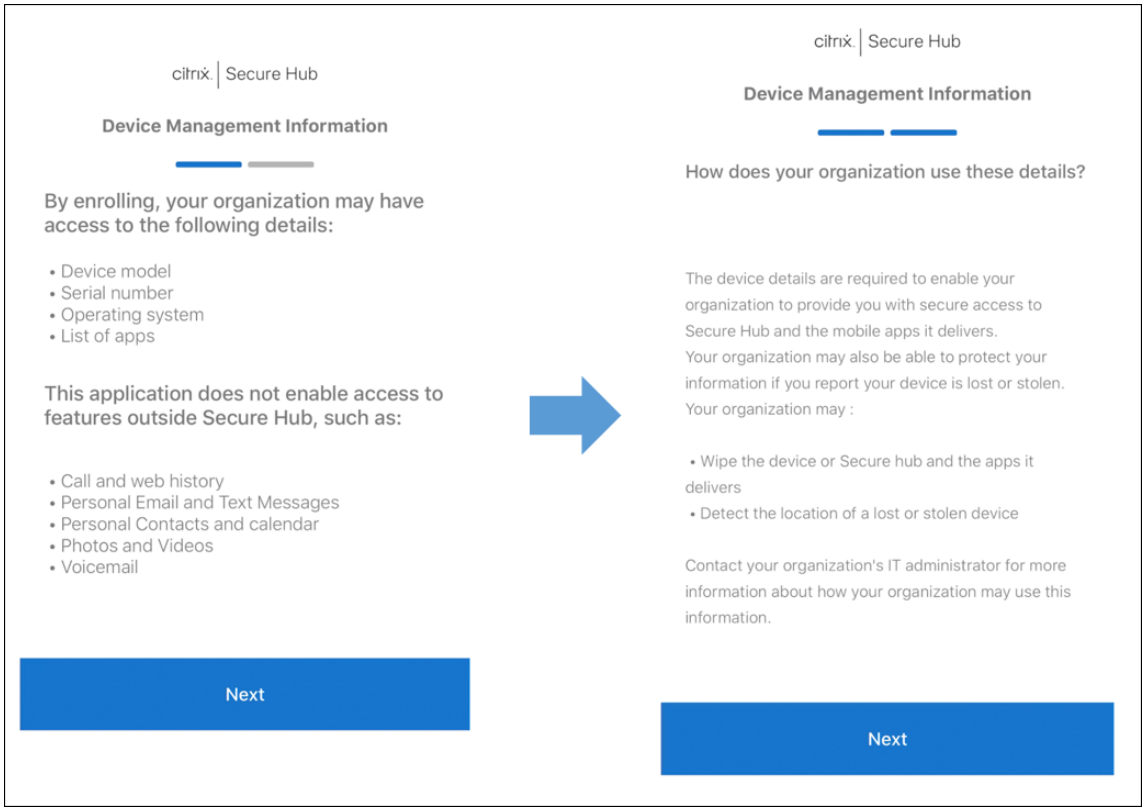
1. Accédez à l'Apple Store sur votre appareil iOS, téléchargez l'application Citrix Secure Hub, puis touchez l'application.
2. Lorsque vous êtes invité à installer l'application, touchez **Suivant**, puis **Installer**.
3. Après l'installation de Secure Hub, touchez **Ouvrir**.
4. Entrez vos informations d'identification d'entreprise, telles que le nom de votre serveur XenMobile Server, le nom d'utilisateur principal (UPN) ou votre adresse e-mail. Cliquez ensuite sur **Suivant**.



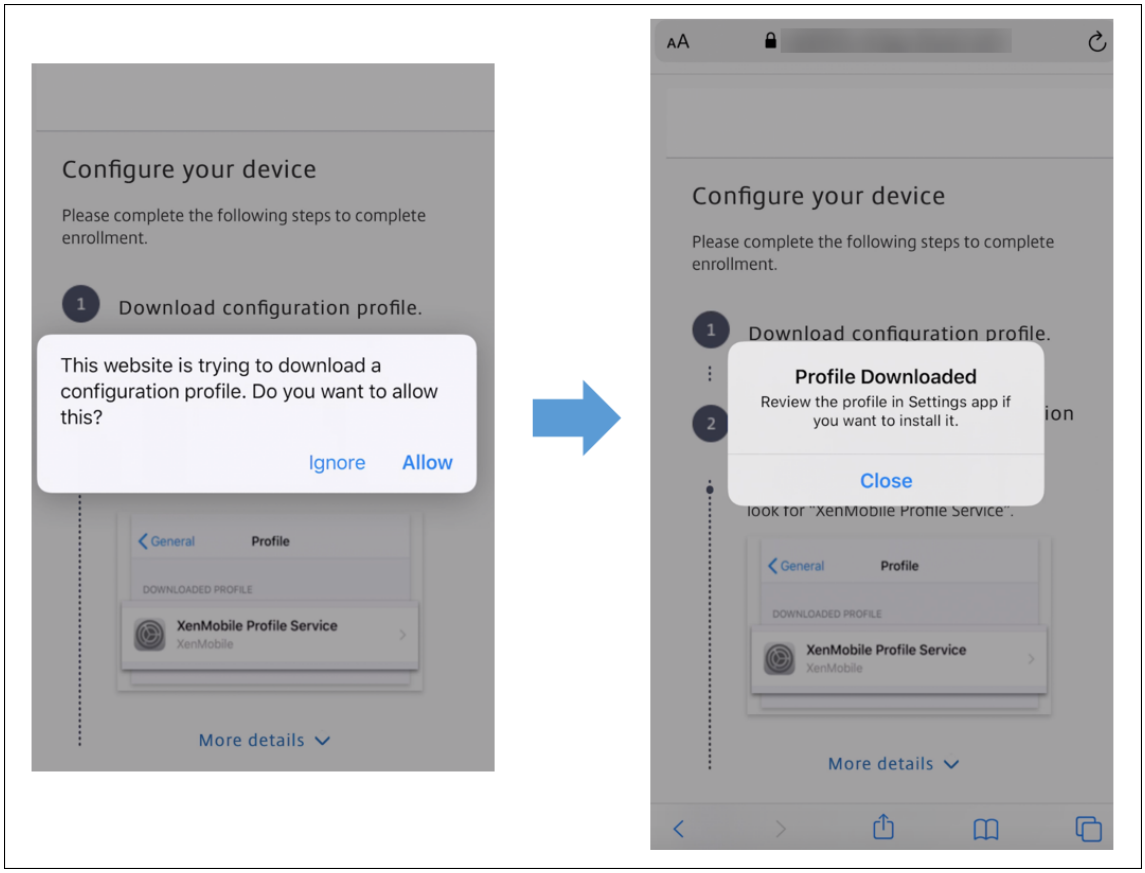
5. Touchez **Oui, inscrire** pour inscrire votre appareil iOS.



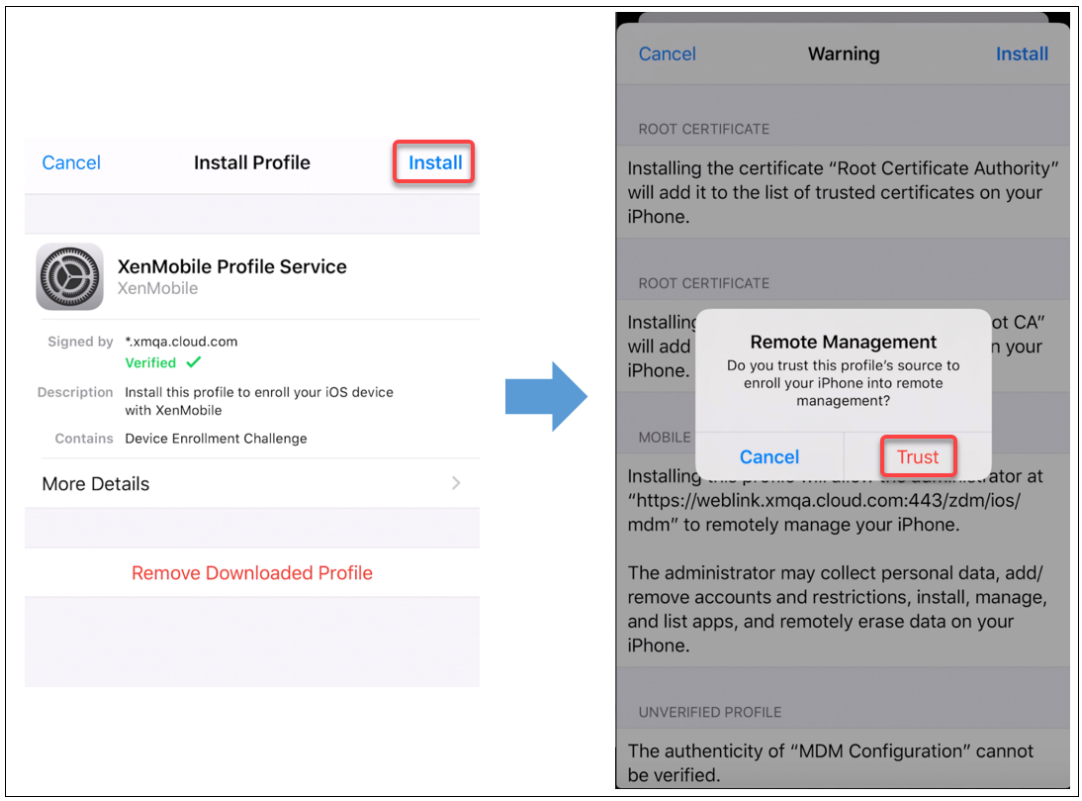
6. Une liste des données collectées par XenMobile Server s'affiche. Cliquez sur **Suivant**. Une explication de la façon dont une organisation utilise ces données apparaît. Cliquez sur **Suivant**.



7. Après avoir tapé vos informations d'identification, appuyez sur **Autoriser** lorsque vous y êtes invité, pour télécharger le profil de configuration. Après avoir téléchargé le profil de configuration, appuyez sur **Fermer**.



8. Dans les paramètres de votre appareil, installez le certificat iOS et ajoutez l'appareil à la liste de confiance.
   - Accédez à **Paramètres > Général > Profil > XenMobile Profile Service** et touchez **Installer** pour ajouter le profil.
   - Dans la fenêtre de notification, touchez **Faire confiance** pour inscrire votre appareil à la gestion à distance.



9. Une fois l'inscription réussie, ouvrez Secure Hub. Si vous vous inscrivez à MDM+MAM : une fois vos informations d'identification validées, créez et confirmez votre code PIN Citrix lorsque vous y êtes invité.
10. Une fois le workflow terminé, l'appareil est inscrit. Vous pouvez ensuite accéder au magasin d'applications pour afficher les applications que vous pouvez installer sur votre appareil iOS.

Actions de sécurisation

iOS prend en charge les actions de sécurisation suivantes. Pour obtenir une description de chaque action, consultez la section Actions de sécurisation.

Contourner le verrouillage d'activation	Mode kiosque	Effacement des applications
Verrouillage d'activation ASM	Renouvellement de certificat	Effacer les restrictions
Activer/Désactiver le mode perdu	Activer/Désactiver le suivi	Effacement complet
Localiser	Verrouiller	Faire sonner
Demander/Arrêter la mise en miroir AirPlay	Redémarrer/Arrêter	Révoquer/Autoriser

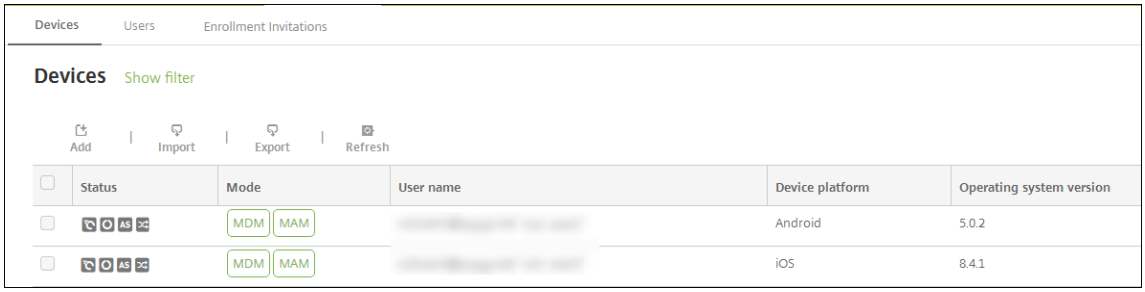
Effacer les données d'entreprise	Déverrouiller

Verrouiller les appareils iOS

Vous pouvez verrouiller un appareil iOS perdu tout en affichant un message et un numéro de téléphone sur l'écran de verrouillage.

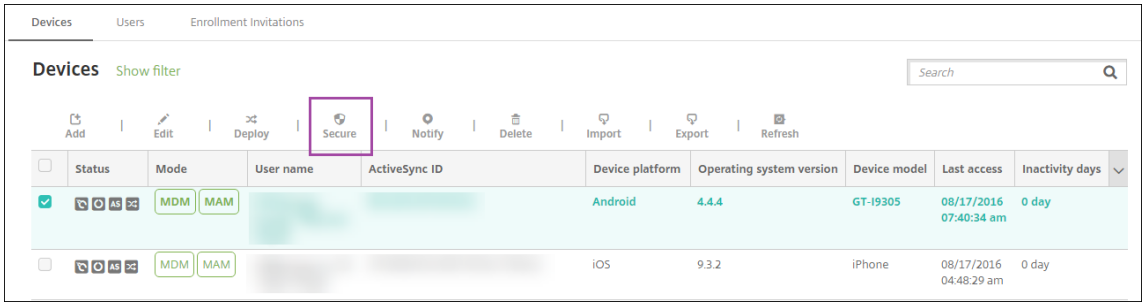
Pour afficher un message et un numéro de téléphone sur un appareil verrouillé, définissez la stratégie Code secret sur **true** dans la console XenMobile Server. Ou bien les utilisateurs peuvent activer le code secret sur l'appareil manuellement.

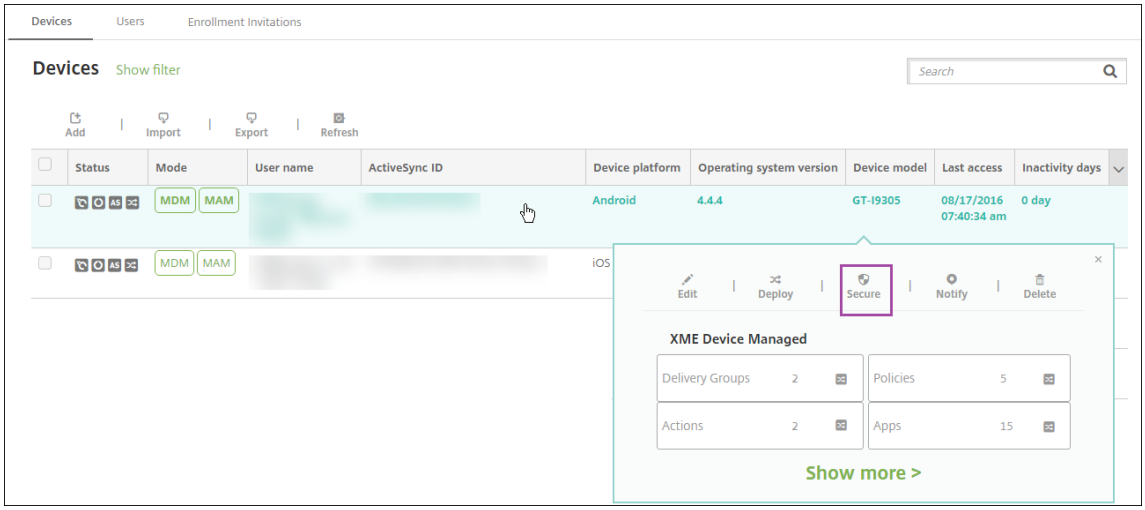
1. Cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.



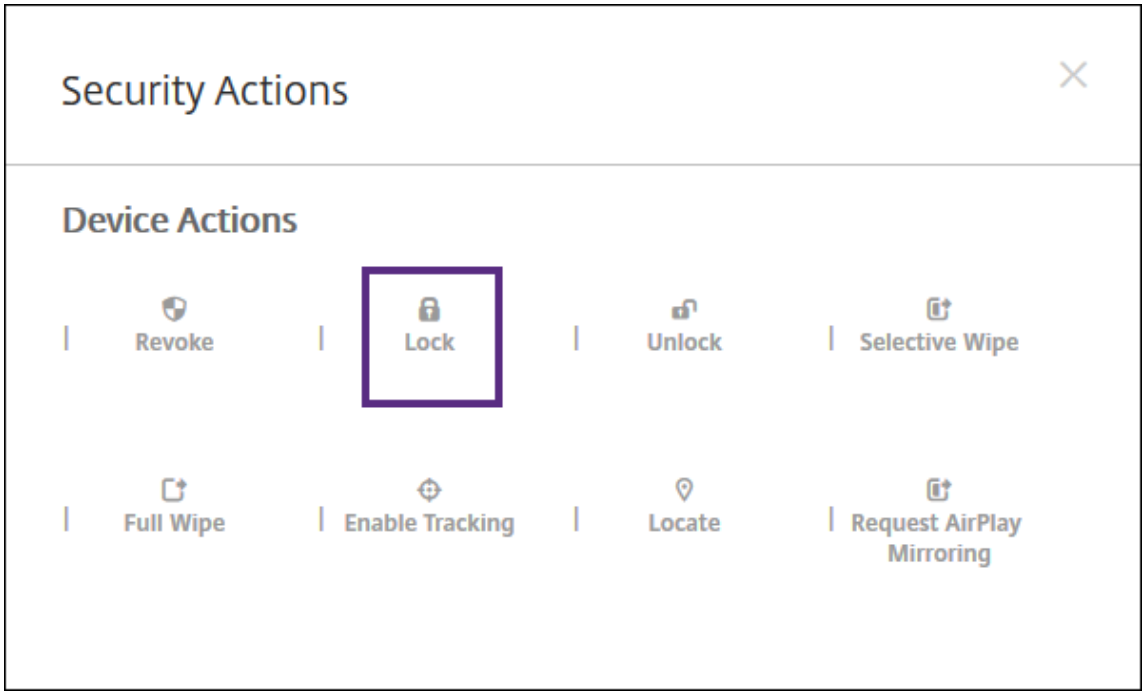
2. Sélectionnez l'appareil iOS que vous voulez verrouiller.

   Sélectionnez la case à cocher en regard d'un appareil pour afficher le menu d'options au-dessus de la liste des appareils. Cliquez dans la liste pour afficher le menu d'options sur le côté droit de la liste.

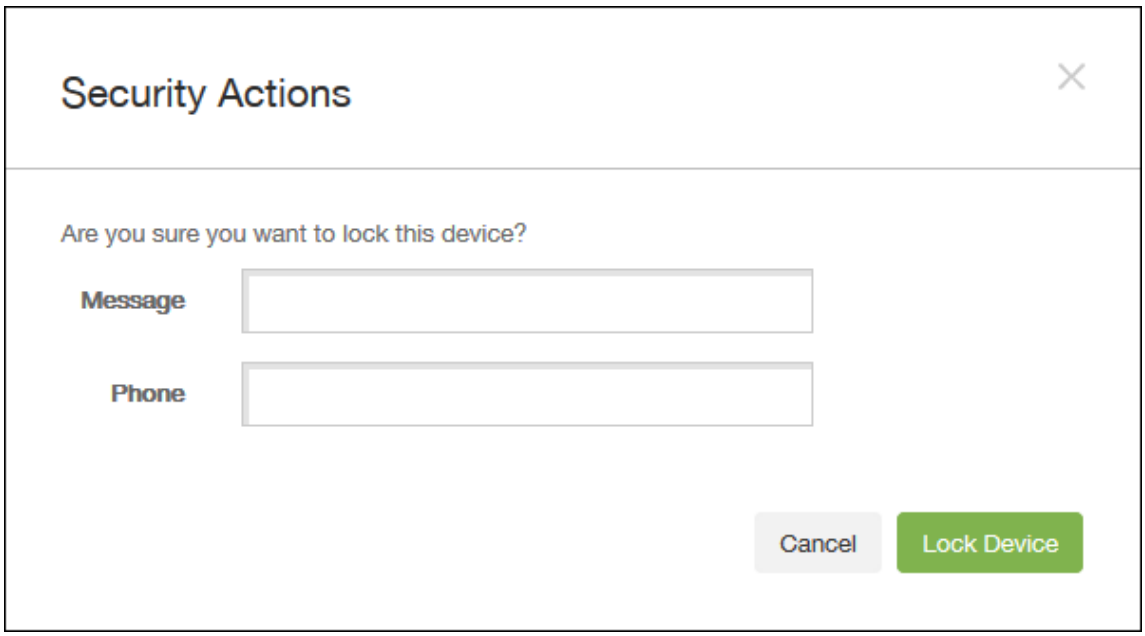




3. Dans le menu d'options, sélectionnez **Sécurité**. La boîte de dialogue **Actions de sécurisation** s'affiche.



4. Cliquez sur **Verrouiller**. La boîte de dialogue **Actions de sécurisation** s'affiche.



5. Si vous le souhaitez, entrez un message et un numéro de téléphone qui s'afficheront sur l'écran de verrouillage de l'appareil.

   iOS ajoute les mots « iPad perdu » au texte entré dans le champ **Message**.

   Si vous laissez le champ **Message** vide et que vous entrez un numéro de téléphone, Apple affiche le message « Appeler propriétaire » sur l'écran de verrouillage de l'appareil.

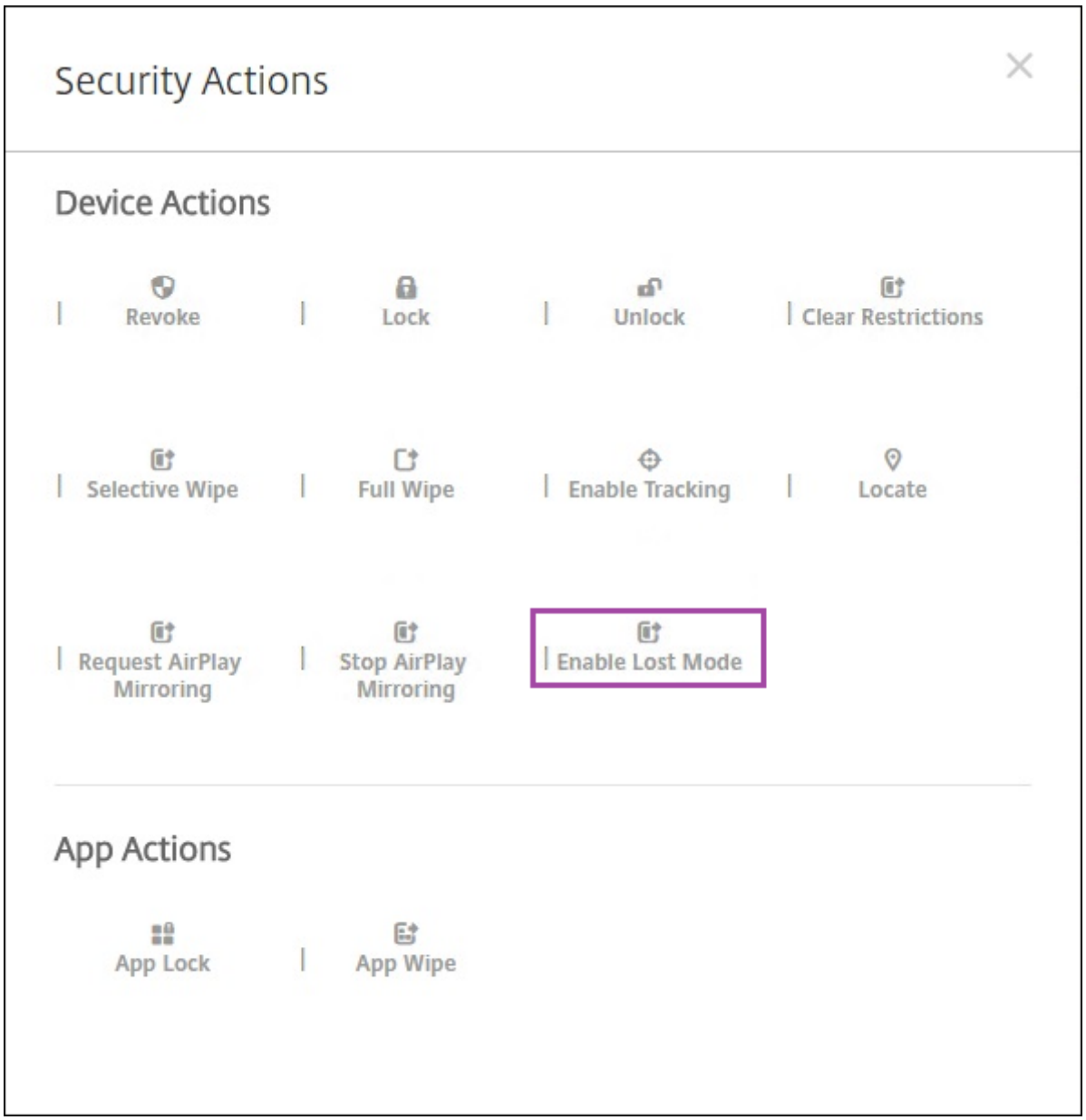
6. Cliquez sur **Verrouiller l'appareil**.

Placer les appareils iOS en Mode perdu

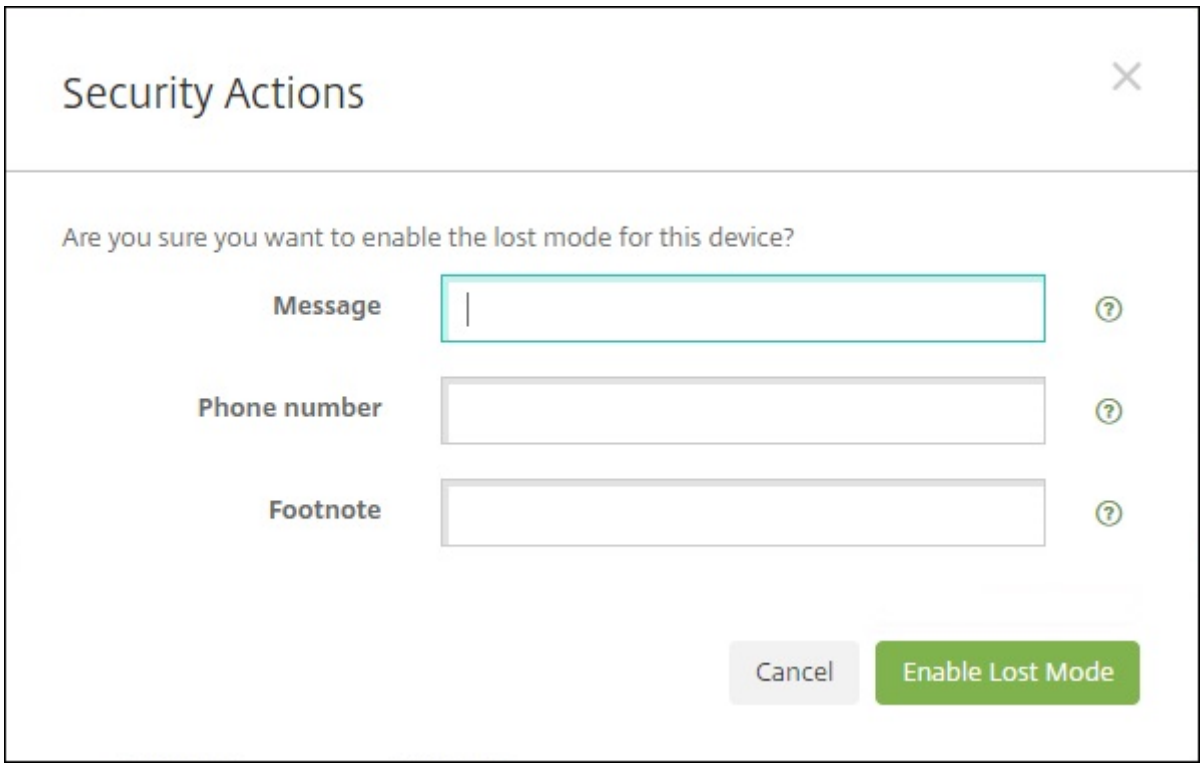
La propriété d'appareil Mode perdu de XenMobile Server place un appareil iOS en Mode perdu. Contrairement au mode perdu géré d'Apple, le mode perdu de XenMobile Server ne nécessite pas qu'un utilisateur effectue une des actions suivantes pour activer la recherche de son appareil : configurer le paramètre **Localiser mon iPhone/iPad** ou activer les Services de géolocalisation pour Citrix Secure Hub.

Dans le mode perdu de XenMobile Server, seul XenMobile Server peut déverrouiller l'appareil. (En revanche, si vous utilisez la fonctionnalité de verrouillage d'appareil de XenMobile Server, les utilisateurs peuvent déverrouiller l'appareil directement à l'aide d'un code PIN que vous devez fournir.

Pour activer ou désactiver le Mode perdu : accédez à **Gérer > Appareils**, choisissez un appareil iOS supervisé et cliquez sur **Sécurisé**. Ensuite, cliquez sur **Activer le mode perdu** ou **Désactiver le mode perdu**.

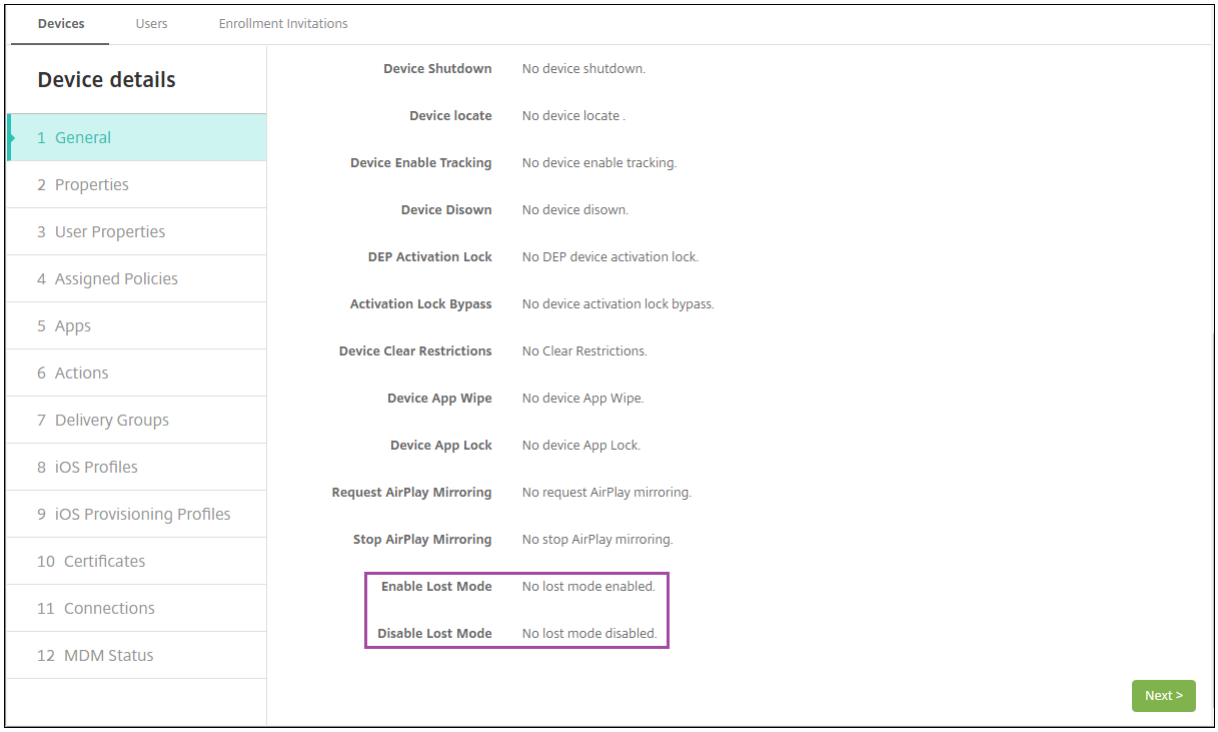


Si vous cliquez sur **Activer le mode perdu**, entrez les informations qui sont affichées sur l'appareil lorsqu'il est en mode perdu.

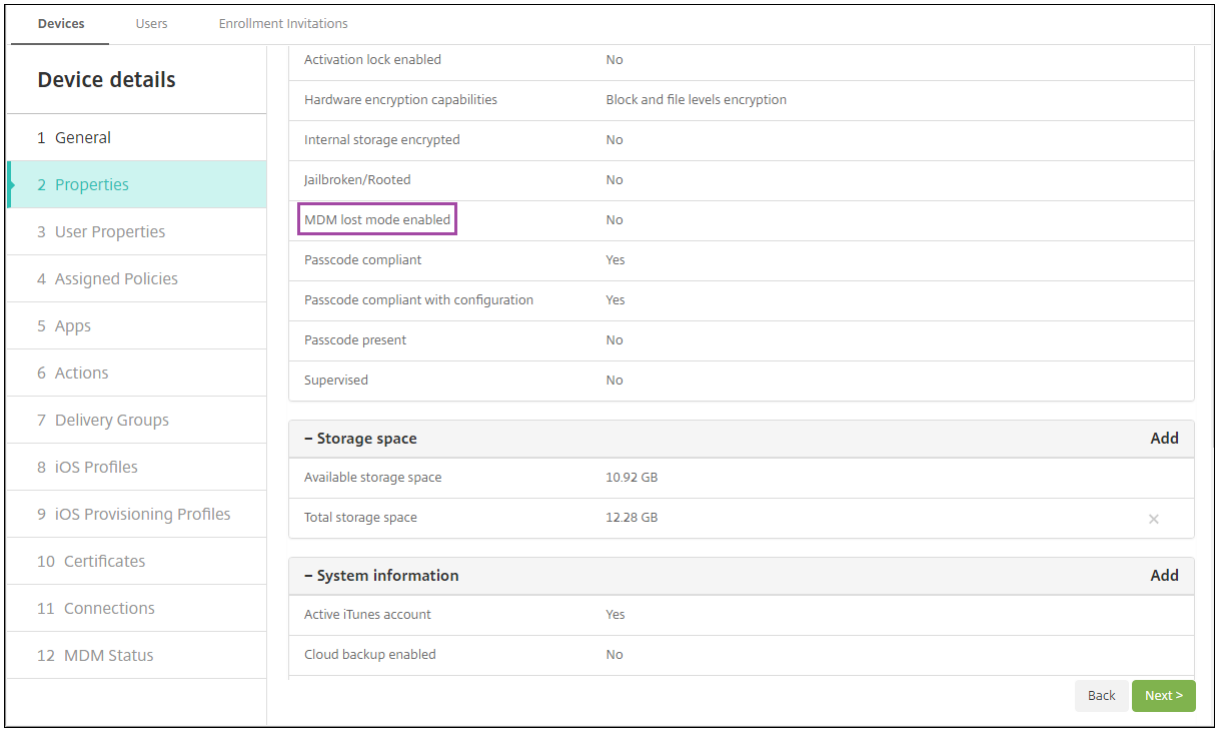


Pour vérifier l'état du mode perdu, utilisez une des méthodes suivantes :

- Dans la fenêtre **Actions de sécurisation**, vérifiez si le bouton indique **Désactiver le mode perdu**.
- Dans **Gérer > Appareils**, dans l'onglet **Général** sous **Sécurité**, consultez la dernière action Activer le mode perdu ou Désactiver le mode perdu.



- Dans **Gérer > Appareils**, dans l'onglet **Propriétés**, vérifiez que la valeur du paramètre **Mode perdu MDM activé** est correcte.



Si vous activez le mode perdu de XenMobile Server sur un appareil iOS, la console XenMobile Server est également modifiée comme suit :

- Dans **Configurer > Actions**, la liste **Actions** ne comprend pas ces actions automatiques : **Révoquer l'appareil**, **Effacer les données d'entreprise de l'appareil** et **Effacer toutes les données de l'appareil**.
- Dans **Gérer > Appareils**, la liste **Actions de sécurisation** n'inclut plus les actions **Révoquer** et **Effacer les données d'entreprise**. Vous pouvez toujours utiliser une action de sécurité pour effectuer une action **Effacement complet**, si nécessaire.

iOS ajoute les mots « iPad perdu » au texte entré dans **Message** dans l'écran **Actions de sécurisation**.

Si vous laissez **Message** vide et que vous entrez un numéro de téléphone, Apple affiche le message « Appeler propriétaire » sur l'écran de verrouillage de l'appareil.

Contourner un verrouillage d'activation iOS

Le verrouillage d'activation est une fonctionnalité de Localiser mon iPhone/iPad qui empêche la réactivation d'un appareil supervisé perdu ou volé. Le verrouillage d'activation requiert l'identifiant Apple et le mot de passe de l'utilisateur pour pouvoir effectuer ces actions : désactiver Localiser mon iPhone/iPad, effacer l'appareil ou réactiver l'appareil. Pour les appareils qui sont la propriété de votre organisation, il est nécessaire de contourner le verrouillage d'activation pour, par exemple, réinitialiser ou réattribuer des appareils.

Pour activer le verrouillage d'activation, configurez et déployez la stratégie Options MDM de XenMobile Server. Vous pouvez ensuite gérer un appareil à partir de la console XenMobile Server sans les informations d'identification Apple de l'utilisateur. Pour contourner l'obligation d'entrer des informations d'identification Apple avec un verrou d'activation, émettez l'action de sécurisation Contourner le verrouillage d'activation depuis la console XenMobile Server.

Par exemple, si l'utilisateur renvoie un téléphone perdu ou pour configurer l'appareil avant ou après un effacement complet : lorsque le téléphone invite à entrer les informations d'identification de compte Apple App Store, vous pouvez ignorer cette étape en émettant l'action de sécurité Contourner le verrouillage d'activation à partir de la console XenMobile Server.

Configuration requise pour le contournement du verrouillage d'activation

- Supervisé par Apple Configurator ou le programme de déploiement Apple
- Configuré avec un compte iCloud
- Localiser mon iPhone/iPad activé
- Inscrit dans XenMobile Server
- Stratégie Options MDM, avec verrouillage d'activation activé, déployée sur les appareils

Pour contourner le verrouillage d'activation avant d'émettre un effacement complet de l'appareil :

1. Accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Sécurisé**, puis cliquez sur **Contourner le verrouillage d'activation**.

2. Effacez l'appareil. L'écran de verrouillage d'activation ne s'affiche pas lors de l'installation de l'appareil.

Pour contourner le verrouillage d'activation après avoir émis un effacement complet de l'appareil :

1. Réinitialisez ou effacez l'appareil. L'écran de verrouillage d'activation s'affiche lors de l'installation de l'appareil.
2. Accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Sécurisé**, puis cliquez sur **Contourner le verrouillage d'activation**.
3. Cliquez sur le bouton Retour sur l'appareil. L'écran d'accueil s'affiche.

Gardez à l'esprit les considérations suivantes :

- Conseillez à vos utilisateurs de ne pas désactiver Localiser mon iPhone/iPad. N'effectuez pas d'effacement complet à partir de l'appareil. Dans ces deux cas, l'utilisateur est invité à entrer le mot de passe du compte iCloud. Après la validation du compte, l'utilisateur ne verra pas d'écran Activer iPhone/iPad après avoir effacé tout le contenu et les paramètres.
- Pour un appareil avec un code de contournement de verrouillage d'activation généré et avec le verrouillage d'activation activé : si vous ne pouvez pas contourner la page Activer iPhone/iPad après un effacement complet, il n'est pas nécessaire de supprimer l'appareil de XenMobile Server. Vous ou l'utilisateur pouvez contacter l'assistance Apple pour débloquer l'appareil directement.
- Lors d'un inventaire matériel, XenMobile Server interroge un appareil pour obtenir un code de contournement de verrouillage d'activation. Si un code de contournement est disponible, l'appareil l'envoie à XenMobile Server. Ensuite, pour supprimer le code de contournement de l'appareil, envoyez l'action de sécurisation Contourner le verrouillage d'activation à partir de la console XenMobile Server. À ce stade, XenMobile Server et Apple ont le code de contournement nécessaire pour débloquer l'appareil.
- L'action de sécurisation Contourner le verrouillage d'activation repose sur la disponibilité d'un service d'Apple. Si l'action ne fonctionne pas, vous pouvez débloquer un appareil comme suit. Sur l'appareil, entrez manuellement les informations d'identification du compte iCloud. Ou, laissez le champ de nom d'utilisateur vide et tapez le code de contournement dans le champ de mot de passe. Pour rechercher le code de contournement, accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Modifier** et cliquez sur **Propriétés**. Le **Code de contournement du verrouillage d'activation** se trouve sous **Informations de sécurité**.

macOS

January 10, 2022

Pour gérer des appareils macOS dans XenMobile, vous devez configurer un certificat Apple Push Noti-

fication Service (APNS). Pour de plus amples informations, consultez la section Certificats APNs.

XenMobile inscrit les appareils macOS dans MDM. XenMobile prend en charge les types d'authentification d'inscription suivants pour les appareils macOS en mode MDM.

- Domaine
- Domaine + mot de passe unique
- URL d'invitation + mot de passe unique

> **Exigences pour les certificats de confiance dans macOS 15 :**
>
> Apple a introduit de nouvelles exigences pour les certificats de serveur TLS. Vérifiez que tous les certificats respectent les nouvelles exigences d'Apple. Consultez la publication Apple, https://support.apple.com/en-us/HT210176. Pour obtenir de l'aide sur la gestion des certificats, consultez la section Chargement de certificats dans XenMobile.

Workflow général pour le démarrage de la gestion des appareils macOS :

1. Configurez les stratégies macOS.
2. Inscrivez les appareils macOS.
3. Configurez les actions de sécurité des appareils et des applications. Consultez la section Actions de sécurisation.

Pour les systèmes d'exploitation pris en charge, consultez la section Systèmes d'exploitation d'appareils pris en charge.

Noms d'hôtes Apple qui doivent rester ouverts

Certains noms d'hôtes Apple doivent rester ouverts pour assurer le bon fonctionnement d'iOS, de macOS et de l'Apple App Store. Le blocage de ces noms d'hôtes peut affecter l'installation, la mise à jour et le bon fonctionnement d'iOS, des applications iOS et de MDM et l'inscription des appareils et des applications. Pour plus d'informations, consultez https://support.apple.com/en-us/HT201999.

Méthodes d'inscription prises en charge

Le tableau suivant indique les méthodes d'inscription prises en charge par XenMobile pour les appareils macOS :

Méthode	Prise en charge
Programme de déploiement d'Apple	Oui
Apple School Manager	Oui
Apple Configurator	Non

Méthode	Prise en charge
Inscription manuelle	Oui
Invitations d'inscription	Oui

Apple propose des programmes d'inscription d'appareil pour les comptes d'entreprise et éducation. Pour les comptes d'entreprise, vous devez vous inscrire au Programme de déploiement d'Apple pour utiliser le programme Apple Device Enrollment Program (DEP) afin de gérer et inscrire des appareils dans XenMobile. Ce programme est pour les appareils iOS et macOS. Voir Déployer des appareils via le programme de déploiement d'Apple.

Pour les comptes éducation, vous devez créer un compte Apple School Manager. Apple School Manager unifie le programme de déploiement et l'achat en volume. Apple School Manager est un type de programme de déploiement Apple Éducation. Consultez la section Intégration avec les fonctionnalités Apple Éducation.

Vous pouvez utiliser le programme de déploiement d'Apple pour inscrire en bloc des appareils iOS et macOS. Vous pouvez acheter ces appareils directement auprès d'Apple, d'un revendeur agréé Apple ou d'un opérateur.

Configurer les stratégies macOS

Utilisez ces stratégies pour configurer l'interaction entre XenMobile et les appareils exécutant macOS. Ce tableau répertorie toutes les stratégies d'appareils disponibles pour les appareils macOS.

Mise en miroir AirPlay	Inventaire des applications	Calendrier (CalDav)
Contacts (CardDAV)	Contrôler mise à jour d'OS	Informations d'identification
Nom de l'appareil	Exchange	FileVault
Pare-feu	Police	Importer le profil iOS et macOS
LDAP	Messagerie	Code secret
Suppression de profil	Restrictions	SCEP
VPN	Clips Web	Wi-Fi

Inscrire les appareils macOS

XenMobile propose deux méthodes pour inscrire des appareils qui exécutent macOS. Les deux méthodes permettent aux utilisateurs macOS de s'inscrire sans fil (OTA) directement depuis leurs appareils.

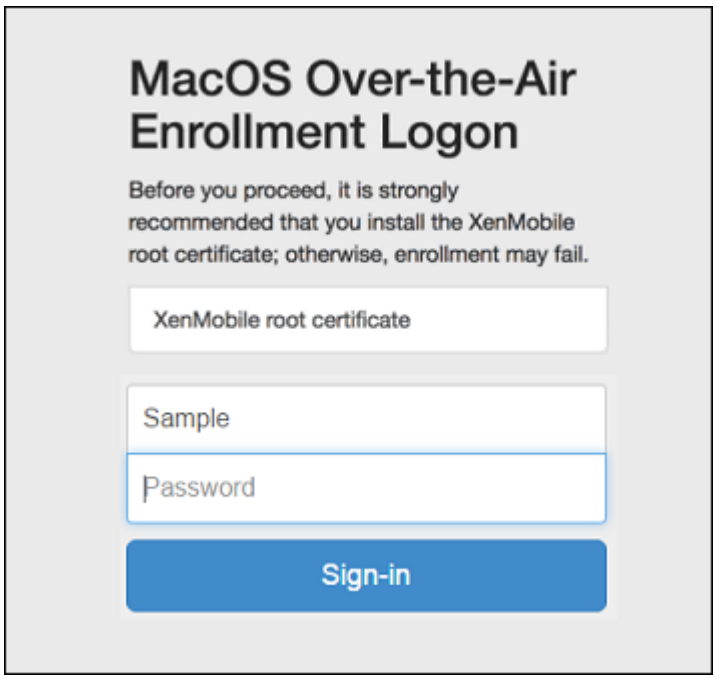
- **Envoyer une invitation d'inscription aux utilisateurs :** cette méthode d'inscription vous permet de définir un des modes d'inscription sécurisée suivants pour les appareils macOS :
  - Nom d'utilisateur + mot de passe
  - Nom d'utilisateur + PIN
  - Authentification à deux facteurs

  Lorsque l'utilisateur suit les instructions de l'invitation d'inscription, un écran de connexion avec le nom d'utilisateur déjà renseigné s'affiche.
- **Envoyer un lien d'inscription aux utilisateurs :** cette méthode d'inscription pour les appareils macOS envoie aux utilisateurs un lien d'inscription qu'ils peuvent ouvrir dans les navigateurs Safari et Chrome. Ensuite, un utilisateur s'inscrit en fournissant son nom d'utilisateur et son mot de passe.

  Pour empêcher l'utilisation d'un lien d'inscription pour les appareils macOS, définissez la propriété de serveur **Activer macOS OTAE** sur **false**. Les utilisateurs macOS peuvent alors s'inscrire uniquement à l'aide d'une invitation d'inscription.

Envoyer une invitation d'inscription aux utilisateurs macOS

1. Ajoutez une invitation pour l'inscription d'utilisateurs macOS. Consultez Créer une invitation d'inscription.
2. Une fois que les utilisateurs reçoivent l'invitation et cliquent sur le lien, l'écran suivant s'affiche dans le navigateur Safari. XenMobile remplit le nom d'utilisateur. Si vous avez choisi **Deux facteurs** pour le mode d'inscription sécurisée, un champ supplémentaire s'affiche.



3. Les utilisateurs installent les certificats, selon les besoins. Les utilisateurs sont invités à installer des certificats si vous avez configuré pour macOS un certificat SSL approuvé publiquement et un certificat de signature numérique approuvé publiquement. Pour de plus amples informations sur les certificats, consultez la section Certificats et authentification.
4. Les utilisateurs entrent les informations d'identification demandées.

   Les stratégies Mac s'installent. Vous pouvez maintenant démarrer la gestion des appareils macOS avec XenMobile tout comme vous gérez les appareils mobiles.

Envoyer un lien d'installation aux utilisateurs macOS

1. Envoyez le lien d'inscription `https://serverFQDN:8443/instanceName/macos/otae` que les utilisateurs peuvent ouvrir dans les navigateurs Safari ou Chrome.

   - **serverFQDN** est le nom de domaine complet du serveur exécutant XenMobile.
   - Le port **8443** est le port sécurisé par défaut. Si vous avez configuré un port différent, utilisez-le à la place de 8443.
   - Le **nom d'instance**, souvent affiché sous la forme `zdm`, est le nom spécifié lors de l'installation du serveur.

   Pour plus d'informations sur l'envoi de liens d'installation, consultez la section Envoyer une invitation d'inscription.
2. Les utilisateurs installent les certificats, selon les besoins. Si vous avez configuré un certificat SSL et un certificat de signature numérique approuvé publiquement pour iOS et macOS, les

utilisateurs sont invités à installer les certificats. Pour de plus amples informations sur les certificats, consultez la section Certificats et authentification.

3. Les utilisateurs se connectent à leur Mac.

   Les stratégies Mac s'installent. Vous pouvez maintenant démarrer la gestion des appareils macOS avec XenMobile tout comme vous gérez les appareils mobiles.

Actions de sécurisation

macOS prend en charge les actions de sécurisation suivantes. Pour obtenir une description de chaque action, consultez la section Actions de sécurisation.

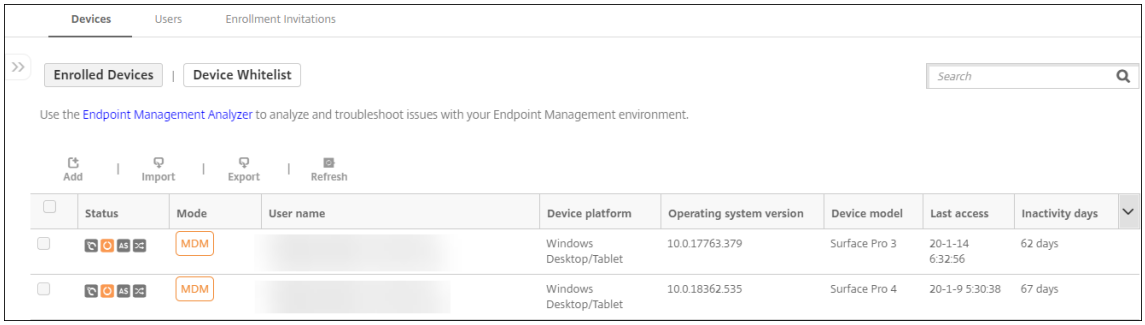
Révoquer	Verrouiller	Effacer les données d'entreprise
Effacement complet	Renouvellement de certificat	

Verrouiller les appareils macOS

Vous pouvez verrouiller à distance un appareil macOS perdu. XenMobile verrouille l'appareil. Ensuite, il génère un code PIN et le configure dans l'appareil. Pour accéder à l'appareil, l'utilisateur devra entrer ce code PIN. Utilisez **Annuler le verrouillage** pour retirer le verrouillage de la console XenMobile.

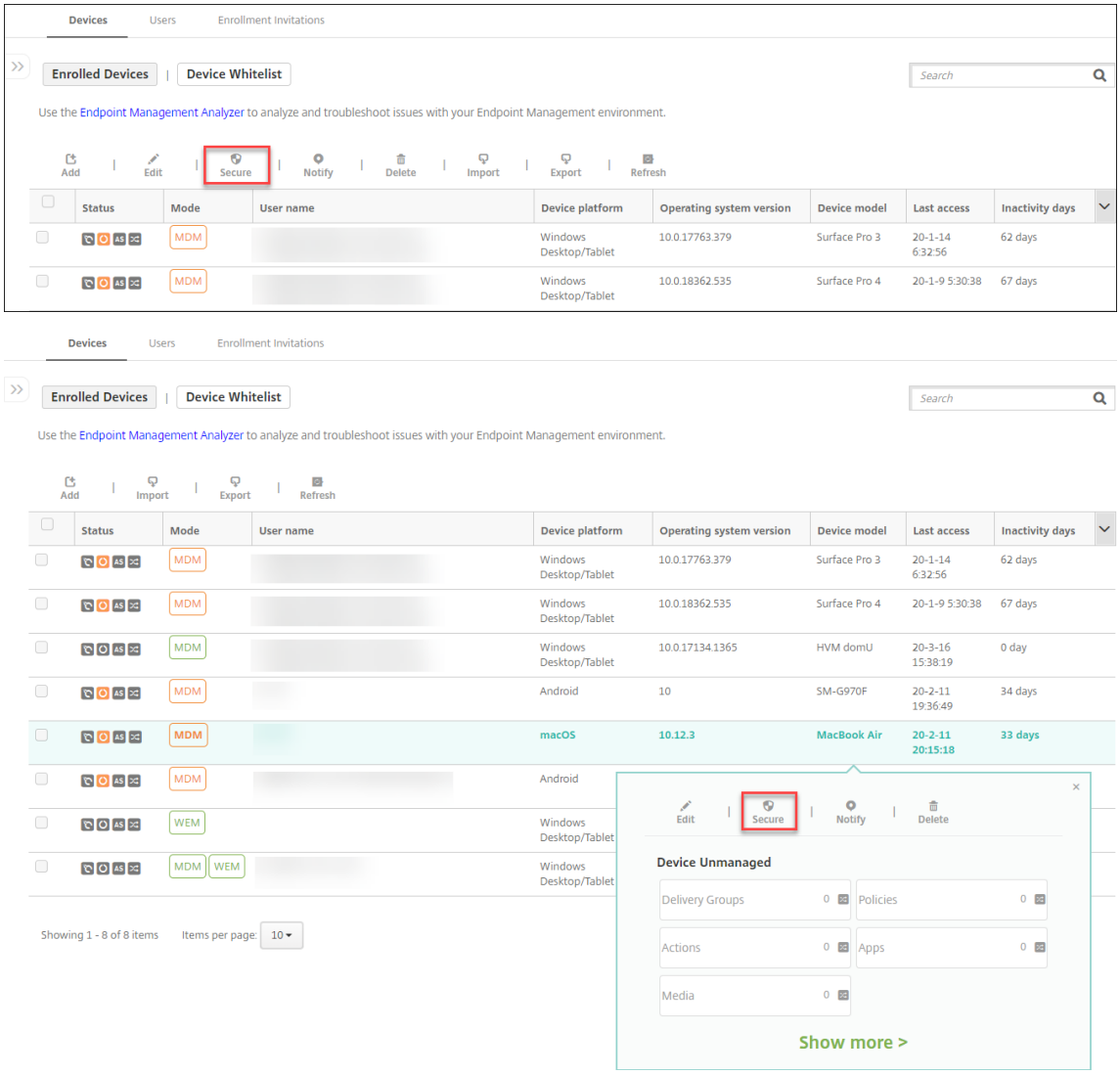
Vous pouvez utiliser la stratégie Code secret pour configurer d'autres paramètres associés au code PIN. Pour plus d'informations, consultez les paramètres macOS.

1. Cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.



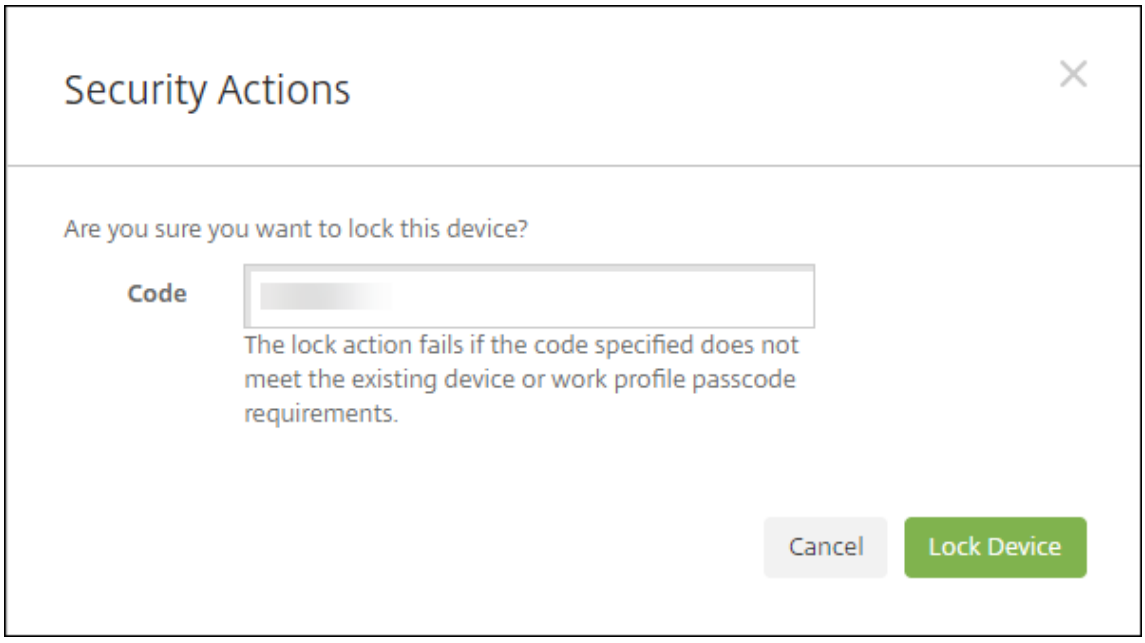
2. Sélectionnez l'appareil macOS que vous voulez verrouiller.

   Sélectionnez la case à cocher en regard d'un appareil pour afficher le menu d'options au-dessus de la liste des appareils. Vous pouvez également cliquer sur un élément répertorié pour afficher le menu des options sur le côté droit de la liste.



3. Dans le menu d'options, sélectionnez **Sécurité**. La boîte de dialogue **Actions de sécurisation** s'affiche.

4. Cliquez sur **Verrouiller**. La boîte de dialogue **Actions de sécurisation** s'affiche.



5. Cliquez sur **Verrouiller l'appareil**.

> **Important :**
>
> Vous pouvez également spécifier un mot de passe au lieu d'utiliser le code généré par XenMobile. L'action Verrouiller échoue si le code spécifié ne correspond pas aux exigences en matière de code de l'appareil ou du profil de travail existant.

Inscription en bloc d'appareils Apple

January 10, 2022

Vous pouvez inscrire un grand nombre d'appareils iOS, iPadOS et macOS dans XenMobile de deux façons.

- Utilisez le programme de déploiement d'Apple pour inscrire les appareils iOS, iPadOS et macOS que vous achetez directement auprès d'Apple, d'un revendeur agréé Apple ou d'un opérateur. Ce support inclut les iPad partagés. XenMobile prend en charge le programme de déploiement d'Apple pour Apple Business Manager (ABM) et Apple School Manager (ASM) pour l'éducation. Cet article décrit comment intégrer plusieurs appareils à votre compte ABM. Pour plus d'informations sur l'inscription à ABM et la connexion de votre compte ABM à XenMobile, consultez Déployer des appareils via le programme de déploiement d'Apple. Pour plus d'informations sur les comptes du programme Apple School Manager, consultez la section Intégration avec les fonctionnalités Apple Éducation.

  Pour l'inscription d'appareils macOS, XenMobile exige que les appareils exécutent macOS 10.10 ou version ultérieure.

- Vous pouvez également utiliser Apple Configurator 2 pour inscrire des appareils iOS, qu'ils aient été achetés ou non directement auprès d'Apple.

Avec ABM :

- Vous n'avez aucune tâche de préparation à effectuer sur les appareils. Vous envoyez simplement les numéros de série des appareils ou les numéros de commande via ABM pour configurer et inscrire les appareils.
- Une fois que XenMobile a inscrit les appareils, ils sont prêts à l'emploi et peuvent être distribués aux utilisateurs. Lorsque vous configurez des appareils avec ABM, vous pouvez supprimer certaines des étapes de l'Assistant d'installation que les utilisateurs doivent d'habitude réaliser la première fois qu'ils démarrent leurs appareils.
- Pour plus d'informations sur la configuration d'ABM, consultez la documentation disponible auprès d'Apple Business Manager.

Avec Apple Configurator 2 :

- Vous associez des appareils iOS à un ordinateur Apple exécutant macOS 10.7.2 ou version ultérieure et l'application Apple Configurator 2. Vous préparez les appareils iOS et configurez des stratégies à l'aide de Apple Configurator 2.
- Après avoir provisionné les appareils avec les stratégies requises, la première fois que les appareils se connectent à XenMobile, les appareils reçoivent les stratégies depuis XenMobile. Vous pouvez alors commencer à gérer les appareils.

- Pour de plus amples informations sur l'utilisation de Apple Configurator 2, consultez l'aide de Apple Configurator.

Conditions préalables

Ouvrez les ports requis pour la connexion entre XenMobile et Apple. Pour plus d'informations, consultez la section Configuration requise pour les ports.

Intégrer votre compte ABM avec XenMobile

Si vous n'avez pas de compte ABM configuré avec XenMobile, Apple Business Manager Déployer des appareils via le programme de déploiement d'Apple.

- S'inscrire à Apple Business Manager
- Connectez votre compte Apple Business Manager à XenMobile.
- Commander des appareils compatibles avec le programme de déploiement
- Gérer les appareils compatibles avec le programme de déploiement

Définir un serveur par défaut pour l'inscription en bloc

Pour attribuer des commandes volumineuses d'appareils iOS, iPadOS et macOS à un serveur MDM, vous pouvez définir XenMobile comme serveur par défaut.

1. Connectez-vous à Apple Business Manager avec un compte disposant du rôle Administrateur ou Gestionnaire d'inscription des appareils.
2. Dans la barre latérale, cliquez sur **Réglages > Réglages de la gestion des appareils**.
3. Choisissez un serveur MDM existant. Sous **Attribution d'appareils par défaut**, cliquez sur **Modifier**. Sélectionnez le serveur XenMobile par défaut pour chaque type d'appareil. Cliquez sur **Terminé**.

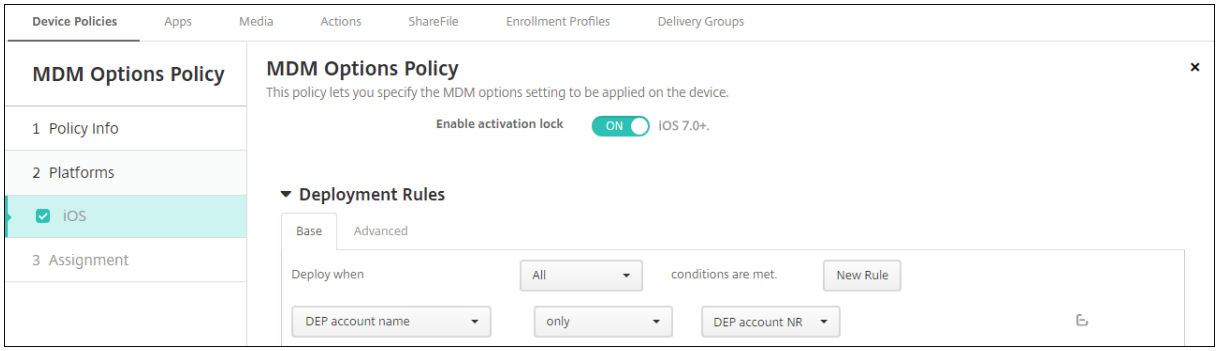
Configurer les règles de déploiement de stratégies et d'applications pour les comptes ABM

Vous pouvez associer les comptes ABM à différentes stratégies et applications à l'aide de la section **Règles de déploiement** sous **Configurer > Stratégies d'appareil** et **Configurer > Applications**. Vous pouvez spécifier l'une des conditions suivantes pour une stratégie ou une application :

- Elle sera déployée uniquement pour un compte ABM particulier.
- Elle sera déployée pour tous les comptes ABM, excepté celui sélectionné.

La liste des comptes ABM contient uniquement les comptes avec l'état activé ou désactivé. Si le compte ABM est désactivé, l'appareil ABM n'appartient pas à ce compte. Par conséquent, XenMobile ne déploie pas l'application ou la stratégie sur l'appareil.

Dans l'exemple suivant, une stratégie est déployée uniquement pour les appareils avec le nom de compte ABM « ABM Account NR ».

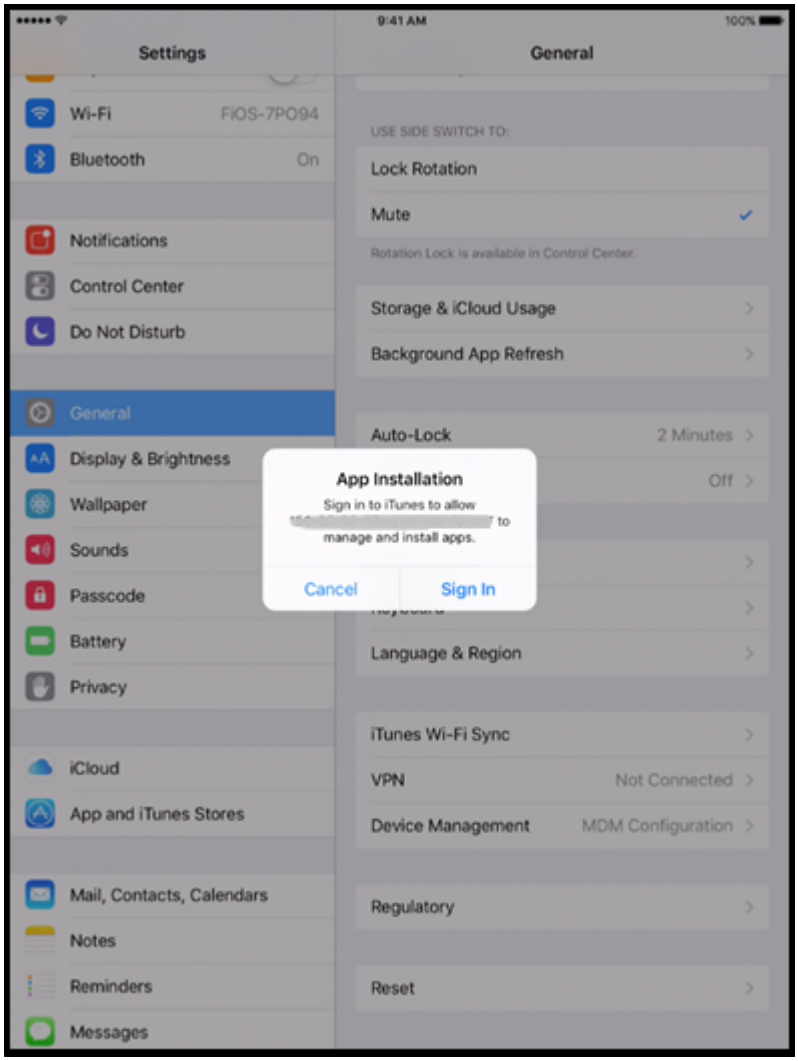


Expérience utilisateur lors de l'inscription d'un appareil compatible avec le programme de déploiement d'Apple

Lorsque les utilisateurs inscrivent un appareil compatible avec le programme de déploiement d'Apple, ils suivent la procédure ci-dessous.

1. Les utilisateurs démarrent leur appareil compatible avec le programme de déploiement d'Apple.
2. XenMobile transmet la configuration du programme de déploiement d'Apple que vous avez configurée dans la console XenMobile à l'appareil.
3. Les utilisateurs configurent les paramètres initiaux sur leur appareil.
4. L'appareil démarre automatiquement le processus d'inscription d'appareils de XenMobile.
5. Les utilisateurs configurent les autres paramètres initiaux sur leur appareil.
6. Dans l'écran d'accueil, les utilisateurs peuvent être invités à se connecter à l'Apple App Store afin de télécharger Citrix Secure Hub.

> **Remarque :**
>
> cette étape est facultative si XenMobile est configuré pour déployer l'application Secure Hub à l'aide de l'attribution d'applications d'achat en volume sur l'appareil. Dans ce cas, vous n'avez pas besoin de créer de compte Apple App Store ou d'utiliser un compte existant.



7. Les utilisateurs ouvrent Secure Hub et entrent leurs informations d'identification. Si cela est requis par la stratégie, les utilisateurs peuvent être invités à créer et vérifier un code PIN Citrix.

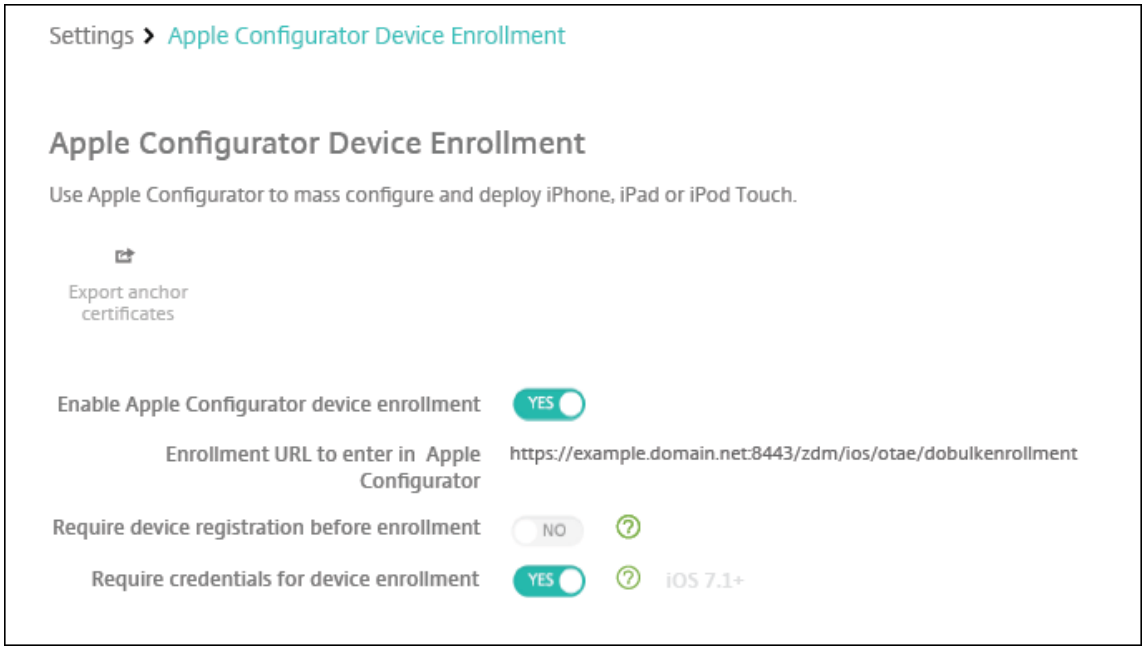
   XenMobile déploie les applications requises restantes sur l'appareil.

Configurer les paramètres d'Apple Configurator 2

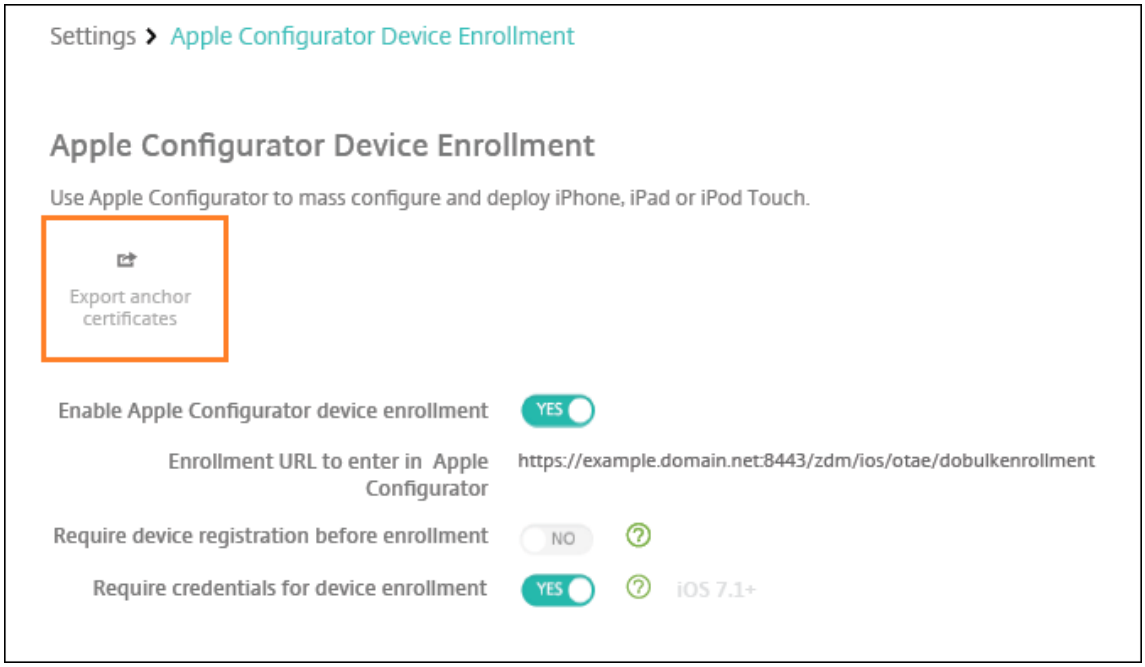
Vous pouvez configurer et déployer des appareils iPhone et iPad en bloc à l'aide d'Apple Configurator 2 au lieu d'Apple Business Manager.

Étape 1 : Configurer les paramètres dans XenMobile

1. Dans la console XenMobile, accédez à **Paramètres > Inscription d'appareils dans Apple Configurator**.



2. Définissez **Autoriser l'inscription d'appareils dans Apple Configurator** sur **Oui**.
3. Le champ **URL XenMobile à entrer dans Apple Configurator** est en lecture seule. Ce paramètre fournit l'adresse URL du serveur XenMobile qui communique avec Apple. Copiez et collez cette URL lorsque vous configurez les paramètres dans Apple Configurator 2. L'adresse URL d'inscription est le nom de domaine complet (FQDN) du serveur XenMobile, comme `mdm.server.url.com`, ou l'adresse IP.
4. Pour empêcher les appareils inconnus de s'inscrire, définissez **Exiger l'enregistrement des appareils avant l'inscription** sur **Oui**. Remarque : si ce paramètre est défini sur **Oui**, vous devez ajouter les appareils configurés à **Gérer > Appareils** dans XenMobile manuellement ou via un fichier CSV avant l'inscription.
5. Pour exiger que les utilisateurs d'appareils iOS entrent leurs informations d'identification lors de l'inscription, définissez **Exiger des informations d'identification pour l'inscription de l'appareil** sur **Oui**. Par défaut, les informations d'identification ne sont pas exigées pour l'inscription.
6. Remarque : si le serveur XenMobile utilise un certificat SSL approuvé, ignorez cette étape. Cliquez sur **Exporter les certificats d'ancrage** et enregistrez le fichier certchain.pem sur le trousseau macOS (de connexion ou système).



Étape 2 : Configurer les paramètres dans Apple Configurator 2

1. Installez Apple Configurator 2 à partir de l'App Store.
2. Utilisez un câble Dock Connector vers USB pour connecter des appareils au Mac exécutant Apple Configurator 2. Vous pouvez configurer simultanément jusqu'à 30 appareils connectés. Si vous ne disposez pas d'un Dock Connector, utilisez un ou plusieurs hubs (alimentés) USB 2.0 haute vitesse pour connecter les appareils.
3. Démarrez Apple Configurator 2. Le configurateur affiche tous les appareils que vous pouvez préparer à des fins de supervision.
4. Pour préparer un appareil à des fins de supervision :
   - Sélectionnez **Superviser des appareils** si vous souhaitez conserver le contrôle de l'appareil en réappliquant régulièrement une configuration. Cliquez sur **Suivant**.

     > **Important :**
     >
     > Le fait de placer un appareil en mode supervisé installe la version sélectionnée d'iOS sur l'appareil, ce qui efface complètement toutes les données et applications précédemment stockées par l'utilisateur.

   - Dans iOS, cliquez sur l'option appropriée afin d'obtenir la version **la plus récente** d'iOS que vous souhaitez installer.
5. Dans **Inscrire au serveur MDM**, choisissez un serveur MDM. Pour ajouter un nouveau serveur, cliquez sur **Suivant**

6. Dans **Définir un serveur MDM**, indiquez un nom pour le serveur et collez l'URL du serveur MDM à partir de la console XenMobile.
7. Dans **Attribuer à l'organisation**, choisissez une organisation pour superviser l'appareil.

   Pour plus d'informations sur la préparation d'appareils avec Apple Configurator 2, consultez la page d'aide d'Apple Configurator Prepare devices.
8. À mesure que chaque appareil est préparé, activez-le pour démarrer l'Assistant d'installation iOS, qui prépare l'appareil pour la première utilisation.

Attribuer des appareils depuis Apple Configurator 2 vers Apple Business Manager

Vous pouvez associer des appareils iPhone et iPad depuis Apple Configurator 2 vers votre compte Apple Business Manager. Lorsque vous ajoutez des appareils, ils apparaissent dans la section **Appareils**. Ces appareils n'incluent plus les paramètres d'inscription attribués via Apple Configurator 2. Pour plus d'informations, consultez Attribuer des appareils ajoutés depuis Apple Configurator 2 vers Apple Business Manager.

Renouveler ou mettre à jour des certificats lors de l'utilisation du programme de déploiement d'Apple

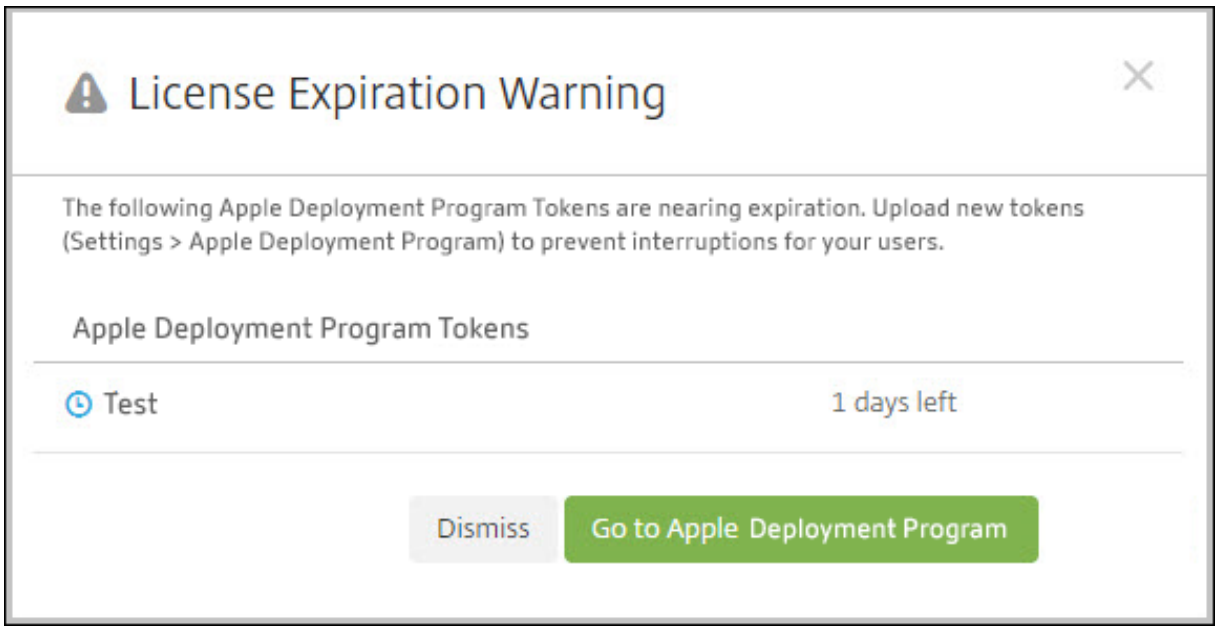
Lorsque le certificat SSL de XenMobile est renouvelé, vous chargez un nouveau certificat dans la console XenMobile dans **Paramètres > Certificats**. Dans la boîte de dialogue **Importer**, dans **Utiliser en tant que**, cliquez sur **Écouteur SSL** afin que le certificat soit utilisé pour SSL. Lorsque vous redémarrez le serveur, XenMobile utilise le nouveau certificat SSL. Pour de plus amples informations sur les certificats dans XenMobile, consultez la section Chargement de certificats dans XenMobile.

Il n'est pas nécessaire de rétablir la relation d'approbation entre le programme de déploiement d'Apple et XenMobile lorsque vous renouvelez ou mettez à jour le certificat SSL. Vous pouvez, cependant, reconfigurer vos paramètres **Programme de déploiement Apple** à tout moment en suivant les étapes précédentes dans cet article.

Pour plus d'informations sur le programme de déploiement d'Apple, consultez la documentation d'Apple.

Renouvelez votre connexion entre le programme de déploiement d'Apple et XenMobile

XenMobile affiche un avertissement d'expiration de licence lorsque votre jeton de serveur d'inscription automatique d'appareils expire.



Remplacez le jeton depuis Apple School Manager/Apple Business Manager.

Étape 1 : Télécharger une clé publique depuis votre serveur XenMobile

1. Dans la console XenMobile, accédez à **Paramètres > Programme de déploiement d'Apple** pour télécharger une nouvelle clé publique.

Étape 2 : Créer et télécharger un fichier de jeton de serveur depuis votre compte Apple

1. Connectez-vous à Apple Business Manager pour télécharger le jeton.
2. Ouvrez **Réglages** et sélectionnez le serveur auprès duquel vous devez vous procurer un jeton. Cliquez sur **Modifier**.
3. Sous **Réglages du serveur MDM**, chargez la nouvelle clé publique que vous avez téléchargée depuis XenMobile et enregistrez les modifications.
4. Cliquez sur **Télécharger le jeton** pour télécharger le nouveau jeton.

Étape 3 : Charger un fichier de jeton de serveur dans XenMobile

1. Dans Citrix XenMobile, accédez à **Paramètres > Programme de déploiement d'Apple**.
2. Sélectionnez le compte du programme de déploiement, cliquez sur **Modifier** et chargez votre fichier de jeton de serveur.
3. Cliquez sur **Suivant** et enregistrez les modifications.

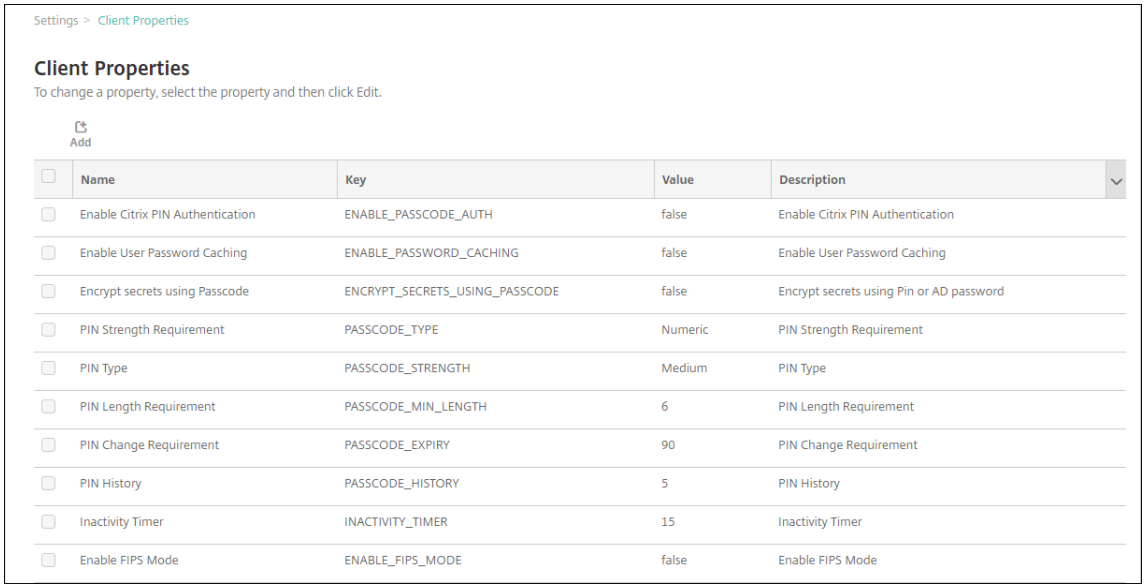
Propriétés du client

January 10, 2022

Les propriétés du client contiennent des informations qui sont fournies directement à Secure Hub sur les appareils des utilisateurs. Vous pouvez utiliser ces propriétés pour configurer des paramètres avancés tels que le code PIN Citrix. Vous obtenez les propriétés du client à partir du support de Citrix.

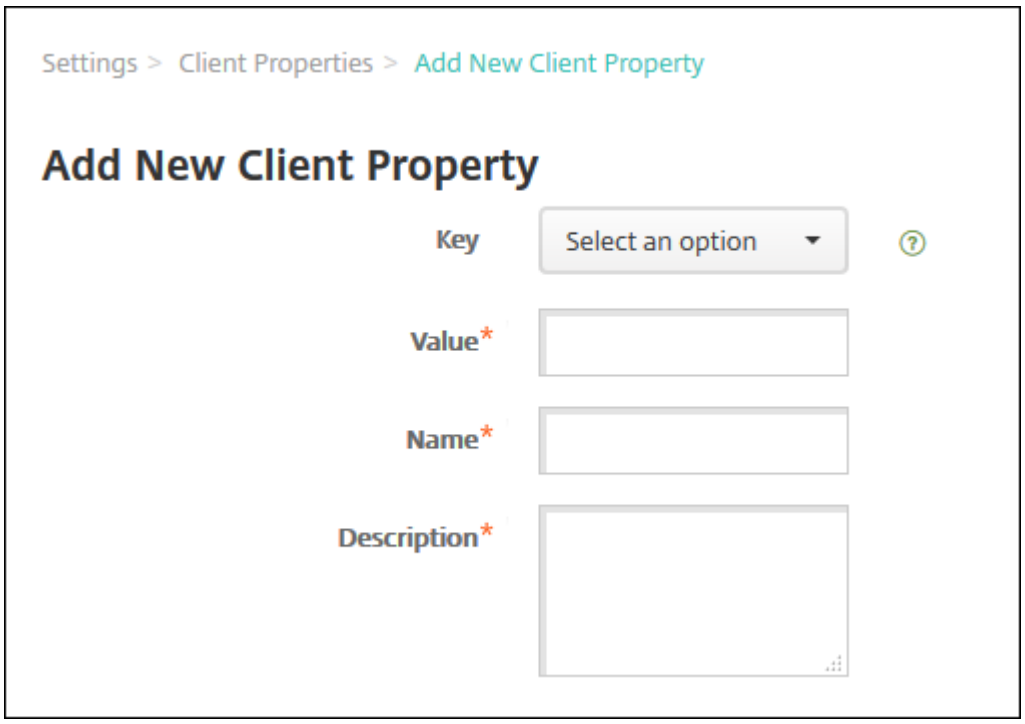
Les propriétés du client sont susceptibles d'être modifiées avec chaque nouvelle version de Secure Hub et occasionnellement pour les applications clientes. Pour de plus amples informations sur les propriétés du client les plus couramment configurées, consultez la section Propriété client, plus loin dans cet article.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Client**, cliquez sur **Propriétés du client**. La page **Propriétés du client** s'affiche. Vous pouvez ajouter, modifier et supprimer des propriétés de client à partir de cette page.



Pour ajouter une propriété de client

1. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle propriété de client** s'affiche.

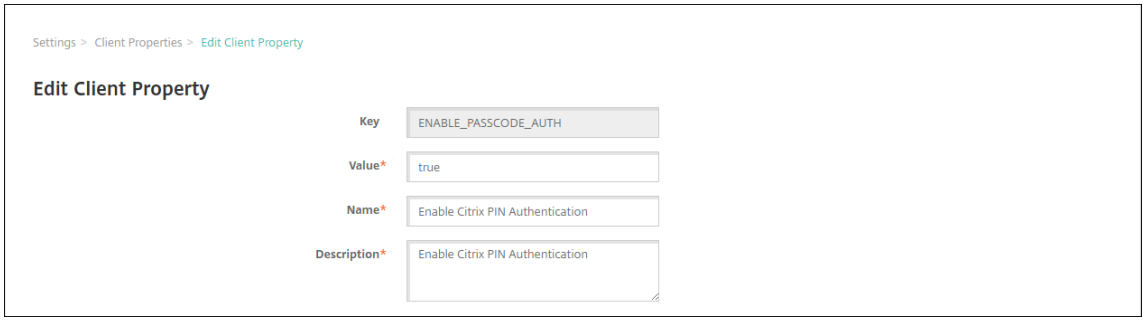


2. Pour configurer ces paramètres :
   - **Clé :** dans la liste, cliquez sur la clé de propriété que vous souhaitez ajouter. Important : contactez le support Citrix avant de mettre à jour les paramètres. Vous pouvez demander une clé spéciale.
   - **Valeur :** valeur de la propriété sélectionnée.
   - **Nom :** nom pour la propriété.
   - **Description :** description pour la propriété.
3. Cliquez sur **Enregistrer**.

Pour modifier une propriété de client

1. Dans le tableau **Propriétés du client**, sélectionnez la propriété de client que vous voulez modifier.

   Lorsque vous sélectionnez la case à cocher en regard d'une propriété de client, le menu d'options s'affiche au-dessus de la liste des propriétés de client. Lorsque vous cliquez dans la liste, le menu d'options s'affiche sur le côté droit de la liste.
2. Cliquez sur **Modifier**. La page **Modifier la propriété client** s'affiche.



3. Modifiez les informations suivantes le cas échéant :
   - **Clé :** vous ne pouvez pas modifier ce champ.
   - **Valeur :** valeur de la propriété.
   - **Nom :** nom de la propriété.
   - **Description :** description de la propriété.
4. Cliquez sur **Enregistrer** pour enregistrer vos modifications ou sur **Annuler** pour laisser la propriété inchangée.

Pour supprimer une propriété de client

1. Dans le tableau **Propriétés du client**, sélectionnez la propriété de client que vous voulez supprimer.

   Vous pouvez sélectionner plusieurs propriétés à supprimer en sélectionnant la case à cocher en regard de chaque propriété.
2. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer**.

Propriété client

Les propriétés client prédéfinies de XenMobile et leurs paramètres par défaut sont comme suit.

- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - Nom d'affichage : MDX Container Self Destruct Period (Période d'auto-destruction du conteneur MDX)
  - La fonction d'auto-destruction empêche l'accès à Secure Hub et aux applications gérées, après un nombre spécifié de jours d'inactivité. Après la limite de temps, les applications ne sont plus utilisables. L'effacement des données inclut la suppression des données d'application pour chaque application installée, y compris le cache et les données d'utilisateur de l'application.

Le délai d'inactivité correspond à une période de temps spécifique pendant laquelle le serveur ne reçoit pas de demande d'authentification pour valider l'utilisateur. Par exemple, si le délai est de 30 jours et que l'utilisateur n'utilise pas les applications pendant plus de 30 jours, la stratégie s'applique.

Cette stratégie de sécurité globale s'applique aux plates-formes iOS et Android et représente une amélioration des stratégies d'effacement et de verrouillage d'application existantes.

- Pour configurer cette stratégie globale, accédez à **Paramètres > Propriétés du client**, puis ajoutez la clé personnalisée **CONTAINER_SELF_DESTRUCT_PERIOD**.
- Valeur : nombre de jours.

- **DEVICE_LOGS_TO_IT_HELP_DESK**
  - Nom d'affichage : Send device logs to IT help desk (Envoyer les journaux de l'appareil au service d'assistance)
  - Cette propriété active ou désactive la possibilité d'envoyer des journaux au service d'assistance informatique.
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **false**
- **DISABLE_LOGGING**
  - Nom d'affichage : Disable Logging (Désactiver la journalisation)
  - Utilisez cette propriété pour empêcher les utilisateurs de collecter et de charger des journaux à partir de leurs appareils. Cette propriété désactive la journalisation pour Secure Hub et pour toutes les applications MDX installées. Les utilisateurs ne peuvent pas envoyer de journaux pour les applications à partir de la page Support. Bien que la boîte de dialogue de composition de messages s'affiche, les journaux ne sont pas joints. Un message indique que la journalisation est désactivée. Ce paramètre empêche également la mise à jour des paramètres de journal dans la console XenMobile pour Secure Hub et les applications MDX.

    Lorsque cette propriété est définie sur **true**, Secure Hub définit **Bloquer les journaux d'application** sur **true**. Par conséquent, les applications MDX arrêtent la journalisation lorsque la nouvelle stratégie est appliquée.
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **false** (la journalisation n'est pas désactivée)
- **ENABLE_CRASH_REPORTING**
  - Nom d'affichage : Enable Crash Reporting (Activer les rapports de plantage)

- Si le paramètre est réglé sur **true**, Citrix collecte les rapports d'incident et les diagnostics pour aider à résoudre les problèmes avec Secure Hub pour iOS et Android. Si ce paramètre est défini sur **false**, aucune donnée n'est collectée.
- Valeurs possibles : **true** ou **false**
- Valeur par défaut : **true**

- **ENABLE_CREDENTIAL_STORE**
  - Nom d'affichage : Activer le magasin d'informations d'identification
  - L'activation du magasin d'informations d'identification signifie que les utilisateurs Android ou iOS entrent leur mot de passe une fois lorsqu'ils accèdent à des applications de productivité mobiles. Vous pouvez utiliser le magasin d'informations d'identification que vous activiez ou non le code PIN Citrix. Si vous n'activez pas le code PIN Citrix, les utilisateurs entrent leur mot de passe Active Directory. XenMobile prend en charge l'utilisation de mots de passe Active Directory avec le magasin d'informations d'identification uniquement pour Secure Hub et les applications du magasin public. XenMobile ne prend pas en charge l'authentification PKI si vous utilisez des mots de passe Active Directory avec le magasin d'informations d'identification.
  - L'inscription automatique dans Secure Mail exige que vous définissiez cette propriété sur **true**.
  - Pour configurer cette stratégie personnalisée, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **ENABLE_CREDENTIAL_STORE** et définissez la **valeur** sur **true**.

- **ENABLE_FIPS_MODE**
  - Nom d'affichage : Enable FIPS Mode (Activer le mode FIPS)
  - Cette propriété active ou désactive le mode FIPS sur les appareils mobiles. Lorsque vous modifiez la valeur, Secure Hub transmet la nouvelle valeur à l'appareil lors de la prochaine authentification en ligne.
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **false**

- **ENABLE_PASSCODE_AUTH**
  - Nom d'affichage : Enable Citrix PIN Authentication (Activer l'authentification du code PIN Citrix)
  - Cette propriété permet d'activer la fonctionnalité de code PIN Citrix. Avec le code PIN ou code secret Citrix, les utilisateurs sont invités à définir un code PIN à utiliser à la place de leur mot de passe Active Directory. Ce paramètre est automatiquement activé si ENABLE_PASSWORD_CACHING est activé ou si XenMobile utilise l'authentification par certificat.

    Pour l'authentification en mode hors connexion, le code PIN Citrix est validé localement

et les utilisateurs sont autorisés à accéder à l'application ou au contenu demandé. Pour l'authentification en ligne, le code PIN ou code secret Citrix déverrouille le mot de passe Active Directory ou le certificat qui est ensuite envoyé à des fins d'authentification auprès de XenMobile.

Si ENABLE_PASSCODE_AUTH est défini sur true et ENABLE_PASSWORD_CACHING est défini sur false, l'authentification en ligne vous invite toujours à entrer le mot de passe car Secure Hub ne l'enregistre pas.

- Valeurs possibles : **true** ou **false**
- Valeur par défaut : **false**

- **ENABLE_PASSWORD_CACHING**
  - Nom d'affichage : Enable User Password Caching (Activer la mise en cache du mot de passe de l'utilisateur)
  - Cette propriété autorise la mise en cache locale des mots de passe Active Directory sur l'appareil mobile. Lorsque vous définissez cette propriété sur **true**, vous devez également définir la propriété **ENABLE_PASSCODE_AUTH** sur **true**. Lorsque la mise en cache du mot de passe de l'utilisateur est activée, les utilisateurs sont invités à créer un code PIN ou code secret Citrix.
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **false**
- **ENABLE_TOUCH_ID_AUTH**
  - Nom d'affichage : Enable Touch ID Authentication (Activer l'authentification TouchID)
  - Pour les appareils qui prennent en charge l'authentification Touch ID, cette propriété active ou désactive l'authentification Touch ID sur l'appareil. Exigences :

    Le code PIN Citrix ou l'authentification LDAP doivent être activés sur les appareils utilisateur. Si l'authentification LDAP est désactivée (par exemple, lorsque seule l'authentification basée sur certificat est utilisée), les utilisateurs doivent définir un code PIN Citrix. Dans ce cas, XenMobile nécessite le code PIN Citrix même si la propriété de client **ENABLE_PASSCODE_AUTH** est **false**.

    Définissez **ENABLE_PASSCODE_AUTH** sur **false** de sorte que, lorsque les utilisateurs lancent une application, ils doivent répondre à une invite à utiliser la fonctionnalité Touch ID.
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **false**
- **ENABLE_WORXHOME_CEIP**
  - Nom d'affichage : Enable Worx Home CEIP (Activer le programme CEIP de Worx Home)

  - Cette propriété active le Programme d'amélioration de l'expérience utilisateur. Cette fonction va envoyer périodiquement des données de configuration et d'utilisation anonymes à Citrix. Les données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de XenMobile.
  - Valeur : **true** ou **false**
  - Valeur par défaut : **false**

- **ENABLE_WORXHOME_GA**
  - Nom d'affichage : Enable Google Analytics in Worx Home (Activer Google Analytics dans Worx Home)
  - Cette propriété active ou désactive la possibilité de collecter des données à l'aide de Google Analytics dans Secure Hub. Lorsque vous modifiez ce paramètre, la nouvelle valeur est appliquée la prochaine fois que l'utilisateur se connecte à Secure Hub (anciennement Worx Home).
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **true**

- **ENCRYPT_SECRETS_USING_PASSCODE**
  - Nom d'affichage : Encrypt secrets using Passcode (Chiffrer les secrets à l'aide d'un code secret)
  - Cette propriété stocke les données sensibles sur l'appareil dans un coffre sécurisé plutôt que dans un magasin natif basé sur la plate-forme, tel que le trousseau iOS. Cette propriété offre un cryptage renforcé des artefacts clés et ajoute une entropie utilisateur. L'entropie utilisateur est un code PIN généré de manière aléatoire connu uniquement de l'utilisateur.

    Citrix vous recommande d'activer cette propriété de manière à fournir une sécurité plus élevée sur les appareils des utilisateurs. Par conséquent, les utilisateurs seront invités plus fréquemment à entrer le code PIN Citrix.
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **false**

- **INACTIVITY_TIMER**
  - Nom d'affichage : Inactivity Timer (Délai d'inactivité)
  - Cette propriété définit la durée pendant laquelle les utilisateurs peuvent laisser leurs appareils inactifs et accéder à une application sans être invité à entrer un code PIN ou code secret Citrix. Pour activer ce paramètre pour une application MDX, vous devez définir le paramètre Code secret d'application sur Activé. Si le paramètre Code secret d'application est défini sur Désactivé, les utilisateurs sont redirigés vers Secure Hub pour effectuer une authentification complète. Lorsque vous modifiez ce paramètre, la valeur prend effet la prochaine fois que les utilisateurs sont invités à s'authentifier.

Sur iOS, le délai d'inactivité gère également l'accès des applications MDX et non MDX à Secure Hub.

- Valeurs possibles : tout entier positif
- Valeur par défaut : **15** (minutes)

- **ON_FAILURE_USE_EMAIL**
  - Nom d'affichage : On failure Use Email to Send device logs to IT help desk (En cas d'échec, utiliser la messagerie pour envoyer les journaux de l'appareil au service d'assistance)
  - Cette propriété active ou désactive la possibilité d'utiliser la messagerie pour envoyer les journaux de l'appareil au service informatique.
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **true**

- **PASSCODE_EXPIRY**
  - Nom d'affichage : PIN Change Requirement (Exigences en matière de modification du code PIN)
  - Cette propriété définit la durée pendant laquelle le code PIN ou code secret Citrix est valide, et après laquelle l'utilisateur est obligé de modifier son code PIN ou code secret Citrix. Lorsque vous modifiez ce paramètre, la nouvelle valeur est définie uniquement lorsque le code PIN ou code secret Citrix expire.
  - Valeurs possibles : **1**-**99** recommandé. Pour éliminer les réinitialisations de code PIN, définissez la valeur sur un nombre très élevé (par exemple, 100 000 000 000). Si vous avez initialement défini une période d'expiration comprise entre 1 et 99 jours et que vous la modifiez au profit d'une valeur beaucoup plus élevée, les codes PIN expirent toujours à la fin de la période initiale mais plus jamais après.
  - Valeur par défaut : **90** (jours)

- **PASSCODE_HISTORY**
  - Nom d'affichage : PIN History (Historique du code PIN)
  - Cette propriété définit le nombre de codes PIN ou codes secrets Citrix précédemment utilisés que les utilisateurs ne sont pas autorisés à réutiliser lorsqu'ils changent leur code PIN ou code secret Citrix. Lorsque vous modifiez ce paramètre, la nouvelle valeur est définie la prochaine fois que les utilisateurs réinitialisent leur code PIN ou code secret Citrix.
  - Valeurs possibles : **1**-**99**
  - Valeur par défaut : **5**

- **PASSCODE_MAX_ATTEMPTS**
  - Nom d'affichage : PIN Attempts (Nombre de tentatives de saisie du code PIN)
  - Cette propriété définit le nombre de tentatives de saisie infructueuses du code PIN ou code secret Citrix que les utilisateurs peuvent effectuer avant d'être invités à fournir une au-

thentification complète. Une fois que les utilisateurs ont effectué une authentification complète, ils sont invités à créer un code PIN ou code secret Citrix.
  - Valeurs possibles : tout entier positif
  - Valeur par défaut : **15**

- **PASSCODE_MIN_LENGTH**
  - Nom d'affichage : PIN Length Requirement (Exigences en matière de longueur du code PIN)
  - Cette propriété définit la longueur minimale des codes PIN Citrix.
  - Valeurs possibles : entre **4** et **10**
  - Valeur par défaut : **6**

- **PASSCODE_STRENGTH**
  - Nom d'affichage : PIN Strength Requirement (Exigences en matière de sûreté du code PIN)
  - Cette propriété définit le niveau de sécurité du code PIN ou code secret Citrix. Lorsque vous modifiez ce paramètre, les utilisateurs sont invités à créer un code PIN ou code secret Citrix la prochaine fois qu'ils sont invités à s'authentifier.
  - Valeurs possibles : **Low**, **Medium**, **High** ou **Strong**
  - Valeur par défaut : **Medium**
  - Les règles de mot de passe pour chaque paramètre de sécurité en fonction du paramètre PASSCODE_TYPE sont les suivantes :

Règles pour code secret numérique :

Niveau de sécurité du code secret	Règles pour code secret numérique	Autorisé	Non autorisée
Faible	Sont autorisés tous les nombres et toute séquence	444444, 123456, 654321	
Medium (paramètre par défaut)	Ne doit contenir aucun chiffre consécutif ou répété.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
Élevé	Ne doit contenir aucun chiffre adjacent identique.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199

Niveau de sécurité du code secret	Règles pour code secret numérique	Autorisé	Non autorisée
Strong	N’utilisez pas le même chiffre plus de deux fois. N’utilisez pas trois chiffres consécutifs ou plus dans une ligne. N’utilisez pas trois chiffres consécutifs ou plus dans l’ordre inverse.	102983, 085085, 824673, 132312	132132, 131313, 902030

Règles pour code secret alphanumérique :

Niveau de sécurité du code secret	Règles pour code secret alphanumérique	Autorisé	Non autorisée
Faible	Doit contenir au moins un chiffre et une lettre.	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef
Medium (paramètre par défaut)	En plus des règles de sécurité pour un code secret de niveau moyen, les lettres et tous les chiffres ne peuvent pas être identiques. Les lettres et les nombres ne peuvent pas être consécutifs.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, ou aaa111 ; abcd12, bcd123, 123abc, xy1234, xyz345 ou cba123
Élevé	Utilisez au moins une lettre majuscule et une lettre minuscule.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2

Niveau de sécurité du code secret	Règles pour code secret alphanumérique	Autorisé	Non autorisée
Strong	Utilisez au moins un nombre, un symbole spécial, une lettre majuscule et une lettre minuscule.	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

- **PASSCODE_TYPE**
  - Nom d'affichage : PIN Type (Type de code PIN)
  - Cette propriété définit si les utilisateurs peuvent définir un code PIN Citrix numérique ou un code secret alphanumérique. Lorsque vous sélectionnez la valeur **Numeric**, les utilisateurs peuvent uniquement utiliser des chiffres (code PIN Citrix). Lorsque vous sélectionnez la valeur **Alphanumeric**, l'utilisateur peut utiliser une combinaison de lettres et de chiffres (code secret).

    Si vous modifiez ce paramètre, les utilisateurs doivent définir un nouveau code PIN ou code secret Citrix la prochaine fois qu'ils sont invités à s'authentifier.
  - Valeurs possibles : **Numeric** ou **Alphanumeric**
  - Valeur par défaut : **Numeric**
- **REFRESHINTERVAL**
  - Nom d'affichage : REFRESHINTERVAL
  - Par défaut, XenMobile envoie un ping au serveur de détection automatique (ADS) afin « d'épingler » les certificats tous les 3 jours. Pour modifier l'intervalle d'actualisation, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **REFRESHINTERVAL** et définissez la **valeur** sur le nombre d'heures.
  - Valeur par défaut : **72** heures (3 jours)
- **SEND_LDAP_ATTRIBUTES**
  - Pour les déploiements MAM exclusif d'appareils Android, iOS ou macOS, vous pouvez configurer XenMobile de manière à ce que les utilisateurs qui s'inscrivent dans Secure Hub avec des informations d'identification de messagerie soient automatiquement inscrits dans Secure Mail. Par conséquent, les utilisateurs ne fournissent pas d'informations supplémentaires et aucune étape supplémentaire n'est nécessaire pour s'inscrire dans Secure Mail.

- Pour configurer cette stratégie globale, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **SEND_LDAP_ATTRIBUTES** et définissez la **valeur** comme suit.
- Valeur : `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme =${ user.samaccountname } , displayName=${ user.displayName } ,mail =${ user.mail }`
- Les valeurs d'attribut sont spécifiées en tant que macros, similaires à des stratégies MDM.
- Voici un exemple de réponse de service de compte pour cette propriété :

```
<property value="userPrincipalName=user@site.com,sAMAccountName=
eng1,displayName=user\,test1,email=user@site.com\,user@site.com"
name="SEND_LDAP_ATTRIBUTES"/>
```

- Pour cette propriété, XenMobile traite les virgules en tant que terminaison de chaîne. Par conséquent, si une valeur d'attribut comprend une virgule, elle doit être précédée d'une barre oblique inverse. La barre oblique inverse empêche le client d'interpréter la virgule comme fin de la valeur d'attribut. Représentez les barres obliques inverses par `"\\"`.

- **HIDE_THREE_FINGER_TAP_MENU**
  - Lorsque cette propriété n'est pas définie ou est définie sur **false**, les utilisateurs peuvent accéder au menu des fonctionnalités masquées en effectuant un tapotement à trois doigts sur leurs appareils. Le menu des fonctions masquées permettait aux utilisateurs de réinitialiser les données de l'application. La définition de cette propriété sur **true** désactive l'accès des utilisateurs au menu des fonctionnalités masquées.
  - Pour configurer cette stratégie globale, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **HIDE_THREE_FINGER_TAP_MENU** et définissez la **valeur**.
- **TUNNEL_EXCLUDE_DOMAINS**
  - Nom d'affichage : Tunnel Exclude Domains
  - Par défaut, MDX exclut le tunnel micro VPN de certains points de terminaison de service que les applications et les kits de développement XenMobile utilisent pour différentes fonctionnalités. Par exemple, ces points de terminaison incluent les services qui ne requièrent pas le routage via les réseaux d'entreprise, tels que Google Analytics, les services Citrix Cloud et les services Active Directory. Utilisez cette propriété de client pour remplacer la liste des domaines exclus.
  - Pour configurer cette stratégie globale, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **TUNNEL_EXCLUDE_DOMAINS** et définissez la **valeur**.
  - Valeur : pour remplacer la liste par défaut avec les domaines que vous souhaitez exclure du tunneling, tapez une liste séparée par des virgules des suffixes de domaine. Pour inclure tous les domaines dans le tunneling, entrez **none**. La valeur par défaut est :


```
app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test
.citrix.com,clientstream,launchdarkly.com,crashlytics.com,events.
launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net
,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf
-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,
stream.launchdarkly.com
```

Déployer des appareils via le programme de déploiement d'Apple

January 10, 2022

Apple propose des programmes d'inscription d'appareil pour les comptes d'entreprise et éducation. Pour les comptes d'entreprise, vous devez vous inscrire au programme de déploiement d'Apple pour utiliser le programme Apple Business Manager (ABM) ou Apple School Manager (ASM) pour inscrire et gérer des appareils dans XenMobile. Ce programme est pour les appareils iOS, iPadOS et macOS.

Le programme Apple Deployment Program est mis à la disposition des organisations mais pas des individus. Vous devez fournir une quantité considérable d'informations et de détails sur l'entreprise pour créer un compte Apple Deployment Program. Par conséquent, la demande et l'obtention de l'approbation peuvent prendre du temps.

Pour les comptes éducation, vous devez créer un compte Apple School Manager. ASM unifie le programme de déploiement d'Apple et l'achat en volume d'Apple. Pour créer un compte Apple School Manager, accédez au site Apple School.

S'inscrire au programme de déploiement d'Apple

Pour vous inscrire à Apple Business Manager, accédez à business.apple.com. Cliquez sur **S'inscrire maintenant** pour demander un nouveau compte. Il est recommandé d'utiliser une adresse e-mail pour votre organisation, par exemple deployment@company.com. Le processus d'inscription peut prendre quelques jours. Après avoir reçu vos informations d'identification d'ouverture de session, suivez les étapes fournies dans Apple Business Manager pour créer un compte.

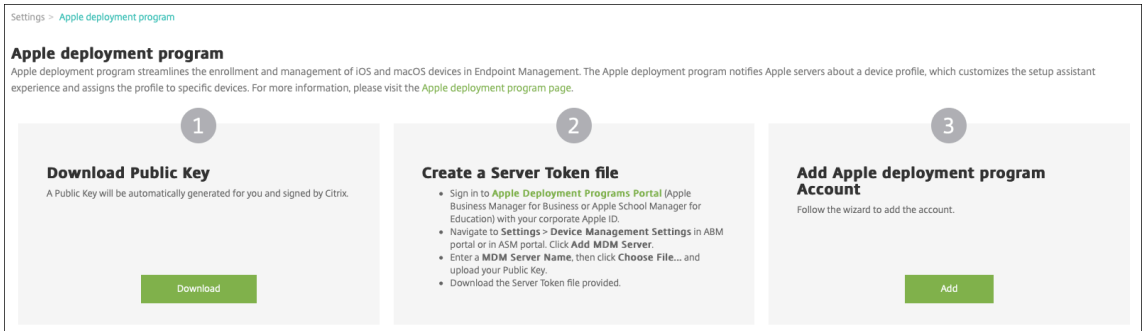
> **Remarque :**
>
> Pour les comptes éducation, consultez la section Intégration aux fonctionnalités Apple Éducation.

Connecter votre compte Apple Business Manager à XenMobile

Pour connecter votre compte Apple Business Manager à votre déploiement XenMobile, entrez les informations dans la console XenMobile et Apple Business Manager. Procédez comme suit :

Étape 1 : Télécharger une clé publique depuis votre serveur XenMobile

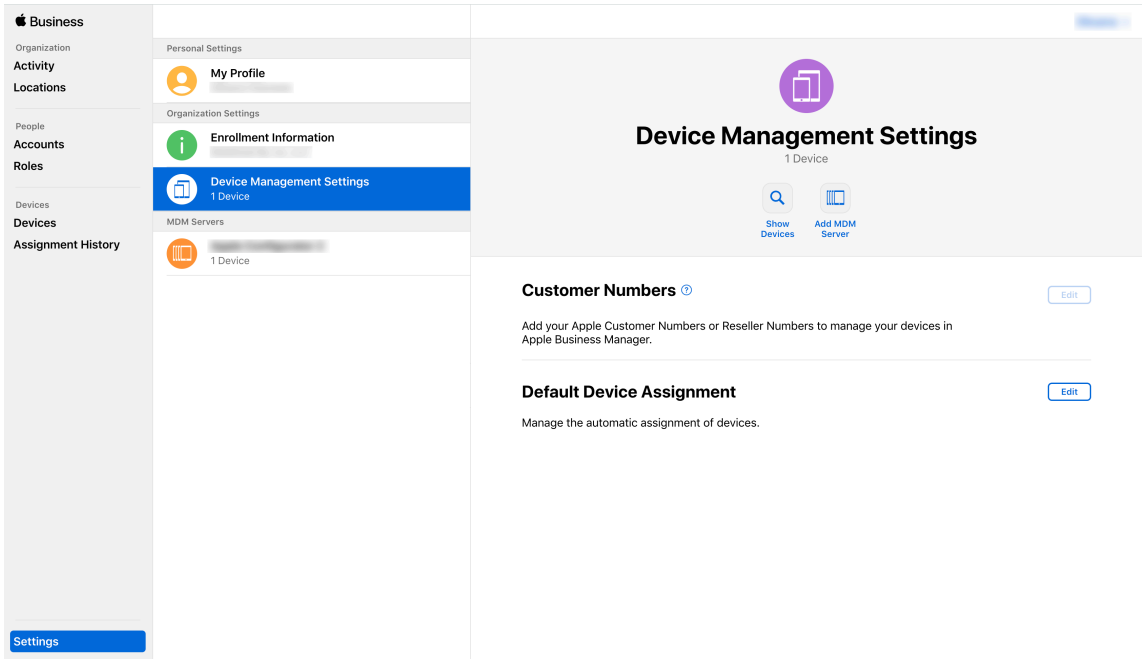
1. Dans la console XenMobile, accédez à **Paramètres > Programme de déploiement d'Apple**.



2. Sous **Télécharger la clé publique**, cliquez sur **Télécharger**.

Étape 2 : Créer et télécharger un fichier de jeton de serveur depuis votre compte Apple

1. Connectez-vous à Apple Business Manager avec un compte disposant du rôle Administrateur ou Gestionnaire d'inscription des appareils.
2. En bas de la barre latérale, cliquez sur **Réglages**, puis cliquez sur **Réglages de gestion des appareils > Ajouter un serveur MDM**.



3. Dans le paramètre **Nom du serveur MDM**, donnez un nom au serveur XenMobile. Le nom du serveur que vous tapez est à titre de référence. Il ne s'agit pas de l'URL ou du nom du serveur.
4. Sous **Charger la clé publique**, cliquez sur **Choisir un fichier**. Chargez la clé publique que vous avez téléchargée depuis XenMobile, puis enregistrez les modifications.

5. Cliquez sur **Télécharger le jeton** pour télécharger le fichier de jeton de serveur sur votre ordinateur.

   Vous devez charger le fichier de jeton de serveur lors de l'ajout du compte ABM à XenMobile. Les informations de votre jeton ABM s'affichent dans la console XenMobile après l'importation du fichier de jeton.

6. Sous **Attribution d'appareils par défaut**, cliquez sur **Modifier**. Choisissez la manière dont vous souhaitez attribuer les appareils et fournissez les informations requises. Pour de plus amples informations, consultez le Guide de l'utilisateur d'ABM.

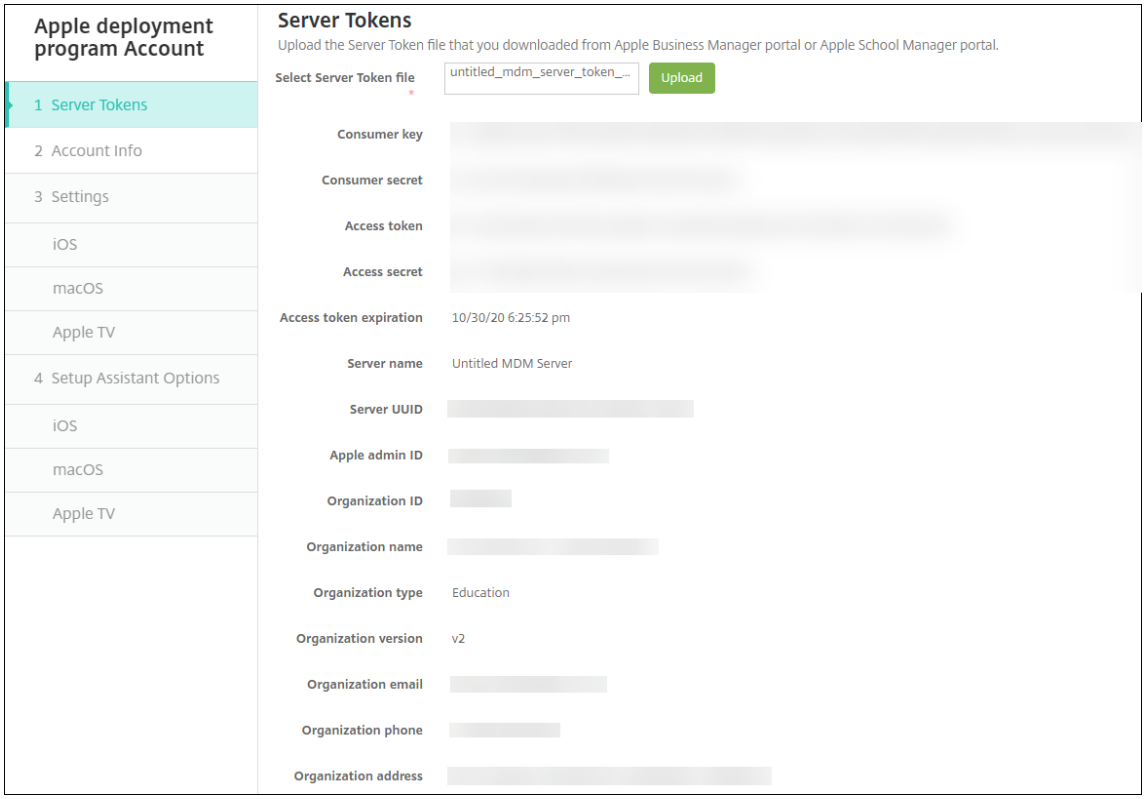
Étape 3 : Ajouter un compte ABM à XenMobile

Vous pouvez ajouter plusieurs comptes ABM à XenMobile. Cette fonctionnalité vous permet d'utiliser différents paramètres d'inscription ainsi que les options de l'Assistant d'installation par pays, département, etc. Vous pouvez associer des comptes ABM à différentes stratégies.

À titre d'exemple, vous pouvez centraliser tous vos comptes ABM provenant de pays différents sur le même serveur XenMobile, de façon à pouvoir importer et surveiller tous les appareils ABM. En personnalisant les paramètres d'inscription et les options de l'Assistant d'installation par département, hiérarchie organisationnelle ou une autre structure, les stratégies fournissent les fonctionnalités appropriées à votre organisation et les utilisateurs reçoivent une aide à l'installation adaptée.

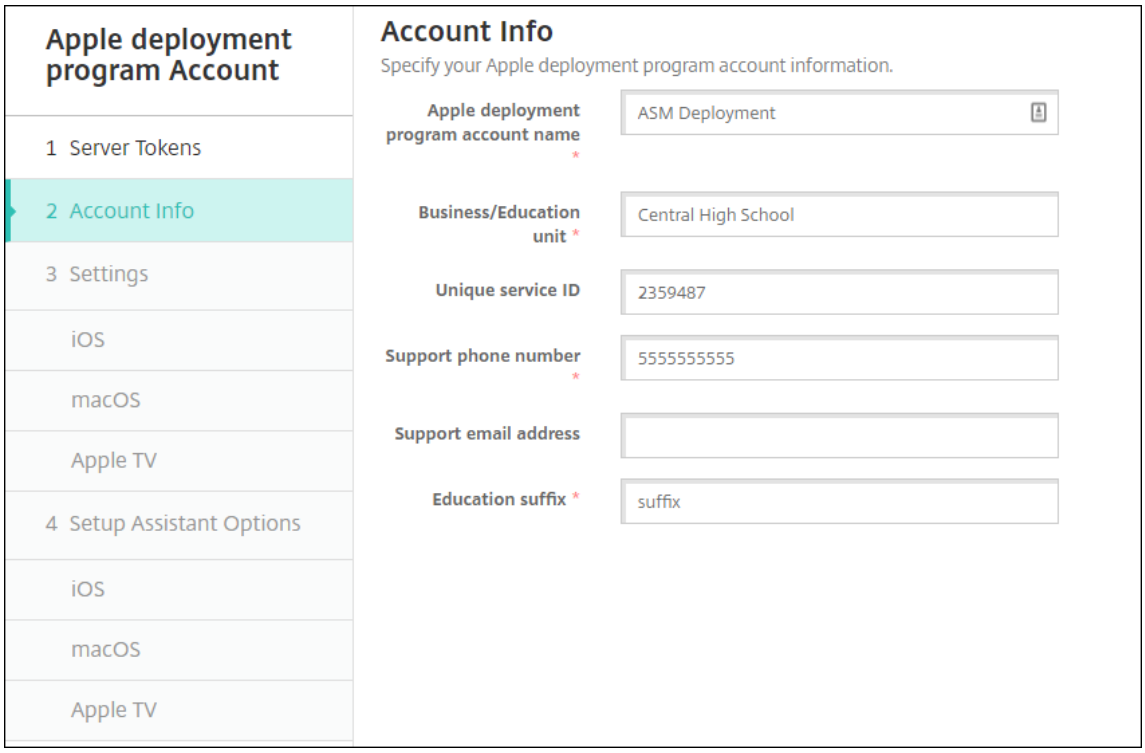
1. Dans la console XenMobile accédez à **Paramètres > Programme de déploiement d'Apple** et sous **Ajouter un compte de programme de déploiement Apple**, cliquez sur **Ajouter** .

2. Sur la page **Jetons de serveur**, spécifiez votre fichier de jeton de serveur, puis cliquez sur **Charger**.



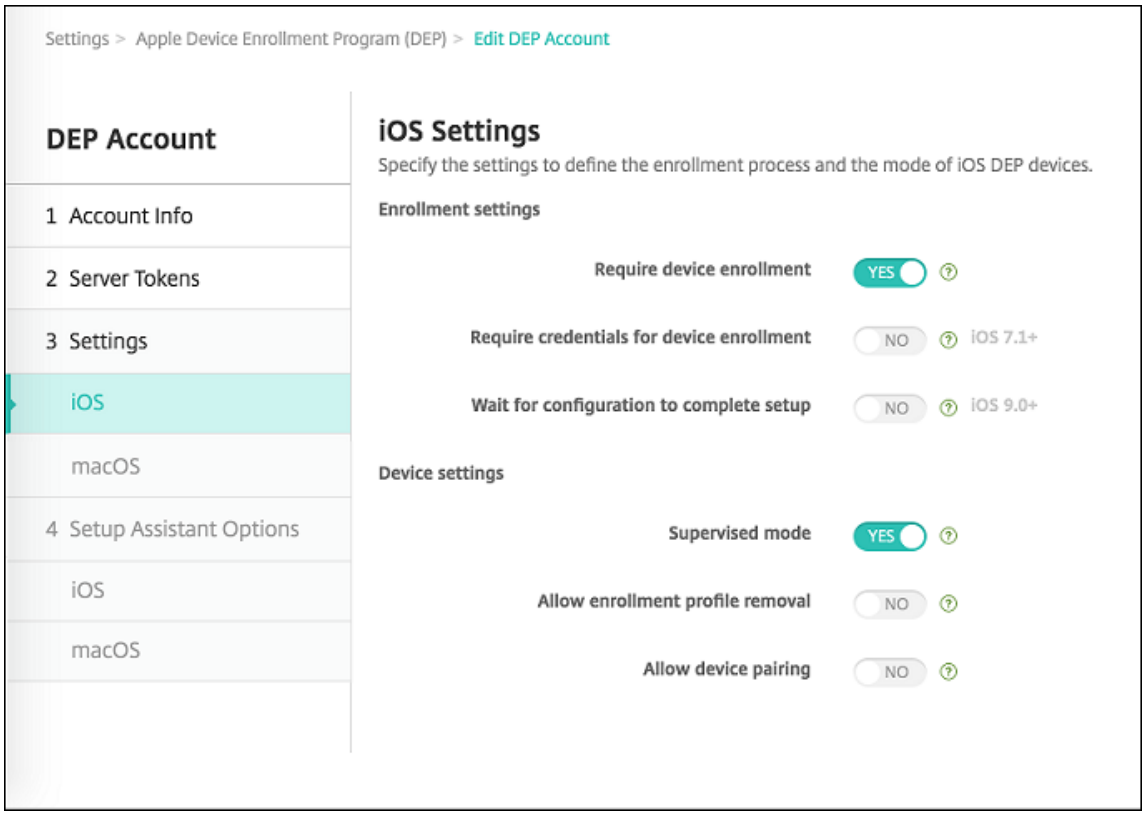
Vos informations de jeton de serveur s'affichent.

3. Sur la page **Infos sur le compte**, spécifiez ces paramètres :



- **Nom du compte du programme de déploiement Apple :** nom unique pour ce compte du programme de déploiement d'Apple. Utilisez des noms qui reflètent la manière dont vous organisez les comptes du programme de déploiement d'Apple, par pays ou hiérarchie organisationnelle par exemple.
- **Division/Département** : division ou département auquel l'appareil est attribué. Ce champ est obligatoire.
- **ID de service unique :** ID unique (facultatif) pour vous aider à identifier le compte.
- **Numéro de téléphone de l'assistance :** numéro de téléphone d'assistance que les utilisateurs peuvent appeler pour obtenir de l'aide au cours de la configuration. Ce champ est obligatoire.
- **Adresse e-mail de l'assistance :** adresse e-mail d'assistance (facultatif) que peuvent utiliser les utilisateurs.

4. Dans **Paramètres iOS**, spécifiez les paramètres suivants :



Paramètres d'inscription :

- **Exiger l'inscription des appareils :** sélectionnez cette option pour obliger les utilisateurs à inscrire leurs appareils. La valeur par défaut est **Oui**.
- **Exiger des informations d'identification pour l'inscription de l'appareil :** indiquez si vous souhaitez demander aux utilisateurs d'entrer leurs informations d'identification lors de la configuration d'ABM. Citrix recommande de demander à tous les utilisateurs

d'entrer leurs informations d'identification lors de l'inscription de l'appareil, afin de limiter l'inscription des appareils aux utilisateurs autorisés. La valeur par défaut est **Oui**.

Lorsque vous activez ABM avant la première configuration et que vous ne sélectionnez pas cette option, XenMobile crée les composants ABM. Cette création inclut des composants tels que l'utilisateur ABM, Secure Hub, l'inventaire logiciel et le groupe de déploiement ABM. Si vous sélectionnez cette option, XenMobile ne crée pas les composants. Par conséquent, si vous désactivez cette option ultérieurement, les utilisateurs qui n'ont pas entré leurs informations d'identification ne peuvent pas s'inscrire à ABM, car ces composants ABM n'existent pas. Pour ajouter les composants ABM, dans ce cas, désactivez, puis activez le compte ABM.

- **Attendre la fin de l'installation :** indiquez si les appareils des utilisateurs doivent rester dans le mode Assistant d'installation jusqu'à ce que toutes les ressources MDM soient déployées sur l'appareil. Ce paramètre est disponible sur les appareils en mode supervisé. La valeur par défaut est **Non**.
- La documentation Apple indique que les commandes suivantes peuvent ne pas fonctionner lorsqu'un appareil est en mode Assistant d'installation :
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

Paramètres de l'appareil :

- **Mode supervisé :** doit être défini sur **Oui** si vous utilisez Apple Configurator pour gérer les appareils inscrits à ABM ou lorsque l'option **Attendre la fin de l'installation** est activée. La valeur par défaut est **Oui**. Pour de plus amples informations sur le placement d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.
- **Autoriser suppression du profil d'inscription :** indiquez si vous souhaitez autoriser les appareils à utiliser un profil que vous pouvez supprimer à distance. La valeur par défaut est **Non**.
- **Autoriser le couplage de l'appareil :** pour les appareils inscrits par le biais d'ABM, sélectionnez cette option pour pouvoir les gérer via Apple Music et Apple Configurator. La valeur par défaut est **Non**.

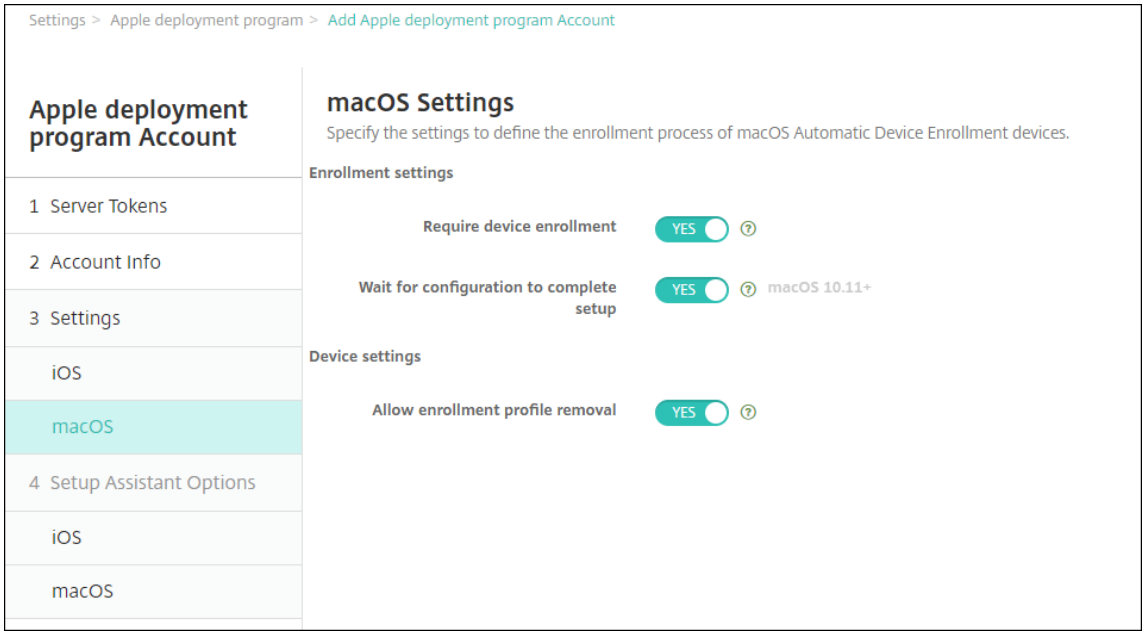
Identités de supervision

Si vous utilisez l'outil GroundControl, vous pouvez ajouter un certificat pour effectuer les opérations suivantes :

- Ignorez les restrictions liées au couplage pour éviter l'invite « Approuver cet hôte ».
- Faites passer les actions des appareils gérés via USB pour effectuer des activités telles que l'installation de profils sans interaction de l'utilisateur. Cela permet à GroundControl d'activer le mode d'application unique et le verrouillage de l'appareil pour l'extraction.
- Restaurez une sauvegarde sur les appareils ABM.

Pour plus d'informations sur GroundControl, consultez le site Web de GroundControl.

5. Dans **Paramètres macOS**, spécifiez les paramètres suivants :



Paramètres d'inscription :

- **Exiger l'inscription des appareils :** sélectionnez cette option pour obliger les utilisateurs à inscrire leurs appareils. La valeur par défaut est **Oui**.
- **Attendre la fin de l'installation :** si **Oui** est sélectionné, l'appareil macOS interrompt l'Assistant d'installation jusqu'à ce que le code secret des ressources MDM soit déployé sur l'appareil. Ce déploiement se produit avant la création du compte local. Ce paramètre est disponible pour macOS 10.11 et versions ultérieures. La valeur par défaut est **Non**.

Paramètres de l'appareil :

- **Autoriser suppression du profil d'inscription :** indiquez si vous souhaitez autoriser les appareils à utiliser un profil que vous pouvez supprimer à distance. La valeur par défaut est **Non**.

6. Dans **Options de l'assistant d'installation iOS**, sélectionnez les étapes que l'Assistant d'installation iOS peut ignorer lorsque les utilisateurs démarrent leurs appareils pour la première fois. Lorsqu'un écran est ignoré, la fonctionnalité associée utilise les paramètres par défaut. Les utilisateurs peuvent configurer les fonctionnalités ignorées une fois l'installation ter-

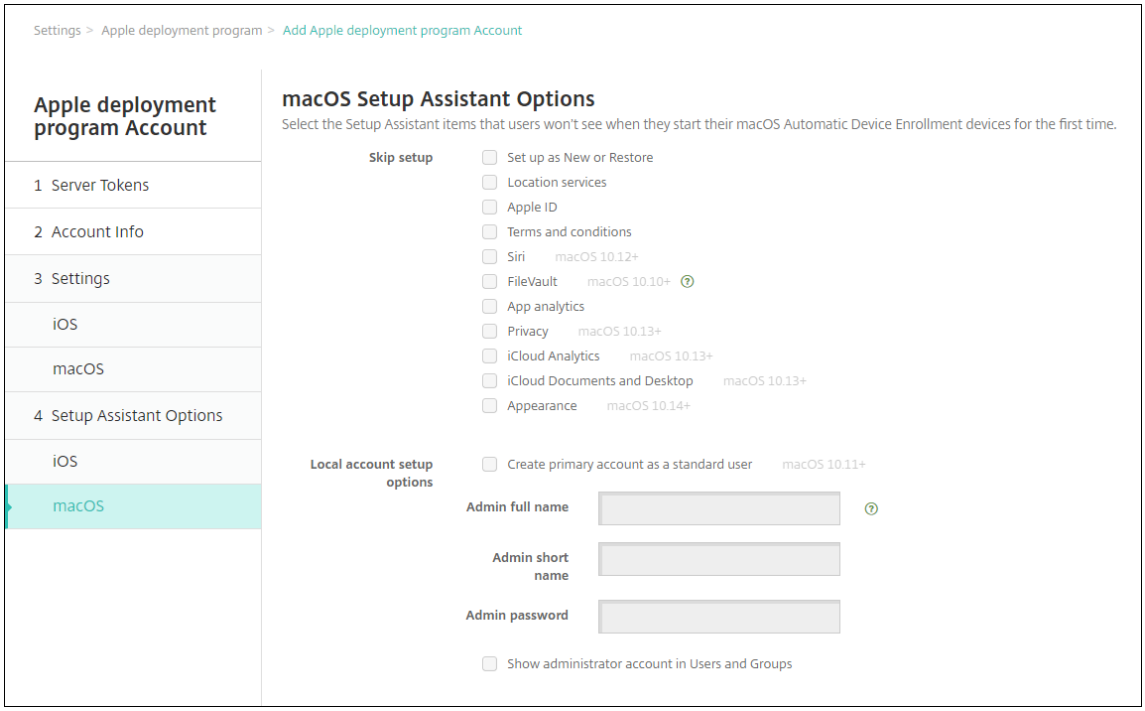
minée, sauf si vous limitez complètement l'accès à ces fonctionnalités. Pour plus d'informations sur la restriction de l'accès aux fonctionnalités, consultez la section Stratégie de restrictions. Par défaut, tous les éléments sont désactivés. Les descriptions suivantes expliquent ce qui se produit lorsqu'un paramètre est sélectionné.

- **Services de localisation :** empêche les utilisateurs de configurer le service de localisation sur l'appareil.
- **Touch ID :** empêche les utilisateurs de configurer Touch ID ou Face ID sur les appareils iOS.
- **Verrouillage par code secret :** empêche les utilisateurs de configurer un code secret pour l'appareil. Si aucun code secret n'existe, les utilisateurs ne peuvent pas utiliser Touch ID ou Apple Pay.
- **Définir comme nouveau ou restaurer :** empêche les utilisateurs de configurer l'appareil comme nouveau ou de le restaurer à partir d'une sauvegarde de l'Apple App Store ou d'iCloud.
- **Déplacer depuis Android :** empêche les utilisateurs de transférer des données à partir d'un appareil Android vers un appareil iOS. Cette option est disponible uniquement lorsque **Définir comme nouveau ou restaurer** est sélectionné (sinon, cette étape est ignorée).
- **Apple ID :** empêche les utilisateurs de configurer un compte Apple ID géré pour l'appareil.
- **Termes et conditions :** empêche les utilisateurs de lire et d'accepter les termes et conditions d'utilisation de l'appareil.
- **Apple Pay :** empêche les utilisateurs de configurer Apple Pay. Si ce paramètre est désactivé, les utilisateurs doivent configurer Touch ID et Apple ID. Assurez-vous que ces paramètres sont effacés.
- **Siri :** empêche les utilisateurs de configurer Siri.
- **Analyse de l'application :** empêche les utilisateurs de configurer le partage des données d'incidents et des statistiques d'utilisation avec Apple.

- **Zoom d'affichage :** empêche les utilisateurs de définir la résolution d'affichage (standard ou zoom) sur les appareils iOS.
- **True Tone :** empêche les utilisateurs de configurer des capteurs à quatre canaux pour régler dynamiquement la balance des blancs de l'affichage.
- **Bouton d'accueil :** empêche les utilisateurs de configurer le style du bouton d'accueil des commentaires.
- **Présentation des nouvelles fonctionnalités :** empêche les utilisateurs d'afficher des écrans qui incluent des informations sur les nouvelles fonctionnalités du logiciel Apple.
- **Confidentialité :** empêche les utilisateurs d'afficher le panneau de données et de confidentialité. Pour iOS 11.3 et versions ultérieures.
- **Mise à jour logicielle :** empêche les utilisateurs de mettre à jour iOS vers la dernière version. Pour iOS 12.0 et versions ultérieures.
- **Screen Time :** empêche les utilisateurs d'activer la fonction Screen Time. Pour iOS 12.0 et versions ultérieures.
- **Configuration de la carte SIM :** empêche les utilisateurs de configurer un forfait de données mobiles. Pour iOS 12.0 et versions ultérieures.
- **iMessage & FaceTime :** empêche les utilisateurs d'activer iMessage et FaceTime. Pour iOS 12.0 et versions ultérieures.
- **Apparence :** empêche les utilisateurs de sélectionner le mode d'apparence. Pour iOS 13.0 et versions ultérieures.
- **Bienvenue :** empêche l'utilisateur d'afficher l'écran **Mise en route**. Pour iOS 13.0 et versions ultérieures.
- **Restauration terminée :** empêche les utilisateurs de voir si une restauration est terminée pendant l'installation. Pour iOS 14.0 et versions ultérieures.
- **Mise à jour terminée :** empêche les utilisateurs de voir si une mise à jour logicielle est terminée pendant l'installation. Pour iOS 14.0 et versions ultérieures.

Le compte ABM apparaît dans **Paramètres > Programme de déploiement d'Apple**.

7. Dans **Options de l'assistant d'installation macOS**, sélectionnez les étapes que l'Assistant d'installation macOS peut ignorer lorsque les utilisateurs démarrent leurs appareils pour la première fois. Lorsqu'un écran est ignoré, la fonctionnalité associée utilise les paramètres par défaut. Les utilisateurs peuvent configurer les fonctionnalités ignorées une fois l'installation terminée, sauf si vous limitez complètement l'accès à ces fonctionnalités. Pour plus d'informations sur la restriction de l'accès aux fonctionnalités, consultez la section Stratégie de restrictions. Par défaut, tous les éléments sont désactivés. Les descriptions suivantes expliquent ce qui se produit lorsqu'un paramètre est sélectionné.



- **Définir comme nouveau ou restaurer :** empêche les utilisateurs de configurer l'appareil comme nouveau ou à partir d'une sauvegarde Time Machine ou d'effectuer une migration système.
- **Services de localisation :** empêche les utilisateurs de configurer le service de localisation sur l'appareil. Pour macOS 10.11 et versions ultérieures.
- **Apple ID :** empêche les utilisateurs de configurer un compte Apple ID géré pour l'appareil.
- **Termes et conditions :** empêche les utilisateurs de lire et d'accepter les termes et conditions d'utilisation de l'appareil.
- **Siri :** empêche les utilisateurs de configurer Siri. Pour macOS 10.12 et versions ultérieures.
- **FileVault :** utilisez FileVault pour crypter le disque de démarrage. XenMobile applique le paramètre FileVault uniquement si le système dispose d'un seul compte utilisateur local et que ce compte est connecté à iCloud.

  Vous pouvez utiliser la fonctionnalité de cryptage de disque FileVault de macOS pour protéger le volume système en cryptant son contenu (https://support.apple.com/en-us/HT204837). Si vous exécutez l'Assistant d'installation sur un Mac portable de modèle récent sur lequel FileVault n'est pas activé, vous pourrez être invité à activer cette fonctionnalité. L'invite s'affiche sur les nouveaux systèmes et les systèmes mis à niveau vers OS X 10.10 ou 10.11, mais uniquement si le système dispose d'un compte d'administrateur local unique et que ce compte est connecté à iCloud.
- **Analyse de l'application :** empêche les utilisateurs de configurer le partage des données

d'incidents et des statistiques d'utilisation avec Apple.

- **Confidentialité :** empêche les utilisateurs d'afficher le panneau de données et de confidentialité. Pour macOS 10.13 et versions ultérieures.
- **Analyse d'iCloud :** empêche les utilisateurs de choisir d'envoyer des données iCloud de diagnostic à Apple. Pour macOS 10.13 et versions ultérieures.
- **Bureau et documents iCloud :** empêche les utilisateurs de configurer le bureau et les documents iCloud. Pour macOS 10.13 et versions ultérieures.
- **Apparence :** empêche les utilisateurs de sélectionner le mode d'apparence. Pour macOS 10.14 et versions ultérieures.
- **Accessibilité :** empêche les utilisateurs d'entendre la fonctionnalité VoiceOver automatiquement. Disponible uniquement si l'appareil est connecté à Ethernet. Pour macOS 11 et versions ultérieures.
- **Biométrie :** empêche l'utilisateur de configurer Touch ID et Face ID. Pour macOS 10.12.4 et versions ultérieures.
- **True Tone :** empêche les utilisateurs de configurer des capteurs à quatre canaux pour régler dynamiquement la balance des blancs de l'affichage. Pour macOS 10.13.6 et versions ultérieures.
- **Apple Pay :** empêche les utilisateurs de configurer Apple Pay. Si ce paramètre est désactivé, les utilisateurs doivent configurer Touch ID et Apple ID. Assurez-vous que les paramètres **Apple ID** et **Biométrie** sont effacés. Pour macOS 10.12.4 et versions ultérieures.
- **Screen Time :** empêche les utilisateurs d'activer la fonction Screen Time. Pour macOS 10.15 et versions ultérieures.
- **Options de configuration du compte local :** spécifiez les paramètres pour créer un compte administrateur sur l'appareil. Les utilisateurs se connectent à leur appareil macOS à l'aide de ces informations. XenMobile crée le compte, à l'aide des informations spécifiées.
  - **Créer un compte principal en tant qu'utilisateur standard :** au lieu d'accorder à l'utilisateur des privilèges d'administrateur sur l'appareil, XenMobile donne à l'utilisateur des autorisations standard. macOS ayant besoin d'un compte administrateur, XenMobile crée d'abord un compte administrateur, puis crée un nouveau compte standard et le définit comme compte principal.
  - **Nom complet de l'administrateur :** saisissez le nom que le système affiche pour le compte administrateur.
  - **Nom court de l'administrateur :** saisissez le nom que l'appareil affiche pour le dossier de base et dans le shell.

- **Mot de passe de l'administrateur :** saisissez un mot de passe sécurisé pour le compte administrateur.
- **Afficher le compte administrateur dans Utilisateurs et groupes :** si cette option n'est pas cochée, le compte administrateur n'apparaît pas dans **Utilisateurs et groupes** dans les paramètres macOS. Si vous créez le compte principal en tant qu'utilisateur standard, activez ce paramètre pour masquer le compte administrateur créé par XenMobile.

Commander des appareils compatibles avec le programme de déploiement

Vous pouvez commander des appareils compatibles avec le programme de déploiement directement auprès d'Apple ou de revendeurs ou d'opérateurs agrées. Pour commander auprès d'Apple, entrez votre ID de client Apple dans le portail du programme de déploiement d'Apple. Votre ID de client permet à Apple d'associer vos appareils achetés à votre compte du programme de déploiement d'Apple.

Pour commander auprès de votre revendeur ou d'un opérateur, contactez-le pour savoir s'il participe au programme de déploiement d'Apple. Lorsque vous achetez des appareils, demandez l'ID du programme de déploiement d'Apple du revendeur. Apple requiert ces informations lorsque vous ajoutez votre revendeur du programme de déploiement d'Apple à votre compte du programme de déploiement d'Apple. Après avoir ajouté l'ID du programme de déploiement d'Apple pour le revendeur, vous recevez un ID client du programme de déploiement. Fournissez cet ID au revendeur, qui l'utilisera pour soumettre les informations sur les appareils que vous avez achetés à Apple. Pour plus d'informations, consultez le site d'inscription des appareils Apple.

Gérer les appareils compatibles avec le programme de déploiement

Une fois votre commande expédiée, vous pouvez associer des appareils iOS, iPadOS et macOS à votre serveur XenMobile.

1. Connectez-vous à Apple Business Manager avec un compte disposant du rôle Administrateur ou Gestionnaire d'inscription des appareils.
2. Dans la barre latérale, cliquez sur **Appareils**. Les appareils que vous avez achetés directement auprès d'Apple apparaissent automatiquement. Pour attribuer des appareils depuis Apple Configurator 2 vers Apple Business Manager, consultez le Guide de l'utilisateur d'Apple Business Manager.
3. Dans la liste, sélectionnez un appareil ou le nombre total d'appareils et cliquez sur **Modifier la gestion des appareils**. Deux options sont disponibles :
   - Pour attribuer un appareil à un serveur MDM, sous **Attribuer à un serveur**, choisissez le nom de votre serveur XenMobile. Cliquez sur **Continuer**.
     Pour attribuer de nouveaux appareils à Apple Business Manager en bloc, définissez un serveur XenMobile par défaut pour le déploiement. Pour plus d'informations, consultez

Définir un serveur par défaut pour l'inscription en bloc.

- Pour annuler l'attribution d'un appareil au serveur XenMobile, choisissez **Retirer**.

Vos appareils du programme de déploiement d'Apple sont maintenant associés au serveur XenMobile sélectionné.

Si vous envoyez un appareil iOS, iPadOS ou macOS à des fins de maintenance, vous devez supprimer l'appareil d'Apple Business Manager. Lorsque vous recevez l'appareil réparé, vous devez réattribuer l'appareil au serveur XenMobile. Lorsque vous remplacez l'appareil, vous pouvez attribuer un nouvel appareil au serveur XenMobile à l'aide d'un numéro de commande.

Pour consulter l'historique des appareils attribués, procédez comme suit :

1. Connectez-vous à Apple Business Manager avec un compte disposant du rôle Administrateur ou Gestionnaire d'inscription des appareils.
2. Dans la barre latérale, cliquez sur **Historique des attributions**. Choisissez ensuite une attribution pour afficher plus d'informations.
3. Cliquez sur **Télécharger** pour télécharger un fichier CSV contenant les numéros de série de tous les appareils attribués et non attribués.

Vous pouvez supprimer les appareils iOS, iPadOS et macOS d'Apple Business Manager si l'appareil a été vendu, volé ou ne peut pas être réparé.

1. Connectez-vous à Apple Business Manager avec un compte disposant du rôle Administrateur ou Gestionnaire d'inscription des appareils.
2. Dans la barre latérale, cliquez sur **Appareils** et recherchez un appareil.
3. Sélectionnez un appareil et cliquez sur **Révoquer des appareils**. Dans la boîte de dialogue, confirmez vos modifications pour supprimer l'appareil du programme. Pour ajouter à nouveau des appareils iOS et iPadOS, utilisez Apple Configurator 2. Vous ne pouvez pas ajouter de nouveaux appareils macOS avec Apple Configurator 2.

Inscrire des appareils

January 10, 2022

Pour gérer les appareils utilisateur à distance et de manière sécurisée, vous devez inscrire les appareils dans XenMobile. Le logiciel client XenMobile est installé sur l'appareil utilisateur et l'identité de l'utilisateur est authentifiée. Ensuite, XenMobile et le profil utilisateur sont installés. Vous pouvez ensuite effectuer les tâches de gestion dans la console XenMobile. Vous pouvez appliquer des stratégies, déployer des applications, envoyer des données sur l'appareil et verrouiller, effacer et localiser des appareils perdus ou volés.

L'inscription d'Azure Active Directory est prise en charge pour les appareils iOS, Android, Windows 10 et Windows 11. Pour plus d'informations sur la configuration d'Azure comme fournisseur d'identité

(IDP), veuillez consulter la section Intégration dans XenMobile d'Azure Active Directory en tant que fournisseur d'identité.

> **Remarque :**
>
> Avant de pouvoir inscrire des utilisateurs d'appareils iOS, vous devez demander un certificat APNS. Pour plus d'informations, consultez la section Certificats et authentification.

Pour mettre à jour les options de configuration pour les utilisateurs et les appareils, accédez à la page **Gérer > Invitations d'inscription**. Pour de plus amples informations, consultez la section Envoyer une invitation d'inscription dans cet article.

Appareils Android

> **Remarque :**
>
> Pour plus d'informations sur l'inscription d'appareils Android Enterprise, consultez la section Android Enterprise.

1. Accédez au magasin Google Play sur votre Android et téléchargez l'application Citrix Secure Hub, puis touchez l'application.
2. Lorsque vous êtes invité à installer l'application, cliquez sur **Suivant**, puis cliquez sur **Installer**.
3. Après l'installation de Secure Hub, touchez **Ouvrir**.
4. Entrez vos informations d'identification d'entreprise, telles que le nom de votre instance de XenMobile Server, le nom d'utilisateur principal (UPN), ou votre adresse e-mail. Cliquez ensuite sur **Suivant**.
5. Dans la boîte de dialogue **Activer l'administrateur de l'appareil**, touchez **Activer**.
6. Entrez votre mot de passe d'entreprise, puis touchez **Se connecter**.
7. En fonction de la manière dont XenMobile est configuré, vous pouvez être invité à créer un code PIN Citrix. Vous pouvez utiliser le code PIN pour vous connecter à Secure Hub et à d'autres applications XenMobile, telles que Secure Mail et Citrix Files. Vous devez entrer votre code PIN Citrix deux fois. Sur l'écran **Créer un code PIN Citrix**, entrez un code PIN.
8. Entrez de nouveau le code PIN. Secure Hub s'affiche. Vous pouvez ensuite accéder à XenMobile Store pour afficher les applications que vous pouvez installer sur votre appareil Android.
9. Si vous avez configuré XenMobile pour distribuer automatiquement des applications sur les appareils après l'inscription, les utilisateurs sont invités à installer les applications. En outre, les stratégies que vous configurez dans XenMobile sont déployées sur l'appareil. Cliquez sur **Installer** pour installer les applications.

Pour désinscrire et réinscrire un appareil Android

Les utilisateurs peuvent se désinscrire depuis Secure Hub. Lorsque les utilisateurs se désinscrivent à l'aide de la procédure suivante, l'appareil s'affiche toujours dans l'inventaire d'appareils dans la con-

sole XenMobile. Cependant, vous ne pouvez pas effectuer d'actions sur l'appareil. Vous ne pouvez pas suivre l'appareil ni contrôler sa conformité.

1. Touchez pour ouvrir l'application Secure Hub.
2. Selon que vous possédez une tablette ou un téléphone, procédez comme suit :

   Sur un téléphone :

   - Balayez l'écran à partir de la gauche pour ouvrir un panneau de paramètres.
   - Touchez **Préférences**, **Comptes**, puis touchez **Supprimer le compte**.

   Sur une tablette :

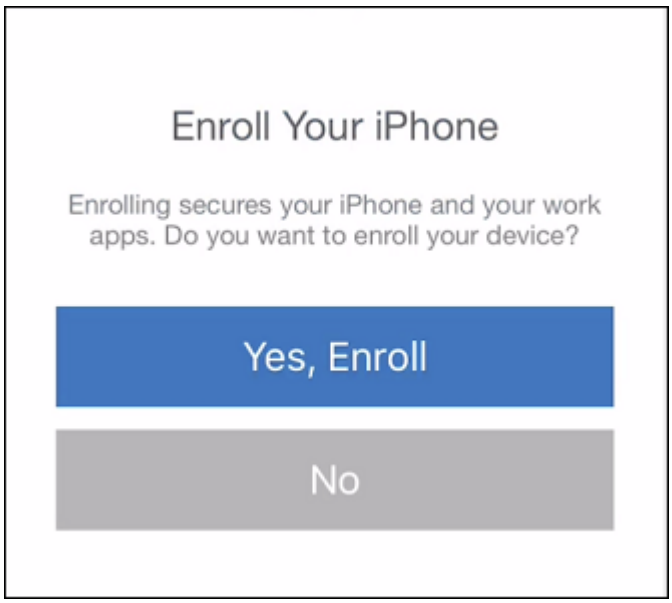
   - Touchez la flèche en regard de votre adresse e-mail sur le coin supérieur droit.
   - Touchez **Préférences**, **Comptes**, puis touchez **Supprimer le compte**.
3. Touchez **Réinscription**. Un message s'affiche afin de confirmer que vous souhaitez réinscrire votre appareil.
4. Touchez **OK**.

   Votre appareil est désinscrit.
5. Suivez les instructions à l'écran pour réinscrire votre appareil.

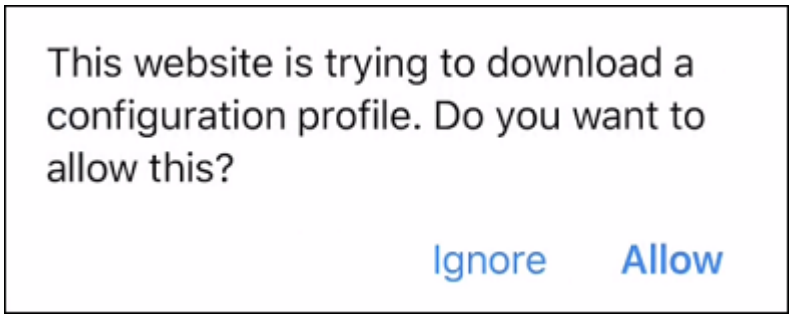
Inscrire des appareils iOS

Cette section explique comment les utilisateurs inscrivent des appareils iOS (12.2 ou version ultérieure) dans XenMobile Server. Pour plus d'informations sur l'inscription iOS, ouvrez la vidéo suivante :

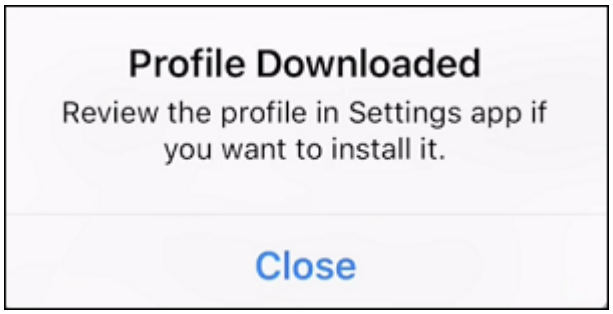
1. Accédez à l'Apple Store sur votre appareil iOS, téléchargez l'application Citrix Secure Hub, puis touchez l'application.
2. Lorsque vous êtes invité à installer l'application, touchez **Suivant**, puis **Installer**.
3. Après l'installation de Secure Hub, touchez **Ouvrir**.
4. Entrez vos informations d'identification d'entreprise, telles que le nom de votre instance de XenMobile Server, le nom d'utilisateur principal (UPN), ou votre adresse e-mail. Cliquez ensuite sur **Suivant**.
5. Touchez **Oui, inscrire** pour inscrire votre appareil iOS.



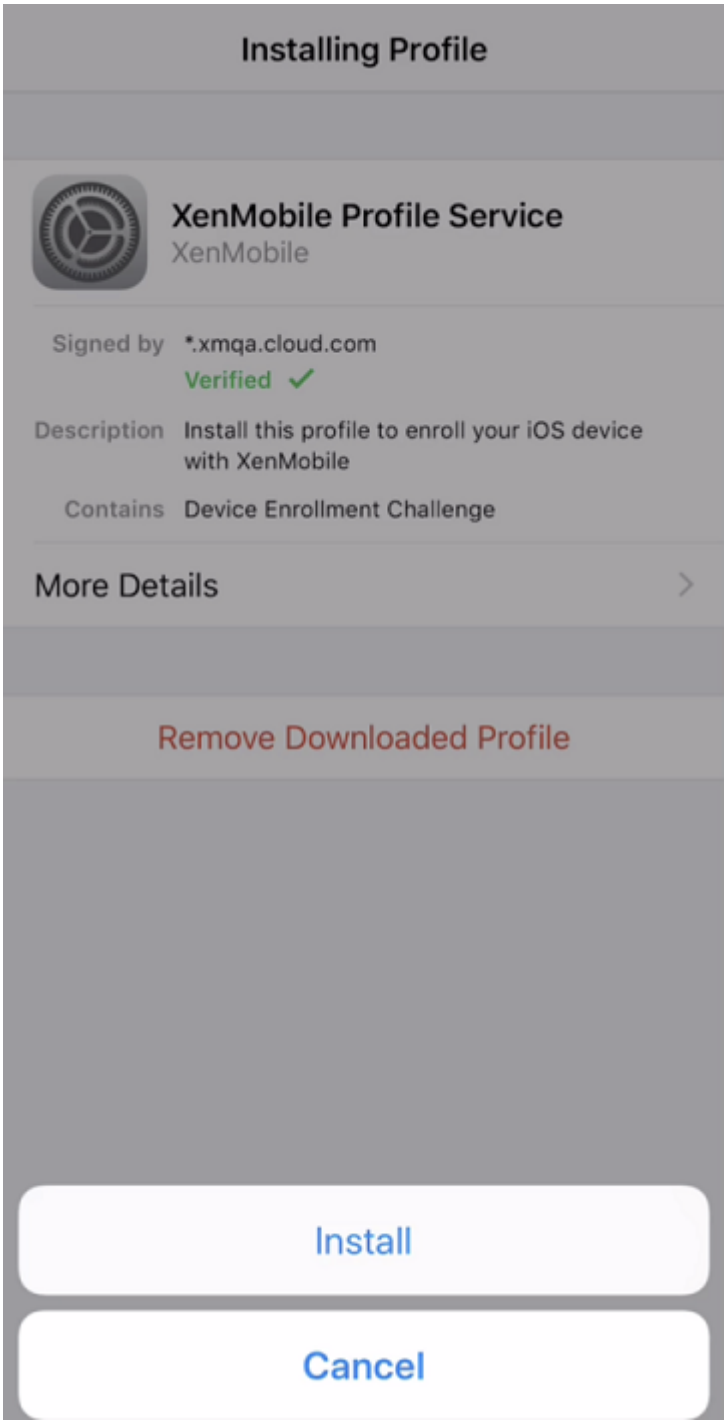
6. Après avoir tapé vos informations d'identification, appuyez sur **Autoriser** lorsque vous y êtes invité, pour télécharger le profil de configuration.



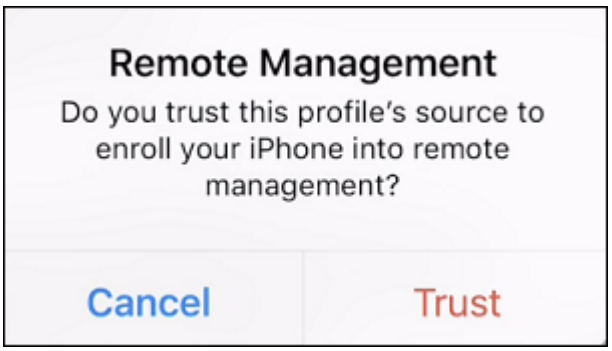
7. Après avoir téléchargé le profil de configuration, appuyez sur **Fermer**.



8. Dans les paramètres de votre appareil, installez le certificat iOS et ajoutez l'appareil à la liste de confiance.
    - Accédez à **Paramètres > Général > Profil > XenMobile Profile Service** et touchez **Installer** pour ajouter le profil.



- Dans la fenêtre de notification, touchez **Faire confiance** pour inscrire votre appareil à la gestion à distance.



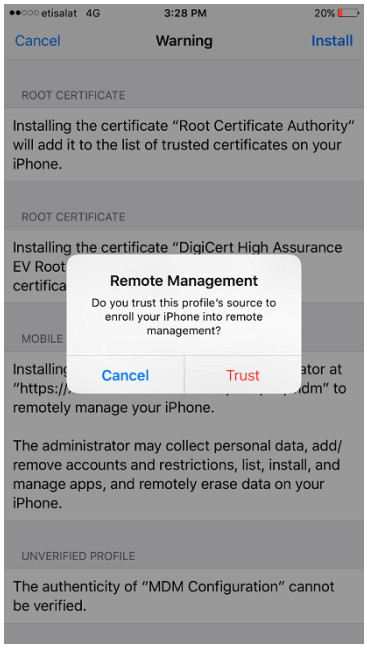
9. Connectez-vous à Secure Hub. Si vous vous inscrivez à MDM+MAM : une fois vos informations d'identification validées, créez et confirmez votre code PIN Citrix lorsque vous y êtes invité.
10. Une fois le workflow terminé, l'appareil est inscrit. Vous pouvez ensuite accéder au magasin d'applications pour afficher les applications que vous pouvez installer sur votre appareil iOS.

Appareils iOS

1. Téléchargez l'application Secure Hub à partir de l'App Store Apple iTunes sur l'appareil, puis installez l'application sur l'appareil.
2. Sur l'écran d'accueil de l'appareil iOS, tapotez l'application Secure Hub.
3. Lorsque l'application Secure Hub s'affiche, entrez l'adresse du serveur fournie par votre service d'assistance.

   Les écrans présentés peuvent différer de ces exemples en fonction de la façon dont XenMobile est configuré.
4. Lorsque vous y êtes invité, entrez vos nom d'utilisateur et mot de passe ou code PIN. Cliquez sur **Suivant**.
5. Lorsque vous êtes invité à vous inscrire, cliquez sur **Oui, inscrire** et entrez vos informations d'identification lorsque vous y êtes invité.
6. Cliquez sur **Installer** pour installer Citrix Profile Services.

7. Appuyez sur **Faire confiance**.



8. Appuyez sur **Ouvrir** puis entrez vos informations d'identification.

Appareils macOS

XenMobile propose deux méthodes pour inscrire des appareils qui exécutent macOS. Les deux méthodes permettent aux utilisateurs macOS de s'inscrire sans fil (OTA) directement depuis leurs appareils.

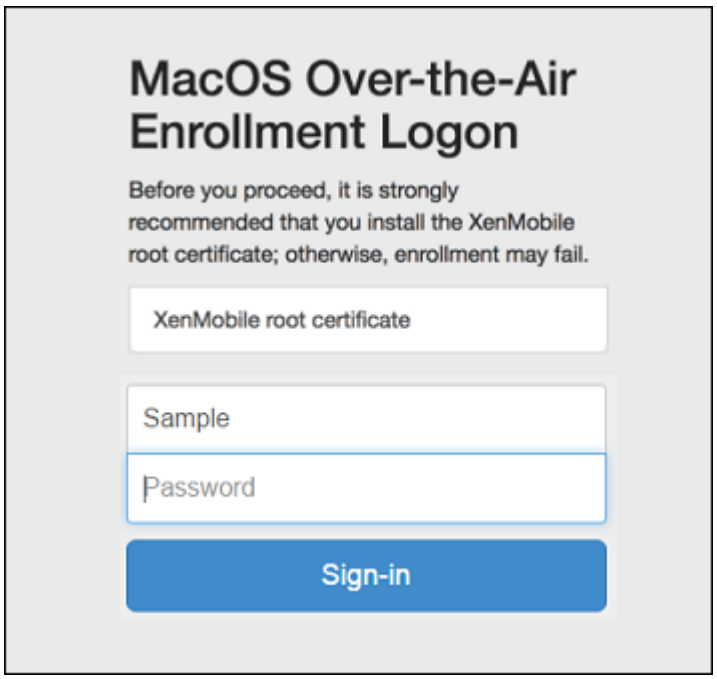
- **Envoyer une invitation d'inscription aux utilisateurs :** cette méthode d'inscription vous permet de définir un des modes d'inscription sécurisée suivants pour les appareils macOS :
  - Nom d'utilisateur + mot de passe
  - Nom d'utilisateur + PIN
  - Deux facteurs

  Lorsque l'utilisateur suit les instructions de l'invitation d'inscription, un écran de connexion avec le nom d'utilisateur déjà renseigné s'affiche.
- **Envoyer un lien d'installation aux utilisateurs :** cette méthode d'inscription pour les appareils macOS envoie aux utilisateurs un lien d'inscription qu'ils peuvent ouvrir dans les navigateurs Safari et Chrome. Ensuite, un utilisateur s'inscrit en fournissant son nom d'utilisateur et son mot de passe.

  Pour empêcher l'utilisation d'un lien d'inscription pour les appareils macOS, définissez la propriété de serveur **Activer macOS OTAE** sur **false**. Les utilisateurs macOS peuvent alors s'inscrire uniquement à l'aide d'une invitation d'inscription.

Envoyer une invitation d'inscription aux utilisateurs

1. Si vous le souhaitez, vous pouvez définir des stratégies macOS dans la console XenMobile. Consultez la section Stratégies d'appareil pour de plus amples informations sur les stratégies d'appareil.
2. Ajoutez une invitation pour l'inscription d'utilisateurs macOS. Pour de plus amples informations, consultez la section Envoyer une invitation d'inscription dans cet article.
3. Une fois que les utilisateurs reçoivent l'invitation et cliquent sur le lien, l'écran suivant s'affiche dans le navigateur Safari. XenMobile remplit le nom d'utilisateur. Si vous avez choisi **Deux facteurs** pour le mode d'inscription sécurisée, un champ supplémentaire s'affiche.



4. Les utilisateurs installent les certificats, selon les besoins. Les utilisateurs sont invités à installer des certificats si vous avez configuré pour macOS un certificat SSL approuvé publiquement et un certificat de signature numérique approuvé publiquement. Pour de plus amples informations sur les certificats, consultez la section Certificats et authentification.
5. Les utilisateurs entrent les informations d'identification demandées.

   Les stratégies Mac s'installent. Vous pouvez maintenant démarrer la gestion des Mac avec XenMobile tout comme vous gérez les appareils mobiles.

Envoyer un lien d'installation aux utilisateurs

1. Si vous le souhaitez, vous pouvez définir des stratégies macOS dans la console XenMobile. Consultez la section Stratégies d'appareil pour de plus amples informations sur les stratégies d'appareil.
2. Envoyez le lien d'inscription `https://serverFQDN:8443/instanceName/macos/otae` que les utilisateurs peuvent ouvrir dans les navigateurs Safari ou Chrome.

   - **serverFQDN** est le nom de domaine complet du serveur exécutant XenMobile.
   - Le port **8443** est le port sécurisé par défaut. Si vous avez configuré un port différent, utilisez-le à la place de 8443.
   - **instanceName**, souvent affiché sous la forme zdm, est le nom spécifié lors de l'installation du serveur.

   Pour de plus amples informations sur l'envoi des liens d'installation, consultez la section Pour envoyer un lien d'installation.

3. Les utilisateurs installent les certificats, selon les besoins. Si vous avez configuré un certificat SSL et un certificat de signature numérique approuvé publiquement pour iOS et macOS, les utilisateurs sont invités à installer les certificats. Pour de plus amples informations sur les certificats, consultez la section Certificats et authentification.
4. Les utilisateurs se connectent à leur Mac.

   Les stratégies Mac s'installent. Vous pouvez maintenant démarrer la gestion des Mac avec XenMobile tout comme vous gérez les appareils mobiles.

Machines Windows

> **Remarque :**
>
> Cette section contient des références aux appareils Windows Phone 8.1, que Microsoft a arrêté de prendre en charge le 11 juillet 2017. XenMobile prend en charge les appareils Windows Phone 8.1 pour l'inscription MDM uniquement.

Les appareils Windows 10 et Windows 11 s'inscrivent auprès d'Azure afin de fédérer l'authentification Active Directory. Vous pouvez associer les appareils Windows 10 et Windows 11 à Microsoft Azure AD de l'une des manières suivantes :

- Inscription dans MDM dans le cadre de Azure AD Join la première fois que l'appareil est mis sous tension.
- Inscription dans MDM dans le cadre de Azure AD Join à partir de la page Paramètres de Windows une fois que l'appareil a été configuré.

Vous pouvez inscrire des appareils dans XenMobile qui exécutent les systèmes d'exploitation Windows suivants :

- Téléphone Windows 10
- Windows 10
- Windows 11
- Windows Phone 8.1

Les utilisateurs peuvent effectuer l'inscription directement via leurs appareils.

> **Remarque :**
>
> Pour Windows 10 RS2 Phone et Tablet, au cours d'une réinscription, un utilisateur n'est pas invité à entrer l'adresse URL du serveur. Pour contourner ce problème, redémarrez l'appareil. Ou, sur l'écran de l'adresse e-mail, touchez le X en regard de **Connexion à un service** pour accéder à la page URL du serveur. Il s'agit d'un problème de tiers.

Vous devez configurer la détection automatique et le service de découverte Windows pour l'inscription de l'utilisateur afin d'autoriser la gestion des appareils Windows pris en charge.

Avant que les utilisateurs d'appareils Windows puissent s'inscrire à l'aide de Azure, vous devez configurer les paramètres du serveur Microsoft Azure dans XenMobile. Pour de plus amples informations, consultez la section Paramètres du serveur Microsoft Azure Active Directory.

Pour inscrire des appareils Windows à l'aide de la détection automatique

Pour activer la gestion des appareils Windows, Citrix vous recommande de configurer le service AutoDiscovery ainsi que le service de découverte Windows. Pour de plus amples informations, consultez la section XenMobile AutoDiscovery Service.

1. Sur l'appareil, recherchez et installez toutes les mises à jour Windows disponibles.
2. Pour Windows 10 et Windows 11 : dans le menu Icônes, touchez **Paramètres**, puis **Comptes > Accès professionnel ou d'école > Connecter à l'entreprise ou l'école**. Pour Windows 8.1 Phone, touchez **Paramètres du PC > Réseau > Espace de travail**.
3. Pour Windows 10 et Windows 11 : saisissez votre adresse e-mail professionnelle, puis appuyez sur **Continuer**. Pour Windows 8.1 : appuyez sur **Activer la gestion des appareils**. Pour vous inscrire en tant qu'utilisateur local, entrez une nouvelle adresse de messagerie avec le nom de domaine correct (par exemple, `foo@mydomain.com`). Cela vous permet de contourner une limitation Microsoft connue dans laquelle l'inscription est réalisée par la gestion des appareils intégrée sur Windows ; dans la boîte de dialogue **Connexion à un service**, entrez le nom d'utilisateur et le mot de passe associés à l'utilisateur local. L'appareil découvre automatiquement XenMobile Server et démarre le processus d'inscription.
4. Entrez votre mot de passe. Utilisez le mot de passe associé à un compte qui est membre d'un groupe d'utilisateurs dans XenMobile.
5. Pour Windows 10 et Windows 11 : dans la boîte de dialogue **Termes d'utilisation**, indiquez que vous acceptez que votre appareil soit géré, puis touchez **Accepter**. Pour Windows 8.1, dans la boîte de dialogue **Autorisez les applications et services de l'administrateur**, indiquez que vous acceptez que votre appareil soit géré, puis touchez **Activer**.

Pour inscrire des appareils Windows sans détection automatique

Il est possible d'inscrire des appareils Windows sans détection automatique. Cependant, Citrix vous recommande de configurer la détection automatique. L'inscription sans détection automatique provoque un appel vers le port 80 avant de se connecter à l'adresse URL de votre choix ; cette méthode de déploiement n'est donc pas recommandée dans un environnement de production. Citrix vous recommande d'utiliser ce processus uniquement dans des environnements de test et des déploiements de preuve de concept.

1. Sur l'appareil, recherchez et installez toutes les mises à jour Windows disponibles.

2. Pour Windows 10 et Windows 11 : dans le menu Icônes, touchez **Paramètres**, puis **Comptes > Accès professionnel ou d'école > Connecter à l'entreprise ou l'école**. Pour Windows 8.1, touchez **Paramètres du PC > Réseau > Espace de travail**.
3. Entrez votre adresse de messagerie d'entreprise.
4. Pour Windows 10 et Windows 11 : si la détection automatique n'est pas configurée, une option vous permettant d'entrer les détails du serveur apparaît, comme décrit dans l'étape 5. Pour Windows 8.1, si l'option **Détecter automatiquement l'adresse du serveur** est **activée**, touchez pour la **désactiver**.
5. Pour Windows 10 et Windows 11, dans le champ **Entrez l'adresse du serveur**, tapez l'adresse : `https://serverfqdn:8443/serverInstance/wpe`.

   Si un port autre que 8443 est utilisé pour les connexions SSL non authentifiées, utilisez ce numéro de port à la place de 8443 dans cette adresse.

   Pour Windows 8.1, tapez l'adresse du serveur au format suivant : `https://serverfqdn:8443/serverInstance/Discovery.svc`.

   Si un port autre que 8443 est utilisé pour les connexions SSL non authentifiées, utilisez ce numéro de port à la place de 8443 dans cette adresse.
6. Tapez votre mot de passe.
7. Pour Windows 10 et Windows 11 : dans la boîte de dialogue **Termes d'utilisation**, indiquez que vous acceptez que votre appareil soit géré, puis touchez **Accepter**. Pour Windows 8.1, dans la boîte de dialogue **Autorisez les applications et services de l'administrateur**, indiquez que vous acceptez que votre appareil soit géré, puis touchez **Activer**.

Pour inscrire des appareils Windows Phone

Pour inscrire des appareils Windows Phone dans XenMobile, les utilisateurs ont besoin de leur adresse e-mail de réseau interne ou Active Directory et d'un mot de passe. Si la détection automatique n'est pas configurée, les utilisateurs ont également besoin de l'adresse Web de XenMobile Server. Ensuite, ils suivent cette procédure sur leurs appareils pour s'inscrire.

> **Remarque :**
>
> Si vous prévoyez de déployer des applications via le magasin d'entreprise Windows Phone, avant que vos utilisateurs ne s'inscrivent, assurez-vous d'avoir configuré une stratégie d'hub d'entreprise (avec une application Secure Hub Windows Phone signée pour chaque plate-forme que vous prenez en charge).

1. Sur l'écran principal du Windows Phone, touchez l'icône **Paramètres**.

- Pour Windows 10 et Windows 11 : en fonction de votre version, touchez **Comptes > Accès professionnel ou d'école > Connecter à l'entreprise ou l'école** ou touchez **Comptes > Accès professionnel > S'inscrire à la gestion des appareils**.
- Pour Windows 8.1, touchez **Paramètres du PC > Réseau > Espace de travail**, puis touchez **Ajouter un compte**.

2. Dans l'écran suivant, entrez une adresse de messagerie et un mot de passe et touchez **s'inscrire**.

   Si la détection automatique est configurée pour votre domaine, les informations requises dans les étapes suivantes sont automatiquement renseignées. Passez à l'étape 8.

   Si la détection automatique n'est pas configurée pour votre domaine, passez à l'étape suivante. Pour vous inscrire en tant qu'utilisateur local, entrez une nouvelle adresse de messagerie avec le nom de domaine correct (par exemple, `foo@mydomain.com`). Cela vous permet de contourner une limitation Microsoft connue ; dans la boîte de dialogue **Connexion à un service**, entrez le nom d'utilisateur et le mot de passe associés à l'utilisateur local.

3. Sur l'écran suivant, entrez l'adresse Web de XenMobile Server, telle que : `https://<xenmobile_server>:<portnumber>/<instancename>/wpe`. Par exemple, `https://mycompany.mdm.com:8443/zdm/wpe`.

   > **Remarque :**
   >
   > Le numéro de port doit être adapté à votre mise en œuvre. Il doit s'agir du port que vous avez utilisé pour une inscription iOS.

4. Entrez le nom d'utilisateur et le domaine si l'authentification est validée à l'aide d'un nom d'utilisateur et un domaine, puis touchez **Connexion**.

5. Sur Windows Phone 8.1, lorsque le compte est ajouté, vous avez la possibilité de sélectionner **Installer l'application de l'entreprise**. Si votre administrateur a configuré un magasin d'applications d'entreprise, sélectionnez cette option et tapotez sur **Terminé**. Si vous désactivez cette option, vous devrez réinscrire votre appareil pour recevoir le magasin d'applications d'entreprise.

6. Sur Windows Phone 8.1, sur l'écran **Compte ajouté**, touchez **Terminé**.

7. Pour forcer une connexion au serveur, cliquez sur l'icône d'actualisation. Si l'appareil ne se connecte pas manuellement au serveur, XenMobile essaye de se reconnecter. XenMobile se connecte à l'appareil toutes les 3 minutes à 5 reprises, puis toutes les 2 heures par la suite. Vous pouvez modifier cet intervalle de connexion dans **Intervalle de pulsation WNS Windows** situé dans **Propriétés du serveur**. Une fois l'inscription terminée, Secure Hub s'inscrit en arrière-plan. Aucun indicateur n'apparaît lorsque l'installation est terminée. Appuyez sur Secure Hub sur l'écran **Toutes les applications**.

Envoyer une invitation d'inscription

Dans la console XenMobile, vous pouvez envoyer une invitation d'inscription aux utilisateurs d'appareils iOS, macOS, Android Enterprise et d'appareils Android d'ancienne génération. Vous pouvez également envoyer un lien d'installation aux utilisateurs d'appareils iOS, Android Enterprise ou d'appareils Android d'ancienne génération.

Des invitations d'inscription sont envoyées comme suit :

- Si l'invitation d'inscription est pour un utilisateur local ou Active Directory : l'utilisateur reçoit l'invitation par SMS sur le numéro de téléphone et le nom d'opérateur que vous spécifiez.
- Si l'invitation d'inscription est pour un groupe : les utilisateurs reçoivent des invitations par SMS. Si les utilisateurs Active Directory ont une adresse e-mail et un numéro de téléphone mobile dans Active Directory, ils reçoivent l'invitation. Les utilisateurs locaux reçoivent l'invitation sur l'e-mail et le numéro de téléphone spécifiés dans les propriétés de l'utilisateur.

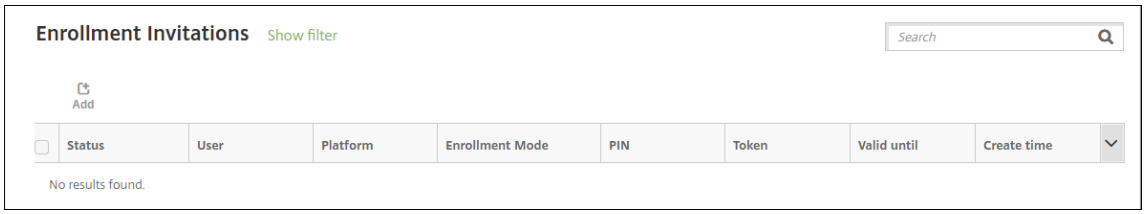
Une fois que les utilisateurs s'inscrivent, leurs appareils apparaissent en tant que gérés sous **Gérer > Appareils**. L'état de l'URL d'invitation s'affiche en tant que **Utilisée**.

Conditions préalables

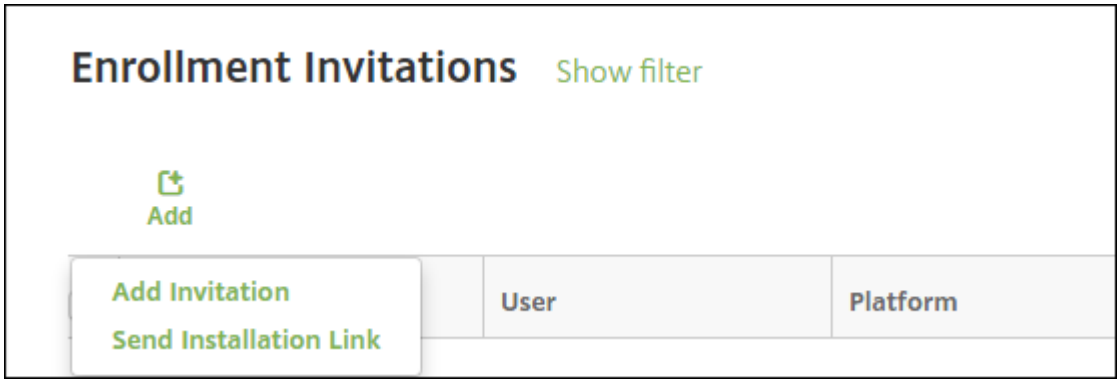
- XenMobile Server configuré en mode Enterprise (XME) ou MDM
- LDAP configuré
- Si vous utilisez des groupes locaux et utilisateurs locaux :
  - Un ou plusieurs groupes locaux.
  - Utilisateurs locaux attribués à des groupes locaux.
  - Des groupes de mise à disposition sont associés à des groupes locaux.
- Utilisation d'Active Directory :
  - Des groupes de mise à disposition sont associés à des groupes Active Directory.

Créer une invitation d'inscription

1. Dans la console XenMobile, cliquez sur **Gérer > Invitations d'inscription**. La page **Invitations d'inscription** s'affiche.



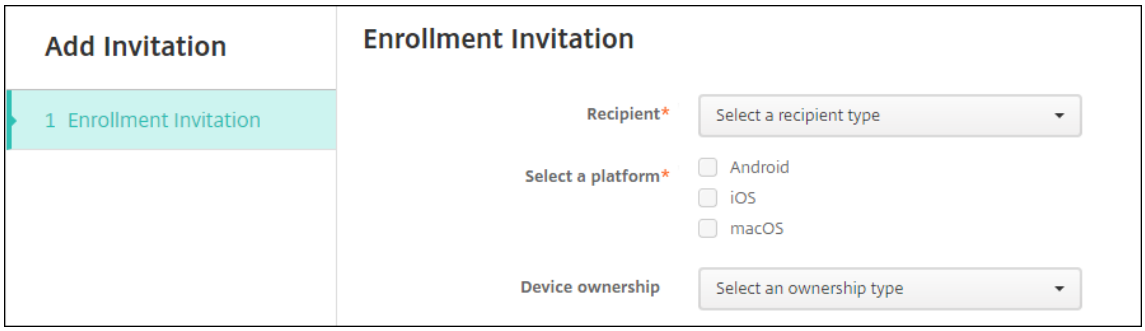
2. Cliquez sur **Ajouter**. Un menu des options d'inscription s'affiche.



   - Pour envoyer une invitation d'inscription à un utilisateur ou un groupe, cliquez sur **Ajouter une invitation**.
   - Pour envoyer un lien d'installation d'inscription à une liste de destinataires via SMTP ou SMS, cliquez sur **Envoyer lien d'installation**.

   L'envoi d'invitations d'inscription et de liens d'installation est décrit après ces étapes.

3. Cliquez sur **Ajouter une invitation**. L'écran **Invitation d'inscription** s'affiche.



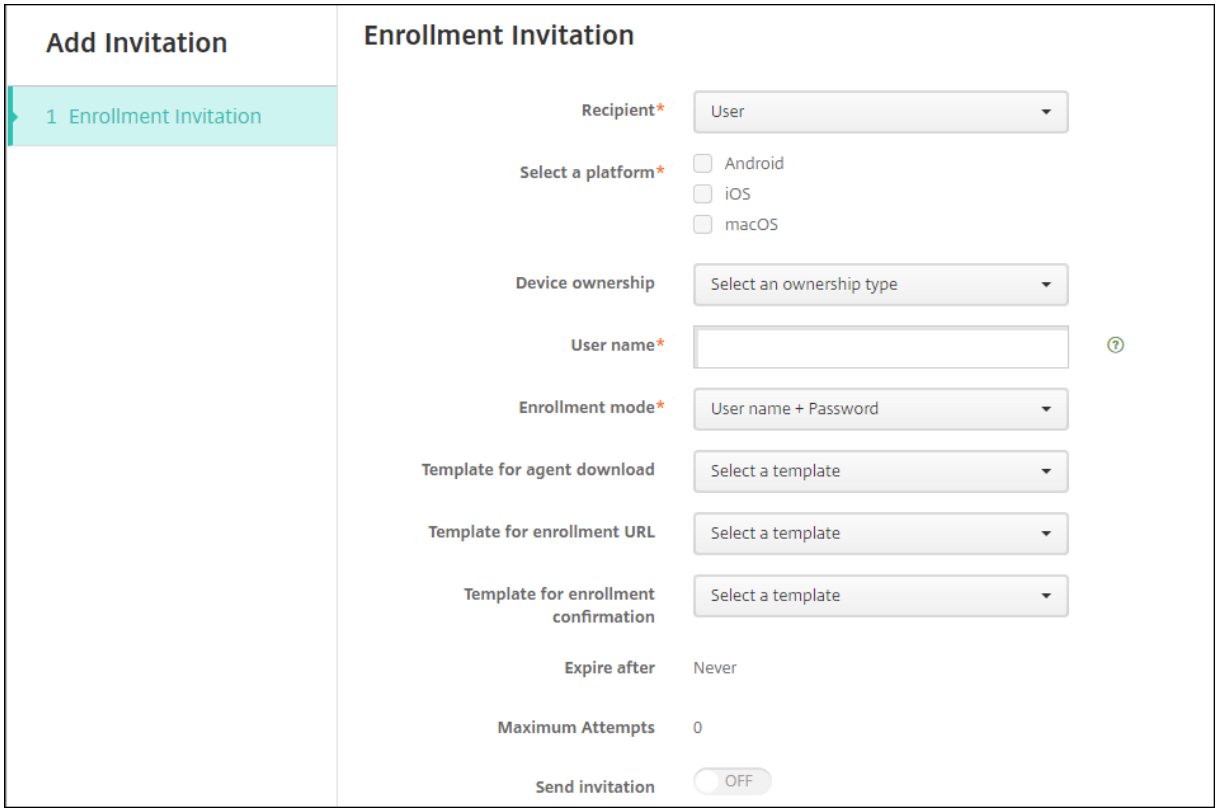
4. Pour configurer ces paramètres :

   - **Destinataire :** choisissez **Groupe** ou **Utilisateur**.
   - **Sélectionner une plate-forme :** si **Destinataire** est défini sur **Groupe**, toutes les plates-formes sont sélectionnées. Vous pouvez modifier la plate-forme sélectionnée. Si **Destinataire** est défini sur **Utilisateur**, aucune plate-forme n'est sélectionnée. Sélectionnez une plate-forme.

     Pour créer une invitation d'inscription pour les appareils Android Enterprise, sélectionnez **Android > Android Enterprise**.
   - **Propriétaire :** sélectionnez **Entreprise** ou **Employé**.

   Les paramètres pour les utilisateurs ou groupes s'affichent, comme décrit dans les sections suivantes.

Pour envoyer une invitation d'inscription à un utilisateur



1. Configurez ces paramètres **Utilisateur** :

   - **Nom d'utilisateur :** entrez un nom d'utilisateur. L'utilisateur doit exister dans XenMobile Server en tant qu'utilisateur local ou en tant qu'utilisateur dans Active Directory. Si l'utilisateur est local, assurez-vous que la propriété Email de l'utilisateur est configurée pour vous permettre de lui envoyer des notifications. S'il s'agit d'un utilisateur Active Directory, assurez-vous que LDAP est configuré.
   - **Infos sur l'appareil :** ce paramètre ne s'affiche pas si vous sélectionnez plusieurs plates-formes, ou si vous sélectionnez macOS uniquement. Choisissez **Numéro de série**, **UDID** ou **IMEI**. Après avoir choisi une option, un champ s'affiche dans lequel vous pouvez entrer la valeur correspondante à l'appareil.
   - **Numéro de téléphone :** ce paramètre ne s'affiche pas si vous sélectionnez plusieurs plates-formes, ou si vous sélectionnez macOS uniquement. Si vous le souhaitez, entrez le numéro de téléphone de l'utilisateur.
   - **Opérateur :** ce paramètre ne s'affiche pas si vous sélectionnez plusieurs plates-formes, ou si vous sélectionnez macOS uniquement. Choisissez un opérateur à associer au numéro de téléphone de l'utilisateur.
   - **Mode d'inscription :** choisissez le mode d'inscription sécurisée pour les utilisateurs. La valeur par défaut est **Nom d'utilisateur + mot de passe**. Certaines des options suivantes ne sont pas disponibles pour toutes les plates-formes :

- Nom d'utilisateur + mot de passe
- Haute sécurité
- URL d'invitation
- URL d'invitation + PIN
- URL d'invitation + mot de passe
- Deux facteurs
- Nom d'utilisateur + PIN

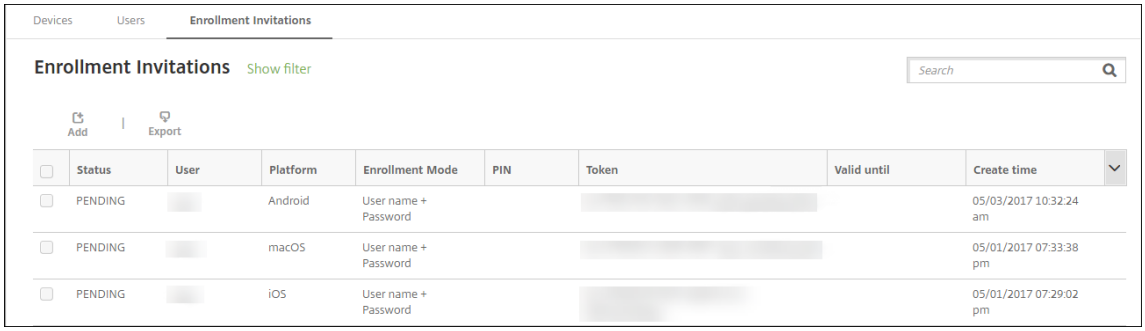
Pour envoyer des invitations d'inscription, vous pouvez uniquement utiliser les modes d'inscription sécurisée **URL d'invitation**, **URL d'invitation + PIN** ou **URL d'invitation + mot de passe**. Pour les appareils qui sont inscrits avec **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + PIN**, les utilisateurs doivent entrer manuellement leurs informations d'identification dans Secure Hub.

Un code PIN d'inscription est également appelé un code PIN à usage unique. Ces codes PIN sont valides uniquement lorsque l'utilisateur s'inscrit.

> **Remarque :**
>
> Lorsque vous sélectionnez un mode d'inscription sécurisée qui comprend un code PIN, le champ **Modèle pour le code PIN d'inscription** s'affiche, dans lequel vous cliquez sur **Code PIN d'inscription**.

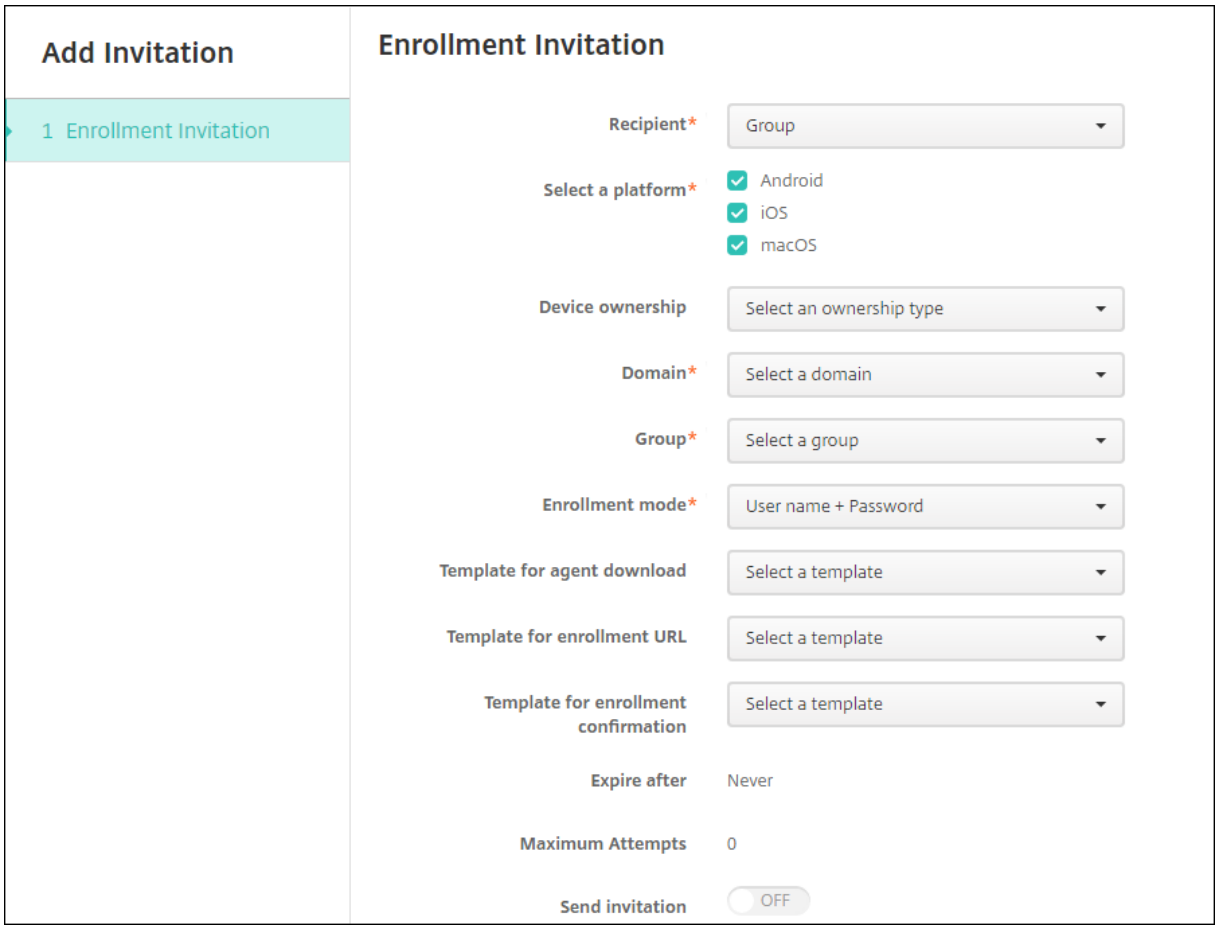
- **Modèle pour téléchargement de l'agent :** choisissez le modèle de lien de téléchargement appelé **Lien de téléchargement**. Ce modèle est destiné à toutes les plates-formes prises en charge.
- **Modèle pour l'URL d'inscription :** choisissez **Invitation d'inscription**.
- **Modèle pour la confirmation d'inscription :** choisissez **Confirmation d'inscription**.
- **Expire après :** ce champ est défini lorsque vous configurez le mode d'inscription et indique quand l'inscription expire. Pour plus d'informations sur la configuration des modes d'inscription sécurisée, veuillez consulter la section Configurer les modes d'inscription sécurisée.
- **Nbre max de tentatives :** ce champ est défini lorsque vous configurez le **mode d'inscription** et indique le nombre maximal de tentatives du processus d'inscription. Pour plus d'informations sur la configuration des modes d'inscription sécurisée, veuillez consulter la section Configurer les modes d'inscription sécurisée.
- **Envoyer invitation :** sélectionnez **Activé** pour envoyer l'invitation immédiatement. Sélectionnez **Désactivé** pour ajouter l'invitation au tableau sur la page **Invitations d'inscription**, mais ne pas l'envoyer.

2. Cliquez sur **Enregistrer et Envoyer** si vous avez activé **Envoyer invitation**. Sinon, cliquez sur **Enregistrer**. L'invitation apparaît dans le tableau sur la page **Invitations d'inscription**.



Pour envoyer une invitation d'inscription à un groupe

La figure suivante montre les paramètres de configuration d'une invitation d'inscription à un groupe.



1. Pour configurer ces paramètres :
    - **Domaine :** choisissez le domaine du groupe qui recevra l'invitation.
    - **Groupe :** choisissez le groupe qui recevra l'invitation.
    - **Mode d'inscription :** choisissez la manière dont vous souhaitez que les utilisateurs du groupe s'inscrivent. La valeur par défaut est **Nom d'utilisateur + mot de passe**. Certaines des options suivantes ne sont pas disponibles pour toutes les plates-formes :

- Nom d'utilisateur + mot de passe
- Haute sécurité
- URL d'invitation
- URL d'invitation + PIN
- URL d'invitation + mot de passe
- Deux facteurs
- Nom d'utilisateur + PIN

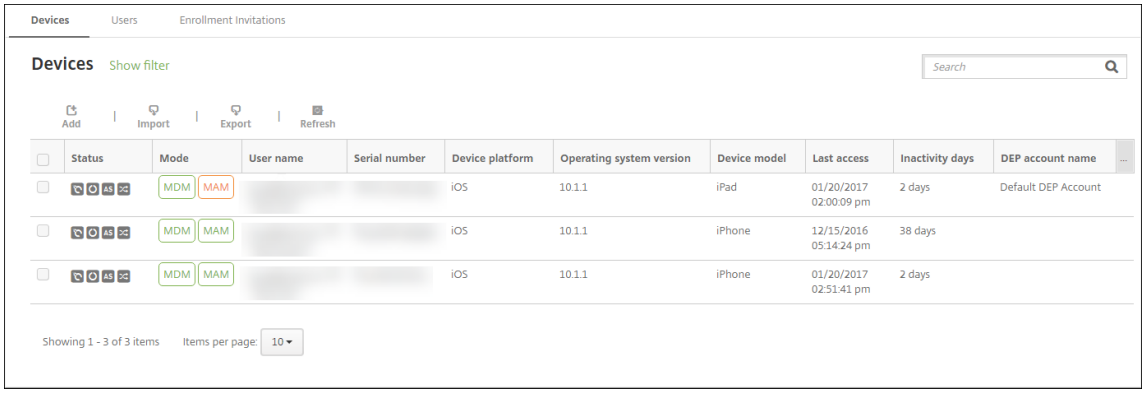
Pour envoyer des invitations d'inscription, vous pouvez uniquement utiliser les modes d'inscription sécurisée **URL d'invitation**, **URL d'invitation + PIN** ou **URL d'invitation + mot de passe**. Pour les appareils qui sont inscrits avec **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + PIN**, les utilisateurs doivent entrer manuellement leurs informations d'identification dans Secure Hub.

Seuls les mode d'inscription sécurisée qui sont valides pour chacune des plates-formes sélectionnées s'affichent.

> **Remarque :**
>
> Lorsque vous sélectionnez un mode d'inscription sécurisée qui comprend un code PIN, le champ **Modèle pour le code PIN d'inscription** s'affiche, dans lequel vous cliquez sur **Code PIN d'inscription**.

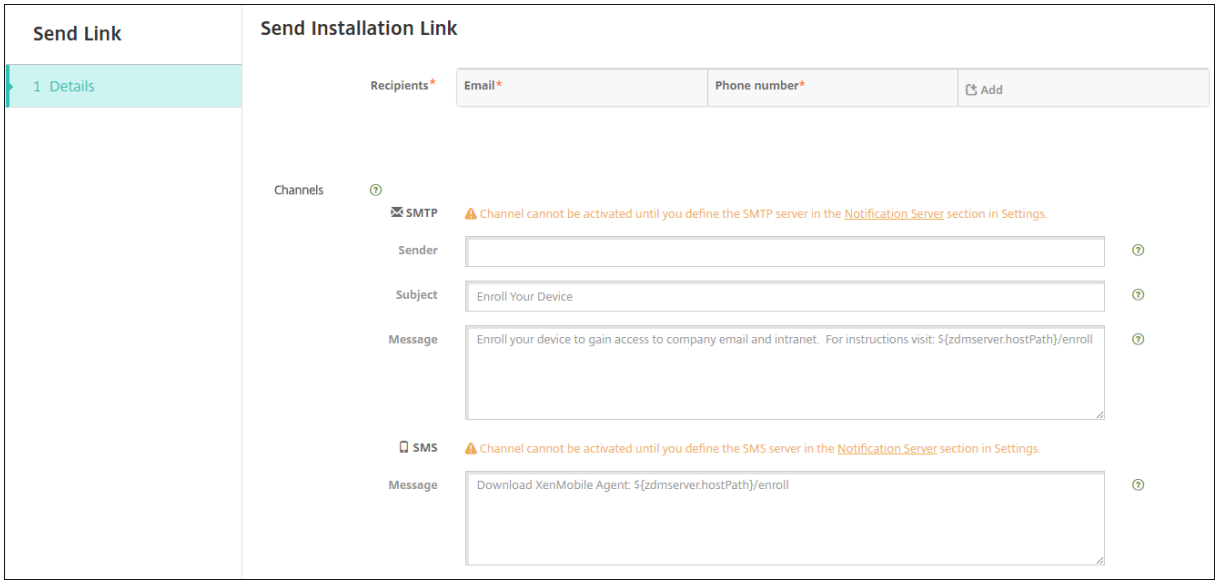
- **Modèle pour téléchargement de l'agent :** choisissez le modèle de lien de téléchargement appelé **Lien de téléchargement**. Ce modèle est destiné à toutes les plates-formes prises en charge.
- **Modèle pour l'URL d'inscription :** choisissez **Invitation d'inscription**.
- **Modèle pour la confirmation d'inscription :** choisissez **Confirmation d'inscription**.
- **Expire après :** ce champ est défini lorsque vous configurez le mode d'inscription et indique quand l'inscription expire. Pour plus d'informations sur la configuration des modes d'inscription sécurisée, veuillez consulter la section Configurer les modes d'inscription sécurisée.
- **Nbre max de tentatives :** ce champ est défini lorsque vous configurez le mode d'inscription et indique le nombre maximal de tentatives du processus d'inscription. Pour plus d'informations sur la configuration des modes d'inscription sécurisée, veuillez consulter la section Configurer les modes d'inscription sécurisée.
- **Envoyer invitation :** sélectionnez **Activé** pour envoyer l'invitation immédiatement. Sélectionnez **Désactivé** pour ajouter l'invitation au tableau sur la page **Invitations d'inscription**, mais ne pas l'envoyer.

2. Cliquez sur **Enregistrer et Envoyer** si vous avez activé **Envoyer invitation**. Sinon, cliquez sur **Enregistrer**. L'invitation apparaît dans le tableau sur la page **Invitation d'inscription**.



Pour envoyer un lien d'installation

Avant de pouvoir envoyer un lien d'installation de l'inscription, vous devez configurer les canaux (SMTP ou SMS) sur le serveur de notification à partir de la page **Paramètres**. Pour plus d'informations, consultez la section [Notifications] (/fr-fr/xenmobile/server/users/notifications.html).



1. Configurez ces paramètres, puis cliquez sur **Enregistrer**.
   - **Destinataire :** pour chaque destinataire que vous souhaitez ajouter, cliquez sur **Ajouter** et procédez comme suit :
     - **Adresse électronique :** entrez l'adresse e-mail du destinataire. Ce champ est obligatoire.
     - **Numéro de téléphone :** entrez le numéro de téléphone de l'utilisateur. Ce champ est obligatoire.

> **Remarque :**
>
> Pour supprimer un destinataire existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.
>
> Pour modifier un destinataire, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Mettez la liste à jour, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

- **Canaux :** sélectionnez un canal à utiliser pour envoyer le lien d'installation de l'inscription. Vous pouvez envoyer des notifications via **SMTP** ou **SMS**. Ces canaux (SMTP ou SMS) ne peuvent pas être activés tant que vous n'avez pas configuré les paramètres du serveur sur la page **Paramètres** dans **Serveur de notification**. Pour plus de détails, consultez la section Notifications.
- **SMTP :** configurez ces paramètres facultatifs. Si vous ne renseignez pas ces champs, les valeurs par défaut spécifiées dans le modèle de notification configuré pour la plate-forme que vous avez sélectionnée sont utilisées :
  - **Expéditeur :** entrez un expéditeur (facultatif).
  - **Sujet :** entrez un sujet pour le message (facultatif). Par exemple, « inscription de votre appareil ».
  - **Message :** entrez le message à envoyer au destinataire (facultatif). Par exemple, « Inscrivez votre appareil pour accéder à la messagerie et aux applications de l'entreprise ».
- **SMS :** configurez ce paramètre. Si vous ne renseignez pas ce champ, la valeur par défaut spécifiée dans le modèle de notification configuré pour la plate-forme que vous avez sélectionnée est utilisée :
  - **Message :** entrez le message à envoyer aux destinataires. Ce champ est obligatoire pour les notifications SMS.

> **Remarque :** en Amérique du Nord, les messages SMS qui dépassent 160 caractères sont remis dans plusieurs messages.

2. Cliquez sur **Envoyer**.

> **Remarque :**
>
> Si votre environnement utilise l'attribut sAMAccountName : après que les utilisateurs aient reçu l'invitation et cliqué sur le lien, ils doivent modifier le nom d'utilisateur pour compléter l'authentification. Le nom d'utilisateur s'affiche au format sAMAc-

> countName@nomdomaine.com. Les utilisateurs doivent supprimer la partie @nomdomaine.com.

Modes d'inscription sécurisée par plateforme

Le tableau suivant affiche les modes d'inscription sécurisée que vous pouvez utiliser pour inscrire des machines utilisateur. Dans le tableau, **Oui** indique quelles plates-formes d'appareils prennent en charge des modes d'inscription et de gestion spécifiques avec différents profils d'inscription.

Mode d'inscription sécurisée MDM	Mode d'inscription sécurisée MAM sur Citrix Gateway	Modes de gestion	Prise en charge de différents profils d'inscription	Android (ancien)	Android Entreprise	iOS (mode d'inscription des utilisateurs)	iOS	macOS	Windows
Azure AD et Okta en tant que fournisseurs d'identité via Citrix Cloud	Certificat client	MDM+MAM ou MDM	Oui	Oui	Oui	Oui	Oui	Non	Non

Mode d'inscription sécurisée MDM	Mode d'inscription sécurisée MAM sur Citrix Gateway	Modes de gestion	Prise en charge de différents profils d'inscription	Android (ancien)	Android Entreprise	iOS (mode d'inscription des utilisateurs)	iOS	macOS	Windows
Nom d'utilisateur + mot de passe	LDAP, LDAP + certificat client et certificat client uniquement	MDM+MAM, MDM ou MAM (le mode MAM exclusif ne prend pas en charge les certificats clients sur Citrix Gateway)	Oui	Oui	Oui	Oui	Oui	Oui	Oui
URL d'invitat	Certifica client	MDM+M ou MDM	Oui	Oui	Oui	Non	Oui	Non	Non
URL d'invitation + PIN	Certificat client	MDM+MAM ou MDM	Oui	Oui	Oui	Non	Oui	Non	Non

Mode d'inscription sécurisée MDM	Mode d'inscription sécurisée MAM sur Citrix Gateway	Modes de gestion	Prise en charge de différents profils d'inscription	Android (ancien)	Android Entreprise	iOS (mode d'inscription des utilisateurs)	iOS	macOS	Windows
URL d'invitat + mot de passe	LDAP, LDAP + certificat client et certificat client uniquement	MDM+MA ou MDM	Oui	Oui	Oui	Non	Oui	Non	Non
Authentification à deux facteurs (nom d'utilisateur + mot de passe + code PIN)	LDAP, LDAP + certificat client et certificat client uniquement	MDM+MAM ou MDM	Oui	Oui	Oui	Non	Oui	Oui	Non
Nom d'utilisa + PIN	Certifica client	MDM+MA ou MDM	Oui	Oui	Oui	Non	Oui	Oui	Non

Le comportement des modes d'inscription sécurisée sur les appareils iOS, Android et Android Enterprise est décrit ci-après :

- **Nom d'utilisateur + mot de passe** (défaut)
  - Envoie à un utilisateur une seule notification contenant une URL d'inscription. Lorsque l'utilisateur clique sur l'URL, Secure Hub s'ouvre. L'utilisateur entre ensuite un nom

d'utilisateur et un mot de passe pour inscrire l'appareil dans XenMobile.

- **URL d'invitation**
  - Envoie à un utilisateur une seule notification contenant une URL d'inscription. Lorsque l'utilisateur clique sur l'URL, Secure Hub s'ouvre. Le nom du serveur XenMobile et le bouton **Oui, inscrire** apparaissent. L'utilisateur appuie sur **Oui, inscrire** pour inscrire l'appareil dans XenMobile.
- **URL d'invitation + PIN**
  - Envoie à un utilisateur les e-mails suivants :
    * Un e-mail avec une URL d'inscription, qui permet à l'utilisateur d'inscrire l'appareil dans XenMobile via Secure Hub.
    * Un e-mail avec un code PIN à usage unique que l'utilisateur doit entrer lors de l'inscription de l'appareil, ainsi que le mot de passe de l'utilisateur Active Directory (ou local).
  - Avec ce mode, l'utilisateur effectue l'inscription uniquement en utilisant l'URL d'inscription inclus dans la notification. Si l'utilisateur perd l'invitation de notification, il ne peut pas effectuer l'inscription. Vous pouvez, cependant, envoyer une autre invitation.
- **URL d'invitation + mot de passe**
  - Envoie à un utilisateur une seule notification contenant une URL d'inscription. Lorsque l'utilisateur clique sur l'URL, Secure Hub s'ouvre. Le nom du serveur XenMobile apparaît, ainsi qu'un champ permettant à l'utilisateur d'entrer un mot de passe.
- **Deux facteurs**
  - Envoie à un utilisateur une seule notification contenant une URL d'inscription et un code PIN unique. Lorsque l'utilisateur clique sur l'URL, Secure Hub s'ouvre. Le nom du serveur XenMobile apparaît, ainsi que deux champs permettant à l'utilisateur d'entrer un mot de passe et le code PIN.
- **Nom d'utilisateur + PIN**
  - Envoie à un utilisateur les e-mails suivants :
    * Un e-mail avec une URL d'inscription, qui permet à l'utilisateur de télécharger et d'installer Secure Hub. Une fois Secure Hub ouvert, l'utilisateur est invité à entrer un nom d'utilisateur et un mot de passe pour inscrire l'appareil dans XenMobile.
    * Un e-mail avec un code PIN à usage unique que l'utilisateur doit entrer lors de l'inscription de l'appareil, ainsi que le mot de passe de l'utilisateur Active Directory (ou local).
  - Si l'utilisateur perd l'invitation de notification, il ne peut pas effectuer l'inscription. Vous pouvez, cependant, envoyer une autre invitation.

Le comportement des modes d'inscription sécurisée sur les appareils macOS est décrit ci-après :

- **Nom d'utilisateur + mot de passe**
  - Envoie à un utilisateur une seule notification contenant une URL d'inscription. Lorsque

l'utilisateur clique sur l'URL, le navigateur Safari s'ouvre. Une page de connexion apparaît, invitant l'utilisateur à entrer un nom d'utilisateur et un mot de passe pour inscrire l'appareil dans XenMobile.

- **Deux facteurs**
  - Envoie à un utilisateur une seule notification contenant une URL d'inscription et un code PIN unique. Lorsque l'utilisateur clique sur l'URL, le navigateur Safari s'ouvre. Une page de connexion apparaît, affichant deux champs permettant à l'utilisateur de taper un mot de passe et le code PIN.
- **Nom d'utilisateur + PIN**
  - Envoie à un utilisateur les e-mails suivants :
    * Un e-mail avec une URL d'inscription. Lorsque l'utilisateur clique sur l'URL, le navigateur Safari s'ouvre. Une page de connexion apparaît, invitant l'utilisateur à entrer un nom d'utilisateur et un mot de passe pour inscrire l'appareil dans XenMobile.
    * Un e-mail avec un code PIN à usage unique que l'utilisateur doit entrer lors de l'inscription de l'appareil, ainsi que le mot de passe de l'utilisateur Active Directory (ou local).
  - Si l'utilisateur perd l'invitation de notification, il ne peut pas effectuer l'inscription. Vous pouvez, cependant, envoyer une autre invitation.

Vous ne pouvez pas envoyer d'invitations d'inscription aux appareils Windows. Les utilisateurs Windows s'inscrivent directement sur leurs appareils.

Firebase Cloud Messaging

January 10, 2022

> **Remarque :**
>
> Firebase Cloud Messaging (FCM) était auparavant connu sous le nom de Google Cloud Messaging (GCM). Certains libellés et messages de la console XenMobile utilisent la terminologie GCM.

Citrix recommande d'utiliser Firebase Cloud Messaging (FCM) pour contrôler quand et comment les appareils Android se connectent à XenMobile. XenMobile, lorsqu'il est configuré pour FCM, envoie des notifications de connexion aux appareils Android activés pour FCM. Toute action de sécurité ou commande de déploiement déclenche une notification push afin d'inviter l'utilisateur à se reconnecter à XenMobile Server.

Une fois que vous avez terminé les étapes de configuration de cet article et qu'un appareil se connecte, l'appareil s'enregistre auprès du service FCM dans XenMobile Server. Cette connexion permet une communication quasi en temps réel de votre service XenMobile avec votre appareil à l'aide de FCM. L'enregistrement FCM fonctionne pour les nouveaux appareils inscrits et les appareils déjà inscrits.

Lorsque XenMobile doit initier une connexion avec l'appareil, il se connecte au service FCM. Ensuite, le service FCM envoie à l'appareil une notification pour qu'il se connecte. Ce type de connexion est similaire à ce qu'Apple utilise pour son service de notification Push (APNs).

Conditions préalables

- Dernier client Secure Hub
- Informations d'identification du compte Google Developer
- Services Google Play installés sur les appareils Android compatibles avec FCM

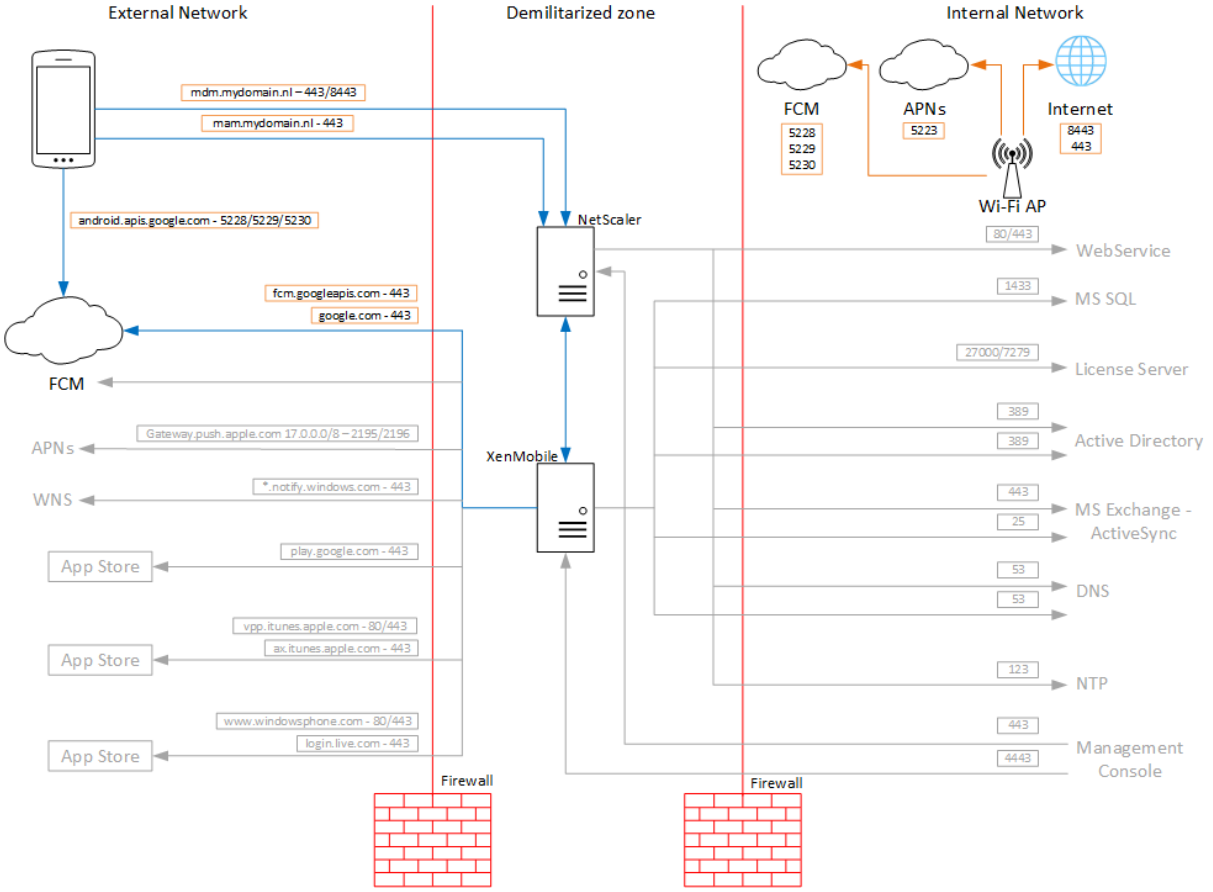
Ports du pare-feu

- Ouvrez le port 443 sur XenMobile vers `fcm.googleapis.com` et `Google.com`.
- Ouvrez la communication Internet sortante pour le réseau Wi-Fi de l'appareil sur les ports 5228, 5229 et 5230.
- Pour autoriser les connexions sortantes, FCM recommande d'autoriser les ports 5228 à 5230 sans restrictions IP. Toutefois, si vous avez besoin de restrictions IP, FCM recommande d'autoriser toutes les adresses IP dans les blocs IPv4 et IPv6. Ces blocs sont répertoriés dans l'ASN 15169 de Google. Mettez à jour cette liste tous les mois.

Pour plus d'informations, consultez la section Configuration requise pour les ports.

Architecture

Ce diagramme illustre le flux de communication pour FCM dans le réseau interne et externe.

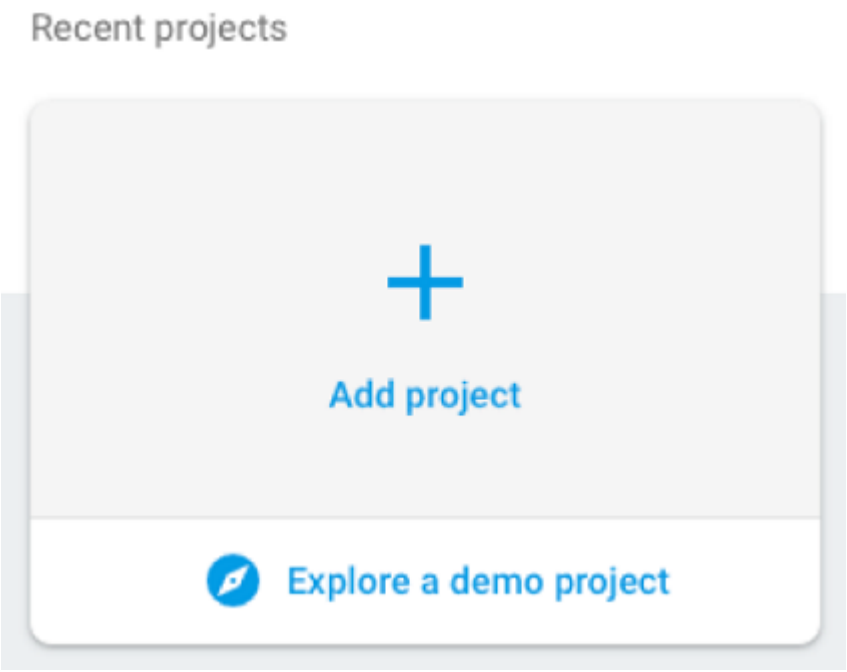


Pour configurer votre compte Google pour FCM

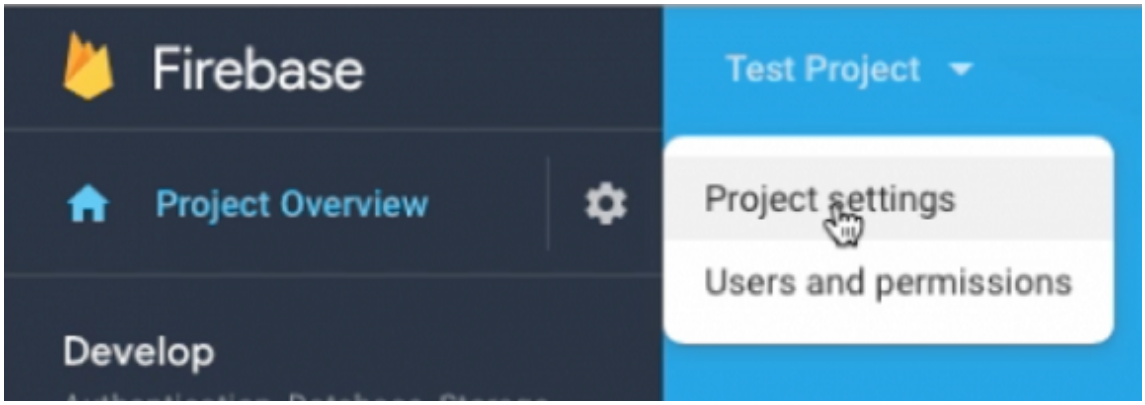
1. Connectez-vous à l'adresse URL suivante à l'aide des informations d'identification de votre compte Google Developer :

   https://console.firebase.google.com/

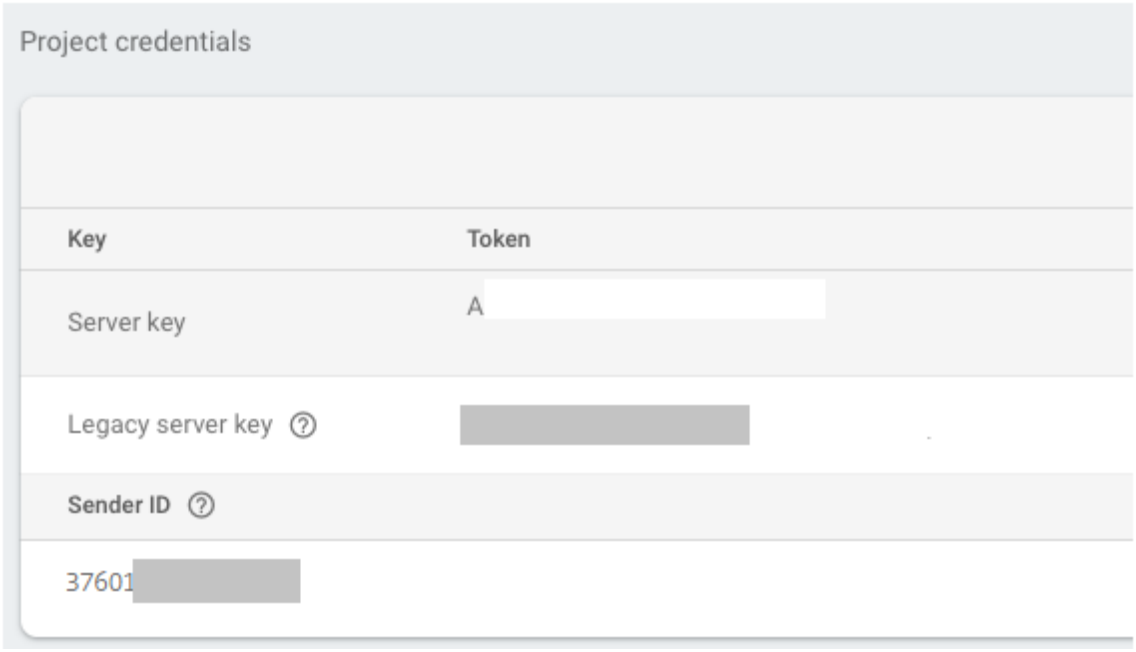
2. Cliquez sur **Ajouter un projet**.



3. Après avoir créé le projet, cliquez sur **Paramètres du projet**.



4. Cliquez sur l'onglet **Cloud Messaging**. Copiez les valeurs **Clé serveur** et **ID d'expéditeur**. Dans la procédure suivante, vous collerez ces valeurs dans la console XenMobile. Depuis octobre 2016, vous devez créer des clés serveur dans la console Firebase.

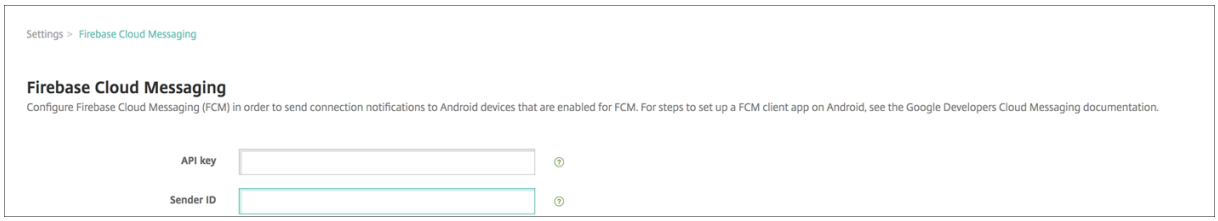


Pour savoir comment configurer une application cliente FCM sur Android, consultez l'article destiné aux développeurs Google Cloud Messaging : https://firebase.google.com/docs/cloud-messaging/android/client.

Pour configurer XenMobile pour FCM

Dans la console XenMobile, accédez à **Paramètres > Firebase Cloud Messaging**.

- Modifiez la **clé API** et entrez la **clé serveur** de Firebase Cloud Messaging que vous avez copiée dans la dernière étape de configuration de Firebase Cloud Messaging.
- Modifiez l'**ID de l'expéditeur** et copiez la valeur de l'**ID de l'expéditeur** que vous avez copiée dans la procédure précédente.

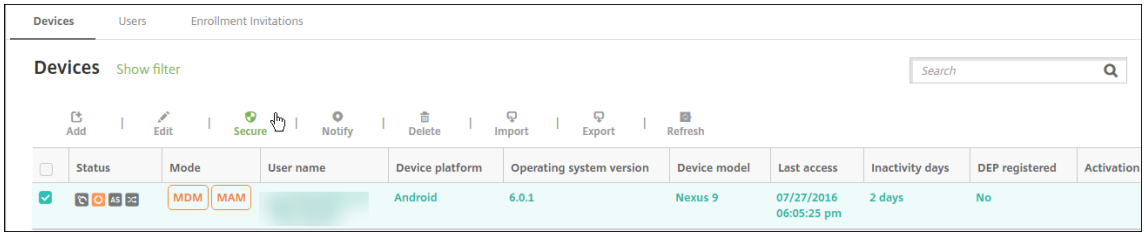


Une fois la configuration terminée, vous pouvez supprimer votre stratégie Planification ou modifier cette stratégie pour vous connecter moins souvent.

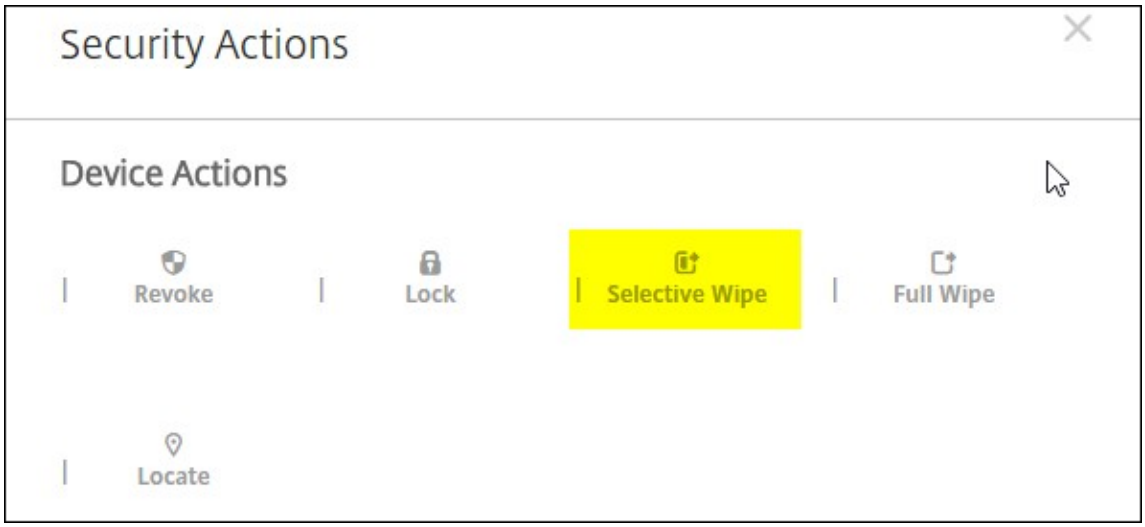
Pour tester votre configuration

1. Inscrivez un appareil Android.

2. Laissez l'appareil inactif pendant un certain temps, de façon à ce qu'il se déconnecte de XenMobile.
3. Connectez-vous à la console XenMobile, cliquez sur **Gérer**, sélectionnez l'appareil Android, puis cliquez sur **Sécurisé**.



4. Sous **Actions de l'appareil**, cliquez sur **Effacer les données d'entreprise**.



Dans une configuration effectuée avec succès, les données d'entreprise sont effacées sur l'appareil.

Intégration aux fonctionnalités Apple Éducation

January 10, 2022

Vous pouvez utiliser XenMobile en tant que solution de gestion d'appareils mobiles (MDM) dans un environnement qui utilise Apple Éducation. La prise en charge XenMobile inclut Apple School Manager (ASM) et l'application En classe pour iPad. La stratégie Configuration de l'éducation de XenMobile configure les appareils des enseignants et des étudiants pour une utilisation avec Apple Éducation.

Vous devez fournir des iPad préconfigurés et supervisés aux instructeurs et aux étudiants. Cette configuration inclut l'inscription à ASM dans XenMobile, un compte Apple ID géré configuré avec un nouveau mot de passe et les applications et iBooks d'achat en volume requis.

Voici une vue d'ensemble de la prise en charge par XenMobile des fonctionnalités d'Apple Éducation.

Apple School Manager

ASM est un service qui vous permet de configurer, déployer et gérer les appareils iOS (iPadOS) et les ordinateurs portables macOS utilisés dans les établissements scolaires. ASM inclut un portail Web qui permet aux administrateurs informatiques d'effectuer les opérations suivantes :

- Attribuer des appareils du programme de déploiement d'Apple à différents serveurs MDM.
- Acheter des licences d'achat en volume pour les applications et les iBooks.
- Créer des **identifiants Apple ID gérés** en bloc. Ces identifiants Apple ID personnalisés fournissent un accès aux services Apple tels que le stockage des documents dans iCloud Drive et l'inscription aux cours de l'Apple App Store.

Vous pouvez ajouter plusieurs comptes ASM à XenMobile. Par exemple, cette fonctionnalité vous permet d'utiliser différents paramètres d'inscription ainsi que les options de l'Assistant d'installation par unité ou département d'éducation. Vous pouvez associer des comptes ASM à différentes stratégies.

Une fois que vous avez ajouté un compte ASM à la console XenMobile, XenMobile récupère les informations de classes et de listes. Lors de la configuration de l'appareil, XenMobile :

- inscrit les appareils ;
- installe les ressources que vous avez configurées pour le déploiement, telles que les stratégies (Configuration de l'éducation, Disposition de l'écran d'accueil, etc.) ;
- installe les applications et les iBooks achetés via l'achat en volume.

Vous devez ensuite fournir les appareils préconfigurés aux instructeurs et aux étudiants. Si un appareil est perdu ou volé, vous pouvez utiliser la fonctionnalité Mode perdu MDM pour verrouiller et localiser les appareils.

Application En classe pour iPad

L'application En classe pour iPad permet aux enseignants de se connecter aux appareils des étudiants et de les gérer. Vous pouvez afficher les écrans de l'appareil, ouvrir des applications sur les iPads, ainsi que partager et ouvrir des liens Web.

L'application En classe est gratuite dans l'App Store. Chargez l'application sur la console XenMobile. Utilisez ensuite la stratégie Configuration de l'éducation pour configurer l'application En classe, que vous déployez sur les appareils des enseignants.

Pour plus d'informations sur les fonctionnalités d'Apple Éducation, consultez le site Éducation d'Apple et le Guide de déploiement dans le secteur de l'éducation d'Apple sur ce site.

Conditions préalables

- Citrix Gateway
- Profil d'inscription configuré pour MDM+MAM.
- Apple iPad 3ème génération (version minimale) ou iPad Mini, avec iOS 9.3 (version minimale)

> **Remarque :**
>
> XenMobile ne valide pas les comptes d'utilisateur ASM auprès d'Active Directory ou de LDAP. Toutefois, vous pouvez connecter XenMobile à Active Directory ou LDAP pour une gestion des utilisateurs et des appareils non liés à des enseignants ou des étudiants ASM. Par exemple, vous pouvez utiliser Active Directory pour fournir Secure Mail et Secure Web à d'autres membres d'ASM, tels que les administrateurs et responsables informatiques.
>
> Étant donné que les étudiants et les instructeurs ASM sont des utilisateurs locaux, il n'est pas nécessaire de déployer Citrix Secure Hub sur leurs appareils.
>
> L'inscription MAM qui comprend l'authentification Citrix Gateway ne prend pas en charge les utilisateurs locaux (uniquement les utilisateurs Active Directory). Par conséquent, XenMobile déploie uniquement les applications et iBooks d'achat en volume requis sur les appareils enseignant et étudiant.

Conditions préalables pour les iPad partagés

- iPad Pro, iPad 5ème génération, iPad Air 2 ou ultérieur et iPad mini 4 ou ultérieur
- Au moins 32 Go de stockage
- Supervisé

Configurer Apple School Manager et XenMobile

Après avoir acheté des iPad auprès d'Apple ou de revendeurs ou d'opérateurs autorisés d'Apple : suivez le workflow de cette section pour configurer votre compte et vos appareils ASM. Ce workflow comprend des étapes à effectuer dans le portail ASM et dans la console XenMobile.

Suivez ces instructions pour configurer votre intégration pour tous les iPad que vous utilisez dans un modèle appareil individuel (un iPad par élève) ou pour les iPad d'instructeur (non partagés). Pour configurer les iPad partagés, consultez la section Configurer les iPad partagés.

Étape 1 : Créer votre compte Apple School Manager et suivre l'Assistant d'installation

Si vous prévoyez d'effectuer une mise à niveau depuis le programme de déploiement Apple, consultez l'article de l'assistance Apple, Mettre à niveau votre établissement vers ASM. Pour créer votre compte

ASM, accédez à https://school.apple.com/ et suivez les instructions d'inscription. Lors de votre première connexion à ASM, l'Assistant d'installation s'ouvre.

- Pour plus d'informations sur la configuration requise pour ASM, l'Assistant réglages et les tâches de gestion, veuillez consulter le guide de l'utilisateur d'Apple School Manager.
- Lorsque vous configurez ASM, utilisez un nom de domaine différent du nom de domaine d'Active Directory. Par exemple, ajoutez au nom de domaine ASM un préfixe tel que `appleid`.
- Lorsque vous connectez ASM à vos données de liste, ASM crée des identifiants Apple ID gérés pour les instructeurs et les étudiants. Vos données de liste comprennent les instructeurs, les étudiants et les classes. Pour plus d'informations sur l'ajout de données de liste à ASM, reportez-vous au Guide de l'utilisateur d'ASM, référencé précédemment.
- Vous pouvez personnaliser le format des identifiants Apple ID pour votre établissement, comme décrit dans le Guide de l'utilisateur d'ASM, référencé précédemment.

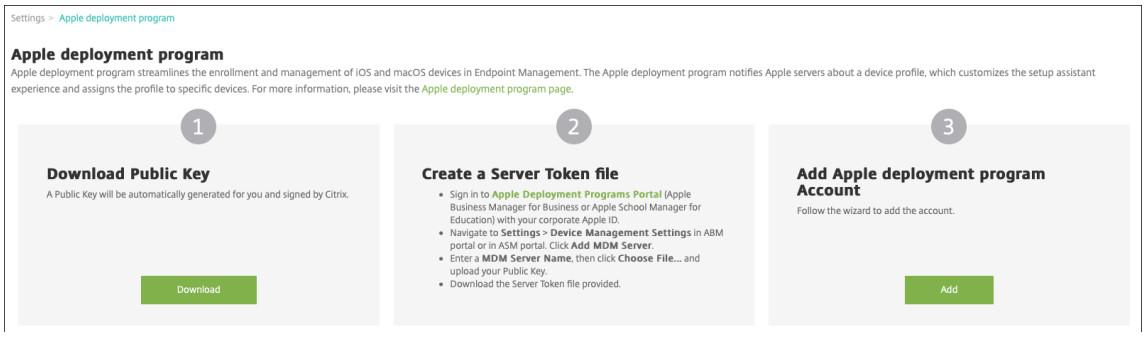
  > **Important :**
  >
  > Ne modifiez pas les identifiants Apple ID gérés après avoir importé des informations ASM dans XenMobile.

- Si vous avez acheté des appareils auprès de revendeurs ou d'opérateurs, liez ces appareils à ASM. Pour plus d'informations, reportez-vous au Guide de l'utilisateur d'ASM, référencé précédemment.

Étape 2 : Configurer XenMobile en tant que serveur MDM pour Apple School Manager et configurer les attributions d'appareils

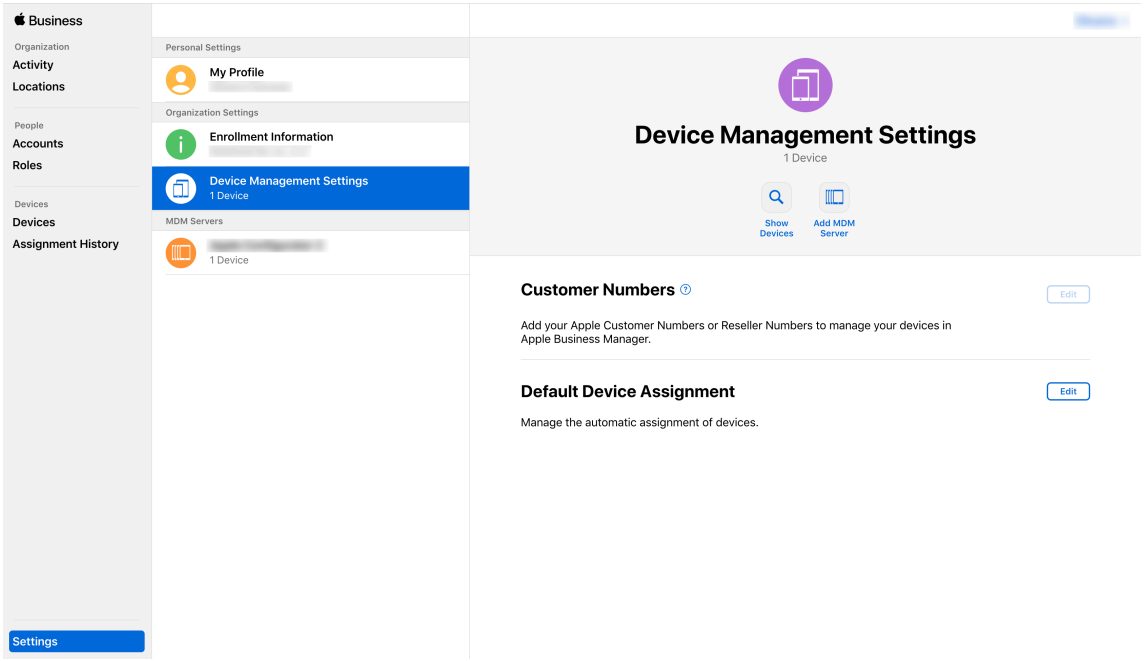
Le portail ASM comprend un onglet **Serveurs MDM**. Vous devez obtenir le fichier de clé publique depuis XenMobile pour effectuer cette configuration.

1. Téléchargez la clé publique de votre XenMobile sur votre ordinateur local : dans la console XenMobile, accédez à **Paramètres > Programme de déploiement d'Apple**.

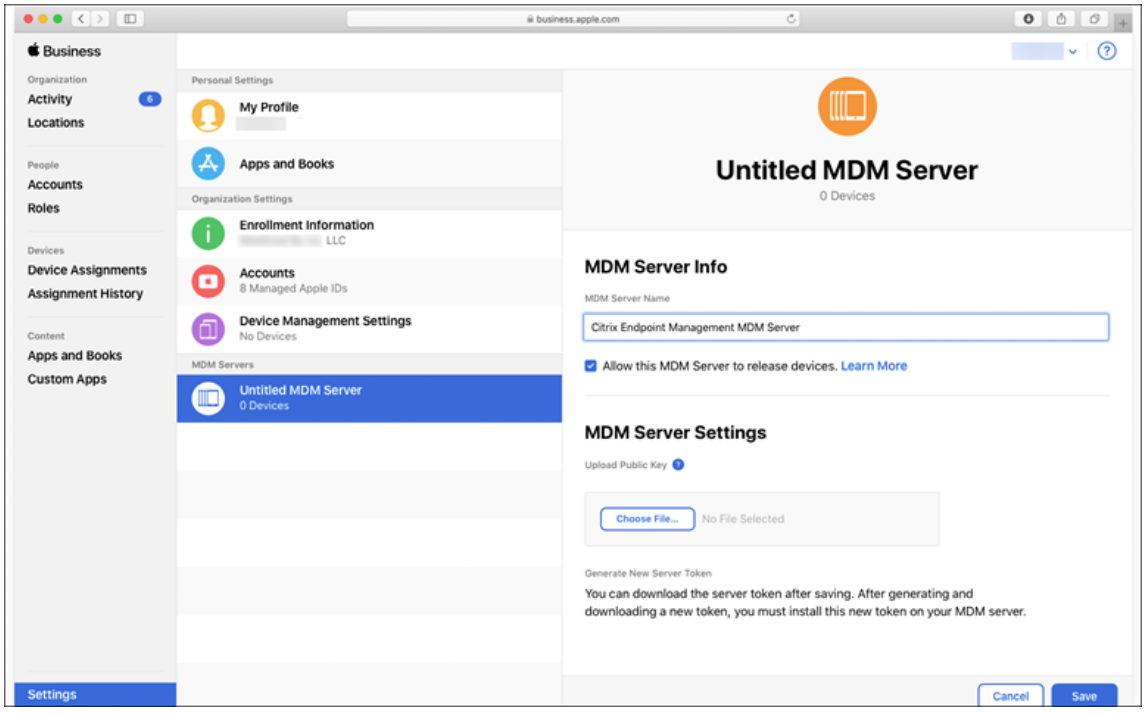


2. Sous **Télécharger la clé publique**, cliquez sur **Télécharger** et enregistrez le fichier PEM.

3. Dans le portail **Apple School Manager**, cliquez sur **Paramètres**, puis sur **Réglages de la gestion des appareils**. Cliquez sur **Ajouter un serveur MDM**.

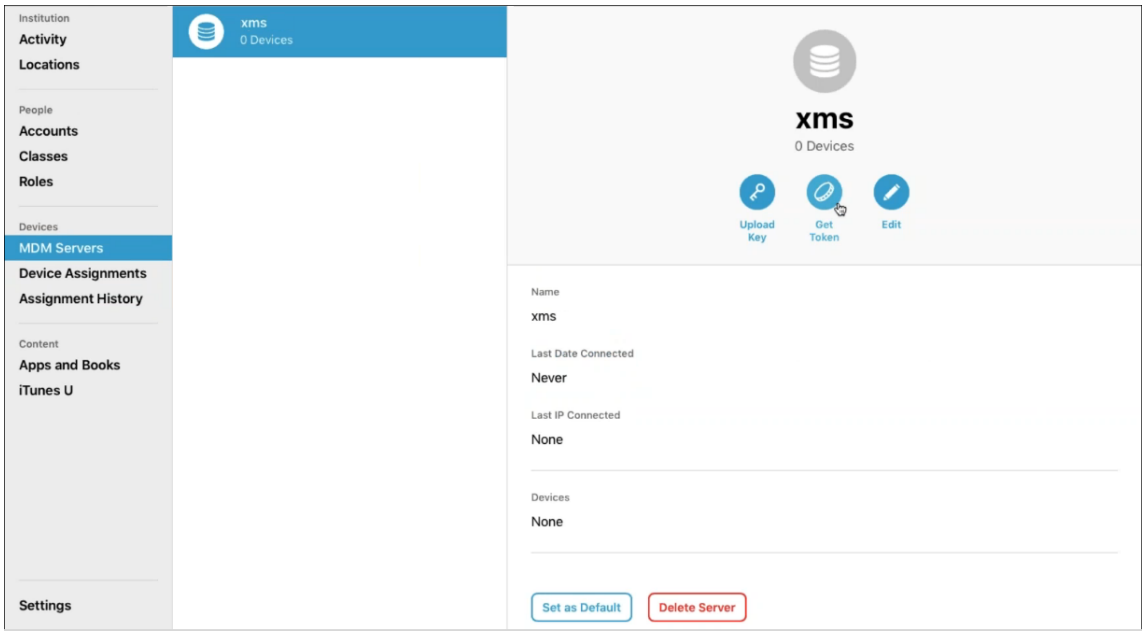


4. Tapez un nom pour XenMobile. Le nom de serveur que vous entrez vous servira de référence et ne correspond pas au nom ou à l'adresse URL du serveur. Sous **Charger la clé publique**, cliquez sur **Choisir un fichier**.



5. Chargez la clé publique que vous avez téléchargée à partir de XenMobile et cliquez sur **Enregistrer**.

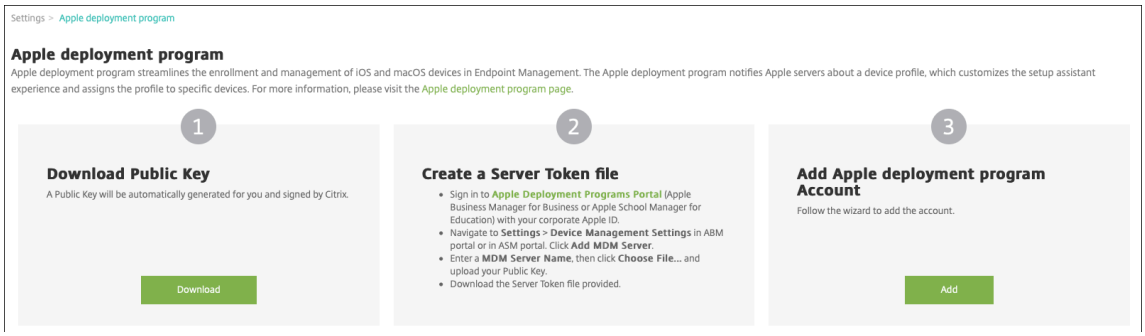
6. Générez un jeton de serveur : cliquez sur **Télécharger le jeton** pour télécharger le fichier de jeton de serveur sur votre ordinateur.



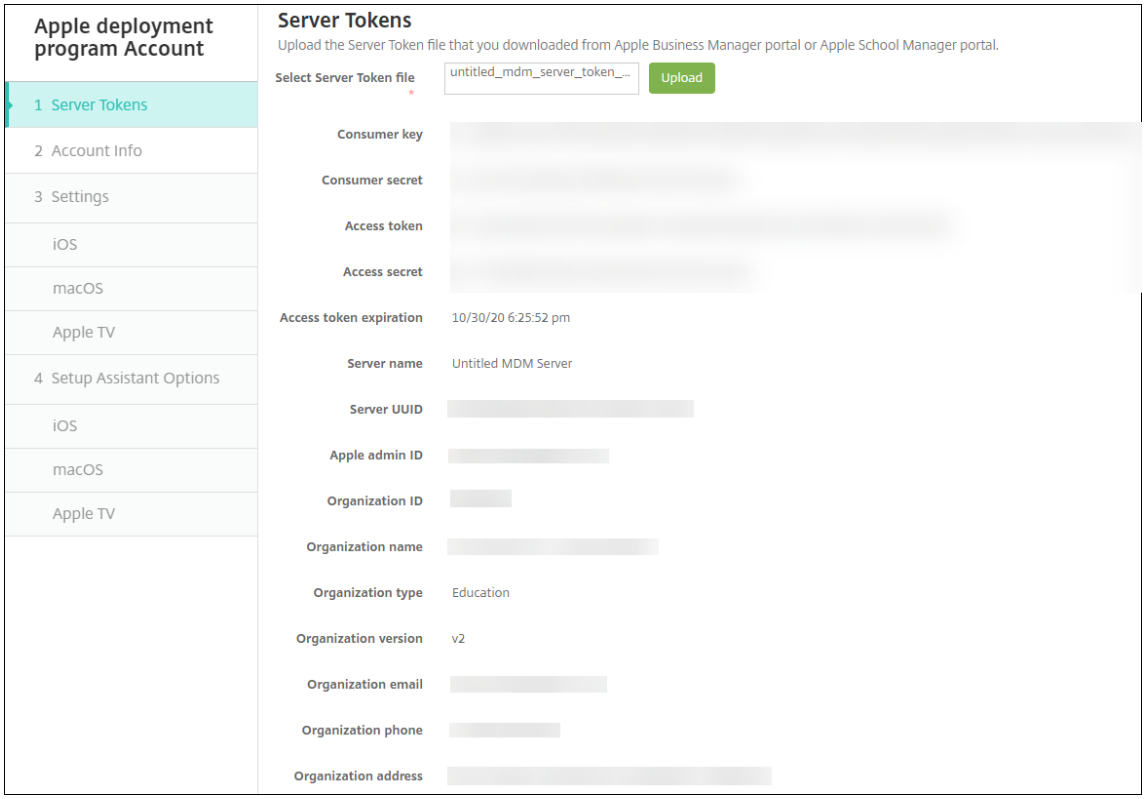
7. Sous **Attribution d'appareils par défaut**, cliquez sur **Modifier**. Choisissez la manière dont vous souhaitez attribuer les appareils et fournissez les informations requises. Pour de plus amples informations, consultez le Guide de l'utilisateur d'ASM.

Étape 3 : Ajouter le compte Apple School Manager à XenMobile

1. Dans la console XenMobile accédez à **Paramètres > Programme de déploiement d'Apple** et sous **Ajouter un compte de programme de déploiement Apple**, cliquez sur **Ajouter** .



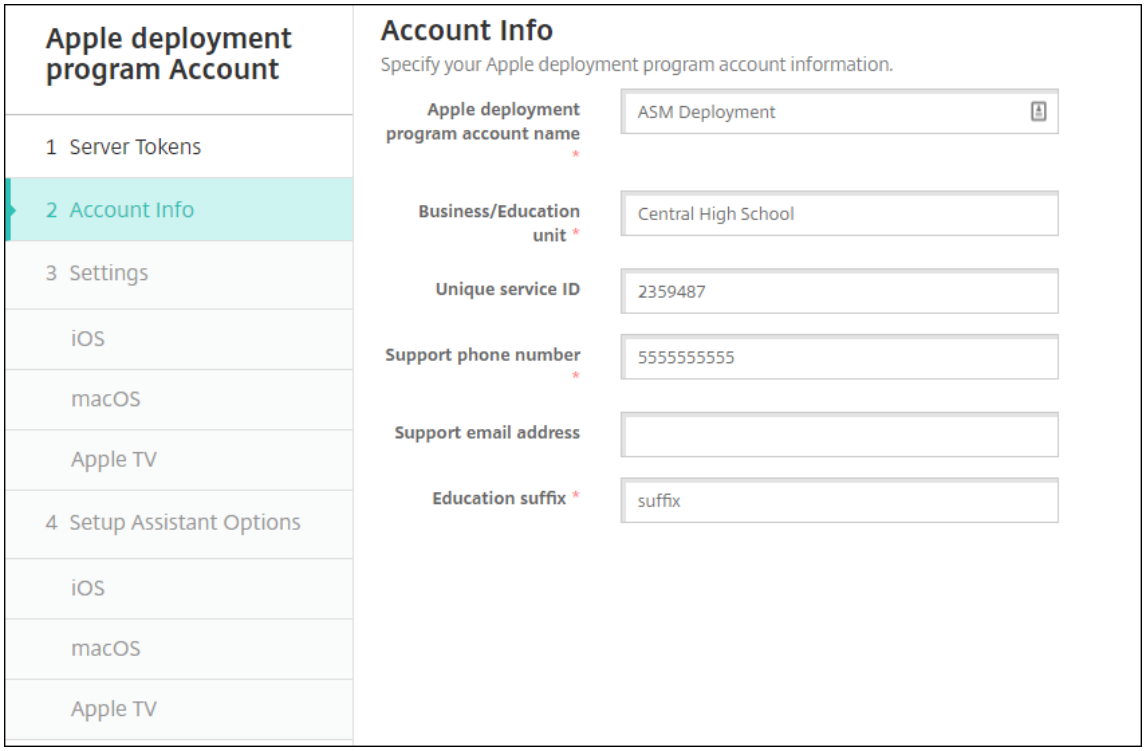
2. Sur la page **Jetons de serveur**, cliquez sur **Charger** et choisissez le fichier de jeton de serveur (fichier P7M) que vous avez téléchargé à partir du portail ASM. Les informations de jeton s'affichent.



Remarques :

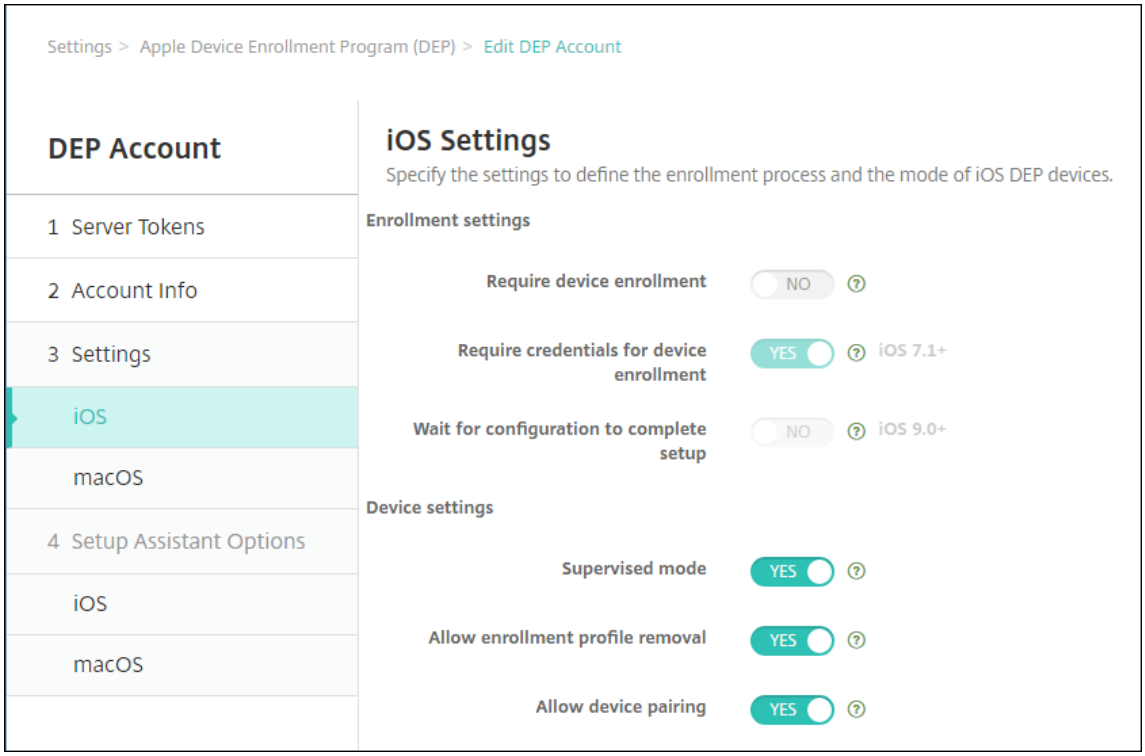
- L'**ID d'organisation** est votre ID client pour le programme de déploiement d'Apple.
- Les comptes ASM sont associés au **type d'organisation Éducation** et à la **version d'organisation v2**.

3. Sur la page **Infos sur le compte**, spécifiez ces paramètres :



- **Nom du compte du programme de déploiement Apple :** nom unique pour ce compte du programme de déploiement d'Apple. Utilisez des noms qui reflètent la manière dont vous organisez les comptes du programme de déploiement d'Apple, par pays ou hiérarchie organisationnelle par exemple.
- **Division/Département:** unité ou département d'éducation pour l'attribution de l'appareil. Ce champ est obligatoire.
- **ID de service unique :** ID unique (facultatif) pour vous aider à identifier le compte.
- **Numéro de téléphone de l'assistance :** numéro de téléphone d'assistance que les utilisateurs peuvent appeler pour obtenir de l'aide au cours de la configuration. Ce champ est obligatoire.
- **Adresse e-mail de l'assistance :** adresse e-mail d'assistance (facultatif) que peuvent utiliser les utilisateurs.
- **Suffixe d'éducation :** identifie les classes pour un compte du programme de déploiement ASM donné. (Le suffixe d'achat en volume signale les applications et les iBooks pour un compte d'achat en volume donné.) Il est recommandé d'utiliser le même suffixe pour les deux comptes, le programme de déploiement ASM et l'achat en volume ASM.

4. Cliquez sur **Suivant**. Dans **Paramètres iOS**, spécifiez les paramètres suivants :



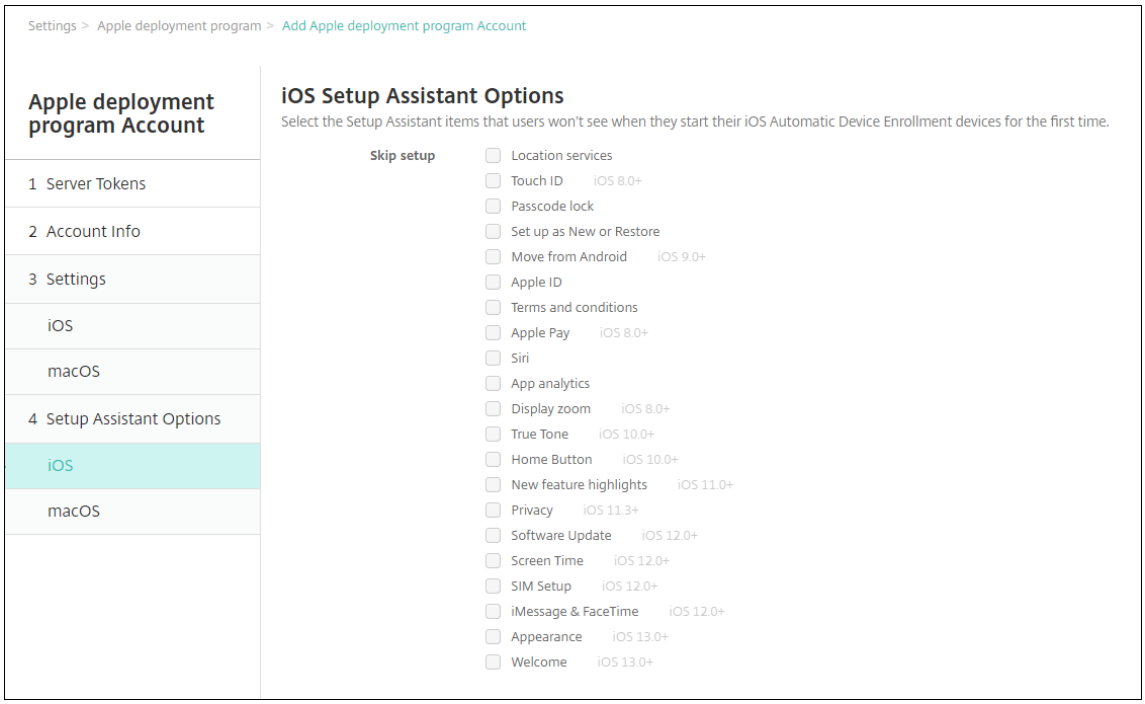
- **Paramètres d'inscription**
  - **Exiger l'inscription des appareils :** cette option oblige les utilisateurs à inscrire leurs appareils. Définissez le paramètre sur **Non**.
  - **Exiger des informations d'identification pour l'inscription d'appareils :** les utilisateurs doivent entrer leurs informations d'identification lors de la configuration du programme de déploiement d'Apple. Pour l'intégration d'ASM à XenMobile, ce paramètre est défini sur **Oui** par défaut et ne peut pas être modifié. Le programme de déploiement d'Apple requiert des informations d'identification pour l'inscription d'appareils.
  - **Attendre la fin de l'installation :** indiquez si les appareils des utilisateurs doivent rester dans le mode Assistant d'installation jusqu'à ce que toutes les ressources MDM soient déployées sur l'appareil. Pour l'intégration d'ASM à XenMobile, ce paramètre est **Non** par défaut. La documentation Apple indique que les commandes suivantes peuvent ne pas fonctionner lorsqu'un appareil est en mode Assistant d'installation :
    - InviteToProgram
    - InstallApplication
    - InstallMedia
    - ApplyRedemptionCode
- **Paramètres de l'appareil**
  - **Mode supervisé :** place les appareils iOS en mode supervisé. Ne modifiez pas la

valeur par défaut, **Oui**. Pour de plus amples informations sur le placement d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

- **Mode partagé :** active le mode partagé sur les iPad. Le partage ne peut pas être activé sur les appareils qui ne présentent pas la configuration minimale requise.
- **Autoriser la suppression du profil d'inscription :** pour l'intégration d'ASM, autorisez l'utilisateur à supprimer le profil d'inscription de l'appareil. Définissez le paramètre sur **Oui**.
- **Autoriser le couplage de l'appareil :** pour l'intégration d'ASM, autorisez le couplage pour pouvoir gérer les appareils via l'Apple App Store et Apple Configurator. Définissez le paramètre sur **Oui**.

5. Dans **Options de l'assistant d'installation iOS**, sélectionnez les étapes de l'Assistant d'installation iOS à ignorer lorsque les utilisateurs démarreront leurs appareils pour la première fois. Par défaut, l'Assistant d'installation comprend toutes les étapes. La suppression d'étapes de l'Assistant d'installation peut simplifier l'expérience utilisateur.

> **Important :**
>
> Citrix vous recommande fortement d'inclure les étapes **Apple ID** et **Termes et conditions**. Ces étapes permettent aux instructeurs et aux étudiants de fournir un nouveau mot de passe pour leur identifiant Apple ID géré et d'accepter les conditions générales.

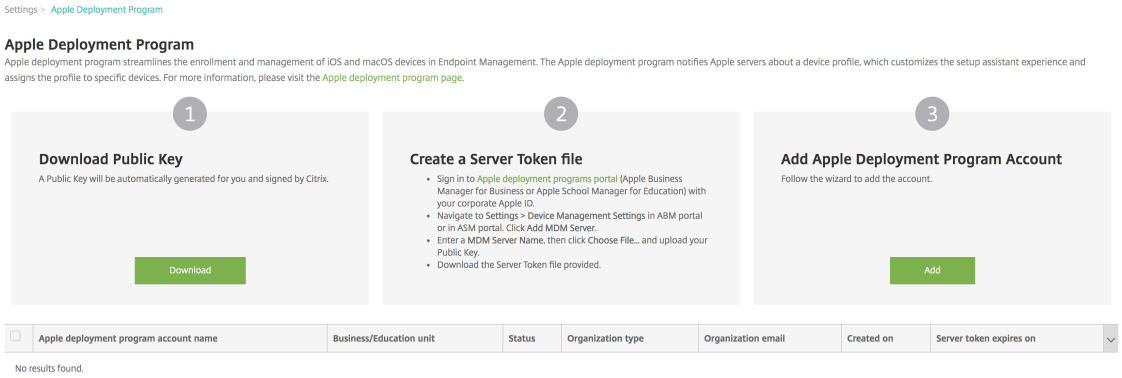


- **Services de localisation :** configurez le service de localisation sur l'appareil.

- **Touch ID :** configurez Touch ID dans iOS.
- **Verrouillage par code secret :** créez un code secret pour l'appareil.
- **Définir comme nouveau ou restaurer :** configurez l'appareil comme nouveau ou restaurez-le à partir d'une sauvegarde de l'Apple App Store ou d'iCloud.
- **Déplacer depuis Android :** activez le transfert des données à partir d'un appareil Android vers un appareil iOS. Cette option est disponible uniquement lorsque **Définir comme nouveau ou Restaurer** est sélectionné (sinon, cette étape est ignorée).
- **Apple ID :** configurez un compte Apple ID pour l'appareil. Citrix recommande de sélectionner la case à cocher pour inclure cette étape.
- **Termes et conditions :** exigez que l'utilisateur accepte les termes et conditions pour utiliser l'appareil. Citrix recommande de sélectionner la case à cocher pour inclure cette étape.
- **Apple Pay :** configurez Apple Pay dans iOS.
- **Siri :** utilisez ou non Siri sur l'appareil.
- **Analyse de l'application :** configurez cette option si vous souhaitez partager les données d'incidents et les statistiques d'utilisation avec Apple.
- **Zoom d'affichage :** définissez la résolution d'affichage (standard ou zoom) sur les appareils iOS.
- **True Tone :** configurez l'affichage de True Tone sur les appareils iOS.
- **Bouton d'accueil :** configurez la sensibilité de l'écran du bouton d'accueil.
- **Présentation des nouvelles fonctionnalités :** configurez les écrans d'information d'intégration, Accès au Dock à partir de n'importe quel emplacement et Basculement entre applications récentes sur les appareils iOS 11.0 (version minimale).
- **Confidentialité :** empêche les utilisateurs de voir les données et le volet de confidentialité lors de la configuration d'appareils du programme de déploiement d'Apple. Pour iOS 11.3 et versions ultérieures.
- **Mise à jour logicielle :** empêche l'utilisateur de voir l'écran de mise à jour logicielle pendant la configuration des appareils du programme de déploiement d'Apple. Pour iOS 12.0 et versions ultérieures.
- **ScreenTime :** empêche l'utilisateur de voir l'écran Screen Time pendant la configuration des appareils du programme de déploiement d'Apple. Pour iOS 12.0 et versions ultérieures.
- **Configuration de la carte SIM :** empêche l'utilisateur de voir l'écran Ajouter forfait de données pendant la configuration des appareils du programme de déploiement d'Apple. Pour iOS 12.0 et versions ultérieures.
- **iMessage & FaceTime :** empêche l'utilisateur de voir l'écran iMessage & FaceTime pendant la configuration des appareils du programme de déploiement d'Apple. Pour iOS 12.0 et versions ultérieures.

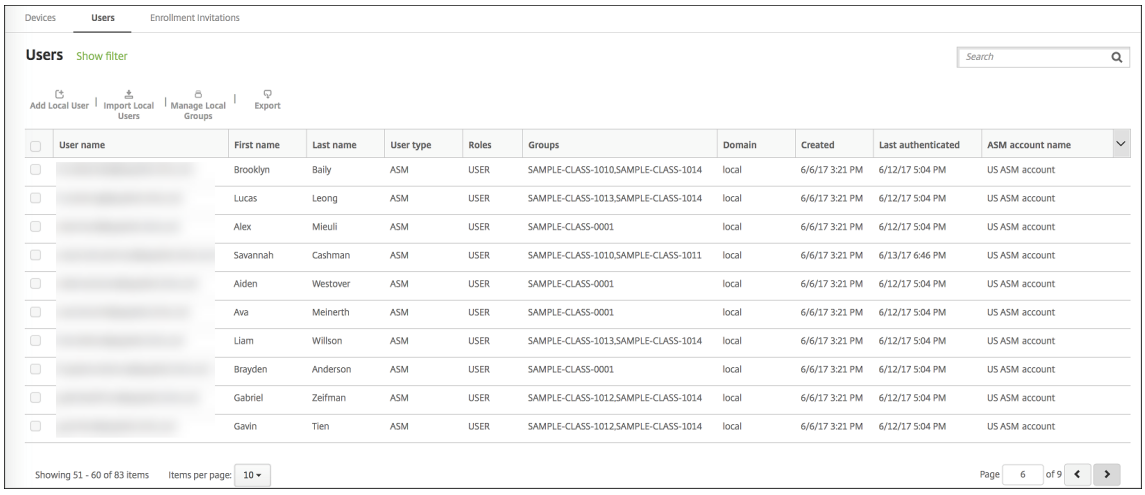
6. Le compte apparaît dans **Paramètres > Programme de déploiement d'Apple**. Pour tester la

connexion entre XenMobile et votre compte ASM, sélectionnez le compte et cliquez sur **Tester la connectivité**.



Un message d'état s'affiche.

Après quelques minutes, les comptes utilisateur d'ASM s'affichent sur la page **Gérer > Utilisateurs**. XenMobile crée des comptes d'utilisateur locaux basés sur l'identifiant Apple ID importé géré pour chaque utilisateur. Dans l'exemple suivant, le préfixe du nom de domaine des identifiants Apple ID personnalisés pour les comptes utilisateur est `appleid`.

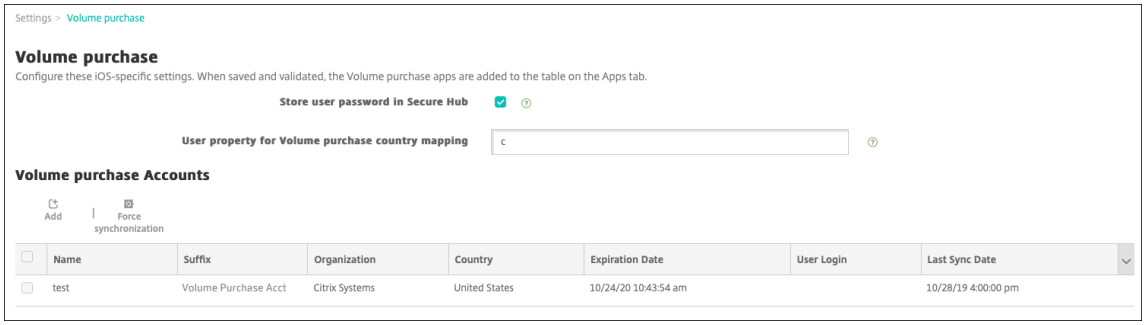


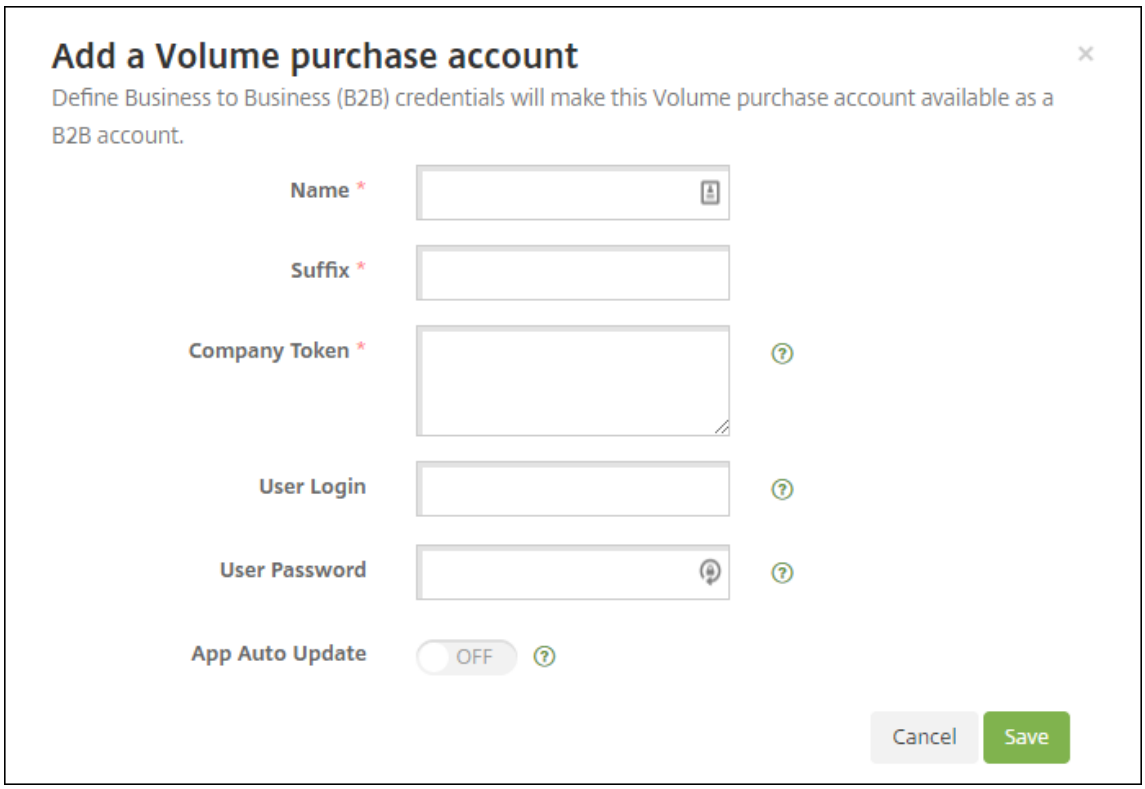
Pour rechercher tous les utilisateurs d'un compte ASM donné, entrez le nom du compte dans le filtre de recherche utilisateur.

Étape 4 : Configurer un compte d'achat en volume Éducation pour Apple School Manager

Dans cette section, vous pointez XenMobile vers le compte d'achat en volume utilisé pour acheter des licences d'achat en volume pour les applications et les iBooks.

1. Pour configurer un compte d'achat en volume Éducation pour ASM, suivez les instructions de la section Achats en volume d'Apple. L'écran Ajouter un compte d'achat en volume demande un jeton d'entreprise. Téléchargez votre jeton directement à partir de votre compte d'achat en volume Éducation et collez-le dans l'écran **Ajouter un compte d'achat en volume**.





2. Patientez quelques minutes pendant l'importation de licences d'achat en volume dans XenMobile.

Étape 5 : Ajouter des mots de passe pour les utilisateurs Apple School Manager

Après l'ajout d'un compte ASM, XenMobile importe les classes et les utilisateurs à partir d'ASM. XenMobile traite les classes en tant que groupes locaux et utilise le terme « groupe » dans la console. Si une classe a un nom de groupe dans ASM, XenMobile attribue le nom du groupe à la classe. Sinon, XenMobile utilise l'ID du système source pour le nom du groupe. XenMobile n'utilise pas le nom du cours pour le nom de classe étant donné que les noms de cours dans ASM ne sont pas uniques.

XenMobile utilise les identifiants Apple ID gérés pour créer des utilisateurs locaux avec le type utilisateur **ASM**. Les utilisateurs sont locaux, car ASM crée les informations d'identification indépendamment de toutes les sources de données externes. Par conséquent, XenMobile n'utilise pas de serveur d'annuaire pour authentifier ces nouveaux utilisateurs.

ASM n'envoie pas de mots de passe utilisateur temporaires à XenMobile. Vous pouvez les importer à partir d'un fichier CSV ou les ajouter manuellement. Pour importer des mots de passe utilisateur temporaires :

1. Obtenez le fichier CSV généré par ASM lorsque vous créez les mots de passe temporaires d'identifiants Apple ID gérés.
2. Modifiez le fichier CSV, en remplaçant les mots de passe temporaires par les nouveaux mots de passe que fournissent les utilisateurs pour s'inscrire à XenMobile. Il n'existe aucune contrainte sur le type de mot de passe dans ce cas.

   Le format d'une entrée dans le fichier CSV est le suivant : `user@appleid.citrix.com`, `Firstname`,`Middle`,`Lastname`,`Password123`!

   Où :

   Utilisateur : `user@appleid.citrix.com`

   Prénom : `Firstname`

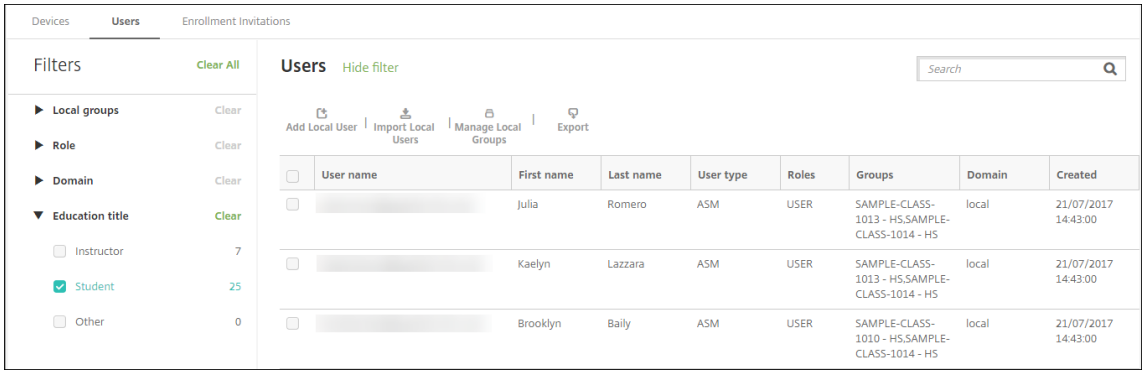
   Deuxième prénom : `Middle`

   Nom : `Lastname`

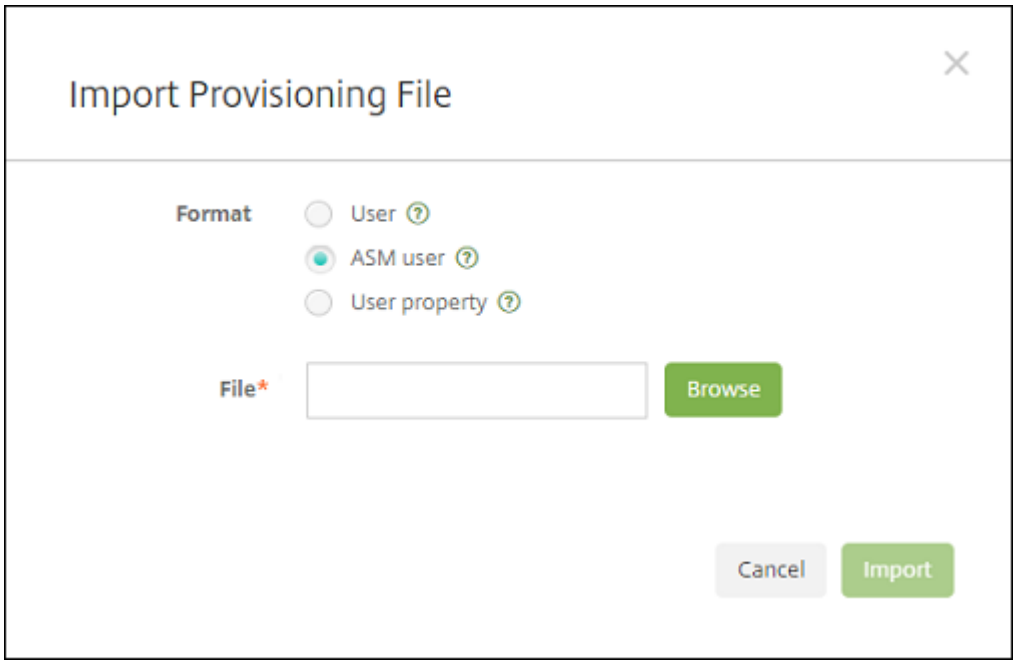
   Mot de passe : `Password123`!
3. Dans la console XenMobile, cliquez sur **Gérer > Utilisateurs**. La page **Utilisateurs** s'affiche.

   L'écran **Gérer > Utilisateurs** suivant présente un exemple de liste d'utilisateurs importée à partir d'ASM. Dans la liste **Utilisateurs** :

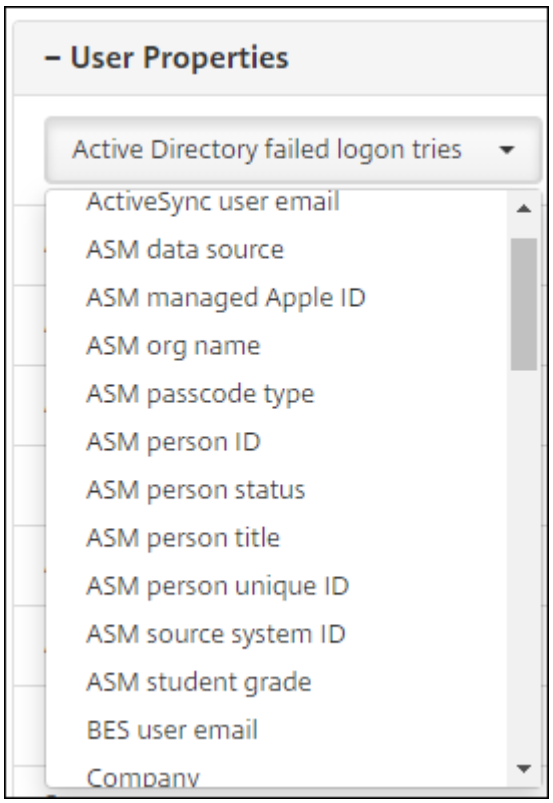
   - L'option **Nom d'utilisateur** affiche l'identifiant Apple ID géré.
   - Le type d'utilisateur est **ASM** pour indiquer que le compte provient d'ASM.
   - L'option **Groupes** indique les classes.



4. Cliquez sur **Importer des utilisateurs locaux**. La boîte de dialogue **Importer le fichier de provisioning** apparaît.
5. Pour le format, choisissez **Utilisateur ASM**, naviguez jusqu'au fichier CSV que vous avez préparé à l'étape 2, puis cliquez sur **Importer**.



6. Pour afficher les propriétés d'un utilisateur local, sélectionnez l'utilisateur, puis cliquez sur **Modifier**.



Outre les propriétés de nom, ces propriétés ASM sont également disponibles :

- **Source de données ASM :** source de données de la classe, telle que **CSV** ou **SFTP**.
- **Identifiant Apple géré par ASM :** un identifiant Apple ID géré peut inclure le nom de votre établissement et votre `appleid`. Par exemple, l'identifiant peut ressembler à johnappleseed@appleid.myschool.edu. XenMobile requiert un identifiant Apple ID géré pour l'authentification.
- **Nom de l'organisation ASM :** nom que vous avez donné au compte dans XenMobile.
- **Type de code d'accès ASM :** stratégie de mot de passe de la personne : **complexe** (mot de passe de huit chiffres et lettres ou plus pour un non-étudiant), **quatre** (chiffres) ou **six** (chiffres).
- **Identifiant unique de l'étudiant ASM :** identifiant de l'utilisateur.
- **Statut de l'étudiant :** spécifie si l'identifiant Apple ID géré est **Actif** ou **Inactif**. Ce statut devient actif une fois que l'utilisateur fournit un nouveau mot de passe pour le compte Apple ID géré.
- **Titre de l'étudiant ASM :** Instructeur, Étudiant ou Autre.
- **Identifiant unique de l'étudiant ASM :** identifiant unique de l'utilisateur.
- **Identifiant du système source ASM :** identifiant de la source système.
- **Niveau scolaire de l'étudiant ASM :** informations sur le niveau scolaire de l'étudiant (non utilisé par les instructeurs).

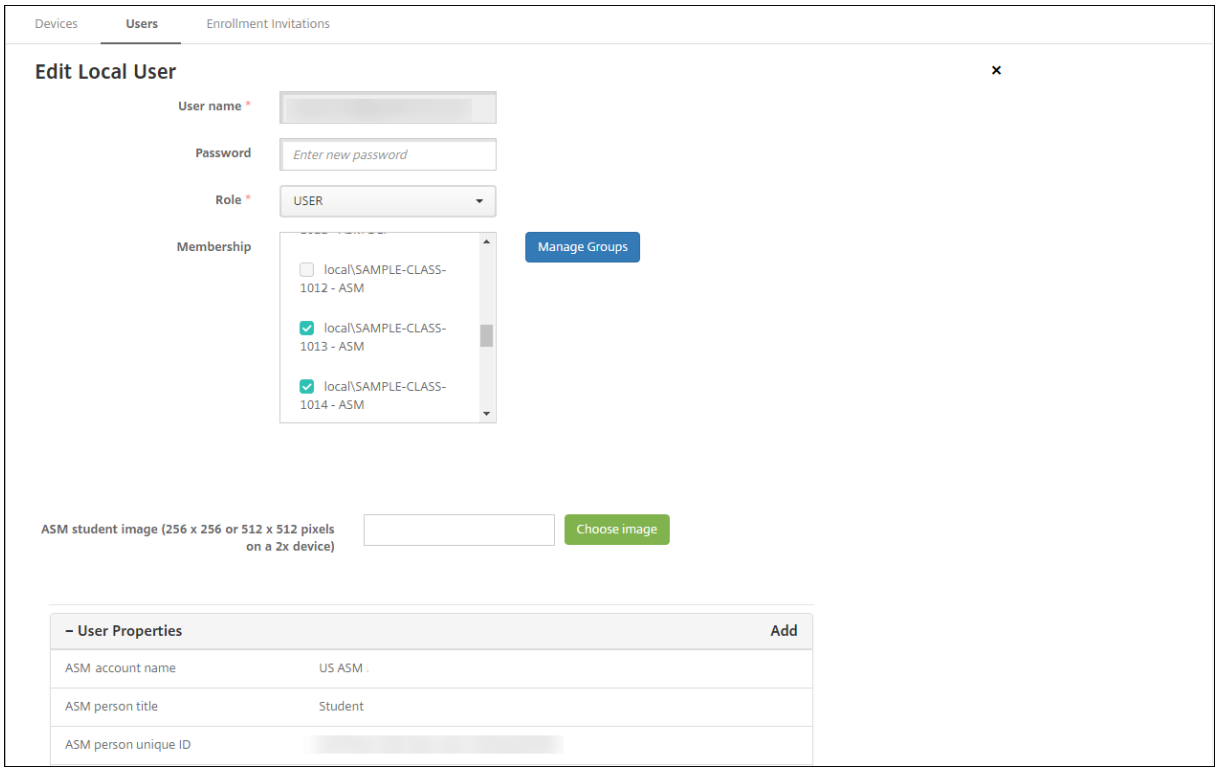
Étape 6 : Ajouter des photos des étudiants (facultatif)

Vous pouvez ajouter une photo de chaque étudiant. Si les instructeurs utilisent l'application En classe d'Apple, les photos s'affichent dans cette application.

Recommandé pour les photos :

- Résolution : 256 x 256 pixels (ou 512 x 512 pixels sur un appareil 2x)
- Format : JPEG, PNG ou TIFF

Pour ajouter une photo, accédez à **Gérer > Utilisateurs**, sélectionnez un utilisateur, cliquez sur **Modifier**, puis cliquez sur **Choisir une image**.



Étape 7 : Planifier et ajouter des ressources et des groupes de mise à disposition à XenMobile

Un groupe de mise à disposition spécifie les ressources à déployer vers des catégories d'utilisateurs. Par exemple, vous pouvez créer un groupe de mise à disposition pour instructeurs et étudiants. Éventuellement, vous pouvez créer plusieurs groupes de mise à disposition afin de pouvoir personnaliser les applications, le contenu multimédia et les stratégies envoyés vers différents instructeurs ou étudiants. Vous pouvez créer un ou plusieurs groupes de mise à disposition par classe. Vous pouvez également créer un ou plusieurs groupes de mise à disposition pour les responsables (autre personnel dans votre établissement scolaire).

Les ressources que vous déployez sur les appareils utilisateur comprennent les stratégies d'appareil, les applications d'achat en volume et les iBooks.

- Stratégies d'appareil :

  Si les instructeurs utilisent l'application En classe, la stratégie Configuration de l'éducation est requise. Veillez à consulter les autres stratégies d'appareil pour déterminer la manière dont vous souhaitez configurer et limiter les iPad des instructeurs et des étudiants.

- Applications d'achat en volume :

  XenMobile requiert le déploiement des applications d'achat en volume en tant qu'applications requises pour les utilisateurs Éducation. XenMobile ne prend pas en charge le déploiement de telles applications d'achat en volume en mode facultatif.

  Si vous utilisez l'application En classe d'Apple, déployez-la uniquement sur les appareils des instructeurs.

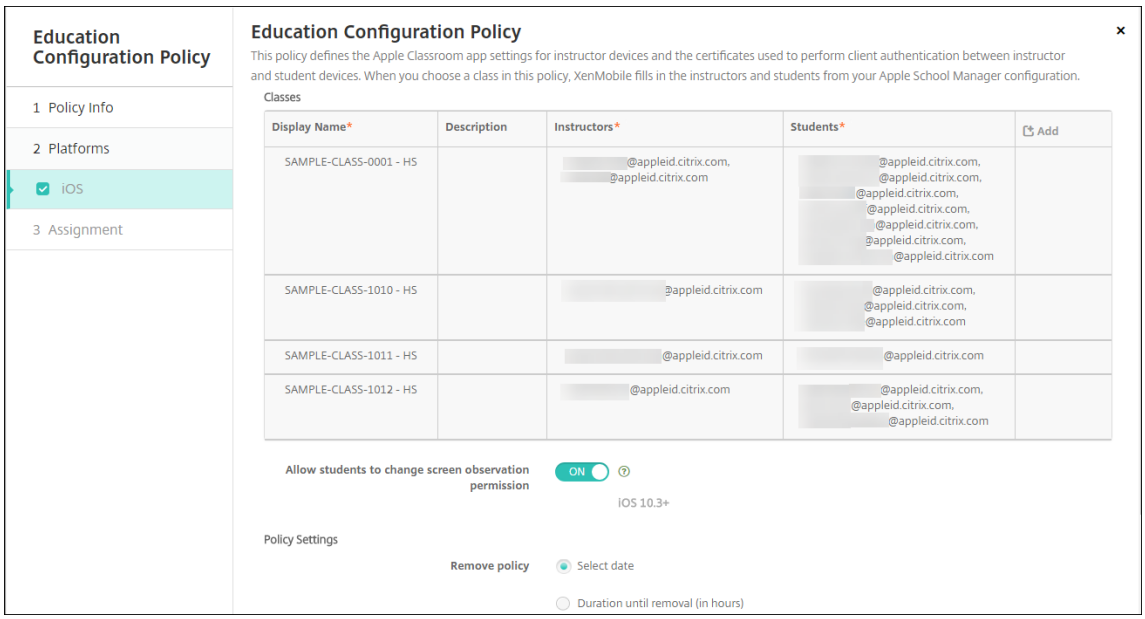
  Déployez toute autre application que vous souhaitez fournir aux instructeurs ou aux étudiants. Cette solution n'utilisant pas l'application Citrix Secure Hub, il n'est pas nécessaire de la déployer vers les instructeurs ou les étudiants.

- iBooks d'achat en volume :

  Une fois que XenMobile s'est connecté à votre compte ASM, vos iBooks achetés s'affichent dans la console XenMobile, dans **Configurer > Média**. Les iBooks répertoriés sur cette page peuvent être ajoutés aux groupes de mise à disposition. XenMobile prend en charge l'ajout d'iBooks en tant que média requis uniquement.

Après avoir planifié les ressources et les groupes de mise à disposition pour les instructeurs et les étudiants, vous pouvez créer ces éléments dans la console XenMobile.

1. Créez les stratégies d'appareil que vous voulez déployer sur les appareils des instructeurs ou des étudiants. Pour de plus amples informations sur la stratégie Configuration de l'éducation, consultez la section Stratégie Configuration de l'éducation.

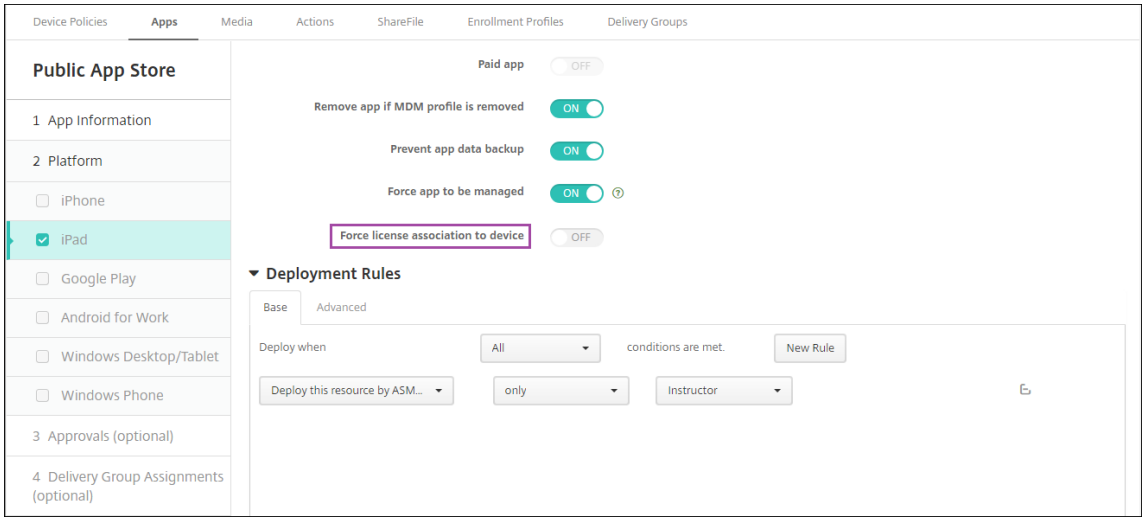


Consultez la section Stratégies d'appareil et les articles de stratégies individuels pour de plus amples informations sur les stratégies d'appareil.

2. Configurez les applications (**Configurer > Applications**) et les iBooks (**Configurer > Média**) :

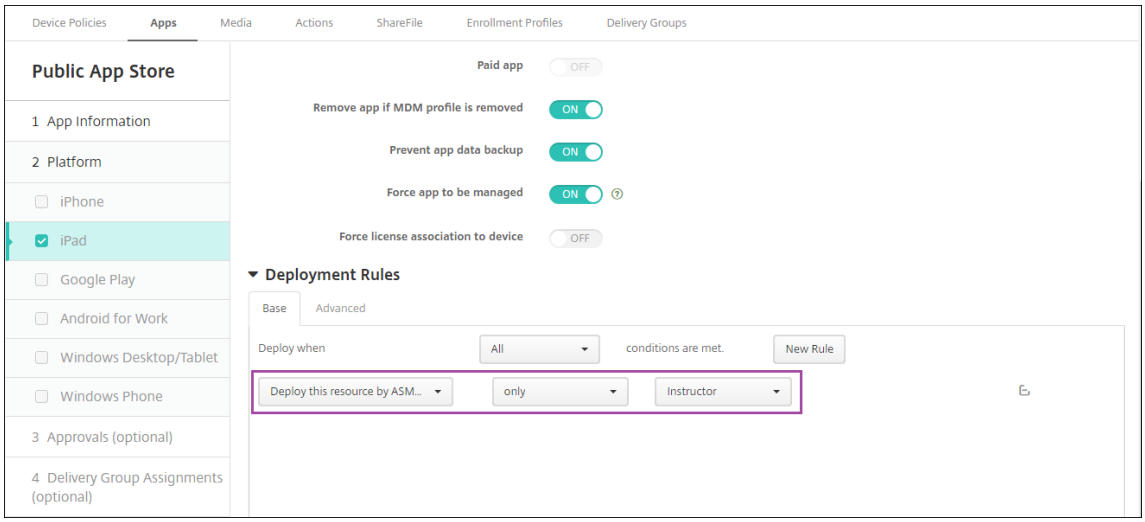
   - Par défaut, XenMobile attribue les applications et les iBooks au niveau de l'utilisateur. Lors du premier déploiement, les instructeurs et les étudiants sont invités à s'enregistrer auprès d'ASM. Après avoir accepté l'invitation, les utilisateurs reçoivent leurs applications et iBooks ASM au cours du déploiement suivant (dans les six heures). Citrix vous recommande de forcer le déploiement d'applications et d'iBooks vers les nouveaux utilisateurs ASM. Pour ce faire, sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.

     Vous pouvez choisir d'attribuer des applications (mais pas des iBooks) au niveau de l'appareil. Pour ce faire, réglez le paramètre **Forcer l'association de licence avec l'appareil** sur **Activé**. Lorsque vous attribuez les applications au niveau de l'appareil, les utilisateurs ne reçoivent pas d'invitation à rejoindre le programme d'achat en volume d'Apple.



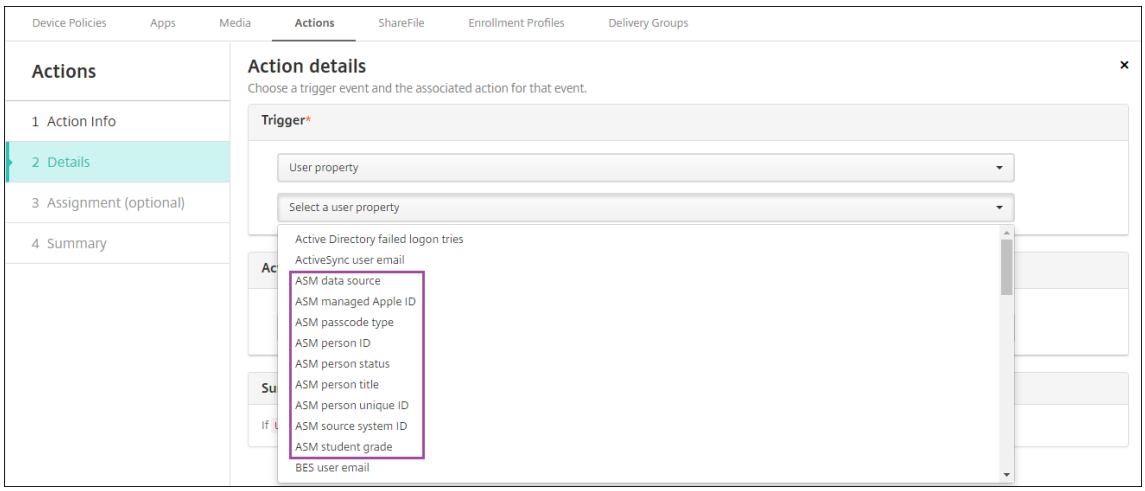
- Pour déployer une application uniquement vers les instructeurs, sélectionnez un groupe de mise à disposition qui comprend uniquement des instructeurs ou utilisez la règle de déploiement suivante :

```
1  Deploy this resource by ASM device type
2  only
3  Instructor
4  <!--NeedCopy-->
```



- Pour obtenir de l'aide sur l'ajout d'applications d'achat en volume, consultez la section Ajouter une application d'un magasin d'applications public.

3. Facultatif. Créez des actions basées sur les propriétés utilisateur ASM. Par exemple, vous pouvez créer une action pour envoyer une notification aux appareils des étudiants lorsqu'une nouvelle application est installée. Éventuellement, vous pouvez créer une action que déclenche une propriété utilisateur, comme illustré dans l'exemple suivant.

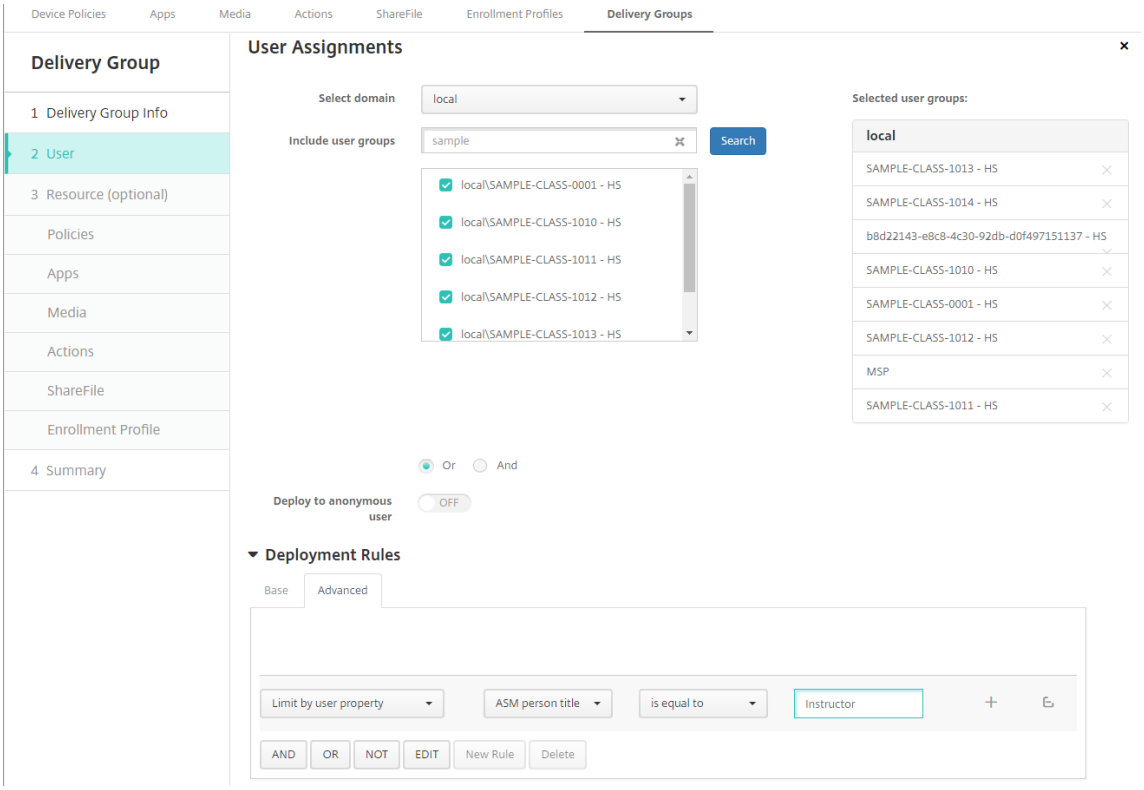


Pour créer une action, accédez à **Configurer > Actions**. Pour de plus amples informations sur la configuration des actions, consultez la section Actions automatisées.

4. Dans **Configurer > Groupes de mise à disposition**, créez des groupes de mise à disposition pour instructeurs et étudiants. Choisissez les classes importées depuis ASM. Créez aussi une règle de déploiement pour instructeurs et étudiants.

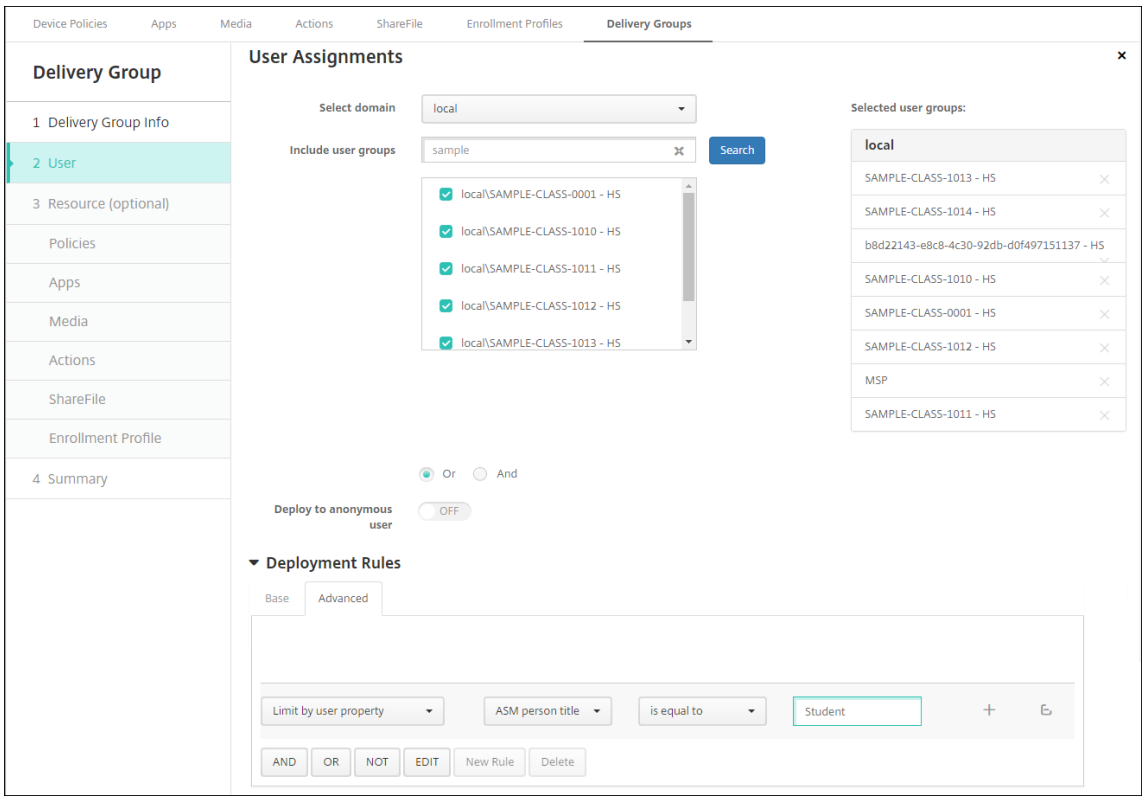
   Par exemple, les affectations utilisateur suivantes sont destinées aux instructeurs. La règle de déploiement est la suivante :

```
Limit by user property
ASM person title
is equal to
Instructor
<!--NeedCopy-->
```

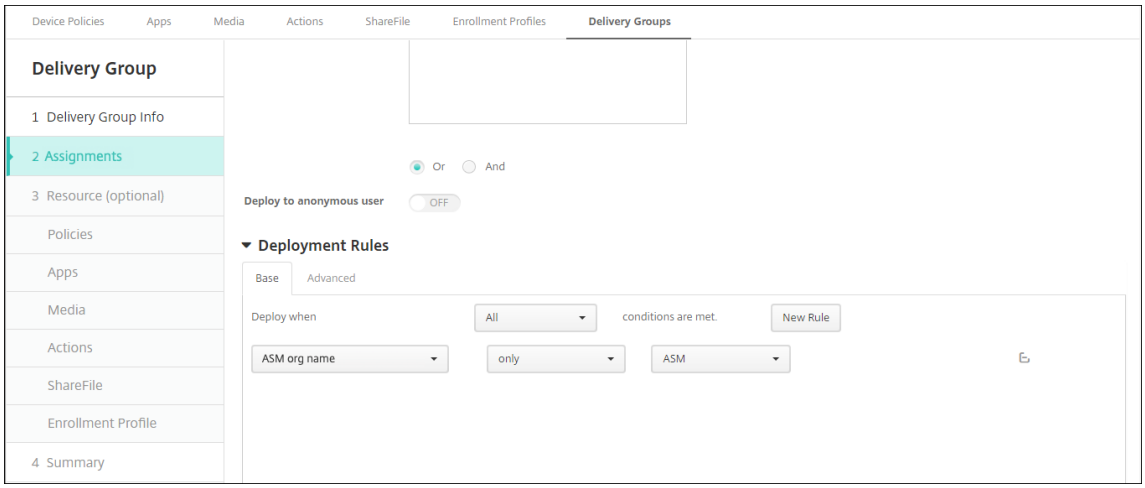



Les affectations utilisateur suivantes sont destinées aux étudiants. La règle de déploiement est la suivante :

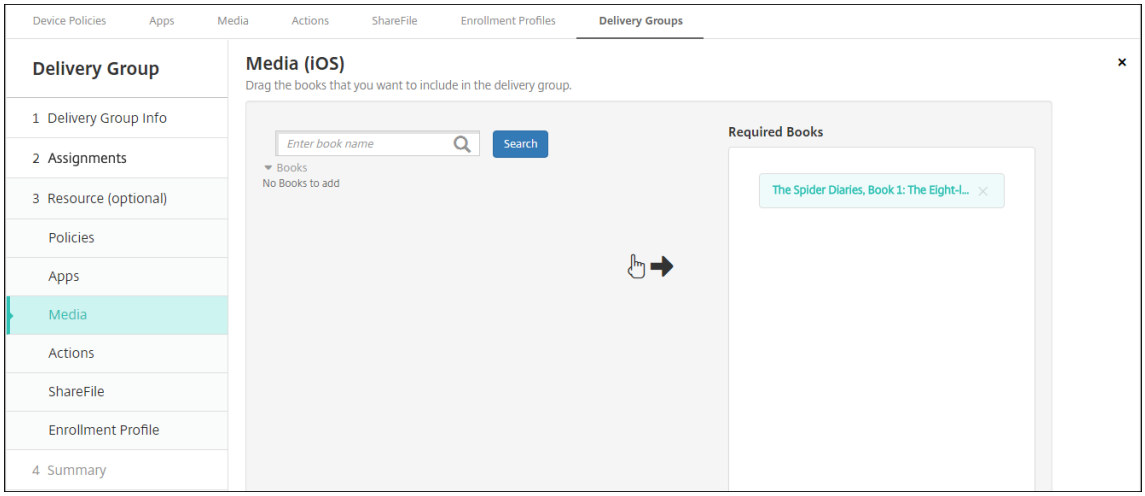
```
Limit by user property
ASM person title
is equal to
Student
<!--NeedCopy-->
```

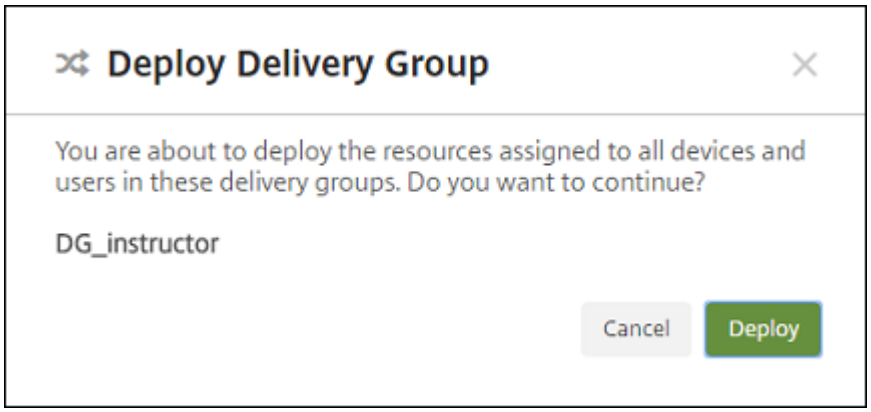
Vous pouvez également filtrer un groupe de mise à disposition à l'aide d'une règle de déploiement basée sur le nom de l'organisation ASM.



5. Attribuez les ressources à des groupes de mise à disposition. L'exemple suivant illustre un iBook contenu dans un groupe de mise à disposition.



L'exemple suivant illustre la boîte de dialogue de confirmation qui s'affiche lorsque vous sélectionnez un groupe de mise à disposition et cliquez sur **Déployer**.



Pour plus d'informations, consultez la section « Pour modifier un groupe de mise à disposition » et « Pour déployer des groupes de mise à disposition » dans Déployer des ressources.

Étape 8 : Tester les inscriptions d'appareil instructeur et étudiant

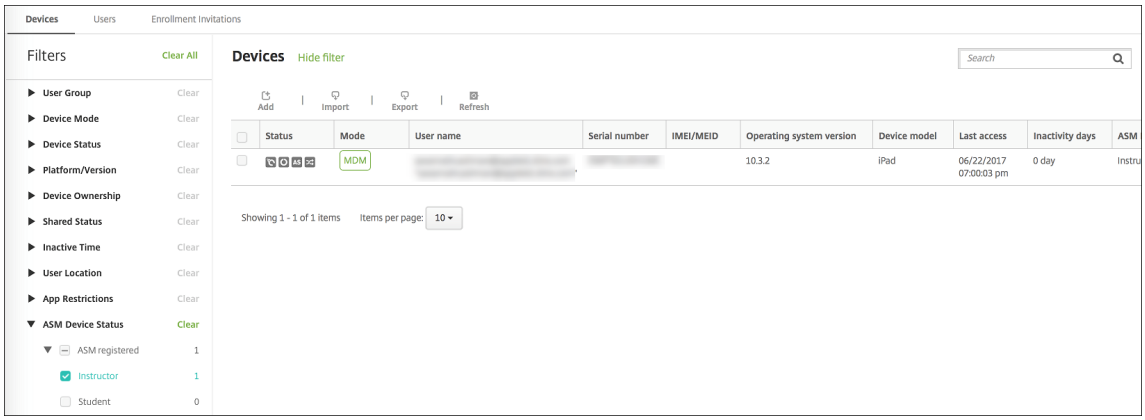
Vous pouvez inscrire des appareils avec une des méthodes suivantes :

- Un administrateur d'établissement scolaire peut inscrire des appareils instructeur et étudiant en utilisant le mot de passe utilisateur que vous pouvez définir dans la console XenMobile. Par conséquent, vous pouvez fournir aux utilisateurs des appareils qui sont déjà configurés avec les applications et les médias.
- Lorsque les utilisateurs reçoivent les appareils, ils peuvent s'inscrire à l'aide du mot de passe utilisateur que vous leur fournissez. Une fois l'inscription terminée, XenMobile envoie les stratégies d'appareil, les applications et le contenu multimédia aux appareils.

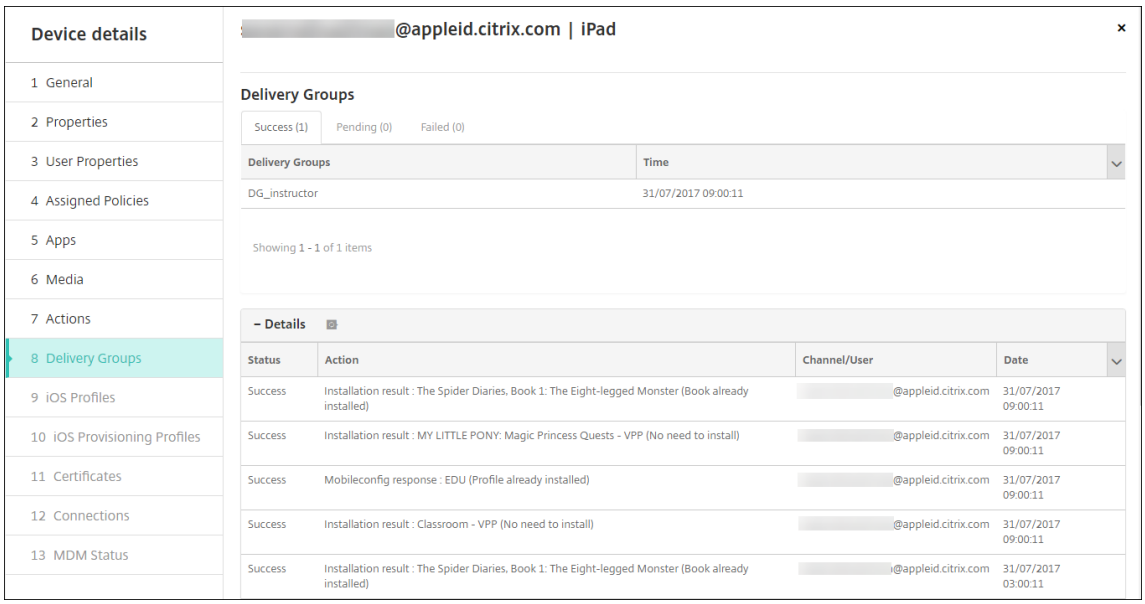
Pour tester l'inscription, utilisez les appareils du programme de déploiement d'Apple liés à ASM.

1. Si les appareils ne sont pas liés à ASM, vous devez effacer leur contenu et leurs paramètres en effectuant une réinitialisation matérielle.
2. Inscrivez un appareil ASM auprès d'un instructeur. Inscrivez ensuite un appareil ASM auprès d'un étudiant.
3. Sur la page **Gérer > Appareils**, vérifiez que les deux appareils ASM sont inscrits dans MDM uniquement.

   Vous pouvez filtrer la page **Appareils** en fonction de l'état de l'appareil ASM : **Enregistré auprès de ASM**, **Partagé avec ASM**, **Instructeur** et **Étudiant**.



4. Pour vérifier que les ressources MDM ont été déployées correctement pour chaque appareil : sélectionnez l'appareil, cliquez sur **Modifier** et vérifiez les différentes pages.



Étape 9 : Distribuer des appareils

Apple vous recommande d'organiser un événement de façon à distribuer les appareils à des instructeurs et à des étudiants.

Si vous ne distribuez pas d'appareils pré-inscrits, vous devez également fournir les éléments suivants à ces utilisateurs :

- Mots de passe XenMobile pour l'inscription
- Mots de passe temporaires ASM pour les identifiants Apple ID gérés

La première expérience utilisateur se présente comme suit.

1. La première fois qu'un utilisateur démarre son appareil après une réinitialisation matérielle, XenMobile l'invite dans l'écran d'inscription à inscrire son appareil.
2. L'utilisateur fournit son mot de passe Apple ID géré et XenMobile utilisé pour s'authentifier auprès de XenMobile
3. Dans l'étape de configuration de l'identifiant Apple ID, l'appareil invite l'utilisateur à entrer son identifiant Apple ID géré et son mot de passe temporaire ASM. Ces éléments authentifient l'utilisateur auprès des services d'Apple.
4. L'appareil invite l'utilisateur à créer un mot de passe pour son Apple ID géré, utilisé pour protéger ses données dans iCloud.
5. À la fin de l'Assistant de configuration, XenMobile démarre l'installation de stratégies, d'applications et de contenu multimédia sur l'appareil. Pour les applications et iBooks attribués au niveau de l'utilisateur, l'assistant invite les instructeurs et les étudiants à s'enregistrer pour l'achat en volume. Après avoir accepté l'invitation, les utilisateurs reçoivent leurs applications et iBooks d'achat en volume au cours du déploiement suivant (dans les six heures).

Configurer les iPad partagés

Plusieurs élèves d'une salle de classe peuvent partager un iPad pour différentes matières enseignées par un ou plusieurs instructeurs.

Vous ou les instructeurs inscrivez les iPad partagés, puis déployez des stratégies, des applications et des médias sur ces appareils. Ensuite, les étudiants fournissent leurs informations d'identification Apple gérées pour se connecter à un iPad partagé. Si vous avez déjà déployé une stratégie Configuration de l'éducation pour les étudiants, ils ne se connectent plus en tant que « Autre utilisateur » pour partager les appareils.

XenMobile utilise deux canaux de communication pour les iPad partagés : le canal système pour le propriétaire de l'appareil (instructeur) et le canal utilisateur pour l'utilisateur résident actuel (étudi-

ant). XenMobile utilise ces canaux pour envoyer les commandes MDM appropriées aux ressources prises en charge par Apple.

Les ressources déployées sur le canal système sont les suivantes :

- Stratégies d'appareil, telles que Configuration de l'éducation, Message sur l'écran de verrouillage, Nombre maximal d'utilisateurs résidents et Période de grâce de verrouillage par code secret
- Applications achetées en volume basées sur les appareils

  Apple ne prend pas en charge les applications d'entreprise ou les applications achetées en volume basées sur les utilisateurs sur les iPad partagés. Les applications installées sur un iPad partagé sont liées à l'appareil et non à l'utilisateur.
- iBooks achetés en volume basés sur l'utilisateur

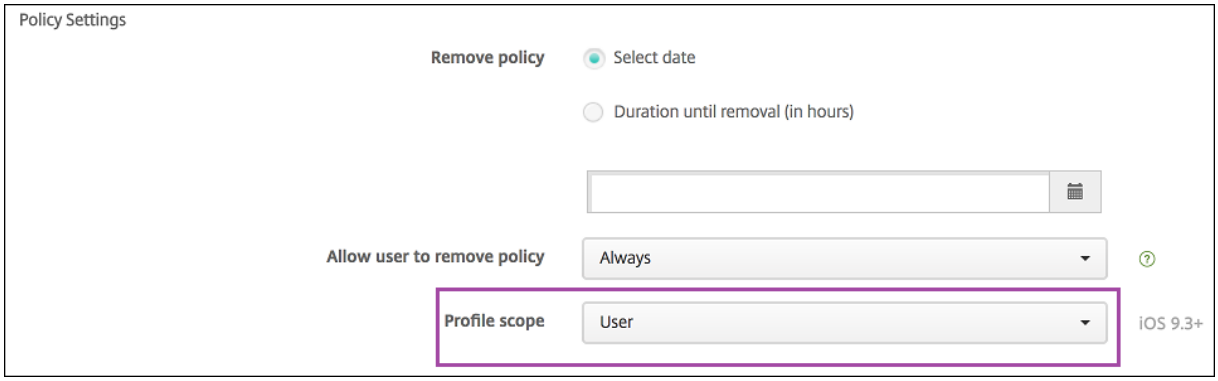
  Apple prend en charge l'attribution d'iBooks achetés en volume basés sur l'utilisateur sur les iPad partagés.

Les ressources déployées sur le canal utilisateur sont les suivantes :

- Stratégies d'appareil : Notifications d'applications, Disposition de l'écran d'accueil et Restrictions

  XenMobile ne prend actuellement en charge que ces stratégies d'appareil sur le canal utilisateur.

Lors de la configuration des stratégies d'appareil, vous spécifiez le canal de déploiement dans le paramètre de stratégie **Étendue du profil**.



Pour supprimer les stratégies d'appareil que vous avez déployées sur le canal utilisateur, réglez l'**étendue de déploiement** sur **Utilisateur** pour la stratégie Suppression de profil.

Workflow général

En général, vous fournissez des iPad préconfigurés et supervisés partagés aux enseignants. Les instructeurs distribuent ensuite les appareils aux étudiants. Si vous ne distribuez pas d'iPad partagés

pré-inscrits aux instructeurs : assurez-vous de fournir aux instructeurs leurs mots de passe du serveur XenMobile afin qu'ils puissent inscrire leurs appareils.

Le workflow général pour la configuration et l'inscription des iPad partagés est le suivant.

1. Utilisez la console du serveur XenMobile pour ajouter des comptes ASM (**Paramètres > Programme de déploiement d'Apple**) avec le **mode partagé** activé. Pour plus d'informations, voir « Gérer les comptes ASM pour les iPad partagés » ci-après.
2. Comme décrit dans cette section, ajoutez les stratégies d'appareil, applications et médias requis à XenMobile. Attribuez ces ressources à des groupes de mise à disposition.
3. Demandez aux instructeurs d'effectuer une réinitialisation matérielle sur les iPad partagés. L'écran de gestion à distance pour l'inscription s'affiche.
4. Les instructeurs inscrivent les iPad partagés.
   XenMobile déploie les ressources configurées sur chaque iPad partagé inscrit. Après un redémarrage automatique, les instructeurs peuvent partager les appareils avec les élèves. Une page de connexion apparaît sur l'iPad.
5. Un étudiant choisit sa classe, puis saisit son identifiant Apple ID géré et son mot de passe ASM temporaire.
   L'iPad partagé s'authentifie auprès d'ASM et invite l'étudiant à créer un mot de passe ASM. Pour sa prochaine connexion à l'iPad partagé, l'étudiant fournit le nouveau mot de passe ASM.
6. Un autre étudiant qui partage l'iPad peut alors se connecter en répétant l'étape précédente.

Gérer les comptes ASM pour les iPad partagés

Si vous utilisez déjà XenMobile avec Apple Éducation : un compte ASM existant est configuré dans XenMobile pour les appareils qui ne sont pas partagés, tels que les appareils utilisés par les instructeurs. Vous pouvez utiliser le même ASM et le même serveur XenMobile pour les appareils partagés et non partagés.

XenMobile prend en charge ces scénarios de déploiement :

- Un groupe d'iPad partagés par classe

  Dans ce scénario, vous attribuez les iPad partagés à une classe d'étudiants. Les iPad restent dans la salle de classe. Les instructeurs qui enseignent différentes matières dans cette classe utilisent les mêmes iPad.

- Un groupe d'iPad partagés par instructeur

  Dans ce scénario, vous attribuez les iPad partagés à un instructeur, qui utilise ces iPad pour les différentes classes auxquelles il enseigne.

Organiser les iPad partagés en groupes d'appareils

ASM vous permet d'organiser les appareils en groupes en créant plusieurs serveurs MDM. Lorsque vous attribuez les iPad partagés à un serveur MDM, créez un groupe d'appareils pour chaque groupe d'iPad partagés, par classe ou par instructeur :

- Groupe 1 d'iPad partagés > Serveur MDM du groupe d'appareils 1
- Groupe 2 d'iPad partagés > Serveur MDM du groupe d'appareils 2
- Groupe N d'iPad partagés > Serveur MDM du groupe d'appareils N

Ajouter des comptes ASM pour chaque groupe d'appareils

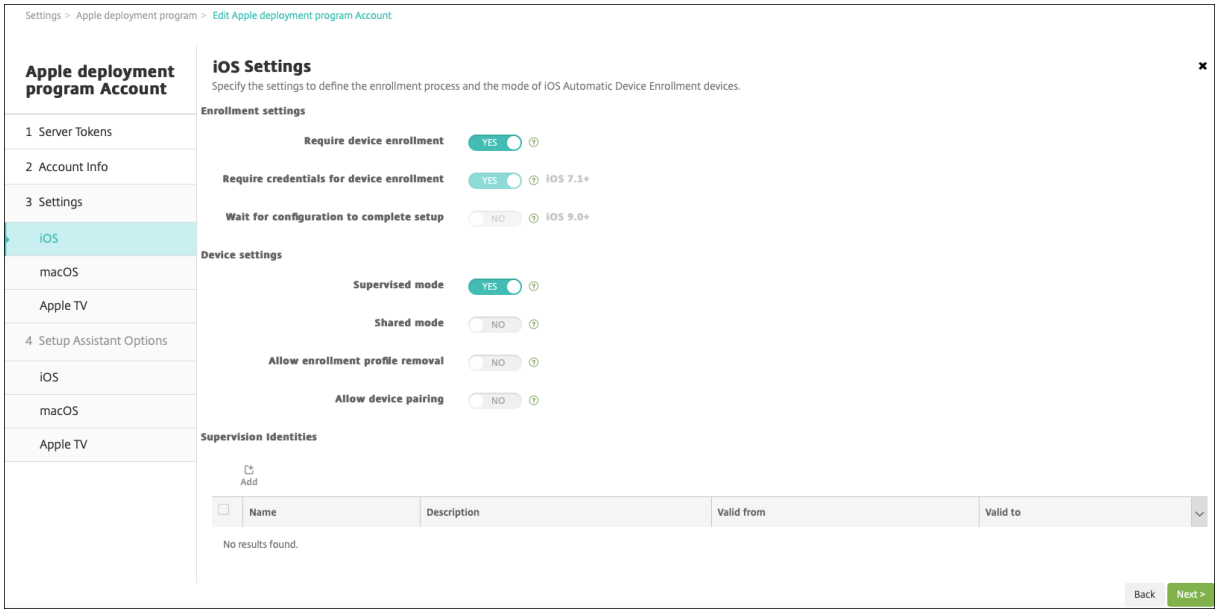
Lorsque vous créez plusieurs comptes ASM à partir de la console du serveur XenMobile, vous importez automatiquement des groupes d'iPad partagés (un pour chaque classe ou chaque instructeur) :

- Serveur MDM du groupe d'appareils 1 > Compte du groupe d'appareils 1
- Serveur MDM du groupe d'appareils 2 > Compte du groupe d'appareils 2
- Serveur MDM du groupe d'appareils N > Compte du groupe d'appareils N

Les exigences spécifiques aux iPad partagés sont les suivantes :

- Un compte ASM pour chaque groupe d'appareils avec ces paramètres activés :
  - **Exiger l'inscription des appareils**
  - **Mode supervisé**
  - **Mode partagé**
- Assurez-vous d'utiliser le même **suffixe d'éducation** pour tous les comptes ASM d'un établissement d'enseignement donné.

Pour ajouter un compte, accédez à **Paramètres > Programme de déploiement d'Apple**.

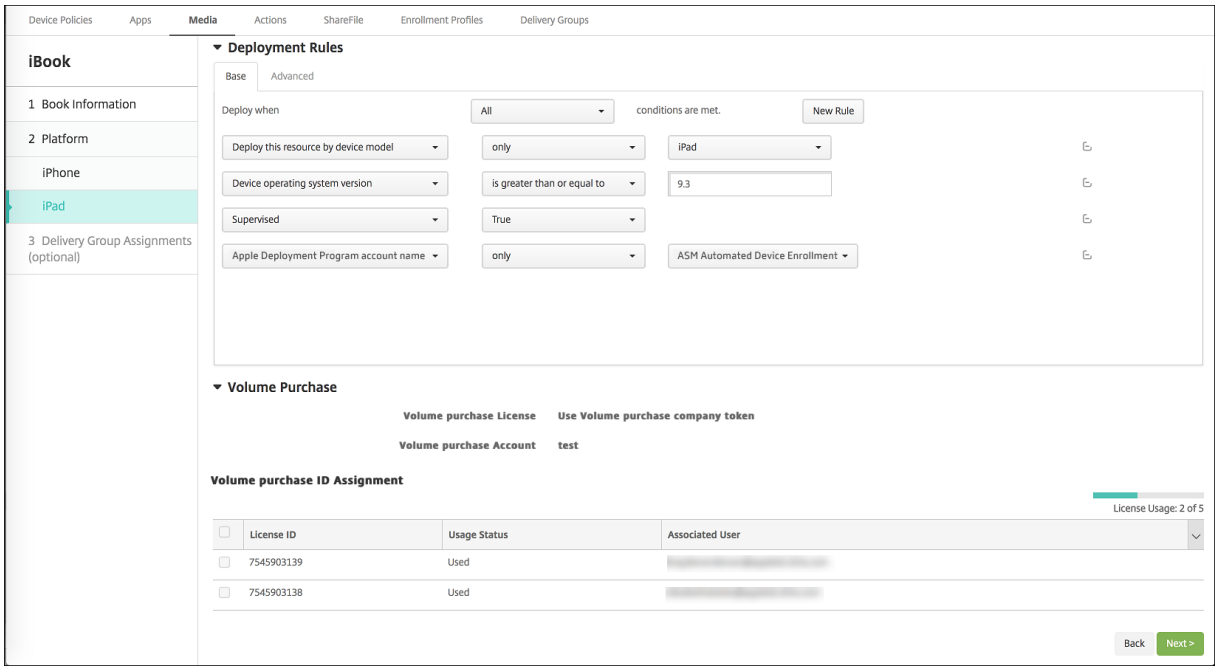


Applications pour iPad partagés

Les iPad partagés prennent en charge l'attribution d'applications d'achat en volume basées sur les appareils. Avant de déployer une application sur un iPad partagé, XenMobile envoie une demande au serveur d'achat en volume d'Apple pour attribuer des licences d'achat en volume aux appareils. Pour vérifier les attributions d'achat en volume, accédez à **Configurer > Applications > iPad** et développez **Achat en volume**.

Médias pour iPad partagés

Les iPad partagés prennent en charge l'attribution d'iBooks achetés en volume basés sur l'utilisateur. Avant de déployer des iBooks sur un iPad partagé, XenMobile envoie une demande au serveur d'achat en volume d'Apple pour attribuer des licences d'achat en volume aux étudiants. Pour vérifier les attributions d'achat en volume, accédez à **Configurer > Média > iPad** et développez **Achat en volume**.



Règles de déploiement pour iPad partagés

Avec le déploiement d'iPad partagés, les règles au niveau du groupe de mise à disposition ne s'appliquent pas, car elles se rapportent aux propriétés utilisateur. Pour filtrer les stratégies, les applications et les médias pour chaque groupe d'appareils : ajoutez une règle de déploiement pour les ressources en fonction du nom du compte. Par exemple :

- Pour le compte du groupe d'appareils 1, définissez cette règle de déploiement :

```
1   Apple Deployment Program account name
2   Only
```



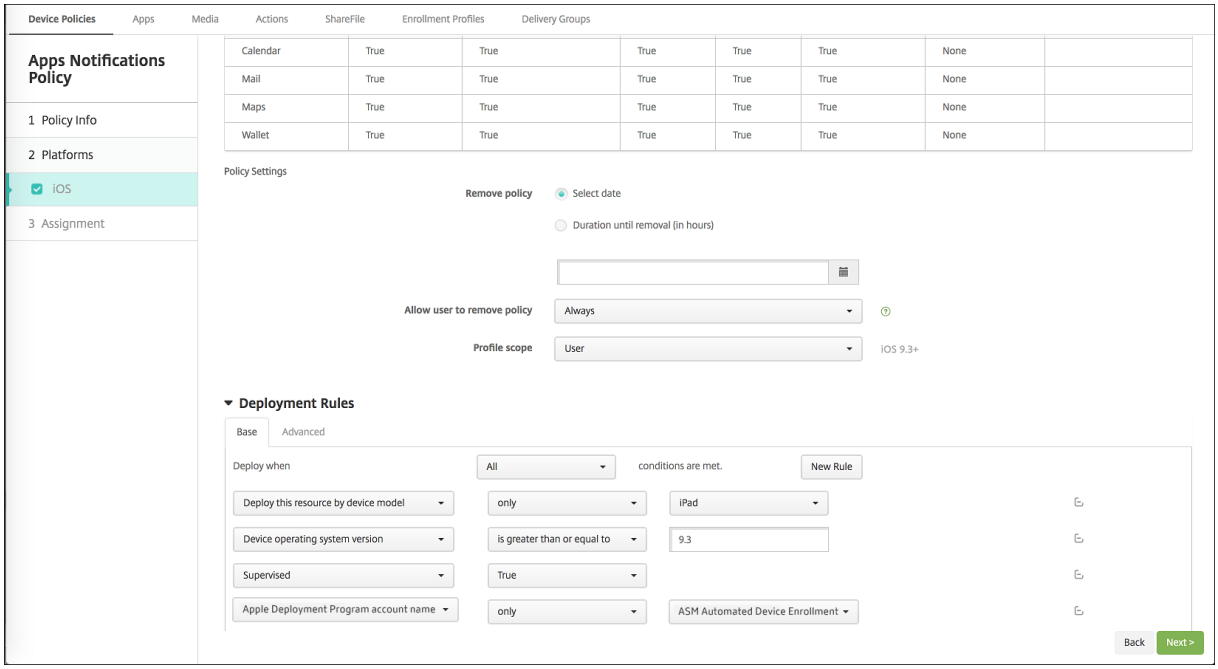
```
Device Group 1 account

<!--NeedCopy-->
```

- Pour le compte du groupe d'appareils 2, définissez cette règle de déploiement :

```
Apple Deployment Program account name
Only
Device Group 2 account

<!--NeedCopy-->
```

- Pour le compte du groupe d'appareils N, définissez cette règle de déploiement :

```
Apple Deployment Program account name
Only
Device Group N account

<!--NeedCopy-->
```



Pour déployer l'application En classe d'Apple uniquement pour les instructeurs (à l'aide d'iPad non partagés), filtrez les ressources par état partagé ASM avec ces règles de déploiement :

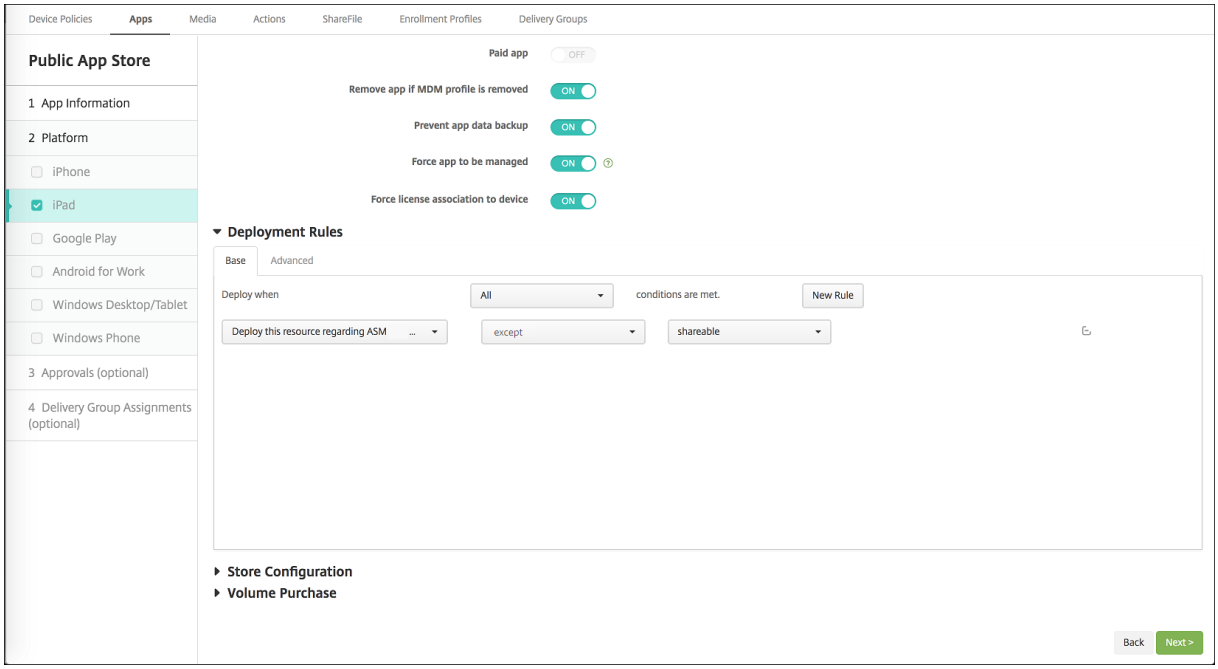
```
Deploy this resource regarding ASM shared mode
only
unshared
```



```
<!--NeedCopy-->
```

Ou :

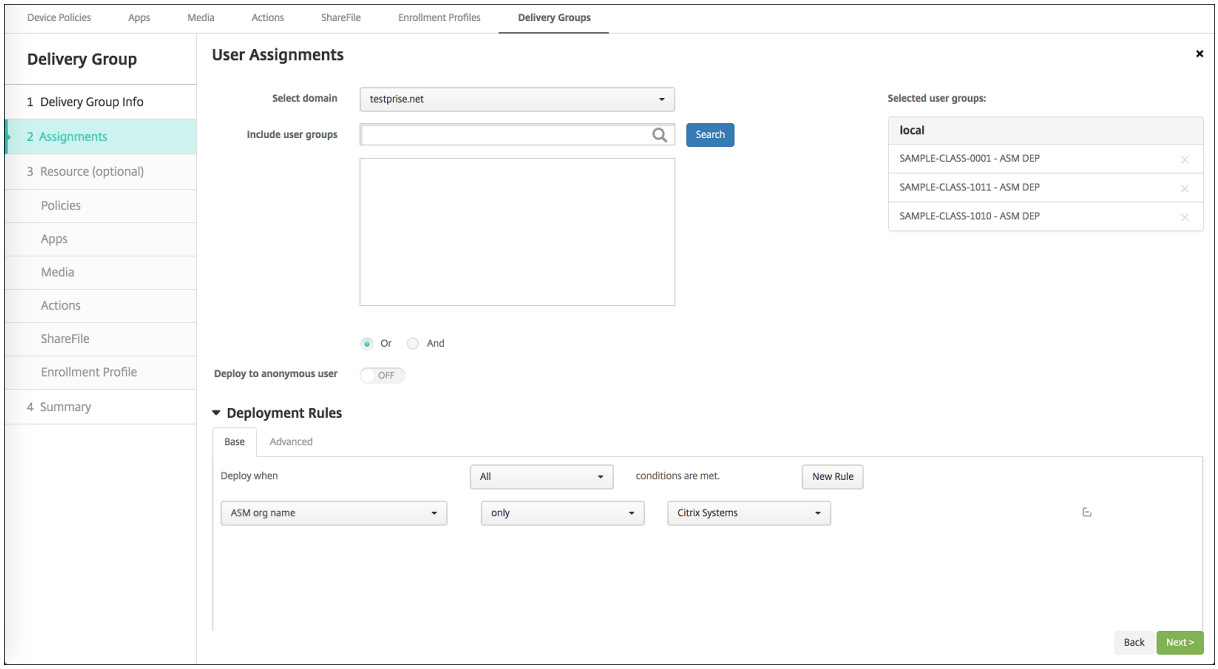
```
Deploy this resource regarding ASM shared mode
except
shareable

<!--NeedCopy-->
```



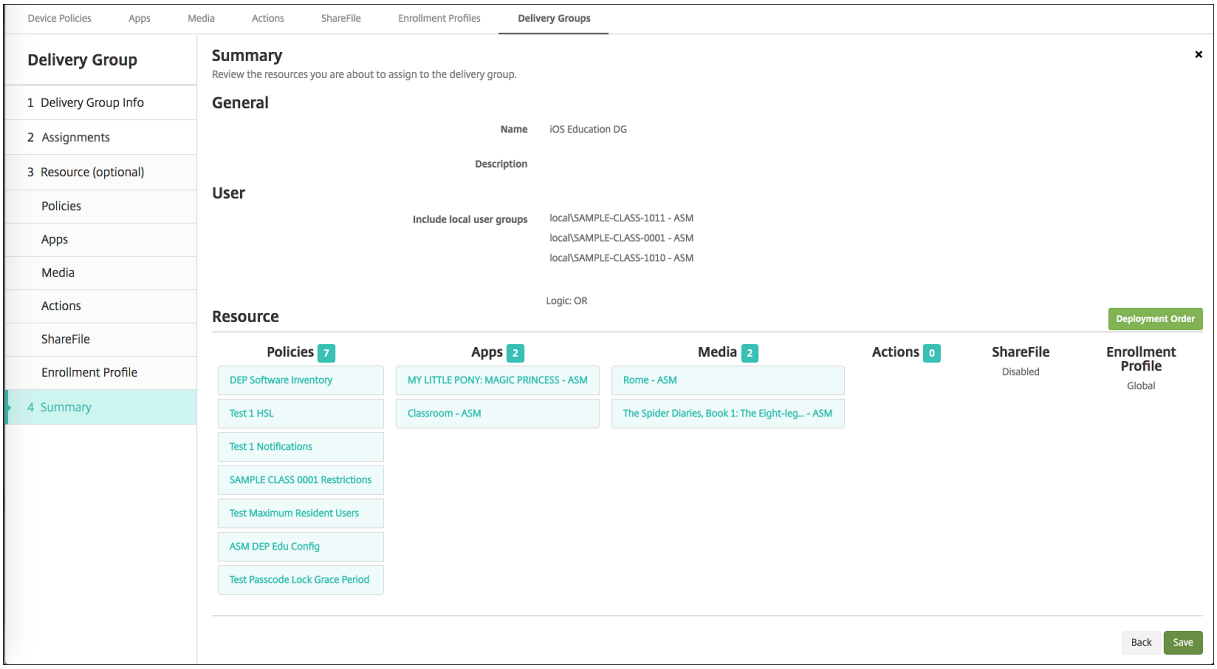
Groupes de mise à disposition pour iPad partagés

Pour le groupe d'appareils pour chaque instructeur :

- Configurez un groupe de mise à disposition. Pour l'instructeur, attribuez toutes les classes définies par la stratégie Configuration de l'éducation.



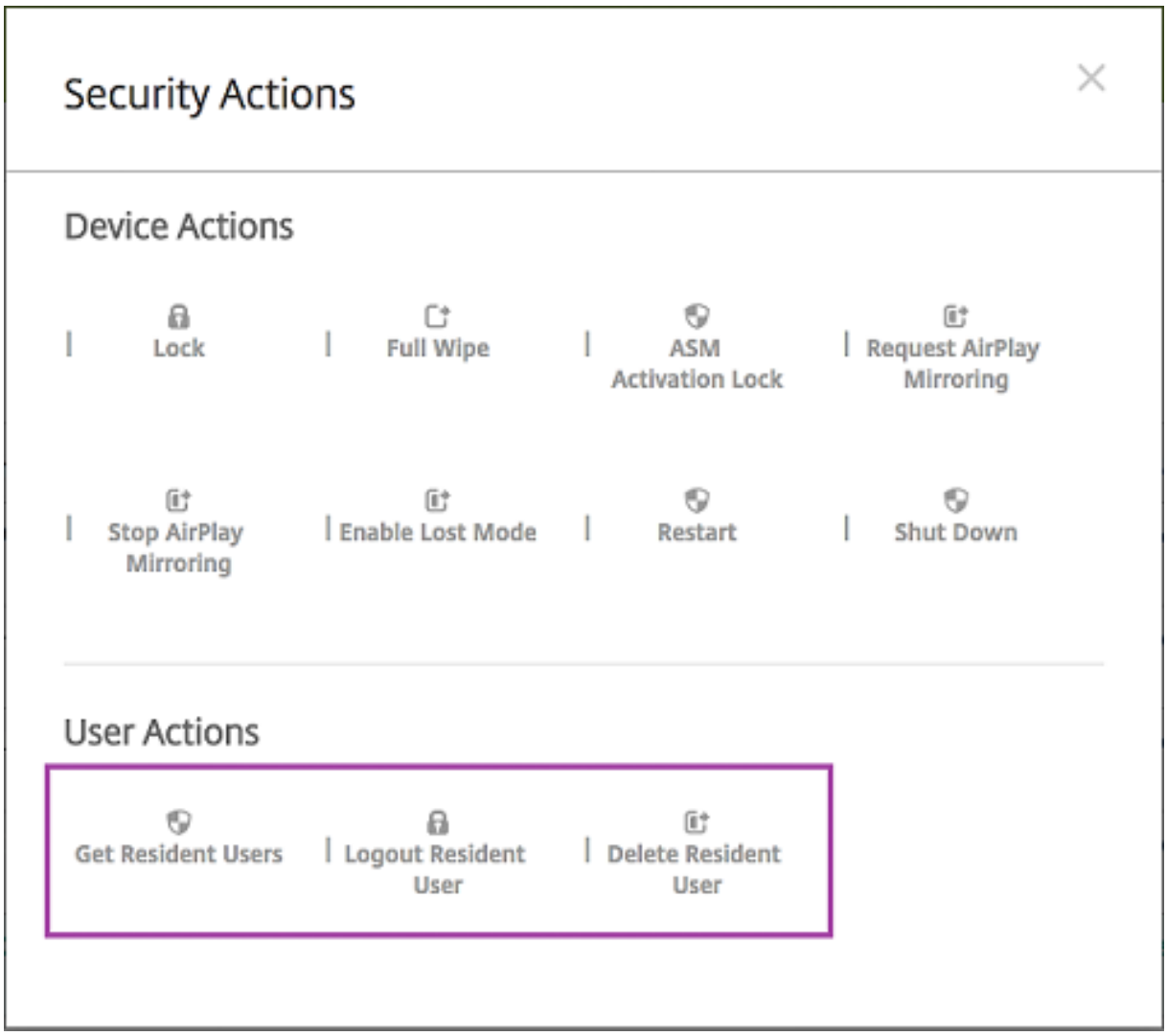
- Ce groupe de mise à disposition doit inclure ces ressources MDM :
  - Stratégies d'appareil :
    - Configuration de l'éducation
    - Message sur l'écran de verrouillage
    - Notifications d'applications
    - Disposition de l'écran d'accueil
    - Restrictions
    - Nombre maximal d'utilisateurs résidents
    - Période de grâce de verrouillage par code secret
  - Applications achetées en volume requises
  - iBooks achetés en volume requis



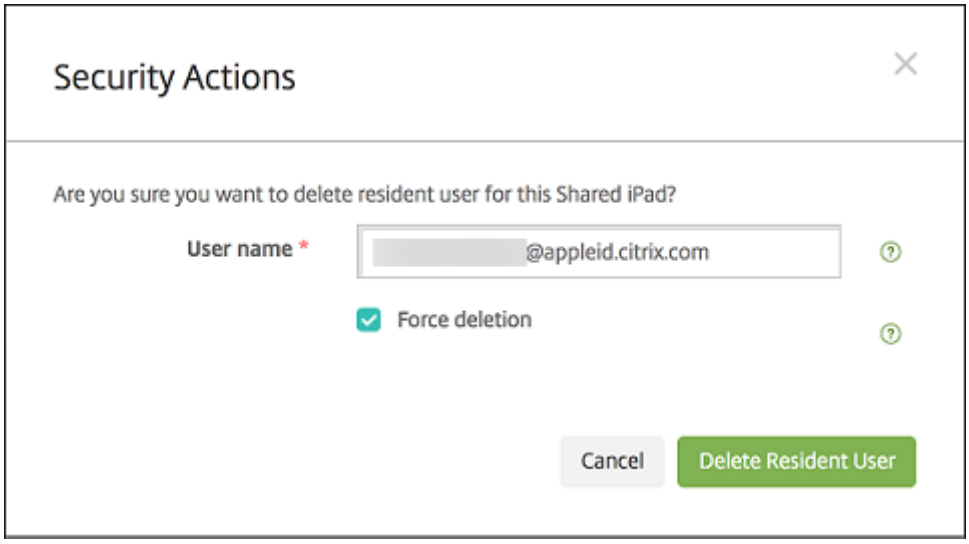
Actions de sécurisation pour iPad partagés

Outre les actions de sécurisation existantes, vous pouvez utiliser ces actions de sécurisation pour les iPad partagés :

- **Obtenir utilisateurs résidents :** répertorie les utilisateurs qui ont des comptes actifs sur l'appareil actuel. Cette action force une synchronisation entre l'appareil et la console XenMobile.
- **Déconnecter utilisateur résident :** force une déconnexion de l'utilisateur actuel.
- **Supprimer utilisateur résident :** supprime la session en cours pour un utilisateur spécifique. L'utilisateur peut se reconnecter.



Après avoir cliqué sur **Supprimer utilisateur résident**, vous pouvez spécifier le nom d'utilisateur.

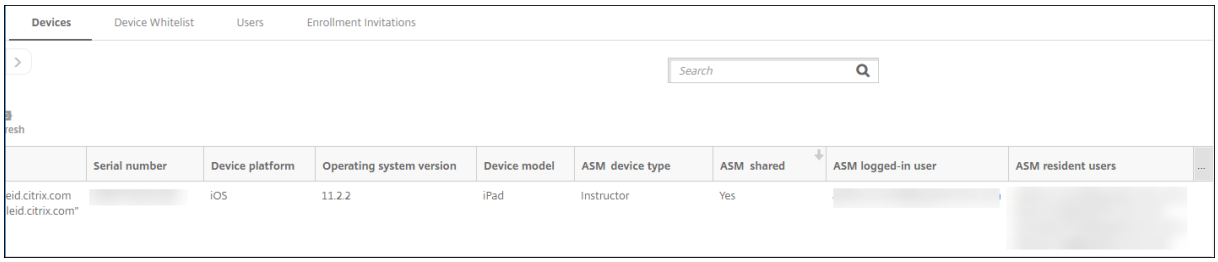


Les résultats des actions de sécurisation apparaissent sur les pages **Gérer > Appareils > Général** et **Gérer > Appareils > Groupes de mise à disposition**.

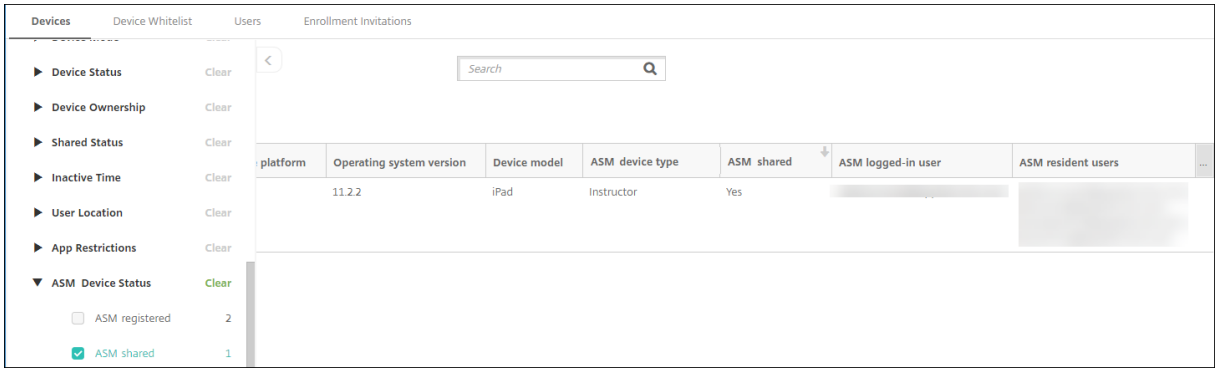
Obtenir des informations sur les iPad partagés

Vous trouverez des informations spécifiques aux iPad partagés sur la page **Gérer > Appareils** :

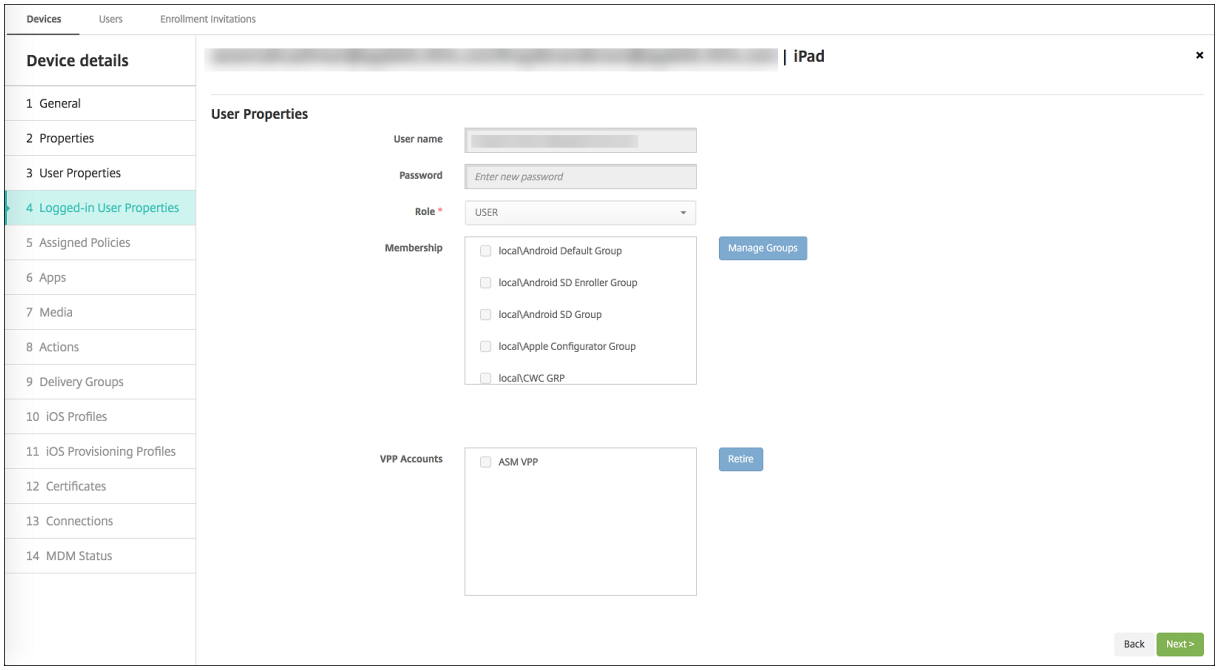
- Vous pouvez vérifier :
  - si un appareil est partagé (**Partagé avec ASM**) ;
  - qui est connecté à l'appareil partagé (**utilisateur ASM connecté**) ;
  - tous les utilisateurs attribués à l'appareil partagé (**utilisateurs résidents ASM**)

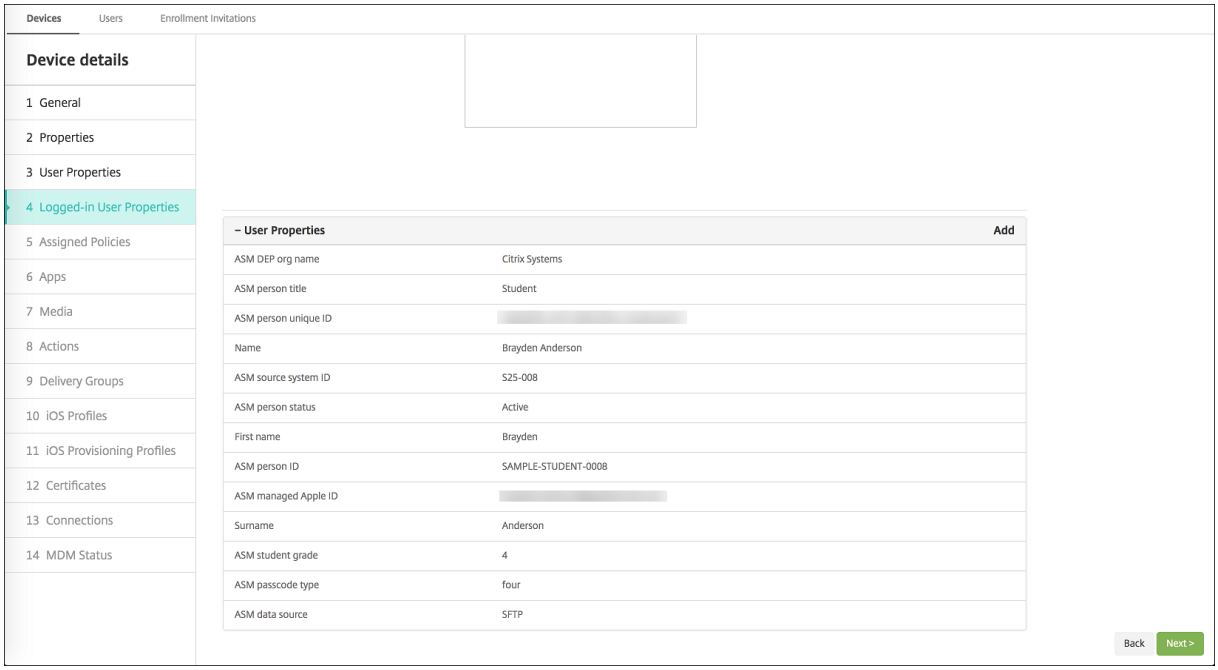


- Filtrez la liste des appareils en fonction de l'**état des appareils ASM** :

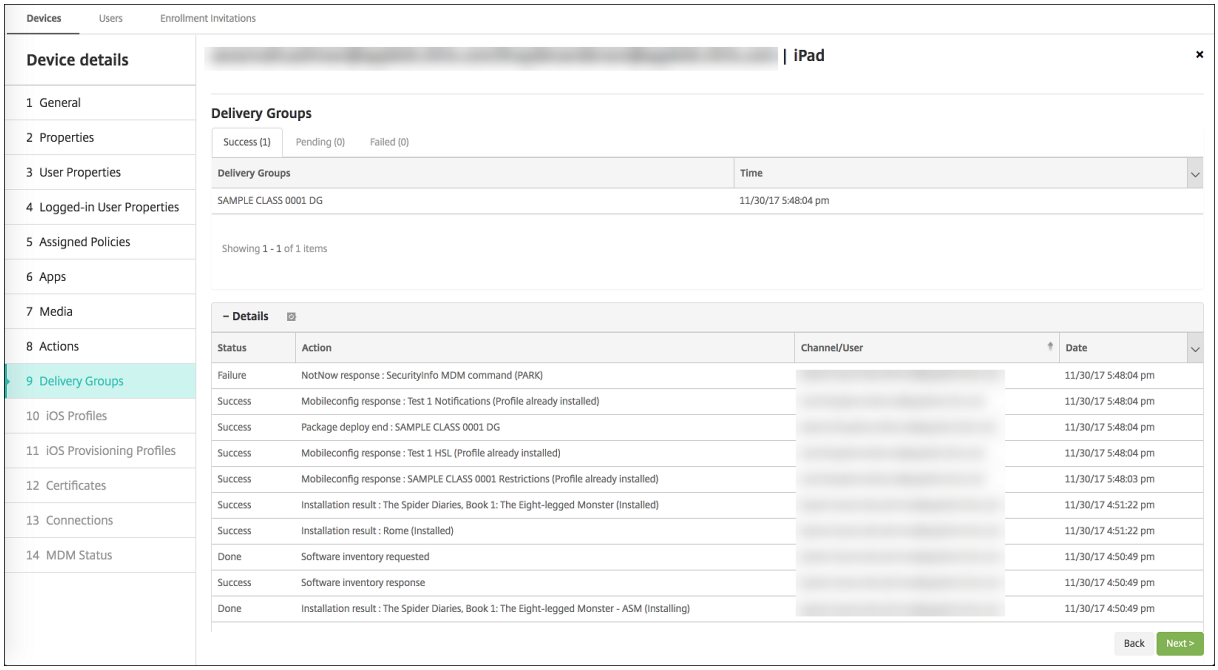


- Vous pouvez afficher les détails sur l'utilisateur connecté à un iPad partagé, depuis la page **Gérer > Appareils > Propriétés de l'utilisateur connecté**.

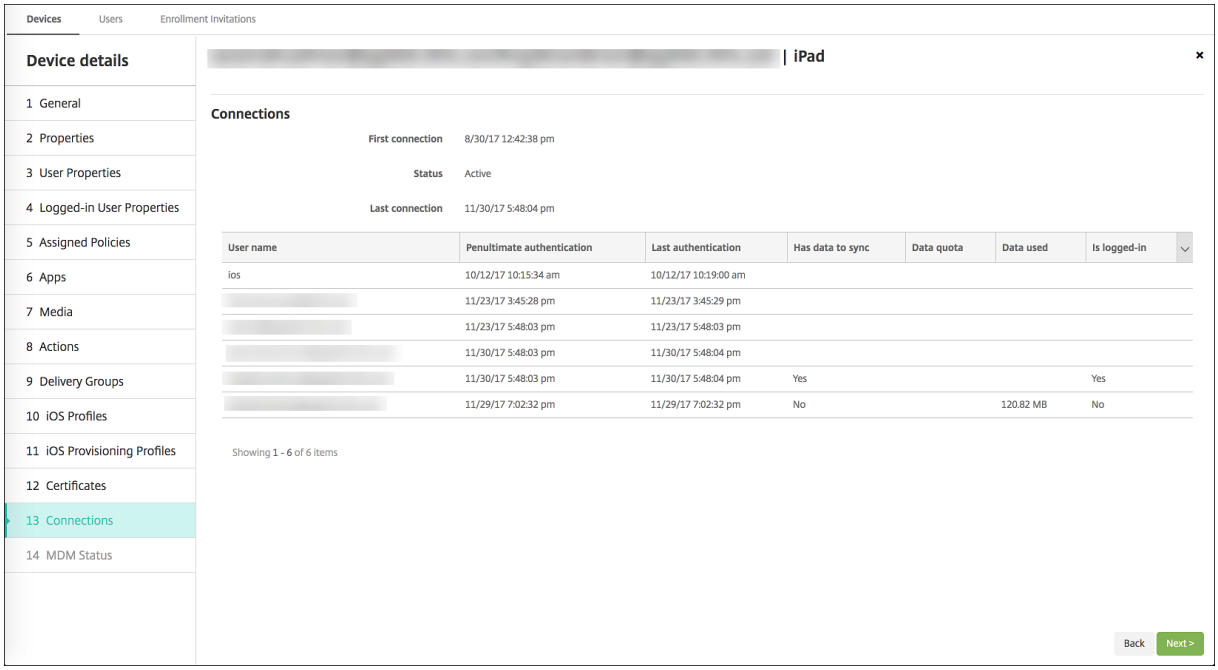




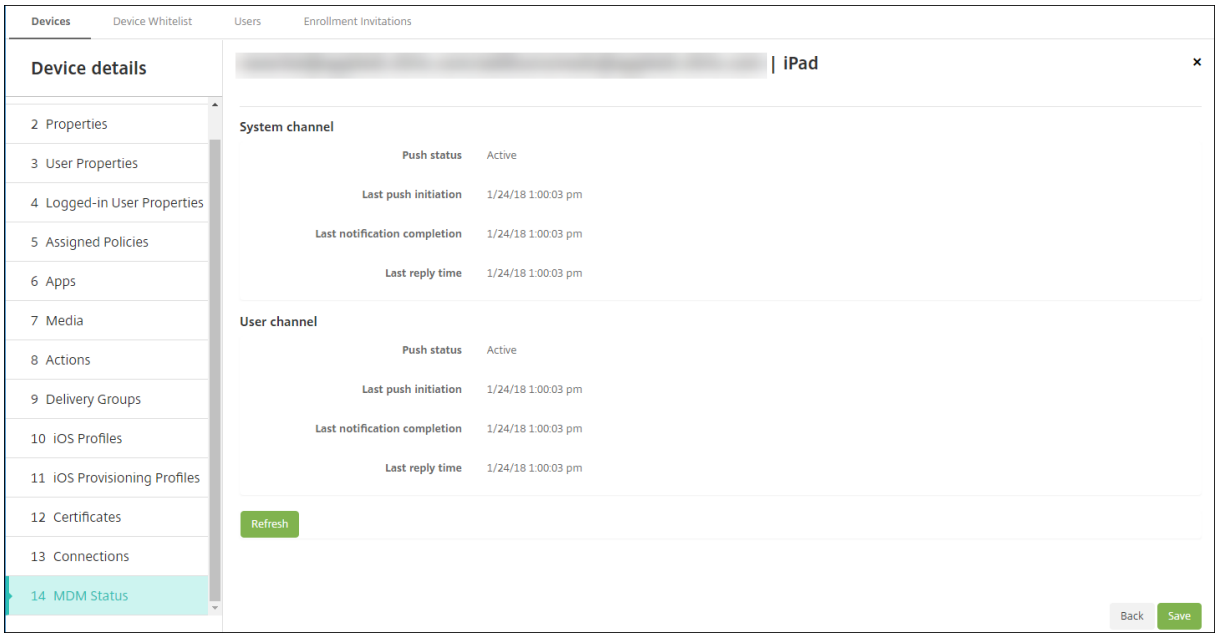
- Vous pouvez voir le canal utilisé pour déployer les ressources pour les instructeurs et les utilisateurs d'un groupe de mise à disposition sur la page **Gérer > Appareils > Groupes de mise à disposition**. La colonne **Canal/utilisateur** affiche le type (**Système** ou **Utilisateur**) et le destinataire (instructeur ou étudiant).



- Vous pouvez obtenir des informations sur les utilisateurs résidents :
  - **Dispose de données à synchroniser :** si l'utilisateur a des données à synchroniser avec le cloud.
  - **Quota de données :** quota de données défini pour l'utilisateur en octets. Un quota peut ne pas apparaître si les quotas utilisateur sont temporairement désactivés ou ne sont pas appliqués pour l'utilisateur.
  - **Données utilisées :** quantité de données utilisée par l'utilisateur en octets. Une valeur peut ne pas apparaître si une erreur se produit lorsque le système rassemble les informations.
  - **Est connecté :** indique si l'utilisateur est connecté à l'appareil.



- Vous pouvez voir l'état de push pour les deux canaux.



Gérer les données des instructeurs, des étudiants et de la classe

Lors de la gestion des données des instructeurs, des étudiants et de la classe, notez ce qui suit :

- Ne modifiez pas les identifiants Apple ID gérés après avoir importé des informations ASM dans XenMobile. XenMobile utilise également les identifiants d'utilisateur ASM pour identifier les utilisateurs.

- Si vous ajoutez ou modifiez des données de classe dans ASM une fois que vous avez créé une ou plusieurs stratégies Configuration de l'éducation : modifiez les stratégies, puis redéployez-les.
- Si l'instructeur d'une classe change après le déploiement de la stratégie Configuration de l'éducation : vérifiez que la stratégie se met bien à jour dans la console XenMobile puis redéployez la stratégie.
- Si vous mettez à jour les propriétés de l'utilisateur dans le portail ASM, XenMobile met également à jour ces propriétés dans la console. Toutefois, XenMobile ne reçoit pas la propriété de fonction de la personne ASM (Instructeur, Étudiant ou Autre) de la même manière qu'il reçoit les autres propriétés. Par conséquent, si vous modifiez la fonction de la personne ASM dans ASM, procédez comme suit pour refléter cette modification dans XenMobile.

Pour gérer les données :

1. Dans le portail ASM, mettez à jour le niveau scolaire de l'étudiant et effacez le niveau scolaire de l'instructeur.
2. Si vous avez transformé un compte étudiant en compte instructeur, supprimez l'utilisateur de la liste des étudiants de la classe. Ensuite, ajoutez l'utilisateur à la liste des instructeurs dans la même classe ou une autre.

   Si vous avez modifié un compte instructeur vers un compte étudiant, supprimez l'utilisateur de la classe. Ensuite, ajoutez l'utilisateur à la liste des étudiants dans la même classe ou une autre. Vos mises à jour s'affichent dans la console XenMobile lors de la prochaine synchronisation (toutes les cinq minutes par défaut) ou récupération (par défaut, toutes les 24 heures).
3. Modifiez la stratégie Configuration de l'éducation pour appliquer la modification et redéployez-la.

   - Si vous supprimez un utilisateur à partir du portail ASM, XenMobile supprime également cet utilisateur de la console XenMobile après une récupération.

     Vous pouvez réduire l'intervalle de ligne de base en modifiant la valeur de cette propriété de serveur : **bulk.enrollment.fetchRosterInfoDelay** (la valeur par défaut est **1440** minutes).
   - Lorsque vous déployez des ressources : si un étudiant rejoint une classe, créez un groupe de mise à disposition avec cet étudiant uniquement et déployez les ressources vers l'étudiant.
   - Si un étudiant ou un instructeur perd son mot de passe temporaire, demandez-lui de contacter l'administrateur ASM. L'administrateur peut fournir le mot de passe temporaire ou en générer un nouveau.

Gérer un appareil perdu ou volé qui est inscrit au programme de déploiement Apple d'Apple School Manager

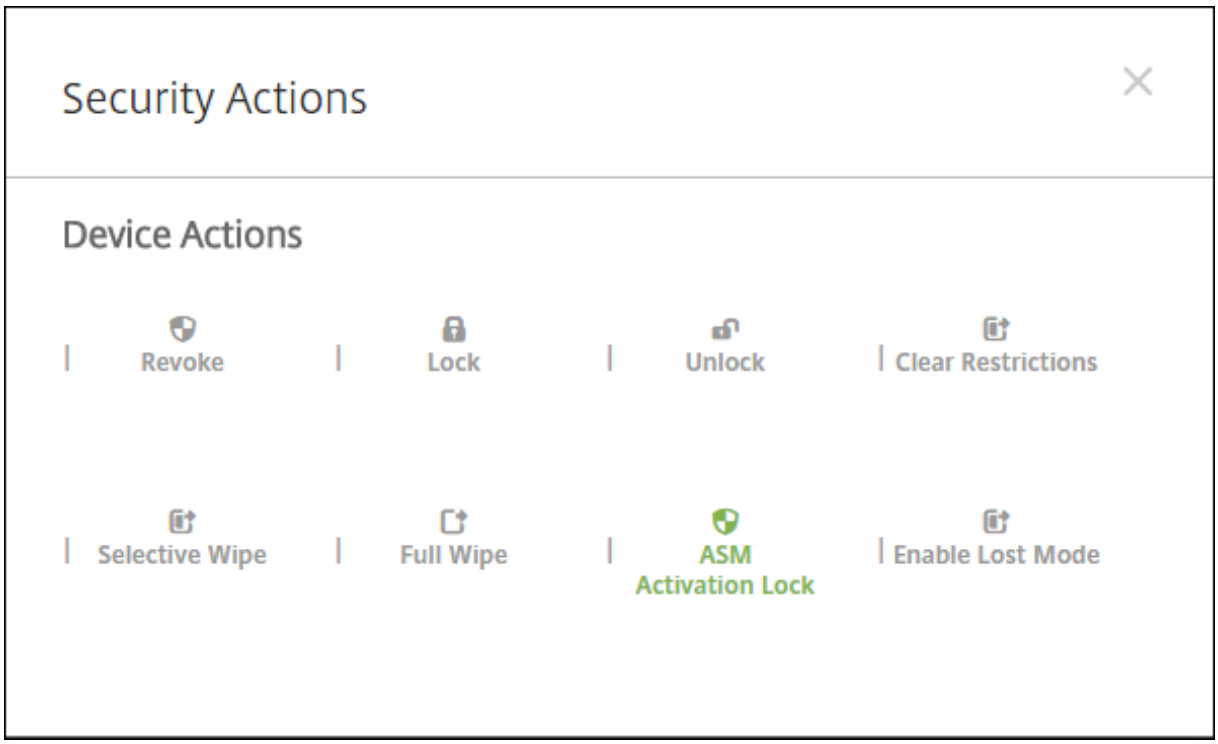
Le service Localiser mon iPhone/iPad d'Apple comprend une fonctionnalité de verrouillage d'activation. Le verrouillage d'activation empêche les utilisateurs non autorisés d'utiliser ou de revendre un appareil perdu ou volé qui est inscrit au programme de déploiement d'Apple.

XenMobile comprend une action de sécurité **Verrouillage d'activation ASM** qui vous permet d'envoyer un code de verrouillage à un appareil inscrit au de déploiement Apple ASM.

Lorsque vous utilisez l'action de sécurité **Verrouillage d'activation ASM**, XenMobile peut localiser les appareils sans obliger les utilisateurs à activer le service Localiser mon iPhone/iPad. Lors d'une réinitialisation matérielle ou d'un effacement complet d'un appareil ASM, l'utilisateur fournit son identifiant Apple ID géré et son mot de passe pour déverrouiller l'appareil.

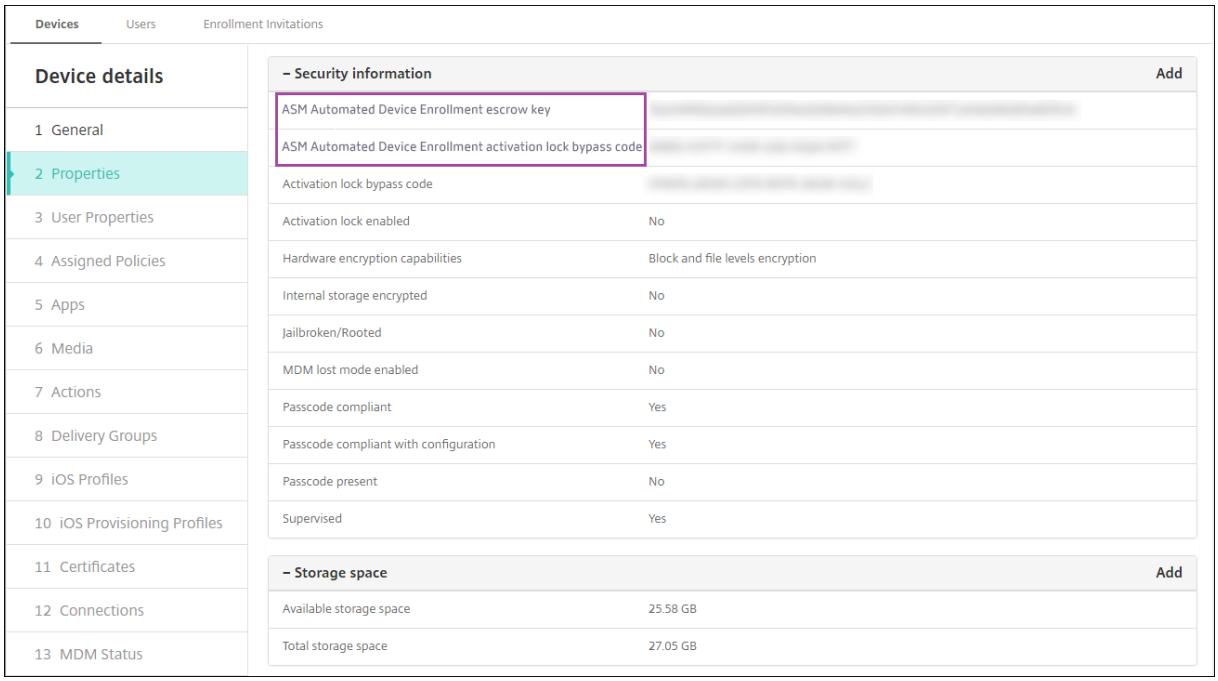
Pour libérer le verrou depuis la console, cliquez sur l'action de sécurité **Contourner le verrouillage d'activation**. Pour plus d'informations sur le contournement d'un verrouillage d'activation, consultez la section Contourner un verrouillage d'activation iOS. L'utilisateur peut également ne pas renseigner les informations de connexion et entrer le **code de contournement du verrouillage d'activation ASM** en tant que mot de passe. Ces informations sont disponibles dans **Détails de l'appareil**, sur l'onglet **Propriétés**.

Pour définir le verrouillage d'activation, accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Sécurité**, puis cliquez sur **Verrouillage d'activation ASM**.

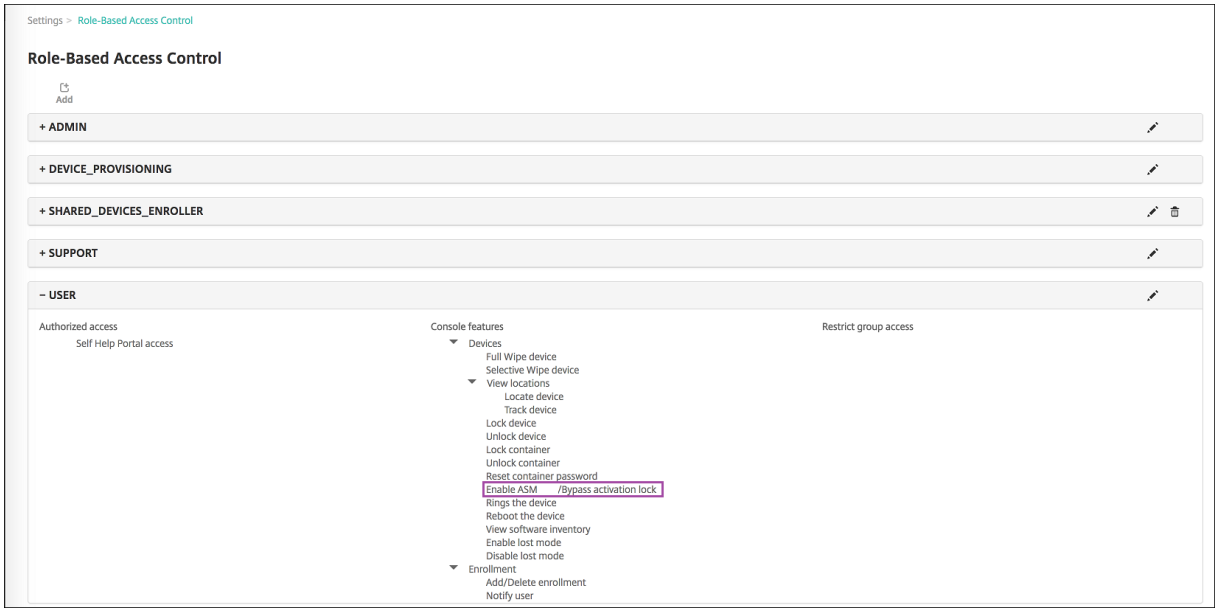


Les propriétés **Dépôt de clé ASM** et **Code de contournement du verrouillage d'activation ASM**

s'affichent dans **Détails de l'appareil**.



L'autorisation RBAC pour un verrouillage d'activation ASM est **Appareils > Activer contournement du verrouillage d'activation ASM**.



Distribuer les applications Apple

January 10, 2022

XenMobile gère les applications déployées sur les appareils. Vous pouvez organiser et déployer les types d'applications iOS/iPadOS et macOS suivants.

- **Apple App Store (iOS/iPadOS uniquement) :** ces applications peuvent être gratuites ou payantes et sont disponibles dans un magasin d'applications public, tel que l'Apple App Store ou Google Play. Par exemple : GoToMeeting.
- **Entreprise (iOS/iPadOS/macOS) :** applications natives pour lesquelles MDX n'est pas activé et qui ne contiennent pas les stratégies associées aux applications MDX.
- **MDX (iOS/iPadOS uniquement) :** applications préparées avec le SDK MAM ou encapsulées avec le MDX Toolkit. Ces applications incluent des stratégies MDX. Vous obtenez des applications MDX à partir de sources internes et de magasins publics.
- **Achat en volume (iOS/iPadOS/macOS) :** applications avec licences gérées via le programme d'achats en volume Apple.
- **Applications personnalisées iOS (iOS/iPadOS uniquement) :** applications propriétaires B2B développées en interne ou par un tiers.

Pour plus d'informations sur les différents types d'applications, reportez-vous à la section Ajouter des applications.

Certains déploiements nécessitent un compte Apple Business Manager (ABM) ou Apple School Manager (ASM). Pour plus d'informations, consultez les sections suivantes.

Pour chaque type d'application et méthode de distribution, Citrix recommande un ensemble de pratiques de configuration. Pour plus d'informations sur la distribution d'applications pour d'autres plates-formes, reportez-vous à la section Ajouter des applications. Les sections suivantes fournissent des informations plus détaillées sur la configuration des applications iOS.

Étapes générales de la distribution des applications

Scénario	Étape 1 : Associer les comptes	Étape 2 : Ajouter et configurer des applications	Étape 3 : Configurer des groupes de mise à disposition et déployer des applications
Applications de magasin d'applications public, y compris les applications de mobilité Citrix	Sans objet	**Dans XenMobile : Configurer > Applications**, ajoutez des applications **Magasin d'applications public** pour iPhone ou iPad. Configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans XenMobile :** configurez et déployez des applications à l'aide de groupes de mise à disposition.
Applications du magasin d'applications public livrées avec l'achat en volume Apple, y compris les applications de mobilité Citrix	Inscrivez-vous au programme de déploiement d'Apple. **Dans XenMobile :** accédez à **Paramètres > Achat en volume** pour ajouter votre compte d'achat en volume.	**Dans ABM ou ASM :** achetez et ajoutez des applications depuis Applications et Books. **Dans XenMobile :** accédez à **Configurer > Applications**, configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans XenMobile :** configurez et déployez des applications à l'aide de groupes de mise à disposition.

Scénario	Étape 1 : Associer les comptes	Étape 2 : Ajouter et configurer des applications	Étape 3 : Configurer des groupes de mise à disposition et déployer des applications
Applications d'entreprise	Sans objet	**Dans XenMobile :** accédez à **Configurer > Applications**. Cliquez sur **Ajouter**, puis sur **Entreprise**. Chargez le fichier IPA. Configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans XenMobile :** configurez et déployez des applications à l'aide de groupes de mise à disposition.
Applications MDX	Sans objet	**Dans XenMobile :** accédez à **Configurer > Applications**. Cliquez sur **Ajouter**, puis sur **MDX**. Assurez-vous de sélectionner **iPad**/**iPhone** pour la plateforme. Chargez le fichier MDX. Configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans XenMobile :** configurez et déployez des applications à l'aide de groupes de mise à disposition.

Scénario	Étape 1 : Associer les comptes	Étape 2 : Ajouter et configurer des applications	Étape 3 : Configurer des groupes de mise à disposition et déployer des applications
Applications MDX distribuées à l'aide d'un achat en volume Apple	Inscrivez-vous au programme de déploiement d'Apple. **Dans XenMobile :** accédez à **Paramètres > Achat en volume** pour ajouter votre compte d'achat en volume.	**Dans ABM :** achetez et ajoutez des applications MDX depuis Applications et Books. Associez l'application à votre compte ABM. **Dans XenMobile :** accédez à **Configurer > Applications**, configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans XenMobile :** configurez et déployez des applications à l'aide de groupes de mise à disposition.
Applications personnalisées	Inscrivez-vous au programme de déploiement d'Apple. **Dans XenMobile :** accédez à **Paramètres > Achat en volume** pour ajouter votre compte d'achat en volume.	**Dans ABM :** ajoutez votre application à l'App Store en tant qu'application privée. Associez l'application à votre compte ABM. **Dans XenMobile :** accédez à **Configurer > Applications**, configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans XenMobile :** configurez et déployez des applications à l'aide de groupes de mise à disposition.

Scénario	Étape 1 : Associer les comptes	Étape 2 : Ajouter et configurer des applications	Étape 3 : Configurer des groupes de mise à disposition et déployer des applications
Applications personnalisées MDX	Inscrivez-vous au programme de déploiement d'Apple. **Dans XenMobile :** accédez à **Paramètres > Achat en volume** pour ajouter votre compte d'achat en volume.	**Dans ABM :** ajoutez votre application à l'App Store en tant qu'application privée. Associez l'application à votre compte ABM. **Dans XenMobile :** accédez à **Configurer > Applications** et chargez le fichier MDX. Configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans XenMobile :** configurez et déployez des applications à l'aide de groupes de mise à disposition.

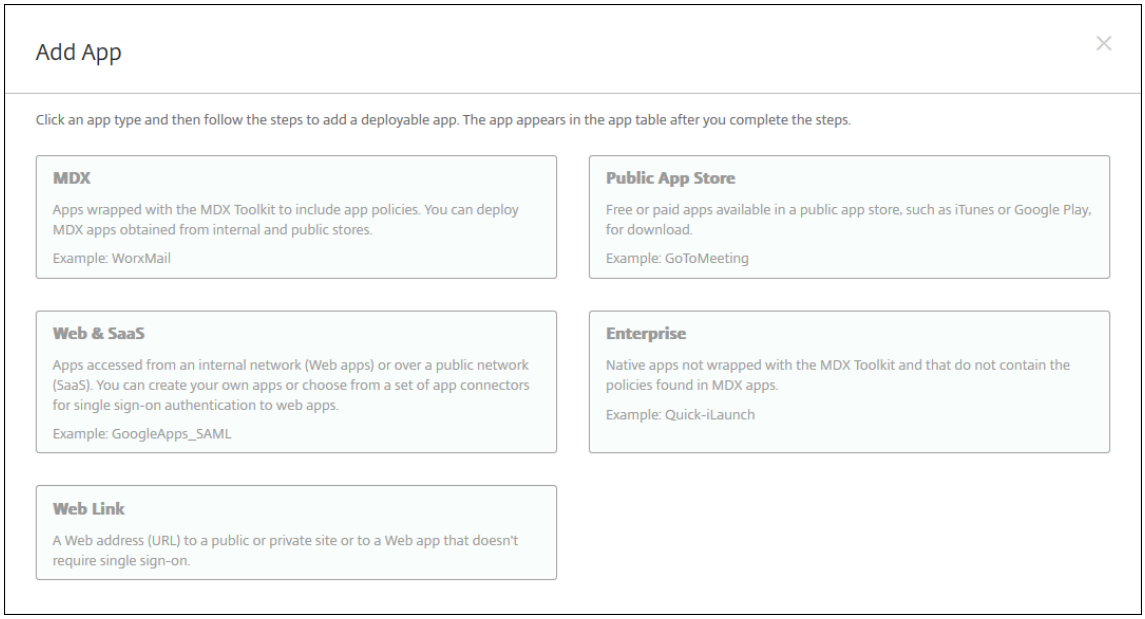
Applications de magasin d'applications public

Vous pouvez ajouter des applications gratuites et payantes disponibles sur l'App Store à XenMobile.

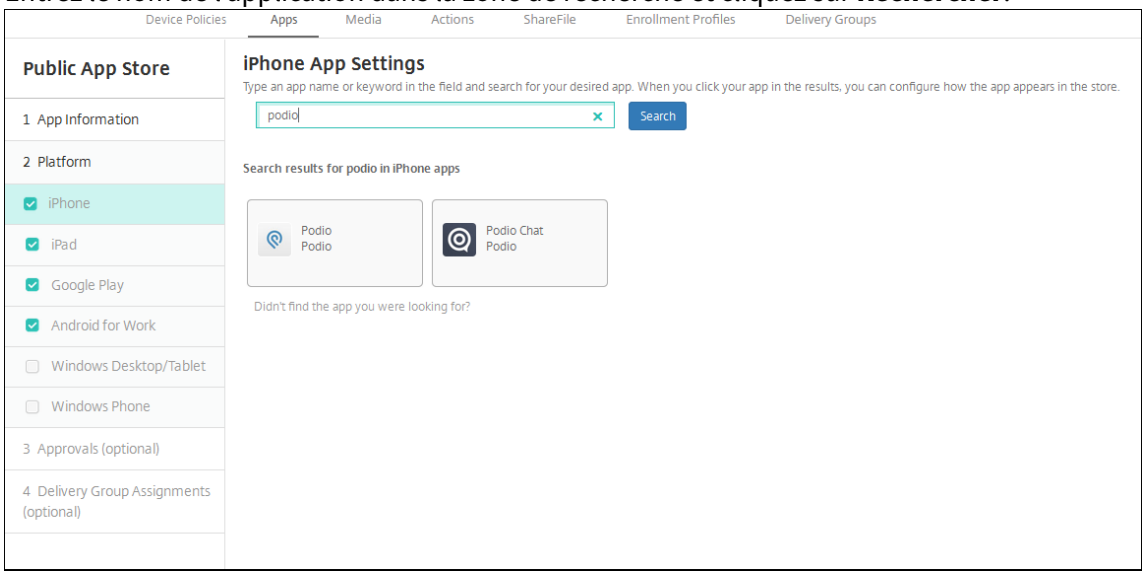
Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Non
Disponible sur	iOS/iPadOS

Étape 1 : Ajouter et configurer des applications

1. Dans la console XenMobile, accédez à **Configurer > Applications**. Cliquez sur **Ajouter**.
2. Cliquez sur **Magasin d'applications public**.



3. Sélectionner **iPhone** ou **iPad** pour les plates-formes
4. Entrez le nom de l'application dans la zone de recherche et cliquez sur **Rechercher**.

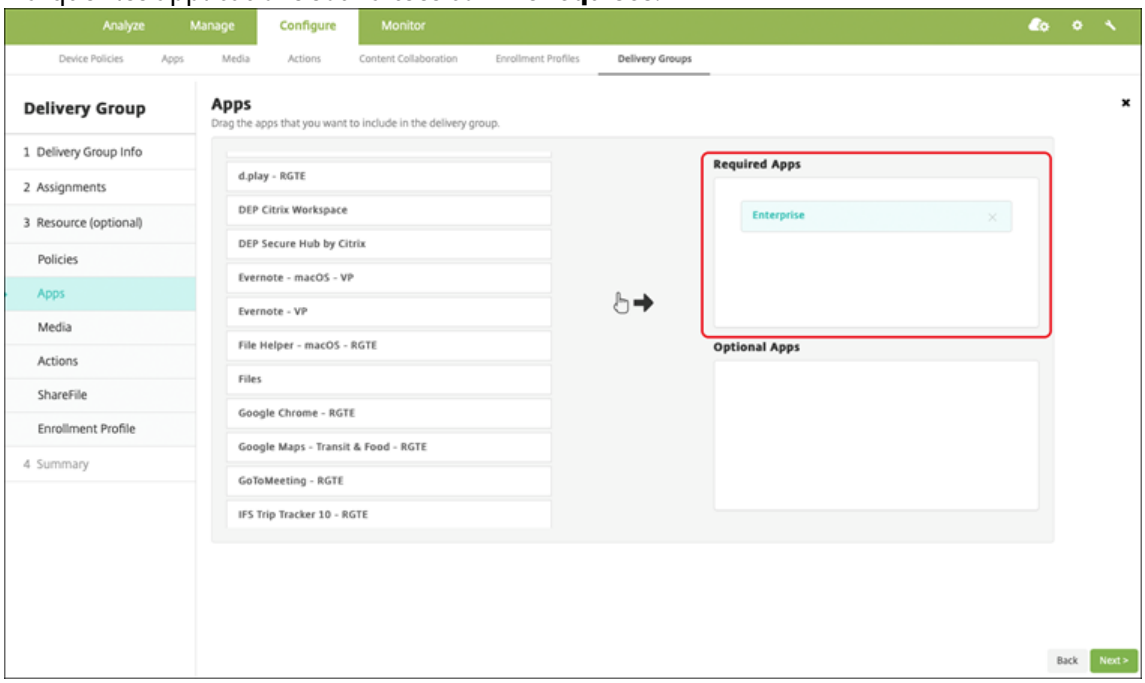


5. Les applications correspondant aux critères de recherche s'affichent. Cliquez sur l'application souhaitée.
6. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**.

Étape 2 : Configurer le déploiement de l'application

1. Dans la console XenMobile, accédez à **Configurer > Applications**.
2. Sélectionnez l'application que vous souhaitez configurer et cliquez sur **Modifier**.
3. Citrix recommande d'activer la fonctionnalité **Forcer l'application à être gérée**.
4. Affectez des groupes de mise à disposition et cliquez sur **Enregistrer**.

5. Accédez à **Configurer > Groupes de mise à disposition > Applications**.
6. Marquez les applications souhaitées comme **requises**.



7. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
8. Sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.
9. Les utilisateurs reçoivent une demande d'installation de l'application et l'application s'installe en arrière-plan une fois qu'ils ont accepté.

Applications du magasin d'applications public livrées avec l'achat en volume Apple

Vous pouvez gérer les licences d'application iOS/iPadOS via le programme d'achat en volume Apple. Procédez comme suit pour ajouter des applications d'achat en volume à XenMobile.

Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Oui
Disponible sur	iOS/iPadOS/macOS

Étape 1 : Associer les comptes

1. Effectuez la configuration et l'inscription dans Apple Business Manager (ABM) ou Apple School Manager (ASM). Pour de plus amples informations sur ces programmes, consultez la documentation Apple.
2. Associez votre compte ABM/ASM à XenMobile. Pour plus d'informations sur l'association de comptes d'achat en volume, reportez-vous à la section Achats en volume Apple.

3. Lorsque vous ajoutez votre compte d'achat en volume, activez **Mise à jour automatique des applications**. Ce paramètre garantit que les applications des appareils utilisateur se mettent automatiquement à jour lorsqu'une mise à jour apparaît dans l'Apple Store.

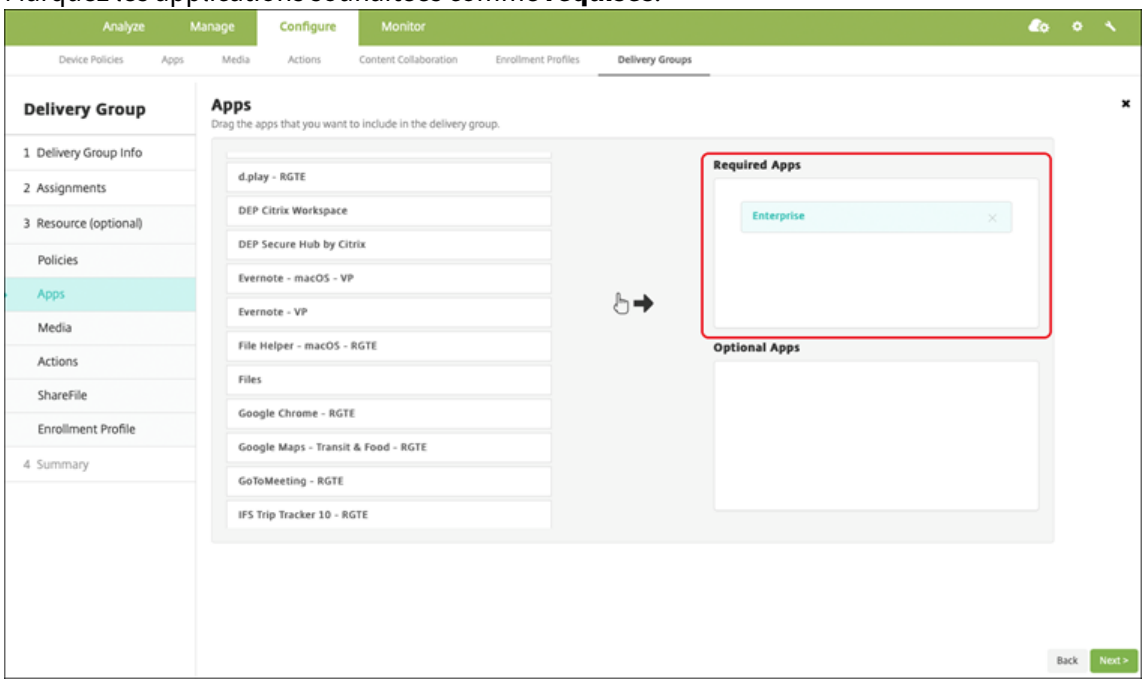
Étape 2 : Obtenir des applications et des licences Apple

Ajoutez les applications sur votre compte ABM/ASM. Vous pouvez ajouter des achats depuis l'Apple App Store ou Apple Books (pour iOS/iPadOS uniquement). N'oubliez pas que vous devez acheter toutes les applications, même si elles sont gratuites.

Pour plus d'informations sur la façon de rendre les applications accessibles à votre entreprise, reportez-vous à la documentation Apple.

Étape 3 : Configurer le déploiement des applications

1. Dans la console XenMobile, accédez à **Configurer > Applications**.
2. Sélectionnez l'application d'achat en volume que vous souhaitez configurer, puis cliquez sur **Modifier**.
3. Sélectionnez les plates-formes : **iPhone**, **iPad** ou **macOS**.
4. Citrix recommande d'activer la fonctionnalité **Forcer l'application à être gérée** (iOS/iPadOS uniquement).
5. Affectez des groupes de mise à disposition et cliquez sur **Enregistrer**.
6. Accédez à **Configurer > Groupes de mise à disposition > Applications**.
7. Marquez les applications souhaitées comme **requises**.



8. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.

9. Sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.
10. Les utilisateurs reçoivent une demande d'installation de l'application et l'application s'installe en arrière-plan une fois qu'ils ont accepté.

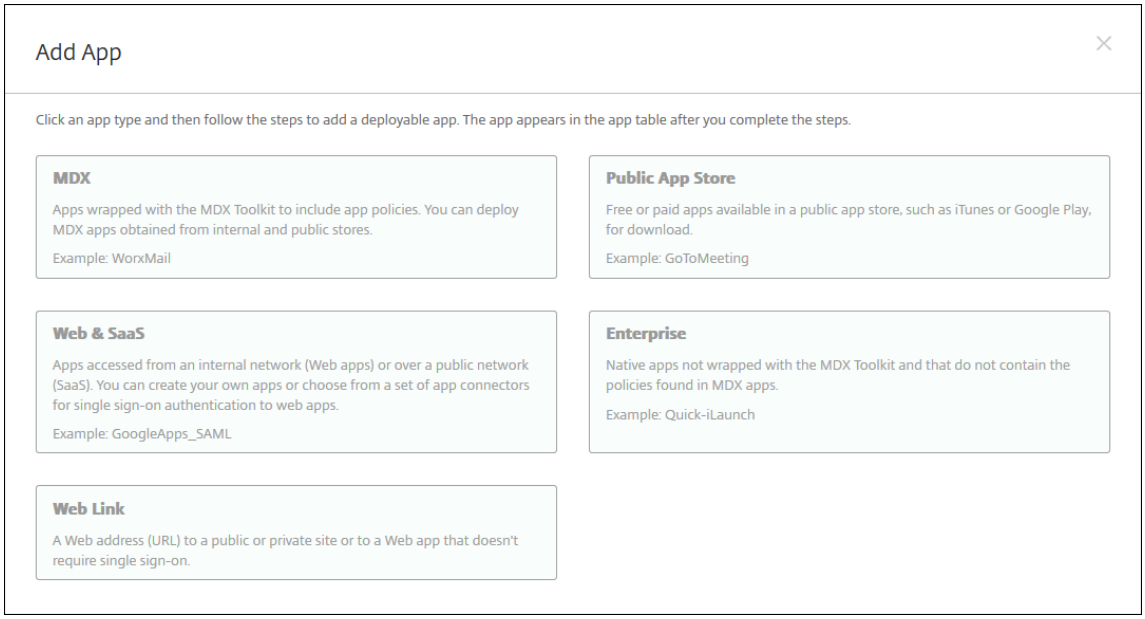
Applications d'entreprise

Vous pouvez également ajouter des applications natives pour lesquelles aucune stratégie MDX n'est associée. Procédez comme suit pour ajouter des applications qui n'existent pas sur l'App Store.

Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Oui
OS	iOS/iPadOS/macOS

Étape 1 : Ajouter et configurer des applications

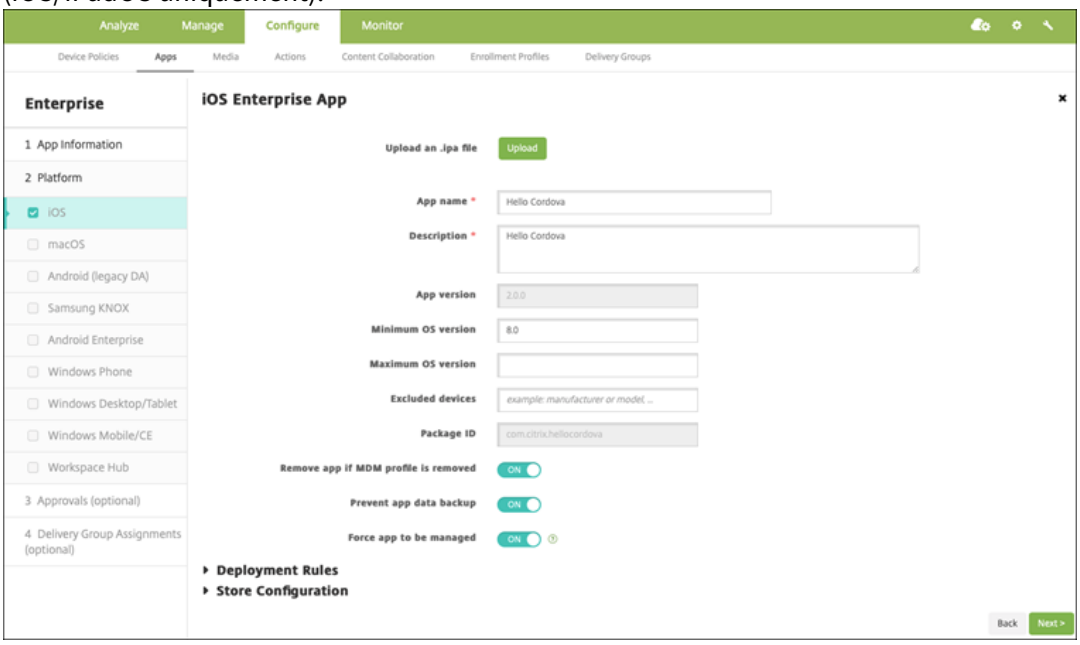
1. Dans la console XenMobile, accédez à **Configurer > Applications**. Cliquez sur **Ajouter**.
2. Cliquez sur **Entreprise**.



3. Sur la page **Informations sur l'application**, configurez les éléments suivants :
   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous Nom de l'application dans le tableau Applications.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application.
4. Cliquez sur **Suivant**. La page **Plates-formes d'applications** s'affiche.
5. Sélectionnez les plates-formes : **iPhone**, **iPad** ou **macOS**.
6. Télécharger le fichier IPA (iOS/iPadOS) ou télécharger le fichier PKG (macOS)
7. Cliquez sur **Suivant**. La page sur les **détails de l'application** s'affiche.
8. Pour configurer ces paramètres :
   - **Nom du fichier :** entrez un nouveau nom pour l'application (facultatif).
   - **Description de l'application :** entrez une nouvelle description pour l'application (facultatif).
   - **Version de l'application :** vous ne pouvez pas modifier ce champ.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
   - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.
   - **Supprimer l'application si le profil MDM est supprimé :** sélectionnez cette option si vous souhaitez supprimer l'application d'un appareil lorsque le profil MDM est supprimé. La valeur par défaut est ON. (iOS/iPados uniquement)
   - **Empêcher la sauvegarde des données d'application :** sélectionnez cette option si vous

souhaitez empêcher l'application de sauvegarder les données. La valeur par défaut est ON. (iOS/iPados uniquement)

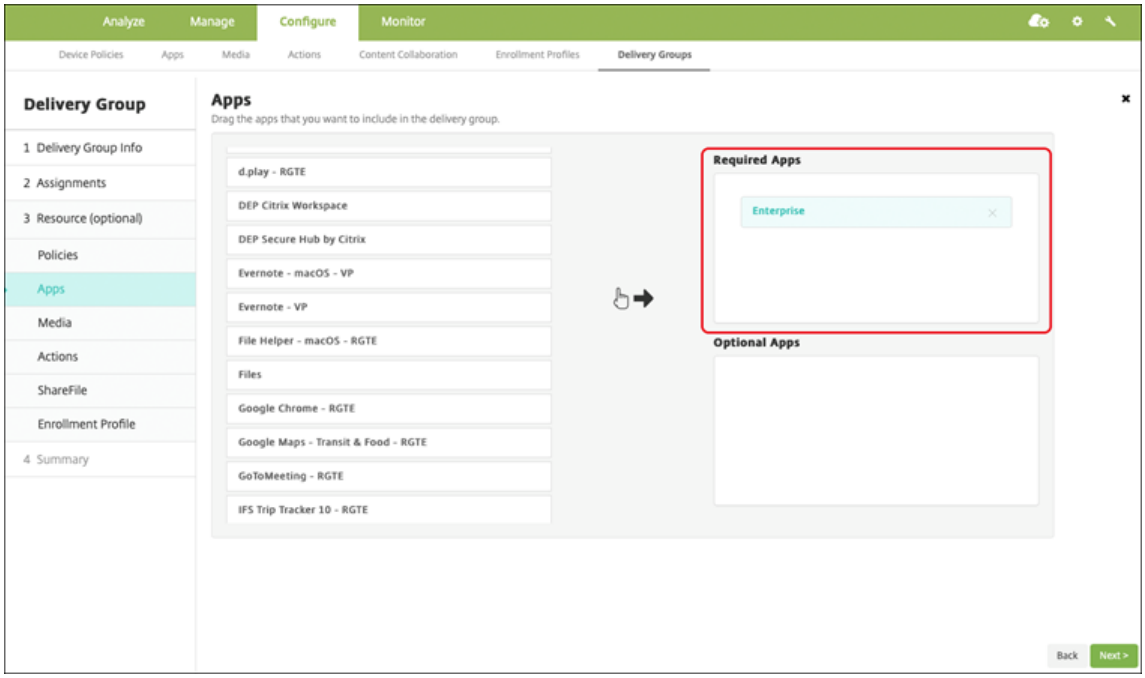
- **Forcer l'application à être gérée :** si vous installez une application non gérée, sélectionnez **Activé** si vous souhaitez que les utilisateurs sur des appareils non supervisés soient invités à autoriser la gestion de l'application. S'ils acceptent l'invite, l'application est gérée (iOS/iPadOS uniquement).



9. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**.

Étape 2 : Configurer le déploiement de l'application

1. Dans la console XenMobile, accédez à **Configurer > Groupes de mise à disposition**. Sélectionnez le groupe de mise à disposition à configurer et cliquez sur la page **Applications**.
2. Marquez les applications souhaitées comme **requises**.



3. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
4. Sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.
5. Les utilisateurs reçoivent une demande d'installation de l'application et l'application s'installe en arrière-plan une fois qu'ils ont accepté.

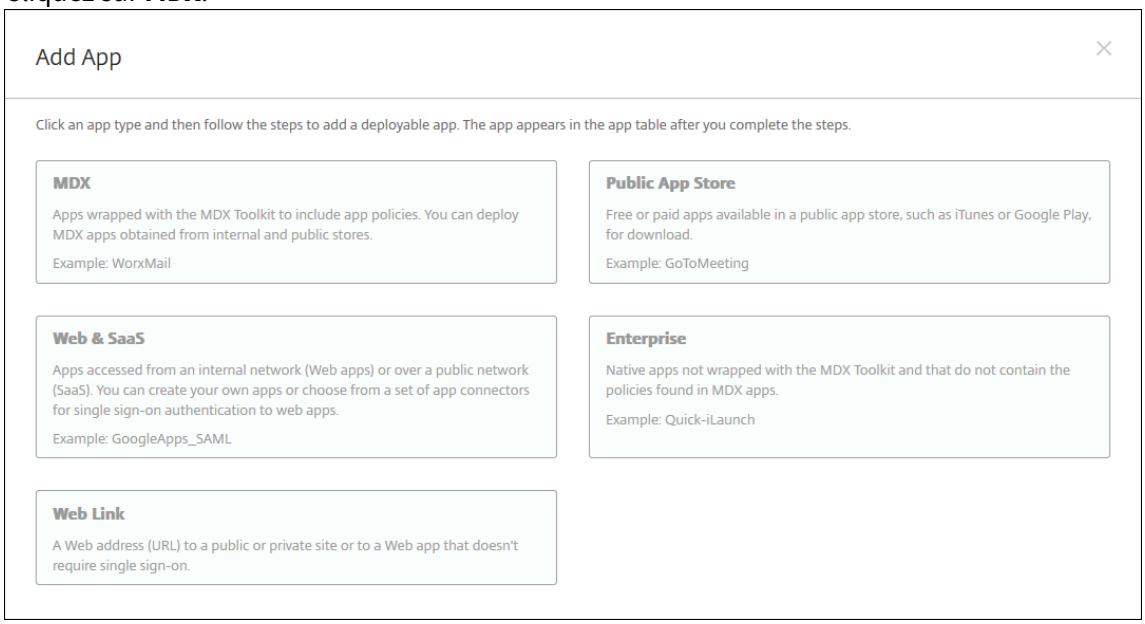
Applications MDX

Pour utiliser les stratégies MDX et les fonctionnalités de sécurité, ajoutez des applications pour lesquelles le SDK MAM est activé ou encapsulées avec MDX. Vous pouvez déployer des applications MDX avec ou sans achat en volume.

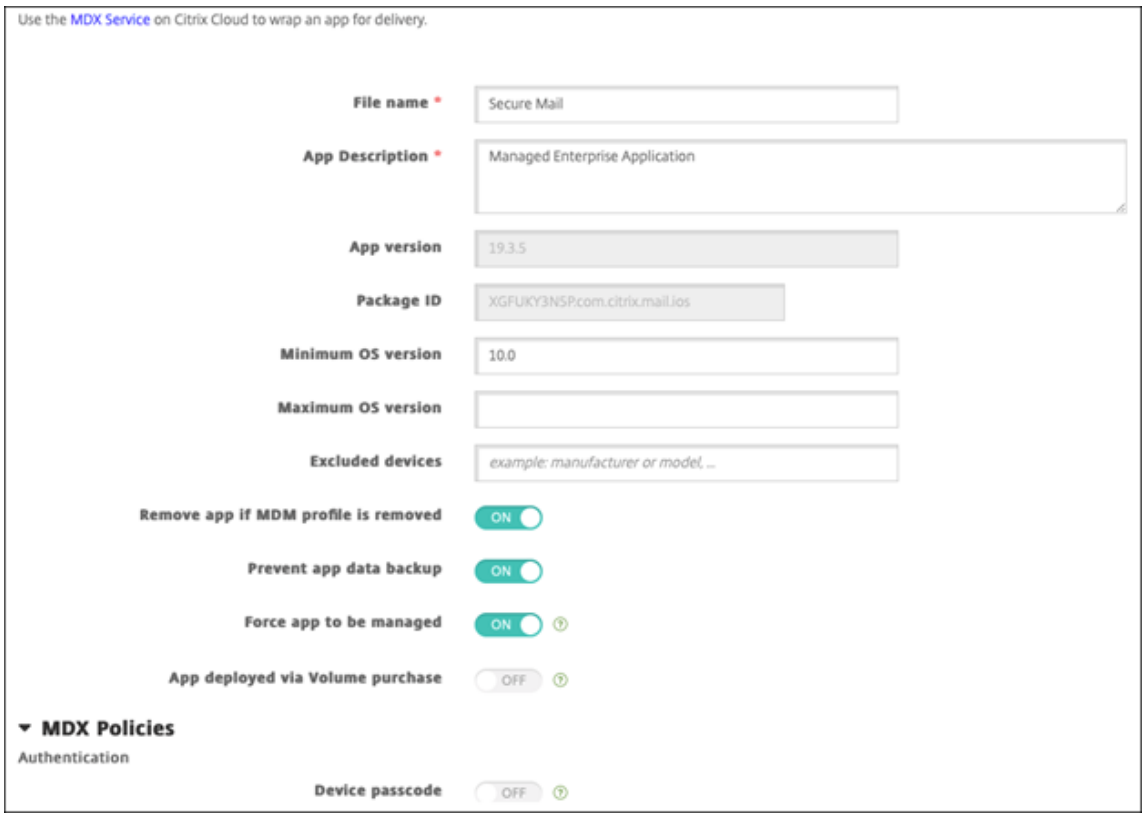
Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Oui
Disponible sur	iOS/iPadOS

Étape 1 : Ajouter et configurer des applications

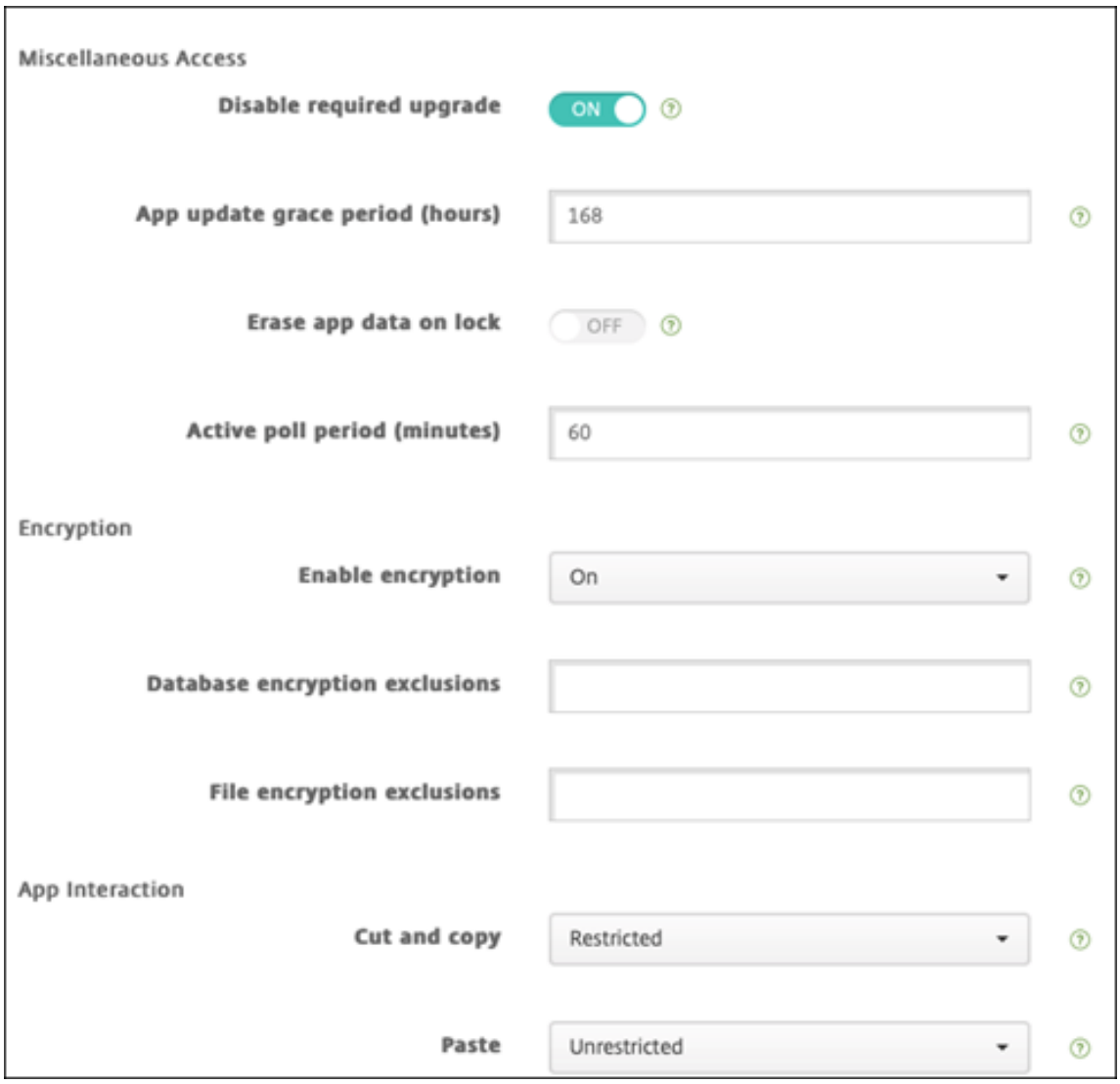
1. Dans la console XenMobile, accédez à **Configurer > Applications**. Cliquez sur **Ajouter**.
2. Cliquez sur **MDX**.



3. Sélectionnez **iPhone** ou **iPad** pour les plates-formes.
4. Chargez le fichier MDX.
5. Configurez les détails de l'application. Définissez **Application déployée via l'achat en volume** sur **Désactivé**. Citrix recommande d'activer la fonctionnalité **Forcer l'application à être gérée**.



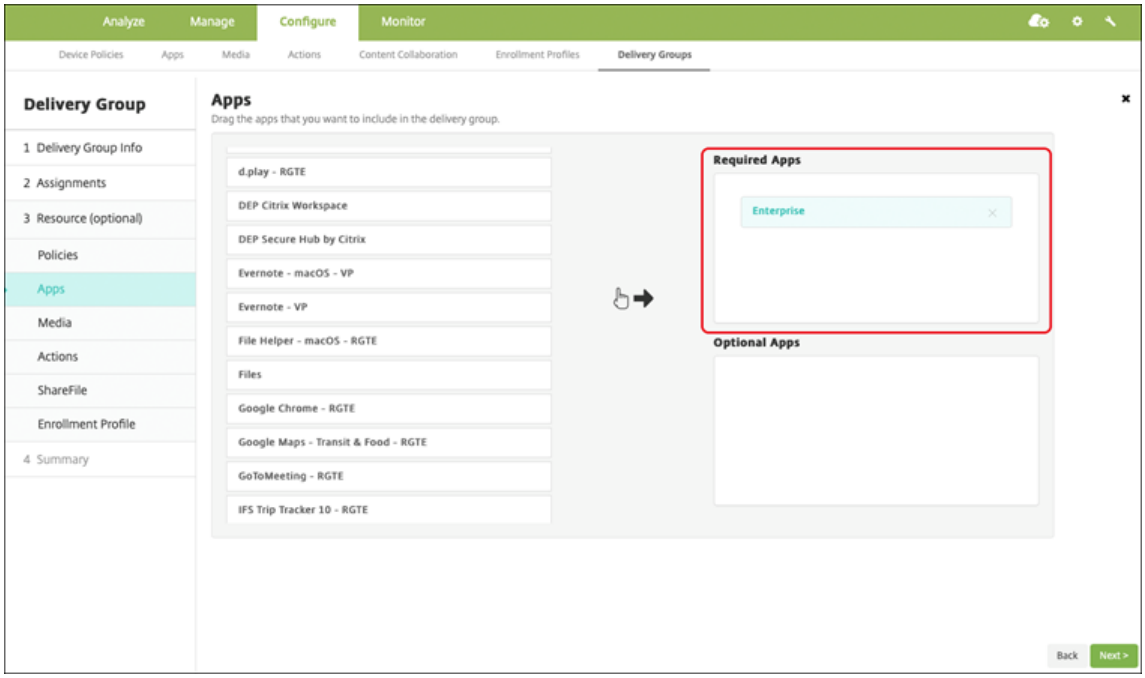
6. Configurez les stratégies MDX. Définissez **Désactiver mise à niveau requise** sur **Activé**.



7. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**.

Étape 2 : Configurer le déploiement de l'application

1. Dans la console XenMobile, accédez à **Configurer > Groupes de mise à disposition > Applications**.
2. Marquez les applications souhaitées comme **requises**.



3. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
4. Sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.
5. Les utilisateurs reçoivent une demande d'installation de l'application et l'application s'installe en arrière-plan une fois qu'ils ont accepté.

Applications MDX distribuées à l'aide d'un achat en volume Apple

Pour utiliser les stratégies MDX et les fonctionnalités de sécurité, ajoutez des applications pour lesquelles le SDK MAM est activé ou encapsulées avec MDX. Pour déployer des applications à l'aide de l'achat en volume, les applications doivent exister sur le magasin d'applications.

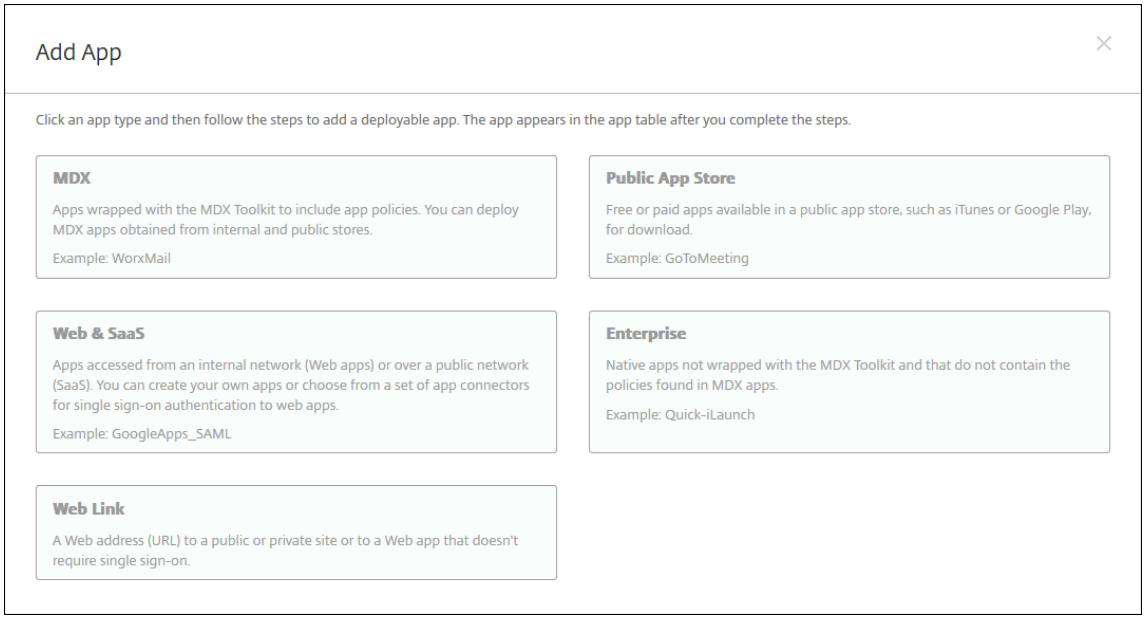
Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Oui
Disponible sur	iOS/iPadOS

Étape 1 : Associer les comptes

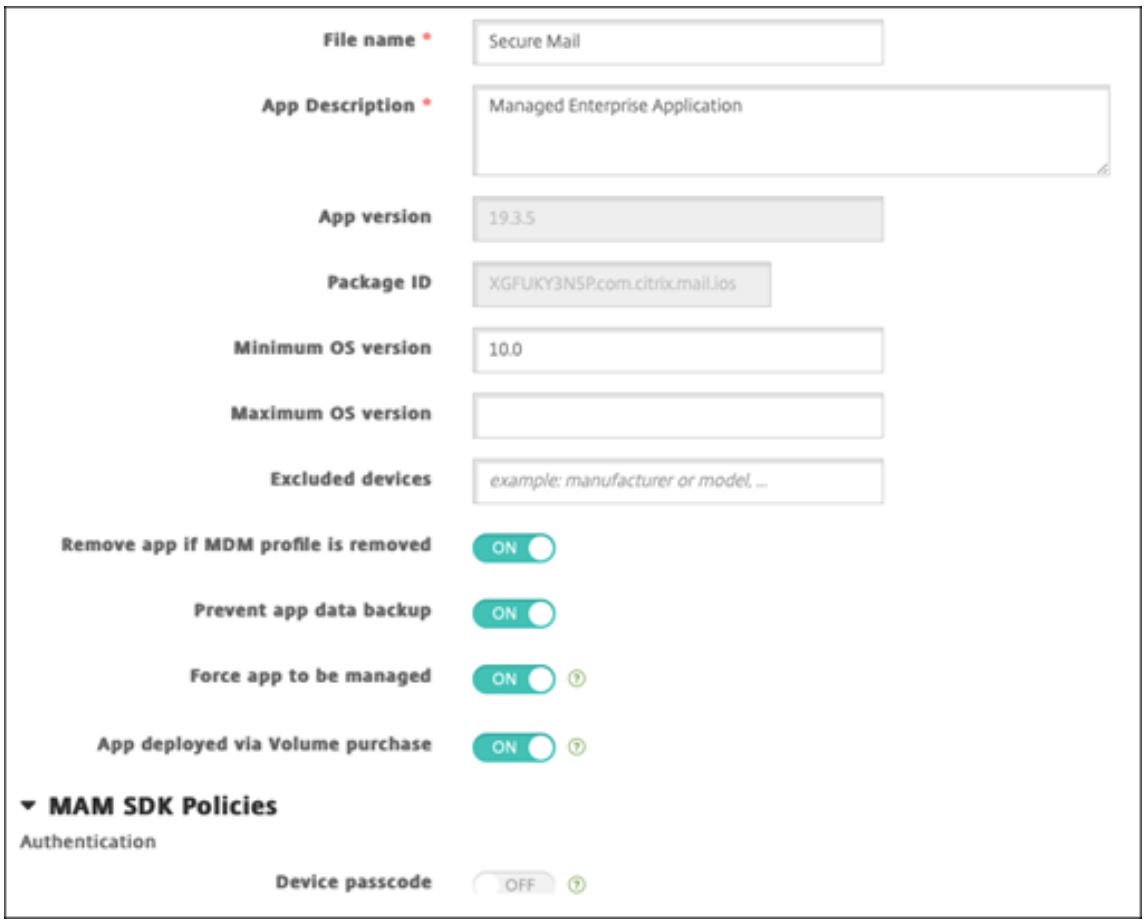
1. Effectuez la configuration et l'inscription dans Apple Business Manager (ABM) ou Apple School Manager (ASM). Pour de plus amples informations sur ces programmes, consultez la documentation Apple.
2. Associez votre compte ABM/ASM à XenMobile. Pour plus d'informations sur l'association de comptes d'achat en volume, reportez-vous à la section Achats en volume Apple.
3. Lorsque vous ajoutez votre compte d'achat en volume, activez **Mise à jour automatique des applications**. Ce paramètre garantit que les applications des appareils utilisateur se mettent automatiquement à jour lorsqu'une mise à jour apparaît dans l'Apple Store.

Étape 2 : Ajouter et configurer des applications

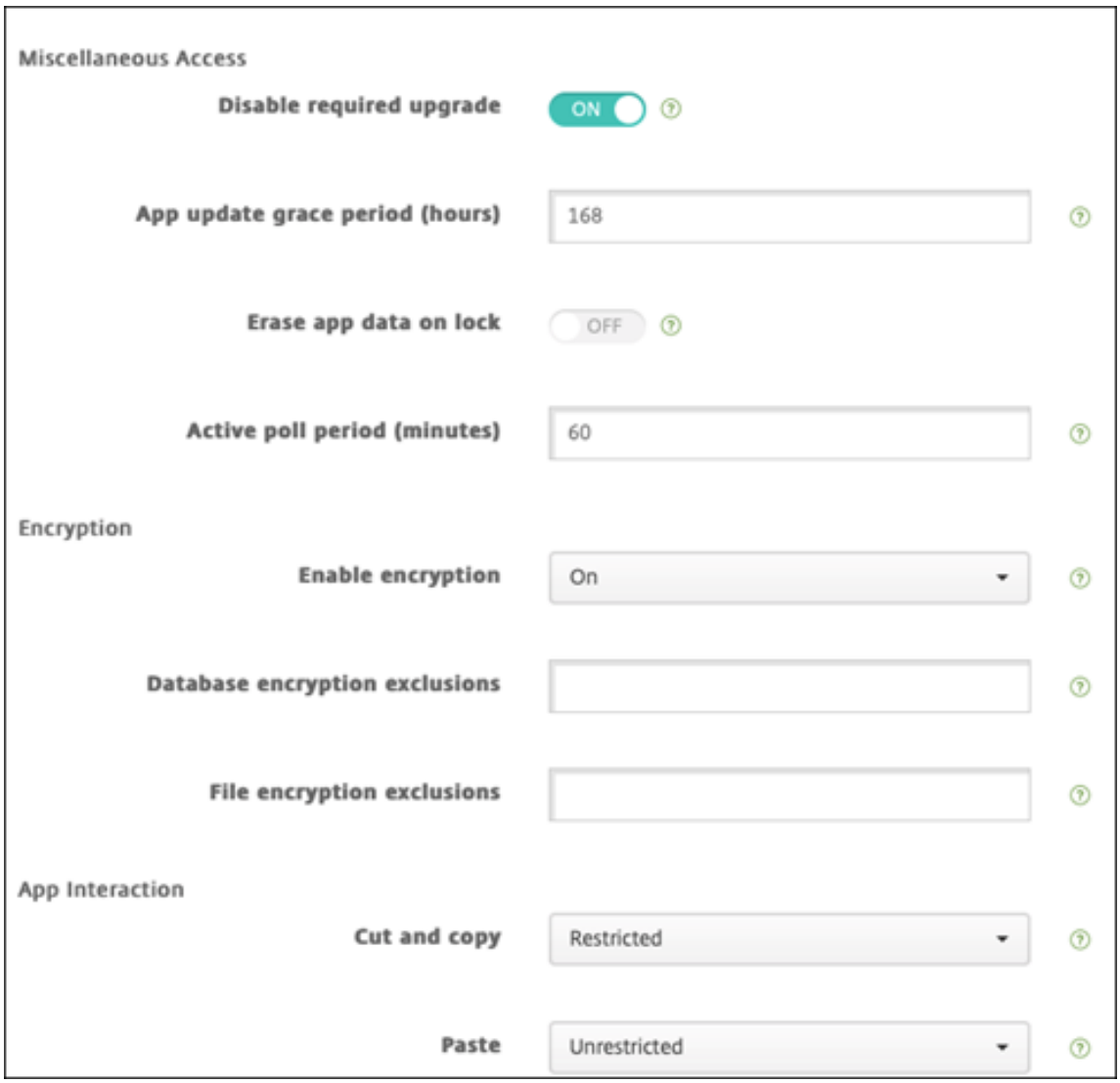
1. Dans la console XenMobile, accédez à **Configurer > Applications**. Cliquez sur **Ajouter**.
2. Cliquez sur **MDX**.



3. Sélectionnez **iPhone** ou **iPad** pour les plates-formes.
4. Chargez le fichier MDX.
5. Configurez les détails de l'application. Définissez **Application déployée via l'achat en volume** sur **Désactivée**. Citrix recommande d'activer la fonctionnalité **Forcer l'application à être gérée**.



6. Configurez les stratégies MDX. Définissez **Désactiver mise à niveau requise** sur **Activé**.

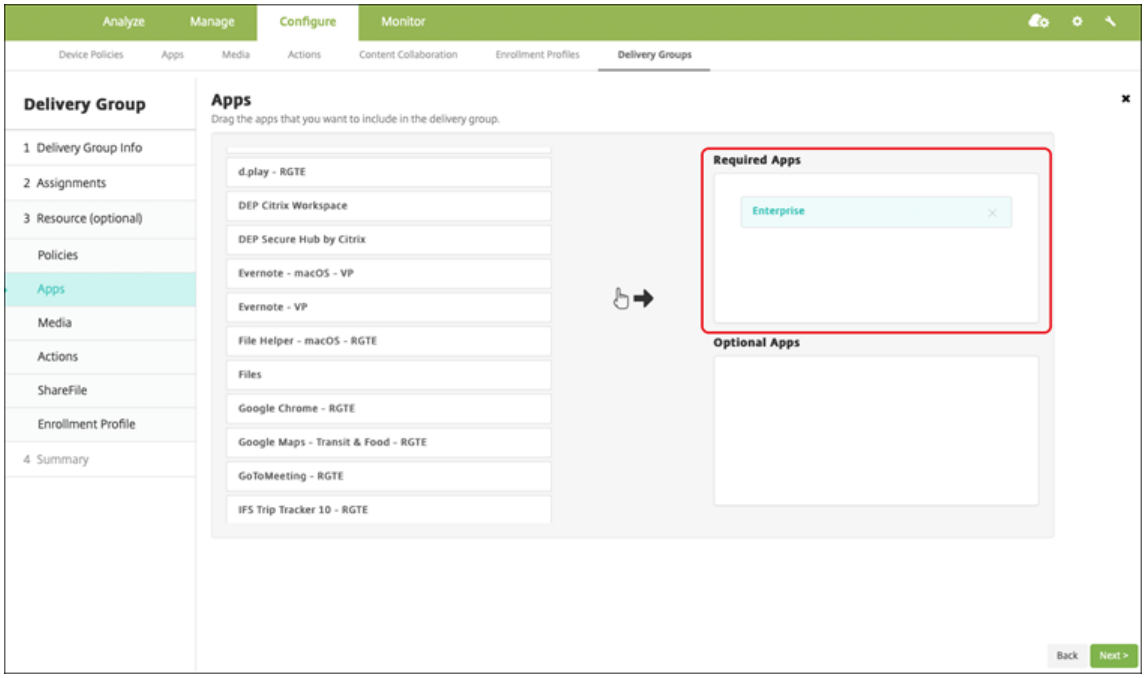


7. Affectez un groupe de mise à disposition à l'application pour chaque plate-forme et cliquez sur **Enregistrer**.

Avec cette configuration, deux entrées sont répertoriées pour cette application dans la liste des applications. Lorsque vous sélectionnez une application à configurer, sélectionnez l'application avec **Type MDX**.

Étape 3 : Configurer le déploiement des applications

1. Dans la console XenMobile, accédez à **Configurer > Groupes de mise à disposition > Applications**.
2. Marquez des applications avec achat en volume comme **requises** si vous le souhaitez.



3. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
4. Sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.
5. Les utilisateurs reçoivent une demande d'installation de l'application et l'application s'installe en arrière-plan une fois qu'ils ont accepté.

Applications personnalisées

Les applications personnalisées sont des applications propriétaires B2B. Vous pouvez utiliser XenMobile et l'achat en volume Apple pour distribuer des applications propriétaires de manière privée et sécurisée. Vous pouvez distribuer les applications à des partenaires, clients, franchisés et employés internes spécifiques.

Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Oui
Disponible sur	iOS/iPadOS

Conditions requises pour les applications personnalisées

- Compte Apple Business Manager ou Apple School Manager
- Compte d'achat en volume Apple (nécessite des appareils avec iOS 7 ou version ultérieure)
- Inscrire des appareils dans XenMobile à l'aide de l'un des modes d'inscription Apple suivants :
  - Inscription automatique des appareils
  - Inscription des appareils
  - Inscription de l'utilisateur

Étape 1 : Associer les comptes

Pour déployer des applications personnalisées à l'aide de l'achat en volume, associez votre compte d'achat en volume à XenMobile.

1. Effectuez la configuration et l'inscription dans Apple Business Manager (ABM). Pour de plus amples informations sur ces programmes, consultez la documentation Apple.
2. Associez votre compte ABM à XenMobile. Pour plus d'informations sur l'association de comptes d'achat en volume, reportez-vous à la section Achats en volume Apple.
3. Lorsque vous ajoutez votre compte d'achat en volume, activez **Mise à jour automatique des applications**. Ce paramètre garantit que les applications des appareils utilisateur se mettent automatiquement à jour lorsqu'une mise à jour apparaît dans l'Apple Store.

Étape 2 : Configurer les applications sur ABM

Ajoutez les applications sur votre compte ABM. Vous pouvez charger et distribuer vos propres applications personnalisées ou acheter des licences pour des applications personnalisées auprès d'autres

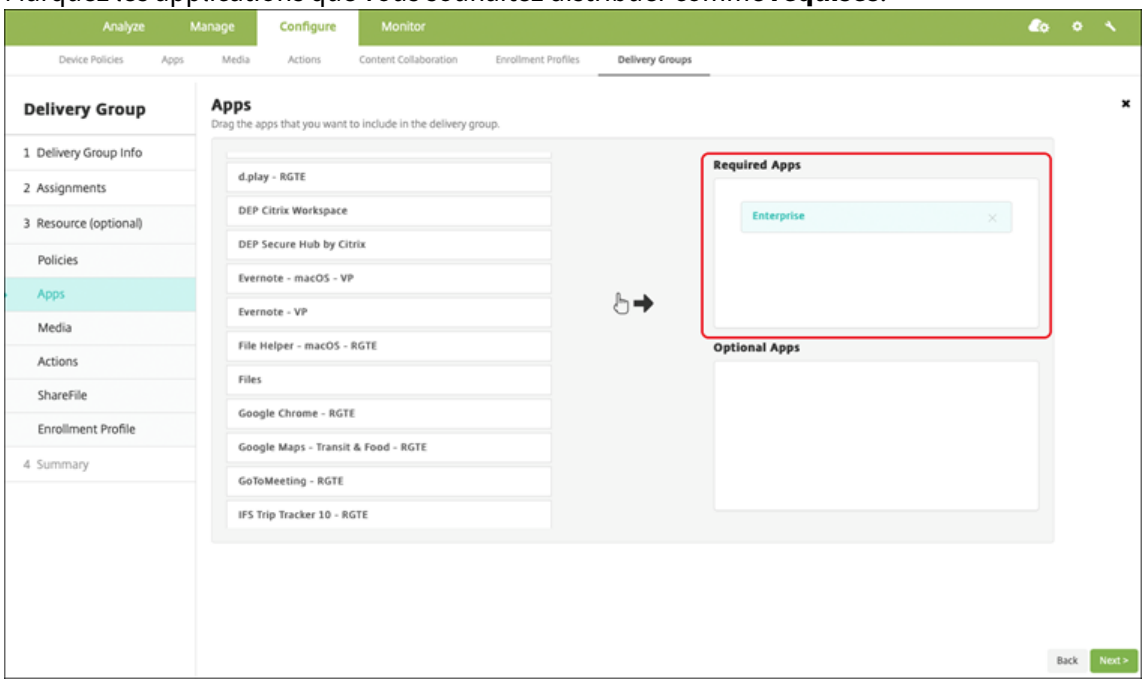
organisations. Pour plus d'informations sur l'ajout et l'activation d'applications personnalisées sur ABM, reportez-vous à la documentation Apple.

Étape 3 : Ajouter et configurer des applications dans XenMobile

1. Dans la console XenMobile, accédez à **Configurer > Applications**. Les applications d'achat en volume apparaissent dans la liste des applications.
2. Sélectionnez l'application que vous souhaitez configurer. Cliquez sur **Modifier**.
3. Sélectionnez les plates-formes : **iPhone**, **iPad** ou **macOS**.
4. Choisissez les groupes de mise à disposition vers lesquels vous souhaitez que l'application soit distribuée. Cliquez sur **Enregistrer**.

Étape 4 : Configurer le déploiement des applications

1. Dans la console XenMobile, accédez à **Configurer > Groupes de mise à disposition > Applications**.
2. Marquez les applications que vous souhaitez distribuer comme **requises**.



3. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
4. Sélectionnez le groupe de mise à disposition que vous souhaitez déployer, puis cliquez sur **Déployer**.
5. Les utilisateurs reçoivent une demande de déploiement d'applications. Les applications s'installent en arrière-plan après que les utilisateurs les ont acceptées.

Applications personnalisées MDX

Pour utiliser les stratégies MDX et les fonctionnalités de sécurité, ajoutez des applications personnalisées pour lesquelles le SDK MAM est activé ou encapsulées avec MDX.

Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Oui
Disponible sur	iOS/iPadOS

Étape 1 : Associer les comptes

Pour déployer des applications personnalisées à l'aide de l'achat en volume, associez votre compte d'achat en volume à XenMobile.

1. Effectuez la configuration et l'inscription dans Apple Business Manager (ABM). Pour de plus amples informations sur ces programmes, consultez la documentation Apple.
2. Associez votre compte ABM à XenMobile. Pour plus d'informations sur l'association de comptes

d'achat en volume, reportez-vous à la section Achats en volume Apple.

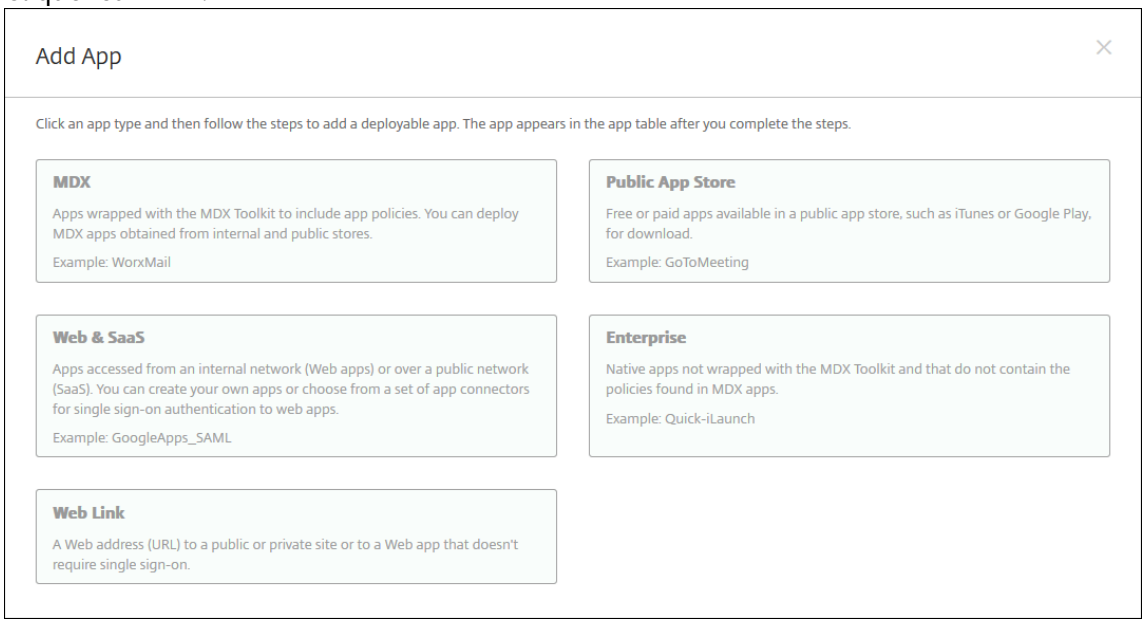
3. Lorsque vous ajoutez votre compte d'achat en volume, activez **Mise à jour automatique des applications**. Ce paramètre garantit que les applications des appareils utilisateur se mettent automatiquement à jour lorsqu'une mise à jour apparaît dans l'Apple Store.

Étape 2 : Configurer les applications sur ABM

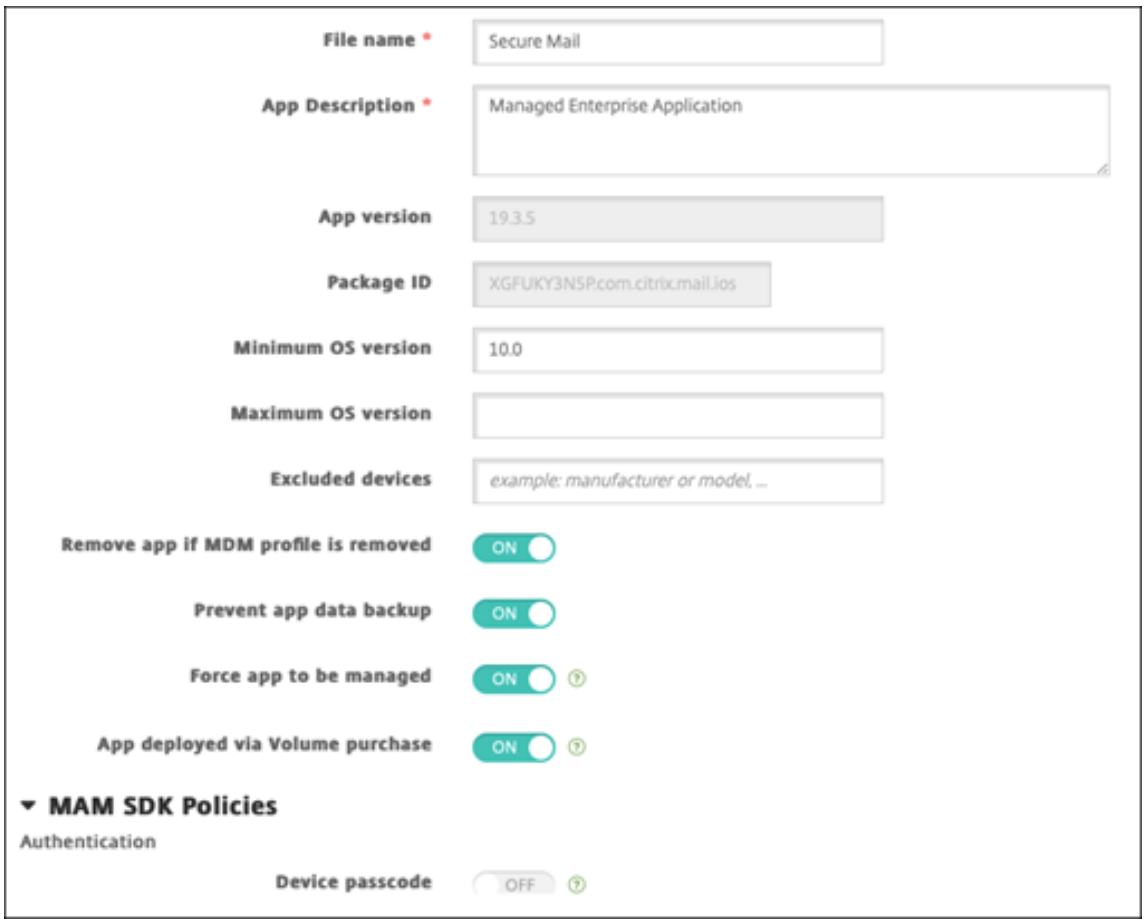
Ajoutez les applications sur votre compte ABM. Vous pouvez charger et distribuer vos propres applications personnalisées ou acheter des licences pour des applications personnalisées auprès d'autres organisations. Pour plus d'informations sur l'ajout et l'activation d'applications personnalisées sur ABM, reportez-vous à la documentation Apple.

Étape 3 : Ajouter et configurer des applications dans XenMobile

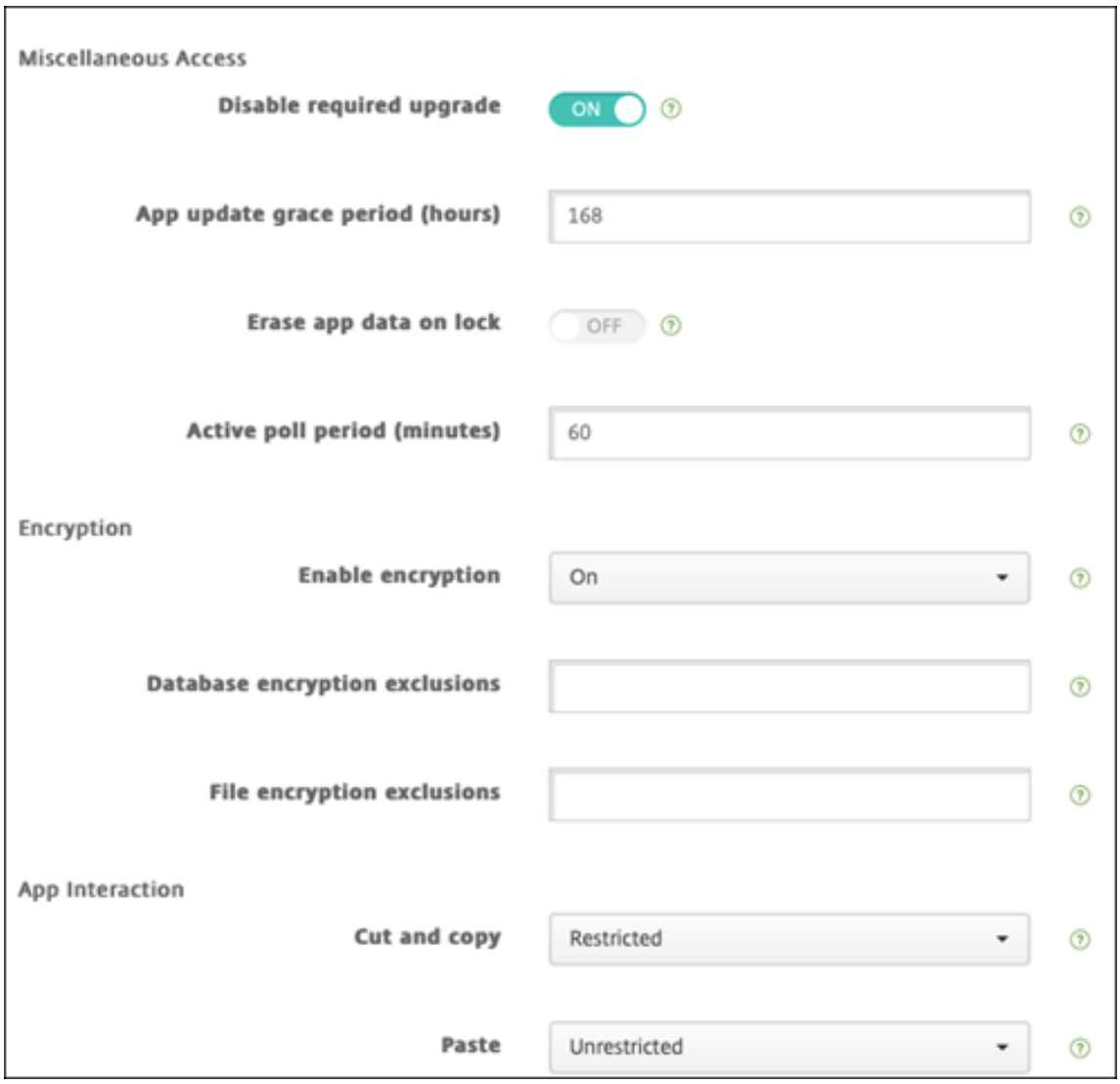
1. Dans la console XenMobile, accédez à **Configurer > Applications**. Cliquez sur **Ajouter**.
2. Cliquez sur **MDX**.



3. Sélectionnez les plateformes **iPhone** ou **iPad**.
4. Chargez le fichier MDX de l'application que vous souhaitez ajouter.
5. Configurez les détails de l'application. Définissez **Application déployée via l'achat en volume** sur **Désactivée**. Citrix recommande d'activer la fonctionnalité **Forcer l'application à être gérée**.



6. Configurez les stratégies MDX. Définissez **Désactiver mise à niveau requise** sur **Activé**.

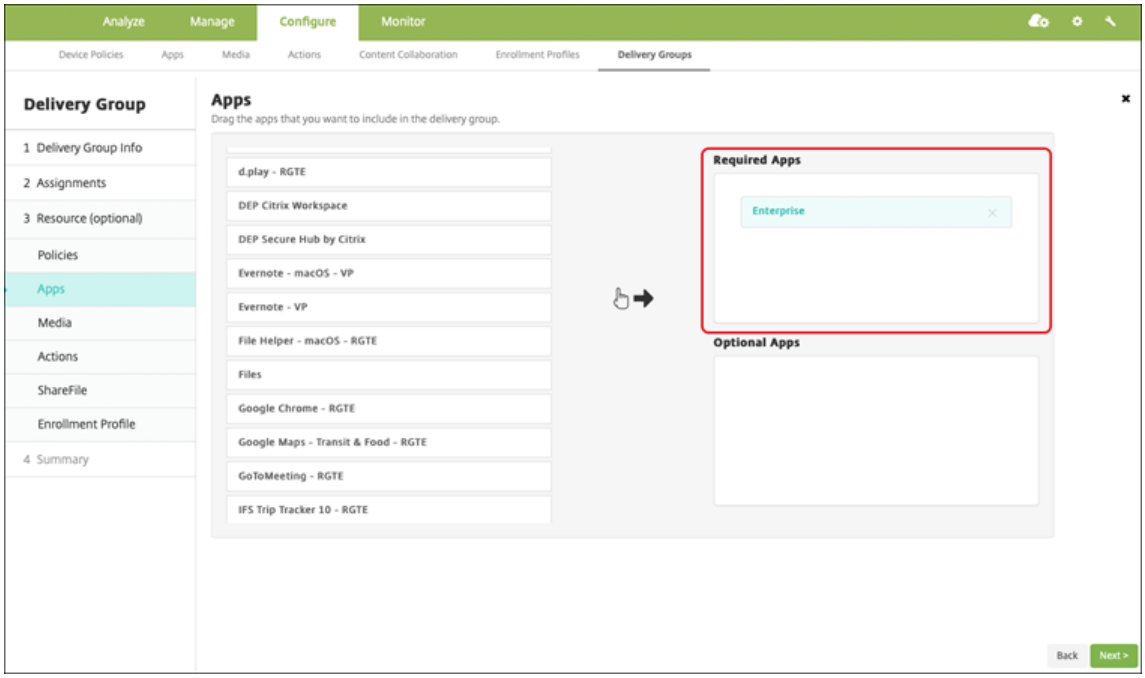


7. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**.

Avec cette configuration, deux entrées sont répertoriées pour cette application dans la liste des applications. Lorsque vous sélectionnez une application à configurer, sélectionnez l'application avec **Type MDX**.

Étape 4 : Configurer le déploiement des applications

1. Dans la console XenMobile, accédez à **Configurer > Applications**. Les applications d'achat en volume apparaissent dans la liste des applications.
2. Sélectionnez l'application que vous souhaitez configurer. Cliquez sur **Modifier**.
3. Choisissez les groupes de mise à disposition vers lesquels vous souhaitez que l'application soit distribuée sur chaque plate-forme. Cliquez sur **Enregistrer**.
4. Naviguez jusqu'à **Configurer > Groupes de mise à disposition > Applications**.
5. Marquez les applications que vous souhaitez distribuer comme **requises**.



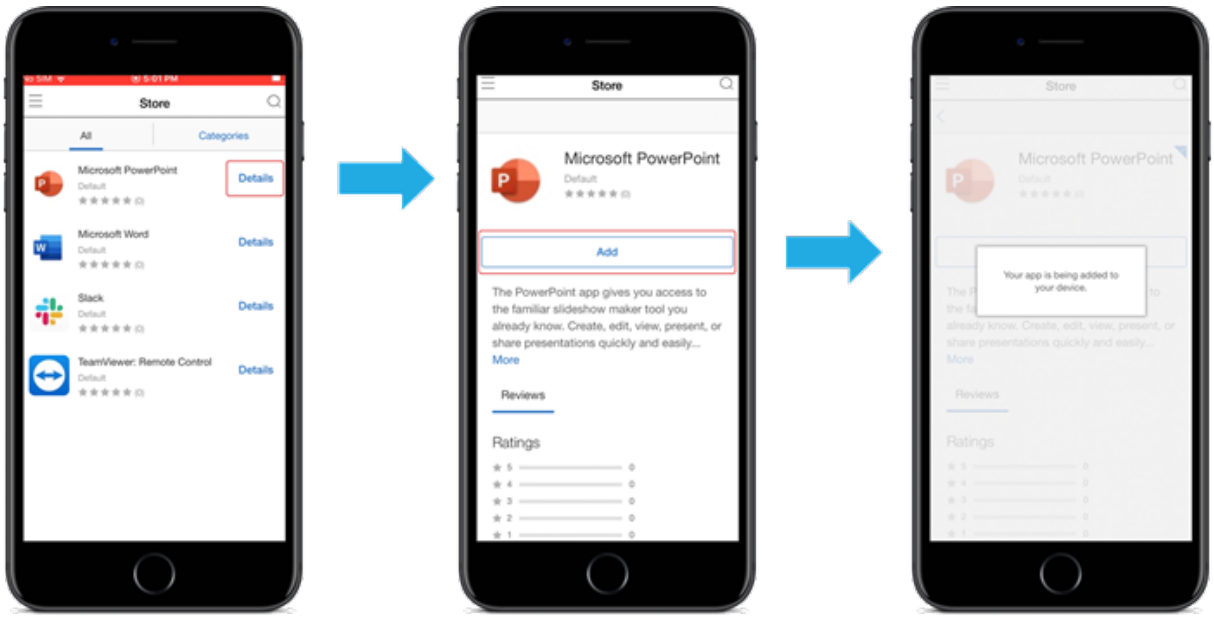
6. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
7. Sélectionnez le groupe de mise à disposition que vous souhaitez déployer, puis cliquez sur **Déployer**.
8. Les utilisateurs reçoivent une demande de déploiement d'applications. Les applications s'installent en arrière-plan après leur acceptation.

Applications facultatives (iOS/iPadOS uniquement)

Citrix recommande le déploiement des applications comme **requises**. Les applications requises s'installent silencieusement sur les appareils utilisateur, ce qui minimise l'interaction. L'activation de cette fonctionnalité permet également aux applications de se mettre à jour automatiquement.

Les applications facultatives permettent aux utilisateurs de choisir les applications à installer, mais les utilisateurs doivent initier l'installation manuellement via Secure Hub.

Pour installer des applications facultatives, les utilisateurs doivent lancer Secure Hub, aller dans le **magasin**, sélectionner **Détails** pour l'application souhaitée, puis cliquer sur **Ajouter**.



Contrôle d'accès réseau

January 10, 2022

Vous pouvez étendre l'évaluation de la sécurité des appareils Endpoint Management via votre solution de contrôle d'accès réseau (NAC) pour les appareils Android et Apple. Votre solution NAC peut utiliser l'évaluation de sécurité XenMobile pour faciliter et gérer les décisions d'authentification. Une fois le boîtier NAC configuré, les stratégies d'appareil et les filtres NAC que vous configurez dans XenMobile sont appliqués.

L'utilisation de XenMobile avec une solution NAC ajoute la qualité de service et un contrôle plus précis sur les appareils internes à votre réseau. Pour un résumé des avantages de l'intégration de NAC avec XenMobile, consultez la section Contrôle d'accès.

Citrix prend en charge ces solutions pour l'intégration avec XenMobile :

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

Citrix ne garantit pas l'intégration avec d'autres solutions NAC.

Avec un boîtier de contrôle d'accès réseau (NAC) dans votre réseau :

- XenMobile prend en charge NAC en tant que fonctionnalité de sécurité de point de terminaison pour les appareils iOS, Android Enterprise et Android.
- Vous pouvez activer les filtres dans XenMobile pour définir les appareils comme conformes ou non conformes pour NAC, en fonction de règles ou de propriétés. Par exemple :
  - Si un appareil géré dans XenMobile ne répond pas aux critères spécifiés, XenMobile marque l'appareil comme étant non conforme. Le boîtier NAC bloque les appareils non conformes sur votre réseau.
  - Si un appareil géré dans XenMobile a installé des applications non conformes, un filtre NAC peut bloquer la connexion VPN. Par conséquent, une machine utilisateur non conforme ne peut pas accéder aux applications ou aux sites Web via le VPN.
  - Si vous utilisez Citrix Gateway pour NAC, vous pouvez activer le split tunneling pour empêcher le plug-in Citrix Gateway d'envoyer du trafic réseau inutile à Citrix Gateway. Pour plus d'informations sur le split tunneling, voir Configurer le split tunneling.

Filtres de conformité NAC pris en charge

XenMobile Server prend en charge les filtres de conformité au contrôle d'accès réseau (NAC) suivants :

Appareils anonymes : vérifie si un appareil est en mode anonyme. Cette vérification est disponible si XenMobile ne parvient pas à authentifier à nouveau l'utilisateur lorsqu'un appareil tente de se reconnecter.

Échec de l'attestation Samsung Knox : vérifie si un appareil n'est pas parvenu à répondre à une requête du serveur d'attestation Samsung Knox.

Applications sur liste noire : vérifie si un appareil dispose d'applications interdites, telles que définies dans une stratégie d'accès aux applications. Pour plus d'informations sur la stratégie, consultez la section Stratégies d'accès aux applications.

Appareils inactifs : vérifie si un appareil est inactif, tel que cela est défini par le paramètre **Nombre de jours maximum d'inactivité** dans la boîte de dialogue **Propriétés du serveur**. Pour de plus amples informations, consultez la section Propriétés du serveur.

Applications requises manquantes : vérifie si des applications nécessaires sont manquantes sur un appareil, tel que cela est défini dans une stratégie d'accès aux applications.

Applications non suggérées : vérifie si un appareil dispose d'applications non suggérées, telles que définies dans une stratégie d'accès aux applications.

Mot de passe non conforme : vérifie si le mot de passe utilisateur est conforme. Sur les appareils iOS et Android, XenMobile peut déterminer si le mot de passe actuel de l'appareil est conforme à la stratégie de code secret envoyée à l'appareil. Par exemple, sur iOS, l'utilisateur dispose de 60 minutes pour définir un mot de passe si XenMobile envoie une stratégie de code secret à l'appareil. Avant qu'un mot de passe ne soit défini par l'utilisateur, le code secret peut ne pas être conforme.

Appareils non conformes : vérifie si un appareil n'est pas conforme, en fonction de la propriété de l'appareil Non conforme. En règle générale, les actions automatisées ou des tiers utilisant les API XenMobile modifient cette propriété d'appareil.

État révoqué : vérifie si le certificat de l'appareil a été révoqué. Un appareil révoqué ne peut pas se réinscrire tant qu'il n'a pas été à nouveau autorisé.

Appareils Android rootés et iOS jailbreakés : vérifie si un appareil Android ou iOS est rooté ou jailbreaké.

Appareils non gérés : vérifie si un appareil est toujours dans un état géré, sous le contrôle de XenMobile. Par exemple, un appareil inscrit en mode MAM ou un appareil non inscrit n'est pas géré.

> **Remarque :**
>
> Le filtre Conformité/non conformité implicite définit la valeur par défaut uniquement sur les appareils qui sont gérés par XenMobile. Par exemple, tous les appareils sur lesquels une application bloquée est installée ou qui ne sont pas inscrits sont marqués comme Non conformes. Le boîtier de contrôle d'accès réseau (NAC) bloque ces appareils de votre réseau.

Présentation de la configuration

Nous vous recommandons de configurer les composants NAC dans l'ordre indiqué.

1. Configurez les stratégies d'appareil pour prendre en charge NAC :

   Pour les appareils iOS : voir Configurer la stratégie VPN pour prendre en charge NAC.

   Pour les appareils Android Enterprise : voir Créer une configuration gérée par Android Enterprise pour Citrix SSO.

   Pour les appareils Android : voir Configurer le protocole Citrix SSO pour Android.

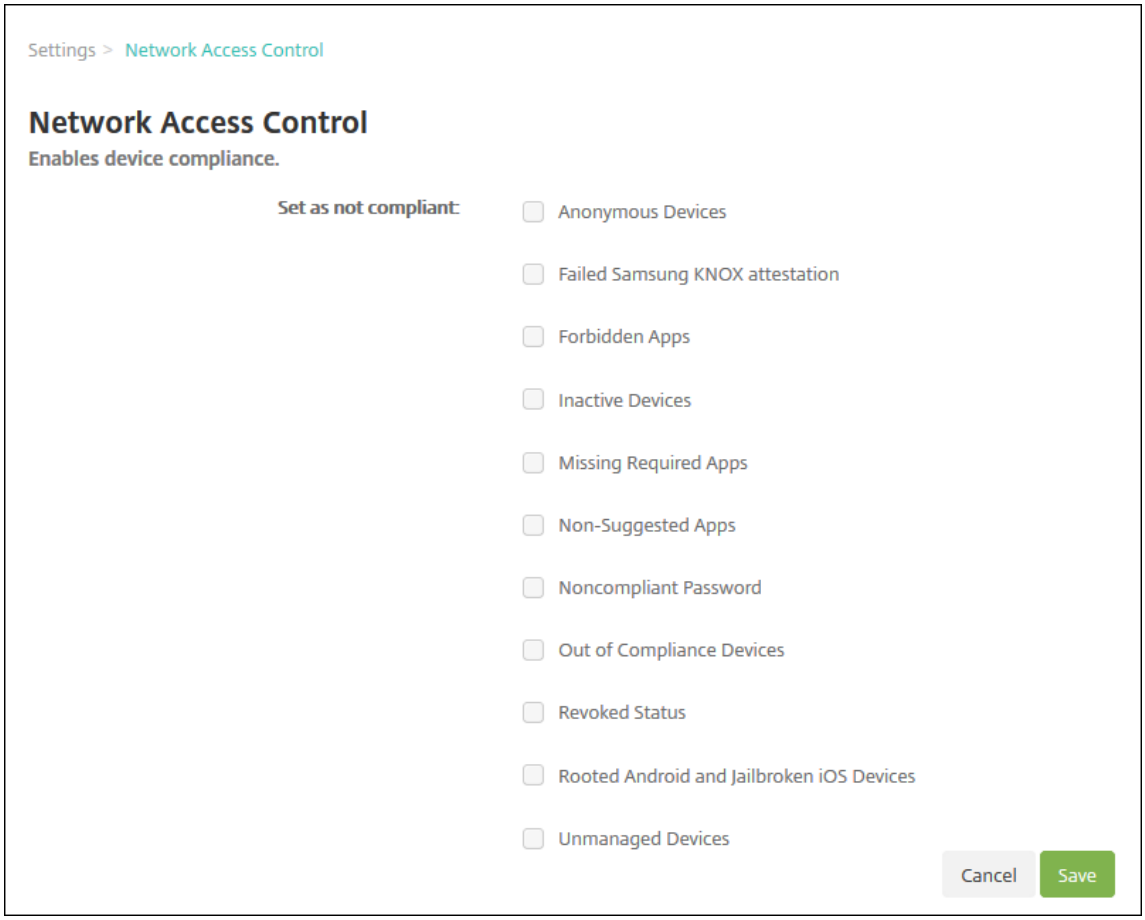
2. Activer les filtres NAC dans XenMobile.
3. Configurer une solution NAC :
   - Citrix Gateway, détaillé dans Mettre à jour les stratégies Citrix Gateway afin de prendre en charge NAC.

     Nécessite l'installation de Citrix SSO sur les appareils. Voir Clients Citrix Gateway.

- Cisco ISE : consultez la documentation Cisco.
- ForeScout : consultez la documentation ForeScout.

Activer les filtres NAC dans XenMobile

1. Dans la console XenMobile, accédez à **Paramètres > Contrôle d'accès réseau**.



2. Cochez les cases correspondant aux filtres **Définir comme non conforme** que vous souhaitez activer.
3. Cliquez sur **Enregistrer**.

Mettre à jour les stratégies Citrix Gateway afin de prendre en charge NAC

Vous devez configurer les stratégies d'authentification avancée (et non classique) et de sessions VPN sur votre serveur virtuel VPN.

Ces étapes mettent à jour Citrix Gateway avec l'une des caractéristiques suivantes :

- Est intégré à un environnement XenMobile Server.

- Ou, est configuré pour VPN, ne fait pas partie de l'environnement XenMobile Server et peut atteindre XenMobile.

Sur votre serveur VPN virtuel, depuis une fenêtre de console, procédez comme suit. Les adresses IP dans les commandes et les exemples sont fictives.

1. Supprimez et annulez la liaison de toutes les stratégies classiques si vous utilisez des stratégies classiques sur votre serveur virtuel VPN. Pour vérifier, tapez :

   ```
   show vpn vserver <VPN_VServer>
   ```

   Supprimez tout résultat contenant le terme « Classic ». Pa exemple : `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

   Pour supprimer la stratégie, tapez :

   ```
   unbind vpn vserver <VPN_VServer> -policy <policy_name>
   ```

2. Créez la stratégie de session avancée correspondante en tapant ce qui suit.

   ```
   add vpn sessionPolicy <policy_name> <rule> <session action>
   ```

   Pa exemple : `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. Liez la stratégie à votre serveur virtuel VPN en tapant ce qui suit.

   ```
   bind vpn vserver _XM_XenMobileGateway -policy vpn_nac -priority 100
   ```

4. Créez un serveur virtuel d'authentification en tapant ce qui suit.

   ```
   add authentication vserver <authentication vserver name> <service type>
    <ip address>
   ```

   Par exemple : `add authentication vserver authvs SSL 0.0.0.0`
   Dans l'exemple, `0.0.0.0` signifie que le serveur virtuel d'authentification n'est pas public.

5. Liez un certificat SSL au serveur virtuel en tapant ce qui suit.

   ```
   bind ssl vserver <authentication vserver name> -certkeyName <Webserver
   certificate>
   ```

   Pa exemple : `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. Associez un profil d'authentification au serveur virtuel d'authentification à partir du serveur virtuel VPN. Commencez par créer le profil d'authentification en tapant ce qui suit.

   ```
   add authentication authnProfile <profile name> -authnVsName <authentication
    vserver name>
   ```

   Par exemple :

   ```
   add authentication authnProfile xm_nac_prof -authnVsName authvs
   ```


7. Associez le profil d'authentification au serveur virtuel VPN en tapant ce qui suit.

   ```
   set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
   ```

   Par exemple :

   ```
   set vpn vserver _XM_XenMobileGateway -authnProfile xm_nac_prof
   ```

8. Vérifiez la connexion de Citrix Gateway à un appareil en tapant ce qui suit.

   ```
   curl -v -k https://<XenMobile server>:4443/Citrix/Device/v1/Check --
   header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
   ```

   Par exemple, cette requête vérifie la connectivité en obtenant l'état de conformité du premier appareil (`deviceid_1`) inscrit dans l'environnement :

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-
   Citrix-VPN-Device-ID: deviceid_1"
   ```

   Un résultat réussi est similaire à l'exemple suivant.

   ```
   1 HTTP/1.1 200 OK
   2 < Server: Apache-Coyote/1.1
   3 < X-Citrix-Device-State: Non Compliant
   4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   5 <!--NeedCopy-->
   ```

9. Lorsque l'étape précédente réussit, créez l'action d'authentification Web sur XenMobile. Commencez par créer une expression de stratégie pour extraire l'ID d'appareil du plug-in VPN iOS. Tapez ce qui suit.

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).
   TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"
   ```

10. Envoyez la requête à XenMobile en tapant ce qui suit. Dans cet exemple, l'adresse IP de XenMobile Server est `10.207.87.82` et le nom de domaine complet est `example.em.server.com :4443`.

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort
     4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP/1.1\r\n"+ "
    Host: example.em.server.com:4443\r\n"+ "X-Citrix-VPN-Device-ID: "+
    xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.
    RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ
    (\"Compliant\")"
    ```

    L'état `HTTP status 200 OK` indique une réussite de NAC XenMobile. La valeur de l'en-tête `X-Citrix-Device-State` doit être `Compliant`.

11. Créez une stratégie d'authentification avec laquelle associer l'action en tapant ce qui suit.


```
add authentication Policy <policy name> -rule <rule> -action <web
authentication action>
```

Pa exemple : `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac`

12. Convertissez la stratégie LDAP existante en une stratégie avancée en tapant ce qui suit.

```
add authentication Policy <policy_name> -rule <rule> -action <LDAP
action name>
```

Pa exemple : `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. Ajoutez un intitulé de stratégie avec lequel associer la stratégie LDAP en tapant ce qui suit.

```
add authentication policylabel <policy_label_name>
```

Pa exemple : `add authentication policylabel ldap_pol_label`

14. Associez la stratégie LDAP à l'intitulé de stratégie en tapant ce qui suit.

```
bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol
 -priority 100 -gotoPriorityExpression NEXT
```

15. Connectez un périphérique compatible pour effectuer un test NAC afin de vérifier si l'authentification LDAP réussit. Tapez ce qui suit.

```
bind authentication vserver <authentication vserver> -policy <web
authentication policy> -priority 100 -nextFactor <ldap policy label> -
gotoPriorityExpression END
```

16. Ajoutez l'interface utilisateur à associer au serveur virtuel d'authentification. Tapez la commande suivante pour récupérer l'ID d'appareil.

```
add authentication loginSchemaPolicy <schema policy>-rule <rule> -
action lschema_single_factor_deviceid
```

17. Liez le serveur virtuel d'authentification en tapant ce qui suit.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority
 100 -gotoPriorityExpression END
```

18. Créez une stratégie d'authentification avancée LDAP pour activer la connexion Secure Hub. Tapez ce qui suit.

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP
```

```
bind authentication vserver authvs -policy ldap_xm_test_pol -priority
110 -gotoPriorityExpression NEXT
```


Samsung Knox

January 10, 2022

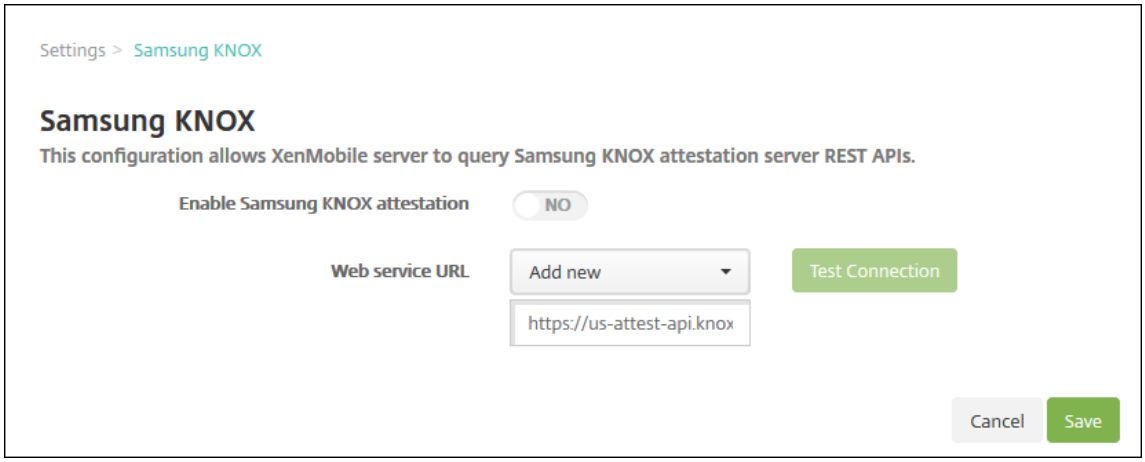
Samsung propose plusieurs solutions compatibles avec XenMobile Server.

- XenMobile prend en charge et étend les stratégies Samsung Knox sur les appareils Samsung compatibles.
- Le plug-in Knox Service (KSP) est une application prenant en charge un sous-ensemble de fonctionnalités Knox Platform for Enterprise (KPE). Pour obtenir des informations de Samsung sur KPE, voir Configure Knox Platform for Enterprise et Overview.

Vous pouvez configurer XenMobile pour interroger les API REST du serveur d'attestation Samsung KNOX.

Samsung Knox utilise des capacités de sécurité du matériel qui fournissent différents niveaux de protection pour le système d'exploitation et les applications. L'un des niveaux de cette sécurité réside sur la plate-forme via l'attestation. Un serveur d'attestation permet de vérifier les logiciels du système de base de l'appareil mobile (par exemple, les chargeurs de démarrage et le noyau). La vérification s'effectue au moment de l'exécution en fonction des données collectées au cours du démarrage sécurisé.

1. Dans la console Web de XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Plates-formes**, cliquez sur **Samsung KNOX**. La page **Samsung KNOX** s'affiche.



3. Dans **Activer la certification Samsung KNOX**, sélectionnez si vous souhaitez activer la certification Samsung Knox. La valeur par défaut est **Non**.
4. Lorsque vous définissez **Activer la certification Samsung KNOX** sur **OUI**, l'option **URL du service Web** est activée. Ensuite, dans la liste, procédez comme suit :
    - Cliquez sur le serveur d'attestation approprié.

- Cliquez sur **Ajouter** et entrez l'URL du service Web.

5. Cliquez sur **Tester la connexion** pour vérifier la connexion. Un message de réussite ou d'échec s'affiche.
6. Cliquez sur **Enregistrer**.

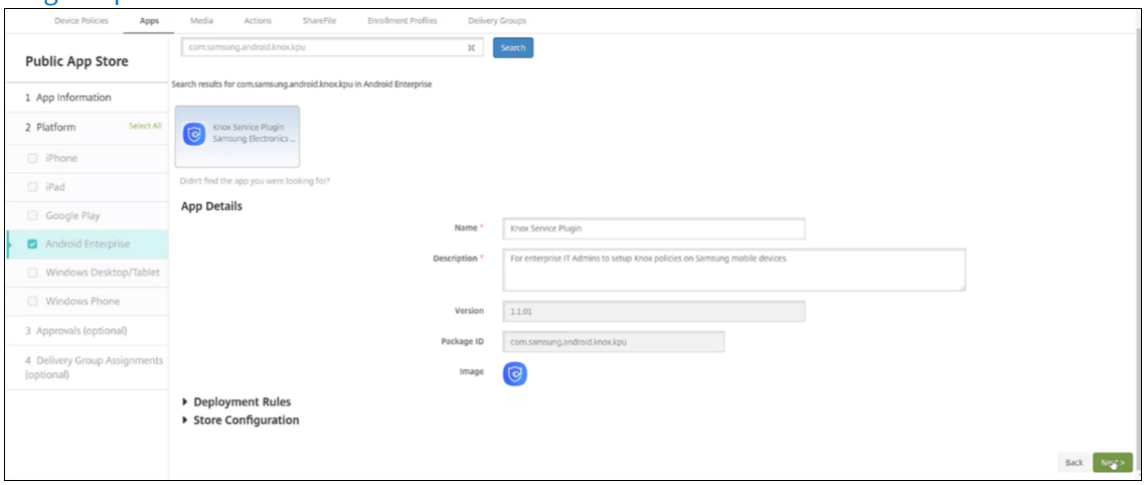
> **Remarque :**
>
> Vous pouvez utiliser Samsung Knox Mobile Enrollment pour inscrire plusieurs appareils Samsung Knox dans XenMobile (ou toute solution de gestion de la flotte mobile) sans avoir à configurer manuellement chaque appareil. Pour de plus amples informations, consultez la section Inscription en bloc Samsung Knox.

Ajouter l'application de plug-in de service Knox

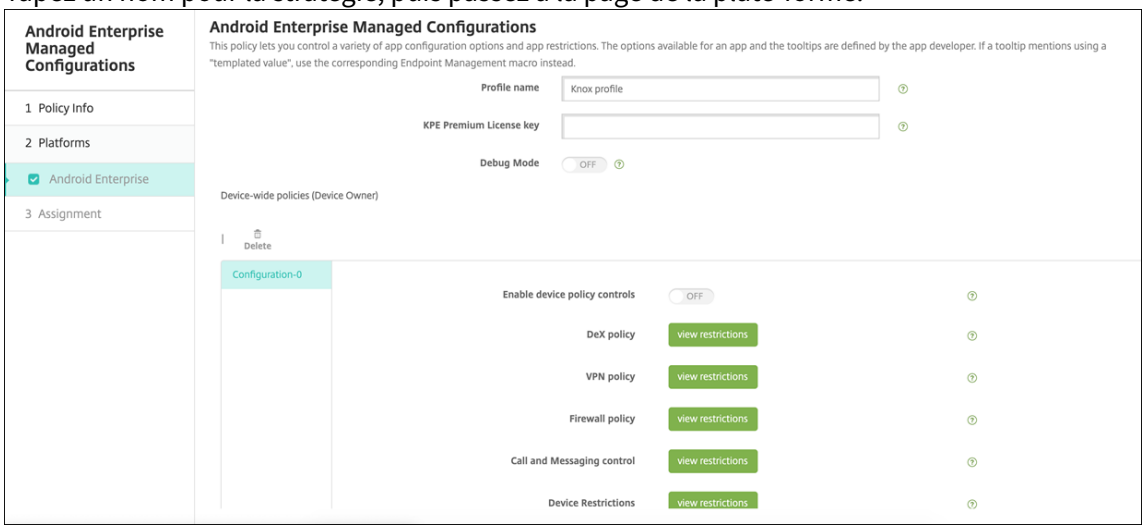
Si vous envisagez d'utiliser Android Enterprise avec Knox, ajoutez le plug-in de service Knox (KSP) à XenMobile. L'application KSP utilise AndroidOemConfig pour prendre en charge des fonctionnalités telles que des stratégies de sécurité, une configuration VPN flexible et des contrôles d'authentification biométrique. AndroidOemConfig permet aux OEM et aux gestionnaires de mobilité de terminaux (EMM) de prendre en charge les API OEM personnalisées. Ces API couvrent les cas d'utilisation non pris en charge par Android Enterprise.

Pour plus d'informations sur KSP, consultez le Knox Service Plug-in Admin Guide.

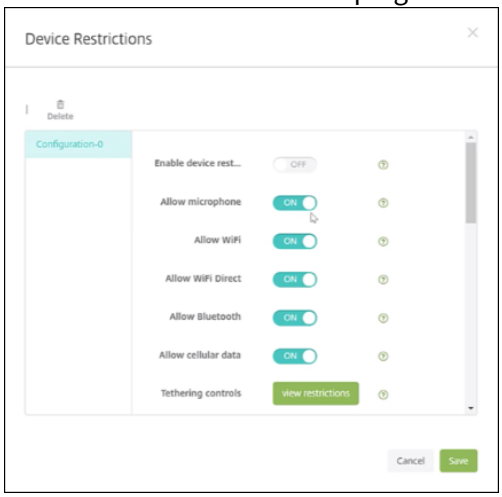
1. Connectez-vous à votre compte Google et accédez à `https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu`. Approuvez l'application de plug-in de service Knox.
2. Connectez-vous à votre console XenMobile et ajoutez le plug-in du service Knox en tant qu'application de magasin d'applications public. Pour plus d'informations sur l'ajout d'applications de magasin d'applications public, reportez-vous à Ajouter une application de magasin public.



3. Dans la console XenMobile, accédez à **Configurer > Stratégies d'appareil**. Cliquez sur **Ajouter**.
4. Cliquez sur **Configurations gérées par Android Entreprise**. Dans la boîte de dialogue qui apparaît, sélectionnez **Knox Service Plugin** dans le menu. Pour plus d'informations sur la stratégie de configuration gérée par Android Enterprise, reportez-vous à la stratégie Configurations gérées par Android Entreprise.
5. Tapez un nom pour la stratégie, puis passez à la page de la plate-forme.



6. Sur la page de la plate-forme, tapez un **nom de profil** pour votre profil Knox et saisissez la **clé de licence KPE Premium** de Samsung. Les stratégies qui apparaissent sous ces champs proviennent de votre déploiement Knox. Pour plus d'informations sur les stratégies Knox, consultez le Guide d'administration du plug-in de service Knox, référencé plus haut dans cette section.



7. Cliquez sur **Suivant** et configurez les règles de déploiement pour la stratégie.
8. Cliquez sur **Enregistrer**.

Inscription en bloc Samsung Knox

January 10, 2022

Pour inscrire plusieurs appareils Samsung Knox dans XenMobile (ou tout autre gestionnaire d'appareil mobile) sans avoir à configurer manuellement chaque appareil, utilisez Knox Mobile Enrollment. L'inscription se produit lors de la première utilisation ou après réinitialisation des paramètres d'usine. Les administrateurs peuvent également transmettre des noms d'utilisateur et des mots de passe directement à l'appareil, de sorte que les utilisateurs n'ont pas besoin de saisir d'informations lors de leur inscription.

> **Remarque :**
>
> L'installation de Knox Mobile Enrollment n'est pas liée au conteneur XenMobile Knox. Pour plus d'informations sur Knox Mobile Enrollment, consultez le guide d'administration de Knox Mobile Enrollment.

Conditions préalables pour Knox Mobile Enrollment

- XenMobile doit être configuré (y compris les licences et les certificats) et exécuté.
- Fichier APK Secure Hub. Vous le chargez lors de la configuration de Knox Mobile Enrollment.
- Pour obtenir une liste des exigences KME, consultez la présentation de Knox Mobile Enrollment.
- Licence Samsung Knox Platform for Enterprise (PKE), requise pour appliquer les stratégies d'appareil. Fournissez la clé de licence dans la stratégie d'appareil XenMobile, Knox Platform for Enterprise.

Pour télécharger le fichier APK Secure Hub

Accédez au Google Play Store pour télécharger le fichier Citrix Secure Hub pour Android.

Configurer des exceptions de pare-feu

Pour accéder à Knox Mobile Enrollment, configurez les exceptions de pare-feu suivantes. Certaines de ces exceptions de pare-feu sont requises pour tous les appareils et certaines sont spécifiques à l'emplacement géographique de l'appareil.

Région de l'appareil	URL	Port	Destination
Toutes	https://gslb.secb2b.com	443	Équilibrage de charge global pour initier Knox Mobile Enrollment
Toutes	https://gslb.secb2b.com	80	Équilibrage de charge global pour initier Knox Mobile Enrollment sur certains appareils limités d'ancienne génération
Toutes	umc-cdn.secb2b.com	443	Serveurs de mise à jour de l'agent Samsung
Toutes	bulkenrollment.s3.amazonaws.com	80	EULA des clients Knox Mobile Enrollment
Toutes	eula.secb2b.com	443	EULA des clients Knox Mobile Enrollment
Toutes	us-be-api-mssl.samsungknox.com	443	Serveurs Samsung pour vérification du numéro IMEI
États-Unis	https://us-segd-api.secb2b.com	443	Samsung Enterprise Gateway pour les États-Unis
Europe	https://eu-segd-api.secb2b.com	443	Samsung Enterprise Gateway pour l'Europe
Chine	https://china-segd-api.secb2b.com	443	Samsung Enterprise Gateway pour la Chine

> **Remarque :**
>
> Vous trouverez une liste complète des exceptions de pare-feu dans le guide d'administration de Knox Mobile Enrollment.

Pour accéder à Knox Mobile Enrollment

Consultez la documentation Samsung pour accéder à Knox Mobile Enrollment sur Prise en main de KME.

Configuration de Knox Mobile Enrollment

Une fois que vous avez accès à Knox Mobile Enrollment, connectez-vous au portail Knox.

Le processus d'inscription suit ces étapes générales.

1. Créez un profil MDM avec les informations et paramètres de votre console MDM.

   Le profil MDM indique à vos appareils comment se connecter à votre MDM.

2. Ajoutez des appareils à votre profil MDM.

   Vous pouvez soit télécharger un fichier CSV avec des informations sur l'appareil, soit installer et utiliser l'application de déploiement Knox à partir de Google Play.

3. Samsung vous informe une fois que le propriétaire de l'appareil a été vérifié.

4. Donnez aux utilisateurs les informations d'identification de connexion au MDM. Demandez aux utilisateurs de se connecter à Internet en Wi-Fi et d'accepter l'invite pour inscrire les appareils.

Pour créer un profil MDM

Suivez les étapes décrites dans la documentation Samsung sur Configuration du profil.

Lorsque vous rencontrez les champs suivants, configurez-les comme décrit ci-dessous :

- **Pick your MDM :** sélectionnez **Citrix** dans le menu. Uniquement pour les profils Propriétaire de l'appareil.
- **MDM Agent APK :** uniquement pour les profils Propriétaire de l'appareil. Tapez l'adresse URL de téléchargement du fichier APK Secure Hub : `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

  Le fichier APK peut résider sur n'importe quel serveur auquel les appareils peuvent accéder au cours de l'inscription. Lors de l'inscription, un appareil :

  - Télécharge Secure Hub depuis l'adresse URL de téléchargement du fichier APK ;
  - Installe Secure Hub ;
  - Ouvre ensuite Secure Hub avec les données JSON personnalisées décrites ci-après.

  La casse du nom de fichier .apk doit correspondre à l'adresse URL que vous entrez. Par exemple, si le nom de fichier est en minuscules, il doit également être en minuscules dans l'URL.

- **MDM Server URI :** ne spécifiez pas l'URI d'un serveur MDM. XenMobile n'utilise pas le protocole MDM de Samsung.

- **Custom JSON Data :** Secure Hub a besoin de l'adresse du serveur XenMobile ainsi que du nom d'utilisateur et du mot de passe pour l'inscription. Vous pouvez fournir ces données dans JSON afin que Secure Hub ne les demande pas aux utilisateurs. Secure Hub invite les utilisateurs à saisir l'adresse du serveur, le nom d'utilisateur ou le mot de passe uniquement si le champ est omis de JSON.

  Le format des données JSON personnalisées est le suivant :

  ```
  { "serverURL": "URL", "xm_username":"Username", "xm_password":"Password
  "}
  ```

  Dans cet exemple, typique de l'inscription en bloc, Secure Hub n'invite pas les utilisateurs à fournir l'adresse du serveur ou leurs informations d'identification lors de l'inscription :

  ```
  { "serverURL":"https://example.com/zdm", "xm_username":"userN", "
  xm_password":"password1234"}
  { "serverURL":"https://pmdm.mycorp-inc.net/zdm", "xm_username":"userN2"
  , "xm_password":"password7890"}
  ```

  Dans cet exemple, typique des appareils basés sur un kiosque, Secure Hub invite les utilisateurs à fournir leurs informations d'identification :

  ```
  { "serverURL":"https://example.com/zdm"}
  ```

  Vous pouvez également entrer des données JSON personnalisées pour l'inscription zero-touch Android Enterprise.

  ```
  1      {
  2
  3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
  4          {
  5
  6              "serverURL":"URL","xm_username":"username","
                     xm_password":"password"
  7           }
  8
  9       }
  10
  11  <!--NeedCopy-->
  ```

Lorsqu'un appareil démarre l'inscription, il télécharge Secure Hub à partir de l'URL donnée, installe Secure Hub et ouvre Secure Hub.

Configuration supplémentaire

Consultez les pages de documentation Samsung suivantes pour plus d'informations sur la configuration :

- Configuration de l'appareil : pour ajouter des appareils en bloc.
- Application de déploiement Samsung Knox : pour inscrire des appareils via l'inscription Bluetooth, NFC ou Wi-Fi Direct.
- Knox Mobile Enrollment : pour consulter la documentation Samsung pour plus d'informations sur Samsung Knox.

Pour inscrire des appareils exécutant un API Knox antérieur à la version 2.4

Sur les appareils dont l'API Knox est antérieure à la version 2.4, l'inscription en bloc ne démarre pas lors de la configuration initiale de l'appareil. Au lieu de cela, les utilisateurs doivent lancer l'inscription. Pour ce faire, les utilisateurs accèdent à un site Samsung pour télécharger le nouveau client Mobile Enrollment et démarrer l'inscription.

Le client d'inscription téléchargé utilise le même profil MDM et les mêmes APK que ceux configurés dans le portail Knox Bulk Enrollment pour les appareils Knox 2.4/2.4.1.

Les utilisateurs doivent généralement suivre ces étapes :

1. Allumez l'appareil et connectez-vous au Wi-Fi. Si Mobile Enrollment ne démarre pas ou que le Wi-Fi n'est pas disponible, procédez comme suit :
   a) Accédez à Samsung Knox Mobile Enrollment.
   b) Touchez le bouton **Next** pour inscrire des appareils avec des données mobiles.
2. Lorsque l'invite **Enroll with Knox** s'affiche, touchez **Continue**.
3. Prenez connaissance des EULA (le cas échéant). Touchez **Next**.
4. Si vous y êtes invité, entrez l'ID utilisateur (**User ID**) et le mot de passe (**Password**) fournis par l'administrateur informatique.

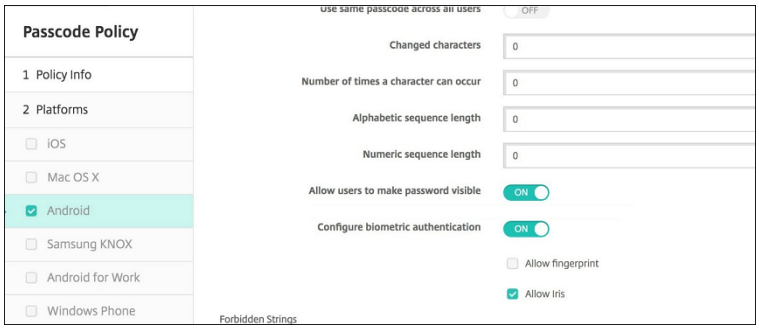
À ce stade, les informations d'identification de l'utilisateur sont validées et son appareil est inscrit dans l'environnement informatique de votre entreprise.

Activation et désactivation de l'authentification biométrique pour les appareils Samsung

XenMobile prend en charge l'authentification par empreinte digitale et par analyse de l'iris, également appelée authentification biométrique. Vous pouvez activer et désactiver l'authentification biométrique pour les appareils Samsung sans nécessiter l'intervention des utilisateurs. Si vous

désactivez l'authentification biométrique dans XenMobile, les utilisateurs et les applications tierces ne peuvent pas activer la fonctionnalité.

1. Dans la console XenMobile, cliquez sur **Configurer** > **Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.
2. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.
3. Cliquez sur **Code secret**. La page d'informations **Stratégie de code secret** s'affiche.
4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :
   - **Nom de la stratégie :** entrez un nom descriptif pour la stratégie.
   - **Description :** entrez une description pour la stratégie (facultatif).
5. Cliquez sur **Suivant**. La page **Plates-formes** s'affiche.
6. Sous **Plates-formes**, sélectionnez **Android** ou **Samsung Knox**.
7. Définissez l'option **Configurer l'authentification biométrique** sur **Activé**.
8. Si vous avez sélectionné **Android**, sous **Samsung SAFE**, sélectionnez **Autoriser empreinte digitale** ou **Autoriser iris** ou les deux.



Actions de sécurisation

January 10, 2022

Vous pouvez exécuter des actions de sécurité au niveau de l'application et de l'appareil à partir de la page **Gérer** > **Appareil**. Vous pouvez exécuter les actions suivantes sur l'appareil : révoquer, verrouiller, déverrouiller et effacer. Vous pouvez exécuter les actions de sécurité suivantes sur les applications : mode kiosque (verrouillage des applications) et effacement des applications.

- **Contourner le verrouillage d'activation :** supprime le verrouillage d'activation d'appareils iOS supervisés avant l'activation de l'appareil. Cette commande ne nécessite pas l'identifiant Apple ID ou le mot de passe personnel d'un utilisateur.

- **Mode kiosque :** refuse l'accès à toutes les applications sur un appareil. Sur Android, après un verrouillage d'application, les utilisateurs ne peuvent pas se connecter à XenMobile. Sur iOS, les utilisateurs peuvent se connecter, mais ils ne peuvent pas accéder aux applications.
- **Effacement des applications:** supprime le compte d'utilisateur de Secure Hub et désinscrit l'appareil. Les utilisateurs ne peuvent pas se réinscrire tant que vous n'avez pas effectué l'action **Annuler effacement des applications**.
- **Verrouillage d'activation du programme de déploiement ASM :** crée un code de contournement du verrouillage d'activation pour les appareils iOS inscrits au programme DEP Apple School Manager.
- **Effacer les restrictions :** sur les appareils iOS supervisés, cette commande permet à XenMobile d'effacer le mot de passe de restrictions et les paramètres de restriction configurés par l'utilisateur.
- **Activer/Désactiver le mode perdu :** place un appareil iOS supervisé en Mode perdu et envoie à l'appareil un message, un numéro de téléphone et une note de bas de page à afficher. La seconde fois que vous envoyez cette commande, l'appareil sort du mode perdu.
- **Activer le suivi :** sur les appareils Android et iOS, cette commande permet à XenMobile d'interroger l'emplacement d'appareils spécifiques à une fréquence que vous définissez. Pour afficher les coordonnées et l'emplacement d'un appareil sur une carte, accédez à **Gérer > Appareils**, sélectionnez un appareil, puis cliquez sur **Modifier**. Les informations sur l'appareil se trouvent dans l'onglet **Général**, sous **Sécurité**. Utilisez **Activer le suivi** pour effectuer un suivi continu de l'appareil. Secure Hub signale périodiquement l'emplacement lorsque l'appareil est en cours d'exécution.
- **Effacement complet :** efface immédiatement toutes les données et applications d'un appareil, y compris des cartes mémoire.
  - Pour les appareils Android, cette demande peut également inclure l'option d'effacement de cartes mémoire.
  - Pour les appareils Android Enterprise entièrement gérés avec profil de travail (appareils COPE), vous pouvez effectuer un effacement complet après qu'un effacement des données d'entreprise a supprimé le profil de travail.
  - Pour les appareils iOS et macOS, l'effacement se produit immédiatement, même si l'appareil est verrouillé. Pour les appareils iOS 11 (version minimale) : lorsque vous confirmez l'effacement complet, vous pouvez choisir de conserver le plan de données cellulaires sur l'appareil.
  - Pour les appareils Windows Phone, un effacement complet supprime toutes les informations XenMobile ainsi que toutes les données utilisateur. Ces données comprennent le contenu personnel tel que les applications, e-mails, contacts et contenus multimédias.

  - Pour les appareils Windows Mobile qui exécutent Windows Mobile 6 ou version ultérieure : après l'effacement, vous devrez peut être renvoyer l'appareil au fabricant pour recharger le système d'exploitation, les logiciels d'origine ou les deux.
  - Si l'utilisateur éteint l'appareil avant que le contenu de la carte mémoire soit supprimé, l'utilisateur peut toujours avoir accès aux données de l'appareil.
  - Vous pouvez annuler la demande d'effacement jusqu'à ce que la demande soit envoyée à l'appareil.

- **Localiser :** localise un appareil et signale l'emplacement de l'appareil, accompagné d'une carte, sur la page **Gérer > Appareils**, sous **Détails de l'appareil > Général**. La fonction Localiser est une action unique. Utilisez **Localiser** pour afficher l'emplacement actuel de l'appareil au moment où vous exécutez l'action. Pour effectuer un suivi continu de l'appareil sur une période donnée, utilisez **Activer le suivi**.
  - Lorsque vous appliquez cette action aux appareils Android (sauf Android Enterprise) ou aux appareils Android Enterprise (appartenant à l'entreprise ou BYOD), tenez compte du comportement suivant :
    * La fonction **Localiser** requiert que l'utilisateur donne accès à la localisation lors de l'inscription. L'utilisateur peut choisir de ne pas accorder l'autorisation de localisation. Si l'utilisateur n'accorde pas l'autorisation lors de l'inscription, XenMobile demande à nouveau l'autorisation de localisation lors de l'envoi de la commande **Localiser**.
  - Lorsque vous appliquez cette fonctionnalité à des appareils iOS ou Android Enterprise, tenez compte des limitations suivantes :
    * Pour les appareils Android Enterprise, cette requête échoue échoue à moins que la stratégie d'appareil Localisation n'ait défini le mode de localisation de l'appareil sur **Haute précision** ou **Économie de batterie**.
    * Pour les appareils iOS, cette commande ne réussit que si les appareils sont en mode perdu MDM.

- **Verrouiller :** verrouille à distance un appareil. Cette action est utile lorsque vous perdez un appareil et que vous ne savez pas s'il a été volé. Ensuite, XenMobile génère un code PIN et le configure dans l'appareil. Pour accéder à l'appareil, l'utilisateur devra entrer ce code PIN. Utilisez **Annuler le verrouillage** pour retirer le verrouillage de la console XenMobile.
- **Verrouiller et réinitialiser le mot de passe :** verrouille un appareil à distance et réinitialise le mot de passe.
  - Non pris en charge pour les appareils inscrits dans Android Enterprise en mode Profil de travail qui exécutent des versions Android antérieures à Android 8.0.
  - Sur les appareils inscrits dans Android Enterprise en mode Profil de travail qui exécutent Android 8.0 ou version ultérieure :

    * Le code secret envoyé verrouille le profil de travail. L'appareil n'est pas verrouillé.
    * Si aucun code secret n'est envoyé ou si le code secret envoyé ne répond pas aux exigences en matière de code secret et qu'aucun code secret n'est déjà défini sur le profil de travail, l'appareil est verrouillé.
    * Si aucun code secret n'est envoyé ou si le code secret envoyé ne répond pas aux exigences en matière de code secret, mais qu'un code secret est déjà défini sur le profil de travail, le profil de travail est verrouillé mais l'appareil ne l'est pas.

- **Notifier (sonnerie) :** émet un son sur les appareils Android.
- **Redémarrer :** redémarre les appareils Windows 10 et Windows 11. Pour Windows Tablet et PC, le message « Le système va bientôt redémarrer » s'affiche, puis le redémarrage se produit dans les cinq minutes. Pour Windows Phone, le redémarrage se produit après quelques minutes sans message d'avertissement pour les utilisateurs.
- **Demander/Arrêter la mise en miroir AirPlay :** démarre et arrête la mise en miroir AirPlay sur les appareils iOS supervisés.
- **Redémarrer/Arrêter :** redémarre ou arrête immédiatement les appareils iOS supervisés.
- **Révoquer :** permet d'empêcher un appareil de se connecter à XenMobile Server.
- **Révoquer/Autoriser (iOS, macOS) :** effectue les mêmes actions que l'effacement des données d'entreprise. Après la révocation, vous pouvez ré-autoriser l'appareil pour le réinscrire.
- **Faire sonner :** si un appareil iOS supervisé est en Mode perdu, cette option le fait sonner. L'appareil sonne jusqu'à ce qu'il soit retiré du mode perdu ou que l'utilisateur désactive le son.
- **Effacer les données d'entreprise :** efface toutes les données et applications d'entreprise d'un appareil, sans toucher aux données et applications personnelles. Après l'effacement des données d'entreprise, un utilisateur peut réinscrire l'appareil.
    - L'effacement des données d'entreprise d'un appareil Android ne déconnecte pas l'appareil de Device Manager et du réseau d'entreprise. Pour empêcher l'appareil d'accéder à Device Manager, vous devez également révoquer les certificats de l'appareil.
    - L'effacement des données d'entreprise d'un appareil Android révoque également l'appareil. Vous ne pouvez réinscrire l'appareil qu'après l'avoir réautorisé ou supprimé de la console.
    - Pour les appareils Android Enterprise entièrement gérés avec profil de travail (appareils COPE), vous pouvez effectuer un effacement complet après qu'un effacement des données d'entreprise a supprimé le profil de travail. Vous pouvez également réinscrire l'appareil avec le même nom d'utilisateur. La réinscription de l'appareil recrée le profil de travail.
    - Si l'API Samsung Knox est activée, l'effacement sélectif de l'appareil supprime également le conteneur Samsung Knox.
    - Pour les appareils iOS et macOS, cette commande supprime le profil installé via MDM.

  - Un effacement des données d'entreprise sur un appareil Windows supprime également le contenu du dossier de profil de tout utilisateur connecté à l'appareil à ce moment-là. Un effacement des données d'entreprise ne supprime pas les clips Web que vous mettez à la disposition des utilisateurs via une configuration. Pour supprimer les clips Web, les utilisateurs doivent désinscrire manuellement leurs appareils. Vous ne pouvez pas réinscrire un appareil dont les données d'entreprise ont été effacées.
  - L'effacement sélectif d'un appareil Windows Phone supprime le jeton d'entreprise qui permet à XenMobile d'installer les applications sur l'appareil. L'effacement supprime également tous les certificats et toutes les configurations de XenMobile déployés sur l'appareil. Vous ne pouvez pas réinscrire un appareil Windows Phone dont les données d'entreprise ont été effacées.

- **Déverrouiller :** efface le code secret envoyé à l'appareil lorsqu'il a été verrouillé. Cette commande ne déverrouille pas l'appareil.

Dans **Gérer > Appareils**, la page **Détails de l'appareil** dresse également la liste des propriétés de sécurité de l'appareil. Ces propriétés incluent ID fort, Verrouiller l'appareil, Contourner le verrouillage d'activation et d'autres informations relatives au type de plate-forme. Le champ **Effacement complet de l'appareil** inclut le code PIN de l'utilisateur. L'utilisateur doit entrer ce code une fois que l'appareil est effacé. Si l'utilisateur oublie le code, vous pouvez le rechercher ici.

Actions de sécurisation pour les appareils Android

Action de sécurisation	Android (à l'exception des appareils Android Enterprise)	Android Enterprise (BYOD)	Android Enterprise (propriété de l'entreprise)
Mode kiosque	Oui	Non	Non
Effacement des applications	Oui	Non	Non
Effacement complet	Oui	Non	Oui

Action de sécurisation	Android (à l'exception des appareils Android Enterprise)	Android Enterprise (BYOD)	Android Enterprise (propriété de l'entreprise)
Localiser	Oui : pour les appareils exécutant Android 6.0+, la fonction Localiser requiert que l'utilisateur donne accès à la localisation lors de l'inscription. L'utilisateur peut choisir de ne pas accorder l'autorisation de localisation. Si l'utilisateur n'accorde pas l'autorisation lors de l'inscription, XenMobile demande à nouveau l'autorisation de localisation lors de l'envoi de la commande Localiser.	Oui : pour les appareils exécutant Android 6.0+, la fonction Localiser requiert que l'utilisateur donne accès à la localisation lors de l'inscription. L'utilisateur peut choisir de ne pas accorder l'autorisation de localisation. Si l'utilisateur n'accorde pas l'autorisation lors de l'inscription, XenMobile demande à nouveau l'autorisation de localisation lors de l'envoi de la commande Localiser.	Oui : pour les appareils exécutant Android 6.0+, la fonction Localiser requiert que l'utilisateur donne accès à la localisation lors de l'inscription. L'utilisateur peut choisir de ne pas accorder l'autorisation de localisation. Si l'utilisateur n'accorde pas l'autorisation lors de l'inscription, XenMobile demande à nouveau l'autorisation de localisation lors de l'envoi de la commande Localiser.
Verrouiller	Oui	Oui	Oui
Verrouiller et réinitialiser un mot de passe	Oui	Non	Oui
Notifier (sonnerie)	Oui	Oui	Oui
Révoquer	Oui	Oui	Oui
Effacer les données d'entreprise	Oui	Oui	Non

Actions de sécurisation pour les appareils iOS et macOS

Action de sécurisation	iOS	macOS
Contourner le verrouillage d'activation	Oui	Non
Mode kiosque	Oui	Non
Effacement des applications	Oui	Non
Verrouillage d'activation du programme de déploiement ASM	Oui	Non
Effacer les restrictions	Oui	Non
Activer/Désactiver le mode perdu	Oui	Non
Activer/Désactiver le suivi	Oui	Non
Effacement complet	Oui	Oui
Localiser	Oui	Non
Verrouiller	Oui	Oui
Faire sonner	Oui	Oui
Demander/Arrêter la mise en miroir AirPlay	Oui	Non
Redémarrer/Arrêter	Oui	Non
Révoquer/Autoriser	Oui	Oui
Effacer les données d'entreprise	Oui	Oui
Déverrouiller	Oui	Non

Actions de sécurisation pour les appareils Windows

Action de sécurisation	Windows Phone 10	Windows Tablet 10	Windows Phone 8.1
Localiser	Oui	Oui	Non
Verrouiller	Oui	Oui	Oui
Verrouiller et réinitialiser un mot de passe	Oui	Non	Oui

Action de sécurisation	Windows Phone 10	Windows Tablet 10	Windows Phone 8.1
Redémarrer	Oui	Oui	Non
Révoquer	Oui	Oui	Oui
Faire sonner	Oui	Non	Oui
Effacer les données d'entreprise	Oui	Oui	Oui
Effacer	Oui	Oui	Oui

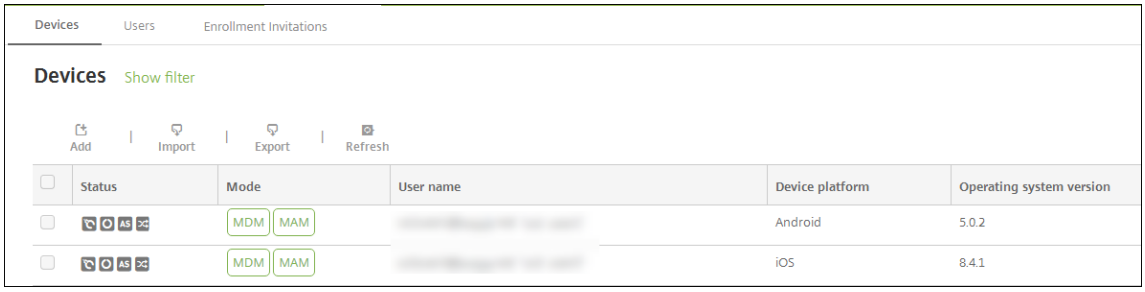
Le reste de cet article fournit les étapes permettant d'effectuer différentes actions de sécurisation. Vous pouvez également automatiser certaines actions. Pour de plus amples informations, consultez la section Actions automatisées.

Verrouiller les appareils iOS

Vous pouvez verrouiller un appareil iOS perdu tout en affichant un message et un numéro de téléphone sur l'écran de verrouillage. Cette fonctionnalité est prise en charge sur les appareils exécutant iOS 7 et versions ultérieures.

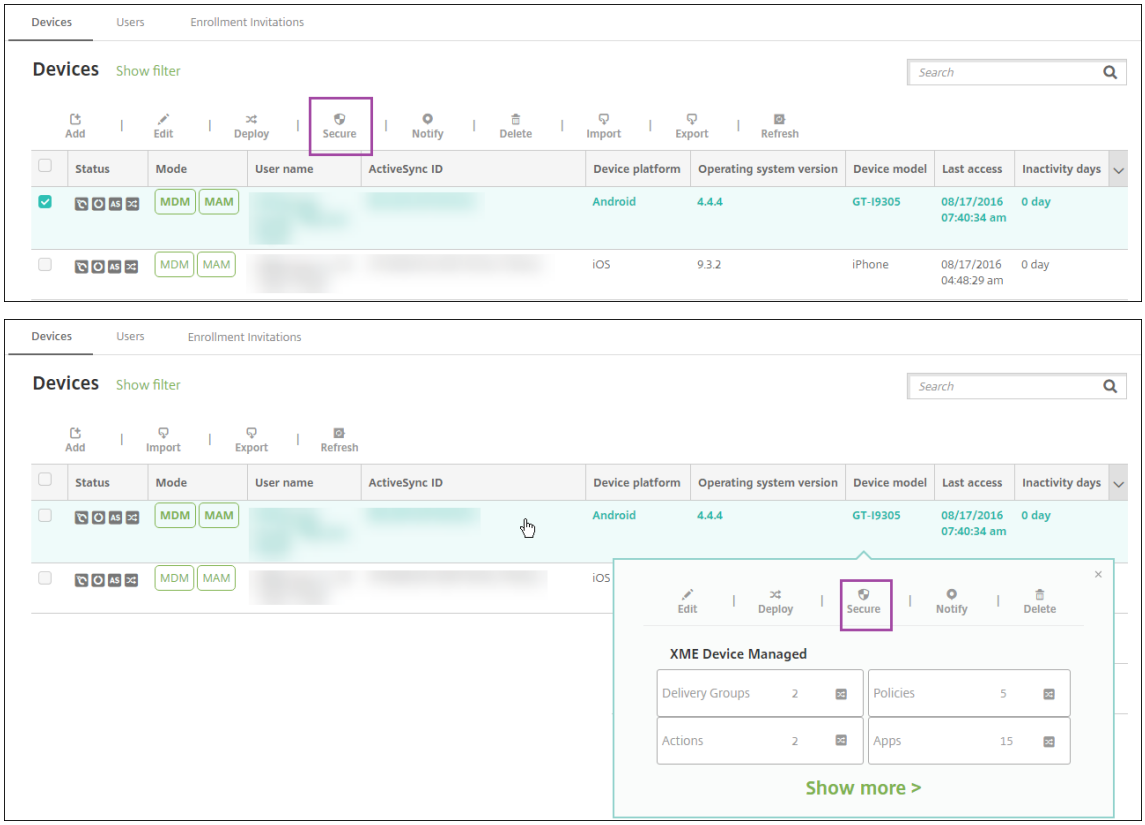
Pour afficher un message et un numéro de téléphone sur un appareil verrouillé, définissez la stratégie Code secret définie sur **true** dans la console XenMobile. Ou bien les utilisateurs peuvent activer le code secret sur l'appareil manuellement.

1. Cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.

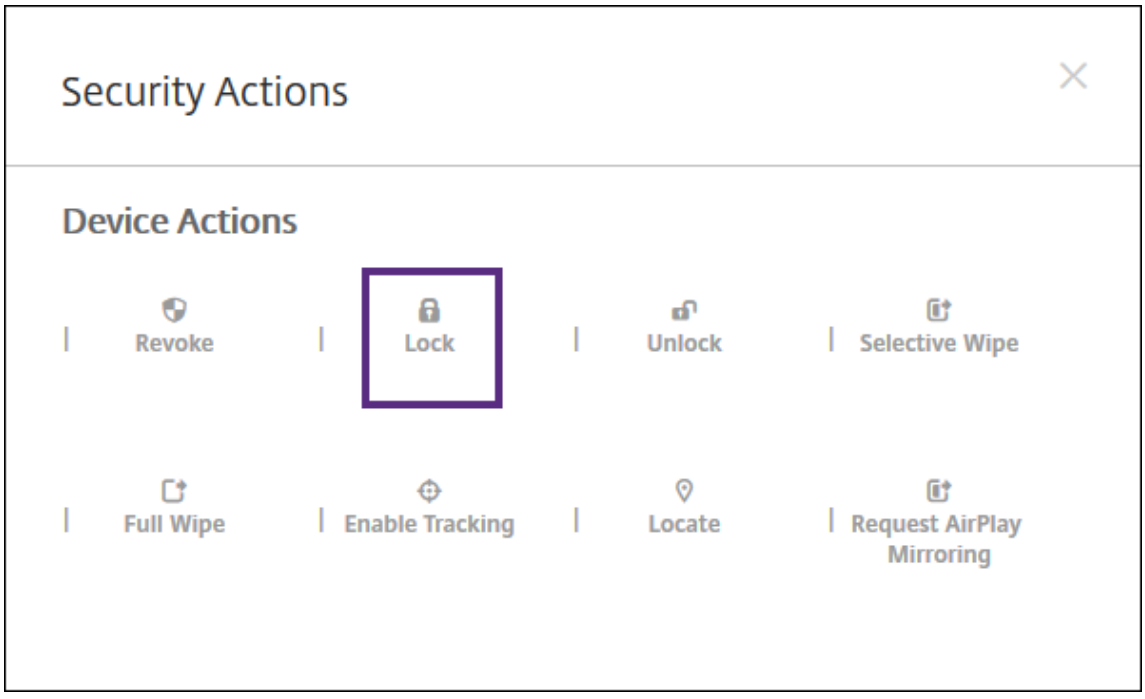


2. Sélectionnez l'appareil iOS que vous voulez verrouiller.

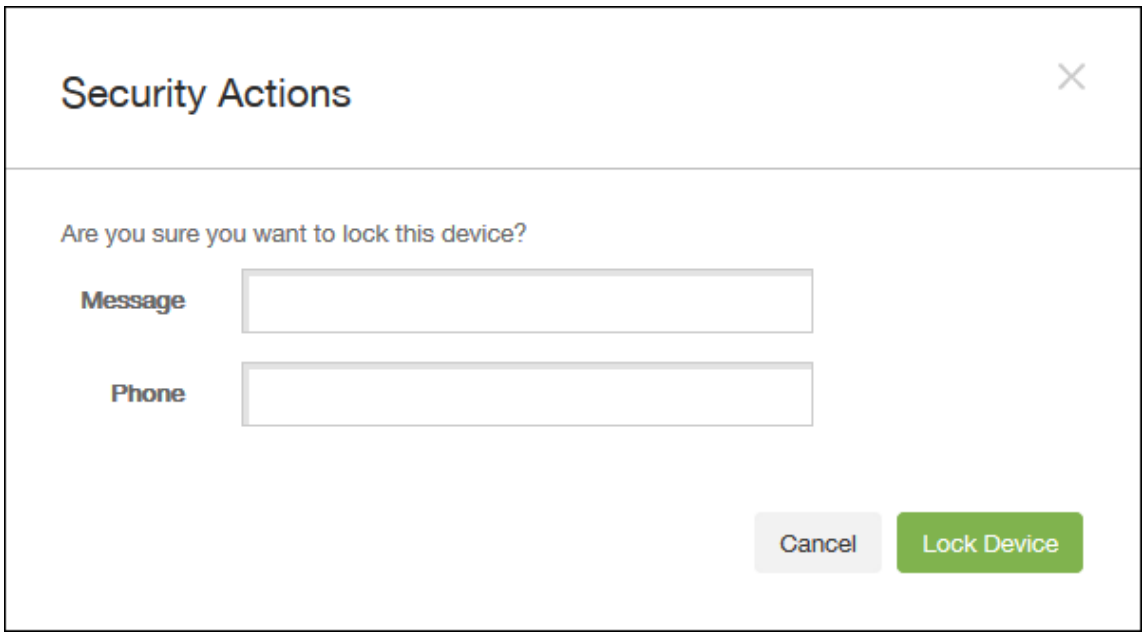
   Lorsque vous sélectionnez la case à cocher en regard d'un appareil, le menu d'options s'affiche au-dessus de la liste d'appareils. Lorsque vous cliquez dans la liste, le menu d'options s'affiche sur le côté droit de la liste.



3. Dans le menu d'options, sélectionnez **Sécurité**. La boîte de dialogue **Actions de sécurisation** s'affiche.



4. Cliquez sur **Verrouiller**. La boîte de dialogue **Actions de sécurisation** s'affiche.



5. Si vous le souhaitez, entrez un message et un numéro de téléphone qui s'afficheront sur l'écran de verrouillage de l'appareil.

   Pour les iPads exécutant iOS 7 et versions ultérieures : iOS ajoute les mots « iPad perdu » au texte entré dans le champ **Message**.

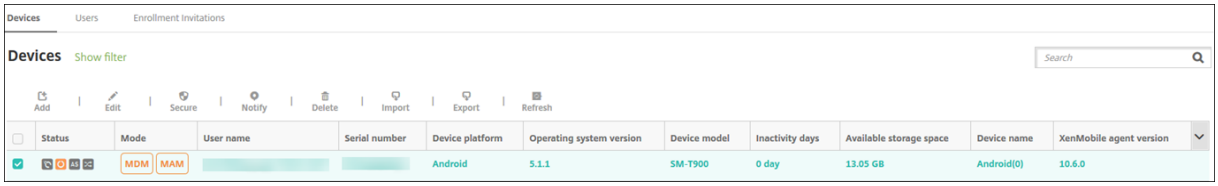
   Pour les iPhones exécutant iOS 7 et versions ultérieures : si vous laissez le champ **Message** vide et que vous entrez un numéro de téléphone, Apple affiche le message « Appeler propriétaire » sur l'écran de verrouillage de l'appareil.

6. Cliquez sur **Verrouiller l'appareil**.

Retirer un appareil de la console XenMobile

> **Important :**
>
> Lorsque vous supprimez un appareil de la console XenMobile, les applications gérées et les données restent sur l'appareil. Pour supprimer les applications gérées et les données de l'appareil, consultez la section « Supprimer un appareil » plus loin dans cet article.

Pour supprimer un appareil de la console XenMobile, accédez à **Gérer > Appareils**, sélectionnez un appareil géré et cliquez sur **Supprimer**.



Effacer les données d'entreprise d'un appareil

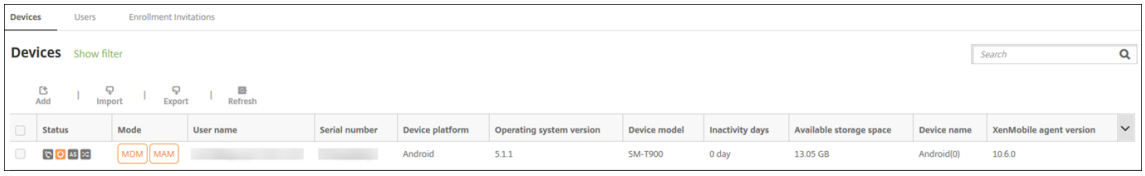
1. Accédez à **Gérer > Appareils**, sélectionnez un appareil géré et cliquez sur **Sécurisé**.
2. Dans **Actions de sécurisation**, cliquez sur **Effacer les données d'entreprise**.
3. Pour les appareils Android uniquement, déconnectez l'appareil du réseau d'entreprise : une fois que l'appareil a été effacé, dans **Actions de sécurisation**, cliquez sur **Révoquer**.

   Pour annuler une demande d'effacement des données d'entreprise avant qu'il ne soit exécuté, dans **Actions de sécurisation**, cliquez sur **Annuler l'effacement des données d'entreprise**.

Supprimer un appareil

Cette procédure supprime les applications gérées et les données de l'appareil et supprime l'appareil de la liste d'appareils dans la console XenMobile. Vous pouvez utiliser l'API REST publique Endpoint Management pour supprimer des appareils en bloc.

1. Accédez à **Gérer > Appareils**, sélectionnez un appareil géré et cliquez sur **Sécurisé**.
2. Cliquez sur **Effacer les données d'entreprise**. Lorsque vous y êtes invité, cliquez sur **Effacer les données d'entreprise de l'appareil**.
3. Pour vérifier que la commande d'effacement a réussi, actualisez **Gérer > Appareils**. Dans la colonne **Mode**, la couleur ambre pour MAM et MDM indique que la commande d'effacement a réussi.



4. Sur la page **Gérer > Appareils**, sélectionnez un appareil et cliquez sur **Supprimer**. Lorsque vous y êtes invité, cliquez de nouveau sur **Supprimer**.

Verrouiller, déverrouiller, effacer ou annuler l'effacement des applications

1. Accédez à **Gérer > Appareils**, sélectionnez un appareil géré et cliquez sur **Sécurisé**.
2. Dans **Actions de sécurisation**, cliquez sur l'action d'application.

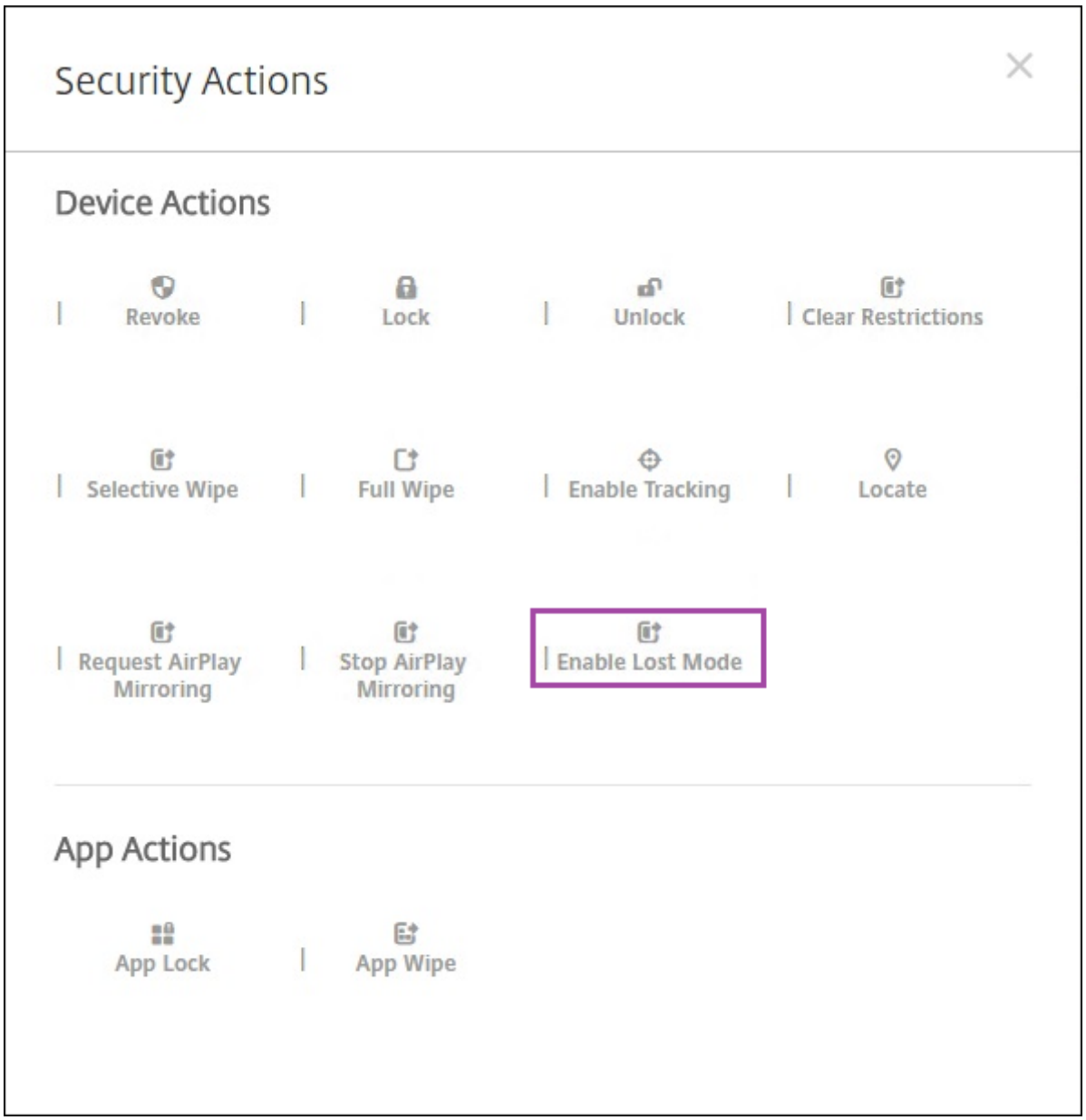
   Vous pouvez également utiliser la boîte de dialogue **Actions de sécurisation** pour vérifier l'état de l'appareil d'un utilisateur dont le compte a été désactivé ou supprimé dans Active Directory. La présence des actions Annuler le mode kiosque ou Annuler effacement des applications indique que les applications sont verrouillées ou effacées.

Placer les appareils iOS en Mode perdu

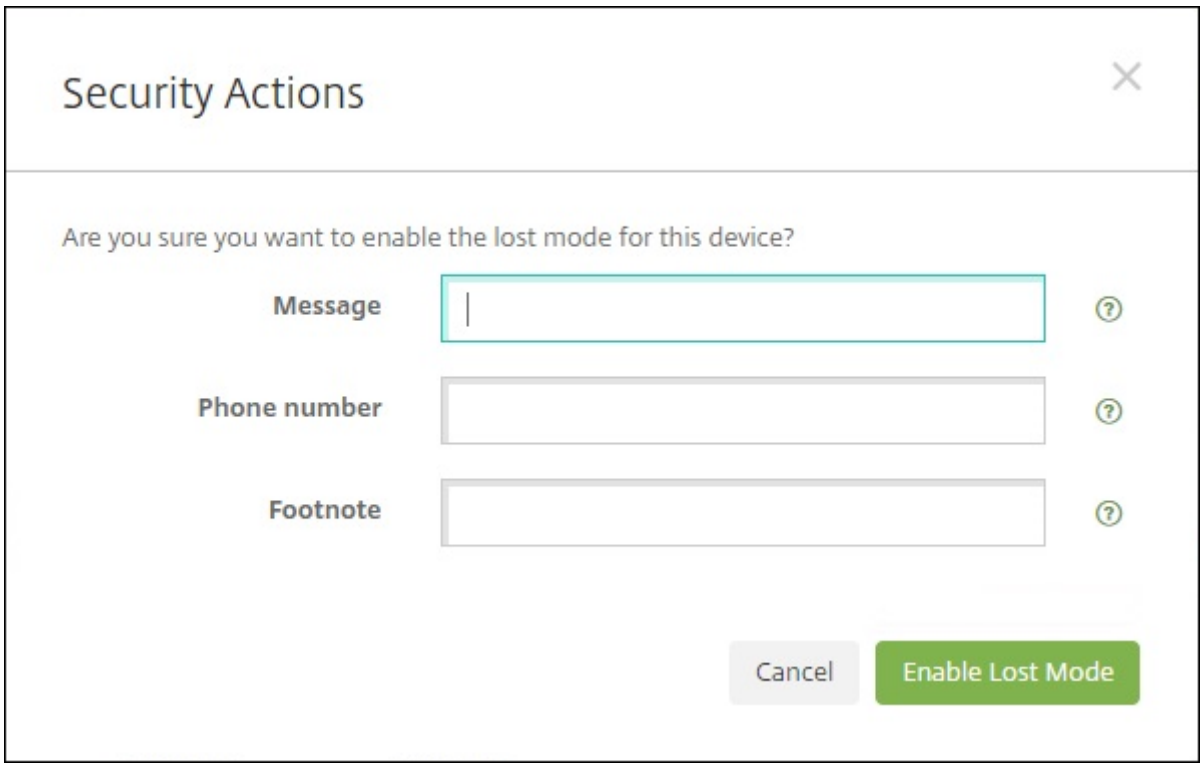
La propriété d'appareil Mode perdu de XenMobile place un appareil iOS en Mode perdu. Contrairement au mode perdu géré d'Apple, le mode perdu de XenMobile ne nécessite pas qu'un utilisateur effectue une des actions suivantes pour activer la recherche de son appareil : configurer le paramètre **Localiser mon iPhone/iPad** ou activer les Services de géolocalisation pour Citrix Secure Hub.

Dans le mode perdu de XenMobile, seul XenMobile Server peut déverrouiller l'appareil. (En revanche, si vous utilisez la fonctionnalité de verrouillage d'appareil de XenMobile, les utilisateurs peuvent déverrouiller l'appareil directement à l'aide d'un code PIN que vous devez fournir.

Pour activer ou désactiver le Mode perdu : accédez à **Gérer > Appareils**, choisissez un appareil iOS supervisé et cliquez sur **Sécurisé**. Ensuite, cliquez sur **Activer le mode perdu** ou **Désactiver le mode perdu**.

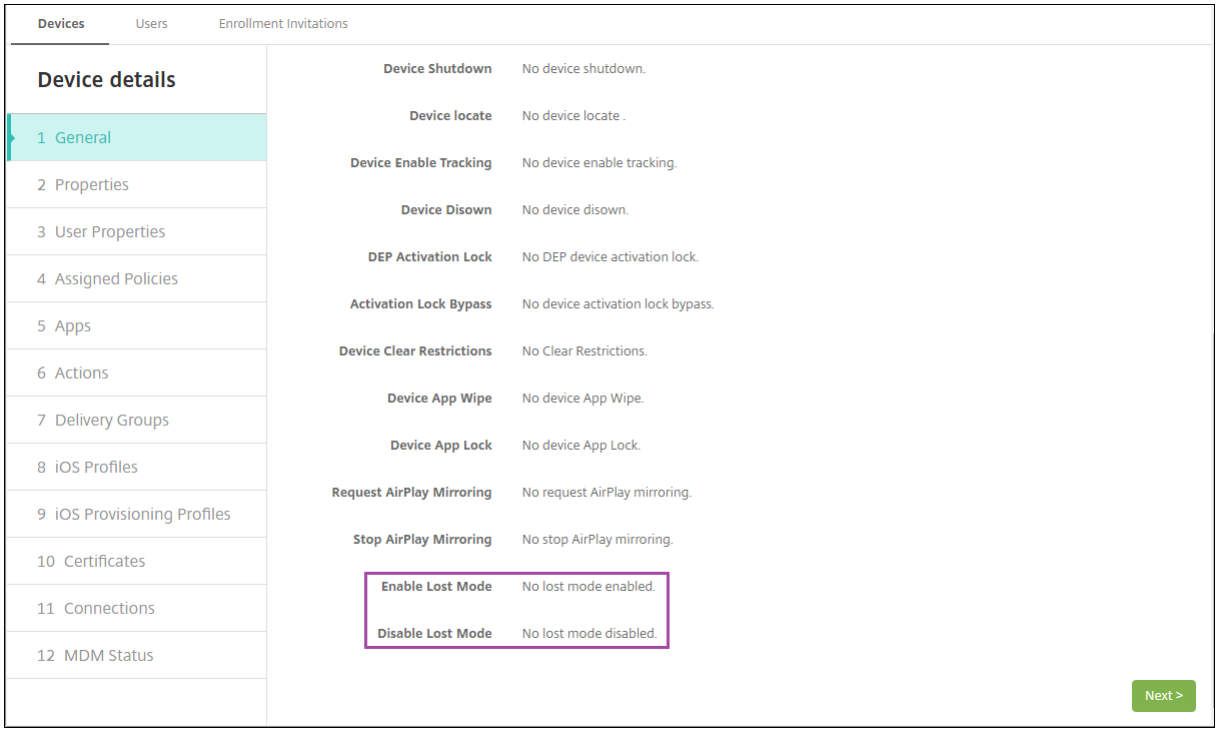


Si vous cliquez sur **Activer le mode perdu**, entrez les informations qui sont affichées sur l'appareil lorsqu'il est en mode perdu.

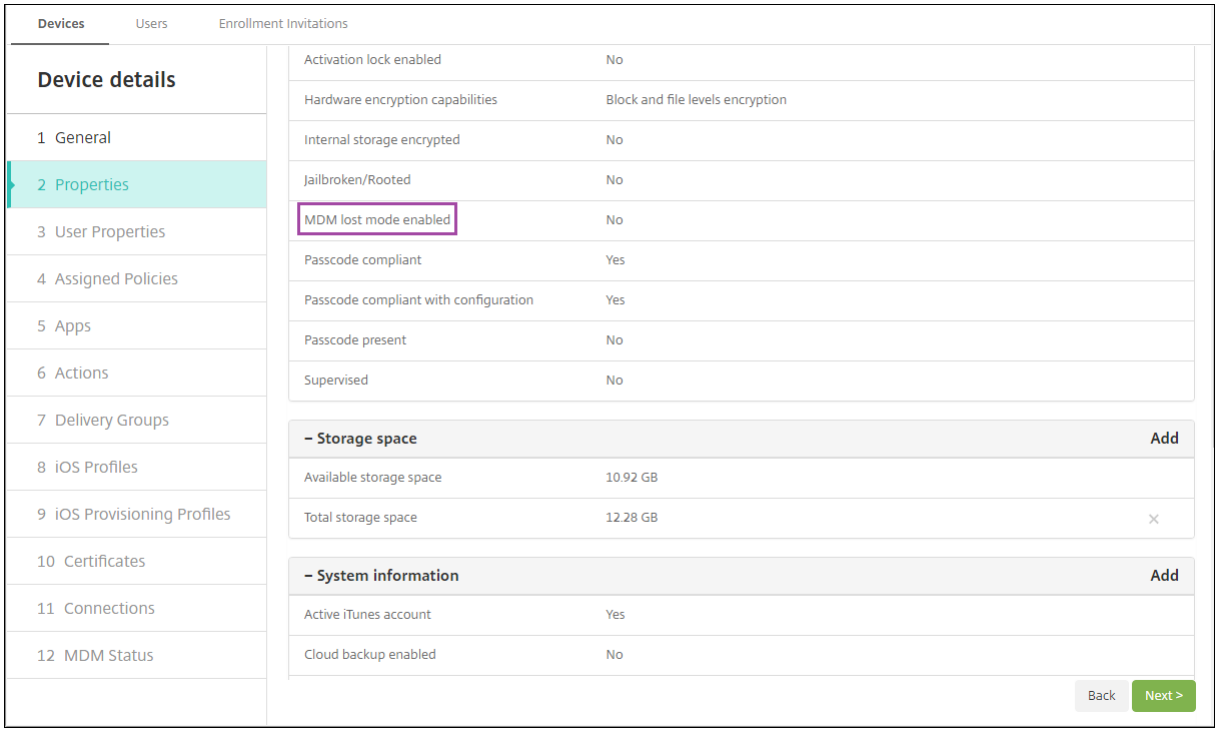


Pour vérifier l'état du mode perdu, utilisez une des méthodes suivantes :

- Dans la fenêtre **Actions de sécurisation**, vérifiez si le bouton indique **Désactiver le mode perdu**.
- Dans **Gérer > Appareils**, dans l'onglet **Général** sous **Sécurité**, consultez la dernière action Activer le mode perdu ou Désactiver le mode perdu.



- Dans **Gérer > Appareils**, dans l'onglet **Propriétés**, vérifiez que la valeur du paramètre **Mode perdu MDM activé** est correcte.



Si vous activez le mode perdu de XenMobile sur un appareil iOS, la console XenMobile est également modifiée comme suit :

- Dans **Configurer > Actions**, la liste **Actions** ne comprend pas ces actions automatiques : **Révoquer l'appareil**, **Effacer les données d'entreprise de l'appareil** et **Effacer toutes les données de l'appareil**.
- Dans **Gérer > Appareils**, la liste **Actions de sécurisation** n'inclut plus les actions **Révoquer** et **Effacer les données d'entreprise**. Vous pouvez toujours utiliser une action de sécurité pour effectuer une action **Effacement complet**, si nécessaire.

Pour les iPads exécutant iOS 7 et versions ultérieures : iOS ajoute les mots « iPad perdu » au texte entré dans **Message** dans l'écran **Actions de sécurisation**.

Pour les iPhones exécutant iOS 7 et versions ultérieures : si vous laissez **Message** vide et que vous entrez un numéro de téléphone, Apple affiche le message « Appeler propriétaire » sur l'écran de verrouillage de l'appareil.

Contourner un verrouillage d'activation iOS

Le verrouillage d'activation est une fonctionnalité de Localiser mon iPhone/iPad qui empêche la réactivation d'un appareil supervisé perdu ou volé. Le verrouillage d'activation requiert l'identifiant Apple et le mot de passe de l'utilisateur pour pouvoir désactiver Localiser mon iPhone/iPad, effacer l'appareil ou réactiver l'appareil. Pour les appareils qui sont la propriété de votre organisation, il est nécessaire de contourner le verrouillage d'activation pour, par exemple, réinitialiser ou réattribuer des appareils.

Pour activer le verrouillage d'activation, configurez et déployez la stratégie Options MDM de XenMobile. Vous pouvez ensuite gérer un appareil à partir de la console XenMobile sans les informations d'identification Apple de l'utilisateur. Pour contourner l'obligation d'entrer des informations d'identification Apple avec un verrou d'activation, émettez l'action de sécurisation Contourner le verrouillage d'activation depuis la console XenMobile.

Par exemple, si l'utilisateur retourne un téléphone perdu ou pour configurer l'appareil avant ou après un effacement complet : lorsque le téléphone invite à entrer les informations d'identification de compte iTunes, vous pouvez ignorer cette étape en émettant l'action de sécurité Contourner le verrouillage d'activation à partir de la console XenMobile.

Configuration requise pour le contournement du verrouillage d'activation

- iOS 7.1 (version minimale)
- Supervisé par Apple Configurator ou Apple DEP
- Configuré avec un compte iCloud
- Localiser mon iPhone/iPad activé
- Inscrit dans XenMobile
- Stratégie Options MDM, avec verrouillage d'activation activé, déployée sur les appareils

Pour contourner le verrouillage d'activation avant d'émettre un effacement complet de l'appareil :

1. Accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Sécurisé**, puis cliquez sur **Contourner le verrouillage d'activation**.
2. Effacez l'appareil. L'écran de verrouillage d'activation ne s'affiche pas lors de l'installation de l'appareil.

Pour contourner le verrouillage d'activation après avoir émis un effacement complet de l'appareil :

1. Réinitialisez ou effacez l'appareil. L'écran de verrouillage d'activation s'affiche lors de l'installation de l'appareil.
2. Accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Sécurisé**, puis cliquez sur **Contourner le verrouillage d'activation**.
3. Cliquez sur le bouton Retour sur l'appareil. L'écran d'accueil s'affiche.

Gardez à l'esprit les considérations suivantes :

- Conseillez à vos utilisateurs de ne pas désactiver Localiser mon iPhone/iPad. N'effectuez pas d'effacement complet à partir de l'appareil. Dans ces deux cas, l'utilisateur est invité à entrer le mot de passe du compte iCloud. Après la validation du compte, l'utilisateur ne verra pas d'écran Activer iPhone/iPad après avoir effacé tout le contenu et les paramètres.
- Pour un appareil avec un code de contournement de verrouillage d'activation généré et avec le verrouillage d'activation activé : si vous ne pouvez pas contourner la page Activer iPhone/iPad après un effacement complet, il n'est pas nécessaire de supprimer l'appareil de XenMobile. Vous ou l'utilisateur pouvez contacter l'assistance Apple pour débloquer l'appareil directement.
- Lors d'un inventaire matériel, XenMobile interroge un appareil pour obtenir un code de contournement de verrouillage d'activation. Si un code de contournement est disponible, l'appareil l'envoie à XenMobile. Ensuite, pour supprimer le code de contournement de l'appareil, envoyez l'action de sécurisation Contourner le verrouillage d'activation à partir de la console XenMobile. À ce stade, XenMobile Server et Apple ont le code de contournement nécessaire pour débloquer l'appareil.
- L'action de sécurisation Contourner le verrouillage d'activation repose sur la disponibilité d'un service d'Apple. Si l'action ne fonctionne pas, vous pouvez débloquer un appareil comme suit. Sur l'appareil, entrez manuellement les informations d'identification du compte iCloud. Ou, laissez le champ de nom d'utilisateur vide et tapez le code de contournement dans le champ de mot de passe. Pour rechercher le code de contournement, accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Modifier** et cliquez sur **Propriétés**. Le **Code de contournement du verrouillage d'activation** se trouve sous **Informations de sécurité**.

Appareils partagés

January 10, 2022

XenMobile vous permet de configurer des appareils que de multiples utilisateurs peuvent partager. Cette fonctionnalité permet, par exemple, aux médecins hospitaliers d'utiliser tout appareil à portée pour accéder à des applications et des données plutôt que d'avoir à transporter un appareil spécifique. Il peut aussi être utile pour les employés travaillant en équipe dans des domaines tels que la force publique, le commerce et le secteur industriel de partager des appareils pour réduire le coût du matériel.

Points clés à propos des appareils partagés

Vous pouvez utiliser n'importe quel appareil iOS et Android pris en charge en tant qu'appareil partagé. Pour obtenir une liste des appareils pris en charge, consultez la section Systèmes d'exploitation d'appareils pris en charge.

Inscription MDM

- Disponible sur tablettes et smartphones iOS et Android. Ne prend pas en charge l'inscription au programme de déploiement d'Apple de base pour un appareil partagé XenMobile Enterprise. Utilisez un programme de déploiement d'Apple autorisé pour inscrire un appareil partagé dans ce mode.
- Ne prend pas en charge l'authentification de certificat client, le code PIN Citrix, Touch ID, l'entropie utilisateur et l'authentification à deux facteurs.

Inscription MDM+MAM

- Disponible uniquement pour les appareils iOS et Android.
- Prend en charge uniquement l'authentification par nom d'utilisateur et mot de passe Active Directory.
- Ne prend pas en charge l'authentification de certificat client, le code de Secure Hub, Touch ID, l'entropie utilisateur et l'authentification à deux facteurs.
- Ne prend pas en charge l'inscription sur MAM-exclusif. Les appareils doivent s'inscrire en mode MDM.
- Prend en charge uniquement Secure Mail, Secure Web et les applications mobiles ShareFile. Ne prend pas en charge les applications HDX.
- Prend en charge uniquement les utilisateurs Active Directory. Ne prend pas en charge les utilisateurs et les groupes locaux.

- Pour effectuer une mise à jour vers MDM+MAM, nécessite la réinscription des appareils partagés MDM exclusif existants uniquement.
- Les utilisateurs ne peuvent pas partager des applications natives sur les appareils.
- Une fois les applications de productivité mobiles téléchargées lors de la première inscription, il est inutile de les télécharger à nouveau lors de la connexion utilisateur.
- Sur Android, afin d'isoler les données de chaque utilisateur pour des raisons de sécurité, définissez la stratégie **Disallow rooted devices** de la console XenMobile sur **Activé**.

Configuration requise pour l'inscription d'appareils partagés

Avant d'inscrire les appareils partagés, vous devez effectuer les opérations suivantes :

- Créer un rôle utilisateur d'inscription d'appareil partagé. Consultez la section Configuration de rôles avec RBAC.
- Créer un utilisateur d'appareil partagé. Consultez Pour ajouter, modifier, verrouiller ou supprimer des comptes utilisateur locaux.
- Créer un groupe de mise à disposition qui contient les stratégies de base, les applications et les actions que vous souhaitez appliquer à l'utilisateur d'appareil partagé. Consultez la section Déployer des ressources.

Conditions préalables pour l'inscription MDM+MAM

1. Créez un groupe Active Directory. Donnez-lui un nom descriptif, tel que **Inscriptions appareils partagés**.
2. Ajoutez à ce groupe les utilisateurs Active Directory qui vont inscrire des appareils partagés. Si vous souhaitez utiliser un nouveau compte à cette fin, créez un utilisateur Active Directory (par exemple **sdenroll**) et ajoutez cet utilisateur au groupe Active Directory.

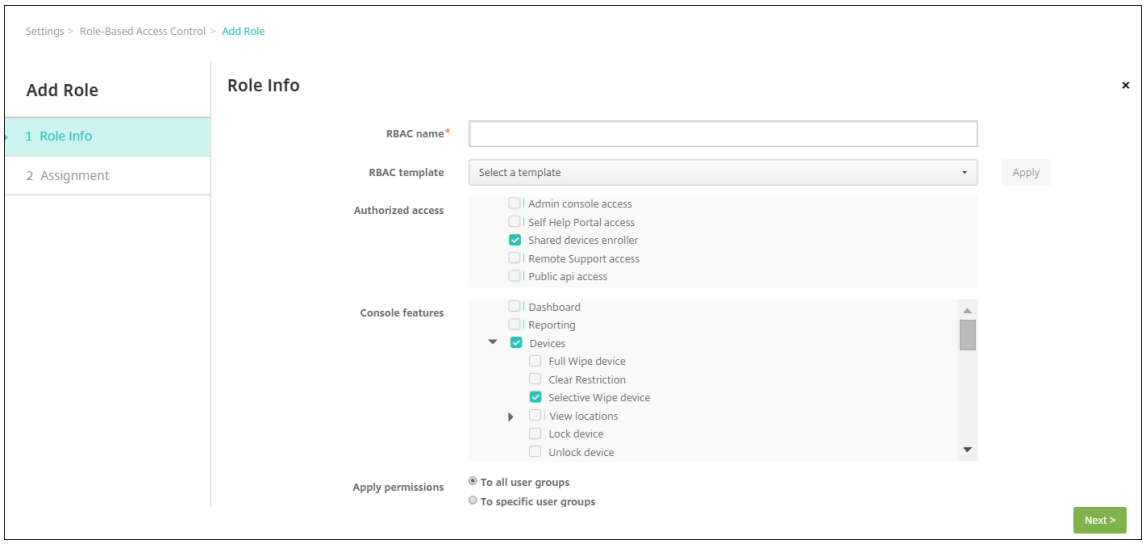
Configuration d'un appareil partagé

Suivez les étapes ci-dessous pour configurer un appareil partagé.

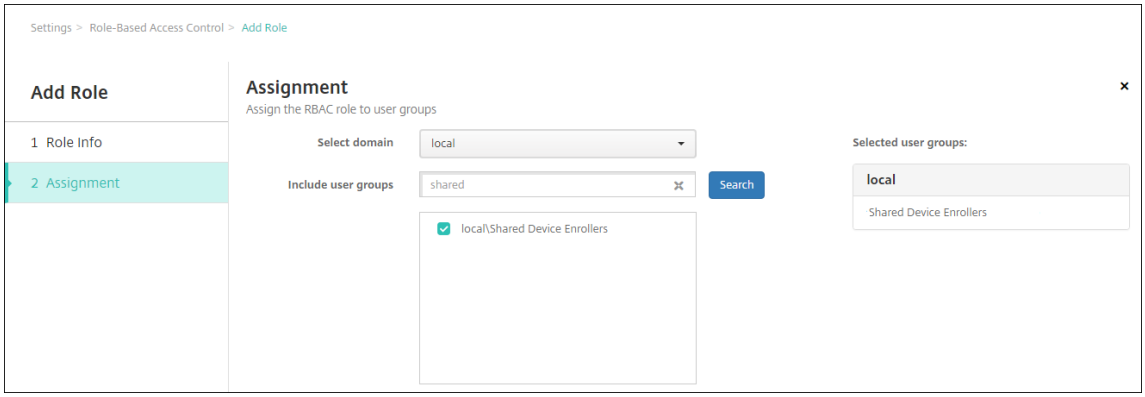
1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Contrôle d'accès basé sur rôle**, puis cliquez sur **Ajouter**. L'écran **Ajouter un rôle** s'affiche.
3. Créez un rôle utilisateur destiné à l'inscription d'appareils partagés, nommé **Utilisateur pour inscription d'appareils partagés**, disposant des autorisations **Assistant d'inscription d'appareils partagés** sous **Accès autorisé**. Veillez à développer **Appareils** dans **Fonctionnalités de la console**, puis sélectionnez **Effacer les données d'entreprise d'un appareil**.

Ce paramètre garantit que les applications et les stratégies configurées à l'aide du compte de l'assistant d'inscription d'appareils partagés sont supprimées via Secure Hub lors de la désinscription de l'appareil.

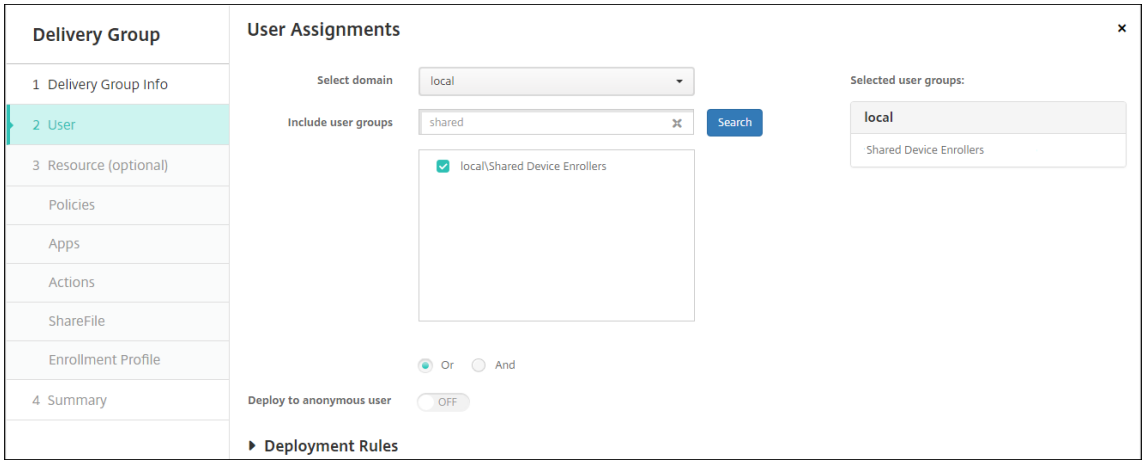
Pour **Appliquer les autorisations**, conservez le paramètre par défaut, qui est **À tous les groupes d'utilisateurs**, ou attribuez des autorisations à des groupes d'utilisateurs Active Directory spécifiques avec le paramètre **À des groupes d'utilisateurs spécifiques**.



Cliquez sur **Suivant** pour passer à l'écran **Attribution**. Attribuez le rôle d'inscription d'appareil partagé que vous venez de créer au groupe Active Directory que vous avez créé pour les utilisateurs destinés à l'inscription d'appareils partagés à l'étape 1 sous Conditions préalables. Dans l'image suivante, **citrix.lab** est le domaine Active Directory et **Shared Device Enrollers** est le groupe Active Directory.



4. Créez un groupe de mise à disposition contenant les stratégies de base, les applications et les actions que vous voulez appliquer à l'appareil lorsqu'un utilisateur n'est pas connecté. Associez ensuite ce groupe de mise à disposition au groupe Active Directory de l'utilisateur d'inscription d'appareil partagé.



5. Installez Secure Hub sur l'appareil partagé et inscrivez-le sur XenMobile à l'aide du compte utilisateur d'inscription sur appareil partagé. Vous pouvez maintenant voir et gérer l'appareil dans la console XenMobile. Pour de plus amples informations, consultez la section Inscription d'appareils.
6. Pour appliquer différentes stratégies ou pour fournir des applications supplémentaires aux utilisateurs authentifiés, vous devez créer un groupe de mise à disposition associé à ces utilisateurs et déployé uniquement sur des appareils partagés. Lors de la création de groupes, configurez des règles de déploiement pour vous assurer que les packages sont déployés sur des appareils partagés. Pour de plus amples informations, consultez la section Déployer des ressources.
7. Pour arrêter le partage de l'appareil, effacez les données d'entreprise pour supprimer le compte utilisateur de l'inscription d'appareil partagé à partir de l'appareil. Supprimez toutes les applications et stratégies déployées sur l'appareil.

Expérience utilisateur relative à l'utilisation d'un appareil partagé

Inscription MDM

Les utilisateurs voient uniquement les ressources qui leur sont disponibles, et leur expérience est la même sur chaque appareil partagé. Les stratégies et applications de l'inscription d'appareil partagé restent toujours sur l'appareil. Lorsqu'un utilisateur non inscrit sur les appareils partagés ouvre une session sur Secure Hub, les stratégies et applications de cette personne sont déployées sur l'appareil. Lorsque l'utilisateur se déconnecte, les stratégies et les applications qui ne font pas partie de l'inscription d'appareil partagé sont supprimées. Les ressources d'inscription d'appareil partagé restent intactes.

Inscription MDM+MAM

Secure Mail et Secure Web sont déployés sur l'appareil lorsqu'ils sont inscrits par l'utilisateur d'inscription d'appareil partagé. Les données utilisateur sont conservées de manière sécurisée sur

l'appareil. Les données ne sont pas affichées pour d'autres utilisateurs lorsqu'ils se connectent à Secure Mail ou Secure Web.

Un seul utilisateur à la fois peut se connecter à Secure Hub. L'utilisateur précédent doit se déconnecter pour que le prochain utilisateur puisse se connecter. Pour des raisons de sécurité, Secure Hub ne stocke pas les informations d'identification de l'utilisateur sur les appareils partagés, si bien que les utilisateurs doivent entrer leurs informations d'identification chaque fois qu'ils se connectent. Secure Hub bloque les nouvelles connexions jusqu'à ce qu'il supprime les stratégies, les applications et les données associées à l'utilisateur précédent.

L'inscription d'appareil partagé ne modifie pas le processus de mise à niveau des applications. Vous pouvez distribuer des mises à niveau aux utilisateurs d'appareils partagés comme vous le faites habituellement. Ces derniers peuvent alors mettre à niveau les applications directement sur leurs appareils.

Stratégies Secure Mail recommandées

- Pour obtenir des performances Secure Mail optimales, définissez la **Période de synchronisation maximale** en fonction du nombre d'utilisateurs qui partagent l'appareil. Il n'est pas recommandé d'autoriser un nombre illimité de synchronisation.

Nombre d'utilisateurs partageant l'appareil	Période de synchronisation maximale recommandée
21–25	1 semaine ou moins
6–20	2 semaines ou moins
5 ou moins	1 mois ou moins

- Bloquez **Activer l'exportation des contacts** afin de ne pas divulguer les contacts d'un utilisateur aux autres utilisateurs qui partagent l'appareil.
- Sur iOS, seuls les paramètres suivants peuvent être définis par utilisateur. Tous les autres paramètres sont communs à tous les utilisateurs qui partagent l'appareil :
  - Notifications
  - Signature
  - Absent(e) du bureau
  - Période de synchronisation des messages
  - S/MIME
  - Vérifier l'orthographe

XenMobile Autodiscovery Service

January 10, 2022

Le service de détection automatique simplifie le processus d'inscription pour les utilisateurs via la détection d'URL basée sur une adresse e-mail. Le service de détection automatique fournit des fonctionnalités telles que la vérification de l'inscription, le certificate pinning, ainsi que des avantages supplémentaires pour les clients Citrix Workspace. Le service, hébergé dans Citrix Cloud, joue un rôle important dans de nombreux déploiements XenMobile.

Avec le service de détection automatique, les utilisateurs :

- Peuvent utiliser leurs informations d'identification de réseau d'entreprise pour inscrire leurs appareils.
- N'ont pas besoin d'entrer les détails de l'adresse de XenMobile Server.
- Entrent leur nom d'utilisateur au format UPN (nom d'utilisateur principal). Par exemple, `user@mycompany.com`.

Nous vous recommandons d'utiliser le service de détection automatique pour les environnements à haute sécurité. Le service de détection automatique prend en charge le certificate pinning de clé publique, qui empêche les attaques « man-in-the-middle ». Le certificate pinning garantit que le certificat signé par votre entreprise est utilisé lorsque les clients Citrix communiquent avec XenMobile. Pour configurer le certificate pinning pour vos sites XenMobile, contactez le support Citrix. Pour plus d'informations, consultez la section Certificate pinning.

Pour accéder au service de détection automatique, accédez à https://adsui.cloud.com (commercial) ou https://adsui.cem.cloud.us (gouvernement).

Conditions préalables

- Le nouveau service de détection automatique dans Citrix Cloud requiert la dernière version de Secure Hub :
  - Pour iOS, Secure Hub version 21.6.0 ou ultérieure
  - Pour Android, Secure Hub version 21.8.5 ou ultérieure

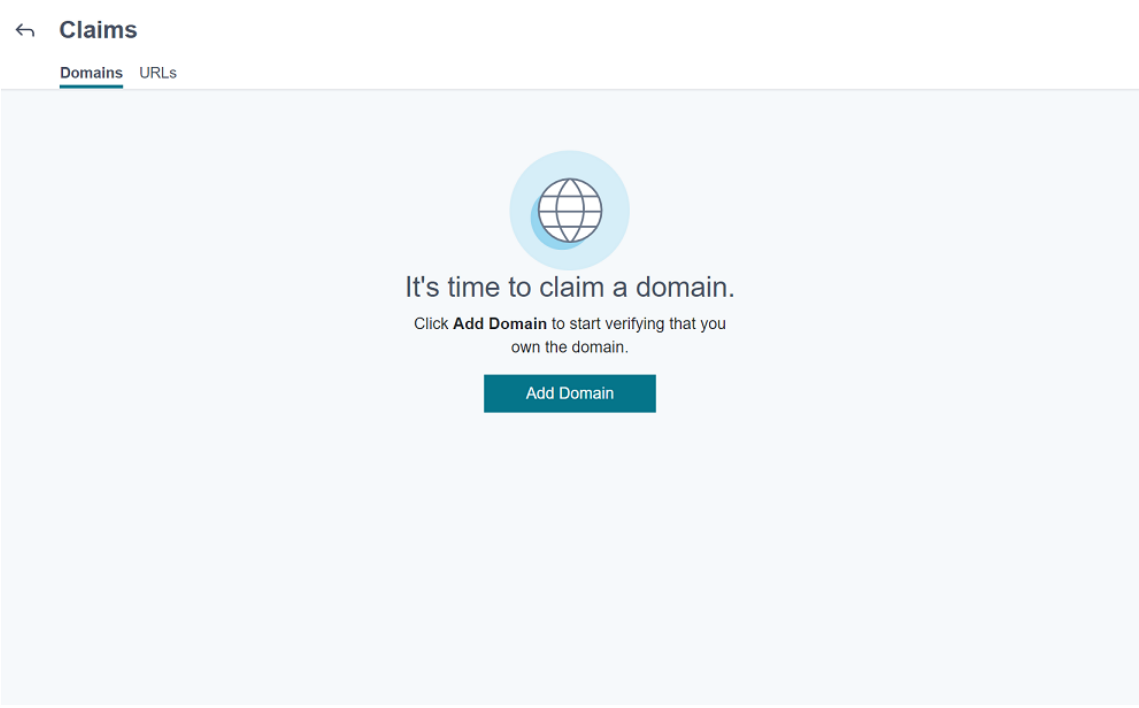
    Les appareils exécutés sur des versions antérieures de Secure Hub peuvent rencontrer des interruptions de service.
- Pour accéder au nouveau service de détection automatique, vous devez disposer d'un compte d'administrateur Citrix Cloud avec un accès complet. Le service de détection automatique ne prend pas en charge les comptes d'administrateur disposant d'un accès personnalisé. Si vous n'avez pas de compte, consultez Ouvrir un compte Citrix Cloud.

Citrix a migré tous les enregistrements de détection automatique existants vers Citrix Cloud sans interruption de service. Les enregistrements migrés n'apparaissent pas automatiquement dans la nouvelle console. Vous devez récupérer les domaines dans le nouveau service de détection automatique pour prouver la propriété. Pour plus d'informations, consultez l'article CTX312339.

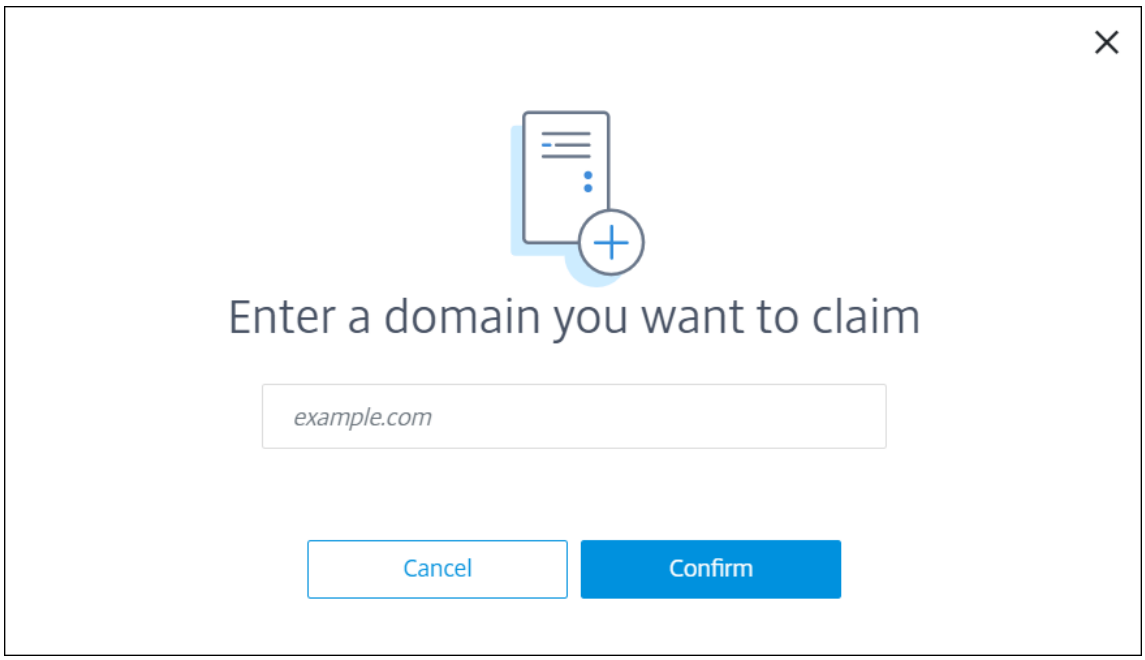
- Avant de commencer à utiliser le service de détection automatique pour vos déploiements Endpoint Management, vérifiez et revendiquez votre domaine. Vous pouvez revendiquer jusqu'à 10 domaines. La revendication associe le domaine vérifié au service de détection automatique. Pour revendiquer plus de 10 domaines, ouvrez un ticket SRE ou contactez le support technique Citrix.
- Utilisez le paramètre Port MAM au lieu de Nom de domaine complet Citrix Gateway pour diriger le trafic MAM vers votre centre de données. Si vous entrez un nom de domaine complet avec le port de votre instance Citrix Gateway, la machine client utilise la configuration du paramètre **Port MAM**.
- Si un bloqueur de publicités empêche l'ouverture du site, assurez-vous de désactiver le bloqueur de publicités pour l'ensemble du site Web.

Revendiquer un domaine

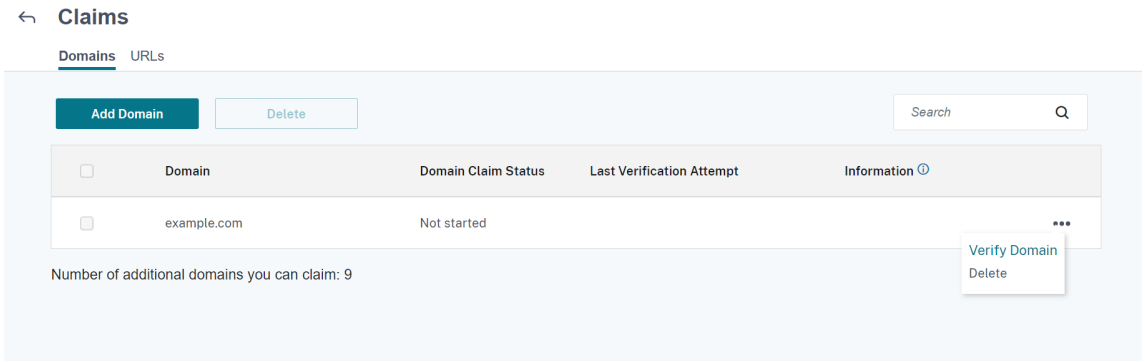
1. Sous l'onglet **Revendications > Domaines**, cliquez sur **Ajouter un domaine**.



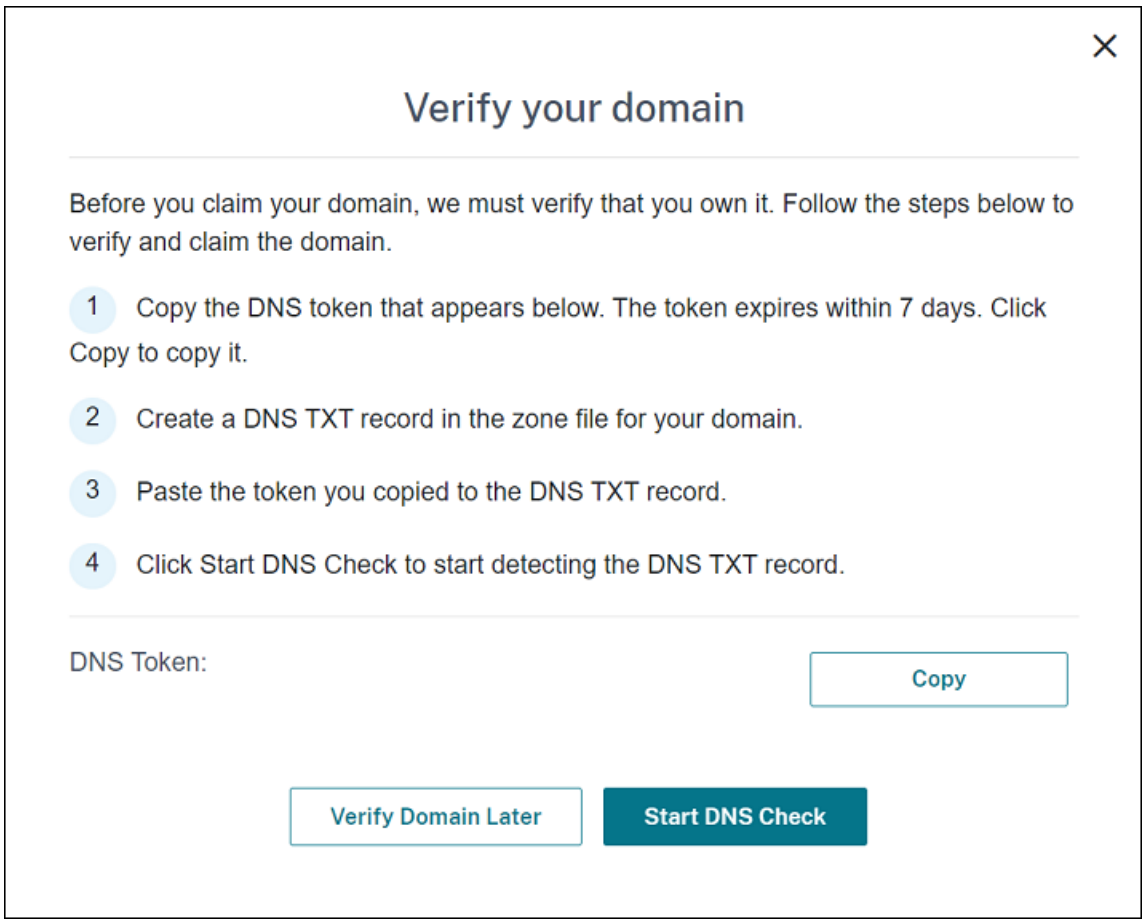
2. Dans la boîte de dialogue qui s'affiche, entrez le nom de domaine de votre environnement XenMobile et cliquez sur **Confirmer**. Votre domaine apparaît dans **Revendications > Domaines**.



3. Dans le domaine que vous avez ajouté, cliquez sur le menu des points de suspension et sélectionnez **Vérifier le domaine** pour démarrer le processus de vérification. La page **Vérifier votre domaine** s'affiche.



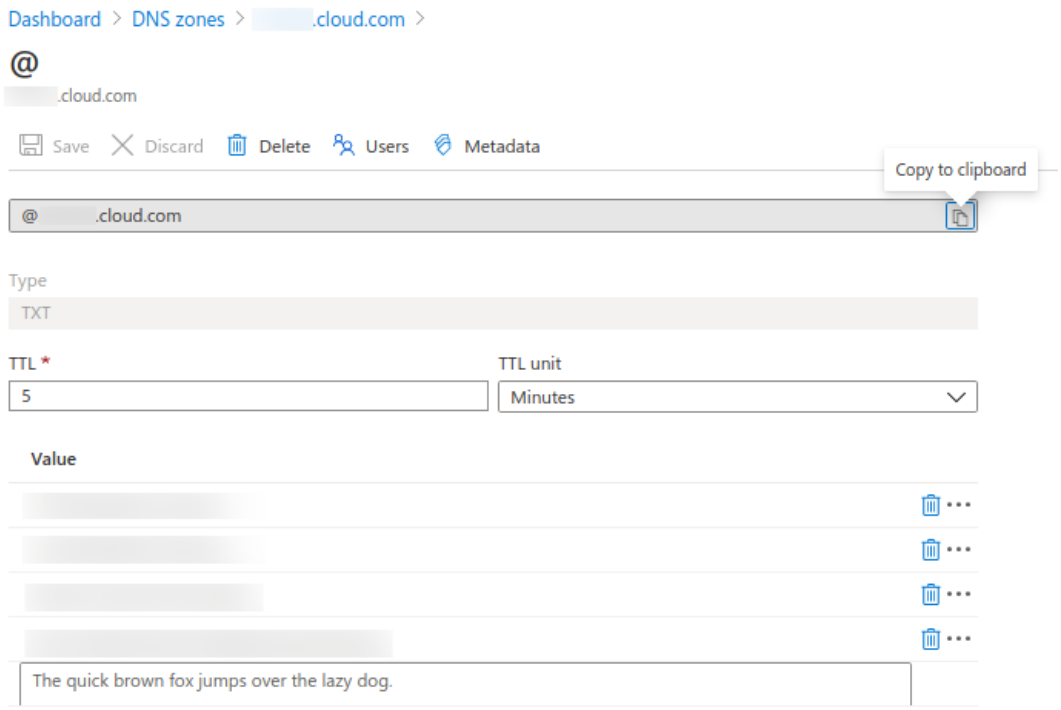
4. Sur la page **Vérifier votre domaine**, suivez les instructions pour vérifier que vous êtes propriétaire du domaine.



a) Cliquez sur **Copier** pour copier le jeton DNS dans le Presse-papiers.

b) Créez un enregistrement TXT DNS dans le fichier zone de votre domaine. Pour ce faire, accédez au portail hébergeur de domaine et ajoutez le jeton DNS que vous avez copié.

   La capture d'écran suivante montre un portail hébergeur de domaine. Votre portail peut sembler différent.



c) Dans Citrix Cloud, sur la page **Vérifier votre domaine**, cliquez sur **Démarrer vérification de DNS** pour commencer à détecter votre enregistrement TXT DNS. Si vous souhaitez vérifier le domaine ultérieurement, cliquez sur **Vérifier le domaine ultérieurement**.

Le processus de vérification prend généralement environ une heure. Cependant, la réponse peut prendre jusqu'à deux jours. Vous pouvez vous déconnecter et vous reconnecter lors de la vérification de l'état.

Une fois la configuration terminée, l'état de votre domaine passe de **En attente** à **Vérifié**.

5. Après avoir revendiqué votre domaine, entrez les informations relatives au service de détection automatique. Cliquez sur le menu des points de suspension du domaine que vous avez ajouté, puis cliquez sur **Ajouter des informations sur Endpoint Management**. La page **Informations sur le service de détection automatique** s'affiche.
6. Entrez les informations suivantes, puis cliquez sur **Enregistrer**.
   - **Nom de domaine complet du serveur Endpoint Management :** entrez le nom de domaine complet du serveur XenMobile Server. Par exemple : `example.xm.cloud.com`. Ce paramètre est utilisé pour le trafic de contrôle MDM et MAM.
   - **Nom de domaine complet de Citrix Gateway :** entrez le nom de domaine complet de Citrix Gateway, sous la forme FQDN ou FQDN:port. Par exemple : `example.com`. Ce paramètre permet de diriger le trafic MAM vers votre centre de données. Pour les déploiements MDM exclusif, laissez ce champ vide.

> **Remarque :**
>
> Citrix vous recommande d'utiliser le paramètre **Port MAM** au lieu de **Nom de domaine complet de Citrix Gateway** pour contrôler le trafic MAM. Si vous entrez un nom de domaine complet avec le port de votre instance Citrix Gateway, la machine client utilise la configuration du paramètre **Port MAM**.

- **Nom de l'instance :** entrez le nom de l'instance XenMobile Server que vous avez configuré ci-dessus. Si vous ne connaissez pas le nom de votre instance, laissez la valeur par défaut **zdm**.
- **Port MDM :** entrez le port utilisé pour le trafic de contrôle MDM et l'inscription MDM. Pour les services basés sur le cloud, la valeur par défaut est 443.
- **Port MAM :** entrez le port utilisé pour le trafic de contrôle MAM, l'inscription MAM, l'inscription iOS et l'énumération des applications. Pour les services basés sur le cloud, la valeur par défaut est 8443.

Demander la détection automatique pour les appareils Windows

Si vous prévoyez d'inscrire des appareils Windows, procédez comme suit :

1. Contactez le support Citrix et créez une demande de support pour activer la détection automatique de Windows.
2. Obtenez un certificat SSL non générique, signé publiquement pour `enterpriseenrollment.mycompany.com`. La partie `mycompany.com` est le domaine qui contient les comptes que les utilisateurs utilisent pour s'inscrire. Joignez le certificat SSL au format .pfx et son mot de passe à la demande de support créée à l'étape précédente.

   Pour utiliser plusieurs domaines pour inscrire des appareils Windows, vous pouvez également utiliser un certificat multi-domaines avec la structure suivante :

   - Un SubjectDN avec un CN (nom commun) qui spécifie le domaine principal qu'il sert (par exemple, enterpriseenrollment.masociété1.com).
   - Les SAN appropriés pour les domaines restants (par exemple, enterpriseenrollment.masociété2.com, enterpriseenrollment.masociété3.com, etc).
3. Créez un nom canonique (CNAME) dans votre DNS et mappez l'adresse de votre certificat SSL (enterpriseenrollment.masociété.com) vers autodisc.xm.cloud.com.

   Lorsqu'un utilisateur d'appareil Windows s'inscrit à l'aide d'un UPN, le serveur d'inscription Citrix :

   - Fournit les détails de votre serveur XenMobile Server.
   - Indique à l'appareil de demander un certificat valide à XenMobile.

À ce stade, vous pouvez inscrire tous les appareils pris en charge. Passez à la section suivante pour préparer la mise à disposition de ressources aux appareils.

Stratégies d'appareil

January 10, 2022

Vous pouvez configurer la façon dont XenMobile interagit avec vos appareils en créant des stratégies. Bien que la plupart des stratégies soient communes à tous les appareils, chaque appareil dispose de stratégies spécifiques à son système d'exploitation. Par conséquent, vous pouvez constater des différences entre les plates-formes et même entre différents fournisseurs d'appareils Android.

Pour obtenir un résumé de chaque stratégie, consultez la section Résumé des stratégies d'appareil dans cet article.

> **Remarque :**
>
> Si votre environnement est configuré avec des objets de stratégie de groupe (GPO) :
>
> Lorsque vous configurez des stratégies d'appareil XenMobile pour des appareils Windows 10 et Windows 11, n'oubliez pas la règle suivante. Si une stratégie sur un ou plusieurs appareils inscrits entraîne un conflit, la stratégie correspondant au GPO est prioritaire.

Pour voir les stratégies prises en charge par le conteneur Android Enterprise, consultez la section Android Enterprise.

Conditions préalables

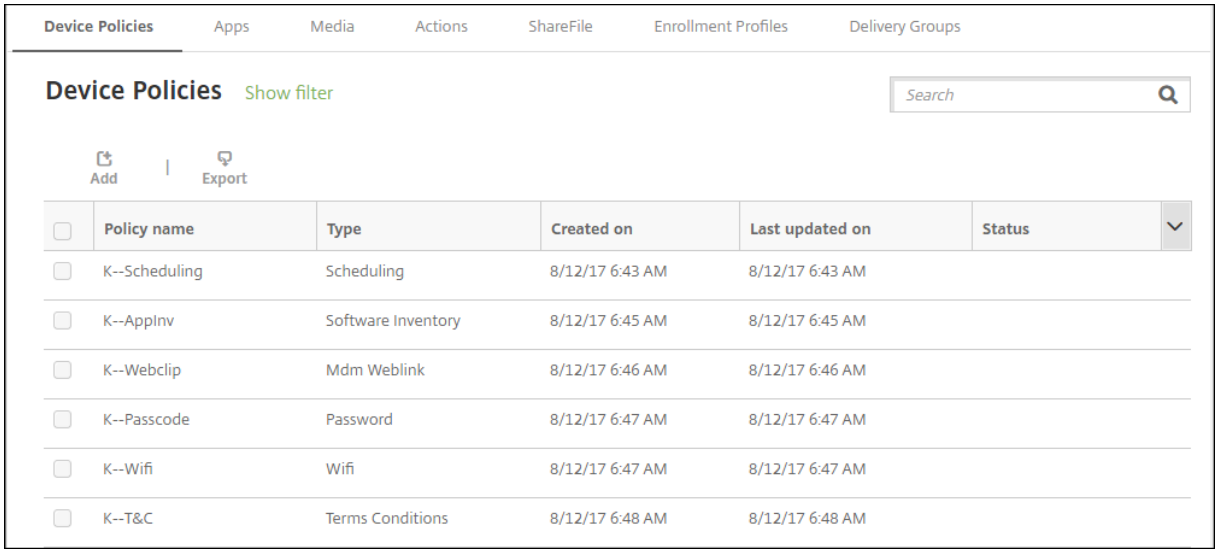
- Créer les groupes de mise à disposition que vous voulez utiliser.
- Installer les certificats d'autorité de certification nécessaires.

Ajouter une stratégie d'appareil

Les étapes de base pour créer une stratégie sont les suivantes :

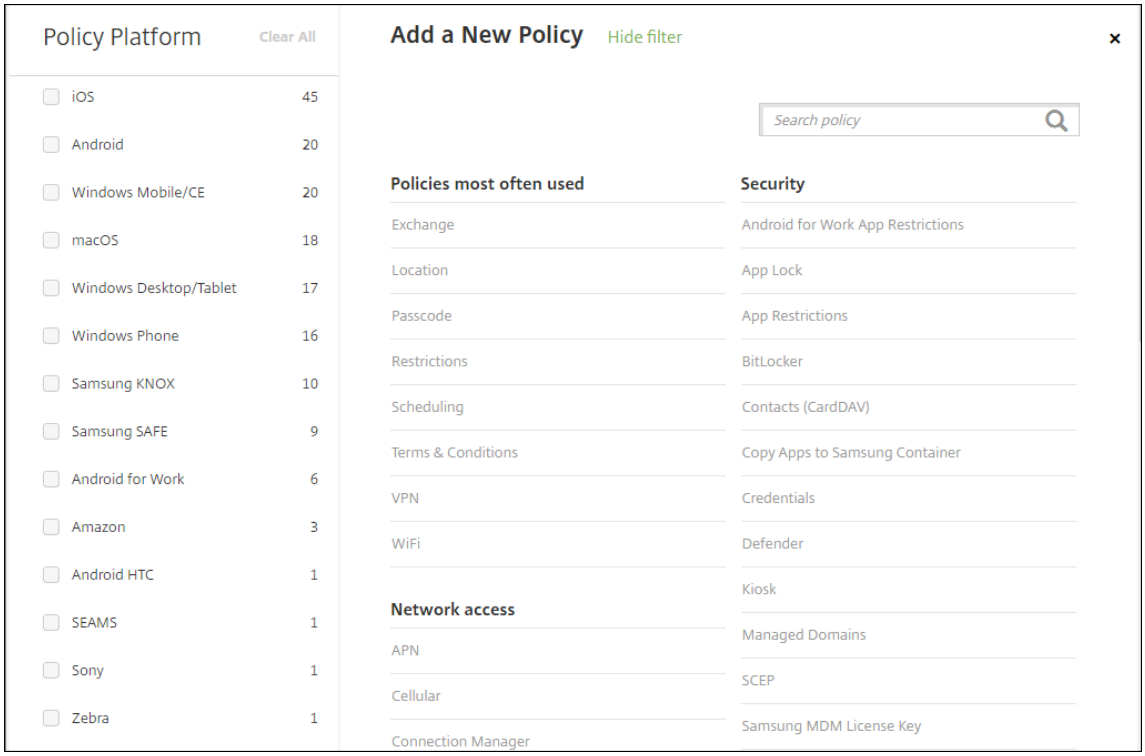
1. Fournissez un nom et une description pour la stratégie.
2. Configurez la stratégie pour une ou plusieurs plates-formes.
3. Créez des règles de déploiement (facultatif).
4. Attribuez la stratégie à des groupes de mise à disposition.
5. Configurez le calendrier de déploiement (facultatif).

Pour créer et gérer les stratégies, accédez à **Configurer > Stratégies d'appareil**.

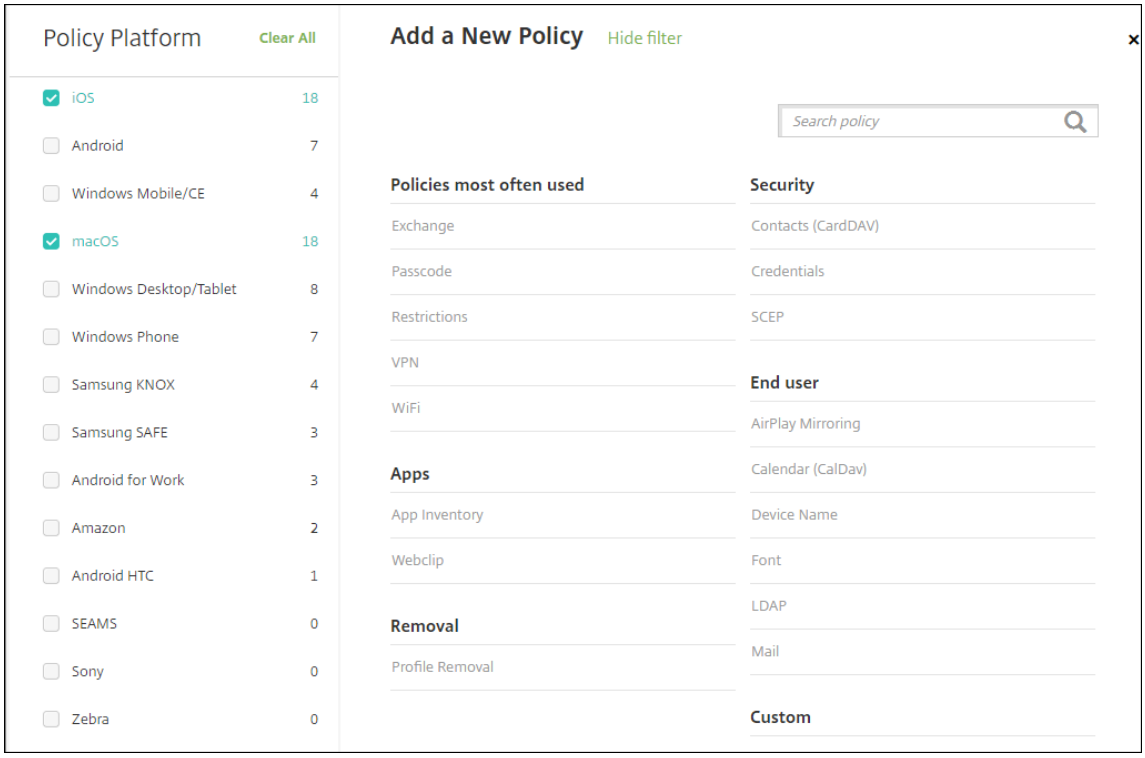


Pour ajouter une stratégie :

1. Sur la page **Stratégies d'appareil**, cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.



2. Cliquez sur une ou plusieurs plates-formes pour afficher une liste des stratégies d'appareil pour les plates-formes sélectionnées. Cliquez sur un nom de stratégie pour continuer avec l'ajout de la stratégie.



Vous pouvez aussi entrer le nom de la stratégie dans le champ de recherche. À mesure que vous tapez, des correspondances potentielles s'affichent. Si votre stratégie figure dans la liste, cliquez dessus. Seule la stratégie sélectionnée reste dans les résultats. Cliquez dessus pour ouvrir la page **Informations de stratégie** pour cette stratégie.

3. Sélectionnez les plates-formes que vous souhaitez inclure dans la stratégie. Les pages de configuration pour les plates-formes sélectionnées s'affichent dans l'étape 5.
4. Remplissez la page **Informations de stratégie** puis cliquez sur **Suivant**. La page **Informations de stratégie** collecte des informations, comme le nom de la stratégie, pour vous aider à identifier et à suivre vos stratégies. Cette page est identique pour toutes les stratégies.
5. Renseignez les pages de plates-formes. Les pages de plates-formes s'affichent pour chaque plate-forme que vous avez sélectionnée dans l'étape 3. Ces pages sont différentes pour chaque stratégie. Une stratégie peut varier d'une plate-forme à l'autre. Toutes les stratégies ne s'appliquent pas à toutes les plates-formes.

   Certaines pages incluent des tableaux d'éléments. Pour supprimer un élément existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

   Pour modifier un élément existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit.

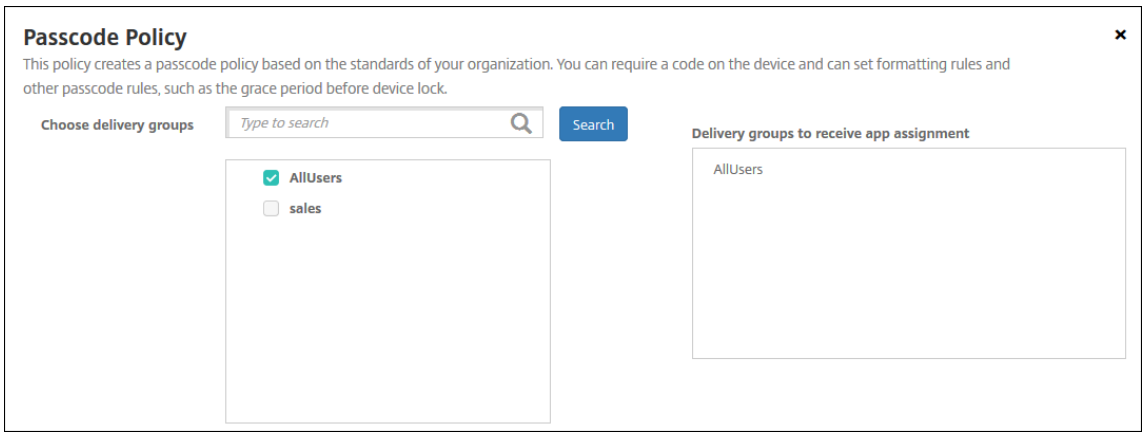
Pour configurer les règles de déploiement, les attributions et le calendrier

Pour de plus amples informations sur la configuration des règles de déploiement, consultez la section Déployer des ressources.

1. Sur la page de la plate-forme, développez **Règles de déploiement** et configurez les paramètres suivants. L'onglet **Base** s'affiche par défaut.
    - Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est **Toutes**.
    - Cliquez sur **Nouvelle règle** pour définir les conditions.
    - Dans la liste, cliquez sur les conditions, telles que **Propriétaire** et **BYOD**.
    - Cliquez sur **Nouvelle règle** de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet **Avancé** pour combiner les règles avec des options booléennes. Les conditions que vous avez choisies sur l'onglet **Base** s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
    - Cliquez sur **ET**, **OU** ou **SAUF**.
    - Dans les listes, sélectionnez les conditions que vous souhaitez ajouter à la règle. Cliquez ensuite sur le signe plus (**+**) sur le côté droit pour ajouter la condition à la règle.

      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur **MODIFIER** pour modifier la condition ou sur **Supprimer** pour supprimer la condition.
    - Cliquez sur **Nouvelle règle** pour ajouter une autre condition.
4. Cliquez sur **Suivant** pour passer à la page de plate-forme suivante, ou lorsque toutes les pages de plate-forme sont remplies, à la page **Attributions**.
5. Sur la page **Attribution**, sélectionnez les groupes de mise à disposition auxquels vous voulez appliquer la stratégie. Si vous cliquez sur un groupe de mise à disposition, le groupe apparaît dans la zone **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

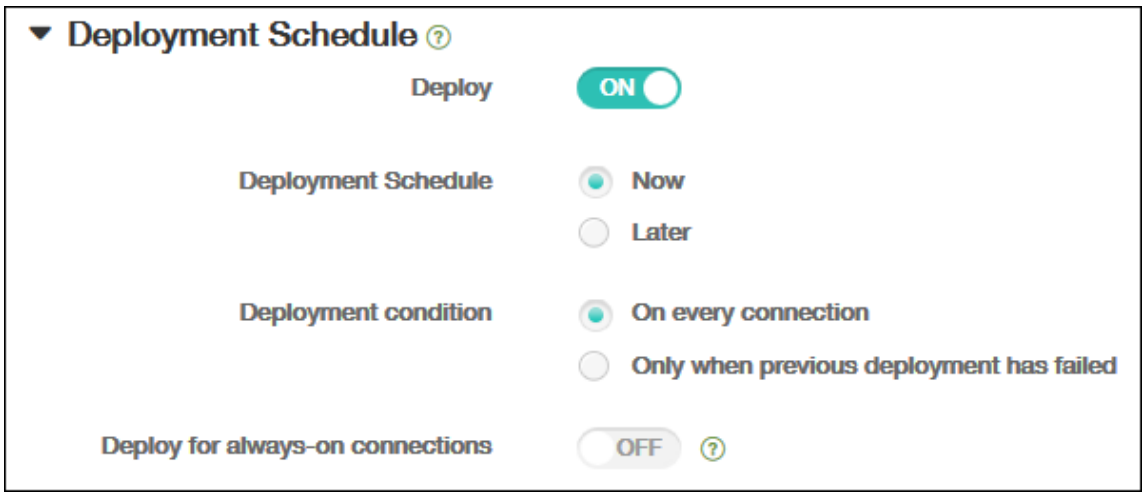
   La zone **Groupes de mise à disposition qui vont recevoir l'attribution d'applications** n'apparaît pas tant que vous n'avez pas sélectionné un groupe de mise à disposition.



6. Sur la page **Attributions**, développez **Calendrier de déploiement** et configurez les paramètres suivants :

   - En regard de **Déployer**, cliquez sur **Activé** pour planifier le déploiement ou cliquez sur **Désactivé** pour empêcher le déploiement. L'option par défaut est **Activé**.
   - En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
   - Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
   - En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
   - En regard de **Déployer pour les connexions permanentes**, cliquez sur **Activé** ou **Désactivé**. L'option par défaut est **Désactivé**.

     > **Remarque :**
     >
     > Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
     >
     > Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.



7. Cliquez sur **Enregistrer**.

   La stratégie apparaît dans le tableau **Stratégies d'appareil**.

Supprimer une stratégie d'un appareil

Les étapes pour supprimer une stratégie d'un appareil dépendent de la plate-forme.

- Android

  Pour supprimer une stratégie d'un appareil Android, utilisez la stratégie de désinstallation de XenMobile. Pour plus d'informations, consultez la section Stratégie de désinstallation de XenMobile.

- iOS et macOS

  Pour supprimer une stratégie d'un appareil iOS ou macOS, utilisez la stratégie de suppression de profil. Sur les appareils iOS et macOS, toutes les stratégies font partie du profil MDM. Vous pouvez ainsi créer une stratégie de suppression de profil uniquement pour la stratégie que vous souhaitez supprimer. Le reste des stratégies et le profil restent sur l'appareil. Pour plus d'informations, consultez la section Stratégie de suppression de profil.

- Windows 10 et Windows 11

  Vous ne pouvez pas supprimer directement une stratégie d'un appareil Windows Desktop et Tablet. Toutefois, vous pouvez utiliser l'une des méthodes suivantes :

  - Désinscrivez l'appareil, puis installez un nouvel ensemble de stratégies sur l'appareil. Les utilisateurs se ré-inscrivent ensuite pour continuer.
  - Effectuez une action de sécurité pour effacer les données d'entreprise d'un appareil spécifique. Cette action supprime toutes les applications et les données d'entreprise de l'appareil. Vous supprimez ensuite la stratégie d'un groupe de mise à disposition con-

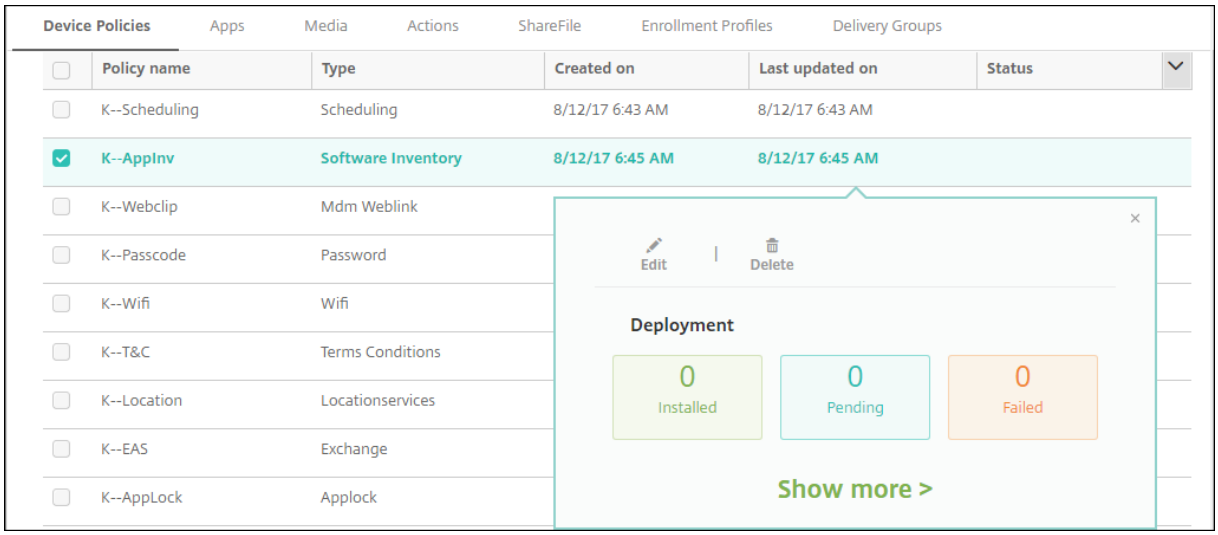
tenant uniquement cet appareil, puis vous transmettez ce groupe de mise à disposition vers l'appareil. Les utilisateurs se ré-inscrivent ensuite pour continuer.

- Chrome OS

  Pour supprimer une stratégie d'un appareil Chrome OS, vous pouvez supprimer la stratégie d'un groupe de mise à disposition contenant uniquement cet appareil. Vous transmettez ensuite le groupe de mise à disposition vers l'appareil.

Modifier une stratégie d'appareil

Pour modifier une stratégie, vous pouvez sélectionner la case à cocher en regard d'une stratégie pour afficher le menu d'options au-dessus de la liste des stratégies. Vous pouvez aussi cliquer sur une stratégie dans la liste pour afficher le menu d'options sur le côté droit de la liste.



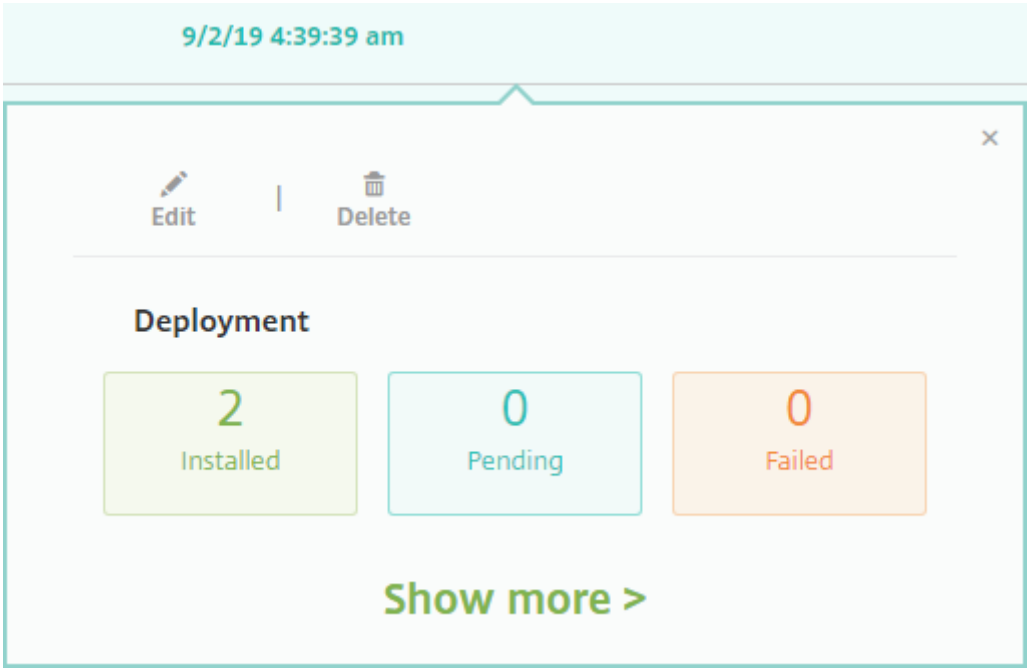
Pour afficher les détails d'une stratégie, cliquez sur **Afficher plus**.

Pour modifier tous les paramètres d'une stratégie, cliquez sur **Modifier**.

Si vous cliquez sur **Supprimer**, une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer** pour supprimer la stratégie.

Vérifier l'état du déploiement de la stratégie

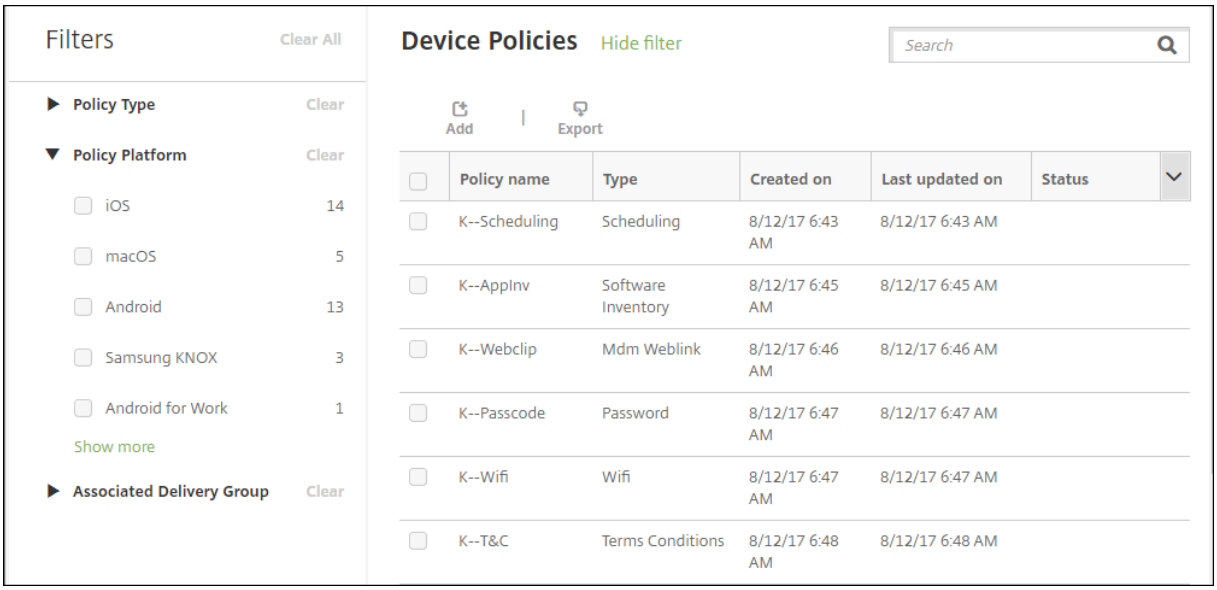
Cliquez sur une ligne de stratégie sur la page **Configurer > Stratégies d'appareil** pour vérifier son état de déploiement.



Lorsqu'un déploiement de stratégie est en attente, les utilisateurs peuvent actualiser la stratégie à partir de Secure Hub en touchant **Préférences > Informations sur l'appareil > Actualiser la stratégie**.

Filtrer la liste des stratégies d'appareil ajoutées

Vous pouvez filtrer la liste des stratégies ajoutées par types de stratégie, plates-formes et groupes de mise à disposition associés. Sur la page **Configurer > Stratégies d'appareil**, cliquez sur **Afficher le filtre**. Dans la liste, sélectionnez les cases à cocher pour les éléments que vous souhaitez voir.



Cliquez sur **ENREGISTRER CETTE VUE** pour enregistrer un filtre. Le nom du filtre s'affiche alors dans

un bouton sous le bouton **ENREGISTRER CETTE VUE**.

Résumé des stratégies d'appareil

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Mise en miroir AirPlay	Ajoute des appareils AirPlay spécifiques (tels qu'un un autre ordinateur Mac) aux appareils iOS. Vous avez également la possibilité d'ajouter des appareils à une liste d'autorisation pour les appareils supervisés. Cette option limite les utilisateurs uniquement aux appareils AirPlay de la liste d'autorisation.
AirPrint	Ajoute les imprimantes AirPrint à la liste d'imprimantes AirPrint sur les appareils iOS. Cette stratégie facilite la prise en charge d'environnements dans lesquels les imprimantes et les appareils figurent sur des sous-réseaux différents.
Autorisation de l'application Android Entreprise	Permet de configurer la façon dont les demandes des applications Android Enterprise dans le cadre de profils de travail gèrent les autorisations qualifiées comme étant « dangereuses » par Google.
Restrictions applicatives Android Enterprise	Met à jour les restrictions associées aux applications Android.
APN	Détermine les paramètres utilisés pour connecter vos appareils au service GPRS d'un opérateur de téléphonie spécifique. Ce paramètre est déjà défini dans la plupart des téléphones récents. Utilisez cette stratégie si votre entreprise n'utilise pas d'APN consommateur pour se connecter à Internet à partir d'un appareil mobile.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Accès aux applications	Permet de définir une liste des applications obligatoires, facultatives ou interdites sur l'appareil. Vous pouvez ensuite créer une action automatisée dont la tâche consiste à vérifier la conformité de l'appareil par rapport à cette liste d'applications.
Attributs d'application	Spécifie des attributs, tels qu'un Bundle ID d'application gérée, ou un identifiant VPN par application pour les appareils iOS.
Configuration d'applications	Configure à distance les différents paramètres et comportements des applications qui prennent en charge la configuration gérée. Pour ce faire, vous déployez un fichier de configuration XML (appelé une liste des propriétés, ou plist) sur des appareils iOS. Vous pouvez également déployer des paires clé/valeur sur un téléphone Windows 10, ou un ordinateur de bureau ou une tablette exécutant des appareils Windows 10 ou Windows 11.
Inventaire des applications	Établit un inventaire des applications sur les appareils gérés. XenMobile compare ensuite l'inventaire avec les stratégies d'accès aux applications déployées sur ces appareils. Vous pouvez ainsi détecter les applications figurant sur une liste d'autorisation ou de blocage et prendre les mesures qui s'imposent.
Mode kiosque	Définit une liste des applications que les utilisateurs peuvent ou ne peuvent pas exécuter sur les appareils iOS ou certains appareils Android.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Utilisation réseau des applications	Définit des règles d'utilisation du réseau pour spécifier la manière dont les applications gérées utilisent les réseaux, tels que les réseaux de données cellulaires, sur les appareils iOS. Les règles s'appliquent uniquement aux applications gérées. Les applications gérées sont des applications que vous déployez sur les appareils des utilisateurs via XenMobile.
Restrictions applicatives	Crée des listes de blocage pour les d'applications que vous ne souhaitez pas que les utilisateurs installent sur des appareils Samsung KNOX. Vous pouvez également créer des listes d'autorisation pour les applications que les utilisateurs peuvent installer.
Désinstallation des applications	Supprime des applications des appareils utilisateur.
Restrictions de désinstallation d'applications	Spécifie les applications que les utilisateurs peuvent ou ne peuvent pas désinstaller.
Notifications d'applications	Permet de contrôler la manière dont les utilisateurs iOS recevront les notifications depuis certaines applications.
Mise à jour automatique des applications gérées	Contrôle la façon dont les applications gérées installées sont mises à jour sur les appareils Android Enterprise.
BitLocker	Configure les paramètres disponibles dans l'interface BitLocker sur les appareils Windows 10 et Windows 11.
Navigateur	Définit si les appareils peuvent utiliser le navigateur ou à quelles fonctions du navigateur les appareils ont accès.
Calendrier (CalDav)	Ajoute un compte de calendrier (CalDAV) aux appareils iOS ou macOS. Le compte CalDAV permet aux utilisateurs de synchroniser les données de planification avec tout serveur qui prend en charge CalDAV.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Cellulaire	Configure les paramètres du réseau cellulaire.
Gestionnaire de connexions	Spécifie les paramètres de connexion pour les applications qui se connectent automatiquement à Internet et à des réseaux privés. Cette stratégie est uniquement disponible pour Windows Pocket PC.
Contacts (CardDAV)	Ajoute un contact iOS (CardDAV) aux appareils iOS ou macOS. Le compte CardDAV permet aux utilisateurs de synchroniser les données de contact avec tout serveur qui prend en charge CardDAV.
Contrôler mise à jour d'OS	Déploie les dernières mises à jour du système d'exploitation sur les appareils pris en charge supervisés.
Copier les applications sur le conteneur Samsung	Copie les applications déjà installées sur un appareil à copier vers un conteneur KNOX sur les appareils Samsung pris en charge. Les applications copiées sur le conteneur KNOX sont disponibles uniquement lorsque les utilisateurs se connectent au conteneur KNOX.
Informations d'identification	Permet l'authentification intégrée avec votre configuration PKI dans XenMobile. Par exemple, avec une entité PKI, un keystore, un fournisseur d'identités ou un certificat de serveur.
XML personnalisé	Personnalise les fonctionnalités telles que le provisioning d'appareils, l'activation de fonctionnalités d'appareil, la configuration d'appareil et la gestion des erreurs.
Defender	Configure les paramètres de Windows Defender pour les bureaux et tablettes Windows 10 et Windows 11.
Supprimer les fichiers et dossiers	Supprime des fichiers ou dossiers spécifiques d'appareils Windows Mobile/CE.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Supprimer des clés et valeurs de Registre	Supprime des clés et valeurs de Registre spécifiques d'appareils Windows Mobile/CE.
Attestation de l'intégrité des appareils	Requiert que les appareils Windows 10 et Windows 11 signalent l'état de leur intégrité. Pour ce faire, ils envoient des informations d'exécution et des données spécifiques au service d'attestation de l'intégrité (HAS) pour analyse. Le service HAS crée et renvoie un certificat d'attestation d'intégrité que l'appareil envoie ensuite à XenMobile. Lorsque XenMobile reçoit le certificat d'attestation d'intégrité, en fonction du contenu de ce certificat, des actions automatiques que vous avez configurées peuvent être déployées.
Nom de l'appareil	Définit les noms sur des appareils iOS et macOS, ce qui vous permet d'identifier les appareils. Vous pouvez utiliser des macros et du texte, ou une combinaison des deux pour définir le nom de l'appareil.
Configuration de l'éducation	Configure les appareils des enseignants et des élèves pour une utilisation avec Apple Éducation. Si les instructeurs utilisent l'application En classe, la stratégie Configuration de l'éducation est requise.
Hub d'entreprise	Distribue des applications d'entreprise aux Windows Phone via le magasin hub d'entreprise. XenMobile prend en charge une seule stratégie d'hub d'entreprise pour un mode Windows Phone Secure Hub. Par exemple, ne créez pas de multiples stratégies d'hub d'entreprise avec différentes versions de Worx Home pour XenMobile Enterprise Edition. Vous pouvez déployer la stratégie d'hub d'entreprise initiale uniquement lors de l'inscription de l'appareil.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Exchange	Active la messagerie ActiveSync pour le client de messagerie natif sur l'appareil.
Fichiers	Ajoute des fichiers de script à XenMobile qui exécutent certaines fonctions pour les utilisateurs. Ou vous pouvez ajouter des fichiers de documents auxquels vous voulez que les utilisateurs Android aient accès sur leurs appareils. Lorsque vous ajoutez le fichier, vous pouvez également spécifier le répertoire dans lequel vous souhaitez que le fichier soit stocké sur l'appareil.
FileVault	Cette stratégie vous permet d'activer le chiffrement FileVault sur les appareils macOS inscrits. Vous pouvez également contrôler combien de fois un utilisateur peut ignorer l'installation de FileVault lors de la connexion. Disponible pour macOS 10.7 ou version ultérieure.
Pare-feu	Configure les paramètres du pare-feu. Vous pouvez entrer les adresses IP, les ports et les noms d'hôte que vous souhaitez autoriser ou empêcher sur les appareils. Vous pouvez également configurer les paramètres de redirection de proxy et de proxy.
Police	Ajoute des polices aux appareils iOS et macOS. Les polices doivent être de type TrueType (.TTF) ou OpenType (.OFT). XenMobile ne prend pas en charge les collections de polices (.TTC ou .OTC).
Disposition de l'écran d'accueil	Définit la disposition des applications et des dossiers pour l'écran d'accueil d'iOS sur les appareils supervisés iOS 9.3 et versions ultérieures.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Importer le profil iOS et macOS	Importe les fichiers XML de configuration d'appareil pour iOS et macOS dans XenMobile. Le fichier contient des stratégies de sécurité et des restrictions que vous préparez avec Apple Configurator.
Gestion du keyguard	Contrôle les fonctionnalités disponibles pour les utilisateurs avant qu'ils déverrouillent le keyguard de l'appareil et le keyguard de challenge professionnel. Vous pouvez également contrôler les fonctions de keyguard d'appareil pour les appareils entièrement gérés et dédiés. Par exemple, vous pouvez désactiver les fonctions d'écran de verrouillage telles que le déverrouillage par empreinte digitale, les agents de confiance et les notifications.
Kiosque	Limite l'utilisation des applications sur les appareils Samsung SAFE. Vous pouvez limiter les applications disponibles à une ou plusieurs applications spécifiques. Cette stratégie est utile pour les appareils d'entreprise conçus pour n'exécuter qu'un type spécifique ou une classe d'applications. Cette stratégie vous permet également de choisir des images personnalisées à utiliser comme fond d'écran de l'écran d'accueil et de l'écran de verrouillage pour le mode Kiosque.
Configuration du Launcher	Spécifie les paramètres de Citrix Launcher sur les appareils Android, tels que les applications autorisées et une image de logo personnalisée pour l'icône Launcher.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
LDAP	Fournit des informations sur un serveur LDAP à utiliser pour les appareils iOS, y compris toute information nécessaire sur le compte telle que le nom d'hôte du serveur LDAP. La stratégie fournit également un ensemble de stratégies de recherche LDAP à utiliser lors de l'interrogation du serveur LDAP.
Emplacement	Permet de géo-localiser les appareils sur une carte, en supposant que le GPS est activé pour Secure Hub sur l'appareil. Après le déploiement de cette stratégie sur l'appareil, vous pouvez envoyer une commande de localisation à partir du serveur XenMobile. L'appareil répond avec ses coordonnées d'emplacement. Les stratégies de géofencing et de suivi sont également prises en charge.
Messagerie	Configure un compte de messagerie sur les appareils iOS ou macOS.
Domaines gérés	Définit des domaines gérés qui s'appliquent à la messagerie et au navigateur Safari. Les domaines gérés vous aident à protéger les données d'entreprise en contrôlant les applications qui peuvent ouvrir des documents téléchargés depuis des domaines à l'aide de Safari. Pour les appareils supervisés iOS 8 et versions ultérieures, vous pouvez spécifier des adresses URL ou des sous-domaines pour contrôler la manière dont les utilisateurs peuvent ouvrir des documents, des pièces jointes et des téléchargements à partir du navigateur.
Options MDM	Gère les fonctions Localiser mon téléphone/Verrouillage d'activation iPad sur les appareils supervisés iOS 7.0 et versions ultérieures.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Infos organisation	Spécifie les informations d'organisation pour les messages d'alerte que XenMobile déploie vers les appareils iOS.
Code secret	Définit un code PIN ou un mot de passe sur un appareil géré. Vous pouvez définir la complexité et les délais d'expiration du code secret sur l'appareil.
Personal Hotspot	Permet aux utilisateurs de se connecter à Internet lorsqu'ils ne sont pas à portée d'un réseau Wi-Fi. Les utilisateurs se connectent via la connexion de données cellulaires de leur appareil iOS, à l'aide de la fonctionnalité de point d'accès personnel.
Suppression de profil	Supprime le profil d'application des appareils iOS ou macOS.
Profil de provisioning	Spécifie un profil de provisioning de distribution d'entreprise à envoyer aux appareils. Lorsque vous développez et codez une application d'entreprise iOS, vous incluez généralement un profil de provisioning. Apple requiert que le profil de l'application s'exécute sur un appareil iOS. Si un profil de provisioning est manquant, ou s'il a expiré, l'application se bloque lorsque l'utilisateur tape pour l'ouvrir.
Suppression du profil de provisioning	Supprime les profils de provisioning iOS.
Proxy	Spécifie les paramètres de proxy HTTP globaux pour les appareils exécutant Windows Mobile/CE et iOS. Vous ne pouvez déployer qu'une stratégie de proxy HTTP globale par appareil.
Registre	Définit les clés et valeurs de registre qui vous permettent de gérer les appareils Windows Mobile/CE. Le registre Windows Mobile/CE stocke des données sur les applications, pilotes, préférences utilisateur et paramètres de configuration.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Assistance à distance	Offre un accès à distance aux appareils Samsung KNOX. L'Assistance à distance n'est plus disponible pour les nouveaux clients à compter du 1er janvier 2019. Les clients existants peuvent continuer à utiliser le produit, mais Citrix ne fournira pas d'améliorations ou de correctifs.
Restrictions	Offre des centaines d'options pour verrouiller et contrôler les fonctionnalités sur les appareils gérés. Exemples d'options de restriction : désactiver l'appareil photo ou le micro, appliquer des règles d'itinérance et imposer l'accès à des services tiers, tels que des magasins d'applications.
Itinérant	Active ou non les services de voix et de données en itinérance sur des appareils iOS et Windows Mobile/CE. Lorsque l'itinérance de la voix est désactivée, l'itinérance des données est automatiquement désactivée.
Clé de licence MDM Samsung	Spécifie la clé Samsung ELM (Enterprise License Management) intégrée que vous devez déployer sur un appareil avant de pouvoir déployer des stratégies et restrictions SAFE. XenMobile prend également en charge le service E-FOTA (Firmware Over-The-Air) Samsung Enterprise. XenMobile prend en charge et étend les stratégies Samsung for Enterprise (SAFE) et Samsung KNOX.
Planification	Requise pour que les appareils Android et Windows Mobile puissent se connecter au serveur XenMobile pour pouvoir utiliser la gestion MDM, distribuer des applications et déployer des stratégies. Si vous n'envoyez pas cette stratégie à des appareils et que vous n'avez pas activé Google FCM, un appareil ne peut pas se reconnecter au serveur.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
SCEP	Configure les appareils iOS et macOS afin de récupérer un certificat à partir d'un serveur SCEP externe. Vous pouvez également fournir un certificat à l'appareil à l'aide du protocole SCEP à partir d'une PKI connectée à XenMobile. Pour ce faire, créez une entité PKI et un fournisseur PKI en mode distribué.
Compte SSO	Crée des comptes SSO pour permettre aux utilisateurs de s'authentifier une seule fois pour accéder à XenMobile et à vos ressources d'entreprise internes. Les utilisateurs n'ont pas à stocker d'informations d'identification sur l'appareil. XenMobile utilise les informations d'identification de l'utilisateur d'entreprise du compte SSO pour toutes les applications, y compris les applications provenant de l'App Store. Cette stratégie est compatible avec l'authentification Kerberos. Disponible sur iOS.
Cryptage du stockage	Permet de crypter le stockage interne et externe. Pour certains appareils, cette stratégie empêche les utilisateurs d'utiliser une carte de stockage sur leurs appareils.
Abonnements calendriers	Ajoute un abonnement calendrier à la liste des calendriers sur les appareils iOS. Vous devez être abonné à un calendrier avant de pouvoir l'ajouter à la liste des abonnements calendriers sur les appareils des utilisateurs.
Termes et conditions	Requiert que les utilisateurs acceptent les stratégies spécifiques de votre entreprise relatives aux connexions au réseau d'entreprise. Lorsque les utilisateurs inscrivent leurs appareils auprès de XenMobile, ils doivent accepter les termes et conditions pour inscrire leurs appareils. Le refus des termes et conditions annule le processus d'inscription.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Tunnel	Utilisée uniquement pour l'assistance à distance. L'Assistance à distance permet aux représentants du service d'assistance de contrôler à distance des appareils mobiles Windows CE et Android gérés. L'Assistance à distance n'est pas disponible pour les déploiements de XenMobile Server locaux en cluster. L'Assistance à distance n'est plus disponible pour les nouveaux clients à compter du 1er janvier 2019. Les clients existants peuvent continuer à utiliser le produit, mais Citrix ne fournira pas d'améliorations ou de correctifs.
VPN	Fournit un accès aux systèmes principaux qui utilisent une technologie de passerelle VPN d'ancienne génération. Cette stratégie fournit des détails de connexion à une passerelle VPN que vous pouvez déployer sur les appareils. XenMobile prend en charge plusieurs fournisseurs VPN, y compris Cisco AnyConnect, Juniper et Citrix VPN. Si la passerelle VPN prend en charge cette option, vous pouvez associer cette stratégie à une autorité de certification et activer le VPN à la demande.
Fond d'écran	Ajoute un fichier .png ou .jpg en tant que fond d'écran sur l'écran d'accueil, l'écran de verrouillage ou les deux. Pour utiliser un fond d'écran différent sur iPad et iPhone, créez différentes stratégies de fond d'écran et les déployer vers les utilisateurs appropriés.
Filtre de contenu Web	Filtre le contenu web sur les appareils iOS. XenMobile utilise la fonction de filtrage automatique d'Apple et les sites que vous ajoutez aux listes d'autorisation et de blocage. Disponible uniquement sur les appareils iOS supervisés.

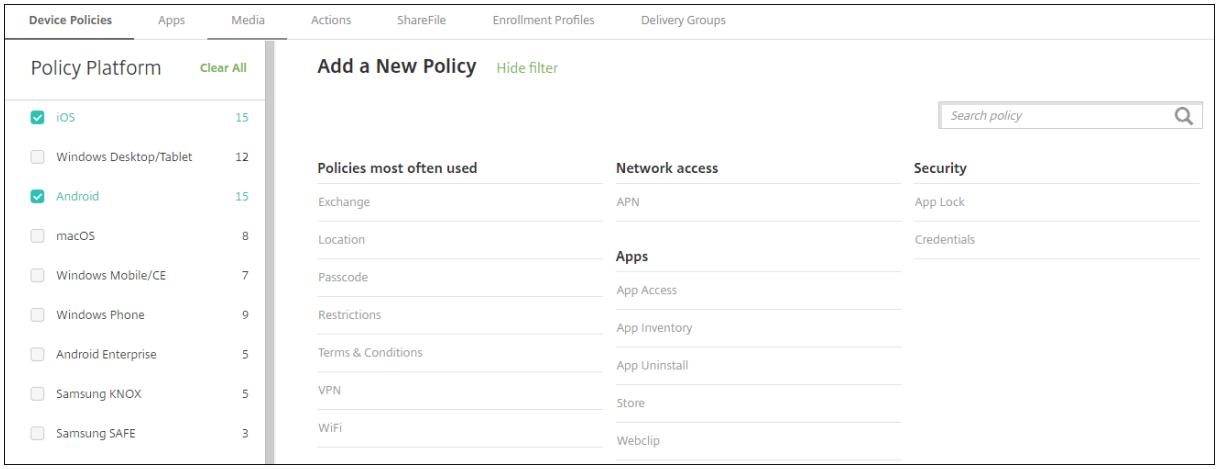
Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Clip Web	Place des raccourcis ou clips Web sur des sites Web de manière à ce qu'ils apparaissent à côté des applications sur les appareils des utilisateurs. Vous pouvez spécifier vos propres icônes pour représenter les clips Web sur des appareils iOS, macOS X et Android. Windows Tablet requiert uniquement un libellé et une adresse URL.
Wi-Fi	Permet aux administrateurs de déployer les détails du routeur Wi-Fi vers des appareils gérés. Les détails du routeur comprennent le SSID, les données d'authentification et les données de configuration.
Certificat Windows CE	Crée et met à disposition des certificats Windows Mobile/CE à partir d'une PKI externe vers les appareils des utilisateurs.
Protection des informations Windows (WIP)	Spécifie les applications qui requièrent la protection des informations de Windows au niveau d'exécution que vous définissez pour la stratégie. La stratégie est pour les appareils supervisés Windows 10 et Windows 11.
XenMobile Store	Indique si un clip Web XenMobile Store s'affiche sur l'écran d'accueil des appareils utilisateur.
Options XenMobile	Configure le comportement de Secure Hub lors de la connexion à XenMobile à partir d'appareils Android et Windows Mobile/CE.
Désinstallation de XenMobile	Désinstalle XenMobile des appareils Android et Windows Mobile/CE. Lorsqu'elle est déployée, cette stratégie supprime XenMobile sur tous les appareils du déploiement.

Stratégies applicatives par plate-forme

January 10, 2022

Pour afficher les stratégies disponibles par plate-forme :

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**.
2. Cliquez sur **Ajouter**.
3. Chaque plate-forme apparaît dans une liste du panneau **Stratégie par plate-forme**. Si ce panneau n'est pas ouvert, cliquez sur **Afficher le filtre**.
4. Pour afficher une liste de toutes les stratégies disponibles pour une plate-forme, sélectionnez cette plate-forme. Pour afficher une liste des stratégies disponibles pour plusieurs plates-formes, sélectionnez chacune de ces plates-formes. Une stratégie apparaît dans la liste uniquement si elle s'applique à chaque plate-forme sélectionnée.



La version la plus récente de XenMobile prend en charge les stratégies d'appareil pour les plates-formes suivantes :

- Amazon
- Android
- Android Entreprise
- Android Zebra
- iOS
- macOS
- Samsung SAFE
- Samsung KNOX
- Ordinateur de bureau/tablette Windows 10 et Windows 11
- Windows 10 Phone
- Windows Mobile/CE

Pour de plus amples informations sur les appareils pris en charge dans la version la plus récente de XenMobile, consultez la section Plates-formes prises en charge.

> **Remarque :**
>
> Si votre environnement est configuré avec des objets de stratégie de groupe (GPO) :

> Lorsque vous configurez des stratégies d'appareil XenMobile pour Windows 10 et Windows 11, n'oubliez pas la règle suivante. Si une stratégie sur un ou plusieurs appareils inscrits entraîne un conflit, la stratégie correspondant au GPO est prioritaire.

Stratégie de mise en miroir AirPlay

January 10, 2022

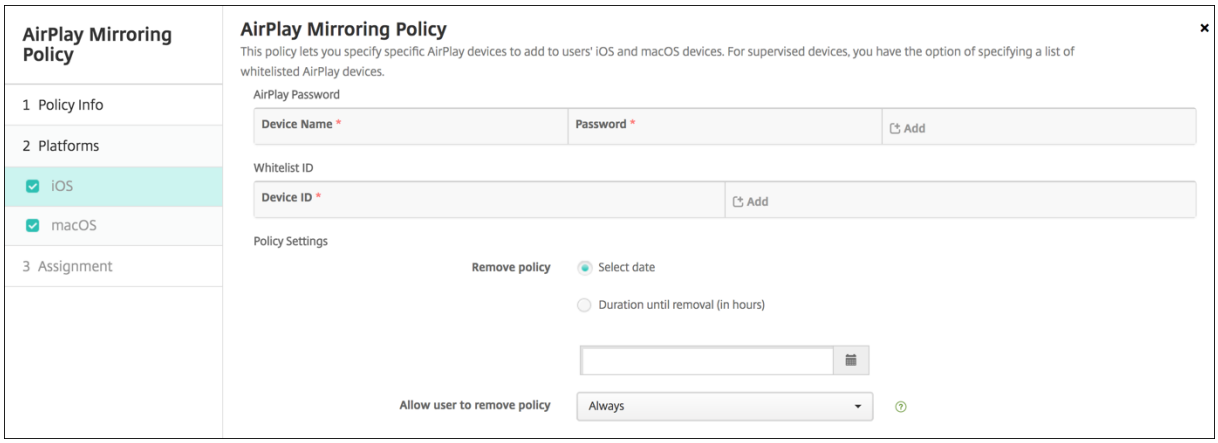
La fonctionnalité Apple AirPlay permet aux utilisateurs de mettre en miroir tout ce qui figure sur l'écran d'un appareil sur un autre ordinateur Mac.

Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin d'ajouter des appareils AirPlay spécifiques (tels qu'un autre ordinateur Mac) aux appareils iOS. Vous avez également la possibilité d'ajouter des appareils à une liste d'autorisation d'appareils supervisés, ce qui limite l'accès des utilisateurs uniquement à ces appareils AirPlay. Pour de plus amples informations sur le placement d'un appareil en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

> **Remarque :**
>
> Avant de continuer, vérifiez que vous disposez des ID et des mots de passe de tous les appareils que vous voulez ajouter.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Mot de passe AirPlay :** pour chaque appareil que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :

  - **ID de l'appareil :** entrez l'adresse du matériel (adresse MAC) au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
  - **Mot de passe :** entrez un mot de passe pour l'appareil (facultatif).
  - Cliquez sur **Ajouter** pour ajouter l'appareil ou cliquez sur **Annuler** pour annuler l'ajout de l'appareil.

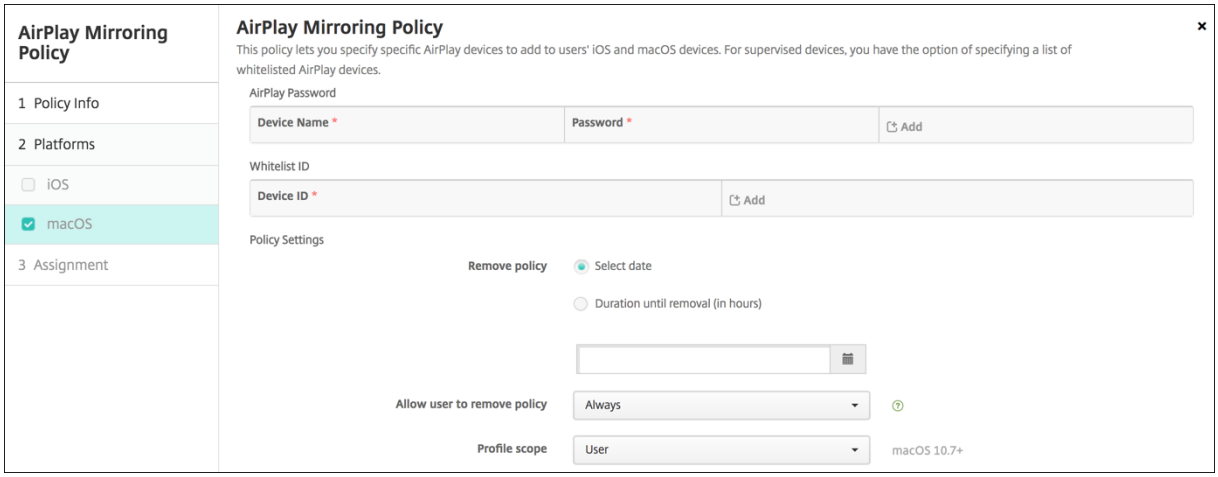
- **ID de liste blanche :** cette liste est ignorée pour les appareils non supervisés. Les ID d'appareil de cette liste sont les seuls appareils AirPlay disponibles pour les utilisateurs. Pour chaque appareil AirPlay que vous souhaitez ajouter à la liste, cliquez sur **Ajouter**, puis procédez comme suit :

  > **Remarque :**
  >
  > La console XenMobile Server utilise les termes « liste noire » et « liste blanche ». Ces termes seront modifiés dans une prochaine version et les termes « liste de blocage » et « liste d'autorisation » les remplaceront.

  - **ID de l'appareil :** entrez l'ID de l'appareil au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
  - Cliquez sur **Ajouter** pour ajouter l'appareil ou cliquez sur **Annuler** pour annuler l'ajout de l'appareil.

- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.

Paramètres macOS



- **Mot de passe AirPlay :** pour chaque appareil que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **ID de l'appareil :** entrez l'adresse du matériel (adresse MAC) au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
  - **Mot de passe :** entrez un mot de passe pour l'appareil (facultatif).
  - Cliquez sur **Ajouter** pour ajouter l'appareil ou cliquez sur **Annuler** pour annuler l'ajout de l'appareil.
- **ID de liste blanche :** cette liste est ignorée pour les appareils non supervisés. Les ID d'appareil de cette liste sont les seuls appareils AirPlay disponibles pour les utilisateurs. Pour chaque appareil AirPlay que vous souhaitez ajouter à la liste, cliquez sur **Ajouter**, puis procédez comme suit :
  - **ID de l'appareil :** entrez l'ID de l'appareil au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
  - Cliquez sur **Ajouter** pour ajouter l'appareil ou cliquez sur **Annuler** pour annuler l'ajout de l'appareil.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.

- **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Stratégie AirPrint

January 10, 2022

Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin d'ajouter des imprimantes AirPrint à la liste des imprimantes AirPrint sur les appareils iOS. Cette stratégie facilite la prise en charge d'environnements dans lesquels les imprimantes et les appareils figurent sur des sous-réseaux différents.

Cette stratégie s'applique à iOS 7.0 et versions supérieures.

> **Remarque :**
>
> Vérifiez que vous disposez de l'adresse IP et du chemin d'accès à la ressource pour chaque imprimante.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Destination AirPrint :** pour chaque destination AirPrint que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Adresse IP :** entrez l'adresse IP de l'imprimante AirPrint.
  - **Chemin d'accès à la ressource :** entrez le chemin d'accès à la ressource associé à l'imprimante. Cette valeur correspond au paramètre de l'enregistrement Bonjour _ipps.tcp. Par exemple, imprimantes/Canon_MG5300_series ou imprimantes/Xerox_Phaser_7600.
  - Cliquez sur **Enregistrer** pour ajouter l'imprimante ou sur **Annuler** pour annuler l'ajout de l'imprimante.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.

* **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Stratégie Configurations gérées par Android Entreprise

January 10, 2022

La stratégie Configurations gérées par Android Enterprise contrôle de nombreuses options de configuration et de restriction d'applications. Le développeur de l'application définit les options disponibles pour une application et les info-bulles. Si une info-bulle mentionne l'utilisation d'une « valeur basée sur un modèle », utilisez plutôt la macro XenMobile correspondante. Pour plus d'informations, consultez la page Remote configuration overview (sur le site développeur Android) et la section Macros.

Les paramètres de configuration de l'application peuvent inclure des éléments tels que :

- Paramètres de messagerie de l'application
- Autoriser ou bloquer les URL d'un navigateur Web
- Possibilité de contrôler la synchronisation du contenu de l'application via une connexion cellulaire ou uniquement via une connexion Wi-Fi

Pour plus d'informations sur les paramètres qui apparaissent pour vos applications, contactez le développeur de l'application.

Conditions préalables

- Terminez les tâches de configuration d'Android Entreprise sur Google et connectez Android Entreprise à Google Play d'entreprise. Pour plus d'informations, consultez la section Android Enterprise.
- Ajoutez des applications Android Enterprise à XenMobile. Pour de plus amples informations, consultez la section Ajout d'applications à XenMobile.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Configuration requise pour les réseaux Per App VPN

Pour créer une stratégie Per App VPN pour AE, vous devez effectuer des étapes supplémentaires, en plus de configurer la stratégie de configurations gérées Android Enterprise. En outre, vous devez vérifier que les conditions préalables suivantes sont remplies :

- Passerelle Citrix Gateway locale

- Les applications suivantes sont installées sur l'appareil :
  - Citrix SSO
  - Citrix Secure Hub

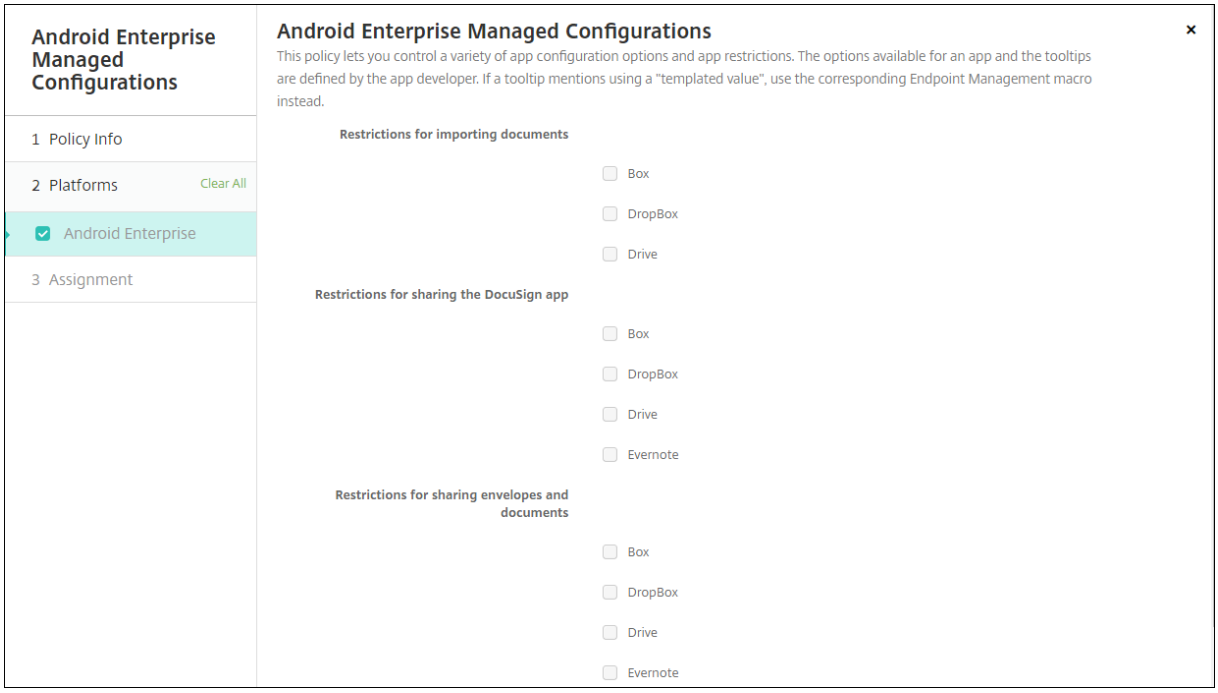
Voici un workflow général pour configurer une stratégie Per App VPN pour les appareils AE :

1. Configurez un profil VPN comme décrit dans cet article.
2. Configurez Citrix ADC pour accepter le trafic provenant du réseau Per App VPN. Pour de plus amples informations, consultez la section Full VPN setup on Citrix Gateway.

Paramètres Android Enterprise

Après avoir choisi d'ajouter une stratégie Configurations gérées par Android Enterprise, une invite permettant de sélectionner une application s'affiche. Si aucune application Android Enterprise n'a été ajoutée à XenMobile, vous ne pouvez pas continuer.

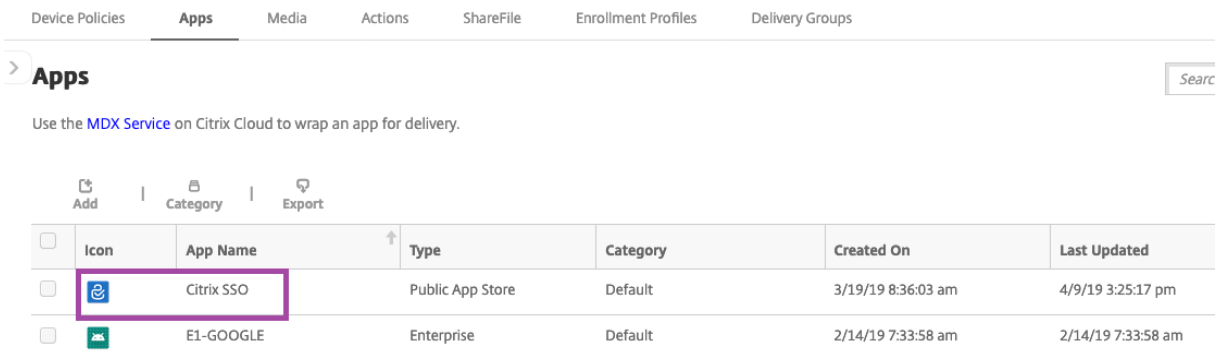
Après avoir sélectionné une application, configurez les paramètres de la stratégie. Les paramètres sont spécifiques à chaque application.



Configurer les profils VPN pour Android Enterprise

Rendez les profils VPN disponibles pour les appareils Android Enterprise à l'aide de l'application Citrix SSO avec la stratégie Configurations gérées par Android Entreprise.

Commencez par ajouter Citrix SSO à la console XenMobile en tant qu'application du magasin Google Play. Consultez la section Ajouter une application de magasin public.

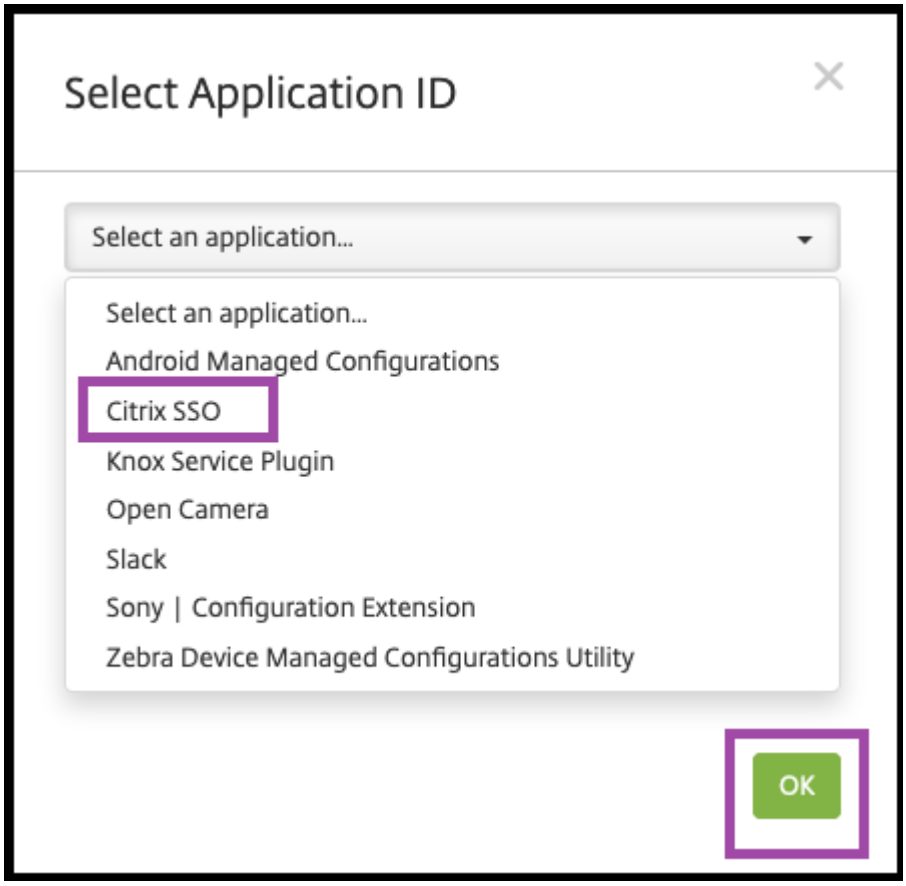


Créer une configuration gérée par Android Enterprise pour Citrix SSO

Configurez la stratégie Configurations gérées par Android Entreprise pour Citrix SSO afin de créer des profils VPN. Les appareils sur lesquels l'application Citrix SSO est installée et la stratégie déployée ont accès aux profils VPN que vous créez.

Vous avez besoin du nom de domaine complet et du port Citrix Gateway.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. Cliquez sur **Ajouter**.
2. Sélectionnez **Android Enterprise**. Cliquez sur **Configurations gérées par Android Entreprise**.
3. Lorsque la fenêtre **Sélectionner un ID d'application** s'affiche, choisissez **Citrix SSO** dans la liste et cliquez sur **OK**.



4. Saisissez un nom et une description pour votre configuration VPN Citrix SSO. Cliquez sur **Suivant**.

5. Configurez les paramètres de profil VPN.

   - **Nom du profil VPN :** saisissez un nom pour le profil VPN. Si vous créez plusieurs pro-

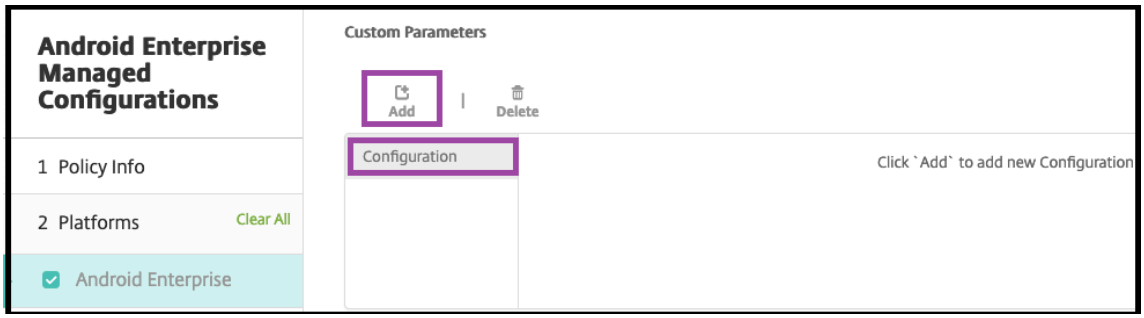
fils VPN, utilisez un nom unique pour chaque profil. Si vous ne fournissez pas de nom, l'adresse que vous avez spécifiée dans le champ **Adresse du serveur** est utilisée comme nom de profil VPN.

- **Adresse du serveur(*) :** saisissez le nom de domaine complet Citrix Gateway. Si le port Citrix Gateway n'est pas 443, saisissez également le port. Utilisez le format URL. Par exemple, `https://gateway.mycompany.com:8443`.
- **Nom d'utilisateur (facultatif) :** indiquez le nom d'utilisateur que les utilisateurs utilisent pour s'authentifier auprès de Citrix Gateway. Vous pouvez utiliser la macro XenMobile {user.username} pour ce champ. (Consultez Macros.) Si vous ne fournissez pas de nom d'utilisateur, les utilisateurs sont invités à fournir un nom d'utilisateur lors de la connexion à Citrix Gateway.
- **Mot de passe (facultatif) :** indiquez le mot de passe que les utilisateurs utilisent pour s'authentifier auprès de Citrix Gateway. Si vous ne fournissez pas de mot de passe, les utilisateurs sont invités à fournir un mot de passe lors de la connexion à Citrix Gateway.
- **Alias de certificat (facultatif) :** Tapez un alias de certificat. L'alias de certificat permet à l'application d'accéder plus facilement au certificat. Lorsque le même alias de certificat est utilisé avec la stratégie d'informations d'identification, l'application récupère le certificat et authentifie le VPN sans aucune action des utilisateurs.
- **Type de VPN par application (facultatif) :** si vous utilisez un VPN par application pour restreindre les applications qui utilisent ce VPN, vous pouvez configurer ce paramètre. Si vous sélectionnez **Autoriser**, le trafic réseau pour les noms de packages d'applications répertoriés dans la **liste des applications Per App VPN** est acheminé via le VPN. Le trafic réseau de toutes les autres applications est acheminé en dehors du VPN. Si vous sélectionnez **Désactiver**, le trafic réseau pour les noms de packages d'applications répertoriés dans la **liste des applications Per App VPN** est acheminé en dehors du VPN. Le trafic réseau de toutes les autres applications est acheminé via le VPN. La valeur par défaut est **Autoriser**.
- **Liste des applications Per App VPN :** liste des applications dont le trafic est autorisé ou bloqué sur le VPN en fonction de la valeur définie pour **Type de VPN par application**. Répertoriez les noms de packages d'applications en les séparant par des virgules ou des points-virgules. Les noms de packages d'applications sont sensibles à la casse et doivent apparaître sur cette liste tels qu'ils figurent dans Google Play Store. Cette liste est facultative. Gardez cette liste vide pour le provisioning de VPN à l'échelle de l'appareil.
- **Profil VPN par défaut :** saisissez le nom du profil VPN à utiliser lorsque les utilisateurs touchent le bouton de connexion dans l'interface utilisateur de l'application Citrix SSO au lieu de toucher un profil spécifique. Si ce champ est vide, le profil principal est utilisé pour la connexion. Si un seul profil est configuré, il est marqué comme profil par défaut. Pour un VPN Always On, ce champ doit être défini sur le nom du profil VPN à utiliser pour établir

un VPN Always On.

- **Désactiver les profils utilisateur :** si ce paramètre est activé, les utilisateurs ne peuvent pas créer leurs propres VPN sur leurs appareils. Si ce paramètre est désactivé, les utilisateurs peuvent créer leurs propres VPN sur leurs appareils. La valeur par défaut est Désactivé.
- **Bloquer serveurs non approuvés :** ce paramètre est désactivé lorsque vous utilisez un certificat auto-signé pour Citrix Gateway ou lorsque le certificat racine de l'autorité de certification qui émet le certificat Citrix Gateway ne figure pas dans la liste d'autorité de certification système. Si ce paramètre est activé, le système d'exploitation Android valide le certificat Citrix Gateway. Si la validation échoue, la connexion n'est pas autorisée. La valeur par défaut est Activé.

6. Vous pouvez également créer des paramètres personnalisés. Les paramètres personnalisés **XenMobileDeviceId** et **UserAgent** sont pris en charge. Sélectionnez la configuration VPN actuelle et cliquez sur **Ajouter**.

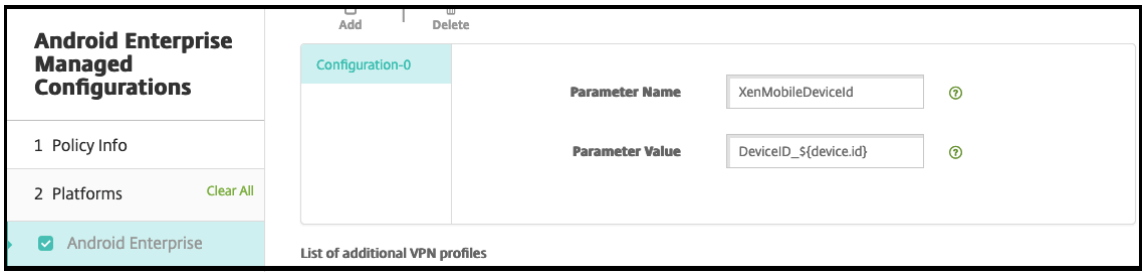


a) Créer un paramètre personnalisé :

- **Nom du paramètre :** saisissez **XenMobileDeviceId**. Il s'agit de l'ID d'appareil à

utiliser pour la vérification d'accès au réseau en fonction de l'inscription de l'appareil dans XenMobile. Si XenMobile inscrit et gère l'appareil, la connexion VPN est autorisée. Sinon, l'authentification est refusée au moment de l'établissement du VPN.

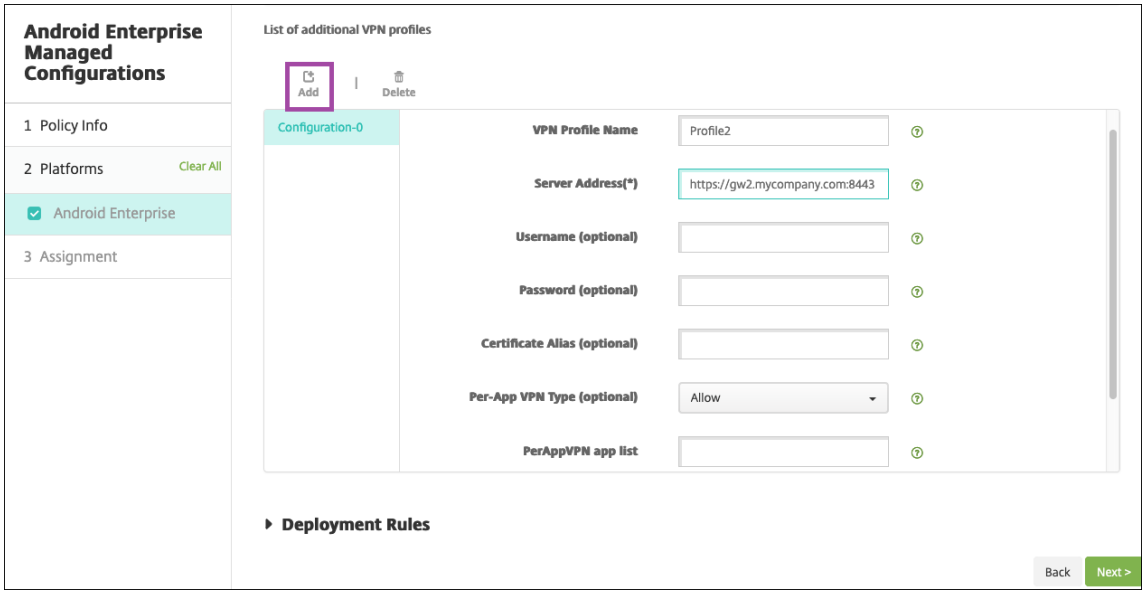
- **Valeur du paramètre :** pour que XenMobile détermine l'état d'inscription et de gestion des appareils, la valeur de XenMobileDeviceId est définie sur `DeviceID_${device.id}`.



a) Pour créer un autre paramètre personnalisé, cliquez à nouveau sur **Ajouter**. Créez ce paramètre personnalisé.

- **Nom du paramètre :** saisissez **UserAgent**. Ce texte a été ajouté à l'en-tête HTTP de l'agent utilisateur pour effectuer une vérification supplémentaire sur Citrix Gateway. La valeur de ce texte est ajoutée à l'en-tête HTTP de l'agent utilisateur par l'application Citrix SSO lors de la communication avec Citrix Gateway.
- **Valeur du paramètre :** saisissez le texte à ajouter à l'en-tête HTTP de l'agent utilisateur. Ce texte doit être conforme aux spécifications HTTP de l'agent utilisateur.

7. Vous pouvez également créer des configurations de profil VPN supplémentaires. Cliquez sur **Ajouter** dans la liste des configurations. Une nouvelle configuration apparaît dans la liste. Sélectionnez la nouvelle configuration et répétez l'étape 5 et, éventuellement, l'étape 6.



8. Lorsque vous avez créé tous les profils VPN de votre choix, cliquez sur **Suivant**.
9. Configurez les règles de déploiement associées à cette configuration gérée pour Citrix SSO.
10. Cliquez sur **Enregistrer**.

Cette configuration gérée pour Citrix SSO apparaît désormais dans la liste des stratégies d'appareil configurées.

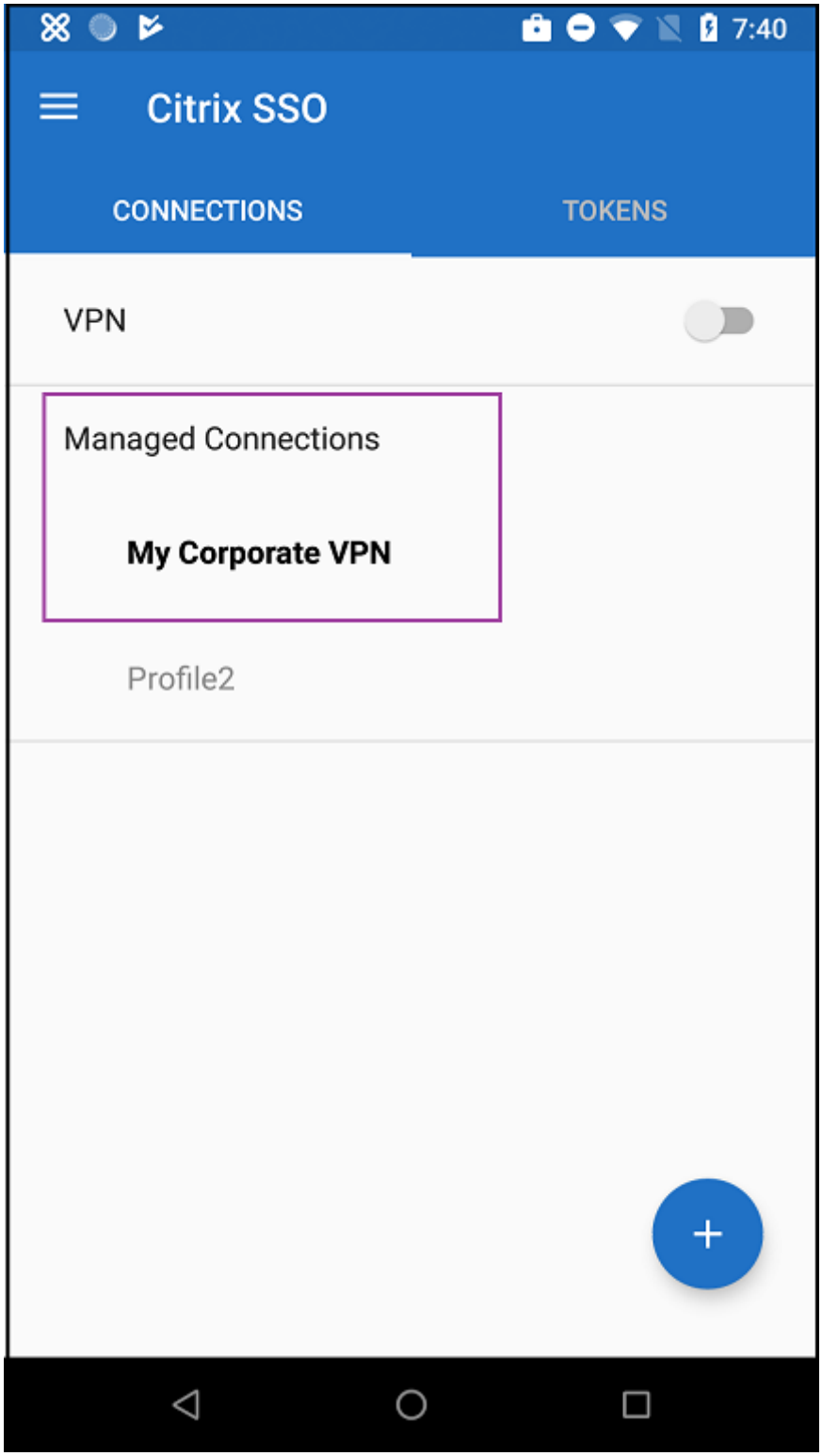
Pour activer l'option Always-On pour les profils VPN que vous avez configurés, définissez la stratégie Options de XenMobile.

> **Remarque :**
> Citrix Secure Hub 19.5.5 ou supérieur est requis pour VPN Always-On pour Android Entreprise.

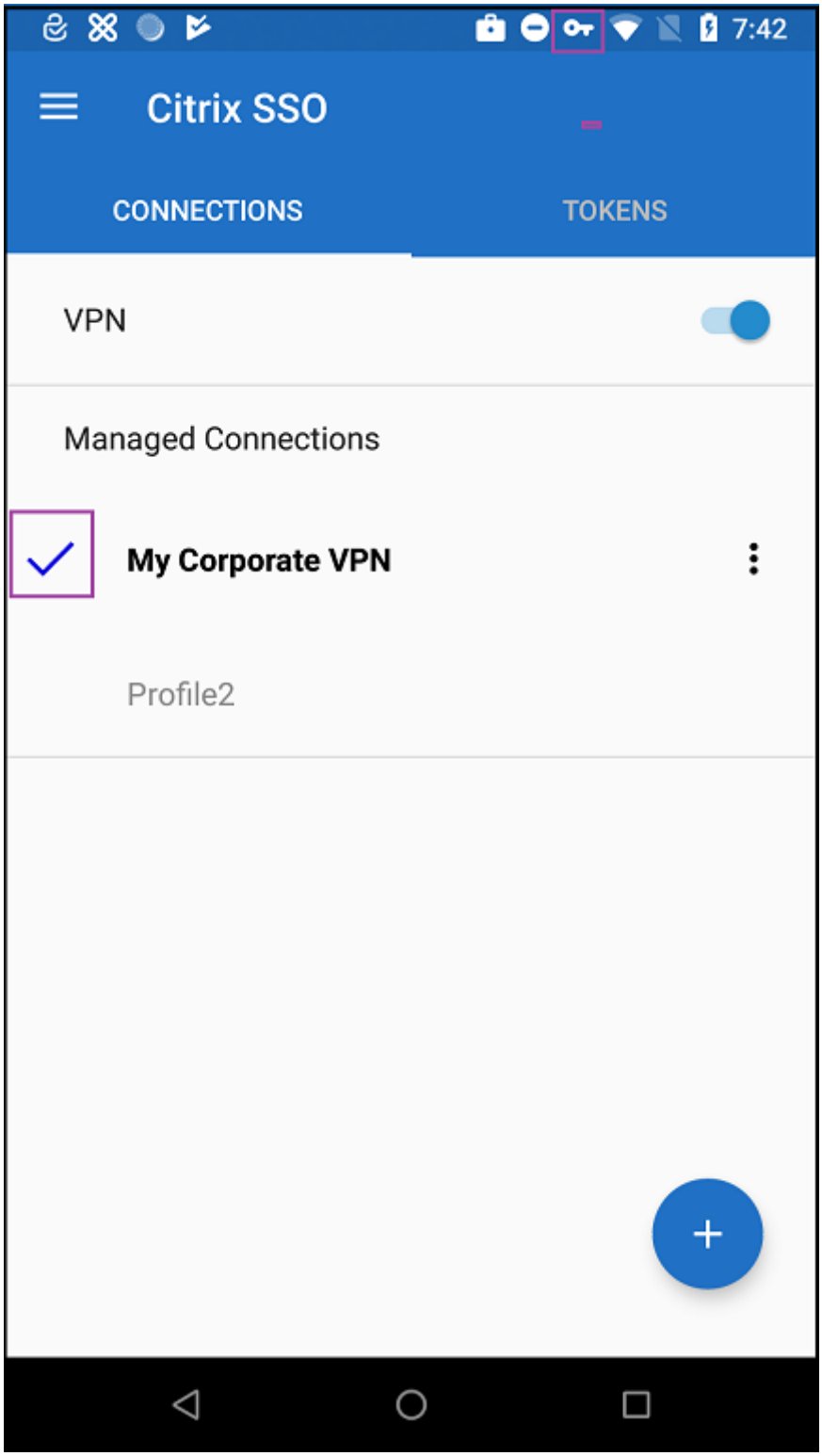
Accéder aux profils VPN à partir de l'appareil

Pour accéder aux profils VPN que vous avez créés, les utilisateurs Android Enterprise installent Citrix SSO à partir de Google Play Store.

Le ou les profils VPN que vous avez configurés apparaissent dans la zone **Connexions gérées** de l'application. Les utilisateurs touchent le profil VPN pour se connecter à l'aide de ce profil.



Une fois les utilisateurs authentifiés et connectés, une coche apparaît en regard du profil VPN. L'icône de clé indique que le VPN est connecté.



Gérer les appareils Zebra Android à l'aide de Zebra OEMConfig

Gérez les appareils Zebra Android à l'aide de l'outil d'administration OEMConfig de Zebra Technologies. Pour plus d'informations sur l'application Zebra OEMConfig, consultez le site Web Zebra Technologies.

XenMobile prend en charge Zebra OEMConfig version 9.2 et supérieure. Pour plus d'informations sur la configuration système requise pour installer Zebra OEMConfig sur les appareils, consultez Configuration d'OEMConfig sur le site Web de Zebra Technologies.

Commencez par ajouter l'application Zebra OEMConfig à la console XenMobile en tant qu'application Google Play Store. Consultez la section Ajouter une application de magasin public.

Créer une configuration gérée par Android Enterprise pour l'application Zebra OEMConfig

Configurez la stratégie Configurations gérées Android Enterprise pour l'application Zebra OEMConfig. La stratégie s'applique aux appareils Zebra sur lesquels l'application Zebra OEMConfig est installée et la stratégie est déployée.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. Cliquez sur **Ajouter**.
2. Sélectionnez **Android Enterprise**. Cliquez sur **Configurations gérées par Android Entreprise**.
3. Lorsque la fenêtre **Sélectionner l'ID d'application** apparaît, choisissez **ZebraOEMConfig powered by MX** dans la liste et cliquez sur **OK** .
4. Saisissez un nom et une description pour votre configuration Zebra OEMConfig. Cliquez sur **Suivant**.
5. Saisissez un nom pour la configuration de Zebra OEMConfig.
6. Configurez les paramètres disponibles. Par exemple :
    - Pour désactiver l'appareil photo situé à l'avant de l'appareil, sélectionnez **Camera Configuration** et définissez **Use of Front Camera** sur **Off**.
    - Pour modifier le format de l'heure des appareils, sélectionnez **Clock Configuration** et définissez **Time Format** sur **12** pour le format 12 heures ou **24** pour le format 24 heures.

Pour obtenir une liste et une description de toutes les configurations disponibles, consultez Zebra Managed Configurations sur le site Web de Zebra Technologies.

1. Vous pouvez également créer des configurations Zebra OEMConfig supplémentaires. Cliquez sur **Ajouter** dans la liste des configurations. Une nouvelle configuration apparaît dans la liste. Sélectionnez la nouvelle configuration et configurez les paramètres.
2. Lorsque vous avez créé toutes les configurations Zebra OEMConfig souhaitées, cliquez sur **Suivant**.

3. Configurez les règles de déploiement associées à cette configuration gérée pour Zebra OEMConfig.
4. Cliquez sur **Enregistrer**.

Autorisation de l'application Android Entreprise

January 10, 2022

Vous pouvez configurer la façon dont les demandes des applications Android Enterprise dans le cadre de profils de travail gèrent les autorisations qualifiées comme étant « dangereuses » par Google. Vous déterminez si les utilisateurs doivent autoriser ou refuser une demande d'autorisation à partir d'applications. Cette fonctionnalité est destinée aux appareils exécutant Android 7.0 et versions ultérieures.

Google définit les autorisations dangereuses comme des autorisations qui permettent à l'application d'accéder à des données ou des ressources impliquant des informations privées de l'utilisateur ou susceptibles d'affecter les données stockées de l'utilisateur ou le fonctionnement d'autres applications. Par exemple, la possibilité de lire les contacts de l'utilisateur est une autorisation dangereuse.

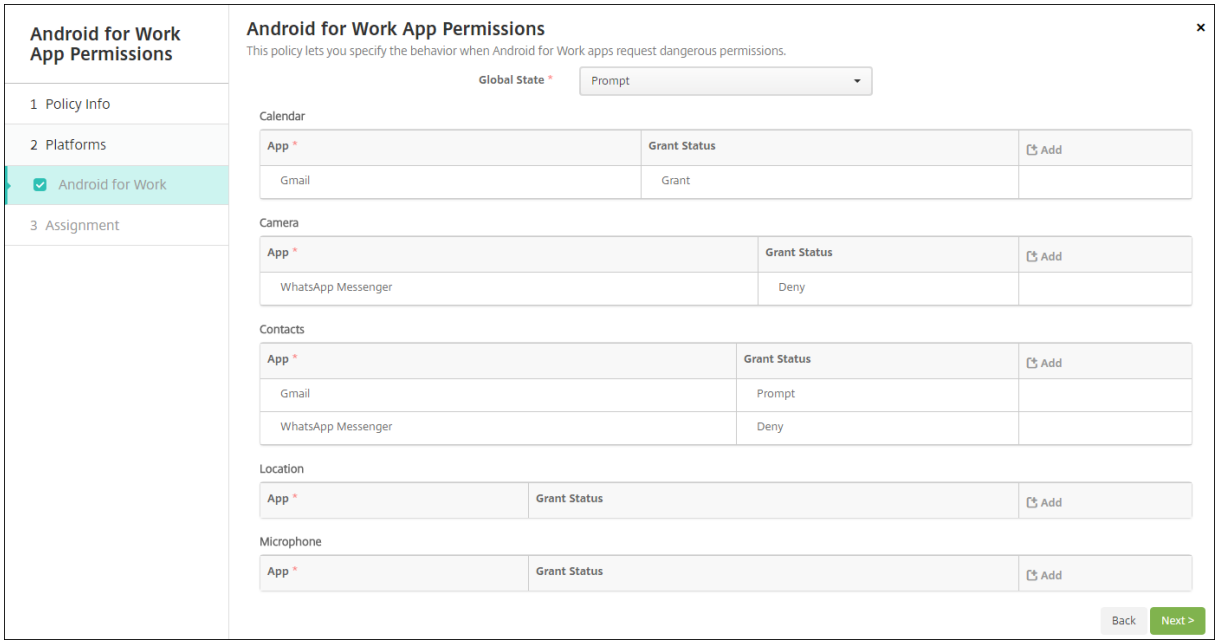
Vous pouvez configurer un état global qui contrôle le comportement de toutes les demandes d'autorisation dangereuses associées aux applications Android Enterprise dans le cadre de profils de travail. Vous pouvez également contrôler le comportement d'une demande d'autorisation dangereuse pour des groupes d'autorisations individuels, tels que définis par Google, associée à chaque application. Ces paramètres individuels remplacent l'état global.

Pour plus d'informations sur la définition des groupes d'autorisations par Google, consultez la section « Groupes d'autorisation » dans le guide des développeurs Android.

Par défaut, les utilisateurs sont invités à autoriser ou refuser les demandes d'autorisation dangereuses.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Android Enterprise



- **État global :** contrôle le comportement de toutes les demandes d'autorisation dangereuses. Dans la liste, cliquez sur **Inviter**, **Accorder** ou **Refuser**.
  - **Inviter :** les utilisateurs sont invités à autoriser ou refuser les demandes d'autorisation dangereuses.
  - **Accorder :** toutes les demandes d'autorisations dangereuses sont accordées. La confirmation de l'utilisateur n'est pas requise.
  - **Refuser :** toutes les demandes d'autorisations dangereuses sont refusées. La confirmation de l'utilisateur n'est pas requise.

  La valeur par défaut est **Inviter**.
- Définissez un comportement individuel pour chaque groupe d'autorisations, pour chaque application. Pour configurer le comportement d'un groupe d'autorisations, cliquez sur **Ajouter**, puis sous **Application**, choisissez une application dans la liste. Si vous configurez des applications système Android Enterprise, cliquez sur **Ajouter** et entrez le nom du package d'application que vous avez activé dans la stratégie Restrictions. Sous l'état de l'accès, choisissez **Inviter**, **Accorder** ou **Refuser**. L'état d'accès remplace l'état global.
  - **Inviter :** les utilisateurs sont invités à autoriser ou refuser les demandes d'autorisation dangereuses provenant de ce groupe d'autorisations pour cette application.
  - **Accorder :** les demandes d'autorisation dangereuses provenant de ce groupe d'autorisations pour cette application sont accordées. La confirmation de l'utilisateur n'est pas requise.
  - **Refuser :** les demandes d'autorisation dangereuses provenant de ce groupe d'autorisations pour cette application sont refusées. La confirmation de l'utilisateur n'est pas requise.

La valeur par défaut est **Inviter**.

- Cliquez sur **Enregistrer** en regard de l'application et l'état de l'accès
- Pour ajouter d'autres applications pour le groupe d'autorisations, cliquez à nouveau sur **Ajouter** et répétez ces étapes.
- Lorsque vous avez défini l'état de l'accès pour tous les groupes d'autorisations souhaités, cliquez sur **Suivant**.

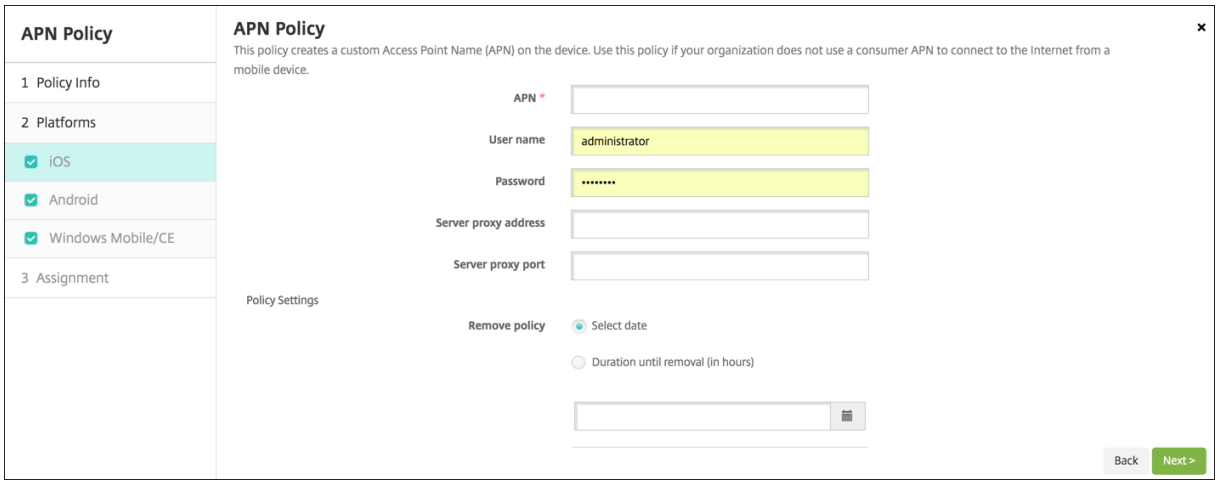
Stratégie APN

January 10, 2022

Vous pouvez ajouter une stratégie de nom de point d'accès (APN) personnalisée pour iOS, Android et Windows Mobile/CE. Vous pouvez utiliser cette stratégie si votre entreprise n'utilise pas d'APN consommateur pour se connecter à Internet à partir d'un appareil mobile. Une stratégie APN détermine les paramètres utilisés pour connecter vos appareils au service GPRS d'un opérateur de téléphonie spécifique. Ce paramètre est déjà défini dans la plupart des téléphones les plus récents.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

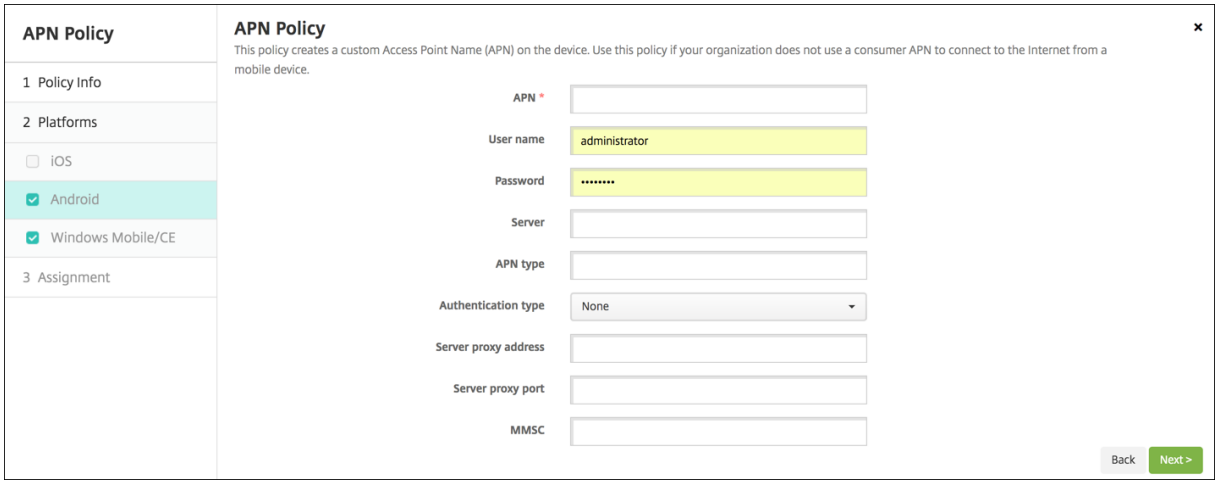
Paramètres iOS



- **APN :** entrez le nom du point d'accès. Ce dernier doit correspondre à un APN iOS accepté ou la stratégie échouera.
- **Nom d'utilisateur :** cette chaîne spécifie le nom d'utilisateur pour ce point d'accès. S'il est manquant, l'appareil invite à saisir la chaîne lors de l'installation du profil.

- **Mot de passe :** mot de passe utilisateur pour ce point d'accès. Afin de masquer le mot de passe, ce dernier est codé. S'il est manquant dans la charge utile, l'appareil vous invite à le saisir lors de l'installation du profil.
- **Adresse du serveur proxy :** adresse IP ou adresse URL du proxy APN.
- **Port du serveur proxy :** numéro de port du proxy APN. Nécessaire que si vous avez entré une adresse de serveur proxy.
- Sous **Paramètres de stratégie**, à côté de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en heures)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

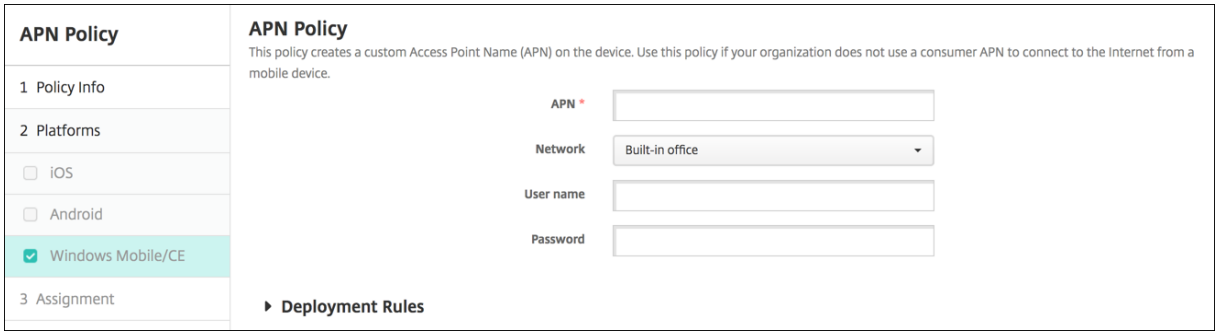
Paramètres Android



- **APN :** entrez le nom du point d'accès. Ce dernier doit correspondre à un APN Android accepté ou la stratégie échouera.

- **Nom d'utilisateur :** cette chaîne spécifie le nom d'utilisateur pour ce point d'accès. S'il est manquant, l'appareil invite à saisir la chaîne lors de l'installation du profil.
- **Mot de passe :** mot de passe utilisateur pour ce point d'accès. Afin de masquer le mot de passe, ce dernier est codé. S'il est manquant dans la charge utile, l'appareil vous invite à le saisir lors de l'installation du profil.
- **Serveur :** ce paramètre, antérieur à l'arrivée des smartphones, est généralement vide. Il fait référence à un serveur de passerelle WAP (Wireless Application Protocol) pour les téléphones qui ne pouvaient pas accéder ou restituer des sites Web standard.
- **Type d'APN :** ce paramètre doit s'aligner avec l'utilisation prévue par l'opérateur du point d'accès. Il s'agit d'une chaîne délimitée par des virgules des spécificateurs de service APN et doit correspondre aux définitions publiées de l'opérateur sans fil. Exemples :
  - *. Tout le trafic transite via ce point d'accès.
  - mms. Le trafic multimédia transite via ce point d'accès.
  - default. Tout le trafic, y compris le multimédia, transite via ce point d'accès.
  - supl. Le protocole SUPL est associé au GPS assisté.
  - dun. L'accès réseau à distance est obsolète et rarement utilisé.
  - hipri. Réseau haute priorité.
  - fota. FOTA (Firmware over the air) est utilisé pour recevoir les mises à jour du firmware.
- **Type d'authentification :** dans la liste, cliquez sur le type d'authentification à utiliser. Valeur par défaut Aucun.
- **Adresse du serveur proxy :** adresse IP ou adresse URL du proxy HTTP APN de l'opérateur.
- **Port du serveur proxy :** numéro de port du proxy APN. Nécessaire que si vous avez entré une adresse de serveur proxy.
- **MMSC :** adresse du serveur MMS fournie par l'opérateur.
- **Adresse du proxy MMS :** serveur du service de messagerie pour le trafic MMS. MMS a succédé à SMS pour l'envoi de messages plus volumineux avec du contenu multimédia, tels que des images ou des vidéos. Ces serveurs nécessitent des protocoles spécifiques (tels que MM1, … MM11).
- **Port MMS :** port utilisé par le proxy MMS.

Paramètres Windows Mobile/CE



- **APN :** entrez le nom du point d'accès. Ce dernier doit correspondre à un APN Android accepté ou la stratégie échouera.
- **Réseau :** dans la liste, cliquez sur le type de réseau à utiliser. La valeur par défaut est **Bureau intégré**.
- **Nom d'utilisateur :** cette chaîne spécifie le nom d'utilisateur pour ce point d'accès. S'il est manquant, l'appareil invite à saisir la chaîne lors de l'installation du profil.
- **Mot de passe :** mot de passe utilisateur pour ce point d'accès. Afin de masquer le mot de passe, ce dernier est codé. S'il est manquant dans la charge utile, l'appareil vous invite à le saisir lors de l'installation du profil.

Stratégie d'accès aux applications

January 15, 2020

La stratégie d'accès aux applications dans XenMobile vous permet de définir une liste d'applications dont l'installation sur les appareils est obligatoire, facultative ou interdite. Vous pouvez ensuite créer une action automatisée dont la tâche consiste à vérifier la conformité de l'appareil par rapport à cette liste d'applications. Vous pouvez créer des stratégies d'accès aux applications pour iOS, Android et Windows Mobile/CE.

Vous ne pouvez configurer qu'un type de stratégie d'accès à la fois. Vous pouvez ajouter une stratégie pour une liste d'applications obligatoires, d'applications suggérées ou d'applications interdites, mais vous ne pouvez pas combiner ces trois types de liste au sein de la même stratégie d'accès. Si vous créez une stratégie pour chaque type de liste, il est conseillé de nommer chaque stratégie avec soin, afin de pouvoir déterminer à quelle stratégie la liste des applications s'applique dans XenMobile.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres de plate-forme

- **Stratégie d'accès :** cliquez sur **Requise**, **Suggérée** ou **Interdite**. La valeur par défaut est **Requise**.
- Pour ajouter une ou plusieurs applications à la liste, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom app :** entrez un nom pour l'application.
  - **Identifiant app :** entrez un identifiant pour l'application (facultatif).
  - Cliquez sur **Enregistrer** ou **Annuler**.
  - Répétez ces étapes pour chaque application à ajouter.

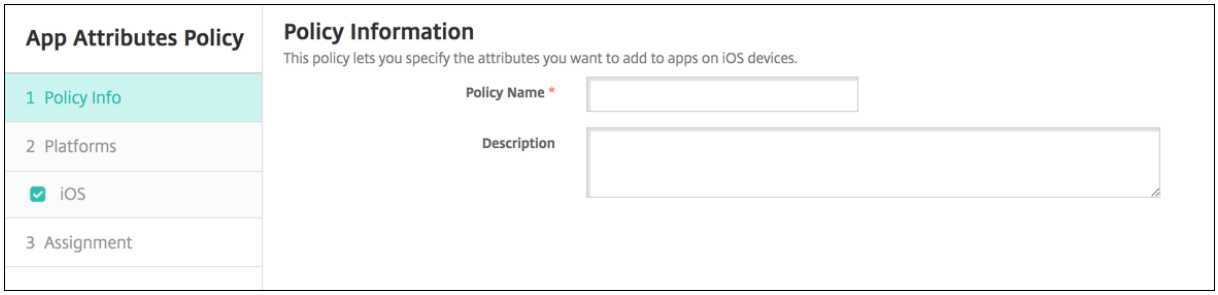
Stratégie d'attributs d'application

August 20, 2019

La stratégie Attributs d'application vous permet de spécifier des attributs, tels qu'un Bundle ID d'application gérée, ou un identifiant VPN par application pour les appareils iOS.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Bundle ID d'application gérée :** dans la liste, cliquez sur un bundle ID d'application ou cliquez sur **Ajouter**.
  - Si vous cliquez sur **Ajouter**, entrez le bundle ID d'application dans le champ qui s'affiche.
- **Identifiant Per App VPN :** dans la liste, cliquez sur l'identifiant Per App VPN.

Stratégie de configuration d'application

January 10, 2022

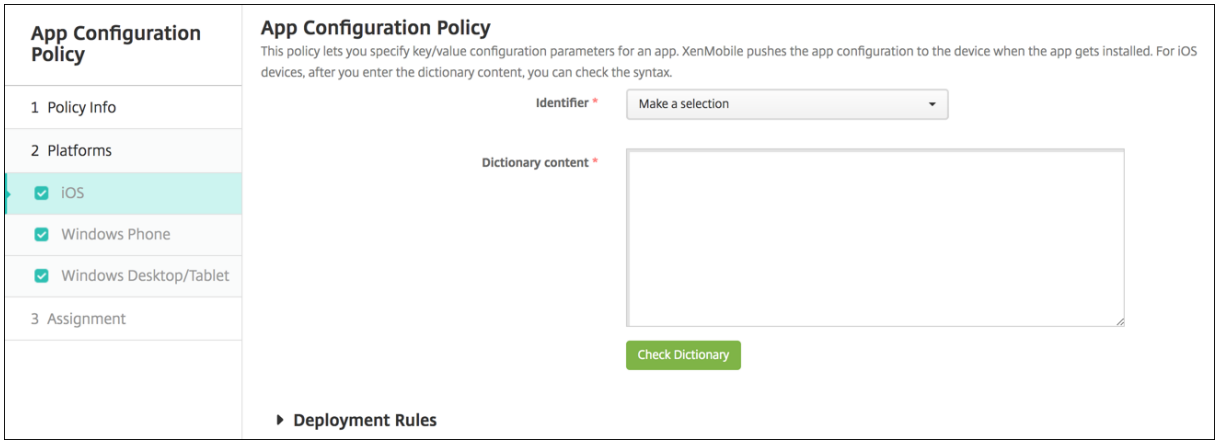
Vous pouvez configurer à distance des applications prenant en charge la configuration gérée en déployant :

- un fichier de configuration XML (appelé une liste des propriétés, ou plist) sur des appareils iOS
- Ou des paires clé/valeur pour les téléphones, tablettes ou ordinateurs de bureau Windows 10 exécutant Windows 10 ou Windows 11

La configuration spécifie différents paramètres et comportements dans l'application. XenMobile transmet la configuration aux appareils lorsque l'utilisateur installe l'application. Les paramètres et les comportements que vous pouvez configurer dépendent de l'application et ne sont pas couverts dans cet article.

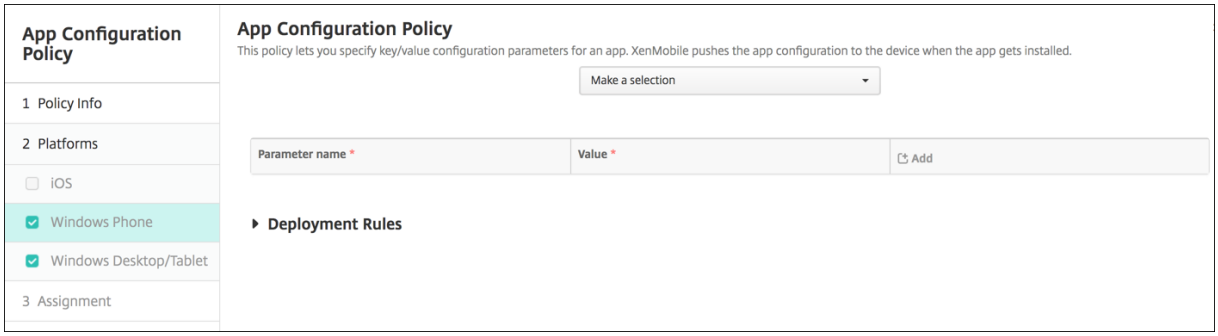
Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

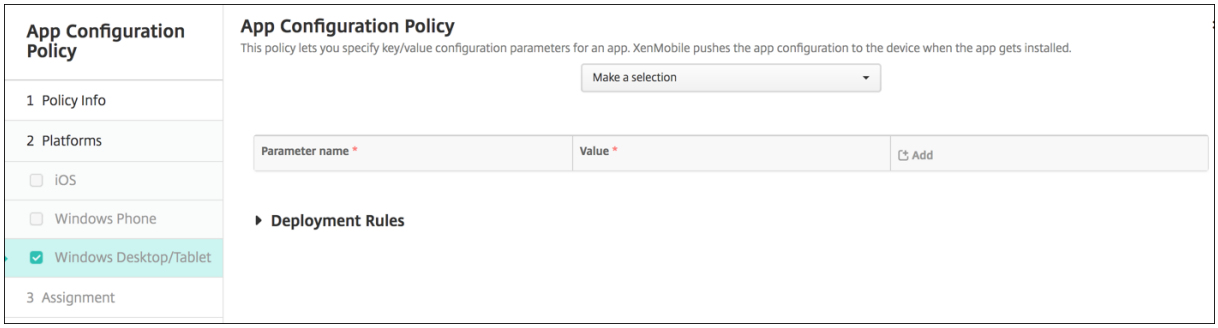
Paramètres iOS



- **Identifiant :** dans la liste, cliquez sur l'application que vous souhaitez configurer, ou cliquez sur **Ajouter** pour ajouter une application à la liste.
  - Si vous cliquez sur **Ajouter**, entrez l'identifiant de l'application dans le champ qui s'affiche.
- **Contenu du dictionnaire :** entrez, ou copiez et collez, les informations de configuration de la liste des propriétés XML (plist).
- Cliquez sur **Vérifier le dictionnaire**. XenMobile vérifie le XML. S'il n'existe aucune erreur, veuillez consulter la section **XML valide** en dessous de la zone de contenu. Si des erreurs de syntaxe s'affichent en dessous de la zone de contenu, vous devez les corriger pour continuer.

Paramètres pour Windows Phone ou Desktop/Tablet





- Dans la liste **Effectuer une sélection**, cliquez sur l'application que vous souhaitez configurer,

ou cliquez sur **Ajouter**pour ajouter une application à la liste.
  - Si vous cliquez sur **Ajouter**, entrez le nom du package dans le champ qui s'affiche.
- Pour chaque paramètre de configuration que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom du paramètre :** entrez le nom de clé d'un paramètre d'application pour le périphérique Windows. Pour de plus amples informations sur les paramètres des applications Windows, reportez-vous à la documentation Microsoft.
  - **Valeur :** entrez la valeur pour ce paramètre.
  - Cliquez sur **Ajouter** pour ajouter le paramètre, ou cliquez sur **Annuler** pour annuler l'ajout du paramètre.

Stratégie d'inventaire des applications

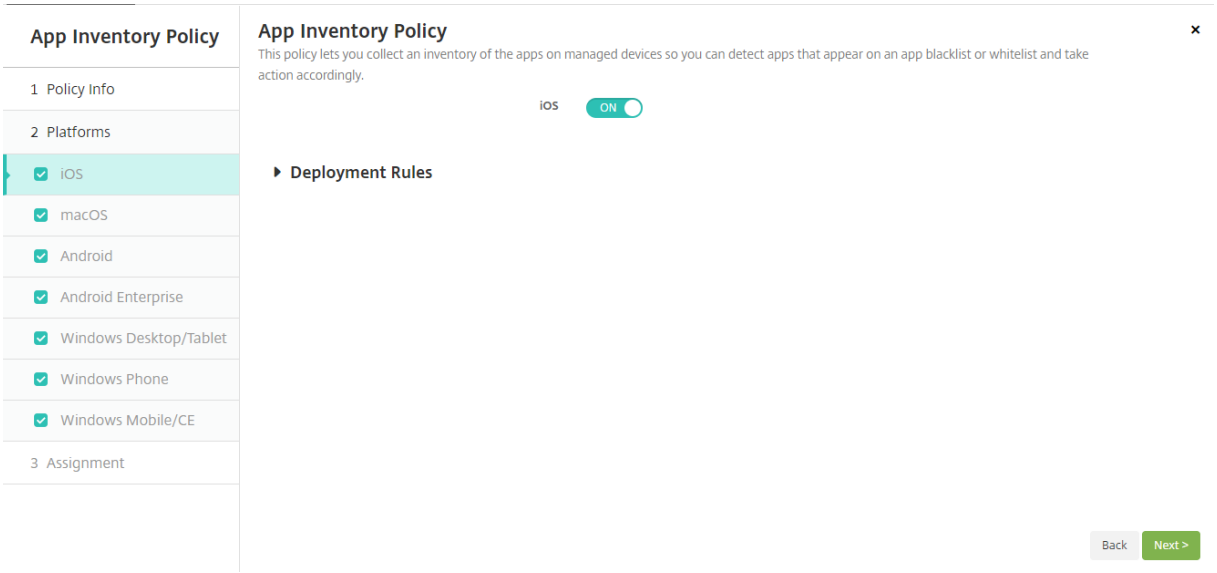
January 10, 2022

La stratégie Inventaire des applications vous permet d'établir un inventaire des applications sur les appareils gérés. XenMobile peut ensuite comparer l'inventaire avec les stratégies d'accès aux applications déployées sur ces appareils. Vous pouvez ainsi détecter les applications figurant sur une liste d'autorisation ou de blocage et prendre les mesures qui s'imposent.

Vous pouvez créer des stratégies d'accès aux applications pour les appareils iOS, macOS, Android, Android Enterprise, Windows Desktop/Tablet, Windows Phone ou Windows Mobile/CE.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres de plate-forme



- Pour chaque plate-forme que vous sélectionnez, conservez le paramètre par défaut ou modifiez le paramètre (**Désactivé**). La valeur par défaut est **Activé**.

Stratégie de mode kiosque

January 10, 2022

La stratégie de mode kiosque permet de définir une liste d'applications dont l'exécution est autorisée ou interdite sur un appareil. Vous pouvez configurer cette stratégie pour les appareils iOS et Android, mais la manière dont la stratégie fonctionne diffère pour chaque plate-forme. Par exemple, vous pouvez bloquer plusieurs applications sur un appareil iOS.

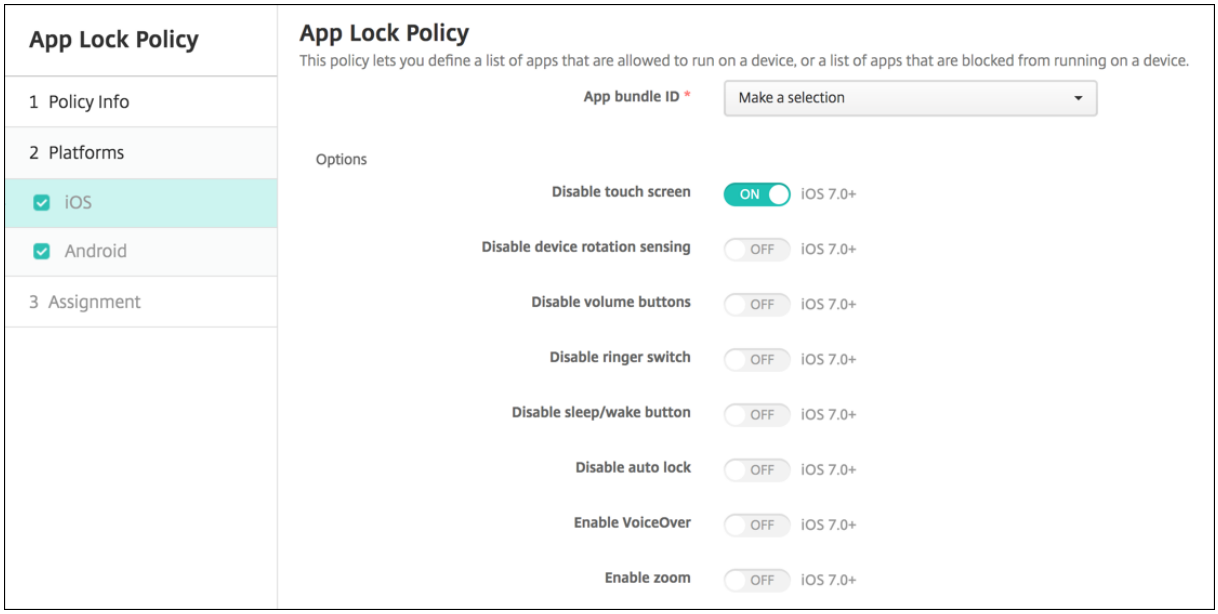
De même, pour les appareils iOS, vous pouvez sélectionner une seule application iOS par stratégie. Cela signifie que les utilisateurs peuvent uniquement utiliser leurs appareils pour exécuter une seule application. Ils ne peuvent effectuer aucune autre activité sur l'appareil, à l'exception des options que vous avez spécifiquement autorisées lorsque la stratégie de mode kiosque est appliquée.

En outre, les appareils iOS doivent être supervisés pour pouvoir transmettre des stratégies de verrouillage d'applications.

Bien que la stratégie d'appareil fonctionne sur la plupart des appareils Android L et M, le verrouillage d'applications ne fonctionne pas sur les appareils Android N ou plus récents en raison de l'abandon par Google de l'API requise.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Bundle ID d'application :** dans la liste, cliquez sur l'application à laquelle cette stratégie s'applique, ou cliquez sur **Ajouter** pour ajouter une application à la liste. Si vous sélectionnez **Ajouter**, entrez le nom de l'application dans le champ qui s'affiche.
- **Options :** chacune des options suivantes s'applique uniquement à iOS 7.0 ou version ultérieure. Pour chaque option, la valeur par défaut est **Désactivé**, sauf pour Désactiver l'écran tactile, qui est réglée par défaut sur **Activé**.
  - Désactiver l'écran tactile
  - Désactiver détection de rotation
  - Désactiver boutons volume
  - Désactiver bouton sonnerie

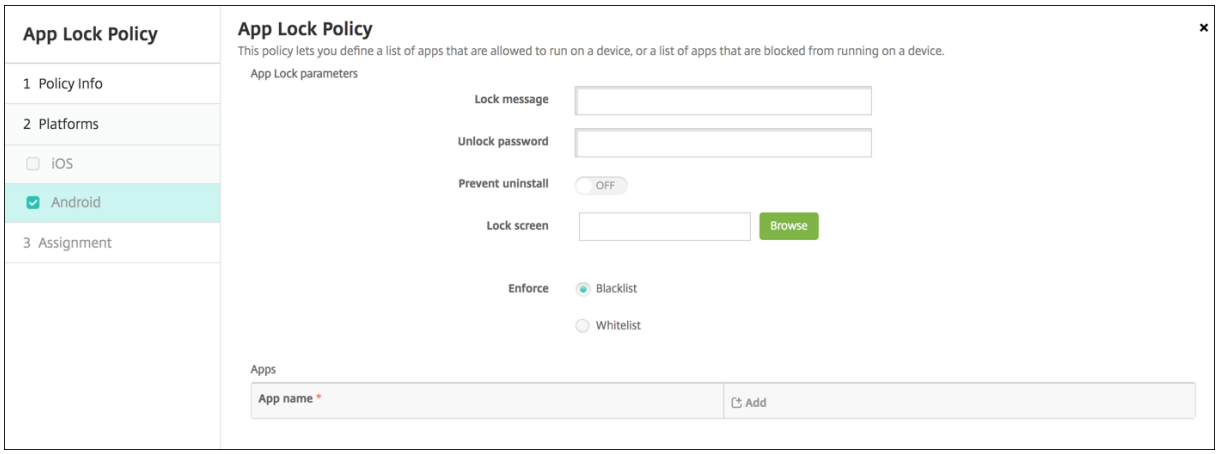
    Lorsque l'option Désactiver bouton sonnerie est définie sur **Activé**, le comportement de la sonnerie dépend de la position dans laquelle se trouvait le bouton lorsqu'il a été désactivé.
  - Désactiver le bouton veille
  - Désactiver verrouillage auto
  - Désactiver VoiceOver
  - Activer zoom
  - Activer l'inversion de couleurs
  - Activer AssistiveTouch
  - Activer Énoncer la sélection
  - Activer l'audio mono
- **Options utilisateur :** chacune des options suivantes s'applique uniquement à iOS 7.0 ou version ultérieure. Pour chaque option, la valeur par défaut est **Désactivé**.
  - Autoriser le réglage de VoiceOver
  - Autoriser le réglage du zoom

- Autoriser le réglage d'inversion des couleurs
- Autoriser le réglage AssistiveTouch

- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres Android

> **Remarque :**
>
> Vous ne pouvez pas bloquer l'application Paramètres Android à l'aide de la stratégie Mode kiosque.



- **Paramètres du mode kiosque**
  - **Message de verrouillage :** entrez un message que les utilisateurs voient lorsqu'ils tentent d'ouvrir une application en mode kiosque.
  - **Mot de passe de déblocage :** entrez le mot de passe pour déverrouiller l'application.
  - **Empêcher la désinstallation :** indiquez si les utilisateurs sont autorisés à désinstaller les applications. La valeur par défaut est **Désactivé**.
  - **Écran de verrouillage** : sélectionnez l'image qui s'affiche sur l'écran de verrouillage de l'appareil en cliquant sur Parcourir et en accédant à l'emplacement du fichier.
  - **Appliquer :** cliquez sur **Liste noire** pour créer une liste d'applications qui ne sont pas autorisées à s'exécuter sur les appareils ou cliquez sur **Liste blanche** pour créer une liste d'applications qui sont autorisées à s'exécuter sur les appareils.

> **Remarque :**
> La console XenMobile Server utilise les termes « liste noire » et « liste blanche ». Ces termes seront modifiés dans une prochaine version et les termes « liste de blocage » et « liste d'autorisation » les remplaceront.

- **Applications :** cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom de l'application :** dans la liste, cliquez sur le nom de l'application à ajouter à la liste d'autorisation ou à la liste de blocage ou cliquez sur **Ajouter** pour ajouter une application à la liste des applications disponibles.
  - Si vous sélectionnez **Ajouter**, entrez le nom de l'application dans le champ qui s'affiche.
  - Cliquez sur **Enregistrer** ou **Annuler**.
  - Répétez ces étapes pour chaque application que vous souhaitez ajouter aux listes d'autorisation ou de blocage.

Stratégie d'utilisation des réseaux

January 10, 2022

Vous pouvez définir des règles d'utilisation du réseau pour spécifier la manière dont les applications gérées utilisent les réseaux, tels que les réseaux de données cellulaires, sur les appareils iOS. Les règles s'appliquent uniquement aux applications gérées. Les applications gérées sont celles que vous déployez sur les appareils des utilisateurs via XenMobile. Elles n'incluent pas les applications que les utilisateurs ont téléchargées directement sur leurs appareils sans qu'elles soient déployées via XenMobile ou celles déjà installées sur les appareils lorsqu'ils ont été inscrits dans XenMobile.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Autoriser les données cellulaires en itinérance :** indiquez si les applications spécifiées peuvent utiliser une connexion de données cellulaires en itinérance. La valeur par défaut est **Désactivé**.
- **Autoriser les données cellulaires :** indiquez si les applications spécifiées peuvent utiliser une connexion de données cellulaires. La valeur par défaut est **Désactivé**.
- **Correspondances de l'identifiant d'application :** pour chaque application que vous souhaitez ajouter à la liste, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Identifiant app :** entrez un identifiant pour l'application.
  - Cliquez sur **Enregistrer** pour enregistrer l'application dans la liste ou sur **Annuler** pour ne pas l'enregistrer dans la liste.

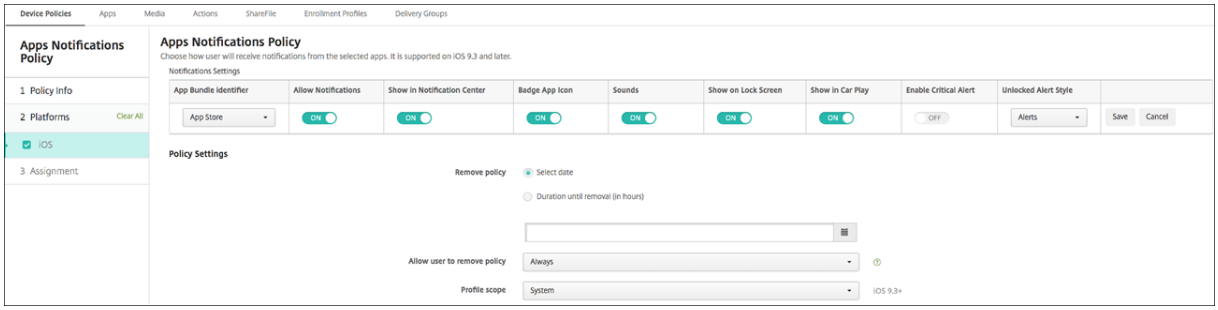
Stratégie Notifications d'applications

January 10, 2022

La stratégie Notifications d'applications vous permet de contrôler la manière dont les utilisateurs iOS recevront les notifications depuis certaines applications. Cette stratégie est prise en charge sur les appareils exécutant iOS 9.3 ou version ultérieure.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Bundle ID d'application :** spécifiez les applications auxquelles vous souhaitez appliquer cette stratégie.
- **Autoriser les notifications :** sélectionnez **Activé** pour autoriser les notifications.
- **Afficher dans le Centre de notifications :** sélectionnez **Activé** pour afficher les notifications dans le Centre de notifications des appareils utilisateur.
- **Pastille sur l'icône d'app :** sélectionnez **Activé** pour afficher une pastille sur l'icône d'application avec les notifications.
- **Sons :** sélectionnez **Activé** pour inclure des sons avec les notifications.
- **Afficher sur l'écran de verrouillage :** sélectionnez **Activé** pour afficher les notifications sur l'écran de verrouillage des appareils utilisateur.
- **Afficher dans CarPlay :** sélectionnez **Activé** pour afficher les notifications dans Apple CarPlay. Disponible dans iOS 12 et versions ultérieures. La valeur par défaut est **Activé**.
- **Activer alerte critique :** sélectionnez **Activé** pour autoriser une application à marquer une notification comme critique qui ignore les paramètres Ne pas déranger et Sonnerie. Disponible dans iOS 12 et versions ultérieures. La valeur par défaut est **Désactivé**.
- **Style d'alerte si déverrouillé :** dans la liste, sélectionnez **Aucune**, **Bannière** ou **Alertes** pour configurer l'apparence des alertes déverrouillées.

- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur iOS 9.3 et versions ultérieures.

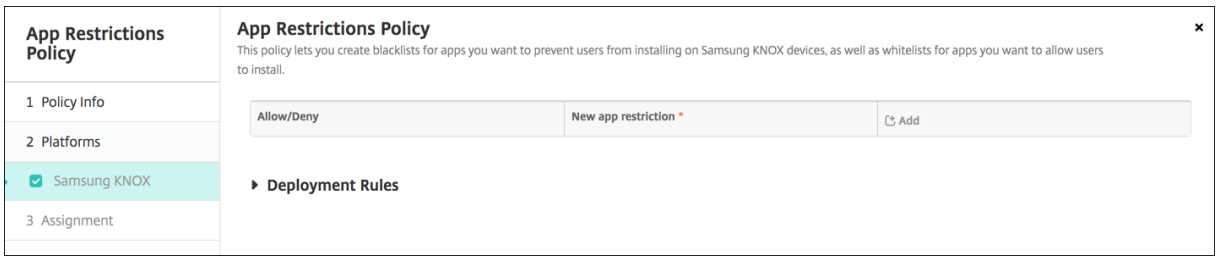
Stratégie de restriction d'application

January 10, 2022

Vous pouvez créer des listes de blocage pour les d'applications que vous ne souhaitez pas que les utilisateurs installent sur des appareils Samsung KNOX. Vous pouvez également créer des listes d'autorisation pour les applications que vous souhaitez autoriser les utilisateurs à installer.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Samsung KNOX



Pour chaque application que vous souhaitez ajouter à la liste Autoriser/refuser, cliquez sur **Ajouter**, puis procédez comme suit :

- **Autoriser/refuser :** indiquez si les utilisateurs sont autorisés à installer l'application.
- **Nouvelle restriction applicative :** entrez l'ID du paquetage de l'application ; par exemple, com.kmdm.af.crackle.
- Cliquez sur **Enregistrer** pour enregistrer l'application dans la liste Autoriser/refuser ou sur **Annuler** pour ne pas l'enregistrer dans la liste.

Stratégie de tunnel applicatif

January 10, 2022

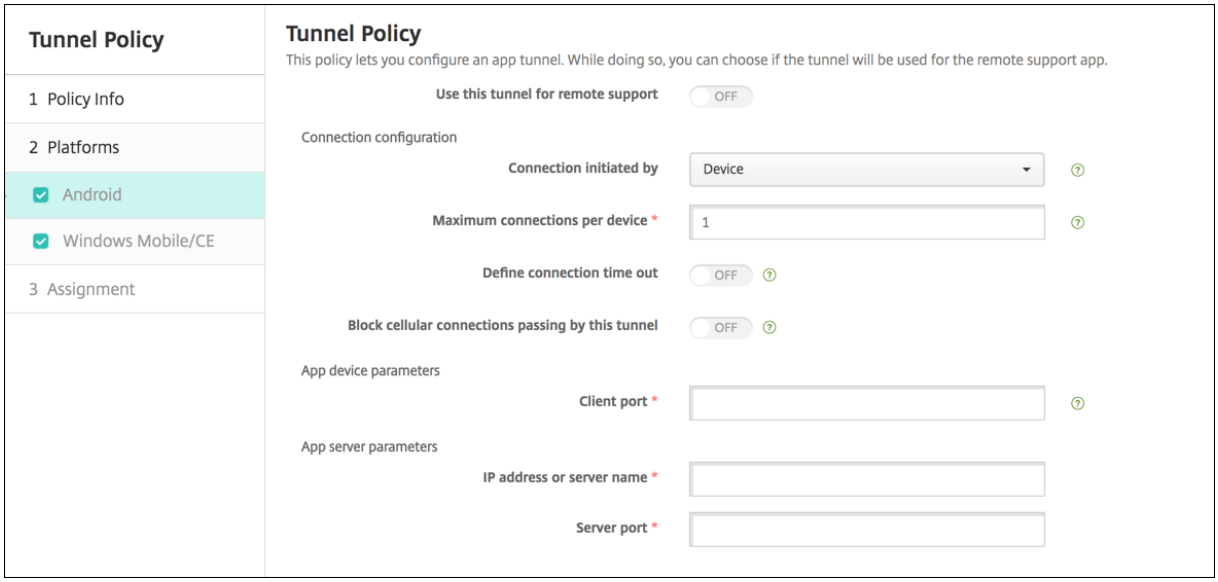
> **Important :**
>
> La stratégie de tunnel applicatif est utilisée uniquement pour l'assistance à distance. Pour plus d'informations sur l'assistance à distance, consultez la section Options d'assistance et assistance à distance. L'Assistance à distance n'est plus disponible pour les nouveaux clients à compter du 1er janvier 2019. Les clients existants peuvent continuer à utiliser le produit, mais Citrix ne fournira pas d'améliorations ou de correctifs.

Les tunnels applicatifs sont conçus pour accroître la continuité du service et la fiabilité du transfert de données pour vos applications mobiles. Les tunnels applicatifs définissent les paramètres proxy entre le composant client de toute application d'appareil mobile et le composant de serveur d'applications. Vous pouvez également utiliser des tunnels applicatifs pour créer des tunnels d'assistance à distance pour la gestion du support. Vous pouvez configurer la stratégie de tunnel applicatif pour les appareils Android et Windows Mobile/CE.

Tout trafic applicatif envoyé via un tunnel que vous définissez dans cette stratégie transite via XenMobile avant d'être redirigé vers le serveur exécutant l'application.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Android



- **Utiliser ce tunnel pour l'assistance à distance :** spécifiez si le tunnel est utilisé pour

l'assistance à distance.

Les étapes de configuration diffèrent selon que l'assistance à distance est sélectionnée ou non.

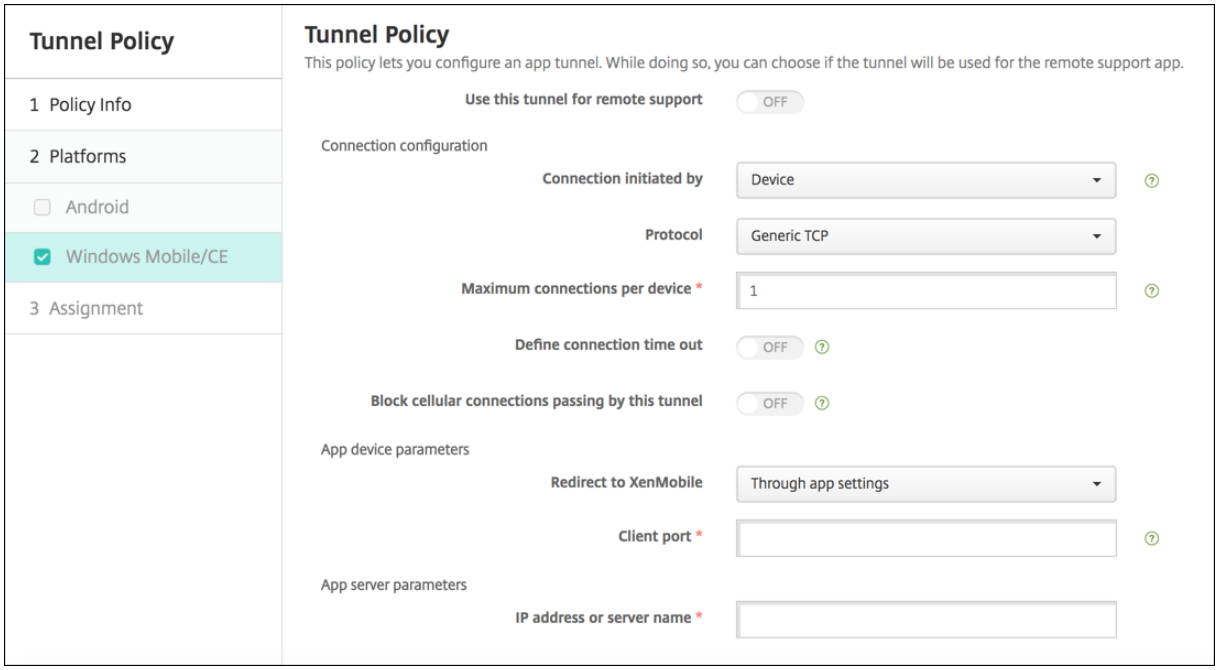
- Si vous ne sélectionnez pas l'assistance à distance, procédez comme suit :
  - **Connexion initiée par :** cliquez sur **Appareil** ou **Serveur** pour spécifier la source lançant la connexion.
  - **Connexions max. par appareil :** tapez un nombre pour définir le nombre de connexions TCP simultanées que l'application peut établir. Ce champ ne s'applique qu'aux connexions initiées par l'appareil.
  - **Définir le délai d'expiration de la connexion :** sélectionnez cette option pour définir une durée pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
    - **Délai d'expiration de la connexion :** si vous définissez **Définir le délai d'expiration de la connexion** sur **Activé**, saisissez la durée en secondes pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
  - **Bloquer les connexions cellulaires transitant par ce tunnel :** sélectionnez cette option pour spécifier si ce tunnel est bloqué en itinérance.

    > **Remarque :**
    >
    > Les connexions Wi-Fi et USB ne sont pas bloquées.

  - **Port client :** entrez le numéro du port du client. Dans la plupart des cas, cette valeur est la même que celle du port serveur.
  - **Adresse IP ou nom du serveur :** entrez l'adresse IP ou le nom du serveur applicatif. Ce champ ne s'applique qu'aux connexions initiées par l'appareil.
  - **Port serveur :** entrez le numéro de port du serveur.
- Si vous sélectionnez l'assistance à distance, procédez comme suit :
  - **Utiliser ce tunnel pour l'assistance à distance :** définissez cette option sur **Activé**.
  - **Définir le délai d'expiration de la connexion :** sélectionnez cette option pour définir une durée pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
    - **Délai d'expiration de la connexion :** si vous définissez **Définir le délai d'expiration de la connexion** sur **Activé**, saisissez la durée en secondes pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
  - **Utiliser une connexion SSL :** indiquez si vous souhaitez utiliser une connexion SSL sécurisée pour ce tunnel.

- **Bloquer les connexions cellulaires transitant par ce tunnel :** sélectionnez cette option pour spécifier si ce tunnel est bloqué en itinérance. Ce paramètre ne bloque pas les connexions WiFi et USB.

Paramètres Windows Mobile/CE



- **Utiliser ce tunnel pour l'assistance à distance :** spécifiez si le tunnel est utilisé pour l'assistance à distance.

Les étapes de configuration diffèrent selon que l'assistance à distance est sélectionnée ou non.

- Si vous ne sélectionnez pas l'assistance à distance, procédez comme suit :
  - **Connexion initiée par :** cliquez sur **Appareil** ou **Serveur** pour spécifier la source lançant la connexion.
  - **Protocole :** dans la liste, cliquez sur le protocole à utiliser. La valeur par défaut est **TCP générique**.
  - **Connexions max. par appareil :** tapez un nombre pour définir le nombre de connexions TCP simultanées que l'application peut établir. Ce champ ne s'applique qu'aux connexions initiées par l'appareil.
  - **Définir le délai d'expiration de la connexion :** sélectionnez cette option pour définir une durée pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
    - **Délai d'expiration de la connexion :** si vous définissez **Définir le délai d'expiration de la connexion** sur **Activé**, saisissez la durée en secondes pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.

- **Bloquer les connexions cellulaires transitant par ce tunnel :** sélectionnez cette option pour spécifier si ce tunnel est bloqué en itinérance.

  > **Remarque :**
  > Les connexions Wi-Fi et USB ne sont pas bloquées.

- **Rediriger vers XenMobile :** dans la liste, cliquez sur la manière dont l'appareil se connecte à XenMobile. La valeur par défaut est **Via les paramètres de l'application**.
  - Si vous sélectionnez **Via un alias local**, tapez l'alias dans **Alias local**. La valeur par défaut est **localhost**.
  - Si vous sélectionnez **Via une plage d'adresses IP**, entrez le début de la plage d'adresses IP dans **Plage d'adresses IP : de** et entrez l'adresse IP de fin dans **Plage d'adresses IP : à**.
- **Port client :** entrez le numéro du port du client. Dans la plupart des cas, cette valeur est la même que celle du port serveur.
- **Adresse IP ou nom du serveur :** entrez l'adresse IP ou le nom du serveur applicatif. Ce champ ne s'applique qu'aux connexions initiées par l'appareil.
- **Port serveur :** entrez le numéro de port du serveur.

• Si vous sélectionnez l'assistance à distance, procédez comme suit :
- **Utiliser ce tunnel pour l'assistance à distance :** définissez cette option sur **Activé**.
- **Définir le délai d'expiration de la connexion :** sélectionnez cette option pour définir une durée pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
  - **Délai d'expiration de la connexion :** si vous définissez **Définir le délai d'expiration de la connexion** sur **Activé**, saisissez la durée en secondes pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
- **Utiliser une connexion SSL :** indiquez si vous souhaitez utiliser une connexion SSL sécurisée pour ce tunnel.
- **Bloquer les connexions cellulaires transitant par ce tunnel :** sélectionnez cette option pour spécifier si ce tunnel est bloqué en itinérance. Les connexions Wi-Fi et USB ne sont pas bloquées.

Stratégie de désinstallation des applications

January 10, 2022

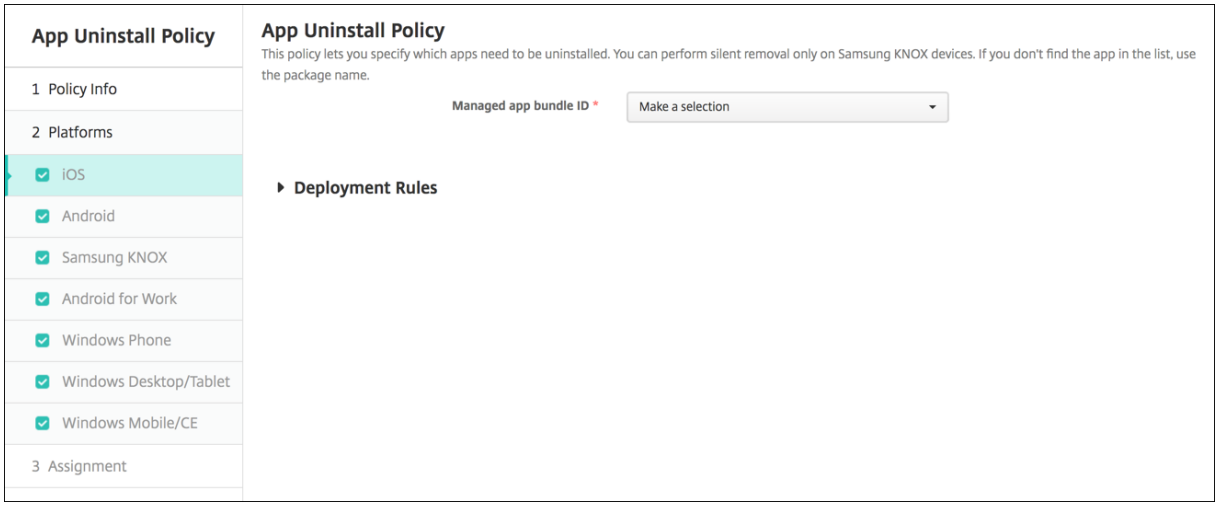
Vous pouvez créer une stratégie de désinstallation d'application pour les plates-formes iOS, Android, Samsung KNOX, Android Enterprise, Windows Desktop/Tablet et Windows Mobile/CE. Une stratégie de désinstallation d'application vous permet de supprimer des applications des appareils utilisateur pour un certain nombre de raisons. Il se peut que vous ne souhaitiez plus prendre en charge certaines applications et que votre entreprise désire remplacer des applications par d'autres similaires mais

provenant d'autres fournisseurs, etc.

Les applications sont supprimées lorsque cette stratégie est déployée sur les appareils des utilisateurs. À l'exception des appareils Samsung KNOX, les utilisateurs reçoivent une invitation à désinstaller l'application ; les utilisateurs d'appareils Samsung KNOX ne reçoivent pas d'invitation à désinstaller l'application.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Bundle ID d'application gérée :** dans la liste, cliquez sur une application existante ou cliquez sur **Ajouter**. s'il n'existe aucune application configurée pour cette plate-forme, la liste est vide et vous devez ajouter une nouvelle application.
  - Lorsque vous cliquez sur **Ajouter** un champ apparaît dans lequel vous pouvez entrer un nom pour l'application.

Tous les autres paramètres de plate-forme

- **Applications à désinstaller :** pour chaque application que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom app :** dans la liste, cliquez sur une application existante ou sur **Ajouter** pour entrer un nouveau nom d'application. s'il n'existe pas d'applications configurées pour cette plate-forme, la liste est vide et vous devez ajouter de nouvelles applications.
  - Cliquez sur **Ajouter** pour ajouter l'application, ou cliquez sur **Annuler** pour annuler l'ajout de l'application.

Désinstaller automatiquement une application d'entreprise une fois que l'application de magasin public correspondante est installée

Vous pouvez configurer XenMobile pour supprimer la version d'entreprise des applications Citrix lors de l'installation de la version de magasin d'applications public. Cette fonctionnalité empêche les appareils utilisateur d'avoir deux icônes d'application identiques après l'installation de la version de magasin d'applications public.

Une condition de déploiement pour la stratégie de désinstallation d'application déclenche la suppression par XenMobile des anciennes applications depuis les appareils utilisateur lors de l'installation de la nouvelle version. Cette fonctionnalité est uniquement disponible pour les appareils iOS gérés connectés à un serveur XenMobile en mode d'entreprise (XME).

Pour configurer une règle de déploiement avec la condition Nom de l'application installée :

- Spécifiez le **Bundle ID d'application gérée** pour l'application d'entreprise.
- Ajouter une règle : cliquez sur **Nouvelle règle**, puis, comme illustré dans l'exemple, choisissez **Nom de l'application installée** et **est égal à**. Entrez le bundle ID d'application pour l'application du magasin d'applications public.

Dans l'exemple, lors de l'installation de l'application de magasin d'applications public (com.citrix.mail.ios) sur un appareil dans les groupes de mise à disposition spécifiés, XenMobile supprime la version d'entreprise (com.citrix.mail).

Stratégie de restriction de désinstallation d'applications

January 10, 2022

Vous pouvez spécifier les applications que les utilisateurs peuvent ou ne peuvent pas désinstaller sur un appareil Samsung SAFE ou Amazon.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Samsung SAFE ou Amazon

- **Paramètres de restriction de désinstallation d'application :** pour chaque règle d'application que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom de l'application :** dans la liste, cliquez sur une application ou sur **Ajouter** pour ajouter une nouvelle application.
  - **Règle :** indiquez si les utilisateurs peuvent désinstaller l'application. Par défaut, la désinstallation est autorisée.

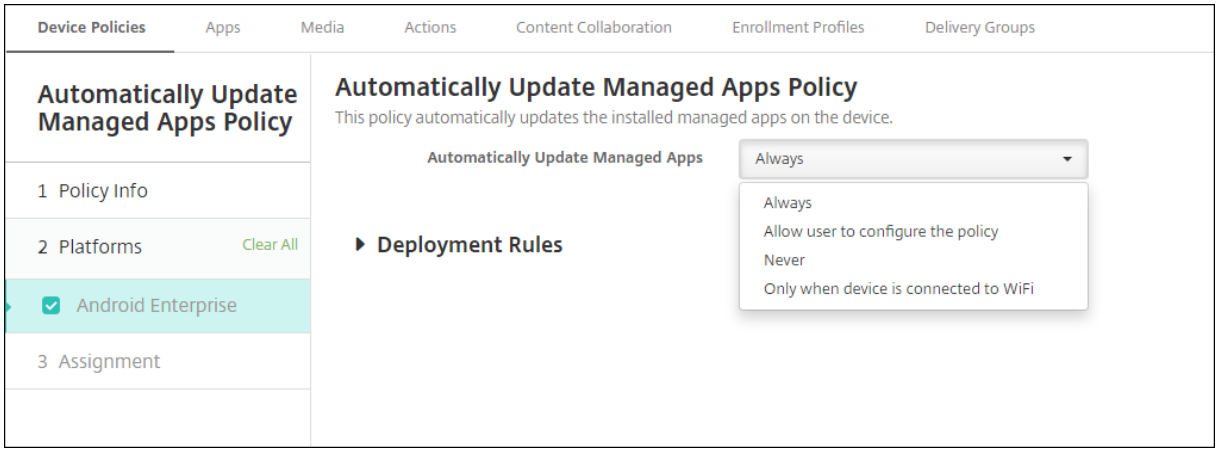
- Cliquez sur **Enregistrer** ou **Annuler**.

Stratégie de mise à jour automatique des applications gérées

January 10, 2022

Cette stratégie contrôle la façon dont les applications gérées installées sont mises à jour sur les appareils Android Enterprise. Vous pouvez limiter la capacité des utilisateurs à autoriser les mises à jour automatiques des applications sur leurs appareils. Si vous autorisez les utilisateurs à contrôler les mises à jour automatiques des applications sur leurs appareils, ils définissent des stratégies de mise à jour automatique des applications dans le Google Play Store d'entreprise.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.



Définissez **Mise à jour automatique des applications gérées**.

- **Toujours** : permet d'activer les mises à jour automatiques des applications. **Toujours** est la valeur par défaut.
- **Autoriser l'utilisateur à configurer la stratégie** : permet à l'utilisateur de configurer la stratégie de mise à jour automatique des applications pour l'appareil dans le Google Play Store d'entreprise.
- **Jamais** : permet de désactiver les mises à jour automatiques des applications.
- **Uniquement lorsque l'appareil est connecté au Wi-Fi** : permet d'autoriser les mises à jour automatiques des applications uniquement lorsque l'appareil est connecté au Wi-Fi.

Stratégie BitLocker

January 10, 2022

Windows 10 et Windows 11 comprennent une fonctionnalité de cryptage de disque appelée BitLocker, qui fournit une protection fichier et système supplémentaire contre tout accès non autorisé à un appareil Windows perdu ou volé. Pour une protection supplémentaire, vous pouvez utiliser BitLocker avec Trusted Platform Module (TPM), version 1.2 ou supérieure. Une puce TPM gère les opérations de chiffrement et génère, stocke et limite l'utilisation des clés cryptographiques.

À compter de Windows 10, build 1703, les stratégies MDM peuvent contrôler BitLocker. Vous pouvez utiliser la stratégie BitLocker dans XenMobile pour configurer les paramètres disponibles dans l'Assistant BitLocker sur les appareils Windows 10 et Windows 11. Par exemple, sur un appareil avec BitLocker activé, BitLocker peut inviter les utilisateurs à indiquer comment ils souhaitent déverrouiller leur lecteur au démarrage, sauvegarder leur clé de secours et déverrouiller un lecteur fixe. La configuration de la stratégie BitLocker permet également d'indiquer si :

- BitLocker doit être activé sur les appareils sans puce TPM ;
- les options de récupération doivent être affichées sur l'interface BitLocker ;
- l'accès en écriture sur un lecteur amovible ou fixe doit être refusé si BitLocker n'est pas activé.

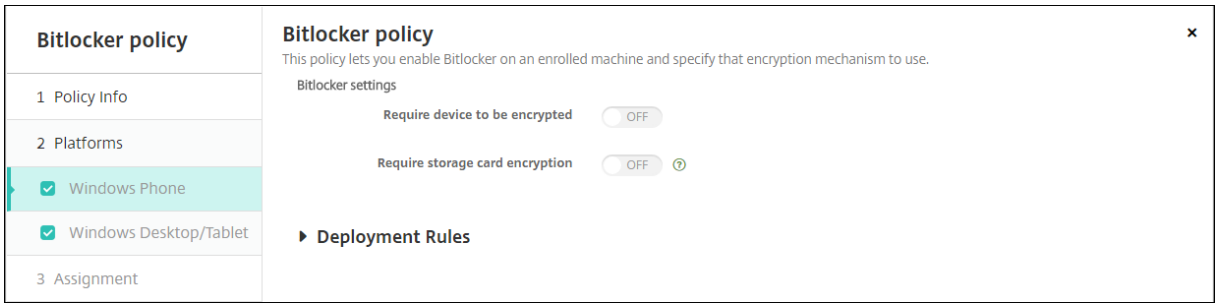
> **Remarque :**
>
> Une fois que le cryptage BitLocker démarre sur un appareil, vous ne pouvez plus par la suite modifier les paramètres de BitLocker sur l'appareil par le déploiement d'une stratégie BitLocker mise à jour.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Exigences

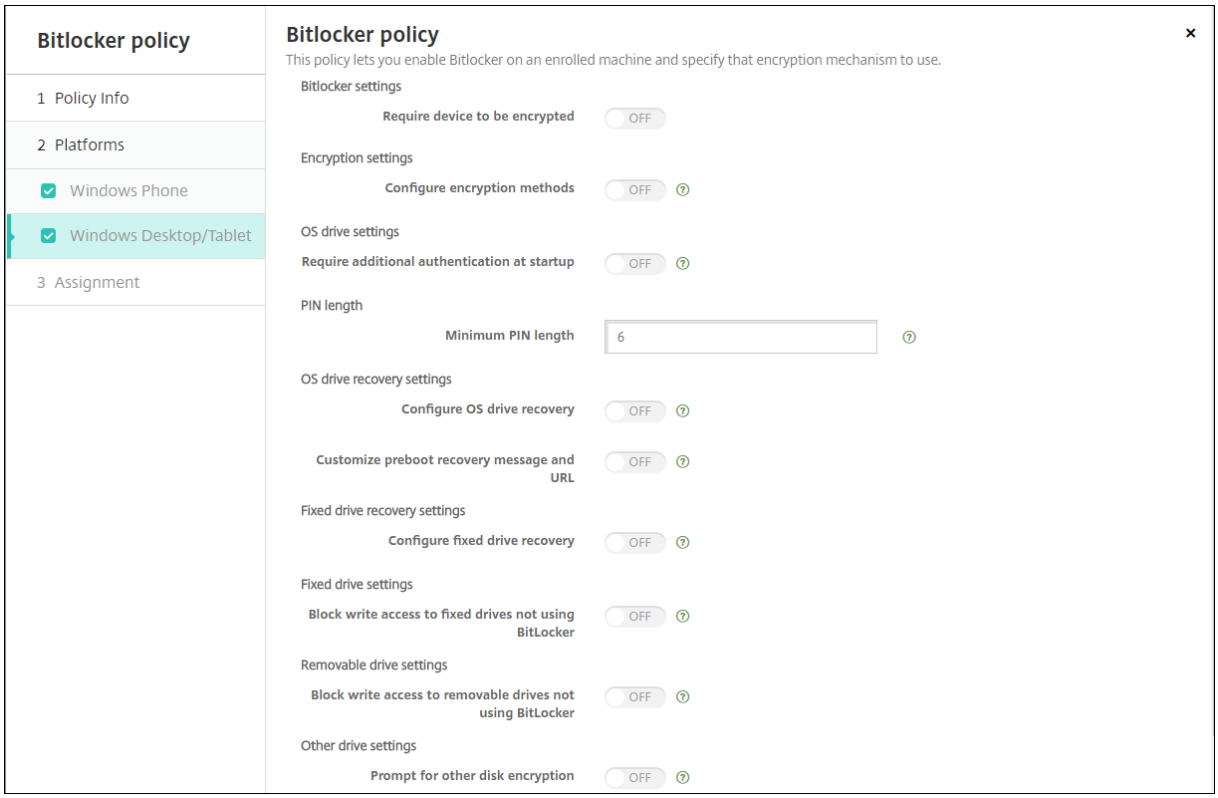
- La stratégie BitLocker requiert Windows 10 ou Windows 11 Enterprise Edition.
- Avant de déployer la stratégie BitLocker, préparez votre environnement pour l'utilisation de BitLocker. Pour plus d'informations, y compris la configuration système requise pour BitLocker et son installation, consultez la page BitLocker de Microsoft et les articles sous ce nœud.

Paramètres Windows Phone



- **Exiger cryptage de l'appareil :** permet d'indiquer si vous souhaitez inviter les utilisateurs à activer le cryptage BitLocker sur une carte de système Windows Phone. Si cette option est définie sur **Activé**, les appareils affichent un message, une fois l'inscription terminée, indiquant que l'entreprise requiert le cryptage de l'appareil. Si l'utilisateur n'accepte pas le cryptage de l'appareil, il ne dispose pas d'accès en écriture sur la carte système. Si cette option est définie sur **Désactivé**, l'utilisateur ne reçoit pas d'invite et la stratégie BitLocker détermine si l'appareil est crypté. La valeur par défaut est **Désactivé**.
- **Exiger cryptage de la carte de stockage :** permet d'indiquer si vous souhaitez inviter les utilisateurs à activer le cryptage BitLocker sur une carte de stockage Windows Phone. Si cette option est définie sur **Activé**, le cryptage de carte de stockage est obligatoire pour bénéficier d'un accès en écriture sur la carte. La valeur par défaut est **Désactivé**.

Paramètres Windows Desktop et Tablet



- **Exiger cryptage de l'appareil :** permet d'indiquer si vous souhaitez inviter les utilisateurs à activer le cryptage BitLocker sur Windows Desktop ou Tablet. Si cette option est définie sur **Activé**, les appareils affichent un message, une fois l'inscription terminée, indiquant que l'entreprise requiert le cryptage de l'appareil. Si cette option est définie sur **Désactivé**, l'utilisateur ne reçoit pas d'invite et BitLocker utilise les paramètres de stratégie. La valeur par défaut est **Désactivé**.
- **Configurer les méthodes de cryptage :** permet d'indiquer les méthodes de cryptage à utiliser

pour des types de lecteurs spécifiques. Si cette option est définie sur **Désactivé**, l'assistant BitLocker invite l'utilisateur à choisir la méthode de cryptage à utiliser pour un type de lecteur. Par défaut, la méthode de cryptage pour tous les lecteurs est XTS-AES 128 bits. La méthode de cryptage pour les lecteurs amovibles est AES-CBC 128 bits par défaut. Si cette option est définie sur **Activé**, BitLocker utilise la méthode de cryptage spécifiée dans la stratégie. Si cette option est définie sur **Activé**, ces paramètres supplémentaires s'affichent : **Lecteur du système d'exploitation**, **Lecteur fixe** et **Lecteur amovible**. Choisissez la méthode de cryptage par défaut pour chaque type de lecteur. La valeur par défaut est **Désactivé**.

- **Exiger authentification supplémentaire au démarrage :** indique l'authentification supplémentaire requise lors du démarrage de l'appareil. Spécifie également si vous souhaitez autoriser BitLocker sur les appareils qui ne possèdent pas de puce TPM. Si cette option est définie sur **Désactivé**, les appareils sans TPM ne peuvent pas utiliser le cryptage BitLocker. Pour plus d'informations sur la puce TPM, consultez l'article de Microsoft, Vue d'ensemble de la technologie de module de plateforme sécurisée. Si cette option est définie sur **Activé**, les paramètres supplémentaires suivants s'affichent. La valeur par défaut est **Désactivé**.
  - **Bloquer BitLocker sur les appareils sans puce TPM :** sur un appareil sans puce TPM, BitLocker exige que les utilisateurs créent un mot de passe de déverrouillage ou une clé de démarrage. La clé de démarrage est stockée sur un lecteur USB, que l'utilisateur doit connecter à l'appareil avant le démarrage. Le mot de passe de déverrouillage doit comporter un minimum de huit caractères. La valeur par défaut est **Désactivé**.
  - **Démarrage de TPM :** sur un appareil avec puce TPM, il existe quatre modes de déverrouillage : TPM uniquement, TPM + code PIN, TPM + clé et TPM + code PIN + clé. Le démarrage de TPM est pour le mode TPM uniquement, avec lequel les clés de cryptage sont stockées dans la puce TPM. Ce mode ne requiert pas qu'un utilisateur fournisse des données de déverrouillage supplémentaires. L'appareil utilisateur se déverrouille automatiquement au cours du redémarrage, à l'aide de la clé de cryptage stockée dans la puce TPM. La valeur par défaut est **Autoriser TPM**.
  - **Code PIN de démarrage de TPM :** ce paramètre correspond au mode de déverrouillage TPM + code PIN. Un code PIN peut contenir jusqu'à 20 chiffres. Utilisez le paramètre **Longueur minimale du code PIN** pour spécifier la longueur minimale du code PIN. Un utilisateur configure un code PIN lors de la configuration de BitLocker et fournit le code PIN lors du démarrage de l'appareil.
  - **Clé de démarrage de TPM :** ce paramètre correspond au mode de déverrouillage TPM + clé. La clé de démarrage est stockée sur un lecteur USB ou autre lecteur amovible, que l'utilisateur doit connecter à l'appareil avant le démarrage.
  - **Clé et code PIN de démarrage de TPM :** ce paramètre correspond au mode de déverrouillage TPM + code PIN + clé.

Si le déverrouillage réussit, le chargement du système d'exploitation démarre. Si le déverrouillage échoue, l'appareil entre en mode de récupération.

- **Longueur minimale du code PIN :** longueur minimale du code PIN de démarrage de la puce TPM. La valeur par défaut est de **6**.
- **Configurer la récupération de lecteur d'OS :** en cas d'échec de l'étape de déverrouillage, BitLocker invite l'utilisateur à fournir la clé de récupération configurée. Ce paramètre permet de configurer les options de récupération de lecteur du système d'exploitation à la disposition des utilisateurs lorsqu'ils ne possèdent pas de mot de passe de déverrouillage ou de clé de démarrage USB. La valeur par défaut est **Désactivé**.
  - **Autoriser agent de récupération de données basé sur certificat :** indique si un agent de récupération des données basé sur certificat est autorisé. Ajoutez un agent de récupération de données depuis les stratégies de clé publique, qui se trouvent dans la Console de gestion des stratégie de groupe (GPMC) ou dans l'éditeur de stratégie de groupe local. Pour plus d'informations sur les agents de récupération de données, consultez l'article Microsoft BitLocker Basic Deployment. La valeur par défaut est **Désactivé**.
  - **Créer un mot de passe de récupération de 48 bits pour la récupération du lecteur d'OS :** indique si vous souhaitez autoriser les utilisateurs à utiliser un mot de passe de récupération ou les y obliger. BitLocker génère le mot de passe et l'enregistre dans un fichier ou un compte Cloud Microsoft. La valeur par défaut est **Autoriser mot de passe de 48 bits**.
  - **Créer une clé de récupération de 256 bits :** indique si vous souhaitez autoriser les utilisateurs à utiliser une clé de récupération ou les y obliger. Une clé de récupération est un fichier BEK, qui est stocké sur un lecteur USB. La valeur par défaut est **Autoriser clé de récupération de 256 bits**.
  - **Masquer les options de récupération de lecteur d'OS :** indique si vous souhaitez afficher ou masquer les options de récupération sur l'interface BitLocker. Si cette option est définie sur **Activé**, aucune option de récupération ne s'affiche sur l'interface BitLocker. Dans ce cas, inscrivez les appareils sur Active Directory, enregistrez les options de récupération sur Active Directory et définissez **Enregistrer les informations de récupération sur AD DS** sur **Activé**. La valeur par défaut est **Désactivé**.
  - **Enregistrer les informations de récupération sur AD DS :** permet d'indiquer si vous souhaitez enregistrer les options de récupération sur les services de domaine Active Directory. La valeur par défaut est **Désactivé**.
  - **Configurer les informations de récupération stockées dans AD DS :** permet d'indiquer si vous souhaitez stocker le mot de passe de récupération BitLocker ou le mot de passe de récupération et le pack de clé dans les services de domaine Active Directory. Le stockage du pack de clé prend en charge la récupération des données à partir d'un lecteur qui est

altéré physiquement. La valeur par défaut est **Sauvegarder le mot de passe de récupération**.

  - **Activer BitLocker après le stockage des informations de récupération dans AD DS :** permet d'indiquer si vous souhaitez empêcher les utilisateurs d'activer BitLocker sauf si l'appareil est connecté à un domaine et si la sauvegarde des informations de récupération BitLocker sur Active Directory réussit. Si cette option est définie sur **Activé**, un appareil doit appartenir à un domaine avant de démarrer BitLocker. La valeur par défaut est **Désactivé**.

- **Personnaliser le message de récupération préalable au démarrage et l'URL :** permet d'indiquer si BitLocker affiche un message et une adresse URL personnalisés sur l'écran de récupération. Si cette option est définie sur **Activé**, les paramètres supplémentaires suivants s'affichent : **Utiliser le message de récupération et l'URL par défaut**, **Utiliser un message de récupération et une URL vides**, **Utiliser un message de récupération personnalisé** et **Utiliser une URL de récupération personnalisée**. Si cette option est définie sur **Désactivé**, le message de récupération et l'URL par défaut s'affichent. La valeur par défaut est **Désactivé**.
- **Configurer la récupération de lecteur fixe :** permet de configurer les options de récupération pour les utilisateurs pour un lecteur fixe crypté par BitLocker. BitLocker n'affiche pas de message sur le cryptage de lecteur fixe. Pour déverrouiller un lecteur au cours du démarrage, un utilisateur fournit un mot de passe ou une carte à puce. Les paramètres de déverrouillage au démarrage, qui ne sont pas dans cette stratégie, s'affichent dans l'interface BitLocker lorsqu'un utilisateur active le cryptage BitLocker sur un lecteur fixe. Pour plus d'informations sur les paramètres connexes, consultez la section **Configurer la récupération de lecteur d'OS**, plus haut dans cette liste. La valeur par défaut est **Désactivé**.
- **Bloquer l'accès en écriture aux lecteurs fixes n'utilisant pas BitLocker :** si cette option est définie sur **Activé**, les utilisateurs peuvent écrire sur les lecteurs fixes uniquement lorsque ces lecteurs sont cryptés avec BitLocker. La valeur par défaut est **Désactivé**.
- **Bloquer l'accès en écriture aux lecteurs amovibles n'utilisant pas BitLocker :** si cette option est définie sur **Activé**, les utilisateurs peuvent écrire sur les lecteurs amovibles uniquement lorsque ces lecteurs sont cryptés avec BitLocker. Configurez ce paramètre en fonction de la politique de votre organisation, selon qu'elle autorise l'accès en écriture sur les lecteurs amovibles d'une autre organisation ou non. La valeur par défaut est **Désactivé**.
- **Demander autre cryptage de disque :** vous permet de désactiver l'invite d'avertissement concernant d'autre cryptage de disque sur les appareils. La valeur par défaut est **Désactivé**.

Stratégie de navigateur

January 10, 2022

Vous pouvez créer des stratégies de navigateur pour Samsung SAFE ou Samsung KNOX afin de définir si les appareils peuvent utiliser le navigateur ou pour limiter les fonctions du navigateur que les appareils peuvent utiliser.

Sur les appareils Samsung, vous pouvez désactiver complètement le navigateur, ou vous pouvez activer ou désactiver les fenêtres publicitaires intempestives JavaScript, les cookies, le remplissage automatique, et l'affichage d'avertissements en cas de visite d'un site frauduleux.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Samsung SAFE et Samsung KNOX

- **Désactiver le navigateur :** sélectionnez cette option pour désactiver complètement le navigateur Samsung sur les appareils des utilisateurs. La valeur par défaut est **Désactivé**, ce qui permet aux utilisateurs d'utiliser le navigateur. Lorsque vous désactivez le navigateur, les options suivantes disparaissent.
- **Désactiver les fenêtres pop-up :** sélectionnez cette option pour autoriser les messages dans le navigateur.
- **Désactiver le Javascript :** sélectionnez cette option pour autoriser l'exécution de JavaScript sur le navigateur.
- **Désactiver les cookies :** sélectionnez cette option pour autoriser les cookies.
- **Désactiver le remplissage automatique :** sélectionnez cette option pour autoriser les utilisateurs à activer la fonction de remplissage automatique du navigateur.
- **Forcer l'avertissement de fraude :** sélectionnez cette option pour afficher un avertissement lorsqu'un utilisateur visite un site Web frauduleux.

Stratégie de calendrier (CalDav)

January 10, 2022

Vous pouvez ajouter une stratégie dans XenMobile afin d'ajouter un compte de calendrier (CalDAV) sur des appareils iOS ou macOS pour permettre à leurs utilisateurs de synchroniser les données de planification avec tout serveur qui prend en charge CalDAV.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Description du compte :** entrez une description du compte. Ce champ est obligatoire.
- **Nom d'hôte :** entrez l'adresse du serveur CalDAV. Ce champ est obligatoire.
- **Port :** entrez le port sur lequel se connecter au serveur CalDAV. Ce champ est obligatoire. La valeur par défaut est **8443**.
- **URL principale :** entrez l'adresse URL du calendrier de l'utilisateur.
- **Nom d'utilisateur :** entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe :** entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CalDAV. La valeur par défaut est **Activé**.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres macOS

- **Description du compte :** entrez une description du compte. Ce champ est obligatoire.
- **Nom d'hôte :** entrez l'adresse du serveur CalDAV. Ce champ est obligatoire.
- **Port :** entrez le port sur lequel se connecter au serveur CalDAV. Ce champ est obligatoire. La valeur par défaut est **8443**.
- **URL principale :** entrez l'adresse URL du calendrier de l'utilisateur.
- **Nom d'utilisateur :** entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe :** entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CalDAV. La valeur par défaut est **Activé**.
- **Paramètres de stratégie**

- **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
  - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
- **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
- **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Stratégie cellulaire

January 10, 2022

Cette stratégie vous permet de configurer des paramètres réseau cellulaire sur un appareil iOS.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Attacher APN**
  - **Nom :** nom de cette configuration.
  - **Type d'authentification :** dans la liste, cliquez sur **CHAP** (Challenge Handshake Authentication Protocol) ou **PAP** (Password Authentication Protocol). La valeur par défaut est **PAP**.
  - **Nom d'utilisateur** et **Mot de passe** : nom d'utilisateur et mot de passe à utiliser pour l'authentification.
- **APN**
  - **Nom :** nom de la configuration du nom du point d'accès (APN).
  - **Type d'authentification :** dans la liste, cliquez sur **CHAP** ou **PAP**. La valeur par défaut est **PAP**.
  - **Nom d'utilisateur** et **Mot de passe** : nom d'utilisateur et mot de passe à utiliser pour l'authentification.
  - **Serveur proxy :** adresse réseau du serveur proxy.

  - **Port du serveur proxy :** port du serveur proxy.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Stratégie du gestionnaire de connexions

January 10, 2022

Dans XenMobile, vous pouvez spécifier les paramètres de connexion pour les applications qui se connectent automatiquement à Internet et à des réseaux privés. Cette stratégie est uniquement disponible pour Windows Pocket PC.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Windows Mobile/CE

> **Remarque :**
>
> **Bureau intégré** signifie que toutes les connexions s'effectuent vers l'intranet de votre entreprise.
> **Internet intégré** signifie que toutes les connexions s'effectuent vers Internet.

- **Les applications qui se connectent à un réseau privé utilisent automatiquement :** dans la liste, cliquez sur **Bureau intégré** ou **Internet intégré**. La valeur par défaut est **Bureau intégré**.
- **Les applications qui se connectent à Internet utilisent automatiquement :** dans la liste, cliquez sur **Bureau intégré** ou **Internet intégré**. La valeur par défaut est **Bureau intégré**.

Stratégie de planification de connexion

January 10, 2022

> **Important :**
>
> Citrix recommande d'utiliser Firebase Cloud Messaging (FCM) pour contrôler les connexions à partir des appareils Android, Android Enterprise et Chrome vers XenMobile Server. Pour plus d'informations sur l'utilisation de FCM, voir Firebase Cloud Messaging.

Si vous choisissez de ne pas utiliser FCM, vous pouvez créer des stratégies de planification de connexion afin de contrôler comment et quand les appareils se connectent à XenMobile Server.

Vous pouvez spécifier que les utilisateurs connectent leurs appareils manuellement ou que les appareils se connectent dans un intervalle de temps défini.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres de plate-forme

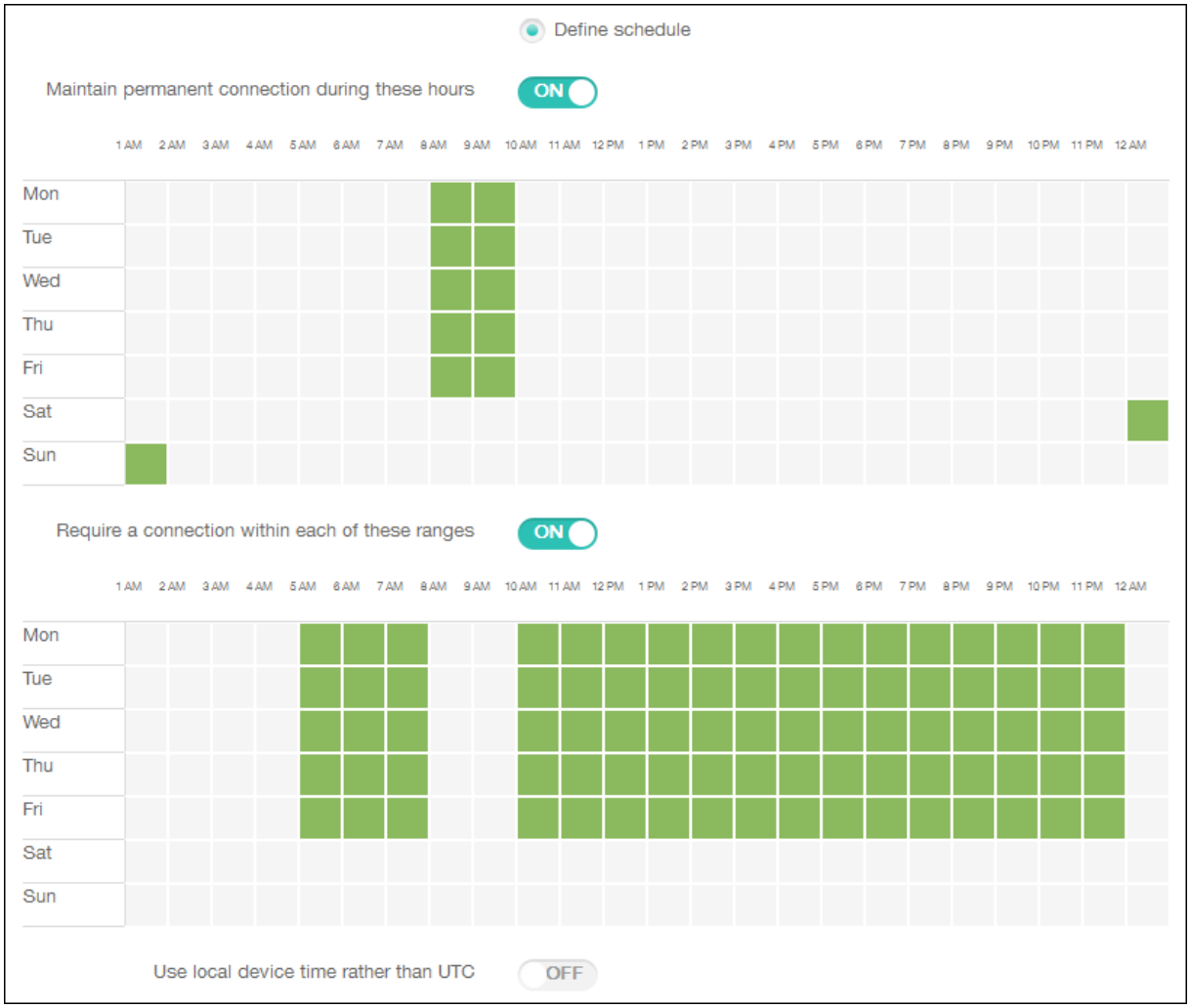
- **Exiger que les appareils se connectent :** cliquez sur l'option que vous souhaitez définir pour cette planification.
  - **Toujours :** conserve la connexion active de façon permanente. Sur l'appareil de l'utilisateur, XenMobile tente de se reconnecter au serveur XenMobile après une perte de connexion réseau et surveille la connexion en transmettant des paquets de contrôle à intervalles réguliers. Citrix recommande cette option pour optimiser la sécurité. Lorsque vous sélectionnez **Toujours**, utilisez également le paramètre **Définir le délai d'expiration de la connexion** pour la **Stratégie de tunnel** pour vous assurer que la connexion ne décharge pas la batterie. En conservant la connexion active, vous pouvez distribuer des commandes de sécurité telles que l'effacement ou le verrouillage de l'appareil à la demande. Vous devez également sélectionner l'option **Calendrier de déploiement Déployer pour les connexions permanentes** dans chaque stratégie déployée sur l'appareil.
  - **Jamais :** connexion manuelle. Les utilisateurs doivent lancer la connexion depuis XenMobile sur leurs appareils. Citrix ne recommande pas cette option pour les déploiements de production, car elle empêche le déploiement des stratégies de sécurité sur les appareils, ce qui signifie que les utilisateurs ne recevront jamais les nouvelles applications ou stratégies.
  - **Toutes les :** se connecte à l'intervalle défini. Lorsque cette option est activée et que vous envoyez une stratégie de sécurité telle qu'un effacement ou verrouillage, XenMobile traite l'action sur l'appareil la prochaine fois que l'appareil se connecte. Lorsque vous sélectionnez cette option, le champ **Se connecter toutes les N minutes** apparaît. Vous devez y entrer le nombre de minutes après lesquelles l'appareil doit se reconnecter. La valeur par défaut est **20**.

- **Définir un calendrier :** lorsque cette option est activée, sur l'appareil de l'utilisateur, XenMobile tente de se reconnecter au serveur XenMobile après une perte de connexion réseau et surveille la connexion en transmettant des paquets de contrôle à intervalles réguliers dans le délai imparti. Pour savoir comment définir un délai de connexion, consultez la section Définition d'un délai de connexion.
  * **Maintenir une connexion permanente durant ces heures :** les appareils des utilisateurs doivent être connectés pendant l'intervalle de temps défini.
  * **Exiger une connexion dans chacun de ces intervalles :** les appareils des utilisateurs doivent être connectés au moins une fois dans les intervalles de temps définis.
  * **Utiliser l'heure locale de l'appareil comme référence et non l'heure UTC :** synchronise les intervalles définis avec l'appareil local plutôt que le temps universel coordonné (UTC).

Définition d'un délai de connexion

Lorsque vous activez les options suivantes, un calendrier s'affiche dans lequel vous pouvez définir les délais souhaités. Vous pouvez activer l'une ou l'autre de ces options ou les deux options pour exiger une connexion permanente durant des heures spécifiques ou exiger une connexion dans des délais impartis. Chaque carré dans le calendrier correspond à 30 minutes, par conséquent si vous souhaitez établir une connexion entre 8:00 AM et 9:00 AM chaque jour de la semaine, cliquez sur les deux carrés sur le calendrier entre 8 AM et 9 AM chaque jour de la semaine.

Par exemple, les deux calendriers dans la figure suivante requièrent une connexion permanente entre 8:00 et 9:00 chaque jour de la semaine, une connexion permanente entre 12:00 AM samedi et 1:00 AM dimanche, et au moins une connexion chaque jour de la semaine entre 5:00 AM et 8:00 AM ou entre 10:00 et 11:00 PM.



Stratégie de contacts (CardDAV)

January 10, 2022

Vous pouvez ajouter une stratégie dans XenMobile afin d'ajouter un compte de contacts iOS (CalDAV) sur des appareils iOS ou macOS pour permettre à leurs utilisateurs de synchroniser les données de contact avec tout serveur qui prend en charge CalDAV.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Description du compte :** entrez une description du compte. Ce champ est obligatoire.

- **Nom d'hôte :** entrez l'adresse du serveur CardDAV. Ce champ est obligatoire.
- **Port :** entrez le port sur lequel se connecter au serveur CardDAV. Ce champ est obligatoire. La valeur par défaut est **8443**.
- **URL principale :** entrez l'adresse URL du calendrier de l'utilisateur.
- **Nom d'utilisateur :** entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe :** entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CardDAV. La valeur par défaut est **Activé**.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres macOS

- **Description du compte :** entrez une description du compte. Ce champ est obligatoire.
- **Nom d'hôte :** entrez l'adresse du serveur CardDAV. Ce champ est obligatoire.
- **Port :** entrez le port sur lequel se connecter au serveur CardDAV. Ce champ est obligatoire. La valeur par défaut est **8443**.
- **URL principale :** entrez l'adresse URL du calendrier de l'utilisateur.
- **Nom d'utilisateur :** entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe :** entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CardDAV. La valeur par défaut est **Activé**.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.

    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Stratégie Contrôler mise à jour d'OS

September 22, 2021

La stratégie Contrôler mises à jour d'OS vous permet de :

- Déployer les dernières mises à jour du système d'exploitation sur les appareils iOS supervisés.

  La stratégie Mise à jour d'OS ne fonctionne que pour les appareils supervisés inscrits au programme de déploiement Apple.

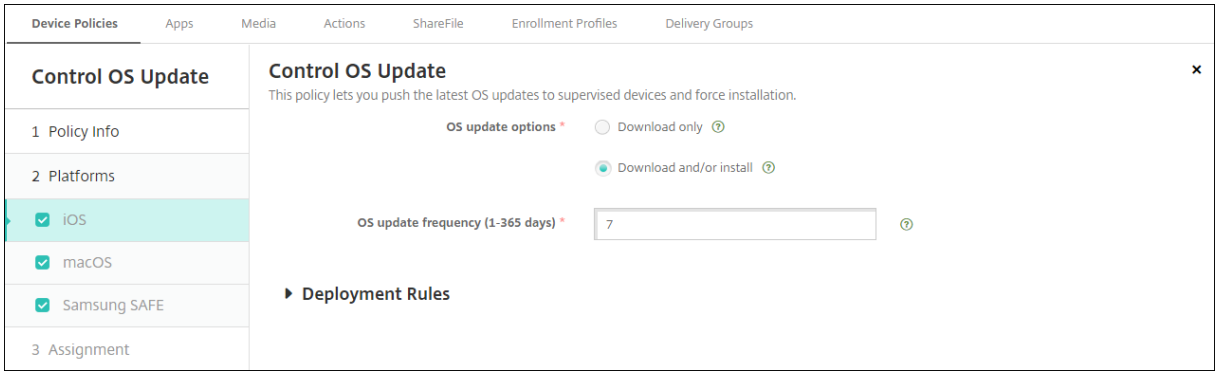
- Déployer le dernier système d'exploitation et les dernières mises à jour de l'application sur les appareils macOS inscrits auprès du programme DEP exécutant macOS 10.11.5 et versions ultérieures.

- Déployer les dernières mises à jour du système d'exploitation sur les appareils Samsung SAFE supervisés.

  Pour les appareils Samsung SAFE, XenMobile envoie la stratégie Contrôler mises à jour d'OS à Secure Hub qui applique ensuite la stratégie à l'appareil. La page **Gérer> Appareils** indique lorsque le serveur XenMobile envoie la stratégie et lorsque l'appareil reçoit la stratégie.

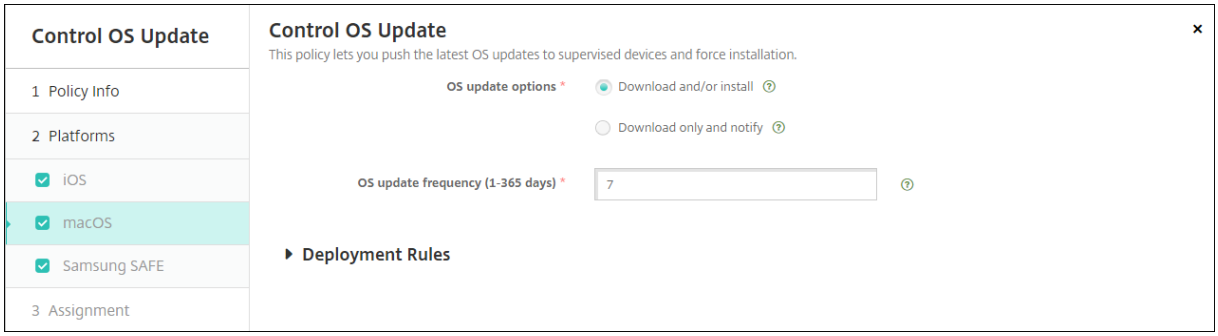
Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Options de mise à jour de l'OS :** les deux options téléchargent les dernières mises à jour du système d'exploitation sur les appareils supervisés selon la **fréquence de mise à jour de l'OS**. L'appareil invite les utilisateurs à installer les mises à jour. L'invite est visible une fois que l'utilisateur a déverrouillé l'appareil.
- **Fréquence de mise à jour de l'OS :** détermine la fréquence à laquelle XenMobile vérifie et met à jour le système d'exploitation de l'appareil. La valeur par défaut est **7** jours.

Paramètres macOS



- **Options de mise à jour de l'OS :** les deux options téléchargent les dernières mises à jour pour macOS selon la **fréquence de mise à jour de l'OS**. Vous pouvez choisir d'installer les mises à jour ou informer l'utilisateur via l'App Store que des mises à jour sont disponibles.
- **Fréquence de mise à jour de l'OS :** détermine la fréquence à laquelle XenMobile vérifie et met à jour le système d'exploitation de l'appareil. La valeur par défaut est **7** jours.

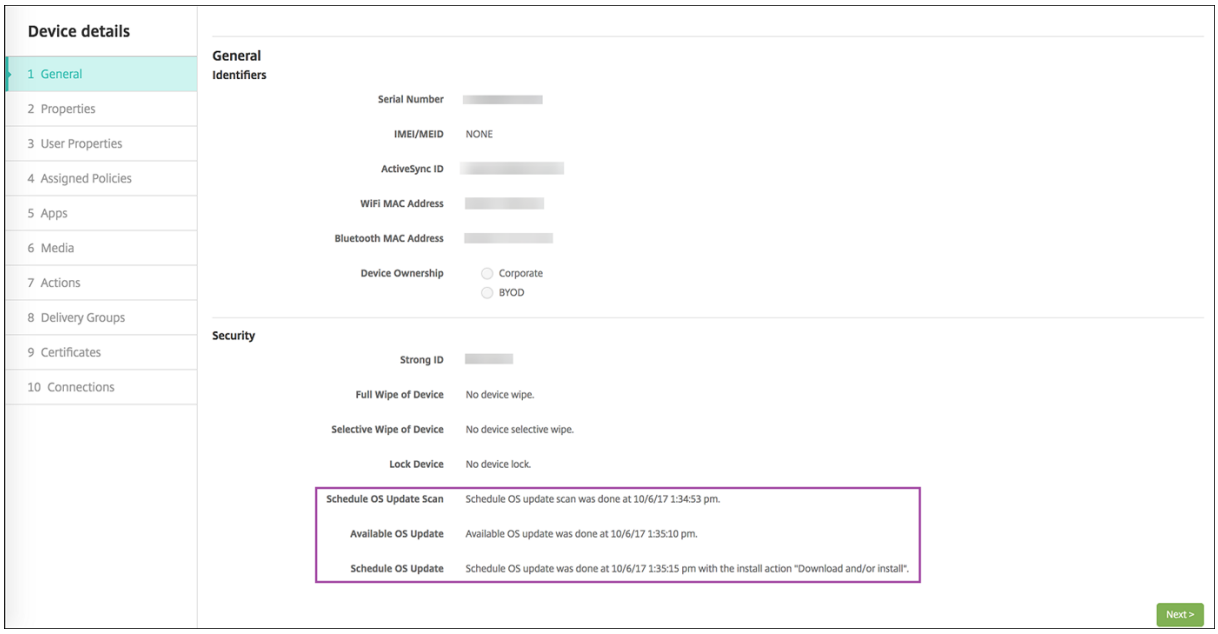
Obtenir l'état des actions de mise à jour pour iOS et macOS

Pour iOS et macOS, XenMobile ne déploie la stratégie Contrôler mises à jour d'OS sur les appareils. Au lieu de cela, XenMobile utilise la stratégie d'envoi de ces commandes MDM aux appareils :

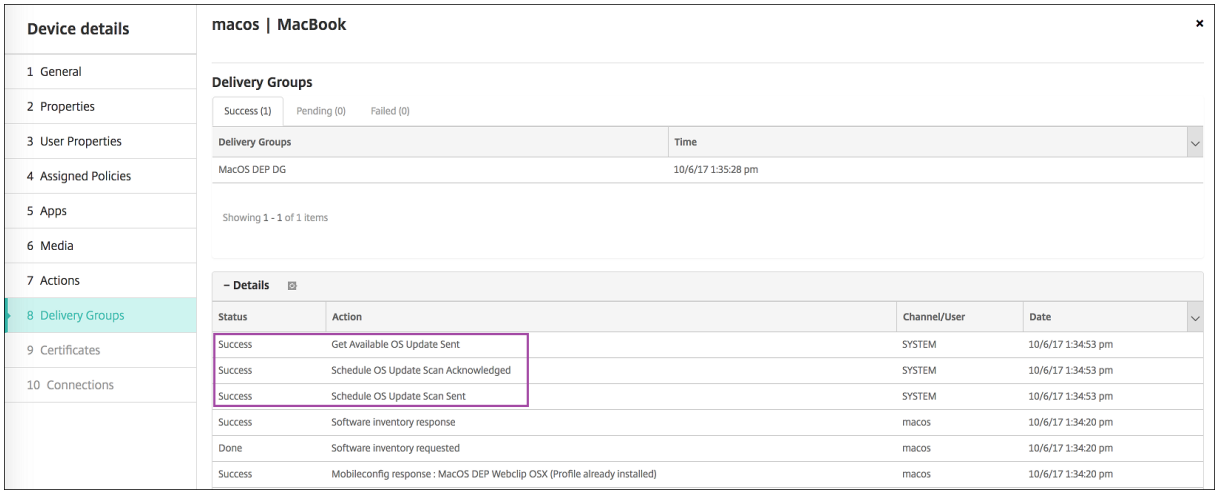
- Planification d'analyse de mise à jour d'OS : permet de demander à l'appareil d'effectuer une analyse en arrière-plan pour les mises à jour du système d'exploitation (optionnel pour iOS).

- Mise à jour d'OS disponible : permet d'interroger l'appareil pour obtenir la liste des mises à jour du système d'exploitation disponibles.
- Planification de mise à jour d'OS : permet de demander à l'appareil d'effectuer des mises à jour macOS, des mises à jour de l'application ou les deux. Par conséquent, le système d'exploitation de l'appareil détermine lorsqu'il doit télécharger ou installer les mises à jour du système d'exploitation et de l'application.

La page **Gérer > Appareils > Détails de l'appareil (Général)** affiche l'état des analyses de mise à jour de système d'exploitation planifiées et disponibles et des mises à jour de macOS et d'applications planifiées.

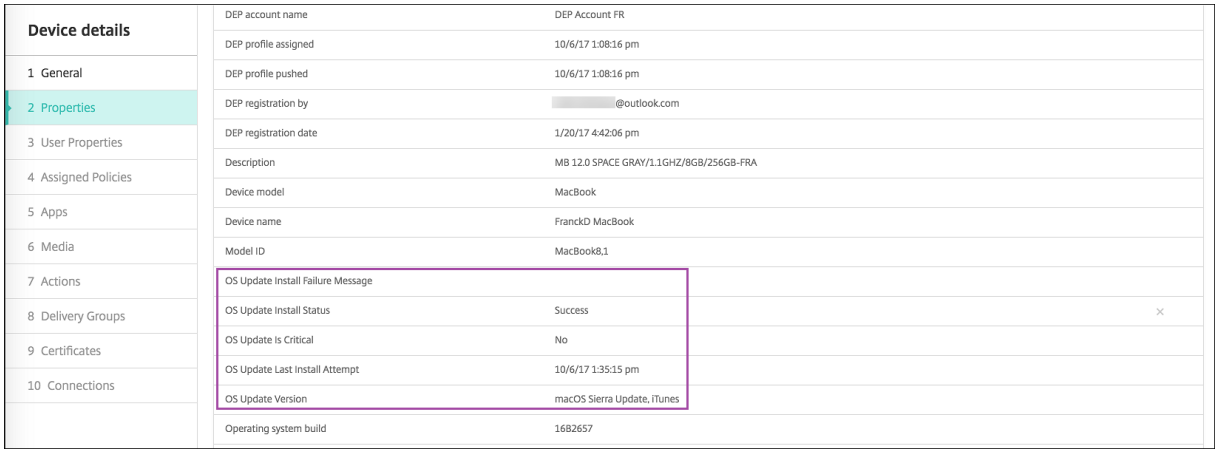


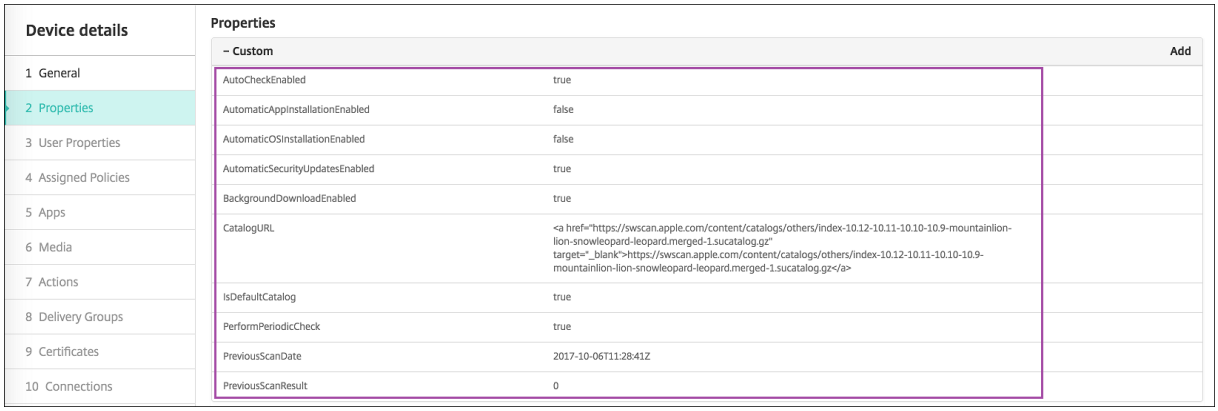
Pour de plus amples informations sur l'état des actions de mise à jour, accédez à la page **Gérer > Appareils > Détails de l'appareil (Groupes de mise à disposition)**.



Pour de plus amples informations telles que les mises à jour du système d'exploitation disponibles

et la dernière tentative d'installation, accédez à la page **Gérer > Appareils > Détails de l'appareil (Propriétés)**.

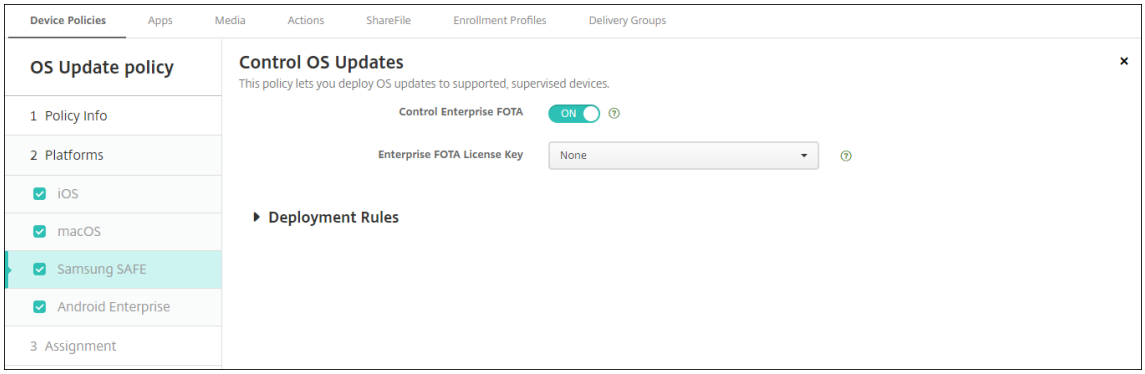




Paramètres Samsung SAFE

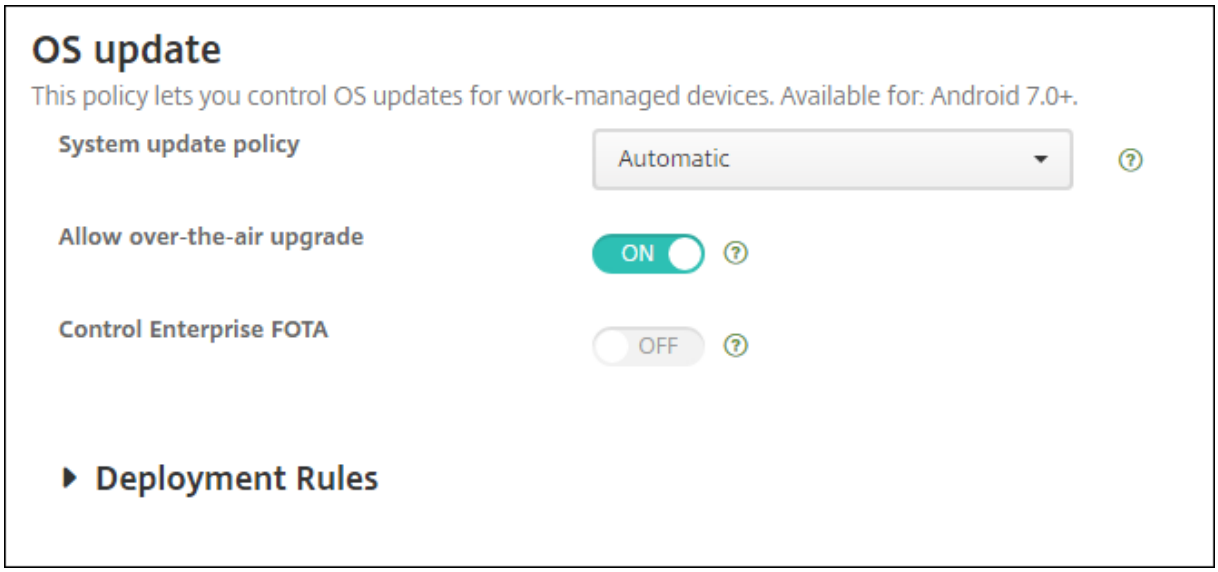
Samsung Enterprise FOTA (ou E-FOTA) vous permet de déterminer quand les appareils sont mis à jour et la version de micrologiciel à utiliser. Pour utiliser E-FOTA :

1. Créez une stratégie de clé de licence MDM Samsung avec les clés et les informations de licence que Samsung vous a fournies. Pour de plus amples informations, consultez la section Stratégie de clé de licence MDM Samsung.
2. Créez une stratégie Contrôler mises à jour d'OS pour activer Enterprise FOTA.



- **Activer Enterprise FOTA :** définissez sur **Activé**.
- **Clé de licence d'Enterprise FOTA :** sélectionnez le nom de la stratégie de clé de licence MDM Samsung.

Paramètres Android Enterprise



- **Stratégie de mise à jour du système :** permet de déterminer quand les mises à jour système se produisent. Si l'option **Contrôler Enterprise FOTA** est activée, les mises à jour se produisent automatiquement, quelle que soit la configuration de ce paramètre.
  - **Automatique :** installe une mise à jour lorsqu'elle est disponible.
  - **Créneau :** installe une mise à jour automatiquement dans la fenêtre de maintenance quotidienne spécifiée dans **Heure de début** et **Heure de fin**.
    - **Heure de début :** le début de la fenêtre de maintenance mesurée en nombre de minutes (**0** - **1440**) à partir de minuit dans l'heure locale de l'appareil. La valeur par défaut est **0**.
    - **Heure de fin :** la fin de la fenêtre de maintenance mesurée en nombre de minutes (**0** - **1440**) à partir de minuit dans l'heure locale de l'appareil. La valeur par défaut est **120**.

  - **Reporter :** permet à un utilisateur de reporter une mise à jour jusqu'à 30 jours.
- **Autoriser mise à jour par réseau cellulaire :** si cette option est désactivée, les machines utilisateur ne peuvent pas recevoir les mises à jour logicielles sans fil. La valeur par défaut est **Activé**.
- **Contrôler Enterprise FOTA :** si cette option est activée, les appareils Samsung vérifient la dernière mise à jour et l'installent automatiquement. Lorsque cette option est désactivée, les utilisateurs peuvent rechercher des mises à jour et les installer manuellement. Pour les appareils Android Enterprise exécutant Samsung Knox 3.0 ou version ultérieure. La valeur par défaut est **Désactivé**.
  - **Clé de licence d'Enterprise FOTA :** sélectionnez la clé de licence à utiliser lors de la recherche de mises à jour. Vous pouvez configurer ce paramètre dans la stratégie Clé de licence MDM Samsung. Pour les appareils Android Enterprise exécutant Samsung Knox 3.0 ou version ultérieure. La valeur par défaut est **Aucun**. La clé peut être définie à l'aide de la stratégie **Clé de licence MDM Samsung** . Consultez la section Stratégie de clé de licence MDM Samsung.

Stratégie Copier les applications sur le conteneur Samsung

January 10, 2022

Pour les applications déjà installées sur un appareil, vous pouvez spécifier de copier les applications vers un KNOX sur les appareils Samsung pris en charge. Pour de plus amples informations sur les appareils pris en charge, consultez la page Samsung Devices built on Knox.

Les applications copiées sur le conteneur KNOX sont disponibles uniquement lorsque les utilisateurs se connectent au conteneur KNOX.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Conditions préalables

- Inscrivez l'appareil dans XenMobile.
- Déployez les clés MDM Samsung (ELM et KLM). Pour savoir comment procéder, consultez la section Stratégie de clé de licence MDM Samsung.
- Installez les applications sur l'appareil.
- Initialisez KNOX sur l'appareil pour copier les applications dans le conteneur KNOX.

Paramètres de plate-forme

- **Nouvelle application :** pour chaque application que vous souhaitez ajouter à la liste, cliquez sur **Ajouter**, puis procédez comme suit :
  - Entrez un ID de package ; par exemple, com.mobiwolf.lacingart pour l'application LacingArt.
  - Cliquez sur **Enregistrer** ou **Annuler**.

Stratégie d'informations d'identification

January 10, 2022

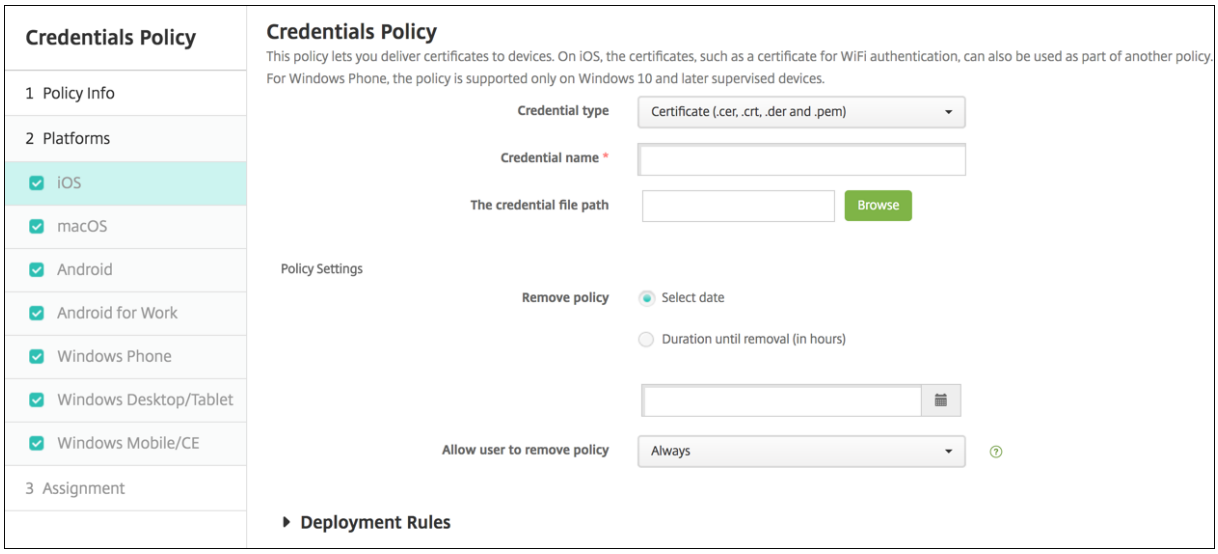
Les stratégies d'informations d'identification pointent vers une infrastructure de clé publique (PKI) configurée dans XenMobile. Par exemple, votre configuration PKI peut inclure une entité PKI, un keystore, un fournisseur d'identités ou un certificat de serveur. Pour de plus amples informations sur les informations d'identification, consultez Certificats et authentification.

Chaque plate-forme prise en charge requiert des valeurs différentes, qui sont décrites dans cet article.

> **Remarque :**
>
> Avant de pouvoir créer cette stratégie, vous devez connaître les informations d'identification que vous projetez d'utiliser pour chaque plate-forme, ainsi que les certificats et les mots de passe.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

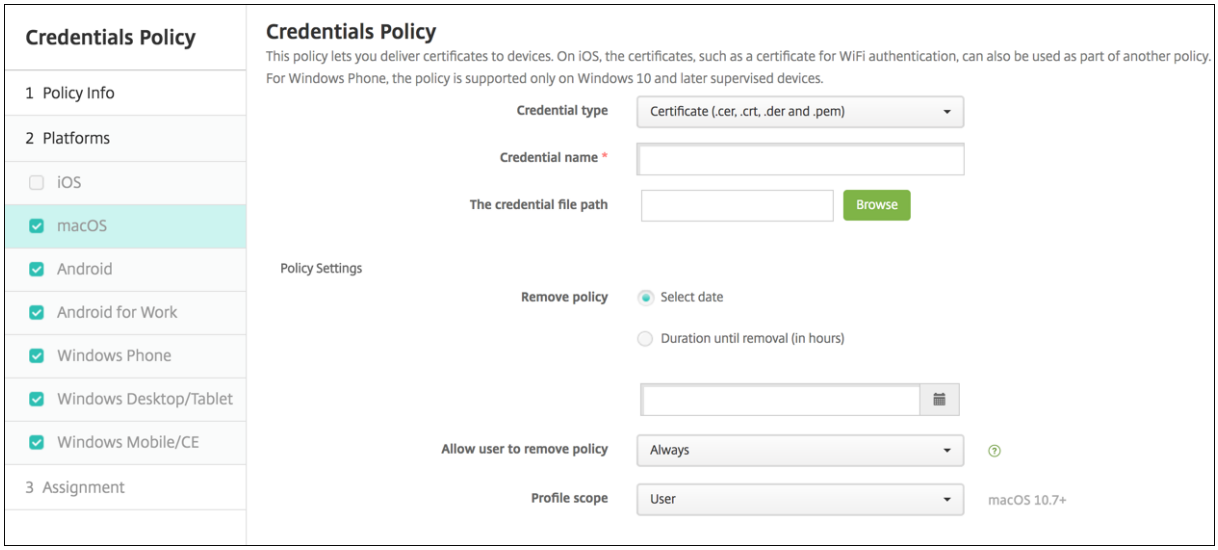
Paramètres iOS



Configurez les paramètres suivants :

- **Type de certificat :** dans la liste, cliquez sur le type de certificat à utiliser avec cette stratégie et entrez les informations suivantes pour le certificat que vous sélectionnez :
  - **Certificat**
    - **Nom du certificat :** entrez un nom unique pour le certificat.
    - **Emplacement du certificat :** sélectionnez le fichier de certificat en cliquant sur Parcourir et accédez à l'emplacement du fichier.
  - **Keystore**
    - **Nom du certificat :** entrez un nom unique pour le certificat.
    - **Emplacement du certificat :** sélectionnez le fichier de certificat en cliquant sur Parcourir et accédez à l'emplacement du fichier.
    - **Mot de passe :** entrez le mot de passe du magasin de clés pour le certificat.
  - **Écran Server certificate**
    - **Certificat serveur :** dans la liste, cliquez sur le certificat à utiliser.
  - **Fournisseur d'identités**
    - **Fournisseur d'identités :** dans la liste, cliquez sur le nom du fournisseur d'identités.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres macOS



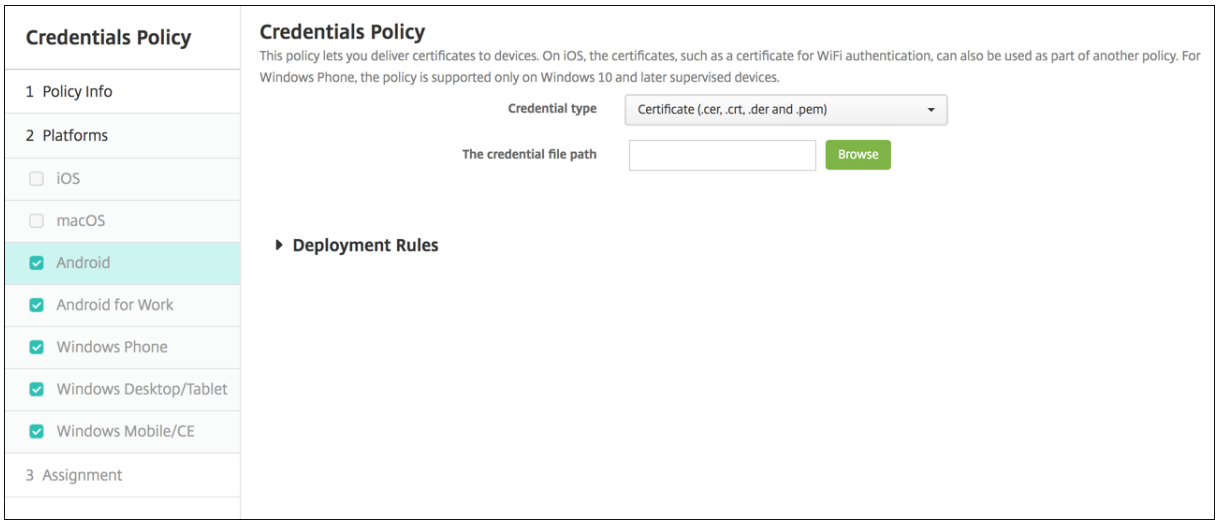
Configurez les paramètres suivants :

- **Type de certificat :** dans la liste, cliquez sur le type de certificat à utiliser avec cette stratégie et entrez les informations suivantes pour le certificat que vous sélectionnez :
  - **Certificat**
    - **Nom du certificat :** entrez un nom unique pour le certificat.
    - **Emplacement du certificat :** sélectionnez le fichier de certificat en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
  - **Keystore**
    - **Nom du certificat :** entrez un nom unique pour le certificat.
    - **Emplacement du certificat :** sélectionnez le fichier de certificat en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
    - **Mot de passe :** entrez le mot de passe du magasin de clés pour le certificat.
  - **Écran Server certificate**
    - **Certificat serveur :** dans la liste, cliquez sur le certificat à utiliser.
  - **Fournisseur d'identités**
    - **Fournisseur d'identités :** dans la liste, cliquez sur le nom du fournisseur d'identités.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les

utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.

- **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

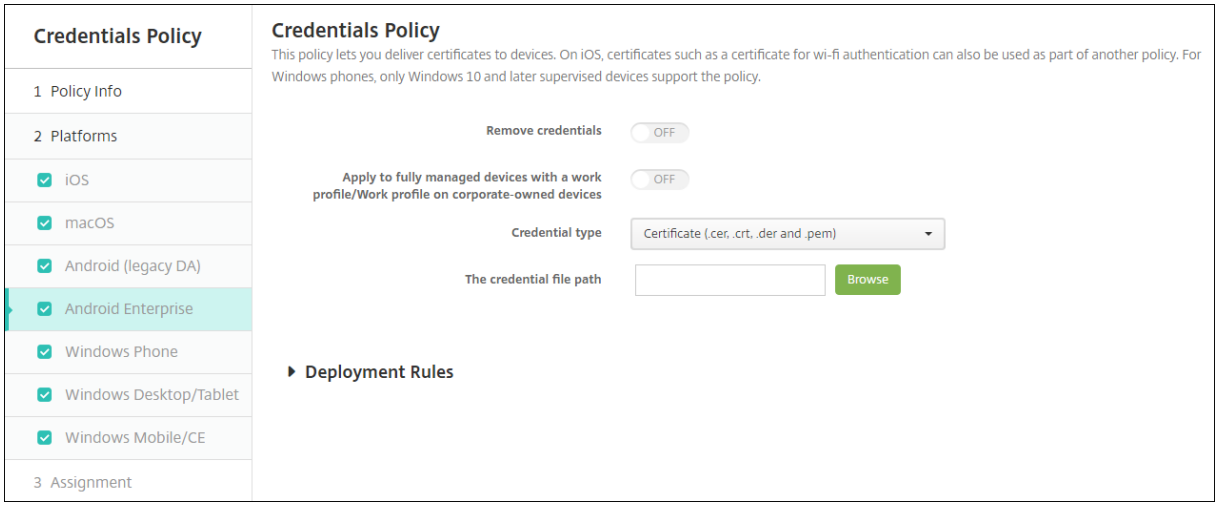
Paramètres Android



Configurez les paramètres suivants :

- **Type de certificat :** dans la liste, cliquez sur le type de certificat à utiliser avec cette stratégie et entrez les informations suivantes pour le certificat que vous sélectionnez :
  - **Certificat**
    - **Nom du certificat :** entrez un nom unique pour le certificat.
    - **Emplacement du certificat :** sélectionnez le fichier de certificat en cliquant sur Parcourir et accédez à l'emplacement du fichier.
  - **Keystore**
    - **Nom du certificat :** entrez un nom unique pour le certificat.
    - **Emplacement du certificat :** sélectionnez le fichier de certificat en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
    - **Mot de passe :** entrez le mot de passe du keystore pour le certificat.
  - **Écran Server certificate**
    - **Certificat serveur :** dans la liste, cliquez sur le certificat à utiliser.
  - **Fournisseur d'identités**
    - **Fournisseur d'identités :** dans la liste, cliquez sur le nom du fournisseur d'identités.

Paramètres Android Enterprise



Configurez ces paramètres pour déterminer comment XenMobile applique les paramètres d'informations d'identification :

- **Supprimer les informations d'identification :** définissez cette option sur **Activé** pour configurer les paramètres suivants. La valeur par défaut est **Désactivé**.
  - **Supprimer les informations d'identification de l'utilisateur :** supprime les certificats du keystore géré. La valeur par défaut est **Désactivé**.
  - **Supprimer les certificats racine approuvés :** désinstalle tous les certificats CA non système. La valeur par défaut est **Désactivé**.
- **Appliquer aux appareils entièrement gérés avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise :** permet de configurer les paramètres de stratégie Informations d'identification pour les appareils entièrement gérés avec profil de travail. Lorsque ce paramètre est défini sur **Activé**, les paramètres d'informations d'identification que vous configurez s'appliquent uniquement au profil de travail. Lorsque ce paramètre est défini sur **Désactivé**, les paramètres d'informations d'identification que vous configurez s'appliquent uniquement à l'appareil. La valeur par défaut est **Désactivé**.

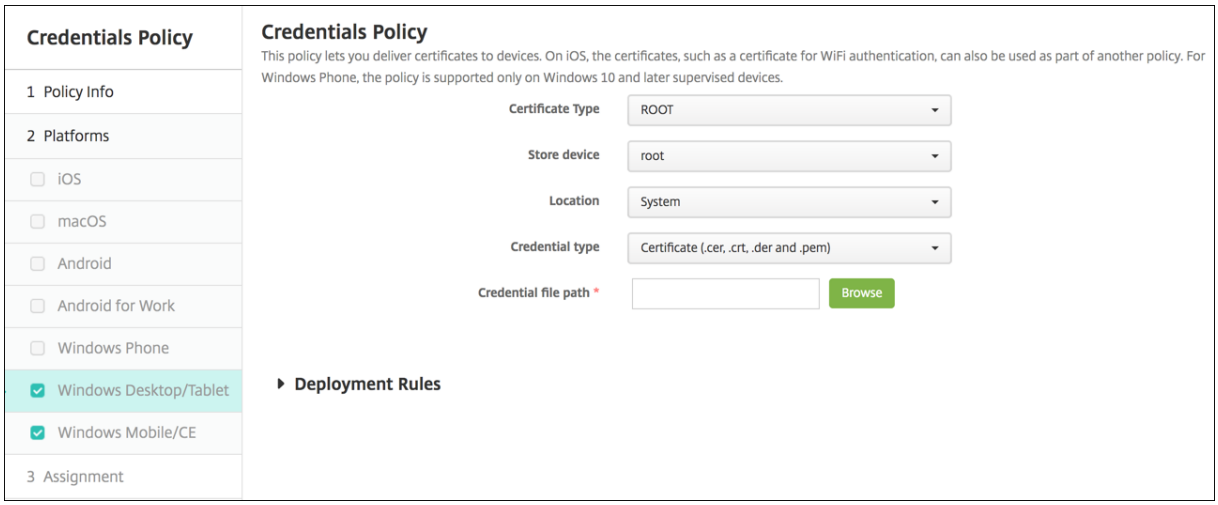
Configurez les paramètres des informations d'identification :

- **Type de certificat :** dans la liste, cliquez sur le type de certificat à utiliser avec cette stratégie et entrez les informations suivantes pour le certificat que vous sélectionnez :
  - **Certificat**
    - **Emplacement du certificat :** sélectionnez le fichier de certificat en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
  - **Keystore**
    - **Emplacement du certificat :** sélectionnez le fichier de certificat en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
    - **Alias de certificat :** un alias de certificat permet à l'application d'accéder plus facile-

ment au certificat. Configurez un alias de certificat dans la stratégie Configurations gérées par Android Entreprise. Entrez ensuite l'alias dans le champ **Alias de certificat** de la stratégie d'informations d'identification Les applications récupèrent le certificat et authentifient le VPN sans aucune action de la part des utilisateurs.

  * **Mot de passe :** entrez le mot de passe du keystore pour le certificat.
- **Écran Server certificate**
  * **Certificat serveur :** dans la liste, cliquez sur le certificat à utiliser.
- **Fournisseur d'identités**
  * **Alias de certificat :** un alias de certificat permet à l'application d'accéder plus facilement au certificat. Configurez un alias de certificat dans la stratégie Configurations gérées par Android Entreprise. Entrez ensuite l'alias dans le champ **Alias de certificat** de la stratégie d'informations d'identification Les applications récupèrent le certificat et authentifient le VPN sans aucune action de la part des utilisateurs.
  * **Fournisseur d'identités :** dans la liste, cliquez sur le nom du fournisseur d'identités.
  * **Applications qui utilisent les certificats :** pour spécifier des applications disposant d'un accès silencieux aux informations d'identification de ce fournisseur : cliquez sur **Ajouter**, sélectionnez une application, puis cliquez sur **Enregistrer**.

Paramètres Windows Desktop/Tablet



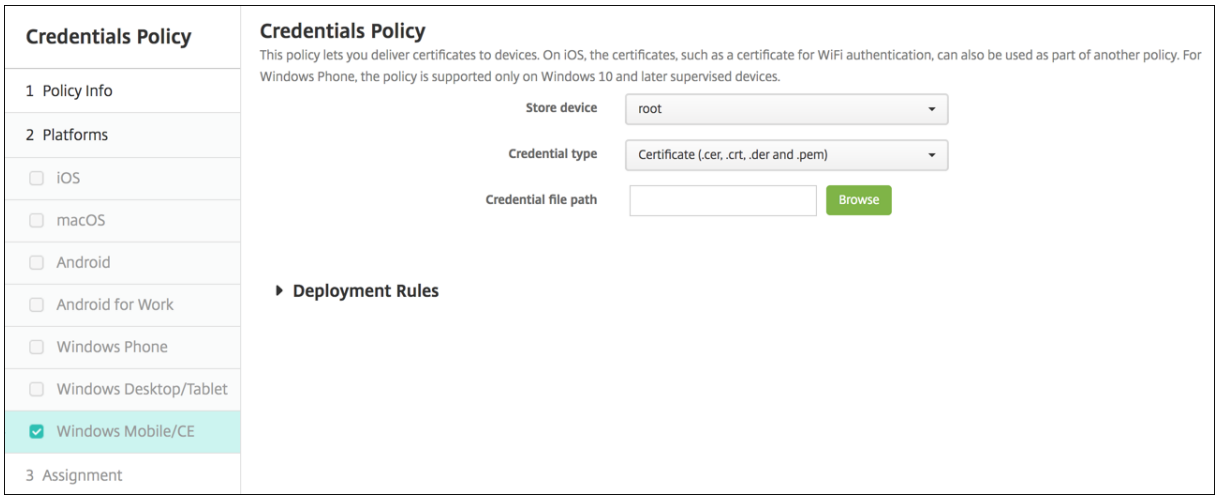
- **Type de certificat :** dans la liste, cliquez sur **ROOT** ou **CLIENT**.
- Si vous avez sélectionné **ROOT**, configurez les paramètres suivants :
  - **Périphérique de stockage :** dans la liste, cliquez sur **racine**, **Mon magasin** ou **Autorité de certification** pour l'emplacement du magasin de certificats pour le certificat. **Mon magasin** stocke les certificats dans les magasins de certificats des utilisateurs.
  - **Emplacement : Système** est le seul emplacement pour les tablettes Windows 10 et Windows 11.
  - **Type de certificat : Certificat** est le seul type de certificat pour tablettes Windows 10 et

Windows 11.

- **Emplacement du certificat :** sélectionnez le fichier de certificat, en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

- Si vous avez sélectionné **CLIENT**, configurez les paramètres suivants :
- **Emplacement : Système** est le seul emplacement pour les tablettes Windows 10 et Windows 11.
- **Type de certificat : Keystore** est le seul type de certificat pour tablettes Windows 10 et Windows 11.
- **Nom du certificat :** entrez un nom pour le certificat. Ce champ est obligatoire.
- **Emplacement du certificat :** sélectionnez le fichier de certificat, en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
- **Mot de passe :** entrez le mot de passe associé au certificat. Ce champ est obligatoire.

Paramètres Windows Mobile/CE



- **Périphérique de stockage :** dans la liste, cliquez sur l'emplacement du magasin de certificats pour le certificat. La valeur par défaut est **racine**. Les options sont les suivantes :
  - **Autorités de certification privilégiées :** les applications signées avec un certificat appartenant à ce magasin s'exécutent avec un niveau de confiance privilégié.
  - **Autorités de certification non privilégiées :** les applications signées avec un certificat appartenant à ce magasin s'exécutent avec un niveau de confiance normal.
  - **Éditeurs de logiciels approuvés :** des éditeurs de logiciels approuvés sont utilisés pour signer les fichiers .cab.
  - **root :** un magasin de certificats qui contient des certificats racines.
  - **Autorité de certification :** magasin de certificats qui contient des informations cryptographiques, y compris des autorités de certificat intermédiaire.
  - **Mon magasin :** magasin de certificats qui contient des certificats personnels.
- **Type de certificat :** le certificat est le seul type de certificat pour appareils Windows Mobile/CE.

- **Emplacement du certificat :** sélectionnez le fichier de certificat en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

Stratégie XML personnalisée

January 10, 2022

Vous pouvez créer des stratégies XML personnalisées dans XenMobile pour personnaliser les fonctionnalités suivantes sur les appareils Windows, Zebra Android et Android Enterprise pris en charge :

- Provisioning, qui comprend la configuration de l'appareil, et l'activation ou la désactivation de fonctionnalités.
- Configuration de l'appareil, ce qui permet aux utilisateurs de modifier les paramètres sur l'appareil.
- Mises à niveau logicielles, qui comprennent la mise à disposition de nouveaux logiciels ou de correctifs de bogues à charger sur l'appareil, y compris des applications et logiciels système.
- Gestion des pannes, ce qui comprend la réception de rapports d'erreur et d'état à partir de l'appareil.

> **Remarque :**
>
> Lorsque vous créez votre contenu XML, utilisez le caractère % avec prudence. Le caractère % est un caractère XML réservé, utilisé uniquement pour échapper les caractères spéciaux XML. Pour utiliser % dans un nom, encodez-le avec %25.

Pour les appareils Windows : vous créez votre propre configuration XML personnalisée à l'aide de l'API Open Mobile Alliance Device Management (OMA DM) dans Windows. La création de code XML personnalisé avec l'API OMA DM n'est pas couverte dans cette rubrique. Pour de plus amples informations sur l'utilisation de l'API OMA DM, veuillez consulter la section [OMA Device Management](https://docs.microsoft.com/en-us/previous-versions/bb737369(v=msdn.10) sur le site de Microsoft Developer Network.

Pour les appareils Android Zebra et Android Enterprise : vous créez la configuration XML personnalisée à l'aide du système de gestion MX (MXMS). La création de code XML personnalisé avec l'API MXMS n'est pas couverte dans cet article. Pour plus d'informations sur l'utilisation de MXMS, consultez la section About MX sur le site Zebra.

> **Remarque :**
>
> Pour Windows 10 RS2 Phone : une fois qu'une stratégie XML personnalisée ou Restrictions qui désactive Internet Explorer a été déployée sur le téléphone, le navigateur reste activé. Pour contourner ce problème, redémarrez le téléphone. Il s'agit d'un problème de tiers.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Windows Phone, Windows Desktop/Tablet, Zebra Android et Android Enterprise

- **Contenu XML :** entrez, ou copiez et collez, le code XML personnalisé que vous souhaitez ajouter à la stratégie.

  Après avoir cliqué sur **Suivant**, XenMobile vérifie la syntaxe du contenu XML. Les erreurs de syntaxe s'affichent en dessous de la zone de contenu. Vous devez résoudre les erreurs avant de continuer.

  S'il n'existe pas d'erreurs de syntaxe, la page d'attribution de la **Stratégie XML personnalisée** s'affiche.

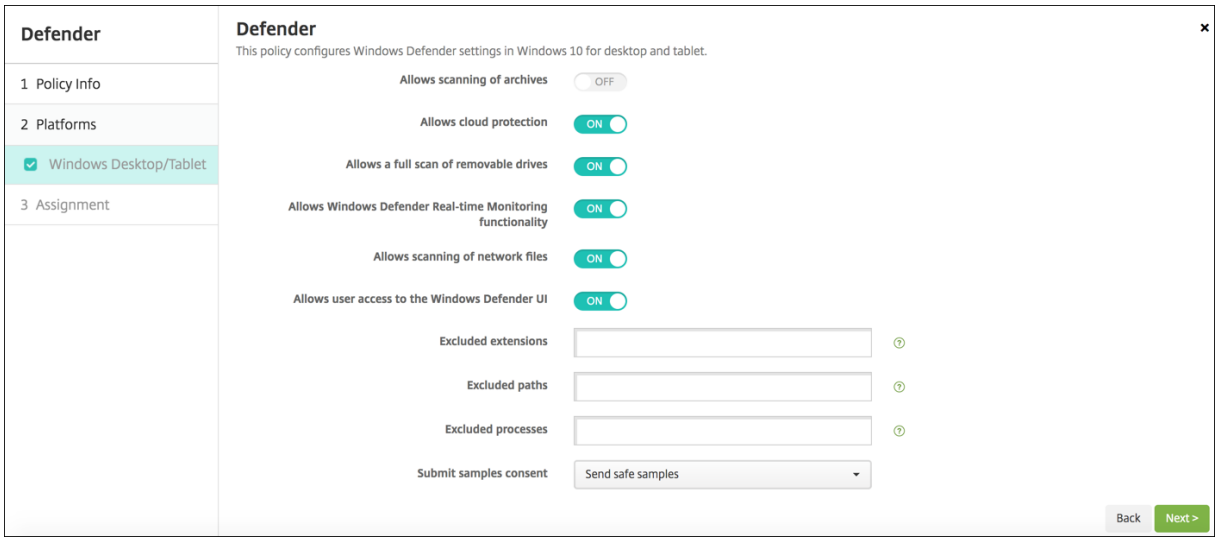
Stratégies d'appareil Defender

January 10, 2022

Windows Defender est une protection contre les logiciels malveillants intégrée à Windows 10 et Windows 11. Vous pouvez utiliser la stratégie d'appareil XenMobile, Defender, pour configurer la stratégie Microsoft Defender pour Windows 10 et Windows 11 pour bureau et tablette.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Windows Desktop et Tablet



- **Permet d'analyser les archives :** autorise ou non Defender à analyser les fichiers archivés. La valeur par défaut est **Désactivé**.
- **Permet de protéger le cloud :** autorise ou non Defender à envoyer des informations relatives aux activités de logiciels malveillants à Microsoft. La valeur par défaut est **Activé**.
- **Permet d'effectuer une analyse complète des lecteurs amovibles :** autorise ou non Defender à analyser les lecteurs amovibles tels que les clés USB. La valeur par défaut est **Activé**.
- **Permet d'utiliser la fonctionnalité d'analyse en temps réel de Windows Defender :** défini par défaut sur **Activé**.
- **Permet d'analyser les fichiers réseau :** autorise ou non Defender à analyser les fichiers réseau. La valeur par défaut est **Activé**.
- **Permet à l'utilisateur d'accéder à l'interface de Windows Defender :** indique si les utilisateurs peuvent accéder à l'interface utilisateur de Windows Defender. Ce paramètre prend effet au prochain démarrage de l'appareil utilisateur. Si ce paramètre est défini sur **Désactivé**, les utilisateurs ne reçoivent aucune notification de Windows Defender. La valeur par défaut est **Activé**.
- **Extensions exclues :** les extensions à exclure des analyses en temps réel ou programmées. Pour séparer les extensions, utilisez le caractère **|**. Par exemple, « lib|obj ».
- **Chemins d'accès exclus :** les chemins à exclure des analyses en temps réel ou programmées. Pour séparer les chemins, utilisez le caractère **|**. Par exemple, « C:\Exemple|C:\Exemple1 ».
- **Processus exclus :** les processus à exclure des analyses en temps réel ou programmées. Pour séparer les processus, utilisez le caractère **|**. Par exemple, « C:\Exemple.exe|C:\Exemple1.exe ».
- **Envoyer échantillons fournis volontairement :** permet de spécifier si vous souhaitez envoyer à Microsoft des fichiers qui peuvent nécessiter une analyse poussée pour déterminer s'ils sont malveillants. Options : **Toujours demander**, **Envoyer des échantillons sécurisés**, **Ne jamais envoyer**, **Envoyer tous les échantillons**. La valeur par défaut est **Envoyer des échantillons sécurisés**.

Stratégie de suppression des fichiers et dossiers

August 20, 2019

Vous pouvez créer une stratégie dans XenMobile pour supprimer des fichiers ou dossiers spécifiques d'appareils Windows Mobile/CE.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Windows Mobile/CE

- **Fichiers et dossiers à supprimer :** pour chaque fichier ou dossier que vous souhaitez supprimer, cliquez sur Ajouter, puis procédez comme suit :
  - **Chemin d'accès :** entrez le chemin d'accès au fichier ou dossier.
  - **Type :** dans la liste, cliquez sur Fichier ou Dossier. La valeur par défaut est Fichier.
  - Cliquez sur **Enregistrer** pour enregistrer le fichier ou dossier, ou cliquez sur **Annuler** pour ne pas enregistrer le fichier ou dossier.

Stratégie de suppression de clés et valeurs de Registre

August 20, 2019

Vous pouvez créer une stratégie dans XenMobile pour supprimer des clés et valeurs de Registre spécifiques d'appareils Windows Mobile/CE.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Windows Mobile/CE

- **Clés et valeurs de Registre à supprimer :** pour chaque clé de Registre et valeur que vous souhaitez supprimer, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Clé :** entrez le chemin de la clé de Registre. Ce champ est obligatoire. Le chemin d'accès doit commencer par HKEY_CLASSES_ROOT\ ou HKEY_CURRENT_USER\ ou HKEY_LOCAL_MACHINE\ ou HKEY_USERS\.
  - **Valeur :** entrez le nom de la valeur à supprimer ou laissez ce champ vide pour supprimer la clé de Registre en entier.
  - Cliquez sur **Enregistrer** pour enregistrer la clé et la valeur, ou cliquez sur **Annuler** pour ne pas enregistrer la clé et la valeur.

Stratégie d'attestation de l'intégrité des appareils

January 10, 2022

Dans XenMobile, vous pouvez exiger que les appareils Windows 10 et Windows 11 communiquent leur état d'intégrité ; pour cela, ces appareils envoient des informations d'exécution et des données spécifiques au service HAS pour analyse. Le service HAS crée et renvoie un certificat d'attestation d'intégrité que l'appareil envoie ensuite à XenMobile. Lorsque XenMobile reçoit le certificat

d'attestation d'intégrité, en fonction du contenu de l'attestation, des actions automatiques que vous avez configurées précédemment peuvent être déployées.

Les données vérifiées par le service HAS sont les suivantes :

- AIK présent ?
- État BitLocker
- Débogage du démarrage activé ?
- Version de la liste de révision du Gestionnaire de démarrage
- Intégrité du code activée ?
- Version de la liste de révision d'intégrité du code
- Stratégie du programme de déploiement d'Apple
- Pilote ELAM chargé ?
- Date d'émission
- Débogage du noyau activé ?
- PCR
- Nombre de réinitialisations
- Nombre de redémarrages
- Mode sans échec activé ?
- Hachage SBCP
- Démarrage sécurisé activé ?
- Signature du test activée ?
- VSM activé ?
- WinPE activé ?

Pour de plus amples informations, reportez-vous à la page Device HealthAttestation CSP de Microsoft.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Pour configurer DHA à l'aide de Microsoft Cloud

Ajoutez une stratégie d'attestation de l'intégrité des appareils et configurez ce paramètre pour chaque plate-forme que vous choisissez :

- **Activer l'attestation de l'intégrité des appareils :** sélectionnez cette option pour exiger l'attestation de l'intégrité des appareils. La valeur par défaut est **Désactivé**.

Pour configurer DHA à l'aide d'un serveur Windows DHA sur site

Pour activer DHA sur site, vous devez d'abord configurer un serveur DHA. Ensuite, vous devez créer une stratégie XenMobile Server pour activer le service DHA sur site.

1. Pour configurer un serveur DHA, installez le rôle de serveur DHA sur une machine exécutant Windows Server 2016 Technical Preview 5 ou version ultérieure. Pour obtenir des instructions, consultez la section sur la configuration d'un serveur d'attestation de l'intégrité des appareils sur site.
2. Ajoutez une stratégie d'attestation de l'intégrité des appareils et configurez ces paramètres :
   - **Activer l'attestation de l'intégrité des appareils :** réglez sur **Activé**.
   - **Configurer Health Attestation Service sur site :** réglez sur **Activé**.
   - **FQDN du serveur DHA sur site :** entrez le nom de domaine complet du serveur DHA que vous avez configuré.
   - **Version de l'API DHA sur site :** sélectionnez la version du service DHA installé sur le serveur DHA.

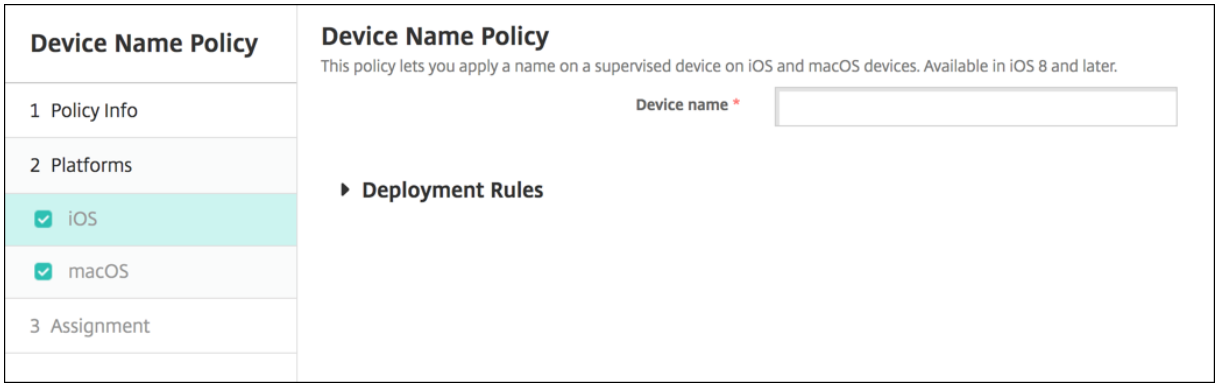
Stratégie de nom d'appareil

January 10, 2022

Vous pouvez définir les noms sur des appareils iOS et macOS, ce qui vous permet d'identifier facilement les appareils. Vous pouvez utiliser des macros et du texte, ou une combinaison des deux pour définir le nom de l'appareil. Par exemple, pour définir le nom de l'appareil à partir du numéro de série de l'appareil, vous devez utiliser ${device.serialnumber}. Pour définir le nom de l'appareil comme la combinaison du nom d'utilisateur et de votre domaine, vous devez utiliser ${user.username}@exemple.com. Pour de plus amples informations sur les macros, consultez la section Macros dans XenMobile.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS et macOS



- **Nom de l'appareil :** entrez la macro, une combinaison de macros, ou une combinaison de macros et de texte pour donner un nom unique à chaque appareil. Par exemple, utilisez ${device.serialnumber} pour définir les noms d'appareil selon leur numéro de série ou utilisez ${device.serialnumber} ${user.username} pour inclure le nom de l'utilisateur dans le nom de l'appareil.

Stratégie Configuration de l'éducation

January 10, 2022

La stratégie Configuration de l'éducation définit les éléments suivants :

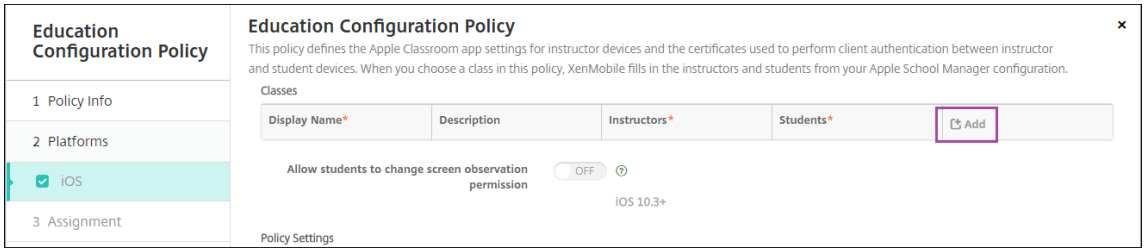
- Les paramètres de l'application En classe d'Apple pour les appareils des enseignants.
- Les certificats utilisés pour effectuer l'authentification du client entre les appareils des enseignants et des élèves.

Lorsque vous choisissez une classe dans cette stratégie, la console XenMobile renseigne les enseignants et les élèves à partir de votre configuration Apple School Manager. Créez une seule stratégie si les paramètres de l'application En salle d'Apple dans cette stratégie sont les mêmes pour toutes les classes.

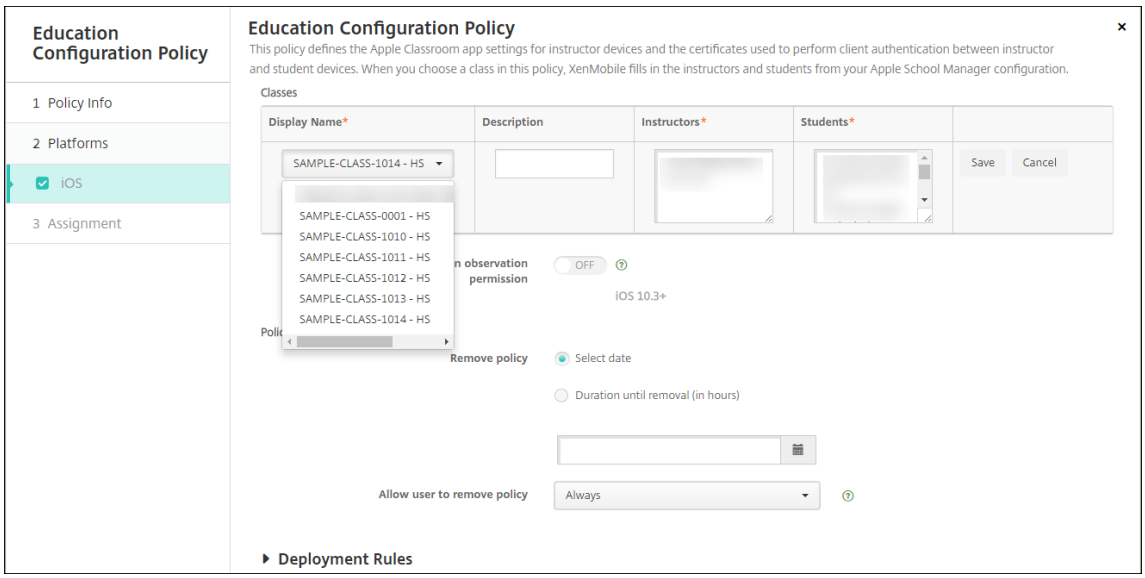
Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

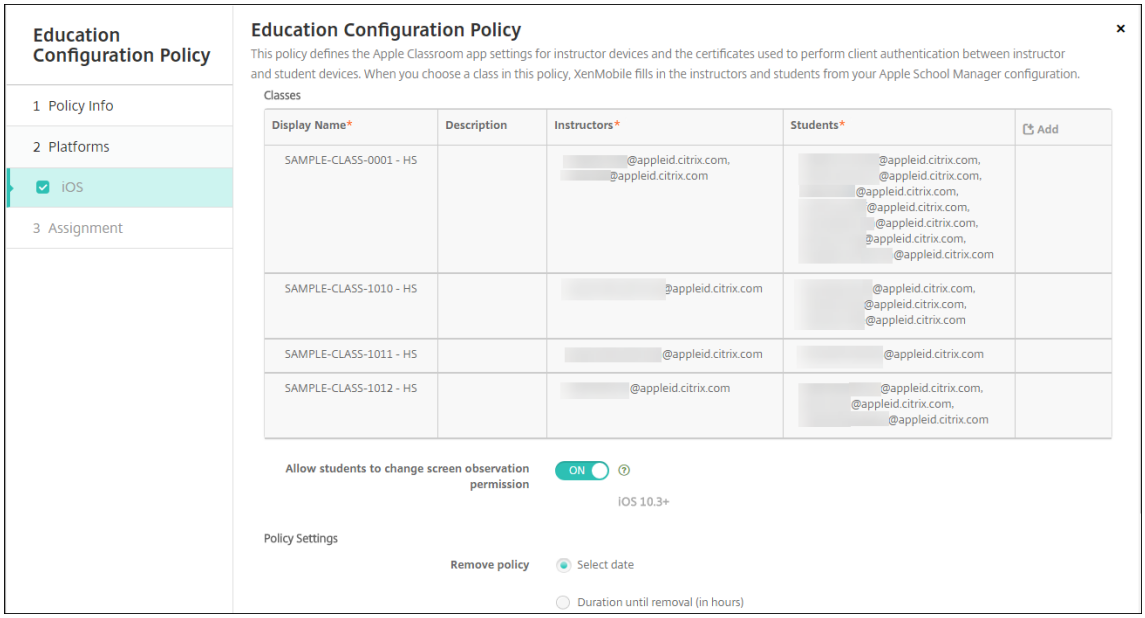
- **Classes :** pour ajouter une classe, cliquez sur **Ajouter**.



Cliquez ensuite sur la liste **Nom d'affichage**. Une liste des classes obtenue à partir de votre compte Apple School Manager connecté s'affiche.



Lorsque vous choisissez une classe dans **Nom d'affichage**, XenMobile renseigne les enseignants et les élèves. Continuez d'ajouter des classes.



- **Autoriser les étudiants à modifier les autorisations d'observation de l'écran :** si cette option est **activée**, les étudiants inscrits dans les classes gérées peuvent choisir d'autoriser leur enseignant à observer les écrans de leurs appareils. La valeur par défaut est **Désactivé**.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique

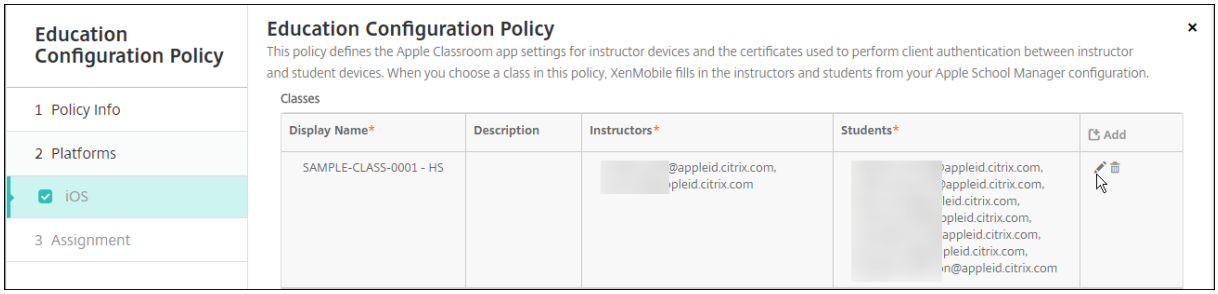
de la suppression.

* **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.

Pour modifier les informations de classe dans la stratégie

Vous pouvez ajouter une description à une classe (« Nom d'affichage » dans l'application En classe). Vous pouvez également ajouter ou supprimer des enseignants et des étudiants. XenMobile n'enregistre pas de telles modifications sur votre compte Apple School Manager. Pour plus d'informations, consultez la section « Gérer les données d'enseignants, d'élèves et de classe » dans Intégration avec les fonctionnalités Apple Éducation.

Placez la souris sur la colonne **Ajouter** pour la classe que vous souhaitez modifier, puis cliquez sur l'icône de crayon.



Pour supprimer une classe de la stratégie, placez la souris sur la colonne **Ajouter** pour la classe que vous souhaitez supprimer, puis cliquez sur l'icône de corbeille.

Stratégie d'hub d'entreprise

October 18, 2019

Une stratégie d'hub d'entreprise pour Windows Phone vous permet de distribuer des applications d'entreprise via le magasin hub d'entreprise.

Avant de pouvoir créer la stratégie, vous avez besoin des éléments suivants :

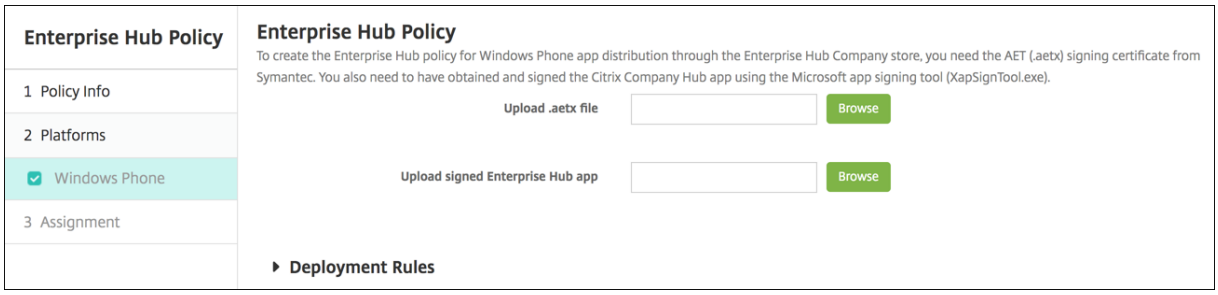
- Un certificat de signature AET (.aetx) de DigiCert
- L'application d'hub d'entreprise Citrix signée à l'aide de l'outil de signature d'applications Microsoft (XapSignTool.exe)

> **Remarque :**
>
> XenMobile prend en charge une seule stratégie d'hub d'entreprise pour un mode Windows Phone Secure Hub. Par exemple, pour télécharger Windows Phone Secure Hub pour XenMobile Enter-

> prise Edition, vous ne devez pas créer de multiples stratégies d'hub d'entreprise avec différentes versions de Worx Home pour XenMobile Enterprise Edition. Vous pouvez uniquement déployer la stratégie d'hub d'entreprise initiale lors de l'inscription de l'appareil.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Windows Phone



- **Charger fichier .aetx :** sélectionnez le fichier .aetx, en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
- **Charger application d'hub d'entreprise signée :** sélectionnez l'application Hub d'entreprise, en cliquant sur **Parcourir** et accédez à l'emplacement de l'application.

Stratégie Exchange

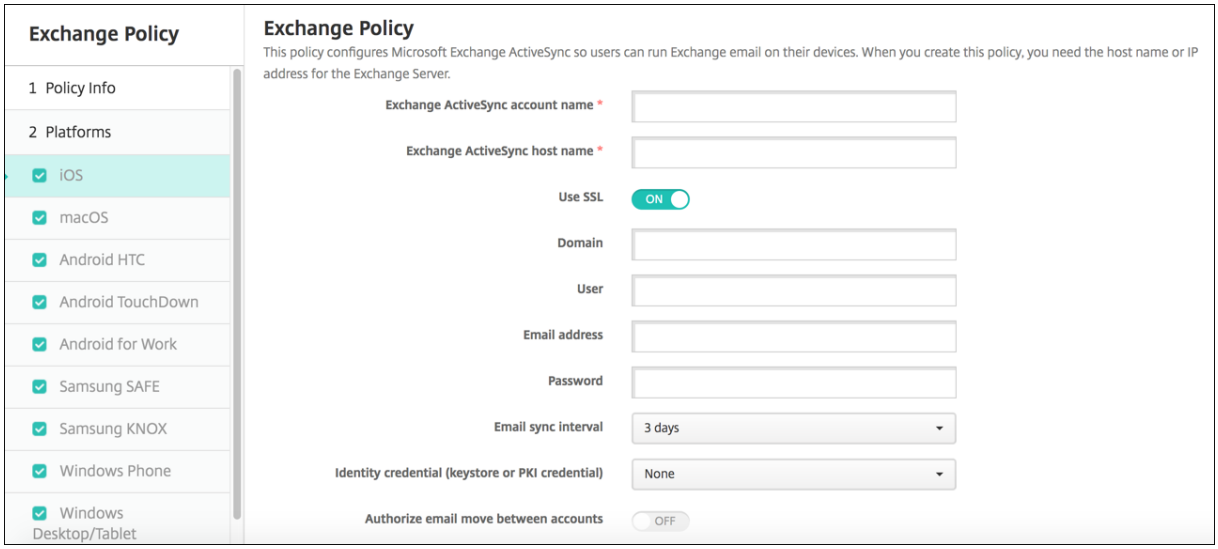
January 10, 2022

Vous pouvez utiliser la stratégie Exchange ActiveSync pour configurer un client de messagerie sur les appareils des utilisateurs pour leur permettre d'accéder à leur messagerie d'entreprise hébergée sur Exchange. Vous pouvez créer des stratégies pour iOS, macOS, Android Enterprise, Samsung SAFE, Samsung KNOX, Windows Phone et Windows Tablet. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans les sections suivantes.

Pour créer cette stratégie, vous avez besoin du nom d'hôte ou de l'adresse IP du serveur Exchange. Pour plus d'informations sur les paramètres ActiveSync, consultez l'article Microsoft ActiveSync CSP.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

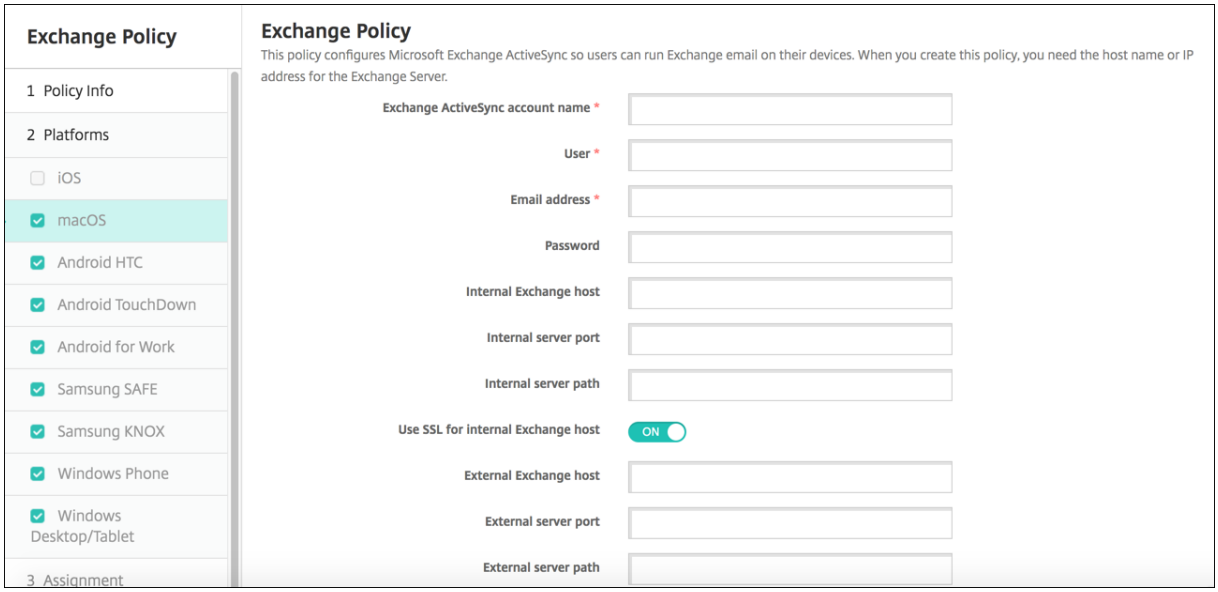


- **Nom du compte Exchange ActiveSync :** entrez la description du compte de messagerie qui est affichée sur les appareils des utilisateurs.
- **Nom d'hôte Exchange ActiveSync :** entrez l'adresse du serveur de messagerie.
- **Utiliser SSL :** sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et le serveur Exchange. La valeur par défaut est **Activé**.
- **Domaine :** entrez le domaine dans lequel réside le serveur Exchange. vous pouvez utiliser la macro système $user.domainname dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
- **Utilisateur :** spécifiez le nom d'utilisateur du compte utilisateur Exchange. vous pouvez utiliser la macro système $user.username dans ce champ pour rechercher automatiquement les noms d'utilisateurs.
- **Adresse e-mail :** spécifiez l'adresse e-mail complète. vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Utiliser OAuth :** si cette option est définie sur **Activé**, la connexion utilise OAuth pour l'authentification. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
- **Mot de passe :** entrez un mot de passe pour le compte utilisateur Exchange. Ce paramètre n'apparaît pas lorsque **Utiliser OAuth** est **activé**.
- **Intervalle de synchronisation des e-mails :** dans la liste, choisissez la fréquence de synchronisation des e-mails avec Exchange Server. La valeur par défaut est **3 jours**.
- **Infos d'identification de l'identité (PKI ou keystore) :** dans la liste, cliquez sur des informations d'identification de l'identité si vous avez configuré un fournisseur d'identités pour XenMobile. Ce champ est requis uniquement lorsque Exchange requiert l'authentification du certificat client. La valeur par défaut est **Aucun**.

- **Autoriser le déplacement des e-mails entre les comptes :** sélectionnez cette option pour autoriser les utilisateurs à déplacer les messages de ce compte vers un autre compte et à transférer des messages et y répondre à partir d'un autre compte. La valeur par défaut est **Désactivé**.
- **N'envoyer le courrier que depuis l'application de messagerie :** sélectionnez cette option si vous voulez que les utilisateurs soient uniquement autorisés à envoyer des e-mails avec l'application de messagerie iOS. La valeur par défaut est **Désactivé**.
- **Désactiver la synchronisation des courriers récents :** sélectionnez cette option pour empêcher les utilisateurs de synchroniser les adresses récentes. La valeur par défaut est **Désactivé**. Cette option s'applique uniquement à iOS 6.0 et versions ultérieures.
- **Activer signature S/MIME :** indiquez si ce compte prend en charge la signature S/MIME. La valeur par défaut est **Activé**. Lorsque la valeur est définie sur **Activé**, les champs suivants apparaissent.
  - **Informations d'identification de l'identité de signature :** choisissez les informations d'identification de signature à utiliser.
  - **Signature S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer et désactiver la signature S/MIME dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
  - **UUID du certificat de signature S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent sélectionner les informations d'identification de signature à utiliser dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
- **Activer chiffrement S/MIME :** sélectionnez cette option si vous souhaitez que ce compte prenne en charge le chiffrement S/MIME. La valeur par défaut est **Désactivé**. Lorsque la valeur est définie sur **Activé**, les champs suivants apparaissent.
  - **Informations d'identification de l'identité de chiffrement :** dans la liste, sélectionnez les informations d'identification de chiffrement à utiliser.
  - **Activer commutateur de chiffrement S/MIME par message :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer ou désactiver le chiffrement S/MIME pour chaque message composé. La valeur par défaut est **Désactivé**.
  - **Chiffrement S/MIME par défaut remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent choisir si S/MIME est activé par défaut dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
  - **UUID du certificat de chiffrement S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer et désactiver l'identité de chiffrement S/MIME dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
- **Paramètres de stratégie**

- **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
  - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres macOS



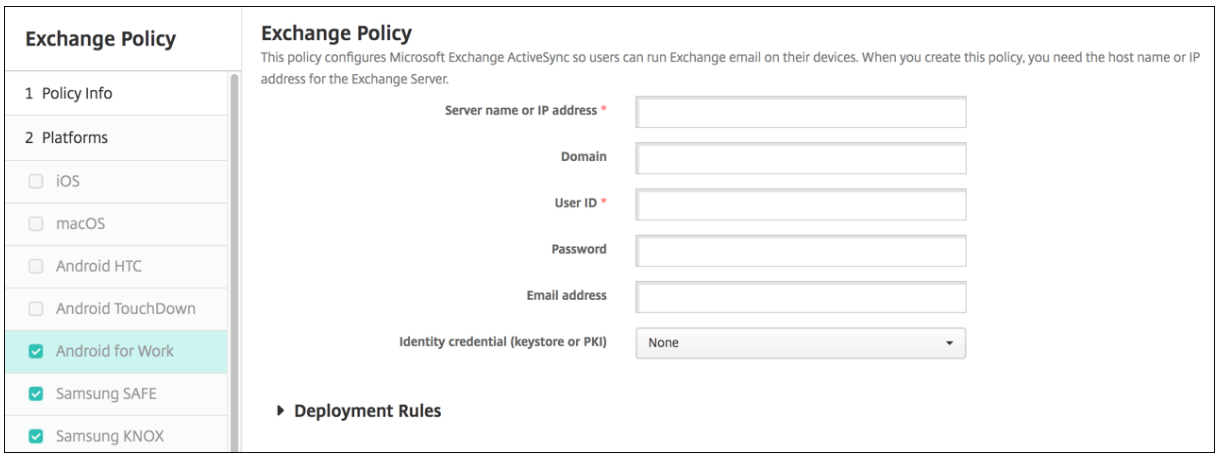
- **Nom du compte Exchange ActiveSync :** entrez la description du compte de messagerie qui est affichée sur les appareils des utilisateurs.
- **Utilisateur :** spécifiez le nom d'utilisateur du compte utilisateur Exchange. vous pouvez utiliser la macro système $user.username dans ce champ pour rechercher automatiquement les noms d'utilisateurs.
- **Adresse e-mail :** spécifiez l'adresse e-mail complète. vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Utiliser OAuth :** si cette option est définie sur **Activé**, la connexion utilise OAuth pour l'authentification. La valeur par défaut est **Désactivé**. Cette option s'applique à macOS 10.14 et versions ultérieures.
- **URL d'authentification OAuth :** spécifie l'URL à charger dans un affichage Web pour l'authentification via OAuth lorsque la détection automatique n'est pas utilisée. Ce champ apparaît lorsque **Utiliser OAuth** est défini sur **Activé**.

- **Mot de passe :** entrez un mot de passe pour le compte utilisateur Exchange. Ce paramètre n'apparaît pas lorsque **Utiliser OAuth** est **activé**.
- **Hôte Exchange interne :** si vous voulez que vos noms d'hôte Exchange interne et externe soient différents, tapez un nom d'hôte Exchange interne (facultatif).
- **Port du serveur interne :** si vous voulez que vos ports de serveur Exchange interne et externe soient différents, tapez un numéro de port Exchange interne (facultatif).
- **Chemin d'accès au serveur interne :** si vous voulez que vos chemins d'accès au serveur Exchange interne et externe soient différents, tapez un chemin d'accès au serveur Exchange interne (facultatif).
- **Utiliser SSL pour l'hôte Exchange interne :** sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et l'hôte Exchange interne. La valeur par défaut est **Activé**.
- **Hôte Exchange externe :** si vous voulez que vos noms d'hôte Exchange interne et externe soient différents, tapez un nom d'hôte Exchange externe (facultatif).
- **Port du serveur externe :** si vous voulez que vos ports de serveur Exchange interne et externe soient différents, tapez un numéro de port Exchange externe (facultatif).
- **Chemin d'accès au serveur externe :** si vous voulez que vos chemins d'accès au serveur Exchange interne et externe soient différents, tapez un chemin d'accès au serveur Exchange externe (facultatif).
- **Utiliser SSL pour l'hôte Exchange externe :** sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et l'hôte Exchange interne. La valeur par défaut est **Activé**.
- **Autoriser Mail Drop :** sélectionnez cette option pour permettre aux utilisateurs de partager sans fil des fichiers entre deux Mac, sans avoir à se connecter à un réseau existant. La valeur par défaut est **Désactivé**.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code**

secret requis ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.

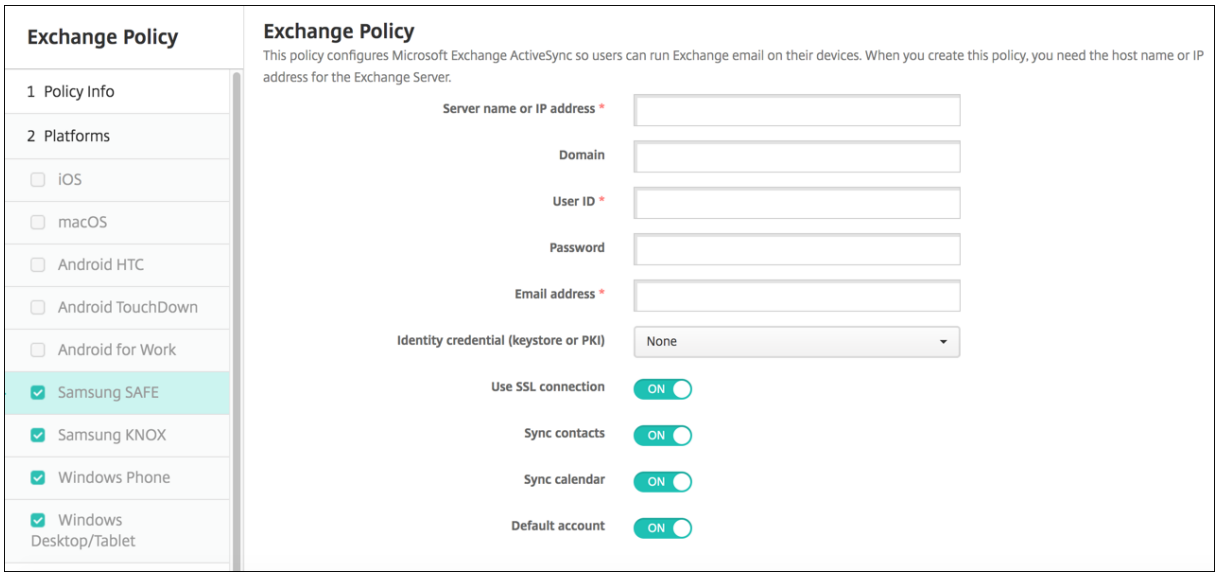
– **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Android Entreprise



- **Nom du serveur ou adresse IP :** entrez le nom d'hôte ou l'adresse IP du serveur Exchange.
- **Domaine :** entrez le domaine dans lequel réside le serveur Exchange. vous pouvez utiliser la macro système $user.domainname dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
- **ID utilisateur :** spécifiez le nom d'utilisateur du compte utilisateur Exchange. vous pouvez utiliser la macro système $user.username dans ce champ pour rechercher automatiquement les noms d'utilisateurs.
- **Mot de passe :** entrez un mot de passe pour le compte utilisateur Exchange.
- **Adresse e-mail :** spécifiez l'adresse e-mail complète. vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Infos d'identification de l'identité (PKI ou keystore) :** dans la liste, cliquez sur des informations d'identification de l'identité si vous avez configuré un fournisseur d'identités pour XenMobile. Ce champ est requis uniquement lorsque Exchange requiert l'authentification du certificat client. La valeur par défaut est **Aucun**.

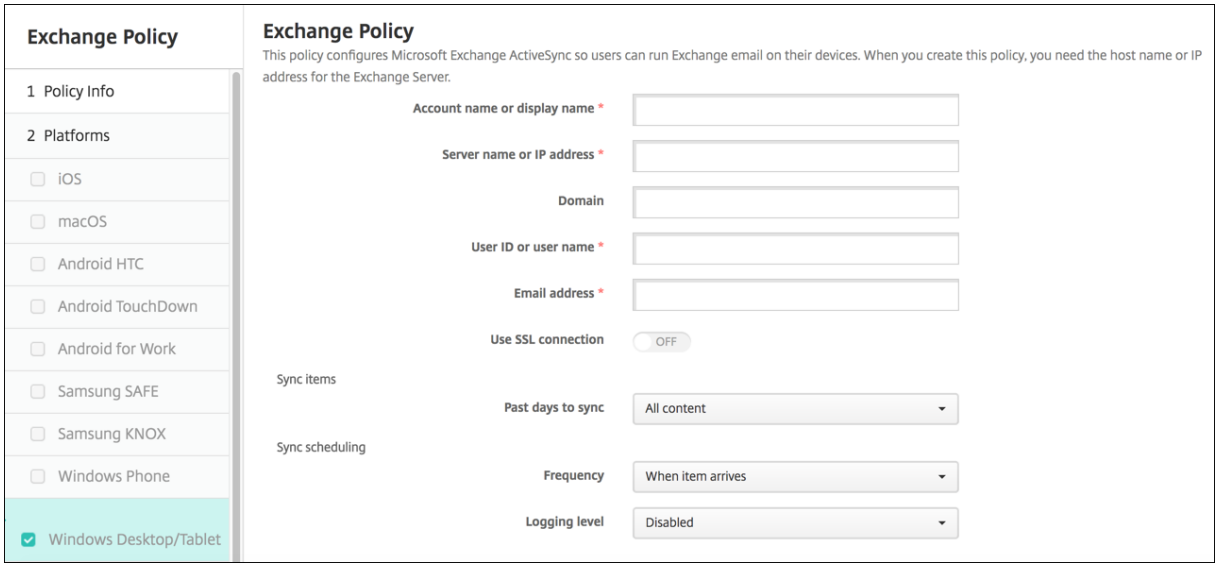
Paramètres Samsung SAFE et Samsung KNOX



- **Nom du serveur ou adresse IP :** entrez le nom d'hôte ou l'adresse IP du serveur Exchange.
- **Domaine :** entrez le domaine dans lequel réside le serveur Exchange. vous pouvez utiliser la macro système $user.domainname dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
- **ID utilisateur :** spécifiez le nom d'utilisateur du compte utilisateur Exchange. vous pouvez utiliser la macro système $user.username dans ce champ pour rechercher automatiquement les noms d'utilisateurs.
- **Mot de passe :** entrez un mot de passe pour le compte utilisateur Exchange.
- **Adresse e-mail :** spécifiez l'adresse e-mail complète. vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Infos d'identification de l'identité (PKI ou keystore) :** dans la liste, cliquez sur des informations d'identification de l'identité si vous avez configuré un fournisseur d'identités pour XenMobile. Ce champ est requis uniquement lorsque Exchange requiert l'authentification du certificat client.
- **Utiliser une connexion SSL :** sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et le serveur Exchange. La valeur par défaut est **Activé**.
- **Synchroniser les contacts :** sélectionnez cette option pour activer la synchronisation des contacts des utilisateurs entre leurs appareils et le serveur Exchange. La valeur par défaut est **Activé**.
- **Synchroniser le calendrier :** sélectionnez cette option pour activer la synchronisation des calendriers des utilisateurs entre leurs appareils et le serveur Exchange. La valeur par défaut est **Activé**.
- **Compte par défaut :** sélectionnez cette option pour faire des comptes Exchange des utilisateurs

le compte par défaut pour l'envoi de courrier électronique à partir de leurs appareils. La valeur par défaut est **Activé**.

Paramètres Windows Phone et Windows Desktop/Tablet



Remarque :

Cette stratégie ne vous permet pas de définir le mot de passe utilisateur. Les utilisateurs doivent définir ce paramètre à partir de leurs appareils après transmission de la stratégie.

- **Nom du compte ou nom d'affichage :** entrez le nom du compte Exchange ActiveSync.
- **Nom du serveur ou adresse IP :** entrez le nom d'hôte ou l'adresse IP du serveur Exchange.
- **Domaine :** entrez le domaine dans lequel réside le serveur Exchange. vous pouvez utiliser la macro système $user.domainname dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
- **ID utilisateur ou nom d'utilisateur :** spécifiez le nom d'utilisateur du compte utilisateur Exchange. vous pouvez utiliser la macro système $user.username dans ce champ pour rechercher automatiquement les noms d'utilisateurs.
- **Adresse e-mail :** spécifiez l'adresse e-mail complète. vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Utiliser une connexion SSL :** sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et le serveur Exchange. La valeur par défaut est **Désactivé**.
- **Contenu à synchroniser :** dans la liste, cliquez sur le nombre de jours à prendre en compte pour synchroniser tout le contenu de l'appareil avec le serveur Exchange. Le paramètre par défaut est **Tout le contenu**.
- **Périodicité :** dans la liste, cliquez sur le calendrier à utiliser lors de la synchronisation des données envoyées à partir du serveur Exchange. La valeur par défaut est **À la réception d'un e-**

mail.

- **Niveau d'enregistrement :** dans la liste, cliquez sur **Désactivé**, **De base** ou **Avancé** pour spécifier le niveau de détail lors de la journalisation des activités Exchange. La valeur par défaut est **Désactivé**.

Stratégie de fichiers

January 10, 2022

Vous pouvez ajouter et déployer des fichiers auxquels les utilisateurs peuvent accéder sur leurs appareils Android et Android Enterprise. Vous spécifiez le répertoire dans lequel vous souhaitez stocker le fichier sur l'appareil. Par exemple, vous souhaitez que les utilisateurs reçoivent un document ou un fichier .pdf d'entreprise. Déployez le fichier sur les appareils et informez les utilisateurs de son emplacement.

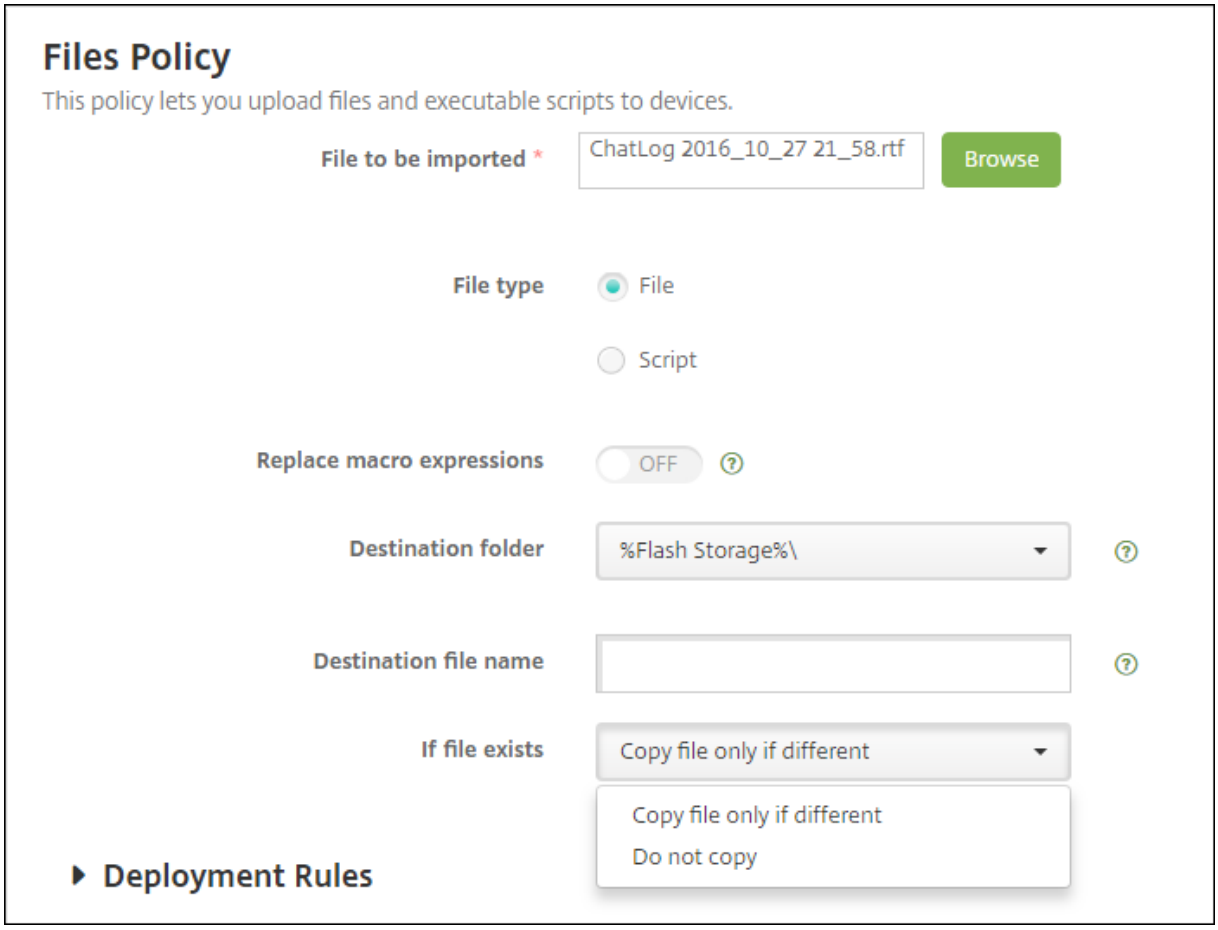
Les appareils Android ne prennent pas en charge l'exécution de scripts en mode natif. Les utilisateurs ont besoin d'un logiciel tiers pour exécuter des scripts.

Vous pouvez ajouter les types de fichiers suivants avec cette stratégie :

- Fichiers texte (.xml, .html, .py, etc.)
- Autres fichiers tels que des documents, images, feuilles de calcul ou présentations
- Pour Windows Mobile and Windows CE uniquement : fichiers de script créés avec MortScript

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Android Enterprise



- **Fichier à importer :** pour sélectionner le fichier à importer, cliquez sur **Parcourir** et accédez à l'emplacement du fichier.
- **Type de fichier :** sélectionnez **Fichier** ou **Script**.
- **Exécuter immédiatement :** lorsque vous sélectionnez **Script**, l'option **Exécuter immédiatement** apparaît. Rien ne se produit lorsque vous activez ce paramètre. Les utilisateurs doivent exécuter le script manuellement. **Substituer les macros :** sélectionnez cette option si vous voulez remplacer les noms des jetons de macro dans un script avec une propriété d'appareil ou d'utilisateur. Pour connaître la syntaxe des macros, reportez-vous à la section Macros. La valeur par défaut est **Désactivé**.
- **Dossier de destination :** dans la liste, sélectionnez l'emplacement dans lequel stocker le fichier chargé ou cliquez sur **Ajouter** pour choisir un emplacement de fichier non répertorié. Vous pouvez utiliser les macros %XenMobile Folder%\ ou %Carte de stockage%\ comme début de chemin d'accès.
- **Nom du fichier de destination :** facultatif. Si vous devez modifier un nom de fichier avant de le déployer sur un appareil, tapez le nom du fichier.
- **Si le fichier existe :** dans la liste, indiquez si vous souhaitez copier un fichier existant. La valeur

par défaut est **Copier le fichier s'ils sont différents**.

Paramètres Android

- **Fichier à importer** : sélectionnez le fichier à importer en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.
- **Type de fichier :** sélectionnez **Fichier** ou **Script**.
- **Exécuter immédiatement :** lorsque vous sélectionnez **Script**, l'option **Exécuter immédiatement** apparaît. Rien ne se produit lorsque vous activez ce paramètre. Les utilisateurs doivent exécuter le script manuellement. **Substituer les macros :** sélectionnez cette option si vous voulez remplacer les noms des jetons de macro dans un script avec une propriété d'appareil ou d'utilisateur. La valeur par défaut est **Désactivé**.
- **Dossier de destination :** dans la liste, sélectionnez l'emplacement dans lequel stocker le fichier chargé ou cliquez sur **Ajouter** pour choisir un emplacement de fichier non répertorié. En outre, vous pouvez utiliser les macros %XenMobile Folder%\ ou %Carte de stockage%\ comme début de chemin d'accès.
- **Nom du fichier de destination :** si vous le souhaitez, entrez un autre nom pour le fichier s'il doit être modifié avant d'être déployé sur un appareil.
- **Copier le fichier s'ils sont différents :** dans la liste, sélectionnez si vous souhaitez copier le fichier s'il est différent du fichier existant. Par défaut, le fichier est copié uniquement s'il est différent.

Paramètres Windows Mobile/CE

- **Fichier à importer :** sélectionnez le fichier à importer en cliquant sur Parcourir et en accédant à l'emplacement du fichier.
- **Type de fichier :** sélectionnez **Fichier** ou **Script**.
- **Exécuter immédiatement :** lorsque vous sélectionnez **Script**, l'option **Exécuter immédiatement** apparaît. Sélectionnez si le script est exécuté dès que le fichier est chargé. La valeur par défaut est **Désactivé**.
- **Substituer les macros :** sélectionnez cette option si vous voulez remplacer les noms des jetons de macro dans un script avec une propriété d'appareil ou d'utilisateur. La valeur par défaut est **Désactivé**.
- **Dossier de destination :** dans la liste, sélectionnez l'emplacement dans lequel stocker le fichier chargé ou cliquez sur **Ajouter** pour choisir un emplacement de fichier non répertorié. En outre, vous pouvez utiliser les macros suivantes comme début de chemin d'accès :
  - %Carte de stockage%\
  - %Dossier Xenmobile%\
  - %Program Files%\
  - %Mes Documents%\

  - %Windows%\
- **Nom du fichier de destination :** si vous le souhaitez, entrez un autre nom pour le fichier s'il doit être modifié avant d'être déployé sur un appareil.
- **Copier le fichier s'ils sont différents :** dans la liste, sélectionnez si vous souhaitez copier le fichier s'il est différent du fichier existant. Par défaut, le fichier est copié uniquement s'il est différent.
- **Fichier en lecture seule :** indiquez si le fichier est en lecture seule. La valeur par défaut est **Désactivé**.
- **Fichier masqué :** indiquez si le fichier ne doit pas être affiché dans la liste de fichiers. La valeur par défaut est **Désactivé**.

Stratégie FileVault

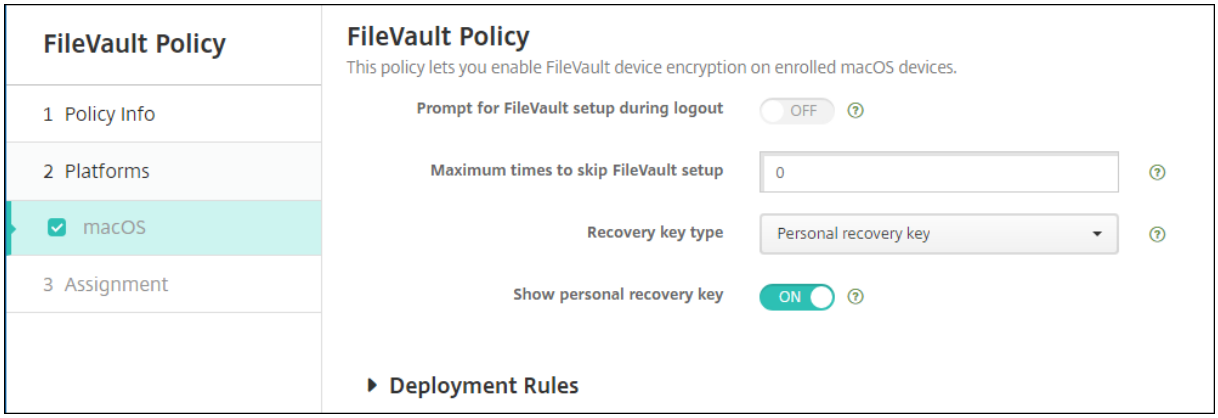
January 10, 2022

La fonctionnalité de cryptage de disque FileVault de macOS protège le volume système en cryptant son contenu. Lorsque FileVault est activé sur un appareil macOS, un utilisateur se connecte avec son mot de passe de compte à chaque démarrage de l'appareil. Si l'utilisateur perd son mot de passe, une clé de récupération (également appelée « clé de secours ») lui permet de déverrouiller le disque et de réinitialiser son mot de passe.

La stratégie XenMobile, FileVault, active les écrans de configuration utilisateur de FileVault et configure les paramètres tels que les clés de récupération. Pour plus d'informations sur FileVault, consultez le site d'assistance Apple https://support.apple.com.

Pour ajouter la stratégie FileVault, accédez à **Configurer > Stratégies d'appareil**.

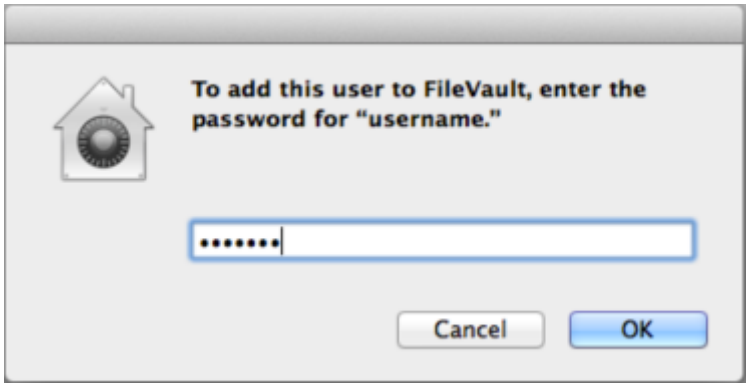
Paramètres macOS



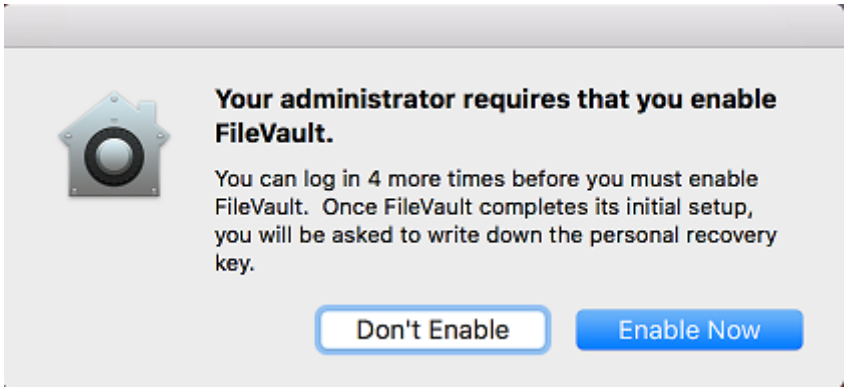
- **Exiger activation de FileVault durant la déconnexion :** si cette option est définie sur **Activé**,

l'utilisateur est invité à activer FileVault au cours des N prochaines déconnexions, comme spécifié par l'option **Nbre max. de fois qu'il est possible d'ignorer l'activation de FileVault**. Si elle est définie sur **Désactivé**, l'invite de mot de passe FileVault ne s'affiche pas.

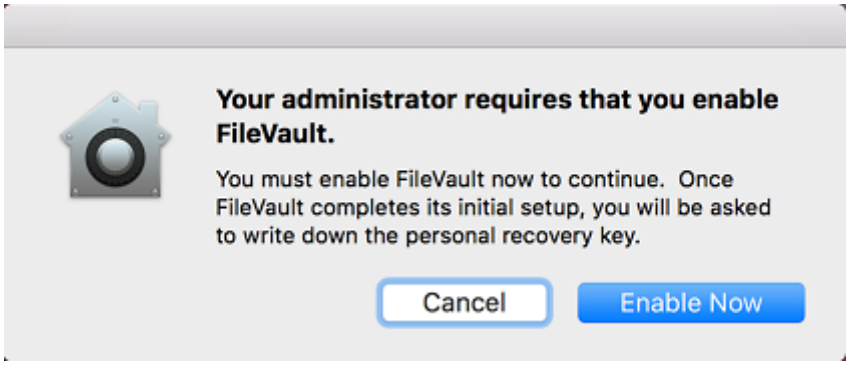
Une fois que vous avez déployé la stratégie FileVault avec ce paramètre activé, l'écran suivant s'affiche lorsqu'un utilisateur se déconnecte de l'appareil. L'écran donne à l'utilisateur l'option d'activer FileVault avant la déconnexion.

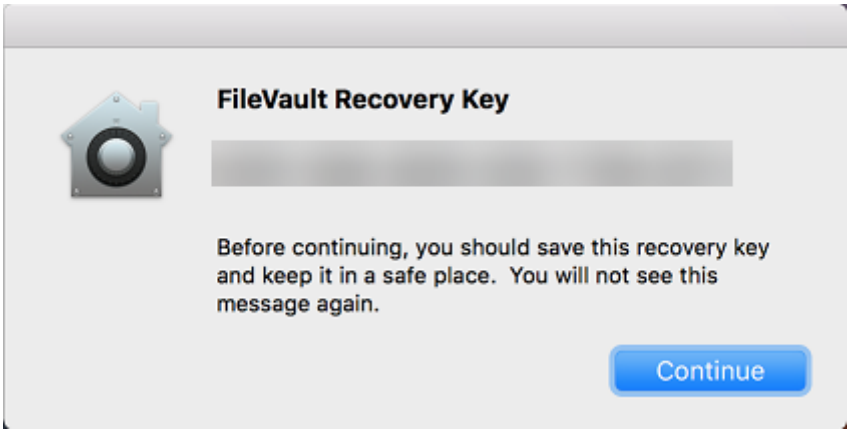


Si la valeur **Nbre max. de fois qu'il est possible d'ignorer l'activation de FileVault** n'est pas définie sur 0 : si vous déployez la stratégie FileVault avec ce paramètre désactivé et que l'utilisateur se connecte, l'écran suivant s'affiche.



Si la valeur **Nbre max. de fois qu'il est possible d'ignorer l'activation de FileVault** est définie sur 0 ou si l'utilisateur a ignoré le nombre maximal de fois, l'écran suivant s'affiche.





Stratégie de police

January 10, 2022

Vous pouvez ajouter une stratégie de police dans XenMobile pour ajouter des polices supplémentaires sur les appareils iOS et macOS. Les polices doivent être de type TrueType (.ttf) ou OpenType (.oft). Les collections de polices (.ttc ou.otc) ne sont pas prises en charge.

Pour iOS, cette stratégie s'applique uniquement à iOS 7.0 et versions supérieures.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Nom visible par l'utilisateur :** entrez le nom que les utilisateurs voient dans leurs listes de polices.
- **Fichier de police :** sélectionnez le fichier de police à ajouter aux périphériques utilisateur en cliquant sur **Parcourir**, puis accédez à l'emplacement du fichier.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres macOS

- **Nom visible par l'utilisateur :** entrez le nom que les utilisateurs voient dans leurs listes de polices.
- **Fichier de police :** sélectionnez le fichier de police à ajouter aux périphériques utilisateur en cliquant sur **Parcourir**, puis accédez à l'emplacement du fichier.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Stratégie Disposition de l'écran d'accueil

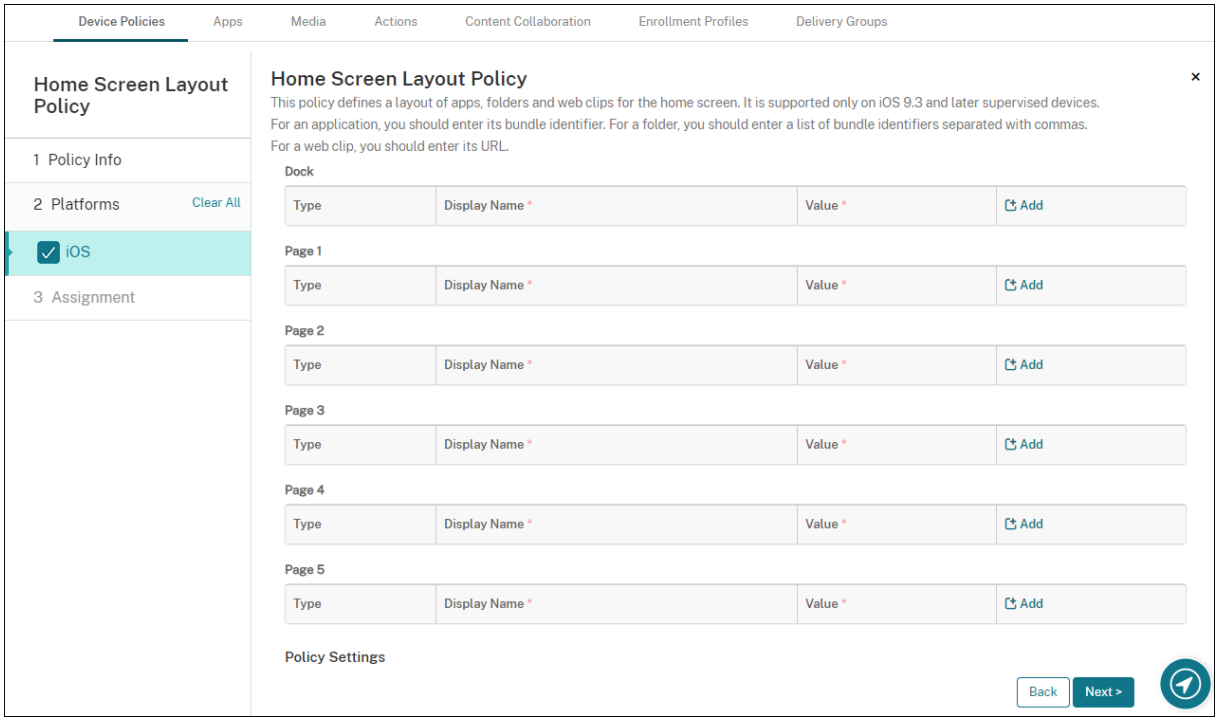
January 10, 2022

Vous pouvez spécifier la disposition des applications et des dossiers pour l'écran d'accueil d'iOS. La stratégie Disposition de l'écran d'accueil est pour les appareils supervisés iOS 9.3 et versions plus récentes.

> **Important :**
>
> Le déploiement de plusieurs stratégies Disposition de l'écran d'accueil sur un appareil entraîne une erreur iOS sur l'appareil. Cette limitation s'applique si vous définissez l'écran d'accueil via cette stratégie XenMobile ou via Apple Configurator.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

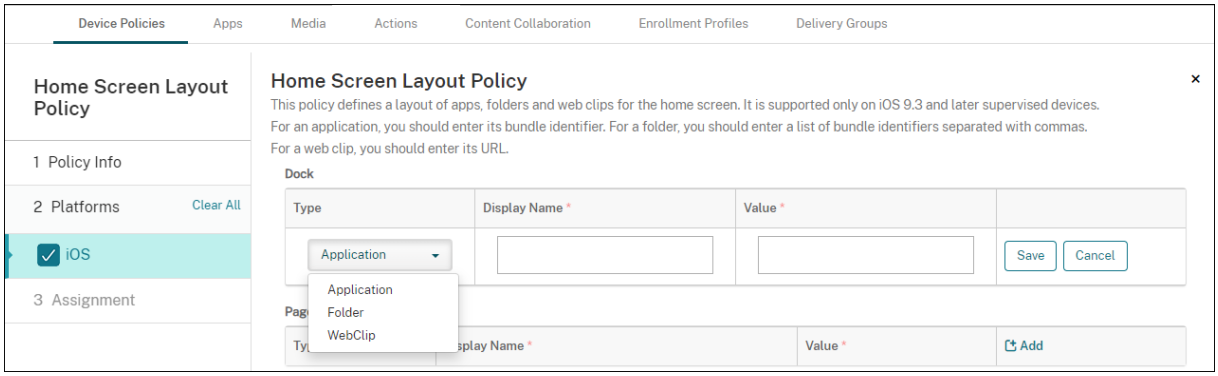
Paramètres iOS



- Pour chacune des zones de l'écran que vous souhaitez configurer (telles que **Dock** ou **Page 1**), cliquez sur **Ajouter**.
- **Type :** choisissez **Application**, **Dossier** ou **Clip Web**.

  Le paramètre **Utilisation restreinte des apps > Autoriser uniquement certaines apps** dans la Stratégie Restrictions peut empêcher les clips Web d'apparaître correctement sur l'écran d'accueil. Pour que les clips Web apparaissent correctement, effectuez l'une des opérations suivantes :

  - Définissez l'option **Utilisation restreinte des apps** sur **Autoriser toutes les applications** ou **Interdire certaines apps**.
  - Si l'option **Utilisation restreinte des apps** est définie sur **Autoriser uniquement certaines apps**, ajoutez une application avec le Bundle ID `com.apple.webapp` pour autoriser les clips Web.



- **Nom d'affichage :** nom qui s'affichera sur l'écran d'accueil pour l'application ou le dossier.
- **Valeur :** pour les applications, entrez le bundle ID. Pour les dossiers, entrez une liste des bundle ID, séparés par des virgules. Pour les clips Web, entrez le bundle ID `com.apple.webClip.managed` et configurez l'URL du clip Web dans la stratégie de clip Web Si plusieurs valeurs de clip Web ont la même URL, le comportement n'est pas défini sur les appareils iOS 11.3 et versions ultérieures.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur iOS 9.3 et versions ultérieures.

Stratégie Importer le profil iOS et macOS

January 10, 2022

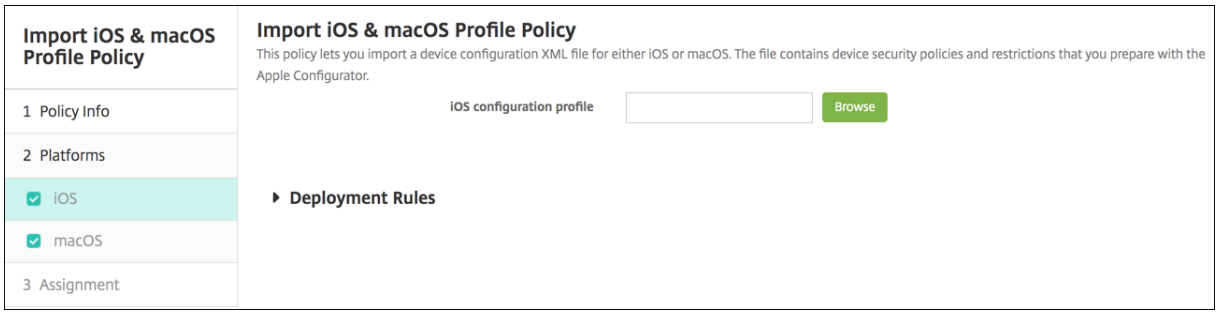
Vous pouvez importer les fichiers XML de configuration d'appareil pour iOS et macOS dans XenMobile. Le fichier contient des stratégies de sécurité et des restrictions que vous préparez avec Apple Configurator.

Vous pouvez placer un appareil iOS en mode supervisé à l'aide de Apple Configurator, comme décrit plus loin dans cet article. Pour de plus amples informations sur l'utilisation d'Apple Configurator pour

créer un fichier de configuration, consultez la page d'aide sur Configurator d'Apple.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS et macOS



- **Profil de configuration iOS** ou **Profil de configuration macOS** : pour sélectionner le fichier de configuration à importer, cliquez sur **Parcourir** et accédez à l'emplacement du fichier.

Placer un appareil iOS en mode supervisé avec Apple Configurator

Pour utiliser Apple Configurator, vous avez besoin d'un ordinateur Apple exécutant macOS 10.7.2 ou version ultérieure.

> **Important :**
>
> Le fait de placer un appareil en mode supervisé installe la version sélectionnée d'iOS sur l'appareil, ce qui efface complètement toutes les données et applications précédemment stockées par l'utilisateur.

1. Installez Apple Configurator depuis iTunes.
2. Connectez l'appareil iOS à votre ordinateur Apple.
3. Démarrez Apple Configurator. Configurator indique que vous possédez un appareil à préparer pour la supervision.
4. Pour préparer l'appareil à des fins de supervision :
    a) Basculer le contrôle de **supervision** sur **Activé**. Citrix vous recommande de sélectionner ce paramètre si vous prévoyez de gérer le contrôle de l'appareil en appliquant à nouveau une configuration régulièrement.
    b) Si vous le souhaitez, entrez un nom pour l'appareil.
    c) Dans iOS, cliquez sur l'option appropriée afin d'obtenir la version **la plus récente** d'iOS que vous souhaitez installer.
5. Lorsque vous êtes prêt à préparer l'appareil pour la supervision, cliquez sur **Préparer**.

Stratégie Gestion du keyguard

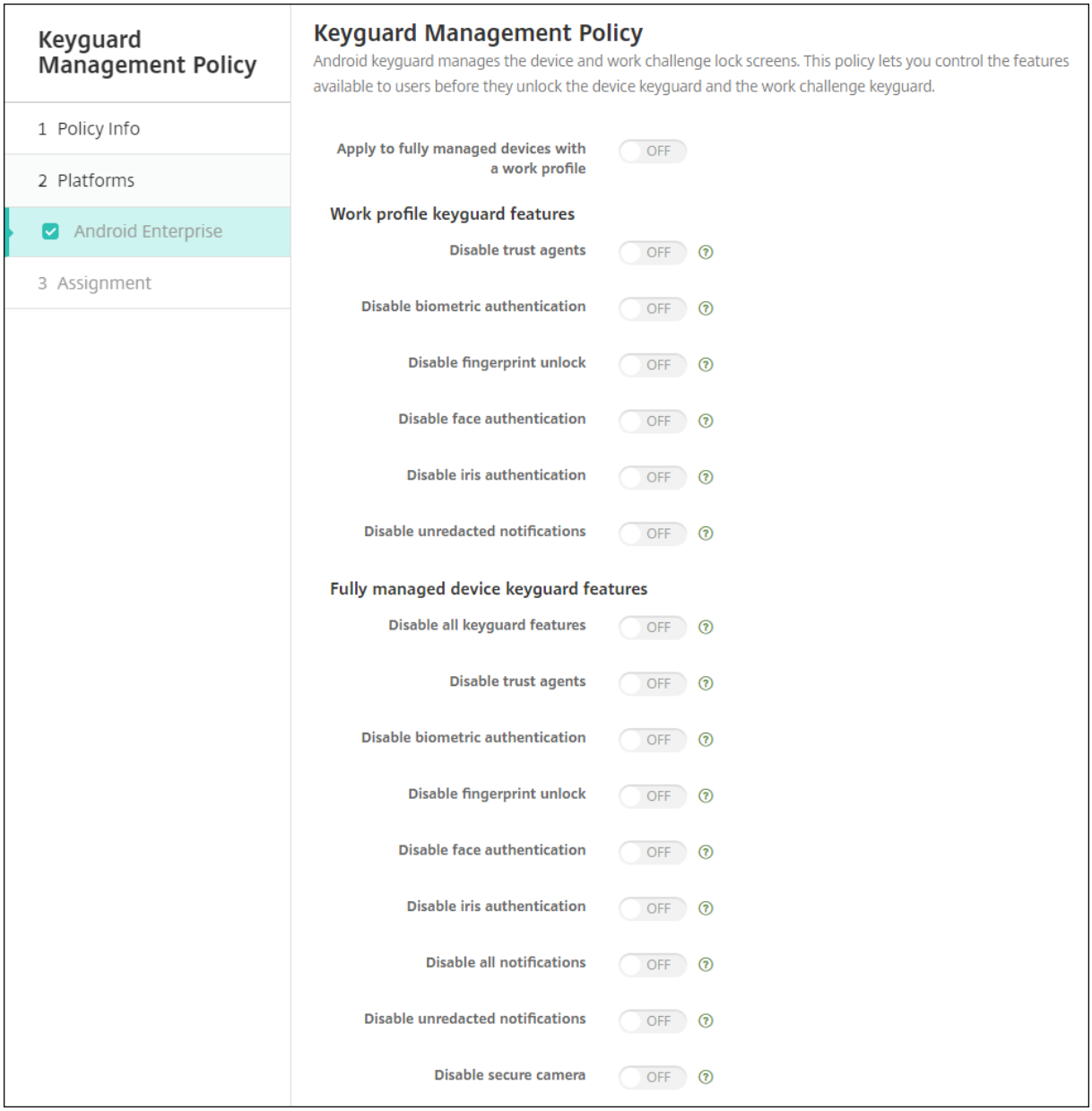
January 10, 2022

Le keyguard Android gère l'appareil et les challenges d'écran de verrouillage des profils professionnels. Cette stratégie vous permet de contrôler les fonctionnalités du keyguard de l'appareil avancé et du keyguard de challenge des profils professionnels Android Entreprise. Vous pouvez contrôler :

- Gestion du keyguard sur les appareils avec profil de travail. Vous pouvez spécifier les fonctionnalités disponibles pour les utilisateurs avant qu'ils déverrouillent le keyguard de l'appareil et le keyguard de challenge professionnel. Par exemple, par défaut, les utilisateurs peuvent utiliser le déverrouillage par empreinte digitale et afficher les notifications non censurées sur l'écran de verrouillage.
- Gestion du keyguard sur des appareils entièrement gérés et dédiés. Vous pouvez spécifier les fonctionnalités disponibles, telles que les agents de confiance et la caméra sécurisée, avant qu'ils déverrouillent l'écran du keyguard. Ou, vous pouvez choisir de désactiver toutes les fonctionnalités du keyguard.
- Gestion des Keyguard sur des appareils entièrement gérés avec profil de travail. Vous pouvez utiliser une stratégie Gestion du keyguard pour appliquer des paramètres distincts à l'appareil et au profil de travail.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Android Enterprise



- **Appliquer aux appareils entièrement gérés dotés d'un profil professionnel :** permet de configurer les paramètres de stratégie Gestion du keyguard pour les appareils entièrement gérés avec profil de travail.

  Lorsque ce paramètre est **activé**, vous pouvez appliquer des paramètres distincts à l'appareil et au profil de travail sur les appareils entièrement gérés avec profil de travail.

  Lorsque ce paramètre est **Désactivé**, vous pouvez appliquer des paramètres aux appareils avec profil de travail ou aux appareils entièrement gérés. Les paramètres que vous configurez pour les profils de travail ne s'appliquent qu'aux appareils avec profil de travail. Les paramètres que

vous configurez pour les appareils entièrement gérés ne s'appliquent qu'aux appareils entièrement gérés.

La valeur par défaut est **Désactivé**.

- **Fonctionnalités keyguard du profil de travail :** contrôle si les fonctions suivantes sont disponibles avant qu'un utilisateur déverrouille le keyguard du profil de travail (écran de verrouillage).
  - **Désactiver les agents de confiance :** si cette option est **désactivée**, les agents de confiance peuvent opérer sur des écrans de keyguard sécurisés lorsqu'un challenge est défini sur le profil de travail. Définissez l'option sur **Activé** pour désactiver tous les agents de confiance du profil de travail. La valeur par défaut est **Désactivé**.
  - **Désactiver authentification biométrique :** si **Désactivé** est sélectionné, l'authentification biométrique est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur le profil de travail. Définissez cette option sur **Activé** pour désactiver l'authentification biométrique sur le profil de travail. Ce paramètre désactive le déverrouillage par empreinte digitale, l'authentification du visage et l'authentification de l'iris. La valeur par défaut est **Désactivé**. Pour Android 9.0 et versions ultérieures.
  - **Désactiver le déverrouillage par empreinte digitale :** si cette option est **activée**, le déverrouillage par empreinte digitale n'est pas disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur le profil de travail. Définissez l'option sur **Désactivé** pour activer le déverrouillage par empreinte digitale sur le profil de travail. La valeur par défaut est **Désactivé**.
  - **Désactiver authentification du visage :** si **Désactivé** est sélectionné, l'authentification du visage est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur le profil de travail. Définissez cette option sur **Activé** pour désactiver l'authentification du visage sur le profil de travail. La valeur par défaut est **Désactivé**. Pour Android 9.0 et versions ultérieures.
  - **Désactiver authentification de l'iris :** si **Désactivé** est sélectionné, l'authentification de l'iris est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur le profil de travail. Définissez cette option sur **Activé** pour désactiver l'authentification de l'iris sur le profil de travail. La valeur par défaut est **Désactivé**. Pour Android 9.0 et versions ultérieures.
  - **Désactiver les notifications non censurées :** si cette option est définie sur **Désactivé**, les notifications censurées et non censurées apparaissent sur les écrans de keyguard sécurisés. Définissez cette option sur **Activé** pour désactiver les notifications non censurées et afficher uniquement les notifications censurées. La valeur par défaut est **Désactivé**.
- **Fonctionnalités keyguard d'appareil entièrement géré :** contrôle si les fonctions suivantes sont disponibles avant qu'un utilisateur déverrouille le keyguard d'appareil (écran de verrouil-

lage). Ces fonctionnalités s'appliquent aux appareils entièrement gérés ou dédiés.

- **Désactiver toutes les fonctionnalités du keyguard :** si cette option est **désactivée**, toutes les personnalisations actuelles et futures de keyguard seront disponibles sur les écrans de keyguard sécurisés. Définissez sur **Activé** pour désactiver toutes les personnalisations de keyguard. La valeur par défaut est **Désactivé**.
- **Désactiver les agents de confiance :** si cette option est **désactivée**, les agents de confiance peuvent opérer sur des écrans de keyguard sécurisés. Définissez sur **Activé** pour désactiver les agents de confiance. La valeur par défaut est **Désactivé**.
- **Désactiver authentification biométrique :** si **Désactivé** est sélectionné, l'authentification biométrique est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur l'appareil. Définissez cette option sur **Activé** pour désactiver l'authentification biométrique sur l'appareil. Ce paramètre désactive le déverrouillage par empreinte digitale, l'authentification du visage et l'authentification de l'iris. La valeur par défaut est **Désactivé**. Pour Android 9.0 et versions ultérieures.
- **Désactiver le déverrouillage par empreinte digitale :** si cette option est **désactivée**, le déverrouillage par empreinte digitale est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur l'appareil. Définissez l'option sur **Activé** pour désactiver le déverrouillage par empreinte digitale sur l'appareil. La valeur par défaut est **Désactivé**.
- **Désactiver authentification du visage :** si **Désactivé** est sélectionné, l'authentification du visage est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur l'appareil. Définissez cette option sur **Activé** pour désactiver l'authentification du visage sur l'appareil. La valeur par défaut est **Désactivé**. Pour Android 9.0 et versions ultérieures.
- **Désactiver authentification de l'iris :** si **Désactivé** est sélectionné, l'authentification de l'iris est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur l'appareil. Définissez cette option sur **Activé** pour désactiver l'authentification de l'iris sur l'appareil. La valeur par défaut est **Désactivé**. Pour Android 9.0 et versions ultérieures.
- **Désactiver toutes les notifications :** si cette option est **désactivée**, toutes les notifications apparaissent sur les écrans de keyguard sécurisés. Définissez l'option sur **Activé** pour afficher toutes les notifications. La valeur par défaut est **Désactivé**.
- **Désactiver les notifications non censurées :** si cette option est définie sur **Désactivé**, les notifications censurées et non censurées apparaissent sur les écrans de keyguard sécurisés. Définissez cette option sur **Activé** pour désactiver les notifications non censurées et afficher uniquement les notifications censurées. La valeur par défaut est **Désactivé**.
- **Désactiver la caméra sécurisée :** si cette option est **désactivée**, la caméra sécurisée est disponible sur les écrans de keyguard sécurisés. Définissez l'option sur **Activé** pour désactiver la caméra sécurisée. La valeur par défaut est **Désactivé**.

Stratégie kiosque

January 10, 2022

La stratégie Kiosque vous permet de restreindre les appareils au mode Kiosque en limitant les applications pouvant s'exécuter. XenMobile ne contrôle pas quelle partie de l'appareil se verrouille en mode Kiosque. L'appareil gère les paramètres du mode Kiosque une fois la stratégie déployée.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Pour placer un appareil Samsung SAFE en mode kiosque

1. Activez la clé d'API Samsung SAFE sur l'appareil mobile, comme décrit dans la section Stratégies de clé de licence MDM Samsung. Cette étape vous permet d'activer des stratégies sur des appareils Samsung SAFE.
2. Activez Firebase Cloud Messaging pour les appareils Android, comme décrit dans la section Firebase Cloud Messaging. Cette étape permet aux appareils Android de se connecter à XenMobile.
3. Ajoutez une stratégie kiosque, comme décrit dans la section suivante.
4. Attribuez ces trois stratégies aux groupes de mise à disposition appropriés. Déterminez si vous souhaitez inclure d'autres stratégies, telles que Inventaire des applications, à ces groupes de mise à disposition.

   Pour supprimer les appareils du mode kiosque ultérieurement, créez une stratégie kiosque pour laquelle le **mode kiosque** est défini sur **Désactiver**. Mettez à jour les groupes de mise à disposition pour supprimer la stratégie kiosque qui activait le mode kiosque et pour ajouter la stratégie kiosque qui désactive le mode kiosque.

Pour ajouter une stratégie kiosque

Toutes les applications que vous spécifiez pour le mode kiosque doivent déjà être installées sur les appareils des utilisateurs.

Certaines options ne s'appliquent qu'à l'API Samsung Mobile Device Management (MDM) 4.0 et versions ultérieures.

Paramètres Samsung SAFE

Vous pouvez spécifier que seules certaines applications peuvent être utilisées. Cette stratégie est utile pour les appareils d'entreprise conçus pour n'exécuter qu'un type spécifique ou une classe

d'applications. Cette stratégie vous permet également de choisir des images personnalisées à utiliser comme fond d'écran de l'écran d'accueil et de l'écran de verrouillage lorsque l'appareil est en mode Kiosque.

- **Mode kiosque :** cliquez sur **Activer** ou **Désactiver**. La valeur par défaut est **Activer**. Lorsque vous cliquez sur **Désactiver**, toutes les options suivantes disparaissent.
- **Paquetage du Launcher :** Citrix vous recommande de laisser ce champ vide si vous avez développé un lanceur interne pour permettre aux utilisateurs d'ouvrir l'application ou les applications kiosque. Si vous utilisez un lanceur interne, entrez le nom complet du paquetage de l'application du lanceur.
- **Téléphone d'urgence :** entrez un numéro de téléphone (facultatif). Toute personne peut utiliser ce numéro pour contacter votre société pour trouver un appareil perdu. S'applique uniquement à MDM 4.0 et versions ultérieures.
- **Autoriser la barre de navigation :** sélectionnez cette option pour permettre aux utilisateurs de voir et utiliser la barre de navigation en mode Kiosque. S'applique uniquement à MDM 4.0 et versions ultérieures. La valeur par défaut est **Activé**.
- **Autoriser le mode multi-fenêtre :** sélectionnez cette option pour permettre aux utilisateurs d'utiliser plusieurs fenêtres en mode Kiosque. S'applique uniquement à MDM 4.0 et versions ultérieures. La valeur par défaut est **Activé**.
- **Autoriser la barre d'état :** sélectionnez cette option pour permettre aux utilisateurs de voir la barre d'état en mode Kiosque. S'applique uniquement à MDM 4.0 et versions ultérieures. La valeur par défaut est **Activé**.
- **Autoriser la barre système :** sélectionnez cette option pour permettre aux utilisateurs de voir la barre système en mode Kiosque. La valeur par défaut est **Activé**.
- **Autoriser le gestionnaire de tâches :** sélectionnez cette option pour permettre aux utilisateurs de voir et utiliser le gestionnaire de tâches en mode Kiosque. La valeur par défaut est **Activé**.
- **Changer code secret SAFE :** ce paramètre permet de se protéger contre les modifications accidentelles du champ Code secret SAFE. Lorsque ce paramètre est **désactivé**, vous ne pouvez pas modifier le champ Code secret SAFE. La valeur par défaut est **Désactivé**.
- **Code secret SAFE :** si vous avez défini une stratégie de code secret générale pour tous les appareils Samsung SAFE, entrez ce code facultatif dans ce champ.
- **Fonds d'écran**
  - **Définir un fond d'écran accueil :** sélectionnez cette option pour utiliser une autre image personnalisée pour l'écran d'accueil en mode Kiosque. La valeur par défaut est **Désactivé**.
    - **Image accueil :** lorsque vous activez **Définir un fond d'écran accueil**, sélectionnez le fichier d'image en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.
  - **Définir un fond d'écran verrou :** sélectionnez cette option pour utiliser une autre image personnalisée pour l'écran de verrouillage en mode Kiosque. La valeur par défaut est **Désactivé**. S'applique uniquement à MDM 4.0 et versions ultérieures.
    - **Image verrou :** lorsque vous activez **Définir un fond d'écran verrou**, sélectionnez le

fichier d'image en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.

- **Applications :** pour chaque application que vous souhaitez ajouter au mode kiosque, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nouvelle application à ajouter :** entrez le nom complet de l'application à ajouter. Par exemple, com.android.calendar permet aux utilisateurs d'utiliser l'application calendrier d'Android.
  - Cliquez sur **Enregistrer** pour ajouter l'application, ou cliquez sur **Annuler** pour annuler l'ajout de l'application.

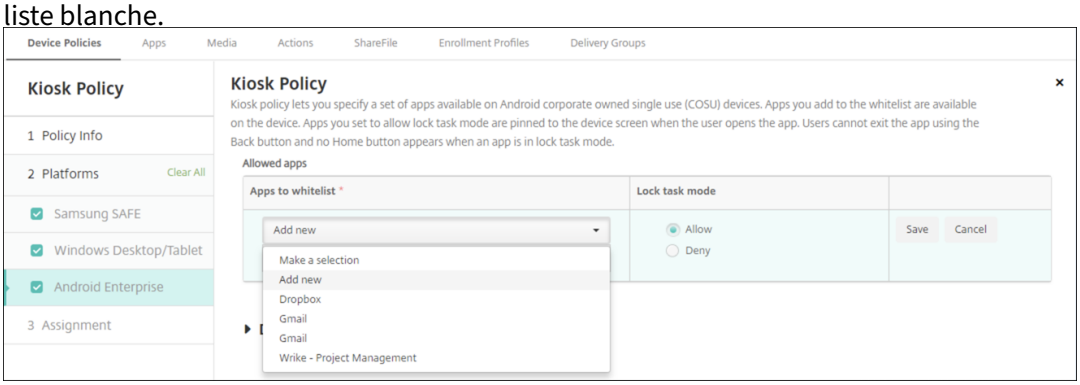
Paramètres Android Enterprise

Vous pouvez autoriser des applications et définir le mode de verrouillage des tâches pour les appareils Android Enterprise dédiés, également appelés appareils d'entreprise à usage unique (COSU). Par défaut, les services Secure Hub et Google Play sont ajoutés à la liste d'autorisation.

Pour autoriser une application, cliquez sur **Ajouter**. Vous pouvez autoriser plusieurs applications. Pour plus d'informations, consultez la section Android Enterprise.

> **Remarque :**
>
> La console XenMobile Server utilise les termes « liste noire » et « liste blanche ». Ces termes seront modifiés dans une prochaine version et les termes « liste de blocage » et « liste d'autorisation » les remplaceront.

- **Applications sur liste blanche :** saisissez le nom de package de l'application que vous souhaitez ajouter à la liste blanche ou sélectionnez son nom dans la liste.
  - Cliquez sur **Ajouter** pour entrer le nom de package de l'application à afficher dans la liste.
  - Sélectionnez l'application existante dans la liste. La liste affiche les applications chargées sur XenMobile Server. Par défaut, les services Secure Hub et Google Play sont ajoutés à la liste blanche.



- **Mode de verrouillage des tâches :** choisissez **Autoriser** pour que l'application soit épinglée sur l'écran de l'appareil lorsque l'utilisateur démarre l'application. Choisissez **Refuser** pour que l'application ne soit pas épinglée. Par défaut, les services Secure Hub et Google Play sont autorisés. La valeur par défaut est **Autoriser**.

Lorsqu'une application est en mode de verrouillage des tâches, elle est épinglée sur l'écran de l'appareil lorsque l'utilisateur l'ouvre. Aucun bouton d'accueil n'apparaît et le bouton Retour est désactivé. L'utilisateur quitte l'application à l'aide d'une action programmée dans l'application, comme la déconnexion.

Stratégie de configuration du Launcher

September 22, 2021

Citrix Launcher vous permet de personnaliser l'expérience de l'utilisateur pour les appareils Android déployés par XenMobile. Citrix Launcher et la stratégie de configuration du Launcher ne sont pas compatibles avec Android Enterprise.

Vous pouvez ajouter une stratégie de configuration du Launcher pour contrôler ces fonctionnalités de Citrix Launcher :

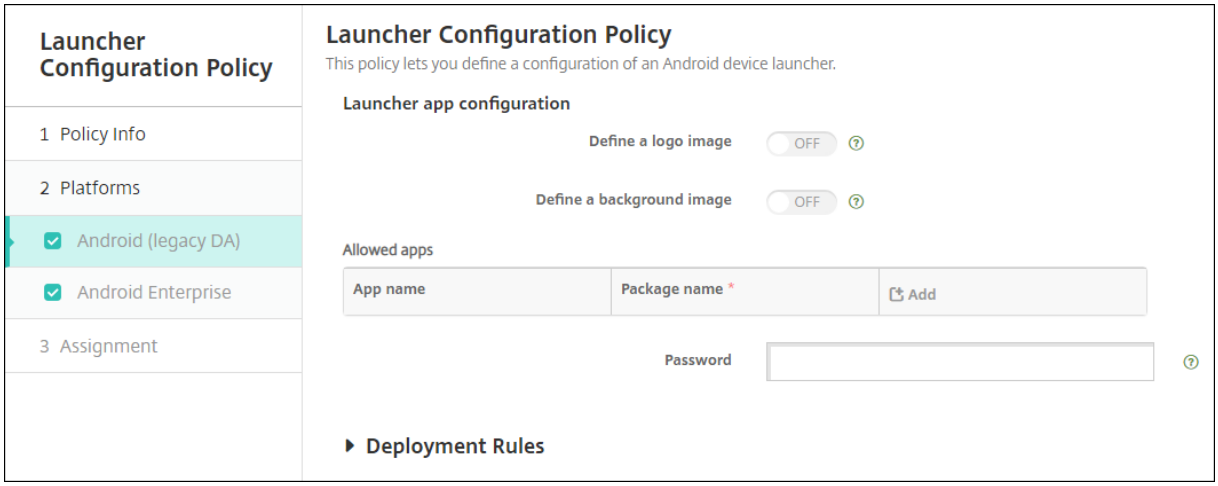
- Gérez les appareils Android, de façon à ce que les utilisateurs puissent uniquement accéder aux applications que vous spécifiez.
- Si vous le souhaitez, vous pouvez spécifier une image de logo personnalisé pour l'icône Citrix Launcher et une image d'arrière-plan personnalisée pour Citrix Launcher.
- Spécifiez un mot de passe que les utilisateurs doivent entrer pour quitter le Launcher.

Si Citrix Launcher vous permet d'appliquer ces restrictions sur l'appareil, il donne aux utilisateurs la flexibilité opérationnelle dont ils ont besoin via un accès intégré à des paramètres de l'appareil tels que les paramètres Wi-Fi, les réglages Bluetooth et les paramètres de code secret de l'appareil. Citrix Launcher n'est pas destiné à être une couche de sécurité supplémentaire venant s'ajouter à ce que la plate-forme de l'appareil offre déjà.

Lorsque vous déployez Citrix Launcher, XenMobile l'installe et il remplace le Launcher Android par défaut.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Android (ancien administrateur de l'appareil) et Android Enterprise



- **Définir une image de logo :** indiquez si vous souhaitez utiliser une image de logo personnalisé pour l'icône Citrix Launcher. La valeur par défaut est **Désactivé**.
- **Image du logo :** lorsque vous activez **Définir une image de logo**, sélectionnez le fichier d'image en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier. Les types de fichier pris en charge sont PNG, JPG, JPEG et GIF.
- **Définir une image d'arrière-plan :** indiquez si vous souhaitez utiliser une image personnalisée pour l'arrière-plan de Citrix Launcher. La valeur par défaut est **Désactivé**.
- **Image d'arrière-plan :** lorsque vous activez **Définir une image d'arrière-plan**, sélectionnez le fichier d'image en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier. Les types de fichier pris en charge sont PNG, JPG, JPEG et GIF.
- **Applications autorisées :** pour chaque application que vous souhaitez autoriser dans Citrix Launcher, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nouvelle application à ajouter :** entrez le nom complet de l'application à ajouter. Par exemple, com.android.calendar pour l'application calendrier d'Android.
  - Cliquez sur **Enregistrer** pour ajouter l'application, ou cliquez sur **Annuler** pour annuler l'ajout de l'application.
- **Mot de passe :** le mot de passe qu'un utilisateur doit entrer pour quitter Citrix Launcher.

Stratégie LDAP

January 10, 2022

Vous créez une stratégie LDAP pour appareils iOS dans XenMobile pour fournir des informations sur un serveur LDAP à utiliser, y compris toute information sur le compte nécessaires. La stratégie fournit également un ensemble de stratégies de recherche LDAP à utiliser lors de l'interrogation du serveur LDAP.

Vous devez utiliser le nom d'hôte LDAP avant de configurer cette stratégie.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Description du compte :** entrez une description du compte(facultatif).
- **Nom d'utilisateur du compte :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe du compte :** entrez un mot de passe (facultatif). Utilisez ce champ uniquement avec des profils chiffrés.
- **Nom d'hôte LDAP :** entrez le nom d'hôte du serveur LDAP. Ce champ est obligatoire.
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur LDAP. La valeur par défaut est **Activé**.
- **Paramètres de recherche :** ajoutez les paramètres de recherche à utiliser lors de l'interrogation du serveur LDAP. vous pouvez entrer autant de paramètres de recherche que vous voulez, mais vous devez ajouter au moins un paramètre de recherche pour faire du compte une ressource utile. Cliquez sur **Ajouter**, puis procédez comme suit :
  - **Description :** entrez une description pour le paramètre de recherche. Ce champ est obligatoire.
  - **Portée :** choisissez **Base**, **Un niveau** ou **Sous-arborescence** pour définir la profondeur de la recherche dans l'arborescence LDAP. La valeur par défaut est **Base**.
    - **Base** recherche le nœud indiqué par la Base de recherche.
    - **Un niveau** recherche le nœud Base et un niveau en dessous.
    - **Sous-arborescence** recherche le nœud Base, ainsi que tous ses enfants, quelle que soit la profondeur.
  - **Base de recherche :** entrez le chemin d'accès au nœud à partir duquel démarrer une recherche. Par exemple, ou=people ou 0=example corp. Ce champ est obligatoire.
  - Cliquez sur **Ajouter** pour ajouter le paramètre de recherche ou cliquez sur **Annuler** pour annuler l'ajout du paramètre de recherche.
  - Répétez ces étapes pour chaque paramètre de recherche à ajouter.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres macOS

- **Description du compte :** entrez une description du compte(facultatif).
- **Nom d'utilisateur du compte :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe du compte :** entrez un mot de passe (facultatif). Utilisez ce champ uniquement avec des profils chiffrés.
- **Nom d'hôte LDAP :** entrez le nom d'hôte du serveur LDAP. Ce champ est obligatoire.
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur LDAP. La valeur par défaut est **Activé**.
- **Paramètres de recherche :** ajoutez les paramètres de recherche à utiliser lors de l'interrogation du serveur LDAP. vous pouvez entrer autant de paramètres de recherche que vous voulez, mais vous devez ajouter au moins un paramètre de recherche pour faire du compte une ressource utile. Cliquez sur **Ajouter**, puis procédez comme suit :
  - **Description :** entrez une description pour le paramètre de recherche. Ce champ est obligatoire.
  - **Portée :** choisissez **Base**, **Un niveau** ou **Sous-arborescence** pour définir la profondeur de la recherche dans l'arborescence LDAP. La valeur par défaut est **Base**.
    * **Base** recherche le nœud indiqué par la Base de recherche.
    * **Un niveau** recherche le nœud Base et un niveau en dessous.
    * **Sous-arborescence** recherche le nœud Base, ainsi que tous ses enfants, quelle que soit la profondeur.
  - **Base de recherche :** entrez le chemin d'accès au nœud à partir duquel démarrer une recherche. Par exemple, ou=people ou 0=example corp. Ce champ est obligatoire.
  - Cliquez sur **Ajouter** pour ajouter le paramètre de recherche ou cliquez sur **Annuler** pour annuler l'ajout du paramètre de recherche.
  - Répétez ces étapes pour chaque paramètre de recherche à ajouter.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur

macOS 10.7 et versions ultérieures.

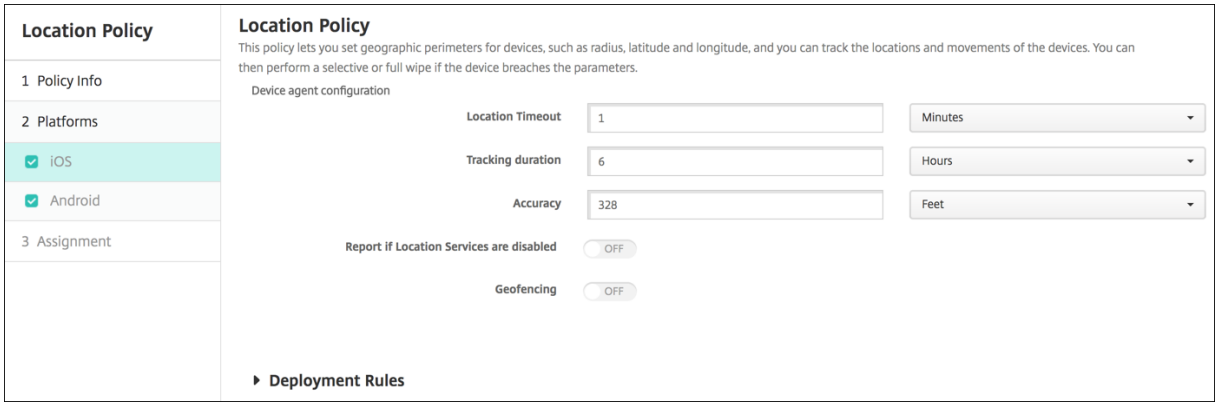
Stratégie d'emplacement

September 22, 2021

Vous pouvez créer des stratégies d'emplacement dans XenMobile pour imposer des limites géographiques. Lorsque les utilisateurs violent le périmètre défini, également appelé *géofencing*, XenMobile peut exécuter certaines actions. Par exemple, vous pouvez configurer la stratégie pour émettre un message d'avertissement aux utilisateurs lorsqu'ils violent le périmètre défini. Vous pouvez également configurer la stratégie pour effacer les données d'entreprise des utilisateurs lorsqu'ils violent un périmètre, immédiatement ou après un délai. Pour plus d'informations sur les actions de sécurité, telles que le suivi et la localisation d'un appareil, reportez-vous à la section Actions de sécurisation.

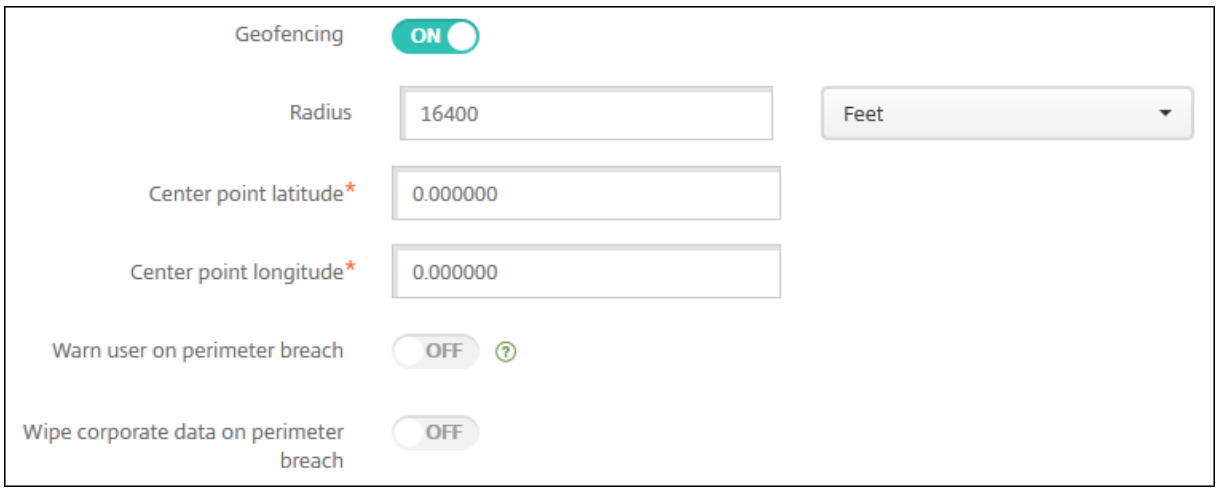
Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Délai max. de localisation :** entrez un chiffre, puis, dans la liste, cliquez sur **Secondes** ou **Minutes** pour définir la fréquence à laquelle XenMobile tente de déterminer l'emplacement de l'appareil. Les valeurs valides sont 60–900 secondes ou 1–15 minutes. La valeur par défaut est 1 minute.
- **Durée du suivi :** entrez un chiffre, puis, dans la liste, cliquez sur **Heures** ou **Minutes** pour définir la durée pendant laquelle XenMobile suit l'appareil. Les valeurs valides sont 1 à 6 heures ou 10 à 360 minutes. La valeur par défaut est 6 heures.
- **Précision :** entrez un chiffre, puis cliquez sur **Mètres**, **Feet** ou **Yards** dans la liste pour définir la précision du suivi effectué par XenMobile. Les valeurs valides sont 10–5000 yards ou mètres ou 30–15000 feet. La valeur par défaut est 328 pieds.

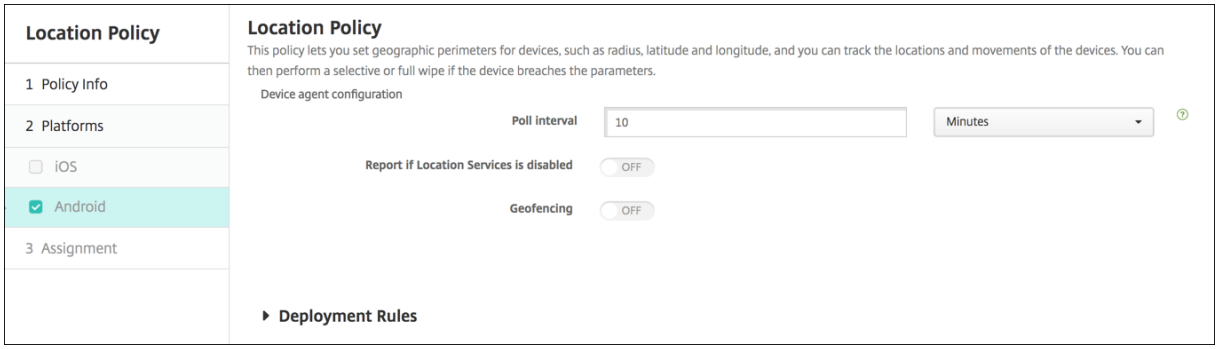
- **M'avertir si les services de localisation sont désactivés :** sélectionnez cette option si vous voulez que l'appareil envoie un rapport à XenMobile lorsque le GPS est désactivé. La valeur par défaut est **Désactivé**.
- **Géofencing**



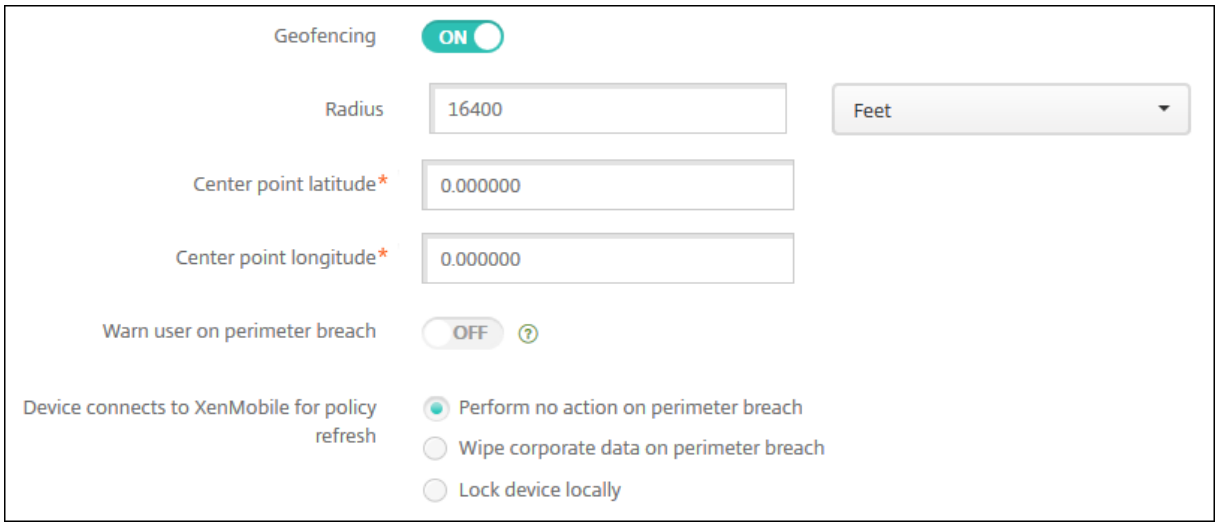
Lorsque vous activez Géofencing, configurez les paramètres suivants :

- **Rayon :** entrez un chiffre, puis, dans la liste, cliquez sur les unités à utiliser pour mesurer le rayon. La valeur par défaut est 16 400 feet. Les valeurs valides pour le rayon sont :
  - 164–164000 feet
  - 50–50000 mètres
  - 54-54680 yards
  - 1–31 miles
- **Latitude du point central :** entrez une latitude, par exemple 37.787454, pour définir la latitude du point central du géofencing.
- **Longitude du point central :** entrez une longitude, par exemple 122.402952, pour définir la longitude du point central du géofencing.
- **Avertir l'utilisateur en cas de violation du périmètre :** choisissez d'afficher un message d'avertissement lorsque les utilisateurs violent le périmètre établi. La valeur par défaut est **Désactivé**. Aucune connexion à XenMobile n'est nécessaire pour afficher le message d'avertissement.
- **Effacer les données d'entreprise en cas de violation du périmètre :** indiquez si vous souhaitez effacer les appareils des utilisateurs lorsqu'ils violent le périmètre. La valeur par défaut est **Désactivé**. Lorsque vous activez cette option, le champ **Délai avant l'effacement local** s'affiche.
  - Entrez un chiffre, puis, dans la liste, cliquez sur **Secondes** ou **Minutes** pour définir la durée du délai avant l'effacement des données d'entreprise sur les appareils des utilisateurs. Ce paramètre offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que XenMobile n'efface leurs appareils. La durée par défaut est 0 seconde.

Paramètres Android



- **Echantillonnage :** entrez un chiffre, puis, dans la liste, cliquez sur **Minutes**, **Heures** ou **Jours** pour définir la fréquence à laquelle XenMobile tente de déterminer l'emplacement de l'appareil. Les valeurs valides sont 1–1440 minutes, 1–24 heures ou un nombre quelconque de jours. La valeur par défaut est 10 minutes. si la valeur définie est inférieure à 10 minutes, cela peut avoir un impact négatif sur l'autonomie de la batterie.
- **M'avertir si les services de localisation sont désactivés :** sélectionnez cette option si vous voulez que l'appareil envoie un rapport à XenMobile lorsque le GPS est désactivé. La valeur par défaut est **Désactivé**.
- **Géofencing**



Lorsque vous activez Géofencing, configurez les paramètres suivants :

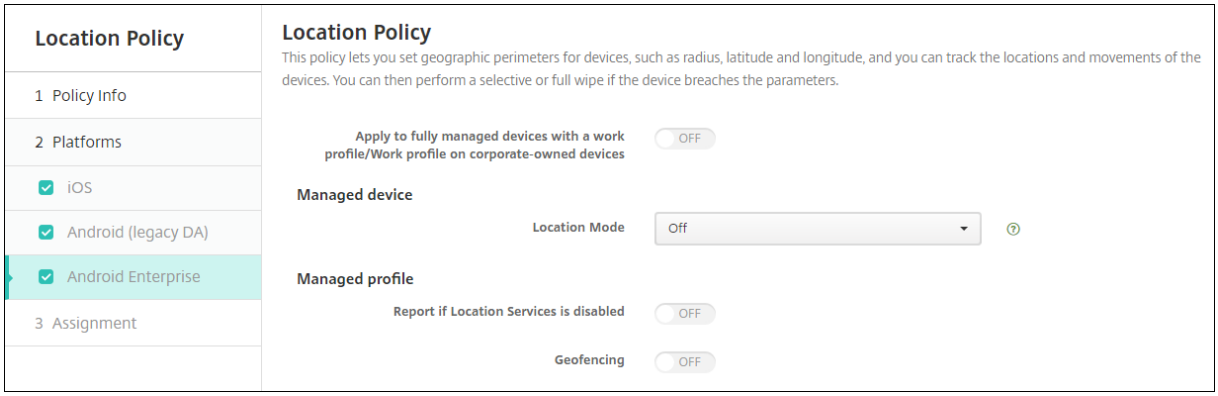
- **Rayon :** entrez un chiffre, puis, dans la liste, cliquez sur les unités à utiliser pour mesurer le rayon. La valeur par défaut est 16 400 feet. Les valeurs valides pour le rayon sont :
  - 164–164000 feet
  - 1–50 kilomètres
  - 50–50000 mètres
  - 54-54680 yards
  - 1–31 miles

- **Latitude du point central :** entrez une latitude, par exemple 37.787454, pour définir la latitude du point central du géofencing.
- **Longitude du point central :** entrez une longitude, par exemple 122.402952, pour définir la longitude du point central du géofencing.
- **Avertir l'utilisateur en cas de violation du périmètre :** choisissez d'afficher un message d'avertissement lorsque les utilisateurs violent le périmètre établi. La valeur par défaut est **Désactivé**. Aucune connexion à XenMobile n'est nécessaire pour afficher le message d'avertissement.
- **L'appareil se connecte à XenMobile pour actualiser la stratégie :** sélectionnez l'une des options suivantes à exécuter lorsque les utilisateurs violent le périmètre :
  - **N'effectuer aucune action en cas de violation du périmètre :** aucune action n'est prise. il s'agit du réglage par défaut.
  - **Effacer les données d'entreprise en cas de violation du périmètre :** les données d'entreprise sont effacées après une durée spécifiée. Lorsque vous activez cette option, le champ **Délai avant l'effacement local** s'affiche.
    * Entrez un chiffre, puis, dans la liste, cliquez sur Secondes ou Minutes pour définir la durée du délai avant l'effacement des données d'entreprise sur les appareils des utilisateurs. Ce paramètre offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que XenMobile n'efface leurs appareils. La durée par défaut est 0 seconde.
  - **Délai du verrouillage :** verrouille les appareils des utilisateurs après une période spécifiée. Lorsque vous activez cette option, le champ **Délai du verrouillage** s'affiche.
    * Entrez un chiffre, puis, dans la liste, cliquez sur Secondes ou Minutes pour définir la durée du délai avant le verrouillage des appareils des utilisateurs. Ce paramètre offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que XenMobile ne verrouille leurs appareils. La durée par défaut est 0 seconde.

Paramètres Android Enterprise

Pour que le suivi de l'emplacement Android fonctionne, assurez-vous de remplir les conditions suivantes :

- Android 8.5 ou version ultérieure
- Paramètre Autoriser partage de position activé dans la stratégie Restrictions pour Android Enterprise
- Planification de connexion (Firebase Cloud Messaging recommandé)



Appliquer aux appareils entièrement gérés dotés d'un profil professionnel

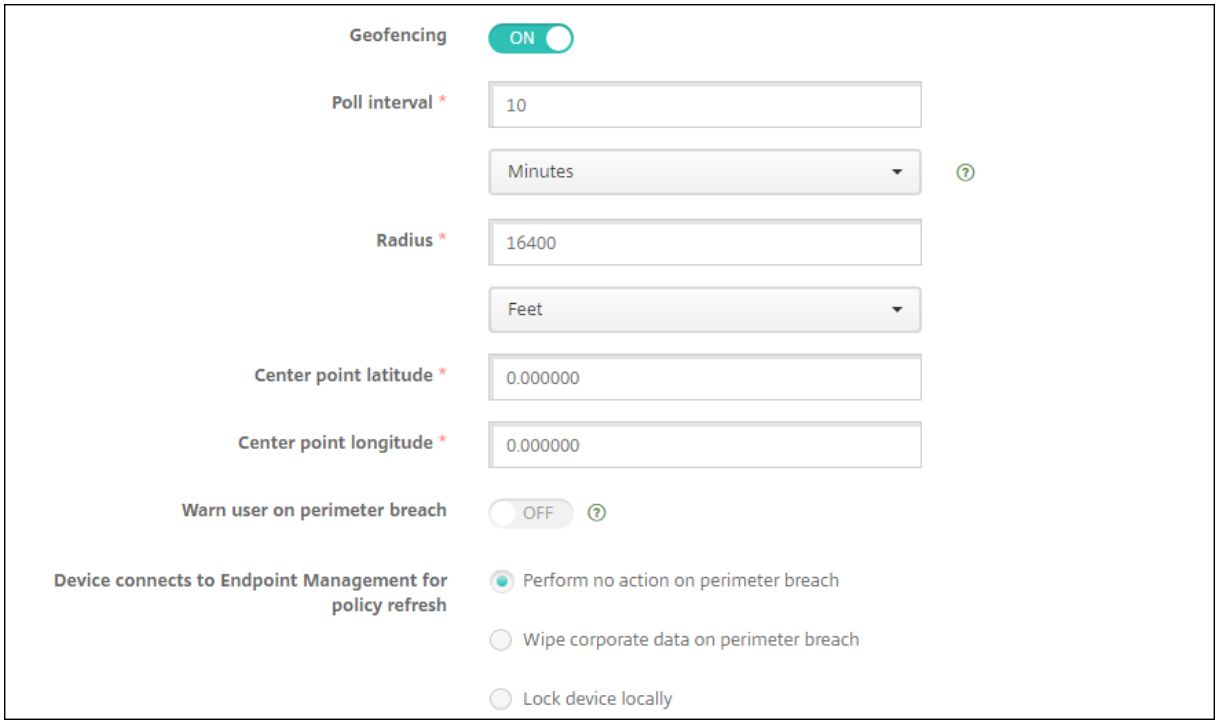
Pour les appareils entièrement gérés avec profil de travail, seul le paramètre de mode de localisation est disponible.

- **Appliquer aux appareils entièrement gérés avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise :** permet de configurer le mode de localisation pour les appareils entièrement gérés avec profil de travail. Lorsque ce paramètre est activé, configurez les paramètres du mode de localisation pour le profil de travail :
  - **M'avertir si les services de localisation sont désactivés :** sélectionnez cette option si vous voulez que l'appareil envoie un rapport à XenMobile Server lorsque le GPS est désactivé. La valeur par défaut est **Désactivé**.
  - **Géofencing :** reportez-vous aux paramètres décrits dans cet article sous Appareil géré.

Lorsque l'option **Appliquer aux appareils entièrement gérés avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise** est désactivée, les paramètres s'appliquent à l'appareil géré et au profil de travail, comme indiqué dans les sections suivantes. La valeur par défaut est **Désactivé**.

Appareil géré

- **Mode de localisation :** spécifiez le degré de détection de localisation à activer. Vous pouvez utiliser l'action de sécurisation Localiser uniquement lorsque le mode de localisation est défini sur Haute précision ou Économie de batterie. La valeur par défaut est Haute précision.
  - **Haute précision :** active toutes les méthodes de détection de localisation, y compris le GPS, les réseaux et autres capteurs.
  - **Capteurs seulement :** active uniquement les capteurs GPS et autres.
  - **Économie de batterie :** active uniquement le fournisseur de localisation réseau.
  - **Désactivé :** désactive la détection de la localisation.
- **Géofencing :**



Lorsque vous activez **Géofencing**, configurez les paramètres suivants :

- **Echantillonnage :** entrez un chiffre, puis cliquez sur **Minutes**, **Heures** ou **Jours** pour définir la fréquence à laquelle XenMobile tente de déterminer l'emplacement de l'appareil. Les valeurs valides sont 1–1440 minutes, 1–24 heures ou un nombre quelconque de jours. La valeur par défaut est **10 minutes**. Si la valeur définie est inférieure à 10 minutes, cela peut avoir un impact négatif sur l'autonomie de la batterie.
- **Rayon :** entrez un chiffre, puis cliquez sur les unités à utiliser pour mesurer le rayon. La valeur par défaut est **5000 mètres** (**16400 pieds**). Les valeurs valides pour le rayon sont :
  - 164–164000 feet
  - 1–50 kilomètres
  - 50–50000 mètres
  - 54-54680 yards
  - 1–31 miles
- **Latitude du point central :** entrez une latitude, par exemple 37.787454, pour définir la latitude du point central du géofencing. Pour vérifier la valeur, accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Sécurité**, puis cliquez sur **Localiser**. Après avoir localisé l'appareil, XenMobile Server signale l'emplacement de l'appareil dans **Détails de l'appareil > Général** sous **Sécurité**.
- **Longitude du point central :** entrez une longitude, par exemple 122.402952, pour définir la longitude du point central du géofencing.

- **Avertir l'utilisateur en cas de violation du périmètre :** choisissez d'afficher un message d'avertissement lorsque les utilisateurs violent le périmètre établi. La valeur par défaut est **Désactivé**. Aucune connexion à XenMobile Server n'est nécessaire pour afficher le message d'avertissement.
- **L'appareil se connecte à XenMobile Server pour actualiser la stratégie :** sélectionnez l'une des options suivantes à exécuter lorsque les utilisateurs violent le périmètre :
  - **N'effectuer aucune action en cas de violation du périmètre :** aucune action n'est prise. il s'agit du réglage par défaut.
  - **Effacer les données d'entreprise en cas de violation du périmètre :** les données d'entreprise sont effacées après une durée spécifiée. Lorsque vous activez cette option, le champ **Délai avant l'effacement local** s'affiche.
    * Entrez un chiffre, puis cliquez sur **Secondes** ou **Minutes** pour définir la durée du délai avant l'effacement des données d'entreprise sur les appareils des utilisateurs. Ce délai offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que XenMobile Server n'efface leurs appareils. La durée par défaut est **0 seconde**.
  - **Verrouiller l'appareil localement :** verrouille les appareils des utilisateurs après une période spécifiée. Lorsque vous activez cette option, le champ **Délai du verrouillage** s'affiche.
    * Entrez un chiffre, puis cliquez sur **Secondes** ou **Minutes** pour définir la durée du délai avant le verrouillage des appareils des utilisateurs. Ce délai offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que XenMobile Server ne verrouille leurs appareils. La durée par défaut est **0 seconde**.

Profil géré

- **M'avertir si les services de localisation sont désactivés :** sélectionnez cette option si vous voulez que l'appareil envoie un rapport à XenMobile Server lorsque le GPS est désactivé. La valeur par défaut est **Désactivé**.
- **Géofencing :** reportez-vous aux paramètres décrits dans cet article sous Appareil géré.

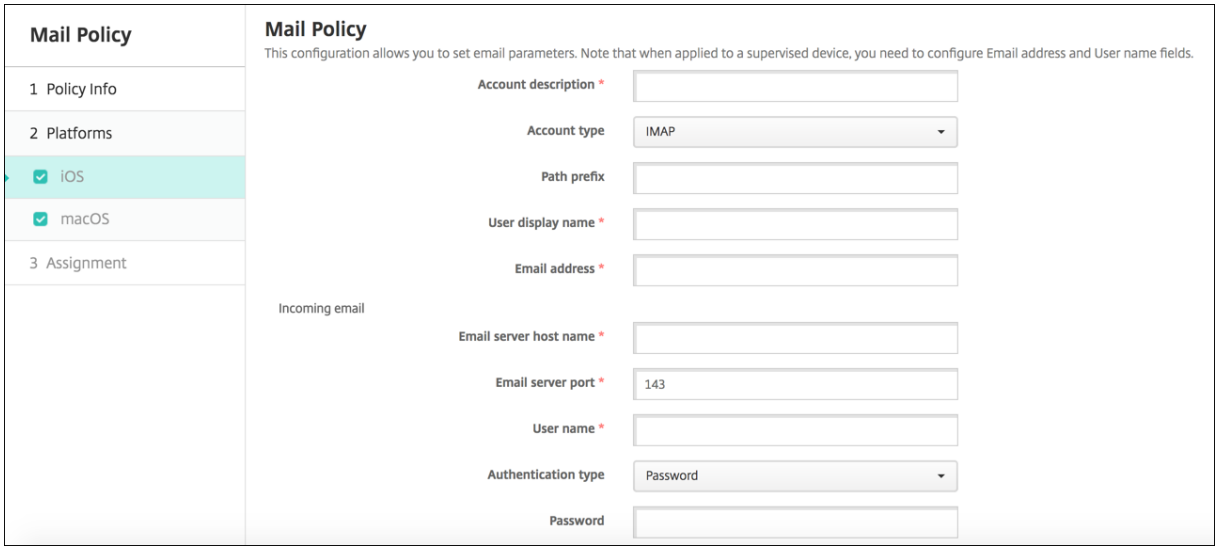
Stratégie de messagerie

March 30, 2020

Vous pouvez ajouter une stratégie de messagerie dans XenMobile pour configurer un compte de messagerie sur les appareils iOS ou macOS des utilisateurs.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS et macOS



- **Description du compte :** entrez une description pour le compte ; elle apparaît dans les applications de messagerie et de paramètres. Ce champ est obligatoire.
- **Type de compte :** cliquez sur **IMAP** ou **POP** pour sélectionner le protocole à utiliser pour les comptes d'utilisateur. La valeur par défaut est **IMAP**. Lorsque vous sélectionnez le protocole **POP**, l'option **Préfixe chemin** disparaît.
- **Préfixe chemin :** entrez **INBOX** ou le chemin d'accès à votre compte de messagerie IMAP. Ce champ est obligatoire.
- **Nom d'affichage de l'utilisateur :** entrez le nom d'utilisateur à utiliser dans les messages, etc. Ce champ est obligatoire.
- **Adresse électronique :** entrez l'adresse e-mail du compte. Ce champ est obligatoire.
- **Paramètres du courrier entrant**
  - **Nom d'hôte du serveur de messagerie :** entrez le nom d'hôte ou l'adresse IP du serveur de messagerie du courrier entrant. Ce champ est obligatoire.
  - **Port du serveur de messagerie :** entrez le numéro de port du serveur de courrier entrant. Le paramètre par défaut est **143** Ce champ est obligatoire.
  - **Nom d'utilisateur :** entrez le nom d'utilisateur du compte de messagerie. Ce nom est généralement le même que l'adresse e-mail à hauteur du caractère @. Ce champ est obligatoire.
  - **Type d'authentification :** choisissez le type d'authentification à utiliser. La valeur par défaut est **Mot de passe**. Lorsque **Aucun** est sélectionné, le champ **Mot de passe** suivant disparaît.
  - **Mot de passe :** entrez un mot de passe pour le serveur de messagerie de courrier entrant (facultatif).
  - **Utiliser SSL :** sélectionnez cette option pour que le serveur de messagerie du courrier entrant utilise l'authentification SSL. La valeur par défaut est **Désactivé**.

- **Paramètres de messagerie du courrier sortant**
  - **Nom d'hôte du serveur de messagerie :** entrez le nom d'hôte ou l'adresse IP du serveur de messagerie du courrier sortant. Ce champ est obligatoire.
  - **Port du serveur de messagerie :** entrez le numéro de port du serveur de courrier sortant. Si vous n'entrez pas de numéro de port, le port par défaut du protocole donné est utilisé.
  - **Nom d'utilisateur :** entrez le nom d'utilisateur du compte de messagerie. Ce nom est généralement le même que l'adresse e-mail à hauteur du caractère @. Ce champ est obligatoire.
  - **Type d'authentification :** choisissez le type d'authentification à utiliser. La valeur par défaut est **Mot de passe**.
  - **Mot de passe :** entrez un mot de passe pour le serveur de messagerie de courrier sortant (facultatif).
  - **Mot de passe sortant identique au mot de passe entrant :** sélectionnez cette option pour spécifier si les mots de passe entrants et sortants sont les mêmes. La valeur par défaut est **Désactivé**, ce qui signifie que les mots de passe sont différents.
  - **Utiliser SSL :** sélectionnez cette option pour que le serveur de messagerie du courrier sortant utilise l'authentification SSL. La valeur par défaut est **Désactivé**.
- **Stratégie**
  - **Autoriser le déplacement des e-mails entre les comptes :** sélectionnez cette option pour autoriser les utilisateurs à déplacer les messages de ce compte vers un autre compte et à transférer des messages et y répondre à partir d'un autre compte. La valeur par défaut est **Désactivé**.
  - **N'envoyer des e-mails que depuis l'application de messagerie :** sélectionnez cette option si vous voulez que les utilisateurs soient uniquement autorisés à envoyer des e-mails avec l'application de messagerie iOS.
  - **Désactiver la synchronisation des e-mails récents :** sélectionnez cette option pour empêcher les utilisateurs de synchroniser les adresses récentes. La valeur par défaut est **Désactivé**. Cette option s'applique uniquement à iOS 6.0 et versions ultérieures.
  - **Autoriser Mail Drop :** sélectionnez cette option pour autoriser l'utilisation d'Apple Mail Drop pour les appareils exécutant iOS 9.2 ou version ultérieure. La valeur par défaut est **Désactivé**.
  - **Activer signature S/MIME :** indiquez si ce compte prend en charge la signature S/MIME. La valeur par défaut est **Activé**. Lorsque la valeur est définie sur **Activé**, les champs suivants apparaissent.
    - **Informations d'identification de l'identité de signature :** choisissez les informations d'identification de signature à utiliser.
    - **Signature S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer et désactiver la signature S/MIME dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option

s'applique à iOS 12.0 et versions ultérieures.

    * **UUID du certificat de signature S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent sélectionner les informations d'identification de signature à utiliser dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.

  – **Activer chiffrement S/MIME :** sélectionnez cette option si vous souhaitez que ce compte prenne en charge le chiffrement S/MIME. La valeur par défaut est **Désactivé**. Lorsque la valeur est définie sur **Activé**, les champs suivants apparaissent.

    * **Informations d'identification de l'identité de chiffrement :** dans la liste, sélectionnez les informations d'identification de chiffrement à utiliser.
    * **Activer commutateur de chiffrement S/MIME par message :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer ou désactiver le chiffrement S/MIME pour chaque message composé. La valeur par défaut est **Désactivé**.
    * **Chiffrement S/MIME par défaut remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent choisir si S/MIME est activé par défaut dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
    * **UUID du certificat de chiffrement S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer et désactiver l'identité de chiffrement S/MIME dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.

- **Paramètres de stratégie**
  – **Supprimer la stratégie :** pour supprimer la stratégie ultérieurement, vous pouvez configurer ce paramètre en utilisant les options **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  – **Autoriser l'utilisateur à supprimer la stratégie :** autorisez les utilisateurs à supprimer la stratégie de messagerie en utilisant les options **Toujours**, **Code secret requis** ou **Jamais**.
  – **Étendue du profil :** pour macOS uniquement, choisissez si la stratégie s'applique au niveau **Utilisateur** ou à l'ensemble du **Système**.

Stratégies de domaines gérés

January 10, 2022

Vous pouvez définir des domaines gérés qui s'appliquent à la messagerie et au navigateur Safari. Les domaines gérés vous aident à protéger les données d'entreprise en contrôlant les applications qui peuvent ouvrir des documents téléchargés depuis des domaines à l'aide de Safari.

Pour les appareils supervisés iOS 8 et versions ultérieures, vous spécifiez des adresses URL ou des sous-domaines pour contrôler la manière dont les utilisateurs peuvent ouvrir des documents, des pièces jointes et des téléchargements à partir du navigateur. Pour les appareils supervisés iOS 9.3 et versions plus récentes, vous pouvez spécifier les adresses URL à partir desquelles les utilisateurs peuvent enregistrer des mots de passe dans Safari.

Pour obtenir les instructions sur la définition d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

Lorsqu'un utilisateur envoie un e-mail à un destinataire dont le domaine n'est pas sur la liste des domaines de messagerie gérés, un message s'affiche sur l'appareil de l'utilisateur pour l'avertir qu'il envoie un message à un utilisateur en dehors de votre domaine d'entreprise.

Pour les éléments tels que document, pièce jointe ou téléchargement : lorsqu'un utilisateur tente d'ouvrir un élément à l'aide de Safari depuis un domaine Web se trouvant sur la liste de domaines gérés, l'application d'entreprise appropriée ouvre l'élément. Si l'élément ne provient pas d'un domaine Web se trouvant sur la liste des domaines Web gérés, l'utilisateur ne peut pas ouvrir l'élément avec une application d'entreprise ; il doit utiliser une application non gérée, personnelle.

Pour les appareils supervisés, même si vous ne spécifiez pas de domaines de remplissage automatique du mot de passe Safari : si l'appareil est configuré pour multi-utilisateurs éphémères, les utilisateurs ne peuvent pas enregistrer de mots de passe. Toutefois, si l'appareil n'est pas configuré pour multi-utilisateurs éphémères, les utilisateurs peuvent enregistrer tous les mots de passe.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

Pour spécifier des domaines :

Format	Description
`example.com`	Traitez n'importe quel chemin sous `example.com` comme géré, mais pas `site.example.com/`.
`foo.example.com`	Traitez n'importe quel chemin sous `foo.example.com` comme géré, mais pas `example.com/` ou `bar.example.com/`.
`\*.example.com`	Traitez n'importe quel chemin sous `foo.example.com` ou `bar.example.com` comme géré, mais pas `example.com/`.

Format	Description
`example.com/sub`	Traitez `example.com/sub` et n'importe quel chemin en dessous comme géré, mais pas `example.com/`.
`foo.example.com/sub`	Traitez n'importe quel chemin sous `foo.example.com/sub` comme géré, mais pas `example.com`, `example.com/sub`, `foo.example.com/` ou `bar.example.com/sub`.
`\*.example.com/sub`	Traitez n'importe quel chemin sous `foo.example.com/sub` ou `bar.example.com/sub` comme géré, mais pas `example.com` ou `foo.example.com/`.

Règles :

- Le « www. » du début et les barres obliques de fin des adresses URL sont ignorés lorsque les domaines sont comparés.
- Si une entrée contient un numéro de port, seules les adresses spécifiant ce numéro de port sont considérées comme gérées. Dans le cas contraire, seuls les ports standard sont considérés comme gérés (port 80 pour http et port 443 pour https). Par exemple, le modèle `*.example.com:8080` correspond à `https://site.example.com:8080/page.html`, mais pas `https://site.example.com/page.html`, alors que le modèle `*.example.com` correspond à `https://site.example.com/page.html` et `https://site.example.com/page.html`, mais pas `https://site.example.com:8080/page.html`.
- Les définitions de domaines Web Safari gérés sont cumulatives. Les modèles définis par toutes les charges utiles des domaines Web Safari gérés sont utilisés pour la correspondance dans le cadre d'une demande d'adresse URL.

Paramètres :

- **Domaines gérés**
  - **Domaines de messagerie non marqués :** pour chaque domaine de messagerie à inclure dans la liste, cliquez sur **Ajouter**, puis procédez comme suit :
    - **Domaine de messagerie géré :** entrez le domaine de messagerie.
    - Cliquez sur **Enregistrer** pour enregistrer le domaine de messagerie ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **Domaines Web Safari gérés :** pour chaque domaine Web à inclure dans la liste, cliquez sur **Ajouter**, puis procédez comme suit :
    - **Domaine Web géré :** entrez le domaine Web.

        * Cliquez sur **Enregistrer** pour enregistrer le domaine Web ou cliquez sur **Annuler** pour ne pas l'enregistrer.
    - **Domaines de remplissage automatique du mot de passe Safari :** pour chaque domaine Web à inclure dans la liste, cliquez sur **Ajouter**, puis procédez comme suit :
        * **Domaine de remplissage automatique du mot de passe Safari :** entrez le domaine de remplissage automatique.
        * Cliquez sur **Enregistrer** pour enregistrer le domaine de remplissage automatique ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **Paramètres de stratégie**
    - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
        * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
        * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Stratégie d'options MDM

January 10, 2022

Vous pouvez créer une stratégie d'appareil dans XenMobile pour gérer les fonctions Localiser mon iPhone/Verrouillage d'activation iPad sur les appareils supervisés iOS 7.0 et versions ultérieures. Pour obtenir les instructions sur la définition d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

Le verrouillage d'activation est une fonctionnalité de Localiser mon iPhone/iPad qui empêche la réactivation d'un appareil supervisé perdu ou volé. Le verrouillage d'activation requiert l'identifiant Apple et le mot de passe de l'utilisateur pour pouvoir désactiver Localiser mon iPhone/iPad, effacer l'appareil ou réactiver l'appareil. Pour les appareils qui sont la propriété de votre organisation, il est nécessaire de contourner le verrouillage d'activation pour, par exemple, réinitialiser ou réattribuer des appareils.

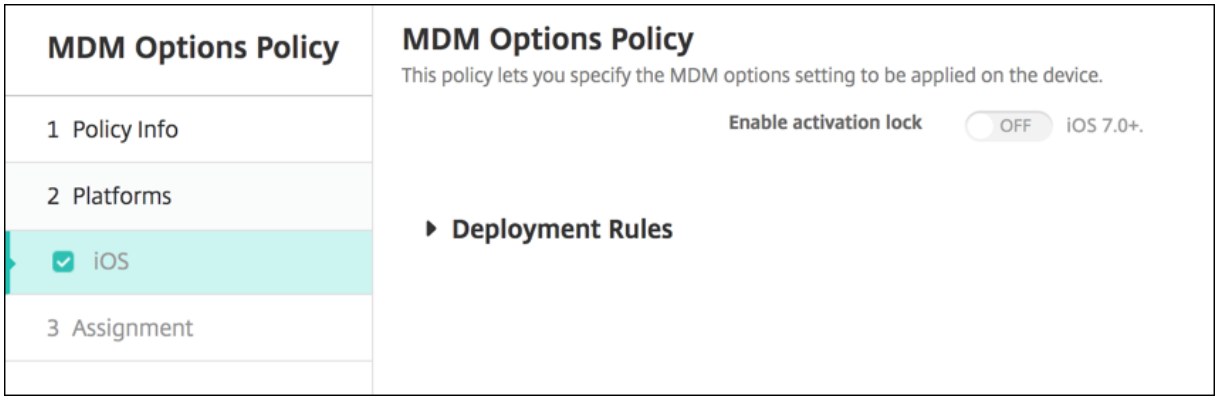
Pour activer le verrouillage d'activation, configurez et déployez la stratégie Options MDM de XenMobile. Vous pouvez ensuite gérer un appareil à partir de la console XenMobile sans les informations d'identification Apple de l'utilisateur. Pour contourner l'obligation d'entrer des informations d'identification Apple avec un verrou d'activation, émettez l'action de sécurisation Contourner le verrouillage d'activation depuis la console XenMobile.

Par exemple, si l'utilisateur retourne un téléphone perdu ou pour configurer l'appareil avant ou

après un effacement complet : lorsque le téléphone invite à entrer les informations d'identification de compte iTunes, vous pouvez ignorer cette étape en émettant l'action de sécurité Contourner le verrouillage d'activation à partir de la console XenMobile.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Activer le verrouillage d'activation :** indiquez si vous souhaitez activer l'option Verrouillage d'activation sur les appareils sur lesquels vous déployez cette stratégie. La valeur par défaut est **Désactivé**.

Après avoir installé le verrouillage d'activation en déployant la stratégie Options MDM : l'action de sécurisation **Contourner le verrouillage d'activation** s'affiche lorsque vous sélectionnez les appareils sur la page **Gérer > Appareils** et cliquez sur **Sécurité**. Un contournement de verrouillage d'activation vous permet de retirer le verrouillage d'activation des appareils supervisés avant l'activation de l'appareil sans connaître l'identifiant Apple et le mot de passe des utilisateurs de l'appareil. Vous pouvez envoyer un contournement de verrouillage d'activation à un appareil avant ou après un effacement complet. Pour plus d'informations, consultez la section Contourner un verrouillage d'activation iOS dans l'article Actions de sécurisation.

Stratégie d'informations sur l'organisation

January 10, 2022

Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin de spécifier les coordonnées de votre organisation à utiliser pour envoyer les messages d'alerte qui sont transmis depuis XenMobile vers les appareils iOS. La stratégie est disponible pour iOS 7 et versions ultérieures.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Nom :** entrez le nom de l'organisation exécutant XenMobile.
- **Adresse :** entrez l'adresse de l'organisation.
- **Téléphone :** entrez le numéro de téléphone d'assistance de l'organisation.
- **Adresse électronique :** entrez l'adresse e-mail d'assistance.
- **Magic :** entrez un mot ou une phrase décrivant les services gérés par l'organisation.

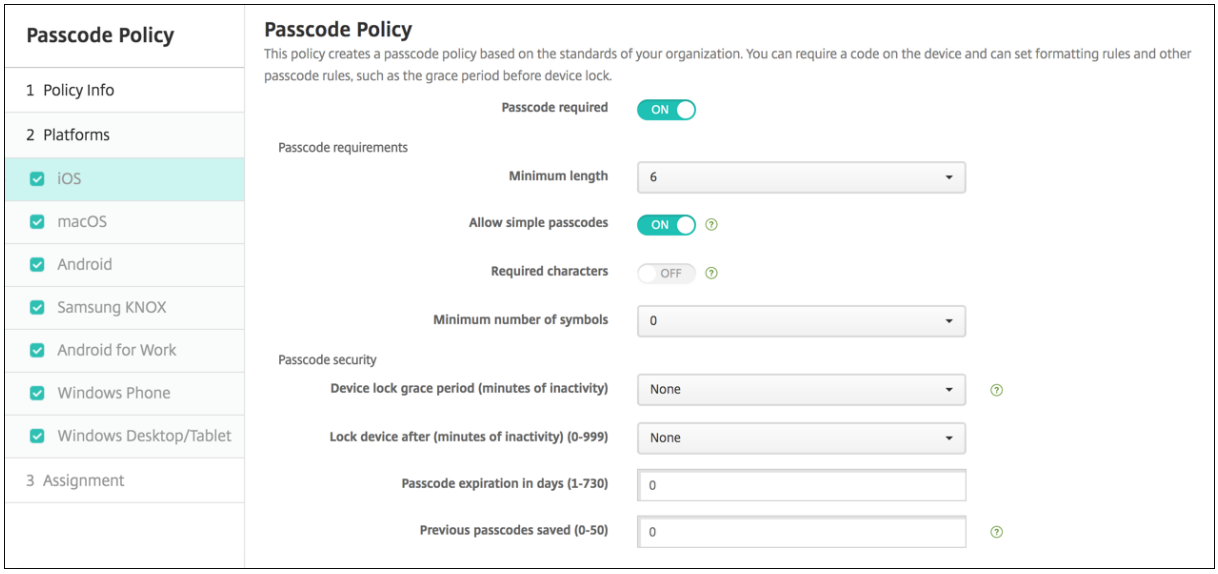
Stratégie de code secret

January 10, 2022

Vous créez une stratégie de code secret dans XenMobile en fonction des normes de votre organisation. Vous pouvez exiger la saisie de codes secrets sur les appareils des utilisateurs et définir diverses règles de code secret et de formatage. Vous pouvez créer des stratégies pour iOS, macOS, Android, Samsung KNOX, Android Enterprise, Windows Phone et Windows Desktop/Tablet. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

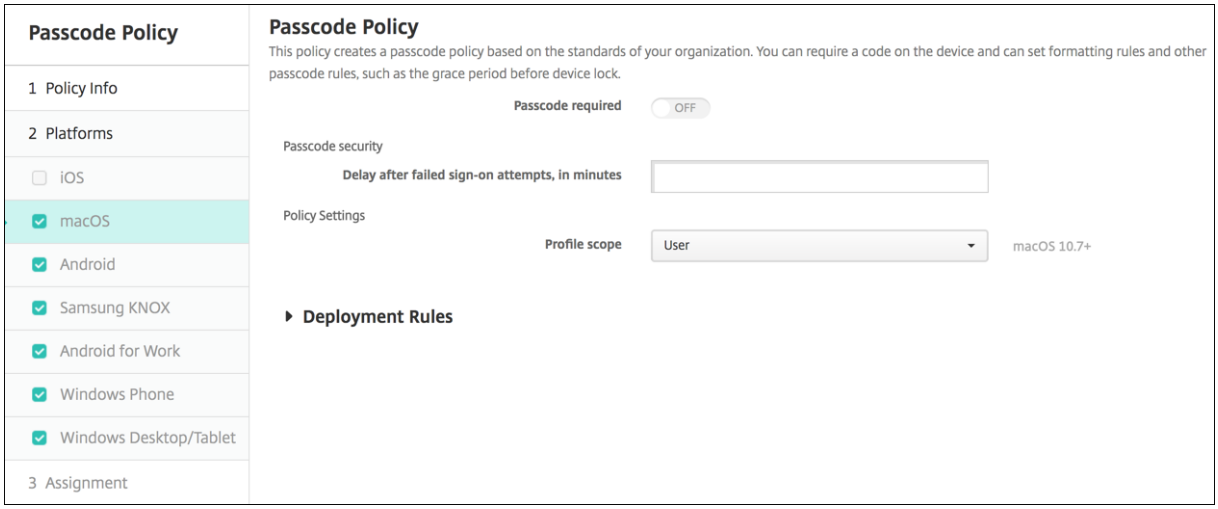
Paramètres iOS



- **Code secret requis :** sélectionnez cette option pour exiger la saisie d'un mot de passe et afficher les options de configuration d'une stratégie de code secret pour iOS. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret, sécurité et paramètres de stratégie.

- **Exigences en matière de code secret**
  - **Longueur minimale :** dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est **6**.
  - **Autoriser les codes secrets simples :** sélectionnez cette option pour autoriser les codes secrets simples. Les codes secrets simples se caractérisent par des caractères répétés ou séquentiels. La valeur par défaut est **Activé**.
  - **Caractères requis :** sélectionnez cette option pour exiger que les codes secrets contiennent au moins une lettre. La valeur par défaut est **Désactivé**.
  - **Nombre minimum de symboles :** dans la liste, cliquez sur le nombre de symboles que le code secret doit contenir. La valeur par défaut est **0**.
- **Sécurité du code secret**
  - **Période de grâce avant verrouillage de l'appareil (minutes d'inactivité) :** dans la liste, cliquez sur la durée après laquelle les utilisateurs doivent entrer un code secret pour déverrouiller un appareil verrouillé. La valeur par défaut est **Aucun**.
  - **Verrouiller l'appareil après (minutes d'inactivité) :** dans la liste, cliquez sur la durée pendant laquelle un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est Aucun.
  - **Expiration du code secret en jours (1-730) :** entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
  - **Mots de passe précédents enregistrés (0-50) :** entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
  - **Nombre maximum de tentatives de connexion infructueuses :** dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil subit un effacement complet. La valeur par défaut est **Aucun nombre défini**.

Paramètres macOS



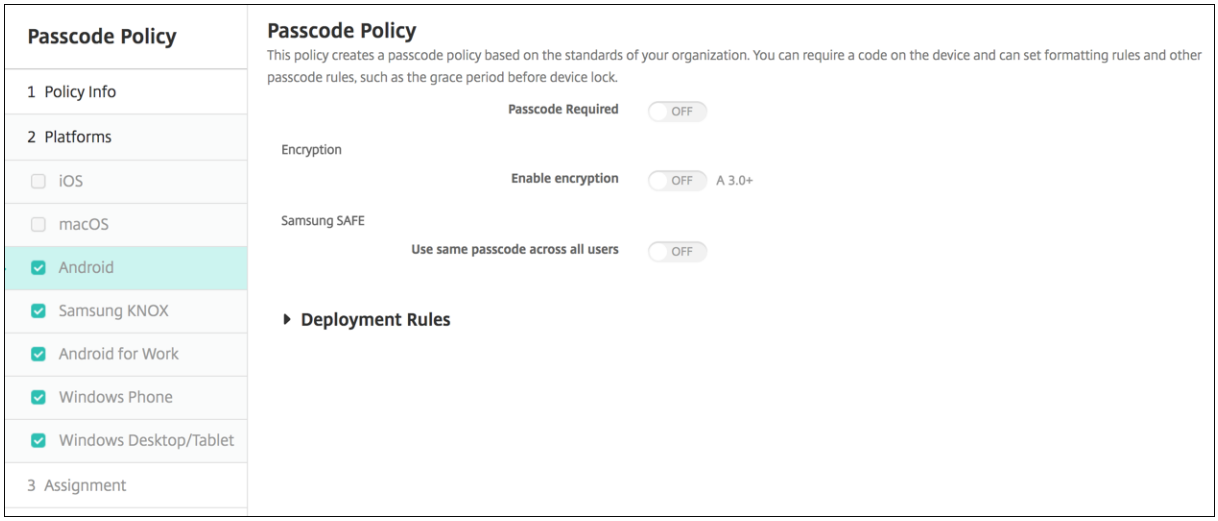
- **Code secret requis :** sélectionnez cette option pour exiger la saisie d'un mot de passe et afficher les options de configuration d'une stratégie de code secret pour iOS. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret, sécurité et paramètres de stratégie.
- Si vous n'activez pas **Code secret requis**, en regard de **Délai après les échecs de tentatives de connexion, en minutes**, entrez le nombre de minutes après lesquelles les utilisateurs peuvent retenter de saisir leur code secret.
- Si vous activez **Code secret requis**, configurez les paramètres suivants :
- **Exigences en matière de code secret**
  - **Longueur minimale :** dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est **6**.
  - **Autoriser les codes secrets simples :** sélectionnez cette option pour autoriser les codes secrets simples. Les codes secrets simples se caractérisent par des caractères répétés ou séquentiels. La valeur par défaut est **Activé**.
  - **Caractères requis :** sélectionnez cette option pour exiger que les codes secrets contiennent au moins une lettre. La valeur par défaut est **Désactivé**.
  - **Nombre minimum de symboles :** dans la liste, cliquez sur le nombre de symboles que le code secret doit contenir. La valeur par défaut est **0**.
- **Sécurité du code secret**
  - **Période de grâce avant verrouillage de l'appareil (minutes d'inactivité) :** dans la liste, cliquez sur la durée après laquelle les utilisateurs doivent entrer un code secret pour déverrouiller un appareil verrouillé. La valeur par défaut est **Aucun**.
  - **Verrouiller l'appareil après (minutes d'inactivité) :** dans la liste, cliquez sur la durée pendant laquelle un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est **Aucun**.
  - **Expiration du code secret en jours (1-730) :** entrez le nombre de jours après lequel le

code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.

- **Mots de passe précédents enregistrés (0-50) :** entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
- **Nombre maximum de tentatives de connexion infructueuses :** dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil est verrouillé. La valeur par défaut est **Aucun nombre défini**.
- **Délai après les échecs de tentatives de connexion, en minutes :** entrez le nombre de minutes après lesquelles les utilisateurs peuvent retenter de saisir leur code secret.
- **Forcer la réinitialisation du code d'accès :** l'utilisateur doit réinitialiser le code d'accès lors de la prochaine authentification.

- **Paramètres de stratégie**
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Paramètres Android



> **Remarque :**
>
> Le paramètre par défaut pour Android est **Désactivé**.

- **Code secret requis :** sélectionnez cette option pour exiger la saisie d'un mot de passe et afficher les options de configuration d'une stratégie de code secret pour Android. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret, sécurité du code secret, cryptage et Samsung SAFE.

- **Exigences en matière de code secret**
  - **Longueur minimale :** dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est 6.
  - **Reconnaissance biométrique :** sélectionnez cette option pour activer la reconnaissance biométrique. Si vous activez cette option, le champ Caractères requis est masqué. La valeur par défaut est **Désactivé**.
  - **Caractères requis** : dans la liste, cliquez sur Aucune restriction, Chiffres et lettres, Chiffres uniquement ou Lettres uniquement pour configurer la manière dont les codes secrets sont composés. La valeur par défaut est Aucune restriction.
  - **Règles avancées :** sélectionnez cette option si vous souhaitez appliquer des règles de code secret avancées. Cette option est disponible pour Android 3.0 et versions ultérieures. La valeur par défaut est **Désactivé**.
  - Lorsque le paramètre **Règles avancées** est activé, à partir de chacune des listes suivantes et pour chaque type de caractère, cliquez sur le nombre minimal de caractère qu'un code secret doit contenir :
    - **Symboles :** nombre minimal de symboles.
    - **Lettres :** nombre minimal de lettres.
    - **Minuscules :** nombre minimum de minuscules.
    - **Majuscules :** nombre minimum de majuscules.
    - **Chiffres ou symboles :** nombre minimal de chiffres ou de symboles.
    - **Chiffres :** nombre minimal de chiffres.
- **Sécurité du code secret**
  - **Verrouiller l'appareil après (minutes d'inactivité) :** dans la liste, cliquez sur la durée pendant laquelle un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est **Aucune**.
  - **Expiration du code secret en jours (1-730) :** entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
  - **Mots de passe précédents enregistrés (0-50) :** entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
  - **Nombre maximum de tentatives de connexion infructueuses :** dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil est effacé. La valeur par défaut est **Aucun nombre défini**.
- **Cryptage**
  - **Activer le chiffrement :** sélectionnez cette option si vous souhaitez activer le chiffrement. Cette option est disponible pour Android 3.0 et versions ultérieures. L'option est

disponible, que le paramètre **Code secret requis** soit sélectionné ou non.

Pour crypter leurs appareils, les utilisateurs doivent commencer avec une batterie chargée et laisser l'appareil branché pendant le délai nécessaire au cryptage, une heure au minimum. Si le processus de cryptage est interrompu, les utilisateurs risquent de perdre certaines ou toutes les données de leurs appareils. Une fois qu'un appareil est crypté, le processus ne peut pas être annulé sauf en effectuant une réinitialisation d'usine, ce qui entraîne la suppression de toutes les données de l'appareil.

- **Samsung SAFE**

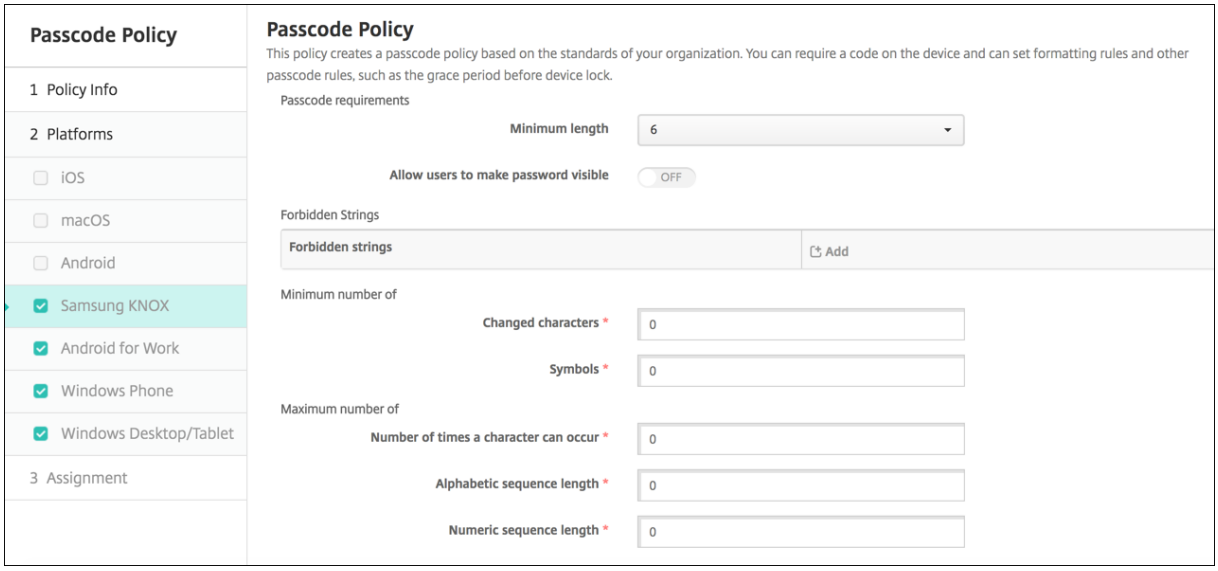
  > **Remarque :**
  >
  > Pour désactiver la reconnaissance de visage ou d'iris sur les appareils Samsung SAFE : créez une stratégie Restrictions pour Samsung SAFE. Dans la stratégie Restrictions, activez **Désactiver les applications** et ajoutez `com.samsung.android.bio.face.service` ou `com.samsung.android.server.iris` à la table. Ensuite, déployez la stratégie Restrictions.

  - **Utiliser le même code secret pour tous les utilisateurs :** sélectionnez cette option si vous souhaitez utiliser le même code secret pour tous les utilisateurs. La valeur par défaut est **Désactivé**. Ce paramètre s'applique uniquement aux appareils Samsung SAFE et il est disponible, que le paramètre **Code secret requis** soit sélectionné ou non.
  - Lorsque vous activez l'option **Utiliser le même code secret pour tous les utilisateurs**, saisissez le code secret à utiliser par les utilisateurs dans le champ **Code secret**.
  - Lorsque vous activez l'option **Code secret requis**, configurez les paramètres suivants pour Samsung SAFE :
    - **Caractères modifiés :** entrez le nombre de caractères que les utilisateurs doivent changer par rapport à leur code secret précédent. La valeur par défaut est **0**.
    - **Nombre d'occurrences d'un caractère :** entrez le nombre maximal d'occurrences d'un caractère dans un code secret. La valeur par défaut est **0**.
    - **Longueur des séquences alphabétiques :** entrez la longueur maximale d'une séquence alphabétique dans un code secret. La valeur par défaut est **0**.
    - **Longueur des séquences numériques :** entrez la longueur maximale d'une séquence numérique dans un code secret. La valeur par défaut est **0**.
    - **Autoriser les utilisateurs à afficher le mot de passe :** indiquez si les utilisateurs peuvent afficher leurs codes secrets. La valeur par défaut est **Activé**.
    - **Configurer l'authentification biométrique**. Indiquez si vous souhaitez activer l'authentification biométrique. La valeur par défaut est **Désactivé**. Si vous la définissez sur **Activé**, vous pouvez définir les options suivantes :
      - **Autoriser empreinte digitale**. Sélectionnez cette option pour autoriser les utilisateurs à s'authentifier à l'aide d'une empreinte digitale.
      - **Autoriser iris**. Sélectionnez cette option pour autoriser les utilisateurs à

s'authentifier à l'aide de l'analyse de l'iris.

* **Chaînes interdites :** créez des chaînes interdites pour empêcher les utilisateurs d'utiliser des chaînes non sécurisées faciles à deviner, telles que « mot de passe », « mdp », « bienvenue », « 123456 », « 111111 », etc. Pour chaque chaîne que vous souhaitez interdire, cliquez sur **Ajouter**, puis procédez comme suit :
  · **Chaînes interdites :** entrez la chaîne que les utilisateurs ne peuvent pas utiliser.
  · Cliquez sur **Enregistrer** pour ajouter la chaîne ou sur **Annuler** pour annuler l'ajout de la chaîne.

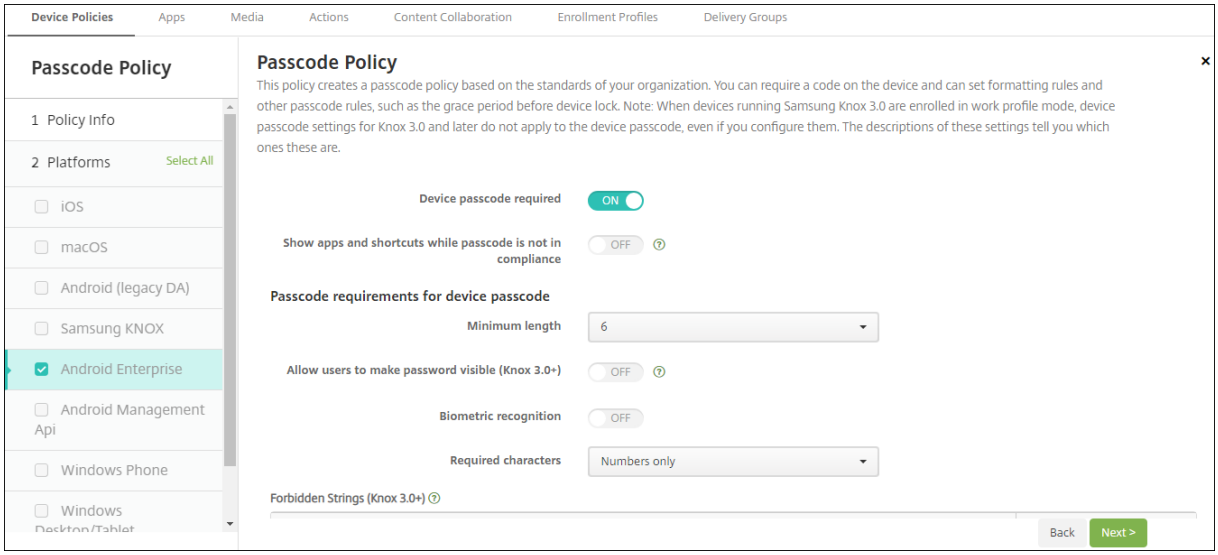
Paramètres Samsung KNOX



- **Exigences en matière de code secret**
  - **Longueur minimale :** dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est **6**.
  - **Autoriser les utilisateurs à afficher les mots de passe :** sélectionnez cette option pour autoriser les utilisateurs à afficher le mot de passe.
  - **Chaînes interdites :** créez des chaînes interdites pour empêcher les utilisateurs d'utiliser des chaînes non sécurisées faciles à deviner, telles que « mot de passe », « mdp », « bienvenue », « 123456 », « 111111 », etc. Pour chaque chaîne que vous souhaitez interdire, cliquez sur Ajouter, puis procédez comme suit :
    * **Chaînes interdites :** entrez la chaîne que les utilisateurs ne peuvent pas utiliser.
    * Cliquez sur **Enregistrer** pour ajouter la chaîne ou sur **Annuler** pour annuler l'ajout de la chaîne.
- **Nombre minimum de**
  - **Caractères modifiés :** entrez le nombre de caractères que les utilisateurs doivent changer par rapport à leur code secret précédent. La valeur par défaut est **0**.

  - **Symboles :** entrez le nombre minimum de symboles requis dans un code secret. La valeur par défaut est **0**.
- **Nombre maximum de**
  - **Nombre d'occurrences d'un caractère :** entrez le nombre maximal d'occurrences d'un caractère dans un code secret. La valeur par défaut est **0**.
  - **Longueur des séquences alphabétiques :** entrez la longueur maximale d'une séquence alphabétique dans un code secret. La valeur par défaut est **0**.
  - **Longueur des séquences numériques :** entrez la longueur maximale d'une séquence numérique dans un code secret. La valeur par défaut est **0**.
- **Sécurité du code secret**
  - **Verrouiller l'appareil après (minutes d'inactivité) :** dans la liste, cliquez sur le nombre de secondes pendant lesquelles un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est **Aucun**.
  - **Expiration du code secret en jours (1-730) :** entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
  - **Mots de passe précédents enregistrés (0-50) :** entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
  - **Si le nombre de tentatives de connexion infructueuses est dépassé, l'appareil est bloqué** : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil est verrouillé. La valeur par défaut est **Aucun nombre défini**.
  - **Si le nombre de tentatives de connexion infructueuses est dépassé, l'appareil est effacé :** dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses qu'un utilisateur peut effectuer avant que le conteneur KNOX (ainsi que les données KNOX) ne soient effacés de l'appareil. Les utilisateurs doivent réinitialiser le conteneur KNOX après l'effacement. La valeur par défaut est **Aucun nombre défini**.

Paramètres Android Enterprise



Pour les appareils Android Enterprise, vous pouvez demander un code secret pour l'appareil ou une question de sécurité pour le profil de travail Android Enterprise ou les deux.

Pour les appareils fonctionnant sous Android 8.0 ou version ultérieure et Samsung Knox 3.0 et versions ultérieures, configurez les paramètres de Samsung Knox sur la page **Android Enterprise**. Pour les appareils exécutant des versions antérieures d'Android ou de Samsung Knox, utilisez la page **Samsung Knox**.

> **Remarque :**
>
> Lorsque les appareils fonctionnant sous Samsung Knox 3.0 sont inscrits en tant qu'appareils avec profil de travail, les paramètres de code secret de l'appareil pour Knox 3.0 et versions ultérieures ne s'appliquent pas au code secret de l'appareil, même si vous les configurez.

- **Code secret de l'appareil requis :** exige un code secret sur l'appareil. Lorsque ce paramètre est défini sur **Activé**, configurez les paramètres sous **Exigences de code secret de l'appareil** et **Sécurité du code secret de l'appareil**. La valeur par défaut est **Désactivé**.
- **Afficher les applications et les raccourcis bien que le code d'accès ne soit pas conforme :**lorsque ce paramètre est **activé**, les applications et les raccourcis de l'appareil ne sont pas masqués, même lorsque le code d'accès n'est pas conforme. Lorsque ce paramètre est **désactivé**, les applications et les raccourcis sont masqués lorsque le code d'accès n'est pas conforme. Si vous activez ce paramètre, Citrix vous recommande de créer une action automatisée pour marquer l'appareil comme non conforme lorsque le code d'accès n'est pas conforme. La valeur par défaut est **Désactivé**.
- **Exigences de code secret de l'appareil :**
  - **Longueur minimale :** spécifie la longueur minimale du code secret. La valeur par défaut est 6.

- **Autoriser les utilisateurs à afficher les mots de passe :** paramètre utilisé pour les appareils fonctionnant sous Samsung Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée. Uniquement pour les appareils entièrement gérés. Ce paramètre ne s'applique pas aux appareils inscrits en tant qu'appareils avec profil de travail. Autorise les utilisateurs à afficher le mot de passe. La valeur par défaut est **Désactivé**.
- **Reconnaissance biométrique :** active la reconnaissance biométrique. Si ce paramètre est défini sur **Activé**, le champ **Caractères requis** est masqué. La valeur par défaut est **Désactivé**.
- **Caractères requis :** spécifie les types de caractères requis pour les codes secrets. Dans la liste, choisissez **Aucune restriction**, **Lettres et chiffres**, **Chiffres uniquement** ou **Lettres uniquement**. Utilisez **Aucune restriction** uniquement pour les appareils exécutant Android 7.0. Android 7.1 et versions ultérieures n'appliquent pas le paramètre **Aucune restriction**. La valeur par défaut est **Chiffres et lettres**.
- **Chaînes interdites :** paramètre utilisé pour les appareils fonctionnant sous Samsung Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée. Uniquement pour les appareils entièrement gérés. Ce paramètre ne s'applique pas aux appareils inscrits en tant qu'appareils avec profil de travail. Spécifie les chaînes que les utilisateurs ne peuvent pas utiliser comme codes secrets. Créez des chaînes interdites pour empêcher les utilisateurs d'utiliser des chaînes non sécurisées faciles à deviner, telles que « mot de passe », « mdp », « bienvenue », « 123456 », « 111111 », etc. Pour chaque chaîne que vous souhaitez refuser, cliquez sur **Ajouter** ; saisissez la chaîne que vous ne souhaitez pas utiliser ; cliquez sur **Enregistrer** pour ajouter la chaîne ou cliquez sur **Annuler** pour annuler l'ajout de la chaîne.
- **Règles avancées :** applique des règles avancées pour les types de caractères pouvant apparaître dans les codes secrets. Lorsque ce paramètre est défini sur **Activé**, configurez les paramètres sous **Nombre minimum de** et **Nombre maximum de**. Ce paramètre n'est pas disponible pour les appareils Android de versions antérieures à Android 5.0. La valeur par défaut est **Désactivé**.
- **Nombre minimum de :**
  * **Symboles :** spécifie le nombre minimal de symboles. La valeur par défaut est **0**.
  * **Lettres :** spécifie le nombre minimal de lettres. La valeur par défaut est **0**.
  * **Minuscules :** spécifie le nombre minimal de minuscules. La valeur par défaut est **0**.
  * **Majuscules :** spécifie le nombre minimal de majuscules. La valeur par défaut est **0**.
  * **Chiffres ou symboles :** spécifie le nombre minimal de chiffres ou de symboles. La valeur par défaut est **0**.
  * **Chiffres :** spécifie le nombre minimal de chiffres. La valeur par défaut est **0**.
  * **Caractères modifiés :** paramètre utilisé pour les appareils fonctionnant sous Samsung Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée. Uniquement pour les appareils entièrement gérés. Ce paramètre ne s'applique

pas aux appareils inscrits en tant qu'appareils avec profil de travail. Spécifie le nombre de caractères que les utilisateurs doivent modifier par rapport à leur code secret précédent. La valeur par défaut est **0**.

- **Nombre maximum de :** paramètre utilisé pour les appareils fonctionnant sous Samsung Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée. Uniquement pour les appareils entièrement gérés. Ce paramètre ne s'applique pas aux appareils inscrits en tant qu'appareils avec profil de travail.
  - **Nombre d'occurrences d'un caractère :** spécifie le nombre maximal d'occurrences d'un caractère dans un code secret. La valeur par défaut est **0**, ce qui signifie qu'il n'y a pas de limite maximale.
  - **Longueur des séquences alphabétiques :** spécifie la longueur maximale d'une séquence alphabétique dans un code secret. La valeur par défaut est **0**, ce qui signifie qu'il n'y a pas de limite maximale.
  - **Longueur des séquences numériques :** spécifie la longueur maximale d'une séquence numérique dans un code secret. La valeur par défaut est **0**, ce qui signifie qu'il n'y a pas de limite maximale.

- **Sécurité du code secret de l'appareil :**
  - **Effacer l'appareil après (tentatives de connexion infructueuses) :** indique le nombre de tentatives de connexion infructueuses pouvant être effectuées par l'utilisateur avant que l'appareil subisse un effacement complet. La valeur par défaut est **Aucun nombre défini**.
  - **Verrouiller l'appareil après (minutes d'inactivité) (0-999) :** indique le nombre de minutes pendant lesquelles un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est **Aucun**.
  - **Expiration du code secret en jours (1-730) :** indique le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
  - **Mots de passe précédents enregistrés (0-50) :** indique le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
  - **Verrouiller l'appareil après (tentatives de connexion infructueuses) :** paramètre utilisé pour les appareils fonctionnant sous Samsung Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée. Uniquement pour les appareils entièrement gérés. Ce paramètre ne s'applique pas aux appareils inscrits en tant qu'appareils avec profil de travail. Indique le nombre de tentatives de connexion infructueuses pouvant être effectuées par l'utilisateur avant que l'appareil ne soit verrouillé. La valeur par défaut est **Aucun nombre défini**.
- **Question de sécurité du profil de travail :** oblige les utilisateurs à répondre à une question de

sécurité pour accéder aux applications exécutées dans un profil de travail Android Enterprise. Cette fonctionnalité est destinée aux appareils exécutant Android 7.0 et versions ultérieures. Lorsque ce paramètre est défini sur **Activé**, configurez les paramètres sous **Exigences de code secret de la question de sécurité du profil de travail** et **Sécurité du code secret de la question de sécurité du profil de travail**. La valeur par défaut est **Désactivé**.

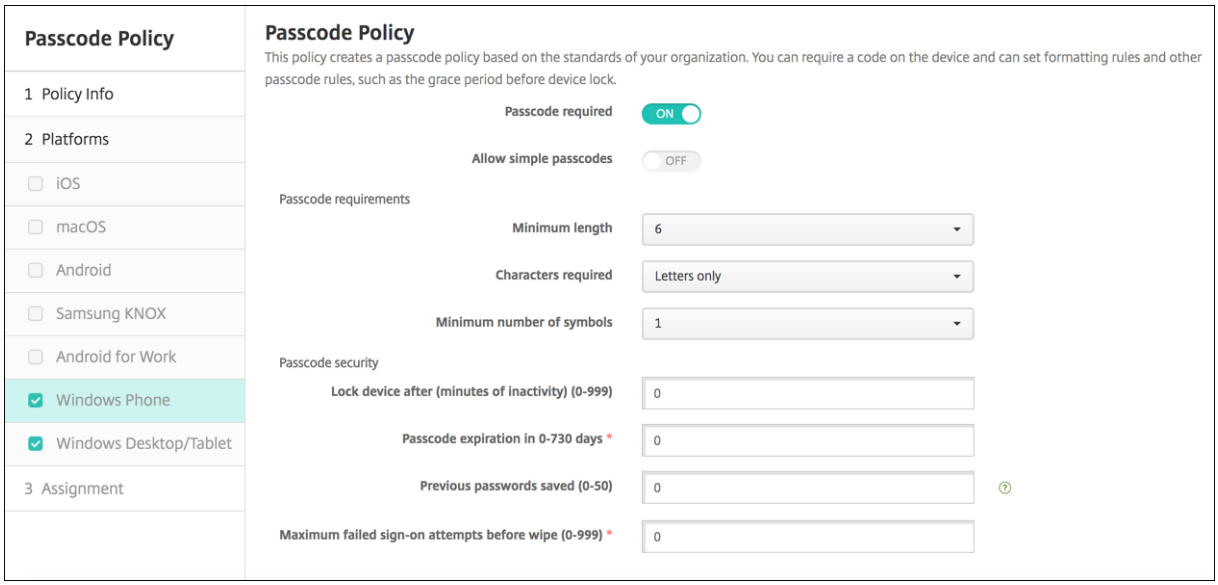
- **Exigences de code secret de validation de la sécurité du profil de travail :**
  - **Longueur minimale :** spécifie la longueur minimale du code secret. La valeur par défaut est 6.
  - **Autoriser les utilisateurs à afficher les mots de passe :** paramètre utilisé pour les appareils fonctionnant sous Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée. Autorise les utilisateurs à afficher le mot de passe. La valeur par défaut est **Désactivé**.
  - **Reconnaissance biométrique :** active la reconnaissance biométrique. Si ce paramètre est défini sur **Activé**, le champ **Caractères requis** est masqué. La valeur par défaut est **Désactivé**.
  - **Caractères requis :** spécifie les types de caractères requis pour les codes secrets. Dans la liste, choisissez **Aucune restriction**, **Lettres et chiffres**, **Chiffres uniquement** ou **Lettres uniquement**. Utilisez **Aucune restriction** uniquement pour les appareils exécutant Android 7.0. Android 7.1 et versions ultérieures n'appliquent pas le paramètre **Aucune restriction**. La valeur par défaut est **Chiffres et lettres**.
  - **Chaînes interdites :** paramètre utilisé pour les appareils fonctionnant sous Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée. Spécifie les chaînes que les utilisateurs ne peuvent pas utiliser comme codes secrets. Créez des chaînes interdites pour empêcher les utilisateurs d'utiliser des chaînes non sécurisées faciles à deviner, telles que « mot de passe », « mdp », « bienvenue », « 123456 », « 111111 », etc. Pour chaque chaîne que vous souhaitez refuser, cliquez sur **Ajouter** ; saisissez la chaîne que vous ne souhaitez pas utiliser ; cliquez sur **Enregistrer** pour ajouter la chaîne ou cliquez sur **Annuler** pour annuler l'ajout de la chaîne.
  - **Règles avancées :** applique des règles avancées pour les types de caractères pouvant apparaître dans les codes secrets. Lorsque ce paramètre est défini sur **Activé**, configurez les paramètres sous **Nombre minimum de** et **Nombre maximum de**. Ce paramètre n'est pas disponible pour les appareils Android de versions antérieures à Android 5.0. La valeur par défaut est **Désactivé**.
  - **Nombre minimum de :**
    - **Symboles :** spécifie le nombre minimal de symboles. La valeur par défaut est **0**.
    - **Lettres :** spécifie le nombre minimal de lettres. La valeur par défaut est **0**.
    - **Minuscules :** spécifie le nombre minimal de minuscules. La valeur par défaut est **0**.
    - **Majuscules :** spécifie le nombre minimal de majuscules. La valeur par défaut est **0**.
    - **Chiffres ou symboles :** spécifie le nombre minimal de chiffres ou de symboles. La

valeur par défaut est **0**.
    * **Chiffres :** spécifie le nombre minimal de chiffres. La valeur par défaut est **0**.
    * **Caractères modifiés :** paramètre utilisé pour les appareils fonctionnant sous Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée. Spécifie le nombre de caractères que les utilisateurs doivent modifier par rapport à leur code secret précédent. La valeur par défaut est **0**.
  - **Nombre maximum de :** paramètre utilisé pour les appareils fonctionnant sous Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée.
    * **Nombre d'occurrences d'un caractère :** spécifie le nombre maximal d'occurrences d'un caractère dans un code secret. La valeur par défaut est **0**, ce qui signifie qu'il n'y a pas de limite maximale.
    * **Longueur des séquences alphabétiques :** spécifie la longueur maximale d'une séquence alphabétique dans un code secret. La valeur par défaut est **0**, ce qui signifie qu'il n'y a pas de limite maximale.
    * **Longueur des séquences numériques :** spécifie la longueur maximale d'une séquence numérique dans un code secret. La valeur par défaut est **0**, ce qui signifie qu'il n'y a pas de limite maximale.
  - **Activer le code secret unifié :** si cette option est définie sur **Activé**, les utilisateurs utilisent un code secret pour leur appareil et leur profil de travail. Si cette option est définie sur **Désactivé** :
    * Les utilisateurs doivent utiliser différents codes secrets pour leur appareil et leur profil de travail.
    * Le paramètre **Utiliser une seule méthode de verrouillage** sur l'appareil, défini par les utilisateurs s'ils souhaitent utiliser le même code secret pour leur appareil et leur profil de travail, est désactivé. L'utilisateur ne peut pas l'activer.
    * Si l'exigence de code secret pour la question de sécurité du profil de travail est plus complexe que le code secret de l'appareil : les utilisateurs dont le paramètre **Utiliser une seule méthode de verrouillage** est activé sont invités à modifier leur code secret de profil de travail.

    La valeur par défaut est **Désactivé**. Disponible à partir d'Android 9.0.
- **Sécurité du code secret de la question de sécurité du profil de travail**
  - **Effacer le conteneur après (tentatives de connexion infructueuses) :** indique le nombre de tentatives de connexion infructueuses pouvant être effectuées par l'utilisateur avant que le profil de travail et ses données ne soient effacés de l'appareil. Les utilisateurs doivent réinitialiser le profil de travail après l'effacement. La valeur par défaut est **Aucun nombre défini**.
  - **Verrouiller le conteneur après (minutes d'inactivité) :** indique le nombre de minutes pendant lesquelles un appareil peut rester inactif avant que le profil de travail ne soit verrouillé. La valeur par défaut est **Aucun**.

- **Expiration du code secret en jours (1-730) :** indique le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
- **Mots de passe précédents enregistrés (0-50) :** indique le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
- **Verrouiller le conteneur après (tentatives de connexion infructueuses) :** paramètre utilisé pour les appareils fonctionnant sous Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée. Indique le nombre de tentatives de connexion infructueuses pouvant être effectuées par l'utilisateur avant que l'appareil ne soit verrouillé. La valeur par défaut est **Aucun nombre défini**.

Paramètres Windows Phone



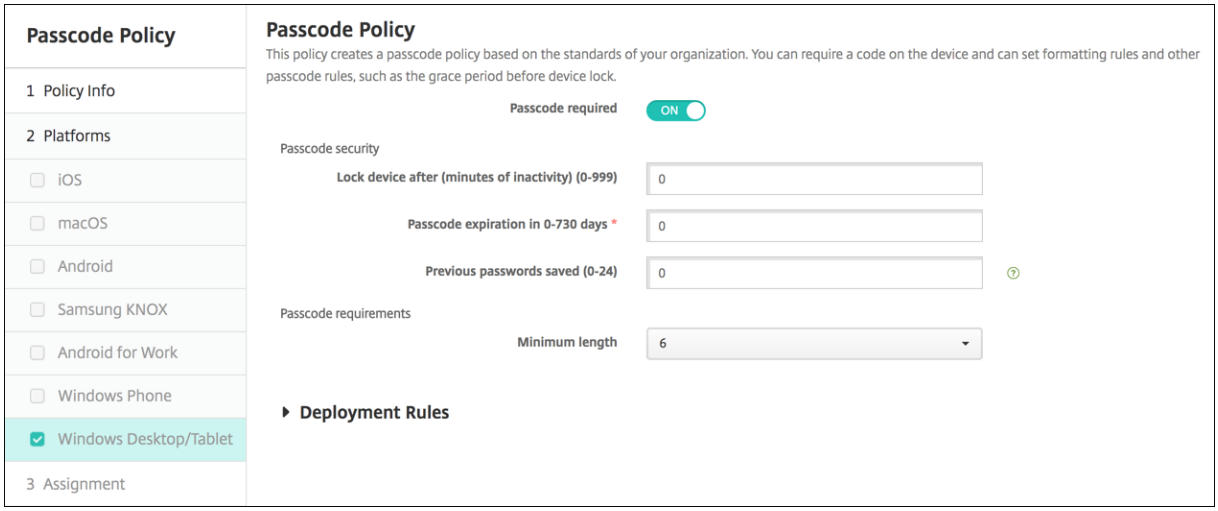
- **Code secret requis :** sélectionnez cette option pour ne pas exiger de code secret sur les appareils Windows Phone. Le paramètre par défaut est **Activé**, ce qui nécessite un code secret. La page se réduit et les options suivantes disparaissent lorsque vous désactivez ce paramètre.
- **Autoriser les codes secrets simples :** sélectionnez cette option pour autoriser les codes secrets simples. Les codes secrets simples se caractérisent par des caractères répétés ou séquentiels. La valeur par défaut est Désactivé.
- **Exigences en matière de code secret**
  - **Longueur minimale :** dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est **6**.
  - **Caractères requis :** dans la liste, cliquez sur **Numérique ou alphanumérique**, **Lettres uniquement** ou **Chiffres uniquement** pour configurer la manière dont les codes secrets

sont composés. La valeur par défaut est **Lettres uniquement**.

- **Nombre minimum de symboles :** dans la liste, cliquez sur le nombre de symboles que le code secret doit contenir. La valeur par défaut est **1**.

- **Sécurité du code secret**
  - **Verrouiller l'appareil après (minutes d'inactivité) :** entrez le nombre de minutes pendant lesquelles un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est **0**.
  - **Expiration du mot de passe dans 0-730 jours :** entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 0-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
  - **Mots de passe précédents enregistrés (0-50) :** entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
  - **Nombre maximum de tentatives de connexion infructueuses avant effacement (0-999) :** entrez le nombre de tentatives de connexion infructueuses qu'un utilisateur peut effectuer avant que les données d'entreprise ne soient effacées de l'appareil. La valeur par défaut est **0**.

Paramètres Windows Desktop/Tablet



- **Interdire les dispositifs de connexion pratiques :** sélectionnez cette option pour autoriser les utilisateurs à accéder à leurs appareils à l'aide de mots de passe image ou d'ouvertures de session biométriques. La valeur par défaut est **Désactivé**.
- **Longueur minimum du code secret :** dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est **6**.
- **Nombre maximum de tentatives de saisie du code secret avant effacement :** dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses qu'un utilisateur peut effectuer

avant que les données d'entreprise ne soient effacées de l'appareil. La valeur par défaut est **4**.

- **Expiration du code secret en jours (0 - 730) :** entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 0-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
- **Historique du code secret (1 - 24) :** entrez le nombre de codes secrets utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des codes secrets figurant dans cette liste. Les valeurs autorisées sont 1-24. Vous devez entrer un nombre compris entre 1 et 24. La valeur par défaut est **0**.
- **Période d'inactivité maximale avant verrouillage de l'appareil en minutes (1-999) :** entrez la durée en minutes pendant laquelle un appareil peut rester inactif avant d'être verrouillé. Les valeurs autorisées sont 1-999. Vous devez entrer un nombre compris entre 1 et 999. La valeur par défaut est **0**.

Stratégie Personal Hotspot

January 10, 2022

Vous pouvez autoriser les utilisateurs à se connecter à Internet lorsqu'ils ne sont pas à portée d'un réseau Wi-Fi en utilisant la connexion des données cellulaires au travers de la fonctionnalité Partage de connexion (Personal Hotspot) de leurs appareils iOS. Disponible sur iOS 7.0 et version ultérieure.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Désactiver Personal Hotspot :** sélectionnez cette option pour désactiver la fonctionnalité Partage de connexion (Personal Hotspot) sur les appareils des utilisateurs. La valeur par défaut est **Désactivé**, ce qui désactive Partage de connexion (Personal Hotspot) sur les appareils des utilisateurs. Cette stratégie ne désactive pas la fonctionnalité. Les utilisateurs peuvent toujours utiliser Partage de connexion (Personal Hotspot) sur leurs appareils, mais lorsque la stratégie est déployée, Personal Hotspot est désactivé de manière à ne pas rester activé par défaut.

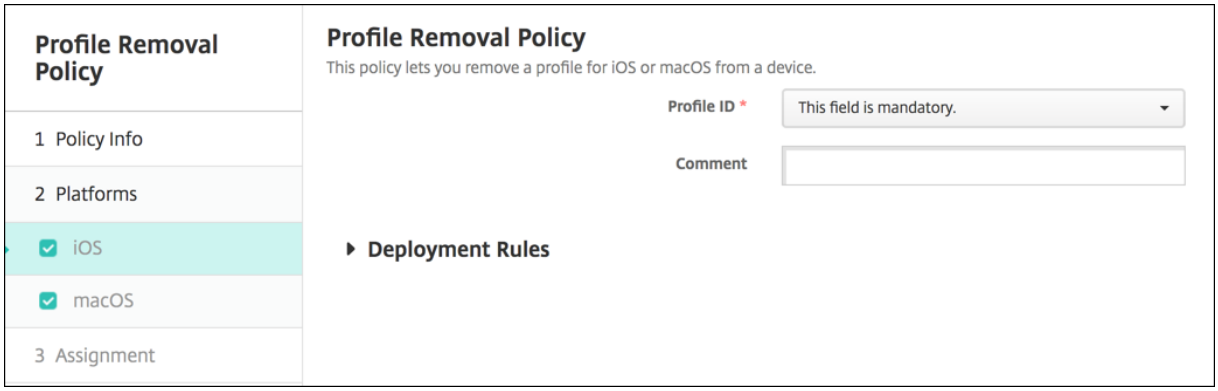
Stratégie de suppression de profil

January 10, 2022

Vous pouvez créer une stratégie de suppression de profil dans XenMobile. La stratégie, lorsqu'elle est déployée, supprime le profil d'application des appareils iOS ou macOS des utilisateurs.

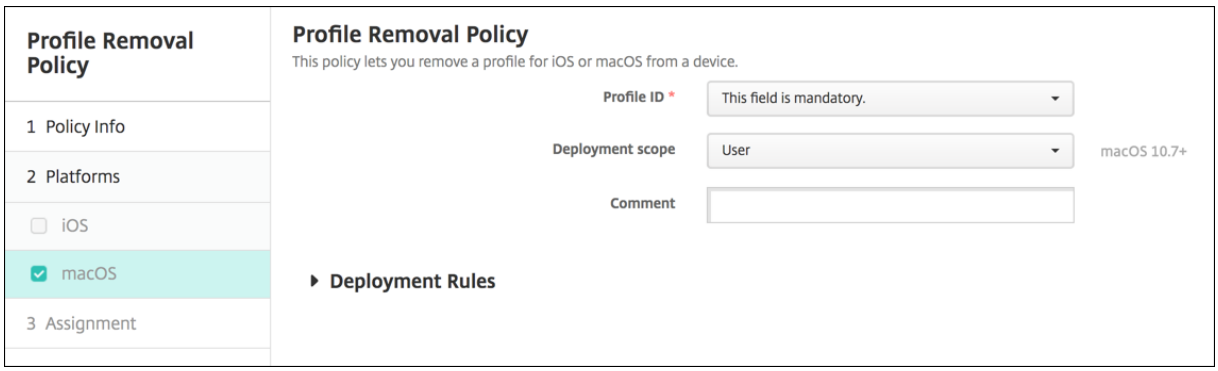
Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **ID du profil :** dans la liste, cliquez sur l'ID du profil d'application. Ce champ est obligatoire.
- **Commentaires :** entrez un commentaire (facultatif).

Paramètres macOS



- **ID du profil :** dans la liste, cliquez sur l'ID du profil d'application. Ce champ est obligatoire.
- **Étendue du déploiement :** dans la liste, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.
- **Commentaires :** entrez un commentaire (facultatif).

Stratégie de profil de provisioning

January 10, 2022

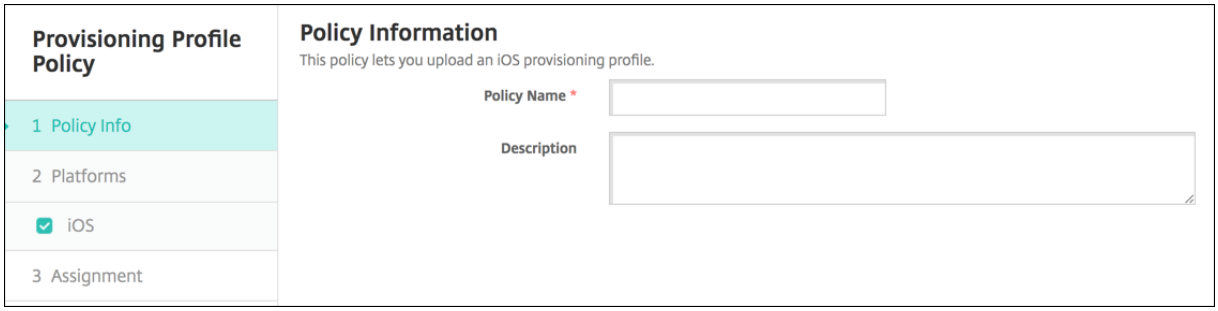
Lorsque vous développez et codez une application d'entreprise iOS, vous incluez généralement un profil de provisioning de distribution d'entreprise, dont Apple a besoin pour que l'application s'exécute sur un appareil iOS. Si un profil de provisioning est manquant, ou s'il a expiré, l'application se bloque lorsque l'utilisateur tape pour l'ouvrir.

Le principal problème avec les profils de provisioning est qu'ils expirent un an après qu'ils sont générés sur le portail Apple Developer et vous devez conserver les dates d'expiration pour tous les profils de provisioning sur tous les appareils iOS inscrits par vos utilisateurs. Le suivi des dates d'expiration non seulement implique de surveiller les dates d'expiration, mais aussi quels utilisateurs utilisent quelle version de l'application. Les deux solutions consistent à envoyer par e-mail les profils de provisioning aux utilisateurs ou à les placer dans un portail Web pour le téléchargement et l'installation. Ces solutions fonctionnent, mais elles peuvent entraîner des erreurs car elles requièrent que les utilisateurs réagissent à des instructions dans un e-mail ou accèdent au portail Web pour télécharger le profil approprié et l'installer.

Pour effectuer cette opération de façon transparente pour les utilisateurs, dans XenMobile, vous pouvez installer et supprimer les profils de provisioning avec les stratégies d'appareil. Les profils manquants ou arrivés à expiration sont supprimés si nécessaire et des profils à jour sont installés sur les appareils des utilisateurs, de façon à ce qu'il leur suffise de taper sur une application pour l'ouvrir.

Avant de pouvoir créer une stratégie de profil de provisioning, vous devez créer un fichier de profil de provisioning. Pour plus d'informations, consultez l'article Apple sur la création d'un profil de provisioning de développement sur le site pour développeurs Apple.

Paramètres iOS



- **Profil de provisioning iOS :** sélectionnez le fichier de profil de provisioning à importer en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

Stratégie de suppression de profil de provisioning

January 10, 2022

Vous pouvez supprimer des profils de provisioning iOS avec des stratégies d'appareil. Pour de plus amples informations sur les profils de provisioning, consultez la section Stratégie de profil de provisioning.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Profil de provisioning iOS :** dans la liste, cliquez sur le profil de provisioning que vous souhaitez supprimer.
- **Commentaire :** si vous le souhaitez, ajoutez un commentaire.

Stratégie de proxy

January 10, 2022

Vous pouvez ajouter une stratégie dans XenMobile pour spécifier les paramètres de proxy HTTP globaux pour les appareils exécutant Windows Mobile/CE et iOS 6.0 ou version ultérieure. Vous ne pouvez déployer qu'une stratégie de proxy HTTP globale par appareil.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Conditions préalables

Avant de déployer cette stratégie, assurez-vous de définir tous les appareils iOS pour lesquels vous souhaitez définir un proxy HTTP global en mode supervisé. Pour plus de détails, consultez Pour placer un appareil iOS en mode supervisé à l'aide d'Apple Configurator ou Déployer des appareils via le programme de déploiement d'Apple.

Définissez des règles de déploiement pour inscrire les appareils avant d'envoyer la stratégie Proxy aux appareils.

Paramètres iOS

- **Configuration du proxy :** cliquez sur **Manuel** ou **Automatique** pour choisir la méthode à utiliser pour configurer le proxy sur les appareils des utilisateurs.
  - Si vous avez sélectionné **Manuel**, configurez les paramètres suivants :
    - **Nom d'hôte ou adresse IP du serveur proxy :** entrez le nom d'hôte ou l'adresse IP du serveur proxy. Ce champ est obligatoire.
    - **Port du serveur proxy :** entrez le numéro de port du serveur proxy. Ce champ est obligatoire.
    - **Nom d'utilisateur :** entrez un nom d'utilisateur pour l'authentification auprès du serveur proxy (facultatif).
    - **Mot de passe :** entrez un mot de passe pour l'authentification auprès du serveur proxy (facultatif).
  - Si vous avez sélectionné **Automatique**, configurez les paramètres suivants :
    - **URL du fichier de configuration automatique de proxy :** entrez l'adresse URL du fichier PAC qui définit la configuration proxy.
    - **Autoriser la connexion directe si le PAC est injoignable :** indiquez si les utilisateurs sont autorisés à se connecter directement à la destination si le fichier PAC est inaccessible. La valeur par défaut est **Activé**. Cette option est disponible uniquement sur iOS 7.0 et versions ultérieures.
- **Autoriser le contournement du proxy pour accéder aux réseaux captifs :** sélectionnez cette option pour autoriser le contournement du proxy afin d'accéder aux réseaux captifs. La valeur par défaut est **Désactivé**.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres Windows Mobile/CE

- **Réseau :** dans la liste, cliquez sur le type de réseau à utiliser. La valeur par défaut est **Bureau intégré**. Les options possibles sont les suivantes :
  - Bureau
  - Internet

  - Bureau intégré
  - Internet intégré
- **Réseau :** dans la liste, cliquez sur le protocole de connexion réseau à utiliser. La valeur par défaut est **HTTP**. Les options possibles sont les suivantes :
  - HTTP
  - WAP
  - Socks 4
  - Socks 5
- **Nom d'hôte ou adresse IP du serveur proxy :** entrez le nom d'hôte ou l'adresse IP du serveur proxy. Ce champ est obligatoire.
- **Port du serveur proxy :** entrez le numéro de port du serveur proxy. Ce champ est obligatoire. La valeur par défaut est **80**.
- **Nom d'utilisateur :** entrez un nom d'utilisateur pour l'authentification auprès du serveur proxy (facultatif).
- **Mot de passe :** entrez un mot de passe pour l'authentification auprès du serveur proxy (facultatif).
- **Nom de domaine :** entrez le nom du domaine (facultatif).
- **Activer :** sélectionnez cette option pour activer le proxy. La valeur par défaut est **Activé**.

Stratégie de Registre

January 10, 2022

Le registre Windows Mobile/CE stocke des données sur les applications, pilotes, préférences utilisateur et paramètres de configuration. Dans XenMobile, vous pouvez définir les clés et valeurs de registre qui vous permettent de gérer les appareils Windows Mobile/CE.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Windows Mobile/CE

Pour chaque clé de registre ou paire de clé/valeur de registre que vous souhaitez ajouter, cliquez sur **Ajouter** et procédez comme suit :

- **Chemin d'accès à la clé de Registre :** entrez le chemin d'accès complet pour la clé de registre. Par exemple, tapez **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows** pour spécifier le chemin vers la clé Windows à partir de la clé racine HKEY_LOCAL_MACHINE.
- **Nom de valeur de Registre :** entrez le nom de la valeur de la clé de registre. Par exemple, tapez **ProgramFilesDir** pour ajouter ce nom de valeur au chemin de la clé de registre

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion. Si vous laissez ce champ vide, cela signifie que vous ajoutez une clé de registre et non une paire clé/valeur de registre.

- **Type :** dans la liste, cliquez sur le type de données pour la valeur. La valeur par défaut est **DWORD**. Les options possibles sont les suivantes :
  - **DWORD :** entier non signé 32 bits.
  - **Chaîne :** toute chaîne.
  - **Chaîne étendue :** valeur de chaîne qui peut contenir des variables d'environnement comme %TEMP% ou %USERPROFILE%.
  - **Binaire :** toutes données binaires arbitraires.
- **Valeur :** entrez la valeur associée au nom de la valeur de registre. Par exemple, pour spécifier la valeur de ProgramFilesDir, tapez **C:\Program Files**.
- Cliquez sur **Enregistrer** pour enregistrer les informations de clé de registre ou cliquez sur **Annuler** pour ne pas enregistrer ces informations de clé de registre.

Stratégie d'assistance à distance

January 10, 2022

> **Remarque :**
>
> Pour les déploiements locaux de XenMobile Server : l'Assistance à distance permet aux représentants du service d'assistance de contrôler à distance des appareils mobiles Windows CE et Android gérés. La capture d'écran est uniquement prise en charge sur les appareils Samsung KNOX.
>
> L'Assistance à distance n'est pas prise en charge pour les déploiements de XenMobile Server locaux en cluster.
>
> Pour plus d'informations, consultez la section Options d'assistance et assistance à distance.

Vous créez une stratégie d'assistance à distance dans XenMobile pour vous permettre d'accéder à distance aux appareils Windows et Android pris en charge. Vous pouvez configurer deux types d'assistance :

- **Assistance à distance de base** : cette option vous permet d'afficher des informations de diagnostic sur l'appareil, telles que les informations système, les processus en cours d'exécution, le gestionnaire des tâches (utilisation de mémoire et de l'UC), le contenu du dossier des logiciels installés, etc.
- **Assistance à distance premium** : cette option vous permet de contrôler à distance l'écran de l'appareil, notamment :
  - contrôler les couleurs (dans la fenêtre principale, où dans une fenêtre séparée flottante)
  - établir une session Voix sur IP (VoIP) entre le service d'assistance et l'utilisateur

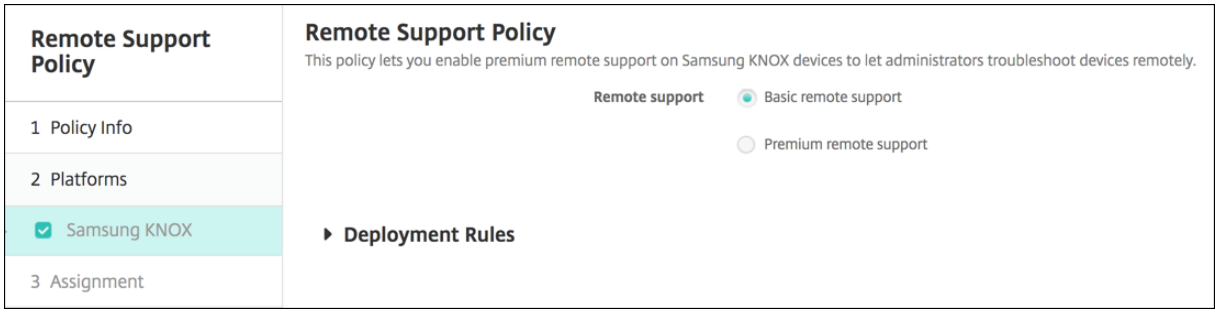
  - configurer les paramètres
  - établir une session de chat entre le support technique et l'utilisateur.

Pour implémenter cette stratégie, vous devez effectuer les tâches suivantes :

- Installez l'application d'assistance à distance XenMobile dans votre environnement.
- Configurez un tunnel applicatif d'assistance à distance. Pour plus de détails, consultez la section Stratégies de tunnel applicatif.
- Configurez une stratégie d'assistance à distance Samsung KNOX comme décrit dans cette rubrique.
- Déployez la stratégie d'assistance à distance de tunnel applicatif et Samsung KNOX sur les appareils des utilisateurs.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Android et Windows CE



- **Assistance à distance :** sélectionnez **Assistance à distance de base** ou **Assistance à distance premium**. La valeur par défaut est **Assistance à distance de base**.

Stratégie de restrictions

January 10, 2022

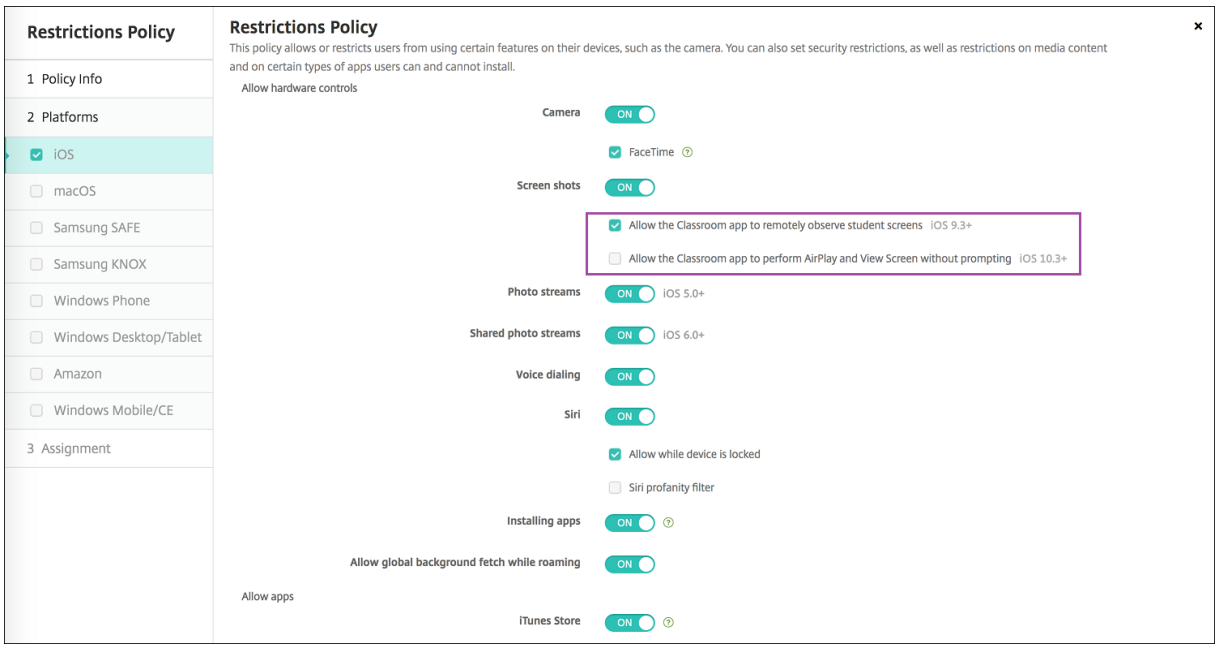
La stratégie Restrictions autorise ou restreint certaines fonctionnalités sur les appareils des utilisateurs, telles que l'appareil photo. Vous pouvez également définir des restrictions de sécurité, des restrictions d'accès au contenu multimédia ainsi que des restrictions sur les types d'applications que les utilisateurs peuvent ou ne peuvent pas installer. La plupart des paramètres de restriction sont réglés par défaut sur **Activé** ou *autorise*. Les principales exceptions sont la fonctionnalité Sécuriser - Forcer dans iOS et toutes les fonctionnalités de Windows Tablet, lesquelles prennent par défaut la valeur **Désactivé** ou appliquent des *restrictions*.

Pour Windows 10 RS2 Phone : une fois qu'une stratégie XML personnalisée ou Restrictions qui désactive Internet Explorer a été déployée sur le téléphone, le navigateur reste activé. Pour contourner ce problème, redémarrez le téléphone. Il s'agit d'un problème de tiers.

> **Conseil :**
>
> Toute option définie sur **Activé** signifie que l'utilisateur peut effectuer l'opération ou utiliser la fonctionnalité. Par exemple :
>
> **Appareil photo**. Si l'option est réglée sur **Activé**, l'utilisateur peut utiliser l'appareil photo sur son appareil. Si l'option est réglée sur **Désactivé**, l'utilisateur ne peut pas utiliser l'appareil photo sur son appareil.
>
> **Captures d'écrans**. Si l'option est réglée sur **Activé**, l'utilisateur peut prendre des captures d'écrans sur son appareil. Si l'option est réglée sur **Désactivé**, l'utilisateur ne peut pas prendre de captures d'écrans sur son appareil.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



Certains paramètres de stratégie de restrictions iOS s'appliquent uniquement à des versions spécifiques d'iOS, comme indiqué ici et sur la page de stratégie Restrictions de la console XenMobile.

Les paramètres de stratégie de restrictions iOS peuvent également s'appliquer lorsque l'appareil est inscrit en mode d'inscription de l'utilisateur, en mode non supervisé (MDM complet) ou en mode supervisé. Le tableau suivant présente les modes d'inscription disponibles pour chaque paramètre de

stratégie de restrictions pour iOS 13 et versions ultérieures.

Comme indiqué dans le tableau, certains paramètres qui étaient auparavant disponibles en mode non supervisé et supervisé ne sont disponibles qu'en mode supervisé à partir de la version iOS 13. Les règles suivantes s'appliquent :

- Si un appareil iOS 13+ supervisé est inscrit dans XenMobile, les paramètres s'appliquent à l'appareil.
- Si un appareil iOS 13+ non supervisé est inscrit dans XenMobile, les paramètres ne s'appliquent pas à l'appareil.
- Si un appareil iOS 12 (ou version inférieure) déjà inscrit dans XenMobile est mis à niveau vers iOS 13, il n'y a aucune modification. Les paramètres s'appliquent à l'appareil comme avant la mise à niveau.

Pour de plus amples informations sur la configuration d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

Paramètre	Inscription de l'utilisateur	Non supervisé	Supervisé
Autoriser le contrôle du matériel			
Caméra	Non	Oui	Oui
FaceTime	Non	Non (nouveau paramètre dans iOS 13)	Oui
Captures d'écran	Oui	Non	Oui
Autoriser l'application En classe à observer à distance les écrans des étudiants	Non	Non	Oui
Autoriser l'application En classe à modifier les autorisations AirPlay et Voir l'écran sans invite	Non	Non	Oui
Flux de photos	Non	Oui	Oui
Flux de photos partagés	Non	Oui	Oui
Composition vocale	Non	Oui	Oui

Paramètre	Inscription de l'utilisateur	Non supervisé	Supervisé
Siri	Oui	Oui	Oui
Autoriser lorsque l'appareil est verrouillé	Oui	Oui	Oui
Filtre d'obscénité de Siri	Non	Non	Oui
Installation d'applications	Non	Non (nouveau paramètre dans iOS 13)	Oui
Autoriser récupération en arrière-plan globale en cas d'itinérance	Non	Oui	Oui
Autoriser les applications			
iTunes Store	Non	Non (nouveau paramètre dans iOS 13)	Oui
Achats dans les applications	Non	Oui	Oui
Exiger le mot de passe iTunes pour tous les achats	Non	Oui	Oui
Safari	Non	Non (nouveau paramètre dans iOS 13)	Oui
Remplissage automatique	Non	Non (nouveau paramètre dans iOS 13)	Oui
Forcer l'avertissement de fraude	Oui	Oui	Oui
Activer JavaScript	Non	Oui	Oui

Paramètre	Inscription de l'utilisateur	Non supervisé	Supervisé
Bloquer les fenêtres contextuelles	Non	Oui	Oui
Accepter les cookies	Non	Oui	Oui
Réseau - Autoriser les actions iCloud			
Documents et données iCloud	Non	Non (nouveau paramètre dans iOS 13)	Oui
Sauvegarde iCloud	Non	Oui	Oui
Trousseau iCloud	Non	Oui	Oui
Photothèque iCloud	Non	Oui	Oui
Sécurité - Forcer			
Copies de sauvegarde chiffrées	Oui	Oui	Oui
Suivi limité des publicités	Non	Oui	Oui
Code secret lors du premier couplage AirPlay	Oui	Oui	Oui
Apple Watch jumelée pour utiliser la détection du poignet	Oui	Oui	Oui
Partage des documents gérés avec AirDrop	Oui	Oui	Oui
Sécurité - Autoriser			
Accepter des certificats SSL non approuvés	Non	Oui	Oui

Paramètre	Inscription de l'utilisateur	Non supervisé	Supervisé
Mise à jour automatique des paramètres d'approbation de certificat	Non	Oui	Oui
Documents provenant d'applications gérées dans les applications non gérées	Oui	Oui	Oui
Les applications non gérées lisent les contacts gérés	Non	Non	Oui
Les applications gérées écrivent sur les contacts non gérés	Non	Non	Oui
Documents provenant d'applications non gérées dans les applications gérées	Oui	Oui	Oui
Envoi d'informations de diagnostic à Apple	Oui	Oui	Oui
Touch ID pour déverrouiller un appareil	Non	Oui	Oui
Notifications Passbook lorsque l'appareil est verrouillé	Non	Oui	Oui
Handoff	Non	Oui	Oui
Synchronisation iCloud pour applications gérées	Oui	Oui	Oui

Paramètre	Inscription de l'utilisateur	Non supervisé	Supervisé
Sauvegarde de livres d'entreprise	Oui	Oui	Oui
Synchronisation des notes et des extraits pour les livres d'entreprise	Oui	Oui	Oui
Résultats Internet dans Spotlight	Non	Oui	Oui
Faire confiance aux applications d'entreprise	Non	Oui	Oui
Paramètres supervisés uniquement - Autoriser			
Effacer tout le contenu et les paramètres	Non	Non	Oui
Configuration des restrictions	Non	Non	Oui
Podcasts	Non	Non	Oui
Installation des profils de configuration	Non	Non	Oui
Modification de l'empreinte digitale	Non	Non	Oui
Installation des applications de l'appareil	Non	Non	Oui
Raccourcis clavier	Non	Non	Oui
Apple Watch couplée	Non	Non	Oui
Modification du code secret	Non	Non	Oui

Paramètre	Inscription de l'utilisateur	Non supervisé	Supervisé
Modification du nom de l'appareil	Non	Non	Oui
Modification du fond d'écran	Non	Non	Oui
Téléchargement automatique des applications	Non	Non	Oui
AirDrop	Non	Non	Oui
iMessage	Non	Non	Oui
Contenu généré par l'utilisateur dans Siri	Non	Non	Oui
iBooks	Non	Non	Oui
Suppression d'applications	Non	Oui	Oui
Game Center	Non	Non (nouveau paramètre dans iOS 13)	Oui
Ajouter des amis	Non	Non	Oui
Jeux multijoueurs	Non	Non (nouveau paramètre dans iOS 13)	Oui
Modification des paramètres de compte	Non	Non	Oui
Modification des paramètres des données cellulaires d'application	Non	Non	Oui
Modification des paramètres des données cellulaires d'application	Non	Non	Oui

Paramètre	Inscription de l'utilisateur	Non supervisé	Supervisé
Modification des paramètres Localiser mes amis	Non	Non	Oui
Couplage avec des hôtes non Configurator	Non	Non	Oui
Claviers intuitifs	Non	Non	Oui
Clavier avec correction automatique	Non	Non	Oui
Clavier avec correction d'orthographe	Non	Non	Oui
Recherche des définitions	Non	Non	Oui
Bundle ID d'application unique			
Actualités	Non	Non	Oui
Service Apple Music	Non	Non	Oui
iTunes Radio	Non	Non	Oui
Modification des notifications	Non	Non	Oui
Utilisation restreinte des apps	Non	Non	Oui
Modification de l'envoi de diagnostics	Non	Non	Oui
Modification Bluetooth	Non	Non	Oui
Autoriser la dictée	Non	Non	Oui

Paramètre	Inscription de l'utilisateur	Non supervisé	Supervisé
Rejoindre uniquement les réseaux Wi-Fi installés par une stratégie Wi-Fi	Non	Non	Oui
Autoriser l'application En classe à modifier les autorisations AirPlay et Voir l'écran sans invite	Non	Non	Oui
Autoriser l'application En classe à verrouiller une application et l'appareil sans invite	Non	Non	Oui
Rejoindre automatiquement les cours de l'application En classe sans invite	Non	Non	Oui
Autoriser AirPrint	Non	Non	Oui
Autoriser le stockage des identifiants AirPrint dans le trousseau	Non	Non	Oui
Autoriser la détection des imprimantes AirPrint à l'aide d'iBeacons	Non	Non	Oui
Autoriser AirPrint uniquement sur les destinations avec des certificats approuvés	Non	Non	Oui
Ajout de configurations VPN	Non	Non	Oui

Paramètre	Inscription de l'utilisateur	Non supervisé	Supervisé
Modification des paramètres du forfait de données	Non	Non	Oui
Suppression des applications système	Non	Non	Oui
Configuration des nouveaux appareils à proximité	Non	Non	Oui
Autoriser le mode restreint USB	Non	Non	Oui
Retarder les mises à jour logicielles	Non	Non	Oui
Délai imposé pour les mises à jour logicielles	Non	Non	Oui
Exiger la permission de En classe pour quitter les classes	Non	Non	Oui
Forcer réglage automatique de la date et l'heure	Non	Non	Oui
Remplissage automatique du mot de passe	Non	Non	Oui
Demander mot de passe des contacts à proximité	Non	Non	Oui
Partage de mot de passe	Non	Non	Oui
Sécurité - Afficher dans l'écran de verrouillage			
Centre de contrôle	Oui	Oui	Oui
Notification	Oui	Oui	Oui

Paramètre	Inscription de l'utilisateur	Non supervisé	Supervisé
Vue Aujourd'hui	Oui	Oui	Oui
Contenu multimédia - Autoriser			
Musique, podcasts et cours iTunes U explicites	Non	Non (nouveau paramètre dans iOS 13)	Oui
Contenu sexuel explicite dans iBooks	Non	Oui	Oui
Classements par région	Non	Oui	Oui
Films	Non	Oui	Oui
Séries TV	Non	Oui	Oui
Applications	Non	Oui	Oui

- **Autoriser le contrôle du matériel**
  - **Appareil photo :** autorise les utilisateurs à utiliser l'appareil photo sur leurs appareils.
    - **FaceTime :** autorise les utilisateurs à utiliser FaceTime sur leurs appareils. Pour les appareils iOS supervisés.
  - **Capture d'écran :** autorise les utilisateurs à prendre des captures d'écrans sur leurs appareils.
    - **Autoriser l'application En classe à observer à distance les écrans des étudiants :** si cette restriction n'est pas sélectionnée, un instructeur ne peut pas utiliser l'application En classe pour observer les écrans des étudiants. Le paramètre par défaut est sélectionné, un instructeur peut utiliser l'application En classe pour observer les écrans des étudiants. Le paramètre **Autoriser l'application En classe à modifier les autorisations AirPlay et Voir l'écran sans invite** détermine si les élèves reçoivent une invite pour autoriser l'instructeur. Pour les appareils iOS supervisés.
    - **Autoriser l'application En classe à modifier les autorisations AirPlay et Voir l'écran sans invite :** si cette restriction est sélectionnée, l'instructeur peut modifier les autorisations AirPlay et voir l'écran de l'appareil d'un étudiant, sans demander d'autorisation. Par défaut, cette restriction n'est pas sélectionnée. Pour les appareils iOS supervisés.
  - **Flux de photos :** autorise les utilisateurs à utiliser MyPhotoStream pour partager des photos avec leurs appareils iOS via iCloud.

- **Flux de photos partagés :** autorise les utilisateurs à utiliser le partage de photos iCloud pour partager des photos avec des collègues, amis et proches.
- **Composition vocale :** active la composition sur les appareils des utilisateurs.
- **Siri :** permet aux utilisateurs d'utiliser Siri.
  - **Autoriser lorsque l'appareil est verrouillé :** permet aux utilisateurs de se servir de Siri lorsque leur appareil est verrouillé.
  - **Filtre d'obscénité de Siri :** active le filtre d'obscénité de Siri. Par défaut, cette fonctionnalité est désactivée, ce qui signifie qu'aucun filtre d'obscénité n'est appliqué. Pour de plus amples informations sur Siri et la sécurité, consultez la section Stratégies de dictée et Siri.
- **Installation d'applications :** autorise les utilisateurs à installer des applications. Pour les appareils iOS supervisés.
- **Autoriser récupération en arrière-plan globale en cas d'itinérance :** autorise un appareil à synchroniser automatiquement les comptes de messagerie vers iCloud lorsqu'il est itinérant. Lorsque **Désactivé** est sélectionné, désactive l'activité de récupération en arrière-plan globale lors de l'itinérance d'un téléphone iOS. La valeur par défaut est **Activé**.

- **Autoriser les applications**
  - **iTunes Store :** autorise les utilisateurs à accéder à l'iTunes Store. Pour les appareils iOS supervisés.
  - **Achats dans les applications :** autorise les utilisateurs à effectuer des achats dans les applications.
    - **Exiger le mot de passe iTunes pour tous les achats :** exige un mot de passe pour les achats dans l'application. Par défaut, cette fonctionnalité est désactivée, ce qui signifie qu'aucun mot de passe n'est requis pour les achats intégrés dans l'application.
  - **Safari :** permet aux utilisateurs d'accéder à Safari. Pour les appareils iOS supervisés.
    - **Remplissage automatique :** autorise les utilisateurs à configurer le remplissage automatique pour les noms d'utilisateurs et mots de passe sur Safari.
    - **Forcer l'avertissement de fraude :** si ce paramètre est activé et qu'un utilisateur visite un site soupçonné d'hameçonnage, Safari alerte l'utilisateur. Par défaut, cette fonctionnalité est désactivée, ce qui signifie qu'aucun avertissement n'est émis.
    - **Activer JavaScript :** autorise JavaScript à s'exécuter sur Safari.
    - **Bloquer les fenêtres contextuelles :** bloque les fenêtres contextuelles lors de l'affichage de sites Web. Par défaut, cette fonctionnalité est désactivée, ce qui signifie que les fenêtres contextuelles ne sont pas bloquées.
  - **Accepter les cookies :** définit dans quelle mesure les cookies sont acceptés. Dans la liste, choisissez sur une option pour activer ou désactiver les cookies. L'option par défaut est **Toujours**, ce qui autorise tous les sites à enregistrer des cookies dans Safari. Les autres options sont **Site Web actuel uniquement**, **Jamais** et **Des sites visités uniquement**.

- **Réseau - Autoriser les actions iCloud**
  - **Documents et données iCloud :** autorise les utilisateurs à synchroniser les documents et les données avec iCloud. Pour les appareils iOS supervisés.
  - **Sauvegarde iCloud :** autorise les utilisateurs à sauvegarder leurs appareils sur iCloud.
  - **Trousseau iCloud :** autorise les utilisateurs à stocker les mots de passe, le réseau Wi-Fi, le numéro de carte de crédit et autres informations dans le trousseau iCloud.
  - **Photothèque iCloud :** autorise les utilisateurs à accéder à leur bibliothèque de photos iCloud.
- **Sécurité - Forcer**

  Par défaut, les fonctionnalités suivantes sont désactivées, ce qui signifie qu'aucune fonctionnalité de sécurité n'est activée.
  - **Copies de sauvegarde chiffrées :** impose le chiffrement des sauvegardes effectuées dans iCloud.
  - **Suivi limité des publicités :** bloque le suivi des publicités ciblées.
  - **Demander code secret lors du premier couplage AirPlay :** exige que les appareils compatibles avec AirPlay soient vérifiés à l'aide d'un code à usage unique s'affichant sur l'écran avant que les utilisateurs puissent utiliser AirPlay.
  - **Apple Watch jumelée pour utiliser la détection du poignet :** requiert une Apple Watch jumelée pour utiliser la **détection du poignet**.
  - **Partage des documents gérés avec AirDrop :** si vous définissez cette option sur **Activé**, AirDrop apparaît comme destination non gérée.
- **Sécurité - Autoriser**
  - **Accepter des certificats SSL non approuvés :** autorise les utilisateurs à accepter les certificats SSL non fiables de sites Web.
  - **Mise à jour automatique des paramètres d'approbation de certificat :** autorise la mise à jour automatique des certificats de confiance.
  - **Documents provenant d'applications gérées dans les applications non gérées :** autorise les utilisateurs à déplacer des données d'applications gérées (d'entreprise) vers des applications non gérées (personnelles).
  - **Documents provenant d'applications non gérées dans les applications gérées :** autorise les utilisateurs à déplacer des données d'applications non gérées (personnelles) vers des applications gérées (d'entreprise).
  - **Envoi d'informations de diagnostic à Apple :** autorise l'envoi à Apple de données de diagnostic anonymes relatives aux appareils des utilisateurs.
  - **Touch ID pour déverrouiller un appareil :** autorise les utilisateurs à utiliser leurs empreintes digitales pour déverrouiller leurs appareils.
  - **Notifications Passbook lorsque l'appareil est verrouillé :** autorise l'affichage de notifications Passbook sur l'écran de verrouillage.

- **Handoff :** autorise les utilisateurs à transférer des activités d'un appareil iOS vers un autre appareil iOS se trouvant à proximité.
- **Synchronisation iCloud pour applications gérées :** autorise les utilisateurs à synchroniser des applications gérées avec iCloud.
- **Sauvegarde de livres d'entreprise :** autorise la sauvegarde des livres d'entreprise dans iCloud.
- **Synchronisation des notes et des extraits pour les livres d'entreprise :** autorise la synchronisation avec iCloud des notes et extraits ajoutés aux livres d'entreprise par les utilisateurs.
- **Faire confiance aux applications d'entreprise :** permet de faire confiance aux applications d'entreprise. Les applications d'entreprise sont toutes les applications qui ont été personnalisées pour votre organisation. Elles peuvent être réalisées en interne ou elles peuvent être développées et achetées auprès d'un fournisseur externe. Pour plus d'informations, consultez Installer des applications d'entreprise personnalisées sur iOS.
- **Résultats Internet dans Spotlight :** autorise Spotlight à afficher les résultats de recherche sur Internet ainsi que sur l'appareil.
- **Les applications non gérées lisent des contacts gérés :** option facultative. Disponible uniquement si l'option **Documents provenant d'applications gérées dans les applications non gérées** est désactivée. Si cette stratégie est activée, des applications non gérées peuvent lire les données des contacts des comptes gérés. La valeur par défaut est **Désactivé**. Disponible à partir d'iOS 12.
- **Les applications gérées écrivent des contacts non gérés :** option facultative. Si cette option est activée, des applications gérées peuvent écrire des contacts dans les contacts des comptes non gérés. Si l'option **Documents provenant d'applications gérées dans les applications non gérées** est activée, cette restriction n'a aucun effet. La valeur par défaut est **Désactivé**. Disponible à partir d'iOS 12.

- **Paramètres supervisés uniquement - Autoriser**

  Ces paramètres s'appliquent uniquement aux appareils supervisés. Pour obtenir les instructions sur la définition d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

  - **Effacer tout le contenu et les paramètres :** autorise les utilisateurs à effacer tout le contenu et les paramètres à partir de leurs appareils.
  - **Configuration des restrictions :** autorise les utilisateurs à configurer le contrôle parental sur leurs appareils.
  - **Podcasts :** autorise les utilisateurs à télécharger et synchroniser des podcasts.
  - **Installation des profils de configuration :** autorise les utilisateurs à installer un autre profil de configuration que celui que vous avez déployé.

- **Modification de l'empreinte digitale :** autorise les utilisateurs à modifier ou supprimer leur empreinte digitale Touch ID.
- **Installation d'applications à partir de l'appareil :** autorise les utilisateurs à installer des applications. La désactivation de ce paramètre empêche les utilisateurs finaux d'installer de nouvelles applications. L'App Store est désactivé et son icône est supprimée de l'écran d'accueil.
- **Raccourcis clavier :** autorise les utilisateurs à créer des raccourcis clavier personnalisés pour les mots ou phrases qu'ils utilisent souvent.
- **Montre jumelée :** autorise les utilisateurs à jumeler une Apple Watch avec un appareil supervisé.
- **Modification du code secret :** autorise les utilisateurs à changer le code secret sur un appareil supervisé.
- **Modification du nom de l'appareil :** autorise les utilisateurs à changer le nom de leur appareil.
- **Modification du fond d'écran :** autorise les utilisateurs à changer le fond d'écran sur leurs appareils.
- **Téléchargement automatique des applications :** autorise le téléchargement des applications.
- **AirDrop :** autorise les utilisateurs à partager des photos, des vidéos, des sites Web, des emplacements et autres avec des appareils iOS se trouvant à proximité.
- **iMessage :** autorise les utilisateurs à envoyer un SMS par Wi-Fi avec iMessage.
- **Contenu généré par l'utilisateur dans Siri :** autorise Siri à interroger le contenu généré par l'utilisateur à partir du Web. Des consommateurs, plutôt que des journalistes ; contenu généré par l'utilisateur. Par exemple, les contenus disponibles sur Twitter ou Facebook sont générés par l'utilisateur.
- **iBooks :** autorise les utilisateurs à utiliser l'application iBooks.
- **Suppression d'applications :** autorise les utilisateurs à supprimer des applications à partir de leurs appareils.
- **Game Center :** autorise les utilisateurs à jouer à des jeux en ligne proposés par Game Center sur leurs appareils.
  - **Ajouter des amis :** autorise les utilisateurs à envoyer une notification à un ami pour l'inviter à rejoindre une partie.
  - **Jeux multijoueurs :** autorise les utilisateurs à lancer un jeu multijoueurs sur leur appareil.

- **Modification des paramètres de compte :** autorise les utilisateurs à modifier les paramètres du compte de leur appareil.
- **Modification des paramètres des données cellulaires d'application :** autorise les utilisateurs à modifier la façon dont les applications utilisent les données cellulaires.
- **Modification des paramètres Localiser mes amis :** autorise les utilisateurs à modifier leurs paramètres Localiser mes amis.
- **Couplage avec des hôtes non Configurator :** autorise l'administrateur à contrôler les appareils avec lesquels l'appareil d'un utilisateur peut être couplé. La désactivation de ce paramètre empêche le couplage sauf avec l'hôte superviseur exécutant Apple Configurator. Si aucun certificat d'hôte superviseur n'est configuré, tous les couplages sont désactivés.
- **Claviers intuitifs :** autorise les appareils des utilisateurs à utiliser le clavier intuitif pour leur suggérer des mots lors de la saisie. Désactivez cette option dans certaines situations spécifiques, par exemple lors de tests standardisés pendant lesquels vous ne voulez pas que les utilisateurs aient accès à des mots suggérés.
- **Clavier avec correction automatique :** autorise les appareils des utilisateurs à utiliser le clavier avec correction automatique. Désactivez cette option dans certaines situations spécifiques, par exemple lors de tests standardisés pendant lesquels vous ne voulez pas que les utilisateurs aient accès à la correction automatique.
- **Clavier avec correction d'orthographe :** autorise les appareils des utilisateurs à utiliser le correcteur orthographique lors de la saisie. Désactivez cette option dans certaines situations spécifiques, par exemple lors de tests standardisés pendant lesquels vous ne voulez pas que les utilisateurs aient accès au correcteur orthographique.
- **Recherche des définitions :** autorise les appareils des utilisateurs à utiliser la recherche de définition lors de la saisie. Désactivez cette option dans certaines situations spécifiques, par exemple lors de tests standardisés pendant lesquels vous ne voulez pas que les utilisateurs puissent rechercher des définitions pendant la saisie.
- **Bundle ID d'application unique :** crée une liste d'applications autorisées à conserver le contrôle de l'appareil et à empêcher les interactions avec d'autres applications ou fonctions.

  Pour ajouter une application, cliquez sur **Ajouter**, tapez un **nom d'application**, puis cliquez sur **Enregistrer**. Répétez cette procédure pour chaque application à ajouter.
- **News :** autorise les utilisateurs à utiliser l'application News.
- **Service Apple Music :** permet aux utilisateurs d'utiliser le service Apple Music. Si vous n'autorisez pas le service Apple Music, l'application Music s'exécute en mode classique.
- **iTunes Radio :** permet aux utilisateurs d'utiliser iTunes Radio.

- **Modification des notifications :** permet aux utilisateurs de modifier les paramètres de notification.
- **Utilisation restreinte des apps :** autorise les utilisateurs à utiliser toutes les applications ou à utiliser ou non certaines applications en fonction des Bundle ID que vous fournissez. S'applique uniquement aux appareils supervisés. Si vous sélectionnez **Autoriser uniquement certaines applications**, ajoutez une application avec le bundle ID `com.apple.webapp` pour autoriser les clips Web.

  > **Remarque :**
  >
  > À partir de iOS 11, Apple a introduit des modifications dans les stratégies disponibles pour les restrictions d'applications. Apple ne vous permet plus de supprimer l'accès à l'application Paramètres et à l'application Téléphone en limitant l'offre d'applications iOS appropriée.

  Après avoir configuré la stratégie Restrictions pour bloquer certaines applications et déployé la stratégie : si vous souhaitez autoriser tout ou partie de ces applications ultérieurement, la modification et le déploiement de la stratégie Restrictions ne modifient pas les restrictions. Dans ce cas, iOS n'applique pas les modifications apportées au profil iOS. Utilisez la stratégie Suppression de profil pour supprimer le profil iOS et déployez la stratégie Restrictions mise à jour.

  Si vous réglez ce paramètre sur **Autoriser uniquement certaines applications** : avant de déployer cette stratégie, demandez aux utilisateurs des appareils inscrits à l'aide du programme de déploiement d'Apple de se connecter à leurs comptes Apple à partir de l'Assistant d'installation. Dans le cas contraire, les utilisateurs devront peut-être désactiver l'authentification à deux facteurs sur leurs appareils pour se connecter à leurs comptes Apple et accéder aux applications autorisées.
- **Modification de l'envoi de diagnostics :** permet aux utilisateurs de modifier les paramètres d'envoi d'informations de diagnostic ainsi que les paramètres d'analyse de l'application dans le panneau **Réglages > Diagnostics et utilisation**.
- **Modification Bluetooth :** permet aux utilisateurs de modifier les paramètres Bluetooth.
- **Autoriser la dictée :** sur appareils supervisés uniquement. Si cette restriction est définie sur **Désactivé**, la dictée n'est pas autorisée, y compris la reconnaissance vocale. Le paramètre par défaut est **Activé**.
- **Rejoindre uniquement les réseaux Wi-Fi installés par une stratégie Wi-Fi :** paramètre facultatif. Supervisé uniquement Si cette restriction est définie sur **Activé**, l'appareil peut rejoindre des réseaux Wi-Fi uniquement lorsqu'ils ont été configurés par le biais d'un profil de configuration. Le paramètre par défaut est **Désactivé**.
- **Autoriser l'application En classe à modifier les autorisations AirPlay et Voir l'écran**

sans invite : si cette restriction est sélectionnée, l'instructeur peut modifier les autorisations AirPlay et voir l'écran de l'appareil d'un étudiant, sans demander d'autorisation. Par défaut, cette restriction n'est pas sélectionnée. Pour les appareils iOS supervisés.

- **Autoriser l'application En classe à verrouiller une application et l'appareil sans invite :** si cette restriction est définie sur **Activé**, l'application En classe verrouille automatiquement les appareils utilisateur sur une application et verrouille l'appareil, sans inviter les utilisateurs. Le paramètre par défaut est **Désactivé**. Pour les appareils supervisés exécutant iOS 11 (version minimale).
- **Rejoindre automatiquement les cours de l'application En classe sans invite :** si cette restriction est définie sur **Activé**, l'application En classe ajoute automatiquement les utilisateurs aux classes, sans inviter les utilisateurs. Le paramètre par défaut est **Désactivé**. Pour les appareils supervisés exécutant iOS 11 (version minimale).
- **Autoriser AirPrint :** si cette restriction est définie sur **Désactivé**, les utilisateurs ne peuvent pas imprimer avec AirPrint. Le paramètre par défaut est **Activé**. Lorsque cette restriction est définie sur **Activé**, les restrictions supplémentaires suivantes s'affichent. Pour les appareils supervisés exécutant iOS 11 (version minimale).
  - **Autoriser le stockage des identifiants AirPrint dans le trousseau :** si cette restriction n'est pas sélectionnée, le nom d'utilisateur et le mot de passe AirPrint ne sont pas stockés dans le trousseau. Par défaut, ce paramètre est sélectionné. Pour les appareils supervisés exécutant iOS 11 (version minimale).
  - **Autoriser la détection des imprimantes AirPrint à l'aide d'iBeacons :** si cette restriction est désactivée, la détection iBeacon des imprimantes AirPrint est désactivée. Cela empêche les balises Bluetooth AirPrint parasites de perpétrer des attaques de phishing sur le trafic réseau. Par défaut, ce paramètre est sélectionné. Pour les appareils supervisés exécutant iOS 11 (version minimale).
  - **Autoriser AirPrint uniquement aux destinations avec des certificats de confiance :** si cette restriction est sélectionnée, les utilisateurs peuvent utiliser AirPrint pour imprimer uniquement vers des destinations avec des certificats de confiance. Par défaut, cette restriction n'est pas sélectionnée. Pour les appareils supervisés exécutant iOS 11 (version minimale).
- **Ajout de configurations VPN :** si cette restriction est définie sur **Désactivé**, les utilisateurs ne peuvent pas créer de configurations VPN. Le paramètre par défaut est **Activé**. Pour les appareils supervisés exécutant iOS 11 (version minimale).
- **Modification des paramètres du forfait de données :** si cette restriction est définie sur **Désactivé**, les utilisateurs ne peuvent pas modifier les paramètres du forfait de données. Le paramètre par défaut est **Activé**. Pour les appareils supervisés exécutant iOS 11 (version minimale).

- **Suppression des applications système :** si cette restriction est définie sur **Désactivé**, les utilisateurs ne peuvent pas supprimer les applications système de leur appareil. Le paramètre par défaut est **Activé**. Pour les appareils supervisés exécutant iOS 11 (version minimale).
- **Configuration des nouveaux appareils à proximité :** si cette restriction est définie sur Désactivé, les utilisateurs ne peuvent pas configurer de nouveaux appareils à proximité. Le paramètre par défaut est Activé. Pour les appareils supervisés exécutant iOS 11 (version minimale).
- **Autoriser le mode restreint USB :** si cette option est **désactivée**, l'appareil peut toujours se connecter aux accessoires USB lorsqu'il est verrouillé. La valeur par défaut est **Activé**. Disponible uniquement sur iOS 11.3 et versions ultérieures sur les appareils supervisés.
- **Retarder les mises à jour logicielles :** si cette option est **activée**, retarde la visibilité des mises à jour logicielles pour l'utilisateur. Avec cette restriction en place, l'utilisateur ne voit pas de mise à jour logicielle avant le nombre de jours spécifié après la date de publication de la mise à jour logicielle. La valeur par défaut est **Désactivé**. Disponible uniquement sur iOS 11.3 et versions ultérieures sur les appareils supervisés.
- **Délai imposé pour les mises à jour logicielles (jours) :** vous permet de spécifier le nombre de jours pendant lequel retarder une mise à jour logicielle sur l'appareil. Le délai maximum est de **90** jours. La valeur par défaut est **30** jours. Disponible uniquement sur iOS 11.3 et versions ultérieures sur les appareils supervisés.
- **Exiger la permission de En classe pour quitter les classes :** si cette option est **activée**, un élève inscrit à un cours non géré avec En classe doit demander la permission à l'enseignant pour quitter le cours. La valeur par défaut est **Désactivé**. Disponible uniquement sur iOS 11.3 et versions ultérieures sur les appareils supervisés.
- **Forcer réglage automatique de la date et de l'heure :** cette option vous permet de définir automatiquement la date et l'heure sur les appareils supervisés. Lorsque ce paramètre est défini sur **Activé**, les utilisateurs de l'appareil ne peuvent pas désactiver l'option **Définir automatiquement** sous **Général > Date et heure**. Le fuseau horaire sur l'appareil est mis à jour uniquement lorsque l'appareil peut déterminer son emplacement, c'est-à-dire lorsqu'un appareil dispose d'une connexion cellulaire ou d'une connexion Wi-Fi avec les services de localisation activés. La valeur par défaut est **Désactivé**. Disponible uniquement sur iOS 12 et versions ultérieures sur les appareils supervisés.
- **Remplissage automatique du mot de passe :** option facultative. Si cette option est désactivée, les utilisateurs ne peuvent pas utiliser les fonctionnalités de remplissage automatique de mot de passe ou de mot de passe fort automatique. La valeur par défaut est **Activé**. Disponible à partir d'iOS 12.
- **Requêtes de proximité de mot de passe :** option facultative. Si cette option est désac-

tivée, les appareils des utilisateurs ne demandent pas de mots de passe aux appareils à proximité. La valeur par défaut est **Activé**. Disponible à partir d'iOS 12.

- **Partage de mot de passe :** option facultative. Si cette option est désactivée, les utilisateurs ne peuvent pas partager leurs mots de passe à l'aide de la fonctionnalité Mots de passe AirDrop. La valeur par défaut est **Activé**. Disponible à partir d'iOS 12.

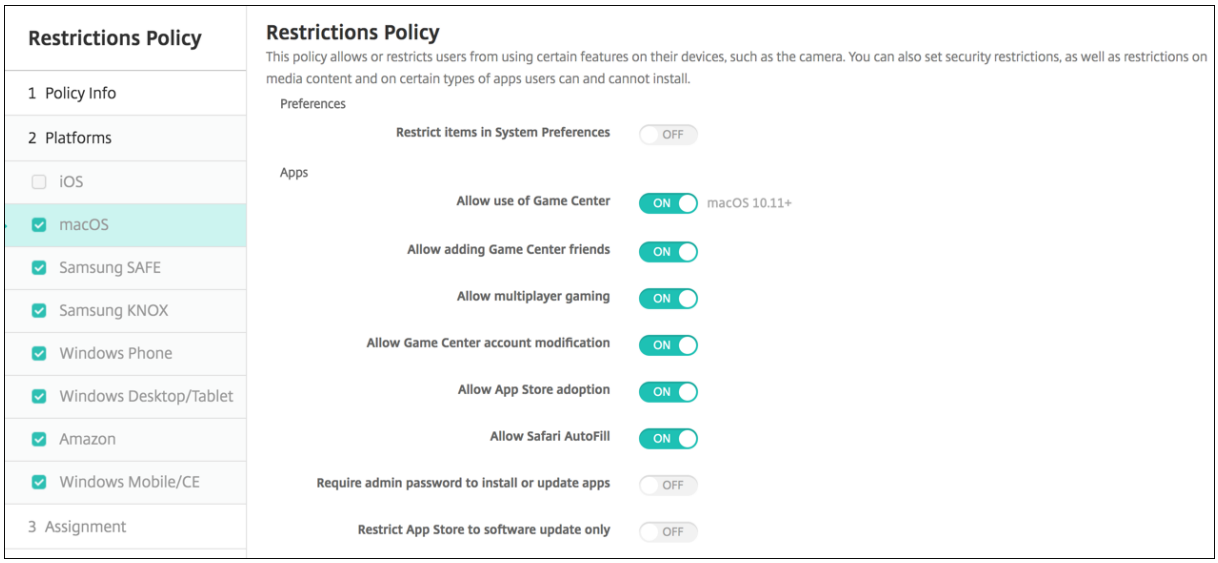
- **Sécurité - Afficher dans l'écran de verrouillage**
  - **Centre de contrôle :** cette option autorise l'accès au centre de contrôle sur l'écran de verrouillage. L'option Centre de contrôle permet aux utilisateurs de modifier facilement les modes Avion, Wi-Fi, Bluetooth, Ne pas déranger et les paramètres Lock Rotation.
  - **Notification :** autorise les notifications sur l'écran de verrouillage.
  - **Vue Aujourd'hui :** autorise l'affichage de la Vue Aujourd'hui, qui effectue l'agrégation d'informations telles que la météo et les éléments du calendrier du jour actuel, sur l'écran de verrouillage.

- **Contenu multimédia - Autoriser**
  - **Musique, podcasts et cours iTunes U explicites :** autorise l'affichage de contenus explicites sur les appareils des utilisateurs.
  - **Contenu sexuel explicite dans iBooks :** autorise le téléchargement de contenus explicites depuis iBooks.
  - **Classements par région :** définit la région à partir de laquelle les classements du contrôle parental sont obtenus. Dans la liste, cliquez sur un pays pour définir la région des classements. La valeur par défaut est **États-Unis**.
  - **Films :** détermine si les films sont autorisés sur les appareils des utilisateurs. Si les films sont autorisés, vous pouvez définir le niveau de contrôle d'accès pour les films. Dans la liste, cliquez sur une option pour autoriser ou interdire les films sur l'appareil. La valeur par défaut est Autoriser tous les films.
  - **Séries TV :** détermine si les séries télévisées sont autorisées sur les appareils des utilisateurs. Si les séries TV sont autorisées, vous pouvez définir leur niveau de contrôle d'accès. Dans la liste, cliquez sur une option pour autoriser ou interdire les séries TV sur l'appareil. La valeur par défaut est Autoriser toutes les séries TV.
  - **Applications :** détermine si les applications sont autorisées sur les appareils des utilisateurs. Si les applications sont autorisées, vous pouvez définir leur niveau de contrôle d'accès. Dans la liste, cliquez sur une option pour autoriser ou interdire les applications sur l'appareil. La valeur par défaut est Autoriser toutes les apps.

- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.

    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur iOS 9.3 et versions ultérieures.

Paramètres macOS



- **Préférences**
  - **Limiter les éléments dans les Préférences système :** autorise ou restreint l'accès des utilisateurs aux Préférences système. La valeur par défaut est **Désactivé**, ce qui donne aux utilisateurs un accès total aux Préférences système. Si cette option est activée, vous pouvez configurer les paramètres suivants :
    * **Volets des préférences système :** indiquez si vous souhaitez que les paramètres que vous sélectionnez soient activés ou désactivés. La valeur par défaut est d'activer tous les paramètres, qui sont définis sur **Activé** par défaut.
      - Utilisateurs ou groupes
      - Général
      - Accessibilité
      - Magasin d'applications
      - Mise à jour de logiciels
      - Bluetooth
      - CD et DVD

- Date/Heure
- Bureau et éco. d'écran
- Moniteurs
- Dock
- Économiseur d'énergie
- Extensions
- Fibre Channel
- iCloud
- Encre
- Comptes Internet
- Clavier
- Langue et texte
- Mission Control
- Souris
- Réseau
- Notifications
- Contrôle parental
- Imprimantes et scanners
- Profils
- Sécurité et confidentialité
- Partage
- Son
- Dictée et parole
- Spotlight
- Disque de démarrage
- Time Machine
- Trackpad
- Xsan

- **Applications**
  - **Autoriser l'utilisation de Game Center :** autorise les utilisateurs à jouer à des jeux en ligne via Game Center. La valeur par défaut est **Activé**.
  - **Autoriser l'ajout d'amis du Game Center :** autorise les utilisateurs à envoyer une notification à un ami pour l'inviter à rejoindre une partie. La valeur par défaut est **Activé**.
  - **Autoriser les jeux multijoueurs :** autorise les utilisateurs à lancer un jeu multijoueurs. La valeur par défaut est **Activé**.
  - **Autoriser la modification du compte Game Center :** autorise les utilisateurs à modifier leurs paramètres de compte Game Center. La valeur par défaut est **Activé**.
  - **Autoriser l'adoption par l'App Store :** autorise ou restreint l'adoption des applications qui préexistent dans OS X par l'App Store. La valeur par défaut est **Activé**.

  - **Autoriser le remplissage automatique Safari :** autorise Safari à remplir automatiquement les champs des sites Web avec les mots de passe, les adresses et autres informations de base que le navigateur a stockés. La valeur par défaut est **Activé**.
  - **Demander un mot de passe administrateur pour installer ou mettre à jour des applications :** exige un mot de passe administrateur pour installer ou mettre à jour des applications. La valeur par défaut est **Désactivé**, ce qui signifie qu'aucun mot de passe administrateur n'est requis.
  - **Autoriser uniquement l'App Store à mettre à jour les logiciels :** restreint l'App Store aux mises à jour, ce qui désactive tous les onglets de l'App Store, à l'exception de Mises à jour. La valeur par défaut est **Désactivé**, ce qui permet un accès complet à l'App Store.
  - **Limiter les applications autorisées :** restreint ou autorise les applications que les utilisateurs peuvent utiliser. La valeur par défaut est Désactivé, ce qui permet à toutes les applications d'être utilisées. Si cette option est activée, vous pouvez configurer les paramètres suivants :
    * **Applications autorisées :** cliquez sur **Ajouter**, entrez le nom et le Bundle ID d'une application autorisée à démarrer, puis cliquez sur **Enregistrer**. Répétez cette étape pour chaque application autorisée à démarrer.
    * **Dossiers interdits :** cliquez sur **Ajouter**, entrez le chemin d'accès d'un dossier pour lequel vous souhaitez restreindre l'accès des utilisateurs (par exemple, /Applications/Utilities), puis cliquez sur **Enregistrer**. Répétez cette étape pour tous les dossiers auxquels vous ne souhaitez pas que les utilisateurs puissent accéder.
    * **Dossiers autorisés :** cliquez sur **Ajouter**, entrez le chemin d'accès d'un dossier pour lequel vous souhaitez accorder l'accès des utilisateurs, puis cliquez sur **Enregistrer**. Répétez cette étape pour tous les dossiers auxquels vous souhaitez que les utilisateurs puissent accéder.

- **Widgets**
  - **Autoriser uniquement l'exécution des widgets du tableau de bord suivants :** autorise ou restreint les widgets du tableau de bord, tels que l'horloge mondiale ou la calculatrice, que les utilisateurs sont autorisés à exécuter. La valeur par défaut est **Désactivé**, ce qui permet aux utilisateurs d'exécuter tous les widgets. Si cette option est activée, vous pouvez configurer le paramètre suivant :
    * **Widgets autorisés :** cliquez sur **Ajouter**, entrez le nom et l'ID d'un widget qui est autorisé à être exécuté, puis cliquez sur **Enregistrer**. Répétez cette étape pour chaque widget que vous souhaitez exécuter sur le tableau de bord.
- **Média**
  - **Autoriser AirDrop :** autorise les utilisateurs à partager des photos, des vidéos, des sites Web, des emplacements et autres avec des appareils iOS se trouvant à proximité.
- **Partage**
  - **Activer automatiquement les nouveaux services de partage :** sélectionnez cette option

pour activer les services de partage.
  - **Messagerie :** sélectionnez cette option pour autoriser une boîte aux lettres partagée.
  - **Facebook :** sélectionnez cette option pour autoriser un compte Facebook partagé.
  - **Services vidéo - Flickr, Vimeo, Tudou et Youku :** sélectionnez cette option pour autoriser les services vidéo partagés.
  - **Ajouter à Aperture :** sélectionnez cette option pour autoriser la capacité partagée d'ajouter à Aperture.
  - **Sina Weibo :** sélectionnez cette option pour autoriser un compte de microblogage Sina Weibo partagé.
  - **Twitter :** sélectionnez cette option pour autoriser un compte Twitter partagé.
  - **Messages :** sélectionnez cette option pour autoriser un accès partagé aux messages.
  - **Ajouter à iPhoto :** sélectionnez cette option pour autoriser la capacité partagée d'ajouter à iPhoto.
  - **Ajouter à la liste de lecture :** sélectionnez cette option pour autoriser la capacité partagée d'ajouter à la liste de lecture.
  - **AirDrop :** sélectionnez cette option pour autoriser un compte AirDrop partagé.
- **Fonctionnalité**
  - **Verrouiller l'image de bureau :** indiquez si les utilisateurs peuvent modifier l'image de bureau. La valeur par défaut est **Désactivé**, ce qui signifie que les utilisateurs peuvent modifier l'image de bureau.
  - **Autoriser l'utilisation de l'appareil photo :** indiquez si les utilisateurs peuvent utiliser l'appareil photo sur leurs appareils Mac. La valeur par défaut est **Désactivé**, ce qui signifie que les utilisateurs ne peuvent pas utiliser l'appareil-photo.
  - **Autoriser Apple Music :** permet aux utilisateurs d'utiliser le service Apple Music (macOS 10.12 et versions ultérieures). Si vous n'autorisez pas le service Apple Music, l'application Music s'exécute en mode classique. S'applique uniquement aux appareils supervisés. La valeur par défaut est **Activé**.
  - **Autoriser les suggestions de Spotlight :** indiquez si les utilisateurs peuvent utiliser les suggestions de Spotlight pour effectuer des recherches sur leur Mac et fournir des suggestions Spotlight à partir d'Internet, iTunes et App Store. La valeur par défaut est **Désactivé**, ce qui empêche les utilisateurs d'utiliser les suggestions de Spotlight.
  - **Autoriser Look Up :** indiquez si les utilisateurs peuvent rechercher les définitions de termes avec le menu contextuel ou le menu de recherche Spotlight. La valeur par défaut est Désactivé, ce qui empêche les utilisateurs d'utiliser Look Up sur leurs appareils Mac.
  - **Autoriser l'utilisation du mot de passe iCloud pour les comptes locaux :** indiquez si les utilisateurs peuvent utiliser leur mot de passe Apple ID et iCloud pour se connecter à leurs appareils Mac. L'activation de cette option signifie que l'utilisateur utilise un seul identifiant et mot de passe pour *tous* les écrans d'ouverture de session sur leurs appareils Mac. La valeur par défaut est **Activé**, ce qui permet aux utilisateurs d'utiliser leur mot de

passe Apple ID et iCloud pour accéder à leurs appareils Mac.

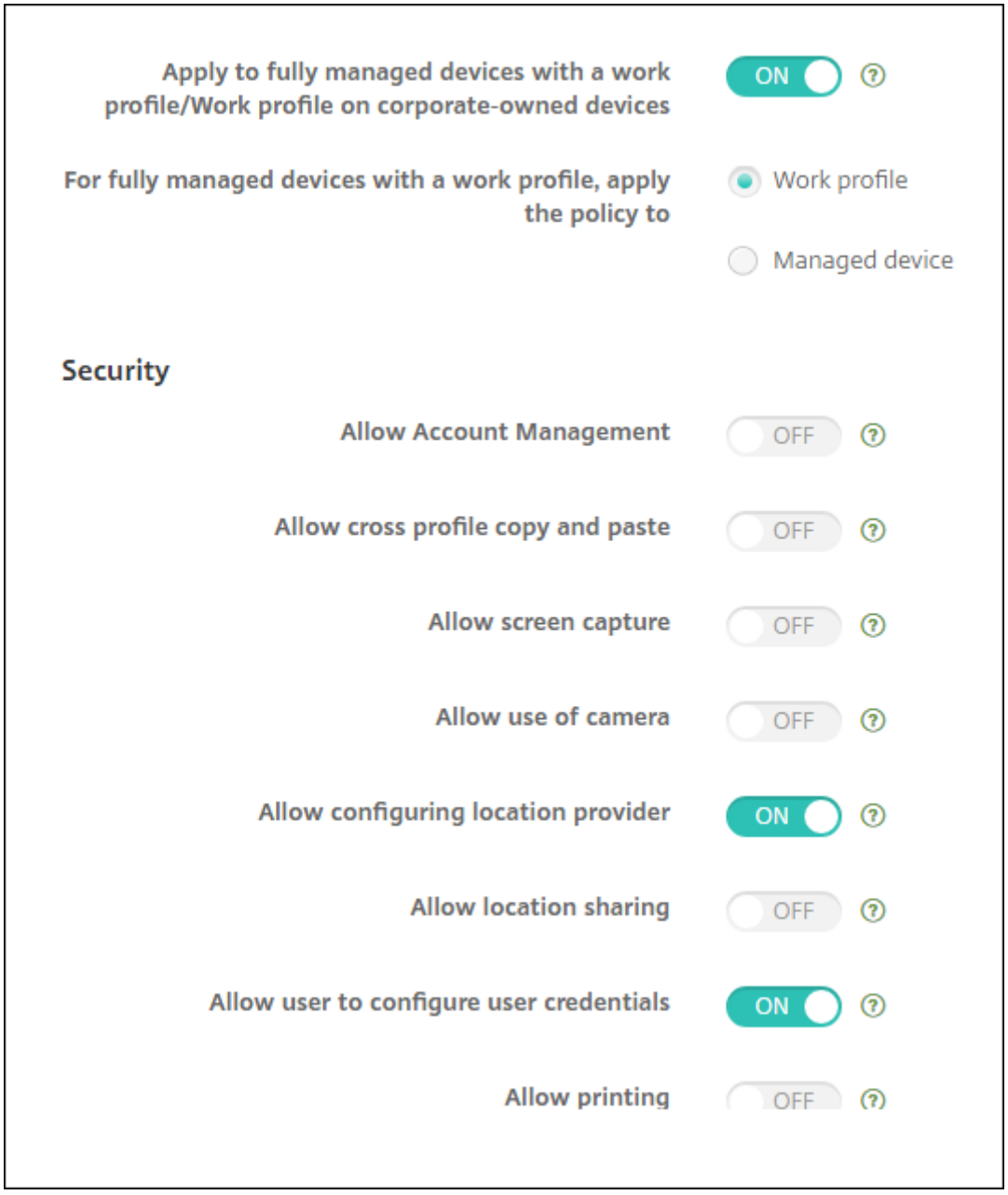
- **Autoriser les documents et données iCloud :** indiquez si les utilisateurs peuvent accéder aux documents et aux données stockés sur iCloud sur des appareils Mac. La valeur par défaut est **Désactivé**, ce qui empêche les utilisateurs d'utiliser les documents et données iCloud sur des appareils Mac.
  - **Autoriser bureau et documents iCloud :** (macOS 10.12.4 et versions ultérieures) sélectionné par défaut.
- **Autoriser la synchronisation du trousseau iCloud** : autorise la synchronisation du trousseau iCloud (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser iCloud Mail :** permet aux utilisateurs d'utiliser iCloud Mail (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser contacts iCloud :** permet aux utilisateurs d'utiliser les contacts iCloud (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser calendriers iCloud :** permet aux utilisateurs d'utiliser les calendriers iCloud (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser rappels iCloud :** permet aux utilisateurs d'utiliser les rappels iCloud (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser signets iCloud :** permet aux utilisateurs de se synchroniser avec les signets iCloud (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser notes iCloud :** permet aux utilisateurs d'utiliser les notes iCloud (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser photos iCloud :** si vous réglez ce paramètre sur **Désactivé**, les photos qui ne sont pas entièrement téléchargées à partir de la bibliothèque de photos iCloud sont supprimées du stockage local de l'appareil (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser déverrouillage automatique :** pour plus d'informations sur cette option et Apple Watch, voir https://www.imore.com/auto-unlock (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser Touch ID pour déverrouiller votre Mac :** (macOS 10.12.4 et versions ultérieures). La valeur par défaut est **Activé**.
- **Retarder les mises à jour logicielles :** s'il est **activé**, ce paramètre retarde la visibilité des mises à jour logicielles pour l'utilisateur. Les utilisateurs ne voient pas de mise à jour logicielle avant le nombre de jours spécifié après la date de publication de la mise à jour logicielle. La valeur par défaut est **Désactivé**. Disponible uniquement pour les appareils supervisés exécutant macOS 10.13.4 et versions ultérieures.
- **Délai imposé pour les mises à jour logicielles (jours) :** spécifie le nombre de jours pendant lequel retarder une mise à jour logicielle sur l'appareil. Le délai maximum est de 90 jours. La valeur par défaut est **30**. Disponible uniquement pour les appareils supervisés exécutant macOS 10.13.4 et versions ultérieures.

- **Remplissage automatique du mot de passe :** option facultative. Si cette option est désactivée, les utilisateurs ne peuvent pas utiliser les fonctionnalités de remplissage automatique de mot de passe ou de mot de passe fort automatique. La valeur par défaut est **Activé**. Disponible à partir de macOS 10.14.
- **Requêtes de proximité de mot de passe :** option facultative. Si cette option est désactivée, les appareils des utilisateurs ne demandent pas de mots de passe aux appareils à proximité. La valeur par défaut est **Activé**. Disponible à partir de macOS 10.14.
- **Partage de mot de passe :** option facultative. Si cette option est désactivée, les utilisateurs ne peuvent pas partager leurs mots de passe à l'aide de la fonctionnalité Mots de passe Airdrop. La valeur par défaut est **Activé**. Disponible à partir de macOS 10.14.

Paramètres Android

- **Appareil photo :** autorise les utilisateurs à utiliser l'appareil photo sur leurs appareils. Si la valeur est définie sur **Désactivé**, l'appareil photo est désactivé. La valeur par défaut est **Activé**.

Paramètres Android Enterprise



Lorsqu'un nouvel appareil Android ou un appareil Android réinitialisé aux paramètres d'usine est inscrit en mode Profil de travail, les appareils exécutant Android 8.0-10.x sont inscrits en tant qu'appareils entièrement gérés avec profil de travail. Les appareils exécutant Android 11+ sont inscrits en mode Profil de travail sur appareils appartenant à l'entreprise. La stratégie de restriction peut s'appliquer au profil de travail sur l'appareil ou à l'appareil géré.

Sur les appareils inscrits en mode profil de travail sur appareils appartenant à l'entreprise, les restrictions suivantes sont uniquement disponibles pour le profil de travail :

- Autoriser service de sauvegarde
- Activer les applications système
- Empêcher Keyguard de verrouiller l'appareil
- Autoriser utilisation de la barre d'état
- Laisser l'écran allumé
- Autoriser l'utilisateur à contrôler les paramètres applicatifs
- Autoriser l'utilisateur à configurer les informations d'identification
- Autoriser configuration du VPN
- Autoriser le stockage de masse USB
- Autoriser réinitialisation des paramètres d'usine
- Autoriser désinstallation d'applications
- Autoriser les applications non Google Play
- Autoriser le copier/coller entre les profils
- Activer vérification de l'application
- Autoriser la gestion des comptes
- Autoriser l'impression
- Autoriser NFC
- Autoriser l'ajout d'utilisateurs

Par défaut, les paramètres **Débogage USB et Sources inconnues** sont désactivés sur un appareil lorsqu'il est inscrit en mode Profil de travail dans Android Entreprise.

Pour les appareils fonctionnant sous Android 8.0-10.x et Samsung Knox 3.0 et versions ultérieures, configurez les paramètres de Samsung Knox et Samsung SAFE sur la page **Android Enterprise**. Pour les appareils exécutant des versions antérieures d'Android ou de Samsung Knox, utilisez les pages **Samsung Knox** et **Samsung SAFE**.

Les restrictions Samsung ne s'appliquent pas aux appareils inscrits en mode profil de travail sur appareils appartenant à l'entreprise. Utilisez Knox Service Plugin (KSP) pour appliquer des restrictions Samsung à ces appareils. Pour plus d'informations, consultez la documentation Samsung.

Nous vous recommandons d'utiliser Samsung Knox 3.4 ou version ultérieure pour les dernières fonctionnalités de gestion Samsung Knox.

- **Appliquer aux appareils entièrement gérés avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise :** permet de configurer les paramètres de stratégie de restrictions pour les appareils entièrement gérés avec profil de travail. Lorsque ce paramètre est **activé**, sélectionnez l'un des paramètres suivants :
  - **Profil de travail :** les paramètres de restrictions que vous configurez s'appliquent uniquement au profil de travail sur l'appareil.
  - **Gérer l'appareil :** les paramètres de restrictions que vous configurez s'appliquent uniquement à l'appareil.

Lorsque ce paramètre est **Désactivé**, les paramètres d'informations d'identification que vous configurez s'appliquent à l'appareil, à l'exception des paramètres qui s'appliquent explicitement au profil de travail. La valeur par défaut est **Désactivé**.

Lorsque l'option **Appliquer aux appareils entièrement gérés avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise** est désactivée, configurez les paramètres suivants :

- **Sécurité**
  - **Autoriser la gestion des comptes :** permet au compte d'être ajouté aux appareils se trouvant dans le profil de travail et aux appareils gérés. La valeur par défaut est **Désactivé**.
  - **Autoriser le copier/coller entre les profils :** si cette option est définie sur **Activé**, les utilisateurs sont autorisés à copier et coller entre les applications du profil Android Enterprise et les applications dans la zone personnelle. La valeur par défaut est **Désactivé**.
  - **Autoriser la capture d'écran :** permet aux utilisateurs d'enregistrer ou de prendre une capture d'écran de l'écran de l'appareil. La valeur par défaut est **Désactivé**.
  - **Autoriser l'utilisation de l'appareil photo :** permet aux utilisateurs de prendre des photos et de créer des vidéos avec l'appareil photo de leurs appareils. La valeur par défaut est **Désactivé**.
  - **Autoriser configuration du VPN :** autorise les utilisateurs à créer des configurations VPN. Pour les appareils en mode Profil de travail fonctionnant sous Android 6 et versions ultérieures et pour les appareils entièrement gérés. La valeur par défaut est **Activé**.
  - **Autoriser service de sauvegarde :** autorise les utilisateurs à sauvegarder leurs données d'application et système sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser NFC :** autorise les utilisateurs à envoyer des pages Web, des photos, des vidéos ou tout autre contenu de leurs appareils à un autre appareil via la communication en champ proche (NFC). Pour MDM 4.0 et versions ultérieures. La valeur par défaut est **Activé**.
  - **Autoriser configuration du fournisseur de localisation :** autorise les utilisateurs à activer le GPS sur leurs appareils. Pour Android API 28 et versions ultérieures. La valeur par défaut est **Activé**.
  - **Autoriser partage de position :** pour les profils gérés, le propriétaire de l'appareil peut modifier ce paramètre. La valeur par défaut est **Désactivé**.

    > **Conseil :**
    >
    > Vous pouvez créer des stratégies d'emplacement dans XenMobile pour imposer des limites géographiques. Voir Stratégie d'emplacement.

- **Autoriser l'utilisateur à configurer les informations d'identification :** indiquez si les utilisateurs peuvent configurer les informations d'identification dans le keystore géré. La valeur par défaut est **Activé**.
- **Autoriser l'impression :** si ce paramètre est défini sur **Activé**, les utilisateurs peuvent imprimer sur une imprimante accessible à partir de la machine utilisateur. La valeur par défaut est **Désactivé**. Disponible pour : Android 9 et versions ultérieures.
- **Autoriser le débogage USB : Désactivé** par défaut.

- **Applications**
  - **Activer les applications système :** permet aux utilisateurs d'exécuter des applications d'appareil préinstallées. La valeur par défaut est **Désactivé**. Pour activer des applications spécifiques, cliquez sur **Ajouter** dans le tableau **Liste des applications système**.
    - **Liste des applications système :** liste des applications système que vous souhaitez activer sur l'appareil. Définissez **Activer les applications système** sur **Activé** et ajoutez le nom du package d'application. Pour rechercher le nom du package d'une application système, vous pouvez utiliser Android Debug Bridge (`adb`) pour appeler la commande de gestionnaire de packages Android (`pm`). Par exemple, `adb shell "pm list packages -f name"`, où « name » fait partie du nom du package. Pour plus d'informations, consultez https://developer.android.com/studio/command-line/adb. Pour les appareils Android Enterprise, vous pouvez restreindre les autorisations des applications à l'aide de la stratégie Autorisations applicatives Android Entreprise.
  - **Désactiver les applications :** bloque l'exécution d'une liste spécifique d'applications sur des appareils. La valeur par défaut est **Désactivé**. Pour désactiver une application installée, définissez le paramètre sur **Activé**, cliquez sur **Ajouter** dans le tableau **Liste d'applications**.
    - **Liste des applications :** liste des applications que vous souhaitez bloquer. Définissez **Désactiver les applications** sur **Activé** et ajoutez l'application. Tapez le nom du package de l'application. La modification et le déploiement d'une liste d'applications écrasent la liste d'applications précédente. Par exemple : si vous désactivez com.example1 et com.example2 et modifiez ensuite la liste vers com.example1 et com.example3, XenMobile active com.example.2.
  - **Activer vérification de l'application :** permet au système d'exploitation d'analyser les applications pour détecter un comportement malveillant. La valeur par défaut est **Activé**.
  - **Activer Google Apps :** permet aux utilisateurs de télécharger des applications à partir de Google Mobile Services sur l'appareil. La valeur par défaut est **Activé**.
  - **Autoriser les applications non Google Play :** permet l'installation d'applications provenant de magasins autres que Google Play. La valeur par défaut est **Désactivé**.
  - **Autoriser l'utilisateur à contrôler les paramètres applicatifs :** permet aux utilisateurs

de désinstaller des applications, de désactiver des applications, d'effacer le cache et les données, de forcer l'arrêt de toute application et d'effacer les paramètres par défaut. Les utilisateurs effectuent ces actions à partir de l'application Paramètres. La valeur par défaut est **Désactivé**.

- **Autoriser désinstallation d'applications :** permet aux utilisateurs de désinstaller des applications depuis le Google Play Store d'entreprise. La valeur par défaut est **Désactivé**. Pour afficher ce paramètre, activez la propriété de serveur `afw.restriction.policy.v2`. Pour plus d'informations sur les propriétés du serveur, veuillez consulter la section Propriétés du serveur.

- **Profil de travail BYOD**
  - **Autoriser les widgets d'applications de profil de travail sur l'écran d'accueil :** si ce paramètre est **Activé**, les utilisateurs peuvent placer des widgets d'application de profil de travail sur l'écran d'accueil de l'appareil. Si ce paramètre est **Désactivé**, les utilisateurs ne peuvent pas placer de widgets d'application de profil de travail sur l'écran d'accueil de l'appareil. La valeur par défaut est **Désactivé**.
    - **Applications avec widgets autorisés :** liste des applications que vous souhaitez autoriser sur l'écran d'accueil. Définissez l'option **Autoriser les widgets d'applications de profil de travail sur l'écran d'accueil** sur **Activé** et ajoutez l'application. Cliquez sur **Ajouter** et sélectionnez dans la liste une application pour laquelle vous souhaitez autoriser l'affichage des widgets sur l'écran d'accueil. Cliquez sur **Enregistrer**. Répétez ce processus pour autoriser plus de widgets d'application.
  - **Autoriser les contacts de profil de travail dans les contacts de l'appareil :** affiche les contacts du profil Android Enterprise géré dans le profil parent pour les appels entrants (Android 7.0 et versions ultérieures). La valeur par défaut est **Désactivé**.

- **Appareil entièrement géré uniquement**
  - **Autoriser l'ajout d'utilisateurs :** permet aux utilisateurs d'ajouter de nouveaux utilisateurs sur un appareil. La valeur par défaut est **Activé**.
  - **Autoriser itinérance des données :** autorise les utilisateurs à utiliser des données cellulaires en itinérance. La valeur par défaut est Désactivé, ce qui désactive l'itinérance sur les appareils des utilisateurs. La valeur par défaut est **Désactivé**.
  - **Autoriser les SMS :** autorise les utilisateurs à envoyer et à recevoir des messages SMS. La valeur par défaut est **Désactivé**.
  - **Autoriser utilisation de la barre d'état :** si ce paramètre est défini sur **Activé**, la barre d'état est activée sur les appareils gérés et les appareils dédiés (également appelés appareils d'entreprise à usage unique ou COSU). Cela désactive les notifications, les paramètres rapides et autres superpositions d'écran qui permettent de sortir du mode plein écran. Les utilisateurs peuvent accéder aux paramètres du système et afficher les notifications. Pour Android 6.0 et versions ultérieures. La valeur par défaut est **Désactivé**.

  - **Autoriser le bluetooth :** autorise les utilisateurs à utiliser Bluetooth. La valeur par défaut est **Activé**.
    * **Autoriser le partage Bluetooth :** si cette option est désactivée, les utilisateurs ne peuvent pas établir de partage Bluetooth sortant sur leurs appareils. Par défaut, ce paramètre est sélectionné. Pour afficher ce paramètre, activez la propriété de serveur `afw.restriction.policy.v2`. Pour plus d'informations sur les propriétés du serveur, veuillez consulter la section Propriétés du serveur.
  - **Autoriser la configuration de la date et de l'heure :** permet aux utilisateurs de modifier la date et l'heure sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser réinitialisation des paramètres d'usine :** autorise les utilisateurs à effectuer une réinitialisation d'usine sur leurs appareils. La valeur par défaut est **Activé**.
  - **Laisser l'écran allumé :** si ce paramètre est **activé**, l'écran de l'appareil reste allumé lorsque l'appareil est branché. La valeur par défaut est **Désactivé**.
  - **Autoriser le stockage de masse USB :** autorise le transfert de fichiers de données volumineux entre les appareils des utilisateurs et un ordinateur via une connexion USB. La valeur par défaut est **Activé**.
  - **Autoriser le microphone :** autorise les utilisateurs à utiliser le microphone sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser le partage de connexion :** permet aux utilisateurs de configurer des points d'accès mobiles et des données de connexion. La valeur par défaut est **Désactivé**.
  - **Empêcher Keyguard de verrouiller l'appareil :** si ce paramètre est **activé**, il désactive Keyguard sur l'écran de verrouillage sur les appareils gérés et les appareils dédiés (également appelés appareils d'entreprise à usage unique). La valeur par défaut est **Désactivé**.
  - **Autoriser les modifications Wi-Fi :** si ce paramètre est **activé**, les utilisateurs peuvent activer ou désactiver le Wi-Fi et se connecter aux réseaux Wi-Fi. La valeur par défaut est **Activé**.
  - **Autoriser transfert de fichiers :** permet le transfert de fichiers via USB. La valeur par défaut est **Désactivé**.

- **Samsung**

  - **Activer le keystore TIMA :** le magasin de clé TIMA fournit un stockage de clé sécurisé basé sur TrustZone pour les clés symétriques. Les paires de clés RSA et les certificats sont routés vers le fournisseur de magasins de clés par défaut à des fins de stockage. La valeur par défaut est **Désactivé**.
  - **Autoriser liste Partager :** autorise les utilisateurs à partager un contenu entre des applications dans la liste Partager via. La valeur par défaut est **Activé**.
  - **Activer le journal d'audit :** autorise la création de journaux d'audit d'événements pour l'analyse poussée d'un appareil. La valeur par défaut est **Désactivé**.

- **Samsung : appareil entièrement géré uniquement**

- **Activer la vérification du démarrage fiable ODE :** utilise la vérification du démarrage fiable ODE pour établir une chaîne d'approbation allant du bootloader vers l'image système. La valeur par défaut est **Activé**.
- **Autoriser les appels d'urgence uniquement :** autorise les utilisateurs à activer le mode Appel d'urgence uniquement sur leurs appareils. La valeur par défaut est **Désactivé**.
- **Autoriser la restauration du firmware :** autorise les utilisateurs à récupérer le firmware sur leurs appareils. La valeur par défaut est **Activé**.
- **Autoriser le cryptage rapide :** autorise le cryptage de l'espace de mémoire utilisé uniquement. Ce cryptage est différent du cryptage complet du disque qui crypte toutes les données. Ces données incluent les paramètres, les données d'application, les fichiers et applications téléchargés, les fichiers multimédias et autres fichiers. La valeur par défaut est **Activé**.
- **Activer le mode Critères communs :** fait passer l'appareil en mode Critères communs. La configuration de type Critère commun applique des processus de sécurité stricts. La valeur par défaut est **Activé**.
- **Activer la bannière de redémarrage :** affiche un message ou une bannière de notification d'utilisation du système approuvée par DoD au redémarrage des appareils. La valeur par défaut est **Désactivé**.
- **Autoriser la modification des paramètres :** permet aux utilisateurs de modifier les paramètres de leurs appareils entièrement gérés. La valeur par défaut est **Activé**.
- **Activer l'utilisation des données en arrière-plan :** permet aux applications de synchroniser les données en arrière-plan. Pour les appareils entièrement gérés. La valeur par défaut est **Activé**.
- **Autoriser le presse-papiers :** autorise les utilisateurs à copier des données dans le Presse-papiers de leurs appareils.
  * **Autoriser le partage du presse-papiers :** autorise les utilisateurs à partager le contenu du Presse-papiers entre leurs appareils et un ordinateur (MDM 4.0 et versions ultérieures).
- **Autoriser la touche Origine :** autorise les utilisateurs à utiliser la touche **Début** sur leurs appareils entièrement gérés. La valeur par défaut est **Activé**.
- **Autoriser positions factices :** autorise les utilisateurs à feindre leur emplacement de géolocalisation. Pour les appareils entièrement gérés. La valeur par défaut est **Désactivé**.
- **NFC :** autorise les utilisateurs à utiliser NFC sur leurs appareils entièrement gérés (MDM 3.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser mise hors tension :** autorise les utilisateurs à arrêter leurs appareils entièrement gérés (MDM 3.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser Wi-Fi direct :** autorise les utilisateurs à se connecter directement à un autre appareil à l'aide de leur connexion Wi-Fi. La valeur par défaut est **Activé**. Si ce paramètre est **activé**, vous devez activer le paramètre **Autoriser modifications du Wi-Fi**.

- **Autoriser carte SD :** autorise les utilisateurs à utiliser une carte SD, le cas échéant, avec leurs appareils. La valeur par défaut est **Activé**.
- **Autoriser le stockage hôte USB :** autorise les appareils des utilisateurs à agir comme hôte USB lorsqu'un périphérique USB se connecte aux appareils. Les appareils des utilisateurs fournissent ensuite l'alimentation au périphérique USB. La valeur par défaut est **Activé**.
- **Autoriser composeur vocal :** autorise les utilisateurs à utiliser le composeur vocal sur leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser S Beam :** autorise les utilisateurs à partager un contenu avec des tiers à l'aide de NFC et Wi-Fi Direct (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser S Voice :** autorise les utilisateurs à utiliser l'assistant personnel intelligent et le navigateur de connaissances sur leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser partage de connexion USB :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion USB. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, **Autoriser le partage de connexion** doit également être défini sur **Activé**.
- **Autoriser partage de connexion Bluetooth :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion Bluetooth. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, **Autoriser le partage de connexion** doit également être défini sur **Activé**.
  - **Autoriser le partage Bluetooth :** si cette option est désactivée, les utilisateurs ne peuvent pas établir de partage Bluetooth sortant sur leurs appareils. Par défaut, ce paramètre est sélectionné. Pour afficher ce paramètre, activez la propriété de serveur `afw.restriction.policy.v2`. Pour plus d'informations sur les propriétés du serveur, veuillez consulter la section Propriétés du serveur.
- **Autoriser partage de connexion Wi-Fi :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion Wi-Fi. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, **Autoriser le partage de connexion** doit également être défini sur **Activé**.
- **Autoriser les MMS entrants :** autorise les utilisateurs à recevoir des messages MMS. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Autoriser les MMS sortants :** autorise les utilisateurs à envoyer des messages MMS. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Autoriser les SMS entrants :** autorise les utilisateurs à recevoir des messages texte. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Autoriser les SMS sortants :** autorise les utilisateurs à envoyer des messages texte.

La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.

- **Configurer réseaux mobiles :** permet aux utilisateurs d'utiliser leurs données cellulaires. La valeur par défaut est **Désactivé**.
- **Limite par jour (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque jour. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Limite par semaine (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque semaine. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Limite par mois (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque mois. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Autoriser uniquement les connexions VPN sécurisées :** autorise les utilisateurs à uniquement utiliser des connexions sécurisées (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser l'enregistrement audio :** autorise les utilisateurs à effectuer des enregistrements audio avec leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser le microphone**.
- **Autoriser l'enregistrement vidéo :** autorise les utilisateurs à effectuer des enregistrements vidéo avec leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser l'utilisation de l'appareil photo**.
- **Autoriser messages push en itinérance :** autorise les utilisateurs à utiliser des données cellulaires pour la transmission. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser itinérance des données**.
- **Autoriser synchronisation automatique en itinérance :** autorise les utilisateurs à utiliser les données cellulaires pour la synchronisation. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser itinérance des données**.
- **Autoriser appels vocaux en itinérance :** autorise les utilisateurs à utiliser des données cellulaires pour les appels vocaux. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser itinérance des données**.

- **Samsung : conteneur Knox/appareil entièrement géré**
  - **Activer la vérification de révocation :** active la vérification des listes de certificats révoqués. La valeur par défaut est **Désactivé**.
- **Samsung : conteneur Knox uniquement**

- **Déplacer les applications sur le conteneur :** autorise les utilisateurs à déplacer des applications entre le conteneur Knox et la zone personnelle sur leurs appareils. La valeur par défaut est **Activé**.
- **Appliquer l'authentification à plusieurs facteurs :** les utilisateurs doivent utiliser une empreinte digitale et une autre méthode d'authentification, comme un mot de passe ou un code PIN, pour ouvrir leurs appareils. La valeur par défaut est **Activé**.
- **Appliquer l'authentification pour le conteneur :** utilisez une méthode d'authentification différente de celle utilisée pour déverrouiller l'appareil pour ouvrir le conteneur KNOX. La valeur par défaut est **Activé**.
- **Activer le clavier sécurisé :** impose aux utilisateurs d'utiliser un clavier sécurisé dans le conteneur Knox. La valeur par défaut est **Activé**.

- **Samsung DeX**
  - **Activer Samsung DeX :** permet aux appareils compatibles Knox pris en charge de fonctionner en mode Samsung DeX. Nécessite Samsung Knox 3.1 (version minimale). La valeur par défaut est **Activé**. Pour plus d'informations sur la configuration requise de l'appareil Samsung DeX et sur la configuration de Samsung DeX, consultez la documentation des développeurs Samsung.
    * **Autoriser Ethernet en mode DeX uniquement :** active l'utilisation d'Ethernet en mode Samsung DeX. Les données cellulaires, le Wi-Fi et le partage de connexion (Wi-Fi, Bluetooth et USB) sont limités en mode DeX. Par défaut, ce paramètre n'est pas sélectionné.
    * **Charger image du logo DeX :** sélectionnez ce paramètre pour spécifier une image .png à utiliser comme icône pour Samsung DeX.
    * **Délai d'expiration de l'écran DeX (secondes) :** spécifiez la durée d'inactivité, en secondes, après laquelle l'écran DeX s'éteint. Pour désactiver le délai d'attente, tapez **0**. La valeur par défaut est **1200** secondes (20 minutes).
    * **Ajouter raccourci d'application dans Samsung DeX :** spécifiez un nom de package d'application pour ajouter un raccourci vers DeX. Pour rechercher un nom de package d'application, accédez à Google Play et sélectionnez l'application. L'URL comprend le nom du package : `https://play.google.com/store/apps/details?id=<package.name><!--NeedCopy-->`.
    * **Supprimer raccourci d'application dans Samsung DeX :** spécifiez un nom de package d'application pour supprimer un raccourci de DeX. Accédez à Google Play pour rechercher les noms de packages d'applications.
    * **Packages d'applications à désactiver dans Samsung DeX :** spécifiez une liste séparée par des virgules des packages d'applications que vous souhaitez bloquer en mode Samsung DeX. Par exemple : `"com.android.chrome", "com.google.android.gm"<!--NeedCopy-->`.

Lorsque l'option **Appliquer aux appareils entièrement gérés dotés d'un profil professionnel** est ac-

tivée et que l'option **Pour les appareils entièrement gérés avec un profil professionnel, appliquez la stratégie à** est définie sur **Profil de travail**, configurez ces paramètres :

- **Sécurité**
  - **Autoriser la gestion des comptes :** permet au compte d'être ajouté aux appareils se trouvant dans le profil de travail et aux appareils gérés. La valeur par défaut est **Désactivé**.
  - **Autoriser le copier/coller entre les profils :** si cette option est définie sur **Activé**, les utilisateurs sont autorisés à copier et coller entre les applications du profil Android Enterprise et les applications dans la zone personnelle. La valeur par défaut est **Désactivé**.
  - **Autoriser la capture d'écran :** permet aux utilisateurs d'enregistrer ou de prendre une capture d'écran de l'écran de l'appareil. La valeur par défaut est **Désactivé**.
  - **Autoriser l'utilisation de l'appareil photo :** permet aux utilisateurs de prendre des photos et de créer des vidéos avec l'appareil photo de leurs appareils. La valeur par défaut est **Désactivé**.
  - **Autoriser configuration du fournisseur de localisation :** autorise les utilisateurs à activer le GPS sur leurs appareils. Pour Android API 28 et versions ultérieures. La valeur par défaut est **Activé**.
  - **Autoriser partage de position :** pour les profils gérés, le propriétaire de l'appareil peut modifier ce paramètre. La valeur par défaut est **Désactivé**.

    > **Conseil :**
    >
    > Vous pouvez créer des stratégies d'emplacement dans XenMobile pour imposer des limites géographiques. Voir Stratégie d'emplacement.

  - **Autoriser l'utilisateur à configurer les informations d'identification :** indiquez si les utilisateurs peuvent configurer les informations d'identification dans le keystore géré. La valeur par défaut est **Activé**.
  - **Autoriser l'impression :** si ce paramètre est défini sur **Activé**, les utilisateurs peuvent imprimer sur une imprimante accessible à partir de la machine utilisateur. La valeur par défaut est **Désactivé**. Disponible pour : Android 9 et versions ultérieures.
- **Applications**
  - **Activer les applications système :** permet aux utilisateurs d'exécuter des applications d'appareil préinstallées. La valeur par défaut est **Désactivé**. Pour activer des applications spécifiques, cliquez sur **Ajouter** dans le tableau **Liste des applications système**.
    - **Liste des applications système :** liste des applications système que vous souhaitez activer sur l'appareil. Définissez **Activer les applications système** sur **Activé** et ajoutez le nom du package d'application. Pour rechercher le

nom du package d'une application système, vous pouvez utiliser Android Debug Bridge (`adb`) pour appeler la commande de gestionnaire de packages Android (`pm`). Par exemple, `adb shell "pm list packages -f name"`, où « name » fait partie du nom du package. Pour plus d'informations, consultez https://developer.android.com/studio/command-line/adb. Pour les appareils Android Enterprise, vous pouvez restreindre les autorisations des applications à l'aide de la stratégie Autorisations applicatives Android Entreprise.

- **Désactiver les applications :** bloque l'exécution d'une liste spécifique d'applications sur des appareils. La valeur par défaut est **Désactivé**. Pour désactiver une application installée, définissez le paramètre sur **Activé**, cliquez sur **Ajouter** dans le tableau **Liste d'applications**.
  - **Liste des applications :** liste des applications que vous souhaitez bloquer. Définissez **Désactiver les applications** sur **Activé** et ajoutez l'application. Tapez le nom du package de l'application. La modification et le déploiement d'une liste d'applications écrasent la liste d'applications précédente. Par exemple : si vous désactivez com.example1 et com.example2 et modifiez ensuite la liste vers com.example1 et com.example3, XenMobile active com.example.2.
- **Activer vérification de l'application :** permet au système d'exploitation d'analyser les applications pour détecter un comportement malveillant. La valeur par défaut est **Activé**.
- **Activer Google Apps :** permet aux utilisateurs de télécharger des applications à partir de Google Mobile Services sur l'appareil. La valeur par défaut est **Activé**.
- **Autoriser les applications non Google Play :** permet l'installation d'applications provenant de magasins autres que Google Play. La valeur par défaut est **Désactivé**.
- **Autoriser l'utilisateur à contrôler les paramètres applicatifs :** permet aux utilisateurs de désinstaller des applications, de désactiver des applications, d'effacer le cache et les données, de forcer l'arrêt de toute application et d'effacer les paramètres par défaut. Les utilisateurs effectuent ces actions à partir de l'application Paramètres. La valeur par défaut est **Désactivé**.
- **Autoriser désinstallation d'applications :** permet aux utilisateurs de désinstaller des applications depuis le Google Play Store d'entreprise. La valeur par défaut est **Désactivé**. Pour afficher ce paramètre, activez la propriété de serveur `afw.restriction.policy.v2`. Pour plus d'informations sur les propriétés du serveur, veuillez consulter la section Propriétés du serveur.

- **Profil de travail BYOD**
  - **Autoriser les widgets d'applications de profil de travail sur l'écran d'accueil :** si ce paramètre est **Activé**, les utilisateurs peuvent placer des widgets d'application de profil de travail sur l'écran d'accueil de l'appareil. Si ce paramètre est **Désactivé**, les utilisateurs ne peuvent pas placer de widgets d'application de profil de travail sur l'écran d'accueil de l'appareil. La valeur par défaut est **Désactivé**.

        * **Applications avec widgets autorisés :** liste des applications que vous souhaitez autoriser sur l'écran d'accueil. Définissez l'option **Autoriser les widgets d'applications de profil de travail sur l'écran d'accueil** sur **Activé** et ajoutez l'application. Cliquez sur **Ajouter** et sélectionnez dans la liste une application pour laquelle vous souhaitez autoriser l'affichage des widgets sur l'écran d'accueil. Cliquez sur **Enregistrer**. Répétez ce processus pour autoriser plus de widgets d'application.
    - **Autoriser les contacts de profil de travail dans les contacts de l'appareil :** affiche les contacts du profil Android Enterprise géré dans le profil parent pour les appels entrants (Android 7.0 et versions ultérieures). La valeur par défaut est **Désactivé**.

- **Samsung**
    - **Activer le keystore TIMA :** le magasin de clé TIMA fournit un stockage de clé sécurisé basé sur TrustZone pour les clés symétriques. Les paires de clés RSA et les certificats sont routés vers le fournisseur de magasins de clés par défaut à des fins de stockage. La valeur par défaut est **Désactivé**.
    - **Autoriser liste Partager :** autorise les utilisateurs à partager un contenu entre des applications dans la liste Partager via. La valeur par défaut est **Activé**.
    - **Activer le journal d'audit :** autorise la création de journaux d'audit d'événements pour l'analyse poussée d'un appareil. La valeur par défaut est **Désactivé**.
- **Samsung : conteneur Knox/appareil entièrement géré**
    - **Activer la vérification de révocation :** active la vérification des listes de certificats révoqués. La valeur par défaut est **Désactivé**.
- **Samsung : conteneur Knox uniquement**
    - **Déplacer les applications sur le conteneur :** autorise les utilisateurs à déplacer des applications entre le conteneur Knox et la zone personnelle sur leurs appareils. La valeur par défaut est **Activé**.
    - **Appliquer l'authentification à plusieurs facteurs :** les utilisateurs doivent utiliser une empreinte digitale et une autre méthode d'authentification, comme un mot de passe ou un code PIN, pour ouvrir leurs appareils. La valeur par défaut est **Activé**.
    - **Appliquer l'authentification pour le conteneur :** utilisez une méthode d'authentification différente de celle utilisée pour déverrouiller l'appareil pour ouvrir le conteneur KNOX. La valeur par défaut est **Activé**.
    - **Activer le clavier sécurisé :** impose aux utilisateurs d'utiliser un clavier sécurisé dans le conteneur Knox. La valeur par défaut est **Activé**.

Lorsque l'option **Appliquer aux appareils entièrement gérés dotés d'un profil professionnel** est activée et que l'option **Pour les appareils entièrement gérés avec un profil professionnel, appliquez la stratégie à** est définie sur **Appareil géré**, configurez ces paramètres :

- **Sécurité**

- **Autoriser la gestion des comptes :** permet au compte d'être ajouté aux appareils se trouvant dans le profil de travail et aux appareils gérés. La valeur par défaut est **Désactivé**.
- **Autoriser le copier/coller entre les profils :** si cette option est définie sur **Activé**, les utilisateurs sont autorisés à copier et coller entre les applications du profil Android Enterprise et les applications dans la zone personnelle. La valeur par défaut est **Désactivé**.
- **Autoriser la capture d'écran :** permet aux utilisateurs d'enregistrer ou de prendre une capture d'écran de l'écran de l'appareil. La valeur par défaut est **Désactivé**.
- **Autoriser l'utilisation de l'appareil photo :** permet aux utilisateurs de prendre des photos et de créer des vidéos avec l'appareil photo de leurs appareils. La valeur par défaut est **Désactivé**.
- **Autoriser configuration du VPN :** autorise les utilisateurs à créer des configurations VPN. Pour les appareils en mode Profil de travail fonctionnant sous Android 6 et versions ultérieures et pour les appareils entièrement gérés. La valeur par défaut est **Activé**.
- **Autoriser service de sauvegarde :** autorise les utilisateurs à sauvegarder leurs données d'application et système sur leurs appareils. La valeur par défaut est **Activé**.
- **Autoriser NFC :** autorise les utilisateurs à envoyer des pages Web, des photos, des vidéos ou tout autre contenu de leurs appareils à un autre appareil via la communication en champ proche (NFC). Pour MDM 4.0 et versions ultérieures. La valeur par défaut est **Activé**.
- **Autoriser configuration du fournisseur de localisation :** autorise les utilisateurs à activer le GPS sur leurs appareils. Pour Android API 28 et versions ultérieures. La valeur par défaut est **Activé**.
- **Autoriser partage de position :** pour les profils gérés, le propriétaire de l'appareil peut modifier ce paramètre. La valeur par défaut est **Désactivé**.

  > **Conseil :**
  >
  > Vous pouvez créer des stratégies d'emplacement dans XenMobile pour imposer des limites géographiques. Voir Stratégie d'emplacement.

- **Autoriser l'utilisateur à configurer les informations d'identification :** indiquez si les utilisateurs peuvent configurer les informations d'identification dans le keystore géré. La valeur par défaut est **Activé**.
- **Autoriser l'impression :** si ce paramètre est défini sur **Activé**, les utilisateurs peuvent imprimer sur une imprimante accessible à partir de la machine utilisateur. La valeur par défaut est **Désactivé**. Disponible pour : Android 9 et versions ultérieures.
- **Autoriser le débogage USB : Désactivé** par défaut.

- **Applications**

- **Activer les applications système :** permet aux utilisateurs d'exécuter des applications d'appareil préinstallées. La valeur par défaut est **Désactivé**. Pour activer des applications spécifiques, cliquez sur **Ajouter** dans le tableau **Liste des applications système**.
  - **Liste des applications système :** liste des applications système que vous souhaitez activer sur l'appareil. Définissez **Activer les applications système** sur **Activé** et ajoutez le nom du package d'application. Pour rechercher le nom du package d'une application système, vous pouvez utiliser Android Debug Bridge (`adb`) pour appeler la commande de gestionnaire de packages Android (`pm`). Par exemple, `adb shell "pm list packages -f name"`, où « name » fait partie du nom du package. Pour plus d'informations, consultez https://developer.android.com/studio/command-line/adb. Pour les appareils Android Enterprise, vous pouvez restreindre les autorisations des applications à l'aide de la stratégie Autorisations applicatives Android Entreprise.
- **Désactiver les applications :** bloque l'exécution d'une liste spécifique d'applications sur des appareils. La valeur par défaut est **Désactivé**. Pour désactiver une application installée, définissez le paramètre sur **Activé**, cliquez sur **Ajouter** dans le tableau **Liste d'applications**.
  - **Liste des applications :** liste des applications que vous souhaitez bloquer. Définissez **Désactiver les applications** sur **Activé** et ajoutez l'application. Tapez le nom du package de l'application. La modification et le déploiement d'une liste d'applications écrasent la liste d'applications précédente. Par exemple : si vous désactivez com.example1 et com.example2 et modifiez ensuite la liste vers com.example1 et com.example3, XenMobile active com.example.2.
- **Activer vérification de l'application :** permet au système d'exploitation d'analyser les applications pour détecter un comportement malveillant. La valeur par défaut est **Activé**.
- **Activer Google Apps :** permet aux utilisateurs de télécharger des applications à partir de Google Mobile Services sur l'appareil. La valeur par défaut est **Activé**.
- **Autoriser les applications non Google Play :** permet l'installation d'applications provenant de magasins autres que Google Play. La valeur par défaut est **Désactivé**.
- **Autoriser l'utilisateur à contrôler les paramètres applicatifs :** permet aux utilisateurs de désinstaller des applications, de désactiver des applications, d'effacer le cache et les données, de forcer l'arrêt de toute application et d'effacer les paramètres par défaut. Les utilisateurs effectuent ces actions à partir de l'application Paramètres. La valeur par défaut est **Désactivé**.
- **Autoriser désinstallation d'applications :** permet aux utilisateurs de désinstaller des applications depuis le Google Play Store d'entreprise. La valeur par défaut est **Désactivé**. Pour afficher ce paramètre, activez la propriété de serveur `afw.restriction.policy.v2`. Pour plus d'informations sur les propriétés du serveur, veuillez consulter la section Propriétés du serveur.

- **Appareil entièrement géré uniquement**
  - **Autoriser l'ajout d'utilisateurs :** permet aux utilisateurs d'ajouter de nouveaux utilisateurs sur un appareil. La valeur par défaut est **Activé**.
  - **Autoriser itinérance des données :** autorise les utilisateurs à utiliser des données cellulaires en itinérance. La valeur par défaut est Désactivé, ce qui désactive l'itinérance sur les appareils des utilisateurs. La valeur par défaut est **Désactivé**.
  - **Autoriser les SMS :** autorise les utilisateurs à envoyer et à recevoir des messages SMS. La valeur par défaut est **Désactivé**.
  - **Autoriser utilisation de la barre d'état :** si ce paramètre est défini sur **Activé**, la barre d'état est activée sur les appareils gérés et les appareils dédiés (également appelés appareils d'entreprise à usage unique ou COSU). Cela désactive les notifications, les paramètres rapides et autres superpositions d'écran qui permettent de sortir du mode plein écran. Les utilisateurs peuvent accéder aux paramètres du système et afficher les notifications. Pour Android 6.0 et versions ultérieures. La valeur par défaut est **Désactivé**.
  - **Autoriser le bluetooth :** autorise les utilisateurs à utiliser Bluetooth. La valeur par défaut est **Activé**.
    - **Autoriser le partage Bluetooth :** si cette option est désactivée, les utilisateurs ne peuvent pas établir de partage Bluetooth sortant sur leurs appareils. Par défaut, ce paramètre est sélectionné. Pour afficher ce paramètre, activez la propriété de serveur `afw.restriction.policy.v2`. Pour plus d'informations sur les propriétés du serveur, veuillez consulter la section Propriétés du serveur.
  - **Autoriser la configuration de la date et de l'heure :** permet aux utilisateurs de modifier la date et l'heure sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser réinitialisation des paramètres d'usine :** autorise les utilisateurs à effectuer une réinitialisation d'usine sur leurs appareils. La valeur par défaut est **Activé**.
  - **Laisser l'écran allumé :** si ce paramètre est **activé**, l'écran de l'appareil reste allumé lorsque l'appareil est branché. La valeur par défaut est **Désactivé**.
  - **Autoriser le stockage de masse USB :** autorise le transfert de fichiers de données volumineux entre les appareils des utilisateurs et un ordinateur via une connexion USB. La valeur par défaut est **Activé**.
  - **Autoriser le microphone :** autorise les utilisateurs à utiliser le microphone sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser le partage de connexion :** permet aux utilisateurs de configurer des points d'accès mobiles et des données de connexion. La valeur par défaut est **Désactivé**. Lorsque ce paramètre est activé, ces paramètres sont disponibles pour les appareils Samsung :
  - **Empêcher Keyguard de verrouiller l'appareil :** si ce paramètre est **activé**, il désactive Keyguard sur l'écran de verrouillage sur les appareils gérés et les appareils dédiés (également appelés appareils d'entreprise à usage unique). La valeur par défaut est **Désactivé**.
  - **Autoriser les modifications Wi-Fi :** si ce paramètre est **activé**, les utilisateurs peuvent

activer ou désactiver le Wi-Fi et se connecter aux réseaux Wi-Fi. La valeur par défaut est **Activé**.
- **Autoriser transfert de fichiers :** permet le transfert de fichiers via USB. La valeur par défaut est **Désactivé**.

- **Samsung**
  - **Activer le keystore TIMA :** le magasin de clé TIMA fournit un stockage de clé sécurisé basé sur TrustZone pour les clés symétriques. Les paires de clés RSA et les certificats sont routés vers le fournisseur de magasins de clés par défaut à des fins de stockage. La valeur par défaut est **Désactivé**.
  - **Autoriser liste Partager :** autorise les utilisateurs à partager un contenu entre des applications dans la liste Partager via. La valeur par défaut est **Activé**.
  - **Activer le journal d'audit :** autorise la création de journaux d'audit d'événements pour l'analyse poussée d'un appareil. La valeur par défaut est **Désactivé**.

- **Samsung : appareil entièrement géré uniquement**
  - **Activer la vérification du démarrage fiable ODE :** utilise la vérification du démarrage fiable ODE pour établir une chaîne d'approbation allant du bootloader vers l'image système. La valeur par défaut est **Activé**.
  - **Autoriser les appels d'urgence uniquement :** autorise les utilisateurs à activer le mode Appel d'urgence uniquement sur leurs appareils. La valeur par défaut est **Désactivé**.
  - **Autoriser la restauration du firmware :** autorise les utilisateurs à récupérer le firmware sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser le cryptage rapide :** autorise le cryptage de l'espace de mémoire utilisé uniquement. Ce cryptage est différent du cryptage complet du disque qui crypte toutes les données. Ces données incluent les paramètres, les données d'application, les fichiers et applications téléchargés, les fichiers multimédias et autres fichiers. La valeur par défaut est **Activé**.
  - **Activer le mode Critères communs :** fait passer l'appareil en mode Critères communs. La configuration de type Critère commun applique des processus de sécurité stricts. La valeur par défaut est **Activé**.
  - **Activer la bannière de redémarrage :** affiche un message ou une bannière de notification d'utilisation du système approuvée par DoD au redémarrage des appareils. La valeur par défaut est **Désactivé**.
  - **Autoriser la modification des paramètres :** permet aux utilisateurs de modifier les paramètres de leurs appareils entièrement gérés. La valeur par défaut est **Activé**.
  - **Activer l'utilisation des données en arrière-plan :** permet aux applications de synchroniser les données en arrière-plan. Pour les appareils entièrement gérés. La valeur par défaut est **Activé**.
  - **Autoriser le presse-papiers :** autorise les utilisateurs à copier des données dans le Presse-

papiers de leurs appareils. La valeur par défaut est **Activé**.

  * **Autoriser le partage du presse-papiers :** autorise les utilisateurs à partager le contenu du Presse-papiers entre leurs appareils et un ordinateur (MDM 4.0 et versions ultérieures).

- **Autoriser la touche Origine :** autorise les utilisateurs à utiliser la touche **Début** sur leurs appareils entièrement gérés. La valeur par défaut est **Activé**.
- **Autoriser positions factices :** autorise les utilisateurs à feindre leur emplacement de géolocalisation. Pour les appareils entièrement gérés. La valeur par défaut est **Désactivé**.
- **NFC :** autorise les utilisateurs à utiliser NFC sur leurs appareils entièrement gérés (MDM 3.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser mise hors tension :** autorise les utilisateurs à arrêter leurs appareils entièrement gérés (MDM 3.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser Wi-Fi direct :** autorise les utilisateurs à se connecter directement à un autre appareil à l'aide de leur connexion Wi-Fi. La valeur par défaut est **Activé**. Si ce paramètre est **activé**, vous devez activer le paramètre **Autoriser modifications du Wi-Fi**.
- **Autoriser carte SD :** autorise les utilisateurs à utiliser une carte SD, le cas échéant, avec leurs appareils. La valeur par défaut est **Activé**.
- **Autoriser le stockage hôte USB :** autorise les appareils des utilisateurs à agir comme hôte USB lorsqu'un périphérique USB se connecte aux appareils. Les appareils des utilisateurs fournissent ensuite l'alimentation au périphérique USB. La valeur par défaut est **Activé**.
- **Autoriser composeur vocal :** autorise les utilisateurs à utiliser le composeur vocal sur leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser S Beam :** autorise les utilisateurs à partager un contenu avec des tiers à l'aide de NFC et Wi-Fi Direct (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser S Voice :** autorise les utilisateurs à utiliser l'assistant personnel intelligent et le navigateur de connaissances sur leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser partage de connexion USB :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion USB. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, **Autoriser le partage de connexion** doit également être défini sur **Activé**.
- **Autoriser partage de connexion Bluetooth :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion Bluetooth. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, **Autoriser le partage de connexion** doit également être défini sur **Activé**.
- **Autoriser partage de connexion Wi-Fi :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion Wi-Fi. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, **Autoriser le partage de connexion** doit également être défini sur **Activé**.

- **Autoriser les MMS entrants :** autorise les utilisateurs à recevoir des messages MMS. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Autoriser les MMS sortants :** autorise les utilisateurs à envoyer des messages MMS. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Autoriser les SMS entrants :** autorise les utilisateurs à recevoir des messages texte. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Autoriser les SMS sortants :** autorise les utilisateurs à envoyer des messages texte. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Configurer réseaux mobiles :** permet aux utilisateurs d'utiliser leurs données cellulaires. La valeur par défaut est **Désactivé**.
- **Limite par jour (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque jour. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Limite par semaine (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque semaine. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Limite par mois (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque mois. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Autoriser uniquement les connexions VPN sécurisées :** autorise les utilisateurs à uniquement utiliser des connexions sécurisées (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser l'enregistrement audio :** autorise les utilisateurs à effectuer des enregistrements audio avec leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser le microphone**.
- **Autoriser l'enregistrement vidéo :** autorise les utilisateurs à effectuer des enregistrements vidéo avec leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser l'utilisation de l'appareil photo**.
- **Autoriser messages push en itinérance :** autorise les utilisateurs à utiliser des données cellulaires pour la transmission. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser itinérance des données**.
- **Autoriser synchronisation automatique en itinérance :** autorise les utilisateurs à utiliser les données cellulaires pour la synchronisation. La valeur par défaut est **Désac-**

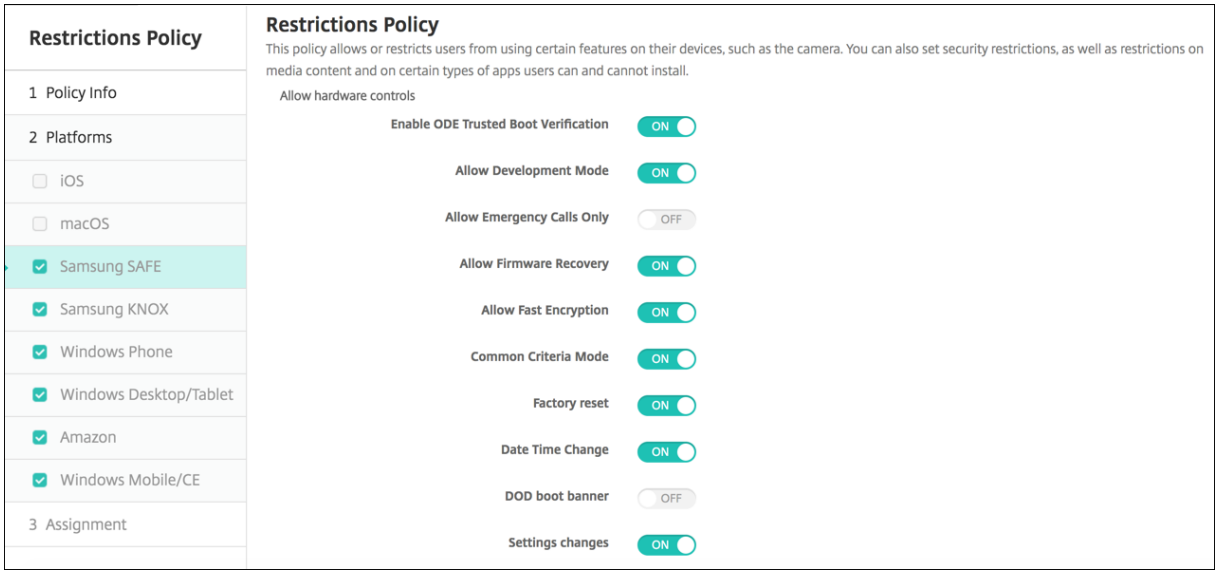
tivé. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser itinérance des données**.

- **Autoriser appels vocaux en itinérance :** autorise les utilisateurs à utiliser des données cellulaires pour les appels vocaux. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser itinérance des données**.

- **Samsung : conteneur Knox/appareil entièrement géré**
  - **Activer la vérification de révocation :** active la vérification des listes de certificats révoqués. La valeur par défaut est **Désactivé**.

- **Samsung : conteneur Knox uniquement**
  - **Déplacer les applications sur le conteneur :** autorise les utilisateurs à déplacer des applications entre le conteneur Knox et la zone personnelle sur leurs appareils. La valeur par défaut est **Activé**.
  - **Appliquer l'authentification à plusieurs facteurs :** les utilisateurs doivent utiliser une empreinte digitale et une autre méthode d'authentification, comme un mot de passe ou un code PIN, pour ouvrir leurs appareils. La valeur par défaut est **Activé**.
  - **Appliquer l'authentification pour le conteneur :** utilisez une méthode d'authentification différente de celle utilisée pour déverrouiller l'appareil pour ouvrir le conteneur KNOX. La valeur par défaut est **Activé**.
  - **Activer le clavier sécurisé :** impose aux utilisateurs d'utiliser un clavier sécurisé dans le conteneur Knox. La valeur par défaut est **Activé**.

Paramètres Samsung SAFE



Certaines options sont uniquement disponibles dans des API de gestion d'appareils mobiles Samsung spécifiques. Ces options sont marquées avec des informations sur la version appropriée.

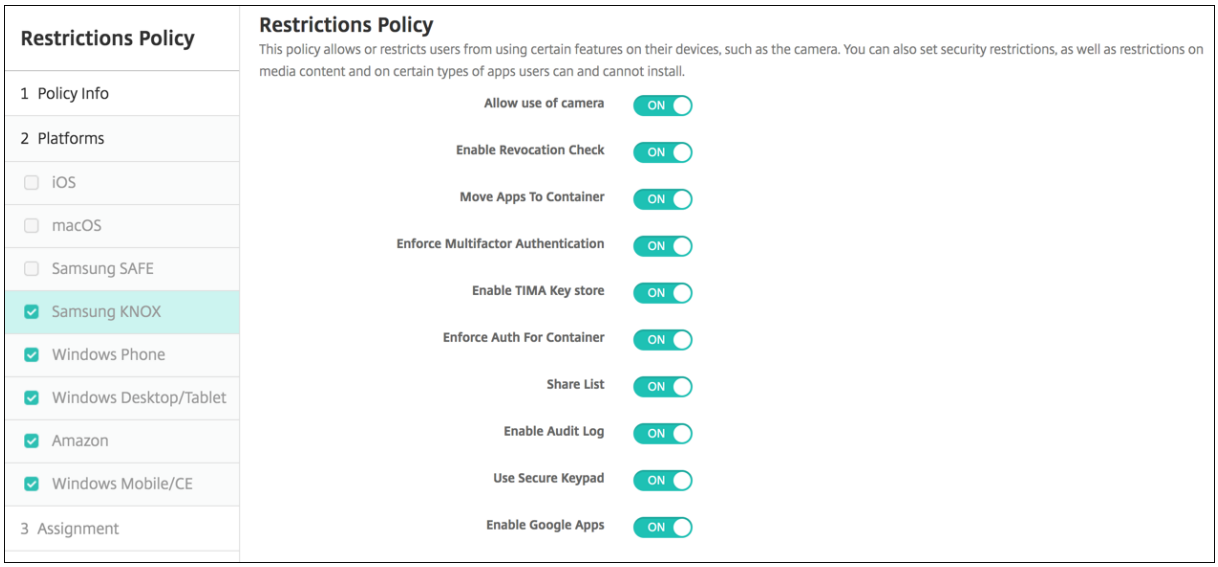
- **Autoriser le contrôle du matériel**
  - **Activer la vérification du démarrage fiable ODE :** utilise la vérification du démarrage fiable ODE pour établir une chaîne d'approbation allant du bootloader vers l'image système.
  - **Autoriser le mode de développement :** autorise les utilisateurs à activer les paramètres développeur sur leurs appareils.
  - **Autoriser les appels d'urgence uniquement :** autorise les utilisateurs à activer le mode Appel d'urgence uniquement sur leurs appareils.
  - **Autoriser la restauration du firmware :** autorise les utilisateurs à récupérer le firmware sur leurs appareils.
  - **Autoriser le cryptage rapide :** autorise le cryptage de l'espace de mémoire utilisé uniquement. Le cryptage de disque complet est différent puisqu'il crypte toutes les données, y compris les paramètres, les données d'application, les fichiers et applications téléchargés, les fichiers multimédias et autres fichiers.
  - **Mode Critère commun :** fait passer l'appareil en mode Critère commun. La configuration de type Critère commun applique des processus de sécurité stricts.
  - **Réinitialisation d'usine :** autorise les utilisateurs à effectuer une réinitialisation d'usine sur leurs appareils.
  - **Modification de la date/l'heure :** autorise les utilisateurs à modifier la date et l'heure sur leurs appareils.
  - **Bannière de démarrage DOD :** affiche un message ou une bannière de notification d'utilisation du système approuvée par DoD au redémarrage des appareils.
  - **Modification des paramètres :** autorise les utilisateurs à modifier les paramètres de leurs appareils.
  - **Sauvegarde :** autorise les utilisateurs à sauvegarder leurs données d'application et système sur leurs appareils.
  - **Mise à jour par réseau cellulaire :** autorise les appareils des utilisateurs à recevoir les mises à jour logicielles sans fil (MDM 3.0 et versions ultérieures).
  - **Fonctionnement en arrière-plan :** autorise les applications à synchroniser les données en arrière-plan.
  - **Appareil photo :** autorise les utilisateurs à utiliser l'appareil photo sur leurs appareils.
  - **Presse-papiers :** autorise les utilisateurs à copier des données dans le Presse-papiers de leurs appareils.
    - **Partage du presse-papiers :** autorise les utilisateurs à partager le contenu du Presse-papiers entre leurs appareils et un ordinateur (MDM 4.0 et versions ultérieures).
  - **Touche début :** autorise les utilisateurs à utiliser la touche Début sur leurs appareils.
  - **Microphone :** autorise les utilisateurs à utiliser le microphone sur leurs appareils.
  - **Localisation :** autorise les utilisateurs à feindre leur emplacement de géolocalisation.
  - **NFC :** autorise les utilisateurs à utiliser la communication NFC (communication en champ

proche) sur leurs appareils (MDM 3.0 et versions ultérieures).
  - **Arrêter :** autorise les utilisateurs à arrêter leurs appareils (MDM 3.0 et versions ultérieures).
  - **Capture d'écran :** autorise les utilisateurs à prendre des captures d'écrans sur leurs appareils.
  - **Carte SD :** autorise les utilisateurs à utiliser une carte SD, le cas échéant, avec leurs appareils.
  - **Composeur vocal :** autorise les utilisateurs à utiliser le composeur vocal sur leurs appareils (MDM 4.0 et versions ultérieures).
  - **SBeam :** autorise les utilisateurs à partager un contenu avec des tiers à l'aide de NFC et Wi-Fi Direct (MDM 4.0 et versions ultérieures).
  - **SVoice :** autorise les utilisateurs à utiliser l'assistant personnel intelligent et le navigateur de connaissances sur leurs appareils (MDM 4.0 et versions ultérieures).
  - **Autoriser utilisateurs multiples :** autorise plusieurs utilisateurs à utiliser un appareil (MDM 4.0 et versions ultérieures). La valeur par défaut est **Désactivé**.
- **Autoriser les applications**
  - **Navigateur :** autorise les utilisateurs à utiliser le navigateur Web.
  - **Youtube :** autorise les utilisateurs à accéder à YouTube.
  - **Google Play/Marketplace :** autorise les utilisateurs à accéder à Google Play et au Google Apps Marketplace.
  - **Autoriser les applications non Google Play :** autorise les utilisateurs à télécharger des applications à partir de sites autres que Google Play et Google Apps Marketplace. Si cette option est définie sur **Activé**, un utilisateur peut utiliser les paramètres de sécurité sur son appareil pour faire confiance aux applications de sources inconnues.
  - **Arrêt des applications système :** autorise les utilisateurs à désactiver les applications système préinstallées (MDM 4.0 et versions ultérieures).
  - **Désactiver les applications :** si cette option est définie sur **Activé**, l'exécution d'une liste spécifique d'applications est bloquée sur les appareils Samsung SAFE.
- **Réseau**
  - **MMS entrants :** autorise les utilisateurs à recevoir des messages MMS.
  - **SMS entrants :** autorise les utilisateurs à recevoir des messages texte.
  - **MMS sortants :** autorise les utilisateurs à envoyer des messages MMS.
  - **SMS sortants :** autorise les utilisateurs à envoyer des messages texte.
  - **Ajout de profils VPN par les utilisateurs :**
  - **Bluetooth :** autorise les utilisateurs à utiliser Bluetooth.
    - **Partage de connexion :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion Bluetooth.
  - **Wi-Fi :** autorise les utilisateurs à se connecter à des réseaux Wi-Fi.
    - **Partage de connexion :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion Wi-Fi.

    * **Direct :** autorise les utilisateurs à se connecter directement à un autre appareil à l'aide de leur connexion Wi-Fi (MDM 4.0 et versions ultérieures).
    * **Modification de l'état :** autorise les applications à modifier l'état de connectivité Wi-Fi.
    * **Modifications de la stratégie utilisateur :** autorise les utilisateurs à modifier les stratégies Wi-Fi. Si cette option n'est pas sélectionnée, les utilisateurs peuvent uniquement modifier le nom d'utilisateur et le mot de passe Wi-Fi. Si cette option est sélectionnée, les utilisateurs peuvent modifier toutes les stratégies Wi-Fi.
  - **Partage de connexion :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil.
  - **Données cellulaires :** autorise les utilisateurs à utiliser leur connexion cellulaire pour les données.
  - **Autoriser l'itinérance :** autorise les utilisateurs à utiliser des données cellulaires en itinérance. La valeur par défaut est Désactivé, ce qui désactive l'itinérance sur les appareils des utilisateurs.
  - **Connexions sécurisées uniquement :** autorise les utilisateurs à uniquement utiliser des connexions sécurisées (MDM 4.0 et versions ultérieures).
  - **Android beam :** autorise les utilisateurs à envoyer des pages Web, des photos, des vidéos ou tout autre contenu de leurs appareils à un autre appareil via NFC (MDM 4.0 et versions ultérieures).
  - **Enregistrement audio :** autorise les utilisateurs à effectuer des enregistrements audio avec leurs appareils (MDM 4.0 et versions ultérieures).
  - **Enregistrement vidéo :** autorise les utilisateurs à effectuer des enregistrements vidéo avec leurs appareils (MDM 4.0 et versions ultérieures).
  - **Services de localisation :** autorise les utilisateurs à activer le GPS sur leurs appareils.
  - **Limite par jour (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque jour. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
  - **Limite par semaine (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque semaine. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
  - **Limite par mois (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque mois. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Autoriser les actions USB :** autorise la connexion USB entre les appareils des utilisateurs et un ordinateur.
  - **Débogage :** autorise le débogage via USB.
  - **Stockage hôte :** autorise les appareils des utilisateurs à agir comme hôte USB lorsqu'un périphérique USB se connecte aux appareils. Les appareils des utilisateurs fournissent

ensuite l'alimentation au périphérique USB.
  - **Stockage de masse :** autorise le transfert de fichiers de données volumineux entre les appareils des utilisateurs et un ordinateur via une connexion USB.
  - **Lecteur multimédia Kies :** autorise les utilisateurs à utiliser l'outil Samsung Kies pour synchroniser les fichiers entre leurs appareils et un ordinateur.
  - **Partage de connexion :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil via une connexion USB.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

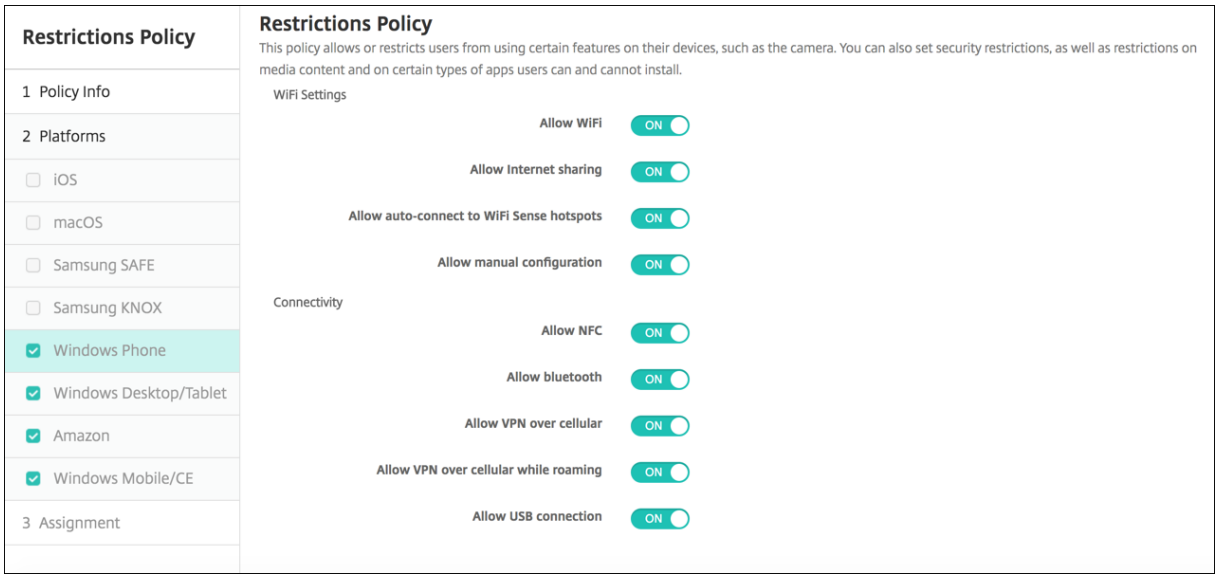
Paramètres Samsung KNOX



Ces options sont uniquement disponibles avec Samsung KNOX Premium (KNOX 2.0).

- **Autoriser l'utilisation de l'appareil photo :** autorise les utilisateurs à utiliser l'appareil photo sur leurs appareils.
- **Autoriser la vérification de révocation :** active la vérification des listes de certificats révoqués.
- **Déplacer les applications sur le conteneur :** autorise les utilisateurs à déplacer des applications entre le conteneur KNOX et la zone personnelle sur leurs appareils.
- **Appliquer l'authentification à plusieurs facteurs :** les utilisateurs doivent utiliser une empreinte digitale et une autre méthode d'authentification, comme un mot de passe ou un code PIN, pour ouvrir leurs appareils.
- **Activer le keystore TIMA :** le magasin de clé TIMA fournit un stockage de clé sécurisé basé sur TrustZone pour les clés symétriques. Les paires de clés RSA et les certificats sont routés vers le fournisseur de magasins de clés par défaut à des fins de stockage.
- **Appliquer l'authentification pour le conteneur :** utilise une authentification distincte, et différente de celle utilisée pour déverrouiller l'appareil, pour ouvrir le conteneur KNOX.
- **Partager la liste :** autorise les utilisateurs à partager un contenu entre des applications dans la liste Partager via.
- **Activer le journal d'audit :** autorise la création de journaux d'audit d'événements pour l'analyse poussée d'un appareil.
- **Utiliser le clavier sécurisé :** impose aux utilisateurs d'utiliser un clavier sécurisé dans le conteneur KNOX.
- **Activer Google Apps :** autorise les utilisateurs à télécharger des applications de Google Mobile Services vers le conteneur KNOX.
- **Authentification du navigateur par carte à puce :** active l'authentification du navigateur sur les appareils équipés d'un lecteur de carte à puce.

Paramètres Windows Phone et Windows Desktop/Tablet

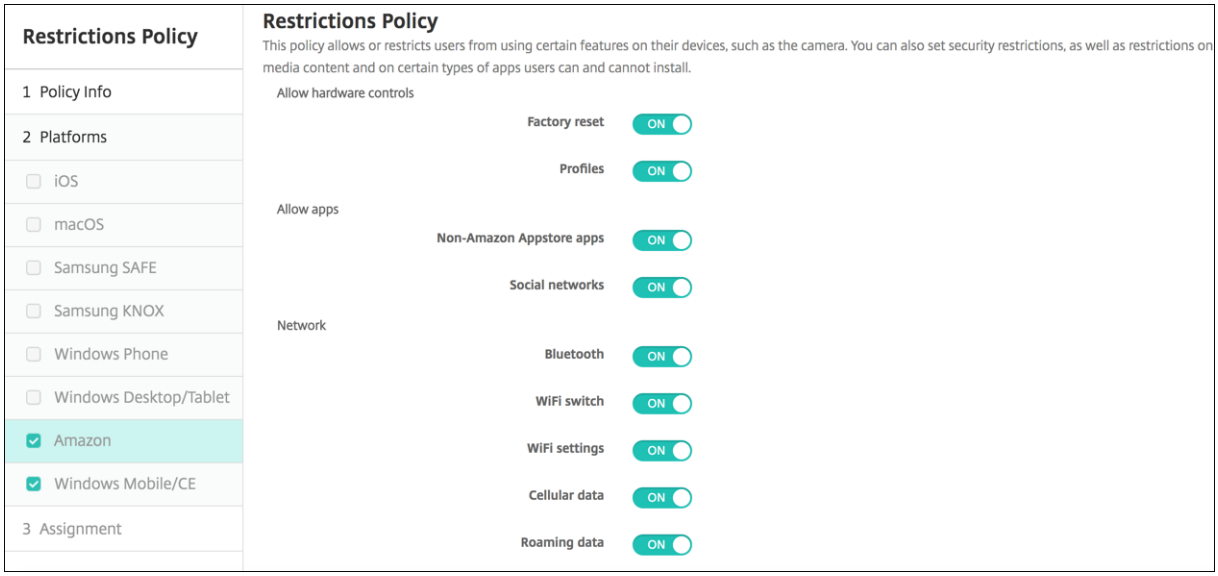


- **Paramètres Wi-Fi**
  - **Autoriser le Wi-Fi :** autorise un appareil à se connecter à un réseau Wi-Fi. Windows Phone uniquement.
  - **Autoriser le partage Internet :** autorise un appareil à partager sa connexion Internet avec d'autres appareils en le transformant en point d'accès Wi-Fi.
  - **Autoriser la connexion automatique aux points d'accès Wi-Fi Sense :** autorise un appareil à se connecter automatiquement à un point d'accès Wi-Fi Sense. Pour que cette option fonctionne, les services de géolocalisation doivent être activés. Pour plus d'informations sur Wi-Fi Sense, consultez le Forum aux questions Windows Phone FAQ Wi-Fi Sense.
  - **Autoriser la configuration manuelle :** autorise les utilisateurs à configurer manuellement les connexions Wi-Fi. Windows Phone uniquement.
- **Connectivité**
  - **Autoriser NFC :** autorise l'appareil à communiquer avec une balise NFC ou avec un autre appareil transmetteur compatible NFC. Windows Phone uniquement.
  - **Autoriser le bluetooth :** autorise l'appareil à se connecter via Bluetooth. Windows Phone uniquement.
  - **Autoriser les connexions VPN via réseau cellulaire :** autorise l'appareil à se connecter à un réseau cellulaire via un VPN.
  - **Autoriser les connexions VPN via réseau cellulaire en itinérance :** autorise l'appareil à se connecter au VPN lorsque l'appareil est en itinérance sur les réseaux cellulaires.
  - **Autoriser les connexions USB :** autorise un bureau à accéder au stockage d'un appareil via une connexion USB. Windows Phone uniquement.
  - **Autoriser les données cellulaires itinérantes :** autorise les utilisateurs à utiliser les données cellulaires en itinérance.
- **Comptes**
  - **Autoriser la connexion au compte Microsoft :** autorise l'appareil à utiliser un compte Microsoft pour l'authentification et les services de connexion sans relation avec la messagerie électronique.
  - **Autoriser les adresses e-mail non-Microsoft :** autoriser l'utilisateur à ajouter des comptes de messagerie autres que Microsoft.
- **Recherche :** Windows Phone uniquement.
  - **Autoriser utilisation des données de localisation :** autorise les recherches à utiliser le service de géolocalisation de l'appareil.
  - **Filtrer le contenu pour adultes :** autorise les contenus pour adultes. La valeur par défaut est **Désactivé**, ce qui signifie que les contenus pour adultes ne sont pas filtrés.
  - **Autoriser Bing Vision à stocker les images :** autorise Bing Vision à stocker les images capturées lors de recherches Bing Vision.
- **System**

  - **Autoriser les cartes de stockage :** autorise l'appareil à utiliser une carte de stockage.
  - **Télémétrie :** dans la liste, cliquez sur une option pour autoriser l'appareil à envoyer des informations de télémétrie ou pour le lui interdire. La valeur par défaut est **Autorisée**. Les autres options sont **Non autorisée** et **Autorisée, à l'exception des demandes de données secondaires**.
  - **Autoriser les services de localisation :** autorise les services de géolocalisation.
  - **Autoriser aperçu des versions internes :** autorise les utilisateurs à afficher un aperçu des versions internes de Microsoft.
- **Appareil photo :** Windows Desktop/Tablet uniquement
  - **Autoriser l'utilisation de l'appareil photo :** autorise les utilisateurs à utiliser l'appareil photo de leur appareil.
- **Bluetooth :** Windows Desktop/Tablet uniquement
  - **Autoriser le mode de découverte :** autoriser les périphériques Bluetooth à trouver le périphérique local.
  - **Nom de l'appareil local :** un nom pour le périphérique local.
- **Sécurité :** Windows Phone uniquement.
  - **Autoriser installation manuelle certificat racine :** autorise les utilisateurs à installer manuellement un certificat racine.
  - **Activer le chiffrement de l'appareil :** exige le chiffrement de l'appareil. N'oubliez pas qu'une fois le chiffrement activé sur un appareil, il ne peut pas être désactivé. La valeur par défaut est **Désactivé**.
  - **Autoriser le copier-coller :** autorise les utilisateurs à copier et coller des données sur leurs appareils.
  - **Autoriser la capture d'écran :** autorise les utilisateurs à créer des captures d'écran sur leurs appareils.
  - **Autoriser l'enregistrement vocal :** autorise les utilisateurs à utiliser l'enregistrement vocal sur leurs appareils.
  - **Autoriser l'enregistrement de fichiers Office :** autorise les utilisateurs à enregistrer des fichiers Office avec l'option Enregistrer sous.
  - **Autoriser notifications du centre de maintenance :** autorise l'affichage de notifications du centre de maintenance sur l'écran de verrouillage de l'appareil.
  - **Autoriser Cortana :** autorise les utilisateurs à accéder à Cortana, l'assistant personnel intelligent et navigateur de connaissances.
  - **Autoriser synchronisation des paramètres de l'appareil :** autorise les utilisateurs à synchroniser les paramètres entre des appareils Windows Phone 8.1 lors de l'itinérance.
- **Expérience :** Windows Desktop/Tablet uniquement
  - **Autoriser Cortana :** autorise les utilisateurs à accéder à Cortana, l'assistant personnel intelligent et navigateur de connaissances.
  - **Autoriser la détection d'appareils :** autoriser la détection réseau de l'appareil.

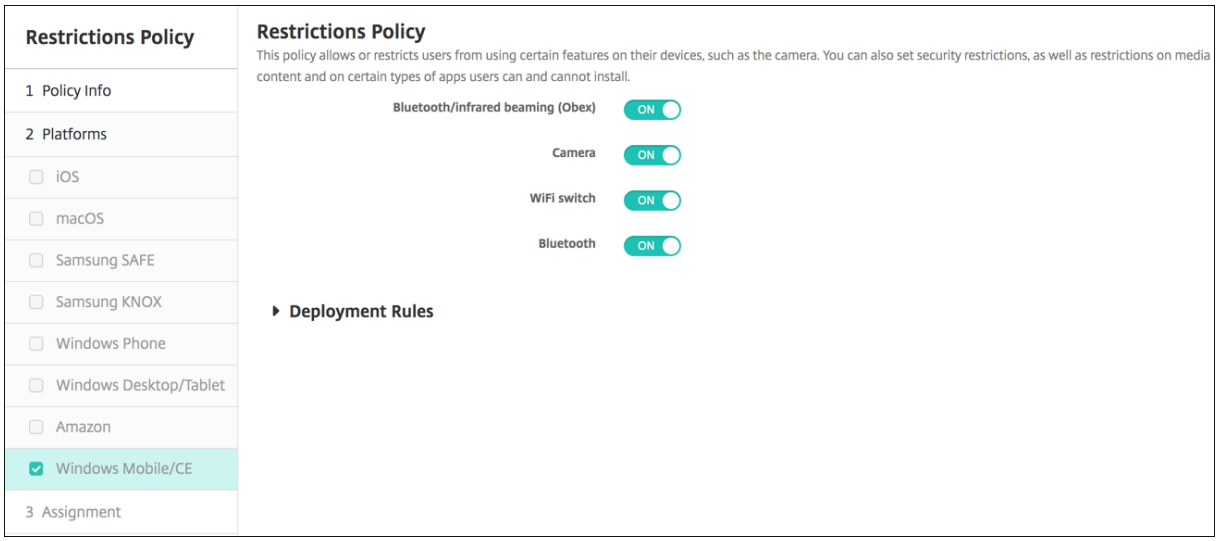
  - **Autoriser la désinscription MDM manuelle :** autorise les utilisateurs à désinscrire manuellement leurs appareils à partir de XenMobile MDM.
  - **Autoriser synchronisation des paramètres de l'appareil :** autorise les utilisateurs à synchroniser les paramètres entre des appareils Windows 10 et Windows 11 lors de l'itinérance.
- **Au dessus de l'écran de verrouillage :** Windows Desktop/Tablet uniquement
  - **Autoriser toasts :** autorise les notifications toast sur l'écran de verrouillage. Windows Desktop/Tablet uniquement
- **Applications**
  - **Autoriser l'accès au magasin :** autorise les utilisateurs à accéder au Microsoft Store. Windows Phone uniquement.
  - **Autoriser le déblocage :** autorise les utilisateurs à enregistrer leurs appareils auprès de Microsoft et à développer ou installer des applications qui ne se trouvent pas dans le magasin d'applications Windows Phone. Windows Phone uniquement.
  - **Autoriser l'accès au navigateur Web :** autorise la présence d'Internet Explorer sur l'appareil. Windows Phone uniquement.
  - **Autoriser la mise à jour automatique de l'App Store :** autorise les applications de l'App Store à se mettre à jour automatiquement. Windows Desktop/Tablet uniquement.
- **Confidentialité :** Windows Desktop/Tablet uniquement
  - **Autoriser personnalisation de la saisie :** permet au service de personnalisation de la saisie de s'exécuter afin d'améliorer les entrées prédictives telles que le stylet et le clavier tactile, en fonction de ce qu'un utilisateur tape.
- **Paramètres :** Windows Desktop/Tablet uniquement.
  - **Autoriser lecture automatique :** permet aux utilisateurs de modifier les paramètres de lecture automatique.
  - **Autoriser assistant Données :** permet aux utilisateurs de modifier les paramètres de l'assistant Données.
  - **Autoriser date et heure :** permet aux utilisateurs de modifier les paramètres de date et d'heure.
  - **Autoriser langue :** permet aux utilisateurs de modifier les paramètres de langue.
  - **Autoriser mise sous tension/mise en veille :** permet aux utilisateurs de modifier les paramètres de mise sous tension et de mise en veille.
  - **Autoriser région :** permet aux utilisateurs de modifier les paramètres de région.
  - **Autoriser options de connexion :** permet aux utilisateurs de modifier les paramètres de connexion.
  - **Autoriser espace de travail :** permet aux utilisateurs de modifier les paramètres de l'espace de travail.
  - **Autoriser votre compte :** permet aux utilisateurs de modifier les paramètres de compte.

Paramètres Amazon



- **Autoriser le contrôle du matériel**
  - **Réinitialisation d'usine :** autorise les utilisateurs à effectuer une réinitialisation d'usine sur leurs appareils.
  - **Profils :** autorise les utilisateurs à modifier le profil matériel sur leurs appareils.
- **Autoriser les applications**
  - **Applications non Amazon Appstore :** autorise les utilisateurs à installer des applications n'appartenant pas à l'Appstore Amazon sur leurs appareils.
  - **Réseaux sociaux :** autorise les utilisateurs à accéder à des réseaux sociaux à partir de leurs appareils.
- **Réseau**
  - **Bluetooth :** autorise les utilisateurs à utiliser Bluetooth.
  - **Commutateur Wi-Fi :** autorise les applications à modifier l'état de connectivité Wi-Fi.
  - **Paramètres Wi-Fi :** autorise les utilisateurs à modifier les paramètres Wi-Fi.
  - **Données cellulaires :** autorise les utilisateurs à utiliser leur connexion cellulaire pour les données.
  - **Données en itinérance :** autorise les utilisateurs à utiliser des données cellulaires en itinérance.
  - **Services de localisation :** autorise les utilisateurs à utiliser le GPS.
- **Actions USB :**
  - **Débogage :** autorise les utilisateurs à se connecter à un ordinateur via USB à des fins de débogage.

Paramètres Windows Mobile/CE



- **Bluetooth/infrarouge (Obex) :** active OBEX (protocole OBjectEXchange) via Bluetooth ou l'infrarouge pour échanger des données entre les appareils.
- **Appareil photo :** active l'appareil photo sur les appareils des utilisateurs.
- **Commutateur Wi-Fi :** autorise les utilisateurs à changer de réseaux Wi-Fi.
- **Bluetooth :** active le Bluetooth sur les appareils des utilisateurs.
- **Appareil photo :** active l'appareil photo sur les appareils des utilisateurs.
- **Commutateur Wi-Fi :** autorise les utilisateurs à changer de réseaux Wi-Fi.
- **Bluetooth :** active le Bluetooth sur les appareils des utilisateurs.

Stratégie d'itinérance

January 10, 2022

Vous pouvez ajouter une stratégie d'itinérance dans XenMobile afin d'activer les services de voix et de données en itinérance sur des appareils iOS et Windows Mobile/CE. Lorsque l'itinérance de la voix est désactivée, l'itinérance des données est automatiquement désactivée. Pour iOS, cette stratégie est uniquement disponible sur les appareils iOS 5.0 et versions ultérieures.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Désactiver l'itinérance de la voix :** sélectionnez cette option pour désactiver l'itinérance vocale. Lorsque cette option est activée, l'itinérance des données est automatiquement désac-

tivée. La valeur par défaut est **Désactivé**, ce qui active l'itinérance de la voix.
- **Désactiver l'itinérance des données :** sélectionnez cette option pour désactiver l'itinérance des données. Cette option est disponible uniquement lorsque l'itinérance de la voix est activée. La valeur par défaut est **Désactivé**, ce qui active l'itinérance des données.

Paramètres Windows Mobile/CE

- **En itinérance**
  - **Utiliser une connexion à la demande seulement :** l'appareil ne se connecte à XenMobile que si les utilisateurs déclenchent manuellement la connexion sur leurs appareils, ou si une application mobile requiert une connexion forcée (tel qu'un e-mail de push si le serveur Exchange Server a été défini en conséquence). Notez que cette option désactive temporairement la stratégie de planification de connexion de l'appareil par défaut.
  - **Bloquer toutes les connexions cellulaires sauf celles gérées par XenMobile :** sauf pour le trafic de données officiellement déclaré dans un tunnel applicatif XenMobile ou autres tâches de gestion de l'appareil XenMobile, aucune autre donnée ne sera envoyée ou reçue par l'appareil. Par exemple, cette option désactivera toutes les connexions à Internet via le navigateur Web de l'appareil.
  - **Bloquer toutes les connexions de cellulaires gérées par XenMobile :** toutes les données d'application passant par un tunnel XenMobile sont bloquées (y compris XenMobile Remote Support). Le trafic de données purement lié à la gestion des appareils, cependant, n'est pas bloqué.
  - **Bloquer toutes les connexions cellulaires à XenMobile :** dans ce cas, jusqu'à ce que l'appareil soit reconnecté via USB, sans fil ou son réseau cellulaire d'opérateur mobile par défaut, aucun trafic n'est autorisé entre l'appareil et XenMobile.
- **En itinérance nationale**
  - **Ignorer l'itinérance nationale :** aucune donnée n'est bloquée lorsque les utilisateurs sont en itinérance nationale.

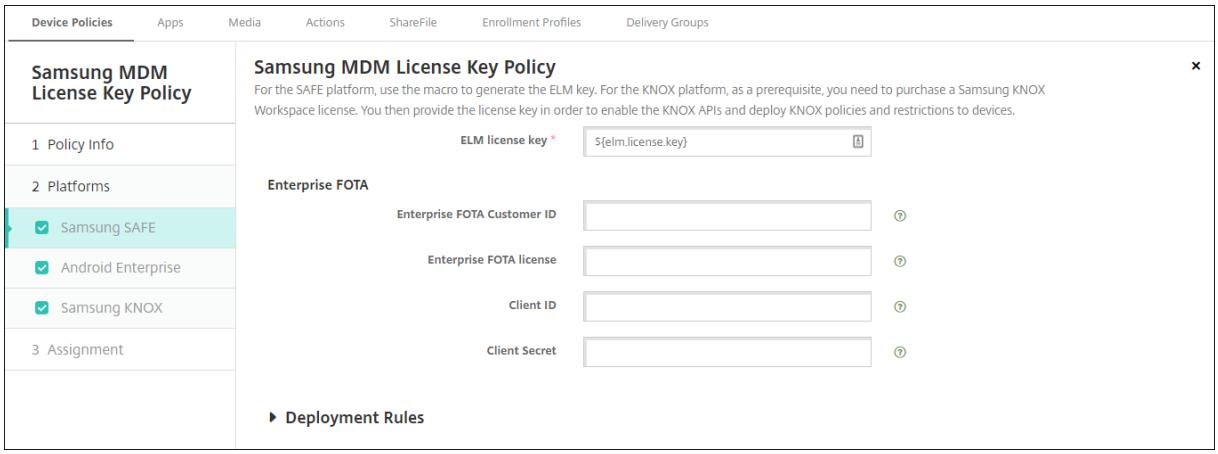
Stratégie de clé de licence MDM Samsung

January 10, 2022

Spécifie la clé Samsung ELM (Enterprise License Management) intégrée que vous devez déployer sur un appareil avant de pouvoir déployer des stratégies et restrictions SAFE. XenMobile prend également en charge le service E-FOTA (Firmware Over-The-Air) Samsung Enterprise. XenMobile prend en charge et étend les stratégies Samsung for Enterprise (SAFE) et Samsung KNOX.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Samsung SAFE



- **Clé de licence ELM :** XenMobile remplit ce champ à l'aide de la macro qui génère la clé de licence ELM. Si le champ est vide, entrez la macro ${elm.license.key}.

Configurer les paramètres pour Samsung E-FOTA

Samsung Enterprise FOTA (E-FOTA) vous permet de déterminer quand les appareils sont mis à jour et la version de micrologiciel à utiliser. E-FOTA vous permet de tester les mises à jour avant de les déployer, afin de vous assurer que les mises à jour sont compatibles avec vos applications. Vous pouvez forcer les appareils à se mettre à jour avec la dernière version de micrologiciel disponible, sans nécessiter d'interaction de la part de l'utilisateur.

Samsung prend en charge E-FOTA pour les appareils Samsung Knox 2.7.1 (version minimale) qui exécutent un micrologiciel autorisé.

XenMobile prend en charge l'ajout d'appareils de la console XenMobile à Knox E-FOTA One. Pour plus d'informations sur l'exportation d'une liste d'appareils à partir de XenMobile, consultez Exporter la liste des appareils. Pour plus d'informations sur l'ajout d'un appareil à Knox E-FOTA One, consultez la documentation Samsung.

XenMobile ne prend pas en charge la solution Knox E-FOTA sur MDM.

Pour configurer une stratégie E-FOTA :

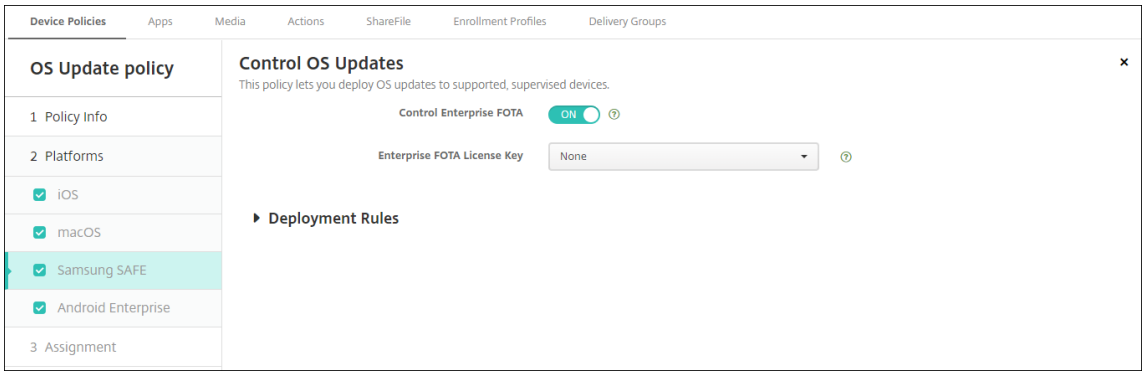
1. Créez une stratégie de clé de licence MDM Samsung avec les clés et les informations de licence que Samsung vous a fournies. XenMobile Server valide puis enregistre les informations. Si XenMobile détecte un problème E-FOTA, un message d'erreur s'affiche pour indiquer le problème. Utilisez le code fourni pour résoudre le problème. Pour de plus amples informations, consultez Guides du développeur.

   Entrez la **Clé de licence ELM :** XenMobile remplit ce champ à l'aide de la macro qui génère la clé de licence ELM. Si le champ est vide, entrez la macro ${elm.license.key}.

Tapez les informations suivantes fournies par Samsung lors de l'achat d'un pack E-FOTA :

- **ID client d'Enterprise FOTA**
- **Licence Enterprise FOTA**
- **ID client**
- **Clé secrète client**

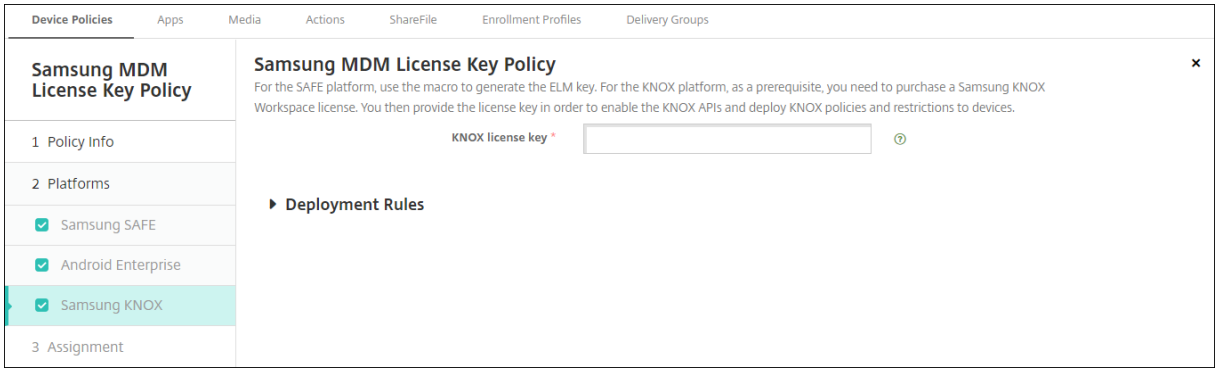
2. Vous pouvez également créer une stratégie Contrôler mise à jour d'OS.



- **Activer Enterprise FOTA :** définissez sur **Activé**.
- **Clé de licence d'Enterprise FOTA :** sélectionnez le nom de la stratégie de clé de licence MDM Samsung que vous avez créée à l'étape 1.

3. Déployez la stratégie Contrôler mise à jour d'OS sur Secure Hub.

Paramètres Android Enterprise et Samsung KNOX



- **Clé de licence KNOX :** entrez la clé de licence KNOX que vous avez obtenue auprès de Samsung.

Stratégie de pare-feu Samsung SAFE

January 10, 2022

Cette stratégie vous permet de configurer les paramètres de pare-feu pour les appareils Samsung. Vous pouvez entrer les adresses IP, les ports et les noms d'hôte que vous souhaitez autoriser ou bloquer. Vous pouvez également configurer les paramètres de redirection de proxy et de proxy.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Samsung SAFE

- **Autoriser/refuser les hôtes :** pour chaque hôte pour lequel vous souhaitez autoriser ou refuser l'accès, cliquez sur **Ajouter** et procédez comme suit :
  - **Nom d'hôte/Plage d'adresses IP :** nom d'hôte ou plage d'adresses IP pour le site concerné.
  - **Port/Plage de ports :** port ou plage de ports.
  - **Filtre de règle d'autorisation/refus :** sélectionnez la **liste blanche** pour autoriser l'accès ou cliquez sur la **liste noire** pour refuser l'accès au site.

    > **Remarque :**
    > La console XenMobile Server utilise les termes « liste noire » et « liste blanche ». Ces termes seront modifiés dans une prochaine version et les termes « liste de blocage » et « liste d'autorisation » les remplaceront.
- **Configuration de redirection :** pour chaque serveur proxy que vous souhaitez configurer, cliquez sur **Ajouter** et procédez comme suit :
  - **Nom d'hôte/adresse IP :** nom d'hôte ou plage d'adresses IP pour la redirection proxy.
  - **Port/Plage de ports :** port ou plage de ports pour la redirection proxy.
  - **IP proxy :** adresse IP du proxy pour la redirection proxy.
  - **Port proxy :** port du proxy pour la redirection proxy.
- **Configuration du proxy**
  - **IP Proxy :** adresse IP du serveur proxy.
  - **Port :** port du serveur proxy.

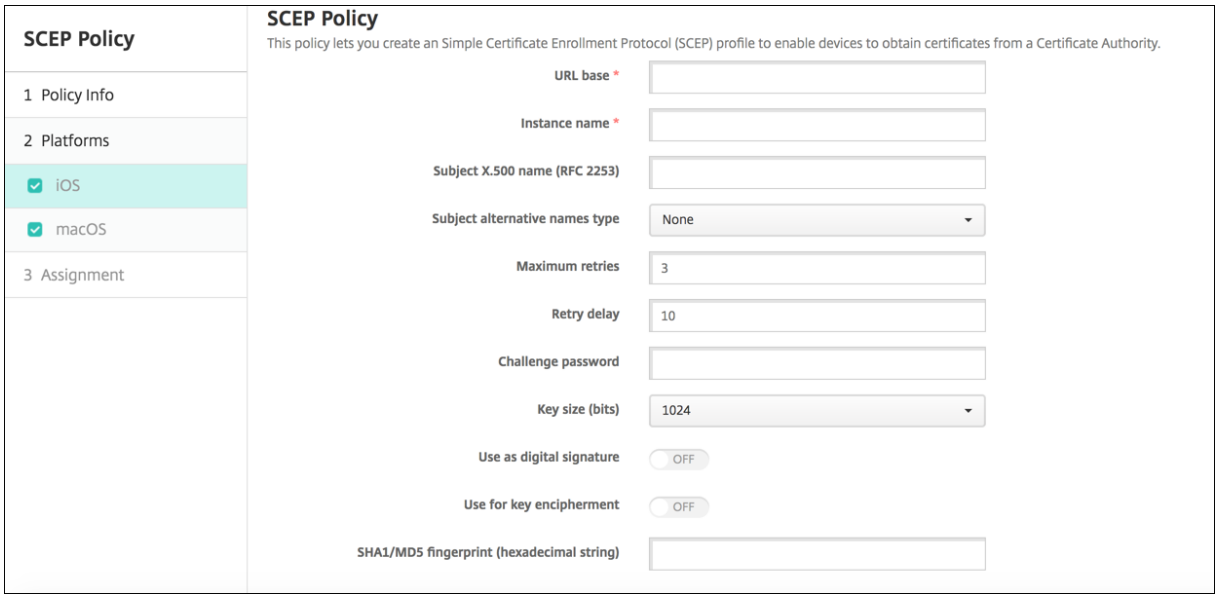
Stratégie SCEP

January 10, 2022

Cette stratégie vous permet de configurer des appareils iOS et macOS afin de récupérer un certificat à l'aide du protocole d'inscription du certificat simple (SCEP) à partir d'un serveur SCEP externe. Si vous souhaitez délivrer un certificat sur l'appareil à l'aide du protocole SCEP à partir d'une PKI connectée à XenMobile, vous devez créer une entité PKI et un fournisseur PKI en mode distribué. Pour plus d'informations, veuillez consulter la section Entités PKI.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

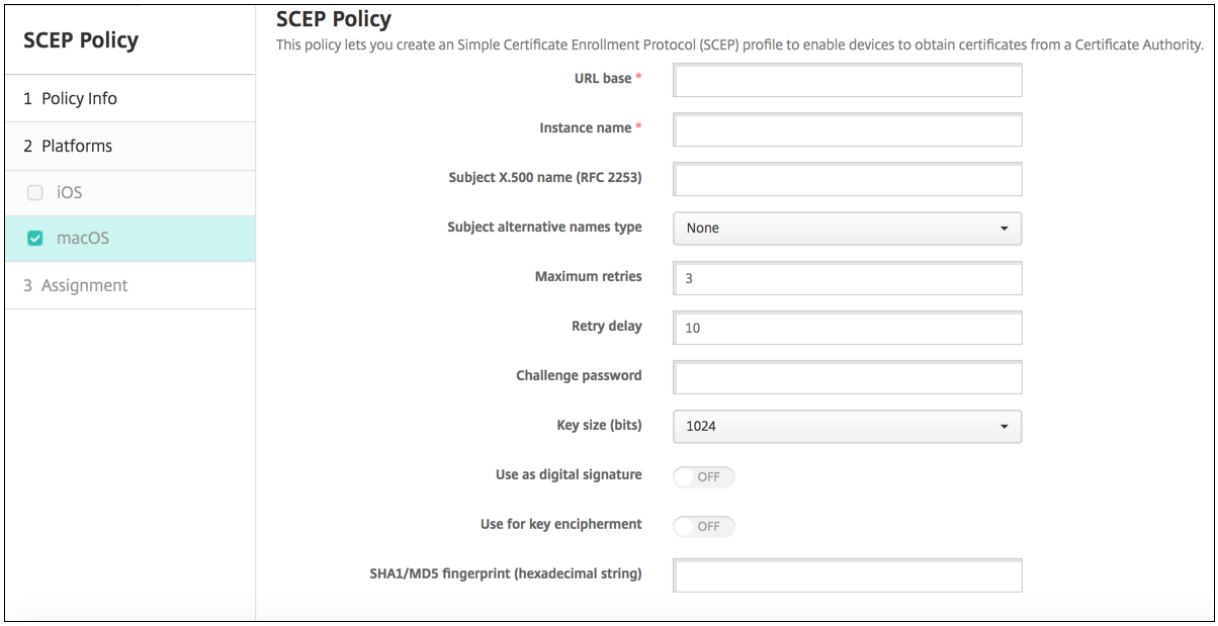
Paramètres iOS



- **URL de base :** entrez l'adresse du serveur SCEP afin de définir où les demandes SCEP sont envoyées, par HTTP ou HTTPS. La clé privée n'est pas envoyée avec la demande de signature de certificat (CSR), il est donc possible d'envoyer la demande non chiffrée sans danger. Si, toutefois le mot de passe à usage unique est autorisé à être réutilisé, vous devez utiliser le protocole HTTPS pour protéger le mot de passe. Cette étape est requise.
- **Nom d'instance :** entrez une chaîne reconnue par le serveur SCEP. Par exemple, il peut s'agir d'un nom de domaine comme exemple.org. Si une autorité de certification dispose de plusieurs certificats d'autorité de certification, vous pouvez utiliser ce champ pour différencier le domaine requis. Cette étape est requise.
- **Nom X.500 du sujet (RFC 2253) :** entrez la représentation d'un nom X.500 représentée sous forme de tableau d'identificateurs d'objets (OID) et de valeurs. Par exemple, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, qui correspond à : [[[“C”, “US”]], [[“O”, “Apple Inc.”]], …, [[“1.2.5.3”, “bar”]]]. Les OID peuvent être représentés en tant que nombres en pointillé, avec des raccourcis pour le pays (C), la ville (L), l'état (ST), l'organisation (O), l'unité d'organisation (OU) et le nom commun (CN).
- **Type de noms de sujet alternatifs :** sélectionnez un type de nom alternatif dans la liste. La stratégie SCEP permet de spécifier un type de nom alternatif facultatif qui fournit les valeurs requises par l'autorité de certification pour l'émission d'un certificat. Vous pouvez spécifier **Aucun**, **Nom RFC 822**, **Nom DNS** ou **URI**.

- **Nombre maximal de tentatives :** entrez le nombre de fois qu'un appareil doit réessayer lorsque le serveur SCEP envoie une réponse PENDING. La valeur par défaut est **3**.
- **Délai entre chaque tentative :** entrez le nombre de secondes entre les tentatives. La première tentative est effectuée sans délai. La valeur par défaut est **10**.
- **Vérifier le mot de passe :** entrez un secret pré-partagé.
- **Taille de la clé (bits) :** sélectionnez **2048** ou une taille en bits plus élevée pour la clé.
- **Utiliser une signature numérique :** spécifiez si vous souhaitez que le certificat soit utilisé en tant que signature numérique. Si le certificat est utilisé pour vérifier une signature numérique, comme vérifier si un certificat a été émis par une autorité de certification, le serveur SCEP vérifie que le certificat peut être utilisé de cette façon avant d'utiliser la clé publique pour déchiffrer le hachage.
- **Utiliser pour le chiffrement des clés :** spécifiez si vous souhaitez que le certificat soit utilisé pour le chiffrement des clés. Si un serveur utilise la clé publique dans un certificat fourni par un client pour vérifier qu'une partie des données a été chiffrée à l'aide de la clé privée, le serveur vérifie d'abord si le certificat peut être utilisé pour le chiffrement de la clé. Sinon, l'opération échoue.
- **Empreinte digitale SHA1/MD5 (chaîne hexadécimale) :** si votre Autorité de certification utilise le protocole HTTP, utilisez ce champ pour fournir l'empreinte digitale du certificat de la CA, que l'appareil utilise pour vérifier l'authenticité de la réponse de l'autorité de certification au cours de l'inscription. Vous pouvez entrer une empreinte digitale MD5 ou SHA1, ou vous pouvez sélectionner un certificat pour importer sa signature.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres macOS



- **URL de base :** entrez l'adresse du serveur SCEP afin de définir où les demandes SCEP sont envoyées, par HTTP ou HTTPS. La clé privée n'est pas envoyée avec la demande de signature de certificat (CSR), il est donc possible d'envoyer la demande non chiffrée sans danger. Si, toutefois le mot de passe à usage unique est autorisé à être réutilisé, vous devez utiliser le protocole HTTPS pour protéger le mot de passe. Cette étape est requise.
- **Nom d'instance :** entrez une chaîne reconnue par le serveur SCEP. Par exemple, il peut s'agir d'un nom de domaine comme exemple.org. Si une autorité de certification dispose de plusieurs certificats d'autorité de certification, vous pouvez utiliser ce champ pour différencier le domaine requis. Cette étape est requise.
- **Nom X.500 du sujet (RFC 2253) :** entrez la représentation d'un nom X.500 représentée sous forme de tableau d'identificateurs d'objets (OID) et de valeurs. Par exemple, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, qui correspond à : [[["C", "US"]], [["O", "Apple Inc."]], …, [["1.2.5.3", "bar"]]]. Les OID peuvent être représentés en tant que nombres en pointillé, avec des raccourcis pour le pays (C), la ville (L), l'état (ST), l'organisation (O), l'unité d'organisation (OU) et le nom commun (CN).
- **Type de noms de sujet alternatifs :** sélectionnez un type de nom alternatif dans la liste. La stratégie SCEP permet de spécifier un type de nom alternatif facultatif qui fournit les valeurs requises par l'autorité de certification pour l'émission d'un certificat. Vous pouvez spécifier **Aucun**, **Nom RFC 822**, **Nom DNS** ou **URI**.
- **Nombre maximal de tentatives :** entrez le nombre de fois qu'un appareil doit réessayer lorsque le serveur SCEP envoie une réponse PENDING. La valeur par défaut est **3**.
- **Délai entre chaque tentative :** entrez le nombre de secondes entre les tentatives. La première

tentative est effectuée sans délai. La valeur par défaut est **10**.

- **Vérifier le mot de passe :** entrez un secret pré-partagé.
- **Taille de la clé (bits) :** sélectionnez **2048** ou une taille en bits plus élevée pour la clé.
- **Utiliser une signature numérique :** spécifiez si vous souhaitez que le certificat soit utilisé en tant que signature numérique. Si le certificat est utilisé pour vérifier une signature numérique, comme vérifier si un certificat a été émis par une autorité de certification, le serveur SCEP vérifie que le certificat peut être utilisé de cette façon avant d'utiliser la clé publique pour déchiffrer le hachage.
- **Utiliser pour le chiffrement des clés :** spécifiez si vous souhaitez que le certificat soit utilisé pour le chiffrement des clés. Si un serveur utilise la clé publique dans un certificat fourni par un client pour vérifier qu'une partie des données a été chiffrée à l'aide de la clé privée, le serveur vérifie d'abord si le certificat peut être utilisé pour le chiffrement de la clé. Sinon, l'opération échoue.
- **Empreinte digitale SHA1/MD5 (chaîne hexadécimale) :** si votre Autorité de certification utilise le protocole HTTP, utilisez ce champ pour fournir l'empreinte digitale du certificat de la CA, que l'appareil utilise pour vérifier l'authenticité de la réponse de l'autorité de certification au cours de l'inscription. Vous pouvez entrer une empreinte digitale MD5 ou SHA1, ou vous pouvez sélectionner un certificat pour importer sa signature.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

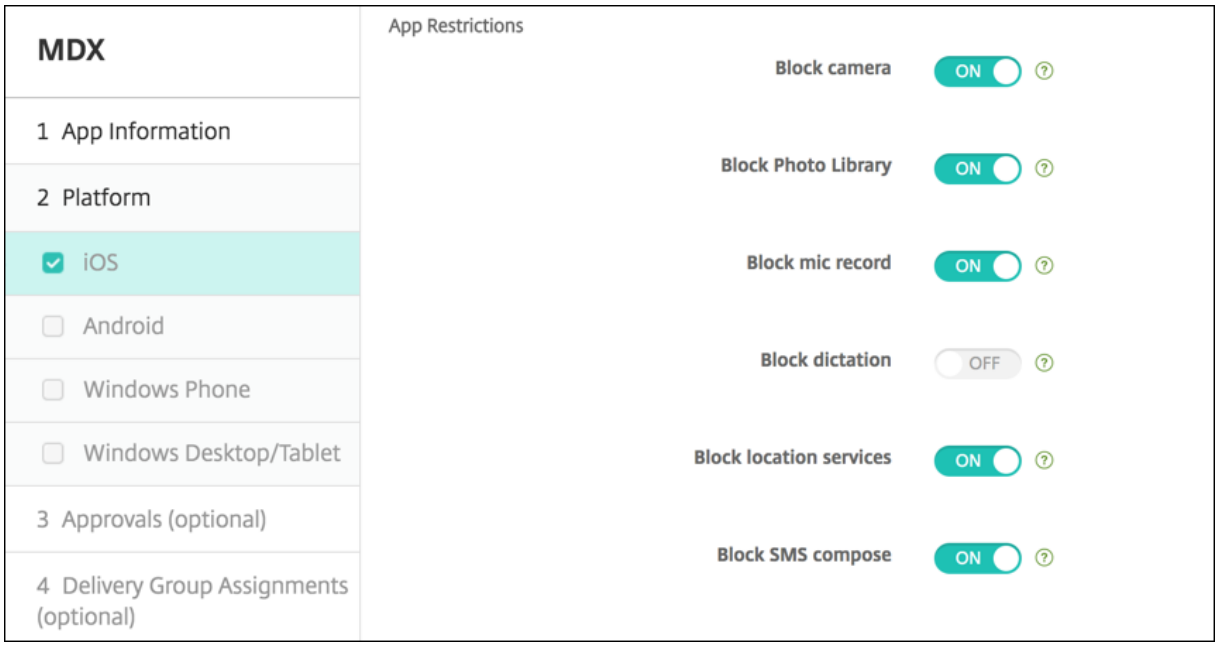
Stratégies de dictée et Siri

January 10, 2022

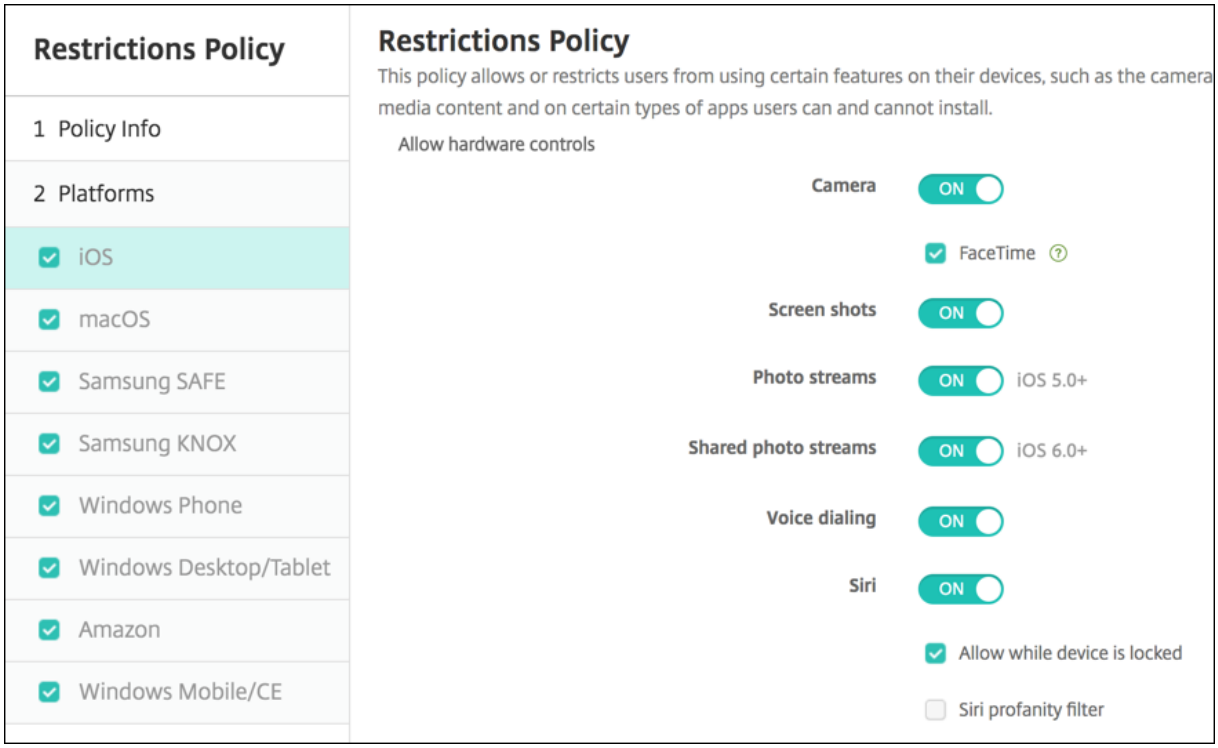
Lorsque les utilisateurs posent une question à Siri ou qu'ils dictent du texte sur des appareils iOS gérés, Apple collecte les données vocales à des fins d'amélioration de Siri. Les données vocales transitent via les services de cloud d'Apple et par conséquent elles existent en dehors du conteneur XenMobile sécurisé. Le texte qui résulte de la dictée vocale reste toutefois dans le conteneur.

XenMobile vous permet de bloquer Siri et les services de dictée, selon vos besoins en matière de sécurité.

Dans les déploiements MAM, la stratégie **Bloquer la dictée** est **activée** par défaut pour chaque application, ce qui désactive le micro de l'appareil. Définissez la valeur sur **Désactivé** si vous souhaitez autoriser la dictée. Vous pouvez trouver la stratégie dans la console XenMobile sous **Configurer > Applications**. Sélectionnez l'application, cliquez sur **Modifier**, puis cliquez sur **iOS**.



Dans les déploiements MDM, vous pouvez également désactiver Siri avec la stratégie Siri sous **Configurer > Stratégies d'appareil**. L'utilisation de Siri est autorisée par défaut.



Quelques points à considérer lorsque vous choisissez d'autoriser Siri et la dictée :

- D'après les informations rendues publiques par Apple, Apple conserve les données des clips vocaux de la dictée et de Siri pendant un maximum de deux années. Pour représenter l'utilisateur, un nombre aléatoire est attribué aux données et les fichiers vocaux sont associés à ce nombre aléatoire. Pour plus d'informations, consultez l'article Wired suivant : Apple reveals how long Siri keeps your data.
- Vous pouvez vérifier la déclaration de confidentialité d'Apple en accédant à **Réglages > Général > Claviers** sur un appareil iOS et en touchant le lien sous **Activer dictée**.

Stratégie de compte SSO

January 10, 2022

Vous créez des comptes SSO dans XenMobile pour permettre aux utilisateurs de s'authentifier une seule fois pour accéder à XenMobile et à vos ressources d'entreprise internes à partir de différentes applications. Les utilisateurs n'ont pas à stocker d'informations d'identification sur l'appareil. Les informations d'identification utilisateur d'entreprise du compte SSO sont utilisées pour toutes les applications, y compris les applications provenant de l'App Store. Cette stratégie est conçue pour fonctionner avec l'authentification Kerberos.

Cette stratégie s'applique uniquement à iOS 7.0 et versions supérieures.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Nom du compte :** entrez le nom du compte SSO Kerberos qui s'affiche sur les appareils des utilisateurs. Ce champ est obligatoire.
- **Nom principal Kerberos :** entrez le nom principal Kerberos. Ce champ est obligatoire.
- **Infos d'identification de l'identité (infos d'identification magasin de clés ou PKI) :** dans la liste, cliquez sur des infos d'identification de l'identité qui peuvent être utilisées pour renouveler les infos d'identification Kerberos sans intervention de l'utilisateur.
- **Domaine Kerberos :** entrez le domaine Kerberos pour cette stratégie. Il s'agit généralement de votre nom de domaine en lettres majuscules (par exemple, EXAMPLE.COM). Ce champ est obligatoire.
- **URL autorisées :** pour chaque adresse URL pour laquelle vous souhaitez demander l'authentification unique (SSO), cliquez sur **Ajouter**, puis procédez comme suit :
  - **URL autorisée :** entrez une adresse URL pour laquelle vous souhaitez demander l'authentification unique (SSO) lorsqu'un utilisateur visite l'URL à partir d'un appareil iOS. Par exemple, lorsqu'un utilisateur tente d'accéder à un site dans Safari et que le site Web lance une demande d'authentification Kerberos, si ce site ne figure pas dans la liste des URL, l'appareil iOS ne tentera pas une authentification unique en fournissant le jeton Kerberos qui a été mis en cache sur l'appareil lors d'une précédente ouverture de session Kerberos. La correspondance doit être exacte sur la partie hôte de l'URL. Par exemple, `https://shopping.apple.com` est valide, mais `https://*.apple.com` ne l'est pas. De même, si Kerberos n'est pas activé en fonction d'une correspondance à l'hôte, l'URL utilise un appel HTTP standard. Cela peut signifier presque tout, y compris un défi de mot de passe standard ou une erreur HTTP si l'URL est uniquement configurée pour l'authentification unique (SSO) à l'aide de Kerberos.
  - Cliquez sur **Ajouter** pour ajouter l'URL, ou cliquez sur **Annuler** pour annuler l'ajout de l'URL.
- **Identifiants application :** pour chaque application autorisée à utiliser cette connexion, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Identifiant app :** entrez un identifiant d'application pour une application qui est autorisée à utiliser cette connexion. si vous n'ajoutez aucun identifiant d'application, cette connexion correspond à **tous** les identifiants d'application.
  - Cliquez sur **Ajouter** pour ajouter l'identifiant d'application, ou cliquez sur **Annuler** pour annuler l'ajout de l'identifiant d'application.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppres-**

sion (en heures).

* **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
* **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Stratégie de chiffrement du stockage

January 10, 2022

Vous pouvez créer des stratégies de chiffrement du stockage dans XenMobile pour chiffrer le stockage interne et externe, et, en fonction de l'appareil, pour empêcher les utilisateurs d'utiliser une carte de stockage sur leurs appareils.

Vous pouvez créer des stratégies pour les appareils Samsung SAFE et Windows Phone. Chaque plateforme requiert des valeurs différentes, qui sont décrites en détail dans cet article.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Conditions préalables

Pour les appareils Samsung SAFE, vérifiez que les conditions suivantes soient remplies avant de configurer cette stratégie :

- Définissez l'option de verrouillage d'écran sur les appareils des utilisateurs.
- Branchez les appareils des utilisateurs et chargez-les à au moins 80%.
- Assurez-vous que l'appareil exige un mot de passe contenant des chiffres et des lettres ou des symboles.

Configurer les paramètres pour Samsung SAFE

- **Chiffrer le stockage interne :** sélectionnez cette option pour chiffrer le stockage interne sur les appareils des utilisateurs. Le stockage interne inclut la mémoire de l'appareil et le stockage interne. La valeur par défaut est **Activé**.
- **Chiffrer le stockage externe :** sélectionnez cette option pour chiffrer le stockage externe sur les appareils des utilisateurs. La valeur par défaut est **Activé**.

Paramètres Windows Phone

- **Activer le cryptage de l'appareil :** sélectionnez cette option pour chiffrer les appareils des utilisateurs. La valeur par défaut est **Désactivé**.
- **Désactiver la carte de stockage :** sélectionnez cette option pour empêcher les utilisateurs d'utiliser une carte de stockage sur leurs appareils. La valeur par défaut est **Désactivé**.

Stratégie de magasin

January 10, 2022

Vous pouvez créer une stratégie dans XenMobile afin de spécifier si les appareils iOS, Android ou Windows Tablet affichent un clip Web XenMobile Store sur l'écran d'accueil des appareils.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres de plate-forme

Pour chaque plate-forme que vous configurez, sélectionnez si un clip Web XenMobile Store apparaît sur les appareils des utilisateurs. La valeur par défaut est **Activé**.

Stratégie d'abonnements calendriers

January 10, 2022

Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin d'ajouter un abonnement calendrier à la liste des calendriers sur les appareils iOS. La liste des calendriers publics auxquels vous pouvez vous abonner est disponible sur www.apple.com/downloads/macosx/calendars.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Conditions préalables

Vous devez être abonné à un calendrier avant de pouvoir l'ajouter à la liste des abonnements calendriers sur les appareils des utilisateurs.

Paramètres iOS

- **Description :** entrez une description pour le calendrier. Ce champ est obligatoire.
- **URL :** entrez l'URL du calendrier. Vous pouvez entrer une URL `webcal://` ou un lien `https://` vers un fichier iCalendar (.ics). Ce champ est obligatoire.
- **Nom d'utilisateur :** entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe :** entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au calendrier. La valeur par défaut est **Désactivé**.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Stratégie termes et conditions

January 10, 2022

Vous créez des stratégies de termes et conditions dans XenMobile lorsque vous souhaitez que les utilisateurs acceptent les stratégies spécifiques à votre entreprise qui régissent les connexions au réseau d'entreprise. Lorsque les utilisateurs inscrivent leurs appareils auprès de XenMobile, ils voient s'afficher les termes et conditions et doivent les accepter pour inscrire leurs appareils. Le refus des termes et conditions annule le processus d'inscription.

Vous pouvez créer différentes stratégies pour les termes et conditions dans différentes langues si votre société dispose d'utilisateurs internationaux pour leur permettre d'accepter les termes et conditions dans leur langue maternelle. Vous devez fournir un fichier pour chaque combinaison de plate-forme et de langue que vous souhaitez déployer. Pour les appareils Android et iOS, vous devez fournir des fichiers PDF. Pour les appareils Windows, vous devez fournir des fichiers texte (.txt) et les fichiers image connexes.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS et Android

- **Fichier à importer :** sélectionnez le fichier de termes et conditions à importer en cliquant sur **Parcourir**, puis accédez à l'emplacement du fichier.
- **Termes et conditions par défaut :** sélectionnez cette option pour désigner ce fichier comme le document par défaut pour les utilisateurs qui sont membres de plusieurs groupes avec différents termes et conditions. La valeur par défaut est **Désactivé**.

Paramètres Windows Phone et Windows Tablet

- **Fichier à importer :** sélectionnez le fichier de termes et conditions à importer en cliquant sur **Parcourir**, puis accédez à l'emplacement du fichier.
- **Image :** sélectionnez le fichier à importer en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
- **Termes et conditions par défaut :** sélectionnez cette option pour désigner ce fichier comme le document par défaut pour les utilisateurs qui sont membres de plusieurs groupes avec différents termes et conditions. La valeur par défaut est **Désactivé**.

Stratégie VPN

January 10, 2022

La stratégie VPN configure les paramètres de réseau privé virtuel (VPN) permettant aux appareils de se connecter de manière sécurisée aux ressources d'entreprise. Vous pouvez configurer la stratégie VPN pour les plates-formes suivantes. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans cet article.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Configuration requise pour les réseaux Per App VPN

Vous configurez la fonctionnalité Per App VPN pour les plates-formes suivantes via des stratégies VPN :

- iOS
- macOS
- Android (ancien administrateur de l'appareil)
- Samsung SAFE
- Samsung Knox

Pour configurer des VPN pour les appareils Android Enterprise, créez une stratégie Configurations gérées par Android Entreprise pour l'application Citrix SSO. Consultez la section Configurer les profils VPN pour Android Enterprise.

Des options Per App VPN sont disponibles pour certains types de connexion. Le tableau suivant indique quand les options Per App VPN sont disponibles.

Plateforme	Type de connexion	Remarque
iOS	Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix SSO ou SSL personnalisé	
macOS	Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA ou SSL personnalisé	
Android (ancien administrateur de l'appareil)	Citrix SSO	
Samsung SAFE	IPSEC, SSL	Type de VPN défini sur **Générique**
Samsung Knox	IPSEC, SSL	Type de VPN défini sur **Générique**

Pour créer une stratégie Per App VPN pour les appareils iOS et Android (ancien administrateur de l'appareil) à l'aide de l'application Citrix SSO, vous devez effectuer des étapes supplémentaires, en plus de la configuration de stratégie VPN. En outre, vous devez vérifier que les conditions préalables suivantes sont remplies :

- Passerelle Citrix Gateway locale
- Les applications suivantes sont installées sur l'appareil :
  - Citrix SSO
  - Citrix Secure Hub

Voici un workflow général pour configurer une stratégie Per App VPN pour les appareils iOS et Android à l'aide de l'application Citrix SSO :

1. Configurez la stratégie VPN selon les instructions de cet article.
   - Pour *iOS*, consultez la section Configurer le protocole Citrix SSO pour iOS. Après avoir configuré le protocole Citrix SSO pour iOS via une stratégie VPN, vous devez également créer

une stratégie d'attributs d'application pour associer une application à la stratégie Per App VPN. Pour de plus amples informations, consultez la section Configurer une stratégie Per App VPN.

  - Pour le champ **Type d'authentification pour la connexion**, si vous sélectionnez **Certificat**, vous devez d'abord configurer l'authentification basée sur les certificats pour Endpoint Management. Consultez la section Authentification certificat client ou certificat + domaine.

- Pour *Android (administration anciens appareils)*, consultez la section Configurer le protocole Citrix SSO pour Android.
  - Pour le champ **Type d'authentification pour la connexion**, si vous sélectionnez **Certificat** ou **Mot de passe et certificat**, vous devez d'abord configurer l'authentification basée sur les certificats pour Endpoint Management. Consultez la section Authentification certificat client ou certificat + domaine.

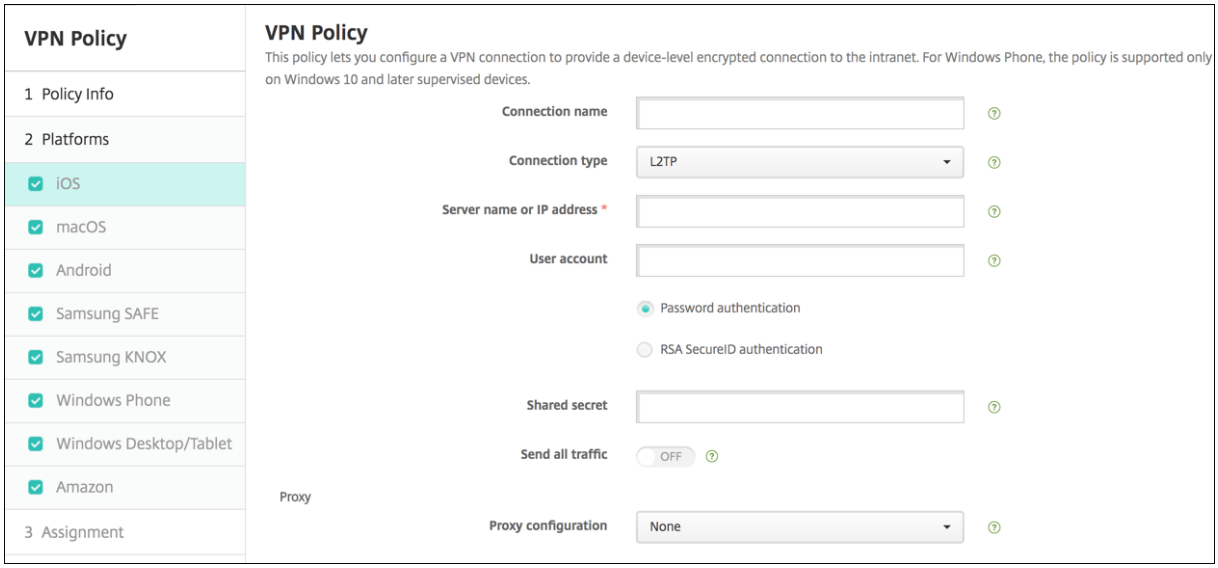
2. Configurez Citrix ADC pour accepter le trafic provenant du réseau Per App VPN. Pour de plus amples informations, consultez la section Full VPN setup on Citrix Gateway.

Paramètres iOS

Pour préparer les mises à niveau des appareils vers iOS 12 :

le type de connexion VPN Citrix dans la stratégie VPN pour iOS ne prend pas en charge iOS 12. Effectuez ces étapes pour supprimer votre stratégie VPN existante et créer une stratégie VPN avec le type de connexion Citrix SSO :

1. Supprimez votre stratégie VPN pour iOS.
2. Ajoutez une stratégie VPN pour iOS. Paramètres importants :
   - **Connection type** = **Citrix SSO**
   - **Enable per-app VPN** = **On**
   - **Provider type** = **Packet tunnel**
3. Ajoutez une stratégie d'attributs d'application pour iOS. Sous **Identifiant Per App VPN**, sélectionnez **iOS_VPN**.



- **Nom de la connexion :** entrez un nom pour la connexion.
- **Type de connexion :** dans la liste, sélectionnez le protocole à utiliser pour cette connexion. La valeur par défaut est **L2TP**.
  - **L2TP :** Layer 2 Tunneling Protocol avec authentification par clé pré-partagée.
  - **PPTP :** protocole PPTP.
  - **IPSec :** votre connexion VPN d'entreprise.
  - **Cisco Legacy AnyConnect :** ce type de connexion requiert que le client Cisco Legacy AnyConnect VPN soit installé sur la machine utilisateur. Cisco élimine progressivement le client Cisco Legacy AnyConnect, basé sur une infrastructure VPN désormais obsolète. Pour de plus amples informations, consultez l'article https://support.citrix.com/article/CTX227708 de l'assistance Citrix.
    Pour utiliser le client Cisco AnyConnect actuel, utilisez un **Type de connexion** de **SSL personnalisé**. Pour plus d'informations sur les paramètres requis, consultez « Configurer le protocole SSL personnalisé » dans cette section.
  - **Juniper SSL :** client Juniper Networks SSL VPN.
  - **F5 SSL :** client F5 Networks SSL VPN.
  - **SonicWALL Mobile Connect :** client VPN Dell unifié pour iOS.
  - **Aruba VIA :** client Aruba Networks Virtual Internet Access.
  - **IKEv2 (iOS uniquement) :** Internet Key Exchange version 2 pour iOS uniquement.
  - **AlwaysOn IKEv2 :** accès Always On à l'aide de IKEv2.
  - **Double configuration AlwaysOn IKEv2 :** accès Always On à l'aide de la double configuration iKEv2.
  - **Citrix SSO:** Client Citrix SSO pour iOS 12 et versions ultérieures.
  - **SSL personnalisé :** Secure Sockets Layer personnalisé. Ce type de connexion est requis pour le client Cisco AnyConnect disposant d'un bundle ID **com.cisco.anyconnect**. Réglez l'option **Nom de la connexion** sur **Cisco AnyConnect**. Vous pouvez également déployer

la stratégie VPN et activer un filtre NAC (Network Access Control) pour les appareils iOS. Le filtre NAC bloque une connexion VPN pour les appareils sur lesquels des applications non conformes sont installées. La configuration nécessite des paramètres spécifiques pour la stratégie VPN d'iOS, comme décrit dans la section iOS suivante. Pour plus d'informations sur les autres paramètres requis pour activer le filtre NAC, voir Contrôle d'accès réseau.

Les sections suivantes répertorient les options de configuration pour chacun des types de connexion précédents.

Configurer le protocole L2TP pour iOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- Sélectionnez **Authentification par mot de passe** ou **Authentification RSA SecurID**.
- **Secret partagé :** entrez la clé de secret partagé IPsec.
- **Envoyer tout le trafic :** sélectionnez cette option pour envoyer tout le trafic via le VPN. La valeur par défaut est **Désactivé**.

Configurer le protocole PPTP pour iOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- Sélectionnez **Authentification par mot de passe** ou **Authentification RSA SecurID**.
- **Niveau de chiffrement :** dans la liste, sélectionnez un niveau de chiffrement. La valeur par défaut est **Aucun**.
  - **Aucun :** le chiffrement n'est pas utilisé.
  - **Automatique :** utilise le niveau de chiffrement le plus élevé pris en charge par le serveur.
  - **Maximum (128 bits) :** utilise toujours le cryptage 128 bits.
- **Envoyer tout le trafic :** sélectionnez cette option pour envoyer tout le trafic via le VPN. La valeur par défaut est **Désactivé**.

Configurer le protocole IPsec pour iOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Secret partagé** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Secret partagé**.
- Si vous sélectionnez **Secret partagé**, configurez les paramètres suivants :
  - **Nom du groupe :** entrez un nom de groupe (facultatif).
  - **Secret partagé :** entrez une clé de secret partagé (facultatif).

  - **Utiliser une authentification hybride :** indiquez si vous souhaitez utiliser l'authentification hybride. Avec l'authentification hybride, le serveur s'authentifie auprès du client, puis le client s'authentifie auprès du serveur. La valeur par défaut est **Désactivé**.
  - **Demander le mot de passe :** indiquez si les utilisateurs doivent être invités à entrer leur mot de passe lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
- Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
  - **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
  - **Exiger PIN à la connexion :** sélectionnez cette option pour demander aux utilisateurs d'entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
  - **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**.
- **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
- **Domaines safari :** cliquez sur **Ajouter** pour ajouter un nom de domaine Safari.

Configurer le protocole Cisco Legacy AnyConnect pour iOS

Pour passer du client Cisco Legacy AnyConnect au nouveau client Cisco AnyConnect, utilisez le protocole SSL personnalisé.

- **Identificateur de bundle de fournisseur :** pour le client Legacy AnyConnect, le bundle ID est com.cisco.anyconnect.gui.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Groupe :** entrez un nom de groupe (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations

d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.

* **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
* **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.

- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  - **Type de fournisseur :** indiquez si le VPN par application est fourni en tant que **Proxy d'application** ou **Tunnel de paquet**. La valeur par défaut est **Proxy d'application**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole SSL Juniper pour iOS

- **Identificateur de bundle de fournisseur :** si votre profil VPN par application contient l'identificateur de bundle d'une application avec plusieurs fournisseurs VPN du même type, spécifiez le fournisseur à utiliser ici.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Domaine :** entrez un nom de domaine (facultatif).
- **Rôle :** entrez un nom de rôle (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.

        * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  - **Type de fournisseur :** indiquez si le VPN par application est fourni en tant que **Proxy d'application** ou **Tunnel de paquet**. La valeur par défaut est **Proxy d'application**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole F5 SSL pour iOS

- **Identificateur de bundle de fournisseur :** si votre profil VPN par application contient l'identificateur de bundle d'une application avec plusieurs fournisseurs VPN du même type, spécifiez le fournisseur à utiliser ici.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.

- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau.
  - **Type de fournisseur :** indiquez si le VPN par application est fourni en tant que **Proxy d'application** ou **Tunnel de paquet**. La valeur par défaut est **Proxy d'application**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole SonicWALL pour iOS

- **Identificateur de bundle de fournisseur :** si votre profil VPN par application contient l'identificateur de bundle d'une application avec plusieurs fournisseurs VPN du même type, spécifiez le fournisseur à utiliser ici.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Groupe ou domaine de connexion :** entrez un groupe ou domaine de connexion (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous définissez cette option sur Activé, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per

App VPN initient une communication réseau.
- **Type de fournisseur :** indiquez si le VPN par application est fourni en tant que **Proxy d'application** ou **Tunnel de paquet**. La valeur par défaut est **Proxy d'application**.
- **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
  * **Domaine :** entrez le domaine à ajouter.
  * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole Ariba VIA pour iOS

- **Identificateur de bundle de fournisseur :** si votre profil VPN par application contient l'identificateur de bundle d'une application avec plusieurs fournisseurs VPN du même type, spécifiez le fournisseur à utiliser ici.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne

pas l'enregistrer.

Configurer les protocoles IKEv2 pour iOS

Cette section contient les paramètres utilisés pour les protocoles IKEv2, AlwaysOn IKEv2 et Double configuration AlwaysOn IKEv2. Pour le protocole Double configuration AlwaysOn IKEv2, configurez tous ces paramètres pour les réseaux cellulaires et Wi-Fi.

- **Autoriser l'utilisateur à désactiver la connexion automatique :** pour les protocoles AlwaysOn. Indiquez si vous souhaitez permettre aux utilisateurs de désactiver la connexion automatique au réseau sur leurs appareils. La valeur par défaut est **Désactivé**.
- **Nom d'hôte ou adresse IP du serveur :** entrez le nom ou l'adresse IP du serveur VPN.
- **Identifiant local :** nom de domaine complet ou adresse IP du client IKEv2. Ce champ est obligatoire.
- **Identifiant distant :** nom de domaine complet ou adresse IP du serveur VPN. Ce champ est obligatoire.
- **Authentification de l'appareil :** choisissez **Secret partagé**, **Certificat** ou **Certificat d'appareil basé sur l'identité de l'appareil** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Secret partagé**.
  - Si vous choisissez **Secret partagé**, entrez une clé de secret partagé (facultatif).
  - Si vous choisissez **Certificat**, choisissez les **Infos d'identification** de l'identité à utiliser. La valeur par défaut est **Aucun**.
  - Si vous choisissez **Certificat d'appareil basé sur l'identité de l'appareil**, choisissez le **type d'identité de l'appareil** à utiliser. La valeur par défaut est **IMEI**. Pour utiliser cette option, importez des certificats de façon groupée à l'aide de l'API REST. Consultez Effectuer un chargement groupé de certificats sur des appareils iOS avec l'API REST. Disponible uniquement lorsque vous sélectionnez **Toujours sur IKEv2**.
- **Authentification étendue activée :** indiquez si vous souhaitez activer le protocole d'authentification étendue (EAP). Si vous choisissez **Activé**, tapez le **compte d'utilisateur** et le **mot de passe d'authentification**.
- **Intervalle DPD :** choisissez la fréquence à laquelle un appareil homologue est contacté pour vous assurer qu'il reste accessible. La valeur par défaut est **Aucun**. Les options sont les suivantes :
  - **Aucun :** désactive DPD.
  - **Faible :** contacte l'homologue toutes les 30 minutes.
  - **Moyen :** contacte l'homologue toutes les 10 minutes.

  - **Élevé :** contacte l'homologue toutes les minutes.

- **Désactiver la mobilité et le multihoming :** sélectionnez cette option pour désactiver cette fonctionnalité.
- **Utilisez les attributs du sous-réseau interne IPv4/IPv6 :** choisissez si vous souhaitez activer cette fonctionnalité.
- **Désactiver les redirections :** choisissez si vous souhaitez désactiver les redirections.
- **Activer Keepalive NAT lorsque l'appareil est en veille :** pour les protocoles AlwaysOn. Les paquets Keepalive maintiennent les mappages NAT pour les connexions IKEv2. La puce envoie ces paquets à intervalle régulier lorsque l'appareil est éveillé. Si ce paramètre est On, la puce envoie des paquets Keepalive même lorsque l'appareil est en veille. L'intervalle par défaut est de 20 secondes via Wi-Fi et de 110 secondes via réseau cellulaire. Vous pouvez modifier l'intervalle en utilisant le paramètre Intervalle Keepalive NAT.
- **Intervalle Keepalive NAT (secondes) :** la valeur par défaut est de 20 secondes.
- **Activer PFS (Perfect Forward Secrecy) :** choisissez si vous souhaitez activer cette fonctionnalité.
- **Adresses IP des serveurs DNS :** facultatif. Une liste des chaînes d'adresses IP du serveur DNS. Ces adresses IP peuvent inclure un mélange d'adresses IPv4 et IPv6. Cliquez sur **Ajouter** pour saisir une adresse.
- **Nom de domaine :** facultatif. Domaine principal du tunnel.
- **Domaines de recherche :** facultatif. Liste de chaînes de domaines utilisés pour donner des noms d'hôte complets uniques.
- **Ajouter des domaines de correspondance supplémentaires à la liste de résolution :** facultatif. Détermine si les domaines figurant dans la liste des domaines correspondants supplémentaires doivent être ajoutés à la liste des domaines de recherche pour la résolution. La valeur par défaut est **Activé**.
- **Domaines correspondant supplémentaires :** facultatif. Liste des chaînes de domaines utilisés pour déterminer les requêtes DNS qui devront utiliser les paramètres de résolution DNS contenus dans les adresses de serveur DNS. Cette clé crée une configuration split DNS où uniquement les hôtes de certains domaines sont résolus à l'aide de la résolution DNS du tunnel. Les hôtes ne se trouvant pas dans l'un des domaines de cette liste sont résolus à l'aide de la résolution par défaut du système.

Si ce paramètre contient une chaîne vide, cette chaîne est utilisée en tant que domaine par défaut. Cette solution permet à une configuration de split-tunnel de diriger toutes les requêtes DNS vers les serveurs de VPN DNS avant les serveurs DNS principaux. Si le tunnel VPN est l'itinéraire par défaut du réseau, les serveurs DNS répertoriés deviennent la résolution par défaut. Dans ce cas, la liste des domaines correspondants supplémentaires est ignorée.

- **Paramètres IKE SA** et **Paramètres SA enfants**. Configurez ces paramètres pour chaque option d'association de sécurité (SA) :
  - **Algorithme de chiffrement :** dans la liste, sélectionnez l'algorithme de chiffrement IKE à utiliser. La valeur par défaut est **3DES**.
  - **Algorithme d'intégrité :** dans la liste, sélectionnez l'algorithme d'intégrité à utiliser. La valeur par défaut est **SHA1-96**.
  - **Groupe Diffie Hellman :** dans la liste, sélectionnez le numéro du groupe Diffie Hellman. La valeur par défaut est **2**.
  - **Durée de vie d'IKE en minutes :** entrez un nombre entier compris entre 10 et 1440 représentant la durée de vie SA (rekey interval). La valeur par défaut est **1440** minutes.
- **Exceptions de service :** pour les protocoles AlwaysOn. Les exceptions de service sont des services du système auxquels n'est pas appliquée l'option VPN toujours connecté. Configurez ces paramètres d'exceptions de service :
  - **Messagerie vocale :** dans la liste, sélectionnez la façon dont l'exception des messages vocaux est traitée. La valeur par défaut est **Autoriser le trafic via le tunnel**.
  - **AirPrint :** dans la liste, sélectionnez la façon dont l'exception AirPrint est traitée. La valeur par défaut est **Autoriser le trafic via le tunnel**.
  - **Autoriser le trafic en provenance de websheets captifs en dehors du tunnel VPN :** sélectionnez cette option pour autoriser les utilisateurs à se connecter à des points d'accès en dehors du tunnel VPN. La valeur par défaut est **Désactivé**.
  - **Autoriser le trafic en provenance de toutes les applications de réseaux captifs en dehors du tunnel VPN :** sélectionnez cette option pour autoriser toutes les applications de réseau de point d'accès en dehors du tunnel VPN. La valeur par défaut est **Désactivé**.
  - **Bundle ID d'applications de réseaux captifs :** pour chaque identificateur de bundle d'applications de réseau auquel les utilisateurs sont autorisés à accéder, cliquez sur **Ajouter** et entrez le **bundle ID** de réseau de point d'accès. Cliquez sur **Enregistrer** pour enregistrer le bundle ID d'application.
- **Per App VPN**. Configurez ces paramètres pour les types de connexion IKEv2.
  - **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**.
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  - **Domaines safari :** cliquez sur **Ajouter** pour ajouter un nom de domaine Safari.

- **Configuration du proxy :** choisissez la façon dont la connexion VPN transite via un serveur proxy. La valeur par défaut est **Aucun**.

Configurer le protocole Citrix SSO pour iOS

Le client Citrix SSO est disponible dans le portail Apple Store https://apps.apple.com/us/app/citrix-sso/id1333396910.

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    - **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    - **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé.**
    - **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé.** Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous définissez cette option sur Activé, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau.
  - **Type de fournisseur :** indiquez si le VPN par application est fourni en tant que **Proxy d'application** ou **Tunnel de paquet**. La valeur par défaut est **Proxy d'application**.
  - **Type de fournisseur :** définissez sur **Tunnel de paquet**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    - **Domaine :** entrez le domaine à ajouter.
    - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **XML personnalisé :** pour chaque paramètre XML personnalisé que vous souhaitez ajouter, cliquez sur **Ajouter** et spécifiez les paires clé/valeur. Les paramètres disponibles sont les suiv-

ants :

- **disableL3 :** désactive le VPN au niveau du système. Autorise uniquement le Per App VPN. Aucune **valeur** n'est requise.
- **useragent :** associe à cette stratégie toute stratégie Citrix Gateway qui cible les clients de plug-in VPN. La **valeur** de cette clé est automatiquement ajoutée au plug-in VPN pour les requêtes initiées par le plug-in.

Configurer le protocole SSL personnalisé pour iOS

Pour passer du client Cisco Legacy AnyConnect au client Cisco AnyConnect :

1. Configurez la stratégie VPN avec le protocole SSL personnalisé. Déployez la stratégie sur les appareils iOS.
2. Chargez le client Cisco AnyConnect depuis https://apps.apple.com/us/app/cisco-anyconnect/id1135064690, ajoutez l'application à XenMobile et déployez l'application sur les appareils iOS.
3. Supprimez l'ancienne stratégie VPN des appareils iOS.

Paramètres :

- **Identifiant SSL personnalisé (format DNS inverse) :** définissez sur le bundle ID. Pour le client Cisco AnyConnect, utilisez **com.cisco.anyconnect**.
- **Identificateur de bundle de fournisseur :** si l'application spécifiée dans **Identifiant SSL personnalisé** a plusieurs fournisseurs VPN du même type (Proxy d'application ou Tunnel de paquet), spécifiez cet identificateur de bundle. Pour le client Cisco AnyConnect, utilisez **com.cisco.anyconnect**.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    - **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    - **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé.**
    - **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé.** Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.

- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous définissez cette option sur Activé, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau.
  - **Type de fournisseur :** un type de fournisseur indique si le fournisseur est un service VPN ou un service de proxy. Pour le service VPN, choisissez **Tunnel de paquet**. Pour le service de proxy, choisissez **Proxy d'application**. Pour le client Cisco AnyConnect, choisissez **Tunnel de paquet**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    - **Domaine :** entrez le domaine à ajouter.
    - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **XML personnalisé :** pour chaque paramètre XML personnalisé que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom du paramètre :** entrez le nom du paramètre à ajouter.
  - **Valeur :** entrez la valeur associée au **nom du paramètre**.
  - Cliquez sur **Enregistrer** pour enregistrer le paramètre ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer la stratégie VPN pour prendre en charge NAC

1. Le **type de connexion SSL personnalisé** est requis pour la configuration du filtre NAC.
2. Spécifiez **VPN** comme **nom de connexion**.
3. Pour **Identifiant SSL personnalisé**, tapez **com.citrix.NetScalerGateway.ios.app**
4. Pour **Identificateur de bundle de fournisseur**, tapez **com.citrix.NetScalerGateway.ios.app.vpnplugin**

Les valeurs des étapes 3 et 4 proviennent de l'installation de Citrix SSO requise pour le filtrage NAC. Vous ne configurez pas de mot de passe d'authentification. Pour plus d'informations sur l'utilisation de la fonction NAC, voir Contrôle d'accès réseau.

Configurer les options de l'activation VPN sur demande pour iOS

- **Domaine sur demande :** pour chaque domaine et action à exécuter lorsque les utilisateurs s'y connectent, cliquez sur **Ajouter** et procédez comme suit :
- **Domaine :** entrez le domaine à ajouter.
- **Action :** dans la liste, sélectionnez l'une des actions possibles :
  - **Toujours établir :** le domaine déclenche toujours une connexion VPN.
  - **Ne jamais établir :** le domaine ne déclenche jamais de connexion VPN.

  - **Établir si nécessaire :** le domaine déclenche une tentative de connexion VPN si la résolution du nom de domaine échoue. L'échec se produit lorsque le serveur DNS ne peut pas résoudre le domaine, redirige la connexion vers un autre serveur ou expire.
  - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **Règles On Demand**
  - **Action :** dans la liste, sélectionnez l'action à exécuter. La valeur par défaut est **EvaluateConnection.** Les actions possibles sont les suivantes :
    * **Autoriser :** autoriser la connexion VPN sur demande.
    * **Connecter :** établir une connexion VPN sans condition.
    * **Déconnecter :** désactiver la connexion VPN et ne pas se reconnecter à la demande tant que la règle est active.
    * **EvaluateConnection :** évaluer la matrice ActionParameters pour chaque connexion.
    * **Ignorer :** conserver toute connexion VPN en cours mais ne pas se reconnecter à la demande tant que la règle est active.
  - **DNSDomainMatch :** pour chaque domaine avec lequel la liste de domaines de recherche d'un appareil peut correspondre, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine DNS :** entrez le nom du domaine. Vous pouvez utiliser le préfixe générique « * » pour la correspondance avec multiples domaines. Par exemple,*.exemple.com peut correspondre à mondomaine.exemple.com, tondomaine.exemple.com et sondomaine.exemple.com.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **DNSServerAddressMatch :** pour chaque adresse IP à laquelle n'importe quel des serveurs DNS spécifiés du réseau peut correspondre, cliquez sur **Ajouter** et procédez comme suit :
    * **Adresse du serveur DNS :** entrez l'adresse du serveur DNS que vous souhaitez ajouter. Vous pouvez utiliser le suffixe générique «*» pour la correspondance avec des serveurs DNS. Par exemple, 17.* correspond à n'importe quel serveur DNS u sous-réseau de classe A.
    * Cliquez sur **Enregistrer** pour enregistrer l'adresse du serveur DNS ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **InterfaceTypeMatch :** dans la liste, sélectionnez le type de matériel d'interface réseau principal utilisé. La valeur par défaut est **Non spécifié**. Valeurs possibles :
    * **Non spécifié :** correspondance avec n'importe quel matériel d'interface réseau. Cette option est la valeur par défaut.
    * **Ethernet :** correspondance uniquement avec le matériel d'interface réseau Ethernet.
    * **Wi-Fi :** correspondance uniquement avec le matériel d'interface réseau Wi-Fi.
    * **Cellulaire :** correspondance uniquement avec le matériel d'interface réseau cellulaire.

- **SSIDMatch :** pour chaque SSID à faire correspondre avec le réseau actuel, cliquez sur **Ajouter** et procédez comme suit.
  - **SSID :** entrez le SSID à ajouter. Si le réseau n'est pas un réseau Wi-Fi, ou si le SSID ne s'affiche pas, la correspondance échoue. Laissez cette liste vide pour une correspondance avec n'importe quel SSID.
  - Cliquez sur **Enregistrer** pour enregistrer le SSID ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **URLStringProbe :** entrez une adresse URL à récupérer. Si cette adresse URL est correctement récupérée sans redirection, cette règle correspond.
- **ActionParameters : Domains :** pour chaque domaine que EvaluateConnection doit vérifier, cliquez sur **Ajouter** et procédez comme suit :
  - **Domaine :** entrez le domaine à ajouter.
  - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **ActionParameters : DomainAction :** dans la liste, sélectionnez le **comportement du VPN** pour les domaines **ActionParameters : Domains** spécifiés. La valeur par défaut est **ConnectIfNeeded**. Les actions possibles sont les suivantes :
  - **ConnectIfNeeded :** le domaine déclenche une tentative de connexion VPN si la résolution du nom de domaine échoue. L'échec se produit lorsque le serveur DNS ne peut pas résoudre le domaine, redirige la connexion vers un autre serveur ou expire.
  - **NeverConnect :** le domaine ne déclenche jamais de connexion VPN.
- **Action Parameters: RequiredDNSServers :** pour chaque adresse IP de serveur DNS à utiliser pour résoudre les domaines spécifiés, cliquez sur **Ajouter** et procédez comme suit :
  - **Serveur DNS :** valide uniquement si **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Tapez le serveur DNS à ajouter. Ce serveur n'a pas besoin de faire partie de la configuration réseau actuelle de l'appareil. Si le serveur DNS n'est pas accessible, une connexion VPN est établie en réponse. Ce serveur DNS doit être un serveur DNS interne ou un serveur DNS externe de confiance.
  - Cliquez sur **Enregistrer** pour enregistrer le serveur DNS ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **ActionParameters : RequiredURLStringProbe :** si vous le souhaitez, entrez une adresse URL HTTP ou HTTPS (recommandé) à interroger, à l'aide d'un requête GET. Si le nom d'hôte de l'adresse URL ne peut pas être résolu, si le serveur est inaccessible ou si le serveur ne répond pas, une connexion VPN est établie. Valide uniquement si **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.
- **OnDemandRules : XML content :** entrez, ou copiez et collez, les règles on demand de la configuration XML.
  - Cliquez sur **Vérifier dict.** pour valider le code XML. Le texte « XML valide » s'affiche en

vert sous la zone de texte **Contenu XML** si le fichier XML est valide. S'il n'est pas valide, un message d'erreur décrivant l'erreur s'affiche en orange.

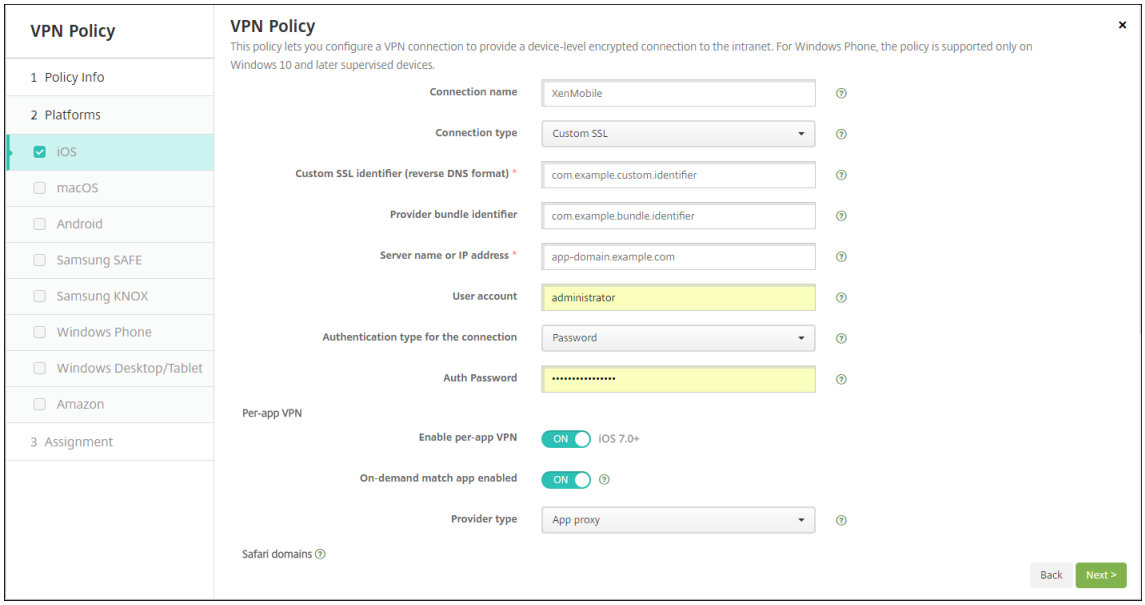
- **Proxy**
  - **Configuration du proxy :** dans la liste, sélectionnez la façon dont la connexion VPN transite via un serveur proxy. La valeur par défaut est **Aucun**.
    - Si vous avez sélectionné **Manuel**, configurez les paramètres suivants :
      - **Nom d'hôte ou adresse IP du serveur proxy :** entrez le nom d'hôte ou l'adresse IP du serveur proxy. Ce champ est obligatoire.
      - **Port du serveur proxy :** entrez le numéro de port du serveur proxy. Ce champ est obligatoire.
      - **Nom d'utilisateur :** entrez un nom d'utilisateur pour le serveur proxy (facultatif).
      - **Mot de passe :** entrez un mot de passe pour le serveur proxy (facultatif).
    - Si vous configurez **Automatique**, configurez ce paramètre :
      - **URL du serveur proxy :** entrez l'adresse URL du serveur proxy. Ce champ est obligatoire.
- **Paramètres de stratégie**
  - Sous **Paramètres de stratégie**, à côté de **Supprimer la stratégie**, sélectionnez **Sélectionner une date** ou **Délai avant suppression (en heures)**.
  - Si vous sélectionnez **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, sélectionnez **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous sélectionnez **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

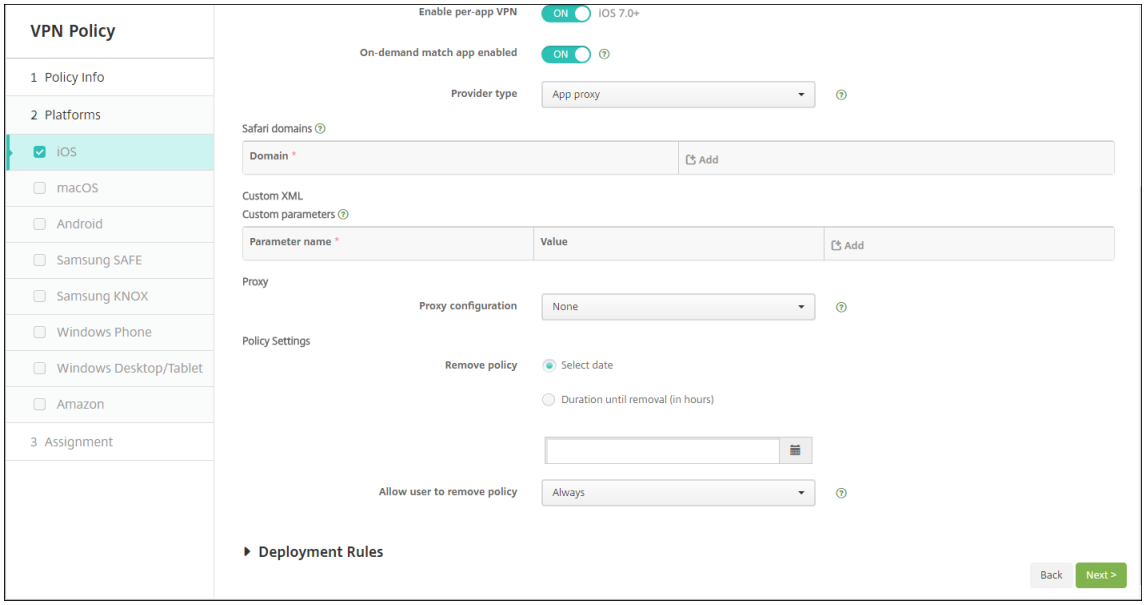
Configurer une stratégie Per App VPN

Des options Per App VPN pour iOS sont disponibles pour ces types de connexion : Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Aruba VIA, Citrix VPN, Citrix SSO et SSL personnalisé.

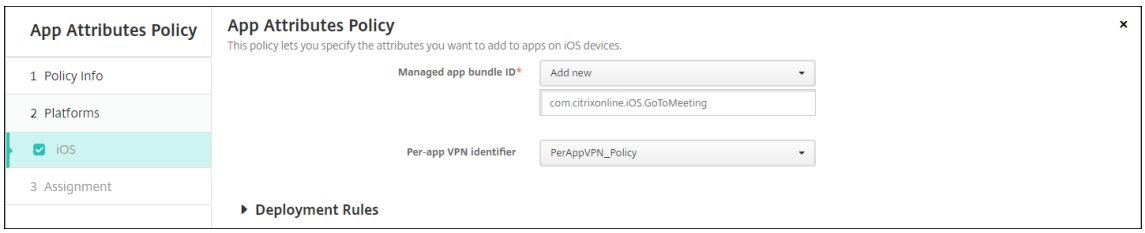
Pour configurer une stratégie Per App VPN :

1. Dans **Configurer > Stratégies d'appareil**, créez une stratégie VPN. Par exemple :



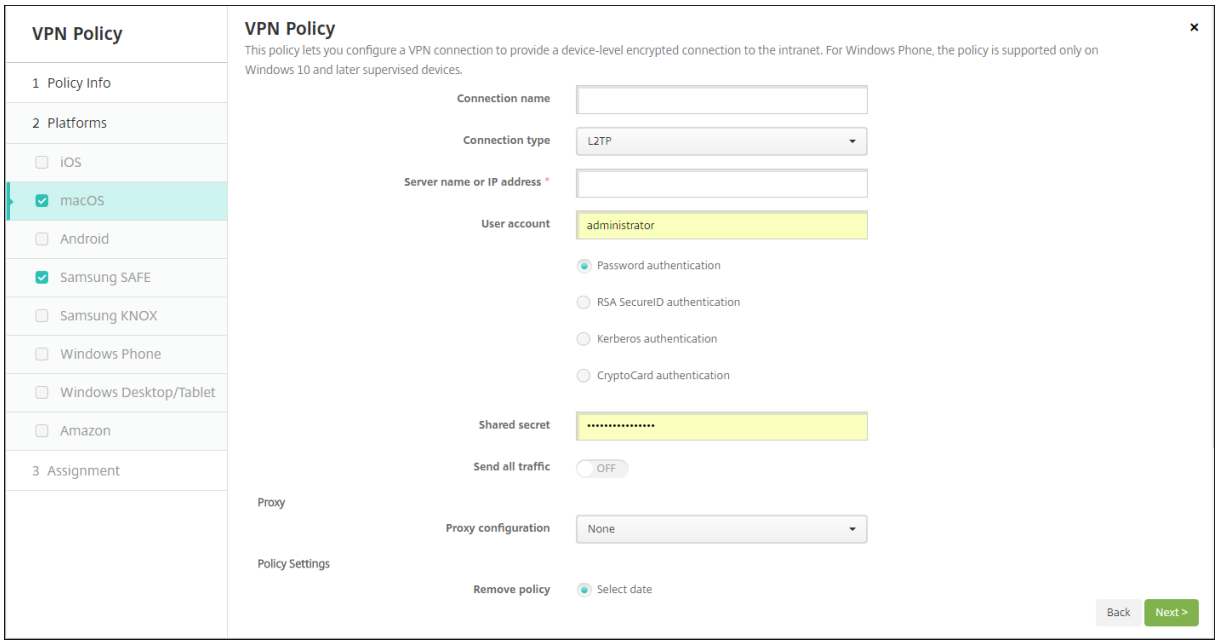


2. Dans **Configurer > Stratégies d'appareil**, créez une stratégie d'attributs d'application pour associer une application à la stratégie Per App VPN. Pour **Identifiant Per App VPN**, choisissez le nom de la stratégie VPN créée à l'étape 1. Pour **Bundle ID d'application gérée**, choisissez dans la liste d'applications ou entrez le bundle ID d'application. (Si vous déployez une stratégie d'inventaire des applications iOS, la liste des applications contient des applications).



- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres macOS



- **Nom de la connexion :** entrez un nom pour la connexion.
- **Type de connexion :** dans la liste, sélectionnez le protocole à utiliser pour cette connexion. La valeur par défaut est L2TP.
  - **L2TP :** Layer 2 Tunneling Protocol avec authentification par clé pré-partagée.
  - **PPTP :** protocole PPTP.
  - **IPSec :** votre connexion VPN d'entreprise.
  - **Cisco AnyConnect :** client Cisco AnyConnect VPN.
  - **Juniper SSL :** client Juniper Networks SSL VPN.
  - **F5 SSL :** client F5 Networks SSL VPN.
  - **SonicWALL Mobile Connect :** client VPN Dell unifié pour iOS.
  - **Aruba VIA :** client Aruba Networks Virtual Internet Access.
  - **Citrix VPN :** client Citrix VPN.
  - **SSL personnalisé :** Secure Sockets Layer personnalisé.

Les sections suivantes répertorient les options de configuration pour chacun des types de connexion précédents.

Configurer le protocole L2TP pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- Sélectionnez **Authentification par mot de passe**, **Authentification RSA SecurID**, **Authentification Kerberos** ou **Authentification CryptoCard**. La valeur par défaut est **Authentification par mot de passe**.
- **Secret partagé :** entrez la clé de secret partagé IPsec.
- **Envoyer tout le trafic :** sélectionnez cette option pour envoyer tout le trafic via le VPN. La valeur par défaut est **Désactivé**.

Configurer le protocole PPTP pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- Sélectionnez **Authentification par mot de passe**, **Authentification RSA SecurID**, **Authentification Kerberos** ou **Authentification CryptoCard**. La valeur par défaut est **Authentification par mot de passe**.
- **Niveau de chiffrement :** sélectionnez le niveau de chiffrement souhaité. La valeur par défaut est **Aucun**.
  - **Aucun :** le chiffrement n'est pas utilisé.
  - **Automatique :** utilise le niveau de chiffrement le plus élevé pris en charge par le serveur.
  - **Maximum (128 bits) :** utilise toujours le cryptage 128 bits.
- **Envoyer tout le trafic :** sélectionnez cette option pour envoyer tout le trafic via le VPN. La valeur par défaut est **Désactivé**.

Configurer le protocole IPsec pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Secret partagé** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Secret partagé**.
  - Si vous sélectionnez l'authentification **Secret partagé**, configurez les paramètres suivants :
    - **Nom du groupe :** entrez un nom de groupe (facultatif).
    - **Secret partagé :** entrez une clé de secret partagé (facultatif).

        * **Utiliser une authentification hybride :** indiquez si vous souhaitez utiliser l'authentification hybride. Avec l'authentification hybride, le serveur s'authentifie auprès du client, puis le client s'authentifie auprès du serveur. La valeur par défaut est **Désactivé**.
        * **Demander le mot de passe :** indiquez si les utilisateurs doivent être invités à entrer leur mot de passe lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    - Si vous avez sélectionné l'authentification **Certificat**, configurez les paramètres suivants :
        * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
        * **Exiger PIN à la connexion :** sélectionnez cette option pour demander aux utilisateurs d'entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
        * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.

Configurer le protocole Cisco AnyConnect pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Groupe :** entrez un nom de groupe (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
    - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
    - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
        * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
        * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
        * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.
    - **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par

défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :

* **Correspondance d'application à la demande activée :** indiquez si une connexion Per App VPN est déclenchée automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
* **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
  · **Domaine :** entrez le domaine à ajouter.
  · Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole SSL Juniper pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Domaine :** entrez un nom de domaine (facultatif).
- **Rôle :** entrez un nom de rôle (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  – Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  – Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  – **Correspondance d'application à la demande activée :** indiquez si une connexion Per App VPN est déclenchée automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  – **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :

        * **Domaine :** entrez le domaine à ajouter.
        * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole F5 SSL pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si une connexion Per App VPN est déclenchée automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole SonicWall Mobile Connect pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Groupe ou domaine de connexion :** entrez un groupe ou domaine de connexion (facultatif).

- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    - **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    - **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    - **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si une connexion Per App VPN est déclenchée automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    - **Domaine :** entrez le domaine à ajouter.
    - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole Ariba VIA pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    - **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    - **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.

        * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si une connexion Per App VPN est déclenchée automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole SSL personnalisé pour macOS

- **Identifiant SSL personnalisé (format DNS inverse) :** entrez l'identifiant SSL au format DNS inverse. Ce champ est obligatoire.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN. Ce champ est obligatoire.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
  - **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé.**
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé.** Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.
  - **Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :

        * **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau.
        * **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
            · **Domaine :** entrez le domaine à ajouter.
            · Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **XML personnalisé :** pour chaque paramètre XML personnalisé que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom du paramètre :** entrez le nom du paramètre à ajouter.
  - **Valeur :** entrez la valeur associée au **nom du paramètre**.
  - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer les options de l'activation VPN sur demande

- **Domaine sur demande :** pour chaque domaine et action à exécuter lorsque les utilisateurs s'y connectent, cliquez sur **Ajouter** et procédez comme suit :
  - **Domaine :** entrez le domaine à ajouter.
  - **Action :** dans la liste, sélectionnez l'une des actions possibles :
    * **Toujours établir :** le domaine déclenche toujours une connexion VPN.
    * **Ne jamais établir :** le domaine ne déclenche jamais de connexion VPN.
    * **Établir si nécessaire :** le domaine déclenche une tentative de connexion VPN si la résolution du nom de domaine échoue. L'échec se produit lorsque le serveur DNS ne peut pas résoudre le domaine, redirige la connexion vers un autre serveur ou expire.
  - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **Règles On Demand**
  - **Action :** dans la liste, sélectionnez l'action à exécuter. La valeur par défaut est **Evaluate-Connection.** Les actions possibles sont les suivantes :
    * **Autoriser :** autoriser la connexion VPN sur demande.
    * **Connecter :** établir une connexion VPN sans condition.
    * **Déconnecter :** désactiver la connexion VPN et ne pas se reconnecter à la demande tant que la règle est active.
    * **EvaluateConnection :** évaluer la matrice **ActionParameters** pour chaque connexion.
    * **Ignorer :** conserver toute connexion VPN en cours mais ne pas se reconnecter à la demande tant que la règle est active.

- **DNSDomainMatch :** pour chaque domaine avec lequel la liste de domaines de recherche d'un appareil peut correspondre, cliquez sur **Ajouter** et procédez comme suit :
  - **Domaine DNS :** entrez le nom du domaine. Vous pouvez utiliser le préfixe générique « * » pour la correspondance avec multiples domaines. Par exemple,*.exemple.com peut correspondre à mondomaine.exemple.com, tondomaine.exemple.com et son-domaine.exemple.com.
  - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **DNSServerAddressMatch :** pour chaque adresse IP à laquelle n'importe quel des serveurs DNS spécifiés du réseau peut correspondre, cliquez sur **Ajouter** et procédez comme suit :
  - **Adresse du serveur DNS :** entrez l'adresse du serveur DNS que vous souhaitez ajouter. Vous pouvez utiliser le suffixe générique «*» pour la correspondance avec des serveurs DNS. Par exemple, 17.* correspond à n'importe quel serveur DNS u sous-réseau de classe A.
  - Cliquez sur **Enregistrer** pour enregistrer l'adresse du serveur DNS ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **InterfaceTypeMatch :** dans la liste, cliquez sur le type de matériel d'interface réseau principal utilisé. La valeur par défaut est **Non spécifié**. Valeurs possibles :
  - **Non spécifié :** correspondance avec n'importe quel matériel d'interface réseau. Cette option est la valeur par défaut.
  - **Ethernet :** correspondance uniquement avec le matériel d'interface réseau Ethernet.
  - **Wi-Fi :** correspondance uniquement avec le matériel d'interface réseau Wi-Fi.
  - **Cellulaire :** correspondance uniquement avec le matériel d'interface réseau cellulaire.
- **SSIDMatch :** pour chaque SSID à faire correspondre avec le réseau actuel, cliquez sur **Ajouter** et procédez comme suit.
  - **SSID :** entrez le SSID à ajouter. Si le réseau n'est pas un réseau Wi-Fi, ou si le SSID ne s'affiche pas, la correspondance échoue. Laissez cette liste vide pour une correspondance avec n'importe quel SSID.
  - Cliquez sur **Enregistrer** pour enregistrer le SSID ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **URLStringProbe :** entrez une adresse URL à récupérer. Si cette adresse URL est correctement récupérée sans redirection, cette règle correspond.
- **ActionParameters : Domains :** pour chaque domaine que EvaluateConnection doit vérifier, cliquez sur **Ajouter** et procédez comme suit :
  - **Domaine :** entrez le domaine à ajouter.
  - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **ActionParameters : DomainAction :** dans la liste, sélectionnez le **comportement du**

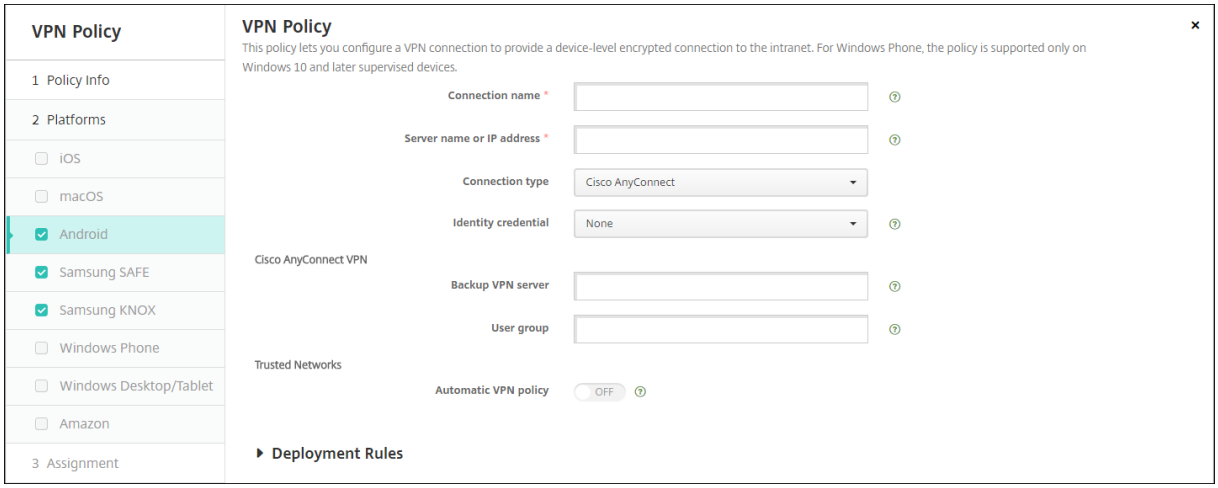
VPN pour les domaines **ActionParameters : Domains** spécifiés. La valeur par défaut est **ConnectIfNeeded**. Les actions possibles sont les suivantes :

  * **ConnectIfNeeded :** le domaine déclenche une tentative de connexion VPN si la résolution du nom de domaine échoue. L'échec se produit lorsque le serveur DNS ne peut pas résoudre le domaine, redirige la connexion vers un autre serveur ou expire.
  * **NeverConnect :** le domaine ne déclenche jamais de connexion VPN.

- **Action Parameters: RequiredDNSServers :** pour chaque adresse IP de serveur DNS à utiliser pour résoudre les domaines spécifiés, cliquez sur **Ajouter** et procédez comme suit :
  * **Serveur DNS :** valide uniquement si **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Tapez le serveur DNS à ajouter. Ce serveur n'a pas besoin de faire partie de la configuration réseau actuelle de l'appareil. Si le serveur DNS n'est pas accessible, une connexion VPN est établie en réponse. Ce serveur DNS doit être un serveur DNS interne ou un serveur DNS externe de confiance.
  * Cliquez sur **Enregistrer** pour enregistrer le serveur DNS ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **ActionParameters : RequiredURLStringProbe :** si vous le souhaitez, entrez une adresse URL HTTP ou HTTPS (recommandé) à interroger, à l'aide d'un requête GET. Si le nom d'hôte de l'adresse URL ne peut pas être résolu, si le serveur est inaccessible ou si le serveur ne répond pas, une connexion VPN est établie. Valide uniquement si **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.
- **OnDemandRules : XML content :** entrez, ou copiez et collez, les règles on demand de la configuration XML.
  * Cliquez sur **Vérifier dict.** pour valider le code XML. Le texte « XML valide » s'affiche en vert sous la zone de texte **Contenu XML** si le fichier XML est valide. S'il n'est pas valide, un message d'erreur décrivant l'erreur s'affiche en orange.

- **Proxy**
  - **Configuration du proxy :** dans la liste, sélectionnez la façon dont la connexion VPN transite via un serveur proxy. La valeur par défaut est **Aucun**.
    * Si vous avez sélectionné **Manuel**, configurez les paramètres suivants :
      · **Nom d'hôte ou adresse IP du serveur proxy :** entrez le nom d'hôte ou l'adresse IP du serveur proxy. Ce champ est obligatoire.
      · **Port du serveur proxy :** entrez le numéro de port du serveur proxy. Ce champ est obligatoire.
      · **Nom d'utilisateur :** entrez un nom d'utilisateur pour le serveur proxy (facultatif).
      · **Mot de passe :** entrez un mot de passe pour le serveur proxy (facultatif).
    * Si vous configurez **Automatique**, configurez ce paramètre :
      · **URL du serveur proxy :** entrez l'adresse URL du serveur proxy. Ce champ est obligatoire.

Paramètres Android



Configurer le protocole Cisco AnyConnect VPN pour Android

- **Nom de la connexion :** entrez un nom pour la connexion au VPN Cisco AnyConnect. Ce champ est obligatoire.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN. Ce champ est obligatoire.
- **Infos d'identification de l'identité :** dans la liste, sélectionnez des Informations d'identification de l'identité.
- **Serveur VPN de sauvegarde :** entrez les informations du serveur VPN de sauvegarde.
- **Groupe d'utilisateurs :** entrez les informations relatives au groupe d'utilisateurs.
- **Réseaux fiables**
  - **Stratégie de VPN automatique :** activez ou désactivez cette option pour définir la façon dont le VPN réagit aux réseaux approuvés et non approuvés. Si cette option est activée, configurez les paramètres suivants :
    - **Stratégie pour réseau fiable :** dans la liste, sélectionnez la stratégie souhaitée. La valeur par défaut est **Déconnecter**. Les options possibles sont les suivantes :
      - **Déconnecter :** le client met fin à la connexion VPN dans le réseau approuvé. il s'agit du réglage par défaut.
      - **Connecter :** le client initie une connexion VPN dans le réseau approuvé.
      - **Ne rien faire :** le client n'exécute aucune action.
      - **Mettre en pause :** met la session VPN en pause lorsqu'un utilisateur accède à un réseau configuré comme approuvé après avoir établi une session VPN à l'extérieur du réseau approuvé. Lorsque l'utilisateur quitte le réseau approuvé, la session reprend. Ce paramètre élimine le besoin de créer une nouvelle session VPN après avoir quitté un réseau approuvé.
    - **Stratégie pour réseau non fiable :** dans la liste, sélectionnez la stratégie souhaitée.

La valeur par défaut est **Connecter**. Les options possibles sont les suivantes :

- **Connecter :** le client initie une connexion VPN dans le réseau non approuvé.
- **Ne rien faire :** le client démarre une connexion VPN dans le réseau non approuvé. Cette option désactive le VPN permanent.

– **Domaines approuvés :** pour chaque suffixe de domaine que l'interface réseau possède lorsque le client est dans le réseau approuvé, cliquez sur **Ajouter** et procédez comme suit :

* **Domaine :** entrez le domaine à ajouter.
* Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

– **Serveurs approuvés :** pour chaque adresse de serveur que l'interface réseau possède lorsque le client est dans le réseau approuvé, cliquez sur **Ajouter** et procédez comme suit :

* **Serveurs :** entrez le serveur à ajouter.
* Cliquez sur **Enregistrer** pour enregistrer le serveur ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole Citrix SSO pour Android

- **Nom de la connexion :** entrez un nom pour la connexion VPN. Ce champ est obligatoire.
- **Nom du serveur ou adresse IP :** entrez le nom de domaine complet ou l'adresse IP du Citrix Gateway.
- **Type d'authentification pour la connexion :** choisissez un type d'authentification et renseignez les champs qui s'affichent pour le type :
  - **Nom d'utilisateur** et **Mot de passe :** saisissez vos informations d'identification VPN pour les **Types d'authentification**, **Mot de passe** ou **Mot de passe et certificat**. Facultatif. Si vous ne fournissez les informations d'identification VPN, l'application Citrix VPN vous invite à entrer un nom d'utilisateur et un mot de passe.
  - **Infos d'identification de l'identité :** s'affiche pour les **Types d'authentification Certificat** ou **Mot de passe et certificat**. Dans la liste, sélectionnez des infos d'identification de l'identité.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. Si vous n'activez pas le per app VPN, tout le trafic transite via le tunnel VPN de Citrix. Si vous activez le per app VPN, spécifiez les paramètres suivants. La valeur par défaut est **Désactivé**.
  - **Liste blanche** ou **liste noire :** si l'option **Liste blanche** est sélectionnée, toutes les applications autorisées transitent via ce VPN. Si l'option **Liste noire** est sélectionnée, toutes les applications sauf celles figurant sur la liste de blocage transitent via ce VPN.

> **Remarque :**
>
> La console XenMobile Server utilise les termes « liste noire » et « liste blanche ». Ces termes seront modifiés dans une prochaine version et les termes « liste de blocage » et « liste d'autorisation » les remplaceront.

  - **Liste des applications :** spécifiez les applications autorisées ou bloquées. Cliquez sur **Ajouter** et tapez une liste de noms de paquetages d'applications séparés par des virgules.

- **XML personnalisé :** cliquez sur **Ajouter**, puis entrez les paramètres personnalisés. XenMobile prend en charge ces paramètres pour Citrix VPN :

  - **DisableUserProfiles :** facultatif. Pour activer ce paramètre, entrez **Yes** pour **Value**. Si ce paramètre est activé, XenMobile n'affiche aucune connexion VPN ajoutée par l'utilisateur et l'utilisateur ne peut pas ajouter de connexion. Ce paramètre est une restriction globale et s'applique à tous les profils VPN.
  - **userAgent :** valeur de chaîne. Vous pouvez spécifier une chaîne d'agent utilisateur personnalisée à envoyer dans chaque requête HTTP. La chaîne d'agent utilisateur spécifiée est ajoutée à l'agent utilisateur Citrix VPN existant.

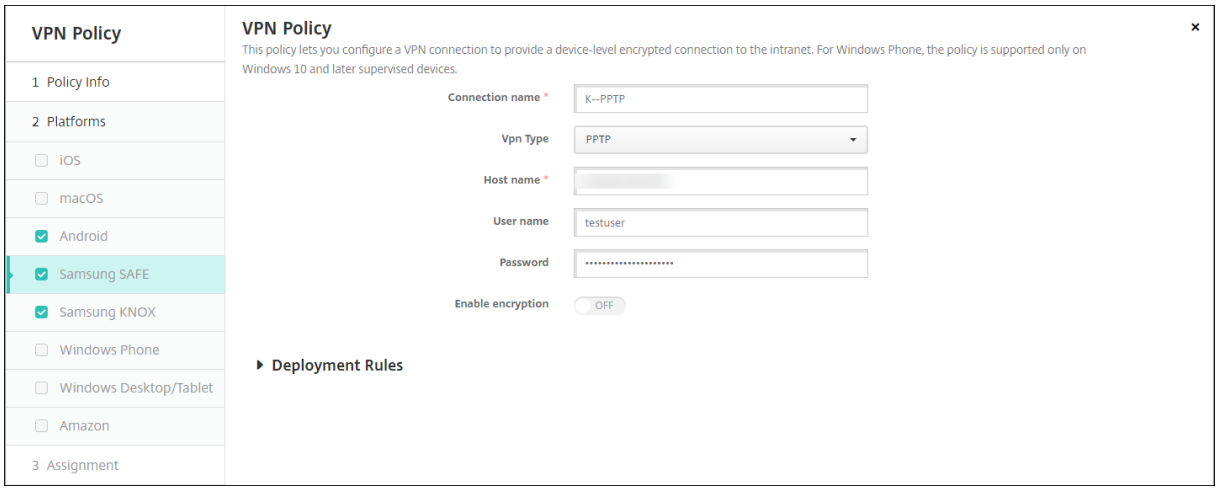
Configurer les VPN pour prendre en charge NAC

1. Définissez **Type de connexion** sur **SSL personnalisé** pour configurer le filtre NAC.
2. Spécifiez **VPN** comme **nom de connexion**.
3. Pour **XML personnalisé**, cliquez sur **Ajouter** et procédez comme suit :
   - **Nom du paramètre :** saisissez **XenMobileDeviceId**. Il s'agit de l'ID d'appareil à utiliser pour la vérification NAC en fonction de l'inscription de l'appareil dans XenMobile. Si XenMobile inscrit et gère l'appareil, la connexion VPN est autorisée. Sinon, l'authentification est refusée au moment de l'établissement du VPN.
   - **Valeur :** tapez **DeviceID_${device.id}** qui est la valeur du paramètre **XenMobileDeviceId**.
   - Cliquez sur **Enregistrer** pour enregistrer le paramètre.

Configurer les VPN pour Android Enterprise

Pour configurer des VPN pour les appareils Android Enterprise, créez une stratégie Configurations gérées par Android Entreprise pour l'application Citrix SSO. Consultez la section Configurer les profils VPN pour Android Enterprise.

Paramètres Samsung SAFE



- **Nom de la connexion :** entrez un nom pour la connexion.
- **Type de VPN :** dans la liste, sélectionnez le protocole à utiliser pour cette connexion. La valeur par défaut est **L2TP avec clé prépartagée**. Les options possibles sont les suivantes :
  - **L2TP avec clé prépartagée :** Layer 2 Tunneling Protocol (L2TP) avec authentification par clé prépartagée. il s'agit du réglage par défaut.
  - **L2TP avec certificat :** Layer 2 Tunneling Protocol avec certificat.
  - **PPTP :** protocole PPTP.
  - **Entreprise :** votre connexion VPN d'entreprise. Applicable aux versions SAFE antérieures à 2.0.
  - **Générique :** connexion VPN générique. Applicable aux versions SAFE 2.0 ou ultérieures.

Configurer le protocole L2TP avec clé prépartagée pour Samsung SAFE

- **Nom d'hôte :** entrez le nom de l'hôte VPN. Cette option est requise.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Clé prépartagée :** entrez la clé prépartagée Cette option est requise.

Configurer L2TP avec le protocole de certificat pour Samsung SAFE

- **Nom d'hôte :** entrez le nom de l'hôte VPN. Cette option est requise.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.

Configurer le protocole PPTP pour Samsung SAFE

- **Nom d'hôte :** entrez le nom de l'hôte VPN. Cette option est requise.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Activer le chiffrement :** sélectionnez cette option si vous souhaitez activer le cryptage sur la connexion VPN.

Configurer le protocole Enterprise pour Samsung SAFE

- **Nom d'hôte :** entrez le nom de l'hôte VPN. Cette option est requise.
- **Activer le serveur de sauvegarde :** sélectionnez cette option pour activer un serveur VPN de sauvegarde. Si cette option est activée, dans **Serveur VPN de sauvegarde**, entrez le nom de domaine complet ou l'adresse IP du serveur VPN de sauvegarde.
- **Activer l'authentification utilisateur :** indiquez si l'authentification de l'utilisateur est exigée. Si cette option est activée, vous pouvez configurer les paramètres suivants :
  - **Nom d'utilisateur :** entrez un nom d'utilisateur.
  - **Mot de passe :** entrez le mot de passe de l'utilisateur.
- **Nom du groupe :** entrez un nom de groupe (facultatif).
- **Méthode d'authentification :** dans la liste, sélectionnez la méthode d'authentification à utiliser. Les options possibles sont les suivantes :
  - **Certificat :** utilise l'authentification par certificat. il s'agit du réglage par défaut. Si cette option est sélectionnée, dans la liste **Infos d'identification de l'identité**, sélectionnez les informations d'identification à utiliser. La valeur par défaut est **Aucun**.
  - **Clé prépartagée :** utilise une clé prépartagée Si cette option est sélectionnée, dans le champ **Clé prépartagée**, entrez la clé du secret partagé.
  - **RSA Hybride :** utilise l'authentification hybride utilisant des certificats RSA
  - **EAP MD5 :** authentifie l'homologue EAP auprès du serveur EAP, mais pas d'authentification mutuelle.
  - **EAP MSCHAPv2 :** utilise l'authentification Challenge-Handshake de Microsoft pour l'authentification mutuelle.
- **Certificat CA :** dans la liste, sélectionnez le certificat à utiliser. La valeur par défaut est **Aucun**.
- **Activer l'itinéraire par défaut :** sélectionnez cette option pour activer un itinéraire par défaut vers le serveur VPN. La valeur par défaut est **Désactivé**.
- **Activer l'authentification par carte à puce :** sélectionnez cette option pour autoriser les utilisateurs à s'authentifier à l'aide de cartes à puce. La valeur par défaut est **Désactivé**.
- **Activer l'option mobile :** sélectionnez cette option si vous souhaitez activer l'option mobile. La valeur par défaut est **Désactivé**.
- **Valeur du groupe Diffie-Hellman (puissance de clé) :** dans la liste, sélectionnez la puissance de clé à utiliser. La valeur par défaut est 0.

- **Type de tunnel de séparation :** dans la liste, sélectionnez le type de tunnel de séparation. La valeur par défaut est **Auto**. Les options possibles sont les suivantes :
  - **Auto :** le tunnel de séparation est automatiquement utilisé.
  - **Manuel :** le tunnel de séparation est utilisé sur l'adresse IP et le port spécifié sur le serveur VPN.
  - **Désactivé :** le tunnel de séparation n'est pas utilisé.
- **Type SuiteB :** dans la liste, sélectionnez le niveau de chiffrement NSA Suite B à utiliser. La valeur par défaut est **GCM-128.** Les options possibles sont les suivantes :
  - **GCM-128** : utilise le chiffrement AES-GCM 128 bits.
  - **GCM-256 :** utilise le chiffrement AES-GCM 256 bits.
  - **GMAC-128 :** utilise le chiffrement AES-GMAC 128 bits.
  - **GMAC-256 :** utilise le chiffrement AES-GMAC 256 bits.
  - **Aucun :** le chiffrement n'est pas utilisé.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole générique pour Samsung SAFE

- **Nom d'hôte :** entrez le nom de l'hôte VPN. Cette option est requise.
- **Activer l'authentification utilisateur :** indiquez si l'authentification de l'utilisateur est exigée. Si cette option est activée, dans le champ **Mot de passe**, entrez le mot de passe utilisateur.
- **Nom d'utilisateur :** entrez un nom d'utilisateur.
- **Nom de paquetage de l'agent VPN :** nom du paquetage ou ID du VPN installé sur l'appareil ; par exemple, Mocana ou Pulse Secure.
- **Type de connexion VPN :** dans la liste, sélectionnez **IPSEC** ou **SSL** pour le type de connexion à utiliser. La valeur par défaut est **IPSEC**. Les sections suivantes décrivent les paramètres de configuration pour chaque type de connexion.

Configurer les paramètres de type de connexion IPSEC pour Samsung SAFE

- **Identité :** entrez un identifiant (facultatif) pour cette configuration.
- **Type d'ID de groupe IPsec :** dans la liste, sélectionnez le type d'ID de groupe IPsec à utiliser. La valeur par défaut est **Valeur par défaut**. Les options possibles sont les suivantes :
  - **Défaut**
  - **Adresse IPv4**
  - **Nom de domaine complet (FQDN)**
  - **Utilisateur FQDN**

  - **ID clé IKE**
- **Version IKE :** dans la liste, sélectionnez la version IKE à utiliser. Le paramètre par défaut est **IKEv1**
- **Méthode d'authentification :** dans la liste, sélectionnez la méthode d'authentification à utiliser. La valeur par défaut est **Certificat**. Les options possibles sont les suivantes :
  - **Certificat :** utilise l'authentification par certificat. Si cette option est sélectionnée, dans la liste **Infos d'identification de l'identité**, sélectionnez les informations d'identification à utiliser. La valeur par défaut est **Aucun**.
  - **Clé prépartagée :** utilise une clé prépartagée Si cette option est sélectionnée, dans le champ **Clé prépartagée**, entrez la clé du secret partagé.
  - **RSA Hybride :** utilise l'authentification hybride utilisant des certificats RSA
  - **EAP MD5 :** authentifie l'homologue EAP auprès du serveur EAP, mais pas d'authentification mutuelle.
  - **EAP MSCHAPv2 :** utilise l'authentification Challenge-Handshake de Microsoft pour l'authentification mutuelle.
  - **Authentification par carte d'accès commune :** utilise un accès CAC (Common Access Card) pour l'authentification.
- **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
- **Certificat CA :** dans la liste, sélectionnez le certificat à utiliser.
- **Activer la détection de perte des connexions :** indiquez s'il est nécessaire de contacter un homologue pour s'assurer qu'il reste actif. La valeur par défaut est **Désactivé**.
- **Activer l'itinéraire par défaut :** sélectionnez cette option pour activer un itinéraire par défaut vers le serveur VPN.
- **Activer l'option mobile :** sélectionnez cette option si vous souhaitez activer l'option mobile.
- **Durée de vie d'IKE en minutes :** entrez le nombre de minutes avant que la connexion VPN soit rétablie. Le paramètre par défaut est de 1440 minutes (24 heures).
- **Durée de vie d'IPSEC en minutes :** entrez le nombre de minutes avant que la connexion VPN soit rétablie. Le paramètre par défaut est de 1440 minutes (24 heures).
- **Valeur du groupe Diffie-Hellman (puissance de clé) :** dans la liste, sélectionnez la puissance de clé à utiliser. La valeur par défaut est **0**.
- **Mode d'échange de clés IKE Phase 1 :** sélectionnez **Principal** ou **Agressif** pour le mode de négociation IKE Phase 1. La valeur par défaut est **Principal**.
  - **Principal :** aucune information n'est exposée aux agresseurs potentiels, mais ce mode est plus lent que le mode **Agressif**.
  - **Agressif :** certaines informations (par exemple, l'identité des homologues de négociation) sont exposées aux agresseurs lors de la négociation, mais ce mode est plus rapide que le mode **Principal**.
- **Perfect forward secrecy (PFS) :** sélectionnez cette option si vous souhaitez utiliser PFS pour

exiger un nouvel échange de clés pour la renégociation d'une connexion.

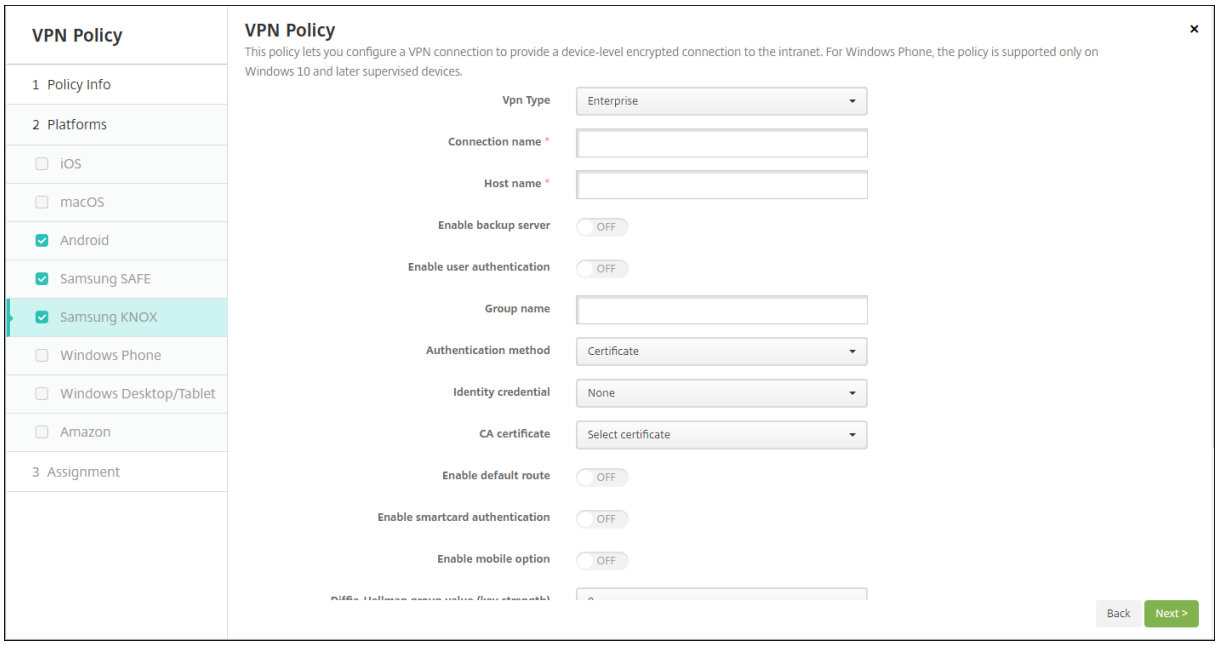
- **Type de tunnel de séparation :** dans la liste, sélectionnez le type de tunnel de séparation. Les options possibles sont les suivantes :
  - **Auto :** le tunnel de séparation est automatiquement utilisé.
  - **Manuel :** le tunnel de séparation est utilisé sur l'adresse IP et le port spécifié sur le serveur VPN.
  - **Désactivé :** le tunnel de séparation n'est pas utilisé.
- **Algorithme de chiffrement IPSEC :** configuration VPN utilisée par le protocole IPsec.
- **Algorithme de chiffrement IKE :** configuration VPN utilisée par le protocole IPsec.
- **Algorithme d'intégrité IKE :** configuration VPN utilisée par le protocole IPsec.
- **Constructeur :** profil personnel pour les agents génériques qui communiquent avec l'API Knox.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **VPN par application :** pour chaque connexion Per App VPN à ajouter, sélectionnez **Ajouter** et procédez comme suit :
  - **VPN par application :** configuration VPN que l'application utilise pour communiquer.
  - Cliquez sur **Enregistrer** pour enregistrer le Per App VPN ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer les paramètres de type de connexion SSL pour Samsung SAFE

- **Méthode d'authentification :** dans la liste, sélectionnez la méthode d'authentification à utiliser. La valeur par défaut est **Non applicable**. Les options possibles sont les suivantes :
  - **Sans objet**
  - **Certificat :** utilise l'authentification par certificat. Si cette option est sélectionnée, dans la liste **Infos d'identification de l'identité**, sélectionnez les informations d'identification à utiliser. La valeur par défaut est **Aucun**.
  - **Authentification par carte d'accès commune :** utilise un accès CAC (Common Access Card) pour l'authentification.
- **Certificat CA :** dans la liste, sélectionnez le certificat à utiliser.
- **Activer l'itinéraire par défaut :** sélectionnez cette option pour activer un itinéraire par défaut vers le serveur VPN.
- **Activer l'option mobile :** sélectionnez cette option si vous souhaitez activer l'option mobile.
- **Type de tunnel de séparation :** dans la liste, sélectionnez le type de tunnel de séparation. Les options possibles sont les suivantes :
  - **Auto :** le tunnel de séparation est automatiquement utilisé.
  - **Manuel :** le tunnel de séparation est utilisé sur l'adresse IP et le port spécifié sur le serveur

VPN.
  - **Désactivé :** le tunnel de séparation n'est pas utilisé.
- **Algorithme SSL :** entrez l'algorithme SSL à utiliser pour la négociation client-serveur.
- **Constructeur :** profil personnel pour les agents génériques qui communiquent avec l'API Knox.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **VPN par application :** pour chaque connexion Per App VPN à ajouter, sélectionnez **Ajouter** et procédez comme suit :
  - **VPN par application :** configuration VPN que l'application utilise pour communiquer.
  - Cliquez sur **Enregistrer** pour enregistrer le Per App VPN ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Paramètres Samsung Knox



Lorsque vous configurez une stratégie pour Samsung Knox, elle s'applique uniquement à l'intérieur du conteneur Samsung Knox.

- **Type de VPN :** dans la liste, sélectionnez le type de connexion VPN à configurer. La connexion peut être définie sur **Entreprise** (applicable aux versions Knox antérieures à 2.0) ou **Générique** (applicable aux versions Knox 2.0 ou ultérieures). La valeur par défaut est **Entreprise**.

Les sections suivantes répertorient les options de configuration pour chacun des types de connexion précédents.

Configurer le protocole Enterprise pour Samsung Knox

- **Nom de la connexion :** entrez un nom pour la connexion. Ce champ est obligatoire.
- **Nom d'hôte :** entrez le nom de l'hôte VPN. Cette option est requise.
- **Activer le serveur de sauvegarde :** sélectionnez cette option pour activer un serveur VPN de sauvegarde. Si cette option est activée, dans **Serveur VPN de sauvegarde**, entrez le nom de domaine complet ou l'adresse IP du serveur VPN de sauvegarde.
- **Activer l'authentification utilisateur :** indiquez si l'authentification de l'utilisateur est exigée. Si cette option est activée, vous pouvez configurer les paramètres suivants :
  - **Nom d'utilisateur :** entrez un nom d'utilisateur.
  - **Mot de passe :** entrez le mot de passe de l'utilisateur.
- **Nom du groupe :** entrez un nom de groupe (facultatif).
- **Méthode d'authentification :** dans la liste, sélectionnez la méthode d'authentification à utiliser. Les options possibles sont les suivantes :

  - **Certificat :** utilise l'authentification par certificat. Pour l'authentification par certificat, sélectionnez également les informations d'identification à utiliser dans la liste **Informations d'identification**.
  - **Clé prépartagée :** utilise une clé prépartagée Si cette option est sélectionnée, dans le champ **Clé prépartagée**, entrez la clé du secret partagé.
  - **RSA Hybride :** utilise l'authentification hybride utilisant des certificats RSA
  - **EAP MD5 :** authentifie l'homologue EAP auprès du serveur EAP, mais pas d'authentification mutuelle.
  - **EAP MSCHAPv2 :** utilise l'authentification Challenge-Handshake de Microsoft pour l'authentification mutuelle.
- **Certificat CA :** dans la liste, sélectionnez le certificat à utiliser.
- **Activer l'itinéraire par défaut :** sélectionnez cette option pour activer un itinéraire par défaut vers le serveur VPN.
- **Activer l'authentification par carte à puce :** sélectionnez cette option pour autoriser les utilisateurs à s'authentifier à l'aide de cartes à puce. La valeur par défaut est **Désactivé**.
- **Activer l'option mobile :** sélectionnez cette option si vous souhaitez activer l'option mobile.
- **Valeur du groupe Diffie-Hellman (puissance de clé) :** dans la liste, sélectionnez la puissance de clé à utiliser. La valeur par défaut est **0**.
- **Type de tunnel de séparation :** dans la liste, sélectionnez le type de tunnel de séparation. Les options possibles sont les suivantes :
  - **Auto :** le tunnel de séparation est automatiquement utilisé.
  - **Manuel :** le tunnel de séparation est utilisé sur l'adresse IP et le port spécifié sur le serveur VPN.
  - **Désactivé :** le tunnel de séparation n'est pas utilisé.
- **Type SuiteB :** dans la liste, sélectionnez le niveau de chiffrement NSA Suite B à utiliser. Les options possibles sont les suivantes :
  - **GCM-128 :** utilise le chiffrement AES-GCM 128 bits. Il s'agit de la valeur par défaut.
  - **GCM-256 :** utilise le chiffrement AES-GCM 256 bits.
  - **GMAC-128 :** utilise le chiffrement AES-GMAC 128 bits.
  - **GMAC-256 :** utilise le chiffrement AES-GMAC 256 bits.
  - **Aucun :** le chiffrement n'est pas utilisé.
- **Routes de transfert :** cliquez sur **Ajouter** pour ajouter des routes de transfert supplémentaires si votre serveur VPN d'entreprise prend en charge plusieurs tables de routage.

Configurer le protocole générique pour Samsung Knox

- **Nom de la connexion :** entrez un nom pour la connexion. Ce champ est obligatoire.
- **Nom de paquetage de l'agent VPN :** nom du paquetage ou ID du VPN installé sur l'appareil ; par exemple, Mocana ou Pulse Secure.
- **Nom d'hôte :** entrez le nom de l'hôte VPN. Cette option est requise.

- **Activer l'authentification utilisateur :** indiquez si l'authentification de l'utilisateur est exigée. Si cette option est activée, vous pouvez configurer les paramètres suivants :
  - **Nom d'utilisateur :** entrez un nom d'utilisateur.
  - **Mot de passe :** entrez le mot de passe de l'utilisateur.
- **Identité :** entrez un identifiant (facultatif) pour cette configuration. S'applique uniquement lorsque **Type de connexion VPN=IPSEC.**
- **Type de connexion VPN :** dans la liste, sélectionnez **IPSEC** ou **SSL** pour le type de connexion à utiliser. La valeur par défaut est **IPSEC**. Les sections suivantes décrivent les paramètres de configuration pour chaque type de connexion.
- **Configurer les paramètres de connexion à IPSEC**
  - **Type d'ID de groupe IPsec :** dans la liste, sélectionnez le type d'ID de groupe IPsec à utiliser. La valeur par défaut est **Valeur par défaut**. Les options possibles sont les suivantes :
    - **Défaut**
    - **Adresse IPv4**
    - **Nom de domaine complet (FQDN)**
    - **Utilisateur FQDN**
    - **ID clé IKE**
  - **Version IKE :** dans la liste, sélectionnez la version IKE à utiliser. Le paramètre par défaut est **IKEv1**
  - **Méthode d'authentification :** dans la liste, sélectionnez la méthode d'authentification à utiliser. La valeur par défaut est **Certificat**. Les options possibles sont les suivantes :
    - **Certificat :** utilise l'authentification par certificat. Si cette option est sélectionnée, dans la liste **Infos d'identification de l'identité**, sélectionnez les informations d'identification à utiliser. La valeur par défaut est **Aucun**.
    - **Clé prépartagée :** utilise une clé prépartagée Si cette option est sélectionnée, dans le champ **Clé prépartagée**, entrez la clé du secret partagé.
    - **RSA Hybride :** utilise l'authentification hybride utilisant des certificats RSA
    - **EAP MD5 :** authentifie l'homologue EAP auprès du serveur EAP, mais pas d'authentification mutuelle.
    - **EAP MSCHAPv2 :** utilise l'authentification Challenge-Handshake de Microsoft pour l'authentification mutuelle.
    - **Authentification par carte d'accès commune :** utilise un accès CAC (Common Access Card) pour l'authentification.
  - **Certificat CA :** dans la liste, sélectionnez le certificat à utiliser.
  - **Activer la détection de perte des connexions :** indiquez s'il est nécessaire de contacter un homologue pour s'assurer qu'il reste actif. La valeur par défaut est **Désactivé**.
  - **Activer l'itinéraire par défaut :** sélectionnez cette option pour activer un itinéraire par défaut vers le serveur VPN.

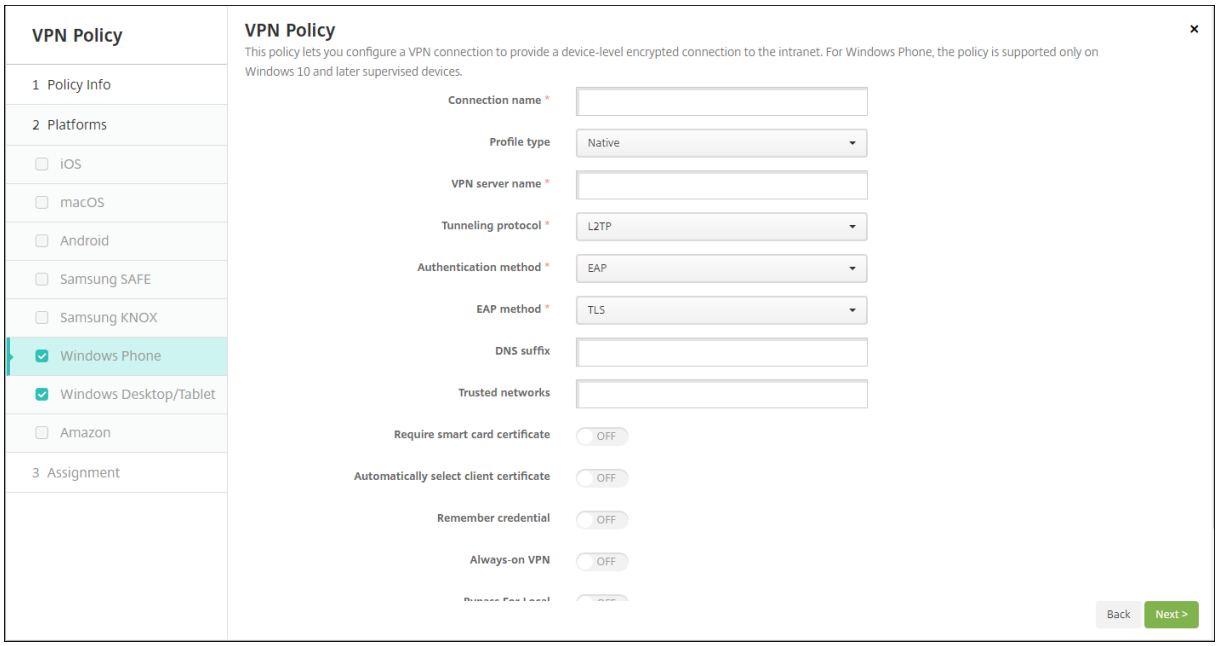
- **Activer l'option mobile :** sélectionnez cette option si vous souhaitez activer l'option mobile.
- **Durée de vie d'IKE en minutes :** entrez le nombre de minutes avant que la connexion VPN soit rétablie. Le paramètre par défaut est de 1440 minutes (24 heures).
- **Durée de vie d'IPSEC en minutes :** entrez le nombre de minutes avant que la connexion VPN soit rétablie. Le paramètre par défaut est de 1440 minutes (24 heures).
- **Valeur du groupe Diffie-Hellman (puissance de clé) :** dans la liste, sélectionnez la puissance de clé à utiliser. La valeur par défaut est **0**.
- **Mode d'échange de clés IKE Phase 1 :** sélectionnez **Principal** ou **Agressif** pour le mode de négociation IKE Phase 1. La valeur par défaut est **Principal**.
  * **Principal :** aucune information n'est exposée aux agresseurs potentiels, mais ce mode est plus lent que le mode **Agressif**.
  * **Agressif :** certaines informations (par exemple, l'identité des homologues de négociation) sont exposées aux agresseurs lors de la négociation, mais ce mode est plus rapide que le mode **Principal**.
- **Perfect forward secrecy (PFS) :** sélectionnez cette option si vous souhaitez utiliser PFS pour exiger un nouvel échange de clés pour la renégociation d'une connexion.
- **Type de tunnel de séparation :** dans la liste, sélectionnez le type de tunnel de séparation. Les options possibles sont les suivantes :
  * **Auto :** le tunnel de séparation est automatiquement utilisé.
  * **Manuel :** le tunnel de séparation est utilisé sur l'adresse IP et le port spécifié sur le serveur VPN.
  * **Désactivé :** le tunnel de séparation n'est pas utilisé.
- **Type SuiteB :** dans la liste, sélectionnez le niveau de chiffrement NSA Suite B à utiliser. La valeur par défaut est **GCM-128.** Les options possibles sont les suivantes :
  * **GCM-128** : utilise le chiffrement AES-GCM 128 bits.
  * **GCM-256 :** utilise le chiffrement AES-GCM 256 bits.
  * **GMAC-128 :** utilise le chiffrement AES-GMAC 128 bits.
  * **GMAC-256 :** utilise le chiffrement AES-GMAC 256 bits.
  * **Aucun :** le chiffrement n'est pas utilisé.
- **Algorithme de chiffrement IPSEC :** configuration VPN utilisée par le protocole IPsec.
- **Algorithme de chiffrement IKE :** configuration VPN utilisée par le protocole IPsec.
- **Algorithme d'intégrité IKE :** configuration VPN utilisée par le protocole IPsec.
- **Knox :** configurations pour Samsung Knox uniquement.
- **Constructeur :** profil personnel pour les agents génériques qui communiquent avec l'API Knox.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :

        * **Route de transfert :** entrez l'adresse IP de la route de transfert.
        * Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.
    - **VPN par application :** pour chaque connexion Per App VPN à ajouter, sélectionnez **Ajouter** et procédez comme suit :
        * **VPN par application :** configuration VPN que l'application utilise pour communiquer.
        * Cliquez sur **Enregistrer** pour enregistrer le Per App VPN ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **Configurer les paramètres de connexion à SSL**
    - **Méthode d'authentification :** dans la liste, cliquez sur la méthode d'authentification à utiliser. Les options possibles sont les suivantes :
        * **Non applicable :** aucune méthode d'authentification n'est appliquée. il s'agit du réglage par défaut.
        * **Certificat :** utilise l'authentification par certificat. il s'agit du réglage par défaut. Si cette option est sélectionnée, dans la liste Infos d'identification de l'identité, sélectionnez les informations d'identification à utiliser. La valeur par défaut est Aucun.
        * **Authentification par carte d'accès commune :** utilise un accès CAC (Common Access Card) pour l'authentification.
    - **Certificat CA :** dans la liste, sélectionnez le certificat à utiliser.
    - **Activer l'itinéraire par défaut :** sélectionnez cette option pour activer un itinéraire par défaut vers le serveur VPN.
    - **Activer l'option mobile :** sélectionnez cette option si vous souhaitez activer l'option mobile.
    - **Type de tunnel de séparation :** dans la liste, sélectionnez le type de tunnel de séparation. Les options possibles sont les suivantes :
        * **Auto :** le tunnel de séparation est automatiquement utilisé.
        * **Manuel :** le tunnel de séparation est utilisé sur l'adresse IP et le port spécifiés.
        * **Désactivé :** le tunnel de séparation n'est pas utilisé.
    - **Type SuiteB :** dans la liste, sélectionnez le niveau de chiffrement NSA Suite B à utiliser. La valeur par défaut est GCM-128. Les options possibles sont les suivantes :
        * **GCM-128** : utilise le chiffrement AES-GCM 128 bits.
        * **GCM-256 :** utilise le chiffrement AES-GCM 256 bits.
        * **GMAC-128 :** utilise le chiffrement AES-GMAC 128 bits.
        * **GMAC-256 :** utilise le chiffrement AES-GMAC 256 bits.
        * **Aucun : aucun chiffrement n'est utilisé :** entrez l'algorithme SSL à utiliser pour la négociation client-serveur.
    - **Algorithme SSL :** entrez l'algorithme SSL à utiliser pour la négociation client-serveur.
    - **Knox :** configurations pour Samsung Knox uniquement.
    - **Constructeur :** profil personnel pour les agents génériques qui communiquent avec l'API

Knox.

- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **VPN par application :** pour chaque connexion Per App VPN à ajouter, sélectionnez **Ajouter** et procédez comme suit :
  - **VPN par application :** configuration VPN que l'application utilise pour communiquer.
  - Cliquez sur **Enregistrer** pour enregistrer le Per App VPN ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Paramètres Windows Phone



Ces paramètres sont uniquement pris en charge sur les téléphones supervisés Windows 10 et versions ultérieures.

- **Nom de la connexion :** entrez un nom pour la connexion Ce champ est obligatoire.
- **Type de profil :** dans la liste, sélectionnez **Natif** ou **Plug-in**. La valeur par défaut est **Natif**. Les sections suivantes expliquent les paramètres de chacune de ces options.
- **Configurer les paramètres du type de profil natif :** ces paramètres s'appliquent au VPN intégré aux téléphones Windows des utilisateurs.
  - **Nom du serveur VPN :** entrez le nom de domaine complet ou l'adresse IP du serveur VPN. Ce champ est obligatoire.

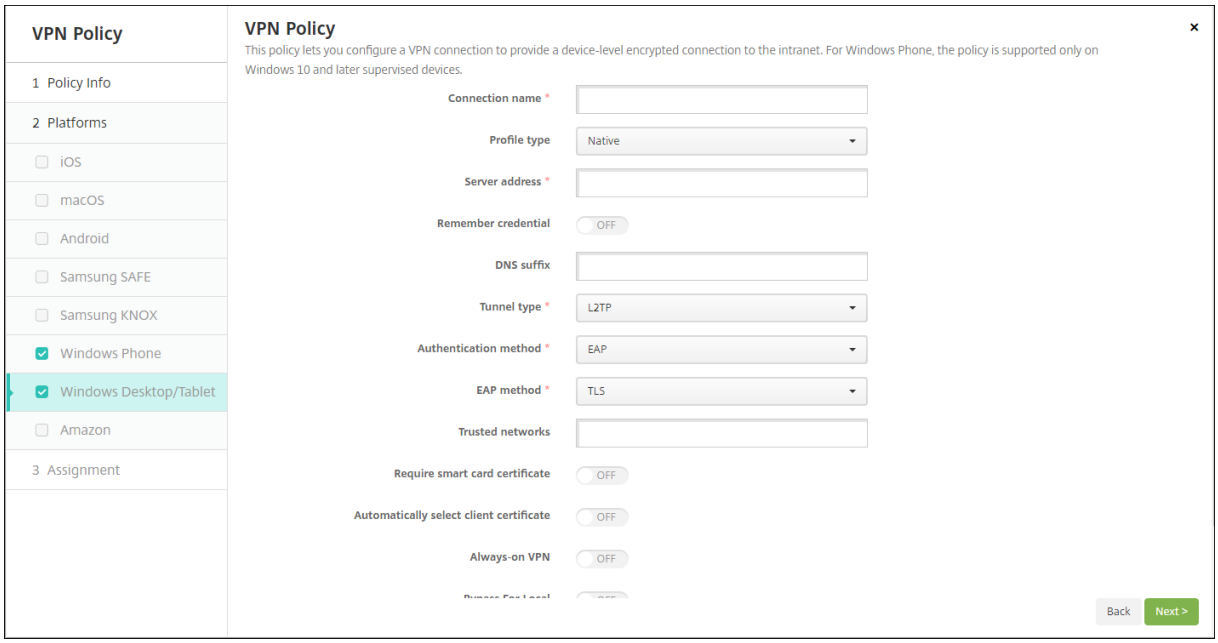
- **Protocole de tunneling :** dans la liste, sélectionnez le type de tunnel VPN à utiliser. La valeur par défaut est **L2TP**. Les options possibles sont les suivantes :
  - **L2TP :** Layer 2 Tunneling Protocol avec authentification par clé pré-partagée.
  - **PPTP :** protocole PPTP.
  - **IKEv2 :** Internet Key Exchange version 2.
- **Méthode d'authentification :** dans la liste, sélectionnez la méthode d'authentification à utiliser. La valeur par défaut est **EAP**. Les options possibles sont les suivantes :
  - **EAP :** protocole d'authentification étendue.
  - **MSChapV2 :** utilise l'authentification Challenge-Handshake de Microsoft pour l'authentification mutuelle. Cette option n'est pas disponible lorsque vous sélectionnez IKEv2 pour le type de tunnel. Lorsque vous choisissez MSChapV2, une option **Utiliser automatiquement les informations d'identification Windows** s'affiche. La valeur par défaut est **Désactivé**.
- **Méthode EAP :** dans la liste, sélectionnez la méthode EAP à utiliser. La valeur par défaut est **TLS**. Ce champ n'est pas disponible lorsque l'authentification MSChapV2 est activée. Les options possibles sont les suivantes :
  - **TLS :** Transport Layer Security
  - **PEAP :** Protected Extensible Authentication Protocol
- **Suffixe DNS :** entrez le suffixe DNS.
- **Réseaux approuvés :** entrez une liste de réseaux séparés par des virgules qui ne nécessitent pas de connexion VPN pour l'accès. Par exemple, lorsque les utilisateurs se trouvent sur le réseau sans fil de votre entreprise, ils peuvent accéder directement aux ressources protégées.
- **Exiger un certificat de carte à puce :** sélectionnez cette option pour exiger un certificat de carte à puce. La valeur par défaut est Désactivé.
- **Sélectionner automatiquement le certificat client :** sélectionnez cette option pour choisir automatiquement le certificat client à utiliser pour l'authentification. La valeur par défaut est Désactivé. Cette option n'est pas disponible lorsque Exiger un certificat de carte à puce est activé.
- **Mémoriser les informations d'identification :** sélectionnez cette option si vous souhaitez mettre en cache les informations d'identification. La valeur par défaut est Désactivé. Lorsque cette option est activée, les informations d'identification sont mises en cache dès que possible.
- **VPN toujours connecté :** sélectionnez cette option pour spécifier si la connexion VPN est toujours activée. La valeur par défaut est Désactivé. Lorsque cette option est activée, la connexion VPN reste active jusqu'à ce que l'utilisateur se déconnecte manuellement.
- **Ne pas utiliser le VPN pour les adresses locales :** entrez l'adresse et le numéro de port pour permettre à des ressources locales pour contourner le serveur proxy.

• **Configurer les paramètres du type de profil plug-in :** ces paramètres s'appliquent aux plug-

ins VPN obtenus à partir du Windows Store et installés sur les appareils des utilisateurs.

- **Adresse du serveur :** entrez l'URL, le nom d'hôte ou l'adresse IP du serveur VPN.
- **ID de l'application cliente :** entrez le nom de famille du package pour le plug-in VPN.
- **XML du profil du plug-in :** sélectionnez le profil de plug-in VPN personnalisé en cliquant sur **Parcourir** et accédez à l'emplacement du fichier. Contactez le fournisseur du plug-in pour des informations sur le format et plus de détails.
- **Suffixe DNS :** entrez le suffixe DNS.
- **Réseaux approuvés :** entrez une liste de réseaux séparés par des virgules qui ne nécessitent pas de connexion VPN pour l'accès. Par exemple, lorsque les utilisateurs se trouvent sur le réseau sans fil de votre entreprise, ils peuvent accéder directement aux ressources protégées.
- **Mémoriser les informations d'identification :** sélectionnez cette option si vous souhaitez mettre en cache les informations d'identification. La valeur par défaut est Désactivé. Lorsque cette option est activée, les informations d'identification sont mises en cache dès que possible.
- **VPN toujours connecté :** sélectionnez cette option pour spécifier si la connexion VPN est toujours activée. La valeur par défaut est Désactivé. Lorsque cette option est activée, la connexion VPN reste active jusqu'à ce que l'utilisateur se déconnecte manuellement.
- **Ne pas utiliser le VPN pour les adresses locales :** entrez l'adresse et le numéro de port pour permettre à des ressources locales pour contourner le serveur proxy.

Paramètres Windows Desktop/Tablet

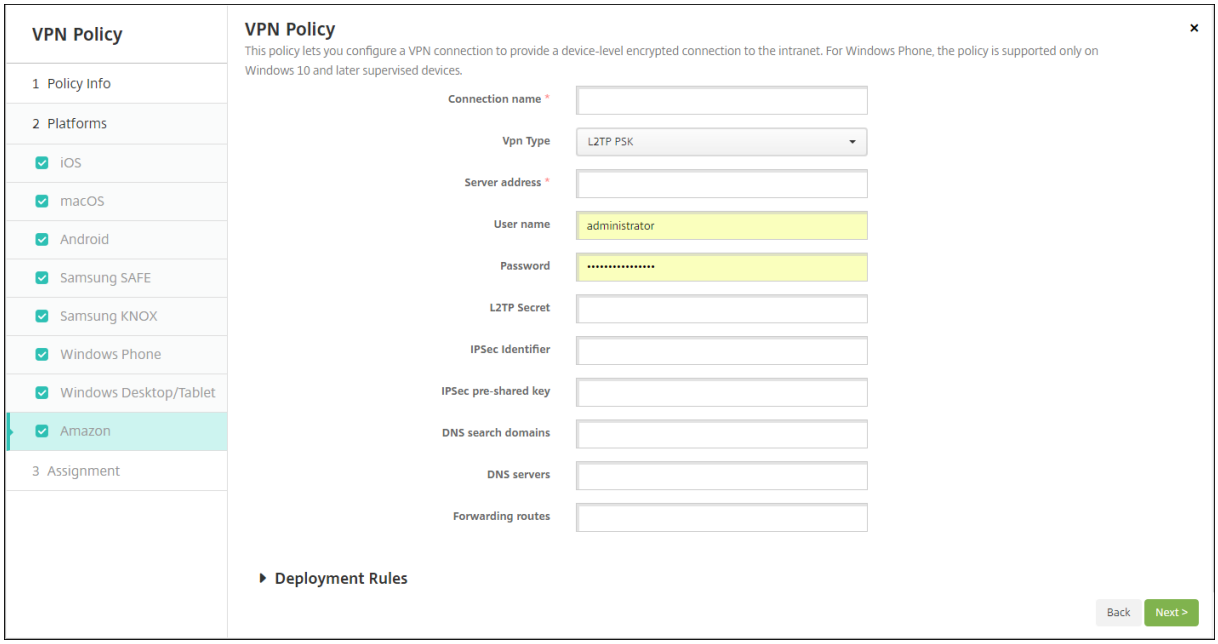


- **Nom de la connexion :** entrez un nom pour la connexion Ce champ est obligatoire.

- **Type de profil :** dans la liste, sélectionnez **Natif** ou **Plug-in**. La valeur par défaut est **Natif**.
- **Configurer le type de profil natif :** ces paramètres s'appliquent au VPN intégré aux appareils Windows des utilisateurs.
  - **Adresse du serveur :** entrez le nom de domaine complet ou l'adresse IP du serveur VPN. Ce champ est obligatoire.
  - **Mémoriser les informations d'identification :** sélectionnez cette option si vous souhaitez mettre en cache les informations d'identification. La valeur par défaut est **Désactivé**. Lorsque cette option est activée, les informations d'identification sont mises en cache dès que possible.
  - **Suffixe DNS :** entrez le suffixe DNS.
  - **Type de tunnel :** dans la liste, sélectionnez le type de tunnel VPN à utiliser. La valeur par défaut est **L2TP**. Les options possibles sont les suivantes :
    - **L2TP :** Layer 2 Tunneling Protocol avec authentification par clé pré-partagée.
    - **PPTP :** protocole PPTP.
    - **IKEv2 :** Internet Key Exchange version 2.
  - **Méthode d'authentification :** dans la liste, sélectionnez la méthode d'authentification à utiliser. La valeur par défaut est **EAP**. Les options possibles sont les suivantes :
    - **EAP :** protocole d'authentification étendue.
    - **MSChapV2 :** utilise l'authentification Challenge-Handshake de Microsoft pour l'authentification mutuelle. Cette option n'est pas disponible lorsque vous sélectionnez **IKEv2** pour le type de tunnel.
  - **Méthode EAP :** dans la liste, sélectionnez la méthode EAP à utiliser. La valeur par défaut est **TLS**. Ce champ n'est pas disponible lorsque l'authentification MSChapV2 est activée. Les options possibles sont les suivantes :
    - **TLS :** Transport Layer Security
    - **PEAP :** Protected Extensible Authentication Protocol
  - **Réseaux approuvés :** entrez une liste de réseaux séparés par des virgules qui ne nécessitent pas de connexion VPN pour l'accès. Par exemple, lorsque les utilisateurs se trouvent sur le réseau sans fil de votre entreprise, ils peuvent accéder directement aux ressources protégées.
  - **Exiger un certificat de carte à puce :** sélectionnez cette option pour exiger un certificat de carte à puce. La valeur par défaut est **Désactivé**.
  - **Sélectionner automatiquement le certificat client :** sélectionnez cette option pour choisir automatiquement le certificat client à utiliser pour l'authentification. La valeur par défaut est **Désactivé**. Cette option n'est pas disponible lorsque vous activez **Exiger un certificat de carte à puce**.
  - **VPN toujours connecté :** sélectionnez cette option pour spécifier si la connexion VPN est toujours activée. La valeur par défaut est **Désactivé**. Lorsque cette option est activée, la connexion VPN reste active jusqu'à ce que l'utilisateur se déconnecte manuellement.

  - **Ne pas utiliser le VPN pour les adresses locales :** entrez l'adresse et le numéro de port pour permettre à des ressources locales pour contourner le serveur proxy.
- **Configurer les paramètres du type de profil plug-in :** ces paramètres s'appliquent aux plug-ins VPN obtenus à partir du Windows Store et installés sur les appareils des utilisateurs.
  - **Adresse du serveur :** entrez le nom de domaine complet ou l'adresse IP du serveur VPN. Ce champ est obligatoire.
  - **Mémoriser les informations d'identification :** sélectionnez cette option si vous souhaitez mettre en cache les informations d'identification. La valeur par défaut est **Désactivé**. Lorsque cette option est activée, les informations d'identification sont mises en cache dès que possible.
  - **Suffixe DNS :** entrez le suffixe DNS.
  - **ID de l'application cliente :** entrez le nom de famille du package pour le plug-in VPN.
  - **XML du profil du plug-in :** sélectionnez le profil de plug-in VPN personnalisé en cliquant sur **Parcourir** et accédez à l'emplacement du fichier. Contactez le fournisseur du plug-in pour des informations sur le format et plus de détails.
  - **Réseaux approuvés :** entrez une liste de réseaux séparés par des virgules qui ne nécessitent pas de connexion VPN pour l'accès. Par exemple, lorsque les utilisateurs se trouvent sur le réseau sans fil de votre entreprise, ils peuvent accéder directement aux ressources protégées.
  - **VPN toujours connecté :** sélectionnez cette option pour spécifier si la connexion VPN est toujours activée. La valeur par défaut est **Désactivé**. Lorsque cette option est activée, la connexion VPN reste active jusqu'à ce que l'utilisateur se déconnecte manuellement.
  - **Ne pas utiliser le VPN pour les adresses locales :** entrez l'adresse et le numéro de port pour permettre à des ressources locales pour contourner le serveur proxy.

Paramètres Amazon



- **Nom de la connexion :** entrez un nom pour la connexion
- **Type de VPN :** sélectionnez le type de connexion. Les options possibles sont les suivantes :
  - **L2TP PSK :** Layer 2 Tunneling Protocol (L2TP) avec authentification par clé pré-partagée. il s'agit du réglage par défaut.
  - **L2TP RSA :** Layer 2 Tunneling Protocol avec authentification RSA.
  - **IPSEC XAUTH PSK :** Internet Protocol Security (IPSec) avec clé pré-partagée et authentification étendue
  - **IPSEC HYBRID RSA :** Internet Protocol Security (IPSec) avec authentification RSA hybride
  - **PPTP :** protocole PPTP.

Les sections suivantes répertorient les options de configuration pour chacun des types de connexion précédents.

Configurer les paramètres L2TP PSK pour Amazon

- **Adresse du serveur :** entrez l'adresse IP du serveur VPN.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Secret L2TP :** entrez la clé du secret partagé.
- **Identificateur IPSec :** entrez le nom de la connexion VPN que les utilisateurs voient sur leurs appareils lors de la connexion.
- **Clé pré-partagée IPSec :** entrez la clé secrète.
- **Domaines de recherche DNS :** entrez les domaines avec lesquels la liste des domaines de recherche de l'appareil d'un utilisateur peut effectuer une correspondance.

- **Serveurs DNS :** entrez les adresses IP des serveurs DNS à utiliser pour résoudre les domaines spécifiés.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer les paramètres L2TP RSA pour Amazon

- **Adresse du serveur :** entrez l'adresse IP du serveur VPN.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Secret L2TP :** entrez la clé du secret partagé.
- **Domaines de recherche DNS :** entrez les domaines avec lesquels la liste des domaines de recherche de l'appareil d'un utilisateur peut effectuer une correspondance.
- **Serveurs DNS :** entrez les adresses IP des serveurs DNS à utiliser pour résoudre les domaines spécifiés.
- **Certificat serveur :** dans la liste, sélectionnez le certificat serveur à utiliser.
- **Certificat CA :** dans la liste, sélectionnez le certificat CA à utiliser.
- **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer les paramètres IPSEC XAUTH PSK pour Amazon

- **Adresse du serveur :** entrez l'adresse IP du serveur VPN.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Identificateur IPSec :** entrez le nom de la connexion VPN que les utilisateurs voient sur leurs appareils lors de la connexion.
- **Clé pré-partagée IPSec :** entrez la clé de secret partagé.
- **Domaines de recherche DNS :** entrez les domaines avec lesquels la liste des domaines de recherche de l'appareil d'un utilisateur peut effectuer une correspondance.
- **Serveurs DNS :** entrez les adresses IP des serveurs DNS à utiliser pour résoudre les domaines spécifiés.

- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer les paramètres IPSEC AUTH RSA pour Amazon

- **Adresse du serveur :** entrez l'adresse IP du serveur VPN.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Domaines de recherche DNS :** entrez les domaines avec lesquels la liste des domaines de recherche de l'appareil d'un utilisateur peut effectuer une correspondance.
- **Serveurs DNS :** entrez les adresses IP des serveurs DNS à utiliser pour résoudre les domaines spécifiés.
- **Certificat serveur :** dans la liste, sélectionnez le certificat serveur à utiliser.
- **Certificat CA :** dans la liste, sélectionnez le certificat CA à utiliser.
- **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer les paramètres IPSEC HYBRID RSA pour Amazon

- **Adresse du serveur :** entrez l'adresse IP du serveur VPN.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Domaines de recherche DNS :** entrez les domaines avec lesquels la liste des domaines de recherche de l'appareil d'un utilisateur peut effectuer une correspondance.
- **Serveurs DNS :** entrez les adresses IP des serveurs DNS à utiliser pour résoudre les domaines spécifiés.
- **Certificat serveur :** dans la liste, sélectionnez le certificat serveur à utiliser.
- **Certificat CA :** dans la liste, sélectionnez le certificat CA à utiliser.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.

- Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer les paramètres PPTP pour Amazon

- **Adresse du serveur :** entrez l'adresse IP du serveur VPN.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Domaines de recherche DNS :** entrez les domaines avec lesquels la liste des domaines de recherche de l'appareil d'un utilisateur peut effectuer une correspondance.
- **Serveurs DNS :** entrez les adresses IP des serveurs DNS à utiliser pour résoudre les domaines spécifiés.
- **Cryptage PPP (MPPE) :** sélectionnez cette option si vous souhaitez activer le cryptage de données avec Microsoft Point-to-Point Encryption (MPPE). La valeur par défaut est **Désactivé**.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Stratégie de fond d'écran

August 18, 2021

Vous pouvez ajouter un fichier .png ou .jpg en tant que fond d'écran sur l'écran d'accueil, l'écran de verrouillage ou les deux. Disponible dans iOS 7.1.2 et versions ultérieures pour les appareils supervisés uniquement. Pour utiliser un fond d'écran différent sur iPad et iPhone, vous devez créer différentes stratégies de fond d'écran et les déployer vers les utilisateurs appropriés.

Le tableau suivant répertorie les dimensions d'image recommandées par Apple pour les appareils iOS.

iPhone

Appareil	Dimensions d'image en pixels
iPhone 12 Pro Max	2 778 x 1 284
iPhone 12 et iPhone 12 Pro	2 532 x 1 170
iPhone 12 Mini	2 340 x 1 080

Appareil	Dimensions d'image en pixels
iPhone 11 Max	2 688 x 1 242
iPhone 11 Pro	2 436 x 1 125
iPhone 11	1 792 x 828
iPhone XS Max	2 688 x 1 242
iPhone X, XS	2 436 x 1 125
iPhone XR	1 792 x 828
iPhone SE 2e génération	1 334 x 750
iPhone 7 Plus, 8 Plus	2 208 x 1 242
iPhone 7, 8	1 334 x 750
iPhone 8 Plus	1 334 x 750
iPhone 8	1 334 x 750

iPad

Appareil	Dimensions d'image en pixels
iPad Pro (1re, 2e et 3e génération 12,9 pouces)	2732 x 2048
iPad Pro 10,5 pouces	2224 x 1668
iPad Pro (9,7 pouces)	1 536 x 2 048
iPad Air 2	2 048 x 1 536

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Appliquer à :** dans la liste, sélectionnez **Écran de verrouillage**, **Ecran d'accueil (liste d'icônes)** ou **Écrans d'accueil et de verrouillage** pour définir si le fond d'écran doit apparaître
- **Fichier de fond d'écran :** sélectionnez le fichier de fond d'écran, en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

Stratégie de filtre de contenu Web

January 10, 2022

Vous pouvez ajouter une stratégie dans XenMobile destinée à filtrer le contenu Web sur les appareils iOS à l'aide de la fonction de filtrage automatique d'Apple en conjonction avec les sites spécifiques que vous ajoutez aux listes d'autorisation et de blocage. Cette stratégie est uniquement disponible sur les appareils iOS 7.0 et versions ultérieures en mode Supervisé. Pour de plus amples informations sur le placement d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Type de filtre :** dans la liste, cliquez sur **Intégré** ou **Plug-in**, puis suivez les procédures ci-dessous pour l'option que vous choisissez. La valeur par défaut est **Intégré**.

Type de filtre Intégré

- **Filtre de contenu Web**
  - **Filtrage automatique activé :** sélectionnez cette option pour spécifier si vous souhaitez utiliser la fonction de filtrage automatique d'Apple afin de détecter tout contenu inapproprié sur les sites Web. La valeur par défaut est **Désactivé**.
  - **URL autorisées :** cette liste est ignorée lorsque l'option **Filtrage automatique activé** est définie sur **Désactivé**. Lorsque l'option **Filtrage automatique activé** est définie sur **Activé**, les éléments figurant dans cette liste sont toujours accessibles, que le filtrage automatique en permette l'accès ou non. Pour chaque adresse URL que vous souhaitez ajouter à la liste d'autorisation, cliquez sur **Ajouter** et procédez comme suit :
    * Entrez l'adresse URL du site Web autorisé. Vous devez ajouter `http://` ou `https://` avant l'adresse Web.
    * Cliquez sur **Enregistrer** pour enregistrer le site Web dans la liste d'autorisation ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **URL sur liste noire :** les éléments dans cette liste sont toujours bloqués. Pour chaque adresse URL que vous souhaitez ajouter à la liste de blocage, cliquez sur **Ajouter** et procédez comme suit :
    * Entrez l'adresse URL du site Web à bloquer. Vous devez ajouter `http://` ou `https://` avant l'adresse Web.

        * Cliquez sur **Enregistrer** pour enregistrer le site Web dans la liste de blocage ou cliquez sur **Annuler** pour ne pas l'enregistrer.

          > **Remarque :**
          > La console XenMobile Server utilise les termes « liste noire » et « liste blanche ». Ces termes seront modifiés dans une prochaine version et les termes « liste de blocage » et « liste d'autorisation » les remplaceront.

- **Liste blanche signets**
  - **Liste blanche signets :** spécifie les sites auxquels les utilisateurs peuvent accéder. Pour activer l'accès aux sites web, ajoutez leur adresse URL.
    * **URL :** URL de chaque site Web auquel les utilisateurs peuvent accéder. Par exemple, pour activer l'accès au magasin Secure Hub, ajoutez l'URL de XenMobile Server à la liste des **URL**. Vous devez ajouter `http://` ou `https://` avant l'adresse Web. Ce champ est obligatoire.
    * **Dossier de signets :** entrez un nom de dossier des signets (facultatif). Si ce champ est vide, le signet est ajouté au répertoire de signets par défaut.
    * **Titre :** entrez un titre descriptif pour le site Web. Par exemple, tapez « Google » pour l'adresse URL `https://google.com`.
    * Cliquez sur **Enregistrer** pour enregistrer le site Web dans la liste d'autorisation ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Type de filtre Plug-in

- **Nom du filtre :** entrez un nom unique pour le filtre.
- **Identifiant :** entrez le Bundle ID du plug-in qui fournit le service de filtrage.
- **Adresse du service :** entrez une adresse de serveur (facultatif). Les formats valides sont une adresse IP, un nom d'hôte ou une adresse URL.
- **Nom d'utilisateur :** entrez un nom d'utilisateur pour le service (facultatif).
- **Mot de passe :** entrez un mot de passe pour le service (facultatif).
- **Certificat :** dans la liste, cliquez sur un certificat d'identité (facultatif) à utiliser pour authentifier l'utilisateur auprès du service. La valeur par défaut est **Aucun**.
- **Filtrer le trafic WebKit :** sélectionnez cette option si vous voulez filtrer le trafic WebKit.
- **Filtrer le trafic de socket :** sélectionnez cette option si vous voulez filtrer le trafic de socket.
- **Données personnalisées :** pour chaque clé personnalisée que vous souhaitez ajouter au filtre Web, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Clé :** entrez la clé personnalisée.
  - **Valeur :** entrez une valeur pour la clé personnalisée.
  - Cliquez sur **Enregistrer** pour enregistrer la clé personnalisée ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **Paramètres de stratégie**

- **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
  - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Stratégie de clip Web

January 10, 2022

Vous pouvez placer des raccourcis ou clips Web sur des sites Web de manière à ce qu'ils apparaissent à côté des applications sur les appareils des utilisateurs. Vous pouvez spécifier vos propres icônes pour représenter les clips Web sur des appareils iOS, iPadOS, macOS et Android. Windows Tablet requiert uniquement un libellé et une adresse URL. Pour les appareils iOS et iPadOS, configurez la stratégie Disposition de l'écran d'accueil pour organiser les clips Web que vous créez. Si vous restreignez l'accès aux applications sur iOS, assurez-vous de configurer la stratégie de restrictions pour autoriser les clips Web. Pour plus d'informations sur la configuration de ces stratégies, voir Stratégie Disposition de l'écran d'accueil et Stratégie Restrictions.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Étiquette :** entrez l'étiquette qui s'affichera avec le clip Web.
- **URL :** entrez l'adresse URL associée avec le clip Web. L'adresse URL doit commencer par un protocole, par exemple, `https://server`.
- **Amovible :** indiquez si les utilisateurs peuvent supprimer le clip Web. La valeur par défaut est **Désactivé**.
- **Icône à mettre à jour :** sélectionnez l'icône à utiliser pour le clip Web en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.
- **Icône précomposée :** indiquez si des effets doivent être appliqués à cette icône (coins arrondis, ombre portée et brillant réflectif). La valeur par défaut est **Désactivé**, ce qui ajoute des effets.
- **Plein écran :** indiquez si la page Web associée s'ouvre en mode plein écran. La valeur par défaut est **Désactivé**.

- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres macOS

- **Étiquette :** entrez l'étiquette qui s'affichera avec le clip Web.
- **URL :** entrez l'adresse URL associée avec le clip Web. L'adresse URL doit commencer par un protocole, par exemple, `https://server`.
- **Icône à mettre à jour :** sélectionnez l'icône à utiliser pour le clip Web en cliquant sur Parcourir et en accédant à l'emplacement du fichier.

Paramètres Android

- **Règle :** indiquez si cette stratégie ajoute ou supprime un clip Web. La valeur par défaut est **Ajouter**.
- **Étiquette :** entrez l'étiquette qui s'affichera avec le clip Web.
- **URL :** entrez l'adresse URL associée avec le clip Web.
- **Définir une icône :** indiquez si vous souhaitez utiliser un fichier d'icône. La valeur par défaut est **Désactivé**.
- **Fichier icône :** si **Définir une icône** est réglé sur **Activé**, sélectionnez le fichier d'icône à utiliser en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.

- **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
- **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Paramètres Windows Desktop/Tablet

- **Nom :** entrez le libellé qui s'affichera avec le clip Web.
- **URL :** entrez l'adresse URL associée avec le clip Web.

Stratégie Wi-Fi

January 10, 2022

Vous pouvez créer ou modifier des stratégies Wi-Fi dans XenMobile sur la page **Configurer > Stratégies d'appareil**. Les stratégies Wi-Fi vous permettent de gérer la manière dont les utilisateurs connectent leurs appareils à des réseaux Wi-Fi en définissant les éléments suivants :

- Noms et types de réseau
- Stratégies d'authentification et de sécurité
- Utilisation de serveur proxy
- Autres détails liés au Wi-Fi

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

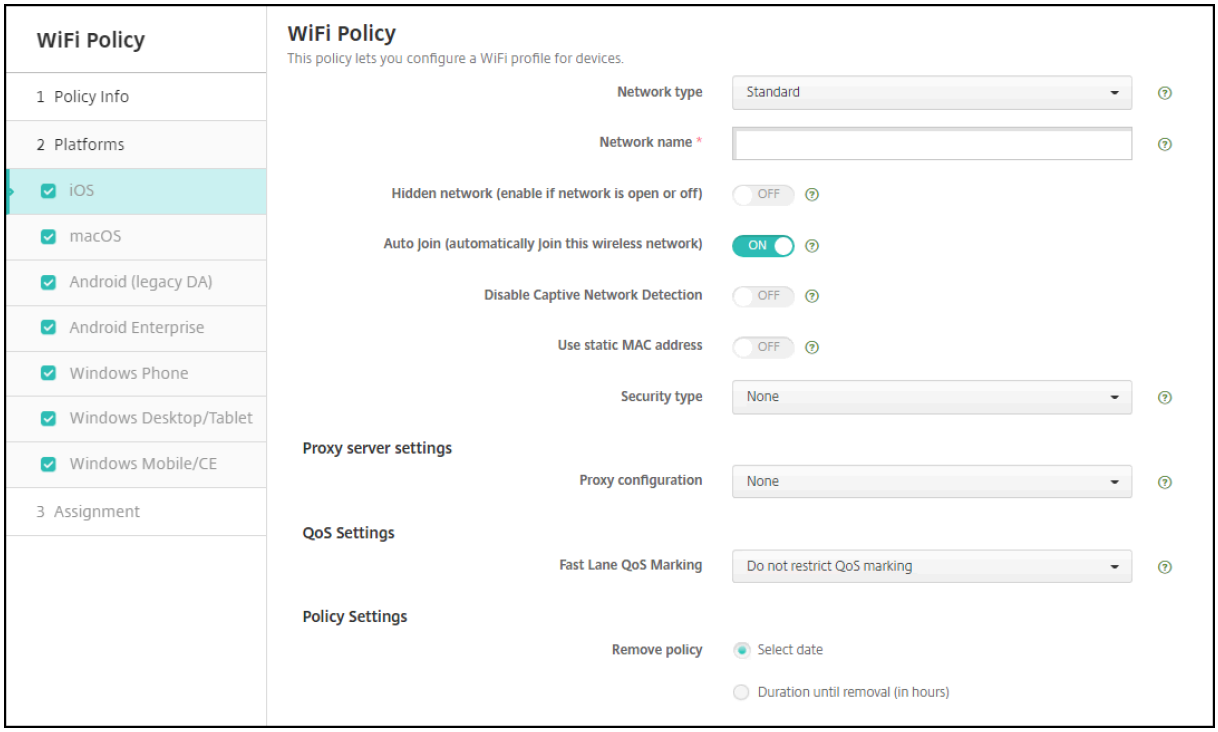
Conditions préalables

Avant de créer une stratégie, vous devez effectuer les étapes suivantes :

- Créer les groupes de mise à disposition que vous voulez utiliser.
- Notez le nom et type de réseau.
- Déterminez les types d'authentification ou de sécurité que vous voulez utiliser.
- Déterminez les informations de serveur proxy dont vous avez besoin.
- Installer les certificats d'autorité de certification nécessaires.
- Vérifiez que vous disposez des clés partagées nécessaires.
- Créez l'entité PKI pour l'authentification par certificat.
- Configurez les fournisseurs d'informations d'identification.

Pour de plus amples informations, consultez la section Authentification et ses sous-articles.

Paramètres iOS



- **Type de réseau :** dans la liste, cliquez sur **Standard**, **Point d'accès d'ancienne génération** ou **Hotspot 2.0** pour définir le type de réseau que vous voulez utiliser.
- **Nom du réseau :** entrez le SSID qui est affiché dans la liste des réseaux disponibles pour l'appareil. Ne s'applique pas à **Hotspot 2.0**.
- **Réseau masqué (activer si le réseau est ouvert ou désactivé) :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Rejoindre automatiquement (Rejoindre automatiquement ce réseau sans fil) :** sélectionnez cette option pour spécifier si le réseau est rejoint automatiquement. Si un appareil iOS est déjà connecté à un autre réseau, il ne rejoint pas ce réseau. L'utilisateur doit se déconnecter du réseau précédent avant que l'appareil ne se connecte automatiquement. La valeur par défaut est **Activé**.
- **Utiliser adresse MAC statique :** les adresses MAC sont des identifiants uniques qu'un appareil transmet au sein d'un réseau. Pour améliorer la confidentialité, les appareils iOS et iPadOS peuvent utiliser une adresse MAC différente chaque fois qu'ils se connectent à un réseau. Si cette option est **activée**, l'appareil utilise toujours la même adresse MAC lors de la connexion à ce réseau. Si cette option est **désactivée**, l'appareil utilise une adresse MAC différente chaque fois qu'il se connecte à ce réseau. La valeur par défaut est **Désactivé**.
- **Type de sécurité :** dans la liste, choisissez le type de sécurité que vous voulez utiliser. Ne s'applique pas à **Hotspot 2.0**.

  - Aucun : ne requiert aucune configuration supplémentaire.
  - WEP
  - WPA/WPA2 Personnel
  - Tous (Personnel)
  - WEP Enterprise
  - WPA/WPA2 Enterprise : l'utilisation de WPA-2 Entreprise nécessite que vous configuriez le protocole SCEP (Protocole d'inscription de certificats simple). XenMobile peut ensuite envoyer le certificat aux appareils pour l'authentification auprès du serveur Wi-Fi. Pour configurer SCEP, accédez à la page Distribution dans **Paramètres > Fournisseurs d'informations d'identification**. Pour de plus amples informations, consultez la section Fournisseurs d'identités.
  - Tous (Entreprise)

Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.

Paramètres WPA, WPA Personnel, Tous (Personnel) pour iOS

Mot de passe : entrez un mot de passe (facultatif). Si vous laissez ce champ vide, les utilisateurs peuvent être invités à entrer leurs mots de passe lorsqu'ils ouvrent une session.

Paramètres WEP Entreprise, WPA Entreprise, WPA2 Entreprise, Tous (Entreprise) pour iOS

Lorsque vous sélectionnez l'un de ces paramètres, leurs paramètres sont répertoriés après **Paramètres du serveur proxy**.

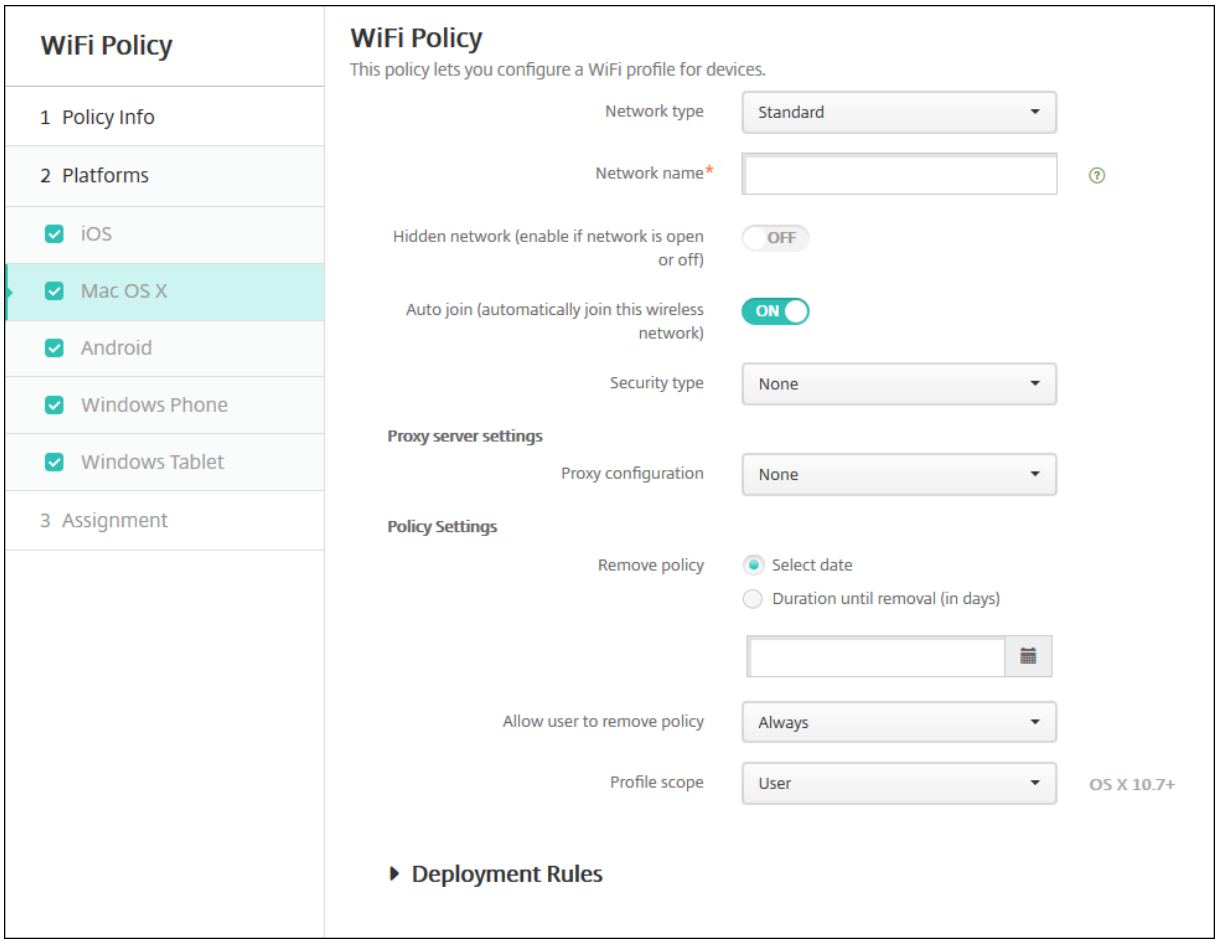
- **Protocoles, types EAP acceptés :** activez les types EAP que vous souhaitez prendre en charge, puis configurez les paramètres associés. La valeur par défaut est **Désactivé** pour chaque type EAP disponible.
- **Authentification interne (TTLS) :** *requis uniquement lorsque vous activez TTLS*. Dans la liste, choisissez la méthode d'authentification interne à utiliser. Les options possibles sont : **PAP**, **CHAP**, **MSCHAP** ou **MSCHAPv2**. La valeur par défaut est **MSCHAPv2**.
- **Protocoles, EAP-FAST :** indiquez si vous souhaitez utiliser les informations d'identification d'accès protégé (PAC).
  - Si vous sélectionnez **Utiliser PAC**, indiquez si vous voulez utiliser un provisioning de PAC.
    * Si vous sélectionnez **Provisioning de PAC**, indiquez si vous souhaitez autoriser une négociation TLS anonyme entre le client et XenMobile.
      · **Provisioning du PAC de manière anonyme**
- **Authentification :**
  - **Nom d'utilisateur :** entrez un nom d'utilisateur.
  - **Mot de passe par connexion :** indiquez si un mot de passe sera exigé chaque fois que les utilisateurs ouvriront une session.

  - **Mot de passe :** entrez un mot de passe (facultatif). Si vous laissez ce champ vide, les utilisateurs peuvent être invités à entrer leurs mots de passe lorsqu'ils ouvrent une session.
  - **Infos d'identification de l'identité (infos d'identification magasin de clés ou PKI) :** dans la liste, cliquez sur le type d'informations d'identification de l'identité. La valeur par défaut est **Aucun**.
  - **Identité externe :** *requis uniquement lorsque vous activez* **PEAP**, **TTLS** *ou* **EAP-FAST**. Entrez le nom d'utilisateur visible en externe. Vous pouvez augmenter la sécurité en tapant un terme générique comme « anonyme » de façon à ce que le nom d'utilisateur ne soit pas être visible.
  - **Requiert un certificat TLS :** sélectionnez cette option pour exiger un certificat TLS.
- **Faire confiance**
  - **Certificats approuvés :** pour ajouter un certificat approuvé, cliquez sur **Ajouter** et, pour chaque certificat que vous souhaitez ajouter, procédez comme suit :
    * **Application :** dans la liste, choisissez l'application que vous souhaitez ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le certificat ou sur **Annuler**.
  - **Noms de certificats serveur de confiance :** pour ajouter des noms communs de certificat de serveur approuvés, cliquez sur **Ajouter** et, pour chaque nom que vous souhaitez ajouter, procédez comme suit :
    * **Certificat :** entrez le nom du certificat de serveur. Vous pouvez utiliser des caractères génériques pour spécifier le nom, comme wpa.*.example.com.
    * Cliquez sur **Enregistrer** pour enregistrer le nom du certificat ou sur **Annuler**.
- **Autoriser les exceptions de fiabilité :** indiquez si vous souhaitez que la boîte de dialogue d'approbation de certificat s'affiche lorsqu'un certificat n'est pas approuvé. La valeur par défaut est **Activé**.
- **Paramètres du serveur proxy**
  - **Configuration du proxy :** dans la liste, cliquez sur **Aucun**, **Manuel** ou **Automatique** pour définir la façon dont la connexion VPN transite via un serveur proxy et configurez des options supplémentaires. La valeur par défaut est **Aucun**, ce qui n'exige aucune configuration supplémentaire.
  - Si vous avez sélectionné **Manuel**, configurez les paramètres suivants :
    * **Nom d'hôte/adresse IP :** entrez le nom d'hôte ou l'adresse IP du serveur proxy.
    * **Port :** entrez le numéro de port du serveur proxy.
    * **Nom d'utilisateur :** entrez un nom d'utilisateur pour l'authentification auprès du serveur proxy (facultatif).
    * **Mot de passe :** entrez un mot de passe pour l'authentification auprès du serveur proxy (facultatif).
  - Si vous avez sélectionné **Automatique**, configurez les paramètres suivants :
    * **URL du serveur :** entrez l'adresse URL du fichier PAC qui définit la configuration proxy.
    * **Autoriser la connexion directe si le PAC est injoignable :** indiquez si les utilisateurs

sont autorisés à se connecter directement à la destination si le fichier PAC est inaccessible. La valeur par défaut est **Activé**. Cette option est disponible uniquement sur iOS 7.0 et versions ultérieures.

- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres macOS



- **Type de réseau :** dans la liste, cliquez sur **Standard**, **Point d'accès d'ancienne génération** ou **Hotspot 2.0** pour définir le type de réseau que vous voulez utiliser.
- **Nom du réseau :** entrez le SSID qui est affiché dans la liste des réseaux disponibles pour

l'appareil. Ne s'applique pas à **Hotspot 2.0**.

- **Réseau masqué (activer si le réseau est ouvert ou désactivé) :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Rejoindre automatiquement (Rejoindre automatiquement ce réseau sans fil) :** sélectionnez cette option pour spécifier si le réseau est rejoint automatiquement. Si un appareil est déjà connecté à un autre réseau, il ne rejoint pas ce réseau. L'utilisateur doit se déconnecter du réseau précédent avant que l'appareil ne se connecte automatiquement. La valeur par défaut est **Activé**.
- **Type de sécurité :** dans la liste, choisissez le type de sécurité que vous voulez utiliser. Ne s'applique pas à **Hotspot 2.0**.
  - Aucun : ne requiert aucune configuration supplémentaire.
  - WEP
  - WPA/WPA2 Personnel
  - Tous (Personnel)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - Tous (Entreprise)

Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.

Paramètres WPA, WPA Personnel, WPA 2 Personnel, Tous (Personnel) pour macOS

- **Mot de passe :** entrez un mot de passe (facultatif). Si vous laissez ce champ vide, les utilisateurs peuvent être invités à entrer leurs mots de passe lorsqu'ils ouvrent une session.

Paramètres WEP Entreprise, WPA Entreprise, WPA2 Entreprise, Tous (Entreprise) pour macOS

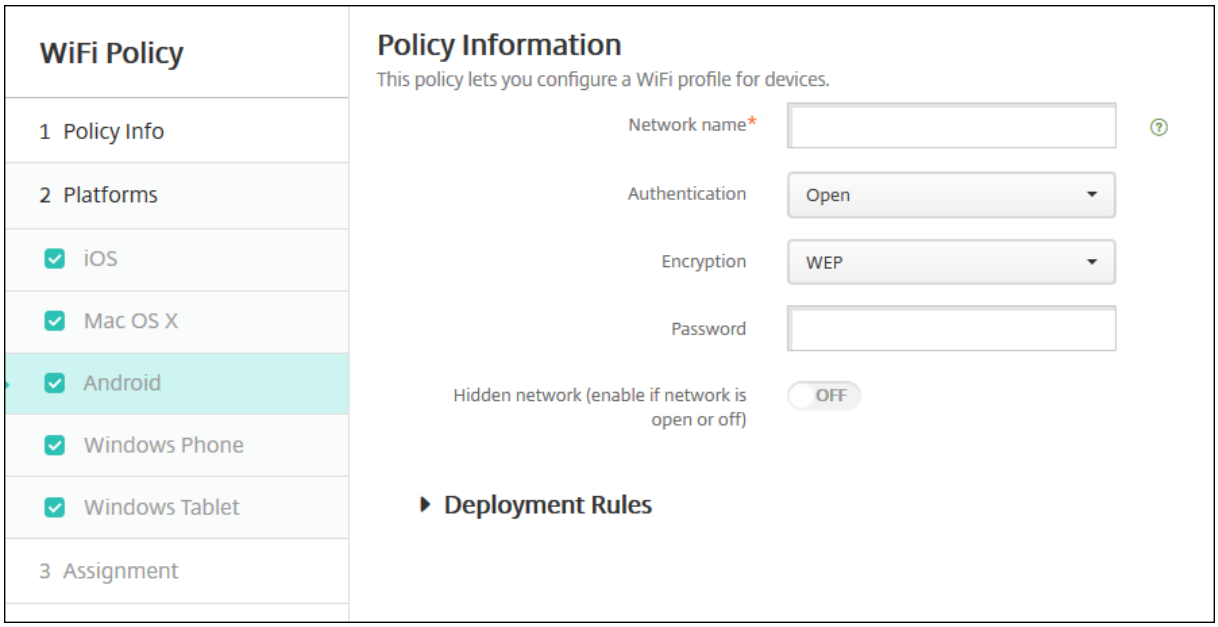
Lorsque vous sélectionnez l'un de ces paramètres, leurs paramètres sont répertoriés après **Paramètres du serveur proxy**.

- **Protocoles, types EAP acceptés :** activez les types EAP que vous souhaitez prendre en charge, puis configurez les paramètres associés. La valeur par défaut est **Désactivé** pour chaque type EAP disponible.
- **Authentification interne (TTLS) :** *requis uniquement lorsque vous activez TTLS*. Dans la liste, choisissez la méthode d'authentification interne à utiliser. Les options possibles sont : **PAP**, **CHAP**, **MSCHAP** ou **MSCHAPv2**. La valeur par défaut est **MSCHAPv2**.
- **Protocoles, EAP-FAST :** indiquez si vous souhaitez utiliser les informations d'identification d'accès protégé (PAC).
  - Si vous sélectionnez **Utiliser PAC**, indiquez si vous voulez utiliser un provisioning de PAC.
    - Si vous sélectionnez **Provisioning de PAC**, indiquez si vous souhaitez autoriser une négociation TLS anonyme entre le client et XenMobile.

        - **Provisioning du PAC de manière anonyme**
- **Authentification :**
  - **Nom d'utilisateur :** entrez un nom d'utilisateur.
  - **Mot de passe par connexion :** indiquez si un mot de passe sera exigé chaque fois que les utilisateurs ouvriront une session.
  - **Mot de passe :** entrez un mot de passe (facultatif). Si vous laissez ce champ vide, les utilisateurs peuvent être invités à entrer leurs mots de passe lorsqu'ils ouvrent une session.
  - **Infos d'identification de l'identité (infos d'identification magasin de clés ou PKI) :** dans la liste, cliquez sur le type d'informations d'identification de l'identité. La valeur par défaut est **Aucun**.
  - **Identité externe :** *requis uniquement lorsque vous activez* **PEAP**, **TTLS** *ou* **EAP-FAST**. Entrez le nom d'utilisateur visible en externe. Vous pouvez augmenter la sécurité en tapant un terme générique comme « anonyme » de façon à ce que le nom d'utilisateur ne soit pas être visible.
  - **Requiert un certificat TLS :** sélectionnez cette option pour exiger un certificat TLS.
- **Faire confiance**
  - **Certificats approuvés :** pour ajouter un certificat approuvé, cliquez sur **Ajouter** et, pour chaque certificat que vous souhaitez ajouter, procédez comme suit :
    - **Application :** dans la liste, choisissez l'application que vous souhaitez ajouter.
    - Cliquez sur **Enregistrer** pour enregistrer le certificat ou sur **Annuler**.
  - **Noms de certificats serveur de confiance :** pour ajouter des noms communs de certificat de serveur approuvés, cliquez sur **Ajouter** et, pour chaque nom que vous souhaitez ajouter, procédez comme suit :
    - **Certificat :** entrez le nom du certificat de serveur que vous souhaitez ajouter. Vous pouvez utiliser des caractères génériques pour spécifier le nom, comme wpa.*.example.com.
    - Cliquez sur **Enregistrer** pour enregistrer le nom du certificat ou sur **Annuler**.
- **Autoriser les exceptions de fiabilité :** indiquez si vous souhaitez que la boîte de dialogue d'approbation de certificat s'affiche lorsqu'un certificat n'est pas approuvé. La valeur par défaut est **Activé**.
- **Utiliser comme configuration de fenêtre de connexion :** indiquez si vous souhaitez utiliser les informations d'identification saisies dans la fenêtre d'ouverture de session pour l'authentification de l'utilisateur.
- **Paramètres du serveur proxy**
  - **Configuration du proxy :** dans la liste, cliquez sur **Aucun**, **Manuel** ou **Automatique** pour définir la façon dont la connexion VPN transite via un serveur proxy et configurez des options supplémentaires. La valeur par défaut est **Aucun**, ce qui n'exige aucune configuration supplémentaire.
  - Si vous avez sélectionné **Manuel**, configurez les paramètres suivants :

        * **Nom d'hôte/adresse IP :** entrez le nom d'hôte ou l'adresse IP du serveur proxy.
        * **Port :** entrez le numéro de port du serveur proxy.
        * **Nom d'utilisateur :** entrez un nom d'utilisateur pour l'authentification auprès du serveur proxy (facultatif).
        * **Mot de passe :** entrez un mot de passe pour l'authentification auprès du serveur proxy (facultatif).
    - Si vous avez sélectionné **Automatique**, configurez les paramètres suivants :
        * **URL du serveur :** entrez l'adresse URL du fichier PAC qui définit la configuration proxy.
        * **Autoriser la connexion directe si le PAC est injoignable :** indiquez si les utilisateurs sont autorisés à se connecter directement à la destination si le fichier PAC est inaccessible. La valeur par défaut est **Activé**. Cette option est disponible uniquement sur iOS 7.0 et versions ultérieures.

Paramètres Android



- **Nom du réseau :** entrez le SSID qui figure dans la liste des réseaux disponibles sur l'appareil de l'utilisateur.
- **Authentification :** dans la liste, choisissez le type de sécurité à utiliser avec la connexion Wi-Fi.
    - Ouverte
    - Partagé
    - WPA
    - WPA-PSK
    - WPA2
    - WPA2-PSK
    - 802.1x EAP

Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.

Paramètres ouverts partagés pour Android

- **Cryptage :** dans la liste, choisissez **Désactivé** ou **WEP**. La valeur par défaut est **WEP**.
- **Mot de passe :** entrez un mot de passe (facultatif).

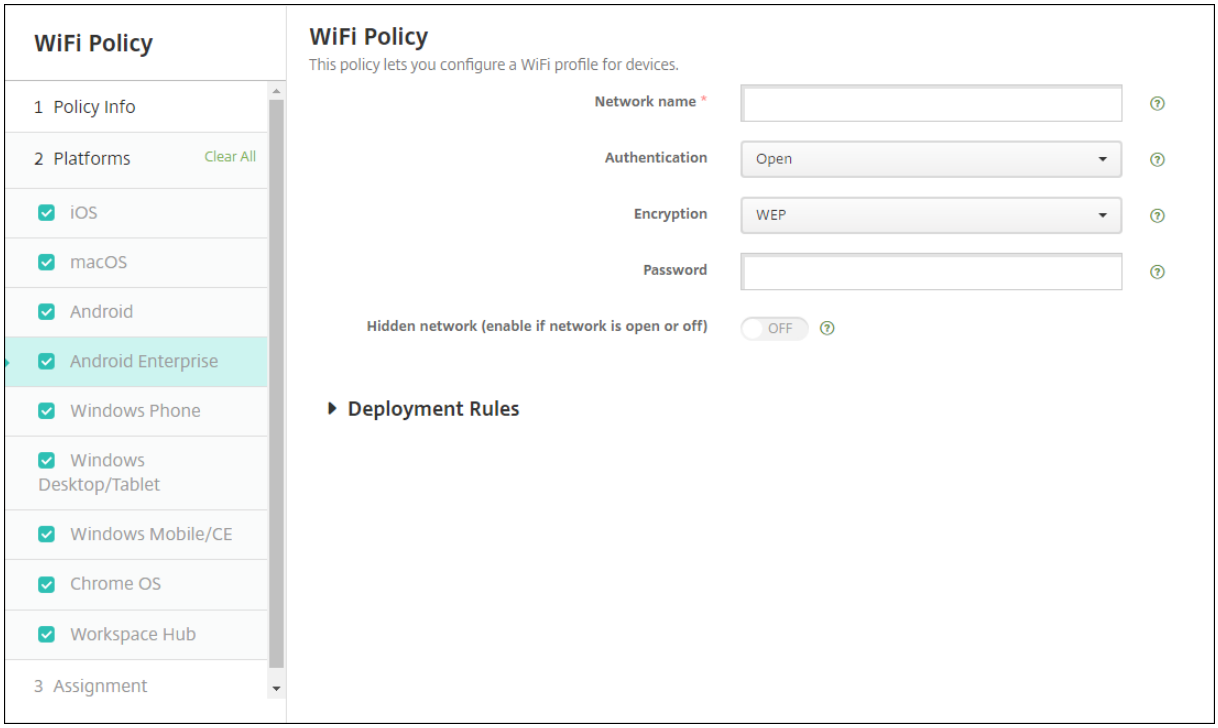
Paramètres WPA, WPA-PSK, WPA2, WPA2-PSK pour Android

- **Cryptage :** dans la liste, choisissez **TKIP** ou **AES**. La valeur par défaut est **TKIP**.
- **Mot de passe :** entrez un mot de passe (facultatif).

Paramètres 802.1x pour Android

- **Type EAP :** dans la liste, choisissez **PEAP**, **TLS** ou **TTLS**. La valeur par défaut est **PEAP**.
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Authentification phase 2 :** dans la liste, choisissez **Aucun**, **PAP**, **MSCHAP**, **MSCHAPPv2** ou **GTC**. La valeur par défaut est **PAP**.
- **Identité :** entrez le nom d'utilisateur et le domaine (facultatif).
- **Anonyme :** entrez le nom d'utilisateur visible en externe (facultatif). Vous pouvez augmenter la sécurité en tapant un terme générique comme « anonyme » de façon à ce que le nom d'utilisateur ne soit pas être visible.
- **Certificat CA :** dans la liste, choisissez le certificat à utiliser.
- **Infos d'identification de l'identité :** dans la liste, choisissez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
- **Réseau masqué (activer si le réseau est ouvert ou désactivé) :** sélectionnez cette option pour spécifier si le réseau est masqué.

Paramètres Android Enterprise



- **Nom du réseau :** entrez le SSID qui figure dans la liste des réseaux disponibles sur l'appareil de l'utilisateur.
- **Authentification :** dans la liste, choisissez le type de sécurité à utiliser avec la connexion Wi-Fi.
  - Ouverte
  - Partagé
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.

Paramètres ouverts partagés pour Android

- **Cryptage :** dans la liste, choisissez **Désactivé** ou **WEP**. La valeur par défaut est **WEP**.
- **Mot de passe :** entrez un mot de passe (facultatif).

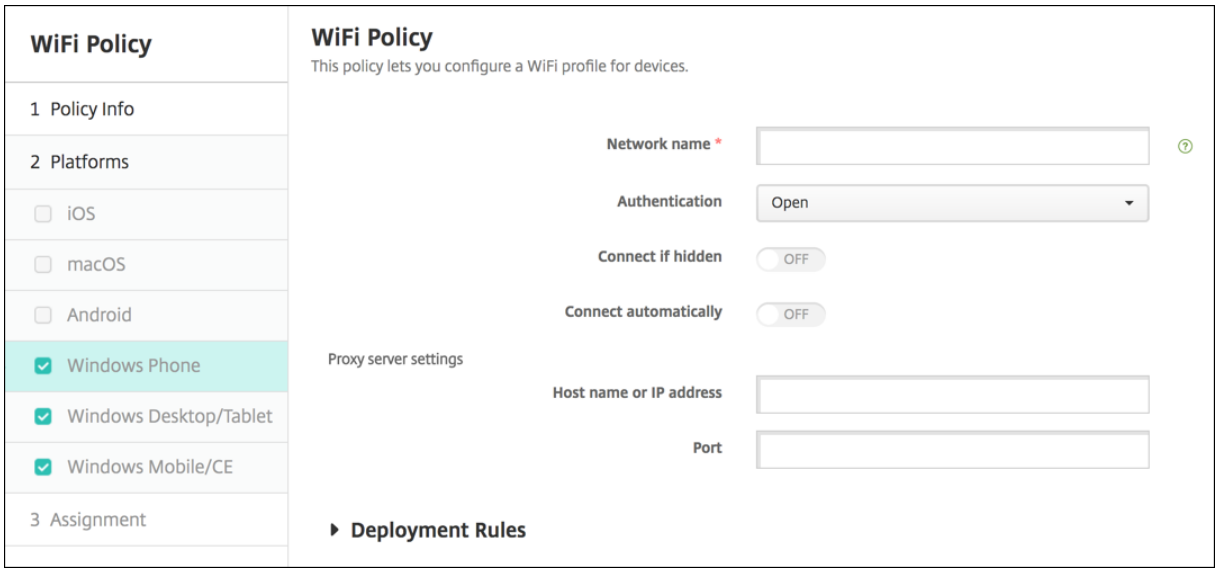
Paramètres WPA, WPA-PSK, WPA2, WPA2-PSK pour Android

- **Cryptage :** dans la liste, choisissez TKIP ou AES. La valeur par défaut est TKIP.
- **Mot de passe :** entrez un mot de passe (facultatif).

Paramètres 802.1x pour Android

- **Type EAP :** dans la liste, choisissez **PEAP**, **TLS** ou **TTLS**. La valeur par défaut est **PEAP**.
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Authentification phase 2 :** dans la liste, choisissez **Aucun**, **PAP**, **MSCHAP**, **MSCHAPPv2** ou **GTC**. La valeur par défaut est **PAP**.
- **Identité :** entrez le nom d'utilisateur et le domaine (facultatif).
- **Anonyme :** entrez le nom d'utilisateur visible en externe (facultatif). Vous pouvez augmenter la sécurité en tapant un terme générique comme « anonyme » de façon à ce que le nom d'utilisateur ne soit pas visible.
- **Certificat CA :** dans la liste, choisissez le certificat à utiliser.
- **Infos d'identification de l'identité :** dans la liste, choisissez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
- **Réseau masqué (activer si le réseau est ouvert ou désactivé) :** sélectionnez cette option pour spécifier si le réseau est masqué.

Paramètres Windows Phone



- **Nom du réseau :** entrez le SSID qui figure dans la liste des réseaux disponibles sur l'appareil de l'utilisateur.
- **Authentification :** dans la liste, choisissez le type de sécurité à utiliser avec la connexion Wi-Fi.
  - Ouverte
  - WPA Personnel
  - WPA-2 Personnel
  - WPA-2 Enterprise : l'utilisation de WPA-2 Enterprise nécessite que vous configuriez SCEP. La configuration SCEP permet à XenMobile d'envoyer le certificat aux appareils pour l'authentification auprès du serveur Wi-Fi. Pour configurer SCEP, accédez à la

page **Distribution** dans **Paramètres > Fournisseurs d'identités**. Pour de plus amples informations, consultez la section Fournisseurs d'identités.

Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.

Paramètres ouverts pour Windows Phone

- **Se connecter si le réseau Wi-Fi est masqué :** sélectionnez cette option pour spécifier si vous souhaitez vous connecter lorsque le réseau est masqué.
- **Se connecter automatiquement :** sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.

Paramètres WPA Personnel, WPA-2 Personnel pour Windows Phone

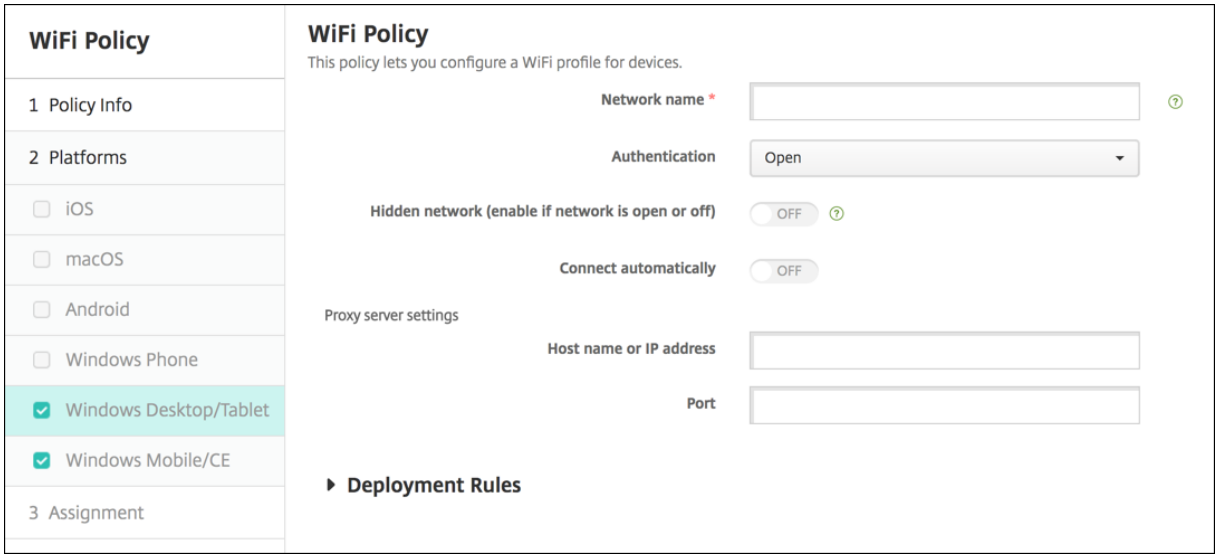
- **Cryptage :** dans la liste, choisissez **AES** ou **TKIP** pour définir le type de cryptage. La valeur par défaut est **AES**.
- **Se connecter si le réseau Wi-Fi est masqué :** sélectionnez cette option pour spécifier si vous souhaitez vous connecter lorsque le réseau est masqué.
- **Se connecter automatiquement :** sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.

Paramètres WPA-2 Enterprise pour Windows Phone

- **Cryptage :** dans la liste, choisissez **AES** ou **TKIP** pour définir le type de cryptage. La valeur par défaut est **AES**.
- **Type EAP :** dans la liste, choisissez **PEAP-MSCHAPv2** ou **TLS** pour définir le type EAP. La valeur par défaut est **PEAP-MSCHAPv2**.
- **Se connecter si le réseau Wi-Fi est masqué :** sélectionnez cette option pour spécifier si vous souhaitez vous connecter lorsque le réseau est masqué.
- **Se connecter automatiquement :** sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.
- **Envoyer certificat par push via SCEP :** indiquez si vous souhaitez distribuer le certificat aux appareils des utilisateurs via le protocole d'inscription du certificat simple (SCEP).
- **Fournisseur d'identités pour SCEP :** dans la liste, choisissez le fournisseur d'identités SCEP. La valeur par défaut est **Aucun**.
- **Paramètres du serveur proxy**
  - **Nom d'hôte ou adresse IP :** entrez le nom ou l'adresse IP du serveur proxy.
  - **Port :** entrez le numéro de port du serveur proxy.
- **Paramètres de stratégie**

- **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
  - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
- **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
- **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Paramètres de Windows 10 et Windows 11



- **Authentification :** dans la liste, cliquez sur le type de sécurité à utiliser avec la connexion Wi-Fi.
  - Ouverte
  - WPA Personnel
  - WPA-2 Personnel
  - WPA Enterprise
  - WPA-2 Enterprise : l'utilisation de WPA-2 Enterprise nécessite que vous configuriez SCEP. La configuration SCEP permet à XenMobile d'envoyer le certificat aux appareils pour l'authentification auprès du serveur Wi-Fi. Pour configurer SCEP, accédez à la page **Distribution** dans **Paramètres > Fournisseurs d'identités**. Pour de plus amples informations, consultez la section Fournisseurs d'identités.

Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.

Paramètres ouverts pour Windows 10 et Windows 11

- **Réseau masqué (activer si le réseau est ouvert ou désactivé) :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Se connecter automatiquement :** sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.

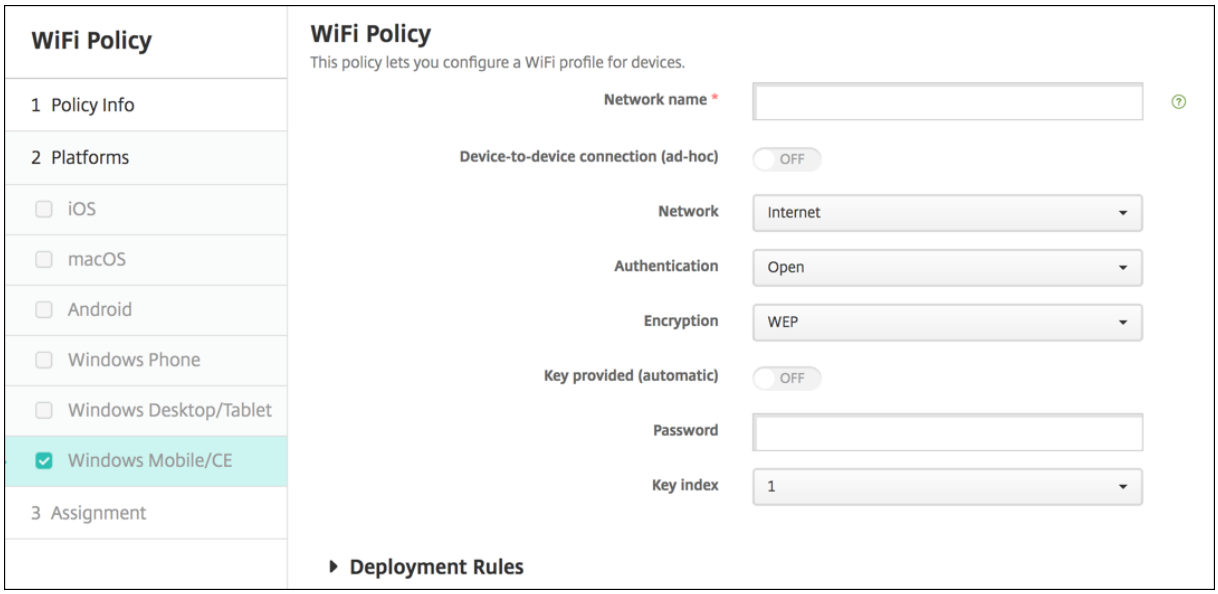
Paramètres WPA Personnel, WPA-2 Personnel pour Windows 10 et Windows 11

- **Cryptage :** dans la liste, choisissez **AES** ou **TKIP** pour définir le type de cryptage. La valeur par défaut est **AES**.
- **Réseau masqué (activer si le réseau est ouvert ou désactivé) :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Se connecter automatiquement :** sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.

Paramètres WPA-2 Enterprise pour Windows 10 et Windows 11

- **Cryptage :** dans la liste, choisissez **AES** ou **TKIP** pour définir le type de cryptage. La valeur par défaut est **AES**.
- **Type EAP :** dans la liste, choisissez **PEAP-MSCHAPv2** ou **TLS** pour définir le type EAP. La valeur par défaut est **PEAP-MSCHAPv2**.
- **Se connecter si le réseau Wi-Fi est masqué :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Se connecter automatiquement :** sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.
- **Envoyer certificat par push via SCEP :** indiquez si vous souhaitez distribuer le certificat aux appareils des utilisateurs via le protocole d'inscription du certificat simple (SCEP).
- **Fournisseur d'identités pour SCEP :** dans la liste, choisissez le fournisseur d'identités SCEP. La valeur par défaut est **Aucun**.

Paramètres Windows Mobile/CE



- **Nom du réseau :** entrez le SSID qui figure dans la liste des réseaux disponibles sur l'appareil de l'utilisateur.
- **Connexion appareil-appareil (ad-hoc) :** permet à deux appareils de se connecter directement. La valeur par défaut est **Désactivé**.
- **Réseau :** indiquez si l'appareil est connecté à une source de données Internet externe ou un intranet.
- **Authentification :** dans la liste, choisissez le type de sécurité à utiliser avec la connexion Wi-Fi.
  - Ouverte
  - WPA Personnel
  - WPA-2 Personnel
  - WPA-2 Entreprise

Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.

Paramètres ouverts pour Windows Mobile/CE

- **Réseau masqué (activer si le réseau est ouvert ou désactivé) :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Se connecter automatiquement :** sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.

Paramètres WPA Personnel, WPA-2 Personnel pour Windows Mobile/CE

- **Cryptage :** dans la liste, choisissez **AES** ou **TKIP** pour définir le type de cryptage. La valeur par défaut est **AES**.

- **Réseau masqué (activer si le réseau est ouvert ou désactivé) :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Se connecter automatiquement :** sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.

Paramètres WPA-2 Enterprise pour Windows Mobile/CE

- **Cryptage :** dans la liste, choisissez **AES** ou **TKIP** pour définir le type de cryptage. La valeur par défaut est **AES**.
- **Type EAP :** dans la liste, choisissez **PEAP-MSCHAPv2** ou **TLS** pour définir le type EAP. La valeur par défaut est **PEAP-MSCHAPv2**.
- **Se connecter si le réseau Wi-Fi est masqué :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Se connecter automatiquement :** sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.
- **Envoyer certificat par push via SCEP :** indiquez si vous souhaitez distribuer le certificat aux appareils des utilisateurs via le protocole d'inscription du certificat simple (SCEP).
- **Fournisseur d'identités pour SCEP :** dans la liste, choisissez le fournisseur d'identités SCEP. La valeur par défaut est **Aucun**.
- **Clé fournie automatiquement :** spécifiez si la clé est fournie automatiquement ou non. La valeur par défaut est **Désactivé**.
- **Mot de passe :** entrez le mot de passe dans ce champ.
- **Index de clé :** indiquez l'index de la clé. Les options disponibles sont **1**, **2**, **3** et **4**.

Stratégie de certificat Windows CE

January 10, 2022

Vous pouvez créer une stratégie d'appareil dans XenMobile afin de créer et de mettre à disposition des certificats Windows Mobile/CE à partir d'une PKI externe vers les appareils des utilisateurs. Pour de plus amples informations sur les certificats et les entités PKI, consultez la section Certificats.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Windows CE

- **Fournisseur d'identités :** dans la liste, cliquez sur le fournisseur d'identités. La valeur par défaut est **Aucun**.

- **Mot de passe généré au format PKCS#12 :** entrez le mot de passe utilisé pour crypter le certificat.
- **Dossier de destination :** dans la liste, cliquez sur le dossier de destination pour le certificat ou cliquez sur **Ajouter** pour ajouter un dossier qui n'est pas déjà dans la liste. Les options prédéfinies sont les suivantes :
  - %Carte de stockage%\
  - %Dossier Xenmobile%\
  - %Program Files%\
  - %Mes Documents%\
  - %Windows%\
- **Nom du fichier de destination :** entrez le nom du fichier de certificat.

Stratégie Protection des informations Windows (WIP)

January 10, 2022

Protection des informations Windows (WIP), précédemment appelée protection des données d'entreprise (EDP), est une technologie de Windows qui protège contre la fuite potentielle de données d'entreprise. Les fuites de données peuvent se produire via le partage des données d'entreprise vers des applications protégées n'appartenant pas à l'entreprise, entre les applications ou en dehors du réseau de votre organisation. Pour plus d'informations, consultez la section Protéger vos données d'entreprise à l'aide de la Protection des informations Windows (WIP).

Vous pouvez créer une stratégie dans XenMobile afin de spécifier les applications nécessitant une protection des informations Windows au niveau d'exécution que vous avez défini. La stratégie Protection des informations Windows est destinée aux téléphones, tablettes et bureaux supervisés Windows 10 ou Windows 11.

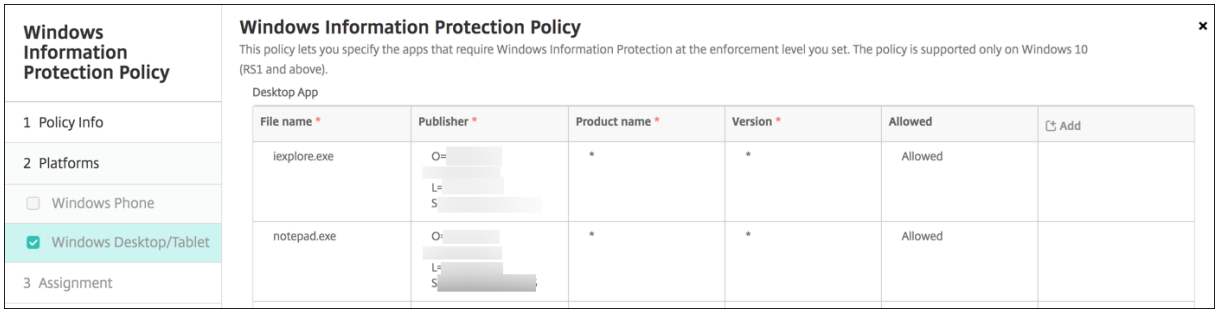
XenMobile comprend des applications courantes et vous pouvez ajouter d'autres applications. Vous spécifiez pour la stratégie un niveau d'exécution qui affecte l'expérience utilisateur. Par exemple, vous pouvez :

- Bloquer tout partage de données inapproprié.
- Avertir sur le partage de données inapproprié et permettre aux utilisateurs de personnaliser la stratégie.
- Exécuter WIP de manière silencieuse lors de l'ouverture de session et du partage de données inapproprié.

Pour exclure des applications de la protection des informations Windows, définissez ces applications dans les fichiers XML AppLocker de Microsoft, puis importez ces fichiers dans XenMobile.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres de Windows 10 et Windows 11



- **Application de bureau** (ordinateur de bureau Windows 10 ou Windows 11), **Magasin d'applications** (Windows 10 Phone et Windows 10 ou tablette Windows 11) : XenMobile inclut certaines applications courantes, comme indiqué dans l'exemple ci-dessus. Vous pouvez modifier ou supprimer ces applications selon vos besoins.

  Pour ajouter d'autres applications : dans le tableau **Application de bureau** ou **Magasin des applications**, cliquez sur **Ajouter** et fournissez les informations d'application.

  Les applications **autorisées** peuvent lire, créer et mettre à jour les données d'entreprise. Les applications **refusées** ne peuvent pas accéder aux données d'entreprise. Les applications avec **exemption** peuvent lire les données d'entreprise, mais ne peuvent pas créer ou modifier les données.

  - **Fichier XML AppLocker :** Microsoft fournit une liste des applications Microsoft qui ont des problèmes de compatibilité connus avec WIP. Pour exclure ces applications de WIP, cliquez sur **Parcourir** pour charger la liste. XenMobile combine le fichier XML AppLocker chargé et les applications de bureau et de magasin configurées dans la stratégie envoyées à l'appareil. Pour plus d'informations, consultez la section Recommended deny list for Windows Information Protection.
  - **Niveau d'exécution :** sélectionnez une option pour spécifier la manière dont vous souhaitez que la protection des informations Windows protège et gère le partage des données. La valeur par défaut est **Désactivé**.
    - **0-Désactivé :** WIP est désactivé et n'effectue aucune protection ni aucun audit de vos données.
    - **1-Silencieux :** WIP s'exécute de manière silencieuse, consigne le partage de données inapproprié et ne bloque rien. Vous pouvez accéder aux journaux via Reporting CSP.
    - **2-Remplacer :** WIP avertit les utilisateurs de partage des données potentiellement dangereux. Les utilisateurs peuvent ignorer les avertissements et partager les don-

nées. Ce mode consigne les actions, y compris les messages ignorés par l'utilisateur, dans votre journal d'audit.

* **3-Bloquer :** WIP empêche les utilisateurs d'effectuer tout partage de données potentiellement dangereux.

- **Noms de domaine protégés :** domaines que votre entreprise utilise pour les identités de ses utilisateurs. Cette liste de domaines d'identités gérés, ainsi que le domaine principal, constituent l'identité de votre entreprise de gestion. Le premier domaine dans la liste est l'identité d'entreprise principale utilisée dans l'interface utilisateur Windows. Utilisez « | » pour séparer les éléments de la liste. Pa exemple : `domain1.com | domain2.com`
- **Certificat de récupération de données :** cliquez sur **Parcourir**, puis sélectionnez un certificat de récupération à utiliser pour la récupération de données de fichiers cryptés. Ce certificat est le même que le certificat de l'agent de récupération de données (DRA) pour le système de fichiers de cryptage (EFS), uniquement mis à disposition via MDM au lieu de la stratégie de groupe. Si un certificat de récupération n'est pas disponible, créez-le. Pour plus d'informations, consultez « Créer un certificat de récupération de données » dans cette section.
- **Noms de domaine réseau :** liste des domaines à l'intérieur de l'entreprise. WIP protège tout le trafic vers les domaines entièrement qualifiés dans cette liste. Ce paramètre, avec le paramètre **Plage d'adresses IP**, détecte si un point de terminaison réseau est de type enterprise ou personnel sur des réseaux privés. Utilisez une virgule pour séparer les éléments de la liste. Par exemple : corp.exemple.com,region.exemple.com
- **Plage d'adresses IP :** liste des plages d'adresses IPv4 et IPv6 d'entreprise qui définissent les ordinateurs dans le réseau d'entreprise. WIP considère ces emplacements comme une destination sûre pour le partage de données d'entreprise. Utilisez une virgule pour séparer les éléments de la liste. Par exemple :

  `10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff`
- **La plage d'adresses IP fait autorité :** pour empêcher la détection automatique des plages d'adresses IP par Windows, réglez ce paramètre sur **Activé**. La valeur par défaut est **Désactivé**.
- **Serveurs proxy :** liste des serveurs proxy que l'entreprise peut utiliser pour les ressources d'entreprise. Ce paramètre est requis si vous utilisez un proxy dans votre réseau. Sans un serveur proxy, les ressources d'entreprise peuvent être indisponibles lorsqu'un client est derrière un proxy. Par exemple, des ressources peuvent être non disponibles à partir de certains points d'accès Wi-Fi dans des hôtels et des restaurants. Utilisez une virgule pour séparer les éléments de la liste. Par exemple :

  `proxy.example.com:80;157.54.11.118:443`

- **Serveurs proxy internes :** liste des serveurs proxy par lesquels vos appareils passent pour accéder à vos ressources cloud. L'utilisation de ce type de serveur indique que les ressources cloud auxquelles vous vous connectez sont des ressources d'entreprise. Veillez à ne pas inclure dans cette liste les serveurs du paramètre **Serveurs proxy**, qui sont utilisés pour le trafic non protégé par WIP. Utilisez une virgule pour séparer les éléments de la liste. Par exemple :

  ```
  example.internalproxy1.com;10.147.80.50
  ```

- **Ressources cloud :** liste des ressources cloud protégées par WIP. Pour chaque ressource cloud, vous pouvez également spécifier un serveur proxy de la liste **Serveurs proxy** pour achemine le trafic pour cette ressource cloud. Tout trafic acheminé via les **serveurs proxy** est traité en tant que trafic d'entreprise. Utilisez une virgule pour séparer les éléments de la liste. Par exemple :

  ```
  domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.
  domain2.com
  ```

- **Configurer protection après verrouillage :** Windows 10 Phone uniquement. Si ce paramètre est réglé sur **Activé**, la stratégie de code secret est également requise. Sinon, le déploiement de la stratégie de protection des informations Windows échoue. En outre, si cette stratégie est réglée sur **Activé**, le paramètre **Exiger protection après verrouillage** s'affiche. La valeur par défaut est **Désactivé**.

- **Exiger protection après verrouillage :** Windows 10 Phone uniquement. Spécifie si vous souhaitez crypter les données d'entreprise à l'aide d'une clé qui est protégée par un code PIN employé sur un appareil verrouillé. Les applications ne peuvent pas lire les données d'entreprise sur un appareil verrouillé. La valeur par défaut est **Activé**.

- **Révoquer certificat WIP après désinscription :** spécifie si vous souhaitez révoquer les clés de cryptage locales d'un appareil utilisateur lorsque ce dernier est désinscrit de la protection des informations de Windows. Une fois que les clés de cryptage sont révoquées, un utilisateur ne peut pas accéder aux données d'entreprise cryptées. Si ce paramètre est réglé sur **Désactivé**, les clés ne sont pas révoquées et l'utilisateur continue d'avoir accès aux fichiers protégés après l'annulation de l'inscription. La valeur par défaut est **Activé**.

- **Afficher icônes de superposition :** spécifie si vous souhaitez inclure la superposition de l'icône de protection des informations de Windows sur les fichiers d'entreprise dans l'Explorateur et les mosaïques des applications d'entreprise dans le menu Démarrer. La valeur par défaut est **Désactivé**.

Créer un certificat de récupération de données

Un certificat de récupération de données est requis pour activer la stratégie **Protection des informations de Windows**.

1. Sur la machine sur laquelle s'exécute la console XenMobile, ouvrez une invite de commandes et naviguez vers un dossier (autre que Windows\System32) sur lequel vous souhaitez créer un certificat.
2. Exécutez cette commande :

   ```
   cipher /r:ESFDRA
   ```

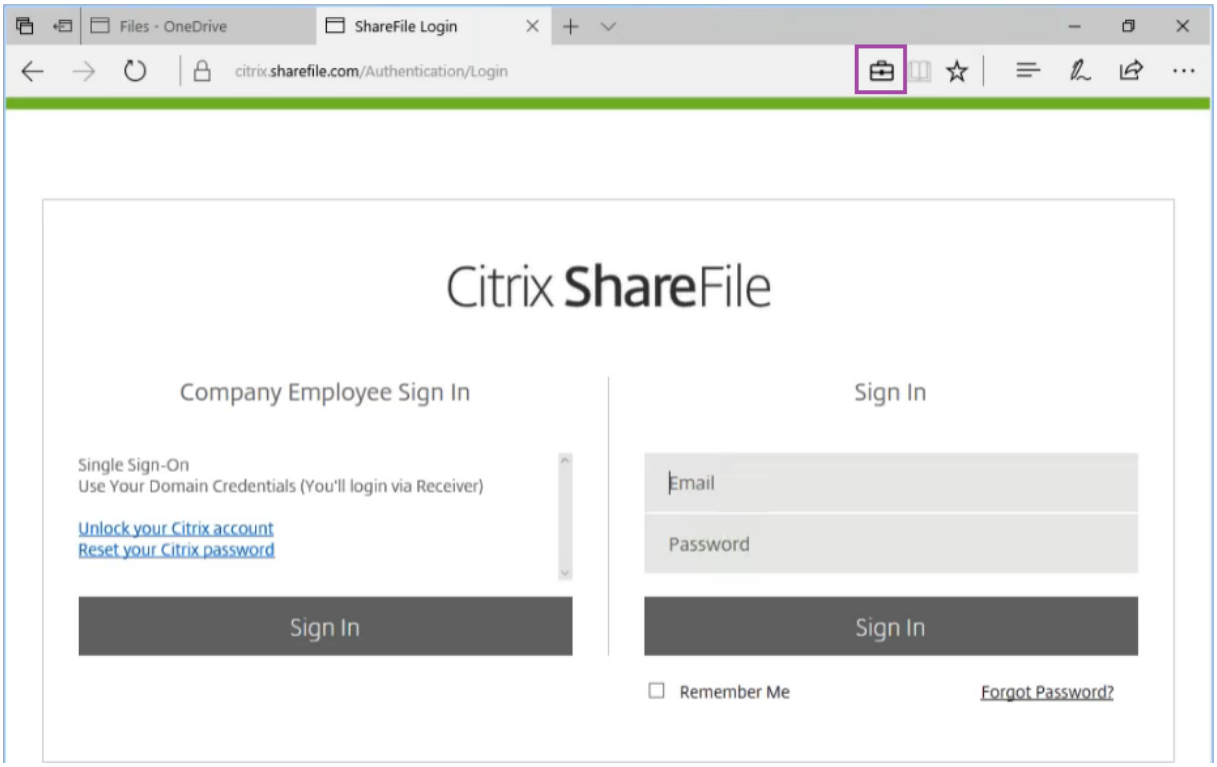
3. Lorsque vous y êtes invité, entrez un mot de passe pour protéger le fichier de clé privée.

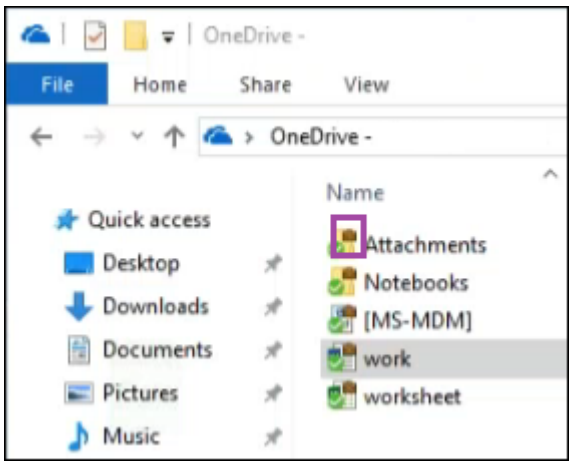
   La commande de chiffrement (cipher) crée un fichier .cer et .pfx.

4. Dans la console XenMobile, accédez à **Paramètres > Certificats** et importez le fichier .cer, qui s'applique aux tablettes Windows 10 et Windows 11 et aux téléphones Windows 10.

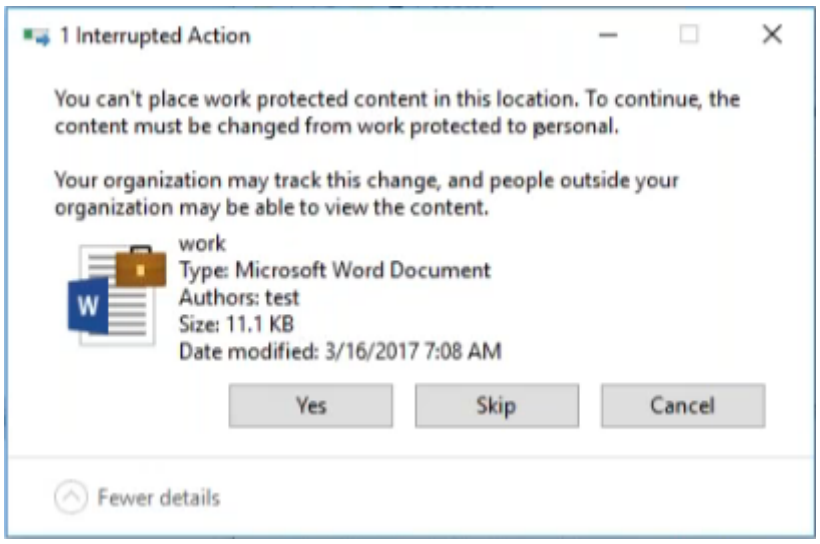
Expérience utilisateur

Lorsque la protection des informations de Windows est activée, les applications et les fichiers sont accompagnés d'une icône :





Si un utilisateur copie ou enregistre un fichier protégé dans un emplacement non protégé, la notification suivante s'affiche, en fonction du niveau d'application configuré.



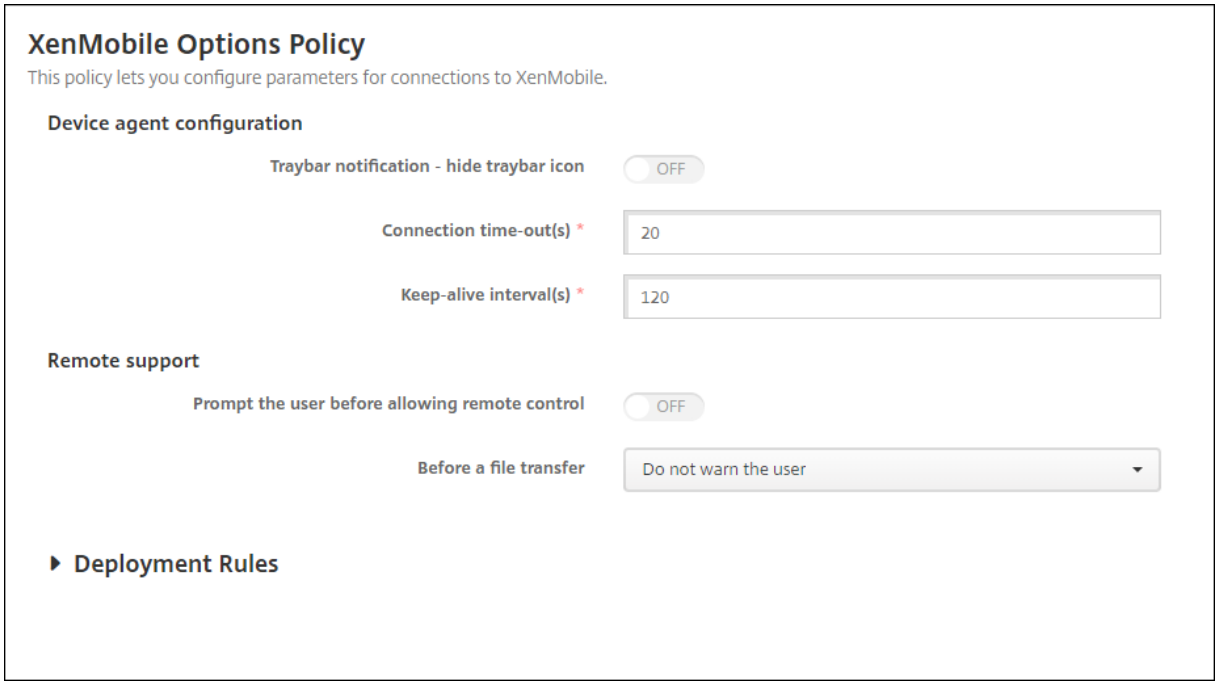
Stratégie d'options XenMobile

January 10, 2022

Vous ajoutez une stratégie d'options XenMobile pour configurer le comportement de Secure Hub lors de la connexion à XenMobile à partir d'appareils Android et Windows Mobile/CE.

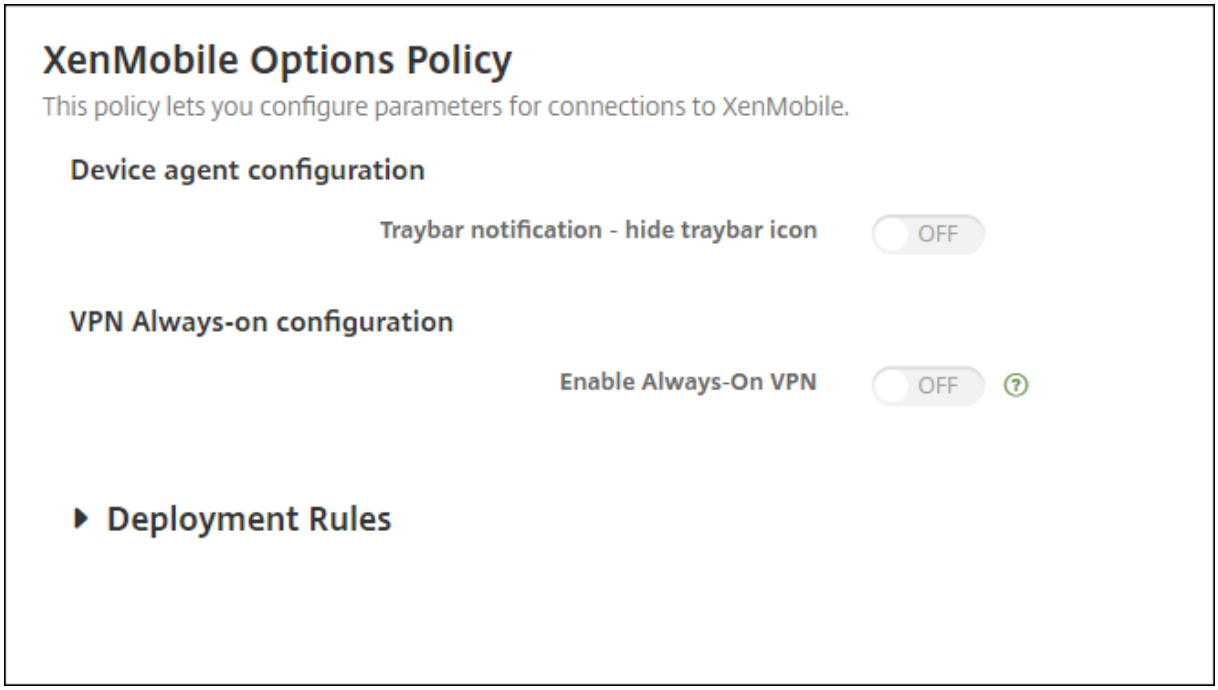
Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Android



- **Zone de notification - icône masquer la zone de notification :** sélectionnez cette option pour spécifier si l'icône de la zone de notification est masquée ou visible. La valeur par défaut est **Désactivé**.
- **Délai d'expiration des connexions :** entrez la durée en secondes pendant laquelle une connexion peut rester inactive avant expiration de la connexion. La durée par défaut est de 20 secondes.
- **Intervalles de persistance des connexions :** entrez la durée en secondes pendant laquelle maintenir une connexion ouverte. La durée par défaut est de 120 secondes.
- **Demander à l'utilisateur avant d'autoriser le contrôle à distance :** indiquez si une invite s'affiche avant d'autoriser le contrôle à distance. La valeur par défaut est **Désactivé**.
- **Avant un transfert de fichiers :** dans la liste, cliquez pour informer l'utilisateur d'un transfert de fichiers ou pour lui demander l'autorisation. Valeurs disponibles : **Ne pas prévenir l'utilisateur**, **Prévenir l'utilisateur** et **Demander à l'utilisateur**. La valeur par défaut est **Ne pas prévenir l'utilisateur**.

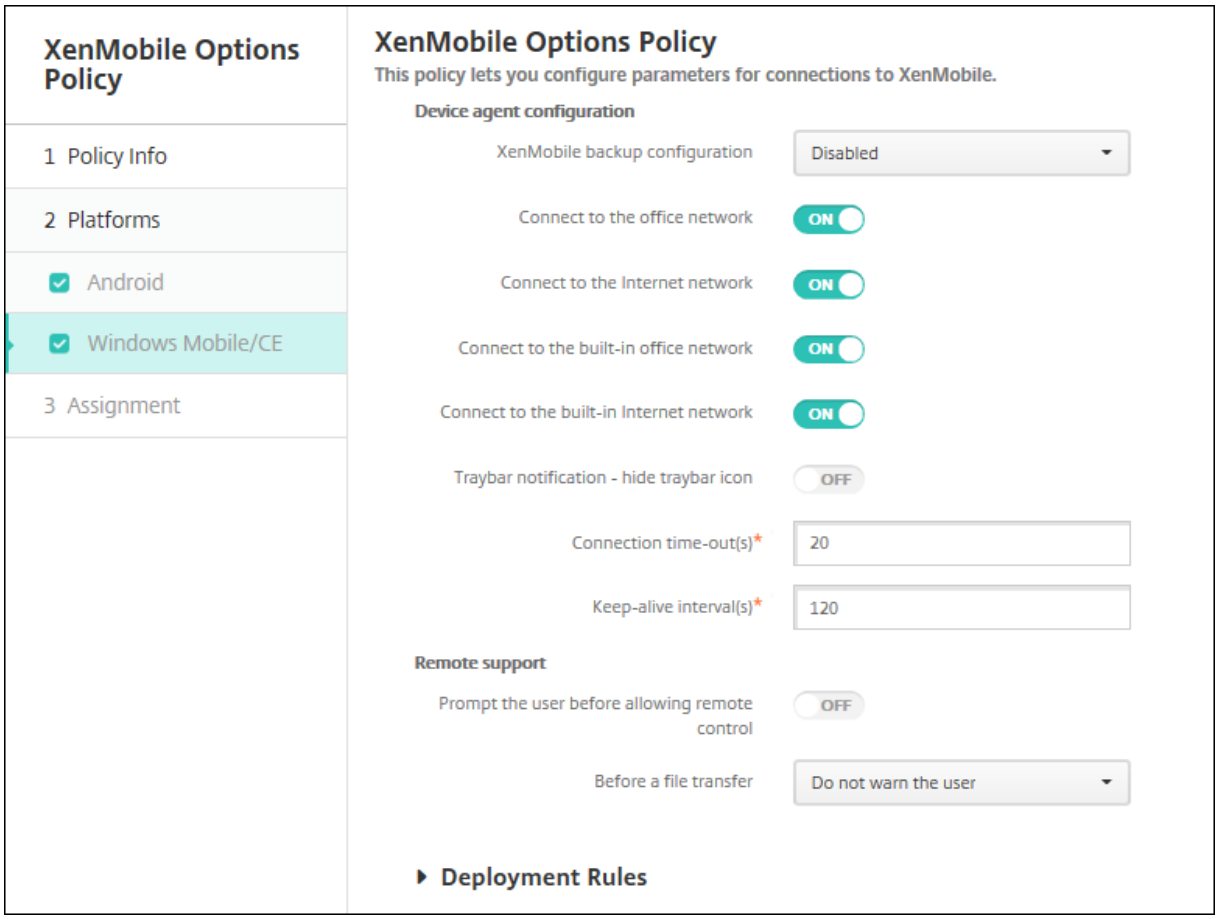
Paramètres Android Enterprise



Prise en charge à partir de la version 7 d'Android.

- **Zone de notification - icône masquer la zone de notification :** sélectionnez cette option pour spécifier si l'icône de la zone de notification est masquée ou visible. La valeur par défaut est **Désactivé**.
- **Activer VPN Always On.** Indiquez si le VPN Always On est activé. Lorsque ce paramètre est **activé**, le service VPN démarre lorsque l'appareil est mis sous tension et continue de s'exécuter pendant que l'appareil est sous tension. La valeur par défaut est **Désactivé**.
- **Package VPN.** Tapez le nom du package de l'application VPN utilisée par l'appareil. Par défaut, le nom du package de l'application Citrix SSO, **com.Citrix.CitrixVPN**, est renseigné automatiquement dans ce champ.

Paramètres Windows Mobile/CE



- **Configuration de l'agent sur l'appareil**
  - **Configuration de la sauvegarde XenMobile :** dans la liste, cliquez sur une option pour sauvegarder la configuration XenMobile sur les appareils des utilisateurs. La valeur par défaut est **Désactivé**. Les options disponibles sont les suivantes :
    - Désactivé
    - À la première connexion après installation de XenMobile
    - À la première connexion après chaque redémarrage
  - **Se connecter au réseau d'entreprise**
  - **Se connecter au réseau Internet**
  - **Se connecter au réseau d'entreprise intégré :** lorsque cette valeur est définie sur **Activé**, XenMobile détecte automatiquement le réseau.
  - **Se connecter au réseau Internet intégré :** lorsque cette valeur est définie sur **Activé**, XenMobile détecte automatiquement le réseau.
  - **Zone de notification - icône masquer la zone de notification :** sélectionnez cette option pour spécifier si l'icône de la zone de notification est masquée ou visible. La valeur par défaut est **Désactivé**.
  - **Délai d'expiration des connexions :** entrez la durée en secondes pendant laquelle une

connexion peut rester inactive avant expiration de la connexion. La durée par défaut est de 20 secondes.
  - **Intervalles de persistance des connexions :** entrez la durée en secondes pendant laquelle maintenir une connexion ouverte. La durée par défaut est de 120 secondes.
- **Assistance à distance**
  - **Demander à l'utilisateur avant d'autoriser le contrôle à distance :** indiquez si une invite s'affiche avant d'autoriser le contrôle à distance. La valeur par défaut est **Désactivé**.
  - **Avant un transfert de fichiers :** dans la liste, cliquez pour informer l'utilisateur d'un transfert de fichiers ou pour lui demander l'autorisation. Valeurs disponibles : **Ne pas prévenir l'utilisateur**, **Prévenir l'utilisateur** et **Demander à l'utilisateur**. La valeur par défaut est **Ne pas prévenir l'utilisateur**.

Stratégie de désinstallation de XenMobile

January 10, 2022

Vous pouvez ajouter une stratégie dans XenMobile afin de désinstaller XenMobile des appareils Android et Windows Mobile/CE. Lorsqu'elle est déployée, cette stratégie supprime XenMobile sur tous les appareils du déploiement.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Configurer les paramètres pour Android et Windows Mobile/CE

- **Désinstaller XenMobile des appareils :** sélectionnez cette option pour désinstaller XenMobile de chaque appareil sur lequel vous déployez cette stratégie. La valeur par défaut est **Désactivé**.

Ajouter des applications

January 10, 2022

L'ajout d'applications à XenMobile fournit des fonctionnalités de gestion d'application mobile (MAM). XenMobile vous aide à prendre en charge la mise à disposition des applications, l'attribution des licences logicielles, la configuration et la gestion du cycle de vie des applications.

Les applications compatibles MDX représentent un élément important dans la préparation de la plupart des types d'applications pour leur distribution sur les machines utilisateur. Pour une présentation de MDX, consultez les sections À propos de MDX Toolkit et Présentation du SDK MAM.

- Citrix recommande d'utiliser le SDK MAM pour les applications MDX. Vous pouvez également continuer à utiliser les applications MDX encapsulées jusqu'à ce que le MDX Toolkit ne soit plus pris en charge. Voir Fin de prise en charge.
- Vous ne pouvez pas utiliser le MDX Toolkit pour encapsuler les applications de productivité mobiles Citrix. Obtenez les fichiers MDX des applications de productivité mobile à partir des téléchargements Citrix.

Lorsque vous ajoutez des applications à la console XenMobile, vous effectuez les actions suivantes :

- Configurer les paramètres de l'application
- (Facultatif) Organiser les applications en catégories dans Secure Hub
- (Facultatif) Définir des workflows pour exiger une approbation avant d'autoriser les utilisateurs à accéder à une application
- Déployer des applications pour les utilisateurs

Cet article couvre les workflows généraux pour ajouter des applications. Consultez les articles suivants pour connaître les caractéristiques de la plate-forme :

- Distribuer des applications Android Enterprise
- Distribuer les applications Apple

Types et fonctionnalités d'applications

Le tableau suivant récapitule les types d'applications que vous pouvez déployer avec XenMobile.

Type d'application	Sources	Remarques	Voir
MDX	Applications iOS et Android que vous développez pour vos utilisateurs. Applications de productivité mobiles Citrix.	Développez des applications iOS ou Android avec le SDK MAM ou encapsulez-les avec le MDX Toolkit. Pour les applications de productivité mobiles, téléchargez les fichiers MDX du magasin public à partir des téléchargements Citrix. Ajoutez ensuite les applications à XenMobile.	Ajouter une application MDX
Magasin d'applications public	Applications gratuites ou payantes provenant de magasins d'applications publics tels que Google Play ou Apple App Store.	Chargez les applications, activez MDX sur les applications, puis ajoutez-les à XenMobile.	Ajouter une application d'un magasin d'applications public
Web et SaaS	Votre réseau interne (applications Web) ou un réseau public (SaaS).	Citrix Workspace fournit une authentification unique mobile aux applications SaaS natives à partir d'appareils iOS et Android inscrits à MDM. Vous pouvez également utiliser les connecteurs d'application SAML (Security Assertion Markup Language).	Ajouter une application Web ou SaaS

Type d'application	Sources	Remarques	Voir
Entreprise	Applications privées, y compris les applications Win32, qui ne sont pas compatibles MDX. Applications Android Enterprise privées qui sont compatibles MDX. Les applications d'entreprise résident dans des emplacements Content Delivery Network ou dans des serveurs XenMobile.	Ajoutez les applications à XenMobile.	Ajouter une application d'entreprise
Lien Web	Adresses Web Internet, adresses Web intranet ou applications Web qui ne nécessitent pas d'authentification unique.	Configurez les liens Web dans XenMobile.	Ajouter un lien Web

Lorsque vous planifiez la distribution d'applications, tenez compte des fonctionnalités suivantes :

- À propos des installations silencieuses
- À propos des applications obligatoires et facultatives
- À propos des catégories d'applications
- Activer les applications Microsoft 365
- Appliquer les workflows
- Personnalisation du magasin d'applications et de Citrix Secure Hub

À propos des installations silencieuses

Citrix prend en charge l'installation silencieuse et la mise à niveau d'applications iOS, Android Enterprise et Samsung. Une installation silencieuse signifie que les utilisateurs ne sont pas invités à installer les applications que vous déployez sur l'appareil. Les applications s'installent automatiquement en arrière-plan.

Conditions préalables requises pour une installation silencieuse :

- Pour iOS, placez l'appareil iOS géré en mode supervisé. Pour de plus amples informations, consultez la section Stratégie Importer le profil iOS et macOS.
- Pour Android Enterprise, les applications s'installent sur le profil de travail Android sur l'appareil. Pour de plus amples informations, consultez la section Android Enterprise.
- Pour les appareils Samsung, activez Samsung Knox sur l'appareil.

  Pour ce faire, vous devez définir la stratégie de clé de licence MDM Samsung pour générer des clés de licence Knox et Samsung ELM. Pour de plus amples informations, consultez la section Stratégies de clé de licence MDM Samsung.

À propos des applications obligatoires et facultatives

Lorsque vous ajoutez des applications à un groupe de mise à disposition, vous devez choisir si elles sont facultatives ou requises. Citrix recommande le déploiement des applications comme **requises**.

- Les applications requises s'installent silencieusement sur les appareils utilisateur, ce qui minimise l'interaction. L'activation de cette fonctionnalité permet également aux applications de se mettre à jour automatiquement.
- Les applications facultatives permettent aux utilisateurs de choisir les applications à installer, mais les utilisateurs doivent initier l'installation manuellement via Secure Hub.

Pour les applications marquées comme requises, les utilisateurs peuvent recevoir les mises à jour plus rapidement dans certaines situations, par exemple :

- Vous chargez une nouvelle application et la marquez comme requise.
- Vous marquez une application existante comme requise.
- Un utilisateur supprime une application requise.
- Une mise à jour de Secure Hub est disponible.

Configuration requise pour le déploiement automatique des applications requises

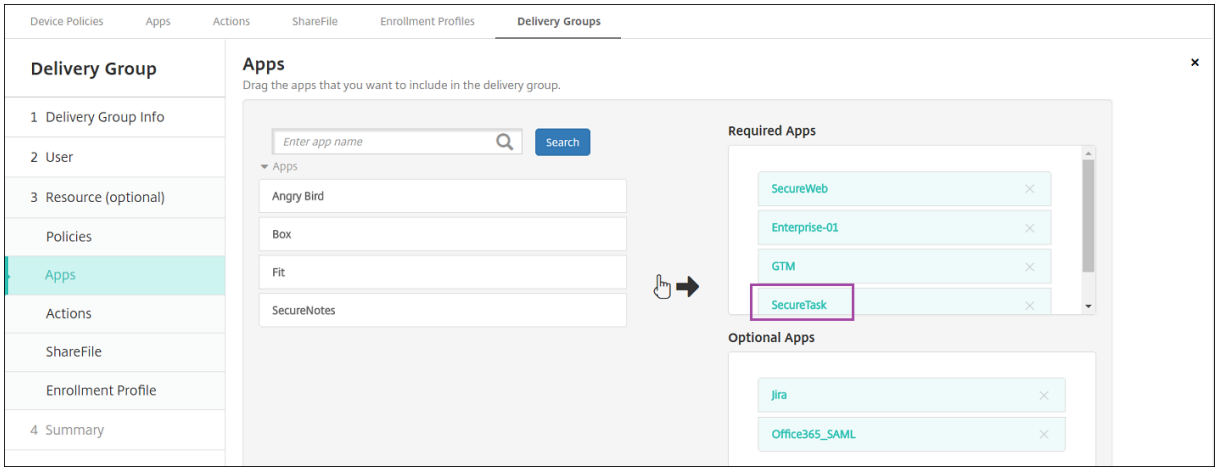
- XenMobile Server 10.6 (version minimum)
- Secure Hub 10.5.15 pour iOS et 10.5.20 pour Android (versions minimales)
- SDK MAM ou MDX Toolkit 10.6 (version minimale)
- Propriété de serveur personnalisée, force.server.push.required.apps

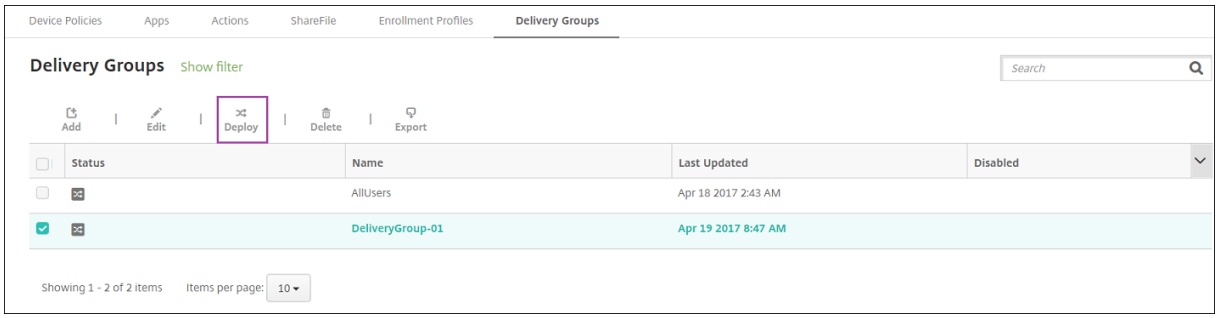
  Le déploiement forcé des applications requises est désactivé par défaut. Pour activer la fonctionnalité, créez une propriété de serveur clé personnalisée. Définissez la **Clé** et le **Nom d'affichage** sur **force.server.push.required.apps** et définissez la **Valeur** sur **true**.

- Une fois que vous avez mis à niveau XenMobile Server et Secure Hub : les utilisateurs dotés d'appareils inscrits doivent se déconnecter, puis se connecter à Secure Hub, une seule fois, pour obtenir les mises à jour du déploiement des applications requises.

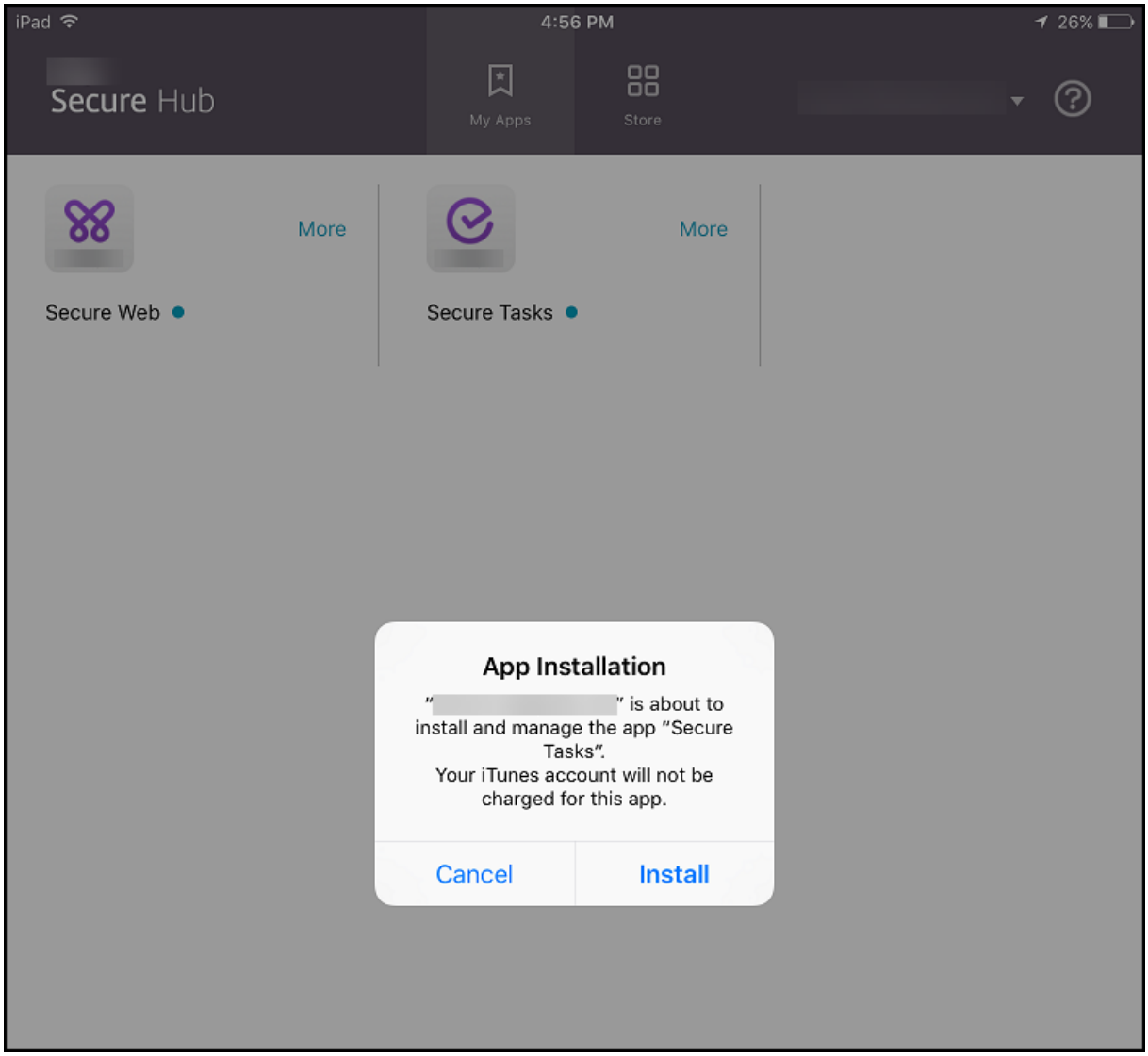
Exemples

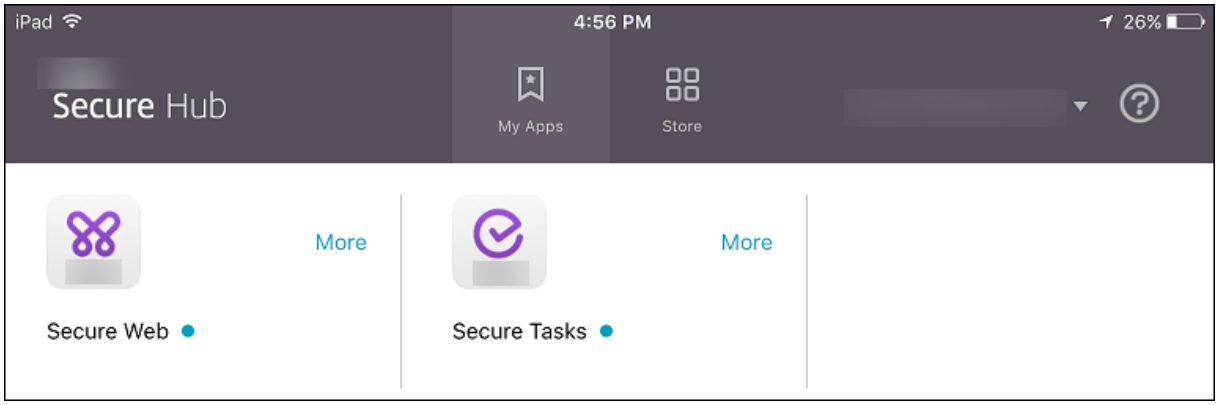
Les exemples suivants expliquent la séquence d'ajout d'une application nommée Secure Tasks à un groupe de mise à disposition et de déploiement du groupe de mise à disposition.





Une fois l'application Secure Tasks déployée vers l'appareil de l'utilisateur, Secure Hub invite l'utilisateur à installer l'application.





Important :

Les applications MDX requises, y compris les applications d'entreprise et les applications de magasin d'applications publiques, sont immédiatement mises à niveau. La mise à niveau se

> produit même si vous configurez une stratégie MDX pour une période de grâce de mise à jour d'application et que l'utilisateur choisit de mettre à niveau l'application ultérieurement.

Workflow des applications iOS requises pour les applications d'entreprise et de magasin public

1. Déployer l'application XenMobile lors de l'inscription initiale. L'application requise est installée sur l'appareil.
2. Mettre à jour l'application dans la console XenMobile.
3. Utiliser la console XenMobile pour déployer les applications requises.
4. L'application sur l'écran d'accueil est mise à jour. Et, pour les applications de magasin public, la mise à niveau démarre automatiquement. Les utilisateurs ne sont pas invités à mettre à jour.
5. Les utilisateurs ouvrent l'application à partir de l'écran d'accueil. Les applications se mettent à niveau immédiatement, même si vous définissez une période de grâce de mise à jour des applications et que l'utilisateur choisit de mettre à niveau l'application plus tard.

Workflow des applications Android requises pour les applications d'entreprise

1. Déployer l'application XenMobile lors de l'inscription initiale. L'application requise est installée sur l'appareil.
2. Utiliser la console XenMobile pour déployer les applications requises.
3. L'application est mise à niveau. (Les appareils Nexus invitent à installer les mises à jour, mais les appareils Samsung effectuent une installation silencieuse).
4. Les utilisateurs ouvrent l'application à partir de l'écran d'accueil. Les applications se mettent à niveau immédiatement, même si vous définissez une période de grâce de mise à jour des applications et que l'utilisateur choisit de mettre à niveau l'application plus tard. (Les appareils Samsung effectuent une installation silencieuse.)

Workflow des applications Android requises pour les applications de magasin public

1. Déployer l'application XenMobile lors de l'inscription initiale. L'application requise est installée sur l'appareil.
2. Mettre à jour l'application dans la console XenMobile.
3. Utiliser la console XenMobile pour déployer les applications requises. Ou, ouvrir le magasin Secure Hub sur l'appareil. L'icône de mise à jour est affichée dans le magasin.
4. La mise à niveau démarre automatiquement. (Les appareils Nexus invitent les utilisateurs à installer la mise à jour.)
5. Ouvrez l'application à partir de l'écran d'accueil. L'application est mise à niveau. Les utilisateurs ne sont pas invités à mettre à jour après une période de grâce. (Les appareils Samsung effectuent une installation silencieuse.)

Désinstaller une application lorsque celle-ci est configurée selon les besoins

Vous pouvez permettre aux utilisateurs de désinstaller une application configurée selon les besoins. Accédez à **Configurer> Groupes de mise à disposition** et déplacez l'application de la zone **Applications requises** vers la zone **Applications facultatives**.

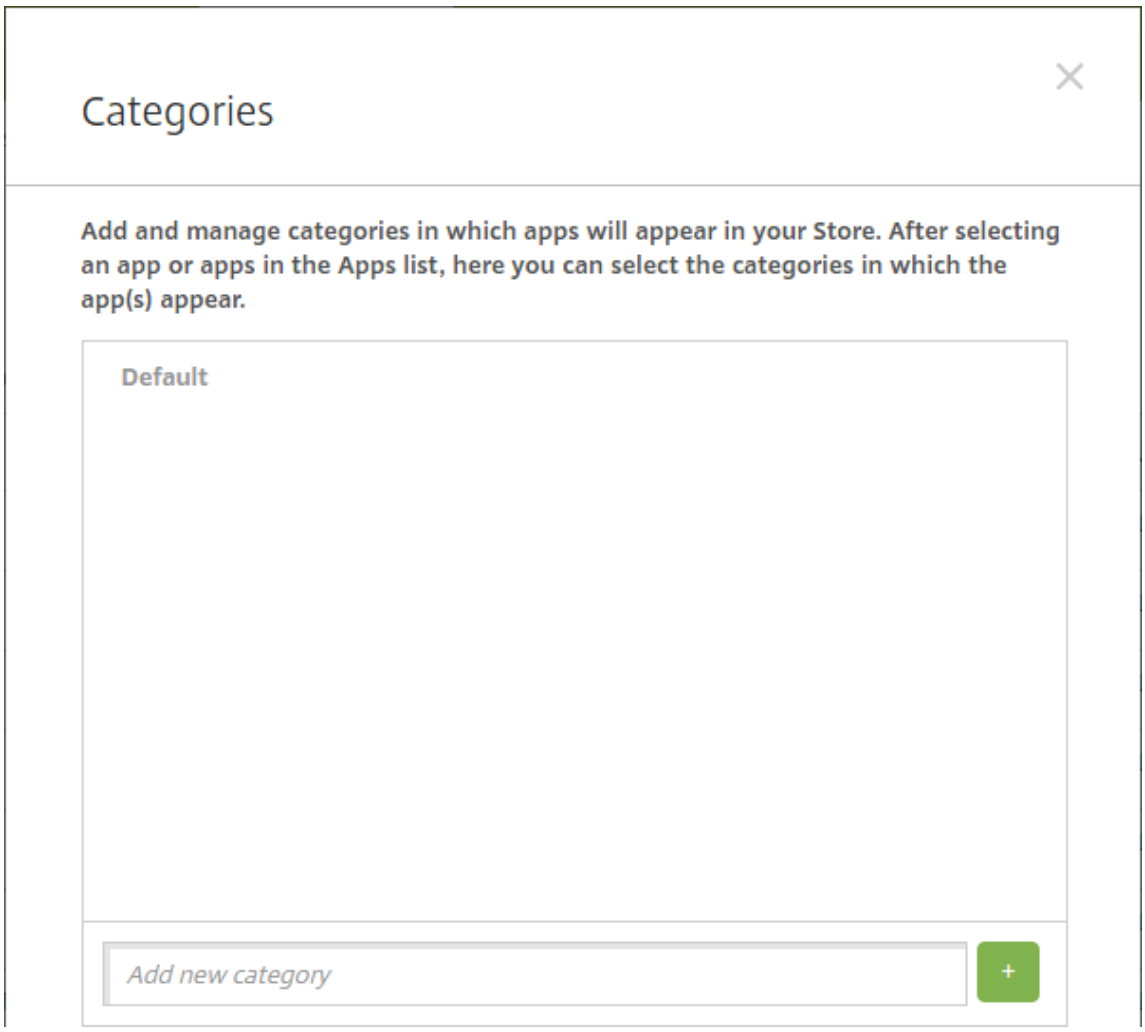
Recommandation : utilisez un groupe de mise à disposition spécial pour modifier temporairement une application et la passer en application facultative afin de permettre à des utilisateurs spécifiques de la désinstaller. Vous pouvez ensuite modifier une application requise existante et la passer en application facultative, déployer l'application sur ce groupe de mise à disposition, puis désinstaller l'application à partir de ces appareils. Si vous souhaitez ensuite que les futures inscriptions de ce groupe de mise à disposition disposent de l'application, vous pouvez redéfinir l'application et la passer en application requise.

À propos des catégories d'applications

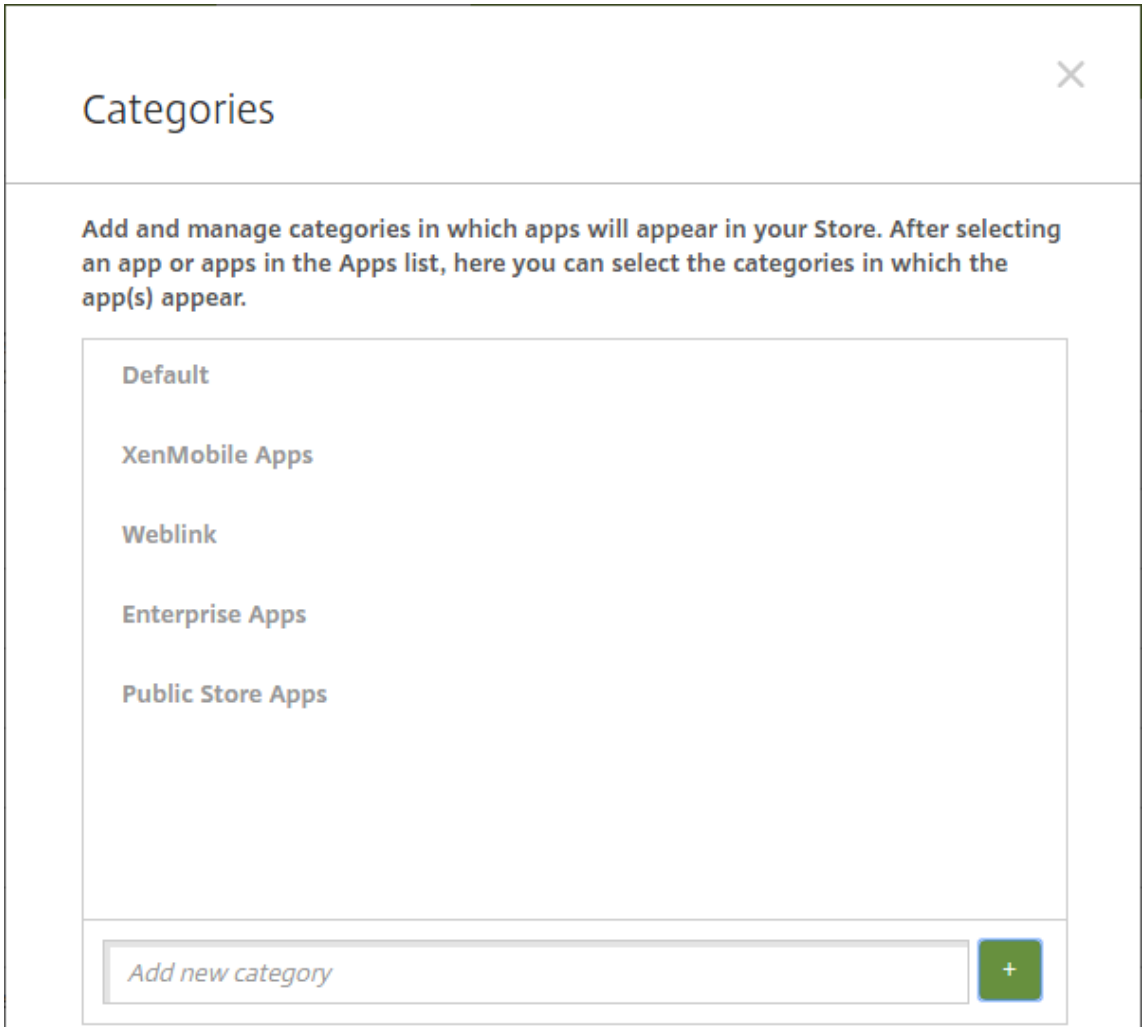
Lorsque les utilisateurs se connectent à Secure Hub, ils obtiennent une liste des applications, des liens Web et des magasins que vous avez configurés dans XenMobile. Vous pouvez utiliser les catégories d'applications pour permettre aux utilisateurs d'accéder uniquement à certaines applications, liens Web ou magasins. Par exemple, il est possible de créer une catégorie Finance et d'y ajouter des applications ayant trait uniquement au secteur de la finance. Ou vous pouvez configurer une catégorie Ventes à laquelle vous attribuez des applications de ventes.

Lorsque vous ajoutez ou modifiez une application, un lien Web ou un magasin, vous pouvez ajouter l'application à l'une ou plusieurs des catégories configurées.

1. Dans la console XenMobile, cliquez sur **Configurer > Applications > Catégorie**. La boîte de dialogue **Catégories** s'affiche.



2. Pour chaque catégorie que vous voulez ajouter, procédez comme suit :
   - Tapez le nom de la catégorie que vous souhaitez ajouter dans le champ **Ajouter une nouvelle catégorie** en bas de la boîte de dialogue. Par exemple, vous pouvez entrer Applications d'entreprise pour créer une catégorie pour les applications d'entreprise.
   - Cliquez sur le signe plus (+) pour ajouter la catégorie. La nouvelle catégorie est ajoutée et s'affiche dans la boîte de dialogue **Catégories**.



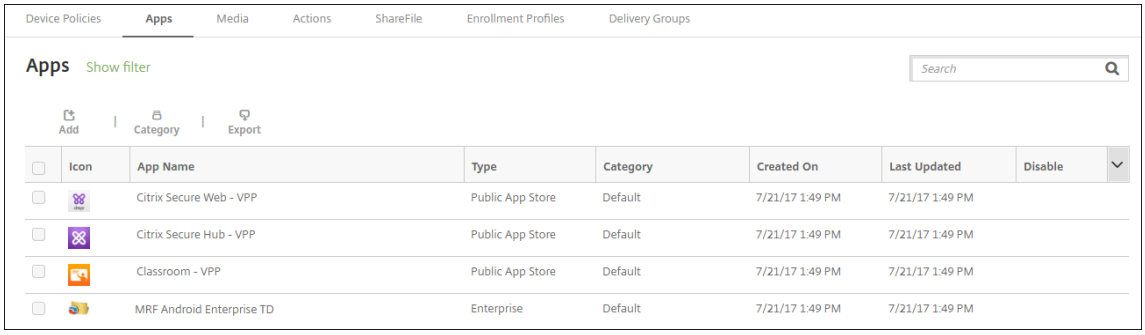
3. Lorsque vous avez terminé d'ajouter des catégories, fermez la boîte de dialogue **Catégories**.
4. Sur la page **Applications**, vous pouvez placer une application existante dans une nouvelle catégorie.
    - Sélectionnez l'application que vous souhaitez classer.
    - Cliquez sur **Modifier**. La page **Informations sur l'application** s'affiche.
    - Dans la liste **Catégorie d'application**, appliquez la nouvelle catégorie en sélectionnant la case à cocher appropriée. Désélectionnez les cases à cocher pour les catégories que vous ne souhaitez pas appliquer à l'application.
    - Cliquez sur l'onglet **Attribution de groupes de mise à disposition** ou cliquez sur **Suivant** sur chacune des pages suivantes pour compléter les autres pages de configuration de l'application.
    - Cliquez sur **Enregistrer** sur la page **Attribution de groupes de mise à disposition** pour appliquer la catégorie. La nouvelle catégorie est appliquée à l'application et l'application s'affiche dans le tableau **Applications**.

Ajouter une application MDX

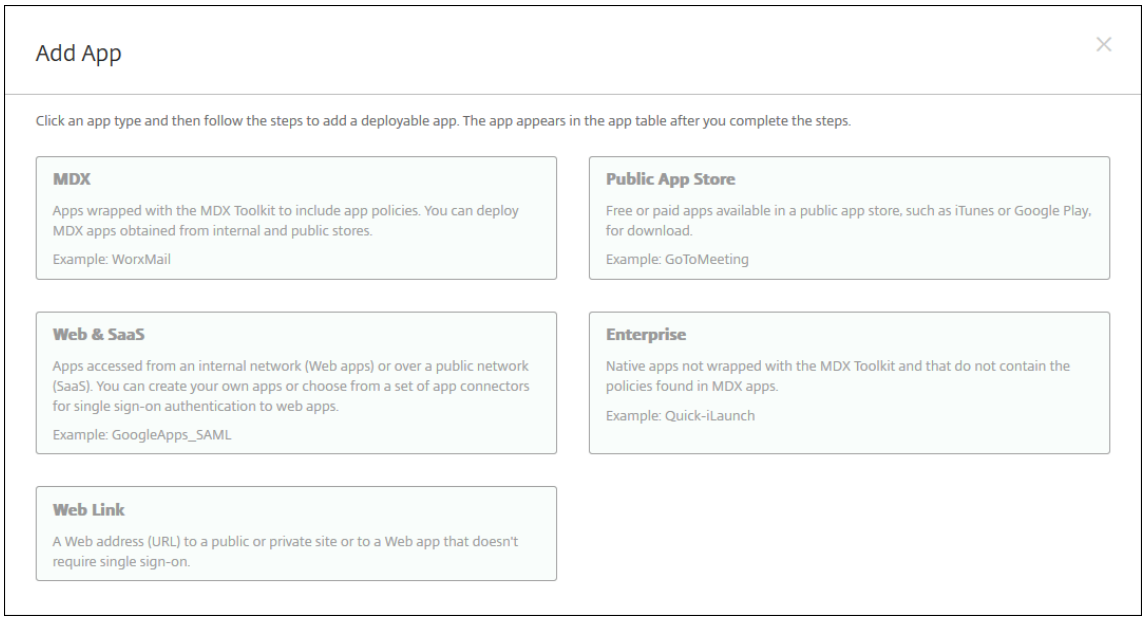
Lorsque vous recevez un fichier MDX pour une application iOS ou Android, vous pouvez charger l'application dans XenMobile. Après le chargement de l'application, vous pouvez configurer les détails de l'application et les paramètres de stratégie. Pour plus d'informations sur les stratégies applicatives disponibles pour chaque type de plate-forme, consultez la section :

- Présentation du SDK MAM
- Synopsis des stratégies MDX

1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'affiche.



2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



3. Cliquez sur **MDX**. La page **Informations sur l'application MDX** s'affiche.
4. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous **Nom de l'application** dans le tableau **Applications**.

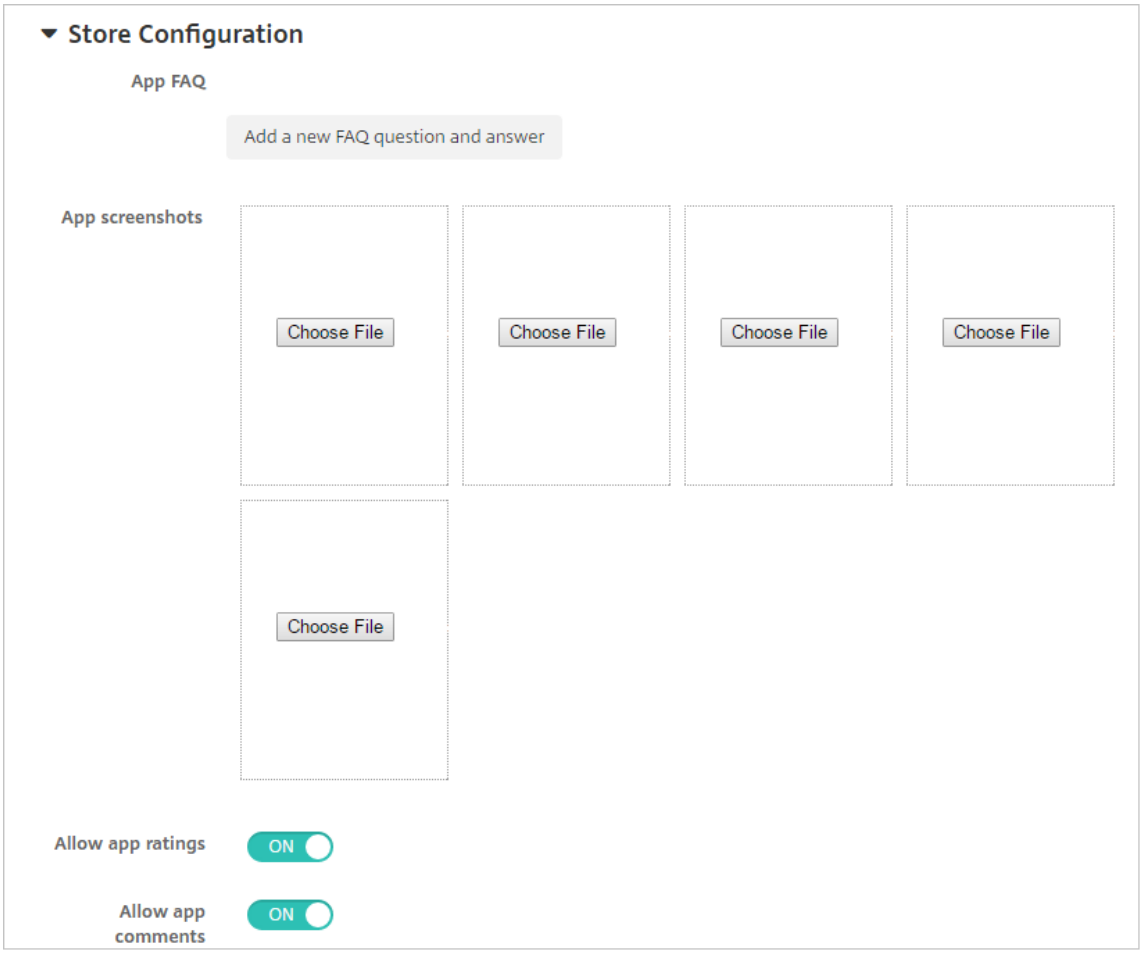
- **Description :** entrez une description pour l'application (facultatif).
- **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.

5. Cliquez sur **Suivant**. La page **Plates-formes d'applications** s'affiche.
6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.
7. Pour sélectionner un fichier MDX à charger, cliquez sur **Charger** et accédez à l'emplacement du fichier.
8. Sur la page **Détails de l'application**, configurez les paramètres suivants :

   - **Nom du fichier :** entrez le nom du fichier associé à l'application.
   - **Description de l'application :** entrez une description pour l'application.
   - **Version de l'application :** si vous le souhaitez, entrez le numéro de version de l'application.
   - **ID de package :** entrez l'ID du package de l'application, obtenu à partir du Google Play Store d'entreprise.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
   - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.
   - **Supprimer l'application si le profil MDM est supprimé :** sélectionnez cette option si vous souhaitez supprimer l'application d'un appareil lorsque le profil MDM est supprimé La valeur par défaut est **Activé**.
   - **Empêcher la sauvegarde des données d'application :** sélectionnez cette option si vous souhaitez empêcher les utilisateurs de sauvegarder les données de l'application sur les appareils iOS. La valeur par défaut est **Activé**.
   - **Suivi du produit :** spécifiez le suivi du produit que vous souhaitez transférer aux appareils iOS. Si vous avez un suivi conçu à des fins de test, vous pouvez le sélectionner et l'affecter à vos utilisateurs. La valeur par défaut est **Production**.
   - **Forcer l'application à être gérée :** lors de l'installation d'une application non gérée, sélectionnez cette option pour spécifier si vous souhaitez inviter les utilisateurs à autoriser l'application à être gérée sur les appareils non supervisés. La valeur par défaut est **Activé**.
   - **Application déployée via l'achat en volume :** indiquez si vous souhaitez déployer l'application à l'aide de l'achat en volume d'Apple. Si vous déployez une version MDX de l'application et que vous utilisez l'achat en volume pour déployer l'application lorsque

cette option est définie sur **Activé**, Secure Hub affiche uniquement l'instance d'achat en volume. La valeur par défaut est **Désactivé**.

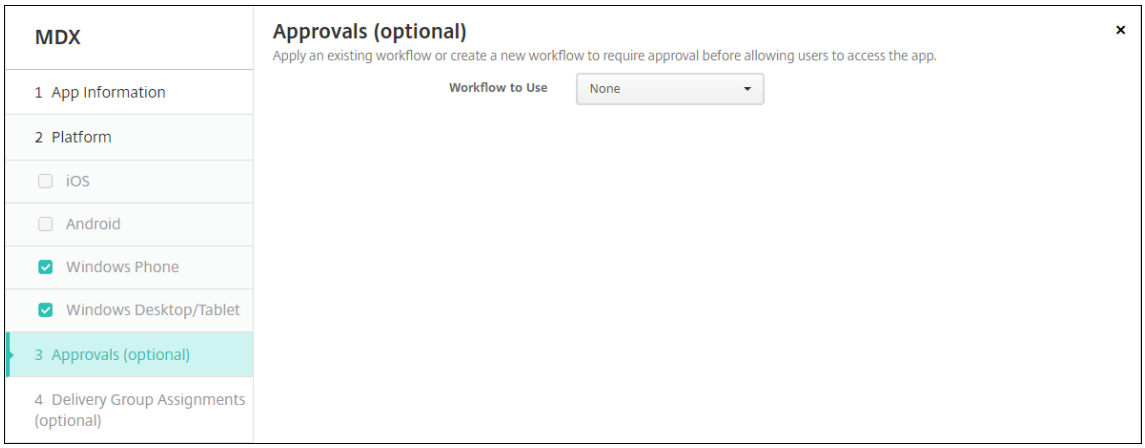
9. Configurez les **stratégies MDX**. Les stratégies MDX varient selon la plate-forme et incluent des options dans des domaines de stratégie tels que l'authentification, la sécurité de l'appareil et les restrictions applicatives. Dans la console, les stratégies ont une info-bulle qui décrit chacune d'entre elles.
10. Configurez les règles de déploiement. Pour plus d'informations, consultez la section Règles de déploiement.
11. Développez **Configuration du magasin**.



- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.
- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des

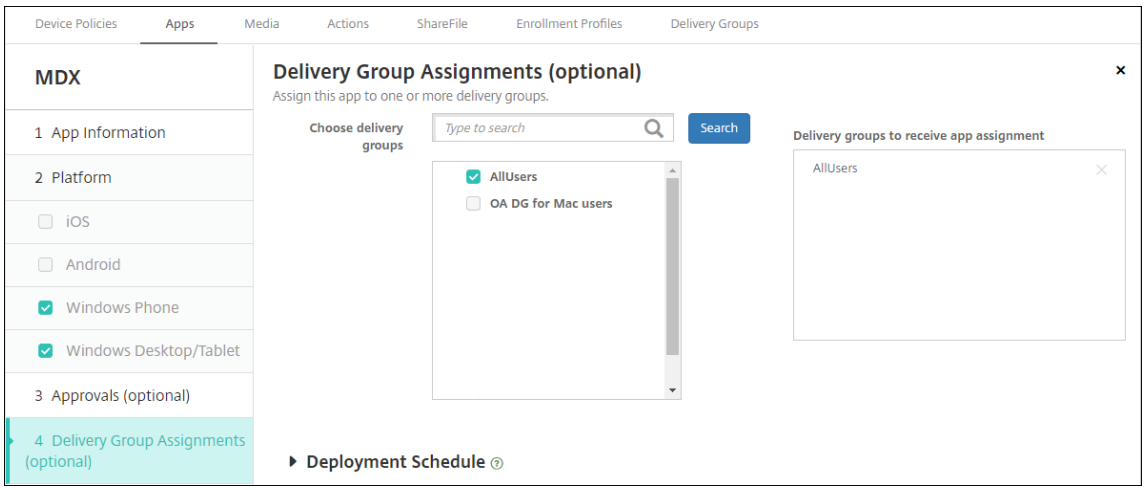
commentaires sur l'application dans l'App Store.

12. Cliquez sur **Suivant**. La page **Approbations** s'affiche.



Pour utiliser des workflows afin d'exiger une approbation avant d'autoriser les utilisateurs à accéder à l'application, consultez la section Appliquer les workflows. Si vous ne souhaitez pas configurer des workflows d'approbation, passez à l'étape suivante.

13. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.



14. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

15. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- **Déployer :** choisissez cette option si vous souhaitez déployer l'application sur les appareils. La valeur par défaut est **Activé**.
- **Calendrier de déploiement :** choisissez l'option **Maintenant** ou **Plus tard** pour déployer l'application. Si vous sélectionnez **Plus tard**, configurez une date et une heure pour déployer l'application. La valeur par défaut est **Maintenant**.

- **Conditions de déploiement :** choisissez **À chaque connexion** pour déployer l'application chaque fois que l'appareil se connecte. Choisissez **Uniquement lorsque le déploiement précédent a échoué** pour déployer l'application lorsque l'appareil n'a pas réussi à recevoir l'application. L'option par défaut est **À chaque connexion**.

L'option **Déployer pour les connexions permanentes** s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

16. Cliquez sur **Enregistrer**.

Ajouter une application d'un magasin d'applications public

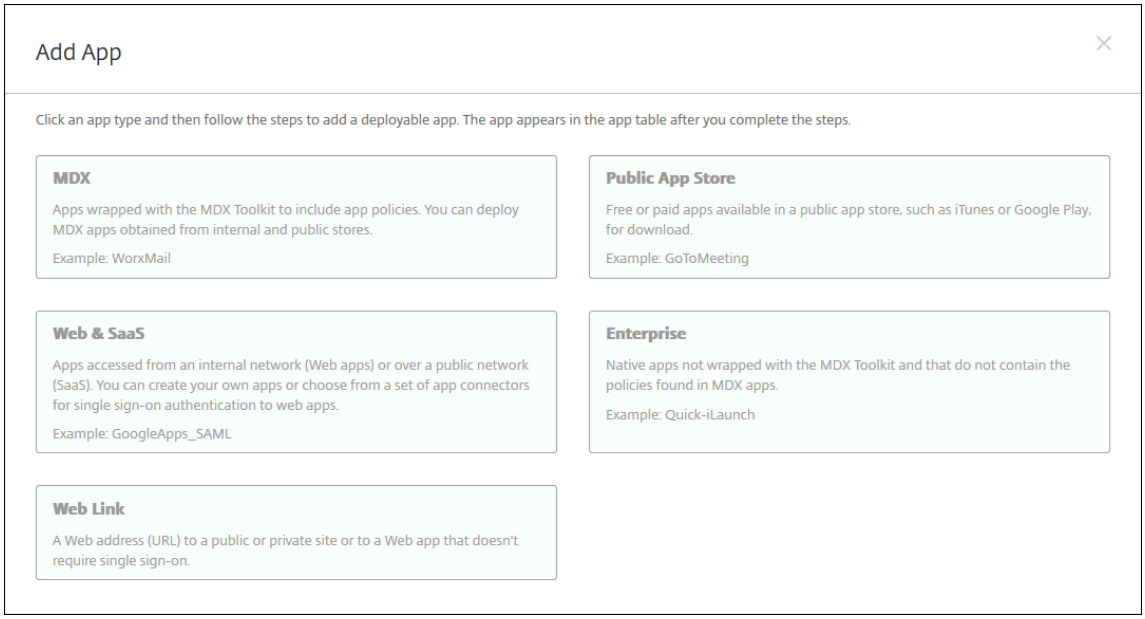
Vous pouvez ajouter des applications gratuites ou payantes à XenMobile qui sont disponibles dans un magasin d'applications public, tel que l'App Store Apple ou Google Play.

Vous pouvez configurer des paramètres afin de récupérer les noms et descriptions des applications dans l'App Store d'Apple. Lorsque vous récupérez les informations d'application dans le magasin, XenMobile remplace le nom et la description existants. Configurez manuellement les informations de l'application Google Play Store.

Lorsque vous ajoutez une application payante provenant d'un magasin d'applications public pour Android Enterprise, vous pouvez vérifier l'état de la licence d'achat groupé. Cet état représente le nombre total de licences disponibles, le nombre en cours d'utilisation et l'adresse e-mail de chaque utilisateur qui consomme des licences. Le plan Achat groupé pour Android Enterprise simplifie la recherche, l'achat et la distribution d'applications et d'autres données en bloc pour une organisation.

Configurez les informations de l'application et choisissez les plates-formes sur lesquelles les mettre à disposition :

1. Dans la console XenMobile, cliquez sur **Configurer > Applications > Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



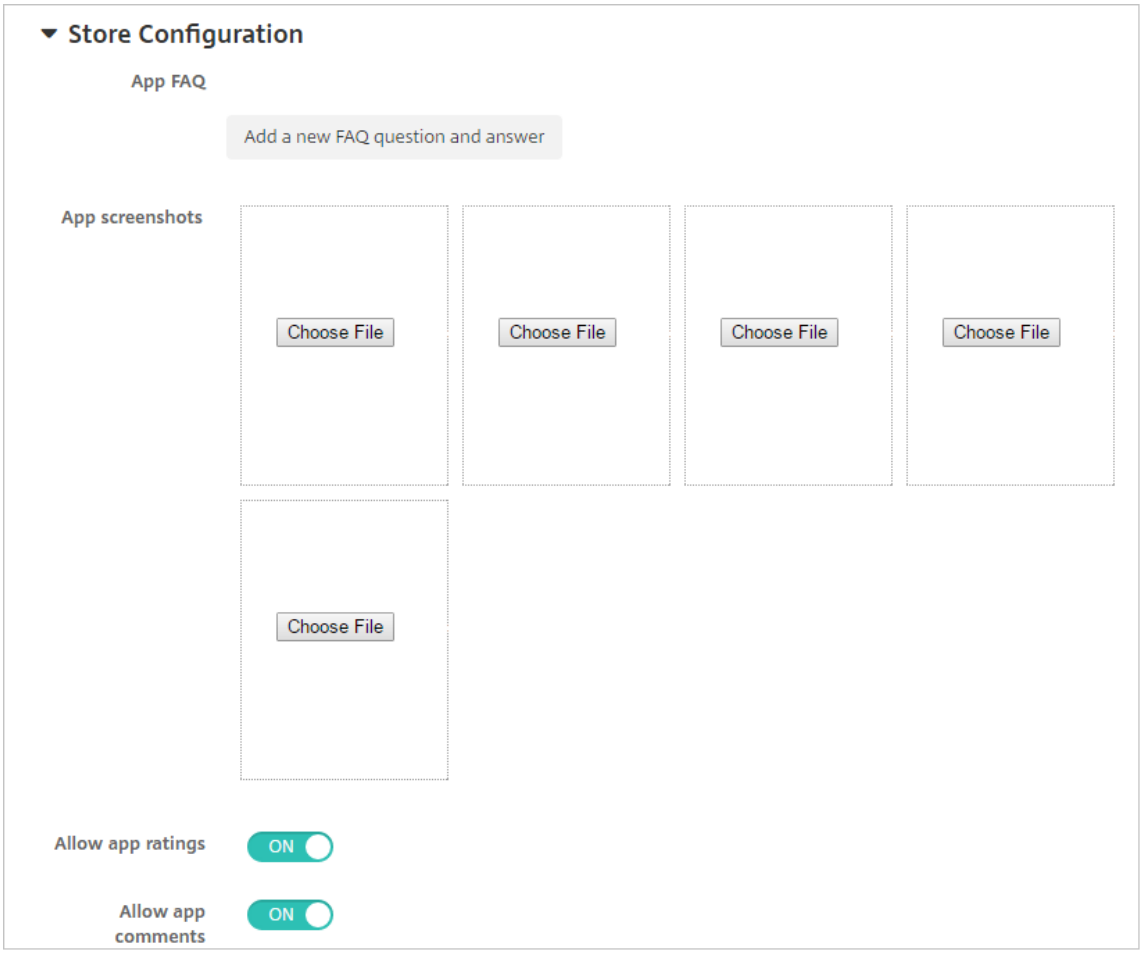
2. Cliquez sur **Magasin d'applications public**. La page **Informations sur l'application** s'affiche.
3. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous **Nom de l'application** dans le tableau **Applications**.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.
4. Cliquez sur **Suivant**. La page **Plates-formes d'applications** s'affiche.
5. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Ensuite, vous configurez les paramètres de l'application pour chaque plate-forme. Consultez :

- Configurer les paramètres d'application pour les applications Google Play
- Applications gérées du magasin d'applications
- Configurer les paramètres applicatifs pour les applications iOS

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, définissez les règles de déploiement de cette plate-forme et la configuration du magasin d'applications.

1. Configurez les règles de déploiement. Pour plus d'informations, consultez la section Règles de déploiement.
2. Développez **Configuration du magasin**.



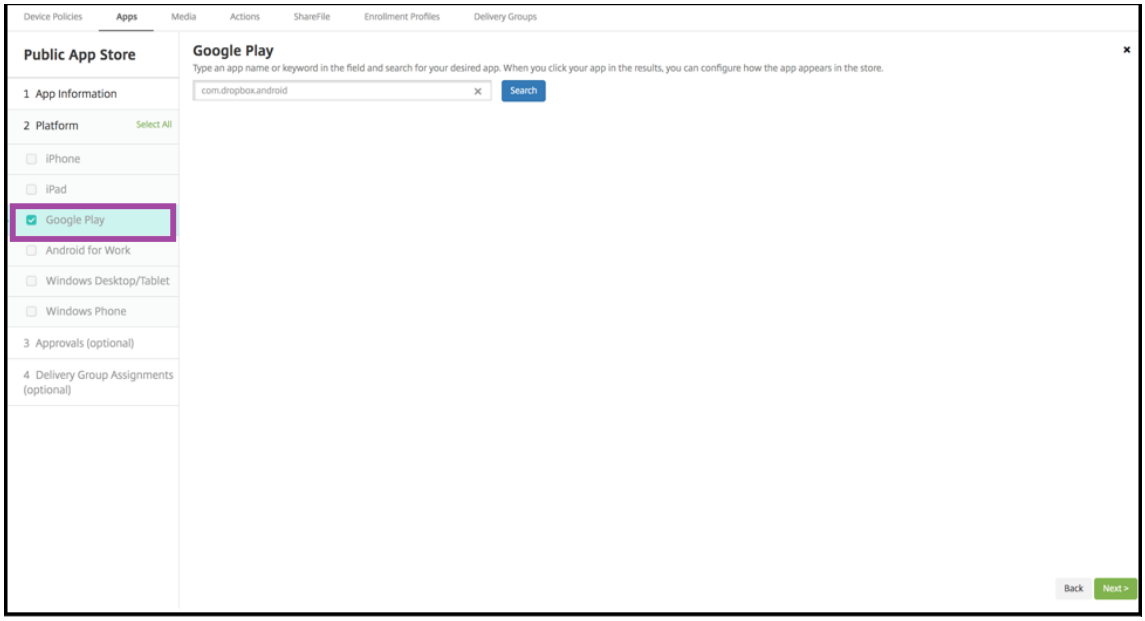
- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.
- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des commentaires sur l'application dans l'App Store.

Configurer les paramètres d'application pour les applications Google Play

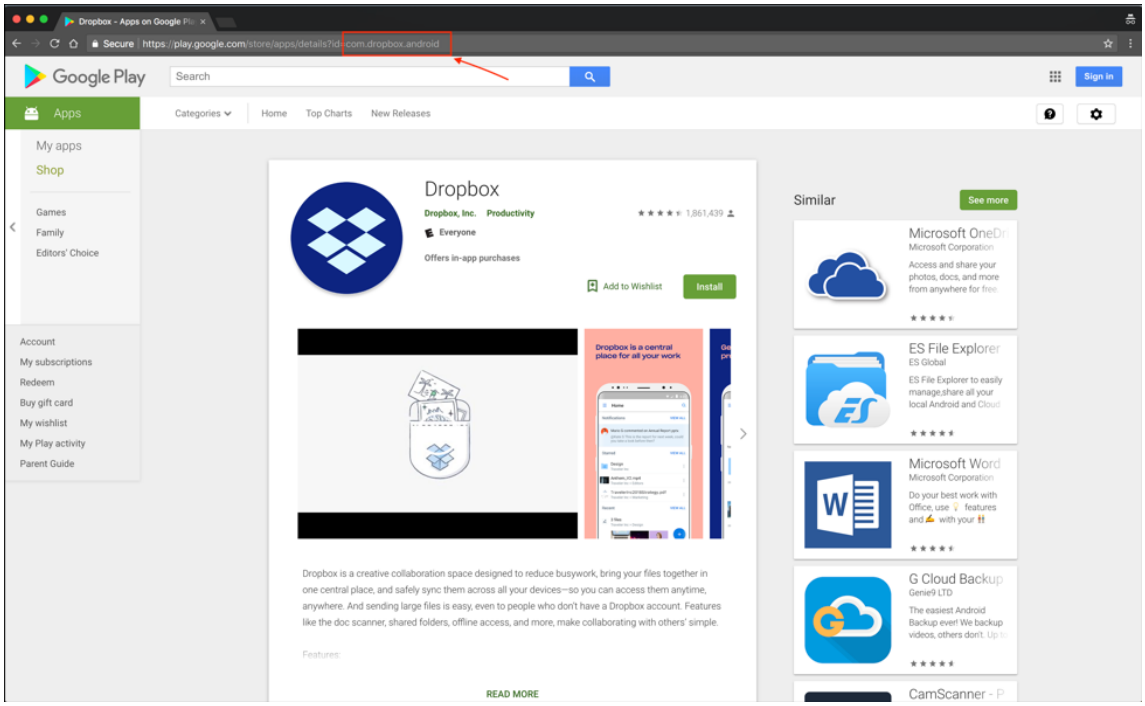
> **Remarque** pour rendre toutes les applications du Google Play Store accessibles depuis le Google Play d'entreprise, utilisez la propriété de XenMobile Server **Accéder à toutes les applications du Google Play Store d'entreprise**. Consultez Propriétés du serveur. La définition de cette propriété sur **true** autorise les applications du Google Play Store public pour tous les utilisateurs d'Android Enterprise. Vous pouvez ensuite utiliser la stratégie Restrictions pour contrôler l'accès à ces applications.

La configuration des paramètres des applications Google Play Store nécessite des étapes différentes de celles des applications d'autres plateformes. Vous devez configurer manuellement les informations de l'application Google Play Store.

1. Assurez-vous que **Google Play** est sélectionné sous **Plates-formes**.

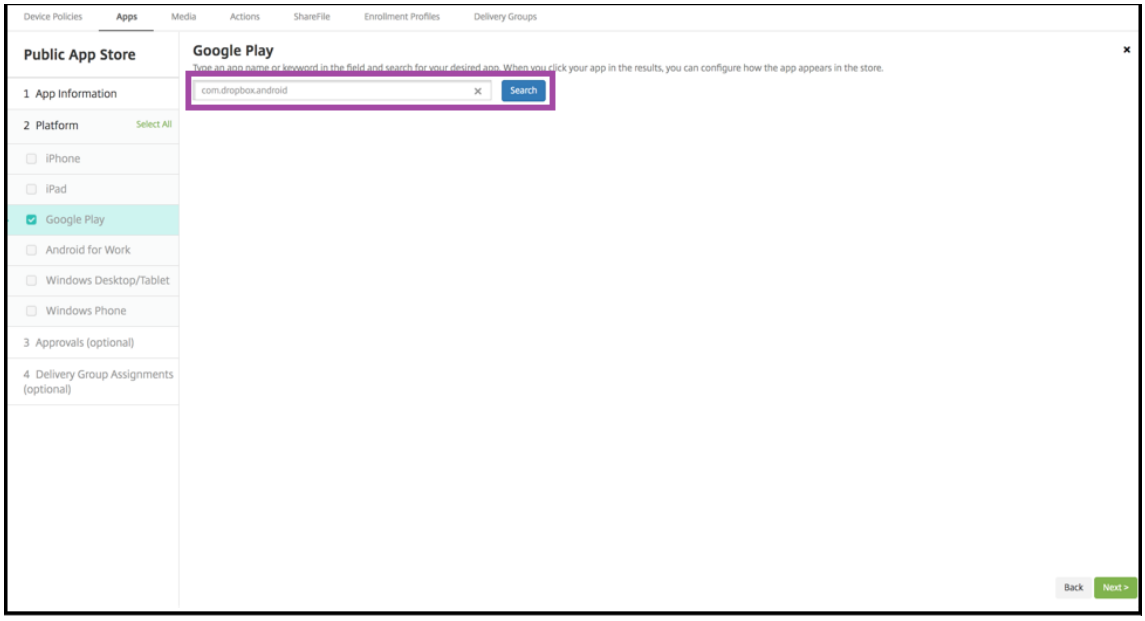


2. Accédez à Google Play. À partir de Google Play, copiez l'ID de package. L'ID se trouve dans l'URL de l'application.

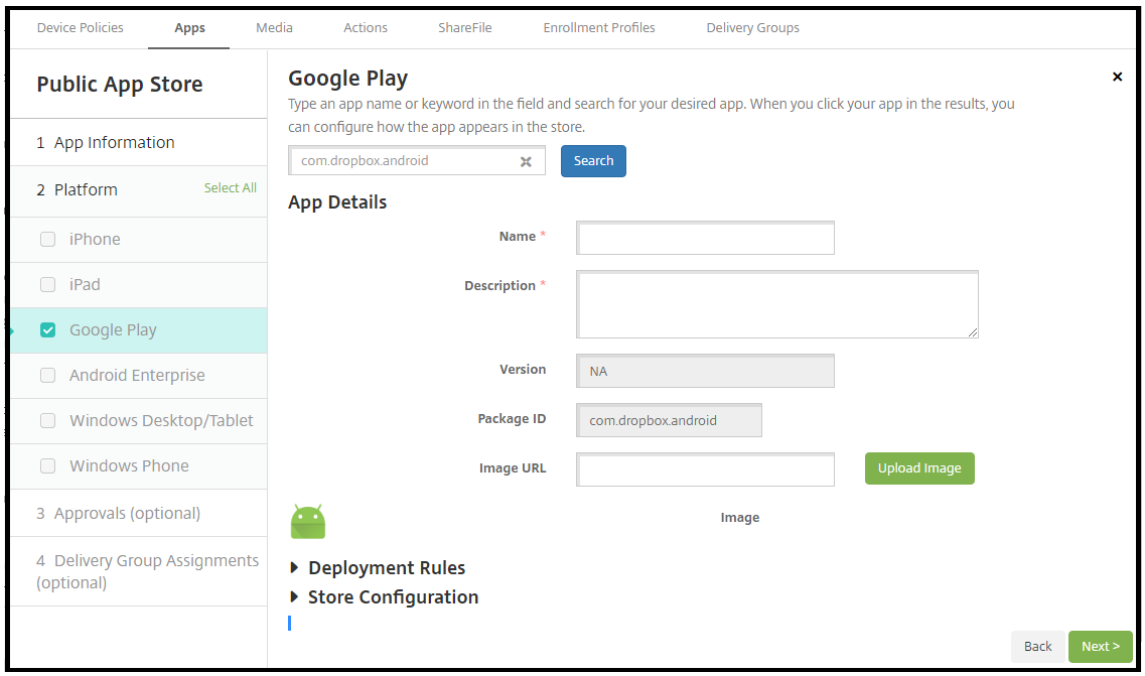


3. Lorsque vous ajoutez une application provenant d'un magasin d'applications public dans la

console XenMobile Server, collez l'ID de package dans la barre de recherche. Cliquez sur **Search**.



4. Si l'ID de package est valide, une interface utilisateur s'affiche pour vous permettre d'entrer les détails de l'application.



5. Vous pouvez configurer l'URL pour que l'image apparaisse avec l'application dans le magasin. Pour utiliser l'image de Google Play :

   a) Accédez à Google Play. Cliquez avec le bouton droit sur l'image de l'application et copiez l'adresse de l'image.

   b) Collez l'adresse de l'image dans le champ **URL d'image**.

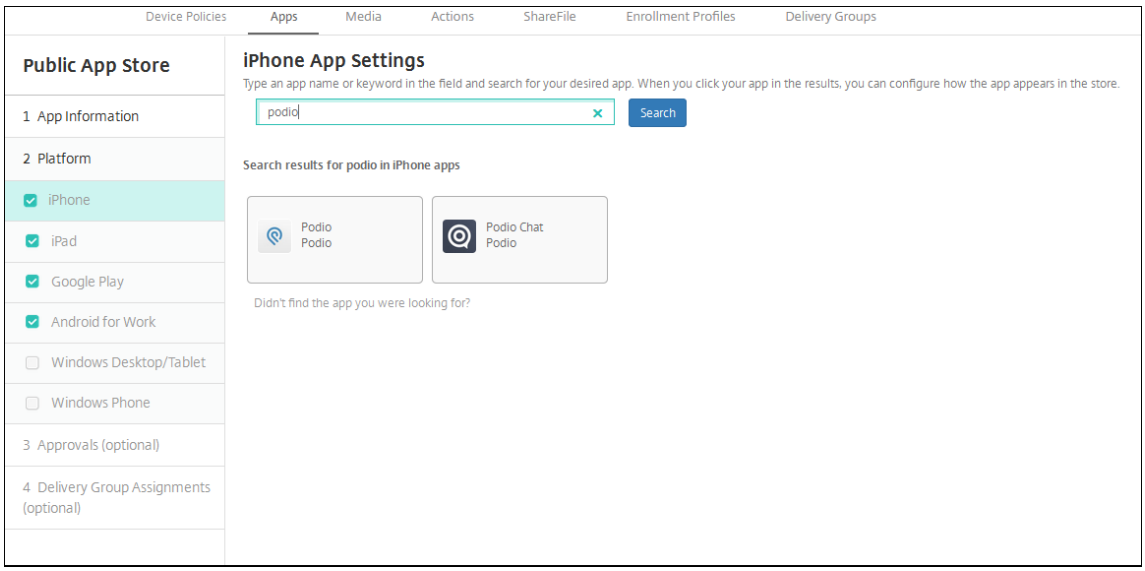
c) Cliquez sur **Charger image**. L'image apparaît à côté de **Image**.

Si vous ne configurez pas d'image, l'image Android générique apparaît avec l'application.

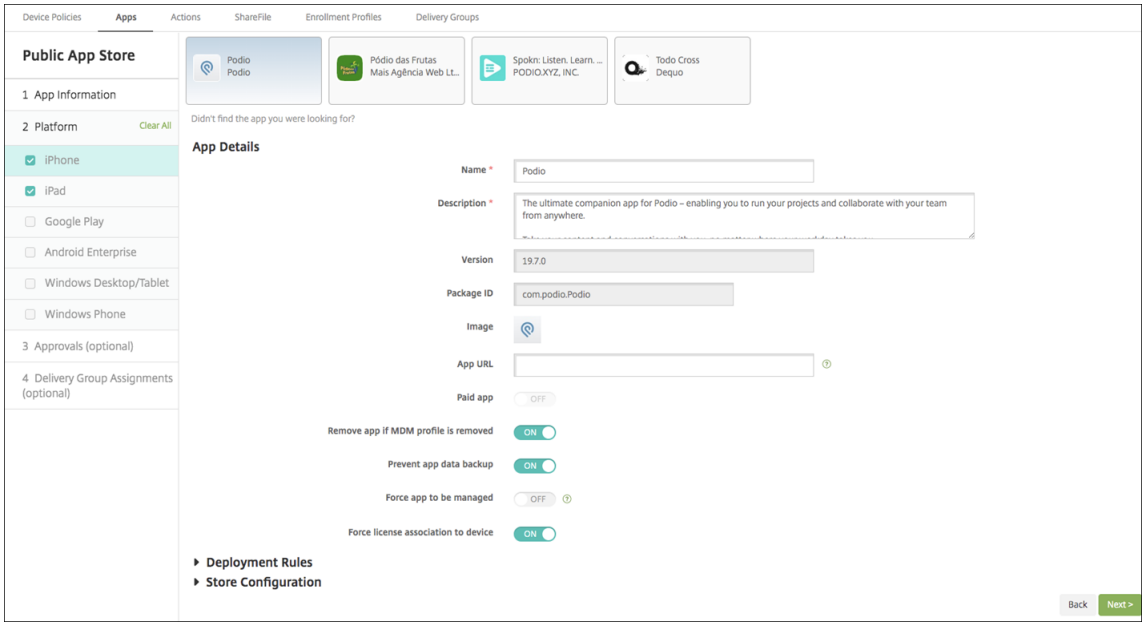
Configurer les paramètres applicatifs pour les applications iOS

1. Entrez le nom de l'application dans la zone de recherche et cliquez sur **Rechercher**. Les applications correspondant aux critères de recherche s'affichent. Les applications correspondant aux critères de recherche s'affichent.

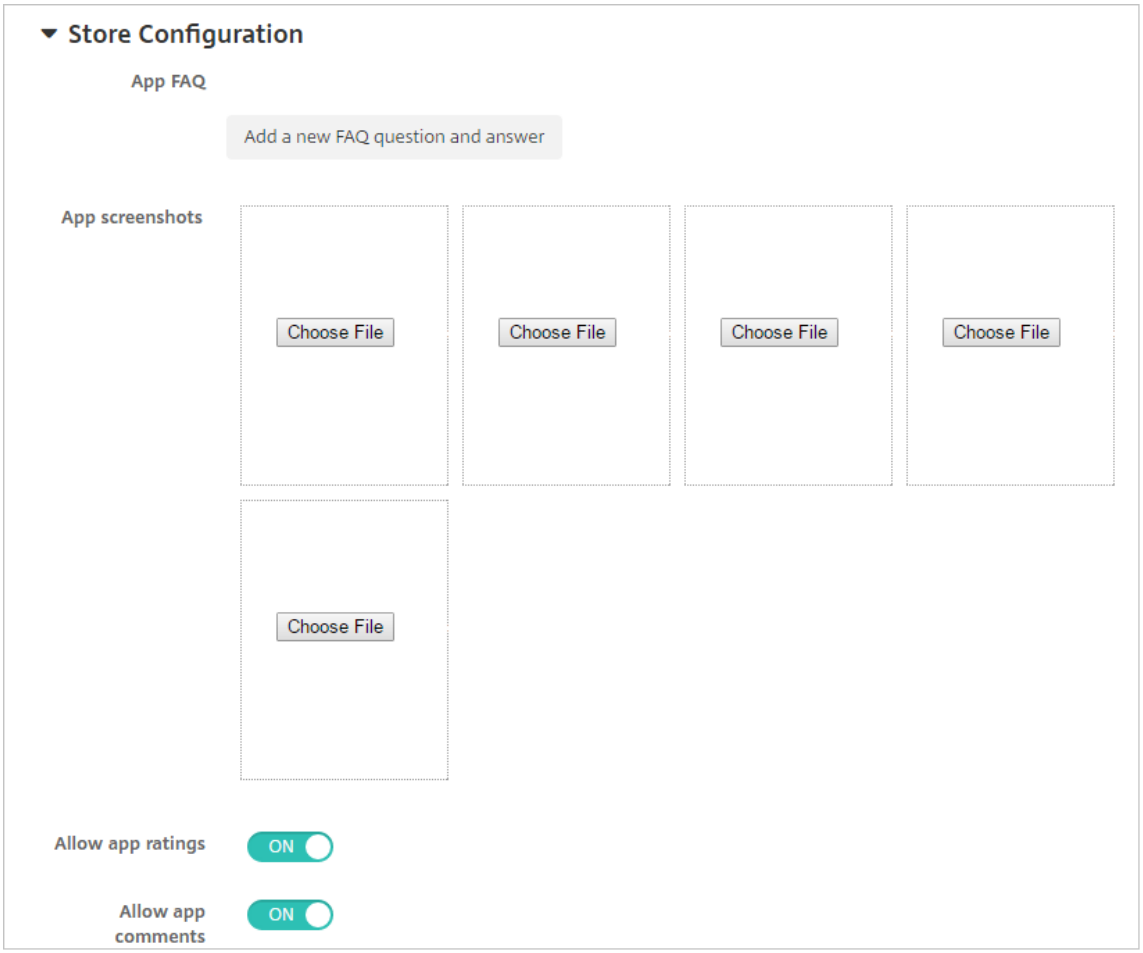
   La figure suivante illustre le résultat de la recherche pour **podio** dans les applications de l'iPhone.



2. Cliquez sur chaque application que vous souhaitez ajouter.
3. Les champs **Détails sur l'application** sont ensuite pré-remplis avec les informations relatives à l'application choisie (y compris le nom, la description, le numéro de version et l'image).



4. Pour configurer ces paramètres :
    - Si nécessaire, modifiez le nom et la description de l'application.
    - **Application payante :** ce champ est préconfiguré et ne peut pas être modifié.
    - **Supprimer l'application si le profil MDM est supprimé :** sélectionnez cette option si vous souhaitez supprimer l'application lorsque le profil MDM est supprimé. La valeur par défaut est **Activé**.
    - **Empêcher la sauvegarde des données d'application :** sélectionnez cette option si vous souhaitez empêcher l'application de sauvegarder les données. La valeur par défaut est **Activé**.
    - **Suivi du produit :** spécifiez le suivi du produit que vous souhaitez transférer aux appareils utilisateur. Si vous avez un suivi conçu à des fins de test, vous pouvez le sélectionner et l'affecter à vos utilisateurs. La valeur par défaut est **Production**.
    - **Forcer l'application à être gérée :** sélectionnez cette option pour spécifier si, lors de l'installation d'une application non gérée, vous souhaitez inviter les utilisateurs à autoriser l'application à être gérée sur les appareils non supervisés. La valeur par défaut est **Désactivé.** Disponible dans iOS 9.0 et versions ultérieures.
    - **Forcer l'association de licence avec l'appareil :** sélectionnez cette option si vous voulez associer une application qui a été développée en association avec un périphérique à un périphérique plutôt qu'à un utilisateur. Disponible sur iOS 9 et version ultérieure. Si l'application que vous avez choisie ne prend pas en charge l'attribution à un appareil, ce champ ne peut pas être modifié.
5. Configurez les règles de déploiement. Pour plus d'informations, consultez la section Règles de déploiement.
6. Développez **Configuration du magasin**.



- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.
- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des commentaires sur l'application dans l'App Store.

7. Pour iPhone ou iPad, développez **Achat en volume**.

   a) Pour permettre à XenMobile d'appliquer une licence d'achat en volume pour l'application : dans la liste **Licence d'achat en volume**, cliquez sur **Charger un fichier de licences d'achat en volume**.

   b) Dans la boîte de dialogue qui s'affiche, importez la licence.

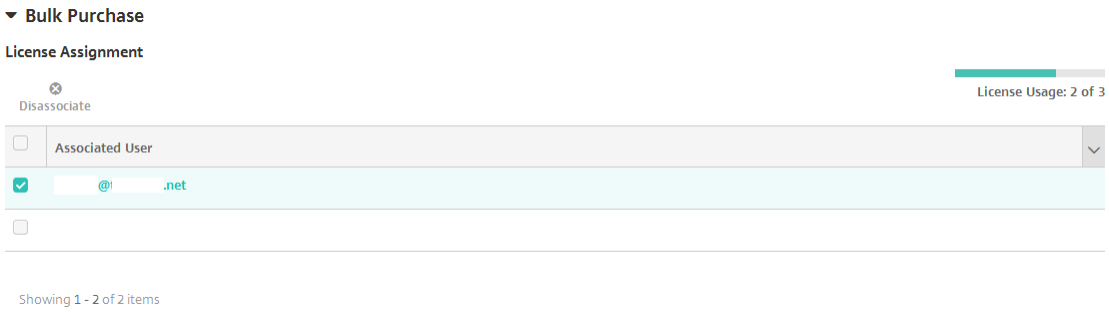
   Le tableau Attribution de licences affiche le nombre de licences en cours d'utilisation pour l'application, par rapport au nombre total de licences disponibles.

Vous pouvez dissocier les licences d'achat en volume pour un utilisateur individuel. Cela met fin aux attributions de licence et libère des licences.

8. Pour Android Enterprise, développez la section **Achat groupé**.

   Le tableau Attribution de licences affiche le nombre de licences en cours d'utilisation pour l'application, par rapport au nombre total de licences disponibles.

   Vous pouvez sélectionner un utilisateur et cliquer sur **Dissocier** pour libérer sa licence afin qu'elle puisse profiter à un autre utilisateur. Veuillez toutefois noter que vous ne pouvez dissocier des licences que si l'utilisateur ne fait pas partie d'un groupe de mise à disposition qui contient l'application spécifique.



9. Après avoir configuré les paramètres **Achat en volume** ou **Achat groupé**, cliquez sur **Suivant**. La page **Approbations** s'affiche.

   Pour utiliser des workflows afin d'exiger une approbation avant d'autoriser les utilisateurs à accéder à l'application, consultez la section Appliquer les workflows. Si vous n'avez pas besoin de workflows d'approbation, passez à l'étape suivante.

10. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.

11. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

12. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

    - **Déployer :** choisissez cette option si vous souhaitez déployer l'application sur les appareils. La valeur par défaut est **Activé**.
    - **Calendrier de déploiement :** choisissez l'option **Maintenant** ou **Plus tard** pour déployer l'application. Si vous sélectionnez **Plus tard**, configurez une date et une heure pour déployer l'application. La valeur par défaut est **Maintenant**.
    - **Conditions de déploiement :** choisissez **À chaque connexion** pour déployer l'application chaque fois que l'appareil se connecte. Choisissez **Uniquement lorsque le déploiement précédent a échoué** pour déployer l'application lorsque l'appareil n'a pas réussi à recevoir l'application. L'option par défaut est **À chaque connexion**.

L'option **Déployer pour les connexions permanentes** s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

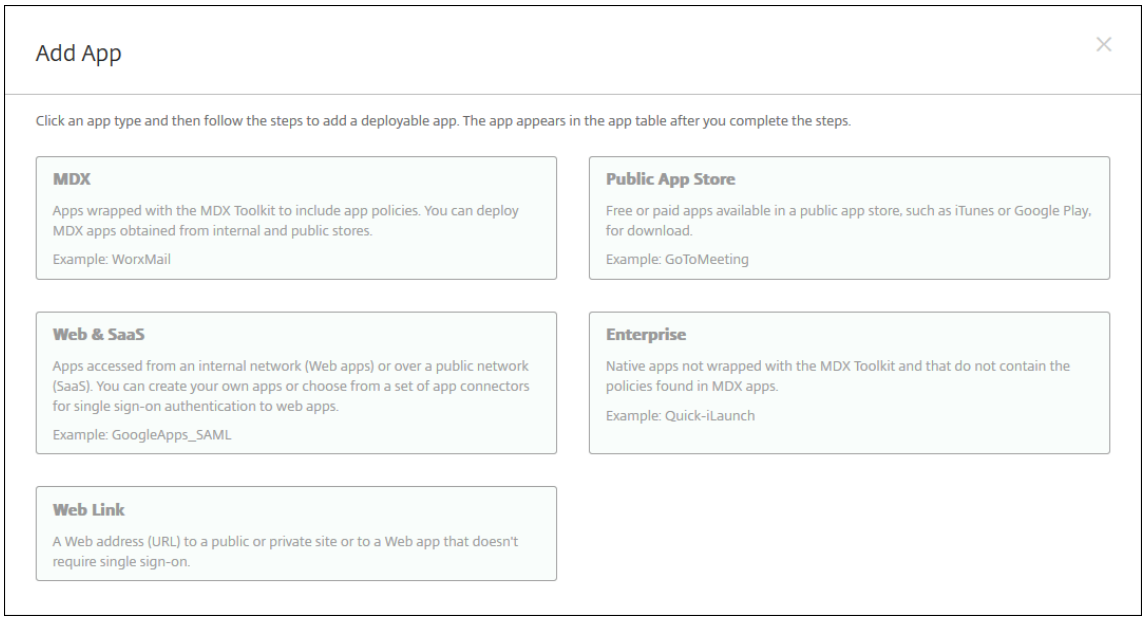
13. Cliquez sur **Enregistrer**.

Ajouter une application Web ou SaaS

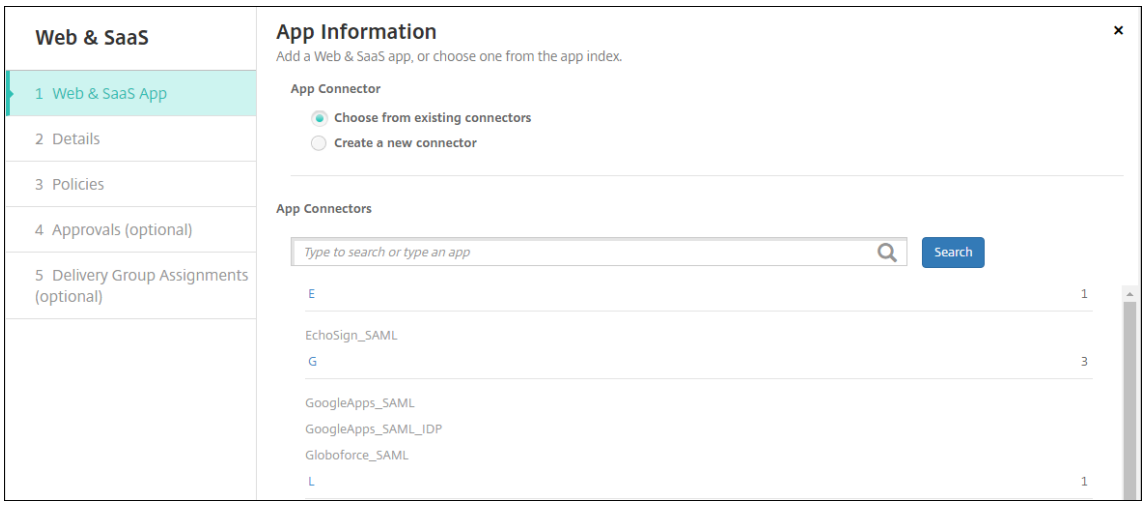
Grâce à la console XenMobile, vous pouvez fournir aux utilisateurs une autorisation d'authentification unique (SSO) à vos applications mobiles, d'entreprise, Web et SaaS. Vous pouvez activer des applications pour l'authentification unique (SSO) à l'aide des modèles de connecteurs d'applications. Pour obtenir une liste des types de connecteurs disponibles dans XenMobile, consultez la section Types de connecteur d'applications. Vous pouvez également créer votre propre connecteur dans XenMobile lorsque vous ajoutez une application Web ou SaaS.

Si une application est uniquement disponible en authentification unique : une fois que vous avez enregistré les paramètres, l'application s'affiche dans l'onglet **Applications** de la console XenMobile.

1. Dans la console XenMobile, cliquez sur **Configurer > Applications > Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



2. Cliquez sur **Web et SaaS**. La page **Informations sur l'application** s'affiche.



3. Configurez un nouveau connecteur d'applications ou un connecteur existant comme suit.

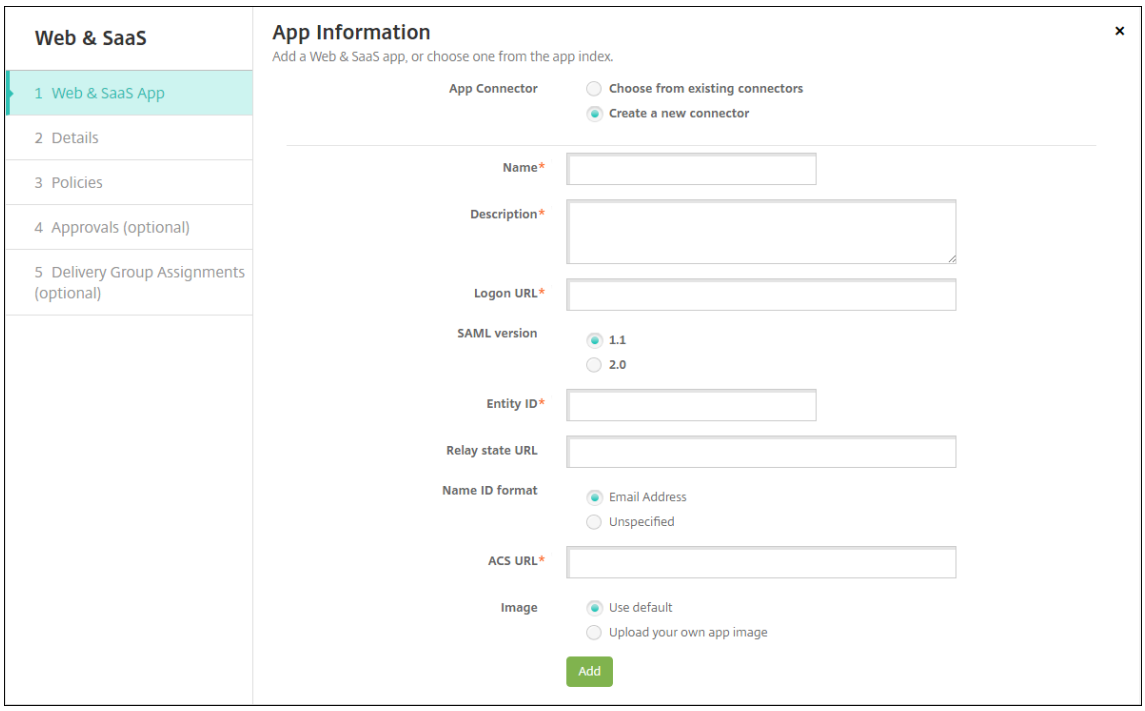
Pour configurer un connecteur d'applications existant

1. Sur la page **Informations sur l'application**, l'option **Choisir parmi les connecteurs existants** est déjà sélectionnée, comme illustré précédemment. Cliquez sur le connecteur que vous souhaitez utiliser dans la liste **Connecteurs d'applications**. Les informations sur le connecteur d'applications s'affichent.
2. Pour configurer ces paramètres :
   - **Nom de l'application :** acceptez le nom attribué ou entrez un nouveau nom.
   - **Description de l'application :** acceptez la description existante ou choisissez la vôtre.
   - **URL :** acceptez l'URL attribuée ou entrez l'adresse Web de l'application. Selon le connecteur que vous choisissez, ce champ peut contenir un paramètre fictif que vous devez remplacer avant de pouvoir passer à la page suivante.
   - **Nom de domaine :** le cas échéant, entrez le nom de domaine de l'application. Ce champ est obligatoire.
   - **L'application est hébergée dans le réseau interne :** indiquez si l'application est exécutée sur un serveur de votre réseau interne. Si les utilisateurs se connectent à l'application interne à partir d'un site distant, ils doivent se connecter par l'intermédiaire de Citrix Gateway. En réglant cette option sur **Activé**, le mot-clé VPN est ajouté à l'application et permet aux utilisateurs de se connecter via Citrix Gateway. La valeur par défaut est **Désactivé.**
   - **Catégorie d'application :** dans la liste, cliquez sur une catégorie à appliquer à l'application (facultatif).
   - **Provisioning du compte utilisateur :** sélectionnez cette option si vous souhaitez créer des comptes utilisateur pour l'application. Si vous utilisez le connecteur Globoforce_SAML, vous devez activer cette option pour assurer une intégration SSO transparente.

- Si vous activez **Provisioning du compte utilisateur**, configurez les paramètres suivants :
  - **Compte de service**
    - **Nom d'utilisateur :** entrez un nom pour l'administrateur de l'application. Ce champ est obligatoire.
    - **Mot de passe :** tapez le mot de passe d'administrateur de l'application. Ce champ est obligatoire.
  - **Compte d'utilisateur**
    - **Lorsque les droits de l'utilisateur prennent fin :** dans la liste, cliquez sur l'action à effectuer lorsque les utilisateurs ne sont plus autorisés à accéder à l'application. La valeur par défaut est **Désactiver le compte**.
  - **Règle de nom d'utilisateur**
    - Pour chaque règle de nom d'utilisateur que vous souhaitez ajouter, procédez comme suit :
      - **Attributs utilisateur :** dans la liste, cliquez sur l'attribut utilisateur à ajouter à la règle.
      - **Longueur (caractères) :** dans la liste, cliquez sur le nombre de caractères (de l'attribut utilisateur) à inclure dans la règle de nom d'utilisateur. Le paramètre par défaut est **All**
      - **Règle :** chaque attribut utilisateur que vous ajoutez est automatiquement ajouté à la règle de nom d'utilisateur.
- **Exigences de mot de passe**
  - **Longueur :** entrez la longueur minimale du mot de passe de l'utilisateur. La valeur par défaut est **8**.
- **Expiration du mot de passe**
  - **Validité (jours) :** tapez le nombre de jours pendant lequel le mot de passe est valable. Les valeurs valides sont **0 - 90**. La valeur par défaut est 90.
  - **Réinitialiser le mot de passe automatiquement après son expiration :** sélectionnez cette option si vous voulez réinitialiser le mot de passe automatiquement lors de l'expiration. La valeur par défaut est **Désactivé.** Si vous n'activez pas ce champ, les utilisateurs ne peuvent pas ouvrir l'application après que leur mot de passe expire.

Pour configurer un nouveau connecteur d'applications

1. Sur la page **Informations sur l'application**, sélectionnez **Créer un nouveau connecteur**. Les champs du connecteur d'applications s'affichent.

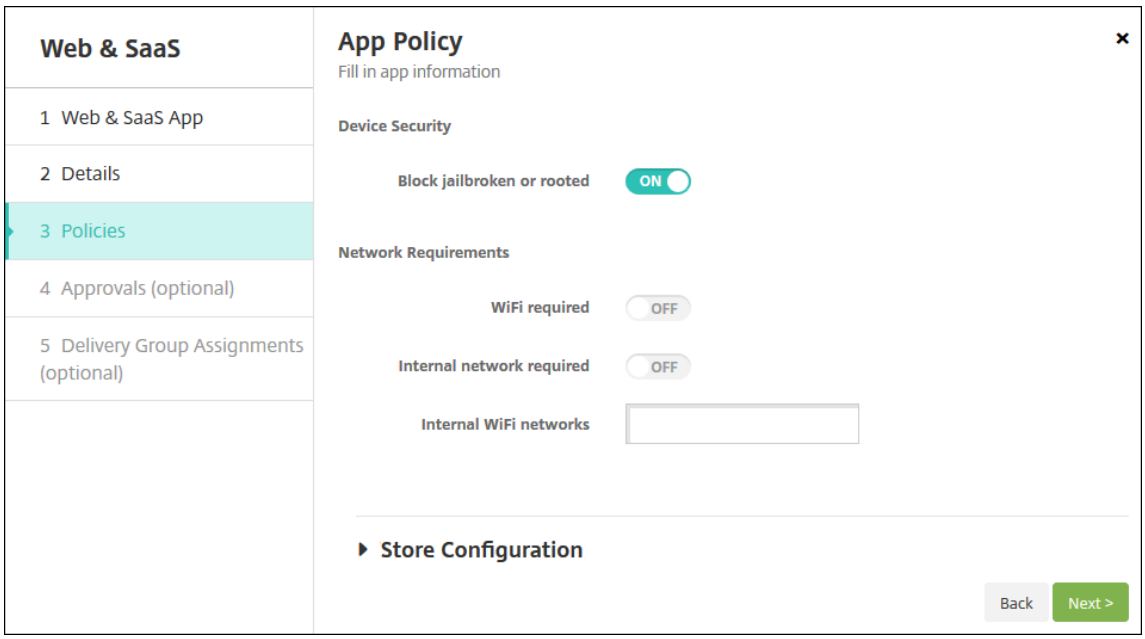


2. Pour configurer ces paramètres :

   - **Nom :** entrez un nom pour le connecteur. Ce champ est obligatoire.
   - **Description :** entrez une description pour le connecteur. Ce champ est obligatoire.
   - **URL de connexion :** entrez, ou copiez et collez, l'adresse URL de l'emplacement sur lequel les utilisateurs ouvrent une session sur le site. Par exemple, si l'application que vous souhaitez ajouter possède une page d'ouverture de session, ouvrez un navigateur Web et accédez à la page d'ouverture de session de l'application. Par exemple, `https://www.example.com/logon`. Ce champ est obligatoire.
   - **Version SAML :** sélectionnez **1.1** ou **2.0**. La valeur par défaut est **1.1**.
   - **ID de l'entité :** entrez l'identité de l'application SAML.
   - **URL d'état du relais :** entrez l'adresse Web de l'application SAML. L'URL d'état du relais représente l'URL de réponse de l'application.
   - **Format de l'ID de nom :** sélectionnez **Adresse e-mail** ou **Non spécifié**. Le paramètre par défaut est **Adresse e-mail**.
   - **URL ACS :** entrez l'URL du service ACS (consommateur d'assertion) du fournisseur de services ou d'identités. L'URL ACS offre aux utilisateurs une fonctionnalité d'authentification unique (SSO).
   - **Image :** indiquez si vous souhaitez utiliser l'image Citrix par défaut ou charger votre propre image d'application. La valeur par défaut est Utiliser valeur par défaut.
     - Pour télécharger votre propre image, cliquez sur **Parcourir** et accédez à l'emplacement du fichier. Le fichier doit être un fichier .PNG. Vous ne pouvez pas charger un fichier GIF ou JPEG. Lorsque vous ajoutez un graphique personnalisé, vous ne pouvez pas le

modifier ultérieurement.

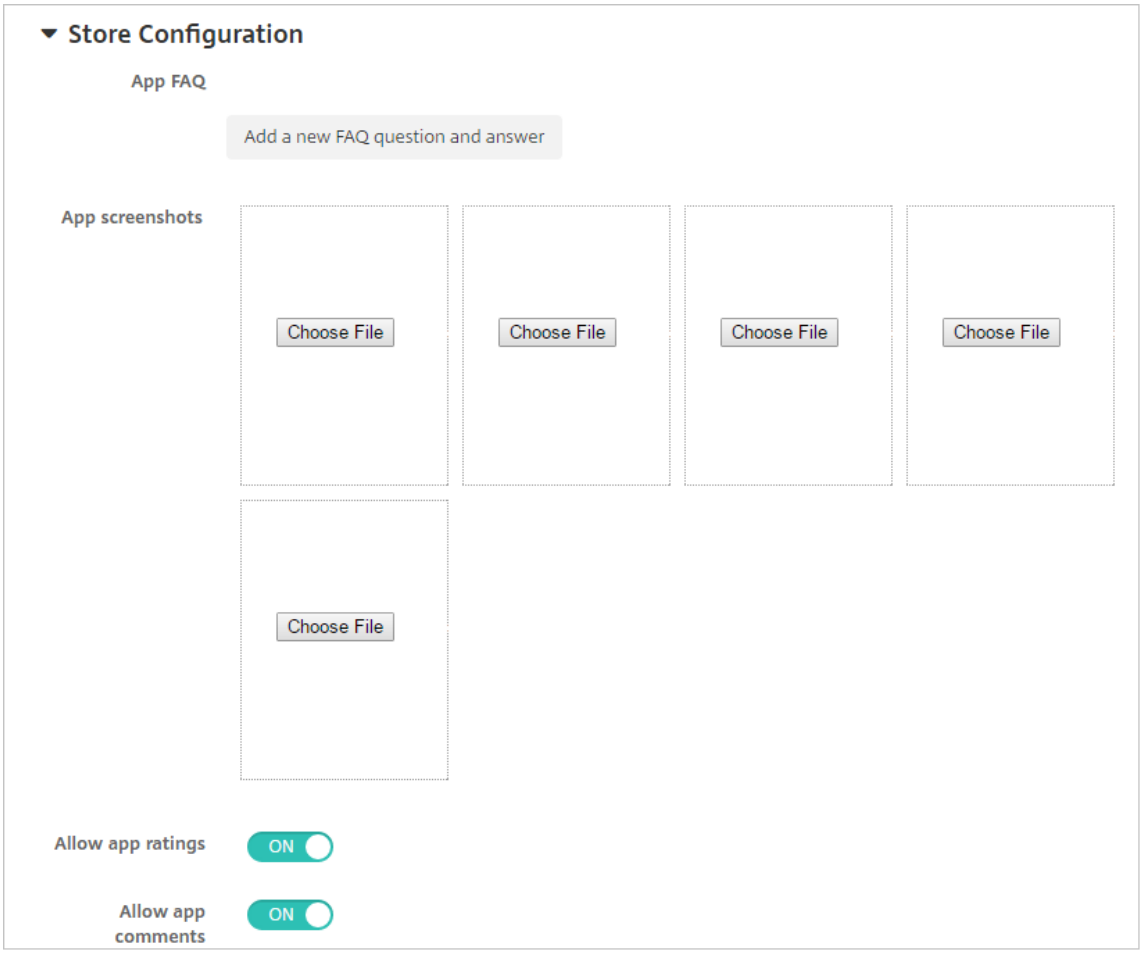
3. Lorsque vous avez terminé, cliquez sur **Ajouter**. La page **Détails** s'affiche.
4. Cliquez sur **Suivant**. La page **Stratégie d'application** s'affiche.



5. Pour configurer ces paramètres :

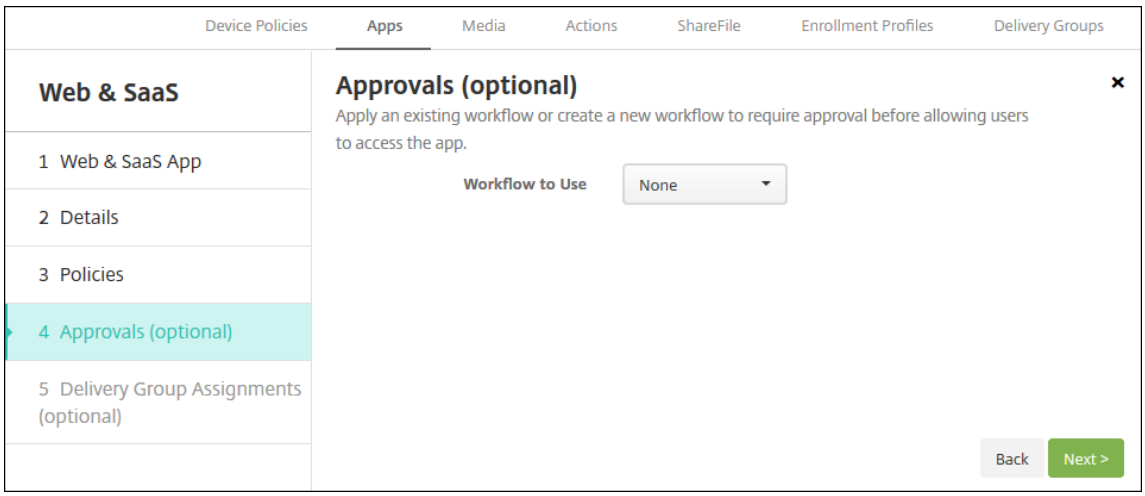
   - **Sécurité de l'appareil**
   - **Bloquer les appareils jailbreakés ou rootés :** sélectionnez cette option pour empêcher les appareils jailbreakés ou rootés d'accéder à l'application. La valeur par défaut est **Activé**.
   - **Configuration réseau requise**
   - **Wi-Fi requis :** sélectionnez cette option pour spécifier qu'une connexion Wi-Fi est requise pour exécuter l'application. La valeur par défaut est **Désactivé**.
   - **Réseau interne requis :** sélectionnez cette option si un réseau interne est requis pour exécuter l'application. La valeur par défaut est **Désactivé**.
   - **Réseaux Wi-Fi internes :** si vous avez activé **Wi-Fi requis**, saisissez les réseaux Wi-Fi internes à utiliser.

6. Configurez les règles de déploiement. Pour plus d'informations, consultez la section Règles de déploiement.
7. Développez **Configuration du magasin**.



- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.
- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des commentaires sur l'application dans l'App Store.

8. Cliquez sur **Suivant**. La page **Approbations** s'affiche.



Pour utiliser des workflows afin d'exiger une approbation avant d'autoriser les utilisateurs à accéder à l'application, consultez la section Appliquer les workflows.

9. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.
10. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.
11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :
    - **Déployer :** choisissez cette option si vous souhaitez déployer l'application sur les appareils. La valeur par défaut est **Activé**.
    - **Calendrier de déploiement :** choisissez l'option **Maintenant** ou **Plus tard** pour déployer l'application. Si vous sélectionnez **Plus tard**, configurez une date et une heure pour déployer l'application. La valeur par défaut est **Maintenant**.
    - **Conditions de déploiement :** choisissez **À chaque connexion** pour déployer l'application chaque fois que l'appareil se connecte. Choisissez **Uniquement lorsque le déploiement précédent a échoué** pour déployer l'application lorsque l'appareil n'a pas réussi à recevoir l'application. L'option par défaut est **À chaque connexion**.

    L'option **Déployer pour les connexions permanentes** s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

    Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.
12. Cliquez sur **Enregistrer**.

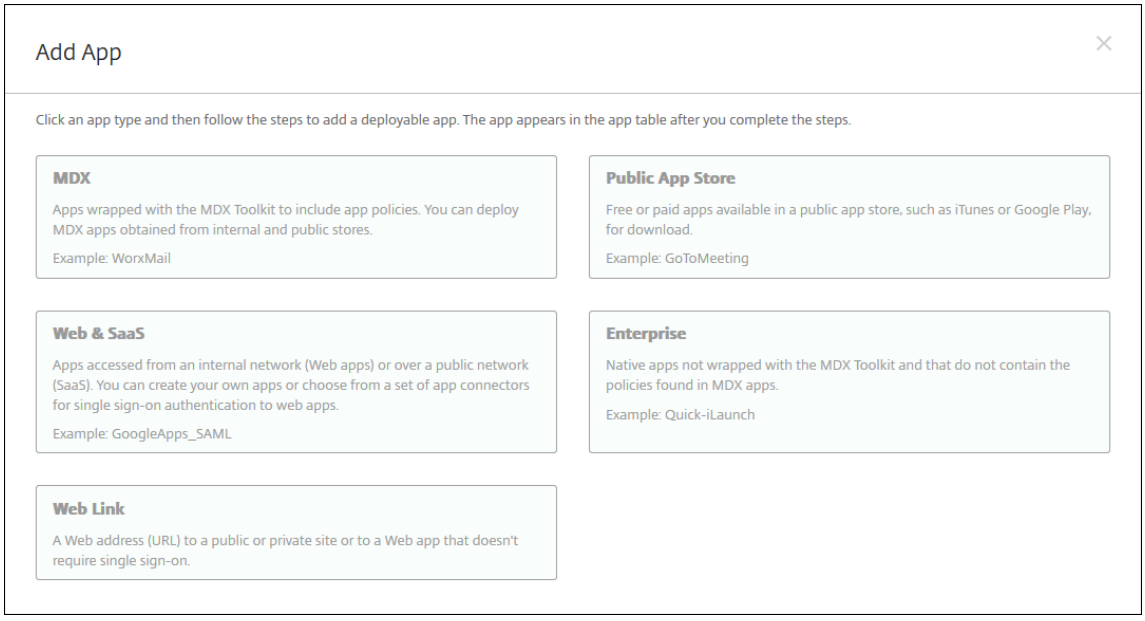
Ajouter une application d'entreprise

Les applications d'entreprise dans XenMobile représentent des applications natives qui ne sont pas préparées avec le SDK MAM ou MDX Toolkit. Ces applications ne contiennent pas les stratégies associées aux applications MDX. Vous pouvez charger une application d'entreprise sur l'onglet **Applications** dans la console XenMobile. Les applications d'entreprise prennent en charge les plates-formes suivantes (et les types de fichiers correspondant) :

- iOS (fichier .ipa)
- Android (fichier .apk)
- Samsung Knox (fichier .apk)
- Android Enterprise (fichier .apk)
- Voir aussi : Applications privées compatibles MDX

L'ajout d'applications téléchargées à partir de Google Play Store en tant qu'applications d'entreprise n'est pas pris en charge. Ajoutez plutôt des applications du Google Play Store en tant qu'applications publiques. Voir Ajouter une application d'un magasin d'applications public.

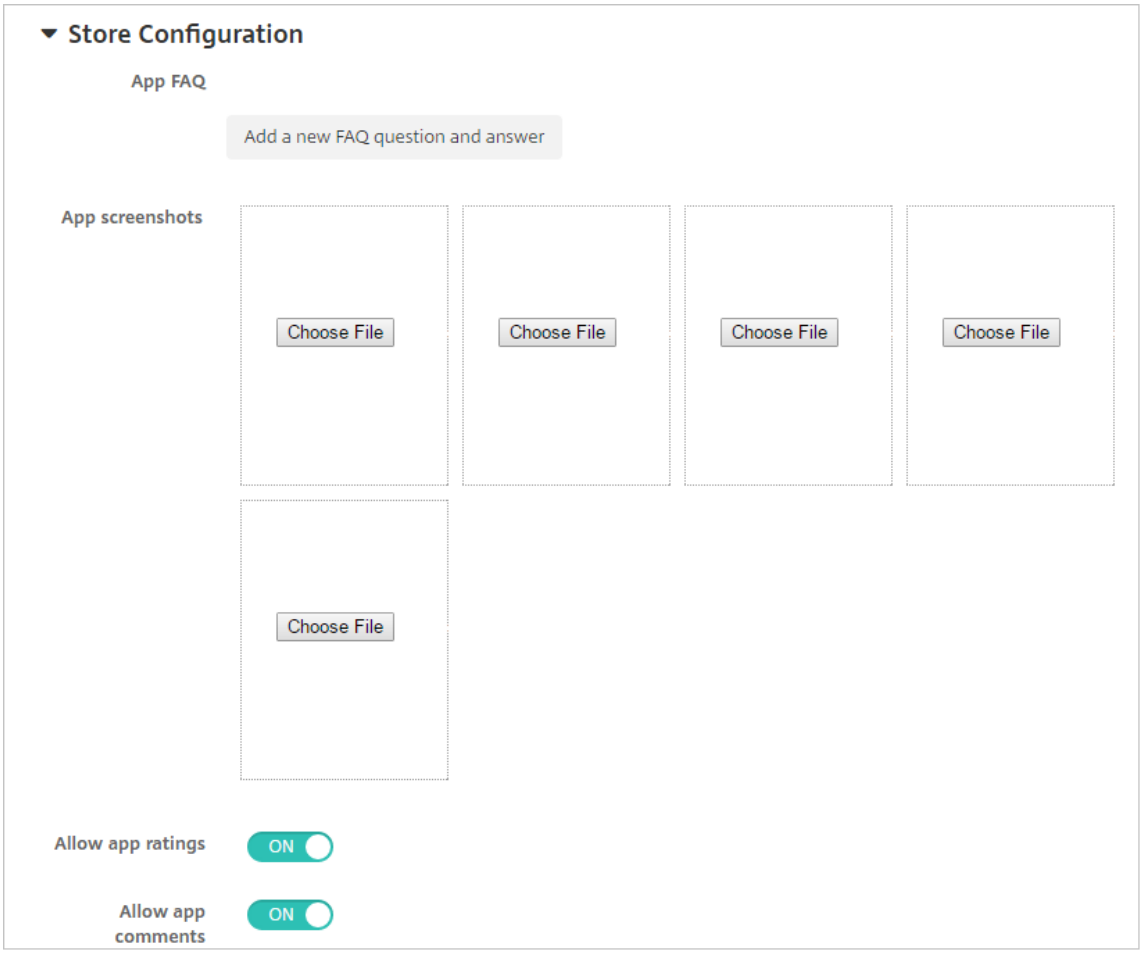
1. Dans la console XenMobile, cliquez sur **Configurer > Applications > Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



2. Cliquez sur **Entreprise**. La page **Informations sur l'application** s'affiche.
3. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
    - **Nom :** entrez un nom descriptif pour l'application. Il apparaît sous Nom de l'application dans le tableau Applications.
    - **Description :** entrez une description pour l'application (facultatif).
    - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations

sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.

4. Cliquez sur **Suivant**. La page **Plates-formes d'applications** s'affiche.
5. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.
6. Pour chaque plate-forme que vous avez choisie, sélectionnez le fichier à charger en cliquant sur **Charger** et accédez à l'emplacement du fichier.
7. Cliquez sur **Suivant**. La page d'informations sur l'application pour la plate-forme s'affiche.
8. Configurez les paramètres pour le type de plate-forme, notamment :
   - **Nom du fichier :** entrez un nouveau nom pour l'application (facultatif).
   - **Description de l'application :** entrez une nouvelle description pour l'application (facultatif).
   - **Version de l'application :** vous ne pouvez pas modifier ce champ.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
   - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.
   - **ID de package :** identifiant unique de votre application.
   - **Supprimer l'application si le profil MDM est supprimé :** sélectionnez cette option si vous souhaitez supprimer l'application d'un appareil lorsque le profil MDM est supprimé. La valeur par défaut est **Activé**.
   - **Empêcher la sauvegarde des données d'application :** sélectionnez cette option si vous souhaitez empêcher l'application de sauvegarder les données. La valeur par défaut est **Activé**.
   - **Forcer l'application à être gérée :** si vous installez une application non gérée, sélectionnez **Activé** si vous souhaitez que les utilisateurs sur des appareils non supervisés soient invités à autoriser la gestion de l'application. S'ils acceptent l'invite, l'application est gérée.
9. Configurez les règles de déploiement. Pour plus d'informations, consultez la section Règles de déploiement.
10. Développez **Configuration du magasin**.



- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.
- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des commentaires sur l'application dans l'App Store.

11. Cliquez sur **Suivant**. La page **Approbations** s'affiche.

    Pour utiliser des workflows afin d'exiger une approbation avant d'autoriser les utilisateurs à accéder à l'application, consultez la section Appliquer les workflows. Si vous n'avez pas besoin d'un workflow d'approbation, passez à l'étape suivante.

12. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.
13. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

14. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

    - **Déployer :** choisissez cette option si vous souhaitez déployer l'application sur les appareils. La valeur par défaut est **Activé**.
    - **Calendrier de déploiement :** choisissez l'option **Maintenant** ou **Plus tard** pour déployer l'application. Si vous sélectionnez **Plus tard**, configurez une date et une heure pour déployer l'application. La valeur par défaut est **Maintenant**.
    - **Conditions de déploiement :** choisissez **À chaque connexion** pour déployer l'application chaque fois que l'appareil se connecte. Choisissez **Uniquement lorsque le déploiement précédent a échoué** pour déployer l'application lorsque l'appareil n'a pas réussi à recevoir l'application. L'option par défaut est **À chaque connexion**.

    L'option **Déployer pour les connexions permanentes** s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

    Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

15. Cliquez sur **Enregistrer**.

Ajouter un lien Web

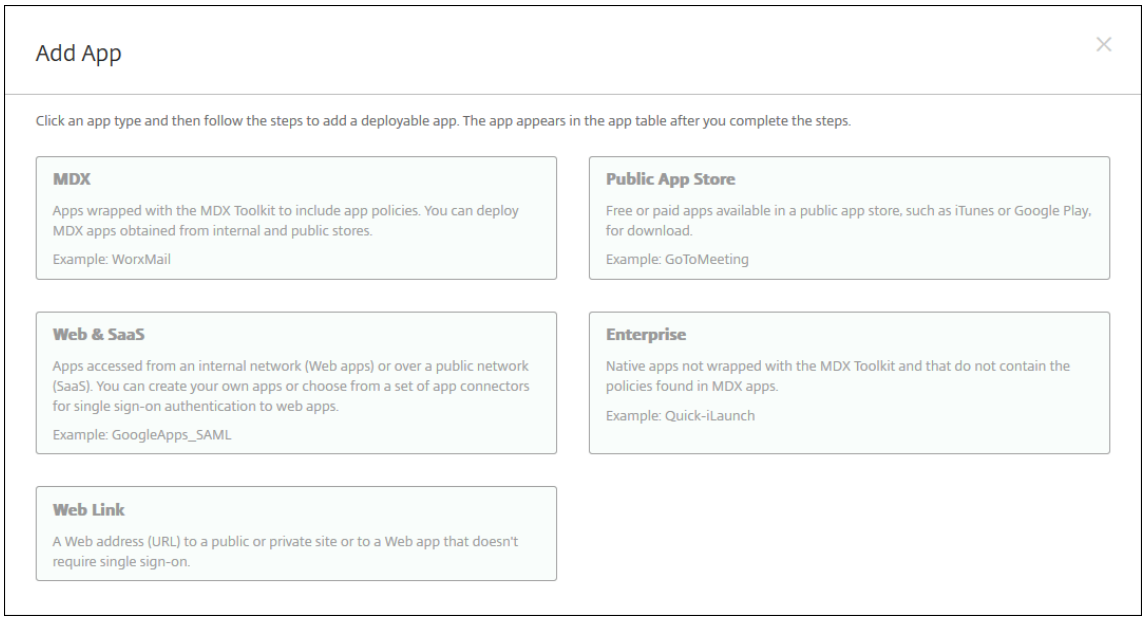
Un lien Web est une adresse Web permettant d'accéder à un site Internet ou intranet. Un lien Web permet également d'accéder à une application Web qui ne requiert pas d'authentification unique (SSO). Une fois que vous avez terminé de configurer un lien Web, celui-ci s'affiche sous forme d'icône dans le magasin d'applications. Lorsque les utilisateurs ouvrent une session avec Secure Hub, le lien s'affiche avec la liste des applications et bureaux disponibles.

Vous pouvez configurer des liens Web dans l'onglet **Applications** de la console XenMobile. Une fois que vous avez terminé de configurer le lien Web, celui-ci s'affiche sous forme d'icône dans le tableau **Applications**. Lorsque les utilisateurs ouvrent une session avec Secure Hub, le lien s'affiche avec la liste des applications et bureaux disponibles.

Pour ajouter le lien, vous devez fournir les informations suivantes :

- Nom du lien
- Description du lien
- Adresse Web (URL)
- Catégorie
- Rôle
- Image au format .png (facultatif)

1. Dans la console XenMobile, cliquez sur **Configurer > Applications > Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.

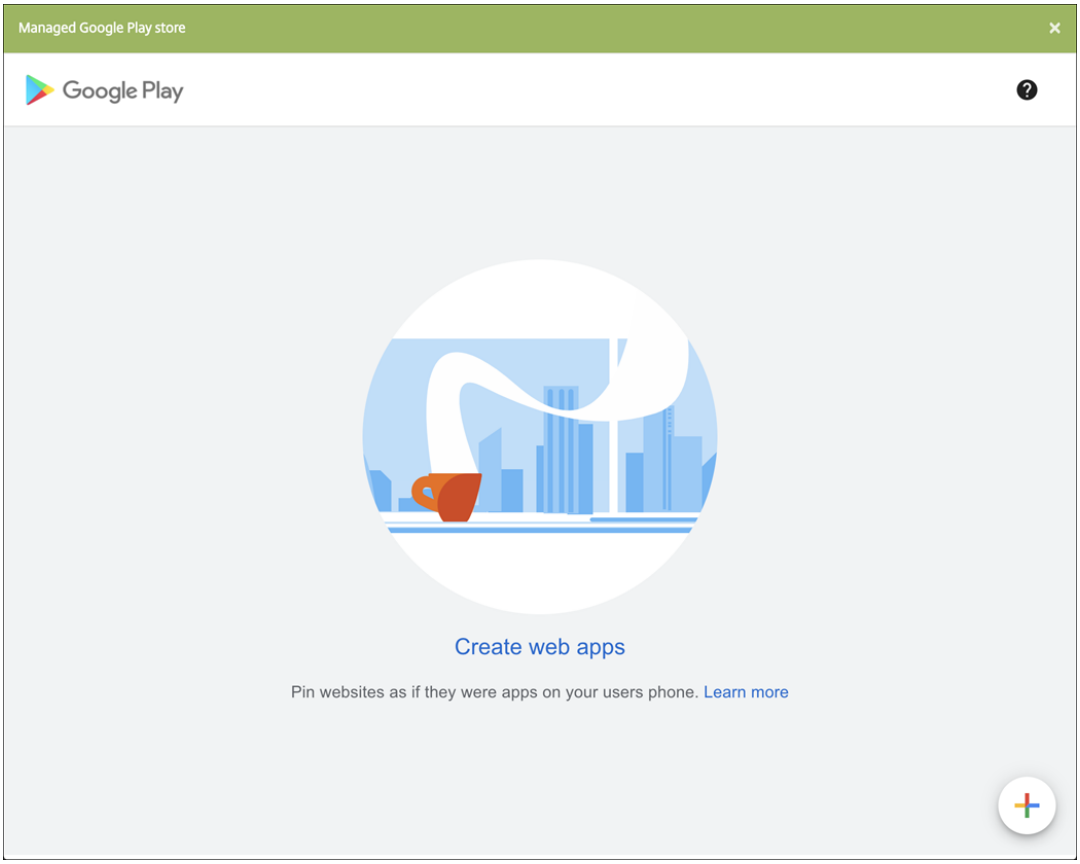


2. Cliquez sur **Lien Web**. La page **Informations sur l'application** s'affiche.
3. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :

   Nom : entrez un nom descriptif pour l'application. Il apparaît sous Nom de l'application dans le tableau Applications.
   Description : entrez une description pour l'application (facultatif).
   Catégorie d'application : si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.

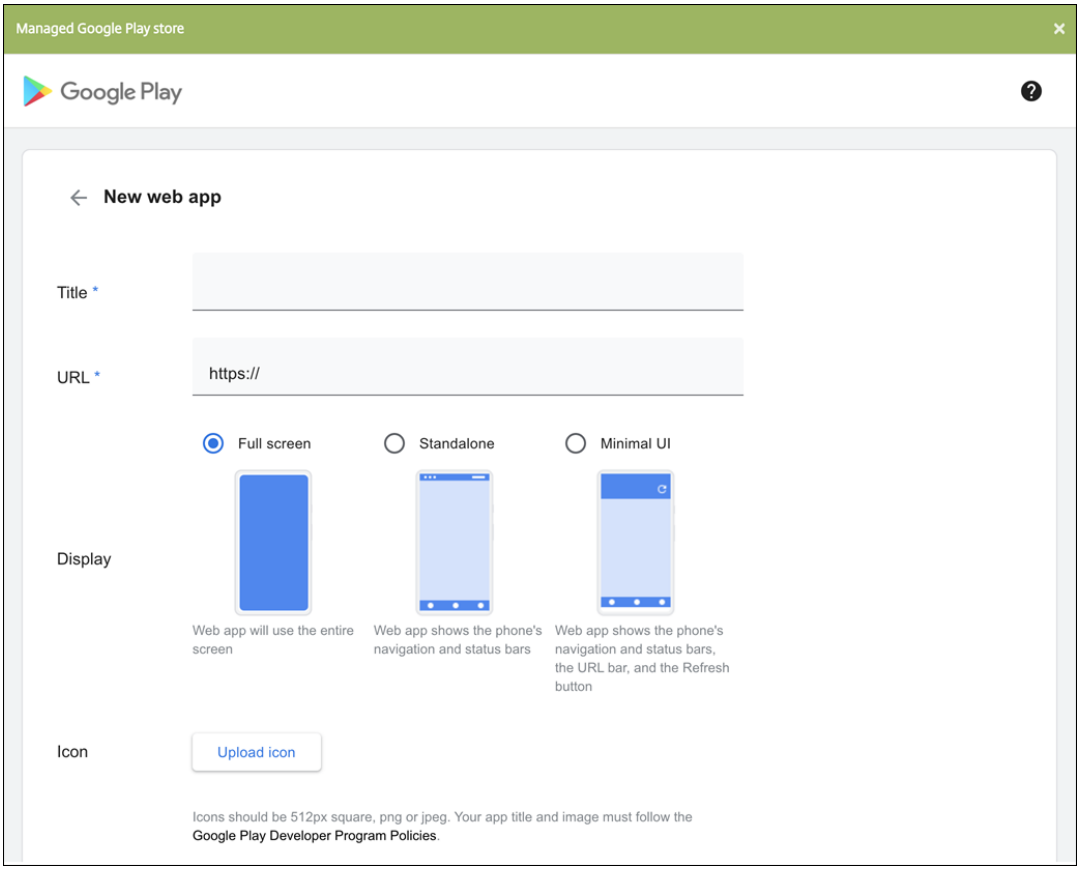
4. Cliquez sur **Suivant**. La page **Plates-formes d'applications** s'affiche.
5. Sous **Plates-formes**, sélectionnez **Autres plates-formes** pour ajouter une application Web pour iOS et Android (ancien administrateur de l'appareil) ou sélectionnez **Android Enterprise**. Désactivez la case à cocher correspondant à l'option que vous ne souhaitez pas ajouter.

   - Si vous sélectionnez **Autres plates-formes**, passez à l'étape suivante pour configurer les paramètres.
   - Si vous sélectionnez **Android Enterprise**, cliquez sur le bouton **Charger** pour ouvrir le magasin Google Play Store d'entreprise. Vous n'avez pas besoin de vous inscrire pour créer un compte de développeur et publier une application Web. Cliquez sur l'icône **Plus** dans le coin inférieur droit pour continuer.



Pour configurer ces paramètres :

- **Titre :** saisissez le nom de l'application Web.
- **URL :** saisissez l'adresse Web de l'application.
- **Affichage :** choisissez comment afficher l'application Web sur les machines utilisateur. Les options disponibles sont **Plein écran**, **Autonome** et **Interface minimale**.
- **Icône :** chargez votre propre image pour représenter l'application Web.



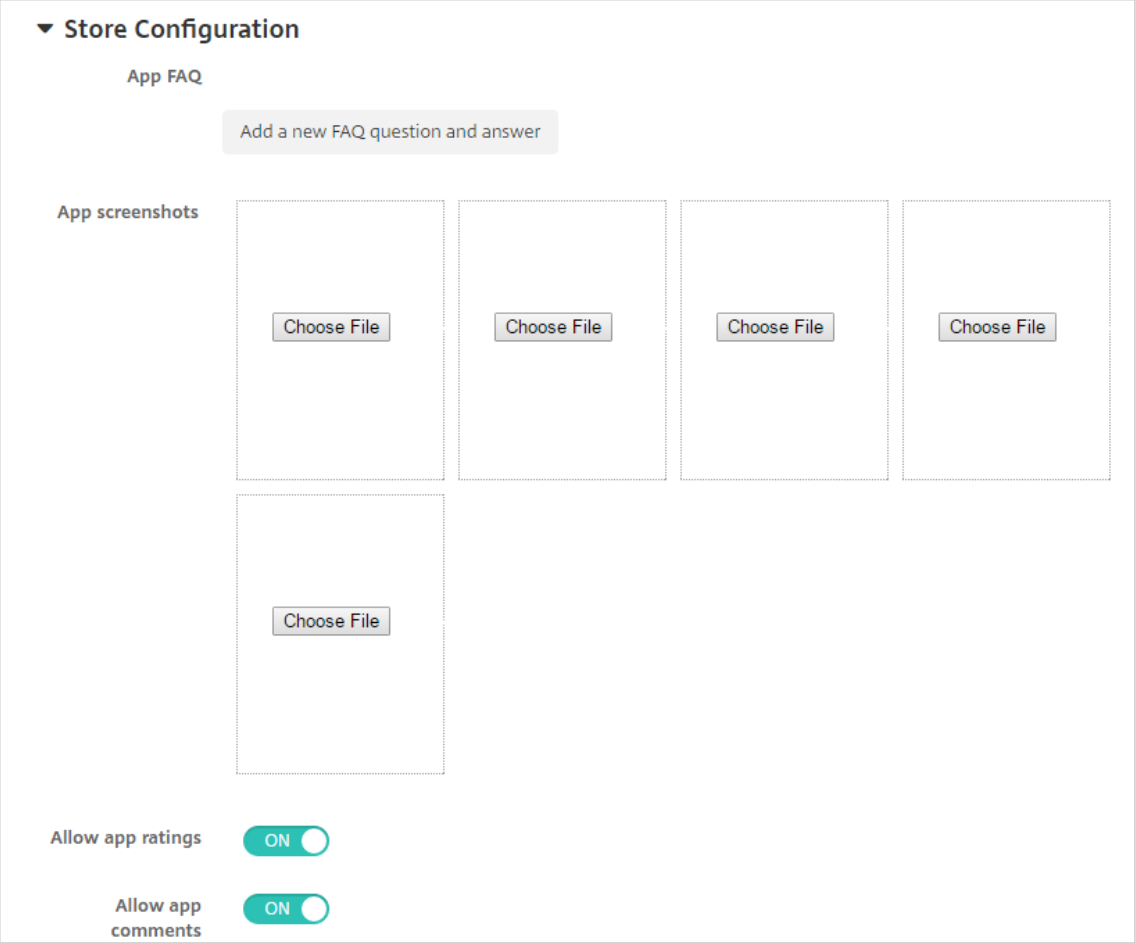
Lorsque vous avez terminé, cliquez sur **Créer**. La publication de votre application Web peut prendre jusqu'à 10 minutes.

6. Pour les plates-formes autres que Android Enterprise, configurez les paramètres suivants :

   - **Nom de l'application :** acceptez le nom attribué ou entrez un nouveau nom.
   - **Description de l'application :** acceptez la description existante ou choisissez la vôtre.
   - **URL :** acceptez l'URL attribuée ou entrez l'adresse Web de l'application. Selon le connecteur que vous choisissez, ce champ peut contenir un paramètre fictif que vous devez remplacer avant de pouvoir passer à la page suivante.
   - **L'application est hébergée dans le réseau interne :** indiquez si l'application est exécutée sur un serveur de votre réseau interne. Si les utilisateurs se connectent à l'application interne à partir d'un site distant, ils doivent se connecter par l'intermédiaire de Citrix Gateway. En réglant cette option sur **Activé**, le mot-clé VPN est ajouté à l'application et permet aux utilisateurs de se connecter via Citrix Gateway. La valeur par défaut est **Désactivé.**
   - **Catégorie d'application :** dans la liste, cliquez sur une catégorie à appliquer à l'application (facultatif).
   - **Image :** indiquez si vous souhaitez utiliser l'image Citrix par défaut ou charger votre propre image d'application. La valeur par défaut est Utiliser valeur par défaut.
     - Pour télécharger votre propre image, cliquez sur **Parcourir** et accédez à l'emplacement

du fichier. Le fichier doit être un fichier .PNG. Vous ne pouvez pas charger un fichier GIF ou JPEG. Lorsque vous ajoutez un graphique personnalisé, vous ne pouvez pas le modifier ultérieurement.

7. Configurez les règles de déploiement. Pour plus d'informations, consultez la section Règles de déploiement.
8. Développez **Configuration du magasin**.



- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.
- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des commentaires sur l'application dans l'App Store.

9. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.
10. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise

à disposition ou sélectionnez un ou des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

    - **Déployer :** choisissez cette option si vous souhaitez déployer l'application sur les appareils. La valeur par défaut est **Activé**.
    - **Calendrier de déploiement :** choisissez l'option **Maintenant** ou **Plus tard** pour déployer l'application. Si vous sélectionnez **Plus tard**, configurez une date et une heure pour déployer l'application. La valeur par défaut est **Maintenant**.
    - **Conditions de déploiement :** choisissez **À chaque connexion** pour déployer l'application chaque fois que l'appareil se connecte. Choisissez **Uniquement lorsque le déploiement précédent a échoué** pour déployer l'application lorsque l'appareil n'a pas réussi à recevoir l'application. L'option par défaut est **À chaque connexion**.

    L'option **Déployer pour les connexions permanentes** s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

    Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

12. Cliquez sur **Enregistrer**.

Activer les applications Microsoft 365

Vous pouvez ouvrir le conteneur MDX pour autoriser Secure Mail, Secure Web et Citrix Files à transférer des documents et données à des applications Microsoft Office 365. Pour de plus amples informations, consultez la section Autoriser l'interaction sécurisée avec les applications Office 365.

Appliquer les workflows

Configurez ces paramètres pour attribuer ou créer un workflow :

- **Workflow à utiliser :** dans la liste, cliquez sur un workflow existant ou cliquez sur **Créer un nouveau workflow**. La valeur par défaut est **Aucun**.

  Si vous sélectionnez **Créer un nouveau workflow**, configurez les paramètres suivants.

  - **Nom :** entrez un nom unique pour le workflow.
  - **Description :** entrez une description pour le workflow (facultatif).
  - **Modèles d'approbation d'e-mail :** dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Lorsque vous cliquez sur l'icône d'œil à droite du champ, une boîte de dialogue s'affiche dans laquelle vous pouvez afficher un aperçu du modèle.

- **Niveaux d'approbation par un responsable :** dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est 1 niveau. Les options possibles sont les suivantes :
  - Pas nécessaire
  - 1 niveau
  - 2 niveaux
  - 3 niveaux
- **Sélectionner un domaine Active Directory :** dans la liste, sélectionnez le domaine Active Directory à utiliser pour le workflow.
- **Rechercher des approbateurs supplémentaires requis :** tapez le nom de la personne dans le champ de recherche et cliquez sur **Rechercher**. Les noms proviennent d'Active Directory.
- Lorsque le nom s'affiche dans le champ, sélectionnez la case à cocher en regard du nom. Le nom et l'adresse e-mail s'affichent dans la liste **Approbateurs supplémentaires requis sélectionnés**.

  Pour supprimer une personne de la liste **Approbateurs supplémentaires requis sélectionnés**, procédez comme suit :
  - Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.
  - Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats de la recherche.
  - Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

Personnalisation du magasin d'applications et de Citrix Secure Hub

Vous pouvez définir la façon dont les applications s'affichent dans le magasin et ajouter un logo pour personnaliser Secure Hub et le magasin d'applications. Ces fonctionnalités de personnalisation sont disponibles pour les appareils iOS et Android.

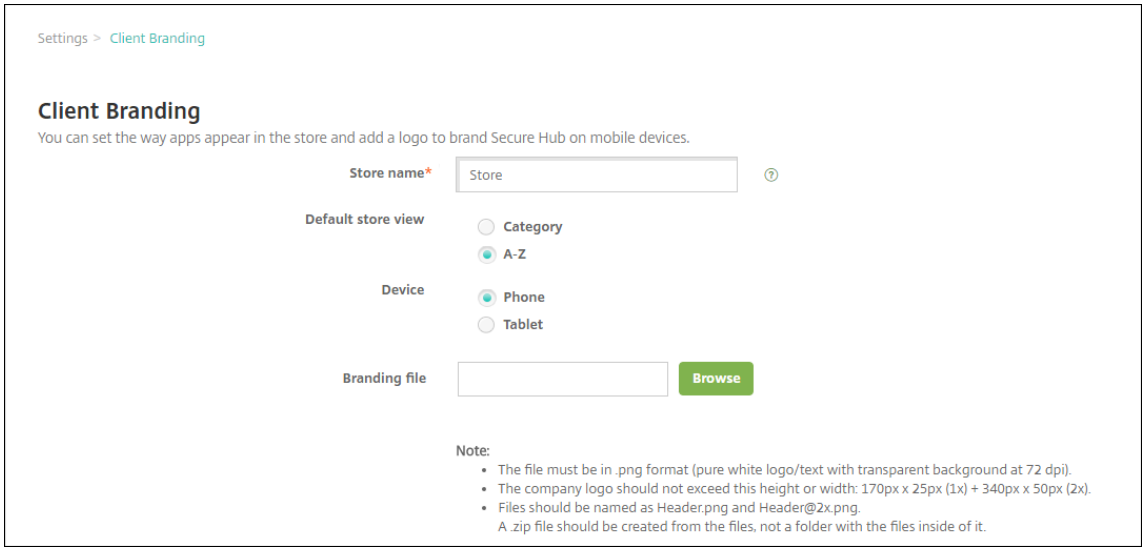
Avant de commencer, assurez-vous que votre image personnalisée est prête et accessible.

L'image personnalisée doit répondre à ces exigences :

- Le fichier doit être au format .png.
- Utilisez un logo blanc pur ou du texte avec un arrière-plan transparent à 72 ppp.
- Le logo de la société ne doit pas dépasser cette hauteur ou largeur : 170 px x 25 px (1x) et 340 px x 50 px (2x).

- Appelez les fichiers Header.png et Header@2x.png
- Créez un fichier .zip à partir des fichiers, et non un dossier contenant les fichiers.

1. Dans la console XenMobile Server, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Client**, cliquez sur **Personnalisation du client**. La page **Personnalisation du client** s'affiche.



Configurez les paramètres suivants :

- **Nom du magasin :** le nom s'affiche dans les informations de compte de l'utilisateur. La modification du nom change également l'adresse URL utilisée pour accéder aux services du magasin. Il n'est généralement pas nécessaire de modifier le nom par défaut.

  > **Important :**
  >
  > Le nom du magasin ne peut contenir que des caractères alphanumériques.

- **Vue du magasin par défaut :** sélectionnez **Catégorie** ou **A-Z**. La valeur par défaut est **A-Z**.
- **Appareil :** sélectionnez **Téléphone** ou **Tablette**. La valeur par défaut est **Téléphone**.
- **Fichier de personnalisation :** sélectionnez une image ou un fichier .zip d'images à utiliser pour la personnalisation en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.

3. Cliquez sur **Enregistrer**.

Types de connecteur d'application

October 17, 2018

Le tableau suivant dresse la liste des connecteurs et des types de connecteurs disponibles dans XenMobile lorsque vous ajoutez une application Web ou SaaS. Vous pouvez également ajouter un nouveau connecteur à XenMobile lorsque vous ajoutez une application Web ou SaaS.

Il indique si le connecteur prend en charge la gestion des comptes d'utilisateur, ce qui permet de créer de nouveaux comptes, de façon automatique ou à l'aide d'un workflow.

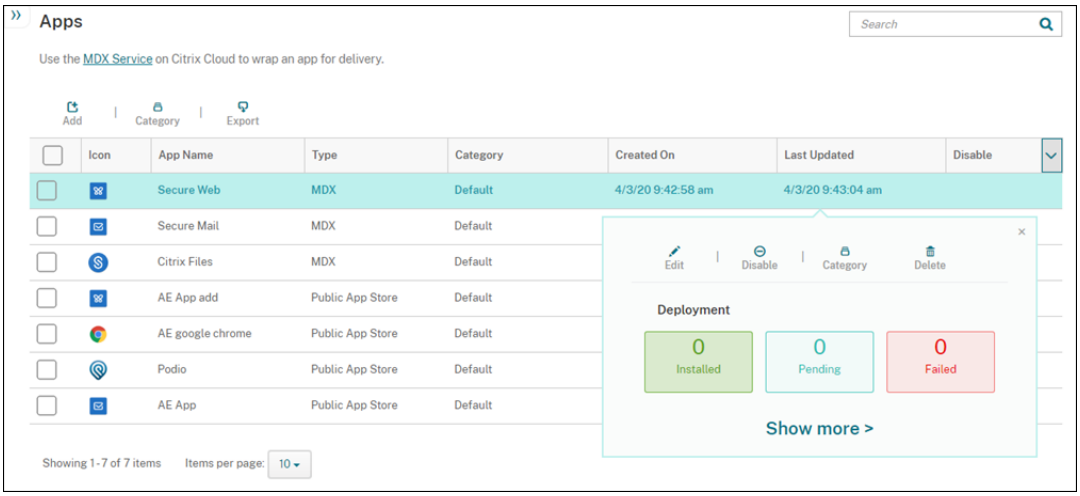
Nom du connecteur	SSO SAML	Prend en charge la gestion des comptes d'utilisateur
EchoSign_SAML	O	O
Globoforce_SAML		**Remarque :** lorsque vous utilisez ce connecteur, vous devez Activer la gestion des utilisateurs pour le provisioning pour assurer une intégration SSO transparente.
GoogleApps_SAML	O	O
GoogleApps_SAML_IDP	O	O
Lynda_SAML	O	O
Office365_SAML	O	O
Salesforce_SAML	O	O
Salesforce_SAML_SP	O	O
SandBox_SAML	O	
SuccessFactors_SAML	O	
ShareFile_SAML	O	
ShareFile_SAML_SP	O	
WebEx_SAML_SP	O	O

Mettre à niveau les applications MDX ou Enterprise

January 10, 2022

Pour mettre à niveau une application MDX ou Enterprise dans XenMobile, désactivez-la dans la console XenMobile, puis téléchargez la nouvelle version de l'application. Vous n'avez pas besoin de désactiver les applications du magasin d'applications public telles que Citrix Secure Mail.

1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'affiche.
2. Pour les appareils gérés (appareils inscrits dans XenMobile pour la gestion des appareils mobiles), passez à l'étape 3. Pour les appareils non gérés (appareils inscrits dans XenMobile uniquement à des fins de gestion des applications d'entreprise), procédez comme suit :
   a) Dans le tableau **Applications**, sélectionnez la case à cocher en regard de l'application, ou cliquez sur la ligne contenant l'application que vous souhaitez mettre à jour.
   b) Cliquez sur **Désactiver** dans le menu qui s'affiche.



   c) Cliquez sur **Désactiver** dans la boîte de dialogue de confirmation. *Désactivé* s'affiche dans la colonne **Désactiver** pour l'application.

> **Remarque :**
>
> Lorsque l'application est désactivée, les utilisateurs ne peuvent pas se reconnecter à l'application après avoir fermé leur session. La désactivation d'applications est un paramètre facultatif, mais nous recommandons de désactiver l'application pour éviter les problèmes avec la fonctionnalité de l'application. Par exemple, une erreur peut se produire lorsque les utilisateurs demandant de télécharger l'application en même temps que vous téléchargez la nouvelle version.

3. Dans le tableau **Applications**, cliquez sur la case à cocher en regard de l'application, ou cliquez sur la ligne contenant l'application que vous souhaitez mettre à jour.
4. Cliquez sur **Modifier** dans le menu qui s'affiche. La page **Informations sur l'application** s'affiche avec la liste des plates-formes que vous avez choisies pour l'application sélectionnée.
5. Pour configurer ces paramètres :

- **Nom :** si vous le souhaitez, vous pouvez modifier le nom de l'application.
- **Description :** si vous le souhaitez, vous pouvez modifier la description de l'application.
- **Catégorie d'application :** si vous le souhaitez, vous pouvez modifier la catégorie.

6. Cliquez sur **Suivant**. La première page de plate-forme sélectionnée s'affiche. Effectuez les opérations suivantes pour chaque plate-forme sélectionnée :

   a) Choisissez le fichier de remplacement que vous voulez charger en cliquant sur le bouton **Charger** et accédez à l'emplacement du fichier. L'application se charge dans XenMobile.

   Si vous chargez une application pour Android Enterprise, une fenêtre Google Play d'entreprise s'affiche. Chargez la nouvelle version de l'application ici. Pour plus de détails, consultez Distribuer des applications Android Enterprise.

   b) Si vous le souhaitez, vous pouvez modifier les détails de l'application et les paramètres de stratégie pour la plate-forme.

   c) Si vous le souhaitez, vous pouvez configurer des règles de déploiement et XenMobile Store. Pour plus d'informations, consultez la section Ajouter une application MDX dans Ajouter des applications.

7. Cliquez sur **Enregistrer**. La page **Applications** s'affiche.
8. Si vous avez désactivé l'application à l'étape 2, effectuez les opérations suivantes :

   a) Dans le tableau des **Applications**, choisissez l'application que vous avez mis à jour puis dans le menu qui s'affiche, cliquez sur **Activer**.
   b) Dans la boîte de dialogue de confirmation qui s'affiche, cliquez sur **Activer**. Les utilisateurs peuvent désormais accéder à l'application et recevoir une notification les invitant à mettre l'application à niveau.

Citrix Launcher

January 10, 2022

Remplacement de Citrix Launcher

Citrix supprime Citrix Launcher de l'App Store en août 2020. Pour remplacer Citrix Launcher, vous pouvez utiliser des fonctionnalités déjà disponibles.

Pour provisionner des appareils kiosques (appareils dédiés), procédez comme suit :

1. Ajoutez un rôle RBAC pour permettre aux administrateurs XenMobile d'inscrire des appareils dédiés à votre déploiement XenMobile. Consultez la section Provisionner des appareils Android Enterprise dédiés.

2. Créez un profil d'inscription avec l'option **Type d'inscription** définie sur **Profil de travail/entièrement géré**. Consultez la section Pour créer un profil d'inscription.
3. Créez une stratégie kiosque pour configurer une application à épingler sur l'écran de l'appareil en activant le paramètre **Mode de verrouillage des tâches**. Consultez Paramètres Android Enterprise.

À propos de Citrix Launcher

Citrix Launcher vous permet de personnaliser l'expérience de l'utilisateur pour les appareils Android déployés par XenMobile. La version minimale d'Android prise en charge pour la gestion Secure Hub de Citrix Launcher est Android 4.0.3. Citrix Launcher et la stratégie de configuration du Launcher ne sont pas compatibles avec Android Enterprise.

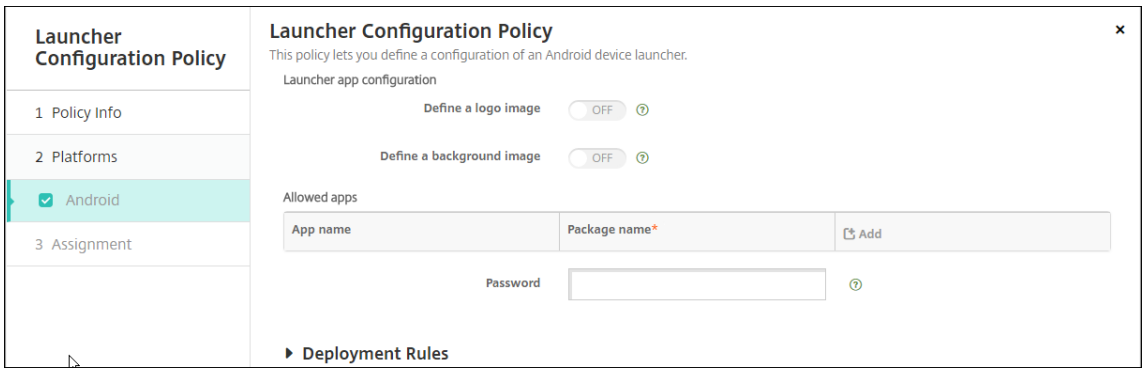
Vous pouvez ajouter la **stratégie de configuration du Launcher** pour contrôler ces fonctionnalités de Citrix Launcher :

- Gérez les appareils Android, de façon à ce que les utilisateurs puissent uniquement accéder aux applications que vous spécifiez.
- Si vous le souhaitez, vous pouvez spécifier une image de logo personnalisé pour l'icône Citrix Launcher et une image d'arrière-plan personnalisée pour Citrix Launcher.
- Spécifiez un mot de passe que les utilisateurs doivent entrer pour quitter le Launcher.

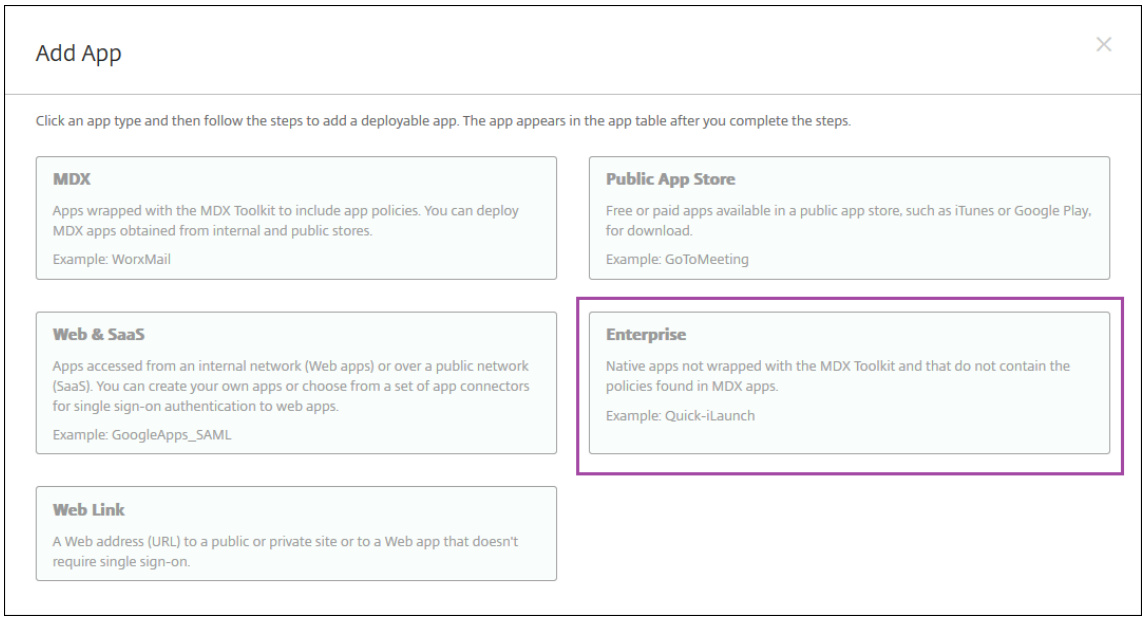
Si Citrix Launcher vous permet d'appliquer ces restrictions sur l'appareil, il donne aux utilisateurs un accès intégré à des paramètres de l'appareil tels que les paramètres Wi-Fi, les réglages Bluetooth et les paramètres de code secret de l'appareil. Citrix Launcher n'est pas destiné à être une couche de sécurité supplémentaire venant s'ajouter à ce que la plate-forme de l'appareil offre déjà.

Pour fournir le Citrix Launcher aux appareils Android, suivez ces étapes.

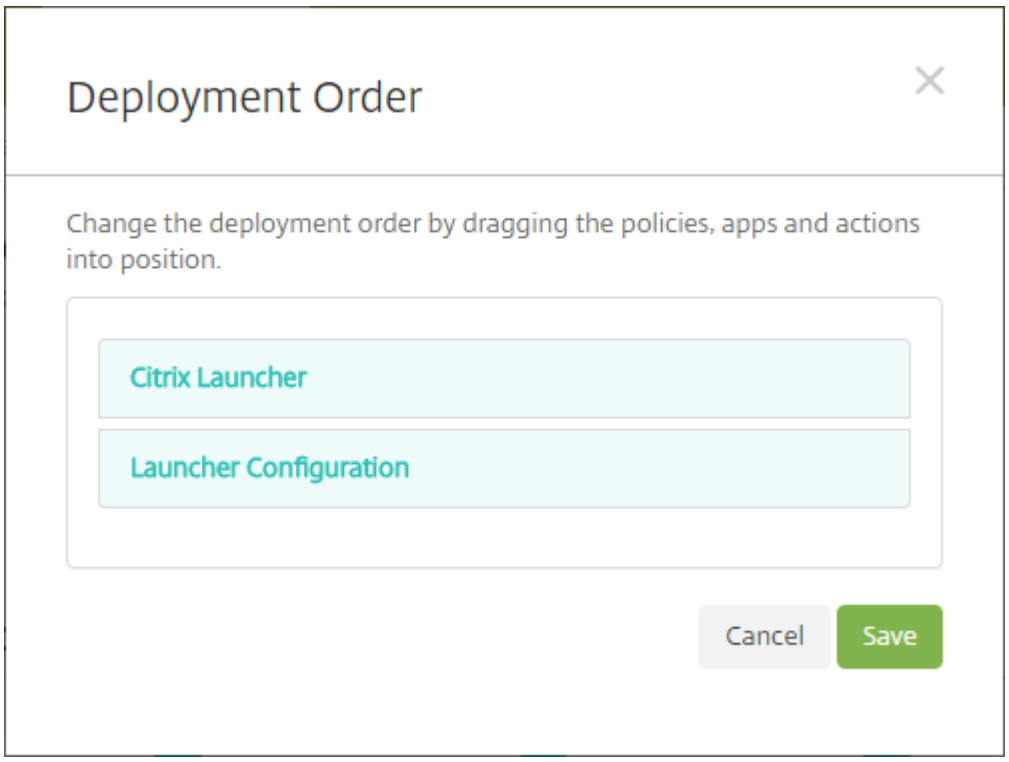
1. Pour télécharger l'application Citrix Launcher, accédez à https://www.citrix.com/downloads. Recherchez **Citrix Launcher**. Le nom du fichier est CitrixLauncher.apk. Le fichier est prêt à être chargé dans XenMobile et ne nécessite pas d'encapsulation.
2. Ajoutez la **Stratégie de configuration du Launcher**. Accédez à **Configurer > Stratégies d'appareil**, cliquez sur **Ajouter**, puis dans la boîte de dialogue **Ajouter une nouvelle stratégie**, commencez à taper **Launcher**. Pour de plus amples informations, consultez la section Stratégie de configuration du Launcher.



3. Ajoutez l'application Citrix Launcher à XenMobile en tant qu'application d'entreprise. Dans **Configurer > Applications**, cliquez sur **Ajouter**, puis cliquez sur **Enterprise**. Pour de plus amples informations, consultez la section Ajouter une application d'entreprise.



4. Créez un groupe de mise à disposition pour Citrix Launcher avec la configuration suivante dans **Configurer > Groupes de mise à disposition**.
   - Sur la page **Stratégies**, ajoutez la **Stratégie de configuration du Launcher**.
   - Sur la page **Applications**, faites glisser **Citrix Launcher** vers **Applications requises**.
   - Sur la page **Résumé**, cliquez sur **Ordre de déploiement** et assurez-vous que l'application **Citrix Launcher** précède la stratégie **Configuration du Launcher**.



Pour de plus amples informations, consultez la section Déployer des ressources.

Achats en volume d'Apple

January 10, 2022

Vous pouvez gérer les licences d'applications iOS à l'aide de l'achat en volume iOS d'Apple. La solution d'achat en volume simplifie la recherche, l'achat et la distribution d'applications et d'autres données en bloc pour une organisation.

Avec l'achat en volume, vous pouvez utiliser XenMobile pour distribuer des applications de magasin d'applications public.

- L'achat en volume n'est pas pris en charge pour l'inscription MAM. Vous devez inscrire les appareils d'achat en volume dans MDM ou MDM+MAM.
- L'achat en volume n'est pas pris en charge pour les applications de productivité mobiles Citrix.
- Bien que vous puissiez distribuer les applications de magasin public de XenMobile avec l'achat en volume, le déploiement n'est pas optimal. Des améliorations de XenMobile et du magasin Secure Hub sont requises pour résoudre ces limitations.
- Pour obtenir la liste des problèmes connus liés à la distribution des applications de magasin public XenMobile via l'achat en volume, consultez cet article dans le Centre de connaissances Citrix.

Avec l'achat en volume, vous pouvez distribuer les applications concernées directement sur vos appareils. Vous pouvez aussi attribuer le contenu à vos utilisateurs à l'aide de codes. Vous configurez des paramètres spécifiques au programme d'achat en volume iOS dans XenMobile.

XenMobile réimporte périodiquement les licences d'achat en volume depuis Apple pour s'assurer que les licences reflètent toutes les modifications. Ces modifications incluent la suppression manuelle d'une application importée à partir de l'achat en volume. Par défaut, XenMobile actualise la ligne de base de licence d'achat en volume toutes les 1440 minutes (24 heures) au minimum. Vous pouvez modifier l'intervalle de ligne de base d'achat en volume via la propriété de serveur `VPP.baseline`. Consultez Propriétés du serveur.

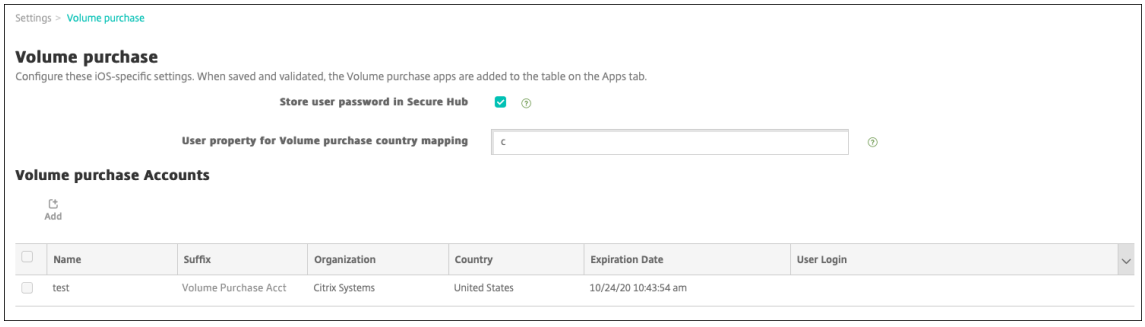
Le paramètre **Mise à jour automatique des applications** repose également sur la propriété du serveur `VPP.baseline`. Les applications sont ainsi mises à jour selon la même planification définie dans cette propriété.

Cet article se concentre sur l'utilisation du programme d'achat en volume avec des licences gérées, ce qui vous permet d'utiliser XenMobile pour distribuer des applications. Si vous utilisez actuellement des codes de téléchargement et que vous souhaitez changer au profit d'une distribution gérée, consultez le document de support Apple, Passage du système de codes de téléchargement au système de distribution gérée, dans le cadre du programme d'achat en volume.

Pour plus d'informations sur le programme d'achat en volume iOS, consultez la section https://volume.itunes.apple.com/us/store. Pour vous inscrire au programme d'achat en volume, accédez à https://deploy.apple.com/qforms/open/register/index/avs. Pour accéder à votre magasin d'achat en volume dans iTunes, rendez-vous sur https://volume.itunes.apple.com/?l=en.

Après avoir enregistré ces paramètres de volume d'achat iOS dans XenMobile, les applications achetées figurent dans le tableau de la page **Configurer > Applications** dans la console XenMobile.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Achat en volume**. La page de configuration de **l'achat en volume** s'affiche.



3. Pour configurer ces paramètres :
   - **Stocker le mot de passe utilisateur dans Secure Hub :** indiquez si un nom d'utilisateur et un mot de passe doivent être stockés dans Secure Hub en vue de l'authentification sur

XenMobile. Par défaut, les informations sont stockées à l'aide de cette méthode sécurisée.

- **Propriété utilisateur pour le choix du pays d'achat en volume :** entrez un code pour autoriser les utilisateurs à télécharger des applications à partir de magasins d'applications spécifiques à un pays.

XenMobile utilise ce mappage pour choisir le pool de propriété de l'achat en volume. Par exemple, lorsque la propriété utilisateur est États-Unis, l'utilisateur ne peut pas télécharger d'applications si le code d'achat en volume correspond au Royaume-Uni. Contactez votre administrateur de programme d'achat en volume pour plus d'informations sur le choix du code de pays.

4. Pour chaque compte d'achat en volume que vous souhaitez ajouter, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un compte d'achat en volume** s'affiche.
5. Configurez ces paramètres pour chaque compte à ajouter :

> **Remarque :**
>
> Si vous utilisez Apple Configurator 1, chargez un fichier de licences : accédez à **Configurer > Applications**, accédez à une page de plate-forme et développez **Achat en volume**.

   - **Nom :** entrez le nom du compte d'achat en volume.
   - **Suffixe :** entrez le suffixe à ajouter au nom des applications obtenues via le compte d'achat en volume. Par exemple, si vous entrez **VP**, l'application Secure Mail s'affiche dans la liste des applications en tant que **Secure Mail - VP**.
   - **Jeton d'entreprise :** copiez et collez le jeton de service d'achat en volume obtenu auprès d'Apple. Pour obtenir le jeton, dans la page de **résumé de compte** du portail d'achat en volume Apple, cliquez sur le bouton **Télécharger** pour générer et télécharger le fichier d'achat en volume. Le fichier contient le jeton de service, ainsi que d'autres informations telles que le code de pays et l'expiration. Enregistrez le fichier dans un emplacement sécurisé.
   - **Connexion utilisateur :** entrez un nom d'administrateur de compte d'achat en volume autorisé facultatif utilisé pour importer des applications B2B personnalisées.
   - **Mot de passe utilisateur :** entrez le mot de passe de l'administrateur du compte d'achat en volume.
   - **Mise à jour automatique des applications :** si cette option est **activée**, les applications d'achat en volume sont automatiquement mises à jour lorsqu'une mise à jour est disponible sur l'Apple Store. La valeur par défaut est **Désactivé**.
6. Cliquez sur **Enregistrer** pour fermer la boîte de dialogue.
7. Cliquez sur **Enregistrer** pour enregistrer la configuration d'achat en volume.

   Un message s'affiche pour vous informer que XenMobile va ajouter des applications à la liste sur la page **Configurer > Applications**. Sur cette page, notez que le nom des applications de votre compte d'achat en volume inclut le suffixe que vous avez spécifié dans la configuration

précédente.

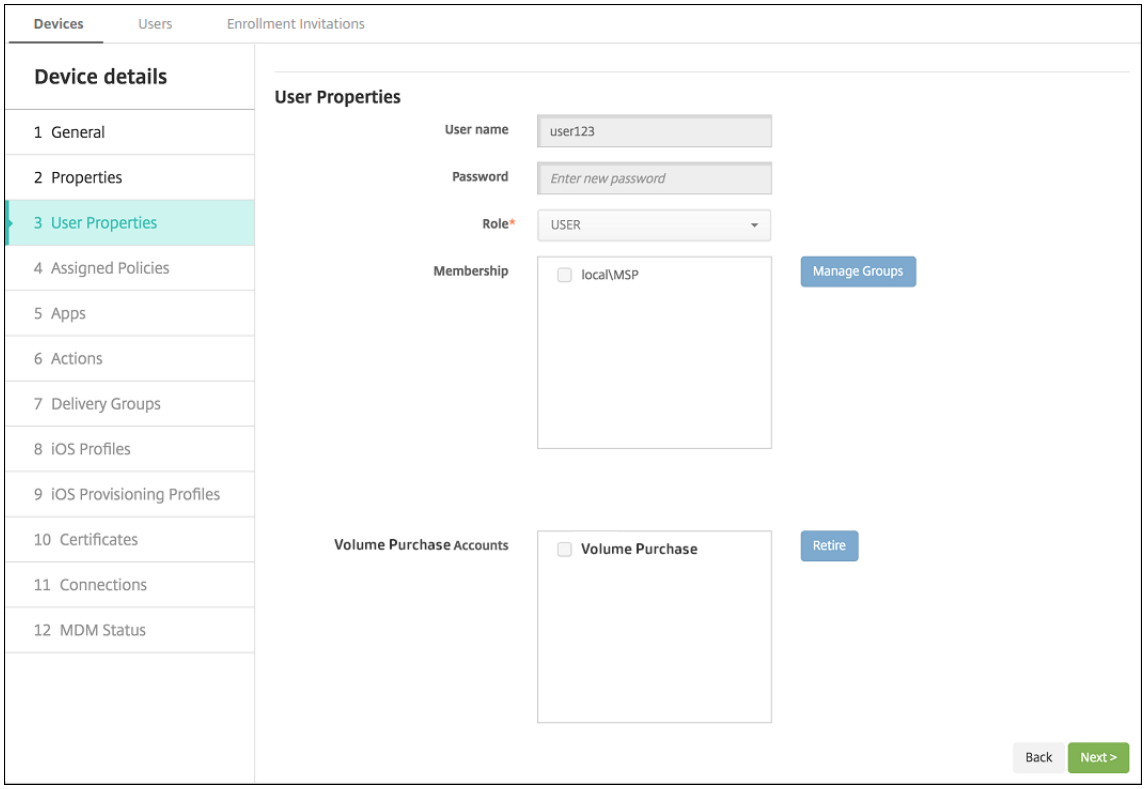
Vous pouvez à présent configurer les paramètres de l'application d'achat en volume, puis régler vos paramètres de groupe de mise à disposition et de stratégie pour les applications d'achat en volume. Une fois que vous avez terminé ces configurations, les utilisateurs peuvent inscrire leurs appareils. Les remarques suivantes fournissent des informations sur ces processus.

- Lors de la configuration des paramètres des applications d'achat en volume (**Configurer > Applications**), activez **Forcer l'association de licence avec l'appareil**. L'un des avantages de l'achat en volume d'Apple et du programme de déploiement avec des appareils supervisés est la possibilité d'utiliser XenMobile pour attribuer l'application au niveau de l'appareil (plutôt qu'au niveau de l'utilisateur). Par conséquent, vous n'avez pas besoin d'utiliser un appareil Apple ID. En outre, les utilisateurs ne reçoivent pas d'invitation à rejoindre le programme d'achat en volume Apple. Les utilisateurs peuvent également télécharger les applications sans se connecter à leur compte iTunes.

  Pour afficher les informations d'achat en volume pour cette application, développez **Achat en volume**. Notez que dans le tableau **Clés de licences d'achat en volume**, la licence est associée à un appareil. Si l'utilisateur supprime le jeton, puis l'importe à nouveau, le mot **Masqué** s'affiche au lieu du numéro de série, en raison de restrictions de confidentialité d'Apple.

  Pour dissocier une licence, cliquez sur la ligne en regard de la licence et cliquez sur **Dissocier**.

  Si vous associez des licences d'achat en volume à des utilisateurs, XenMobile intègre les utilisateurs dans votre compte d'achat en volume et associe leur ID iTunes au compte d'achat en volume. L'ID iTunes des utilisateurs n'est pas visible par votre entreprise ou le serveur XenMobile. Apple crée l'association de manière à protéger la confidentialité des utilisateurs. Vous pouvez retirez un utilisateur de l'achat en volume Apple afin de dissocier toutes les licences du compte utilisateur. Pour retirer un utilisateur, accédez à **Gérer > Appareils**.



- Lorsque vous attribuez une application à un groupe de mise à disposition, XenMobile identifie par défaut l'application en tant qu'application facultative. Pour vous assurer que XenMobile déploie une application sur les appareils, accédez à **Configurer > Groupes de mise à disposition**. Sur la page **Applications**, déplacez l'application dans la liste **Applications requises**.
- Lorsqu'une mise à jour est disponible pour une application d'un magasin d'applications public : lorsque l'achat en volume transmet l'application, elle se met à jour automatiquement sur les appareils. Pour transmettre une mise à jour pour Secure Hub, lorsqu'elle est attribuée à l'appareil et non à un utilisateur, procédez comme suit. Dans **Configurer > Applications**, sur une page de plate-forme, cliquez sur **Rechercher les mises à jour** et appliquez la mise à jour.

  XenMobile affiche un avertissement d'expiration de licence lorsque l'achat en volume Apple a expiré.

Virtual Apps and Desktops via Citrix Secure Hub

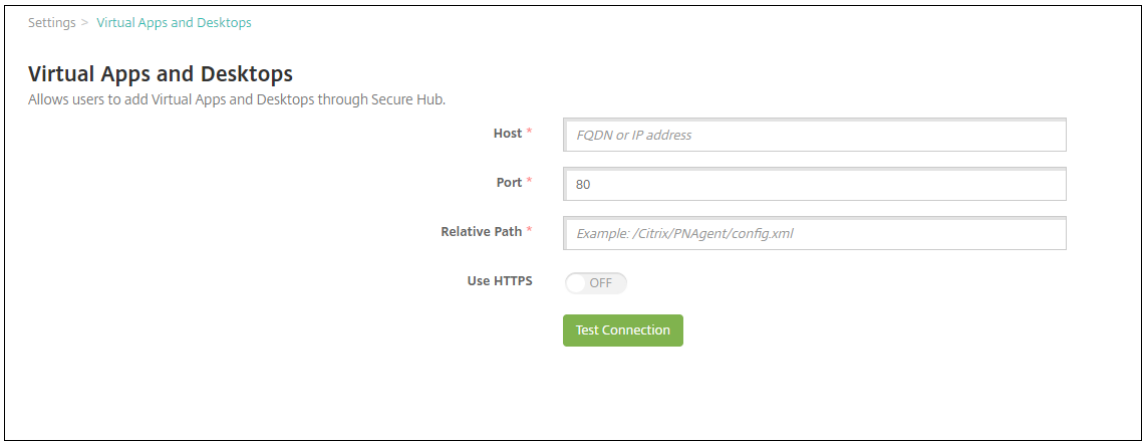
January 10, 2022

XenMobile peut collecter des applications depuis Virtual Apps and Desktops et les rendre disponibles aux utilisateurs d'appareils mobiles dans XenMobile Store. Les utilisateurs s'abonnent directement aux applications dans XenMobile Store et les lancent depuis Secure Hub. Citrix Receiver doit être

installé sur les appareils des utilisateurs pour lancer des applications, mais n'a pas besoin d'être configuré.

Pour configurer ce paramètre, vous devez connaître le nom de domaine complet (FQDN) ou l'adresse IP et le numéro de port du site Interface Web ou StoreFront.

1. Dans la console Web de XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Virtual Apps and Desktops**. La page **Virtual Apps and Desktops** s'affiche.



3. Pour configurer ces paramètres :
   - **Hôte :** entrez le nom de domaine complet (FQDN) ou l'adresse IP pour StoreFront ou le site Interface Web.
   - **Port :** entrez le numéro de port pour StoreFront ou le site Interface Web. La valeur par défaut est 80.
   - **Chemin relatif :** entrez le chemin d'accès. Par exemple, /Citrix/PNAgent/config.xml
   - **Utiliser HTTPS :** sélectionnez cette option si vous souhaitez activer l'authentification sécurisée entre le site Interface Web ou StoreFront et l'appareil client. La valeur par défaut est **Désactivé.**
4. Cliquez sur **Tester la connexion** pour vérifier que XenMobile peut se connecter au serveur Virtual Apps and Desktops spécifié.
5. Cliquez sur **Enregistrer**.

Utiliser Citrix Content Collaboration avec XenMobile

January 10, 2022

XenMobile dispose de deux options d'intégration avec Citrix Content Collaboration : Citrix Files et les connecteurs StorageZone. L'intégration avec Citrix Files ou les connecteurs StorageZone requiert

XenMobile Enterprise Edition.

Citrix Files

Si vous disposez de XenMobile Enterprise Edition, vous pouvez configurer XenMobile pour fournir l'accès à votre compte Citrix Files. Cette configuration :

- Permet aux utilisateurs mobiles d'accéder à l'ensemble des fonctionnalités Enterprise, notamment le partage de fichiers, la synchronisation de fichiers et les connecteurs StorageZone.
- Permet à Citrix Files de bénéficier de l'authentification unique des utilisateurs XenMobile Apps, ainsi que des stratégies de contrôle d'accès complètes.
- Fournit la configuration Citrix Files, le suivi de niveau de service et le contrôle de l'utilisation des licences via la console XenMobile.

Pour plus d'informations sur la configuration de XenMobile pour Citrix Files, consultez SAML pour l'authentification unique avec Citrix Files.

Connecteurs StorageZone

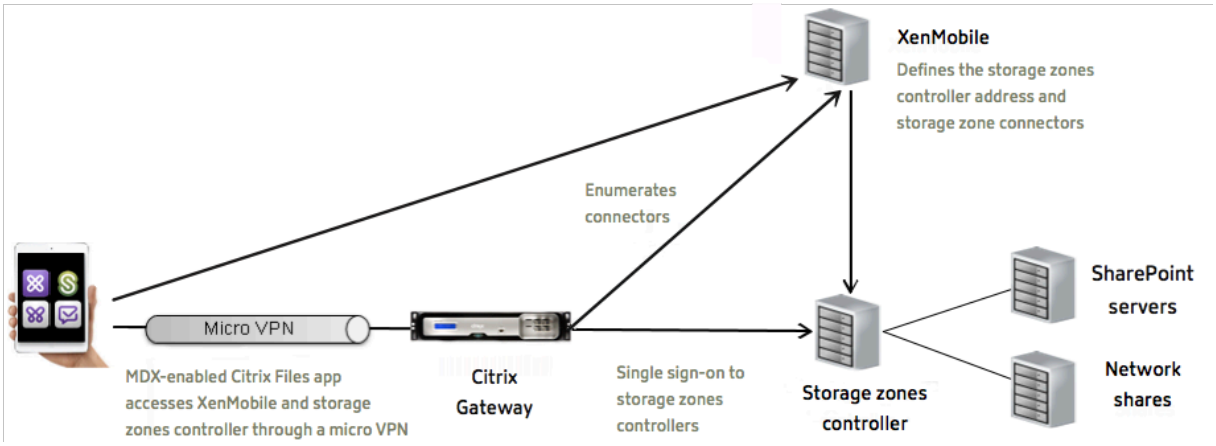
Vous pouvez configurer XenMobile pour fournir l'accès uniquement aux connecteurs StorageZone que vous créez via la console XenMobile. Cette configuration :

- Donne un accès mobile sécurisé aux référentiels de stockage locaux existants, tels que des sites SharePoint et des partages de fichiers réseau.
- Ne nécessite pas la configuration d'un sous-domaine Citrix Content Collaboration ou l'hébergement de données Citrix Files.
- Donne aux utilisateurs un accès mobile aux données via les applications de productivité mobiles Citrix Files pour iOS et Android. Les utilisateurs peuvent modifier des documents Microsoft Office. Les utilisateurs peuvent aussi afficher un aperçu et annoter des fichiers PDF Adobe depuis des appareils mobiles
- Est conforme aux restrictions de sécurité contre la fuite d'informations utilisateur en dehors du réseau d'entreprise.
- Fournit une configuration simple des connecteurs StorageZone via la console XenMobile. Si vous décidez d'utiliser toutes les fonctionnalités Citrix Files avec XenMobile, vous pouvez modifier la configuration dans la console XenMobile.
- Requiert XenMobile Enterprise Edition.

Pour une intégration XenMobile avec connecteurs StorageZone uniquement :

- Citrix Content Collaboration utilise votre configuration d'authentification unique à Citrix Gateway pour s'authentifier auprès du StorageZones Controller.
- XenMobile ne s'authentifie par le biais de SAML, car le plan de contrôle de Citrix Files n'est pas utilisé.

Le diagramme suivant illustre l'architecture lors de l'utilisation de XenMobile avec des connecteurs StorageZone.



Exigences

- Versions minimales des composants :
  - XenMobile Server 10.5 (sur site)
  - ShareFile pour iOS (MDX) 5.3
  - ShareFile pour Android (MDX) 5.3
  - StorageZones Controller 5.0

    Cet article contient des instructions pour configurer le StorageZones Controller 5.0.
- Assurez-vous que le serveur qui exécutera le StorageZones Controller répond à la configuration système requise. Pour la configuration requise, consultez la section Configuration requise.

La configuration requise pour les zones de stockage pour les données Citrix Files et pour les zones de stockage restreintes ne s'applique pas à une intégration XenMobile utilisant uniquement des connecteurs StorageZone.

XenMobile ne prend pas en charge les connecteurs Documentum.

- Pour exécuter des scripts PowerShell :
  - Exécutez les scripts dans la version 32 bits (x86) de PowerShell.

Tâches d'installation

Effectuez les tâches suivantes, dans l'ordre présenté, pour installer et configurer le StorageZones Controller. Ces étapes s'appliquent à une intégration XenMobile avec connecteurs StorageZone uniquement : Certains de ces articles se trouvent dans la documentation relative au StorageZones Controller.

1. Configurer Citrix ADC pour StorageZones Controller

   Vous pouvez utiliser Citrix ADC comme proxy DMZ pour StorageZones Controller.

2. Installer un certificat SSL

   Un StorageZones Controller qui héberge des zones standard nécessite un certificat SSL. Un StorageZones Controller qui héberge des zones restreintes et utilise une adresse interne ne nécessite pas de certificat SSL.

3. Préparer votre serveur

   Une configuration IIS et ASP.NET est nécessaire pour les connecteurs StorageZone.

4. Installer le StorageZones Controller
5. Préparer le StorageZones Controller pour une utilisation avec des connecteurs StorageZone uniquement
6. Spécifier un serveur proxy pour les zones de stockage

   La console StorageZones Controller vous permet de spécifier un serveur proxy correspondant. Vous pouvez également spécifier un serveur proxy à l'aide d'autres méthodes.

7. Configurer le contrôleur de domaine pour faire confiance au StorageZones Controller pour la délégation

   Configurez le contrôleur de domaine pour prendre en charge l'authentification NTLM ou Kerberos sur des partages réseau ou des sites SharePoint.

8. Joindre un StorageZones Controller secondaire à une zone de stockage

   Pour configurer une zone de stockage pour une haute disponibilité, connectez au moins deux StorageZones Controller à celle-ci.

Installer le StorageZones Controller

1. Téléchargez et installez le logiciel du StorageZones Controller :

   a) Accédez à https://www.citrix.com/downloads. Recherchez **ShareFile**, puis téléchargez le dernier programme d'installation de StorageZones Controller.

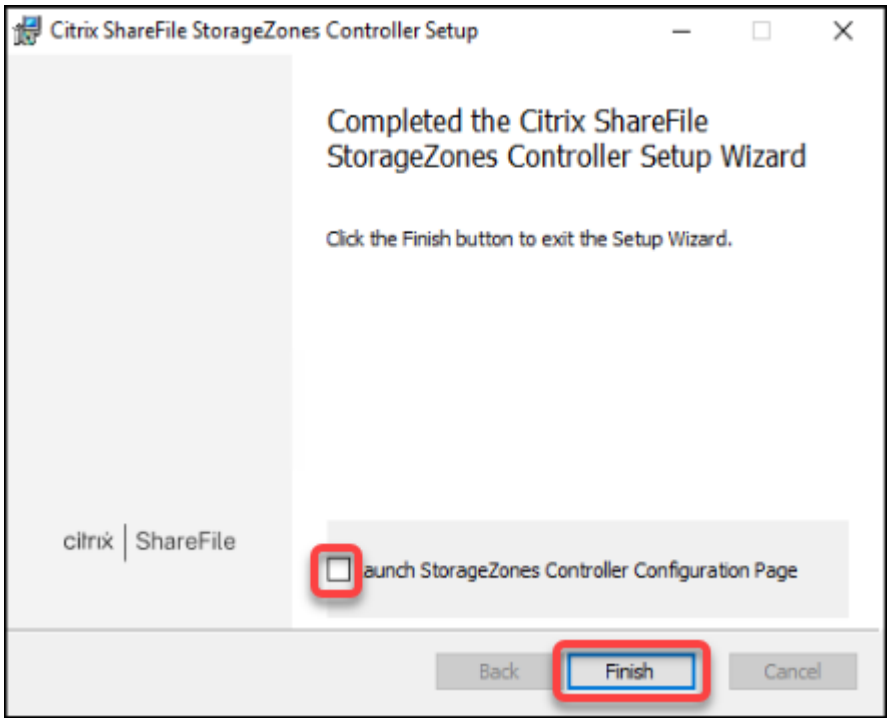
   b) L'installation du StorageZones Controller modifie le site Web par défaut sur le serveur vers le chemin d'installation du contrôleur. Activez l'**authentification anonyme** sur le site Web par défaut.

2. Sur le serveur où vous souhaitez installer le StorageZones Controller, exécutez StorageCenter.msi.

   L'assistant d'installation du StorageZones Controller démarre.

3. Répondez aux invites :

- Dans la page **Destination Folder**, si Internet Information Services (IIS) est installé dans l'emplacement par défaut, laissez les valeurs par défaut. Si ce n'est pas le cas, accédez à l'emplacement d'installation d'IIS.
- Lorsque l'installation est terminée, désactivez la case à cocher **Launch Storage Zones Controller Configuration Page**, puis cliquez sur **Finish**.



4. Lorsque vous y êtes invité, redémarrez le StorageZones Controller.
5. Pour tester la réussite de l'installation, accédez à `https://localhost/`. Si l'installation est réussie, le logo de Citrix Files s'affiche.

   Si le logo Citrix Files n'apparaît pas, désactivez le cache du navigateur et essayez à nouveau.

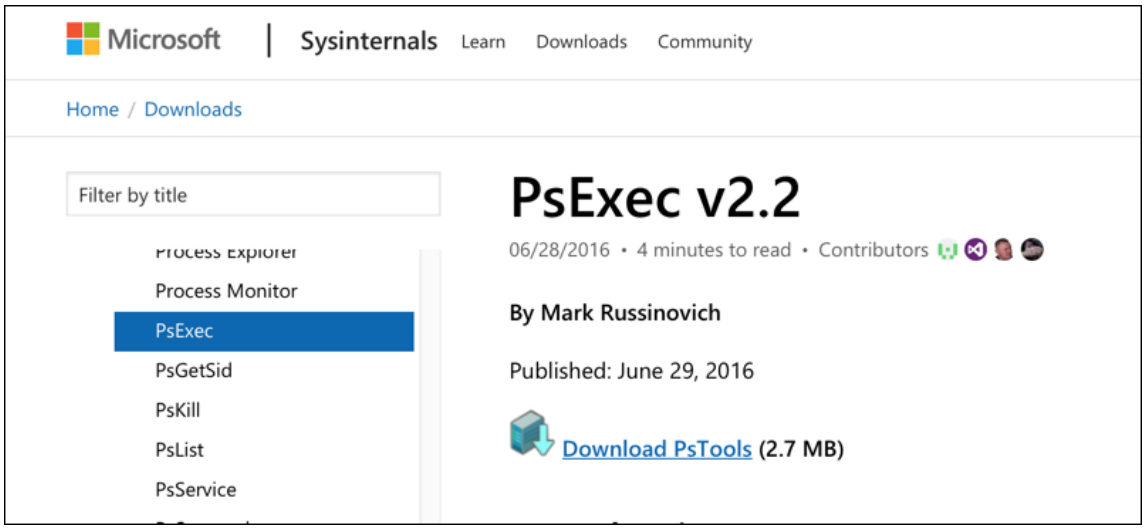
   > **Important :**
   >
   > Si vous prévoyez de cloner le StorageZones Controller, capturez l'image de disque avant de procéder à la configuration du StorageZones Controller.

Préparer le StorageZones Controller pour une utilisation avec des connecteurs StorageZone uniquement

Pour une intégration avec des connecteurs StorageZone uniquement, vous n'utilisez pas la console d'administration du StorageZones Controller. Cette interface nécessite un compte d'administrateur Citrix Files, qui n'est pas nécessaire pour cette solution. Par conséquent, vous exécutez un script PowerShell pour préparer le StorageZones Controller pour une utilisation sans le plan de contrôle Citrix Files. Le script effectue les actions suivantes :

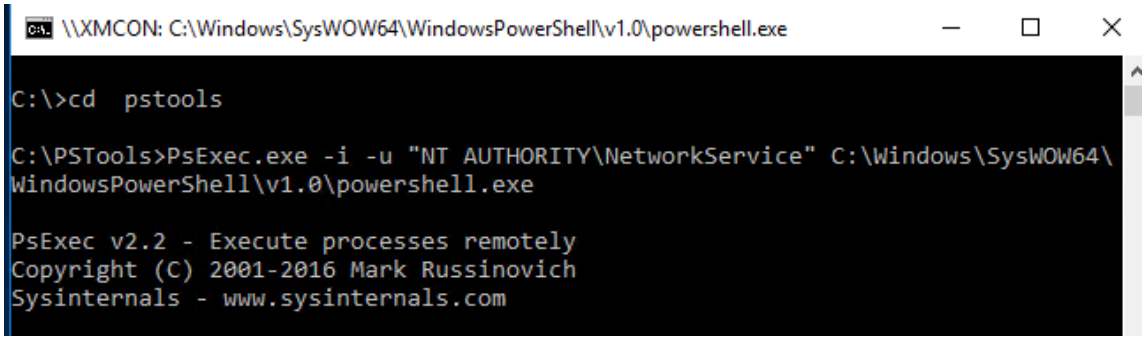
- Enregistre le StorageZones Controller actuel en tant que StorageZones Controller principal. Vous pouvez joindre des StorageZones Controller secondaires au contrôleur principal plus tard.
- Crée une zone et définit la phrase secrète pour celle-ci.

1. À partir de votre serveur StorageZone Controller, téléchargez l'outil PsExec : accédez à Microsoft Windows Sysinternals, puis cliquez sur **Download PsTools**. Extrayez l'outil dans la racine du lecteur C.

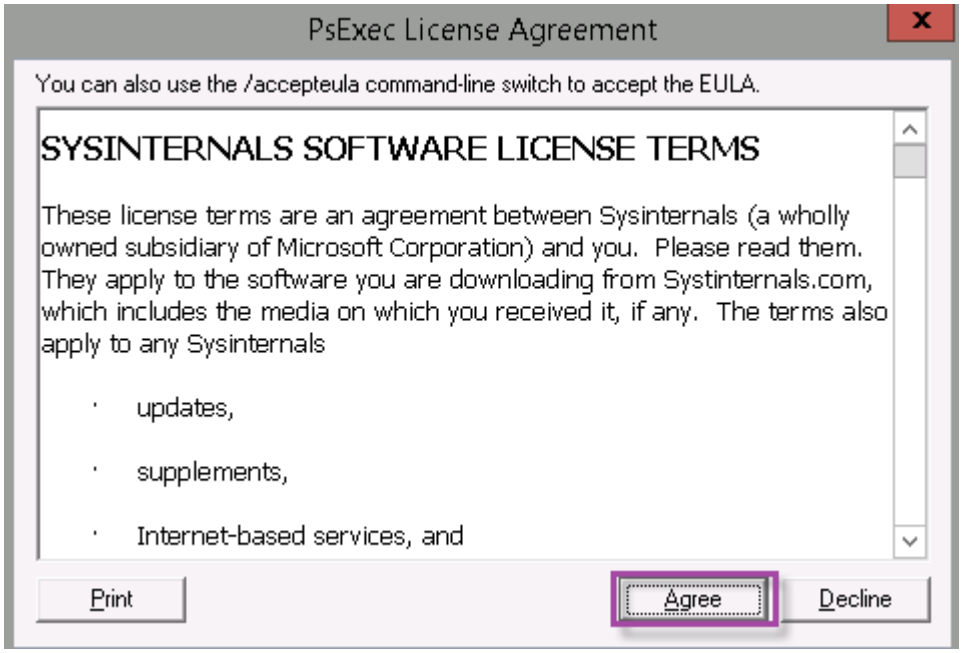


2. Exécutez l'outil PsExec : ouvrez l'invite de commande en tant qu'utilisateur administrateur et tapez ce qui suit :

```
cd c:\pstools
PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
    \WindowsPowerShell\v1.0\powershell.exe
<!--NeedCopy-->
```



3. Lorsque vous y êtes invité, cliquez sur **Agree** pour exécuter l'outil Sysinternals.



Une fenêtre PowerShell s'ouvre.

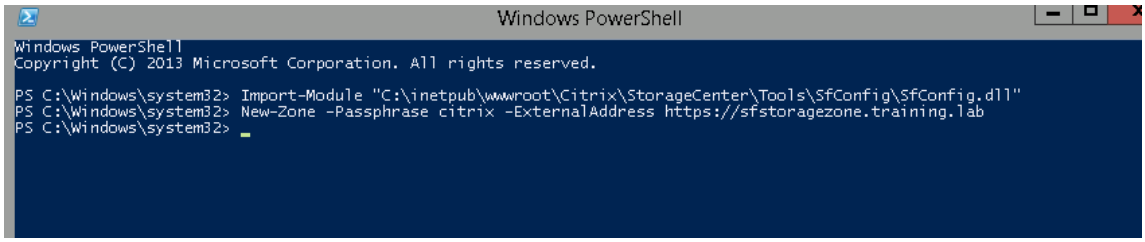
4. Dans la fenêtre PowerShell, tapez ce qui suit :

```
1 Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\
    SfConfig\SfConfig.dll"
2 New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
    com
3 <!--NeedCopy-->
```

Où :

Passphrase : phrase secrète que vous souhaitez attribuer au site. Prenez note de cette dernière. Vous ne pouvez pas récupérer la phrase secrète à partir du contrôleur. Si vous perdez la phrase secrète, vous ne pouvez pas réinstaller le StorageZones Controller. Joignez d'autres StorageZones Controller à la zone de stockage ou récupérez la zone de stockage si le serveur échoue.

ExternalAddress : nom de domaine complet externe du serveur du StorageZones Controller.



Votre StorageZones Controller principal est maintenant prêt.

Avant de vous connecter à XenMobile pour créer des connecteurs StorageZone : effectuez la configuration suivante, le cas échéant :

Spécifier un serveur proxy pour les zones de stockage

Configurer le contrôleur de domaine pour faire confiance au StorageZones Controller pour la délégation

Joindre un StorageZones Controller secondaire à une zone de stockage

Pour créer des connecteurs StorageZone, reportez-vous à la section Définir des connexions StorageZones Controller dans XenMobile.

Joindre un StorageZones Controller secondaire à une zone de stockage

Pour configurer une zone de stockage pour une haute disponibilité, connectez au moins deux StorageZones Controller à celle-ci. Pour joindre un StorageZones Controller secondaire à une zone, installez le StorageZones Controller sur un second serveur. Joignez ensuite ce contrôleur à la zone du contrôleur principal.

1. Ouvrez une fenêtre PowerShell sur le serveur du StorageZones Controller que vous voulez joindre au serveur principal.
2. Dans la fenêtre PowerShell, tapez ce qui suit :

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
   ```

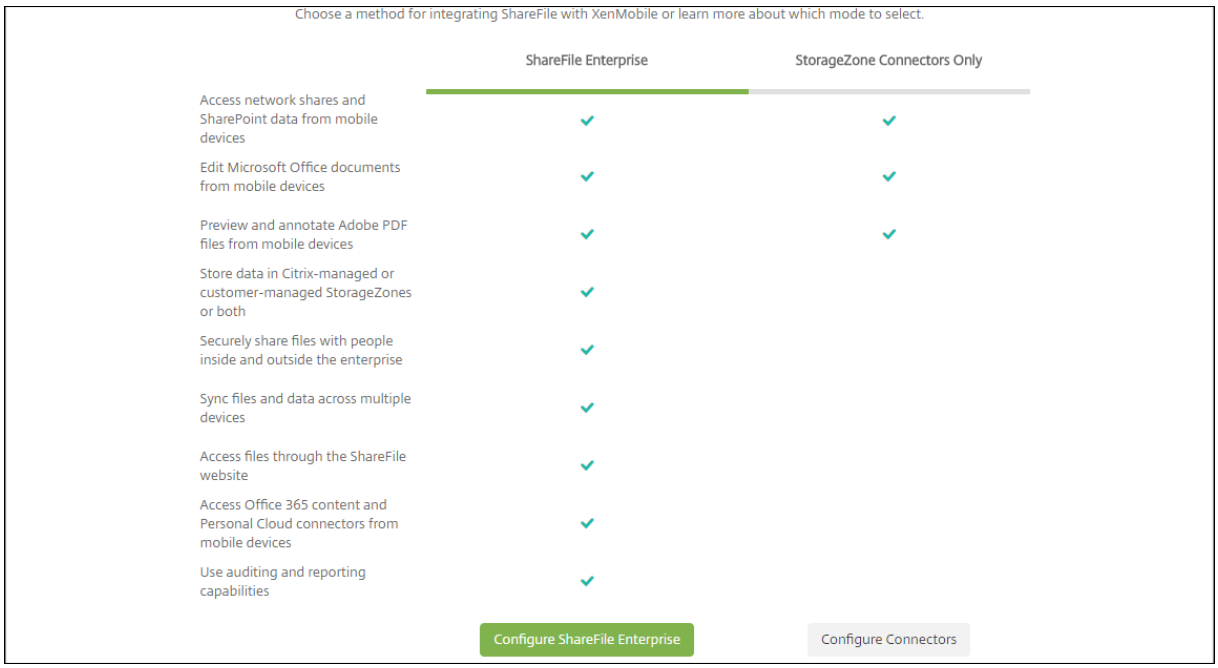
   Par exemple :

   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

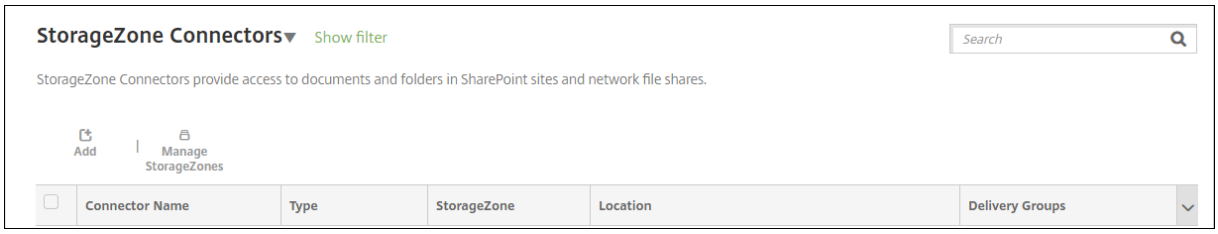
Définir des connexions StorageZones Controller dans XenMobile

Avant d'ajouter des connecteurs StorageZone, vous configurez les informations de connexion pour chaque StorageZones Controller activé pour les connecteurs StorageZone. Vous pouvez définir les StorageZones Controller comme décrit dans cette section, ou lorsque vous ajoutez un connecteur.

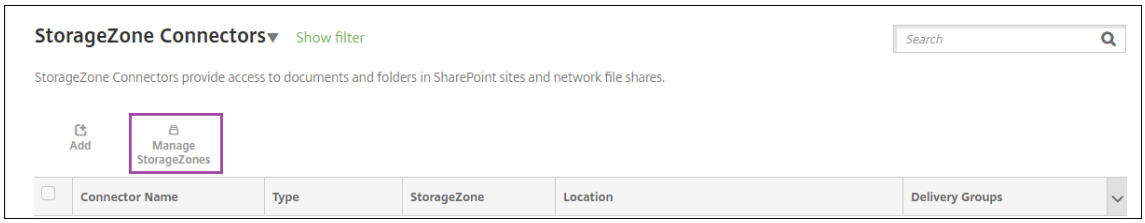
Lors de votre premier accès à la page **Configurer > ShareFile**, la page résume les différences entre l'utilisation des comptes XenMobile pour Enterprise et des connecteurs StorageZone.



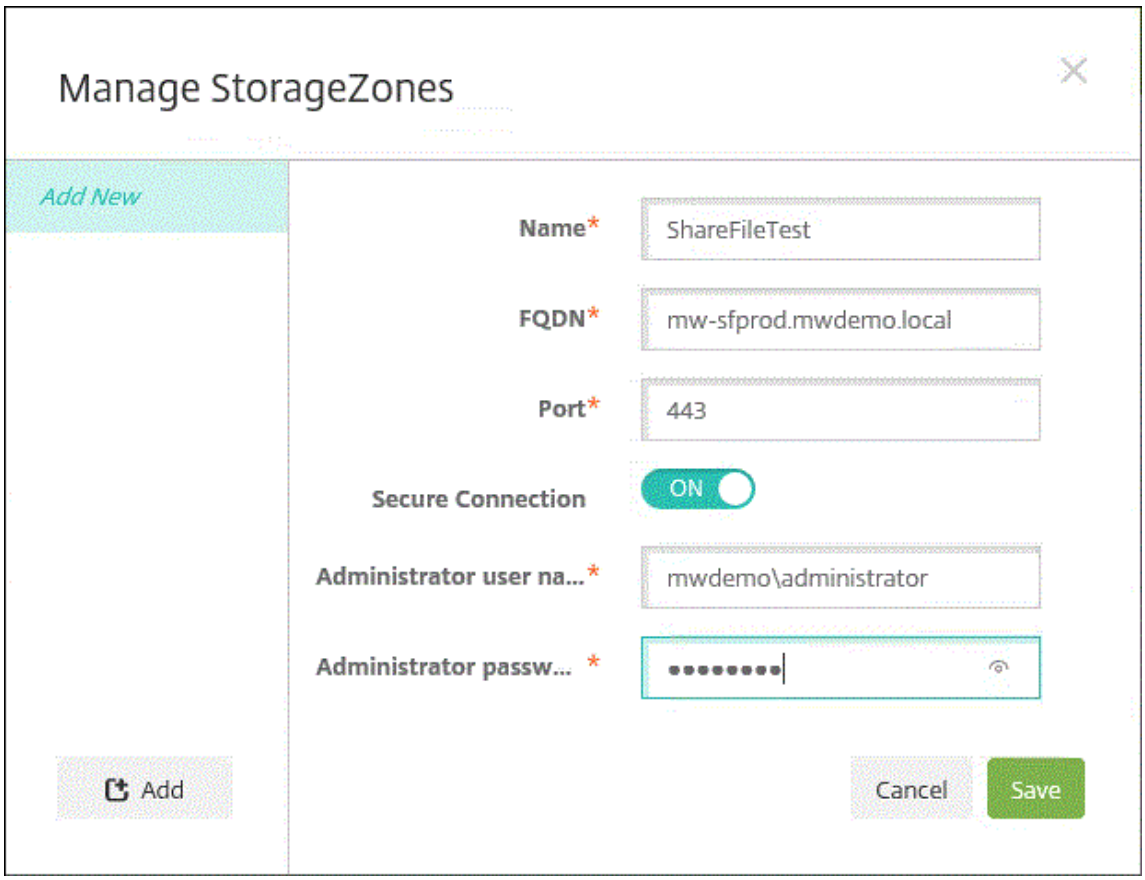
Cliquez sur **Configurer des connecteurs** pour suivre les étapes de configuration décrites dans cet article.



1. Dans **Configurer > ShareFile**, cliquez sur **Gérer les StorageZone**.



2. Dans **Gérer les StorageZone**, ajoutez les informations de connexion.



- **Nom :** nom descriptif pour la StorageZone, utilisé pour identifier la StorageZone dans XenMobile. N'insérez pas d'espace ou de caractères spéciaux dans le nom.
- **Nom de domaine complet et port :** nom de domaine complet et numéro de port pour un StorageZones Controller accessible depuis XenMobile Server.
- **Connexion sécurisée :** si vous utilisez SSL pour les connexions au StorageZones Controller, utilisez le paramètre par défaut, Activé. Si vous n'utilisez pas SSL pour les connexions, définissez ce paramètre sur Désactivé.
- **Nom d'utilisateur administrateur** et **Mot de passe administrateur** : nom d'utilisateur du compte de service administrateur (au format domaine\administrateur) et mot de passe. Sinon, un compte d'utilisateur avec les autorisations Lire et Écrire sur les StorageZones Controller.

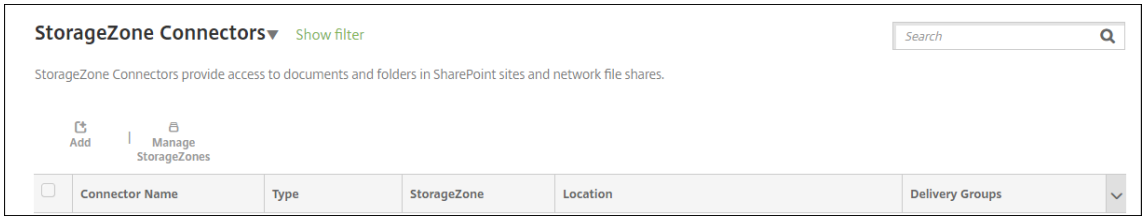
3. Cliquez sur **Enregistrer**.
4. Pour tester la connexion, vérifiez que le serveur XenMobile peut accéder au nom de domaine complet du StorageZones Controller sur le port 443.
5. Pour définir une autre connexion au StorageZones Controller, cliquez sur le bouton **Ajouter** dans **Gérer les StorageZone**.

   Pour modifier ou supprimer les informations d'une connexion de StorageZones Controller, sélectionnez le nom de la connexion dans **Gérer les StorageZone**. Cliquez ensuite sur **Modifier**

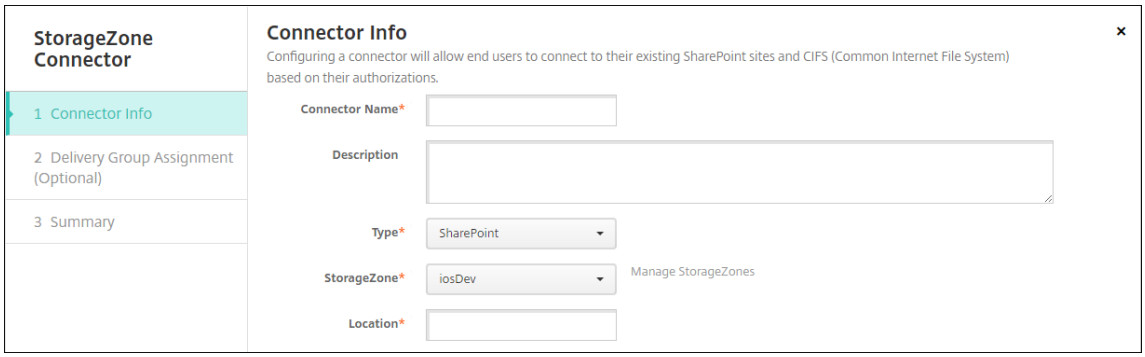
ou **Supprimer**.

Ajouter un connecteur StorageZone dans XenMobile

1. Accédez à **Configurer > ShareFile**, puis cliquez sur **Ajouter**.

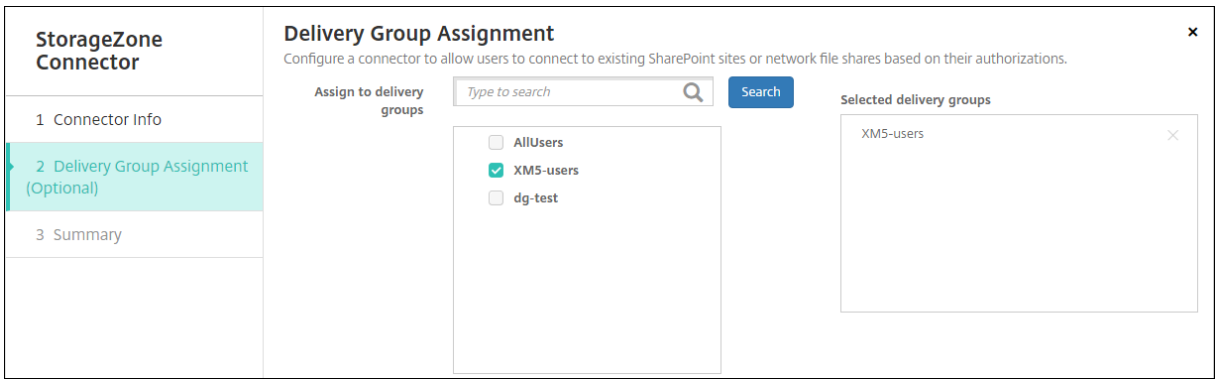


2. Sur la page **Informations sur le connecteur**, configurez les paramètres suivants :



   - **Nom du connecteur :** nom qui identifie le connecteur StorageZone dans XenMobile.
   - **Description :** notes facultatives sur ce connecteur.
   - **Type :** choisissez **SharePoint** ou **Réseau**.
   - **StorageZone :** choisissez la StorageZone associée au connecteur. Si la zone de stockage ne figure pas dans la liste, cliquez sur **Gérer les StorageZone** pour définir le StorageZones Controller.
   - **Emplacement :** pour SharePoint, spécifiez l'URL du site SharePoint au niveau racine, de la collection du site ou de la bibliothèque de documents, au format `https://sharepoint.company.com`. Pour un partage réseau, spécifiez le nom de domaine complet du chemin d'accès UNC (Uniform Naming Convention), au format \\serveur\partage.

3. (Facultatif) Sur la page **Attribution de groupes de mise à disposition**, attribuez le connecteur à des groupes de mise à disposition. Vous pouvez également associer des connecteurs à des groupes de mise à disposition à l'aide de **Configurer > Groupes de mise à disposition**.



1. Sur la page **Résumé**, vous pouvez vérifier les options que vous avez configurées. Pour régler la configuration, cliquez sur **Précédent**.
2. Cliquez sur **Enregistrer** pour enregistrer le connecteur.
3. Testez le connecteur :

    a) Lorsque vous encapsulez les clients Citrix Files, procédez comme suit :

    - Définissez la stratégie Accès réseau sur **Tunnélisé vers le réseau interne**.

    Dans ce mode de fonctionnement, l'infrastructure XenMobile MDX intercepte tout le trafic réseau à partir du client Citrix Files. Le trafic est redirigé via Citrix Gateway à l'aide d'un VPN micro spécifique à l'application.

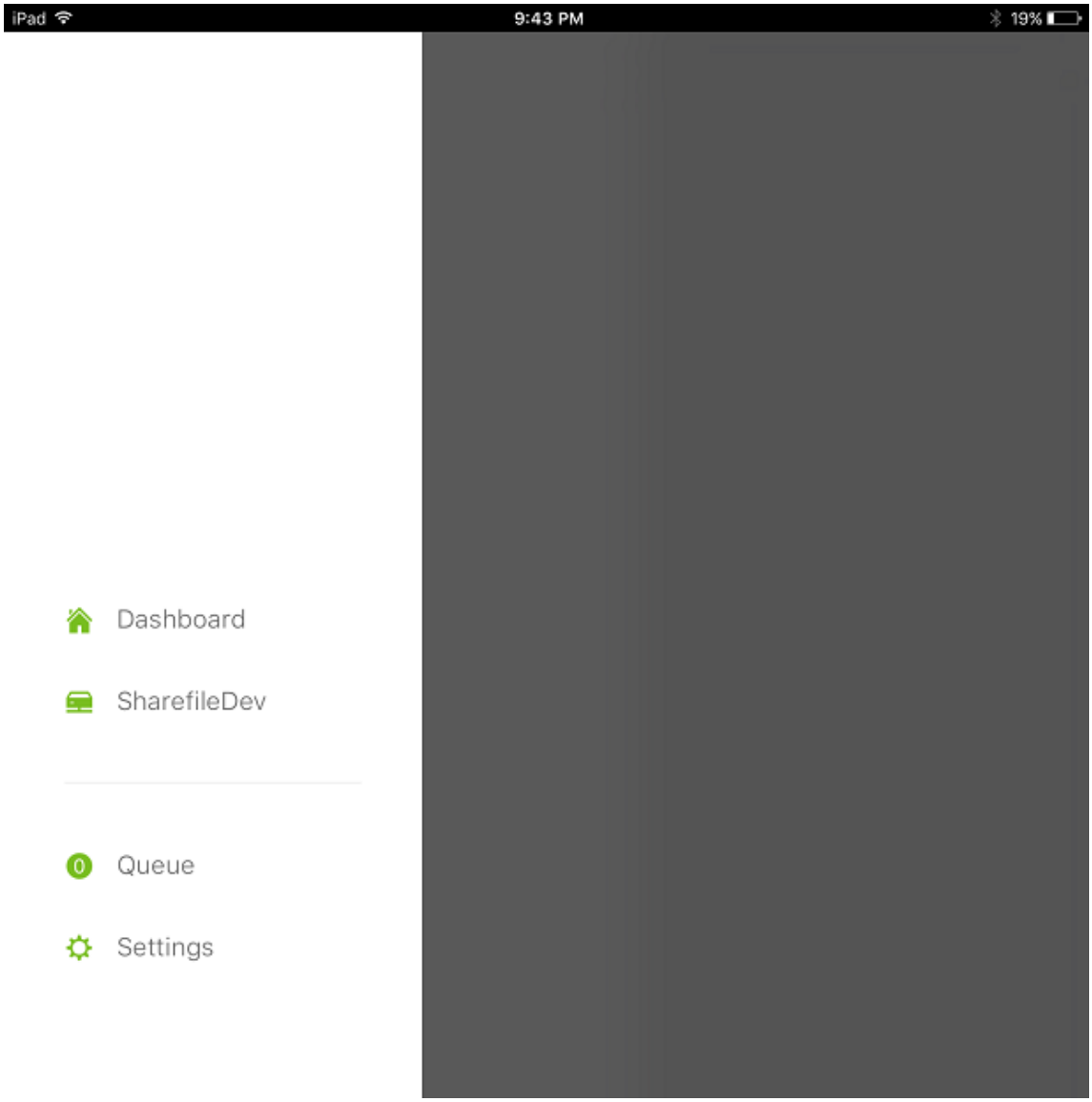
    - Définissez la stratégie Mode VPN préféré sur **Tunnel - SSO Web**.

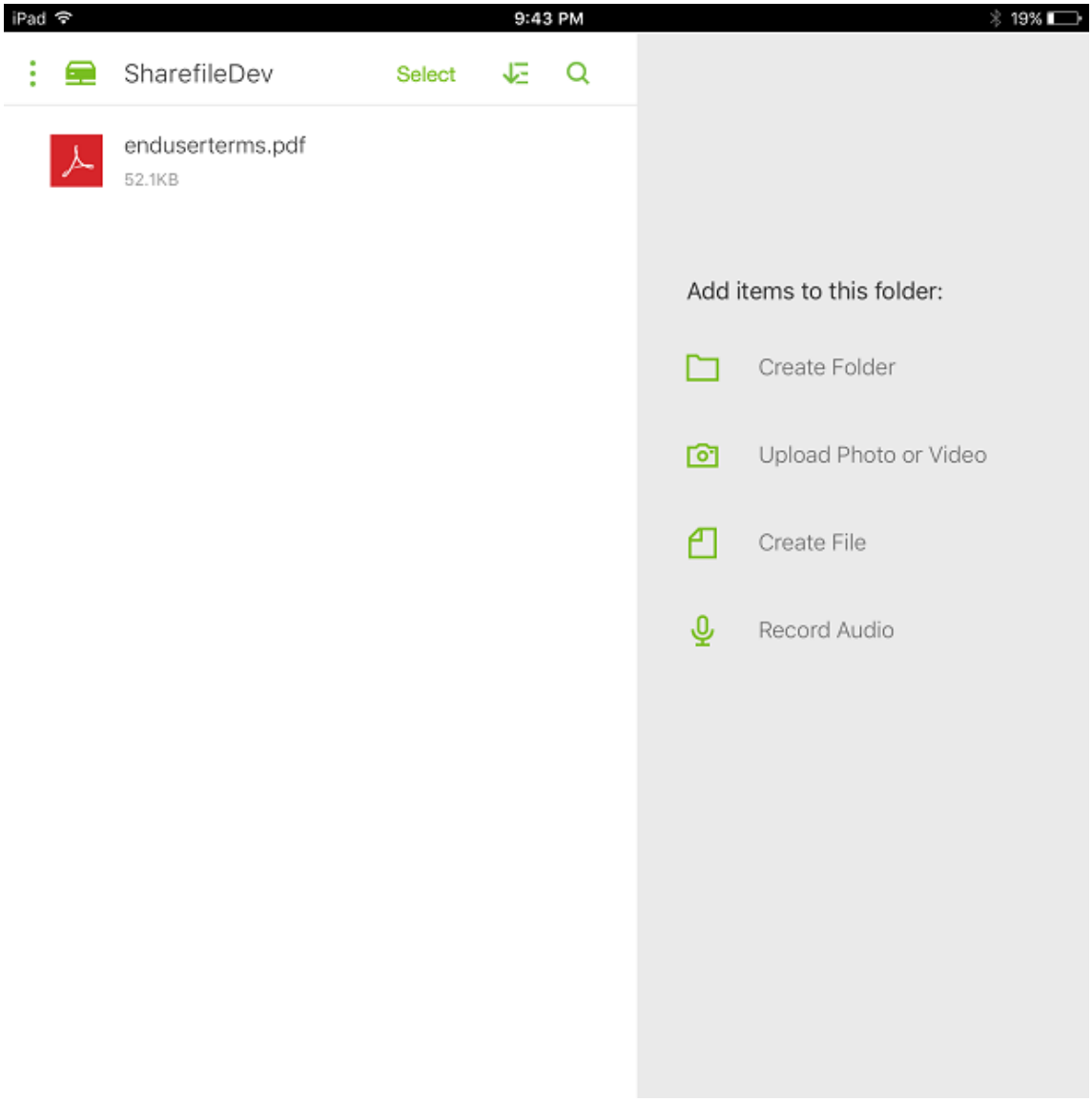
    Dans ce mode de tunneling, l'infrastructure MDX arrête le trafic SSL/HTTP en provenance d'une application MDX, puis initialise de nouvelles connexions aux connexions internes pour le compte de l'utilisateur. Ce paramètre de stratégie permet à l'infrastructure MDX de détecter et de répondre aux demandes d'authentification émises par des serveurs Web.

    b) Ajoutez les clients Citrix Files à XenMobile. Pour plus de détails, voir Intégration et mise à disposition des clients Citrix Files pour Endpoint Management.

    c) À partir d'un appareil pris en charge, vérifiez l'authentification unique à Citrix Files et aux connecteurs.

    Dans les exemples suivants, SharefileDev est le nom d'un connecteur.

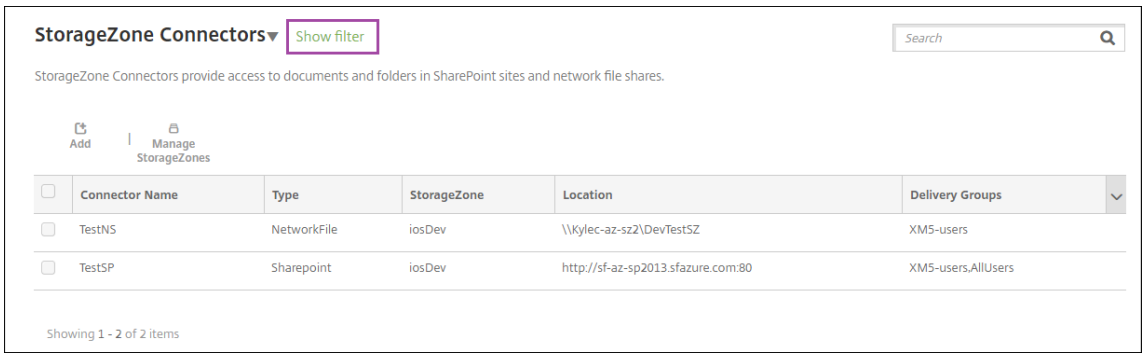




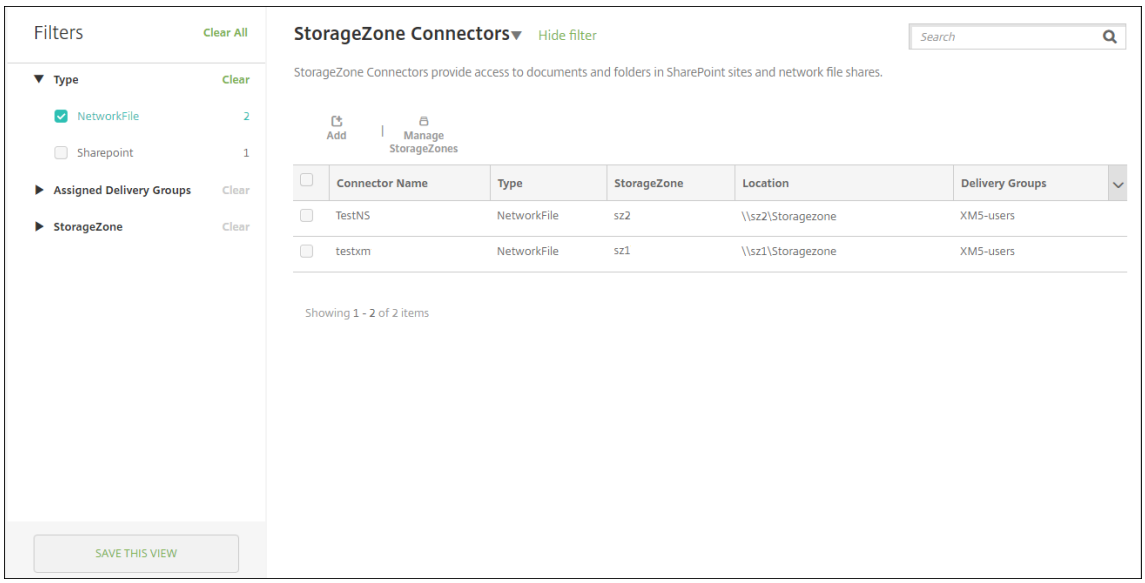
Filtrer la liste des connecteurs StorageZone

Vous pouvez filtrer la liste des connecteurs StorageZone par type de connecteur, groupes de mise à disposition attribués et StorageZone.

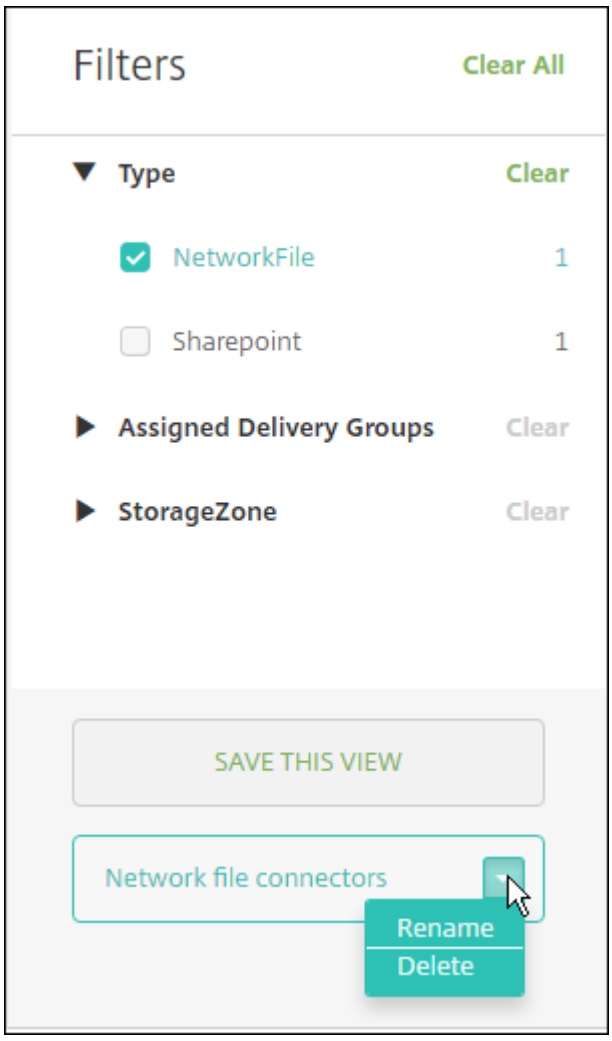
1. Accédez à **Configurer > ShareFile**, puis cliquez sur **Afficher le filtre**.



2. Développez les en-têtes de filtre pour effectuer une sélection. Pour enregistrer un filtre, cliquez sur **Enregistrer cette vue**, entrez le nom du filtre et cliquez sur **Enregistrer**.



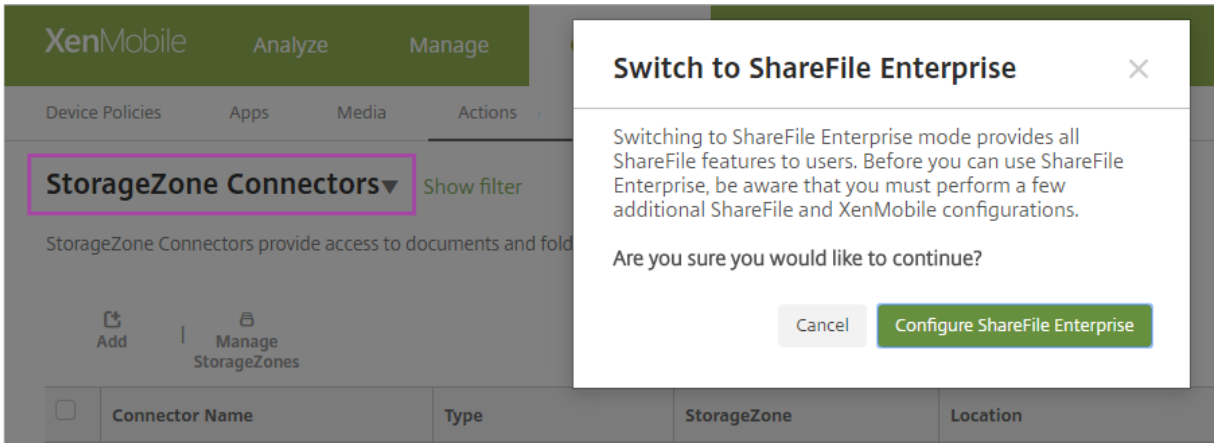
3. Pour renommer ou supprimer un filtre, cliquez sur l'icône de flèche en regard du nom du filtre.



Basculer vers Citrix Files

Après l'intégration des connecteurs StorageZone avec XenMobile, vous pouvez basculer vers l'ensemble complet des fonctionnalités Enterprise. L'utilisation de l'ensemble des fonctionnalités Citrix Files requiert XenMobile Enterprise Edition. XenMobile conserve vos paramètres d'intégration de connecteur StorageZone existants.

Accédez à **Configurer > ShareFile**, cliquez sur le menu déroulant **Connecteurs StorageZone**, puis cliquez sur **Configurer ShareFile Enterprise**.



Pour plus d'informations sur la configuration de Citrix Files, consultez la section SAML pour l'authentification unique avec Citrix Files.

SmartAccess pour applications HDX

January 10, 2022

Cette fonctionnalité vous permet de contrôler l'accès aux applications HDX en fonction des propriétés d'un appareil, des propriétés utilisateur d'un appareil ou des applications installées sur un appareil. Pour utiliser cette fonctionnalité, vous définissez des actions automatisées pour marquer l'appareil comme non conforme pour refuser l'accès de cet appareil. Utilisées en conjonction avec cette fonctionnalité, les applications HDX sont configurées dans Virtual Apps and Desktops à l'aide d'une stratégie SmartAccess qui refuse l'accès aux appareils non conformes. XenMobile communique l'état de l'appareil à StoreFront à l'aide d'une balise signée et cryptée. Ensuite, StoreFront autorise ou refuse l'accès en fonction de la stratégie de contrôle d'accès de l'application.

Pour utiliser cette fonctionnalité, votre déploiement requiert :

- Virtual Apps and Desktops 7.6
- StoreFront 3.7 ou 3.8
- XenMobile Server configuré avec des applications HDX agrégées à partir d'un serveur StoreFront
- XenMobile Server configuré avec un certificat SAML à utiliser pour la signature et le cryptage des balises. Le même certificat sans clé privée est chargé sur le serveur StoreFront.

Pour commencer à utiliser cette fonctionnalité :

- Configurer le certificat du serveur XenMobile pour le magasin StoreFront
- Configurer au moins un groupe de mise à disposition Virtual Apps and Desktops avec la stratégie SmartAccess requise
- Définir l'action automatisée dans XenMobile

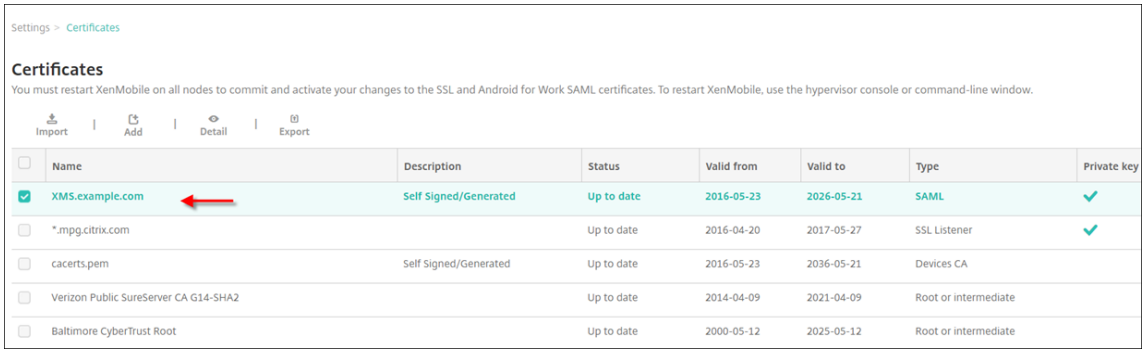
Exporter et configurer le certificat du serveur XenMobile et le charger vers le magasin StoreFront

SmartAccess utilise des balises signées et cryptées pour communiquer entre les serveurs StoreFront et XenMobile. Pour activer cette communication, vous ajoutez le certificat du serveur XenMobile au magasin StoreFront.

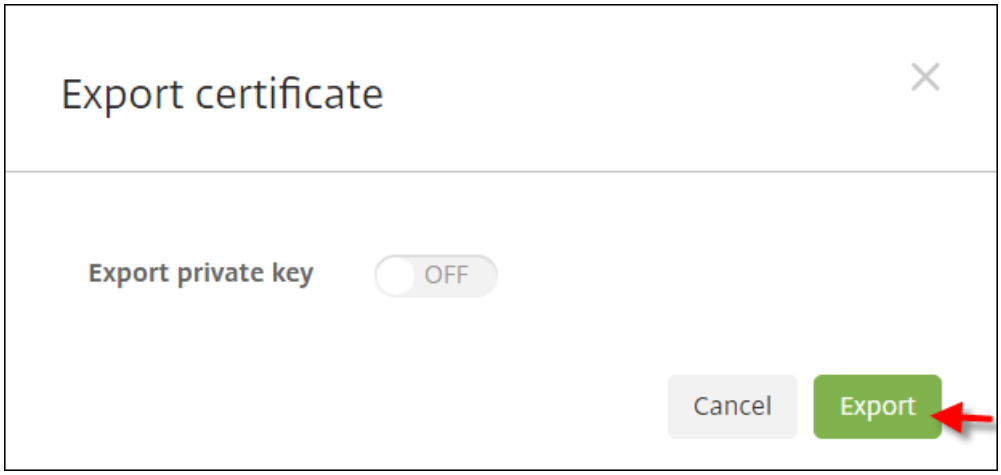
Pour plus d'informations sur l'intégration de StoreFront et XenMobile lorsque XenMobile est activé avec l'authentification basée sur domaine et sur certificats, consultez le Centre de connaissances.

Exporter le certificat SAML à partir du serveur XenMobile

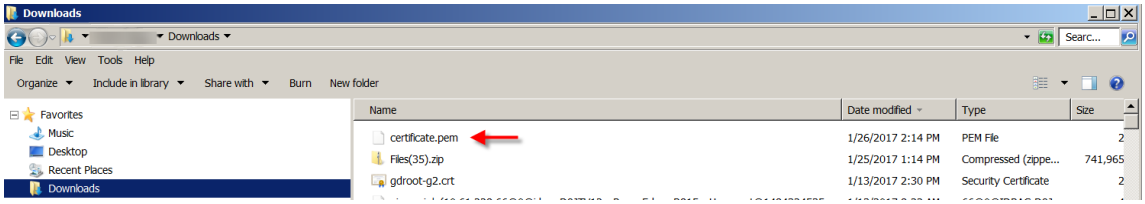
1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche. Cliquez sur **Certificats**.
2. Localisez le certificat SAML pour le serveur XenMobile.



3. Assurez-vous que **Exporter clé privée** est défini sur **Désactivé**. Cliquez sur **Exporter** pour exporter le certificat vers votre répertoire de téléchargement.

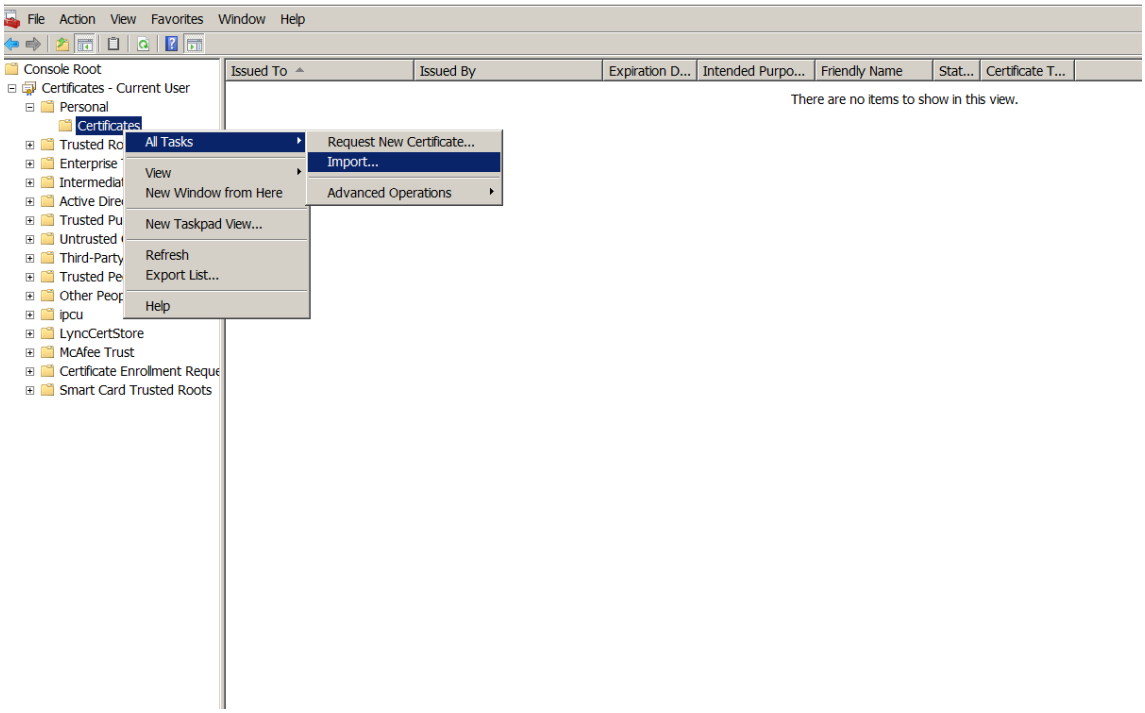


4. Localisez le certificat dans votre répertoire de téléchargement. Le certificat est au format PEM.

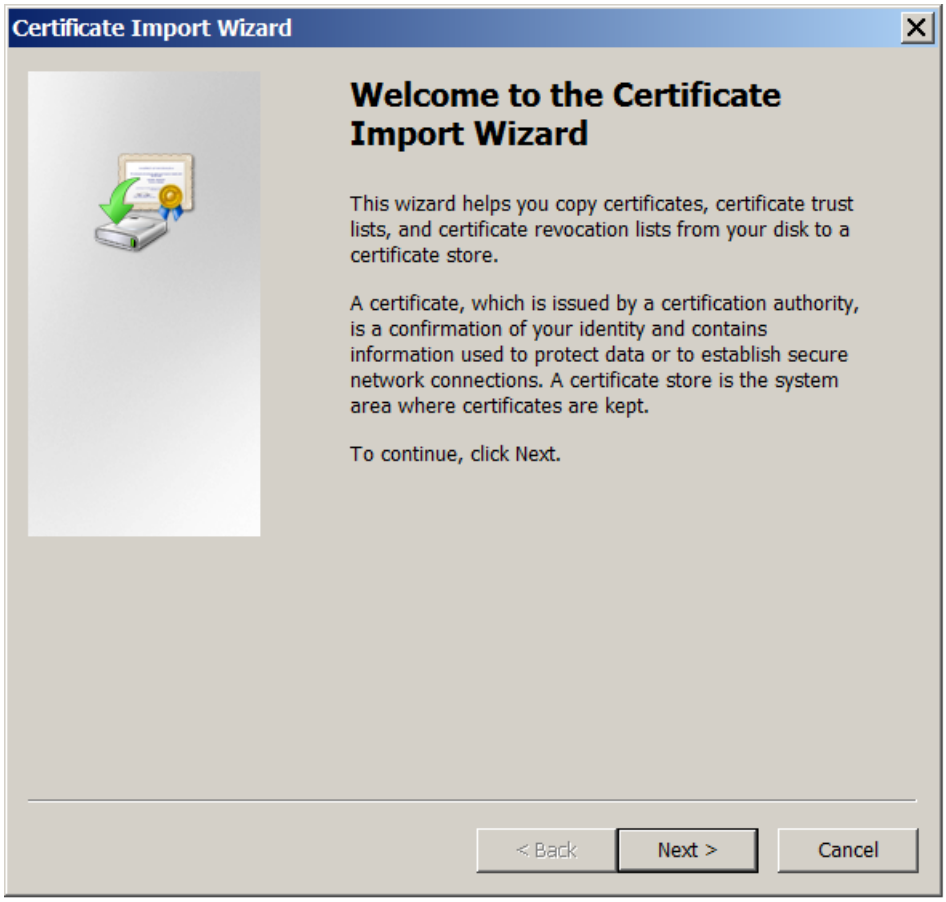


Convertir le certificat de PEM vers CER

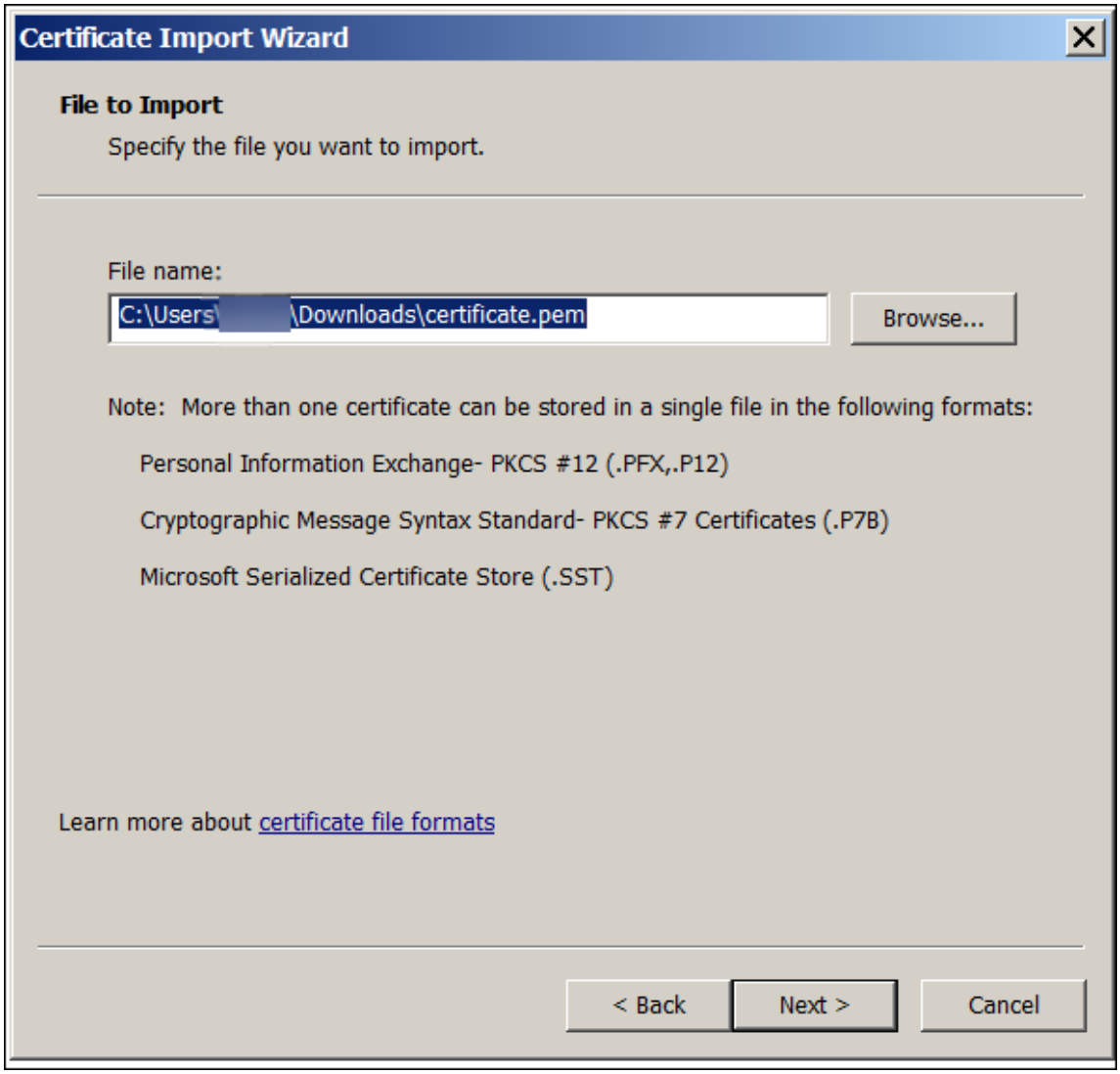
1. Ouvrez la console Microsoft Management Console (MMC) et cliquez avec le bouton droit sur **Certificats > Toutes les tâches > Importer**.



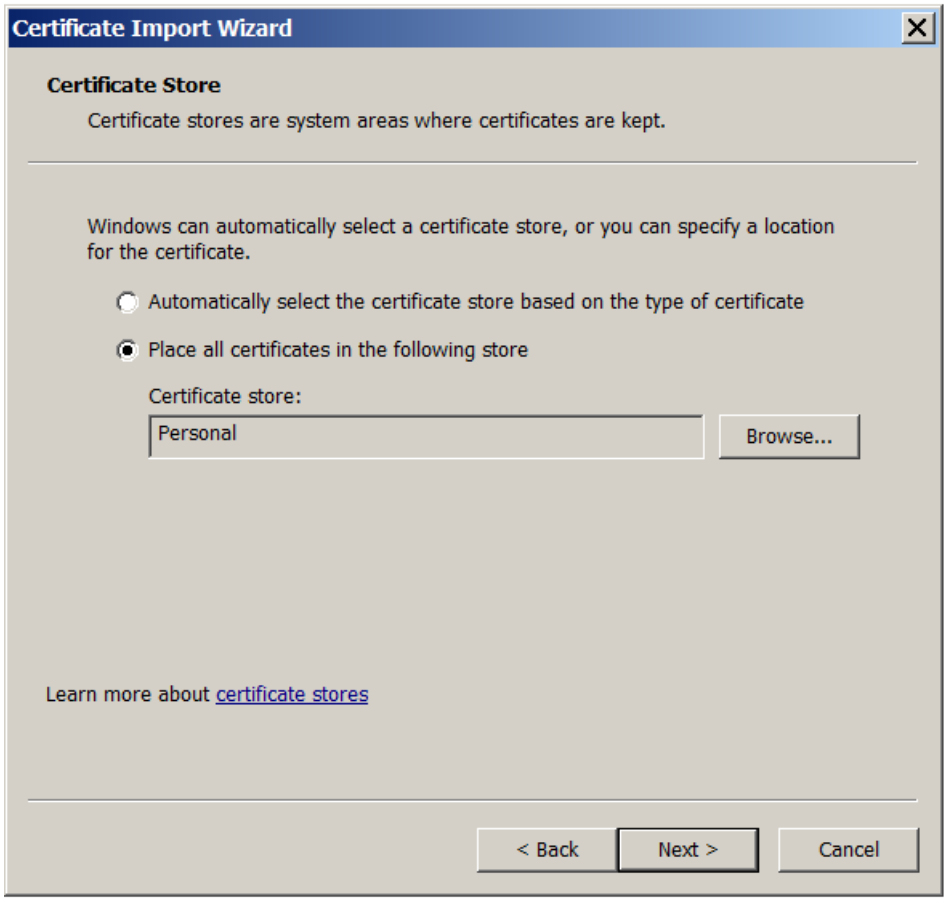
2. Lorsque l'Assistant Importation de certificat apparaît, cliquez sur **Suivant**.



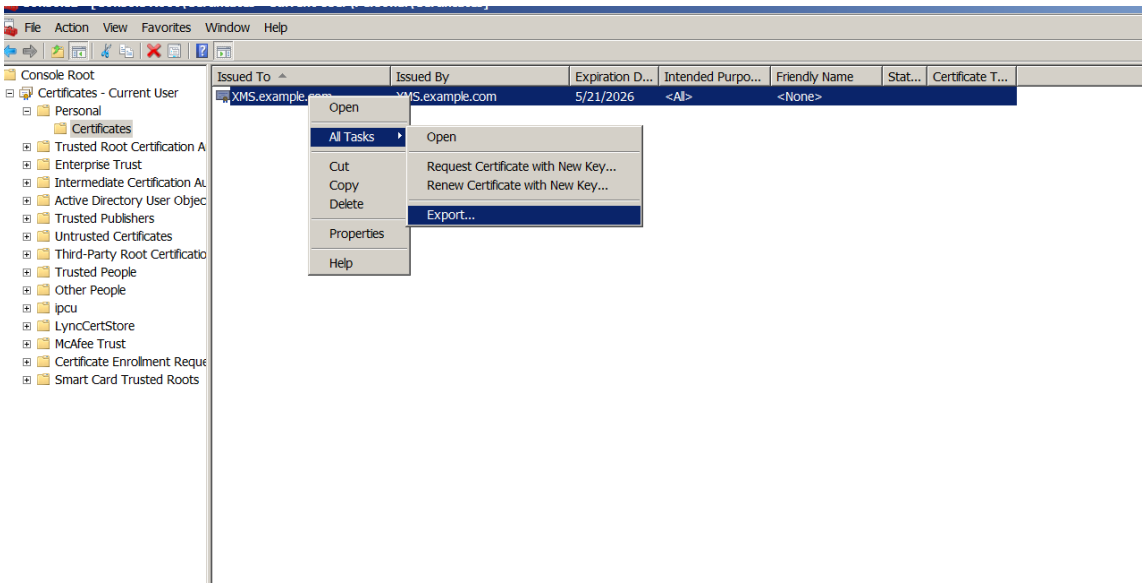
3. Accédez au certificat dans votre répertoire de téléchargement.



4. Sélectionnez **Placer tous les certificats dans le magasin suivant** et sélectionnez **Personnel** comme magasin de certificats. Cliquez sur **Suivant**.

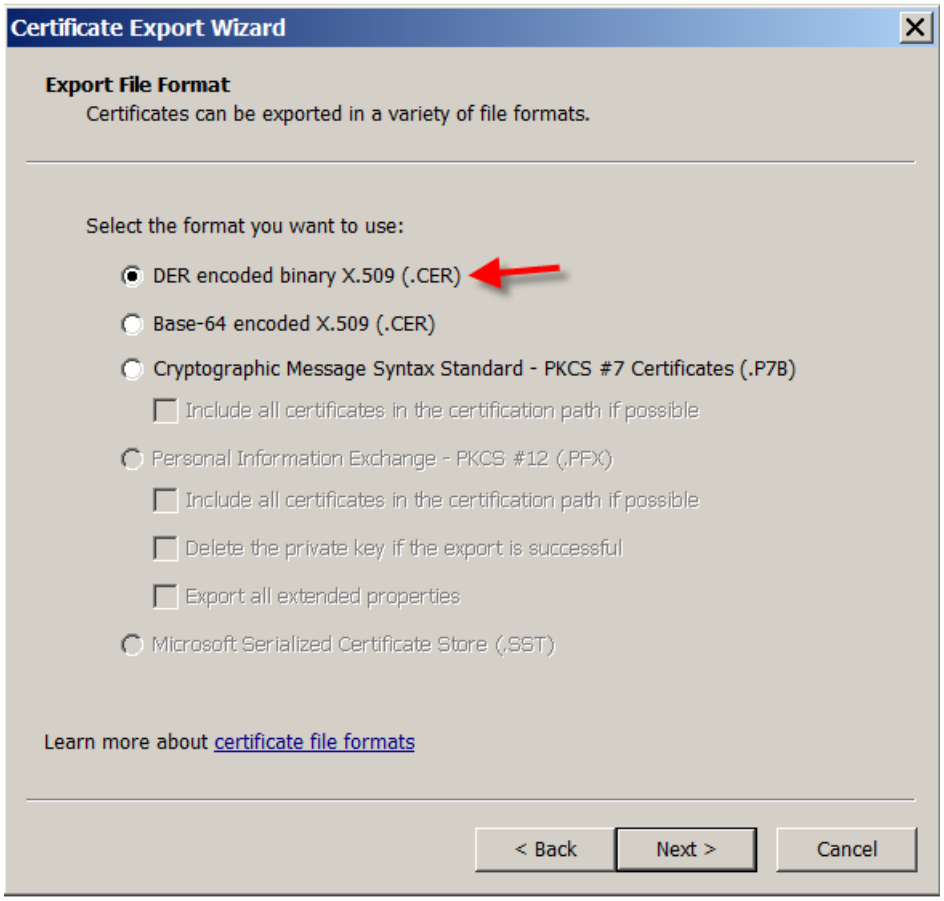


5. Vérifiez vos sélections et cliquez sur **Terminer**. Cliquez sur **OK** dans la fenêtre de confirmation.
6. Dans la console MMC, cliquez avec le bouton droit de la souris sur le certificat et sélectionnez **Toutes les tâches > Exporter**.

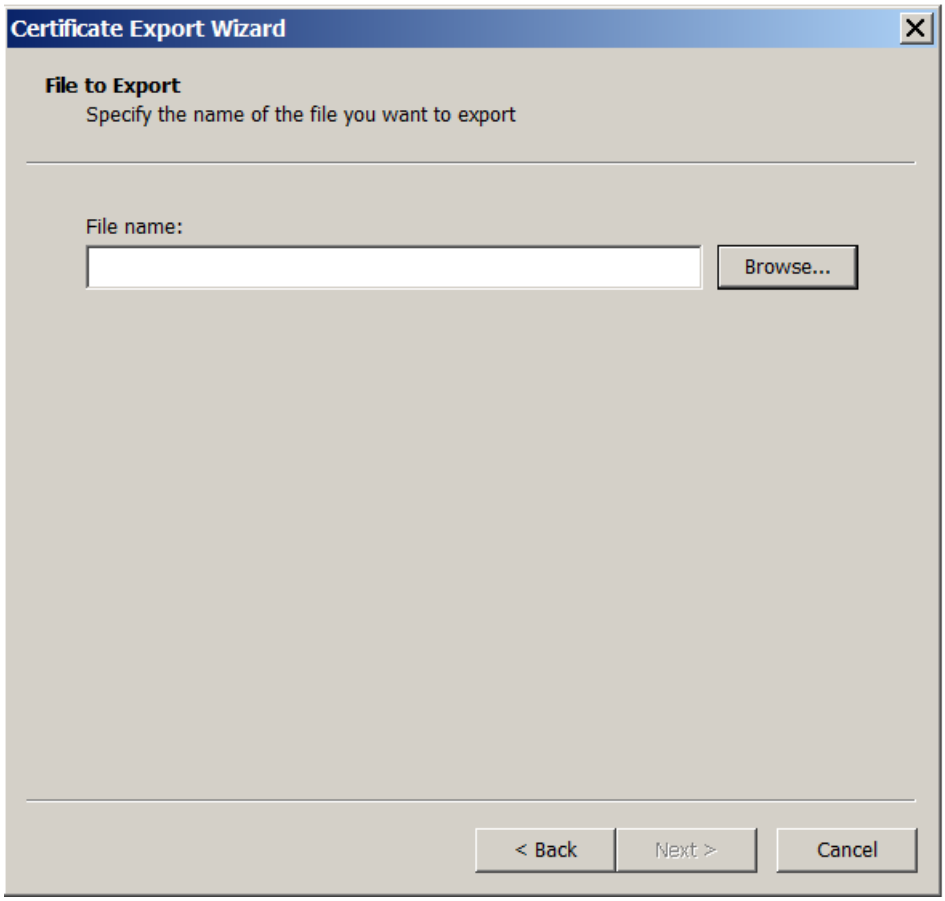


7. Lorsque l'Assistant Exportation de certificat apparaît, cliquez sur **Suivant**.

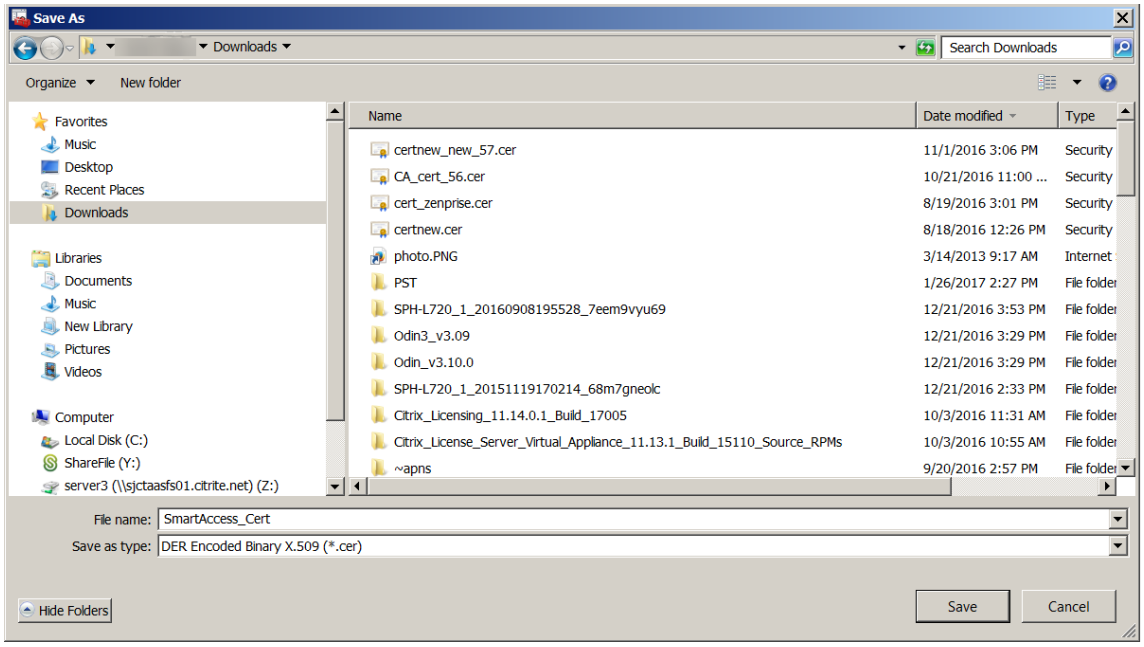
8. Choisissez le format **X.509 binaire encodé DER (*.cer)**. Cliquez sur **Suivant**.



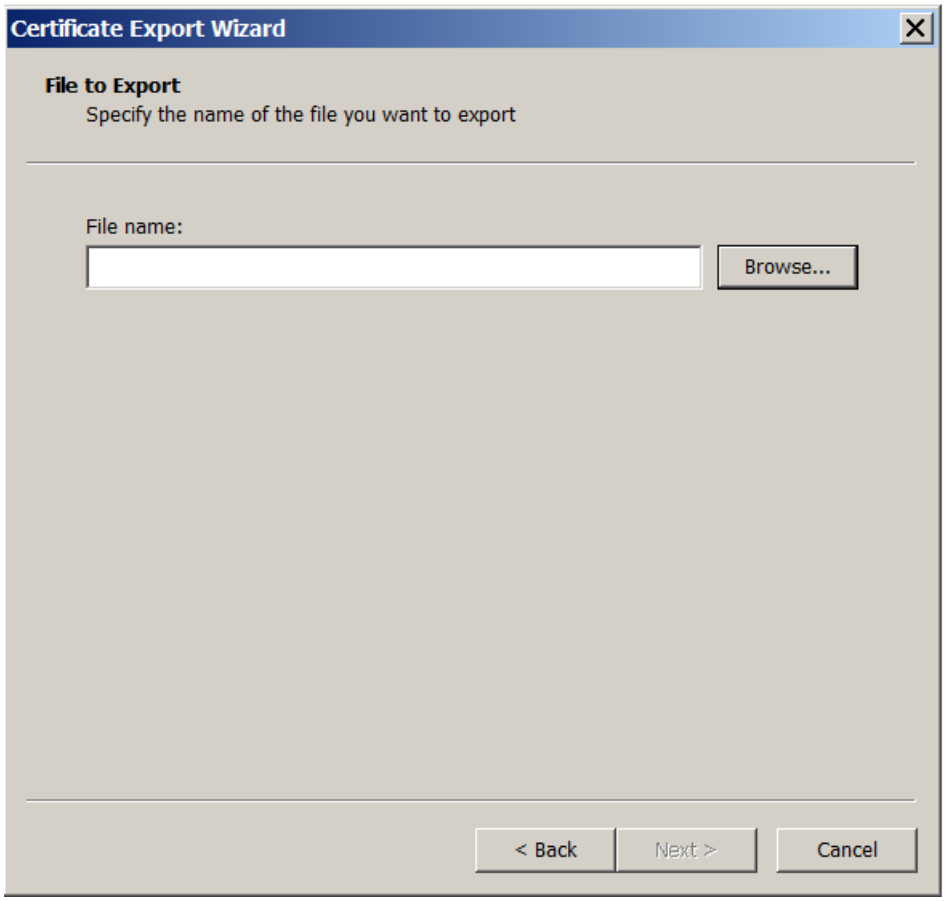
9. Localisez le certificat. Saisissez un nom pour le certificat et cliquez sur **Suivant**.



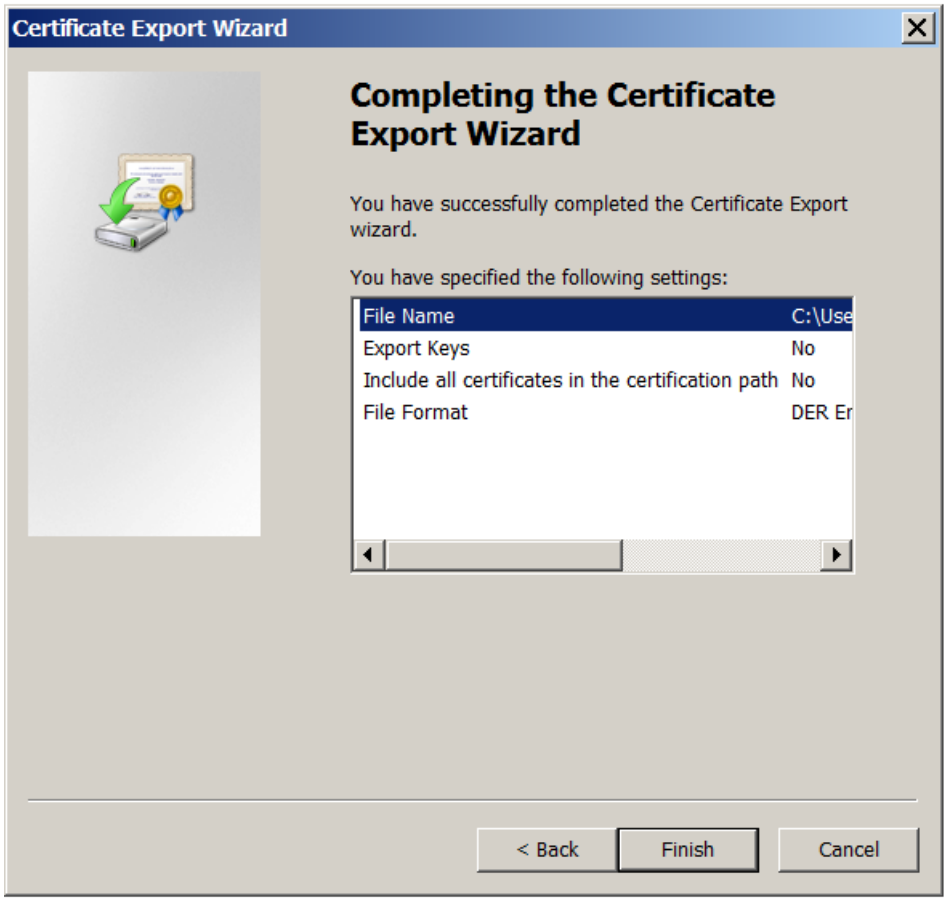
10. Enregistrez le certificat.



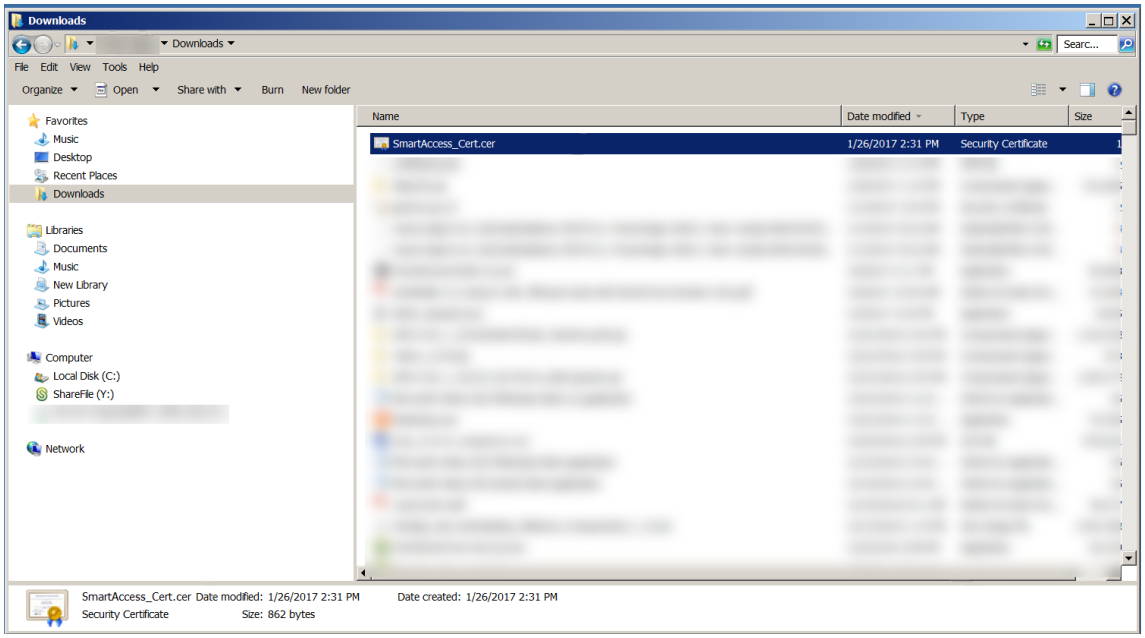
11. Localisez le certificat et cliquez sur **Suivant**.



12. Vérifiez vos sélections et cliquez sur **Terminer**. Cliquez sur **OK** dans la fenêtre de confirmation.

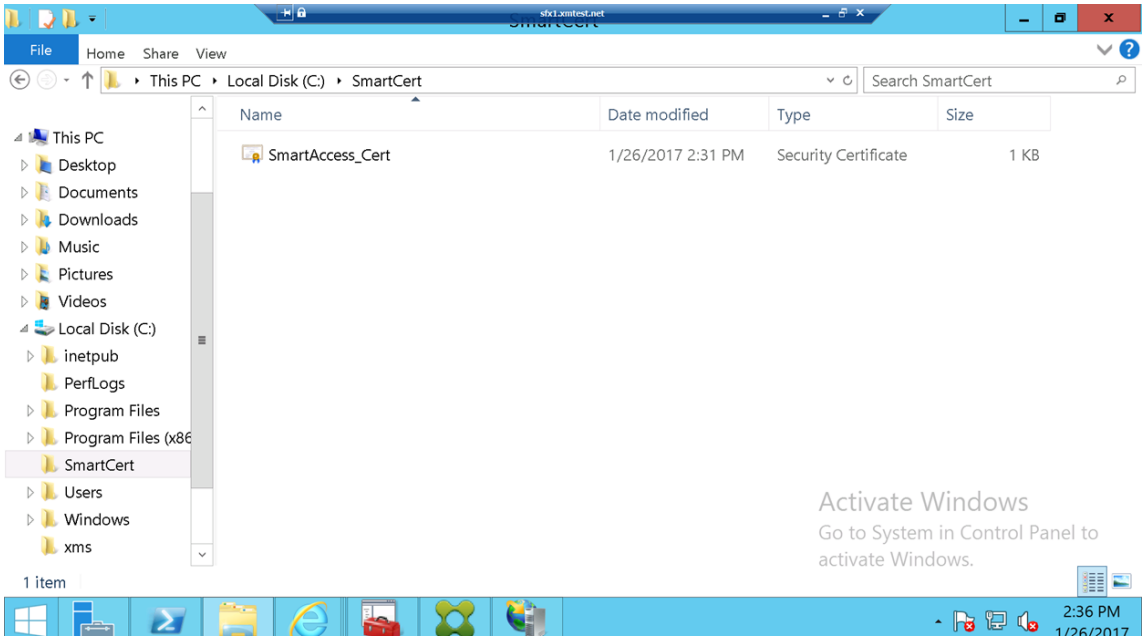


13. Localisez le certificat dans votre répertoire de téléchargement. Veuillez noter que le certificat est au format CER.



Copiez le certificat vers le serveur StoreFront

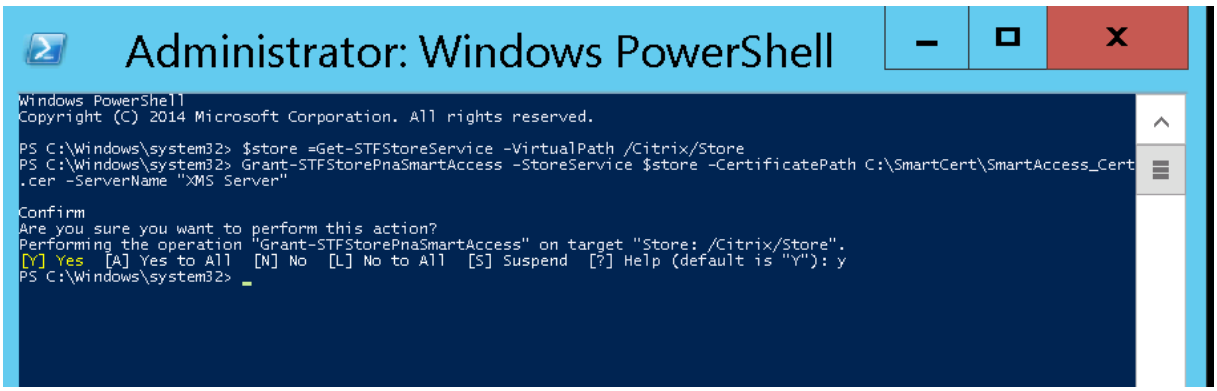
1. Sur le serveur StoreFront, créez un dossier appelé **SmartCert**.
2. Copiez le certificat dans le dossier **SmartCert**.



Configurer le certificat sur le magasin StoreFront

Sur le serveur StoreFront, exécutez cette commande PowerShell pour configurer le certificat du serveur XenMobile converti sur le magasin :

```
1    Grant-STFStorePnaSmartAccess -StoreService $store -
        CertificatePath "C:\xms\xms.cer" -ServerName "XMS server"
2  <!--NeedCopy-->
```



S'il existe des certificats dans le magasin StoreFront, exécutez cette commande PowerShell pour les révoquer :


```
    Revoke-STFStorePnaSmartAccess  -StoreService $store  -All
<!--NeedCopy-->
```

Vous pouvez également exécuter l'une de ces commandes PowerShell sur le serveur StoreFront pour révoquer des certificats existants sur le magasin StoreFront :

- Révoquer par nom :

```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -ServerName  "
       My XM Server"
<!--NeedCopy-->
```

- Révoquer par empreinte numérique :

```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -
       CertificateThumbprint  "ReplaceWithThumbprint"
<!--NeedCopy-->
```

- Révoquer par objet serveur :

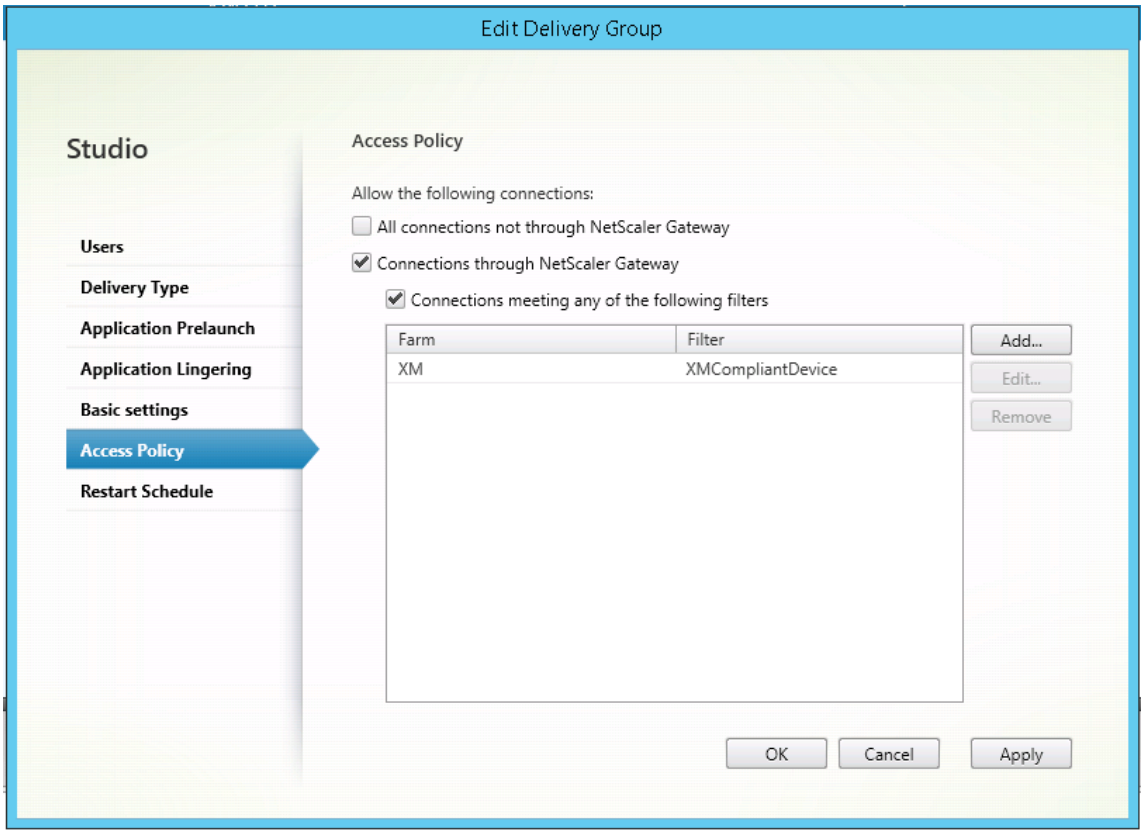
```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    $access = Get-STFStorePnaSmartAccess  -StoreService $store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -SmartAccess
       $access.AccessConditionsTrusts[0]
<!--NeedCopy-->
```

Configurer la stratégie SmartAccess pour Virtual Apps and Desktops

Pour ajouter la stratégie SmartAccess requise au groupe de mise à disposition de l'application HDX :

1. Sur le serveur Virtual Apps and Desktops, ouvrez Citrix Studio.
2. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.

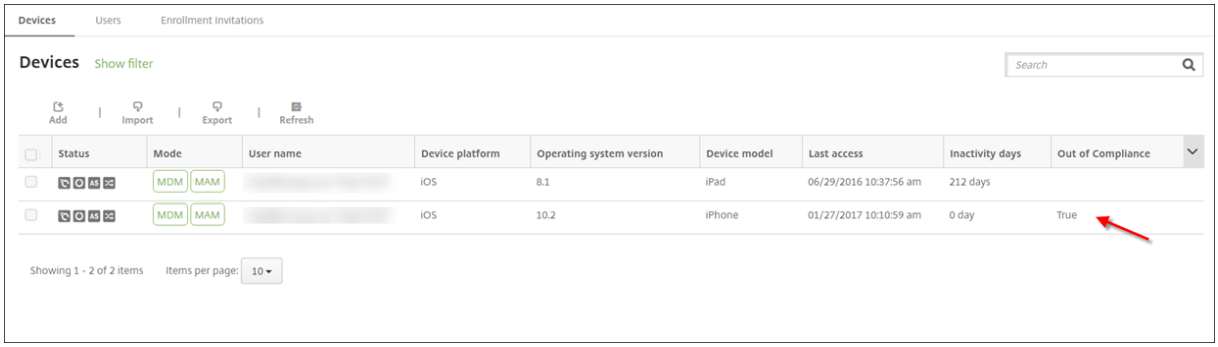
3. Sélectionnez un groupe mettant à disposition l'application ou les applications dont vous souhaitez contrôler l'accès. Sélectionnez **Modifier le groupe de mise à disposition** dans le volet **Actions**.
4. Dans la page **Stratégie d'accès**, sélectionnez **Connexions transitant par NetScaler Gateway** et **Connexions remplissant l'un des critères de filtre suivants**.
5. Cliquez sur **Ajouter**.
6. Ajoutez une stratégie d'accès dans laquelle **Batterie** est **XM** et **Filtre** est **XMCompliantDevice**.



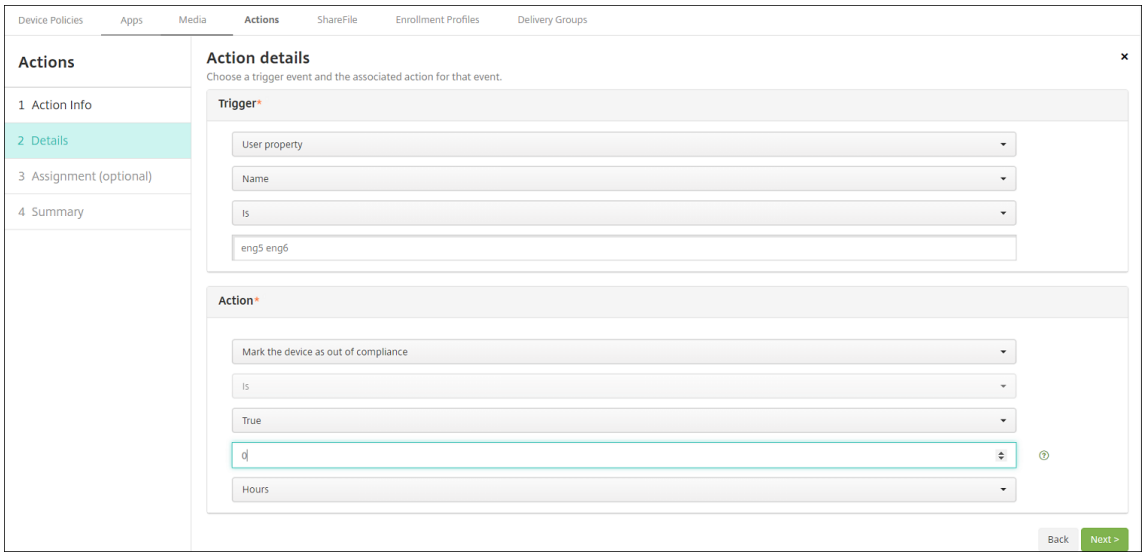
7. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Définir les actions automatisées dans XenMobile

La stratégie SmartAccess que vous avez définie dans le groupe de mise à disposition pour une application HDX refuse l'accès à un appareil lorsque l'appareil n'est pas conforme. Utilisez des actions automatisées pour marquer l'appareil comme non conforme.



1. Dans la console XenMobile, cliquez sur **Configurer > Actions**. La page **Actions** s'affiche.
2. Cliquez sur **Ajouter** pour ajouter une action. La page **Informations sur l'action** s'affiche.
3. Sur la page **Informations sur l'action**, entrez un nom et une description pour l'action.
4. Cliquez sur **Suivant**. La page sur les **Détails de l'action** s'affiche. Dans l'exemple suivant, un déclencheur est créé qui marque immédiatement les appareils comme non conformes s'ils ont le nom de propriété utilisateur **eng5** ou **eng6**.



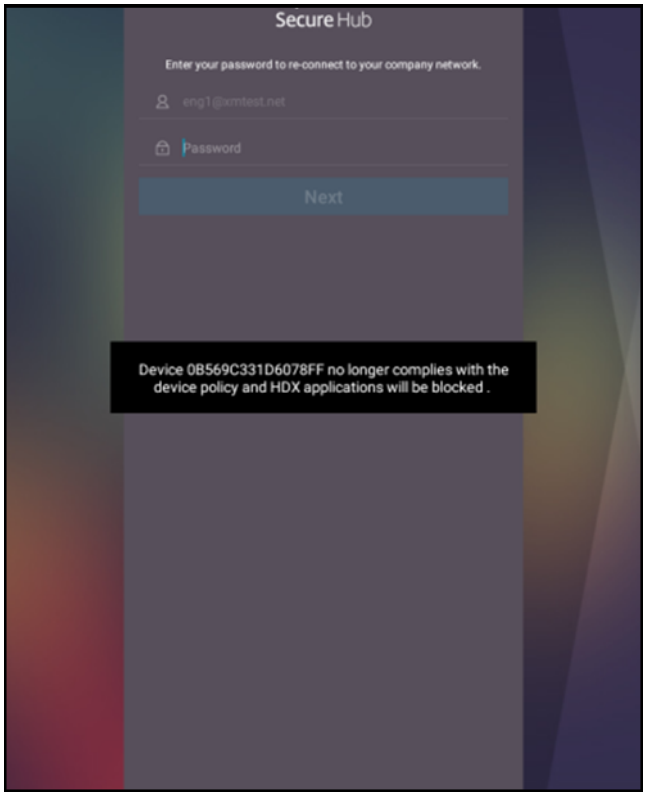
5. Dans la liste **Déclencheur**, sélectionnez **Propriété de l'appareil**, **Propriété utilisateur** ou **Nom de l'application installée**. SmartAccess ne prend pas en charge les déclencheurs d'événements.
6. Dans la liste **Action** :
   - Choisissez **Marquer l'appareil comme non conforme.**
   - Choisissez **Est**.
   - Choisissez **Vrai**.
   - Pour que l'action marque l'appareil comme non conforme dès que la condition de déclencheur est remplie, définissez le délai sur **0**.
7. Choisissez les groupes de mise à disposition XenMobile auxquels appliquer cette action.

8. Vérifiez le récapitulatif de l'action.
9. Cliquez sur **Suivant**, puis cliquez sur **Enregistrer**.

Lorsque l'appareil est marqué comme non conforme, les applications HDX ne s'affichent plus dans le magasin Secure Hub. L'utilisateur n'est plus abonné aux applications. Aucune notification n'est envoyée à l'appareil et rien dans le magasin Secure Hub n'indique que les applications HDX ont été disponibles.

Si vous souhaitez que les utilisateurs soient avertis lorsqu'un appareil est marqué comme non conforme, créez une notification, puis créez une action automatique pour envoyer cette notification.

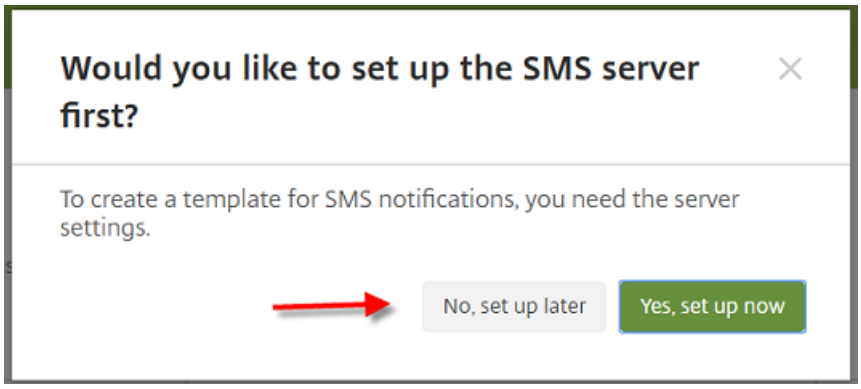
Cet exemple crée et envoie cette notification lorsqu'un appareil est marqué comme non conforme : « L'appareil (numéro de série ou numéro de téléphone) n'est plus conforme avec la stratégie et les applications HDX vont être bloquées. »



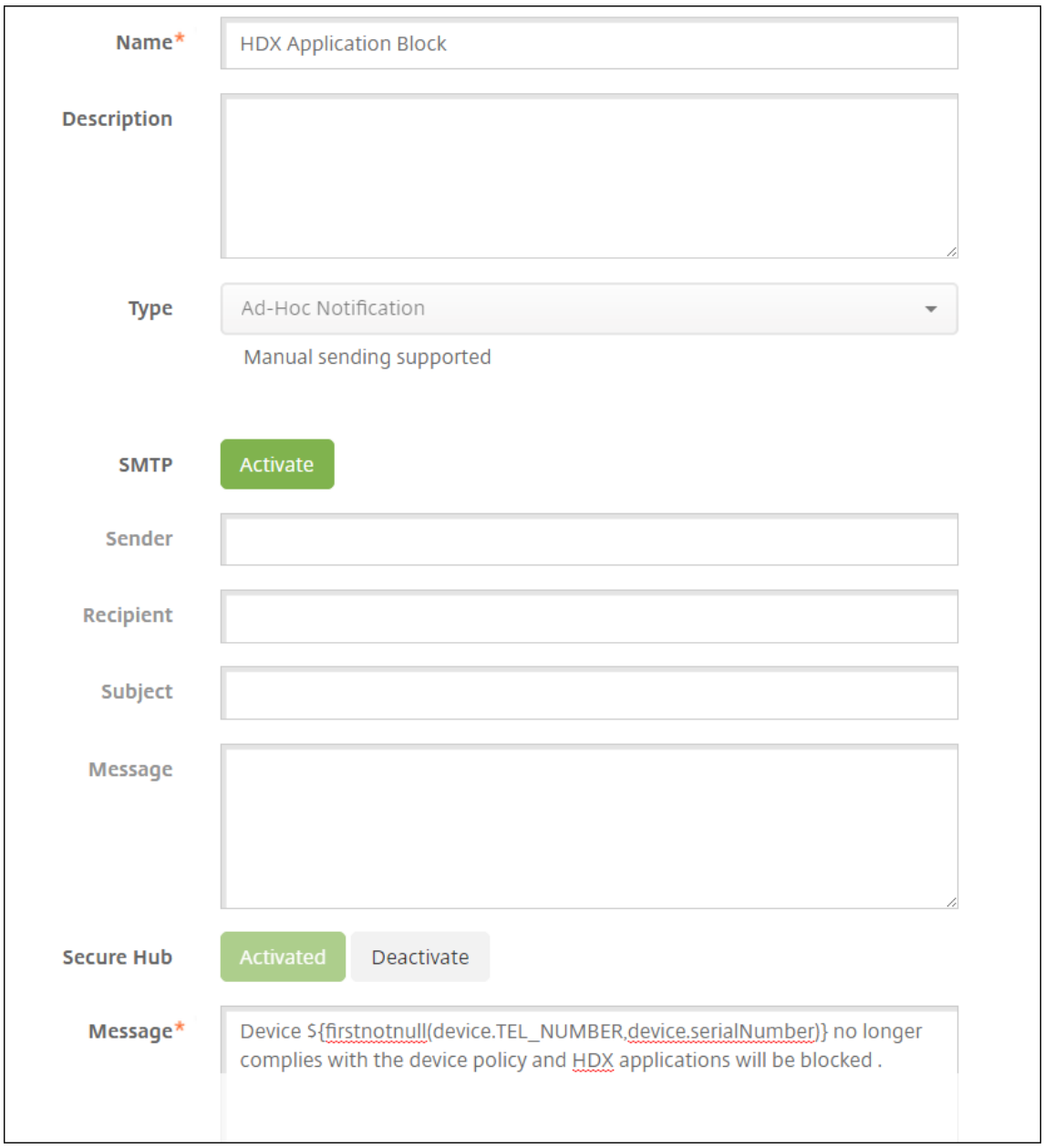
Créer la notification que les utilisateurs voient lorsqu'un appareil est marqué comme non conforme

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Modèles de notification**. La page **Modèles de notification** s'affiche.

3. Cliquez sur **Ajouter** pour ajouter un nouveau modèle de notification sur la page **Modèles de notification**.
4. Lorsque vous êtes invité à configurer le serveur SMS, cliquez sur **Non, configurer plus tard**.



5. Pour configurer ces paramètres :
   - **Nom :** Blocage application HDX
   - **Description :** notification de l'agent lorsque l'appareil n'est pas conforme
   - **Type :** notification ad hoc
   - **Secure Hub :** Activé
   - **Message :** L'appareil ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} n'est plus conforme avec la stratégie et les applications HDX vont être bloquées.



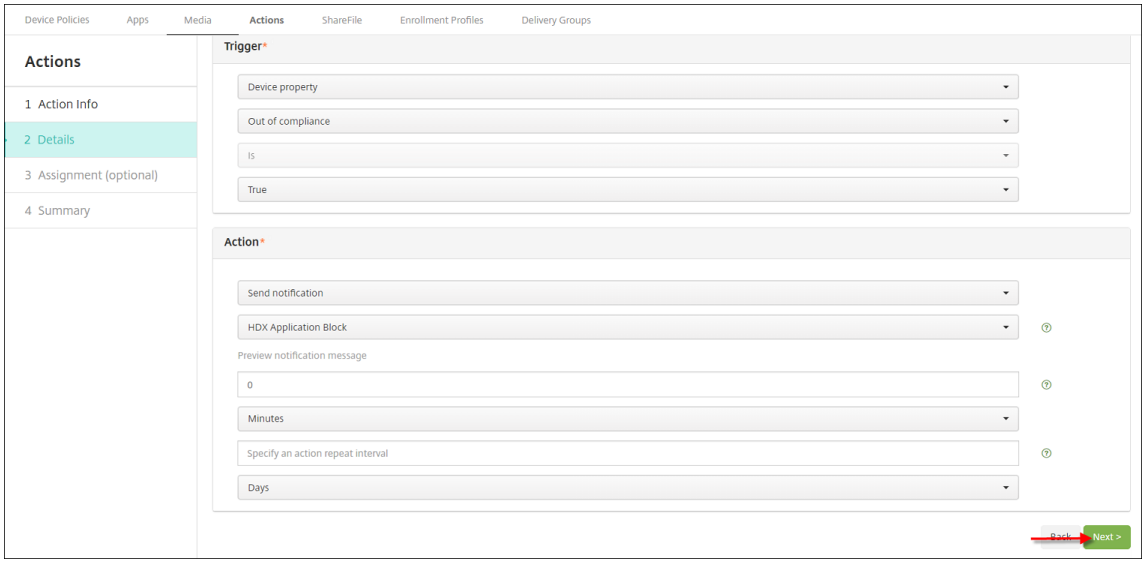
6. Cliquez sur **Enregistrer**.

Créer l'action qui envoie la notification lorsqu'un appareil est marqué comme non conforme

1. Dans la console XenMobile, cliquez sur **Configurer > Actions**. La page **Actions** s'affiche.
2. Cliquez sur **Ajouter** pour ajouter une action. La page **Informations sur l'action** s'affiche.
3. Sur la page **Informations sur l'action**, entrez un nom et une description pour l'action.
   - **Nom :** notification HDX bloquée

- **Description :** notification HDX bloquée car l'appareil n'est pas conforme

4. Cliquez sur **Suivant**. La page sur les **Détails de l'action** s'affiche.
5. Dans la liste **Déclencheur** :
   - Choisissez **Propriété de l'appareil**.
   - Choisissez **Non conforme.**
   - Choisissez **Est**.
   - Choisissez **Vrai**.



6. Dans la liste **Action**, spécifiez les actions qui se produisent lorsque le critère du déclencheur est rencontré :
   - Choisissez **Envoyer une notification**.
   - Choisissez **L'application HDX a bloqué la notification que vous avez créée**.
   - Choisissez **0**. Lorsque cette valeur est définie sur 0, la notification est envoyée dès que la condition du déclencheur est rencontrée.
7. Choisissez les groupes de mise à disposition XenMobile auxquels appliquer cette action. Dans cet exemple, choisissez **AllUsers**.
8. Vérifiez le récapitulatif de l'action.
9. Cliquez sur **Suivant**, puis cliquez sur **Enregistrer**.

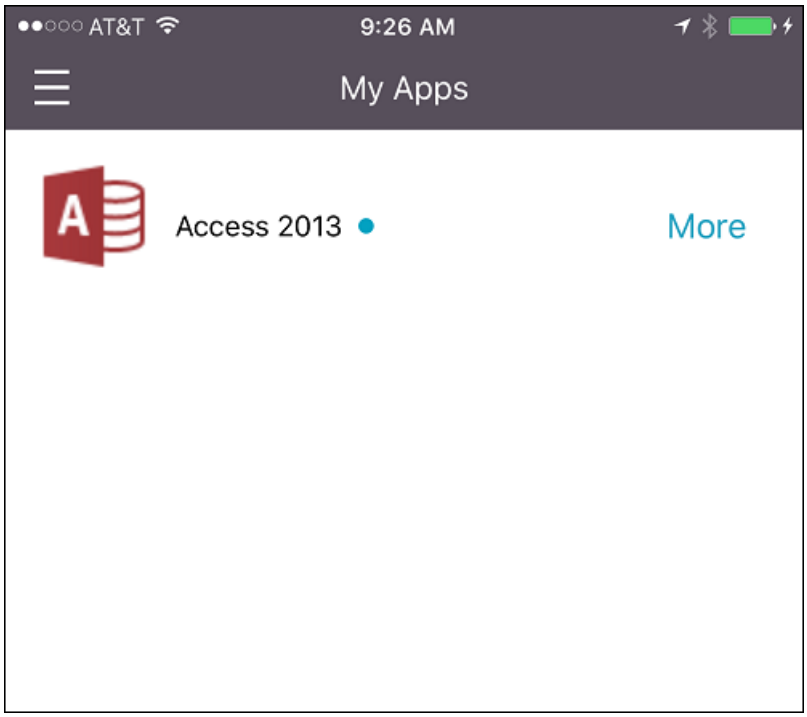
Pour de plus amples informations sur la configuration d'actions automatiques, consultez la section Actions automatisées.

Comment les utilisateurs peuvent rétablir l'accès aux applications HDX

Les utilisateurs peuvent de nouveau accéder aux applications HDX une fois que la conformité de l'appareil est rétablie :

1. Sur l'appareil, accédez au magasin Secure Hub pour actualiser les applications dans le magasin.
2. Accédez à l'application et touchez **Ajouter** à l'application.

Une fois que l'application est ajoutée, elle s'affiche dans Mes applications avec un point bleu, car il s'agit d'une application nouvellement installée.



Ajouter un média

January 10, 2022

Vous pouvez ajouter un média à XenMobile, afin de le déployer vers les appareils utilisateur. Vous pouvez utiliser XenMobile pour déployer Apple Books que vous obtenez via l'achat en volume d'Apple.

Une fois que vous avez configuré un compte d'achat en volume dans XenMobile, vos livres achetés et gratuits s'affichent dans **Configurer > Média**. À partir des pages **Média**, vous pouvez configurer les livres pour le déploiement vers les appareils iOS en choisissant des groupes de mise à disposition et en spécifiant les règles de déploiement.

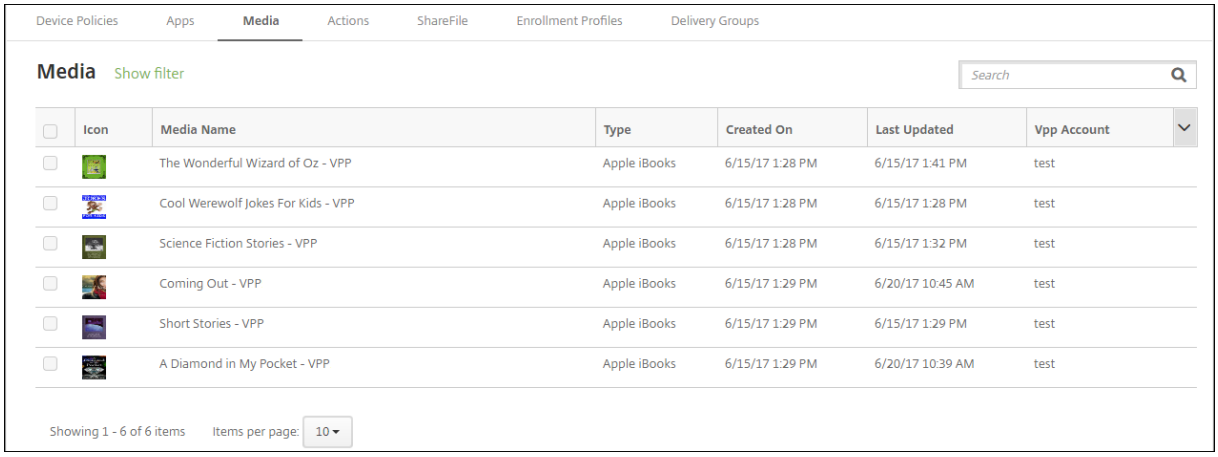
La première fois qu'un utilisateur reçoit un livre et accepte la licence d'achat en volume, les livres déployés s'installent sur l'appareil. Les livres s'affichent dans l'application Apple Books. Vous ne pouvez pas dissocier la licence du livre de l'utilisateur ou supprimer le livre de l'appareil. XenMobile installe les livres en tant que média obligatoire. Si un utilisateur supprime un livre installé de son appareil, le livre reste dans l'application Apple Book, prêt à être téléchargé.

Conditions préalables

- Appareils iOS
- Configurez l'achat en volume Apple dans XenMobile, comme décrit dans la section Achat en volume Apple.

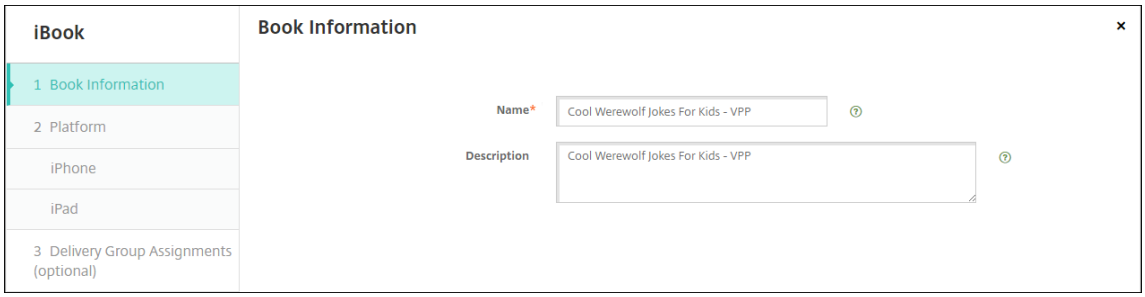
Configurer Apple Books

Les livres Apple Books obtenus via l'achat en volume s'affichent sur la page **Configurer > Média**.



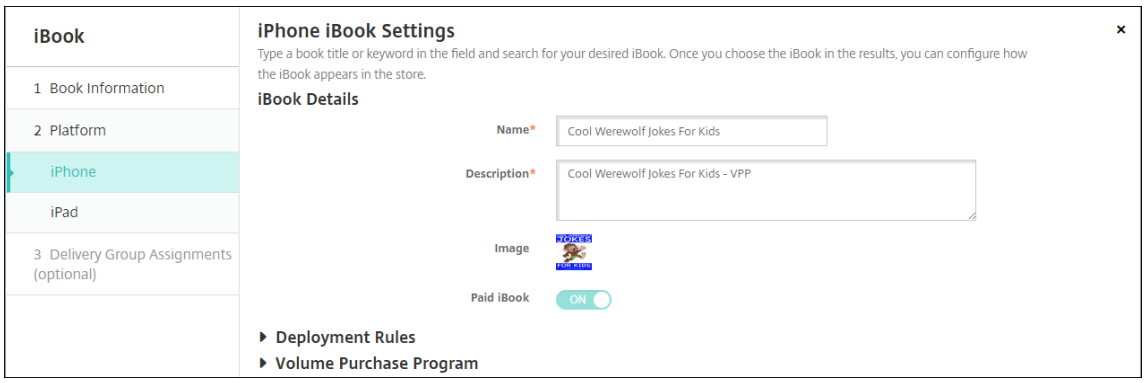
Pour configurer un livre Apple Book en vue du déploiement

1. Dans **Configurer > Média**, sélectionnez un livre et cliquez sur **Modifier**. La page **Informations sur le livre** s'affiche.

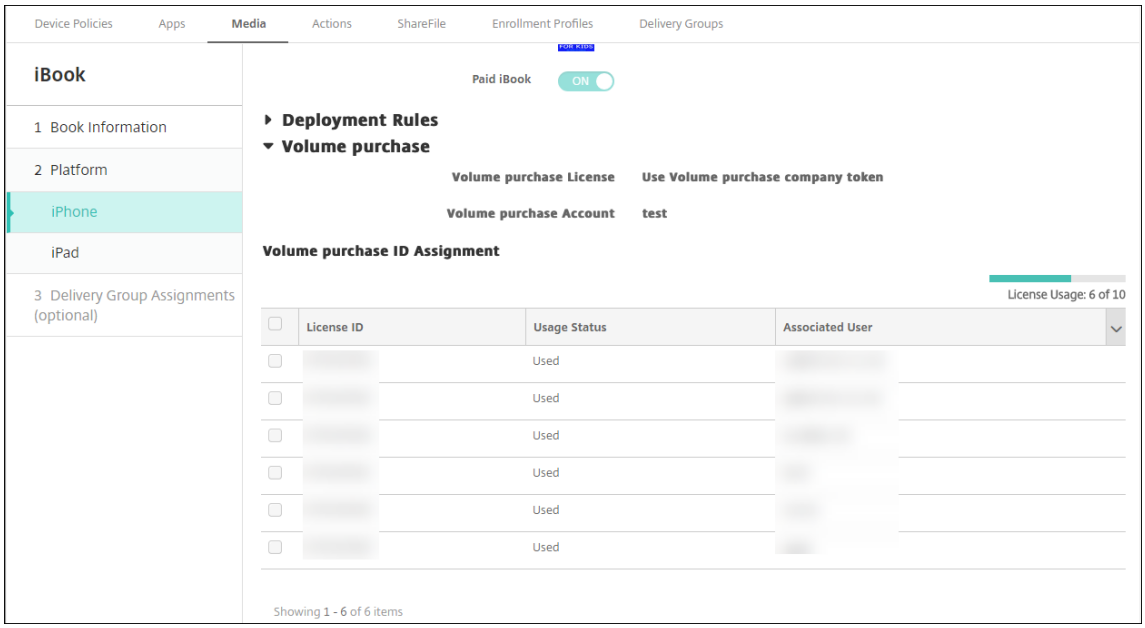


   Les champs **Nom** et **Description** n'apparaissent que dans les journaux et la console XenMobile.

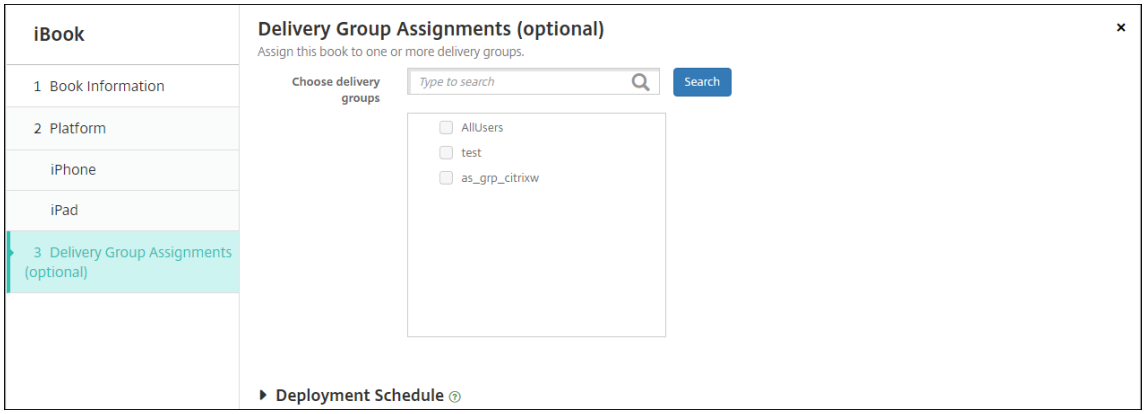
2. Dans les pages **Paramètres iBook iPhone** et **Paramètres iBook iPad** : vous pouvez modifier le nom et la description du livre, mais Citrix vous recommande de ne pas modifier ces paramètres. L'image est fournie à titre indicatif et n'est pas modifiable. **iBook payant** indique qu'un livre a été acheté via l'achat en volume.



Vous pouvez également spécifier des règles de déploiement ou afficher des informations relatives à l'achat en volume.

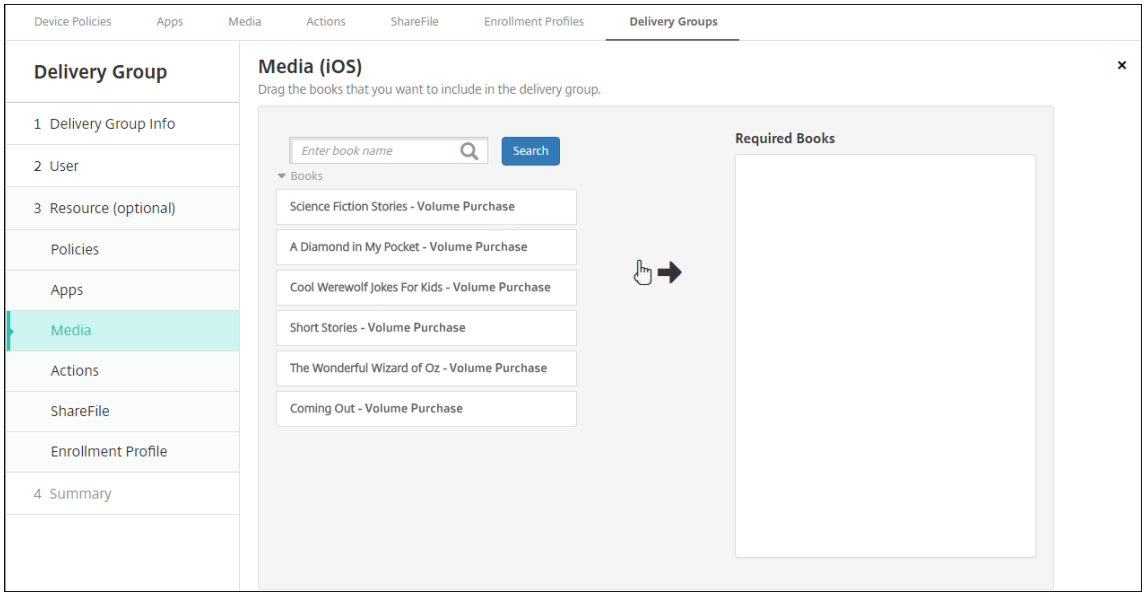


3. Si vous le souhaitez, attribuez le livre à des groupes de mise à disposition et définissez un calendrier de déploiement.

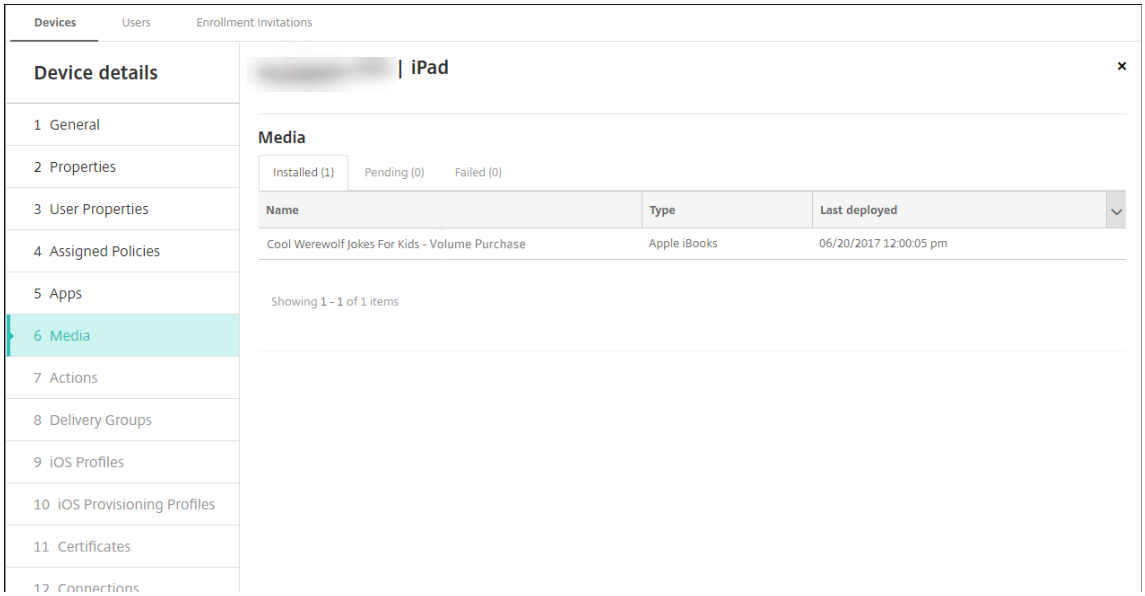


Vous pouvez également attribuer des livres à des groupes de mise à disposition à partir de

l'onglet **Média** sous **Configurer > Groupes de mise à disposition**. XenMobile prend en charge le déploiement de livres requis uniquement.

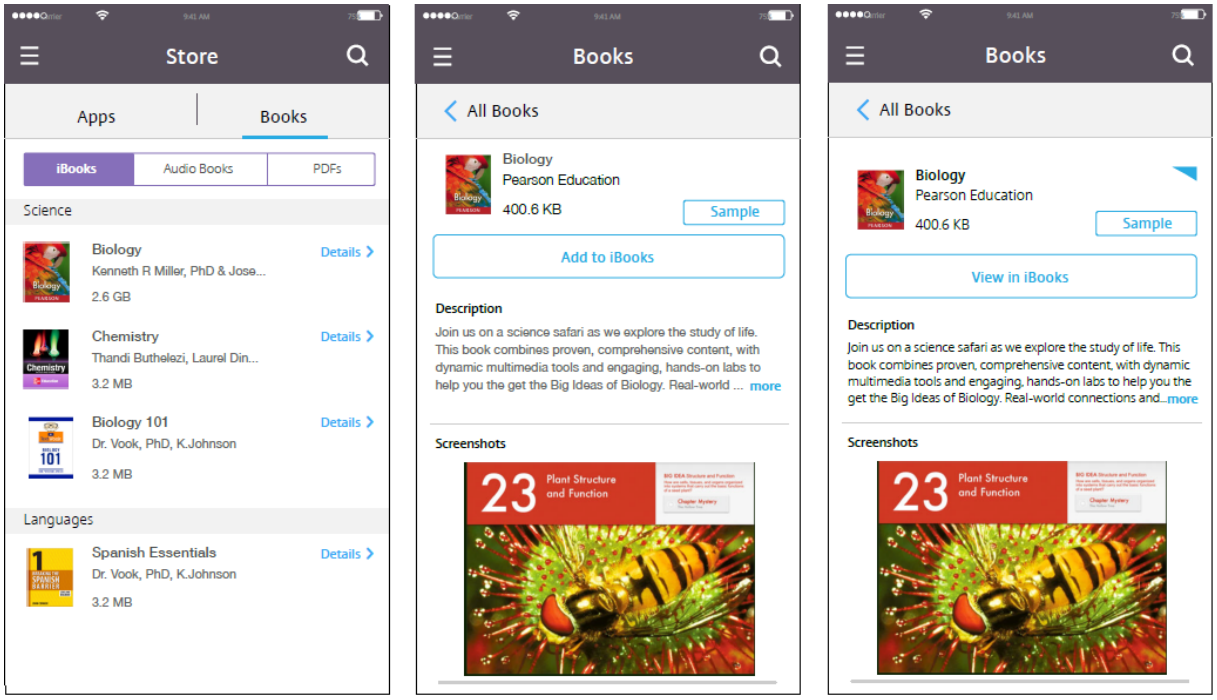


4. Utilisez l'onglet **Média** sous **Gérer > Appareils** pour afficher l'état du déploiement.



> **Remarque :**
>
> Sur la page **Configurer > Média**, si vous sélectionnez un livre et cliquez sur **Supprimer**, XenMobile supprime le livre de la liste. Toutefois, la prochaine fois que XenMobile se synchronise avec l'achat en volume Apple, le livre s'affiche de nouveau sur la liste sauf s'il a été supprimé de l'achat en volume. La suppression d'un livre de la liste ne le supprime pas des appareils.

Les livres s'affichent sur les appareils utilisateur comme illustré dans l'exemple suivant.



Déployer des ressources

January 10, 2022

La gestion et la configuration d'appareils impliquent généralement la création de ressources (stratégies, applications et média) et d'actions dans la console XenMobile, puis le packaging de ces dernières à l'aide de groupes de mise à disposition. L'ordre dans lequel XenMobile transmet les ressources et les actions dans un groupe de mise à disposition aux appareils est appelé ordre de déploiement. Cet article explique comment :

- Ajouter, gérer et déployer des groupes de mise à disposition
- Modifier l'ordre de déploiement des ressources et des actions dans les groupes de mise à disposition
- XenMobile détermine l'ordre de déploiement lorsqu'un utilisateur figure dans plusieurs groupes de mise à disposition qui comportent des stratégies conflictuelles ou en doublons.

Les groupes de mise à disposition définissent la catégorie d'utilisateurs pour lesquels vous déployez des combinaisons de stratégies, d'applications, de médias et d'actions. L'inclusion dans un groupe de mise à disposition est basée sur les caractéristiques des utilisateurs, telles que l'entreprise, le pays, le département, l'adresse et la fonction. Les groupes de mise à disposition vous permettent de mieux contrôler les personnes qui reçoivent les ressources et à quel moment. Vous pouvez déployer un groupe de mise à disposition à tout le monde ou à un groupe d'utilisateurs défini de manière plus précise.

Le déploiement sur un groupe de mise à disposition implique l'envoi d'une notification de type push à tous les utilisateurs équipés d'appareils iOS et Windows pris en charge. Les utilisateurs doivent appartenir au groupe de mise à disposition les invitant à se reconnecter à XenMobile. Vous pouvez réévaluer les appareils et déployer des applications, des stratégies, des médias et des actions dans le cadre d'un groupe de mise à disposition.

Pour les utilisateurs avec des appareils Android : s'ils sont déjà connectés, ils reçoivent les ressources immédiatement. Sinon, en fonction de leur stratégie de planification, ils reçoivent les ressources la prochaine fois qu'ils se connectent.

Le groupe de mise à disposition par défaut AllUsers est créé lorsque vous installez et configurez XenMobile. Il contient à tous les utilisateurs locaux et utilisateurs Active Directory. Vous ne pouvez pas supprimer le groupe AllUsers, mais vous pouvez le désactiver si vous ne souhaitez pas envoyer des ressources à tous les utilisateurs.

Ordre de déploiement

L'ordre de déploiement est la séquence dans laquelle XenMobile transmet les ressources aux appareils. L'ordre de déploiement s'applique uniquement aux appareils d'un groupe de mise à disposition dont le profil d'inscription est configuré pour la gestion des appareils (MDM).

Pour déterminer l'ordre de déploiement, XenMobile applique des filtres et des critères de contrôle, tels que des règles de déploiement et un calendrier de déploiement, aux ressources. Les ressources comprennent les stratégies, les applications, les actions et les groupes de mise à disposition. Avant d'ajouter des groupes de mise à disposition, considérez la façon dont les informations de cette section se rapportent à vos objectifs de déploiement.

Voici un résumé des concepts principaux liés à l'ordre de déploiement :

- **Ordre de déploiement :** séquence dans laquelle XenMobile transmet les ressources (stratégies, applications et médias) et actions à un appareil. L'ordre de déploiement de certaines stratégies, telles que les termes et conditions et l'inventaire logiciel, n'a aucun effet sur les autres ressources. L'ordre dans lequel les actions sont déployées n'a aucun effet sur les autres ressources, leur position est donc ignorée lorsque XenMobile déploie les ressources.
- **Règles de déploiement :** XenMobile utilise les règles de déploiement que vous spécifiez pour les propriétés d'appareil pour filtrer les stratégies, les applications, les médias, les actions et les groupes de mise à disposition. Par exemple, une règle de déploiement peut spécifier la distribution du paquetage de déploiement lorsqu'un nom de domaine correspond à une valeur particulière.
- **Calendrier de déploiement :** XenMobile utilise le calendrier de déploiement que vous spécifiez pour les actions, les applications, les médias et les stratégies pour contrôler le déploiement de ces éléments. Vous pouvez spécifier un déploiement immédiat, à une date et heure particulières, ou en fonction de conditions de déploiement.

Le tableau suivant présente les critères de filtre et de contrôle pour les différents types d'objet et de ressource. Les règles de déploiement sont basées sur les propriétés d'appareil.

Objet/Ressource	Plate-forme de l'appareil	Règle de déploiement	Une planification du déploiement	Utilisateur/groupes
Stratégie d'appareil	O	O	O	-
Application	O	O	O	-
Média	O	O	O	-
Action	-	O	O	-
Groupe de mise à disposition	-	O	-	O

Il est très probable que dans un environnement standard, plusieurs groupes de mise à disposition soient attribués à un seul utilisateur, avec les résultats possibles suivants :

- Des objets dupliqués existent dans les groupes de mise à disposition.
- Une stratégie spécifique est configurée différemment dans plus d'un groupe de mise à disposition qui est attribué à un utilisateur.

Lorsque l'une de ces situations se produit, XenMobile calcule un ordre de déploiement pour tous les objets qu'il doit délivrer sur un appareil ou pour lesquels il doit intervenir. Les étapes de calcul sont indépendantes de la plate-forme de l'appareil.

Étapes de calcul

1. Détermine tous les groupes de mise à disposition d'un utilisateur spécifique, en fonction des filtres de groupes, d'utilisateurs et des règles de déploiement.
2. Créez une liste ordonnée de toutes les ressources (applications, actions, médias et stratégies) dans les groupes de mise à disposition sélectionnés. La liste est basée sur les filtres de plate-forme d'appareil, les règles de déploiement et le calendrier de déploiement. L'algorithme utilisé est le suivant :
    a) Placez les ressources provenant des groupes de mise à disposition qui ont un ordre de déploiement défini par l'utilisateur avant les ressources provenant des groupes de mise à disposition ne disposant pas d'un ordre de déploiement. Le principe derrière ce raisonnement est décrit après ces étapes.

b) Pour départager les groupes de mise à disposition, classez les ressources provenant de groupes de mise à disposition par nom de groupe de mise à disposition. Par exemple, placez les ressources provenant du groupe de mise à disposition A avant les ressources provenant du groupe de mise à disposition B.

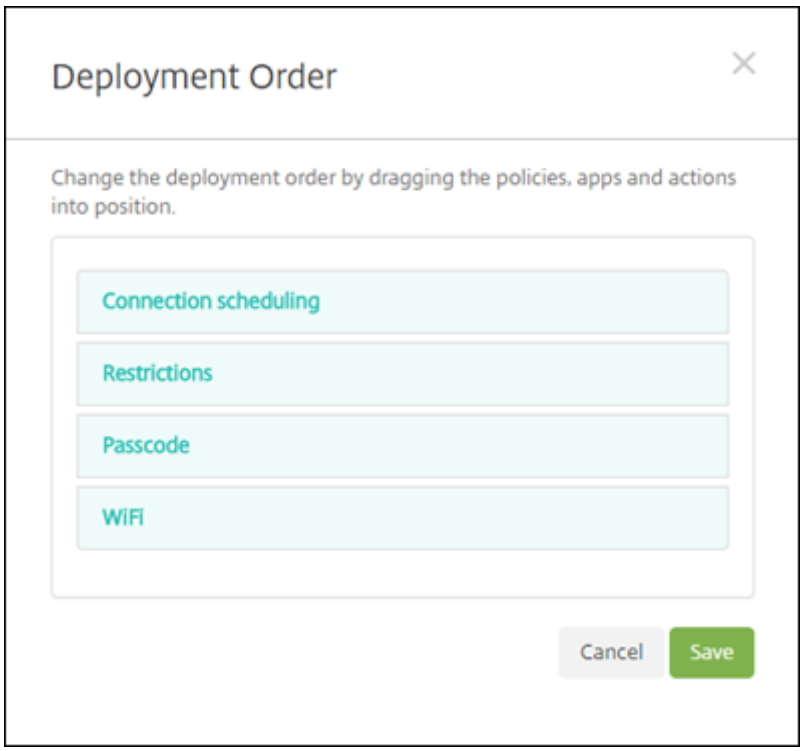
c) Tout en effectuant le tri, si un ordre de déploiement défini par un utilisateur est spécifié pour les ressources d'un groupe de mise à disposition, conservez cet ordre. Sinon, triez les ressources dans ce groupe de mise à disposition par nom de ressource.

d) Si la même ressource apparaît plus d'une fois, supprimez la ressource dupliquée.

Les ressources pour lesquelles un ordre a été défini par un utilisateur sont déployées avant les ressources pour lesquelles aucun ordre n'a été défini par un utilisateur. Une ressource peut exister dans plusieurs groupes de mise à disposition attribués à un utilisateur. Comme indiqué dans les étapes ci-dessus, l'algorithme de calcul supprime les ressources redondantes et met uniquement à disposition la première ressource de la liste. En supprimant les ressources en double de cette façon, XenMobile applique l'ordre défini par l'administrateur XenMobile.

Supposons par exemple que vous disposiez de deux groupes de mise à disposition comme suit :

- Groupe de mise à disposition, Gestionnaires de comptes 1 : avec un ordre **non spécifié** pour les ressources. Contient les stratégies **Wi-Fi** et **Code secret**.
- Groupe de mise à disposition, Gestionnaires de comptes 2 : avec un ordre **spécifié** pour les ressources. Contient les stratégies **Planification de connexion**, **Restrictions**, **Code secret** et **Wi-Fi**. Dans ce cas, vous souhaitez mettre à disposition la stratégie **Code secret** avant la stratégie **Wi-Fi**.



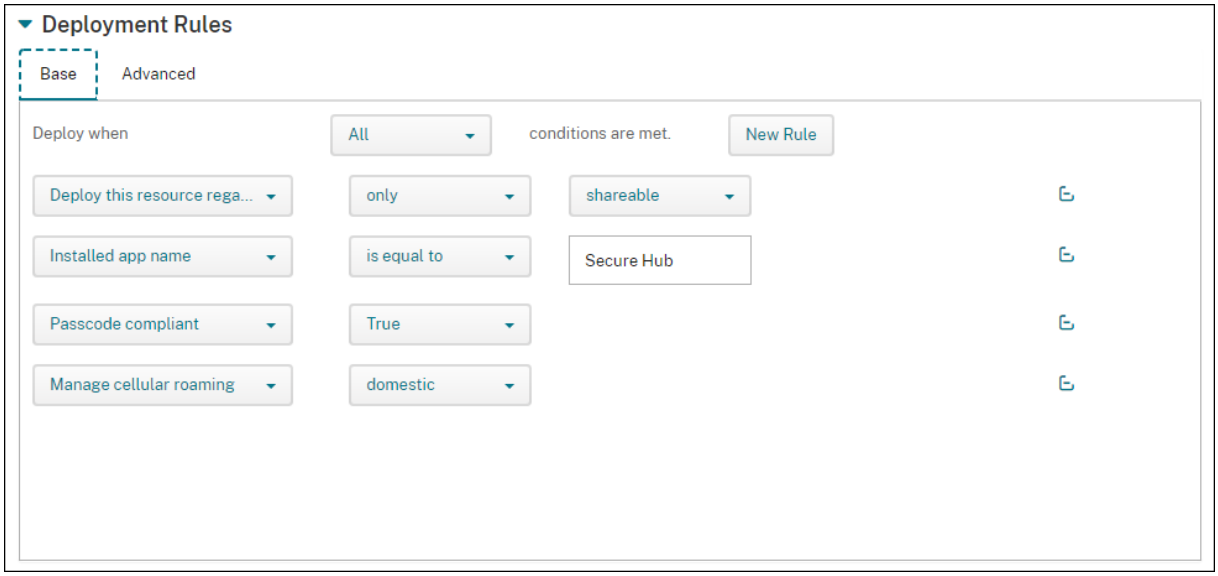
Si l'algorithme de calcul classait uniquement les groupes de déploiement par nom, XenMobile réaliserait le déploiement dans cet ordre, en commençant par le groupe de mise à disposition Gestionnaires de comptes 1 : **Wi-Fi**, **Code secret**, **Planification de connexion** et **Restrictions**. XenMobile ignorerait **Code secret** et **Wi-Fi**, des doublons du groupe de mise à disposition Gestionnaires de comptes 2.

Cependant, le groupe Gestionnaires de comptes 2 a un ordre de déploiement spécifié par l'administrateur. Par conséquent, l'algorithme de calcul place les ressources provenant du groupe de mise à disposition Gestionnaires de comptes 2 dans une position plus élevée dans la liste que les ressources de l'autre groupe de mise à disposition. Par conséquent, XenMobile déploie les stratégies dans cet ordre : **Planification de connexion**, **Restrictions**, **Code secret** et **Wi-Fi**. XenMobile ignore les stratégies **Wi-Fi** et **Code secret** du groupe de mise à disposition Gestionnaires de comptes 1, car elles sont dupliquées. Par conséquent, cet algorithme respecte l'ordre spécifié par l'administrateur XenMobile.

Règles de déploiement

Configurez des règles de déploiement pour mettre des ressources à disposition uniquement lorsque des conditions spécifiques existent. Vous pouvez configurer des règles de déploiement de base ou avancées.

Lorsque vous ajoutez une règle de déploiement à l'aide de l'éditeur de règles de base, sélectionnez d'abord quand déployer la ressource.

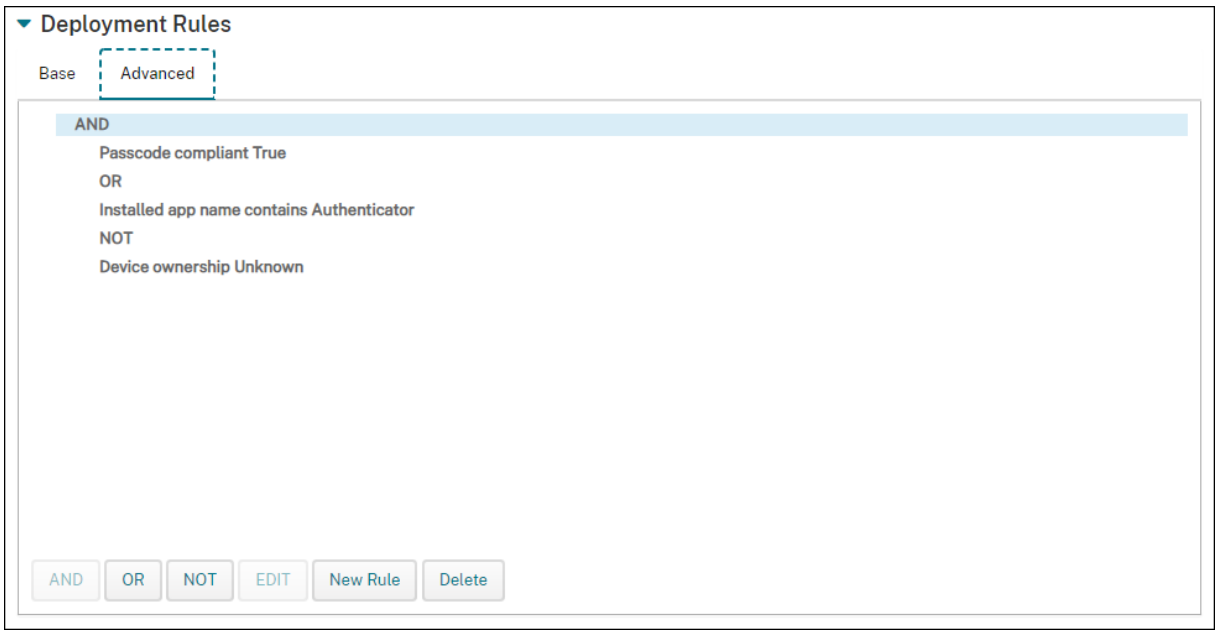


- **Toutes :** mettez la ressource à disposition lorsque l'utilisateur ou l'appareil remplit toutes les conditions que vous configurez.
- **Une :** mettez la ressource à disposition lorsque l'utilisateur ou l'appareil remplit au moins l'une des conditions que vous configurez.

Cliquez sur **Nouvelle règle** pour ajouter une condition. Les règles varient en fonction de la ressource déployée et de la plate-forme pour laquelle vous configurez la ressource. Il existe plusieurs types de règles. Vous pouvez choisir de déployer la ressource :

- uniquement lorsque la propriété sélectionnée existe ou sauf lorsque la propriété sélectionnée existe ;
- lorsque la propriété correspond exactement au texte que vous avez entré, lorsque la propriété contient le texte que vous avez entré ou lorsque la propriété ne correspond pas au texte que vous avez entré ;
- lorsque l'appareil ou l'utilisateur est conforme à la propriété sélectionnée ou n'est pas conforme à la propriété sélectionnée ;
- lorsque les propriétés de l'appareil ou de l'utilisateur correspondent à la condition que vous sélectionnez dans une liste prédéfinie.

Utilisez l'éditeur de règles avancées pour créer des règles de déploiement plus complexes. Vous pouvez sélectionner d'autres règles et vous pouvez combiner différents opérateurs logiques booléens lors de la création d'une règle avancée.

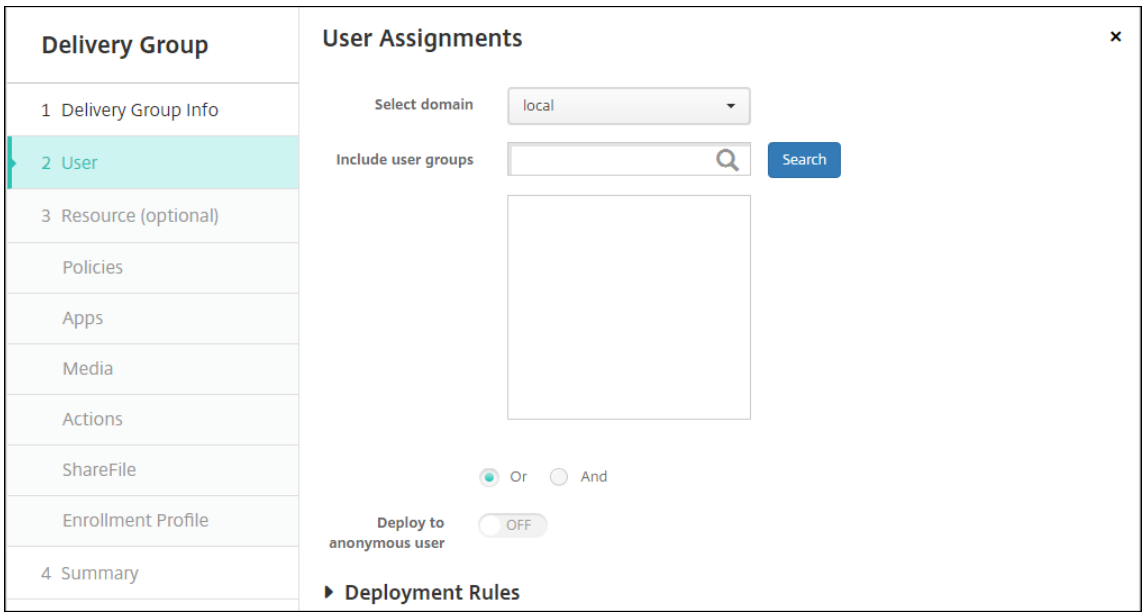


Pour ajouter un groupe de mise à disposition

Citrix recommande de créer des groupes de mise à disposition avant de créer des stratégies d'appareil et des profils d'inscription.

1. Dans la console, cliquez sur **Configurer > Groupes de mise à disposition**.
2. Sur la page **Groupes de mise à disposition**, cliquez sur **Ajouter**.
3. Dans la page **Informations sur le groupe de mise à disposition**, tapez un nom et une description pour le groupe de mise à disposition, puis cliquez sur **Suivant**.

   Si un utilisateur appartient à plusieurs groupes de mise à disposition qui ont des profils d'inscription différents, le nom du groupe de mise à disposition détermine le profil d'inscription utilisé. XenMobile sélectionne le groupe de mise à disposition qui apparaît en dernier dans une liste alphabétique des groupes de mise à disposition. Pour plus d'informations, voir Profils d'inscription.
4. Sur la page **Attributions utilisateur**, indiquez comment gérer les attributions utilisateur du groupe de mise à disposition.



> **Important :**
>
> Vous ne pouvez pas modifier le paramètre **Gérer les attributions d'utilisateurs** après la création du groupe d'utilisateurs.

- **Sélectionner un domaine :** sélectionnez le domaine à partir duquel choisir les utilisateurs dans la liste.
- **Inclure des groupes d'utilisateurs :** effectuez l'une des opérations suivantes :
  - Dans la liste des groupes d'utilisateurs, cliquez sur les groupes que vous souhaitez ajouter. Les groupes sélectionnés s'affichent dans la liste **Groupes d'utilisateurs sélectionnés**.
  - Cliquez sur **Rechercher** pour afficher une liste de tous les groupes d'utilisateurs dans le domaine sélectionné.
  - Tapez un nom de groupe complet ou partiel dans la zone de recherche, puis cliquez sur **Rechercher** pour limiter la liste des groupes d'utilisateurs.

  Pour supprimer un groupe d'utilisateurs de la liste **Groupes d'utilisateurs sélectionnés**, effectuez l'une des opérations suivantes :

  - Dans la liste **Groupes d'utilisateurs sélectionnés**, cliquez sur le **X** en regard de chaque groupe que vous souhaitez supprimer.
  - Cliquez sur **Rechercher** pour afficher une liste de tous les groupes d'utilisateurs dans le domaine sélectionné. Parcourez la liste et décochez la case à cocher en regard de chaque groupe à supprimer.
  - Tapez un nom de groupe complet ou partiel dans la zone de recherche, puis cliquez sur **Rechercher** pour limiter la liste des groupes d'utilisateurs. Parcourez la liste et décochez la case à cocher en regard de chaque groupe à supprimer.

- **Ou/Et :** sélectionnez cette option pour spécifier si les utilisateurs peuvent appartenir à n'importe quel groupe (Ou) ou s'ils doivent figurer dans tous les groupes (Et) pour que la ressource puisse leur être déployée.
- **Déployer auprès d'un utilisateur anonyme :** sélectionnez cette option si vous voulez déployer auprès d'utilisateurs non authentifiés dans le groupe de mise à disposition. Les utilisateurs non authentifiés sont des utilisateurs que vous n'avez pas réussi à authentifier, mais dont les appareils sont autorisés à se connecter à XenMobile.

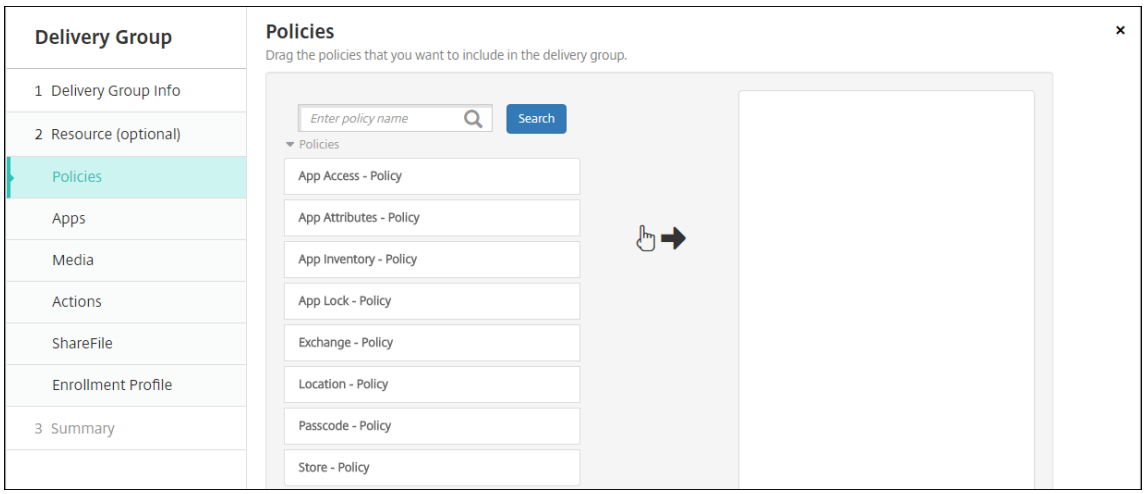
5. Configurez les règles de déploiement.
6. Cliquez sur **Suivant**. La page **Ressources du groupe de mise à disposition** s'affiche. Vous pouvez éventuellement ajouter des stratégies, des applications ou des actions pour le groupe de mise à disposition. Pour ignorer cette étape, sous **Groupe de mise à disposition**, cliquez sur **Résumé** pour afficher un résumé de la configuration du groupe de mise à disposition.

   Pour ignorer une ressource, sous **Ressources (facultatif)**, cliquez sur la ressource que vous souhaitez ajouter et suivez les étapes pour cette ressource.

Pour ajouter des stratégies

1. Pour chaque stratégie que vous voulez ajouter, procédez comme suit :
   - Parcourez la liste des stratégies disponibles pour trouver la stratégie que vous souhaitez ajouter.
   - Ou pour limiter la liste des stratégies, entrez un nom de stratégie complet ou partiel dans la zone de recherche et cliquez sur **Rechercher**.
   - Cliquez sur la stratégie que vous souhaitez ajouter et faites-la glisser dans la zone de droite.

   Pour supprimer une stratégie, cliquez sur le **X** en regard du nom de la stratégie dans la zone de droite.



2. Cliquez sur **Suivant**. La page **Applications** s'affiche.

Pour ajouter des applications

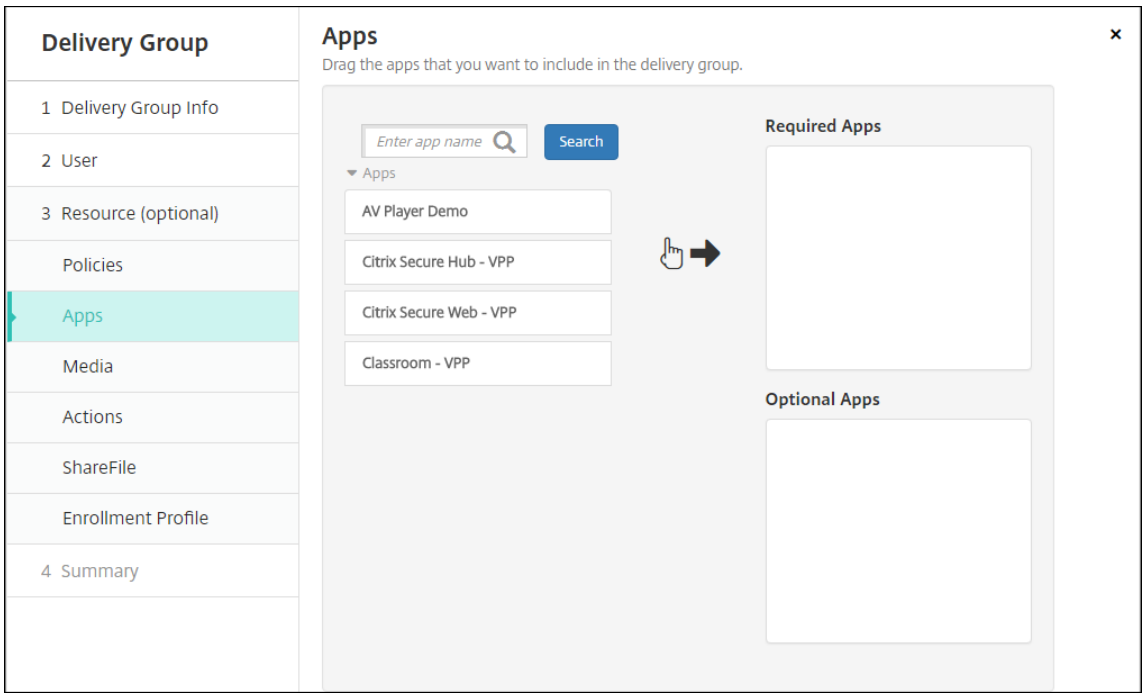
1. Pour chaque application que vous souhaitez ajouter, procédez comme suit :

    - Parcourez la liste des applications disponibles pour trouver l'application que vous souhaitez ajouter.
    - Ou pour limiter la liste des applications, entrez un nom d'application complet ou partiel dans la zone de recherche et cliquez sur **Rechercher**.
    - Cliquez sur l'application que vous souhaitez ajouter et faites-la glisser dans la zone **Applications requises** ou **Applications facultatives**.

    Pour les applications marquées comme requises, les utilisateurs peuvent recevoir les mises à jour plus rapidement dans certaines situations, par exemple :

    - Vous chargez une nouvelle application et la marquez comme requise.
    - Vous marquez une application existante comme requise.
    - Un utilisateur supprime une application requise.
    - Une mise à jour de Secure Hub est disponible.

    Pour plus d'informations sur le déploiement forcé des applications obligatoires, notamment sur la façon d'activer la fonctionnalité, voir À propos des applications obligatoires et facultatives.

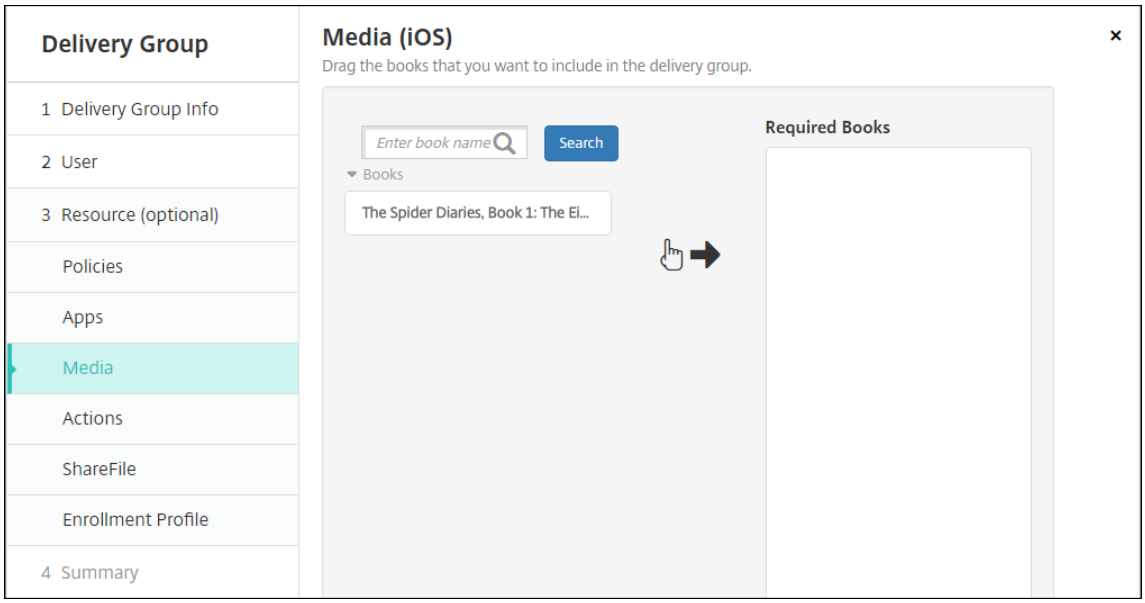


    Pour supprimer une application, cliquez sur le **X** en regard du nom de l'application dans la zone de droite.

2. Cliquez sur **Suivant**. La page **Média** s'ouvre.

Pour ajouter un média

1. Pour chaque livre que vous souhaitez ajouter, procédez comme suit :
    - Parcourez la liste des livres disponibles pour trouver le livre que vous souhaitez ajouter.
    - Ou pour limiter la liste des livres, entrez un nom de livre complet ou partiel dans la zone de recherche et cliquez sur **Rechercher**.
    - Cliquez sur le livre que vous souhaitez ajouter et faites-le glisser dans la zone **Livres obligatoires**.



Pour les livres marquées comme requis, les utilisateurs reçoivent les mises à jour plus rapidement dans certaines situations, par exemple :

- Vous chargez un nouveau livre et le marquez comme requis.
- Vous marquez un livre existant comme requis.
- Un utilisateur supprime un livre requis.
- Une mise à jour de Secure Hub est disponible.

Pour supprimer un livre, cliquez sur le **X** en regard du nom du livre dans la zone de droite.

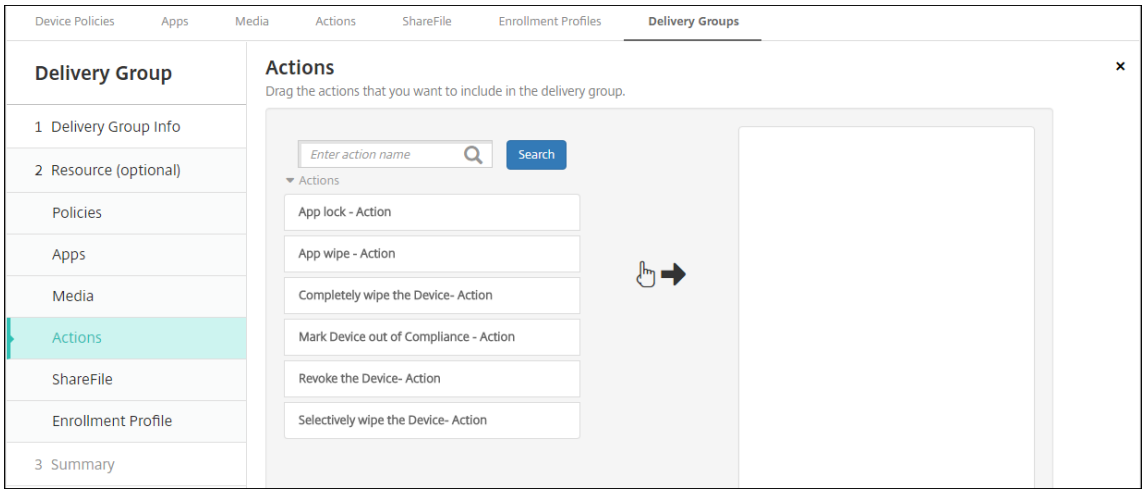
2. Cliquez sur **Suivant**. La page **Actions** s'affiche.

Pour ajouter des actions

1. Pour chaque action que vous voulez ajouter, procédez comme suit :
    - Parcourez la liste des actions disponibles pour trouver l'action que vous souhaitez ajouter.
    - Ou pour limiter la liste des actions, entrez un nom d'action complet ou partiel dans la zone de recherche et cliquez sur **Rechercher**.

- Cliquez sur l'action que vous souhaitez ajouter et faites-la glisser dans la zone de droite.

Pour supprimer une action, cliquez sur le **X** en regard du nom de l'action dans la zone de droite.

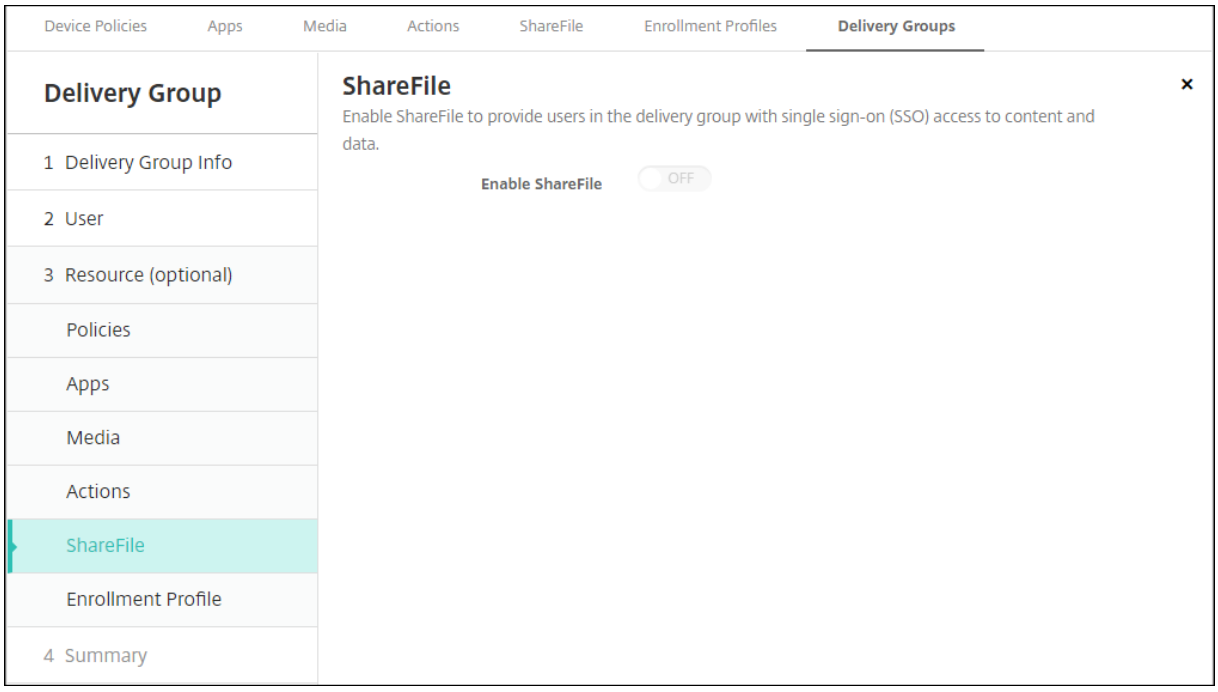


2. Cliquez sur **Suivant**. La page **ShareFile** s'affiche.

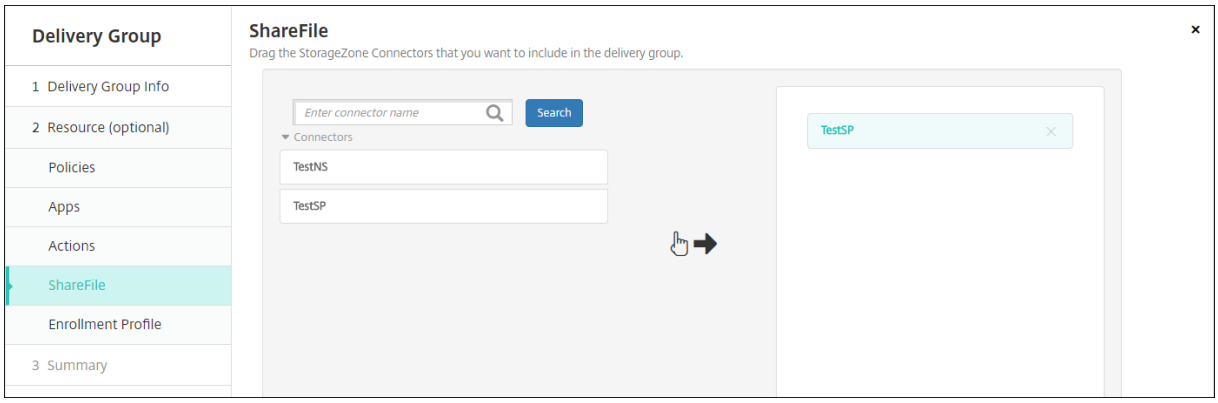
Pour appliquer la configuration de Content Collaboration

La page Content Collaboration diffère si avez configuré XenMobile (**Configurer > ShareFile**) pour les comptes Enterprise ou pour les connecteurs StorageZone.

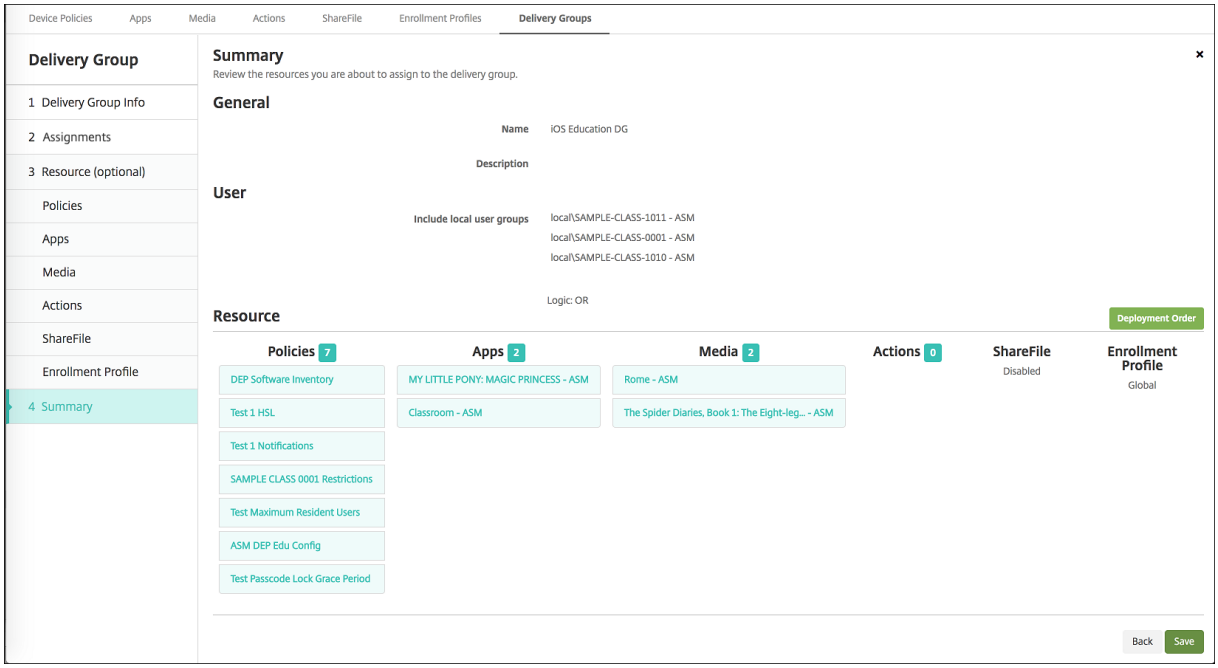
Si vous avez configuré des comptes Enterprise pour les utiliser avec XenMobile : définissez **Activer ShareFile** sur **Activé** pour fournir au groupe de mise à disposition l'accès avec authentification unique au contenu et aux données Content Collaboration.



Si vous avez configuré des connecteurs StorageZone à utiliser avec XenMobile, sélectionnez les connecteurs StorageZone à inclure dans le groupe de mise à disposition.

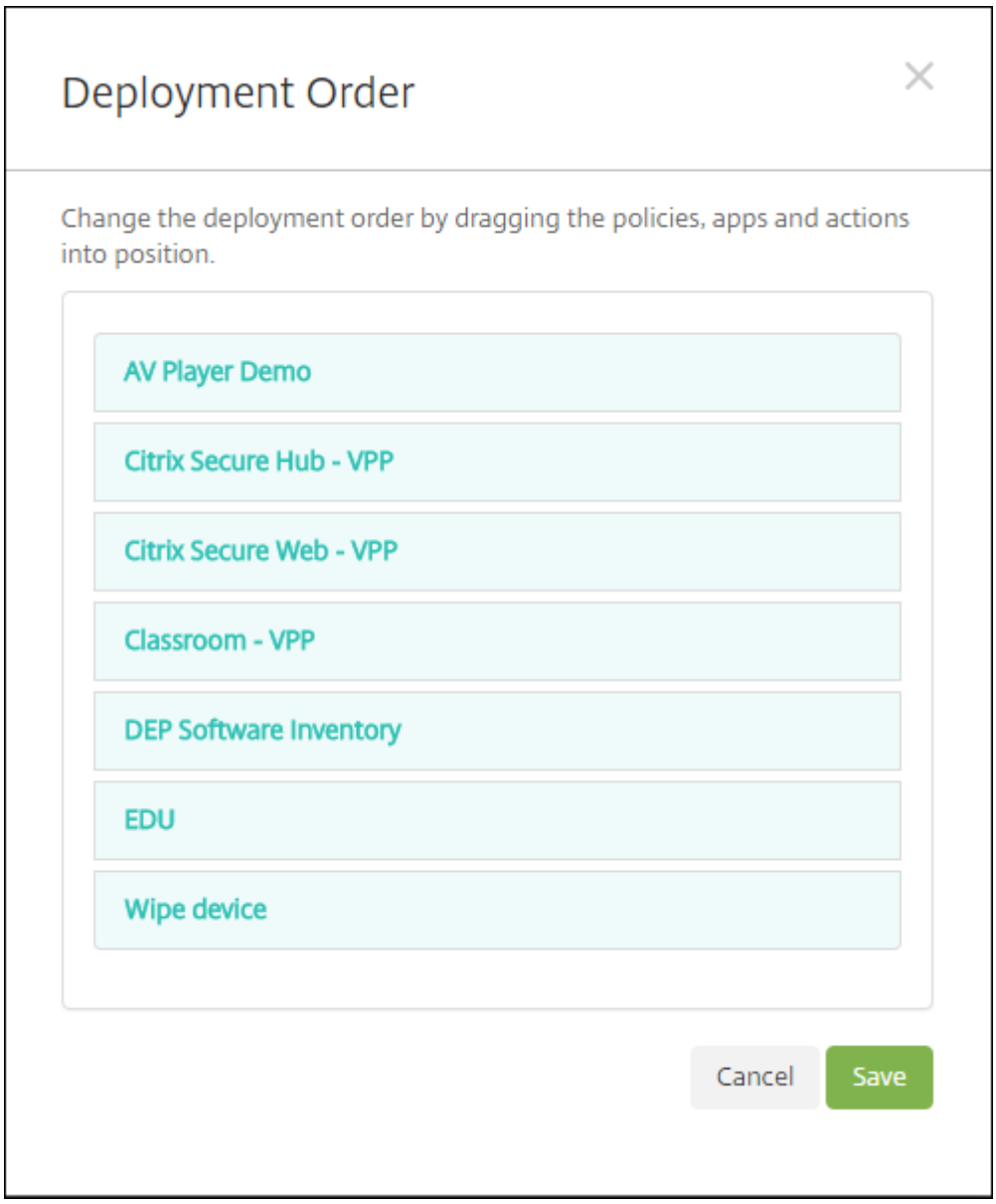


Pour consulter les options configurées et modifier l'ordre de déploiement



Sur la page **Résumé**, vous pouvez vérifier les options que vous avez configurées pour le groupe de mise à disposition et modifier l'ordre de déploiement des ressources. La page Résumé affiche vos ressources par catégorie. La page Résumé ne pas reflète pas l'ordre de déploiement.

1. Cliquez sur **Précédent** pour revenir sur les pages précédentes pour modifier la configuration le cas échéant.
2. Cliquez sur **Ordre de déploiement** pour afficher l'ordre de déploiement ou réorganiser l'ordre de déploiement. La boîte de dialogue **Ordre de déploiement** s'affiche.



3. Cliquez sur une ressource et faites-la glisser vers l'emplacement à partir duquel vous voulez la déployer. Lorsque vous modifiez l'ordre de déploiement, XenMobile déploie les ressources dans la liste de haut en bas.
4. Cliquez sur **Enregistrer** pour enregistrer l'ordre de déploiement.
5. Cliquez sur **Enregistrer** pour enregistrer le groupe de mise à disposition.

Pour modifier un groupe de mise à disposition

Vous ne pouvez pas modifier le nom d'un groupe de mise à disposition existant. Pour mettre à jour les autres paramètres : accédez à **Configurer > Groupes de mise à disposition**, sélectionnez le groupe que vous souhaitez modifier, puis cliquez sur **Modifier**.

Pour activer et désactiver le groupe de mise à disposition AllUsers

AllUsers est le seul groupe de mise à disposition que vous pouvez activer ou désactiver.

Sur la page **Groupes de mise à disposition**, sélectionnez le groupe de mise à disposition AllUsers en sélectionnant la case à cocher en regard de **AllUsers** ou en cliquant sur la ligne contenant AllUsers. Procédez ensuite comme suit :

- Cliquez sur **Désactiver** pour désactiver le groupe de mise à disposition AllUsers. Cette commande est uniquement disponible si AllUsers est activé (paramètre par défaut). **Désactivé** s'affiche sous le titre **Désactivé** dans le tableau des groupes de mise à disposition.
- Cliquez sur **Activer** pour activer le groupe de mise à disposition AllUsers. Cette commande est uniquement disponible si AllUsers est désactivé. **Désactivé** disparaît du titre **Désactivé** dans le tableau des groupes de mise à disposition.

Pour déployer sur des groupes de mise à disposition

Le déploiement sur un groupe de mise à disposition implique l'envoi d'une notification de type push à tous les utilisateurs équipés d'appareils iOS, Windows Phone et Windows Tablet. Les utilisateurs doivent appartenir au groupe de mise à disposition les invitant à se reconnecter à XenMobile. Cela permet de réévaluer les appareils et de déployer des applications, des stratégies et des actions.

Pour les utilisateurs avec d'autres plates-formes d'appareil : si ces appareils sont déjà connectés à XenMobile, ils reçoivent les ressources immédiatement. Sinon, en fonction de leur stratégie de planification, ils reçoivent les ressources la prochaine fois qu'ils se connectent.

Pour mettre à jour les applications affichées dans la liste des applications disponibles dans le XenMobile Store sur les appareils Android des utilisateurs : vous devez d'abord déployer une stratégie d'inventaire des applications sur les appareils des utilisateurs.

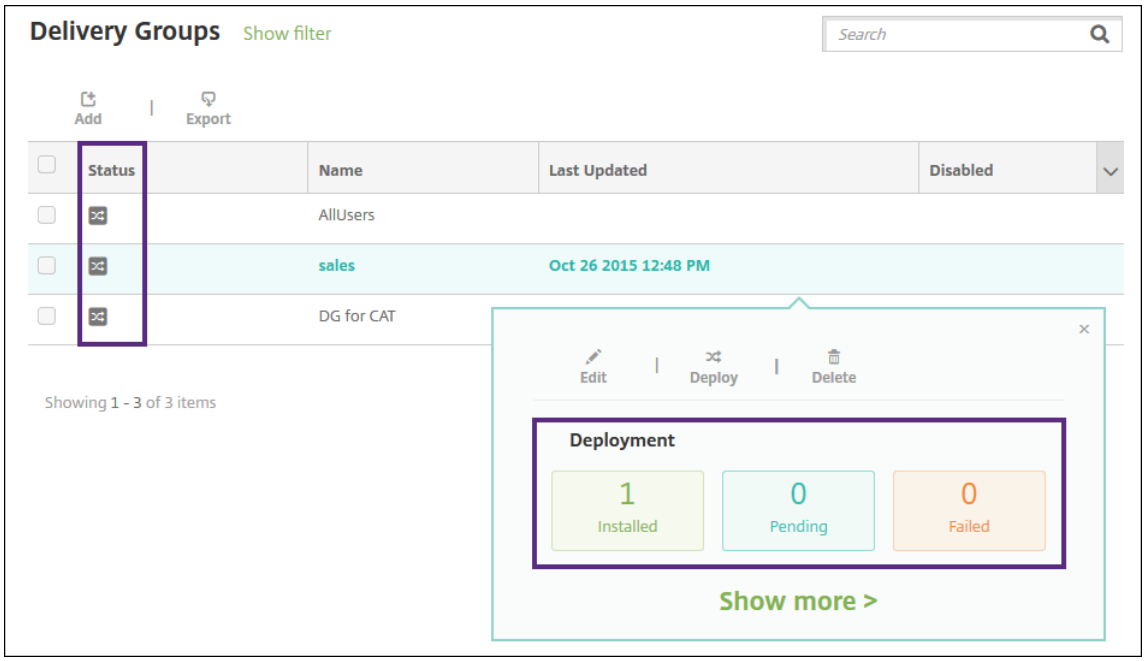
1. Sur la page **Groupes de mise à disposition**, effectuez l'une des opérations suivantes :
    - Pour déployer sur plus d'un groupe de mise à disposition à la fois, sélectionnez les cases à cocher en regard des groupes sur lesquels vous voulez déployer.
    - Pour déployer sur un seul groupe de mise à disposition, sélectionnez la case à cocher en regard de son nom ou cliquez sur la ligne contenant son nom.
2. Cliquez sur **Déployer**.

    En fonction de la manière dont vous sélectionnez un groupe de mise à disposition, la commande **Déployer** apparaît au-dessus ou à droite du groupe de mise à disposition.

    Vérifiez que les groupes auprès desquels vous souhaitez déployer des applications, des stratégies et des actions sont répertoriés et cliquez sur **Déployer**. Les applications, stratégies et actions sont déployées auprès des groupes sélectionnés en fonction de la plate-forme d'appareil et de la stratégie de planification.

Vous pouvez vérifier l'état du déploiement sur la page **Groupes de mise à disposition** de l'une des façons suivantes :

- Examinez l'icône de déploiement sous l'en-tête **État** pour le groupe de mise à disposition, qui indique les échecs de déploiement.
- Cliquez sur la ligne contenant le groupe de mise à disposition pour afficher une superposition indiquant si les déploiements sont **installés**, **en attente** ou qu'ils ont **échoué**.



Pour supprimer des groupes de mise à disposition

vous ne pouvez pas supprimer le groupe de mise à disposition AllUsers, mais vous pouvez le désactiver si vous ne souhaitez pas envoyer des ressources à tous les utilisateurs.

1. Sur la page **Groupes de mise à disposition**, effectuez l'une des opérations suivantes :
   - Pour supprimer plus d'un groupe de mise à disposition à la fois, sélectionnez les cases à cocher en regard des groupes que vous voulez supprimer.
   - Pour supprimer sur un seul groupe de mise à disposition, sélectionnez la case à cocher en regard de son nom ou cliquez sur la ligne contenant son nom.
2. Cliquez sur **Supprimer**. La boîte de dialogue **Supprimer** s'affiche.

   En fonction de la manière dont vous sélectionnez un groupe de mise à disposition, la commande **Supprimer** apparaît au-dessus ou à droite du groupe de mise à disposition.

   > **Important :**
   >
   > Vous ne pouvez pas annuler une suppression.

3. Cliquez sur **Supprimer**.

Pour exporter le tableau des groupes de mise à disposition

1. Cliquez sur le bouton **Exporter** au-dessus du tableau **Groupes de mise à disposition**. XenMobile extrait les informations du tableau **Groupes de mise à disposition** et les convertit en fichier .csv.
2. Ouvrez ou enregistrez le fichier .csv en suivant les étapes habituelles de votre navigateur. Vous pouvez également annuler l'opération.

Macros

January 10, 2022

XenMobile fournit des macros qui permettent de renseigner les données de propriété utilisateur ou appareil dans le champ de texte des éléments suivants :

- Stratégies
- Notifications
- Modèles d'inscription
- Actions automatisées
- Demandes de signature de certificat de fournisseurs d'identité

XenMobile remplace une macro avec les valeurs utilisateur ou système correspondantes. Par exemple, vous pouvez pré-remplir la valeur boîte aux lettres pour un utilisateur dans un seul profil Exchange pour des milliers d'utilisateurs.

Syntaxe des macros

Une macro peut prendre la forme suivante :

- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)] }`

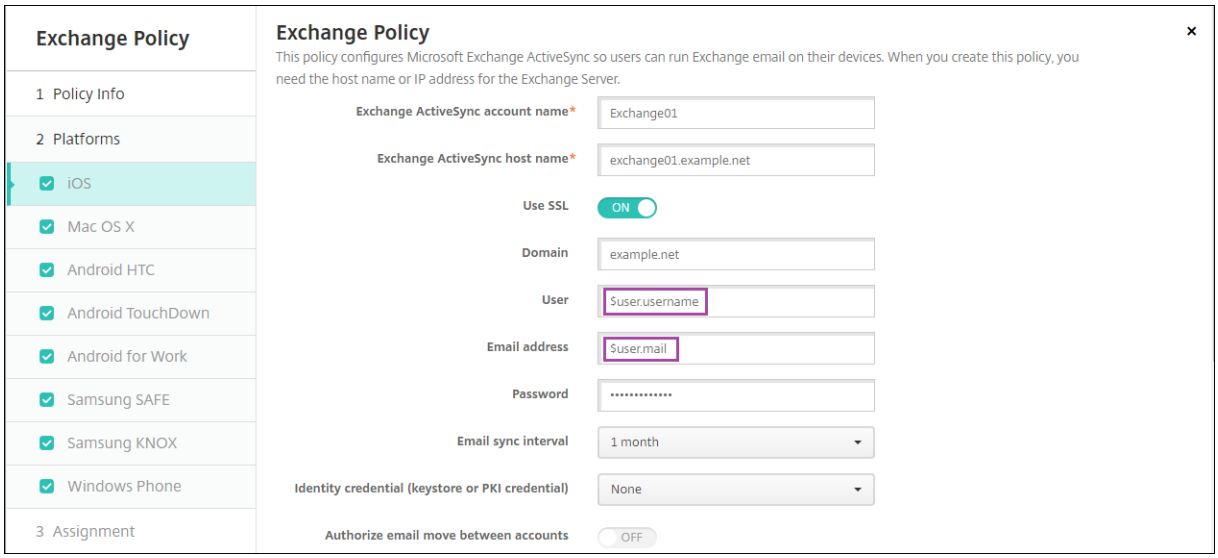
Placez toute syntaxe suivie du symbole dollar ($) entre accolades ({ }).

- Les noms de propriétés qualifiés font référence à une propriété utilisateur, à une propriété d'appareil ou à une propriété personnalisée.
- Les noms de propriétés qualifiés consistent en un préfixe, suivi par le nom de propriété réel.

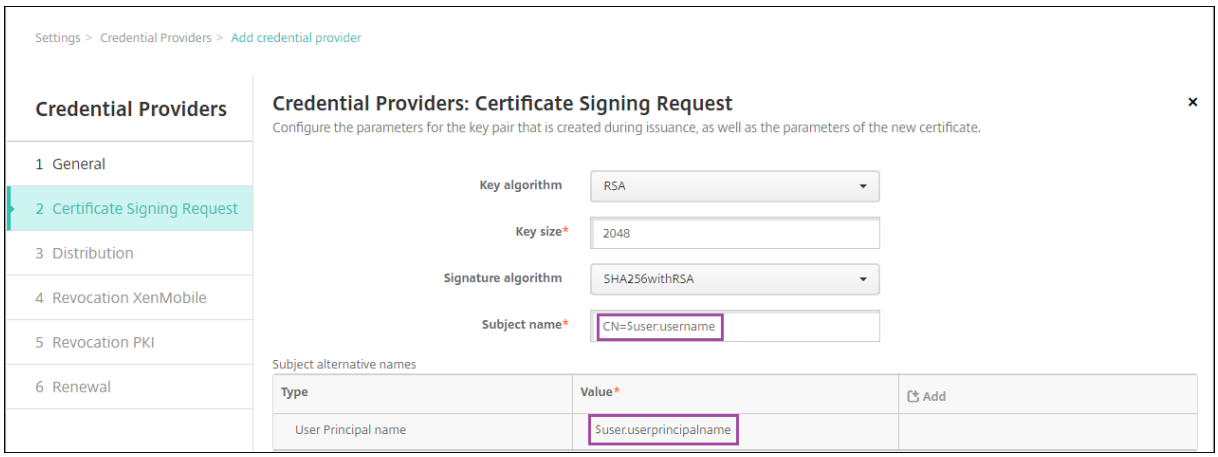
- Les propriétés de l'utilisateur prennent la forme `${ user.[PROPERTYNAME] (prefix="user.")}`.
- Les propriétés d'appareil prennent la forme `${ device.[PROPERTYNAME] (prefix="device.")}`.
- Les noms de propriétés sont sensibles à la casse.
- Une fonction peut être une liste limitée ou un lien vers une référence tierce qui définit les fonctions. La macro suivante pour un message de notification comprend la fonction **firstnotnull**.

  L'appareil `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` a été bloqué …
- Pour les macros personnalisées (propriétés que vous définissez), le préfixe est `${ custom }`. Vous pouvez ignorer le préfixe.

Voici un exemple de macro couramment utilisée, `${ user.username }`, qui remplit la valeur de nom d'utilisateur dans le champ de texte d'une stratégie. Cette macro est utile pour la configuration des profils Exchange ActiveSync et d'autres profils utilisés par plusieurs utilisateurs. L'exemple suivant illustre comment utiliser les macros dans une stratégie Exchange. La macro pour **Utilisateur** est **`${ user.username }`**. La macro pour **Adresse e-mail** est **`${ user.mail }`**.

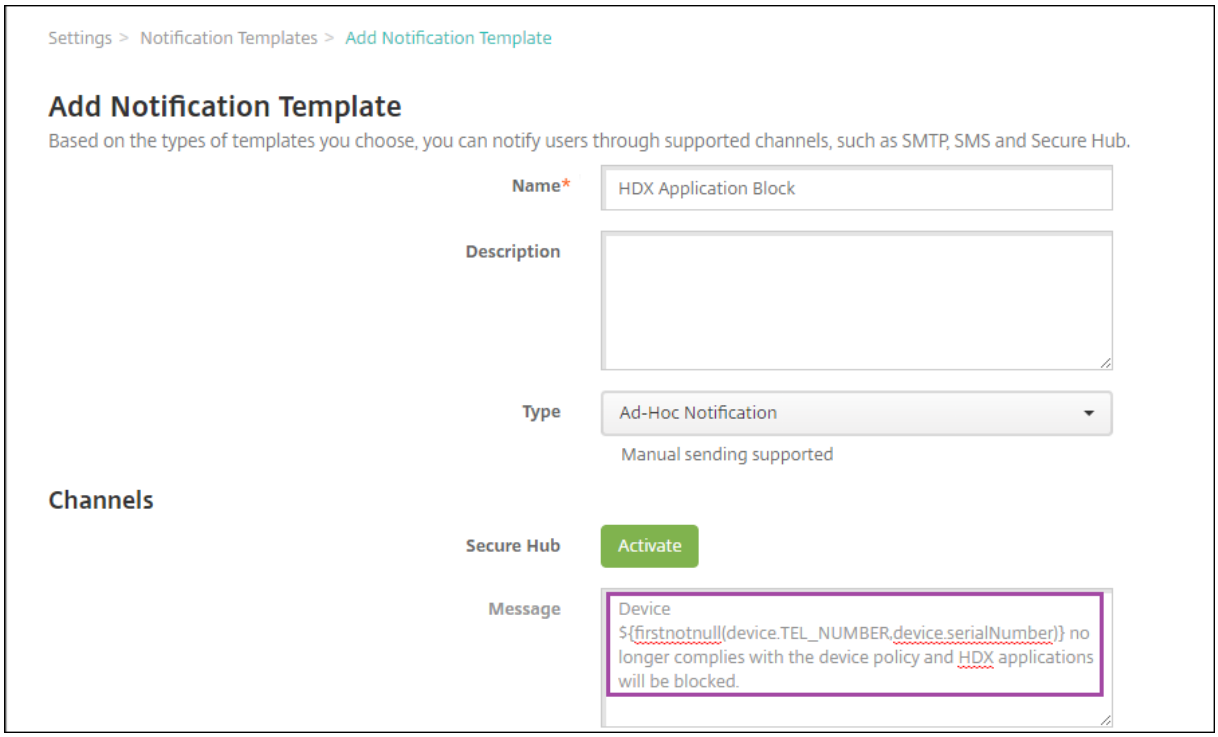


L'exemple suivant illustre comment utiliser les macros pour une demande de signature de certificat. La macro pour **Nom du sujet** est **`CN=$user.username`**. La macro pour la **Valeur** d'un **Autre nom de l'objet** est **`$user.userprincipalname`**.



L'exemple suivant illustre comment utiliser les macros dans un modèle de notification. Le modèle en exemple définit le message envoyé à un utilisateur lorsque les applications HDX sont bloquées en raison d'un appareil non conforme. La macro pour le **Message** est :

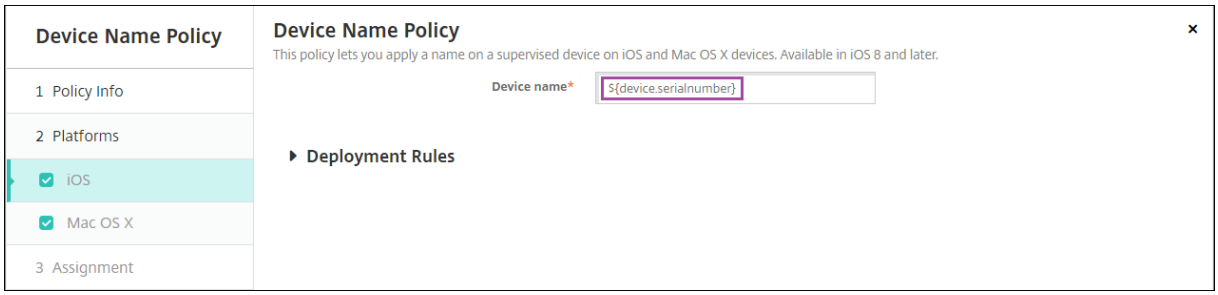
L'appareil `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` n'est plus conforme avec la stratégie et les applications HDX vont être bloquées.



Pour plus d'exemples de macros utilisées dans les notifications, accédez à **Paramètres > Modèles de notification**, sélectionnez un modèle prédéfini et cliquez sur **Modifier**.

L'exemple suivant illustre une macro dans la stratégie de nom de l'appareil. Vous pouvez entrer une macro, une combinaison de macros, ou une combinaison de macros et de texte pour donner un nom unique à chaque appareil. Par exemple, utilisez `${ device.serialnumber }` pour définir le nom

de l'appareil à partir du numéro de série de l'appareil. Utilisez `${ device.serialnumber } ${ user.username }` pour inclure le nom d'utilisateur dans le nom de l'appareil. La stratégie de nom d'appareil fonctionne sur les appareils supervisés iOS et macOS.



Macros pour les modèles de notification par défaut

Les macros suivantes sont utilisées dans les modèles de notification par défaut :

- `${ account.SUPPORT_EMAIL }`
- `${ applicationName }`
- `${ enrollment.andriod.agent.download.url }`
- `${ enrollment.ios.agent.download.url }`
- `${ enrollment.pin }`
- `${ enrollment.url }`
- `${ enrollment.urls }`
- `${ enrollment.ios.url }`
- `${ enrollment.macos.url }`
- `${ enrollment.android.url }`
- `${ enrollment.ios.platform }`
- `${ enrollment.macos.platform }`
- `${ enrollment.android.platform }`
- `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}`
- `${ firstnotnull(device.TEL_NUMBER,user.mobile)}`
- `${ outofcompliance.reason(smg_block)}`
- `${ outofcompliance.reason(whitelist_blacklist_apps_name)}`

> **Remarque :**
>
> La console XenMobile Server utilise les termes « liste noire » et « liste blanche ». Ces termes seront modifiés dans une prochaine version et les termes « liste de blocage » et « liste d'autorisation » les remplaceront.

- `${ vpp.account }`
- `${ vpp.appname }`
- `${ vpp.url }`
- `${ zdmserver.hostPath } /enroll`

Macros pour les stratégies spécifiques

Pour la stratégie Nom de l'appareil (pour iOS et macOS), vous pouvez utiliser ces macros pour le **nom de l'appareil** :

- `${ device.serialnumber }`
- `${ user.username } @example.com`
- `${ device.serialnumber }`
- `${ device.serialnumber }`
- `${ user.username }`
- `${ enrollment.pin }`
- `${ user.dnsroot }`

Pour la stratégie de clip Web, vous pouvez utiliser cette macro pour l'**URL** :

- `${ webeas-url }`

Pour la stratégie de clé de licence MDM Samsung, vous pouvez utiliser cette macro pour la **clé de licence ELM** :

- `${ elm.license.key }`

Macros pour obtenir des propriétés d'appareils intégrés

Nom d'affichage	Macros
ID de l'appareil	`$device.id`
GUID de l'appareil	`$device.uniqueid`
IMEI de l'appareil	`$device.imei`
OS	`$device.OSFamily`

Nom d'affichage	Macros
Numéro de série	`$device.serialNumber`

Macros pour toutes les propriétés d'appareil

La liste suivante fournit le nom d'affichage, l'élément Web et les macros.

Compte suspendu ?

- GOOGLE_AW_DIRECTORY_SUSPENDED
- ${device.GOOGLE_AW_DIRECTORY_SUSPENDED

Code de contournement du verrouillage d'activation

- ACTIVATION_LOCK_BYPASS_CODE
- ${device.ACTIVATION_LOCK_BYPASS_CODE

Verrouillage d'activation activé

- ACTIVATION_LOCK_ENABLED
- ${device.ACTIVATION_LOCK_ENABLED

Compte iTunes actif

- ACTIVE_ITUNES
- ${device.ACTIVE_ITUNES}

Appareil ActiveSync connu par MSP

- AS_DEVICE_KNOWN_BY_ZMSP
- ${device.AS_DEVICE_KNOWN_BY_ZMSP

ID ActiveSync

- EXCHANGE_ACTIVESYNC_ID
- ${device.EXCHANGE_ACTIVESYNC_ID

Administrateur désactivé

- ADMIN_DISABLED
- ${device.ADMIN_DISABLED

AIK présent ?

- WINDOWS_HAS_AIK_PRESENT
- ${device.WINDOWS_HAS_AIK_PRESENT

API Amazon MDM disponible

- AMAZON_MDM

- ${device.AMAZON_MDM

ID appareil Android Enterprise

- GOOGLE_AW_DEVICE_ID
- ${device.GOOGLE_AW_DEVICE_ID

Appareil compatible avec Android Enterprise ?

- GOOGLE_AW_ENABLED_DEVICE
- ${device.GOOGLE_AW_ENABLED_DEVICE

Type d'installation Android Enterprise

- GOOGLE_AW_INSTALL_TYPE
- ${device.GOOGLE_AW_INSTALL_TYPE

État de la signature de l'antispyware

- ANTI_SPYWARE_SIGNATURE_STATUS
- ${device.ANTI_SPYWARE_SIGNATURE_STATUS

État de l'antispyware

- ANTI_SPYWARE_STATUS
- ${device.ANTI_SPYWARE_STATUS

État de la signature de l'antivirus

- ANTI_VIRUS_SIGNATURE_STATUS
- ${device.ANTI_VIRUS_SIGNATURE_STATUS

État de l'antivirus

- ANTI_VIRUS_STATUS
- ${device.ANTI_VIRUS_STATUS

Code de contournement du verrouillage d'activation DEP ASM

- DEP_ACTIVATION_LOCK_BYPASS_CODE
- ${device.DEP_ACTIVATION_LOCK_BYPASS_CODE

Dépôt de clé DEP ASM

- DEP_ESCROW_KEY
- ${device.DEP_ESCROW_KEY

Numéro d'identification

- ASSET_TAG
- ${device.ASSET_TAG

Rechercher automatiquement les mises à jour logicielles

- AutoCheckEnabled
- ${device.AutoCheckEnabled

Télécharger automatiquement les mises à jour logicielles en arrière-plan

- BackgroundDownloadEnabled
- ${device.BackgroundDownloadEnabled

Installer automatiquement les mises à jour applicatives

- AutomaticAppInstallationEnabled
- ${device.AutomaticAppInstallationEnabled

Installer automatiquement les mises à jour d'OS

- AutomaticOSInstallationEnabled
- ${device.AutomaticOSInstallationEnabled

Installer automatiquement les mises à jour de sécurité

- AutomaticSecurityUpdatesEnabled
- ${device.AutomaticSecurityUpdatesEnabled

État de la mise à jour automatique

- AUTOUPDATE_STATUS
- ${device.AUTOUPDATE_STATUS

RAM disponible

- MEMORY_AVAILABLE
- ${device.MEMORY_AVAILABLE

Mises à jour logicielles disponibles

- AVAILABLE_OS_UPDATE_HUMAN_READABLE
- ${device.AVAILABLE_OS_UPDATE_HUMAN_READABLE

Espace de stockage disponible

- FREEDISK
- ${device.FREEDISK

Batterie de secours

- BACKUP_BATTERY_PERCENT
- ${device.BACKUP_BATTERY_PERCENT

Version du firmware radio

- MODEM_FIRMWARE_VERSION
- ${device.MODEM_FIRMWARE_VERSION

Batterie en charge

- BATTERY_CHARGING_STATUS
- ${device.BATTERY_CHARGING_STATUS

Batterie en charge

- BATTERY_CHARGING
- ${device.BATTERY_CHARGING

Batterie restante

- BATTERY_ESTIMATED_CHARGE_REMAINING
- ${device.BATTERY_ESTIMATED_CHARGE_REMAINING

Autonomie de la batterie

- BATTERY_RUNTIME
- ${device.BATTERY_RUNTIME

État de la batterie

- BATTERY_STATUS
- ${device.BATTERY_STATUS

Appareil Bes connu par MS

- BES_DEVICE_KNOWN_BY_ZMSP
- ${device.BES_DEVICE_KNOWN_BY_ZMSP

Code PIN BES

- BES_PIN
- ${device.BES_PIN

ID de l'agent du serveur BES

- AGENT_ID
- ${device.AGENT_ID

Nom du serveur BES

- BES_SERVER
- ${device.BES_SERVER

Version du serveur BES

- BES_VERSION
- ${device.BES_VERSION

Infos du BIOS

- BIOS_INFO

- ${device.BIOS_INFO

État de BitLocker

- WINDOWS_HAS_BIT_LOCKER_STATUS
- ${device.WINDOWS_HAS_BIT_LOCKER_STATUS

Adresse MAC Bluetooth

- BLUETOOTH_MAC
- ${device.BLUETOOTH_MAC

Débogage du démarrage activé ?

- WINDOWS_HAS_BOOT_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED

Version de la liste de révision du Gestionnaire de démarrage

- WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION
- ${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION

Code de l'opérateur

- CARRIER_CODE
- ${device.CARRIER_CODE

Version des paramètres opérateur

- CARRIER_SETTINGS_VERSION
- ${device.CARRIER_SETTINGS_VERSION

URL du catalogue

- CatalogURL
- ${device.CatalogURL

Altitude cellulaire

- GPS_ALTITUDE_FROM_CELLULAR
- ${device.GPS_ALTITUDE_FROM_CELLULAR

Parcours cellulaire

- GPS_COURSE_FROM_CELLULAR
- ${device.GPS_COURSE_FROM_CELLULAR

Précision horizontale cellulaire

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR

Cellulaire - Latitude

- GPS_LATITUDE_FROM_CELLULAR
- ${device.GPS_LATITUDE_FROM_CELLULAR

Cellulaire - Longitude

- GPS_LONGITUDE_FROM_CELLULAR
- ${device.GPS_LONGITUDE_FROM_CELLULAR

Vitesse cellulaire

- GPS_SPEED_FROM_CELLULAR
- ${device.GPS_SPEED_FROM_CELLULAR

Technologie cellulaire

- CELLULAR_TECHNOLOGY
- ${device.CELLULAR_TECHNOLOGY

Cellulaire - Horodatage

- GPS_TIMESTAMP_FROM_CELLULAR
- ${device.GPS_TIMESTAMP_FROM_CELLULAR

Précision verticale cellulaire

- GPS_VERTICAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}

Changer le mot de passe lors de la prochaine connexion ?

- GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN
- ${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

ID de l'appareil client

- CLIENT_DEVICE_ID
- ${device.CLIENT_DEVICE_ID

Sauvegarde sur cloud activée

- CLOUD_BACKUP_ENABLED
- ${device.CLOUD_BACKUP_ENABLED

Intégrité du code activée ?

- WINDOWS_HAS_CODE_INTEGRITY_ENABLED
- ${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED

Version de la liste de révision d'intégrité du code

- INDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION
- ${Device.Windows_HASS_CODE_INTGTY_REV_LIST_VERSION

Couleur

- COLOR
- ${device.COLOR

Fréquence du processeur

- CPU_CLOCK_SPEED
- ${device.CPU_CLOCK_SPEED

Type de processeur

- CPU_TYPE
- ${device.CPU_TYPE}

Date de création

- GOOGLE_AW_DIRECTORY_CREATION_TIME
- ${device.GOOGLE_AW_DIRECTORY_CREATION_TIME

Mises à jour logicielles critiques

- AVAILABLE_OS_UPDATE_IS_CRITICAL
- ${device.AVAILABLE_OS_UPDATE_IS_CRITICAL

Réseau de l'opérateur actuel

- CARRIER
- ${device.CARRIER

Indicatif de pays du mobile actuel

- CURRENT_MCC
- ${device.CURRENT_MCC

Code réseau du mobile actuel

- CURRENT_MNC
- ${device.CURRENT_MNC

Itinérance des données autorisée

- DATA_ROAMING_ENABLED
- ${device.DATA_ROAMING_ENABLED

Date de la dernière sauvegarde iCloud

- LAST_CLOUD_BACKUP_DATE
- ${device.LAST_CLOUD_BACKUP_DATE}

Catalogue par défaut

- IsDefaultCatalog

- ${device.IsDefaultCatalog

Nom du compte DEP

- BULK_ENROLLMENT_DEP_ACCOUNT_NAME
- ${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME

Stratégie DEP

- WINDOWS_HAS_DEP_POLICY
- ${device.WINDOWS_HAS_DEP_POLICY

Profil DEP attribué

- PROFILE_ASSIGN_TIME
- ${device.PROFILE_ASSIGN_TIME

Profil DEP transmis

- PROFILE_PUSH_TIME
- ${device.PROFILE_PUSH_TIME

Profil DEP supprimé

- PROFILE_REMOVE_TIME
- ${device.PROFILE_REMOVE_TIME

Enregistrement auprès de DEP d'ici le

- DEVICE_ASSIGNED_BY
- ${device.DEVICE_ASSIGNED_BY

Date d'enregistrement auprès de DEP

- DEVICE_ASSIGNED_DATE
- ${device.DEVICE_ASSIGNED_DATE

Description

- DESCRIPTION
- ${device.DESCRIPTION

Identificateur d'appareil

- Activesyncid
- ${device.activesyncid

Modèle d'appareil

- SYSTEM_OEM
- ${device.SYSTEM_OEM

Nom de l'appareil

- DEVICE_NAME
- ${device.DEVICE_NAME

Type d'appareil

- DEVICE_TYPE
- ${device.DEVICE_TYPE

Ne pas déranger activé

- DO_NOT_DISTURB
- ${device.DO_NOT_DISTURB

Pilote ELAM chargé ?

- WINDOWS_HAS_ELAM_DRIVER_LOADED
- ${device.WINDOWS_HAS_ELAM_DRIVER_LOADED

Conformité du chiffrement

- ENCRYPTION_COMPLIANCE
- ${device.ENCRYPTION_COMPLIANCE

ENROLLMENT_KEY_GENERATION_DATE

- ENROLLMENT_KEY_GENERATION_DATE
- ${device.ENROLLMENT_KEY_GENERATION_DATE

ID d'entreprise

- ENTERPRISEID
- ${device.ENTERPRISEID

Stockage externe 1 : espace disponible

- EXTERNAL_STORAGE1_FREE_SPACE
- ${device.EXTERNAL_STORAGE1_FREE_SPACE

Stockage externe 1 : nom

- EXTERNAL_STORAGE1_NAME
- ${device.EXTERNAL_STORAGE1_NAME

Stockage externe 1 : espace total

- EXTERNAL_STORAGE1_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE1_TOTAL_SPACE

Stockage externe 2 : espace disponible

- EXTERNAL_STORAGE2_FREE_SPACE
- ${device.EXTERNAL_STORAGE2_FREE_SPACE

Stockage externe 2 : nom

- EXTERNAL_STORAGE2_NAME
- ${device.EXTERNAL_STORAGE2_NAME

Stockage externe 2 : espace total

- EXTERNAL_STORAGE2_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE2_TOTAL_SPACE

Stockage externe chiffré

- EXTERNAL_ENCRYPTION
- ${device.EXTERNAL_ENCRYPTION

FileVault activé

- IS_FILEVAULT_ENABLED
- ${device.IS_FILEVAULT_ENABLED

État du pare-feu

- DEVICE_FIREWALL_STATUS
- ${device.DEVICE_FIREWALL_STATUS

État du pare-feu

- FIREWALL_STATUS
- ${device.FIREWALL_STATUS

Version du firmware

- FIRMWARE_VERSION
- ${device.FIRMWARE_VERSION

Première synchronisation

- ZMSP_FIRST_SYNC
- ${device.ZMSP_FIRST_SYNC

Alias Google Directory

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- ${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS

Nom de famille Google Directory

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- ${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME

Nom Google Directory

- GOOGLE_AW_DIRECTORY_NAME

- ${device.GOOGLE_AW_DIRECTORY_NAME}

E-mail principal Google Directory

- GOOGLE_AW_DIRECTORY_PRIMARY
- ${device.GOOGLE_AW_DIRECTORY_PRIMARY}

ID utilisateur Google Directory

- GOOGLE_AW_DIRECTORY_USER_ID
- ${device.GOOGLE_AW_DIRECTORY_USER_ID}

GPS - Altitude

- GPS_ALTITUDE_FROM_GPS
- ${device.GPS_ALTITUDE_FROM_GPS

Parcours GPS

- GPS_COURSE_FROM_GPS
- ${device.GPS_COURSE_FROM_GPS

Précision horizontale GPS

- GPS_HORIZONTAL_ACCURACY_FROM_GPS
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS

GPS - Latitude

- GPS_LATITUDE_FROM_GPS
- ${device.GPS_LATITUDE_FROM_GPS

GPS - Longitude

- GPS_LONGITUDE_FROM_GPS
- ${device.GPS_LONGITUDE_FROM_GPS

Vitesse GPS

- GPS_SPEED_FROM_GPS
- ${device.GPS_SPEED_FROM_GPS

GPS - Horodatage

- GPS_TIMESTAMP_FROM_GPS
- ${device.GPS_TIMESTAMP_FROM_GPS

Précision verticale GPS

- GPS_VERTICAL_ACCURACY_FROM_GPS
- ${device.GPS_VERTICAL_ACCURACY_FROM_GPS

ID du périphérique matériel

- HW_DEVICE_ID
- ${device.HW_DEVICE_ID

Capacités de chiffrement du matériel

- HARDWARE_ENCRYPTION_CAPS
- ${device.HARDWARE_ENCRYPTION_CAPS

HAS_CONTAINER

- HAS_CONTAINER
- ${device.HAS_CONTAINER

Hash du compte iTunes Store actuellement connecté

- ITUNES_STORE_ACCOUNT_HASH
- ${device.ITUNES_STORE_ACCOUNT_HASH

Opérateur de la carte SIM

- SIM_CARRIER_NETWORK
- ${device.SIM_CARRIER_NETWORK

Indicatif de pays du mobile domestique

- SIM_MCC
- ${device.SIM_MCC

Code réseau de la carte SIM

- SIM_MNC
- ${device.SIM_MNC

ICCID

- ICCID
- ${device.ICCID

Identité

- AS_DEVICE_IDENTITY
- ${device.AS_DEVICE_IDENTITY

Numéro IMEI/MEID

- IMEI
- ${device.IMEI

IMSI

- SIM_ID
- ${device.SIM_ID

Stockage interne chiffré

- LOCAL_ENCRYPTION
- ${device.LOCAL_ENCRYPTION

Adresse IP

- IP_LOCATION
- ${device.IP_LOCATION

Adresse IPv4

- IP_ADDRESSV4
- ${device.IP_ADDRESSV4

Adresse IPv6

- IP_ADDRESSV6
- ${device.IP_ADDRESSV6

Date d'émission

- WINDOWS_HAS_ISSUED_AT
- ${device.WINDOWS_HAS_ISSUED_AT

Jailbreaké/rooté

- ROOT_ACCESS
- ${device.ROOT_ACCESS

Débogage du noyau activé ?

- WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED

Mode Kiosque

- IS_KIOSK
- ${device.IS_KIOSK

Dernière adresse IP connue

- LAST_IP_ADDR
- ${device.LAST_IP_ADDR

Dernière date de mise à jour de la stratégie

- LAST_POLICY_UPDATE_TIME
- ${device.LAST_POLICY_UPDATE_TIME

Date dernière recherche

- PreviousScanDate

- ${device.PreviousScanDate

Résultat dernière recherche

- PreviousScanResult
- ${device.PreviousScanResult

Dernières mises à jour logicielles planifiées

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- ${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME

Dernier message d'échec des mises à jour logicielles planifiées

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- ${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG

Dernier état des mises à jour logicielles planifiées

- AVAILABLE_OS_UPDATE_INSTALL_STATUS
- ${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS

Dernière synchronisation

- ZMSP_LAST_SYNC
- ${device.ZMSP_LAST_SYNC

Service de localisation activé

- DEVICE_LOCATOR
- ${device.DEVICE_LOCATOR

Adresse MAC

- MAC_ADDRESS
- ${device.MAC_ADDRESS

Connexion réseau de l'adresse MAC

- MAC_NETWORK_CONNECTION
- ${device.MAC_NETWORK_CONNECTION

Type d'adresse MAC

- MAC_ADDRESS_TYPE
- ${device.MAC_ADDRESS_TYPE

Configuration de la boîte aux lettres

- GOOGLE_AW_DIRECTORY_MAILBOX_SETUP
- ${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP

Batterie principale

- MAIN_BATTERY_PERCENT
- ${device.MAIN_BATTERY_PERCENT

Mode perdu MDM activé

- IS_MDM_LOST_MODE_ENABLED
- ${device.IS_MDM_LOST_MODE_ENABLED

MDX_SHARED_ENCRYPTION_KEY

- MDX_SHARED_ENCRYPTION_KEY
- ${device.MDX_SHARED_ENCRYPTION_KEY

MEID

- MEID
- ${device.MEID

Numéro de téléphone

- TEL_NUMBER
- ${device.TEL_NUMBER

ID du modèle

- MODEL_ID
- ${device.MODEL_ID}

Numéro de modèle

- MODEL_NUMBER
- ${device.MODEL_NUMBER

Type de carte réseau

- NETWORK_ADAPTER_TYPE
- ${device.NETWORK_ADAPTER_TYPE

Build du système d'exploitation

- SYSTEM_OS_BUILD
- ${device.SYSTEM_OS_BUILD

Édition du système d'exploitation

- OS_EDITION
- ${device.OS_EDITION

Langue du système d'exploitation (paramètres régionaux)

- SYSTEM_LANGUAGE
- ${device.SYSTEM_LANGUAGE

Version du système d'exploitation

- SYSTEM_OS_VERSION
- ${device.SYSTEM_OS_VERSION

Adresse de l'organisation

- ORGANIZATION_ADDRESS
- ${device.ORGANIZATION_ADDRESS

E-mail de l'organisation

- ORGANIZATION_EMAIL
- ${device.ORGANIZATION_EMAIL

Organisation Magic

- ORGANIZATION_MAGIC
- ${device.ORGANIZATION_MAGIC

Nom de l'organisation

- ORGANIZATION_NAME
- ${device.ORGANIZATION_NAME

N° de tél. de l'organisation

- ORGANIZATION_PHONE
- ${device.ORGANIZATION_PHONE

Non conforme

- OUT_OF_COMPLIANCE
- ${device.OUT_OF_COMPLIANCE

Appartient à

- CORPORATE_OWNED
- ${device.CORPORATE_OWNED

Code secret conforme

- PASSCODE_IS_COMPLIANT
- ${device.PASSCODE_IS_COMPLIANT

Code secret conforme à la configuration

- PASSCODE_IS_COMPLIANT_WITH_CFG
- ${device.PASSCODE_IS_COMPLIANT_WITH_CFG

Code secret présent

- PASSCODE_PRESENT

- ${device.PASSCODE_PRESENT

PCR0

- WINDOWS_HAS_PCR0
- ${device.WINDOWS_HAS_PCR0

Violation du périmètre

- GPS_PERIMETER_BREACH
- ${device.GPS_PERIMETER_BREACH

Recherche périodique

- PerformPeriodicCheck
- ${device.PerformPeriodicCheck

Personal Hotspot activé

- PERSONAL_HOTSPOT_ENABLED
- ${device.PERSONAL_HOTSPOT_ENABLED

Code PIN du géofencing

- PIN_CODE_FOR_GEO_FENCE
- ${device.PIN_CODE_FOR_GEO_FENCE

Plateforme

- SYSTEM_PLATFORM
- ${device.SYSTEM_PLATFORM}

Niveau d'API de la plate-forme

- API_LEVEL
- ${device.API_LEVEL

Nom de la stratégie

- POLICY_NAME
- ${device.POLICY_NAME

Numéro de téléphone principal

- IDENTITY1_PHONENUMBER
- ${device.IDENTITY1_PHONENUMBER

Opérateur de la carte SIM principale

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY1_CARRIER_NETWORK_OPERATOR

ICCID de la carte SIM principale

- IDENTITY1_ICCID
- ${device.IDENTITY1_ICCID

N° IMEI de la carte SIM principale

- IDENTITY1_IMEI
- ${device.IDENTITY1_IMEI

N° IMSI de la carte SIM principale

- IDENTITY1_IMSI
- ${device.IDENTITY1_IMSI

Itinérance de la carte SIM principale

- IDENTITY1_ROAMING
- ${device.IDENTITY1_ROAMING

Conformité de la carte SIM principale avec l'itinérance

- IDENTITY1_ROAMING_COMPLIANCE
- ${device.IDENTITY1_ROAMING_COMPLIANCE

Nom du produit

- PRODUCT_NAME
- ${device.PRODUCT_NAME

ID d'éditeur de l'appareil

- PUBLISHER_DEVICE_ID
- ${device.PUBLISHER_DEVICE_ID

Nombre de réinitialisations

- WINDOWS_HAS_RESET_COUNT
- ${device.WINDOWS_HAS_RESET_COUNT

Nombre de redémarrages

- WINDOWS_HAS_RESTART_COUNT
- ${device.WINDOWS_HAS_RESTART_COUNT

Mode sans échec activé ?

- WINDOWS_HAS_SAFE_MODE
- ${device.WINDOWS_HAS_SAFE_MODE

API Samsung KNOX disponible

- SAMSUNG_KNOX
- ${device.SAMSUNG_KNOX

Version API Samsung KNOX

- SAMSUNG_KNOX_VERSION
- ${device.SAMSUNG_KNOX_VERSION

Attestation Samsung KNOX

- SAMSUNG_KNOX_ATTESTED
- ${device.SAMSUNG_KNOX_ATTESTED

Date de mise à jour de l'attestation Samsung KNOX

- SAMSUNG_KNOX_ATT_UPDATED_TIME
- ${device.SAMSUNG_KNOX_ATT_UPDATED_TIME

API Samsung SAFE disponible

- SAMSUNG_MDM
- ${device.SAMSUNG_MDM

Version API Samsung SAFE

- SAMSUNG_MDM_VERSION
- ${device.SAMSUNG_MDM_VERSION

Hachage SBCP

- WINDOWS_HAS_SBCP_HASH
- ${device.WINDOWS_HAS_SBCP_HASH

Écran : hauteur

- SCREEN_HEIGHT
- ${device.SCREEN_HEIGHT

Écran : nombre de couleurs

- SCREEN_NB_COLORS
- ${device.SCREEN_NB_COLORS

Écran : taille

- SCREEN_SIZE
- ${device.SCREEN_SIZE

Écran : largeur

- SCREEN_WIDTH
- ${device.SCREEN_WIDTH

Écran : résolution axe X

- SCREEN_XDPI

- ${device.SCREEN_XDPI

Écran : résolution axe Y

- SCREEN_YDPI
- ${device.SCREEN_YDPI

Numéro de téléphone secondaire

- IDENTITY2_PHONENUMBER
- ${device.IDENTITY2_PHONENUMBER

Opérateur de la carte SIM secondaire

- IDENTITY2_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY2_CARRIER_NETWORK_OPERATOR

ICCID de la carte SIM secondaire

- IDENTITY2_ICCID
- ${device.IDENTITY2_ICCID

N° IMEI de la carte SIM secondaire

- IDENTITY2_IMEI
- ${device.IDENTITY2_IMEI

N° IMSI de la carte SIM secondaire

- IDENTITY2_IMSI
- ${device.IDENTITY2_IMSI

Itinérance de la carte SIM secondaire

- IDENTITY2_ROAMING
- ${device.IDENTITY2_ROAMING

Conformité de la carte SIM secondaire avec l'itinérance

- IDENTITY2_ROAMING_COMPLIANCE
- ${device.IDENTITY2_ROAMING_COMPLIANCE

Démarrage sécurisé activé ?

- WINDOWS_HAS_SECURE_BOOT_ENABLED
- ${device.WINDOWS_HAS_SECURE_BOOT_ENABLED

État du démarrage sécurisé

- SECURE_BOOT_STATE
- ${device.SECURE_BOOT_STATE

Conteneur sécurisé activé

- DLP_ACTIVE
- ${device.DLP_ACTIVE

Niveau de correctif de sécurité

- SYSTEM_SECURITY_PATCH_LEVEL
- ${device.SYSTEM_SECURITY_PATCH_LEVEL

Numéro de série

- SERIAL_NUMBER
- ${device.SERIAL_NUMBER

Prise en charge des SMS

- IS_SMS_CAPABLE
- ${device.IS_SMS_CAPABLE

Supervisé

- SUPERVISED
- ${device.SUPERVISED

Motif de la suspension

- GOOGLE_AW_DIRECTORY_SUSPENTION_REASON
- ${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON

État altéré

- TAMPERED_STATUS
- ${device.TAMPERED_STATUS

Termes et conditions

- TERMS_AND_CONDITIONS
- ${device.TERMS_AND_CONDITIONS

Termes et conditions acceptés ?

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- ${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS

Signature du test activée ?

- WINDOWS_HAS_TEST_SIGNING_ENABLED
- ${device.WINDOWS_HAS_TEST_SIGNING_ENABLED

RAM totale

- MEMORY
- ${device.MEMORY

Espace de stockage total

- TOTAL_DISK_SPACE
- ${device.TOTAL_DISK_SPACE

Version du TPM

- TPM_VERSION
- ${device.TPM_VERSION

UDID

- UDID
- ${device.UDID}

État du contrôle de compte d'utilisateur

- UAC_STATUS
- ${device.UAC_STATUS

Agent utilisateur

- USER_AGENT
- ${device.USER_AGENT

Défini par l'utilisateur #1

- USER_DEFINED_1
- ${device.USER_DEFINED_1

Défini par l'utilisateur #2

- USER_DEFINED_2
- ${device.USER_DEFINED_2

Défini par l'utilisateur #3

- USER_DEFINED_3
- ${device.USER_DEFINED_3

Langue de l'utilisateur (paramètres régionaux)

- USER_LANGUAGE
- ${device.USER_LANGUAGE

Fournisseur

- VENDOR
- ${device.VENDOR

Prise en charge de la voix

- IS_VOICE_CAPABLE

- ${device.IS_VOICE_CAPABLE

Itinérance voix autorisée

- VOICE_ROAMING_ENABLED
- ${device.VOICE_ROAMING_ENABLED

VSM activé ?

- WINDOWS_HAS_VSM_ENABLED
- ${device.WINDOWS_HAS_VSM_ENABLED

Adresse MAC Wi-Fi

- WIFI_MAC
- ${device.WIFI_MAC}

WINDOWS_ENROLLMENT_KEY

- WINDOWS_ENROLLMENT_KEY
- ${device.WINDOWS_ENROLLMENT_KEY

WinPE activé ?

- WINDOWS_HAS_WINPE
- ${device.WINDOWS_HAS_WINPE

État de la notification WNS

- PROPERTY_WNS_PUSH_STATUS
- ${device.PROPERTY_WNS_PUSH_STATUS

URL de notification WNS

- PROPERTY_WNS_PUSH_URL
- ${device.PROPERTY_WNS_PUSH_URL

Date d'expiration de l'URL de notification WNS

- PROPERTY_WNS_PUSH_URL_EXPIRY
- ${device.PROPERTY_WNS_PUSH_URL_EXPIRY

ID d'agent XenMobile

- ENROLLMENT_AGENT_ID
- ${device.ENROLLMENT_AGENT_ID

Révision de l'agent XenMobile

- EW_REVISION
- ${device.EW_REVISION

Version de l'agent XenMobile

- EW_VERSION
- ${device.EW_VERSION

API Zebra disponible

- ZEBRA_MDM
- ${device.ZEBRA_MDM

Version du MXMF Zebra

- ZEBRA_MDM_VERSION
- ${device.ZEBRA_MDM_VERSION

Version du patch Zebra

- ZEBRA_PATCH_VERSION
- ${device.ZEBRA_PATCH_VERSION}

Macros pour obtenir des propriétés utilisateur intégrés

Nom d'affichage	Macros
domainname (nom de domaine, domaine par défaut)	`${ user.domainname }`
loginname (nom d'utilisateur + nom de domaine)	`${ user.loginname }`
username (nom d'ouverture de session moins le domaine, si présent)	`${ user.username }`

Macros pour toutes les propriétés utilisateur

Nom d'affichage	Élément Web	Macros
Échecs de connexion à Active Directory	badpwdcount	`${ user.badpwdcount }`
E-mail de l'utilisateur ActiveSync	asuseremail	`${ user.asuseremail }`
Source de données ASM	asmpersonsource	`${ user. asmpersonsource }`
Nom du compte DEP ASM	asmdepaccount	`${ user.asmdepaccount }`

Nom d'affichage	Élément Web	Macros
Identifiant Apple ID géré par ASM	asmpersonmanagedappleid	${ user.asmpersonmanagedappleid }
Type de code d'accès ASM	asmpersonpasscodetype	${ user.asmpersonpasscodetype }
Identifiant d'étudiant ASM	asmpersonid	${ user.asmpersonid }
Statut de l'étudiant ASM	asmpersonstatus	${ user.asmpersonstatus }
Titre de l'étudiant ASM	asmpersontitle	${ user.asmpersontitle }
Identifiant unique de l'étudiant ASM	asmpersonuniqueid	${ user.asmpersonuniqueid }
Identifiant du système source ASM	asmpersonsourcesystemid	${ user.asmpersonsourcesystemid }
Niveau scolaire de l'étudiant ASM	asmpersongrade	${ user.asmpersongrade }
E-mail de l'utilisateur BES	besuseremail	${ user.besuseremail }
Société	company	${ user.company }
Nom de la société	companyname	${ user.companyname }
Pays	c	${ user.c }
Département	department	${ user.department }
Description	description	${ user.description }
Utilisateur désactivé	disableduser	${ user.disableduser }
Nom d'affichage	nomaffiché	${ user.displayname }
Nom unique	distinguishedname	${ user.distinguishedname }
Nom de domaine	domainname	${ user.domainname }
E-mail	mail	${ user.mail }
Prénom	givenname	${ user.givenname }

Nom d'affichage	Élément Web	Macros
Adresse (domicile)	homestreetaddress	${ user.homestreetaddress }
Ville (domicile)	homecity	${ user.homecity }
Pays (domicile)	homecountry	${ user.homecountry }
Fax (domicile)	homefax	${ user.homefax }
Téléphone domicile	homephone	${ user.homephone }
Dép./Région (domicile)	homestate	${ user.homestate }
Code postal (domicile)	homezip	${ user.homezip }
Tél. IP	ipphone	${ user.ipphone }
Second prénom	middleinitial	${ user.middleinitial }
Deuxième prénom	middlename	${ user.middlename }
Tél. portable	mobile	${ user.mobile }
Nom	cn	${ user.cn }
Adresse du bureau	physicaldeliveryofficename	${ user.physicaldeliveryofficename }
Ville (bureau)	l	${ user.l }
Fax du bureau	facsimiletelephonenumber	${ user.facsimiletelephonenumber }
Dép./Région du bureau	st	${ user.st }
Rue du bureau	officestreetaddress	${ user.officestreetaddress }
Tél. bureau	telephonenumber	${ user.telephonenumber }
Code postal du bureau	postalcode	${ user.postalcode }
Boîte postale	postofficebox	${ user.postofficebox }
Bipeur	pager	${ user.pager }
ID du groupe principal	primarygroupid	${ user.primarygroupid }

Nom d'affichage	Élément Web	Macros
Compte SAM	samaccountname	`${ user.samaccountname }`
Adresse	streetaddress	`${ user.streetaddress }`
Nom de famille	sn	`${ user.sn }`
Titre	title	`${ user.title }`
Nom de connexion de l'utilisateur	userprincipalname	`${ user.userprincipalname }`

Actions automatisées

January 10, 2022

Vous créez des actions automatisées dans XenMobile pour programmer des réactions à des événements, à des propriétés utilisateur/appareil ou l'existence d'applications sur les appareils utilisateur. Lorsque vous créez une action automatisée, les déclencheurs définis pour l'action déterminent ce qui se passe sur l'appareil de l'utilisateur lorsqu'il est connecté à XenMobile. Lorsqu'un événement est déclenché, vous pouvez envoyer une notification à l'utilisateur pour résoudre un problème avant qu'une action plus sérieuse ne soit nécessaire.

Les effets automatiques que vous pouvez paramétrer sont :

- Effacement complet ou effacement des données d'entreprise de l'appareil.
- Rendre l'appareil non-conforme.
- Révoquer l'appareil.
- Envoyer un message à l'utilisateur pour qu'il résolve un problème avant que des actions plus sévères ne soient entreprises.

Vous pouvez configurer des actions de verrouillage et d'effacement des applications en mode MAM uniquement.

> **Remarque :**
>
> Pour avertir les utilisateurs, vous devez avoir configuré les serveurs de notification dans les paramètres de XenMobile pour SMTP et SMS afin que XenMobile puisse envoyer des messages. Pour de plus amples informations, consultez la section Notifications. Vous devez également configurer les modèles de notification que vous prévoyez d'utiliser avant de continuer. Pour de plus amples informations, consultez la section Créer et mettre à jour des modèles de

> notification.

Exemples d'actions

Voici quelques exemples d'utilisation d'actions automatisées :

Exemple 1

- Vous souhaitez détecter une application que vous avez précédemment bloquée (par exemple, « Words with Friends »). Vous pouvez spécifier un déclencheur qui rend l'appareil utilisateur non conforme lorsque l'application « Words with Friends » est détectée. L'action avertit les utilisateurs qu'ils doivent supprimer l'application pour que leurs appareils soient à nouveau conformes. Vous pouvez également définir un délai pour que les utilisateurs se conforment. Après ce délai, une action définie se produit, comme l'effacement sélectif de l'appareil.

Exemple 2

- Vous souhaitez vérifier si les clients utilisent le dernier firmware et bloquer l'accès aux ressources si les utilisateurs doivent mettre à jour leurs appareils. Vous pouvez spécifier un déclencheur qui rend l'appareil utilisateur non conforme lorsqu'il ne dispose pas de la dernière version. Vous utilisez des actions automatisées pour bloquer les ressources et pour informer les clients.

Exemple 3

- Un appareil utilisateur est placé dans un état de non-conformité, puis l'utilisateur répare l'appareil de façon à ce qu'il soit conforme. Vous pouvez configurer une stratégie permettant de déployer un package qui réinitialise l'appareil dans un état de conformité.

Exemple 4

- Vous souhaitez marquer des appareils utilisateur qui ont été inactifs pendant une certaine période de temps comme étant non conformes. Vous pouvez créer une action automatisée pour les appareils inactifs comme suit :

  1. Dans la console XenMobile, accédez à **Paramètres > Contrôle d'accès réseau**, puis sélectionnez **Appareils inactifs**. Pour plus d'informations sur le paramètre **Appareils inactifs**, consultez la section Contrôle d'accès réseau.
  2. Suivez les étapes pour ajouter une action, comme indiqué dans Ajouter et gérer des actions. La seule différence est que vous configurez les paramètres comme suit sur la page **Détails de l'action** :
     - **Déclencheur** : sélectionnez **Propriété de l'appareil**, **Non conforme** et **Vrai**.
     - **Action**. sélectionnez **Envoyer notification** et sélectionnez un modèle que vous avez créé à l'aide du champ **Modèle de notification** dans **Paramètres**. Ensuite, définissez le délai en jours, heures ou minutes avant d'exécuter l'action. Définissez l'intervalle auquel l'action se répète jusqu'à ce que l'utilisateur corrige le problème déclencheur.

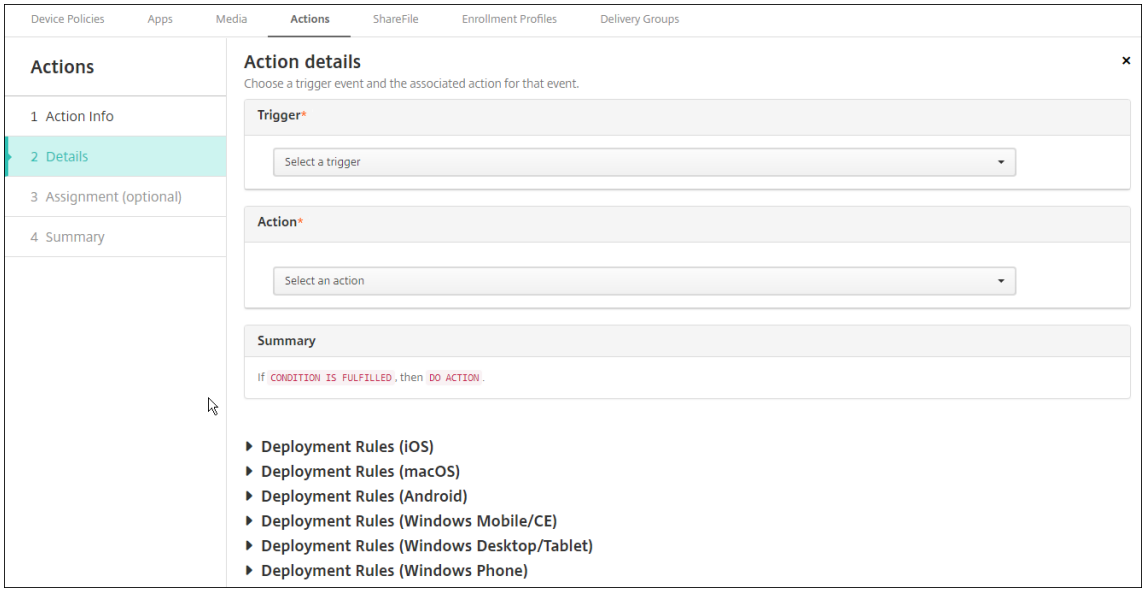
> **Conseil :**
>
> Pour supprimer des appareils inactifs en bloc, utilisez l'API publique des services REST. Vous obtenez d'abord manuellement les ID d'appareils pour les appareils inactifs que vous souhaitez supprimer, puis vous exécutez l'API delete pour les supprimer en bloc.

Ajouter et gérer des actions

Pour ajouter, modifier et filtrer des actions automatisées :

1. Dans la console XenMobile, cliquez sur **Configurer > Actions**. La page **Actions** s'affiche.
2. Sur la page **Actions**, effectuez l'une des actions suivantes :
   - Cliquez sur **Ajouter** pour ajouter une action.
   - Sélectionnez une action existante à modifier ou à supprimer. Cliquez sur l'option que vous voulez utiliser.
3. La page **Informations sur l'action** s'affiche.
4. Sur la page **Informations sur l'action**, entrez ou modifiez les informations suivantes :
   - **Nom :** entrez un nom permettant d'identifier l'action. Ce champ est obligatoire.
   - **Description :** décrivez ce que l'action doit faire.
5. Cliquez sur **Suivant**. La page sur les **Détails de l'action** s'affiche.

   L'exemple suivant illustre comment configurer un déclencheur **d'événement**. Si vous sélectionnez un autre déclencheur, les options sont différentes de celles affichées ici.



6. Sur la page **Détails de l'action**, entrez ou modifiez les informations suivantes :

Dans la liste des **Déclencheurs**, cliquez sur le type de déclencheur d'événements pour cette action. Signification des déclencheurs :

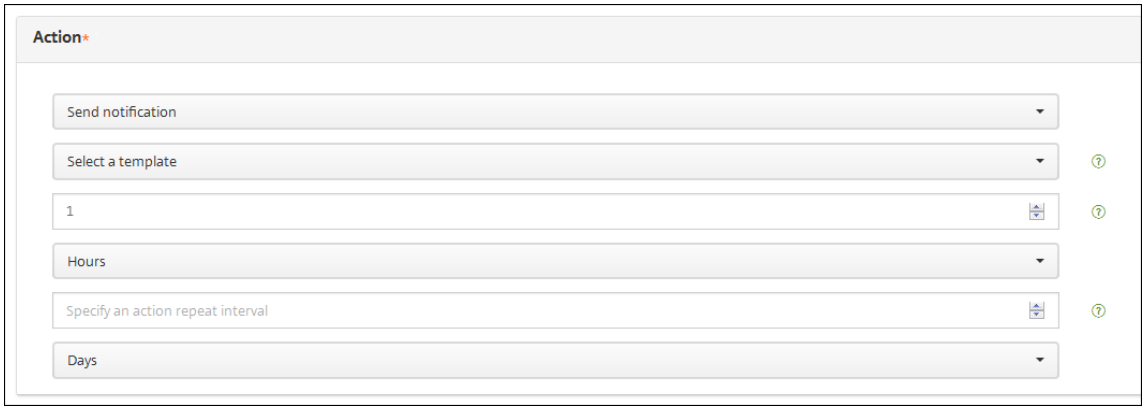
- **Événement :** réagit à un événement prédéfini.
- **Propriété de l'appareil :** recherche un attribut d'appareil sur l'appareil géré par MDM et y réagit. Pour de plus amples informations, consultez la section Noms et valeurs des propriétés d'appareil.
- **Propriété utilisateur :** réagit à un attribut utilisateur, généralement à partir d'Active Directory.
- **Nom de l'application installée :** réagit à une application installée. Ne s'applique pas au mode MAM exclusif. Requiert que la stratégie d'inventaire des applications soit activée sur l'appareil. Par défaut, la stratégie d'inventaire des applications est activée sur toutes les plates-formes. Pour de plus amples informations, consultez la section Pour ajouter une stratégie d'inventaire des applications.

7. Dans la liste suivante, cliquez sur la réponse au déclencheur.
8. Dans la liste **Action**, cliquez sur l'action à effectuer lorsque le critère du déclencheur est rencontré. À l'exception de **Envoyer une notification**, vous choisissez un délai au cours duquel les utilisateurs devront avoir résolu le problème qui a activé le déclencheur. Si le problème n'est pas résolu dans ce délai, l'action sélectionnée est entreprise. Pour une définition des actions, consultez la section Actions de sécurisation.

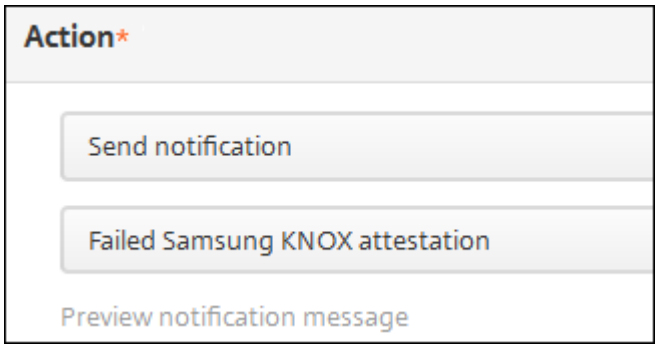
   Si vous sélectionnez **Envoyer une notification**, procédez comme suit pour envoyer une action de notification.

9. Dans la liste suivante, sélectionnez le modèle à utiliser pour la notification. Les modèles de notification correspondant à l'événement sélectionné apparaissent, sauf si aucun modèle n'existe pour le type de notification. Dans ce cas, le message suivant vous invite à configurer un modèle : Aucun modèle de notification pour ce type d'événement. Créez un modèle à l'aide de **Modèle de notification** dans **Paramètres**.

   Pour avertir les utilisateurs, vous devez avoir configuré les serveurs de notification dans Paramètres pour SMTP et SMS afin que XenMobile puisse envoyer des messages, consultez Notifications. Vous devez également configurer les modèles de notification que vous prévoyez d'utiliser avant de continuer. Pour de plus amples informations sur la configuration des modèles de notification, consultez la section Créer et mettre à jour des modèles de notification.



Après avoir sélectionné le modèle, vous pouvez afficher un aperçu de la notification en cliquant sur **Aperçu du message de notification**.



10. Dans les champs suivants, définissez le délai en jours, heures ou minutes avant d'effectuer l'action. Définissez l'intervalle auquel l'action se répète jusqu'à ce que l'utilisateur corrige le problème déclencheur.

11. Dans **Résumé**, vérifiez que vous avez créé les actions automatisées comme prévu.

12. Après avoir configuré les détails de l'action, vous pouvez configurer des règles de déploiement pour chaque plate-forme individuellement. Pour ce faire, suivez l'étape 13 pour chacune des plates-formes que vous choisissez.

13. Configurez les règles de déploiement. Pour des informations générales sur la configuration des règles de déploiement, consultez la section Déployer des ressources.

    Pour cet exemple :

    - Le propriétaire de l'appareil doit être **BYOD**.
    - Le chiffrement local de l'appareil doit être **True**.
    - L'appareil doit avoir un code secret conforme.
    - Le code de pays mobile de l'appareil ne peut pas être uniquement Andorre.

14. Lorsque vous avez terminé de configurer les règles de déploiement par plate-forme pour l'action, cliquez sur **Suivant**. La page d'**attribution d'actions** s'affiche. Sur cette page, vous pouvez attribuer l'action à un ou plusieurs groupes de mise à disposition. Cette étape est facultative.

15. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

16. Développez Calendrier de déploiement et configurez les paramètres suivants :

    - En regard de **Déployer**, cliquez sur **Activé** pour planifier le déploiement ou cliquez sur **Désactivé** pour empêcher le déploiement. L'option par défaut est **Activé**. Si vous choisissez **Désactivé**, aucune autre option n'est requise.
    - En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
    - Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    - En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
    - En regard de **Déployer pour les connexions permanentes**, cliquez sur **Activé** ou **Désactivé**. L'option par défaut est **Désactivé**.

      Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.

    Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

17. Cliquez sur **Suivant**. La page **Résumé** s'affiche, où vous pouvez vérifier la configuration de l'action.

18. Cliquez sur **Enregistrer** pour enregistrer l'action.

Actions de verrouillage et d'effacement des applications en mode MAM uniquement

Vous pouvez effacer ou verrouiller les applications d'un appareil en réponse à quatre catégories de déclencheurs répertoriées dans la console XenMobile : événement, propriété de l'appareil, propriété utilisateur et nom de l'application installée.

Pour configurer le déclenchement automatique de l'effacement des applications ou du mode kiosque

1. Dans la console XenMobile, cliquez sur **Configurer > Actions**.
2. Sur la page **Actions**, cliquez sur **Ajouter**.
3. Sur la page **Informations sur l'action**, entrez un nom pour l'action et une description facultative.
4. Sur la page **Détails de l'action**, sélectionnez le déclencheur de votre choix.
5. Dans **Action**, sélectionnez une action.

   Pour cette étape, tenez compte des conditions suivantes :

   Lorsque le type de déclencheur est **Événement** et que la valeur n'est pas Utilisateur **Active Directory désactivé**, les actions **Effacement des applications** et **Mode kiosque** ne s'affichent pas.

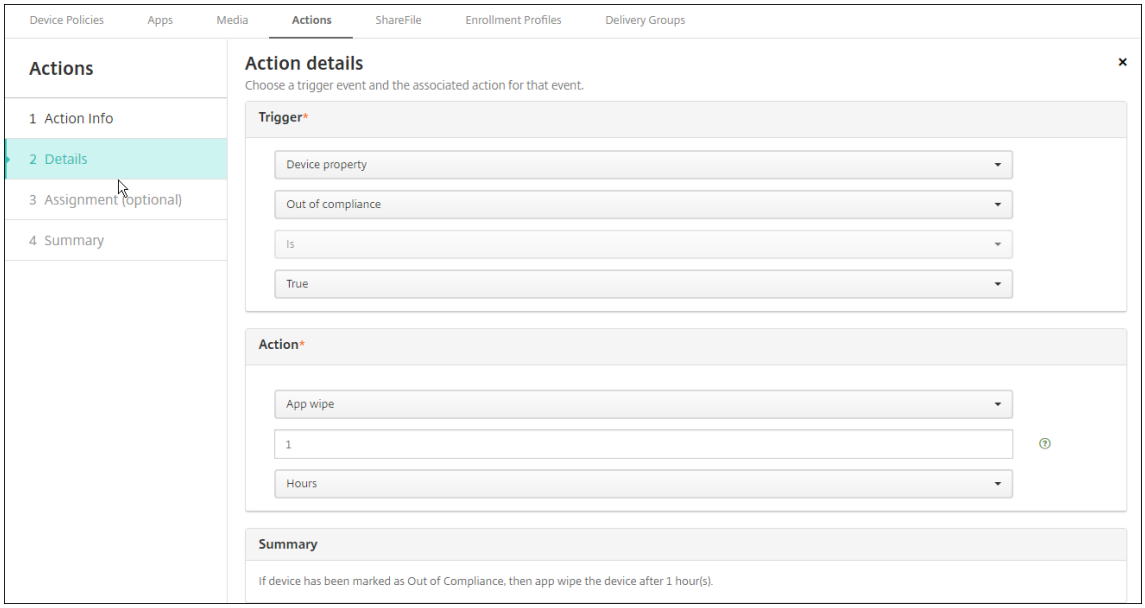
   Lorsque le type de déclencheur est **Propriété de l'appareil** et que la valeur est **Mode perdu MDM activé**, les actions suivantes ne s'affichent pas :

   - Effacer les données d'entreprise de l'appareil
   - Effacer toutes les données de l'appareil
   - Révoquer l'appareil

   Pour chaque option, un délai de 1 heure est automatiquement défini, mais vous pouvez sélectionner la durée de ce délai en minutes, heures ou jours. Le but du délai est de donner aux utilisateurs le temps de résoudre un problème avant que l'action ne se produise. Pour plus d'informations sur les actions de réinitialisation de l'application et de verrouillage de l'application, voir Actions de sécurité.

   > **Remarque :**
   >
   > Si vous définissez le déclencheur sur **Événement**, l'intervalle de répétition est réglé automatiquement sur un minimum d'1 heure. L'appareil doit actualiser les stratégies pour se synchroniser avec le serveur pour que la notification soit envoyée. En règle générale,

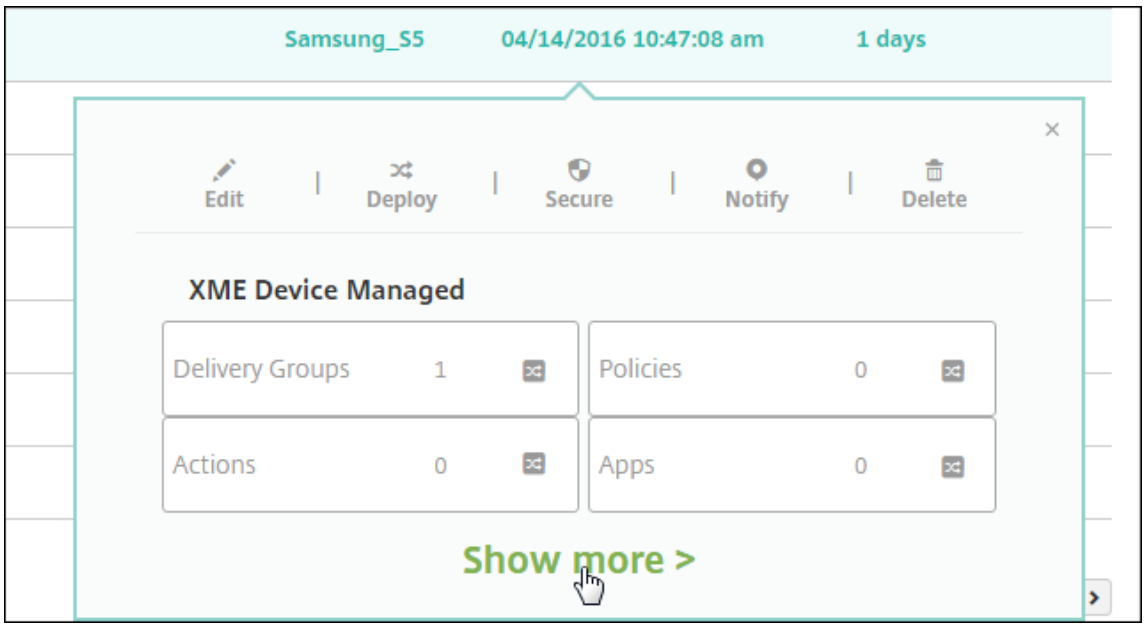
> un appareil se synchronise avec le serveur lorsque les utilisateurs se connectent ou actualisent manuellement leurs stratégies Secure Hub.
>
> Un délai supplémentaire d'environ une heure avant l'exécution de l'action est également possible, afin de permettre la synchronisation de la base de données Active Directory avec XenMobile.



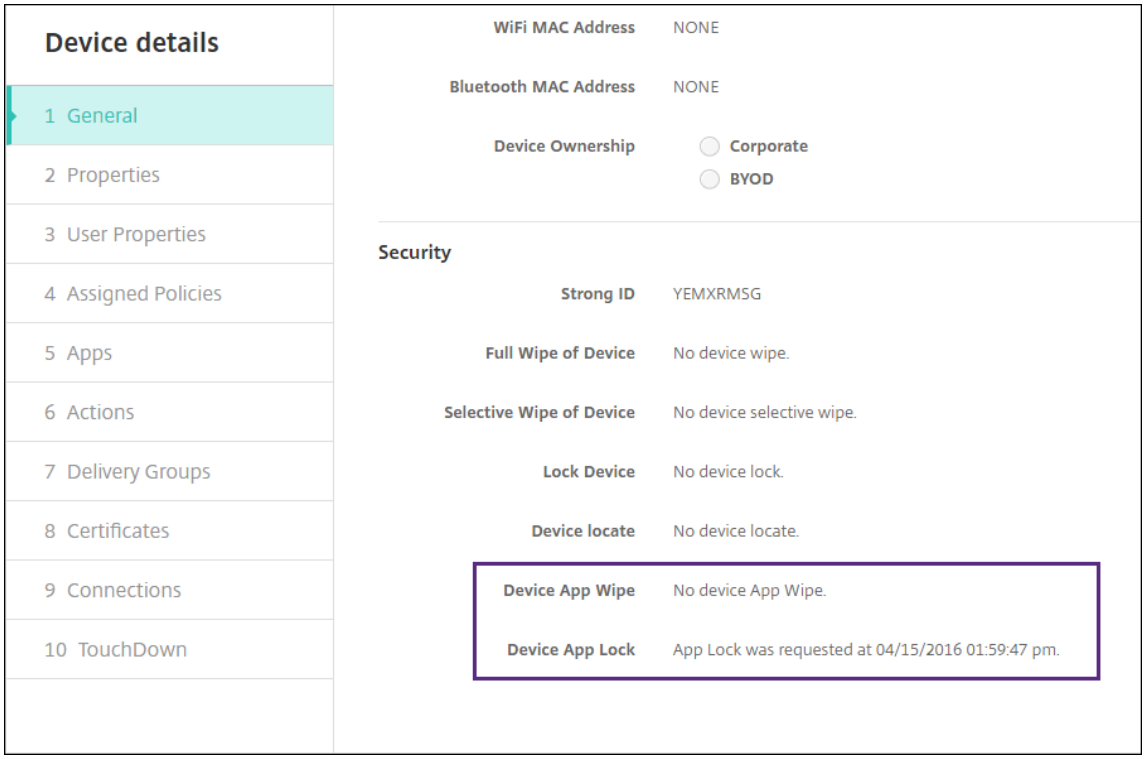
6. Configurez les règles de déploiement, puis cliquez sur **Suivant**.
7. Configurez les attributions de groupe de mise à disposition et un calendrier de déploiement, puis cliquez sur **Suivant**.
8. Cliquez sur **Enregistrer**.

Pour vérifier l'état de verrouillage ou d'effacement d'une application

1. Accédez à **Gérer > Appareils**, cliquez sur un appareil et sur **Afficher plus**.



2. Faites défiler jusqu'à **Effacement des applications sur l'appareil** et **Mode kiosque sur l'appareil**.



Une fois qu'un appareil est effacé, l'utilisateur est invité à entrer un code PIN. Si l'utilisateur oublie le code, vous pouvez le rechercher dans Détails de l'appareil.

Surveillance et support

January 10, 2022

Vous pouvez utiliser le tableau de bord de XenMobile et la page Support de XenMobile afin de contrôler et de résoudre les problèmes de votre serveur XenMobile. Utilisez la page Support de XenMobile pour accéder à des informations et outils de support.

Avec un serveur XenMobile Server sur site, vous pouvez également effectuer des actions à partir de la CLI XenMobile. Pour de plus amples informations, consultez la section Options d'interface de ligne de commande.

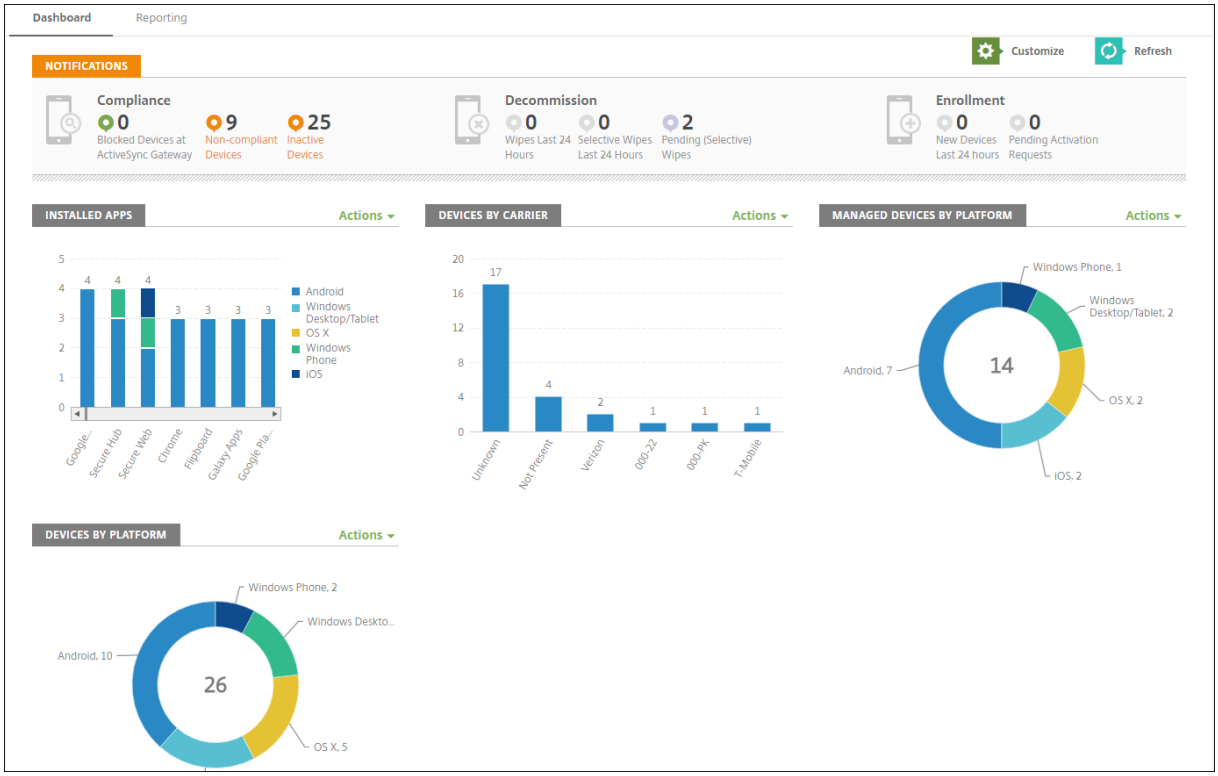
Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit.

La page Dépannage et support s'ouvre.

Utilisez la page **Support** de XenMobile pour :

- Accéder aux diagnostics.
- Créer des packs d'assistance (uniquement pour les installations sur site).
- Accéder aux liens de la documentation produit et du centre de connaissances Citrix.
- Accéder au journal des opérations.
- Utiliser les options de configuration avancée.
- Accéder à un ensemble d'outils et d'utilitaires.

Vous pouvez également afficher un synopsis des informations en accédant au tableau de bord de votre console XenMobile. Avec ces informations, vous pouvez voir un aperçu rapide des problèmes et des résolutions en utilisant des widgets.



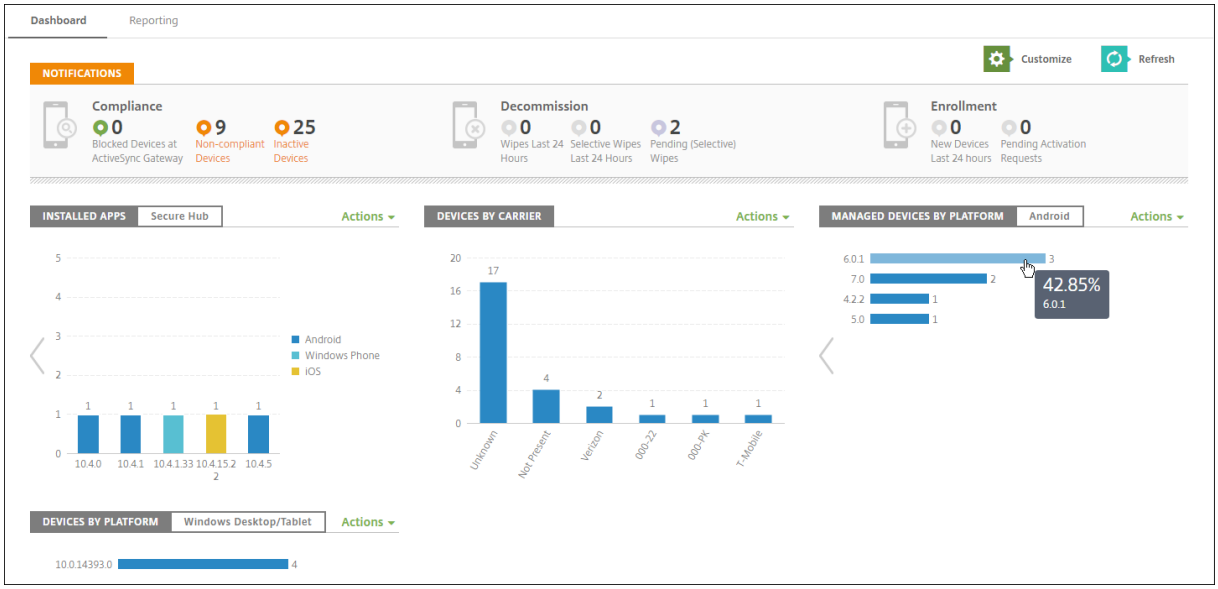
Le tableau de bord est généralement la page qui s'affiche lorsque vous vous connectez à la console XenMobile. Pour accéder au tableau de bord ailleurs dans la console, cliquez sur **Analyser**. Cliquez sur **Personnaliser** dans le tableau de bord pour modifier la configuration de la page et pour modifier les widgets qui s'affichent.

- **Mes tableaux de bord :** vous pouvez enregistrer jusqu'à quatre tableaux de bord. Vous pouvez modifier ces tableaux de bord séparément et afficher chacun d'entre eux en sélectionnant le tableau de bord enregistré.
- **Disposition :** dans cette ligne, vous pouvez sélectionner le nombre de widgets qui s'affichent sur votre tableau de bord et la manière dont les widgets sont disposés.
- **Sélection des widgets :** vous pouvez choisir les informations qui s'affichent dans votre tableau de bord.
  - **Notifications :** cochez la case au-dessus des chiffres sur la gauche pour ajouter une barre Notifications au-dessus de vos widgets. Cette barre affiche le nombre d'appareils compatibles, d'appareils inactifs et d'appareils effacés ou inscrits dans les dernières 24 heures.
  - **Appareils par plate-forme :** affiche le nombre d'appareils gérés et non gérés par plate-forme.
  - **Appareils par opérateurs :** affiche le nombre d'appareils gérés et non gérés par opérateur. Cliquez sur chaque barre pour afficher la répartition par plate-forme.
  - **Appareils gérés par plate-forme :** affiche le nombre d'appareils gérés par plate-forme.
  - **Appareils non gérés par plate-forme :** affiche le nombre d'appareils non gérés par plate-forme. Les appareils qui s'affichent dans ce graphique peuvent avoir un agent installé,

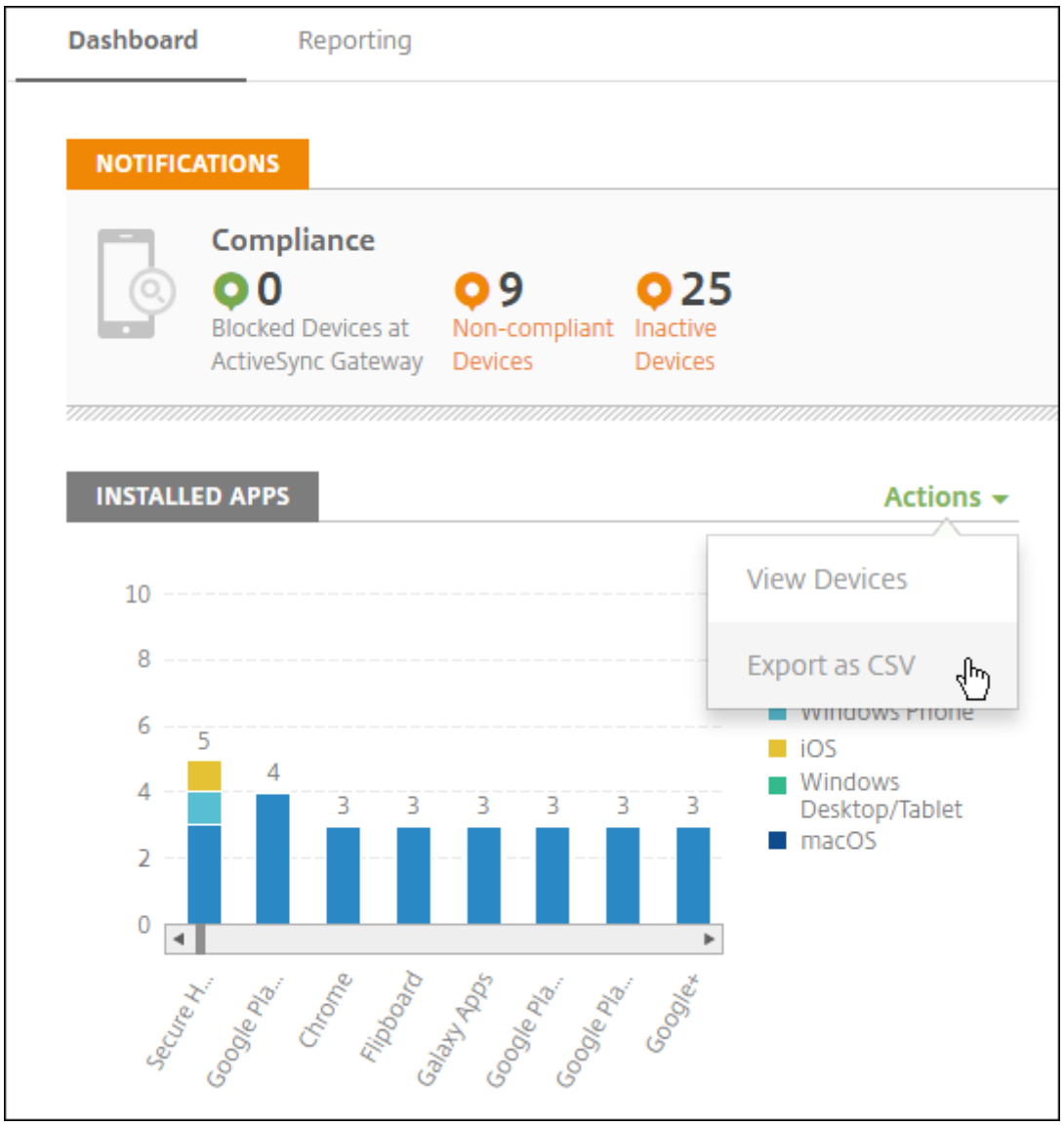
mais leurs privilèges ont été révoqués ou ils ont été effacés.

- **Appareils par état ActiveSync Gateway :** affiche le nombre d'appareils regroupés par état ActiveSync Gateway. Les informations affichent l'état Inconnu, Autorisé ou Bloqué. Vous pouvez cliquer sur chaque barre pour décomposer les données par plate-forme.
- **Appareils par appartenance :** affiche le nombre d'appareils regroupés par état d'appartenance. Les informations affichent l'état Appartenant à la société, Appartenant à l'employé ou Inconnu.
- **Déploiements de groupes de mise à disposition ayant échoué :** affiche le nombre total d'échecs de déploiements par package. Seuls les packages avec des échecs de déploiements s'affichent.
- **Appareils par motif de blocage :** affiche le nombre d'appareils bloqués par ActiveSync
- **Applications installées :** entrez un nom d'application pour un graphique des informations sur l'application.
- **Licences utilisées par les applications d'achat en volume :** affiche des statistiques d'utilisation de licences pour les applications d'achat en volume d'Apple.

Avec chaque widget, vous pouvez cliquer sur les parties individuelles pour affiner les informations.



Vous pouvez également exporter les informations sous forme de fichier .csv en cliquant sur le menu déroulant **Action**.



Anonymiser les données dans les packs d'assistance

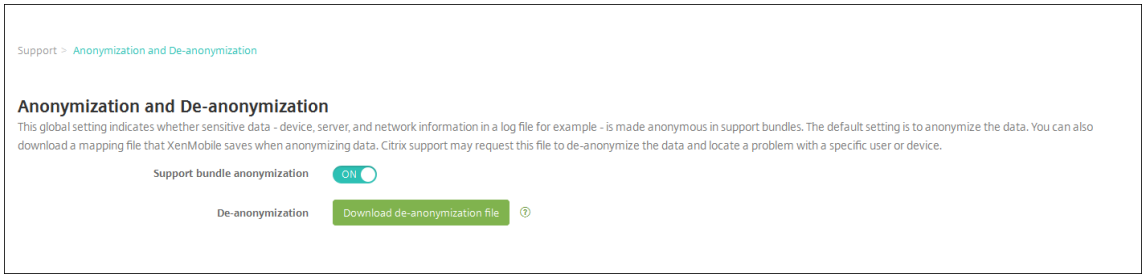
April 25, 2019

Lorsque vous créez des packs d'assistance dans XenMobile, les données sensibles liées aux utilisateurs, serveurs et réseaux sont rendues anonymes par défaut. Vous pouvez modifier ce comportement sur la page Anonymisation et réidentification. Vous pouvez également télécharger un fichier de mappage que XenMobile enregistre lors de l'anonymisation des données. Le support Citrix peut avoir besoin de ce fichier pour réidentifier les données et localiser un problème avec un utilisateur ou un appareil spécifique.

1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page

Support s'affiche.

2. Sur la page **Support**, sous **Avancé**, cliquez sur **Anonymisation et réidentification**. La page **Anonymisation et réidentification** s'affiche.



3. Dans **Anonymisation du pack d'assistance**, sélectionnez si les données sont anonymes. La valeur par défaut est **Activé**.
4. En regard de **Réidentification**, cliquez sur **Télécharger le fichier de réidentification** pour télécharger le fichier de mappage à envoyer au service de support Citrix lorsqu'il a besoin d'informations spécifiques sur l'appareil ou l'utilisateur pour diagnostiquer un problème.

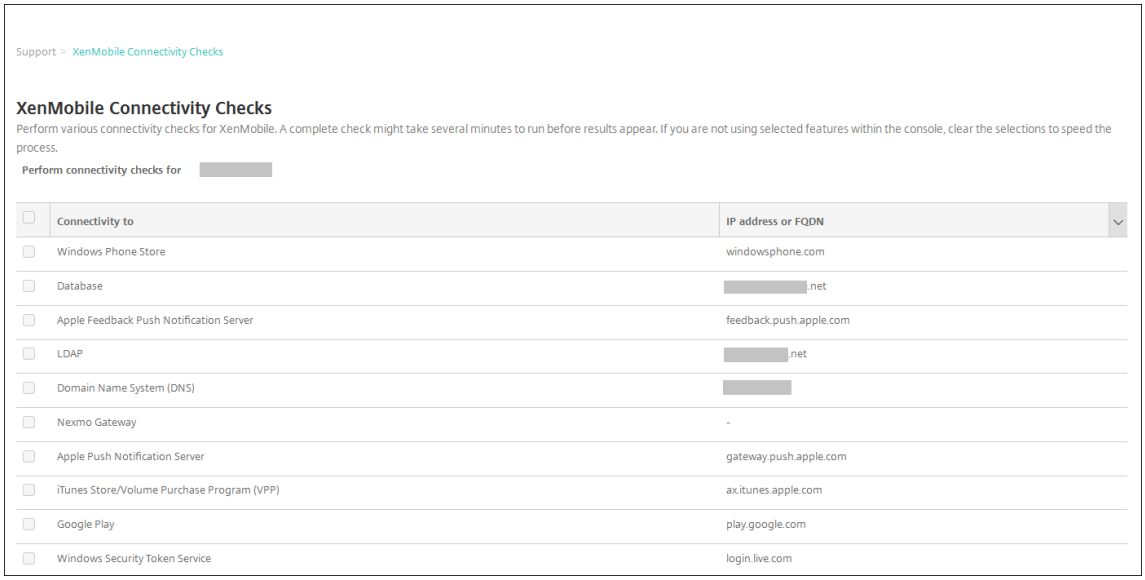
Tests de connectivité

November 11, 2020

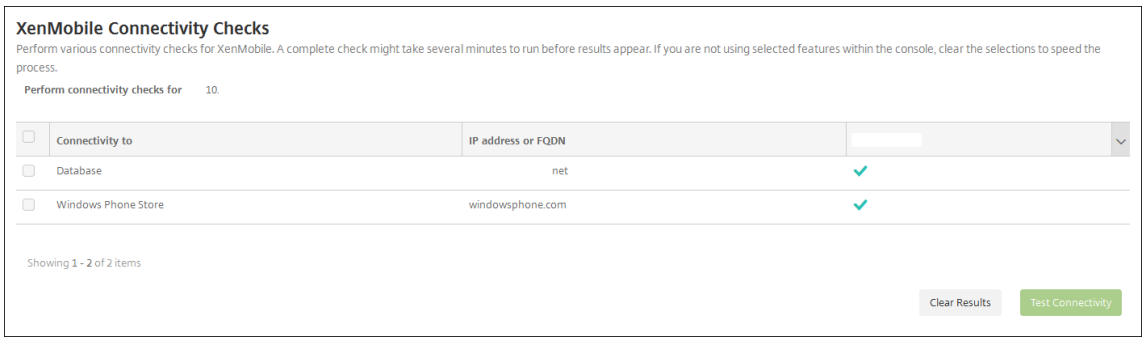
Depuis la page **Support** de XenMobile, vous pouvez vérifier la connexion de XenMobile à Citrix Gateway et à d'autres serveurs et emplacements.

Réalisation de contrôles de connectivité dans XenMobile

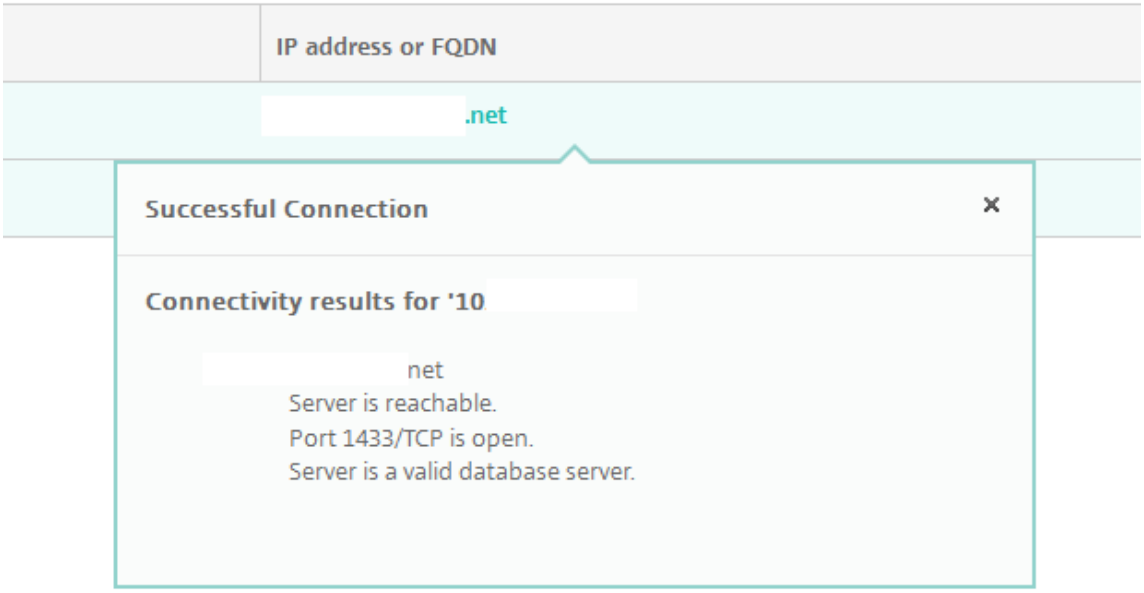
1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Support** s'affiche.
2. Sous **Diagnostics**, cliquez sur **Test de la connectivité XenMobile**. La page **Test de la connectivité XenMobile** s'affiche. Si votre environnement XenMobile contient des nœuds en cluster, tous les nœuds sont affichés.



3. Sélectionnez les serveurs que vous souhaitez inclure dans le test de connectivité, puis cliquez sur **Tester la connectivité**. La page des résultats du test s'affiche.

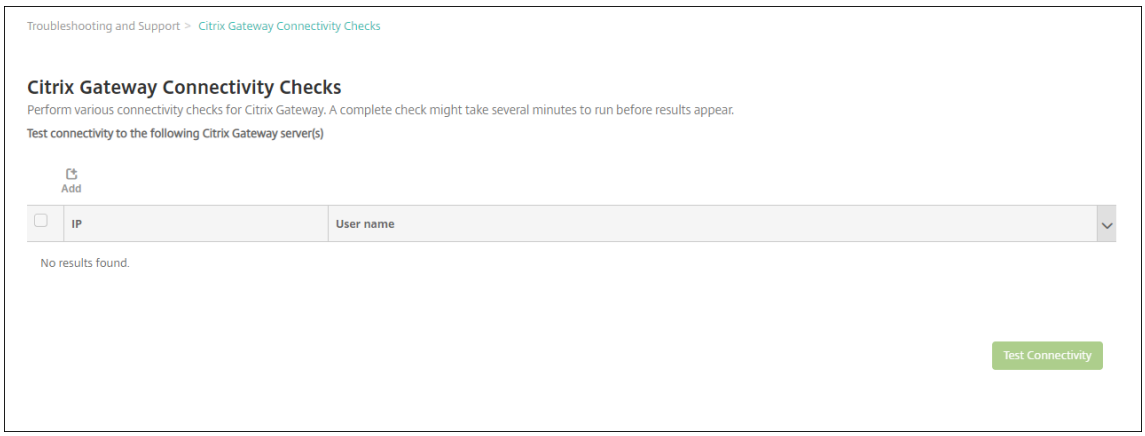


4. Sélectionnez un serveur dans le tableau des résultats du test pour afficher les résultats détaillés pour ce serveur.

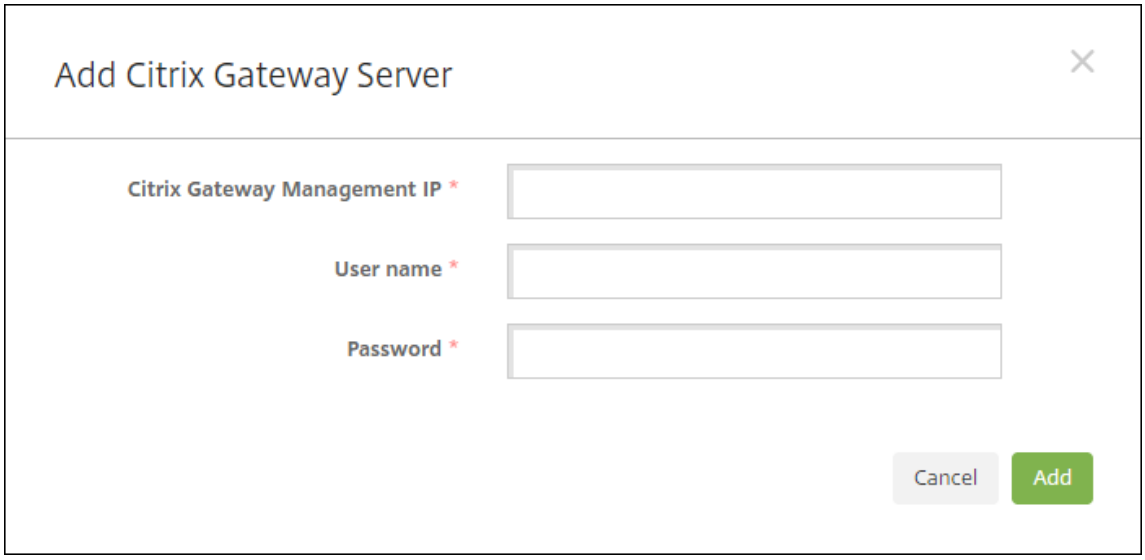


Réalisation de tests de la connectivité Citrix Gateway

1. Sur la page **Support**, sous **Diagnostics**, cliquez sur **Test de la connectivité Citrix Gateway** . La page **Test de la connectivité Citrix Gateway** s'affiche. Le tableau est vide si vous n'avez pas ajouté de serveurs Citrix Gateway.



2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un serveur Citrix Gateway** s'affiche.



3. Dans **IP de gestion de Citrix Gateway**, entrez l'adresse IP de gestion du serveur exécutant Citrix Gateway que vous voulez tester.

   > **Remarque :**
   >
   > Si vous effectuez un test de connectivité pour un serveur Citrix Gateway qui a déjà été ajouté, l'adresse IP est renseignée.

4. Tapez vos informations d'identification d'administrateur pour cette instance de Citrix Gateway.

   > **Remarque :**
   >
   > Si vous effectuez un contrôle de connectivité pour un serveur Citrix Gateway qui a déjà été ajouté, le nom d'utilisateur est renseigné.

5. Cliquez sur **Ajouter**. La passerelle Citrix Gateway est ajoutée au tableau sur la page **Test de la connectivité Citrix Gateway**.
6. Sélectionnez le serveur Citrix Gateway et cliquez sur **Tester la connectivité**. Les résultats du test s'affichent dans un tableau.
7. Sélectionnez un serveur dans le tableau des résultats du test pour afficher les résultats détaillés pour ce serveur.

Programme d'amélioration de l'expérience utilisateur

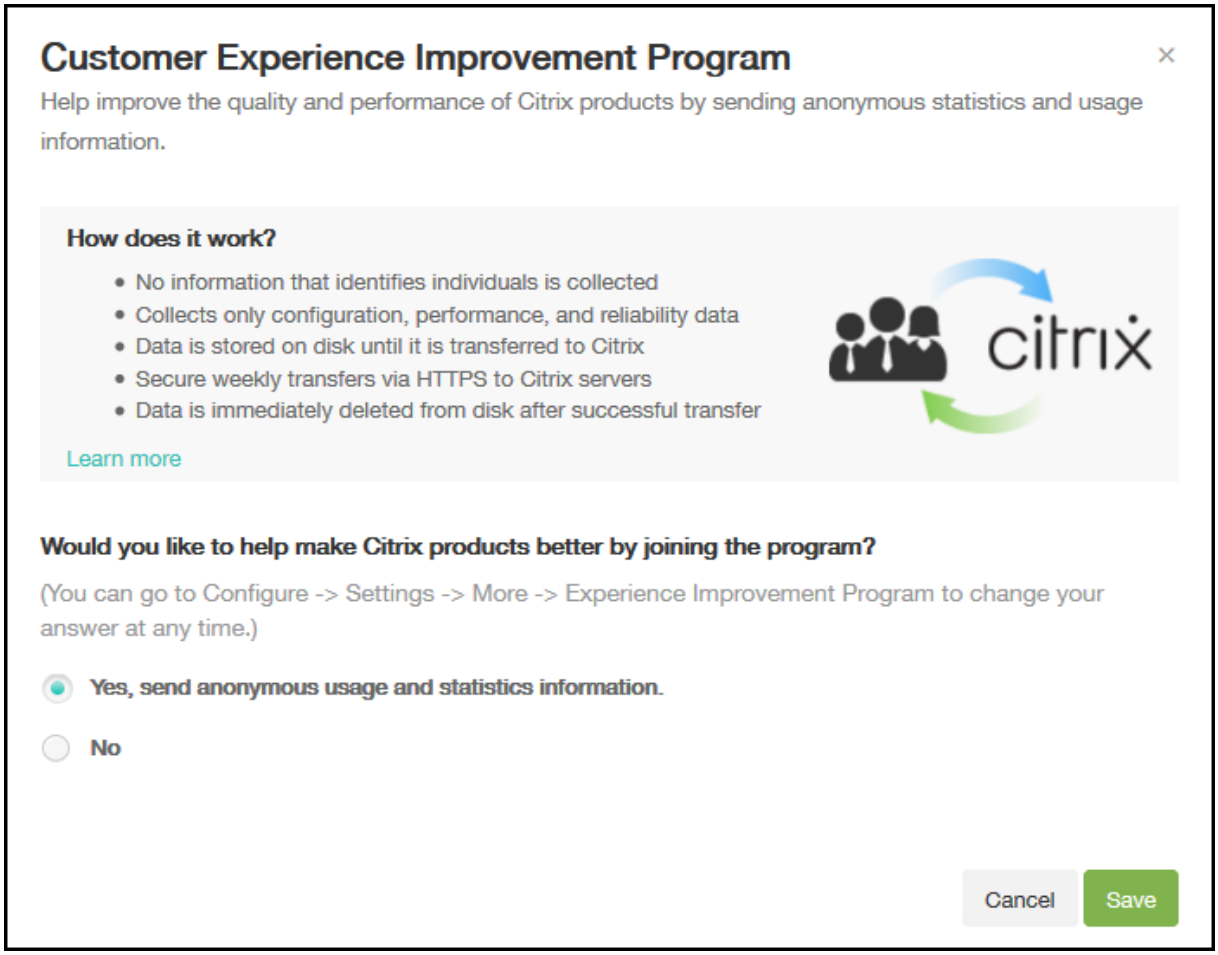
January 10, 2022

Le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) rassemble des données de configuration et d'utilisation anonymes à partir de XenMobile et les envoie automatiquement à Citrix.

Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de XenMobile. La participation au programme CEIP est complètement volontaire. Lorsque vous installez XenMobile pour la première fois, ou lorsque vous installez une mise à jour, vous avez la possibilité de participer au programme CEIP. Lorsque vous acceptez de participer, les données de configuration sont généralement recueillies chaque semaine, et les données relatives aux performances et à l'utilisation sont recueillies toutes les heures. Les données sont stockées sur disque et transférées de manière sécurisée via HTTPS à Citrix une fois par semaine. Vous pouvez modifier votre participation au programme CEIP dans la console XenMobile. Pour plus d'informations sur le programme CEIP, veuillez consulter la section À propos du Programme d'amélioration de l'expérience utilisateur Citrix (CEIP).

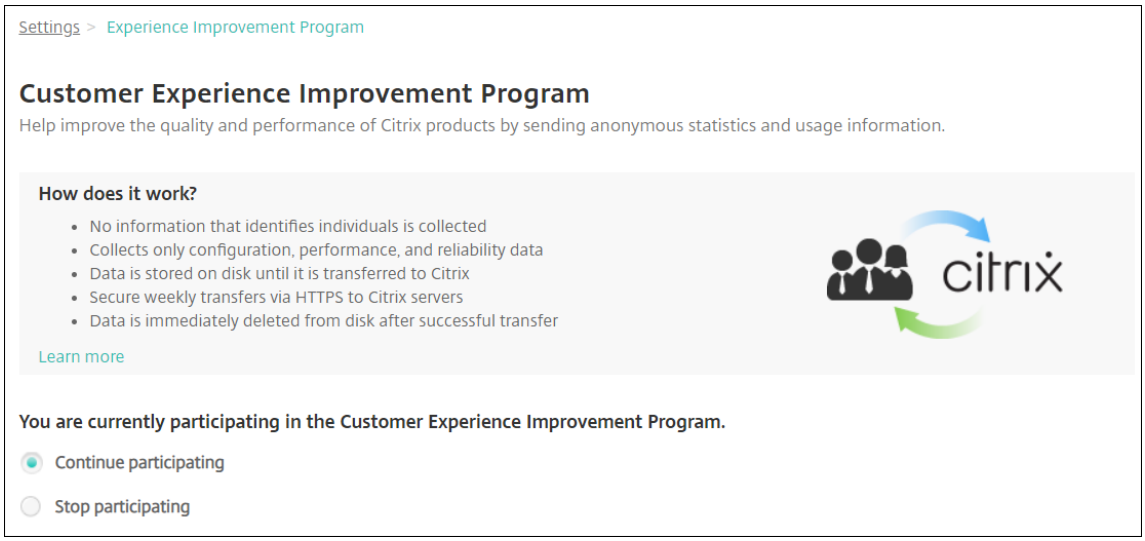
Choisir de participer au programme CEIP

La première fois que vous installez XenMobile ou lorsque vous effectuez une mise à jour, la boîte de dialogue suivante vous invite à participer au programme.



Modification de votre paramètre de participation au programme CEIP

1. Pour modifier votre paramètre de participation au programme CEIP, dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console pour ouvrir la page **Paramètres**.
2. Dans **Serveur**, cliquez sur **Programme d'amélioration de l'expérience utilisateur**. La page **Programme d'amélioration de l'expérience utilisateur** s'affiche. La page exacte qui s'affiche change selon que vous participez au programme CEIP ou non.



3. Si vous participez actuellement au programme CEIP et que vous voulez arrêter, cliquez sur **Ne plus participer au programme**.
4. Si vous ne participez pas actuellement au programme CEIP et que vous voulez y adhérer, cliquez sur **Participer au programme**.
5. Cliquez sur **Enregistrer**.

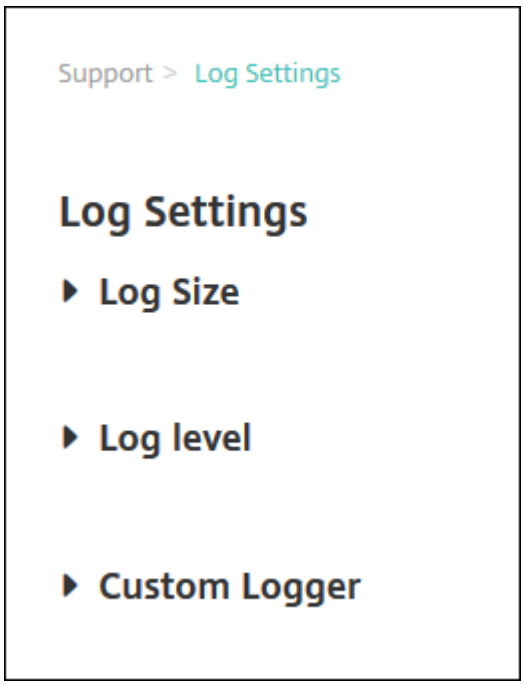
Journaux

January 10, 2022

Vous pouvez configurer les paramètres du journal pour personnaliser les journaux générés par XenMobile. Si vous avez mis en cluster les serveurs XenMobile, lorsque vous configurez les paramètres de journal dans la console XenMobile, ces paramètres sont partagés avec tous les autres serveurs dans le cluster.

1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Support** s'affiche.

2. Sous **Opérations du journal**, cliquez sur **Paramètres du journal**. La page **Paramètres du journal** s'affiche.

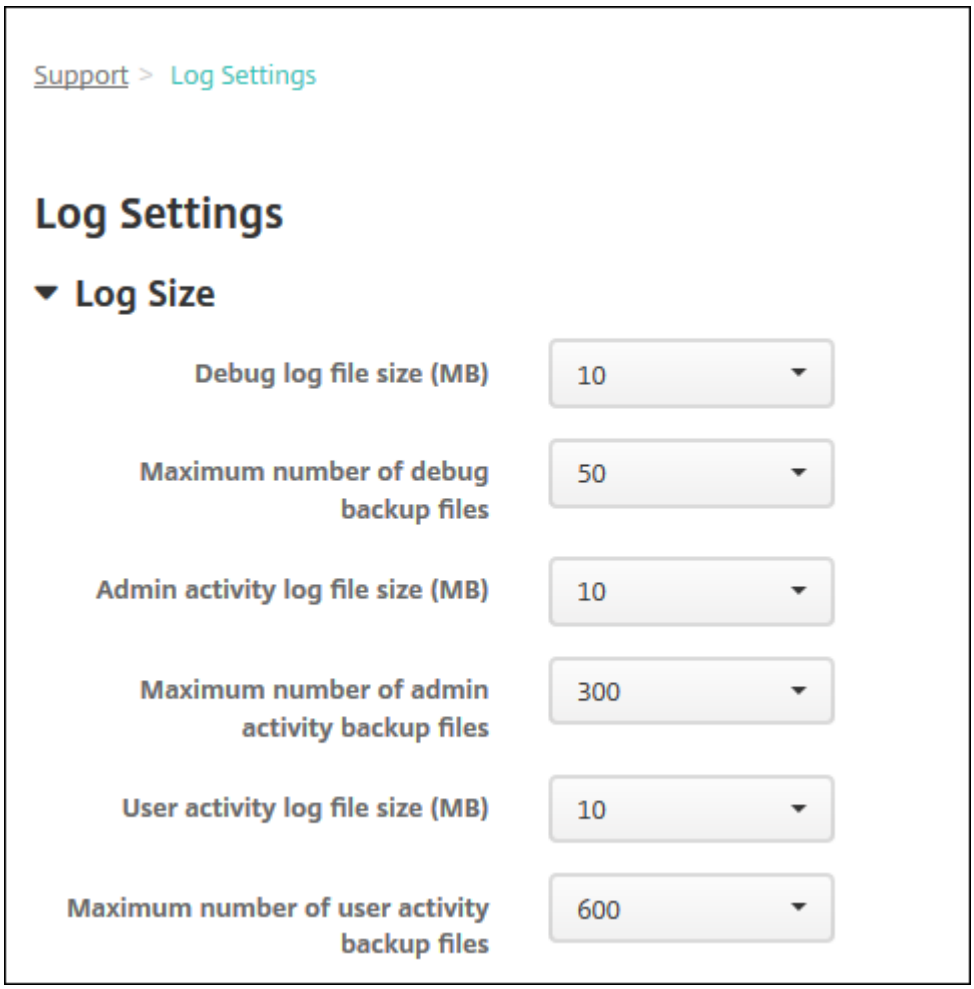


Sur la page **Paramètres du journal**, vous pouvez accéder aux options suivantes :

- **Taille du journal**. Utilisez cette option pour contrôler la taille du fichier journal et le nombre maximal de fichiers de sauvegarde du journal conservés dans la base de données. La taille du journal s'applique à tous les journaux pris en charge par XenMobile (journal de débogage, journal des activités de l'administrateur et journal des activités de l'utilisateur).
- **Niveau du journal**. Utilisez cette option pour modifier le niveau de journalisation ou pour conserver les paramètres.
- **Enregistreur d'événements personnalisé**. Utilisez cette option pour créer un enregistreur d'événements personnalisé ; un journal personnalisé requiert un nom de classe et un niveau de journalisation.

Pour configurer les options de taille du journal

1. Sur la page **Paramètres du journal**, développez **Taille du journal**.



2. Pour configurer ces paramètres :

   - **Taille du fichier journal de débogage (Mo) :** dans la liste, sélectionnez une taille comprise entre 5 et 20 Mo pour modifier la taille maximale du fichier de débogage. La valeur par défaut de la taille du fichier est de **10 Mo**.
   - **Nombre maximum de fichiers de sauvegarde de débogage :** dans la liste, cliquez sur le nombre maximal de fichiers de débogage conservés par le serveur. Par défaut, XenMobile conserve 50 fichiers de sauvegarde sur le serveur.
   - **Taille du fichier journal des activités des administrateurs (Mo) :** dans la liste, sélectionnez une taille comprise entre 5 et 20 Mo pour modifier la taille maximale du fichier des activités des administrateurs. La valeur par défaut de la taille du fichier est de **10 Mo**.
   - **Nombre maximum de fichiers de sauvegarde des activités des administrateurs :** dans la liste, cliquez sur le nombre maximal des fichiers d'activités des administrateurs conservés par le serveur. Par défaut, XenMobile conserve 300 fichiers de sauvegarde sur le serveur.
   - **Taille du fichier journal des activités des utilisateurs (Mo) :** dans la liste, sélectionnez une taille comprise entre 5 et 20 Mo pour modifier la taille maximale du fichier des activités

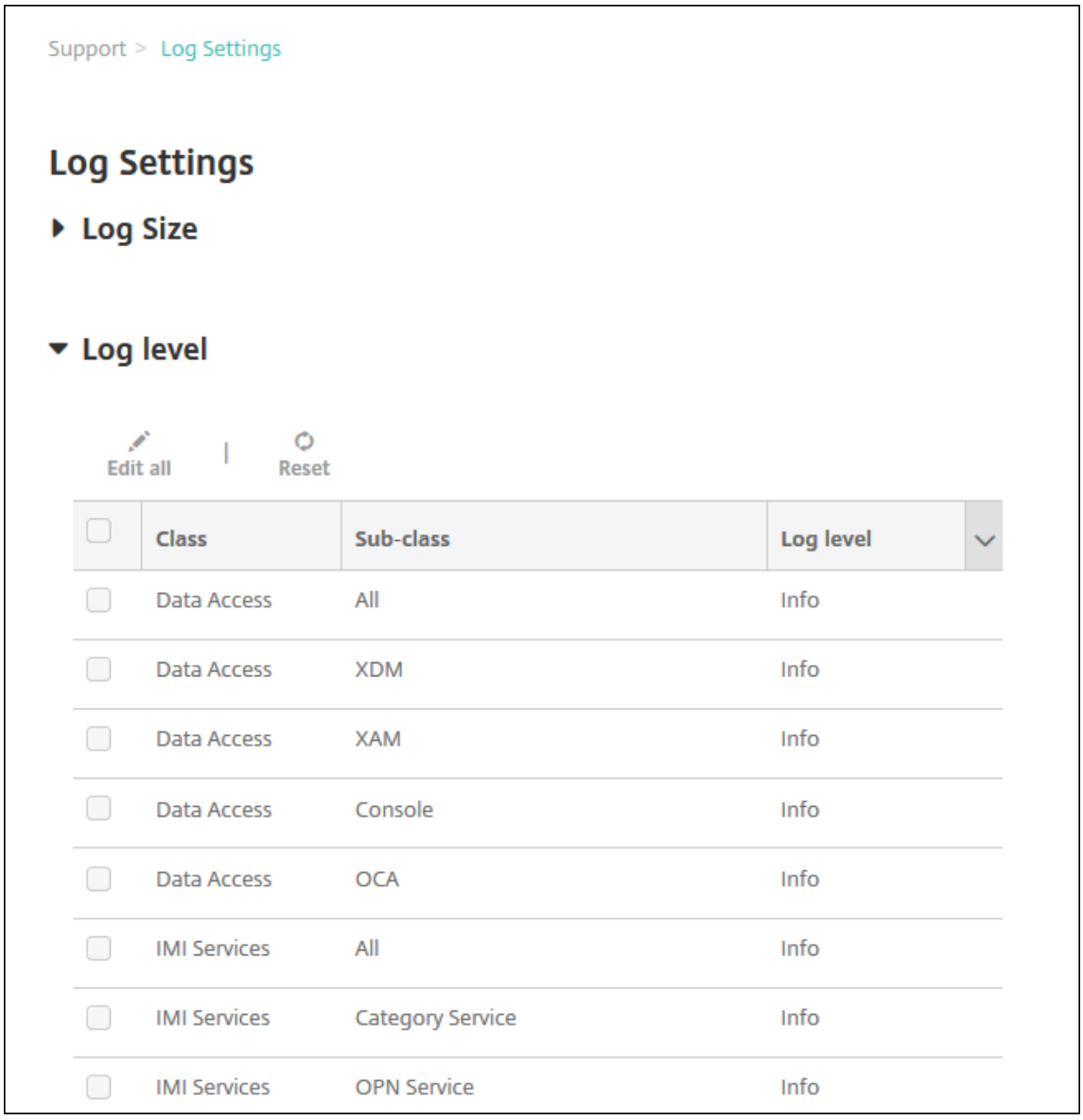
des utilisateurs. La valeur par défaut de la taille du fichier est de **10 Mo**.

- **Nombre maximum de fichiers de sauvegarde des activités des utilisateurs :** dans la liste, cliquez sur le nombre maximal des fichiers d'activités des utilisateurs conservés par le serveur. Par défaut, XenMobile conserve 300 fichiers de sauvegarde sur le serveur.

Pour configurer les options de niveau de journalisation

Le niveau de journalisation vous permet de spécifier le type d'informations que XenMobile collecte dans le journal. Vous pouvez définir le même niveau pour toutes les classes ou vous pouvez définir des niveaux spécifiques pour des classes individuelles.

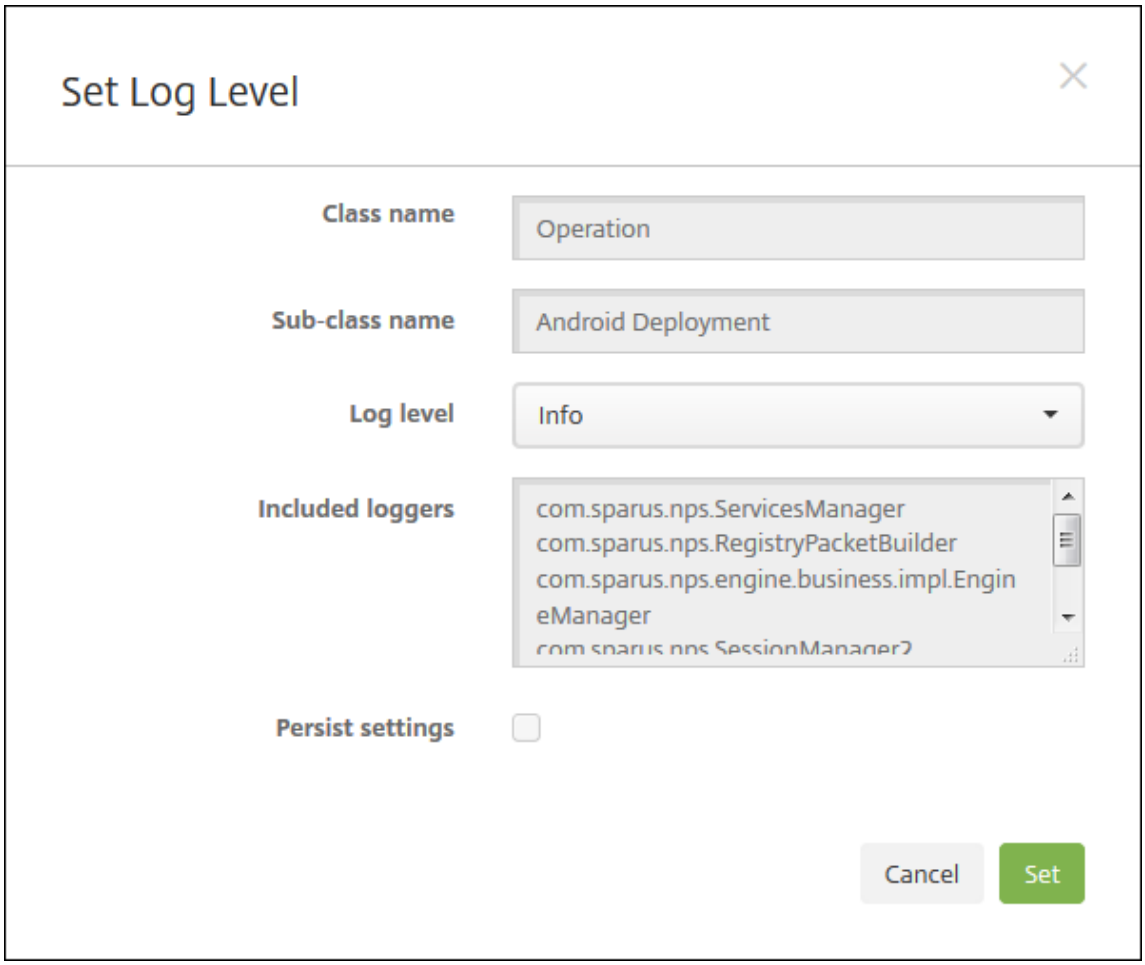
1. Sur la page **Paramètres du journal**, développez **Niveau de journalisation**. Un tableau de toutes les classes de journal s'affiche.



2. Procédez comme suit :

   - Cliquez sur la case à cocher en regard de Classe, puis cliquez sur **Définir le niveau** pour modifier uniquement le niveau de journalisation de cette classe.
   - Cliquez sur **Tout modifier** pour appliquer la modification apportée au niveau de journalisation à toutes les classes dans le tableau.

   La boîte de dialogue **Définir le niveau du journal** qui s'affiche vous permet de définir le niveau de journalisation et d'indiquer si les paramètres associés doivent être conservés lors du redémarrage de XenMobile Server.



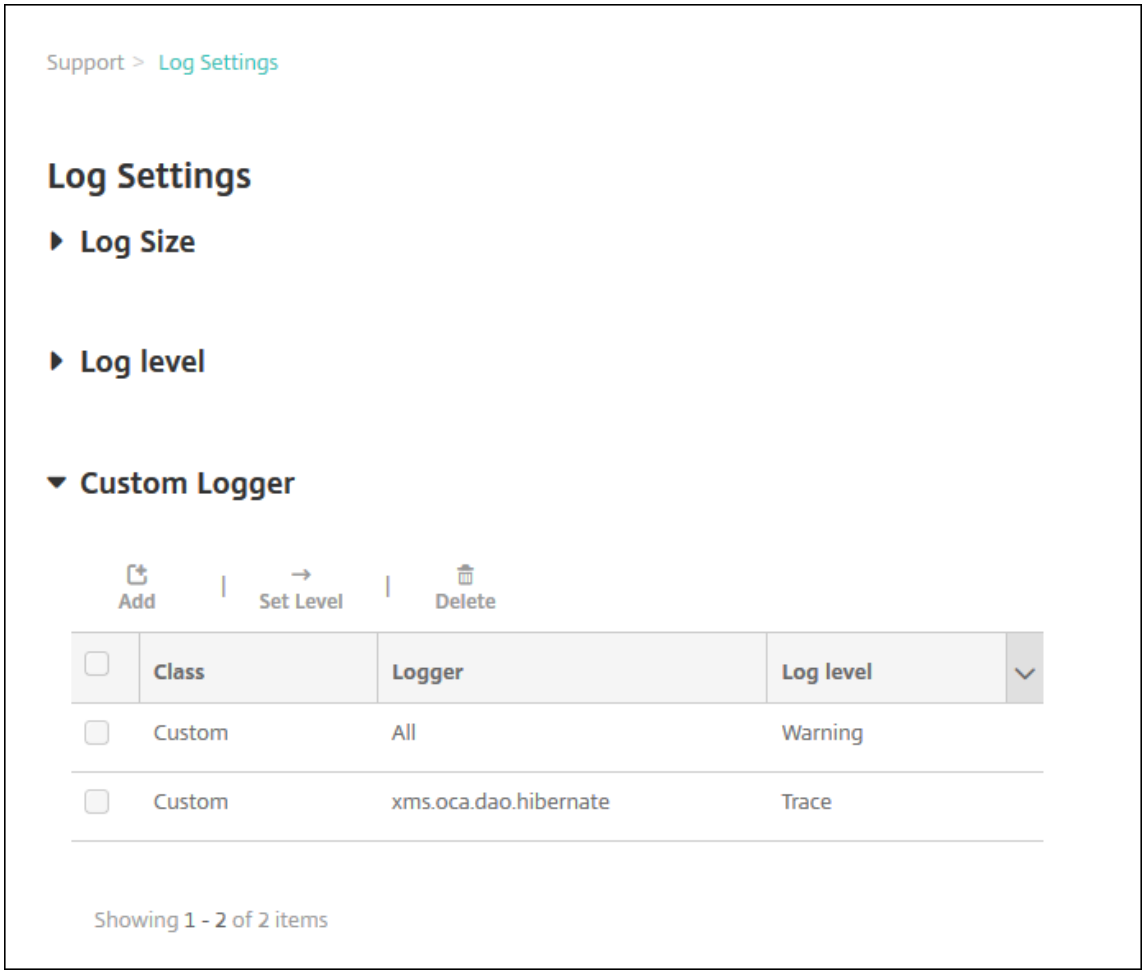
   - **Nom de la classe :** ce champ affiche Tout lorsque vous modifiez le niveau de journalisation pour toutes les classes ou il affiche le nom de la classe individuelle ; il n'est pas modifiable.
   - **Nom de la sous-classe :** ce champ affiche Tout lorsque vous modifiez le niveau de journalisation pour toutes les classes ou il affiche le nom de la sous-classe individuelle ; il n'est pas modifiable.
   - **Niveau de journalisation :** dans la liste, cliquez sur un niveau de journalisation. Les niveaux de journalisation pris en charge sont les suivants :
     - Fatal

  - Error
  - Warning
  - Info
  - Débogage
  - Trace
  - Désactivé
- **Enregistreurs d'événements inclus :** ce champ est vide lorsque vous modifiez le niveau de journalisation pour toutes les classes ou il affiche les enregistreurs d'événements actuellement configurés pour une classe individuelle ; il n'est pas modifiable.
- **Conserver les paramètres :** si vous souhaitez conserver les paramètres de niveau de journalisation lorsque vous redémarrez le serveur, cochez cette case. Si vous ne sélectionnez pas cette case à cocher, cela indique que les paramètres de niveau de journalisation par défaut sont rétablis lorsque vous redémarrez le serveur.

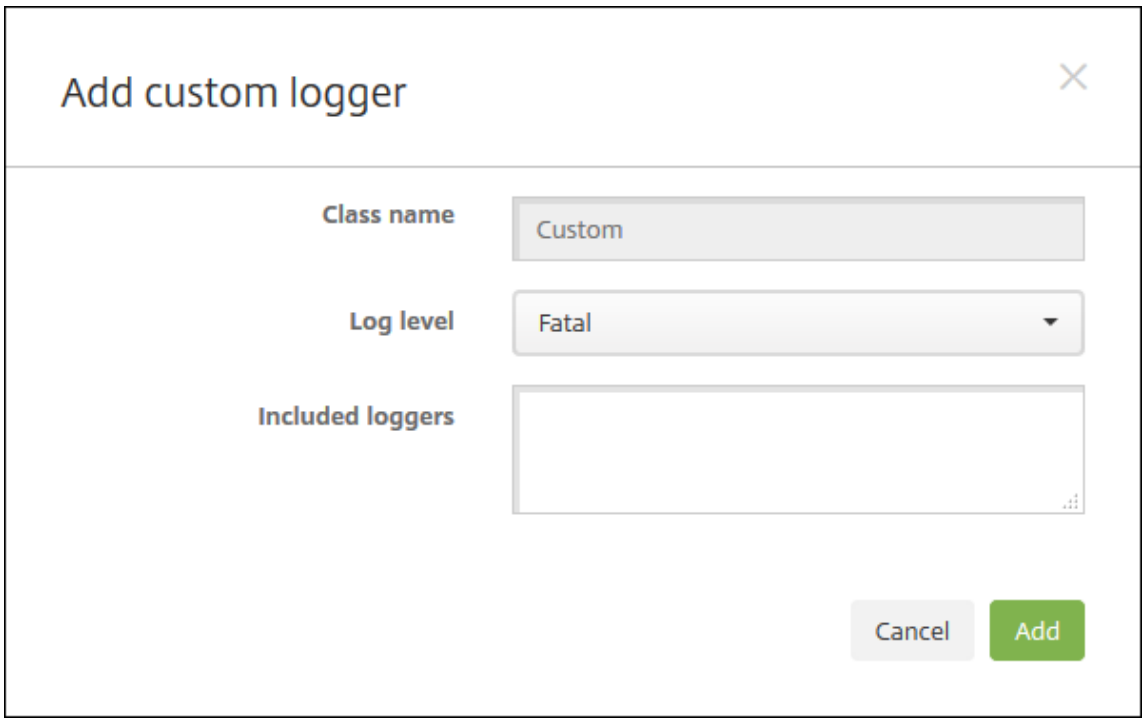
3. Cliquez sur **Définir** pour valider vos modifications.

Pour ajouter un enregistreur d'événements personnalisé

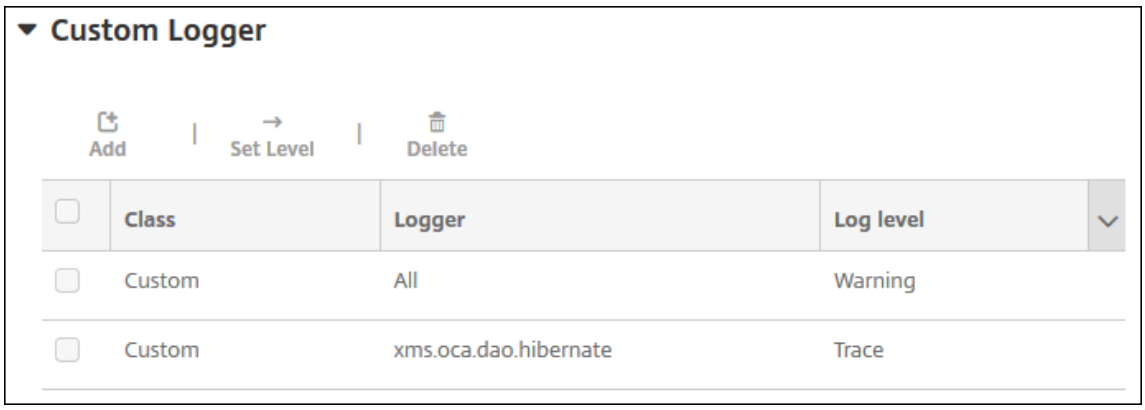
1. Sur la page **Paramètres du journal**, développez **Enregistreur d'événements personnalisé**. Le tableau **Enregistreur d'événements personnalisé** s'affiche. Si vous n'avez pas ajouté d'enregistreurs d'événements personnalisés, le tableau est initialement vide.



2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un enregistreur d'événements personnalisé** apparaît.



3. Pour configurer ces paramètres :
   - **Nom de la classe :** ce champ affiche **Personnaliser** ; il n'est pas modifiable.
   - **Niveau de journalisation :** dans la liste, cliquez sur un niveau de journalisation. Les niveaux de journalisation pris en charge sont les suivants :
     - Fatal
     - Error
     - Warning
     - Info
     - Débogage
     - Trace
     - Désactivé
   - **Enregistreurs d'événements inclus :** entrez les enregistreurs d'événements que vous souhaitez inclure dans l'enregistreur personnalisé ou laissez ce champ vide pour inclure tous les enregistreurs d'événements.
4. Cliquez sur **Ajouter**. L'enregistreur d'événements personnalisé est ajouté au tableau **Enregistreur d'événements personnalisé**.



Pour supprimer un enregistreur d'événements personnalisé

1. Sur la page **Paramètres du journal**, développez **Enregistreur d'événements personnalisé**.
2. Sélectionnez l'enregistreur d'événements personnalisé que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**. Une boîte de dialogue s'affiche vous demandant si vous souhaitez supprimer l'enregistreur d'événements personnalisé. Cliquez sur **OK**.

> **Important :**
>
> vous ne pouvez pas annuler cette opération.

Fournisseur de services mobiles

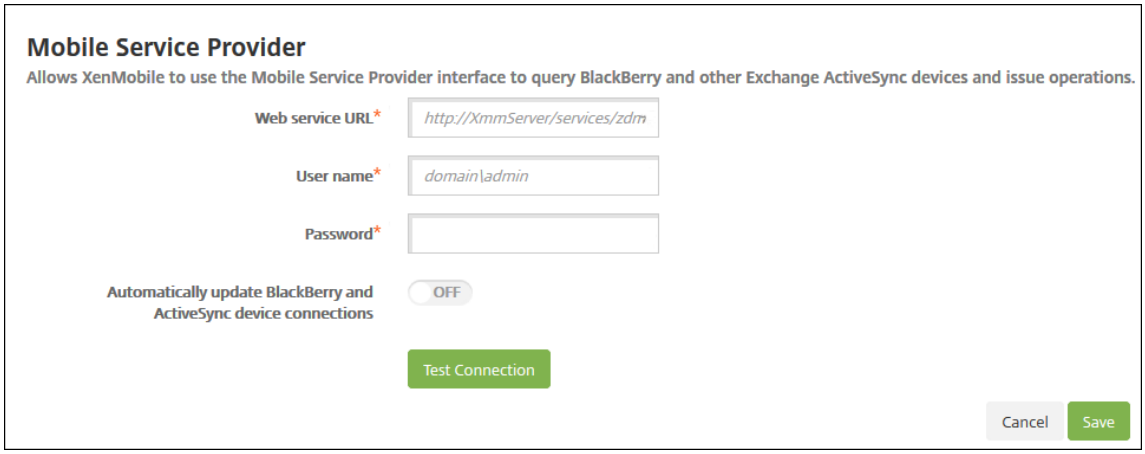
January 10, 2022

Vous pouvez configurer XenMobile de manière à ce qu'il utilise l'interface du fournisseur de services mobiles pour interroger les appareils BlackBerry et des appareils Exchange ActiveSync et effectuer des opérations.

Par exemple, votre entreprise peut compter plus de 1 000 utilisateurs et chaque utilisateur peut utiliser un ou plusieurs appareils. Lorsque vous signalez à chaque utilisateur qu'il doit inscrire ses appareils auprès de XenMobile à des fins de gestion, la console XenMobile indique le nombre d'appareils que les utilisateurs inscrivent. Si vous configurez ce paramètre, vous pouvez déterminer le nombre d'appareils qui se connectent au serveur Exchange. Cela vous permet d'effectuer ce qui suit :

- Déterminer si certains utilisateurs n'ont pas encore inscrit leurs appareils.
- Émettre des commandes sur les appareils utilisateur se connectant à un serveur Exchange, telles que l'effacement de données.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Dans **Serveur**, cliquez sur **Fournisseur de services mobiles**. La page **Fournisseur de services mobiles** s'affiche.



3. Pour configurer ces paramètres :
   - **URL du service Web :** entrez l'adresse URL du service Web, par exemple, `https://<XmmServer>/services/xdmservice`.
   - **Nom d'utilisateur :** entrez le nom d'utilisateur au format domaine\administrateur.
   - **Mot de passe :** entrez le mot de passe.
   - **Mettre à jour automatiquement les connexions aux appareils BlackBerry et ActiveSync :** activez cette option si vous souhaitez mettre à jour automatiquement les connexions aux appareils. La valeur par défaut est **Désactivé.**
   - Cliquez sur **Tester la connexion** pour vérifier la connexion.
4. Cliquez sur **Enregistrer**.

Rapports

August 10, 2020

XenMobile propose les rapports prédéfinis suivants qui vous permettent d'analyser vos déploiements d'applications et d'appareils. Chaque rapport s'affiche sous forme de tableau et de graphique. Vous pouvez trier et filtrer les tableaux par colonne. Vous pouvez sélectionner des éléments des graphiques à partir d'informations plus détaillées.

- **Nbre total de tentatives de déploiement d'application :** répertorie les applications déployées que les utilisateurs ont essayé d'installer sur leurs appareils.

- **Applications par plate-forme :** répertorie les applications et les versions des applications par plate-forme et version de l'appareil.
- **Application par type :** répertorie les applications par version, type et catégorie.
- **Inscription d'appareils :** répertorie tous les appareils inscrits.
- **Appareils et applications :** répertorie les appareils qui exécutent des applications gérées.
- **Appareils inactifs :** répertorie les appareils sans activité pendant le nombre de jours spécifié par la propriété device.inactivity.days.threshold de XenMobile Server.
- **Appareils jailbreakés/rootés :** répertorie les appareils iOS rootés et les appareils Android jailbreakés.
- **Termes et conditions :** répertorie les utilisateurs qui ont accepté et refusé les conditions générales. Vous pouvez sélectionner des zones du graphique pour afficher plus de détails.
- **Top 10 des applications :** échec du déploiement : répertorie le top 10 des applications dont le déploiement a échoué.
- **Applications sur liste noire par appareil et utilisateur :** répertorie les applications bloquées présentes sur les appareils des utilisateurs.

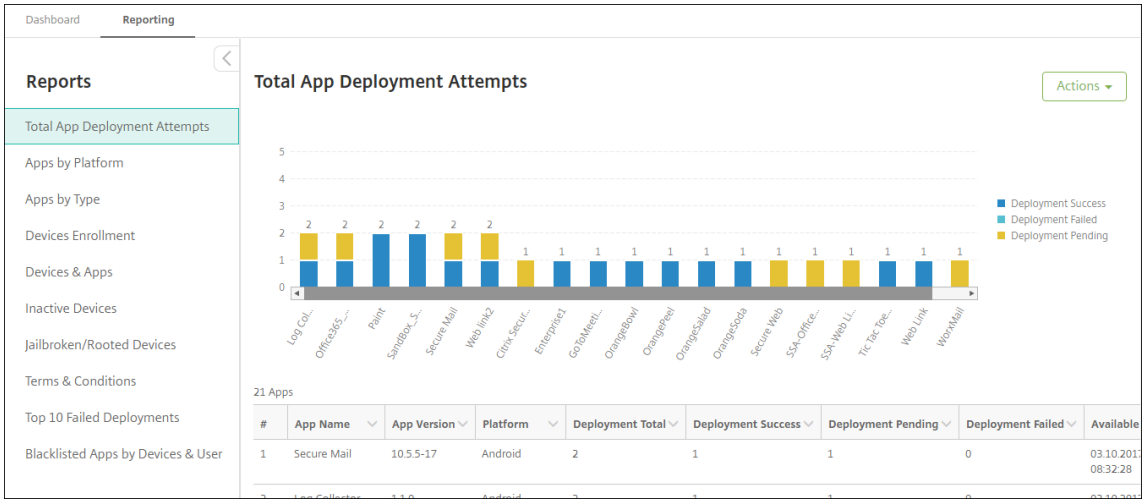
  > **Remarque :**
  >
  > La console XenMobile Server utilise les termes « liste noire » et « liste blanche ». Ces termes seront modifiés dans une prochaine version et les termes « liste de blocage » et « liste d'autorisation » les remplaceront.

- **Appareils non conformes :** répertorie les appareils qui ne répondent pas aux critères de conformité, par exemple si l'appareil est jailbreaké, si la version du système d'exploitation est en cours d'exécution et si l'appareil possède un code secret.

Vous pouvez exporter les données de chaque tableau au format .csv, que vous pouvez ouvrir à l'aide de programmes tels que Microsoft Excel. Vous pouvez exporter le graphique de chaque rapport au format PDF.

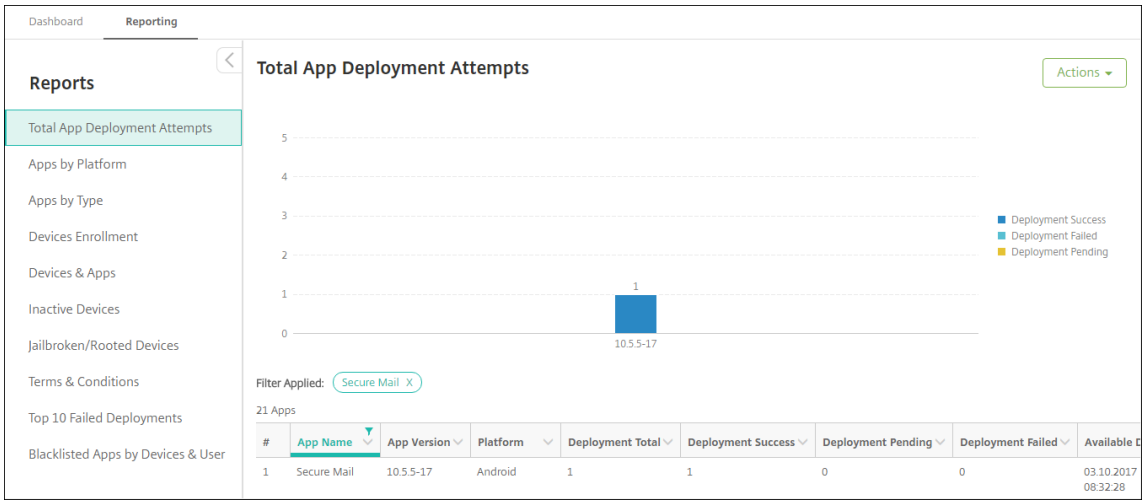
Pour générer un rapport

1. Dans la console XenMobile, cliquez sur l'onglet **Analyser > Rapports**. La page **Rapports** s'affiche.
2. Cliquez sur le rapport que vous souhaitez générer.

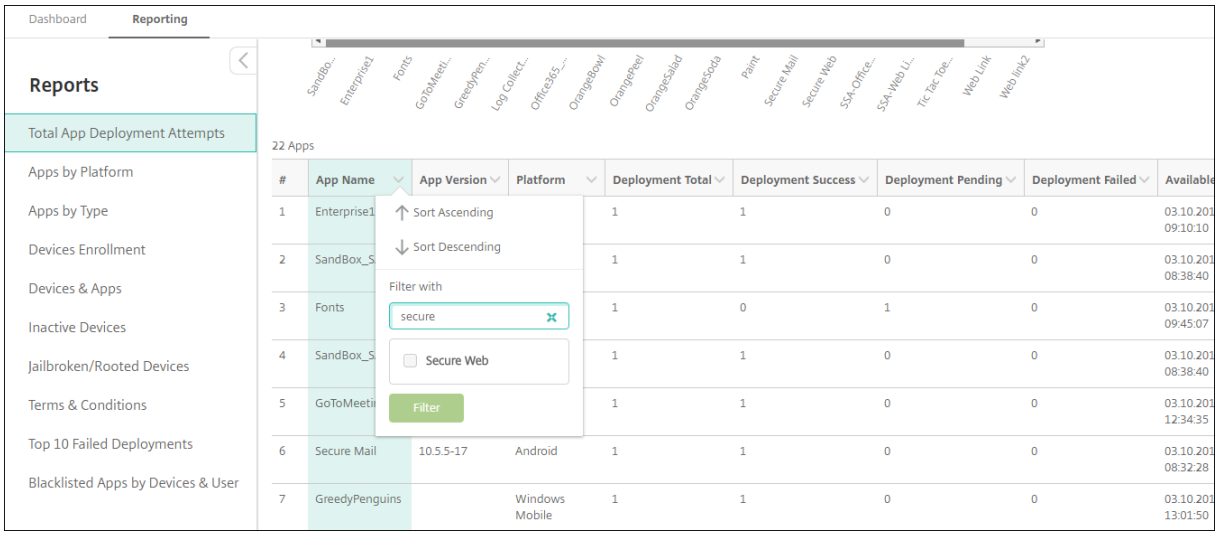


Pour afficher des détails supplémentaires dans un rapport

1. Cliquez sur les zones du graphique pour afficher des informations plus détaillées.

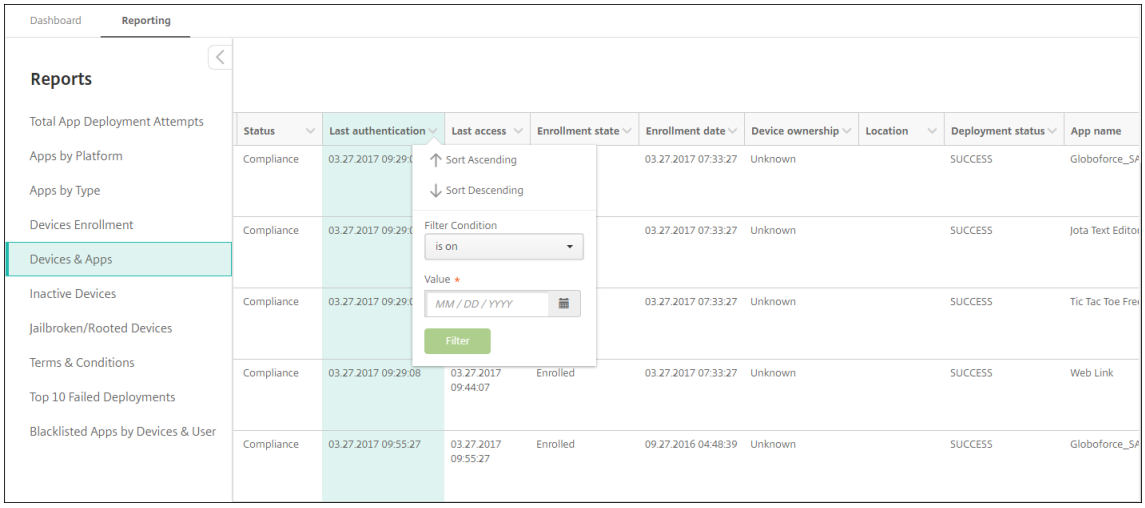


Pour trier, filtrer ou rechercher une colonne d'un tableau, cliquez sur l'en-tête de la colonne

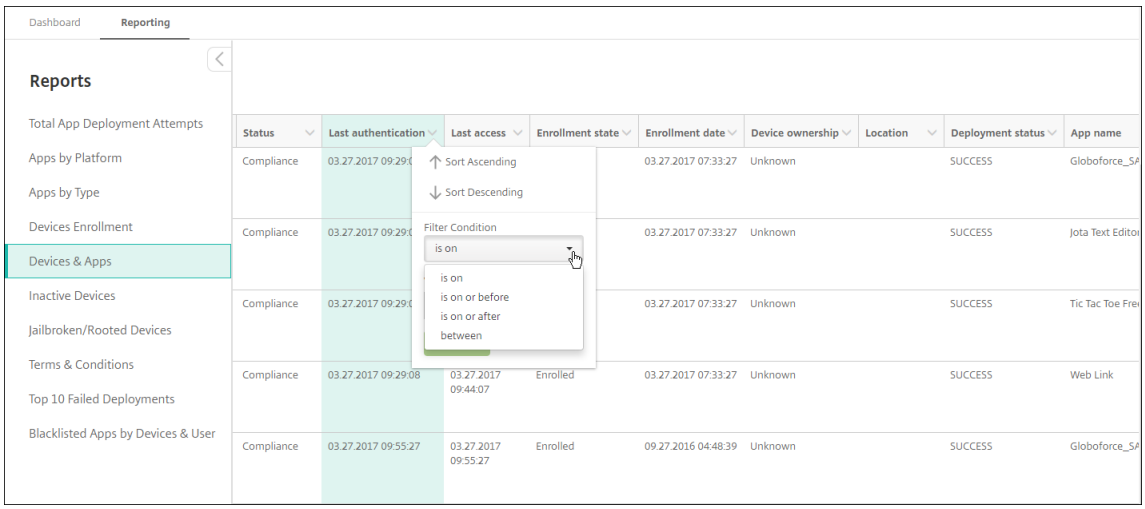


Pour filtrer le rapport par date

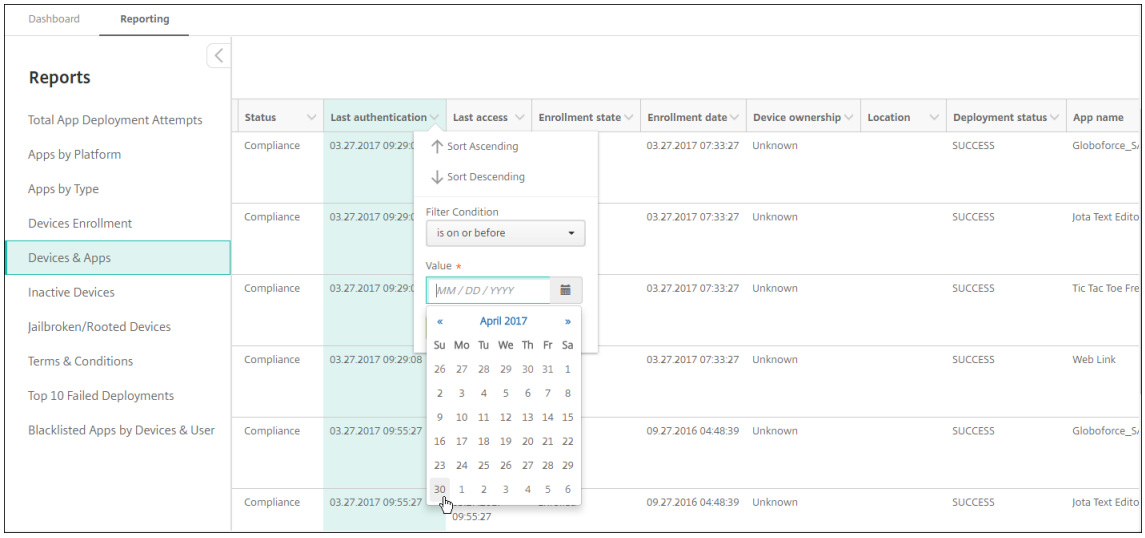
1. Cliquez sur un en-tête de colonne pour afficher les paramètres de filtre.



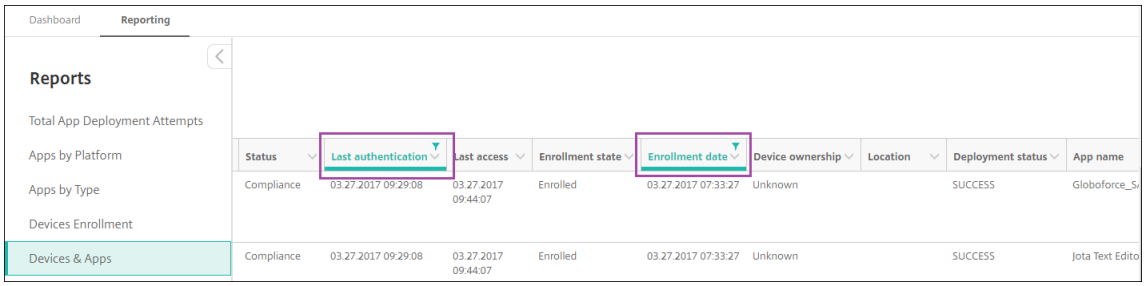
2. Dans **Condition de filtre**, choisissez la manière dont vous souhaitez restreindre les dates du rapport.



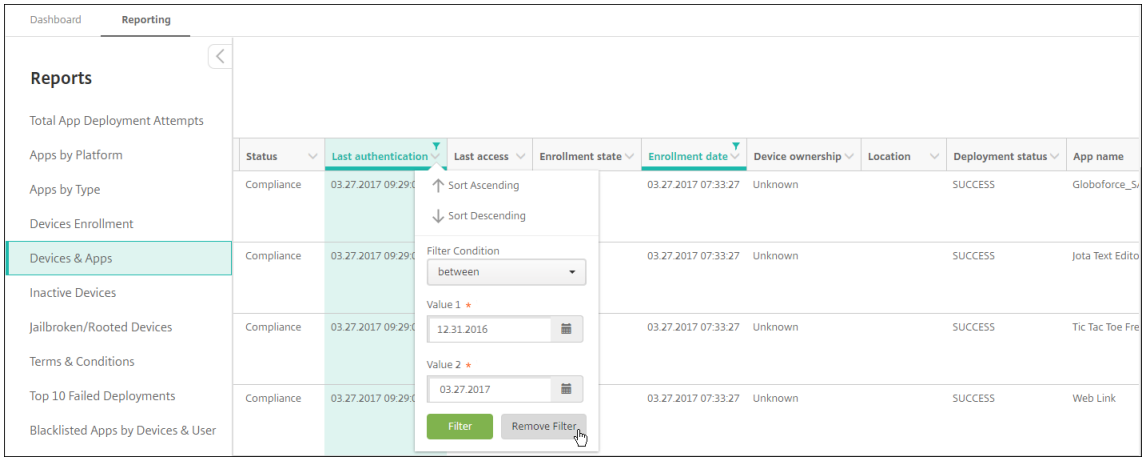
3. Utilisez le sélecteur de date pour spécifier les dates.



4. Une colonne avec un filtre de date s'affiche comme illustré dans l'exemple suivant.

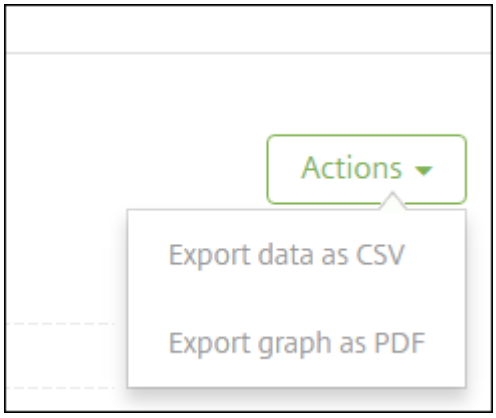


5. Pour supprimer un filtre, cliquez sur l'en-tête de colonne, puis cliquez sur **Supprimer le filtre**.



Pour exporter un graphique ou un tableau

- Pour exporter le graphique au format PDF, cliquez sur **Action** puis sur **Exporter graphique au format PDF**.
- Pour exporter les données du tableau au format CSV, cliquez sur **Action** puis sur **Exporter graphique au format CVS**.



> **Important :**
>
> Bien qu'il soit possible d'utiliser SQL Server pour créer des rapports personnalisés, Citrix ne recommande pas cette méthode. Citrix ne publie pas le schéma et peut modifier le schéma sans notification. Si vous décidez d'utiliser cette méthode de création de rapports, assurez-vous que les requêtes SQL sont exécutées à l'aide d'un compte en lecture seule. Veuillez noter qu'une requête avec plusieurs clauses JOIN qui prend un certain temps à s'exécuter aura un impact sur les performances de XenMobile Server durant son exécution.

Surveillance SNMP

January 10, 2022

Vous pouvez activer la surveillance SNMP dans XenMobile Server pour permettre aux systèmes de surveillance d'interroger et d'obtenir des informations sur vos nœuds XenMobile. Les requêtes utilisent des paramètres tels que la charge du processeur, la charge moyenne, l'utilisation de la mémoire et la connectivité. Pour plus d'informations sur SNMP v3, telles que les spécifications d'authentification et de cryptage, consultez la documentation SNMP officielle de RFC 3414.

> **Remarque :**
>
> La surveillance SNMP v3 est prise en charge avec XenMobile Server 10.8 et versions ultérieures.

Vous pouvez utiliser diverses applications de surveillance prenant en charge la surveillance SNMP, telles que SCOM. Pour de plus amples informations sur la configuration de SCOM, consultez cet article du centre de connaissances Citrix.

Conditions préalables

Configurez les ports TCP suivants :

- **Port 161 (UDP) :** utilisé pour le trafic SNMP à l'aide du protocole UDP. La source est le gestionnaire SNMP et la destination est XenMobile.
- **Port 162 (UDP) :** utilisé pour l'envoi d'alertes d'interruption SNMP vers le gestionnaire SNMP à partir de XenMobile. La source est XenMobile et la destination est le gestionnaire SNMP.

Pour plus d'informations sur les ports XenMobile, consultez la section Configuration requise pour les ports.

Pour afficher un diagramme d'architecture d'un déploiement XenMobile sur site incluant SNMP, consultez l'article Architecture de référence pour les déploiements sur site.

Les étapes générales de configuration SNMP sont les suivantes.

1. **Ajouter des utilisateurs :** les utilisateurs héritent de l'autorisation de recevoir des traps et de surveiller XenMobile Server.
2. **Ajouter un gestionnaire SNMP pour recevoir des traps :** les traps sont des alertes générées par XenMobile lorsque le nœud XenMobile dépasse le seuil maximum défini par l'utilisateur.
3. **Configurer le gestionnaire SNMP pour interagir avec XenMobile :** XenMobile Server utilise certaines bases d'informations de gestion (MIB) pour effectuer des opérations. Vous pouvez télécharger les MIB depuis la page **Paramètres > Configuration SNMP** de la console XenMobile. Vous pouvez importer ensuite les MIB dans le gestionnaire SNMP en utilisant un importateur MIB.

> **Remarque :**
>
> Chaque gestionnaire SNMP a son propre importateur MIB.

4. **Activer les traps :** vous pouvez activer les traps dans la console XenMobile et définir les intervalles et les seuils en fonction de votre environnement.
5. **Afficher les traps dans le gestionnaire SNMP tiers :** pour afficher les traps, vérifiez le gestionnaire SNMP. Toutefois, dans certains gestionnaires, vous pouvez configurer les paramètres pour activer les notifications en dehors du gestionnaire. Vous pouvez configurer les notifications pour qu'elles apparaissent, par exemple, dans les e-mails.

Vous pouvez générer les traps suivants à partir de XenMobile.

Nom du trap : Charge du processeur

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.2.1.25.3.3.1.2
- **Description :** Surveille la charge processeur du système pour l'intervalle défini par l'utilisateur. Si la charge dépasse la valeur de seuil personnalisé, XenMobile génère le trap SNMP.

Nom du trap : Charge moyenne pendant 1 minute

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.2021.10.1.5.1
- **Description :** Surveille la charge moyenne du système sur une période d'une minute pour l'intervalle défini par l'utilisateur. Si la charge moyenne dépasse la valeur de seuil personnalisé, XenMobile génère le trap SNMP.

Nom du trap : Charge moyenne pendant 5 minutes

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.2021.10.1.5.2
- **Description :** Surveille la charge moyenne du système sur une période de cinq minutes pour l'intervalle défini par l'utilisateur. Si la charge moyenne dépasse la valeur de seuil personnalisé, XenMobile génère le trap SNMP.

Nom du trap : Charge moyenne pendant 15 minutes

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.2021.10.1.5.3
- **Description :** Surveille la charge moyenne du système sur une période de 15 minutes pour chaque intervalle défini par l'utilisateur. Si la charge moyenne dépasse la valeur de seuil personnalisé, XenMobile génère le trap SNMP.

Nom du trap : Mémoire totale disponible

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.2021.4.11
- **Description :** Surveille la mémoire disponible pour chaque intervalle défini par l'utilisateur. Si la mémoire disponible tombe en dessous de la valeur de seuil personnalisé, XenMobile génère le trap SNMP. Remarque : la mémoire totale disponible inclut à la fois la RAM et la mémoire d'échange (mémoire virtuelle). Pour récupérer la mémoire totale d'échange, vous

pouvez effectuer une requête à l'aide de l'OID SNMP .1.3.6.1.4.1.2021.4.3. Pour récupérer la mémoire d'échange disponible, vous pouvez effectuer une requête à l'aide de l'OID SNMP .1.3.6.1.4.1.2021.4.4.

Nom du trap : Total du stockage sur disque utilisé

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.2021.9.1.9.1
- **Description :** Surveille le stockage sur disque système pour chaque intervalle défini par l'utilisateur. Si le stockage sur disque dépasse la valeur de seuil personnalisé, XenMobile génère le trap SNMP.

Nom du trap : Utilisation de la mémoire Heap de Java

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.2.4.0
- **Description :** Surveille l'utilisation de la mémoire Heap de la machine virtuelle Java (JVM) de XenMobile pour chaque intervalle défini par l'utilisateur. Si l'utilisation dépasse la valeur de seuil personnalisé, XenMobile génère le trap SNMP.

Nom du trap : Utilisation du méta-espace Java

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.2.5.0
- **Description :** Surveille l'utilisation du méta-espace Java de XenMobile pour chaque intervalle défini par l'utilisateur. Si l'utilisation dépasse la valeur de seuil, XenMobile génère le trap SNMP.

Nom du trap : Connectivité LDAP

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.1.0
- **Description :** Surveille la connectivité entre le serveur LDAP et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité DNS

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.2.0
- **Description :** Surveille la connectivité entre le serveur DNS et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec le serveur Google Store

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.3.0
- **Description :** Surveille la connectivité entre le serveur Google Store et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec Windows Phone Store

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.4.0

- **Description :** Surveille la connectivité entre le serveur Windows Phone Store et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec Windows Tab Store

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.5.0
- **Description :** Surveille la connectivité entre le serveur Windows Tab Store et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec le serveur du jeton de sécurité Windows

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.6.0
- **Description :** Surveille la connectivité entre le serveur du jeton de sécurité Windows et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec le serveur de notification Windows

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.7.0
- **Description :** Surveille la connectivité entre le serveur de notification Windows et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec le serveur APNs (Apple Push Notification Service)

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.8.0
- **Description :** Surveille la connectivité entre le serveur APNs et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec le serveur Apple Feedback

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.9.0
- **Description :** Surveille la connectivité entre le serveur Apple Feedback et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec le serveur Apple Store

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.10.0
- **Description :** Surveille la connectivité entre le serveur Apple Store et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec la base de données XenMobile

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.11.0

- **Description :** Surveille la connectivité entre la base de données XenMobile et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec le serveur Firebase Cloud Messaging

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.12.0
- **Description :** Surveille la connectivité entre le serveur Firebase Cloud Messaging et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec le serveur de licences Citrix

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.13.0
- **Description :** Surveille la connectivité entre le serveur de licences Citrix et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec Citrix Gateway

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.15.0
- **Description :** Surveille la connectivité entre Citrix Gateway et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité entre les nœuds XenMobile

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.16.0
- **Description :** Surveille la connectivité entre les nœuds de cluster XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

Nom du trap : Connectivité avec le service de nœud Tomcat de XenMobile

- **Surveillance de l'ID d'objet (OID) :** .1.3.6.1.4.1.3845.5.1.1.18.17.0
- **Description :** Surveille la connectivité entre le service de nœud Tomcat de XenMobile et le nœud XenMobile pendant chaque intervalle défini par l'utilisateur. XenMobile génère le trap SNMP en cas d'échec de la connectivité.

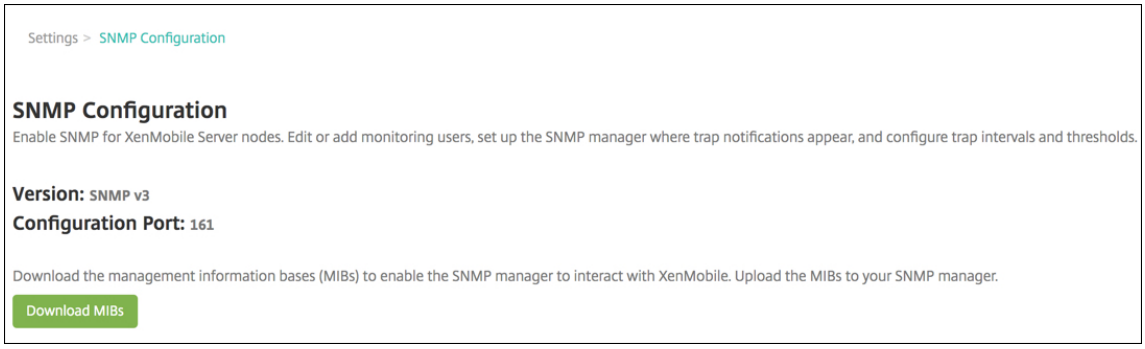
Pour obtenir les meilleures performances du serveur lors de la configuration des seuils SNMP, gardez à l'esprit les facteurs suivants :

- Fréquence des appels
- Collecte des données trap et vérifications de seuil
- Mécanisme de communication entre les nœuds
- Fréquence des vérifications de connectivité
- Délai d'expiration pour toute défaillance pendant les vérifications

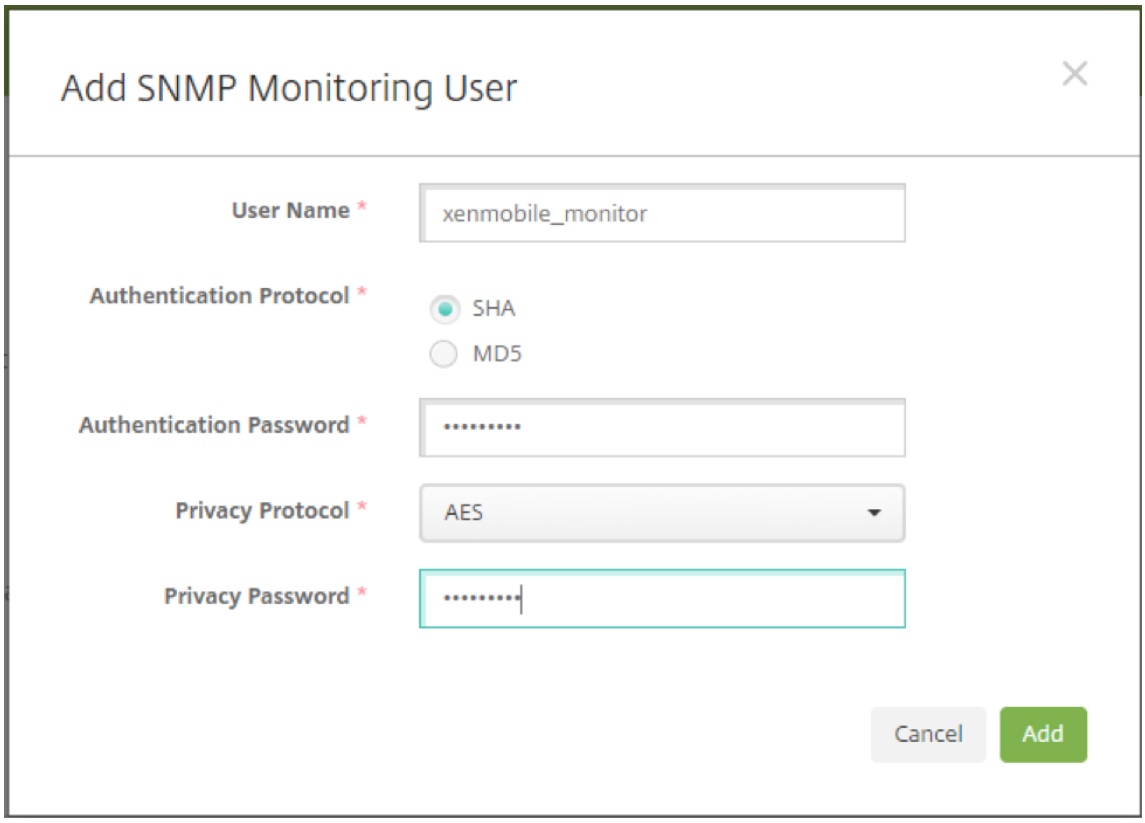
Pour ajouter les utilisateurs SNMP

Les utilisateurs SNMP interagissent avec les gestionnaires SNMP et reçoivent des traps.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Surveillance**, cliquez sur **Configuration SNMP**. La page **Configuration SNMP** s'affiche.



3. Sous **Utilisateurs de surveillance SNMP**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Ajouter utilisateur de surveillance SNMP**, configurez les paramètres suivants :



Nom d'utilisateur : le nom d'utilisateur utilisé pour se connecter au gestionnaire SNMP. Bien que vous puissiez utiliser des caractères alphanumériques, des traits de soulignement et des

traits d'union, vous ne pouvez pas utiliser d'espaces et d'autres caractères spéciaux pour votre nom d'utilisateur.

> **Remarque :**
>
> Vous ne pouvez pas ajouter le nom de l'utilisateur « xmsmonitor » car XenMobile réserve le nom pour un usage interne.

Protocoles d'authentification :

- **SHA** (recommandé)
- **MD5**

Mot de passe d'authentification : entrez un mot de passe de 8 à 18 caractères. Vous pouvez inclure des caractères alphanumériques et spéciaux.

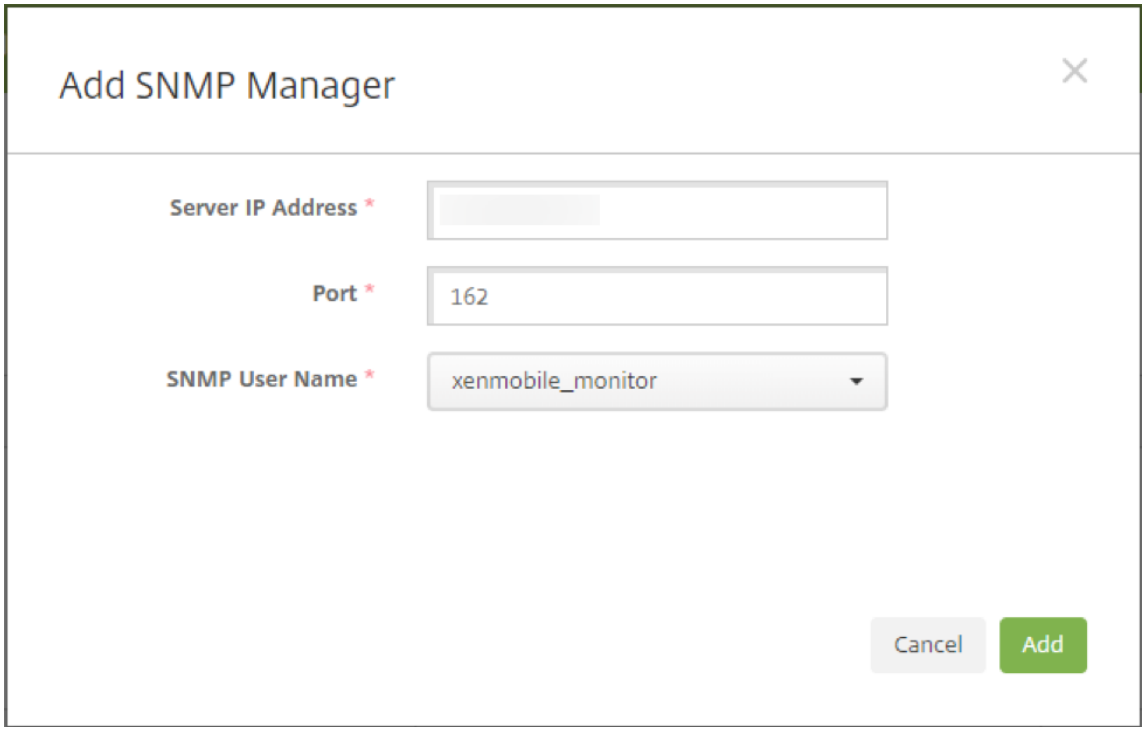
Protocole de confidentialité :

- **DES**
- **AES 128** (recommandé)

Mot de passe de confidentialité : entrez un mot de passe de 8 à 18 caractères. Vous pouvez inclure des caractères alphanumériques et spéciaux.

Pour ajouter un gestionnaire SNMP

1. Sous **Gestionnaires SNMP**, cliquez sur **Ajouter**.
2. Dans la boîte de dialogue **Ajouter gestionnaire SNMP**, configurez les paramètres suivants :



Adresse IP du serveur : entrez l'adresse IP du gestionnaire SNMP.

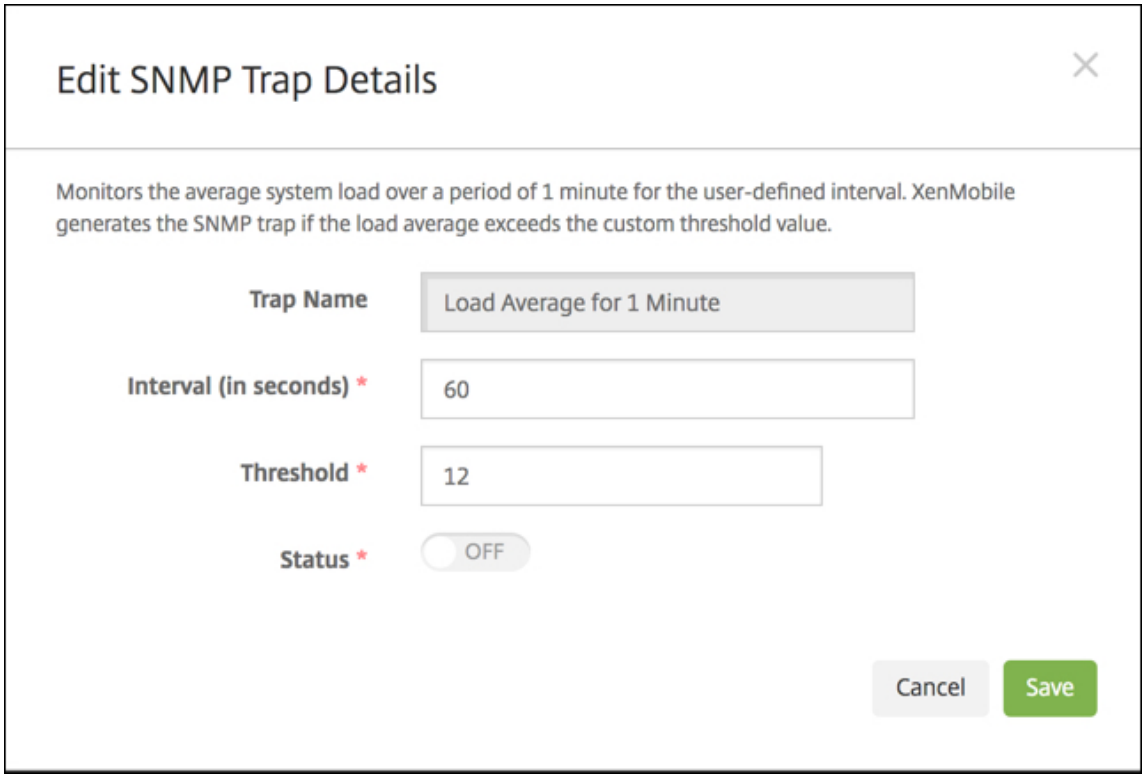
Port : modifiez le numéro de port si nécessaire. La valeur par défaut est 162.

Nom d'utilisateur SNMP : sélectionnez le nom d'un utilisateur ayant accès au gestionnaire.

Pour activer et configurer des traps SNMP

Pour vous aider à déterminer les paramètres trap appropriés pour votre environnement, consultez la section Capacité à monter en charge et performances. Par exemple, pour surveiller la charge moyenne XenMobile pendant une minute, vous pouvez activer Charge moyenne pendant 1 minute et fournir une valeur de seuil. Si la valeur définie dans Charge moyenne pendant 1 minute pour XenMobile Server dépasse le seuil spécifié, vous recevez un trap dans les gestionnaires SNMP configurés.

1. Pour activer les traps individuels, effectuez l'une des opérations suivantes :
   - Sélectionnez la case à cocher en regard du paramètre, puis cliquez sur **Activer**.
   - Pour activer tous les traps dans la liste, sélectionnez la case à cocher dans la partie supérieure, puis cliquez sur **Activer**.
2. Pour modifier un trap, sélectionnez le paramètre, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier les détails du trap SNMP**, vous pouvez modifier les valeurs de seuil pour les traps individuels.



Nom du trap : nom attribué au trap. Vous ne pouvez pas modifier ce champ.

Intervalle (en secondes) : la plage autorisée est comprise entre 60 et 86 400 (24 heures).

Seuil : vous pouvez modifier le seuil uniquement pour les traps suivants :

- Charge du processeur
- Charge moyenne pendant 1 minute
- Charge moyenne pendant 5 minutes
- Charge moyenne pendant 15 minutes
- Mémoire totale disponible
- Total du stockage sur disque utilisé
- Utilisation de la mémoire Heap de Java
- Utilisation du méta-espace Java

État : sélectionnez **Activé** pour activer la surveillance SNMP pour le trap. Sélectionnez **Désactivé** pour désactiver la surveillance.

Pour plus d'informations utiles sur la surveillance de XenMobile à l'aide de SNMP, consultez cet article de blog.

Packs d'assistance

January 10, 2022

Pour signaler un problème à Citrix ou résoudre un problème, créez un pack d'assistance. Puis chargez le pack d'assistance sur Citrix Insight Services (CIS)

Par défaut, un pack d'assistance comprend un maximum de 100 archives de sauvegarde de fichiers suivants. La valeur par défaut de la taille du fichier est de 10 Mo.

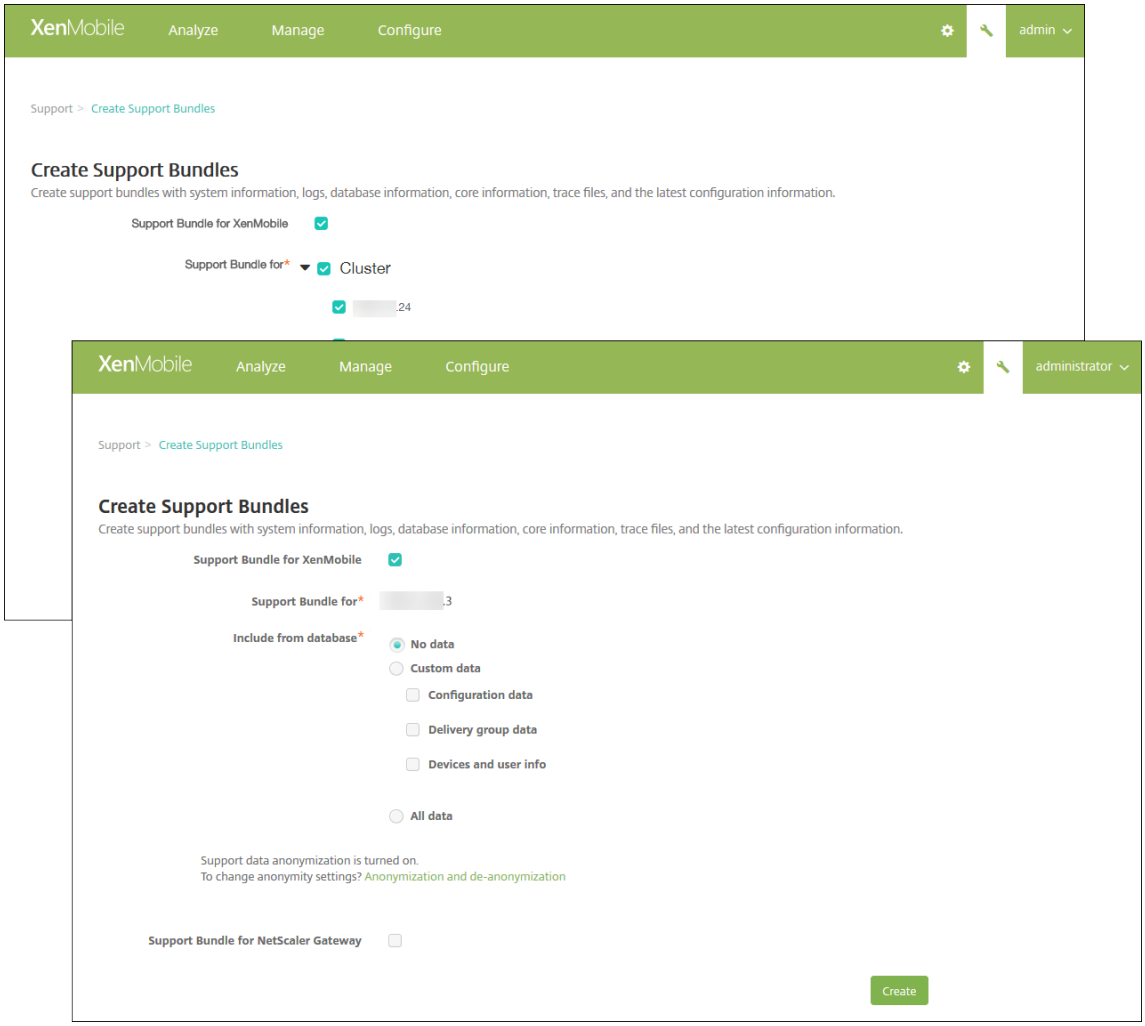
- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

Lorsque le pack d'assistance inclut 100 fichiers d'archive de journal pour chacune de ces catégories, le fichier journal est remplacé. Si vous configurez un nombre maximal inférieur de fichiers journaux, XenMobile supprime immédiatement les fichiers journaux superflus pour ce nœud. Pour configurer le nombre de fichiers journaux, accédez à **Dépannage et Support > Paramètres de journal**.

Pour créer un pack d'assistance :

1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Support** s'affiche.

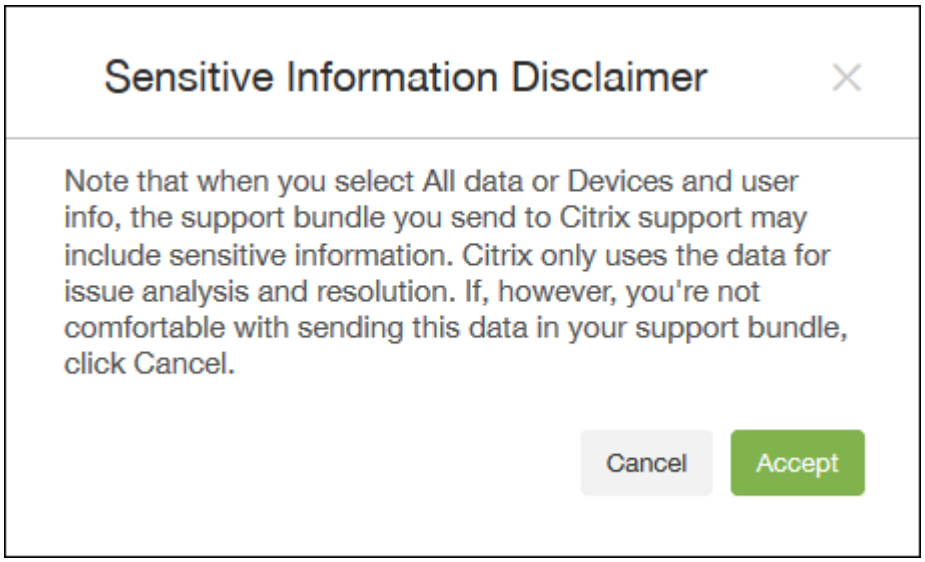
2. Sur la page **Support**, cliquez sur **Créer des packs d'assistance**. La page **Créer des packs d'assistance** s'affiche. Si votre environnement XenMobile contient des nœuds en cluster, tous les nœuds sont affichés.



3. Assurez-vous que la case à cocher **Pack d'assistance pour XenMobile** est sélectionnée.
4. Si votre environnement XenMobile contient des nœuds en cluster, dans **Pack d'assistance pour**, vous pouvez sélectionner tous les nœuds ou une combinaison de nœuds à partir desquels extraire des données.
5. Dans **Inclure depuis la base de données**, effectuez l'une des opérations suivantes :
   - Cliquez sur **Aucune donnée**.
   - Cliquez sur **Données personnalisées**. Par défaut, toutes ces options sont sélectionnées.
     - **Données de configuration :** comprend les configurations de certificat et les stratégies de gestionnaire d'appareils.
     - **Données du groupe de mise à disposition :** comprend des informations sur les groupes de mise à disposition d'applications ; contient des détails sur les types

d'applications et la stratégie de mise à disposition.
  - **Infos sur l'utilisateur et les appareils :** comprend les stratégies d'appareil, les applications, les actions et les groupes de mise à disposition.
- Cliquez sur **Toutes les données**.

> **Remarque :**
>
> Si vous choisissez **Infos sur l'utilisateur et les appareils** ou **Toutes les données**, et s'il s'agit du premier pack d'assistance que vous créez, la boîte de dialogue **Avis de non-responsabilité : données sensibles** s'affiche. Lisez l'avis, puis cliquez sur **Accepter** ou **Annuler**. Si vous cliquez sur **Annuler**, le pack d'assistance ne peut pas être chargé dans Citrix. Si vous cliquez sur **Accepter**, vous pouvez le charger sur Citrix et vous ne voyez pas l'avis de non-responsabilité la prochaine fois que vous créez un pack d'assistance qui comprend des données de l'appareil ou de l'utilisateur.

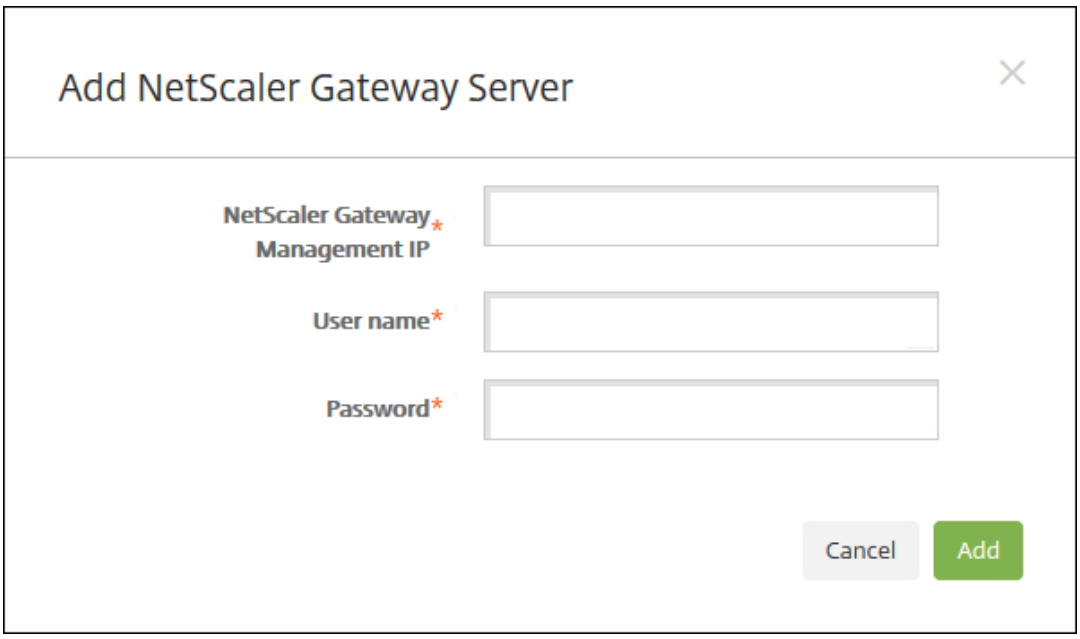


6. L'option **L'anonymisation des données d'assistance est activée** indique que le paramètre par défaut anonymise les données. L'anonymisation des données signifie que les données d'utilisateur, de serveur et de réseau sensibles sont rendues anonymes dans les packs d'assistance.

   Pour modifier ce paramètre, cliquez sur **Anonymisation et réidentification**. Pour de plus amples informations sur l'anonymisation des données, consultez la section Anonymisation des données dans les packs d'assistance.

7. Sélectionnez la case à cocher **Pack d'assistance pour Citrix Gateway** pour inclure des packs d'assistance Citrix Gateway, puis procédez comme suit :

   a) Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un serveur Citrix Gateway** s'affiche.



b) Dans **Adresse IP de gestion de Citrix Gateway**, entrez l'adresse IP de gestion de Citrix ADC pour l'instance Citrix Gateway à partir de laquelle vous voulez extraire les données de votre pack d'assistance.

> **Remarque :**
>
> Si vous créez un pack à partir d'un serveur Citrix Gateway qui est déjà ajouté, l'adresse IP est renseignée.

c) Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification utilisateur requises pour accéder au serveur exécutant Citrix Gateway.

> **Remarque :**
>
> Si vous créez un pack à partir d'un serveur Citrix Gateway qui est déjà ajouté, le nom d'utilisateur est renseigné.

8. Cliquez sur **Ajouter**. Le nouveau pack d'assistance Citrix Gateway est ajouté au tableau.
9. Répétez l'étape 7 pour ajouter des packs d'assistance Citrix Gateway supplémentaires.
10. Cliquez sur **Créer**. Le pack d'assistance est créé et deux nouveaux boutons, **Charger sur CIS** et **Télécharger sur le client** s'affichent.

Chargement de packs d'assistance sur Citrix Insight Services

Après la création d'un pack d'assistance, vous pouvez le charger sur Citrix Insight Services (CIS) ou télécharger le pack sur votre ordinateur.

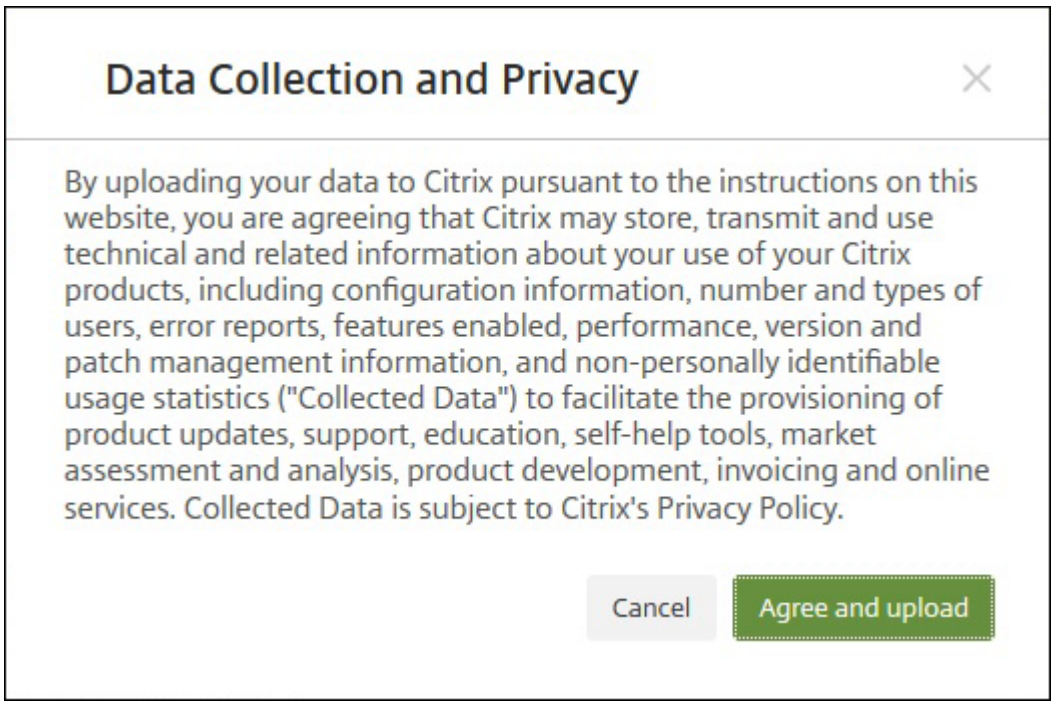
Le téléchargement de XenMobile vers CIS s'effectue via une connexion sortante SSL. Ouvrez le port 443

à l'adresse IP du serveur CIS (52.88.24.76, 52.88.118.220, 52.11.72.119). Si vous disposez d'un serveur proxy pour le trafic HTTPS, vérifiez que le serveur proxy peut contacter l'adresse IP du serveur CIS.

Ces étapes vous montrent comment charger le pack sur CIS. Vous avez besoin d'un ID et d'un mot de passe My Citrix pour le chargement sur CIS.

1. Sur la page **Créer des packs d'assistance**, cliquez sur **Charger sur CIS**. La boîte de dialogue **Charger sur Citrix Insight Services (CIS)** s'affiche.
2. Dans le champ **Nom d'utilisateur**, entrez votre ID My Citrix.
3. Dans le champ **Mot de passe**, entrez votre mot de passe My Citrix.
4. Si vous souhaitez associer ce pack à un numéro de demande de service existant, sélectionnez la case à cocher **Associer avec la SR n°** et dans les deux nouveaux champs qui apparaissent, procédez comme suit :
   - Dans **N° de SR**, tapez le numéro de la SR composé de huit chiffres auquel vous souhaitez associer ce groupe.
   - Dans le champ **Description de la SR**, entrez une description pour la SR.
5. Cliquez sur **Charger**.

   Si c'est la première fois que vous chargez un pack d'assistance sur CIS, que vous n'avez pas créé de compte sur CIS par le biais d'un autre produit et que vous n'avez pas accepté les termes concernant la collecte de données et la confidentialité, la boîte de dialogue suivante s'affiche ; vous devez accepter les termes du contrat avant que le chargement puisse commencer. Si vous disposez d'un compte sur CIS et avez précédemment accepté les termes du contrat, le pack d'assistance est chargé immédiatement.



6. Veuillez lire le contrat et cliquer sur **Accepter et charger**. Le pack d'assistance est chargé.

Téléchargement de packs d'assistance sur votre ordinateur

Après la création d'un pack d'assistance, vous pouvez le charger sur CIS ou le télécharger sur votre ordinateur. Si vous voulez résoudre le problème par vous-même, téléchargez le pack d'assistance sur votre ordinateur.

Sur la page Créer des packs d'assistance, cliquez sur Télécharger sur le client. Le pack est téléchargé sur votre ordinateur.

Le bundle de support contient des fichiers de valeur analytique variable. Reportez-vous au tableau suivant pour obtenir la liste des fichiers et leur valeur analytique.

Nom du fichier	Type	Description	Valeur
DbDump.json	Vidage de la base de données JSON	Informations sur les utilisateurs/périphériques/applications	Élevé
Garbage.html	Fichier HTML	Garbage Collector Java	Faible

Nom du fichier	Type	Description	Valeur
MemoryInfo.html	Fichier HTML	Utilisation de la mémoire - utilisation de la mémoire liée à Java	Élevé
MultiNodeClusterInfo.html	Fichier HTML	Configuration de cluster	Élevé
Patches.html	Fichier HTML	Informations sur les correctifs. Better to xmspatches.txt	Élevé
pg_dump0.sql	Vidage PG	vidage d'instance Postgress par défaut	Medium (Moyen)
rt_db/*	Copie de BDD (redondant, il s'agit d'une représentation binaire de pg_dump0.sql)		S.O.
sas_config/c3p0.properties	Fichier de propriétés	Propriétés de configuration de la base de données C3P0	Medium (Moyen)
sas_config/catalina.pol	Fichier de stratégie	Stratégies du serveur Web Catalina - Les fichiers ne changent pas	Faible
sas_config/catalina.properties	Fichier de propriétés	Propriétés du serveur Web Catalina - Les fichiers ne changent pas	Faible
sas_config/ew-config.properties	Fichier de propriétés	Informations sur la configuration du serveur XM	Élevé
sas_config/ew-config-reloadable.properties	Fichier de propriétés	Informations sur le modèle de sécurité	Élevé
sas_config/hazelcast.xr	Fichier XML	Journaux Hazelcast - Pas très utiles.	Faible

Nom du fichier	Type	Description	Valeur
sas_config/pki.xml	Fichier XML	Peut être utilisé pour déterminer si un serveur PKI tiers est utilisé.	Élevé
sas_config/push_servic	Fichier XML	Services Push - Les fichiers ne changent pas	Faible
sas_config/server.xml	Fichier XML	Informations de chiffrement ici - Liées à la sécurité	Élevé
sas_config/sftu_config/	Fichier de propriétés	AppC Properties - Les fichiers ne changent pas	Faible
sas_config/sftu_config/catalina.policy	Fichier de stratégie	Stratégies Catalina - Les fichiers ne changent pas	Faible
sas_config/sftu_config/	Fichier de propriétés	Propriétés Catalina - Les fichiers ne changent pas	Faible
sas_config/sftu_config/logging.properties	Fichier de propriétés	Propriétés de journalisation - Les fichiers ne changent pas	Faible
sas_config/sftu_config/	Fichier XML	Informations de chiffrement ici - Liées à la sécurité	Élevé
sas_config/sftu_config/server_migration.xml	Fichier XML	Informations sur la migration	Élevé
sas_config/sftu_config/	Fichier XML	Paramètres utilisateur de première utilisation	Élevé
sas_config/sftu_config/tomcat-users.xml	Fichier XML	Utilisateurs TomCat - Les fichiers ne changent pas	Faible

Nom du fichier	Type	Description	Valeur
sas_config/sftu_config/	Fichier XML	Web - Les fichiers ne changent pas	Faible
sas_config/sftu.properties	Fichier de propriétés	Propriétés de configuration SFTU	Élevé
sas_config/variables.xml	Fichier XML	Variables - Les fichiers ne changent pas	Faible
sas_config/web.xml	Fichier XML	Informations relatives au serveur Web	Medium (Moyen)
sas_log/AdminAuditLog	Fichier journal Linux	Toute modification de configuration	Élevé
sas_log/create_sb_output.log	Fichier journal Linux	Sortie de commande de génération de support	Faible
sas_log/DebugLogFile.log	Fichier journal Linux	Journal de toutes les fonctionnalités	Élevé
sas_log/HibernateStats.log	Fichier journal Linux	Journal Hibernatestats	Faible
sas_log/kafka-consumer.log	Fichier journal Linux	Journal Kafka	Faible
sas_log/kafka-server.log	Fichier journal Linux	Journal Kafka	Faible
sas_log/kafka-topics.log	Fichier journal Linux	Journal Kafka	Faible
sas_log/LPE.log	Fichier journal Linux	Journal LPE	Faible
sas_log/migration.log	Fichier journal Linux	Sortie du processus de migration	Medium (Moyen)
sas_log/PlatformAuditLogFile.log	Fichier journal Linux	Informations sur le niveau de l'audit du back-end	Élevé
sas_log/PlatformDebug	Fichier texte	Journaux liés au serveur principal	Élevé
sas_log/postgres.log	Fichier journal Linux	Journaux PostGres	Medium (Moyen)
sas_log/SFTU.log	Fichier journal Linux	Journal SFTU	Medium (Moyen)

Nom du fichier	Type	Description	Valeur
sas_log/tc1/catalina.log	Fichier journal Linux	Journal Catalina	Faible
sas_log/tc1/console	Fichier journal Linux	Console	Faible
sas_log/tc1/host-manager.log	Fichier journal Linux	Gestionnaire d'hôte	Faible
sas_log/tc1/localhost.l	Fichier journal Linux	LocalHost	Faible
sas_log/updates.log	Fichier journal Linux	Sortie du processus de correction	Medium (Moyen)
sas_log/UserAuditLogF	Fichier journal Linux	Actions utilisateur	Élevé
sas_log/zookeeper.txt	Fichier texte	Journal Zookeeper	Faible
snmp/snmpd_etc_nets	Fichier de propriétés	Propriétés de configuration SNMP	Faible
snmp/snmpd_privileges.conf	Fichier de propriétés	Propriétés de configuration SNMP	Faible
sys_info/arp_entries.txt	Fichier texte	Entrées ARP dans le serveur XMS	Medium (Moyen)
sys_info/chrony.txt	Fichier texte	Journal Chrony	Faible
sys_info/diskspace_usa	Fichier texte	Utilisation de l'espace disque	Élevé
sys_info/firewall_rules.txt	Fichier texte	Règles de pare-feu définies dans XMS	Medium (Moyen)
sys_info/interface_conf	Fichier texte	Sortie de commande système	Medium (Moyen)
sys_info/net_connections.txt	Fichier texte	Sortie de commande système	Medium (Moyen)
sys_info/root_account_	Fichier texte	Sortie de commande système	Medium (Moyen)
sys_info/routing_table.txt	Fichier texte	Valeur élevée	Élevé
sys_info/running_proce	Fichier texte	Valeur élevée	Élevé
sys_info/top.txt	Fichier texte	Sortie de commande système	Medium (Moyen)
ThreadDump.html	Fichier HTML	N'est plus utilisée.	Faible

Nom du fichier	Type	Description	Valeur
ThreadDumpV2.html	Fichier HTML	Traces de pile de thread, etc.	Medium (Moyen)
var_log/auth.log	Fichier journal Linux	Journal de niveau système d'exploitation	Medium (Moyen)
var_log/boot.log	Fichier journal Linux	Journal de niveau système d'exploitation	Medium (Moyen)
var_log/btmp	Fichier journal Linux	Journal de niveau système d'exploitation	Medium (Moyen)
var_log/daemon.log	Fichier journal Linux	Journal de niveau système d'exploitation	Medium (Moyen)
var_log/kern.log	Fichier journal Linux	Journal de niveau système d'exploitation	Medium (Moyen)
var_log/lastlog	Fichier journal Linux	Journal de niveau système d'exploitation	Medium (Moyen)
var_log/mail.log	Fichier journal Linux	Journal de niveau système d'exploitation	Medium (Moyen)
var_log/sys.log	Fichier journal Linux	Journal de niveau système d'exploitation	Medium (Moyen)
var_log/user.log	Fichier journal Linux	Journal de niveau système d'exploitation	Medium (Moyen)
var_log/wtmp	Fichier journal Linux	Journal de niveau système d'exploitation	Medium (Moyen)
version.txt	Fichier texte	Version du serveur XM	Medium (Moyen)

Nom du fichier	Type	Description	Valeur
XENMOBILE-<IP Address>-ConnectivityCheckResults.xml	Fichier XML	Résultats de la vérification de la connectivité sur le serveur XMS	Medium (Moyen)
xmspatches.txt	Fichier texte	Informations sur les correctifs.	Élevé

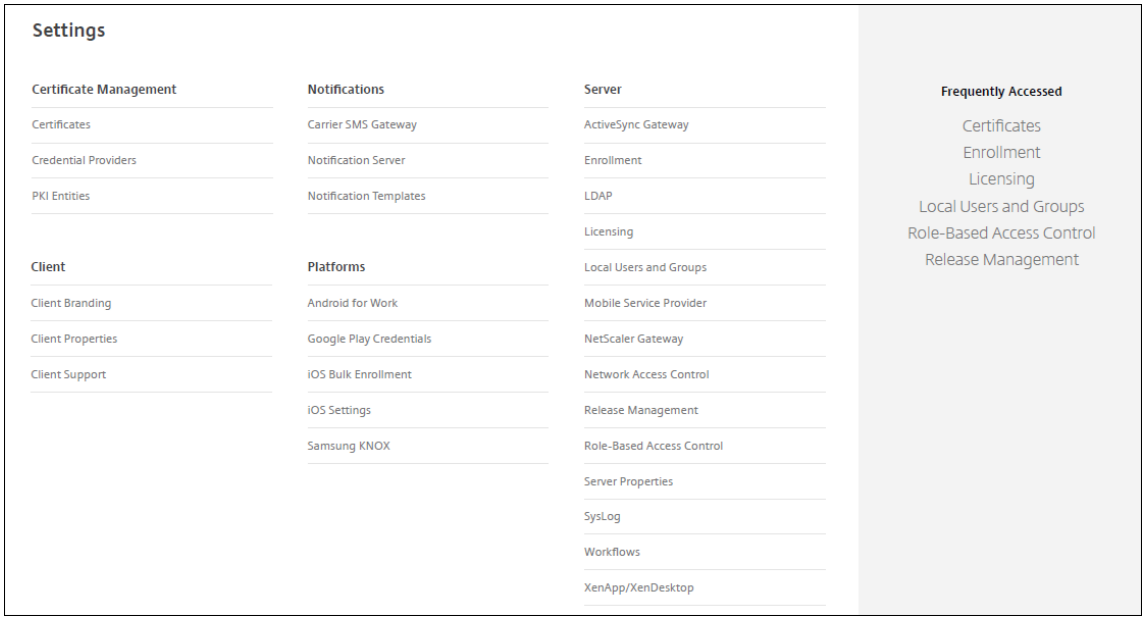
Options d'assistance et assistance à distance

January 10, 2022

Vous pouvez fournir une adresse e-mail aux utilisateurs pour contacter le personnel d'assistance technique. Lorsque des utilisateurs demandent une assistance depuis leurs appareils, ils voient l'adresse e-mail.

Vous pouvez également configurer la manière dont les utilisateurs envoient les journaux à l'assistance technique depuis leurs appareils. Les journaux peuvent être envoyés directement ou par e-mail.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.



2. Sous **Client**, cliquez sur **Support client**. La boîte de dialogue **Support client** s'affiche.
3. Configurez les paramètres suivants :

- **E-mail de l'assistance (support technique) :** entrez l'adresse e-mail pour le contact de votre service d'assistance informatique.
- **Envoyer les journaux de l'appareil au service d'assistance :** indiquez si vous souhaitez que les journaux de l'appareil soient envoyés **directement** ou **par e-mail**. La valeur par défaut est **par e-mail**.
  - Lorsque vous sélectionnez **directement**, les paramètres liés au stockage des journaux sur ShareFile (maintenant appelé Citrix Content Collaboration) s'affichent. Si vous activez le stockage des journaux sur Citrix Content Collaboration, les journaux sont envoyés directement à Citrix Files. Sinon, les journaux sont envoyés à XenMobile, puis envoyés par e-mail à l'assistance technique. L'option **Si l'envoi direct échoue, utiliser e-mail** s'affiche également ; elle est activée par défaut. Vous pouvez désactiver cette option si vous ne voulez pas utiliser la messagerie du client pour envoyer les journaux en cas de problème de serveur. Si, toutefois, vous désactivez cette option et qu'un problème de serveur se produit, les journaux ne sont pas envoyés.
  - Lorsque vous activez **par e-mail**, la messagerie du client est toujours utilisée pour envoyer les journaux.

4. Cliquez sur **Enregistrer**.

Assistance à distance

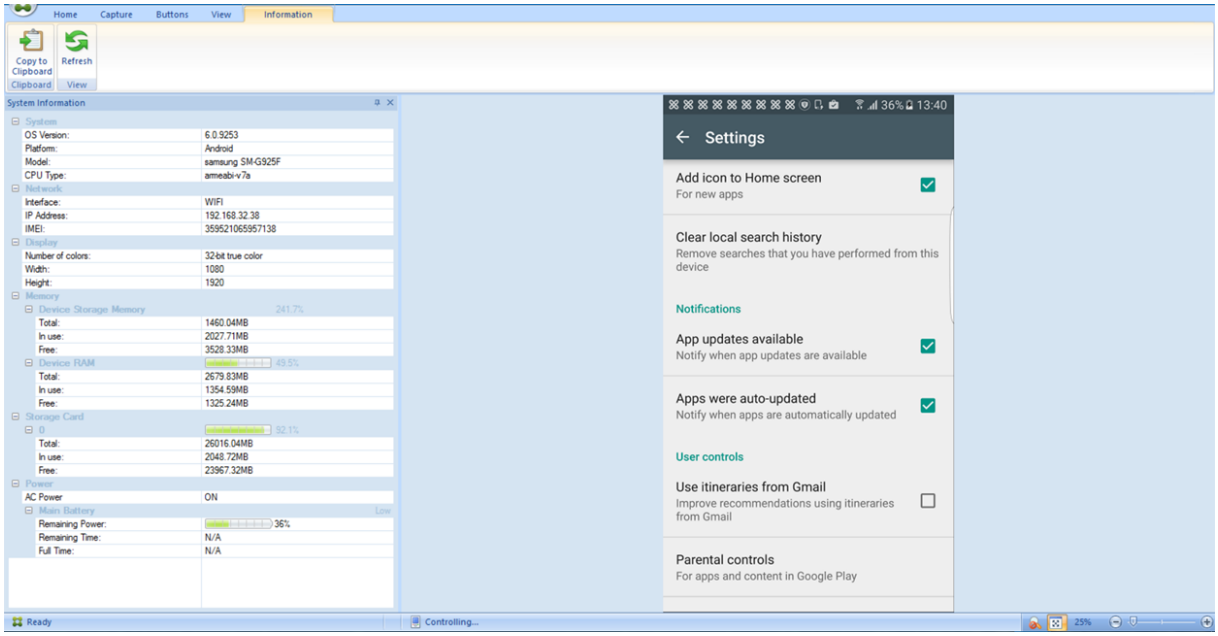
> **Remarque :**
>
> L'Assistance à distance n'est plus disponible pour les nouveaux clients à compter du 1er janvier 2019. Les clients existants peuvent continuer à utiliser le produit, mais Citrix ne fournira pas d'améliorations ou de correctifs.

Pour les déploiements locaux de XenMobile Server : l'Assistance à distance permet aux représentants du service d'assistance de contrôler à distance des appareils mobiles Windows CE et Android gérés. La capture d'écran est uniquement prise en charge sur les appareils Samsung Knox.

L'Assistance à distance n'est pas disponible pour les déploiements de XenMobile Server locaux en cluster.

Pendant une session de contrôle à distance :

- Les utilisateurs voient une icône sur leur appareil mobile indiquant qu'une session de contrôle à distance est active.
- Les utilisateurs d'Assistance à distance voient la fenêtre de l'application Assistance à distance et une fenêtre de contrôle à distance affichant un rendu de l'appareil contrôlé.



Avec l'Assistance à distance, vous pouvez effectuer les opérations suivantes :

- Se connecter à distance à l'appareil d'un utilisateur et contrôler l'écran. Les utilisateurs peuvent vous voir parcourir leur écran, ce qui peut s'avérer utile dans le cadre de formations.
- Parcourir et réparer un appareil distant en temps réel. Vous pouvez modifier les configurations, résoudre les problèmes liés au système d'exploitation, et désactiver ou arrêter les applications ou les processus qui posent problème.
- Isoler et contenir les menaces avant qu'elles ne se propagent sur d'autres appareils mobiles en désactivant à distance l'accès réseau, en arrêtant les processus indésirables et en supprimant les applications et les logiciels malveillants.
- Activer à distance la sonnerie et appeler le téléphone, pour aider l'utilisateur à localiser l'appareil. Si un utilisateur ne peut pas trouver l'appareil, vous pouvez l'effacer pour vous assurer que vos données confidentielles ne sont pas compromises.

L'assistance à distance permet également au personnel du service d'assistance technique d'effectuer ce qui suit :

- Afficher une liste de tous les appareils connectés à une ou plusieurs instances de XenMobile.
- Afficher des informations sur le système, notamment le modèle de l'appareil, niveau de système d'exploitation, numéro d'identité internationale d'équipement mobile (IMEI) et numéro de série, mémoire, état de la batterie et connectivité.
- Afficher les utilisateurs et les groupes de XenMobile.
- Exécuter le gestionnaire des tâches de l'appareil afin de pouvoir afficher, mettre fin à des processus en cours et redémarrer l'appareil mobile.
- Exécuter le transfert de fichiers à distance, notamment le transfert de fichiers bidirectionnel entre les appareils mobiles et un serveur de fichiers central.

- Télécharger et installer des logiciels par lots sur un ou plusieurs appareils mobiles.
- Configurer des paramètres de clé de registre sur l'appareil.
- Optimiser le temps de réponse sur les réseaux cellulaires à faible bande passante à l'aide d'un contrôle à distance de l'écran de l'appareil en temps réel.
- Afficher le thème de l'appareil de la plupart des marques et modèles d'appareils mobiles. Afficher un éditeur de thème afin d'ajouter de nouveaux modèles d'appareils et de mapper les touches physiques.
- Activer la capture d'écran sur l'appareil, enregistrer et lire avec la possibilité de capturer une séquence d'interactions sur l'appareil afin de créer un fichier vidéo AVI.
- Tenir des réunions en direct à l'aide d'un tableau blanc partagé, utiliser des communications audio VoIP et effectuer des chats entre utilisateurs mobiles et l'équipe d'assistance.

Configuration système requise pour l'Assistance à distance

Le logiciel Assistance à distance est installé sur les ordinateurs Windows qui répondent aux conditions suivantes. Pour les exigences en matière de port, consultez la section Configuration requise pour les ports.

Plates-formes prises en charge :

- Intel Xeon/Pentium 4 - 1 GHz minimum
- 512 Mo minimum de RAM
- 100 Mo minimum d'espace disque libre

Systèmes d'exploitation pris en charge :

- Microsoft Windows Server 2003 Standard Edition ou Enterprise Edition SP1 ou version ultérieure
- Microsoft Windows 2000 Professionnel SP4
- Microsoft Windows XP SP2 ou version ultérieure
- Microsoft Windows Vista SP1 ou version ultérieure
- Microsoft Windows 10 ou Windows 11
- Microsoft Windows 8
- Microsoft Windows 7

Pour installer l'Assistance à distance à partir de la ligne de commande

Exécutez la commande suivante :

```
1 \*RemoteSupport\*.exe /S
```

RemoteSupport correspond au nom du programme d'installation. Par exemple :

```
1 XenMobileRemoteSupport-9.0.0.35265.exe /S
```

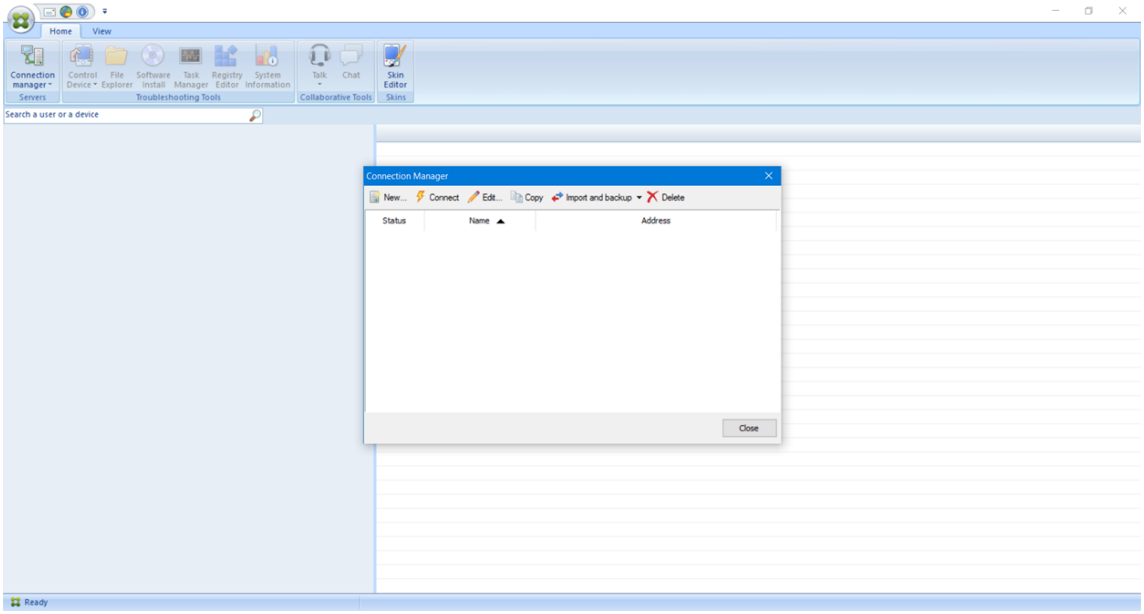

Vous pouvez utiliser les variables suivantes lors de l'installation du logiciel Assistance à distance :

- /S: pour installer de manière silencieuse le logiciel Assistance à distance avec les paramètres par défaut.
- /D=dir: pour spécifier un répertoire d'installation personnalisé.

Pour connecter l'Assistance à distance à XenMobile

Pour établir des connexions d'assistance à distance avec des appareils gérés, vous devez ajouter une connexion depuis l'Assistance à distance vers un ou plusieurs serveurs XenMobile qui gèrent les appareils. Cette connexion s'exécute sur un tunnel applicatif que vous définissez dans la stratégie de tunnel MDM, une stratégie pour appareils Android et Windows Mobile/CE. Définissez le tunnel applicatif avant de pouvoir connecter l'Assistance à distance à XenMobile. Pour plus de détails, consultez la section Stratégies de tunnel applicatif.

1. Démarrez le logiciel Assistance à distance et utilisez vos informations d'identification XenMobile pour ouvrir une session.
2. Dans **Connection Manager**, cliquez sur **New**.



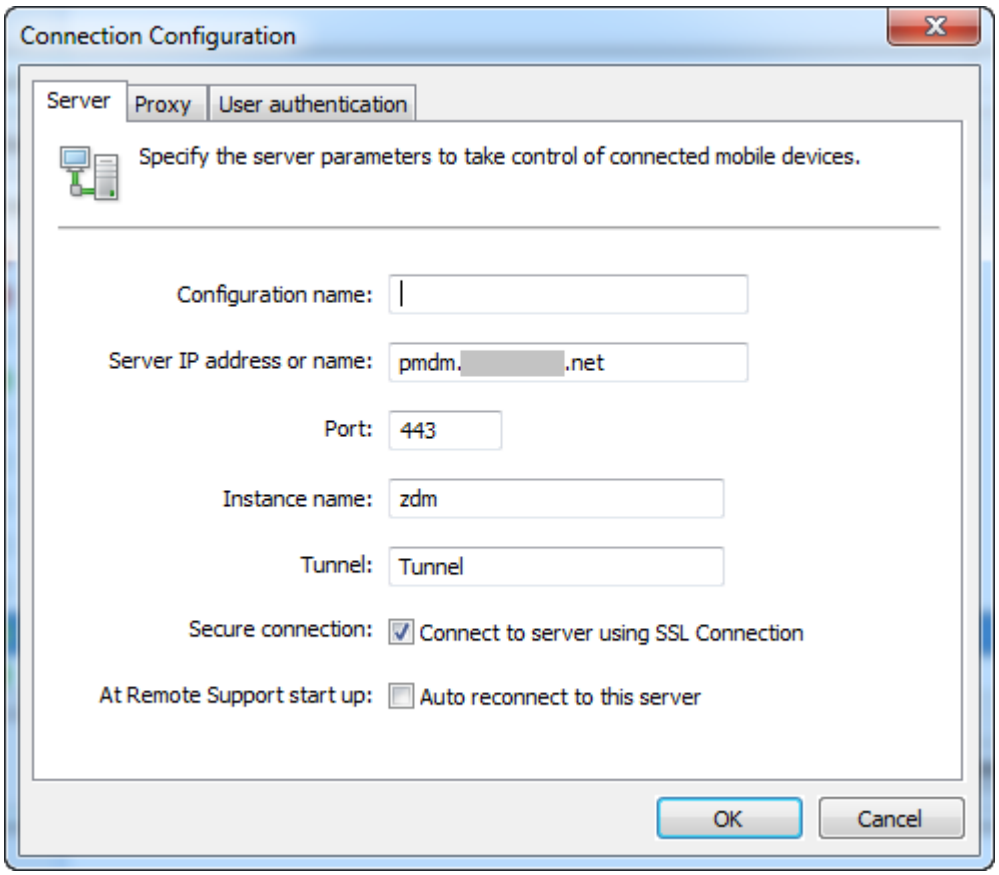
3. Dans la boîte de dialogue **Connection Configuration**, sur l'onglet **Server**, entrez les valeurs suivantes :
    a) Dans **Configuration name**, entrez un nom pour l'entrée de configuration.
    b) Dans **Server IP address or name**, entrez l'adresse IP ou le nom DNS de XenMobile Server.
    c) Dans **Port**, entrez un numéro de port TCP, comme défini dans la configuration de XenMobile Server.

d) Dans **Instance name**, si XenMobile fait partie d'un déploiement Multi-Tenant, entrez un nom d'instance.

e) Dans **Tunnel**, entrez le nom de la Stratégie de tunnel.

f) Cochez la case **Connect to server using SSL Connection**.

g) Sélectionnez la case **Auto reconnect to this server** pour vous connecter au serveur XenMobile configuré chaque fois que l'application Assistance à distance démarre.



4. Sur l'onglet **Proxy**, sélectionnez **Use an http proxy server** et entrez les informations suivantes :

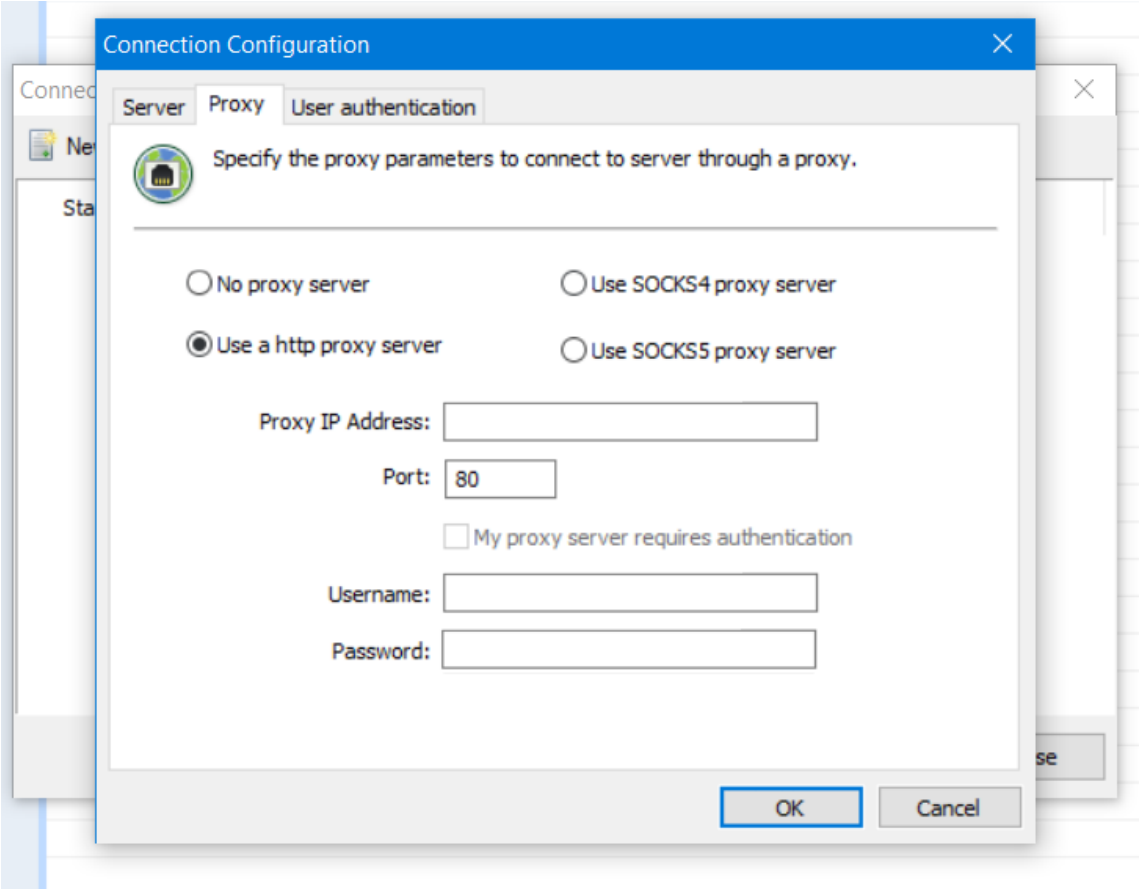
a) En regard de **Proxy IP Address**, saisissez l'adresse IP du serveur proxy.

b) En regard de **Port**, saisissez le numéro de port TCP utilisé par le proxy.

c) Sélectionnez la case **My proxy server requires authentication** si le serveur proxy requiert une authentification pour autoriser le trafic.

d) En regard de **Username**, saisissez le nom de l'utilisateur qui doit être authentifié sur le serveur proxy.

e) En regard de **Password**, saisissez le mot de passe qui doit être authentifié sur le serveur proxy.



5. Sur l'onglet **User Authentication**, sélectionnez la case **Remember my login and password** et entrez les informations d'identification.
6. Cliquez sur **OK**.

Pour vous connecter à XenMobile, double-cliquez sur la connexion que vous avez créée, puis entrez le nom d'utilisateur et le mot de passe que vous avez configurés pour la connexion.

Pour activer l'assistance à distance des appareils Samsung Knox

Vous créez une stratégie d'assistance à distance dans XenMobile pour vous permettre d'accéder à distance aux appareils Samsung Knox. Vous pouvez configurer deux types d'assistance :

- **Assistance à distance de base :** vous permet de visualiser les informations de diagnostic concernant l'appareil. Par exemple, les informations système, les processus en cours d'exécution, le gestionnaire des tâches (utilisation de mémoire et de l'UC), le contenu du dossier des logiciels installés.
- **Assistance à distance premium :** vous permet de contrôler à distance l'écran de l'appareil. Par exemple, contrôler les couleurs de la fenêtre, établir une session VoIP entre le service d'assistance et l'utilisateur et établir une session de chat entre le service d'assistance et

l'utilisateur.

Avec l'assistance Premium, vous devez configurer la stratégie de clé de licence MDM Samsung dans la console XenMobile. Lorsque vous configurez cette stratégie, sélectionnez la plate-forme **Samsung KNOX** uniquement. Pour la plate-forme Samsung SAFE, la clé ELM est déployée automatiquement sur les appareils Samsung lorsqu'ils s'inscrivent dans XenMobile. Par conséquent, ne sélectionnez pas la plate-forme Samsung SAFE pour cette stratégie. Pour de plus amples informations, consultez la section Clé de licence MDM Samsung.

Pour plus d'informations sur la configuration de la stratégie d'assistance à distance, consultez la section Stratégie d'assistance à distance.

Pour utiliser une session d'Assistance à distance

Lorsque vous démarrez l'Assistance à distance, la partie gauche de la fenêtre de l'application Assistance à distance présente des groupes d'utilisateurs XenMobile, comme défini dans la console XenMobile. Par défaut, seuls les groupes contenant des utilisateurs qui sont actuellement connectés sont affichés. Vous pouvez afficher l'appareil pour chaque utilisateur en regard de l'entrée de l'utilisateur.

1. Pour afficher tous les utilisateurs, développez chaque groupe à partir de la colonne de gauche. Les utilisateurs actuellement connectés au serveur XenMobile sont indiqués par une icône verte.
2. Pour afficher tous les utilisateurs, y compris ceux qui ne sont pas actuellement connectés, cliquez sur **View** et sélectionnez **Non-connected devices**.
   Les utilisateurs non connectés s'affichent sans la petite icône verte.

Les appareils connectés au serveur XenMobile, mais non affectés à un utilisateur s'affichent en mode anonyme. (La chaîne **Anonymous** s'affiche dans la liste). Vous pouvez contrôler ces appareils de la même façon que l'appareil d'un utilisateur connecté.

Pour contrôler un appareil, sélectionnez l'appareil en cliquant sur sa ligne, puis cliquez sur **Control Device**. Un rendu de l'appareil s'affiche dans la fenêtre Remote Control. Vous pouvez interagir avec un appareil contrôlé de l'une des manières suivantes :

- Contrôler l'écran de l'appareil, y compris les couleurs, dans la fenêtre principale, où dans une fenêtre séparée flottante.
- Établir une session VoIP entre le support technique et l'utilisateur. Configurer les paramètres VoIP.
- Établir une session de chat avec l'utilisateur.
- Accéder au Gestionnaire des tâches de l'appareil pour gérer des éléments tels que l'utilisation de la mémoire, l'utilisation d'UC et les applications en cours d'exécution.
- Explorer les répertoires locaux de l'appareil mobile. Transférer des fichiers.
- Modifier le registre de l'appareil sur des appareils mobiles Windows.
- Afficher les informations système de l'appareil et tous les logiciels installés.

- Mettre à jour de l'état de connexion de l'appareil mobile avec le serveur XenMobile.

Syslog

November 11, 2020

Vous pouvez configurer XenMobile Server (sur site uniquement) de manière à envoyer les fichiers journaux à un serveur syslog. Vous avez besoin du nom d'hôte ou de l'adresse IP du serveur.

Syslog est un protocole de journalisation standard constitué de deux composants : un module d'audit (qui s'exécute sur l'appliance) et un serveur, qui peut être exécuté sur un système distant. Le protocole Syslog utilise le protocole UDP pour le transfert des données. Les événements d'administrateur et les événements d'utilisateur sont enregistrés.

Vous pouvez configurer le serveur afin de collecter les informations suivantes :

- Les journaux système qui contiennent un enregistrement des actions effectuées par XenMobile.
- Les journaux d'audit qui contiennent un enregistrement chronologique des activités système de XenMobile.

Les informations de journal collectées par un serveur syslog à partir d'une appliance sont stockées dans un fichier journal sous forme de messages. Ces messages contiennent généralement les informations suivantes :

- L'adresse IP de l'appliance qui a généré le message de journal
- Un horodatage
- Le type de message
- Le niveau de journalisation associé à un événement (critique, erreur, remarque, avertissement, informatif, débogage, alerte ou urgence)
- Les informations de message

XenMobile utilise l'appender syslog log4j pour envoyer des messages syslog formatés RFC5424. Les données du message syslog sont du texte brut sans format spécifique.

Vous pouvez utiliser ces informations pour analyser la source de l'alerte et prendre des mesures correctives si nécessaire.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Syslog**. La page **Syslog** s'affiche.
3. Pour configurer ces paramètres :
    - **Serveur :** entrez une adresse IP ou le nom de domaine complet (FQDN) de votre serveur syslog.

- **Port :** saisissez le numéro du port. Le port est défini par défaut sur 514.
- **Informations à consigner :** sélectionnez ou désélectionnez **Journaux système** et **Audit**.
  - Les journaux système contiennent les actions effectuées par XenMobile.
  - Les journaux d'audit contiennent un enregistrement chronologique des activités système de XenMobile.
  - Journaux de débogage pour XenMobile.

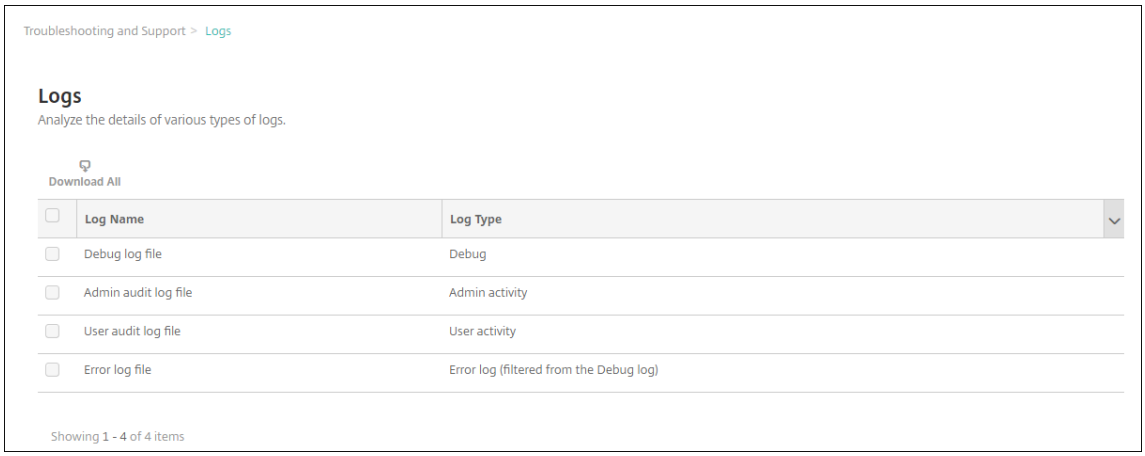
4. Cliquez sur **Enregistrer**.

Afficher les fichiers journaux dans XenMobile

September 21, 2021

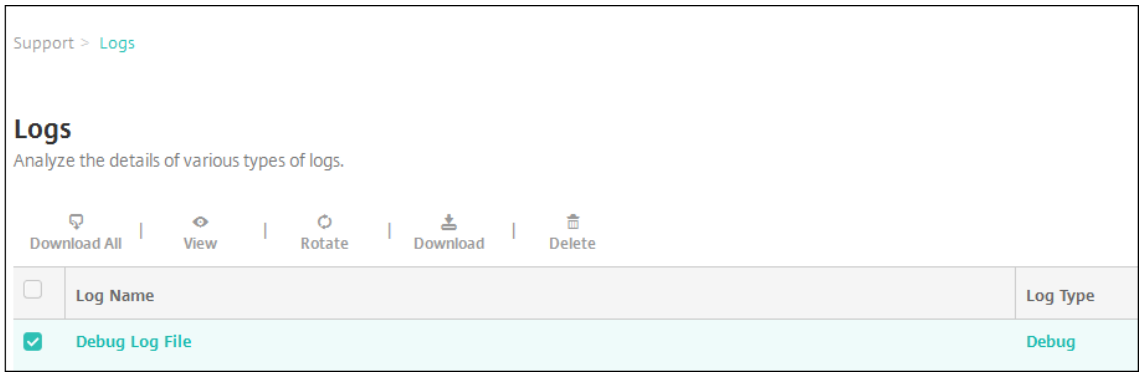
Affichez, manipulez et téléchargez des journaux pour faciliter la gestion avec XenMobile.

1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Support** s'ouvre.
2. Sous **Opérations du journal**, cliquez sur **Journaux**. La page **Journaux** s'affiche. Des journaux individuels apparaissent dans un tableau.



3. Sélectionnez le journal que vous souhaitez afficher :
   - Les fichiers journaux de débogage contiennent des informations utiles pour le support Citrix, telles que des messages d'erreur et des actions liées au serveur.
   - Les fichiers journaux d'audit administrateur contiennent des informations d'audit relatives à l'activité sur la console XenMobile.
   - Les fichiers journaux d'audit utilisateur contiennent des informations relatives aux utilisateurs configurés.
   - Les fichiers journaux d'erreur contiennent uniquement des messages d'erreur filtrés à partir du journal de débogage.

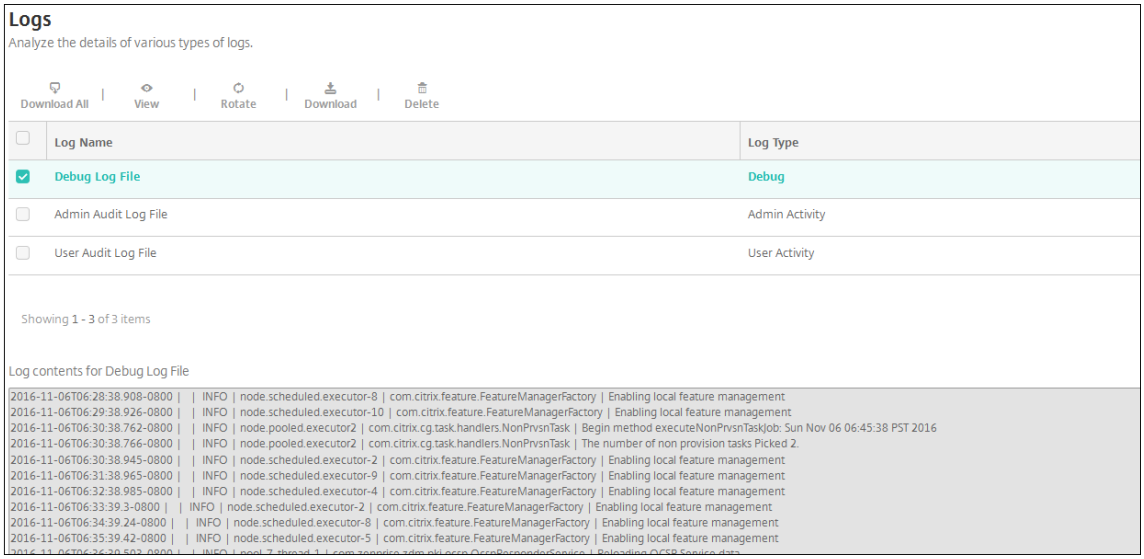
4. Utilisez les actions en haut du tableau pour télécharger tout, afficher, alterner, télécharger un journal ou supprimer le journal sélectionné.



> **Remarque :**
>
> - Si vous sélectionnez plus d'un fichier journal, seules les options **Tout télécharger** et **Alterner** sont disponibles.
> - Si vous avez mis en cluster des serveurs XenMobile, vous pouvez uniquement afficher les journaux pour le serveur auquel vous êtes connecté. Pour afficher les journaux d'autres serveurs, utilisez l'une des options de téléchargement.

5. Procédez comme suit :

   - **Tout télécharger :** la console télécharge tous les journaux présents sur le système (y compris les journaux de débogage, d'activité des utilisateurs/administrateurs, de serveur, etc.).
   - **Afficher :** affiche le contenu du journal sélectionné en dessous du tableau.
   - **Alterner :** archive le fichier journal actuel et crée un nouveau fichier pour capturer les entrées de journal. Une boîte de dialogue s'affiche lors de l'archivage d'un fichier journal ; cliquez sur Alterner pour continuer.
   - **Télécharger :** la console télécharge uniquement le type de fichier journal sélectionné ; elle télécharge également tous les journaux archivés pour ce même type.
   - **Supprimer :** supprime de manière définitive les fichiers journaux sélectionnés.



XenMobile Analyzer Tool

January 10, 2022

XenMobile Analyzer est un outil sur cloud que vous pouvez utiliser pour diagnostiquer et résoudre les problèmes de configuration de XenMobile ainsi que les problèmes liés à d'autres fonctionnalités. L'outil recherche les problèmes d'inscription d'utilisateurs et d'appareils et d'authentification dans votre environnement XenMobile.

Configurez l'outil afin qu'il pointe vers XenMobile Server et fournissez des informations, telles que le type de déploiement de serveur, la plate-forme mobile, le type d'authentification et les informations d'identification utilisateur. L'outil se connecte ensuite au serveur et analyse votre environnement afin de détecter d'éventuels problèmes de configuration. Si XenMobile Analyzer découvre des problèmes, l'outil fournit des recommandations visant à les résoudre.

Fonctionnalités principales

- Micro-service sécurisé dans le cloud permettant de dépanner tous les problèmes liés à XenMobile.
- Recommandations précises pour résoudre les problèmes avec la configuration de XenMobile.
- Réduction du nombre d'appels à l'assistance et accélération du dépannage des environnements XenMobile.
- Assistance le jour même pour les versions de XenMobile Server.
- Programmation des vérifications d'intégrité selon une fréquence quotidienne ou hebdomadaire.

- Vérifications de la configuration de Citrix ADC.
- Tests Secure Web pour l'accessibilité aux sites intranet.
- Vérifications du service de détection automatique Secure Mail.
- Vérifications du Single Sign-On (SSO) Citrix Files.

Nouveautés

- Le rapport de configuration Citrix ADC affiche une notification par badge indiquant le nombre de recommandations. Les recommandations sont basées sur les vérifications de configuration essentielles sur une passerelle Citrix Files Gateway particulière.
- Les icônes dans la barre de navigation globale sur la page de la liste d'environnements de test ont été réorganisées pour une meilleure expérience utilisateur.

La vidéo suivante présente les modifications de la navigation dans l'interface utilisateur.

Citrix XenMobile Analyzer : nouvelle interface utilisateur de liste d'environnement

Cette vidéo est intégrée. Cliquez sur le lien pour la visionner

> **Remarque :**
>
> Cette vidéo ne contient aucun son. Le mode plein écran est le mieux adapté pour le visionnage.

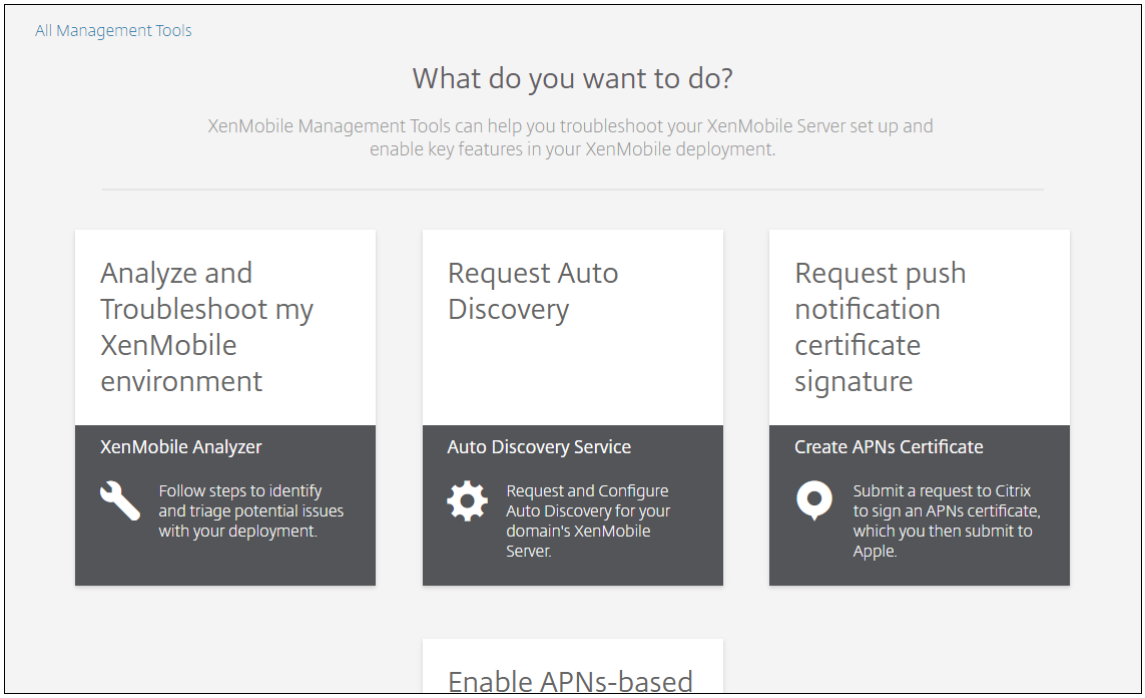
Accès à XenMobile Analyzer

Conditions préalables

Produit	Version prise en charge
XenMobile Server	10.1.0 et versions ultérieures
Citrix Gateway	10.5 et versions ultérieures
Simulation d'inscription de client	iOS et Android

Accédez à XenMobile Analyzer en utilisant l'une de ces méthodes :

- Dans la console XenMobile, cliquez sur l'icône de clé dans le coin supérieur droit pour ouvrir la page **Dépannage et support**.
- Utilisez les informations d'identification My Citrix pour accéder à l'outil depuis https://tools.xm.cloud.com/. Sur la page XenMobile Management Tools qui s'affiche, pour démarrer XenMobile Analyzer, cliquez sur **Analyze and Troubleshoot my XenMobile Environment**.



XenMobile Analyzer contient cinq options conçues pour vous guider à travers le processus de triage et réduire le nombre de tickets d'assistance. Ces options peuvent réduire les coûts pour tout le monde.

Les options sont les suivantes :

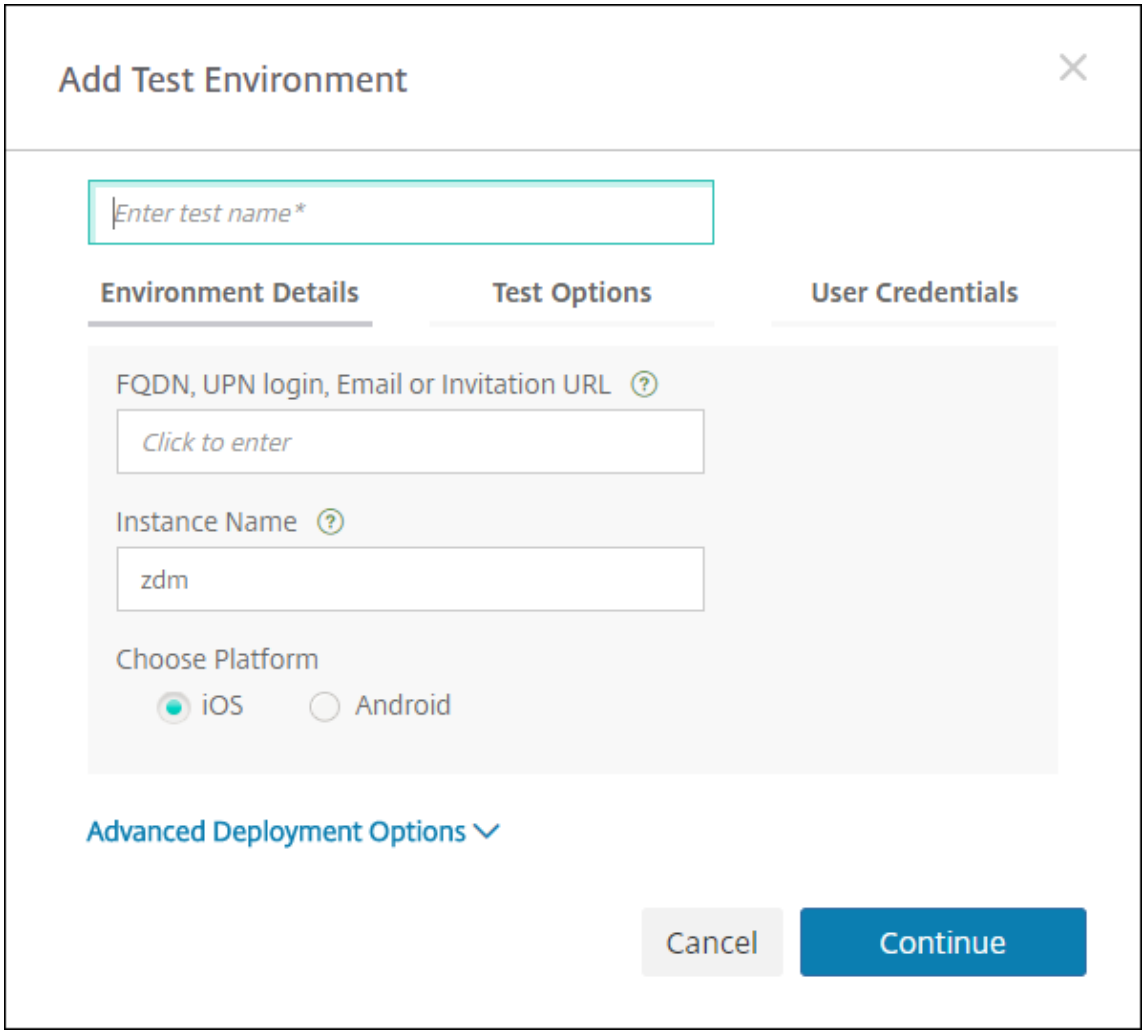
- **Environment Check :** cette étape vous guide dans la configuration de tests destinés à détecter les problèmes d'installation. L'étape propose également des recommandations et des solutions permettant des régler les problèmes d'appareil, d'inscription d'utilisateur et d'authentification.
- **Citrix ADC Check :** cette étape vous guide dans la vérification de vos configurations Citrix ADC pour la préparation au déploiement de XenMobile.
- **Advanced Diagnostics :** cette étape fournit des informations sur l'utilisation de Citrix Insight Services afin d'identifier d'autres problèmes éventuels que la vérification de l'environnement n'aurait pas détecté.
- **Server Connectivity Checks :** cette étape vous invite à tester la connectivité de vos serveurs.
- **Contact Citrix Support :** cette étape vous dirige vers le site à partir duquel vous pouvez créer un ticket de support technique Citrix si vous rencontrez toujours des problèmes.

Les sections suivantes décrivent chaque option de façon plus détaillée.

Vérification de l'environnement

1. Ouvrez une session sur XenMobile Analyzer et cliquez sur **XenMobile Environment**.

2. Cliquez sur **Add Test Environment**.
3. Dans la boîte de dialogue **Add Test Environment**, procédez comme suit :



a) Fournissez un nom unique pour le test, cela vous aidera à l'identifier dans le futur.

b) Dans **FQDN, UPN login, Email or URL Invitation**, entrez les informations qui seront utilisées pour accéder au serveur.

c) Dans **Instance Name**, si vous utilisez une instance personnalisée, vous pouvez fournir cette valeur.

d) Dans **Choose Platform**, sélectionnez **iOS** ou **Android** en tant que plate-forme pour le test.

e) Si vous développez **Advanced Deployment Options**, dans la liste **Deployment Mode**, vous pouvez sélectionner le mode de votre déploiement XenMobile. Les options disponibles sont **Enterprise (MDM + MAM)**, **App Management (MAM)** ou **Device Management (MDM)**.

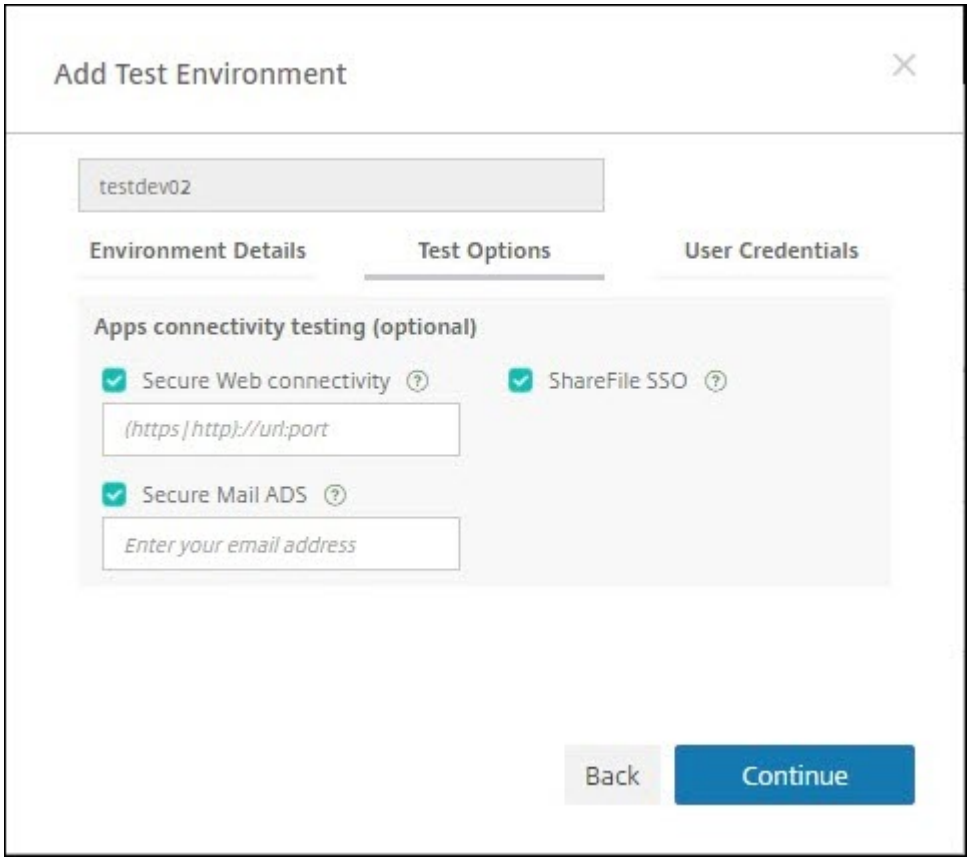
f) Cliquez sur **Continuer**.

4. Dans l'onglet **Test Options**, choisissez un ou plusieurs des tests suivants puis cliquez sur **Continue**.

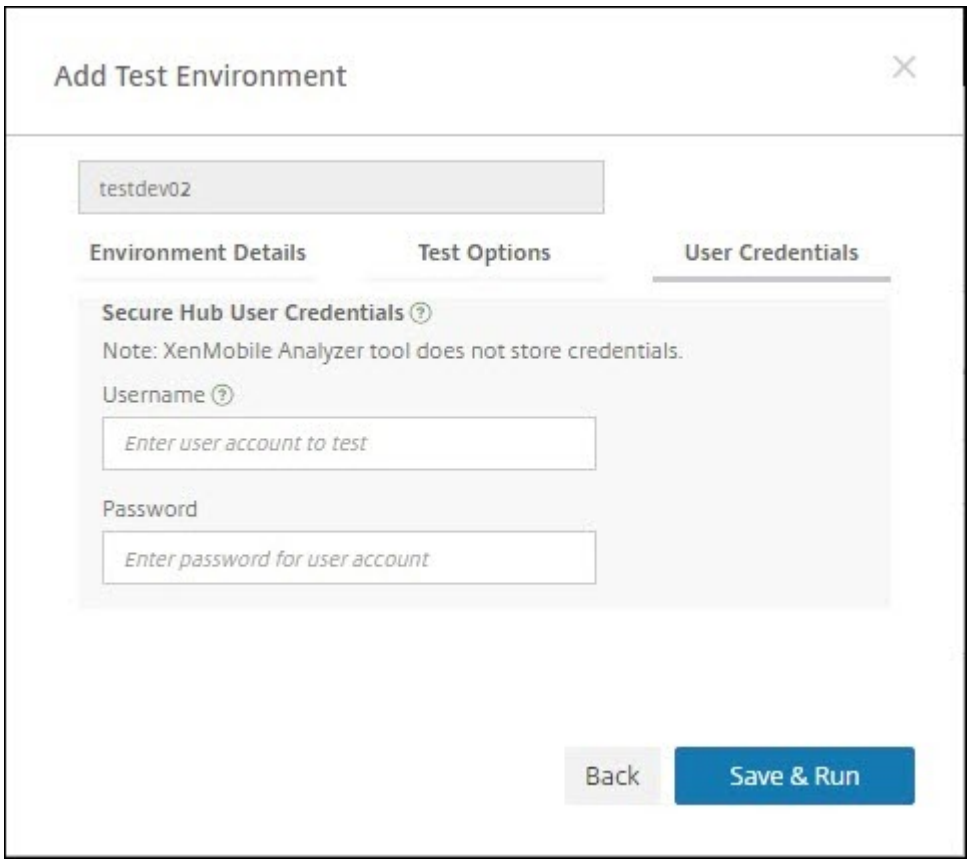
a) **Connectivité Secure Web**. Fournissez une adresse URL intranet. Cet outil teste l'accessibilité de l'adresse URL. Cette opération détecte s'il existe des problèmes de connectivité qui pourraient se produire dans l'application Secure Web lors de la tentative d'accès aux adresses URL intranet.

b) **Secure Mail ADS**. Entrez un ID d'e-mail utilisateur. Cet ID est utilisé pour tester la détection automatique de Microsoft Exchange Server dans votre environnement XenMobile. Il détecte s'il existe des problèmes liés à la détection automatique Secure Mail.

c) **ShareFile SSO**. Si cette option est sélectionnée, XenMobile Analyzer teste si la résolution DNS de Citrix Files s'effectue avec succès. L'outil vérifie également si Citrix Files Single Sign-On (SSO) est compatible avec les informations d'identification utilisateur fournies.



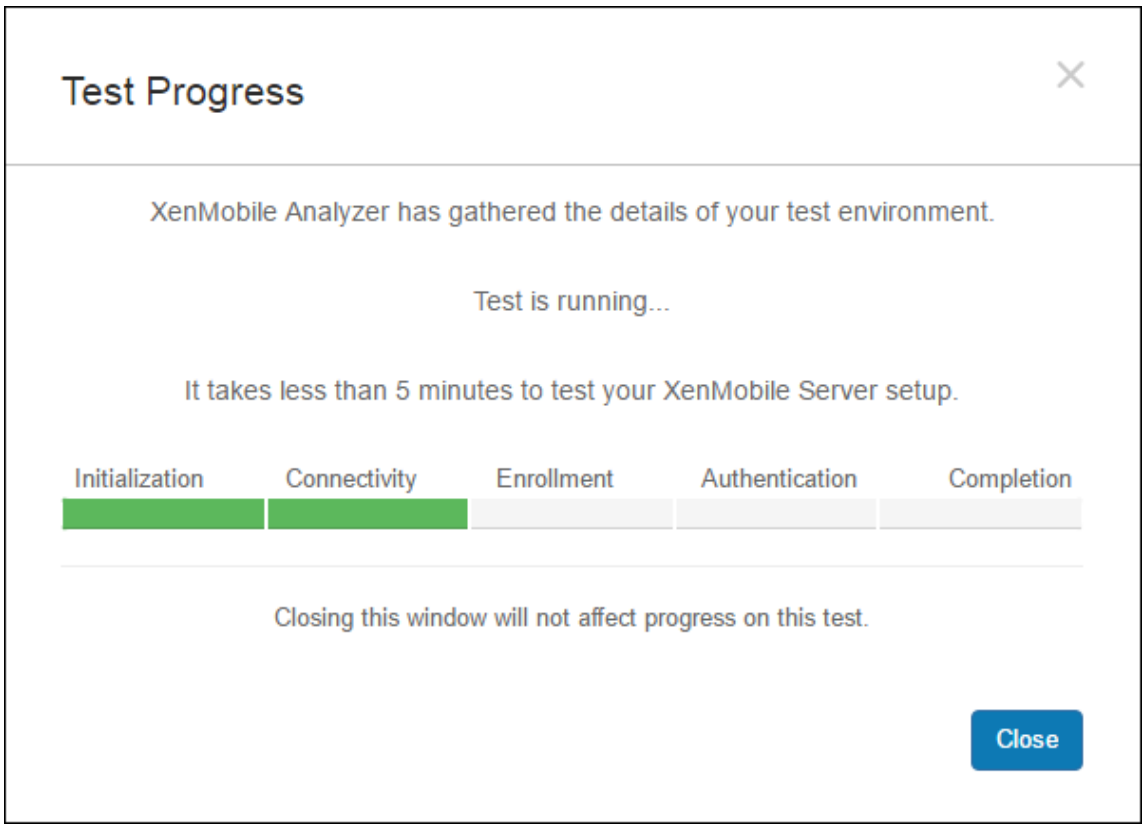
5. Sur l'onglet **User Credentials**, en fonction de la configuration de votre serveur, il est possible que différents champs soient disponibles. Les champs possibles sont **Username**, **Username et Password** ou **Username, Password** et **Enrollment PIN**.



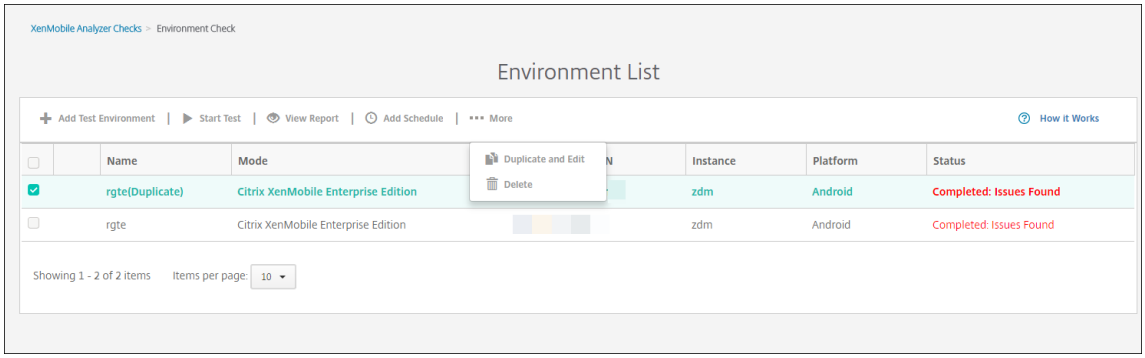
6. Cliquez sur **Save & Run** pour démarrer les tests.

   Une notification de progression s'affiche. Vous pouvez laisser la boîte de dialogue de progression ouverte ou la fermer et les tests continuent à s'exécuter.

   Les tests qui ont réussi s'affichent en vert. Ceux qui ont échoué s'affichent en rouge.



Après fermeture de la boîte de dialogue de progression, vous pouvez revenir à la page **Environments List**.



La page **Results** affiche les détails du test, des recommandations ainsi que les résultats.

7. Cliquez sur l'icône **View Report** pour voir les résultats des tests.

   Si les recommandations s'accompagnent d'articles de la base de connaissances Citrix, les articles sont répertoriés sur cette page.

8. Cliquez sur l'onglet **Results** pour afficher la catégorie et les tests individuels effectués par l'outil, avec leurs résultats.

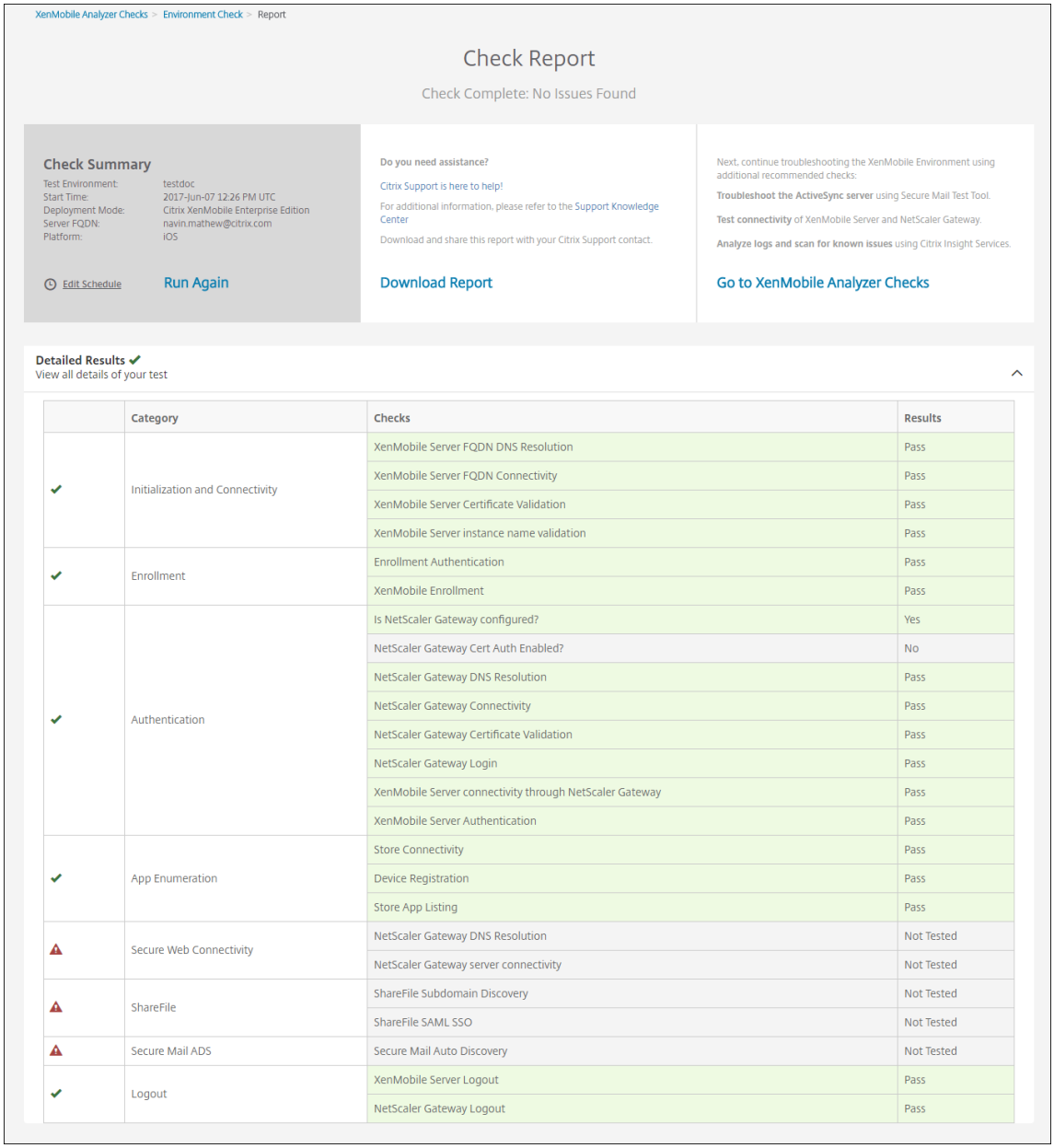
   a) Pour télécharger le rapport, cliquez sur **Download Report**.

   b) Pour revenir à la liste des environnements de test, cliquez sur **Environment Check**.

c) Pour réexécuter le même test, cliquez sur **Run Again**.

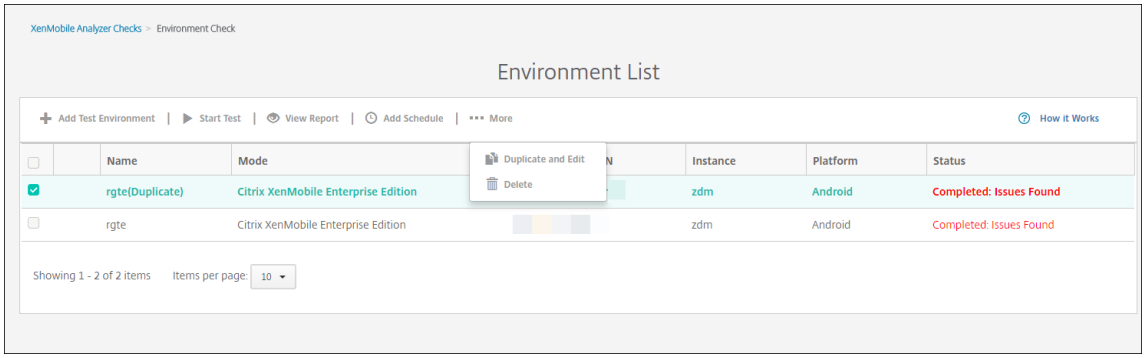
d) Si vous souhaitez réexécuter un autre test, revenez à **Test Environments**, sélectionnez le test et cliquez sur **Start Test**.

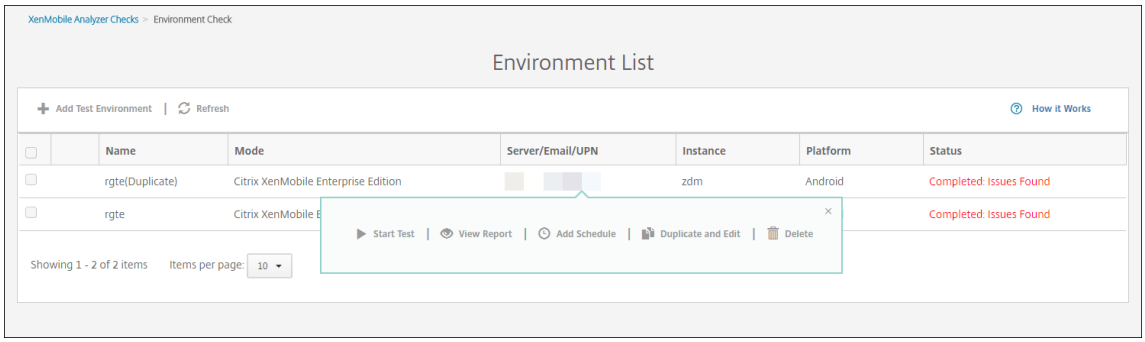
e) Pour sélectionner une autre option de XenMobile Analyzer, cliquez sur **Go To XenMobile Analyzer Checks**.

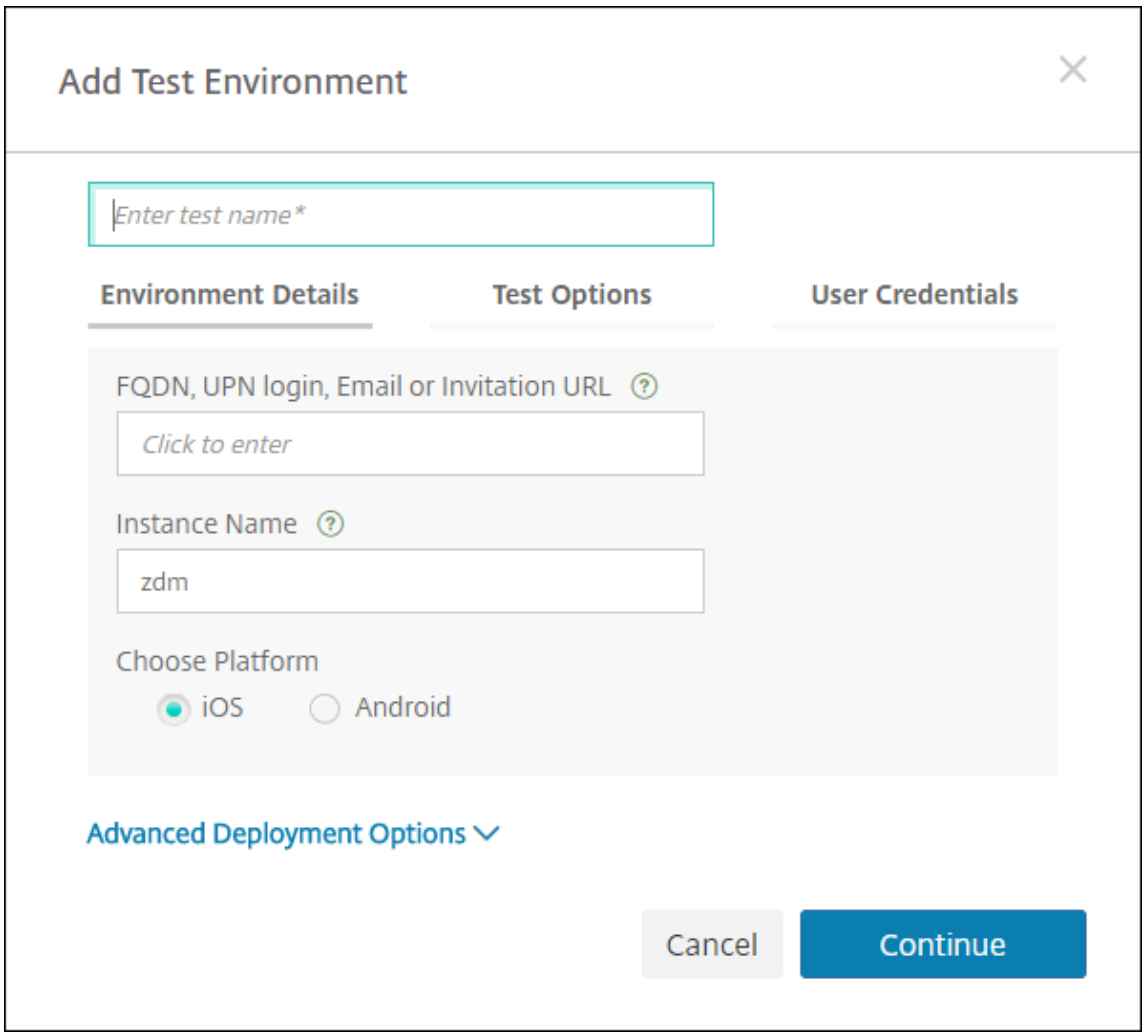


9. À partir de la page Test Environments, vous pouvez copier et modifier des tests. Pour ce faire, sélectionnez un test, cliquez sur **More** et sélectionnez **Duplicate and Edit**.

   Une copie du test sélectionné sera créée et la boîte de dialogue Add Test Environment s'ouvrira, ce qui vous permet de modifier le nouveau test.



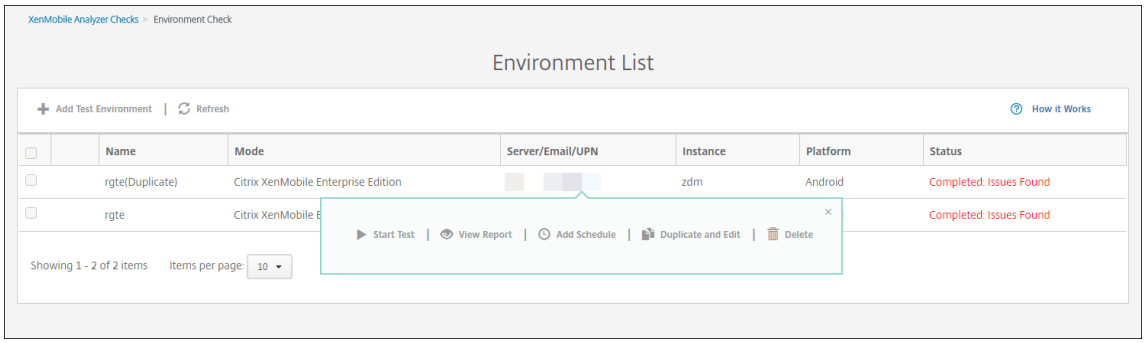




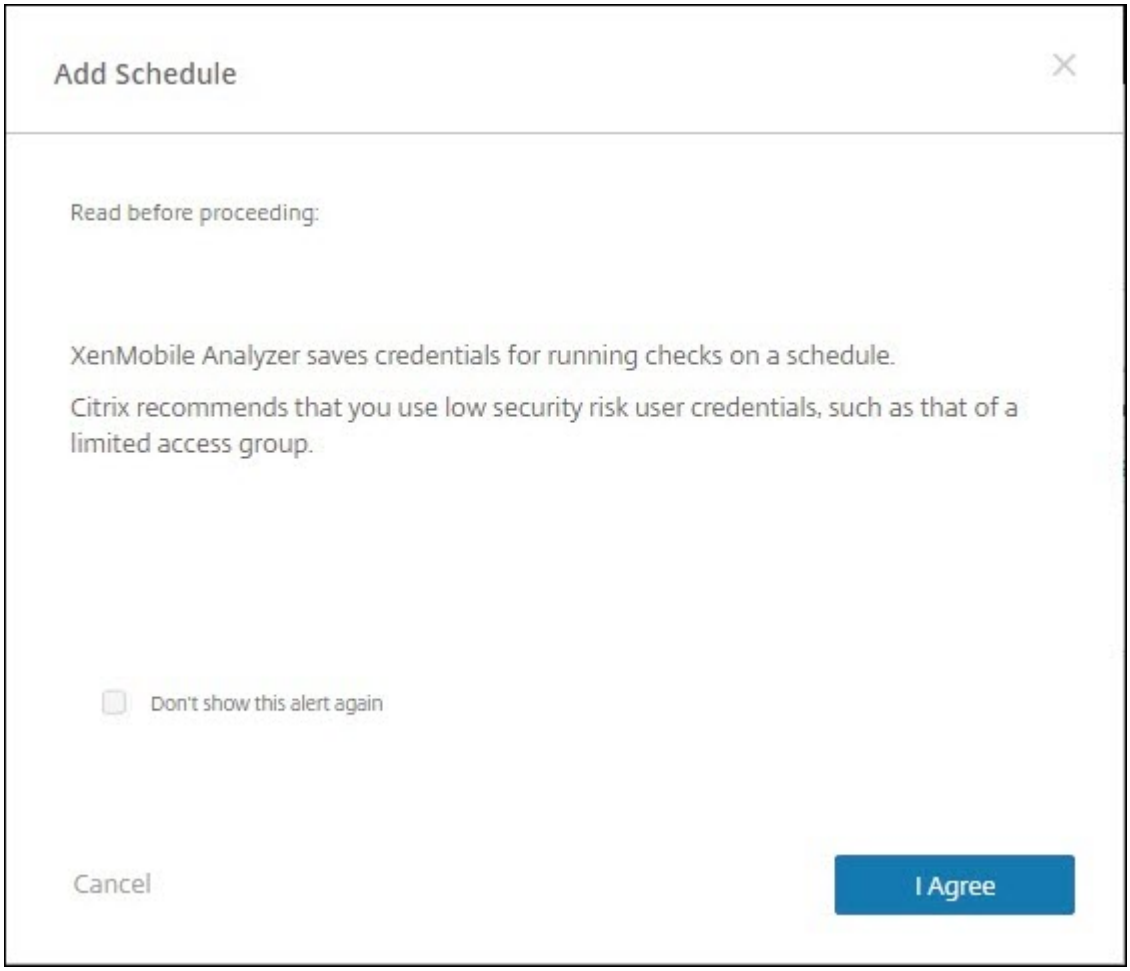
Ajout d'un programme pour les vérifications de l'environnement

Vous pouvez configurer des tests à exécuter selon un programme automatique avec envoi des résultats à une liste d'utilisateurs que vous définissez.

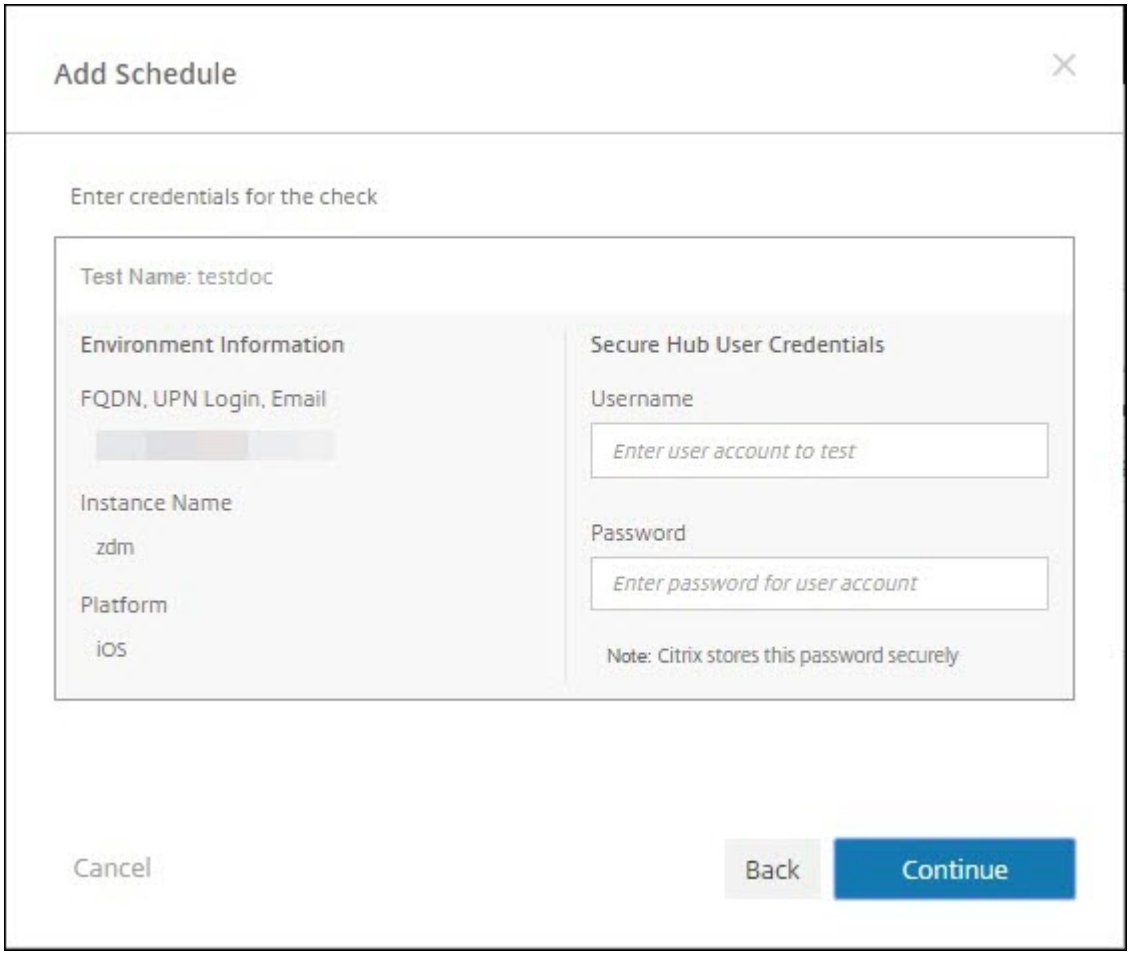
1. Sur la page **Environment List**, sélectionnez l'environnement pour lequel vous souhaitez définir un programme, cliquez sur **Add Schedule**.



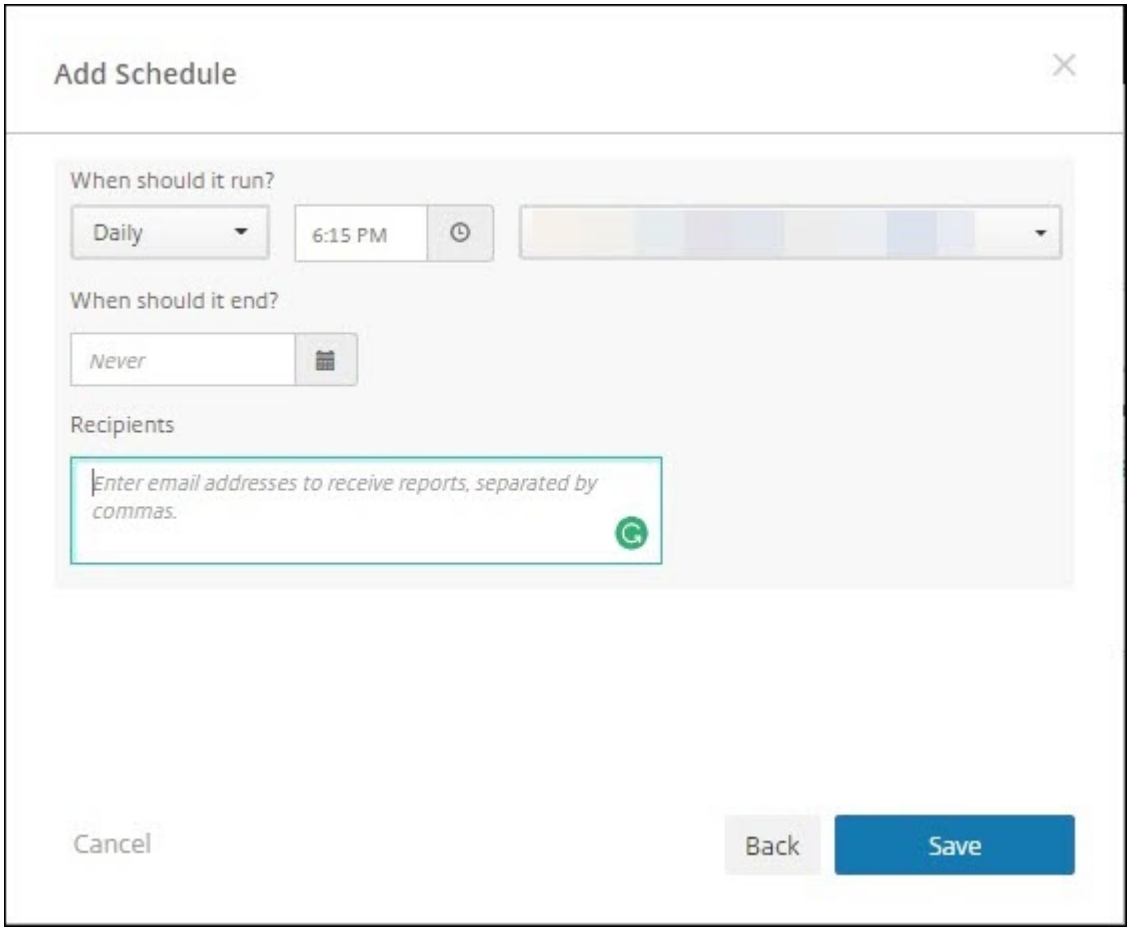
2. La fenêtre **Add Schedule** affiche un message vous avertissant que XenMobile Analyzer enregistre les informations d'identification pour l'exécution des tests selon un programme. Citrix recommande que vous utilisiez un compte possédant un accès limité pour l'exécution de tests programmés. Cliquez sur **I Agree** pour continuer.



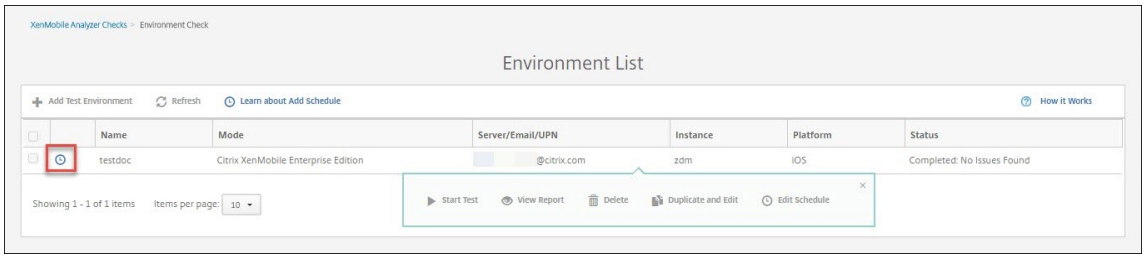
3. Entrez un **nom d'utilisateur** et un **mot de passe** pour exécuter le test.



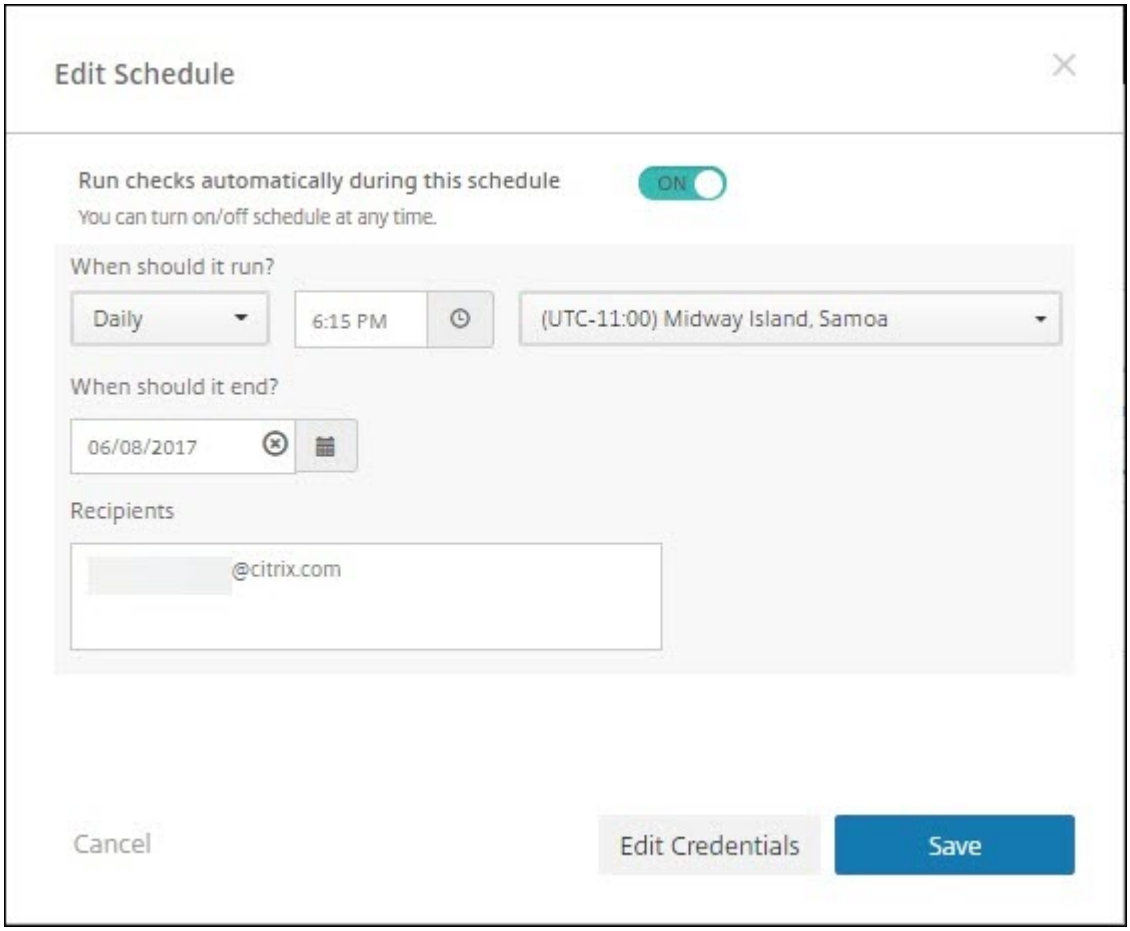
4. Configurez un programme pour le test à exécuter. Vous pouvez sélectionner **Daily** (quotidien) ou **Weekly** (hebdomadaire) dans le menu déroulant. Sélectionnez une heure de la journée pour exécuter le test ainsi que le fuseau horaire. Utilisez le sélecteur de date pour sélectionner une date d'arrêt du test programmé ou laissez le champ vide pour que le test s'exécute indéfiniment. Entrez une liste d'adresses e-mail qui recevront les rapports, séparées par des virgules : Cliquez sur **Enregistrer**.



5. Un symbole d'horloge à gauche de votre test indique qu'un programme est configuré. Si vous sélectionnez votre test, vous pouvez cliquer sur **Edit Schedule** pour changer le programme.



6. Dans cette fenêtre, vous pouvez modifier le programme du test. Vous pouvez également le désactiver, en cliquant sur le commutateur en haut. Cliquez sur **Save** lorsque vous avez terminé.



Autres vérifications informatives

Vous pouvez interagir directement avec l'étape Environment Check de XenMobile Analyzer pour effectuer des tests, alors que les autres options sont purement informatives. Chacune de ces options fournit des informations concernant d'autres outils de support que vous pouvez utiliser pour vous assurer que votre environnement XenMobile est configuré correctement.

- **Advanced Diagnostics :** vous invite à recueillir des informations sur votre environnement, puis à les charger sur Citrix Insight Services. L'outil analyse vos données et fournit un rapport personnalisé avec les résolutions recommandées.
- **Secure Mail Readiness :** vous invite à télécharger et exécuter l'application XenMobile Exchange ActiveSync Test. L'application veille à ce que les serveurs ActiveSync soient prêts en vue de leur déploiement dans des environnements XenMobile. Une fois l'application exécutée, vous pouvez afficher les rapports ou les partager avec d'autres utilisateurs.
- **Server Connectivity Checks :** fournit des instructions sur la vérification de vos connexions à XenMobile, de l'authentification et des serveurs Content Collaboration.
- **Contact Citrix Support :** en dernier ressort, vous pouvez créer un ticket d'assistance auprès de l'assistance Citrix.

Problèmes connus

Les problèmes suivants sont connus dans XenMobile Analyzer :

- La saisie de plusieurs adresses URL dans la zone de texte n'est pas prise en charge lors des tests de connectivité Secure Web.
- La fonctionnalité d'authentification des appareils partagés de Secure Hub n'est pas prise en charge.
- Les tests Secure Web vérifient uniquement la connectivité avec les adresses URL saisies et non l'authentification avec les sites correspondants.

Problèmes résolus

Les problèmes suivants avec XenMobile Analyzer ont été résolus :

- Lors de l'exécution d'une vérification à l'aide de l'invitation d'inscription, le test réussit mais l'invitation d'inscription n'est pas utilisée.

API REST

January 10, 2022

> **Remarque :**
>
> Cet article traite des API REST pour XenMobile Server. Pour les API REST pour Endpoint Management, consultez la section API REST.

Avec l'API REST XenMobile, vous pouvez appeler les services qui sont exposés au travers de la console XenMobile. Vous pouvez appeler les services REST à l'aide d'un client REST quelconque. L'API n'exige pas de connexion à la console XenMobile pour appeler les services.

Pour consulter une liste complète des API actuellement disponibles, téléchargez le PDF Public API for REST Services.

Autorisations requises pour accéder à l'API REST

Pour accéder à l'API REST, vous devez disposer de l'une des autorisations suivantes :

- Autorisation d'accès à l'API publique définie dans le cadre de la configuration de l'accès basé sur rôle. Pour plus d'informations, veuillez consulter la section Configuration de rôles avec RBAC.
- Autorisation de super utilisateur

Pour appeler les services D'API REST

Vous pouvez appeler les services d'API REST à l'aide du client REST ou de commandes CURL. Les exemples suivants utilisent le client Advanced REST pour Chrome.

> **Remarque :**
>
> Dans les exemples suivants, modifiez le nom de l'hôte et le numéro de port afin qu'ils correspondent à votre environnement.

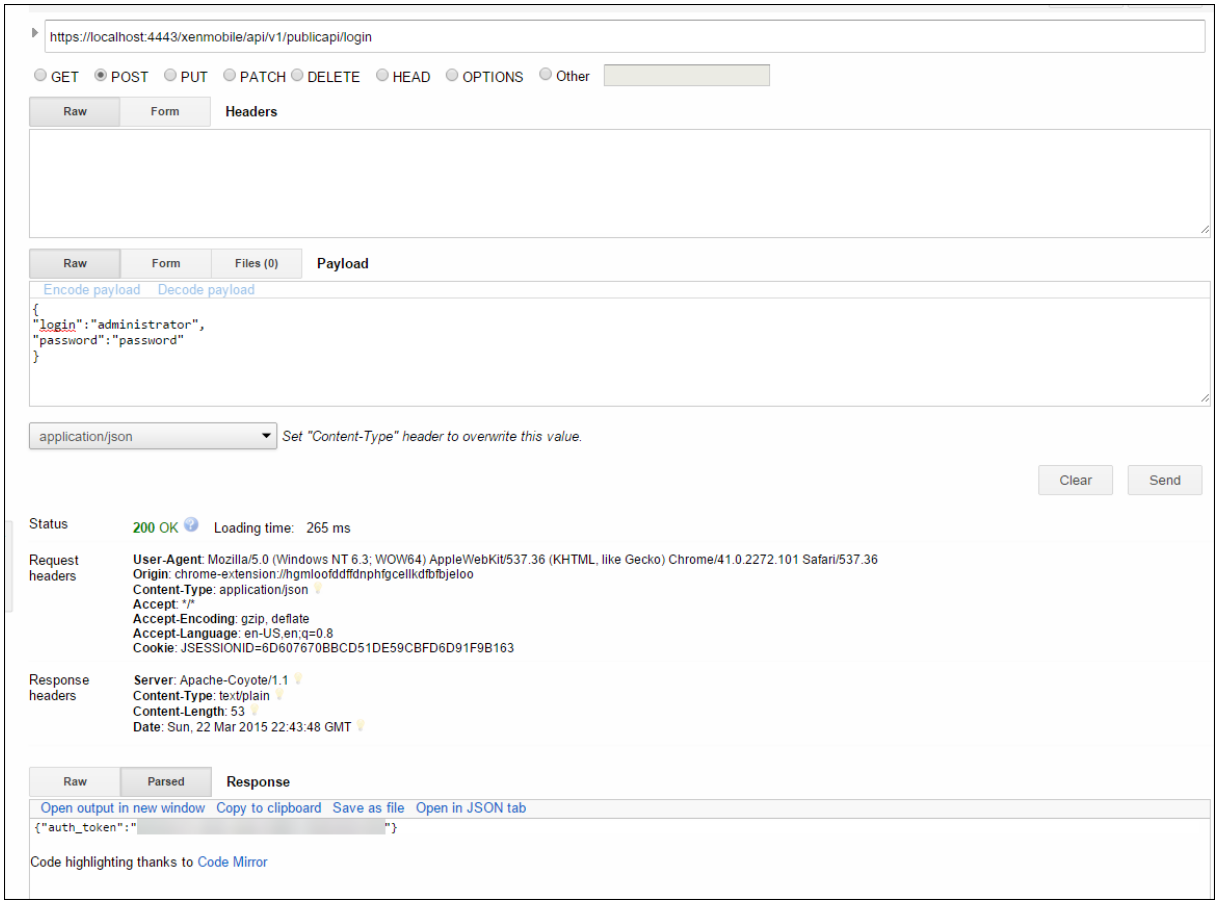
Connexion

URL : `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

Requête : `{ "login":"administrator", "password":"password"}`

Type de méthode : POST

Type de contenu : application/json



Informations connexes

- API REST XenMobile

Endpoint Management Connector pour Exchange ActiveSync

January 10, 2022

XenMobile Mail Manager est maintenant nommé Endpoint Management Connector pour Exchange ActiveSync. Pour plus de détails sur le portefeuille unifié de Citrix, consultez le guide des produits Citrix.

Le connecteur étend les capacités de XenMobile des façons suivantes :

- Contrôle d'accès dynamique des appareils EAS (Exchange Active Sync). L'accès des appareils EAS aux services Exchange peut être automatiquement autorisé ou bloqué.
- Permet à XenMobile d'accéder aux informations de partenariat d'appareil EAS fournies par Exchange.
- Permet à XenMobile d'effacer un appareil mobile en fonction de l'état EAS.
- Permet à XenMobile d'accéder à des informations sur des appareils Blackberry, et de réaliser des opérations de contrôle telles que l'effacement à distance (Wipe) et la réinitialisation du mot de passe (ResetPassword).

Pour effacer un appareil en fonction de l'état EAS, configurez une action automatisée avec un déclencheur ActiveSync. Consultez la section Actions automatisées.

Pour télécharger Endpoint Management Connector pour Exchange ActiveSync :

1. Accédez à https://www.citrix.com/downloads.
2. Accédez à **Citrix Endpoint Management (et Citrix XenMobile Server) > XenMobile Server (local) > Logiciel produit > XenMobile Server 10 > Composants serveur**.
3. Sur la vignette **Citrix Endpoint Management connector for Exchange ActiveSync**, cliquez sur **Download File**.

Nouveautés

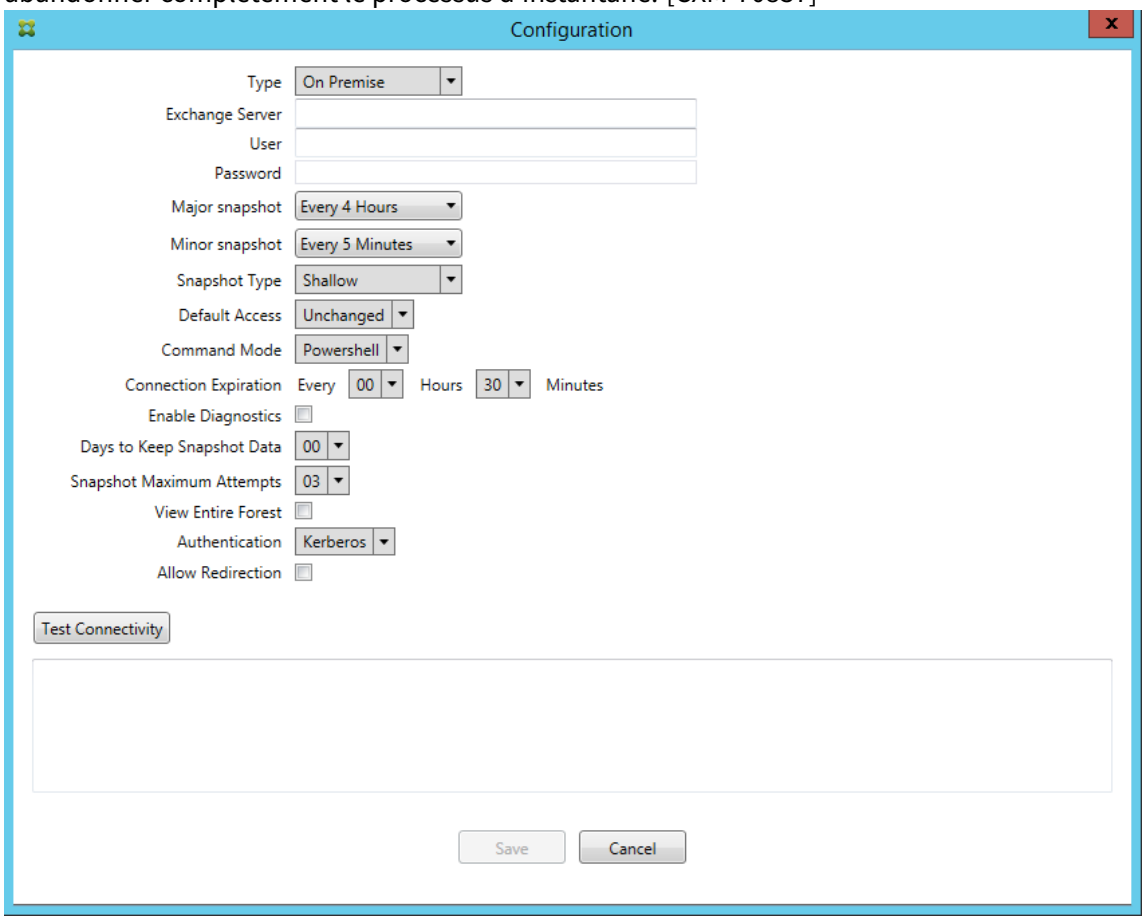
Les sections suivantes répertorient les nouveautés d'Endpoint Management Connector pour Exchange ActiveSync, anciennement XenMobile Mail Manager.

Nouveautés dans la version 10.1.10

Les problèmes suivants ont été résolus dans la version 10.1.10 :

- Les clients qui rencontrent des problèmes réseau fréquents peuvent ne pas être en mesure de réaliser un instantané au cours des trois tentatives qui étaient précédemment fournies. Avec cette version, un administrateur peut configurer le nombre maximum de tentatives (1-10). Ce correctif permet à un instantané de subir plusieurs interruptions de communication sans

abandonner complètement le processus d'instantané. [CXM-70837]



- Dans les versions précédentes, le type d'instantané n'apparaissait pas dans la liste des configurations Exchange. Maintenant, le type d'instantané apparaît. [CXM-70846]
- L'exception PSRemotingTransport signalée par PowerShell indique que la session vers Exchange n'est plus viable. L'état est ajouté par défaut à la liste Erreurs critiques dans le fichier de configuration. Ce faisant, lorsque l'exception PSRemotingTransport est détectée, la connexion est marquée comme une Erreur à des fins d'élimination ultérieure. La communication suivante utilise une connexion valide ou crée une nouvelle connexion. [XMHELP-2184, CXM-70836]
- Lorsqu'une modification de configuration est enregistrée, il est possible que les composants internes configurés précédemment n'aient pas tous été supprimés correctement avant de charger la nouvelle configuration. Ce problème peut conduire à un comportement imprévisible. Le comportement dépend de la modification spécifique et si la modification est en conflit avec la configuration précédente. Dans cette version, tous les composants internes sont supprimés avant de charger la nouvelle configuration. [XMHELP-2259, CXM-71388]

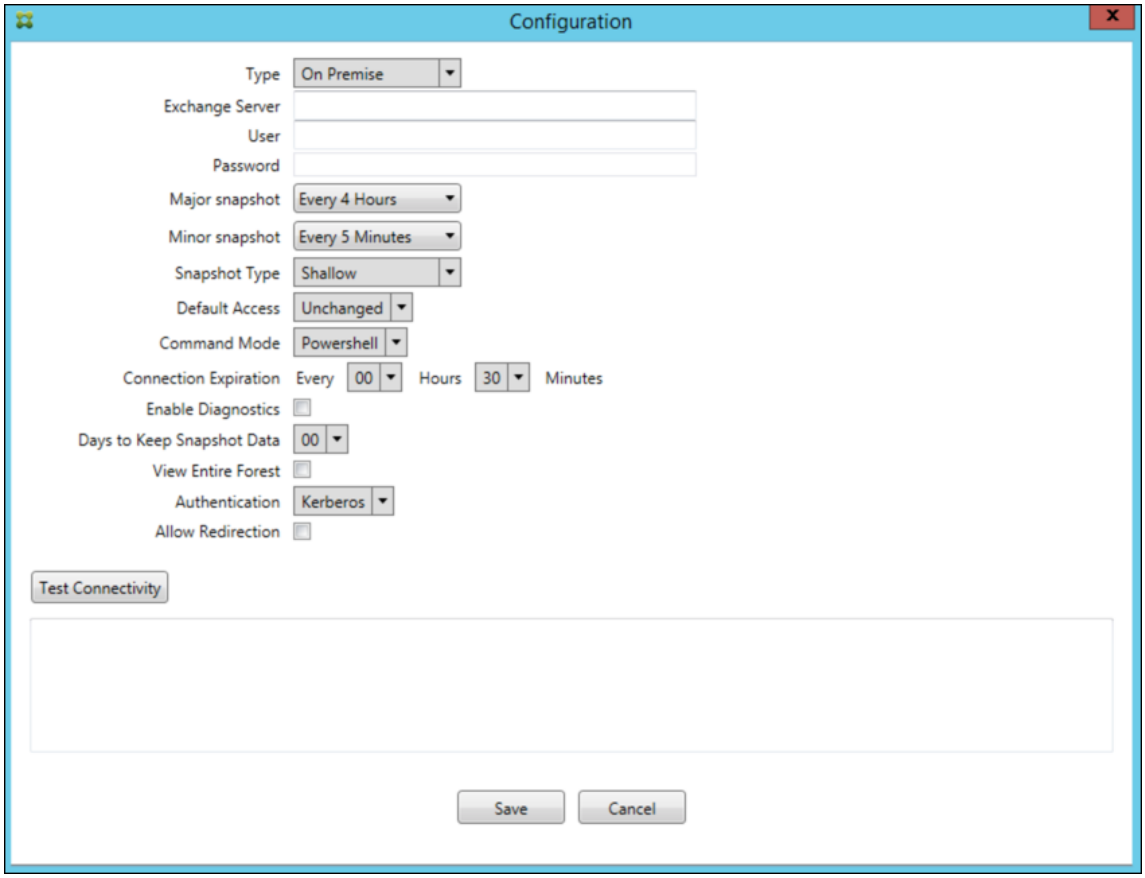
Nouveautés dans les versions précédentes

La section suivante répertorie les fonctionnalités et les problèmes résolus dans les versions antérieures de Endpoint Management Connector pour Exchange ActiveSync.

Nouveautés dans la version 10.1.9

Les problèmes suivants ont été résolus dans la version 10.1.9 :

- Les modifications de configuration sont désormais gérées de manière plus cohérente. Lorsque le service détecte un changement de configuration, chaque sous-système interne est arrêté, ce qui signifie que tout traitement actif ou planifié est interrompu. Ensuite, la nouvelle configuration est chargée et les sous-systèmes sont redémarrés, ce qui signifie que tous les programmes et autres infrastructures internes sont rétablis avec de nouveaux paramètres. Ce problème corrige un problème connu dans la version 10.1.8. [CXM-47709, CXM-61330]
- Lors d'une mise à niveau, la configuration de base de données existante n'était pas fusionnée dans le nouveau fichier de configuration. La configuration de base de données est maintenant fusionnée dans le fichier de configuration mis à niveau. [CXM-49326]
- Dans les fichiers de diagnostic liés aux instantanés, les en-têtes de colonne étaient manquants. Les en-têtes sont restaurés. [CXM-62680]
- Lors de la mise à niveau à partir d'une version précédente, la section par défaut du fichier de configuration était remplacée par la section analogue du fichier de configuration utilisé. Ce problème empêchait les ajouts ou les améliorations à la section par défaut d'être chargés par le service après la mise à niveau. À partir de cette version, la section par défaut reflète toujours la dernière configuration. [CXM-62681]
- Les administrateurs ne peuvent plus accéder à certaines options en appuyant sur Maj lors de l'exécution de l'application. Ces options étaient auparavant disponibles avec l'autorisation Citrix. Certaines options sont désormais entièrement disponibles, telles que Autoriser la redirection, tandis que d'autres, telles que Détection de blocage et Correction de comptage, sont obsolètes. [CXM-62767]



Nouveautés dans la version 10.1.8

Les problèmes suivants ont été résolus dans la version 10.1.8 :

- Il est possible qu'Exchange limite trop fréquemment l'envoi de commandes par le service de Citrix Endpoint Management Connector pour Exchange ActiveSync. C'est un comportement courant dans les connexions à Office 365. Avec cette limitation, le service doit se mettre en pause pendant une période de temps spécifiée avant d'envoyer la commande suivante. La console Configurer affiche désormais le temps de pause restant. [CXM-48044]
- Lorsque des modifications sont apportées aux sections « Watchdog » ou « SpecialistsDefaults » du fichier de configuration (config.xml), les modifications ne sont pas reflétées dans le fichier de configuration après une mise à niveau. Avec cette version, les modifications sont fusionnées correctement dans le nouveau fichier de configuration. [CXM-52523]
- Plus de détails ont été ajoutés aux analyses envoyées à Google Analytics, notamment concernant les instantanés. [CXM-56691]
- La fonctionnalité de connectivité de test Exchange tentait d'initialiser la connexion une seule fois. Étant donné que les connexions Office 365 peuvent être limitées, il était possible qu'une connectivité de test semble échouer lors de la limitation. Le connecteur Citrix Endpoint Management pour Exchange ActiveSync tente désormais d'initier une connexion jusqu'à trois fois.

[CXM-58180]

- Afin d'appliquer des stratégies sur Exchange, le connecteur Citrix Endpoint Management pour Exchange ActiveSync doit compiler une commande **Set-CASMailbox** qui inclut tous les appareils concernés pour chaque boîte aux lettres, dans deux listes : autoriser et bloquer. Si un appareil n'est pas inclus dans l'une ou l'autre des listes, Exchange revient à son état d'accès par défaut. Si cet état d'accès par défaut est différent de l'état souhaité pour un appareil, cet appareil n'est plus conforme. Par conséquent, un utilisateur peut perdre l'accès à son courrier électronique si l'état d'accès par défaut d'Exchange est bloqué alors qu'il devrait être autorisé. Ou bien, un utilisateur dont l'accès au courrier électronique devrait être bloqué peut se voir accorder l'accès. Le connecteur Citrix Endpoint Management pour Exchange ActiveSync garantit désormais que tous les appareils avec un état souhaité valide sont inclus dans chaque commande **Set-CasMailbox**. [CXM-61251]

Le problème suivant est connu dans la version 10.1.8 :

Si un administrateur apporte une modification dans l'application Configurer qui modifie les données de configuration, alors que le service effectue des opérations de longue durée, telles qu'un instantané ou une évaluation des stratégies, le service peut entrer dans un état indéterminé. Un symptôme peut être que les modifications de stratégie ne sont pas traitées ou que les instantanés ne sont pas initiés. Pour rétablir l'état de fonctionnement du service, il doit être redémarré. Vous devrez peut-être utiliser le gestionnaire de services Windows pour mettre fin au processus avant de démarrer le service. [CXM-61330]

Nouveautés dans la version 10.1.7

- XenMobile Mail Manager est maintenant nommé Endpoint Management Connector pour Exchange ActiveSync.
- L'option **Disable Pipelining** dans la boîte de dialogue de configuration Exchange est désormais obsolète. Vous pouvez obtenir la même fonctionnalité en configurant plusieurs étapes pour chaque commande dans le fichier config.xml. [CXM-54593]

Les problèmes suivants ont été résolus dans la version 10.1.7 :

- Dans la fenêtre de l'historique des instantanés, les messages d'erreur peuvent être affichés avec peu de contexte. À présent, les messages d'erreur sont précédés du contexte dans lequel les erreurs se sont produites. [CXM-49157]
- Le fichier XmmGoogleAnalytics.dll ne possédait pas la version de fichier correspondante à la version commerciale. [CXM-52518]
- Pour améliorer les diagnostics, nous avons récemment modifié le format de chaîne relatif à une liste d'ID d'appareils utilisés pour définir l'état Autorisé/Bloqué de la boîte aux lettres. Cependant, si un nombre trop important d'appareils est spécifié, la taille de chaîne maximale est dépassée. Nous utilisons maintenant une structure de données de tableau interne. Cette structure

n'a pas de limite de taille et formate également les données de manière appropriée à des fins de diagnostic. [CXM-52610]

- Lorsque des stratégies d'appareil qui ne sont pas synchronisées avec Exchange sont détectées, leurs commandes peuvent inclure des appareils n'appartenant pas à la boîte aux lettres appropriée. Endpoint Management Connector pour Exchange ActiveSync s'assure désormais que les commandes destinées à Exchange représentent uniquement les appareils appartenant à leurs boîtes aux lettres respectives. [CXM-54842]
- Dans certains environnements, un assembly Microsoft n'est pas disponible. L'assembly requis est maintenant explicitement installé avec l'application. [CXM-55439]
- Si les noms uniques d'appareils ou de boîtes aux lettres comportent des espaces entre le nom de l'attribut et le signe égal et/ou des espaces après le signe égal et avant la valeur, Endpoint Management Connector pour Exchange ActiveSync peut ne pas faire correspondre un appareil à sa boîte aux lettres, et inversement. Par conséquent, certains appareils et/ou boîtes aux lettres peuvent être rejeté(e)s lors du rapprochement des instantanés. [CXM-56088]

> **Remarque :**
>
> Les sections suivantes font référence à Endpoint Management Connector pour Exchange ActiveSync sous son ancien nom XenMobile Mail Manager. Le nom a changé à partir de la version 10.1.7.

Mise à jour dans la version 10.1.6.20

Une mise à jour vers 10.1.6 contient le correctif suivant dans la version 10.1.6.20 :

- Lorsque des stratégies d'appareil qui ne sont pas synchronisées avec Exchange sont détectées, leurs commandes peuvent inclure des appareils n'appartenant pas à la boîte aux lettres appropriée. XenMobile Mail Manager s'assure désormais que les commandes destinées à Exchange représentent uniquement les appareils appartenant à leurs boîtes aux lettres respectives. [CXM-54842]

Nouveautés dans la version 10.1.6

XenMobile Mail Manager version 10.1.6 contient les améliorations et les problèmes résolus suivants :

- La fenêtre d'historique des instantanés entre parfois dans un état où la fenêtre n'est plus mise à jour. Le mécanisme d'actualisation de Windows a été amélioré pour une mise à jour plus fiable. [CXM-47983]
- Deux modes et chemins de code distincts étaient utilisés pour les instantanés partitionnés et non partitionnés. Étant donné que les instantanés non partitionnés sont équivalents aux instantanés partitionnés avec une configuration utilisant une seule partition "*", le mode instantané non partitionné a été éliminé. Le mode instantané par défaut est désormais partitionné avec 36 partitions (0-9, A-Z). [CXM-49093]

- Dans la fenêtre de l'historique des instantanés, les messages d'erreur sont écrasés par les messages d'état. Désormais, XenMobile Mail Manager fournit deux champs distincts pour que les utilisateurs puissent voir l'état et les erreurs simultanément. [CXM-51942]
- Lors de la connexion à Exchange Online (Office 365), les requêtes liées aux images instantanées pouvaient entraîner des données tronquées. Ce problème peut se produire lorsque XenMobile Mail Manager exécute un script en pipeline à plusieurs commandes. La commande en amont ne peut pas transmettre les données assez rapidement à la commande en aval, qui termine alors le travail prématurément ; en conséquence, les données sont incomplètes. XenMobile Mail Manager peut maintenant reproduire le pipeline lui-même et attendre que la commande en amont soit effectuée avant d'appeler la commande en aval. Ce changement devrait entraîner le traitement et la capture de toutes les données. [CXM-52280]
- Si une erreur non résolue se produit dans une commande de mise à jour de stratégie vers Exchange, la même commande est renvoyée à la file d'attente de travail à plusieurs reprises pendant une longue période. Cette situation entraînait l'envoi de la commande à Exchange à plusieurs reprises. Dans cette version de XenMobile Mail Manager, une commande entraînant une erreur est renvoyée à la file d'attente uniquement un nombre discret de fois. [CXM-52633]
- Si une mise à jour de stratégie pour une boîte aux lettres spécifique impliquait l'autorisation ou le blocage de tous les appareils : la commande **Set-CASMailbox** émise échouait car la liste vide était convertie en une chaîne vide au lieu de **NULL**. Désormais, les données correctes sont envoyées. [CXM-53759]
- Lors du traitement d'un nouvel appareil, Exchange peut renvoyer l'état "DeviceDiscovery" pendant un certain temps (généralement 15 minutes). XenMobile Mail Manager ne traitait pas spécifiquement cet état. XenMobile Mail Manager gère maintenant cet état. Dans l'onglet Monitor de l'interface utilisateur, les utilisateurs peuvent filtrer les appareils dans cet état. [CXM-53840]
- XenMobile Mail Manager ne vérifiait pas la possibilité d'écrire dans la base de données XenMobile Mail Manager. Par conséquent, si les autorisations étaient restreintes, le comportement était imprévisible. XenMobile Mail Manager capture et valide désormais les autorisations requises à partir de la base de données. XenMobile Mail Manager indique les autorisations restreintes lors du test de la connexion (message affiché) ou dans l'indicateur Base de données (survol du message) en bas de la fenêtre principale de configuration. [CXM-54219]
- Selon la charge de travail en cours, lorsqu'il est dirigé vers XenMobile Mail Manager, le service peut ne pas s'arrêter rapidement. Par conséquent, le service semble être dans un état qui ne répond pas. Les améliorations permettent d'interrompre les tâches en cours, entraînant un arrêt plus rapide. [CXM-54282]

Nouveautés dans la version 10.1.5

XenMobile Mail Manager version 10.1.5 contient les problèmes résolus suivants :

- Lorsque Exchange applique une limitation aux activités de XenMobile Mail Manager, rien

n'indique (en dehors des journaux) que la limitation est en cours. Avec cette version, un utilisateur peut survoler l'instantané actif et un état de limitation apparaît. De plus, pendant que XenMobile Mail Manager est limité, le début d'un instantané majeur est interdit jusqu'à ce que Exchange mette fin à la limitation. [CXM-49617]

- Si XenMobile Mail Manager est limité par Exchange au cours d'un instantané majeur : il est possible qu'un délai insuffisant s'écoule avant la prochaine tentative d'instantané. Ce problème entraîne une limitation supplémentaire et l'échec de l'instantané. XenMobile Mail Manager attend maintenant le délai minimum spécifié par Exchange entre les tentatives d'instantanés. [CXM-49618]
- Lorsque les diagnostics sont activés, le fichier de commandes affiche les commandes **Set-CasMailbox** qui ne contiennent pas de tirets avant chaque nom de propriété. Ce problème se produit uniquement lors du formatage du fichier de diagnostics et non de la commande elle-même vers Exchange. L'absence de tiret empêche un utilisateur de couper la commande et de la coller directement dans une invite PowerShell de test ou de validation. Les tirets ont été ajoutés. [CXM-52520]
- Si une identité de boîte aux lettres est au format "nom, prénom", Exchange ajoute une barre oblique inverse avant la virgule lors du renvoi de données à partir d'une requête. Cette barre oblique inverse doit être supprimée lorsque XenMobile Mail Manager utilise l'identité pour demander davantage de données. [CXM-52635]

Limitation connue

> **Remarque :**
>
> La limitation suivante est résolue dans la version 10.1.6.

XenMobile Mail Manager a une limitation connue qui peut entraîner l'échec des commandes Exchange. Pour appliquer des modifications de stratégie à Exchange, une commande **Set_CASMailbox** est émise par XenMobile Mail Manager. Cette commande peut utiliser deux listes d'appareils : une pour autoriser et une pour bloquer. La commande est appliquée aux appareils associés à une boîte aux lettres.

Ces listes sont limitées à 256 caractères chacune par l'API Microsoft. Si l'une de ces listes dépasse la limite, la commande échoue dans son intégralité, empêchant toutes les stratégies pour ces appareils de la boîte aux lettres d'être définies. L'erreur signalée, qui apparaîtra dans les journaux XenMobile Mail Manager, ressemble à ceci. L'exemple représente la liste bloquée.

"Message:'Cannot bind parameter 'ActiveSyncBlockedDeviceIDs' to the target. Exception setting "ActiveSyncBlockedDeviceIDs": "The length of the property is too long. The maximum length is 256 and the length of the value provided is …"

Les longueurs d'ID d'appareil peuvent varier, mais un bon principe à suivre est qu'environ 10 appareils Autorisés ou Bloqués simultanément peuvent dépasser la limite. Bien qu'il soit rare que de nombreux appareils soient associés à une boîte aux lettres spécifique, c'est un scénario possible. Tant que Xen-

Mobile Mail Manager n'est pas amélioré pour gérer un tel scénario, nous vous recommandons de limiter le nombre d'appareils associés à un utilisateur et à une boîte aux lettres à 10 ou moins. [CXM-52633]

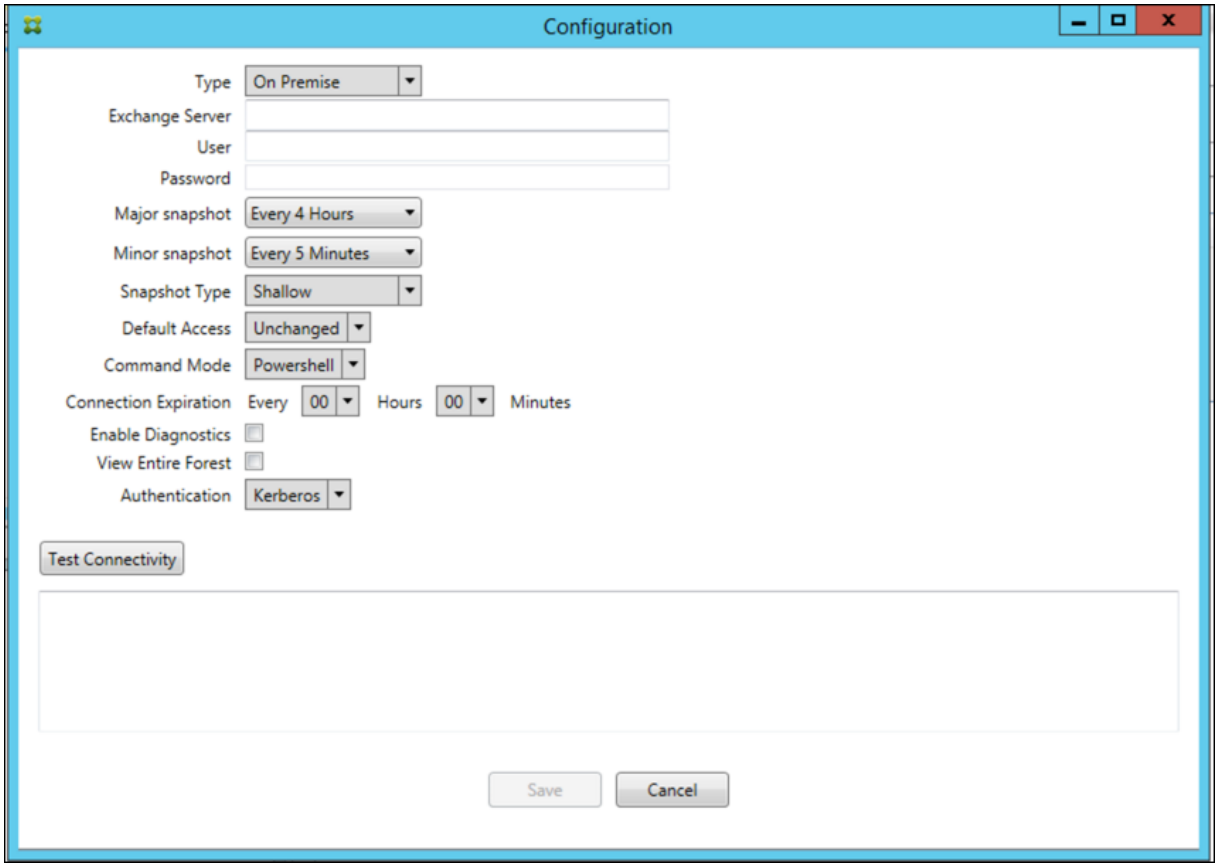
Nouveautés dans la version 10.1.4

XenMobile Mail Manager version 10.1.4 contient les problèmes résolus suivants :

- en raison de ses risques pour la sécurité, TLS 1.0 est abandonné par le PCI Council. La prise en charge de TLS 1.1 et 1.2 est ajoutée à XenMobile Mail Manager. [CXM-38573, CXM-32560]
- XenMobile Mail Manager inclut un nouveau fichier de diagnostic. Lorsque l'option **Enable Diagnostics** est sélectionnée dans la spécification Exchange, un nouveau fichier d'historique des instantanés est généré. À chaque tentative d'instantané, une ligne est ajoutée au fichier avec les résultats de l'instantané. [CXM-49631]
- Dans le fichier de diagnostic Commands, la liste des appareils autorisés ou bloqués n'apparaît pas pour la commande **Set-CASMailbox**. Au lieu de cela, le nom de classe interne était affiché dans le fichier pour les arguments associés. XenMobile Mail Manager affiche désormais la liste des appareils sous forme de liste délimitée par des virgules. [CXM-50693]
- Lorsqu'une tentative d'acquisition d'une connexion à Exchange échoue en raison d'une spécification incorrecte : Le message d'erreur est remplacé par un message incorrect : "All connections in use". Des messages plus descriptifs apparaissent maintenant, tels que "All connections are inoperable", "Connection pool is empty", "All connections are throttled" et "No available connections". [CXM-50783]
- Dans certains cas, les commandes Autoriser / Bloquer / Effacer sont mises en file d'attente plusieurs fois dans le cache interne de XenMobile Mail Manager. Ce problème provoque un retard dans la commande envoyée à Exchange. XenMobile Mail Manager ne met en file d'attente qu'une seule instance de chaque commande. [CXM-51524]

Nouveautés dans la version 10.1.3

- **Prise en charge de Google Analytics :** nous souhaitons savoir comment vous utilisez XenMobile Mail Manager afin de pouvoir nous concentrer sur l'amélioration du produit.
- **Paramètre d'activation des diagnostics :** une case à cocher **Enable Diagnostic** s'affiche dans la console Configure de la boîte de dialogue **Configuration**.



Problèmes résolus dans la version 10.1.3

- Dans la fenêtre **Snapshot History**, les infobulles qui montrent l'état actuel de l'instantané ne reflètent pas l'état actuel. [CXM-5570]
  Parfois, XenMobile Mail Manager ne peut pas écrire dans le fichier de diagnostic Commands. Lorsque cela se produit, l'historique des commandes n'est pas consigné dans son intégralité. [CXM-49217]
- Lorsqu'une erreur se produit avec une connexion, la connexion peut ne pas être marquée comme "erronée" (errored). Par conséquent, une commande ultérieure peut tenter d'utiliser la connexion et provoquer une autre erreur. [CXM-49495]
- Lors d'une limitation en provenance du serveur Exchange, une exception peut être envoyée dans la routine Check Health. Par conséquent, les connexions ayant rencontré une erreur ou ayant expiré risquent de ne pas être purgées. En outre, XenMobile Mail Manager peut ne pas créer de connexions jusqu'à ce que le délai de limitation expire. [CXM-49794].
- Lorsque le nombre maximal de sessions pour Exchange est dépassé, XenMobile Mail Manager signale l'erreur "Device Capture Failed", qui n'est pas un message exact. Au lieu de cela, le message doit indiquer que les deux sessions que XenMobile Mail Manager utilise normalement pour la communication Exchange sont en cours d'utilisation. [CXM-49994]

Nouveautés dans la version 10.1.2

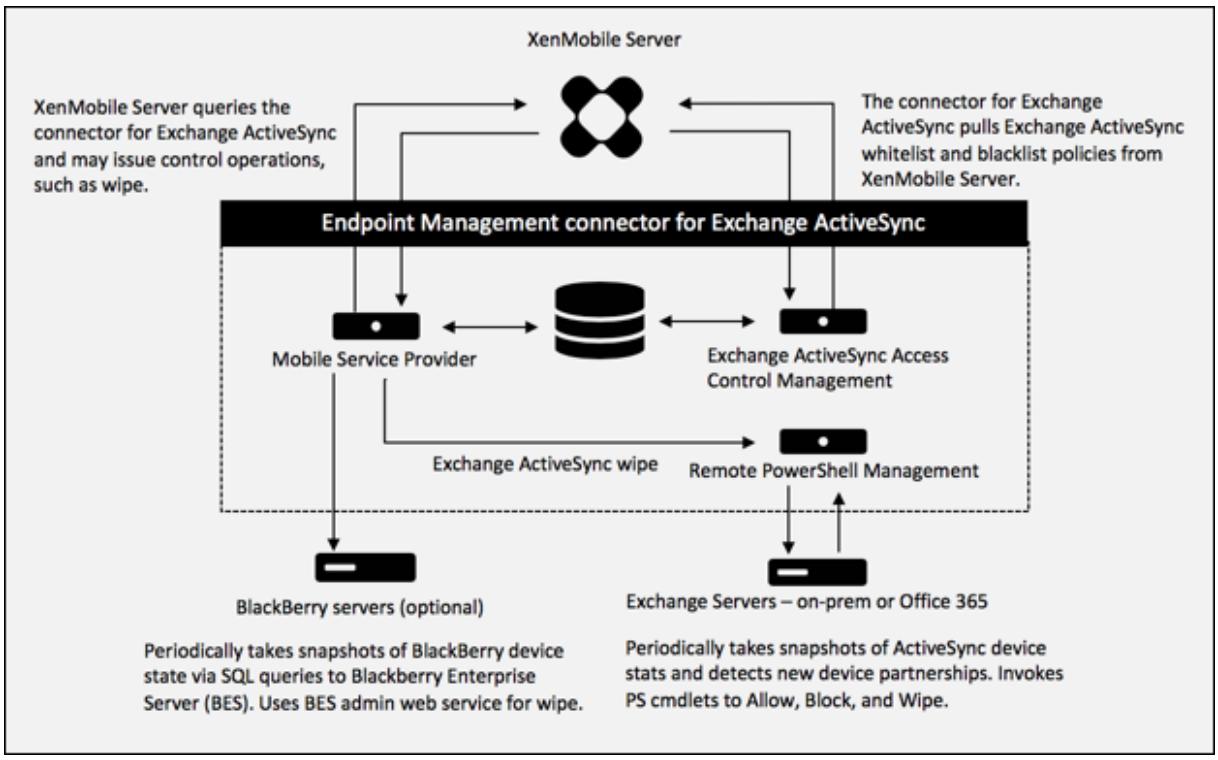
- **Connexion améliorée à Exchange :** XenMobile Mail Manager utilise des sessions PowerShell pour communiquer avec Exchange. Une session PowerShell, en particulier avec Office 365, peut devenir instable après un certain temps, empêchant les commandes suivantes de réussir. XenMobile Mail Manager peut maintenant définir une période d'expiration pour les connexions. Lorsque la connexion atteint son heure d'expiration, XenMobile Mail Manager arrête la session PowerShell et crée une session. Ce faisant, la session PowerShell est moins susceptible de devenir instable, ce qui réduit considérablement les risques d'échec d'un instantané.
- **Flux de travail instantané amélioré :** les instantanés importants représentent une opération longue et fastidieuse. Si une erreur se produit pendant un instantané, XenMobile Mail Manager tente désormais à plusieurs reprises (jusqu'à trois) d'effectuer une capture instantanée. Les tentatives suivantes ne commencent pas depuis le début. XenMobile Mail Manager continue là où il s'est arrêté. Ce changement améliore le taux de réussite des instantanés en général en permettant aux erreurs transitoires de passer pendant qu'un instantané est encore en cours.
- **Amélioration des diagnostics :** le dépannage des opérations de capture d'instantané est maintenant plus facile avec trois nouveaux fichiers de diagnostic pouvant être générés au cours d'un instantané. Ces fichiers permettent d'identifier les problèmes de commande PowerShell, les boîtes aux lettres avec informations manquantes et les appareils qui ne peuvent pas être associés à une boîte aux lettres. Un administrateur peut utiliser ces fichiers pour identifier les données qui peuvent ne pas être correctes dans Exchange.
- **Amélioration de l'utilisation de la mémoire :** XenMobile Mail Manager utilise désormais plus efficacement la mémoire. Les administrateurs peuvent planifier le redémarrage automatique de XenMobile Mail Manager pour fournir une version nettoyée du système.
- **Microsoft .NET Framework 4.6 :** la version requise de Microsoft .NET Framework est maintenant la version 4.6.

Problèmes résolus

- Erreur d'invite d'informations d'identification : l'instabilité de session Office 365 a souvent causé cette erreur. L'amélioration de la connexion à Exchange résout le problème. (XMHELP-293, XMHELP-311, XMHELP-801)
- La boîte aux lettres et le nombre d'appareils sont inexacts : l'algorithme d'association de boîte aux lettres de XenMobile Mail Manager a été amélioré. La fonction d'amélioration des diagnostics facilite l'identification des boîtes aux lettres et des appareils que XenMobile Mail Manager considère comme n'étant pas sous sa responsabilité. (XMHELP-623)
- Les commandes Autoriser / Bloquer / Effacer ne sont pas reconnues : correction d'un bogue avec lequel les commandes Autoriser / Bloquer / Effacer de XenMobile Mail Manager ne sont pas reconnues. (XMHELP-489)
- Gestion de la mémoire : meilleure gestion de la mémoire. (XMHELP-419)

Architecture

La figure suivante présente les principaux composants de Endpoint Management Connector pour Exchange ActiveSync. Pour un diagramme d'architecture de référence détaillé, voir Architecture.



Les trois composants principaux sont :

- **Exchange ActiveSync Access Control Management :** communique avec XenMobile pour récupérer une stratégie Exchange ActiveSync depuis XenMobile, puis fusionne cette stratégie avec toutes les stratégies définies localement pour déterminer les appareils Exchange ActiveSync ayant le droit ou non d'accéder à Exchange. Les stratégies locales permettent d'étendre les règles de stratégie pour autoriser le contrôle d'accès par un groupe Active Directory, utilisateur, type d'appareil ou agent utilisateur de l'appareil (généralement la version de la plate-forme mobile).
- **Remote PowerShell Management :** ce composant est responsable de la planification et de l'appel des commandes PowerShell à distance afin d'appliquer la stratégie compilée par la gestion du contrôle d'accès à Exchange ActiveSync. Il crée régulièrement un instantané de la base de données Exchange ActiveSync pour détecter de nouveaux périphériques ou des périphériques modifiés Exchange ActiveSync.
- **Fournisseur de services mobiles :** fournit une interface de service Web permettant à XenMobile d'interroger Exchange ActiveSync, d'interroger des appareils Blackberry, et d'émettre des opérations de contrôle, telles que l'effacement des appareils ActiveSync et Blackberry.

Configuration système requise et conditions préalables

La configuration système minimale suivante est nécessaire pour utiliser Endpoint Management Connector pour Exchange ActiveSync :

- Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2008 R2 Service Pack 1. Doit être un serveur en anglais. La prise en charge de Windows Server 2008 R2 Service Pack 1 prend fin le 14 janvier 2020.
- Microsoft SQL Server 2016 Service Pack 2 ou SQL Server 2014 Service Pack 3.
- Microsoft .NET Framework 4.6.
- Blackberry Enterprise Service, version 5 (facultatif).

Versions minimales prises en charge de Microsoft Exchange Server :

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 Service Pack 3 (la prise en charge prend fin le 14 janvier 2020)

Conditions préalables

- Windows Management Framework doit être installé.
  - PowerShell V5, V4 et V3
- La stratégie d'exécution de PowerShell doit être paramétrée sur RemoteSigned via Set-ExecutionPolicy RemoteSigned.
- Le port TCP 80 doit être ouvert entre l'ordinateur exécutant Endpoint Management Connector pour Exchange ActiveSync et le serveur Exchange distant.
- **Clients de messagerie d'appareil :** les clients de messagerie ne renvoient pas tous le même ID ActiveSync pour un appareil. Étant donné qu'Endpoint Management Connector pour Exchange ActiveSync s'attend à un ID ActiveSync unique pour chaque appareil, seuls les clients de messagerie qui génèrent toujours le même ID ActiveSync unique pour chaque appareil sont pris en charge. Ces clients de messagerie ont été testés par Citrix et aucune erreur n'a été détectée :
  - Client de messagerie natif Samsung
  - Client de messagerie natif iOS
- **Exchange :** la configuration requise pour l'ordinateur local exécutant Exchange est la suivante :

  Les informations d'identification spécifiées dans l'interface utilisateur de la console Exchange Configuration doivent être en mesure de se connecter au serveur Exchange Server et bénéficier d'un accès complet pour exécuter les applets de commande PowerShell spécifiques à Exchange suivantes :

- **Pour Exchange Server 2010 SP2 :**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- **Pour Exchange Server 2013 et Exchange Server 2016 :**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- Si Endpoint Management Connector pour Exchange ActiveSync est configuré pour afficher l'ensemble de la forêt, l'autorisation doit avoir été accordée pour exécuter : **Set-AdServerSettings -ViewEntireForest $true**
- Les informations d'identification fournies doivent avoir été autorisées à se connecter au serveur Exchange Server via le Shell distant. Par défaut, l'utilisateur qui a installé Exchange possède ce droit.
- Afin d'établir une connexion à distance et exécuter les commandes distantes, les informations d'identification doivent correspondre à un utilisateur qui est un administrateur sur l'appareil distant. Vous pouvez utiliser Set-PSSessionConfiguration pour éliminer les exigences administratives, mais cette commande n'entre pas dans le cadre de ce document. Pour plus d'informations, consultez l'article Microsoft À propos des configurations de session.
- Le serveur Exchange doit être configuré pour prendre en charge les requêtes PowerShell distantes via HTTP. En règle générale, un administrateur exécutant la commande PowerShell suivante sur le serveur Exchange est la seule exigence requise : WinRM QuickConfig.
- Exchange possède de nombreuses stratégies de limitation. L'une de ces stratégies contrôle combien de connexions PowerShell simultanées sont autorisées par utilisateur. Par défaut, le nombre de connexions simultanées autorisées pour un utilisateur est de 18 sur Exchange 2010. Lorsque la limite de connexion est atteinte, Endpoint Management Con-

nector pour Exchange ActiveSync ne peut pas se connecter au serveur Exchange. Il existe plusieurs méthodes pour changer le nombre maximal de connexions simultanées autorisées via PowerShell qui ne sont pas couvertes dans cette documentation. Si vous êtes intéressé, renseignez-vous au sujet des stratégies de limitation d'Exchange relatives à la gestion à distance avec PowerShell.

Configuration requise pour Office 365 Exchange

- **Autorisations :** les informations d'identification spécifiées dans l'interface utilisateur de la console Exchange Configuration doivent être en mesure de se connecter à Office 365 et bénéficier d'un accès complet pour exécuter les applets de commande PowerShell spécifiques à Exchange suivantes :
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- **Privilèges :** les informations d'identification fournies doit avoir été autorisées à se connecter au serveur Office 365 via le Shell distant. Par défaut, l'administrateur d'Office 365 Online possède les privilèges requis.
- **Stratégies de limitation :** Exchange possède de nombreuses stratégies de limitation. L'une de ces stratégies contrôle combien de connexions PowerShell simultanées sont autorisées par utilisateur. Par défaut, le nombre de connexions simultanées autorisées pour un utilisateur est de trois sur Office 365. Lorsque la limite de connexion est atteinte, Endpoint Management Connector pour Exchange ActiveSync ne peut pas se connecter au serveur Exchange. Il existe plusieurs méthodes pour changer le nombre maximal de connexions simultanées autorisées via PowerShell qui ne sont pas couvertes dans cette documentation. Si vous êtes intéressé, renseignez-vous au sujet des stratégies de limitation d'Exchange relatives à la gestion à distance avec PowerShell.

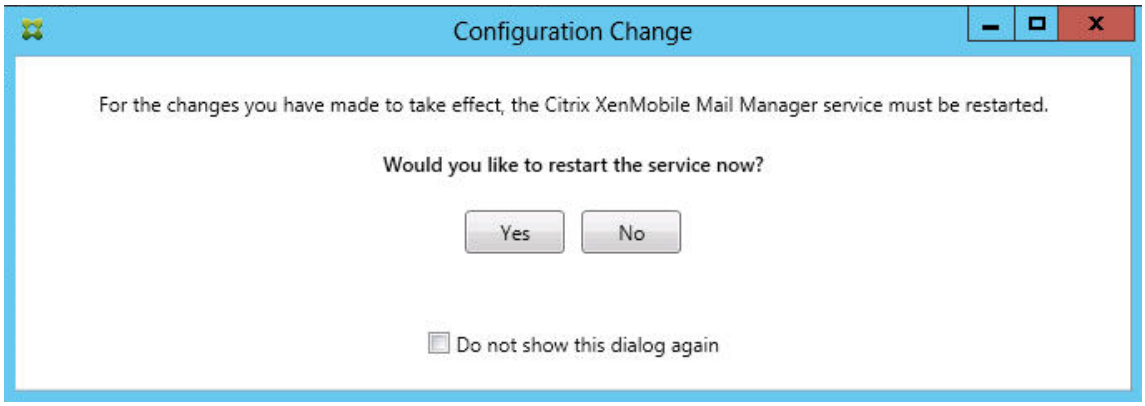
Installer et configurer

1. Cliquez sur le fichier XmmSetup.msi puis suivez les instructions de l'assistant pour installer Endpoint Management Connector pour Exchange ActiveSync.
2. Laissez l'option **Launch the Configure utility** sélectionnée dans le dernier écran de l'assistant.

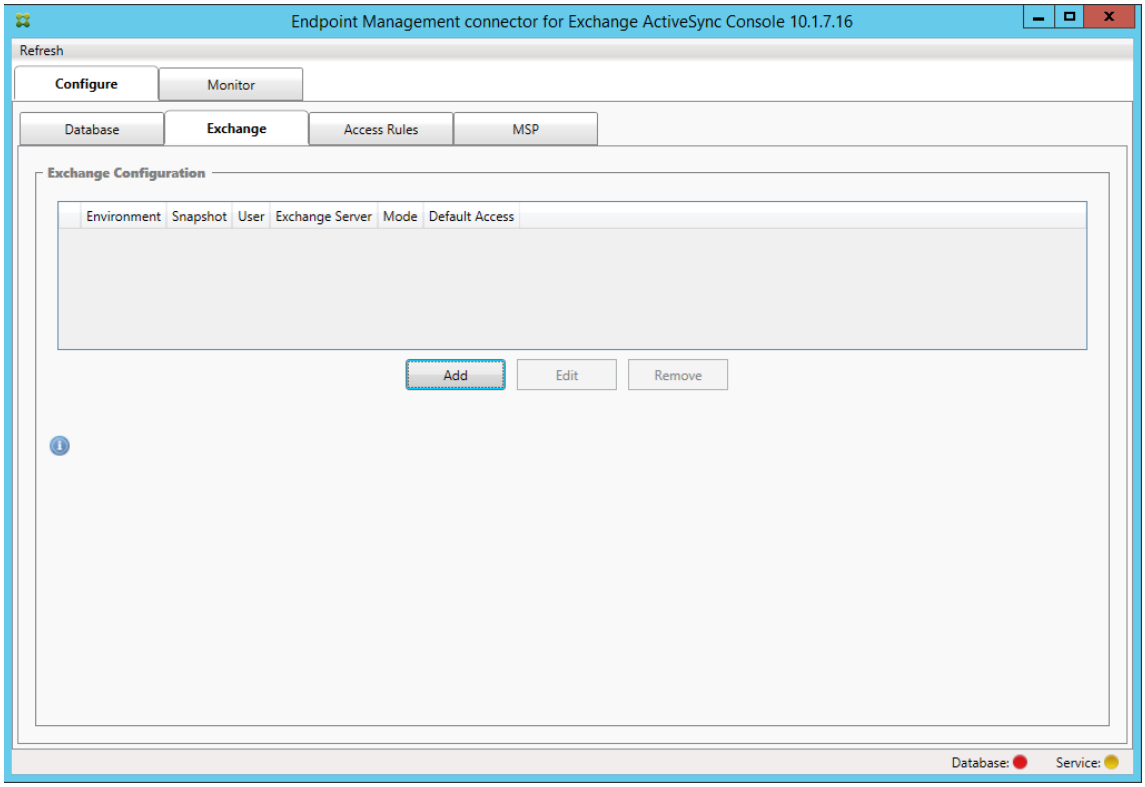
Vous pouvez également ouvrir Endpoint Management Connector pour Exchange ActiveSync à partir du menu **Démarrer**.

3. Configurez les propriétés de base de données suivantes :
   - Sélectionnez l'onglet **Configure > Database**.
   - Entrez le nom du serveur SQL (localhost par défaut).
   - Conservez la base de données par défaut **CitrixXmm**.
4. Sélectionnez l'un des modes d'authentification suivants utilisés pour SQL :
   - **SQL :** entrez le nom d'utilisateur et le mot de passe d'un utilisateur SQL valide.
   - **Windows Integrated :** si vous sélectionnez cette option, les informations d'identification d'ouverture de session du service Endpoint Management Connector pour Exchange ActiveSync doivent être remplacées par un compte Windows disposant des autorisations nécessaires pour accéder au serveur SQL. Pour ce faire, ouvrez le **Panneau de configuration > Outils d'administration > Services**, cliquez avec le bouton droit de la souris sur l'entrée du service Endpoint Management Connector pour Exchange ActiveSync, puis sélectionnez l'onglet **Log On** (Connexion).

   Si Windows Integrated est également choisi pour la connexion à la base de données BlackBerry, le compte Windows spécifié ici doit également pouvoir accéder à la base de données BlackBerry.
5. Cliquez sur **Test Connectivity** pour vérifier qu'une connexion peut être établie avec le serveur SQL, puis cliquez sur **Save**.
6. Un message vous invite à redémarrer le service. Cliquez sur **Yes**.



7. Configurez un ou plusieurs serveurs Exchange :
   - Si vous ne gérez qu'un seul environnement Exchange, spécifiez un seul serveur. Si vous gérez plusieurs environnements Exchange, spécifiez un seul serveur Exchange pour chaque environnement Exchange.
   - Cliquez sur l'onglet **Configure > Exchange**, puis cliquez sur **Add**.

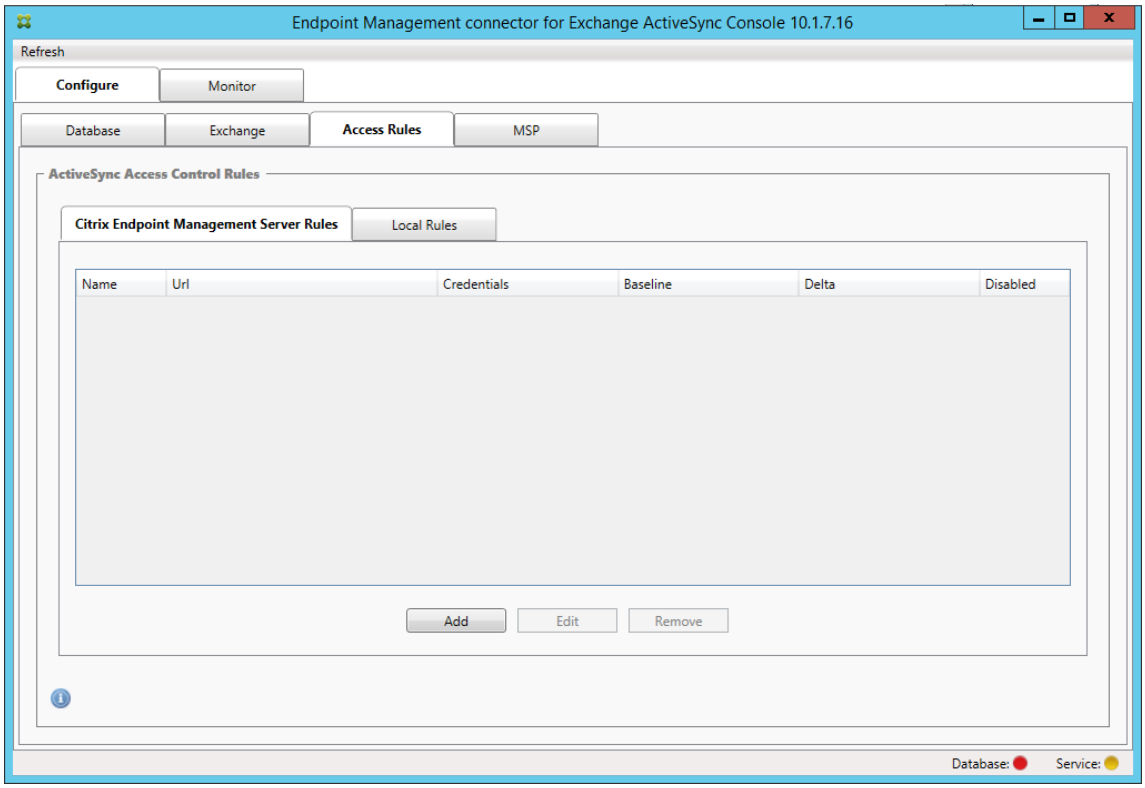


8. Sélectionnez le type d'environnement de serveur Exchange, soit **On Premise** soit **Office 365**.

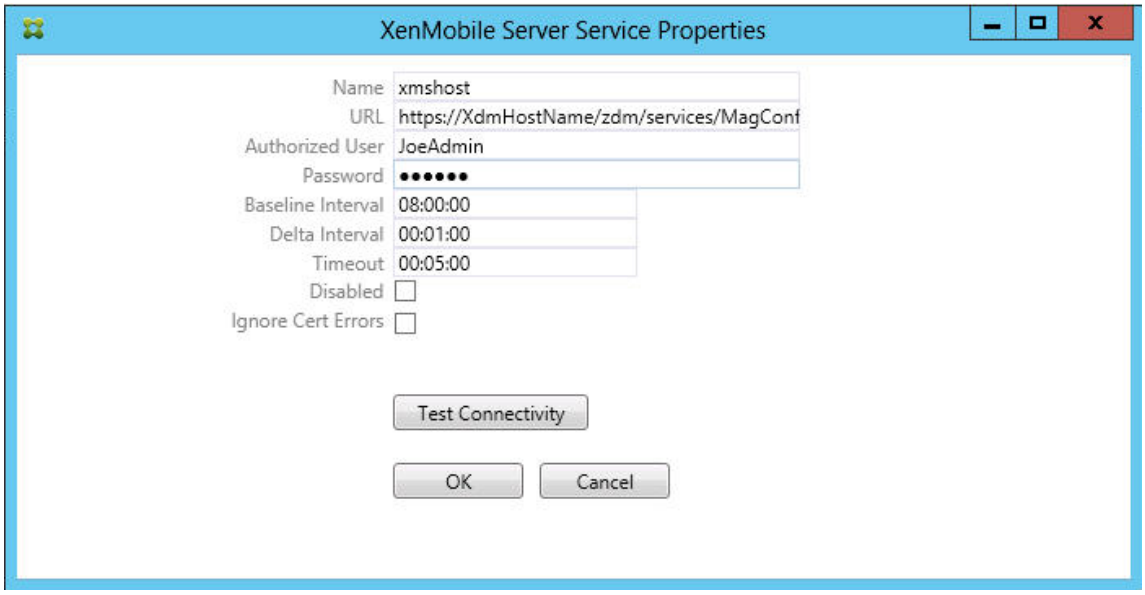
   - Si vous sélectionnez **On Premise**, entrez le nom du serveur Exchange qui sera utilisé pour les commandes PowerShell à distance.
   - Entrez le **nom d'utilisateur** d'une identité Windows disposant des droits appropriés sur le serveur Exchange comme indiqué dans la section Configuration requise et entrez le **mot de passe** de l'utilisateur.
   - Sélectionnez la planification d'exécution de captures d'instantanés principaux. Un instantané principal détecte tous les partenariats Exchange ActiveSync.
   - Sélectionnez la planification d'exécution des captures d'instantanés secondaires. Un instantané secondaire détecte les partenariats Exchange ActiveSync nouvellement créés.
   - Sélectionnez le type d'instantané : **Deep** ou **Shallow**. Les instantanés superficiels sont généralement plus rapides et suffisent pour exécuter toutes les fonctions de contrôle d'accès Exchange ActiveSync d'Endpoint Management Connector pour Exchange ActiveSync. Les instantanés complets peuvent prendre plus de temps et sont nécessaires uniquement si Mobile Service Provider est activé pour ActiveSync. Cette option permet à XenMobile d'interroger les appareils non gérés.
   - Sélectionnez les paramètres d'accès par défaut : **Allow**, **Block** ou **Unchanged**. Ce paramètre contrôle la façon dont sont traités tous les appareils autres que ceux identifiés explicitement par des règles locales ou XenMobile. Si vous sélectionnez **Allow**, l'accès à ActiveSync à tous ces appareils est autorisé. Si vous sélectionnez **Block**, l'accès est refusé. Si vous sélectionnez **Unchanged**, aucune modification n'est effectuée.

- Sélectionnez le mode de commande ActiveSync : **PowerShell** ou **Simulation**.
- En mode **PowerShell**, Endpoint Management Connector pour Exchange ActiveSync émet des commandes PowerShell afin d'appliquer le contrôle d'accès souhaité. En mode Simulation, Endpoint Management Connector pour Exchange ActiveSync n'émet pas de commandes PowerShell, mais consigne la commande prévue et les résultats escomptés dans la base de données. En mode Simulation, l'utilisateur peut alors utiliser l'onglet **Monitor** pour voir ce qui serait arrivé si le mode PowerShell était activé.
- Dans **Connection Expiration**, définissez les heures et les minutes pour la durée de vie d'une connexion. Lorsqu'une connexion atteint la durée spécifiée, elle est marquée comme expirée et n'est pas réutilisée. Lorsque la connexion expirée n'est plus utilisée, Endpoint Management Connector pour Exchange ActiveSync l'arrête. Lorsqu'une connexion est de nouveau nécessaire, une nouvelle connexion est initialisée si aucune n'est disponible. Si aucune valeur n'est spécifiée, la valeur par défaut de 30 minutes est utilisée.
- Sélectionnez **View Entire Forest** pour configurer Endpoint Management Connector pour Exchange ActiveSync de manière à ce qu'il affiche la forêt Active Directory entière dans l'environnement Exchange.
- Sélectionnez le protocole d'authentification : **Kerberos** ou **Basic**. Endpoint Management Connector pour Exchange ActiveSync prend en charge l'authentification de base pour les déploiements locaux. Cela permet d'utiliser Endpoint Management Connector pour Exchange ActiveSync lorsque le serveur Endpoint Management Connector pour Exchange ActiveSync n'est pas membre du domaine dans lequel réside le serveur Exchange Server.
- Cliquez sur **Test Connectivity** pour vérifier qu'une connexion peut être établie avec le serveur Exchange, puis cliquez sur **Save**.
- Un message vous invite à redémarrer le service. Cliquez sur **Yes**.

9. Configurer les règles d'accès : sélectionnez l'onglet **Configure > Access Rules** et cliquez sur l'onglet **XMS Rules**, puis sur **Add**.



10. Dans la page **XenMobile server Service Properties**, modifiez la chaîne d'URL pour qu'elle pointe vers le serveur XenMobile. Par exemple, si le nom de l'instance est **zdm**, entrez `https://<XdmHostName>/zdm/services/MagConfigService`. Dans l'exemple, remplacez **XdmHostName** par l'adresse IP ou DNS du serveur XenMobile Server.

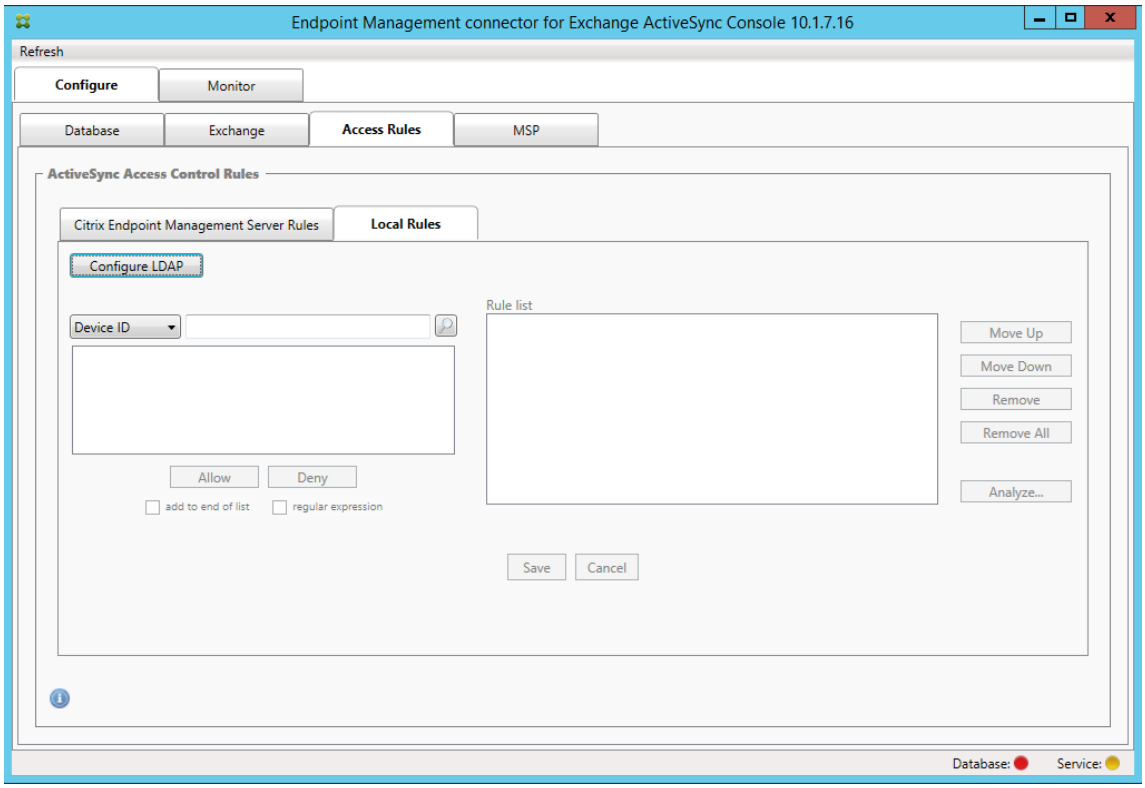


- Entrez un utilisateur autorisé sur le serveur.
- Entrez le mot de passe de l'utilisateur.
- Conservez les valeurs par défaut **Baseline Interval**, **Delta Interval**, et **Timeout** values.

- Cliquez sur **Test Connectivity** pour tester la connexion au serveur, puis cliquez sur **OK**.

Si la case **Disabled** est cochée, XenMobile Mail Service ne collecte pas de stratégie depuis XenMobile.

11. Cliquez sur l'onglet **Local Rules**.



- Vous pouvez ajouter des règles locales basées sur ActiveSync Device ID, Device Type, AD Group, User ou UserAgent. Sélectionnez le type approprié dans la liste.
- Tapez le texte ou les fragments de texte dans la zone de texte. Si vous le souhaitez, cliquez sur le bouton de requête pour afficher les entités qui correspondent au fragment.

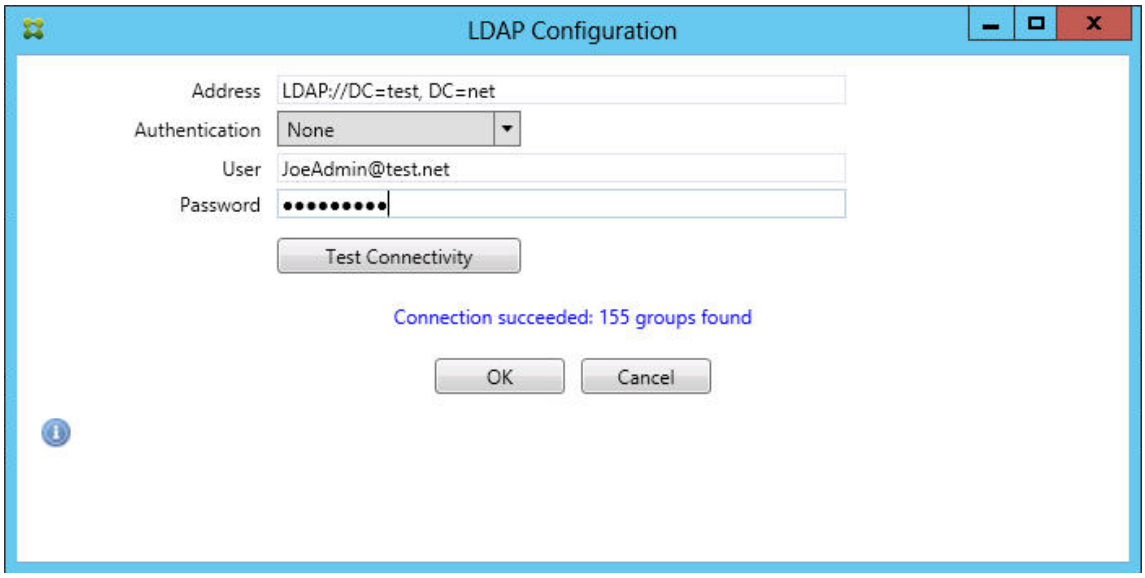
Pour tous les types autres que Group, le système s'appuie sur les appareils qui ont été localisés dans un instantané. Par conséquent, si vous démarrez et que vous n'avez pas réalisé d'instantané, aucune entité n'est disponible.

- Sélectionnez une valeur de texte, puis cliquez sur **Allow** ou **Deny** pour l'ajouter à la **Rule List** sur le côté droit. Vous pouvez modifier l'ordre des règles ou les supprimer en utilisant les boutons situés à droite du panneau de **Rule List**. L'ordre est important car pour un utilisateur et un appareil donné, les règles sont évaluées dans l'ordre indiqué. Dans le cas d'une correspondance à une règle de niveau élevé (près du haut de la liste), les règles se trouvant plus bas dans la liste n'ont pas d'effet. Par exemple, si vous possédez une règle qui autorise tous les iPad, et une règle suivante bloquant l'utilisateur « Matt », l'iPad de Matt sera autorisé car la règle « iPad » possède une priorité plus élevée que la règle « Matt

».

- Pour effectuer une analyse des règles dans la liste de règles afin de rechercher des remplacements, des conflits ou des constructions supplémentaires potentielles, cliquez sur **Analyze**, puis sur **Save**.

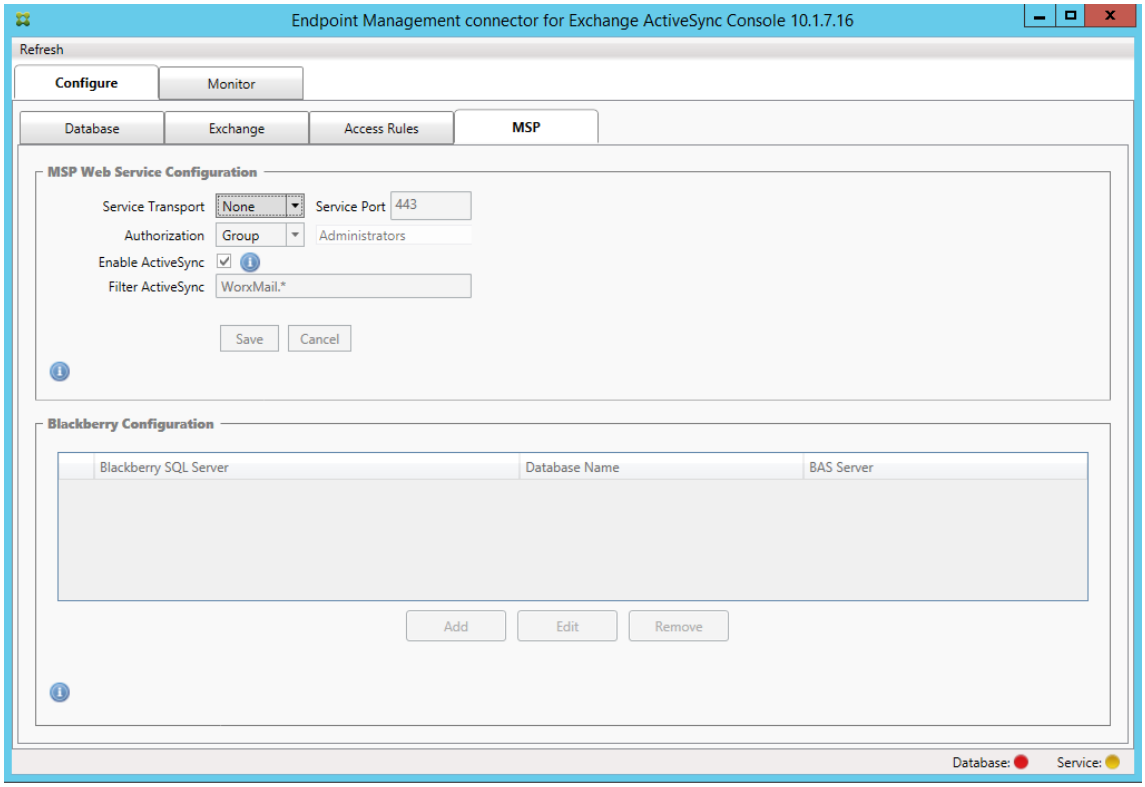
12. Si vous souhaitez créer des règles locales qui fonctionnent sur des groupes Active Directory, cliquez sur **Configure LDAP**, puis configurez les propriétés de connexion LDAP.



13. Configurez le Mobile Service Provider.

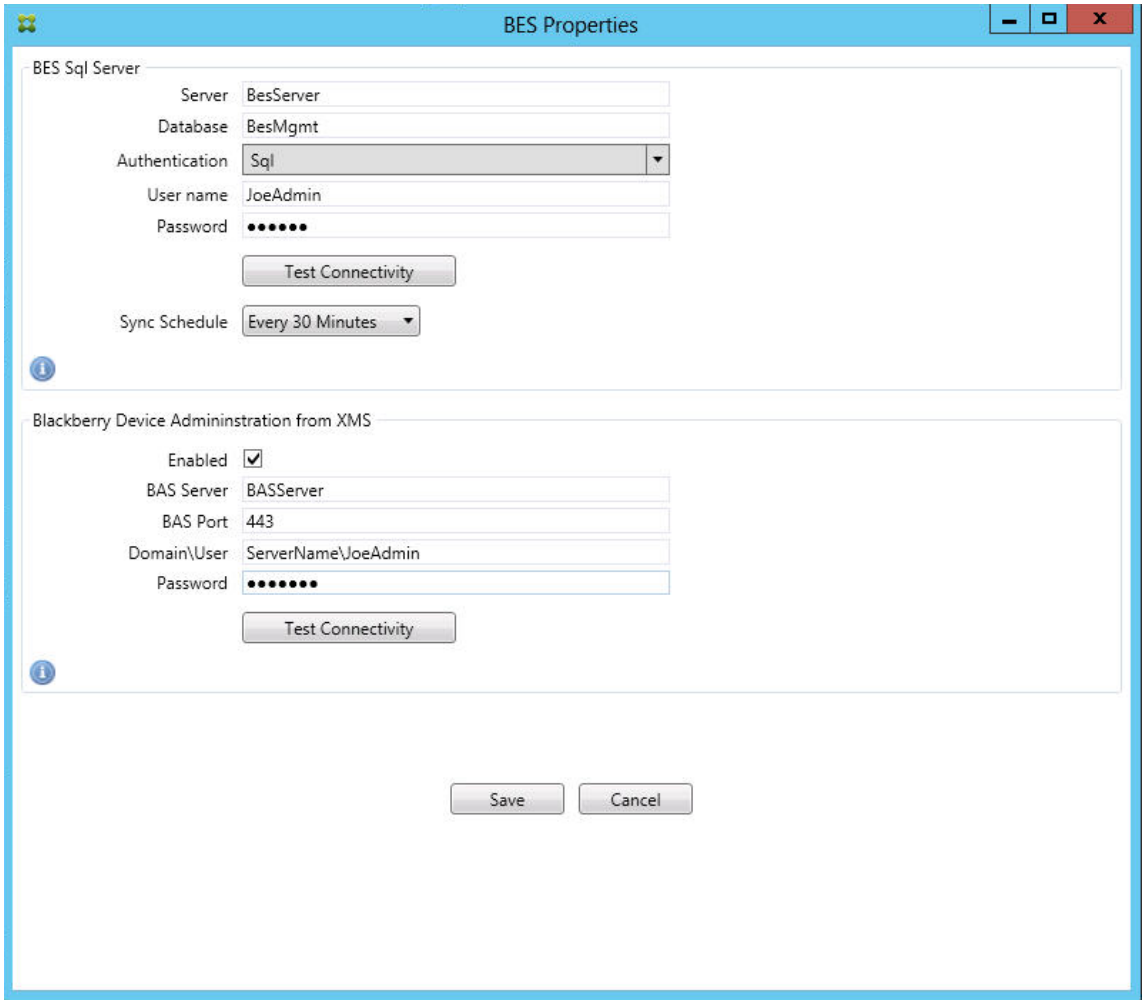
    Le fournisseur de services mobiles est facultatif. Ce paramètre est uniquement nécessaire si XenMobile est également configuré pour utiliser l'interface Mobile Service Provider pour interroger les appareils non gérés.

    - Cliquez sur l'onglet **Configure > MSP**.



- Définissez le type de transport de service sur **HTTP** ou **HTTPS** pour le service fournisseur de services mobiles.
- Définissez le **port de service** (généralement 80 ou 443) pour le service Fournisseur de services mobiles. Si vous utilisez le port 443, le port requiert un certificat SSL lié dans IIS.
- Définissez le **groupe** ou l'**utilisateur d'autorisation**. Cela définit l'utilisateur ou l'ensemble des utilisateurs qui peuvent se connecter au service fournisseur de services mobiles XenMobile.
- Paramétrer si les requêtes ActiveSync sont actives ou non. Si les requêtes ActiveSync sont activées pour le serveur XenMobile Server, le type Snapshot pour un ou plusieurs serveurs Exchange doit être défini sur **Deep**. Ce paramètre peut entraîner des coûts de performances significatifs liés à la prise d'instantanés.
- Par défaut, les appareils ActiveSync correspondants à l'expression régulière WorxMail.*ne seront pas envoyés à XenMobile. Pour changer ce comportement, vous pouvez modifier le champ **Filter ActiveSync** si nécessaire.
  S'il est laissé vide, cela signifie que tous les appareils sont transférés vers XenMobile.
- Cliquez sur **Enregistrer**.

14. Vous pouvez également configurer une ou plusieurs instances de BlackBerry Enterprise Server (BES) : cliquez sur **Add**, puis entrez le nom du serveur BES SQL Server.



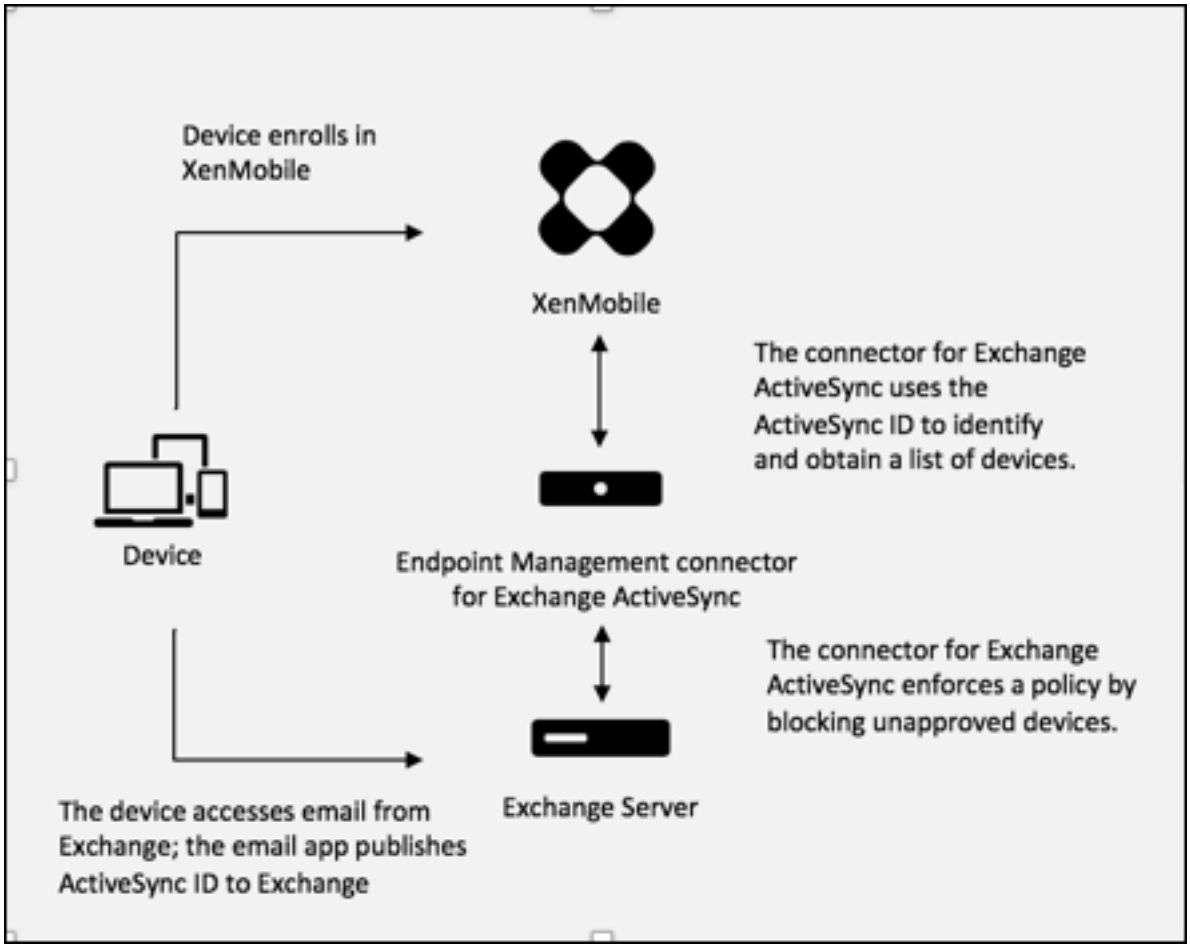
- Tapez le nom de la base de données de gestion BES.
- Sélectionnez le mode **Authentication**. Si vous sélectionnez l'authentification intégrée Windows, le compte utilisateur du service Endpoint Management Connector pour Exchange ActiveSync est le compte utilisé pour se connecter au serveur BES SQL. Si vous choisissez également Windows Integrated pour la connexion à la base de données d'Endpoint Management Connector pour Exchange ActiveSync, le compte Windows spécifié doit également disposer d'un droit d'accès à la base de données d'Endpoint Management Connector pour Exchange ActiveSync.
- Si vous sélectionnez **SQL authentication**, entrez le nom d'utilisateur et le mot de passe.
- Définissez **Sync Schedule**. Il s'agit du calendrier utilisé pour se connecter au serveur BES SQL et rechercher toute mise à jour d'appareil.
- Cliquez sur **Test Connectivity** pour vérifier la connectivité avec le serveur SQL. Si Windows Integrated est sélectionné, ce test utilise l'utilisateur actuellement connecté et non l'utilisateur du service Endpoint Management Connector pour Exchange ActiveSync et par conséquent ne teste pas correctement l'authentification SQL.
- Pour prendre en charge l'effacement à distance (Wipe) et la réinitialisation du mot de passe

(ResetPassword) d'appareils BlackBerry depuis XenMobile, sélectionnez la case **Enabled**.
- Entrez le nom de domaine complet BES.
- Entrez le port BES utilisé pour le service Web d'administration.
- Entrez le nom d'utilisateur complet et le mot de passe requis par le service BES.
- Cliquez sur **Test Connectivity** pour tester la connexion au serveur BES.
- Cliquez sur **Enregistrer**.

Appliquer les stratégies de messagerie avec des ID ActiveSync

Votre stratégie de messagerie d'entreprise peut refuser l'accès à la messagerie d'entreprise à certains appareils. Pour vous conformer à cette stratégie, vous devez vous assurer que les employés ne peuvent pas accéder à la messagerie d'entreprise à partir de tels appareils. Endpoint Management Connector pour Exchange ActiveSync et XenMobile fonctionnent ensemble pour appliquer une telle stratégie de messagerie. XenMobile définit la stratégie d'accès à la messagerie d'entreprise, et lorsqu'un appareil non approuvé s'inscrit auprès de XenMobile, Endpoint Management Connector pour Exchange ActiveSync applique la stratégie.

Le client de messagerie sur un appareil se fait connaître d'Exchange Server (ou Office 365) à l'aide de l'D d'appareil, également appelé ID ActiveSync, qui est utilisé pour identifier l'appareil. Secure Hub obtient un identificateur similaire et envoie l'identificateur à XenMobile lorsque l'appareil est inscrit. En comparant les ID des deux appareils, Endpoint Management Connector pour Exchange ActiveSync peut déterminer si un appareil spécifique est autorisé à accéder à la messagerie d'entreprise. La figure suivante illustre ce concept :



Si XenMobile envoie à Endpoint Management Connector pour Exchange ActiveSync un ID ActiveSync différent de l'ID publié auprès d'Exchange par l'appareil, Endpoint Management Connector pour Exchange ActiveSync ne peut pas indiquer à Exchange l'action à exécuter avec l'appareil.

La correspondance des ID ActiveSync fonctionne de manière fiable sur la plupart des plates-formes. Cependant, Citrix a constaté que sur certaines implémentations Android, l'ID ActiveSync de l'appareil est différent de l'ID publié par le client de messagerie auprès d'Exchange. Pour pallier ce problème, vous pouvez effectuer les tâches suivantes :

- Sur la plate-forme Samsung SAFE, distribuez la configuration ActiveSync de l'appareil depuis XenMobile.

Pour garantir que votre stratégie d'accès à la messagerie d'entreprise est appliquée correctement, vous pouvez adopter une approche de sécurité défensive et configurer Endpoint Management Connector pour Exchange ActiveSync de manière à bloquer les e-mails en définissant la stratégie statique sur Deny par défaut. Cela signifie que si un employé configure un client de messagerie sur un appareil Android, et que la détection de l'ID ActiveSync ne fonctionne pas correctement, l'employé se voit refuser l'accès à la messagerie d'entreprise.

Règles de contrôle d'accès

Endpoint Management Connector pour Exchange ActiveSync propose une approche basée sur des règles permettant de configurer dynamiquement le contrôle d'accès aux appareils Exchange ActiveSync. Une règle de contrôle d'accès à Endpoint Management Connector pour Exchange ActiveSync se compose de deux parties : une expression correspondante et un état d'accès souhaité (Autoriser ou Bloquer). Une règle doit être testée par rapport à un appareil ActiveSync Exchange donné pour déterminer si elle s'applique à l'appareil ou correspond à ce dernier. Il existe plusieurs types d'expressions correspondantes ; une règle peut, par exemple, correspondre à tous les appareils d'un type d'appareil donné ou à un ID d'appareil ActiveSync Exchange spécifique, ou encore à tous les appareils d'un utilisateur spécifique, etc.

À tout moment lors de l'ajout, la suppression et la réorganisation de règles dans la liste, si vous cliquez sur le bouton **Cancel**, l'état dans lequel se trouvait la liste lors de la première ouverture est rétabli. Si vous fermez l'outil de configuration sans cliquer sur **Save**, les modifications apportées sur cette fenêtre seront perdues.

Endpoint Management Connector pour Exchange ActiveSync propose trois types de règles : les règles locales, les règles de XenMobile Server (aussi appelées règles XDM), et la règle d'accès par défaut.

Local rules (Règles locales) : les règles locales ont la priorité la plus élevée : si un appareil est identifié par une règle locale, l'évaluation de la règle ne s'applique pas. Ni les règles de XenMobile Server ni la règle d'accès par défaut ne seront consultées. Les règles locales se configurent localement sur Endpoint Management Connector pour Exchange ActiveSync via l'onglet **Configure > Access Rules > Local Rules**. La prise en charge de correspondance se base sur l'appartenance des utilisateurs à un groupe Active Directory donné. La prise en charge de correspondance se base sur des expressions régulières pour les champs suivants :

- Active Sync Device ID
- ActiveSync Device Type
- User Principal Name (UPN)
- ActiveSync User Agent (généralement la plate-forme de l'appareil ou le client de messagerie)

Si un instantané principal a été effectué et qu'il a trouvé des appareils, vous pouvez ajouter une règle d'expressions normales ou régulières. Si aucun instantané principal n'a été effectué, vous pouvez uniquement ajouter des règles d'expressions régulières.

Règles du serveur XenMobile : les règles de XenMobile Server sont des références à un serveur XenMobile externe qui fournit des règles aux appareils gérés. XenMobile Server peut être configuré avec ses propres règles de haut niveau qui identifient les appareils à autoriser ou à bloquer en fonction des propriétés connues par XenMobile, par exemple si l'appareil est jailbreaké ou s'il contient des applications interdites. XenMobile évalue les règles de haut niveau et génère un ensemble d'ID d'appareils ActiveSync autorisés ou bloqués, qui sont ensuite envoyés à Endpoint Management Connector pour Exchange ActiveSync.

Default access rule (Règle d'accès par défaut) : la règle d'accès par défaut est unique car elle peut potentiellement s'appliquer à tous les appareils et elle est toujours évaluée en dernier. C'est la règle passe-partout, ce qui signifie que si un appareil donné ne correspond pas à une règle locale ou de XenMobile Server, l'état d'accès souhaité de l'appareil est déterminé par l'état d'accès souhaité de la règle d'accès par défaut.

- **Default Access – Allow (Accès par défaut - Autoriser) :** tout appareil ne correspondant pas à une règle locale ou de XenMobile Server sera autorisé.
- **Default Access – Block (Accès par défaut - Bloquer) :** tout appareil ne correspondant pas à une règle locale ou de XenMobile Server sera bloqué.
- **Default Access - Unchanged (Accès par défaut - Inchangé) :** l'état d'accès de tout appareil non associé à une règle locale ou de XenMobile Server ne pourra pas être modifié par Endpoint Management Connector pour Exchange ActiveSync. Si un appareil a été placé en quarantaine par Exchange, aucune action n'est prise ; par exemple, la seule manière de retirer un appareil en quarantaine est de posséder une règle locale ou XDM qui outrepasse explicitement la quarantaine.

À propos des évaluations de règles

Pour chaque appareil pour lequel Exchange remet des rapports à Endpoint Management Connector pour Exchange ActiveSync, les règles sont évaluées dans l'ordre, de la priorité la plus élevée à la plus faible, comme suit :

- Règles locales
- Règles de XenMobile Server
- Règle d'accès par défaut

Lorsqu'une correspondance est trouvée, l'évaluation s'arrête. Par exemple, si un appareil correspond à une règle locale, l'appareil ne sera pas évalué par rapport aux règles de XenMobile Server ou à la règle d'accès par défaut. Cela reste aussi vrai pour un type de règle donné. Par exemple, s'il existe plus d'une correspondance pour un appareil donné dans la liste des règles locales, l'évaluation s'arrête dès la première correspondance.

Endpoint Management Connector pour Exchange ActiveSync réévalue l'ensemble des règles déjà définies lorsque les propriétés d'un appareil sont modifiées, lorsque des appareils sont ajoutés ou supprimés ou lorsque les règles sont modifiées. Les instantanés principaux détectent la suppression d'appareils ainsi que les modifications apportées à leurs propriétés à intervalles configurables. Les instantanés secondaires détectent les nouveaux appareils à intervalles configurables.

Exchange ActiveSync possède aussi des règles régissant l'accès. Il est important de bien comprendre le fonctionnement de ces règles dans l'environnement Endpoint Management Connector pour Exchange ActiveSync. Exchange peut être configuré avec trois niveaux de règles : les exemptions personnelles, les règles d'appareil et les paramètres d'organisation. Endpoint Management Connec-

tor pour Exchange ActiveSync automatise le contrôle d'accès en envoyant des requêtes PowerShell à distance via un programme pour modifier la liste des exemptions personnelles. Il s'agit de listes d'ID d'appareils Exchange ActiveSync autorisés ou bloqués associés à une boîte aux lettres donnée. Lorsqu'il est déployé, Endpoint Management Connector pour Exchange ActiveSync prend en charge la gestion des listes d'exemptions dans Exchange. Pour plus de détails, consultez l'article Microsoft, Controlling Device Access.

L'analyse est particulièrement utile dans les situations dans lesquelles plusieurs règles ont été définies pour le même champ. Vous pouvez résoudre les relations entre les règles. Vous pouvez effectuer des analyses depuis la perspective des champs de règle ; par exemple, les règles sont analysées par groupes en fonction du champ remplissant la condition, tel que ActiveSync device ID, ActiveSync device type, User, User Agent, et ainsi de suite.

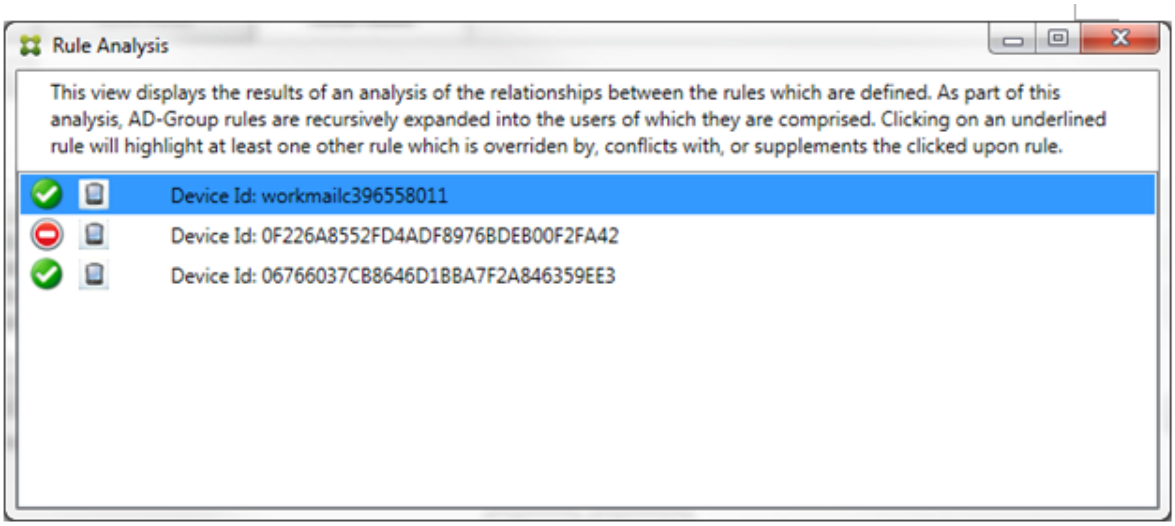
Terminologie relative aux règles

- **Règle absolue :** une substitution se produit lorsque plusieurs règles s'appliquent à un même appareil. Étant donné que les règles sont évaluées par priorité dans la liste, la ou les dernières instances de règle devant s'appliquer peuvent ne jamais être évaluées.
- **Règle conflictuelle :** un conflit survient quand plusieurs règles s'appliquent à un même appareil et que l'accès (Autoriser/Bloquer) ne correspond pas. Si les règles conflictuelles ne sont pas des expressions régulières, un conflit se traduit toujours implicitement par une substitution.
- **Règle complémentaire :** un complément a lieu lorsque plusieurs règles sont des expressions régulières et par conséquent, il peut s'avérer nécessaire de vérifier que les deux expressions régulières (ou plus) peuvent être combinées en une seule expression ou qu'il n'y ait pas duplication de fonctionnalités. Une règle complémentaire peut également causer des problèmes de conflit d'accès (Autoriser/Bloquer).
- **Règle principale :** la règle principale est la règle sur laquelle l'utilisateur a cliqué dans la boîte de dialogue. La règle est indiquée visuellement par une bordure. La règle aura également une ou deux flèches vertes pointant vers le haut ou vers le bas. Si une flèche pointe vers le haut, cela indique qu'il existe des règles secondaires qui précèdent la règle principale. Si une flèche pointe vers le bas, cela indique qu'il existe des règles secondaires qui s'appliquent après la règle principale. Seule une règle principale peut être active à tout moment.
- **Règle secondaire :** une règle secondaire est liée d'une certaine manière à la règle principale que ce soit via une relation de remplacement, de conflit ou supplémentaire. Les règles sont indiquées visuellement par une bordure en pointillés. Pour chaque règle principale, il peut y avoir une ou plusieurs règles secondaires. Lorsque vous cliquez sur une entrée soulignée, la ou les règles secondaires sélectionnées le sont toujours du point de vue de la règle principale. Par exemple, la règle secondaire est remplacée par la règle principale et/ou la règle secondaire entrera en conflit avec la règle principale et/ou la règle secondaire complétera la règle principale.

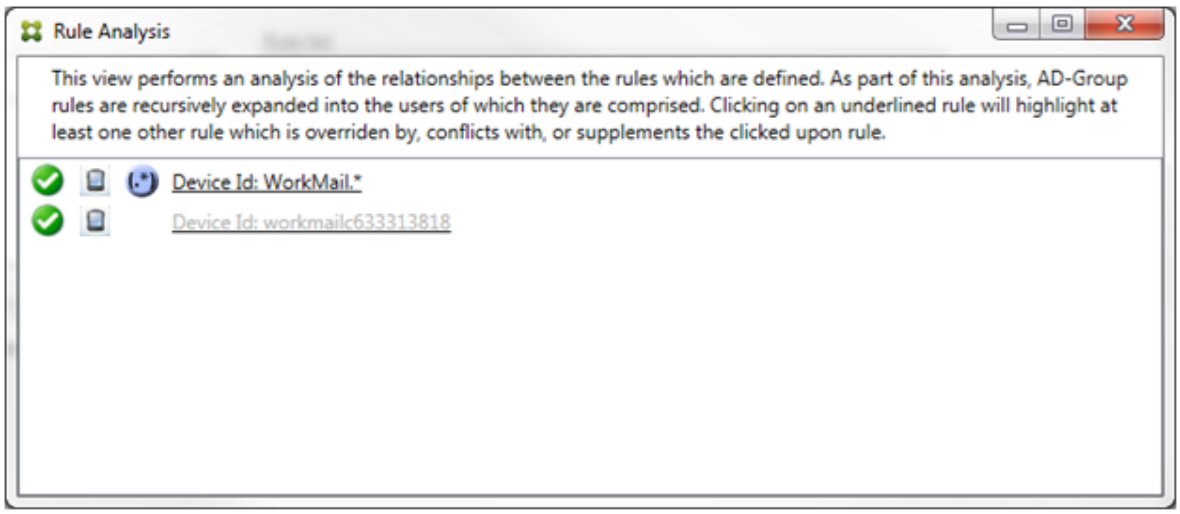
Apparence des types de règles dans la boîte de dialogue d'analyse des règles

Lorsqu'il n'y a aucun conflit, remplacement, ou complément, il n'y a pas d'entrées soulignées dans la boite de dialogue Rule Analysis. Par exemple, cliquer sur des éléments n'a pas d'impact, les éléments normaux sélectionnés sont mis en évidence.

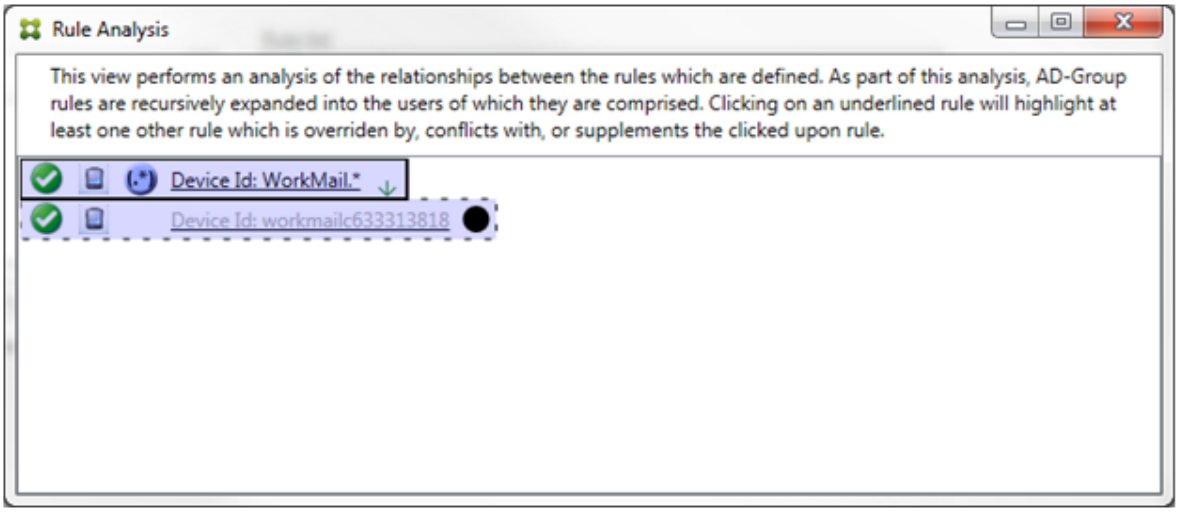
La fenêtre Rule Analysis contient une case qui, lorsqu'elle est sélectionnée, affiche uniquement les conflits, remplacements, redondances ou compléments.



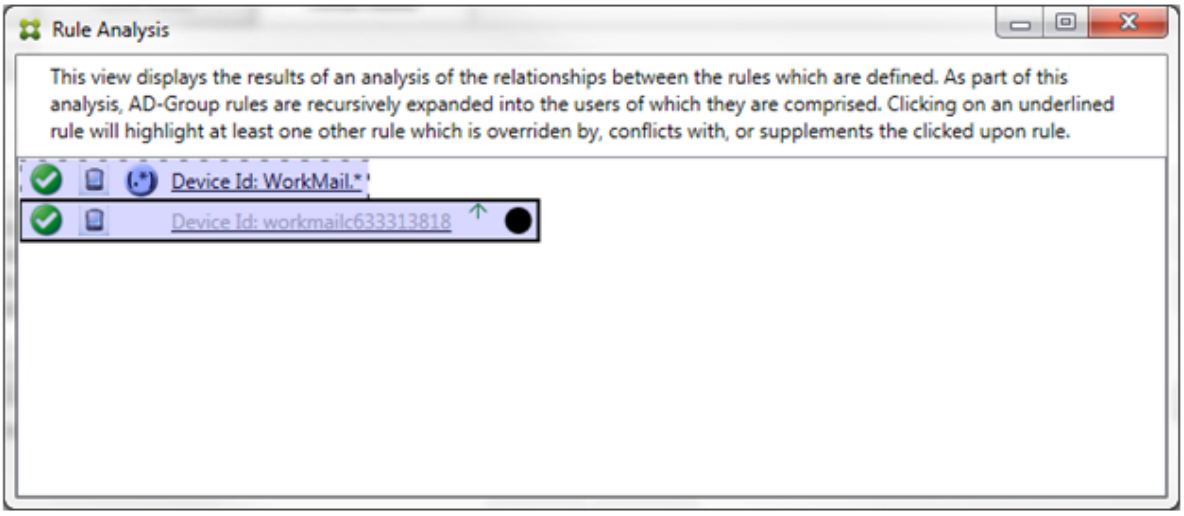
Lorsqu'une substitution se produit, au moins deux règles sont soulignées : la règle principale et la ou les règles secondaires. Au moins une règle secondaire s'affiche dans une police plus claire pour indiquer que la règle a été remplacée par une règle de priorité plus élevée. Vous pouvez cliquer sur les règles remplacées pour déterminer la ou les règles qui ont remplacé la règle. Lorsqu'une règle remplacée a été soulignée que ce soit parce que la règle est une règle principale ou secondaire, un cercle noir apparaît à côté en guise d'indication visuelle signifiant que la règle est inactive. Par exemple, avant que vous cliquiez sur la règle, la boîte de dialogue se présente comme suit :



Lorsque vous cliquez sur la règle prioritaire, la boîte de dialogue se présente comme suit :



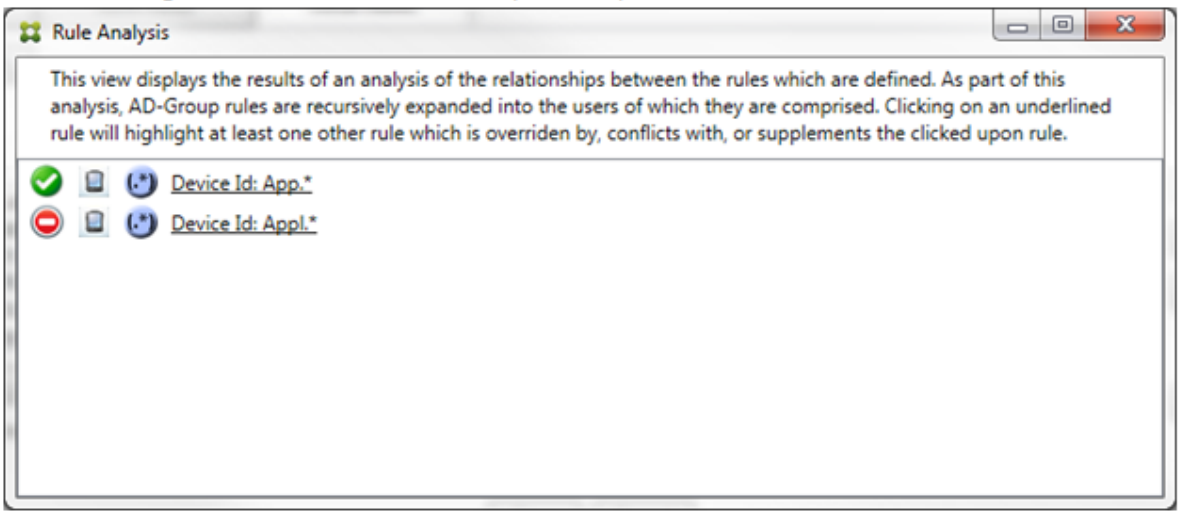
Dans cet exemple, la règle d'expression régulière `WorkMail.*` est la règle principale (indiquée par une bordure pleine) et la règle normale `workmailc633313818` est une règle secondaire (indiquée par une bordure en pointillés). Le point noir à côté de la règle secondaire est une indication visuelle qui signifie que la règle est inactive (ne sera jamais évaluée) en raison de la règle d'expression régulière prioritaire. Une fois que vous avez cliqué sur la règle remplacée, la boîte de dialogue se présente comme suit :



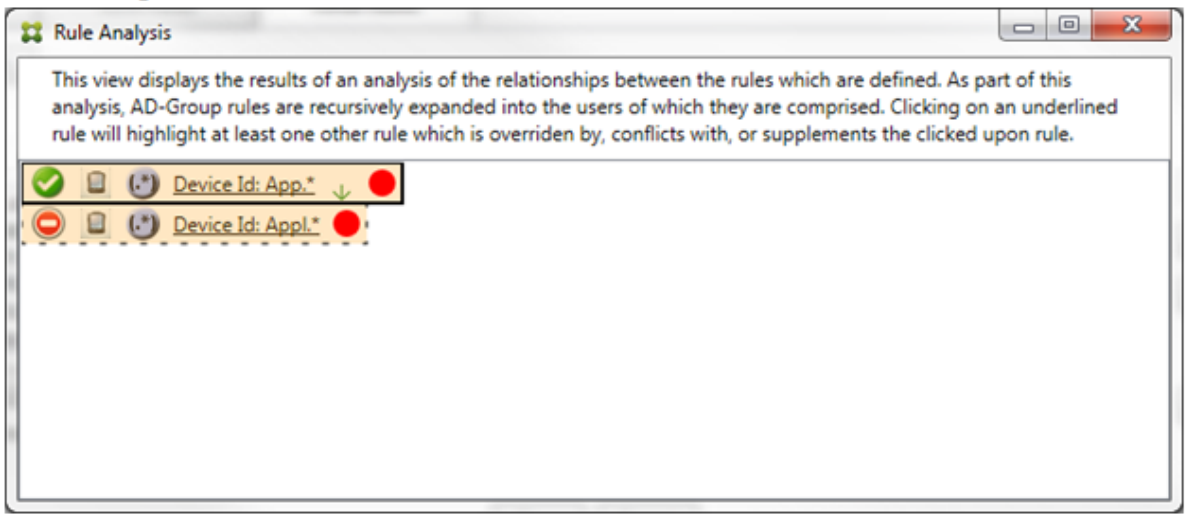
Dans l'exemple précédent, la règle d'expression régulière `WorkMail.*` est la règle secondaire (indiquée par une bordure en pointillés) et la règle normale `workmailc633313818` est une règle principale (indiquée par une bordure pleine). Pour cet exemple simple, il n'y a pas grande différence. Pour un exemple plus compliqué, consultez l'exemple d'expression complexe plus en avant dans cette rubrique. Dans un scénario avec de nombreuses règles définies, cliquer sur la règle remplacée permet d'identifier rapidement par quelles règles elle a été remplacée.

Lorsqu'un conflit se produit, au moins deux règles sont soulignées : la règle principale et la ou les

règles secondaires. Les règles en conflit sont indiquées par un point rouge. Le cas de règles qui entrent seulement en conflit avec une autre règle est uniquement possible avec deux ou plusieurs règles d'expressions régulières définies. Dans tous les autres cas de conflit, il y aura non seulement un conflit, mais aussi un remplacement. Avant que vous cliquiez sur des règles dans un exemple simple, la boîte de dialogue se présente comme suit :



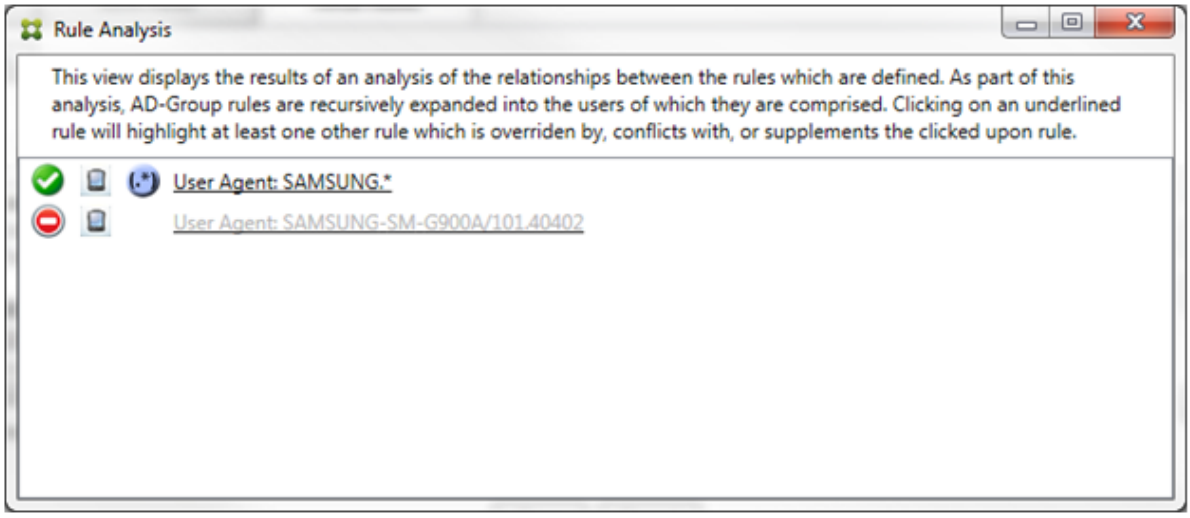
En inspectant les deux règles d'expressions régulières, il est évident que la première règle autorise tous les appareils avec un ID d'appareil contenant « App » et que la deuxième règle refuse tous les appareils avec un ID d'appareil contenant « Appl ». En outre, même si la deuxième règle refuse tous les appareils avec un ID d'appareil contenant « Appl », aucun appareil correspondant à ces critères ne verra son accès refusé en raison de la priorité plus élevée de la règle l'y autorisant. Une fois que vous avez cliqué sur la première règle, la boîte de dialogue se présente comme suit :



Dans le cas précédent, la règle principale (règle d'expression régulière `App.*`) et la règle secondaire (règle d'expression régulière `Appl.*`) sont toutes deux affichées en jaune. Il s'agit simplement d'une indication visuelle vous alertant du fait que vous avez appliqué plus d'une règle d'expression régulière

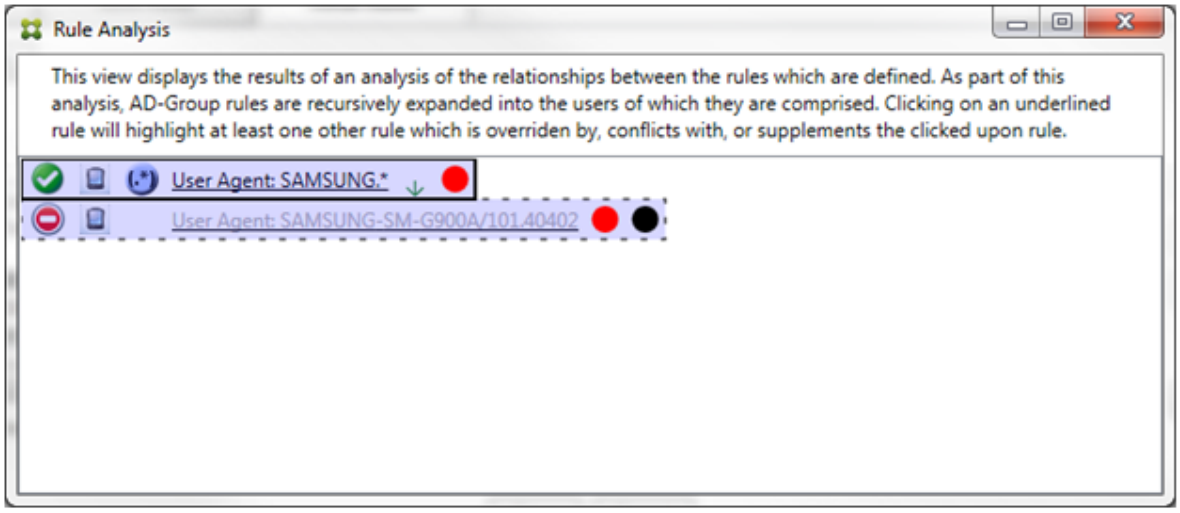
à un même champ de correspondance, ce qui peut entraîner un problème de redondance ou quelque chose de plus sérieux.

Dans un cas regroupant un conflit et un remplacement, la règle principale (règle d'expression régulière `App.*`) et la règle secondaire (règle d'expression régulière `Appl.*`) sont surlignées en jaune. Il s'agit simplement d'une indication visuelle vous alertant du fait que vous avez appliqué plus d'une règle d'expression régulière à un même champ de correspondance, ce qui peut entraîner un problème de redondance ou quelque chose de plus sérieux.



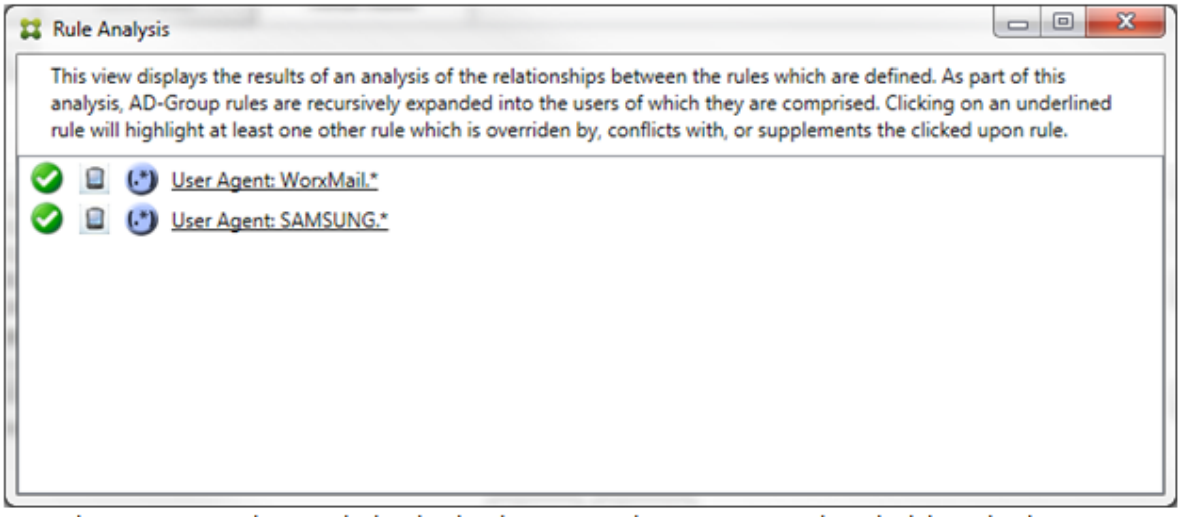
Il est facile de voir dans l'exemple précédent que la première règle (règle d'expression régulière `SAMSUNG.*`) ne remplace pas seulement la règle suivante (règle normale `SAMSUNG-SM-G900A/101.40402`), mais que l'accès des deux règles est différent (la règle principale indique Autoriser, la règle secondaire indique Bloquer). La deuxième règle (règle normale `SAMSUNG-SM-G900A/101.40402`) est affichée dans une police plus claire pour indiquer qu'elle a été remplacée et qu'elle n'est donc pas active.

Une fois que vous avez cliqué sur la règle d'expression régulière, la boîte de dialogue se présente comme suit :

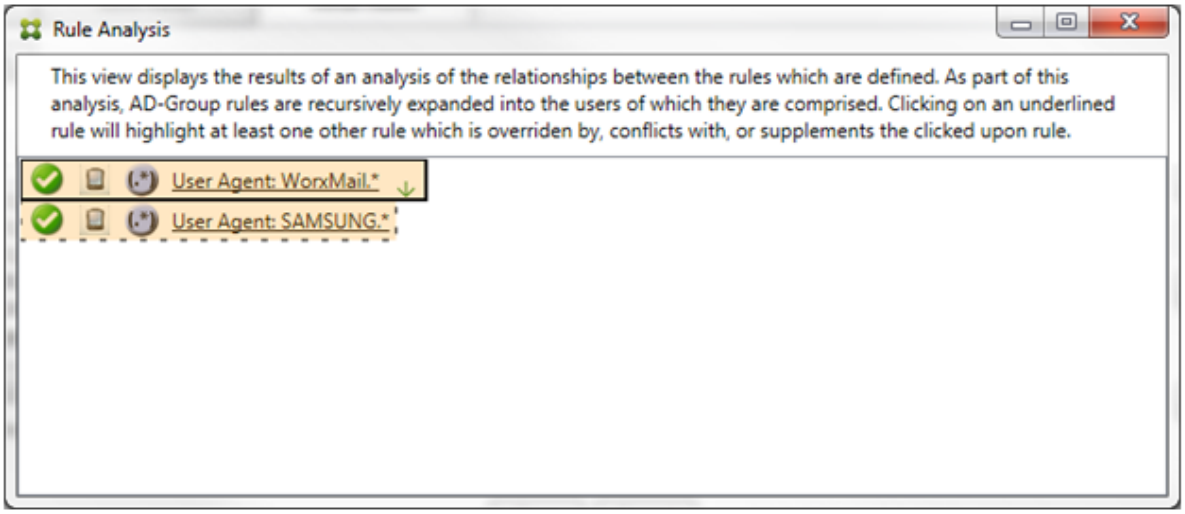


La règle principale (règle d'expression régulière `SAMSUNG.*`) est suivie d'un point rouge indiquant qu'elle entre en conflit avec une ou plusieurs règles secondaires. La règle secondaire (règle normale `SAMSUNG-SM-G900A/101.40402`) est suivie d'un point rouge pour indiquer que son état d'accès est en conflit avec la règle principale. Cette règle est également suivie d'un point noir pour indiquer qu'elle est substituée et donc inactive.

Au moins deux règles sont soulignées : la règle principale et la ou les règles secondaires. Les règles qui se complètent uniquement entre elles n'impliquent que des règles d'expressions régulières. Lorsque des règles se complètent entre elles, elles sont surlignées en jaune. Avant que vous cliquiez sur des règles dans un exemple simple, la boîte de dialogue se présente comme suit :



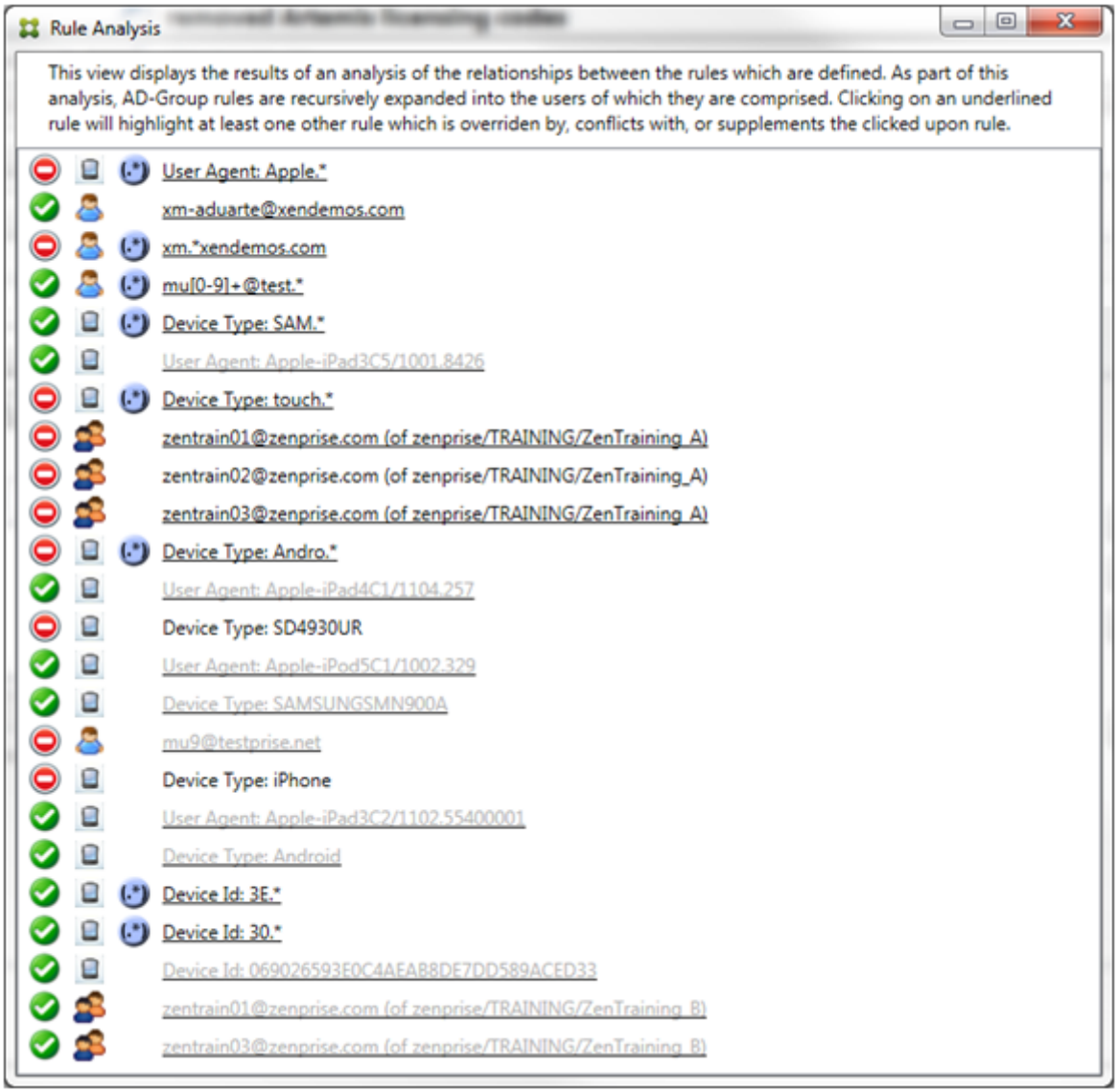
L'inspection visuelle révèle facilement que les deux règles sont des règles d'expressions régulières qui s'appliquent toutes les deux au champ ActiveSync device ID dans Endpoint Management Connector pour Exchange ActiveSync. Une fois que vous avez cliqué sur la première règle, la boîte de dialogue se présente comme suit :



La règle principale (règle d'expression régulière `WorkMail.*`) est surlignée en jaune pour indiquer qu'il existe au moins une autre règle secondaire qui est une expression régulière. La règle secondaire (règle d'expression régulière `SAMSUNG.*`) est surlignée en jaune pour indiquer que celle-ci et la règle principale sont des règles d'expressions régulières qui s'appliquent à un même champ dans Endpoint Management Connector pour Exchange ActiveSync. Dans ce cas, ce champ est ActiveSync device ID. Les expressions régulières peuvent ou non se chevaucher. C'est à vous de décider si vos expressions régulières sont correctement conçues.

Exemple d'expression complexe

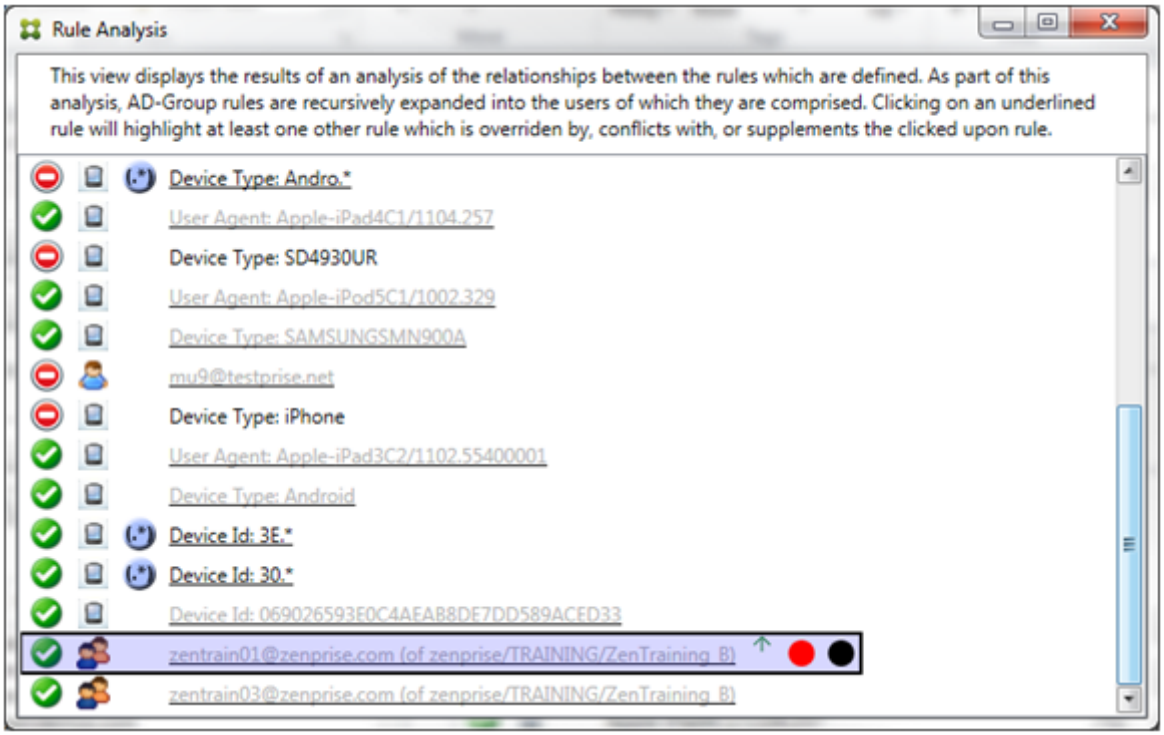
De nombreux remplacements, conflits ou compléments sont susceptibles de se produire, c'est pourquoi il est impossible de fournir des exemples couvrant tous les scénarios envisageables. L'exemple suivant explique ce qu'il ne faut pas faire, et sert aussi à illustrer toute la portée de la présentation visuelle de l'analyse des règles. La plupart des éléments sont soulignés dans la figure ci-après. Plusieurs des éléments s'affichent dans une police plus claire, ce qui indique que la règle en question a été remplacée par une règle dont la priorité est plus élevée. Un certain nombre de règles d'expressions régulières sont incluses dans la liste, comme l'indique l'icône  .



Comment analyser un remplacement

Pour afficher la ou les règles qui ont remplacé une règle particulière, cliquez sur cette dernière.

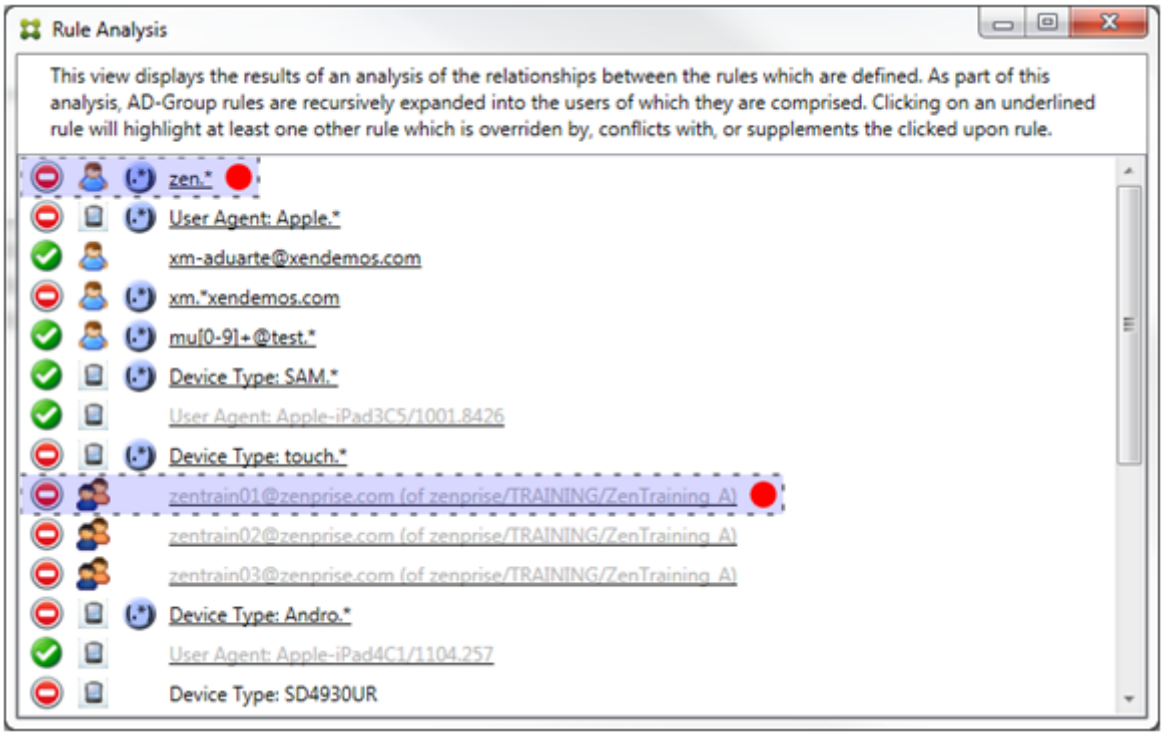
Exemple 1 : cet exemple explique pourquoi `zentrain01@zenprise.com` a été remplacée.



La règle principale (règle de groupe AD `zenprise/TRAINING/ZenTraining B`, dont `zentrain01@zenprise.com` est un membre) présente les caractéristiques suivantes :

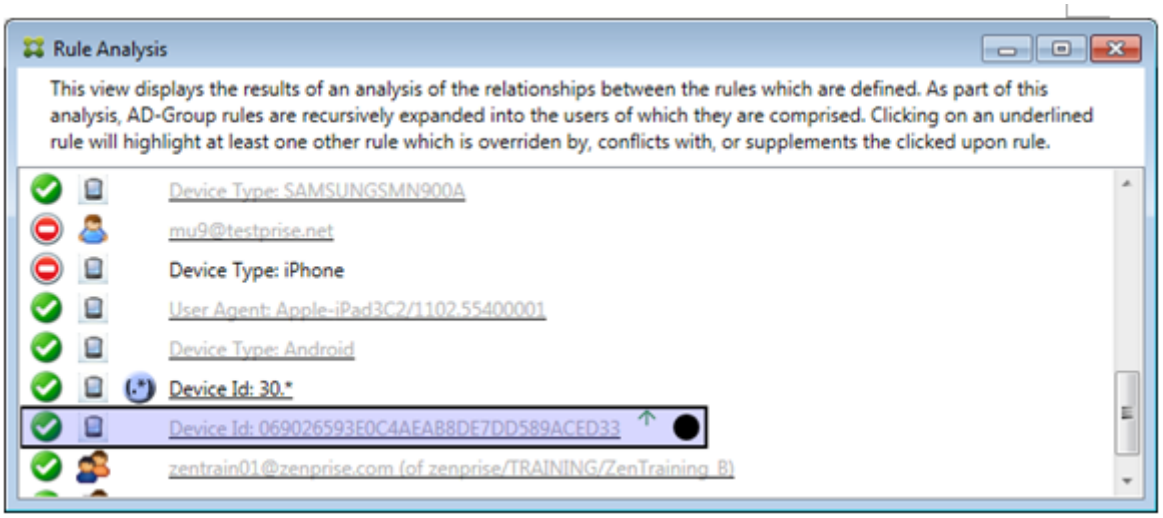
- Est surlignée en bleu et encadrée par une bordure pleine.
- A une flèche verte pointant vers le haut (pour indiquer que la règle secondaire ou l'ensemble des règles se trouvent au-dessus).
- Est suivie d'un cercle rouge et d'un cercle noir pour indiquer respectivement qu'une ou plusieurs règles secondaires sont en conflit et que la règle principale a été remplacée et n'est donc pas active.

Si vous faites défiler vers le haut, vous pouvez voir ce qui suit :



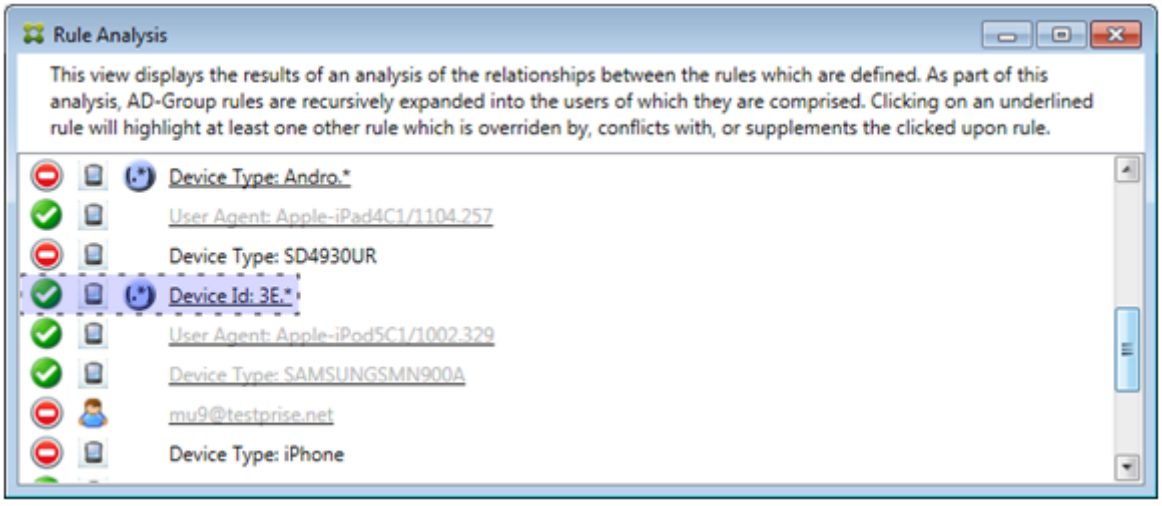
Dans ce cas, il existe deux règles secondaires qui remplacent la règle principale : la règle d'expression régulière `zen.*` et la règle normale `zentrain01@zenprise.com` (de `zenprise`/`TRAINING`/`ZenTraining A`). Dans le cas de la dernière règle secondaire, la règle de groupe Active Directory `ZenTraining A` contient l'utilisateur `zentrain01@zenprise.com` et la règle de groupe Active Directory `ZenTraining B` contient aussi l'utilisateur `zentrain01@zenprise.com`. Toutefois, étant donné que la règle secondaire a une priorité plus élevée que la règle principale, la règle principale a été remplacée. L'accès à la règle principale est Autoriser. Et comme l'accès des deux règles secondaires est Bloquer, toutes sont suivies d'un cercle rouge indiquant un conflit d'accès.

Exemple 2 : cet exemple illustre la raison pour laquelle l'appareil avec l'ID d'appareil ActiveSync `069026593E0C4AEAB8DE7DD589ACED33` a été remplacé :



La règle principale (règle d'ID d'appareil normale `069026593E0C4AEAB8DE7DD589ACED33`) présente les caractéristiques suivantes :

- Est surlignée en bleu et encadrée par une bordure pleine.
- A une flèche verte pointant vers le haut (pour indiquer que la règle secondaire doit se trouver au-dessus).
- Est suivie par un cercle noir indiquant qu'une règle secondaire a remplacé la règle principale et que la règle est par conséquent inactive.

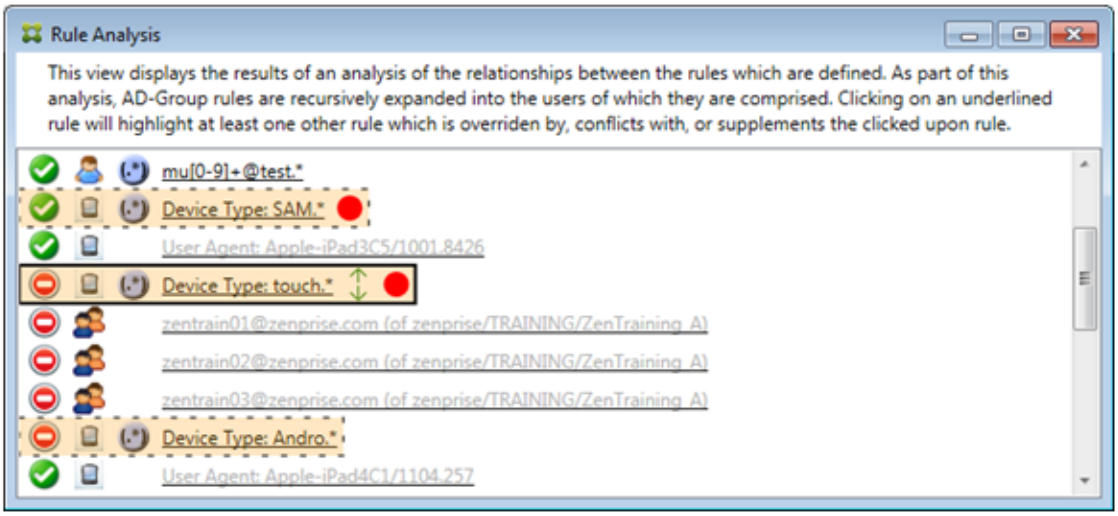


Dans ce cas, une seule règle secondaire remplace la règle principale : la règle d'expression régulière d'ID d'appareil ActiveSync est `3E.*`. Comme l'expression régulière `3E.*` correspond à `069026593E0C4AEAB8DE7DD589ACED33`, la règle ne sera jamais évaluée.

Comment analyser un supplément et un conflit

Dans ce cas, la règle principale est la règle d'expression régulière de type d'appareil ActiveSync `touch .*` Les caractéristiques sont les suivantes :

- Est signalée par une bordure pleine et surlignée en jaune indiquant qu'il y a plus d'une seule règle d'expression régulière appelant le même champ de règle, dans ce cas, ActiveSync device type.
- Deux flèches pointant vers le haut et vers le bas, ce qui indique qu'il existe au moins une règle secondaire avec une priorité plus élevée et au moins une règle secondaire avec une priorité inférieure.
- Le cercle rouge à côté indique qu'au moins une règle secondaire a son accès défini sur Allow, ce qui entre en conflit avec l'accès de la règle principale qui est défini sur Block.
- Il existe deux règles secondaires : la règle d'expression régulière ActiveSync Device Type `SAM.*` et la règle d'expression régulière ActiveSync Device Type `Andro.*`.
- Les deux règles secondaires sont encadrées par des pointillés pour indiquer qu'elles sont secondaires.
- Les règles secondaires sont surlignées en jaune pour indiquer qu'elles s'appliquent en aussi au champ de la règle ActiveSync Device Type.
- Vous devez vous assurer dans de tels scénarios que leurs règles d'expressions régulières ne sont pas redondantes.



Comment améliorer l'analyse des règles

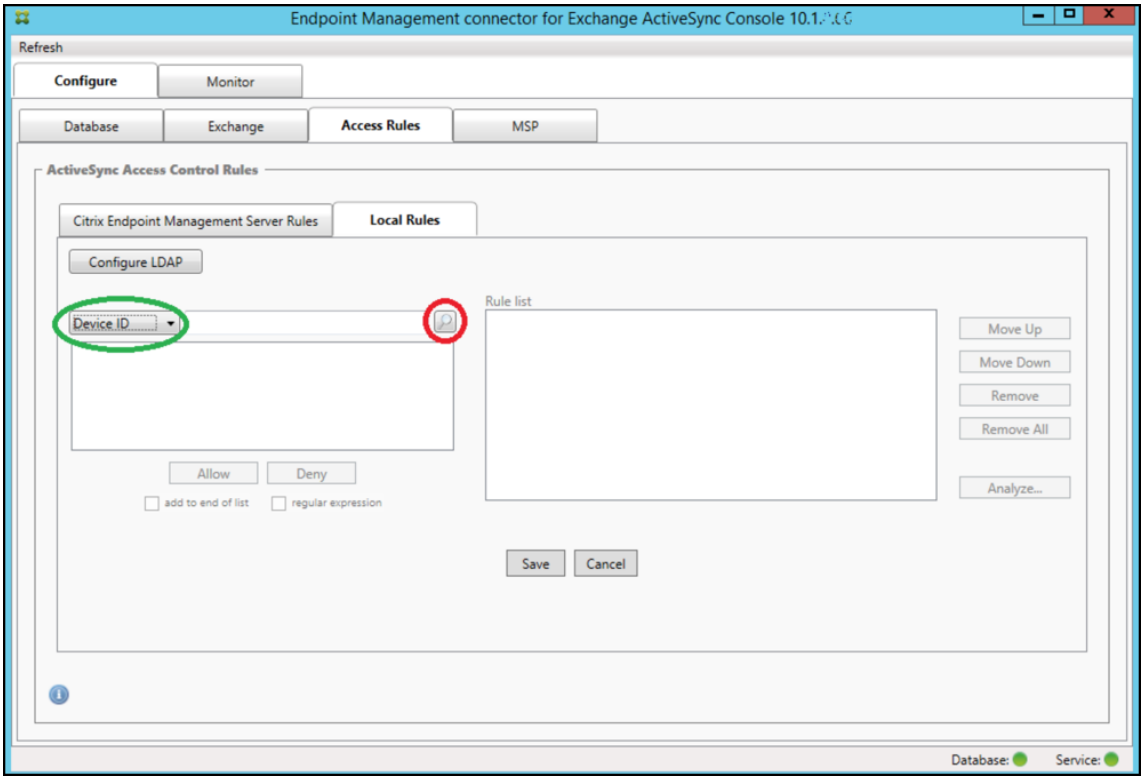
Cet exemple explique pourquoi les relations entre les règles sont toujours abordées du point de vue de la règle principale. L'exemple précédent a montré comment un clic sur la règle d'expression régulière

s'appliquait au champ de règle de type de périphérique avec une valeur de `touch.*`. Un clic sur la règle secondaire `Andro.*` montre un ensemble différent de règles secondaires mises en évidence.

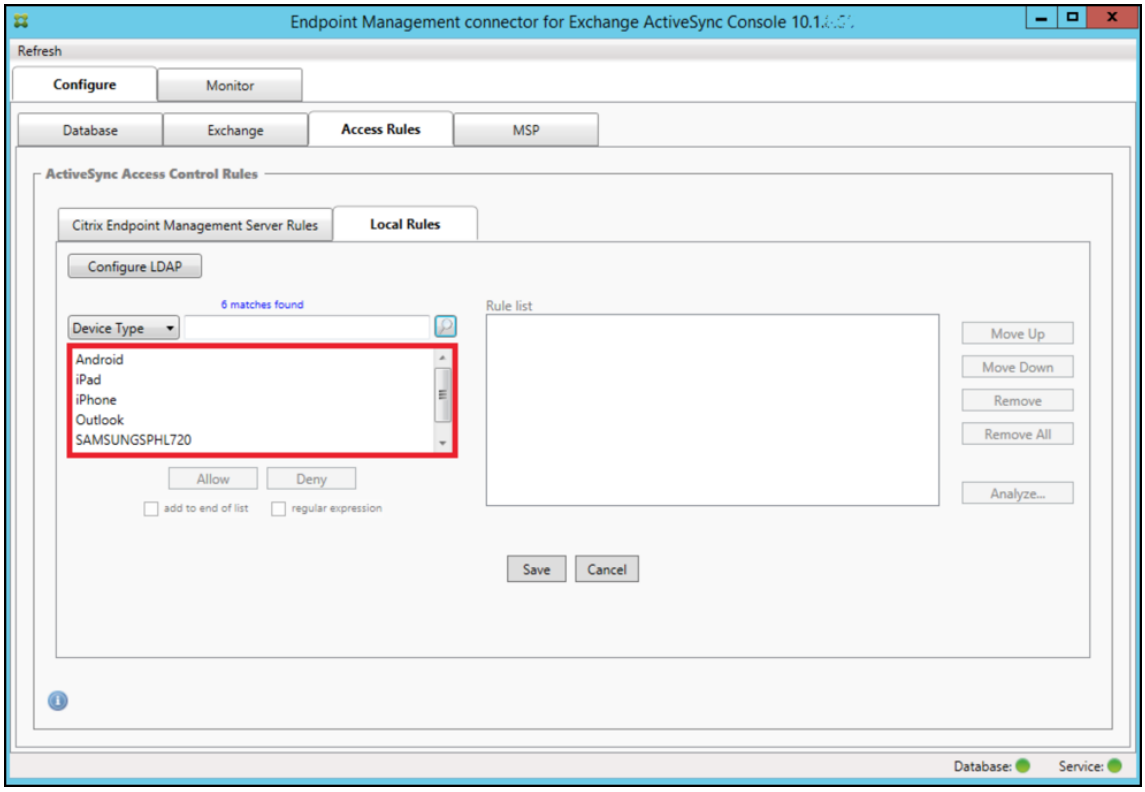
Cet exemple présente une règle remplacée qui est inclue dans la relation de règle. Cette règle est la règle normale ActiveSync Device Type `Android`, qui est remplacée (indiquée par une police plus claire et un cercle noir à côté) et qui entre également en conflit avec la règle d'expression régulière principale ActiveSync Device Type `Andro.*`. Cette règle était auparavant une règle secondaire avant d'être sélectionnée. Dans l'exemple précédent, la règle normale ActiveSync Device Type `Android` n'était pas affichée en tant que règle secondaire, car du point de vue de la règle principale (règle d'expression régulière ActiveSync Device Type `touch.*`), elle n'était pas liée.

Pour configurer une règle locale d'expression normale

1. Cliquez sur l'onglet **Access Rules**.



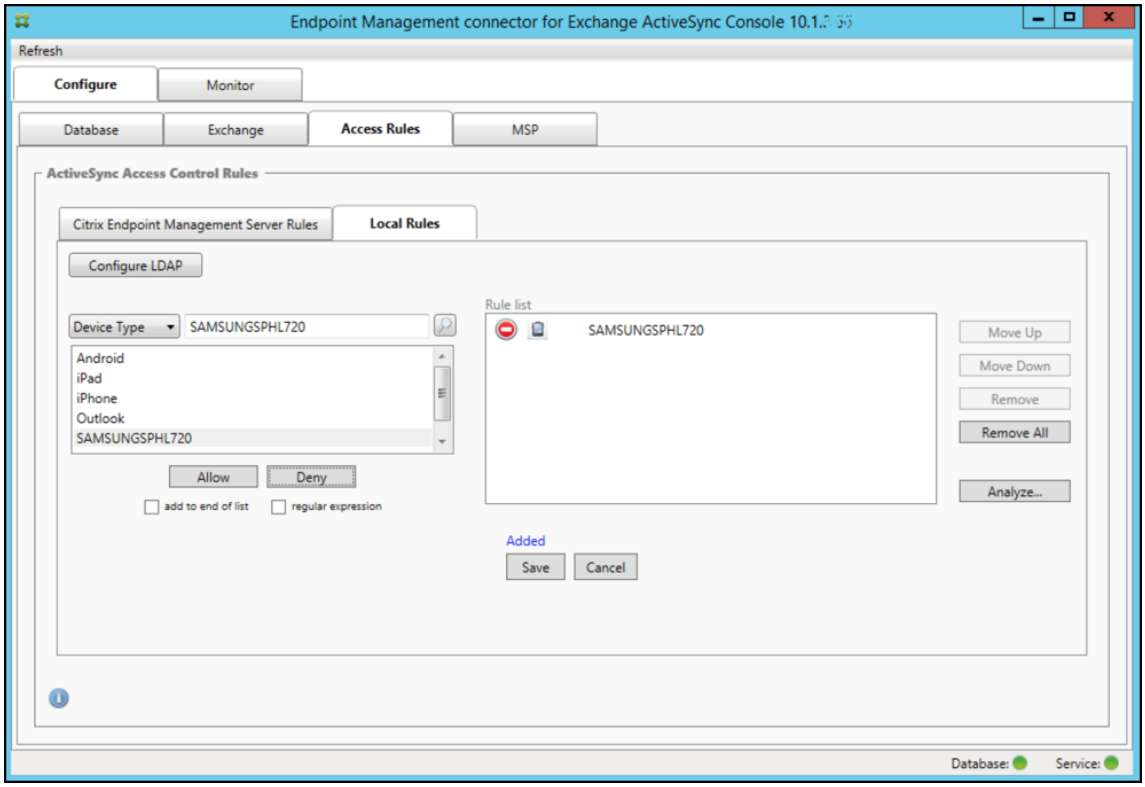
2. Dans la liste **Device ID**, sélectionnez le champ pour lequel vous souhaitez créer une règle locale.
3. Cliquez sur l'icône de la loupe pour afficher tous les résultats uniques pour le champ sélectionné. Dans cet exemple, le champ **Device Type** a été choisi et les choix sont affichés ci-dessous dans la zone de liste.



4. Cliquez sur un des éléments dans la liste des résultats et cliquez sur l'une des options suivantes :

   - **Allow** signifie qu'Exchange sera configuré pour permettre le trafic ActiveSync pour tous les appareils correspondant.
   - **Deny** signifie que Exchange sera configuré de manière à refuser le trafic ActiveSync de tous les appareils correspondant.

   Dans cet exemple, les appareils dont le type est SamsungSPhl720 se voient refuser l'accès.



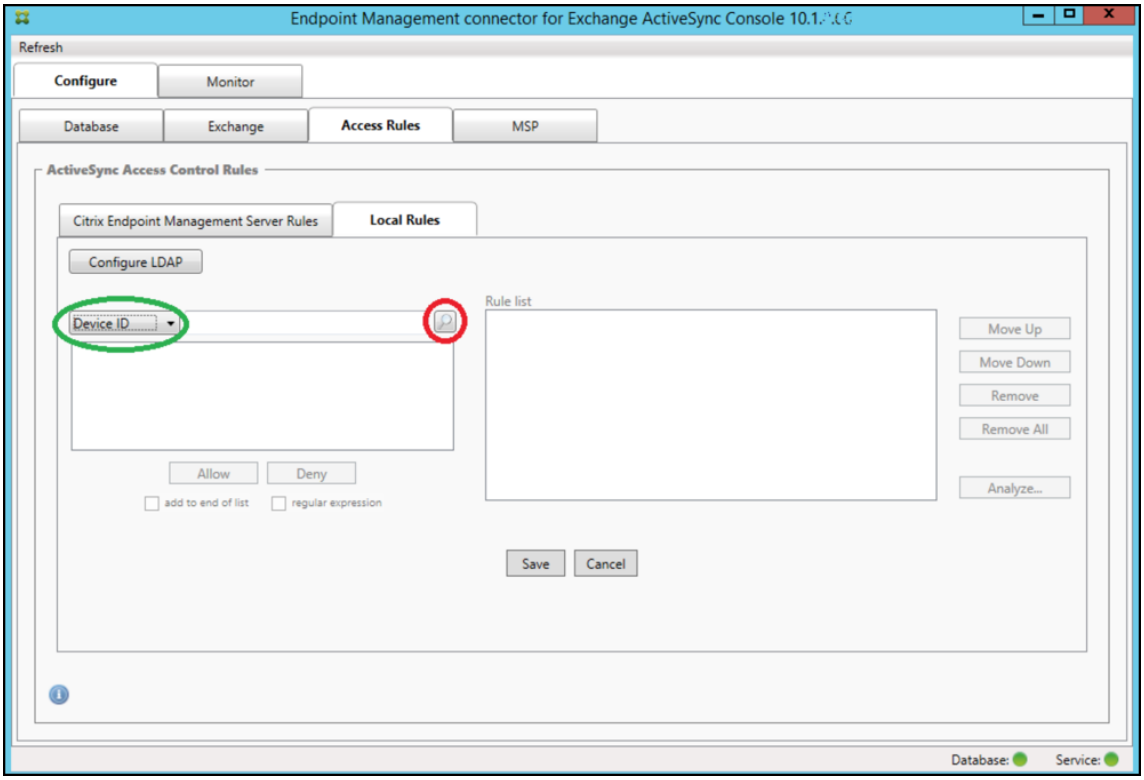
Pour ajouter une expression régulière

Les règles locales d'expressions régulières peuvent être différenciées par l'icône qui s'affiche à leur côté -  .

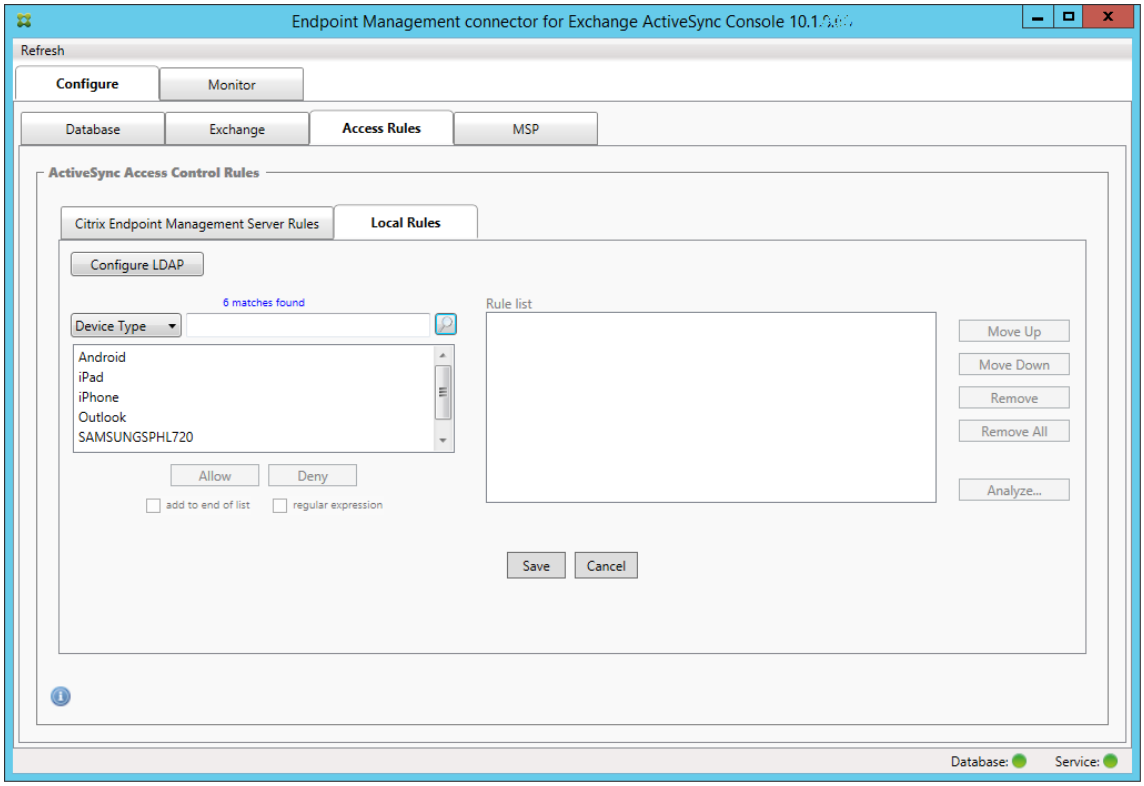
Pour ajouter une règle d'expression régulière, vous pouvez créer une règle d'expression régulière à partir d'une valeur existante dans la liste des résultats pour un champ donné (si un instantané principal a été effectué), ou vous pouvez simplement saisir l'expression régulière que vous souhaitez.

Pour créer une expression régulière à partir d'une valeur de champ existant

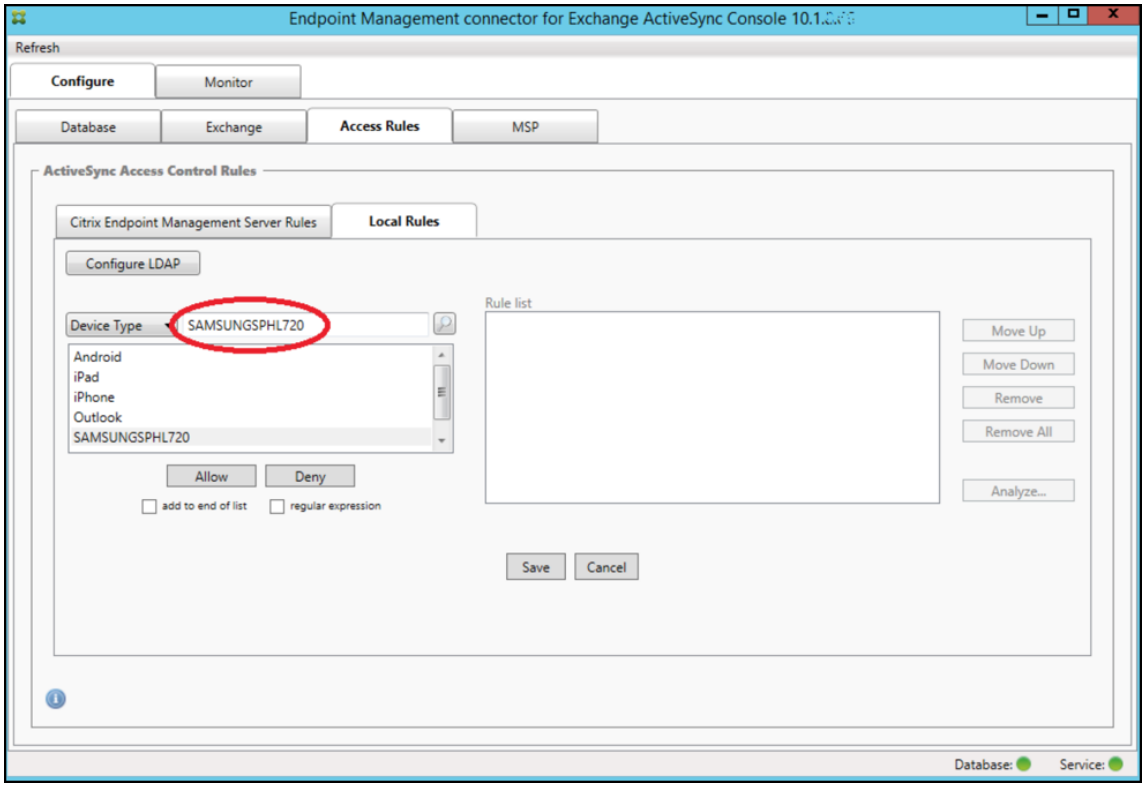
1. Cliquez sur l'onglet **Access Rules**.



2. Dans la liste **Device ID**, sélectionnez le champ pour lequel vous souhaitez créer une règle d'expression régulière locale.
3. Cliquez sur l'icône de la loupe pour afficher tous les résultats uniques pour le champ sélectionné. Dans cet exemple, le champ **Device Type** a été choisi et les choix sont affichés ci-dessous dans la zone de liste.



4. Cliquez sur un des éléments dans la liste des résultats. Dans cet exemple, **SAMSUNGSPHL720** a été sélectionné et s'affiche dans la zone de texte adjacente à **Device Type**.



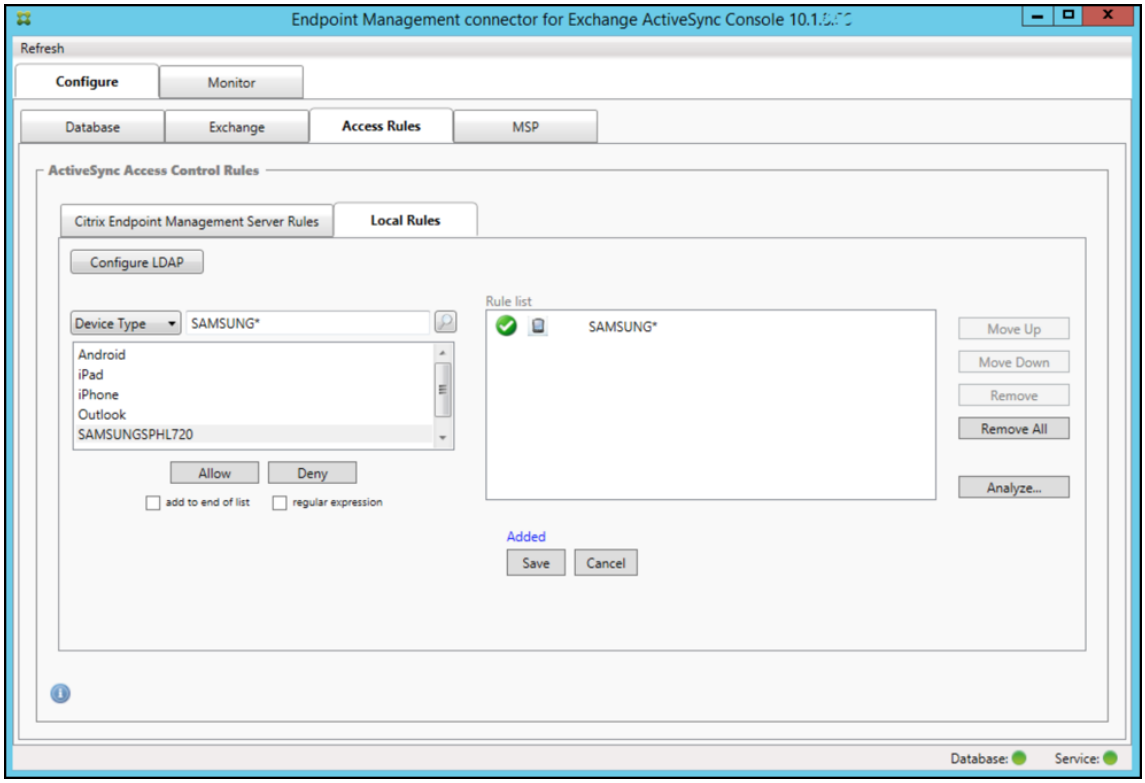
5. Pour autoriser tous les types d'appareils qui ont « Samsung » dans leur valeur Device Type, ajoutez une règle d'expression régulière en suivant les étapes suivantes :

   a) Cliquez dans la zone de texte de l'élément sélectionné.

   b) Remplacez le texte **SAMSUNGSPHL720** par **SAMSUNG.***.

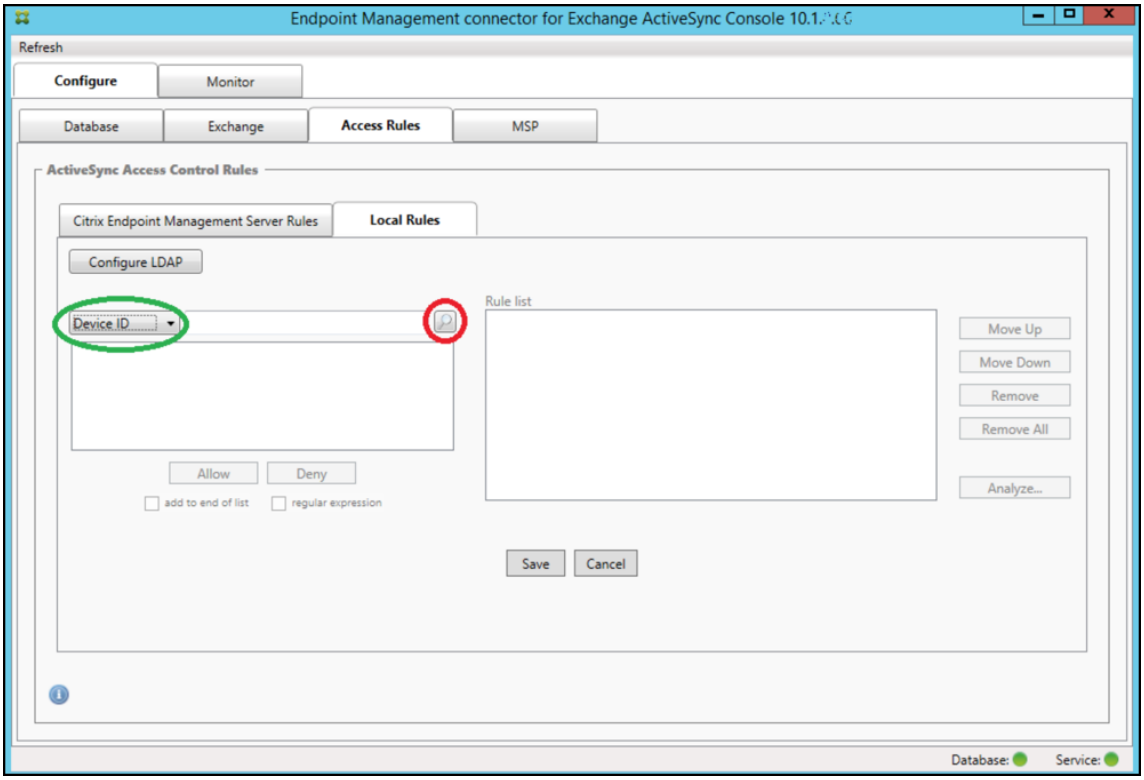
   c) Vérifiez que la case regular expression est cochée.

   d) Cliquez sur **Allow**.

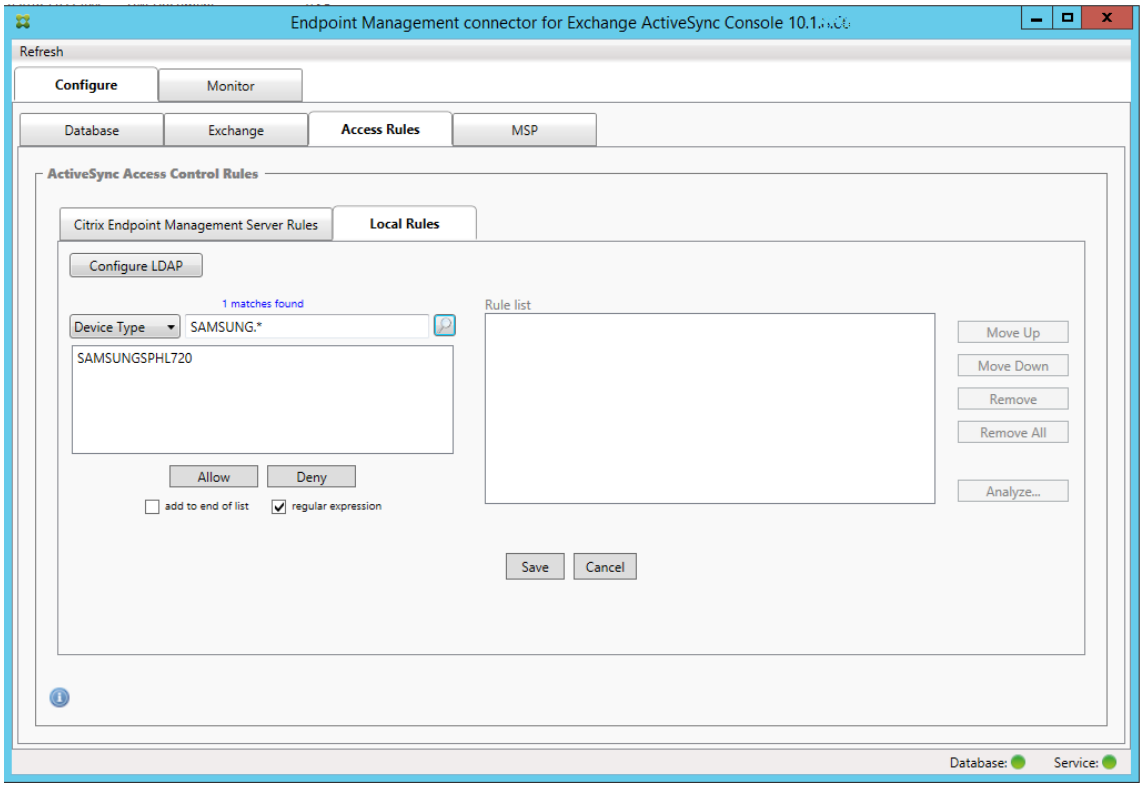


Pour créer une règle d'accès

1. Cliquez sur l'onglet **Local Rules**.
2. Pour entrer l'expression régulière, vous devez utiliser la liste Device ID et la zone de texte de l'élément sélectionné.



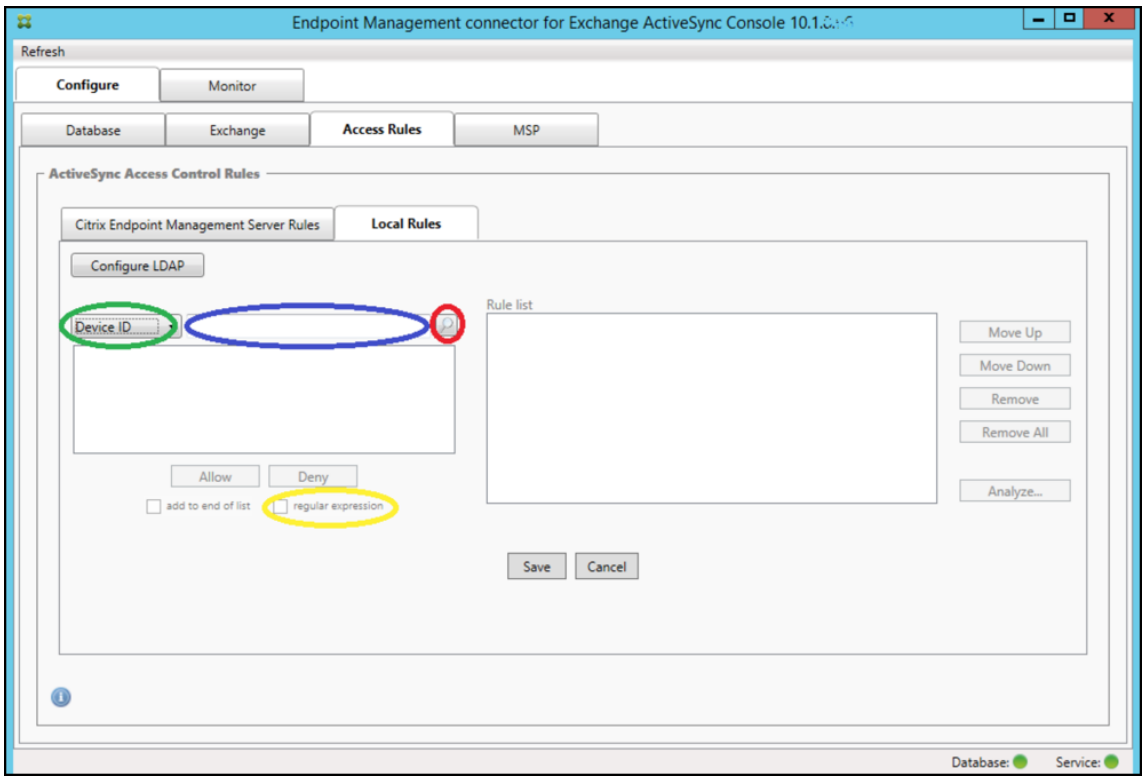
3. Sélectionnez le champ que vous voulez mettre en correspondance. Cet exemple utilise Device Type.
4. Entrez l'expression régulière. Cet exemple utilise `samsung.*`
5. Assurez-vous que la case regular expression est cochée et cliquez sur **Allow** ou **Deny**. Dans cet exemple, le choix est **Allow**. Le résultat final est le suivant :



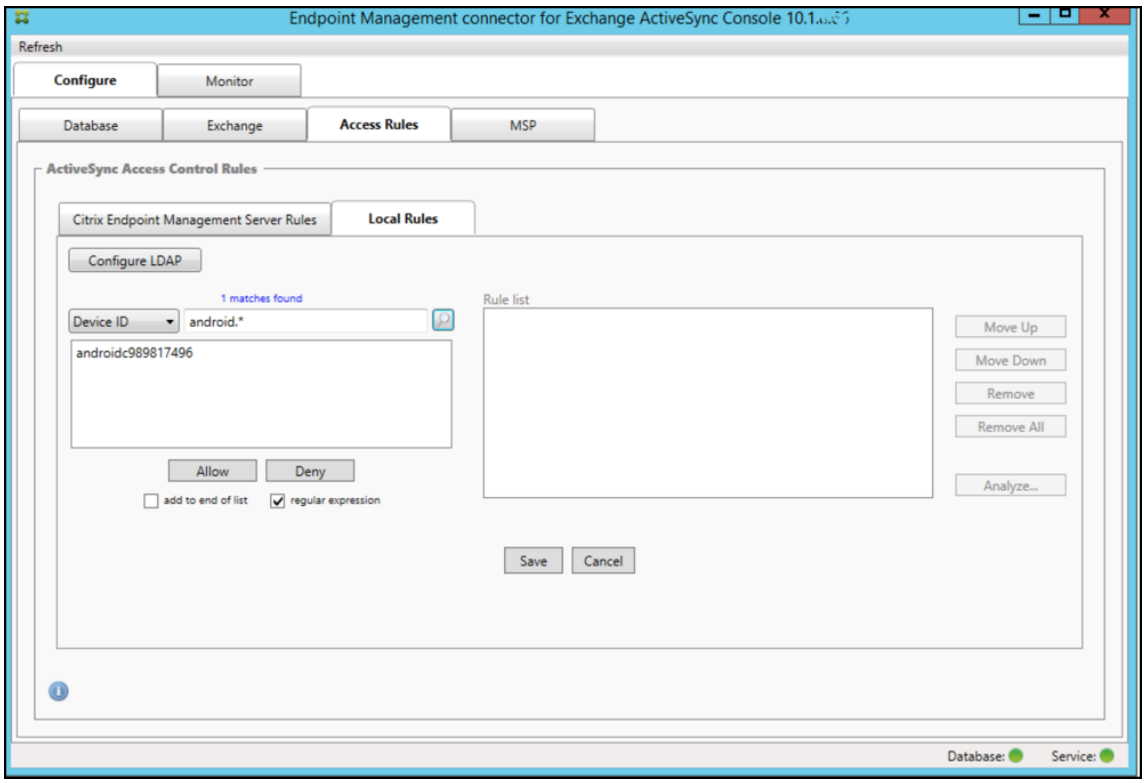
Pour rechercher des appareils

En cochant la case « regular expression », vous pouvez rechercher des appareils correspondant à l'expression donnée. Cette fonction est uniquement disponible si un instantané principal a été effectué. Vous pouvez utiliser cette fonction, même si vous ne prévoyez pas d'utiliser des règles d'expressions régulières. Imaginons que vous souhaitiez rechercher tous les appareils contenant « workmail » dans l'ID d'appareil ActiveSync. Pour ce faire, suivez cette procédure.

1. Cliquez sur l'onglet **Access Rules**.
2. Assurez-vous que le sélecteur de champ d'appareil est défini sur Device ID (valeur par défaut).



3. Cliquez sur la zone de texte de l'élément sélectionné (comme illustré en bleu dans la figure précédente) puis tapez `workmail.*`.
4. Vérifiez que la case regular expression est cochée et cliquez sur l'icône de la loupe pour afficher les correspondances comme illustré dans la figure suivante.

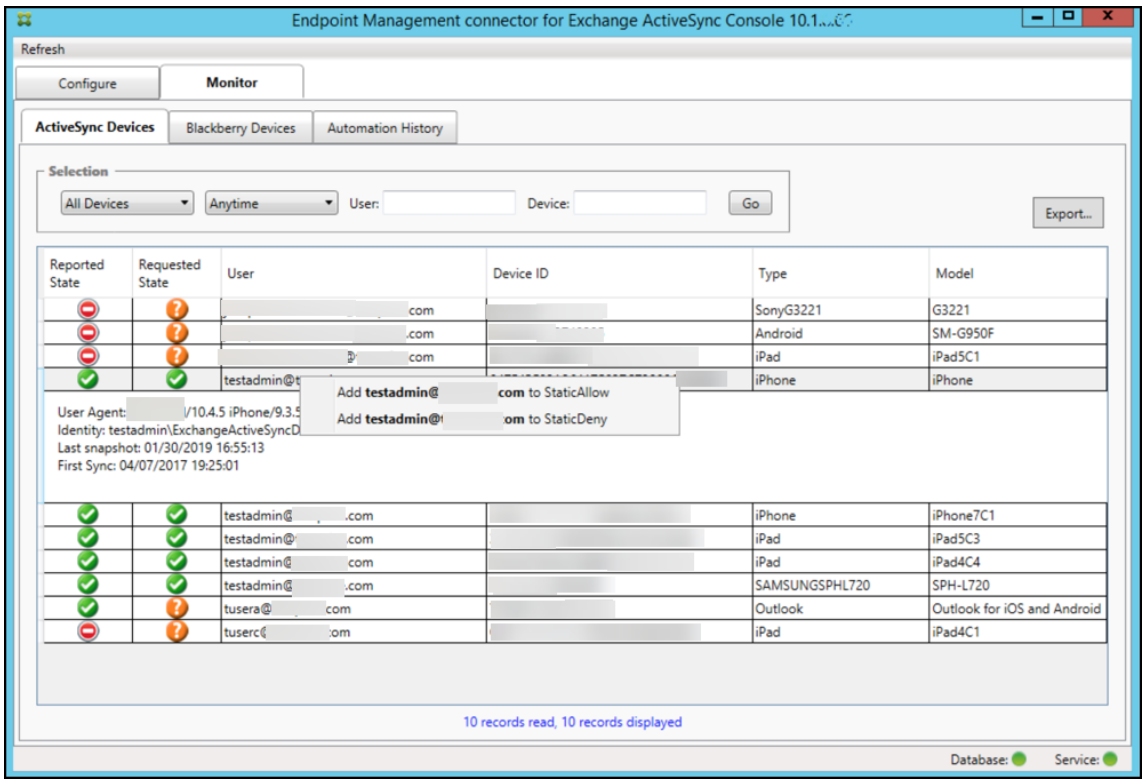


Pour ajouter un seul utilisateur, appareil ou type d'appareil à une règle statique

Vous pouvez ajouter des règles statiques basées sur l'utilisateur, l'ID d'appareil ou le type d'appareil sur l'onglet ActiveSync Devices.

1. Cliquez sur l'onglet **ActiveSync Devices**.
2. Dans la liste, cliquez avec le bouton droit sur un utilisateur, un appareil ou un type d'appareil et choisissez si vous souhaitez autoriser ou refuser votre sélection.

   L'image suivante montre l'option Allow/Deny lorsque user1 est sélectionné.



Surveillance des appareils

L'onglet **Monitor** de Endpoint Management Connector pour Exchange ActiveSync permet de visualiser les appareils Exchange ActiveSync et BlackBerry qui ont été détectés et l'historique des commandes PowerShell automatisées qui ont été émises. L'onglet **Monitor** inclut les trois onglets suivants :

- **Appareils ActiveSync** :
  - Vous pouvez exporter les partenariats d'appareils ActiveSync affichés en cliquant sur le bouton **Export**.
  - Vous pouvez ajouter des règles locales (statiques) en cliquant avec le bouton droit sur les colonnes **User**, **Device ID** où **Type** et en choisissant la règle d'autorisation ou de blocage appropriée.
  - Pour réduire une ligne développée, faites un Ctrl-clic sur la ligne développée.
- **Appareils BlackBerry**
- **Historique d'automatisation**

L'onglet **Configure** affiche l'historique de tous les instantanés. L'historique d'instantané affiche le moment où l'instantané a été capturé, la durée nécessaire à la capture, le nombre d'appareils détectés et toutes les erreurs qui se sont produites :

- Sur l'onglet **Exchange**, cliquez sur l'icône d'information pour le serveur Exchange Server désiré.
- Sous l'onglet **MSP**, cliquez sur l'icône d'information pour le serveur BlackBerry désiré.

Dépannage et diagnostics

Endpoint Management Connector pour Exchange ActiveSync consigne les erreurs et d'autres informations opérationnelles dans son fichier journal : *dossier d'installation*\log\XmmWindowsService.log. Endpoint Management Connector pour Exchange ActiveSync consigne également les événements importants dans le journal d'événements Windows.

Modifier le niveau de journalisation

Le connecteur Endpoint Management pour Exchange ActiveSync inclut les niveaux de journalisation suivants : Error, Info, Warn, Debug et Trace.

> **Remarque :**
>
> Chaque niveau successif génère plus de détails (plus de données). Par exemple, le niveau Error fournit le moins de détails, tandis que le niveau Trace fournit le plus de détails.

Pour modifier le niveau de journalisation, procédez comme suit :

1. Dans C:\Program Files\Citrix\Citrix Endpoint Management connector, ouvrez le fichier nlog.config.
2. Dans la section `<rules>`, remplacez le paramètre *minilevel* par le niveau de journalisation souhaitée. Par exemple :

```
1      <rules>
2
3      <logger name="*" writeTo="file" minlevel="Debug" />
4
5      </rules>
6  <!--NeedCopy-->
```

3. Enregistrez le fichier.

   Les modifications prennent effet immédiatement. Vous n'avez pas besoin de redémarrer le connecteur pour Exchange ActiveSync.

Erreurs fréquentes

La liste suivante contient des erreurs courantes :

- Le service Endpoint Management Connector pour Exchange ActiveSync ne démarre pas

  En cas d'erreurs, consultez le fichier journal et le journal des événements Windows. Les raisons habituelles sont les suivantes :

  - Le service Endpoint Management Connector pour Exchange ActiveSync ne peut pas accéder au serveur SQL. Cela peut être dû aux problèmes suivants :

    * Le service SQL Server n'est pas exécuté.
    * Échec de l'authentification.

    Si l'authentification Windows Integrated est configurée, le compte utilisateur du service Endpoint Management Connector pour Exchange ActiveSync doit être une ouverture de session SQL autorisée. Le compte du service Endpoint Management Connector pour Exchange ActiveSync est par défaut le compte système local, mais il peut être remplacé par un autre compte disposant des privilèges d'administrateur local. Si l'authentification SQL est configurée, l'ouverture de session SQL doit être correctement configurée dans SQL.

  - Le port configuré pour le fournisseur de services mobiles (MSP) n'est pas disponible. Le port d'écoute sélectionné ne doit pas être utilisé par un autre processus du système.

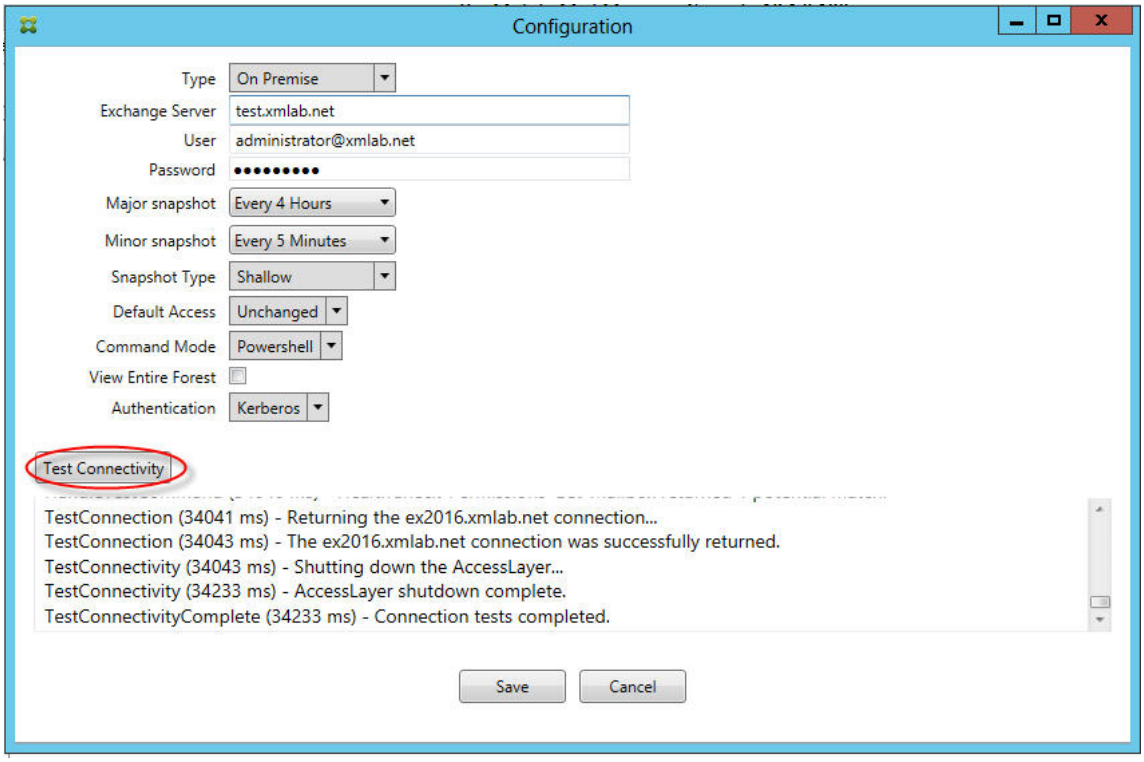
- XenMobile ne peut pas se connecter au MSP

  Vérifiez que le port du service MSP et le transport sont correctement configurés dans l'onglet **Configure > MSP** de la console Endpoint Management Connector pour Exchange ActiveSync. Vérifiez qu'un groupe ou utilisateur d'autorisations est correctement défini.

  Si le protocole HTTPS est configuré, vous devez installer un certificat de serveur SSL valide. Si IIS est installé, vous pouvez utiliser le gestionnaire IIS (Internet Information Services) pour installer le certificat. Si IIS n'est pas installé, consultez la section Procédure : Configurer un port avec un certificat SSL pour plus de détails sur l'installation des certificats.

  Endpoint Management Connector pour Exchange ActiveSync contient un utilitaire qui permet de tester la connectivité au service MSP. Exécutez le programme *DossierInstallation*\MspTestServiceClient.exe et paramétrez l'URL et les informations d'identification afin qu'elles correspondent à celles qui seront configurées dans XenMobile, puis cliquez sur **Test Connectivity**. Cela simule les requêtes de service Web que XenMobile Server émet. Notez que si le protocole HTTPS est configuré, vous devez spécifier le nom d'hôte actuelle du serveur (le nom spécifié dans le certificat SSL).

  Lors de l'utilisation de **Test Connectivity**, assurez-vous d'avoir au moins un enregistrement ActiveSyncDevice ou le test risque d'échouer.



Outils de résolution des problèmes

Des utilitaires PowerShell destinés au dépannage sont disponibles dans le dossier Support\PowerShell.

Un outil de dépannage effectue une analyse approfondie des boîtes aux lettres et appareils des utilisateurs, détecte les conditions d'erreur et les zones de défaillance potentielles, et réalise également une analyse approfondie des RBAC (contrôle d'accès basé sur un rôle) des utilisateurs. Il peut enregistrer les sorties brutes de toutes les applets de commande sur un fichier texte.

Citrix Gateway Connector pour Exchange ActiveSync

January 10, 2022

XenMobile Citrix ADC Connector est maintenant nommé Citrix Gateway Connector pour Exchange ActiveSync. Pour plus de détails sur le portefeuille unifié de Citrix, consultez le guide des produits Citrix.

Ce connecteur pour Exchange ActiveSync fournit un service d'autorisation au niveau de l'appareil des clients ActiveSync à Citrix ADC qui fait office de proxy inverse pour le protocole Exchange ActiveSync. L'autorisation est contrôlée par une combinaison de stratégies que vous définissez dans XenMobile et par des règles définies localement par Citrix Gateway Connector pour Exchange ActiveSync.

Pour de plus amples informations, consultez la section ActiveSync Gateway.

Pour un diagramme d'architecture de référence détaillé, voir Architecture.

La version actuelle de Citrix Gateway Connector pour Exchange ActiveSync est la version 8.5.2.

Nouveautés

Les sections suivantes répertorient les nouveautés des versions actuelles et antérieures de Citrix Gateway Connector pour Exchange ActiveSync, anciennement XenMobile Citrix ADC Connector.

Nouveautés dans la version 8.5.3

- Cette version ajoute la prise en charge des protocoles ActiveSync 16.0 et 16.1.
- Plus de détails ont été ajoutés aux analyses envoyées à Google Analytics, notamment concernant les instantanés. [CXM-52261]

Nouveautés dans la version 8.5.2

- XenMobile Citrix ADC Connector est maintenant nommé Citrix Gateway Connector pour Exchange ActiveSync.

Les problèmes suivants ont été résolus dans cette version :

- Si plusieurs critères sont utilisés dans la définition d'une règle de stratégie et si l'un des critères implique l'ID utilisateur, le problème suivant peut se produire. Si un utilisateur a plusieurs alias, les alias ne sont pas également vérifiés lors de l'application de la règle. [CXM-55355]

> **Remarque :**
>
> La section Nouveautés suivante fait référence à Citrix Gateway Connector pour Exchange ActiveSync sous son ancien nom XenMobile Citrix ADC Connector. Le nom a changé à partir de la version 8.5.2.

Nouveautés dans la version 8.5.1.11

- **Modification de la configuration système requise :** la version actuelle de Citrix ADC Connector requiert Microsoft .NET Framework 4.5.
- **Prise en charge de Google Analytics :** nous souhaitons savoir comment vous utilisez XenMobile Citrix ADC Connector afin de pouvoir nous concentrer sur l'amélioration du produit.
- **Prise en charge de TLS 1.1 et 1.2 :** en raison de ses risques pour la sécurité, TLS 1.0 est abandonné par le PCI Council. La prise en charge de TLS 1.1 et 1.2 est ajoutée à XenMobile Citrix ADC Connector.

Surveillance de Citrix Gateway Connector pour Exchange ActiveSync

L'utilitaire de configuration Citrix Gateway Connector pour Exchange ActiveSync offre une journalisation détaillée que vous pouvez utiliser pour afficher tout le trafic transitant par le biais de votre serveur Exchange Server qui est autorisé ou bloqué par Secure Mobile Gateway.

Utilisez l'onglet **Log** pour afficher l'historique des demandes ActiveSync transmises à Citrix ADC Connector pour Exchange ActiveSync pour autorisation.

De plus, pour vous assurer que le service Web Citrix Gateway Connector pour Exchange ActiveSync est en cours d'exécution, vous pouvez charger l'adresse URL suivante dans un navigateur sur le serveur du connecteur `https://<host:port>/services/ActiveSync/Version`. Si l'adresse URL retourne la version du produit en tant que chaîne, le service Web est réactif.

Simulation de trafic ActiveSync avec Citrix Gateway Connector pour Exchange ActiveSync

Vous pouvez utiliser Citrix Gateway Connector pour Exchange ActiveSync pour simuler le trafic ActiveSync en conjonction avec vos stratégies. Dans l'outil de configuration du connecteur, sélectionnez l'onglet **Simulator**. Les résultats vous montrent comment vos stratégies s'appliquent aux règles que vous avez configurées.

Choix des filtres pour Citrix Gateway Connector pour Exchange ActiveSync

Les filtres Citrix Gateway Connector pour Exchange ActiveSync analysent un appareil à la recherche d'une violation de stratégie ou d'un paramètre de propriété donné. Si l'appareil est conforme aux critères, l'appareil est placé dans une liste d'appareils. Cette liste d'appareils n'est ni une liste d'autorisation ni une liste de blocage. Il s'agit d'une liste d'appareils qui répondent aux critères définis. Les filtres suivants sont disponibles pour le connecteur dans XenMobile. Les deux options pour chaque filtre sont **Autoriser** ou **Refuser**.

- **Appareils anonymes :** autorise ou refuse les appareils qui sont inscrits dans XenMobile, mais l'identité de l'utilisateur est inconnue. Par exemple, ceci peut être un utilisateur qui a été inscrit, mais le mot de passe Active Directory de l'utilisateur a expiré ou un utilisateur s'est inscrit avec des informations d'identification inconnues.
- **Échec de l'attestation Samsung KNOX :** les appareils Samsung sont dotés de fonctionnalités de sécurité et de diagnostic. Ce filtre fournit la confirmation que l'appareil est configuré pour KNOX. Pour de plus amples informations, consultez la section Samsung Knox.
- **Applications sur liste noire :** autorise ou refuse les appareils en fonction de la liste des appareils définie par les stratégies de liste de blocage et la présence d'applications bloquées.
- **Autorisations et refus implicite :** crée une liste d'appareils de tous les appareils qui ne répondent pas à tous les critères de règle de filtre et les autorise ou les refuse en se basant sur cette

liste. L'option Autorisation/refus implicite garantit que l'état de Citrix Gateway Connector pour Exchange ActiveSync dans l'onglet Appareils est activé et affiche l'état du connecteur pour vos appareils. L'option Autorisation/refus implicite contrôle également tous les autres filtres du connecteur qui n'ont pas été sélectionnés. Par exemple, le connecteur refuse les applications bloquées tout en autorisant tous les autres filtres car l'option Autorisation/refus implicite est définie sur **Autoriser**.

- **Appareils inactifs :** crée une liste d'appareils des appareils qui n'ont pas communiqué avec XenMobile dans une période de temps spécifiée. Ces appareils sont considérés comme inactifs. Le filtre autorise ou refuse les appareils en conséquence.
- **Applications requises manquantes :** lorsqu'un utilisateur s'inscrit, l'utilisateur reçoit une liste des applications requises qui doivent être installées. Le filtre des applications requises manquantes indique qu'une ou plusieurs applications ne sont plus présentes ; par exemple, l'utilisateur a supprimé une ou plusieurs applications.
- **Applications non suggérées :** lorsqu'un utilisateur s'inscrit, l'utilisateur reçoit une liste des applications qu'il doit installer. Le filtre des applications non suggérées vérifie que l'appareil ne contient pas d'applications qui ne figurent pas dans cette liste.
- **Mot de passe non conforme :** crée une liste d'appareils de tous les appareils qui ne disposent pas d'un code secret sur l'appareil.
- **Appareils non conformes :** vous permet d'interdire ou d'autoriser des appareils qui répondent à vos critères de conformité informatiques internes. La conformité est un paramètre arbitraire défini par la propriété d'appareil nommée Non conforme, qui est un indicateur booléen qui peut être soit **True** soit **False**. (Vous pouvez créer cette propriété manuellement et définir sa valeur, ou vous pouvez utiliser les actions automatisées pour créer cette propriété sur un appareil si l'appareil correspond ou pas aux critères spécifiques.)
  - **Non conforme = True**. Si un appareil ne répond pas aux normes de conformité et aux définitions de stratégie définies par votre service informatique, l'appareil n'est pas conforme.
  - **Non conforme = False.** Si un appareil répond aux normes de conformité et aux définitions de stratégie définies par votre service informatique, l'appareil est conforme.
- **État révoqué :** crée une liste d'appareils de tous les appareils révoqués et les autorise ou les refuse en fonction de l'état de révocation.
- **Android rootés/iOS jailbreakés**. Crée une liste d'appareils de tous les appareils marqués comme rootés et les autorise ou les refuse en se basant sur leur état racine.
- **Appareils non gérés**. Crée une liste d'appareils de tous les appareils dans la base de données XenMobile. Mobile Application Gateway doit être déployé dans un mode Block.

Configuration d'une connexion à Citrix Gateway Connector pour Exchange ActiveSync

Citrix Gateway Connector pour Exchange ActiveSync communique avec XenMobile et d'autres fournisseurs de configuration à distance via les services Web sécurisés.

1. Dans l'outil de configuration du connecteur, cliquez sur l'onglet **Config Providers**, puis cliquez sur **Add**.
2. Dans la boîte de dialogue **Config Providers**, dans **Name**, entrez un nom d'utilisateur disposant des privilèges d'administration et qui est utilisé pour l'autorisation HTTP de base avec XenMobile Server.
3. Dans **Url**, entrez l'adresse Web du service XenMobile GCS (Gateway Configuration Service), généralement au format `https://<FQDN>/<instanceName>/services/<MagConfigService>`. Le nom *MagConfigService* est sensible à la casse.
4. Dans **Password**, saisissez le mot de passe qui sera utilisé pour l'autorisation HTTP de base avec le XenMobile Server.
5. Dans **Managing Host**, entrez le nom du serveur du connecteur.
6. Dans **Baseline Interval**, spécifiez une période de temps après laquelle un nouveau ruleset dynamique actualisé est extrait depuis Device Manager.
7. Dans **Delta interval**, spécifiez une période de temps après laquelle une mise à jour de règles dynamiques est extraite.
8. Dans **Request Timeout**, spécifiez l'intervalle d'expiration du délai de demande du serveur.
9. Dans **Config Provider**, sélectionnez si l'instance de serveur du fournisseur de configuration fournit la configuration de la stratégie.
10. Dans **Events Enabled**, activez cette option si vous souhaitez que le connecteur informe XenMobile lorsqu'un appareil est bloqué. Cette option est requise si vous utilisez les règles du connecteur dans l'une de vos actions automatisées XenMobile.
11. Cliquez sur **Save**, puis cliquez sur **Test Connectivity** pour tester la connectivité du fournisseur de configuration vers la passerelle. Si la connexion échoue, vérifiez que les paramètres du pare-feu local acceptent la connexion ou contactez votre administrateur.
12. Si la connexion réussit, désactivez la case à cocher **Disabled**, puis cliquez sur **Save**.

Lorsque vous ajoutez un nouveau fournisseur de configuration, Citrix Gateway Connector pour Exchange ActiveSync crée automatiquement une ou plusieurs stratégies associées au fournisseur. Ces stratégies sont définies par une définition de modèle contenue dans config\policyTemplates.xml de la section NewPolicyTemplate. Pour chaque élément Policy est défini dans cette section, une nouvelle stratégie est créée.

L'opérateur peut ajouter, supprimer ou modifier les éléments de stratégie si les conditions suivantes sont remplies : l'élément de stratégie est conforme à la définition du schéma et les chaînes de substitution standard (entre accolades) ne sont pas modifiées. Ajoutez ensuite de nouveaux groupes pour le fournisseur et mettez à jour la stratégie pour inclure les nouveaux groupes.

Pour importer une stratégie depuis XenMobile

1. Dans l'outil de configuration Citrix Gateway Connector pour Exchange ActiveSync, cliquez sur l'onglet **Config Providers**, puis cliquez sur **Add**.

2. Dans la boîte de dialogue **Config Providers**, dans **Name**, entrez un nom d'utilisateur qui sera utilisé pour l'autorisation HTTP de base avec XenMobile Server et disposant de privilèges d'administrateur.
3. Dans **Url**, entrez l'adresse Web du service XenMobile GCS (Gateway Configuration Service), généralement au format `https://<xdmHost>/xdm/services/<MagConfigService>`. Le nom MagConfigService est sensible à la casse.
4. Dans **Password**, saisissez le mot de passe qui est utilisé pour l'autorisation HTTP de base avec XenMobile Server.
5. Cliquez sur **Test Connectivity** pour tester la connectivité du fournisseur de configuration vers la passerelle. Si la connexion échoue, vérifiez que vos paramètres locaux de pare-feu autorisent la connexion ou contactez votre administrateur.
6. Lorsqu'une connexion est établie, désactivez la case à cocher **Disabled**, puis cliquez sur **Save**.
7. Dans **Managing Host**, laissez la valeur par défaut du nom DNS de l'ordinateur hôte. Ce paramètre est utilisé pour coordonner les communications avec XenMobile lorsque plusieurs serveurs Forefront Threat Management Gateway (TMG) sont configurés dans un tableau.

   Lorsque vous enregistrez les paramètres, ouvrez le GCS.

Configuration du mode de stratégie de Citrix Gateway Connector pour Exchange ActiveSync

Citrix Gateway Connector pour Exchange ActiveSync peut être exécuté dans les six modes suivants :

- **Allow All**. Ce mode de stratégie accorde l'accès à tout le trafic passant via le connecteur. Aucune autre règle de filtrage n'est utilisée.
- **Deny All**. Ce mode de stratégie bloque l'accès à tout le trafic passant via le connecteur. Aucune autre règle de filtrage n'est utilisée.
- **Static Rules: Block Mode**. Ce mode de stratégie exécute des règles statiques avec une instruction implicite de blocage ou de refus à la fin. Le connecteur bloque les appareils qui ne sont pas autorisés par d'autres règles de filtre.
- **Static Rules: Permit Mode**. Ce mode de stratégie exécute des règles statiques avec une instruction implicite d'acceptation ou d'autorisation à la fin. Les appareils qui ne sont pas bloqués ou refusés par d'autres règles de filtre sont autorisés via le connecteur.
- **Static + ZDM Rule**s: Block Mode. Ce mode de stratégie exécute tout d'abord des règles statiques, suivies par des règles dynamiques depuis XenMobile avec une instruction implicite de blocage ou de refus à la fin. Les appareils sont autorisés ou refusés en se basant sur des filtres définis et des règles Device Manager. Tous les appareils qui ne correspondent pas à des filtres et des règles définis sont bloqués.

- **Static + ZDM Rule**s: Permit Mode. Ce mode de stratégie exécute tout d'abord des règles statiques, suivies par des règles dynamiques depuis XenMobile avec une instruction implicite d'acceptation ou d'autorisation à la fin. Les appareils sont autorisés ou refusés en se basant sur des filtres définis et des règles XenMobile. Tous les appareils qui ne correspondent pas à des filtres et des règles définis sont autorisés.

Le processus Citrix Gateway Connector pour Exchange ActiveSync autorise ou bloque les règles dynamiques en se basant sur des ID ActiveSync uniques pour appareils mobiles iOS et Windows reçus de XenMobile. Les appareils Android changent de comportement en fonction du fabricant et certains n'exposent pas directement d'ID unique ActiveSync. Pour compenser, XenMobile envoie les informations d'ID de l'utilisateur pour les appareils Android pour effectuer une décision d'autorisation ou de blocage. Par conséquent, si un utilisateur possède un seul appareil Android, la fonctionnalité d'autorisation et de blocage fonctionne normalement. Si l'utilisateur possède plusieurs appareils Android, tous les appareils sont autorisés, car les appareils Android ne peuvent pas être différenciés. Vous pouvez configurer la passerelle pour bloquer de façon statique ces appareils par ActiveSyncID, s'ils sont connus. Vous pouvez également configurer la passerelle pour qu'elle effectue un blocage en fonction de l'agent utilisateur ou du type d'appareil.

Pour spécifier le mode de stratégie, dans l'outil SMG Controller Configuration, procédez comme suit :

1. Cliquez sur l'onglet **Path Filters**, puis cliquez sur **Add**.
2. Dans la boîte de dialogue **Path Properties**, sélectionnez un mode de stratégie à partir de la liste **Policy**, puis cliquez sur **Save**.

Vous pouvez vérifier les règles sur l'onglet **Policies** de l'outil de configuration. Les règles sont traitées de haut en bas sur Citrix Gateway Connector pour Exchange ActiveSync. Les stratégies autorisées sont affichées avec une coche verte. Les stratégies refusées s'affichent un cercle rouge traversé d'une ligne. Pour actualiser l'écran et afficher les règles mises à jour le plus récemment, cliquez sur **Refresh**. Vous pouvez également modifier l'ordre des règles dans le fichier config.xml.

Pour tester les règles, cliquez sur l'onglet **Simulator**. Spécifiez des valeurs dans les champs. Elles peuvent également être obtenues à partir des journaux. Un message de résultat apparaît spécifiant Allow ou Block.

Pour configurer des règles statiques

Entrez des règles statiques avec les valeurs qui sont lues par le filtrage ISAPI des lectures de demandes HTTP de connexion ActiveSync. Les règles statiques permettent à Citrix Gateway Connector pour Exchange ActiveSync d'autoriser ou de bloquer le trafic en fonction des critères suivants :

- **Utilisateur**. Citrix Gateway Connector pour Exchange ActiveSync utilise la valeur de l'utilisateur autorisé et la structure de nom qui a été capturée lors de l'inscription de l'appareil. Ceci est couramment détecté en tant que domaine\nomutilisateur comme référencé par le serveur qui

exécute XenMobile connecté à Active Directory via LDAP. L'onglet **Log** de l'outil de configuration du connecteur affiche les valeurs qui sont transmises via le connecteur. Les valeurs sont transmises si la structure de valeur doit être déterminée ou est différente.

- **Deviceid (ActiveSyncID)**. Également appelée ActiveSyncID de l'appareil connecté. Cette valeur est généralement présente dans la page de propriétés spécifiques de l'appareil dans la console XenMobile. Cette valeur peut également être vue depuis l'onglet Log de l'outil de configuration du connecteur.
- **DeviceType**. Le connecteur peut déterminer si un appareil est un iPhone, un iPad ou tout autre type d'appareil et peut l'autoriser ou le bloquer en fonction de ces critères. Comme avec d'autres valeurs, l'outil de configuration du connecteur peut révéler tous les types d'appareils connectés en cours de traitement pour la connexion ActiveSync.
- **UserAgent**. Contient des informations sur le client ActiveSync utilisé. Dans la plupart des cas, la valeur spécifiée correspond à une version spécifique d'un système d'exploitation et à la version de plate-forme de l'appareil mobile.

L'outil de configuration du connecteur en cours d'exécution sur le serveur gère toujours les règles statiques.

1. Dans l'utilitaire SMG Controller Configuration, cliquez sur l'onglet **Static Rules**, puis cliquez sur **Add**.
2. Dans la boîte de dialogue **Static Rule Properties**, spécifiez les valeurs que vous voulez utiliser en tant que critères. Par exemple, vous pouvez entrer un utilisateur pour autoriser l'accès en entrant le nom d'utilisateur (par exemple, AllowedUser), puis désactiver la case à cocher **Disabled**.
3. Cliquez sur **Enregistrer**.

   La règle statique est maintenant effective. Par ailleurs, vous pouvez utiliser des expressions régulières pour définir des valeurs, mais vous devez activer le mode de traitement de la règle dans le fichier config.xml.

Pour configurer les règles dynamiques

Les stratégies et les propriétés d'appareils dans XenMobile définissent les règles dynamiques et peuvent déclencher un filtre Citrix Gateway Connector pour Exchange ActiveSync dynamique. Les déclencheurs sont basés sur la présence d'une violation de stratégie ou d'un paramètre de propriété. Les filtres du connecteur analysent un appareil à la recherche d'une violation de stratégie ou d'un paramètre de propriété donné. Si l'appareil est conforme aux critères, l'appareil est placé dans une liste d'appareils. Cette liste d'appareils n'est ni une liste d'autorisation ni une liste de blocage. Il s'agit d'une liste d'appareils qui satisfait au critère défini. Les options de configuration suivantes vous permettent de définir si vous souhaitez autoriser ou refuser les appareils dans la liste d'appareils en utilisant le connecteur.

> **Remarque :**
>
> Vous devez utiliser la console XenMobile pour configurer les règles dynamiques.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Serveur**, cliquez sur **ActiveSync Gateway**. La page ActiveSync Gateway s'affiche.
3. Dans **Activer la ou les règles suivantes**, sélectionnez une ou plusieurs règles à activer.
4. Dans Android uniquement, dans **Envoyer les utilisateurs de domaine Android vers ActiveSync Gateway**, cliquez sur **Oui** pour vous assurer que XenMobile envoie les informations de l'appareil Android à Secure Mobile Gateway.

   Lorsque cette option est activée, XenMobile envoie les informations de l'appareil Android à Citrix Gateway Connector pour Exchange ActiveSync lorsqu'il ne dispose pas de l'identificateur ActiveSync de l'utilisateur de l'appareil Android.

Pour configurer des stratégies personnalisées en modifiant le fichier XML de Citrix Gateway Connector pour Exchange ActiveSync

Vous pouvez afficher les stratégies de base dans la configuration par défaut sur l'onglet **Policies** de l'outil de configuration Citrix Gateway Connector pour Exchange ActiveSync. Si vous souhaitez créer des stratégies personnalisées, vous pouvez modifier le fichier de configuration XML du connecteur (config\config.xml).

1. Recherchez la section **PolicyList** dans le fichier, puis ajoutez un nouvel élément **Policy**.
2. Si un nouveau groupe est également requis, tel qu'un groupe statique ou un groupe pour prendre en charge un autre GCP, ajoutez le nouvel élément **Group** à la section **GroupList**.
3. Si vous le souhaitez, vous pouvez modifier l'ordre des groupes dans une stratégie existante en réorganisant les éléments **GroupRef**.

Configuration du fichier XML de Citrix Gateway Connector pour Exchange ActiveSync

Citrix Gateway Connector pour Exchange ActiveSync utilise un fichier de configuration XML pour déterminer les actions du connecteur. Entre autres entrées, le fichier spécifie les fichiers du groupe et les actions associées que le filtre effectue lors de l'évaluation des requêtes HTTP. Par défaut, le fichier est appelé config.xml et est situé à l'emplacement suivant : ..\Program Files\Citrix\XenMobile Citrix ADC Connector\config.

Nœuds GroupRef

Les nœuds GroupRef définissent les noms des groupes logiques. Les valeurs par défaut sont AllowGroup et DenyGroup.

> **Remarque :**
>
> L'ordre des nœuds GroupRef tels qu'ils apparaissent dans le nœud GroupRefList est significatif.

La valeur de l'ID d'un nœud GroupRef identifie un conteneur logique ou une collection de membres qui sont utilisés pour la mise en correspondance des comptes d'utilisateurs ou d'appareils spécifiques. Les attributs d'action spécifient la façon dont le filtre traite un membre qui correspond à une règle dans la collection. Par exemple, un compte d'utilisateur ou un appareil qui correspond à une règle dans l'ensemble AllowGroup sera « pass. » « pass » signifie qu'il est autorisé à accéder à Exchange CAS. Un compte d'utilisateur ou un appareil qui correspond à une règle dans l'ensemble DenyGroup est « rejected. » « rejected » signifie qu'il n'est pas autorisé à accéder à Exchange CAS.

Lorsqu'un compte utilisateur/appareil particulier ou une combinaison des deux répond aux règles dans les deux groupes, une convention de priorité est utilisée pour diriger le résultat de la requête. La priorité est incorporée dans l'ordre des nœuds GroupRef dans le fichier config.xml de haut en bas. Les nœuds GroupRef sont classés par ordre de priorité. Les règles pour une condition donnée dans le groupe Allow seront toujours prioritaires sur les règles de la même condition du groupe Deny.

Nœuds de groupe

De plus, le fichier config.xml définit les nœuds Groupe. Ces nœuds fournissent une liaison entre les conteneurs logiques AllowGroup et DenyGroup vers les fichiers XML externes. Les entrées stockées dans les fichiers externes forment la base des règles de filtre.

> **Remarque :**
>
> Dans cette version, seuls les fichiers XML externes sont pris en charge.

L'installation par défaut implémente deux fichiers XML de configuration : allow.xml et deny.xml.

Configuration de Citrix Gateway Connector pour Exchange ActiveSync

Vous pouvez configurer Citrix Gateway Connector pour Exchange ActiveSync pour bloquer ou autoriser les demandes ActiveSync de manière sélective en vous basant sur les propriétés suivantes : **Active Sync Service ID**, **Device type**, **User Agent** (système d'exploitation de l'appareil), **Authorized user** et **ActiveSync Command**.

La configuration par défaut prend en charge une combinaison de groupes statiques et dynamiques. Vous pouvez gérer les groupes statiques à l'aide de l'utilitaire de configuration SMG Controller. Les groupes statiques peuvent être composés de catégories d'appareils connues, telles que les appareils utilisant un agent utilisateur donné.

Une source externe appelée fournisseur de configuration de passerelle gère les groupes dynamiques. Citrix Gateway Connector pour Exchange ActiveSync connecte les groupes régulièrement. XenMobile peut exporter des groupes d'appareils et d'utilisateurs autorisés et bloqués vers le connecteur.

Les groupes dynamiques sont gérés par une source externe appelée Gateway Configuration Provider et sont régulièrement collectés par Citrix Gateway Connector pour Exchange ActiveSync. XenMobile peut exporter des groupes d'appareils et d'utilisateurs autorisés et bloqués vers le connecteur.

Une stratégie est une liste ordonnée de groupes dans laquelle chaque groupe est associé à une action (autoriser ou bloquer) et une liste des membres du groupe. Une stratégie peut contenir n'importe quel nombre de groupes. L'ordre du groupe dans une stratégie est important car lorsqu'une correspondance est localisée, l'action du groupe est prise, et les autres groupes ne sont pas évalués.

Un membre définit une façon de faire correspondre les propriétés d'une demande. Il peut correspondre à une seule propriété, telle que l'ID d'appareil ou plusieurs propriétés, telles que le type d'appareil et l'agent utilisateur.

Choix d'un modèle de sécurité pour Citrix Gateway Connector pour Exchange ActiveSync

L'établissement d'un modèle de sécurité est nécessaire au succès d'un déploiement d'appareils mobiles pour les organisations de toutes tailles. Il est courant d'utiliser un contrôle de réseau protégé ou en quarantaine pour autoriser l'accès à un utilisateur, un ordinateur ou un appareil par défaut. Cette pratique n'est pas toujours idéale. Chaque organisation qui gère la sécurité informatique peut avoir une approche légèrement différente ou adaptée à la sécurité pour les appareils mobiles.

La même logique s'applique à la sécurité des appareils mobiles. Un modèle permissif est un choix inadapté étant donné le grand nombre de types et d'appareils mobiles, d'appareils mobiles par utilisateur et de plates-formes de systèmes d'exploitation et d'applications disponibles. Dans la plupart des organisations, le modèle restrictif sera le choix le plus logique.

Les scénarios de configuration que Citrix autorise pour l'intégration de Citrix Gateway Connector pour Exchange ActiveSync avec XenMobile sont les suivants :

Modèle permissif (Permit Mode)

Le modèle de sécurité permissif fonctionne sur le principe que l'accès est autorisé par défaut. Un blocage et une restriction seront appliqués uniquement via des règles et un filtrage. Le modèle de sécurité permissif est adapté aux organisations dans lesquelles la sécurité n'est pas une préoccupation principale pour les appareils mobiles. Le modèle applique uniquement des contrôles restrictifs pour refuser l'accès lorsque cela est approprié (lorsqu'une règle de stratégie a échoué).

Modèle restrictif (Block Mode)

Le modèle de sécurité restrictif est basé sur le principe que l'accès n'est pas autorisé par défaut. Tout le contenu transitant par le point de vérification est filtré et inspecté, et l'accès est refusé, sauf si les

règles autorisant l'accès sont satisfaites. Le modèle de sécurité restrictif est adapté aux organisations qui possèdent des mesures de sécurité relativement strictes pour les appareils mobiles. Le mode accorde seulement l'accès (à des fins d'utilisation et aux fonctionnalités) aux services réseau lorsque toutes les règles autorisant l'accès sont observées.

Gestion de Citrix Gateway Connector pour Exchange ActiveSync

Vous pouvez utiliser Citrix Gateway Connector pour Exchange ActiveSync pour créer des règles de contrôle d'accès. Les règles autorisent ou bloquent l'accès aux demandes de connexion ActiveSync des appareils gérés. L'accès dépend de l'état de l'appareil, des listes d'autorisation ou de blocage et d'autres critères de conformité.

À l'aide de l'outil de configuration Citrix Gateway Connector pour Exchange ActiveSync, vous pouvez créer des règles dynamiques et statiques qui appliquent des stratégies de messagerie d'entreprise, ce qui vous permet de bloquer les utilisateurs qui ne respectent pas ces règles. Vous pouvez également configurer le cryptage des pièces jointes aux e-mails, de sorte que toutes les pièces jointes qui sont transmises par le biais de votre serveur Exchange vers les appareils gérés sont cryptées et uniquement disponibles sur les appareils gérés par des utilisateurs autorisés.

Désinstallation de Citrix Gateway Connector pour Exchange ActiveSync

1. Exécutez XncInstaller.exe avec un compte d'administrateur.
2. Suivez les instructions à l'écran pour procéder à la désinstallation.

Installation, mise à niveau ou désinstallation de Citrix Gateway Connector pour Exchange ActiveSync

1. Exécutez XncInstaller.exe avec un compte administrateur pour installer le connecteur ou autoriser la mise à niveau ou la suppression d'un connecteur existant.
2. Suivez les instructions à l'écran pour procéder à l'installation, la mise à niveau ou la désinstallation.

Après avoir installé le connecteur, vous devez redémarrer manuellement le service de configuration et le service de notification de XenMobile.

Installation de Citrix Gateway Connector pour Exchange ActiveSync

Vous installez Citrix Gateway Connector pour Exchange ActiveSync sur son propre serveur Windows.

La charge d'UC que le connecteur place sur un serveur dépend du nombre d'appareils gérés. Pour un grand nombre d'appareils (plus de 50 000), il se peut que vous deviez provisionner plus d'un noyau si

vous ne disposez pas d'un environnement en cluster. L'encombrement mémoire du connecteur n'est pas assez important pour justifier plus de mémoire.

Configuration système requise pour Citrix Gateway Connector pour Exchange ActiveSync

Citrix Gateway Connector pour Exchange ActiveSync communique avec Citrix ADC sur un pont SSL configuré sur l'appliance Citrix ADC. La passerelle permet à l'appliance d'acheminer tout le trafic sécurisé directement vers XenMobile. Le connecteur requiert la configuration système minimale suivante :

Composant	Exigences
Ordinateur et processeur	733 MHz Pentium III 733 MHz ou processeur supérieur. 2.0 GHz Pentium III ou processeur supérieur (recommandé)
Citrix ADC	Appliance Citrix ADC avec version du logiciel 10
Mémoire	1 Go
Disque dur	Partition locale au format NTFS avec 150 Mo d'espace disque dur disponible
OS	Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2008 R2 Service Pack 1. Doit être un serveur en anglais. La prise en charge de Windows Server 2008 R2 Service Pack 1 prend fin le 14 janvier 2020.
Autres périphériques	Carte réseau compatible avec le système d'exploitation hôte pour les communications avec le réseau interne.
Microsoft .NET Framework	La version 8.5.1.11 requiert Microsoft .NET Framework 4.5.
Afficher	Moniteur VGA ou de plus haute résolution

L'ordinateur hôte pour Citrix Gateway Connector pour Exchange ActiveSync requiert l'espace disque disponible suivant :

- **Application :** 10 -15 Mo (100 Mo recommandés)
- **Logging.** 1 Go (20 Go recommandés)

Pour de plus amples informations sur les plates-formes prises en charge pour Citrix Gateway Connector pour Exchange ActiveSync, consultez Systèmes d'exploitation d'appareils pris en charge.

Clients de messagerie d'appareil

Les clients de messagerie ne renvoient pas tous le même ID ActiveSync pour un appareil. Étant donné que Citrix Gateway Connector pour Exchange ActiveSync s'attend à un ID ActiveSync unique pour chaque appareil, seuls les clients de messagerie qui génèrent toujours le même ID ActiveSync unique pour chaque appareil sont pris en charge. Citrix a testé ces clients de messagerie et aucune erreur n'a été détectée :

- Client de messagerie natif Samsung
- Client de messagerie natif iOS

Déploiement de Citrix Gateway Connector pour Exchange ActiveSync

Citrix Gateway Connector pour Exchange ActiveSync vous permet d'utiliser Citrix ADC pour servir de proxy et équilibrer la charge des communications du XenMobile Server avec les appareils gérés XenMobile. Le connecteur communique périodiquement avec XenMobile pour synchroniser les stratégies. Le connecteur et XenMobile peuvent être en cluster, ensemble ou indépendamment, et leur charge peut être équilibrée par Citrix ADC.

Composants de Citrix Gateway Connector pour Exchange ActiveSync

- **Service Citrix Gateway Connector pour Exchange ActiveSync :** ce service offre une interface de service Web REST pouvant être invoquée par Citrix ADC pour déterminer si une demande ActiveSync provenant d'un appareil est autorisée.
- **Service de configuration XenMobile :** ce service communique avec XenMobile pour synchroniser les modifications apportées aux stratégies XenMobile avec le connecteur.
- **Service de notification XenMobile :** ce service envoie des notifications d'accès non autorisé à XenMobile. De cette façon, XenMobile peut prendre les mesures appropriées, envoyer à l'utilisateur une notification expliquant pourquoi l'appareil a été bloqué par exemple.
- **Outil de configuration de Citrix Gateway Connector pour Exchange ActiveSync :** cette application permet à l'administrateur de configurer et de surveiller le connecteur.

Configuration d'adresses d'écoute pour Citrix Gateway Connector pour Exchange ActiveSync

Pour que Citrix Gateway Connector pour Exchange ActiveSync reçoive des demandes de Citrix ADC pour autoriser le trafic ActiveSync, procédez comme suit. Indiquez le port sur lequel le connecteur écoute les appels de service Citrix ADC.

1. Dans le menu **Démarrer**, sélectionnez l'outil de configuration Citrix Gateway Connector pour Exchange ActiveSync.

2. Cliquez sur l'onglet **Web Service**, puis entrez les adresses d'écoute pour le service Web du connecteur. Vous pouvez sélectionner le protocole **HTTP** et/ou **HTTPS**. Si le connecteur est co-résident avec XenMobile (installé sur le même serveur), sélectionnez les valeurs de port qui ne sont pas en conflit avec XenMobile.
3. Une fois les valeurs configurées, cliquez sur **Save**, puis sur **Start Service** pour démarrer le service Web.

Configuration de stratégies de contrôle d'accès à l'appareil dans Citrix Gateway Connector pour Exchange ActiveSync

Pour configurer la stratégie de contrôle d'accès que vous souhaitez appliquer à vos appareils gérés, effectuez les opérations suivantes :

1. Dans l'outil de configuration Citrix Gateway Connector pour Exchange ActiveSync, cliquez sur l'onglet **Path Filters**.
2. Sélectionnez la première ligne, **Microsoft-Server-ActiveSync is for ActiveSync**, puis cliquez sur **Edit**.
3. À partir de la liste **Policy**, sélectionnez la stratégie désirée. Pour une stratégie qui comprend des stratégies XenMobile, sélectionnez **Static + ZDM: Permit Mode ou Static + ZDM: Block Mode**. Ces stratégies combinent des règles locales (ou statiques) avec les règles de XenMobile. Permit Mode signifie que tous les appareils non identifiés de manière explicite par les règles sont autorisés à accéder à ActiveSync. Block Mode signifie que de tels appareils sont bloqués.
4. Après avoir défini les stratégies, cliquez sur **Save**.

Pour configurer les communications avec XenMobile

Spécifiez le nom et les propriétés du XenMobile Server (également appelé fournisseur de configuration) que vous souhaitez utiliser avec Citrix Gateway Connector pour Exchange ActiveSync et Citrix ADC.

> **Remarque :**
>
> Cette tâche suppose que vous avez déjà installé et configuré XenMobile.

1. Dans l'outil de configuration Citrix Gateway Connector pour Exchange ActiveSync, cliquez sur l'onglet **Config Providers**, puis cliquez sur **Add**.
2. Entrez le nom et l'URL de XenMobile Server que vous utilisez pour ce déploiement. Si vous disposez de plusieurs serveurs XenMobile déployés dans un déploiement multi-locataire, ce nom doit être unique pour chaque instance de serveur. Par exemple, pour le champ **Nom**, vous pouvez entrer **XMS**.
3. Dans **Url**, entrez l'adresse Web du service XenMobile GCS (Gateway Configuration Service), généralement au format `https://<FQDN>/<instanceName>/services/<MagConfigService`

>. Le nom *MagConfigService* est sensible à la casse.

4. Dans **Password**, saisissez le mot de passe qui sera utilisé pour l'autorisation HTTP de base avec le serveur Web XenMobile.
5. Dans **Managing Host**, entrez le nom du serveur sur lequel vous avez installé Citrix Gateway Connector pour Exchange ActiveSync.
6. Dans **Baseline Interval**, spécifiez une période de temps après laquelle un nouveau ruleset dynamique actualisé est extrait depuis XenMobile.
7. Dans **Request Timeout**, spécifiez l'intervalle d'expiration du délai de demande du serveur.
8. Dans **Config Provider**, sélectionnez si l'instance de serveur du fournisseur de configuration fournit la configuration de la stratégie.
9. Dans **Events Enabled**, activez cette option si vous souhaitez que Secure Mobile Gateway informe XenMobile lorsqu'un appareil est bloqué. Cette option est requise si vous utilisez les règles Secure Mobile Gateway dans l'une des actions automatisées de votre Device Manager.
10. Une fois que le serveur est configuré, cliquez sur **Test Connectivity** pour tester la connexion à XenMobile.
11. Lorsque la connexion est établie, cliquez sur **Save**.

Déploiement de Citrix Gateway Connector pour Exchange ActiveSync pour la redondance et la capacité à monter en charge

Si vous voulez étendre votre déploiement Citrix Gateway Connector pour Exchange ActiveSync et XenMobile, vous pouvez installer des instances du connecteur sur plusieurs serveurs Windows, et les faire pointer vers la même instance de XenMobile, puis utiliser Citrix ADC pour équilibrer la charge des serveurs.

Il existe deux modes de configuration de Citrix Gateway Connector pour Exchange ActiveSync :

- En mode non partagé, chaque instance de Citrix Gateway Connector pour Exchange ActiveSync communique avec un XenMobile Server et conserve sa propre copie privée de la stratégie résultante. Par exemple, si vous possédez un cluster de XenMobile Server, vous pouvez exécuter une instance du connecteur sur chaque XenMobile Server et le connecteur obtiendra des stratégies depuis l'instance locale de XenMobile.
- En mode partagé, un nœud du connecteur est désigné comme nœud principal et il communique avec XenMobile. La configuration résultante est partagée entre les autres nœuds soit par un partage réseau Windows soit par une réplication Windows (ou tierce).

La totalité de la configuration du connecteur se trouve dans un dossier unique (composé de plusieurs fichiers XML). Le processus du connecteur détecte les modifications apportées à tout fichier dans ce dossier et recharge automatiquement la configuration. Il n'y a pas de basculement du nœud principal en mode partagé. Toutefois, le système peut tolérer le fait que le serveur principal soit arrêté pendant quelques minutes (par exemple, pour redémarrer), car la dernière configuration correcte connue est mise en cache dans le processus du connecteur.

Concepts avancés

January 10, 2022

> **Remarque :**
>
> Cet article traite des concepts avancés pour XenMobile Server. Pour plus d'informations sur Endpoint Management, consultez la section Concepts avancés.

Les articles Concepts avancés de XenMobile offrent une analyse approfondie de la documentation produit sur XenMobile. L'objectif est de réduire les temps de déploiement via des techniques proposées par des experts. Ces articles peuvent citer l'expert technique qui a rédigé le contenu.

Pour obtenir des points de décision et des conseils, accéder aux questions fréquemment posées et à des cas d'utilisation relatifs à votre environnement XenMobile, consultez le Manuel de déploiement de XenMobile dans cette section.

Vous trouverez les forums de support de la communauté XenMobile dans Citrix Discussions.

Interaction de XenMobile sur site avec Active Directory

January 10, 2022

Contribution de Siddartha Vuppala

Cet article décrit l'interaction entre XenMobile Server et Active Directory. XenMobile Server interagit avec Active Directory à la fois en ligne et en arrière-plan. Les sections suivantes fournissent plus d'informations sur les opérations en ligne et en arrière-plan qui impliquent une interaction avec Active Directory.

> **Remarque :**
>
> Cet article est une vue d'ensemble de l'interaction et ne couvre pas tous les détails. Pour plus d'informations sur la configuration d'Active Directory et de LDAP dans la console XenMobile, consultez Authentification domaine ou domaine + jeton de sécurité.

Interactions en ligne

XenMobile Server communique avec Active Directory à l'aide des paramètres LDAP configurés par un administrateur. Les paramètres récupèrent les informations sur les utilisateurs et les groupes. Vous trouverez ci-après les opérations résultant de l'interaction entre XenMobile Server et Active Directory.

1. **Configuration LDAP.** La configuration d'Active Directory entraîne une interaction avec Active Directory. XenMobile Server tente de valider les informations en authentifiant les informations

auprès d'Active Directory. Pour ce faire, le serveur utilise le protocole Internet, le port et les informations d'identification du compte de service fournis. Une liaison réussie indique que la connexion est correctement configurée.

2. **Interactions basées sur des groupes.**

   a) Recherchez un ou plusieurs groupes lors de la création de la définition du contrôle d'accès basé sur rôle (RBAC) et de groupes de distribution. L'administrateur de XenMobile Server entre une chaîne à rechercher dans la console XenMobile. XenMobile Server recherche dans le domaine sélectionné tous les groupes qui contiennent la sous-chaîne fournie. Ensuite, XenMobile Server récupère les attributs objectGUID, sAMAccountName et de nom unique des groupes identifiés dans la recherche.

   > **Remarque :**
   >
   > Ces informations ne sont pas stockées dans la base de données de XenMobile Server.

   b) Ajout ou mise à jour de la définition du groupe de déploiement et de RBAC. L'administrateur de XenMobile Server sélectionne les groupes Active Directory d'intérêt en fonction de la recherche précédente et les inclut dans la définition du groupe de déploiement. XenMobile Server recherche le groupe spécifique, un à la fois, dans Active Directory. XenMobile Server recherche l'attribut objectGUID et récupère les attributs sélectionnés, y compris les informations d'appartenance. Les informations d'appartenance à un groupe vous permettent de déterminer l'appartenance entre le groupe récupéré et les utilisateurs ou groupes existants dans la base de données de XenMobile Server. Les modifications apportées à l'appartenance à un groupe entraînent la dérivation de groupe de déploiement et RBAC pour les membres utilisateurs affectés, qui se traduit par des droits d'utilisateurs.

   > **Remarque :**
   >
   > Les modifications apportées à la définition du groupe de déploiement peuvent entraîner des modifications dans les droits des applications ou des stratégies pour les utilisateurs affectés.

   c) **Invitations avec code PIN à usage unique (OTP)**. L'administrateur de XenMobile Server sélectionne un groupe dans la liste des groupes Active Directory présents dans la base de données de XenMobile Server. Pour ce groupe, tous les utilisateurs, directs et indirects, sont extraits d'Active Directory. Les invitations avec code PIN à usage unique (OTP) sont envoyées aux utilisateurs qui ont été identifiés à l'étape précédente.

   > **Remarque :**
   >
   > Les trois interactions précédentes impliquent que les interactions basées sur des groupes sont déclenchées en fonction des modifications apportées à la config-

> uration de XenMobile Server. Lorsqu'aucune modification n'est apportée à la configuration, les interactions impliquent qu'il n'y a aucune interaction avec Active Directory. Elles supposent également qu'il n'est pas nécessaire pour les tâches en arrière-plan de capturer les modifications du côté du groupe de façon périodique.

3. **Interaction basée sur l'utilisateur.**

   a) L'authentification utilisateur. Le workflow d'authentification utilisateur implique deux interactions avec Active Directory :

      - Utilisé pour authentifier l'utilisateur avec les informations d'identification fournies.
      - Ajouter ou mettre à jour les attributs utilisateur sur la base de données de XenMobile Server, y compris objectGUID, sAMAccountName, le nom unique et l'appartenance directe aux groupes. Les modifications apportées à l'appartenance au groupe entraînent la réévaluation des droits des applications, des stratégies et d'accès.

      L'utilisateur peut s'authentifier à partir du périphérique ou de la console XenMobile Server. Dans les deux cas, l'interaction avec Active Directory respecte le même comportement.

   b) Accès et actualisation de l'App Store. Une actualisation du magasin entraîne une actualisation des attributs utilisateur, y compris les appartenances directes à des groupes. Cette action permet de réévaluer les droits des utilisateurs.

   c) Archivages de périphérique. Les administrateurs peuvent configurer des archivages de périphérique de manière périodique dans la console XenMobile. Chaque fois qu'un périphérique est archivé, les attributs utilisateur correspondants sont actualisés, y compris les appartenances directes aux groupes. Ces archivages permettent de réévaluer les droits des utilisateurs.

   d) Invitations OTP par groupe. L'administrateur de XenMobile Server sélectionne un groupe dans la liste des groupes Active Directory présents dans la base de données de XenMobile Server. Les membres utilisateurs, directs et indirects (en raison de l'imbrication), sont extraits d'Active Directory et enregistrés dans la base de données de XenMobile Server. Les invitations avec code PIN à usage unique (OTP) sont envoyées aux membres utilisateurs identifiés à l'étape précédente.

   e) Invitations OTP par utilisateur. L'administrateur entre une chaîne à rechercher dans la console XenMobile. XenMobile Server interroge Active Directory et renvoie les enregistrements utilisateur qui correspondent à la chaîne de texte. L'administrateur sélectionne ensuite l'utilisateur auquel envoyer l'invitation OTP. XenMobile Server récupère les informations utilisateur à partir d'Active Directory et met à jour les mêmes détails dans la base de données avant d'envoyer l'invitation à l'utilisateur.

Interactions en arrière-plan

Une des conclusions à tirer de la communication en ligne avec Active Directory est que les interactions basées sur des groupes sont déclenchées suite à des modifications apportées à la configuration de XenMobile Server. Lorsqu'aucune modification n'est apportée à la configuration, cela signifie qu'il n'existe aucune interaction avec Active Directory pour les groupes.

Cette interaction requiert des tâches en arrière-plan qui se synchronisent régulièrement avec Active Directory et mettent à jour les modifications pertinentes sur les groupes intéressés.

Vous trouverez ci-après les tâches en arrière-plan qui interagissent avec Active Directory.

1. **Tâche de synchronisation de groupe**. Cette tâche vise à interroger Active Directory, un seul groupe à la fois, à propos des groupes intéressés afin d'identifier les modifications apportées aux attributs sAMAccountName et de nom unique. La requête de recherche dans Active Directory utilise l'attribut objectGUID du groupe intéressé pour obtenir les valeurs actuelles des attributs de nom unique et sAMAccountName. Les modifications apportées aux valeurs de nom unique ou sAMAccountName pour les groupes intéressés sont mises à jour sur la base de données.

   > **Remarque :**
   >
   > Cette tâche n'actualise pas les informations d'appartenance d'utilisateurs à des groupes.

2. **Tâche de synchronisation de groupes imbriqués**. Cette tâche met à jour les modifications dans la hiérarchie imbriquée des groupes intéressés. XenMobile Server permet à la fois aux membres directs et indirects d'un groupe intéressé d'obtenir les droits. L'appartenance directe des utilisateurs est mise à jour lors des interactions en ligne des utilisateurs. Cette tâche, exécutée en arrière-plan, effectue le suivi des appartenances indirectes. Les appartenances indirectes correspondent à un utilisateur qui est membre d'un groupe qui est lui-même membre d'un groupe intéressé.

   Cette tâche recueille la liste des groupes Active Directory de la base de données de XenMobile Server. Ces groupes font partie de la définition du groupe déploiement ou de RBAC. Pour chaque groupe dans cette liste, XenMobile Server obtient les membres du groupe. Les membres d'un groupe sont une liste de noms uniques qui représentent à la fois des utilisateurs et des groupes. XenMobile Server interroge de nouveau Active Directory pour obtenir uniquement les membres utilisateurs du groupe intéressé. La différence entre les deux listes donne uniquement les membres du groupe pour le groupe intéressé. Les modifications apportées aux groupes de membres sont mises à jour sur la base de données. Le même processus est répété pour tous les groupes dans la hiérarchie.

   Les modifications apportées à l'imbrication entraînent le traitement des utilisateurs affectés pour les modifications de droits.

3. **Vérification des utilisateurs désactivés**. Cette tâche est exécutée uniquement lorsque

l'administrateur XenMobile crée une action afin de vérifier les utilisateurs désactivés. La tâche s'exécute dans le cadre d'une tâche de synchronisation de groupe. La tâche interroge Active Directory pour vérifier l'état désactivé des utilisateurs intéressés, un seul utilisateur à la fois.

Questions fréquentes

Quelle est la fréquence d'exécution par défaut des tâches en arrière-plan ?

- Les tâches de synchronisation de groupes s'exécutent toutes les cinq heures et commencent à 02:00 heure locale.
- Les tâches de synchronisation de groupes imbriqués s'exécutent une fois par jour à minuit heure locale.

Pourquoi une tâche de synchronisation de groupe est-elle nécessaire ?

- L'attribut memberOf d'un enregistrement utilisateur dans Active Directory fournit la liste des groupes auxquels l'utilisateur est un membre direct. Si un groupe est déplacé d'une unité d'organisation à une autre, l'attribut memberOf reflète la dernière valeur du nom unique. La base de données de XenMobile Server utilise également la dernière valeur actualisée. S'il existe des différences dans les noms uniques du groupe, les utilisateurs peuvent perdre l'accès au groupe de déploiement. Les utilisateurs peuvent également perdre les applications et les stratégies associées à ce groupe de déploiement.
- La tâche d'arrière-plan conserve l'attribut de nom unique du groupe à jour dans la base de données de XenMobile Server pour s'assurer que les utilisateurs ont accès à leurs droits.
- Les tâches de synchronisation sont planifiées toutes les cinq heures parce qu'il est supposé que les modifications de groupes dans Active Directory sont rares.

Est-il possible de désactiver une tâche de synchronisation de groupe ?

- Vous pouvez désactiver les tâches lorsque vous savez que les groupes intéressés ne sont pas modifiés pas d'une unité d'organisation à l'autre.

Pourquoi une tâche en arrière-plan de traitement d'un groupe imbriqué est-elle nécessaire ?

- Les modifications apportées aux groupes imbriqués dans Active Directory ne sont pas effectuées quotidiennement. Les modifications de la hiérarchie d'imbrication de groupes intéressés entraînent des modifications des droits des utilisateurs concernés. Lorsqu'un groupe est ajouté à la hiérarchie, ses utilisateurs membres se voient accorder l'accès aux rôles respectifs. Lorsqu'un groupe est retiré de l'imbrication, les utilisateurs membres du groupe peuvent perdre l'accès aux droits basés sur les rôles.
- Les modifications apportées à l'imbrication ne sont pas capturées lors de l'actualisation utilisateur. Étant donné que les modifications d'imbrication ne peuvent pas être effectuées à la demande, les modifications sont capturées via une tâche en arrière-plan.

- Les modifications de l'imbrication étant supposées être rares, la tâche en arrière-plan s'exécute une fois par jour pour vérifier les modifications.

Est-il possible de désactiver une tâche de traitement d'un groupe imbriqué ?

- Vous pouvez désactiver les tâches lorsque vous savez que les modifications d'imbrication ne s'appliquent pas aux groupes intéressés.

Déploiement XenMobile

November 12, 2020

Il existe un grand nombre d'éléments à prendre en compte lorsque vous planifiez un déploiement XenMobile :

- Quels appareils choisir ?
- Comment gérer les appareils ?
- Comment s'assurer que votre réseau est sécurisé tout en proposant une expérience utilisateur optimale ?
- Quel matériel est nécessaire et comment le dépanner ?

Les articles de cette section visent à aider à répondre à ces questions. Vous y trouverez des cas d'utilisation et des recommandations sur des sujets qui couvrent vos problèmes de déploiement.

Gardez à l'esprit qu'une directive ou une recommandation peut ne pas s'appliquer à tous les environnements ou cas d'utilisation. Assurez-vous de configurer un environnement de test avant de lancer un déploiement XenMobile.

Les articles de cette section couvrent les domaines suivants :

- **Évaluation :** cas d'utilisation courants et questions à prendre en compte lors de la planification de votre déploiement.
- **Conception et configuration :** recommandations pour la conception et la configuration de votre environnement.
- **Fonctionnement et surveillance :** assurer le bon fonctionnement de votre environnement d'exécution.

Évaluation

Comme pour tout déploiement, l'évaluation de vos besoins est la priorité absolue. Pourquoi avez-vous besoin de XenMobile ? Avez-vous besoin de gérer tous les appareils de votre environnement ou seulement les applications ? Vous devrez peut-être gérer les deux. De quel niveau de sécurité nécessitez-vous pour votre environnement XenMobile ? Examinons les cas d'utilisation courants et les questions à prendre en compte lors de la planification de votre déploiement.

- Modes de gestion
- Configuration requise par l'appareil
- Sécurité et expérience utilisateur
- Applications
- Communautés d'utilisateurs
- Stratégie de messagerie
- Intégration de XenMobile
- Configuration requise multisite

Conception et configuration

Une fois que vous avez terminé d'évaluer vos besoins de déploiement, vous pouvez déterminer la conception et la configuration de votre environnement. Voici quelques conseils liés à la planification :

- Choisir le matériel pour votre serveur
- Configuration de stratégies pour les applications et les appareils
- Inscription des utilisateurs

Cette section contient des cas d'utilisation et des recommandations pour chacun de ces scénarios et bien plus encore.

- Intégration avec Citrix ADC et Citrix Gateway
- Considérations SSO et proxy pour les applications MDX
- Authentification
- Architecture de référence pour les déploiements sur site
- Propriétés du serveur
- Stratégies d'appareil et d'application
- Options d'inscription des utilisateurs
- Optimisation des opérations XenMobile

Fonctionnement et surveillance

Une fois que votre environnement XenMobile est opérationnel, vous devez le surveiller pour garantir son bon fonctionnement. La section Surveillance explique où vous pouvez trouver les différents journaux et messages générés par XenMobile et ses composants, ainsi que la manière de lire ces journaux. Cette section comprend également différentes procédures de dépannage communes que vous pouvez suivre pour réduire le temps de réponse du service client.

- Provisioning et deprovisioning d'applications
- Opérations basées sur le tableau de bord
- Contrôle d'accès basé sur les rôles et support XenMobile

- Suivi du système
- Récupération d'urgence
- Processus de support Citrix

Modes de gestion

January 10, 2022

Pour chaque instance XenMobile (un seul serveur ou un cluster de nœuds), vous pouvez choisir de gérer les appareils, les applications ou les deux. XenMobile utilise les termes suivants pour les modes de gestion d'appareils et d'applications :

- Mode de gestion d'appareils mobiles (mode MDM)
- Mode de gestion d'applications mobiles (mode MAM)
- Mode MDM + MAM (mode Enterprise)

Gestion d'appareils mobiles (mode MDM)

> **Important :**
>
> Si vous configurez le mode MDM et passez ensuite au mode ENT, veillez à utiliser la même authentification (Active Directory). XenMobile ne prend pas en charge la modification du mode d'authentification après l'inscription de l'utilisateur. Pour plus d'informations, consultez la section Mettre à niveau.

Grâce au mode MDM, vous pouvez configurer, sécuriser et prendre en charge les appareils mobiles. MDM vous permet de protéger les appareils et les données sur les appareils au niveau du système. Vous pouvez configurer des stratégies, des actions et des fonctions de sécurité. Par exemple, vous pouvez effacer un appareil de manière sélective si l'appareil est perdu, volé ou non conforme. Bien que la gestion des applications ne soit pas disponible en mode MDM, vous pouvez distribuer des applications mobiles, telles que les applications publiques et les applications d'entreprise, dans ce mode. Voici les cas d'utilisation courants pour le mode MDM :

- MDM est pris en compte pour les appareils appartenant à l'entreprise dans lesquels des stratégies ou des restrictions de gestion au niveau de l'appareil, telles que l'effacement complet, l'effacement sélectif ou la géolocalisation, sont requises.
- Lorsque les clients nécessitent la gestion d'un appareil réel, mais ne nécessitent pas de stratégies MDX, telles que la conteneurisation d'applications, les contrôles sur le partage de données d'application ou un micro VPN.
- Lorsque les utilisateurs nécessitent uniquement l'envoi d'e-mails à leurs clients de messagerie natifs sur leurs appareils, et Exchange ActiveSync ou le serveur d'accès au client est déjà acces-

sible de l'extérieur. Dans ce cas, vous pouvez utiliser MDM pour configurer la distribution des e-mails.
- Lorsque vous déployez des applications d'entreprise natives (non-MDX), des applications de magasin d'applications publiques ou des applications MDX fournies par des magasins publics. Considérez qu'une solution MDM seule peut ne pas empêcher la fuite de données d'informations confidentielles entre les applications sur l'appareil. Des fuites de données peuvent se produire lors des opérations Copier et coller ou Enregistrer sous dans les applications Office 365.

Gestion d'applications mobiles (mode MAM)

Le mode MAM protège les données d'application et vous permet de contrôler le partage de données d'application. MAM facilite également la gestion des données et des ressources de l'entreprise, indépendamment des données personnelles. Lorsque XenMobile est configuré avec le mode MAM, vous pouvez utiliser des applications mobiles compatibles MDX pour fournir la conteneurisation et le contrôle par application. Le mode MAM est également appelé mode MAM exclusif. Ce terme distingue ce mode d'un ancien mode MAM.

En s'appuyant sur les stratégies MDX, XenMobile offre un contrôle au niveau de l'application sur l'accès au réseau (tel que le micro VPN), l'interaction entre l'application et l'appareil, le cryptage des données et l'accès aux applications.

Le mode MAM est souvent adapté à l'environnement BYOD (Bring Your Own Device, Apportez votre propre appareil) car, bien que l'appareil ne soit pas géré, les données de l'entreprise restent protégées. MDX dispose de nombreuses stratégies MAM exclusif qui ne nécessitent pas de contrôle MDM.

MAM prend également en charge les applications de productivité mobiles. Cette prise en charge inclut la distribution de la messagerie sécurisée à Citrix Secure Mail, le partage des données entre les applications de productivité mobiles sécurisées et le stockage sécurisé des données dans Citrix Files. Pour plus de détails, consultez la section Applications de productivité mobiles.

Le mode MAM convient souvent aux scénarios suivants :

- Vous mettez à disposition des applications mobiles, telles que les applications MDX, gérées au niveau de l'application.
- Vous n'êtes pas obligé de gérer les appareils au niveau du système.

MDM + MAM (Mode Enterprise)

MDM + MAM est un mode hybride, également appelé Mode Enterprise, qui permet d'activer tous les ensembles de fonctionnalités disponibles dans la solution de gestion de la mobilité d'entreprise XenMobile. La configuration de XenMobile avec le mode MDM + MAM active à la fois les fonctionnalités MDM et MAM.

XenMobile vous permet de spécifier si les utilisateurs peuvent choisir de désactiver la gestion des appareils ou si la gestion des appareils est requise. Cette flexibilité est utile pour les environnements qui incluent une combinaison de cas d'utilisation. Ces environnements peuvent ou non nécessiter la gestion d'un appareil via des stratégies MDM pour accéder à vos ressources MAM.

Le mode MDM + MAM convient aux scénarios suivants :

- Vous disposez d'un cas d'utilisation unique dans lequel le mode MDM et le mode MAM sont requis. MDM est requis pour accéder à vos ressources MAM.
- Certains cas d'utilisation nécessitent MDM alors que dans d'autres cas MDM n'est pas requis.
- Certains cas d'utilisation nécessitent MAM alors que dans d'autres cas MAM n'est pas requis.

Vous pouvez spécifier le mode de gestion pour XenMobile Server via la propriété Mode de serveur. Vous pouvez configurer le paramètre dans la console XenMobile. Le mode peut être MDM, MAM ou ENT (pour MDM + MAM).

L'édition XenMobile pour laquelle vous disposez d'une licence détermine les modes de gestion et les autres fonctions disponibles, comme indiqué dans le tableau suivant.

XenMobile MDM Edition	XenMobile Advanced Edition	XenMobile Enterprise Edition
Fonctionnalités MDM	Fonctionnalités MDM	Fonctionnalités MDM
-	Fonctionnalités MAM	Fonctionnalités MAM
-	MDX Toolkit	MDX Toolkit
Secure Hub	Secure Hub	Secure Hub
-	Secure Mail	Secure Mail
-	Secure Web	Secure Web
QuickEdit	QuickEdit	QuickEdit
-	-	ShareConnect
-	-	Citrix Files

Modes de gestion et profils d'inscription

Les modes de gestion et les profils d'inscription fonctionnent ensemble. Vous utilisez un profil d'inscription pour configurer les options d'inscription de gestion des appareils et de gestion des applications pour les appareils Android et iOS. Pour Android, les options d'inscription disponibles pour le mode serveur MDM+MAM diffèrent des options du mode MDM. Pour plus d'informations, voir

Profils d'inscription.

Gestion des appareils et inscription MDM

Un environnement XenMobile Enterprise peut inclure une combinaison de cas d'utilisation, dont certains nécessitent une gestion des appareils via des stratégies MDM pour autoriser l'accès aux ressources MAM. Avant de déployer des applications de productivité mobiles pour les utilisateurs, évaluez entièrement vos cas d'utilisation et décidez si vous avez besoin d'une inscription MDM. Si vous décidez ultérieurement de modifier la configuration requise pour l'inscription MDM, il est probable que les utilisateurs devront réinscrire leurs appareils.

> **Remarque :**
>
> Pour spécifier si vous souhaitez que les utilisateurs s'inscrivent dans MDM, utilisez la propriété XenMobile Server **Inscription requise** dans la console XenMobile (**Paramètres > Propriétés du serveur**). Cette propriété de serveur globale s'applique à tous les utilisateurs et appareils de l'instance XenMobile. La propriété s'applique uniquement lorsque le mode de XenMobile Server est défini sur ENT.

Voici un résumé des avantages et des inconvénients (ainsi que des options d'atténuation) de la demande d'inscription MDM dans un déploiement XenMobile en mode Enterprise.

Lorsque l'inscription MDM est facultative

Avantages :

- Les utilisateurs peuvent accéder aux ressources MAM sans placer leurs appareils sous la gestion MDM. Cette option peut augmenter l'adoption par les utilisateurs.
- Il est possible de sécuriser l'accès aux ressources MAM pour protéger les données de l'entreprise.
- Les stratégies MDX telles que **Code secret d'application** permettent de contrôler l'accès à l'application pour chaque application MDX.
- La configuration de Citrix ADC, de XenMobile Server et des délais d'attente par application, associée au code PIN Citrix, offre une couche de protection supplémentaire.
- Bien que les actions MDM ne s'appliquent pas à l'appareil, certaines stratégies MDX peuvent être utilisées pour refuser l'accès MAM. Le refus doit être basé sur les paramètres système, tels que les appareils jailbreakés ou rootés.
- Les utilisateurs peuvent choisir d'inscrire leur appareil avec MDM lors de la première utilisation.

Inconvénients :

- Les ressources MAM sont disponibles pour les appareils non inscrits dans MDM.
- Les stratégies et les actions MDM sont disponibles uniquement pour les appareils inscrits dans MDM.

Options d'atténuation :

- Demandez aux utilisateurs d'accepter les conditions générales d'une entreprise qui les tient responsables en cas de non-conformité. Demandez aux administrateurs de surveiller les appareils non gérés.
- Gérez l'accès et la sécurité des applications en utilisant des minuteurs d'application. Les valeurs de délai d'attente réduites augmentent la sécurité, mais peuvent affecter l'expérience de l'utilisateur.
- Un deuxième environnement XenMobile avec l'inscription MDM requise est possible. Lorsque vous envisagez cette option, gardez à l'esprit les frais supplémentaires liés à la gestion de deux environnements et les ressources supplémentaires requises.

Lorsque l'inscription MDM est requise

Avantages :

- Il est possible de restreindre l'accès aux ressources MAM uniquement aux appareils gérés par MDM.
- Les stratégies et les actions MDM peuvent s'appliquer à tous les appareils de l'environnement, selon vos besoins.
- Les utilisateurs ne peuvent pas désactiver l'inscription de leur appareil.

Inconvénients :

- Tous les utilisateurs doivent s'inscrire avec MDM.
- Cette option peut diminuer l'adoption par les utilisateurs qui s'opposent à la gestion d'entreprise de leurs appareils personnels.

Options d'atténuation :

- Informez les utilisateurs de ce que XenMobile gère réellement sur leurs appareils et des informations auxquelles les administrateurs peuvent accéder.
- Vous pouvez utiliser un deuxième environnement XenMobile avec un mode serveur MAM (également appelé mode MAM exclusif) pour les appareils qui n'ont pas besoin d'une gestion MDM. Lorsque vous envisagez cette option, gardez à l'esprit les frais supplémentaires liés à la gestion de deux environnements et les ressources supplémentaires requises.

À propos des modes MAM et des modes MAM d'ancienne génération

XenMobile 10.3.5 a introduit un nouveau mode de serveur MAM exclusif. Pour faire la distinction entre les anciens et les nouveaux modes MAM, la documentation utilise les termes suivants. Le nouveau mode est appelé « mode MAM exclusif » ou MA. Le mode MAM antérieur est appelé « ancien mode MAM ».

Le mode MAM exclusif prend effet lorsque la propriété de mode de serveur de XenMobile est MAM. Les appareils s'enregistrent en mode MAM.

L'ancienne fonctionnalité MAM prend effet lorsque la propriété de mode de serveur de XenMobile est ENT et que les utilisateurs choisissent de ne pas utiliser la gestion des appareils. Dans ce cas, les appareils s'enregistrent en mode MAM. Les utilisateurs qui désactivent la gestion MDM continuent à recevoir l'ancienne fonctionnalité MAM.

> **Remarque :**
>
> Précédemment, la définition de la propriété de serveur sur MAM avait le même effet que de la définir sur ENT : les utilisateurs qui avaient choisi de ne pas utiliser la gestion MDM recevaient l'ancienne fonctionnalité MAM.

Le tableau suivant décrit le paramètre de mode de serveur à utiliser pour un type de licence particulier et un mode d'appareil souhaité :

Vos licences pour cette édition	Vous voulez que les appareils s'inscrivent dans ce mode	Définissez la propriété du mode de serveur sur
Enterprise/ Advanced/MDM	Mode MDM	MDM
Enterprise/Advanced	Mode MAM (également appelé mode MAM exclusif)	MAM
Enterprise/Advanced	Mode MDM+MAM	ENT (les utilisateurs qui ont choisi de ne pas utiliser la gestion des appareils utilisent l'ancien mode MAM)

Le mode MAM exclusif prend en charge les fonctionnalités suivantes qui étaient auparavant disponibles uniquement pour ENT. Ces fonctionnalités ne sont pas disponibles pour Windows Phone.

- **Authentification basée sur certificat :** le mode MAM exclusif prend en charge l'authentification basée sur les certificats. Les utilisateurs pourront continuer à accéder à leurs applications même si leur mot de passe Active Directory expire. Si vous utilisez l'authentification basée sur certificat pour les appareils MAM, vous devez configurer votre instance Citrix Gateway. Par défaut, dans **Paramètres XenMobile > Citrix Gateway**, l'option Délivrer un certificat utilisateur pour l'authentification est définie sur **Désactivé**, ce qui signifie que l'authentification par nom d'utilisateur et mot de passe est utilisée. Modifiez ce paramètre sur **Activé** pour activer l'authentification basée sur certificat.

- **Portail en libre-service :** cette fonctionnalité permet aux utilisateurs de verrouiller et d'effacer eux-mêmes leurs applications. Ces actions s'appliquent à toutes les applications sur l'appareil. Vous pouvez configurer les actions de verrouillage et d'effacement d'applications dans **Configurer> Actions**.
- **Tous les modes d'inscription sécurisée :** tous les modes d'inscription, y compris Haute sécurité, URL d'invitation et Deux facteurs sont configurés via **Gérer > Invitations d'inscription**.
- **Limite d'enregistrement d'appareils pour les appareils Android et iOS :** la propriété de serveur **Nombre d'utilisateurs par appareil** a été déplacée vers **Configurer > Profils d'inscription** et s'applique désormais à tous les modes de serveur.
- **API MAM exclusif :** pour les appareils en mode MAM exclusif, vous pouvez appeler les services REST à l'aide de n'importe quel client REST et utiliser l'API REST XenMobile pour appeler les services exposés au travers de la console XenMobile.
- Les API du mode MAM exclusif vous permettent d'effectuer les actions suivantes :
  - Envoyer une URL d'invitation et un code PIN à usage unique
  - Envoyer la commande Verrouillage des applications (mode kiosque) ou Effacement des applications sur des appareils

Le tableau suivant résume les différences entre les fonctionnalités de l'ancien mode MAM et du mode MAM exclusif.

Scénarios d'inscription et autres fonctionnalités	Ancien mode MAM (le mode de serveur est ENT)	Mode MAM exclusif (le mode de serveur est MAM)
Authentification du certificat	Non pris en charge.	Pris en charge. Pour utiliser l'authentification basée sur certificat, Citrix Gateway est requis.
Exigences en matière de déploiement	Le serveur XenMobile n'a pas besoin d'être directement accessible à partir des appareils.	Le serveur XenMobile n'a pas besoin d'être directement accessible à partir des appareils.
Options d'inscription	Utiliser le nom de domaine complet de Citrix Gateway ou lors de l'utilisation du nom de domaine complet de MDM, ne pas s'inscrire.	Utiliser le nom de domaine complet du serveur XenMobile.

Méthodes d'inscription*	Nom d'utilisateur + mot de passe	Nom d'utilisateur + mot de passe, Haute sécurité, URL d'invitation, URL d'invitation + code PIN, URL d'invitation + mot de passe, Deux facteurs, Nom d'utilisateur + code PIN
Mode kiosque et effacement des applications	Pris en charge.	Pris en charge.
Portail en libre-service Options du mode kiosque et d'effacement des applications	Non pris en charge.	Pris en charge.
Comportement d'effacement des applications	Les applications restent sur l'appareil mais ne sont pas utilisables. XenMobile supprime le compte sur le client uniquement.	Les applications restent sur l'appareil mais ne sont pas utilisables. XenMobile supprime le compte sur le client uniquement.
Actions automatisées pour les utilisateurs du mode MAM exclusif.	Les actions liées aux événements, aux propriétés d'appareil et aux propriétés d'utilisateur sont prises en charge. Les actions automatisées basées sur les applications installées ne sont pas prises en charge.	Les actions liées aux événements, aux propriétés d'appareil et aux propriétés d'utilisateur, ainsi que certaines actions basées sur les applications, telles que l'effacement d'applications ou le verrouillage d'applications (mode kiosque), sont prises en charge.
Action intégrée lorsqu'un utilisateur Active Directory est supprimé	L'effacement des applications est pris en charge.	L'effacement des applications est pris en charge.
Limite d'inscription	Pris en charge ; configuré au moyen d'un profil d'inscription.	Pris en charge ; configuré au moyen d'un profil d'inscription.

un inventaire logiciel	Pris en charge. XenMobile dresse la liste des applications installées sur un appareil.	Non pris en charge.

***Concernant les notifications :** SMTP est la seule méthode prise en charge pour l'envoi d'invitations d'inscription.

> **Important :**
>
> Pour le mode MAM exclusif, les utilisateurs inscrits précédemment doivent réinscrire leurs appareils. N'oubliez pas de fournir le nom de domaine complet de XenMobile Server à vos utilisateurs car ils en auront besoin pour l'inscription. Dans le mode MAM exclusif, comme avec le mode ENT, les appareils s'inscrivent à l'aide du nom de domaine complet de XenMobile Server. (Dans les versions antérieures du mode MAM, les appareils s'inscrivent à l'aide du nom de domaine complet de Citrix Gateway).

Configuration requise par l'appareil

January 10, 2022

Un point important à prendre en compte pour tout déploiement est l'appareil que vous souhaitez déployer. Sur les plateformes iOS, Android et Windows, les options sont nombreuses. Pour de plus amples informations sur les appareils pris en charge dans XenMobile, consultez la section Plates-formes prises en charge.

Dans un environnement BYOD (Amenez votre propre appareil), un mélange de plates-formes prises en charge est possible. Toutefois, tenez compte des limitations décrites dans l'article Plates-formes prises en charge lorsque vous informez les utilisateurs des appareils qu'ils peuvent inscrire. Même si vous n'autorisez qu'un ou deux appareils dans votre environnement, XenMobile fonctionne légèrement différemment sur les appareils iOS, Android et Windows. Différentes fonctionnalités sont disponibles sur chaque plate-forme.

En outre, toutes les conceptions d'applications ne ciblent pas les facteurs de forme des tablettes et des téléphones. Avant de procéder à des modifications générales, testez les applications pour vous assurer qu'elles correspondent à l'écran de l'appareil que vous souhaitez déployer.

Vous pouvez également prendre en compte les facteurs d'inscription. Apple et Google proposent des programmes d'inscription d'entreprise. Grâce au programme Apple Deployment (DEP) et à Google

Android Entreprise, vous pouvez acheter des appareils préconfigurés et prêts à être utilisés par les employés.

Pour plus d'informations sur l'inscription, consultez la section Options d'inscription des utilisateurs.

Sécurité et expérience utilisateur

January 10, 2022

La sécurité est importante pour toute organisation, mais vous devez trouver un équilibre entre la sécurité et l'expérience utilisateur. Par exemple, vous pouvez avoir un environnement hautement sécurisé qui est difficile à utiliser pour les utilisateurs. Ou votre environnement peut être si convivial que le contrôle d'accès n'est pas aussi strict. Les autres sections de ce manuel virtuel couvrent en détail les fonctionnalités de sécurité. Le but de cet article est de donner un aperçu général des problèmes de sécurité courants et des options de sécurité disponibles dans XenMobile.

Voici quelques considérations clés à garder à l'esprit pour chaque cas d'utilisation :

- Voulez-vous sécuriser certaines applications, l'appareil entier ou tout ?
- Comment voulez-vous que vos utilisateurs authentifient leur identité ? Prévoyez-vous d'utiliser LDAP, l'authentification basée sur les certificats ou une combinaison des deux ?
- Comment voulez-vous gérer les délais d'expiration de session utilisateur ? Gardez à l'esprit qu'il existe différentes valeurs de délai d'expiration pour les services d'arrière-plan, Citrix ADC et pour accéder aux applications en mode hors connexion.
- Souhaitez-vous que les utilisateurs configurent un code d'accès au niveau de l'appareil, un code d'accès au niveau de l'application ou les deux ? Combien de tentatives de connexion souhaitez-vous offrir aux utilisateurs ? Gardez à l'esprit l'impact sur l'expérience utilisateur que peuvent avoir les exigences supplémentaires d'authentification par application implémentées avec MAM.
- Quelles autres restrictions voulez-vous appliquer aux utilisateurs ? Souhaitez-vous donner aux utilisateurs l'accès à des services cloud tels que Siri ? Que peuvent-ils faire et ne pas faire avec chaque application que vous mettez à leur disposition ? Souhaitez-vous déployer des stratégies Wi-Fi d'entreprise pour empêcher que les forfaits de données cellulaires ne soient consommés à l'intérieur des espaces de bureau ?

Application ou Appareil

L'une des premières choses à faire est de déterminer si vous ne devez sécuriser que certaines applications à l'aide de la gestion des applications mobiles (MAM). Ou si vous souhaitez également gérer l'ensemble de l'appareil à l'aide de la gestion des appareils mobiles (MDM). Le plus souvent, si vous

n'avez pas besoin d'un contrôle au niveau de l'appareil, vous n'avez besoin que de gérer les applications mobiles, en particulier si votre organisation prend en charge Bring Your Own Device (BYOD).

Les utilisateurs équipés d'appareils qui ne sont pas gérés peuvent installer des applications via le magasin d'applications. À la place des contrôles au niveau de l'appareil, comme l'effacement partiel ou complet, vous contrôlez l'accès aux applications via des stratégies d'application. Les stratégies, selon les valeurs que vous avez définies, requièrent que l'appareil vérifie régulièrement XenMobile pour confirmer que les applications sont toujours autorisées à s'exécuter.

MDM vous permet de sécuriser l'ensemble d'un appareil, y compris la possibilité de faire l'inventaire de tous les logiciels d'un appareil. Vous pouvez empêcher l'inscription si l'appareil est jailbreaké, rooté ou si un logiciel non sécurisé est installé. Toutefois, les utilisateurs se méfient d'un tel niveau de contrôle sur leurs appareils personnels et cela peut réduire les taux d'inscription.

Authentification

C'est au niveau de l'authentification qu'une grande partie de l'expérience de l'utilisateur a lieu. Si votre organisation exécute déjà Active Directory, l'utilisation d'Active Directory est le moyen le plus simple d'autoriser vos utilisateurs à accéder au système.

Les délais d'expiration représentent aussi une partie importante de l'expérience de l'utilisateur avec l'authentification. Un environnement de haute sécurité peut obliger les utilisateurs à se connecter à chaque fois qu'ils accèdent au système, mais cette option n'est pas idéale pour toutes les organisations. Par exemple, demander aux utilisateurs d'entrer leurs informations d'identification chaque fois qu'ils veulent accéder à leur messagerie peut avoir un effet négatif sur l'expérience des utilisateurs.

Entropie utilisateur

Pour plus de sécurité, vous pouvez activer une fonctionnalité appelée *entropie utilisateur*. Citrix Secure Hub et d'autres applications partagent souvent des données communes telles que les mots de passe, les codes confidentiels et les certificats pour garantir le bon fonctionnement de tous les éléments. Ces informations sont stockées dans un coffre générique dans Secure Hub. Si vous activez l'entropie utilisateur via l'option **Crypter les secrets** (Encrypt Secrets), XenMobile crée un nouveau coffre appelé UserEntropy. XenMobile déplace les informations du coffre-fort générique vers le nouveau coffre-fort. Pour que Secure Hub ou une autre application accède aux données, les utilisateurs doivent entrer un mot de passe ou un code PIN.

L'activation de l'entropie utilisateur ajoute une couche d'authentification supplémentaire à plusieurs emplacements. Par conséquent, les utilisateurs doivent entrer un mot de passe ou un code PIN chaque fois qu'une application nécessite l'accès à des données partagées, y compris des certificats, dans le coffre-fort UserEntropy.

Pour en savoir plus sur l'entropie utilisateur, consultez la section À propos de MDX Toolkit dans la documentation XenMobile. Pour activer l'entropie utilisateur, vous pouvez trouver les paramètres associés dans les propriétés du client.

Stratégies

Les stratégies MDX et MDM offrent une grande flexibilité aux organisations, mais elles peuvent également restreindre les utilisateurs. Par exemple, vous pouvez souhaiter bloquer l'accès à des applications cloud telles que Siri ou iCloud qui sont susceptibles d'envoyer des données sensibles à différents endroits. Vous pouvez configurer une stratégie pour bloquer l'accès à ces services, mais gardez à l'esprit qu'une telle stratégie peut avoir des conséquences imprévues. Le micro du clavier iOS dépend également de l'accès au cloud et vous pouvez également bloquer l'accès à cette fonctionnalité.

Applications

La gestion de la mobilité d'entreprise (EMM) inclut la gestion d'appareils mobiles (MDM) et gestion d'applications mobiles (MAM). Alors que MDM permet aux entreprises de sécuriser et de contrôler les appareils mobiles, MAM facilite la livraison et la gestion des applications. Avec l'adoption croissante de la stratégie BYOD (Apportez votre propre appareil), vous pouvez généralement implémenter une solution MAM pour vous aider à prendre en charge la mise à disposition des applications, l'attribution des licences logicielles, la configuration et la gestion du cycle de vie des applications.

Avec XenMobile, vous pouvez aller plus loin dans la sécurisation des applications en configurant des stratégies MAM et des paramètres VPN spécifiques pour éviter les fuites de données et autres menaces de sécurité. XenMobile offre aux entreprises la flexibilité nécessaire pour déployer l'une des solutions suivantes :

- Environnement MAM exclusif
- Environnement MDM exclusif
- Environnement unifié XenMobile Enterprise qui fournit à la fois des fonctionnalités MDM et MAM sur la même plate-forme

En plus de la possibilité de mettre à disposition des applications sur des appareils mobiles, XenMobile propose la conteneurisation d'applications via la technologie MDX. MDX sécurise les applications grâce à un cryptage distinct du cryptage au niveau de l'appareil fourni par les plates-formes. Vous pouvez effacer ou verrouiller l'application. Les applications sont soumises à des contrôles granulaires basés sur des stratégies. Les éditeurs de logiciels indépendants peuvent appliquer ces contrôles à l'aide du SDK Mobile Apps.

Dans un environnement d'entreprise, les utilisateurs utilisent diverses applications mobiles pour les aider dans leur travail. Les applications peuvent inclure des applications du magasin d'applications public, des applications développées en interne et des applications natives. XenMobile classe ces applications comme suit :

Applications publiques : ces applications peuvent être gratuites ou payantes et sont disponibles dans un magasin d'applications public, tel que l'Apple App Store ou Google Play. Les fournisseurs externes à l'organisation mettent souvent à disposition leurs applications dans des magasins d'applications publics. Cette option permet aux clients de télécharger les applications directement depuis Internet. Vous pouvez utiliser de nombreuses applications publiques dans votre organisation en fonction des besoins des utilisateurs. Des exemples de telles applications incluent les applications GoToMeeting, Salesforce et EpicCare.

Citrix ne prend pas en charge le téléchargement des fichiers binaires des applications directement à partir des magasins d'applications publics ou l'encapsulation avec MDX Toolkit pour la distribution d'entreprise. Pour activer MDX pour des applications tierces, contactez le fournisseur de votre application pour obtenir les fichiers binaires de l'application. Vous pouvez encapsuler les fichiers binaires à l'aide du MDX Toolkit ou intégrer le SDK MAM aux fichiers binaires.

Applications internes : de nombreuses organisations ont des développeurs internes qui créent des applications fournissant des fonctionnalités spécifiques et étant développées et distribuées indépendamment au sein de l'organisation. Dans certains cas, certaines organisations peuvent également avoir des applications fournies par des éditeurs de logiciels indépendants. Vous pouvez déployer ces applications en tant qu'applications natives ou vous pouvez les conteneuriser en utilisant une solution MAM, telle que XenMobile. Par exemple, une organisation de soins de santé peut créer une application interne qui permet aux médecins de consulter les informations sur les patients à partir d'appareils mobiles. Une organisation peut alors activer le SDK MAM pour l'application ou l'encapsuler par MDM pour sécuriser les informations du patient et activer l'accès VPN au serveur de base de données du patient principal.

Applications Web et Saas : ces applications comprennent les applications accessibles à partir d'un réseau interne (applications web) ou sur un réseau public (SaaS). XenMobile vous permet également de créer des applications Web et SaaS personnalisées à l'aide d'une liste de connecteurs d'applications. Ces connecteurs d'application peuvent faciliter l'authentification unique (SSO) aux applications Web existantes. Pour de plus amples informations, consultez la section Types de connecteur d'application. Par exemple, vous pouvez utiliser Google Apps SAML pour l'authentification unique basée sur le langage SAML (Security Assertion Markup Language) de Google Apps.

Applications de productivité mobiles Citrix : applications développées par Citrix et incluses avec la licence XenMobile. Pour plus de détails, consultez la section À propos des applications de productivité mobiles. Citrix propose également d'autres applications prêtes à l'emploi que les éditeurs de logiciels indépendants peuvent développer à l'aide du SDK Mobile Apps.

Applications HDX : applications hébergées par Windows que vous publiez avec StoreFront. Si vous disposez d'un environnement Citrix Virtual Apps and Desktops, vous pouvez intégrer les applications à XenMobile pour les mettre à la disposition des utilisateurs inscrits.

Selon le type d'applications mobiles que vous prévoyez de déployer et de gérer avec XenMobile, la configuration et l'architecture sous-jacentes diffèrent. Par exemple, si plusieurs groupes d'utilisateurs

ayant un niveau d'autorisation différent utilisent une même application, vous aurez peut-être besoin de groupes de mise à disposition distincts pour déployer deux versions de l'application. En outre, vous devez vous assurer que l'appartenance au groupe d'utilisateurs est mutuellement exclusive pour éviter les incohérences de stratégie sur les appareils de l'utilisateur.

Vous pouvez également gérer les licences d'applications iOS à l'aide de l'achat en volume d'Apple. Vous devrez pour cela vous inscrire à l'achat en volume Apple et configurer les paramètres d'achat en volume XenMobile dans la console XenMobile pour distribuer les applications avec les licences d'achat en volume. Avec une telle variété de cas d'utilisation, il est important d'évaluer et de planifier votre stratégie MAM avant la mise en œuvre de l'environnement XenMobile. Vous pouvez commencer à planifier votre stratégie MAM en définissant les éléments suivants :

Types d'applications : répertoriez les différents types d'applications que vous envisagez d'utiliser et attribuez-leur des catégories. Par exemple : applications de productivité publiques, natives, mobiles, Web, en interne, applications ISV, etc. En outre, catégorisez les applications selon différentes plates-formes d'appareils, telles que iOS et Android. Cette catégorisation permet d'aligner les paramètres XenMobile requis pour chaque type d'application. Par exemple, certaines applications peuvent ne pas être éligibles à l'encapsulation ou peuvent nécessiter l'utilisation du SDK Mobile Apps pour activer des API spéciales pour l'interaction avec d'autres applications.

Exigences en matière de réseau : configurez les applications avec des paramètres appropriés pour répondre aux exigences d'accès réseau spécifiques. Par exemple, certaines applications peuvent nécessiter l'accès à votre réseau interne via VPN. Certaines applications peuvent nécessiter un accès Internet pour acheminer l'accès via la DMZ. Afin de permettre à ces applications de se connecter au réseau requis, vous devez configurer divers paramètres en conséquence. La définition des exigences réseau par application vous aide à finaliser vos décisions architecturales dès le début, ce qui simplifie le processus de mise en œuvre global.

Exigences en matière de sécurité : Il est primordial de définir les exigences de sécurité qui s'appliquent à des applications individuelles ou à toutes les applications. Cette planification garantit que vous créez les bonnes configurations lorsque vous installez XenMobile Server. Bien que des paramètres, tels que les stratégies MDX, s'appliquent aux applications individuelles, les paramètres de session et d'authentification s'appliquent à toutes les applications. Certaines applications peuvent avoir des exigences spécifiques en matière de chiffrement, de conteneurisation, d'encapsulage, de chiffrement, d'authentification, de géofencing, de code d'accès ou de partage de données que vous pouvez définir à l'avance pour simplifier votre déploiement.

Exigences en matière de déploiement : vous pouvez utiliser un déploiement basé sur des stratégies pour autoriser le téléchargement des applications publiées uniquement par des utilisateurs compatibles. Par exemple, vous pouvez souhaiter pour certaines applications que :

- le cryptage de l'appareil basé sur la plate-forme soit activé
- l'appareil soit géré
- l'appareil réponde à une version minimale du système d'exploitation

- certaines applications soient disponibles uniquement pour les utilisateurs d'entreprise

Vous pouvez également exiger que certaines applications soient uniquement disponibles pour les utilisateurs d'entreprise. Définissez ces exigences à l'avance afin de pouvoir configurer les stratégies ou les actions de déploiement appropriées.

Exigences en matière de licence : enregistrez les exigences en matière de licence liées à l'application. Ces notes vous aident à gérer efficacement l'utilisation des licences et à décider si vous devez configurer des fonctionnalités spécifiques dans XenMobile pour faciliter l'attribution de licences. Par exemple, si vous déployez une application iOS gratuite ou payante, Apple applique les exigences de licence sur l'application en demandant aux utilisateurs de se connecter à leur compte iTunes. Vous pouvez vous inscrire à l'achat en volume d'Apple pour distribuer et gérer ces applications via XenMobile. L'achat en volume permet aux utilisateurs de télécharger les applications sans se connecter à leur compte iTunes. En outre, des outils tels que Samsung SAFE et Samsung Knox présentent des exigences de licence spéciales qui doivent être satisfaites avant le déploiement de ces fonctionnalités.

Exigences en matière de liste d'autorisation/liste de blocage : vous souhaitez probablement empêcher les utilisateurs d'installer ou d'utiliser certaines applications. Créez une liste d'autorisation d'applications qui définit la machine utilisateur comme étant hors conformité. Ensuite, configurez des stratégies pour qu'elles se déclenchent lorsqu'un appareil devient non conforme. D'un autre côté, une application peut être acceptable pour une utilisation, mais peut tomber sous la liste de blocage pour une raison quelconque. Dans ce cas, vous pouvez ajouter l'application à une liste d'autorisation et indiquer que l'utilisation de l'application est acceptable mais n'est pas requise. De plus, gardez à l'esprit que les applications préinstallées sur les nouveaux appareils peuvent inclure certaines applications couramment utilisées qui ne font pas partie du système d'exploitation. Ces applications peuvent entrer en conflit avec votre stratégie de liste de blocage.

Cas d'utilisation des applications

Une organisation de soins de santé prévoit de déployer XenMobile en tant que solution MAM pour leurs applications mobiles. Les applications mobiles sont mises à disposition des utilisateurs professionnels et BYOD. Le département informatique décide de mettre à disposition et de gérer les applications suivantes :

- **Applications de productivité mobiles :** applications iOS et Android fournies par Citrix.
- **Secure Mail :** application messagerie, calendrier et contact.
- **Secure Web :** navigateur Web sécurisé qui permet d'accéder aux sites Internet et intranet.
- **Citrix Files :** application permettant d'accéder aux données partagées et de partager, synchroniser et éditer des fichiers.

Magasin d'applications public

- **Secure Hub :** client utilisé par tous les appareils mobiles pour communiquer avec XenMobile. Le département informatique envoie les paramètres de sécurité, les configurations et les applications mobiles vers les appareils mobiles via le client Secure Hub. Les appareils Android et iOS s'inscrivent dans XenMobile via Secure Hub.
- **Citrix Receiver :** application mobile permettant aux utilisateurs d'ouvrir des applications hébergées par Virtual Apps and Desktops sur des appareils mobiles.
- **GoToMeeting :** un client de réunion, de partage de bureau et de visioconférence en ligne qui permet aux utilisateurs de se rencontrer en temps réel avec d'autres utilisateurs, clients ou collègues via Internet.
- **SalesForce1 :** Salesforce1 permet aux utilisateurs d'accéder à Salesforce à partir d'appareils mobiles et rassemble toutes les applications Chatter, CRM et applications personnalisées, ainsi que les processus d'entreprise, pour une expérience unifiée pour tout utilisateur Salesforce.
- **RSA SecurID :** jeton logiciel pour l'authentification à deux facteurs.
- **Applications EpicCare :** ces applications offrent aux professionnels de la santé un accès sécurisé et portable aux dossiers des patients, aux listes de patients, aux calendriers et aux messages.
  - **Haiku :** application mobile pour les téléphones iPhone et Android.
  - **Canto :** application mobile pour l'iPad.
  - **Rover :** applications mobiles pour iPhone et l'iPad.

HDX : ces applications sont mises à disposition via Citrix Virtual Apps and Desktops.

- **Epic Hyperspace :** application Epic client pour la gestion électronique des dossiers de santé.

ISV

- **Vocera :** application VoIP et de messagerie compatible HIPAA qui étend les avantages de la technologie vocale Vocera à tout moment, n'importe où, via l'iPhone et les smartphones Android.

Applications internes

- **HCMail :** application qui permet de composer des messages cryptés, d'effectuer des recherches dans des carnets d'adresses sur des serveurs de messagerie internes et d'envoyer les messages cryptés aux contacts à l'aide d'un client de messagerie.

Applications web internes

- **PatientRounding :** application Web utilisée pour enregistrer les informations sur la santé des patients par différents départements.
- **Outlook Web Access :** permet l'accès à la messagerie via un navigateur Web.
- **SharePoint :** utilisé pour le partage de fichiers et de données à l'échelle de l'organisation.

Le tableau suivant répertorie les informations de base requises pour la configuration MAM.

Nom de l'application	Type d'application	Encapsulation MDX	iOS	Android
Secure Mail	Applications XenMobile	Pas pour la version 10.4.1 et versions ultérieures	Oui	Oui
Secure Web	Applications XenMobile	Pas pour la version 10.4.1 et versions ultérieures	Oui	Oui
Citrix Files	Applications XenMobile	Pas pour la version 10.4.1 et versions ultérieures	Oui	Oui
Secure Hub	Application publique	SO	Oui	Oui
Citrix Receiver	Application publique	SO	Oui	Oui
GoToMeeting	Application publique	SO	Oui	Oui
SalesForce1	Application publique	SO	Oui	Oui
RSA SecurID	Application publique	SO	Oui	Oui
Epic Haiku	Application publique	SO	Oui	Oui
Epic Canto	Application publique	SO	Oui	Non
Epic Rover	Application publique	SO	Oui	Non
Epic Hyperspace	Application HDX	SO	Oui	Oui

Vocera	Application d'éditeur de logiciels indépendant	Oui	Oui	Oui
HCMail	Application interne	Oui	Oui	Oui
PatientRounding	Application Web	SO	Oui	Oui
Outlook Web Access	Application Web	SO	Oui	Oui
SharePoint	Application Web	SO	Oui	Oui

Les tableaux suivants répertorient les exigences spécifiques que vous pouvez consulter lorsque vous configurez les stratégies MAM dans XenMobile.

Nom de l'application	**VPN requis**	**Interaction**	**Interaction**	**Cryptage de l'appareil basé sur la plate-forme**
		(avec applis hors du conteneur)	**(depuis applis hors du conteneur)**	
———————	—	———————————	———————————	————
Secure Mail	O	Autorisé de manière sélective	Autorisé	Non requis
Secure Web	O	Autorisé	Autorisé	Non requis
Citrix Files	O	Autorisé	Autorisé	Non requis
Secure Hub	O	S.O.	S.O.	S.O.
Citrix Receiver	O	S.O.	S.O.	S.O.
GoToMeeting	N	S.O.	S.O.	S.O.
SalesForce1	N	S.O.	S.O.	S.O.
RSA SecurID	N	S.O.	S.O.	S.O.
Epic Haiku	O	S.O.	S.O.	S.O.
Epic Canto	O	S.O.	S.O.	S.O.
Epic Rover	O	S.O.	S.O.	S.O.
Epic Hyperspace	O	S.O.	S.O.	S.O.
Vocera	O	Bloqué	Bloqué	Non requis
HCMail	O	Bloqué	Bloqué	Requis
PatientRounding	O	S.O.	S.O.	Requis
Outlook Web Access	O	S.O.	S.O.	Non requis
SharePoint	O	S.O.	S.O.	Non requis

Nom de l'application	Filtrage par proxy	Gestion des licences	Géofencing	SDK Applications mobiles	Version du système d'exploitation minimum
Secure Mail	Requis	S.O.	Requis de manière sélective	S.O.	Appliqué
Secure Web	Requis	S.O.	Non requis	S.O.	Appliqué
Citrix Files	Requis	S.O.	Non requis	S.O.	Appliqué
Secure Hub	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
Citrix Receiver	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
GoToMeeting	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
SalesForce1	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
RSA SecurID	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
Epic Haiku	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
Epic Canto	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
Epic Rover	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
Epic Hyperspace	Non requis	S.O.	Non requis	S.O.	Non appliqué
Vocera	Requis	S.O.	Requis	Requis	Appliqué
HCMail	Requis	S.O.	Requis	Requis	Appliqué
PatientRoundir	Requis	S.O.	Non requis	S.O.	Non appliqué
Outlook Web Access	Requis	S.O.	Non requis	S.O.	Non appliqué
SharePoint	Requis	S.O.	Non requis	S.O.	Non appliqué

Communautés d'utilisateurs

Chaque organisation est composée de diverses communautés d'utilisateurs qui opèrent dans différents rôles fonctionnels. Ces communautés d'utilisateurs exécutent différentes tâches et fonctions de bureau à l'aide de diverses ressources que vous fournissez via des appareils mobiles. Les utilisateurs peuvent travailler à domicile ou dans des bureaux distants à l'aide d'appareils mobiles que vous fournissez. Les utilisateurs peuvent également utiliser leurs appareils mobiles personnels, ce qui leur permet d'accéder à des outils soumis à certaines règles de conformité de sécurité.

Avec un plus grand nombre de communautés d'utilisateurs utilisant des appareils mobiles, la gestion de la mobilité d'entreprise devient essentielle pour éviter la fuite de données et pour appliquer les restrictions de sécurité. Pour une gestion efficace et plus sophistiquée des appareils mobiles, vous pouvez catégoriser vos communautés d'utilisateurs. Cela simplifie le mappage des utilisateurs aux ressources et garantit que les bonnes stratégies de sécurité s'appliquent aux utilisateurs appropriés.

L'exemple suivant illustre comment les communautés d'utilisateurs d'une organisation de soins de santé sont classées pour EMM.

Cas d'utilisation des communautés d'utilisateurs

Cet exemple d'organisation de soins de santé fournit des ressources technologiques et un accès à plusieurs utilisateurs, y compris des employés et des bénévoles du réseau et de sociétés affiliées. L'organisation a choisi de déployer la solution EMM auprès des utilisateurs non-cadres uniquement.

Vous pouvez répartir les rôles utilisateur et les fonctions de cette organisation en sous-groupes, y compris personnel médical, personnel non-médical et sous-traitants. Un ensemble sélectionné d'utilisateurs reçoit des appareils mobiles d'entreprise tandis que d'autres peuvent accéder aux ressources limitées de l'entreprise à partir de leurs appareils personnels. Pour appliquer le niveau approprié de restrictions de sécurité et empêcher la fuite de données, l'organisation a décidé que l'informatique de l'entreprise gère chaque appareil inscrit, qu'il appartienne à l'entreprise ou à l'utilisateur. En outre, les utilisateurs ne peuvent inscrire qu'un seul appareil.

La section suivante donne un aperçu des rôles et des fonctions de chaque sous-groupe :

Personnel médical

- Infirmiers/Infirmières
- Médecins (docteurs, chirurgiens, etc.)
- Spécialistes (diététiciens, anesthésistes, radiologues, cardiologues, oncologues, etc.)
- Médecins externes (médecins non-employés et employés de bureau travaillant dans des bureaux éloignés)
- Services de santé à domicile (employés de bureau et travailleurs mobiles exécutant des services médicaux lors de visites à domicile auprès de patients)

- Spécialistes en recherche (travailleurs intellectuels et utilisateurs avancés dans six instituts de recherche médicale)
- Éducation et formation (infirmiers/infirmières, médecins et spécialistes en phase d'éducation et de formation)

Personnel non-médical

- Services partagés (employés de bureau effectuant diverses fonctions administratives, y compris RH, gestion des salaires, comptes fournisseurs, service de la chaîne d'approvisionnement, etc.)
- Services médicaux (employés de bureau effectuant divers services de gestion des soins de santé, services administratifs et solutions de processus commerciaux aux fournisseurs, y compris : services administratifs, analyse commerciale et intelligence économique, systèmes commerciaux, services aux clients, finances, gestion des soins, solutions d'accès patient, solutions de cycle des revenus, etc.)
- Services de support (employés de bureau remplissant diverses fonctions non-médicales, y compris : administration des avantages sociaux, intégration clinique, communications, rémunération et gestion du rendement, services d'équipement et de site, systèmes de technologie des RH, services d'information, vérification interne et amélioration des processus, etc.)
- Programmes philanthropiques (employés de bureau et mobiles qui exécutent diverses fonctions pour soutenir les programmes philanthropiques)

Sous-traitants

- Partenaires fabricants et fournisseurs (connectés sur site et à distance via un VPN site à site fournissant diverses fonctions de support non-médical)

Sur la base des informations précédentes, l'organisation a créé les entités suivantes. Pour plus d'informations sur les groupes de mise à disposition dans XenMobile, consultez la section Déployer des ressources.

Unités d'organisation et groupes Active Directory

Unité d'organisation **=** Ressources XenMobile :

- Unité d'organisation = personnel médical ; Groupes =
  - XM - Infirmiers/Infirmières
  - XM - Médecins
  - XM - Spécialistes
  - XM - Médecins externes
  - XM - Services de santé à domicile
  - XM - Spécialistes en recherche
  - XM - Éducation et formation

- Unité d'organisation = non-médical ; Groupes =
  - XM - Services partagés
  - XM - Services médicaux
  - XM - Services de support
  - XM - Programmes philanthropiques

Utilisateurs et groupes locaux XenMobile

Groupe = sous-traitants ; Utilisateurs =

- Fournisseur 1
- Fournisseur 2
- Fournisseur 3
- … Fournisseur 10

Groupes de mise à disposition XenMobile

- Personnel médical - Infirmiers/Infirmières
- Personnel médical - Médecins
- Personnel médical - Spécialistes
- Personnel médical - Médecins externes
- Personnel médical - Services de santé à domicile
- Personnel médical - Spécialistes en recherche
- Personnel médical - Éducation et formation
- Personnel non-médical - Services partagés
- Personnel non-médical - Services médicaux
- Personnel non-médical - Services de support
- Personnel non-médical - Programmes philanthropiques

Groupe de mise à disposition et mappage de groupe d'utilisateurs

Groupes Active Directory	Groupes de mise à disposition XenMobile
XM - Infirmiers/Infirmières	Personnel médical - Infirmiers/Infirmières
XM - Médecins	Personnel médical - Médecins
XM - Spécialistes	Personnel médical - Spécialistes
XM - Médecins externes	Personnel médical - Médecins externes
XM - Services de santé à domicile	Personnel médical - Services de santé à domicile

XM - Spécialistes en recherche	Personnel médical - Spécialistes en recherche
XM - Éducation et formation	Personnel médical - Éducation et formation
XM - Services partagés	Personnel non-médical - Services partagés
XM - Services médicaux	Personnel non-médical - Services médicaux
XM - Services de support	Personnel non-médical - Services de support
XM - Programmes philanthropiques	Personnel non-médical - Programmes philanthropiques

Groupe de mise à disposition et mappage des ressources

Les tableaux suivants illustrent les ressources affectées à chaque groupe de mise à disposition dans ce cas d'utilisation. Le premier tableau présente les attributions d'applications mobiles. Le deuxième tableau présente les ressources d'applications publiques, d'applications HDX et de gestion des appareils.

Groupes de mise à disposition XenMobile	Applications mobiles Citrix	Applications mobiles publiques	Applications mobiles HDX
Personnel médical - Infirmiers/Infirmières	X		
Personnel médical - Médecins			
Personnel médical - Spécialistes			
Personnel médical - Médecins externes	X		
Personnel médical - Services de santé à domicile	X		
Personnel médical - Spécialistes en recherche	X		

Personnel médical - Éducation et formation		X	X
Personnel non-médical - Services partagés		X	X
Personnel non-médical - Services médicaux		X	X
Personnel non-médical - Services de support	X	X	X
Personnel non-médical - Programmes philanthropiques	X	X	X
Sous-traitants	X	X	X

Groupes de mise à disposition XenMobile	Application publique : RSA SecurID	Application publique : EpicCare Haiku	Application HDX : Epic Hyperspace	Stratégie de code secret	Restriction d'appareil	Actions automatisées	Stratégie Wi-Fi
Personnel médical - Infirmiers/Infirmières							X
Personnel médical - Médecins					X		

Personnel médical - Spécialistes				
Personnel médical - Médecins externes				
Personnel médical - Services de santé à domicile				
Personnel médical - Spécialistes en recherche				
Personnel médical - Éducation et formation	X	X		
Personnel non-médical - Services partagés	X	X		
Personnel non-médical - Services médicaux	X	X		

Personnel non-médical - Services de support	X	X

Notes et considérations

- XenMobile crée un groupe de mise à disposition par défaut appelé Tous les utilisateurs lors de la configuration initiale. Si vous ne désactivez pas de ce groupe de mise à disposition, tous les utilisateurs Active Directory ont le droit de s'inscrire à XenMobile.
- XenMobile synchronise les utilisateurs et les groupes Active Directory à la demande en utilisant une connexion dynamique au serveur LDAP.
- Si un utilisateur fait partie d'un groupe qui n'est pas mappé dans XenMobile, cet utilisateur ne peut pas s'inscrire. De même, si un utilisateur est membre de plusieurs groupes, XenMobile catégorise l'utilisateur comme étant uniquement dans les groupes mappés à XenMobile.
- Pour rendre l'inscription MDM obligatoire, définissez l'option Inscription requise sur Vrai dans Propriétés du serveur dans la console XenMobile. Pour de plus amples informations, consultez la section Propriétés du serveur.
- Vous pouvez supprimer un groupe d'utilisateurs d'un groupe de mise à disposition XenMobile, en supprimant l'entrée dans la base de données SQL Server, sous dbo.userlistgrps.
  Avertissement : avant d'effectuer cette action, créez une copie de sauvegarde de XenMobile et de la base de données.

À propos de l'appartenance des appareils dans XenMobile Device

Vous pouvez regrouper les utilisateurs en fonction du propriétaire d'un appareil utilisateur. L'appartenance des appareils comprend les appareils appartenant à l'entreprise et les appareils appartenant aux utilisateurs, un programme plus communément appelé Apportez votre propre appareil (BYOD). Vous pouvez contrôler la façon dont les appareils BYOD se connectent à votre réseau à deux endroits dans la console XenMobile : sur la page Règles de déploiement de chaque type de ressource et via les propriétés du serveur sur la page **Paramètres**. Pour de plus amples informations sur les règles de déploiement, consultez la section Configuration des règles de déploiement dans la documentation XenMobile. Pour de plus amples informations sur les propriétés de serveur, consultez la section Propriétés du serveur.

Vous pouvez demander à tous les utilisateurs BYOD d'accepter que leurs appareils soient gérés par

l'entreprise avant qu'ils puissent accéder à des applications. Vous pouvez également autoriser les utilisateurs à accéder aux applications d'entreprise sans gérer leurs appareils.

Lorsque vous définissez la propriété de serveur **wsapi.mdm.required.flag** sur **Vrai**, tous les appareils BYOD sont gérés par XenMobile et tout utilisateur refusant l'inscription se voit refuser l'accès aux applications. Le paramétrage de **wsapi.mdm.required.flag** sur **Vrai** doit être envisagé dans les environnements dans lesquels les équipes informatiques ont besoin d'un haut niveau de sécurité avec une expérience utilisateur positive, en inscrivant des appareils utilisateur dans XenMobile.

Si vous laissez la valeur **wsapi.mdm.required.flag** sur **Faux**, qui est le paramètre par défaut, les utilisateurs pourront refuser l'inscription, mais ne pourront toujours accéder aux applications sur leurs appareils via le XenMobile Store. Le paramétrage de **wsapi.mdm.required.flag** sur **Faux** doit être envisagé dans les environnements dans lesquels les contraintes juridiques, de confidentialité et imposées par la législation ne requièrent pas la gestion des appareils mais uniquement la gestion des applications d'entreprise.

Les utilisateurs équipés d'appareils qui ne sont pas gérés peuvent installer des applications via XenMobile Store. À la place des contrôles au niveau de l'appareil, comme l'effacement partiel ou complet, vous contrôlez l'accès aux applications via des stratégies d'application. Les stratégies, selon les valeurs que vous avez définies, requièrent que l'appareil vérifie XenMobile Server pour confirmer que les applications sont toujours autorisées à s'exécuter.

Exigences en matière de sécurité

La quantité de considérations de sécurité à prendre en compte lors du déploiement d'un environnement XenMobile peut rapidement devenir écrasante. Il existe de nombreux composants et de paramètres imbriqués. Pour vous aider à démarrer et à choisir un niveau de protection acceptable, Citrix fournit des recommandations pour une sécurité élevée, supérieure et la plus élevée, décrites dans le tableau suivant.

Votre choix de mode de déploiement n'est pas déterminé que par la sécurité. Il est également important d'examiner les exigences des cas d'utilisation et de décider si vous pouvez atténuer les problèmes de sécurité avant de choisir votre mode de déploiement.

Sécurité élevée : l'utilisation de ces paramètres offre une expérience utilisateur optimale tout en maintenant un niveau de sécurité de base acceptable pour la plupart des organisations.

Sécurité supérieure : ces paramètres établissent un meilleur équilibre entre sécurité et facilité d'utilisation.

Sécurité la plus élevée : suivre ces recommandations fournit un haut niveau de sécurité au détriment de la facilité d'utilisation et de l'adoption par les utilisateurs.

Considérations sur la sécurité du mode de déploiement

Le tableau suivant spécifie les modes de déploiement pour chaque niveau de sécurité.

Haute sécurité	Sécurité plus élevée	Sécurité la plus élevée
MAM ou MDM	MDM+MAM	MDM+MAM ; plus FIPS

Remarques :

- Selon le cas d'utilisation, un déploiement MDM exclusif ou MAM exclusif peut répondre aux exigences de sécurité et offrir une bonne expérience utilisateur.
- Si vous n'avez pas besoin de conteneurisation d'applications, de micro-VPN ou de stratégies spécifiques aux applications, MDM doit être suffisant pour gérer et sécuriser les appareils.
- Pour les cas d'utilisation tels que le BYOD dans lequel toutes les exigences de l'entreprise et de sécurité peuvent être satisfaites uniquement avec la conteneurisation d'applications, Citrix recommande le mode MAM exclusif.
- Pour les environnements à haute sécurité (et les appareils fournis par les entreprises), Citrix recommande MDM+MAM pour tirer parti de toutes les fonctionnalités de sécurité disponibles. Veillez à forcer l'inscription MDM.
- Options FIPS pour les environnements ayant les besoins de sécurité les plus élevés, tels que le gouvernement fédéral.

Si vous activez le mode FIPS, vous devez configurer SQL Server pour chiffrer le trafic SQL.

Considérations relatives à la sécurité de Citrix ADC et Citrix Gateway

Le tableau suivant spécifie les recommandations Citrix ADC et Citrix Gateway pour chaque niveau de sécurité.

Haute sécurité	Sécurité plus élevée	Sécurité la plus élevée

Citrix ADC est recommandé. Citrix Gateway est requis pour MAM et ENT ; recommandé pour MDM	Configuration standard de l'assistant Citrix ADC pour XenMobile avec pont SSL si XenMobile se trouve dans la zone zone démilitarisée. Ou décharge SSL si nécessaire pour respecter les normes de sécurité lorsque XenMobile Server se trouve sur le réseau interne.	Décharge SSL avec cryptage de bout en bout

Remarques :

- Exposer le XenMobile Server à Internet via NAT ou des proxys tiers existants et des équilibreurs de charge peut être une option pour MDM. Toutefois, cette configuration nécessite que le trafic SSL se termine sur XenMobile Server, ce qui pose un risque potentiel de sécurité.
- Pour les environnements hautement sécurisé, Citrix ADC défini avec la configuration XenMobile par défaut respecte ou dépasse en général les exigences de sécurité.
- Pour les environnements MDM ayant les besoins de sécurité les plus élevés, la terminaison SSL sur Citrix ADC permet l'inspection du trafic sur le périmètre et maintient le cryptage SSL de bout en bout.
- Options pour définir les chiffrements SSL/TLS.
- Un matériel SSL FIPS Citrix ADC est également disponible.
- Pour plus d'informations, voir Intégration avec Citrix Gateway et Citrix ADC.

Considérations de sécurité d'inscription

Le tableau suivant spécifie les recommandations Citrix ADC et Citrix Gateway pour chaque niveau de sécurité.

Haute sécurité	Sécurité plus élevée	Sécurité la plus élevée

Appartenance à un groupe Active Directory uniquement. Groupe de mise à disposition Tous les utilisateurs désactivé.	Mode d'inscription sécurisée sur invitation uniquement. Appartenance à un groupe Active Directory uniquement. Groupe de mise à disposition Tous les utilisateurs désactivé	Mode d'inscription sécurisée lié à l'ID d'appareil. Appartenance à un groupe Active Directory uniquement. Groupe de mise à disposition Tous les utilisateurs désactivé

Remarques :

- Citrix vous recommande généralement de limiter l'inscription aux utilisateurs appartenant à des groupes Active Directory prédéfinis uniquement. Cette configuration nécessite de désactiver le groupe de mise à disposition intégré Tous les utilisateurs.
- Vous pouvez utiliser des invitations d'inscription pour restreindre l'inscription aux utilisateurs avec une invitation. Les invitations d'inscription ne sont pas disponibles pour les appareils Windows.
- Vous pouvez utiliser des invitations à s'inscrire par code PIN unique (OTP) comme solution d'authentification à deux facteurs et contrôler le nombre d'appareils qu'un utilisateur peut inscrire. Les invitations OTP ne sont pas disponibles pour les appareils Windows.

Considérations de sécurité pour le code secret des appareils

Le tableau suivant spécifie les recommandations de code secret de l'appareil pour chaque niveau de sécurité.

Haute sécurité	Sécurité plus élevée	Sécurité la plus élevée
Recommandée. Une haute sécurité est requise pour le cryptage au niveau de l'appareil. Appliquée à l'aide de MDM. Vous pouvez définir une sécurité élevée comme requis pour MAM exclusif en utilisant la stratégie MDX, Comportement des appareils non conformes.	Appliquée en utilisant une stratégie MDM et MDX, ou les deux.	Appliquée en utilisant une stratégie MDM et MDX. Stratégie de code secret complexe.

Remarques :

- Citrix recommande l'utilisation d'un code secret d'appareil.
- Vous pouvez appliquer un code secret d'appareil via une stratégie MDM.
- Vous pouvez utiliser une stratégie MDX pour que le code secret d'un appareil soit obligatoire pour l'utilisation des applications gérées ; par exemple, pour les cas d'utilisation BYOD.
- Citrix recommande de combiner les options de stratégie MDM et MDX pour une sécurité accrue dans les environnements MDM+MAM.
- Pour les environnements ayant les exigences de sécurité les plus élevées, vous pouvez configurer des stratégies de code d'accès complexes et les appliquer avec MDM. Vous pouvez configurer des actions automatiques pour informer les administrateurs ou émettre des effacements sélectifs/complets lorsqu'un appareil ne respecte pas une stratégie de code d'accès.

Applications

January 10, 2022

La gestion de la mobilité d'entreprise (EMM) inclut la gestion d'appareils mobiles (MDM) et gestion d'applications mobiles (MAM). Alors que MDM permet aux entreprises de sécuriser et de contrôler les appareils mobiles, MAM facilite la livraison et la gestion des applications. Dans le cadre de l'adoption du BYOD, vous pouvez généralement implémenter une solution MAM, telle que XenMobile, pour vous aider avec les opérations suivantes :

- mise à disposition d'applications
- attribution de licences logicielles
- configuration
- gestion du cycle de vie des applications

Vous pouvez obliger ou autoriser les utilisateurs à opter pour la gestion MDM.

Avec XenMobile, vous pouvez aller plus loin dans la sécurisation des applications en configurant des stratégies MAM et des paramètres VPN spécifiques pour éviter les fuites de données et autres menaces de sécurité. XenMobile offre aux entreprises la flexibilité nécessaire pour déployer leur solution en tant que :

- Environnement MAM exclusif
- Environnement MDM exclusif
- Environnement unifié XenMobile Enterprise qui fournit à la fois des fonctionnalités MDM et MAM

En plus de la possibilité de mettre à disposition des applications sur des appareils mobiles, XenMobile propose la conteneurisation d'applications via la technologie MDX. Les applications sont soumises à des contrôles granulaires basés sur des stratégies. Les éditeurs de logiciels indépendants peuvent appliquer ces contrôles à l'aide du SDK Mobile Apps.

Dans un environnement d'entreprise, les utilisateurs utilisent diverses applications mobiles pour les aider dans leur travail. Les applications peuvent inclure des applications du magasin d'applications public, des applications développées en interne ou des applications natives. XenMobile classe ces applications comme suit :

- **Applications publiques :** ces applications peuvent être gratuites ou payantes et sont disponibles dans un magasin d'applications public, tel que l'Apple App Store ou Google Play. Les fournisseurs externes à l'organisation mettent souvent à disposition leurs applications dans des magasins d'applications publics. Cette option permet aux clients de télécharger les applications directement depuis Internet. Vous pouvez utiliser de nombreuses applications publiques dans votre organisation en fonction des besoins des utilisateurs. Des exemples de telles applications incluent les applications GoToMeeting, Salesforce et EpicCare.
  - **Si vous utilisez le SDK MAM :** obtenez les binaires d'application auprès du fournisseur de votre application. Ensuite, intégrez le SDK MAM dans l'application.
  - **Si vous utilisez MDX Toolkit :** Citrix ne prend pas en charge le téléchargement des fichiers binaires des applications directement à partir des magasins d'applications publics ou l'encapsulation avec MDX Toolkit pour la distribution d'entreprise. Pour encapsuler des applications tierces, collaborez avec le fournisseur de votre application pour obtenir les fichiers binaires de l'application. Vous pouvez ensuite encapsuler les fichiers binaires à l'aide de l'outil MDX Toolkit.
- **Applications internes :** de nombreuses organisations ont des développeurs internes qui créent des applications fournissant des fonctionnalités spécifiques et étant développées et distribuées indépendamment au sein de l'organisation. Dans certains cas, certaines organisations peuvent également avoir des applications fournies par des éditeurs de logiciels indépendants. Vous pouvez déployer ces applications en tant qu'applications natives ou vous pouvez les conteneuriser en utilisant une solution MAM, telle que XenMobile.

  Par exemple, une organisation de soins de santé peut créer une application interne qui permet aux médecins de consulter les informations sur les patients à partir d'appareils mobiles. Une organisation peut ensuite sécuriser les informations des patients et activer l'accès VPN à la base de données des patients en utilisant l'une des méthodes suivantes :
  - SDK MAM
  - MDX Toolkit
- **Applications Web et Saas :** ces applications comprennent les applications accessibles à partir d'un réseau interne (applications web) ou sur un réseau public (SaaS). XenMobile vous permet également de créer des applications Web et SaaS personnalisées à l'aide d'une liste de connecteurs d'applications. Ces connecteurs d'application peuvent faciliter l'authentification unique (SSO) aux applications Web existantes. Pour de plus amples informations, consultez la section Types de connecteur d'application. Par exemple, vous pouvez utiliser Google Apps

SAML pour l'authentification unique basée sur le langage SAML (Security Assertion Markup Language) de Google Apps.

- **Applications de productivité mobiles Citrix :** il s'agit d'applications développées par Citrix et incluses avec la licence XenMobile. Pour plus de détails, consultez la section À propos des applications de productivité mobiles. Citrix propose également d'autres applications prêtes à l'emploi que les éditeurs de logiciels indépendants peuvent développer à l'aide du SDK Mobile Apps.
- **Applications HDX :** il s'agit d'applications hébergées par Windows que vous publiez avec StoreFront. Si vous utilisez Citrix Virtual Apps and Desktops et Citrix Workspace, les applications HDX sont disponibles pour les utilisateurs inscrits.

Selon le type d'applications mobiles que vous prévoyez de déployer et de gérer avec XenMobile, la configuration sous-jacente peut varier. Par exemple, si plusieurs groupes d'utilisateurs ayant un niveau d'autorisation différent utilisent une même application, vous pouvez créer des groupes de mise à disposition distincts pour déployer deux versions distinctes de la même application. Vous devez par ailleurs vous assurer que l'appartenance au groupe d'utilisateurs est mutuellement exclusive pour éviter les incohérences de stratégie sur les appareils des utilisateurs.

Vous pouvez également gérer les licences d'applications iOS à l'aide de l'achat en volume d'Apple. Vous devrez pour cela vous inscrire au programme d'achat en volume et configurer les paramètres d'achat en volume dans la console XenMobile. Cette configuration vous permet de distribuer les applications avec les licences d'achat en volume. Avec une telle variété de cas d'utilisation, il est important d'évaluer et de planifier votre stratégie MAM avant la mise en œuvre de l'environnement XenMobile. Vous pouvez commencer à planifier votre stratégie MAM en définissant les éléments suivants :

- **Types d'applications :** répertoriez les différents types d'applications que vous souhaitez prendre en charge et catégorisez-les, tels que public, natif, Web, interne ou applications d'éditeurs de logiciels indépendants. En outre, catégorisez les applications selon différentes plates-formes d'appareils, telles que iOS et Android. Cette catégorisation permet d'aligner les différents paramètres XenMobile requis pour chaque type d'application. Par exemple, certaines applications peuvent nécessiter l'utilisation du SDK Mobile Apps pour activer des API spéciales pour l'interaction avec d'autres applications.
- **Exigences en matière de réseau :** configurez les paramètres d'applications avec des exigences d'accès réseau spécifiques. Par exemple, certaines applications peuvent nécessiter l'accès à votre réseau interne via VPN. Certaines applications peuvent nécessiter un accès Internet pour acheminer l'accès via la DMZ. Pour permettre à ces applications de se connecter au réseau requis, vous devez configurer divers paramètres en conséquence. La définition des exigences réseau par application vous aide à finaliser vos décisions architecturales dès le début, ce qui simplifie le processus de mise en œuvre global.
- **Exigences en matière de sécurité :** vous pouvez définir des exigences de sécurité qui

s'appliquent à des applications individuelles ou à toutes les applications.

  - Les paramètres, tels que les stratégies MDX, s'appliquent à des applications individuelles
  - Les paramètres de session et d'authentification s'appliquent à toutes les applications
  - Certaines applications peuvent avoir des exigences spécifiques en matière de conteneurisation, de MDX, d'authentification, de géofencing, de code d'accès ou de partage de données

Définissez ces exigences à l'avance afin de simplifier votre déploiement. Pour de plus amples informations sur la sécurité dans Endpoint Management, consultez la section Sécurité et expérience utilisateur.

- **Exigences en matière de déploiement :** vous pouvez utiliser un déploiement basé sur des stratégies pour autoriser le téléchargement des applications publiées uniquement par des utilisateurs compatibles. Par exemple, certaines applications peuvent exiger que l'appareil soit géré ou que l'appareil corresponde à une version minimale du système d'exploitation. Vous pouvez également exiger que certaines applications soient uniquement disponibles pour les utilisateurs d'entreprise. Définissez ces exigences à l'avance afin de pouvoir configurer les stratégies ou les actions de déploiement appropriées.
- **Exigences en matière de licence :** enregistrez les exigences en matière de licence liées à l'application. Vos notes peuvent vous aider à gérer efficacement l'utilisation des licences et à décider si vous devez configurer des fonctionnalités spécifiques dans XenMobile pour faciliter l'attribution de licences. Par exemple, si vous déployez une application iOS gratuite ou payante, Apple applique les exigences de licence sur l'application. Par conséquent, les utilisateurs doivent se connecter à leur compte Apple App Store.

  Cependant, vous pouvez vous inscrire à l'achat en volume d'Apple pour distribuer et gérer ces applications via XenMobile. L'achat en volume permet aux utilisateurs de télécharger les applications sans se connecter à leur compte Apple App Store.

  Certaines plates-formes telles que Samsung SAFE et Samsung Knox présentent des exigences de licence spéciales qui doivent être satisfaites avant le déploiement de ces fonctionnalités.
- **Exigences en matière de liste d'autorisation/liste de blocage :** vous pouvez identifier des applications que les utilisateurs ne doivent pas installer ou utiliser. La création d'une liste de blocage définit un événement hors conformité. Vous pouvez ensuite configurer des stratégies pour qu'elles se déclenchent lorsque l'événement se produit. D'un autre côté, une application peut être acceptable pour une utilisation, mais peut tomber sous la liste de blocage pour une raison quelconque. Dans ce cas, vous pouvez ajouter l'application à une liste d'autorisation et indiquer que l'utilisation de l'application est acceptable mais n'est pas requise. De plus, gardez à l'esprit que les applications préinstallées sur les nouveaux appareils peuvent inclure certaines applications couramment utilisées qui ne font pas partie du système d'exploitation. De telles applications peuvent entrer en conflit avec votre stratégie de liste de blocage.

Cas d'utilisation

Une organisation de soins de santé prévoit de déployer XenMobile en tant que solution MAM pour leurs applications mobiles. Les applications mobiles sont mises à disposition des utilisateurs professionnels et BYOD. Le département informatique décide de mettre à disposition et de gérer les applications suivantes :

Applications de productivité mobiles : applications iOS et Android fournies par Citrix. Pour plus de détails, consultez la section Applications de productivité mobiles.

Citrix Secure Hub : client utilisé par tous les appareils mobiles pour communiquer avec XenMobile. Vous envoyez les paramètres de sécurité, les configurations et les applications mobiles vers les appareils mobiles via Secure Hub. Les appareils Android et iOS s'inscrivent dans XenMobile via Secure Hub.

Citrix Receiver : application mobile permettant aux utilisateurs d'appareils mobiles d'ouvrir des applications hébergées par Citrix Virtual Apps.

GoToMeeting : un client de réunion, de partage de bureau et de visioconférence en ligne qui permet aux utilisateurs de se rencontrer en temps réel avec d'autres utilisateurs, clients ou collègues via Internet.

SalesForce1 : Salesforce1 permet aux utilisateurs d'accéder à Salesforce à partir d'appareils mobiles et rassemble toutes les applications Chatter, CRM et applications personnalisées, ainsi que les processus d'entreprise, pour une expérience unifiée pour tout utilisateur Salesforce.

RSA SecurID : jeton logiciel pour l'authentification à deux facteurs.

Applications EpicCare : ces applications offrent aux professionnels de la santé un accès sécurisé et portable aux dossiers des patients, aux listes de patients, aux calendriers et aux messages.

Haiku : application mobile pour les téléphones iPhone et Android.

Canto : application mobile pour l'iPad.

Rover : applications mobiles pour iPhone et l'iPad.

HDX : Citrix Virtual Apps fournit les applications HDX.

- **Epic Hyperspace :** application Epic client pour la gestion électronique des dossiers de santé.

ISV :

- **Vocera :** application VoIP et de messagerie compatible HIPAA qui étend les avantages de la technologie vocale Vocera à tout moment, n'importe où, via l'iPhone et les smartphones Android.

Applications internes :

- **HCMail :** application qui permet de composer des messages cryptés, d'effectuer des recherches dans des carnets d'adresses sur des serveurs de messagerie internes et d'envoyer les messages cryptés aux contacts à l'aide d'un client de messagerie.

Applications web internes :

- **PatientRounding :** application Web utilisée pour enregistrer les informations sur la santé des patients par différents départements.
- **Outlook Web Access :** permet l'accès à la messagerie via un navigateur Web.
- **SharePoint :** utilisé pour le partage de fichiers et de données à l'échelle de l'organisation.

Le tableau suivant répertorie les informations de base requises pour la configuration MAM.

Nom de l'application	Type d'application	Intégration du SDK MAM ou encapsulation MDX	iOS	Android
Secure Mail	Applications XenMobile	Pas pour la version 10.4.1 et versions ultérieures	Oui	Oui
Secure Web	Applications XenMobile	Pas pour la version 10.4.1 et versions ultérieures	Oui	Oui
Citrix Files	Applications XenMobile	Pas pour la version 10.4.1 et versions ultérieures	Oui	Oui
Secure Hub	Application publique	S.O.	Oui	Oui
Citrix Receiver	Application publique	S.O.	Oui	Oui
GoToMeeting	Application publique	S.O.	Oui	Oui
SalesForce1	Application publique	S.O.	Oui	Oui
RSA SecurID	Application publique	S.O.	Oui	Oui
Epic Haiku	Application publique	S.O.	Oui	Oui

Epic Canto	Application publique	S.O.	Oui	Non
Epic Rover	Application publique	S.O.	Oui	Non
Epic Hyperspace	Application HDX	S.O.	Oui	Oui
Vocera	Application d'éditeur de logiciels indépendant	Oui	Oui	Oui
HCMail	Application interne	Oui	Oui	Oui
PatientRounding	Application Web	S.O.	Oui	Oui
Outlook Web Access	Application Web	S.O.	Oui	Oui
SharePoint	Application Web	S.O.	Oui	Oui

Le tableau suivant répertorie les exigences spécifiques que vous pouvez consulter en configurant les stratégies MAM dans XenMobile.

Nom de l'application	VPN requis	Interaction (avec des applications en dehors du conteneur)	Interaction (à partir d'applications en dehors du conteneur)	Filtrage par proxy	Gestion des licences	Géofencing	SDK Applications mobiles	Version du système d'exploitation minimum
Secure Mail	O	Autorisé de manière sélective	Autorisé	Requis	S.O.	Requis de manière sélective	S.O.	Appliqué
Secure Web	O	Autorisé	Autorisé	Requis	S.O.	Non requis	S.O.	Appliqué

Nom de l'application	VPN requis	Interaction (avec des applications en dehors du conteneur)	Interaction (à partir d'applications en dehors du conteneur)	Filtrage par proxy	Gestion des licences	Géofencing	SDK Applications mobiles	Version du système d'exploitation minimum
Citrix Files	O	Autorisé	Autorisé	Requis	S.O.	Non requis	S.O.	Appliqué
Secure Hub	O	S.O.	S.O.	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
Citrix Receiver	O	S.O.	S.O.	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
GoToMeetin	Ng	S.O.	S.O.	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
SalesForc	N	S.O.	S.O.	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
RSA SecurID	N	S.O.	S.O.	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
Epic Haiku	O	S.O.	S.O.	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
Epic Canto	O	S.O.	S.O.	Non requis	Achat en volume	Non requis	S.O.	Non appliqué
Epic Rover	O	S.O.	S.O.	Non requis	Achat en volume	Non requis	S.O.	Non appliqué

Nom de l'application	VPN requis	Interaction (avec des applications en dehors du conteneur)	Interaction (à partir d'applications en dehors du conteneur)	Filtrage par proxy	Gestion des licences	Géofencing	SDK Applications mobiles	Version du système d'exploitation minimum
Epic Hyperspace	O	S.O.	S.O.	Non requis	S.O.	Non requis	S.O.	Non appliqué
Vocera	O	Bloqué	Bloqué	Requis	S.O.	Requis	Requis	Appliqué
HCMail	O	Bloqué	Bloqué	Requis	S.O.	Requis	Requis	Appliqué
PatientRc	O	S.O.	S.O.	Requis	S.O.	Non requis	S.O.	Non appliqué
Outlook Web Access	O	S.O.	S.O.	Requis	S.O.	Non requis	S.O.	Non appliqué
SharePoi	O	S.O.	S.O.	Requis	S.O.	Non requis	S.O.	Non appliqué

Communautés d'utilisateurs

January 10, 2022

Chaque organisation est composée de diverses communautés d'utilisateurs qui opèrent dans différents rôles fonctionnels. Ces communautés d'utilisateurs exécutent différentes tâches et fonctions de bureau à l'aide de diverses ressources que vous fournissez via des appareils mobiles. Les utilisateurs peuvent travailler à domicile ou dans des bureaux distants à l'aide d'appareils mobiles que vous fournissez. Les utilisateurs peuvent également utiliser des appareils mobiles personnels, ce qui leur permet d'accéder à des outils soumis à certaines règles de conformité de sécurité.

Avec un plus grand nombre de communautés d'utilisateurs utilisant des appareils mobiles, la gestion de la mobilité d'entreprise devient essentielle pour éviter la fuite de données et pour appliquer les restrictions de sécurité de l'organisation. Pour une gestion efficace et plus sophistiquée des appareils mobiles, vous pouvez catégoriser vos communautés d'utilisateurs. Cela simplifie le mappage des util-

isateurs aux ressources et garantit que les bonnes stratégies de sécurité s'appliquent aux utilisateurs appropriés.

La catégorisation des communautés d'utilisateurs peut inclure l'utilisation des composants suivants :

- Unités d'organisation et groupes Active Directory

  Les utilisateurs ajoutés à des groupes de sécurité Active Directory spécifiques peuvent recevoir des stratégies et des ressources, telles que des applications. La suppression des utilisateurs des groupes de sécurité Active Directory supprime l'accès aux ressources XenMobile précédemment autorisé.

- Utilisateurs et groupes locaux XenMobile

  Pour les utilisateurs qui n'ont pas de compte dans Active Directory, vous pouvez créer des utilisateurs en tant qu'utilisateurs XenMobile locaux. Vous pouvez ajouter des utilisateurs locaux à des groupes de mise à disposition et leur affecter des ressources de la même manière que les utilisateurs Active Directory.

- Groupes de mise à disposition XenMobile

  Si plusieurs groupes d'utilisateurs avec différents niveaux d'autorisations doivent utiliser une seule application, vous devrez peut-être créer des groupes de mise à disposition distincts. Avec des groupes de mise à disposition distincts, vous pouvez déployer deux versions distinctes de la même application.

- Groupe de mise à disposition et mappage de groupe d'utilisateurs

  Le groupe de mise à disposition vers les mappages de groupe Active Directory peut avoir soit une relation un-à-un (one-to-one), soit une relation un-à-plusieurs (one-to-many). Attribuez des stratégies et des applications de base à un mappage de groupe de mise à disposition un-à-plusieurs. Attribuez des stratégies et des applications spécifiques à une fonction à des mappages de groupe de disposition un-à-un.

- Groupe de mise à disposition et mappage des ressources des applications

  Attribuez des applications spécifiques à chaque groupe de mise à disposition.

- Groupe de mise à disposition et mappage des ressources MDM

  Attribuez des applications et des ressources de gestion d'appareils spécifiques à chaque groupe de mise à disposition. Par exemple, configurez un groupe de mise à disposition avec une combinaison des éléments suivants : types d'applications (public, HDX, etc.), applications spécifiques par type d'application et ressources telles que les stratégies d'appareil et les actions automatisées.

L'exemple suivant illustre comment les communautés d'utilisateurs d'une organisation de soins de santé sont classées pour EMM.

Cas d'utilisation

Cet exemple d'organisation de soins de santé fournit des ressources technologiques et un accès à plusieurs utilisateurs, y compris des employés et des bénévoles du réseau et de sociétés affiliées. L'organisation a choisi de déployer la solution EMM auprès des utilisateurs non-cadres uniquement.

Vous pouvez répartir les rôles utilisateur et les fonctions de cette organisation en sous-groupes, y compris personnel médical, personnel non-médical et sous-traitants. Un ensemble sélectionné d'utilisateurs reçoit des appareils mobiles d'entreprise tandis que d'autres peuvent accéder aux ressources limitées de l'entreprise à partir de leurs appareils personnels (BYOD). Pour appliquer le niveau approprié de restrictions de sécurité et empêcher la fuite de données, l'organisation a décidé que l'informatique de l'entreprise gère chaque appareil inscrit. En outre, les utilisateurs ne peuvent inscrire qu'un seul appareil.

Les sections suivantes donnent un aperçu des rôles et des fonctions de chaque sous-groupe :

Personnel médical

- Infirmiers/Infirmières
- Médecins (docteurs, chirurgiens, etc.)
- Spécialistes (diététiciens, phlébotomistes, anesthésistes, radiologues, cardiologues, oncologues, etc.)
- Médecins externes (médecins non-employés et employés de bureau travaillant dans des bureaux éloignés)
- Services de santé à domicile (employés de bureau et travailleurs mobiles exécutant des services médicaux lors de visites à domicile auprès de patients)
- Spécialistes en recherche (travailleurs intellectuels et utilisateurs avancés dans six instituts de recherche médicale)
- Éducation et formation (infirmiers/infirmières, médecins et spécialistes en phase d'éducation et de formation)

Personnel non-médical

- Services partagés (employés de bureau effectuant diverses fonctions administratives, y compris RH, gestion des salaires, comptes fournisseurs, service de la chaîne d'approvisionnement, etc.)
- Services médicaux (employés de bureau effectuant divers services de gestion des soins de santé, services administratifs et solutions de processus commerciaux aux fournisseurs, y compris : services administratifs, analyse commerciale et intelligence économique, systèmes commerciaux, services aux clients, finances, gestion des soins, solutions d'accès patient, solutions de cycle des revenus, etc.)
- Services de support (employés de bureau remplissant diverses fonctions non-médicales, y compris : administration des avantages sociaux, intégration clinique, communications, rémunéra-

tion et gestion du rendement, services d'équipement et de site, systèmes de technologie des RH, services d'information, vérification interne et amélioration des processus, etc.)
- Programmes philanthropiques (employés de bureau et mobiles qui exécutent diverses fonctions pour soutenir les programmes philanthropiques)

Sous-traitants

- Partenaires fabricants et fournisseurs (connectés sur site et à distance via un VPN site à site fournissant diverses fonctions de support non-médical)

Sur la base des informations précédentes, l'organisation a créé les entités suivantes. Pour plus d'informations sur les groupes de mise à disposition dans XenMobile, consultez la section Déployer des ressources dans la documentation XenMobile.

Unités d'organisation et groupes Active Directory

Unité d'organisation = Ressources XenMobile

- Unité d'organisation = personnel médical ; Groupes =
  - XM - Infirmiers/Infirmières
  - XM - Médecins
  - XM - Spécialistes
  - XM - Médecins externes
  - XM - Services de santé à domicile
  - XM - Spécialistes en recherche
  - XM - Éducation et formation
- Unité d'organisation = non-médical ; Groupes =
  - XM - Services partagés
  - XM - Services médicaux
  - XM - Services de support
  - XM - Programmes philanthropiques

Utilisateurs et groupes locaux XenMobile

Groupe = sous-traitants ; Utilisateurs =

- Fournisseur 1
- Fournisseur 2
- Fournisseur 3
- … Fournisseur 10

Groupes de mise à disposition XenMobile

- Personnel médical - Infirmiers/Infirmières
- Personnel médical - Médecins
- Personnel médical - Spécialistes
- Personnel médical - Médecins externes
- Personnel médical - Services de santé à domicile
- Personnel médical - Spécialistes en recherche
- Personnel médical - Éducation et formation
- Personnel non-médical - Services partagés
- Personnel non-médical - Services médicaux
- Personnel non-médical - Services de support
- Personnel non-médical - Programmes philanthropiques

Groupe de mise à disposition et mappage de groupe d'utilisateurs

Groupes Active Directory	Groupes de mise à disposition XenMobile
XM - Infirmiers/Infirmières	Personnel médical - Infirmiers/Infirmières
XM - Médecins	Personnel médical - Médecins
XM - Spécialistes	Personnel médical - Spécialistes
XM - Médecins externes	Personnel médical - Médecins externes
XM - Services de santé à domicile	Personnel médical - Services de santé à domicile
XM - Spécialistes en recherche	Personnel médical - Spécialistes en recherche
XM - Éducation et formation	Personnel médical - Éducation et formation
XM - Services partagés	Personnel non-médical - Services partagés
XM - Services médicaux	Personnel non-médical - Services médicaux
XM - Services de support	Personnel non-médical - Services de support
XM - Programmes philanthropiques	Personnel non-médical - Programmes philanthropiques

Groupe de mise à disposition et mappage des ressources des applications

	Secure Mail	Secure Web	ShareFil	Receiver	SalesFor	RSA Se-curID	EpicCare Haiku	Epic Hyper-space
Personnel médi-cal - Infir-mier-s/Infir-mières	X	X	X					
Personne médi-cal - Médecins								
Personnel médi-cal - Spécial-istes								
Personne médi-cal - Médecins ex-ternes	X		X					
Personnel médi-cal - Ser-vices de santé à domi-cile	X		X					

Personnel médical - Spécialistes en recherche	X	X				
Personnel médical - Éducation et formation					X	X
Personnel non-médical - Services partagés					X	X
Personnel non-médical - Services médicaux					X	X
Personnel non-médical - Services de support	X	X			X	X

Personnel non-médical - Programmes philanthropiques	X		X			X	X
Sous-traitants	X		X	X	X	X	X

Groupe de mise à disposition et mappage des ressources MDM

	MDM : Stratégie de code secret	MDM : Restrictions d'appareil	MDM : Actions automatisées	Stratégie Wi-Fi
Personnel médical - Infirmiers/Infirmières				X
Personnel médical - Médecins		X		
Personnel médical - Spécialistes				
Personnel médical - Médecins externes				
Personnel médical - Services de santé à domicile				

Personnel médical - Spécialistes en recherche		
Personnel médical - Éducation et formation		
Personnel non-médical - Services partagés		
Personnel non-médical - Services médicaux		
Personnel non-médical - Services de support		
Personnel non-médical - Programmes philanthropiques		
Sous-traitants	X	

Notes et considérations

- XenMobile crée un groupe de mise à disposition par défaut appelé Tous les utilisateurs lors de la configuration initiale. Si vous ne désactivez pas de ce groupe de mise à disposition, tous les utilisateurs Active Directory ont le droit de s'inscrire à XenMobile.
- XenMobile synchronise les utilisateurs et les groupes Active Directory à la demande en utilisant une connexion dynamique au serveur LDAP.
- Si un utilisateur fait partie d'un groupe qui n'est pas mappé dans XenMobile, cet utilisateur ne peut pas s'inscrire. De même, si un utilisateur est membre de plusieurs groupes, XenMobile catégorise uniquement l'utilisateur comme étant dans les groupes mappés à XenMobile.

- Pour rendre l'inscription MDM obligatoire, définissez l'option **Inscription requise** sur **Vrai** dans **Propriétés du serveur** dans la console XenMobile. Pour de plus amples informations, consultez la section Propriétés du serveur.
- Pour supprimer un groupe d'utilisateurs d'un groupe de mise à disposition XenMobile, supprimez l'entrée dans la base de données SQL Server, sous dbo.userlistgrps.

> **Attention :**
>
> Avant d'effectuer cette action, créez une copie de sauvegarde de XenMobile et de la base de données.

À propos de l'appartenance des appareils dans XenMobile Device

Vous pouvez regrouper les utilisateurs en fonction du propriétaire d'un appareil utilisateur. L'appartenance des appareils comprend les appareils appartenant à l'entreprise et les appareils appartenant aux utilisateurs, un programme plus communément appelé Apportez votre propre appareil (BYOD). Vous pouvez contrôler la façon dont les appareils BYOD se connectent à votre réseau à deux endroits dans la console XenMobile : sur la page Règles de déploiement et via les propriétés du serveur XenMobile sur la page **Paramètres**. Pour de plus amples informations sur les règles de déploiement, consultez la section Déployer des ressources dans la documentation XenMobile. Pour de plus amples informations sur les propriétés de serveur, consultez la section Propriétés du serveur dans ce guide.

En définissant les propriétés du serveur, vous pouvez demander à tous les utilisateurs BYOD d'accepter que leurs appareils soient gérés par l'entreprise avant qu'ils puissent accéder à des applications. Vous pouvez également autoriser les utilisateurs à accéder aux applications d'entreprise sans gérer leurs appareils.

Lorsque vous définissez la propriété de serveur **wsapi.mdm.required.flag** sur **Vrai**, tous les appareils BYOD sont gérés par XenMobile et tout utilisateur refusant l'inscription se voit refuser l'accès aux applications. Le paramétrage de **wsapi.mdm.required.flag** sur **Vrai** doit être envisagé dans les environnements dans lesquels les équipes informatiques ont besoin d'un haut niveau de sécurité avec une expérience utilisateur positive lors de l'inscription.

Si vous laissez la propriété **wsapi.mdm.required.flag** sur **faux** (paramètre par défaut), les utilisateurs peuvent refuser l'inscription. Toutefois, ils peuvent accéder aux applications sur leurs appareils via XenMobile Store. Le paramétrage de **wsapi.mdm.required.flag** sur **Faux** doit être envisagé dans les environnements dans lesquels les contraintes juridiques, de confidentialité et imposées par la législation ne requièrent pas la gestion des appareils mais uniquement la gestion des applications d'entreprise.

Les utilisateurs équipés d'appareils qui ne sont pas gérés peuvent installer des applications via XenMobile Store. À la place des contrôles au niveau de l'appareil, comme l'effacement partiel ou com-

plet, vous contrôlez l'accès aux applications via des stratégies d'application. Certaines stratégies requièrent que l'appareil vérifie régulièrement XenMobile Server pour confirmer que les applications sont toujours autorisées à s'exécuter.

Stratégie de messagerie

January 10, 2022

L'accès sécurisé aux e-mails à partir d'appareils mobiles est l'un des principaux moteurs de l'initiative de gestion de la mobilité de toute organisation. Décider de la bonne stratégie de messagerie est souvent un élément clé de toute conception XenMobile. XenMobile offre plusieurs options pour prendre en charge différents cas d'utilisation, en fonction de la sécurité, de l'expérience utilisateur et de l'intégration requises. Cet article couvre le processus de décision type pour la conception et les points à prendre en compte pour choisir la bonne solution, de la sélection du client à la circulation du courrier.

Choisir vos clients de messagerie

La sélection des clients est généralement une priorité pour la conception globale de la stratégie de messagerie. Vous pouvez choisir parmi plusieurs clients : Citrix Secure Mail, la messagerie native fournie avec un système d'exploitation de plateforme mobile particulier ou d'autres clients tiers disponibles via les magasins d'applications publics. En fonction de vos besoins, vous pouvez éventuellement prendre en charge les communautés d'utilisateurs avec un seul client (standard) ou utiliser une combinaison de clients.

Le tableau suivant présente des considérations de conception pour les différentes options client disponibles :

Rubrique	Secure Mail	Natif (par exemple, iOS Mail)	Messagerie tierce
Édition XenMobile minimale	Advanced	MDM	MDM

Configuration	Profils de compte Exchange configurés via une stratégie MDX.	Profils de compte Exchange configurés via une stratégie MDM. La prise en charge d'Android est limitée à : SAFE/KNOX et Android Enterprise. Tous les autres clients sont considérés comme des clients tiers.	Nécessite généralement une configuration manuelle par l'utilisateur.
Sécurité	Sécurisé de par sa conception, offrant la plus haute sécurité. Utilise les stratégies MDX avec des niveaux de cryptage de données supplémentaires. Secure Mail est une application entièrement gérée via une stratégie MDX. Couche d'authentification supplémentaire avec code PIN Citrix.	Basé sur l'ensemble de fonctionnalités fournisseur/application. Fournit une sécurité plus élevée. Utilise les paramètres de chiffrement de l'appareil (sans sécurité via les stratégies MDX). S'appuie sur l'authentification au niveau de l'appareil pour accéder à l'application.	Basé sur l'ensemble de fonctionnalités fournisseur/application. Fournit une sécurité élevée.

Intégration	Permet l'interaction avec les applications gérées (MDX) par défaut. Ouverture d'URL Web avec Citrix Secure Web. Enregistrement des fichiers dans Citrix Files et fichiers en pièce jointe à partir de Citrix Files. Connexion directe à GoToMeeting.	Ne peut interagir qu'avec d'autres applications non gérées (non-MDX) par défaut.	Ne peut interagir qu'avec d'autres applications non gérées (non-MDX) par défaut.
Déploiement/Licence	Vous pouvez utiliser Secure Mail via MDM, directement depuis les magasins d'applications publics. Inclus avec les licences XenMobile Advanced et Enterprise.	Application client incluse avec le système d'exploitation de la plateforme. Aucune licence supplémentaire requise.	Peut être déployé par push via MDM, en tant qu'application d'entreprise ou directement à partir des magasins d'applications publics. Modèle/coûts de licence associés basés sur le fournisseur de l'application.

Support	Prise en charge d'un fournisseur unique pour le client et la solution EMM (Citrix). Informations de contact d'assistance intégrées dans les fonctionnalités de journalisation de débogage Secure Hub/application. Assistance pour un seul client.	Assistance définie par le fournisseur (Apple/Google). Une assistance pour différents clients peut être nécessaire en fonction de la plate-forme de l'appareil.	Assistance définie par le fournisseur. Assistance pour un seul client, en supposant que le client tiers est pris en charge sur toutes les plates-formes des appareils gérés.

Flux et filtrage du trafic de messagerie

Cette section présente les trois scénarios principaux et les points à prendre en compte pour la conception concernant le flux du trafic de messagerie (ActiveSync) dans le contexte de XenMobile.

Scénario 1 : Exchange exposé

Les environnements prenant en charge des clients externes disposent généralement de services Exchange ActiveSync exposés sur Internet. Les clients Mobile ActiveSync se connectent via ce chemin externe via un proxy inverse (Citrix ADC, par exemple) ou via un serveur Edge. Cette option est requise pour l'utilisation de clients de messagerie natifs ou tiers, ce qui fait de ces clients l'option de choix pour ce scénario. Bien que ce ne soit pas une pratique courante, vous pouvez également utiliser le client Secure Mail dans ce scénario. Ce faisant, vous bénéficiez des fonctionnalités de sécurité offertes par l'utilisation des stratégies MDX et de la gestion de l'application.

Scénario 2 : Tunneling via Citrix ADC (micro VPN et STA)

Ce scénario est le scénario par défaut lors de l'utilisation du client Secure Mail, en raison de ses capacités micro VPN. Dans ce cas, le client Secure Mail établit une connexion sécurisée à ActiveSync via Citrix Gateway. En substance, vous pouvez considérer Secure Mail comme le client se connectant directement à ActiveSync à partir du réseau interne. Les clients Citrix standardisent souvent Secure Mail comme client mobile ActiveSync de leur choix. Cette décision fait partie d'une initiative visant

à éviter d'exposer les services ActiveSync à Internet sur un serveur Exchange exposé, comme décrit dans le premier scénario.

Seules les applications sur lesquelles le SDK MAM est activé ou encapsulées avec le MDX peuvent utiliser la fonction micro VPN. Ce scénario ne s'applique pas aux clients natifs si vous utilisez un encapsulage MDX. Même s'il est possible d'encapsuler les clients tiers avec MDX Toolkit, cette pratique n'est pas courante. L'utilisation de clients VPN au niveau des appareils pour permettre l'accès par tunnel aux clients natifs ou tiers s'est avérée fastidieuse et n'est pas une solution viable.

Scénario 3 : Services Exchange hébergés sur le cloud

Les services Exchange hébergés sur le cloud, tels que Microsoft Office 365, gagnent en popularité. Dans le contexte de XenMobile, ce scénario peut être traité de la même manière que le premier scénario, car le service ActiveSync est également exposé sur Internet. Dans ce cas, les exigences des fournisseurs de services cloud dictent les choix des clients. Ces choix incluent généralement la prise en charge de la plupart des clients ActiveSync, tels que Secure Mail et d'autres clients natifs ou tiers.

La solution XenMobile peut être avantageuse dans trois domaines pour ce scénario :

- Clients avec stratégies MDX et gestion des applications avec Secure Mail
- Configuration du client avec l'utilisation d'une stratégie MDM sur les clients de messagerie pris en charge
- Options de filtrage ActiveSync avec Endpoint Management Connector pour Exchange ActiveSync

Filtrage du trafic de messagerie

Comme avec la plupart des services exposés sur Internet, vous devez sécuriser le chemin et fournir un filtrage pour un accès autorisé. La solution XenMobile comprend deux composants conçus spécifiquement pour fournir des fonctionnalités de filtrage ActiveSync aux clients natifs et tiers : Citrix Gateway Connector pour Exchange ActiveSync et Endpoint Management Connector pour Exchange ActiveSync.

Citrix Gateway Connector pour Exchange ActiveSync

Citrix Gateway Connector pour Exchange ActiveSync fournit un filtrage ActiveSync sur le périmètre en utilisant Citrix ADC comme proxy pour le trafic ActiveSync. Le composant de filtrage se trouve donc sur le chemin du flux de trafic de messagerie, interceptant le courrier à l'entrée ou à la sortie de l'environnement. Citrix Gateway Connector pour Exchange ActiveSync agit comme un intermédiaire entre Citrix ADC et XenMobile Server. Lorsqu'un appareil communique avec Exchange via le serveur virtuel ActiveSync sur Citrix ADC, Citrix ADC envoie un appel HTTP au connecteur pour le service Exchange ActiveSync. Ce service vérifie ensuite l'état de l'appareil auprès de XenMobile. En fonction

de l'état de l'appareil, le connecteur pour Exchange ActiveSync répond à Citrix ADC d'autoriser ou de refuser la connexion. Vous pouvez également configurer des règles statiques pour filtrer l'accès en fonction de l'utilisateur, de l'agent et du type ou de l'ID de l'appareil.

Cette configuration permet aux services Exchange ActiveSync d'être exposés sur Internet avec une couche de sécurité supplémentaire pour empêcher tout accès non autorisé. Les points à prendre en compte pour la conception sont les suivants :

- Windows Server : le connecteur pour Exchange ActiveSync nécessite un serveur Windows Server.
- Ensemble de règles de filtrage : le connecteur pour Exchange ActiveSync est conçu pour le filtrage basé sur l'état et les informations de l'appareil, plutôt que sur les informations de l'utilisateur. Bien que vous puissiez configurer des règles statiques pour filtrer par ID utilisateur, aucune option n'existe pour le filtrage basé sur l'appartenance à un groupe Active Directory, par exemple. Si le filtrage de groupe Active Directory est requis, vous pouvez utiliser Endpoint Management Connector pour Exchange ActiveSync à la place.
- Évolutivité Citrix ADC : étant donné que le trafic ActiveSync doit utiliser un proxy via Citrix ADC, le dimensionnement correct de l'instance Citrix ADC est essentiel pour prendre en charge la charge de travail supplémentaire de toutes les connexions SSL ActiveSync.
- Mise en cache intégrée Citrix ADC : la configuration du connecteur pour Exchange ActiveSync sur Citrix ADC utilise la fonction de mise en cache intégrée pour mettre en cache les réponses du connecteur pour Exchange ActiveSync. Avec cette configuration, Citrix ADC n'a pas besoin d'envoyer une demande à Citrix Gateway Connector pour Exchange ActiveSync pour chaque transaction ActiveSync dans une session donnée. Cette configuration est également essentielle pour des performances et une montée en charge adéquates. La mise en cache intégrée est disponible avec Citrix ADC Platinum Edition ou vous pouvez acquérir la licence séparément pour les éditions Enterprise.
- Stratégies de filtrage personnalisées : vous devrez peut-être créer des stratégies Citrix ADC personnalisées pour restreindre certains clients ActiveSync en dehors des clients mobiles natifs standard. Cette configuration nécessite des connaissances sur les requêtes HTTP ActiveSync et la création de stratégies de répondeur Citrix ADC.
- Clients Secure Mail : Secure Mail dispose de fonctionnalités micro VPN qui éliminent le besoin de filtrage sur le périmètre. Le client Secure Mail est généralement traité comme un client ActiveSync interne (de confiance) lorsqu'il est connecté via Citrix Gateway. Si la prise en charge de clients natifs et tiers (avec le connecteur pour Exchange ActiveSync) et Secure Mail est requise : Citrix recommande de ne pas acheminer le trafic Secure Mail via le serveur virtuel Citrix ADC utilisé pour le connecteur pour Exchange ActiveSync. Vous pouvez acheminer ce flux de trafic via DNS et empêcher la stratégie du connecteur pour Exchange ActiveSync d'affecter les clients Secure Mail.

Vous trouverez un diagramme de Citrix Gateway Connector pour Exchange ActiveSync dans un déploiement XenMobile dans la section Architecture de référence pour les déploiements sur site.

Endpoint Management Connector pour Exchange ActiveSync

Endpoint Management Connector pour Exchange ActiveSync est un composant de XenMobile qui fournit un filtrage ActiveSync au niveau du service Exchange. Par conséquent, le filtrage ne se produit qu'une fois que le courrier parvient au service Exchange, et non lorsqu'il entre dans l'environnement XenMobile. Mail Manager utilise PowerShell pour interroger Exchange ActiveSync sur les informations de partenariat d'appareil et contrôler l'accès via des actions de mise en quarantaine des appareils. Ces actions mettent des appareils en quarantaine et les sortent de la quarantaine en fonction des critères de règle d'Endpoint Management Connector pour Exchange ActiveSync. De la même manière que Citrix Gateway Connector pour Exchange ActiveSync, Endpoint Management Connector pour Exchange ActiveSync vérifie l'état de l'appareil auprès de XenMobile pour filtrer l'accès en fonction de la conformité des appareils. Vous pouvez également configurer des règles statiques pour filtrer l'accès en fonction du type ou de l'ID de l'appareil, de la version de l'agent et de l'appartenance à un groupe Active Directory.

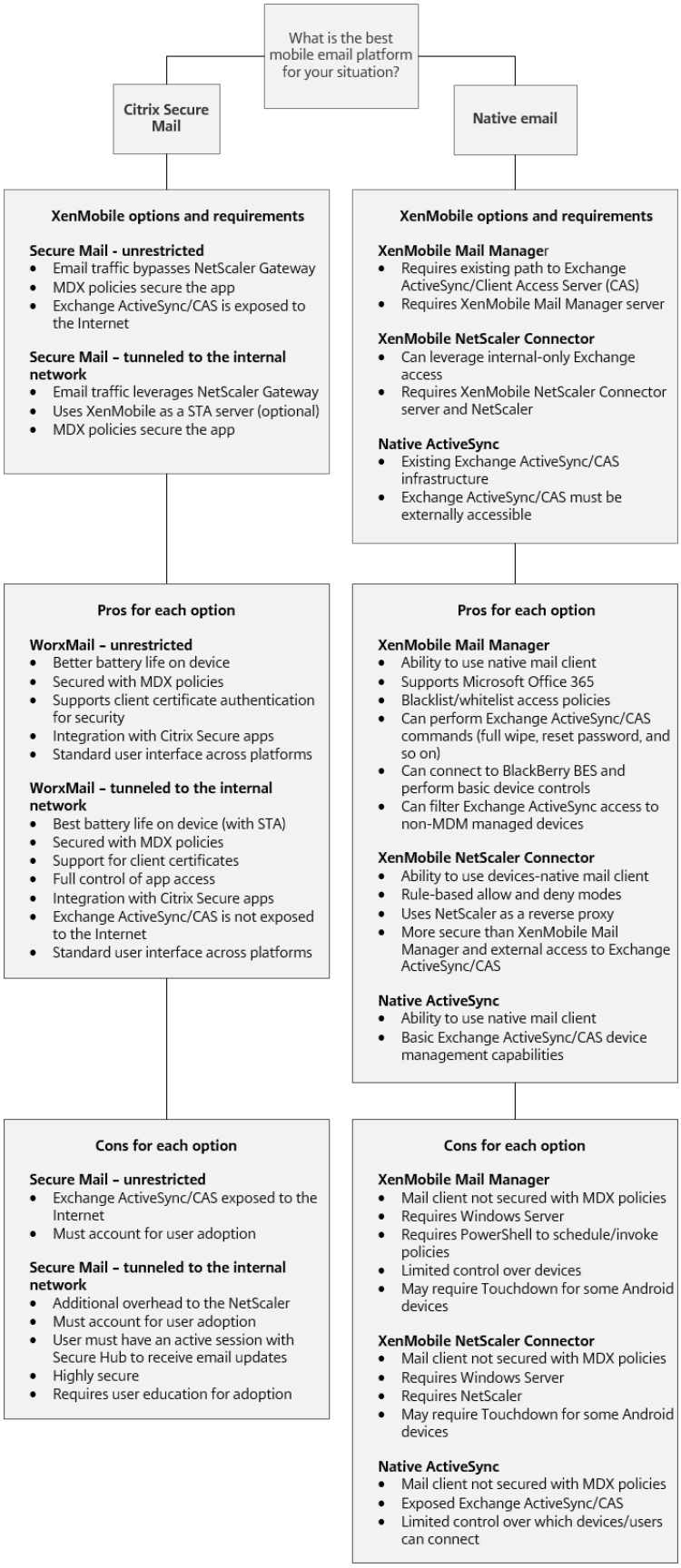
Cette solution ne nécessite pas l'utilisation de Citrix ADC. Vous pouvez déployer Endpoint Management Connector pour Exchange ActiveSync sans modifier le routage du trafix ActiveSync existant. Les points à prendre en compte pour la conception sont les suivants :

- Windows Server : Endpoint Management Connector pour Exchange ActiveSync nécessite le déploiement de Windows Server.
- Ensemble de règles de filtrage : tout comme Citrix Gateway Connector pour Exchange ActiveSync, Endpoint Management Connector pour Exchange ActiveSync inclut des règles de filtrage pour évaluer l'état des appareils. En outre, Endpoint Management Connector pour Exchange ActiveSync prend également en charge les règles statiques pour filtrer en fonction de l'appartenance à un groupe Active Directory.
- Intégration Exchange : Endpoint Management Connector pour Exchange ActiveSync requiert un accès direct au serveur d'accès du client Exchange (CAS) hébergeant le rôle ActiveSync et le contrôle des actions de mise en quarantaine des appareils. Cette exigence pourrait présenter un défi selon l'architecture de l'environnement et les méthodes de sécurité. Il est essentiel d'évaluer cette exigence technique dès le départ.
- Autres clients ActiveSync : étant donné qu'Endpoint Management Connector pour Exchange ActiveSync filtre au niveau du service ActiveSync, tenez compte des autres clients ActiveSync hors de l'environnement XenMobile. Vous pouvez configurer des règles statiques Endpoint Management Connector pour Exchange ActiveSync pour éviter tout impact involontaire sur d'autres clients ActiveSync.
- Fonctions Exchange étendues : grâce à l'intégration directe avec Exchange ActiveSync, Endpoint Management Connector pour Exchange ActiveSync permet à XenMobile d'effectuer un effacement Exchange ActiveSync sur un appareil mobile. Endpoint Management Connector pour Exchange ActiveSync permet également à XenMobile d'accéder aux informations sur les appareils Blackberry et d'effectuer d'autres opérations de contrôle.

Vous trouverez un diagramme d'Endpoint Management Connector pour Exchange ActiveSync dans un déploiement XenMobile dans la section Architecture de référence pour les déploiements sur site.

Arbre de décision pour la plateforme de messagerie

La figure suivante vous aide à distinguer les avantages et les inconvénients de l'utilisation de solutions de messagerie natives ou Secure Mail dans votre déploiement XenMobile. Chaque choix permet aux options et aux exigences XenMobile associées d'activer l'accès au serveur, au réseau et à la base de données. Les avantages et inconvénients incluent des détails sur les considérations concernant la sécurité, la stratégie et l'interface utilisateur.



Intégration de XenMobile

January 10, 2022

Cet article décrit les éléments à prendre en compte lors de la planification de l'intégration de XenMobile à votre réseau et à vos solutions. Par exemple, si vous utilisez déjà Citrix ADC pour Citrix Virtual Apps and Desktops :

- Devez-vous utiliser l'instance existante de Citrix ADC ou une nouvelle instance dédiée ?
- Voulez-vous intégrer à XenMobile les applications HDX publiées avec StoreFront ?
- Avez-vous l'intention d'utiliser Citrix Files avec XenMobile ?
- Avez-vous une solution de contrôle d'accès réseau que vous souhaitez intégrer dans XenMobile ?
- Déployez-vous des serveurs proxy Web pour tout le trafic sortant de votre réseau ?

Citrix ADC et Citrix Gateway

Citrix Gateway est obligatoire pour les modes ENT et MAM de XenMobile. Citrix Gateway fournit un chemin micro VPN pour l'accès à toutes les ressources de l'entreprise et fournit une prise en charge de l'authentification forte à multi-facteurs. L'équilibrage de charge Citrix ADC est requis pour tous les modes d'appareil XenMobile Server :

- Si vous avez plusieurs instances de XenMobile Server.
- Ou, si XenMobile Server est à l'intérieur de votre zone démilitarisée ou réseau interne (et donc le trafic circule des appareils vers Citrix ADC vers XenMobile).

Vous pouvez utiliser des instances Citrix ADC existantes ou en configurer de nouvelles pour XenMobile. Les sections suivantes expliquent les avantages et les inconvénients de l'utilisation d'instances Citrix ADC dédiées existantes ou nouvelles.

Instance MPX Citrix ADC partagée avec une adresse IP virtuelle (VIP) Citrix Gateway créée pour XenMobile

Avantages :

- Utilise une instance Citrix ADC commune pour toutes les connexions distantes Citrix : Citrix Virtual Apps and Desktops, VPN complet et VPN sans client.
- Utilise les configurations Citrix ADC existantes, telles que l'authentification par certificat et l'accès à des services tels que DNS, LDAP et NTP.
- Utilise une seule licence de plateforme Citrix ADC.

Inconvénients :

- Il est plus difficile de planifier l'échelle du déploiement lorsque vous gérez deux cas d'utilisation très différents sur la même instance Citrix ADC.
- Parfois, vous avez besoin d'une version spécifique de Citrix ADC pour une utilisation spécifique de Citrix Virtual Apps and Desktops. Cette même version peut présenter des problèmes connus pour XenMobile. Ou XenMobile peut présenter des problèmes connus pour la version Citrix ADC.
- Si une instance Citrix Gateway existe, vous ne pouvez pas exécuter l'assistant Citrix ADC for XenMobile une deuxième fois pour créer la configuration Citrix ADC pour XenMobile.
- Sauf lorsque des licences Platinum sont utilisées pour Citrix Gateway 11.1 ou version ultérieure : les licences d'accès utilisateur installées sur Citrix ADC et requises pour la connectivité VPN sont regroupées. Comme ces licences sont disponibles pour tous les serveurs virtuels Citrix ADC, des services autres que XenMobile peuvent potentiellement les consommer.

Instance VPX/MPX Citrix ADC dédiée

Avantages :

Citrix recommande d'utiliser une instance dédiée de Citrix ADC.

- Plus facile à planifier en termes d'échelle et sépare le trafic XenMobile d'une instance Citrix ADC qui pourrait déjà être limitée en ressources.
- Évite les problèmes lorsque XenMobile et Citrix Virtual Apps and Desktops ont besoin de versions différentes du logiciel Citrix ADC. Il est généralement préférable d'utiliser la dernière version/build de Citrix ADC compatible pour XenMobile.
- Permet la configuration XenMobile de Citrix ADC via l'assistant Citrix ADC for XenMobile intégré.
- Séparation virtuelle et physique des services.
- Sauf lorsque les licences Platinum sont utilisées pour Citrix Gateway 11.1 ou version ultérieure, les licences d'accès utilisateur requises pour XenMobile sont uniquement disponibles pour les services XenMobile sur Citrix ADC.

Inconvénients :

- Nécessite l'installation de services supplémentaires sur Citrix ADC pour prendre en charge la configuration XenMobile.
- Nécessite une autre licence de plate-forme Citrix ADC. Licence pour chaque instance Citrix ADC pour Citrix Gateway.

Pour plus d'informations sur les éléments à prendre en compte lors de l'intégration de Citrix Gateway et Citrix ADC avec chaque mode de serveur XenMobile, consultez Intégration avec Citrix Gateway et Citrix ADC.

StoreFront

Si vous disposez d'un environnement Citrix Virtual Apps and Desktops, vous pouvez intégrer des applications HDX avec XenMobile à l'aide de StoreFront. Lorsque vous intégrez des applications HDX avec XenMobile :

- Les applications sont disponibles pour les utilisateurs inscrits avec XenMobile.
- Les applications s'affichent dans le magasin XenMobile avec d'autres applications mobiles.
- XenMobile utilise le site PNAgent (services) hérité sur StoreFront.
- Lorsque Citrix Receiver est installé sur un appareil, les applications HDX commencent à utiliser Receiver.

StoreFront est limité à un site de services par instance. Supposons que vous ayez plusieurs magasins et que vous souhaitiez le séparer d'autres utilisations de production. Dans ce cas, Citrix vous recommande généralement d'envisager une nouvelle instance de StoreFront avec un nouveau site de services pour XenMobile.

Les points à prendre en compte sont les suivants :

- Existe-t-il des exigences d'authentification différentes pour StoreFront ? Le site de services StoreFront nécessite des informations d'identification Active Directory pour la connexion. Les clients utilisant uniquement l'authentification par certificat ne peuvent pas énumérer les applications via XenMobile en utilisant la même instance de Citrix Gateway.
- Utiliser le même magasin ou en créer un nouveau ?
- Utiliser le même serveur StoreFront ou un serveur différent ?

Les sections suivantes indiquent les avantages et les inconvénients de l'utilisation d'instances StoreFront séparées ou combinées pour Receiver et pour les applications de productivité mobiles.

Intégrer votre instance StoreFront existante avec XenMobile Server

Avantages :

- Même magasin : aucune configuration supplémentaire de StoreFront n'est requise pour XenMobile, à condition que vous utilisiez le même accès par VIP Citrix ADC pour HDX. Supposons que vous choisissiez d'utiliser le même magasin et que vous souhaitiez diriger l'accès de Receiver vers une nouvelle VIP Citrix ADC. Dans ce cas, ajoutez la configuration Citrix Gateway appropriée à StoreFront.
- Même serveur StoreFront : utilise l'installation et la configuration de StoreFront existantes.

Inconvénients :

- Même magasin : toute reconfiguration de StoreFront pour gérer les charges de travail Virtual Apps and Desktops peut également avoir un effet négatif sur XenMobile.

- Même serveur StoreFront : dans les environnements de grande taille, considérez la charge supplémentaire que représente l'utilisation de PNAgent par XenMobile pour l'énumération et le démarrage des applications.

Utiliser une nouvelle instance StoreFront dédiée pour l'intégration avec XenMobile Server

Avantages :

- Nouveau magasin : les modifications de configuration du magasin StoreFront pour XenMobile ne devraient pas affecter les charges de travail Virtual Apps and Desktops existantes.
- Nouveau serveur StoreFront : les modifications de configuration du serveur ne devraient pas affecter le flux de travail Virtual Apps and Desktops. De plus, la charge hors de l'utilisation de PNAgent par XenMobile pour l'énumération et le lancement des applications ne devrait pas affecter la capacité à monter en charge.

Inconvénients :

- Nouveau magasin : configuration du magasin StoreFront.
- Nouveau serveur StoreFront : requiert une nouvelle installation et une nouvelle configuration de StoreFront.

Pour de plus amples informations, consultez la section Virtual Apps and Desktops via Citrix Secure Hub dans la documentation de XenMobile.

Citrix Content Collaboration et Citrix Files

Citrix Files permet aux utilisateurs d'accéder à toutes leurs données et de les synchroniser à partir de n'importe quel appareil. Avec Citrix Files, les utilisateurs peuvent partager des données en toute sécurité avec des personnes à l'intérieur et à l'extérieur de l'organisation. Si vous intégrez Citrix Content Collaboration avec XenMobile Advanced Edition ou Enterprise Edition, XenMobile peut fournir à Citrix Files les fonctions suivantes :

- Authentification à connexion unique pour les utilisateurs de l'application XenMobile.
- Provisionnement de compte d'utilisateur basé sur Active Directory.
- Stratégies de contrôle d'accès complètes

Les utilisateurs mobiles peuvent bénéficier de l'ensemble des fonctionnalités de compte Enterprise.

Vous pouvez également configurer XenMobile pour une intégration exclusivement avec des connecteurs StorageZone. Grâce aux connecteurs StorageZone, Citrix Files donne accès aux éléments suivants :

- Documents et dossiers
- Partages de fichiers réseau
- Dans les sites SharePoint : collections de sites et bibliothèques de documents.

Les partages de fichiers connectés peuvent inclure les mêmes lecteurs de base réseau que ceux utilisés dans les environnements Citrix Virtual Apps and Desktops. Vous utilisez la console XenMobile pour configurer l'intégration avec Citrix Files ou avec les StorageZones Controller. Pour plus d'informations, consultez Utilisation de Citrix Files avec XenMobile.

Les sections suivantes indiquent les questions à poser lors de la prise de décision concernant la conception pour Citrix Files.

Intégration à Citrix Files ou uniquement aux connecteurs StorageZone

Questions à poser :

- Avez-vous besoin de stocker des données dans des zones de stockage gérées par Citrix ?
- Voulez-vous fournir aux utilisateurs des fonctions de partage de fichiers et de synchronisation ?
- Voulez-vous permettre aux utilisateurs d'accéder aux fichiers sur le site Web Citrix Files ? Ou d'accéder à du contenu Office 365 et à des connecteurs Personal Cloud depuis des appareils mobiles ?

Décision de conception :

- Si la réponse à l'une de ces questions est « oui », effectuez une intégration avec Citrix Files.
- Une intégration aux connecteurs StorageZone uniquement offre aux utilisateurs iOS un accès mobile sécurisé aux référentiels de stockage locaux existants, tels que des sites SharePoint et des partages de fichiers réseau. Dans cette configuration, la configuration d'un sous-domaine Content Collaboration, le provisioning d'utilisateurs pour Citrix Files ou l'hébergement de données Citrix Files ne sont pas nécessaires. L'utilisation de connecteurs StorageZone avec XenMobile est conforme aux restrictions de sécurité contre la fuite d'informations utilisateur en dehors du réseau d'entreprise.

Emplacement des serveurs StorageZones Controller

Questions à poser :

- Avez-vous besoin d'un stockage sur site ou de fonctionnalités telles que des connecteurs StorageZone ?
- Si vous utilisez les fonctionnalités locales de Citrix Files, où se trouveront les StorageZones Controller sur le réseau ?

Décision de conception :

- Déterminez si vous souhaitez placer les serveurs StorageZones Controller dans le cloud Citrix Files, dans votre système de stockage local à locataire unique ou dans un stockage cloud tiers pris en charge.

- Les StorageZones Controller doivent disposer d'un accès à Internet pour communiquer avec le plan de contrôle Citrix Files. Vous pouvez vous connecter de plusieurs manières, y compris par accès direct, configurations NAT/PAT ou configurations du proxy.

Connecteurs StorageZone

Questions à poser :

- Quels sont les chemins de partage CIFS ?
- Quelles sont les URL SharePoint ?

Décision de conception :

- Déterminez si les StorageZones Controller locaux doivent accéder à ces emplacements.
- En raison de la communication des connecteurs StorageZone avec des ressources internes telles que des référentiels de fichiers, des partages CIFS et SharePoint : Citrix recommande que les StorageZones Controller résident dans le réseau interne derrière les pare-feu DMZ et devant Citrix ADC.

Intégration de SAML avec XenMobile Enterprise

Questions à poser :

- L'authentification avec Active Directory est-elle requise pour Citrix Files ?
- La première utilisation de l'application Citrix Files for XenMobile nécessite-t-elle une authentification unique ?
- Existe-t-il un fournisseur d'identité standard dans votre environnement actuel ?
- Combien de domaines sont requis pour utiliser SAML ?
- Existe-t-il plusieurs alias d'adresse e-mail pour les utilisateurs d'Active Directory ?
- Des migrations de domaine Active Directory sont-elles en cours ou prévues pour bientôt ?

Décision de conception :

Les environnements XenMobile Enterprise peuvent choisir d'utiliser SAML comme mécanisme d'authentification pour Citrix Files. Les options d'authentification sont les suivantes :

- Utiliser XenMobile Server en tant que fournisseur d'identité (IdP) pour SAML

Cette option peut fournir une excellente expérience utilisateur et automatiser la création de compte Citrix Files, ainsi qu'activer les fonctionnalités SSO de l'application mobile.

- XenMobile Server est adapté à ce processus : il ne nécessite pas la synchronisation d'Active Directory.
- Utilisez l'outil de gestion des utilisateurs Citrix Files pour provisionner des utilisateurs.
- Utiliser un fournisseur tiers pris en charge en tant que fournisseur d'identité pour SAML

Si vous disposez déjà d'un fournisseur d'identité et pris en charge et que vous n'avez pas besoin de fonctionnalités d'authentification unique pour les applications mobiles, cette option peut vous convenir. Cette option nécessite également l'utilisation de l'outil de gestion des utilisateurs Citrix Files pour le provisionnement des comptes.

L'utilisation de solutions d'identité tierces telles qu'ADFS peut également fournir des fonctionnalités d'authentification unique du côté client Windows. Veillez à évaluer les cas d'utilisation avant de choisir votre fournisseur d'identité SAML Citrix Files.

En outre, pour satisfaire aux deux cas d'utilisation, vous pouvez configurer ADFS et XenMobile en tant que fournisseur d'identité double.

Applications mobiles

Questions à poser :

- Quelle application mobile Citrix Files envisagez-vous d'utiliser (public, MDM, MDX) ?

Décision de conception :

- Vous pouvez distribuer les applications de productivité mobiles à partir de l'App Store d'Apple et de Google Play Store. Avec cette distribution depuis des magasins publics, vous obtenez des applications encapsulées à partir de la page de téléchargements Citrix.
- Si la sécurité est faible et que vous n'avez pas besoin de conteneurisation, l'application publique Citrix Files peut ne pas convenir. Dans un environnement MDM exclusif, vous pouvez fournir la version MDM de l'application Citrix Files à l'aide de XenMobile en mode MDM.
- Pour plus d'informations, consultez les sections Applications et Citrix Files pour XenMobile.

Sécurité, stratégies et contrôle d'accès

Questions à poser :

- Quelles restrictions sont requises pour les utilisateurs de bureau, Web et mobiles ?
- Quels paramètres de contrôle d'accès standard souhaitez-vous pour les utilisateurs ?
- Quelle stratégie de rétention des fichiers comptez-vous utiliser ?

Décision de conception :

- Citrix Files vous permet de gérer les autorisations des employés et la sécurité des appareils. Pour plus d'informations, consultez les sections Autorisations des employés et Gestion des appareils et des applications.
- Certains paramètres de sécurité des appareils Citrix Files et certaines stratégies MDX contrôlent les mêmes fonctionnalités. Dans ce cas, les stratégies XenMobile sont prioritaires, suivies des paramètres de sécurité des appareils Citrix Files. Exemples : si vous désactivez des applications

externes dans Citrix Files, mais les activez dans XenMobile, les applications externes sont désactivées dans Citrix Files. Vous pouvez configurer les applications pour que XenMobile n'exige pas de code PIN/code secret, mais que l'application Citrix Files requiert un code PIN/code secret.

Zones de stockage standard ou restreintes

Questions à poser :

- Avez-vous besoin de zones de stockage restreintes ?

Décision de conception :

- Une zone de stockage standard est conçue pour stocker les données non sensibles et permet aux employés de partager des données avec des personnes autres que des employés. Cette option prend en charge les workflows qui impliquent le partage de données en dehors de votre domaine.
- Une zone de stockage restreinte protège les données sensibles : seuls les utilisateurs de domaine authentifiés peuvent accéder aux données stockées dans la zone.

Serveurs proxy Web

Le scénario le plus probable pour acheminer le trafic XenMobile via un proxy HTTP(S)/SOCKS est lorsque le sous-réseau dans lequel réside le serveur XenMobile ne dispose pas d'un accès Internet sortant aux adresses IP Apple, Google ou Microsoft requises. Vous pouvez spécifier les paramètres du serveur proxy dans XenMobile pour acheminer tout le trafic Internet vers le serveur proxy. Pour de plus amples informations, consultez la section Activer les serveurs proxy.

Le tableau suivant décrit les avantages et les inconvénients du serveur proxy le plus couramment utilisé avec XenMobile.

Option	Avantages	Inconvénients
Utiliser un serveur proxy HTTP(S)/SOCKS avec XenMobile Server	Dans les cas où les stratégies n'autorisent pas les connexions Internet sortantes à partir du sous-réseau de XenMobile Server, vous pouvez configurer un proxy HTTP(S) ou SOCKS pour fournir la connectivité Internet.	Si le serveur proxy échoue, la connectivité APN (iOS) ou Firebase Cloud Messaging (Android) est interrompue. Par conséquent, les notifications d'appareil échouent pour tous les appareils iOS et Android.

Utiliser un serveur proxy HTTP(S) avec Secure Web	Vous pouvez surveiller le trafic HTTP/HTTPS pour vous assurer que l'activité Internet est conforme aux normes de votre organisation.	Cette configuration nécessite que tout le trafic Internet Secure Web soit redirigé vers le réseau d'entreprise par tunnel avant d'être renvoyé sur Internet. Si votre connexion Internet limite la navigation, cette configuration peut affecter les performances de navigation sur Internet.

La configuration de votre profil de session Citrix ADC pour le split tunneling affecte le trafic de la manière suivante.

Lorsque le split tunneling Citrix ADC est **désactivé** :

- Lorsque la stratégie MDX **Accès réseau** est définie sur **Tunnélisé vers le réseau interne**, tout le trafic est forcé à utiliser le tunnel micro VPN ou le tunnel VPN sans client (cVPN) vers Citrix Gateway.
- Configurez les stratégies et profils de trafic Citrix ADC pour le serveur proxy et liez-les à l'adresse IP virtuelle de Citrix Gateway.

> **Important :**
>
> Veillez à exclure le trafic cVPN de Secure Hub du serveur proxy.

- Pour plus d'informations, consultez la page XenMobile Secure Hub Traffic Through Proxy Server in Secure Browse Mode.

Lorsque le **split tunneling Citrix ADC** est **activé** :

- Lorsque les applications sont configurées avec la stratégie MDX **Accès au réseau** définie sur **Tunnellisé vers le réseau interne**, les applications tentent d'abord d'obtenir la ressource Web directement. Si la ressource Web n'est pas publiquement disponible, ces applications reviennent ensuite à Citrix Gateway.
- Configurez les stratégies et profils de trafic Citrix ADC pour le serveur proxy. Ensuite, liez ces stratégies et profils à l'adresse IP virtuelle de Citrix Gateway.

> **Important :**
>
> Veillez à exclure le trafic cVPN de Secure Hub du serveur proxy.

La configuration de profil de session Citrix ADC pour **Split DNS** (sous **Expérience client**) fonctionne de la même manière que l'option Split Tunneling.

Option **Split DNS** activée et définie sur **Les deux** :

- Le client tente d'abord de résoudre le nom de domaine complet localement, puis revient à Citrix ADC pour la résolution DNS en cas d'échec.

Option **Split DNS** définie sur **Distant** :

- La résolution DNS se produit uniquement sur Citrix ADC.

Option **Split DNS** définie sur **Local** :

- Le client tente de résoudre le nom de domaine complet localement. Citrix ADC n'est pas utilisé pour la résolution DNS.

Contrôle d'accès

Les entreprises peuvent gérer les appareils mobiles à l'intérieur et à l'extérieur des réseaux. Les solutions de gestion de la mobilité d'entreprise telles que XenMobile sont excellentes pour fournir sécurité et contrôle pour les appareils mobiles, indépendamment de leur emplacement. Toutefois, en utilisant également une solution de contrôle d'accès réseau (NAC), vous pouvez ajouter une qualité de service et un contrôle plus précis aux appareils internes de votre réseau. Cette combinaison vous permet d'étendre l'évaluation de la sécurité des appareils XenMobile via votre solution NAC. Votre solution NAC peut ensuite utiliser l'évaluation de sécurité XenMobile pour faciliter et gérer les décisions d'authentification.

Vous pouvez utiliser l'une de ces solutions pour appliquer les stratégies NAC :

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

Citrix ne garantit pas l'intégration à d'autres solutions NAC.

Les avantages d'une intégration de solution NAC avec XenMobile sont les suivants :

- Sécurité, conformité et contrôle améliorés pour tous les points de terminaison sur un réseau d'entreprise.
- Une solution NAC peut :
  - Détecter les appareils au moment où ils tentent de se connecter à votre réseau.
  - Interroger XenMobile sur les attributs de l'appareil.
  - Utiliser ces informations pour déterminer si ces appareils doivent être autorisés, bloqués, limités ou redirigés. Ces décisions dépendent des stratégies de sécurité que vous choisissez d'appliquer.

- Une solution NAC fournit aux administrateurs informatiques une vue des appareils non gérés et non conformes.

Vous trouverez une description des filtres de conformité NAC pris en charge par XenMobile et une vue d'ensemble de la configuration dans la section Contrôle d'accès réseau.

Configuration requise multisite

January 10, 2022

Vous pouvez concevoir et configurer des déploiements XenMobile comprenant plusieurs sites pour la haute disponibilité et la récupération d'urgence. Cet article fournit une vue d'ensemble des modèles de haute disponibilité et de récupération d'urgence utilisés dans les déploiements XenMobile.

Haute disponibilité

- Pour les nœuds de cluster XenMobile, Citrix ADC gère l'équilibrage de charge. Pour plus d'informations, consultez Configurer la mise en cluster.
- Les nœuds XenMobile Server fonctionnent dans une configuration active/active.
- Des nœuds XenMobile Server supplémentaires sont ajoutés à un cluster à haute disponibilité en fonction de la capacité requise. Un seul nœud peut gérer environ 8 500 machines utilisateur (consultez la page Capacité à monter en charge et performances pour plus de détails).
- Citrix recommande de configurer "n + 1" serveurs XenMobile : un serveur pour 8 500 machines utilisateur et un serveur supplémentaire pour la redondance.
- Citrix recommande, dans la mesure du possible, la mise en œuvre d'une haute disponibilité sur toutes les instances Citrix ADC afin de permettre aux configurations de se synchroniser avec une seconde instance Citrix ADC.
- La paire haute disponibilité Citrix ADC standard fonctionne dans une configuration active/passive.

Un déploiement XenMobile haute disponibilité typique comprend généralement les composants suivants :

- Deux instances de Citrix ADC (VPX ou MPX). Si la plate-forme SDX Citrix ADC est utilisée, la haute disponibilité doit également être prise en compte.
- Deux serveurs XenMobile ou plus configurés avec les mêmes paramètres de base de données.

Récupération d'urgence

Vous pouvez configurer XenMobile pour la récupération d'urgence sur deux centres de données avec un centre de données actif et un centre de données passif. Citrix ADC et Global Server Load Balancing

(GSLB) permettent de créer un chemin de données actif/actif de sorte que l'expérience utilisateur soit celle d'une configuration active/active.

Dans le cadre de la récupération d'urgence, un déploiement XenMobile comprend les composants suivants :

- Deux centres de données ; chacun contient une ou plusieurs instances Citrix ADC, serveurs XenMobile et bases de données SQL Server.
- Un serveur GSLB pour diriger le trafic vers les centres de données. Le serveur GSLB est configuré pour l'URL d'inscription XenMobile et l'URL Citrix Gateway gérant le trafic sur le site.
- Lorsque vous utilisez l'assistant Citrix ADC for XenMobile pour configurer Citrix Gateway, GSLB n'est pas activé pour résoudre le trafic sur le serveur d'inscription XenMobile et le trafic sur Citrix Gateway en route vers le serveur d'équilibrage de charge MAM. Par conséquent, des étapes supplémentaires sont nécessaires. Pour plus d'informations sur la préparation et la mise en œuvre de ces étapes, consultez la section Récupération d'urgence.
- Groupes de disponibilité AlwaysOn en cluster de SQL Server
- La latence entre les serveurs XenMobile et SQL Server doit être inférieure à 5 ms.

> **Remarque :**
>
> Les méthodes de récupération d'urgence décrites dans ce manuel fournissent uniquement une récupération d'urgence automatisée pour la couche d'accès. Vous devez démarrer manuellement tous les nœuds XenMobile Server et la base de données SQL Server sur le site de basculement avant que les appareils ne puissent se connecter à XenMobile Server.

Intégrer avec Citrix Gateway et Citrix ADC

January 10, 2022

Lorsqu'il est intégré à XenMobile, Citrix Gateway fournit aux appareils MAM un mécanisme d'authentification pour l'accès des appareils distants au réseau interne. Cette intégration permet aux applications de productivité mobiles de se connecter à des serveurs d'entreprise situés dans l'intranet via un micro VPN. Le micro VPN est créé à partir des applications sur l'appareil mobile vers Citrix Gateway. Citrix Gateway fournit un chemin micro VPN pour l'accès à toutes les ressources de l'entreprise et fournit une prise en charge de l'authentification forte à multi-facteurs.

L'équilibrage de charge Citrix ADC est requis pour tous les modes d'appareil XenMobile Server dans les cas suivants :

- Si vous avez plusieurs instances de XenMobile Server.
- Ou, si XenMobile Server est à l'intérieur de votre zone démilitarisée ou réseau interne (et donc le trafic circule des appareils vers Citrix ADC vers XenMobile).

Exigences d'intégration pour les modes de XenMobile Server

Les exigences d'intégration de Citrix Gateway et Citrix ADC diffèrent selon les modes de XenMobile Server : MAM, MDM et ENT.

MAM

Avec XenMobile Server en mode MAM :

- **Citrix Gateway** est requis. Citrix Gateway fournit un chemin micro VPN pour l'accès à toutes les ressources de l'entreprise et fournit une prise en charge de l'authentification forte à multi-facteurs.
- **Citrix ADC** est recommandé pour l'équilibrage de charge.

  Citrix vous recommande de déployer XenMobile dans une configuration à haute disponibilité, ce qui nécessite un équilibreur de charge au premier plan, devant XenMobile. Pour de plus amples informations, consultez la section À propos des modes MAM et des modes MAM anciens.

MDM

Avec XenMobile Server en mode MDM :

- Citrix Gateway n'est pas requis. Pour les déploiements MDM, Citrix recommande Citrix Gateway pour les appareils VPN mobiles.
- Citrix ADC est recommandé pour la sécurité et l'équilibrage de charge.

  Citrix vous recommande de déployer une appliance Citrix ADC au premier plan, devant XenMobile Server, à des fins de sécurité et d'équilibrage de la charge. Pour les déploiements standard avec XenMobile dans la DMZ, Citrix recommande l'assistant Citrix ADC for XenMobile ainsi que l'équilibrage de la charge de XenMobile Server en mode pont SSL. Vous pouvez également envisager la décharge SSL pour les déploiements dans lesquels :

  - XenMobile Server réside dans le réseau interne plutôt que dans la zone démilitarisée
  - Votre équipe de sécurité nécessite une configuration SSL Bridge

  Citrix ne recommande pas d'exposer XenMobile Server à Internet via NAT ou des proxys tiers existants ou des équilibreurs de charge pour MDM. Ces configurations présentent un risque potentiel de sécurité, même si le trafic SSL se termine sur XenMobile Server (SSL Bridge).

  Pour les environnements hautement sécurisé, Citrix ADC défini avec la configuration XenMobile par défaut respecte ou dépasse les exigences de sécurité.

  Pour les environnements MDM ayant les besoins de sécurité les plus élevés, la terminaison SSL sur Citrix ADC permet d'inspecter le trafic sur le périmètre tout en assurant le cryptage SSL de bout en bout. Pour de plus amples informations, consultez la section Exigences en matière de

sécurité. Citrix ADC offre des options pour définir les chiffrements SSL/TLS et le matériel SSL FIPS Citrix ADC.

ENT (MAM + MDM)

Avec XenMobile Server en mode ENT :

- Citrix Gateway est requis. Citrix Gateway fournit un chemin micro VPN pour l'accès à toutes les ressources de l'entreprise et fournit une prise en charge de l'authentification forte à multi-facteurs.

  Lorsque le mode de XenMobile Server est défini sur ENT et qu'un utilisateur refuse l'inscription MDM, l'appareil fonctionne dans l'ancien mode MAM. Dans les versions antérieures du mode MAM, les appareils s'inscrivent à l'aide du nom de domaine complet de Citrix Gateway. Pour de plus amples informations, consultez la section À propos des modes MAM et des modes MAM anciens.

- Citrix ADC est recommandé pour l'équilibrage de charge. Pour plus d'informations, consultez les remarques associées à Citrix ADC plus haut dans cet article sous « MDM ».

> **Important :**
>
> Pour l'inscription initiale, le trafic des appareils utilisateur s'authentifie sur XenMobile Server, que vous configuriez des serveurs virtuels d'équilibrage de charge sur Déchargement SSL ou Pont SSL.

Décisions de conception

Les sections suivantes résument les nombreuses décisions de conception à prendre en compte lors de la planification d'une intégration de Citrix Gateway avec XenMobile.

Licence et édition

Détails de la décision :

- Quelle édition de Citrix ADC prévoyez-vous d'utiliser ?
- Avez-vous appliqué des licences Platform à Citrix ADC ?
- Si vous avez besoin de la fonctionnalité MAM, avez-vous appliqué les licences Citrix ADC Universal Access ?

Conseils de conception :

Assurez-vous d'appliquer les licences appropriées à Citrix Gateway. Si vous utilisez Citrix Gateway Connector pour Exchange ActiveSync, la mise en cache intégrée peut être requise. Par conséquent, vous devez vous assurer que l'édition Citrix ADC appropriée est en place.

Les exigences en matière de licence pour activer les fonctionnalités Citrix ADC sont les suivantes.

- L'équilibrage de charge XenMobile MDM nécessite au minimum une licence de plate-forme standard Citrix ADC.
- L'équilibrage de la charge Content Collaboration avec StorageZones Controller nécessite au minimum une licence de plate-forme standard Citrix ADC.
- L'édition XenMobile Enterprise inclut les licences Citrix Gateway Universal requises pour MAM.
- L'équilibrage de charge Exchange nécessite une licence de plate-forme Citrix ADC Platinum ou une licence de plate-forme Citrix ADC Enterprise en plus d'une licence de mise en cache intégrée.

Version de Citrix ADC pour XenMobile

Détails de la décision :

- Quelle version de Citrix ADC est en cours d'exécution dans l'environnement XenMobile ?
- Avez-vous besoin d'une instance distincte ?

Conseils de conception :

Citrix vous recommande d'utiliser une instance dédiée de Citrix ADC pour votre serveur virtuel Citrix Gateway. Assurez-vous que la version/build de Citrix ADC minimale requise est utilisée dans l'environnement XenMobile. Il est généralement préférable d'utiliser la dernière version/build de Citrix ADC compatible pour XenMobile. Si la mise à niveau de Citrix Gateway affecte vos environnements existants, une seconde instance dédiée pour XenMobile peut être appropriée.

Si vous souhaitez partager une instance Citrix ADC pour XenMobile et d'autres applications utilisant des connexions VPN, vérifiez que vous disposez de suffisamment de licences VPN. Gardez à l'esprit que les environnements de test et de production XenMobile ne peuvent pas partager une instance Citrix ADC.

Certificats

Détails de la décision :

- Avez-vous besoin d'un niveau de sécurité plus élevé pour les inscriptions et l'accès à l'environnement XenMobile ?
- Pourriez-vous considérez le protocole LDAP ?

Conseils de conception :

La configuration par défaut pour XenMobile est l'authentification par nom d'utilisateur et mot de passe. Pour ajouter une autre couche de sécurité pour l'inscription et l'accès à l'environnement XenMobile, vous pouvez utiliser l'authentification basée sur certificats. Vous pouvez utiliser des certificats avec LDAP pour l'authentification à deux facteurs, ce qui permet d'offrir un degré de sécurité supérieur sans avoir besoin d'un serveur RSA.

Si vous n'autorisez pas LDAP et utilisez des cartes à puce ou méthodes similaires, la configuration des certificats vous permet de représenter une carte à puce auprès de XenMobile. Les utilisateurs s'inscrivent alors à l'aide d'un code PIN unique généré par XenMobile. Une fois qu'un utilisateur a accès, XenMobile crée et déploie le certificat utilisé ensuite pour s'authentifier auprès de l'environnement XenMobile.

XenMobile prend en charge la liste de révocation de certificats (CRL) uniquement pour une autorité de certification tierce. Si vous disposez d'une autorité de certification Microsoft configurée, XenMobile utilise Citrix ADC pour gérer la révocation. Lorsque vous configurez l'authentification basée sur un certificat client, vous devez décider si vous avez besoin de configurer le paramètre Liste de révocation de certificats (CRL) Citrix ADC, **Enable CRL Auto Refresh**. Cette étape garantit que l'utilisateur d'un appareil inscrit en mode MAM exclusif ne peut pas s'authentifier à l'aide d'un certificat existant sur l'appareil. XenMobile émet un nouveau certificat, car il n'interdit pas à un utilisateur de générer un certificat utilisateur si un certificat est révoqué. Ce paramètre renforce la sécurité des entités PKI lorsque la CRL vérifie la présence d'entités PKI expirées.

Topologie réseau

Détails de la décision :

- Quelle topologie Citrix ADC est requise ?

Conseils de conception :

Citrix recommande d'utiliser une instance Citrix ADC pour XenMobile. Toutefois, il se peut que vous ne vouliez pas que le trafic soit acheminé du réseau interne vers la DMZ. Dans ce cas, envisagez de configurer une instance supplémentaire de Citrix ADC. Utilisez une instance de Citrix ADC pour les utilisateurs internes et une instance pour les utilisateurs externes. Lorsque les utilisateurs basculent entre les réseaux internes et externes, la mise en cache des enregistrements DNS peut entraîner une augmentation des invites de connexion Secure Hub.

XenMobile ne prend pas en charge Citrix Gateway Double Hop.

VIP Citrix Gateway dédiés ou partagés

Détails de la décision :

- Utilisez-vous actuellement Citrix Gateway pour Virtual Apps and Desktops ?
- XenMobile utilisera-t-il la même appliance Citrix Gateway que Virtual Apps and Desktops ?
- Quelles sont les exigences d'authentification pour les deux flux de trafic ?

Conseils de conception :

Lorsque votre environnement Citrix comprend XenMobile, ainsi que Virtual Apps and Desktops, vous pouvez utiliser la même instance Citrix ADC et le même serveur virtuel Citrix Gateway pour les deux.

En raison de conflits de version et d'isolement d'environnement potentiels, une instance Citrix ADC dédiée et Citrix Gateway sont recommandées pour chaque environnement XenMobile. Toutefois, si une instance Citrix ADC dédiée n'est pas possible, Citrix recommande d'utiliser un serveur virtuel Citrix Gateway dédié pour séparer les flux de trafic de Secure Hub. Cette configuration remplace un serveur virtuel partagé entre XenMobile et Virtual Apps and Desktops.

Si vous utilisez l'authentification LDAP, Receiver et Secure Hub peuvent s'authentifier auprès de la même instance Citrix Gateway sans problème. Si vous utilisez l'authentification par certificat, XenMobile envoie un certificat dans le conteneur MDX et Secure Hub utilise le certificat pour s'authentifier auprès de Citrix Gateway. Receiver est distinct de Secure Hub et ne peut pas utiliser le même certificat que Secure Hub pour s'authentifier sur la même instance Citrix Gateway.

Vous pouvez envisager la solution suivante, ce qui vous permet d'utiliser le même nom de domaine complet pour deux VIP Citrix Gateway.

- Créez deux adresses IP virtuelles (VIP) Citrix Gateway avec la même adresse IP. Le VIP de Secure Hub utilise le port 443 standard et le VIP de Citrix Virtual Apps and Desktops (qui déploient Receiver) utilise le port 444.
- Un nom de domaine complet résout la même adresse IP.
- Si vous utilisez cette solution, vous pouvez configurer StoreFront pour renvoyer un fichier ICA pour le port 444, au lieu du port 443 par défaut. Avec cette solution, les utilisateurs n'ont pas besoin d'entrer un numéro de port.

Délais d'expiration de Citrix Gateway

Détails de la décision :

- Comment voulez-vous configurer les délais d'expiration Citrix Gateway pour le trafic XenMobile ?

Conseils de conception :

Citrix Gateway inclut les paramètres Délai d'expiration de session et Délai d'expiration forcé. Pour de plus amples informations, consultez la section Configurations recommandées. Gardez à l'esprit qu'il existe différentes valeurs de délai d'expiration pour les services d'arrière-plan, Citrix ADC et pour accéder aux applications en mode hors connexion.

Adresse IP de l'équilibreur de charge XenMobile pour MAM

Détails de la décision :

- Utilisez-vous des adresses IP internes ou externes pour les VIP ?

Conseils de conception :

Dans les environnements où vous pouvez utiliser des adresses IP publiques pour les VIP Citrix Gateway, l'attribution du VIP et de l'adresse d'équilibrage de charge XenMobile de cette manière entraîne des échecs d'inscription.

Assurez-vous que le VIP d'équilibrage de charge utilise une adresse IP interne pour éviter les échecs d'inscription dans ce scénario. Cette adresse IP virtuelle doit suivre la norme RFC 1918 des adresses IP privées. Si vous utilisez une adresse IP non privée pour ce serveur virtuel, Citrix ADC ne peut pas contacter XenMobile Server au cours du processus d'authentification. Pour plus de détails, consultez https://support.citrix.com/article/CTX200430.

Mécanisme d'équilibrage de charge MDM

Détails de la décision :

- Comment Citrix Gateway va-t-il équilibrer la charge des instances de XenMobile Server ?

Conseils de conception :

Utilisez le mode Pont SSL si XenMobile est dans la DMZ. Utilisez le mode Déchargement SSL si nécessaire pour respecter les normes de sécurité lorsque XenMobile se trouve sur le réseau interne.

- Lorsque vous effectuez l'équilibrage de charge de XenMobile Server avec des VIP Citrix ADC en mode Pont SSL, le trafic Internet passe directement à XenMobile Server, là où les connexions se terminent. Le mode Pont SSL est le mode le plus simple à configurer et à résoudre.
- Lorsque vous effectuez l'équilibrage de charge de XenMobile Server avec des VIP Citrix ADC en mode Déchargement SSL, le trafic Internet passe directement à Citrix ADC, là où les connexions se terminent. Citrix ADC établit ensuite de nouvelles sessions de Citrix ADC vers XenMobile Server. Le mode Déchargement SSL implique une complexité supplémentaire lors de l'installation et du dépannage.

Port de service pour l'équilibrage de charge MDM avec déchargement SSL

Détails de la décision :

- Si vous utilisez le mode Déchargement SSL pour l'équilibrage de charge, quel port le service principal utilisera-t-il ?

Conseils de conception :

Pour le mode Déchargement SSL, choisissez le port 80 ou 8443 comme suit :

- Utilisez le port 80 vers XenMobile Server pour un vrai déchargement.
- Le cryptage de bout en bout, c'est-à-dire le recryptage du trafic, n'est pas pris en charge. Pour de plus amples informations, consultez l'article de support Citrix Architectures prises en charge entre NetScaler et XenMobile Server.

Inscription du nom de domaine complet

Détails de la décision :

- Que comptez-vous utiliser comme nom de domaine complet pour l'inscription et l'instance/le VIP d'équilibrage de charge XenMobile ?

Conseils de conception :

La configuration initiale de la première instance de XenMobile Server d'un cluster nécessite l'entrée du nom de domaine complet de XenMobile Server. Ce nom de domaine complet doit correspondre à votre URL VIP MDM et à votre URL VIP MAM LB interne. (Un enregistrement d'adresse Citrix ADC interne résout le VIP MAM LB.) Pour plus de détails, consultez la section « Nom de domaine complet d'inscription pour chaque mode de gestion » plus loin dans cet article.

En outre, vous devez utiliser le même certificat que le suivant :

- Certificat d'écoute SSL XenMobile
- Certificat VIP LB MAM interne
- Certificat VIP MDM (si vous utilisez le déchargement SSL pour VIP MDM)

> **Important :**
>
> Après avoir configuré le nom de domaine complet de l'inscription, vous ne pouvez pas le modifier. Un nouveau nom de domaine complet d'inscription nécessite une nouvelle base de données SQL Server et une nouvelle build de XenMobile Server.

Trafic de Secure Web

Détails de la décision :

- Prévoyez-vous de limiter Secure Web à la navigation Web interne uniquement ?
- Prévoyez-vous d'activer Secure Web pour la navigation Web interne et externe ?

Conseils de conception :

Si vous envisagez d'utiliser Secure Web uniquement pour la navigation Web interne, la configuration de Citrix Gateway est simple. Par défaut, Secure Web doit atteindre tous les sites internes. Vous devrez peut-être configurer des pare-feu et des serveurs proxy.

Si vous envisagez d'utiliser Secure Web pour la navigation interne et externe, vous devez activer l'adresse IP de sous-réseau pour avoir un accès Internet sortant. Les services informatiques considèrent généralement les appareils inscrits (à l'aide du conteneur MDX) comme une extension du réseau d'entreprise. Ainsi, ils souhaitent généralement que les connexions Secure Web reviennent à Citrix ADC, passent par un serveur proxy, puis sortent vers l'Internet. Par défaut, Secure Web utilise un tunnel VPN par application vers le réseau interne pour tous les accès réseau. Citrix ADC utilise des paramètres de split tunneling.

Pour une description des connexions Secure Web, consultez la section Configuration des connexions utilisateur.

Notifications push pour Secure Mail

Détails de la décision :

- Prévoyez-vous d'utiliser les notifications push ?

Conseils sur la conception pour iOS :

Votre configuration Citrix Gateway peut inclure une autorité STA (Secure Ticket Authority), avec split tunneling désactivé. Citrix Gateway doit autoriser le trafic en provenance de Secure Mail vers les URL du service d'écoute Citrix, comme spécifié dans les notifications push pour Secure Mail sous iOS.

Conseil sur la conception pour Android :

Utilisez Firebase Cloud Messaging (FCM) pour contrôler quand et comment les appareils Android doivent se connecter à XenMobile. Avec la configuration de FCM, toute action de sécurité ou commande de déploiement déclenche une notification push à Secure Hub afin d'inviter l'utilisateur à se reconnecter à XenMobile Server.

HDX STA

Détails de la décision :

- Quelles STA utiliser si vous prévoyez d'intégrer l'accès aux applications HDX ?

Conseils de conception :

Les STA HDX doivent correspondre aux STA dans StoreFront et doivent être valides pour la batterie Virtual Apps and Desktops.

Citrix Files et Citrix Content Collaboration

Détails de la décision :

- Prévoyez-vous d'utiliser des StorageZones Controller dans l'environnement ?
- Quelle URL VIP Citrix Files prévoyez-vous d'utiliser ?

Conseils de conception :

Si vous souhaitez inclure les StorageZones Controller dans votre environnement, assurez-vous de configurer correctement les éléments suivants :

- Le VIP de commutation Citrix Files (utilisé par le plan de contrôle Citrix Files pour communiquer avec les serveurs StorageZones Controller)
- Les VIP d'équilibrage de charge Citrix Files

- Toutes les stratégies et profils requis

Pour plus d'informations, veuillez consulter la documentation d StorageZones Controller.

Fournisseur d'identité SAML

Détails de la décision :

- Si SAML est requis pour Citrix Files, voulez-vous utiliser XenMobile comme fournisseur d'identité SAML ?

Conseils de conception :

La méthode recommandée est d'intégrer Citrix Files à XenMobile Advanced Edition ou XenMobile Enterprise Edition, une approche plus simple que la configuration de la fédération SAML. Lorsque vous utilisez Citrix Files avec ces éditions XenMobile, XenMobile fournit Citrix Files avec :

- Authentification unique (SSO) des utilisateurs d'applications de productivité mobiles
- Provisioning des comptes utilisateur basé sur Active Directory
- Stratégies de contrôle d'accès complètes

La console XenMobile vous permet de configurer Citrix Files et de contrôler les niveaux de service et la consommation de licences.

Il existe deux types de clients Citrix Files : clients Citrix Files for XenMobile (également appelés clients Citrix Files encapsulés) et clients mobiles Citrix Files (également appelés clients Citrix Files non encapsulés). Pour comprendre les différences, consultez la section Différences entre les clients Citrix Files pour XenMobile et les clients mobiles Citrix Files.

Vous pouvez configurer XenMobile et Citrix Content Collaboration pour qu'ils utilisent SAML pour fournir un accès SSO aux composants suivants :

- Applications mobiles Citrix Files
- Clients Citrix Files non encapsulés, tels que le site Web, Outlook Plug-in ou les clients de synchronisation

Pour utiliser XenMobile comme fournisseur d'identité SAML pour Citrix Files, assurez-vous que les configurations appropriées sont en place. Pour plus d'informations, consultez la section SAML pour l'authentification unique avec Citrix Files.

Connexions directes ShareConnect

Détails de la décision :

- Les utilisateurs doivent-ils accéder à un ordinateur hôte à partir d'un ordinateur ou d'un appareil mobile exécutant ShareConnect à l'aide de connexions directes ?

Conseils de conception :

ShareConnect permet aux utilisateurs de se connecter à leurs ordinateurs en toute sécurité au travers d'iPads, de tablettes et de téléphones Android pour accéder à leurs fichiers et applications. Pour les connexions directes, XenMobile utilise Citrix Gateway pour sécuriser l'accès aux ressources en dehors du réseau local. Pour plus d'informations sur la configuration, consultez la section ShareConnect.

Nom de domaine complet d'inscription pour chaque mode de gestion

Mode de gestion	Inscription du nom de domaine complet
Enterprise (MDM + MAM) avec inscription MDM obligatoire	Nom de domaine complet de XenMobile Server
Enterprise (MDM + MAM) avec inscription MDM facultative	Nom de domaine complet de XenMobile Server ou nom de domaine complet Citrix Gateway
MDM exclusif	Nom de domaine complet de XenMobile Server
Mode MAM uniquement (ancien mode)	Nom de domaine complet Citrix Gateway
MAM exclusif	Nom de domaine complet de XenMobile Server

Récapitulatif du déploiement

Citrix vous recommande d'utiliser l'assistant Citrix ADC for XenMobile pour garantir une configuration correcte. Vous ne pouvez utiliser l'assistant qu'une seule fois. Si vous disposez de plusieurs instances XenMobile, telles que les environnements de test, de développement et de production, vous devez configurer manuellement Citrix ADC pour les environnements supplémentaires. Lorsque vous disposez d'un environnement de travail, prenez note des paramètres avant de tenter de configurer manuellement Citrix ADC pour XenMobile.

La décision clé que vous prenez lors de l'utilisation de l'assistant consiste à utiliser HTTPS ou HTTP pour la communication avec XenMobile Server. HTTPS fournit une communication principale sécurisée, car le trafic entre Citrix ADC et XenMobile est crypté. Le recryptage impacte les performances du serveur XenMobile Server. HTTP offre de meilleures performances pour XenMobile Server. Le trafic entre Citrix ADC et XenMobile n'est pas crypté. Les tableaux suivants répertorient les exigences de port HTTP et HTTPS pour XenMobile Server et Citrix ADC.

HTTPS

Citrix recommande généralement le mode Pont SSL pour les configurations de serveur virtuel Citrix ADC MDM. Pour utiliser le mode Déchargement SSL de Citrix ADC avec les serveurs virtuels MDM, XenMobile prend en charge uniquement le port 80 en tant que service principal.

Mode de gestion	Méthode d'équilibrage de charge Citrix ADC	Ré-cryptage SSL	Port de XenMobile Server
MDM	Pont SSL	S.O.	443, 8443
MAM	Déchargement SSL	Enabled	8443
Entreprise	MDM : Pont SSL	S.O.	443, 8443
Entreprise	MAM : Déchargement SSL	Enabled	8443

HTTP

Mode de gestion	Méthode d'équilibrage de charge Citrix ADC	Ré-cryptage SSL	Port de XenMobile Server
MDM	Déchargement SSL	Non pris en charge	80
MAM	Déchargement SSL	Enabled	8443
Entreprise	MDM : Déchargement SSL	Non pris en charge	80
Entreprise	MAM : Déchargement SSL	Enabled	8443

Vous trouverez des diagrammes de Citrix Gateway dans les déploiements XenMobile dans la section Architecture de référence pour les déploiements sur site.

Considérations SSO et proxy pour les applications MDX

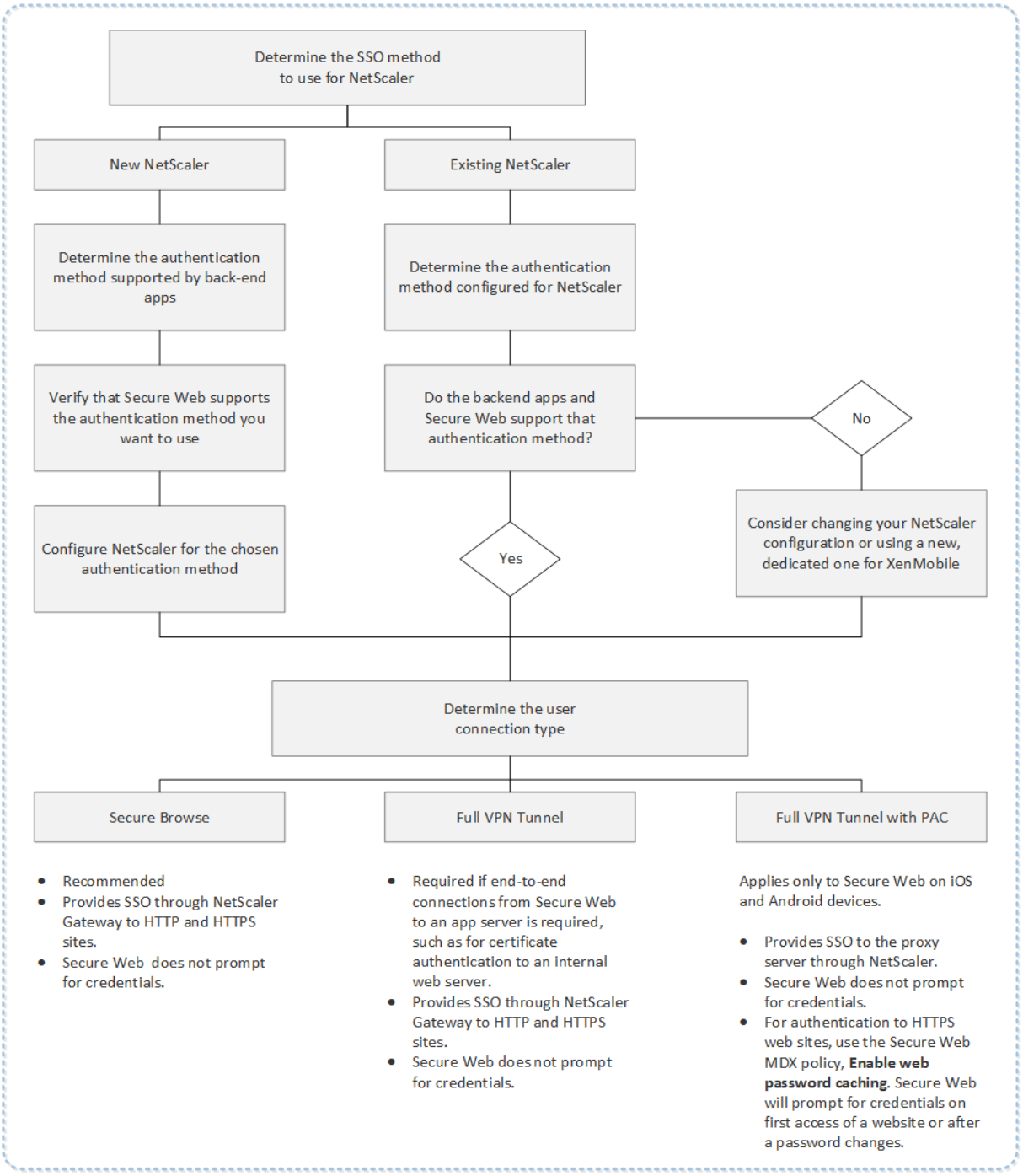
January 10, 2022

L'intégration de XenMobile avec Citrix ADC vous permet de fournir aux utilisateurs une authentification unique (SSO) à toutes les ressources HTTP/HTTPS principales. En fonction de vos exigences d'authentification unique (SSO), vous pouvez configurer les connexions utilisateur d'une application MDX pour utiliser l'une des options suivantes :

- Secure Browse, qui est un type de VPN sans client
- Tunnel VPN complet

Si Citrix ADC n'est pas le meilleur moyen de fournir une authentification unique dans votre environnement, vous pouvez configurer une application MDX avec une mise en cache de mot de passe locale basée sur une stratégie. Cet article explore les différentes options SSO et proxy, en mettant l'accent sur Secure Web. Les concepts s'appliquent à d'autres applications MDX.

L'organigramme suivant résume le flux décisionnel pour les connexions SSO et utilisateur.



Méthodes d’authentification Citrix ADC

Cette section fournit des informations générales sur les méthodes d’authentification prises en charge par Citrix ADC.

Authentification SAML

Lorsque vous configurez Citrix ADC pour le langage SAML (Assertion Marking Language), les utilisateurs peuvent se connecter aux applications Web prenant en charge le protocole SAML pour l'authentification unique. Citrix Gateway prend en charge l'authentification unique de fournisseur d'identité pour les applications Web SAML.

Configuration requise :

- Configurez l'authentification unique SAML dans le profil de trafic Citrix ADC.
- Configurez le fournisseur d'identité SAML pour le service demandé.

Authentification NTLM

Si l'authentification unique pour les applications Web est activée dans le profil de session, Citrix ADC effectue automatiquement l'authentification NTLM.

Configuration requise :

- Activez l'authentification unique dans le profil de trafic ou de session Citrix ADC.

Emprunt d'identité Kerberos

XenMobile prend en charge Kerberos pour Secure Web uniquement. Lorsque vous configurez Citrix ADC pour Kerberos SSO, Citrix ADC utilise l'emprunt d'identité lorsqu'un utilisateur est disponible pour Citrix ADC. L'emprunt d'identité signifie que Citrix ADC utilise des informations d'identification utilisateur pour obtenir le ticket requis pour accéder aux services, tels que Secure Web.

Configuration requise :

- Configurez la stratégie de session Citrix ADC "Worx" pour lui permettre d'identifier le domaine Kerberos à partir de votre connexion.
- Configurez un compte Kerberos Constrained Delegation (KCD) sur Citrix ADC. Configurez ce compte sans mot de passe et associez-le à une stratégie de trafic sur votre passerelle XenMobile.
- Pour plus de détails sur la configuration, consultez le blog Citrix : WorxWeb and Kerberos Impersonation SSO.

Délégation Kerberos contrainte

XenMobile prend en charge Kerberos pour Secure Web uniquement. Lorsque vous configurez Citrix ADC pour Kerberos SSO, Citrix Gateway utilise la délégation contrainte lorsqu'un mot de passe utilisateur n'est pas disponible pour Citrix ADC.

Avec une délégation contrainte, Citrix ADC utilise un compte d'administrateur spécifié pour obtenir des tickets au nom des utilisateurs et des services.

Configuration requise :

- Configurez un compte KCD dans Active Directory avec les autorisations requises et un compte KCD sur Citrix ADC.
- Activez l'authentification unique dans le profil de trafic Citrix ADC.
- Configurez le site Web principal pour l'authentification Kerberos.

Authentification par remplissage de formulaire

Lorsque vous configurez Citrix ADC pour l'authentification par remplissage de formulaire, les utilisateurs peuvent se connecter une seule fois pour accéder à toutes les applications protégées de votre réseau. Cette méthode d'authentification s'applique aux applications qui utilisent les modes Navigation sécurisée ou VPN complet.

Configuration requise :

- Configurez l'authentification unique par remplissage de formulaire dans le profil de trafic Citrix ADC.

Authentification HTTP Digest

Si vous activez l'authentification unique pour les applications Web dans le profil de session, Citrix ADC effectue automatiquement l'authentification HTTP Digest. Cette méthode d'authentification s'applique aux applications qui utilisent les modes Navigation sécurisée ou VPN complet.

Configuration requise :

- Activez l'authentification unique dans le profil de trafic ou de session Citrix ADC.

Authentification HTTP de base

Si vous activez l'authentification unique pour les applications Web dans le profil de session, Citrix ADC effectue automatiquement l'authentification HTTP de base. Cette méthode d'authentification s'applique aux applications qui utilisent les modes Navigation sécurisée ou VPN complet.

Configuration requise :

- Activez l'authentification unique dans le profil de trafic ou de session Citrix ADC.

Navigation sécurisée, tunnel VPN complet ou tunnel VPN complet avec PAC

Les sections suivantes décrivent les types de connexion utilisateur pour Secure Web. Pour plus d'informations, consultez cet article sur Secure Web dans la documentation Citrix, Configuration des connexions utilisateur.

Tunnel VPN complet

Les connexions qui sont tunnelisées sur le réseau interne peuvent utiliser un tunnel VPN complet. Utilisez la stratégie Mode VPN préféré de Secure Web pour configurer un tunnel VPN complet. Citrix recommande un tunnel VPN complet pour les connexions qui utilisent des certificats clients ou des connexions SSL de bout en bout vers une ressource dans le réseau interne. Full VPN tunnel gère tout protocole sur TCP. Vous pouvez utiliser un tunnel VPN complet avec les appareils Windows, Mac, iOS et Android.

En mode Tunnel VPN complet, Citrix ADC n'a pas de visibilité dans une session HTTPS.

Secure Browse

Les connexions qui sont tunnelisées sur le réseau interne peuvent utiliser une variante d'un VPN sans client, appelé Navigation sécurisée. Navigation sécurisée est la configuration par défaut spécifiée pour la stratégie **Mode VPN préféré** de Secure Web. Citrix recommande Navigation sécurisée pour les connexions qui nécessitent l'authentification unique (SSO).

En mode Navigation sécurisée, Citrix ADC divise la session HTTPS en deux parties :

- Du client à Citrix ADC
- De Citrix ADC au serveur de ressources principal

De cette manière, Citrix ADC a une visibilité complète sur toutes les transactions entre le client et le serveur, ce qui lui permet de fournir une authentification unique.

Vous pouvez également configurer des serveurs proxy pour Secure Web lorsque vous utilisez le mode Navigation sécurisée. Pour plus d'informations, consultez le blog XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode.

Tunnel VPN complet avec PAC

Vous pouvez utiliser un fichier PAC (Proxy Automatic Configuration) avec un déploiement de tunnel VPN complet pour Secure Web sur les appareils Android. XenMobile prend en charge l'authentification proxy fournie par Citrix ADC. Un fichier PAC contient des règles qui définissent la manière dont les navigateurs Web sélectionnent un serveur proxy pour accéder à une URL spécifiée. Les règles du fichier PAC peuvent spécifier la procédure à suivre pour les sites internes et externes. Secure Web analyse les règles du fichier PAC et envoie les informations sur le serveur proxy à Citrix Gateway. Citrix Gateway ignore le fichier PAC ou le serveur proxy.

Pour l'authentification aux sites Web HTTPS : la stratégie MDX de Secure Web **Activer la mise en cache du mot de passe Web** permet à Secure Web de s'authentifier et de fournir l'authentification unique (SSO) au serveur proxy via MDX.

Split tunneling Citrix ADC

Lors de la planification de votre configuration SSO et proxy, vous devez également décider si vous souhaitez utiliser la fonction split tunneling de Citrix ADC. Citrix vous recommande d'utiliser le split tunneling de Citrix ADC uniquement si nécessaire. Cette section fournit un aperçu général de la manière dont le split tunneling fonctionne : Citrix ADC détermine le chemin du trafic en fonction de sa table de routage. Lorsque le split tunneling de Citrix ADC est activé, Secure Hub distingue le trafic réseau interne (protégé) du trafic Internet. Secure Hub procède en fonction du suffixe DNS et des applications intranet. Secure Hub tunnellise uniquement le trafic réseau interne via le tunnel VPN. Lorsque le split tunneling de Citrix ADC est désactivé, tout le trafic passe par le tunnel VPN.

- Si vous préférez surveiller tout le trafic pour des raisons de sécurité, désactivez le split tunneling de Citrix ADC. Dans ce cas, tout le trafic passe par le tunnel VPN.
- Si vous utilisez un tunnel VPN complet avec PAC, vous devez désactiver le split tunneling de Citrix Gateway. Si le split tunneling est activé et qu'un fichier PAC est configuré, les règles du fichier PAC remplacent les règles de split tunneling de Citrix ADC. Un serveur de proxy configuré dans une stratégie de trafic ne remplace pas les règles de split tunneling de Citrix ADC.

Par défaut, la stratégie **Accès réseau** est définie sur **Tunnélisé vers le réseau interne** pour Secure Web. Avec cette configuration, les applications MDX utilisent les paramètres de split tunneling de Citrix ADC. La stratégie **Accès réseau** par défaut diffère pour certaines autres applications de productivité mobiles.

Citrix Gateway dispose également d'un mode de split tunneling inverse à micro VPN. Cette configuration prend en charge une liste d'exclusion d'adresses IP qui ne sont pas tunnellisées sur Citrix ADC. Ces adresses sont envoyées en utilisant la connexion Internet de l'appareil. Pour plus d'informations sur le split tunneling inverse, veuillez consulter la documentation relative à Citrix Gateway.

XenMobile inclut une **liste d'exclusion de split tunneling inversé**. Pour empêcher que certains sites Web soient envoyés par un tunnel via Citrix Gateway : ajoutez une liste séparée par des virgules des noms de domaine complet (FQDN) ou des suffixes DNS qui se connectent à l'aide du réseau LAN. Cette stratégie s'applique uniquement au mode Navigation sécurisée avec Citrix Gateway configuré pour le split tunneling inverse.

Authentification

January 10, 2022

Dans un déploiement XenMobile, plusieurs considérations entrent en jeu lorsque vous choisissez la manière de configurer l'authentification. Cette section vous aidera à comprendre les différents facteurs qui affectent l'authentification en discutant des éléments suivants :

- Principales stratégies MDX, propriétés du client XenMobile et paramètres Citrix Gateway impliqués dans l'authentification
- Interaction des stratégies, des propriétés client et des paramètres
- Compromis de chaque choix

Cet article contient également trois exemples de configurations recommandées pour augmenter le niveau de sécurité.

D'une manière générale, une sécurité renforcée entraîne une expérience utilisateur moins optimale, car les utilisateurs doivent s'authentifier plus souvent. La façon dont vous conciliez ces préoccupations dépend des besoins et des priorités de votre organisation. En examinant les trois configurations recommandées, vous devriez mieux comprendre l'interaction entre les mesures d'authentification disponibles et la meilleure façon de déployer votre propre environnement XenMobile.

Modes d'authentification

Authentification en ligne : permet aux utilisateurs d'accéder au réseau XenMobile. Nécessite une connexion Internet.

Authentification hors connexion : se produit sur l'appareil. Les utilisateurs déverrouillent un coffre sécurisé et disposent d'un accès hors connexion à des éléments, tels que le courrier téléchargé, les sites Web mis en cache et les notes.

Méthodes d'authentification

Facteur unique

LDAP : vous pouvez configurer une connexion dans XenMobile à un ou plusieurs annuaires, tels que Active Directory, qui sont compatibles avec le protocole LDAP (Lightweight Directory Access Protocol). Cette méthode est couramment utilisée pour fournir une authentification unique (SSO) aux environnements d'entreprise. Vous pouvez choisir le code PIN Citrix avec la mise en cache du mot de passe Active Directory pour améliorer l'expérience utilisateur avec LDAP tout en assurant la sécurité des mots de passe complexes lors de l'inscription, de l'expiration du mot de passe et du verrouillage du compte.

Pour de plus amples informations, consultez la section Domaine ou domaine + STA.

Certificat client : XenMobile peut s'intégrer aux autorités de certification standard pour utiliser les certificats comme seule méthode d'authentification en ligne. XenMobile fournit ce certificat après l'inscription de l'utilisateur, ce qui nécessite un mot de passe à usage unique, une URL d'invitation ou des informations d'identification LDAP. Lorsque vous utilisez un certificat client comme méthode d'authentification principale, un code PIN Citrix est requis dans les environnements de certificat client uniquement pour sécuriser le certificat sur l'appareil.

XenMobile prend en charge la liste de révocation de certificats (CRL) uniquement pour une autorité de certification tierce. Si vous disposez d'une autorité de certification Microsoft configurée, XenMobile utilise Citrix ADC pour gérer la révocation. Lorsque vous configurez l'authentification basée sur un certificat client, vous devez décider si vous avez besoin de configurer le paramètre Liste de révocation de certificats (CRL) Citrix ADC, Enable CRL Auto Refresh. Cette étape permet de s'assurer que l'utilisateur d'un appareil en mode MAM exclusif ne peut pas s'authentifier à l'aide d'un certificat existant sur l'appareil. XenMobile émet de nouveau un nouveau certificat, car il n'interdit pas à un utilisateur de générer un certificat utilisateur si un certificat a été révoqué. Ce paramètre renforce la sécurité des entités PKI lorsque la CRL vérifie la présence d'entités PKI expirées.

Pour afficher un diagramme indiquant le déploiement requis si vous envisagez d'utiliser l'authentification par certificat pour les utilisateurs ou si vous devez utiliser votre autorité de certification d'entreprise pour émettre des certificats d'appareil, consultez l'article Architecture de référence pour les déploiements sur site.

Deux facteurs

LDAP + Certificat client : dans l'environnement XenMobile, cette configuration est la meilleure combinaison de sécurité et d'expérience utilisateur. Vous disposez des meilleures solutions d'authentification unique (SSO) couplées à une sécurité assurée par l'authentification à deux facteurs sur Citrix ADC. L'utilisation de LDAP et d'un certificat client assure la sécurité à l'aide d'informations déjà connues des utilisateurs (leurs mots de passe Active Directory) et de composants dont ils disposent déjà (les certificats clients sur leurs appareils). Secure Mail (et certaines autres applications de productivité mobiles) peut offrir et configurer automatiquement une première expérience d'utilisation des plus simples grâce à l'authentification du certificat client. Il faut pour cela qu'un environnement de serveur d'accès au client Exchange soit correctement configuré. Pour une utilisabilité optimale, vous pouvez combiner cette option avec le code PIN Citrix et la mise en cache du mot de passe Active Directory.

LDAP + jeton : il s'agit de la configuration classique des informations d'identification LDAP plus un mot de passe à usage unique, via le protocole RADIUS. Pour une utilisabilité optimale, vous pouvez combiner cette option avec le code PIN Citrix et la mise en cache du mot de passe Active Directory.

Stratégies, paramètres et propriétés client clés liés à l'authentification

Les stratégies, paramètres et propriétés client suivants entrent en jeu avec les trois configurations recommandées suivantes :

Stratégies MDX

Code secret d'application : si cette option est définie sur **Activé**, un code PIN ou un code secret Citrix est requis pour déverrouiller l'application lorsqu'elle démarre ou reprend après une période

d'inactivité. La valeur par défaut est **Activé**.

Pour configurer le délai d'inactivité pour toutes les applications, définissez la valeur INACTIVITY_TIMER en minutes dans **Propriétés du client** sur l'onglet **Paramètres**. La valeur par défaut est 15 minutes. Pour désactiver le délai d'inactivité, de façon à ce qu'une invite de saisie du code PIN ou du code secret invite s'affiche uniquement lorsque l'application démarre, définissez la valeur sur zéro.

> **Remarque :**
>
> si vous sélectionnez Secure offline pour la stratégie Encryption keys, cette stratégie est automatiquement activée.

Session en ligne requise : si cette option est définie sur **Activé**, l'utilisateur doit disposer d'une connexion au réseau d'entreprise et d'une session active. Si cette option est définie sur **Désactivé**, aucune session active n'est requise pour accéder à l'application sur l'appareil. La valeur par défaut est **Désactivé**.

Période hors connexion maximale (heures) : définit la durée maximale pendant laquelle une application peut s'exécuter sans avoir à reconfirmer les identifiants liés à l'application ni à actualiser les stratégies de XenMobile. Lorsque vous définissez la période hors connexion maximale, si Secure Hub pour iOS dispose d'un jeton Citrix Gateway valide, l'application récupère les nouvelles stratégies des applications MDX depuis XenMobile sans aucune interruption pour les utilisateurs. Si Secure Hub ne dispose pas d'un jeton Citrix ADC valide, les utilisateurs doivent s'authentifier via Secure Hub pour que les stratégies applicatives soient mises à jour. Le jeton Citrix ADC peut devenir non valide en cas d'absence d'activité dans la session Citrix Gateway ou de l'application d'une stratégie d'expiration de session. Lorsque les utilisateurs se connectent de nouveau à Secure Hub, ils peuvent continuer à exécuter l'application.

Les utilisateurs sont invités à se connecter 30, 15 et 5 minutes avant l'expiration de ce délai. Après expiration, l'application est bloquée jusqu'à ce que les utilisateurs se connectent. La valeur par défaut est **72 heures (3 jours)**. La période minimale est 1 heure.

> **Remarque :**
>
> N'oubliez pas que dans un scénario dans lequel les utilisateurs voyagent souvent et peuvent utiliser l'itinérance internationale, la valeur par défaut de 72 heures (3 jours) peut être trop courte.

Expiration du ticket des services d'arrière-plan : durée pendant laquelle un ticket de service réseau d'arrière-plan reste valide. Lorsque Secure Mail se connecte au travers de Citrix Gateway à un serveur Exchange exécutant ActiveSync, XenMobile délivre un jeton que Secure Mail utilise pour se connecter au serveur Exchange interne. Ce paramètre de propriété détermine la durée pendant laquelle Secure Mail peut utiliser le jeton sans requérir de nouveau jeton pour l'authentification et la connexion au serveur Exchange. Lorsque la limite de temps expire, les utilisateurs doivent ouvrir une session à

nouveau pour générer un nouveau jeton. La valeur par défaut est **168 heures (7 jours)**. Lorsque ce délai expire, les notifications par e-mail sont interrompues.

Période de grâce requise pour la session en ligne : détermine le nombre de minutes pendant lesquelles un utilisateur peut utiliser l'application hors ligne avant que la stratégie Session en ligne requise n'empêche son utilisation (jusqu'à ce que la session en ligne soit validée). La valeur par défaut est 0 (pas de période de grâce).

Pour plus d'informations sur les stratégies d'authentification, consultez

- Si vous utilisez le SDK MAM : Présentation du SDK MAM
- Si vous utilisez le MDX Toolkit : stratégies MDX pour iOS et stratégies MDX pour Android

Propriétés du client XenMobile

> **Remarque :**
>
> Les propriétés du client sont un paramètre global qui s'applique à tous les appareils qui se connectent à XenMobile.

Code PIN Citrix : pour une expérience de connexion simple, vous pouvez choisir d'activer le code PIN Citrix. Avec le code PIN, les utilisateurs n'ont pas besoin d'entrer d'autres informations d'identification de manière répétée, telles que leurs noms d'utilisateur et mots de passe Active Directory. Vous pouvez configurer le code PIN Citrix en tant qu'authentification hors connexion autonome uniquement, ou associer le code PIN avec la mise en cache du mot de passe Active Directory pour simplifier l'authentification pour une utilisabilité optimale. Vous pouvez configurer le code PIN Citrix dans **Paramètres > Client > Propriétés du client** dans la console XenMobile.

Vous trouverez ci-dessous un récapitulatif des propriétés les plus importantes. Pour de plus amples informations, consultez la section Propriétés du client.

ENABLE_PASSCODE_AUTH

Nom d'affichage : Enable Citrix PIN Authentication (Activer l'authentification du code PIN Citrix)

Cette clé permet d'activer la fonctionnalité de code PIN Citrix. Avec le code PIN ou code secret Citrix, les utilisateurs sont invités à définir un code PIN à utiliser à la place de leur mot de passe Active Directory. Activez ce paramètre si **ENABLE_PASSWORD_CACHING** est activé ou si XenMobile utilise l'authentification par certificat.

Valeurs possibles : true ou **false**

Valeur par défaut : false

ENABLE_PASSWORD_CACHING

Nom d'affichage : Enable User Password Caching (Activer la mise en cache du mot de passe de l'utilisateur)

Cette clé vous permet d'autoriser la mise en cache locale du mot de passe Active Directory de l'utilisateur sur l'appareil mobile. Lorsque vous définissez cette clé sur true, les utilisateurs sont invités à créer un code PIN ou code secret Citrix. La clé ENABLE_PASSCODE_AUTH doit être définie sur true lorsque vous définissez cette clé sur **true**.

Valeurs possibles : true ou **false**

Valeur par défaut : false

PASSCODE_STRENGTH

Nom d'affichage : PIN Strength Requirement (Exigences en matière de sûreté du code PIN)

Cette clé définit le niveau de sécurité du code PIN ou du code secret Citrix. Lorsque vous modifiez ce paramètre, les utilisateurs sont invités à définir un nouveau code PIN ou code secret Citrix la prochaine fois qu'ils sont invités à s'authentifier.

Valeurs possibles : Low, **Medium** ou **Strong**

Valeur par défaut : Medium

INACTIVITY_TIMER

Nom d'affichage : Inactivity Timer (Délai d'inactivité)

Cette clé définit la durée en minutes pendant laquelle les utilisateurs peuvent laisser leurs appareils inactifs et accéder à une application sans être invité à entrer un code PIN ou code secret Citrix. Pour activer ce paramètre pour une application MDX, vous devez définir le paramètre Code secret d'application sur **Activé**. Si le paramètre Code secret d'application est défini sur **Désactivé**, les utilisateurs sont redirigés vers Secure Hub pour effectuer une authentification complète. Lorsque vous modifiez ce paramètre, la valeur prend effet la prochaine fois que les utilisateurs sont invités à s'authentifier. La valeur par défaut est 15 minutes.

ENABLE_TOUCH_ID_AUTH

Nom d'affichage : Enable Touch ID Authentication (Activer l'authentification TouchID)

Permet l'utilisation du lecteur d'empreintes digitales (dans iOS uniquement) pour l'authentification hors connexion. L'authentification en ligne nécessitera toujours la méthode d'authentification principale.

ENCRYPT_SECRETS_USING_PASSCODE

Nom d'affichage : Encrypt secrets using Passcode (Chiffrer les secrets à l'aide d'un code secret)

Cette clé permet de stocker les données sensibles sur l'appareil mobile dans un coffre sécurisé plutôt que dans un magasin natif basé sur la plate-forme, tel que le trousseau iOS Cette clé de configuration permet un cryptage renforcé des artefacts clés, mais ajoute également une entropie utilisateur (un code PIN généré de manière aléatoire connu uniquement de l'utilisateur).

Valeurs possibles : true ou **false**

Valeur par défaut : false

Paramètres de Citrix ADC

Session time-out : si vous activez ce paramètre, Citrix Gateway déconnecte la session si Citrix ADC ne détecte aucune activité réseau pour l'intervalle spécifié. Ce paramètre est appliqué aux utilisateurs qui se connectent avec le plug-in Citrix Gateway, Citrix Receiver, Secure Hub ou via un navigateur Web. La valeur par défaut est **1440 minutes**. Si vous passez cette valeur à 0, ce paramètre est désactivé.

Force time-out : si vous activez ce paramètre, Citrix Gateway déconnecte la session une fois ce délai expiré, quelle que soit l'activité de l'utilisateur à ce moment. Une fois ce délai expiré, l'utilisateur ne peut rien faire pour empêcher cette déconnexion. Ce paramètre est appliqué aux utilisateurs qui se connectent avec le plug-in Citrix Gateway, Citrix Receiver, Secure Hub ou via un navigateur Web. Si Secure Mail utilise STA, un mode Citrix ADC spécial, le paramètre Force time-out ne s'applique pas aux sessions de Secure Mail. La valeur par défaut est **1440 minutes**. Si vous laissez cette valeur vide, le paramètre est désactivé.

Pour plus d'informations sur la configuration des paramètres de délai d'expiration dans Citrix Gateway, veuillez consulter la documentation relative à Citrix ADC.

Pour plus d'informations sur les scénarios qui invitent les utilisateurs à s'authentifier auprès de XenMobile en entrant des informations d'identification sur leurs appareils, consultez Scénarios d'invite d'authentification.

Paramètres de configuration par défaut

Ces paramètres sont les paramètres par défaut fournis par :

- Assistant NetScaler pour XenMobile
- SDK MAM ou MDX Toolkit
- Console XenMobile

Paramètre	Où trouver le paramètre	Paramètre par défaut
Session time-out	Citrix Gateway	1440 minutes
Force time-out	Citrix Gateway	1440 minutes
Période hors connexion maximale	Stratégies MDX	72 heures
Expiration du ticket des services d'arrière-plan	Stratégies MDX	168 heures (7 jours)
Session en ligne requise	Stratégies MDX	Désactivé

Paramètre	Où trouver le paramètre	Paramètre par défaut
Période de grâce requise pour la session en ligne	Stratégies MDX	0
Code secret d'application	Stratégies MDX	Activé
Encrypt secrets using passcode	Propriétés du client XenMobile	false
Enable Citrix PIN Authentication	Propriétés du client XenMobile	false
PIN Strength Requirement	Propriétés du client XenMobile	Medium (Moyen)
PIN Type	Propriétés du client XenMobile	Numeric
Enable User Password Caching	Propriétés du client XenMobile	false
Inactivity Timer	Propriétés du client XenMobile	15
Enable Touch ID Authentication	Propriétés du client XenMobile	false

Configurations recommandées

Cette section présente des exemples de trois configurations XenMobile allant de la sécurité la plus faible à une expérience utilisateur optimale, en passant par la sécurité la plus élevée et une expérience utilisateur plus intrusive. Ces exemples devraient vous fournir des points de référence utiles pour déterminer où sur l'échelle vous souhaitez placer votre propre configuration. Sachez que la modification de ces paramètres peut vous obliger à modifier d'autres paramètres. Par exemple, la période hors connexion maximale doit toujours être inférieure au délai d'expiration de la session.

Sécurité la plus élevée

Cette configuration offre le plus haut niveau de sécurité mais comporte des compromis importants en termes d'utilisabilité.

Paramètre	Où trouver le paramètre	Réglage recommandé	Impact du comportement
Session time-out	Citrix Gateway	1440	Les utilisateurs entrent leurs informations d'identification Secure Hub uniquement lorsqu'une authentification en ligne est requise : toutes les 24 heures.
Force time-out	Citrix Gateway	1440	L'authentification en ligne sera strictement requise toutes les 24 heures. L'activité ne prolonge pas la durée de la session.
Période hors connexion maximale	Stratégies MDX	23	Nécessite une actualisation de la stratégie tous les jours.

Expiration du ticket des services d'arrière-plan	Stratégies MDX	72 heures	Délai d'expiration pour STA, ce qui permet des sessions de longue durée sans jeton de session Citrix Gateway. Dans le cas de Secure Mail, un délai d'expiration STA plus long que le délai d'expiration de la session évite que les notifications par e-mail s'arrêtent sans que l'utilisateur ne soit invité à ouvrir l'application avant l'expiration de la session.
Session en ligne requise	Stratégies MDX	Désactivé	Assure une connexion réseau valide et une session Citrix Gateway pour utiliser les applications.
Période de grâce requise pour la session en ligne	Stratégies MDX	0	Aucune période de grâce (si vous avez activé la session en ligne requise).
Code secret d'application	Stratégies MDX	Activé	Exige un code secret pour l'application.
Encrypt secrets using passcode	Propriétés du client XenMobile	true	Une clé dérivée de l'entropie utilisateur protège le coffre.

Enable Citrix PIN Authentication	Propriétés du client XenMobile	true	Active le code PIN Citrix pour une expérience d'authentification simplifiée.
PIN Strength Requirement	Propriétés du client XenMobile	Strong	Exigence de complexité pour le mot de passe élevée
PIN Type	Propriétés du client XenMobile	Alphanumérique	Le code PIN est une séquence alphanumérique.
Activer la mise en cache du mot de passe	Propriétés du client XenMobile	false	Le mot de passe Active Directory n'est pas mis en cache et le code PIN Citrix sera utilisé pour les authentifications hors connexion.
Inactivity Timer	Propriétés du client XenMobile	15	Si l'utilisateur n'utilise pas les applications MDX ou Secure Hub pendant cette période, demandez une authentification hors connexion.
Enable Touch ID Authentication	Propriétés du client XenMobile	false	Désactive Touch ID pour les cas d'utilisation d'authentification hors connexion dans iOS.

Sécurité plus élevée

Cette configuration, une approche intermédiaire, nécessite que les utilisateurs s'authentifient plus souvent, tous les 3 jours au plus, au lieu de 7, augmentant ainsi le niveau de sécurité. L'augmentation du nombre d'authentifications permet de verrouiller le conteneur plus souvent, assurant la sécurité des données lorsque les appareils ne sont pas utilisés.

Paramètre	Où trouver le paramètre	Réglage recommandé	Impact du comportement
Session time-out	Citrix Gateway	4320	Les utilisateurs entrent leurs informations d'identification Secure Hub uniquement lorsqu'une authentification en ligne est requise : tous les 3 jours.
Force time-out	Citrix Gateway	Aucune valeur	Les sessions seront prolongées s'il y a une activité.
Période hors connexion maximale	Stratégies MDX	71	Nécessite une actualisation de la stratégie tous les 3 jours. La différence d'heure est pour permettre une actualisation avant l'expiration de la session.

Expiration du ticket des services d'arrière-plan	Stratégies MDX	168 heures	Délai d'expiration pour STA, ce qui permet des sessions de longue durée sans jeton de session Citrix Gateway. Dans le cas de Secure Mail, un délai d'expiration STA plus long que le délai d'expiration de la session évite que les notifications par e-mail s'arrêtent sans que l'utilisateur ne soit invité à ouvrir l'application avant l'expiration de la session.
Session en ligne requise	Stratégies MDX	Désactivé	Assure une connexion réseau valide et une session Citrix Gateway pour utiliser les applications.
Période de grâce requise pour la session en ligne	Stratégies MDX	0	Aucune période de grâce (si vous avez activé la session en ligne requise).
Code secret d'application	Stratégies MDX	Activé	Exige un code secret pour l'application.
Encrypt secrets using passcode	Propriétés du client XenMobile	false	Ne nécessite pas d'entropie utilisateur pour crypter le coffre.

Enable Citrix PIN Authentication	Propriétés du client XenMobile	true	Active le code PIN Citrix pour une expérience d'authentification simplifiée.
PIN Strength Requirement	Propriétés du client XenMobile	Medium (Moyen)	Applique des règles de complexité de mot de passe moyennes.
PIN Type	Propriétés du client XenMobile	Numeric	Le code PIN est une séquence numérique.
Activer la mise en cache du mot de passe	Propriétés du client XenMobile	true	Le code PIN de l'utilisateur met en cache et protège le mot de passe Active Directory.
Inactivity Timer	Propriétés du client XenMobile	30	Si l'utilisateur n'utilise pas les applications MDX ou Secure Hub pendant cette période, demandez une authentification hors connexion.
Enable Touch ID Authentication	Propriétés du client XenMobile	true	Active Touch ID pour les cas d'utilisation d'authentification hors connexion dans iOS.

Haute sécurité

Cette configuration, la plus pratique pour les utilisateurs, fournit une sécurité de base.

Paramètre	Où trouver le paramètre	Réglage recommandé	Impact du comportement
Session time-out	Citrix Gateway	10080	Les utilisateurs entrent leurs informations d'identification Secure Hub uniquement lorsqu'une authentification en ligne est requise : tous les 7 jours.
Force time-out	Citrix Gateway	Aucune valeur	Les sessions seront prolongées s'il y a une activité.
Période hors connexion maximale	Stratégies MDX	167	Nécessite une actualisation de la stratégie chaque semaine (tous les 7 jours). La différence d'heure est pour permettre une actualisation avant l'expiration de la session.

Expiration du ticket des services d'arrière-plan	Stratégies MDX	240	Délai d'expiration pour STA, ce qui permet des sessions de longue durée sans jeton de session Citrix Gateway. Dans le cas de Secure Mail, un délai d'expiration STA plus long que le délai d'expiration de la session évite que les notifications par e-mail s'arrêtent sans que l'utilisateur ne soit invité à ouvrir l'application avant l'expiration de la session.
Session en ligne requise	Stratégies MDX	Désactivé	Assure une connexion réseau valide et une session Citrix Gateway pour utiliser les applications.
Période de grâce requise pour la session en ligne	Stratégies MDX	0	Aucune période de grâce (si vous avez activé la session en ligne requise).
Code secret d'application	Stratégies MDX	Activé	Exige un code secret pour l'application.
Encrypt secrets using passcode	Propriétés du client XenMobile	false	Ne nécessite pas d'entropie utilisateur pour crypter le coffre.

Enable Citrix PIN Authentication	Propriétés du client XenMobile	true	Active le code PIN Citrix pour une expérience d'authentification simplifiée.
PIN Strength Requirement	Propriétés du client XenMobile	Faible	Aucune exigence de complexité pour le mot de passe
PIN Type	Propriétés du client XenMobile	Numeric	Le code PIN est une séquence numérique.
Activer la mise en cache du mot de passe	Propriétés du client XenMobile	true	Le code PIN de l'utilisateur met en cache et protège le mot de passe Active Directory.
Inactivity Timer	Propriétés du client XenMobile	90	Si l'utilisateur n'utilise pas les applications MDX ou Secure Hub pendant cette période, demandez une authentification hors connexion.
Enable Touch ID Authentication	Propriétés du client XenMobile	true	Active Touch ID pour les cas d'utilisation d'authentification hors connexion dans iOS.

Utilisation de l'authentification renforcée

Certaines applications peuvent nécessiter une authentification améliorée (par exemple, un facteur d'authentification secondaire, tel qu'un jeton ou des délais d'expiration de session agressifs). Vous contrôlez cette méthode d'authentification via une stratégie MDX. La méthode nécessite également un serveur virtuel distinct pour contrôler les méthodes d'authentification (sur les mêmes appliances ou sur des appliances Citrix ADC distinctes).

Paramètre	Où trouver le paramètre	Réglage recommandé	Impact du comportement
Citrix Gateway Alternatif	Stratégies MDX	Nécessite le nom de domaine complet et le port de l'appliance Citrix ADC secondaire.	Permet une authentification améliorée contrôlée par les stratégies d'authentification et de session de l'appliance Citrix ADC secondaire.

Si un utilisateur ouvre une application qui se connecte à l'autre instance Citrix Gateway, toutes les autres applications utiliseront cette instance Citrix Gateway pour communiquer avec le réseau interne. La session ne reviendra à l'instance Citrix Gateway de sécurité inférieure que lorsque la session de l'instance Citrix Gateway avec une sécurité renforcée expire.

Utilisation de Session en ligne requise

Pour certaines applications telles que Secure Web, vous pouvez vous assurer que les utilisateurs n'exécutent une application que lorsqu'ils ont une session authentifiée et que l'appareil est connecté à un réseau. Cette stratégie applique cette option et permet une période de grâce afin que les utilisateurs puissent terminer leur travail.

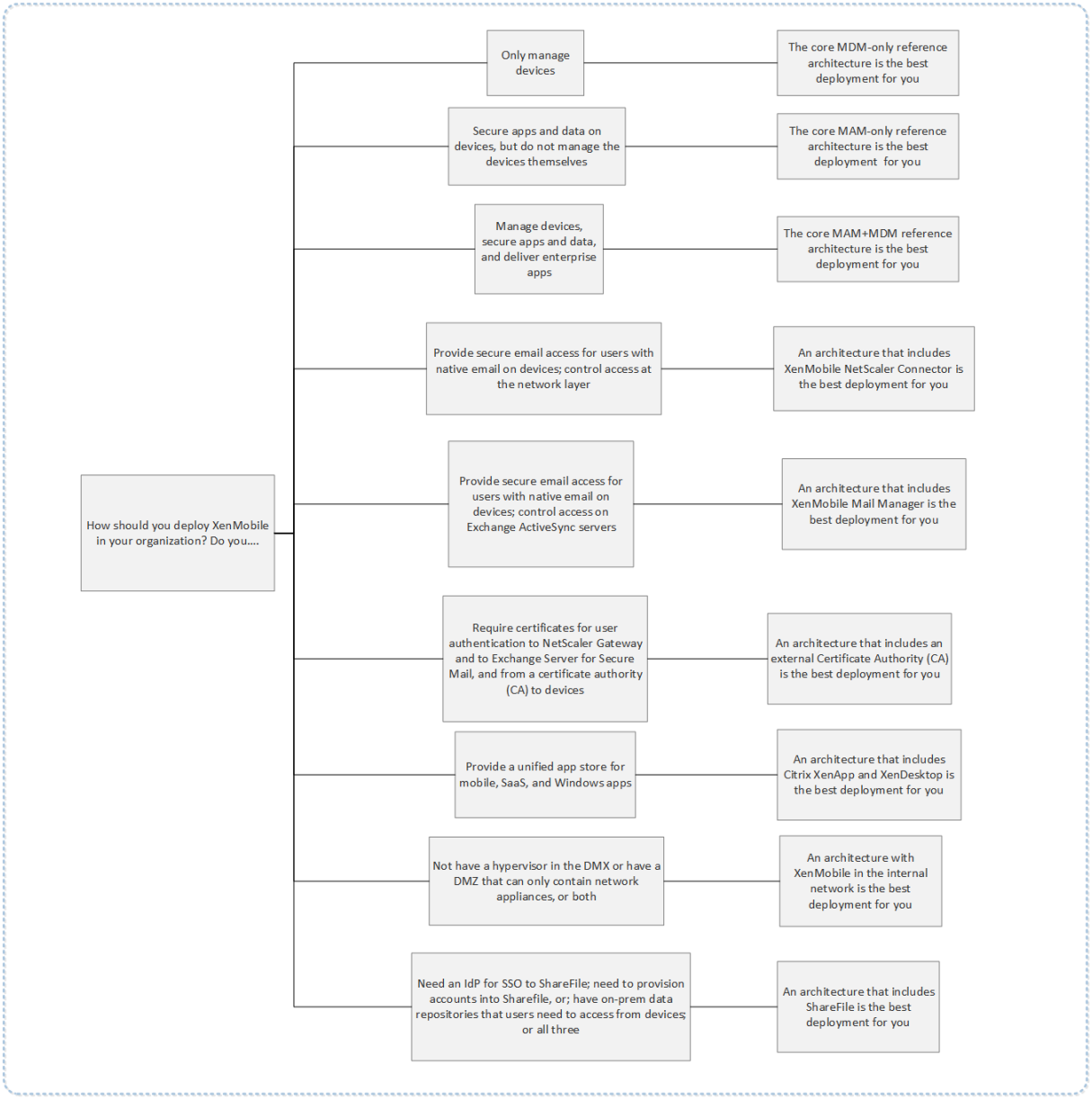
Paramètre	Où trouver le paramètre	Réglage recommandé	Impact du comportement
Session en ligne requise	Stratégies MDX	Activé	S'assure que l'appareil est en ligne et possède un jeton d'authentification valide.
Période de grâce requise pour la session en ligne	Stratégies MDX	15	Autorise une période de grâce de 15 minutes avant que l'utilisateur ne puisse plus utiliser les applications

Architecture de référence pour les déploiements sur site

January 10, 2022

Les figures de cet article illustrent les architectures de référence pour le déploiement de XenMobile sur site. Les scénarios de déploiement incluent le mode MDM exclusif, le mode MAM exclusif et le mode MDM + MAM en tant qu'architectures principales, ainsi que celles comprenant des composants tels que le gestionnaire SNMP, Citrix Gateway Connector pour Exchange ActiveSync, Endpoint Management Connector pour Exchange ActiveSync et Virtual Apps and Desktops. Les figures montrent les composants minimaux requis pour XenMobile.

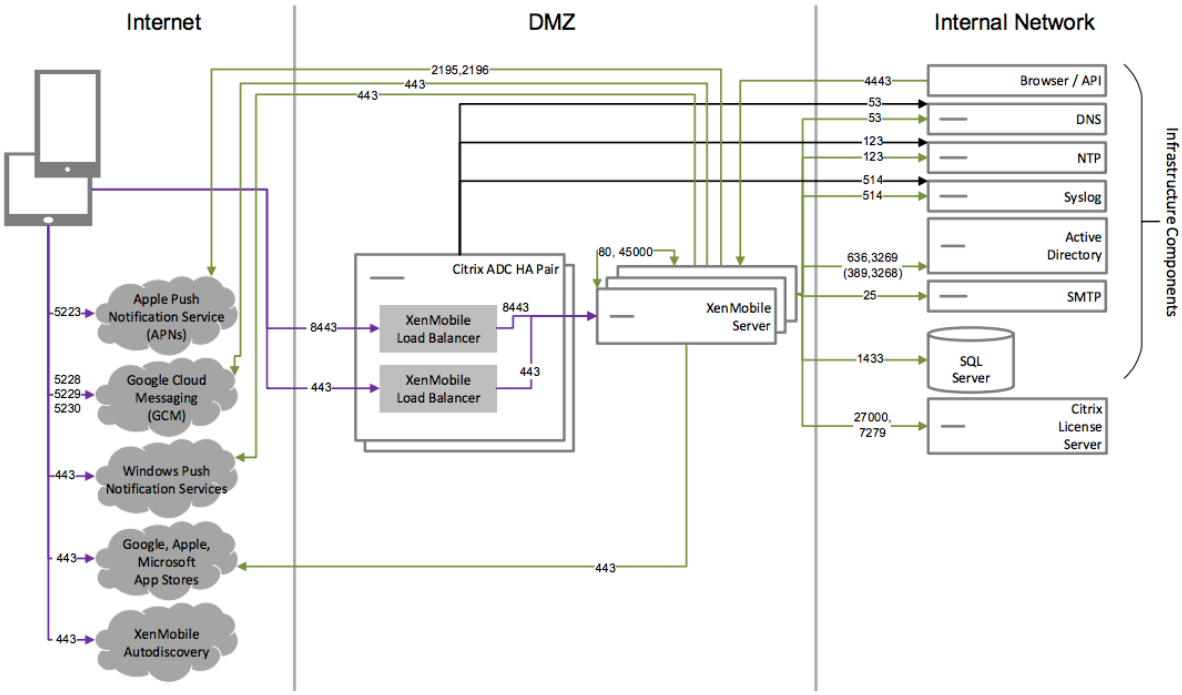
Utilisez ce tableau comme guide général pour vos décisions de déploiement.



Dans ces figures, les nombres sur les connecteurs représentent les ports devant être ouverts pour permettre les connexions entre les composants. Pour obtenir une liste complète des ports, consultez la section Configuration requise pour les ports dans la documentation XenMobile.

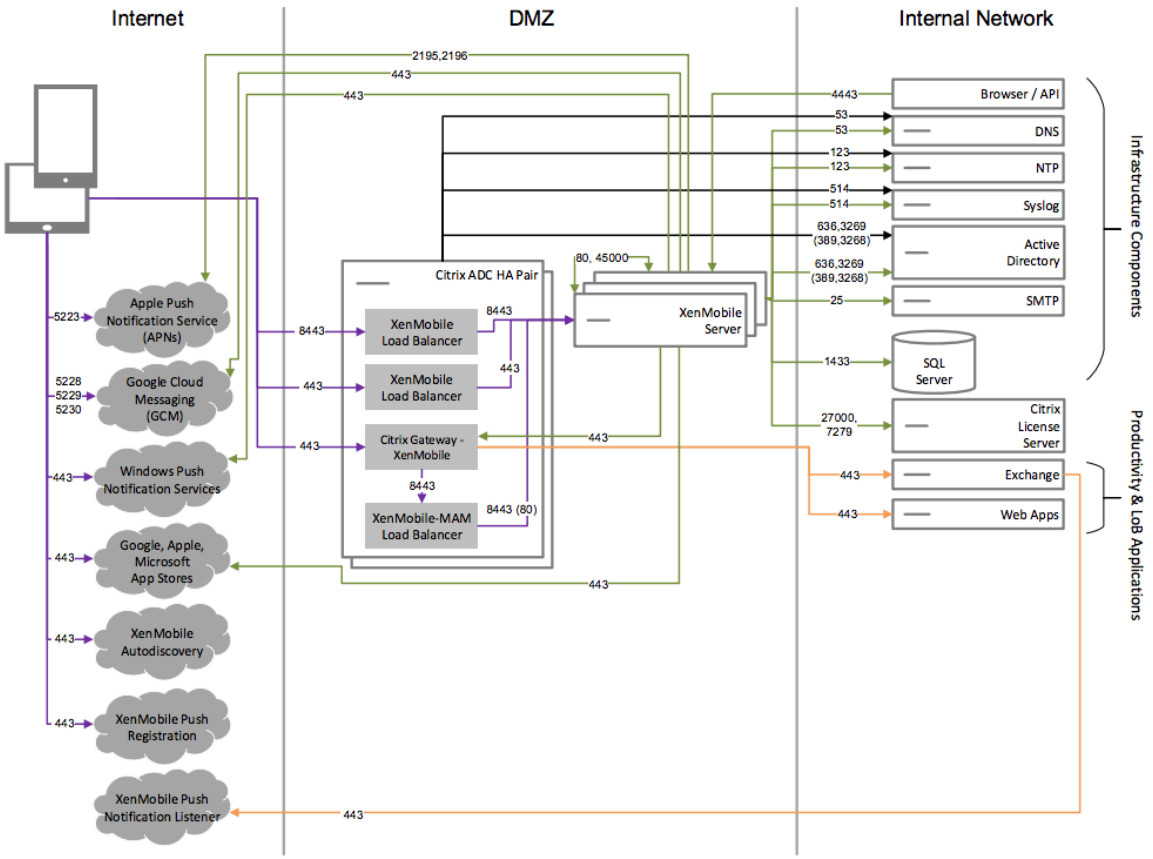
Architecture de référence principale pour le mode MDM exclusif

Déployez cette architecture si vous projetez d'utiliser uniquement les fonctionnalités MDM de XenMobile. Par exemple, vous devez gérer un appareil fourni par l'entreprise via MDM afin de déployer des stratégies, des applications et récupérer des inventaires logiciels, de même que pour pouvoir réaliser des actions sur les appareils, telles que l'effacement.



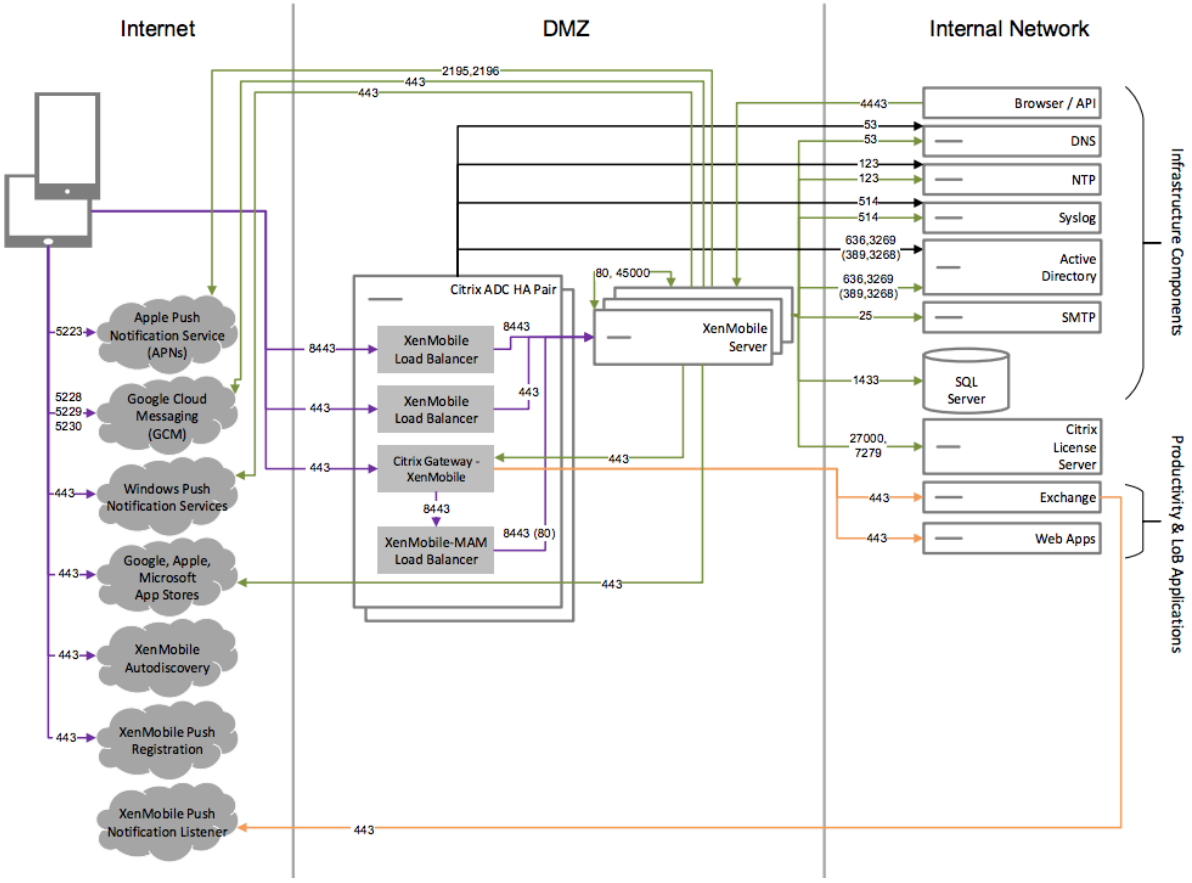
Architecture de référence principale pour le mode MAM exclusif

Déployez cette architecture si vous projetez d'utiliser uniquement les fonctionnalités MAM de XenMobile sans inscrire d'appareils auprès de MDM. Par exemple, vous souhaitez sécuriser les applications et données sur des appareils mobiles BYO ; vous souhaitez mettre à disposition des applications mobiles d'entreprise tout en ayant la possibilité de les verrouiller ou d'effacer les données des appareils. Les appareils ne peuvent pas être inscrits auprès de MDM.



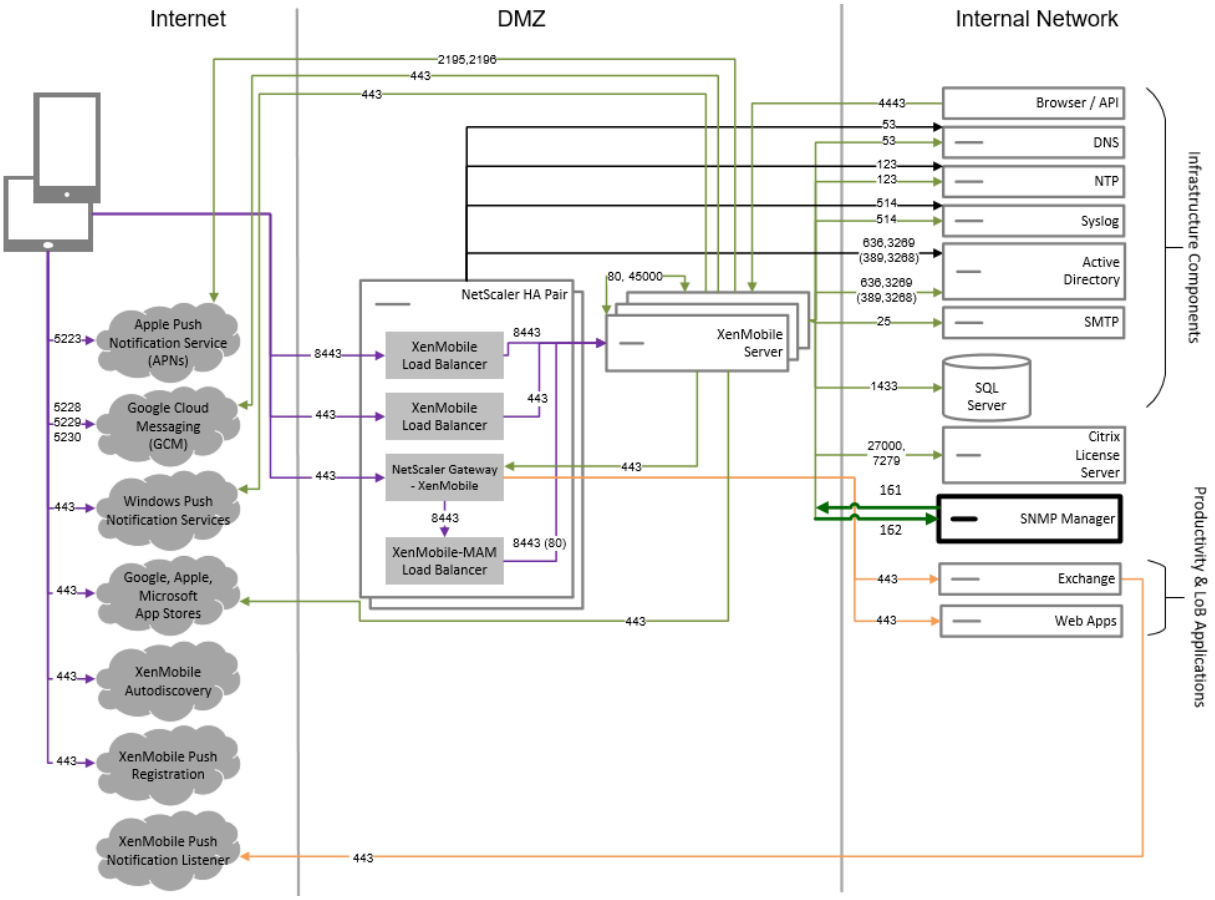
Architecture de référence principale pour le mode MAM+MDM

Déployez cette architecture si vous projetez d'utiliser les fonctionnalités MDM+MAM de XenMobile. Par exemple, vous souhaitez gérer un appareil fourni par l'entreprise via MDM ; vous souhaitez déployer des stratégies et des applications, récupérer l'inventaire des logiciels et être en mesure d'effacer les appareils. Vous souhaitez également mettre à disposition des applications mobiles d'entreprise tout en ayant la possibilité de les verrouiller ou d'effacer les données des appareils.



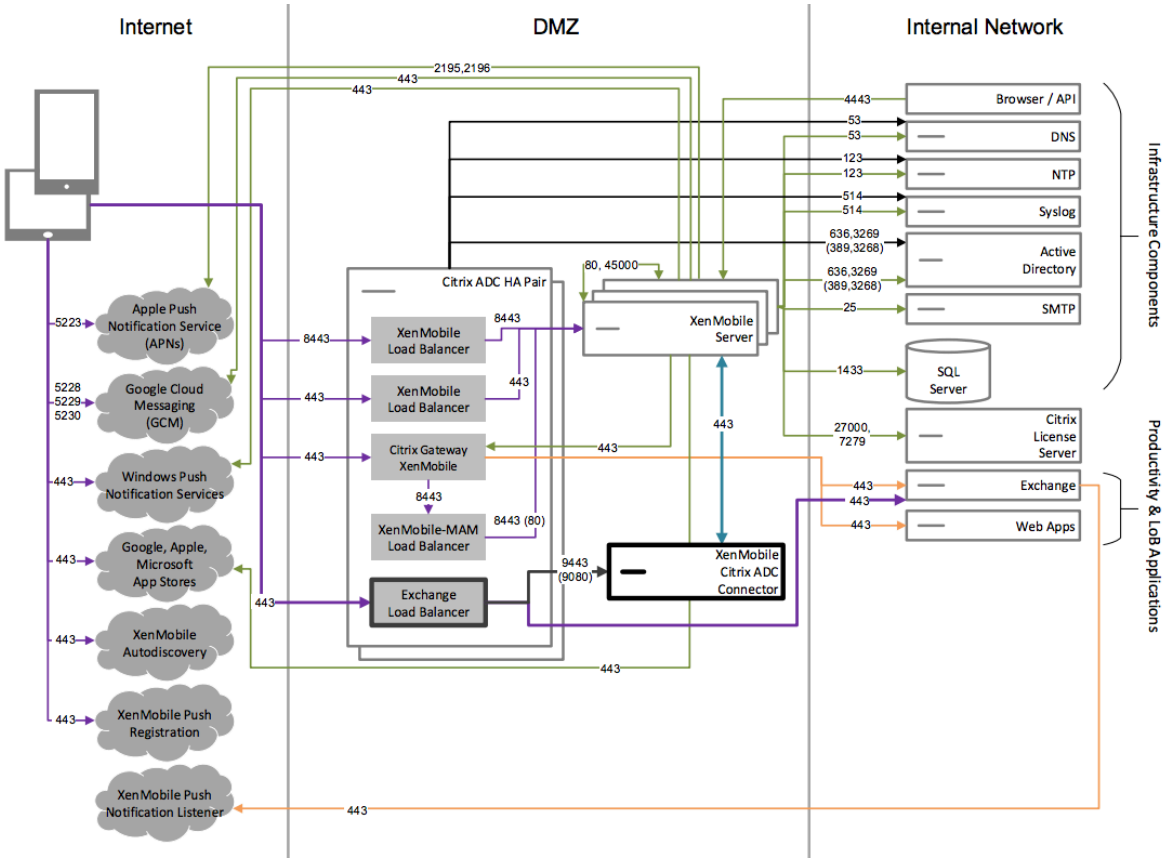
Architecture de référence avec SNMP

Déployez cette architecture si vous prévoyez d'activer la surveillance SNMP avec XenMobile. Par exemple, vous souhaitez autoriser les systèmes de surveillance à interroger et à obtenir des informations sur vos nœuds XenMobile. Pour plus d'informations, consultez la section Surveillance SNMP.



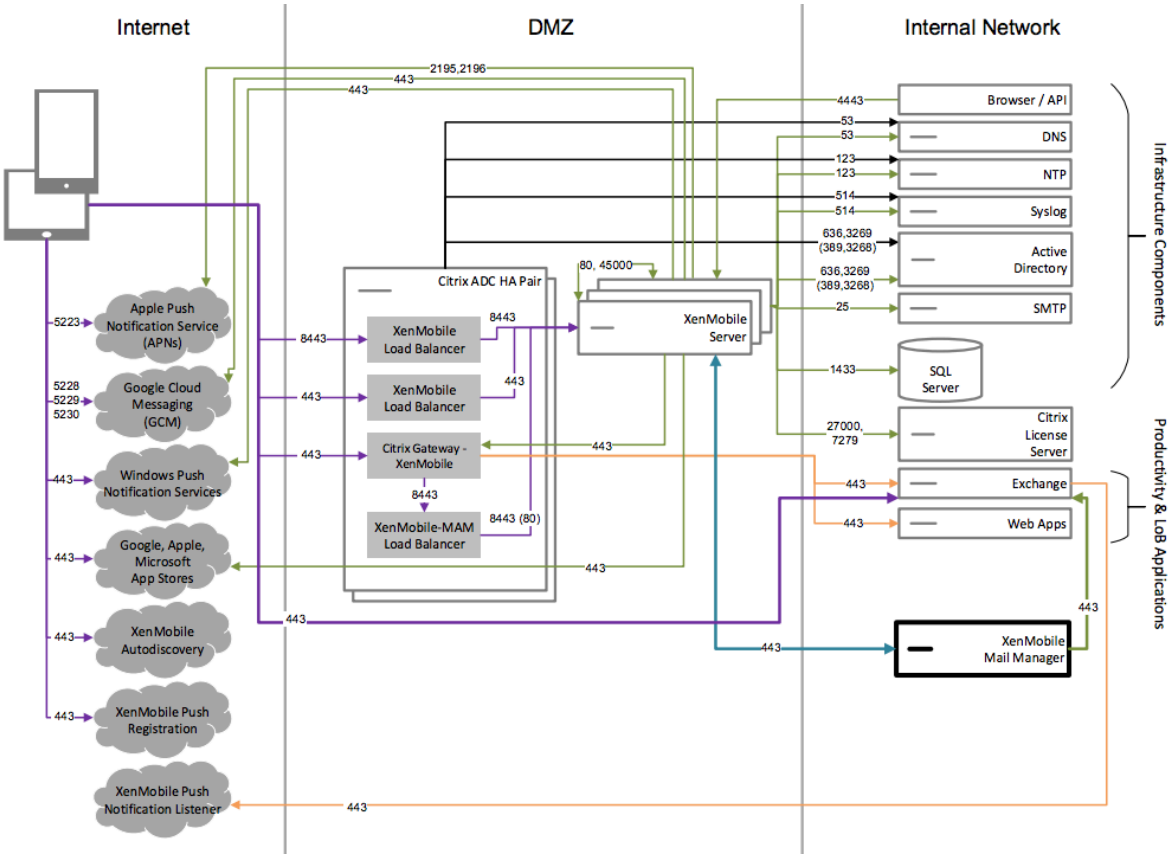
Architecture de référence avec Citrix Gateway Connector pour Exchange ActiveSync

Déployez cette architecture si vous envisagez d'utiliser Citrix Gateway Connector pour Exchange ActiveSync avec XenMobile. Par exemple, vous devez fournir un accès sécurisé à la messagerie aux utilisateurs qui utilisent des applications de messagerie mobile natives. Ces utilisateurs continueront à accéder à la messagerie via une application native ou vous pourrez les transférer au fil du temps vers Citrix Secure Mail. Le contrôle d'accès doit avoir lieu au niveau de la couche réseau avant que le trafic n'atteigne les serveurs Exchange Active Sync. Même si le diagramme illustre le déploiement du connecteur pour Exchange ActiveSync dans une architecture MDM ou MAM, vous pouvez également déployer le connecteur pour Exchange ActiveSync dans une architecture pour le mode MDM exclusif.



Architecture de référence avec Endpoint Management Connector pour Exchange ActiveSync

Déployez cette architecture si vous envisagez d'utiliser Endpoint Management Connector pour Exchange ActiveSync avec XenMobile. Par exemple, vous souhaitez fournir un accès sécurisé à la messagerie aux utilisateurs qui utilisent des applications de messagerie mobile natives. Ces utilisateurs continueront à accéder à la messagerie via une application native ou vous pourrez les transférer au fil du temps vers Secure Mail. Vous pouvez obtenir un contrôle d'accès sur les serveurs Exchange ActiveSync. Même si le diagramme présente le déploiement d'Endpoint Management connector pour Exchange ActiveSync dans une architecture MDM et MAM, vous pouvez également déployer Endpoint Management Connector pour Exchange ActiveSync dans une architecture pour le mode MDM exclusif.

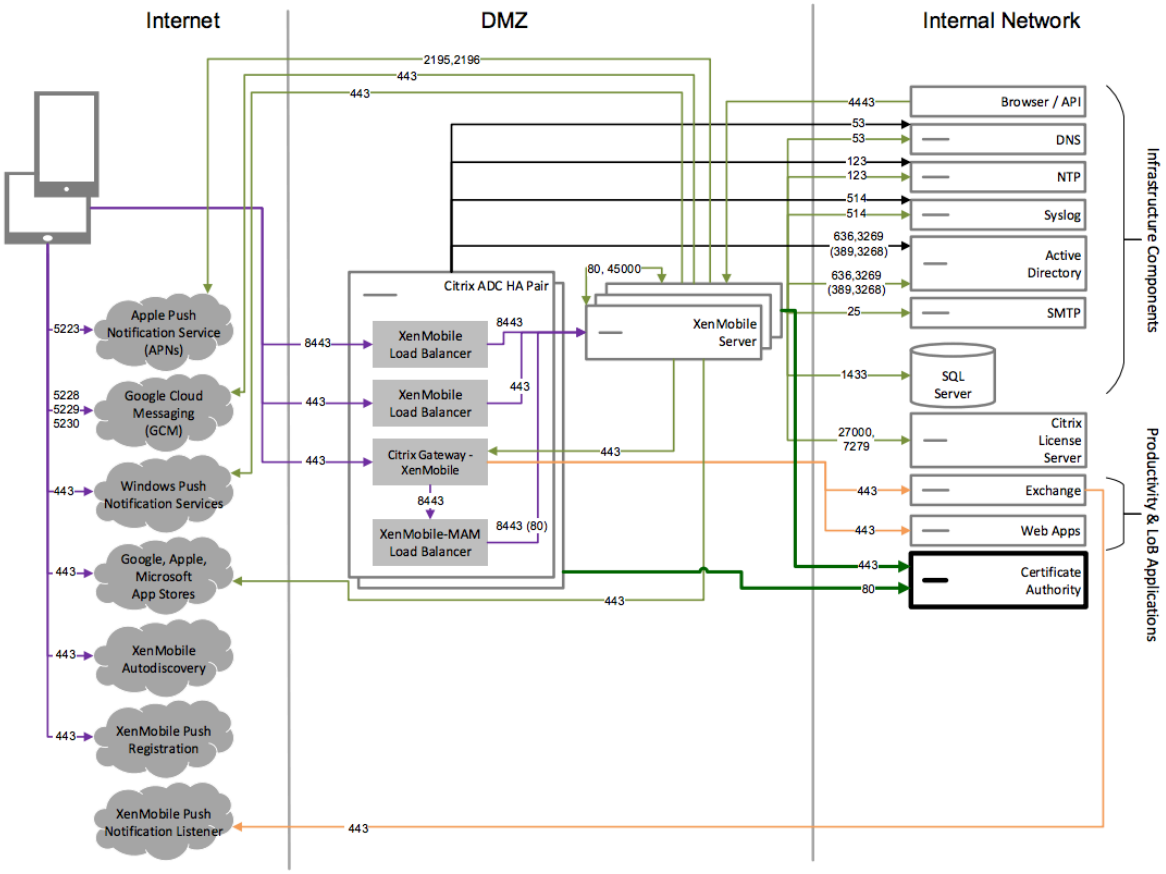


Architecture de référence avec une autorité de certification externe

Un déploiement incluant une autorité de certification externe est recommandé pour répondre à une ou plusieurs des exigences suivantes :

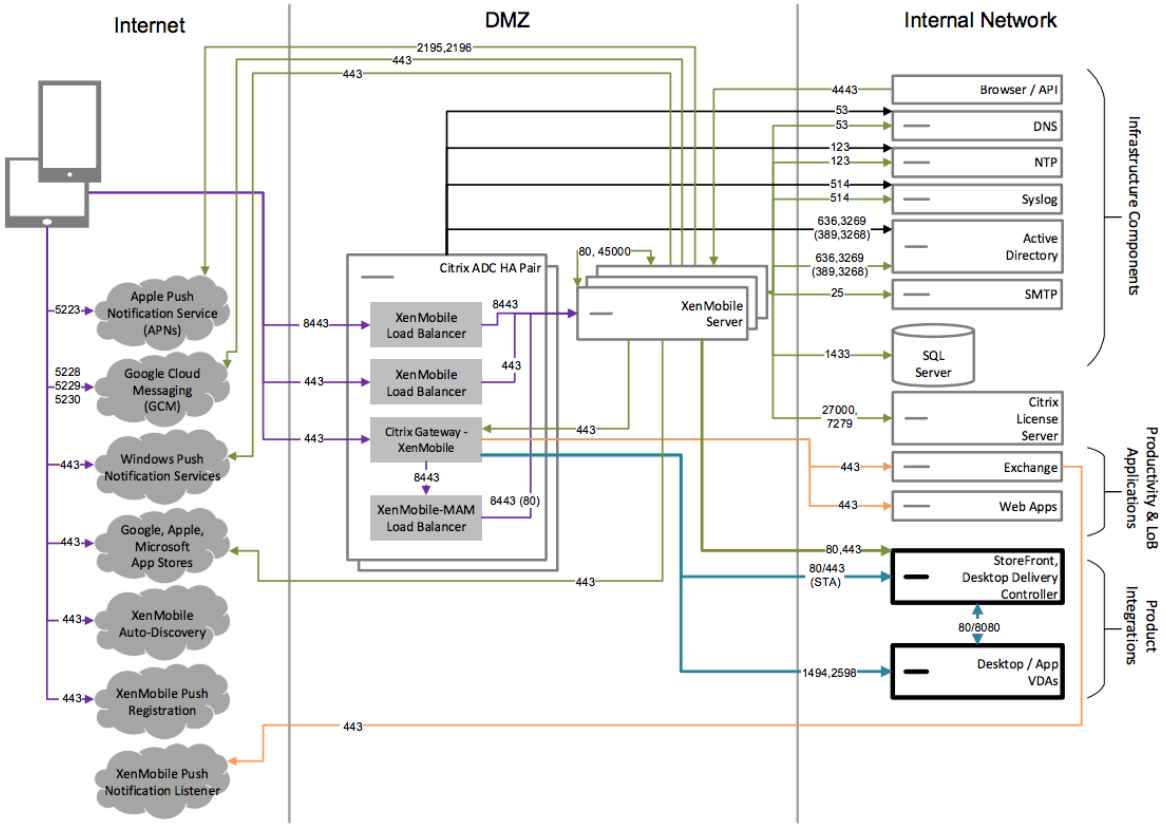
- Vous avez besoin de certificats utilisateur pour l'authentification utilisateur auprès de Citrix Gateway (pour un accès intranet).
- Les utilisateurs de Secure Mail doivent s'authentifier auprès de Exchange Server à l'aide d'un certificat utilisateur.
- Par exemple, vous devez transférer les certificats émis par l'autorité de certification de votre entreprise sur des appareils mobiles pour un accès WiFi.

Même si le diagramme illustre le déploiement d'une autorité de certification externe dans une architecture MDM et MAM, vous pouvez également déployer une autorité de certification externe dans une architecture pour le mode MDM exclusif ou pour le mode MAM exclusif.



Architecture de référence avec Virtual Apps and Desktops

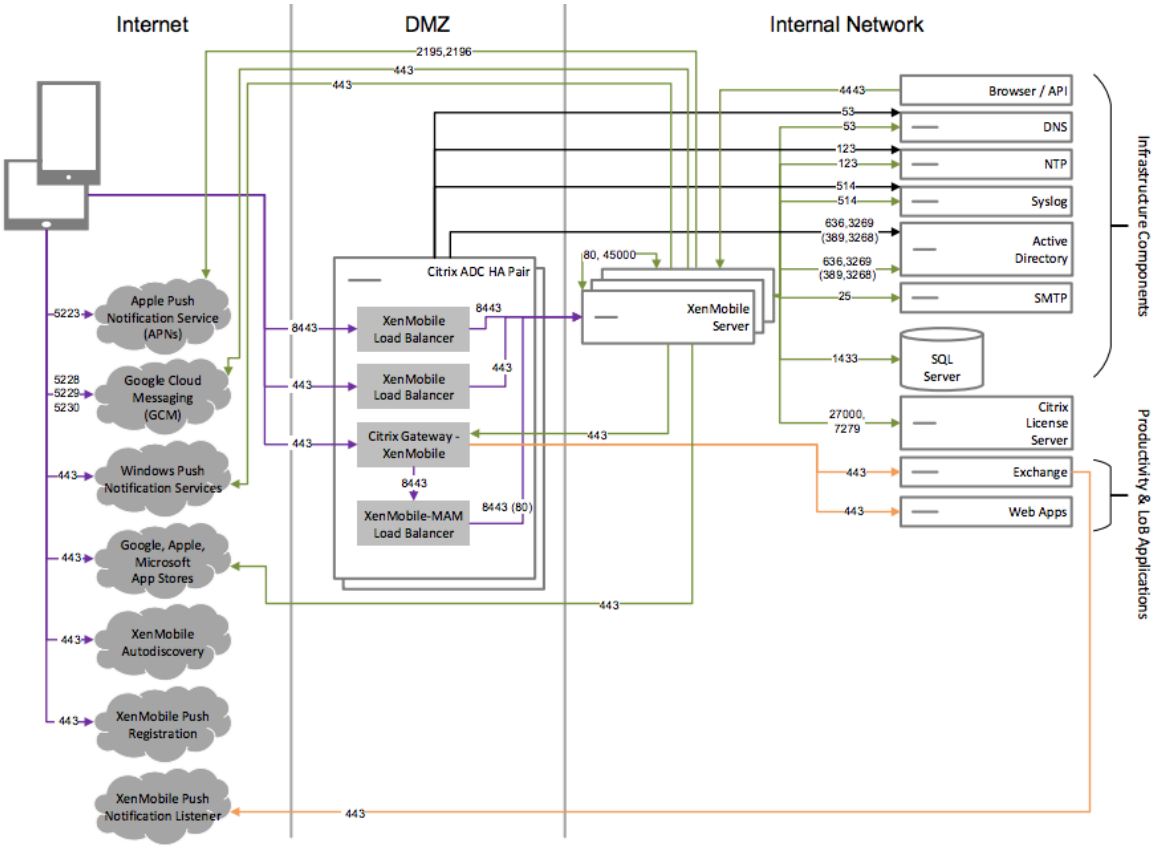
Déployez cette architecture si vous souhaitez intégrer Virtual Apps and Desktops à XenMobile. Par exemple, vous devez fournir un magasin d'applications unifié aux utilisateurs mobiles pour tous les types d'applications (mobile, SaaS et Windows). Même si le diagramme illustre le déploiement de Virtual Desktops dans une architecture MDM et MAM, vous pouvez également déployer ces bureaux dans une architecture pour le mode MAM exclusif.



Architecture de référence avec XenMobile dans le réseau interne

Vous pouvez déployer une architecture avec XenMobile dans le réseau interne afin de répondre à une ou plusieurs des exigences suivantes :

- Vous ne disposez pas d'un hyperviseur dans la zone démilitarisée (DMZ) ou vous n'êtes pas autorisé à disposer d'un hyperviseur dans la DMZ.
- Votre DMZ peut uniquement contenir des appliances de réseau.
- Vos exigences en matière de sécurité nécessitent l'utilisation du déchargement SSL.



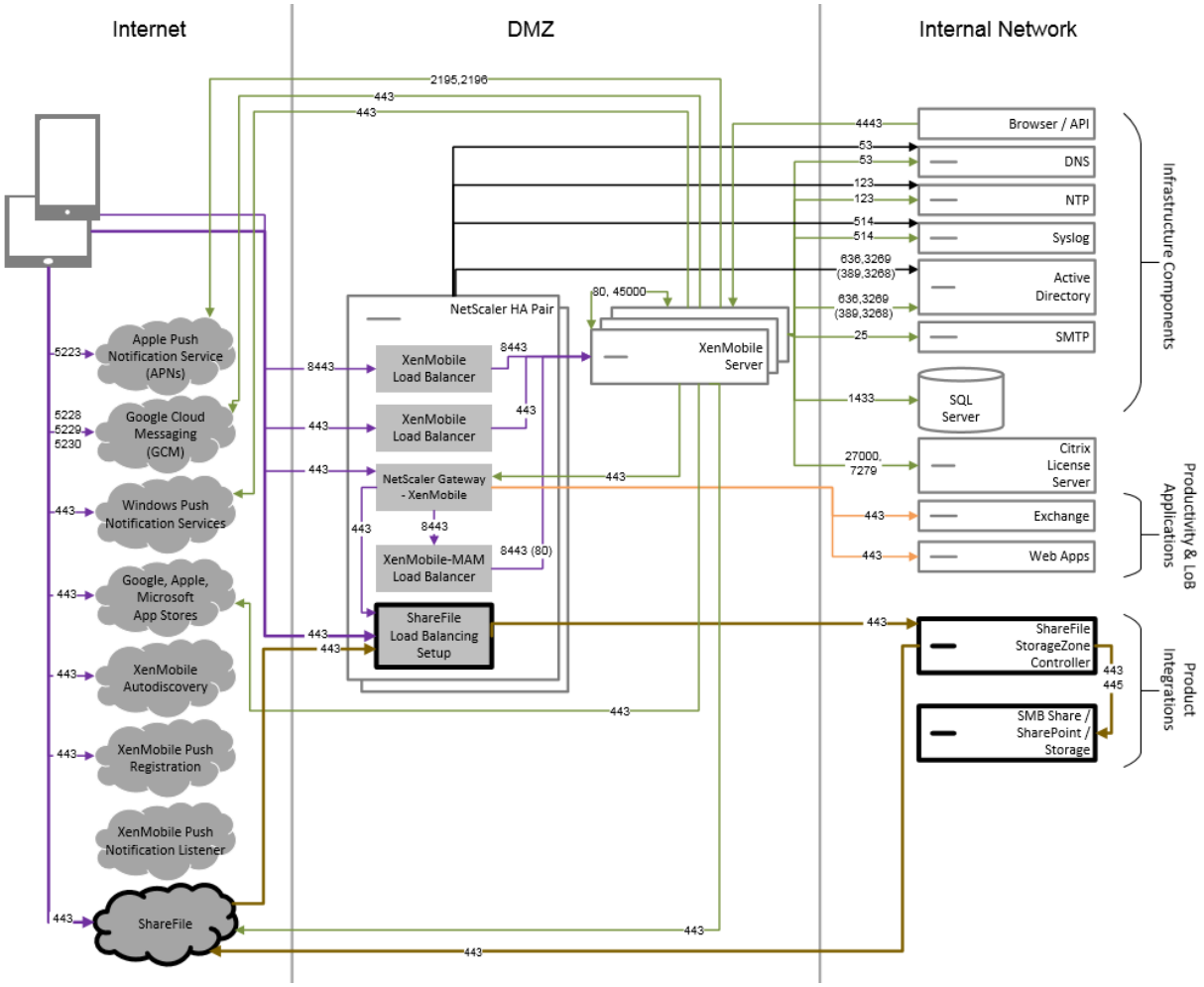
Architecture de référence avec Citrix Content Collaboration

Déployez cette architecture si vous souhaitez intégrer Citrix Files ou uniquement des connecteurs StorageZone avec XenMobile. L'intégration de Citrix Files vous permet de répondre à une ou plusieurs des exigences suivantes :

- Vous avez besoin d'un fournisseur d'identité pour donner aux utilisateurs une authentification unique (SSO) à ShareFile.com.
- Vous avez besoin d'un moyen de provisionner des comptes dans ShareFile.com.
- Vous avez des référentiels de données sur site auxquels vous devez accéder à partir d'appareils mobiles.

Une intégration avec des connecteurs StorageZone exclusivement donne aux utilisateurs un accès mobile sécurisé aux référentiels de stockage locaux existants, tels que des sites SharePoint et des partages de fichiers réseau. Dans cette configuration, la configuration d'un sous-domaine Citrix Content Collaboration, le provisioning d'utilisateurs pour Citrix Files ou l'hébergement de données Citrix Files ne sont pas nécessaires.

Même si le diagramme illustre le déploiement de Citrix Files dans une architecture MDM et MAM, vous pouvez également déployer Citrix Files dans une architecture pour le mode MAM exclusif.



Propriétés du serveur

January 10, 2022

Les propriétés de serveur sont des propriétés globales qui s'appliquent aux opérations, utilisateurs et appareils sur une instance XenMobile entière. Citrix vous recommande d'évaluer pour votre environnement les propriétés de serveur abordées dans cet article. Assurez-vous de consulter Citrix avant de modifier d'autres propriétés du serveur.

La modification de certaines propriétés de serveur nécessite un redémarrage de chaque nœud de serveur XenMobile. XenMobile vous informe lorsqu'un redémarrage est requis.

Certaines propriétés de serveur contribuent à améliorer les performances et la stabilité. Pour plus d'informations, consultez la section Optimisation des opérations XenMobile.

Mettre à disposition les applications Android d'ancienne génération sur les appareils Android Enterprise : si l'option `afw.allow.legacy.apps` est définie sur **`true`**, les appareils Android Enter-

prise reçoivent à la fois les applications Android d'ancienne génération et les applications Android Enterprise. Si l'option est définie sur **false**, les appareils Android Enterprise reçoivent uniquement les applications Android Enterprise. La valeur par défaut est **true**.

Autoriser les extensions de fichier pour la stratégie de fichiers : configurez l'option `file.extension.whitelist` à l'aide d'une liste séparée par des virgules des types de fichiers que les administrateurs peuvent charger à l'aide de la stratégie de fichiers. Les types de fichiers suivants ne peuvent pas être chargés même si vous les ajoutez à cette liste d'autorisation :

- .cab
- .appx
- .ipa
- .apk
- .xap
- .mdx
- .exe

La valeur par défaut est `7z,rar,zip,csv,xls,xlsx,jad,jar,pdf,bmp,gif,jpg,png,pps,ppt,pptx,bsh,js,lua,mscr,pl,py,rb,sh,tcl,txt,htm,html,doc,docx,rtf,xap`.

Accéder à toutes les applications du Google Play Store d'entreprise. Si la valeur est **true**, XenMobile rend toutes les applications du Google Play Store public accessibles depuis le Google Play Store d'entreprise. La définition de cette propriété sur **true** autorise les applications du Google Play Store public pour tous les utilisateurs d'Android Entreprise. Les administrateurs peuvent ensuite utiliser la stratégie Restrictions pour contrôler l'accès à ces applications. Valeur par défaut **false**.

Inscription d'appareils Android Enterprise en mode profil de travail sur appareils appartenant à l'entreprise. Lorsque l'option `afw.work_profile_for_corporate_owned_device.enrollment_mode.enabled` est définie sur **true**, les appareils exécutant Android 11 ou version ultérieure peuvent s'inscrire au mode profil de travail sur appareils appartenant à l'entreprise (mode WPCOD). La console XenMobile Server reflète les modifications apportées à ce mode d'inscription. Si cette option est définie sur **false**, aucun paramètre WPCOD n'est disponible. La valeur par défaut est **true**.

Paramètres de restrictions Android Enterprise supplémentaires. Si la propriété `afw.restriction.policy.v2` est définie sur **true**, les paramètres de restriction suivants sont disponibles pour les appareils Android Enterprise :

- Autoriser désinstallation d'applications
- Autoriser le partage Bluetooth

Pour de plus amples informations sur ces paramètres, consultez la section Stratégies de restrictions.

Restrictions Android Enterprise pour les appareils COPE. Définissez l'option `afw.restriction.cope` sur **true** pour activer le paramètre **Appliquer aux appareils entièrement gérés avec un profil**

de travail/profil de travail sur appareils appartenant à l'entreprise dans la stratégie de restrictions. La valeur par défaut est **true**. Pour de plus amples informations sur ce paramètre, consultez la section Stratégies de restrictions.

Autoriser les noms d'hôte pour les liens App Store iOS : la propriété `ios.app.store.allowed.hostnames` est une liste des noms d'hôtes autorisés utilisés lors du chargement d'applications publiques de l'App Store sur le serveur à l'aide des API publiques. Si vous envisagez de charger des applications publiques de l'App Store à l'aide des API publiques plutôt que de les charger via le serveur, configurez cette propriété. La valeur par défaut est `itunes.apple.com,vpp.itunes.apple.com,apps.apple.com`.

Port APNS secondaire. Vous pouvez utiliser le port 2197 au lieu du port 443 pour envoyer et recevoir des notifications APNs depuis `api.push.apple.com`. Le port utilise l'API du fournisseur APNs basé sur HTTP/2. Définissez la propriété `apns.http2.alternate.port.enabled` sur **true** pour utiliser le port 2197. La valeur par défaut de la propriété de serveur `apns.http2.alternate.port.enabled` est **false**.

Activer la validation du mot de passe pour empêcher l'ajout d'utilisateurs locaux possédant des mots de passe faibles. Si l'option `enable.password.strength.validation` est définie sur **true**, vous ne pouvez pas ajouter d'utilisateurs locaux possédant un mot de passe faible. Si cette option est définie sur **false**, vous pouvez créer des utilisateurs locaux possédant un mot de passe faible à l'aide de l'API publique. La valeur par défaut est **true**.

Bloquer l'inscription des appareils iOS jailbreakés et des appareils Android rootés : lorsque cette propriété est définie sur **true**, XenMobile bloque les inscriptions pour les appareils Android rootés et les appareils iOS jailbreakés. La valeur par défaut est **true**. Le paramètre recommandé est **true** pour tous les niveaux de sécurité.

Inscription requise : `wsapi.mdm.required.flag` cette propriété, qui s'applique uniquement lorsque le mode de XenMobile Server est défini sur ENT, indique si vous souhaitez que les utilisateurs s'inscrivent à MDM. La propriété s'applique à tous les utilisateurs et appareils de l'instance XenMobile. La nécessité d'une inscription offre un niveau de sécurité supérieur. Cependant, cette décision dépend si vous voulez exiger MDM ou non. Par défaut, l'inscription n'est pas requise.

Lorsque cette propriété est définie sur **false**, les utilisateurs pourront refuser l'inscription, mais ne pourront toujours accéder aux applications sur leurs appareils via le XenMobile Store. Lorsque cette propriété est définie sur **true**, tout utilisateur refusant l'inscription se voit refuser l'accès aux applications.

Si vous modifiez cette propriété après l'inscription des utilisateurs, les utilisateurs doivent se réinscrire.

Pour plus d'informations sur l'exigence (ou non) d'une inscription MDM, consultez la section Gestion des appareils et inscription MDM.

Enable multimode enrollment : la propriété `enable.multimode.xms` permet de créer des profils d'inscription sur un XenMobile Server qui contrôle les paramètres d'inscription pour la gestion des appareils et des applications pour Android et iOS. En outre, la nouvelle fonctionnalité de profils d'inscription améliorés permet l'inscription d'appareils dédiés pour Android et l'inscription MAM exclusif pour les appareils Android et iOS. Lorsque cette propriété est **`false`**, ces options d'inscription ne sont pas disponibles lors de la configuration de profils d'inscription. La valeur par défaut est **`true`**. Les appareils qui s'inscrivent lorsque cette propriété est **`true`** fonctionnent toujours si vous réglez la propriété sur **`false`**.

Activer le portail d'auto-assistance : si `shp.console.enable` est **`false`**, empêche l'accès au portail en libre-service. Les utilisateurs qui accèdent au portail en libre-service sur le port 443 reçoivent une erreur 404. Les utilisateurs qui accèdent au portail sur le port 4443 reçoivent un message « Accès refusé ». Si cette propriété est définie sur **`true`**, permet d'accéder au portail en libre-service via le port 443. Valeur par défaut **`false`**.

Local user account lockout limit : à l'aide de la stratégie de restriction, vous pouvez définir une limite sur les tentatives de connexion pour les utilisateurs Active Directory. Utilisez la clé `local.user.account.lockout.limit` pour faire de même pour les comptes d'utilisateurs locaux. Une fois que les utilisateurs ont tenté de se connecter le nombre de fois que vous spécifiez, ils ne peuvent pas réessayer tant qu'un certain temps ne s'est pas écoulé. Configurez ce délai avec la propriété **Local user account lockout time**. La valeur par défaut est `6`.

Local user account lockout time : la propriété `local.user.account.lockout.time` vous permet de définir un nombre de minutes qui doivent s'écouler avant qu'un compte d'utilisateur local verrouillé puisse tenter de se connecter à nouveau. La valeur par défaut est de `30` minutes.

Maximum size of file upload restriction enabled : activez la restriction de la taille maximale de fichier pour les chargements, paramètre `max.file.size.upload.restriction` sur **`true`**. Si vous activez cette restriction, configurez la taille maximale du fichier à l'aide de `max.file.size.upload.allowed`. La valeur par défaut de cette propriété est **`true`**.

Maximum size of file upload allowed : avec `max.file.size.upload.allowed`, vous pouvez définir une taille maximale de fichier pour les chargements. Exemples de valeur : `500 B`, `1 KB`, `1 MB`, `1 MiB`, `1 G` ou `1 GiB`. La valeur par défaut est `5 MB`.

Délai d'inactivité en minutes : il s'agit du nombre de minutes après lequel XenMobile ferme la session d'un utilisateur inactif qui utilisait l'API publique de XenMobile Server pour accéder à la console XenMobile ou à toute application tierce. Un délai d'expiration de `0` signifie qu'un utilisateur inactif reste connecté. Pour les applications tierces qui accèdent à l'API, il est généralement nécessaire de rester connecté. La valeur par défaut est `5`.

Inscription à la gestion des appareils iOS : installer l'autorité de certification racine si nécessaire : le dernier workflow d'inscription d'Apple nécessite que les utilisateurs installent manuellement les profils MDM. Ce workflow ne s'applique pas à l'inscription MDM aux serveurs affectés dans

Apple Business Manager ou Apple School Manager. Toutefois, lors de l'inscription manuelle dans MDM, les utilisateurs d'appareils iOS reçoivent uniquement l'invite de certificat d'appareil MDM lors de l'inscription.

Pour améliorer l'expérience utilisateur lors de l'inscription manuelle, Citrix recommande de modifier la propriété du serveur `ios.mdm.enrollment.installRootCaIfRequired` sur **`false`**. La valeur par défaut est **`true`**. Avec cette modification, une fenêtre Safari s'ouvre pendant l'inscription MDM afin de simplifier l'installation du profil pour les utilisateurs.

Intervalle de ligne de base minimum VPP : la propriété `vpp.baseline` définit l'intervalle minimum après lequel XenMobile ré-importe les licences d'achat en volume depuis Apple. L'actualisation des informations de licence permet de s'assurer que XenMobile reflète toutes les modifications, par exemple en cas de suppression manuelle d'une application importée à partir de l'achat en volume. Par défaut, XenMobile actualise la ligne de base de licence d'achat en volume toutes les `1440` minutes au minimum.

Si de nombreuses licences d'achat en volume sont installées (plus de 50 000, par exemple), Citrix vous recommande d'augmenter l'intervalle de ligne de base pour réduire la charge de l'importation de licences. Si vous prévoyez des modifications fréquentes de licence d'achat en volume depuis Apple, Citrix vous recommande de réduire la valeur pour que XenMobile reste à jour. L'intervalle minimal entre deux lignes de base est de 60 minutes. Étant donné que la tâche cron s'exécute toutes les 60 minutes, si l'intervalle entre les références d'achat en volume est de 60 minutes, l'intervalle entre les références peut être retardé, jusqu'à 119 minutes.

Intervalle max d'inactivité sur le portail en libre-service de XenMobile MDM (minutes) : ce nom de propriété reflète les anciennes versions de XenMobile. La propriété contrôle l'intervalle maximal d'inactivité de la console XenMobile. Cet intervalle est le nombre de minutes après lesquelles XenMobile ferme la session d'un utilisateur inactif sur la console XenMobile. Un délai d'expiration de 0 signifie qu'un utilisateur inactif reste connecté. La valeur par défaut est `30`.

Stratégies d'appareil et d'application

January 10, 2022

Les stratégies d'appareil et d'application XenMobile vous permettent d'optimiser l'équilibre entre les facteurs, tels que :

- Sécurité d'entreprise
- Protection de données et des ressources d'entreprise
- Confidentialité des utilisateurs
- Expériences utilisateur productives et positives

L'équilibre optimal entre ces facteurs peut varier. Par exemple, les organisations hautement réglementées, telles que celles du secteur financier, exigent des contrôles de sécurité plus stricts que d'autres industries, telles que l'éducation et la vente au détail, dans lesquelles la productivité des utilisateurs est une considération primordiale.

Vous pouvez contrôler et configurer de manière centralisée les stratégies en fonction de l'identité, de l'appareil, de l'emplacement et du type de connectivité des utilisateurs afin de limiter l'utilisation malveillante du contenu de l'entreprise. En cas de perte ou de vol d'un appareil, vous pouvez désactiver, verrouiller ou effacer à distance les applications et les données d'entreprise. Le résultat global est une solution qui augmente la satisfaction et la productivité des employés, tout en assurant la sécurité et le contrôle administratif.

L'objectif principal de cet article concerne les nombreuses stratégies relatives aux appareils et aux applications liées à la sécurité.

Stratégies répondant aux risques de sécurité

Les stratégies relatives aux appareils et aux applications XenMobile répondent à de nombreuses situations pouvant présenter un risque de sécurité, notamment :

- Lorsque les utilisateurs tentent d'accéder à des applications et des données à partir d'appareils non approuvés et d'emplacements imprévisibles.
- Lorsque les utilisateurs transmettent des données d'un appareil à l'autre.
- Lorsqu'un utilisateur non autorisé essaie d'accéder aux données.
- Lorsqu'un utilisateur qui a quitté l'entreprise a utilisé son propre appareil (BYOD).
- Lorsqu'un utilisateur a égaré un appareil.
- Lorsque les utilisateurs doivent accéder au réseau en toute sécurité à tout moment.
- Lorsque les utilisateurs ont leur propre appareil géré et que vous devez séparer les données professionnelles des données personnelles.
- Lorsqu'un appareil est inactif et nécessite une nouvelle vérification des informations d'identification de l'utilisateur.
- Lorsque les utilisateurs copient et collent du contenu sensible dans des systèmes de messagerie non protégés.
- Lorsque les utilisateurs reçoivent des pièces jointes à un e-mail ou des liens Web contenant des données sensibles sur un appareil qui contient des comptes personnels et d'entreprise.

Ces situations concernent deux principaux domaines de préoccupation lors de la protection des données de l'entreprise, à savoir lorsque les données sont :

- Au repos
- En transit

Protection des données au repos par XenMobile

Les données stockées sur les appareils mobiles sont appelées données au repos. XenMobile utilise le cryptage de l'appareil fourni par les plates-formes iOS et Android. XenMobile complète le cryptage basé sur la plate-forme avec des fonctionnalités telles que la vérification de la conformité, disponibles via le SDK Citrix MAM.

Les fonctionnalités de gestion des applications mobiles (MAM) de XenMobile permettent une gestion, une sécurité et un contrôle complets des applications de productivité mobiles, des applications compatibles MDX et des données associées.

Le SDK Applications mobiles permet aux applications d'être déployées pour XenMobile via l'utilisation de la technologie de conteneur d'applications Citrix MDX. La technologie de conteneur sépare les applications et les données d'entreprise des applications et des données personnelles sur un appareil utilisateur. Cette séparation des données vous permet de sécuriser toute application mobile personnalisée, développée par une tierce partie ou BYO avec des contrôles complets basés sur des stratégies.

XenMobile inclut également le cryptage au niveau de l'application. XenMobile crypte séparément les données stockées dans toute application compatible MDX sans nécessiter de code secret de l'appareil et sans que vous ayez besoin de gérer l'appareil pour appliquer la stratégie.

Les stratégies et le SDK des applications mobiles vous permettent de :

- Séparer les applications et données professionnelles et personnelles dans un conteneur mobile sécurisé.
- Sécuriser les applications avec le cryptage et les autres technologies de prévention de perte de données mobiles.

Les stratégies MDX fournissent de nombreux contrôles opérationnels. Vous pouvez activer l'intégration transparente entre les applications pour lesquelles le SDK MAM est activé ou encapsulées avec MDX, tout en contrôlant toutes les communications. De cette manière, vous pouvez appliquer des stratégies, par exemple pour vous assurer que les données ne sont accessibles que par les applications pour lesquelles le SDK MAM est activé ou encapsulées avec MDX.

Au-delà du contrôle de la stratégie d'appareil et d'application, la meilleure façon de protéger les données au repos est le cryptage. XenMobile ajoute une couche de cryptage aux données stockées dans une application compatible MDX, ce qui vous permet de contrôler, par l'intermédiaire de stratégies, les fonctionnalités telles que le cryptage de fichiers publics, le cryptage de fichiers privés et les exclusions de cryptage. Le SDK des applications mobiles utilise le cryptage AES 256 bits compatible FIPS 140-2 avec les clés stockées dans un coffre sécurisé Citrix Secret Vault.

Protection des données en transit par XenMobile

Les données déplacées entre les appareils mobiles de votre utilisateur et votre réseau interne sont appelées données en transit. La technologie de conteneur d'applications MDX fournit un accès VPN

spécifique aux applications à votre réseau interne via Citrix Gateway.

Considérez la situation dans laquelle un employé souhaite accéder aux ressources suivantes résidant sur le réseau d'entreprise sécurisé à partir d'un appareil mobile :

- Serveur de messagerie d'entreprise
- Application Web SSL hébergée sur l'intranet d'entreprise
- Documents stockés sur un serveur de fichiers ou Microsoft SharePoint

MDX permet l'accès à toutes ces ressources d'entreprise à partir d'appareils mobiles via un micro VPN spécifique à l'application. Chaque appareil possède son propre tunnel micro VPN dédié.

La fonctionnalité Micro VPN ne nécessite pas de VPN à l'échelle de l'appareil, ce qui peut compromettre la sécurité sur les appareils mobiles non approuvés. En conséquence, le réseau interne n'est pas exposé à des logiciels malveillants ou à des attaques susceptibles d'infecter l'ensemble du système de l'entreprise. Les applications mobiles d'entreprise et les applications mobiles personnelles peuvent coexister sur un même appareil.

Pour offrir des niveaux de sécurité encore plus élevés, vous pouvez configurer des applications compatibles MDX avec une stratégie Passerelle Citrix Gateway alternative, utilisée pour l'authentification et pour les sessions micro VPN avec une application. Vous pouvez utiliser une stratégie Passerelle Citrix Gateway alternative avec la stratégie Session en ligne requise pour forcer les applications à se réauthentifier sur la passerelle spécifique. Ces types de passerelles ont généralement des exigences d'authentification et des stratégies de gestion du trafic différentes (meilleur contrôle).

En plus des fonctionnalités de sécurité, le micro VPN offre également des techniques d'optimisation des données, y compris des algorithmes de compression. Les algorithmes de compression garantissent que :

- Seules des données minimales sont transférées.
- Le transfert se fait dans les plus brefs délais. La vitesse améliore l'expérience utilisateur, qui est un facteur clé de succès dans l'adoption d'appareils mobiles.

Réévaluez vos stratégies d'appareil périodiquement, par exemple dans les situations suivantes :

- Lorsqu'une nouvelle version de XenMobile inclut des stratégies nouvelles ou mises à jour en raison de la publication des mises à jour du système d'exploitation de l'appareil.
- Lorsque vous ajoutez un type d'appareil :

  Bien que la plupart des stratégies soient communes à tous les appareils, chaque appareil dispose de stratégies spécifiques à son système d'exploitation. Par conséquent, vous pouvez constater des différences entre appareils iOS, Android et Windows et même entre appareils Android de différents fournisseurs.

- Pour que l'opération XenMobile reste synchronisée avec les modifications de l'entreprise ou de l'industrie, telles que les nouvelles stratégies de sécurité de l'entreprise ou les réglementations de conformité.

- Lorsqu'une nouvelle version du SDK MAM inclut des stratégies nouvelles ou mises à jour
- Lorsque vous ajoutez ou mettez à jour une application.
- Pour intégrer de nouveaux workflows pour vos utilisateurs à la suite de nouvelles applications ou de nouvelles exigences.

Stratégies d'application et scénarios de cas d'utilisation

Bien que vous puissiez choisir les applications disponibles via Secure Hub, vous pouvez également définir la manière dont ces applications interagissent avec XenMobile. Utilisez les stratégies d'application :

- Si vous souhaitez que les utilisateurs s'authentifient après une certaine période.
- Si vous souhaitez fournir aux utilisateurs un accès hors connexion à leurs informations.

Les sections suivantes incluent certaines des stratégies et des exemples d'utilisation.

- Pour obtenir la liste des stratégies tierces que vous pouvez intégrer dans votre application iOS et Android à l'aide du SDK MAM, reportez-vous à la section Présentation du SDK MAM.
- Pour un tableau des stratégies applicatives MDX par plate-forme, consultez la section Synopsis des stratégies MDX.

Stratégies d'authentification

- **Code secret de l'appareil**

  Utilisation de cette stratégie : activez la stratégie Code secret de l'appareil pour qu'un utilisateur puisse accéder à une application MDX uniquement si le code secret de l'appareil est activé sur le terminal. Cette fonctionnalité garantit l'utilisation du cryptage iOS au niveau de l'appareil.

  Exemple pour l'utilisateur : l'activation de cette stratégie signifie que l'utilisateur doit définir un code secret sur son appareil iOS avant de pouvoir accéder à l'application MDX.

- **Code secret d'application**

  Utilisation de cette stratégie : activez la stratégie Code secret d'application pour que Secure Hub invite un utilisateur à s'authentifier auprès de l'application gérée avant de pouvoir ouvrir l'application et accéder aux données. L'utilisateur peut s'authentifier avec son mot de passe Active Directory, son code PIN Citrix ou son code TouchID iOS, selon la configuration choisie sous Propriétés du client dans Paramètres du serveur XenMobile. Vous pouvez définir un délai d'inactivité dans Propriétés du Client afin que, en cas d'utilisation continue, Secure Hub n'invite pas l'utilisateur à s'authentifier à nouveau auprès de l'application gérée jusqu'à l'expiration du délai.

  Le code secret de l'application diffère du code secret de l'appareil. Lorsqu'une stratégie de code secret est déployée sur un appareil, Secure Hub demande à l'utilisateur de configurer un code

secret ou un code PIN qu'il doit déverrouiller avant de pouvoir accéder à son appareil lorsqu'il l'allume ou lorsque le délai d'inactivité expire. Pour plus d'informations, consultez l'article Authentification dans XenMobile.

Exemple pour l'utilisateur : lors de l'ouverture de l'application Citrix Secure Web sur l'appareil, l'utilisateur doit entrer son code PIN Citrix avant de pouvoir parcourir les sites Web si la période d'inactivité a expiré.

- **Session en ligne requise**

  Utilisation de cette stratégie : si une application nécessite l'accès à une application Web (service Web) pour s'exécuter, activez cette stratégie afin que XenMobile invite l'utilisateur à se connecter au réseau de l'entreprise ou ait une session active avant d'utiliser l'application.

  Exemple pour l'utilisateur : lorsqu'un utilisateur tente d'ouvrir une application MDX sur laquelle la stratégie Session en ligne requise est activée, il ne peut pas utiliser l'application tant qu'elle n'est pas connectée au réseau à l'aide d'un service cellulaire ou Wi-Fi.

- **Période hors connexion maximale**

  Utilisation de cette stratégie : utilisez cette stratégie en tant qu'option de sécurité supplémentaire pour vous assurer que les utilisateurs ne peuvent pas exécuter une application en mode hors connexion pendant de longues périodes sans reconfirmer les droits d'accès aux applications et actualiser les stratégies XenMobile.

  Exemple pour l'utilisateur : si vous configurez une application MDX avec la stratégie Période hors connexion maximale, les utilisateurs peuvent ouvrir et utiliser l'application en mode hors connexion jusqu'à ce que la période hors connexion expire. À ce stade, l'utilisateur doit se reconnecter au réseau via un service cellulaire ou Wi-Fi et se réauthentifier, si le système le demande.

Stratégies d'accès diverses

- **Période de grâce de mise à jour des applications (heures)**

  Utilisation de cette stratégie : la stratégie Période de grâce de mise à jour des applications correspond au temps dont dispose l'utilisateur pour pouvoir mettre à jour une application dont la version plus récente est disponible sur XenMobile Store. Au moment de l'expiration, l'utilisateur doit mettre à jour l'application avant de pouvoir accéder aux données de l'application. Lors de la définition de cette valeur, gardez à l'esprit les besoins de votre personnel mobile, en particulier les personnes qui peuvent traverser de longues périodes hors connexion lors de déplacements à l'étranger.

  Exemple pour l'utilisateur : vous chargez une nouvelle version de Secure Mail dans XenMobile Store, puis définissez une période de grâce de mise à jour des applications de 6 heures. Tous les utilisateurs de Secure Mail verront un message leur demandant de mettre à jour leur application

Secure Mail avant l'expiration des 6 heures. À l'expiration des 6 heures, Secure Hub achemine les utilisateurs vers le XenMobile Store.

- **Période d'interrogation active (minutes)**

  Utilisation de cette stratégie : la stratégie Période d'interrogation active est l'intervalle durant lequel XenMobile vérifie les applications pour effectuer des actions de sécurité, telles que le verrouillage et l'effacement d'applications.

  Exemple pour l'utilisateur : si vous définissez la stratégie Période d'interrogation active sur 60 minutes, lorsque vous envoyez la commande Verrouillage des applications (Mode kiosque) depuis XenMobile sur l'appareil, le verrouillage se produit dans les 60 minutes suivant la dernière interrogation.

Stratégies de comportement des appareils non conformes

Lorsqu'un appareil se trouve en dessous des exigences minimales de conformité, la stratégie Appareils non conformes vous permet de sélectionner les mesures à prendre : Pour de plus amples informations, consultez la section Comportement des appareils non conformes.

Stratégies d'interaction des applications

Utilisation de ces stratégies : utilisez les stratégies d'interaction des applications pour contrôler le flux de documents et de données des applications MDX vers d'autres applications sur l'appareil. Par exemple, vous pouvez empêcher un utilisateur de déplacer des données vers ses applications personnelles en dehors du conteneur ou de coller des données provenant de l'extérieur du conteneur dans les applications conteneurisées.

Exemple pour l'utilisateur : vous définissez une stratégie d'interaction des applications sur Restreint, ce qui signifie qu'un utilisateur peut copier du texte de Secure Mail vers Secure Web, mais ne peut pas copier ces données vers son navigateur personnel Safari ou Chrome hors du conteneur. En outre, un utilisateur peut ouvrir une pièce jointe à partir de Secure Mail dans Citrix Files ou Quick Edit, mais ne peut pas ouvrir la pièce jointe dans son propre fichier personnel en affichant des applications en dehors du conteneur.

Stratégies de restrictions applicatives

Utilisation de ces stratégies : utilisez les stratégies de restriction applicatives pour contrôler les fonctionnalités auxquelles les utilisateurs peuvent accéder à partir d'une application MDX lorsqu'elle est ouverte. Cela permet de s'assurer qu'aucune activité malveillante ne peut avoir lieu pendant que l'application est en cours d'exécution. Les stratégies de restriction applicatives varient légèrement entre iOS et Android. Par exemple, dans iOS, vous pouvez bloquer l'accès à iCloud lors de l'exécution

de l'application MDX. Dans Android, vous pouvez arrêter l'utilisation de la technologie NFC pendant l'exécution de l'application MDX.

Exemple pour l'utilisateur : si vous activez la stratégie de restrictions applicatives pour bloquer la dictée sur iOS dans une application MDX, l'utilisateur ne peut pas utiliser la fonction de dictée sur le clavier iOS lorsque l'application MDX est en cours d'exécution. Ainsi, les données de dictée des utilisateurs ne sont pas transmises au service de dictée de cloud tiers non sécurisé. Lorsque l'utilisateur ouvre son application personnelle en dehors du conteneur, l'option de dictée reste disponible pour l'utilisateur pour ses communications personnelles.

Stratégies d'accès au réseau d'applications

Utilisation de ces stratégies : utilisez les stratégies d'accès au réseau d'entreprise pour fournir l'accès aux données stockées dans votre réseau d'entreprise à partir d'une application MDX dans le conteneur sur l'appareil. Pour la stratégie d'accès au réseau, définissez l'option **Tunnélisé vers le réseau interne** pour automatiser un micro VPN de l'application MDX via Citrix ADC vers un service Web principal ou un magasin de données.

Exemple pour l'utilisateur : lorsqu'un utilisateur ouvre une application MDX, telle que Secure Web, sur laquelle le tunneling est activé, le navigateur s'ouvre et lance un site intranet sans que l'utilisateur ait besoin de démarrer un VPN. L'application Secure Web accède automatiquement au site interne à l'aide de la technologie micro VPN.

Stratégies de géolocalisation et géofencing d'application

Utilisation de ces stratégies : les stratégies qui contrôlent la géolocalisation et le géofencing des applications incluent la longitude du point central, la latitude du point central et le rayon. Ces stratégies contiennent l'accès aux données dans les applications MDX vers une zone géographique spécifique. Les stratégies définissent une zone géographique par un rayon de coordonnées de latitude et de longitude. Si un utilisateur tente d'utiliser une application en dehors du rayon défini, l'application reste verrouillée et l'utilisateur ne peut pas accéder aux données de l'application.

Exemple pour l'utilisateur : un utilisateur peut accéder aux données de fusion et d'acquisition pendant qu'elles se trouvent dans leur emplacement de bureau. Lorsqu'elles sont déplacées à l'extérieur de leur emplacement de bureau, ces données sensibles deviennent inaccessibles.

Stratégies d'application Secure Mail

- **Services réseau d'arrière-plan**

  Utilisation de cette stratégie : les es services réseau en arrière-plan dans Secure Mail s'appuient sur Secure STA (Secure Ticket Authority) qui est effectivement un proxy SOCKS5

pour se connecter via Citrix Gateway. STA prend en charge les connexions à longue durée de vie et offre une meilleure autonomie de la batterie par rapport au micro VPN. Ainsi, STA est idéal pour le service de messagerie qui se connecte constamment. Citrix vous recommande de configurer ces paramètres pour Secure Mail. L'assistant Citrix ADC for XenMobile configure automatiquement STA pour Secure Mail.

Exemple pour l'utilisateur : lorsque STA n'est pas activé et qu'un utilisateur Android ouvre Secure Mail, il est invité à ouvrir un VPN qui reste ouvert sur l'appareil. Lorsque STA est activé et qu'un utilisateur Android ouvre Secure Mail, Secure Mail se connecte de manière transparente sans VPN requis.

- **Intervalle de synchronisation par défaut**

  Utilisation de cette stratégie : ce paramètre spécifie les jours de messagerie par défaut qui se synchronisent avec Secure Mail lorsque l'utilisateur accède à Secure Mail pour la première fois. Sachez que 2 semaines de messagerie prennent plus de temps à se synchroniser que 3 jours et prolongent le processus d'installation pour l'utilisateur.

  Exemple pour l'utilisateur : si l'intervalle de synchronisation par défaut est défini sur 3 jours lorsque l'utilisateur configure Secure Mail pour la première fois, il peut voir dans sa boîte de réception les e-mails qu'il a reçus jusqu'à 3 jours auparavant. Si un utilisateur souhaite voir les e-mails datant de plus de 3 jours, il peut effectuer une recherche. Secure Mail affiche ensuite les e-mails les plus anciens stockés sur le serveur. Après l'installation de Secure Mail, chaque utilisateur peut modifier ce paramètre pour mieux répondre à ses besoins.

Stratégies d'appareil et cas d'utilisation

Les stratégies d'appareil, parfois appelées stratégies MDM, déterminent le fonctionnement de XenMobile avec les appareils. Bien que la plupart des stratégies soient communes à tous les appareils, chaque appareil dispose de stratégies spécifiques à son système d'exploitation. La liste suivante inclut certaines des stratégies d'appareil et explique leur utilisation. Pour obtenir une liste de toutes les stratégies d'appareil, consultez les articles sous Stratégies d'appareil.

- **Stratégie d'inventaire des applications**

  Utilisation de cette stratégie : déployez la stratégie d'inventaire des applications sur un appareil si vous souhaitez voir les applications installées par un utilisateur. Si vous ne déployez pas la stratégie d'inventaire des applications, vous ne pouvez voir que les applications qu'un utilisateur a installées à partir de XenMobile Store et non les applications installées personnellement. Vous devez utiliser cette stratégie si vous souhaitez bloquer certaines applications et les empêcher de s'exécuter sur les appareils d'entreprise.

  Exemple pour l'utilisateur : un utilisateur disposant d'un appareil géré par MDM ne peut pas désactiver cette fonctionnalité. Les applications installées personnellement par l'utilisateur

sont visibles par les administrateurs XenMobile.

- **Stratégie de mode kiosque**

  Utilisation de cette stratégie : la stratégie Mode kiosque pour Android vous permet de bloquer ou d'autoriser des applications. Par exemple, en autorisant des applications, vous pouvez configurer un appareil kiosque. Généralement, vous déployez la stratégie Mode kiosque uniquement sur les appareils appartenant à l'entreprise car elle permet de limiter les applications que les utilisateurs peuvent installer. Vous pouvez définir un mot de passe de remplacement pour permettre aux utilisateurs d'accéder aux applications bloquées.

  Exemple pour l'utilisateur : supposons que vous déployiez une stratégie Mode kiosque qui bloque l'application Angry Birds. L'utilisateur peut installer l'application Angry Birds à partir de Google Play, mais quand il ouvre l'application, un message l'informe que son administrateur a bloqué l'application.

- **Stratégie de planification de connexion**

  Utilisation de cette stratégie : vous devez utiliser la stratégie de planification de connexion pour que les appareils Windows Mobile puissent se reconnecter à XenMobile Server pour la gestion MDM, la mise à disposition d'applications et le déploiement de stratégie. Pour les appareils Android, Android Enterprise et Chrome, utilisez la messagerie Google Firebase Cloud Messaging (FCM), au lieu de cette stratégie, pour contrôler les connexions à XenMobile Server. Les options de planification sont les suivantes :

  - **Toujours :** conserve la connexion active de façon permanente. Citrix recommande cette option pour optimiser la sécurité. Lorsque vous sélectionnez **Toujours**, utilisez également la stratégie de minuteur de connexion pour vous assurer que la connexion ne décharge pas la batterie. En conservant la connexion active, vous pouvez distribuer des commandes de sécurité telles que l'effacement ou le verrouillage de l'appareil à la demande. Vous devez également sélectionner l'option de calendrier de déploiement **Déployer pour les connexions permanentes** dans chaque stratégie déployée sur l'appareil.
  - **Jamais :** permet une connexion manuelle. Citrix ne recommande pas l'option **Jamais** pour les déploiements de production, car elle empêche le déploiement des stratégies de sécurité sur les appareils, ce qui signifie que les utilisateurs ne recevront jamais les nouvelles applications ou stratégies.
  - **Toutes les :** se connecte à l'intervalle défini. Lorsque cette option est activée et que vous envoyez une stratégie de sécurité telle qu'un effacement ou verrouillage, XenMobile traite la stratégie sur l'appareil la prochaine fois que l'appareil se connecte.
  - **Définir un calendrier :** lorsque cette option est activée, XenMobile tente de reconnecter l'appareil de l'utilisateur au serveur XenMobile après une perte de connexion réseau et surveille la connexion en transmettant des paquets de contrôle à intervalles réguliers dans le délai imparti.

Exemple pour l'utilisateur : vous souhaitez déployer une stratégie de code secret pour les appareils inscrits. La stratégie de planification garantit que les appareils se connectent de nouveau au serveur à intervalles réguliers pour collecter la nouvelle stratégie.

- **Stratégie d'informations d'identification**

  Utilisation de cette stratégie : souvent utilisée en conjonction avec une stratégie Wi-Fi, cette stratégie permet aux entreprises de déployer des certificats pour l'authentification auprès de ressources internes qui nécessitent une authentification par certificat.

  Exemple pour l'utilisateur : vous déployez une stratégie Wi-Fi qui configure un réseau sans fil sur l'appareil. Le réseau Wi-Fi nécessite un certificat d'authentification. La stratégie d'informations d'identification déploie un certificat qui est ensuite stocké dans le keystore du système d'exploitation. L'utilisateur peut alors sélectionner le certificat lorsqu'il est connecté à la ressource interne.

- **Stratégie Exchange**

  Utilisation de cette stratégie : avec XenMobile, vous disposez de deux options pour envoyer des e-mails Microsoft Exchange ActiveSync.

  - **Application Secure Mail :** envoyez des e-mails à l'aide de l'application Secure Mail que vous distribuez à partir du magasin d'applications public ou de XenMobile Store.
  - **Application de messagerie native :** vous pouvez utiliser la stratégie Exchange pour activer la messagerie ActiveSync pour le client de messagerie natif sur l'appareil. La stratégie Exchange pour la messagerie native vous permet d'utiliser des macros pour remplir les données utilisateur à partir de leurs attributs Active Directory, tels que ${user.username} pour renseigner le nom d'utilisateur et ${user.domain} pour renseigner le domaine utilisateur.

  Exemple pour l'utilisateur : lors de la mise à disposition de la stratégie Exchange, vous envoyez les détails du serveur Exchange à l'appareil. Secure Hub invite l'utilisateur à s'authentifier et la messagerie commence à être synchronisée.

- **Stratégie d'emplacement**

  Utilisation de cette stratégie : cette stratégie vous permet de géo-localiser les appareils sur une carte, en supposant que le GPS est activé pour Secure Hub sur l'appareil. Après avoir déployé cette stratégie, puis envoyé une commande locate depuis le serveur XenMobile, l'appareil répond avec les coordonnées d'emplacement.

  Exemple pour l'utilisateur : lorsque vous déployez la stratégie de localisation et que le GPS est activé sur l'appareil, si les utilisateurs déplacent leur appareil, ils peuvent se connecter au portail en libre-service XenMobile et choisir l'option de localisation pour afficher l'emplacement de leur appareil sur une carte. Notez que l'utilisateur choisit d'autoriser Secure Hub à utiliser

les services de localisation. Vous ne pouvez pas imposer l'utilisation des services de localisation lorsque les utilisateurs inscrivent eux-mêmes un appareil. Une autre considération pour l'utilisation de cette stratégie est l'effet sur la vie de la batterie.

- **Stratégie de code secret**

  Utilisation de cette stratégie : une stratégie de code secret vous permet de définir un code PIN ou un mot de passe sur un appareil géré. Cette stratégie de code secret vous permet de définir la complexité et les délais d'expiration du code secret sur l'appareil.

  Exemple pour l'utilisateur : lorsque vous déployez une stratégie de code secret sur un appareil géré, Secure Hub invite l'utilisateur à configurer un code secret ou un code PIN qu'il doit déverrouiller avant de pouvoir accéder à son appareil lorsqu'il l'allume ou lorsque le délai d'inactivité expire.

- **Stratégie de suppression de profil**

  Utilisation de cette stratégie : supposons que vous déployiez une stratégie sur un groupe d'utilisateurs et que vous deviez ensuite supprimer cette stratégie d'un sous-ensemble d'utilisateurs. Vous pouvez supprimer la stratégie pour les utilisateurs sélectionnés en créant une stratégie de suppression de profil et en utilisant des règles de déploiement pour déployer la stratégie de suppression de profil uniquement sur des noms d'utilisateur spécifiés.

  Exemple pour l'utilisateur : lorsque vous déployez une stratégie de suppression de profil sur des appareils utilisateur, les utilisateurs peuvent ne pas remarquer la modification. Par exemple, si la stratégie de suppression de profil supprime une restriction qui a désactivé la caméra de l'appareil, l'utilisateur ne saura pas que l'utilisation de la caméra est maintenant autorisée. Pensez à informer les utilisateurs lorsque des modifications affectent leur expérience utilisateur.

- **Stratégie de restrictions**

  Utilisation de cette stratégie : la stratégie de restriction vous offre plusieurs façons de verrouiller et de contrôler les fonctionnalités sur l'appareil géré. Vous pouvez activer des centaines d'options de restriction sur des appareils pris en charge, en passant par la désactivation de l'appareil photo ou du micro d'un appareil jusqu'à l'application de règles d'itinérance et d'accès aux services de tiers tels que des magasins d'applications.

  Exemple pour l'utilisateur : si vous déployez une restriction sur un appareil iOS, il se peut que l'utilisateur ne puisse pas accéder à iCloud ou à l'App Store d'Apple.

- **Stratégie termes et conditions**

  Utilisation de cette stratégie : vous devrez peut-être informer les utilisateurs des implications juridiques de la gestion de leur appareil. En outre, vous pouvez vous assurer que les utilisateurs sont conscients des risques de sécurité lorsque les données d'entreprise sont transmises

à l'appareil. Le document Termes et conditions personnalisé vous permet de publier des règles et des avis avant l'inscription de l'utilisateur.

Exemple pour l'utilisateur : un utilisateur voit les informations de termes et conditions durant le processus d'inscription. S'il refuse d'accepter les conditions énoncées, le processus d'inscription prend fin et il ne peut pas accéder aux données de l'entreprise. Vous pouvez générer un rapport à fournir aux équipes RH/Juridique/Conformité pour indiquer qui a accepté ou refusé les conditions.

- **Stratégie VPN**

  Utilisation de cette stratégie : utilisez la stratégie VPN pour fournir un accès aux systèmes principaux en utilisant la technologie VPN Gateway plus ancienne. La stratégie prend en charge un certain nombre de fournisseurs VPN, y compris Cisco AnyConnect, Juniper ainsi que Citrix VPN. Il est également possible d'associer cette stratégie à une autorité de certification et d'activer le VPN à la demande si la passerelle VPN prend en charge cette option.

  Exemple pour l'utilisateur : lorsque la stratégie VPN est activée, l'appareil d'un utilisateur ouvre une connexion VPN lorsque l'utilisateur accède à un domaine interne.

- **Stratégie de clip Web**

  Utilisation de cette stratégie : utilisez la stratégie de clip Web si vous souhaitez envoyer aux appareils une icône qui s'ouvre directement sur un site Web. Un clip Web contient un lien vers un site Web et peut inclure une icône personnalisée. Sur un appareil un clip Web ressemble à une icône d'application.

  Exemple pour l'utilisateur : un utilisateur peut cliquer sur une icône de clip Web pour ouvrir un site Internet qui fournit les services auxquels il doit accéder. L'utilisation d'un lien Web est plus pratique que d'ouvrir une application de navigation et de taper une adresse de lien.

- **Stratégie Wi-Fi**

  Utilisation de cette stratégie : la stratégie Wi-Fi vous permet de déployer les détails du réseau Wi-Fi, tels que le SSID, les données d'authentification et les données de configuration, sur un appareil géré.

  Exemple pour l'utilisateur : lorsque vous déployez la stratégie Wi-Fi, l'appareil se connecte automatiquement au réseau Wi-Fi et authentifie l'utilisateur afin qu'il puisse accéder au réseau.

- **Stratégie de protection des informations Windows**

  Utilisation de cette stratégie : utilisez la stratégie WIP (Windows Information Protection) pour vous protéger contre la fuite potentielle de données d'entreprise. Vous pouvez spécifier les applications nécessitant une protection des informations Windows au niveau d'exécution que vous avez défini. Par exemple, vous pouvez bloquer tout partage de données inapproprié ou mettre en garde sur le partage de données approprié et permettre aux utilisateurs de remplacer

la stratégie. Vous pouvez exécuter WIP de manière silencieuse lors de l'ouverture de session et du partage de données inapproprié.

Exemple pour l'utilisateur : supposons que vous configuriez la stratégie WIP pour bloquer le partage de données inapproprié. Si un utilisateur copie ou enregistre un fichier protégé dans un emplacement non protégé, un message semblable au suivant s'affiche : « Vous ne pouvez pas placer de contenu protégé dans cet emplacement ».

- **Stratégie XenMobile Store**

  Utilisation de cette stratégie : XenMobile Store est un magasin d'applications unifié où les administrateurs peuvent publier toutes les applications d'entreprise et les ressources de données dont leurs utilisateurs ont besoin. Un administrateur peut ajouter les applications suivantes :

  - Applications Web, applications SaaS et applications sur lesquelles le SDK MAM est activé ou applications encapsulées avec MDX
  - Applications de productivité mobiles Citrix
  - Applications mobiles natives telles que les fichiers .ipa ou .apk
  - Applications Apple App Store et Google Play
  - Liens Web
  - Citrix Virtual Apps publiées à l'aide de Citrix StoreFront

  Exemple pour l'utilisateur : lorsqu'un utilisateur inscrit son appareil dans XenMobile, il accède à XenMobile via l'application Citrix Secure Hub. L'utilisateur peut alors voir toutes les applications et services d'entreprise mis à sa disposition. Les utilisateurs peuvent cliquer sur une application pour l'installer, accéder aux données, évaluer et vérifier l'application, et télécharger les mises à jour d'applications à partir de XenMobile Store.

Options d'inscription des utilisateurs

September 22, 2021

Vous pouvez demander aux utilisateurs d'inscrire leurs appareils dans XenMobile de plusieurs manières. Avant d'examiner les détails, décidez quels appareils vous souhaitez inscrire à MDM+MAM, MDM ou MAM. Pour plus d'informations sur ces modes de gestion, consultez la section Modes de gestion.

Au plus haut niveau, il y a quatre options d'inscription :

- **Invitation d'inscription :** envoyez une invitation d'inscription ou une URL d'invitation aux utilisateurs. Les invitations et les URL d'inscription ne sont pas disponibles pour les appareils Windows.

- **Portail en libre-service :** configurez un portail que les utilisateurs peuvent visiter pour télécharger Secure Hub et enregistrer leurs appareils ou leur envoyer une invitation d'inscription.
- **Inscription manuelle :** envoyez un e-mail, un manuel ou toute autre communication permettant aux utilisateurs de savoir que le système est disponible pour l'inscription. Les utilisateurs téléchargent ensuite Secure Hub et inscrivent leurs appareils manuellement.
- **Enterprise :** l'inscription des appareils peut également s'effectuer via un programme de déploiement d'Apple et Google Android Enterprise. Grâce à chacun de ces programmes, vous pouvez acheter des appareils préconfigurés, prêts à être utilisés par les employés. Pour plus d'informations, consultez les articles sur le programme de déploiement d'Apple de l'assistance Apple et la documentation sur Google Android Enterprise sur le site Web Android Enterprise.

Invitation d'inscription

Vous pouvez envoyer une invitation d'inscription aux utilisateurs d'appareils iOS, macOS, Android Enterprise et d'appareils Android d'ancienne génération. Les invitations et les URL d'inscription ne sont pas disponibles pour les appareils Windows.

Vous pouvez également envoyer un lien d'installation via SMTP ou SMS aux utilisateurs d'appareils iOS, macOS, Android ou Windows. Pour de plus amples informations, consultez la section Inscription d'appareils.

Si vous choisissez d'utiliser la méthode d'invitation d'inscription, vous pouvez :

- Choisissez les modes d'inscription sécurisée **URL d'invitation**, **URL d'invitation + PIN** ou **URL d'invitation + mot de passe**.
- Utilisez n'importe quelle combinaison de modes.
- Activez ou désactivez les modes à partir de la page **Paramètres**.

Pour de plus amples informations sur chaque mode d'inscription sécurisée, consultez la section Configurer les modes d'inscription sécurisée.

Les invitations servent à plusieurs fins. L'utilisation la plus courante des invitations consiste à informer les utilisateurs que le système est disponible et qu'ils peuvent s'inscrire. Les URL d'invitation sont uniques. Une fois qu'un utilisateur a utilisé une URL d'invitation, cette URL n'est plus disponible. Vous pouvez utiliser cette propriété pour limiter les utilisateurs ou les appareils qui s'enregistrent sur votre système.

Lors de la configuration d'un profil d'inscription, vous pouvez contrôler le nombre d'appareils que des utilisateurs spécifiques peuvent inscrire, en fonction des groupes Active Directory. Par exemple, vous pouvez autoriser un seul appareil par utilisateur pour votre service financier.

Soyez conscient des coûts supplémentaires et des problèmes de certaines options d'inscription. Par exemple, l'envoi d'invitations par SMS nécessite une infrastructure supplémentaire. Pour de plus am-

ples informations, consultez la section Notifications.

En outre, pour envoyer des invitations par e-mail, assurez-vous que les utilisateurs disposent d'un moyen d'accéder à leurs e-mails en dehors de Secure Hub. Vous pouvez utiliser des modes d'inscription sécurisée à mot de passe à usage unique (OTP) comme alternative aux mots de passe Active Directory pour l'inscription MDM.

Portail en libre-service

Les utilisateurs peuvent demander une invitation d'inscription via le portail en libre-service. Pour plus d'informations sur la configuration du portail en libre-service, consultez la section Configurer les modes d'inscription sécurisée.

Inscription manuelle

Lors de l'inscription manuelle, les utilisateurs se connectent à XenMobile via la détection automatique ou en entrant les informations du serveur. Si la détection automatique est activée, les utilisateurs se connectent avec uniquement leur adresse e-mail ou leurs informations d'identification Active Directory au format Nom d'utilisateur principal. Si la détection automatique n'est pas activée, ils doivent entrer l'adresse du serveur et leurs informations d'identification Active Directory. Pour plus d'informations sur la configuration de la détection automatique, consultez la section XenMobile Autodiscovery Service.

Vous pouvez faciliter l'inscription manuelle de plusieurs façons. Vous pouvez créer un guide, le distribuer aux utilisateurs et leur demander de s'inscrire eux-mêmes. Vous pouvez demander à votre département informatique d'inscrire manuellement des groupes d'utilisateurs dans certains créneaux horaires. Vous pouvez utiliser n'importe quelle méthode similaire où les utilisateurs doivent entrer leurs informations d'identification, les informations sur le serveur ou les deux.

Intégration de l'utilisateur

Une fois l'environnement configuré, vous devez décider comment intégrer les utilisateurs dans votre environnement. Une section précédente de cet article traite des spécificités des modes d'inscription sécurisée des utilisateurs. Cette section traite de la manière dont vous communiquez avec les utilisateurs.

Inscription ouverte ou invitation sélective

Lors de l'intégration d'utilisateurs, vous pouvez autoriser l'inscription par deux méthodes de base :

- Inscription ouverte. Par défaut, tout utilisateur disposant d'informations d'identification LDAP et d'informations d'environnement XenMobile peut s'inscrire.

- Inscription limitée. Vous pouvez limiter le nombre d'utilisateurs en autorisant uniquement les utilisateurs ayant des invitations d'inscription. Vous pouvez également limiter l'inscription ouverte par groupe Active Directory.

Avec la méthode d'invitation, vous pouvez également limiter le nombre d'appareils qu'un utilisateur peut inscrire. Dans la plupart des situations, l'inscription ouverte est acceptable, mais il y a quelques points à considérer :

- Pour l'inscription MAM, vous pouvez facilement limiter l'inscription ouverte via l'appartenance à un groupe Active Directory.
- Pour l'inscription MDM, vous pouvez limiter le nombre d'appareils pouvant s'inscrire en fonction de l'appartenance à un groupe Active Directory. Si vous autorisez uniquement les appareils d'entreprise dans votre environnement, cette limitation ne pose normalement pas de problème. Toutefois, vous pouvez envisager cette méthode dans un environnement de travail BYOD dans lequel vous souhaitez limiter le nombre d'appareils.

L'invitation sélective est généralement effectuée moins souvent car elle nécessite un peu plus de travail que l'inscription ouverte. Pour que les utilisateurs puissent inscrire leurs appareils dans votre environnement, vous devez envoyer une invitation unique à chaque utilisateur. Pour plus d'informations sur l'envoi d'une invitation d'inscription, reportez-vous à la section Envoi d'une invitation d'inscription.

Bien que vous puissiez utiliser des groupes Active Directory pour créer des invitations par lots, vous devez effectuer cette approche par vagues.

Premier contact avec les utilisateurs

Après avoir décidé entre l'inscription ouverte ou l'invitation sélective, puis configuré ces environnements, vous devez informer les utilisateurs de leurs options d'inscription.

Si vous utilisez la méthode d'invitation sélective, les e-mails et SMS font partie du processus. Vous pouvez également envoyer des e-mails via la console XenMobile pour une inscription ouverte. Pour de plus amples informations, consultez la section Envoyer une invitation d'inscription.

Dans les deux cas, notez que vous avez besoin d'un serveur SMTP pour les e-mails. Vous avez besoin d'un serveur SMS pour les messages texte. Cela peut occasionner des coûts supplémentaires à prendre en compte lors de votre prise de décision. Avant de sélectionner une méthode, tenez compte de la manière dont vous souhaitez que les nouveaux utilisateurs accèdent aux informations, comme les e-mails. Si vous souhaitez que tous les utilisateurs accèdent à leurs e-mails via XenMobile, leur envoyer un e-mail d'invitation serait problématique.

Vous pouvez également envoyer des communications par un autre moyen en dehors de XenMobile pour un environnement d'inscription ouvert. Pour cette option, assurez-vous d'inclure toutes les informations pertinentes. Indiquez aux utilisateurs où ils peuvent obtenir l'application Secure Hub et

quelle méthode utiliser pour s'inscrire. Si la détection est désactivée, indiquez également aux utilisateurs l'adresse de XenMobile Server. Pour plus d'informations sur la détection automatique, consultez la section XenMobile AutoDiscovery Service.

Optimisation des opérations XenMobile

May 21, 2021

Les performances et la stabilité des opérations XenMobile impliquent de nombreux paramètres sur XenMobile et dépendent de votre configuration de base de données Citrix ADC et SQL Server. Cet article se concentre sur les paramètres liés à l'optimisation de XenMobile les plus souvent configurés par les administrateurs. Citrix vous recommande d'évaluer chacun des paramètres de cet article avant de déployer XenMobile.

> **Important :**
>
> Ces instructions supposent que l'UC et la RAM de XenMobile Server sont adaptés au nombre d'appareils. Pour plus d'informations sur la montée en charge, consultez la section Capacité à monter en charge et performances.

Les propriétés de serveur suivantes s'appliquent globalement aux opérations, utilisateurs et appareils sur une instance XenMobile entière. La modification de certaines propriétés de serveur nécessite un redémarrage de chaque nœud de serveur XenMobile. XenMobile vous informe lorsqu'un redémarrage est requis.

Ces instructions d'optimisation s'appliquent à la fois aux environnements en cluster et sans cluster.

hibernate.c3p0.idle_test_period

Cette propriété XenMobile Server, une clé personnalisée, détermine le temps d'inactivité en secondes avant qu'une connexion soit automatiquement validée. Configurez la clé comme suit. La valeur par défaut est **30**.

- Clé : **Clé personnalisée**
- Clé : **hibernate.c3p0. idle_test_period**
- Valeur : **120**
- Nom d'affichage : **hibernate.c3p0. idle_test_period**
- Description : **Période d'inactivité prolongée de test**

hibernate.c3p0.max_size

Cette clé personnalisée détermine le nombre maximal de connexions que XenMobile peut ouvrir pour la base de données SQL Server. XenMobile utilise la valeur que vous spécifiez pour cette clé personnalisée en tant qu'une limite supérieure. Les connexions s'ouvrent uniquement si vous en avez besoin. Basez vos paramètres sur la capacité de votre serveur de base de données.

Notez l'équation suivante dans une configuration en cluster. Votre connexion c3p0 multipliée par le nombre de nœuds est égale au nombre maximum de connexions que XenMobile peut ouvrir à la base de données SQL Server.

Dans une configuration en cluster et sans cluster, la définition d'une valeur trop élevée avec un serveur SQL Server sous-dimensionné peut entraîner des problèmes de ressources côté SQL pendant la charge de pointe. Si vous définissez une valeur trop faible, vous ne pourrez peut-être pas tirer parti des ressources SQL disponibles.

Configurez la clé comme suit. La valeur par défaut est **1000**.

- Clé : **hibernate.c3p0.max_size**
- Valeur : **1000**
- Nom d'affichage : **hibernate.c3p0.max_size**
- Description : Connexions de base de données à SQL

hibernate.c3p0.min_size

Cette clé personnalisée détermine le nombre minimal de connexions que XenMobile ouvre pour la base de données SQL Server. Configurez la clé comme suit. La valeur par défaut est **100**.

- Clé : **hibernate.c3p0.min_size**
- Valeur : **100**
- Nom d'affichage : **hibernate.c3p0.min_size**
- Description : Connexions de base de données à SQL

hibernate.c3p0.timeout

Cette clé personnalisée détermine le délai d'inactivité. Si vous utilisez le basculement de cluster de base de données, Citrix vous recommande d'ajouter cette clé personnalisée et de la définir pour réduire le délai d'inactivité. La valeur par défaut est **120**.

- Clé : **Clé personnalisée**
- Clé : **hibernate.c3p0.timeout**
- Valeur : **120**
- Nom d'affichage : **hibernate.c3p0.timeout**
- Description: Délai d'inactivité de la base de données

Intervalle de pulsation des services Push

Ce paramètre détermine la fréquence à laquelle un appareil iOS vérifie si une notification APNs n'est pas fournie entre temps. L'augmentation de la fréquence de pulsation APNs peut optimiser les communications de la base de données. Une valeur trop grande peut ajouter une charge inutile. Ce paramètre s'applique uniquement aux appareils iOS. La valeur par défaut est de **20** heures.

Si vous avez un grand nombre d'appareils iOS dans votre environnement, l'intervalle de pulsation peut entraîner une charge plus importante que nécessaire. Les actions de sécurité, telles que l'effacement sélectif, le verrouillage ou l'effacement complet, ne reposent pas sur cette pulsation, une notification APNs étant envoyée à l'appareil lorsque les actions sont exécutées. Cette valeur détermine la rapidité de mise à jour d'une stratégie après la modification de l'appartenance au groupe Active Directory. Par conséquent, il est souvent approprié d'augmenter cette valeur entre 12 et 20 heures pour réduire la charge.

Taille du pool de connexions APNS iOS MDM

Un pool de connexions APNs trop petit peut affecter négativement les performances de l'activité APNs lorsque vous avez plus de 100 appareils. Les problèmes de performances incluent un déploiement plus lent des applications et des stratégies sur les appareils et un ralentissement de l'enregistrement des appareils. La valeur par défaut est **1**. Nous vous recommandons d'augmenter cette valeur de 1 pour tous les 400 appareils.

auth.ldap.connect.timeout

Pour compenser les réponses LDAP lentes, Citrix recommande d'ajouter des propriétés de serveur pour la clé personnalisée suivante.

- Clé : **Clé personnalisée**
- Clé : **auth.ldap.connect.timeout**
- Valeur : **60000**
- Nom d'affichage : **auth.ldap.connect.timeout**
- Description : **Délai d'expiration de la connexion LDAP**

auth.ldap.read.timeout

Pour compenser les réponses LDAP lentes, Citrix recommande d'ajouter des propriétés de serveur pour la clé personnalisée suivante.

- Clé : **Clé personnalisée**
- Clé : **auth.ldap.read.timeout**
- Valeur : **60000**

- Nom d'affichage : **auth.ldap.read.timeout**
- Description : **Délai d'expiration de la lecture LDAP**

Autres optimisations de serveur

Propriété du serveur	Paramètre par défaut	Pourquoi modifier ce paramètre ?
Déploiement en arrière-plan	1440 minutes	Fréquence des déploiements de stratégie en arrière-plan, en minutes. S'applique uniquement aux connexions permanentes pour les appareils Android. L'augmentation de la fréquence des déploiements de stratégies réduit la charge du serveur. Le paramètre recommandé est **1440** (24 heures).
Inventaire matériel en arrière-plan	1440 minutes	Fréquence de l'inventaire matériel en arrière-plan, en minutes. S'applique uniquement aux connexions permanentes pour les appareils Android. L'augmentation de la fréquence d'inventaire matériel réduit la charge du serveur. Le paramètre recommandé est **1440** (24 heures).

Intervalle pour vérifier l'utilisateur Active Directory supprimé.	15 minutes	L'heure de synchronisation standard pour Active Directory est **15** minutes. La valeur **0** empêche XenMobile de rechercher les utilisateurs Active Directory supprimés. Le paramètre recommandé est **15** minutes.
MaxNumberOfWorker	3	Nombre de threads utilisé lors de l'importation d'un grand nombre de licences d'achat en volume. La valeur par défaut est **3**. Si vous avez besoin d'une plus grande optimisation, vous pouvez augmenter le nombre de threads. Toutefois, notez qu'avec un nombre important de threads (6, par exemple), une importation d'achat en volume entraîne une forte utilisation de l'UC.

Vérification des blocages dans une base de données SQL et suppression des données historiques

Lorsque vous rencontrez des blocages, exécutez la requête suivante pour les afficher. Un administrateur de base de données ou l'équipe Microsoft SQL pourra ensuite confirmer les informations.

Requête SQL

```
SELECT

db.name DB_Service,

tl.request_session_id,

wt.blocking_session_id,
```



```
8
9  OBJECT_NAME(p.OBJECT_ID) BlockedObjectName,
10
11 tl.resource_type,
12
13 h1.TEXT AS RequestingText,
14
15 h2.TEXT AS BlockingTest,
16
17 tl.request_mode
18
19 FROM sys.dm_tran_locks AS tl
20
21 INNER JOIN sys.databases db ON db.database_id = tl.resource_database_id
22
23 INNER JOIN sys.dm_os_waiting_tasks AS wt ON tl.lock_owner_address = wt.
      resource_address
24
25 INNER JOIN sys.partitions AS p ON p.hobt_id = tl.
      resource_associated_entity_id
26
27 INNER JOIN sys.dm_exec_connections ec1 ON ec1.session_id = tl.
      request_session_id
28
29 INNER JOIN sys.dm_exec_connections ec2 ON ec2.session_id = wt.
      blocking_session_id
30
31 CROSS APPLY sys.dm_exec_sql_text(ec1.most_recent_sql_handle) AS h1
32
33 CROSS APPLY sys.dm_exec_sql_text(ec2.most_recent_sql_handle) AS h2
34
35 GO
36 <!--NeedCopy-->
```

Nettoyer la base de données

> **Important :**
>
> Sauvegardez votre base de données avant d'apporter des modifications aux tables.

1. Exécutez la requête suivante pour vérifier les données historiques.

```
1 select COUNT(\*) as total_record from dbo.EWDEPLOY_HISTO;
2 select COUNT(\*) as total_record from dbo.EWSESS;
3 select COUNT(*) as total_record from dbo.EWAUDIT;
```



```
<!--NeedCopy-->
```

2. Supprimez les données des trois tables précédentes.

> **Remarque :**
>
> Vous pouvez ne pas voir les données historiques dans une table. Si c'est le cas, passez l'exécution de la requête de troncature pour la table en question.

```
truncate TABLE dbo.EWDEPLOY_HISTO;
truncate TABLE dbo.EWSESS;
truncate TABLE dbo.EWAUDIT;
<!--NeedCopy-->
```

3. Débloquez les requêtes SELECT qui ont été bloquées en raison des blocages. Cette étape prend en charge les autres blocages.

```
ALTER DATABASE <database_name> SET       READ_COMMITTED_SNAPSHOT
    ON WITH ROLLBACK IMMEDIATE
<!--NeedCopy-->
```

4. Par défaut, le nettoyage de la base de données est de sept jours pour la conservation de la rétention de la session et les données de rétention d'audit, ce qui est élevé pour un grand nombre d'utilisateurs. Modifiez la valeur de nettoyage à 1 ou 2 jours. Dans les propriétés du serveur, effectuez les modifications suivantes :

```
zdm.dbcleanup.sessionRetentionTimeInDays = 1 day
zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day
zdm.dbcleanup.auditRetentionTimeInDays=1 day
<!--NeedCopy-->
```

Nettoyer les orphelins dans la table KEYSTORE

Si les performances des nœuds XenMobile ne sont pas satisfaisantes, vérifiez que la table KEYSTORE ne soit pas trop grande. XenMobile stocke les certificats d'inscription dans les tables ENROLLMENT_CERTIFICATE et KEYSTORE. Lorsque vous supprimez ou réinscrivez des appareils, les certificats de la table ENROLLMENT_CERTIFICATE sont supprimés. Les entrées de la table KEYSTORE sont conservées, ce qui peut entraîner des problèmes de performances. Effectuez la procédure suivante pour nettoyer les orphelins de la table KEYSTORE.

> **Important :**
>
> Sauvegardez votre base de données avant d'apporter des modifications aux tables.

1. Exécutez la requête suivante pour vérifier les données historiques.


```
select COUNT(*) from KEYSTORE
<!--NeedCopy-->
```

2. Recherchez les orphelins dans la table KEYSTORE avec la requête suivante.

```
WITH cte(KEYSTORE_ID)
AS (SELECT KEYSTORE_ID
    FROM ENROLLMENT_CERTIFICATE
    UNION
    SELECT CA_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT CLIENT_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT KEYSTORE_ID
    FROM SAML_SERVICE_PROVIDER
    UNION
    SELECT KEYSTORE_ID
    FROM SERVER_CERTIFICATE)
SELECT keystore.id
FROM keystore
    LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
WHERE KEYSTORE_ID IS NULL;
<!--NeedCopy-->
```

3. Effacez les orphelins à l'aide de la requête suivante.

```
WITH cte(KEYSTORE_ID)
    AS (SELECT KEYSTORE_ID
        FROM ENROLLMENT_CERTIFICATE
        UNION
        SELECT CA_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT CLIENT_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT KEYSTORE_ID
        FROM SAML_SERVICE_PROVIDER
        UNION
        SELECT KEYSTORE_ID
        FROM SERVER_CERTIFICATE)
    DELETE FROM keystore
```



```
    WHERE id IN
    (
        SELECT keystore.id
        FROM keystore
            LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
        WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'
    );
<!--NeedCopy-->
```

4. Ajoutez un index à la table KEYSTORE pour améliorer l'efficacité de la recherche.

```
DROP INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE";
ALTER TABLE "KEYSTORE" ALTER COLUMN "NAME" NVARCHAR(255) NULL;
CREATE INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE"("NAME") INCLUDE ("
    ID", "TYPE", "CONTENT", "PASSWORD", "PUBLICLY_TRUSTED", "
    DESCRIPTION", "ALIAS", "MODIFICATION_DATE");
<!--NeedCopy-->
```

Provisioning et deprovisioning d'applications

January 10, 2022

Le provisioning des applications s'articule autour de la gestion du cycle de vie des applications mobiles : préparer, configurer, distribuer et gérer des applications mobiles dans un environnement XenMobile. Dans certains cas, le développement ou la modification du code d'application peut également faire partie du processus de provisioning. XenMobile est équipé de divers outils et processus que vous pouvez utiliser pour le provisioning d'applications.

Avant de lire cet article sur le provisioning des applications, nous vous recommandons de lire les articles suivants :

- Applications - Communautés d'utilisateurs

Lorsque vous avez finalisé le type d'applications que votre organisation prévoit d'offrir aux utilisateurs, vous pouvez définir le processus de gestion des applications tout au long de leur cycle de vie.

Tenez compte des points suivants lors de la définition du processus de provisioning de votre application :

- **Profilage des applications :** votre organisation peut commencer par un nombre limité d'applications. Toutefois, le nombre d'applications que vous gérez peut augmenter rapidement à mesure que les taux d'adoption par les utilisateurs augmentent et que votre environnement se développe. Définissez des profils d'application spécifiques dès le début

afin de simplifier le provisioning des applications. Le profilage des applications vous permet de catégoriser les applications en groupes logiques d'un point de vue non technique. Par exemple, vous pouvez créer des profils d'application en fonction des facteurs suivants :

- Version : version de l'application pour le suivi
- Instances : plusieurs instances déployées pour un ensemble différent d'utilisateurs, par exemple avec différents niveaux d'accès
- Plate-forme : iOS, Android ou Windows
- Public cible : utilisateurs standard, départements, cadres de niveau C
- Propriété : département propriétaire de l'application
- Type : MDX, Public, Web et SaaS, ou liens Web
- Cycle de mise à niveau : fréquence à laquelle l'application est mise à niveau
- Licences : exigences en matière de licence et propriété
- Stratégies SDK MAM ou MDX : pour appliquer des fonctionnalités MDX à vos applications mobiles
- Accès réseau : type d'accès, tel que la navigation sécurisée ou VPN complet

> **Remarque :**
> Tunnel - SSO Web est le nom de la navigation sécurisée dans les paramètres. Le comportement est le même.

Exemple :

Facteur	Secure Mail	Messagerie	En interne	Epic Rover
Version	10.1	10.1	X.x	X.x
Instance	VIP	Médecins	Personnel médical	Personnel médical
Plateforme	iOS	iOS	iOS	iOS
Utilisateurs cible	Utilisateurs VIP	Médecins	Personnel médical	Personnel médical
Appartenance	Département informatique	Département informatique	Département informatique	Département informatique
Type	MDX	MDX	Natif	Public
Cycle de mise à niveau	Trimestriel	Trimestriel	Annuel	S.O.
Gestion des licences	S.O.	S.O.	S.O.	Achat en volume
Stratégies MDX	Oui	Oui	Oui	Non
Accès réseau	VPN	VPN	VPN	Public

- **Gestion des versions des applications :** la gestion et le suivi des versions des applications constituent un élément essentiel du processus de provisioning. La gestion des versions est transparente pour les utilisateurs. Ils ne reçoivent des notifications que lorsqu'une nouvelle version de l'application est disponible en téléchargement. De votre point de vue, la vérification et le test de chaque version de l'application dans une capacité de non-production est également essentiel afin d'éviter l'impact sur la production.

  Il est également important d'évaluer si une mise à niveau spécifique est requise. Les mises à niveau d'application sont généralement de deux types : une mise à niveau mineure, comme la correction d'un bug spécifique et une version majeure, qui apporte des changements et des améliorations significatifs à l'application. Dans les deux cas, examinez attentivement les notes de mise à jour de l'application pour évaluer si la mise à niveau est nécessaire.

- **Développement d'applications :** lorsque vous intégrez le SDK MAM dans les applications mobiles que vous développez, vous appliquez des fonctionnalités MDX à ces applications. Consultez la section Présentation du SDK MAM.

  Le SDK MAM remplace l'outil MDX Toolkit, dont la fin de prise en charge est prévue en mars 2022. Pour de plus amples informations sur l'encapsulation d'applications, consultez la section MDX Toolkit. Le processus de provisioning d'application pour une application encapsulée est différent du processus de provisioning pour une application standard non encapsulée.

- **Sécurité de l'application :** vous définissez les exigences en matière de sécurité des applications individuelles ou des profils d'application dans le cadre du processus de provisioning. Vous pouvez mapper des exigences de sécurité à des stratégies MDM ou MAM spécifiques avant de déployer les applications. Cette planification simplifie et accélère le déploiement des applications. Par exemple :

  - Vous pouvez déployer certaines applications différemment.
  - Il peut être utile d'apporter des modifications architecturales à votre environnement XenMobile. Les modifications dépendent du type de conformité de sécurité requis par les applications. Par exemple, vous pouvez souhaiter que l'appareil soit crypté afin de permettre l'utilisation d'une application décisionnelle critique, ou qu'une application particulière nécessite un cryptage SSL ou un géofencing de bout en bout.

- **Mise à disposition de l'application :** XenMobile vous permet de mettre à disposition des applications en tant qu'applications MDM, ou en tant qu'applications MAM. Les applications MDM s'affichent dans XenMobile Store. Ce magasin vous permet de fournir facilement des applications publiques ou natives aux utilisateurs. Le seul contrôle d'application MDM que vous devez gérer est la mise en œuvre des restrictions au niveau de l'appareil. En revanche, la mise à disposition des applications à l'aide de MAM permet un contrôle total sur la mise à disposition de l'application et sur l'application elle-même. La mise à disposition des applications via MAM est généralement la meilleure solution.

- **Maintenance de l'application :**
  - Effectuer un audit initial : effectuez le suivi de la version de l'application présente dans votre environnement de production, ainsi que le dernier cycle de mise à niveau. Prenez note des fonctionnalités spécifiques ou des corrections de bogues qui ont nécessité la mise à niveau.
  - Établir des références : conservez une liste de la dernière version stable de chaque application. Cette version de l'application doit être utilisée en cas de problèmes inattendus après la mise à niveau. Élaborer également un plan de restauration. Tester les mises à niveau d'application dans un environnement de test avant de les déployer en production. Si possible, déployer la mise à niveau vers un sous-ensemble d'utilisateurs de production d'abord, puis vers l'ensemble de la base d'utilisateurs.
  - S'abonner aux notifications de mises à jour logicielles Citrix et à toutes les notifications de fournisseurs de logiciels tiers : ceci est essentiel pour rester à jour avec la dernière version des applications. Une version EAR (Early Access Release) peut être disponible pour les tests.
  - Concevoir une stratégie pour informer les utilisateurs : définir une stratégie pour informer les utilisateurs lorsque des mises à niveau d'application sont disponibles. Préparer les utilisateurs avec une formation avant le déploiement. Vous pouvez envoyer plusieurs notifications avant de mettre à jour les applications. Selon l'application, la meilleure méthode de notification peut être des notifications par e-mail ou des sites Web.

La gestion du cycle de vie de l'application représente le cycle de vie complet d'une application depuis son déploiement initial jusqu'à sa mise hors service. Le cycle de vie d'une application comporte les phases suivantes :

1. Configuration requise pour les spécifications : commencez par l'analyse de rentabilisation et les exigences de l'utilisateur.
2. Développement : vérifiez que l'application répond aux besoins de l'entreprise.
3. Test : identifiez les utilisateurs de test, les problèmes et les bogues.
4. Déploiement : déployez l'application aux utilisateurs de production.
5. Maintenance : mettez à jour de la version de l'application. Déployez l'application dans un environnement de test avant de mettre à jour l'application dans un environnement de production.

Exemple de cycle de vie de l'application à l'aide de Secure Mail

1. Configuration requise pour les spécifications : en matière d'exigence de sécurité, vous avez besoin d'une application de messagerie conteneurisée prenant en charge les stratégies de sécurité MDX.
2. Développement : vérifiez que l'application répond aux besoins de l'entreprise. Vous devez être en mesure d'appliquer des contrôles de stratégie MDX à l'application.

3. Test : affectez Secure Mail à un groupe d'utilisateurs test et déployez le fichier MDX correspondant à partir de XenMobile Server. Les utilisateurs test vérifient qu'ils peuvent envoyer et recevoir des e-mails et qu'ils disposent d'un accès au calendrier et aux contacts. Les utilisateurs test signalent également des problèmes et identifient des bogues. En fonction des commentaires des utilisateurs test, vous optimisez la configuration de Secure Mail pour une utilisation en production.
4. Déploiement : lorsque la phase de test est terminée, vous affectez Secure Mail aux utilisateurs de production et déployez le fichier MDX correspondant à partir de XenMobile.
5. Maintenance : une nouvelle mise à jour de Secure Mail est disponible. Vous téléchargez le nouveau fichier MDX à partir des téléchargements Citrix et remplacez le fichier MDX existant sur XenMobile Server. Demandez aux utilisateurs d'effectuer la mise à jour. Remarque : Citrix vous recommande d'effectuer et de tester ce processus dans un environnement de test. Ensuite, téléchargez l'application dans un environnement de production XenMobile et déployez l'application auprès des utilisateurs.

Pour de plus amples informations, consultez la section Encapsulation des applications mobiles iOS et Encapsulation des applications mobiles Android.

Opérations basées sur le tableau de bord

January 21, 2021

Vous pouvez afficher un synopsis des informations en accédant au tableau de bord de votre console XenMobile. Avec ces informations, vous pouvez voir un aperçu rapide des problèmes et des résolutions en utilisant des widgets.

Le tableau de bord est généralement l'écran qui s'affiche lorsque vous vous connectez à la console XenMobile. Pour accéder au tableau de bord ailleurs dans la console, cliquez sur **Analyser**. Cliquez sur **Personnaliser** dans le tableau de bord pour modifier la configuration de la page et pour modifier les widgets qui s'affichent.

- **Mes tableaux de bord :** vous pouvez enregistrer jusqu'à quatre tableaux de bord. Vous pouvez modifier ces tableaux de bord séparément et afficher chacun d'entre eux en sélectionnant le tableau de bord enregistré.
- **Disposition :** dans cette ligne, vous pouvez sélectionner le nombre de widgets qui s'affichent sur votre tableau de bord et la manière dont les widgets sont disposés.
- **Sélection des widgets :** vous pouvez choisir les informations qui s'affichent dans votre tableau de bord.
  - **Notifications :** cochez la case au-dessus des chiffres sur la gauche pour ajouter une barre Notifications au-dessus de vos widgets. Cette barre affiche le nombre d'appareils compatibles, d'appareils inactifs et d'appareils effacés ou inscrits dans les dernières 24 heures.

- **Appareils par plate-forme :** affiche le nombre d'appareils gérés et non gérés par plate-forme.
- **Appareils par opérateurs :** affiche le nombre d'appareils gérés et non gérés par opérateur. Cliquez sur chaque barre pour afficher la répartition par plate-forme.
- **Appareils gérés par plate-forme :** affiche le nombre d'appareils gérés par plate-forme.
- **Appareils non gérés par plate-forme :** affiche le nombre d'appareils non gérés par plate-forme. Les appareils qui s'affichent dans ce graphique peuvent avoir un agent installé, mais leurs privilèges ont été révoqués ou ils ont été effacés.
- **Appareils par état ActiveSync Gateway :** affiche le nombre d'appareils regroupés par état ActiveSync Gateway. Les informations affichent l'état Inconnu, Autorisé ou Bloqué. Vous pouvez cliquer sur chaque barre pour décomposer les données par plate-forme.
- **Appareils par appartenance :** affiche le nombre d'appareils regroupés par état d'appartenance. Les informations affichent l'état Appartenant à la société, Appartenant à l'employé ou Inconnu.
- **Déploiements de groupes de mise à disposition ayant échoué :** affiche le nombre total d'échecs de déploiements par package. Seuls les packages avec des échecs de déploiements s'affichent.
- **Appareils par motif de blocage :** affiche le nombre d'appareils bloqués par ActiveSync
- **Applications installées :** ce widget vous permet d'entrer le nom d'une application pour afficher un graphique contenant des informations sur cette application.
- **Licences utilisées par les applications d'achat en volume :** affiche des statistiques d'utilisation de licences pour les applications d'achat en volume d'Apple.

Cas d'utilisation

Voici quelques exemples de nombreuses façons d'utiliser les widgets de tableau de bord pour surveiller votre environnement.

- Vous avez déployé des applications de productivité mobiles et recevez des tickets d'assistance concernant les applications de productivité mobiles dont l'installation sur les appareils a échoué. Utilisez les widgets **Appareils non conformes** et **Applications installées** pour afficher les appareils sur lesquels les applications de productivité mobiles n'ont pas été installées.
- Vous souhaitez surveiller les appareils inactifs afin de pouvoir supprimer les appareils de votre environnement et récupérer des licences. Utilisez le widget **Appareils inactifs** pour suivre cette statistique.
- Vous recevez des tickets d'assistance concernant des données qui ne sont pas synchronisées correctement. Vous pouvez utiliser les widgets **Appareils par état ActiveSync Gateway** et **Appareils par motif de blocage** pour déterminer si le problème est lié à ActiveSync.

Rapports

Une fois votre environnement configuré et les utilisateurs inscrits, vous pouvez exécuter des rapports pour en savoir plus sur votre déploiement. XenMobile est équipé d'un certain nombre de rapports intégrés pour vous aider à mieux comprendre les appareils fonctionnant sur votre environnement. Pour plus de détails, consultez la section Rapports.

> **Important :**
>
> Bien qu'il soit possible d'utiliser SQL Server pour créer des rapports personnalisés, Citrix ne recommande pas cette méthode. L'utilisation de la base de données SQL Server de cette façon peut avoir des conséquences imprévues sur votre déploiement XenMobile. Si vous décidez d'utiliser cette méthode de création de rapports, assurez-vous que les requêtes SQL sont exécutées à l'aide d'un compte en lecture seule.

Contrôle d'accès basé sur les rôles et support XenMobile

January 10, 2022

XenMobile utilise le contrôle d'accès basé sur les rôles (RBAC) pour restreindre l'accès des utilisateurs et des groupes aux fonctions du système XenMobile, telles que la console XenMobile, l'assistance à distance Remote Support et l'API publique. Cet article décrit les rôles intégrés à XenMobile et inclut des notions importantes à prendre en compte pour décider d'un modèle de support pour XenMobile qui exploite RBAC.

> **Remarque :**
>
> L'Assistance à distance n'est plus disponible pour les nouveaux clients à compter du 1er janvier 2019. Les clients existants peuvent continuer à utiliser le produit, mais Citrix ne fournira pas d'améliorations ou de correctifs.

Rôles intégrés

Vous pouvez modifier l'accès accordé aux rôles intégrés suivants et vous pouvez ajouter des rôles. Pour obtenir l'ensemble des autorisations d'accès et de fonctionnalité associés à chaque rôle et leurs paramètres par défaut, téléchargez Paramètres par défaut du contrôle d'accès basé sur les rôles à partir de la documentation XenMobile. Pour une définition de chaque fonctionnalité, consultez la section Configuration de rôles avec RBAC dans la documentation XenMobile.

Rôle d'administrateur

Accès par défaut accordé :

- Accès complet au système, sauf à l'assistance à distance.
- Par défaut, les administrateurs peuvent effectuer certaines tâches de support, telles que la vérification de la connectivité et la création de packs d'assistance.

Notions importantes :

- Certains ou tous vos administrateurs ont-ils besoin d'accéder à l'assistance à distance ? Si c'est le cas, vous pouvez modifier le rôle Admin ou ajouter des rôles d'administrateur.
- Pour restreindre davantage l'accès à certains administrateurs ou groupes d'administrateurs, ajoutez des rôles en fonction du modèle d'administration et modifiez les autorisations.

Provisioning d'appareils

Accès par défaut accordé :

- Accès à la console XenMobile pour effectuer une administration de base sur les appareils Windows CE : ajout, modification et suppression d'appareils ; utilisez la page Paramètres.

Notions importantes :

- S'applique uniquement aux appareils Windows CE.

Support

Accès par défaut accordé :

- Accès à l'assistance à distance.

Notions importantes :

- Pour les déploiements locaux de XenMobile Server : l'Assistance à distance permet aux représentants du service d'assistance de contrôler à distance des appareils mobiles Windows CE et Android gérés. La capture d'écran est uniquement prise en charge sur les appareils Samsung KNOX.
- L'Assistance à distance n'est pas disponible pour les déploiements de XenMobile Server locaux en cluster.

Utilisateur

Accès par défaut accordé :

- Accès restreint à la console XenMobile : fonctionnalités d'appareil (par exemple, réinitialisation de l'appareil, verrouillage/déverrouillage de l'appareil, verrouillage/déverrouillage du conteneur ; affichage de l'emplacement et définition des restrictions géographiques, sonnerie de l'appareil, réinitialisation du mot de passe du conteneur) ; ajout, suppression et envoi des invitations d'inscription.

Notions importantes :

- Le rôle d'utilisateur permet aux utilisateurs de s'aider eux-mêmes.
- Pour prendre en charge les appareils partagés, créez un rôle d'utilisateur pour l'inscription des appareils partagés.

Notions importantes pour un modèle de support XenMobile

Les modèles de support que vous pouvez adopter peuvent varier considérablement et impliquer des tierces parties gérant les niveaux 1 et 2, tandis que les employés prennent en charge les niveaux 3 et 4. Quelle que soit la manière dont vous répartissez la charge de support, gardez à l'esprit les notions de cette section spécifiques à votre déploiement et à votre base d'utilisateurs XenMobile.

Les utilisateurs ont-ils des appareils appartenant à l'entreprise ou BYO ?
La principale question qui influence le support est de savoir à qui appartiennent les appareils utilisateur dans votre environnement XenMobile. Si vos utilisateurs possèdent des appareils appartenant à l'entreprise, vous pouvez proposer un niveau de support inférieur afin de verrouiller les appareils. Dans ce cas, vous pouvez fournir un service d'assistance qui aide les utilisateurs à résoudre les problèmes liés aux appareils et à l'utilisation des appareils. En fonction des types d'appareils que vous devez prendre en charge, pensez à la manière dont vous pouvez utiliser les rôles de provisioning et de prise en charge des appareils RBAC pour votre service d'assistance.

Si vos utilisateurs disposent d'appareils BYO, votre organisation peut s'attendre à ce que les utilisateurs trouvent leurs propres sources pour la prise en charge de l'appareil. Dans ce cas, le support fourni par votre organisation est davantage un rôle administratif centré sur les problèmes spécifiques à XenMobile.

Quel est votre modèle de support pour les ordinateurs de bureau ?
Déterminez si votre modèle de support pour les ordinateurs de bureau est approprié pour les autres appareils appartenant à l'entreprise. Pouvez-vous utiliser la même organisation de support ? De quelle formation supplémentaire aura-t-elle besoin ?

Voulez-vous autoriser les utilisateurs à accéder au portail en libre-service XenMobile ?
Utilisez **Paramètres > Inscription** pour activer le portail en libre-service et définir un mode d'inscription sécurisée. À partir du portail en libre-service, les utilisateurs peuvent générer des liens d'inscription qui leur permettent d'inscrire leurs appareils ou de s'envoyer à eux-mêmes une invitation d'inscription. Consultez Configurer les modes d'inscription sécurisée.

Suivi du système

January 10, 2022

Pour garantir une disponibilité optimale de l'accès et de la connectivité aux applications, vous devez surveiller les composants principaux suivants dans l'environnement XenMobile.

XenMobile Server

XenMobile Server génère et stocke des journaux sur le stockage local que vous pouvez également exporter vers un serveur de journal système (syslogs). Vous pouvez configurer les paramètres de journal pour spécifier les contraintes de taille, le niveau de journalisation ou créer des journaux personnalisés pour filtrer des événements spécifiques. Vous pouvez consulter les journaux de XenMobile Server depuis la console XenMobile à tout moment. Vous pouvez également exporter des informations dans les journaux via le serveur syslog vers vos serveurs de journalisation Splunk de production.

La liste suivante décrit les différents types de fichiers journaux disponibles dans XenMobile :

Fichier journal de débogage : contient des informations de niveau de débogage sur les services Web de base de XenMobile, y compris les messages d'erreur et les actions liées au serveur.

Format du message :

```
<date> <timestamp> <loglevel> <class name (including the package)> - <id> <
log message>
```

- où <id> est un identifiant unique comme sessionID.
- où <log message> est le message fourni par l'application.

Fichier journal d'audit administrateur : contient des informations d'audit relatives à l'activité sur la console XenMobile.

> **Remarque :**
>
> Le même format est utilisé pour les journaux d'audit administrateur et les journaux d'audit utilisateur.

Format du message :

À l'exception des valeurs Date et Timestamp requises, tous les autres attributs sont facultatifs. Les champs facultatifs sont représentés par " " dans le message.

```
<date> <timestamp> "<username/id>""<sessionid>""<deviceid>""<clientip>"
"<action>""<status>""<application name>""<app user id>""<user agent>""<
details>"
```

Le tableau suivant répertorie les événements du journal d'audit administrateur disponibles :

Messages du journal d'audit administrateur pour les événements	État
Login	success/failure

Messages du journal d'audit administrateur pour les événements	État
Logout	success/failure
Get admin	success/failure
Update admin	success/failure
Get application	success/failure
Add application	success/failure
Update application	success/failure
Delete application	success/failure
Bind application	success/failure
Unbind application	success/failure
Disable application	success/failure
Enable application	success/failure
Get category	success/failure
Add category	success/failure
Update category	success/failure
Delete category	success/failure
Add certificate	success/failure
Delete certificate	success/failure
Active certificate	success/failure
CSR certificate	success/failure
Export certificate	success/failure
Delete certificate chain	success/failure
Add certificate chain	success/failure
Get connector	success/failure
Add connector	success/failure
Delete connector	success/failure
Update connector	success/failure
Get device	success/failure
Lock device	success/failure

Messages du journal d'audit administrateur pour les événements	État
Unlock device	success/failure
Wipe device	success/failure
Unwipe device	success/failure
Delete device	success/failure
Get role	success/failure
Add role	success/failure
Update role	success/failure
Delete role	success/failure
Bind role	success/failure
Unbind role	success/failure
Update config settings	success/failure
Update workflow email	success/failure
Add workflow	success/failure
Delete workflow	success/failure
Add Active Directory	success/failure
Update Active Directory	success/failure
Add masteruserlist	success/failure
Update masteruserlist	success/failure
Update DNS	success/failure
Update Network	success/failure
Update log server	success/failure
Transfer log from log server	success/failure
Update syslog	success/failure
Update receiver updates	success/failure
Update time server	success/failure
Update trust	success/failure
Add service record	success/failure
Update service record	success/failure

Messages du journal d'audit administrateur pour les événements	État
Update receiver email	success/failure
Upload patch	success/failure
Import snapshot	success/failure
Fetch app store app details	success/failure
Update MDM	success/failure
Delete MDM	success/failure
Add HDX	success/failure
Update HDX	success/failure
Delete HDX	success/failure
Add Branding	success/failure
Delete Branding	success/failure
Update SSL offload	success/failure
Add account property	success/failure
Delete account property	success/failure
Update account property	success/failure
Add beacon	success/failure

Fichier journal d'audit utilisateur : contient des informations relatives à l'activité de l'utilisateur provenant d'appareils inscrits.

> **Remarque :**
>
> Le même format est utilisé pour les journaux d'audit administrateur et les journaux d'audit utilisateur.

Format du message :

À l'exception des valeurs Date et Timestamp requises, tous les autres attributs sont facultatifs. Les champs facultatifs sont représentés par " " dans le message. Par exemple,

```
<date> <timestamp> "<username/id>""<sessionid>""<deviceid>""<clientip>"
"<action>""<status>""<application name>""<app user id>""<user agent>""<
details>"
```

Le tableau suivant répertorie les événements du journal d'audit utilisateur disponibles :

Messages du journal d'audit utilisateur pour les événements	État
Login	success/failure
Session time-out	success/failure
Subscribe	success/failure
Unsubscribe	success/failure
Pre-launch	success/failure
AGEE SSO	success/failure
Jeton SAML pour Citrix Files	success/failure
Enregistrement de l'appareil	success/failure
Device check	lock/wipe
Device update	success/failure
Token refresh	success/failure
Secret saved	success/failure
Secret retrieved	success/failure
User initiated change password	success/failure
Mobile client download	success/failure
Logout	success/failure
Discovery Service	success/failure
Endpoint Service	success/failure

Fonctions MDM	État
REGHIVE	success/failure
Cab inventory	success/failure
Cab	success/failure
Cab auto install	success/failure
Cab shell install	success/failure
Cab create folder	success/failure
Cab file get	success/failure
File create folder	success/failure

Fonctions MDM	État
File get	success/failure
File sent	success/failure
Script create folder	success/failure
Script get	success/failure
Script sent	success/failure
Script shell execution	success/failure
Script auto execution	success/failure
APK inventory	success/failure
APK	success/failure
APK shell install	success/failure
APK auto install	success/failure
APK create folder	success/failure
APK file get	success/failure
APK App	success/failure
EXT App	success/failure
List get	success/failure
List sent	success/failure
Locate device	success/failure
CFG	success/failure
Déverrouiller	success/failure
SharePoint wipe	success/failure
SharePoint Configuration	success/failure
Remove profile	success/failure
Remove application	success/failure
Remove unmanaged application	success/failure
Remove unmanaged profile	success/failure
IPA App	success/failure
EXT App	success/failure
Apply redemption code	success/failure

Fonctions MDM	État
Apply settings	success/failure
Enable tracking device	success/failure
App management policy	success/failure
SD card wipe	success/failure
Encrypted email attachment	success/failure
Branding	success/failure
Secure browser	success/failure
Container browser	success/failure
Container unlock	success/failure
Container password reset	success/failure
AG client auth creds	success/failure

Citrix ADC surveille également l'état du service Web XenMobile qui est configuré avec des outils d'analyse de surveillance intelligents pour simuler des demandes HTTP à chaque nœud de cluster XenMobile Server. Les outils d'analyse déterminent si le service est en ligne et répondent ensuite en fonction de la réponse reçue. Dans le cas où un nœud ne répond pas comme prévu, Citrix ADC marque le serveur comme étant en panne. En outre, Citrix ADC extrait le nœud du pool d'équilibrage de charge et enregistre l'événement pour générer des alertes via la solution de surveillance Citrix ADC.

Vous pouvez également utiliser des outils de surveillance d'hyperviseur standard pour surveiller les machines virtuelles XenMobile et fournir des alertes pertinentes concernant les mesures d'utilisation du processeur, de la mémoire et du stockage.

SQL Server et base de données

Les performances de SQL Server et de la base de données affectent directement les services XenMobile. L'instance XenMobile requiert l'accès à la base de données à tout moment et se déconnecte (par exemple, elle ne répond plus) en cas de panne de l'infrastructure SQL. La console XenMobile peut continuer à fonctionner pendant un certain temps après des problèmes d'espace disque avec SQL Server. Pour garantir un temps d'activité maximal de la base de données et des performances adéquates pour la charge de travail XenMobile, vous devez surveiller de manière proactive l'état de vos serveurs SQL. Pour plus d'informations sur la surveillance de vos serveurs SQL, consultez Présentation de la surveillance et du réglage des performances. En outre, vous devez ajuster l'allocation des ressources pour le

processeur, la mémoire et le stockage afin de garantir les accords de niveau de service lorsque votre environnement XenMobile continue de se développer.

Citrix ADC

Citrix ADC permet de consigner des mesures dans un stockage interne ou d'envoyer des journaux à un serveur de journalisation externe. Vous pouvez configurer le serveur syslog pour exporter les journaux Citrix ADC vers vos serveurs de journalisation Splunk de production. Les niveaux de journalisation suivants sont disponibles dans Citrix ADC :

- Emergency
- Alert
- Critical
- Error
- Warning
- Information

Les fichiers journaux sont également stockés dans le stockage Citrix ADC dans le répertoire /var/log/ns.log et sont appelés « newnslog ». Citrix ADC regroupe et compresse les fichiers en utilisant l'algorithme GZIP. Les fichiers journaux sont appelés « newnslog.xx.gz », où xx représente un numéro d'ordre.

Citrix ADC prend également en charge les traps et les alertes SNMP en tant qu'option de surveillance. Pour obtenir une liste des traps SNMP, consultez la section Surveillance SNMP.

Récupération d'urgence

January 10, 2022

Vous pouvez concevoir et configurer des déploiements XenMobile comprenant plusieurs sites pour la récupération d'urgence à l'aide d'une stratégie de basculement active-passive.

La stratégie de récupération d'urgence recommandée dans cet article comprend les éléments suivants :

- Un seul site actif XenMobile dans le centre de données d'un lieu géographique desservant tous les utilisateurs de l'entreprise dans le monde, appelé site principal.
- Un deuxième site XenMobile dans le centre de données d'un deuxième emplacement géographique, appelé site de récupération d'urgence. Ce site de récupération d'urgence fournit un basculement actif-passif du site si une défaillance du centre de données à l'échelle du site se produit sur le site principal. Le site principal comprend XenMobile, la base de données SQL et

l'infrastructure Citrix ADC afin de faciliter le basculement et de fournir aux utilisateurs un accès à XenMobile via un événement d'échec de la connectivité au site principal.

Les serveurs XenMobile du site de récupération d'urgence restent hors connexion pendant les opérations normales et sont mis en ligne uniquement lors des scénarios de récupération d'urgence où le basculement complet du site (du site principal au site de récupération d'urgence) est requis. Les serveurs SQL sur le site de récupération d'urgence doivent être actifs et prêts à desservir les connexions avant que les serveurs XenMobile ne puissent être redémarrés sur le site de récupération d'urgence.

Cette stratégie de récupération d'urgence repose sur le basculement manuel du niveau d'accès Citrix ADC au moyen de modifications DNS pour acheminer les connexions MDM et MAM vers le site de récupération d'urgence en cas de panne.

> **Remarque :**
>
> Pour utiliser cette architecture, vous devez mettre en place un processus de sauvegarde asynchrone des bases de données, ainsi qu'un moyen d'assurer la haute disponibilité de l'infrastructure SQL.

Processus de basculement de récupération d'urgence

1. Si vous testez votre processus de basculement de récupération d'urgence, arrêtez les serveurs XenMobile du site principal pour simuler une défaillance du site.
2. Modifiez les enregistrements DNS publics des serveurs XenMobile pour qu'ils pointent vers les adresses IP externes du site de récupération d'urgence.
3. Modifiez l'enregistrement DNS interne pour que le serveur SQL pointe sur l'adresse IP du serveur SQL du site de récupération d'urgence.
4. Mettez les bases de données SQL XenMobile en ligne sur le site de récupération d'urgence. Assurez-vous que SQL Server et la base de données sont actifs et prêts à desservir les connexions des serveurs XenMobile locaux sur le site.
5. Activez les serveurs XenMobile sur le site de récupération d'urgence.

Processus de mise à jour de XenMobile Server

Suivez ces étapes chaque fois que vous mettez à jour XenMobile avec des correctifs et des versions afin de préserver l'uniformité du code des serveurs principal et de récupération d'urgence.

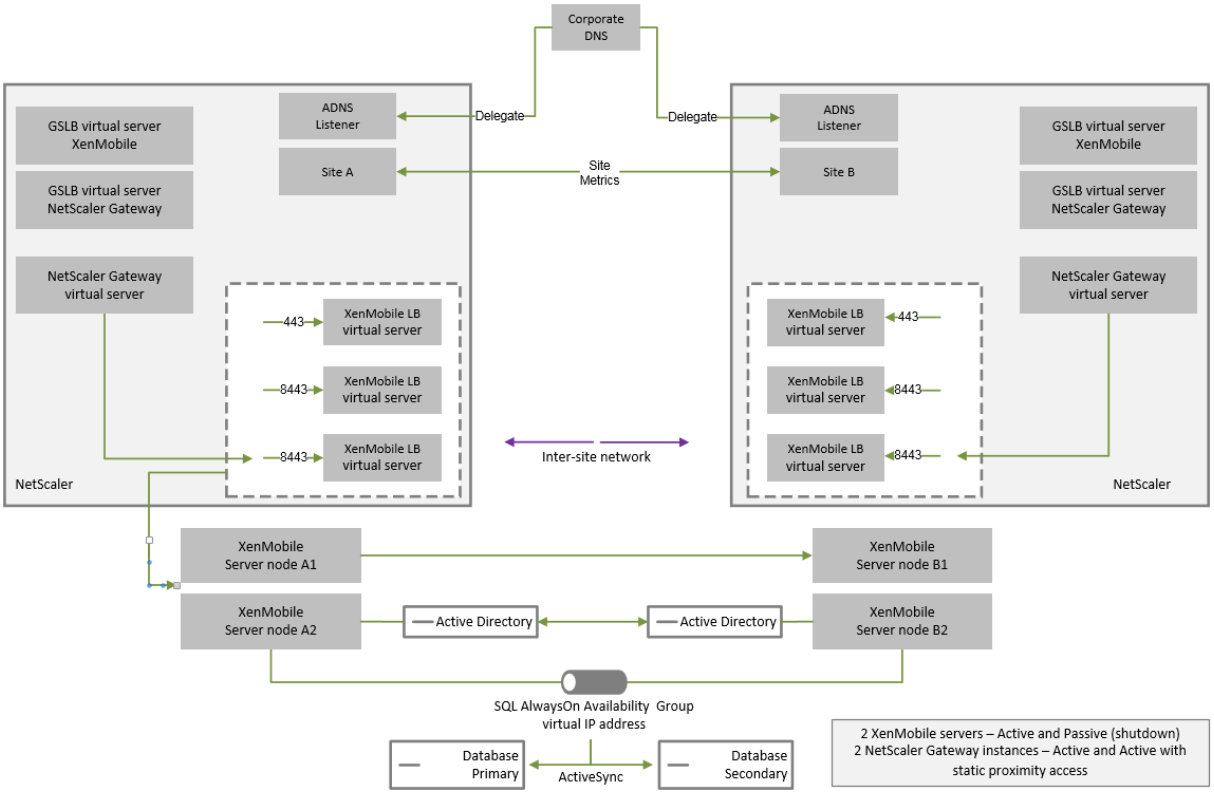
1. Assurez-vous que les serveurs XenMobile du site principal ont été corrigés ou mis à niveau.
2. Assurez-vous que l'enregistrement DNS pour SQL Server est associé à la base de données SQL Server active sur le site principal.
3. Mettez les serveurs XenMobile du site de récupération d'urgence en ligne. Les serveurs se connectent à la base de données du site principal sur le WAN uniquement au cours du processus de

mise à niveau.

4. Appliquez les correctifs et les mises à jour requis sur tous les serveurs XenMobile du site de récupération d'urgence.
5. Redémarrez les serveurs XenMobile et vérifiez que le correctif ou la mise à niveau a été appliqué(e).

Diagramme d'architecture de référence de récupération d'urgence

Le diagramme suivant illustre l'architecture de haut niveau d'un déploiement de XenMobile pour la récupération d'urgence.



GSLB pour la récupération d'urgence

Un élément clé de cette architecture est l'utilisation de GSLB (Global Server Load Balancing) pour diriger le trafic vers le centre de données approprié.

Par défaut, l'assistant Citrix ADC for XenMobile configure Citrix Gateway de manière à ne pas activer l'utilisation de GSLB pour la récupération d'urgence. Par conséquent, vous devez prendre des mesures supplémentaires.

Fonctionnement de GSLB

GSLB est à la base une forme de DNS. Les appareils Citrix ADC participants agissent en tant que serveurs DNS faisant autorité et associent les enregistrements DNS à l'adresse IP correcte (généralement le VIP censé recevoir le trafic). L'appliance Citrix ADC vérifie l'intégrité du système avant de répondre à une requête DNS dirigeant le trafic vers ce système.

Lorsqu'un enregistrement est associé, le rôle de GSLB dans la résolution du trafic est terminé. Le client communique directement avec l'adresse IP virtuelle (VIP) cible. Le comportement du client DNS joue un rôle important dans le contrôle de la méthode et de la date d'expiration d'un enregistrement. Ce comportement se situe en grande partie en dehors des limites du système Citrix ADC. Ainsi, GSLB est soumis aux mêmes limitations que la résolution de noms DNS. Les clients mettent en cache les réponses. Par conséquent, l'équilibrage de charge dans ce contexte n'est pas effectué en temps réel, contrairement à l'équilibrage de charge traditionnel.

La configuration GSLB sur Citrix ADC, y compris les sites, les services et les moniteurs, existe afin de fournir la résolution de nom DNS correcte.

La configuration réelle des serveurs de publication (dans ce scénario, la configuration créée par l'assistant Citrix ADC for XenMobile) n'est pas affectée par GSLB. GSLB est un service distinct sur Citrix ADC.

Défis liés à la délégation de domaine lors de l'utilisation de GSLB avec XenMobile

L'assistant Citrix ADC for XenMobile configure Citrix Gateway pour XenMobile. Cet assistant génère trois serveurs virtuels d'équilibrage de charge et un serveur virtuel Citrix Gateway.

Deux des serveurs virtuels d'équilibrage de charge gèrent le trafic MDM sur les ports 443 et 8443. Citrix Gateway reçoit le trafic MAM et le transmet au troisième serveur, le serveur virtuel d'équilibrage de charge MAM, sur le port 8443. Tout le trafic vers le serveur virtuel d'équilibrage de charge MAM est transmis via Citrix Gateway.

Le serveur virtuel d'équilibrage de charge MAM nécessite le même certificat SSL que les serveurs XenMobile et utilise le même nom de domaine complet que celui utilisé lors de l'inscription d'appareils. Le serveur d'équilibrage de charge MAM utilise également le même port (8443) que l'un des serveurs d'équilibrage de charge MDM. Pour permettre la résolution du trafic, l'assistant Citrix ADC for XenMobile crée un enregistrement DNS local sur Citrix Gateway. L'enregistrement DNS correspond au nom de domaine complet utilisé lors de l'inscription d'appareils.

Cette configuration est efficace lorsque l'URL du serveur XenMobile n'est pas une URL de domaine GSLB. Si une URL de domaine GSLB est utilisée en tant qu'URL de serveur XenMobile, comme l'exige la récupération d'urgence, l'enregistrement DNS local empêche Citrix Gateway de résoudre le trafic sur les serveurs d'équilibrage de charge MDM.

Utilisation de la méthode CNAME pour la récupération d'urgence GSLB

Pour résoudre les problèmes liés à la configuration par défaut créée par l'assistant Citrix ADC for XenMobile, vous pouvez créer un enregistrement CNAME associé au nom de domaine complet du serveur XenMobile dans le domaine parent (`company.com`) et pointez un enregistrement vers la sous-zone déléguée (`gslb.company.com`) pour laquelle Citrix ADC fait autorité. Cela permet la création d'un enregistrement A DNS statique pour l'adresse VIP d'équilibrage de charge MAM requise pour résoudre le trafic.

1. Sur le DNS externe, créez un CNAME associé au nom de domaine complet du serveur XenMobile qui pointe vers le nom de domaine complet du domaine GSLB sur Citrix ADC GSLB. Vous avez besoin de deux domaines GSLB : un pour le trafic MDM et un autre pour le trafic MAM (Citrix Gateway).

   Exemple :

   ```
   CNAME = xms.company.com IN CNAME xms.gslb.comany.com
   ```

2. Sur l'instance Citrix Gateway de chaque site, créez un serveur virtuel GSLB avec un nom de domaine complet correspondant à celui indiqué par l'enregistrement CNAME.

   Exemple :

   ```
   bind gslb vserver xms-gslb -domainName xms.gslb.company.com
   ```

   Lorsque vous utilisez l'assistant Citrix ADC for XenMobile pour déployer Citrix Gateway, utilisez l'URL du serveur XenMobile lors de la configuration du serveur d'équilibrage de charge MAM. Cela permet de créer un enregistrement A DNS statique pour l'URL du serveur XenMobile.

3. Testez avec les clients qui s'inscrivent sur Secure Hub à l'aide de l'URL du serveur XenMobile (`xms.company.com`).

   Cet exemple utilise les noms de domaine complets suivants :

   - `xms.company.com` est l'URL utilisée par le trafic MDM et par les appareils lors de l'inscription, configurée dans cet exemple à l'aide de l'assistant Citrix ADC for XenMobile.
   - `xms.gslb.company.com` est le nom de domaine complet du domaine GSLB pour le serveur XenMobile.

Processus de support Citrix

January 10, 2022

Vous pouvez activer les services de support technique Citrix pour résoudre les problèmes liés aux produits Citrix. Le groupe travaille conjointement avec les équipes de développement pour propose des solutions et des résolutions aux problèmes.

Les services de conseil, Citrix Consulting Services, ou les services de formation, Citrix Education Services, proposent une assistance liée à la formation sur les produits et des conseils sur l'utilisation, la configuration et l'installation des produits, ainsi que sur la conception et l'architecture de l'environnement.

Citrix Consulting aide les projets liés aux produits Citrix, notamment la validation des concepts, l'évaluation de l'impact économique, la vérification de l'infrastructure, l'analyse des exigences de conception, la vérification de la conception de l'architecture, l'intégration et le développement des processus opérationnels.

Citrix Education offre une formation et une certification informatique de premier ordre sur les technologies de virtualisation, de cloud et de réseau Citrix.

Citrix vous recommande de tirer pleinement parti des ressources d'auto-assistance et des recommandations Citrix avant de créer un ticket d'assistance. Par exemple, vous pouvez accéder à plusieurs articles et bulletins écrits par des experts techniques Citrix, consulter la documentation produit relative aux solutions et aux technologies Citrix, ou lire des conseils directs des responsables, des équipes produit et des experts techniques Citrix. Consultez les pages Centre de connaissances, Documentation produit et Blogs.

Pour une assistance plus interactive, vous pouvez participer à des forums de discussion où vous pouvez poser des questions et obtenir des réponses d'autres clients, partager des idées, des opinions, des informations techniques et des meilleures pratiques au sein de groupes d'utilisateurs et de groupes d'intérêt ou interagir avec les techniciens Citrix qui contrôlent les sites de réseaux sociaux liés au support Citrix. Consultez les pages Support Forums et Citrix Community.

Vous avez également accès à des cours de formation et de certification pour développer vos compétences. Consultez la page Citrix Education.

Citrix Insight Services propose une plate-forme simple de dépannage en ligne et de contrôle de l'état de votre environnement Citrix. Disponible pour XenMobile, Citrix Virtual Apps and Desktops, Citrix Hypervisor et Citrix Gateway. Consultez la page Outil d'analyse.

Pour obtenir un support technique, vous pouvez créer un ticket d'assistance par téléphone ou via le web. Vous pouvez utiliser le site Web pour les problèmes dont le niveau de gravité est faible ou moyen et utiliser l'option de téléphone pour les problèmes dont le niveau de gravité est élevé. Pour plus d'informations sur le contact du support technique pour les problèmes XenMobile, consultez la page Comment contacter le support technique.

Si vous recherchez un point de contact unique hautement qualifié avec une vaste expérience dans la distribution des solutions Citrix, Citrix Services propose un gestionnaire de relations techniques. Pour plus d'informations sur les avantages et offre des services Citrix, consultez la section Citrix Worldwide Services.

Envoi d'invitations d'inscription de groupe dans XenMobile

September 22, 2021

Contribution de John Bartel III

Vous pouvez envoyer des invitations d'inscription à des groupes et des groupes imbriqués dans XenMobile Server. Les invitations d'inscription ne sont pas disponibles pour les appareils Windows.

Lors de la configuration de l'invitation de groupe, vous pouvez spécifier une ou plusieurs plates-formes d'appareil. Vous pouvez également marquer les appareils pour, par exemple, distinguer les appareils appartenant à l'entreprise des appareils appartenant aux employés. Vous définissez ensuite le type d'authentification pour les machines utilisateur.

> **Remarque :**
>
> Si vous prévoyez d'utiliser des modèles de notification personnalisés, vous devez définir les modèles avant de configurer des modes de sécurité d'inscription. Pour de plus amples informations sur les modèles de notification, consultez la section Création et mise à jour de modèles de notification.

Pour plus d'informations sur les configurations de base sur les comptes utilisateur, les rôles, les modes d'inscription sécurisée et les invitations, consultez la section Comptes utilisateur, rôles et inscription.

Étapes générales

1. Dans la console XenMobile, cliquez sur **Gérer > Invitations d'inscription**.
2. Cliquez sur **Ajouter** dans le coin supérieur gauche de l'écran, puis cliquez sur **Ajouter une Invitation**.
3. Cliquez sur **Groupe** dans le menu **Destinataire**.

   Cette étape vous permet de choisir une ou plusieurs plates-formes. Si vous disposez de plusieurs plates-formes de système d'exploitation au sein de votre entreprise, choisissez toutes les plates-formes. Ne désactivez la sélection de plate-forme que si vous êtes sûr qu'aucun utilisateur n'utilise la plate-forme particulière.
4. Vous pouvez choisir de marquer les appareils pendant le processus d'invitation. Choisissez **Entreprise** ou **Employé**.

   Le marquage facilite la séparation des appareils appartenant à l'entreprise et des appareils appartenant aux employés.
5. Dans la liste **Domaine**, choisissez le domaine dans lequel le groupe existe.
6. Dans la liste **Groupe**, sélectionnez le groupe Active Directory auquel vous souhaitez envoyer les invitations.

7. L'option **Mode d'inscription** vous permet de définir le type d'authentification sécurisée que vous préférez pour les utilisateurs.

   - Nom d'utilisateur + mot de passe
   - Haute sécurité
   - URL d'invitation
   - URL d'invitation + PIN
   - URL d'invitation + mot de passe
   - Deux facteurs
   - Nom d'utilisateur + PIN

   > **Remarque :**
   >
   > Pour envoyer des invitations d'inscription, vous pouvez uniquement utiliser les modes d'inscription sécurisée **URL d'invitation**, **URL d'invitation + PIN** ou **URL d'invitation + mot de passe**. Pour les appareils qui sont inscrits avec **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + PIN**, les utilisateurs doivent entrer manuellement leurs informations d'identification dans Secure Hub.

8. Pour les modèles **Téléchargement de l'agent**, **URL d'inscription**, **Code PIN d'inscription** et **Confirmation d'inscription**, choisissez le modèle de notification personnalisé que vous avez créé antérieurement. Ou choisissez la valeur par défaut qui est répertorié.

   Si vous prévoyez d'utiliser des modèles de notification personnalisés, vous devez définir les modèles avant de configurer des modes de sécurité d'inscription. Pour plus d'informations sur les modèles de notifications, veuillez consulter la section Notifications.

   Pour ces modèles de notification, utilisez la configuration du serveur SMTP définie dans XenMobile. Définissez d'abord vos informations SMTP avant de poursuivre.

   > **Remarque :**
   >
   > Les options **Expire après** et **Nbre max de tentatives** varient en fonction de l'option **Mode d'inscription** que vous choisissez. Vous ne pouvez pas modifier ces options.

9. Sélectionnez Activé pour **Envoyer invitation**, puis cliquez sur **Enregistrer et envoyer** pour terminer le processus.

Prise en charge des groupes imbriqués

Vous pouvez utiliser des groupes imbriqués pour envoyer des invitations. Généralement, les groupes imbriqués sont utilisés dans des environnements à grande échelle dans lesquels des groupes ayant des autorisations similaires sont liés entre eux.

Accédez à **Paramètres > LDAP** puis à activer l'option **Prendre en charge les groupes imbriqués**.

Dépannage et limitations connues

Problème : des invitations sont envoyées aux utilisateurs même s'ils ont été supprimés d'un groupe Active Directory.

Solution : selon la taille de votre environnement Active Directory, la propagation des modifications à tous les serveurs peut prendre jusqu'à six heures. Si un utilisateur ou un groupe imbriqué est récemment supprimé, XenMobile peut toujours considérer ces utilisateurs comme faisant partie du groupe.

Par conséquent, il est préférable d'attendre jusqu'à six heures avant d'envoyer une autre invitation de groupe à votre groupe.

Configuration d'un serveur d'attestation de l'intégrité des appareils sur site

January 10, 2022

Contribution de Sanket Mishra

Vous pouvez activer l'attestation de l'intégrité des appareils (DHA) pour appareils mobiles Windows 10 et Windows 11 via un serveur Windows local. Pour activer DHA sur site, vous devez d'abord configurer un serveur DHA.

Après la configuration d'un serveur DHA, vous devez créer une stratégie XenMobile Server pour activer le service DHA sur site. Pour plus d'informations sur la création de cette stratégie, consultez la section Stratégie d'attestation de l'intégrité des appareils.

Configuration requise pour un serveur DHA

- Un serveur exécutant Windows Server Technical Preview 5 ou version ultérieure, installé à l'aide de l'option d'installation de Desktop Experience.
- Une ou plusieurs machines clientes Windows 10 et Windows 11. Ces machines doivent avoir TPM 1.2 ou 2.0 exécutant la dernière version de Windows.
- Ces certificats :
  - **Certificat SSL DHA.** Un certificat SSL x.509 qui s'enchaîne à une racine de confiance d'entreprise avec une clé privée exportable. Ce certificat protège les communications de données DHA en transit, y compris les communications serveur à serveur (service DHA et serveur MDM) et serveur à client (service DHA et appareil Windows 10 ou Windows 11).
  - **Certificat de signature DHA.** Un certificat x.509 qui est lié à la racine de confiance d'entreprise avec une clé privée exportable. Le service DHA utilise ce certificat pour la signature numérique.

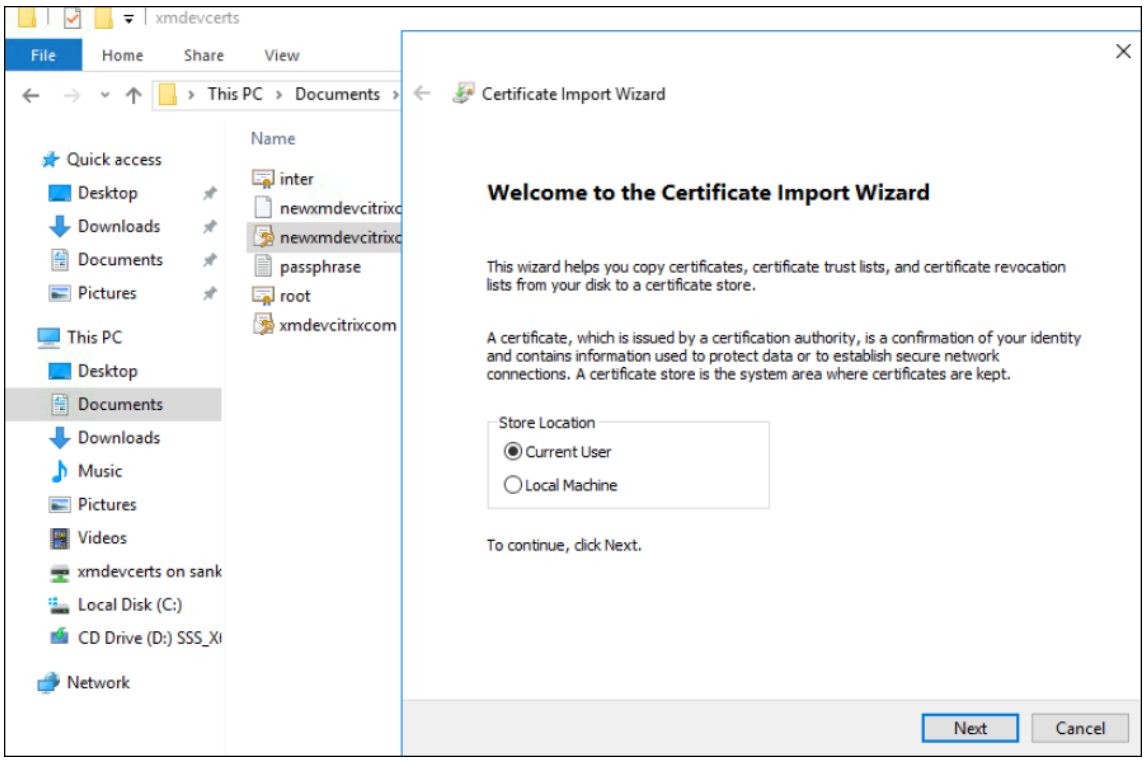
  - **Certificat de chiffrement DHA.** Un certificat x.509 qui est lié à la racine de confiance d'entreprise avec une clé privée exportable. Le service DHA utilise également ce certificat pour le cryptage.
- Choisissez l'un de ces modes de validation de certificat :
  - **EKCert.** Le mode de validation EKCert est optimisé pour les appareils des organisations qui ne sont pas connectées à Internet. Les appareils qui se connectent à un service DHA s'exécutant en mode de validation EKCert n'ont pas d'accès direct à Internet.
  - **AIKCert.** Le mode de validation AIKCert est optimisé pour les environnements opérationnels qui ont accès à Internet. Les appareils qui se connectent à un service DHA s'exécutant en mode de validation AIKCert doivent avoir un accès direct à Internet et pouvoir obtenir un certificat AIK auprès de Microsoft.

Ajouter le rôle de serveur DHA au serveur Windows

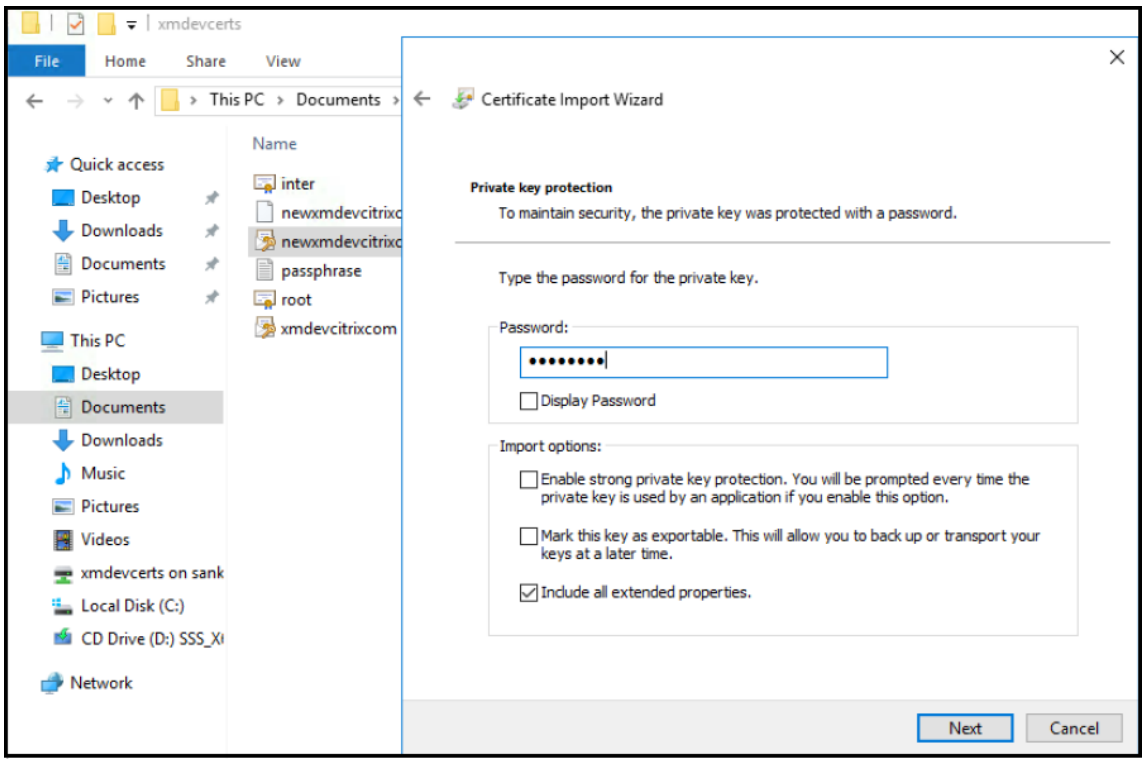
1. Sur le serveur Windows, si le Gestionnaire de serveur n'est pas déjà ouvert, cliquez sur **Démarrer**, puis sur **Gestionnaire de serveur**.
2. Cliquez sur **Ajouter des rôles et fonctionnalités**.
3. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Sélectionner un serveur du pool de serveurs**, sélectionnez le serveur, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner le rôle de serveur**, cochez la case Attestation d'intégrité de l'appareil.
7. Facultatif : cliquez sur **Ajouter les fonctionnalités** pour installer d'autres services et fonctionnalités de rôle requis.
8. Cliquez sur **Suivant**.
9. Sur la page **Sélectionner une fonctionnalité**, cliquez sur **Suivant**.
10. Sur la page **Rôle Serveur Web (IIS)**, cliquez sur **Suivant**.
11. Sur la page **Sélectionner les services de rôle**, cliquez sur **Suivant**.
12. Sur la page **Service d'attestation d'intégrité de l'appareil**, cliquez sur **Suivant**.
13. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
14. Une fois l'installation terminée, cliquez sur **Fermer**.

Ajouter le certificat SSL au magasin de certificats du serveur

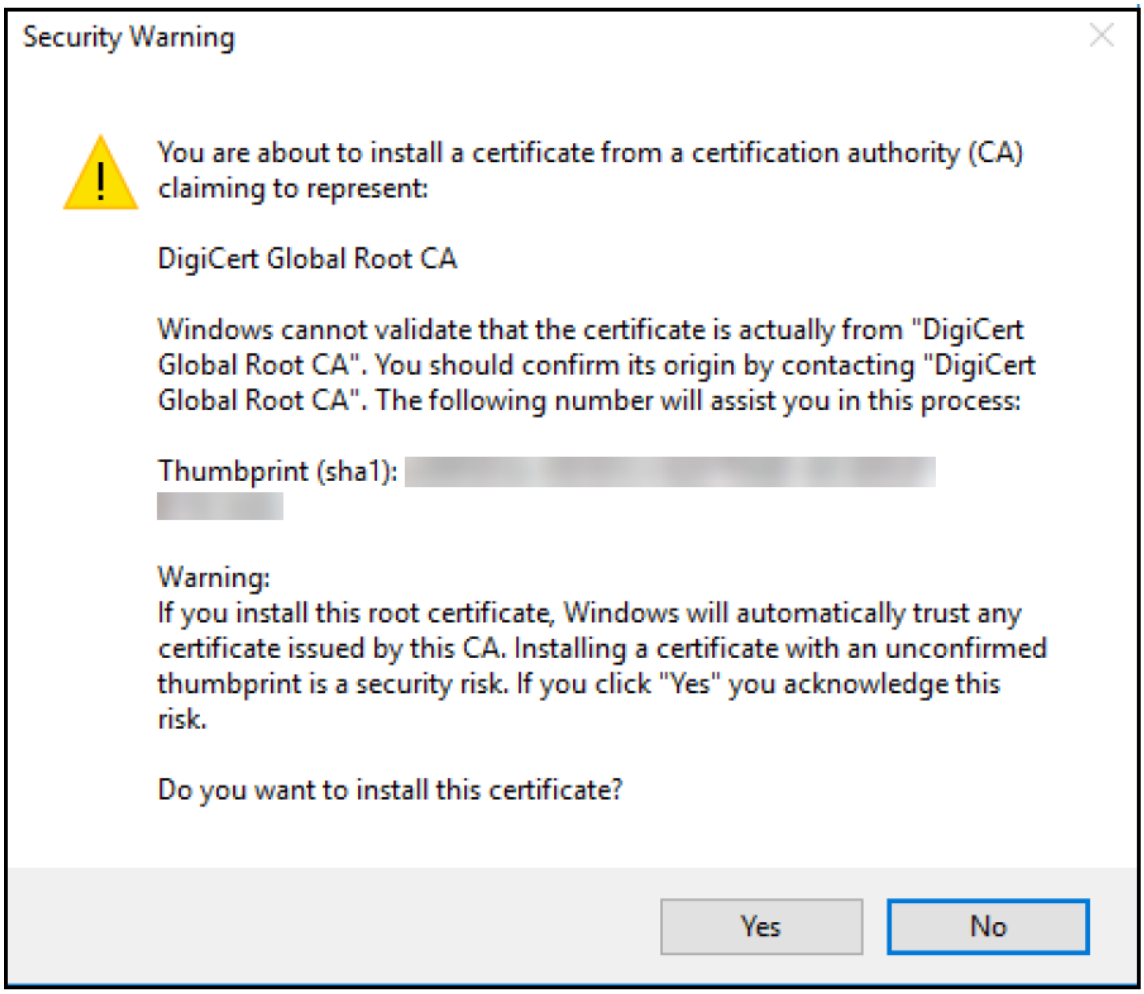
1. Accédez au fichier de certificat SSL et sélectionnez-le.
2. Sélectionnez **Utilisateur actuel** comme emplacement du magasin et cliquez sur **Suivant**.



3. Tapez le mot de passe affecté à la clé privée.
4. Assurez-vous que l'option d'importation **Inclure toutes les propriétés étendues** est sélectionnée. Cliquez sur **Suivant**.

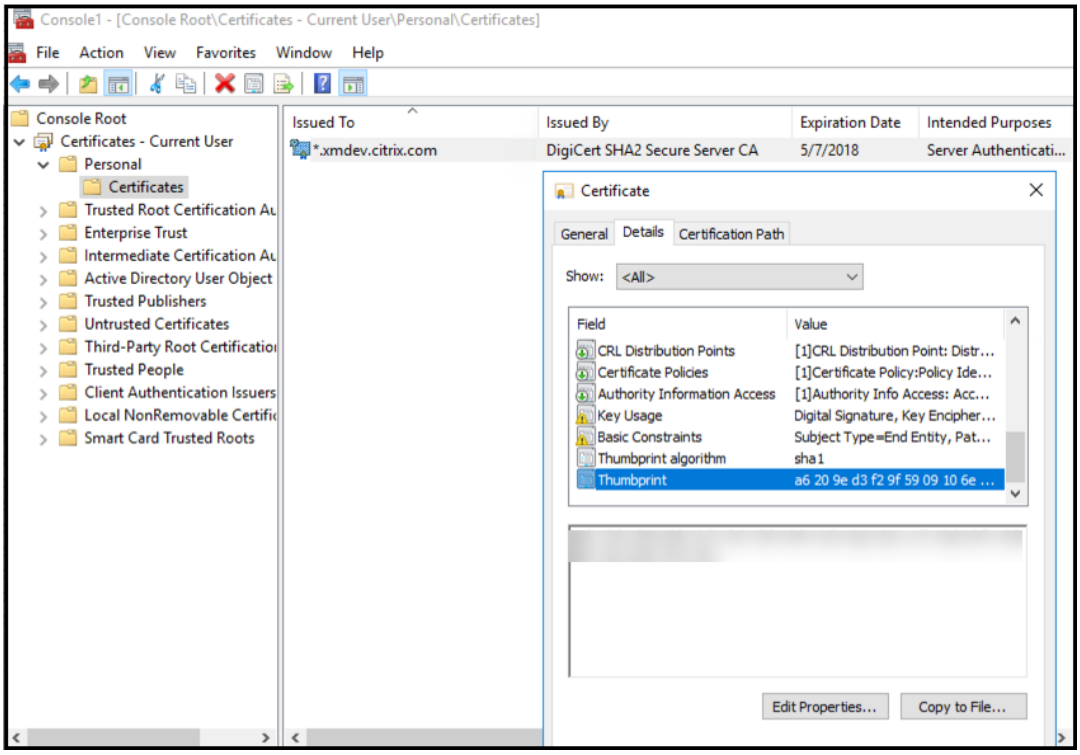


5. Lorsque cette fenêtre s'affiche, cliquez sur **Oui**.

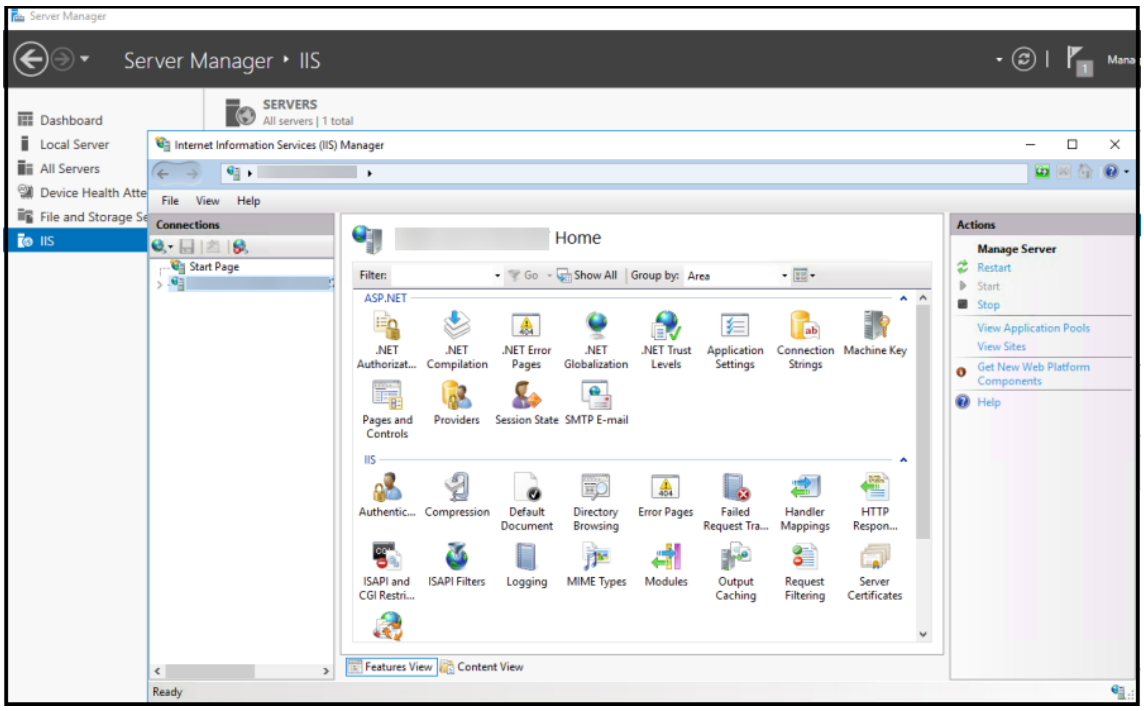


6. Vérifiez que le certificat est installé :
    a) Ouvrez une fenêtre d'invite de commandes.
    b) Tapez **mmc** et appuyez sur la touche Entrée. Pour afficher les certificats dans le magasin de machines local, vous devez être dans le rôle Administrateur.
    c) Dans le menu Fichier, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
    d) Cliquez sur **Ajouter**.
    e) Dans la boîte de dialogue Ajout d'un composant logiciel enfichable autonome, sélectionnez **Certificats**.
    f) Cliquez sur **Ajouter**.
    g) Dans la boîte de dialogue Composant logiciel enfichable Certificats, sélectionnez **Mon compte d'utilisateur.** (Si vous êtes connecté en tant que titulaire de compte de service, sélectionnez **Compte de service**.)

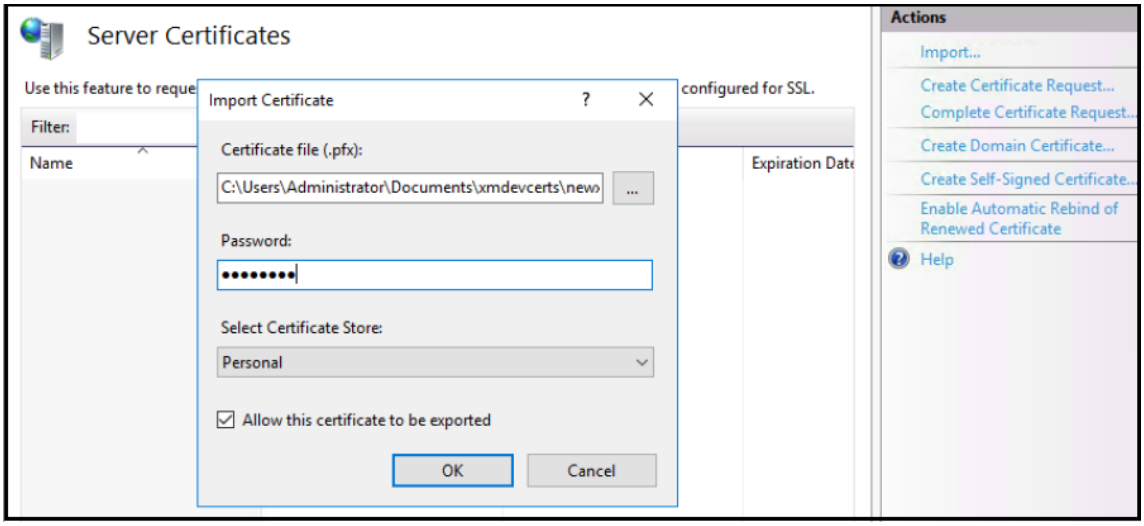
h) Dans la boîte de dialogue Sélectionner un ordinateur, cliquez sur **Terminer**.



7. Accédez à **Gestionnaire de serveur > IIS** et sélectionnez **Certificats de serveur** dans la liste des icônes.

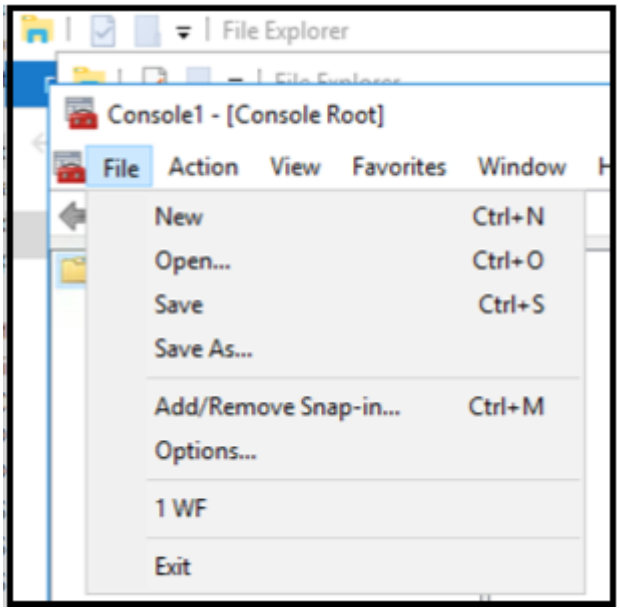


8. À partir du menu Action, sélectionnez **Importer...** pour importer le certificat SSL.

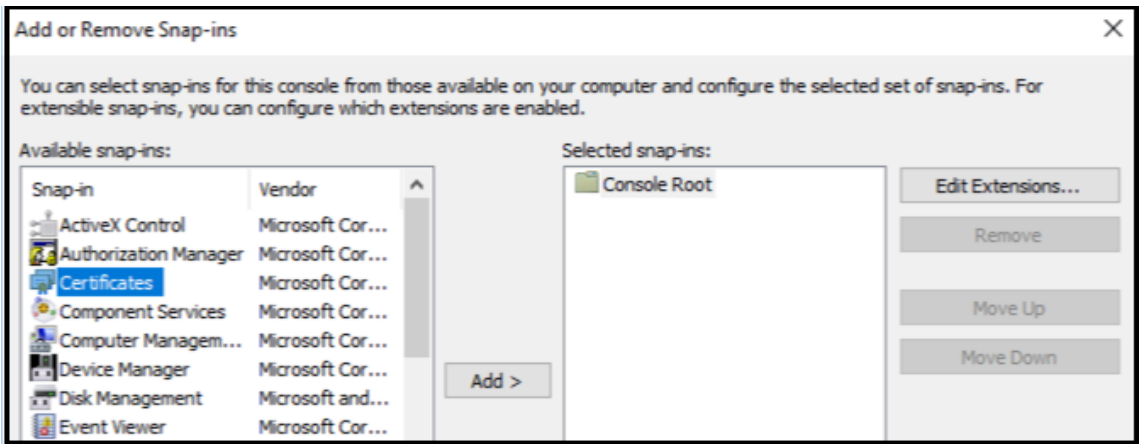


Récupérer et enregistrer l'empreinte numérique du certificat

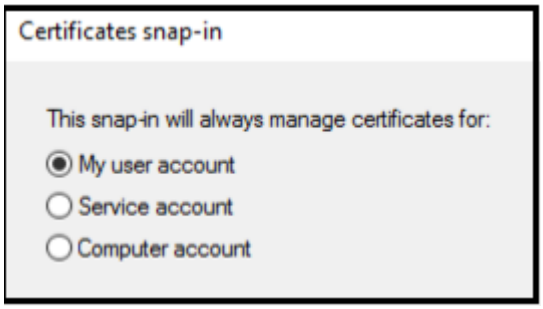
1. Dans la barre de recherche Explorateur de fichiers, tapez **mmc**.
2. Dans la fenêtre Racine de la console, cliquez sur **Fichier > Ajouter/Supprimer un composant logiciel enfichable...**.



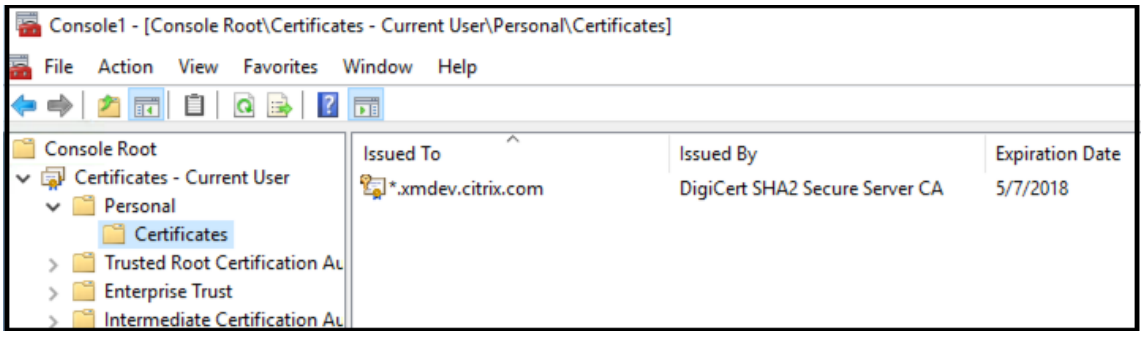
3. Sélectionnez le certificat du composant logiciel enfichable disponible et ajoutez-le aux composants logiciels enfichables sélectionnés.



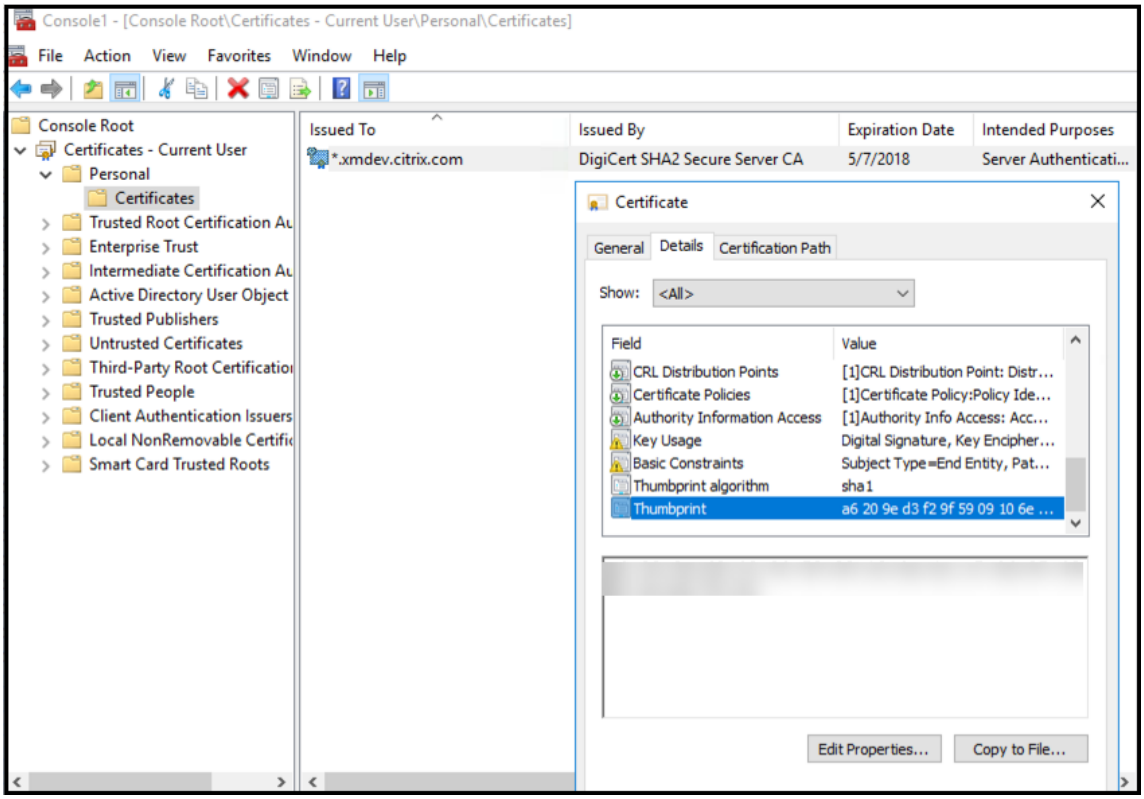
4. Sélectionnez **Mon compte d'utilisateur**.



5. Sélectionnez le certificat et cliquez sur **OK**.



6. Cliquez deux fois sur le certificat, puis sélectionnez l'onglet **Détails**. Faites défiler la liste vers le bas pour afficher l'empreinte numérique du certificat.



7. Copiez l'empreinte numérique dans un fichier. Supprimez les espaces lors de l'utilisation de l'empreinte numérique dans les commandes PowerShell.

Installer les certificats de signature et de cryptage

Exécutez ces commandes PowerShell sur le serveur Windows pour installer les certificats de signature et de cryptage.

Remplacez l'espace réservé ReplaceWithThumbprint et placez-le à l'intérieur des guillemets doubles comme indiqué.

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
 $_.Thumbprint -like "ReplaceWithThumbprint" }


$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName

$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys" +
   $keyname icacls $keypath /grant IIS_IUSRS`:R
<!--NeedCopy-->
```


Extraire le certificat racine du module de plateforme sécurisée (TPM) et installer le package de certificat de confiance

Exécutez ces commandes sur le serveur Windows :

```
mkdir .\TrustedTpm

expand -F:* .\TrustedTpm.cab .\TrustedTpm

cd .\TrustedTpm

.\setup.cmd
<!--NeedCopy-->
```

Configurer le service DHA

Exécutez cette commande sur le serveur Windows pour configurer le service DHA.

Remplacez l'espace réservé ReplaceWithThumbprint.

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
    ReplaceWithThumbprint

-SigningCertificateThumbprint ReplaceWithThumbprint

-SslCertificateStoreName My -SslCertificateThumbprint
    ReplaceWithThumbprint

-SupportedAuthenticationSchema "AikCertificate"
<!--NeedCopy-->
```

Exécutez ces commandes sur le serveur Windows pour configurer la stratégie de chaîne de certificat pour le service DHA :

```
$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
<!--NeedCopy-->
```

Répondez aux invites suivantes :

```
  Confirm

```



```
Are you sure you want to perform this action?

Performing the operation "Install-DeviceHealthAttestation" on
   target "WIN-N27D1FKCEBT".

[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?]
   Help (default is "Y"): A

Adding SSL binding to website 'Default Web Site'.

Add SSL binding?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.

Add application pool?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Adding web application 'DeviceHealthAttestation' to website '
   Default Web Site'.

Add web application?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Adding firewall rule 'Device Health Attestation Service' to allow
   inbound connections on port(s) '443'.

Add firewall rule?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Setting initial configuration for Device Health Attestation Service
   .

Set initial configuration?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Registering User Access Logging.

Register User Access Logging?

```



```
43      [Y] Yes   [N] No   [S] Suspend   [?] Help (default is "Y"): Y
44  <!--NeedCopy-->
```

Vérifier la configuration

Pour vérifier si le certificat DHASActiveSigningCertificate est actif, exécutez cette commande sur le serveur :

```
Get-DHASActiveSigningCertificate
```

Si le certificat est actif, le type de certificat (signature) et l'empreinte numérique sont affichés.

Pour vérifier si le certificat DHASActiveSigningCertificate est actif, exécutez ces commandes sur le serveur

Remplacez l'espace réservé ReplaceWithThumbprint et placez-le à l'intérieur des guillemets doubles comme indiqué.

```
1  Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
       -Force
2
3  Get-DHASActiveEncryptionCertificate
4  <!--NeedCopy-->
```

Si le certificat est actif, l'empreinte numérique est affichée.

Pour effectuer une dernière vérification, accédez à cette URL :

```
https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate
/v1
```

Si le service DHA est en cours d'exécution, le message « Méthode non autorisée » est affiché.

Configuration de l'authentification basée sur certificat pour EWS pour les notifications push de Secure Mail

January 10, 2022

Contribution de Vijay Kumar Kunchakuri

Pour vous assurer que les notifications push de Secure Mail fonctionnent, vous devez configurer Exchange Server pour l'authentification basée sur certificat. Cette exigence est particulièrement nécessaire lorsque Secure Hub est inscrit dans XenMobile avec l'authentification basée sur certificat.

Vous devez configurer le répertoire virtuel Active Sync et Exchange Web Services (EWS) sur le serveur de messagerie Exchange avec l'authentification basée sur certificat.

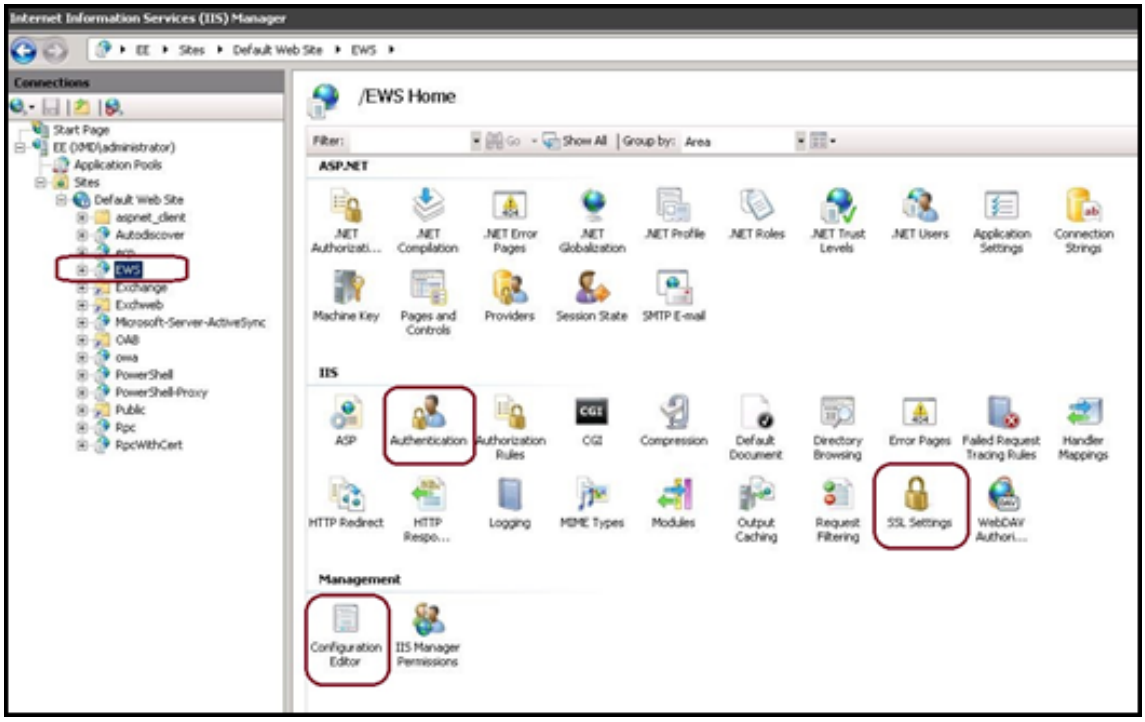
Si vous ne terminez pas ces configurations, l'abonnement aux notifications push de Secure Mail échoue et aucune mise à jour de badge ne se produit dans Secure Mail.

Cet article décrit les étapes pour configurer l'authentification basée sur certificat. Les configurations sont spécifiquement conçues pour le répertoire virtuel EWS sur Exchange Server.

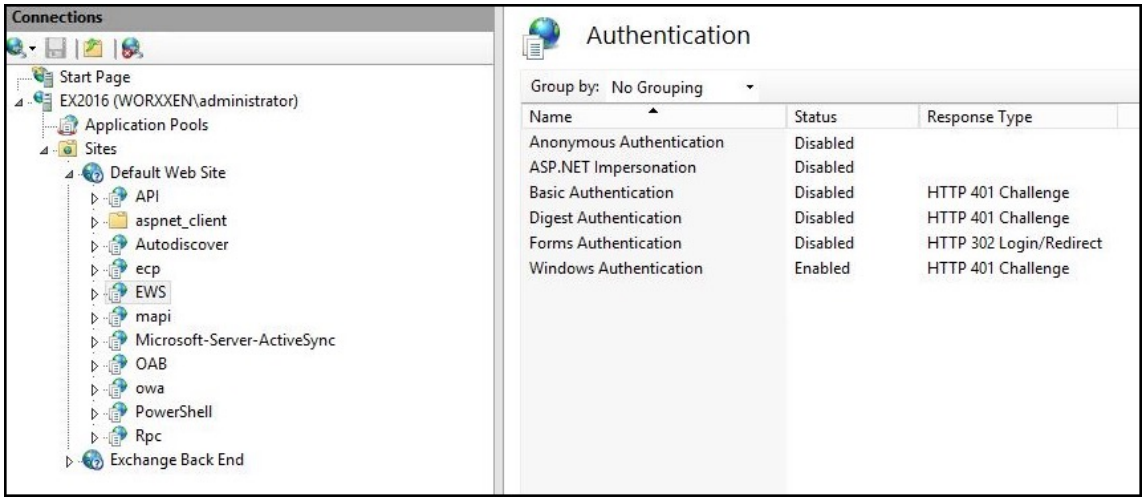
Pour commencer la configuration, procédez comme suit :

1. Connectez-vous au serveur ou aux serveurs sur lesquels le répertoire virtuel EWS est installé.
2. Ouvrez la console du gestionnaire IIS.
3. Sous **Site Web par défaut**, cliquez sur le répertoire virtuel EWS.

   Les composants logiciels enfichables Authentification, SSL et Éditeur de configuration sont situés sur le côté droit de la console du gestionnaire IIS.



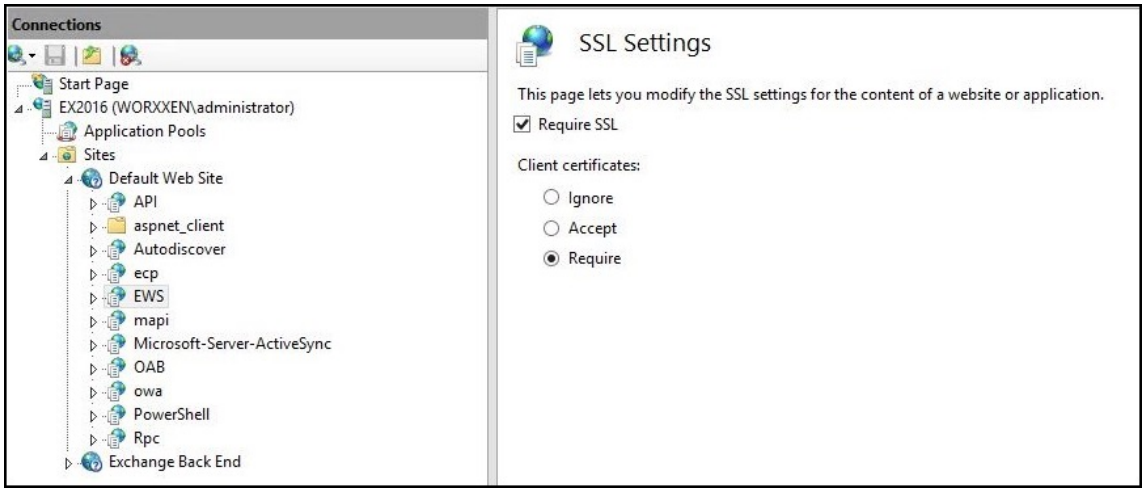
4. Assurez-vous que les paramètres **Authentification** pour EWS sont configurés comme indiqué dans la figure suivante.



5. Configurez **Paramètres SSL** pour le répertoire virtuel EWS.

   a) Sélectionnez la case à cocher **Exiger SSL**.

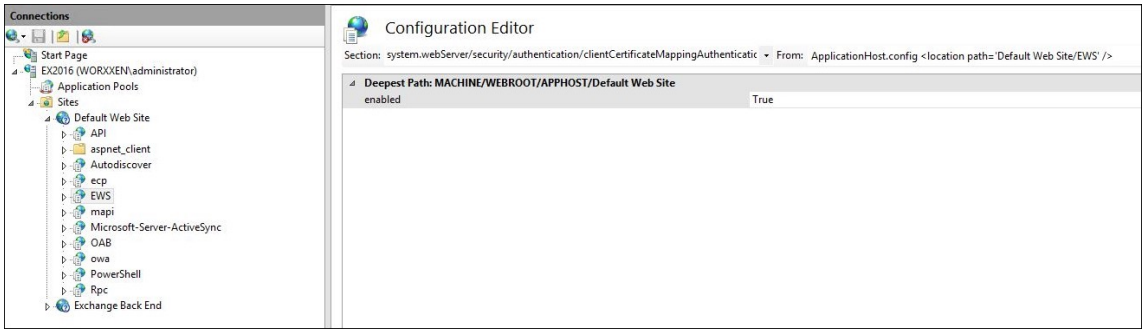
   b) Sous **Certificats clients**, cliquez sur **Exiger**. Vous pouvez définir cette option sur **Accepter** si d'autres clients de messagerie EWS se connectent avec un nom d'utilisateur et un mot de passe comme informations d'identification pour s'authentifier et se connecter au serveur Exchange.



6. Cliquez sur **Éditeur de configuration** et dans la liste déroulante **Section**, accédez à la section suivante :

   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. Définissez la valeur **enabled** sur **True**.

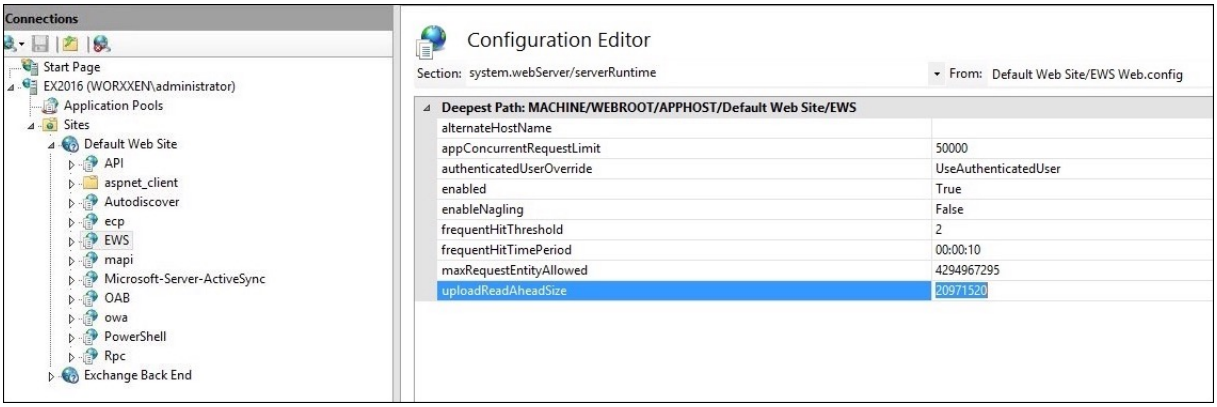


8. Cliquez sur **Éditeur de configuration** et dans la liste déroulante **Section**, accédez à la section suivante :
    - **system.webServer/serverRuntime**
9. Définissez la valeur **uploadReadAheadSize** sur **10485760** (10 Mo) ou **20971520** (20 Mo) ou sur la valeur requise par votre organisation.

> **Important :**
>
> Si vous ne définissez pas cette valeur correctement, l'authentification basée sur certificat lors de l'abonnement aux notifications push EWS peut échouer avec un code d'erreur 413.
>
> Ne définissez pas cette valeur sur **0.**

Pour plus d'informations, consultez les ressources tierces suivantes :

- Moteur d'exécution du serveur Microsoft IIS
- Blog Butsch Client Management



Pour plus d'informations sur le dépannage des problèmes de Secure Mail avec les notifications push iOS, consultez cet article du Centre de connaissances du support Citrix.

Informations connexes

Notifications push pour Secure Mail pour iOS

Intégrer la gestion d'appareils mobiles XenMobile avec Cisco Identity Services Engine (ISE)

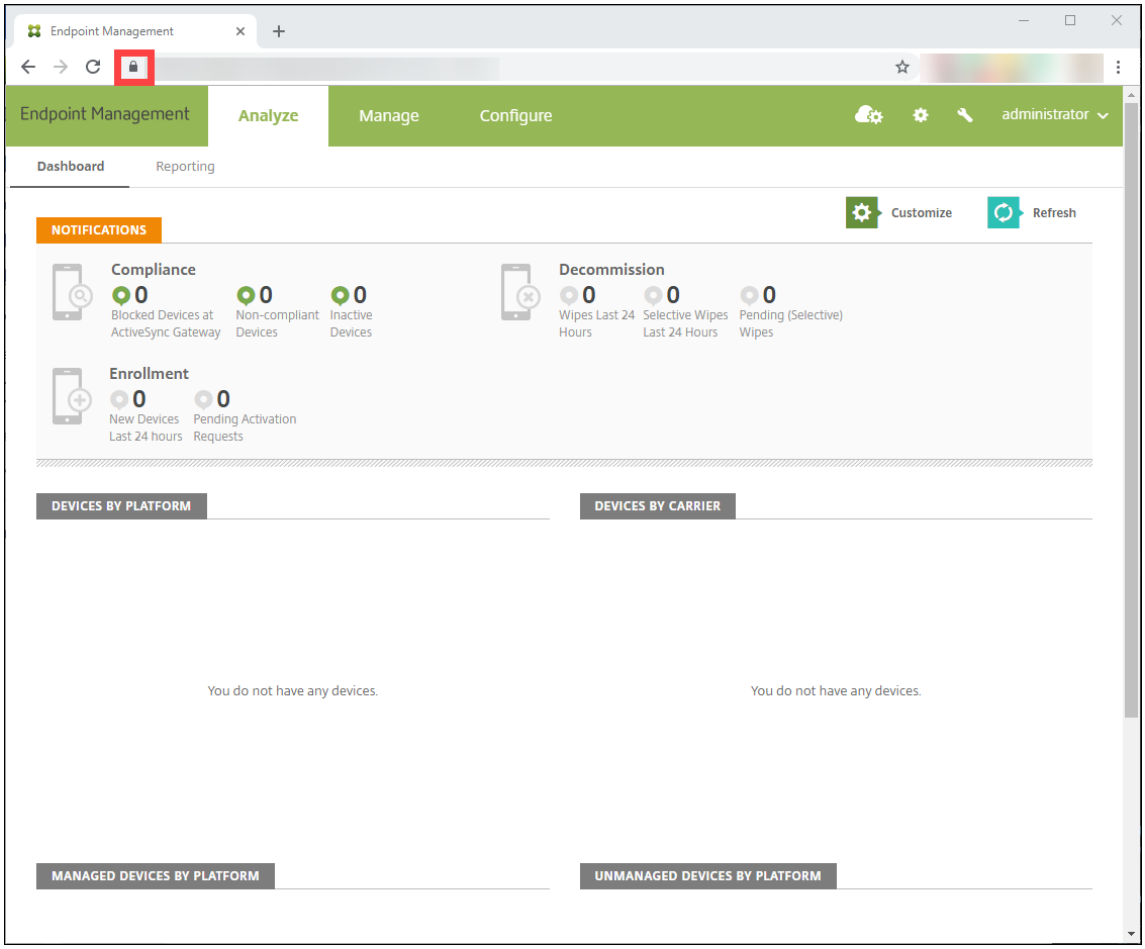
January 10, 2022

Contribution de John Bartel III

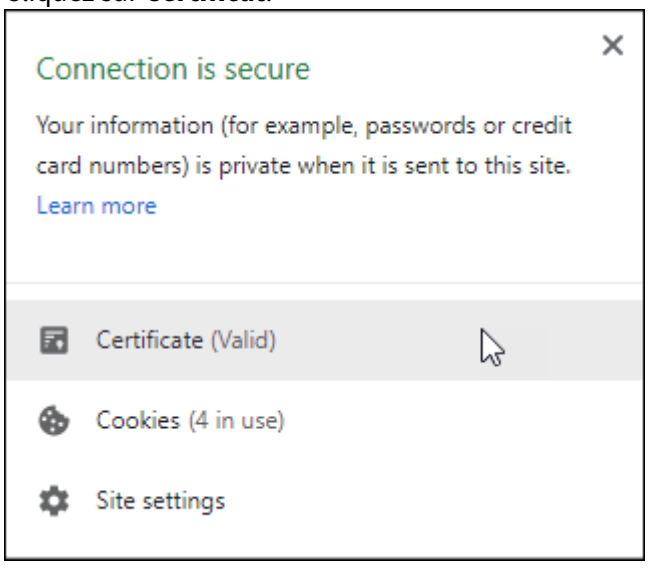
Cisco ISE est utilisé pour déployer, sécuriser, surveiller, intégrer et gérer des appareils mobiles sur le lieu de travail. Le logiciel téléchargé sur l'appareil mobile contrôle la distribution des applications et des correctifs, ainsi que les données et la configuration sur le point de terminaison. XenMobile peut s'intégrer à Cisco ISE pour gérer les appareils non conformes et les appareils non gérés sur la console Cisco ISE. XenMobile vous permet également d'autoriser, de refuser ou de placer en quarantaine l'accès aux services d'entreprise de manière sélective.

Pour configurer l'intégration avec XenMobile, créez un compte de service local sur XenMobile Server avec le rôle d'administrateur RBAC qui lui est attribué. Ce rôle permet à Cisco ISE d'accéder à l'API XenMobile. ISE doit faire confiance au certificat XenMobile. Pour télécharger ce certificat, ouvrez un navigateur Web, accédez à l'adresse URL de votre serveur et connectez-vous.

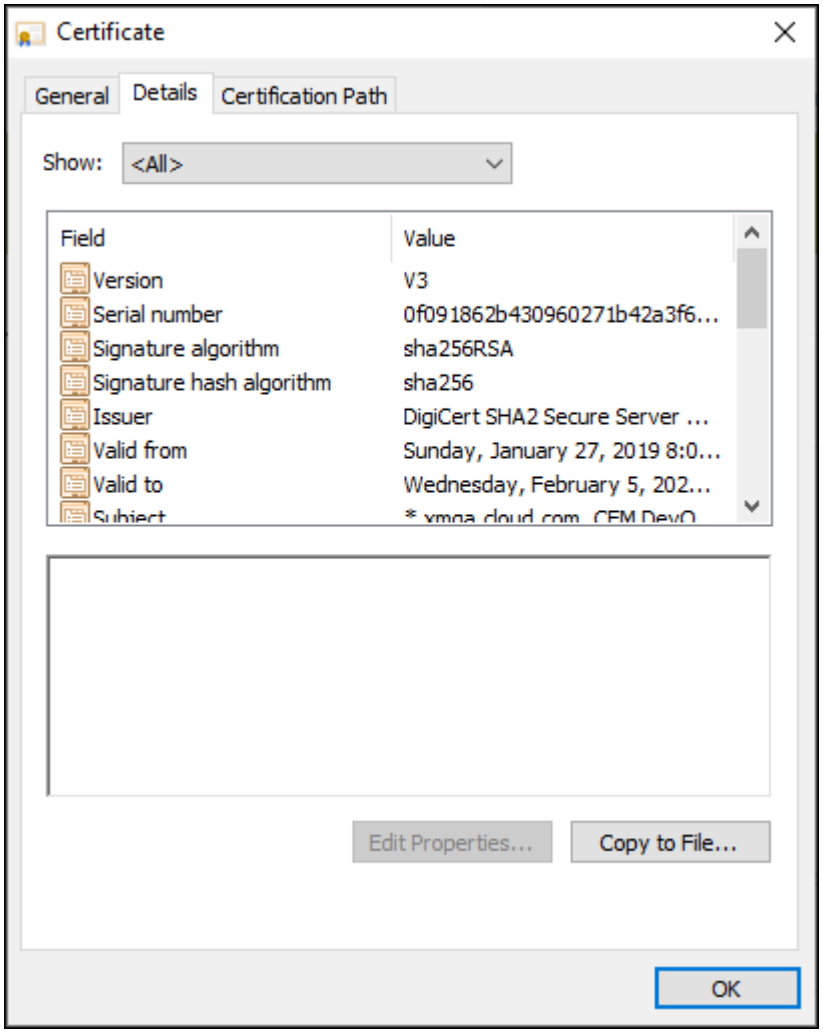
1. Une fois connecté, cliquez sur le verrou en regard de l'adresse URL dans la barre d'adresse.



2. Cliquez sur **Certificat**.



3. Sélectionnez l'onglet **Détails** et cliquez sur **Copier dans un fichier**.



4. Suivez l'assistant pour enregistrer le certificat localement.
5. Connectez-vous à votre console Cisco ISE et importez le certificat XenMobile que vous avez téléchargé précédemment. Importez le certificat dans le magasin de certificats de confiance de Cisco ISE. Cette importation est nécessaire pour que Cisco ISE fasse confiance à la communication avec XenMobile Server.
   a) Accédez à **Administration > System > Certificates > Certificate Management > Trusted Certificates**. Cliquez sur **Importer**.
   b) Donnez un nom au certificat et cochez les cases **Trust for authentication within ISE** et **Trust for authentication of Cisco Services**.
6. Ajoutez XenMobile en tant que gestion d'appareils mobiles externe dans Cisco ISE.
   a) Accédez à **Administration > Network Resource > External MDM**. Cliquez sur **Add** et renseignez les champs suivants :
      - **Server Host :** nom de domaine complet XenMobile
      - **Port :** 443
      - **Instance name :** nom de l'instance de votre serveur XenMobile Server. Le nom de

l'instance est « zdm » par défaut sur la plupart des déploiements.
- **User Name :** nom de l'utilisateur que vous avez créé pour cette tâche. L'utilisateur doit être un compte d'administrateur local dans le groupe d'administrateur RBAC d'origine.
- **Password :** mot de passe de l'utilisateur que vous venez d'ajouter.
- Vérifiez le champ **Enable**.

7. Si le test réussit, cliquez sur **Submit**.

Pour plus d'informations sur Cisco ISE, consultez la documentation de Cisco.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States