À propos du serveur XenMobile 10.3.6

Oct 17, 2016

Vous pouvez effectuer une mise à niveau directe vers XenMobile 10.3.6 Service Pack uniquement depuis XenMobile 10.3.5.

> ## Remarque
>
> Avant de mettre à niveau vers XenMobile 10.3.6, la date Subscription Advantage (SA) de votre licence Citrix doit être à postérieure au 1er juin 2016. Vous pouvez visualiser la date de votre abonnement à SA en regard de la licence dans le serveur de licences. Pour renouveler la date de votre abonnement à SA sur votre licence, téléchargez la dernière version du fichier de licences sur le portail Citrix et chargez le fichier sur le serveur de licences. Consultez l'article http://support.citrix.com/article/CTX209580 pour de plus amples informations.

Pour effectuer la mise à niveau, vous devez utiliser xms_10.3.0.6,310.bin. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Gestion des versions**. Cliquez sur **Mettre à niveau** et chargez ensuite le fichier xms_10.3.6.310.bin. Pour plus d'informations sur la mise à niveau de la console, veuillez consulter la rubrique Mise à niveau de XenMobile.

Pour procéder à une nouvelle installation de XenMobile 10.3.6, consultez la section Installation de XenMobile.

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, consultez le manuel de déploiement de XenMobile.

Nouveautés dans XenMobile 10.3.6

La version 10.3.6 de XenMobile est principalement axée sur la qualité et la capacité à monter en charge. Pour de plus amples informations sur les corrections de bogues, consultez la section Problèmes connus et problèmes résolus dans XenMobile 10.3.6. XenMobile 10.3.6 comprend également les nouvelles fonctionnalités suivantes.

Les améliorations substantielles de qualité apportées au serveur XenMobile 10.3.6 fournissent également une meilleure capacité à monter en charge et de meilleures performances dans les domaines tels que la communication entre le serveur XenMobile et la base de données, l'intégration de XenApp, les notifications de déploiement aux appareils et les recherches LDAP.

- L'énumération HDX s'est améliorée de près de 40 % par rapport à XenMobile 10.3.5.
- Lorsque vous utilisez la commande **Server Tuning** dans le menu principal de ligne de commande de XenMobile (option **5** sous **Advanced Settings**), les valeurs par défaut appliquées pour les paramètres suivants diffèrent comme suit :

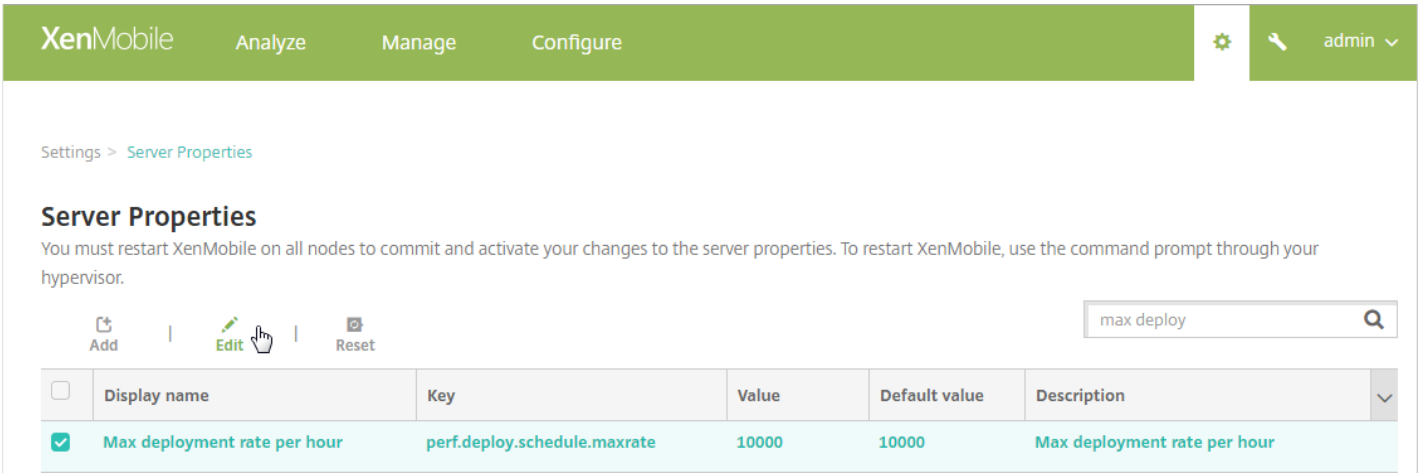
  Maximum connections on port 443: la valeur par défaut est passée de **10 000** à **12 000**.

  Maximum connections on port 8443: la valeur par défaut est passée de **10 000** à **12 000**.

  Maximum threads on port 443: la valeur par défaut est passée de **750** à **2 000**.

Maximum threads on port 8443: la valeur par défaut est passée de **750** à **2 000**.

- XenMobile envoie maintenant des notifications de manière échelonnée pour éviter des pics dans les requêtes de reconnexion d'appareils iOS et Windows Phone, ainsi que d'appareils Android configurés pour Google Cloud Messaging. Le taux de déploiement par défaut est de 10 000 appareils par heure. Pour modifier le taux de déploiement, modifiez la propriété de serveur **Max deployment rate** (perf.deploy.schedule.maxrate).



- Désormais, les déploiements XenMobile ciblent uniquement les appareils qui font partie des groupes de mise à disposition cibles. Précédemment, tous les appareils étaient déployés, quel qu'ait été le rôle.

Worx Home

- **Envoyer des journaux avec WorxMail**. Lorsque les utilisateurs envoient des journaux tout en signalant un problème, WorxMail s'ouvre désormais par défaut. Cela permet aux utilisateurs d'envoyer des fichiers volumineux avec succès. Dans les versions antérieures de Worx Home, l'envoi de fichiers volumineux échouait parfois.

WorxMail

- **Prise en charge d'Exchange Server 2016**. Vous pouvez maintenant intégrer WorxMail avec Exchange Server 2016. Active Sync 14 est pris en charge, mais WorxMail doit également être compatible avec Active Sync 16.
- **Joindre des fichiers depuis ShareFile (Android)**. Les utilisateurs peuvent cliquer sur **Joindre dans ShareFile** pour joindre des fichiers à des e-mails ou des événements de calendrier.
- **Joindre des fichiers depuis des StorageZones restreintes ShareFile et des connecteurs (iOS)**. Lorsque les utilisateurs tapotent sur **Joindre à partir de ShareFile** dans un e-mail ou un événement de calendrier, ils peuvent non seulement joindre des fichiers depuis ShareFile, mais aussi à partir de StorageZones restreintes et de connecteurs, tels que SharePoint et des partages réseau.
- **Partager des données de contact avec des fichiers .vcard**. Les utilisateurs peuvent importer les informations de contact de pièces jointes envoyées en tant que fichiers .vcard.
- **Nouveau paramètre par défaut pour l'accès réseau**. La valeur par défaut de la stratégie **Accès réseau** dans le MDX Toolkit est maintenant **Tunnélisé vers le réseau interne**. Cette modification devrait réduire le nombre d'erreurs de configuration.

WorxWeb

- **Fenêtres contextuelles bloquées par défaut**. Si vous souhaitez que les fenêtres contextuelles pour Safari soient bloquées par défaut, utilisez la console XenMobile pour définir l'option **Bloquer les fenêtres contextuelles** de la stratégie **Restrictions**sur **Activé**. Si vous avez **désactivé Bloquer les fenêtres contextuelles** avant de procéder à la mise à niveau vers la version 10.3.6, le paramètre reste désactivé. Sinon, le paramètre est **activé** et les fenêtres contextuelles sont bloquées dans Safari.
- **Ouvrir des liens dans ShareFile**. ShareFile 4.0 permet aux utilisateurs de choisir d'ouvrir les liens dans un navigateur ou directement dans ShareFile.

Tech Preview WorxChat

- **Prise en charge de Android.** WorxChat est maintenant disponible sur Android.
- **Prise en charge de Lync 2013 et de Skype Entreprise 2015**. Vous pouvez intégrer WorxChat avec Lync 2013 et Skype Entreprise 2015 dans le même pool.

Secure Forms

- **Prise en charge des zones restreintes ShareFile**. Vous pouvez maintenant configurer Secure Forms avec des zones restreintes ShareFile. Suivez les instructions de configuration de la section Intégration de Secure Forms à ShareFile.
- **iBeacon**. À l'aide de la technologie iBeacon, vous pouvez configurer et contrôler les balises qui permettent aux utilisateurs de remplir automatiquement des formulaires sur l'application mobile. Les informations de balise sont incluses lorsque les utilisateurs soumettent des formulaires. Pour de plus amples informations sur la configuration des balises, veuillez consulter la section Balises.
- **Nom du créateur**. Secure Formas Composer affiche maintenant le nom de la personne qui a créé un formulaire. Cette fonctionnalité facilite le suivi lorsque plusieurs utilisateurs accèdent au Composer.
- **Plages de numéros**. Dans le champ **Number** du Composer, vous pouvez spécifier une plage de numéros que les utilisateurs sont autorisés à entrer lorsqu'ils remplissent les formulaires.
- **Nouveau format de nom de fichier.** Les formulaires et les pièces jointes envoyés sur l'application mobile sont désormais enregistrés avec le nom de l'expéditeur et un horodatage, ce qui facile la lecture et l'organisation des noms de fichiers.

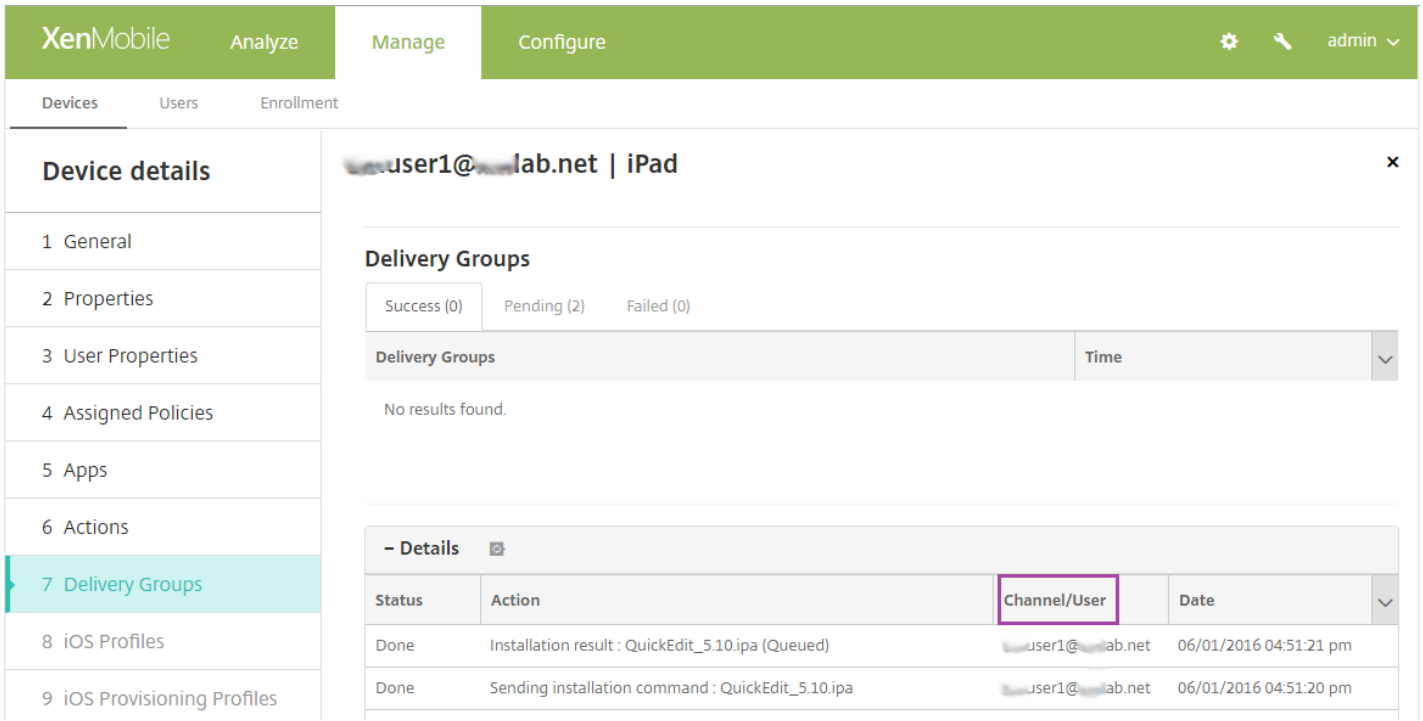
Pour de plus amples informations, consultez la section Nouveautés dans les applications mobiles Worx.

- **Prise en charge de versions de composants Citrix supplémentaires.**
  - NetScaler Gateway 10.5.x, 11.0.x et 11.1.x (XenMobile sur site)
  - NetScaler Gateway 10.5.57.7 (XenMobile Cloud)
  - XenApp et XenDesktop 7.9 et 7.8
  - StoreFront 3.6
  - Serveur de licences 11.13.1.2
- **Réseaux Wi-Fi sur liste blanche.** La stratégie Réseaux Wi-Fi sur liste blanche vous permet de spécifier les réseaux autorisés. Les applications fonctionnent uniquement lorsqu'elles sont connectées à l'un des réseaux figurant dans la liste. Cette fonctionnalité est uniquement disponible en mode MDM+MAM.
- **Prise en charge des appareils partagés dans ShareFile.** L'application mobile ShareFile version 4.4 prend désormais en charge les appareils partagés en mode MDM+MAM, ce qui permet à de multiples utilisateurs de partager un appareil sans avoir à se réinscrire. Pour de plus amples informations, consultez la section Appareils partagés dans XenMobile.
- **Gestion des icônes (iOS).** Les développeurs d'applications peuvent maintenant placer des fichiers d'icônes dans le dossier racine du bundle d'applications, ce qui constitue une solution alternative à la pratique habituelle consistant à les placer dans le fichier info.plist. Pour que le toolkit puisse localiser les fichiers d'icônes, leurs noms doivent être aux formats

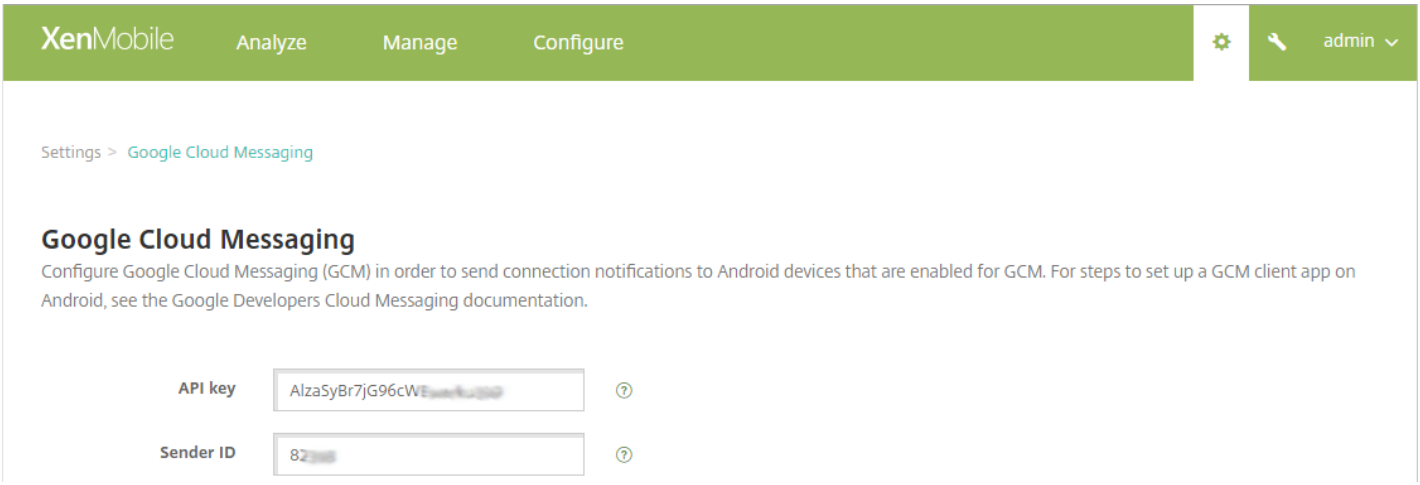
suivants :

- icon.png
- icon-60x2.pn
- icon-72.png
- icon-76.png

- **Synchronisation des messages améliorée (iOS).** Les mises à jour apportées à la synchronisation des messages et à l'intégration avec ShareFile ont rendues la synchronisation plus fiable.
- **Informations supplémentaires sur l'appareil.** La page **Détails de l'appareil** de la console XenMobile comprend maintenant une colonne **Canal/utilisateur** qui indique la cible d'une action de déploiement sur l'appareil. La cible peut afficher l'utilisateur qui a inscrit l'appareil, les utilisateurs connectés à un appareil partagé, les paramètres à l'échelle du système ou les actions de déploiement non associées à un utilisateur spécifique. Vous pouvez utiliser ces informations pour effectuer un meilleur suivi du processus de déploiement, plus particulièrement lorsque de nombreux utilisateurs utilisent une machine ou de nombreux conteneurs sur une plate-forme telle que Mac OS X.

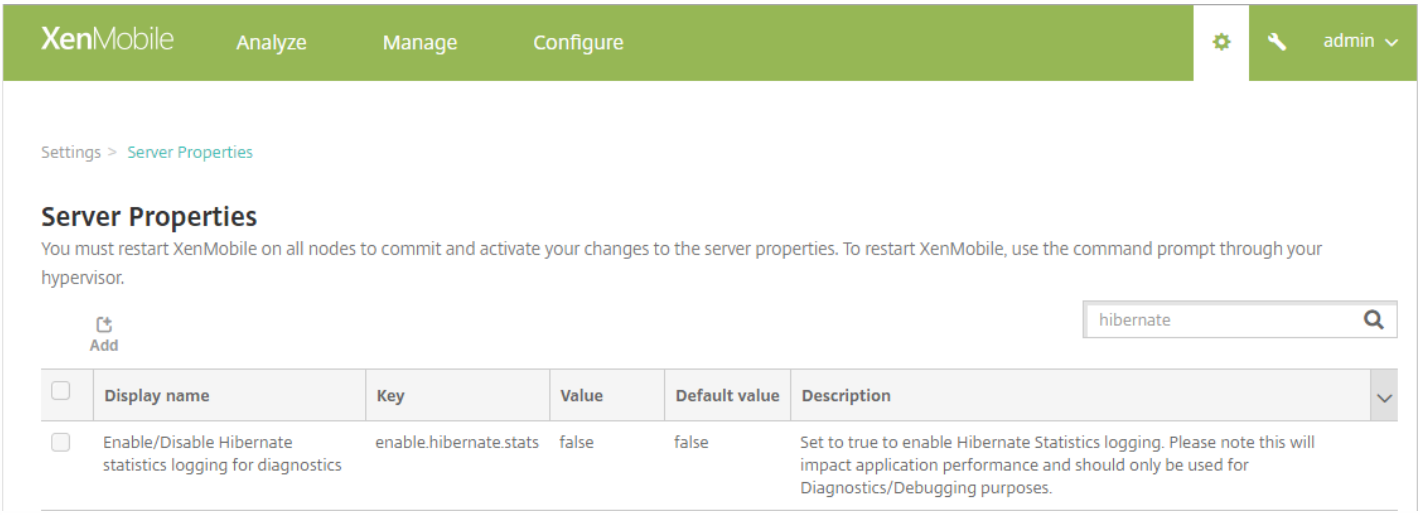


- **Nouvelle page dans la console XenMobile.** La console XenMobile comprend une nouvelle page, **Paramètres > Google Cloud Messaging**, où vous pouvez spécifier la **clé API** et l'**ID d'expéditeur** de votre GCM. Précédemment, ces éléments apparaissaient uniquement dans **Propriétés du serveur**.



- **Enregistrement des statistiques Hibernate à des fins de diagnostic.** Pour faciliter la résolution des problèmes de performances des applications, XenMobile peut maintenant fournir un rapport d'enregistrement des statistiques pour Hibernate, un composant utilisé pour les connexions XenMobile à Microsoft SQL Server.

  Pour activer la journalisation des statistiques Hibernate, modifiez la propriété de serveur **Enable/Disable Hibernate statistics logging for diagnostics** (enable.hibernate.stats) sur **true**. 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.



- **Mises à jour dans l'App Store Android.** L'App Store Android affichera une version mise à jour de l'application uniquement si la version installée sur l'appareil Android est antérieure à la version dans l'App Store.
- **XenMobile Analyzer Tool.** Lorsque vous rencontrez un problème avec votre environnement XenMobile, contacter l'assistance Citrix peut s'avérer couteux en matière de temps et d'argent. Avec XenMobile Analyzer, vous pouvez analyser les problèmes courants par vous-même avant de contacter l'assistance. XenMobile Analyzer Tool prend en charge de nombreux cas d'utilisation et d'options de déploiement, y compris MMDM, MDM+MAM et MAM exclusif, 5 différents scénarios d'authentification et des environnements mobiles iOS et Android.

  XenMobile Analyzer peut effectuer les opérations suivantes :
  - Détecter des problèmes dans votre environnement et recommander des solutions. Les vérifications de l'environnement

effectuées par XenMobile Analyzer peuvent identifier des problèmes au niveau de l'appareil, des problèmes d'inscription des utilisateurs et des problèmes d'authentification.
- Vous guider à travers les étapes requises pour recevoir un diagnostic avancé.
- Vous diriger vers les outils permettant de vérifier la disponibilité de WorxMail (WorxMail Readiness) et de tester la connectivité du serveur (Server Connectivity Checks).
- En dernier ressort, l'outil fournit un lien direct vers l'assistance Citrix.

Pour de plus amples informations, consultez la section XenMobile Analyzer Tool.

- **XenMobile AutoDiscovery Service**. Jusqu'à présent, l'activation de la détection automatique nécessitait la création d'un ticket d'assistance. Avec le portail AutoDiscovery Service, vous pouvez configurer vous-même la détection automatique. Le service vous guide à travers les étapes requises pour revendiquer votre domaine puis pour créer des enregistrements de détection automatique. Pour de plus amples informations, consultez la section XenMobile AutoDiscovery Service.

Problèmes connus et problèmes résolus dans XenMobile 10.3.6

Jul 27, 2016

Les problèmes suivants sont connus ou ont été résolus dans XenMobile 10.3.6 :

Problèmes connus

Lorsque les utilisateurs tentent d'inscrire leurs appareils personnels avec un compte professionnel Microsoft, l'inscription échoue. [#597037]

Lorsque les utilisateurs s'inscrivent auprès de XenMobile via un compte Active Directory Azure, même après effacement ou révocation de l'appareil, ils peuvent s'inscrire à nouveau sans autorisation. Il s'agit d'un problème de tiers. [#628865]

Une fois la mise à jour de XenMobile vers la version 10.3.6, dans une configuration en cluster, l'inscription d'appareils iOS peut échouer. Pour contourner le problème, consultez cet article du centre de connaissances. [#650061]

Problèmes résolus

Les administrateurs XenMobile qui essayent d'accéder à la console XenMobile peuvent être dirigés vers le portail en libre-service de XenMobile. Cela peut se produire lorsque des groupes d'administrateurs XenMobile sont créés avec un contrôle d'accès basé sur un rôle et qu'un groupe est déplacé d'une unité d'organisation Active Directory à une autre. [#585032]

Cette correction garantit que lorsqu'un utilisateur définit la taille du fichier journal et le nombre maximal de fichiers journaux de sauvegarde à conserver, ces valeurs sont correctement configurées dans XenMobile et les fichiers sont substitués correctement. Toutefois, la console XenMobile peut ne pas refléter les valeurs mises à jour comme indiqué dans le problème connu #551199. [#597772]

Dans les éditions XenMobile qui incluent MDM et MAM, il arrive parfois que les appareils iOS ne soient pas complètement inscrits. L'appareil peut être inscrit auprès de MDM, mais pas de MAM, ou vice versa. [#610847]

Lorsque vous configurez une stratégie Exchange ActiveSync pour Windows et que vous définissez l'option **Uniquement lorsque le déploiement précédent a échoué** dans les règles de déploiement, le problème suivant se produit : après modification de l'heure de synchronisation de la messagerie Exchange Server par les utilisateurs Windows Phone, les modifications des utilisateurs sont écrasées la prochaine fois que XenMobile transmet une stratégie Exchange ActiveSync à l'appareil Windows. [#616725]

Si vous recherchez un appareil ou un utilisateur dans la console XenMobile et que la base de données contient une grande quantité de données, l'utilisation de l'UC peut atteindre des pics sur le serveur SQL Server et la recherche peut prendre plus d'une minute. [#618371]

Lorsque les utilisateurs d'appareils iOS s'inscrivent auprès de Worx Home, il peut arriver parfois que Worx Home ne réponde pas pendant deux minutes avant d'inviter les utilisateurs à créer un code PIN Worx. Après l'apparition de ce problème, lorsque les utilisateurs ouvrent WorxStore, Worx Home cesse à nouveau de répondre. [#619945]

Les tentatives d'envoi de notifications SMS depuis le serveur XenMobile sur des appareils exécutant Windows 10 peuvent échouer. [#621229]

Lorsque vous ajoutez un groupe Active Directory enfant à un groupe parent contenant plus de 1500 membres, les actions que vous effectuez dans la console XenMobile, telles que l'attribution de groupes de mise à disposition, ne sont pas appliquées aux utilisateurs dans le groupe enfant ajouté. [#622523]

Après l'inscription d'appareils iOS, les utilisateurs ne sont pas invités à installer les applications requises tant qu'ils n'ouvrent pas le WorxStore ou qu'ils tentent d'ajouter une application manuellement. [#622789]

Les utilisateurs ne peuvent pas s'authentifier auprès de Worx Home après une mise à niveau de XenMobile 9.0 vers XenMobile 10.0, si vous définissez ensuite l'option LDAP « Recherche utilisateur par » sur sAMAccountName puis que vous mettez à niveau vers XenMobile 10.3.x. [#624340]

Le déploiement de stratégies et l'attribution de rôles RBAC peuvent échouer si le nom UPN explicite ne correspond pas au nom UPN implicite de l'utilisateur. [#624612]

Dans les déploiements de serveurs en cluster, des problèmes relatifs aux maps distribuées Hazelcast et à la connectivité au serveur SQL peuvent entraîner l'arrêt du serveur XenMobile, ce qui empêche les connexions et provoque l'échec des inscriptions. [#624931]

Lorsqu'un appareil Android se connecte au serveur XenMobile pour la première fois ou qu'il se reconnecte, les applications Android sont lentes à se télécharger ou leur téléchargement échoue. [#625199]

La liste d'applications ne s'affiche pas pour les utilisateurs Worx Home 10.3 si une application publique contenant le caractère ASCII 16 (caractère d'échappement transmission) dans son nom ou sa description est ajoutée à la console XenMobile. [#627059]

Les serveurs en cluster peuvent cesser de répondre par intermittence si une map distribuée Hazelcast a été implémentée. [#627114]

Après la mise à niveau de deux instances de serveurs vers XenMobile 10.3, après un certain temps d'utilisation, le premier serveur ne répond plus. [#628270]

Une fois qu'ils se sont enregistrés correctement, les appareils iOS peuvent parfois ne pas pouvoir se connecter à WorxStore et ce message s'affiche: « Impossible de récupérer les ressources requises pour continuer. Veuillez réessayer. » Ce problème se produit car le serveur XenMobile ne trouve pas l'appareil par ID d'appareil MAM. [#629900]

Les appareils supprimés de la console XenMobile continuent d'autoriser l'accès aux ressources MAM. [#630137]

Les données d'entreprise des utilisateurs iOS sont parfois effacées. [#630466]

Dans XenMobile 10.3.x, la vue des catégories de Worx Home pouvait parfois ne pas afficher les applications HDX. Le dossier « Autre » qui contenait les applications HDX pouvait ne pas s'afficher dans la vue des catégories dans les versions antérieures de XenMobile. [#631439]

Lorsque les utilisateurs inscrivent un appareil, l'inscription MDM réussit mais il peut arriver parfois que l'enregistrement MAM échoue avec une erreur, et vos applications sont verrouillées. [#632073]

Les applications Android compilées avec Android SDK version 22 ou version ultérieure ou Obfuscated avec Dexguard ne sera pas chargées sur XenMobile. [#632146]

Après que les utilisateurs s'inscrivent auprès de Worx Home, ils sont parfois invités à désinstaller et réinstaller Worx Home. [#633095]

Lorsque vous effacez les données d'entreprise, toutes les données ou que vous supprimez un compte ou appareil dans la console XenMobile, il peut arriver parfois que les licences VPP associées aux applications qui ont été configurées sur l'appareil ne soient pas libérées. [#633366]

Certaines licences VPP ont des ID négatifs, par exemple -123441212, ce qui empêche la distribution des applications publiques. [#631443]

Lorsque les utilisateurs inscrivent un appareil, il peut parfois arriver que Worx Home se bloque avec un message d'erreur 403 indiquant que le magasin d'applications est verrouillé. Parfois, les utilisateurs peuvent s'inscrire avec succès, mais lors du téléchargement d'une application, la même erreur se produit ou une erreur indiquant « Impossible de récupérer les détails ». [#633515]

Lorsque des utilisateurs tentent de configurer une stratégie Wi-Fi avec une clé partagée dans la console XenMobile pour des appareils Windows, après qu'ils modifient le type d'authentification sur WPA Personnel ou WPA-2 Personnel, l'option de clé partagée ne s'affiche pas comme prévu. [#633897]

Si vous disposez d'un NetScaler configuré en tant que proxy de transfert, les vérifications de la connectivité de XenMobile 10.3 renvoient des résultats incorrects. [#633902]

Après la mise à niveau vers XenMobile 10.3.5, les appareils ne sont plus inscrits en mode MAM. En outre, le déploiement de stratégies et d'applications échoue pour les appareils qui sont inscrits en mode MDM+MAM. [#634034]

Dans les éditions de XenMobile qui incluent MDM et MAM, l'authentification MAM peut échouer pour les appareils DEP autorisés lorsque le champ de recherche « utilisateur » est défini sur samAccountName dans les paramètres LDAP. Par conséquent, l'enregistrement Worx Home peut ne pas se terminer et l'appareil peut uniquement être inscrit auprès de MDM. [#637599]

Capacité à monter en charge et performances de XenMobile

Oct 17, 2016

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 fournit les réponses aux questions les plus courantes quant à la configuration requise pour les déploiements à petite et grande échelle.

Les données de cet article offrent des directives permettant de déterminer les performances et la capacité à monter en charge d'une infrastructure XenMobile 10.3.6. Les deux facteurs clés pour déterminer la manière de configurer votre serveur et la base de données sont la capacité à monter en charge (nombre maximal d'utilisateurs/d'appareils) et le taux d'ouverture de session.

- La capacité à monter en charge est définie comme le nombre maximal d'utilisateurs exécutant simultanément une charge de travail déterminée. Pour de plus amples informations sur les flux utilisés pour charger l'infrastructure XenMobile, reportez-vous à la section Charges de travail.
- Le taux d'ouverture de session est défini comme l'intégration de nouveaux utilisateurs et l'authentification des utilisateurs existants.
  - Le taux d'intégration est le nombre maximal d'appareils pouvant être inscrits dans l'environnement pour la première fois. Appelé Première utilisation ou FTU dans cet article, ce point de données est important lors de l'orchestration d'une stratégie de déploiement.
  - Le taux d'utilisateur existant est le nombre maximal d'utilisateurs authentifiés dans l'environnement et qui se sont déjà inscrits et connectés avec leur appareil. Ces tests englobent la création de sessions pour les utilisateurs déjà inscrits et l'exécution des applications WorxMail et WorxWeb.

Le tableau suivant affiche des directives relatives à la capacité à monter en charge basées sur les résultats de test pour l'environnement XenMobile correspondant.

Capacité à monter en charge	Jusqu'à 45 000 appareils	
Taux d'ouverture de session	Intégration (FTU)	Jusqu'à 833 appareils par heure
	Utilisateurs existants	Jusqu'à 2 812 appareils par heure
Configuration	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	Cluster à 6 nœuds du serveur XenMobile
	Base de données	Base de données externe Microsoft SQL Server

> **Important**
>
> Les exigences en matière d'automatisation pour ce rapport sont de 1 000 à 60 000 machines. Toute exigence supérieure à 60 000 machines dépasse le cadre de ce rapport.

Cette section décrit la configuration Active Directory, le nombre de stratégies XenMobile, le nombre et le type d'applications, les actions utilisateur simulées et les actions administrateur simulées du profil test qui a été utilisé pour chaque configuration matérielle ainsi que la charge de travail utilisée pour calculer les résultats du test dans cet article.

> **Remarque**
>
> Ce profil test est conçu pour utiliser plus de ressources que les profils utilisés pour tester la capacité à monter en charge des versions antérieures de XenMobile. Par conséquent, les résultats de ces tests ne sont pas directement comparables aux résultats de capacité à monter en charge des versions antérieures.

Configuration Active Directory (AD) :

- 100 000 utilisateurs AD uniques
- 200 000 groupes AD uniques
- 5 niveaux d'imbrication pour les groupes AD
- 200 utilisateurs par groupe AD

Groupes de mise à disposition :
- 20 groupes de mise à disposition
- 50 applications attribuées aux groupes de mise à disposition
- 10 groupes AD par groupe de mise à disposition

Stratégies XenMobile :
- 300 stratégies
- 20 stratégies par utilisateur

Applications :
- 200 applications natives provenant d'un magasin public
- 50 applications d'entreprise natives distribuées
- 100 applications Web et SaaS
- 50 applications par utilisateur

Actions utilisateur XenMobile :
- Total de 50 actions configurées
- Lancements Worx Store :

- Nouveaux utilisateurs (FTU) : 4
- Utilisateurs déjà enregistrés (RU) : 1

- Lancements d'applications :
  - MDX : 1
  - Web/SaaS : 1
- 150 validations STA par utilisateur

Opérations administrateur XenMobile :

- Énumération des appareils (pour simuler des scénarios d'appel du service d'assistance) : 32 opérations toutes les 8 heures, à raison d'une toutes les 15 à 20 minutes.
- Génération de rapports: 2 fois toutes les 8 heures.

Cette section décrit la configuration matérielle utilisée et les résultats de l'exécution de la charge de travail d'intégration (FTU), ainsi que les tests de capacité à monter en charge pour la charge de travail des utilisateurs existants.

Le tableau suivant définit les recommandations matérielles et de configuration pour XenMobile lors de la montée en charge de 1 000 à 60 000 appareils. Ces directives sont basées sur les résultats des tests et leurs charges de travail associées. Les recommandations tiennent compte de la marge d'erreur acceptable comme défini dans les critères de sortie.

L'analyse des résultats des tests a mené à ces conclusions :

- Le taux d'ouverture de session est un facteur important pour déterminer la capacité à monter en charge d'un système. Outre l'ouverture de session initiale, les taux d'ouverture de session dépendent des valeurs d'expiration de l'authentification configurées dans votre environnement. Par exemple, si vous avez défini une valeur d'expiration de l'authentification trop faible, les utilisateurs doivent exécuter des demandes de connexion plus fréquentes. Par conséquent, vous devez comprendre clairement la manière dont ces valeurs d'expiration affectent votre environnement.
- Le nombre de connexions par session utilisateur sur NetScaler est un facteur important.
- Pour atteindre une montée en charge maximale, les ressources en matière d'UC et de RAM ont été augmentées sur XenMobile.
- La configuration du cluster à 6 nœuds a été la plus grande configuration validée. La montée en charge au-delà de 6 nœuds requiert une implémentation supplémentaire de XenMobile.

Le tableau suivant présente les taux d'ouverture de session recommandés pour les nouveaux clients et les clients existants basés sur la configuration XenMobile, le boîtier NetScaler Gateway, les paramètres de cluster et la base de données. Utilisez les données de ce tableau pour planifier un calendrier d'inscriptions optimal pour les nouveaux déploiements et les taux d'utilisateurs/d'appareils déjà inscrits pour les déploiements existants. La section Configuration associe les données de performances d'inscription et d'ouverture de session aux recommandations matérielles appropriées.

Nombre attendu d'appareils	1 000	10 000	30 000	45 000
Nombre réel d'appareils	1 000	9 998	29 977	44 991
Taux d'ouverture de session				
Intégration (FTU)	250	625	833	833
Utilisateurs existants (Worx uniquement)	1 000	1 666	3 750	883
Configuration				
Environnement de référence	VPX-XenMobile en mode autonome	MPX-XenMobile en mode autonome	MPX-XenMobile en cluster (3)	MPX-XenMobile en cluster (6)
NetScaler Gateway	VPX avec 2 Go de RAM Deux processeurs virtuels	MPX-10500	MPX-11500	MPX-11500
XenMobile - mode	Autonome*	Autonome*	Cluster	Cluster
XenMobile - cluster	S.O.	S.O.	3	6
XenMobile - boîtier virtuel	8 Go de RAM et 4 processeurs virtuels	8 Go de RAM et 4 processeurs virtuels	16 Go de RAM et 6 processeurs virtuels	16 Go de RAM et 8 processeurs virtuels
Active Directory (AD)	8 Go de RAM et 4 processeurs virtuels	8 Go de RAM et 4 processeurs virtuels	16 Go de RAM et 4 processeurs virtuels	16 Go de RM et 4 processeurs virtuels
Base de données	Externe	Externe – Microsoft SQL Server Mémoire = 16 Go Processeurs virtuels = 12	Externe – Microsoft SQL Server Mémoire = 32 Go Processeurs virtuels = 12	Externe – Microsoft SQL Server Mémoire = 48 Go Processeurs virtuels = 16

MPX-XenMobile en cluster (3)

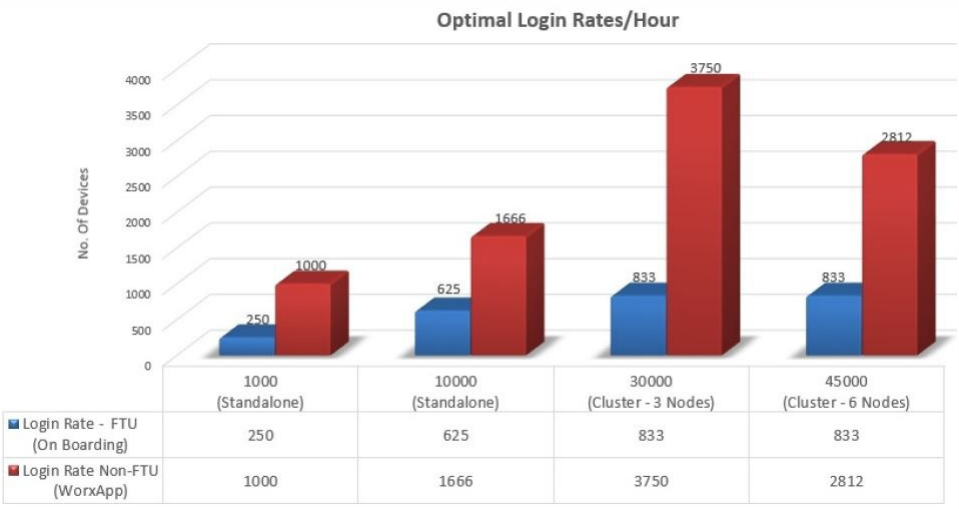
Cluster
Cluster
Cluster
Cluster
8 Go de RAM et 4 processeurs virtuels
8 Go de RAM et 4 processeurs virtuels

* Les déploiements autonomes ne sont pas recommandés pour les applications qui exigent une haute disponibilité. Citrix recommande des déploiements en cluster à haute disponibilité pour la plupart des clients.

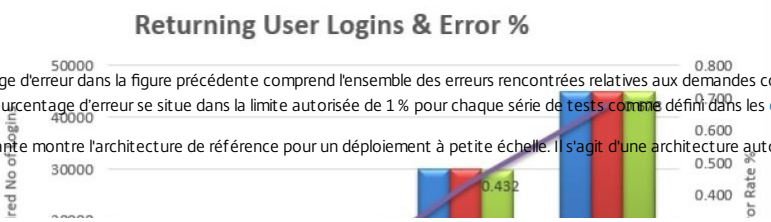
Remarque : vous allez rencontrer les situations suivantes si vous dépassez les recommandations en termes de taux ou de matériel lors du dimensionnement de votre système.

Les informations suivantes fournissent des points de données supplémentaires qui ont été enregistrés et qui affectent les résultats dans le tableau précédent.

- Latence d'inscription ou d'ouverture de session (durée aller-retour)
  - Latence moyenne totale : 0,5 à 1,5 secondes
  - Latence moyenne pour une ouverture de session NetScaler Gateway : >120 à 440 ms
  - Latence moyenne pour une demande Worx Store : 2 à 3 secondes
- Une détérioration de la performance physique, telle qu'une insuffisance des ressources d'UC et de mémoire, a été observée sur les composants de l'infrastructure lorsque les limites de la montée en charge ont été atteintes.
  - Réponses non valides sur les boîtiers NetScaler Gateway et XenMobile.
  - Réponse lente de la console XenMobile lors des périodes pendant lesquelles les charges sont élevées.

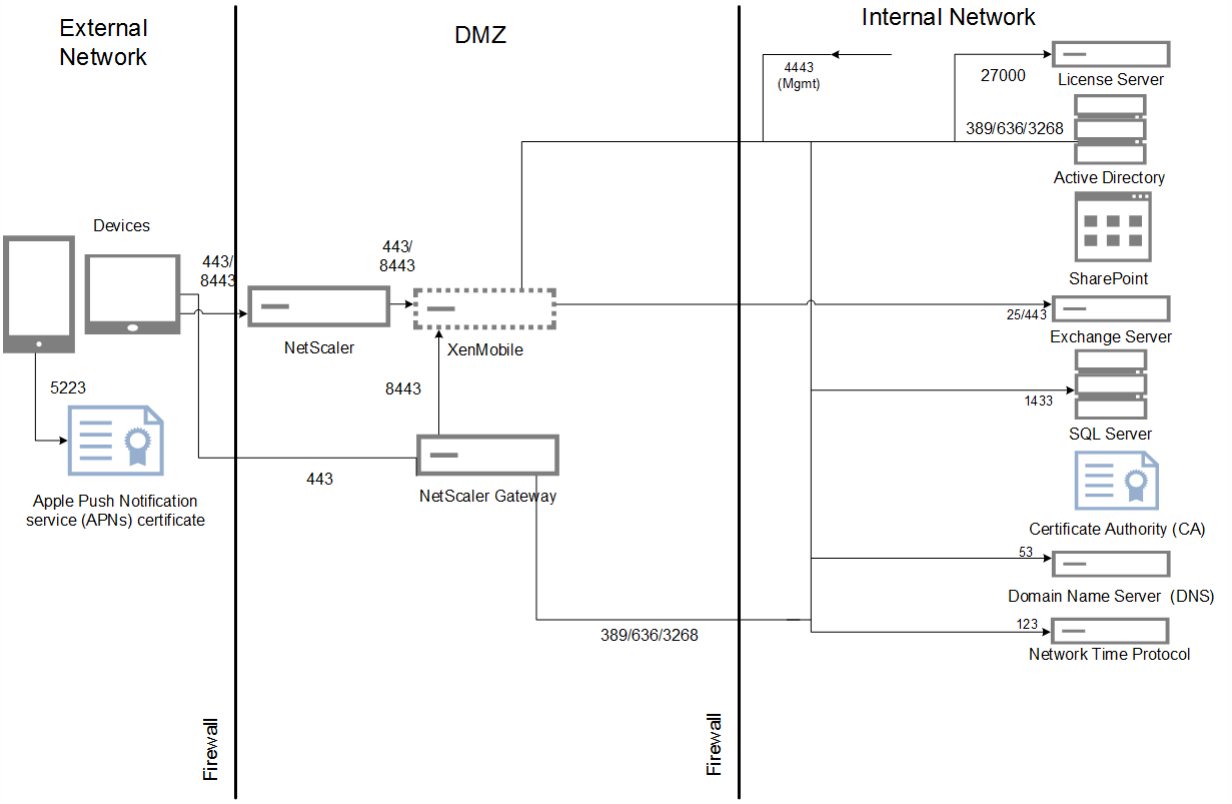


	1000 (Standalone)	10000 (Standalone)	30000 (Cluster - 3 Nodes)	45000 (Cluster - 6 Nodes)
Login Rate - FTU (On Boarding)	250	625	833	833
Login Rate Non-FTU (WorxApp)	1000	1666	3750	2812

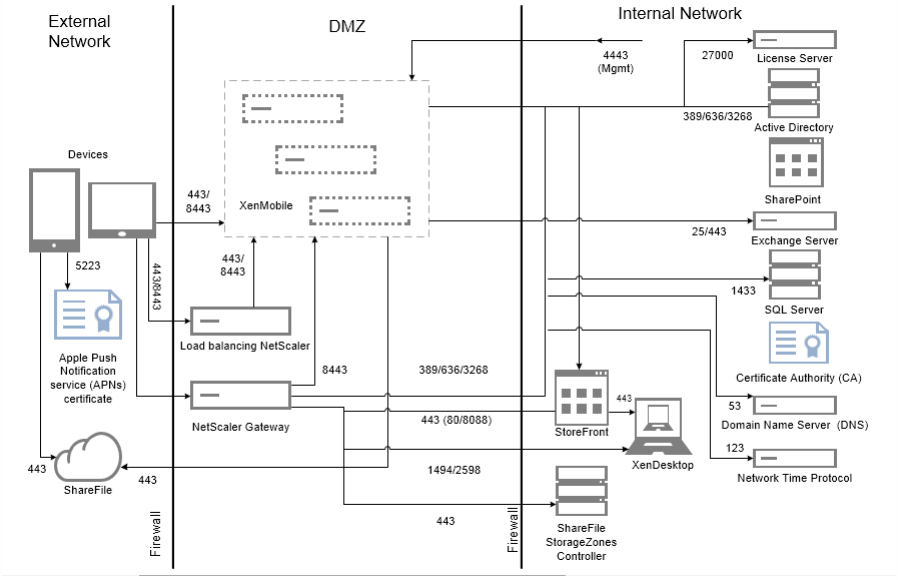


Le pourcentage d'erreur dans la figure précédente comprend l'ensemble des erreurs rencontrées relatives aux demandes correspondant à chaque opération et n'est pas limité aux ouvertures de session. Le pourcentage d'erreur se situe dans la limite autorisée de 1 % pour chaque série de tests comme défini dans les critères de sortie.

La figure suivante montre l'architecture de référence pour un déploiement à petite échelle. Il s'agit d'une architecture autonome qui prend en charge jusqu'à 10 000 appareils.



La figure suivante montre l'architecture de référence pour un déploiement d'entreprise. Il s'agit d'une architecture en cluster avec déchargement SSL pour MAM sur HTTP qui prend en charge 10 000 appareils ou plus.



Les tests ont été exécutés sur XenMobile Enterprise pour établir un banc d'essai. En vue de cibler les déploiements à petite et à grande échelle, 1 000 à 60 0000 appareils ont été utilisés pour les mesures.

Des charges de travail ont été créées pour simuler des cas d'utilisation réels. Ces charges de travail ont été exécutées pour chaque test afin d'étudier les effets sur l'inscription et les taux d'ouverture de session. L'objectif de ces tests était d'obtenir un taux d'ouverture de session optimal compris dans la marge d'erreur autorisée, comme détaillé dans les critères de sortie. Les taux d'ouverture de session sont un facteur critique pour déterminer la configuration matérielle recommandée pour les composants d'infrastructure.

Les demandes d'ouverture de session des charges de travail intégrées (FTU) comprenaient les opérations de détection automatique, d'authentification et d'enregistrement des appareils. Les abonnements aux applications, ainsi que les opérations d'installation et de démarrage ont été réparties de manière uniforme au cours de la période de test, ce qui a réuni les meilleures conditions pour une simulation réelle des actions de l'utilisateur. Au terme du test, la session a été fermée. Les demandes d'ouverture de session pour la charge de travail des utilisateurs existants comprenaient uniquement des demandes d'authentification.

Les charges de travail des utilisateurs sont définies comme suit :

Sessions utilisateur et appareils	Inclut les ouvertures de session NetScaler Gateway, les énumérations, l'enregistrement des appareils, et ainsi de suite pour chaque session.
Worx Store démarre	Les utilisateurs lancent Worx Store à plusieurs reprises et chaque fois qu'ils s'abonnent à une ou à plusieurs applications, ou qu'ils les installent, qu'il s'agisse d'applications mobiles (Web/SaaS/MDX) ou Windows (HDX).
Authentification unique des applications Web ou SaaS par appareil	Permet de lancer une séquence d'applications Web/SaaS jusqu'à ce que XenMobile exécute l'authentification unique et renvoie l'URL de l'application réelle. Le trafic n'a pas été envoyé aux applications réelles.
Téléchargements d'applications MDX par appareil	Compte le nombre de téléchargements d'applications MDX (peut se produire sur les lancements Worx Store). Pour iOS, cela comprend également l'automatisation de l'installation d'applications depuis Apple ITMS, qui utilise les nouvelles API du service de jeton/tms sur NetScaler Gateway.

Notes et hypothèses

Les scénarios suivants ne sont pas couverts dans le cadre des tests de capacité à monter en charge. Ces scénarios seront pris en compte pour l'amélioration des tests :

- Le déploiement de paquetage n'est pas testé.
- La plate-forme Windows n'est pas testée.

La transmission de stratégies a été testée sur les appareils iOS et Android.
Chaque XenMobile prend en charge un maximum de 10 000 connexions simultanées.

Les tests ont été exécutés dans des conditions idéales sur un réseau local pour ignorer les problèmes de latence réseau. Dans un environnement réel, la capacité à monter en charge dépend également de la bande passante disponible, plus particulièrement pour les téléchargements d'applications.

Tests de reconnexion

Les tests de reconnexion ont été effectués séparément des tests des scénarios First Time Use (première utilisation) et Returning User (utilisateur déjà enregistré).

Les tests de reconnexion ont été exécutés pour un maximum de 15 000 appareils.

Le taux de reconnexion pris en charge pour Android est de 17 appareils par seconde. Le taux de reconnexion pour iOS est de 8 appareils par seconde. Afin d'atteindre ce nombre, le compteur maxThread a été défini sur 1000 dans le fichier /opt/sas/tomcat/conf/server.xml.

INFORMATIONS SUR LES STRATÉGIES DE RECONNEXION RECOMMANDÉES

Charge de travail intégrée (FTU)
La charge de travail intégrée (FTU) est définie comme la première fois qu'un utilisateur accède à l'environnement XenMobile. Les opérations comprises dans cette charge de travail étaient les suivantes :

- Découverte automatique
- Inscription
- Authentification
- Enregistrement de l'appareil
- Mise à disposition d'applications (Web, SaaS et mobiles MDX)
  - Abonnement aux applications (y compris les téléchargements d'images et d'icônes)
  - Installation des applications MDX souscrites
- Lancement des applications (Web, SaaS et mobiles MDX) y compris vérification de l'état des appareils
- Transmission de stratégies (pour iOS)
- Nombre minimal de connexions WorxMail et WorxWeb (tunnels VPN) : deux connexions
- Installation des applications requises via XenMobile

Les paramètres de charge de travail sont définis dans le tableau suivant :

Appareils	Enregistrements d'appareils	Énumérations	Applications énumérées par appareil	Lancements WorxStore par appareil	Authentification unique des applications Web ou SaaS par appareil	Téléchargements d'applications MDX par appareil	Téléchargements d'applications obligatoires déclenchés par le serveur XenMobile	Stratégies déployées par appareil (iOS)
1000	1000	1000	50	4	40	10	2	20
10 000	10 000	10 000	50	4	40	10	2	20

30 000	30 000	30 000	50	4	40	10	2	20
60000	60000	60000	50	4	40	10	2	20

Charge des utilisateurs existants qui utilisent uniquement des connexions Worx

Le tableau suivant affiche la charge des utilisateurs existants (avec des connexions Worx uniquement). Cette charge de travail simulait un utilisateur utilisant les applications WorxMail et WorxWeb. Cette simulation a été utilisée pour mesurer la capacité à monter en charge de NetScaler Gateway dans la configuration XenMobile. Ceci est réalisable car en utilisant uniquement ces deux applications Worx, la charge réseau est minimale. Pour l'application WorxWeb, l'utilisateur accède à des sites Web internes qui ne déclenchent pas l'authentification unique (SSO) au serveur XenMobile. Les opérations dans ce mode étaient les suivantes :

- Authentification (NetScaler Gateway et XenMobile)
- Nombre de connexions WorxMail et WorxWeb (tunnels VPN) : quatre connexions

Le tableau suivant présente les paramètres de charge de travail pour les utilisateurs existants.

Appareils	Énumérations	Applications énumérées par appareil	Tunnels VPN par appareil[1]
1000	1000	50	3
10 000	10 000	50	3
30 000	30 000	50	3
60000	60000	50	3

1. Le nombre de tunnels VPN correspond aux connexions WorxMail et WorxWeb.

Les profils de connexion pour WorxMail et WorxWeb sont décrits dans le tableau suivant :

Connexion d'appareils	Type de connexion	Données envoyées par session[1]	Données reçues par session[1]
Connexion WorxMail n° 1	Type 1[2]	4,1 Mo	4,1 Mo
Connexion WorxMail n° 2	Type 1	6,3 Mo	12,5 Mo
Connexion WorxWeb n° 1	Type 2[3]	5,2 Mo	15,7 Mo
Connexion WorxWeb n° 2	Type 2	4,1 Mo	3,4 Mo
Nombre total d'octets transférés par session[1]		~ 19,7 Mo	~ 40,7 Mo

1. Par session : 8 heures.

2. Type 1 : envoi et réception asymétriques avec des connexions à long terme (WorxMail avec une connexion à une boîte aux lettres Microsoft Exchange dédiée).

3. Type 2 : envoi et réception asymétriques avec des connexions qui se ferment et s'ouvrent de nouveau après un certain délai (connexions WorxWeb).

Ces recommandations sont basées sur les profils WorxMail et WorxWeb utilisés pour automatiser
une charge « moyenne ». Les modifications apportées aux détails de connexion affectent les résultats de l'analyse. Par exemple, si le nombre de connexions par utilisateur est augmenté, le nombre de sessions de NetScaler Gateway prises en charge peut être réduit.

Profils WorxMail et WorxWeb

Les profils utilisés pour chaque application sont conçus pour automatiser une charge « très importante ». Les tableaux suivants affichent les détails des profils de WorxMail et WorxWeb.

Profil WorxMail pour une charge de travail moyenne

Messages envoyés par jour	20
Messages reçus par jour	80
Messages lus par jour	80
Messages supprimés par jour	20
Taille moyenne des messages (Ko)	200

Profil WorxWeb pour charge de travail moyenne

Nombre d'applications Web lancées	10
Nombre de pages Web ouvertes manuellement	10
Nombre moyen de paires demande–réponse par application Web	100
Taille moyenne de la demande (octets)	300
Taille moyenne de la réponse (octets)	1000

Configuration et paramètres

Les configurations suivantes ont été utilisées lors de l'exécution des tests de capacité à monter en charge :

- Les serveurs virtuels de NetScaler Gateway et d'équilibrage de charge coexistaient sur le même boîtier NetScaler Gateway.
- Délai d'expiration de la session NetScaler configuré sur 60 minutes.
- Une clé de 2 048 bits a été utilisée sur NetScaler Gateway pour les transactions SSL.

Les taux d'ouverture de session constituent la base de cette analyse. Ils servent de ligne directive pour les composants d'infrastructure et leur configuration respective. Il est important de noter que les taux d'ouverture de session prennent en compte une marge d'erreur qui se compose des éléments suivants :

- Réponses non valides
  - Une réponse avec le code d'état 401/404 à la place de 200 est considérée comme non valide.
- Délais d'expiration des demandes
  - Une réponse est attendue dans les 120 secondes.
- Erreurs de connexion
  - Une réinitialisation de la connexion s'est produite.
  - Un arrêt brutal de connexion s'est produit.

Le taux d'ouverture de session est acceptable si le taux d'erreur global est inférieur à 1 % du nombre total de demandes envoyées à partir d'un appareil donné. Le taux d'erreur inclut les erreurs correspondant à chaque opération de charge de travail individuelle, ainsi que la performance physique du composant d'infrastructure, comme l'insuffisance des ressources d'UC et de mémoire.

Le tableau suivant dresse la liste des logiciels d'infrastructure XenMobile utilisés pour ces tests.

Composant	Version
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0.824
Base de données externe	Microsoft SQL Server 2014

Les tests de capacité à monter en charge ont été exécutés sur une plate-forme XenServer comme décrit dans le tableau suivant.

Fournisseur	Genuine Intel
Modèle	UC Intel Xeon — E5645 @ 2,40 GHz (nombre d'UC = 24)

Cela comprend les services de base d'infrastructure (par exemple, Active Directory, Windows Domain Name Service (DNS), autorité de certification, Microsoft Exchange, etc.), ainsi que les composants XenMobile (boîtier virtuel XenMobile et boîtier virtuel NetScaler Gateway VPX, le cas échéant).

Capacité à monter en charge et performances de XenMobile

Jul 27, 2016

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 fournit les réponses aux questions les plus courantes quant à la configuration requise pour les déploiements à petite et grande échelle.

Les données de cet article offrent des directives permettant de déterminer les performances et la capacité à monter en charge d'une infrastructure XenMobile 10.3.6. Les deux facteurs clés pour déterminer la manière de configurer votre serveur et la base de données sont la capacité à monter en charge (nombre maximal d'utilisateurs/d'appareils) et le taux d'ouverture de session.

- La capacité à monter en charge est définie comme le nombre maximal d'utilisateurs exécutant simultanément une charge de travail déterminée. Pour de plus amples informations sur les flux utilisés pour charger l'infrastructure XenMobile, reportez-vous à la section Charges de travail.
- Le taux d'ouverture de session est défini comme l'intégration de nouveaux utilisateurs et l'authentification des utilisateurs existants.
  - Le taux d'intégration est le nombre maximal d'appareils pouvant être inscrits dans l'environnement pour la première fois. Appelé Première utilisation ou FTU dans cet article, ce point de données est important lors de l'orchestration d'une stratégie de déploiement.
  - Le taux d'utilisateur existant est le nombre maximal d'utilisateurs authentifiés dans l'environnement et qui se sont déjà inscrits et connectés avec leur appareil. Ces tests englobent la création de sessions pour les utilisateurs déjà inscrits et l'exécution des applications WorxMail et WorxWeb.

Le tableau suivant affiche des directives relatives à la capacité à monter en charge basées sur les résultats de test pour l'environnement XenMobile correspondant.

Capacité à monter en charge	Jusqu'à 45 000 appareils	
Taux d'ouverture de session	Intégration (FTU)	Jusqu'à 833 appareils par heure
	Utilisateurs existants	Jusqu'à 2 812 appareils par heure
Configuration	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	Cluster à 6 nœuds du serveur XenMobile
	Base de données	Base de données externe Microsoft SQL Server

> **Important**
>
> Les exigences en matière d'automatisation pour ce rapport sont de 1 000 à 60 000 machines. Toute exigence supérieure à 60 000 machines dépasse le cadre de ce rapport.

Cette section décrit la configuration Active Directory, le nombre de stratégies XenMobile, le nombre et le type d'applications, les actions utilisateur simulées et les actions administrateur simulées du profil test qui a été utilisé pour chaque configuration matérielle ainsi que la charge de travail utilisée pour calculer les résultats du test dans cet article.

> **Remarque**
>
> Ce profil test est conçu pour utiliser plus de ressources que les profils utilisés pour tester la capacité à monter en charge des versions antérieures de XenMobile. Par conséquent, les résultats de ces tests ne sont pas directement comparables aux résultats de capacité à monter en charge des versions antérieures.

Configuration Active Directory (AD) :

- 100 000 utilisateurs AD uniques
- 200 000 groupes AD uniques
- 5 niveaux d'imbrication pour les groupes AD
- 200 utilisateurs par groupe AD

Groupes de mise à disposition :
- 20 groupes de mise à disposition
- 50 applications attribuées aux groupes de mise à disposition
- 10 groupes AD par groupe de mise à disposition

Stratégies XenMobile :
- 300 stratégies
- 20 stratégies par utilisateur

Applications :
- 200 applications natives provenant d'un magasin public
- 50 applications de distribution d'entreprise natives
- 100 applications Web et SaaS
- 50 applications par utilisateur

Actions utilisateur XenMobile :
- Total de 50 actions configurées
- Lancements Worx Store :

- Nouveaux utilisateurs (FTU) : 4
- Utilisateurs déjà enregistrés (RU) : 1

- Lancements d'applications :
  - MDX : 1
  - Web/SaaS : 1
- 150 validations STA par utilisateur

Opérations administrateur XenMobile :

- Énumération des appareils (pour simuler des scénarios d'appel du service d'assistance) : 32 opérations toutes les 8 heures, à raison d'une toutes les 15 à 20 minutes.
- Génération de rapports: 2 fois toutes les 8 heures.

Cette section décrit la configuration matérielle utilisée et les résultats de l'exécution de la charge de travail d'intégration (FTU), ainsi que les tests de capacité à monter en charge pour la charge de travail des utilisateurs existants.

Le tableau suivant définit les recommandations matérielles et de configuration pour XenMobile lors de la montée en charge de 1 000 à 60 000 appareils. Ces directives sont basées sur les résultats des tests et leurs charges de travail associées. Les recommandations tiennent compte de la marge d'erreur acceptable comme défini dans les critères de sortie.

L'analyse des résultats des tests a mené à ces conclusions :

- Le taux d'ouverture de session est un facteur important pour déterminer la capacité à monter en charge d'un système. Outre l'ouverture de session initiale, les taux d'ouverture de session dépendent des valeurs d'expiration de l'authentification configurées dans votre environnement. Par exemple, si vous avez défini une valeur d'expiration de l'authentification trop faible, les utilisateurs doivent exécuter des demandes de connexion plus fréquentes. Par conséquent, vous devez comprendre clairement la manière dont ces valeurs d'expiration affectent votre environnement.
- Le nombre de connexions par session utilisateur sur NetScaler est un facteur important.
- Pour atteindre une montée en charge maximale, les ressources en matière d'UC et de RAM ont été augmentées sur XenMobile.
- La configuration du cluster à 6 nœuds a été la plus grande configuration validée. La montée en charge au-delà de 6 nœuds requiert une implémentation supplémentaire de XenMobile.

Le tableau suivant présente les taux d'ouverture de session recommandés pour les nouveaux clients et les clients existants basés sur la configuration XenMobile, le boîtier NetScaler Gateway, les paramètres de cluster et la base de données. Utilisez les données de ce tableau pour planifier un calendrier d'inscriptions optimal pour les nouveaux déploiements et les taux d'utilisateurs/d'appareils déjà inscrits pour les déploiements existants. La section Configuration associe les données de performances d'inscription et d'ouverture de session aux recommandations matérielles appropriées.

Nombre attendu d'appareils	1 000	10 000	30 000	45 000
Nombre réel d'appareils	1 000	9 998	29 977	44 991
Taux d'ouverture de session				
Intégration (FTU)	250	625	833	833
Utilisateurs existants (Worx uniquement)	1 000	1 666	3 750	883
Configuration				
Environnement de référence	VPX-XenMobile en mode autonome	MPX-XenMobile en mode autonome	MPX-XenMobile en cluster (3)	MPX-XenMobile en cluster (6)
NetScaler Gateway	VPX avec 2 Go de RAM Deux processeurs virtuels	MPX-10500	MPX-11500	MPX-11500
XenMobile - mode	Autonome*	Autonome*	Cluster	Cluster
XenMobile - cluster	S.O.	S.O.	3	6
XenMobile - boîtier virtuel	8 Go de RAM et 4 processeurs virtuels	8 Go de RAM et 4 processeurs virtuels	16 Go de RAM et 6 processeurs virtuels	16 Go de RAM et 8 processeurs virtuels
Active Directory (AD)	8 Go de RAM et 4 processeurs virtuels	8 Go de RAM et 4 processeurs virtuels	16 Go de RAM et 4 processeurs virtuels	16 Go de RM et 4 processeurs virtuels
Base de données	Externe	Externe – Microsoft SQL Server Mémoire = 16 Go Processeurs virtuels = 12	Externe – Microsoft SQL Server Mémoire = 32 Go Processeurs virtuels = 12	Externe – Microsoft SQL Server Mémoire = 48 Go Processeurs virtuels = 16

MPX-XenMobile en cluster (3)

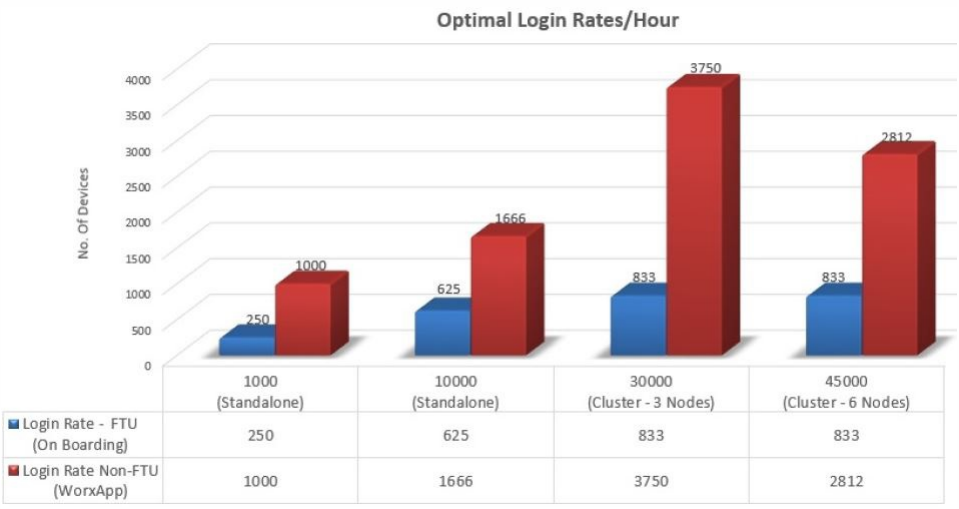
Cluster
Cluster
Cluster
Cluster
8 Go de RAM et 4 processeurs virtuels
8 Go de RAM et 4 processeurs virtuels

* Les déploiements autonomes ne sont pas recommandés pour les applications qui exigent une haute disponibilité. Citrix recommande des déploiements en cluster à haute disponibilité pour la plupart des clients.

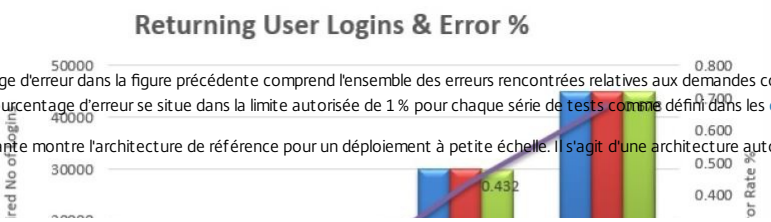
Remarque : vous allez rencontrer les situations suivantes si vous dépassez les recommandations en termes de taux ou de matériel lors du dimensionnement de votre système.

Les informations suivantes fournissent des points de données supplémentaires qui ont été enregistrés et qui affectent les résultats dans le tableau précédent.

- Latence d'inscription ou d'ouverture de session (durée aller-retour)
  - Latence moyenne totale : 0,5 à 1,5 secondes
  - Latence moyenne pour une ouverture de session NetScaler Gateway : >120 à 440 ms
  - Latence moyenne pour une demande Worx Store : 2 à 3 secondes
- Une détérioration de la performance physique, telle qu'une insuffisance des ressources d'UC et de mémoire, a été observée sur les composants de l'infrastructure lorsque les limites de la montée en charge ont été atteintes.
  - Réponses non valides sur les boîtiers NetScaler Gateway et XenMobile.
  - Réponse lente de la console XenMobile lors des périodes pendant lesquelles les charges sont élevées.

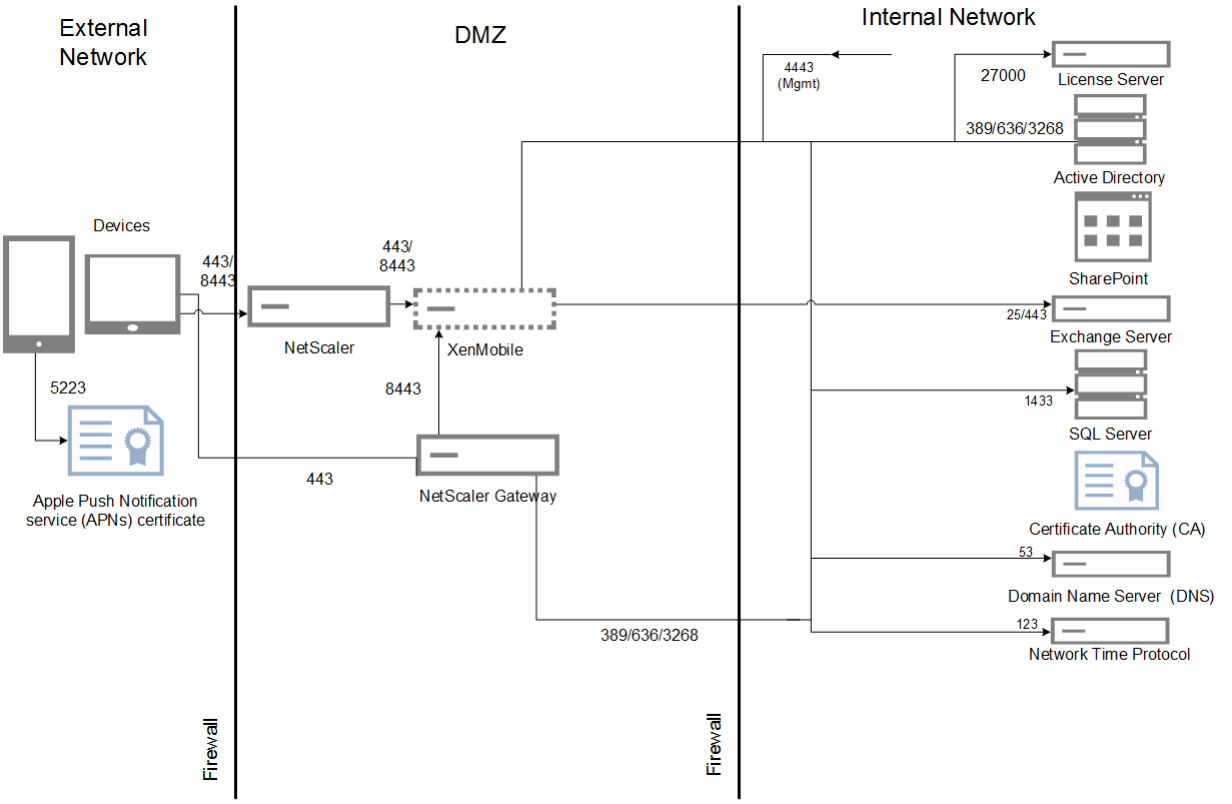


	1000 (Standalone)	10000 (Standalone)	30000 (Cluster - 3 Nodes)	45000 (Cluster - 6 Nodes)
Login Rate - FTU (On Boarding)	250	625	833	833
Login Rate Non-FTU (WorxApp)	1000	1666	3750	2812

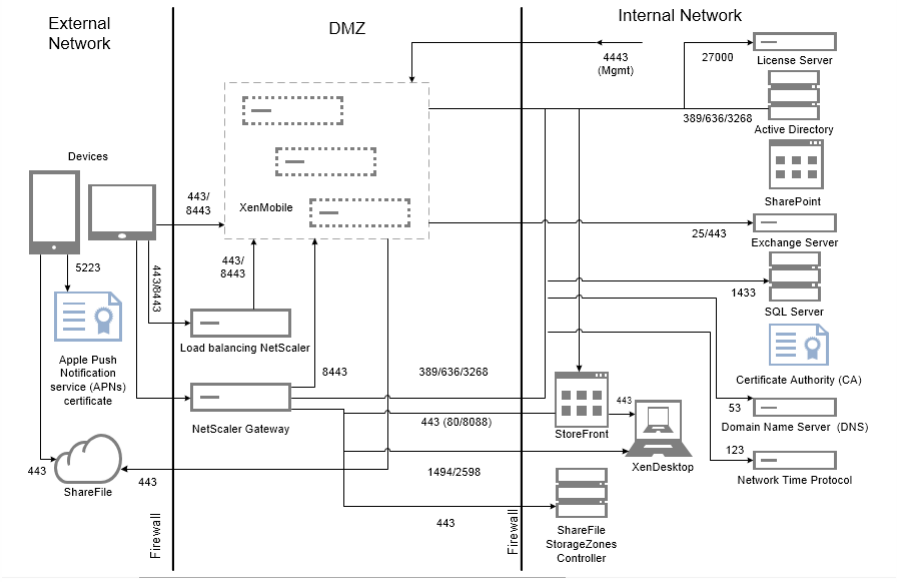


Le pourcentage d'erreur dans la figure précédente comprend l'ensemble des erreurs rencontrées relatives aux demandes correspondant à chaque opération et n'est pas limité aux ouvertures de session. Le pourcentage d'erreur se situe dans la limite autorisée de 1 % pour chaque série de tests comme défini dans les critères de sortie.

La figure suivante montre l'architecture de référence pour un déploiement à petite échelle. Il s'agit d'une architecture autonome qui prend en charge jusqu'à 10 000 appareils.



La figure suivante montre l'architecture de référence pour un déploiement d'entreprise. Il s'agit d'une architecture en cluster avec déchargement SSL pour MAM sur HTTP qui prend en charge 10 000 appareils ou plus.



Les tests ont été exécutés sur XenMobile Enterprise pour établir un banc d'essai. En vue de cibler les déploiements à petite et à grande échelle, 1 000 à 60 0000 appareils ont été utilisés pour les mesures.

Des charges de travail ont été créées pour simuler des cas d'utilisation réels. Ces charges de travail ont été exécutées pour chaque test afin d'étudier les effets sur l'inscription et les taux d'ouverture de session. L'objectif de ces tests était d'obtenir un taux d'ouverture de session optimal compris dans la marge d'erreur autorisée, comme détaillé dans les critères de sortie. Les taux d'ouverture de session sont un facteur critique pour déterminer la configuration matérielle recommandée pour les composants d'infrastructure.

Les demandes d'ouverture de session des charges de travail intégrées (FTU) comprenaient les opérations de détection automatique, d'authentification et d'enregistrement des appareils. Les abonnements aux applications, ainsi que les opérations d'installation et de démarrage ont été réparties de manière uniforme au cours de la période de test, ce qui a réuni les meilleures conditions pour une simulation réelle des actions de l'utilisateur. Au terme du test, la session a été fermée. Les demandes d'ouverture de session pour la charge de travail des utilisateurs existants comprenaient uniquement des demandes d'authentification.

Les charges de travail des utilisateurs sont définies comme suit :

Sessions utilisateur et appareils	Inclut les ouvertures de session NetScaler Gateway, les énumérations, l'enregistrement des appareils, et ainsi de suite pour chaque session.
Worx Store démarre	Les utilisateurs lancent Worx Store à plusieurs reprises et chaque fois qu'ils s'abonnent à une ou à plusieurs applications, ou qu'ils les installent, qu'il s'agisse d'applications mobiles (Web/SaaS/MDX) ou Windows (HDX).
Authentification unique des applications Web ou SaaS par appareil	Permet de lancer une séquence d'applications Web/SaaS jusqu'à ce que XenMobile exécute l'authentification unique et renvoie l'URL de l'application réelle. Le trafic n'a pas été envoyé aux applications réelles.
Téléchargements d'applications MDX par appareil	Compte le nombre de téléchargements d'applications MDX (peut se produire sur les lancements Worx Store). Pour iOS, cela comprend également l'automatisation de l'installation d'applications depuis Apple ITMS, qui utilise les nouvelles API du service de jeton/tms sur NetScaler Gateway.

Notes et hypothèses

Les scénarios suivants ne sont pas couverts dans le cadre des tests de capacité à monter en charge. Ces scénarios seront pris en compte pour l'amélioration des tests :

- Le déploiement de paquetage n'est pas testé.
- La plate-forme Windows n'est pas testée.

La transmission de stratégies a été testée sur les appareils iOS et Android.
Chaque XenMobile prend en charge un maximum de 10 000 connexions simultanées.

Les tests ont été exécutés dans des conditions idéales sur un réseau local pour ignorer les problèmes de latence réseau. Dans un environnement réel, la capacité à monter en charge dépend également de la bande passante disponible, plus particulièrement pour les téléchargements d'applications.

Tests de reconnexion

Les tests de reconnexion ont été effectués séparément des tests des scénarios First Time Use (première utilisation) et Returning User (utilisateur déjà enregistré).

Les tests de reconnexion ont été exécutés pour un maximum de 15 000 appareils.

Le taux de reconnexion pris en charge pour Android est de 17 appareils par seconde. Le taux de reconnexion pour iOS est de 8 appareils par seconde. Afin d'atteindre ce nombre, le compteur maxThread a été défini sur 1000 dans le fichier /opt/sas/tomcat/conf/server.xml.

INFORMATIONS SUR LES STRATÉGIES DE RECONNEXION RECOMMANDÉES

Charge de travail intégrée (FTU)
La charge de travail intégrée (FTU) est définie comme la première fois qu'un utilisateur accède à l'environnement XenMobile. Les opérations comprises dans cette charge de travail étaient les suivantes :

- Découverte automatique
- Inscription
- Authentification
- Enregistrement de l'appareil
- Mise à disposition d'applications (Web, SaaS et mobiles MDX)
  - Abonnement aux applications (y compris les téléchargements d'images et d'icônes)
  - Installation des applications MDX souscrites
- Lancement des applications (Web, SaaS et mobiles MDX) y compris vérification de l'état des appareils
- Transmission de stratégies (pour iOS)
- Nombre minimal de connexions WorxMail et WorxWeb (tunnels VPN) : deux connexions
- Installation des applications requises via XenMobile

Les paramètres de charge de travail sont définis dans le tableau suivant :

Appareils	Enregistrements d'appareils	Énumérations	Applications énumérées par appareil	Lancements WorxStore par appareil	Authentification unique des applications Web ou SaaS par appareil	Téléchargements d'applications MDX par appareil	Téléchargements d'applications obligatoires déclenchés par le serveur XenMobile	Stratégies déployées par appareil (iOS)
1000	1000	1000	50	4	40	10	2	20
10 000	10 000	10 000	50	4	40	10	2	20

30 000	30 000	30 000	50	4	40	10	2	20
60000	60000	60000	50	4	40	10	2	20

Charge des utilisateurs existants qui utilisent uniquement des connexions Worx

Le tableau suivant affiche la charge des utilisateurs existants (avec des connexions Worx uniquement). Cette charge de travail simulait un utilisateur utilisant les applications WorxMail et WorxWeb. Cette simulation a été utilisée pour mesurer la capacité à monter en charge de NetScaler Gateway dans la configuration XenMobile. Ceci est réalisable car en utilisant uniquement ces deux applications Worx, la charge réseau est minimale. Pour l'application WorxWeb, l'utilisateur accède à des sites Web internes qui ne déclenchent pas l'authentification unique (SSO) au serveur XenMobile. Les opérations dans ce mode étaient les suivantes :

- Authentification (NetScaler Gateway et XenMobile)
- Nombre de connexions WorxMail et WorxWeb (tunnels VPN) : quatre connexions

Le tableau suivant présente les paramètres de charge de travail pour les utilisateurs existants.

Appareils	Énumérations	Applications énumérées par appareil	Tunnels VPN par appareil[1]
1000	1000	50	3
10 000	10 000	50	3
30 000	30 000	50	3
60000	60000	50	3

1. Le nombre de tunnels VPN correspond aux connexions WorxMail et WorxWeb.

Les profils de connexion pour WorxMail et WorxWeb sont décrits dans le tableau suivant :

Connexion d'appareils	Type de connexion	Données envoyées par session[1]	Données reçues par session[1]
Connexion WorxMail n° 1	Type 1[2]	4,1 Mo	4,1 Mo
Connexion WorxMail n° 2	Type 1	6,3 Mo	12,5 Mo
Connexion WorxWeb n° 1	Type 2[3]	5,2 Mo	15,7 Mo
Connexion WorxWeb n° 2	Type 2	4,1 Mo	3,4 Mo
Nombre total d'octets transférés par session[1]		~ 19,7 Mo	~ 40,7 Mo

1. Par session : 8 heures.

2. Type 1 : envoi et réception asymétriques avec des connexions à long terme (WorxMail avec une connexion à une boîte aux lettres Microsoft Exchange dédiée).

3. Type 2 : envoi et réception asymétriques avec des connexions qui se ferment et s'ouvrent de nouveau après un certain délai (connexions WorxWeb).

Ces recommandations sont basées sur les profils WorxMail et WorxWeb utilisés pour automatiser
une charge « moyenne ». Les modifications apportées aux détails de connexion affectent les résultats de l'analyse. Par exemple, si le nombre de connexions par utilisateur est augmenté, le nombre de sessions de NetScaler Gateway prises en charge peut être réduit.

Profils WorxMail et WorxWeb

Les profils utilisés pour chaque application sont conçus pour automatiser une charge « très importante ». Les tableaux suivants affichent les détails des profils de WorxMail et WorxWeb.

Profil WorxMail pour une charge de travail moyenne

Messages envoyés par jour	20
Messages reçus par jour	80
Messages lus par jour	80
Messages supprimés par jour	20
Taille moyenne des messages (Ko)	200

Profil WorxWeb pour charge de travail moyenne

Nombre d'applications Web lancées	10
Nombre de pages Web ouvertes manuellement	10
Nombre moyen de paires demande–réponse par application Web	100
Taille moyenne de la demande (octets)	300
Taille moyenne de la réponse (octets)	1000

Configuration et paramètres

Les configurations suivantes ont été utilisées lors de l'exécution des tests de capacité à monter en charge :

- Les serveurs virtuels de NetScaler Gateway et d'équilibrage de charge coexistaient sur le même boîtier NetScaler Gateway.
- Délai d'expiration de la session NetScaler configuré sur 60 minutes.
- Une clé de 2 048 bits a été utilisée sur NetScaler Gateway pour les transactions SSL.

Les taux d'ouverture de session constituent la base de cette analyse. Ils servent de ligne directive pour les composants d'infrastructure et leur configuration respective. Il est important de noter que les taux d'ouverture de session prennent en compte une marge d'erreur qui se compose des éléments suivants :

- Réponses non valides
  - Une réponse avec le code d'état 401/404 à la place de 200 est considérée comme non valide.
- Délais d'expiration des demandes
  - Une réponse est attendue dans les 120 secondes.
- Erreurs de connexion
  - Une réinitialisation de la connexion s'est produite.
  - Un arrêt brutal de connexion s'est produit.

Le taux d'ouverture de session est acceptable si le taux d'erreur global est inférieur à 1 % du nombre total de demandes envoyées à partir d'un appareil donné. Le taux d'erreur inclut les erreurs correspondant à chaque opération de charge de travail individuelle, ainsi que la performance physique du composant d'infrastructure, comme l'insuffisance des ressources d'UC et de mémoire.

Le tableau suivant dresse la liste des logiciels d'infrastructure XenMobile utilisés pour ces tests.

Composant	Version
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0.824
Base de données externe	Microsoft SQL Server 2014

Les tests de capacité à monter en charge ont été exécutés sur une plate-forme XenServer comme décrit dans le tableau suivant.

Fournisseur	Genuine Intel
Modèle	UC Intel Xeon — E5645 @ 2,40 GHz (nombre d'UC = 24)

Cela comprend les services de base d'infrastructure (par exemple, Active Directory, Windows Domain Name Service (DNS), autorité de certification, Microsoft Exchange, etc.), ainsi que les composants XenMobile (boîtier virtuel XenMobile et boîtier virtuel NetScaler Gateway VPX, le cas échéant).

À propos du serveur XenMobile 10.3.5

Oct 17, 2016

Vous pouvez effectuer une mise à niveau directe vers XenMobile 10.3.5 dans la console XenMobile depuis les versions suivantes :

- XenMobile 10.3 Rolling Patch 1
- XenMobile 10.3
- XenMobile 10.1 Rolling Patch 4
- XenMobile 10,1

Pour effectuer la mise à niveau, vous devez utiliser xms_10.3.5.354.bin. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Gestion des versions**. Cliquez sur **Mettre à niveau** et chargez ensuite le fichier xms_10.3.0.5,354.bin. Pour plus d'informations sur la mise à niveau de la console, veuillez consulter la rubrique Mise à niveau de XenMobile.

Pour procéder à une nouvelle installation de XenMobile 10.3.5, consultez la section Installation de XenMobile.

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, consultez le manuel de déploiement de XenMobile.

Nouveautés dans XenMobile 10.3.5

XenMobile 10.3.5 fournit des corrections de bogues et les nouvelles fonctionnalités suivantes.

Votre équipe de services de cloud peut mettre à jour votre déploiement de cloud de serveur XenMobile de la version 10.3 à la version 10.3.5 sans interruption.

Vous pouvez autoriser les utilisateurs Android M à activer ou bloquer quatre types d'autorisations. Lorsque les utilisateurs s'inscrivent auprès de Worx Home, ils voient une série de quatre messages leur demandant d'autoriser ou de refuser les autorisations suivantes à Worx Home :

- Accès aux informations de l'appareil pour assurer le bon fonctionnement de Worx Home.
- Possibilité de passer des appels et de gérer les appels téléphoniques.
- Accès aux photos, au multimédia et aux fichiers de l'appareil.
- Accès à l'emplacement de l'appareil.

Avec cette version, vous pouvez autoriser les utilisateurs iOS à se réauthentifier auprès de Worx Home ainsi qu'aux applications Worx à l'aide de la fonction Touch ID. Pour les appareils iOS 8 et iOS 9, lorsque l'authentification unique est activée pour Worx Home et que Touch ID est activé sur l'appareil, cette combinaison remplace l'utilisation d'un code PIN. Les utilisateurs seront toujours tenus d'entrer un code PIN chaque fois que l'authentification en ligne via NetScaler

Gateway est requise. Ceci est nécessaire dans les cas suivants :

- La session de l'utilisateur a expiré.
- L'utilisateur redémarre l'appareil.
- Worx Home n'est pas en cours d'exécution et l'utilisateur le démarre ou démarre une application MDX.

Vous pouvez désormais créer des profils d'inscription pour des appareils Android et iOS sur la nouvelle page **Configurer > Profils d'inscription** de la console XenMobile. Un profil d'inscription s'applique à tous les modes du serveur. Vous pouvez créer plusieurs profils d'inscription et les associer à différents groupes de mise à disposition.

Remarque : la page **Profils d'inscription** ne s'applique pas aux appareils Windows. Pour de plus amples informations sur l'inscription d'appareils Windows, consultez la section Appareils Windows.

Vous avez précédemment configuré le nombre maximal d'appareils par utilisateur par le biais de la propriété de serveur **Nombre d'appareils par utilisateur**. Cette propriété de serveur est désormais obsolète. Vous pouvez à présent configurer le nombre maximal d'appareils sur la nouvelle page **Configurer > Profils d'inscription**. Auparavant, vous pouviez limiter le nombre d'appareils uniquement pour le mode MDM. Désormais, vous pouvez également limiter le nombre d'appareils pour le mode MAM.

Par défaut, le nombre d'appareils qu'un utilisateur peut inscrire est illimité. Pour de plus amples informations, consultez la section Limite d'inscription d'appareils.

XenMobile 10.3.5 prend en charge le WorxStore en hébreu et en chinois traditionnel.

XenMobile 10.3.5 introduit un nouveau mode de serveur MAM exclusif. Pour faire la distinction entre les anciens et les nouveaux modes MAM, la documentation Citrix fait référence au nouveau mode comme le « mode MAM exclusif » et fait référence à l'ancien mode MAM en tant qu' « ancien mode MAM ». L'ancienne fonctionnalité MAM reste inchangée et Citrix n'y apportera aucune amélioration dans les versions futures.

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. Les appareils s'enregistrent en mode MDM+MAM. En mode MDM+MAM, les utilisateurs qui ont choisi de ne pas utiliser la gestion MDM continuent de recevoir l'ancienne fonctionnalité MAM, que vous ayez ou non mis à niveau vers XenMobile 10.3.5.

Remarque : précédemment, la définition de la propriété de serveur sur **MAM** avait le même effet que de la définir sur **ENT** : les appareils s'enregistraient en mode MDM+MAM ; les utilisateurs qui avaient choisi de ne pas utiliser la gestion MDM recevaient l'ancienne fonctionnalité MAM.

Les avantages du mode MAM exclusif comprennent un cryptage supplémentaire (et pas seulement un code secret), un VPN mobile et une meilleure confidentialité des utilisateurs, ce qui fait du mode MAM exclusif la solution idéale pour les appareils BYO.

Si votre serveur XenMobile est actuellement en mode MAM, vous pouvez mettre à niveau vers le nouveau mode MAM exclusif pour bénéficier des fonctionnalités suivantes qui étaient uniquement disponibles pour MDM. Ces fonctionnalités ne sont pas disponibles pour Windows Phone.

- **Authentification basée sur certificats**
  Le mode MAM exclusif prend en charge l'authentification basée sur les certificats. Les utilisateurs profiteront d'un accès continu à leurs applications, même lorsque leur mot de passe AD expire. Si vous choisissez d'utiliser l'authentification basée sur certificats pour les appareils MAM, vous devez configurer NetScaler Gateway. Par défaut, dans **Paramètres > NetScaler 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. Vous devez modifier ce paramètre sur **Activé** pour activer l'authentification par certificats.
- **Portail en libre-service**, pour permettre 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 Effacement des applications sur l'appareil et Mode kiosque sur l'appareil dans **Configurer > Actions**.
- **Tous les modes d'inscription**, y compris Haute sécurité, URL d'invitation et Deux facteurs, configurés via **Gérer > Inscription**.
- **Limite d'enregistrement d'appareils** pour les appareils Android et iOS. La propriété de serveur **Nombre d'appareils par utilisateur** a été déplacée vers la nouvelle page **Configurer > Profils d'inscription** et s'applique maintenant également au nouveau mode MAM exclusif.
- **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 disponibles dans cette version vous permettent d'effectuer ce qui suit :
  - Envoyer une URL d'invitation et un code PIN à usage unique
  - Envoyer la commande Mode kiosque ou Effacement des applications sur des appareils

> ### Important
>
> Pour utiliser le nouveau mode MAM exclusif, vous devez configurer XenMobile comme décrit dans cet article et vos utilisateurs doivent réinscrire leurs appareils. N'oubliez pas de donner le nom de domaine complet (FQDN) du serveur XenMobile à vos utilisateurs car ils en auront besoin pour l'inscription.
>
> Dans le nouveau mode MAM exclusif, comme avec le mode ENT, les appareils s'inscrivent à l'aide du nom de domaine complet du serveur XenMobile. (Dans les versions antérieures du mode MAM, les appareils s'inscrivent à l'aide du nom de domaine complet de NetScaler Gateway).

Comment cette mise à niveau affecte-t-elle les appareils inscrits ?

Le tableau suivant décrit la manière dont les nouvelles fonctionnalités de XenMobile 10.3.5 affectent les appareils inscrits.

Pour les appareils actuellement inscrits en tant que :	XenMobile 10.3.5 offre	Tâches administrateur	Tâches utilisateur
MDM			

• Mode serveur = MDM	• Corrections de bogues • Nouvelles fonctionnalités	Installation de XenMobile 10.3.5	Aucun(e)
MDM+MAM • Mode serveur = ENT • Utilisateurs ayant opté pour la gestion des appareils	• Corrections de bogues • Nouvelles fonctionnalités	Installation de XenMobile 10.3.5	Aucun(e)
MAM • Mode serveur = ENT • Utilisateurs ayant opté de ne pas utiliser la gestion des appareils	• Corrections de bogues • Nouvelles fonctionnalités Remarque : dans ce cas, les appareils s'inscrivent dans l'ancien mode MAM. Si vous souhaitez offrir la nouvelle fonctionnalité MAM aux utilisateurs, définissez un nouveau serveur XenMobile.	Installation de XenMobile 10.3.5	Aucun(e)
MAM • Mode serveur = MAM	• Corrections de bogues • Nouvelles fonctionnalités • Mise à niveau facultative vers le nouveau mode MAM exclusif	Pour continuer à utiliser l'ancienne fonctionnalité MAM : Installation de XenMobile 10.3.5 Pour mettre à niveau vers le mode MAM exclusif : 1. Installation de XenMobile 10.3.5 2. Consultez la section Présentation de la configuration du mode MAM exclusif ci-après pour obtenir des informations de configuration supplémentaires.	Aucun(e) Réinscrire des appareils

Présentation de la configuration du mode MAM exclusif

Le *mode MAM exclusif* fait référence au mode de serveur MAM lorsqu'il est utilisé avec des licences Enterprise ou Advanced. Le mode MAM exclusif diffère du *mode MDM+MAM*, qui est utilisé si votre serveur XenMobile est en mode ENT. En mode

MDM+MAM, les utilisateurs qui ont choisi de ne pas utiliser la gestion MDM reçoivent l'ancienne fonctionnalité MAM, que vous ayez ou non mis à niveau vers XenMobile 10.3.5.

> **Important**
>
> L'ancienne fonctionnalité MAM fonctionne de la même façon que pour les versions antérieures et ne sera pas optimisée dans les versions futures.

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
ENT/ADV/MDM	Mode MDM	MDM
ENT/ADV	Mode MAM (également appelé mode MAM exclusif)	MAM
ENT/ADV	Mode MDM+MAM	ENT Les utilisateurs qui ont choisi de ne pas utiliser la gestion des appareils utiliseront l'ancien mode MAM.

Vous devez configurer le mode MAM exclusif *uniquement* si :

- Votre serveur XenMobile utilise un **mode de serveur MAM** et vous voulez le changer au profit du nouveau mode MAM exclusif pour bénéficier des fonctionnalités supplémentaires.
- Vous souhaitez définir un serveur XenMobile pour fournir la fonctionnalité MAM exclusif à tous les utilisateurs qui se connectent à ce serveur.

Les principales étapes de configuration du mode MAM exclusif sont les suivantes :

1. Installer ou mettre à niveau vers XenMobile 10.3.5.
2. Sur la page **Gérer > Appareils**, cochez l'option **Mode de serveur**. Si le **mode de serveur** est **MDM** ou **ENT**, n'effectuez pas les étapes décrites dans cette procédure, car la configuration qui en résulterait ne prendrait pas en charge la gestion des appareils.
3. Ouvrez les ports 443 et 8443 sur votre serveur XenMobile et pare-feu à Internet pour que les appareils puissent se connecter au serveur XenMobile. L'inscription doit se produire sur votre serveur XenMobile.
4. Si vous mettez à niveau un serveur dont le **mode de serveur** est déjà défini sur **MAM**, passez à l'étape suivante. Si vous effectuez une nouvelle installation de XenMobile 10.3.5, le **mode de serveur** du serveur XenMobile est par défaut le mode **ENT**. Pour activer le mode MAM exclusif, vous devez définir la propriété de serveur **Mode de serveur** sur **MAM**. Pour de plus amples informations, consultez la section Configuration du mode de serveur pour MAM exclusif.
5. Si vous souhaitez utiliser l'authentification basée sur les certificats, configurez XenMobile et votre NetScaler Gateway de manière à prendre en charge l'authentification basée sur les certificats. Par défaut, dans **Paramètres > NetScaler**

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. Vous devez modifier ce paramètre sur **Activé**. Pour plus d'informations sur la configuration, consultez la section Authentification par certificat en mode MAM exclusif.

6. Lors du choix ou de la configuration d'un modèle de notification à utiliser avec le mode MAM exclusif, rappelez-vous que SMTP est la seule méthode prise en charge pour envoyer des invitations d'inscription.
7. Si vos utilisateurs font l'objet d'une mise à niveau vers le nouveau mode MAM exclusif, donnez-leur le nom de domaine complet (FQDN) du serveur XenMobile et informez-les qu'ils doivent se réinscrire.
   Dans le nouveau mode MAM exclusif, comme avec le mode ENT, les appareils s'inscrivent à l'aide du nom de domaine complet du serveur XenMobile. (Dans les versions antérieures du mode MAM, les appareils s'inscrivent à l'aide du nom de domaine complet de NetScaler Gateway).

Le tableau suivant décrit les différences entre l'ancienne fonctionnalité MAM (XenMobile 10.3 et XenMobile 10.3.5) et le nouveau mode MAM exclusif (XenMobile 10.3.5).

Scénarios d'inscription et autres fonctionnalités	XenMobile 10.3 Ancien mode MAM (le mode de serveur est ENT)	XenMobile 10.3.5 Ancien mode MAM (le mode de serveur est ENT)	XenMobile 10.3.5 Mode MAM exclusif (le mode de serveur est MAM)
Authentification par certificats	Non pris en charge.	Non pris en charge.	Pris en charge. Pour utiliser l'authentification par certificats, NetScaler 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.	Le serveur XenMobile doit être accessible à partir des appareils.
Options d'inscription	Utiliser le nom de domaine complet de NetScaler Gateway ou ne pas s'inscrire.	Utiliser le nom de domaine complet de NetScaler Gateway ou 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	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.	Pris en charge.

Portail en libre-service Options du mode kiosque et d'effacement des applications	Non pris en charge.	Non pris en charge.	Pris en charge.
Comportement d'effacement des applications	Les applications restent sur l'appareil mais ne sont pas utilisables. Le compte est uniquement supprimé sur le client.	Les applications restent sur l'appareil mais ne sont pas utilisables. Le compte est uniquement supprimé sur le client.	Les applications restent sur l'appareil mais ne sont pas utilisables. Le compte est uniquement supprimé sur le client.
Actions automatisées pour les utilisateurs du mode MAM exclusif.	Non pris en charge.	Les actions liées aux événements, propriétés d'appareil et 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, propriétés d'appareil et propriétés d'utilisateur sont prises en charge. Les actions automatisées basées sur les applications installées ne sont pas prises en charge.
Action intégrée lorsqu'un utilisateur AD est supprimé	Non pris en charge.	L'effacement des applications est pris en charge.	L'effacement des applications est pris en charge.
Limite d'inscription	Pris en charge pour MDM uniquement ; configuré via une propriété de serveur.	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	Pris en charge ; XenMobile dresse la liste des applications installées sur un appareil	Non pris en charge.

Dans un déploiement MAM exclusif de XenMobile, vous pouvez déployer un cluster de serveurs XenMobile dans la zone démilitarisée (DMZ) ou dans le réseau interne. Dans chaque scénario, l'authentification se produit au travers de NetScaler Gateway.

Notez que, contrairement à un déploiement XenMobile Enterprise, XenMobile NetScaler Connector (XNC) et XenMobile Mail Manager (XMM) ne sont pas requis.

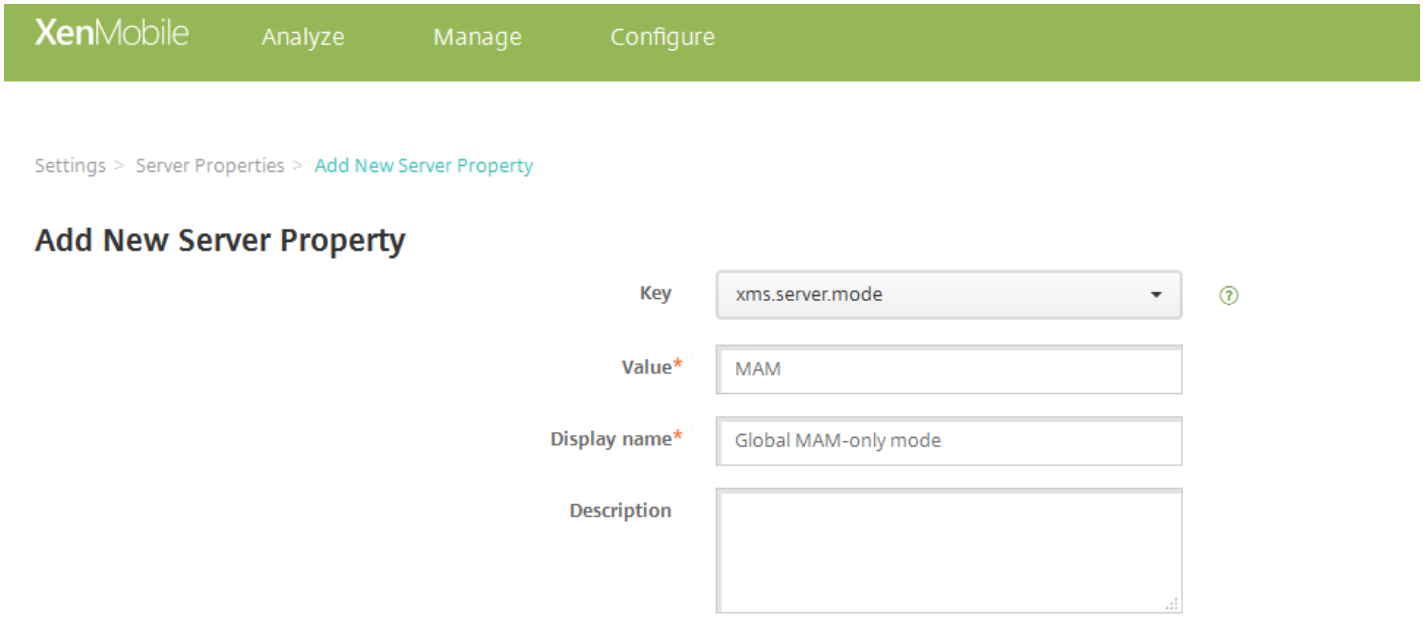
Pour accéder à un diagramme d'architecture de référence, consultez la section Reference Architecture for On-Premises Deployments du Manuel de déploiement de XenMobile.

- Les applications requises ne sont pas installées automatiquement. Les utilisateurs doivent les ajouter manuellement depuis le WorxStore.
- Les utilisateurs iOS doivent faire confiance au certificat iOS Developer. Les utilisateurs Android doivent activer le paramètre pour pouvoir installer des applications à partir de magasins d'applications tiers.
- Les utilisateurs reçoivent des notifications de mise à jour des applications uniquement dans WorxStore.
- Lorsqu'un utilisateur supprime Worx Home ou qu'il se désinscrit de Worx Home, les applications installées restent sur l'appareil jusqu'à ce que l'utilisateur les supprime.
- Le mode MAM exclusif ne prend pas en charge APNS ou Google Cloud Messaging.
- La console XenMobile n'affiche pas l'état jailbreaké/rooté des appareils inscrits en mode MAM exclusif, toutefois la stratégie **Bloquer les appareils jailbreakés ou rootés** fonctionne pour ces appareils.

Après une nouvelle installation, le serveur est par défaut en mode ENT. Pour activer le mode MAM exclusif pour XenMobile 10.3.5, configurez le serveur comme suit :

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit pour ouvrir la page **Paramètres**.
2. Sur la page **Paramètres**, cliquez sur **Propriétés du serveur**.
3. Cliquez sur **Ajouter**.
4. Dans **Clé**, cliquez sur **xms.server.mode**.
5. Dans **Valeur**, entrez **MAM**.
6. Dans **Nom d'affichage**, entrez une description à afficher dans le tableau **Propriétés du serveur**.

Si vous le souhaitez, entrez une description et cliquez sur **Enregistrer**.



Important

Après avoir configuré la propriété xms.server.mode sur le mode MAM exclusif, la console XenMobile affiche toujours des zones qui s'appliquent au mode MDM, telles que les propriétés de l'appareil. Les paramètres ne fonctionneront pas.

Authentification par certificat en mode MAM uniquement

Jul 27, 2016

Pour utiliser l'authentification par certificat en mode MAM uniquement, vous devez configurer le serveur Microsoft, le serveur XenMobile et le serveur NetScaler Gateway. Les étapes générales suivantes sont détaillées 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 le serveur XenMobile :

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 NetScaler Gateway afin de fournir un certificat utilisateur pour l'authentification.

Sur NetScaler Gateway :

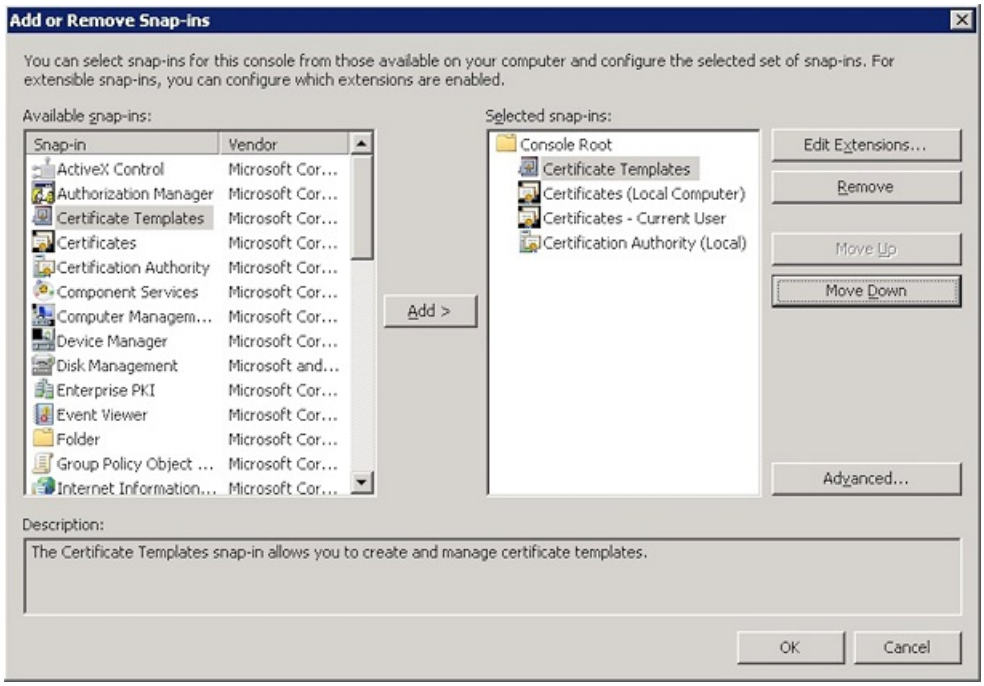
1. Configurez NetScaler Gateway pour XenMobile pour l'authentification par certificat en mode MAM uniquement

Pour ajouter un composant logiciel enfichable pour les certificats dans la console Microsoft Management Console

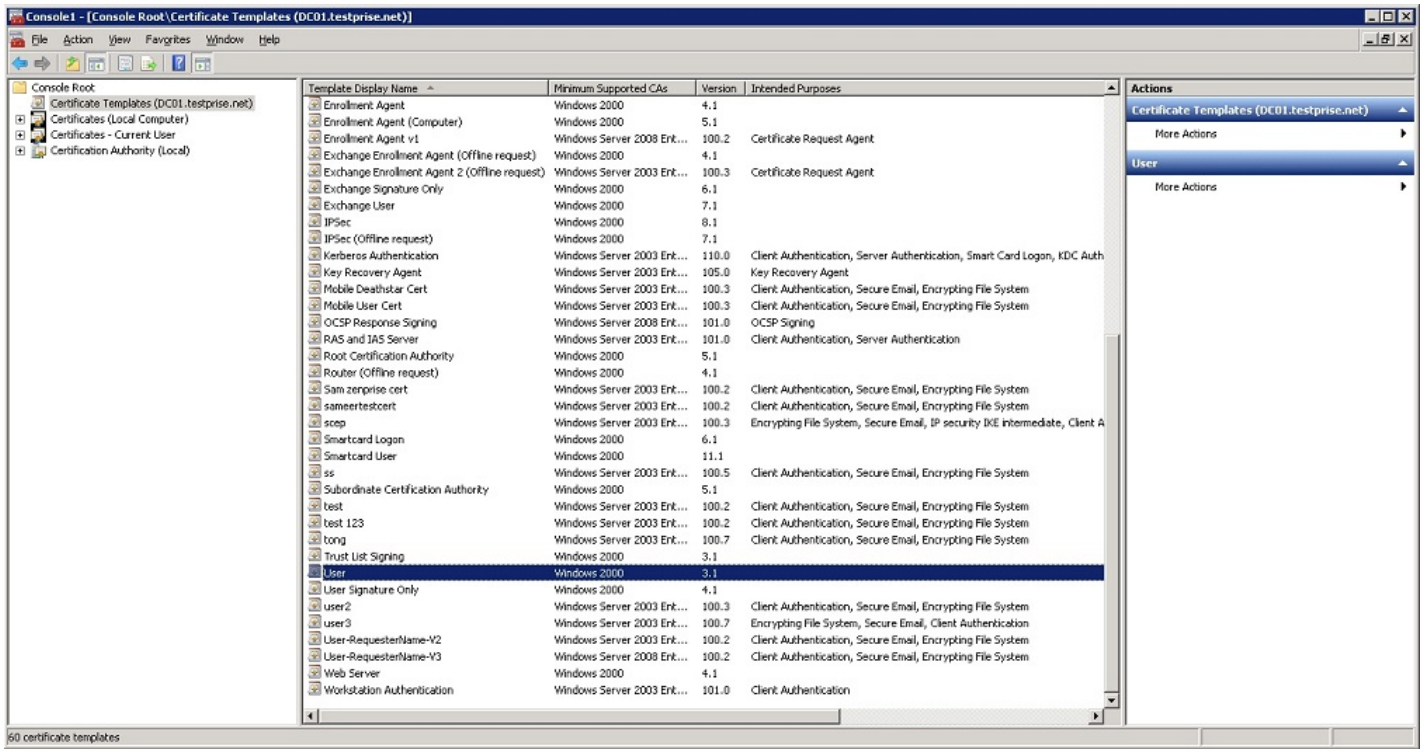
1. Ouvrez la console et cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.

2. Ajoutez les composants logiciels enfichables suivants :

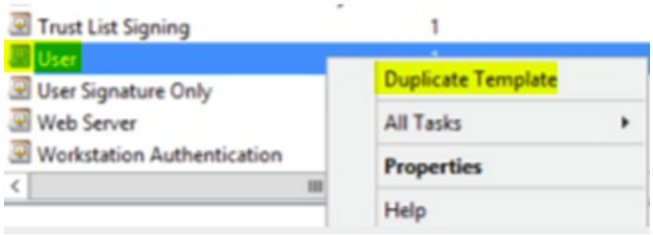
Modèles de certificats
Certificats (ordinateur local)
Certificats - Utilisateur actuel
Autorité de certification (locale)



3. Développez **Modèles de certificats**.



4. Sélectionnez le modèle **Utilisateur** et **Dupliquer le modèle**.

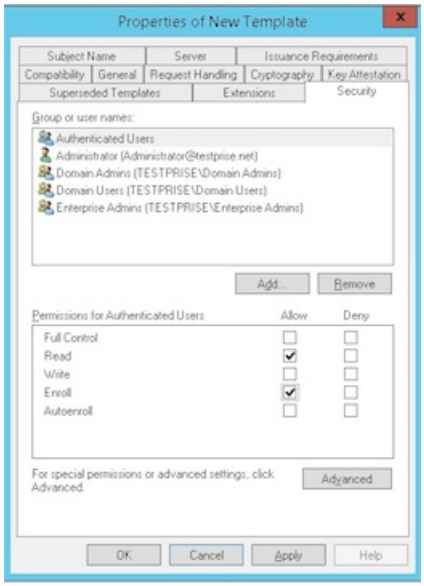


5. Fournissez le nom du modèle.

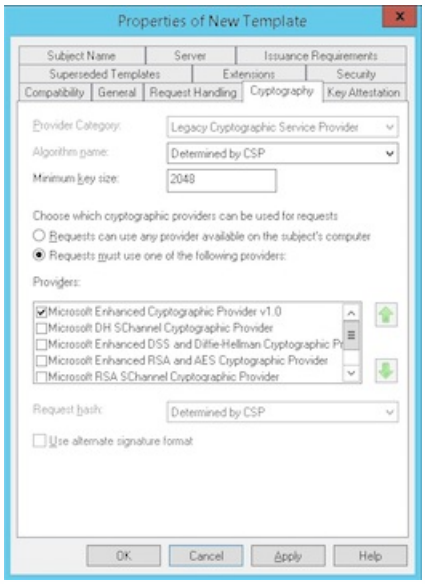
> **Important :** ne sélectionnez pas la case **Publier le certificat dans Active Directory** sauf si cela est nécessaire. Si cette option est sélectionnée, tous les certificats client utilisateur seront émis/créés dans Active Directory, ce qui pourrait encombrer votre base de données Active Directory.

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.

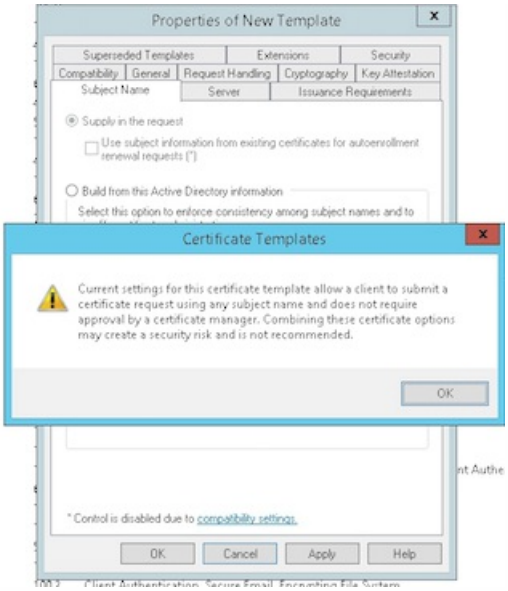
7. Sous **Sécurité**, sélectionnez l'option **Inscrire** dans la colonne **Autoriser** pour les utilisateurs authentifiés.



8. Sous **Cryptographie**, n'oubliez pas de fournir la taille de clé, que vous devrez entrer lors de la configuration de XenMobile.



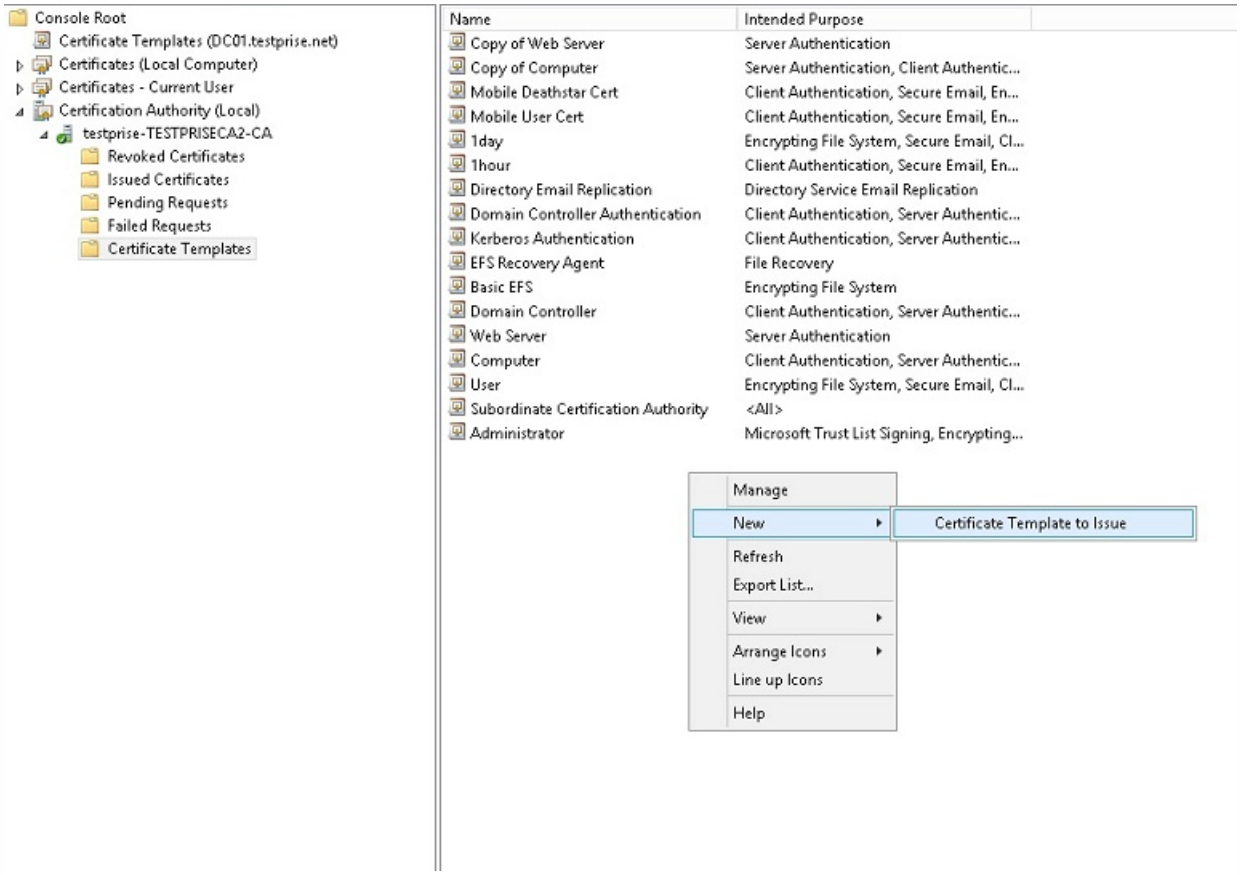
9. Sous **Nom du sujet**, sélectionnez **Fournir dans la demande**. Appliquez les modifications et enregistrez.



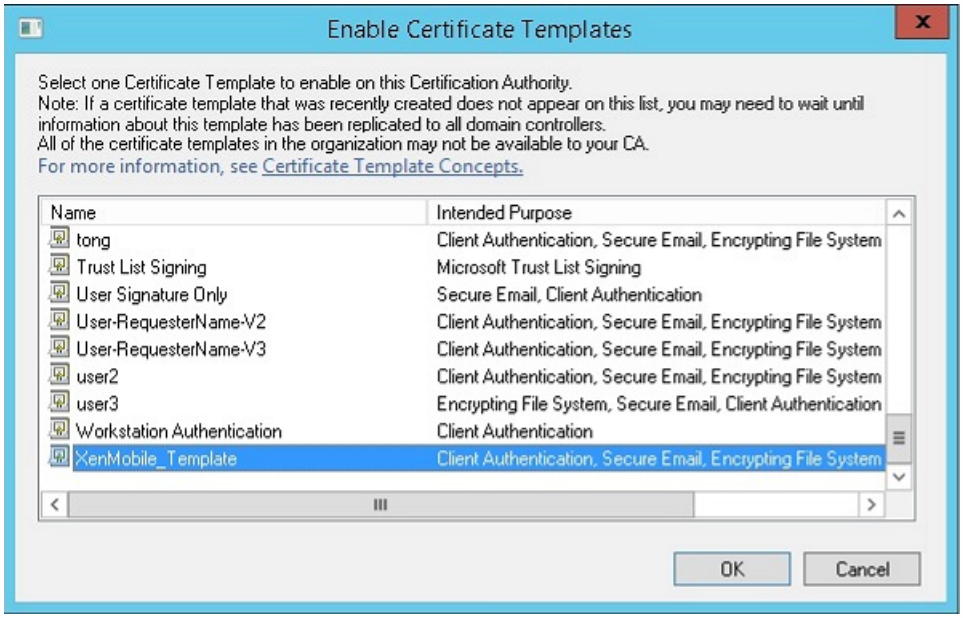
Pour ajouter le modèle à l'autorité de certification (CA)

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.

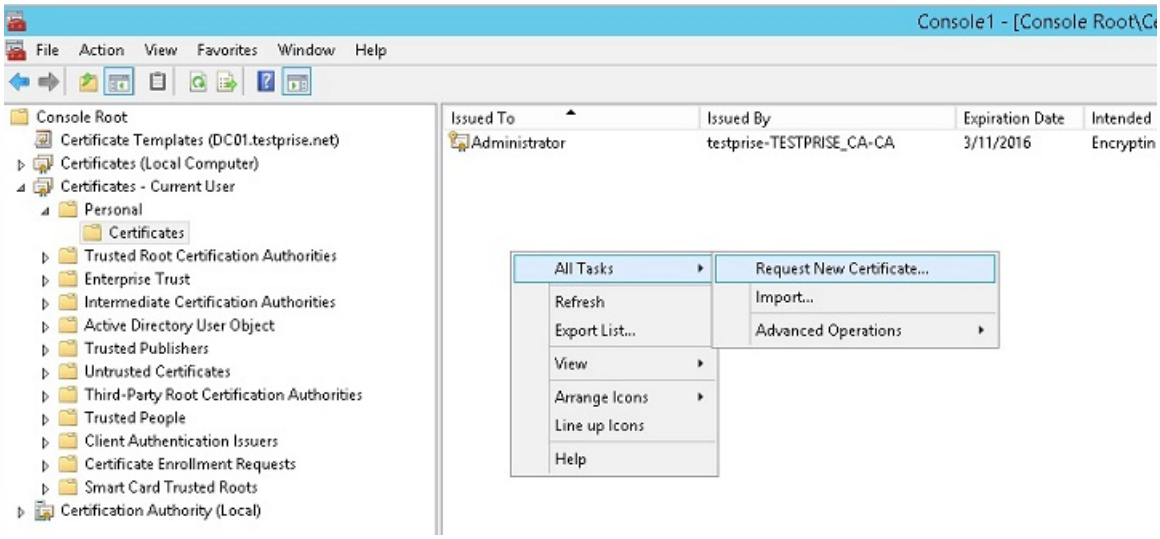


Pour créer un certificat PFX depuis le serveur CA

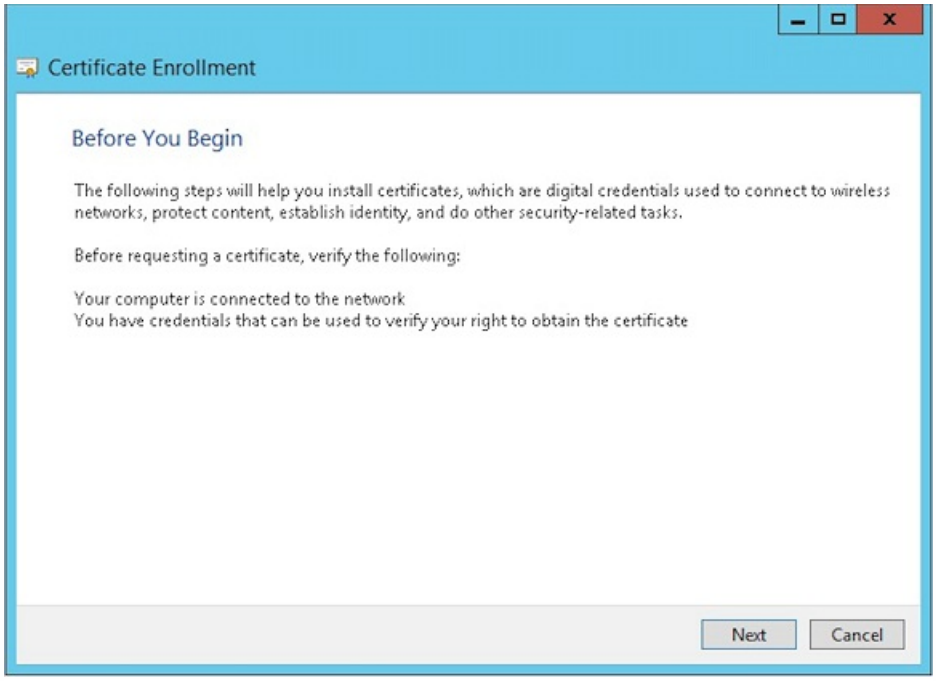
1. Créez un certificat utilisateur .pfx à l'aide du compte de service avec lequel vous vous êtes connecté. Ce fichier .pfx sera chargé dans XenMobile, qui demandera un certificat utilisateur de la part des utilisateurs qui inscrivent leurs appareils.

2. Sous **Utilisateur actuel**, développez **Certificats**.

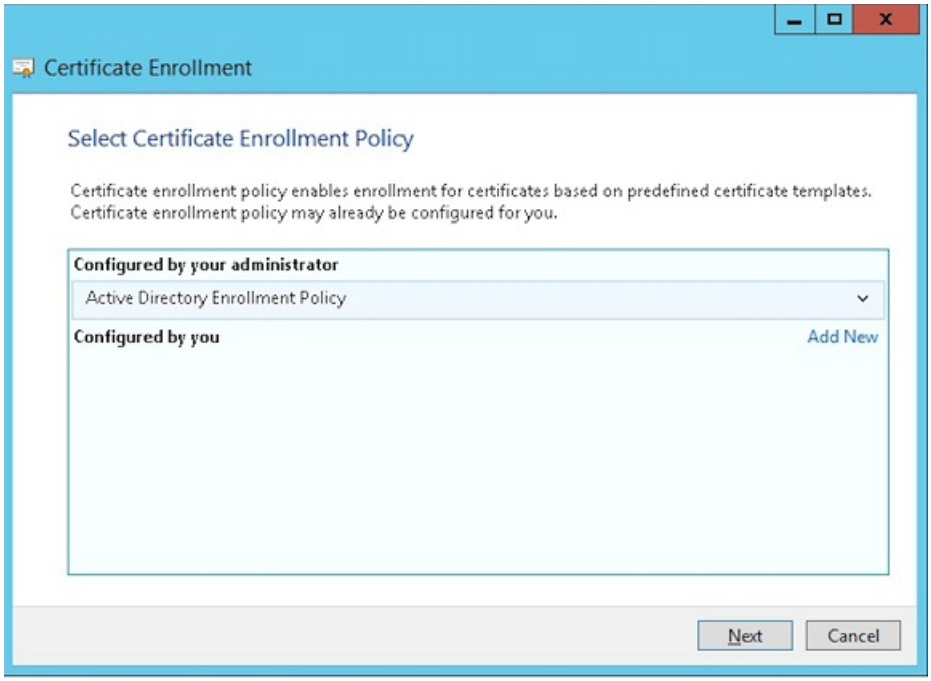
3. Cliquez avec le bouton droit dans le panneau de droite et cliquez sur **Demander un nouveau certificat**.



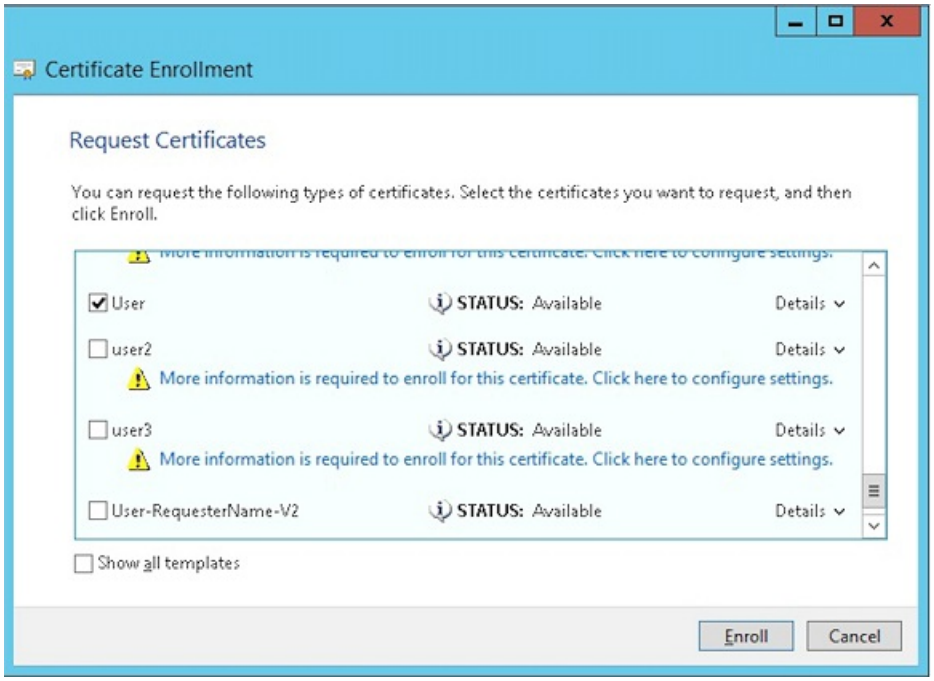
4. L'écran **Inscription de certificats** s'affiche. Cliquez sur **Suivant**.



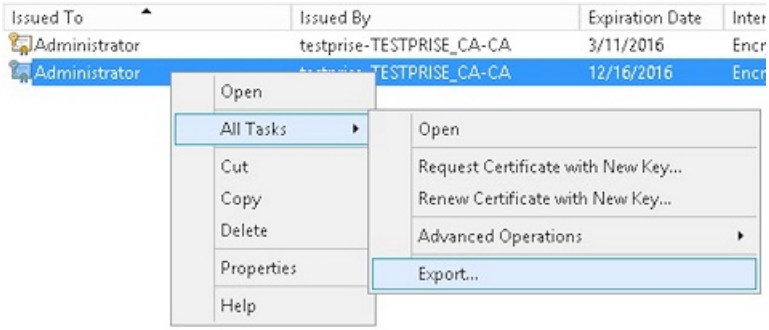
5. Sélectionnez **Stratégie d'inscription à Active Directory** et cliquez sur **Suivant**.



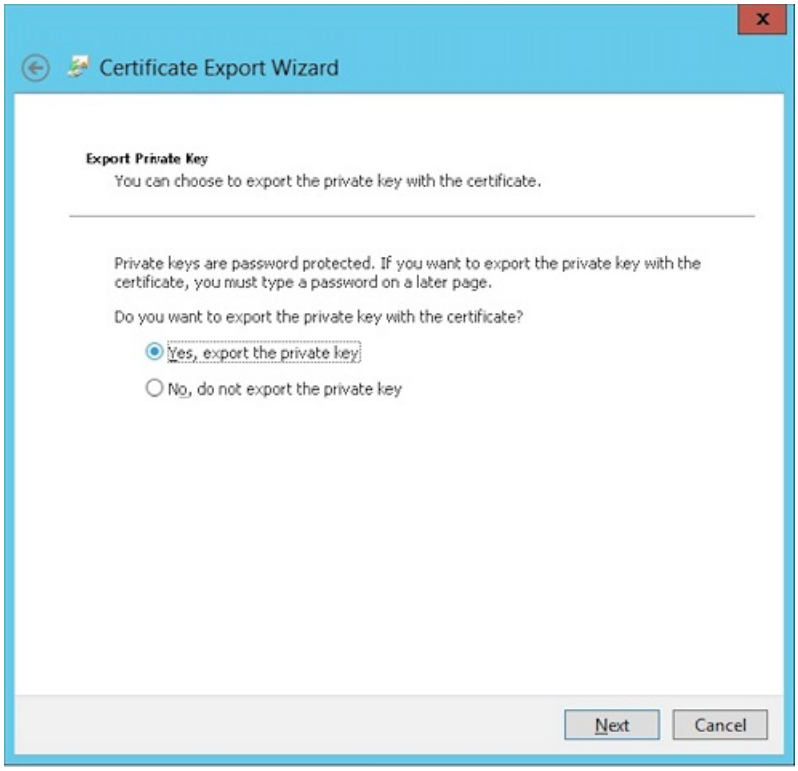
6. Sélectionnez le modèle **Utilisateur** et cliquez sur **Inscrire**.



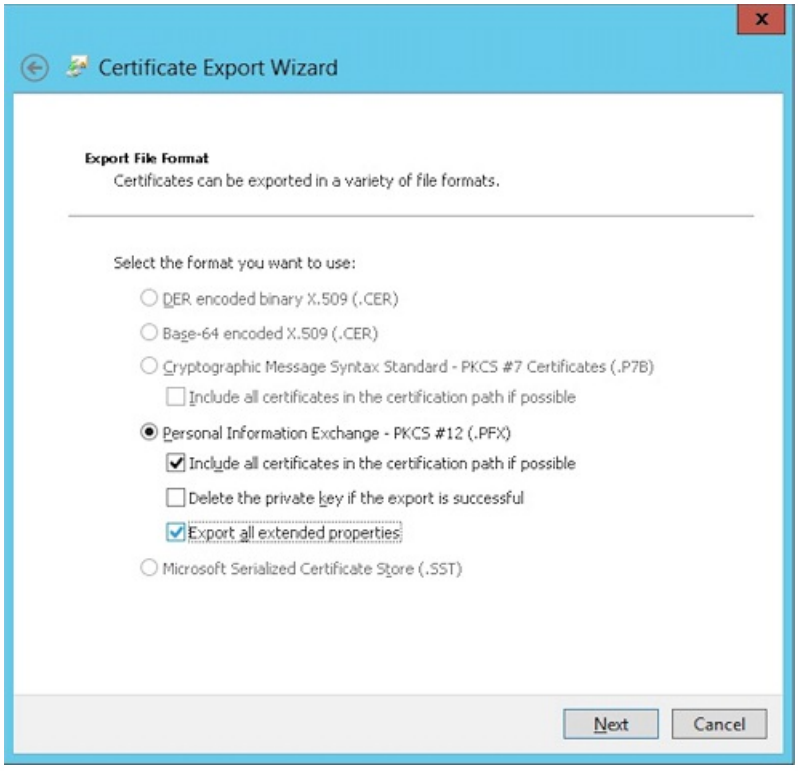
7. Exportez le fichier .pfx que vous avez créé à l'étape précédente.



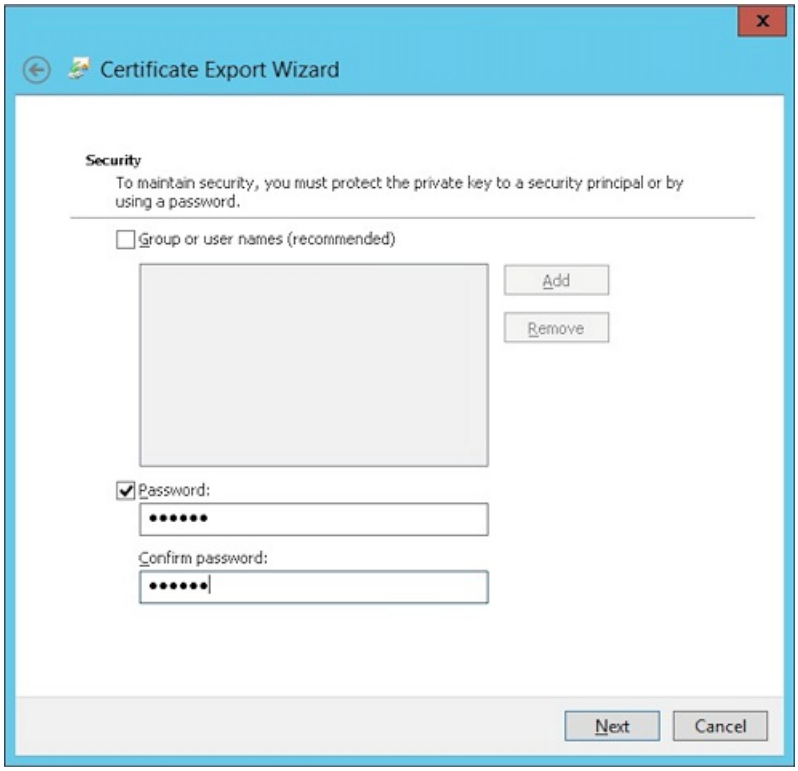
Cliquez sur **Oui, exporter la clé privée**.



Sélectionnez les cases **Si possible inclure tous les certificats dans le chemin d'accès de certification si possible** et **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.

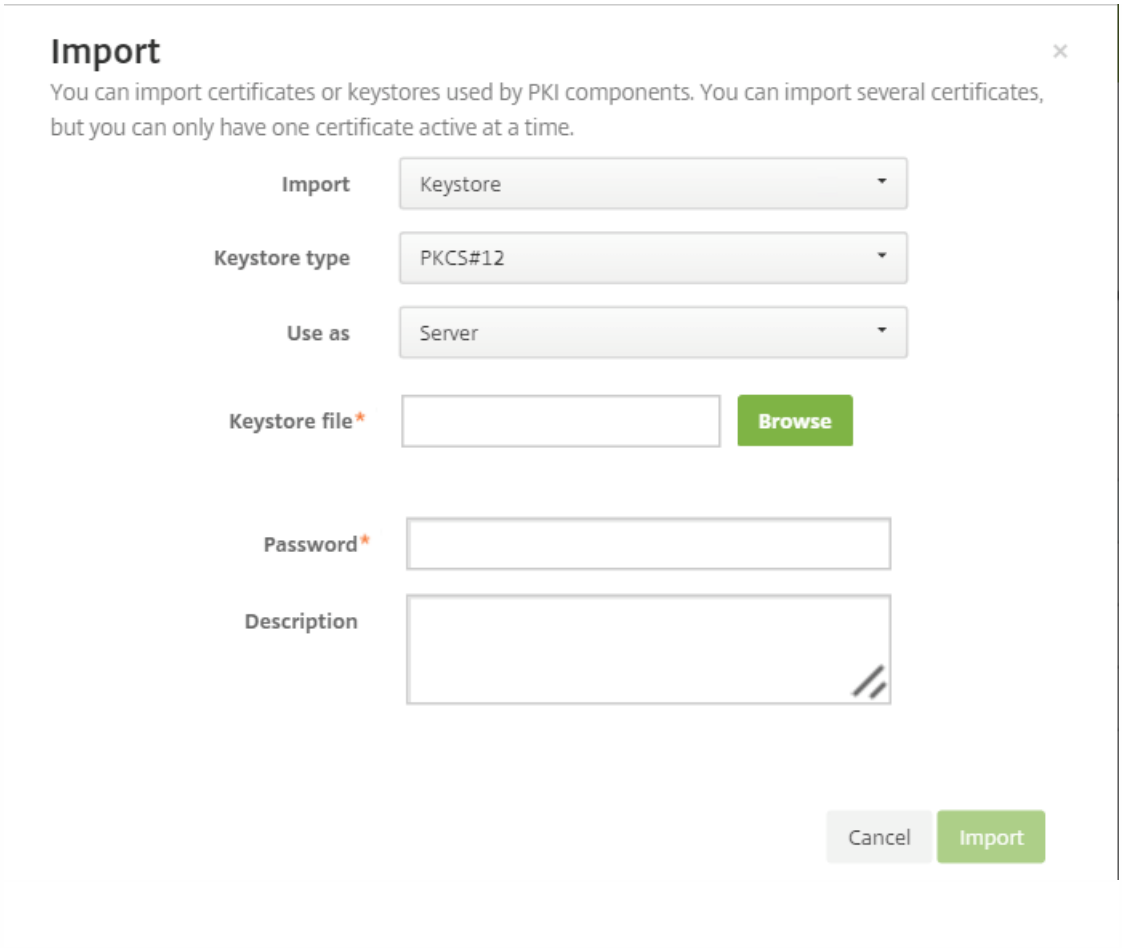
Pour charger le certificat sur XenMobile

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 venez de créer.
- **Mot de passe** : entrez le mot de passe que vous avez créé pour ce certificat.



5. Cliquez sur **Importer**.

6. Vérifiez que le certificat a été installé correctement. Il doit s'afficher en tant que certificat Utilisateur.

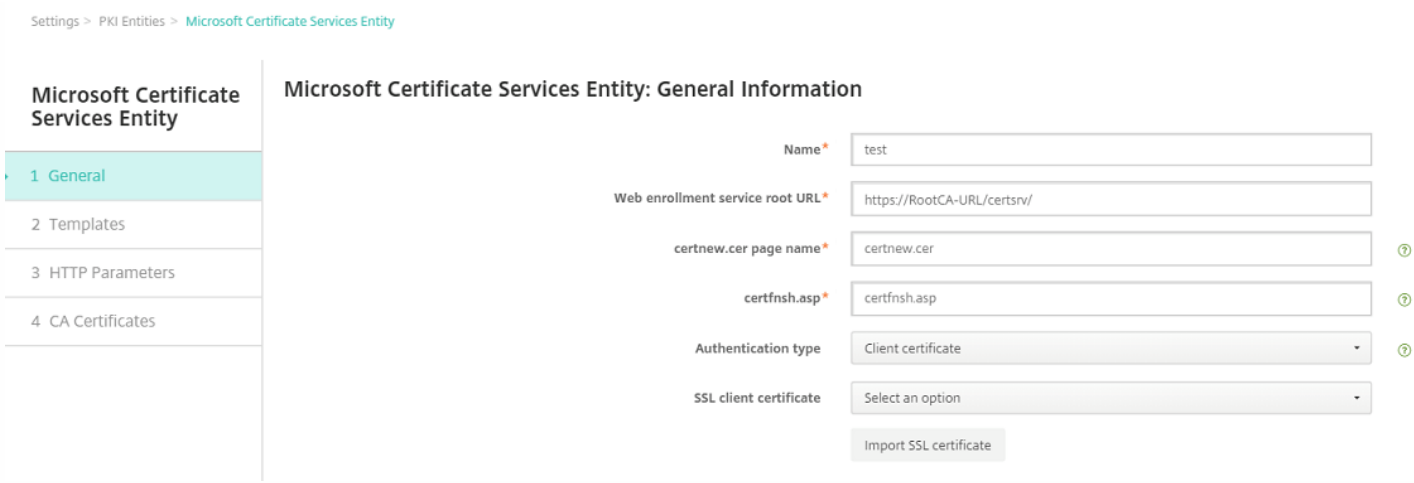
Pour créer l'entité PKI pour l'authentification par certificat

1. Dans **Paramètres**, accédez à **Plus > Gestion des certificats > Entités PKI**.

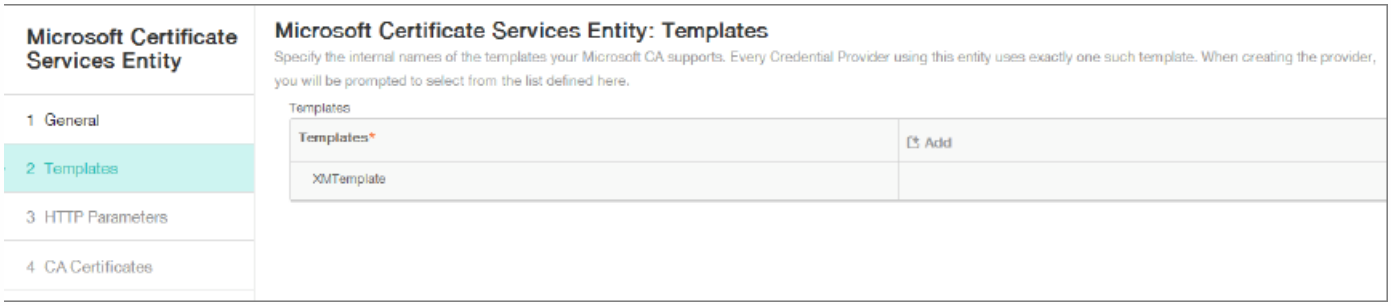
2. Cliquez sur **Ajouter** et sur **Entité Services de certificats Microsoft**. La page Entité Services de certificats Microsoft : informations générales s'affiche.

3. Entrez les paramètres suivants :

- **Nom** : entrez un nom quelconque
- **URL racine du service d'inscription Web** : https://RootCA-URL/certsrv/
  Remarque : 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 l'autorité de certification racine qui a signé le certificat client XenMobile.

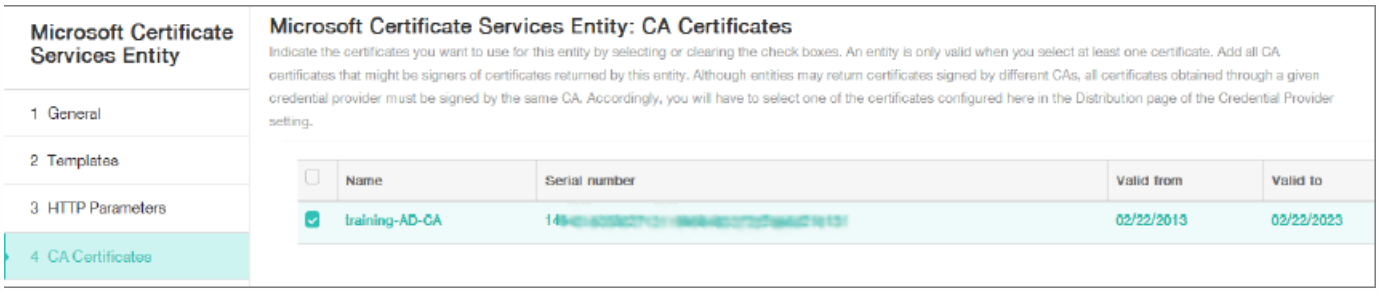


4. Sous **Modèles**, ajoutez le modèle que vous avez créé lors de la configuration du certificat Microsoft. Veillez à ne pas ajouter d'espaces.



5. Ignorez les paramètres HTTP et cliquez sur **Certificats CA**.

6. Sélectionnez le certificat utilisateur à utiliser pour émettre le certificat client XenMobile. Cela fait partie de la chaîne importée depuis le certificat client XenMobile.



7. Cliquez sur **Enregistrer**.

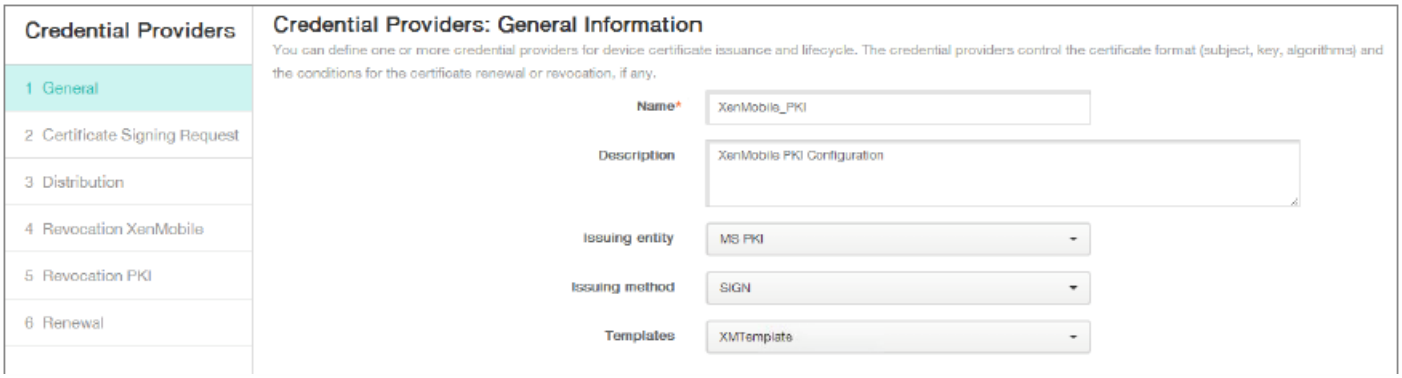
Pour configurer les fournisseurs d'informations d'identification

1. Dans Paramètres, accédez à **Plus > Gestion des certificats > Fournisseurs d'identités**.

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.



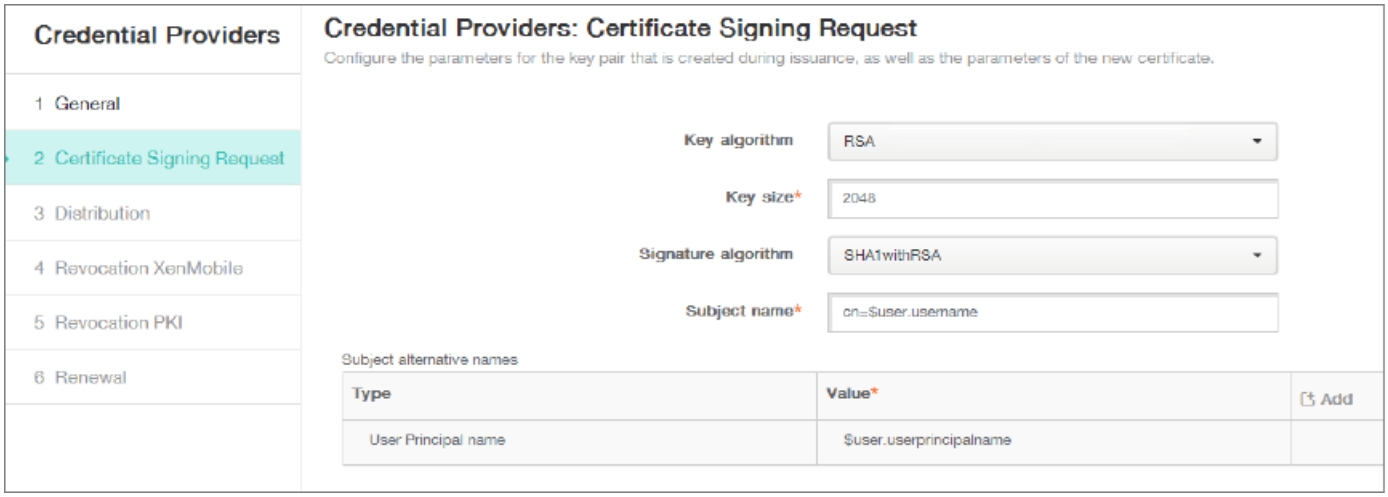
4. Cliquez ensuite sur **Demande de signature de certificat** et entrez les paramètres suivants :

- **Algorithme de clé** : RSA
- **Taille de la clé** : 2048
- **Algorithme de signature** : SHA1withRSA
- **Nom du sujet**: cn=$user.username

  Le nom du sujet fait référence au sAMAccountName. Cela permet à NetScaler d'utiliser le champ Nom d'utilisateur pour l'authentification.

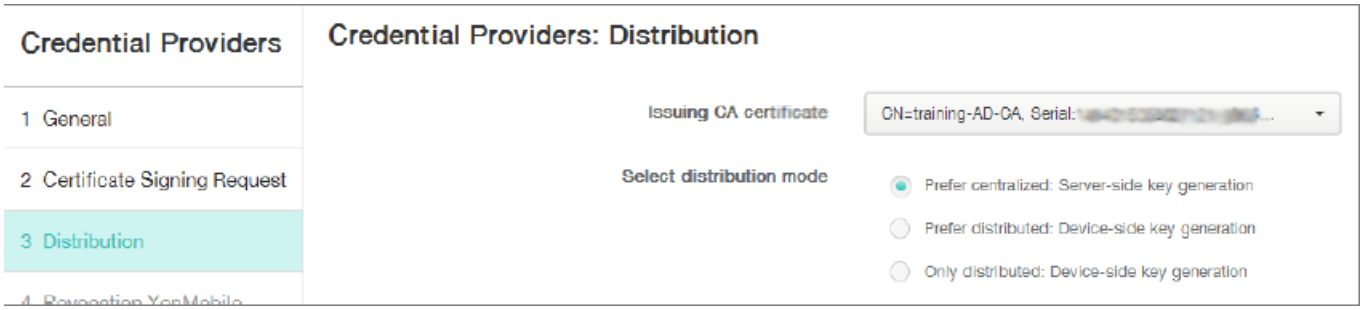
5. Pour **Noms de sujet alternatifs**, cliquez sur **Ajouter** et entrez les paramètres suivants :

- **Type** : nom principal de l'utilisateur
- **Valeur** : $user.userprincipalname



6. 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**.

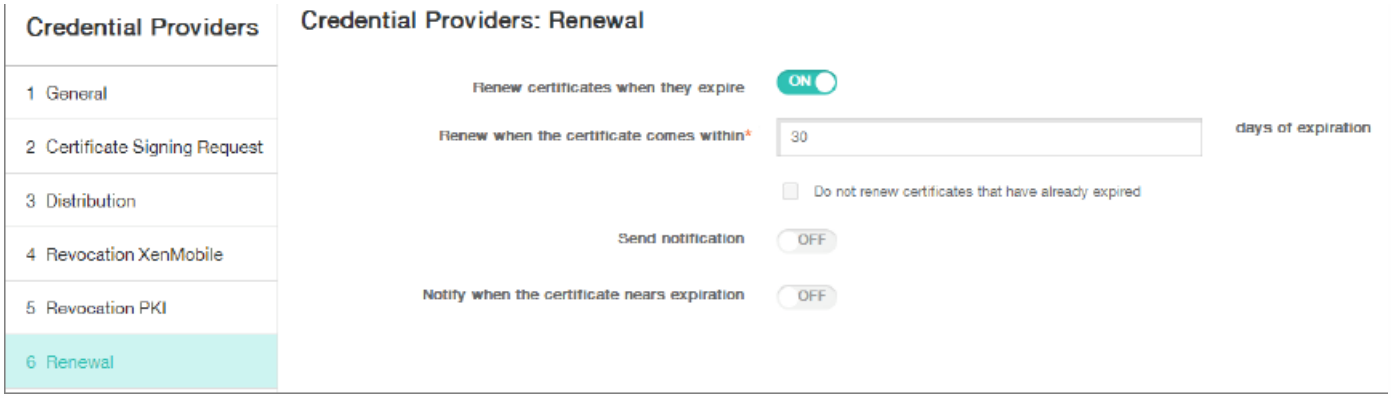


7. Pour les deux prochaines sections —**Révocation XenMobile** et **Révocation PKI** --définissez les paramètres comme vous le souhaitez. Pour les besoins de cet article, ces deux options ont été ignorées.

8. Cliquez sur **Renouvellement**.

9. Pour **Renouveler les certificats lorsqu'ils expirent**, sélectionnez **Activé**.

10. Laissez tous les autres paramètres par défaut ou modifiez-les comme vous le souhaitez.



11. Cliquez sur **Enregistrer**.

Pour configurer la remise de certificats NetScaler 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 **NetScaler Gateway**.

3. Si NetScaler Gateway n'est pas déjà ajouté, cliquez sur **Ajouter** et spécifiez les paramètres :

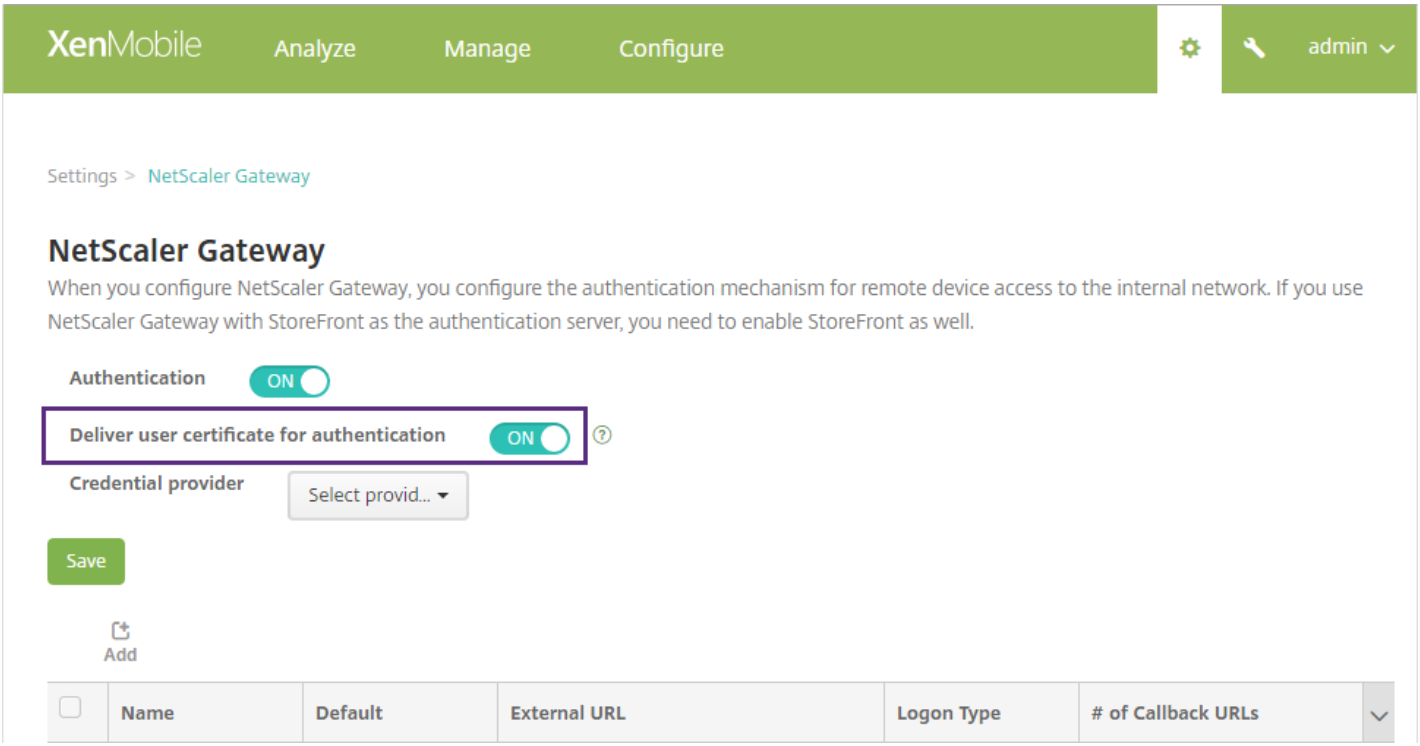
   URL externe : https://VotreURLNetScalerGateway

   Type d'ouverture de session : Certificat

   Mot de passe requis : DÉSACTIVÉ

   Définir par défaut : ACTIVÉ

4. Pour **Délivrer un certificat utilisateur pour l'authentification**, sélectionnez **Activé**, puis cliquez sur **Enregistrer**.



5. Pour **Fournisseur d'identités**, sélectionnez un fournisseur et cliquez sur **Enregistrer**.

Pour configurer NetScaler Gateway pour l'authentification par certificat

Suivez ces étapes sur votre boîtier NetScaler pour configurer l'authentification par certificat dans XenMobile en mode MAM exclusif.

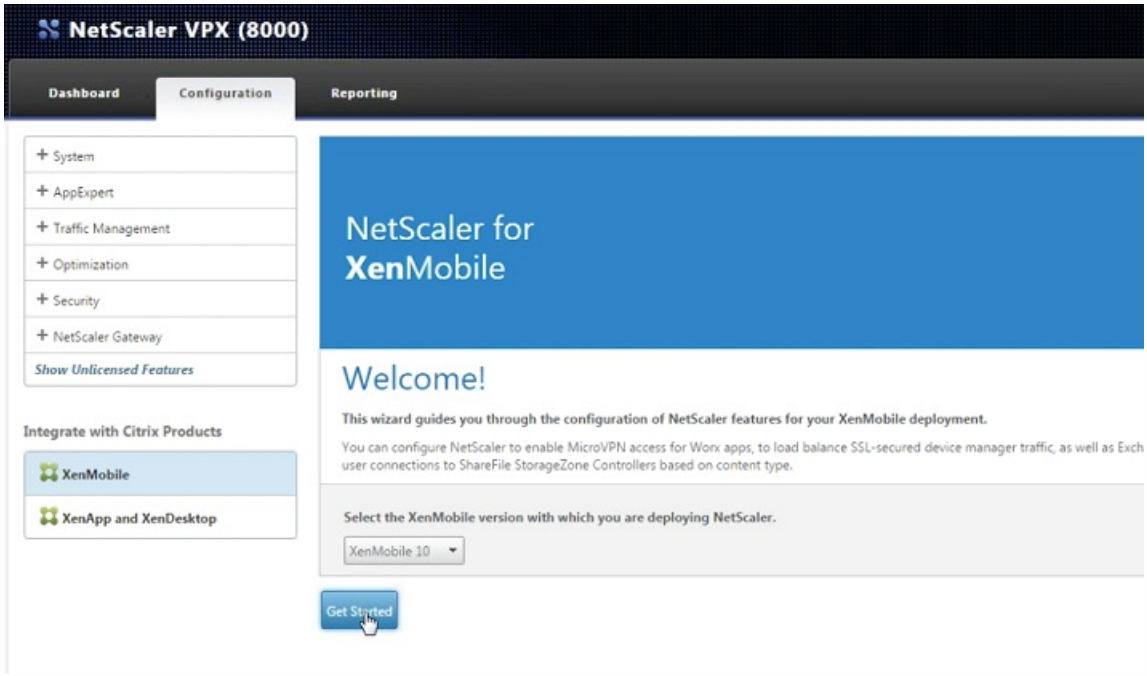
1. Ouvrez une session sur NetScaler.

2. Sous **Configuration**, accédez à **Integrate with Citrix Products**, puis sélectionnez **XenMobile**.

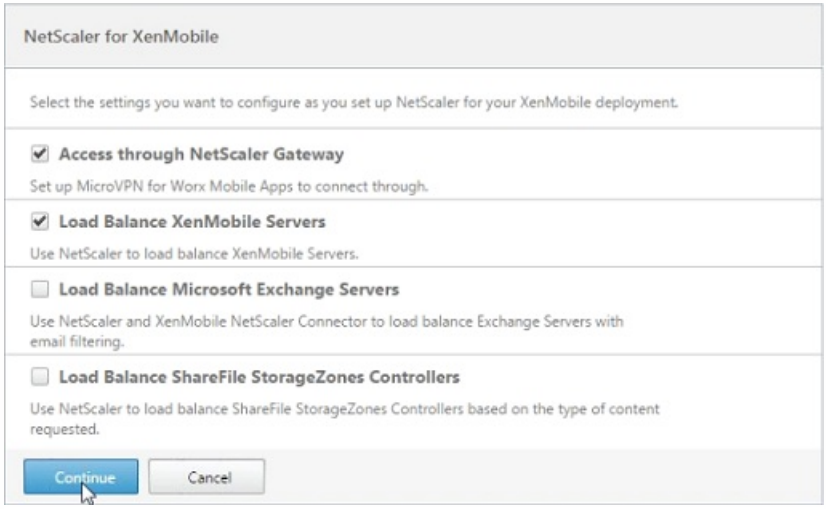
   Un assistant destiné à la configuration des fonctionnalités NetScaler pour votre déploiement XenMobile s'ouvre.

3. Choisissez **XenMobile 10**.

4. Cliquez sur **Get Started**.



5. Sur l'écran suivant, sélectionnez **Access through NetScaler Gateway** et **Load Balance XenMobile Servers**, puis cliquez sur **Continue**.



6. Sur l'écran suivant, entrez l'adresse IP externe de NetScaler Gateway, puis cliquez sur **Continue**.

   L'écran Server Certificate for NetScaler Gateway s'affiche.

7. Vous devez utiliser un certificat existant ou en installer un. Cliquez sur **Continue**.

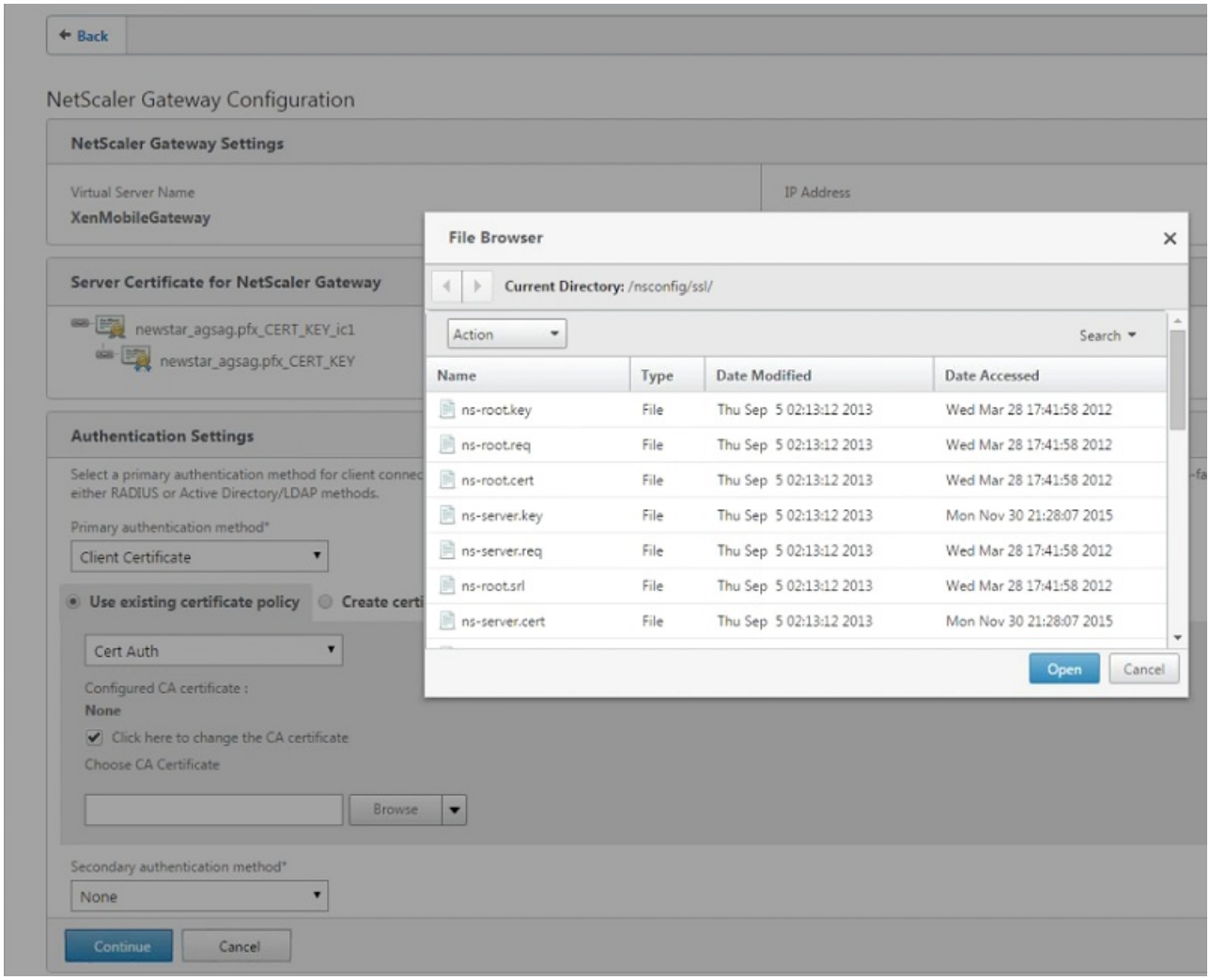
   L'écran **Authentication Settings** s'affiche.

8. Dans le champ **Primary authentication method**, sélectionnez **Client Certificate**.

   Use existing certificate policy et **Cert Auth** seront automatiquement sélectionnés dans les deux champs suivants.

9. Sélectionnez **Click here to change the CA certificate**, puis dans la liste **Browse**, accédez à l'emplacement du

certificat de l'autorité de certification de votre choix.



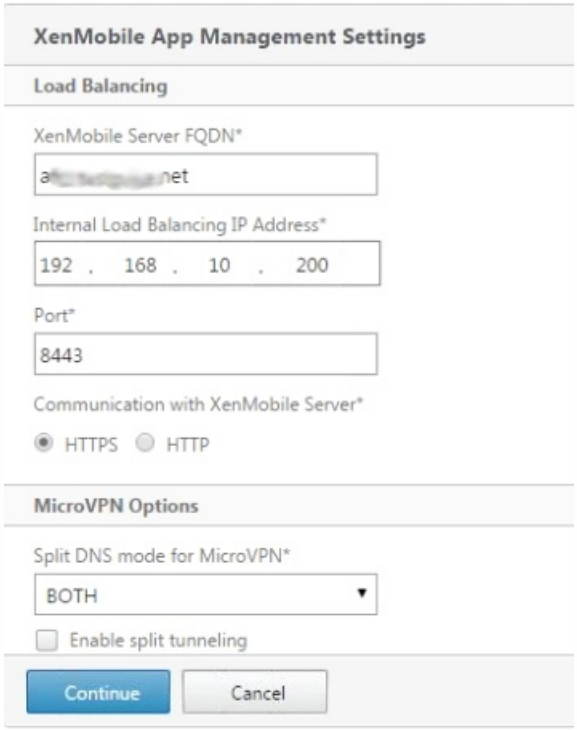
10. Laissez le champ **Second authentication method** définit sur **None**, puis cliquez sur **Continue**.

11. Sur l'écran **Load Balancing**, entrez le nom de domaine complet (FQDN) du serveur XenMobile et une adresse IP d'équilibrage de charge interne MAM exclusif.

12. Étant donné qu'il s'agit d'un déploiement de déchargement SSL, sélectionnez **HTTP** dans **Communication with XenMobile Server**.

    Le champ **Split DNS mode for MicroVPN** indique **BOTH**.

13. Cliquez sur **Continue**.



14. Sur l'écran **XenMobile Server Certificate**, choisissez un certificat de serveur existant ou installez un nouveau certificat. Si vous exécutez plusieurs serveurs XenMobile, vous devez ajouter un certificat pour chacun d'entre eux. Cliquez sur **Continue**.

15. Sur l'écran **Device certificate**, s'il n'est pas déjà installé, vous devez exporter ce certificat depuis la console XenMobile. Pour ce faire :

    a. Sur la console, cliquez sur l'icône d'engrenage dans le coin supérieur droit pour ouvrir l'écran **Paramètres**.

    b. Cliquez sur **Certificat**, puis choisissez le certificat de l'autorité de certification dans la liste.

    c. Cliquez sur **Exporter**.

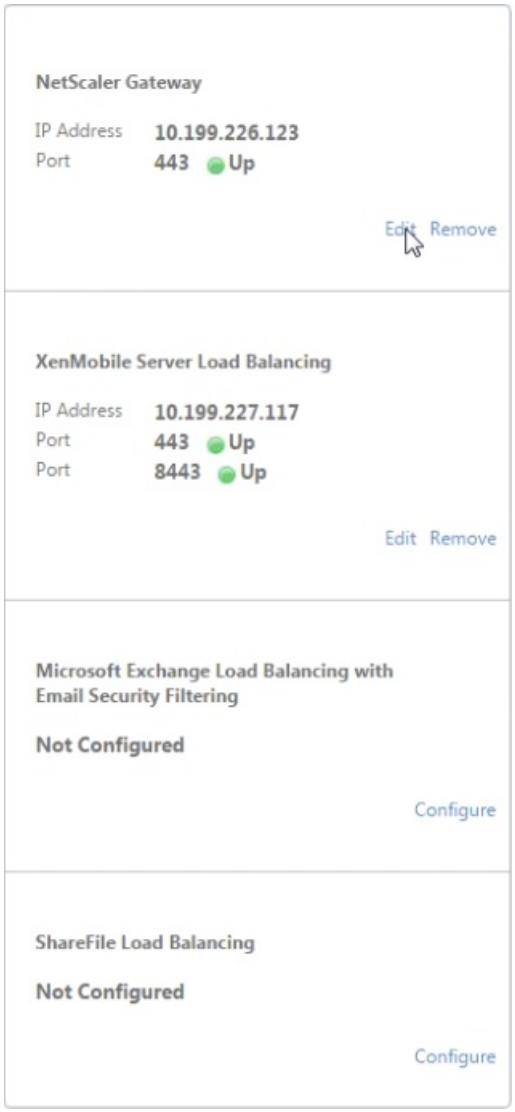
    d. Revenez dans l'assistant NetScaler et sélectionnez le certificat que vous avez exporté (téléchargé) pour l'installer.

    e. Cliquez sur **Continue**.

Les adresses IP du serveur XenMobile que vous avez configurées s'affichent.

16. Cliquez sur **Continue**.

    Sur le tableau de bord NetScaler, vérifiez que NetScaler Gateway et l'équilibrage de charge XenMobile sont configurés :



Limite d'inscription d’appareils

Jul 27, 2016

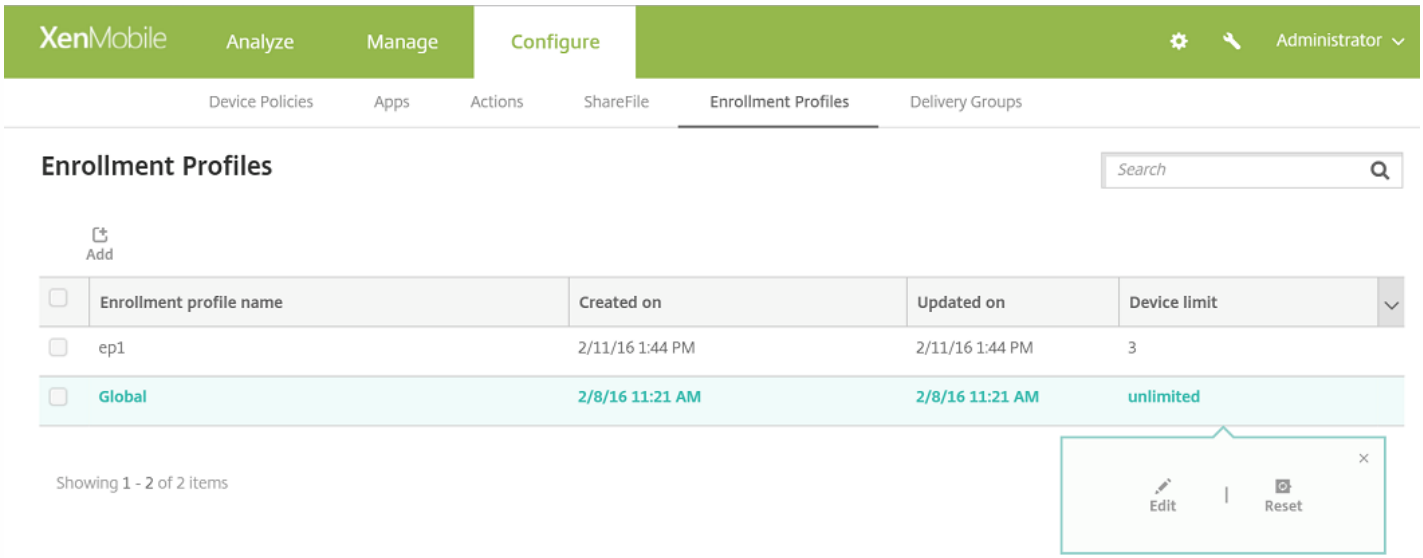
Vous pouvez limiter le nombre d'appareils qu'un utilisateur peut inscrire sous **Configurer > Profils d'inscription** dans la console XenMobile, en modes de serveur ENT, MDM et MAM. Ces limitations peuvent s'appliquer de manière globale ou par groupe de mise à disposition. Vous pouvez créer plusieurs profils d'inscription et les associer à différents groupes de mise à disposition.

Si vous ne définissez aucune limite, les utilisateurs peuvent inscrire un nombre illimité d'appareils. Cette fonctionnalité est uniquement prise en charge sur les appareils iOS et Android. Pour de plus amples informations sur l'inscription d'appareils Windows, consultez la section Appareils Windows.

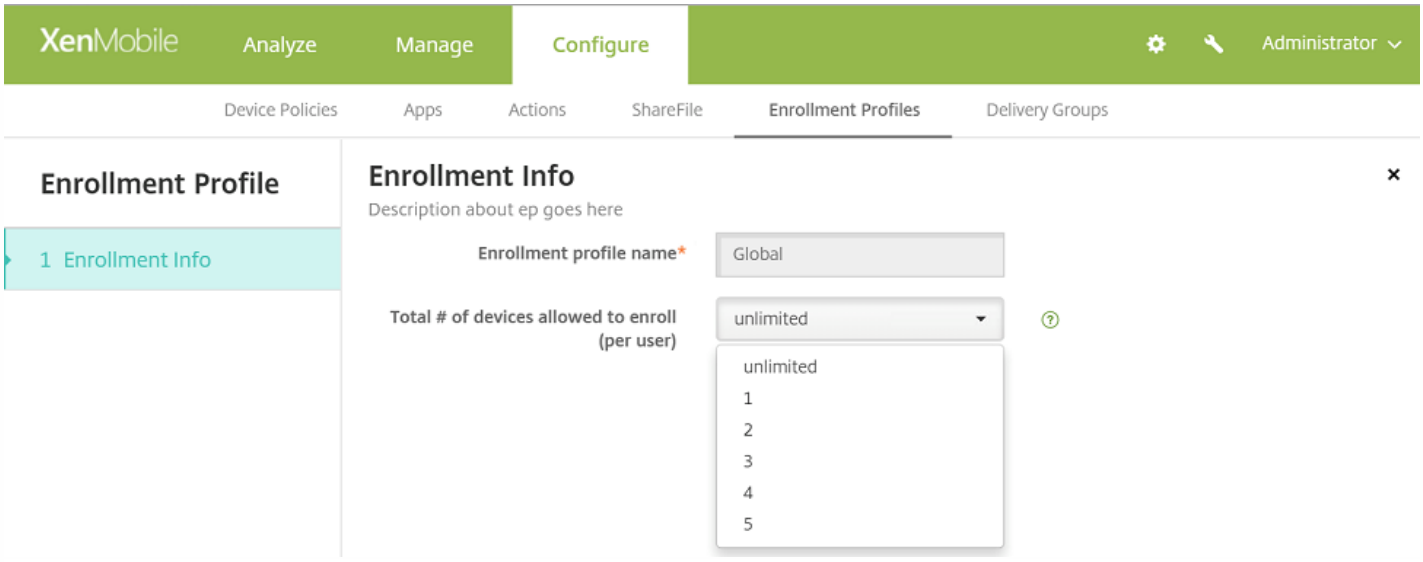
Pour configurer une limite d'inscription d'appareils globale

1. Accédez à **Configurer > Profils d'inscription**.

2. Cliquez sur **Global** et sélectionnez **Modifier**.



L'écran **Infos d'inscription** s'affiche et **Global** est renseigné automatiquement en tant que nom de profil. À ce stade, vous pouvez sélectionner le nombre total d'appareils que les utilisateurs sont autorisés à inscrire. Cette limitation s'appliquera à tous les utilisateurs inscrits auprès de XenMobile.

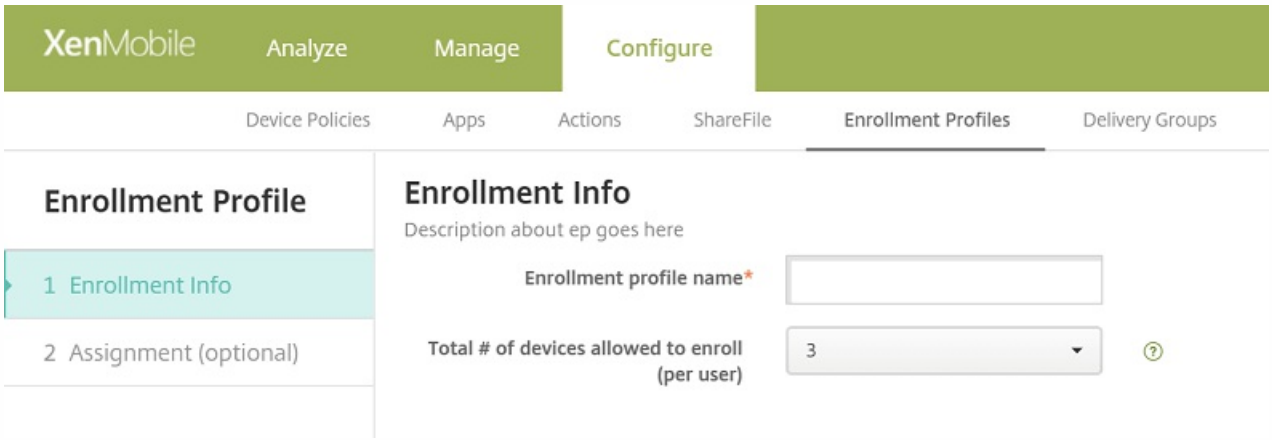


Pour configurer une limite d'inscription d'appareils pour un groupe de mise à disposition

1. Accédez à **Configurer** > **Profils d'inscription** > **Ajouter**.

   L'écran **Infos d'inscription** s'affiche.

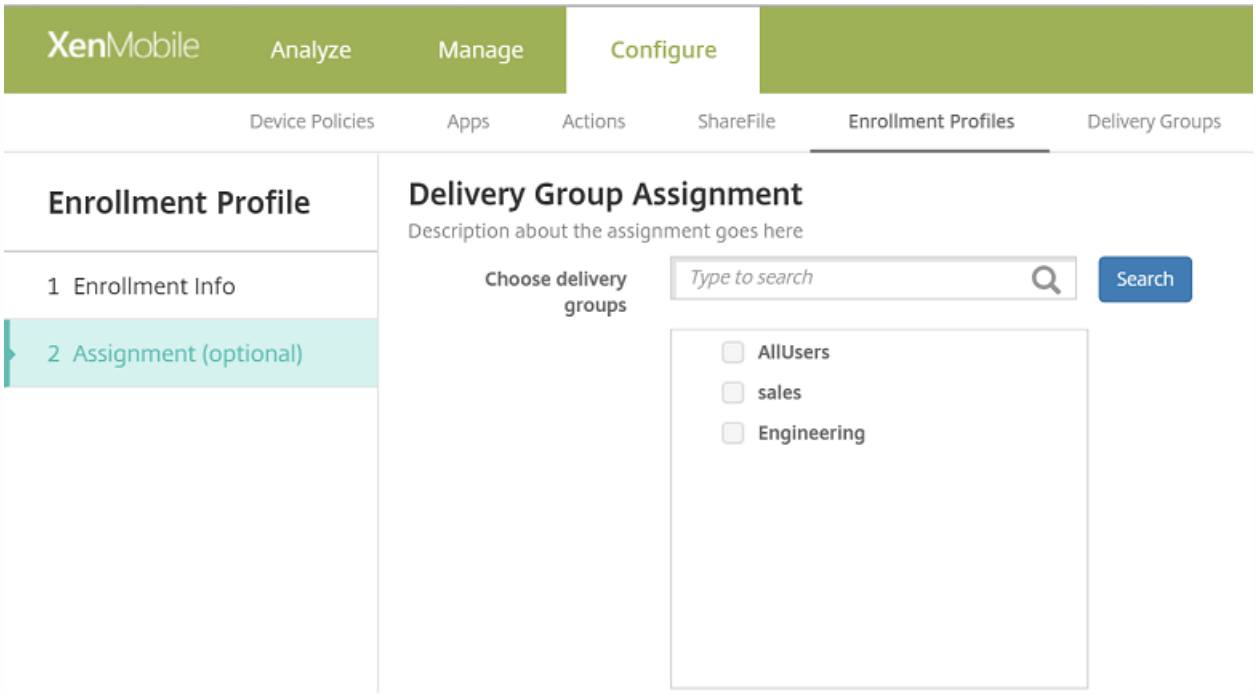
2. Entrez un nom pour le nouveau profil d'inscription, puis sélectionnez le nombre d'appareils que les membres de ce profil sont autorisés à inscrire.



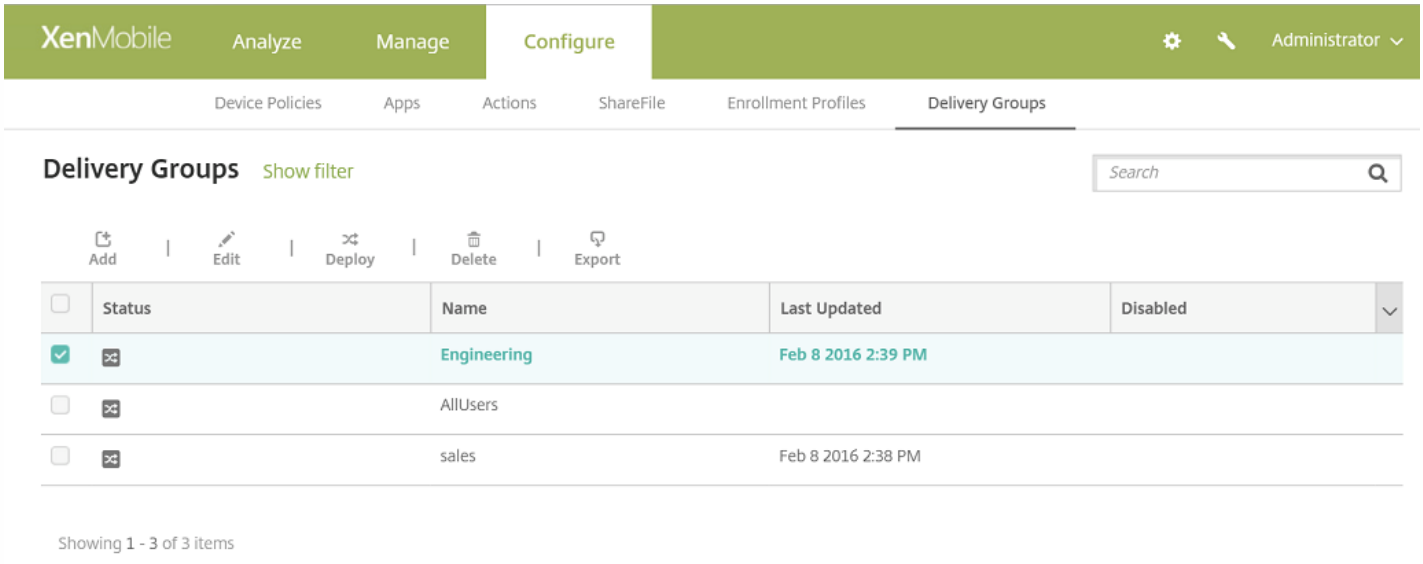
3. Cliquez sur **Suivant**.

   L'écran **Attribution de groupes de mise à disposition** s'affiche.

4. Sélectionnez les groupes de mise à disposition auxquels la limite d'inscription d'appareils doit s'appliquer, puis cliquez sur **Enregistrer**.

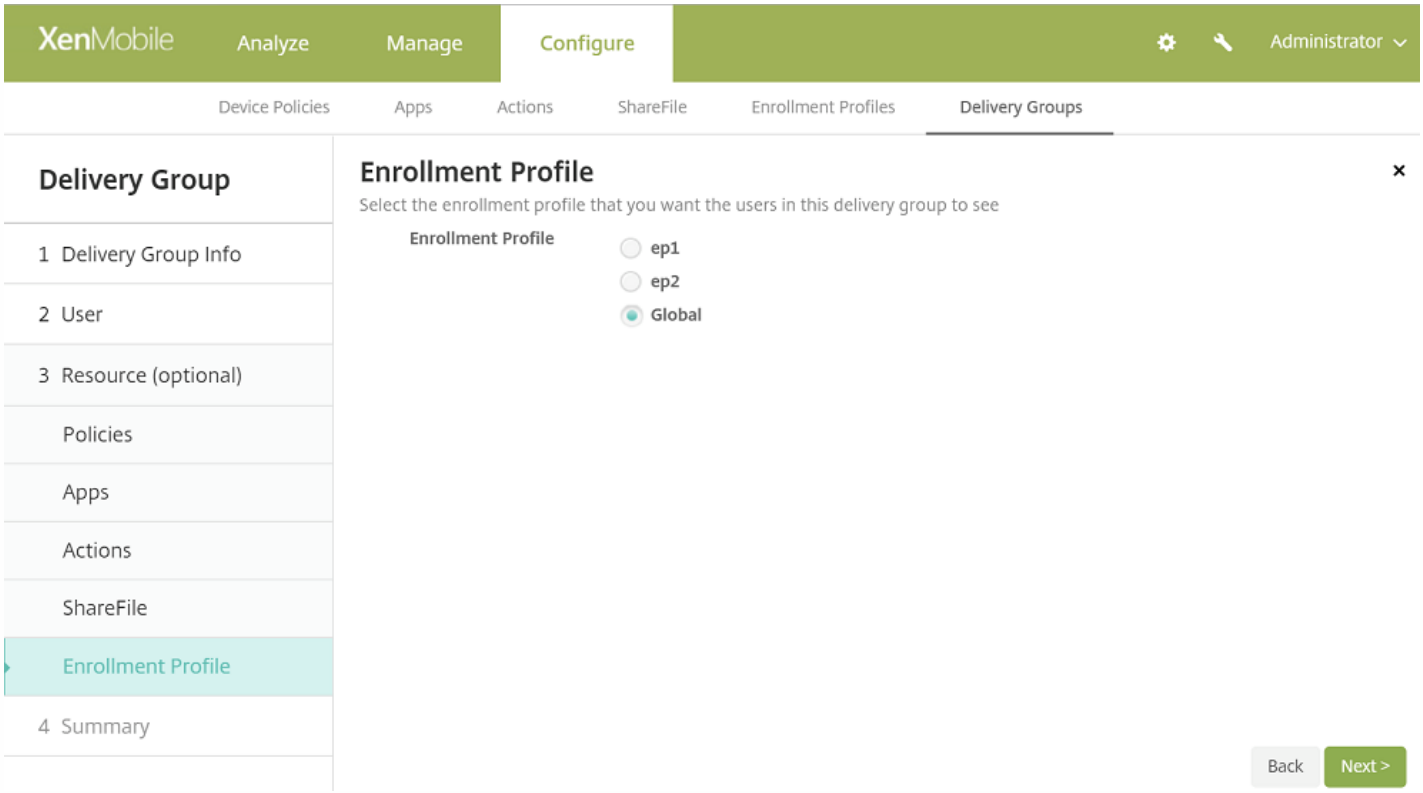


Si vous souhaitez modifier le profil d'inscription d'un groupe de mise à disposition ultérieurement, accédez à **Configurer > Groupes de mise à disposition**. Sélectionnez le groupe en question, puis cliquez sur **Modifier**.



L'écran **Profil d'inscription** s'affiche.

5. Sur cet écran, sélectionnez le profil d'inscription que vous souhaitez appliquer à ce groupe de mise à disposition, puis cliquez sur **Suivant** pour afficher et enregistrer vos modifications.



Expérience utilisateur avec une limite d'inscription d'appareils

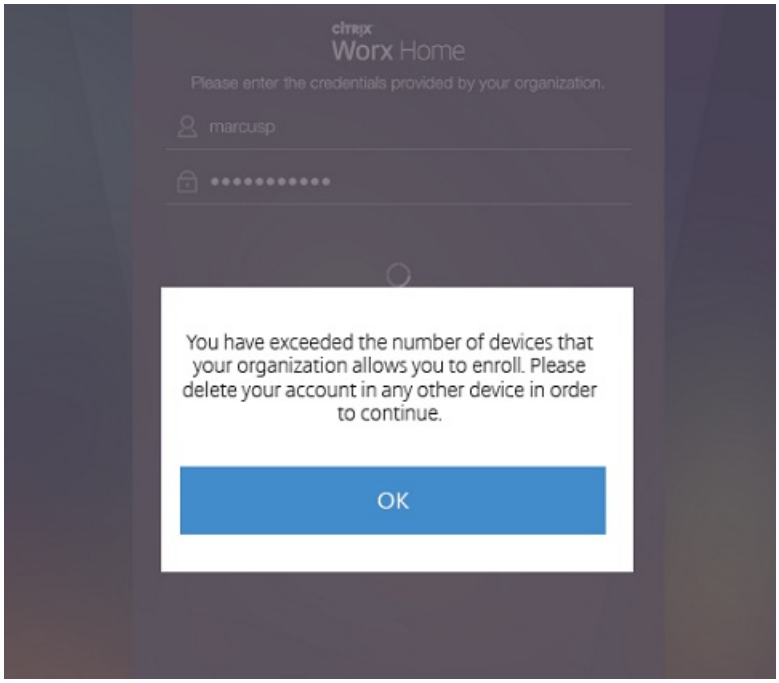
Lorsque vous définissez la limite d'inscription d'appareils et que les utilisateurs tentent d'inscrire un appareil, ils procèdent comme suit :

1. Ils se connectent à Worx Home.

2. Ils entrent une adresse de serveur pour s'inscrire.

3. Ils entrent leurs informations d'identification.

4. Si la limite d'appareils est atteinte, un message d'erreur s'affiche, indiquant à l'utilisateur que le nombre maximal d'enregistrements d'appareils est dépassé et qu'il doit contacter un administrateur.



L'écran d'inscription de Worx Home s'affiche à nouveau.

Actions de verrouillage et d'effacement des applications en mode MAM uniquement

Aug 22, 2016

En créant des actions, vous définissez sur l'appareil d'un utilisateur des réponses automatiques à certains déclencheurs, tels que l'installation d'une application interdite ou la suppression d'un utilisateur d'Active Directory. Vous pouvez également envoyer des notifications aux utilisateurs afin de résoudre un problème avant qu'une action plus sérieuse ne devienne nécessaire.

À compter de XenMobile 10.3.5, 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. Auparavant, seule la catégorie événement proposait cette fonctionnalité.

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**.

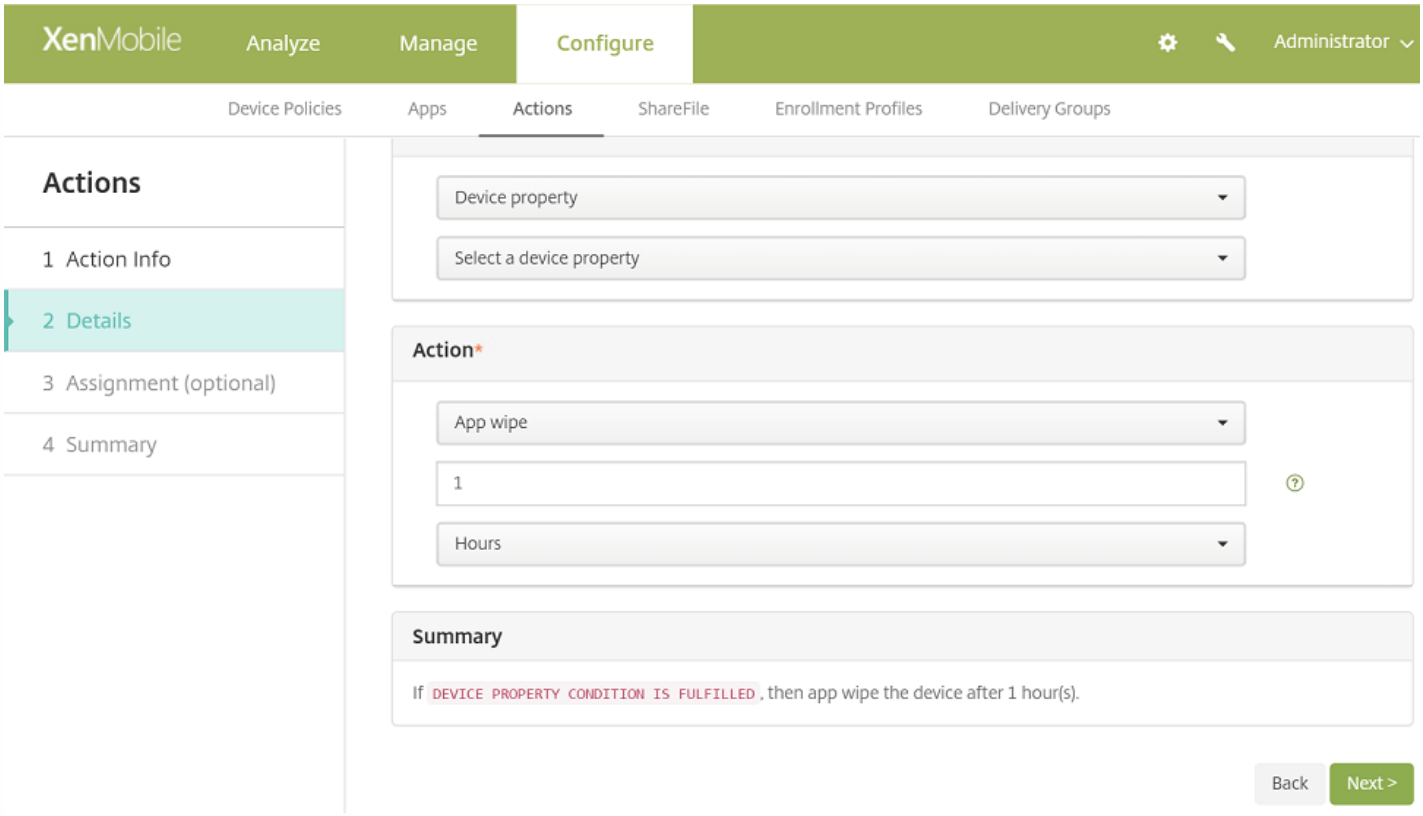
3. Sur la page **Informations sur l'action**, entrez un nom pour l'action et une description facultative.

4. Sur la page **Détails de l'action**, sélectionnez le déclencheur de votre choix.

5. Sous **Action**, sélectionnez **Effacement des applications** ou **Mode kiosque**.

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 délai donne aux utilisateurs la possibilité de tenter de résoudre un problème avant l'exécution de l'action. Vous pouvez en apprendre davantage sur les actions Effacement des applications et Mode kiosque dans la rubrique Rôles et autorisations RBAC.

> ## Remarque
>
> 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**.

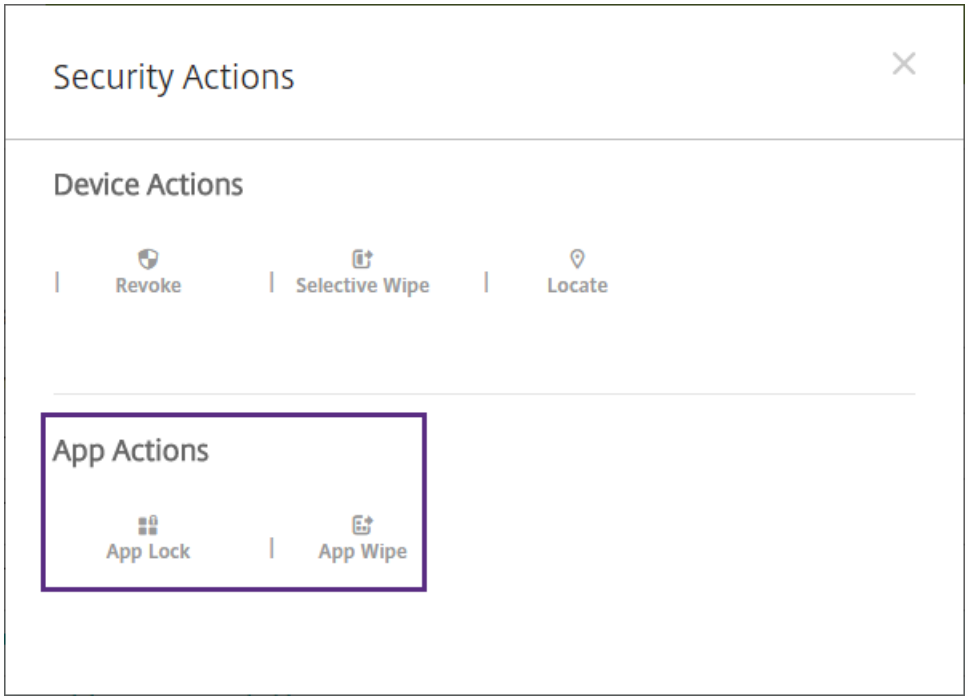
8. Cliquez sur **Enregistrer**.

Pour verrouiller, déverrouiller, effacer ou annuler l'effacement d'une application :

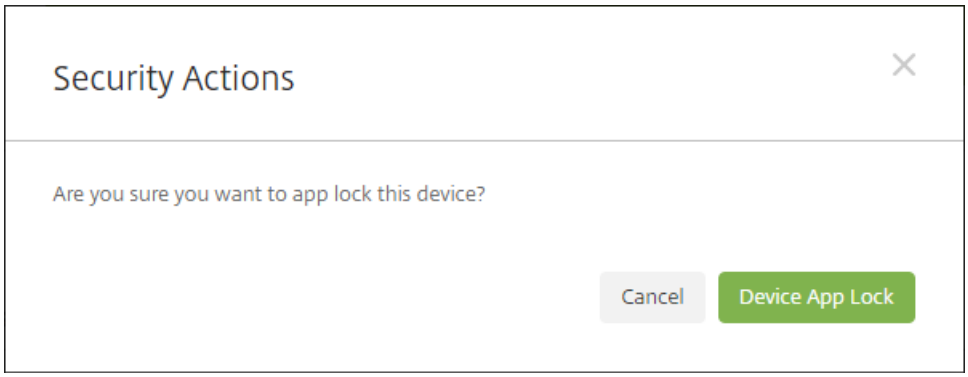
1. Accédez à **Gérer > Appareils**, sélectionnez l'appareil, et cliquez sur **Sécurisé**.

2. Dans la boîte de dialogue **Actions de sécurisation**, cliquez sur une action.

> Remarque : vous pouvez également utiliser cette boîte de dialogue pour vérifier l'état de l'appareil d'un utilisateur dont vous savez qu'il 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 des utilisateurs sont actuellement verrouillées ou effacées.

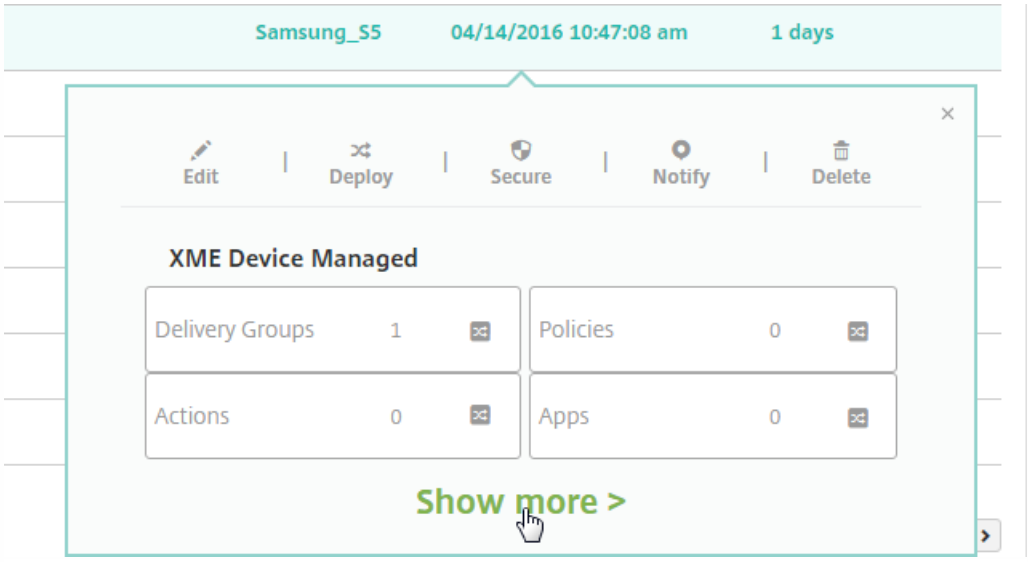


3. Confirmez l'action.

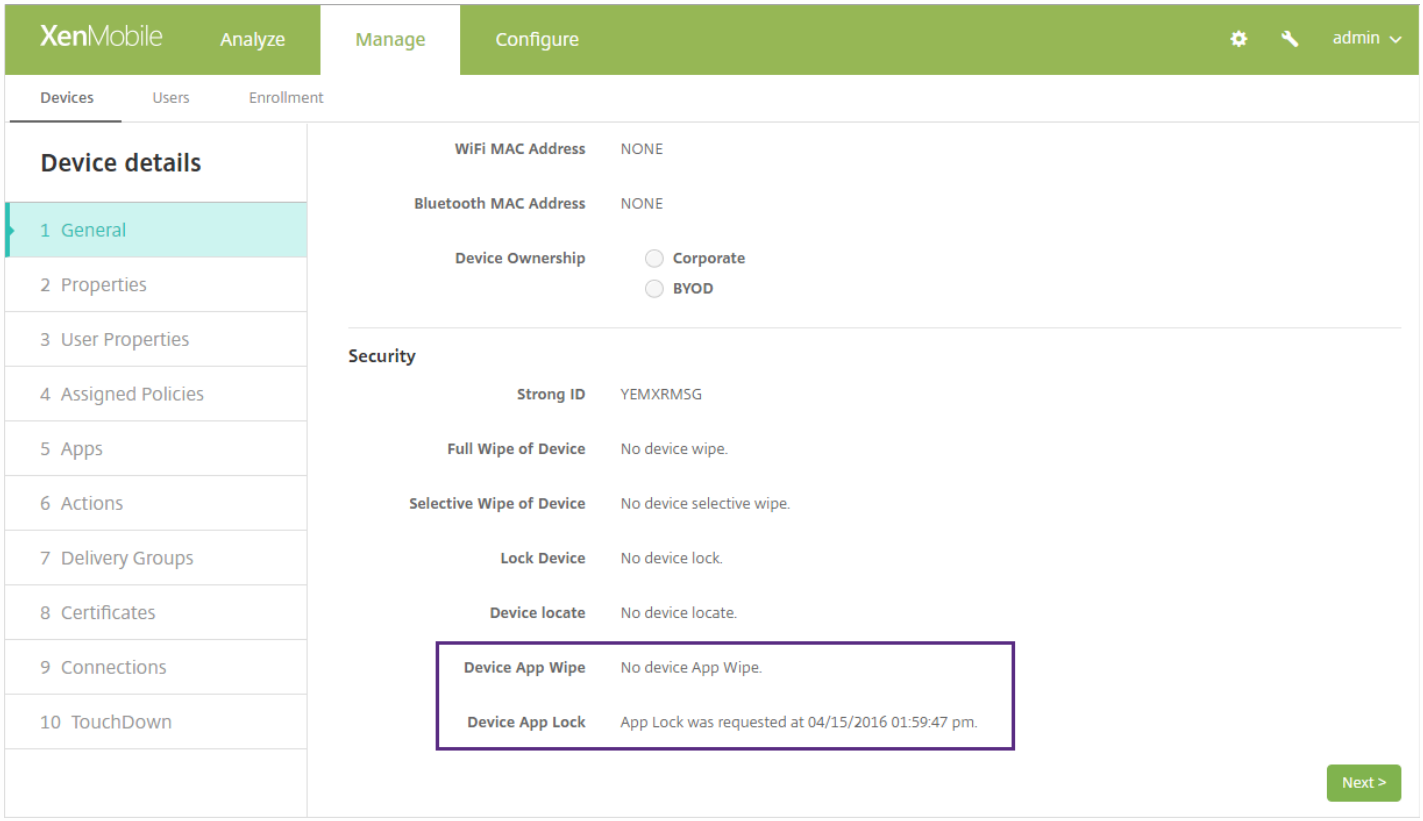


Pour vérifier l'état de verrouillage ou d'effacement d'une application :

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**.



API de services REST en mode MAM uniquement

Jul 27, 2016

Pour les appareils en mode MAM exclusif, vous pouvez utiliser tout client REST et l'API REST XenMobile pour appeler les services REST exposés au travers de la console XenMobile. L'API n'exige pas de connexion à la console XenMobile pour appeler les services décrits dans cette section.

Vous pouvez appeler les services d'API REST à l'aide du client REST.

Les nouvelles API REST vous permettent d'effectuer les opérations suivantes :

- **Envoyer une URL d'invitation et un code PIN à usage unique**

  Vous pouvez utiliser l'API REST XenMobile afin de permettre aux utilisateurs de demander un accès BYOD par le biais d'un portail en libre-service. Une fois cette demande approuvée, le système appelle le serveur XenMobile et envoie une demande d'exécution des opérations suivantes :

  - Génération et envoi d'une URL d'invitation d'inscription à l'utilisateur.

  - Génération et envoi d'un code PIN à usage unique à l'utilisateur.

  Remarque : cette fonctionnalité est prise en charge pour les appareils iOS et Android, mais pas pour les appareils Windows.

- **Envoyer la commande Mode kiosque ou Effacement des applications sur des appareils**

  Vous pouvez utiliser l'API XenMobile pour rechercher des appareils qui appartiennent à un utilisateur en recherchant l'intégralité des appareils, par exemple pour effacer toutes les applications présentes sur l'appareil ou pour verrouiller les applications.

Le reste de cet article répertorie les API d'appareils et les API d'inscription avec code PIN à usage unique disponibles à partir de XenMobile 10.3.5. Pour accéder à la documentation complète des API actuellement disponibles, téléchargez le PDF API REST XenMobile : références.

APIs de la machine

- Obtenir des appareils en fonction de filtres
- Obtenir des informations sur un appareil en fonction de l'ID
- Obtenir les applications d'un appareil en fonction de l'ID de l'appareil
- Obtenir les actions d'un appareil en fonction de l'ID de l'appareil
- Obtenir les groupes de mise à disposition d'un appareil en fonction de l'ID de l'appareil
- Obtenir l'inventaire logiciel géré d'un appareil en fonction de l'ID de l'appareil
- Obtenir les stratégies d'un appareil en fonction de l'ID de l'appareil
- Obtenir l'inventaire logiciel d'un appareil en fonction de l'ID de l'appareil
- Obtenir les coordonnées GPS d'un appareil en fonction de l'ID de l'appareil
- Envoyer une notification à une liste d'appareils/utilisateurs
- Autoriser une liste d'appareils
- Contourner le verrouillage d'activation sur une liste d'appareils

- Mode kiosque sur une liste d'appareils
- Effacer les applications sur une liste d'appareils
- Verrouiller le conteneur sur une liste d'appareils
- Annuler le verrouillage du conteneur sur une liste d'appareils
- Déverrouiller le conteneur sur une liste d'appareils
- Annuler le déverrouillage du conteneur sur une liste d'appareils
- Réinitialiser le mot de passe du conteneur sur une liste d'appareils
- Annuler la réinitialisation du mot de passe du conteneur sur une liste d'appareils
- Exclure une liste d'appareils
- Rechercher une liste d'appareils
- Annuler la recherche d'une liste d'appareils
- Activer le suivi GPS sur une liste d'appareils
- Annuler le suivi GPS sur une liste d'appareils
- Verrouiller une liste d'appareils
- Annuler le verrouillage d'une liste d'appareils
- Déverrouiller une liste d'appareils
- Annuler le déverrouillage d'une liste d'appareils
- Déployer une liste d'appareils
- Demander une mise en miroir AirPlay sur une liste d'appareils
- Annuler la demande de mise en miroir AirPlay sur une liste d'appareils
- Arrêter la mise en miroir AirPlay sur une liste d'appareils
- Annuler l'arrêt de la mise en miroir AirPlay sur une liste d'appareils
- Effacer toutes les restrictions sur une liste d'appareils
- Annuler l'effacement de toutes les restrictions sur une liste d'appareils
- Révoquer une liste d'appareils
- Faire sonner une liste d'appareils
- Annuler la sonnerie sur une liste d'appareils
- Effacer une liste d'appareils
- Annuler l'effacement sur une liste d'appareils
- Effacer les données d'entreprise sur une liste d'appareils
- Annuler l'effacement des données d'entreprise sur une liste d'appareils
- Effacer la carte SD sur une liste d'appareils
- Annuler l'effacement de la carte SD sur une liste d'appareils
- Obtenir toutes les propriétés connues de l'appareil
- Obtenir toutes les propriétés utilisées de l'appareil
- Récupérer toutes les propriétés d'un appareil en fonction de l'ID de l'appareil
- Mettre à jour toutes les propriétés d'un appareil en fonction de l'ID de l'appareil
- Ajouter ou mettre à jour une propriété d'appareil en fonction de l'ID de l'appareil
- Supprimer une propriété d'appareil en fonction de l'ID de l'appareil
- Récupérer l'état du MDM iOS d'un appareil en fonction de l'ID de l'appareil
- Générer un code PIN

API d'inscription avec code PIN à usage unique

- Obtenir les modes d'inscription

- Obtenir les informations d'inscription
- Déclencher une notification d'inscription
- Créer une invitation d'inscription
- Obtenir les enregistrements d'inscriptions en fonction d'un filtre

Problèmes connus et problèmes résolus dans XenMobile 10.3.5

Aug 22, 2016

Les problèmes suivants sont connus ou ont été résolus dans XenMobile 10.3.5 :

- Limitation : les fonctionnalités du nouveau mode MAM exclusif, telles que l'authentification basée sur les certificats, les actions de mode kiosque et d'effacement des applications, et les API MAM, ne sont pas disponibles pour Windows Phone.
- Lorsque des utilisateurs se réinscrivent dans Worx Home plusieurs fois, puis qu'ils tentent d'installer une application à partir du WorxStore, une erreur s'affiche indiquant que l'application a été supprimée. Pour contourner le problème, vous pouvez supprimer l'appareil dans la console XenMobile dans **Gérer > Appareils** et demander aux utilisateurs de se réinscrire. [#611172]
- Pour pouvoir inscrire des appareils Windows, le certificat d'écoute SSL doit être un certificat SSL. L'inscription échoue si vous avez chargé un certificat SSL auto-signé. [#618390]
- Une fois que vous avez atteint le nombre maximal d'inscriptions d'appareils dans la console XenMobile, le message d'erreur correspondant ne s'affiche pas sur l'appareil, mais l'inscription est bien empêchée. [#623475]
- Lorsque les utilisateurs s'inscrivent auprès de XenMobile via un compte Active Directory Azure, même après effacement ou révocation de l'appareil, ils peuvent s'inscrire à nouveau sans autorisation. Il s'agit d'un problème de tiers. [#628865]
- Lorsque vous supprimez un appareil iOS à partir de la console XenMobile, il peut arriver que, lorsque les utilisateurs réinscrivent l'appareil en mode XenMobile Enterprise (MAM et MDM), l'inscription en mode MAM échoue. [#629021]
- Lorsque vous désactivez l'option permettant de renouveler les certificats dans le serveur XenMobile, les utilisateurs peuvent tout de même renouveler un certificat expiré dans Worx Home. [#630894]
- Certaines licences VPP ont des ID négatifs, par exemple -123441212, ce qui empêche la distribution des applications publiques. [#631443]
- Si des informations d'identification Google Play sont configurées avec un ID d'appareil non valide, lorsque vous ajoutez une application provenant d'un magasin d'applications public pour Google Play et que vous cliquez pour rechercher l'application dans le magasin Google Play, la recherche échoue ou affiche des résultats de recherche incorrects. [#633845]
- Vous ne pouvez pas trouver votre ID Android en entrant *#*#8255#*#*sur votre téléphone, comme indiqué sur la page **Paramètres > Identifiants Google Play** de XenMobile. Utilisez une application d'ID d'appareil à partir du Google Play Store pour rechercher votre ID d'appareil. [#633854]
- Dans la console XenMobile, **Paramètres > Contrôle d'accès basé sur rôle** comporte les problèmes suivants relatifs aux paramètres par défaut.
  - Dans la console XenMobile pour les déploiements de cloud, l'autorisation **Assistant d'inscription d'appareils partagés** est définie par défaut pour le rôle Admin. Cette autorisation ne doit pas être définie par défaut. [#638069]
  - L'autorisation de fonctionnalités de la console **Appareil exclu** est obsolète et ne doit pas s'afficher. [#638303]
  - Dans la console XenMobile pour les déploiements sur site, les fonctionnalités suivantes ne sont pas sélectionnées par défaut pour le rôle Admin. N'oubliez pas de sélectionner ces paramètres selon vos besoins pour le rôle Administrateur par défaut ou tout rôle que vous avez créé à partir du modèle Admin. [#638314]

    Verrouiller le conteneur
    Déverrouiller le conteneur

Réinitialiser le mot de passe du conteneur
Ne pas utiliser le verrouillage d'activation
Appelle l'appareil

- Dans la console XenMobile pour les déploiements sur cloud et sur site, les fonctionnalités suivantes ne sont pas sélectionnées par défaut pour le rôle Admin. N'oubliez pas de sélectionner ces paramètres selon vos besoins pour le rôle Administrateur par défaut ou tout rôle que vous avez créé à partir du modèle Admin. [#638322]

  Demander la mise en miroir AirPlay
  Arrêter la mise en miroir AirPlay

- L'authentification unique de ShareFile échoue en raison de problèmes liés à la durée de synchronisation qui se produisent entre XenMobile et Hyper-V. [#588249]
- Lorsque vous activez l'imbrication dans vos paramètres LDAP pour XenMobile et que vous configurez des groupes de mise à disposition et des paramètres RBAC avec des groupes de domaines correspondants, si vous supprimez ultérieurement le domaine dans vos paramètres LDAP, les informations sur les groupes imbriqués sont conservées dans la base de données. [#590363]
- Lorsque vous supprimez un utilisateur dans Active Directory, cet utilisateur peut toujours ouvrir le WorxStore et s'abonner à des applications. [#592825]
- Après avoir vérifié la présence de mises à jour pour les applications d'un magasin d'applications public dans la console XenMobile, Worx Home met à jour ces applications vers leur version la plus récente, mais ces applications s'affichent encore dans la liste des mises à jour en attente sur l'appareil. [#593034]
- Lorsque les utilisateurs reçoivent des invitations de calendrier depuis un compte Exchange dans WorxMail, l'invitation n'est pas reçue instantanément, comme elle le devrait. [#594542]
- Lorsqu'un appareil iOS est enregistré dans le Device Enrollment Program (DEP), le téléchargement de Worx Home sur l'appareil iOS peut échouer. [#595822]
- Des problèmes d'écart temporel peuvent se produire avec le serveur XenMobile, par exemple un échec de l'authentification unique (SSO) SAML pour ShareFile, si vous ne configurez pas un client NTP.

  Remarque : effectuez la configuration suivante pour activer le correctif :

  1. Ouvrez une session dans l'interface de ligne de commande XenMobile de l'hyperviseur sur lequel vous avez installé XenMobile, à savoir Citrix XenServer ou VMware ESXi.

  2. Accédez à **[2] System**.

  3. Accédez à **[3] Set NTP Server** et fournissez les détails nécessaires sur le serveur NTP.

  4. Redémarrez le serveur.

  Important : si votre système est configuré en mode cluster, effectuez la configuration ci-dessus sur chaque nœud. [#597757]

- Lorsque les utilisateurs tentent de supprimer une application ou un lien Web à partir de Worx Home, le message d'erreur suivant s'affiche : Worx Home n'a pas réussi à se connecter. [#599934]
- L'inscription basée sur code PIN peut échouer si plusieurs codes PIN sont en attente pour les utilisateurs. [#600264]
- Lorsque vous importez des licences VPP dans XenMobile, si certaines d'entre elles ont été remboursées par Apple, elles sont considérées comme valides dans XenMobile alors qu'elles ne le sont pas. Par conséquent, les utilisateurs ne peuvent

pas installer d'applications sur des appareils iOS via le WorxStore. [#601845]

- Lorsque vous créez une action, si vous donnez à cette action le même nom que celui que porte l'une des stratégies ou des applications de votre appareil, il est impossible de la supprimer ultérieurement. [#602958]
- Lors de l'utilisation d'un Samsung Galaxy Note 5 pour accéder au WorxStore, le WorxStore s'affiche en mode tablette sur une partie de l'écran seulement, plutôt qu'en mode téléphone comme il le devrait. [#604295]
- Lorsque vous créez une invitation d'inscription nécessitant un code PIN à usage unique à des destinataires qui se trouvent à la racine d'un groupe Active Directory, les groupes imbriqués reçoivent l'invitation, mais l'inscription échoue pour les groupes imbriqués de troisième niveau. Ce problème se produit même lorsque vous envoyez une invitation à un groupe de troisième niveau. [#603434]
- Lorsque vous disposez d'un type de licence Avancé et que vous cochez la case Inscription requise dans la console XenMobile, les utilisateurs peuvent s'enregistrer en mode MAM exclusif et accéder au WorxStore. [#604113]
- Les propriétés **$user.dnsroot** et **$user.netbiosename** sont utilisées dans des macros pour déployer des stratégies à l'aide de propriétés utilisateur. Les propriétés utilisateur **dnsroot** et **netbiosename** ont été rendues obsolètes dans XenMobile 10.1. Ce correctif permet de réactiver ces propriétés dans XenMobile 10.3. [#604240]
- Une erreur de profil non valide se produit lorsque vous essayez de configurer le programme Device Enrollment Program (DEP) iOS dans la console XenMobile. Il s'agit d'un problème de tiers. [#607143]
- Dans les paramètres de Personnalisation du client de la console XenMobile, le nom du magasin prend uniquement en charge les caractères alphanumériques (ASCII) ; si vous remplacez le nom par défaut par des caractères non ASCII, les utilisateurs ne peuvent pas se connecter à Worx Home. [#609535]
- Une fois que vous avez configuré LDAP avec des noms uniques de base différents pour les utilisateurs et les groupes, après la mise à jour vers XenMobile 10.3, vous ne pouvez pas ajouter de nouveaux groupes à des groupes de mise à disposition. [#610014]
- Lorsque vous configurez une stratégie Wi-Fi, même si le calendrier de déploiement est défini sur **Uniquement lorsque le déploiement précédent a échoué**, la stratégie Wi-Fi est transmise aux appareils à chaque fois qu'ils se connectent. [#610325]
- Ce correctif résout une vulnérabilité de type « zero-day » dans Java, qui affecte la désérialisation d'objet dans Apache Commons Collections. [#610427]
- Lorsque vous définissez un rôle RBAC pour permettre aux utilisateurs de se connecter à la console XenMobile à l'aide d'un nom d'utilisateur au format sAMAccountName, ils sont redirigés vers le portail en libre-service. [#610915]
- Après la première installation de XenMobile 10.1 ou la mise à niveau de XenMobile 9 en mode MAM et MDM vers XenMobile 10.1, dans la console XenMobile, sous **Gérer** > **Appareil**, après l'actualisation des groupes de mise à disposition et des stratégies, le nombre de groupes de mise à disposition et de stratégies est incorrect. [#611630]
- Lorsque vous avez plus de 10 domaines LDAP configurés dans des versions de XenMobile antérieures à XenMobile 10.1, dans XenMobile 10 et après la mise à niveau vers XenMobile 10.1, seuls 10 domaines s'affichent dans la console XenMobile. [#613502]
- Vous ne pouvez pas ajouter ni mettre à jour une application MDX si vous ne définissez pas pour les utilisateurs un rôle RBAC qui comprend des autorisations pour les applications publiques. [#614496]
- Si vous modifiez le nom d'instance par défaut lors de la configuration initiale de XenMobile, lorsque vous effectuez la mise à niveau vers la version 10.3, cette modification n'est pas conservée. Par conséquent, les appareils inscrits ne peuvent pas se connecter. [#614604]
- Lorsque vous configurez LDAP avec une limite de verrouillage, après la mise à niveau vers XenMobile 10.3, lorsqu'un nouvel utilisateur se trouvant dans le même domaine inscrit un appareil dans Worx Home à l'aide d'informations d'identification non valides, telles qu'un mot de passe mal orthographié, Worx Home cesse de répondre et SQL Server se bloque. [#615179]
- Une fois la mise à jour de XenMobile 10.1 vers XenMobile 10.3 effectuée, vous ne pouvez pas envoyer d'invitation d'inscription aux utilisateurs à l'aide de l'option **Ajouter une invitation**. [#616584]

- Ce correctif active la prise en charge d'une racine multidomaine LDAP dans une forêt unique. Cette prise en charge était disponible dans XenMobile 9, mais ne l'était plus dans XenMobile 10.x. [#616633, #618899, #620541]
- Lorsque vous configurez une stratégie de restriction iOS dans la console XenMobile et que vous modifiez la valeur par défaut de l'option **Autoriser l'utilisateur à supprimer la stratégie**, cette valeur n'est pas enregistrée. [#616751]
- Lorsqu'un serveur dispose d'un nom d'instance personnalisé, après la mise à jour de XenMobile 10.1 vers XenMobile 10.3, les utilisateurs ne peuvent pas inscrire d'appareils. [#616954]
- Lorsque les utilisateurs inscrivent un appareil DEP en mode XenMobile Enterprise, s'ils réinitialisent leur propre appareil à ses paramètres d'usine (effacement complet) puis le réinscrivent, Worx Home n'est pas automatiquement déployé sur l'appareil, comme il le devrait. [#616986]
- Il arrive que le serveur XenMobile passe en mode de récupération au bout d'environ 20 à 30 minutes en raison d'un problème connu lié à JRE (Java Runtime Environment). Après le redémarrage du serveur, le problème se produit à nouveau. [#616992]
- Sur les appareils iOS et Android, les utilisateurs ne peuvent pas ouvrir le WorxStore à partir de Worx Home si vous supprimez le **nom du magasin** dans **Paramètres > Personnalisation du client**. [#617003]
- Lorsque vous chargez un fichier .ipa sur la console XenMobile, l'erreur « icône introuvable » s'affiche. [#617195]
- Lorsque vous déployez une stratégie VPN avec les options Activer Per App VPN et Correspondance d'application à la demande activée définies sur **ON** ainsi qu'une stratégie Attributs d'application pour une application gérée sur laquelle la stratégie VPN est appliquée, lorsque les utilisateurs ouvrent l'application gérée, la connexion VPN n'est pas lancée automatiquement comme elle le devrait. Les utilisateurs doivent activer le paramètre **Connecter à la demande** manuellement sur leur appareil. [#617803]
- Dans la console XenMobile, sous **Gérer** > **Utilisateurs**, il existe un délai dans l'affichage des utilisateurs existants. Par conséquent, vous ne pouvez pas effectuer d'opérations sur les utilisateurs locaux. [#618094]
- XenMobile 10.x prend en charge le LDAP multidomaine dans une forêt Active Directory unique. [#618375]
- Lorsque vous envoyez une invitation d'inscription et entrez du code HTML, les utilisateurs reçoivent un e-mail en texte brut sans aucun lien HTML. [#618504]
- Lorsque les utilisateurs chargent un fichier .appx en tant qu'application d'entreprise pour des appareils Windows 10, cette application n'est pas déployée sur les appareils. [#628611]
- Les utilisateurs ne peuvent pas inscrire d'appareils Windows 10 dans XenMobile en mode MDM si leur ID utilisateur ou leur champ de mot de passe contient des caractères spéciaux. [#618870]
- Sur iPad, XenMobile 10.3 effectue toujours les actions de suppression (ou de retrait) en premier, quel que soit l'ordre que vous avez défini dans la console XenMobile. [#620459]
- Lorsque vous mettez à jour une application d'entreprise iOS dans la console XenMobile et que le fichier .ipa possède un ID de bundle différent, lorsque vous déployez une application mise à jour sur les appareils, des problèmes de déploiement des applications se produisent sur les appareils. [#621009]
- Lors de l'ajout d'informations d'identification Google Play dans le serveur XenMobile, l'erreur « ID d'appareil non valide » s'affiche et vous ne pouvez pas vous connecter. [#623182]
- Si vous supprimez dans XenMobile une application que vous avez importée à l'aide du programme VPP, l'application n'est pas automatiquement importée à nouveau tant que vous n'avez pas supprimé et rajouté le jeton. [#623403]
- Si vous supprimez ou effacez les données d'entreprise d'un appareil, toute licence VPP associée à cet appareil n'est pas automatiquement libérée. Par conséquent, vous devez manuellement dissocier la licence pour pouvoir l'utiliser sur un autre appareil. [#623716]

À propos du serveur XenMobile 10.3

Oct 17, 2016

Vous pouvez effectuer la mise à niveau de XenMobile 10,1 vers XenMobile 10.3 dans la console XenMobile. Pour effectuer la mise à niveau, vous devez utiliser xms_10.3.0.824.bin. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Gestion des versions**. Cliquez sur **Mettre à niveau**, puis chargez le fichier xms_10.3.0.824.bin. Pour plus d'informations sur la mise à niveau de la console, consultez la rubrique Mise à niveau de XenMobile.

Pour procéder à une nouvelle installation de XenMobile 10.3, consultez la section Installation de XenMobile.

> ## Remarque
>
> Le client d'assistance à distance n'est pas disponible dans XenMobile Cloud versions 10.x pour Windows CE et pour appareils Samsung Android.

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, consultez le manuel de déploiement de XenMobile.

Les fonctionnalités suivantes sont nouvelles dans XenMobile 10.3.

Nouvelle apparence de la console

XenMobile 10.3 présente un nouvel aspect. La console a été mise à jour avec de nouvelles couleurs et polices, de nouveaux onglets et des fonctionnalités améliorées.

- L'onglet Tableau de bord des versions précédentes de la console de l'appareil a été déplacé dans le nouvel onglet Analyser, qui comprend également le nouvel onglet Rapports. Pour plus de détails, consultez la section Rapports.
- L'onglet Gérer comprend maintenant le nouvel onglet Utilisateurs où vous pouvez gérer les utilisateurs et groupes locaux.
- L'onglet Configurer comprend maintenant le nouvel onglet ShareFile où vous pouvez définir les paramètres pour la connexion au compte ShareFile.
- Vous pouvez accéder aux Paramètres, anciennement sous l'onglet Configurer, en cliquant sur l'icône d'engrenage dans le coin supérieur droit de la console.
- L'onglet Support s'ouvre désormais dans le même onglet que la console plutôt que dans un nouvel onglet.

Prise en charge de nouvelles plates-formes

XenMobile 10.3 prend désormais en charge les plates-formes suivantes :

- Mac OS X
- Android HTC
- Android Sony
- Samsung SEAMS
- Windows Mobile/CE

- Windows Phone 10 : gestion des appareils en mode XenMobile MDM et XenMobile Enterprise.
- Windows 10 Desktop/Tablet : gestion des appareils en mode XenMobile MDM et XenMobile Enterprise.

Pour obtenir des instructions détaillées sur l'inscription d'appareils Mac OS X, consultez la section Appareils Mac OS X.

Pour obtenir des instructions détaillées sur l'inscription d'appareils Windows 10, consultez la section Appareils Windows.

> **Remarque**
>
> La prise en charge des appareils Symbian est obsolète dans XenMobile 10.3.

Stratégies d'appareil

Les nouvelles stratégies MDM suivantes sont disponibles dans XenMobile 10.3 :

- **Mode kiosque**. Permet de définir une liste d'applications dont l'exécution est autorisée ou interdite sur un appareil. Disponible sur iOS et Android. 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.
- **Utilisation des réseaux.** Permet de 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. Les règles s'appliquent uniquement aux applications gérées. Disponible sur iOS.
- **Gestionnaire de connexions**. Permet de configurer comment les applications se connectent à Internet ou à un réseau privé. Ces paramètres ne fonctionnent que pour les Pocket PC (appareils avec écran tactile). Disponible sur Windows Mobile/CE.
- **Copier les applications dans le conteneur Samsung**. Permet de créer un conteneur SEAMS ou KNOX pour les applications sur les appareils Samsung. Disponible sur Samsung SEAMS ou Samsung KNOX.
- **Supprimer les fichiers et dossiers**. Permet de spécifier les fichiers et les dossiers qui doivent être supprimés. Disponible sur Windows Mobile/CE.
- **Attestation de l'intégrité des appareils**. Active l'attestation d'intégrité des appareils, une fonctionnalité de sécurité et de prévention des pertes de données (DLP) dans Windows 10 qui vous permet d'évaluer l'intégrité d'un appareil Windows 10 et de prendre les mesures qui s'imposent pour satisfaire aux exigences de conformité. Les charges utiles sont uniquement prises en charge sur les appareils supervisés Windows 10 et versions ultérieures. Disponible sur Windows Phone et Windows Tablet.
- **Nom de l'appareil.** Permet de définir les noms sur des appareils iOS et Mac OS X, 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.
- **Supprimer des clés et valeurs de registre**. Permet de spécifier les clés et valeurs de registre qui doivent être supprimées. Une valeur vide signifie que l'entrée est une clé de registre. Disponible sur Windows Mobile/CE.
- **Protection des données d'entreprise.** Permet de spécifier les applications qui nécessitent une protection des données d'entreprise (EDP) au niveau d'exécution requis. Cette stratégie s'applique aux téléphones et tablettes Windows.
- **Importer le profil iOS et Mac OS X**. La possibilité de configurer cette stratégie pour Mac OS X est une nouveauté dans XenMobile 10.3. Cette stratégie vous permet d'importer un fichier XML de configuration d'appareil pour iOS ou Mac OS X. Le fichier contient des stratégies de sécurité et des restrictions que vous préparez avec Apple Configurator.
- **Registre**. Le registre Windows Mobile/CE stocke des données sur les applications, pilotes, préférences utilisateur et

paramètres de configuration. Vous pouvez définir les clés et valeurs de registre qui vous permettent de gérer les appareils Windows Mobile/CE.
- **Fond d'écran.** Permet d'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 version ultérieure. 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.
- **Certificat Windows CE**. Permet de créer et de délivrer un certificat provenant d'une PKI externe à votre appareil.

Pour un tableau de toutes les stratégies d'appareils par plate-forme, nouvelles et existantes, consultez la section Stratégies XenMobile par plate-forme.

Synthèse des nouvelles fonctionnalités et améliorations pour chaque type de plate-forme

iOS

- **Nouvelles stratégies d'appareil**. Utilisation des réseaux, Nom de l'appareil et Fond d'écran
- **Transition d'une application du mode géré au mode non géré**. Option iOS 9.0 pour passer une application du mode géré au mode non géré. Lorsque vous ajoutez et configurez des paramètres pour une application provenant d'un magasin d'applications public pour iOS dans la console XenMobile, vous pouvez configurer une option permettant de **Forcer l'application à être gérée**. Cette option est définie sur **OFF** par défaut. Si vous sélectionnez **ON**, lorsque l'application est installée en mode non géré, les utilisateurs sont invités à autoriser l'application à être gérée sur les appareils non supervisés. Pour de plus amples informations, consultez la section Ajout d'un magasin d'applications public à XenMobile.
- **Nouvelles restrictions et options de stratégie Apple Configurator 1.7.2**. Pour plus de détails, consultez la section Stratégies de restrictions.
- **Prise en charge des commandes RequestMirroring et StopMirroring**. Pour de plus amples informations, consultez la section API REST XenMobile : références.
- **Améliorations de l'assistant d'installation d'appareil DEP**. Pour de plus amples informations, consultez la section Inscription en bloc d'appareils iOS.
- **Clé OnDemandRules VPN**. Pour de plus amples informations, consultez la section Stratégies VPN.

Android

- **Configurations du conteneur Samsung KNOX**. Pour de plus amples informations, consultez la section Stratégie Copier les applications sur le conteneur Samsung.
- **API Samsung SAFE**. Pour de plus amples informations, consultez la section API REST XenMobile : références.
- **Clé ELM pour appareils Android Samsung**.
- **Stratégie de mode kiosque**. Pour de plus amples informations, consultez la section Stratégie de mode kiosque.

Windows CE

- **Configurations du fournisseur d'informations d'identification**. Pour de plus amples informations, consultez la section Stratégies d'informations d'identification.
- **Configurations de certificat Windows CE**. Pour de plus amples informations, consultez la section Stratégie de certificat Windows CE.
- **Stratégie de stockage sur registre**. Pour de plus amples informations, consultez la section Stratégie de Registre.
- **Possibilité de se connecter à la réception d'un SMS/appel**.
- **Autres nouvelles stratégies** : Gestionnaire de connexions, Supprimer les fichiers et dossiers, Supprimer des clés et valeurs de Registre.

Windows Phone 10 et Windows Tablet 10

- Nouvelle stratégie : Protection des données d'entreprise et Attestation de l'intégrité des appareils
- Nouvelles options de stratégie pour Windows Phone et Windows Tablet :

  Inventaire des applications
  Informations d'identification
  XML personnalisé
  Code secret
  Restrictions
  Termes et conditions
  VPN
  Wi-Fi

- Nouvelles options de stratégie pour Windows Tablet :

  Désinstallation d'applications
  Clé de sideloading
  Certificat de signature
  Clip Web
  WorxStore

- Nouvelles options de stratégie pour Windows Phone :

  Hub d'entreprise
  Chiffrement du stockage

Mac OS X

- Inscription via OTAE. Pour de plus amples informations, consultez la section Mac OS X.
- Informations de gestion d'appareil dans la console XenMobile, affichant les propriétés de l'appareil, les certificats, les rapports et les profils pris en charge.
- Actions de sécurité sur les appareils Mac OS X : effacement des données d'entreprise, verrouillage, révocation, effacement des données.
- Nouvelles options de stratégie :

  Nom de l'appareil
  Importer le profil iOS et Mac OS X
  Mise en miroir AirPlay
  Inventaire des applications
  Calendrier (CalDav)
  Contacts (CardDAV)
  Informations d'identification
  Exchange
  Police
  LDAP
  Messagerie
  Code secret
  Suppression de profil
  Restrictions

SCEP
VPN
clip Web
Wi-Fi

Nouvelles fonctionnalités et améliorations pour la prise en charge de Android for Work

- **Prise en charge des appareils antérieurs à Android.**
- **Provisioning du mode Device Owner pour Android for Work**

  Outre la gestion des applications Android for Work ou des appareils Android en mode BYOD, vous pouvez également gérer les appareils appartenant à l'entreprise en provisionnant le mode Device Owner (Attribution du propriétaire de l'appareil). Pour ce faire, vous cognez les appareils à l'aide du partage NFC. Un appareil exécute l'application Worx Provisioning Tool et cogne un tout nouvel appareil ou un appareil dont les paramètres d'usine ont été réinitialisés. Le mode Device Owner est le mode des appareils appartenant à l'entreprise pour la plupart des appareils exécutant Android 5.x.x.

- **Achat en bloc Android for Work**

  Vous pouvez gérer les licences en matière d'achat en bloc dans la console XenMobile pour les applications activées pour Android for Work. Le plan Achat groupé pour Android for Work simplifie la recherche, l'achat et la distribution d'applications et d'autres données en bloc pour une organisation. Lorsque vous ajoutez une application payante provenant d'un magasin d'applications public pour Android for Work à XenMobile, vous pouvez vérifier l'état de la licence d'achat groupé : le nombre total de licences disponibles. Après avoir déployé l'application auprès des utilisateurs, vous pouvez vérifier le nombre de licences en cours d'utilisation, ainsi que l'adresse e-mail de chaque utilisateur qui consomme des licences. 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.

Appareils partagés

XenMobile vous permet de configurer des appareils qui peuvent être partagés par de multiples utilisateurs. Pour de plus amples informations, consultez la section Appareils partagés dans XenMobile.

Langues prises en charge

La console XenMobile dans XenMobile 10.3 est disponible en coréen, en allemand et en portugais. Les stratégies MDX sont désormais traduites lorsqu'elles sont affichées dans la console XenMobile. Pour de plus amples informations, consultez la section Langues prises en charge dans XenMobile.

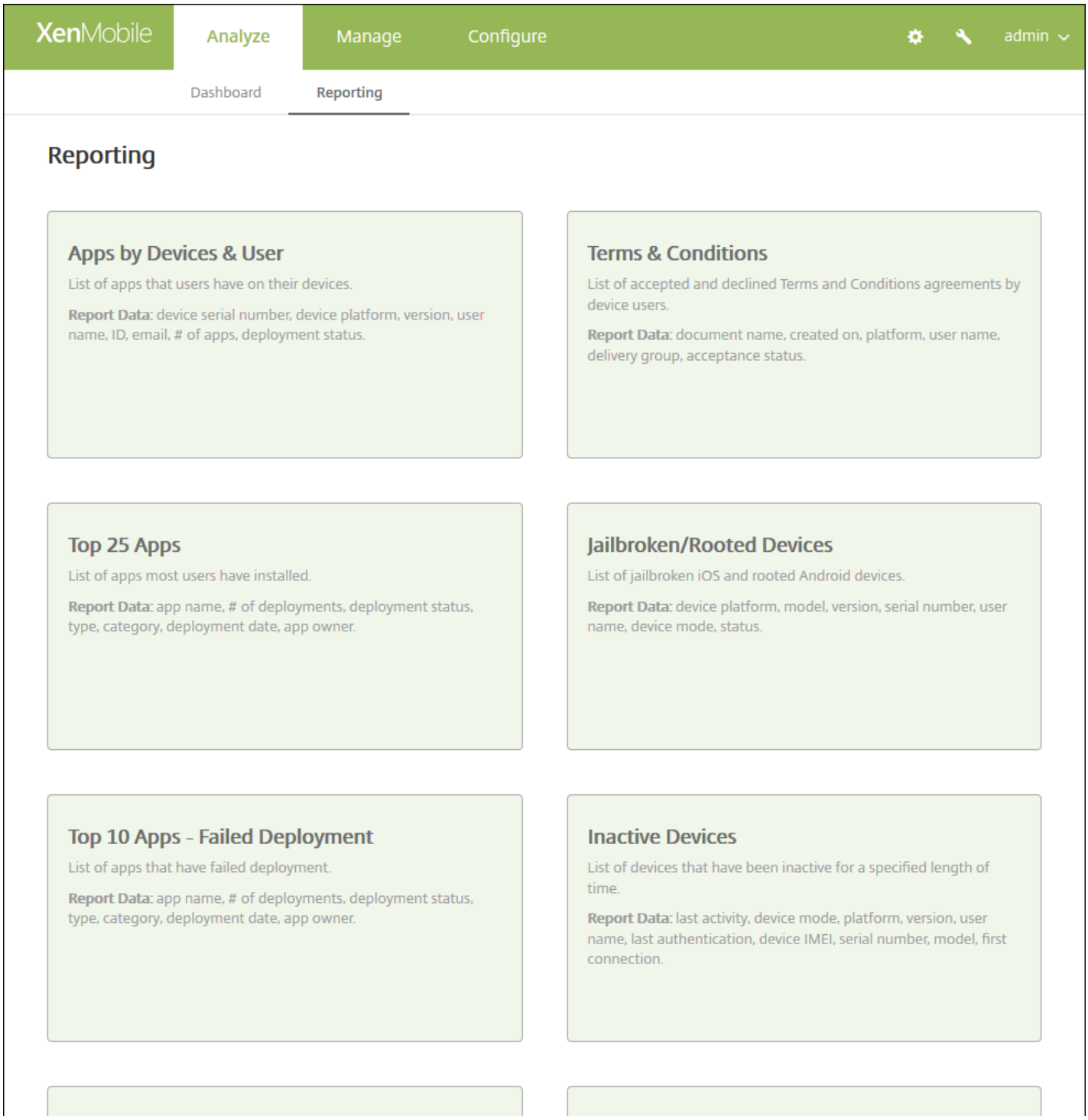
Rapports

Dans l'onglet **Rapports**, vous pouvez générer 10 rapports prédéfinis à partir de la console XenMobile.

- **Applications par appareils et utilisateur** : répertorie les applications que les utilisateurs ont sur leur appareil.
- **Termes et conditions** : répertorie les utilisateurs qui ont accepté et refusé les conditions générales.
- **Top 25 des applications** : répertorie jusqu'à 25 applications que la plupart des utilisateurs ont sur leurs appareils.
- **Appareils jailbreakés/rootés** : répertorie les appareils iOS rootés et les appareils Android jailbreakés.
- **Top 10 des applications - échec du déploiement** : répertorie les applications dont le déploiement a échoué.
- **Appareils inactifs** : répertorie les appareils qui sont inactifs depuis une période de temps spécifiée.

- **Application par type et catégorie** : répertorie les applications par version, type et catégorie.
- **Inscription d'appareils** : répertorie les appareils inscrits pendant une période spécifiée.
- **Applications par plate-forme** : répertorie les applications et les versions des applications par plate-forme et version de l'appareil.
- **Appareils et applications** : répertorie tous les appareils, toutes les données de l'appareil et toutes les applications installées.

Pour exécuter des rapports, cliquez sur l'onglet **Analyser** dans la console XenMobile, puis cliquez sur **Rapports**. Les rapports sont au format .csv, que vous pouvez ouvrir avec des programmes tels que Microsoft Excel. Pour de plus amples informations, consultez la section Rapports dans XenMobile.



Apps by Type & Category

List of apps and app versions by app type (MDX, Public, Web & SaaS, Enterprise, Web Link) and defined categories.

Report Data: app name, version, # of deployments, deployment status, type, category, deployment date, app owner.

Device Enrollment

List of devices that have been enrolled during a specified length of time.

Report Data: first connection, device mode, platform, version, model, user name, last authentication, phone number.

Apps by Platform

List of apps and app versions installed on various device platforms and device versions.

Report Data: app name, version, # of deployments, deployment status, deployment date, app owner, device platform, version, model, model name.

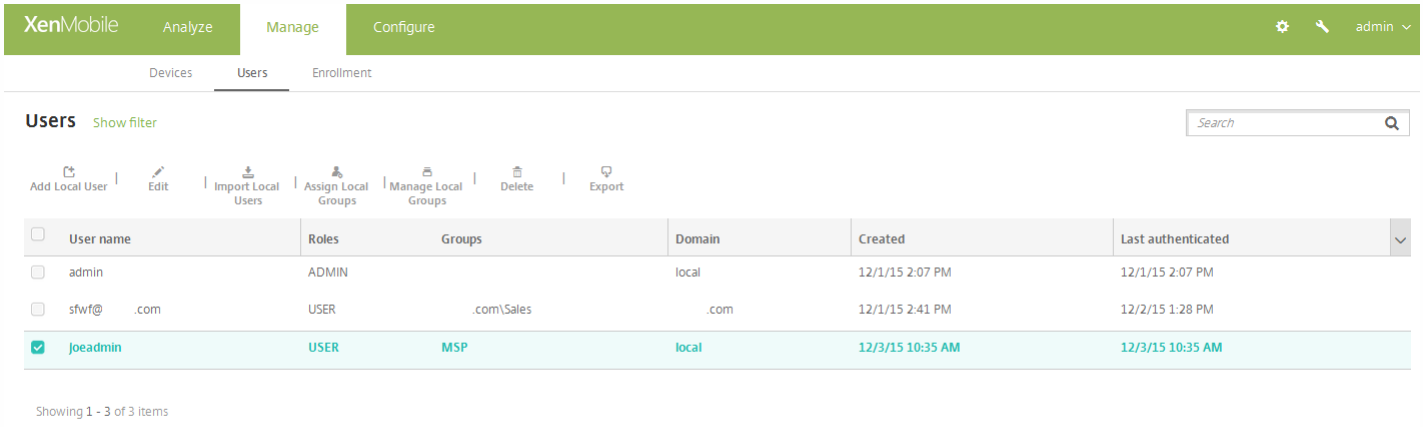
Devices & Apps

List of all devices, device data, and apps installed.

Report Data: device serial number, user name, ID, email, device platform, version, model, mode, status, last connection, enrollment status, enrollment date, device ownership, location, certificate expiration, app name, version, deployment status, type, category, deployment date, app owner, app ID.

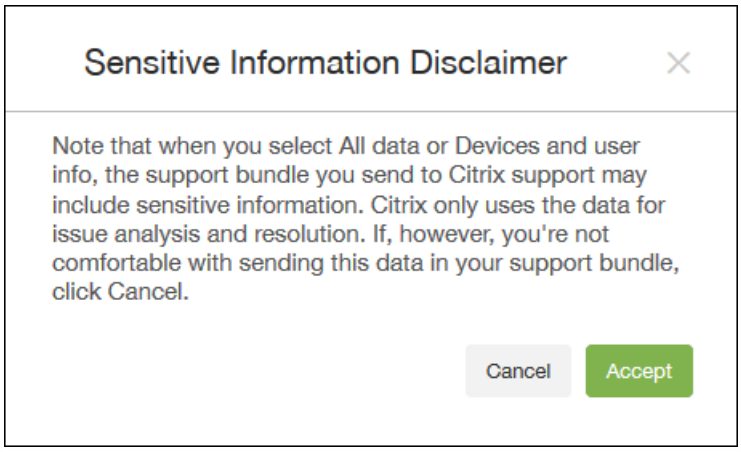
Ajout de membres LDAP (utilisateurs locaux) aux groupes

De nombreuses organisations ne configurent pas de groupes Active Directory, mais peuvent avoir besoin d'un groupe local pour un usage particulier, dans le cadre d'un pilote par exemple. Dans XenMobile 10.3, vous pouvez définir des utilisateurs locaux LDAP comme membres d'un groupe local. Ensuite, vous pouvez définir un groupe de mise à disposition qui contient le groupe local. Ces utilisateurs peuvent accéder aux applications et aux stratégies attribuées au groupe de mise à disposition, sans avoir à réinscrire leurs appareils. Pour de plus amples informations, consultez la section Pour ajouter, modifier ou supprimer des utilisateurs locaux dans XenMobile.



Contrat du pack de support

La première fois que vous téléchargez un pack d'assistance sur Citrix Insight Services (CIS), vous êtes invité à accepter un contrat. Pour de plus amples informations, consultez la section Création de packs d'assistance dans XenMobile.



Anonymisation des données dans les packs d'assistance

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. Pour de plus amples informations, consultez la section Anonymisation des données dans les packs d'assistance.

Tests de connectivité

Depuis la page Support de XenMobile, vous pouvez vérifier la connexion de XenMobile à NetScaler Gateway et à d'autres serveurs et emplacements. Pour de plus amples informations, consultez la section Réalisation de contrôles de connectivité.

Microsoft Azure

Vous pouvez associer les appareils Windows 10 à Microsoft Windows Azure AD pour les autoriser à s'inscrire à Azure afin de fédérer l'authentification Active Directory. Pour de plus amples informations, consultez la section Paramètres Microsoft Azure.

Problèmes résolus de XenMobile 10.3

Jul 27, 2016

Les problèmes suivants ont été résolus dans XenMobile 10.3. Pour connaître les problèmes résolus dans XenMobile 10.3.5, consultez la section Problèmes connus et problèmes résolus dans XenMobile 10.3.5.

Un préfixe d'envoi d'e-mail peut être ajouté deux fois à une adresse e-mail lors de l'envoi d'e-mails à partir d'un serveur SMTP via la passerelle SMS d'un opérateur. [#492629]

Les requêtes HTTP GET de Cisco Identity Service Engine vers XenMobile peuvent échouer avec une erreur 404. [#555554]

Lorsqu'une stratégie de chargement de fichier est définie pour distribuer un fichier auprès d'appareils Android, la distribution du fichier sur les appareils peut échouer. Au lieu de cela, les « Termes et conditions » peuvent apparaître sur l'appareil. [#564144]

Dans certains cas, lorsque des certificats d'identité MDM sont distribués via SCEP et sont publiés à l'aide de la PKI intégrée, XenMobile ne révoque pas correctement le certificat précédent lorsque ces identités sont renouvelées. Par conséquent, dans certains cas, les appareils affectés perdent la fonctionnalité MDM. [#569999]

Après avoir configuré un serveur proxy, les tests de connectivité créent du trafic réseau qui ne transite via le serveur proxy et la connexion échoue. [#571467]

Si les utilisateurs sont membres d'un domaine enfant, la connexion aux applications SAML échoue. [#571851]

Si une application MDX iOS figure dans la liste des appareils exclus, l'application ne s'affiche pas dans Worx Store lorsque l'appareil est en mode de gestion des applications mobiles (mode MAM). [#571900]

Après la mise à niveau vers XenMobile 10, la recherche d'un appareil peut prendre jusqu'à 30 secondes et l'utilisation de l'UC atteint également 100 %. [#577010]

Lorsque vous parcourez des sites intranet avec WorxWeb dans un environnement de clusters comprenant de multiples nœuds, il se peut que les utilisateurs ne puissent pas à accéder aux adresses URL et que le message « Error Invalid OTT » s'affiche. [#577273]

Si vous configurez XenMobile avec un serveur proxy, les tentatives d'ajout d'informations d'identification Google Play ou de création d'une application dans le magasin d'applications Android peuvent échouer. [#578727]

Une page blanche apparaît lors de la tentative d'ouverture de la console XenMobile dans une version publiée d'Internet Explorer 11. [#578729]

Cette version prend désormais en charge WPA2 Personal et WPA2 Enterprise pour iOS 8. [#579616]

Si vous ajoutez ou chargez une application dans la console XenMobile, une erreur peut se produire lorsque vous chargez l'application sur XenMobile à l'aide du même nom de fichier d'application qu'une application existante. [#580359]

Les tentatives de téléchargement d'applications Worx depuis le Worx Store échouent sur les appareils Android. [#582044]

Lors de la saisie d'une macro avec le nom d'utilisateur et le numéro de téléphone, le fichier de transformation ne traduit pas correctement le numéro de téléphone. [#589130]

La commande Ne pas utiliser le verrouillage d'activation peut ne pas fonctionner sur certains appareils iOS. [#589991]

Si la valeur de la propriété « memberOf » dépasse 255 caractères, le message d'erreur « Aucun groupe trouvé » s'affiche. Si les utilisateurs tentent d'ouvrir une application Windows via Worx Home, l'énumération réussit, mais l'application ne s'ouvre pas. Les utilisateurs reçoivent le message d'erreur « Impossible d'ajouter le compte. » [#590046]

Si vous créez une stratégie CEP qui requiert la vérification du mot de passe, vous ne pouvez pas enregistrer la stratégie. Avec cette version, le champ de vérification du mot de passe est facultatif. [#590798]

Si vous configurez XenMobile afin qu'il utilise un serveur proxy, Android for Work ne peut pas établir de connexion à des sites Web externes. [#591707]

Les tentatives de chargement d'une application IPA sur App Controller échouent avec le message d'erreur « Type de package non valide pour l'application sélectionnée. » Le message s'affiche lorsque l'image PNG contient une erreur. [#592748]

Lorsque les utilisateurs tentent de s'inscrire, ils reçoivent le message d'erreur « L'utilisateur n'existe pas. » L'erreur se produit après suppression et réinscription des utilisateurs. Lorsque ce problème se produit, les utilisateurs sont recréés dans Active Directory. [#593028]

Si vous créez une invitation de calendrier depuis un compte Microsoft Outlook ou Microsoft Exchange, elle peut prendre un certain temps à s'afficher dans WorxMail. [#594542]

Si vous configurez un workflow et que vous utilisez un numéro de port autre que 443 (valeur par défaut), les utilisateurs ne peuvent pas ouvrir le lien de workflow. [#599441]

Les utilisateurs ne peuvent pas mettre à jour une application Android sur leur appareil depuis le serveur XenMobile. [#601251]

Les utilisateurs ne peuvent pas se connecter à des applications Worx lors de l'inscription via Azure Active Directory. [#608505]

À partir de décembre 2015, Nexmo SMS prend uniquement en charge les connexions HTTPS. Dans XenMobile, le paramètre par défaut est **ON**. Rien ne se produit si vous modifiez la valeur sur **OFF**. Après la mise à niveau, la valeur affiche toujours **OFF**, mais les connexions sont sécurisées. [#609306]

Worx Store requiert un utilisateur VPP bien que la licence s'applique uniquement à l'appareil. [#610338]

Problèmes connus de XenMobile Server 10.3

Jul 27, 2016

Vous trouverez ci-dessous les problèmes connus dans XenMobile 10.3. Pour connaître les problèmes connus dans XenMobile 10.3.5, consultez la section Problèmes connus et problèmes résolus dans XenMobile 10.3.5.

- Les bogues suivants sont associés à une intégration entre XenMobile et NetScaler pour les versions suivantes de NetScaler lorsque le protocole de sécurité TLS 1.2 est configuré sur NetScaler :
  - Versions de NetScaler 11.x antérieures à 11.0.64
  - 10.5.59
  - 10.5.58

  Veuillez noter que le problème ne se produit pas lorsque votre déploiement MAM XenMobile comprend un équilibrage de charge NetScaler entre le serveur XenMobile et NetScaler Gateway.

  Les communications entre NetScaler Gateway et XenMobile en mode MAM échouent en raison de problèmes avec une session TLS 1.2 principale. Par conséquent, les utilisateurs ne peuvent pas télécharger d'applications à partir du WorxStore, ni de fichiers depuis ShareFile, lors de la connexion au réseau interne.
  [#591600,#595713,#596566,#604409]
- La distribution d'applications en push échoue après la désinstallation d'une application d'entreprise. [#591450]
- Après suppression de la licence d'une application, l'application reste sur l'appareil de l'utilisateur. Il s'agit d'un problème de tiers. [#596656]
- Lorsque les utilisateurs tentent d'inscrire leurs appareils personnels avec un compte professionnel Microsoft, l'inscription échoue. [#597037]
- La stratégie Termes et conditions n'affiche pas un état installé ou en attente dans la console XenMobile, même si la stratégie est déployée avec succès sur l'appareil. [#598407]
- Les stratégies de restriction prennent effet sur les appareils Windows 10. Toutefois, les utilisateurs ne reçoivent pas de message indiquant qu'une fonctionnalité bloquée est désactivée. [#599064,#606651]
- Si vous ajoutez une catégorie avec des applications publiques et d'entreprise et que vous inscrivez un appareil dans XenMobile, lorsque les utilisateurs synchronisent des applications dans Worx Home, la catégorie ne s'affiche pas. [#599495]
- Si vous n'ajoutez pas l'autorisation Effacer les données d'entreprise d'un appareil lors de la création d'un rôle RBAC Appareils partagés, lorsque les utilisateurs tentent de supprimer leur compte dans Worx Home sur un appareil iOS (en mode XenMobile Enterprise), les utilisateurs doivent supprimer manuellement le profil Device Manager de l'appareil. [#600705]
- Si après avoir déployé les stratégies Inventaire des applications et Hub d'entreprise pour une application et créé une application publique avec une description et un nom différents, les utilisateurs ouvrent l'application à partir de Worx Home, le nom et la description de l'application sont les mêmes. [#600369]
- Si vous configurez Microsoft SQL Server en mode SSL lors de la première utilisation, et que le certificat d'autorité de certification ne correspond pas au certificat du serveur SQL Server, la connexion échoue. Si vous tentez de relancer la

connexion avec le certificat d'autorité de certification qui correspond au certificat du serveur SQL Server, la connexion échoue quand même. Pour que le certificat fonctionne, redémarrez le serveur XenMobile pour effacer le cache truststore. [#602609]

- Les noms d'utilisateur doivent être en anglais sur les appareils partagés. Les appareils partagés ne prennent pas en charge les noms d'utilisateur non ASCII. [#605544]
- Lorsque les utilisateurs reçoivent leur mot de passe à usage unique pour la liaison IMEI (nom d'utilisateur et mot de passe) et les notifications SMS et SMTP, le premier profil s'installe avec succès mais l'installation du second profil échoue avec le message d'erreur « Profile Installation Fails. A connection to the server could not be established. » Les iPhone 6 et iPhone 6 Plus comprennent deux numéros, un numéro IMEI et un numéro MEID, et le mot de passe à usage unique est lié au numéro MEID plutôt qu'au numéro IMEI. Vous pouvez remplacer le numéro IMEI grâce à l'identifiant unique (UDID) de l'iPhone ou utiliser un numéro de téléphone ordinaire. [#606162]
- Après la mise à niveau vers XenMobile 10.3, les informations de licence s'affichent en tant que période d'évaluation de 30 jours et le serveur de licences configuré est défini sur true. Après la mise à niveau du serveur XenMobile, chargez la même licence sur le serveur, ce qui supprime la licence de la version d'évaluation. [#607939]
- Sur les tablettes Windows 8.1, les utilisateurs peuvent supprimer des applications de l'appareil. Les applications d'entreprise continuent à s'afficher dans la console XenMobile dans les propriétés de l'appareil. [#608184]
- Les options Effacement des applications et Effacer les données d'entreprise fonctionnent de la même manière dans le mode XenMobile Enterprise. [#608715]
- Le serveur XenMobile ne répond plus lorsque vous enregistrez ou ouvrez un fichier dans Internet Explorer. Vous pouvez redémarrer le serveur pour continuer à travailler. [#608724]
- Après la mise à niveau vers XenMobile 10.3, Android for Work n'existe pas dans la stratégie de navigateur, bien que les adresses Web et les signets bloqués soient présents. [#609002]
- Sur les tablettes exécutant Windows 8.1 et Windows 10, après suppression des comptes manuellement à partir de l'appareil, certaines stratégies subsistent. [#609201]
- Sur les tablettes Windows 10, si les utilisateurs modifient le paramètre Autoupdate sur l'appareil, les modifications ne s'affichent pas dans la section Informations de sécurité dans les propriétés de l'appareil dans la console XenMobile. [#609254]
- Le nom du Worx Store prend uniquement en charge les caractères anglais (ASCII). [#609535]
- Si vous essayez de télécharger une demande de signature de certificat (CSR) à partir de navigateurs Web Internet Explorer et Firefox, les tentatives échouent avec l'erreur « La page Web ne peut pas être affichée. » Le téléchargement de la demande de signature de certificat fonctionne à partir du navigateur Web Chrome. [#609552]
- Si vous ouvrez une session sur la console XenMobile, que vous accédez à **Analyser** > **Rapports**, puis que vous cliquez sur **Appareils inactifs**, une page blanche s'affiche au lieu de la page de téléchargement du fichier. [#609649]
- Lors de la configuration d'un espace de travail dans Citrix Workspace Cloud, les groupes de mise à disposition ne sont pas mis à jour avec les utilisateurs ou les groupes Active Directory appartenant à des domaines enfants et petits-enfants. [#609673]
- L'inscription d'un appareil Windows 10 échoue si plusieurs stratégies Termes et conditions sont déployées et qu'aucune

des stratégies n'est la stratégie Termes et conditions par défaut. [#609694]

- Si vous supprimez une stratégie d'un groupe de mise à disposition, que vous cliquez sur le bouton **Résumé** et que vous enregistrez la stratégie, la ressource reste dans le groupe de mise à disposition. Si vous cliquez sur **Suivant** au lieu de **Résumé**, la stratégie est supprimée du groupe de mise à disposition. [#610109]
- Pour conserver l'extension du fichier d'origine sur un appareil Windows CE, ne spécifiez pas le nom du fichier de destination dans la stratégie. [#610601]
- Lorsque vous configurez une stratégie VPN pour Mac OS X, l'option **VPN** s'affiche dans la liste des **types de connexion**. Toutefois, vous ne pouvez pas configurer cette option pour les appareils Mac OS X. [#612846]
- Lors de la mise à jour de XenMobile 10.0 vers la version 10.3, si le WorxStore a un nom personnalisé, vous devez rétablir le nom par défaut du magasin sur **Store** et déployer le paramètre sur les appareils avant de procéder à la mise à jour. Si vous ne procédez pas de la sorte, le nom du magasin personnalisé entraîne des problèmes avec l'inscription auprès de XenMobile 10.3, avec l'accès à Worx Home et WorxStore, et avec le déploiement d'applications sur les appareils iOS. [#614049]
- Vous ne pouvez pas activer Android for Work dans la console XenMobile. Lorsque vous configurez des paramètres de compte Android for Work et que vous entrez l'ID de compte de service que vous obtenez à partir de Google, qui contient uniquement des chiffres, une erreur s'affiche lorsque vous enregistrez les paramètres. Si vous entrez l'ID de compte de service à l'aide du format Google antérieur qui contenait des chiffres et des caractères, la même erreur se produit car ce format ne correspond pas à l'ID de compte de service du serveur XenMobile. Il s'agit d'un problème de tiers.

  Pour contourner le problème et activer Android for Work, ajoutez une propriété de serveur à l'ID du client Google.

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

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

  3. Dans la liste **Clé**, cliquez sur **Clé personnalisée**.

  4 Dans **Clé**, entrez **google.aw.enterprise.client.id**

  5. Dans **Valeur**, entrez la valeur numérique de l'ID client, telle que 3838383838388383.

  6. Entrez un **nom d'affichage**, tel que Google « ID client du domaine Google. »

  7. Cliquez sur **Enregistrer**.

  [#615118]

- Sur Mac OS X et iPads, XenMobile 10.3 effectue toujours les actions de suppression (ou de retrait) en premier, quel que soit l'ordre que vous avez défini dans la console XenMobile. [#620459]
- Après avoir activé l'inscription en bloc iOS et mis à jour l'autorité de certification (CA) racine du certificat SSL XenMobile, l'inscription ou la réinscription de l'appareil peut échouer. Ce problème peut se produire lorsque vous passez d'un certificat auto-signé à un certificat public, que vous achetez un certificat auprès d'un nouveau fournisseur, ou que vous passez à une autorité de certification d'entreprise interne. Ce problème n'affecte pas les appareils déjà inscrits. Pour contourner le problème, effectuez les opérations suivantes :

1. Dans la console XenMobile, cliquez sur **Paramètres** > **Inscription en bloc iOS**.
2. Sous **Configuration DEP**, en regard de **Autoriser Device Enrollment Program (DEP)**, cliquez sur **NON**, puis sur **Enregistrer**. Patientez quelques secondes. Cette étape supprime le profil DEP précédent des appareils DEP sur le portail DEP d'Apple.
3. Cliquez sur **Gérer** > **Appareils**. Vérifiez qu'aucun appareil DEP enregistré n'apparaît dans la colonne **Enregistré auprès du Device Enrollment Program**.
4. Cliquez sur **Paramètres** > **Inscription en bloc iOS**.
5. Sous **Configuration DEP**, en regard de **Autoriser Device Enrollment Program (DEP)**, cliquez sur **OUI**, puis sur **Enregistrer**. Patientez quelques secondes. Cette étape permet de forcer l'ajout d'un nouveau profil à tous les appareils DEP.
6. Cliquez sur **Tester la connexion** pour vous assurer que la connexion entre le serveur XenMobile et les serveurs DEP d'Apple fonctionne toujours.
7. Cliquez de nouveau sur **Gérer** > **Appareils**. Vérifiez que tous les appareils DEP sont enregistrés dans la colonne **Enregistré auprès du Device Enrollment Program**.

Pour de plus amples informations sur le programme DEP d'Apple, consultez la section Inscription en bloc d'appareils iOS. [#635699]

Aperçu de l'architecture

Oct 17, 2016

Les composants XenMobile dans l'architecture de référence XenMobile que vous déployez sont basés sur les besoins en matière de gestion des applications ou appareils de votre organisation. Les composants XenMobile sont modulaires et complémentaires. Par exemple, vous souhaitez accorder aux utilisateurs de votre organisation un accès à distance à des applications mobiles et vous devez connaître les types d'appareils avec lesquels les utilisateurs se connectent. Dans ce scénario, vous pouvez déployer XenMobile avec NetScaler Gateway. XenMobile est l'emplacement à partir duquel vous gérez les applications et les appareils, et NetScaler Gateway permet aux utilisateurs de se connecter à votre réseau.

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 NetScaler Gateway pour accéder à des applications et des 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.
- Applications Web, SaaS et mobiles. Les utilisateurs peuvent accéder à leurs applications Web, SaaS, mobiles à partir de XenMobile via Worx Home.
- 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 partie ou l'ensemble de ces fonctionnalités, Citrix vous recommande de déployer les composants XenMobile dans l'ordre suivant :

- NetScaler Gateway. Vous pouvez configurer les paramètres dans NetScaler 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 NetScaler Gateway, vous devez installer XenMobile, StoreFront ou l'Interface Web de façon à pouvoir communiquer avec ces derniers.
- 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 wrappez avec le MDX Toolkit et que vous chargez sur la console.
- MDX Toolkit. MDX Toolkit peut wrapper une application qui a été créée au sein de votre organisation ou une application mobile développée par des tiers, telle que les applications Citrix Worx. Après avoir wrappé une application, vous pouvez utiliser la console XenMobile pour ajouter l'application à XenMobile et modifier la configuration de la stratégie en fonction de vos besoins. Vous pouvez également ajouter des catégories d'applications, appliquer des workflows et déployer des applications sur des groupes de mise à disposition. Consultez la section À propos de MDX Toolkit.
- StoreFront (facultatif) Vous pouvez fournir l'accès à des applications et des bureaux virtuels Windows à partir de StoreFront via des connexions avec Receiver.
- ShareFile Enterprise (facultatif). Si vous déployez ShareFile, 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 de plus amples informations sur la configuration de fournisseurs d'identité pour ShareFile, consultez le site de support de ShareFile.

XenMobile prend en charge une solution intégrée qui 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 NetScaler peut réduire la charge sur le serveur XenMobile et augmenter le débit. Pour de plus amples informations sur la configuration de la mise en cluster pour XenMobile 10.x en configurant deux adresses IP virtuelles d'équilibrage de charge sur NetScaler, consultez la section Configuration de la mise en cluster pour XenMobile 10.

Pour de plus amples informations sur la manière de configurer XenMobile 10 Enterprise Edition pour un déploiement de récupération d'urgence (comprend un diagramme d'architecture), consultez le Guide de récupération d'urgence pour XenMobile.

Les sections suivantes décrivent différentes architectures de référence pour le déploiement XenMobile. Pour accéder à des diagrammes d'architecture de référence, consultez les articles Reference Architecture for On-Premises Deployments et Reference Architecture for Cloud Deployments du Manuel de déploiement de XenMobile. Pour obtenir une liste complète des ports, consultez la section Exigences requises par XenMobile en matière de port.

Mode de gestion de la flotte mobile (MDM)

XenMobile MDM Edition permet de gérer les appareils mobiles pour iOS, Android, Amazon et Windows Phone (voir Plates-formes prises en charge dans XenMobile). Vous déployez XenMobile en mode MDM si vous prévoyez 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.

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

Mode de gestion des applications mobiles (MAM)

MAM prend en charge les appareils iOS et Android, mais pas les appareils Windows Phone (voir Plates-formes prises en charge dans XenMobile). Vous déployez XenMobile en mode MAM (également appelé mode MAM exclusif) si vous prévoyez 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.

Dans ce modèle de déploiement, le serveur XenMobile est positionné avec un NetScaler 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 iOS, Android, et Windows Phone (voir Plates-formes prises en charge dans XenMobile). Vous déployez XenMobile en mode ENT (enterprise) si vous prévoyez 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.

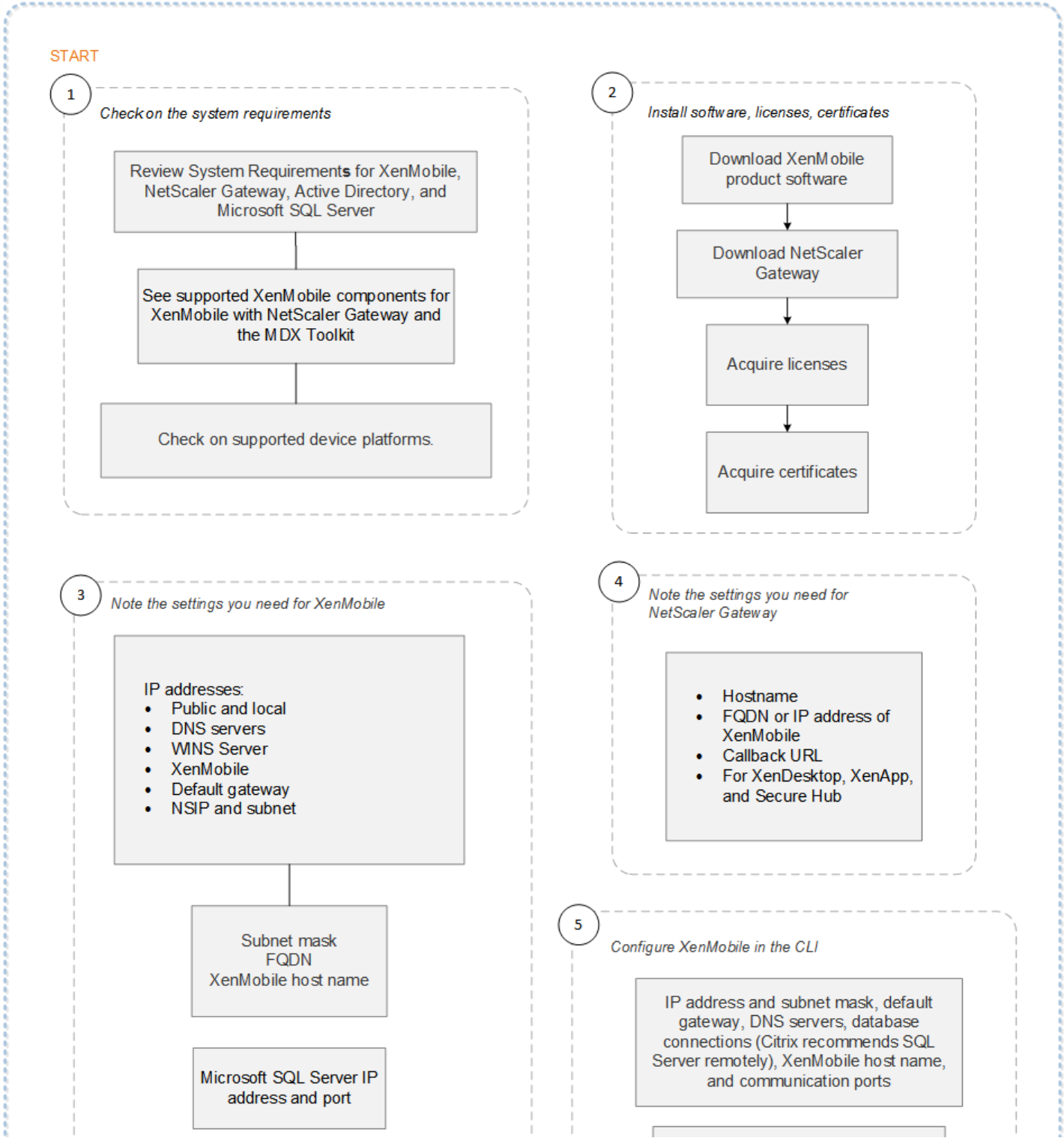
Dans le modèle de déploiement recommandé, le serveur XenMobile est positionné dans la zone démilitarisée (DMZ) avec un NetScaler Gateway au premier plan, ce qui offre une protection renforcée pour XenMobile.

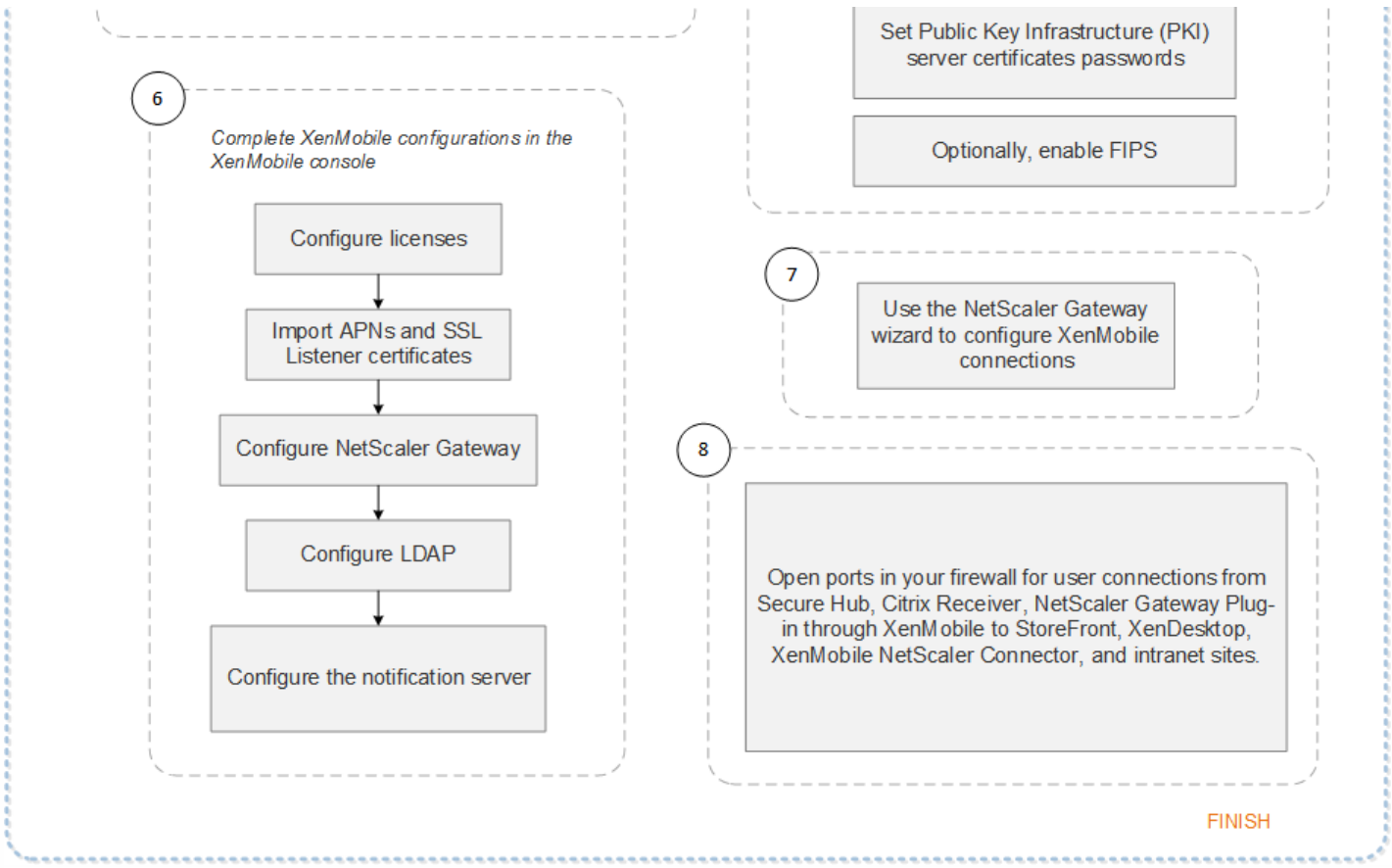
XenMobile dans le réseau interne : une autre option de déploiement consiste à positionner le serveur XenMobile dans le réseau interne, plutôt que dans la DMZ. Ce type de déploiement est utilisé si votre stratégie de sécurité autorise uniquement le positionnement d'appliances réseau dans la DMZ. Étant donné que le serveur XenMobile n'est pas dans la DMZ, 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.

Organigramme du déploiement de XenMobile avec NetScaler Gateway

Oct 17, 2016

Vous pouvez utiliser cet organigramme pour vous guider dans les étapes principales du déploiement XenMobile 10.3 avec NetScaler Gateway. Vous trouverez des liens vers des rubriques liées à chaque étape après la figure.





1

- Configuration système requise pour XenMobile 10,3
- Compatibilité XenMobile
- Plates-formes prises en charge dans XenMobile 10,3

2

- Installation de XenMobile
- Certificats dans XenMobile
- Licences pour XenMobile

3

- Check-list de pré-installation XenMobile

4

- Check-list de pré-installation XenMobile

5

- Configuration de XenMobile dans la fenêtre d'invite de commande

6

- Configuration de XenMobile dans un navigateur Web

7

- Configuration des paramètres de votre environnement XenMobile

8

- Exigences requises par XenMobile en matière de port

L'organigramme est également disponible au format PDF.

Organigramme pour le déploiement de XenMobile

Capacité à monter en charge de XenMobile

Oct 17, 2016

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 fournit les réponses aux questions les plus courantes quant à la configuration requise pour les déploiements à petite et grande échelle.

Les données de cet article offrent des directives permettant de déterminer les performances et la capacité à monter en charge d'une infrastructure XenMobile 10.3. Les deux facteurs clés pour déterminer la manière de configurer votre serveur et la base de données sont la capacité à monter en charge (nombre maximal d'utilisateurs/d'appareils) et le taux d'ouverture de session.

- La capacité à monter en charge est définie comme le nombre maximal d'utilisateurs exécutant simultanément une charge de travail déterminée. Pour de plus amples informations sur les flux utilisés pour charger l'infrastructure XenMobile, reportez-vous à la section Charges de travail.
- Le taux d'ouverture de session est défini comme l'intégration de nouveaux utilisateurs et l'authentification des utilisateurs existants.
  - Le taux d'intégration est le nombre maximal d'appareils pouvant être inscrits dans l'environnement pour la première fois. Appelé Première utilisation ou FTU dans cet article, ce point de données est important lors de l'orchestration d'une stratégie de déploiement.
  - Le taux d'utilisateur existant est le nombre maximal d'utilisateurs authentifiés dans l'environnement et qui se sont déjà inscrits et connectés avec leur appareil. Ces tests englobent la création de sessions pour les utilisateurs déjà inscrits et l'exécution des applications WorxMail et WorxWeb.

Le tableau suivant affiche des directives relatives à la capacité à monter en charge basées sur les résultats de test pour l'environnement XenMobile correspondant.

Capacité à monter en charge	Jusqu'à 100 000 appareils	
Taux d'ouverture de session	Intégration (FTU)	Jusqu'à 2 777 appareils par heure
	Utilisateurs existants	Jusqu'à 16 667 appareils par heure
Configuration	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	Cluster à 10 nœuds du serveur XenMobile
	Base de données	Base de données externe Microsoft SQL Server

> **Important**
>
> Les exigences en matière d'automatisation pour ce rapport sont de 1 000 à 100 000 machines. Toute exigence supérieure à 100 000 machines dépasse le cadre de ce rapport.

Cette section décrit la configuration matérielle utilisée et les résultats de l'exécution de la charge de travail d'intégration (FTU), ainsi que les tests de capacité à monter en charge pour la charge de travail des utilisateurs existants.

Le tableau suivant définit les recommandations matérielles et de configuration pour XenMobile lors de la montée en charge de 1 000 à 100 000 appareils. Ces directives sont basées sur les résultats des tests et leurs charges de travail associées. Les recommandations tiennent compte de la marge d'erreur acceptable comme défini dans les critères de sortie.

L'analyse des résultats des tests a mené à ces conclusions :

- Le taux d'ouverture de session est un facteur important pour déterminer la capacité à monter en charge d'un système. Outre l'ouverture de session initiale, les taux d'ouverture de session dépendent des valeurs d'expiration de l'authentification configurées dans votre environnement. Par exemple, si vous avez défini une valeur d'expiration de l'authentification trop faible, les utilisateurs doivent exécuter des demandes de connexion plus fréquentes. Par conséquent, vous devez comprendre clairement la manière dont ces valeurs d'expiration affectent votre environnement.
- Le nombre de connexions par session utilisateur sur NetScaler est un facteur important.
- Une base de données externe (SQL Server) avec 128 Go de RAM, 300 Go d'espace disque et 24 processeurs virtuels a été utilisée pour conduire les tests et est recommandée pour les environnements de production.
- Pour atteindre une montée en charge maximale, les ressources en matière d'UC et de RAM ont été augmentées sur XenMobile.
- La configuration du cluster à 10 nœuds a été la plus grande configuration validée. La montée en charge au-delà de 10 nœuds requiert une implémentation supplémentaire de XenMobile.

Le tableau suivant présente les taux d'ouverture de session recommandés pour les nouveaux clients et les clients existants basés sur la configuration XenMobile, le boîtier NetScaler Gateway, les paramètres de cluster et la base de données. Utilisez les données de ce tableau pour planifier un calendrier d'inscriptions optimal pour les

nouveaux déploiements et les taux d'utilisateurs/d'appareils déjà inscrits pour les déploiements existants. La section Configuration associe les données de performances d'inscription et d'ouverture de session aux recommandations matérielles appropriées.

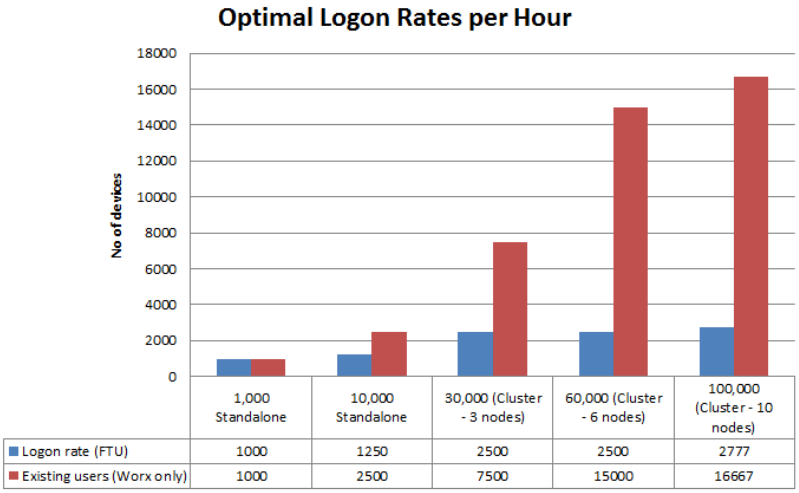
Nombre attendu d'appareils	1 000	10 000	30 000	60 000	100 000
Nombre réel d'appareils	1 000	9 997	29 976	59 831	99 645
Taux d'ouverture de session					
Intégration (FTU)	125	1 250	2 500	2 500	2 777
Utilisateurs existants (Worx uniquement)	1 000	2 500	7 500	15 000	16 667
Configuration					
Environnement de référence	VPX-XenMobile en mode autonome	MPX-XenMobile en mode autonome	MPX-XenMobile en cluster (3)	MPX-XenMobile en cluster (6)	MPX-XenMobile en cluster (10)
NetScaler Gateway	VPX avec 2 Go de RAM Deux processeurs virtuels	MPX-10500		MPX-20500	
XenMobile - mode	Autonome	Autonome	Cluster		
XenMobile - cluster	S.O.	S.O.	3	6	10
XenMobile - boîtier virtuel	8 Go de RAM et 4 processeurs virtuels	8 Go de RAM et 4 processeurs virtuels	8 Go de RAM et 4 processeurs virtuels	16 Go de RAM et 4 processeurs virtuels	16 Go de RAM et 4 processeurs virtuels
Base de données	Externe	Externe – Microsoft SQL Server Mémoire = 16 Go Processeurs virtuels = 12	Externe – Microsoft SQL Server Mémoire = 16 Go Processeurs virtuels = 12	Externe – Microsoft SQL Server Mémoire = 32 Go Processeurs virtuels = 12	Externe – Microsoft SQL Server Mémoire = 32 Go Processeurs virtuels = 16

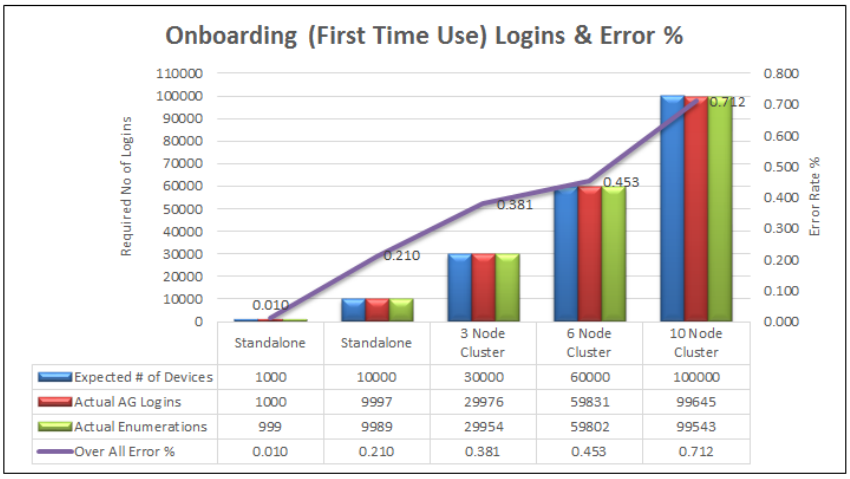
Remarque : vous allez rencontrer les situations suivantes si vous dépassez les recommandations en termes de taux ou de matériel lors du dimensionnement de votre système.

Les informations suivantes fournissent des points de données supplémentaires qui ont été enregistrés et qui affectent les résultats dans le tableau précédent.

- Latence d'inscription ou d'ouverture de session (durée aller-retour)
  - Latence moyenne totale : 0,5 à 1,5 secondes
  - Latence moyenne pour une ouverture de session NetScaler Gateway : >120 à 440 ms
  - Latence moyenne pour une demande Worx Store : 2 à 3 secondes
- Une détérioration de la performance physique, telle qu'une insuffisance des ressources d'UC et de mémoire, a été observée sur les composants de l'infrastructure lorsque les limites de la montée en charge ont été atteintes.

- Réponses non valides sur les boîtiers NetScaler Gateway et XenMobile.
- Réponse lente de la console XenMobile lors des périodes pendant lesquelles les charges sont élevées.



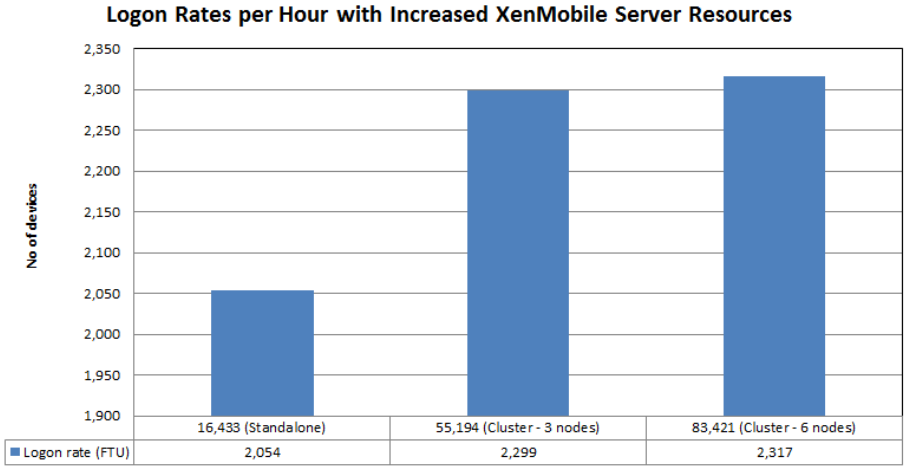


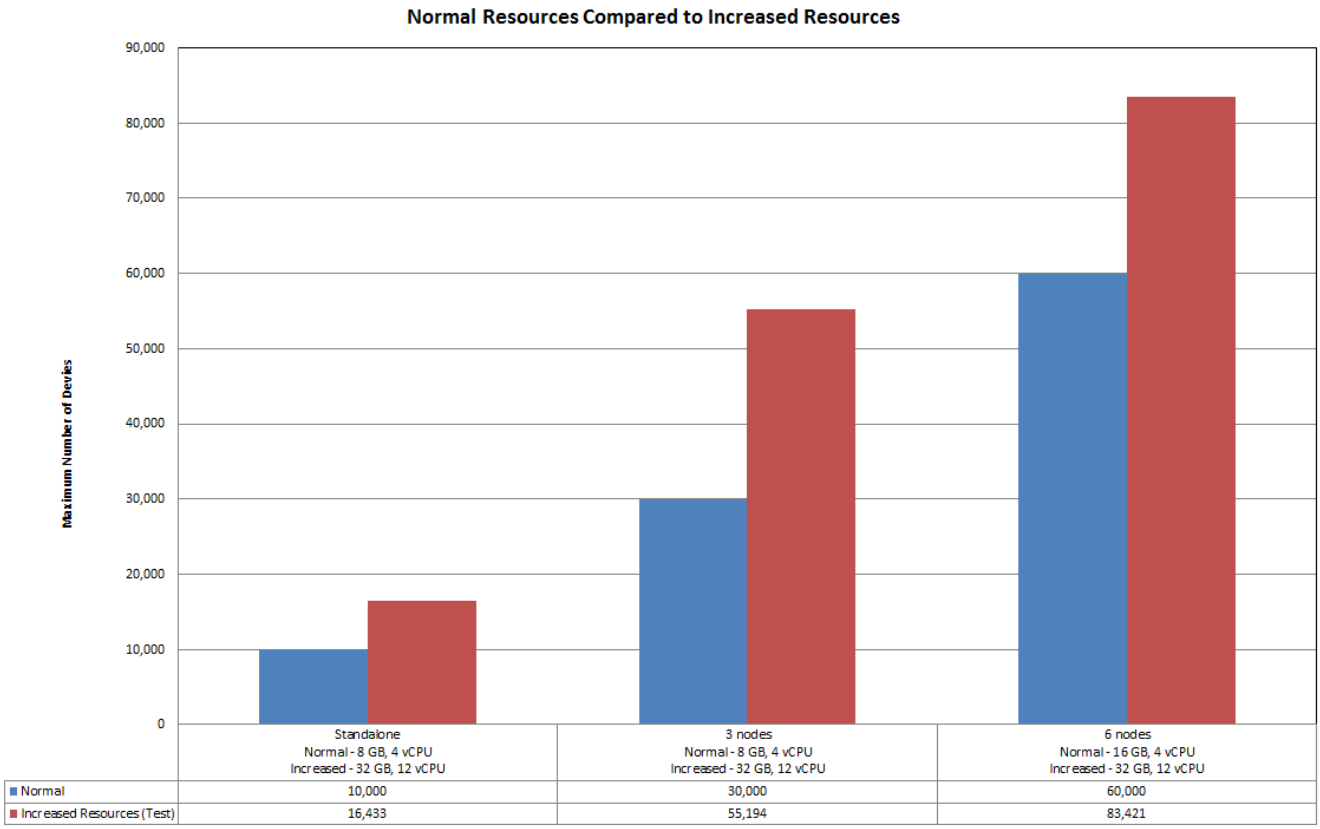
Le pourcentage d'erreur dans la figure précédente comprend l'ensemble des erreurs rencontrées relatives aux demandes correspondant à chaque opération et n'est pas limité aux ouvertures de session. Le pourcentage d'erreur se situe dans la limite autorisée de 1 % pour chaque série de tests comme défini dans les critères de sortie.

Les résultats de ce test fournissent des indications sur la stratégie de déploiement de XenMobile Enterprise Edition avec un nombre inférieur de nœuds afin de prendre en charge plus d'appareils. Le test a été effectué avec des ressources supplémentaires pour les composants matériels (processeur et mémoire) de chaque nœud du serveur XenMobile, de façon à pouvoir mesurer les capacités de montée en charge. Cela s'est traduit par une augmentation du nombre maximal de sessions/appareils pris en charge par les nœuds du serveur XenMobile, en comparaison avec les tests effectués avec des ressources normales et le même nombre de nœuds.

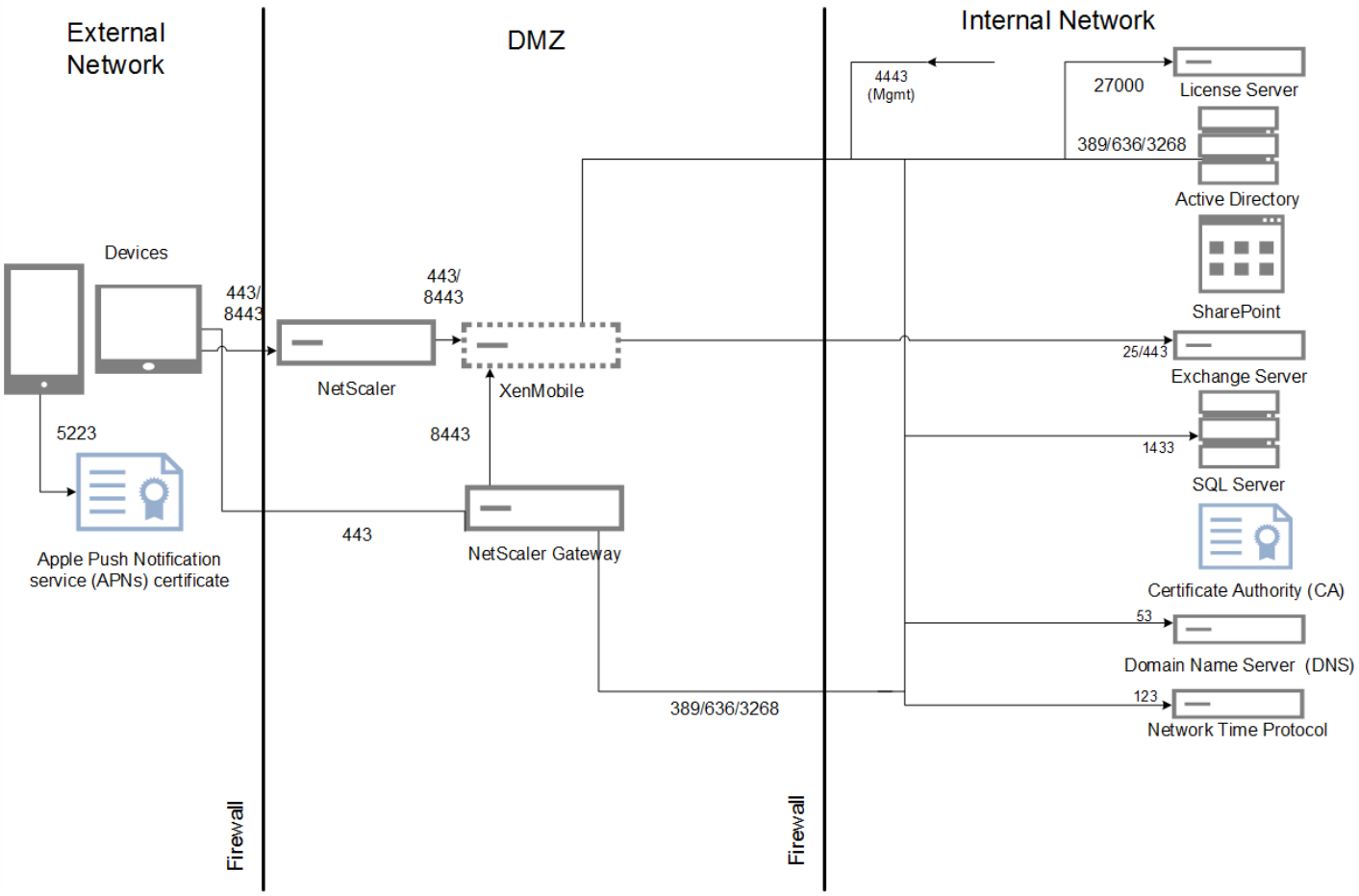
Capacité à monter en charge			
Nombre maximal d'appareils réels	16 433	55 194	83 421
Taux d'ouverture de session			
Première utilisation - ajout de nouveaux utilisateurs	2 054	2 299	2 317
Configuration			

Environnement de référence	VPX-XenMobile en mode autonome	MPX-XenMobile en cluster 3	MPX-XenMobile en cluster 6
NetScaler Gateway	MPX-10500	MPX-10500	MPX-20500
XenMobile - mode	Autonome	Cluster	Cluster
XenMobile - cluster	S.O.	3	6
XenMobile - boîtier virtuel	Mémoire : 32 Go Processeurs virtuels : 12	Mémoire : 32 Go Processeurs virtuels : 12	Mémoire : 32 Go Processeurs virtuels : 12
Base de données Device Manager	Externe - S SQL Server Mémoire : 16 Go Processeurs virtuels : 12	Externe - SQL Server Mémoire : 32 Go Processeurs virtuels : 12	Externe - SQL Server Mémoire : 32 Go Processeurs virtuels : 16
Active Directory	Mémoire : 8 Go Processeurs virtuels = 4	Mémoire : 16 Go Processeurs virtuels : 4	Mémoire : 16 Go Processeurs virtuels : 4

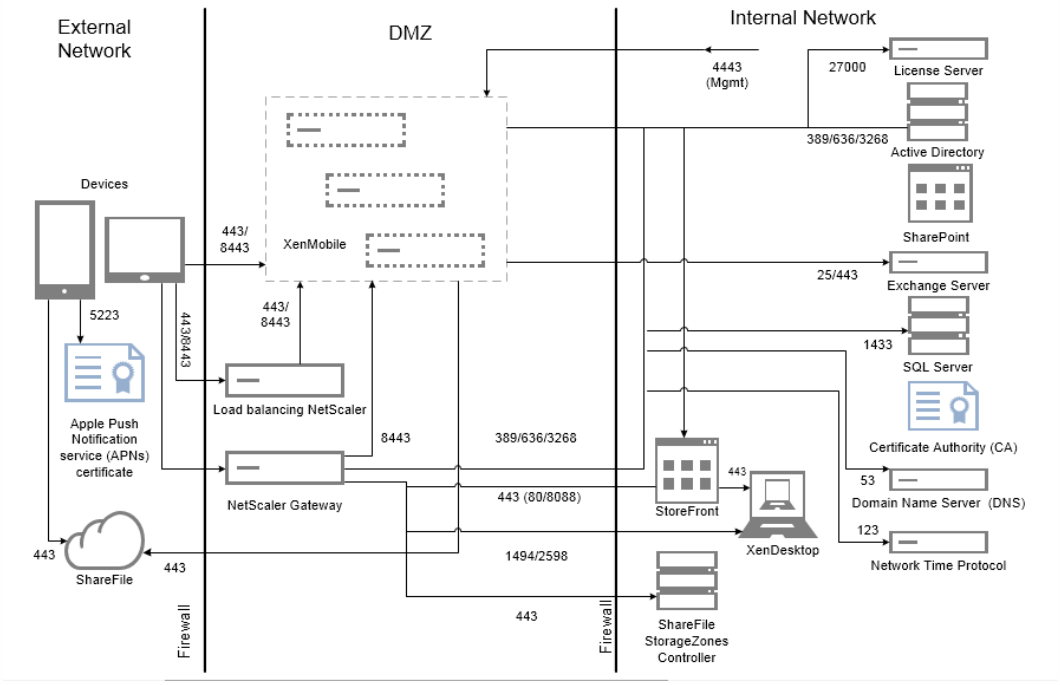




La figure suivante montre l'architecture de référence pour un déploiement à petite échelle. Il s'agit d'une architecture autonome qui prend en charge jusqu'à 10 000 appareils.



La figure suivante montre l'architecture de référence pour un déploiement d'entreprise. Il s'agit d'une architecture en cluster avec déchargement SSL pour MAM sur HTTP qui prend en charge 10 000 appareils ou plus.



Les tests ont été exécutés sur XenMobile Enterprise pour établir un banc d'essai. En vue de cibler les déploiements à petite et à grande échelle, 1 000 à 100 0000 appareils ont été utilisés pour les mesures.

Des charges de travail ont été créées pour simuler des cas d'utilisation réels. Ces charges de travail ont été exécutées pour chaque test afin d'étudier les effets sur l'inscription et les taux d'ouverture de session. L'objectif de ces tests était d'obtenir un taux d'ouverture de session optimal compris dans la marge d'erreur autorisée, comme détaillé dans les critères de sortie. Les taux d'ouverture de session sont un facteur critique pour déterminer la configuration matérielle recommandée pour les composants d'infrastructure.

Les demandes d'ouverture de session des charges de travail intégrées (FTU) comprenaient les opérations de détection automatique, d'authentification et d'enregistrement des appareils. Les abonnements aux applications, ainsi que les opérations d'installation et de démarrage ont été réparties de manière uniforme au cours de la période de test, ce qui a réuni les meilleures conditions pour une simulation réelle des actions de l'utilisateur. Au terme du test, la session a été fermée. Les demandes d'ouverture de session pour la charge de travail des utilisateurs existants comprenaient uniquement des demandes d'authentification.

Les charges de travail des utilisateurs sont définies comme suit :

Sessions utilisateur et appareils	Inclut les ouvertures de session NetScaler Gateway, les énumérations, l'enregistrement des appareils, et ainsi de suite pour chaque session.
Worx Store démarre	Les utilisateurs lancent Worx Store à plusieurs reprises et chaque fois qu'ils s'abonnent à une ou à plusieurs applications, ou qu'ils les installent, qu'il s'agisse d'applications mobiles (Web/SaaS/MDX) ou Windows (HDX).
Authentification unique des applications Web ou SaaS par appareil	Permet de lancer une séquence d'applications Web/SaaS jusqu'à ce que XenMobile exécute l'authentification unique et renvoie l'URL de l'application réelle. Le trafic n'a pas été envoyé aux applications réelles.
Téléchargements d'applications MDX par appareil	Compte le nombre de téléchargements d'applications MDX (peut se produire sur les lancements Worx Store). Pour iOS, cela comprend également l'automatisation de l'installation d'applications depuis Apple ITMS, qui utilise les nouvelles API du service de jeton/tms sur NetScaler Gateway.

Notes et hypothèses

Afin d'étendre les capacités de XenMobile au-delà de 30 000 appareils, vous devez régler les paramètres de serveur suivants :

Config File - /opt/sas/sw/tomcat/inst1/webapps/ROOT/WEB-INF/classes/push_services.xml

-

Config File - /opt/sas/sw/tomcat/inst1/webapps/ROOT/WEB-INF/classes/ew-config.properties

- ios.mdm.apns.connectionPoolSize=15
- hibernate.c3p0.max_size=1000

Vous devez effectuer ces modifications sur tous les nœuds XenMobile, puis redémarrer le serveur.

Les scénarios suivants ne sont pas couverts dans le cadre des tests de capacité à monter en charge. Ces scénarios seront pris en compte pour l'amélioration des tests :

- Les appareils connectés Android ne sont pas testés.
- Le déploiement de paquetage n'est pas testé.
- La plate-forme Windows n'est pas testée.

Chaque XenMobile prend en charge un maximum de 10 000 connexions simultanées.

Les tests ont été exécutés dans des conditions idéales sur un réseau local pour ignorer les problèmes de latence réseau. Dans un environnement réel, la capacité à monter en charge dépend également de la bande passante disponible, plus particulièrement pour les téléchargements d'applications.

Charge de travail intégrée (FTU)

La charge de travail intégrée (FTU) est définie comme la première fois qu'un utilisateur accède à l'environnement XenMobile. Les opérations comprises dans cette charge de travail étaient les suivantes :

- Découverte automatique
- Inscription
- Authentification
- Enregistrement de l'appareil
- Mise à disposition d'applications (Web, SaaS et mobiles MDX)
  - Abonnement aux applications (y compris les téléchargements d'images et d'icônes)
  - Installation des applications MDX souscrites

- Lancement des applications (Web, SaaS et mobiles MDX) y compris vérification de l'état des appareils
- Transmission de stratégies (pour iOS)
- Nombre minimal de connexions WorxMail et WorxWeb (tunnels VPN) : deux connexions
- Installation des applications requises via XenMobile

Les paramètres de charge de travail sont définis dans le tableau suivant :

Appareils	Enregistrements d'appareils	Énumérations	Applications énumérées par appareil	Lancements WorxStore par appareil	Authentification unique des applications Web ou SaaS par appareil	Téléchargements d'applications MDX par appareil	Téléchargements d'applications obligatoires déclenchés par le serveur XenMobile	Stratégies déployées par appareil (iOS)
1000	1000	1000	14	4	4	2	2	2
10 000	10 000	10 000	14	4	4	2	2	2
30 000	30 000	30 000	14	4	4	2	2	2
60000	60000	60000	14	4	4	2	2	2
100000	100000	100000	14	4	4	2	2	2

Charge des utilisateurs existants qui utilisent uniquement des connexions Worx

Le tableau suivant affiche la charge des utilisateurs existants (avec des connexions Worx uniquement). Cette charge de travail simulait un utilisateur utilisant les applications WorxMail et WorxWeb. Cette simulation a été utilisée pour mesurer la capacité à monter en charge de NetScaler Gateway dans la configuration XenMobile. Ceci est réalisable car en utilisant uniquement ces deux applications Worx, la charge réseau est minimale. Pour l'application WorxWeb, l'utilisateur accède à des sites Web internes qui ne déclenchent pas l'authentification unique (SSO) au serveur XenMobile. Les opérations dans ce mode étaient les suivantes :

- Authentification (NetScaler Gateway et XenMobile)
- Nombre de connexions WorxMail et WorxWeb (tunnels VPN) : quatre connexions

Le tableau suivant présente les paramètres de charge de travail pour les utilisateurs existants.

Appareils	Énumérations	Applications énumérées par appareil	Tunnels VPN par appareil[1]
1000	1000	14	4
10 000	10 000	14	4
30 000	30 000	14	4
60000	60000	14	4
100000	100000	14	4

1. Le nombre de tunnels VPN correspond aux connexions WorxMail et WorxWeb.

Les profils de connexion pour WorxMail et WorxWeb sont décrits dans le tableau suivant :

Connexion d'appareils	Type de connexion	Données envoyées par session[1]	Données reçues par session[1]
Connexion WorxMail n° 1	Type 1[2]	4,1 Mo	4,1 Mo
Connexion WorxMail n° 2	Type 1	6,3 Mo	12,5 Mo

Connexion WorxWeb n° 1	Type 2[3]	5,2 Mo	15,7 Mo
Connexion WorxWeb n° 2	Type 2	4,1 Mo	3,4 Mo
Nombre total d'octets transférés par session[1]		~ 19,7 Mo	~ 40,7 Mo

1. Par session : 8 heures.

2. Type 1 : envoi et réception asymétriques avec des connexions à long terme (WorxMail avec une connexion à une boîte aux lettres Microsoft Exchange dédiée).

3. Type 2 : envoi et réception asymétriques avec des connexions qui se ferment et s'ouvrent de nouveau après un certain délai (connexions WorxWeb).

Ces recommandations sont basées sur les profils WorxMail et WorxWeb utilisés pour automatiser
une charge « moyenne ». Les modifications apportées aux détails de connexion affectent les résultats de l'analyse. Par exemple, si le nombre de connexions par utilisateur est augmenté, le nombre de sessions de NetScaler Gateway prises en charge peut être réduit.

Profils WorxMail et WorxWeb

Les profils utilisés pour chaque application sont conçus pour automatiser une charge « très importante ». Les tableaux suivants affichent les détails des profils de WorxMail et WorxWeb.

Profil WorxMail pour une charge de travail moyenne

Messages envoyés par jour	20
Messages reçus par jour	80
Messages lus par jour	80
Messages supprimés par jour	20
Taille moyenne des messages (Ko)	200

Profil WorxWeb pour charge de travail moyenne

Nombre d'applications Web lancées	10
Nombre de pages Web ouvertes manuellement	10
Nombre moyen de paires demande–réponse par application Web	100
Taille moyenne de la demande (octets)	300
Taille moyenne de la réponse (octets)	1000

Configuration et paramètres

Les configurations suivantes ont été utilisées lors de l'exécution des tests de capacité à monter en charge :

- Les serveurs virtuels de NetScaler Gateway et d'équilibrage de charge coexistaient sur le même boîtier NetScaler Gateway.
- Une clé de 2 048 bits a été utilisée sur NetScaler Gateway pour les transactions SSL.

Les taux d'ouverture de session constituent la base de cette analyse. Ils servent de ligne directive pour les composants d'infrastructure et leur configuration respective. Il est important de noter que les taux d'ouverture de session prennent en compte une marge d'erreur qui se compose des éléments suivants :

- Réponses non valides
  - Une réponse avec le code d'état 401/404 à la place de 200 est considérée comme non valide.
- Délais d'expiration des demandes
  - Une réponse est attendue dans les 120 secondes.
- Erreurs de connexion
  - Une réinitialisation de la connexion s'est produite.
  - Un arrêt brutal de connexion s'est produit.

Le taux d'ouverture de session est acceptable si le taux d'erreur global est inférieur à 1 % du nombre total de demandes envoyées à partir d'un appareil donné. Le taux d'erreur inclut les erreurs correspondant à chaque opération de charge de travail individuelle, ainsi que la performance physique du composant d'infrastructure, comme l'insuffisance des ressources d'UC et de mémoire.

Le tableau suivant dresse la liste des logiciels d'infrastructure XenMobile utilisés pour ces tests.

Composant	Version
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0.824
Base de données externe	Microsoft SQL Server 2014

Les tests de capacité à monter en charge ont été exécutés sur une plate-forme XenServer comme décrit dans le tableau suivant.

Fournisseur	Genuine Intel
Modèle	UC Intel Xeon — E5645 @ 2,40 GHz (nombre d'UC = 24)

Cela comprend les services de base d'infrastructure (par exemple, Active Directory, Windows Domain Name Service (DNS), autorité de certification, Microsoft Exchange, etc.), ainsi que les composants XenMobile (boîtier virtuel XenMobile et boîtier virtuel NetScaler Gateway VPX, le cas échéant).

À propos de XenMobile Cloud

Jul 27, 2016

XenMobile Cloud est un service qui offre un environnement de gestion de la mobilité d'entreprise (EMM) XenMobile permettant de gérer les applications et les appareils, ainsi que les utilisateurs ou les groupes d'utilisateurs. Avec XenMobile Cloud, Citrix gère la configuration et la maintenance de l'infrastructure sur site via le groupe Citrix Cloud Operations. La séparation vous permet de vous concentrer uniquement sur l'expérience utilisateur et sur la gestion des appareils, des stratégies et des applications. XenMobile Cloud remplace également le besoin d'acheter et de gérer des licences avec des frais d'abonnement.

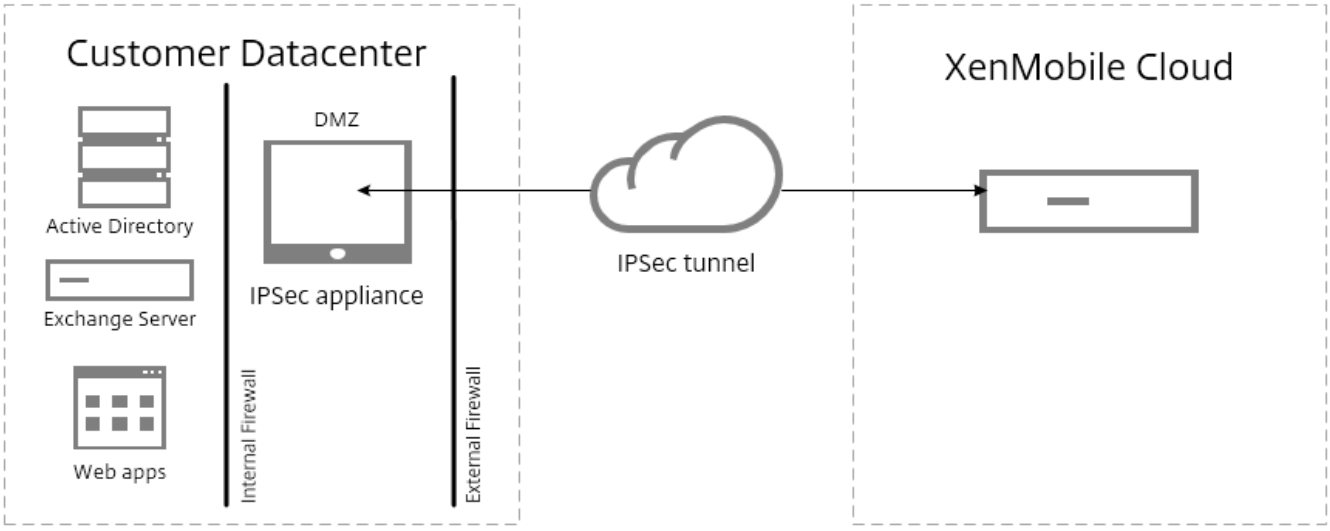
Les administrateurs de Cloud Operations peuvent gérer la maintenance et la configuration de la connectivité réseau, ainsi que l'intégration de produits Citrix tels que NetScaler, XenApp, XenDesktop, StoreFront et ShareFile. L'environnement de cloud est hébergé dans des centres de données Amazon situés dans le monde entier pour assurer des performances élevées, une réponse et une assistance rapides.

Pour commencer à utiliser XenMobile Cloud, accédez à https://www.citrix.com/products/xenmobile/tech-info/cloud.html

Remarque

- Le client d'assistance à distance n'est pas disponible dans XenMobile Cloud versions 10.x pour Windows CE et pour appareils Samsung Android.
- Les composants côté serveur de XenMobile Cloud ne sont pas conformes à la norme FIPS 140-2.
- Citrix ne prend pas en charge l'intégration de syslog dans XenMobile Cloud avec un serveur syslog sur site. Au lieu de cela, vous pouvez télécharger les journaux à partir de la page de support dans la console XenMobile. Ce faisant, vous devez cliquer sur **Tout télécharger** pour obtenir les journaux système. Pour de plus amples informations, consultez la section Visualisation et analyse des fichiers journaux dans XenMobile.

L'architecture de base de XenMobile Cloud est illustrée dans la figure suivante. Pour accéder à des diagrammes d'architecture de référence détaillés, consultez la section « Reference Architecture for Cloud Deployments » du Manuel de déploiement de XenMobile.



Vous pouvez intégrer l'architecture XenMobile Cloud au sein de votre infrastructure en installant et en déployant Citrix CloudBridge ou à l'aide d'une passerelle IPsec existante dans votre centre de données.

Cette architecture vous permet de bénéficier de l'utilisation de NetScaler dans le cloud, géré par le groupe Cloud Operations, ou dans votre centre de données. Lorsqu'il est utilisé dans le centre de données, NetScaler vous offre un point de gestion unique pour contrôler l'accès et limiter les actions au cours des sessions en fonction de l'identité de l'utilisateur et du périphérique de point de terminaison. Ce déploiement améliore la sécurité des applications, la protection des données et la gestion de la conformité.

Pour télécharger et installer Citrix CloudBridge, accédez à https://www.citrix.com/downloads/cloudbridge.html

Rôles dans XenMobile Cloud

XenMobile Cloud utilise le même contrôle d'accès basé sur un rôle (RBAC) qu'un déploiement de XenMobile. La différence avec XenMobile Cloud est que le groupe Citrix Cloud Operations gère tout rôle, y compris le provisioning, lié à l'infrastructure.

La figure suivante illustre la console RBAC pour XenMobile Cloud.

XenMobile implémente quatre rôles utilisateur par défaut de façon à séparer logiquement l'accès aux fonctions système. Les rôles par défaut sont les suivants :

- **Administrateur**. Accorde un accès complet au système.
- **Assistance**. Accorde l'accès à l'assistance à distance.
- **Utilisateur**. Accorde aux utilisateurs l'accès à l'inscription d'appareils et à l'utilisation du portail en libre-service.
- **Provisioning**. Accorde aux administrateurs la capacité de provisionner tous les appareils Windows Mobile/CE en tant que groupe à l'aide de l'outil de provisioning d'appareil. Ce rôle est géré par le groupe Cloud Operations.

Vous pouvez aussi utiliser les rôles par défaut en tant que modèles que vous personnalisez pour créer de nouveaux rôles utilisateur autorisés à accéder à des fonctions système spécifiques au-delà des fonctions définies par les rôles par défaut.

Vous pouvez attribuer des rôles à des utilisateurs (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, si les utilisateurs ADGroupA peuvent localiser les appareils appartenant à l'entreprise, et que les utilisateurs ADGroupB peuvent réinitialiser les appareils appartenant aux employés, alors un utilisateur qui appartient aux deux groupes peut localiser et réinitialiser les appareils appartenant à l'entreprise et aux 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 nouveau rôle.
- Ajouter des groupes à un rôle.
- Associer des utilisateurs locaux aux rôles.

Vous pouvez attribuer les rôles suivants. Le groupe Citrix Cloud Operations gère tout rôle qui ne se trouve pas sur cette liste.

Section principale	Section	Page	Page visible pour
Tableau de bord	ALL	ALL	Administrateur informatique
Gérer	Appareils	ALL	Administrateur informatique
Gérer	Inscription	ALL	Administrateur informatique
Configurer	Stratégies applicatives	ALL	Administrateur informatique
Configurer	Applications	ALL	Administrateur informatique
Configurer	Actions	ALL	Administrateur informatique
Configurer	Groupes de mise à disposition	ALL	Administrateur informatique

Configurer	Settings	Certificats	Administrateur cloud et administrateur informatique
Configurer	Settings	Modèles de notification	Administrateur informatique
Configurer	Settings	Contrôle d'accès basé sur un rôle	Administrateur cloud et administrateur informatique
Configurer	Settings	Inscription	Administrateur informatique
Configurer	Settings	Utilisateurs et groupes locaux	Administrateur cloud et administrateur informatique
Configurer	Settings	Gestion des versions	Administrateur cloud et administrateur informatique
Configurer	Settings	Workflows	Administrateur informatique
Configurer	Settings	Fournisseurs d'informations d'identification	Administrateur informatique
Configurer	Settings	Entités PKI	Administrateur informatique
Configurer	Settings	Propriétés de client	Administrateur informatique
Configurer	Settings	NetScaler Gateway	Administrateur cloud uniquement Ou administrateur informatique uniquement
Configurer	Settings	Passerelle SMS opérateur	Administrateur informatique
Configurer	Settings	Serveur de notification	Administrateur cloud et administrateur informatique
Configurer	Settings	ActiveSync Gateway	Administrateur informatique
Configurer	Settings	VPP iOS	Administrateur informatique
Support	Opérations de journal	Paramètres du journal	Administrateur cloud et administrateur informatique et

			support technique
Configurer	Settings	Propriétés du serveur	Administrateur cloud et administrateur informatique et support technique
Configurer	Settings	Informations d'identification Google Play	Administrateur informatique
Configurer	Settings	LDAP	Administrateur informatique
Configurer	Settings	Contrôle d'accès réseau	Administrateur informatique
Support	Pack de support	Créer des packs d'assistance	Administrateur cloud et support technique
Configurer	Settings	iOS Device Enrollment Program	Administrateur informatique
Configurer	Settings	Fournisseur de services mobiles	Administrateur informatique
Configurer	Settings	Samsung KNOX	Administrateur informatique
Configurer	Settings	XenApp/ XenDesktop	Administrateur informatique
Configurer	Settings	ShareFile	Administrateur informatique
Support	Advanced	Informations de cluster	Administrateur cloud et support technique
Support	Advanced	Nettoyage de la mémoire	Administrateur cloud et support technique
Support	Advanced	Propriétés de la mémoire Java	Administrateur cloud et support technique
Support	Advanced	Macros	Administrateur informatique
Assistant FTU	Configuration initiale	NetScaler Gateway	Administrateur cloud uniquement Ou administrateur informatique uniquement

Configurer	Settings	Assistance Worx Home	Administrateur informatique
Configurer	Settings	Personnalisation Worx Store	Administrateur informatique
Support	Diagnostics	Contrôles de connectivité dans NetScaler Gateway	Administrateur cloud et administrateur informatique et support technique
Support	Diagnostics	Contrôles de connectivité dans XenMobile	Administrateur cloud et administrateur informatique et support technique
Support	Opérations de journal	Journaux	Administrateur cloud et administrateur informatique et support technique
Support	Advanced	Configuration du PKI	Administrateur cloud et administrateur informatique
Support	Outils	Utilitaire de signature APNS	Support technique
Support	Outils	Citrix Insight Services	Administrateur cloud et administrateur informatique et support technique
Assistant FTU	Configuration initiale	Certificat SSL	Administrateur cloud et administrateur informatique
Assistant FTU	Configuration initiale	Configuration du LDAP	Administrateur informatique
Assistant FTU	Configuration initiale	Serveur de notification	Administrateur cloud et administrateur informatique
Assistant FTU	Configuration initiale	Récapitulatif	Administrateur cloud et administrateur informatique
Support	Liens	Centre de connaissances de Citrix	Administrateur cloud et administrateur informatique et support technique
Support	Outils	État NetScaler Connector de	Administrateur informatique

		l'appareil	
Support	Opérations de journal	Paramètres de journal->Taille du journal	Administrateur cloud et support technique

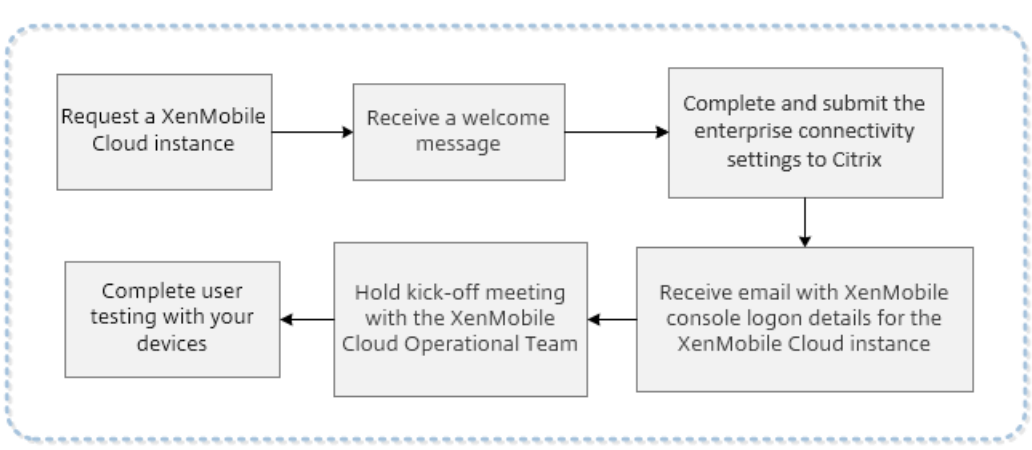
Pour obtenir des instructions détaillées sur la personnalisation des rôles, veuillez consulter la section Configuration de rôles avec RBAC.

Pour demander un redémarrage des nœuds du serveur, contactez le support technique à l'adresse https://www.citrix.com/contact/technical-support.html

Administration et conditions requises par XenMobile Cloud

Jul 27, 2016

Les étapes qui composent le processus d'intégration à partir du moment où vous demandez une instance de XenMobile Cloud jusqu'aux tests utilisateur avec les appareils dans votre organisation sont illustrées dans la figure suivante. Lors de l'évaluation ou de l'achat de XenMobile Cloud, l'équipe XenMobile Cloud Operational offre un soutien constant tant au niveau de l'intégration que de la communication afin de s'assurer que les services XenMobile Cloud essentiels sont opérationnels et configurés correctement.



Citrix héberge et met à disposition votre solution XenMobile Cloud. Certaines exigences en matière de port et de communication, cependant, sont requises pour se connecter à l'infrastructure XenMobile Cloud pour les services d'entreprise, tels que Active Directory. Consultez les sections suivantes pour préparer votre déploiement XenMobile Cloud.

Passerelles de tunnel IPSec XenMobile Cloud

Vous pouvez utiliser un connecteur d'entreprise XenMobile, un tunnel IPsec pour connecter l'infrastructure XenMobile Cloud avec les services d'entreprise, tels que Active Directory.

Les passerelles IPsec répertoriées sur le site Web des services Web Amazon suivant ont été officiellement testées et sont prises en charge avec la solution XenMobile Cloud : http://aws.amazon.com/vpc/faqs/. Accédez à « Q : Quels sont les périphériques de passerelle client dont la compatibilité avec Amazon VPC a été vérifiée ? » pour trouver la liste des passerelles prises en charge.

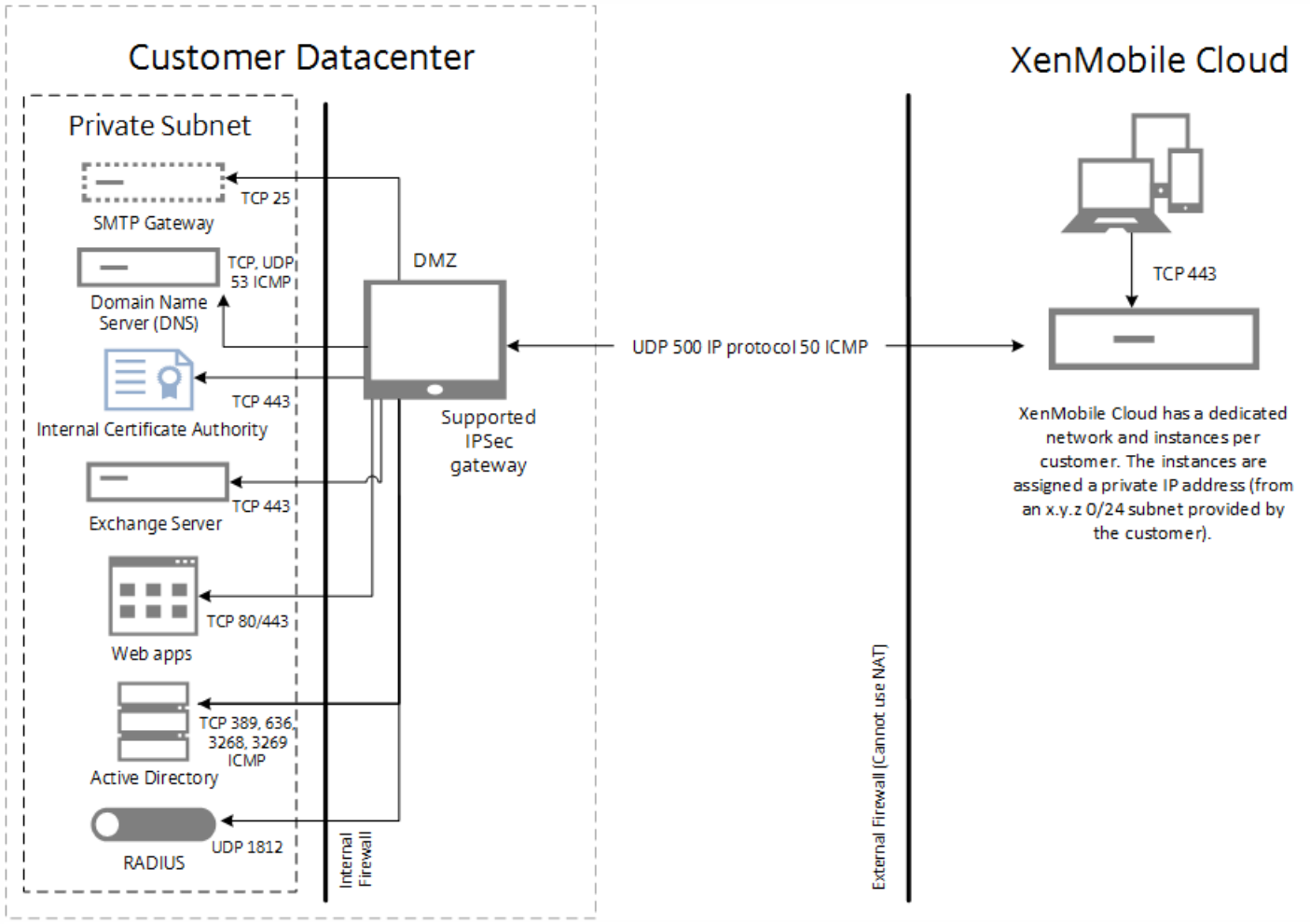
> ## Remarque
>
> Si votre passerelle IPSec ne figure pas dans la liste, il est possible qu'elle fonctionne avec XenMobile Cloud, mais elle prendra plus de temps à configurer, et vous devrez peut-être utiliser l'une des passerelles IPSec officiellement prises en charge comme solution de secours.

Votre passerelle IPSec doit disposer d'une adresse IP publique qui lui a été attribuée directement et l'adresse ne peut pas utiliser la traduction d'adresse réseau (NAT).

Votre connexion VPN AWS requiert une connexion persistance initiée du côté client. Configurez un ping permanent depuis votre environnement vers le sous-réseau Amazon VPC afin de garantir la continuité du service.

Votre connexion VPN AWS ne prend pas en charge de multiples associations de sécurité configurées sur la passerelle IPsec. Vous êtes limité à une seule paire d'association de sécurité par tunnel, une entrante et une sortante. Consolidez vos règles et filtres pour vous assurer qu'ils n'autorisent pas le trafic indésirable.

La figure suivante montre comment le tunnel IPsec est configuré dans la solution XenMobile Cloud pour se connecter aux services de votre entreprise via plusieurs ports.



Le tableau suivant présente les exigences en matière de port et de communication pour un déploiement XenMobile Cloud, y compris les exigences du tunnel IPSec.

Source	Destination	Protocoles	Port	Description
Pare-feu externe (edge) : règles de trafic entrant				

Adresses IP publiques de XenMobile Cloud (AWS) IPCSEC VPN [1]	Appliance IPSec client	UPD	500	Configuration IPSec IKE.
Adresses IP publiques de XenMobile Cloud (AWS) IPCSEC VPN [1]	Appliance IPSec client	ID du protocole IP	50	Protocole ESP IPSec.
Adresses IP publiques de XenMobile Cloud (AWS) IPCSEC VPN [1]	Appliance IPSec client	ICMP		Pour la résolution des problèmes (peut être supprimé après la configuration).
Pare-feu externe (edge) : règles de trafic sortant				
Sous-réseau de la zone démilitarisée (DMZ) cliente	Adresses IP publiques de XenMobile Cloud (AWS) IPSec VPN [1]	UDP	500	Configuration IPSec IKE.
Sous-réseau de la zone démilitarisée (DMZ) cliente	Adresses IP publiques de XenMobile Cloud (AWS) IPSec VPN [1]	ID du protocole IP	50, 51	Protocole ESP IPSec.
Sous-réseau de la zone démilitarisée (DMZ) cliente	Adresses IP publiques de XenMobile Cloud (AWS) IPSec VPN [2]	ICMP		Pour la résolution des problèmes (peut être supprimé après la configuration).
Pare-feu internet : règles de trafic entrant				
Sous-réseau client /24 inutilisé et routable [2]	Serveurs DNS internes dans le data center client	TCP, UPP, ICMP	53	Résolution DNS.
Sous-réseau client /24 inutilisé et routable [2]	Contrôleurs de domaine Active Directory dans le data center client	LDAP (TCP)	389, 636 3268, 3269	Pour l'authentification de l'utilisateur Active Directory et les requêtes d'annuaire aux contrôleurs de domaine.
Sous-réseau client /24 inutilisé et	Contrôleurs de domaine Active	ICMP		Pour la résolution des problèmes (peut être supprimé une fois

routable [2]	Directory dans le data center client			l'installation complète terminée).
Sous-réseau client /24 inutilisé et routable [2]	Serveurs Exchange dans le data center client	SMTP (TCP)	25	Facultatif : pour les notifications par e-mail XenMobile.
Sous-réseau client /24 inutilisé et routable [2]	Serveurs Exchange dans le data center client	HTTP, HTTPS (TCP)	80, 443	Exchange ActiveSync, qui est nécessaire si le trafic ActiveSync est envoyé depuis l'appareil vers l'infrastructure XenMobile Cloud (via le tunnel IPSec) aux serveurs Exchange. Ceci n'est PAS nécessaire si l'appareil utilisateur communique avec un nom de domaine complet ActiveSync public via Internet et qu'il n'utilise pas le tunnel IPSec XenMobile pour accéder aux serveurs Exchange.
Sous-réseau client /24 inutilisé et routable [2]	Serveurs d'application, tels que des serveurs intranet/Web, des serveurs SharePoint, et ainsi de suite.	HTTP, HTTPS (TCP)	80, 443	Accès aux serveurs intranet et/ou d'application à partir d'appareils mobiles via le tunnel IPSec XenMobile. Chaque serveur d'application doit être ajouté aux règles de pare-feu avec le numéro de port nécessaire pour accéder à l'application (généralement le port 80 et/ou 443).
Sous-réseau client /24 inutilisé et routable [2]	Serveur PKI (si une PKI sur site est utilisée)	HTTPS (TCP)	443	Facultatif (non utilisé pour les POC XenMobile) : Cela peut être utilisé pour établir une intégration entre l'infrastructure de XenMobile Cloud et une infrastructure PKI sur site (telle qu'une autorité de certification Microsoft) pour établir une authentification par certificat au sein de la solution XenMobile.

Sous-réseau client /24 inutilisé et routable [2]	Serveur RADIUS	UDP	1812	Facultatif (non utilisé pour les POC XenMobile) : Cela peut être utilisé pour établir une authentification à deux facteurs dans la solution XenMobile.
Pare-feu internet : règles de trafic sortant				
Sous-réseaux clients internes, à partir desquels la console XenMobile doit être disponible	Sous-réseau client /24 inutilisé et routable [2]	TCP	4443	Console XenMobile App Controller (MAM) dans l'infrastructure de XenMobile Cloud.

[1] Sera fourni par l'équipe de XenMobile Cloud lorsque l'instance de XenMobile Cloud et les composants IPSec sont provisionnés dans l'infrastructure de XenMobile Cloud.

[2] Sous-réseau /24 inutilisé fourni par le client dans le cadre du processus de provisioning, qui n'entre pas en conflit avec les sous-réseaux internes du data center du client ; il est routable.

Si vous prévoyez de déployer XenMobile Mail Manager ou XenMobile NetScaler Connector pour filtrer la messagerie native, par exemple pour bloquer ou autoriser la connectivité à la messagerie à partir de clients de messagerie natifs sur les appareils mobiles des utilisateurs, veuillez consulter les exigences supplémentaires suivantes.

Certificat APNS Apple XenMobile

Si vous envisagez de gérer des appareils iOS avec votre déploiement XenMobile Cloud, vous avez besoin d'un certificat APNS d'Apple. Vous devez préparer le certificat avant de déployer la solution XenMobile Cloud. Pour obtenir des instructions détaillées, consultez la section Faire une demande de certificat APNS.

Certificat de notification push WorxMail pour iOS

Si vous souhaitez utiliser la notification push pour votre déploiement WorxMail, vous devez préparer un certificat APNS Apple pour la notification push iOS WorxMail. Pour de plus amples informations, veuillez consulter la section Notifications push pour WorxMail pour iOS.

MDX Toolkit XenMobile

Le MDX Toolkit est une technologie de wrapping d'application qui prépare les applications en vue de les déployer en toute sécurité avec XenMobile. Si vous voulez wrapper des applications, telles que Citrix WorxMail, WorxMail, WorxNotes,

QuickEdit, etc., vous devez installer le MDX Toolkit. Pour de plus amples informations, consultez la section À propos du MDX Toolkit.

Si vous envisagez de wrapper des applications iOS, vous devez disposer d'un compte Apple Developer pour créer les profils de distribution Apple nécessaires. Pour de plus amples informations, consultez la section Configuration système requise par le MDX Toolkit et le site Web Apple Developer.

Si vous envisagez de wrapper des applications pour des appareils Windows Phone 8.1, consultez la section Configuration système requise.

Découverte automatique XenMobile pour l'inscription d'appareils Windows Phone

Si vous souhaitez utiliser le service de découverte automatique de XenMobile pour votre Windows Phone 8.1, assurez-vous que vous disposez d'un certificat SSL public. Pour de plus amples informations, consultez la section Activer la découverte automatique pour l'inscription utilisateur dans XenMobile.

Console XenMobile

La solution XenMobile Cloud utilise la même console Web qu'un déploiement XenMobile sur site. L'administration quotidienne de votre solution Cloud, telle que la gestion des stratégies, la gestion des applications, la gestion des appareils, etc., est donc similaire à l'administration d'un déploiement XenMobile sur site. Pour de plus amples informations sur la gestion des applications et des appareils dans la console XenMobile, consultez la section Prise en main de la console XenMobile.

Inscription d'appareils XenMobile

Pour de plus amples informations sur les options d'inscription de XenMobile pour les différentes plates-formes, consultez la section Inscription d'utilisateurs et d'appareils.

Prise en charge de XenMobile

Pour de plus amples informations sur la manière d'accéder à des informations et outils de support dans la console XenMobile, consultez la section Support et maintenance de XenMobile.

Prise en charge des plates-formes dans XenMobile Cloud

Jul 27, 2016

Après avoir demandé une instance de XenMobile Cloud, vous pouvez, si vous le souhaitez, commencer la préparation de la prise en charge des plates-formes Android, iOS et Windows. À mesure que vous effectuez les étapes qui s'appliquent à votre environnement, conservez les informations à portée de façon à pouvoir les utiliser lors de la configuration des paramètres dans la console XenMobile.

Notez que ces exigences sont un sous-ensemble des exigences en matière de port et de communication que constitue le processus d'intégration de XenMobile Cloud. Pour de plus amples informations, consultez la section Administration et conditions requises par XenMobile Cloud.

- Créer les informations d'identification Google Play. Pour de plus amples informations, consultez la section Google Play Getting Started with Publishing.
- Créer un compte d'administrateur Android for Work. Pour de plus amples informations, consultez la section Gestion des appareils avec Android for Work dans XenMobile.
- Vérifier votre nom de domaine avec Google. Pour de plus amples informations, consultez la section Vérifier votre domaine pour Google Apps.
- Activer les API et créer un compte de service pour Android for Work. Pour de plus amples informations, consultez la section Google for Work Android.

- 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). Pour de plus amples informations, consultez le portail Apple Push Certificates Portal.
- Créer un jeton d'entreprise VPP (Volume Purchase Program). Pour de plus amples informations, consultez la section Programme d'achat en volume d'Apple.

- Créer un compte de développeur Microsoft Windows Store. Pour de plus amples informations, consultez la section Microsoft Windows Dev Center.
- Obtenir un ID Microsoft Windows Store Publisher. Pour de plus amples informations, consultez la section Microsoft Windows Dev Center.
- Obtenir un certificat d'entreprise de Symantec. Pour de plus amples informations, consultez la section Microsoft Windows Dev Center.
- Créer un jeton d'inscription d'application (AET). Pour de plus amples informations, consultez la section Microsoft Windows Dev Center.

Configuration système requise

Oct 17, 2016

Pour exécuter XenMobile 10,3, vous avez besoin de la configuration système minimale suivante :

- L'un des suivants :
  - XenServer (versions prises en charge : 6.5.x ou 6.2.x) ; pour plus de détails, reportez-vous à XenServer
  - VMware (versions prises en charge : ESXi 5.1, ESXi 5.5 ou ESXi 6.0) ; pour de plus amples informations, voir VMware. Veuillez noter que ESXi 6.0 est uniquement pris en charge sur XenMobile 10.3.x
  - Hyper-V (versions prises en charge : Windows Server 2008 R2, Windows Server 2012 ou Windows Server 2012 R2) ; pour de plus amples informations, voir Hyper-V
- Processeur double cœur
- Quatre processeurs virtuels
- 8 Go de RAM
- 50 Go d'espace disque

La configuration recommandée pour 10 000 périphériques et plus est la suivante :

- Processeur quadruple cœur avec 8 Go de RAM pour chaque nœud.

XenMobile version 10.3.x requiert le serveur de licences Citrix 11.12.1 ou une version plus récente.

Pour exécuter NetScaler Gateway avec XenMobile 10,3, vous avez besoin de la configuration système minimale suivante :

- L'un des suivants :
  - XenServer (versions prises en charge : 6.2.x, 6.1.x ou 6.0.x)
  - VMWare (versions prises en charge : ESXi 4.1, ESXi 5.1, ESXi 5.5, ESXi 6.0)
  - Hyper-V (versions prises en charge : Windows Server 2008 R2, Windows Server 2012 ou Windows Server 2012 R2)
- Deux processeurs virtuels
- 2 Go de RAM
- 20 Go d'espace disque

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.

XenMobile nécessite l'une des bases de données suivantes :

- Microsoft SQL Server

  Le référentiel XenMobile nécessite une base de données Microsoft SQL Server exécutant une des versions prises en charge suivantes (pour de plus amples informations sur les bases de données Microsoft SQL Server, voir Microsoft SQL Server) :

  Microsoft SQL Server 2016
  Microsoft SQL Server 2014
  Microsoft SQL Server 2012
  Microsoft SQL Server 2008 R2

Microsoft SQL Server 2008

XenMobile 10.1 prend en charge les groupes de disponibilité AlwaysOn SQL Server.

Citrix vous recommande d'utiliser Microsoft SQL à distance.

Remarque : vérifiez que le compte de service du serveur SQL à utiliser sur XenMobile dispose de l'autorisation de rôle DBcreator. Pour de plus amples informations sur les comptes de service SQL Server, consultez les pages suivantes sur le site Microsoft Developer Network (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**) :

Server Configuration - Service Accounts

Configure Windows Service Accounts and Permissions

Server-Level Roles

- PostgreSQL

  PostgreSQL est inclus avec XenMobile. Vous pouvez l'utiliser localement ou à distance.

  Remarque : toutes les éditions de XenMobile prennent en charge Remote PostgreSQL 9.3.11 pour Windows avec les limitations suivantes :

  - Jusqu'à 300 appareils pris en charge

    Utilisez SQL Server localement pour plus de 300 appareils.

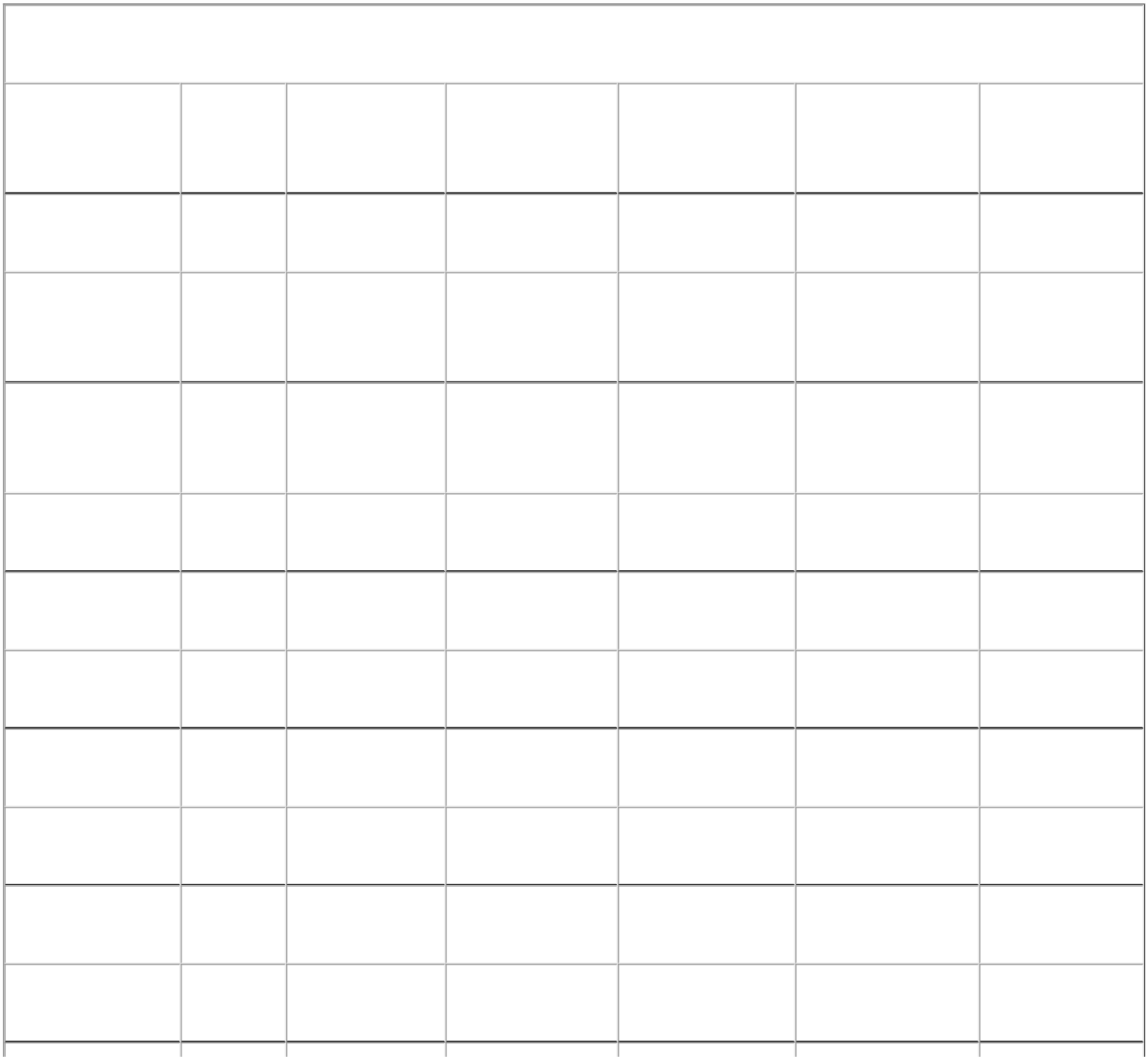
  - Mise en cluster non prise en charge

StoreFront 3.6
StoreFront 3.5
StoreFront 3.0
StoreFront 2.6
Interface Web 5.4
XenApp et XenDesktop 7.9
XenApp et XenDesktop 7.8
XenApp et XenDesktop 7.7
XenApp et XenDesktop 7.6
XenApp et XenDesktop 7.5
XenApp 6.5

XenMobile 10.3 prend en charge les serveurs de messagerie suivants :

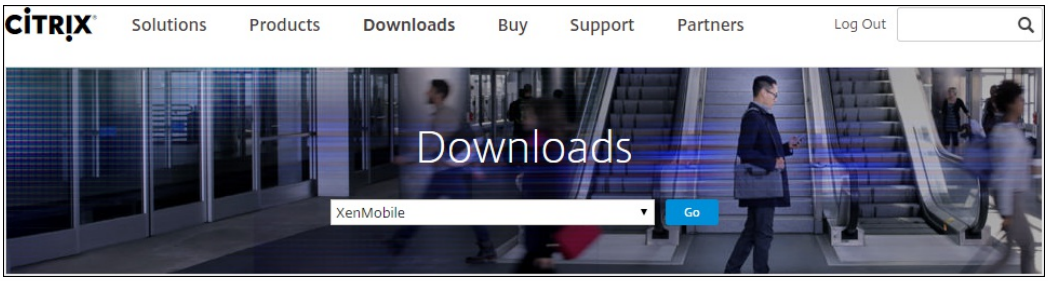
- Exchange 2016
- Exchange 2013
- Exchange 2010

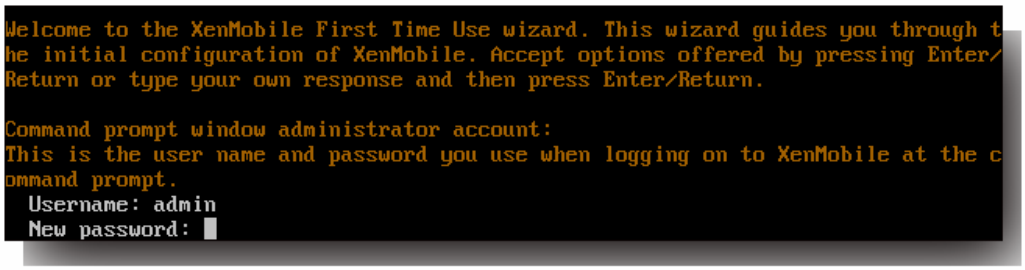
-
-



	• •		

•			





```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```

```
Database connection:
  Local or remote [l/r]: r
  Type (Microsoft SQL, PostgreSQL or MySQL) [mi/p/my]: mi
  Use SSL [y/n]: n
  Server: 198.0.2.10
  Port: 5432
  Username: postgres
  Password:
```

-
-

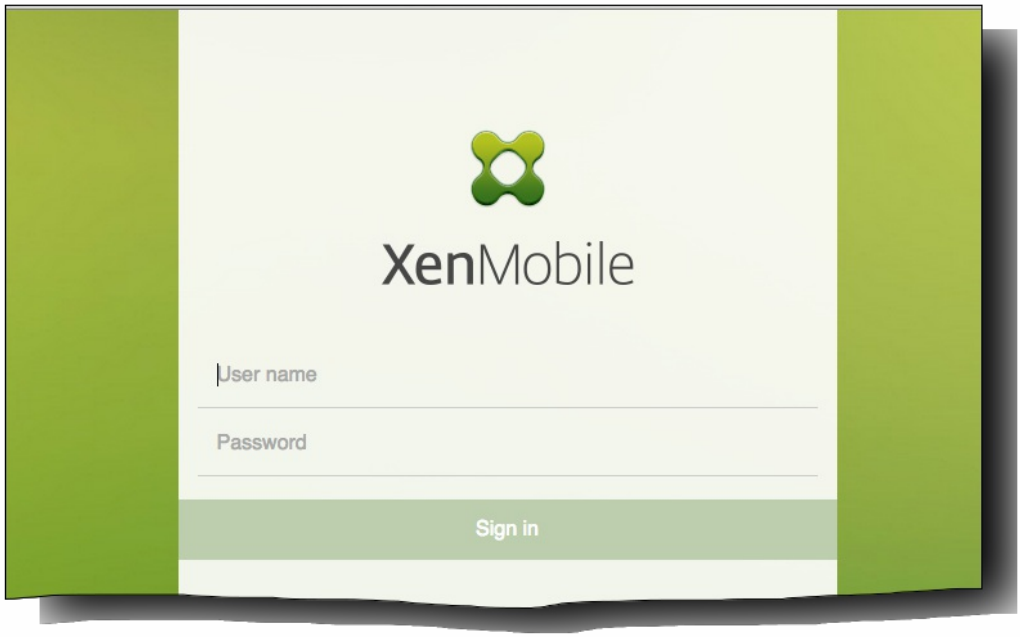
```
XenMobile hostname:
  Hostname: justan.example.com
```

```
HTTP [80]: 80
HTTPS with certificate authentication [443]: 443
HTTPS with no certificate authentication [8443]: 8443
HTTPS for management [4443]: 4443
```

```
The wizard will now generate an internal Public Key Infrastructure (PKI):
 - A root certificate
 - An intermediate certificate to issue device certificates during enrollment
 - An intermediate certificate to issue an SSL certificate
 - An SSL certificate for your connectors
  Do you want to use the same password for all the certificates of the PKI [y]:
  New password:
  Re-enter new password:
```

```
XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile cons
ole through a web browser.
  Username [administrator]: administrator
  Password:
  Re-enter new password:
```

```
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!

Upgrade:
  Upgrade from previous release (y/n) [n]:

Stopping configuration app...                                  [ OK ]
Starting configuration app...
  application started successfully                             [ OK ]
Stopping main app...                                           [ OK ]
Starting main app...
  this may take a few minutes.....................................................
.................................
  application started successfully                             [ OK ]

  To access the console, from a web browser, go to the following location and
  log on with your console credentials:
    https://203.0.113.8:4443/

Starting monitoring...                                         [ OK ]
```



-
-

-
-
-

-
-
-
-
-

-
-

-

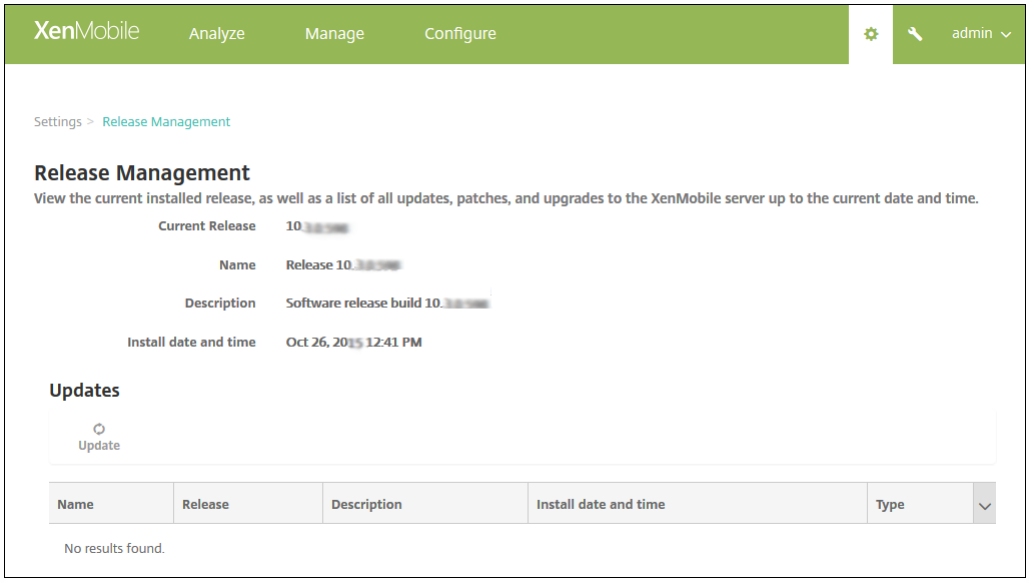
-

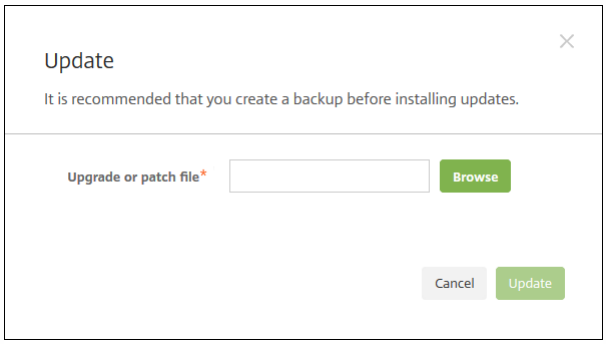
-

-

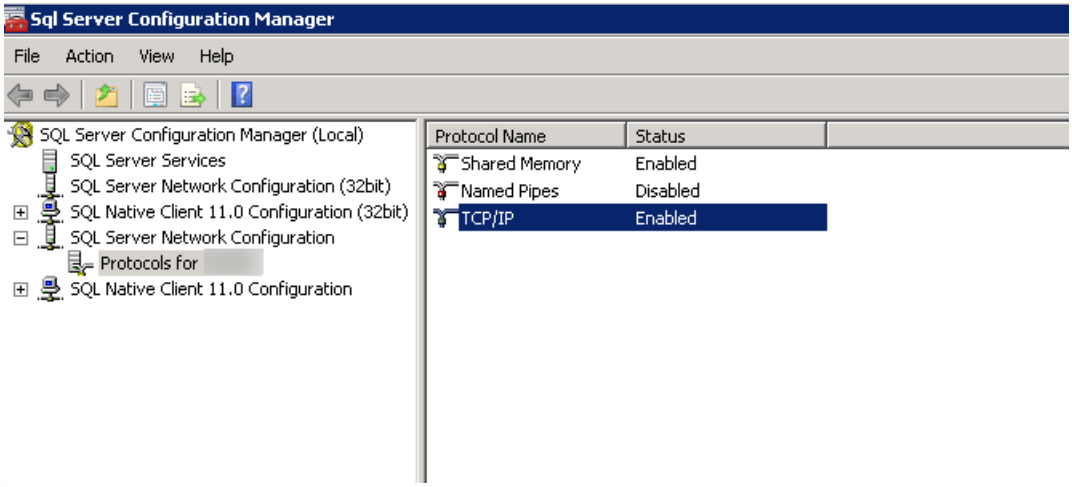
-

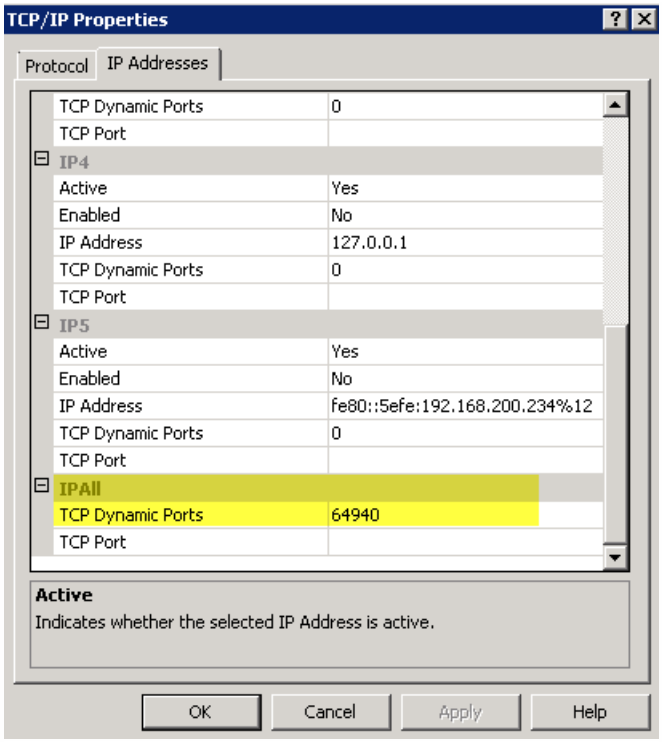
-
-
-

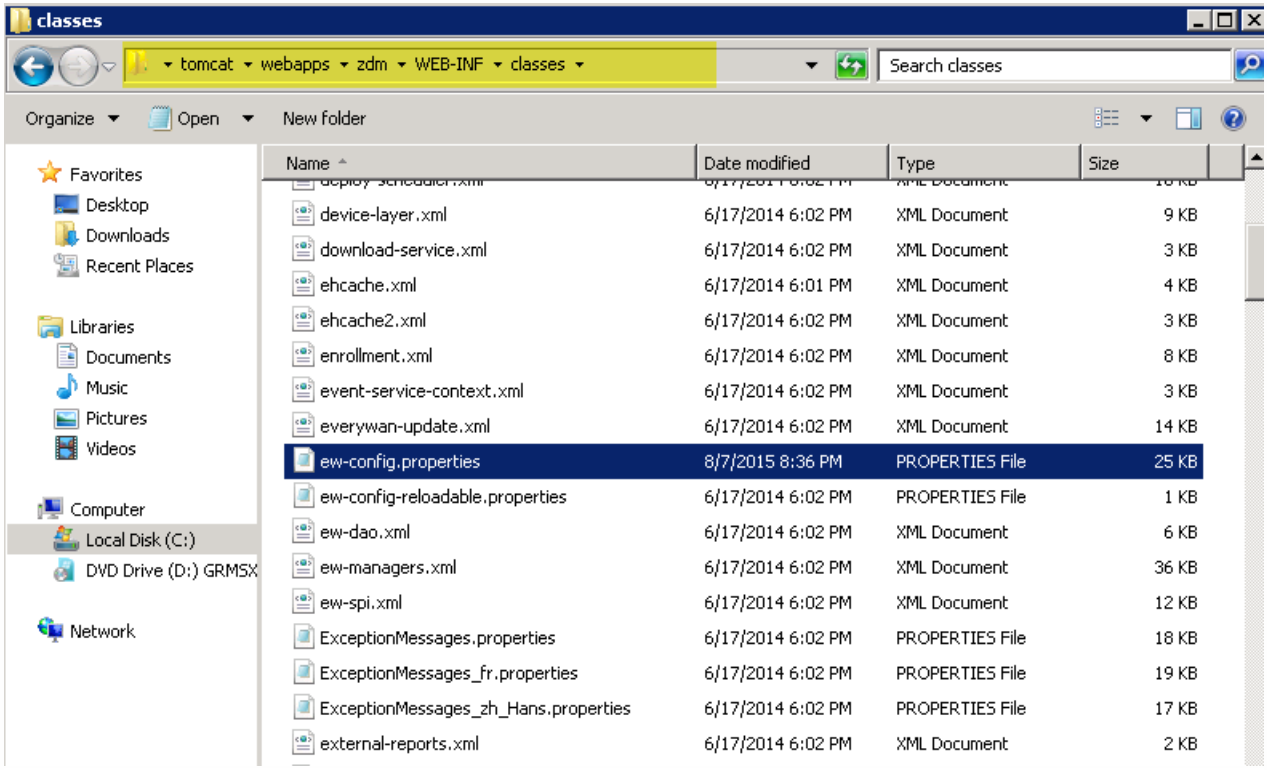




-
-
-





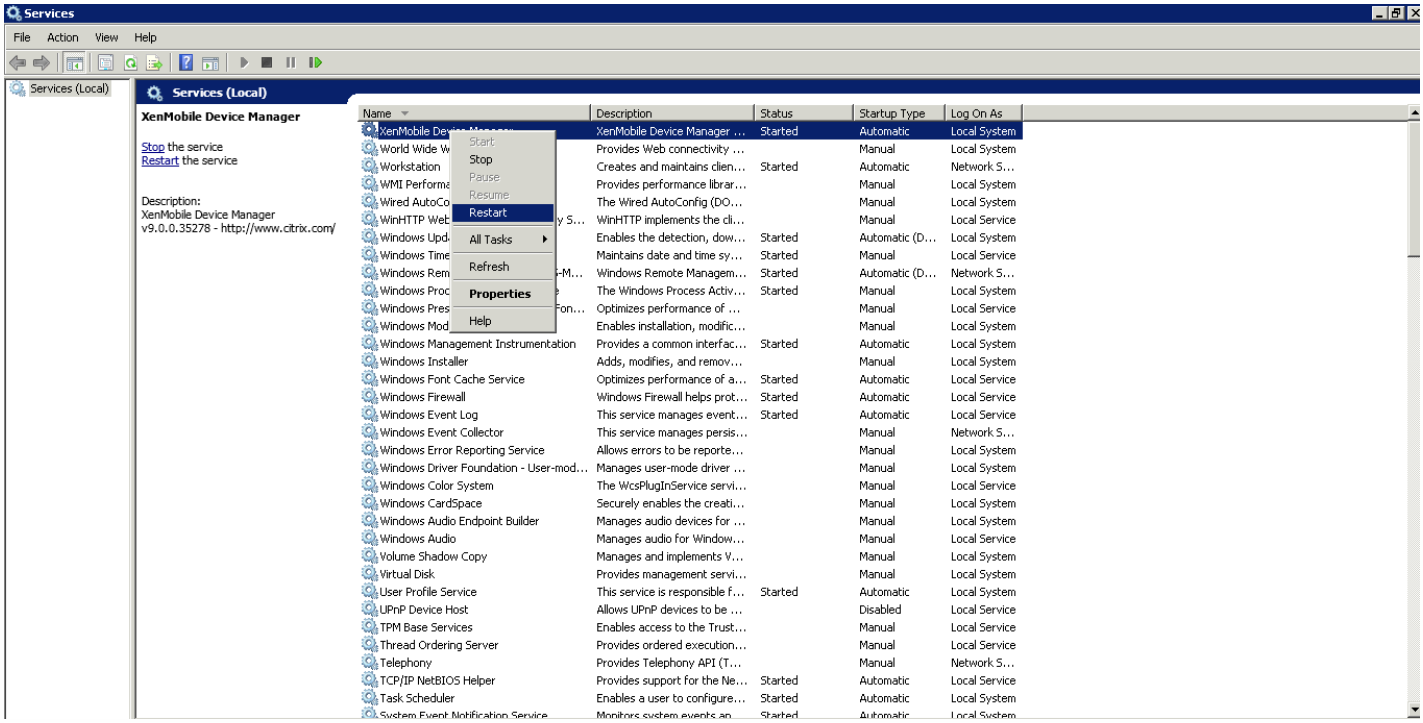


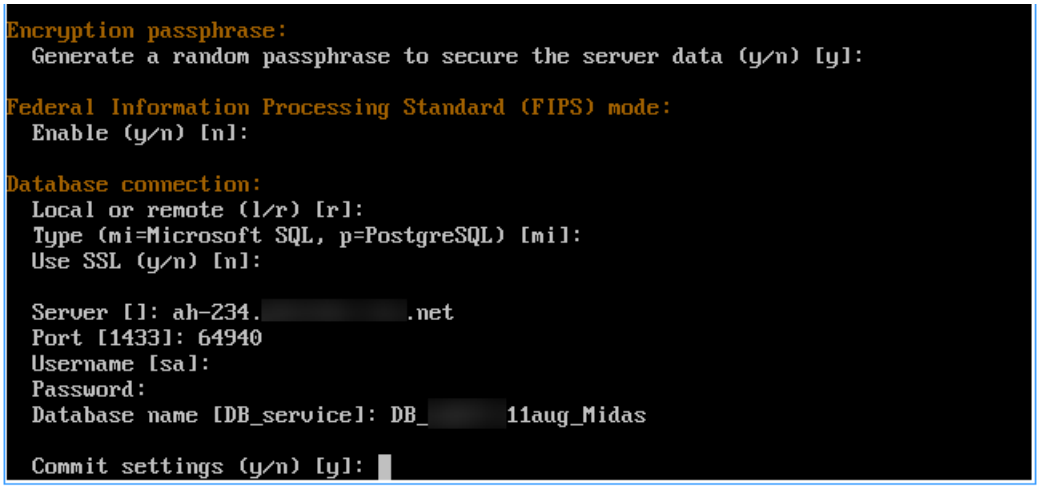
ew-config.properties

```
# For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
# For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress
# For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress;domain=sparus-
# Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@//localhost:1521/everywan
pooled.datasource.url=jdbc:jtds:sqlserver://ah-234              net/          -llaug;instance=
# Pooled datasource host name
pooled.datasource.hostname=ah-234.          .net
# Pooled datasource database
pooled.datasource.database=           aug
# Pooled datasource user
pooled.datasource.user=sa
# Pooled datasource password
# For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
pooled.datasource.password={aes}                        ==

# No pooled datasource driver
#no.pooled.datasource.driver=org.postgresql.Driver
# No pooled datasource url
#no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everywan
# No pooled datasource user
#no.pooled.datasource.user=everywan
# No pooled datasource password
#no.pooled.datasource.password=everywan

# Audit datasource driver
audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
# Audit datasource url
audit.datasource.url=jdbc:jtds:sqlserver://ah-234                /          -llaug;instance=
# Audit datasource host name
audit.datasource.hostname=ah-234           .net
# Audit datasource database
audit.datasource.database=          -llaug
# Audit datasource user
audit.datasource.user=sa
# Audit datasource password
```

ew-config.properties

```
# For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
# For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress
# For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress;domain=sparus-s
# Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@//localhost:1521/everywan
pooled.datasource.url=jdbc:jtds:sqlserver://ah-234.                net:                -llaug
# Pooled datasource host name
pooled.datasource.hostname=ah-234.          .net
# Pooled datasource database
pooled.datasource.database=          -llaug
# Pooled datasource user
pooled.datasource.user=sa
# Pooled datasource password
# For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
pooled.datasource.password={aes}                    ==

# No pooled datasource driver
#no.pooled.datasource.driver=org.postgresql.Driver
# No pooled datasource url
#no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everywan
# No pooled datasource user
#no.pooled.datasource.user=everywan
# No pooled datasource password
#no.pooled.datasource.password=everywan

# Audit datasource driver
audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
# Audit datasource url
audit.datasource.url=jdbc:jtds:sqlserver://                -inc.net:                -llaug
# Audit datasource host name
audit.datasource.hostname=ah-234.          .net
# Audit datasource database
audit.datasource.database=          -llaug
# Audit datasource user
audit.datasource.user=sa
# Audit datasource password
```





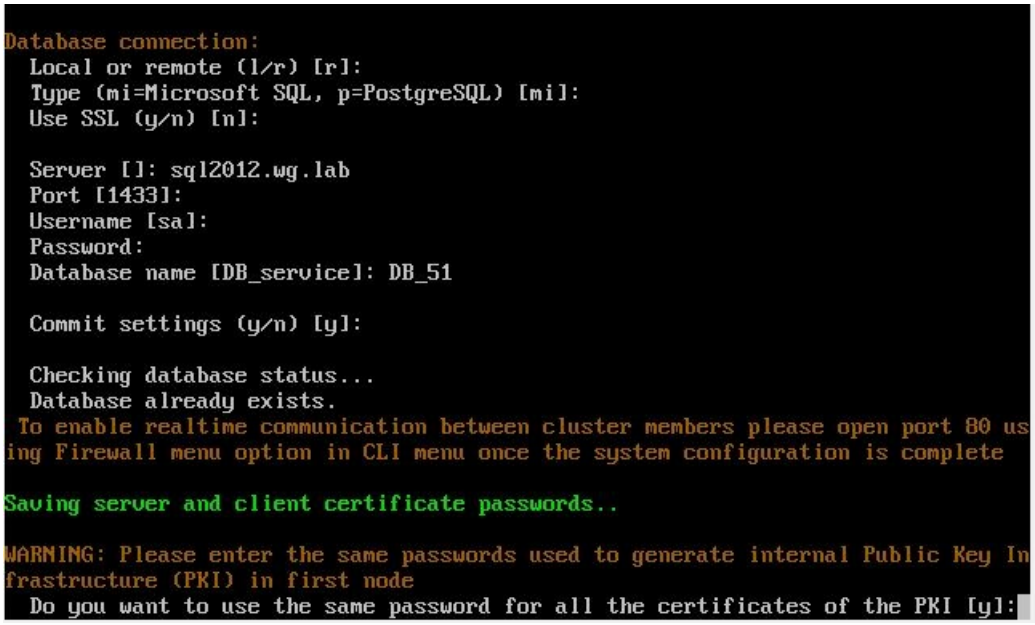
-
-
-
-
-
-

```
Network settings:
  IP address []: 10.147.75.51
  Netmask []: 255.255.255.0
  Default gateway []: 10.147.75.1
  Primary DNS server []: 10.147.75.240
  Secondary DNS server (optional) []:

  Commit settings (y/n) [y]:
Applying network settings...
eth0: intr type 3, mode 0, 3 vectors allocated
eth0: NIC Link is Up 10000 Mbps
```

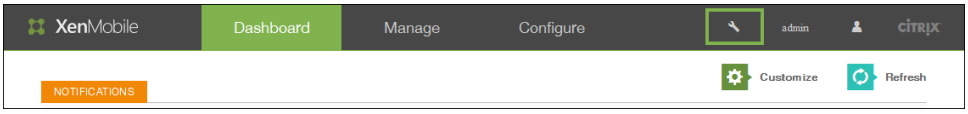
```
Encryption passphrase:
  Generate a random passphrase to secure the server data (y/n) [y]:
```

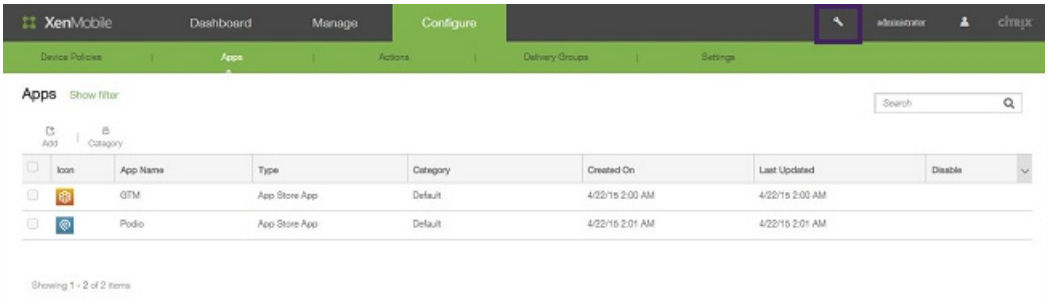
```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```

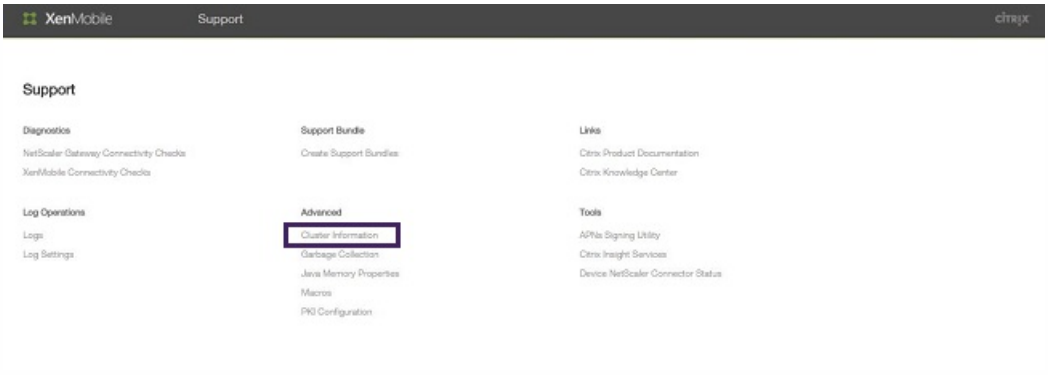
```
Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:

  Server []: sql2012.wg.lab
  Port [1433]:
  Username [sa]:
  Password:
  Database name [DB_service]: DB_51

  Commit settings (y/n) [y]:

  Checking database status...
  Database already exists.
 To enable realtime communication between cluster members please open port 80 us
ing Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..
```

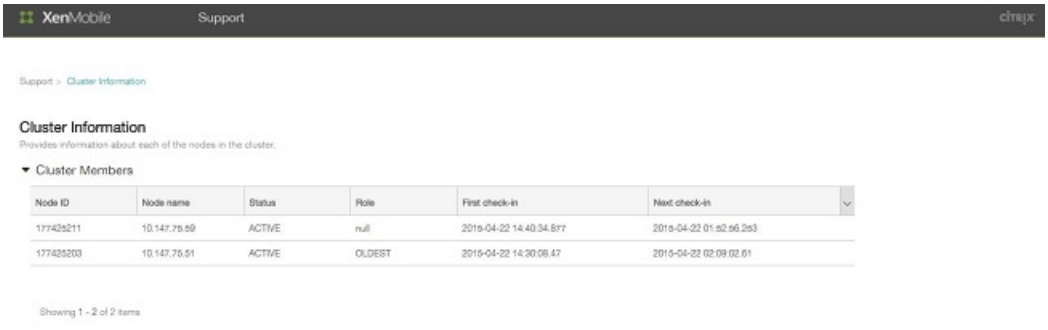


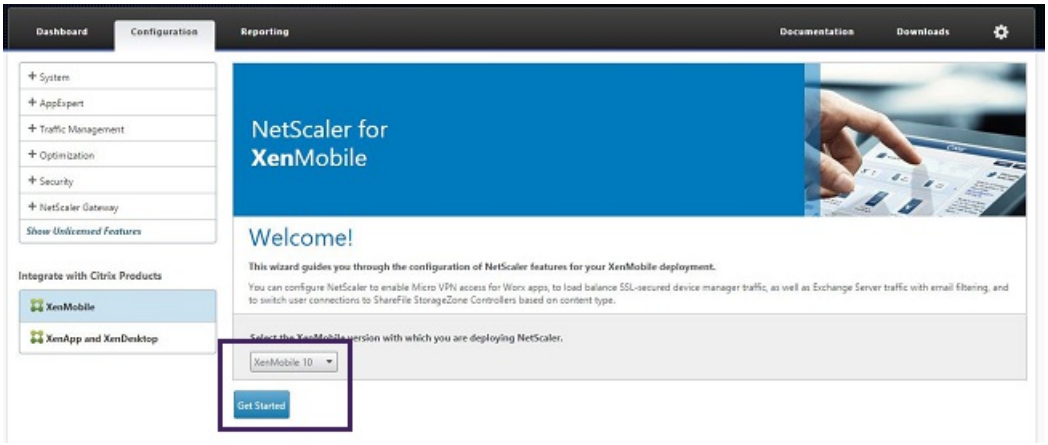
```
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app...                                    [ OK ]
Starting configuration app...
  this may take a few seconds.......
  application started                                            [ OK ]
Stopping main app...                                             [ OK ]
Starting main app...
  this may take a few minutes.....................^[.....................
.................................
  application started                                            [ OK ]

  To access the console, from a web browser, go to the following location and
  log on with your console credentials:
    https://10.147.75.59:4443/

Starting monitoring...                                           [ OK ]

xms51.wg.lab login:
```

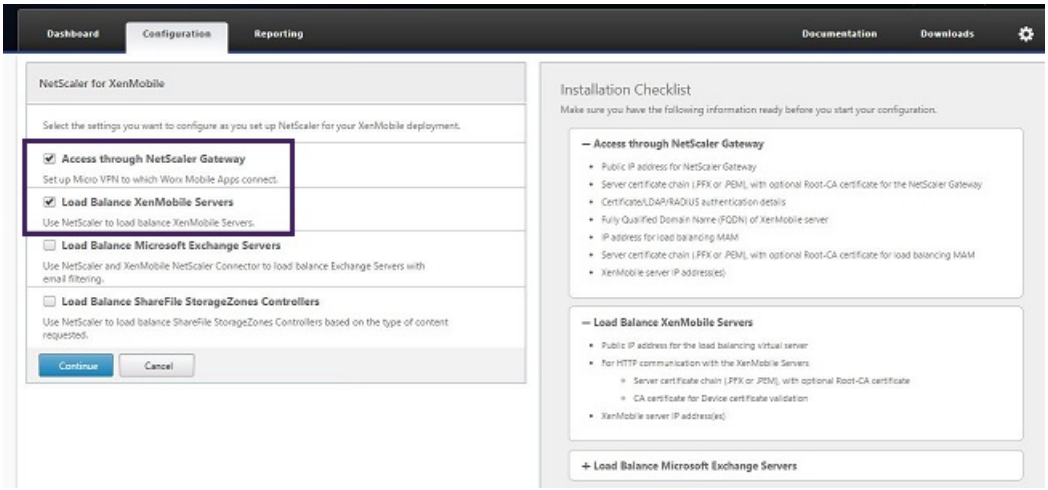


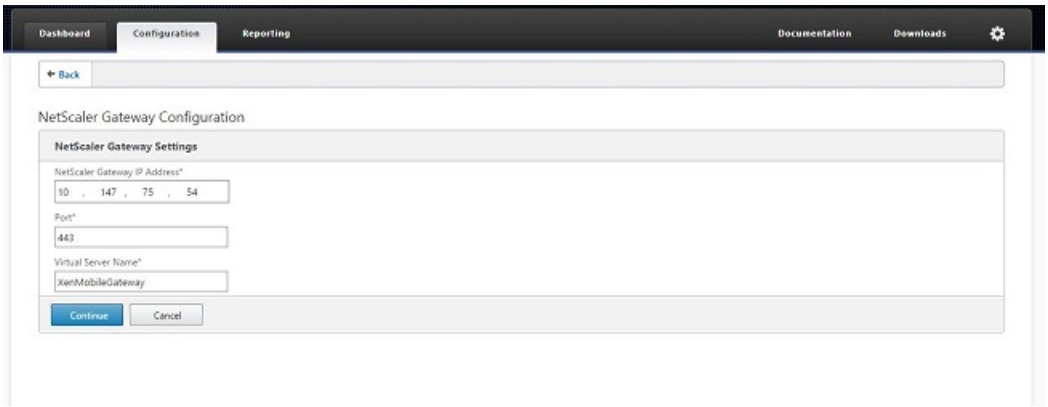




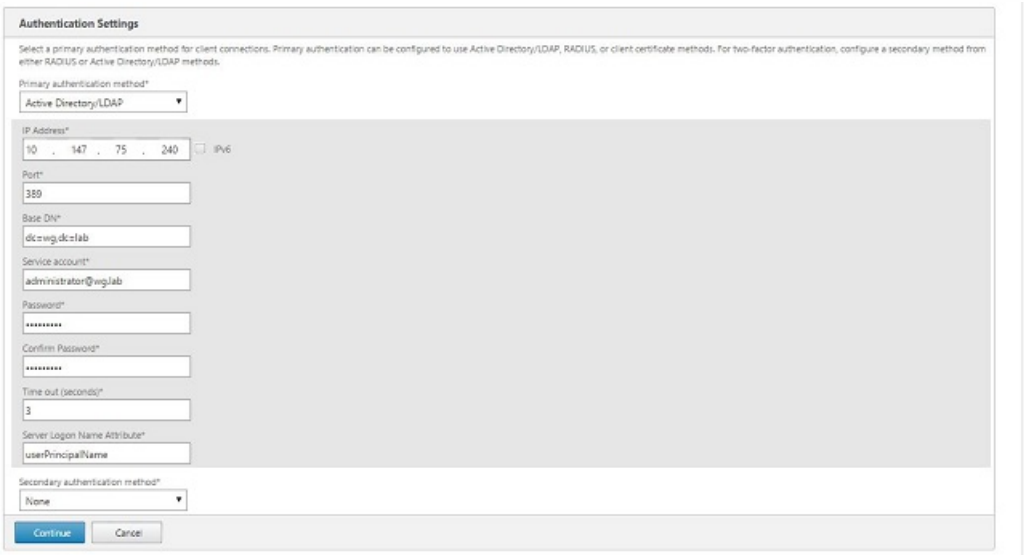


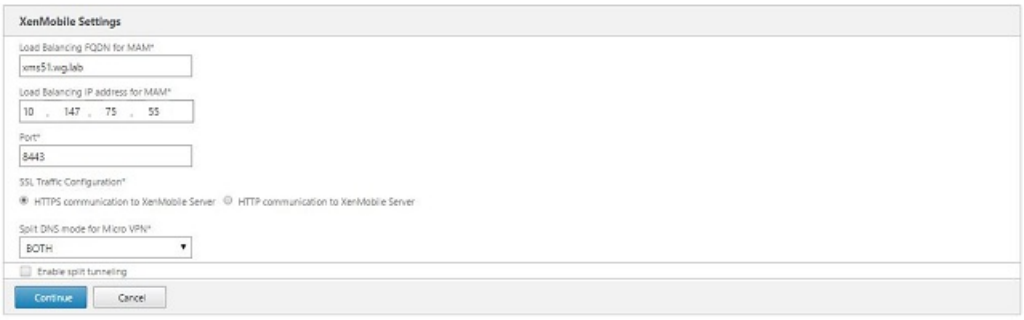


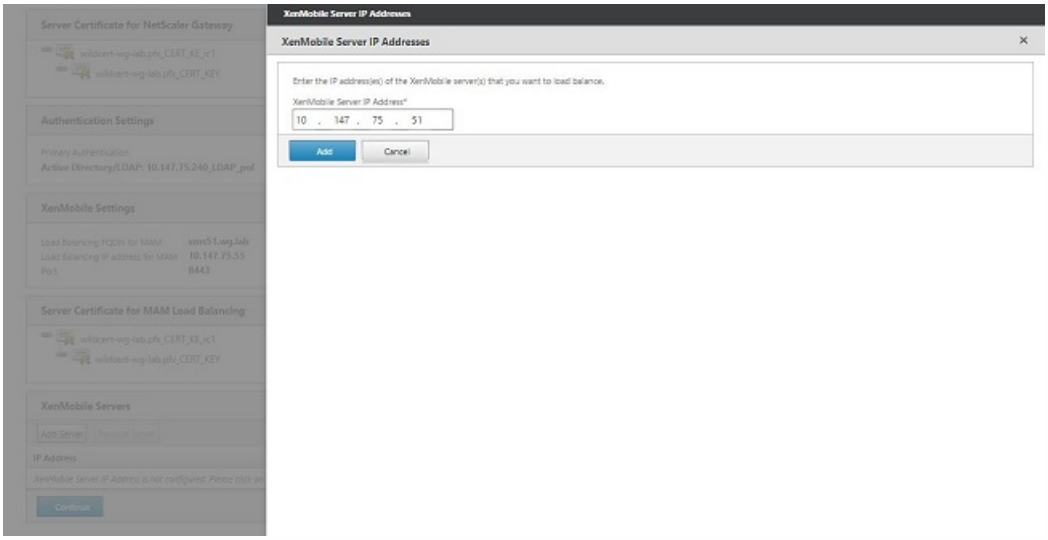


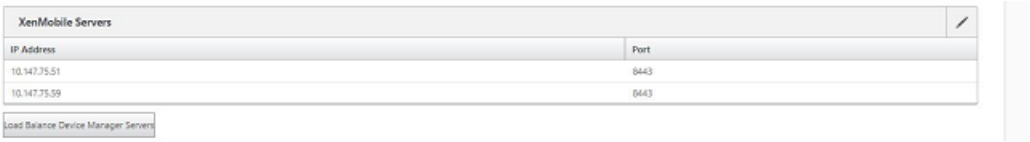


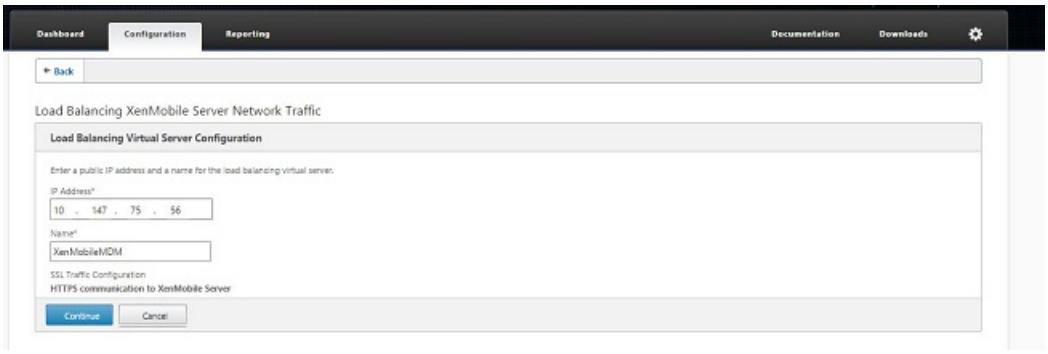
-
-

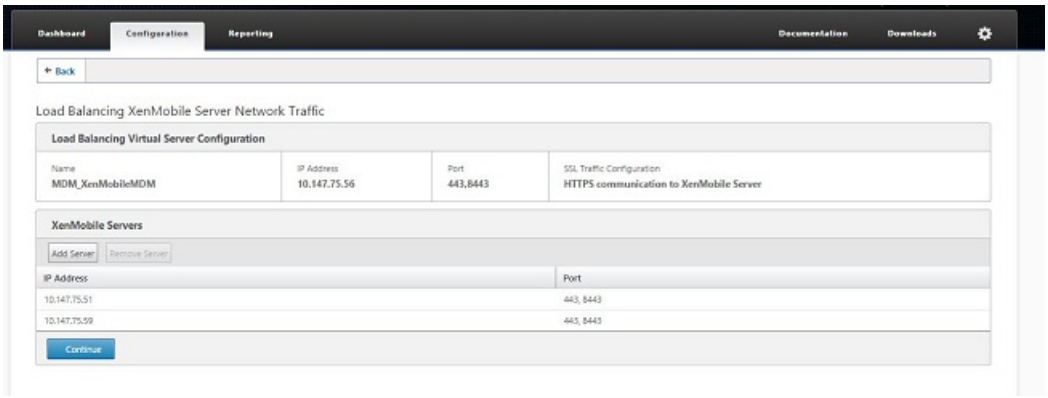


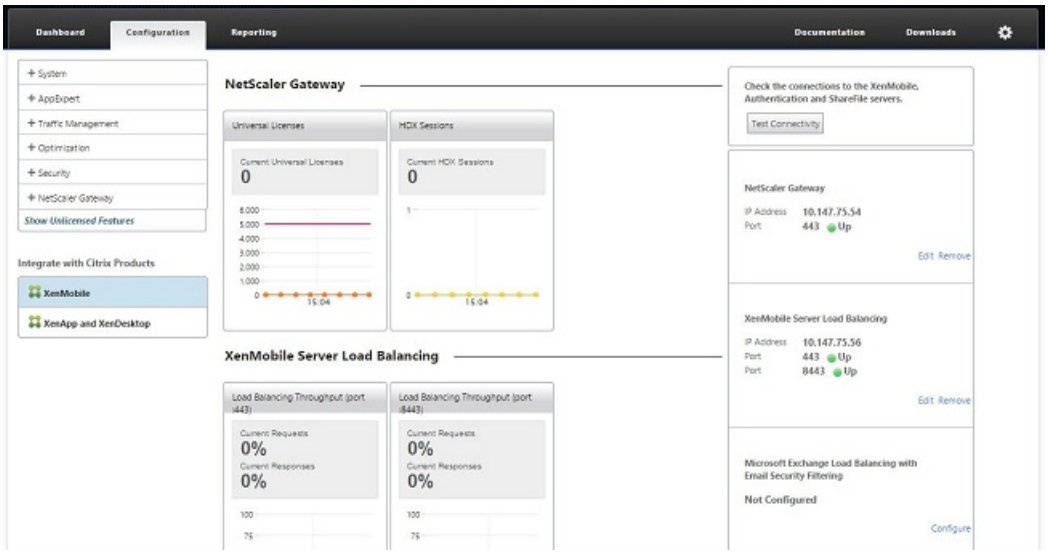


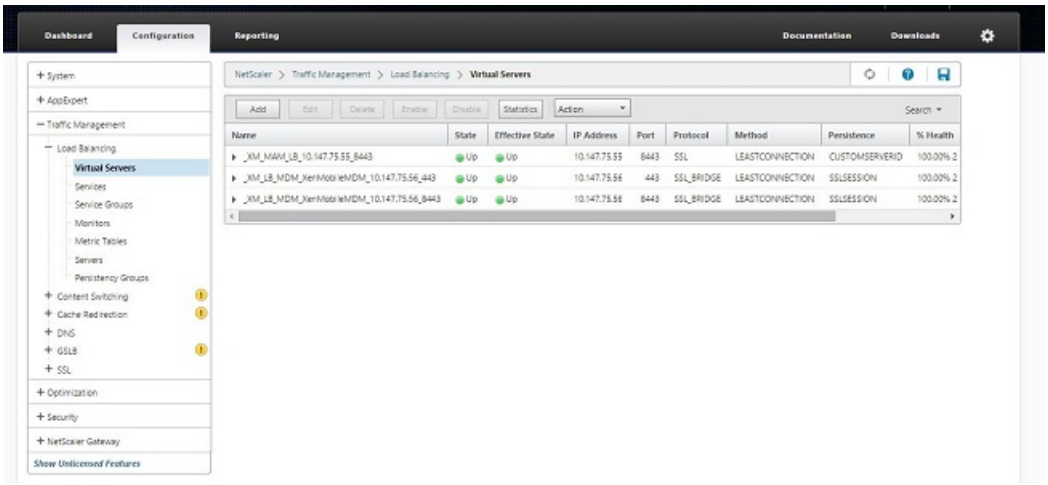


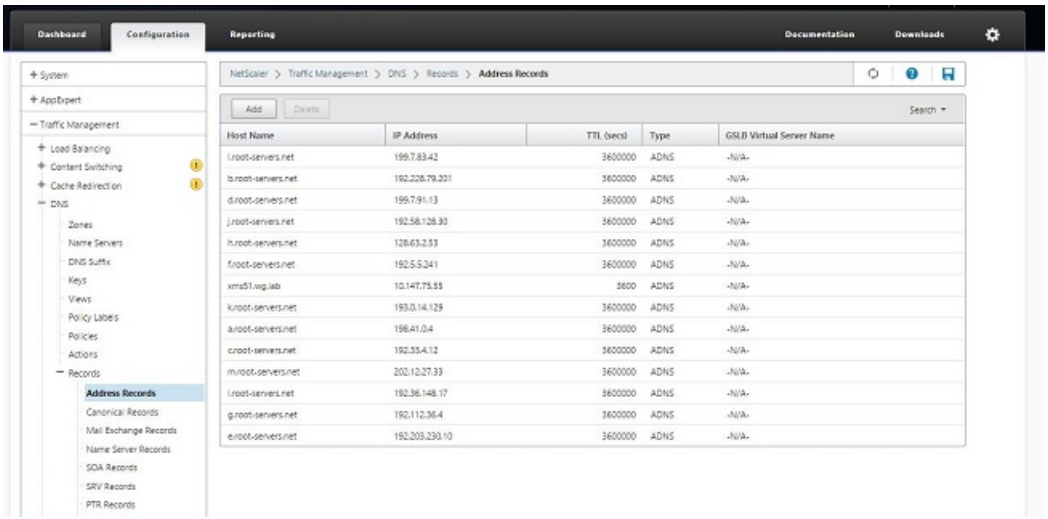


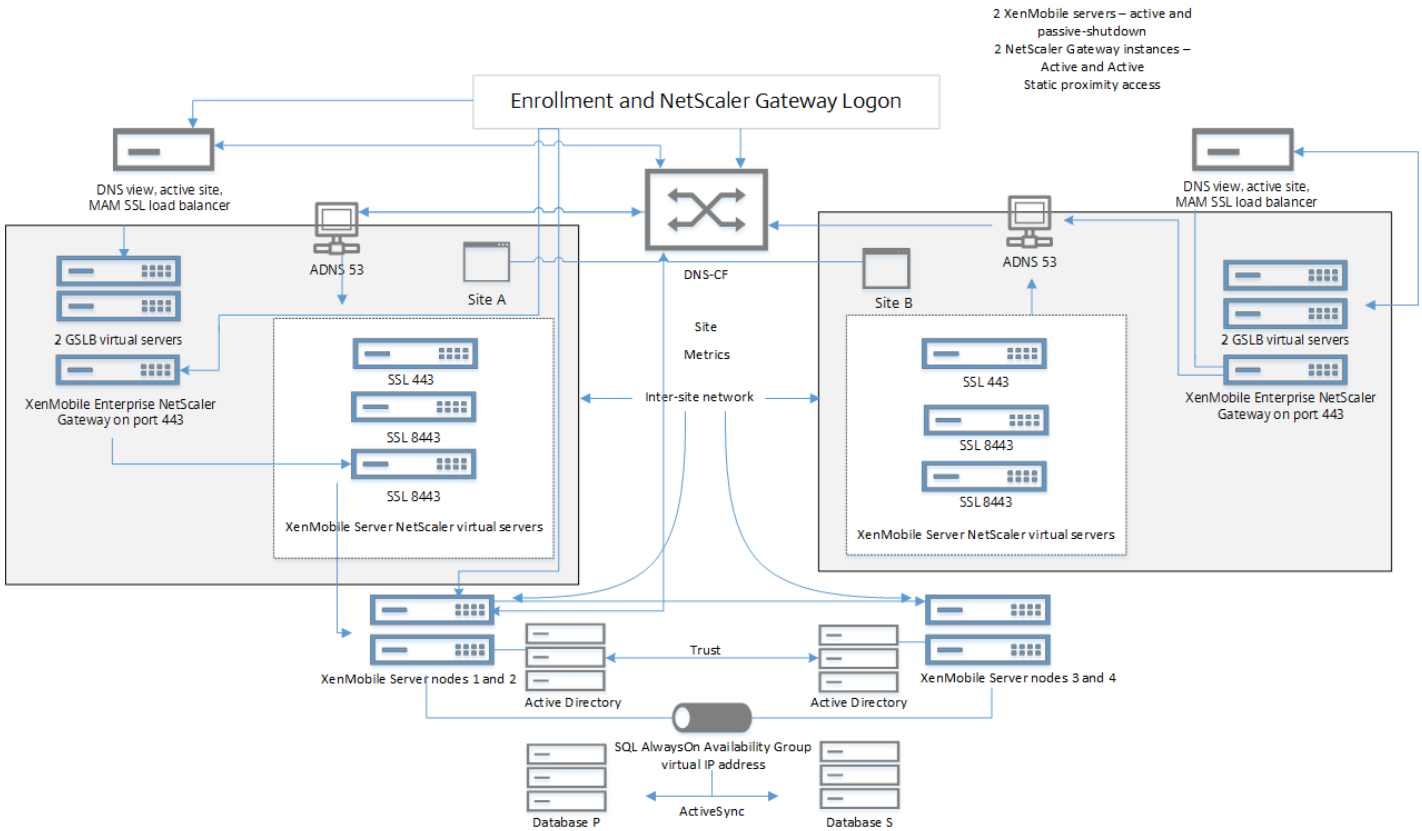


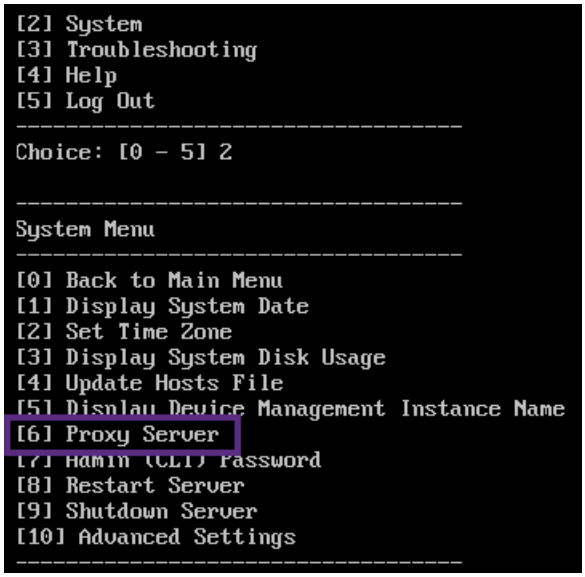


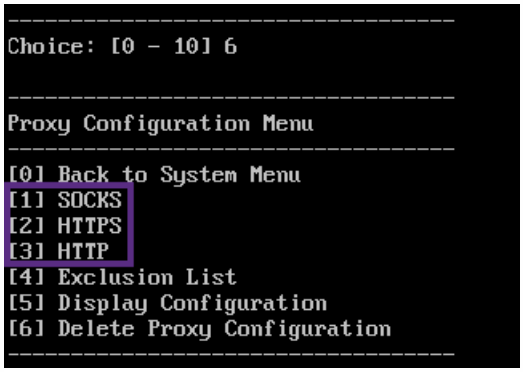


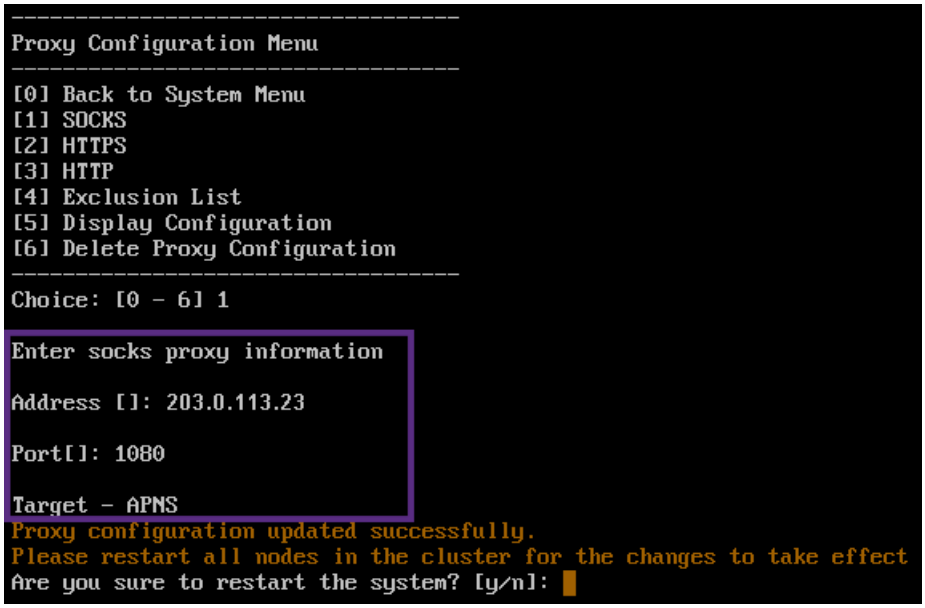


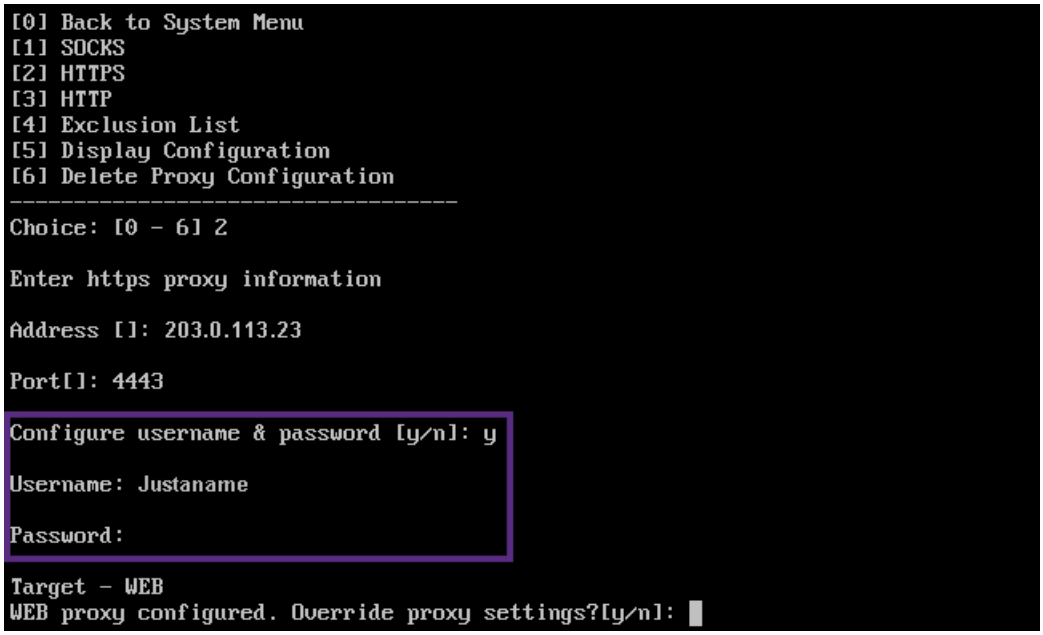


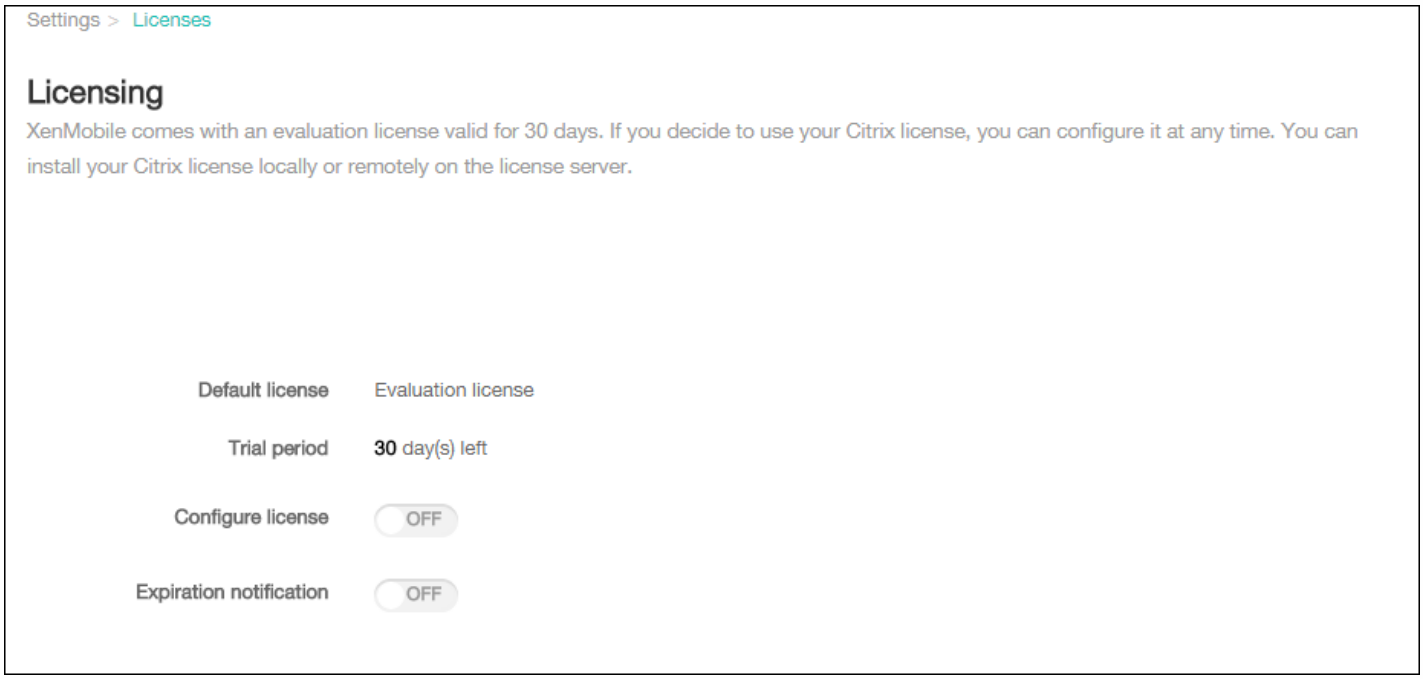


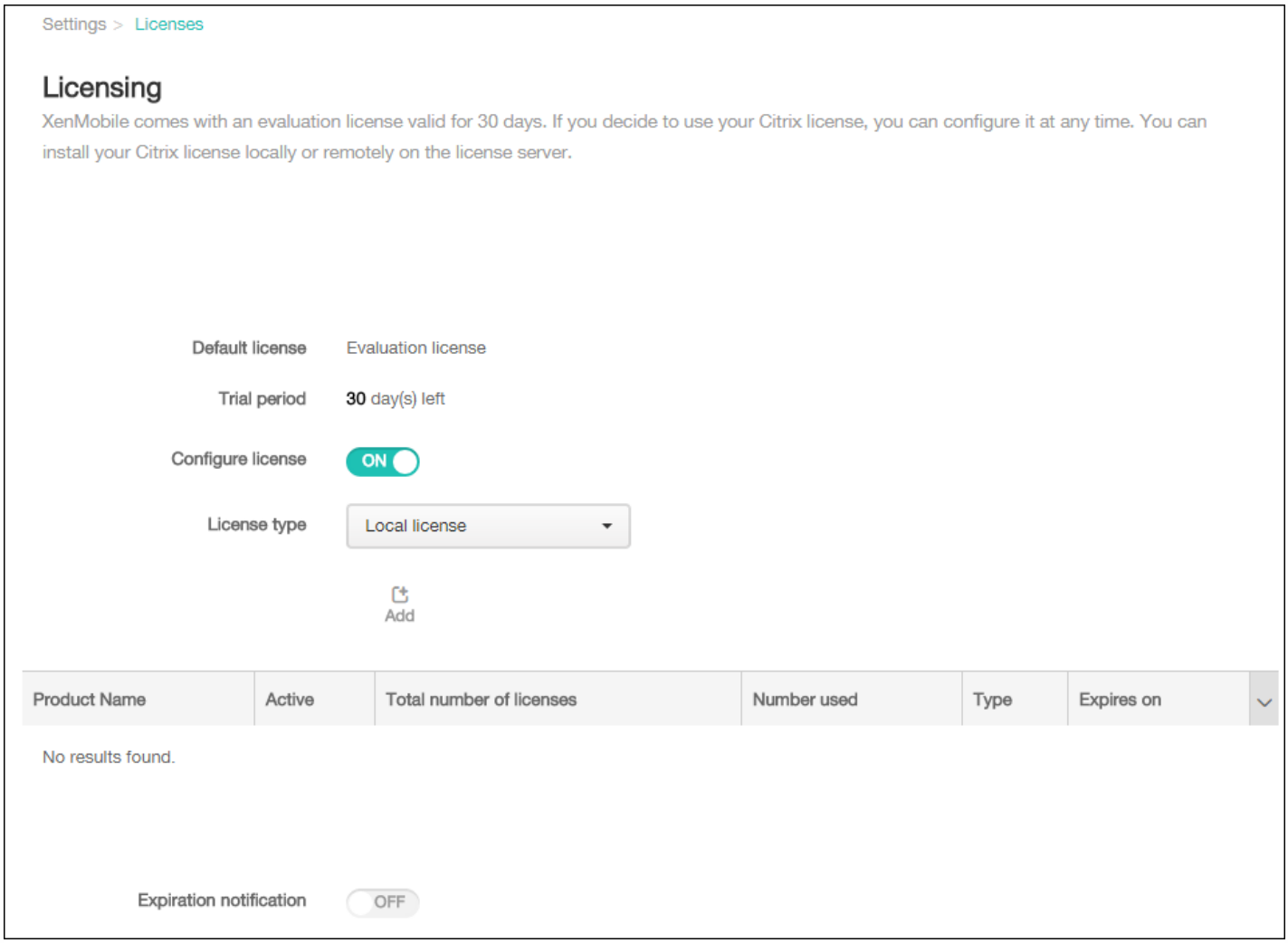


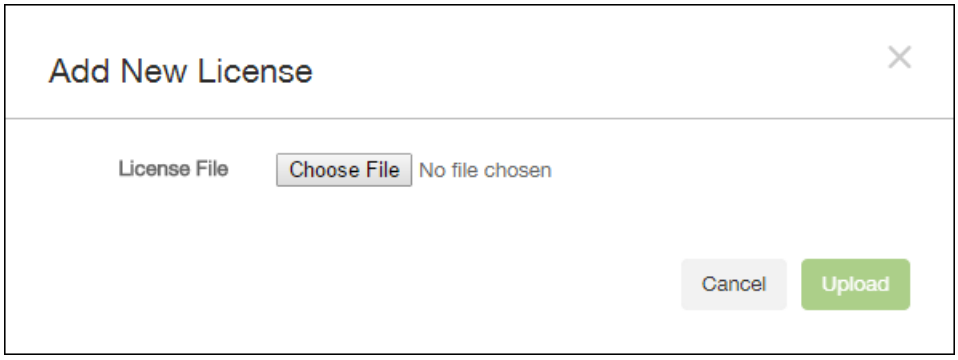


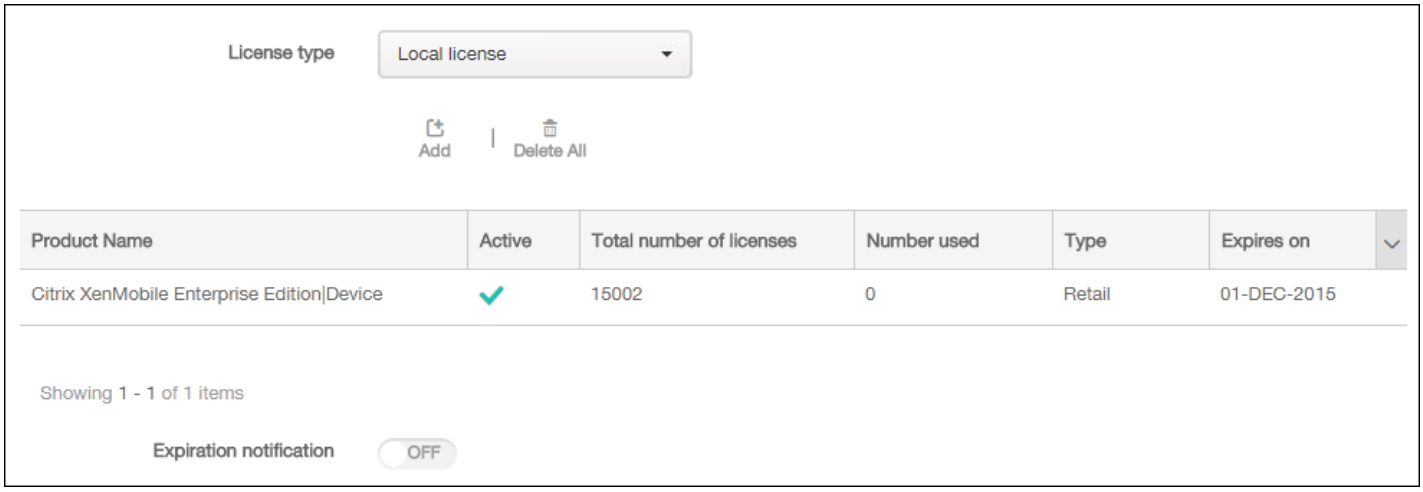


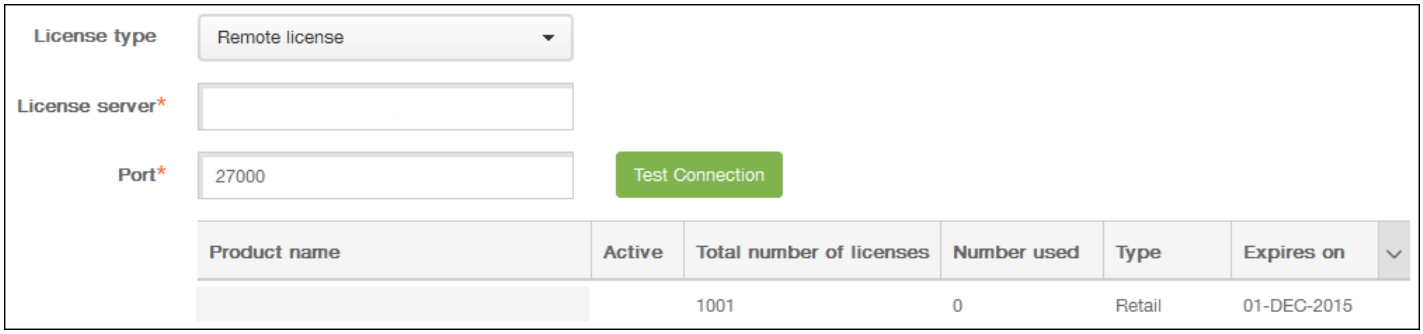






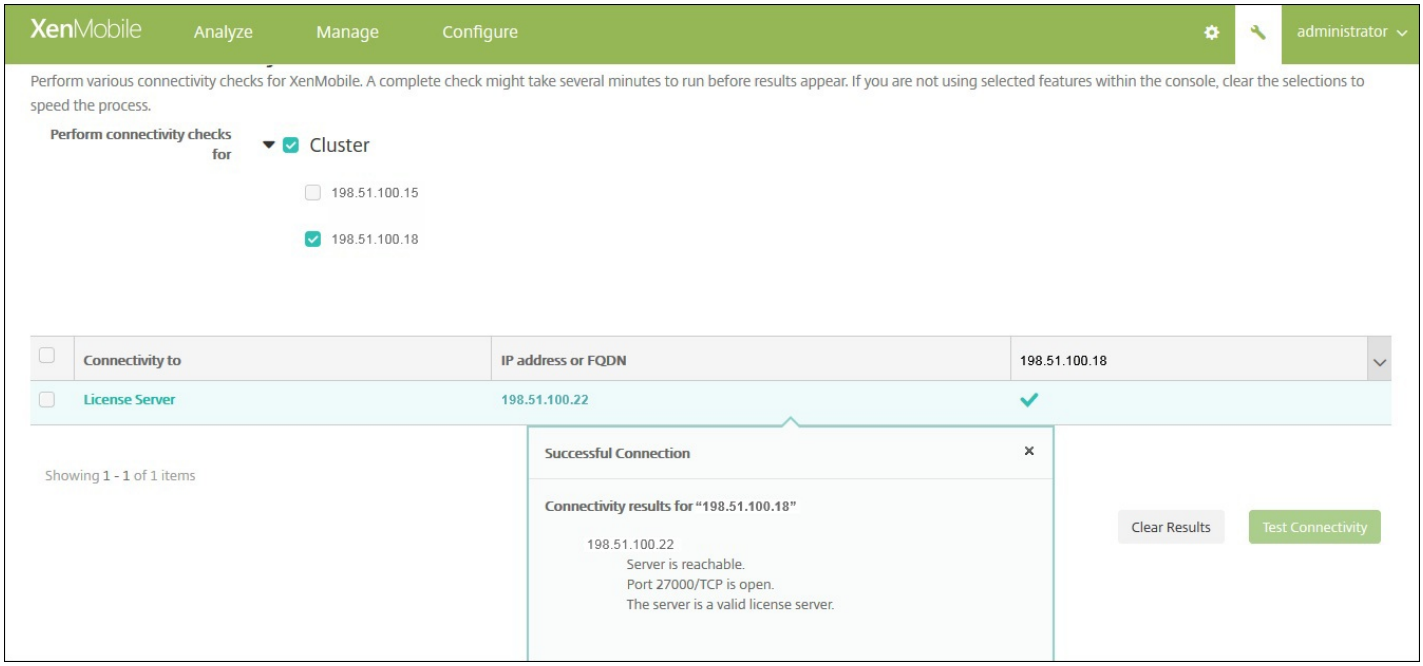


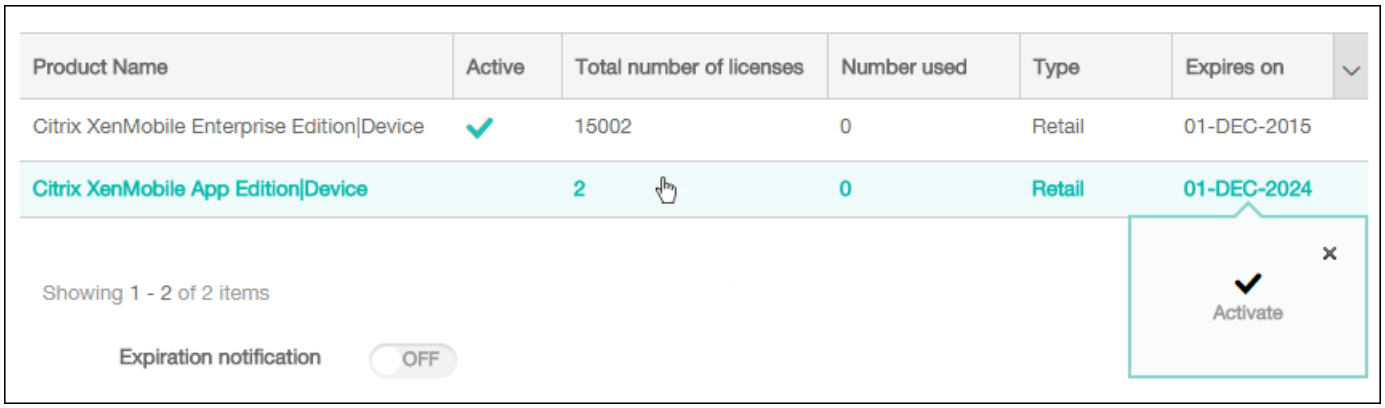


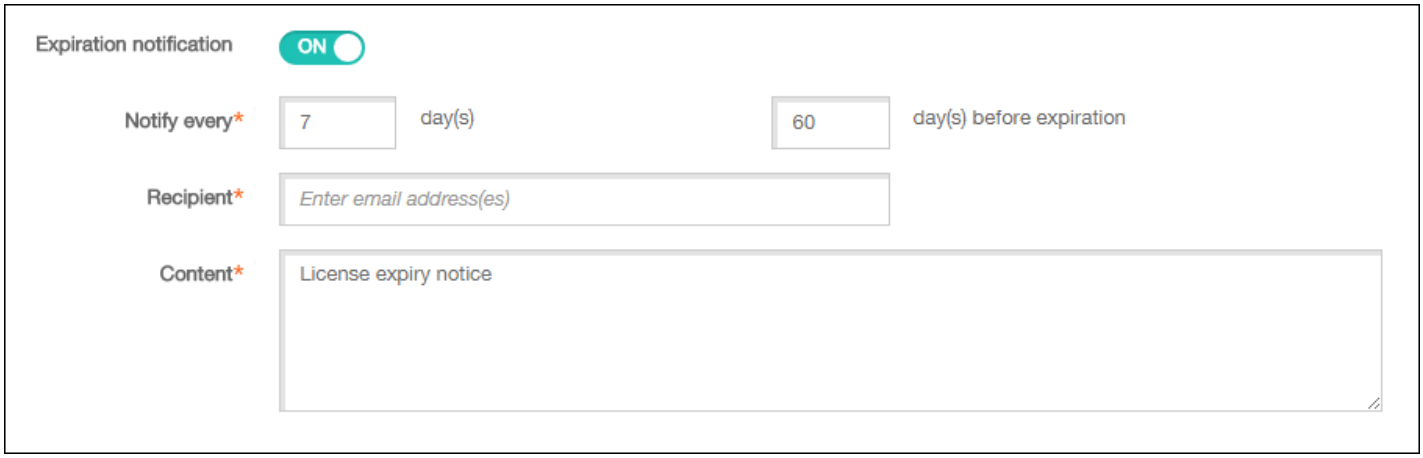


-
-

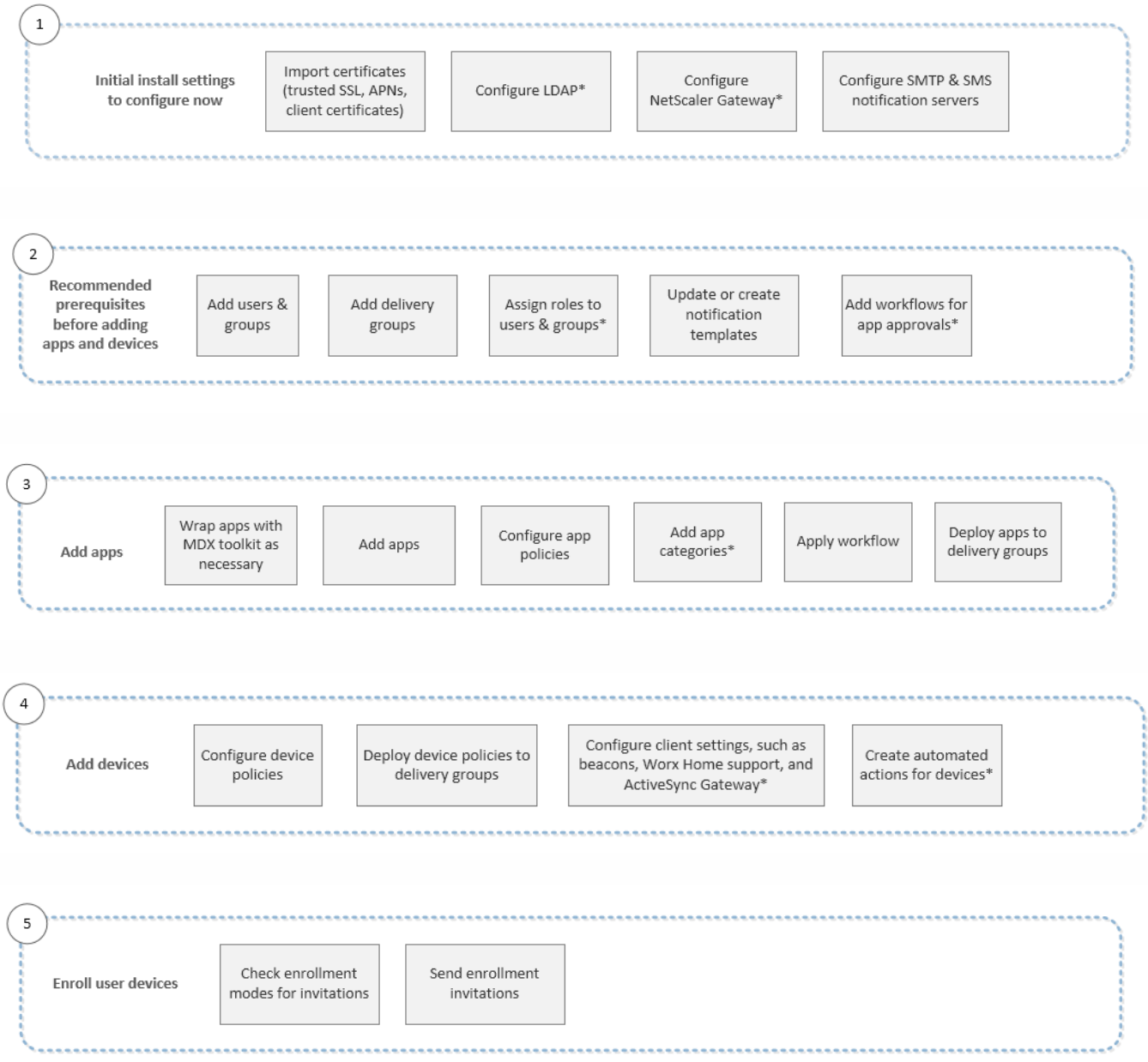
-
-
-

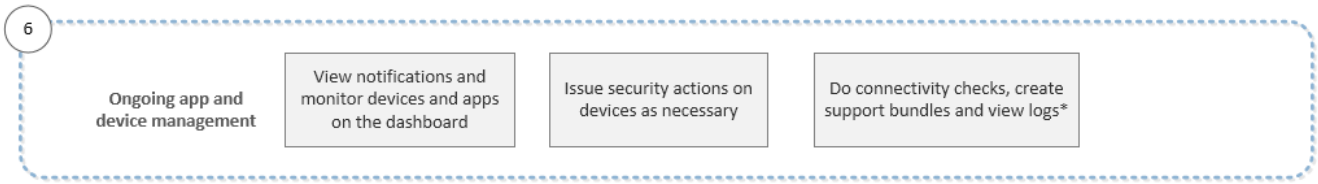


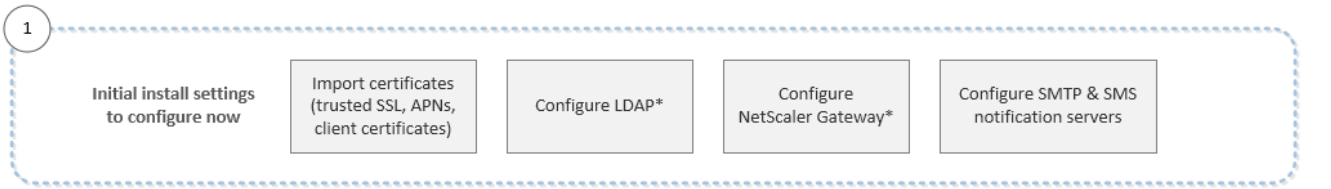




-
  -
  -
-
-

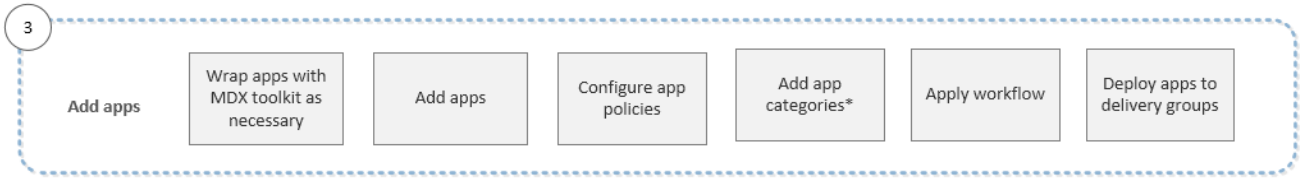




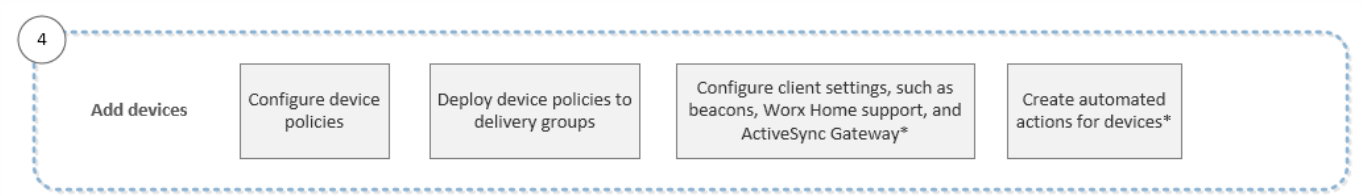


-
-
-
-

-
-
-
-
-
-



-
-
-
-
-
-



-
-
-
-
-

-
-

Workflow de gestion des applications et appareils

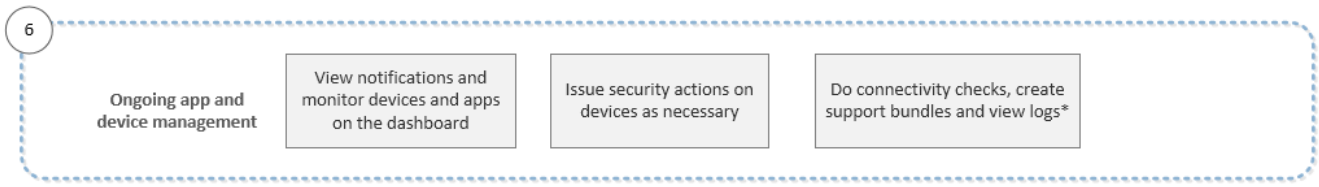
Jul 27, 2016

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. Si vous avez ignoré certaines configurations, vous pouvez afficher les paramètres initiaux recommandés dans Workflow des paramètres initiaux.

Ensuite, vous pouvez configurer certains prérequis avant d'ajouter des applications et des appareils en suivant le Workflow de la configuration requise pour la console. Ensuite, vous pouvez ajouter des applications en suivant les instructions de la section Workflow d'ajout d'applications et ajouter et enregistrer des appareils en suivant les instructions de la section Workflow d'ajout d'appareils. Une fois que vous avez terminé les quatre premiers workflows, inscrivez les appareils utilisateur en suivant les instructions de la section Workflow d'inscription d'appareils utilisateur. Pour afficher l'ensemble du workflow, reportez-vous à la section Prise en main de la console XenMobile.

Ce sixième et dernier workflow affiche les activités de gestion des applications et des appareils recommandées 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, veuillez consulter la section Support et maintenance de XenMobile.

Filtres et tableaux dans la console XenMobile

Jul 27, 2016

Vous pouvez rechercher des filtres et des tableaux dans la console XenMobile. Ils figurent sur les onglets Appareils, Inscription, Stratégies d'appareil, Applications, Actions et Groupes de mises à disposition, ainsi que sur la plupart des pages sous Paramètres. Les filtres vous permettent d'affiner les informations dans toutes ces zones de la console afin de localiser les informations exactes que vous voulez afficher ou pour lesquelles vous souhaitez entreprendre une action. Dans les tableaux, vous pouvez cliquer sur un ou plusieurs éléments afin d'afficher les options que vous pouvez effectuer sur les éléments sélectionnés. Les options peuvent changer en fonction du nombre d'éléments que vous sélectionnez.
Le tableau suivant répertorie les options les plus courantes ainsi que leur emplacement.

Option de menu	Action	Tableau où l'option apparaît
Ajouter	Ajouter un nouvel élément au tableau.	Tous
Catégorie	Ajouter et gérer des catégories pour les applications.	Applications
Copier l'URL	Copier l'URL dans le Presse-papiers.	Inscription
Supprimer ou Tout supprimer	Supprimer définitivement les éléments sélectionnés.	Tous
Déployer	Déployer des ressources auprès d'utilisateurs et d'appareils.	Appareils et groupes de mise à disposition
Désactiver	Désactiver une application ou le groupe de mise à disposition AllUsers.	Applications et groupes de mise à disposition
Modifier	Apporter des modifications à un élément existant.	Tous, sauf Inscription
Exporter	Envoyer le contenu du tableau dans un fichier .csv.	Tous
Importer	Ajouter des appareils à partir d'un fichier de provisioning.	Appareils
	Ajouter des utilisateurs et des groupes locaux à partir d'un fichier.	Utilisateurs et groupes locaux
Gérer les groupes locaux	Ajouter un groupe local pour la gestion.	Utilisateurs et groupes locaux
Notifier	Envoyer une notification aux utilisateurs et appareils sélectionnés.	Inscription et appareils
Actualiser	Mettre à jour le tableau.	Appareils

Option de menu	Action	Tableau où l'option apparaît
Supprimer	Appliquer des actions sur l'appareil sélectionné.	Appareils
Portail en libre-service	Activer le portail libre-service en tant que mode d'inscription.	Inscription
Mettre à jour	Mettre à jour les valeurs dans un tableau.	Gestion des versions

Pour afficher les options dans les tableaux de la console XenMobile

Pour réaliser des actions sur les informations présentes dans les tableaux de la console, vous pouvez afficher les différentes options de plusieurs manières différentes :

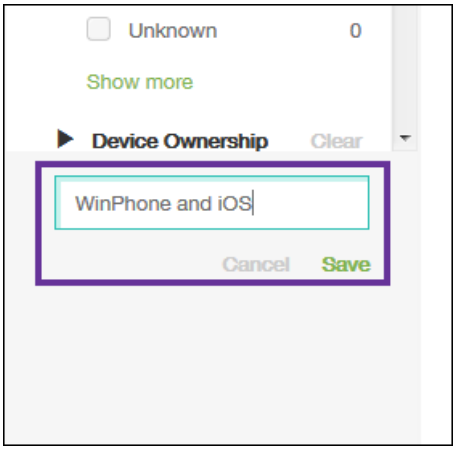
- Vous pouvez sélectionner la case à cocher en regard d'un élément pour afficher le menu d'options au-dessus de la liste.
- Vous pouvez sélectionner la case à cocher en regard de plusieurs éléments pour exécuter une action sur tous ces éléments simultanément. Les actions que vous pouvez exécuter sur plusieurs éléments dépendent du tableau que vous consultez.
- Vous pouvez cliquer sur un élément dans la liste pour afficher le menu d'options sur le côté droit de la liste. Lorsque vous cliquez sur Afficher plus, des détails sur cet élément s'afficheront. Ce que vous voyez dépend du tableau que vous consultez.
- Vous pouvez entrer un nom complet ou partiel dans la zone Rechercher pour limiter le nombre d'éléments répertoriés.

Seuls 10 éléments sont affichés par page dans la zone Stratégies d'appareil de la console. Cliquez sur les triangles dans la partie inférieure droite de la page pour vous déplacer d'une page à l'autre.

Pour filtrer les informations dans la console XenMobile

Lorsque vous voulez afficher un sous-ensemble spécifique d'informations dans une zone de la console, tel que Appareils, Inscription, Stratégies d'appareil, Applications, Actions, Groupes de mise à disposition et Groupes et utilisateurs locaux, vous pouvez filtrer la liste en fonction de critères que vous sélectionnez. Cette procédure utilise la page Appareils comme exemple, mais les étapes permettant de filtrer les résultats sont identiques dans toute la console.

1. Sur la page Appareils, cliquez sur Afficher le filtre.
   Le panneau de filtre apparaît et répertorie les critères que vous pouvez appliquer pour filtrer la liste Appareils. Lorsque vous affichez le filtre pour la première fois, tous les critères sont réduits.
2. Cliquez sur le triangle à gauche d'un filtre pour afficher les critères disponibles pour ce filtre. Les chiffres à droite de chaque critère représentent le nombre d'appareils qui remplissent ce critère.
3. Sélectionnez le critère de filtration à utiliser. La liste Appareils est limitée aux appareils qui répondent aux critères sélectionnés.
4. Procédez comme suit :
   - Cliquez sur Masquer le filtre pour continuer à travailler avec la liste filtrée.
   - Cliquez sur Tout effacer pour revenir à la liste complète.
   - Cliquez sur Effacer en regard d'un critère spécifique pour supprimer ce filtre et supprimer ces éléments dans la liste filtrée.
5. Si vous voulez enregistrer les critères sélectionnés en tant que filtre personnalisé, dans le champ Enregistrer le filtre en bas du panneau Filtrer, tapez un nom descriptif et cliquez sur Enregistrer. Si vous décidez de ne pas enregistrer le filtre, cliquez sur Annuler.



6. Après avoir enregistré le filtre, vous pouvez le sélectionner en bas du panneau Filtre pour filtrer les informations dans le tableau.
   Remarque : si vous cliquez sur le triangle à droite du nom de filtre, vous pouvez renommer ou supprimer le filtre.

Rapports dans XenMobile

Jul 27, 2016

XenMobile propose 10 rapports prédéfinis qui vous permettent d'analyser les déploiements d'applications et d'appareils :

- **Applications par appareils et utilisateur** : répertorie les applications que les utilisateurs ont sur leur appareil.
- **Termes et conditions** : répertorie les utilisateurs qui ont accepté et refusé les conditions générales.
- **Top 25 des applications** : répertorie jusqu'à 25 applications que la plupart des utilisateurs ont sur leurs appareils.
- **Appareils jailbreakés/rootés** : répertorie les appareils iOS rootés et les appareils Android jailbreakés.
- **Top 10 des applications - échec du déploiement** : répertorie les applications dont le déploiement a échoué.
- **Appareils inactifs** : répertorie les appareils qui sont inactifs depuis une période de temps spécifiée.
- **Application par type et catégorie** : répertorie les applications par version, type et catégorie.
- **Inscription d'appareils** : répertorie les appareils inscrits pendant une période spécifiée.
- **Applications par plate-forme** : répertorie les applications et les versions de l'application par plate-forme et version de l'appareil.
- **Appareils et applications** : répertorie tous les appareils, toutes les données de l'appareil et toutes les applications installées.

Les rapports sont au format .csv, que vous pouvez ouvrir avec des programmes tels que Microsoft Excel. Le tableau suivant dresse la liste des en-têtes et des rapports dans lesquels ils sont utilisés.

En-tête	Description	Rapport
ACCEPTANCE_STATUS	État d'acceptation des termes et conditions	Termes et conditions
APP_CATEGORY	Catégorie sous laquelle l'application est affichée sur les appareils (par exemple, magasin d'applications public ou applications d'entreprise)	Top 10 des applications - échec du déploiement, Application par type et catégorie, Appareils et applications
APP_ID	Identifiant d'application unique	Appareils et applications
APP_NAME	Nom app	Top 25 des applications, top 10 des applications - échec du déploiement, Application par type et catégorie, Appareils et applications
APP_OWNER	Propriétaire de l'application (par exemple, Citrix.com pour les applications Worx)	Top 25 des applications, top 10 des applications - échec du déploiement, Application par type et catégorie, Applications par plate-forme, Appareils et

		applications
APP_TYPE	Type d'application (par exemple, magasin d'applications public ou d'entreprise)	Top 25 des applications, top 10 des applications - échec du déploiement, Application par type et catégorie, Appareils et applications
APP_VERSION	Version de l'application	Top 25 des applications, top 10 des applications - échec du déploiement, Application par type et catégorie, Applications par plate-forme, Appareils et applications
APPS_ON_DEVICE	Nombre d'applications installées sur l'appareil	Applications par appareils et utilisateur
CERTIFICATE_EXPIRATION	Date d'expiration du certificat	Appareils et applications
CREATION_DATE	Date de création du fichier des termes et conditions	Termes et conditions
DELIVERY_GROUP	Groupe de mise à disposition associé avec la ressource déployée	Termes et conditions
DEPLOYMENT_DATE	Date de déploiement de la ressource	Top 25 des applications, top 10 des applications - échec du déploiement, Application par type et catégorie, Appareils et applications
DEPLOYMENT_SUCCESS, DEPLOYMENT_FAILED, DEPLOYMENT_PENDING	État du déploiement	Applications par appareils et utilisateur, top 25 des applications, top 10 des applications - échec du déploiement, Application par type et catégorie, Applications par plate-forme, Appareils et applications
DEPLOYMENT_TOTAL	Nombre total de tentatives de déploiement	Top 25 des applications, top 10 des applications - échec du

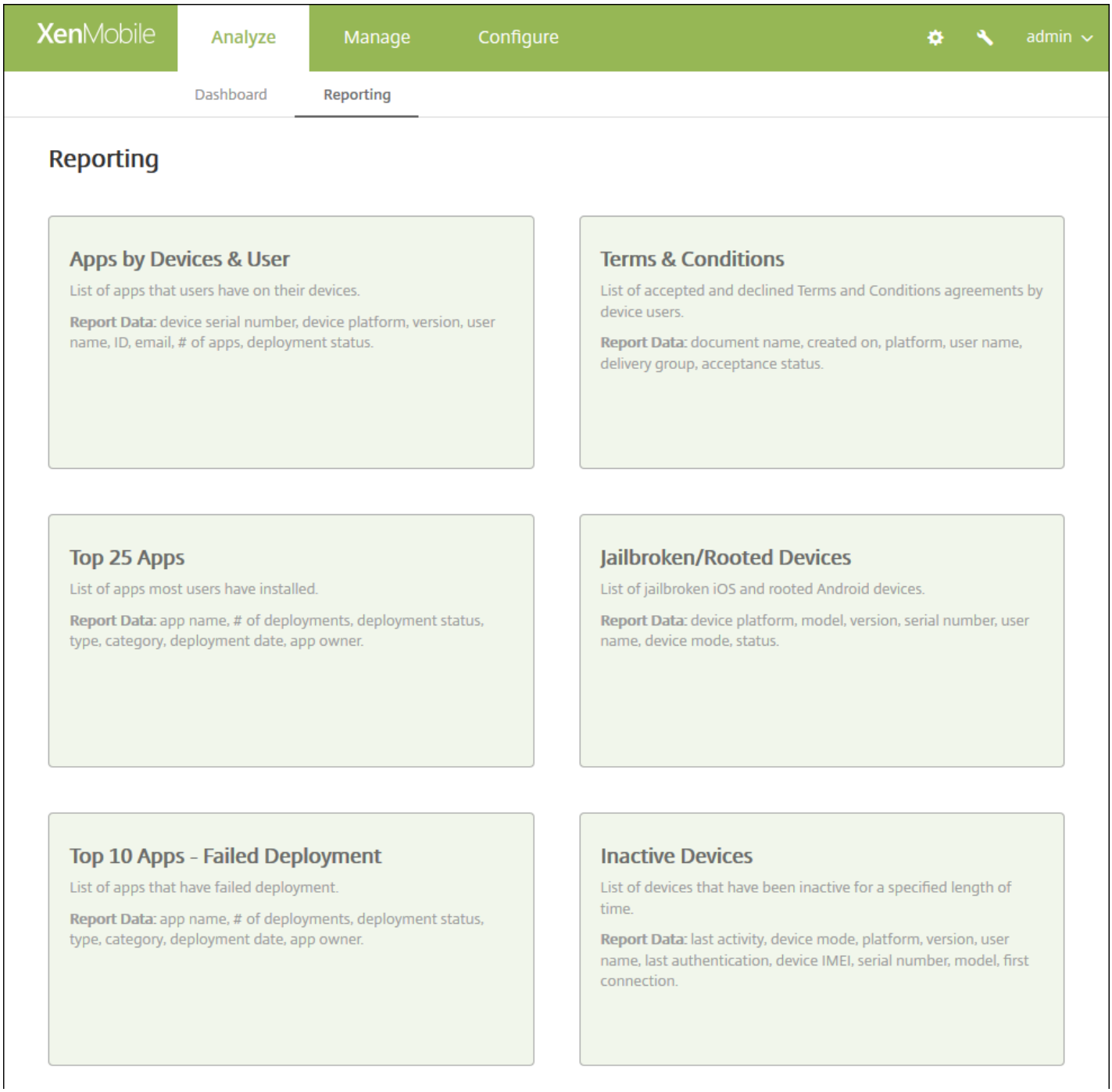
		déploiement, Application par type et catégorie, Applications par plate-forme, Appareils et applications
DEVICE_MODE	Mode d'appareil (appareils gérés ou non gérés)	Appareils jailbreakés/rootés, Appareils inactifs, Inscription d'appareils, Appareils et applications, Appareils et applications
DEVICE_OWNERSHIP	Catégorisation du propriétaire de l'appareil (BYOD, Entreprise ou inconnu)	Appareils et applications
DEVICE_PLATFORM	La plate-forme de l'appareil	Applications par plate-forme
DEVICE_STATUS	État de la conformité de l'appareil	Appareils et applications
DEVICE_VERSION	Numéro de version du système d'exploitation de l'appareil	Applications par plate-forme
DOCUMENT_NAME	Nom du fichier Termes et conditions	Termes et conditions
EMAIL	Adresse e-mail de l'utilisateur	Appareils et applications
ENROLLMENT_DATE	Date d'inscription de l'appareil dans XenMobile	Appareils et applications
ENROLLMENT_STATUS	État de l'inscription de l'appareil (inscrit ou non inscrit)	Appareils et applications
FIRST_CONNECTION_DATE	Date à laquelle l'appareil s'est connecté à XenMobile pour la première fois	Appareils inactifs, Inscription d'appareils
IMEI	Numéro IMEI (identité internationale d'équipement mobile) de l'appareil	Appareils inactifs
LAST_ACTIVITY	Date de dernière activité de l'appareil	Appareils inactifs
LAST_AUTH_DATE	Dernière date à laquelle l'appareil s'est authentifié auprès de XenMobile	Appareils inactifs, Inscription d'appareils, Appareils et

		applications
LAST_USERNAME	Dernier nom associé à l'appareil	Appareils jailbreakés/rootés, Appareils inactifs, Inscription d'appareils
LOCATION	Emplacement géographique de l'appareil	Appareils et applications
MANAGED	Indique si l'appareil est géré ou non géré	Appareils jailbreakés/rootés
MODEL	Modèle d'appareil	Appareils jailbreakés/rootés, Appareils inactifs, Inscription d'appareils, Appareils par plate-forme
MODEL_NAME	Modèle d'appareil	Appareils et applications
OS_VERSION	Version du système d'exploitation sur l'appareil	Applications par appareils et utilisateur, Appareils inactifs, Inscription d'appareils, Appareils et applications;
PHONE_NUMBER	Numéro de téléphone de l'utilisateur	Inscription d'appareils
PLATFORM	La plate-forme de l'appareil	Applications par appareils et utilisateur, Termes et conditions, Appareils jailbreakés/rootés, Appareils inactifs, Inscription d'appareils, Appareils et applications;
SERIAL_NUMBER	N° série appareil	Applications par appareils et utilisateur Appareils jailbreakés/rootés, Appareils inactifs, Appareils et applications
USER E-MAIL	Adresse e-mail de l'utilisateur	Applications par appareils et utilisateur
USER_ID	Numéro unique de l'utilisateur	Appareils et applications

USER_NAME	Nom d'utilisateur	Applications par appareils et utilisateur, Termes et conditions, Appareils et applications
USERID	Utilisateur ID	Applications par appareils et utilisateur

Suivez les instructions ci-dessous pour créer un rapport :

1. Dans la console XenMobile, cliquez sur l'onglet **Analyser**, puis cliquez sur **Rapports**. La page **Rapports** s'affiche.



Apps by Type & Category

List of apps and app versions by app type (MDX, Public, Web & SaaS, Enterprise, Web Link) and defined categories.

Report Data: app name, version, # of deployments, deployment status, type, category, deployment date, app owner.

Device Enrollment

List of devices that have been enrolled during a specified length of time.

Report Data: first connection, device mode, platform, version, model, user name, last authentication, phone number.

Apps by Platform

List of apps and app versions installed on various device platforms and device versions.

Report Data: app name, version, # of deployments, deployment status, deployment date, app owner, device platform, version, model, model name.

Devices & Apps

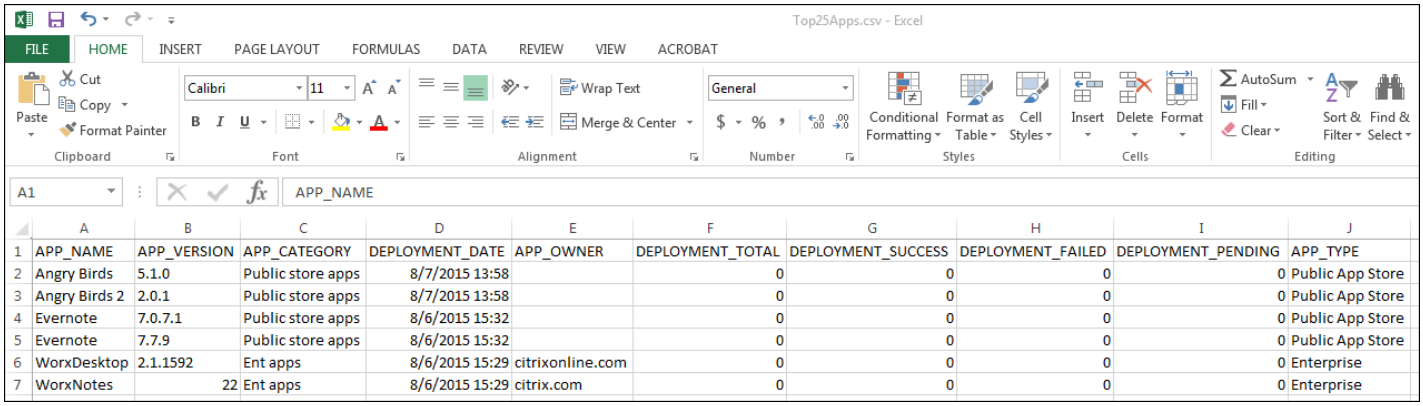
List of all devices, device data, and apps installed.

Report Data: device serial number, user name, ID, email, device platform, version, model, mode, status, last connection, enrollment status, enrollment date, device ownership, location, certificate expiration, app name, version, deployment status, type, category, deployment date, app owner, app ID.

2. Cliquez sur le rapport que vous souhaitez créer. En fonction du navigateur que vous utilisez, le fichier est automatiquement téléchargé ou vous êtes invité à enregistrer le fichier.

3. Répétez l'étape 2 pour chaque rapport que vous souhaitez créer.

Vous trouverez ci-dessous un exemple de rapport « Top 25 des applications » ouvert dans Microsoft Excel :



	A	B	C	D	E	F	G	H	I	J
1	APP_NAME	APP_VERSION	APP_CATEGORY	DEPLOYMENT_DATE	APP_OWNER	DEPLOYMENT_TOTAL	DEPLOYMENT_SUCCESS	DEPLOYMENT_FAILED	DEPLOYMENT_PENDING	APP_TYPE
2	Angry Birds	5.1.0	Public store apps	8/7/2015 13:58		0	0	0	0	Public App Store
3	Angry Birds 2	2.0.1	Public store apps	8/7/2015 13:58		0	0	0	0	Public App Store
4	Evernote	7.0.7.1	Public store apps	8/6/2015 15:32		0	0	0	0	Public App Store
5	Evernote	7.7.9	Public store apps	8/6/2015 15:32		0	0	0	0	Public App Store
6	WorxDesktop	2.1.1592	Ent apps	8/6/2015 15:29	citrixonline.com	0	0	0	0	Enterprise
7	WorxNotes	22	Ent apps	8/6/2015 15:29	citrix.com	0	0	0	0	Enterprise

Notifications

Jul 27, 2016

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 lorsque l'accès au domaine d'entreprise est sur le point d'être bloqué en raison d'un problème de conformité, ou lorsqu'un appareil est 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 Webou de systèmes de communication mobiles. Il 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.

Les procédures décrites dans cet article expliquent comment configurer un serveur SMTP, une passerelle SMS et une passerelle SMS opérateur.

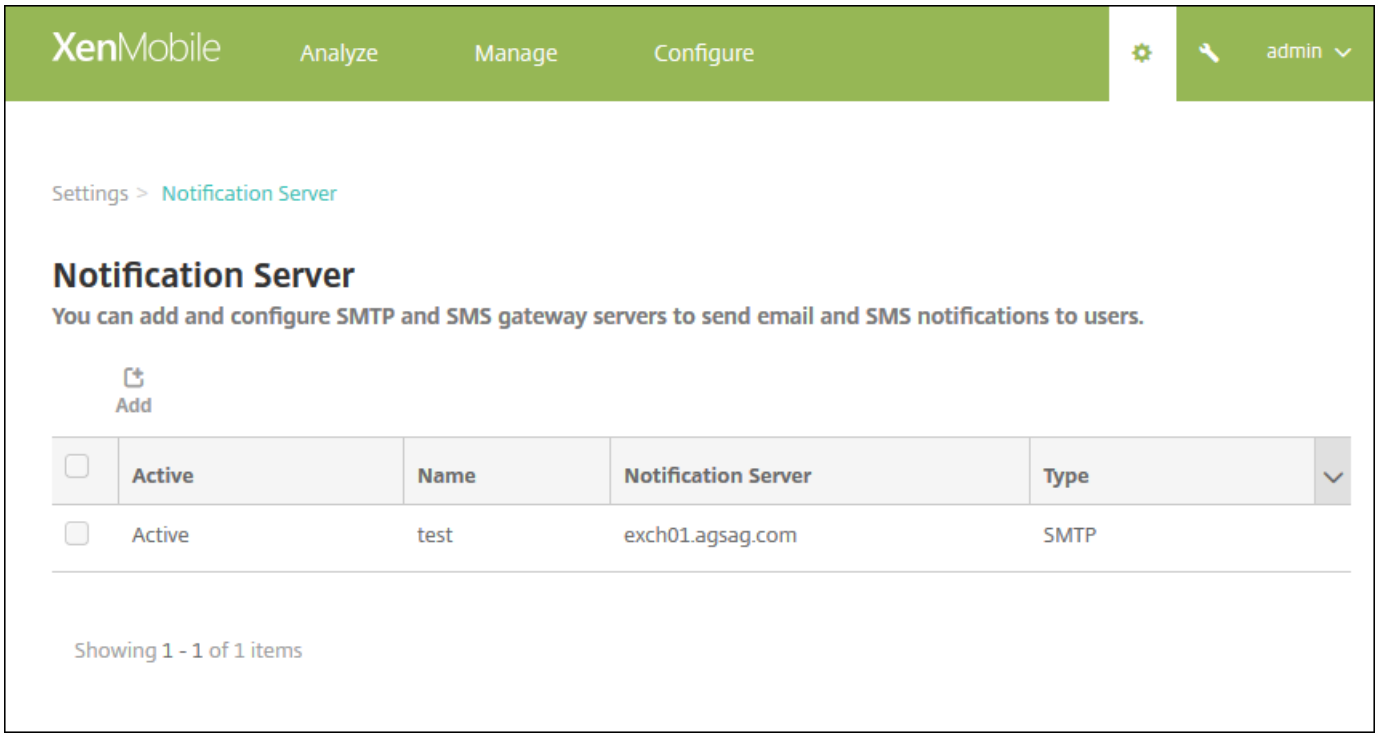
Conditions préalables

- 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, auquel cas vous aurez besoin des informations du site Web du fournisseur de services.
- Vous devez configurer 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.
- Un seul serveur SMTP et un seul serveur SMS sont actifs à la fois.
- Le port 25 doit être ouvert depuis XenMobile dans la zone démilitarisée (DMZ) de votre réseau afin de pointer vers le serveur SMTP sur votre réseau interne pour que les notifications soient envoyées avec succès.

Pour 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.

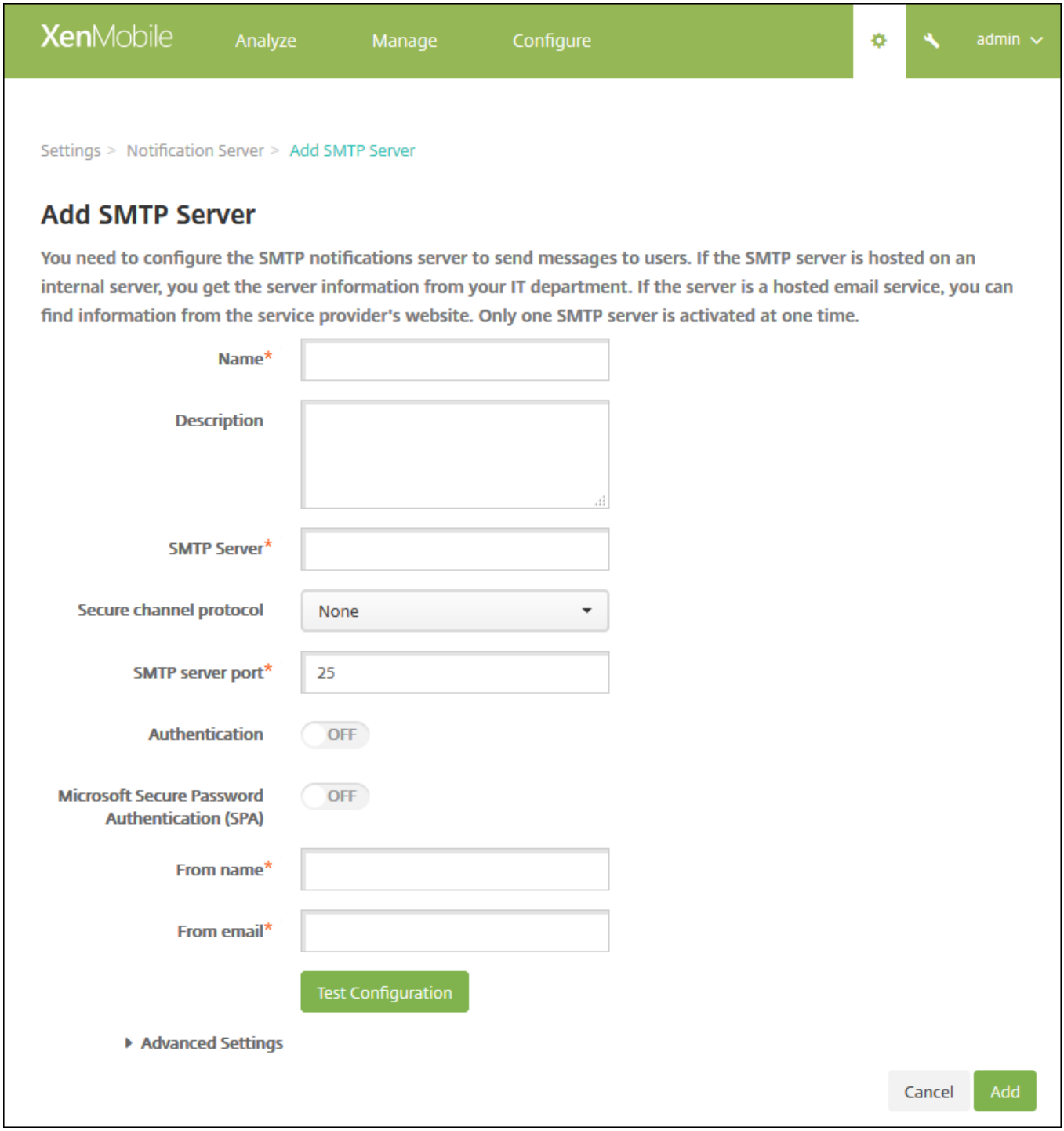
2. Sous **Notifications**, cliquez sur **Serveur de notification**. La page **Serveur de notification** s'affiche.



2. Cliquez sur **Add**. Un menu s'affiche avec les options permettant de 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.

Pour ajouter un serveur SMTP



1. Configurez les paramètres suivants :

- **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 **ON** ou **OFF**. La valeur par défaut est **OFF**.
- Si vous avez activé **Authentification**, configurez les paramètres suivants :
  - **Nom d'utilisateur**: entrez le nom de l'utilisateur pour l'authentification
  - **Mot de passe** : entrez le mot de passe de l'utilisateur.
- **Authentification par mot de passe sécurisé (SPA) Microsoft** : si le serveur SMTP utilise la SPA, cliquez sur **ON**. La valeur par défaut est **OFF**.
- **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.

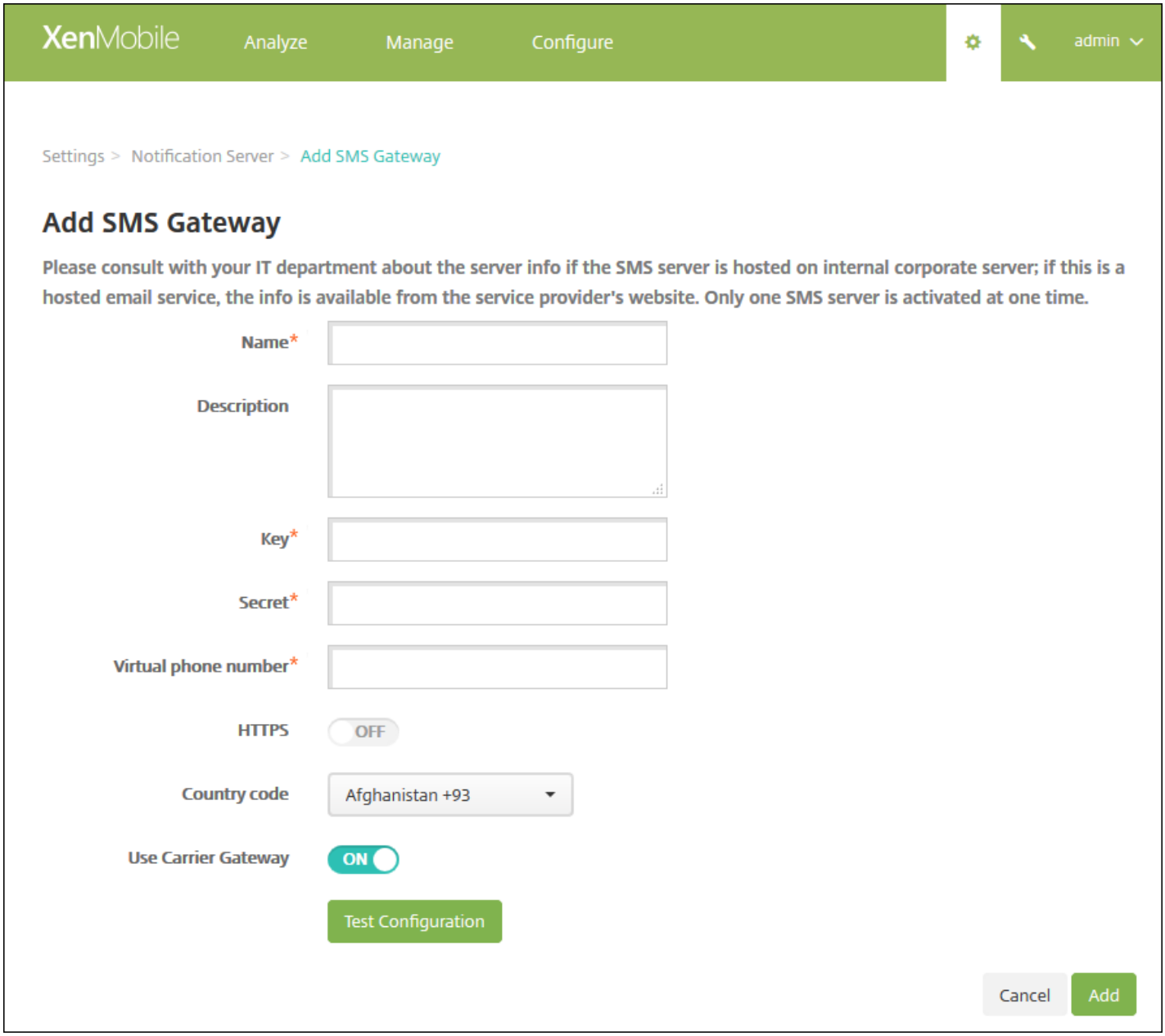
2. Cliquez sur **Tester la configuration** pour envoyer une notification par e-mail test.

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 **Add**.

Pour 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 ; sinon, entrez une étiquette ou un nom significatif. 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 **OFF**.
- **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.

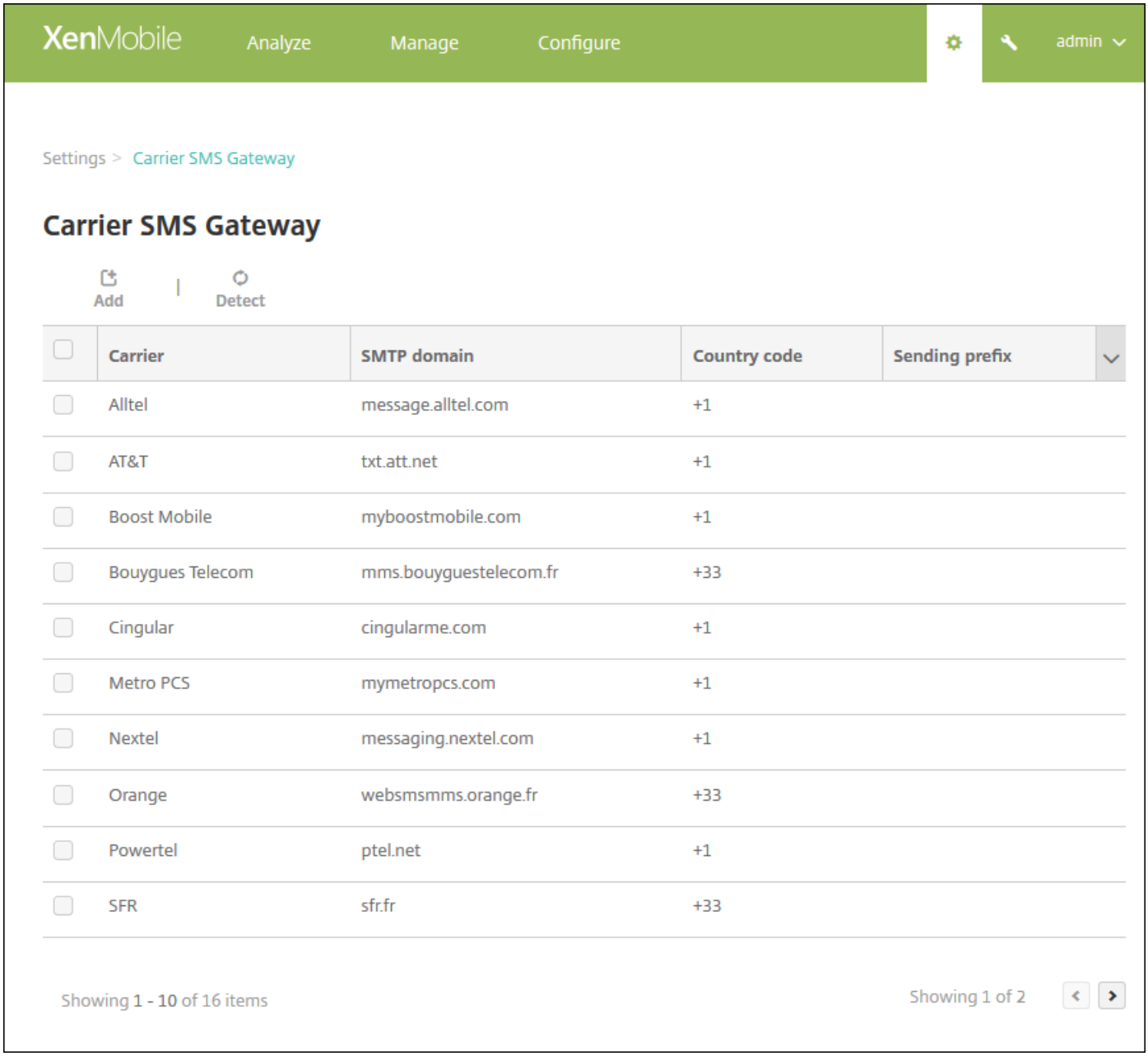
2. Cliquez sur **Add**.

Pour ajouter une passerelle SMS d'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.

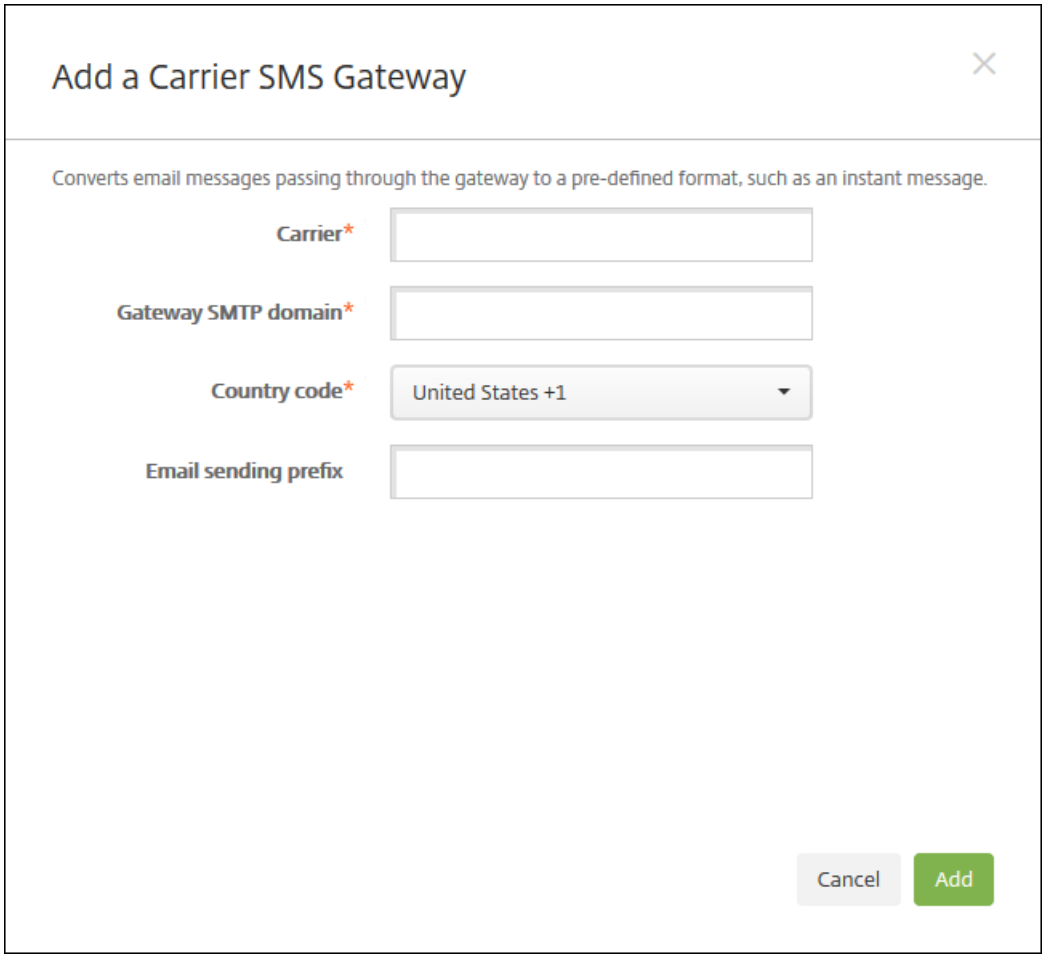
1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

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. Configurez les paramètres suivants :

- **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.

NetScaler Gateway et XenMobile

Oct 17, 2016

Lorsque vous configurez NetScaler 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 en créant un micro VPN depuis les applications vers NetScaler Gateway sur l'appareil. Vous configurez NetScaler Gateway dans la console XenMobile.

Remarque : pour les versions prises en charge de NetScaler Gateway avec XenMobile, consultez la section Compatibilité XenMobile. Pour de plus amples informations sur la configuration de NetScaler Gateway pour XenMobile sur NetScaler, consultez la section Configuration de paramètres pour votre environnement XenMobile.

Authentification

Plusieurs composants participent au processus d'authentification durant les opérations de XenMobile :

- **Serveur XenMobile** : le serveur XenMobile est l'emplacement dans lequel vous définissez la sécurité relative à l'inscription ainsi que l'expérience d'inscription. Les options d'ajout de nouveaux utilisateurs permettent de spécifier si l'inscription est ouverte à tous ou uniquement sur invitation et si une authentification à deux ou trois facteurs est requise. Via les propriétés clientes de XenMobile, vous pouvez activer l'authentification par code PIN Worx et configurer la complexité et l'expiration du code PIN.
- **NetScaler** : NetScaler fournit un point de terminaison pour les sessions SSL micro VPN, assure 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.
- **Worx Home** : Worx Home travaille en tandem avec le serveur XenMobile sur les opérations d'inscription. Worx Home est l'entité installée sur un appareil qui communique avec NetScaler : si une session expire, Worx Home obtient un ticket d'authentification de NetScaler et le transmet aux applications MDX. Citrix recommande d'utiliser le certificate pinning, ce qui évite les attaques « man-in-the-middle ». Pour de plus amples informations, consultez la section sur le certificate pinning dans l'article Worx Home.

  Worx Home facilite également le conteneur de sécurité MDX : Worx Home transmet les stratégies, crée une nouvelle session avec NetScaler lorsqu'une application expire, et définit le délai d'expiration MDX et l'expérience d'authentification. Worx Home 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. Le mode MDX dirige les connexions micro VPN sur NetScaler, applique les restrictions du mode hors connexion et applique les stratégies des clients, telles que des délais d'expiration.

Pour de plus amples informations sur l'authentification, y compris les méthodes d'authentification à un et deux facteurs, les stratégies, les paramètres et les propriétés clientes impliqués dans l'authentification, ainsi que des exemples de trois configurations XenMobile allant d'une sécurité la plus faible à la plus élevée, consultez la section Authentification.

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

Configuration de l'authentification par jeton de sécurité et domaine

Configuration de l'authentification du certificat client

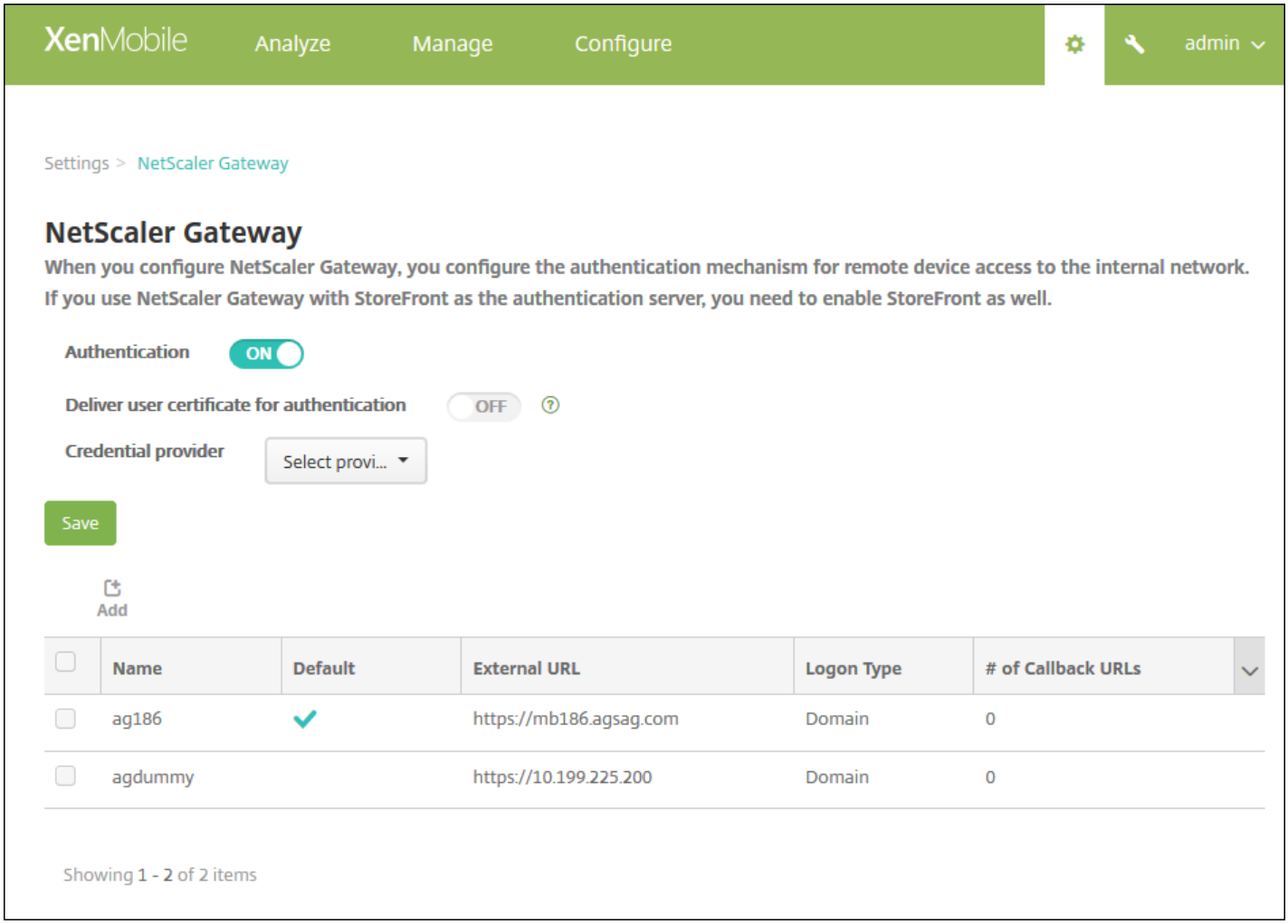
Configuration de XenMobile pour l'authentification par certificat et jeton de sécurité

Configuration de XenMobile et de l'application ShareFile pour l'authentification unique à l'aide de SAML

Pour configurer NetScaler Gateway

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

2. Sous **Serveur**, cliquez sur **NetScaler Gateway**. La page **NetScaler Gateway** s'affiche.



Pour configurer ces paramètres :

- **Authentification** : sélectionnez cette option pour activer l'authentification. La valeur par défaut est **ON**.
- **Délivrer un certificat utilisateur pour l'authentification** : indiquez si vous voulez que XenMobile partage le certificat d'authentification avec Worx Home afin que NetScaler Gateway gère l'authentification du certificat client. La valeur par défaut est **OFF**.
- **Fournisseur d'identités** : dans la liste, cliquez sur le fournisseur d'identités. Pour de plus amples informations, consultez la section Fournisseur d'identités.

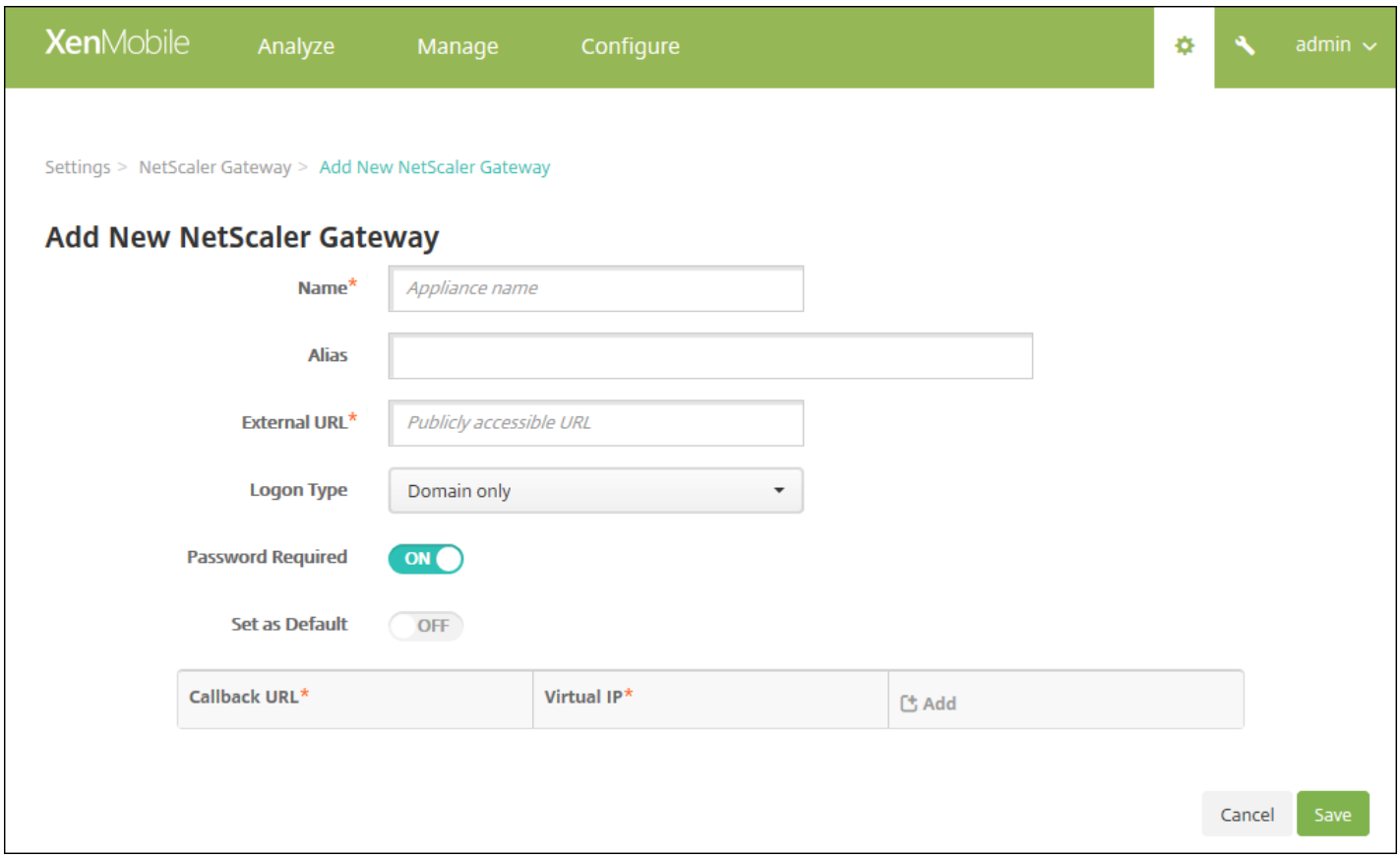
3. Cliquez sur **Enregistrer**.

Pour ajouter une nouvelle instance NetScaler Gateway

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 **NetScaler Gateway**. La page **NetScaler Gateway** s'affiche.

3. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle passerelle NetScaler Gateway** s'affiche.



4. Configurez les paramètres suivants :

- **Nom** : entrez un nom pour l'instance NetScaler Gateway.
- **Alias** : entrez un alias (facultatif).
- URL externe : entrez l'adresse URL publiquement accessible de NetScaler Gateway. Par exemple, https://receiver.com.
- **Type d'ouverture de session**: cliquez sur un type d'ouverture de session dans la liste. 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 est **Domaine uniquement**.

  Si vous disposez de plusieurs domaines, **Domaine uniquement** ne fonctionnera pas, vous devez utiliser **Certificat et domaine**. Pour certaines options, par exemple **Domaine uniquement**, vous ne pouvez pas modifier le champ **Mot de passe**.

  Pour ce type d'ouverture de session, le champ est toujours **ON**. Par ailleurs, les valeurs par défaut pour le champ **Mot de passe requis** changent selon le **Type d'ouverture de session** sélectionné.

  Si vous utilisez **Certificat et jeton de sécurité**, des configurations supplémentaires sont requises sur NetScaler

Gateway pour prendre en charge Worx Home. Pour de plus amples informations, consultez la section Configuration de XenMobile pour l'authentification par certificat et jeton de sécurité.

- **Mot de passe requis** : indiquez si vous souhaitez demander l'authentification par mot de passe. La valeur par défaut est **ON**.
- **Définir par défaut** : indiquez si cette passerelle NetScaler Gateway doit être utilisée par défaut. La valeur par défaut est **OFF**.

5. Cliquez sur **Enregistrer**. La nouvelle passerelle NetScaler Gateway est ajoutée et s'affiche dans le tableau. Vous pouvez modifier ou supprimer une instance en cliquant sur le nom dans la liste.

Après avoir ajouté l'instance NetScaler Gateway, vous pouvez ajouter une adresse URL de rappel et spécifier l'adresse IP virtuelle d'un VPN NetScaler Gateway. **Remarque :** la spécification d'une telle adresse est facultative, mais peut être configurée pour plus de sécurité, plus particulièrement lorsque le serveur XenMobile est dans la DMZ.

1. Dans l'écran NetScaler Gateway, sélectionnez la passerelle NetScaler Gateway dans le tableau et cliquez sur **Ajouter**. La page **Ajouter une nouvelle passerelle NetScaler Gateway** s'affiche.

2. Dans le tableau répertoriant les adresses URL de rappel, cliquez sur **Ajouter**.

3. Spécifiez l'URL de rappel. Ce champ représente le nom de domaine complet (FQDN) et vérifie que la demande émane de NetScaler Gateway.

4. Entrez l'adresse IP virtuelle NetScaler Gateway et cliquez sur **Enregistrer**.

Configuration du LDAP

Aug 22, 2016

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). Vous pouvez ensuite utiliser la configuration LDAP pour importer des groupes, des comptes d'utilisateurs et les propriétés associées. 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. Une utilisation courante du protocole LDAP consiste à fournir une authentification unique (SSO) pour les utilisateurs, dans le cadre de laquelle un seul mot de passe (par utilisateur) est partagé entre plusieurs services, ce qui permet à un utilisateur d'ouvrir une seule session sur un site Web d'entreprise, et d'être automatiquement connecté à l'intranet d'entreprise.

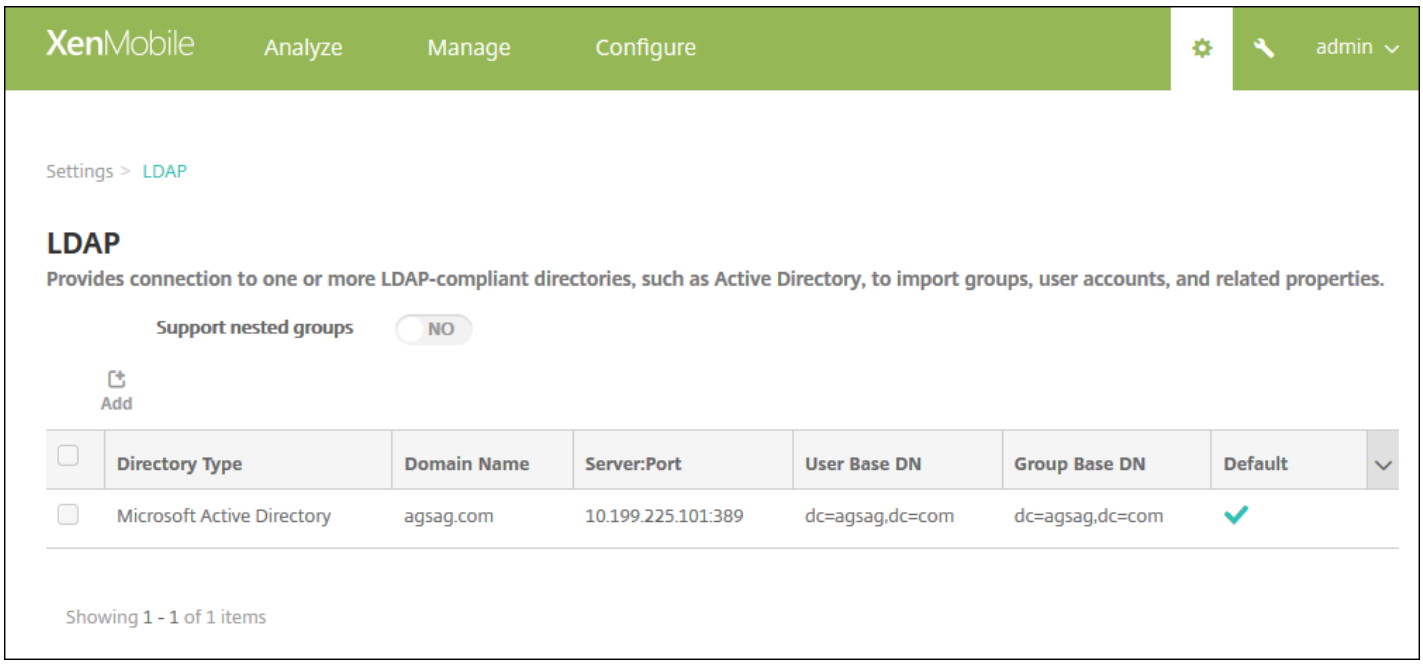
Comment fonctionne LDAP

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.

Pour ajouter des connexions LDAP dans XenMobile

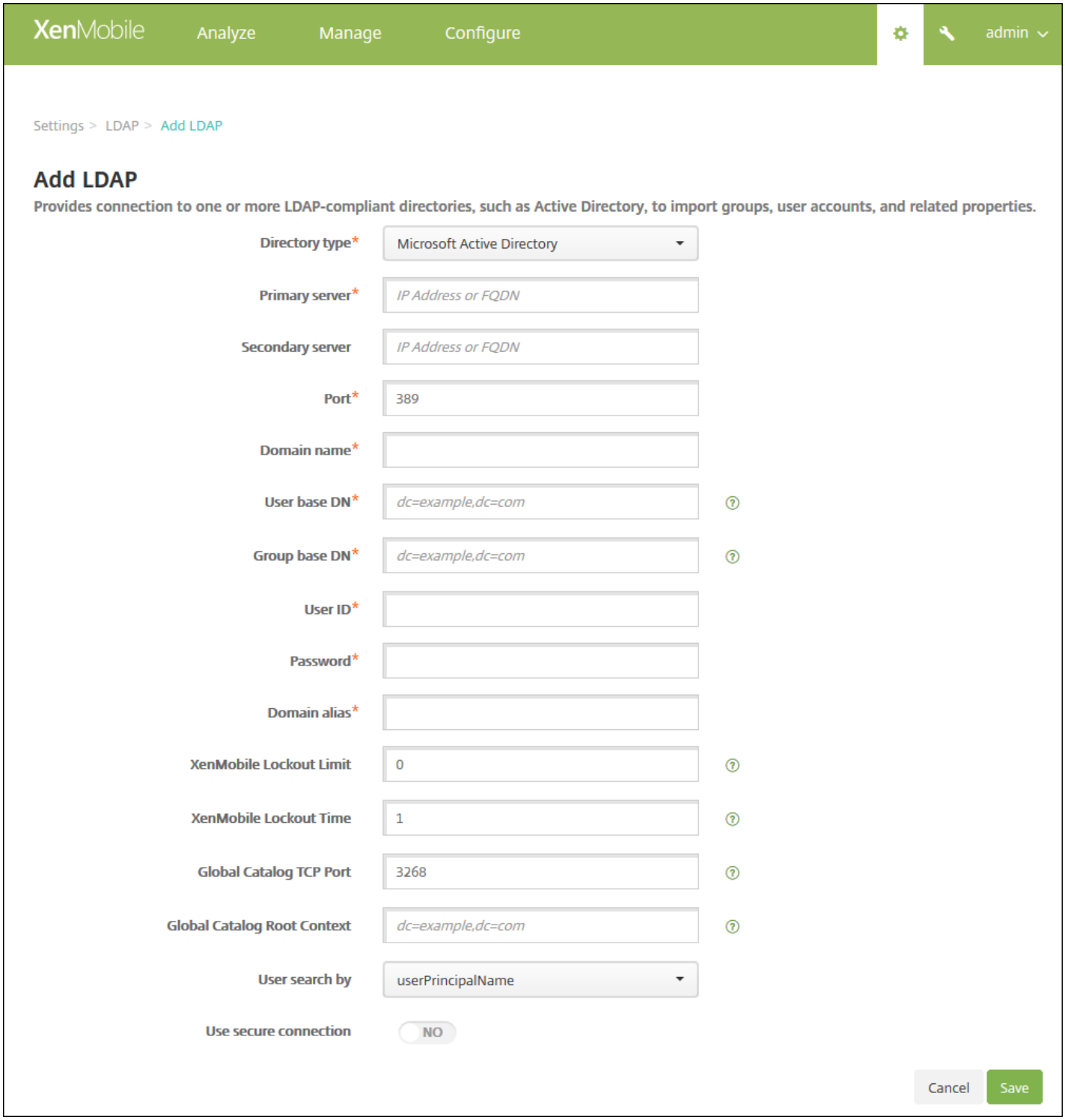
1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Serveur**, cliquez sur **LDAP**. La page **LDAP** s'affiche. Vous pouvez ajouter, modifier ou supprimer des annuaires compatibles LDAP à partir de cette page.



Pour ajouter un annuaire compatible LDAP

1. Sur la page **LDAP**, cliquez sur **Ajouter**. La page **Ajouter LDAP** s'affiche.



2. Configurez les paramètres suivants :

- **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** : 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** : 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=utilisateurs, dc=exemple ou dc=com.
- **Nom unique du groupe de base** : entrez le nom unique du groupe de base spécifié comme cn=nomgroupe. Par exemple, cn=utilisateurs, dc=nomserveur, dc=net où cn=utilisateurs est le nom du groupe ; le nom unique et nomserveur 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.
- **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 vous définissez ce champ 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. Si vous définissez ce champ sur 0, l'utilisateur n'est pas obligé 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**.
- **Utiliser une connexion sécurisée** : indiquez si des connexions sécurisées doivent être utilisées. La valeur par défaut est **NO**.

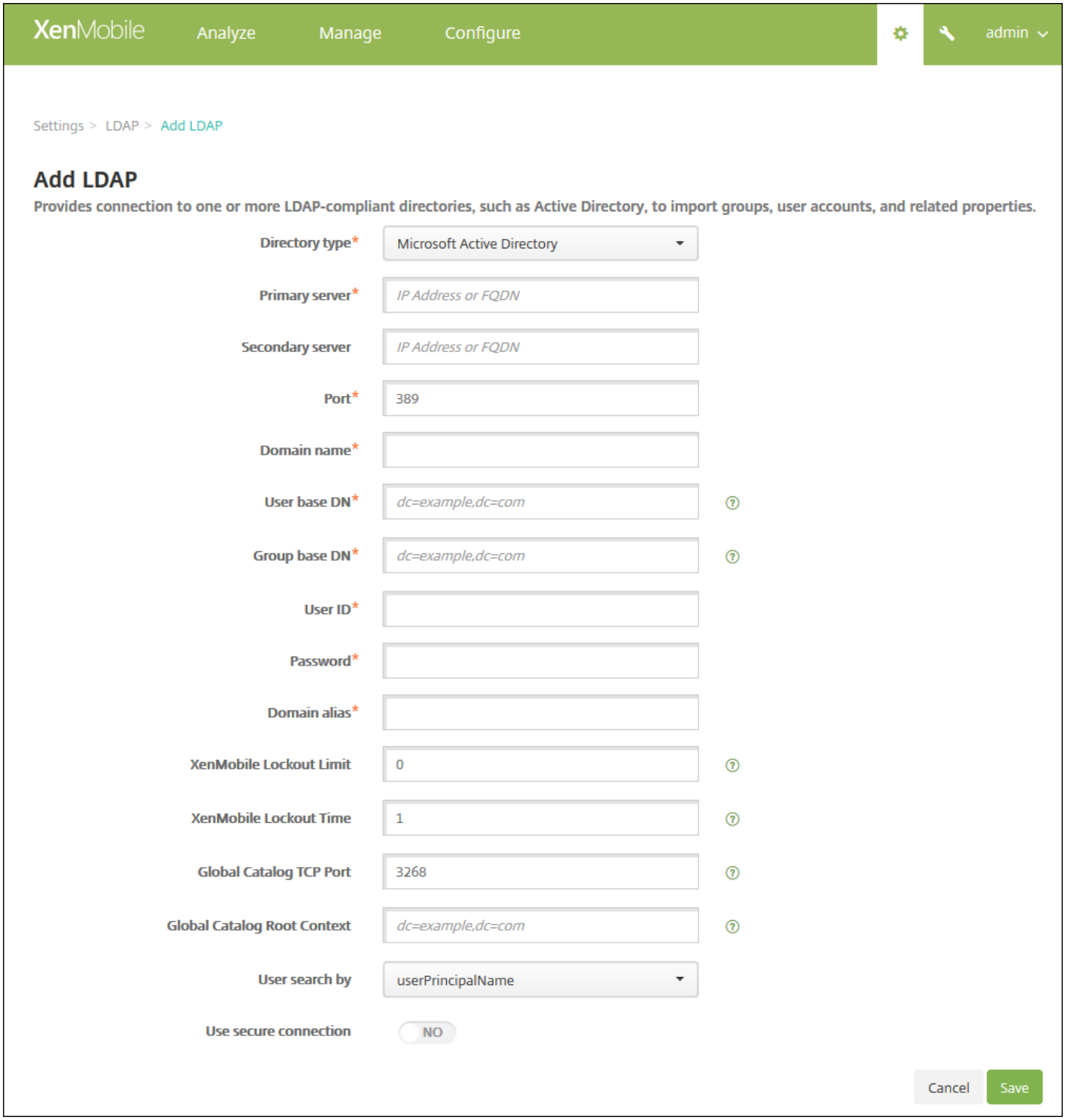
3. Cliquez sur **Enregistrer**.

Pour modifier un annuaire compatible LDAP

1. Dans le tableau **LDAP**, sélectionnez l'annuaire que vous souhaitez modifier.

> **Remarque :** lorsque vous sélectionnez la case à cocher en regard d'un annuaire, le menu d'options s'affiche au-dessus de la liste LDAP ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

Cliquez sur **Modifier**. La page **Ajouter 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=utilisateurs, dc=exemple ou dc=com.
- **Nom unique du groupe de base** : entrez le nom unique du groupe de base spécifié comme cn=nomgroupe. Par exemple, cn=utilisateurs, dc=nomserveur, dc=net où cn=utilisateurs est le nom du groupe ; le nom unique et et nomserveur 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.
- **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 vous définissez ce champ 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. Si vous définissez ce champ sur 0, l'utilisateur n'est pas obligé 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**.
- **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.

   Remarque : 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 par jeton de sécurité et domaine

Oct 17, 2016

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.

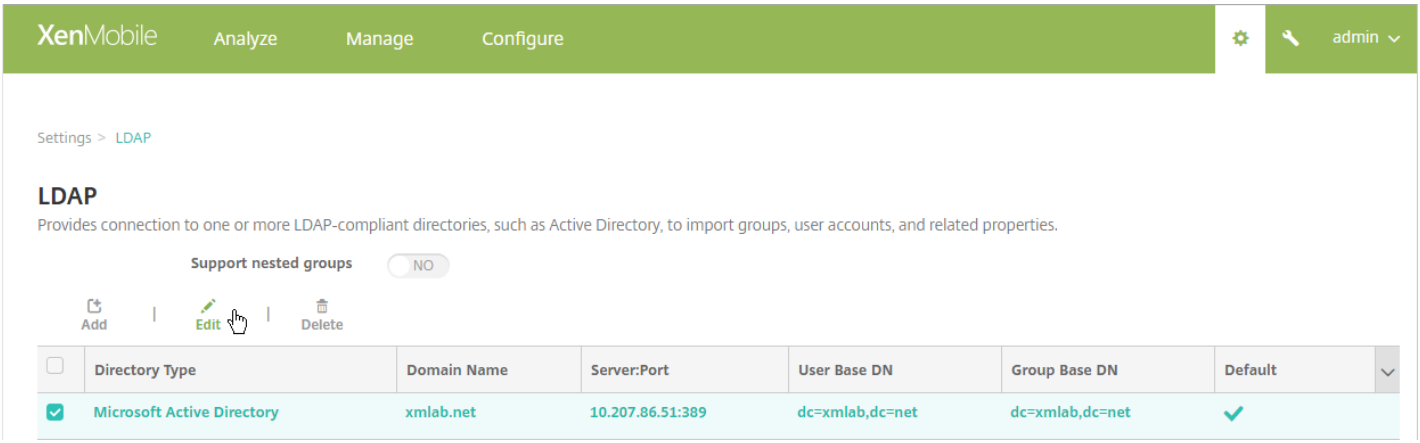
Pour une utilisabilité optimale, vous pouvez combiner cette configuration avec un code PIN Worx et la mise en cache du mot de passe Active Directory de façon à ce que les utilisateurs n'aient pas à entrer de manière répétée leur nom d'utilisateur et mot de passe Active Directory. Les utilisateurs devront entrer leurs noms et mots de passe lors de l'inscription, de l'expiration du mot de passe et du verrouillage du compte.

Configuration des 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.

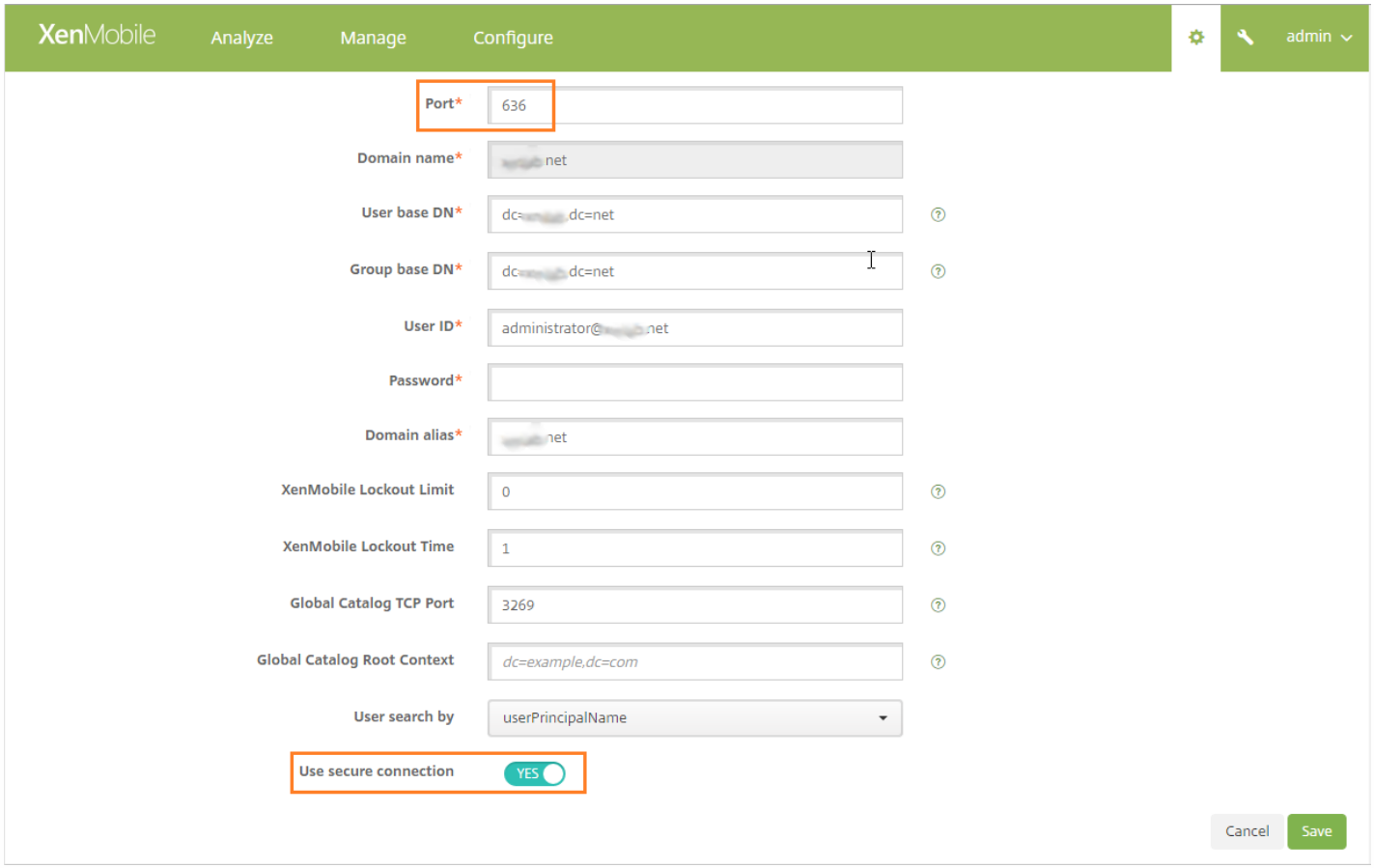
1. Dans **Paramètres**, cliquez sur **LDAP**.

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**.



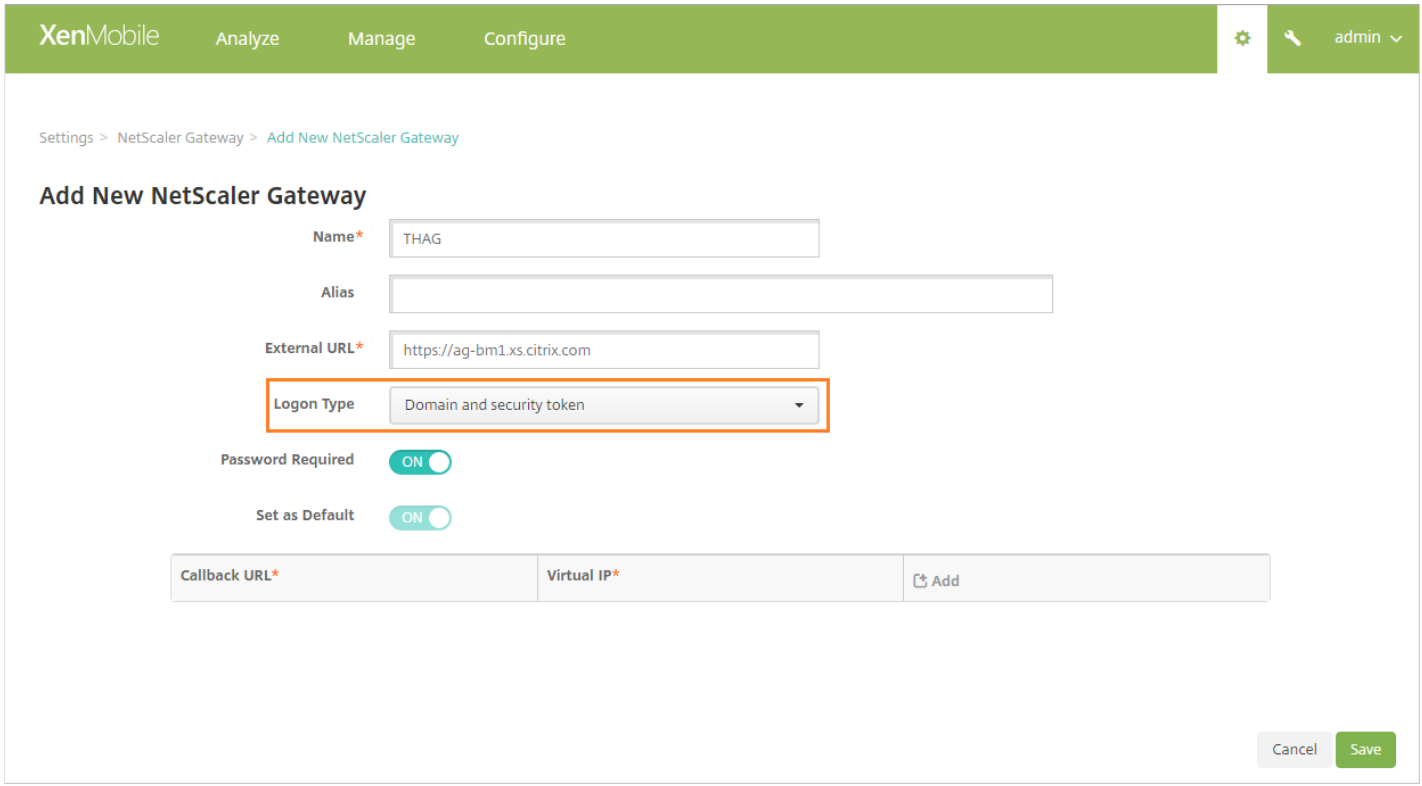
Configuration des paramètres de NetScaler Gateway

Les étapes suivantes supposent que vous avez déjà ajouté une instance NetScaler Gateway à XenMobile. Pour ajouter une instance NetScaler Gateway, consultez la section NetScaler Gateway et XenMobile.

1. Dans **Paramètres**, cliquez sur **NetScaler Gateway**.

2. Sélectionnez le NetScaler Gateway et cliquez sur **Modifier**.

3. Depuis **Type d'ouverture de session**, sélectionnez **Domaine et jeton de sécurité**.



Activation du code PIN Worx et de la mise en cache du mot de passe Active Directory

Pour activer le code PIN Worx et la mise en cache du mot de passe Active Directory, accédez à **Paramètres > Propriétés du client** et sélectionnez les cases **Activer l'authentification par code PIN Worx** et **Activer la mise en cache du mot de passe de l'utilisateur**. Pour de plus amples informations, consultez la section Référence des propriétés du client.

Configuration de NetScaler Gateway pour l'authentification par jeton de sécurité et domaine

Configurez des profils de sessions NetScaler Gateway et des stratégies pour les serveurs virtuels que vous utilisez avec XenMobile. Pour de plus amples informations, consultez la section Configuration de l'authentification par jeton de sécurité et domaine pour XenMobile dans la documentation de NetScaler Gateway.

Certificats

Oct 17, 2016

Dans XenMobile, les certificats permettent d'établir des connexions sécurisées et d'authentifier les utilisateurs.

Par défaut, XenMobile est équipé d'un certificat SSL auto-signé qui est généré lors de l'installation afin de sécuriser les communications sur le serveur. Citrix vous recommande de 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 Worx pour accéder en Single Sign-On aux applications Worx. Le code secret Worx simplifie également l'expérience utilisateur pour l'authentification. Le code secret Worx 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, vous devez configurer et créer un certificat Apple Push Notification Service (APNS). Pour obtenir des instructions détaillées, consultez la section Faire une demande de certificat 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**
NetScaler Gateway	PEM (BASE64) PFX (PKCS#12)	SSL, racine NetScaler Gateway convertit automatiquement un fichier PFX vers PEM.
Serveur XenMobile	PEM ou PFX (PKCS#12)	SSL, SAML, APNS XenMobile génère également une PKI complète durant le processus d'installation. Le serveur XenMobile ne prend pas en charge les certificats avec une extension .pem. Utilisez la commande openssl pour générer un fichier PFX à partir d'un fichier PEM : openssl pkcs12 -export -out certificate.pfx -in certificate.pem
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. Veuillez noter que les certificats 1024 bits peuvent être facilement compromis.

Pour NetScaler Gateway et le serveur XenMobile, 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 NetScaler 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 NetScaler Gateway ou XenMobile.

Certificats clients pour l'authentification

Dans l'environnement XenMobile, l'association d'un certificat client et de l'authentification LDAP constitue la solution la plus apte à garantir la sécurité tout en offrant une expérience utilisateur maximale. En outre, cette association vous permet de bénéficier des meilleures capacités de SSO et d'une sécurité fournie par l'authentification à deux facteurs sur NetScaler. L'utilisation d'un certificat client et de LDAP 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). WorxMail (et certaines autres applications Worx) 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 Worx et la mise en cache du mot de passe Active Directory.

L'authentification du certificat client est basée sur les attributs du certificat client qui est présenté au serveur virtuel. Vous devez lier un certificat racine au serveur virtuel sur NetScaler Gateway. Lorsque les utilisateurs ouvrent une session sur NetScaler Gateway, les informations relatives au nom d'utilisateur sont extraites à partir du champ spécifié du certificat. Ce champ est généralement Subject:CN. Si le nom d'utilisateur est extrait avec succès, l'utilisateur est authentifié. S'il ne fournit pas de certificat valide durant la négociation SSL ou si l'extraction du nom d'utilisateur échoue, l'authentification échoue.

Remarques :

- L'authentification du certificat client peut également être utilisée avec un autre type d'authentification, tel que RADIUS.
- Vous pouvez authentifier les utilisateurs en fonction du certificat client en définissant le type d'authentification par défaut de manière à utiliser le certificat client. Vous pouvez également créer une action de certificat dont la tâche est de définir les opérations à réaliser durant l'authentification basée sur un certificat client SSL.
- WorxMail (et certaines autres applications Worx) 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 Worx et la mise en cache du mot de passe Active Directory.
- L'authentification des appareils avec NetScaler Gateway n'est pas prise en charge pour les certificats obtenus via une autorité de certification discrétionnaire.
- XenMobile ne prend pas en charge l'authentification du certificat client pour les appareils partagés.

PKI XenMobile

La fonctionnalité d'intégration de l'infrastructure de clé publique (PKI) XenMobile vous permet de gérer la distribution et le cycle de vie des certificats de sécurité utilisés sur vos appareils.

XenMobile crée une PKI interne pour l'authentification de l'appareil lors du processus d'installation.

Les PKI externes peuvent également être utilisées pour émettre des certificats sur les appareils que vous pouvez utiliser dans les stratégies de configuration ou pour l'authentification des clients à NetScaler Gateway.

La fonction principale du système PKI est l'entité PKI. Une entité PKI présente un composant backend pour les opérations

PKI. Ce composant fait partie de votre infrastructure d'entreprise, telle que Microsoft, RSA, Entrust Symantex ou OpenTrust PKI. L'entité PKI gère l'émission et la révocation de certificats backend. Elle représente la source de référence pour le statut du certificat. La configuration XenMobile doit normalement contenir une entité PKI par composant PKI backend.

La fonction secondaire du système PKI est le fournisseur d'identités. Un fournisseur d'identités est une configuration particulière d'émission et de cycle de vie de certificat. Il contrôle des éléments comme le format du certificat (sujet, clé, algorithmes) et les conditions de sa révocation ou de son renouvellement, le cas échéant. Les fournisseurs d'identités délèguent des opérations aux entités PKI. En d'autres termes, bien que les fournisseurs d'identités contrôlent le moment où les opérations PKI sont exécutées et la nature des données avec lesquelles elles sont effectuées, les entités PKI contrôlent la manière dont ces opérations sont réalisées. La configuration XenMobile contient normalement plusieurs fournisseurs d'identités par entité PKI.

Administration des certificats XenMobile

Nous vous recommandons d'effectuer un suivi des certificats que vous utilisez dans votre déploiement XenMobile, et plus particulièrement leurs dates d'expiration et mots de passe associés. Cette section vise à faciliter l'administration des certificats dans XenMobile.

Votre environnement peut inclure une partie ou l'ensemble des certificats suivants :

Serveur XenMobile
Certificat SSL pour le nom de domaine complet MDM
Certificat SAML (pour ShareFile)
Certificats d'autorité de certification racine et intermédiaire pour les certificats ci-dessus et toute autre ressource interne (StoreFront/Proxy, etc)
Certificats APNS pour la gestion des appareils iOS
Certificat APNS interne pour les notifications Worx Home au serveur XenMobile
Certificat utilisateur PKI pour la connectivité aux infrastructures de clé publique (PKI)

MDX Toolkit
Certificat Apple Developer
Profil de provisioning Apple (par application)
Certificat APNS Apple (à utiliser avec WorxMail)
Fichier keystore Android
Windows Phone – Certificat Symantec

NetScaler
Certificat SSL pour le nom de domaine complet MDM
Certificat SSL pour le nom de domaine complet de la passerelle
Certificat SSL pour le nom de domaine complet des StorageZone Controller (SZC) ShareFile
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 précédents

Stratégie d'expiration des certificats XenMobile

Si vous laissez un certificat expirer, ce certificat n'est plus valide. Par conséquent vous ne pouvez plus effectuer de transactions sécurisées sur votre environnement ni accéder aux ressources XenMobile.

> **Remarque**
>
> L'autorité de certification (CA) vous invitera à renouveler votre certificat SSL avant la date d'expiration.

Certificats APNS pour WorxMail

Étant donné que les certificats du service de notification push d'Apple (APNS) expirent tous les ans, n'oubliez pas de créer de nouveaux certificats SSL pour le service de notification push d'Apple et de les mettre à niveau sur le portail Citrix avant que les certificats n'expirent. Si le certificat expire, les utilisateurs rencontreront des incohérences dans les notifications push de WorxMail. En outre, vous ne pourrez plus envoyer de notifications push pour vos applications.

Certificats APNS pour la gestion des appareils iOS

Pour inscrire et gérer des appareils iOS avec XenMobile, vous devez configurer et créer un certificat APNS d'Apple. Si le certificat expire, les utilisateurs ne peuvent pas s'inscrire auprès de XenMobile et vous ne pouvez pas gérer leurs appareils iOS. Pour de plus amples informations, consultez la section Faire une demande de certificat APNS.

Vous pouvez afficher l'état et la date d'expiration du certificat APNS en vous connectant au portail **Apple Push Certificates Portal**. Vous devez vous connecter à l'aide du même utilisateur que celui qui a créé le certificat.

Apple vous enverra également une notification par e-mail 30 et 10 jours avant la date d'expiration avec les informations suivantes :

« The following Apple Push Notification Service certificate, created for AppleID *CustomersID* will expire on *Date*. Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

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.

Thank You,

Apple Push Notification Service »

MDX Toolkit (certificat de distribution iOS)

Toute application exécutée sur un appareil iOS physique (autres que des applications dans l'App Store d'Apple) doit être signée avec un profil de provisioning et un certificat correspondant.

Veuillez noter qu'un certificat et un profil de provisioning iOS Developer for Enterprise existants peuvent ne pas être compatibles avec iOS 9. Pour de plus amples informations, consultez la section Wrapping d'applications Worx pour iOS 9.

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 wrapper avec le MDX Toolkit. Un exemple d'ID d'application acceptable est : com.NomSociété.NomProduit.
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 de plus amples informations, consultez la section Wrapping des applications mobiles iOS.

Pour confirmer que tous les certificats du serveur XenMobile sont valides, procédez comme suit :

1. Dans la console XenMobile, cliquez sur **Paramètres** et sur **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.

Certificats d'entreprise Symantec pour Windows Phone

Symantec est le fournisseur exclusif des certificats de signature de code du service Microsoft App Hub. Les développeurs et les éditeurs de logiciels rejoignent le App Hub pour distribuer des applications Windows Phone et Xbox 360 en vue de leur téléchargement via le Windows Marketplace. Pour de plus amples informations, consultez Symantec Code Signing Certificates for Windows Phone dans la documentation de Symantec.

Si le certificat expire, les utilisateurs Windows Phone ne peuvent pas s'inscrire, installer une application publiée et signée par l'entreprise, ou démarrer une application d'entreprise qui a été installée sur le téléphone.

NetScaler

Pour de plus amples informations sur la façon de gérer l'expiration des certificats pour NetScaler, consultez l'article How to handle certificate expiry on NetScaler dans le centre de connaissances Citrix.

Un certificat NetScaler ayant expiré empêche les utilisateurs de s'inscrire, d'accéder au Worx Store, de se connecter au Exchange Server lors de l'utilisation de WorxMail, et d'énumérer et d'ouvrir des applications HDX (en fonction du certificat qui a expiré).

Le Expiry Monitor et le Command Center peuvent vous aider à suivre vos certificats NetScaler et vous informeront lorsque le certificat expire. Ces deux outils permettent d'assurer le suivi des certificats Netscaler suivants :

Certificat SSL pour le nom de domaine complet MDM
Certificat SSL pour le nom de domaine complet de la passerelle
Certificat SSL pour le nom de domaine complet des StorageZone Controller (SZC) ShareFile
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 précédents

Chargement de certificats dans XenMobile

Oct 17, 2016

Les certificats sont utilisés par le serveur XenMobile. Vous devez charger des certificats sur XenMobile via la zone **Certificats** de la console XenMobile. Ces certificats 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 la zone Certificats en tant qu'emplacement de stockage pour les certificats que vous voulez déployer sur des appareils. Cette utilisation s'applique particulièrement aux autorités de certification utilisées pour établir une relation de confiance sur l'appareil.

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 êtes invité à choisir des certificats de serveur répondant à des critères spécifiques au contexte dans une liste. Par exemple, il se peut que vous souhaitiez configurer XenMobile pour s'intégrer à Microsoft CA. 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, veuillez consulter la section Configuration de l'authentification du certificat client.

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 que vous chargez.

Chargement de certificats sur la console

Vous pouvez charger le certificat d'autorité de certification (sans la clé privée) que l'autorité de certification utilise pour signer les demandes, et un certificat client SSL (avec la clé privée) pour l'authentification du client. Lors de la configuration de l'entité Microsoft CA, vous devez spécifier le certificat d'autorité de certification, que vous pouvez sélectionner à partir d'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.

XenMobile prend en charge les formats d'entrée suivants pour les certificats :

- fichiers de certificat codés PEM ou DER ;
- fichiers de certificat codés PEM ou DER avec un fichier de clé privée associé au format codé PEM ou DER ;
- keystores PKCS#12 (P12 ; également connus sous le nom de fichier PFX sous Windows).

Important : le serveur XenMobile ne prend pas en charge les certificats avec une extension .pem. Utilisez la commande openssl pour générer un fichier PFX à partir d'un fichier PEM :

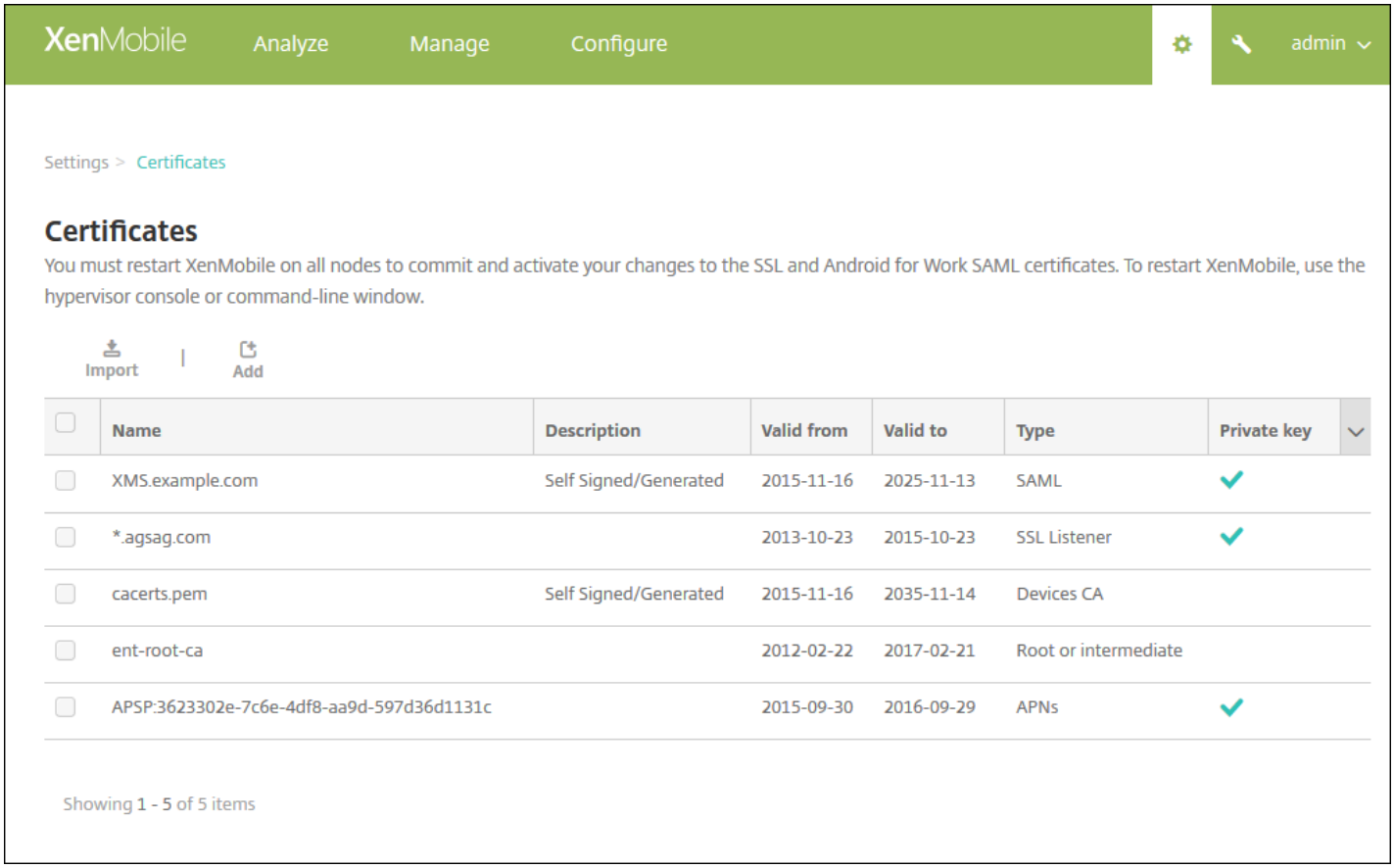
openssl pkcs12 -export -out certificate.pfx -in certificate.pem

Pour importer un keystore

Les keystores, de par leur conception, peuvent comporter plusieurs entrées. Lors du chargement à partir d'un keystore, par conséquent, 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.

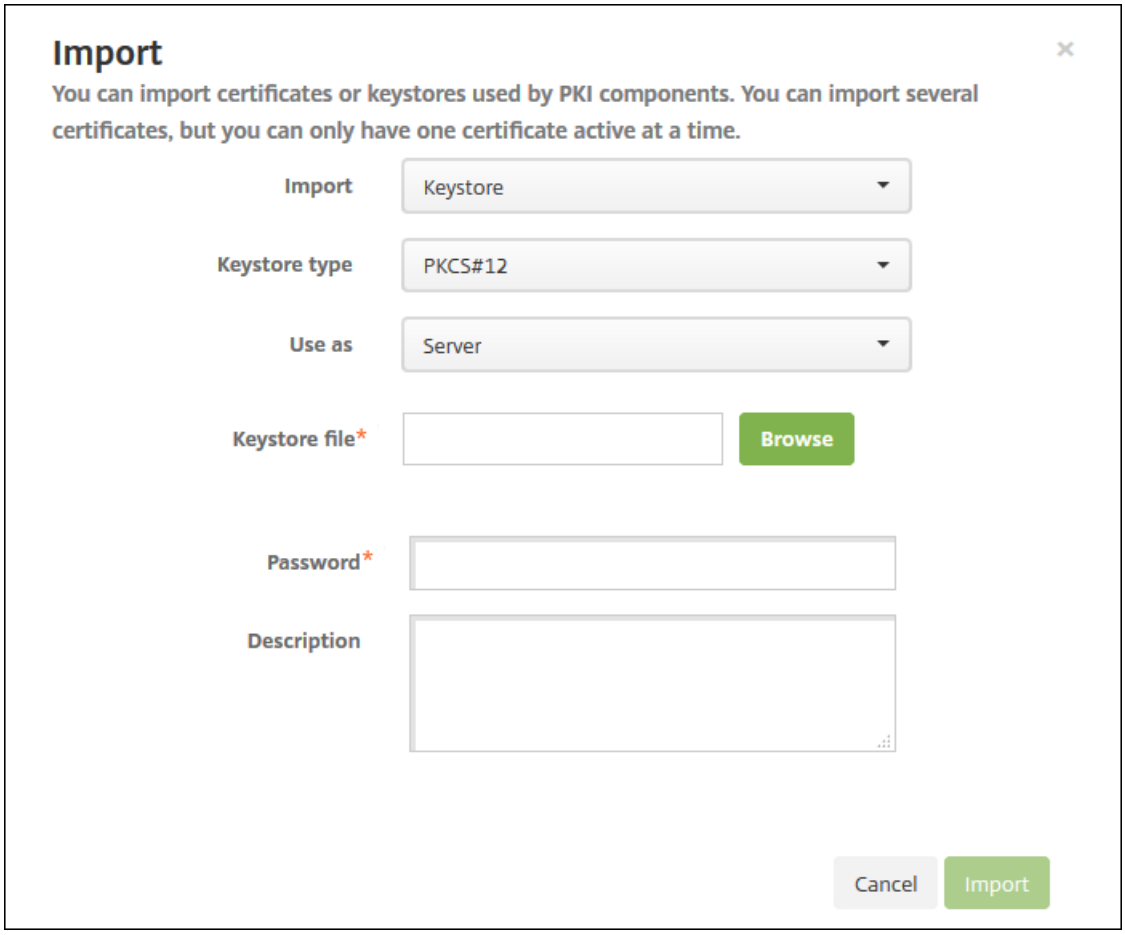
2. Cliquez sur **Certificats**. La page **Certificats** s'affiche.



3. Cliquez sur **Importer**. La boîte de dialogue **Importer** apparaît.

4. Configurez les paramètres suivants :

- **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 utilisez le keystore. Les options disponibles sont :
  - **Serveur**. Les certificats de serveur sont des certificats utilisés par le serveur XenMobile 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** : sélectionnez le fichier de keystore que vous souhaitez importer, en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
- **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 et importe tous les certificats dans cette chaîne (créant 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, comme si chaque certificat suivant de la chaîne est l'émetteur du certificat précédent.

Vous pouvez ajouter une description facultative pour le certificat importé à des fins heuristiques. 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**, cliquez pour spécifier la manière dont vous utilisez le keystore. Les options disponibles sont :

- **Serveur**. Les certificats de serveur sont des certificats utilisés par le serveur XenMobile 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. Parcourez pour trouver le certificat que vous voulez importer.

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.

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 donné. Si vous essayez d'importer un certificat pour la même paire de clés qu'un certificat déjà importé, vous avez l'option de remplacer l'entrée existante ou de la supprimer.

Pour une mise à jour efficace de vos certificats, dans la console XenMobile, 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.

Configuration de l'authentification du certificat client

Jul 27, 2016

Pour utiliser l'authentification du certificat client dans les modes XenMobile ENT et MAM, vous devez configurer le serveur Microsoft, le serveur XenMobile et NetScaler Gateway. Les étapes générales suivantes sont détaillées 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 le serveur XenMobile :

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 NetScaler Gateway afin de fournir un certificat utilisateur pour l'authentification.

Sur NetScaler Gateway :

1. Configurez NetScaler Gateway pour XenMobile pour l'authentification par certificat en mode MAM.

Conditions préalables

- Pour les appareils Windows Phone 8.1 utilisant l'authentification du certificat client et le déchargement SSL, vous devez désactiver la réutilisation de session SSL pour le port 443 sur les serveurs virtuels d'équilibrage de charge dans NetScaler. Pour ce faire, exécutez la commande suivante sur les serveurs virtuels pour le port 443 :

  set ssl vserver sessReuse DISABLE

  Remarque : la désactivation de la réutilisation de la session SSL désactive certaines des optimisations fournies par NetScaler, ce qui peut entraîner une diminution des performances sur NetScaler.

- Pour configurer l'authentification basée sur certificat pour Exchange ActiveSync, consultez le blog de Microsoft.
- 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 ont été installés sur les appareils mobiles. Sinon, l'authentification basée sur certificat échouera lors de la configuration de la boîte aux lettres dans WorxMail. 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**.
- Assurez-vous que WorxMail pour iOS, Android, et Windows Phone sont wrappés avec la dernière version du MDX Toolkit.

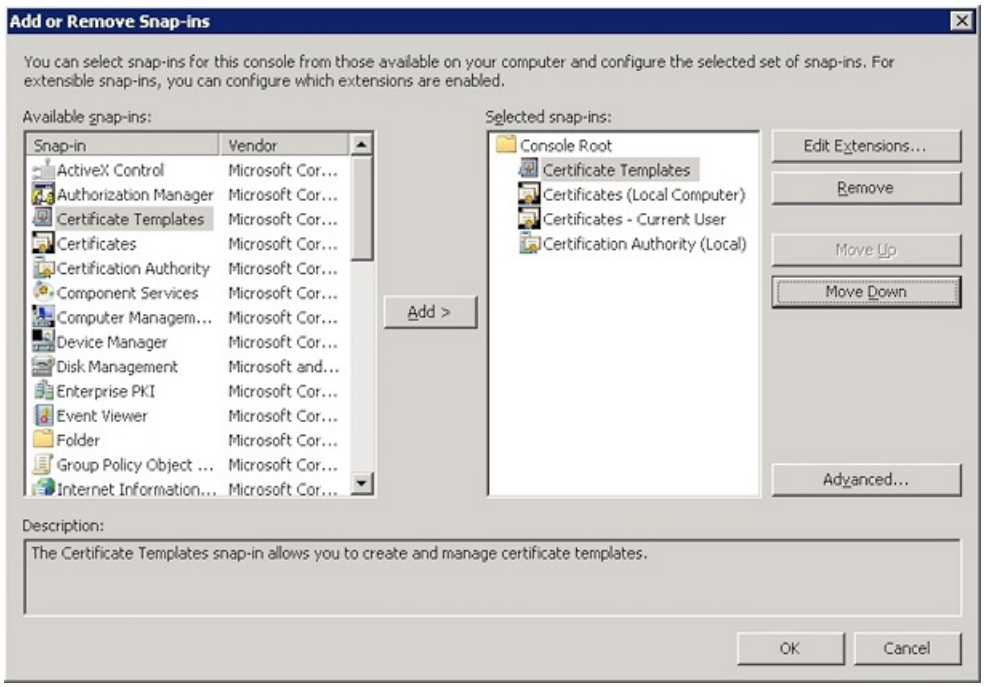
Ajout d'un composant logiciel enfichable pour les

certificats dans la console Microsoft Management Console

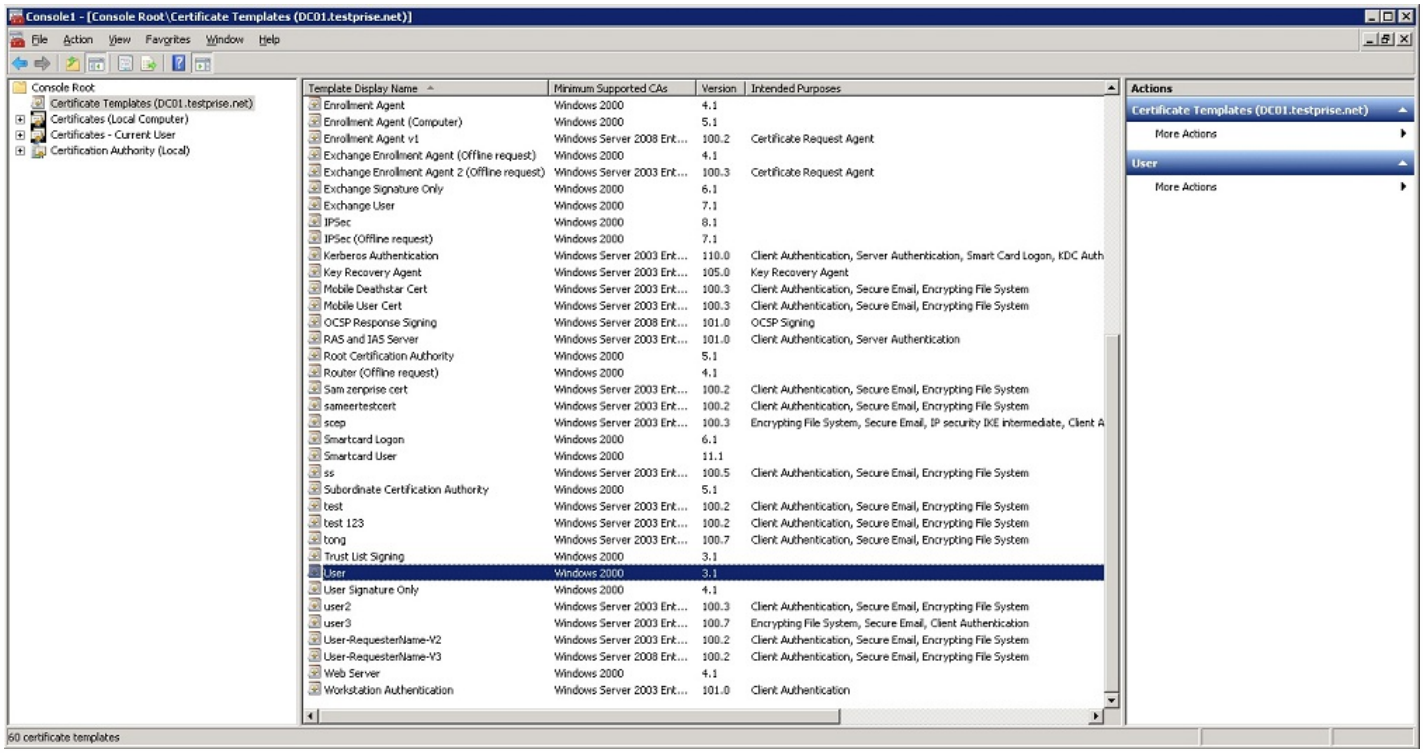
1. Ouvrez la console et cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.

2. Ajoutez les composants logiciels enfichables suivants :

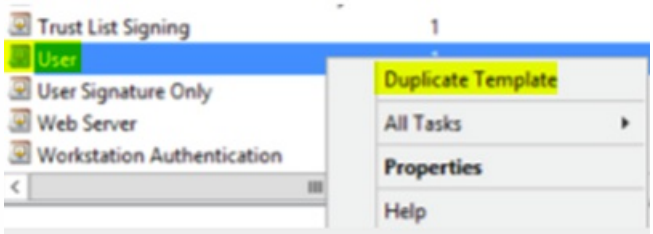
    Modèles de certificats
    Certificats (ordinateur local)
    Certificats - Utilisateur actuel
    Autorité de certification (locale)



3. Développez **Modèles de certificats**.



4. Sélectionnez le modèle **Utilisateur** et **Dupliquer le modèle**.

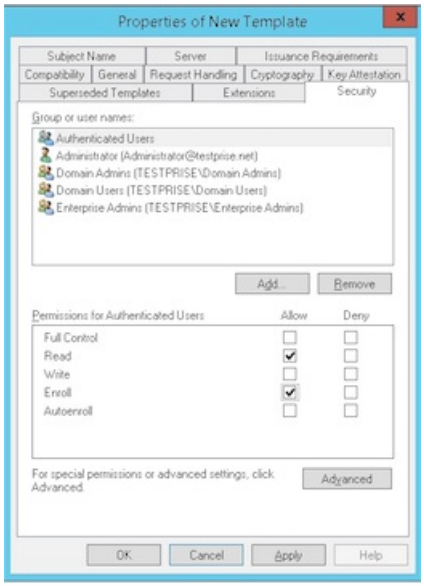


5. Fournissez le nom du modèle.

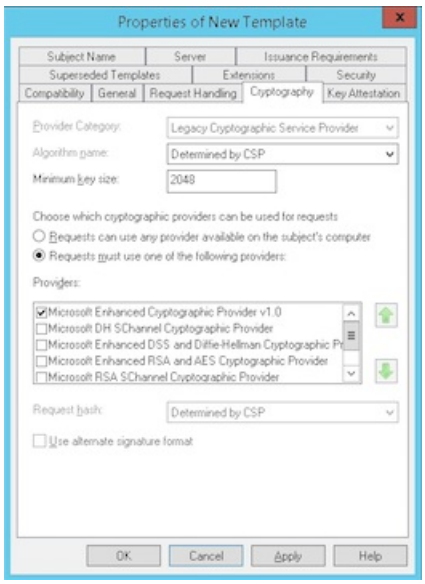
> **Important :** ne sélectionnez pas la case **Publier le certificat dans Active Directory** sauf si cela est nécessaire. Si cette option est sélectionnée, tous les certificats client utilisateur seront émis/créés dans Active Directory, ce qui pourrait encombrer votre base de données Active Directory.

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**.

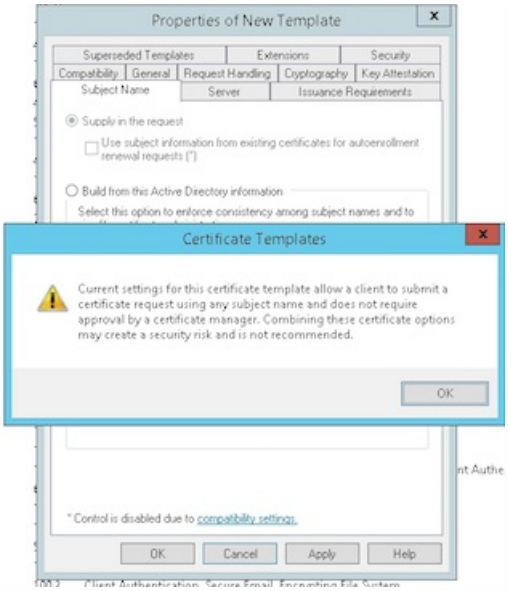
7. Sous **Sécurité**, sélectionnez l'option **Inscrire** dans la colonne **Autoriser** pour les utilisateurs authentifiés.



8. Sous **Cryptographie**, n'oubliez pas de fournir la taille de clé, que vous devrez entrer lors de la configuration de XenMobile.



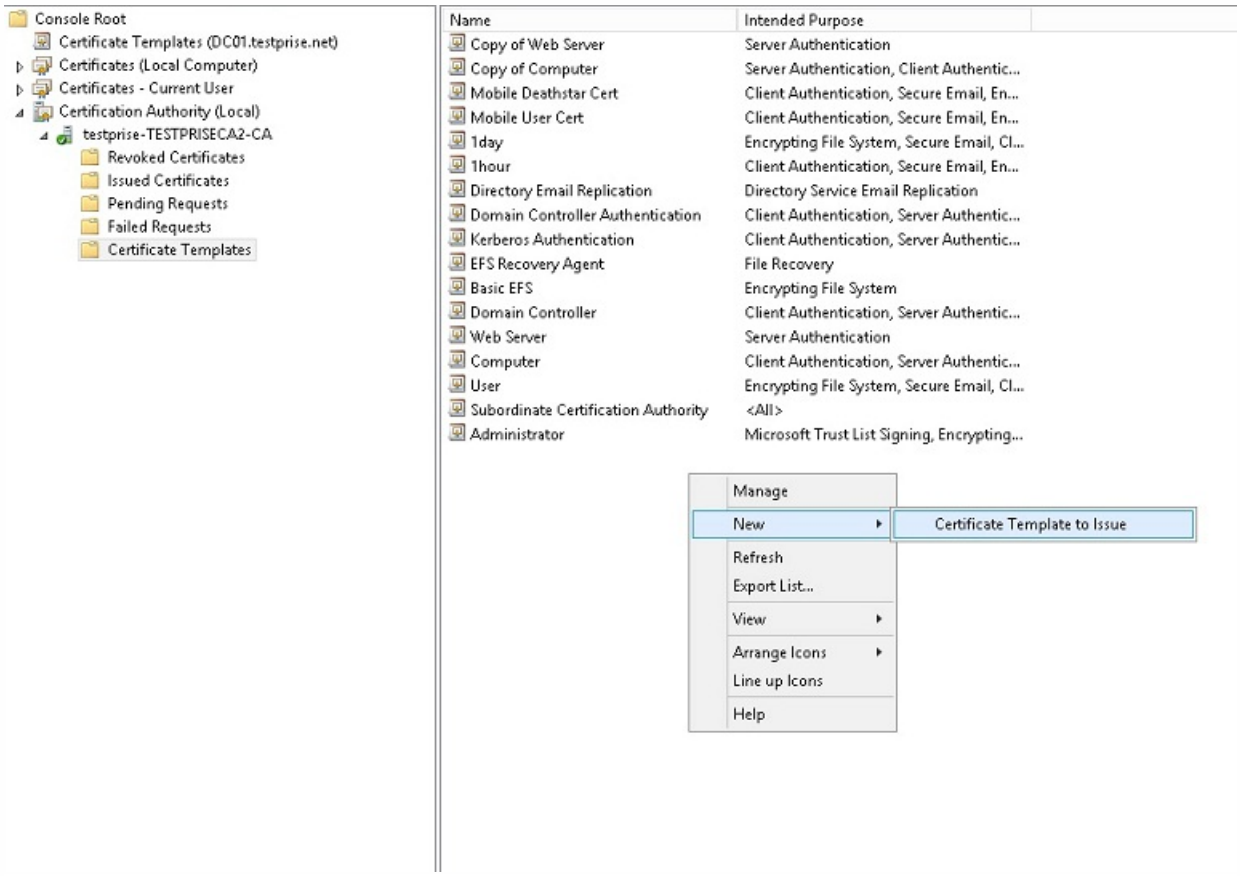
9. Sous **Nom du sujet**, sélectionnez **Fournir dans la demande**. Appliquez les modifications et enregistrez.



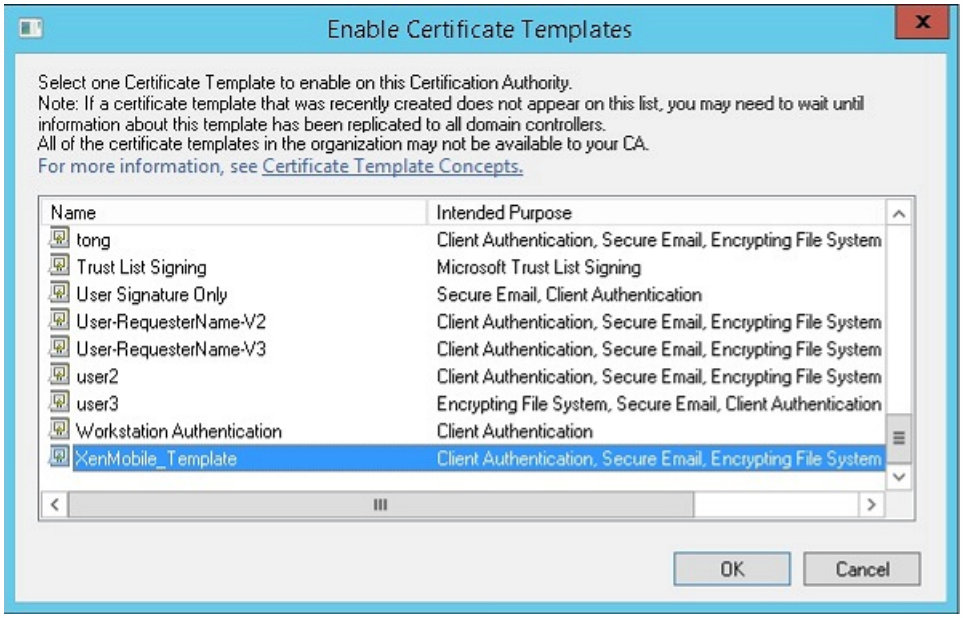
Ajout du modèle à l'autorité de certification (CA)

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**.

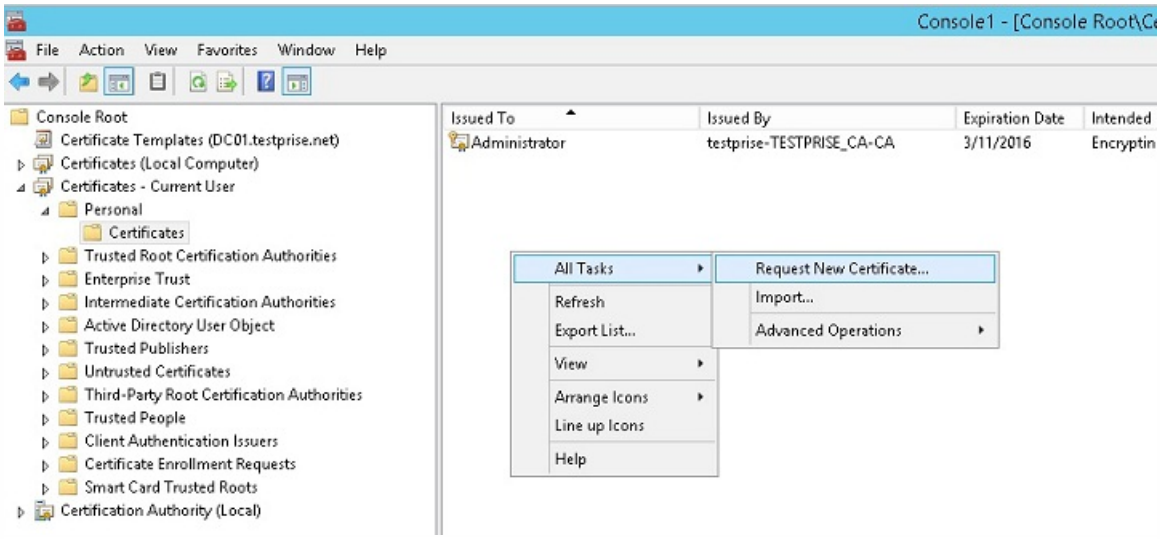


Création d'un certificat PFX depuis le serveur CA

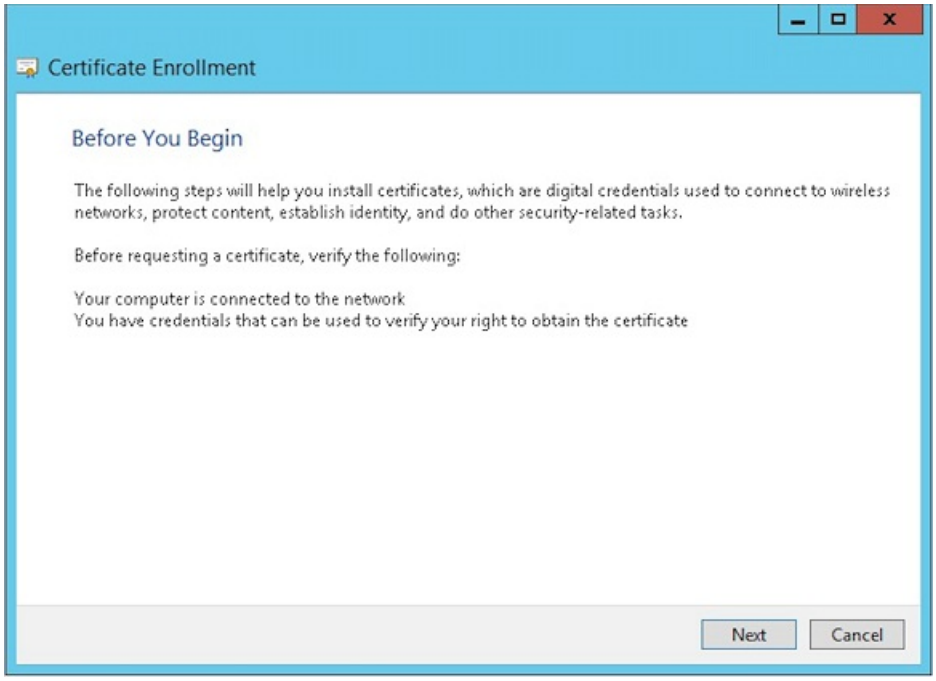
1. Créez un certificat utilisateur .pfx à l'aide du compte de service avec lequel vous vous êtes connecté. Ce fichier .pfx sera chargé dans XenMobile, qui demandera un certificat utilisateur de la part des utilisateurs qui inscrivent leurs appareils.

2. Sous **Utilisateur actuel**, développez **Certificats**.

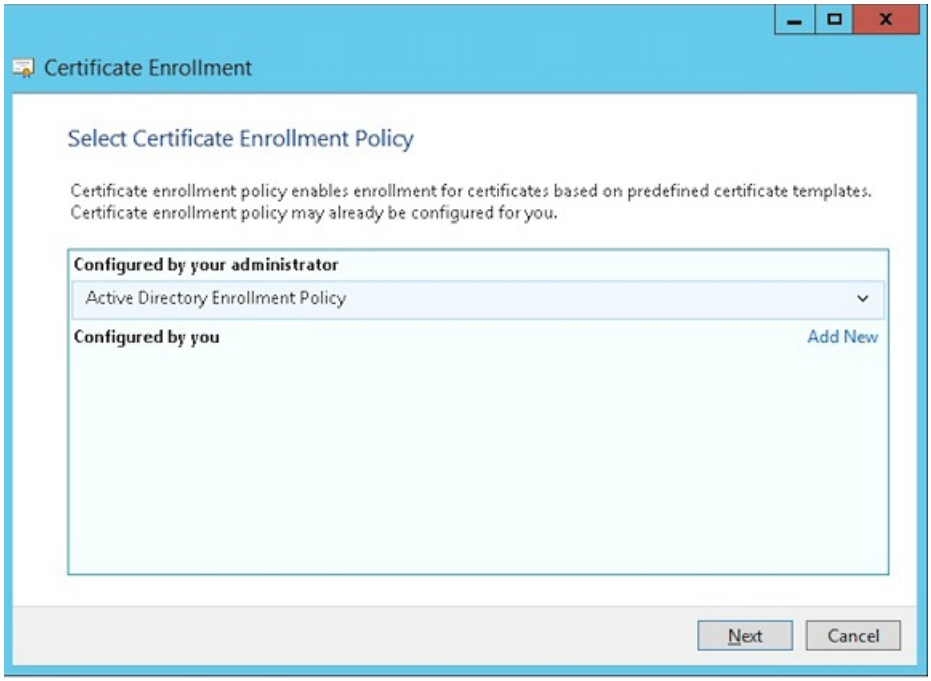
3. Cliquez avec le bouton droit dans le panneau de droite et cliquez sur **Demander un nouveau certificat**.



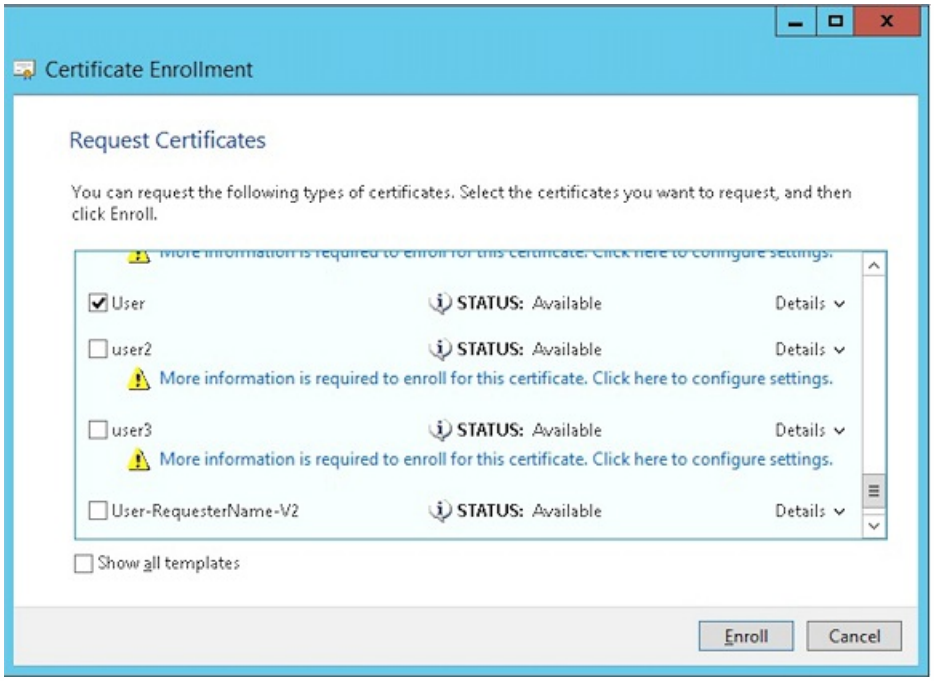
4. L'écran **Inscription de certificats** s'affiche. Cliquez sur **Suivant**.



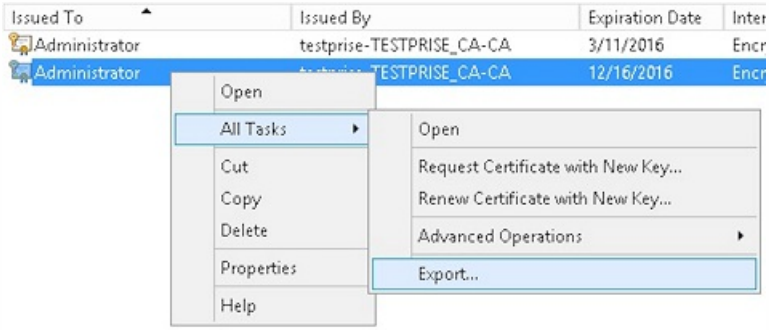
5. Sélectionnez **Stratégie d'inscription à Active Directory** et cliquez sur **Suivant**.



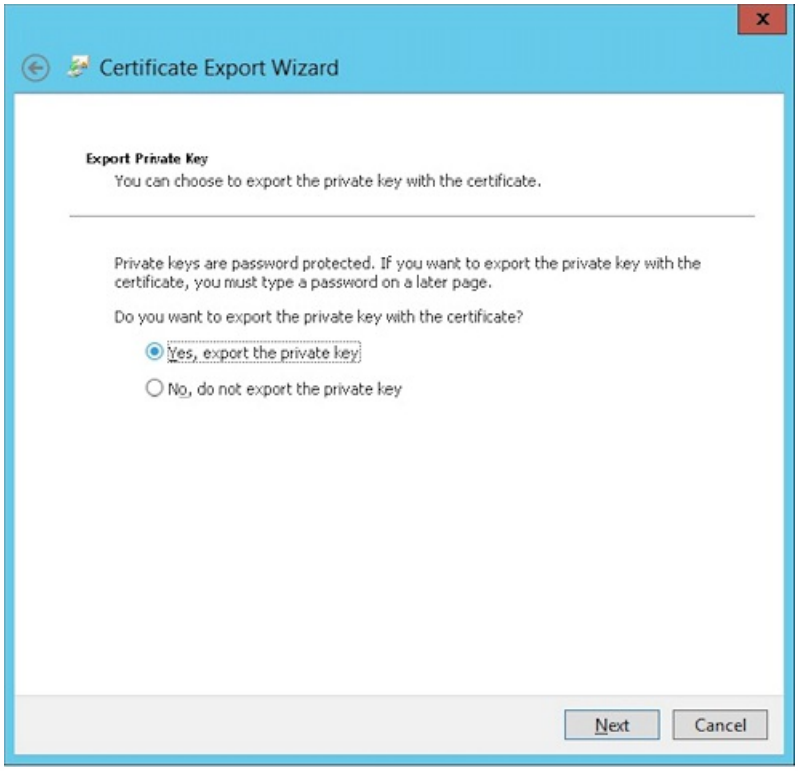
6. Sélectionnez le modèle **Utilisateur** et cliquez sur **Inscrire**.



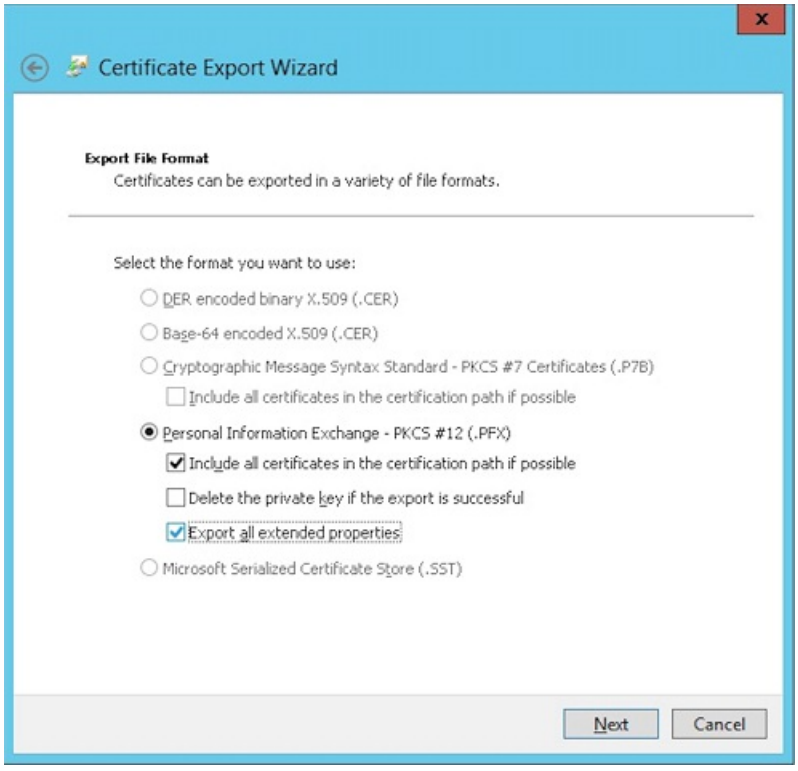
7. Exportez le fichier .pfx que vous avez créé à l'étape précédente.



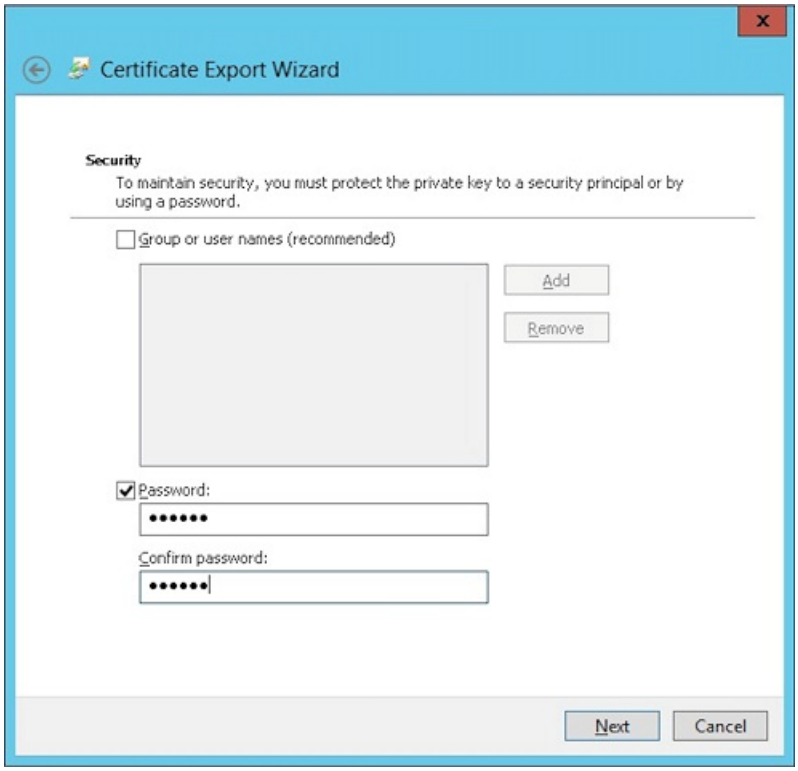
8. Cliquez sur **Oui, exporter la clé privée**.



Sélectionnez les cases **Si possible inclure tous les certificats dans le chemin d'accès de certification si possible** et **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.

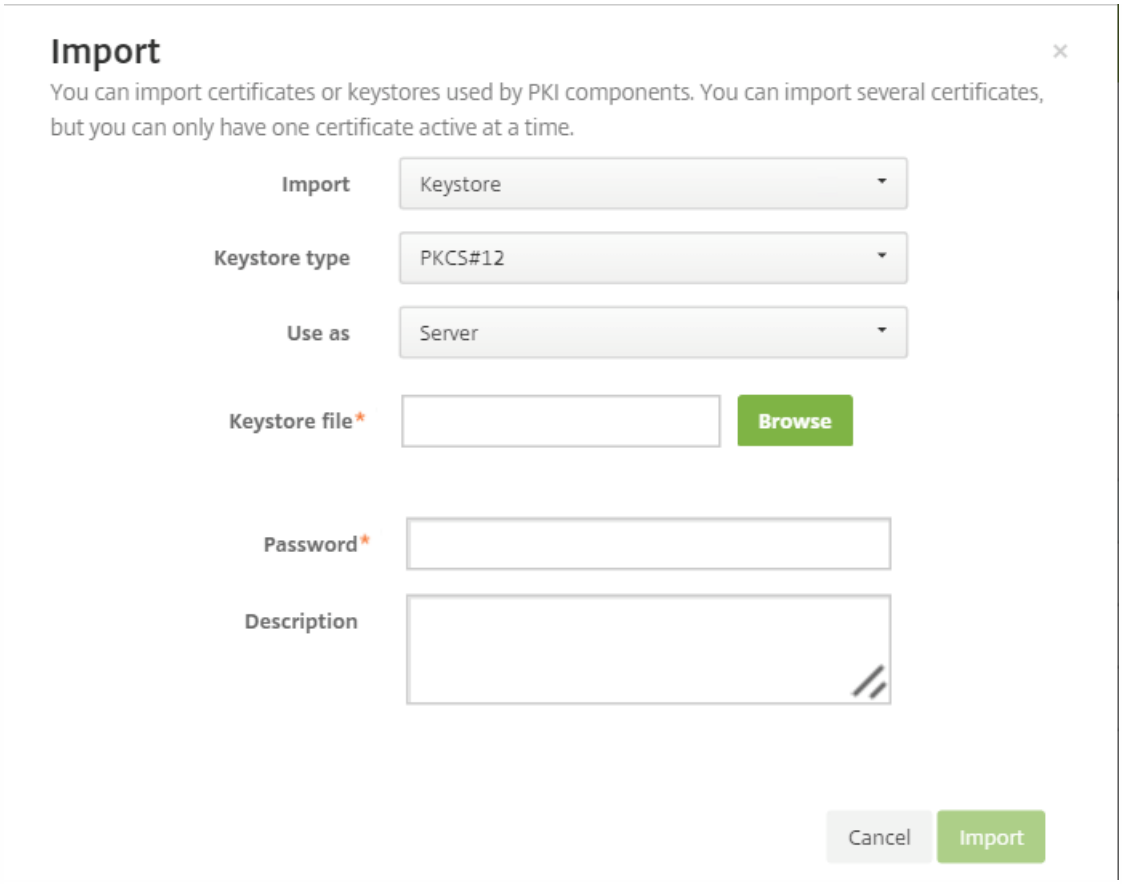
Chargement du certificat sur XenMobile

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 venez de créer.
- **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. Il doit s'afficher en tant que certificat Utilisateur.

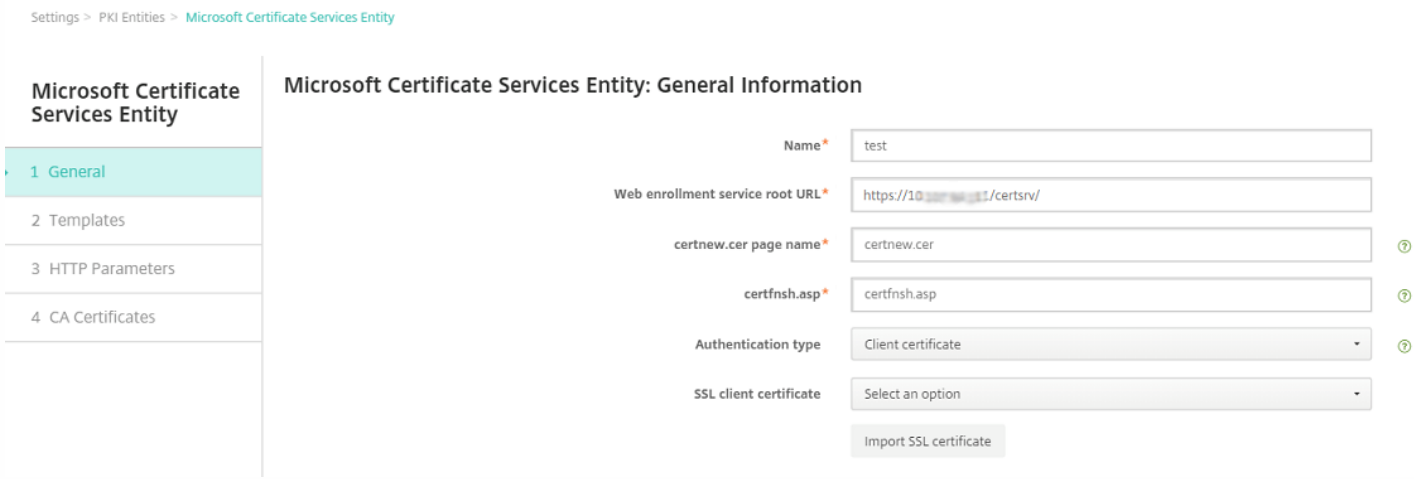
Création de l'entité PKI pour l'authentification par certificat

1. Dans **Paramètres**, accédez à **Plus > Gestion des certificats > Entités PKI**.

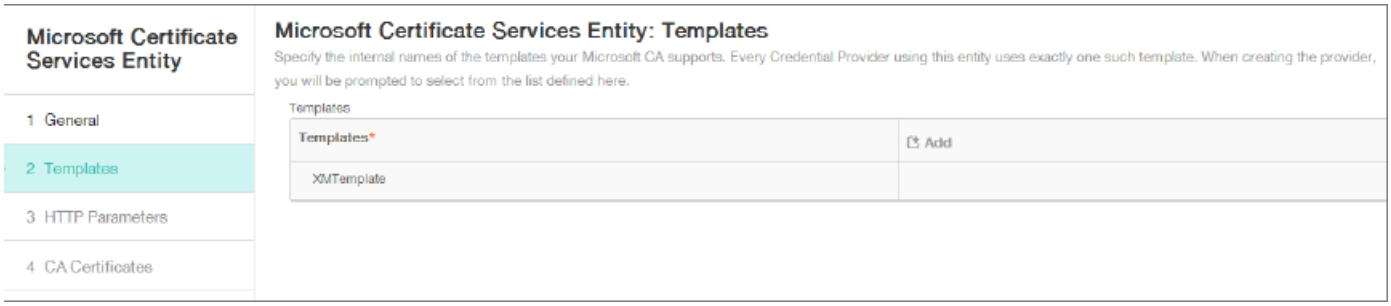
2. Cliquez sur **Ajouter** et sur **Entité Services de certificats Microsoft**. La page **Entité Services de certificats Microsoft : informations générales** s'affiche.

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.

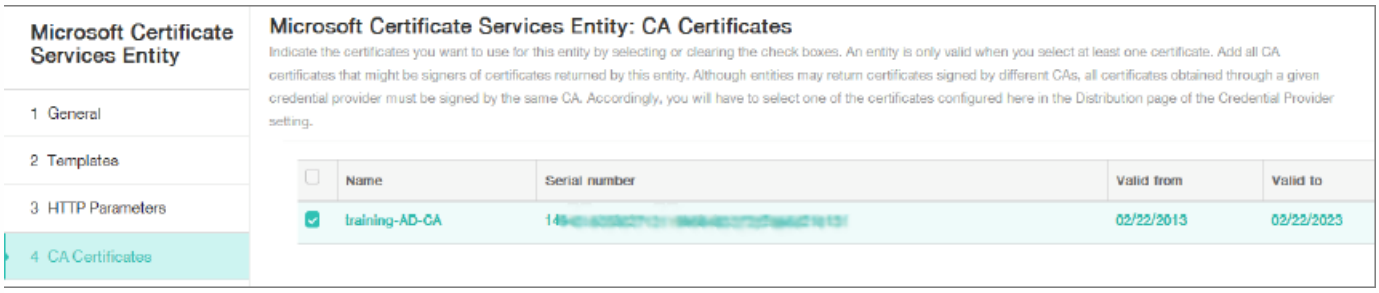


4. Sous **Modèles**, ajoutez le modèle que vous avez créé lors de la configuration du certificat Microsoft. Veillez à ne pas ajouter d'espaces.



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**.

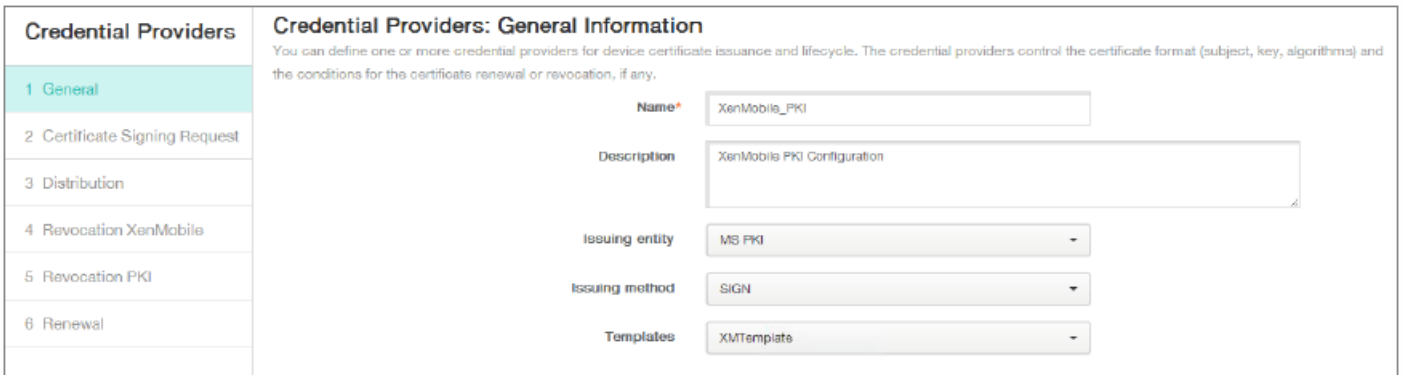
Configuration des fournisseurs d'identités

1. Dans **Paramètres**, accédez à **Plus > Gestion des certificats > Fournisseurs d'identités**.

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.

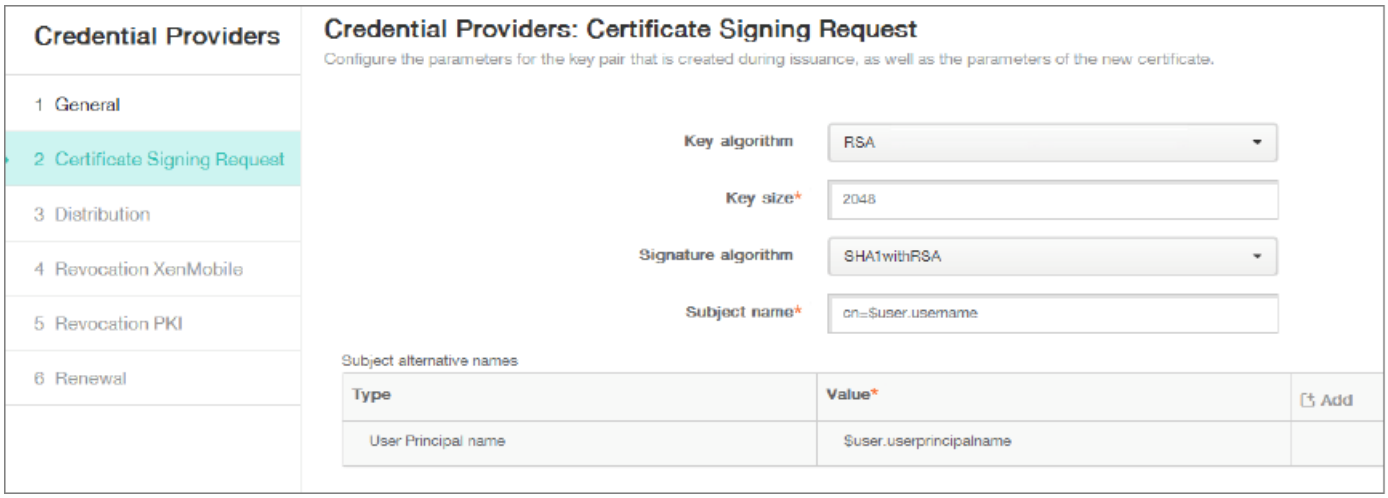


4. Cliquez sur **Demande de signature de certificat** et entrez les paramètres suivants :

- **Algorithme de clé** : RSA
- **Taille de la clé** : 2048
- **Algorithme de signature** : SHA1withRSA
- **Nom du sujet**: cn=$user.username

Pour **Noms de sujet alternatifs**, cliquez sur **Ajouter** et entrez les paramètres suivants :

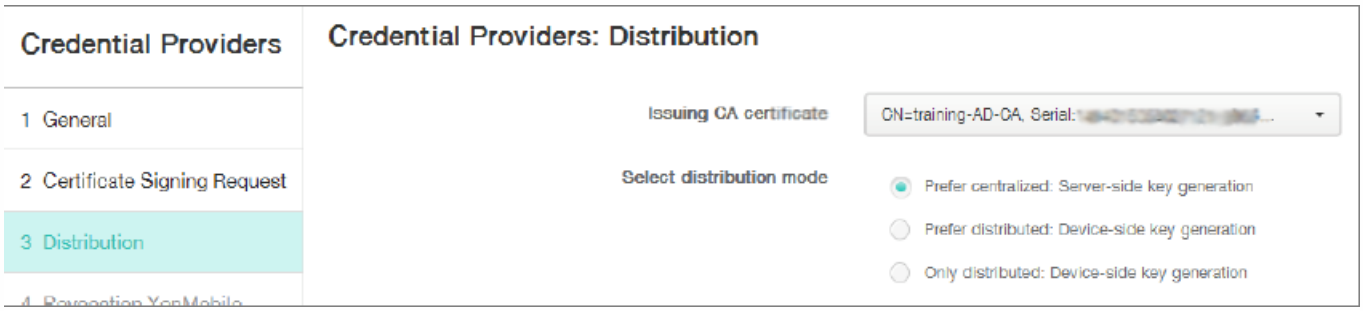
- **Type** : nom principal de l'utilisateur
- **Valeur** : $user.userprincipalname



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**.

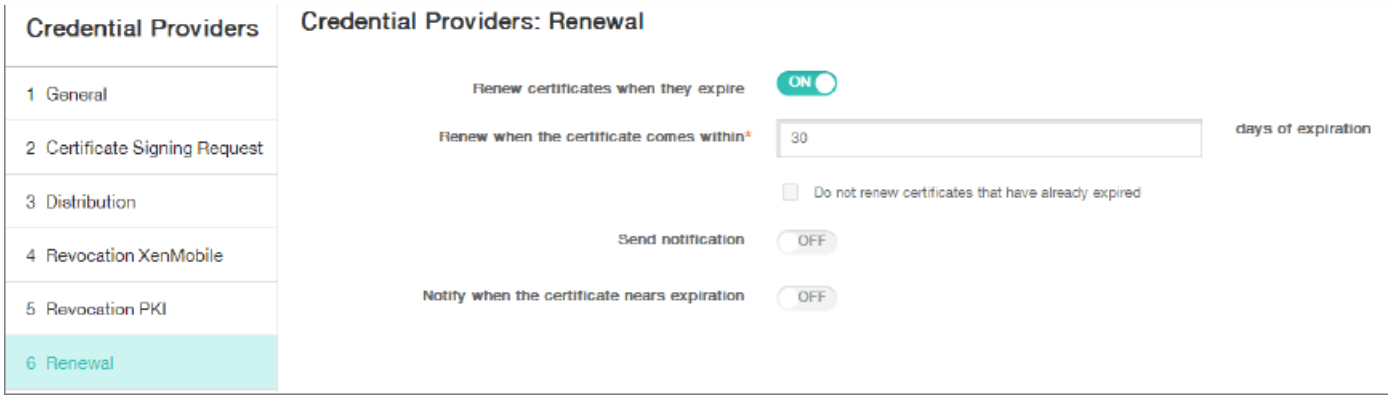


6. Pour les deux prochaines sections -- **Révocation XenMobile** et **Révocation PKI** -- définissez les paramètres comme vous le souhaitez. Pour les besoins de cet article, ces deux options ont été ignorées.

7. Cliquez sur **Renouvellement**.

8. Pour **Renouveler les certificats lorsqu'ils expirent**, sélectionnez **Activé**.

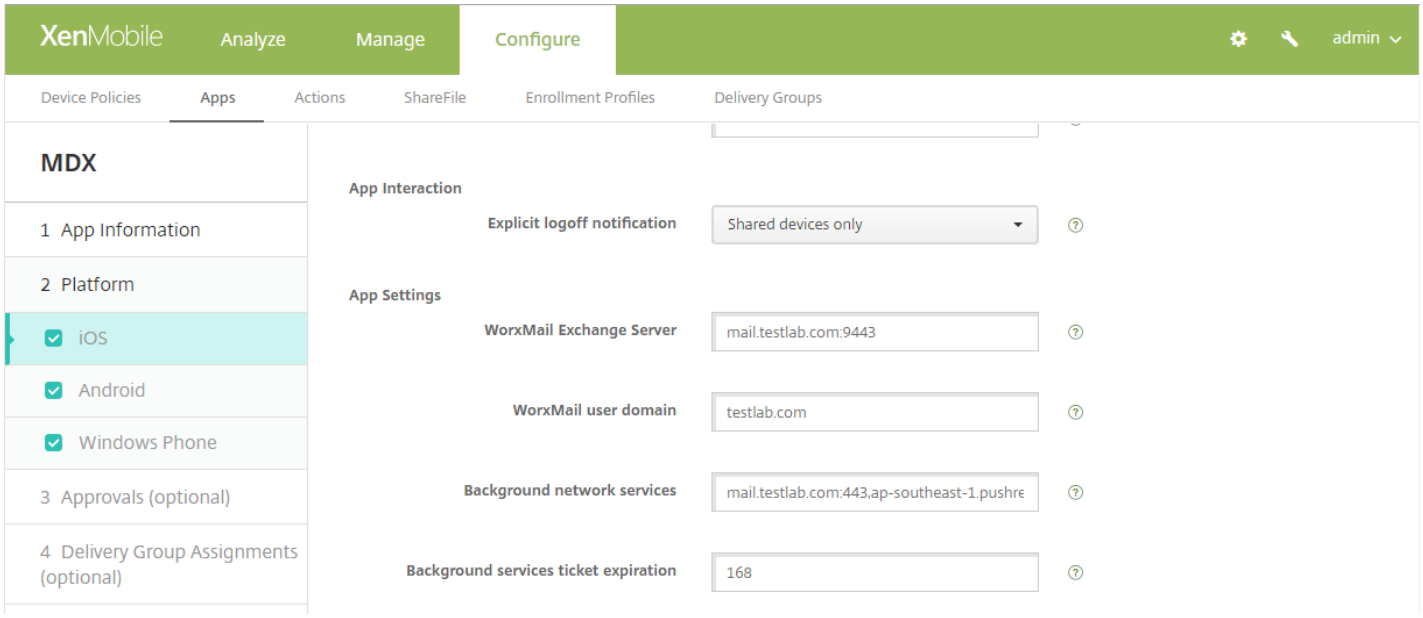
9. Laissez tous les autres paramètres par défaut ou modifiez-les comme vous le souhaitez.



10. Cliquez sur **Enregistrer**.

Configuration de WorxMail pour utiliser l'authentification par certificat

Lorsque vous ajoutez WorxMail à XenMobile, n'oubliez pas de configurer les paramètres Exchange sous **Paramètres applicatifs**.



Configuration de la remise de certificats NetScaler dans XenMobile

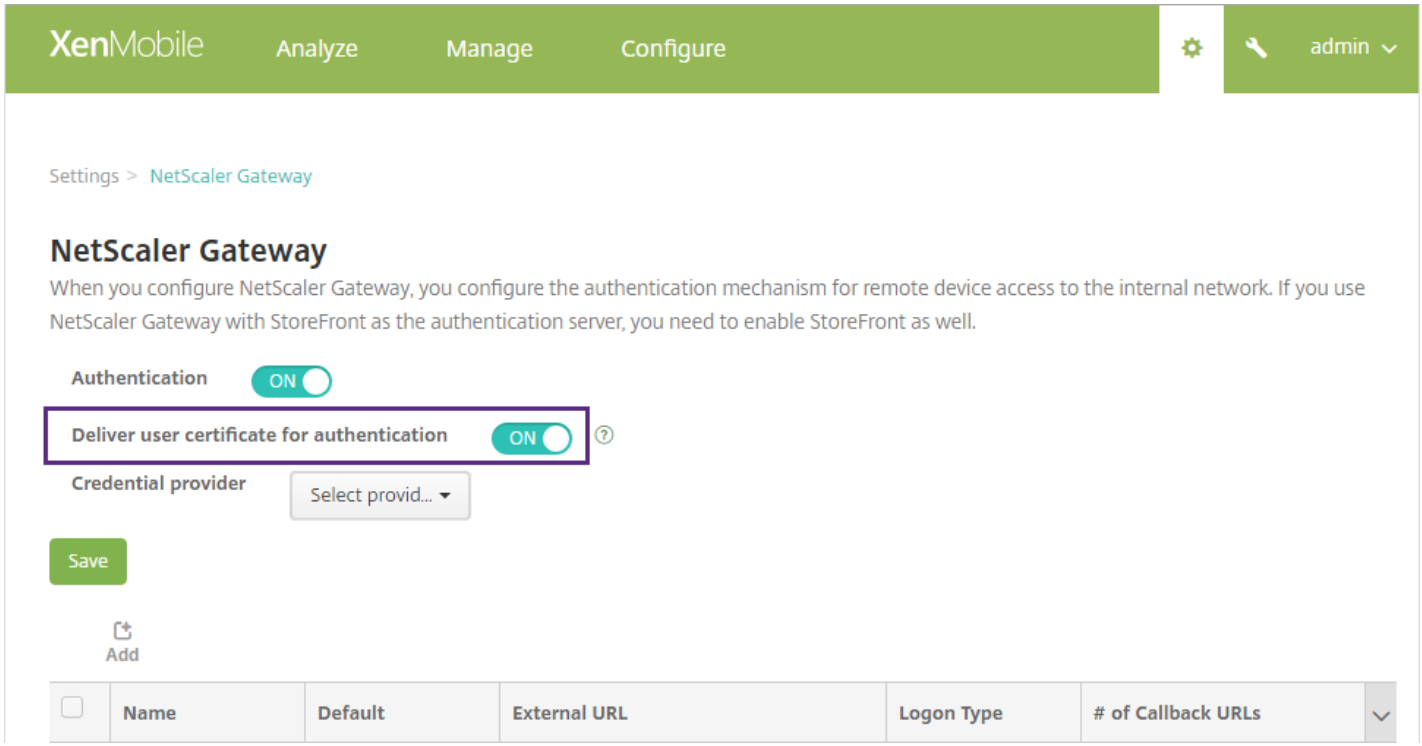
1. Connectez-vous à la console XenMobile et cliquez sur l'icône d'engrenage dans le coin supérieur droit. L'écran **Paramètres** s'affiche.

2. Sous **Serveur**, cliquez sur **NetScaler Gateway**.

3. Si NetScaler Gateway n'est pas déjà ajouté, cliquez sur **Ajouter** et spécifiez les paramètres :

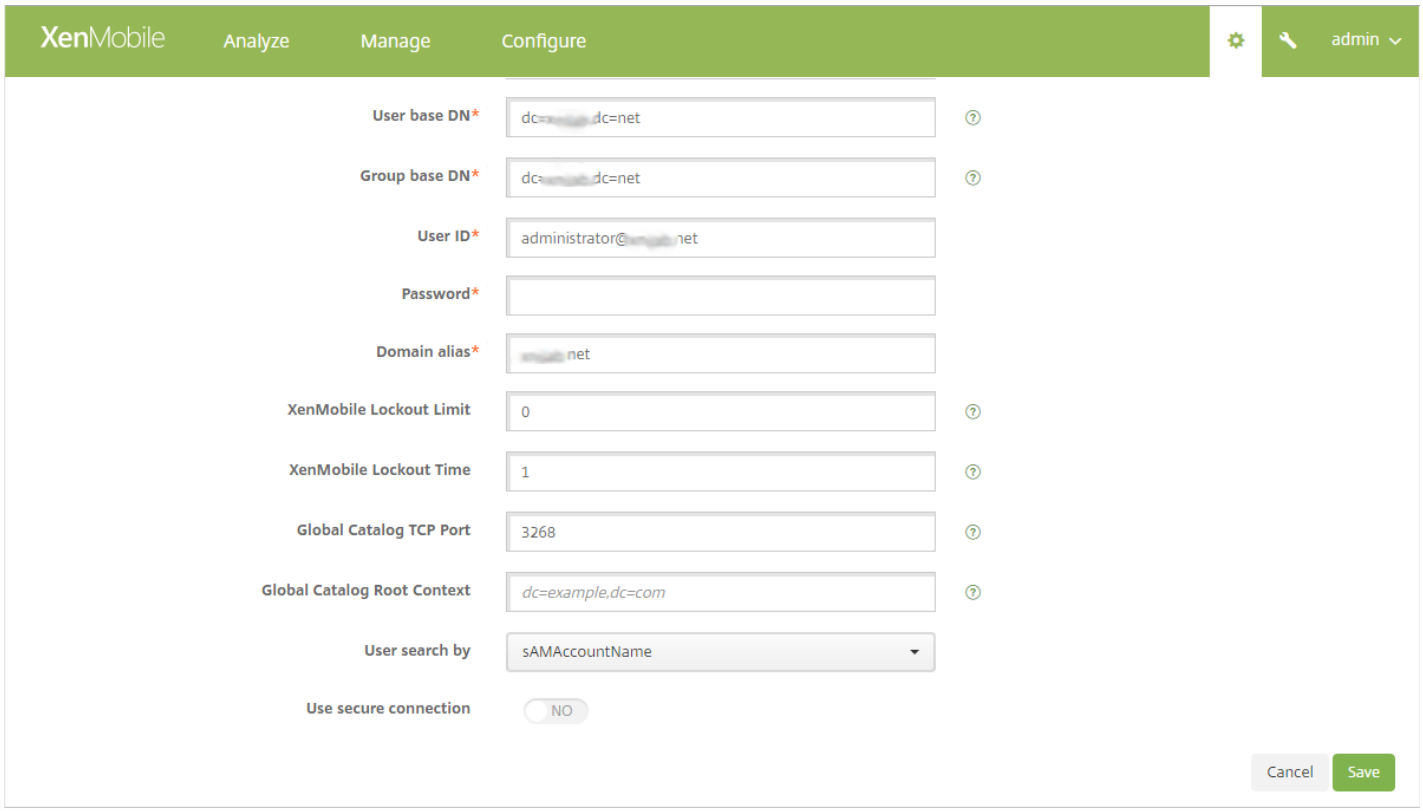
- **URL externe** : https://VotreURLNetScalerGateway
- **Type d'ouverture de session** : Certificat
- **Mot de passe requis** : DÉSACTIVÉ
- **Définir par défaut** : ACTIVÉ

4. Pour **Délivrer un certificat utilisateur pour l'authentification**, sélectionnez **Activé**.



5. Pour **Fournisseur d'identités**, sélectionnez un fournisseur et cliquez sur **Enregistrer**.

6. Si vous utilisez 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**.



Création d'une stratégie d'hub d'entreprise pour Windows Phone 8.1

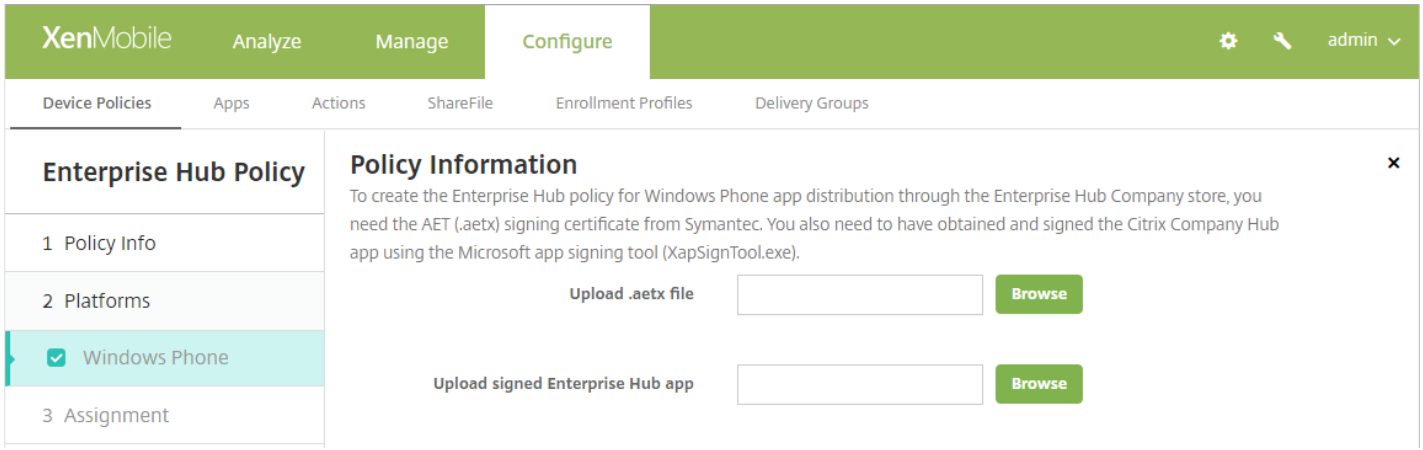
Pour les appareils Windows Phone 8.1, vous devez créer une stratégie d'hub d'entreprise pour délivrer le fichier AETX et le client Worx Home.

> **Remarque**
>
> Assurez-vous que les fichiers AETX et Worx Home utilisent le même certificat d'entreprise que celui du fournisseur de certificats et le même ID d'éditeur que celui du compte de 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 Worx Home signée pour le hub d'entreprise.



4. Attribuez la stratégie à des groupes de mise à disposition et enregistrez-la.

Utilisation de l'assistant de NetScaler pour XenMobile pour configurer NetScaler Gateway pour l'authentification par certificat

> **Remarque**
>
> Vous ne pouvez exécuter l'assistant NetScaler pour XenMobile qu'une seule fois. Si vous avez déjà utilisé l'assistant, suivez les

instructions de la section « Pour configurer manuellement NetScaler Gateway pour l'authentification par certificat » ci-après.

Suivez ces étapes sur votre boîtier NetScaler pour configurer l'authentification par certificat dans XenMobile.

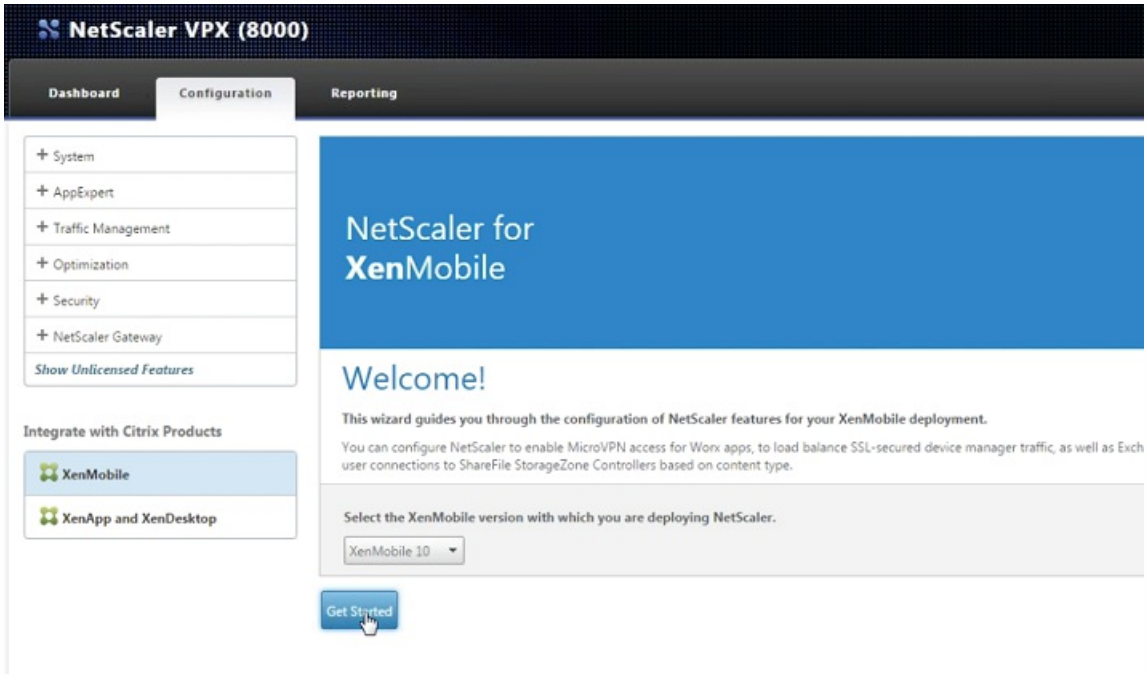
1. Ouvrez une session sur NetScaler.

2. Sous **Configuration**, accédez à **Integrate with Citrix Products**, puis sélectionnez **XenMobile**.

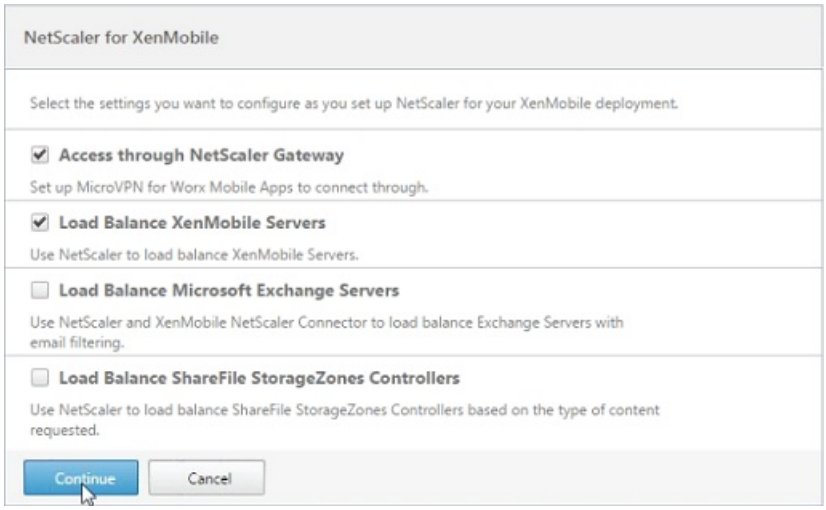
Un assistant destiné à la configuration des fonctionnalités NetScaler pour votre déploiement XenMobile s'ouvre.

3. Choisissez **XenMobile 10**.

4. Cliquez sur **Get Started**.



5. Sur l'écran suivant, sélectionnez **Access through NetScaler Gateway** (pour les modes ENT et MAM) et **Load Balance XenMobile Servers** et cliquez sur **Continue**.



6. Sur l'écran suivant, entrez l'adresse IP externe de NetScaler Gateway, puis cliquez sur **Continue**.

L'écran Server Certificate for NetScaler Gateway s'affiche.

7. Vous devez utiliser un certificat existant ou en installer un. Cliquez sur **Continue**.

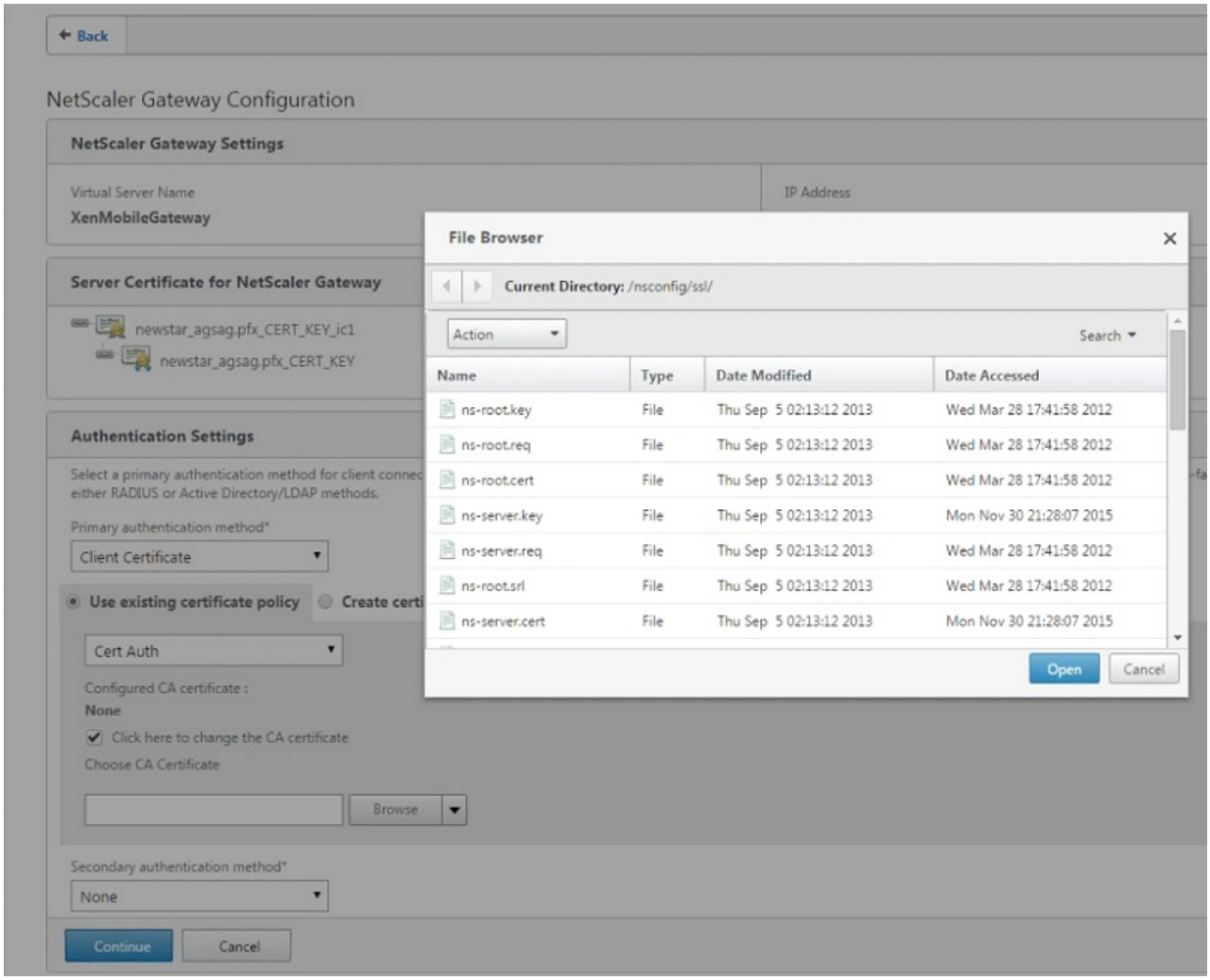
L'écran **Authentication Settings** s'affiche.

8. Dans le champ **Primary authentication method**, sélectionnez **Client Certificate**.

Use existing certificate policy et **Cert Auth** seront automatiquement sélectionnés dans les deux champs suivants. Les étapes suivantes supposent que vous disposez déjà d'une stratégie de certificat.

Si vous avez besoin de créer une stratégie de certificat, cliquez sur **Create certificate policy** et renseignez les paramètres. Sur l'écran **XenMobile Server Certificate**, choisissez un certificat de serveur existant ou installez un nouveau certificat. Si vous exécutez plusieurs serveurs XenMobile, vous devez ajouter un certificat pour chacun d'entre eux. Pour **Server Logon Name Attribute**, spécifiez **userPrincipalName** ou **samAccountName.**

9. Sélectionnez **Click here to change the CA certificate**, puis dans la liste **Browse**, accédez à l'emplacement du certificat de l'autorité de certification de votre choix.



10. Laissez le champ **Second authentication method** définit sur **None**, puis cliquez sur **Continue**.

11. Sur l'écran **Device certificate**, si le certificat n'est pas déjà installé, vous devez exporter ce certificat depuis la console XenMobile. Pour ce faire :

    a. Sur la console, cliquez sur l'icône d'engrenage dans le coin supérieur droit pour ouvrir l'écran **Paramètres**.

    b. Cliquez sur **Certificat**, puis choisissez le certificat de l'autorité de certification dans la liste.

    c. Cliquez sur **Exporter**.

    d. Revenez dans l'assistant NetScaler et sélectionnez le certificat que vous avez exporté (téléchargé) pour l'installer.

    e. Cliquez sur **Continue**.

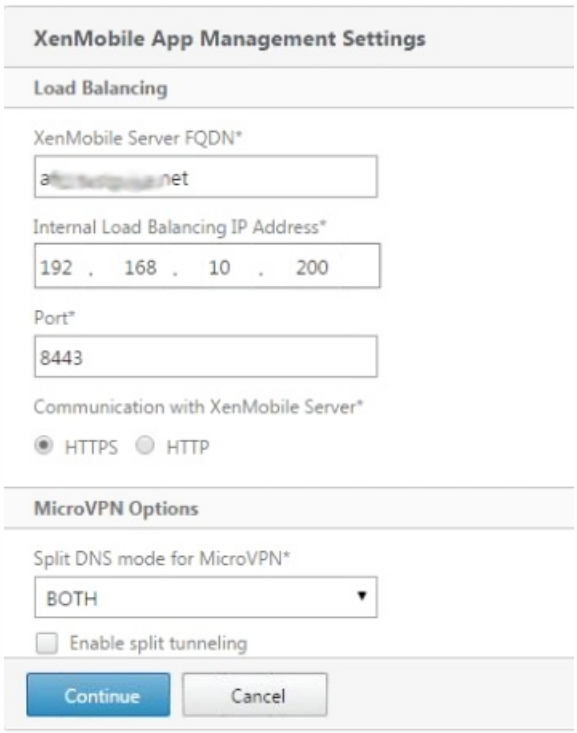
    Les adresses IP du serveur XenMobile que vous avez configurées s'affichent.

12. Sur l'écran **Load Balancing**, entrez le nom de domaine complet (FQDN) du serveur XenMobile et une adresse IP d'équilibrage de charge interne MAM exclusif.

13. Étant donné qu'il s'agit d'un déploiement de déchargement SSL, sélectionnez **HTTP** dans **Communication with XenMobile Server**.

Le champ **Split DNS mode for MicroVPN** indique **BOTH**.

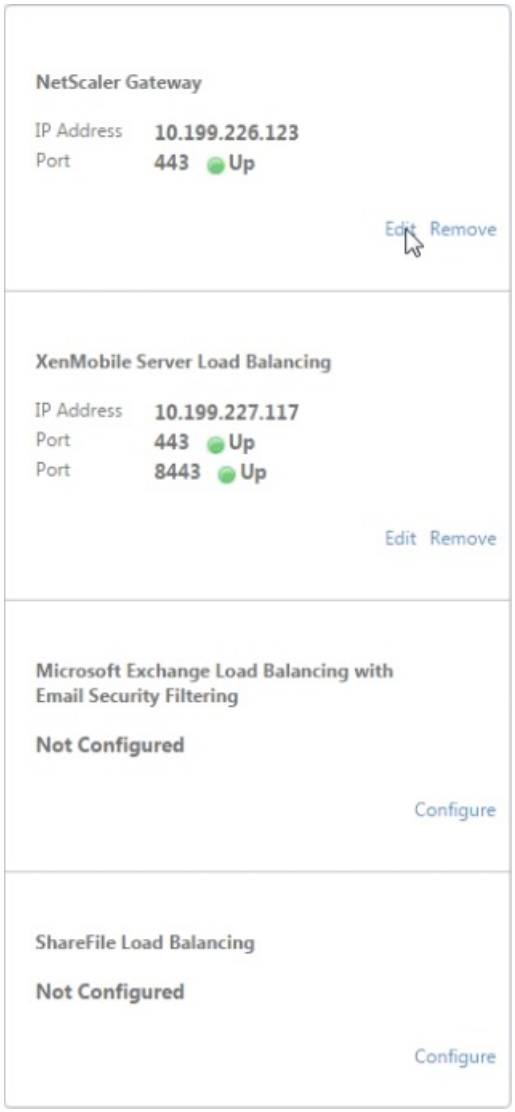
14. Cliquez sur **Continue**.



Les adresses IP du serveur XenMobile que vous avez configurées s'affichent.

15. Cliquez sur **Continue**.

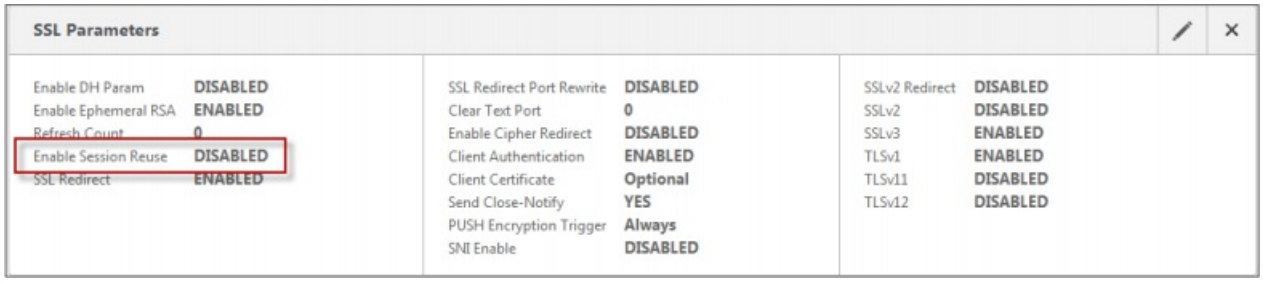
Sur le tableau de bord NetScaler, vérifiez que NetScaler Gateway et l'équilibrage de charge XenMobile sont configurés comme suit :



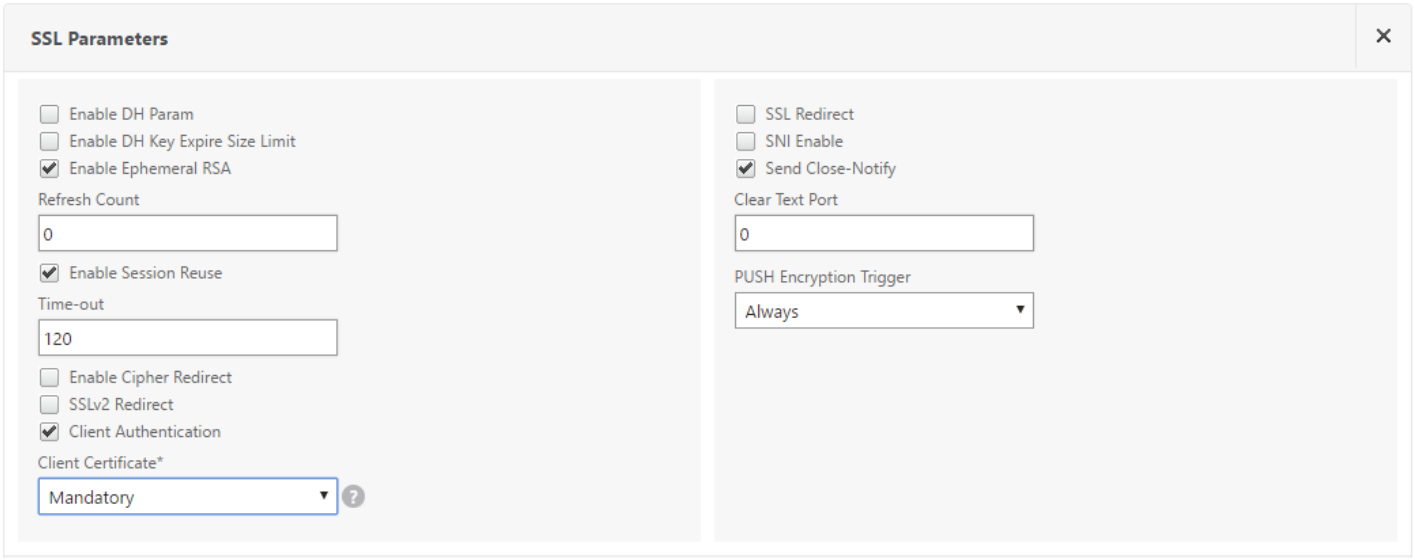
16. Si vous allez utiliser des attributs sAMAccount dans les certificats utilisateur comme une alternative au nom d'utilisateur principal (UPN), configurez le profil de certificat comme décrit dans la section suivante.

Configuration manuelle de NetScaler Gateway pour l'authentification par certificat

1. Sous **Traffic Management > Load Balancing > Virtual Servers**, accédez à chaque serveur virtuel (443 et 8443), mettez à jour **SSL Parameters** et définissez **Enable Session Reuse** sur **DISABLED**.



2. Sur le serveur virtuel NetScaler Gateway, sur **Enable Client Authentication -> Client Certificate**, sélectionnez **Client Authentication** et pour **Client Certificate**, sélectionnez **Mandatory**.



3. Créez une nouvelle stratégie d'authentification par certificat de manière à ce que XenMobile puisse extraire le **User Principal Name** ou le **sAMAccount** provenant du certificat client fourni par Worx Home sur NetScaler Gateway.

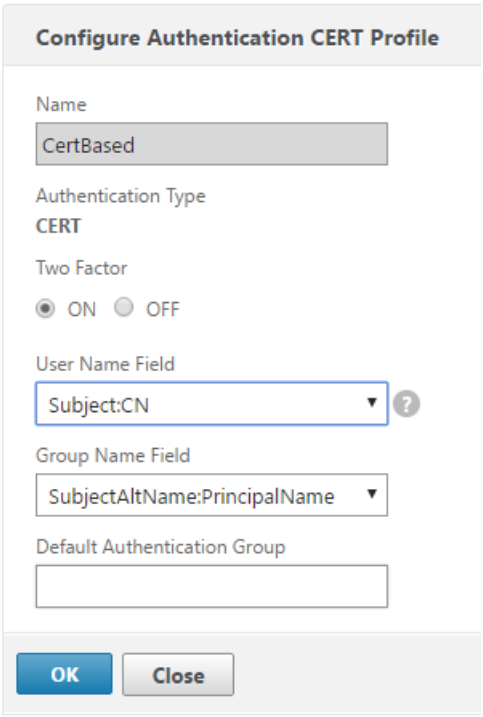
4. Définissez les paramètres suivants pour le profil de certificat :

Type d'authentification : **CERT**

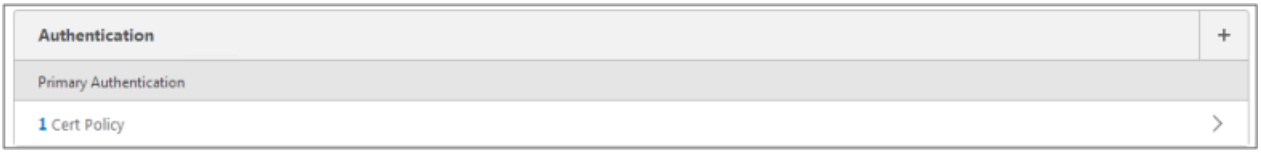
Deux facteurs : **ON** or **OFF**

Champ Nom d'utilisateur : **Subject:CN**

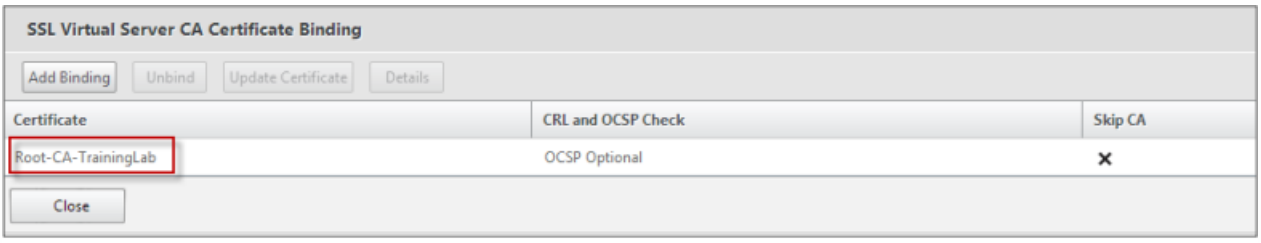
Champ Nom du groupe : **SubjectAltName:PrincipalName**

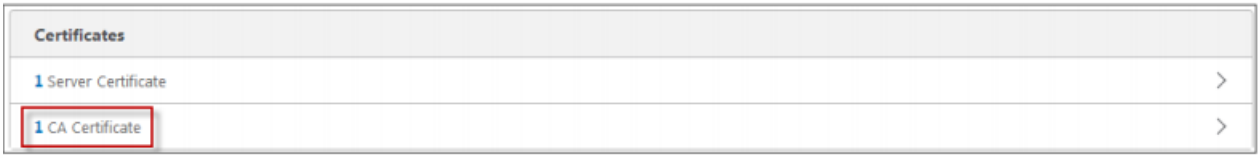


5. Liez uniquement la stratégie d'authentification par certificat en tant qu'**authentification principale** sur le serveur virtuel NetScaler Gateway.



6. Liez le certificat d'autorité de certification racine pour valider l'approbation du certificat client présenté à NetScaler Gateway.





Résolution des problèmes de configuration du

certificat client

Une fois la configuration terminée, 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 Worx.

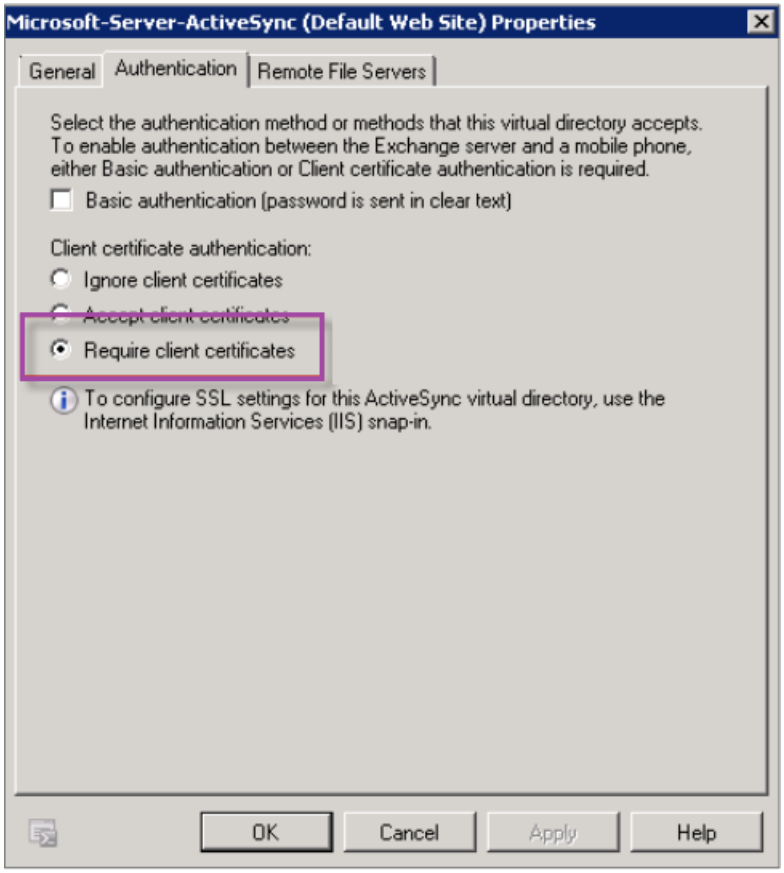
3. Les utilisateurs sont redirigés vers Worx Store.

4. Lorsque les utilisateurs démarrent WorxMail pour iOS, Android ou Windows Phone 8.1, XenMobile ne les invite pas à entrer d'informations d'identification afin de configurer leurs boîtes aux lettres. Au lieu de cela, WorxMail demande le certificat client de Worx Home et l'envoie à Microsoft Exchange Server pour authentification. Si XenMobile invite les utilisateurs à entrer des informations d'identification lorsqu'ils démarrent WorxMail, vérifiez votre configuration.

Si les utilisateurs peuvent télécharger et installer WorxMail, mais que WorxMail ne termine pas la configuration durant la configuration de la boîte aux lettres :

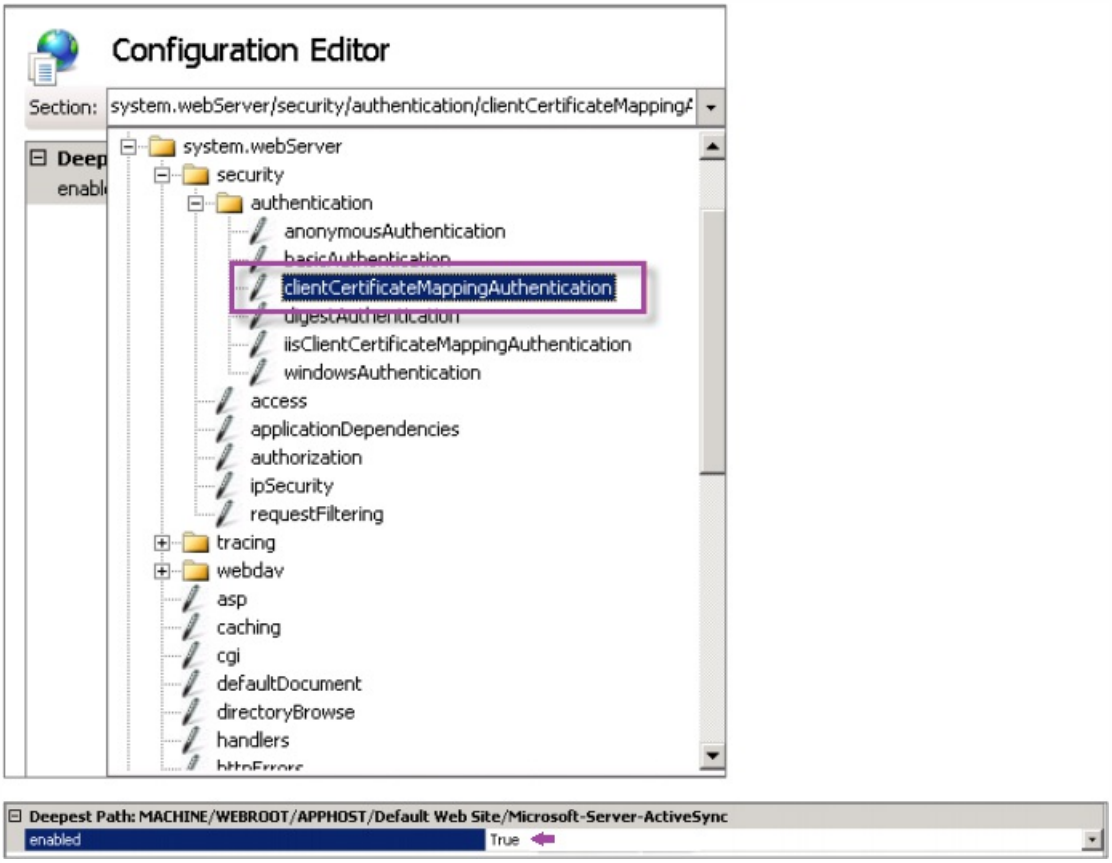
1. Si Microsoft Exchange Server ActiveSync utilise des certificats de serveur SSL privé pour sécuriser le trafic, vérifiez que les certificats racine/intermédiaire sont installés sur l'appareil mobile.

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 activer l'authentification par

mappage de certificat client (elle est désactivée par défaut). L'option figure sous **Éditeur de configuration > Sécurité > Authentification**.



Remarque : après avoir sélectionné **Vrai**, cliquez sur **Appliquer** pour que les modifications prennent effet.

4. Vérifiez les paramètres de NetScaler 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**, comme indiqué précédemment dans « Pour configurer la remise de certificats NetScaler dans XenMobile ».

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 NetScaler 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=609da5df280d1f54a7deb714fb2c5435c94e05da appid={4dc3e181-e14b-4a21-b022-59fc669b0914} certstorename=ExampleCertStoreName 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 WorxMail n'est pas installé correctement sur Windows Phone 8.1 :

- Vérifiez que le fichier de jeton d'inscription d'application (.AETX) est délivré via XenMobile à l'aide de la stratégie d'hub d'entreprise.
- Vérifiez que 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 wrapper WorxMail et signer les applications Worx Home.
- Vérifiez que le même ID d'éditeur est utilisé pour signer et wrapper Worx Home, WorxMail et le jeton d'inscription d'application.

Entités PKI

Oct 17, 2016

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 peuvent être internes à XenMobile, auquel cas ils sont appelés discrétionnaires, ou externes à XenMobile, s'ils font partie de votre infrastructure d'entreprise.

XenMobile prend en charge les types d'entités PKI suivantes :

- Autorités de certification discrétionnaires (CA)
- PKI génériques (GPKI)
- Services de certificats Microsoft

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 :

- signature : émission d'un nouveau certificat, basé sur une demande de signature de certificat (CSR).
- récupération : récupération d'un certificat existant et d'une paire de clés.
- révocation : révocation d'un certificat client.

À propos des certificats CA

Lorsque vous configurez une entité PKI, vous devez informer XenMobile de la nature du certificat d'autorité de certification qui sera le signataire des certificats émis par (ou récupérés depuis) cette entité. Une seule et même entité PKI peut renvoyer (récupérés ou nouvellement signés) des certificats signés par un certain nombre d'autorités de certification différentes. Vous devez fournir 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 discrétionnaire, le certificat est implicitement le certificat de l'autorité de certification de signature, mais pour les entités externes, vous devez le spécifier manuellement.

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 :

- signature: la carte est capable de prendre des demandes de signature de certificat (CSR), de les transmettre à la PKI et de retourner des certificats nouvellement signés.
- récupération : la carte est capable de récupérer des certificats existants et des paires de clés (selon les paramètres d'entrée) depuis la PKI.
- révocation : 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. En d'autres termes, il existe une carte GPKI pour RSA, une autre pour EnTrust, etc.

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 qui sont définis par l'adaptateur GPKI pour une opération spécifique et dont vous avez besoin pour fournir des valeurs à XenMobile. XenMobile détermine les opérations prises en charge par la carte (quelles capacités elle possède) et les paramètres requis par la carte pour chacune des opérations en analysant le fichier WSDL. 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 **Configurer** > **Paramètres** > **Plus** > **Entités PKI**.

2. Sur la page **Entités PKI**, cliquez sur **Ajouter**.

Une liste répertoriant les types de PKI que vous pouvez ajouter 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.
- **Aucun(e)**
- **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.

Remarque : bien que les entités puissent retourner des certificats signés par des autorités de certification différentes, tous les certificats obtenus via un fournisseur de certificats donné doivent être signés par la même autorité de certification. 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.

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).

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.

Pour 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 **Plus** > **Entités PKI**.

2. Sur la page **Entités PKI**, cliquez sur **Ajouter**.

Une liste répertoriant les types de PKI que vous pouvez ajouter 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, procédez comme suit :

- 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.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 : cliquez sur la méthode d'authentification à utiliser.
- Aucun(e)
- HTTP basique : fournissez le nom d'utilisateur et mot de passe requis pour se connecter.
- Certificat client : sélectionnez le certificat client SSL correct.

5. 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'identités, 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 les exigences en matière de modèles des Services de certificats Microsoft, reportez-vous à la documentation Microsoft correspondant à votre version de Microsoft Server. XenMobile n'a aucune exigence en ce qui concerne les

certificats qu'il distribue autre que les formats de certificat indiqués dans Certificats.

6. 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.

7. Cliquez sur **Suivant**.

La page **Entité Services de certificats Microsoft : paramètres HTTP** s'affiche. Sur cette page, spécifiez des paramètres personnalisés que XenMobile doit insérer dans la requête HTTP auprès de l'interface d'inscription Web de Microsoft. Ceci sera utile uniquement si des scripts personnalisés sont exécutés sur l'autorité de certification.

8. 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, il vous sera demandé d'informer XenMobile des signataires des certificats que le système va obtenir par le biais de cette entité. Lorsque votre certificat d'autorité de certification est renouvelé, mettez-le à jour dans XenMobile, puis la modification est appliquée de manière transparente à l'entité.

9. Sur la page **Entité Services de certificats Microsoft : certificats CA**, sélectionnez les certificats que vous voulez utiliser pour cette entité.

10. Cliquez sur **Enregistrer**.

L'entité s'affiche sur le tableau Entités PKI.

Liste de révocation de certificats (CRL) NetScaler

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 NetScaler 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) NetScaler, **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.

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 avez la possibilité d'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, pointant vers le répondeur OCSP interne de XenMobile situé à l'adresse suivante.

`https://serveur/instance/ocsp`

Lors de la configuration du service OCSP, vous devez spécifier 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. Si vous voulez 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 une extension 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).

Pour 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**.

Une liste répertoriant les types de PKI que vous pouvez ajouter 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 > **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 **On**. 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.

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 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.

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 **On**. Cette extension pointe vers le répondeur OCSP de l'autorité de certification sur https://serveur/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

Jul 27, 2016

Les fournisseurs d'identités sont les configurations de certificat réelles que vous utilisez dans différentes parties du système XenMobile. Ils définissent les sources, les paramètres et les cycles de vie de vos certificats, qu'ils fassent partie de configurations d'appareils ou qu'ils soient autonomes, c'est-à-dire transmis tels quels, vers 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, alors 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, et les paramètres de révocation pour D s'appliquent également lorsque C est supprimé ou que D est révoqué.

Dans ce contexte, la configuration du fournisseur d'identités effectue ce qui suit dans XenMobile :

- Détermine la source des certificats.
- Détermine 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.
- Détermine 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, le nom unique, les extensions de certificat, etc.
- Détermine la façon dont les certificats sont mis à disposition sur l'appareil.
- Détermine 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 lorsque la configuration d'appareil associé 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 ; en d'autres termes, sa révocation dans XenMobile peut provoquer sa révocation sur la PKI.
- Détermine les paramètres de renouvellement. Les certificats obtenus via un fournisseur d’identités peuvent être automatiquement renouvelés lors de leur expiration, ou des notifications peuvent être émises lorsque cette expiration approche.

La mesure dans laquelle les différentes options de configuration sont disponibles 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 :

- Signature. 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).
- Récupération. 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 même 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, et doit prouver au client qu'il possède l'autorité d'agir en tant que tel. Cette autorité est établie en offrant à XenMobile les 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. Chaque fournisseur d'identités peut être configuré 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 8	Non	Non

Contexte	SCEP pris en charge	SCEP requis
Configuration de Windows Phone	Non	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. Ce statut est pris en compte lorsque XenMobile évalue un certificat qui lui est présenté, ou lorsque XenMobile doit fournir des informations sur le statut du protocole OCSP pour certains certificats. 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 obtenus auprès du fournisseur de certificats doivent être 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 la 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 conjointement. La révocation interne est provoquée soit par une révocation externe, soit par des observations indépendantes, et à son tour, la révocation interne entraîne 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.

Notez que XenMobile tente tout d'abord d'obtenir le nouveau certificat avant de révoquer le certificat précédent, afin d'éviter une discontinuité du service si l'émission échoue. Si une mise à disposition distribuée (prise en charge par SCEP) est utilisée, la révocation se produit une fois que le certificat a été correctement installé sur l'appareil, sinon la révocation se produit avant que le certificat ne soit envoyé à l'appareil et indépendamment de la réussite ou de l'échec de son installation.

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 c'est le cas, un renouvellement est tenté.

Pour 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 un fournisseur d'identités qui utilise une entité interne, telle que discrétionnaire, et un fournisseur d'identités qui utilise une entité externe, telle que Microsoft CA ou GPKI. La méthode d'émission pour une entité discrétionnaire est toujours signature,ce qui 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.

1. Dans la console Web XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Plus** > **Fournisseurs d'identités**.

2. Sur la page **Fournisseurs d'identités**, cliquez sur **Ajouter**.

La page **Fournisseurs d'identités : informations générales** s'affiche.

3. Sur la page **Fournisseurs d'identités : 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 dans le futur pour vous aider à vous souvenir 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 du certificat client, utilisez **Signer**.
- Si la liste des modèles est disponible, sélectionnez un modèle pour le fournisseur d'identités.

4. Cliquez sur **Suivant**.

Remarque : ces modèles deviennent disponibles lorsque les entités Services de certificats Microsoft sont ajoutées sur **Paramètres** > **Plus** > **Entités PKI**.

La page **Fournisseur d'identités : demande de signature de certificat** s'affiche.

5. Sur la page **Fournisseur d'identités : demande de signature de certificat**, procédez comme suit :

- **Algorithme de clé** : cliquez sur 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. Il s'agit d'un champ obligatoire.
  Remarque : 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 dépendront 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** : entrez le nom unique (DN) du sujet du nouveau certificat. Par exemple : CN=${user.username}, OU=${user.department}, O=${user.companyname},C=${user.c}\endquotation. Il s'agit d'un champ obligatoire.

  Par exemple, pour l'authentification du certificat client, utilisez ces paramètres :

  Algorithme de clé : RSA
  Taille de la clé : 2048
  Algorithme de signature : SHA1withRSA
  Nom du sujet: cn=$user.username

6. Pour ajouter une nouvelle 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

Remarque : comme avec le nom du sujet, vous pouvez utiliser les macros XenMobile dans le champ de valeur.

7. Cliquez sur **Suivant**.

La page **Fournisseurs d'identités : distribution** s'affiche.

8. Sur la page **Fournisseurs d'identités : 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 ; il sera présenté ici à des fins de cohérence avec les configurations qui utilisent 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 NetScaler 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.

9. 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.

12. 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 **On** 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 **On** 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.

13. Cliquez sur **Suivant**.

La page **Fournisseurs d'identités : 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.

14. Sur la page **Fournisseurs d'identités : révocation PKI**, procédez comme suit si vous souhaitez révoquer les certificats de la PKI :

- Modifiez le paramètre **Activer les vérifications de révocation externe** sur **On**. 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 nouveau certificat. **Remarque :** vous pouvez utiliser les macros XenMobile pour les valeurs de champ de nom unique. Par 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 **On**.

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.

15. Cliquez sur **Suivant**.

La page **Fournisseurs d'identités : renouvellement** s'affiche. Sur cette page, vous pouvez configurer XenMobile pour effectuer les opérations suivantes :

- Renouveler le certificat et envoyer (facultatif) une notification lorsque cette opération est terminée (notification envoyée 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).

16. Sur la page **Fournisseurs d'identités: renouvellement**, procédez comme suit si vous souhaitez renouveler les certificats lorsqu'ils expirent : Réglez **Renouveler les certificats lorsqu'ils expirent** sur **On**.

Des champs supplémentaires s'affichent.

- 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**. **Remarque :** dans ce cas, « expiré » signifie que la date NotAfter (fin de validité) du certificat est dans le passé, et non pas qu'il a été révoqué. XenMobile ne renouvellera pas les certificats une fois qu'ils ont été révoqués en interne.

17. Si vous voulez que XenMobile envoie une notification lorsque le certificat a été renouvelé, définissez **Envoyer une**

notification sur **On**. 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.

18. Si vous voulez que XenMobile envoie une notification lorsque la certification arrive à échéance, définissez **Notifier quand un certificat va expirer** sur **On**. 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.

19. 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.

20. Cliquez sur **Enregistrer**.

Le fournisseur d'identités est ajouté à la table Fournisseur d'identités.

Faire une demande de certificat APNS

Jul 27, 2016

Pour inscrire et gérer des appareils iOS avec XenMobile, vous devez configurer et créer un certificat Apple Push Notification Service (APNS). Cette section présente les étapes de base à suivre pour demander le certificat APNS :

- Utiliser un serveur Windows 2012 R2 ou Windows 2008 R2 et Microsoft Internet Information Server (IIS) ou un ordinateur Mac pour générer une demande de signature de certificat (CSR).
- Faire signer la demande de signature de certificat (CSR) par Citrix.
- Demander un certificat APNS à Apple.
- Importer le certificat dans XenMobile.

Remarque :

- Le certificat APNS d'Apple permet de gérer les appareils mobiles via le réseau Apple Push Network. 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 devrez peut-être intervenir en raison de la migration des certificats existants vers le portail Apple Push Certificats Portal.

Les rubriques expliquant les procédures détaillées sont répertoriées par ordre dans cette section comme suit :

Étape 1	Créer une demande de signature de certificat dans IIS Créer une demande de signature de certificat sur un Mac	Générez une demande de signature de certificat avec un serveur Windows 2012 R2 ou Windows 2008 R2 et Microsoft IIS ou sur un ordinateur Mac. Citrix recommande cette méthode.
Étape 2	Pour signer la CSR	Envoyez la CSR à Citrix sur le site Web XenMobile APNs CSR Signing (un ID MyCitrix est requis). 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.
Étape 3	Soumettre la demande de signature de certificat (CSR) signée à Apple	Envoyez la demande de signature de certificat (CSR) signée à Apple sur le portail Apple Push certificat Portal (Apple ID obligatoire), puis téléchargez le certificat APNS d'Apple.
Étape 4	Pour créer un certificat APNS .pfx avec Microsoft IIS Pour créer un certificat APNS .pfx sur un Mac Créer un certificat	Exporter le certificat APN comme certificat PCKS #12 (.pfx) (sur IIS, Mac ou SSL).

	APNS .pfx en utilisant OpenSSL	
Étape 5	Importer un certificat APNS dans XenMobile	Importez le certificat dans XenMobile.

Informations de migration du certificat Push MDM Apple

Les certificats push MDM (gestion des appareils mobiles) créés dans le iOS Developer Enterprise Program ont été migrés vers le portail Apple Push Certificats Portal. Cette migration affecte la création de nouveaux certificats push MDM, ainsi que le renouvellement, la révocation et le téléchargement de certificats push MDM existants. La migration n'affecte pas les autres certificats APNS (non MDM).

Si votre certificat push MDM a été créé dans le iOS Developer Enterprise Program, les situations suivantes s'appliquent :

- Le certificat a été migré automatiquement pour vous.
- Vous pouvez renouveler le certificat dans le portail Apple Push Certificats Portal sans affecter vos utilisateurs.
- Vous devez utiliser le programme iOS Developer Enterprise Program pour révoquer ou télécharger un certificat préexistant.

Si aucun de vos certificats push MDM n'est proche de l'expiration, vous n'avez rien à faire. Si vous disposez d'un certificat push MDM dont l'expiration est proche, contactez le fournisseur de votre solution MDM. Ensuite, demandez à votre iOS Developer Program Agent de se connecter au portail Apple Push Certificates Portal avec son Apple ID.

Tous les nouveaux certificats push MDM doivent être créés dans le portail Apple Push Certificats Portal. Le programme iOS Developer Enterprise Program n'autorisera plus la création d'un Apple ID avec un identificateur de bundle (section APNS) contenant com.apple.mgmt.

Remarque : vous devez conserver l'Apple ID utilisé pour créer le certificat. En outre, l'Apple ID doit être un ID d'entreprise et non un ID personnel.

Pour créer une demande de signature de certificat à l'aide de Microsoft IIS

La première étape de génération d'une demande de certificat APNS pour les appareils iOS consiste à créer une demande de signature de certificat (CSR). Sur un serveur Windows 2012 R2 où Windows 2008 R2, vous pouvez générer une demande de signature de certificat 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**.

Pour créer une demande de signature de certificat sur un Mac

1. Sur un Mac exécutant Mac OS X, sous **Applications** > **Utilitaires**, démarrez l'application Trousseau d'accès.
2. Ouvrez le menu **Trousseau d'accès** et cliquez sur **Préférences**.

3. Cliquez sur l'onglet **Certificats**, définissez les options **OCSP** et **CRL** sur **Désactivé**, puis fermez la fenêtre Préférences.
4. Dans le menu **Trousseau d'accès**, cliquez sur **Assistant de certification** > **Demander un certificat à une autorité de certification**.
5. L'Assistant de certification vous invite à entrer les informations suivantes :
   1. **Adresse e-mail**. Adresse de messagerie de la personne ou du compte de rôle qui est responsable de la gestion du certificat.
   2. **Nom commun**. Nom commun de la personne ou compte de rôle qui est responsable de la gestion du certificat.
   3. **Adresse e-mail de l'AC**. Adresse de messagerie de l'autorité de certification.
6. Sélectionnez **Enregistrée sur le disque** et **Me laisser indiquer les informations sur la bi-clé** et cliquez sur **Continuer**.
7. Entrez un nom pour le fichier CSR, enregistrez le fichier sur votre ordinateur, puis cliquez sur **Enregistrer**.
8. 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.
9. Cliquez sur **Terminé** lorsque l'Assistant de certification termine le processus de demande de signature de certificat.

Pour créer une demande de signature de certificat avec OpenSSL

Si vous ne pouvez pas utiliser un serveur Windows 2012 R2 ou Windows 2008 R2 et Microsoft Internet Information Server (IIS) ou un ordinateur Mac pour générer une demande de signature de certificat (CSR) à soumettre à Apple afin d'obtenir le certificat Apple Push Notification Service (APNS), vous pouvez utiliser OpenSSL.

Remarque : pour pouvoir utiliser OpenSSL pour créer une demande de signature de certificat, vous devez 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.
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.

   Country Name (2 letter code) [AU]:FR
   State or Province Name (full name) [Some-State]:Province
   Locality Name (eg, city) []:Paris
   Organization Name (eg, company) [Internet Widgits Pty Ltd]:Citrix
   Organizational Unit Name (eg, section) []:Marketing
   Common Name (eg, YOUR name) []:Guillaume Martin
   Email Address []:guillaume.martin@client.com

3. Dans le message suivant, entrez un mot de passe pour la clé privée de la demande de signature de certificat.
   Please enter the following 'extra' attributes
   to be sent with your certificate request
   A challenge password []:
   An optional company name []:

4. Envoyez la demande de signature de certificat à Citrix.

Citrix prépare la demande de signature de certificat (CSR) signée et renvoie le fichier par courrier électronique.

Pour signer la CSR

Avant d'envoyer le certificat à Apple, ce dernier doit être signé par Citrix de façon à pouvoir être utilisé avec XenMobile.

1. Dans votre navigateur, accédez au site Web XenMobile APNs CSR Signing.
2. Cliquez sur **Upload the CSR**.
3. Localisez et sélectionnez le certificat.
   Remarque : le certificat doit être au format .pem/txt.
4. Sur la page XenMobile APNs CSR Signing, cliquez sur **Sign**. La CSR est signée et automatiquement enregistrée sur votre dossier de téléchargement configuré.

Pour soumettre la demande de signature de certificat (CSR) à Apple afin d'obtenir le certificat APNS

Après la réception de votre demande de signature de certificat (CSR) signée de Citrix, vous devez la soumettre à Apple pour obtenir le certificat APNS.

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 (http://developer.apple.com/devcenter/ios/index.action) avant d'accéder au lien identity.apple.com dans l'étape 1.

1. Dans un navigateur, accédez à https://identity.apple.com/pushcert.
2. Cliquez sur **Create a Certificate**.
3. Si c'est 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 CSR signée, accédez à la demande sur votre ordinateur, puis cliquez sur **Upload**. Un message de confirmation doit s'afficher indiquant que le chargement a réussi.
5. Cliquez sur **Download** pour récupérer le certificat .pem.
   Remarque : si vous utilisez Internet Explorer et que l'extension de fichier est manquante, cliquez sur **Cancel** à deux reprises puis sur Download dans la fenêtre suivante.

Pour créer un certificat APNS .pfx avec Microsoft IIS

Pour utiliser le certificat APNS d'Apple avec XenMobile, vous devez effectuer la demande de certificat dans Microsoft IIS, exporter le certificat comme fichier PCKS #12 (.pfx), puis importer le certificat APNS dans XenMobile.

Important : pour cette tâche, vous devez utiliser le même serveur IIS que le serveur utilisé pour générer la CSR.

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**.
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**.
   Remarque : vous devez fournir le mot de passe pour le certificat au cours de l'installation de XenMobile.
7. Copiez le certificat .pfx sur le serveur sur lequel XenMobile sera installé.
8. Ouvrez une session sur la console XenMobile en tant qu'administrateur.

9. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
10. Cliquez sur **Certificats**. La page **Certificats** s'affiche.
11. Cliquez sur **Importer**. La boîte de dialogue **Importer** apparaît.
12. Depuis le menu **Importer**, sélectionnez **Keystore**.
13. Dans **Utiliser en tant que**, choisissez **APNS**.
14. Dans le fichier **keystore**, sélectionnez le fichier de keystore que vous souhaitez importer, en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
15. Dans **Mot de passe**, entrez le mot de passe affecté au certificat.
16. Cliquez sur **Importer**.

Pour créer un certificat APNS .pfx sur un Mac

1. Sur le même ordinateur Mac exécutant Mac OS X que vous avez utilisé pour générer la demande de signature de certificat, localisez le certificat .pem que vous avez reçu d'Apple.
2. Cliquez deux fois sur le fichier de certificat pour importer le fichier dans le trousseau.
3. Si vous êtes invité à ajouter le certificat à un trousseau spécifique, conservez le trousseau de connexion sélectionné par défaut, puis cliquez sur **OK**. Le certificat qui vient d'être ajouté apparaîtra dans votre liste de certificats.
4. Cliquez sur le certificat puis sur le menu **Fichier**, cliquez sur **Exporter** pour commencer l'exportation du certificat dans un certificat PCKS #12 (.pfx).
5. Donnez au fichier de certificat un nom unique à utiliser dans le serveur XenMobile, 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 invitera à saisir le mot de passe ou le trousseau sélectionné. Entrez le mot de passe, puis cliquez sur **OK**. Le certificat enregistré est maintenant prêt à être utilisé avec le serveur XenMobile.
   Remarque : si vous ne souhaitez pas conserver l'ordinateur et le compte d'utilisateur que vous avez utilisés pour générer la demande de signature de certificat et terminer le processus d'exportation du certificat, Citrix vous recommande d'enregistrer ou d'exporter les clés publiques ou personnelles du système local. Sinon, l'accès aux certificats APNS à des fins de réutilisation sera annulé et vous devrez répéter le processus de demande de signature de certificat et APNs depuis le début.

Pour créer un certificat APNS .pfx avec OpenSSL

Lorsque vous utilisez OpenSSL pour créer une demande de signature de certificat (CSR), vous pouvez également utiliser OpenSSL pour créer un certificat APNS .pfx.

1. À l'invite de commandes ou shell, exécutez la commande suivante.
   openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer.key.pem -out apns_identity.p12
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, puis copiez le fichier sur le serveur XenMobile, de façon à pouvoir utiliser la console XenMobile pour charger le fichier.

Pour importer un certificat APNS dans XenMobile

Une fois que vous avez demandé et reçu un nouveau certificat APNS, vous devez l'importer dans XenMobile pour ajouter le certificat (pour la première fois) ou remplacer un certificat existant.

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. Depuis le menu **Importer**, sélectionnez **Keystore**.
5. Dans **Utiliser en tant que**, choisissez **APNS**.
6. Accédez au fichier .p12 sur votre ordinateur.
7. Entrez un mot de passe et cliquez sur **Importer**.

Pour de plus amples informations sur les certificats dans XenMobile, consultez la section Certificats.

Pour renouveler un certificat APNS

Pour renouveler un certificat APNS, vous devez effectuer la même procédure que si vous en créiez un nouveau. Ensuite, visitez le portail Apple Push Certificats Portal et chargez le nouveau certificat. Après avoir ouvert une session, vous pourrez voir votre certificat existant ou un certificat qui a été importé à partir de votre ancien compte Apple Developers. 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.

Remarque : pour déterminer la date à laquelle votre certificat APNS expire, dans la console XenMobile, cliquez sur **Configurer** > **Paramètres** > **Certificats**. Si le certificat a expiré, cependant, ne le révoquez pas.

1. Générez une demande de signature de certificat via Microsoft Internet Information Services (IIS).
2. Sur le site Web XenMobile APNs CSR Signing, chargez la nouvelle CSR et cliquez sur **Sign**.
3. Soumettez la demande de signature de certificat (CSR) signée à Apple sur le portail Apple Push certificat Portal.
4. Cliquez sur **Renew**.
5. Générez un certificat APNS PCKS #12 (.pfx) à l'aide de Microsoft IIS.
6. Mettez à jour le nouveau certificat APNS dans la console XenMobile. Cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console. La page **Paramètres** s'affiche.
7. Cliquez sur **Certificats**. La page **Certificats** s'affiche.
8. Cliquez sur **Importer**. La boîte de dialogue **Importer** apparaît.
9. Depuis le menu **Importer**, sélectionnez **Keystore**.
10. Dans **Utiliser en tant que**, choisissez **APNS**.
11. Accédez au fichier .p12 sur votre ordinateur.
12. Entrez un mot de passe et cliquez sur **Importer**.

Comptes utilisateur, rôles et paramètres d'inscription

Jul 27, 2016

Dans XenMobile, vous configurez des utilisateurs et des groupes, des rôles pour les utilisateurs et les groupes, ainsi que le mode d'inscription et les invitations dans la page Paramètres de la console XenMobile. Pour ouvrir la page **Paramètres**, cliquez sur l'icône d'engrenage dans le coin supérieur droit.

Depuis la page **Paramètres**, vous pouvez effectuer ce qui suit :

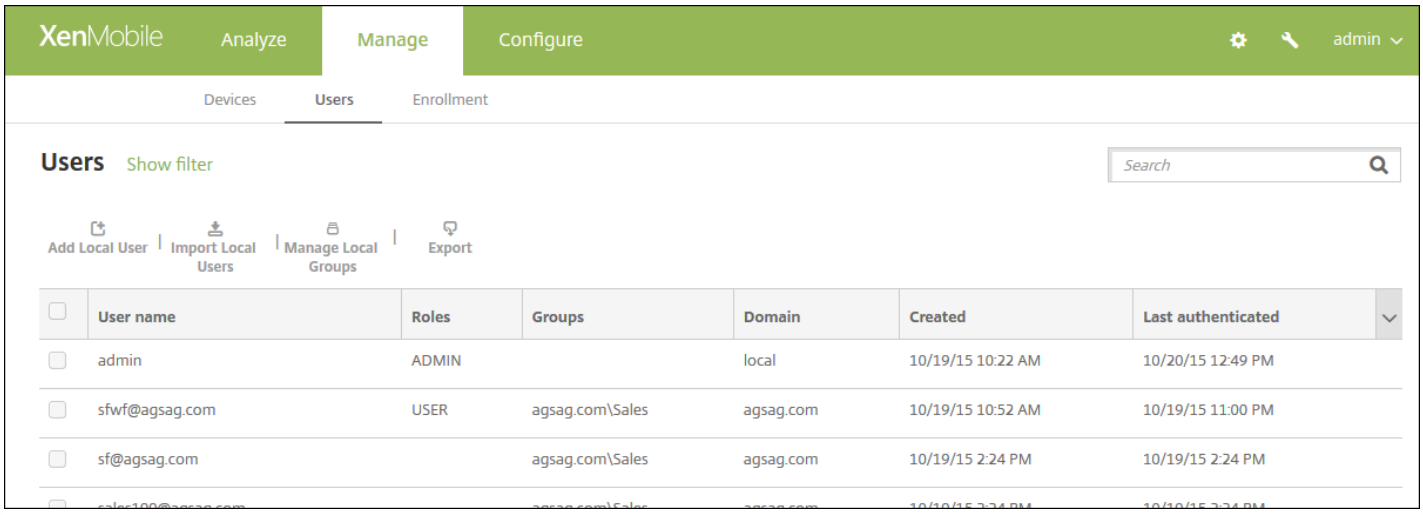
- Cliquez sur **Utilisateurs et groupes locaux** pour ajouter des comptes utilisateur manuellement ou utilisez un fichier de provisioning .csv pour importer des comptes et gérer des groupes locaux. Pour plus de détails, consultez :
  - Pour ajouter, modifier ou supprimer des utilisateurs locaux dans XenMobile
  - Pour importer des comptes utilisateur à l'aide d'un fichier de provisioning .csv et Formats des fichiers de provisioning
  - Pour ajouter ou supprimer des groupes dans XenMobile
- Cliquez sur **Inscription** pour configurer jusqu'à sept modes, chacun disposant de son propre niveau de sécurité et d'étapes que les utilisateurs doivent suivre pour inscrire leurs appareils, et pour envoyer des invitations d'inscription. Pour plus de détails, consultez :
  - Pour configurer des modes d'inscription et activer le portail en libre-service
  - Activer la découverte automatique pour l'inscription utilisateur dans XenMobile
- Cliquez sur **Contrôle d'accès basé sur rôle** pour attribuer 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 de détails, consultez :
  - Configuration de rôles avec RBAC et Rôles et autorisations RBAC
- Cliquez sur les **Modèles de notification** à utiliser dans les actions automatisées, l'inscription et les messages de notification standard envoyés aux utilisateurs. Vous configurez les modèles de notification pour l'envoi de messages sur trois canaux différents : Worx Home, SMTP ou SMS. Pour plus de détails, consultez :
  - Création et mise à jour de modèles de notification

Pour ajouter, modifier ou supprimer des utilisateurs locaux dans XenMobile

Jul 27, 2016

Vous pouvez ajouter des comptes d'utilisateur locaux à XenMobile manuellement ou vous pouvez utiliser un fichier de provisioning pour importer les comptes. Consultez la section Pour importer des comptes utilisateur à l'aide d'un fichier de provisioning .csv pour la procédure d'importation des utilisateurs à partir d'un fichier de provisioning.

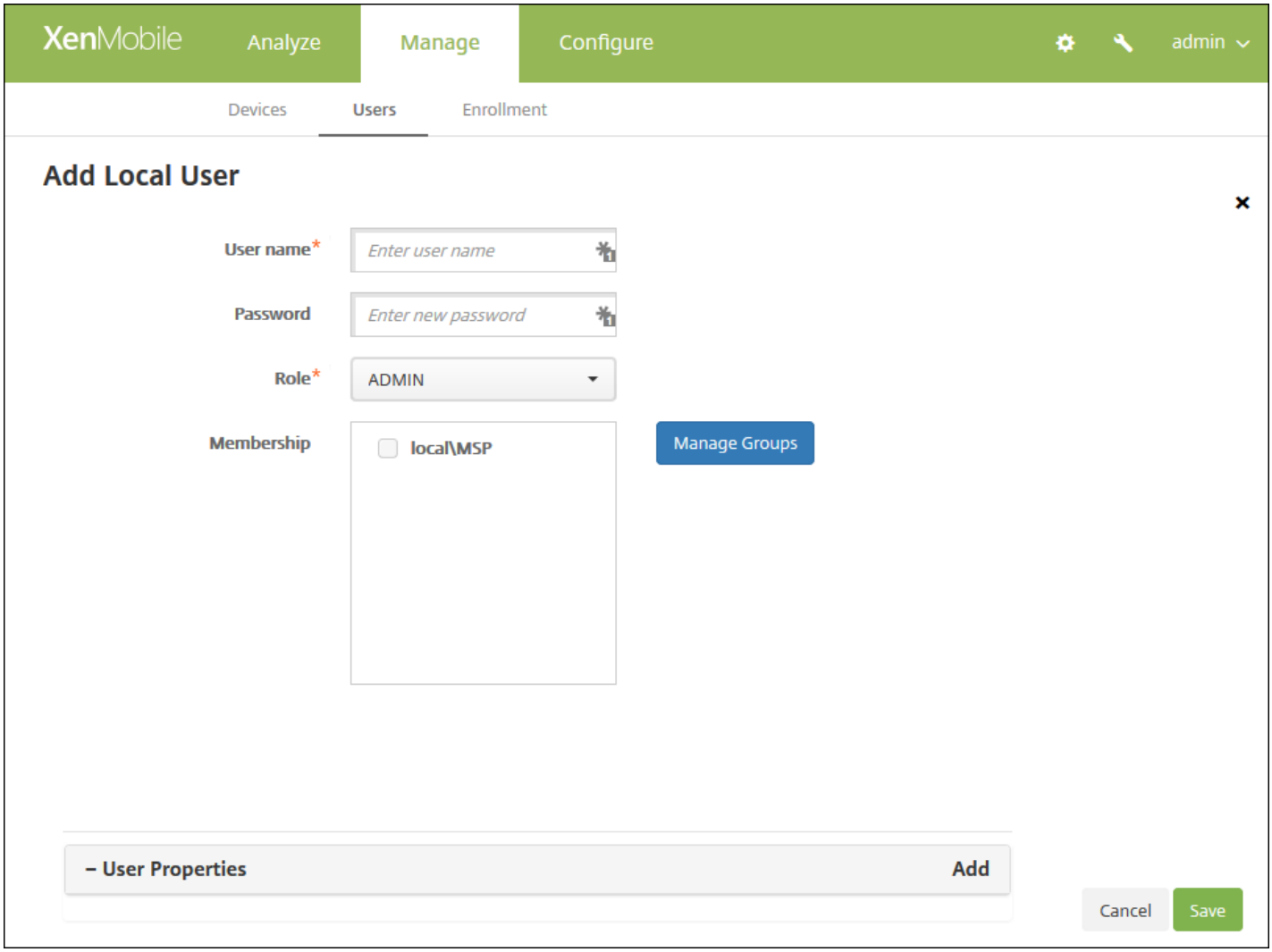
1. Dans la console XenMobile, cliquez sur **Gérer > Utilisateurs**. La page **Utilisateurs** s'affiche.



Pour ajouter un utilisateur local

Cette procédure ajoute un seul utilisateur à la fois à XenMobile. Pour ajouter plusieurs utilisateurs, consultez la section Pour importer des comptes utilisateur à l'aide d'un fichier de provisioning .csv.

1. Sur la page **Utilisateurs**, cliquez sur **Ajouter un utilisateur local**. La page **Ajouter un utilisateur local** s'affiche.



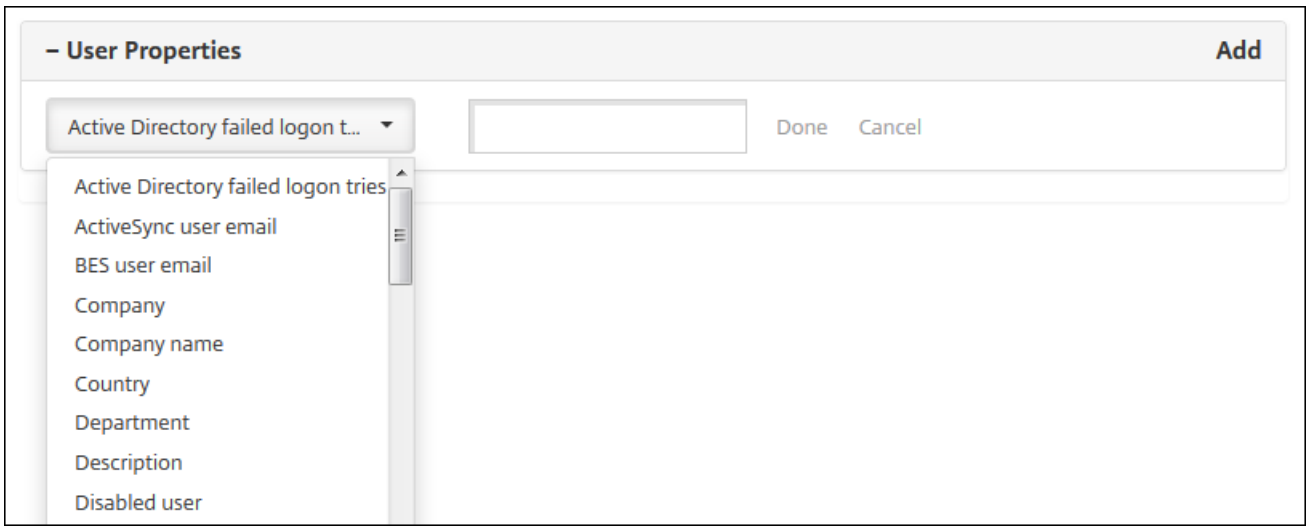
2. Configurez les paramètres suivants :

- **Nom d'utilisateur** : entrez le nom de l'utilisateur. Il s'agit d'un 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).
- **Rôle** : dans la liste, cliquez sur le rôle d'utilisateur. Pour plus d'informations sur les rôles, veuillez consulter les sections Configuration de rôles avec RBAC et Rôles et autorisations 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 annuler l'opération.

    Remarque : 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.

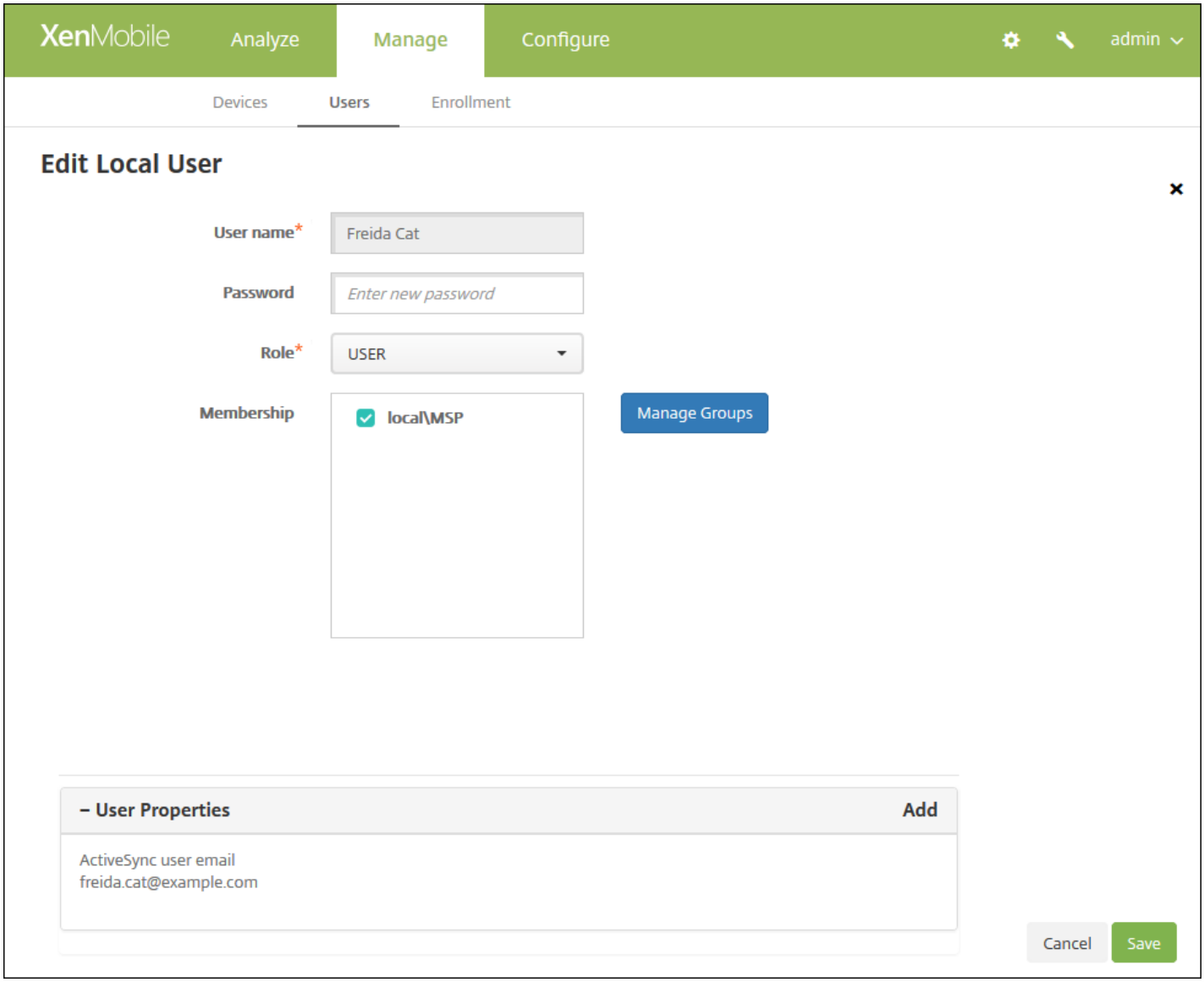
Pour modifier une propriété utilisateur, cliquez sur la propriété et effectuez les modifications. Cliquez sur **Terminé** pour enregistrer les modifications ou sur **Annuler** pour laisser la propriété inchangée.



3. Cliquez sur **Enregistrer**.

Pour modifier un 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. Voir Filtres et tableaux dans la console XenMobile pour de plus amples informations sur la sélection des éléments dans le tableau.



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 d'utilisateur.
- **Adhésion** : dans la liste, cliquez sur le groupe ou les groupes auxquels ajouter l'utilisateur. Pour supprimer un 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 annuler l'opération.
  - 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 supprimer un utilisateur local

1. Sur la page **Utilisateurs**, dans la liste des utilisateurs, cliquez pour sélectionner un utilisateur.

   Remarque : vous pouvez sélectionner plusieurs utilisateurs à supprimer en sélectionnant la case à cocher en regard de chaque utilisateur.

2. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche.

3. Cliquez sur **Supprimer** pour supprimer l'utilisateur ou cliquez sur **Annuler** pour ne pas supprimer l'utilisateur.

Importation de comptes utilisateur

Oct 17, 2016

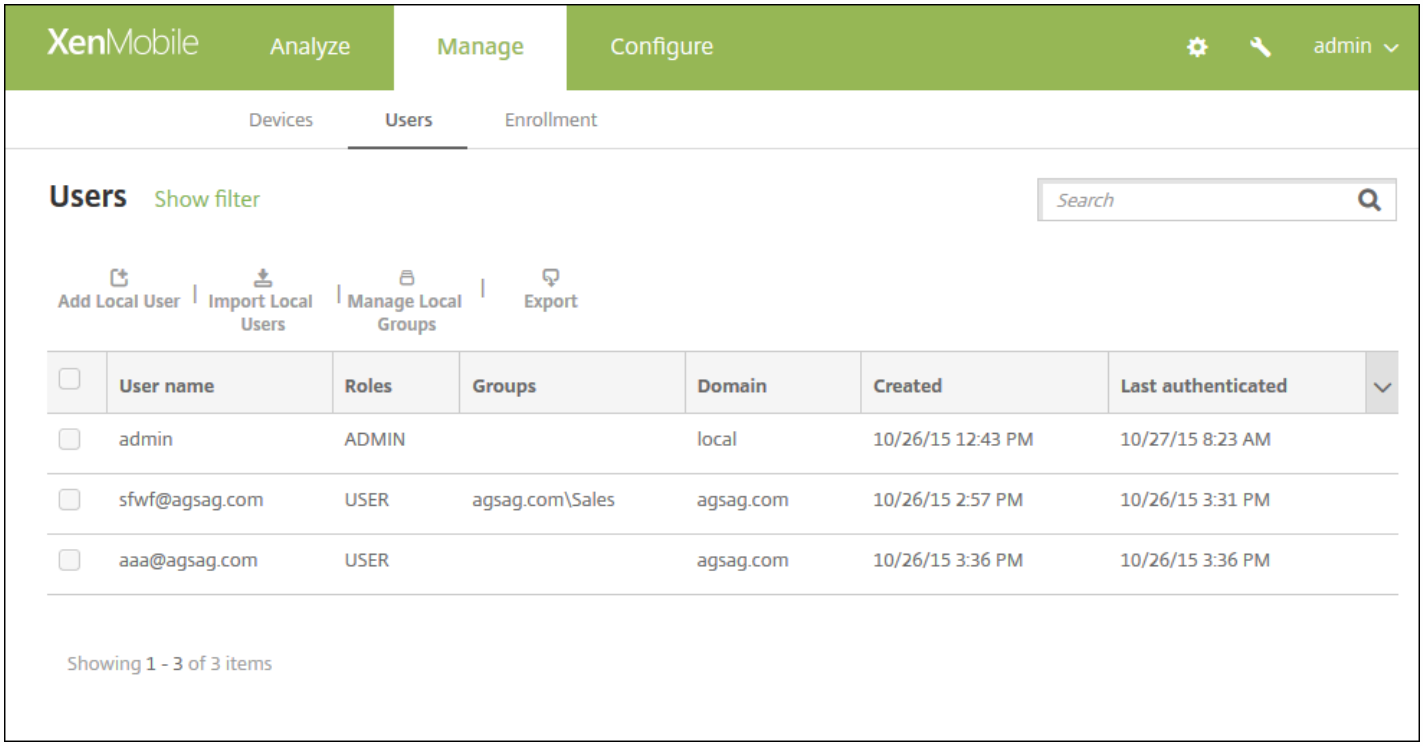
Vous pouvez importer des comptes utilisateur et des propriétés à partir d'un fichier .csv appelé fichier de provisioning, que vous pouvez créer manuellement. Pour de plus amples informations sur la mise en forme des fichiers de provisioning, consultez Formats des fichiers de provisioning.

Remarque :

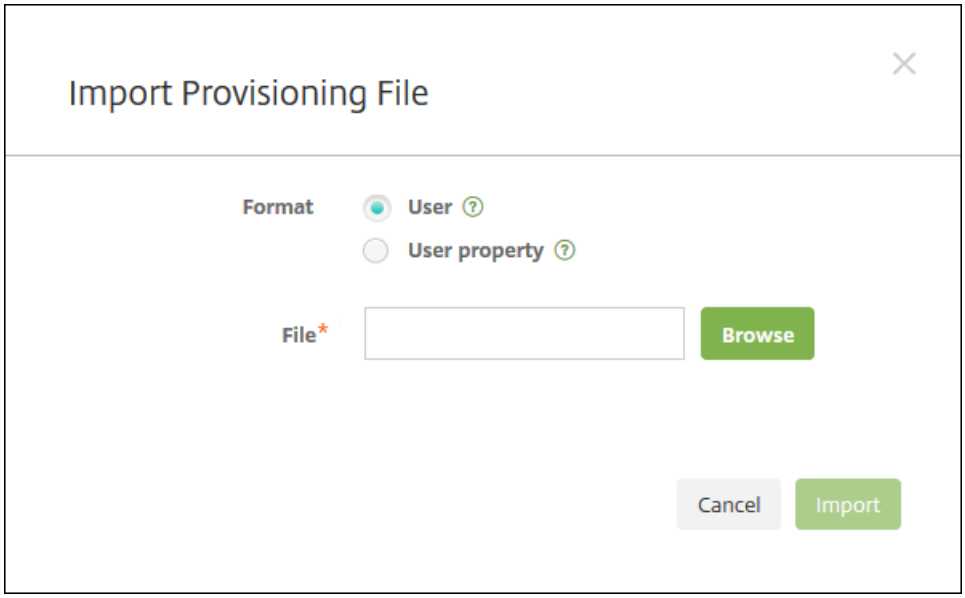
- Si vous importez des utilisateurs à partir d'un annuaire LDAP, utilisez le nom de domaine et le nom d'utilisateur dans le fichier d'importation. Par exemple, spécifiez le nomd'utilisateur@domaine.com. Cette syntaxe empêche d'autres recherches qui ralentiraient la vitesse d'importation.
- Si vous importez des utilisateurs sur l'annuaire utilisateur interne XenMobile, désactivez le domaine par défaut pour accélérer le processus d'importation. Vous pouvez réactiver le domaine par défaut après l'importation des utilisateurs internes.
- Les utilisateurs locaux peuvent être au format « Nom d'utilisateur principal (UPN) », mais 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

Aug 22, 2016

Un fichier de provisioning que vous créez manuellement et utilisez pour l'importation de comptes utilisateur et de propriétés sur Device Manager doit être dans un des formats suivants :

- Champs des fichiers de provisioning utilisateur : user,password;role;group1;group2
- Champs du fichier de provisioning d'attribut utilisateur : user;propertyName1;propertyValue1;propertyName2;propertyValue2

Remarque :

- Les champs dans le fichier de provisioning sont séparés par un point-virgule (;). Si une partie d'un champ contient un point-virgule, elle doit être précédée d'une barre oblique inverse (\). Exemple : la propriété propertyV;test;1;2 doit être saisie en tant que propertyV;1;test\;2 dans le fichier de provisioning.
- Les valeurs valides pour Role sont les rôles prédéfinis USER ADMIN, SUPPORT et DEVICE_PROVISIONING, ainsi que tout autre rôle que vous avez défini.
- Le point (.) est utilisé comme séparateur pour créer la hiérarchie de groupe ; par conséquent, vous ne pouvez pas utiliser de point dans les noms de groupes.
- Les attributs de propriété dans les fichiers de provisioning d'attribut doivent être en minuscules. La base de données est sensible à la casse.

Exemple de contenu de provisioning utilisateur

Cette entrée, user01;pwd\;01;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

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

Cette 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 valeur

Ajout ou suppression de groupes

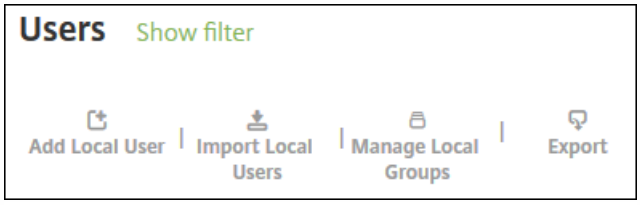
Jul 27, 2016

Vous gérez les groupes dans la boîte de dialogue Gérer les groupes dans la console XenMobile, que vous pouvez trouver sur la page **Utilisateurs**, la page **Ajouter un utilisateur local** où la page **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.

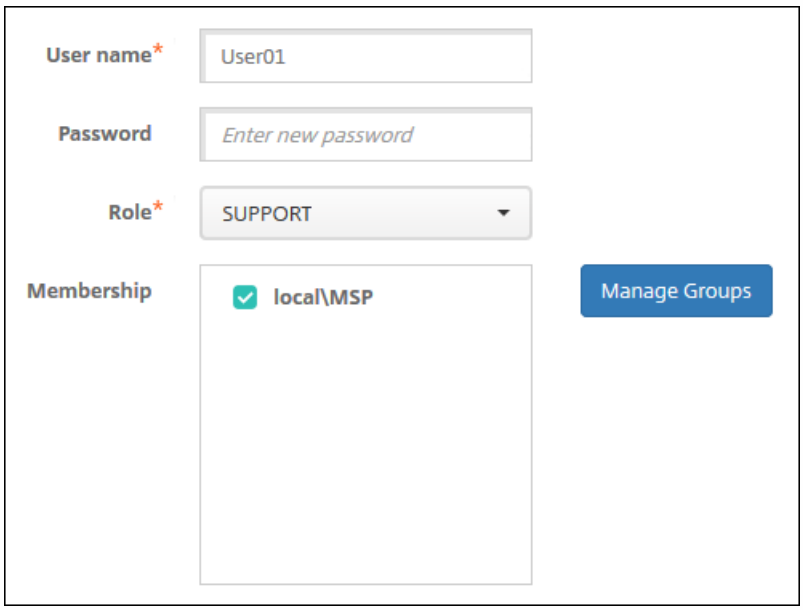
Pour ajouter un groupe local

1. Procédez comme suit :

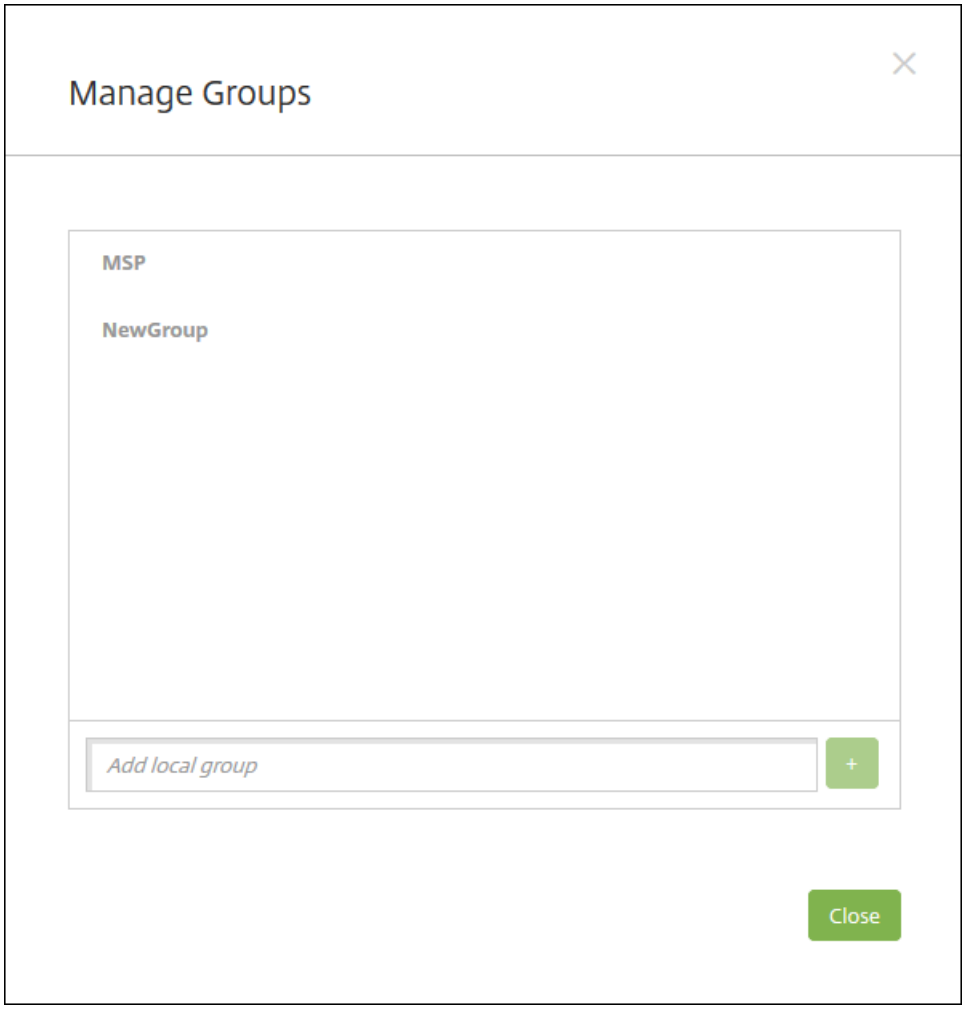
- Sur la page **Utilisateurs**, cliquez sur **Gérer les groupes locaux**.



- 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 la liste 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**.

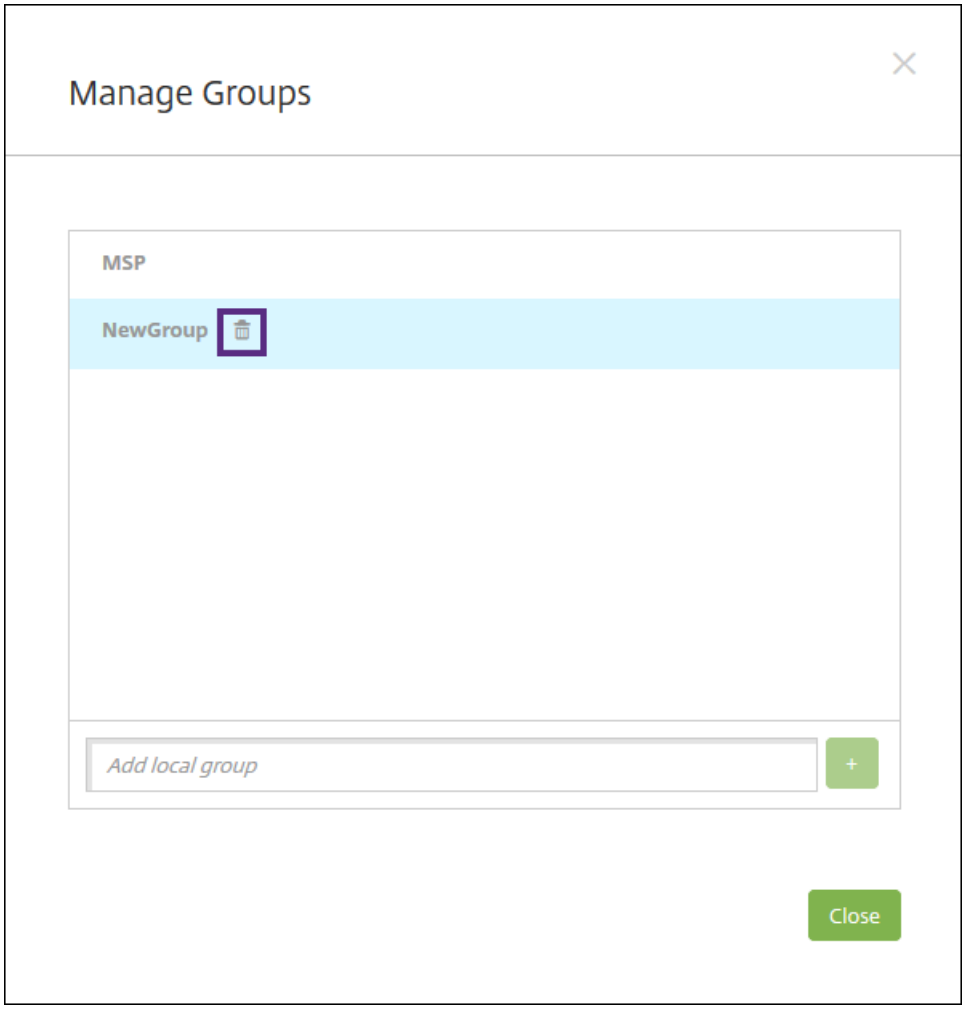
Pour supprimer un groupe

Remarque : 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 ; 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.

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**.

Configuration de rôles avec RBAC

Oct 17, 2016

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 aussi utiliser les rôles par défaut en tant que modèles que vous personnalisez pour créer de nouveaux rôles utilisateur autorisés à accéder 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, si les utilisateurs ADGroupA peuvent localiser les appareils appartenant à l'entreprise, et que les utilisateurs ADGroupB peuvent réinitialiser les appareils appartenant aux employés, alors un utilisateur qui appartient aux deux groupes peut localiser et réinitialiser les appareils appartenant à l'entreprise et aux employés.

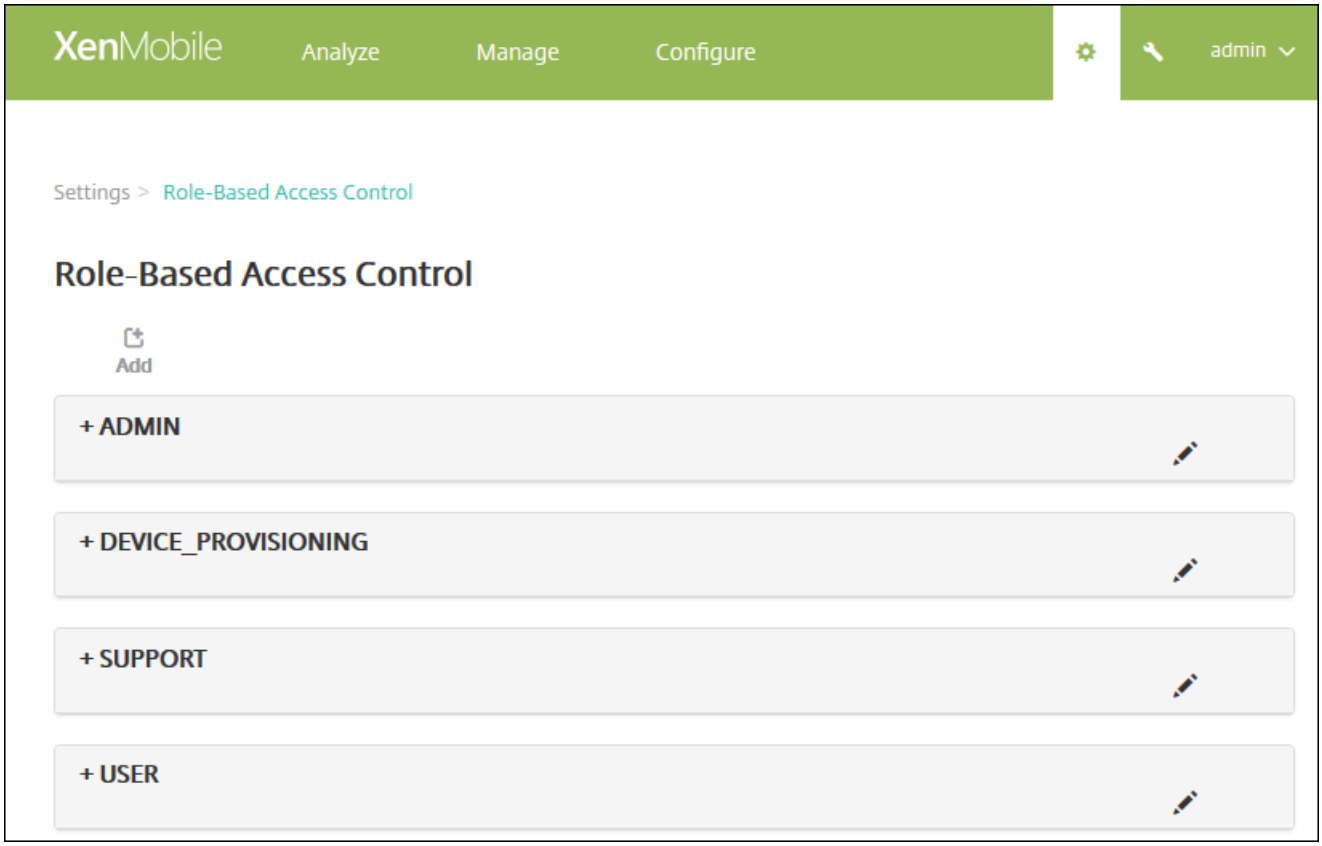
Remarque : un seul rôle peut être attribué aux utilisateurs locaux.

Vous pouvez utiliser la fonctionnalité RBAC dans XenMobile pour effectuer les opérations suivantes :

- Créer un nouveau rôle.
- Ajouter des groupes à un rôle.
- Associer des utilisateurs locaux aux rôles.

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**. 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.

3. Cliquez sur **Ajouter** pour ajouter un nouveau rôle utilisateur, cliquez sur l'icône de crayon à droite d'un rôle existant pour modifier le rôle, ou cliquez sur l'icône de corbeille à droite d'un rôle que vous avez précédemment défini pour supprimer le 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.

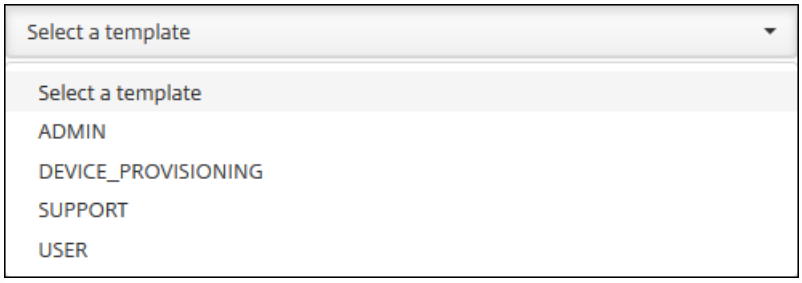
4. Entrez les informations suivantes pour créer un nouveau rôle utilisateur ou pour modifier un rôle utilisateur existant :

- **Nom RBAC** : entrez un nom descriptif pour le nouveau rôle utilisateur. Vous ne pouvez pas modifier le nom d'un rôle

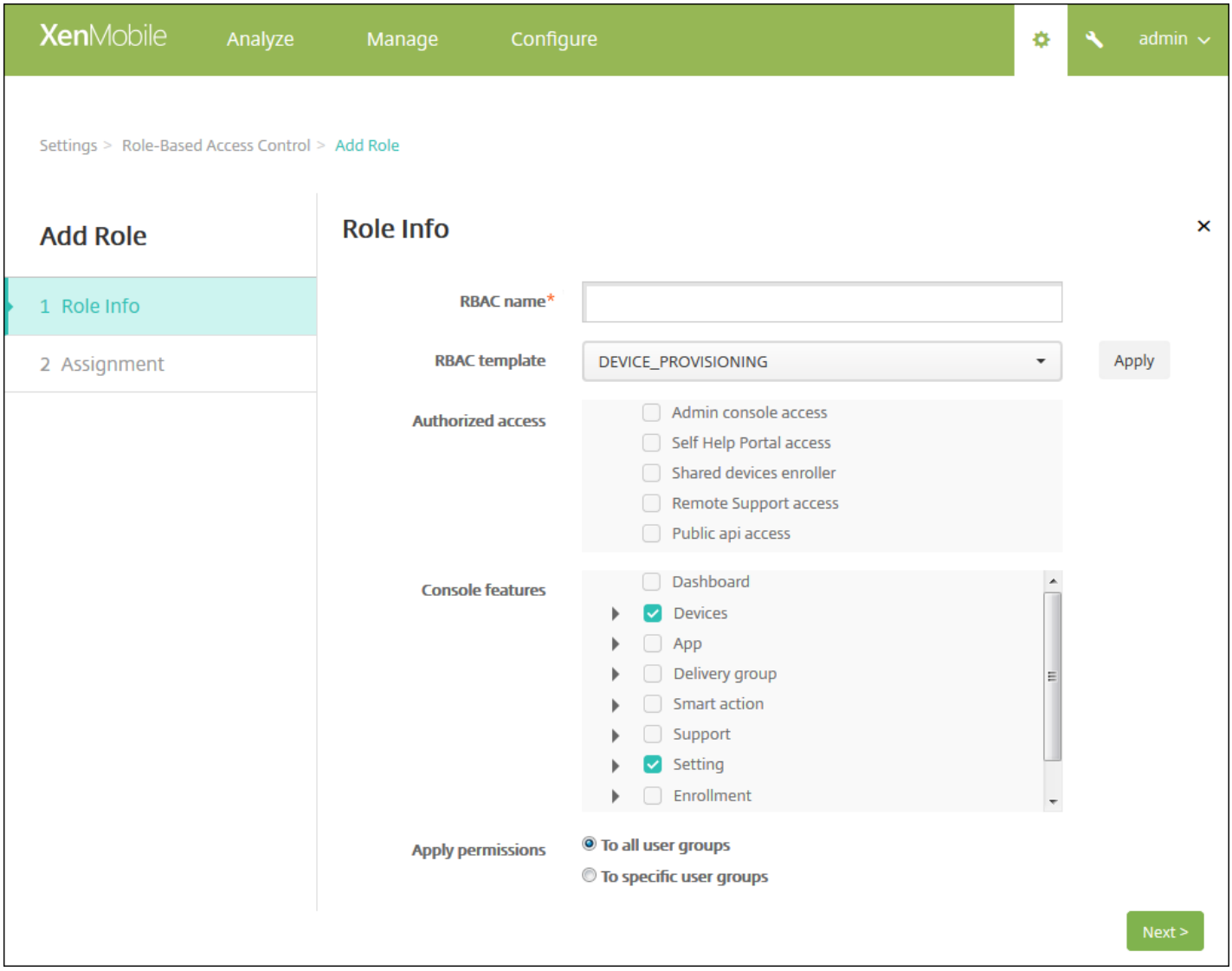
existant.

- **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**.

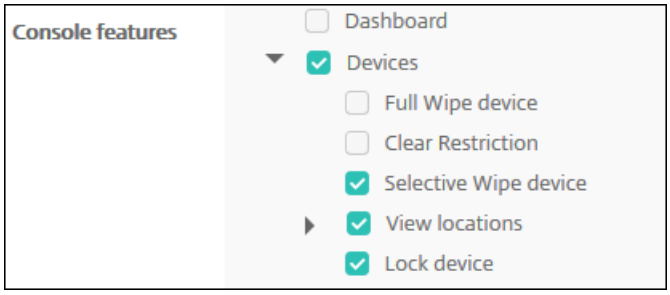


5. Cliquez sur **Appliquer** à droite du champ **Modèle RBAC** pour renseigner les cases **Accès autorisé** et **Fonctionnalités de la console** avec les autorisations d'accès prédéfinies pour le modèle sélectionné.

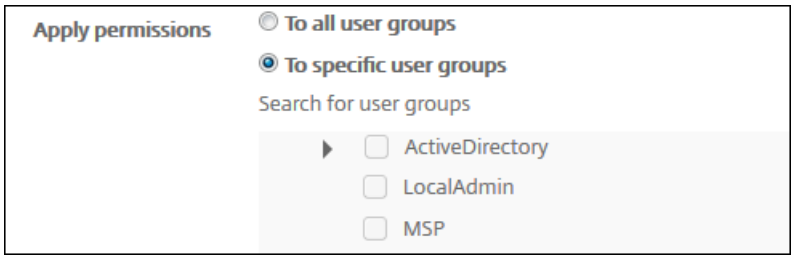


6. Sélectionnez et décochez les cases à cocher appropriées dans **Accès autorisé** et **Fonctionnalités de la console** pour personnaliser le rôle.

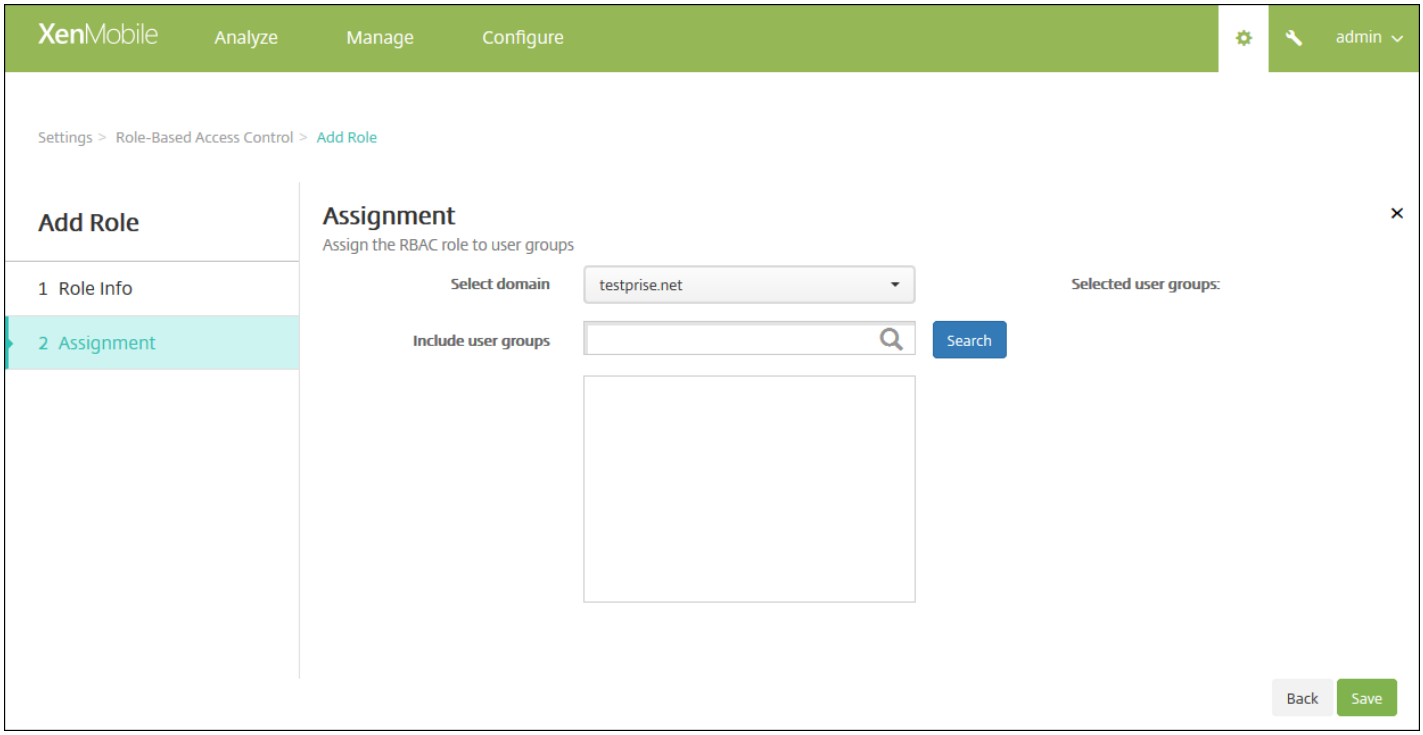
si vous cliquez sur le triangle à côté de Fonctionnalités de la console, les autorisations spécifiques à cette fonctionnalité s'affichent de façon à ce que vous puissiez les sélectionner ou les désélectionner. La case à cocher de niveau supérieur empêche l'accès à cette partie de la console ; vous devez sélectionner des options individuelles en-dessous du 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 sur la console pour les utilisateurs attribués au rôle, mais les options sélectionnées s'affichent.



7. **Appliquer les autorisations** : sélectionnez les groupes auxquels vous voulez appliquer les autorisations sélectionnées. 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.

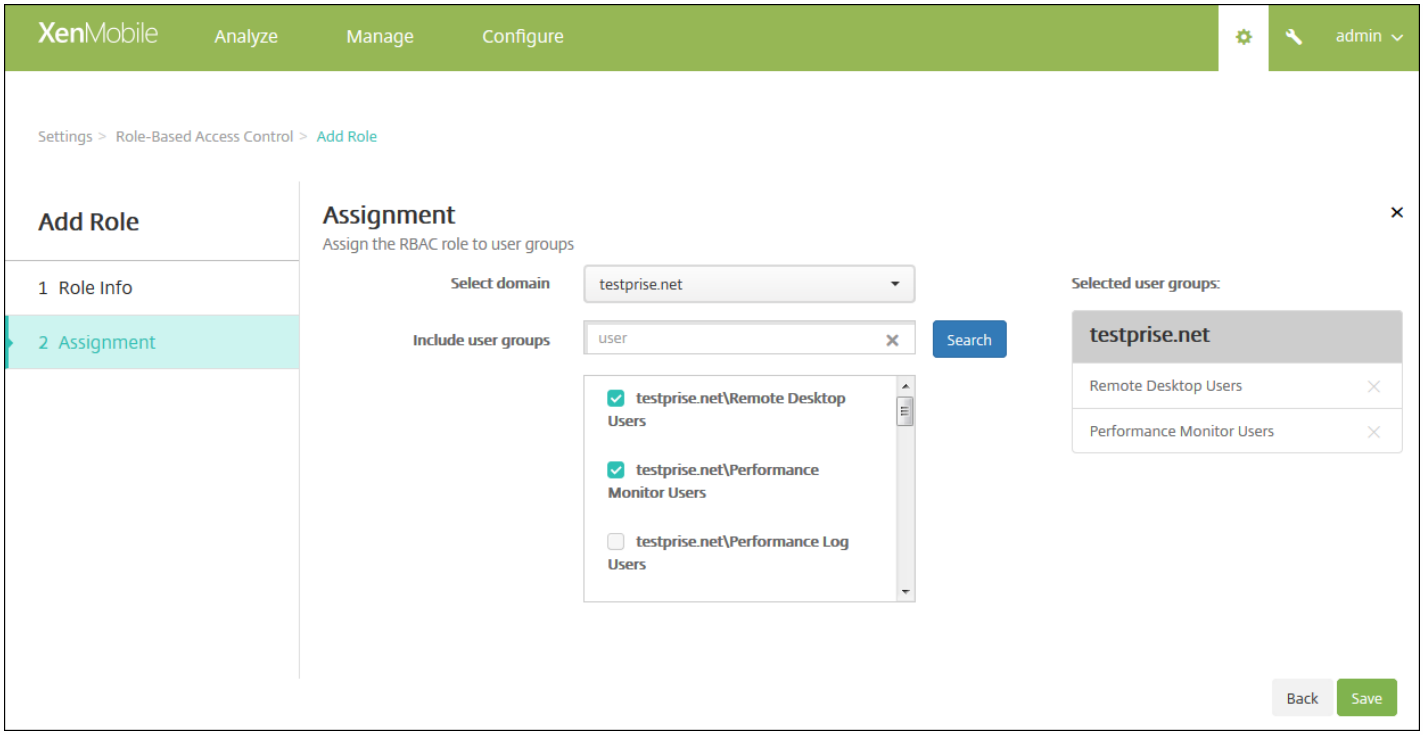


8. Cliquez sur **Next**. La page **Attribution** s'affiche.



9. 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.

10. Cliquez sur **Enregistrer**.

Rôles et autorisations RBAC

Aug 22, 2016

Chaque rôle RBAC prédéfini dispose de certains accès et de certaines autorisations associés à ce rôle. 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.

Pour plus d'informations sur la manière de configurer les rôles RBAC, consultez la section Configuration de rôles avec RBAC.

- Rôle d'administrateur
- Rôle de provisioning d'appareils
- Rôle Support
- Rôle Utilisateur

Pour configurer des modes d'inscription et activer le portail en libre-service

Jul 27, 2016

Vous configurez des modes d'inscription d'appareils pour autoriser les utilisateurs à inscrire leurs appareils dans XenMobile. XenMobile offre sept modes, chacun doté de son propre niveau de sécurité et de ses propres étapes que les utilisateurs doivent suivre pour inscrire leurs appareils. Vous pouvez mettre à disposition certains modes sur le portail en libre-service, à partir duquel les utilisateurs peuvent ouvrir une session et générer des liens d'inscription. Cela leur permet d'inscrire leurs appareils eux-mêmes ou de s'envoyer une invitation d'inscription.

Vous configurez les modes d'inscription dans la console XenMobile sur la page **Paramètres > Inscription**. Vous envoyez des invitations d'inscription depuis la console XenMobile, à partir de la page **Gérer > Inscription** (voir Inscription d'utilisateurs et d'appareils dans XenMobile).

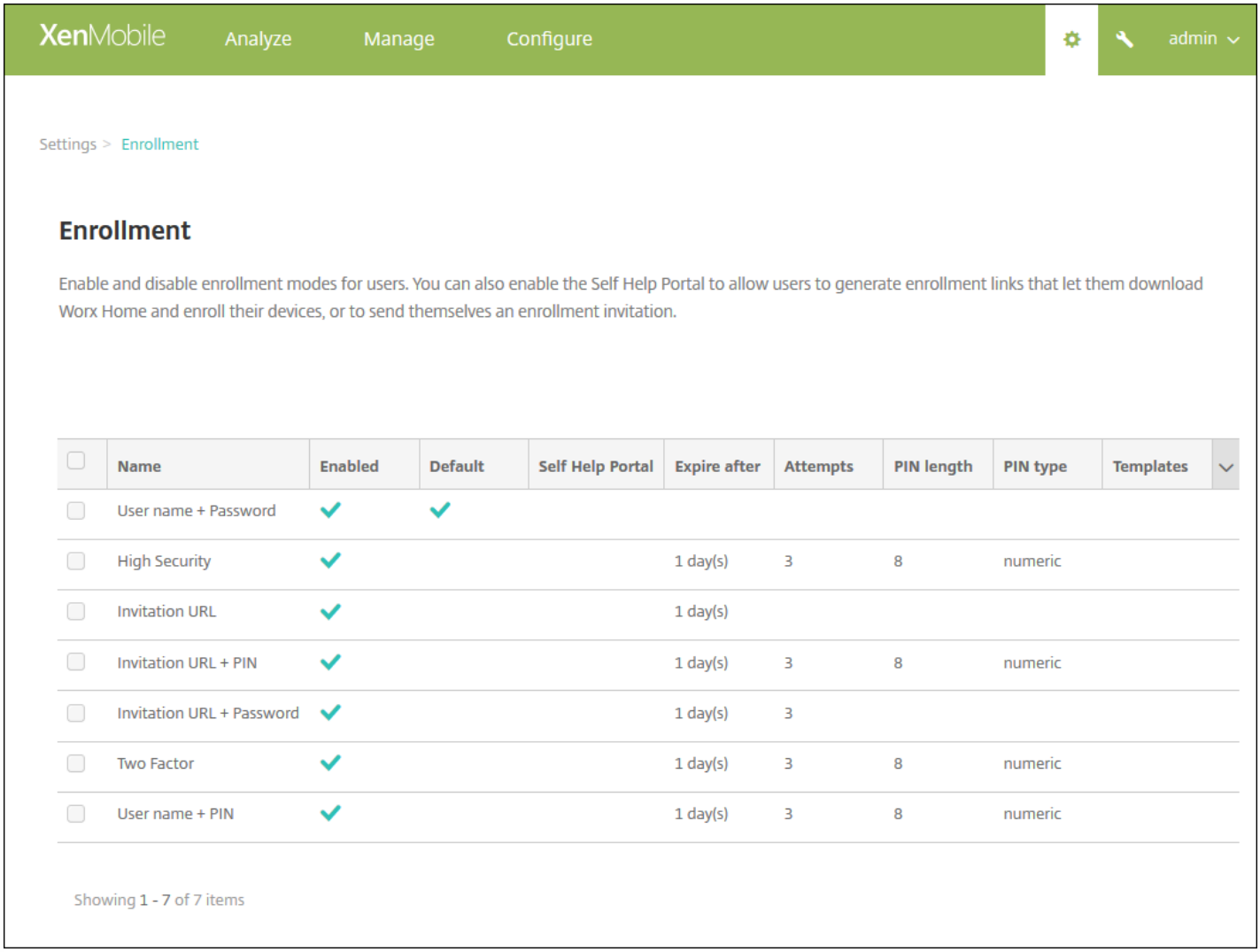
Remarque : si vous prévoyez d'utiliser des modèles de notification personnalisés, vous devez définir les modèles avant de configurer des modes d'inscription. Pour de plus amples informations sur les modèles de notification, consultez la section Création et mise à jour de modèles de notification.

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 disponibles. Par défaut, tous les modes d'inscription sont activés.

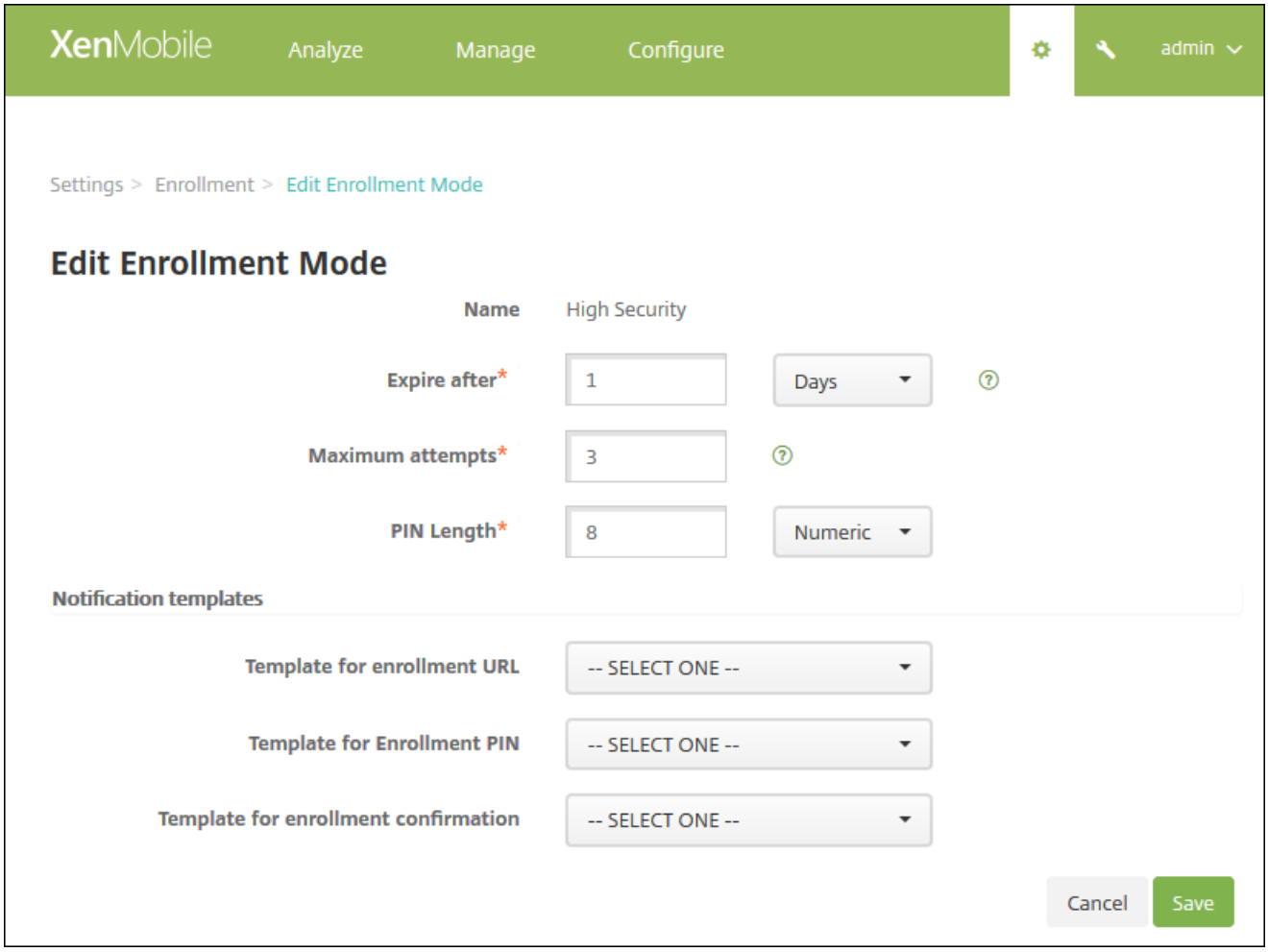
3. Sélectionnez un mode d'inscription à modifier dans la liste, puis définissez le mode comme le mode par défaut, supprimez le mode ou autorisez l'accès des utilisateurs via le portail en libre-service.

Remarque : lorsque vous activez la case à cocher en regard d'un mode d'inscription, le menu d'options s'affiche au-dessus de la liste des modes d'inscription ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.



Pour modifier un mode d'inscription

1. Dans la liste **Inscription**, sélectionnez un mode d'inscription, puis cliquez sur Modifier. La page **Modifier le mode d'inscription** apparaît. Selon le mode que vous sélectionnez, vous pouvez voir différentes options.



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.
  Remarque : entrez 0 pour empêcher l'invitation d'expirer.

- **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.
  Remarque : entrez 0 pour autoriser un nombre illimité de tentatives.

- **Longueur du code PIN** : entrez le nombre de chiffres ou de caractères que le code PIN généré doit contenir.
- **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 SMS en fonction de la façon dont vous avez configuré le modèle qui leur permet d'inscrire leurs appareils dans XenMobile. Pour de plus amples informations sur les modèles de notification, consultez la section Création et mise à jour de 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 comme mode par défaut

Lorsque vous définissez un mode d'inscription 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 n'est défini par défaut, vous devez créer une demande d'inscription pour chaque inscription d'appareil.

Remarque : seuls **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + PIN** peuvent être définis en tant que mode d'inscription par défaut.
1. Sélectionnez **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + PIN** comme mode d'inscription par défaut.

Remarque : le mode sélectionné doit être activé pour être défini comme mode par défaut.
2. Cliquez sur **Mode par défaut**. Le mode sélectionné est maintenant le mode par défaut. Si un autre mode d'inscription a été défini comme mode par défaut, le mode n'est plus le mode par défaut.

Pour désactiver un mode d'inscription

La désactivation d'un mode d'inscription 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 vous autorisez les utilisateurs à inscrire leurs appareils en désactivant un mode d'inscription et en activant un autre.

1. Sélectionnez un mode d'inscription.

Remarque : vous ne pouvez pas désactiver le mode d'inscription par défaut. Pour désactiver le mode d'inscription par défaut, vous devez d'abord lui retirer son état de mode par défaut.
2. Cliquez sur **Désactiver**. Le mode d'inscription n'est plus activé.

Pour activer un mode d'inscription sur le portail en libre-service

L'activation d'un mode d'inscription sur le portail en libre-service permet aux utilisateurs d'inscrire leurs appareils dans XenMobile individuellement.

Remarque :

- Le mode d'inscription 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 à la fois sur le portail en libre-service.

1. Sélectionnez un mode d'inscription.

2. Cliquez sur **Portail en libre-service**. Le mode d'inscription 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.

Activer la découverte automatique pour l'inscription utilisateur dans XenMobile

Jul 27, 2016

La découverte automatique simplifie le processus d'inscription pour les utilisateurs. Ils peuvent utiliser leurs noms d'utilisateur réseau et leurs mots de passe Active Directory pour inscrire leurs appareils, et n'ont pas besoin d'entrer des détails sur le serveur XenMobile. Le nom d'utilisateur doit être entré au format UPN (nom d'utilisateur principal) ; par exemple, utilisateur@monentreprise.com.

Pour activer la détection automatique, vous pouvez accéder au portail Autodiscovery Service sur https://xenmobiletools.citrix.com. Pour plus d'informations sur le portail Autodiscovery Service, consultez la rubrique relative à XenMobile Autodiscovery Service.

Il se peut, dans certains cas limités, que vous deviez contacter le support technique Citrix pour activer la détection automatique. Pour ce faire, vous pouvez suivre les procédures ci-dessous pour transmettre vos informations de déploiement à l'équipe d'assistance technique, et dans le cas d'appareils Windows, un certificat SSL. Après que Citrix a reçu ces informations, lorsque les utilisateurs inscrivent leurs appareils, les informations de domaine sont extraites et mappées à une adresse de serveur. Ces informations sont conservées dans la base de données XenMobile afin qu'elles soient toujours accessibles et disponibles lorsque les utilisateurs s'inscrivent.

1. Si vous ne parvenez pas à activer la détection automatique à l'aide du portail Autodiscovery Service sur https://xenmobiletools.citrix.com, ouvrez un ticket de support technique Citrix à l'aide du portail d'assistance Citrix et fournissez les informations suivantes :

- Le domaine contenant les comptes avec les utilisateurs vont s'inscrire.
- Le nom de domaine complet (FQDN) du serveur XenMobile.
- Le nom de l'instance XenMobile. Par défaut, le nom de l'instance est zdm et est sensible à la casse.
- Le type d'ID utilisateur, qui peut être UPN ou E-mail. Le paramètre par défaut est UPN.
- Le port utilisé pour l'inscription iOS si vous avez modifié le numéro de port par défaut 8443.
- Le port sur lequel le serveur XenMobile accepte les connexions si vous avez modifié le numéro de port par défaut 443.
- Si vous le souhaitez, une adresse e-mail pour votre administrateur XenMobile.

2. Si vous prévoyez d'inscrire des appareils Windows, procédez comme suit :

- Obtenez un certificat SSL non générique signé publiquement pour enterpriseenrollment.masociété.com, où masociété.com est le domaine contenant les comptes avec lesquels les utilisateurs vont s'inscrire. Joignez le certificat SSL au format .pfx et son mot de passe à votre demande.
- Créez un enregistrement de nom canonique (CNAME) dans votre DNS et mappez l'adresse de votre certificat SSL (enterpriseenrollment.masociété.com) vers autodisc.zc.zenprise.com. Lorsque l'utilisateur d'un appareil Windows s'inscrit à l'aide d'un nom UPN, en plus de fournir les détails de votre serveur XenMobile, le serveur d'inscription Citrix invite l'appareil à demander un certificat valide auprès du serveur XenMobile.

Votre ticket de support technique sera mis à jour lorsque vos informations et votre certificat, si nécessaire, sont ajoutés aux serveurs Citrix. À ce stade, les utilisateurs peuvent démarrer l'inscription à l'aide de la découverte automatique.

Remarque : vous pouvez également utiliser un certificat multi-domaines si vous voulez vous inscrire à l'aide de plus d'un domaine. Le certificat multi-domaines doit avoir 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).

Création et mise à jour de modèles de notification

Jul 27, 2016

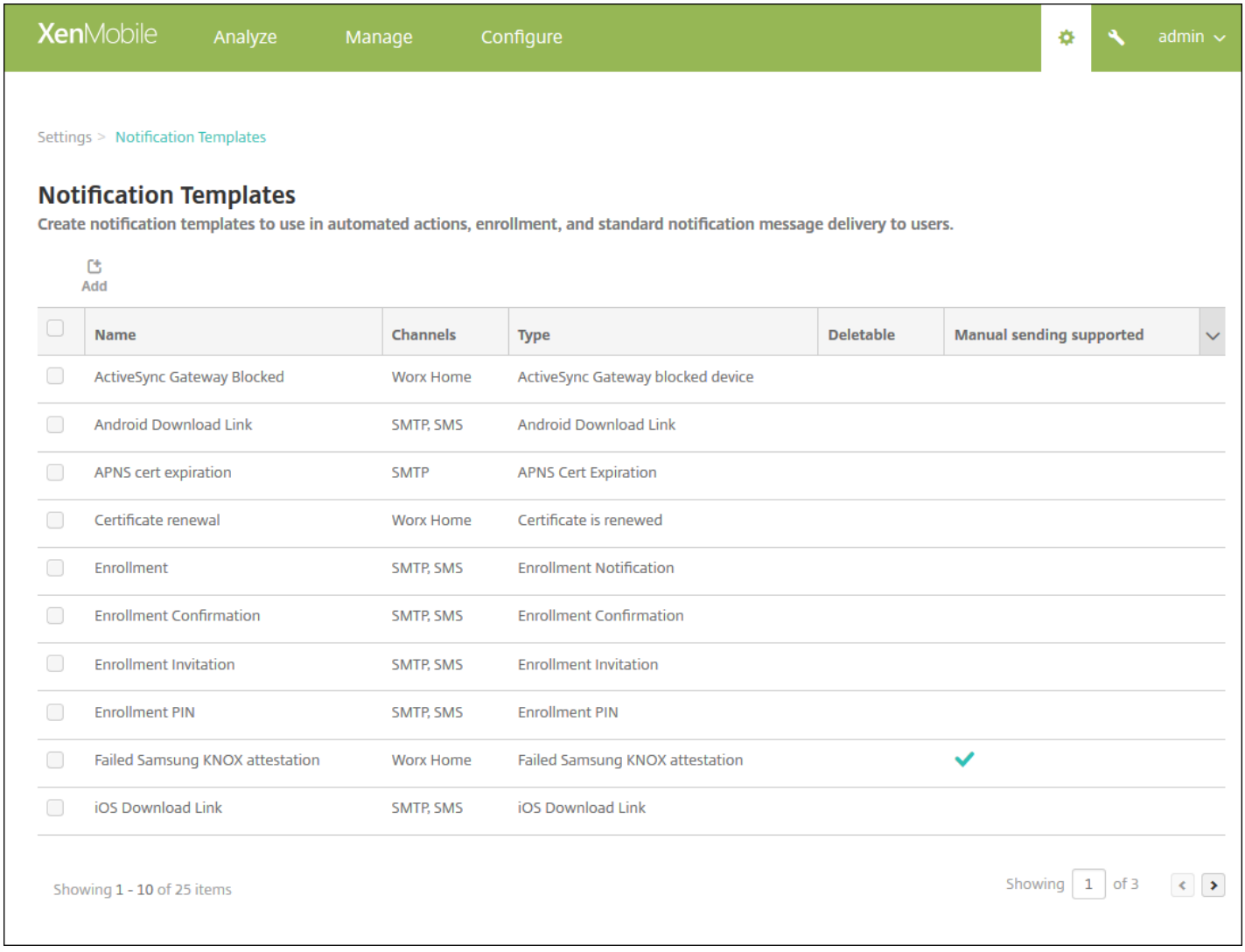
Vous pouvez créer ou mettre à jour des modèles de notification dans XenMobile à utiliser dans les actions automatisées, l'inscription, et les messages de notifications standard envoyés aux utilisateurs. Vous configurez les modèles de notification pour l'envoi de messages sur trois canaux différents : Worx Home, 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. Pour de plus amples informations, consultez la section Notifications dans 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 **Modèles de notification**. La page **Modèles de notification** s'affiche.



Pour ajouter un modèle de notification

1. Cliquez sur **Add**. 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. La page **Ajouter un modèle de notification** s'affiche.

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. Configurez les paramètres suivants :

- **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)}
- ${outofcompliance.reason(smg_block)}

3. Sous **Canaux**, entrez ou modifiez 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 **Worx Home**, 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.

Worx Home :

- **Activer** : cliquez pour activer le canal de notification.
- **Message** : entrez le message à envoyer à l'utilisateur. Ce champ est obligatoire si vous utilisez Worx Home.
- **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.

Important : vous ne pouvez activer la notification SMTP que si vous avez déjà 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 de plus amples informations, consultez la section Ajout d'appareils et affichage des détails des appareils dans XenMobile.
- **Sujet** : entrez un sujet pour la notification. Ce champ est obligatoire.
- **Message** : entrez le message à envoyer à l'utilisateur.

SMS :

- **Activer** : cliquez pour activer le canal de notification.

Important : vous ne pouvez activer la notification SMS que si vous avez déjà configuré la passerelle SMS.

- **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.

5. Cliquez sur **Ajouter**. Lorsque tous les canaux sont correctement configurés, ils apparaissent dans cet ordre sur la page **Modèles de notification** : SMTP, SMS et Worx Home. Tout canal qui n'est pas correctement configuré apparaît après les canaux correctement configurés.

Pour 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**.

Pour supprimer un modèle de notification

Remarque : vous ne pouvez supprimer que les modèles de notification que vous avez ajoutés ; vous ne pouvez pas supprimer des modèles de notification prédéfinis.

1. Sélectionnez un modèle de notification.

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.

Gestion des groupes de mise à disposition

Jul 27, 2016

La gestion et la configuration d'appareils impliquent généralement la création de ressources (stratégies et applications) 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, comment changer l'ordre de déploiement des ressources et des actions dans les groupes de mise à disposition, et la façon dont XenMobile détermine l'ordre de déploiement lorsqu'un utilisateur figure dans plusieurs groupes de mise à disposition qui comportent des stratégies conflictuelles ou en double.

Les groupes de mise à disposition définissent la catégorie d'utilisateurs pour lesquels vous déployez des combinaisons de stratégies, d'applications 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, la fonction, etc. 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, Windows Phone et Windows Tablet qui appartiennent au groupe de mise à disposition les invitant à se reconnecter à XenMobile, ce qui permet de réévaluer les appareils et de déployer des applications, des stratégies et des actions ; les utilisateurs équipés d'autres plates-formes reçoivent les ressources immédiatement s'ils sont déjà connectés, ou en fonction de leur stratégie de planification, 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. La fonctionnalité d'ordre de déploiement est uniquement prise en charge avec le mode 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 stratégies, applications, actions et 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 et applications) 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 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 et les stratégies d'appareil 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 ces conditions et d'autres critères que vous pouvez associer à des objets ou ressources spécifiques pour les filtrer ou contrôler leur déploiement.

Objet/Ressource	**Filtre/Critères de contrôle**
Stratégies d'appareil	La plate-forme de l'appareil Règle de déploiement (basée sur les propriétés d'appareil) Une planification du déploiement
App	La plate-forme de l'appareil Règle de déploiement (basée sur les propriétés d'appareil) Une planification du déploiement
Action	Règle de déploiement (basée sur les propriétés d'appareil) Une planification du déploiement
Groupe de mise à disposition	Utilisateur/ groupes Règle de déploiement (basée sur les propriétés d'appareil)

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. Déterminez 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 (stratégies, actions et applications) dans les groupes de mise à disposition sélectionnés qui s'appliquent en fonction des filtres de la plate-forme de l'appareil, des règles de déploiement et du 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 celles 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 celles provenant du groupe de mise à disposition B.

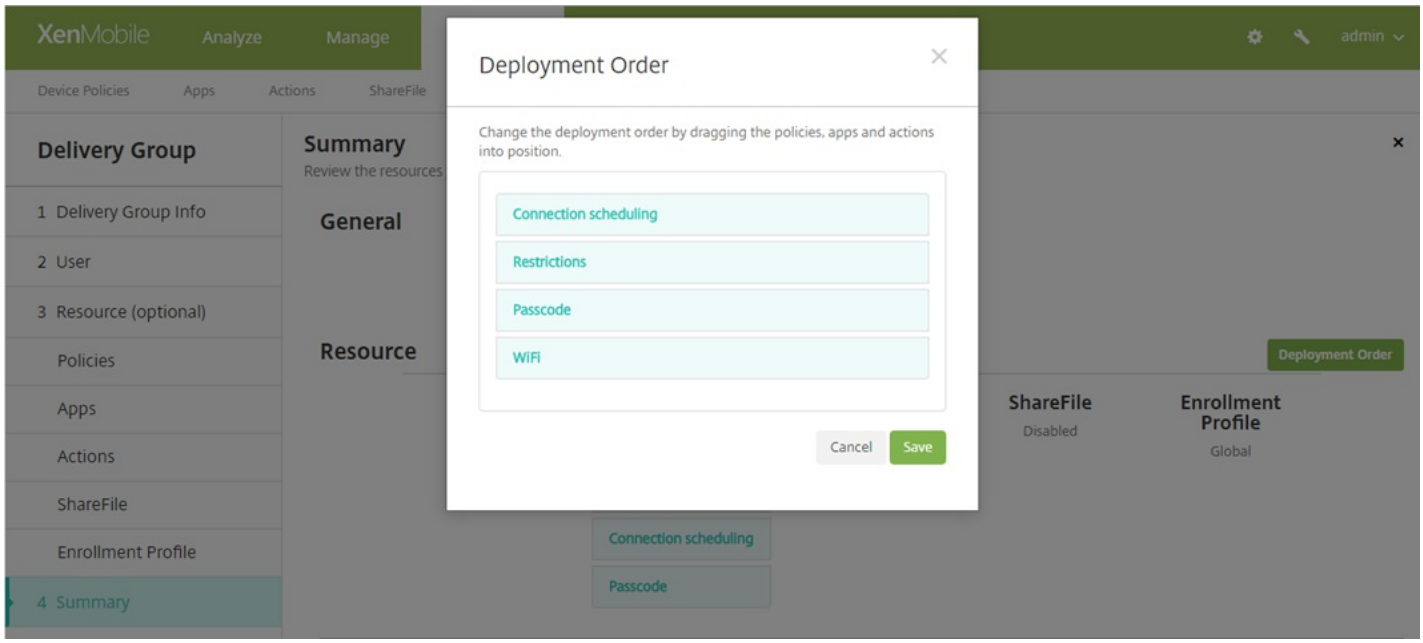
c. Tout en effectuant le tri, si un ordre de déploiement défini par un utilisateur est spécifié pour les ressources d'un groupe de mise à disposition, conservez cet ordre. Sinon, triez les ressources dans ce groupe de mise à disposition par nom de ressource.

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 délivre uniquement la première ressource dans cette liste. En supprimant les ressources dupliquées 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**.



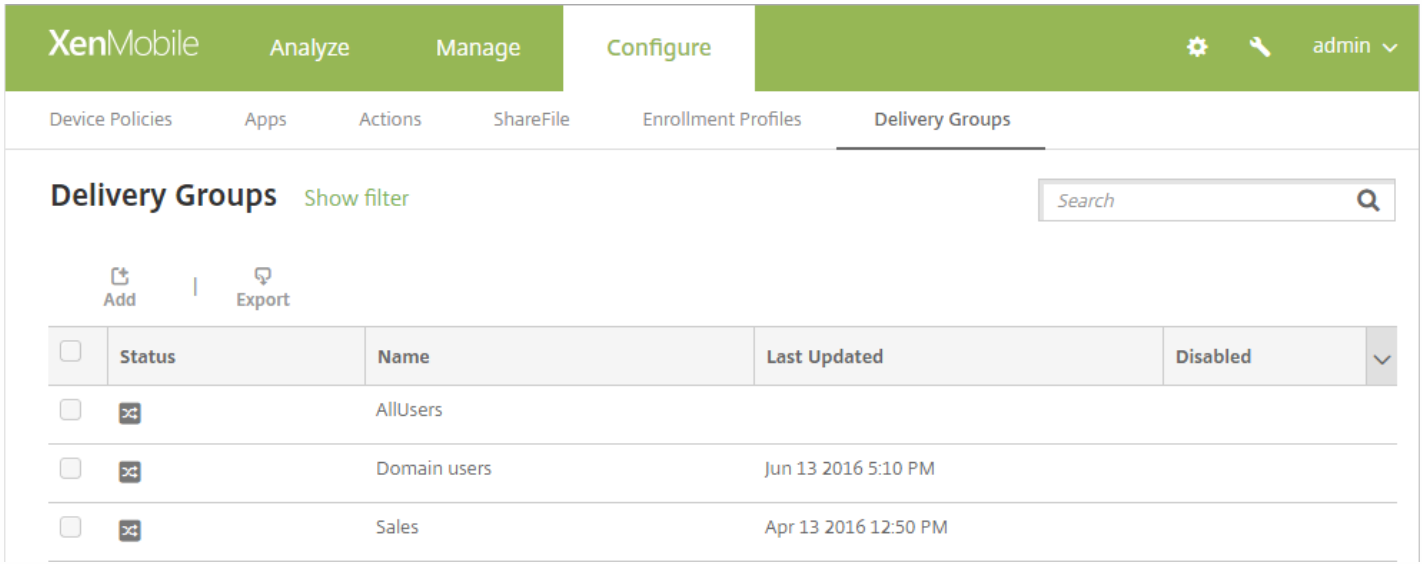
Si l'algorithme de calcul classe uniquement les groupes de déploiement par nom, XenMobile réaliserait le déploiement dans cet ordre, en commençant par le groupe de mise à disposition Gestionnaires de comptes 1 : **Wi-Fi**, **Code secret**, **Planification de connexion** et **Restrictions**. XenMobile ignorerait **Code secret** et **Wi-Fi**, des doublons du groupe de mise à

disposition Gestionnaires de comptes 2.

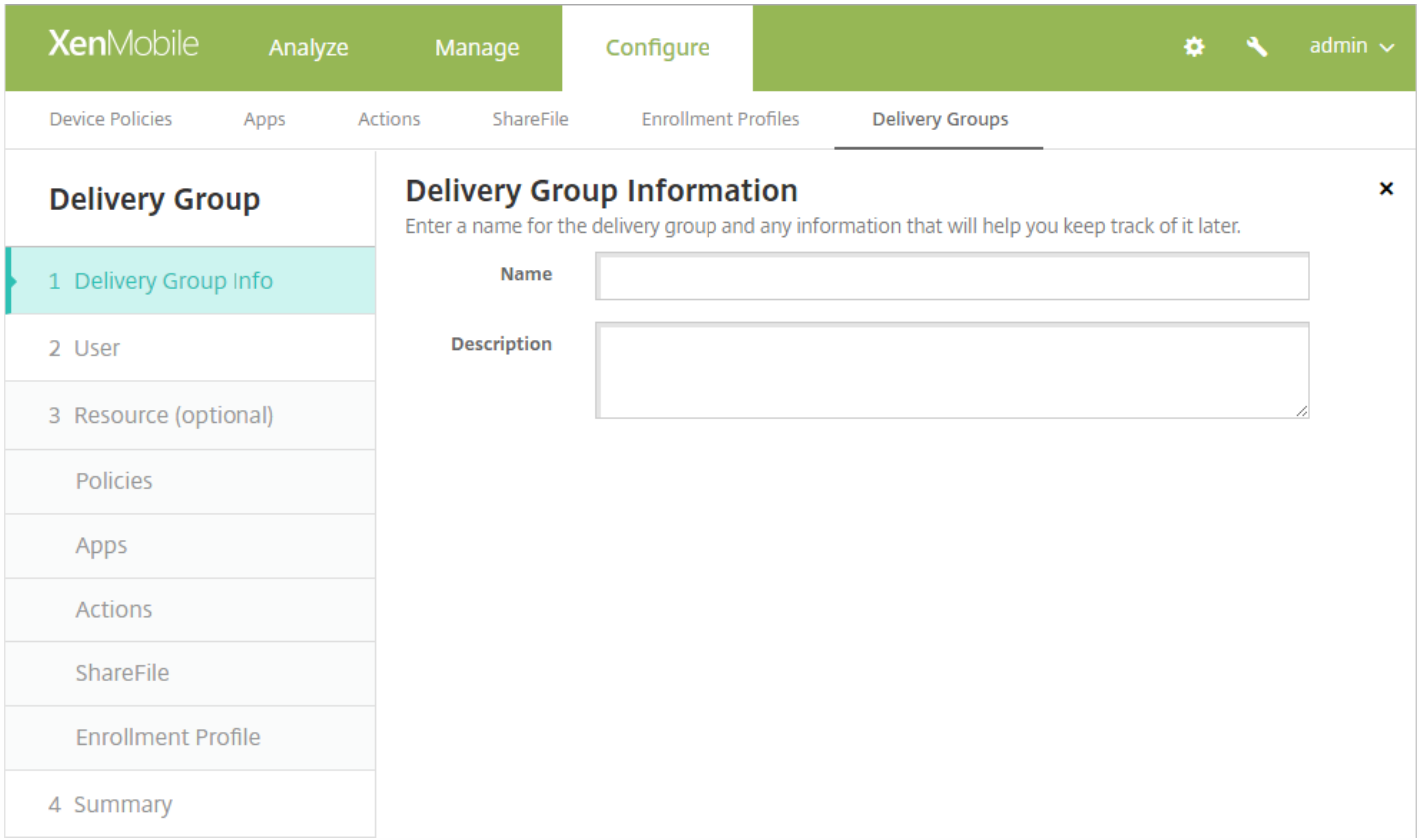
Toutefois, étant donné que l'ordre de déploiement du groupe Gestionnaires de comptes 2 a été spécifié par un administrateur, l'algorithme de calcul place les ressources du groupe de mise à disposition Gestionnaires de comptes 2 plus haut dans la liste que celles du groupe de mise à disposition Gestionnaires de comptes 1. 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.

Pour ajouter un groupe de mise à disposition

1. Dans la console XenMobile, cliquez sur **Configurer > Groupes de mise à disposition**. La page **Groupes de mise à disposition** s'affiche.



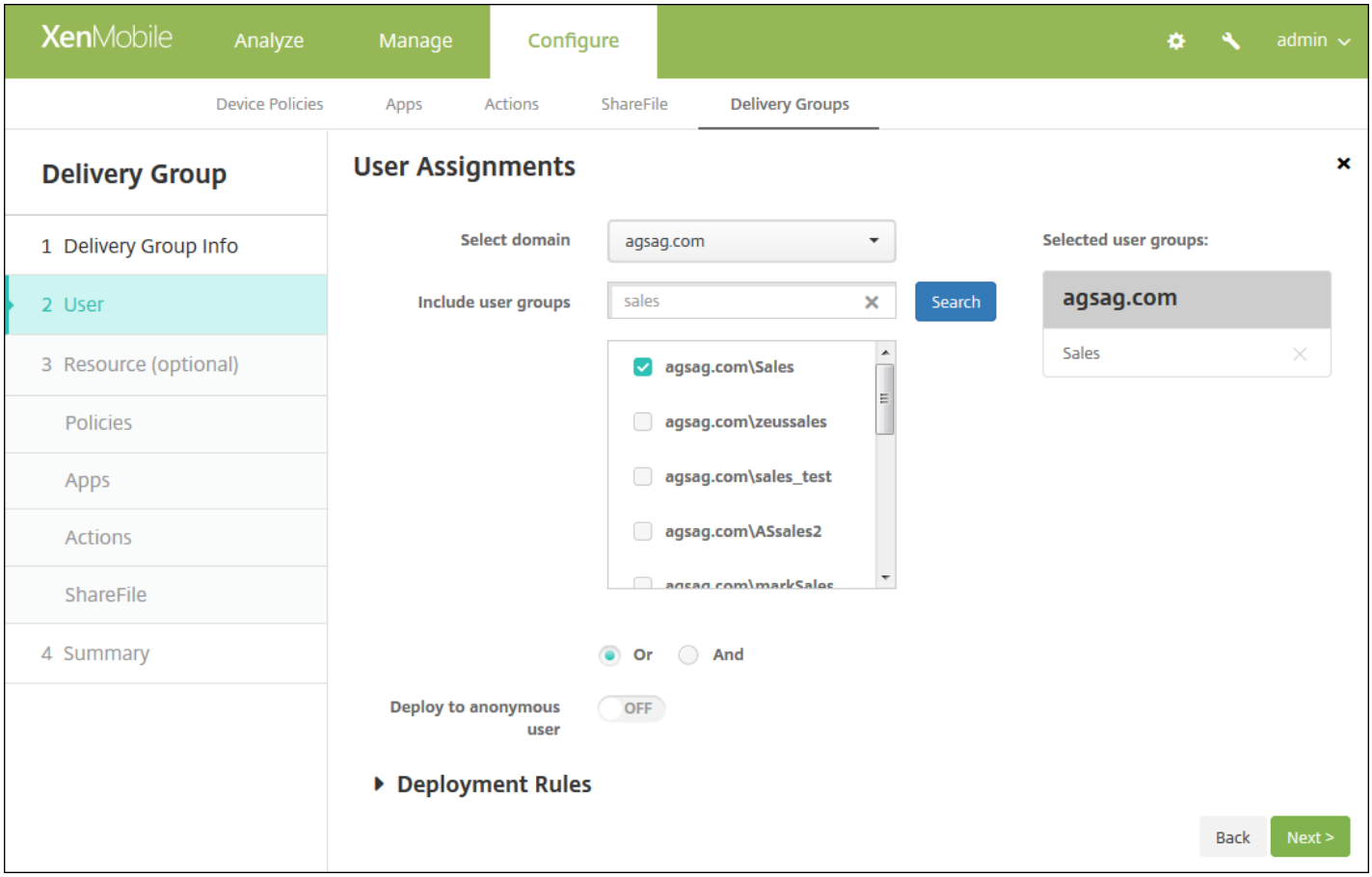
2. Depuis la page **Groupes de mise à disposition** , cliquez sur **Ajouter**. La page **Informations sur le groupe de mise à disposition** s'affiche.



3. Sur la page **Informations sur le groupe de mise à disposition**, entrez les informations suivantes :

- **Nom** : entrez un nom descriptif pour le groupe de mise à disposition.
- **Description** : entrez une description pour le groupe de mise à disposition (facultatif).

4. Cliquez sur **Suivant**. La page **Attributions utilisateur** s'affiche.



5. Configurez les paramètres suivants :

- **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.

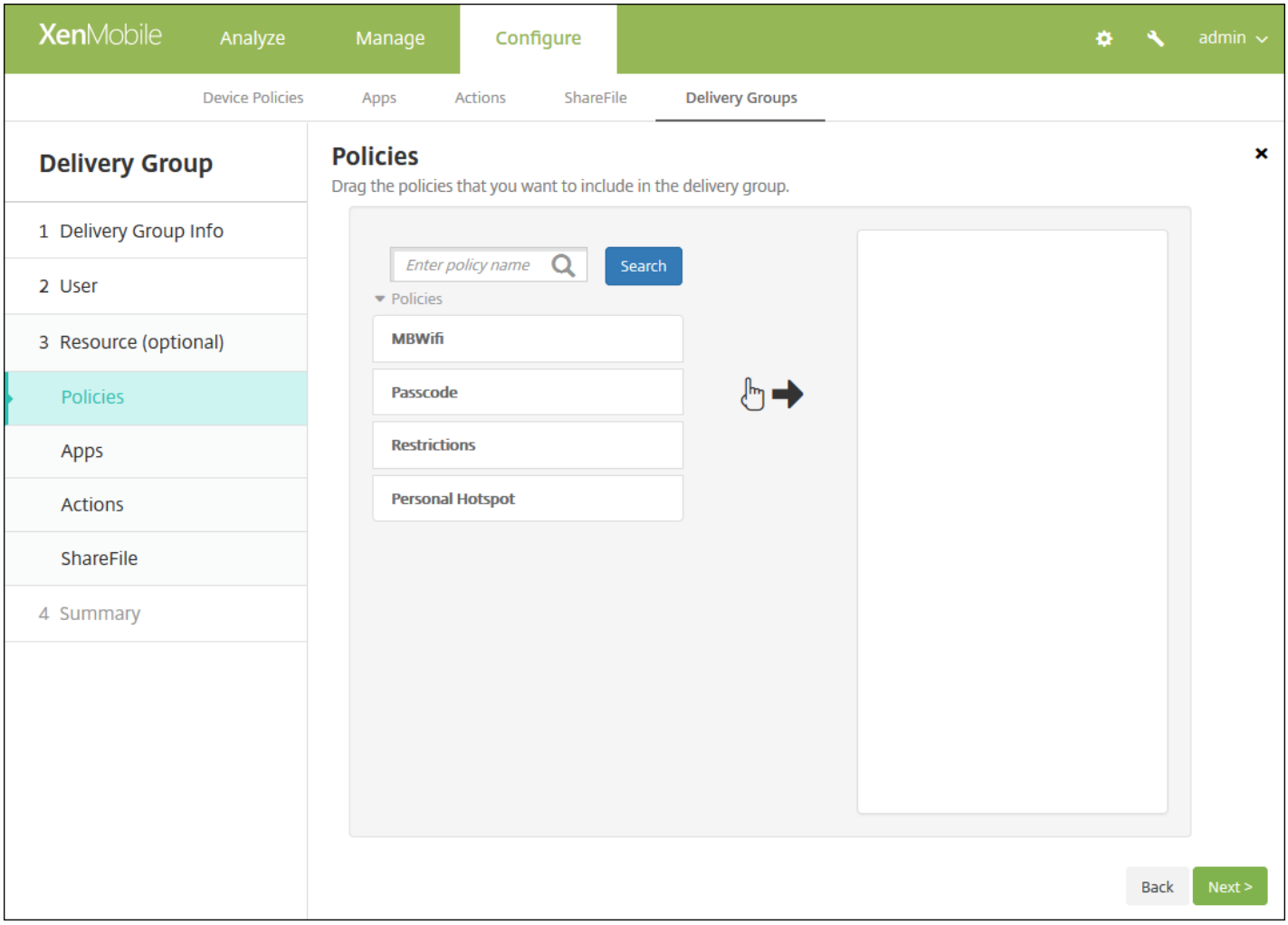
Remarque : les utilisateurs non authentifiés sont des utilisateurs que vous n'avez pas réussi à authentifier, mais dont les appareils sont autorisés à se connecter à XenMobile.

6. Configurez les règles de déploiement.

Pour ajouter des ressources supplémentaires pour les groupes de mise à disposition

Vous pouvez ajouter des ressources supplémentaires pour les groupes de mise à disposition pour appliquer des stratégies spécifiques, fournir les applications obligatoires et facultatives, ajouter des actions automatiques et activer ShareFile pour l'authentification unique pour le contenu et les données. Les sections suivantes décrivent comment ajouter des stratégies, des applications et des actions et comment activer ShareFile. Vous pouvez ajouter n'importe quelle de ces ressources, toutes ou aucune pour le groupe de mise à disposition. Pour ajouter une ressource, cliquez sur la ressource, ou cliquez sur **Résumé** pour ne pas ajouter de ressource.

Ajouter des stratégies



1. Pour chaque stratégie que vous voulez ajouter, procédez comme suit :

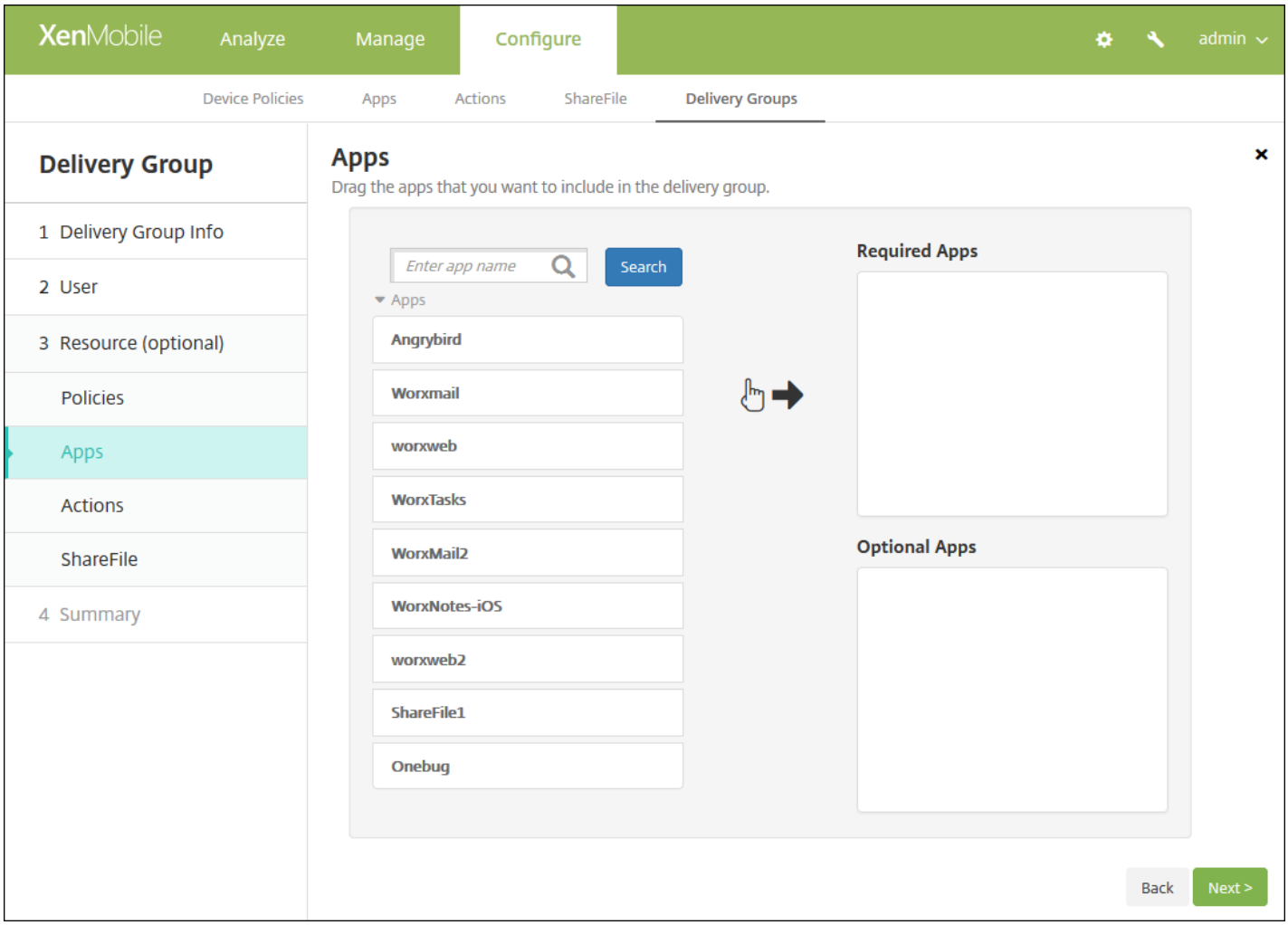
- Parcourez la liste des stratégies disponibles pour trouver la stratégie que vous souhaitez ajouter.
- Ou pour limiter la liste des stratégies, entrez un nom de stratégie complet ou partiel dans la zone de recherche et cliquez sur **Rechercher**.

- Cliquez sur la stratégie que vous souhaitez ajouter et faites-la glisser dans la zone de droite.

Remarque : pour supprimer une stratégie, cliquez sur le **X** en regard du nom de la stratégie dans la zone de droite.

2. Cliquez sur **Next**. La page **Applications** s'affiche.

Ajouter des applications.



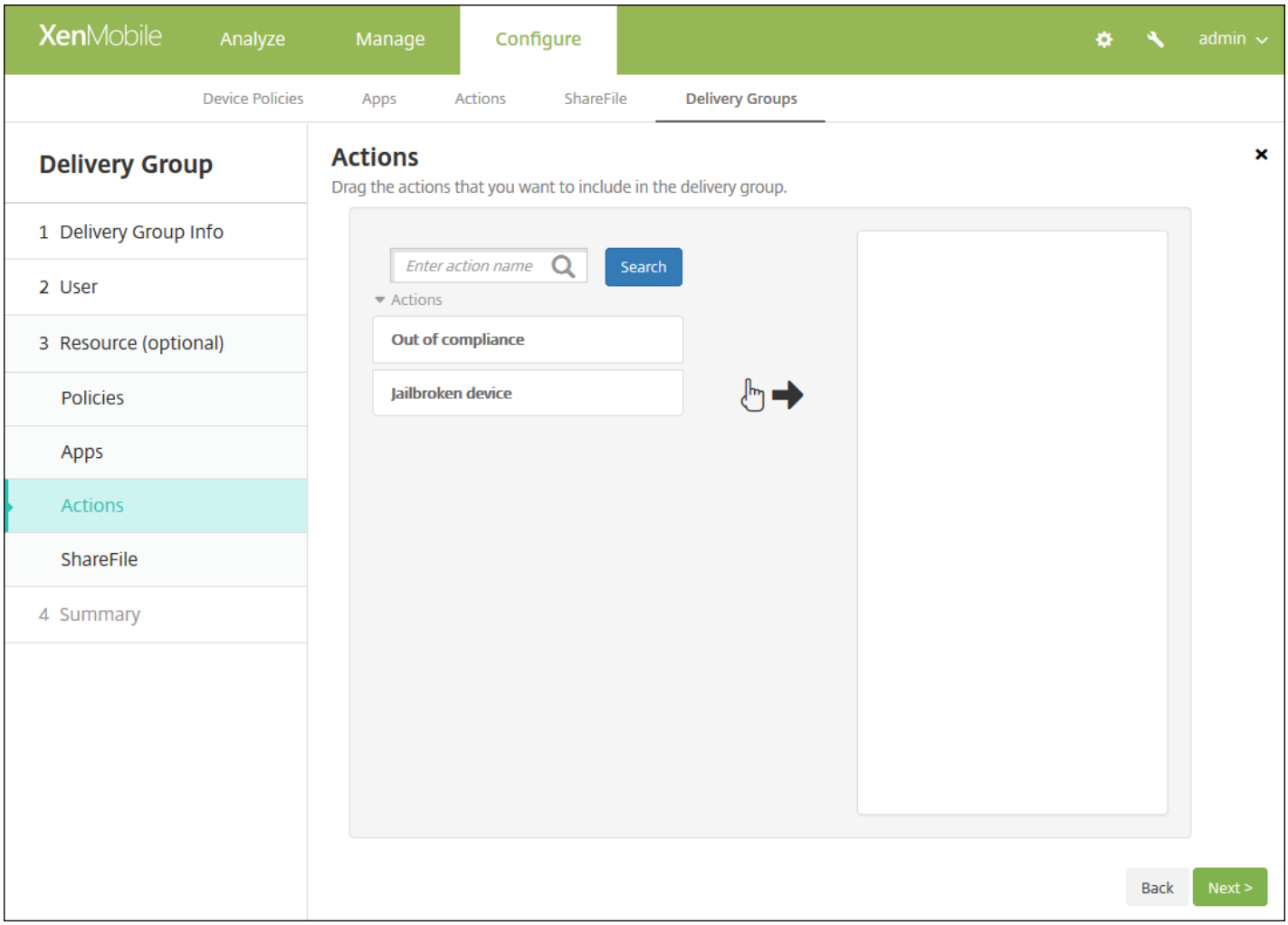
1. Pour chaque application que vous voulez ajouter, procédez comme suit :

- 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**.

Remarque : pour supprimer une application, cliquez sur le **X** en regard du nom de l'application dans la zone de droite.

2. Cliquez sur **Next**. La page **Actions** s'affiche.

Ajouter des actions



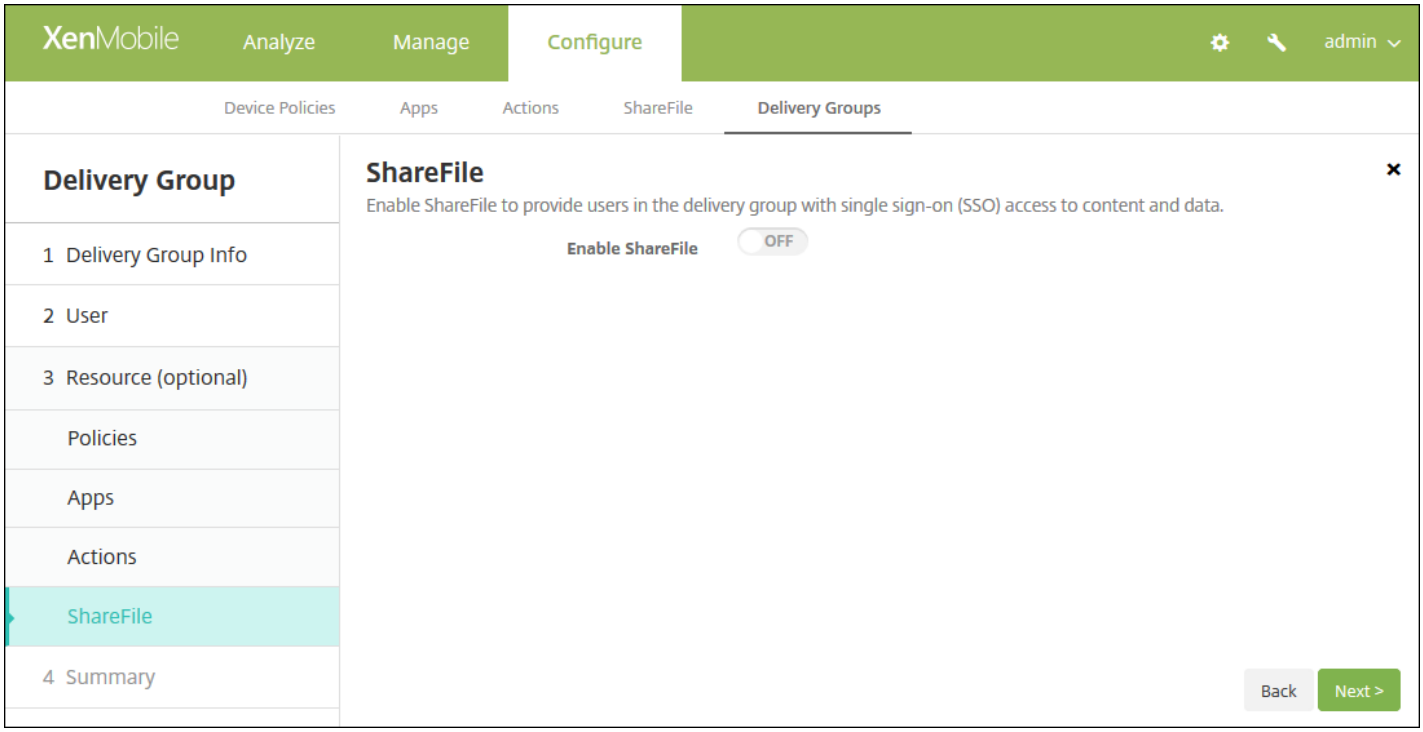
1. Pour chaque action que vous souhaitez ajouter, procédez comme suit :

- 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.

Remarque : pour supprimer une action, cliquez sur le **X** en regard du nom de l'action dans la zone de droite.

2. Cliquez sur **Next**. La page **ShareFile** s'ouvre.

Activer ShareFile

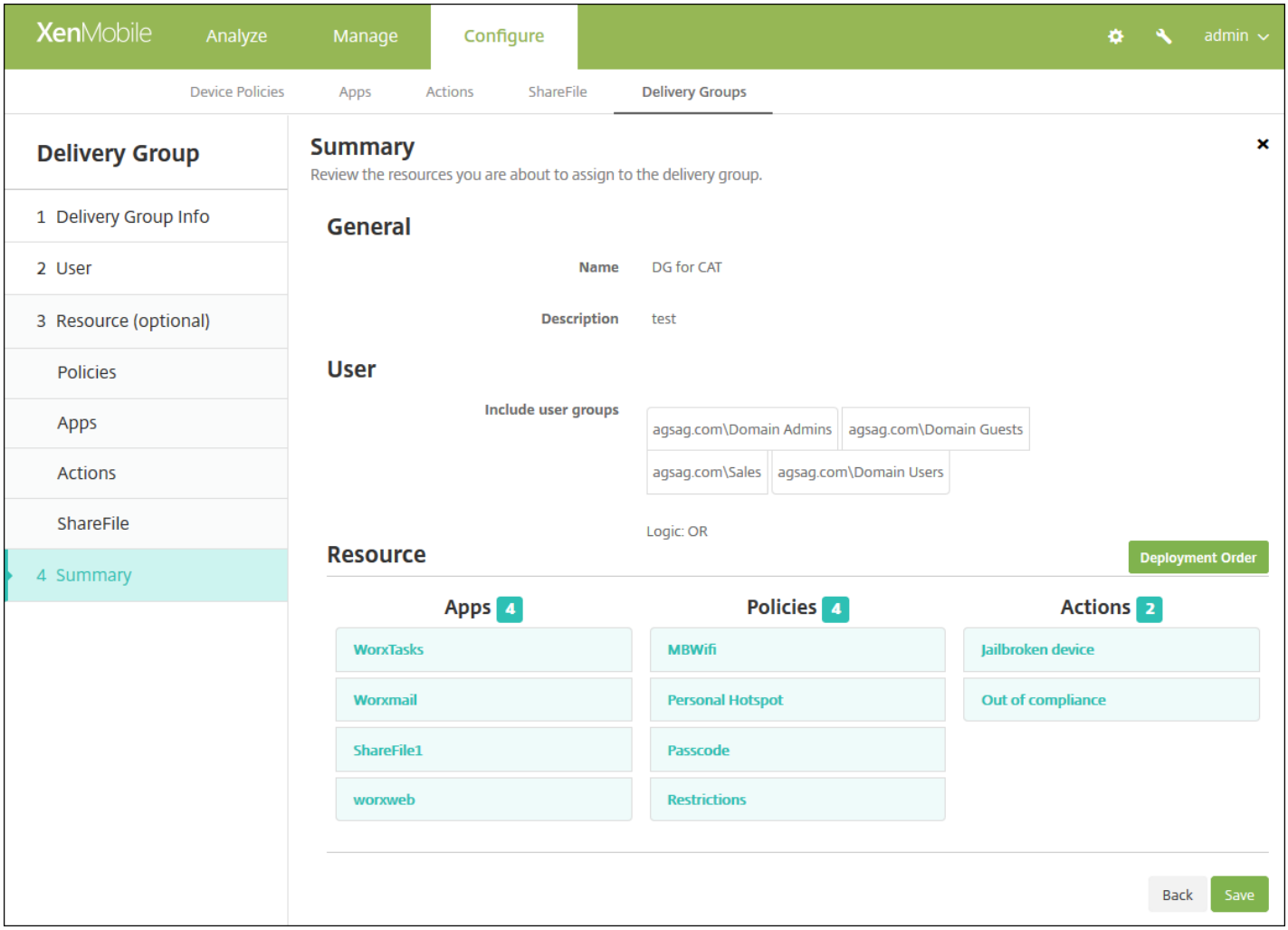


1. Configurez ce paramètre :

- **Activer ShareFile** : cliquez sur **ON** pour activer l'accès par authentification unique ShareFile au contenu et aux données.

2. Cliquez sur **Next**. La page **Résumé** s'affiche.

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 ; elle ne pas reflète pas l'ordre de déploiement.

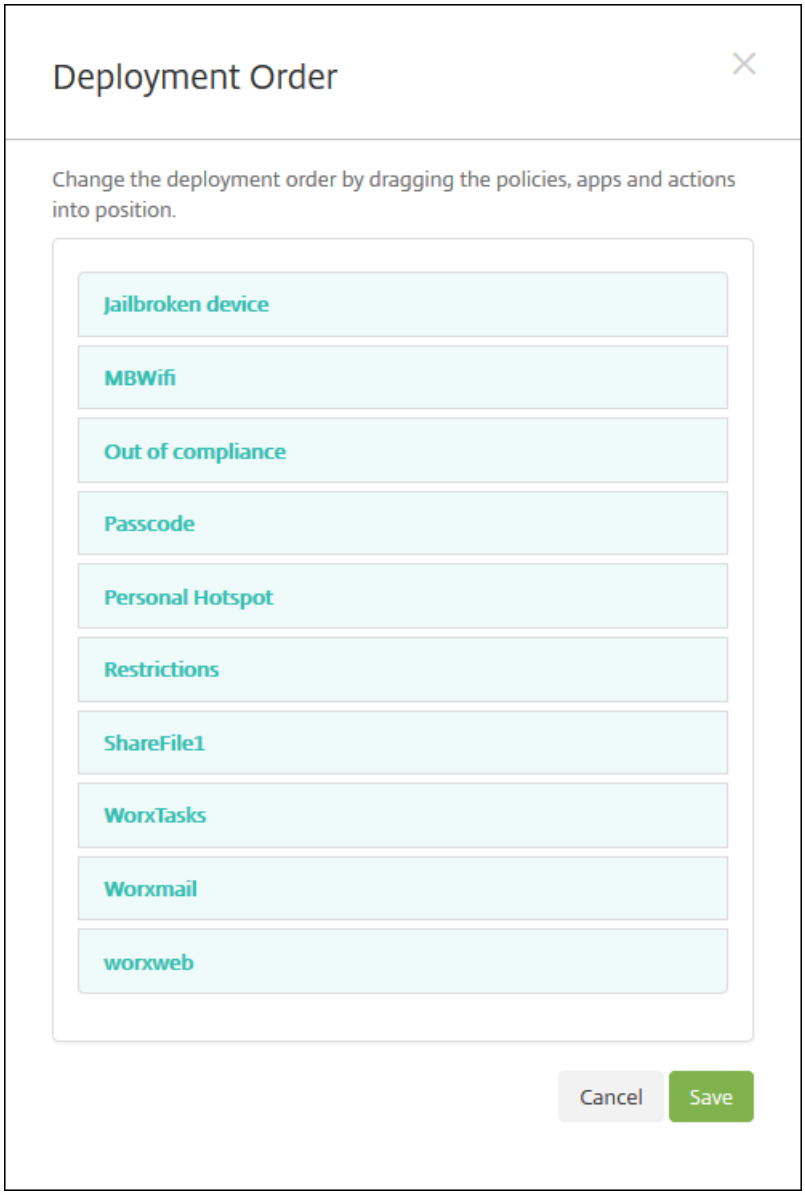
1. Cliquez sur **Précédent** pour revenir sur les pages précédentes pour modifier la configuration le cas échéant.

2. Cliquez sur **Ordre de déploiement** pour afficher l'ordre de déploiement ou réorganiser l'ordre de déploiement.

3. Cliquez sur **Enregistrer** pour enregistrer le groupe de mise à disposition.

Pour modifier l'ordre de déploiement

1. Cliquez sur le bouton **Ordre de déploiement**. La boîte de dialogue **Ordre de déploiement** s'affiche.



2. 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.

3. Cliquez sur **Enregistrer** pour enregistrer l'ordre de déploiement.

Pour modifier un groupe de mise à disposition

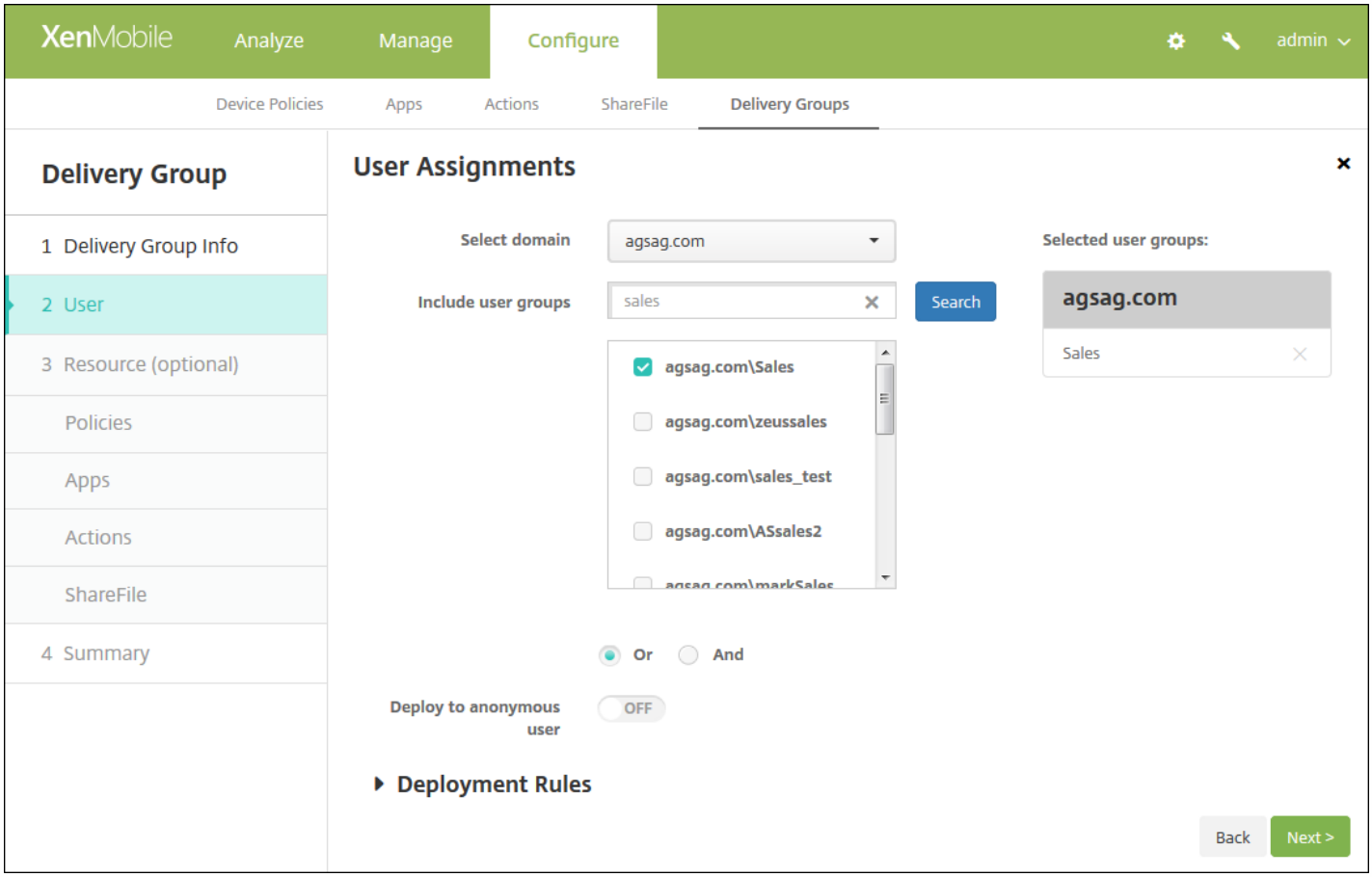
1. Sur la page **Groupes de mise à disposition**, sélectionnez le groupe de mise à disposition que vous voulez modifier en sélectionnant la case à cocher en regard de son nom ou en cliquant sur la ligne contenant son nom, puis cliquez sur **Modifier**. La page de modification des **Informations sur le groupe de mise à disposition** s'affiche.

> **Remarque**
>
> En fonction de la manière dont vous avez sélectionné le groupe de mise à disposition, la commande **Modifier** apparaît au-dessus ou à droite du groupe de mise à disposition.

2. Ajoutez ou modifiez la **description**.

Remarque : vous ne pouvez pas modifier le nom d'un groupe existant.

3. Cliquez sur **Suivant**. La page **Attributions utilisateur** apparaît.



4. Sur la page **Sélectionner des groupes d'utilisateurs**, entrez ou modifiez les informations suivantes :

- **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.

    Remarque : pour supprimer des groupes d'utilisateurs, cliquez sur **Rechercher**, puis dans la liste des groupes d'utilisateurs, désactivez la case à cocher en regard du groupe ou des groupes que vous souhaitez supprimer. Vous pouvez taper un nom de groupe complet ou partiel dans la zone de recherche, puis cliquez sur **Rechercher** pour limiter le nombre de groupes d'utilisateurs affichés dans la liste.

- **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 le déploiement.
- **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.

Remarque : 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. Développez **Règles de déploiement** et configurez les paramètres comme à l'étape 5 de cette procédure.

6. Cliquez sur **Suivant**. La page **Ressources du groupe de mise à disposition** s'affiche. Ajoutez ou supprimez des stratégies, des applications ou des actions. 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.

7. Lorsque vous avez terminé de modifier une ressource, cliquez sur **Suivant** ou sous **Groupe de mise à disposition**, cliquez sur **Résumé**.

8. 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.

9. Cliquez sur **Précédent** pour revenir sur les pages précédentes pour modifier la configuration le cas échéant.

10. Cliquez sur **Ordre de déploiement** pour réorganiser l'ordre de déploiement des ressources ; pour plus d'informations sur la modification de l'ordre de déploiement, consultez la section Pour modifier l'ordre de déploiement.

11. Cliquez sur **Enregistrer** pour enregistrer le groupe de mise à disposition.

Pour activer et désactiver le groupe de mise à disposition AllUsers

> **Remarque**
>
> AllUsers est le seul groupe de mise à disposition que vous pouvez activer ou désactiver.

1. Dans 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 :

Remarque : en fonction de la manière dont vous avez sélectionné AllUsers, la commande **Activer** ou **Désactiver** apparaît au-dessus ou à droite du groupe de mise à disposition AllUsers.

- 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 qui appartiennent 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. Les utilisateurs équipés d'autres plates-formes reçoivent les ressources immédiatement s'ils sont déjà connectés, ou en fonction de leur stratégie de planification, la prochaine fois qu'ils se connectent.

Remarque : pour mettre à jour les applications affichées dans la liste des applications disponibles dans le Worx 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.

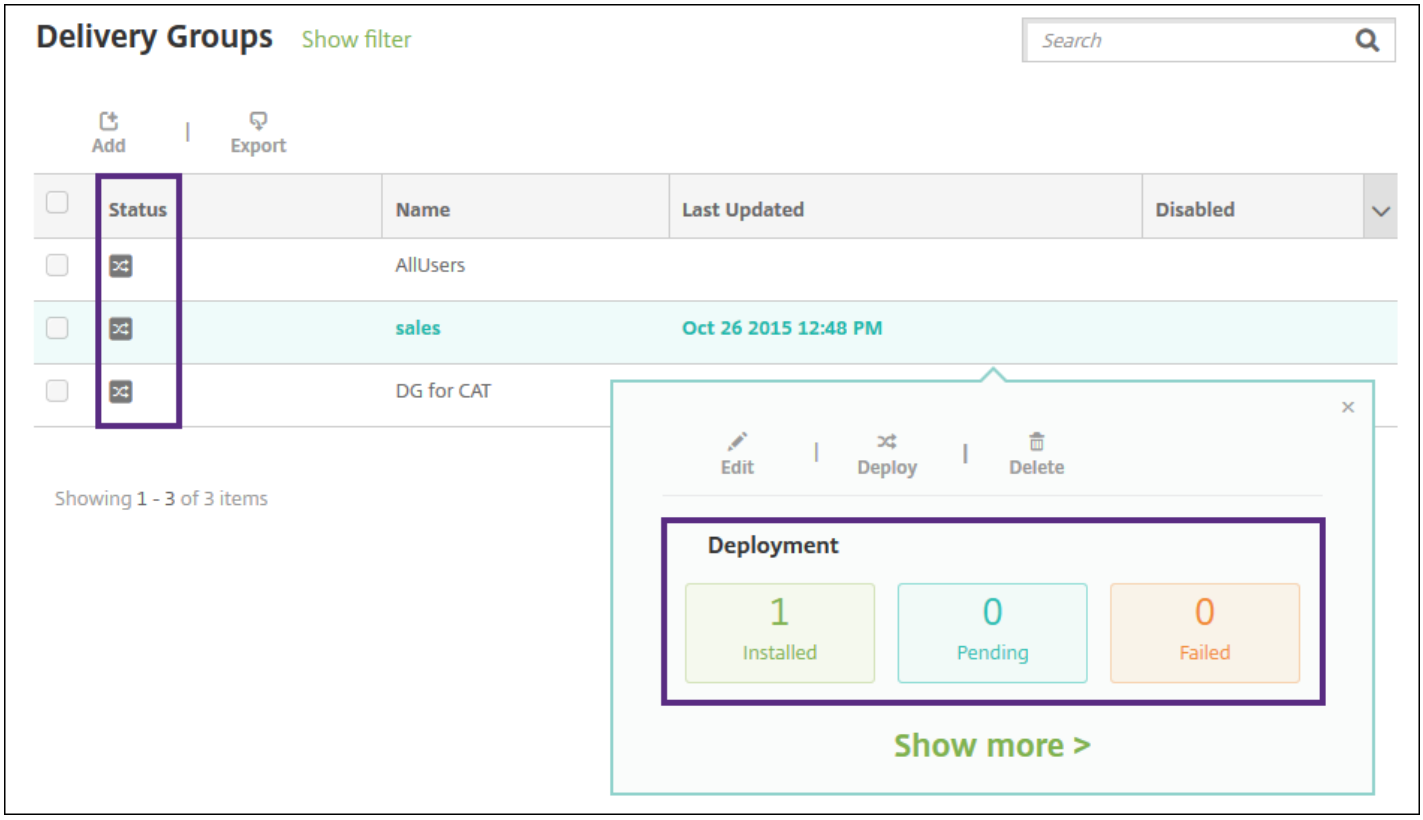
2. Cliquez sur **Déployer**.

Remarque : 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

> **Remarque**
>
> 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.

Remarque : 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.

3. Cliquez sur **Supprimer**.

> **Important**
>
> vous ne pouvez pas annuler cette opération.

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. Cette opération dépend du navigateur que vous utilisez. Vous pouvez également annuler l'opération.

Inscription d'utilisateurs et d'appareils

Aug 22, 2016

Pour gérer les appareils utilisateur à distance et de manière sécurisée, ces derniers doivent être inscrits dans XenMobile. Le logiciel client XenMobile est installé sur l'appareil utilisateur et l'identité de l'utilisateur est authentifiée, suivi de XenMobile et du profil de l'utilisateur. Une fois que les appareils sont inscrits dans la console XenMobile, vous pouvez effectuer des tâches de gestion sur l'appareil, telles que l'application de stratégies, le déploiement d'applications, l'envoi de données sur l'appareil, le verrouillage, l'effacement, et la localisation des appareils perdus ou volés.

Remarque : avant de pouvoir inscrire des utilisateurs d'appareils iOS, vous devez demander un certificat APNS. Consultez la section Certificats dans XenMobile pour plus d'informations.

Pour accéder aux options de configuration pour les utilisateurs et appareils dans la console XenMobile, cliquez sur **Configurer > Inscription** :

Appareils Android

Jul 27, 2016

1. Accédez au magasin Google Play ou Amazon App sur votre Android et téléchargez l'application Citrix Worx Home, puis tapotez sur l'application.
2. Lorsque vous êtes invité à installer l'application, cliquez sur Suivant, puis cliquez sur Installer.
3. Après l'installation de Worx Home, touchez Ouvrir.
4. Entrez vos informations d'identification d'entreprise, telles que le nom du serveur XenMobile de votre organisation, le nom d'utilisateur principal (UPN), ou votre adresse e-mail et cliquez 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 Worx, que vous pouvez utiliser pour vous connecter à Worx Home et à d'autres applications Worx, telles que WorxMail, WorxWeb, ShareFile, et bien plus encore. Vous devez entrer votre code PIN Worx deux fois. Sur l'écran Créer un code PIN Worx, entrez un code PIN contenant une série de six chiffres.
8. Entrez de nouveau le code PIN. Worx Home s'ouvre. Vous pouvez ensuite accéder à Worx 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 des utilisateurs après l'inscription, des messages les inviteront à installer les applications. Cliquez sur Installer pour installer les applications.

Pour désinscrire et réinscrire un appareil Android

Avant de réinscrire un appareil, il doit d'abord être désinscrit. Durant la période pendant laquelle l'appareil est désinscrit mais pas encore réinscrit, ce dernier n'est pas géré par XenMobile, bien qu'il apparaisse toujours dans l'inventaire des appareils dans la console XenMobile. Vous ne pouvez pas suivre l'appareil ni vérifier s'il respecte les exigences de conformité lorsqu'il n'est pas géré par XenMobile.

1. Touchez pour ouvrir l'application Worx Home.
2. Touchez l'icône Paramètres en haut à gauche de la fenêtre d'application.
3. Touchez Re-Enroll. Un message s'affiche afin de confirmer que vous souhaitez réinscrire votre appareil.
4. Touchez OK. Cela entraîne la désinscription de l'appareil.
5. Suivez les instructions à l'écran pour réinscrire votre appareil.

Appareils iOS

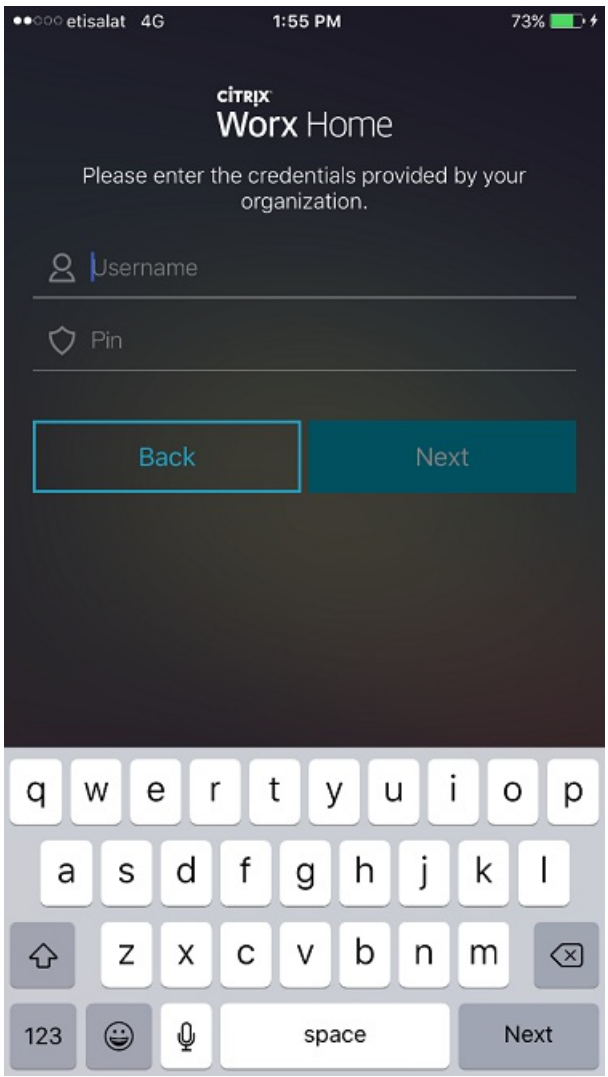
Jul 27, 2016

1. Téléchargez l'application Worx Home à partir de l'App Store Apple iTunes sur l'appareil, puis installez l'application sur l'appareil.

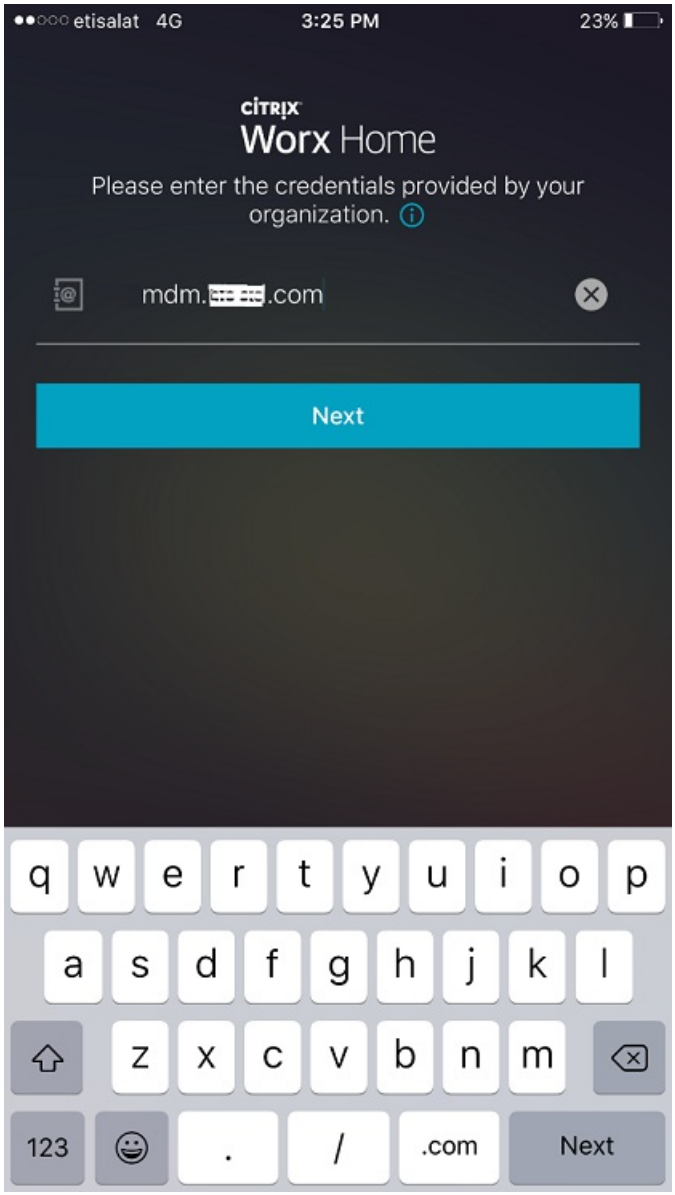
2. Sur l'écran d'accueil de l'appareil iOS, tapotez l'application Worx Home.

3. Lorsque l'application Worx Home s'affiche, entrez vos informations d'identification d'entreprise, telles que le nom du serveur XenMobile de votre entreprise, le nom d'utilisateur principal (UPN), ou votre adresse e-mail et cliquez sur **Suivant**.

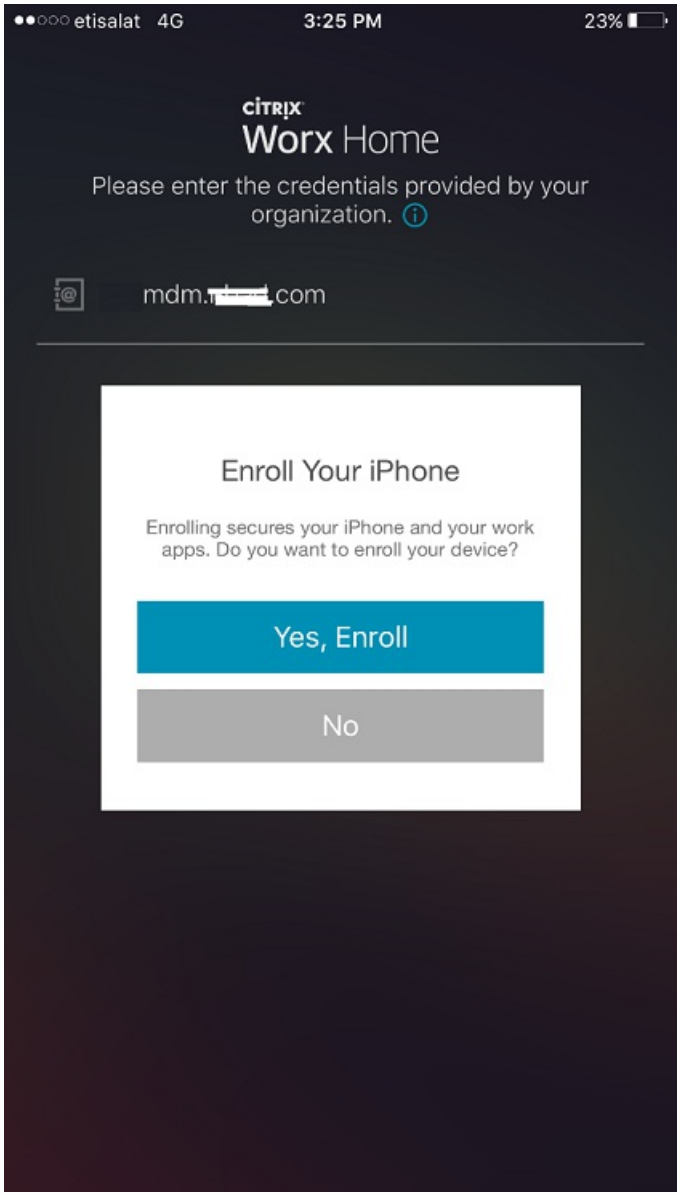
Les écrans présentés peuvent différer de ces exemples en fonction de la façon dont XenMobile est configuré.

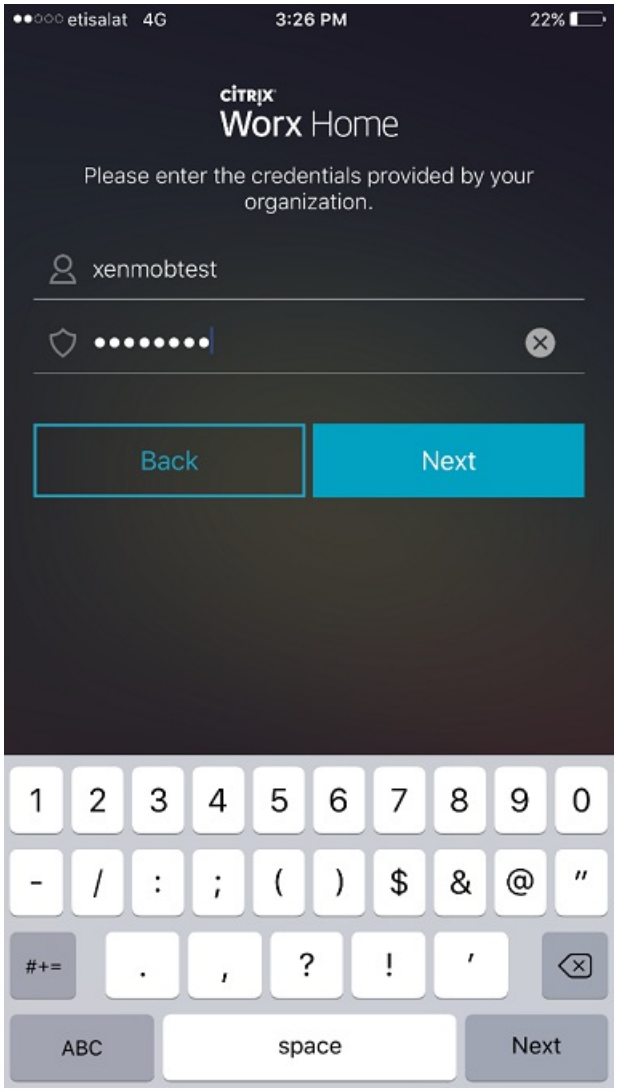


4. Entrez l'adresse fournie par votre service d'assistance.



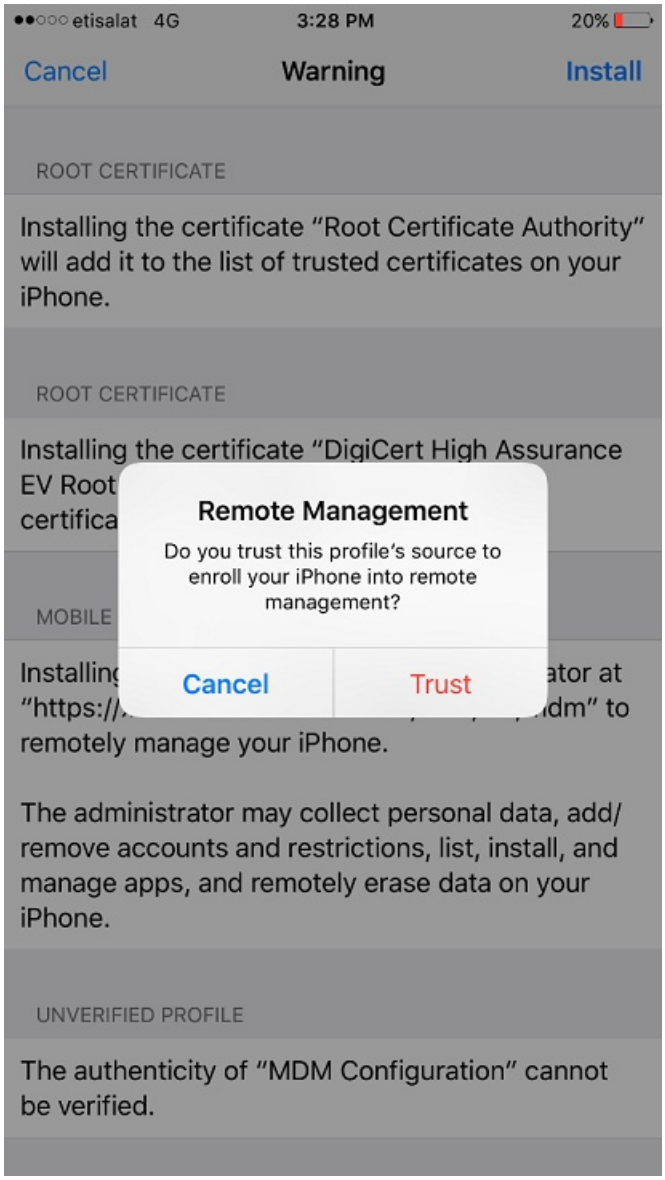
5. Lorsque vous êtes invité à vous inscrire, cliquez sur **Oui, inscrire** et entrez vos informations d'identification lorsque vous y êtes invité.



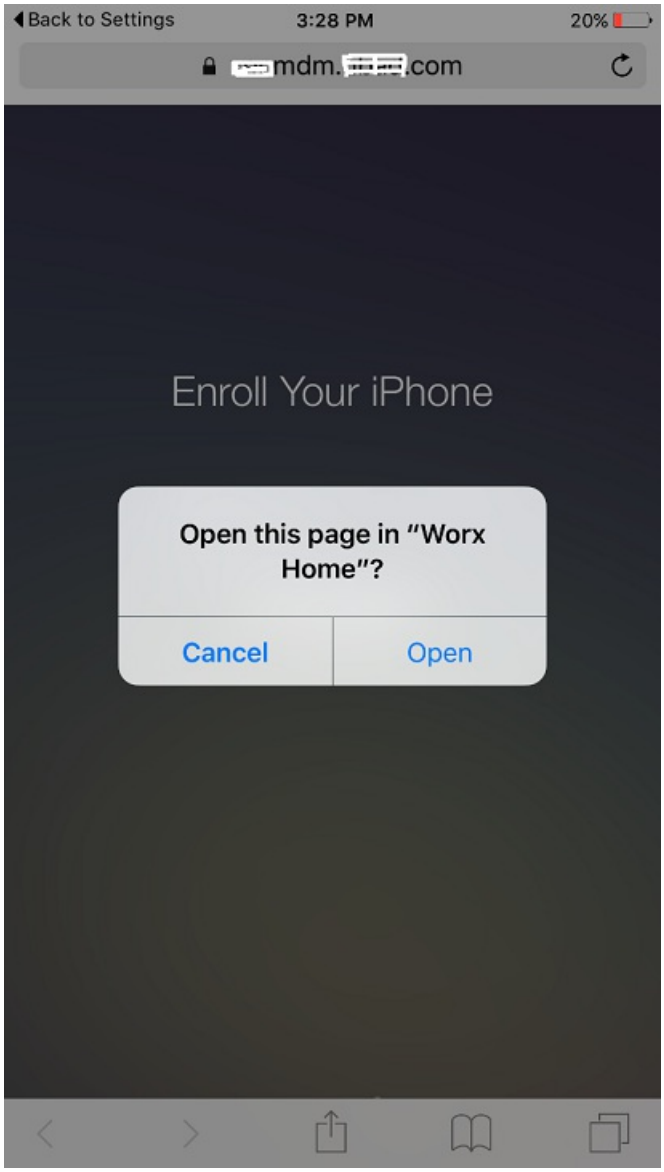


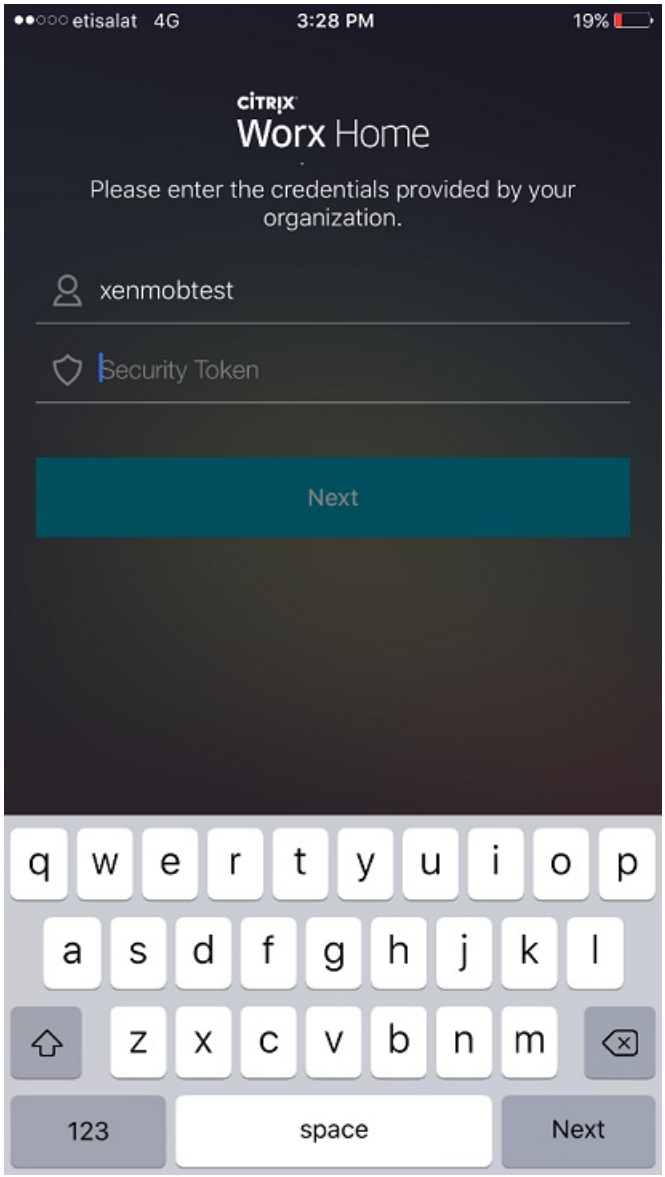
6. Cliquez sur **Installer** pour installer Citrix Profile Services.

7. Appuyez sur **Faire confiance**.



8. Appuyez sur **Ouvrir** puis entrez vos informations d'identification.





Appareils Mac OS X

Jul 27, 2016

Vous pouvez inscrire dans XenMobile des appareils Mac qui exécutent Mac OS X. Les utilisateurs Mac s'inscrivent directement à partir de leurs appareils.

Les étapes permettant d'inscrire des appareils Mac sont les suivantes :

1. Si vous le souhaitez, vous pouvez définir des stratégies Mac dans la console XenMobile. Consultez la section Stratégies d'appareil pour de plus amples informations sur les stratégies d'appareil. Pour savoir quelles stratégies d'appareils vous pouvez configurer pour Mac, consultez la section Stratégies XenMobile par plate-forme.

2. Envoyez le lien d'inscription https://FQDNserveur:8443/zdm/macos/otae, que les utilisateurs ouvrent dans Safari. Où

- FQDNserveur 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.
- Zdm est le nom d'instance utilisé 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. Les utilisateurs sont invités à installer des certificats si vous avez configuré un certificat SSL approuvé publiquement et un certificat de signature numérique approuvé publiquement pour iOS et Mac OS. Pour de plus amples informations sur les certificats, consultez Certificats.

4. Les utilisateurs se connectent à leur Mac.

5. Les stratégies Mac s'installent.

Vous pouvez maintenant démarrer la gestion des Mac avec XenMobile tout comme vous gérez les appareils mobiles.

Appareils Windows

Jul 27, 2016

Vous pouvez inscrire des appareils dans XenMobile qui exécutent les systèmes d'exploitation Windows suivants :

- Windows 8.1 et 10
- Windows Phone 8.1 et 10

Les utilisateurs Windows et Windows Phone s'inscrivent directement au travers de leurs appareils.

Vous devez configurer la découverte automatique et le service de découverte Windows pour l'inscription de l'utilisateur afin d'autoriser la gestion des appareils Windows et Windows Phone.

> ## Remarque
>
> Pour pouvoir inscrire des appareils Windows, le certificat d'écoute SSL doit être un certificat SSL. L'inscription échoue si vous avez chargé un certificat SSL auto-signé.

Pour inscrire des appareils Windows à l'aide de la découverte automatique

Les utilisateurs peuvent inscrire des appareils exécutant Windows RT 8.1, les versions 32 bits et 64 bits de Windows 8.1 Professionnel et Windows 8.1 Entreprise et Windows 10. Pour activer la gestion des appareils Windows, Citrix vous recommande de configurer la découverte automatique ainsi que le service de découverte Windows. Pour de plus amples informations, consultez la section Pour activer la découverte automatique pour l'inscription utilisateur dans XenMobile.

1. Sur l'appareil, recherchez et installez toutes les mises à jour Windows disponibles. Cette étape est particulièrement importante lors de la mise à niveau de Windows 8 vers Windows 8.1 car les utilisateurs risquent de ne pas être automatiquement avertis de toutes les mises à jour disponibles.

2. Dans le menu Icônes, touchez **Paramètres** et :

- Pour Windows 8.1, touchez **Réseau** > **Lieu de travail**.
- Pour Windows 10, touchez **Comptes** > **Accès professionnel** > **S'inscrire à MDM**.

3. Entrez votre adresse de messagerie d'entreprise, puis touchez **Activer** sur Windows 8.1, ou **Continuer** sur Windows 10. Pour vous inscrire en tant qu'utilisateur local, entrez une nouvelle adresse de messagerie avec le nom de domaine correct (par exemple, foo@mondomaine.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 un serveur XenMobile 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 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 Windows 10, dans la boîte de dialogue des **conditions d'utilisation**, indiquez que vous acceptez que votre appareil soit géré, puis touchez **Accepter**.

Pour inscrire des appareils Windows sans découverte automatique

Il est possible d'inscrire des appareils Windows sans découverte automatique. Cependant, Citrix vous recommande de configurer la découverte automatique. L'inscription sans découverte 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. Cette étape est particulièrement importante lors de la mise à niveau de Windows 8 vers Windows 8.1 car les utilisateurs risquent de ne pas être automatiquement avertis de toutes les mises à jour disponibles.

2. Dans le menu Icônes, touchez **Paramètres** et :

- Pour Windows 8.1, touchez **Réseau** > **Lieu de travail**.
- Pour Windows 10, touchez **Comptes** > **Accès professionnel** > **S'inscrire à MDM**.

3. Entrez votre adresse de messagerie d'entreprise.

4. Sur Windows 10, si la découverte automatique n'est pas configurée, une option vous permettant d'entrer les détails du serveur apparaît, comme décrit dans l'étape 5. Sur Windows 8.1, si l'option **Détecter automatiquement l'adresse du serveur** est activée, touchez pour la désactiver.

5. Dans le champ **Entrer l'adresse du serveur** :

- Pour Windows 8.1, tapez l'adresse du serveur au format suivant : https://*fqdnserveur:8443/Instanceserveur*/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.
- Pour Windows 10, utilisez cette adresse : https://beta.managedm.com:8443/zdm/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.

6. Entrez votre mot de passe.

7. 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 Windows 10, dans la boîte de dialogue des **conditions d'utilisation**, indiquez que vous acceptez que votre appareil soit géré, puis touchez **Accepter**.

Pour inscrire les appareils Windows Phone dans XenMobile

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 découverte automatique n'est pas configurée, les utilisateurs ont également besoin de l'adresse Web du serveur XenMobile. 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 Citrix Worx Home Windows Phone 8 signée pour chaque plate-forme que vous prenez en charge).
1. Sur l'écran principal de Windows Phone, touchez l'icône **Paramètres**.

2. Pour Windows Phone 8.1, touchez **Système** > **Lieu de travail** et touchez **Ajouter un compte**. Pour Windows 10 Phone, touchez **Comptes** > **Accès professionnel** > **S'inscrire à MDM**.

3. Dans l'écran suivant, entrez une adresse de messagerie et un mot de passe et touchez **s'inscrire**.

Si la découverte automatique est configurée pour votre domaine, les informations requises dans les étapes suivantes sont automatiquement renseignées. Passez à l'étape 8.

Si la découverte 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@mondomaine.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.

Sur l'écran suivant, entrez l'adresse Web du serveur XenMobile, telle que : https://://wpe. Par exemple : https://monentreprise.mdm.com:8443/zdm/wpe. **Remarque** : le numéro de port doit être adapté à votre implémentation, mais doit être le même port que vous avez utilisé pour une inscription iOS.

5. 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 **s'inscrire**.

6. Si un écran apparaît indiquant un problème avec le certificat, l'erreur est due à l'utilisation d'un certificat auto-signé. Si le serveur est approuvé, touchez **continuer**. Sinon, cliquez sur **Annuler**.

7. 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 touchez **Terminé**. Si vous désactivez cette option, vous devrez réinscrire votre appareil pour recevoir le magasin d'applications d'entreprise.

8. Sur Windows Phone 8.1, sur l'écran **Compte ajouté**, touchez **terminé**.

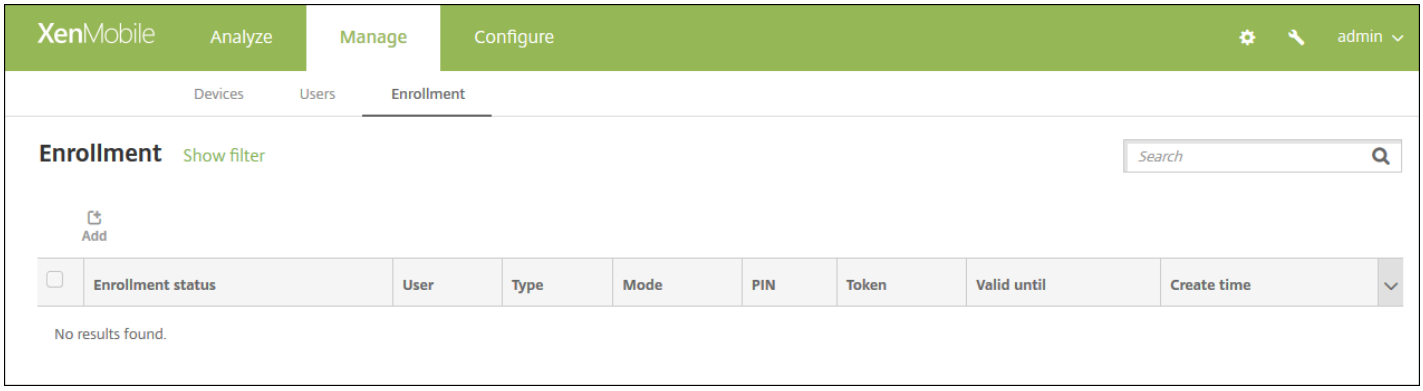
9. Pour forcer une connexion au serveur, touchez l'icône d'actualisation. Si l'appareil ne se connecte pas manuellement au serveur, XenMobile essaye de se reconnecter. XenMobile se connecte à l'appareil toutes les 3 minutes à 5 reprises, puis toutes les 2 heures par la suite. Vous pouvez modifier cet intervalle de connexion dans **Intervalle de pulsation WNS Windows** situé dans **Propriétés du serveur**. Une fois l'inscription terminée, Worx Home s'inscrit en arrière-plan. Aucun indicateur n'apparaît lorsque l'installation est terminée. Ouvrez Worx Home à partir de l'écran **Toutes les applications**.

Envoi d'une invitation d'inscription dans XenMobile

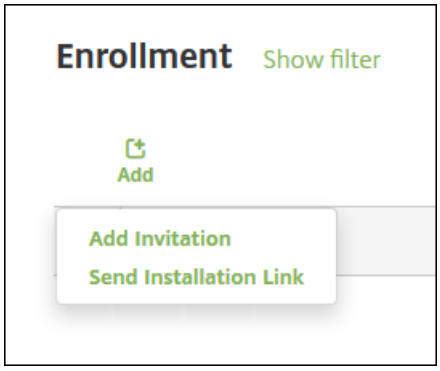
Oct 17, 2016

Dans la console XenMobile, vous pouvez envoyer une invitation d'inscription aux utilisateurs d'appareils iOS ou Android. Vous pouvez également envoyer un lien d'installation aux utilisateurs d'appareils iOS, Android, Windows ou Mac.

1. Dans la console XenMobile, cliquez sur **Gérer > Inscription**. La page **Inscription** s'affiche.



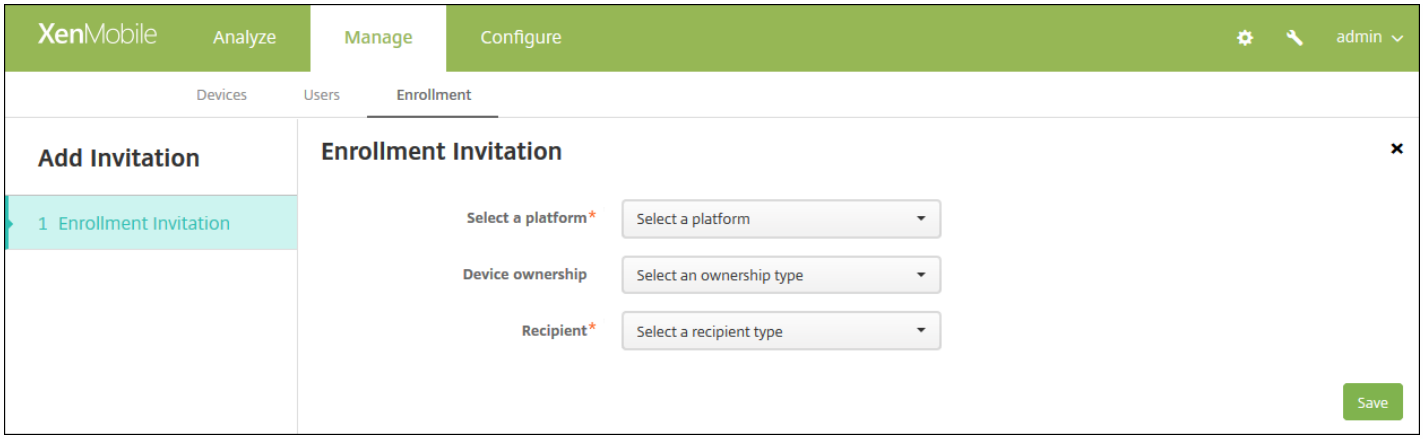
2. Cliquez sur **Ajouter**. Un menu répertoriant les options d'inscription s'affiche.



- Pour envoyer une invitation d'inscription à un utilisateur ou groupe, cliquez sur **Ajouter une invitation**, puis consultez la section Pour envoyer une invitation pour connaître les étapes suivantes.
- Pour envoyer un lien d'installation d'inscription à une liste de destinataires via SMTP ou SMS, cliquez sur **Envoyer lien d'installation**, puis consultez la section Pour envoyer un lien d'installation pour connaître les étapes suivantes.

Pour envoyer une invitation

1. Cliquez sur **Ajouter une invitation**. L'écran **Invitation d'inscription** s'affiche.

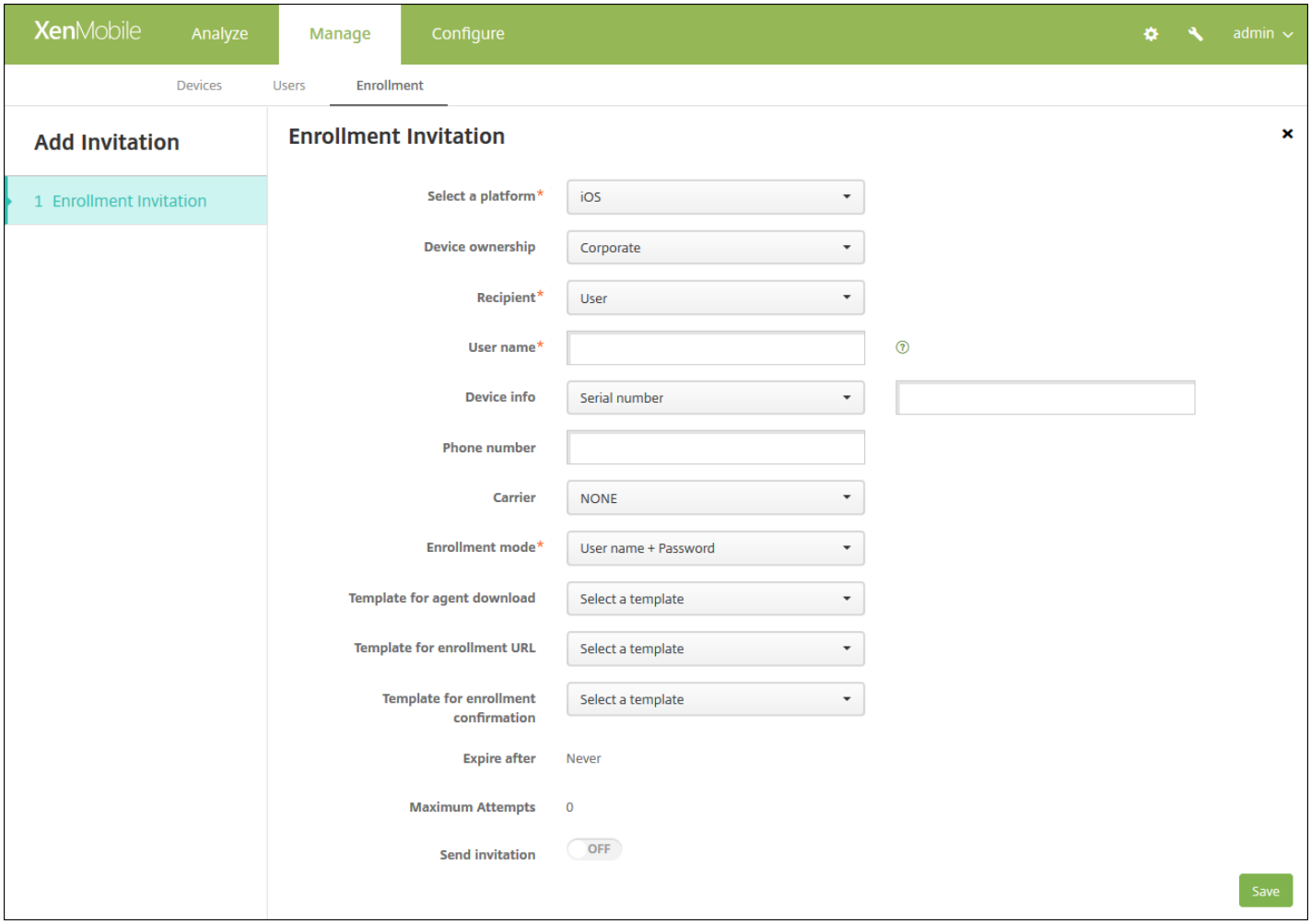


2. Configurez les paramètres suivants :

- **Sélectionner une plate-forme** : dans la liste, cliquez sur **iOS** ou **Android**.
- **Propriétaire** : dans la liste, cliquez sur **Entreprise** ou **Employé**.
- **Destinataire** : dans la liste, cliquez sur **Utilisateur** ou **Groupe**.

En fonction du destinataire que vous sélectionnez, vous pouvez voir des paramètres de configuration supplémentaires. Pour les paramètres **Utilisateur**, consultez la section Pour envoyer une invitation d'inscription à un utilisateur ; pour les paramètres **Groupe**, consultez la section Pour envoyer une invitation d'inscription à un groupe.

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 le serveur XenMobile 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 appareil** : dans la liste, cliquez sur **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**: si vous le souhaitez, entrez le numéro de téléphone de l'utilisateur.
- **Opérateur** : dans la liste, sélectionnez un opérateur auquel associer le numéro de téléphone de l'utilisateur.
- **Mode d'inscription** : dans la liste, cliquez sur la manière dont vous souhaitez que les utilisateurs s'inscrivent. La valeur par défaut est **Nom d'utilisateur + mot de passe**. Les options possibles sont les suivantes :
  - Haute sécurité
  - URL d'invitation
  - URL d'invitation + PIN
  - URL d'invitation + mot de passe
  - Deux facteurs
  - Nom d'utilisateur + PIN

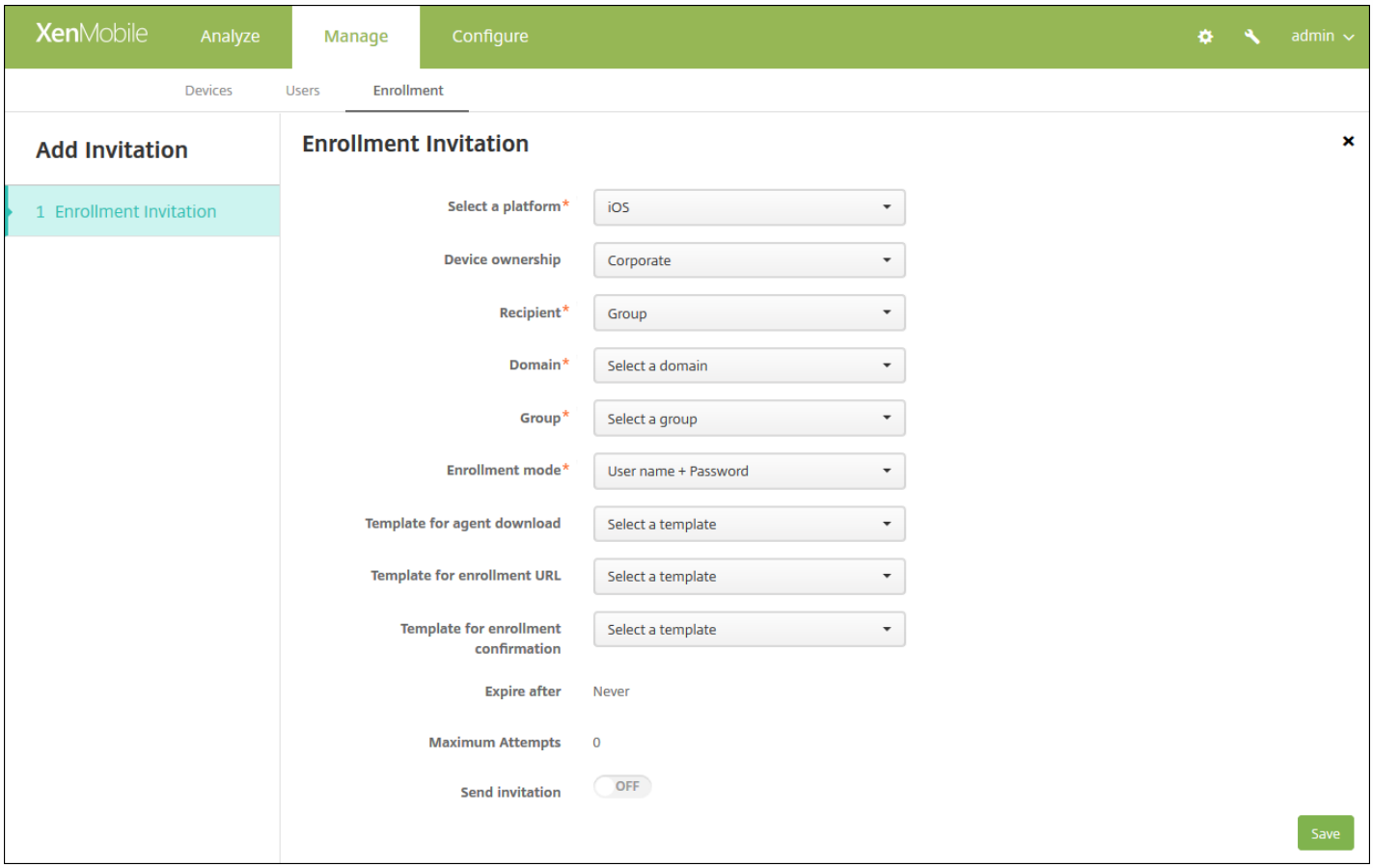
  Remarque : lorsque vous sélectionnez un mode d'inscription qui comprend un code PIN, le champ **Modèle pour le**

code PIN d'inscription s'affiche, dans lequel vous cliquez sur **Code PIN d'inscription**.

- **Modèle pour téléchargement de l'agent**: dans la liste, cliquez sur le modèle à utiliser pour l'invitation d'inscription. Les choix pour cette option sont basés sur le type de plate-forme. Par exemple, le **lien de téléchargement iOS** s'affiche si vous avez sélectionné **iOS** en tant que plate-forme.
- **Modèle pour l'URL d'inscription** : dans la liste, cliquez sur **Invitation d'inscription**.
- **Modèle pour la confirmation d'inscription** : dans la liste, cliquez sur **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, veuillez consulter la section Pour configurer les modes d'inscription.
- **Nbre max de tentatives** : ce champ est défini lorsque vous configurez le Mode d'inscription et indique le nombre maximal de fois que le processus d'inscription peut être tenté. Pour plus d'informations sur la configuration des modes d'inscription, veuillez consulter la section Pour configurer les modes d'inscription.
- **Envoyer invitation** : sélectionnez **ON** pour envoyer l'invitation immédiatement ou cliquez sur **OFF** pour uniquement ajouter l'invitation au tableau de la page **Inscription**.

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 **Inscription**.

Pour envoyer une invitation d'inscription à un groupe



1. Configurez les paramètres suivants :

- **Domaine** : dans la liste, cliquez sur le domaine à partir duquel choisir le groupe.

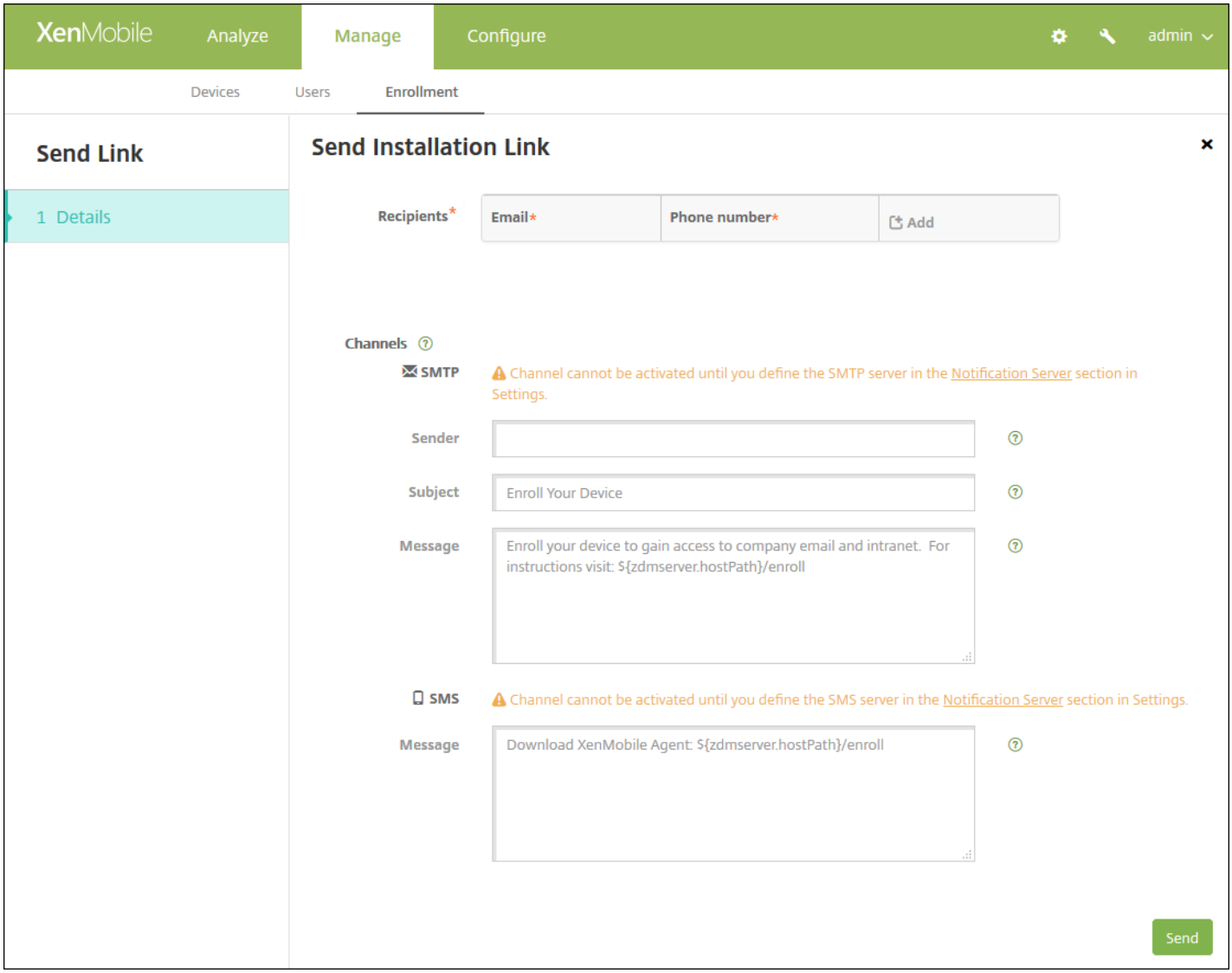
- **Groupe**: dans la liste, cliquez sur le groupe qui recevra l'invitation.
- **Mode d'inscription** : dans la liste, cliquez sur la manière dont vous souhaitez que les utilisateurs du groupe s'inscrivent. La valeur par défaut est **Nom d'utilisateur + mot de passe**. Les options possibles sont les suivantes :
  - Haute sécurité
  - URL d'invitation
  - URL d'invitation + PIN
  - URL d'invitation + mot de passe
  - Deux facteurs
  - Nom d'utilisateur + PIN

  Remarque : lorsque vous sélectionnez un mode d'inscription 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**: dans la liste, cliquez sur le modèle à utiliser pour l'invitation d'inscription. Les choix pour cette option sont basés sur le type de plate-forme. Par exemple, le **lien de téléchargement iOS** s'affiche si vous avez sélectionné **iOS** en tant que plate-forme.
- **Modèle pour l'URL d'inscription** : dans la liste, cliquez sur **Invitation d'inscription**.
- **Modèle pour la confirmation d'inscription** : dans la liste, cliquez sur **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, veuillez consulter la section Pour configurer les modes d'inscription.
- **Nbre max de tentatives** : ce champ est défini lorsque vous configurez le Mode d'inscription et indique le nombre maximal de fois que le processus d'inscription peut être tenté. Pour plus d'informations sur la configuration des modes d'inscription, veuillez consulter la section Pour configurer les modes d'inscription.
- **Envoyer invitation** : sélectionnez **ON** pour envoyer l'invitation immédiatement ou cliquez sur **OFF** pour uniquement ajouter l'invitation au tableau de la page **Inscription**.

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 **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 de détails, consultez la section Notifications.

1. Configurez les paramètres suivants :

- **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.
  - Cliquez sur **Save**.

    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. Effectuez toutes les modifications nécessaires à la liste, 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 tire parti de 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. Par exemple, ils doivent supprimer nomdomaine dans SAMAccountName@nomdomaine.com.

Appareils partagés dans XenMobile

Jul 27, 2016

XenMobile vous permet de configurer des appareils qui peuvent être partagés par de multiples utilisateurs. 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

Mode MDM

- Disponible sur tablettes et smartphones iOS et Android. L'inscription au programme Device Enrollment Program (DEP) de base n'est pas prise en charge pour un appareil partagé XenMobile Enterprise. Vous devez utiliser une DEP autorisée pour inscrire un appareil partagé dans ce mode.
- L'authentification de certificat client, le code PIN Worx, Touch ID et l'entropie utilisateur ne sont pas pris en charge.

Mode MDM+MAM

- Disponible uniquement sur tablettes iOS et Android.
- Pris en charge uniquement sur serveurs et clients XenMobile 10.3.x.
- Le mode MAM exclusif n'est pas pris en charge. Les appareils doivent s'inscrire en mode MDM.
- Seuls WorxMail, WorxWeb, et l'application mobile ShareFile (version 4.4) sont pris en charge. Les applications HDX ne sont pas prises en charge.
- Seuls les utilisateurs Active Directory sont pris en charge, contrairement aux utilisateurs et aux groupes locaux.
- Une réinscription est requise pour les appareils partagés en mode MDM exclusif afin de mettre à jour vers le mode MDM+MAM.
- Les utilisateurs peuvent uniquement partager des applications Worx et des applications wrappées MDX, mais ils ne peuvent pas partager d'applications natives sur les appareils.
- Une fois les applications Worx téléchargées lors de la première inscription, il est inutile de les télécharger à nouveau à chaque fois qu'un utilisateur se connecte sur l'appareil. Le nouvel utilisateur peut récupérer l'appareil, ouvrir une session, et se lancer.
- Sur Android, afin d'isoler les données de chaque utilisateur pour des raisons de sécurité, la stratégie **Disallow rooted devices** de la console XenMobile doit être définie 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. Voir Configuration de rôles avec RBAC.
- Créer un utilisateur d'appareil partagé. Voir Pour ajouter, modifier ou supprimer des utilisateurs locaux dans XenMobile.

- 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'inscription d'appareil partagé. Voir Gestion des groupes de mise à disposition.

Conditions préalables pour le mode MDM+MAM

1. Créez un groupe Active Directory nommé, par exemple, **Shared Device Enrollers**.
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 requise pour les appareils partagés

Pour garantir une expérience utilisateur optimale, y compris l'installation et la suppression silencieuse des applications, Citrix recommande de configurer les appareils partagés sur les plates-formes suivantes :

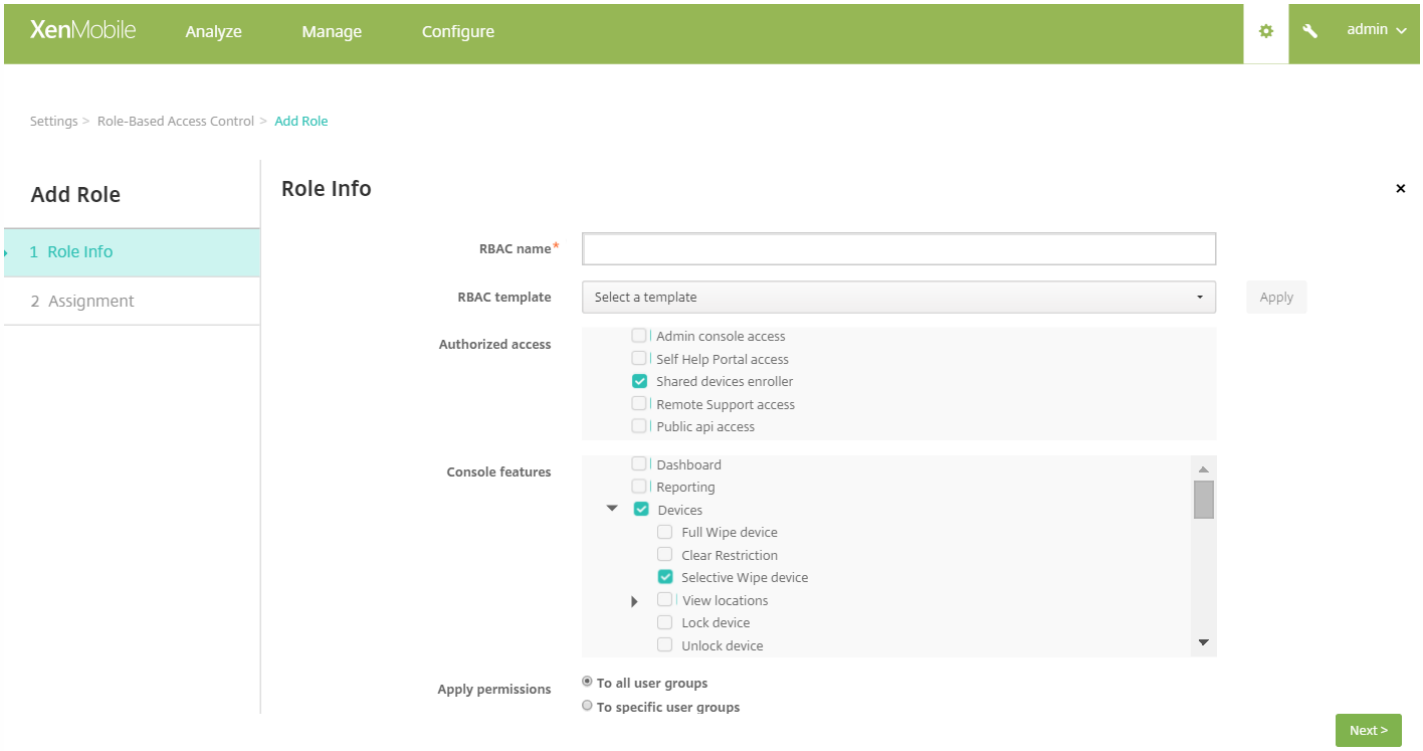
- iOS 9
- iOS 8
- Android M
- Android 5.x
- Android 4,4.x
- Android 4.0.x (mode MDM exclusif)

Configuration d'un appareil partagé

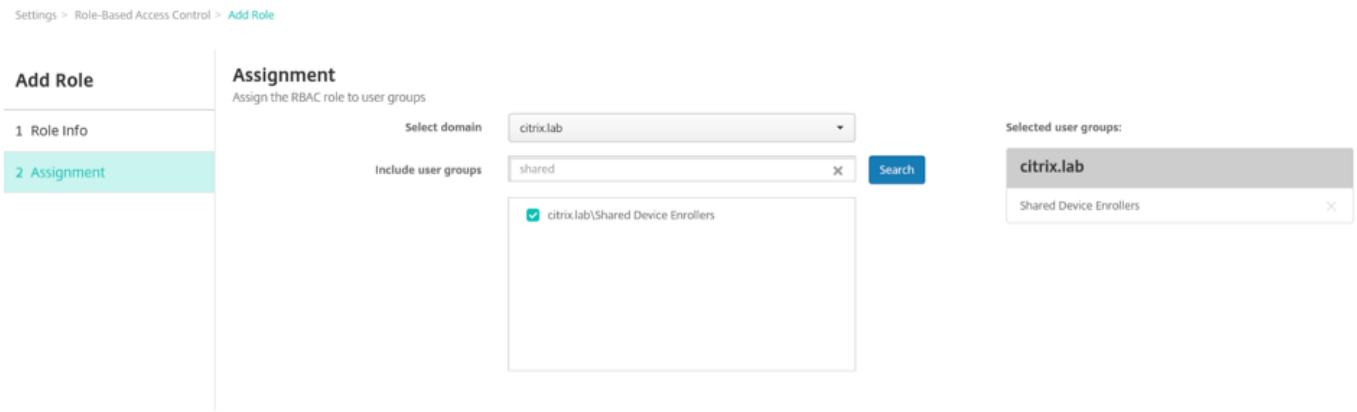
Suivez les étapes ci-dessous pour configurer un appareil partagé.

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 Worx Home lors de la désinscription de l'appareil.

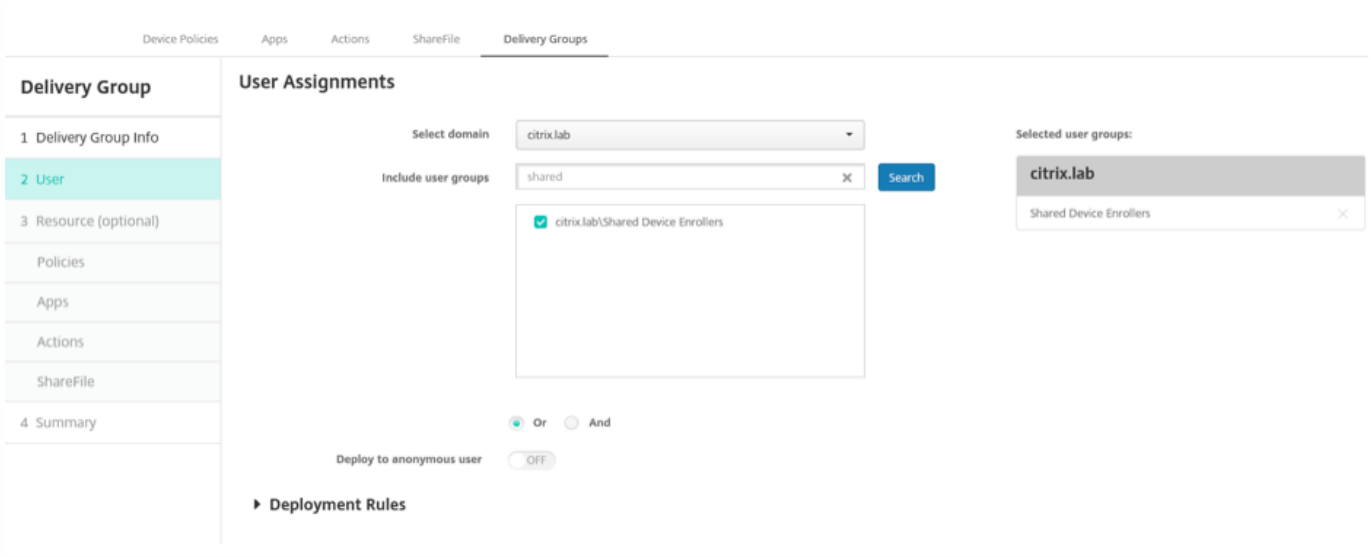
   Pour **Appliquer les autorisations**, conservez le paramètre par défaut, qui est **À tous les groupes d'utilisateurs**, ou attribuez des autorisations à des groupes d'utilisateurs Active Directory spécifiques avec le paramètre **À des groupes d'utilisateurs spécifiques**.



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 ci-dessous, **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 Worx Home 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 plus d'informations, consultez la section Configuration des règles de déploiement.

7. Pour arrêter le partage de l'appareil, effacez les données d'entreprise afin de supprimer le compte utilisateur d'inscription sur appareil partagé de l'appareil, ainsi que toute application ou stratégie ayant été déployée sur cet appareil.

Expérience utilisateur relative à l'utilisation d'un appareil partagé

Mode 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 Worx Home, les stratégies et applications de cette personne sont déployées sur l'appareil. Lorsque cet utilisateur se déconnecte, les stratégies et les applications qui diffèrent de celles de l'inscription d'appareil partagé sont supprimées, tandis que les ressources de l'inscription d'appareil partagé restent intactes.

Mode MDM+MAM

WorxMail et WorxWeb sont déployés sur l'appareil lorsque l'utilisateur inscrit des appareils partagés. Les données utilisateur sont conservées de manière sécurisée sur l'appareil. Les autres utilisateurs ne peuvent pas afficher ces données lorsqu'ils se connectent à WorxMail ou WorxWeb.

Un seul utilisateur à la fois peut se connecter à Worx Home. L'utilisateur précédent doit se déconnecter pour que le

prochain utilisateur puisse se connecter. Pour des raisons de sécurité, Worx Home 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. Pour vous assurer qu'un nouvel utilisateur ne puisse pas accéder aux ressources destinées à l'utilisateur précédent, Worx Home n'autorise pas les nouveaux utilisateurs à se connecter alors que des stratégies, applications et données associées à l'utilisateur précédent sont en cours de suppression.

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 WorxMail recommandées

- Pour obtenir des performances WorxMail 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 à 25	1 semaine ou moins
6 à 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 seront 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

Gestion des appareils avec Android for Work dans XenMobile

Oct 17, 2016

Android for Work est un espace de travail disponible sur les appareils Android exécutant Android 5.0 et version ultérieure qui isole les comptes, applications et données d'entreprise des comptes, applications et données personnels. Dans XenMobile, vous pouvez gérer les appareils BYOD et les appareils Android appartenant à l'entreprise en permettant aux utilisateurs de créer un profil professionnel séparé sur leurs appareils, ce qui, combiné avec le cryptage du matériel et les stratégies que vous déployez, sépare de manière sécurisée les zones professionnelles et personnelles sur un appareil. Vous pouvez gérer toutes les stratégies, applications et données d'entreprise à distance et vous pouvez effacer les stratégies, applications et données de l'appareil sans affecter la zone personnelle de l'utilisateur. Pour de plus amples informations sur la prise en charge des appareils Android, consultez la page appareils de Google.

Dans XenMobile, vous pouvez également gérer les appareils exécutant Android 4.0 - 4.4 en demandant aux utilisateurs de télécharger et d'installer l'application Android for Work, qui fournit les fonctionnalités d'espace de travail sécurisé intégrées dans les appareils exécutant Android 5.0 et version ultérieure.

Vous utilisez Google Play for Work pour ajouter, acheter et approuver les applications pour le déploiement vers l'espace de travail d'un appareil Android for Work. Vous pouvez utiliser la console Google Play for Work pour déployer vos applications Android privées, ainsi que des applications tierces et publiques. Lorsque vous ajoutez une application payante provenant d'un magasin d'applications public à XenMobile pour un Android for Work, vous pouvez vérifier l'état de la licence d'achat groupé : le nombre total de licences disponibles, ainsi que l'adresse e-mail de chaque utilisateur qui consomme les licences. Pour de plus amples informations, consultez la section Pour ajouter un magasin d'applications public à XenMobile.

Configuration requise pour Android for Work :

- Un domaine publiquement accessible
- Un compte d'administrateur Google
- Des appareils exécutant Android 5.0+ Lollipop avec prise en charge de profils gérés ou des appareils exécutant Android 4.0 - 4.4 (Ice Cream Sandwich, Jelly Bean et KitKat) avec l'application Android for Work
- Un compte Google avec Google Play installé dans le profil personnel de l'utilisateur
- Un profil de travail configuré sur l'appareil.

Avant de pouvoir définir des restrictions applicatives Android for Work, vous devez effectuer les opérations suivantes :

- Effectuer les tâches de configuration d'Android for Work sur Google.
- Créer des informations d'identification Google Play.
- Configurer les paramètres de serveur Android for Work.
- Créer au moins une stratégie Android for Work.
- Ajouter, acheter et approuver des applications Android for Work dans le magasin d'applications Google Play for Work.

Vous pouvez utiliser les liens suivants lorsque vous gérez Android for Work :

- Console d'administration Google : https://admin.google.com/AdminHome
- Console d'administration Play for Work : https://play.google.com/work/apps
- Publication sur Play pour les applications de chaînes privées et auto-hébergées : https://play.google.com/apps/publish
- Console Google Developer pour la création de compte de service : https://console.developers.google.com

Conditions préalables pour Android for Work

Avant de pouvoir administrer Android for Work dans XenMobile, vous devez effectuer les opérations suivantes :

- Créer un compte Android for Work.
- Configurer un compte de service.
- Télécharger un certificat Android for Work.
- Activer et autoriser les API SDK et MDM d'administrateur Google.
- Autoriser votre compte de service à utiliser Directory et Google Play.
- Obtenir un jeton de liaison.

Les sections suivantes expliquent comment effectuer chacune de ces tâches. Après avoir effectué ces tâches, vous pouvez créer des informations d'identification Google Play, configurer les paramètres Android for Work et gérer les applications Android for Work dans XenMobile.

> **Avertissement**
>
> Un problème connu tiers existe qui vous empêche d'utiliser la console XenMobile pour activer Android for Work. Pour de plus amples informations sur ce problème et la façon de configurer une propriété de serveur pour le résoudre, consultez le problème #615118 dans la section Problèmes connus de XenMobile Server 10.3.

Créer un compte Android for Work

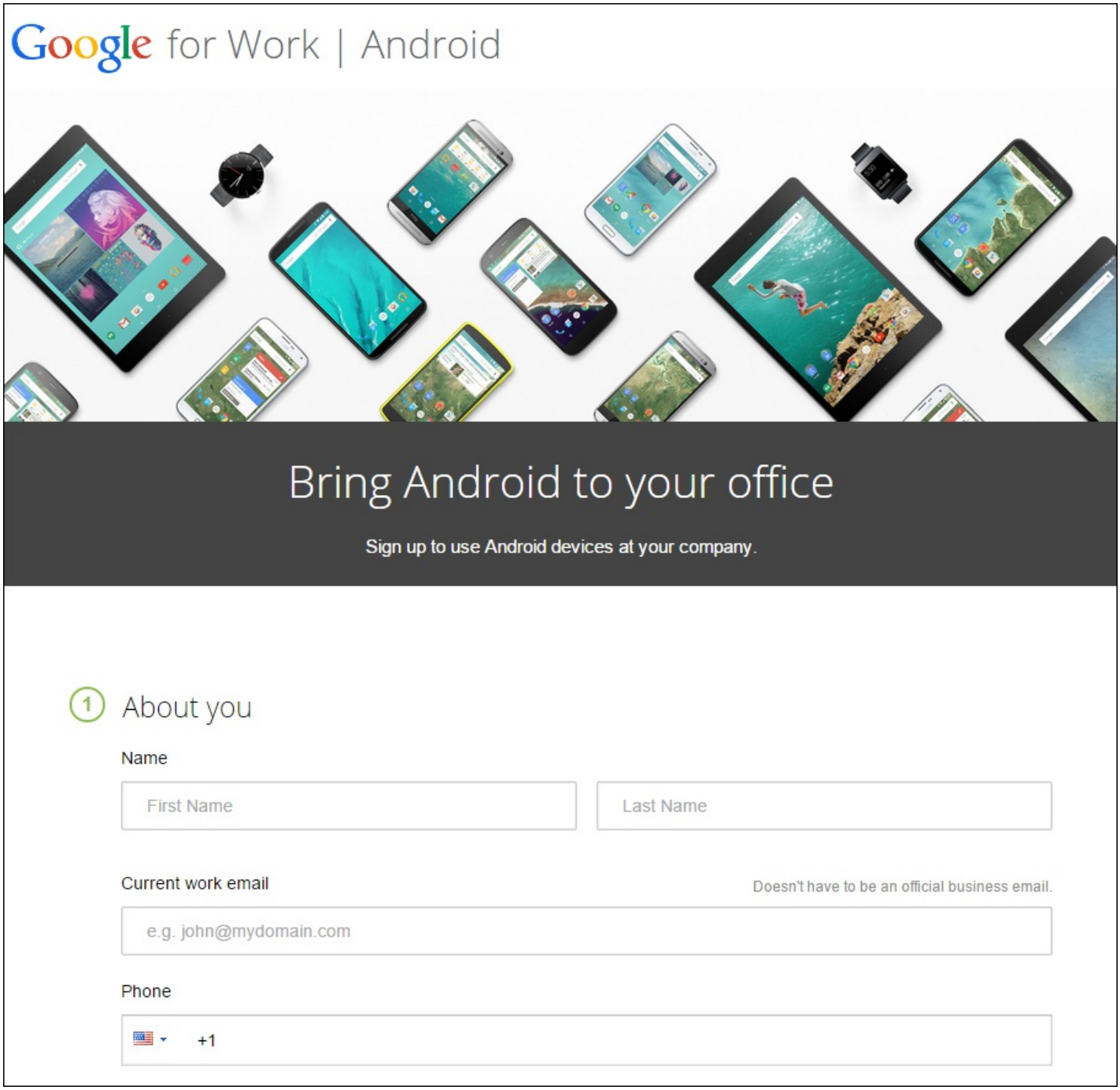
Vous devez remplir les conditions préalables suivantes avant de pouvoir configurer un compte Android for Work :

- Vous devez disposer d'un nom de domaine ; par exemple, exemple.com.
- Vous devez autoriser Google à vérifier que le domaine vous appartient.
- Vous devez activer et administrer Android for Work par le biais d'un fournisseur de gestion de la mobilité d'entreprise (EMM) (XenMobile 10.0 ou version ultérieure).

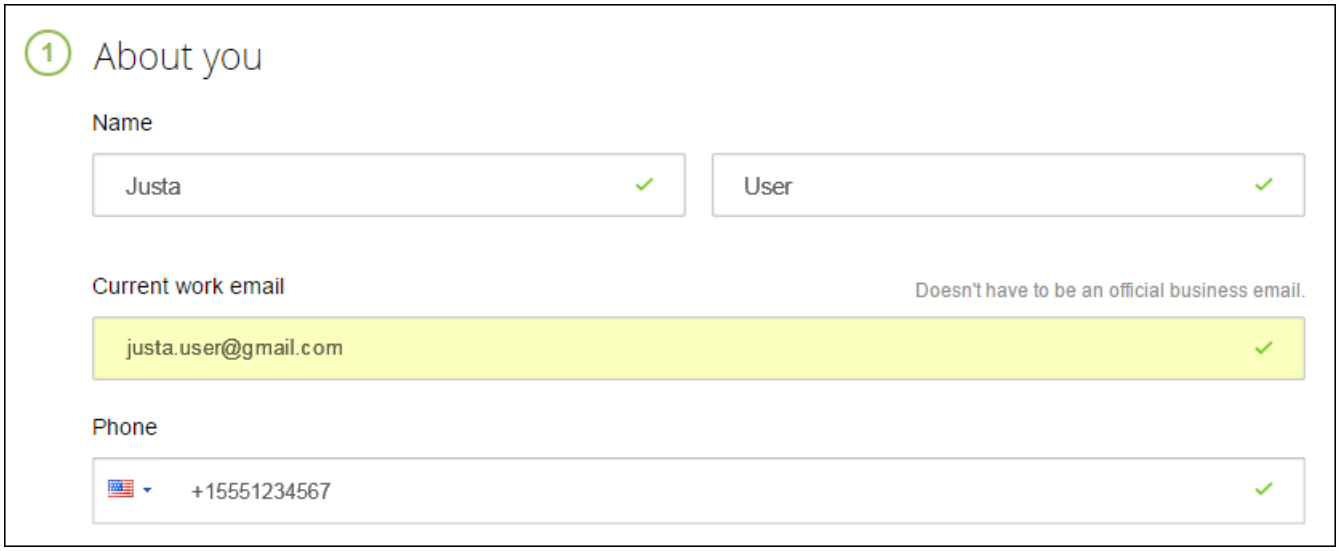
Si vous avez déjà vérifié votre nom de domaine auprès de Google, vous pouvez passer à cette étape : Configurer un compte de service Android for Work et télécharger un certificat Android for Work.

1. Accédez à https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

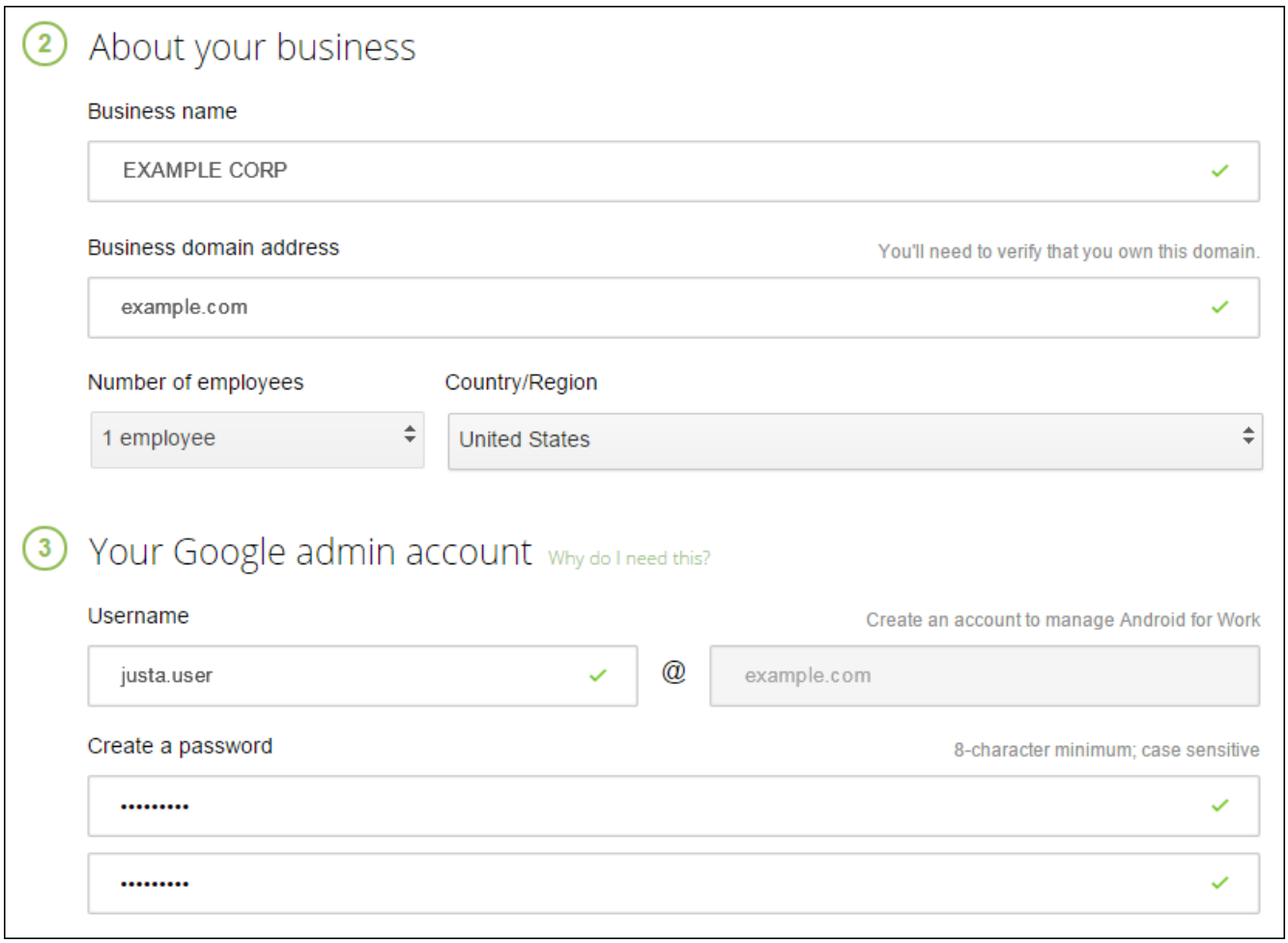
Vous serez dirigé vers la page suivante où vous entrez vos informations d'administrateur et les informations sur l'entreprise.



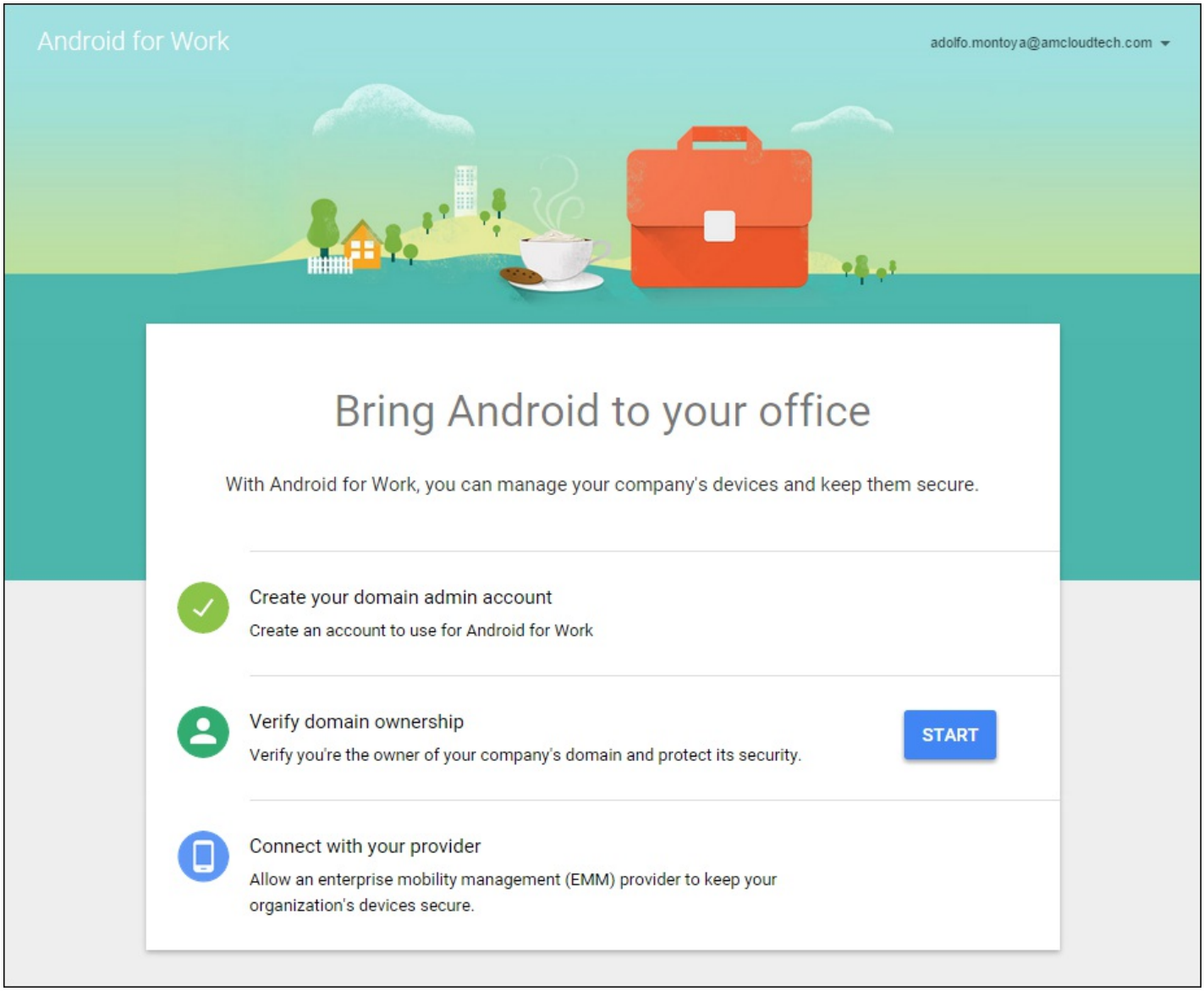
2. Entrez vos informations d'utilisateur administrateur.



3. Entrez les informations de votre entreprise, ainsi que les informations sur votre compte d'administrateur.



La première étape de ce processus est terminée et la page suivante s'affiche.

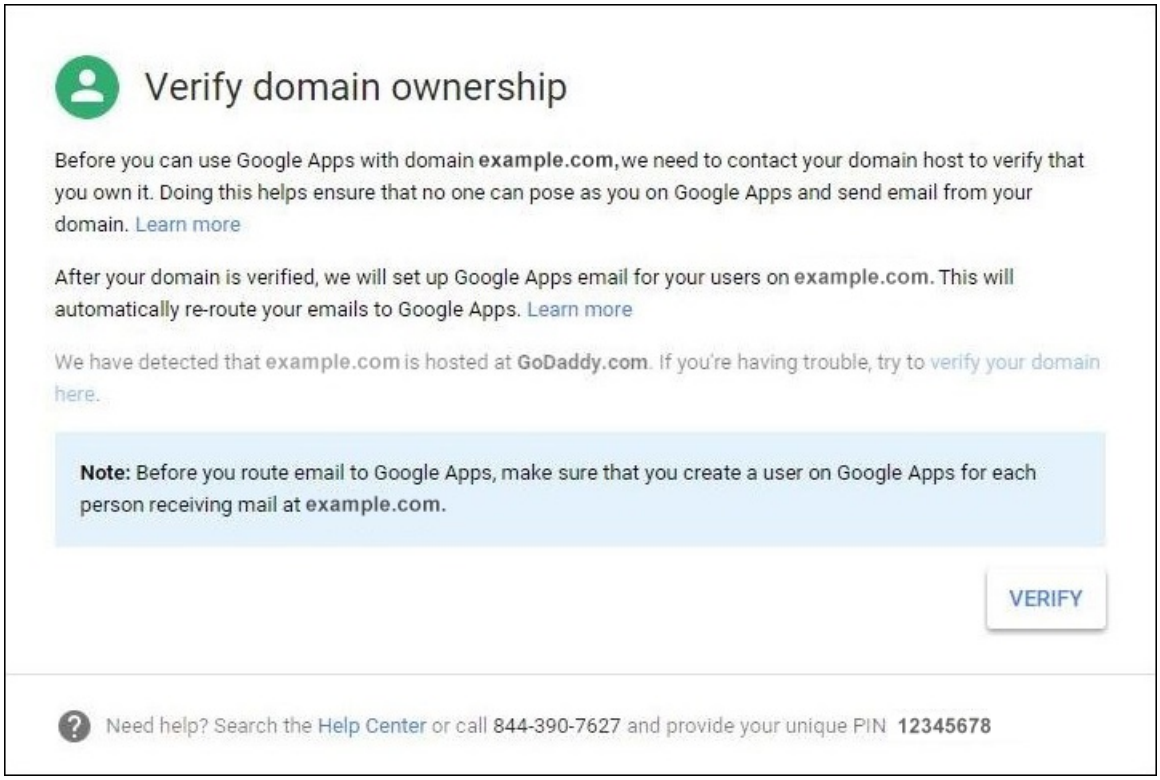


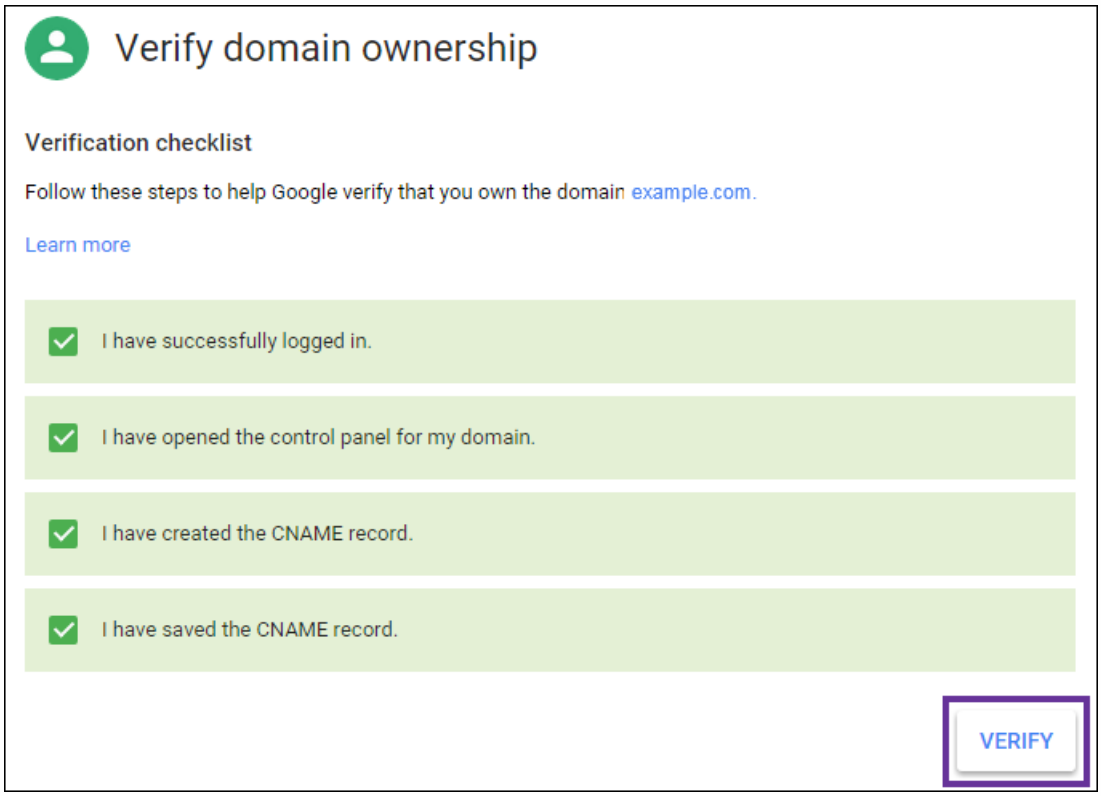
Vérifier le propriétaire du domaine

Vous devez maintenant autoriser Google à vérifier votre domaine. Il existe trois méthodes différentes pour vérifier votre domaine : ajouter un enregistrement TXT ou CNAME au site Web de l'hôte de votre domaine, charger un fichier HTML sur le serveur Web de votre domaine, ou ajouter une balise à votre page d'accueil. Google recommande la première méthode. Les étapes permettant de vérifier que votre domaine vous appartient ne sont pas couvertes dans cet article, mais vous pouvez trouver les informations dont vous avez besoin sur : https://support.google.com/a/answer/6095407/.

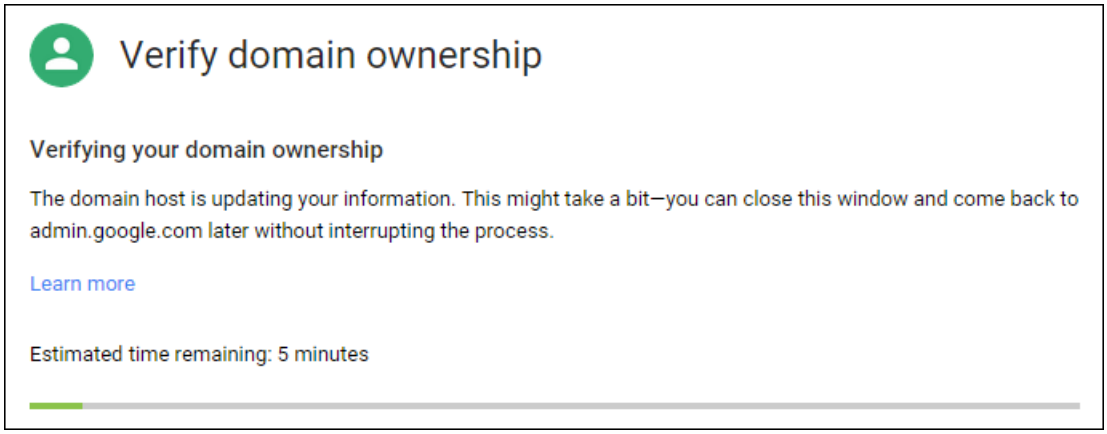
1. Cliquez sur **Démarrer** pour commencer la vérification de votre domaine. La page **Valider la propriété du domaine** s'affiche. Suivez les instructions pour vérifier votre domaine.

2. Lorsque vous avez terminé, cliquez sur **Vérifier**.

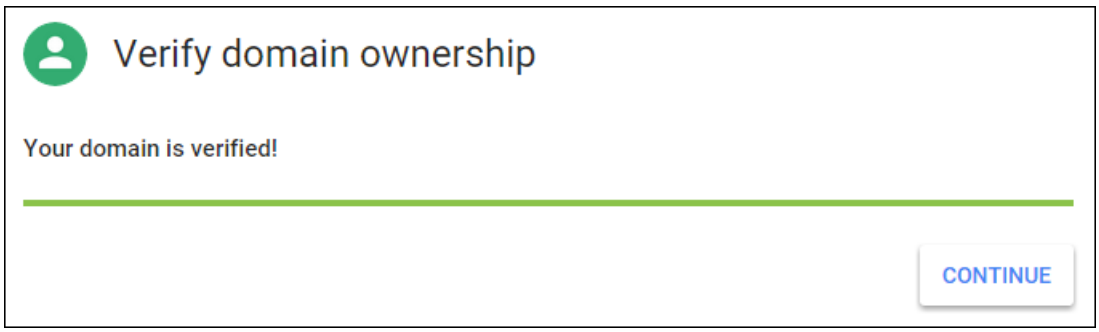




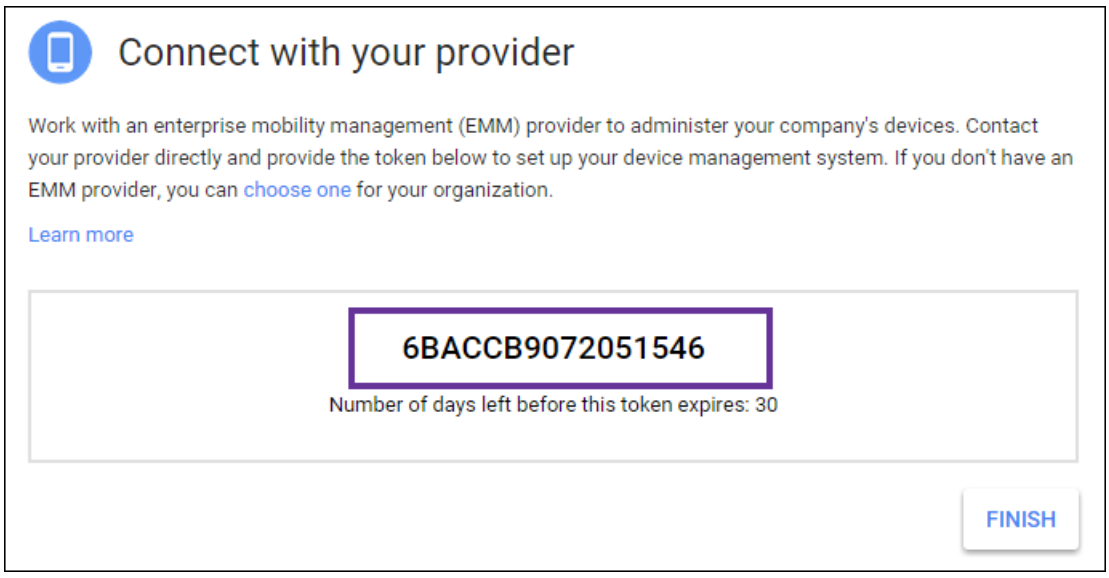
3. Google vérifie que vous êtes le propriétaire du domaine.



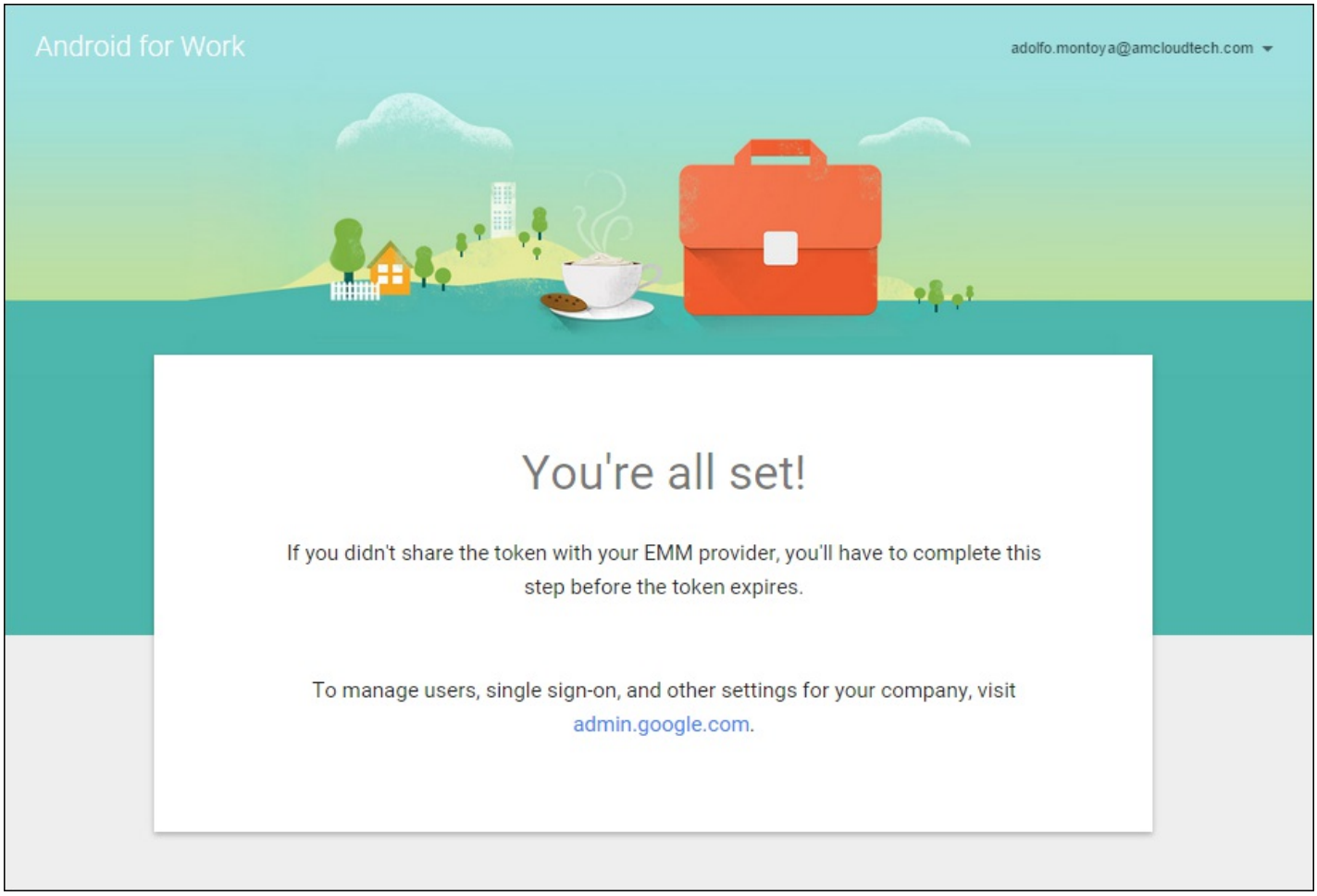
4. La page suivante s'affiche si la vérification réussit. Cliquez sur **Continue**.



5. Google crée un jeton de liaison EMM que vous fournissez à Citrix lorsque vous configurez les paramètres d'Android for Work. Copiez et enregistrez le jeton ; vous en aurez besoin plus tard lors de la configuration.



6. Cliquez sur **Finish** pour terminer la configuration Android for Work.



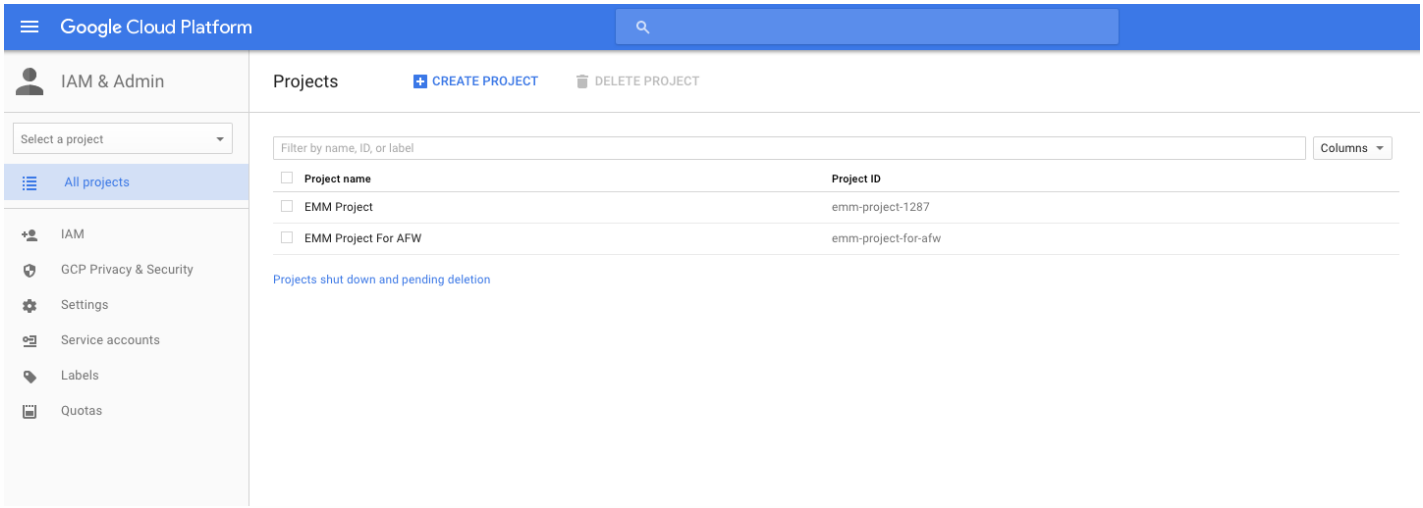
11. Une fois que vous avez créé un compte de service Android for Work, vous pouvez ouvrir une session sur la console d'administration Google pour gérer vos paramètres de gestion de la mobilité Android for Work.

Définissez un compte de service Android for Work et téléchargez un certificat Android for Work

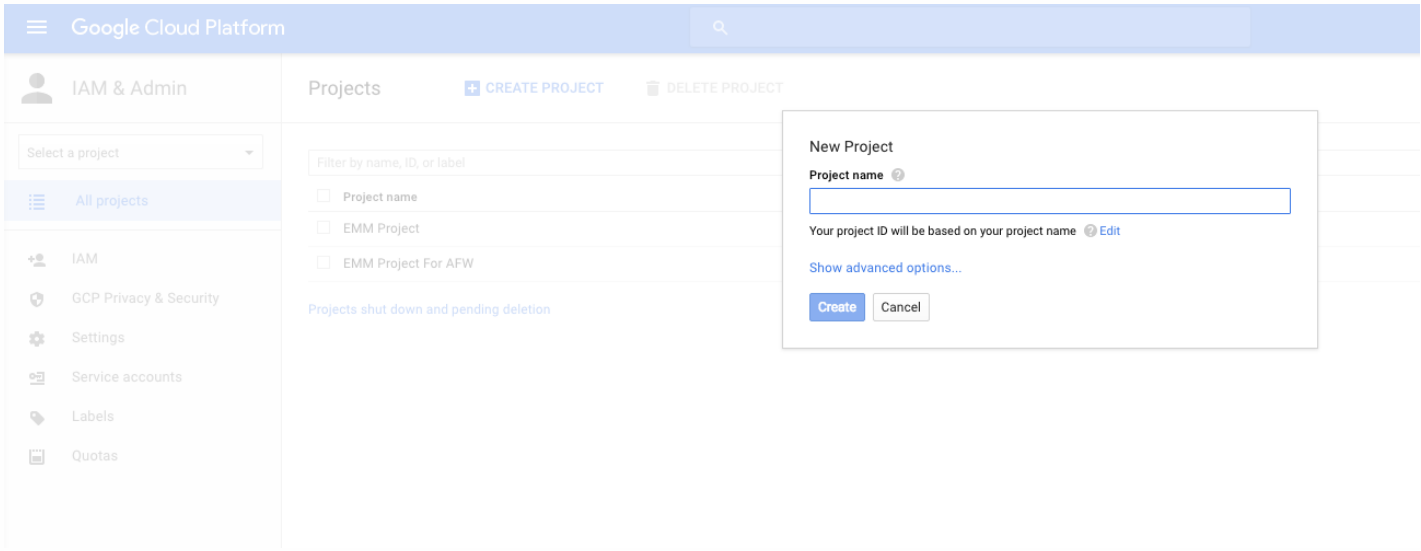
Pour autoriser XenMobile à contacter les services Google Play et Directory, vous devez créer un nouveau compte de service à l'aide du portail Project de Google destiné aux développeurs. Ce compte de service est utilisé pour permettre les communications entre serveurs entre XenMobile et les services Google pour Android for Work. Pour de plus amples 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.

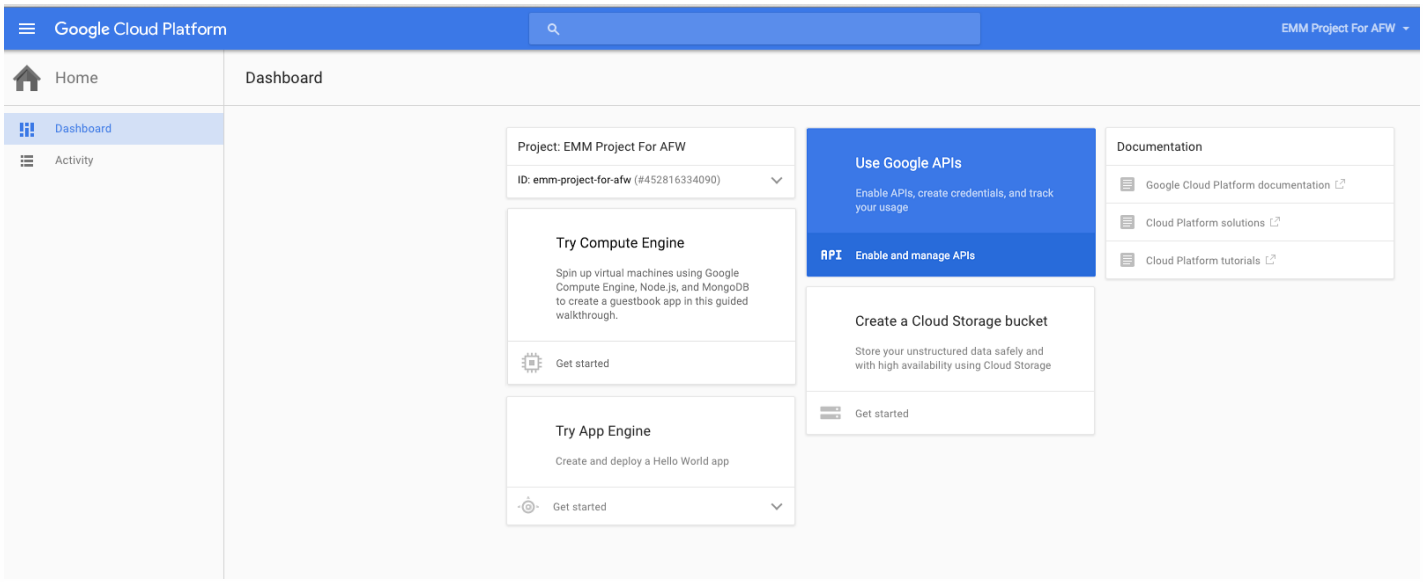
2. Dans la liste **Projects**, cliquez sur **Create Project**.



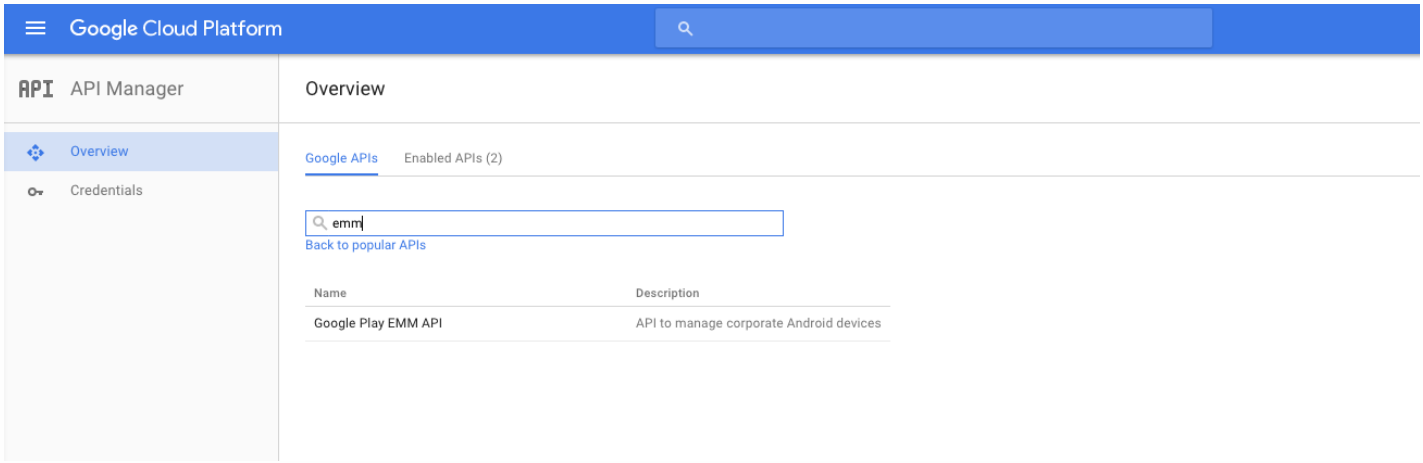
3. Dans **Project name**, entrez un nom pour le projet.



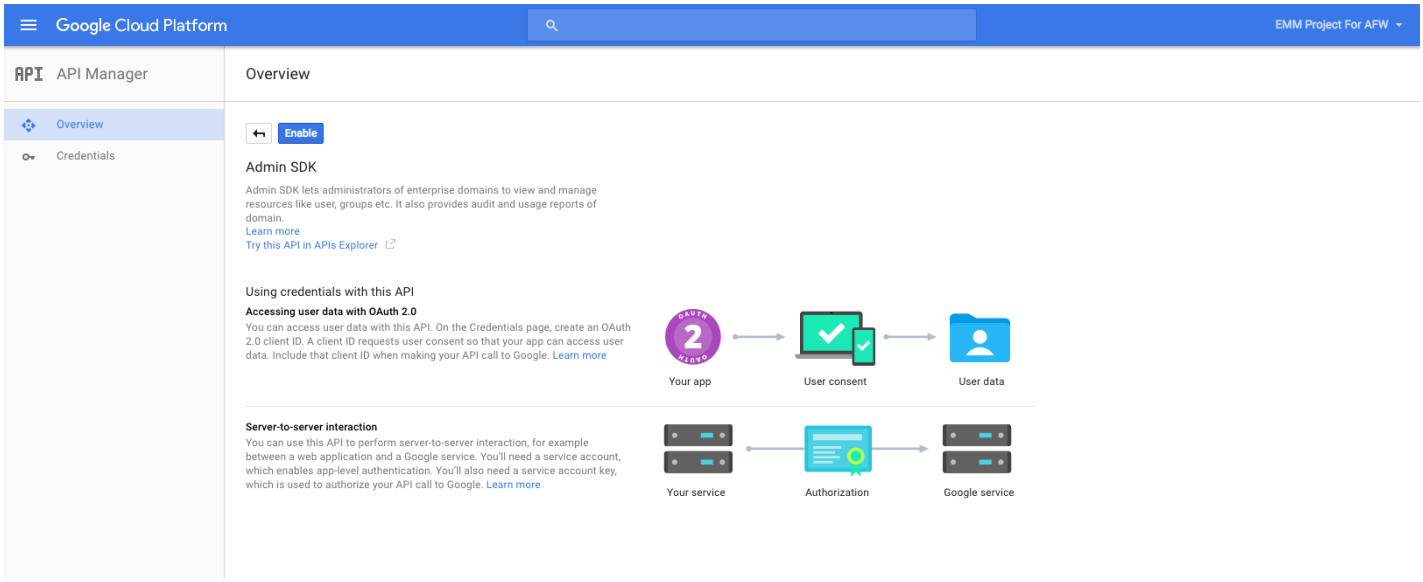
4. Sur le tableau de bord, cliquez sur **Use Google APIs**.



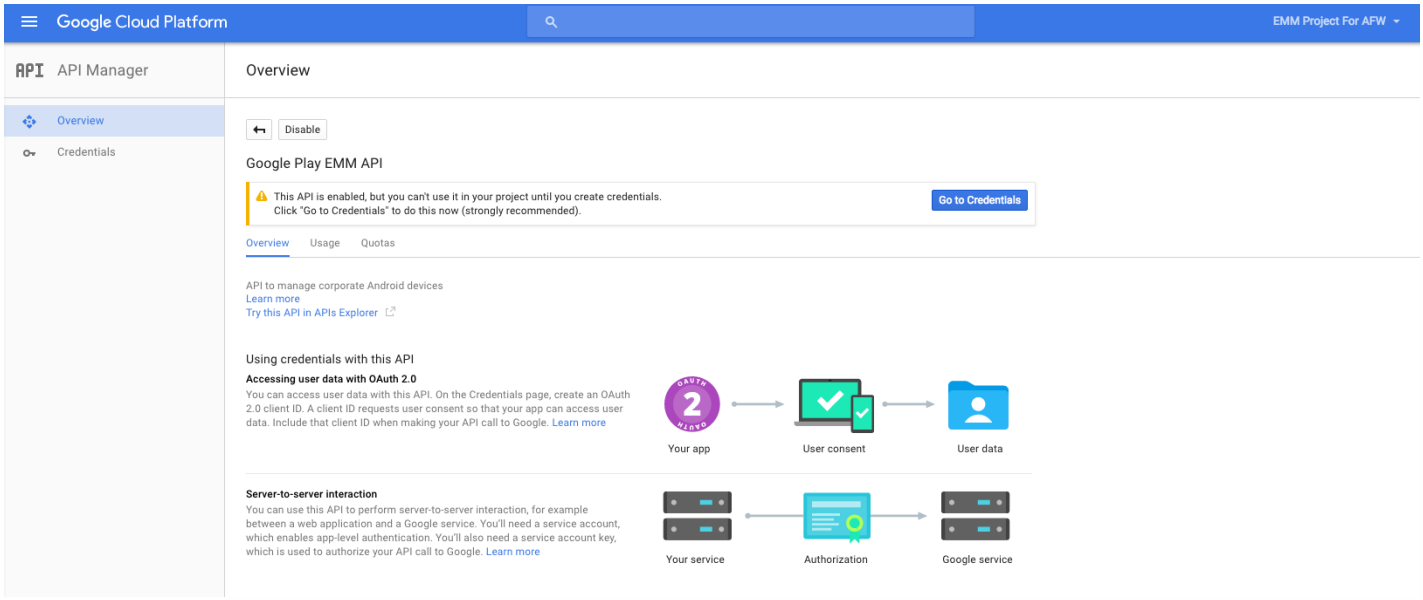
5. Sur la page Google APIs, dans **Search**, entrez **EMM** puis cliquez sur les résultats de la recherche.



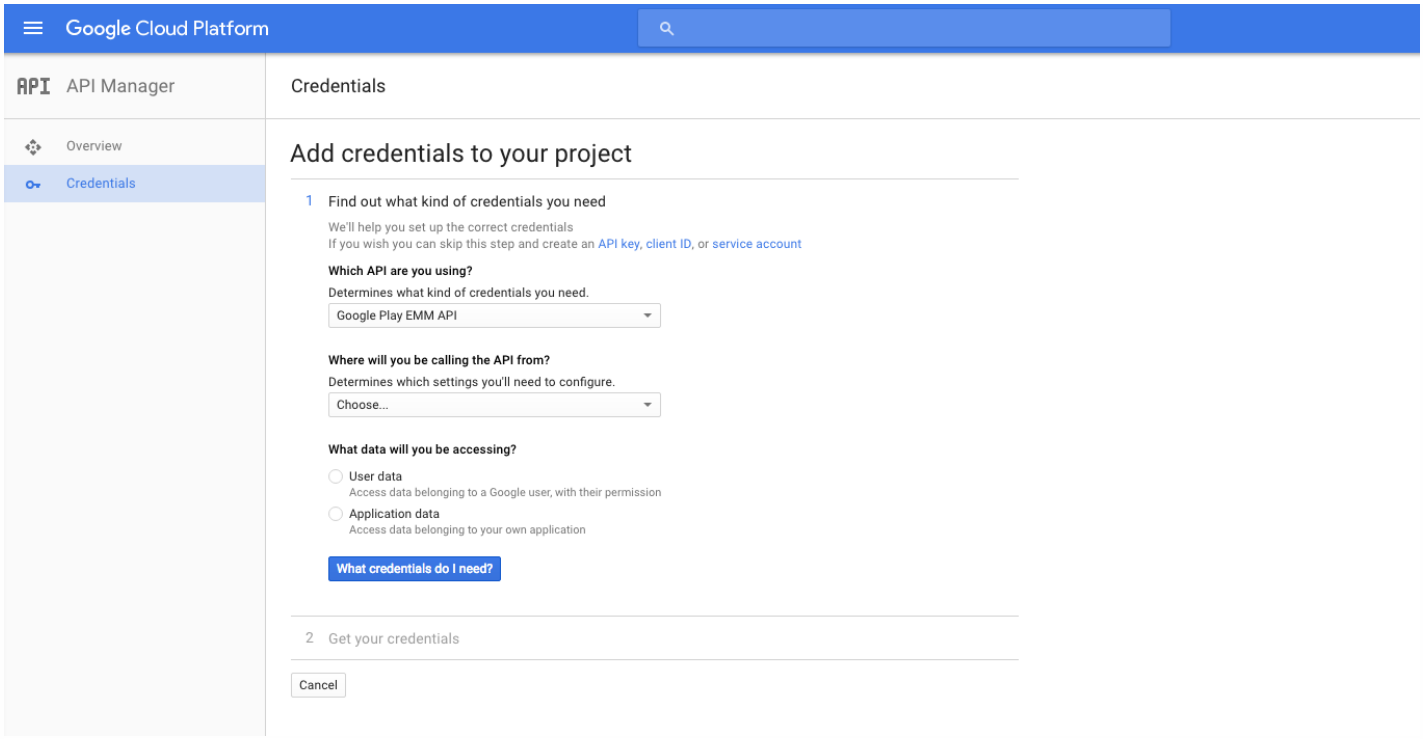
6. Sur la page Overview, cliquez sur **Enable**.



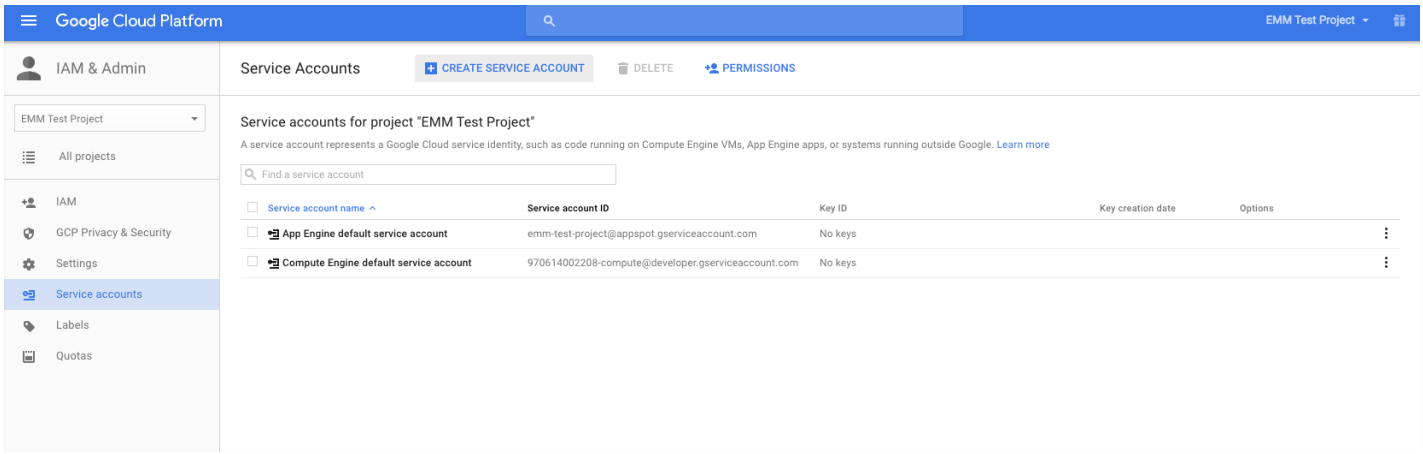
7 En regard de **Google Play EMM API**, cliquez sur **Go to Credentials**.



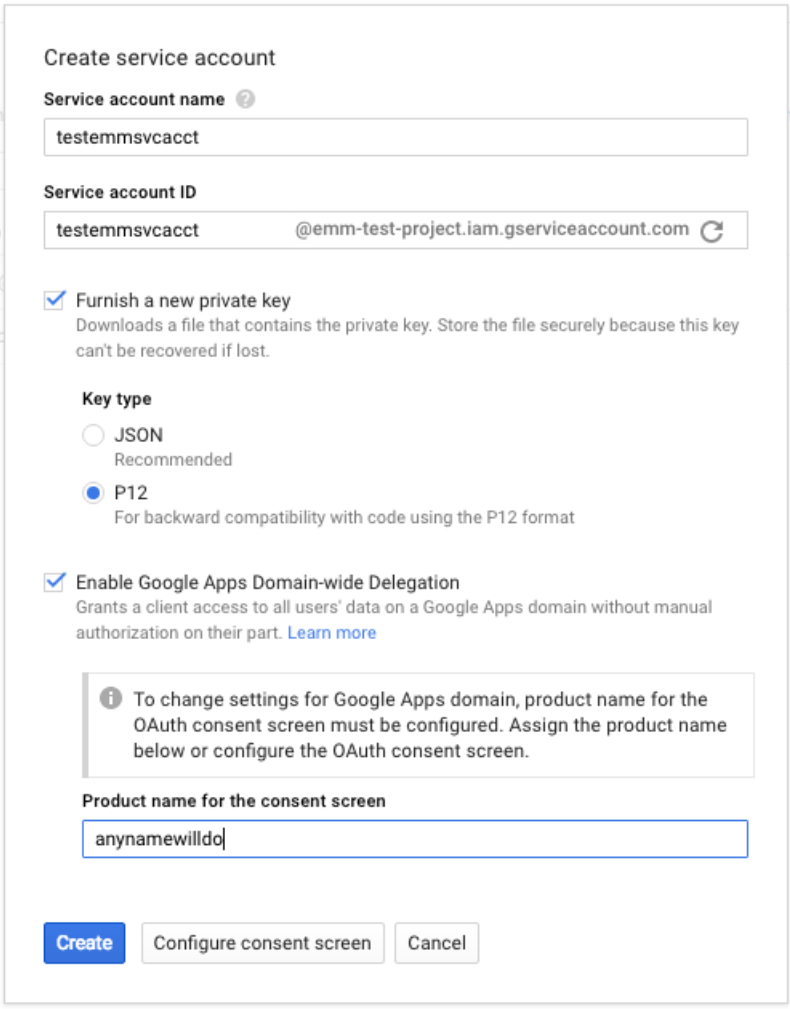
8. Dans la liste **Add credentials to our project**, dans l'étape 1, cliquez sur **service account**.



9. Sur la page **Service Accounts**, cliquez sur **Create Service Account**.

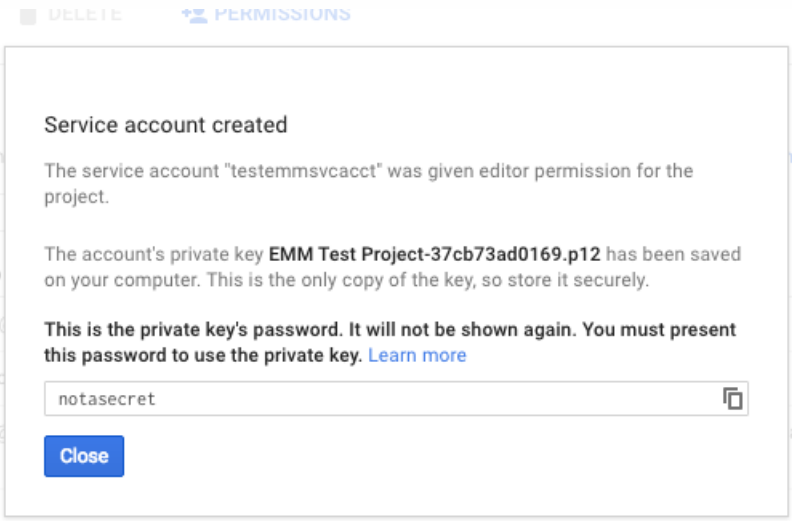


10. Dans **Create service account**, nommez le compte, sélectionnez la case à cocher **Furnish a new private key**, cliquez sur **P12**, sélectionnez la case **Enable Google Apps Domain-wide Delegation** et cliquez sur **Create.**

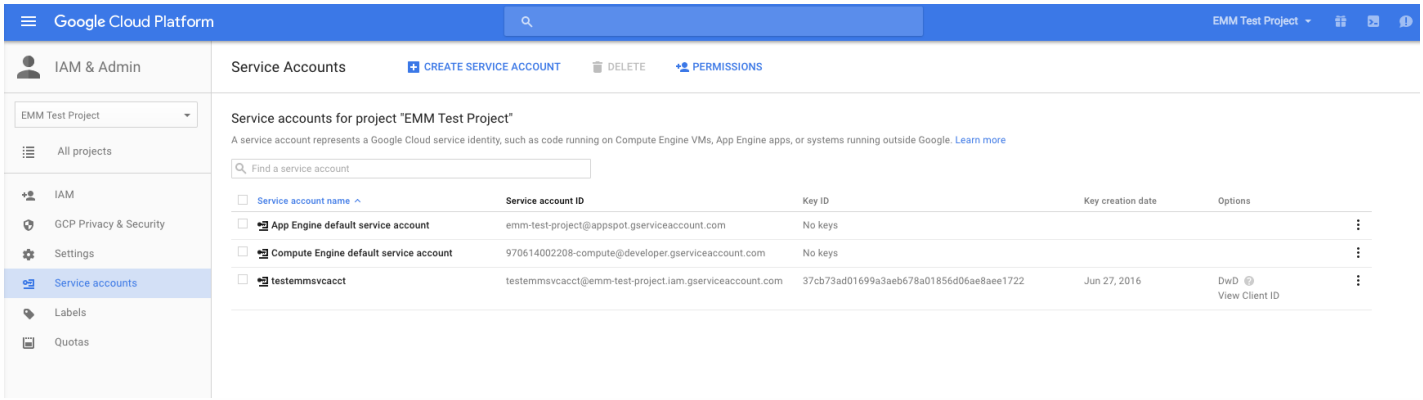


Le certificat (fichier P12) est téléchargé sur votre ordinateur. Veillez à enregistrer le certificat dans un emplacement sécurisé.

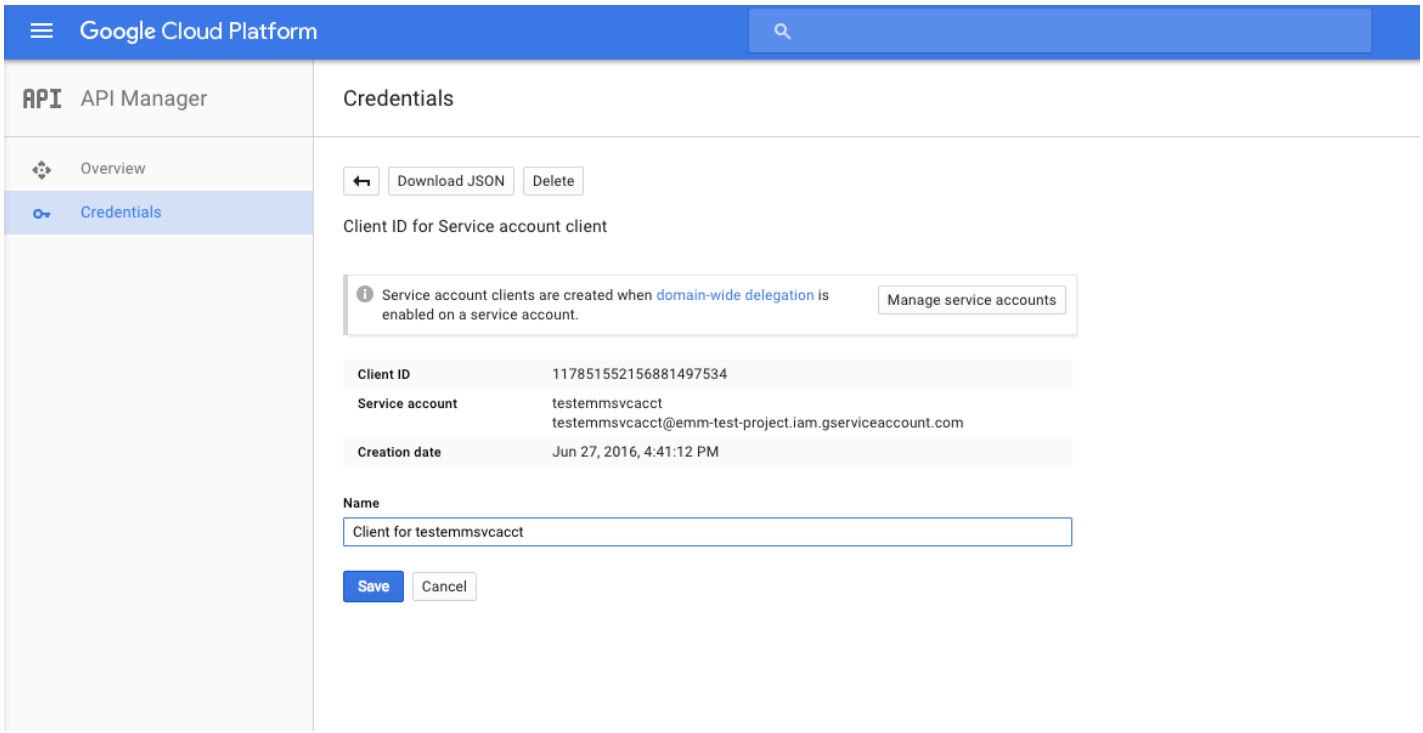
11. Sur l'écran de confirmation **Service account created**, cliquez sur **Close**.



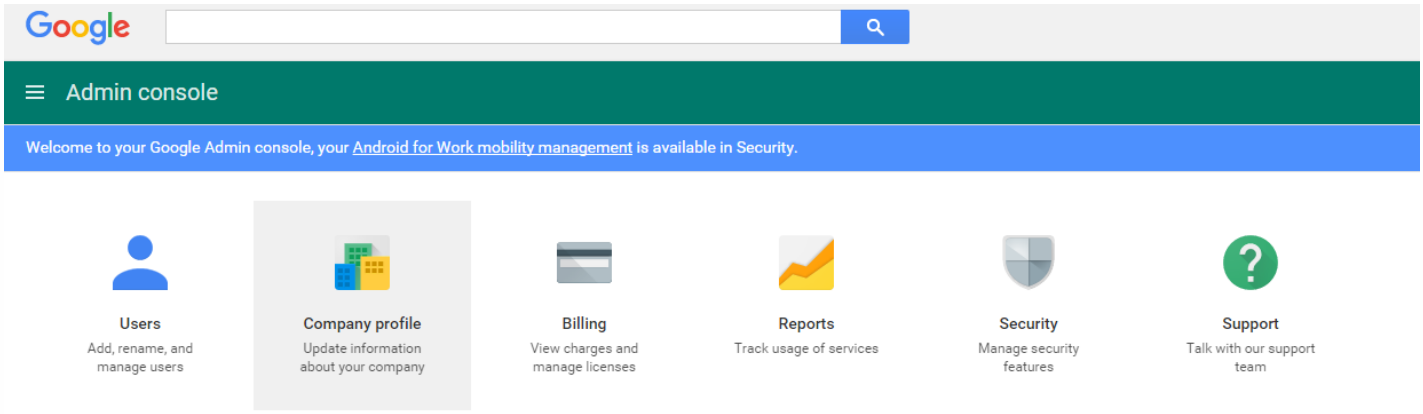
12. Dans **Permissions**, cliquez sur **Service accounts**, puis sous **Options** pour votre compte de service, cliquez sur **View Client ID**.



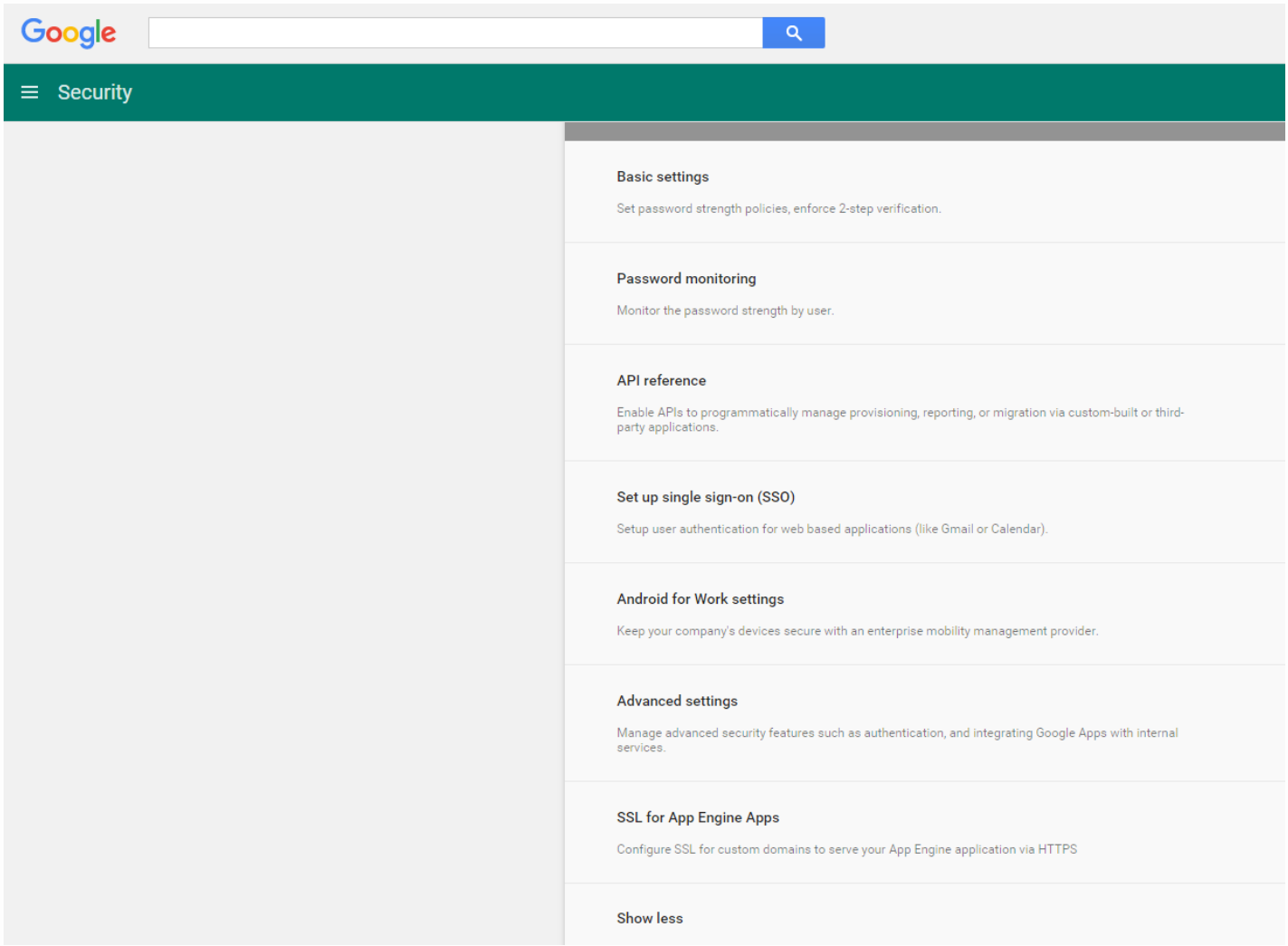
13. Les détails requis pour l'autorisation du compte sur la console d'administration Google s'affichent. Copiez les valeurs des champs **Client ID** et **Service account ID** sur un emplacement où vous pourrez récupérer les informations ultérieurement. Vous aurez besoin de ces informations, ainsi que du nom de domaine afin de les envoyer à l'assistance Citrix afin qu'ils puissent les placer en liste blanche.



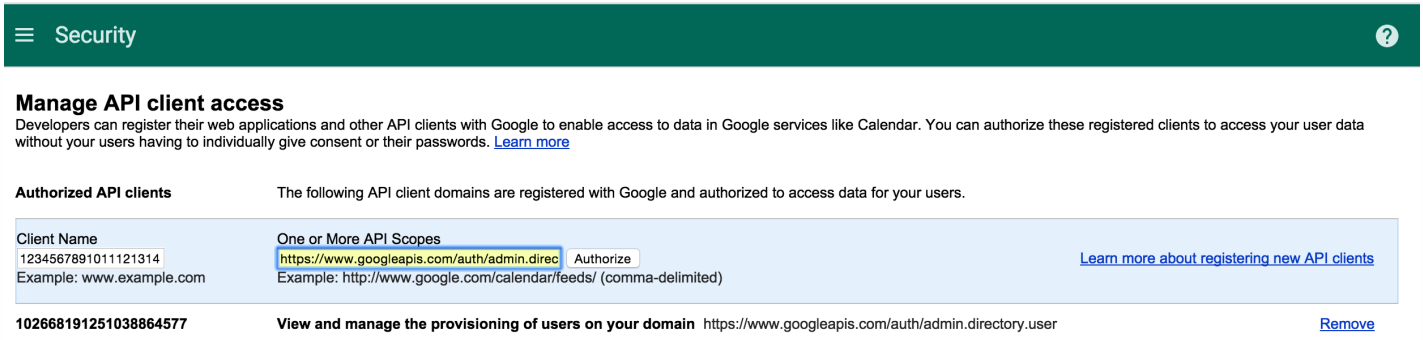
14. Ouvrez la console d'administration Google pour votre domaine et cliquez sur **Security**.



15. Cliquez sur les paramètres **Android for Work**.



16. Dans **Client Name**, entrez l'ID de client que vous avez enregistré précédemment, dans **One or More API Scopes**, entrez https://www.googleapis.com/auth/admin.directory.user puis cliquez sur **Authorize**.

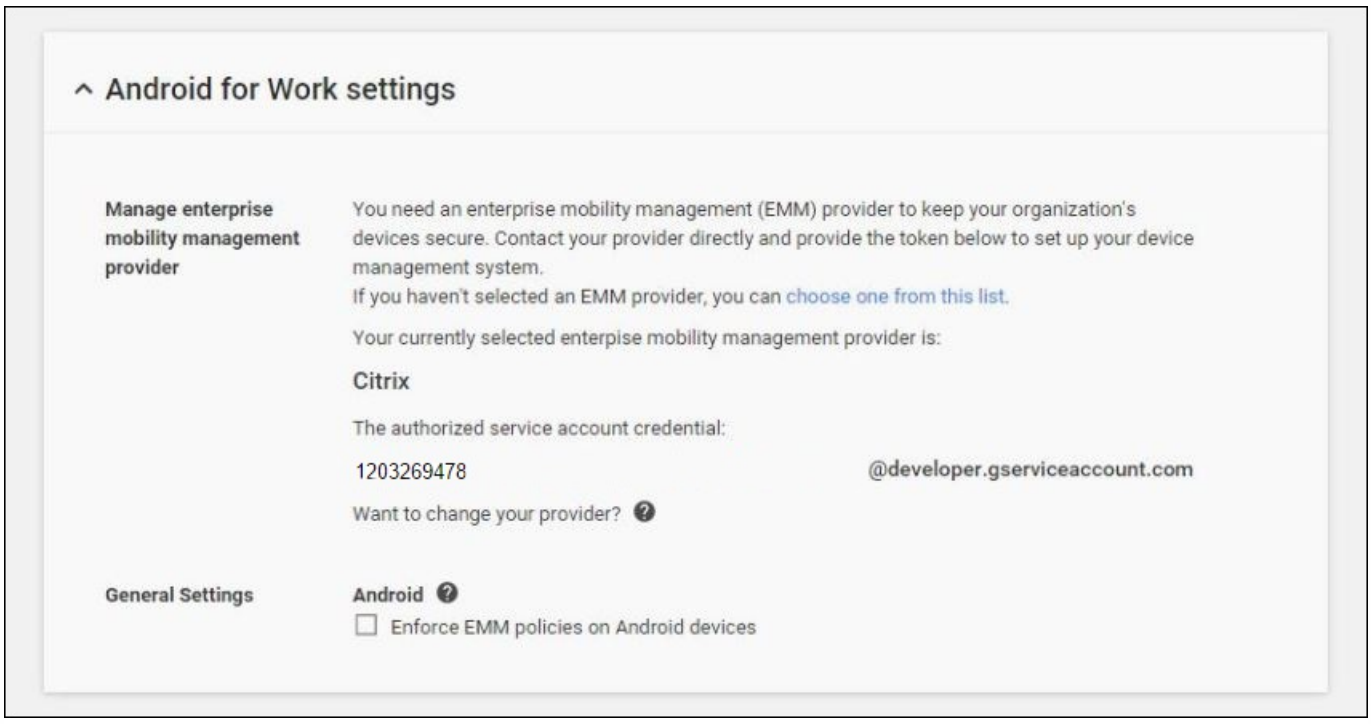


Liaison à EMM

Avant de pouvoir utiliser XenMobile pour gérer vos appareils Android for Work, vous devez contacter l'assistance technique de Citrix (https://www.citrix.com/contact/technical-support.html) et fournir votre nom de domaine, compte de service et jeton de liaison. Citrix liera le jeton à XenMobile en tant que fournisseur de gestion de la mobilité d'entreprise (EMM).

1. Pour confirmer la liaison, ouvrez une session sur le portail de la console d'administration Google et cliquez sur **Sécurité**.

2. Cliquez sur **Paramètres Android for Work**. Vous verrez que votre compte Google Android for Work est lié à Citrix en tant que fournisseur EMM.



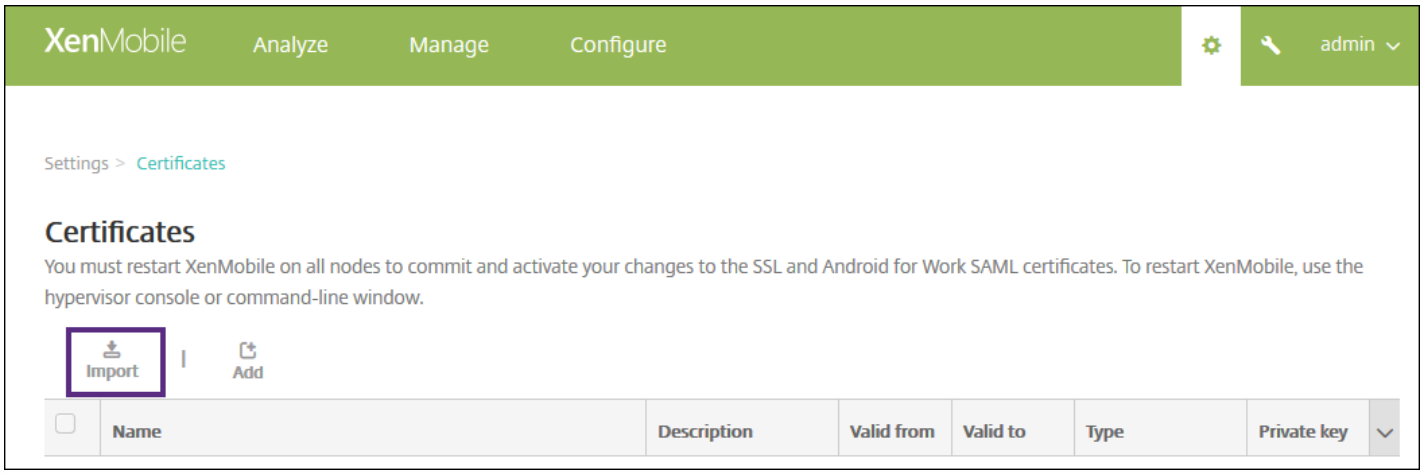
Après avoir confirmé la liaison du jeton, vous pouvez commencer à utiliser XenMobile pour gérer vos appareils Android for Work. Vous devez importer le certificat P12 que vous avez généré à l'étape 14, configurer les paramètres du serveur Android for Work, activer l'authentification unique SAML et définir au moins une stratégie d'appareil Android for Work.

Importer le certificat P12

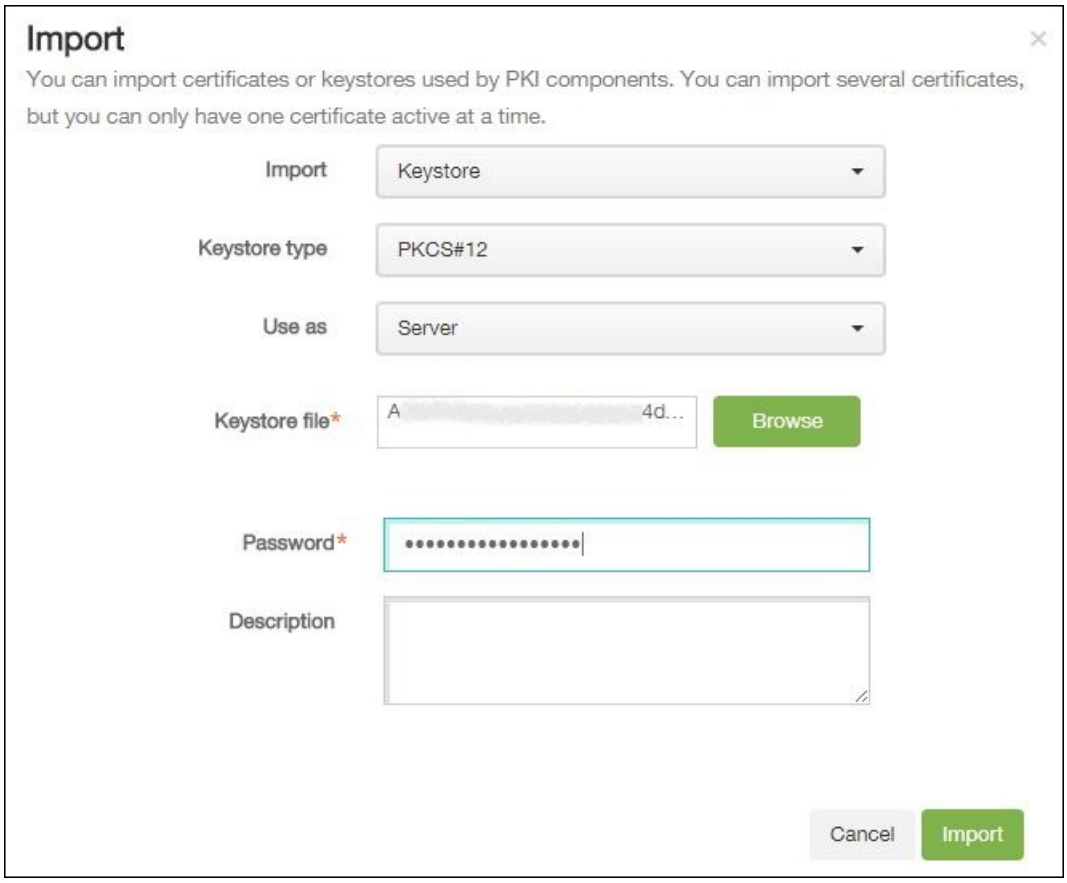
Suivez ces étapes pour importer votre certificat P12 Android for Work :

1. Ouvrez une session sur 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**.

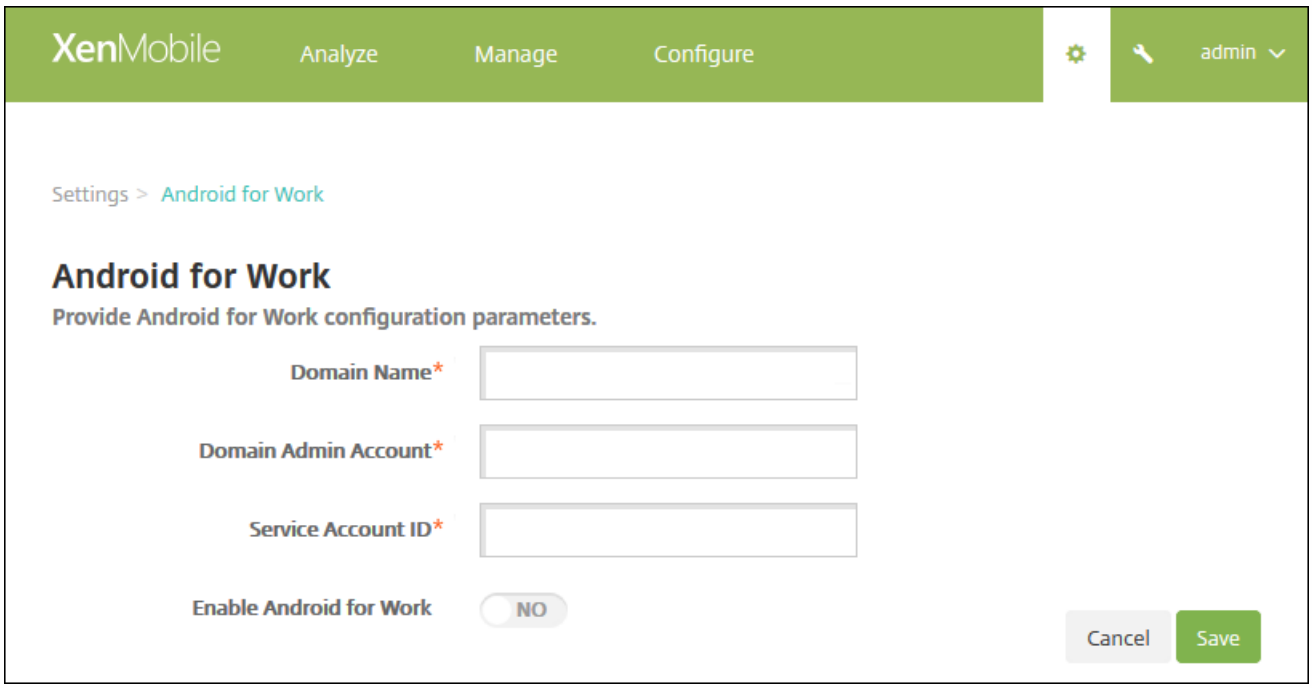
- **Utiliser en tant que** : dans la liste, cliquez sur **Serveur**.
- **Fichier de keystore** : cliquez sur **Parcourir** et accédez au certificat P12.
- **Mot de passe** : entrez le mot de passe du keystore.
- **Description** : entrez une description pour le certificat.

4. Cliquez sur **Importer**.

Configurer les paramètres du serveur Android for Work

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 **Android for Work**. La page **Android for Work** s'affiche.



Configurez les paramètres suivants :

- **Nom de domaine** : entrez votre nom de domaine Android for Work ; 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).
- **Activer Android for Work** : cliquez pour activer ou désactiver Android for Work.

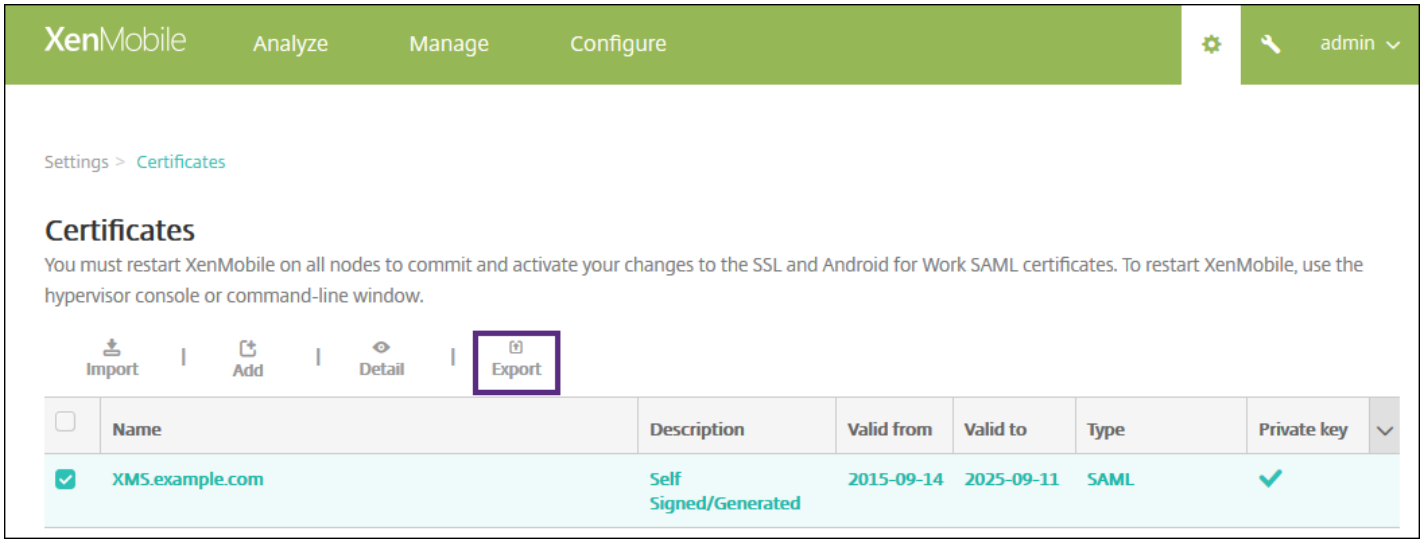
3. Cliquez sur **Enregistrer**.

Activer l'authentification unique SAML

1. Ouvrez une session sur la console XenMobile.

2. Cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

Cliquez sur **Certificats**. La page **Certificats** s'affiche.

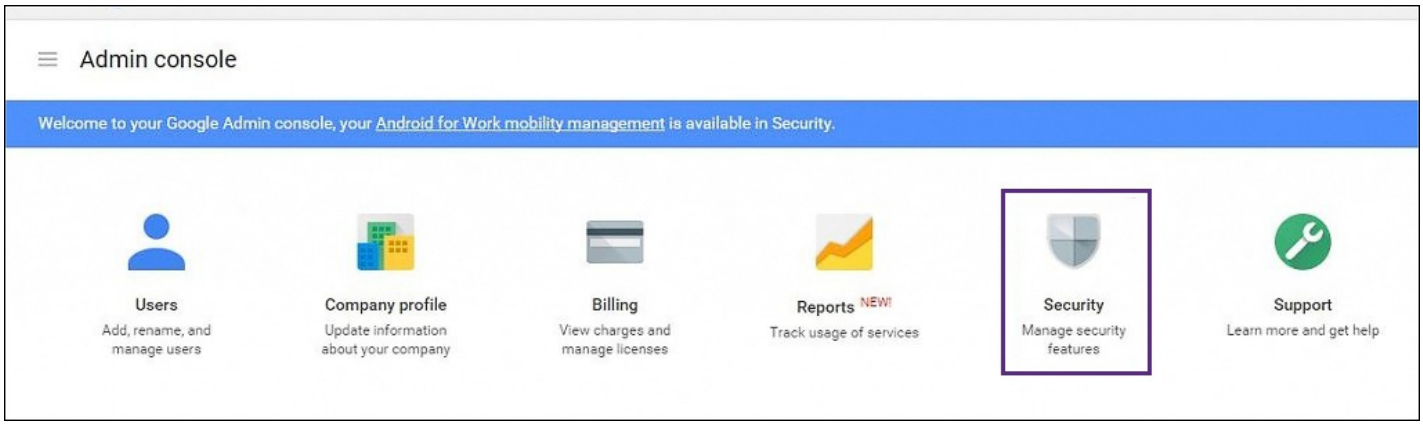


3. Dans la liste des certificats, cliquez sur le certificat SAML.

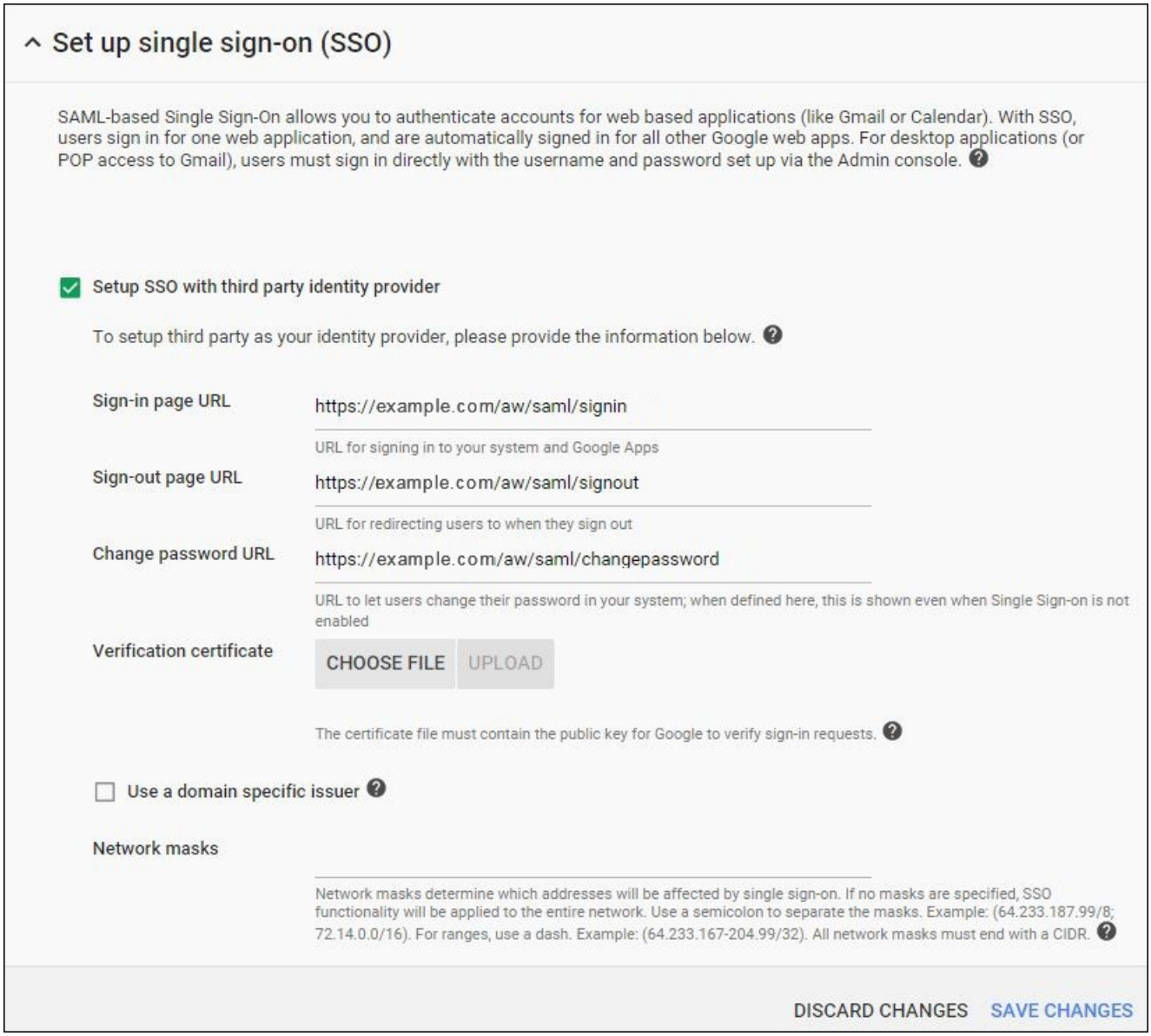
4. Cliquez sur **Exporter** et enregistrez le certificat sur votre ordinateur.

5. Ouvrez une session sur le portail de la console d'administration Google (https://admin.google.com) avec vos identifiants d'administrateur Android for Work.

6. Cliquez sur **Sécurité**.



7. Dans **Sécurité**, cliquez sur **Configurer l'authentification unique (SSO)** et configurez les paramètres suivants :

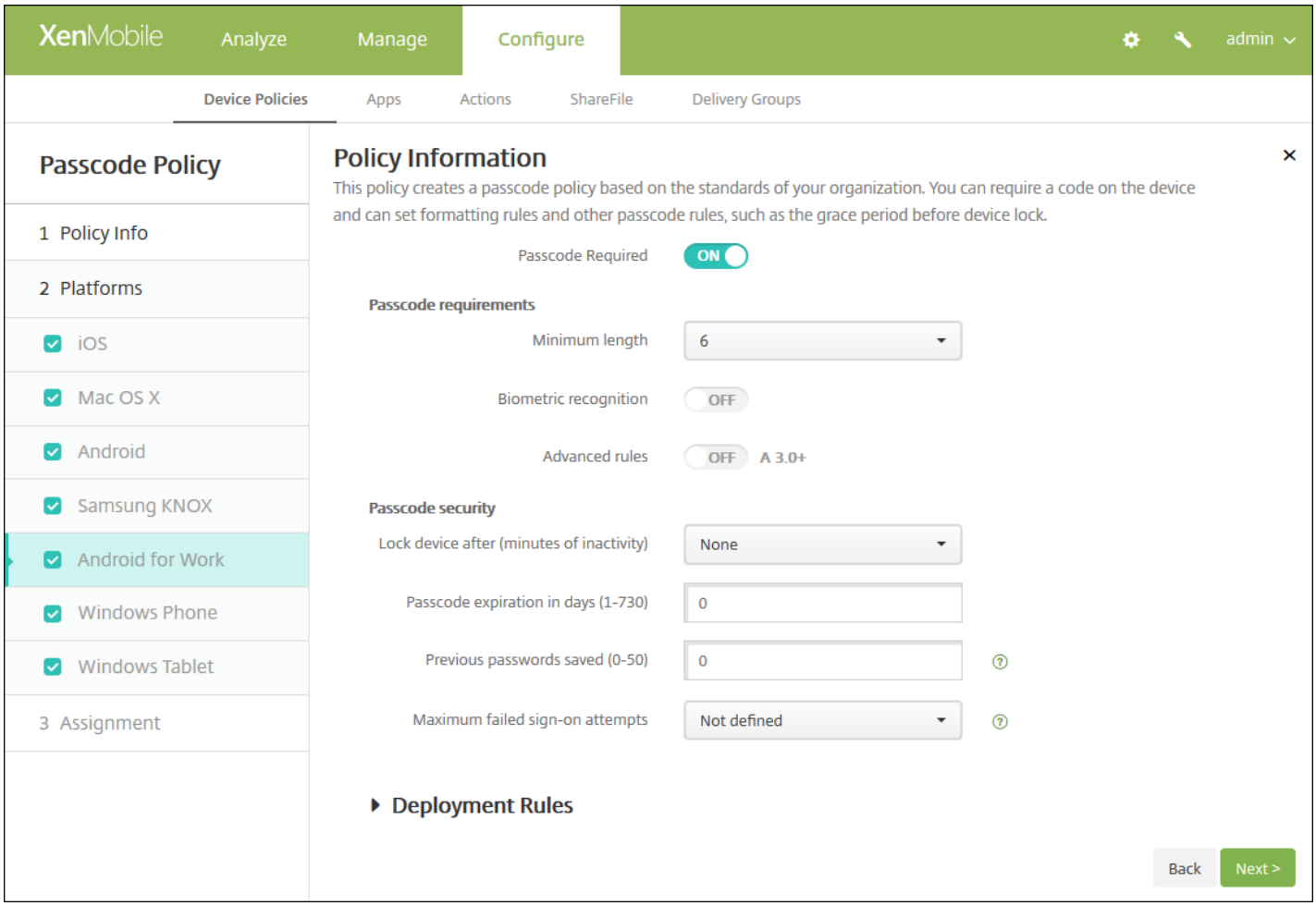


- **URL de la page de connexion** : entrez l'adresse URL des utilisateurs qui se connectent prendre part votre système et Google Apps. Par exemple : https:///aw/saml/signin.
- **URL de la page de déconnexion** : entrez l'adresse URL vers laquelle les utilisateurs sont redirigés lorsqu''ils se déconnectent. Par exemple : https:///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:///aw/saml/changepassword. Lorsque cette option est définie ici, les utilisateurs voient cette fonctionnalité même si SSO n'est pas disponible.
- **Certificat de vérification :** cliquez sur CHOISIR FICHIER et accédez à l'emplacement du certificat SAML exporté depuis XenMobile.

8. Cliquez sur **ENREGISTRER LES MODIFICATIONS**.

Configurer une stratégie d'appareil Android for Work

Vous pouvez configurer n'importe quelle stratégie, mais il est recommandé de configurer 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. Ouvrez une session sur la console XenMobile.

2. Cliquez sur **Configurer > 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 for Work** et configurez les paramètres pour la stratégie.

6. Attribuez la stratégie à un groupe de mise à disposition.

Pour de plus amples informations sur la configuration d'autres stratégies disponibles pour Android for Work, consultez la section Stratégies XenMobile par plate-forme.

Configurer les paramètres de compte Android for Work.

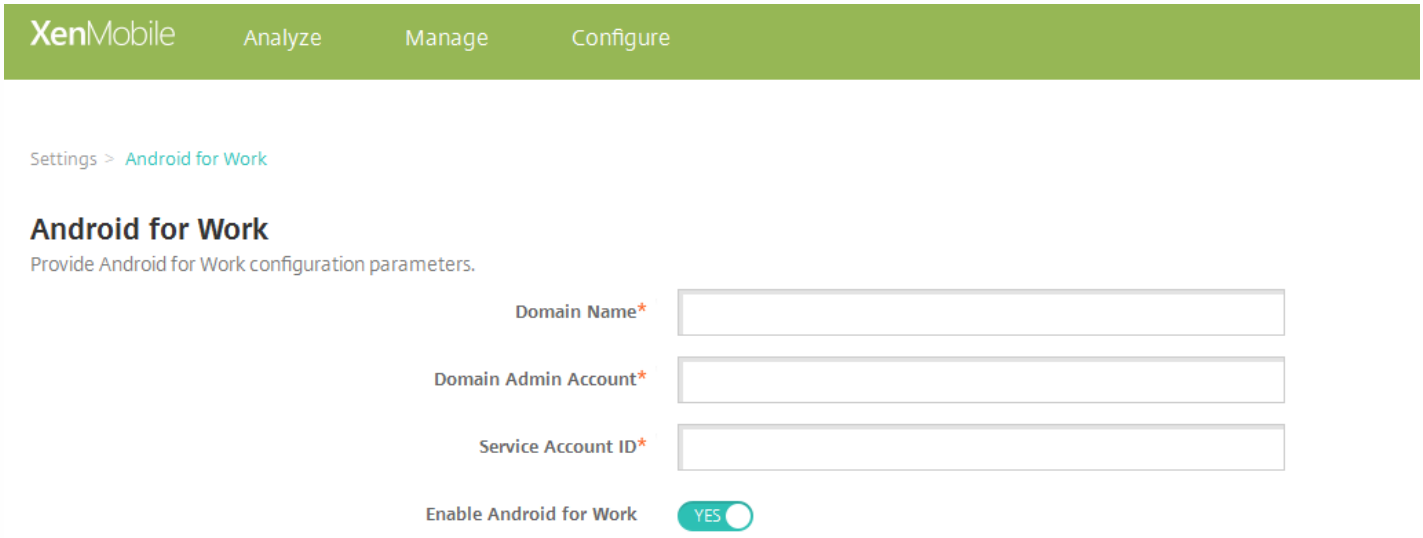
Jul 27, 2016

> ## Avertissement
>
> Un problème connu tiers existant vous empêche d'utiliser la console XenMobile pour activer Android for Work. Pour de plus amples informations sur ce problème et la façon de configurer une propriété de serveur pour le résoudre, consultez le problème #615118 dans la section Problèmes connus de XenMobile Server 10.3.

Avant de démarrer la gestion des applications et des stratégies Android for Work sur les appareils des utilisateurs, vous devez définir les informations de domaine et de compte Android for Work dans XenMobile. Avant de procéder, toutefois, vous devez effectuer les tâches de configuration Android for Work sur Google pour configurer un administrateur de domaine et obtenir un ID de compte de service et un jeton de liaison. Pour de plus amples informations sur les tâches de configuration Android for Work sur Google, consultez la section Gestion des appareils avec Android for Work.

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 **Serveur**, cliquez sur **Android for Work**. La page de configuration **Android for Work** s'affiche.



3. Sur la page **Android for Work**, 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.
- **Activer Android for Work** : sélectionnez cette option pour activer Android for Work.

4. Cliquez sur **Enregistrer**.

Provisioning du mode Device Owner dans Android for Work

Jul 27, 2016

Pour provisionner Android for Work en mode Device Owner, vous devez transférer les données via NFC en cognant deux appareils, l'un exécutant l'application Worx Provisioning Tool et un autre dont les paramètres d'usine ont été réinitialisés, et suivre les étapes détaillées dans ce document. Le mode Device Owner est uniquement disponible pour les appareils appartenant à l'entreprise.

Pourquoi utiliser le NFC ? 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 comprend dans cet état.

Pour obtenir un aperçu du déploiement d'Android for Work dans l'environnement XenMobile, consultez la section Gestion des appareils avec Android for Work dans XenMobile.

Conditions préalables

- Un serveur XenMobile avec Android for Work – versions 10.1 et 10.3.
- Un appareil dont les paramètres d'usine ont été réinitialisés, provisionné pour Android for Work en mode Device Owner. Les étapes à suivre sont décrites ci-dessous.
- Un autre appareil avec capacité NFC, exécutant l'application Worx Provisioning Tool configurée. Worx Provisioning Tool est disponible dans Worx Home 10.3 où sur la page des téléchargements de Citrix.

Chaque appareil ne peut disposer que d'un profil Android pour Work, géré par une application de gestion de la mobilité d'entreprise (EMM). Dans XenMobile, Worx Home est l'application EMM. Un seul profil est autorisé sur chaque appareil. Si vous essayez d'ajouter une deuxième application EMM, la première sera supprimée.

Vous pouvez démarrer le mode Device Owner sur de tout nouveaux appareils ou sur des appareils dont les paramètres d'usine ont été réinitialisés. La gestion de l'appareil sera effectuée entièrement sur XenMobile.

Partage de données à l'aide du NFC en mode Device Owner mode

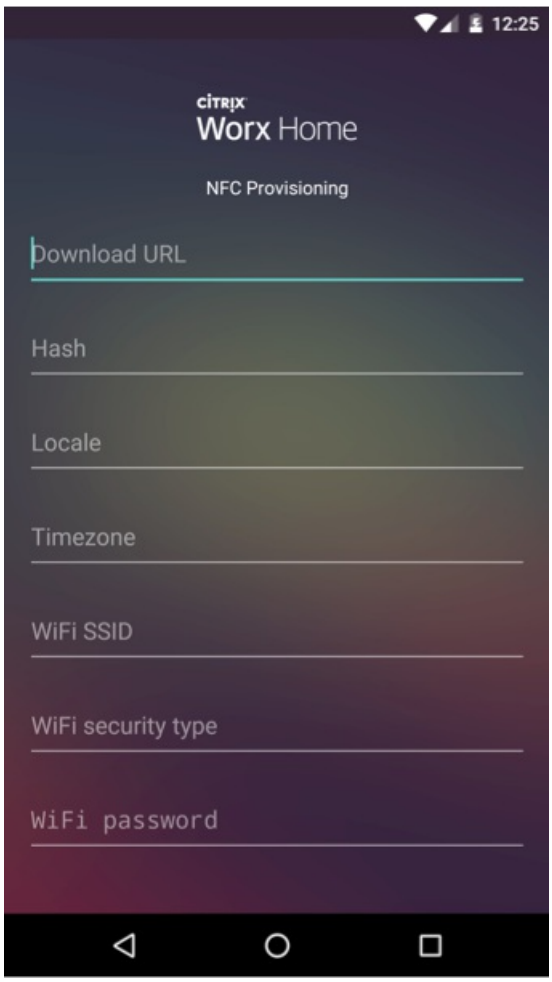
Le provisioning d'un appareil dont les paramètres d'usine ont été réinitialisés requiert que vous envoyiez les données suivantes via NFC pour lancer Android for Work :

- Nom du package de l'application EMM du fournisseur qui fera office de propriétaire de l'appareil (Worx Home).
- 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. (Android ne prend pas charge 802.1x Wi-Fi pour ce flux).
- Fuseau horaire de l'appareil (facultatif).
- Emplacement géographique de l'appareil (facultatif).

Lorsque les deux appareils sont « cognés », les données de Worx Provisioning Tool sont envoyées à l'appareil dont les paramètres d'usine ont été réinitialisés. Ces données sont ensuite utilisées pour télécharger Worx Home avec des paramètres d'administrateur. Si vous ne précisez pas le fuseau horaire ni l'emplacement, Android les configurera automatiquement sur le nouvel appareil.

Configuration de Worx Provisioning Tool

Avant de partager des données avec NFC, vous devez configurer Worx 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. 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.

Configuration à l'aide d'un fichier texte

Appelez le fichier **nfcprovisioning.txt** et placez-le sur la carte SD de l'appareil dans le dossier /sdcard/Downloads. 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=
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 (à l'aide du SSID, du type de sécurité et du mot de passe entrés dans l'écran ci-dessus), 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=

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 cette somme sont détaillées ci-dessous.

android.app.extra.PROVISIONING_WIFI_SSID=
Il s'agit du SSID Wi-Fi connecté de l'appareil sur lequel Worx Provisioning Tool est exécuté.

android.app.extra.PROVISIONING_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=
Si le Wi-Fi n'est pas protégé, ce champ doit être vide.

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. Si vous n'entrez aucun code, la langue et le pays sont automatiquement renseignés.

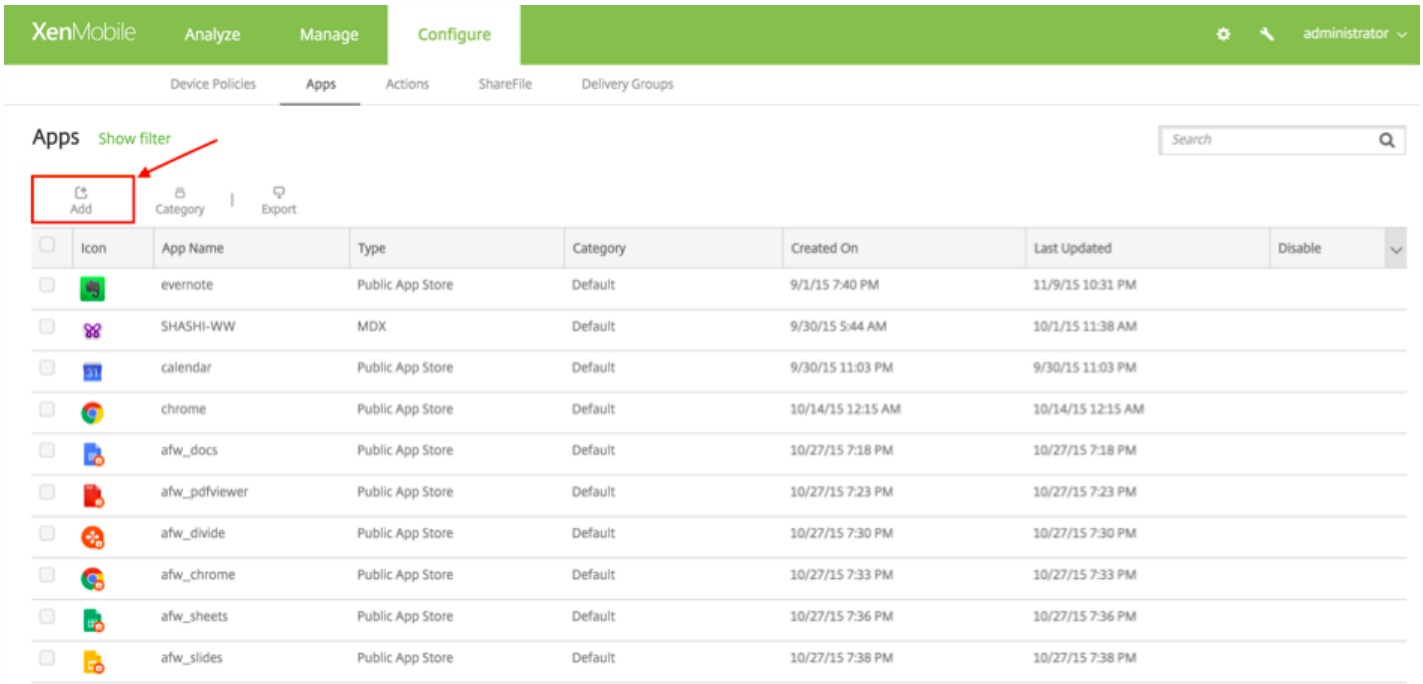
android.app.extra.PROVISIONING_TIME_ZONE=
Fuseau horaire dans lequel l'appareil est exécuté. Entrez un nom basé sur la base de données Olson au format zone/emplacement. Par exemple, Europe/Paris pour l'heure de l'Europe occidentale. Si vous n'entrez rien, le fuseau horaire est automatiquement renseigné.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=
Ce nom n'est pas requis car la valeur est codée en dur dans l'application Worx Home. Il n'est mentionné ici que par souci de complétude.

Obtention de la somme de contrôle Worx Home

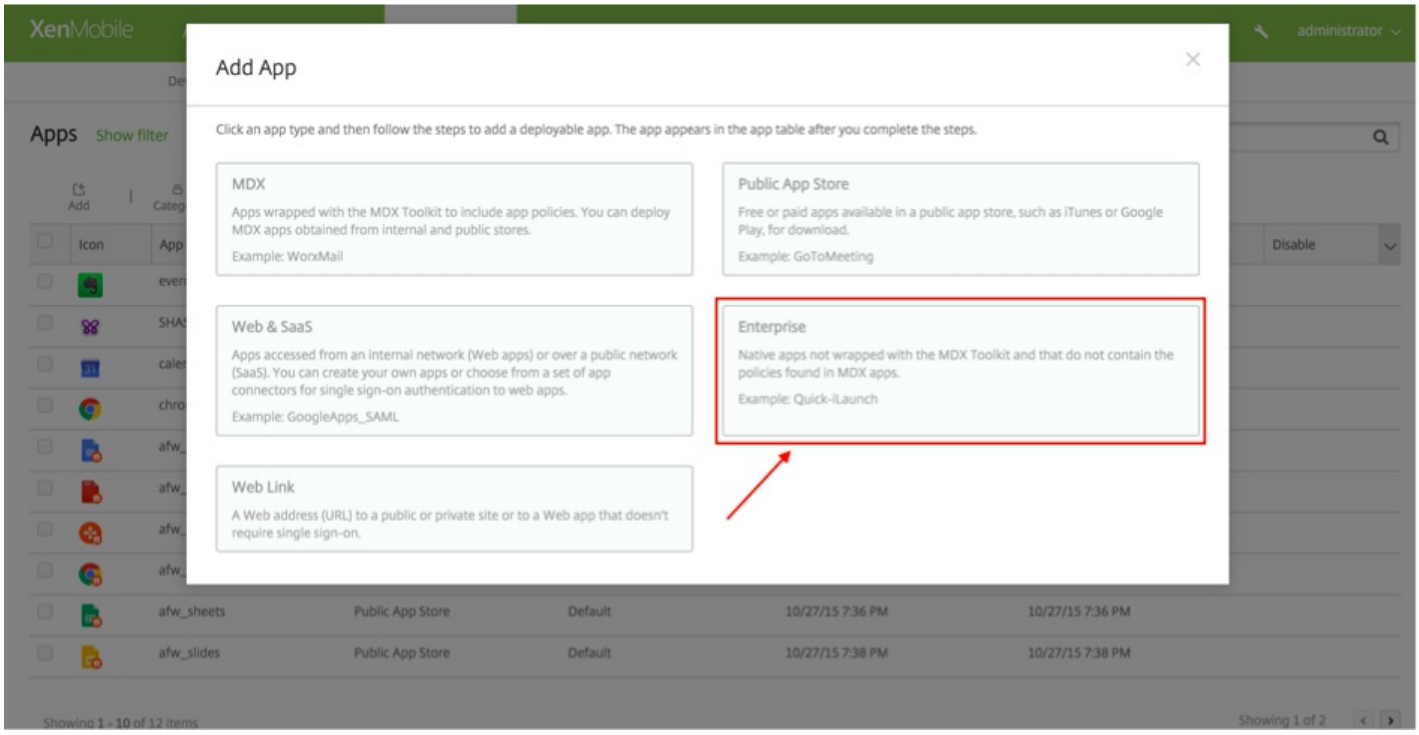
Pour obtenir la somme de contrôle d'une application, ajoutez l'application en tant qu'application d'entreprise.

1. Dans la console XenMobile, Accédez à **Configurer > Applications > Ajouter**.



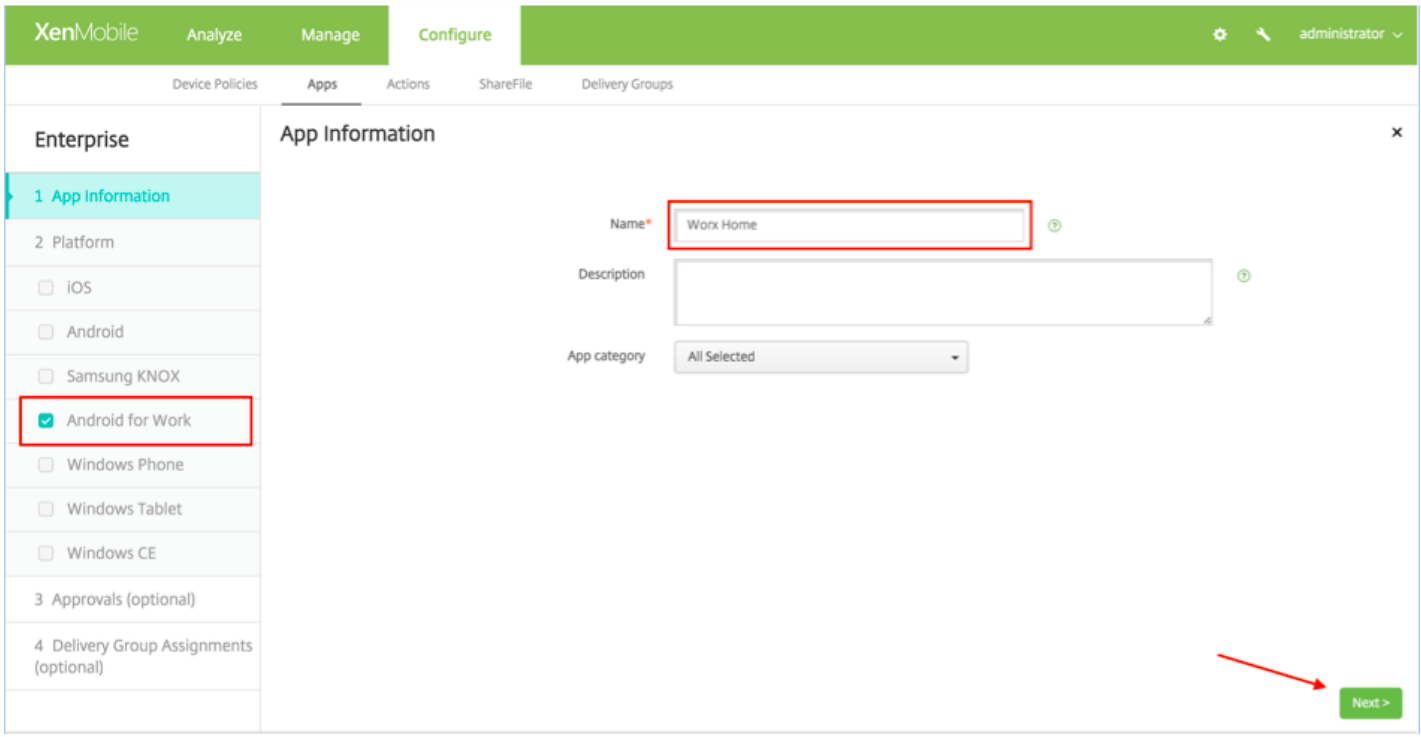
La fenêtre Ajouter une application s'affiche.

2. Cliquez sur **Entreprise**.



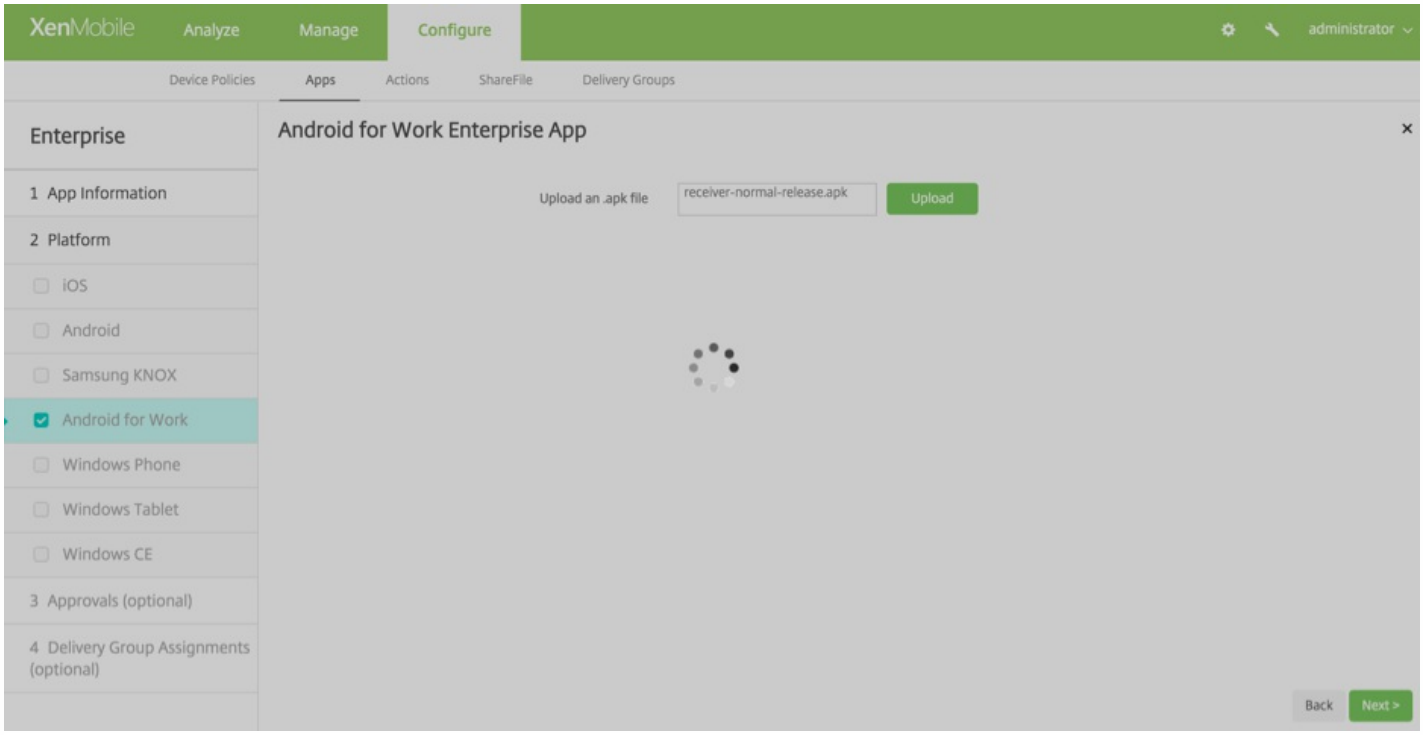
L'écran **Informations sur l'application** s'affiche.

3. Sélectionnez la configuration suivante et cliquez sur **Suivant**.

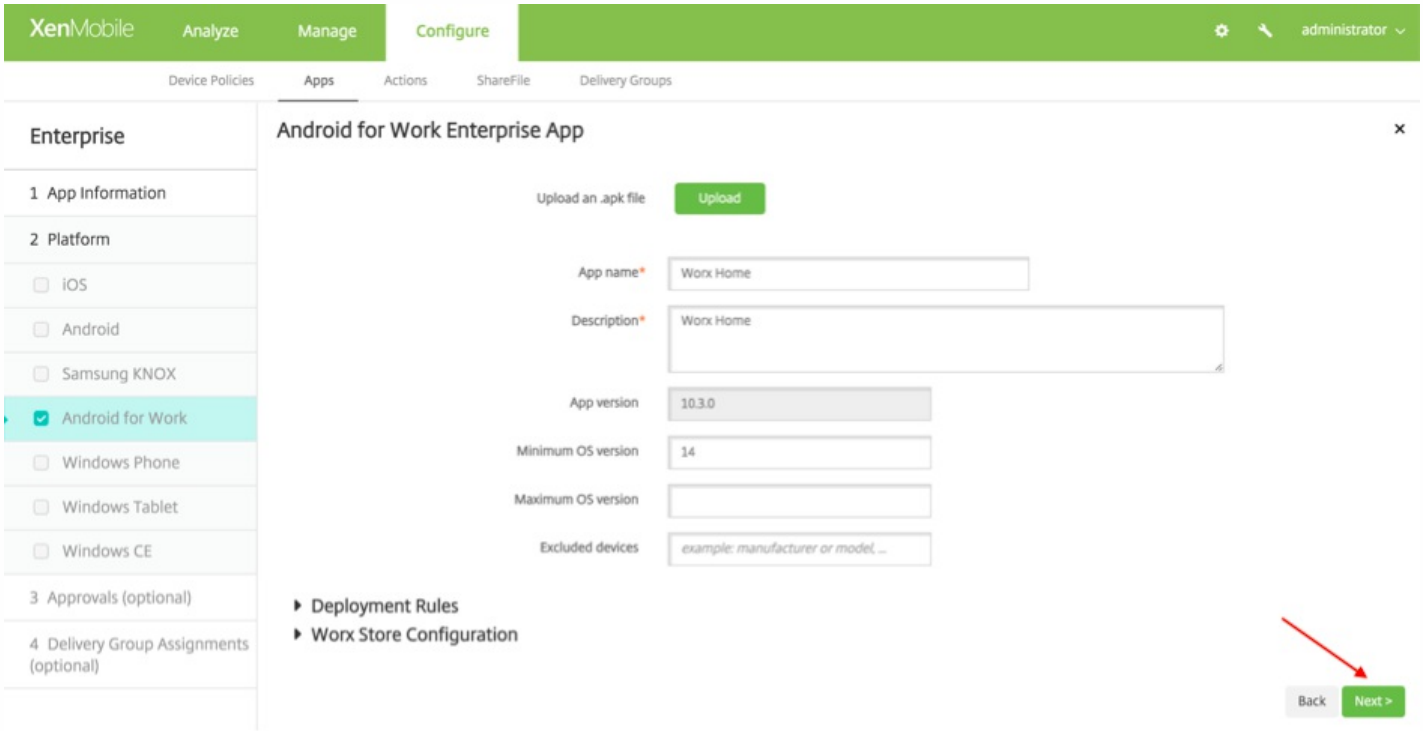


L'écran **Application Android for Work d'entreprise** s'affiche.

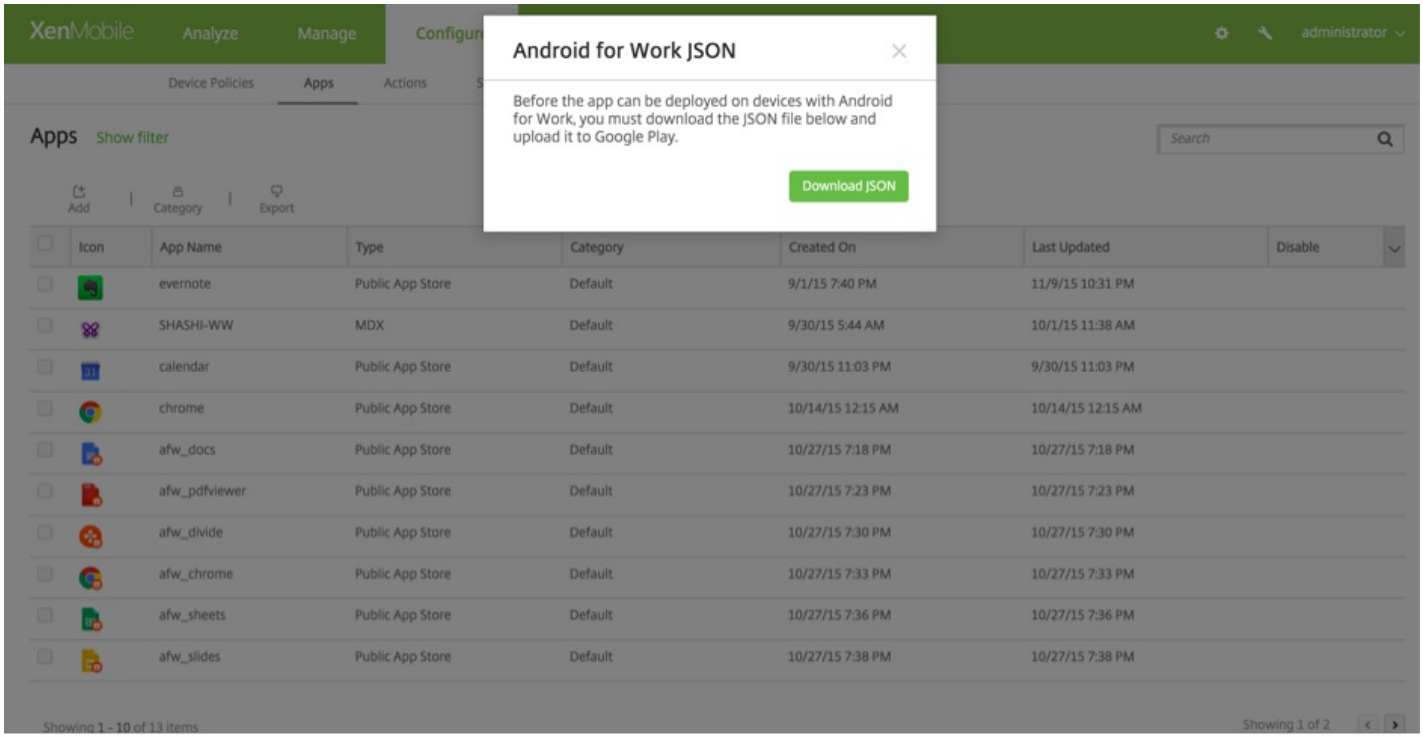
4. Fournissez le chemin d'accès au fichier .apk et cliquez sur **Suivant** pour charger le fichier.



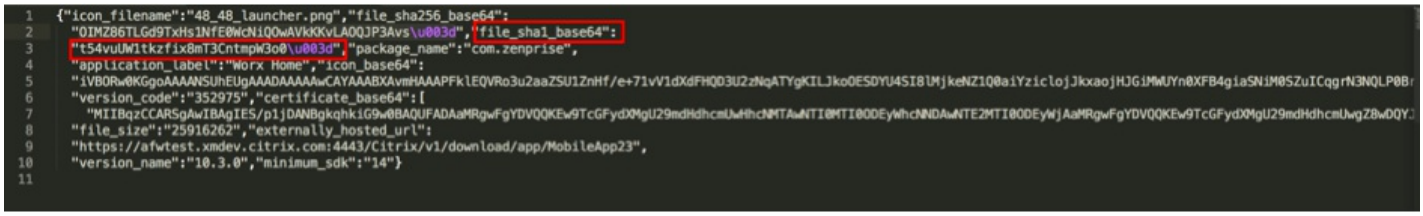
Une fois le chargement terminé, vous verrez les détails du package chargé.



5. Cliquez sur **Suivant** pour afficher un écran permettant de télécharger le fichier JSON, que vous pouvez ensuite utiliser pour le chargement sur Google Play. Pour Worx Home, 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 Worx 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 **=**

L'application procèdera à la conversion de sécurité si vous stockez le hachage dans le fichier nfcprovisioning.txt de la carte SD de l'appareil. Toutefois, si vous décidez d'entrer le hachage manuellement, il est de votre responsabilité de vous assurer que l'URL est sécurisée.

Bibliothèques utilisées

Worx Provisioning Tool utilise les bibliothèques suivantes dans son code source :

- Bibliothèque v7 appcompat par Google sous licence Apache 2.0

- Bibliothèque Design Support par Google sous licence Apache 2.0
- Bibliothèque v7 Palette par Google sous licence Apache 2.0
- Butter Knife par Jake Wharton sous licence Apache 2.0

Configuration des règles de déploiement

Oct 17, 2016

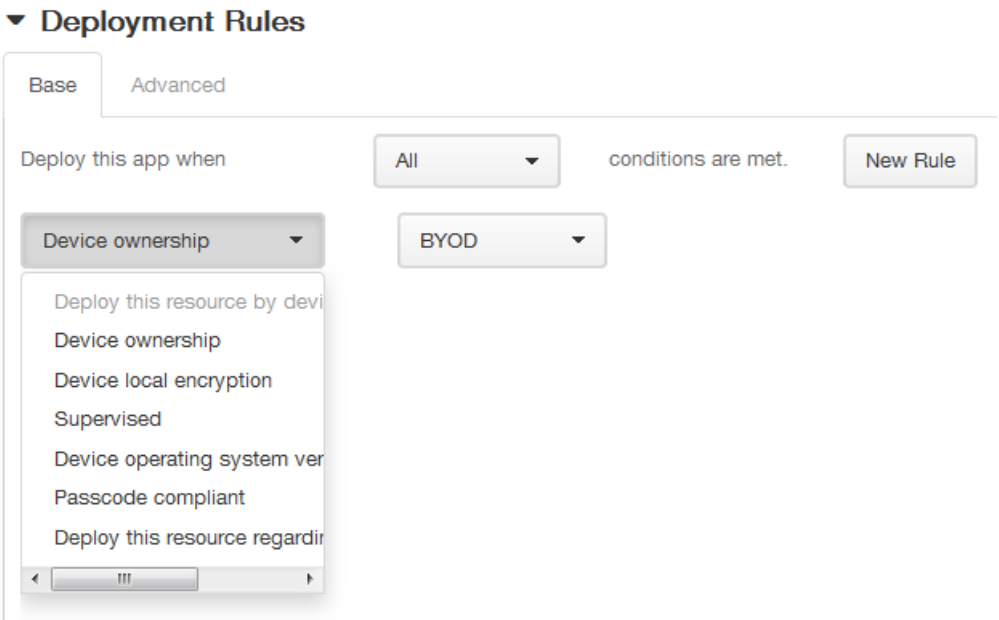
Cette section décrit :

- Les règles de déploiement : paramètres qui affectent le déploiement d'un paquetage.
- Les calendriers de déploiement : options qui spécifient quand XenMobile transmet les paquetages à un appareil.

Configuration des règles de déploiement

Les règles de déploiement sont des paramètres qui affectent le résultat du déploiement d'un paquetage. Vous pouvez spécifier des règles de déploiement pour des propriétés d'appareil, des applications et des actions. XenMobile utilise les règles de déploiement que vous spécifiez pour les propriétés d'appareil pour filtrer les stratégies, les applications, les actions et les groupes de mise à disposition afin de déterminer l'ordre de déploiement d'un paquetage. Pour de plus amples informations, consultez la section Ordre de déploiement.

Vous pouvez baser le déploiement d'un paquetage sur une version spécifique d'un système d'exploitation, sur une plate-forme matérielle particulière, ou une autre combinaison. Dans cet assistant utilisé pour ajouter et modifier les propriétés d'appareil, les applications et les actions sont un éditeur de règles **de base** et **avancé**. Le mode **Avancé** est un éditeur à format libre. L'image ci-dessous illustre l'écran **Règles de déploiement** accessible lors de l'ajout ou de la modification d'une application :



Règles de déploiement de base

Les règles de déploiement de base comprennent des tests prédéfinis et les actions résultantes. Lorsque cela est possible, les résultats sont préconfigurés dans des tests exemples. Par exemple, lorsque vous basez un déploiement de paquetage sur une plate-forme matérielle, toutes les plates-formes connues existantes sont entrées dans un test résultant, réduisant de manière drastique la durée de création de vos règles, et limitant les erreurs possibles.

Cliquez sur **Nouvelle règle** pour ajouter une règle au paquetage.

Remarque : le créateur de règles contient davantage d'informations, spécifiques à chaque test.

Pour créer une nouvelle règle, sélectionnez un modèle de règle, sélectionnez le type de condition, puis personnalisez la règle. La personnalisation de la règle inclut la modification de la description. Lorsque vous avez terminé les paramètres de configuration, vous devez ajouter la règle pour le paquetage.

Vous pouvez ajouter autant de règles que vous voulez. Le paquetage est déployé lorsque toutes les règles correspondent.

Règles de déploiement avancées

Si vous cliquez sur l'onglet **Avancé**, l'**Éditeur des règles avancées** s'affiche.

Dans ce mode, vous pouvez spécifier la relation définie entre les règles. Les opérateurs **AND**, **OR** et **NOT** sont disponibles.

Configuration de calendriers de déploiement

XenMobile utilise le calendrier de déploiement que vous spécifiez pour les actions, les applications et les stratégies d'appareil 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 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 du paramètre **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS. iOS utilise APNS.

Si vous ne modifiez pas les options de planification du déploiement, les déploiements se produisent immédiatement sur chaque connexion. Les options de planification du déploiement sont les suivantes :

Déployer : la valeur par défaut est **ON**. Pour empêcher le déploiement, modifiez ce paramètre sur **OFF**.

Calendrier de déploiement : la valeur par défaut est **Maintenant**. Pour spécifier une date de déploiement, sélectionnez **Plus tard**, puis choisissez une date et une heure.

Conditions de déploiement : la valeur par défaut est **À chaque connexion**. Pour limiter les déploiements, modifiez ce paramètre sur **Uniquement lorsque le déploiement précédent a échoué**.

Déployer pour les connexions permanentes : la valeur par défaut est **OFF**. Cette stratégie s'applique uniquement aux appareils Android. La propriété de serveur XenMobile, **Déploiement en arrière-plan**, nécessite que vous définissiez **Déployer pour les connexions permanentes** sur **ON** pour chaque stratégie déployée sur des appareils Android. Pour de plus amples informations sur les connexions permanentes, consultez les articles du manuel de déploiement de XenMobile « Other Server Optimizations » et « Optimizing Deployment Scheduling for Android Devices » dans la rubrique Tuning XenMobile Operations et l'article « Scheduling policy » dans la rubrique Device and App Policies.

Ajout d'appareils et affichage des détails des appareils

Jul 27, 2016

La base de données du serveur XenMobile stocke une liste des appareils mobiles. Chaque appareil mobile est défini par un numéro de série unique ou un numéro IMEI (identité internationale d'équipement mobile)/MEID (identifiant de l'équipement mobile). 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.

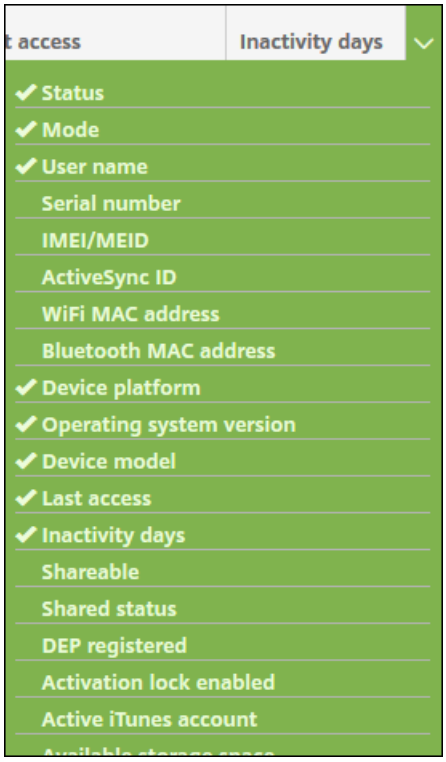
Sur la page **Appareils** dans la console XenMobile, vous trouverez un tableau répertoriant tous les appareils, avec les informations suivantes : **État** (icônes qui représentent l'état jailbreaké de l'appareil, indiquent s'il est géré, si Active Sync Gateway est disponible et l'état de son déploiement), **Mode** (si le mode est MDM, MAM ou les deux), **Nom d'utilisateur**, **Plate-forme de l'appareil**, **Version du système d'exploitation**, **Modèle d'appareil**, **Dernier accès** et **Jours d'inactivité**.

Vous pouvez ajouter des appareils manuellement, importer des appareils à partir d'un fichier de provisioning, modifier les détails de l'appareil, envoyer des notifications aux appareils et supprimer des appareils. Vous pouvez également exporter toutes les données de tableau d'un appareil dans un fichier .csv, ce qui vous permet de générer un rapport personnalisé. Le serveur exporte tous les attributs de l'appareil et si vous appliquez des filtres, ces derniers sont pris en compte lors de la création du fichier .csv.

Remarque : les en-têtes précédents sont les valeurs par défaut. Vous pouvez personnaliser les éléments affichés dans le tableau **Appareils** en cliquant sur la flèche vers le bas sur le dernier en-tête, puis en cliquant sur les en-têtes supplémentaires vous voulez voir dans le tableau ou en supprimant ceux que vous ne souhaitez pas voir.

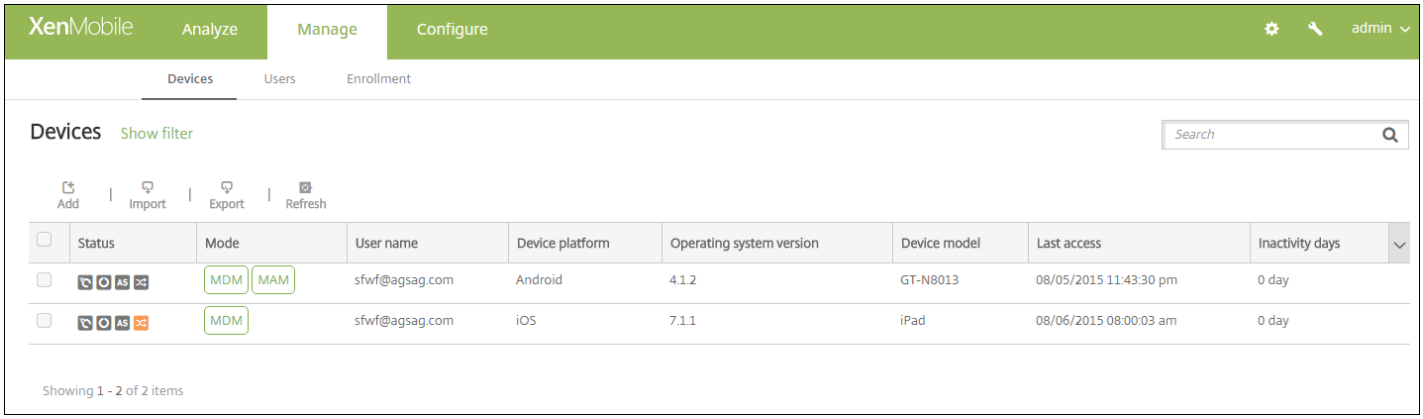
Consultez les sections suivantes pour connaître les différentes actions que vous pouvez effectuer dans le tableau **Appareils** :

- Ajouter un appareil manuellement
- Importer des appareils à partir d'un fichier de provisioning
- Modifier un appareil
- Envoyer des notifications aux appareils
- Supprimer des appareils
- Exporter le tableau **Appareils** dans un fichier .csv

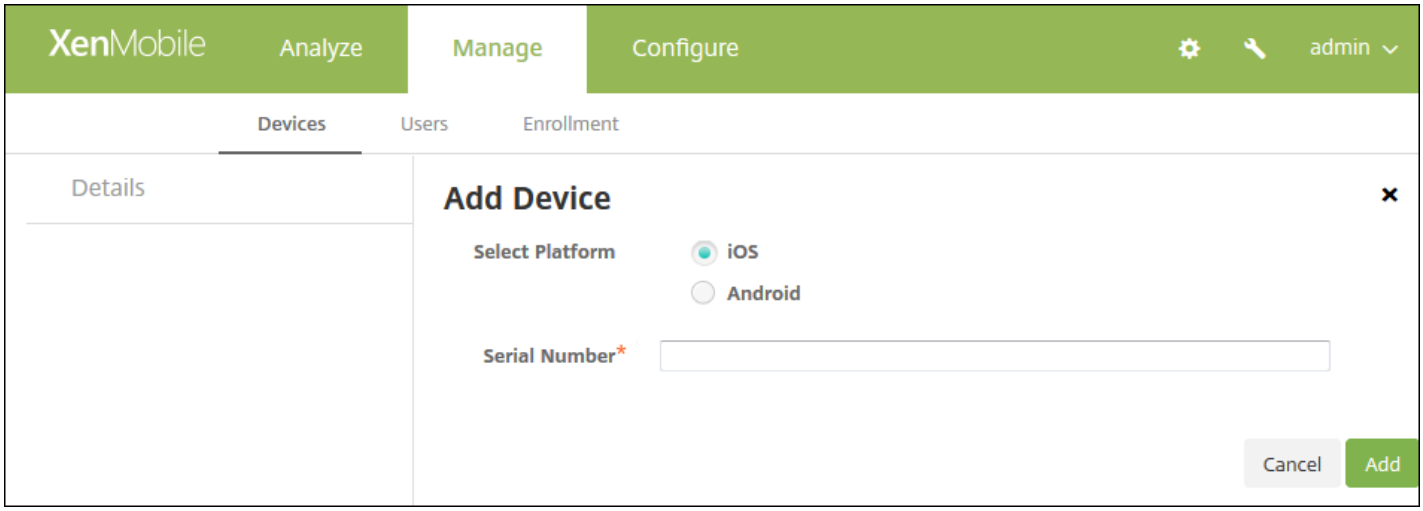


Pour ajouter un appareil manuellement

1. Dans la console XenMobile, cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.



2. Cliquez sur **Add**. La page **Ajouter un appareil** s'affiche.

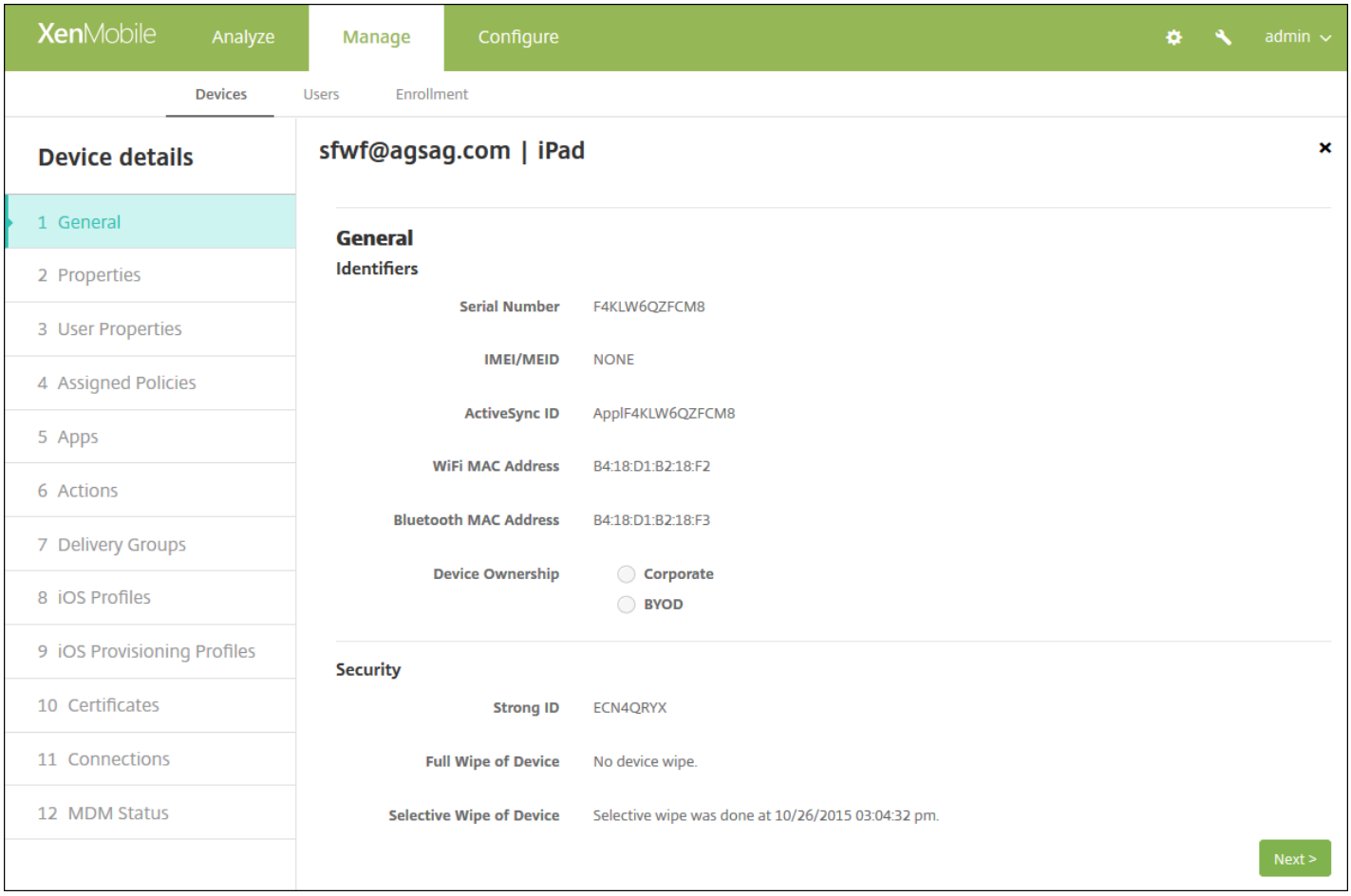


3. Configurez les paramètres suivants :

- **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 **Add**. Le tableau **Appareils** s'affiche avec l'appareil ajouté en bas de la liste. Dans 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 ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.



5. Sous **Général : identificateurs**, confirmez les informations affichées (la liste exacte varie en fonction du type de plate-forme):

- Numéro de série
- IMEI/MEID
- ID ActiveSync
- Adresse MAC Wi-Fi
- Adresse MAC Bluetooth
- Propriétaire

6. Sous **Sécurité**, confirmez les informations affichées (la liste exacte varie en fonction du type de plate-forme):

- Identifiant fort
- Effacement complet de l'appareil
- Effacement des données d'entreprise de l'appareil
- Verrouiller l'appareil
- Déverrouiller l'appareil
- Localisation de l'appareil
- Activer le suivi de l'appareil
- Exclusion de l'appareil
- Contourner le verrouillage d'activation
- Effacer les restrictions sur l'appareil

- Demander la mise en miroir AirPlay
- Arrêter la mise en miroir AirPlay

Remarque : le verrouillage de l'appareil pour iOS est disponible pour iOS 7 et versions ultérieures.

7. Cliquez sur **Suivant**. La page **Propriétés** apparaît dans laquelle vous pouvez ajouter des propriétés pour l'appareil.

8. Cliquez sur **Add**. Une liste des propriétés disponibles s'affiche.

9. Pour chaque propriété que vous voulez ajouter, procédez comme suit :

- Cliquez sur la propriété à provisionner et définissez sa valeur. Par exemple, vous pouvez sélectionner la propriété **Verrouillage d'activation activé** et définir la valeur sur **Oui** ou **Non**.
- Cliquez sur **Terminé**.

10. Cliquez sur **Suivant**.

Remarque : lorsque vous ajoutez des propriétés, elles sont répertoriées sous **Propriétés**. Lorsque vous revenez sur la page **Propriétés** ultérieurement, les propriétés sont séparées dans différentes catégories.

La section **Stratégies attribuées** et les sections suivantes contiennent les informations récapitulatives sur l'appareil.

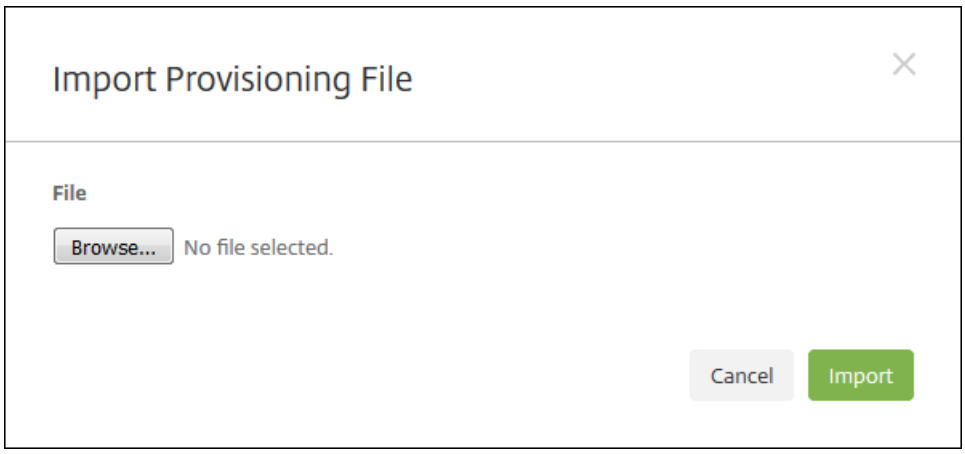
- **Stratégies attribuées** : affiche le nombre des stratégies attribuées, y compris le nombre de stratégies déployées, en attente ou ayant échoué. Les informations relatives au nom, au type et à la dernière date de déploiement s'affichent également pour chaque stratégie.
- **Applications** : affiche le nombre d'applications lors du dernier inventaire, ce qui comprend le nombre d'applications installées, en attente et ayant échoué.
- **Installé** : affiche les informations suivantes : nom, propriétaire, version, auteur, taille, installé, identifiant et type.
- Applications **En attente et Échec** : affiche les informations suivantes : nom, dernier déploiement, identifiant et type.
- **Actions** : affiche le nombre d'actions, ce qui comprend le nombre d'actions déployées, en attente et qui ont échoué. Chaque action affiche le nom du déploiement et la date à laquelle il a été déployé pour la dernière fois.
- **Groupes de mise à disposition** : affiche le nombre de groupes de mise à disposition ayant réussi, en attente et qui ont échoué. Les **groupes de mise à disposition** et des informations sur l'heure s'affichent pour chaque action. En outre, des informations plus détaillées s'affichent pour le **groupe de mise à disposition**, comprenant notamment l'état, le propriétaire et la date de l'action.
- **Profils iOS** (appareils iOS uniquement) : affiche le dernier inventaire de profil iOS et comprend notamment le nom, le type, l'organisation et une description.
- **Certificats** : affiche le nombre de certificats valides et de certificats révoqués ou ayant expiré, y compris le type, le fournisseur, l'émetteur, le numéro de série et la date de validité.
- **Connexions** : affiche l'état de la première connexion et de la dernière connexion. Pour chaque connexion, le nom d'utilisateur, l'avant-dernière authentification et la dernière authentification s'affichent.
- **TouchDown** (appareils Android uniquement) : affiche la dernière authentification de l'appareil et le dernier utilisateur à s'être authentifié. Chaque nom de stratégie et valeur de stratégie applicables s'affiche.

12. Cliquez sur **Enregistrer**.

Pour 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. Voir Formats des fichiers de provisioning.
1. Dans le menu au-dessus du tableau **Appareils**, cliquez sur **Importer**. La boîte de dialogue **Importer le fichier de**

provisioning apparaît.

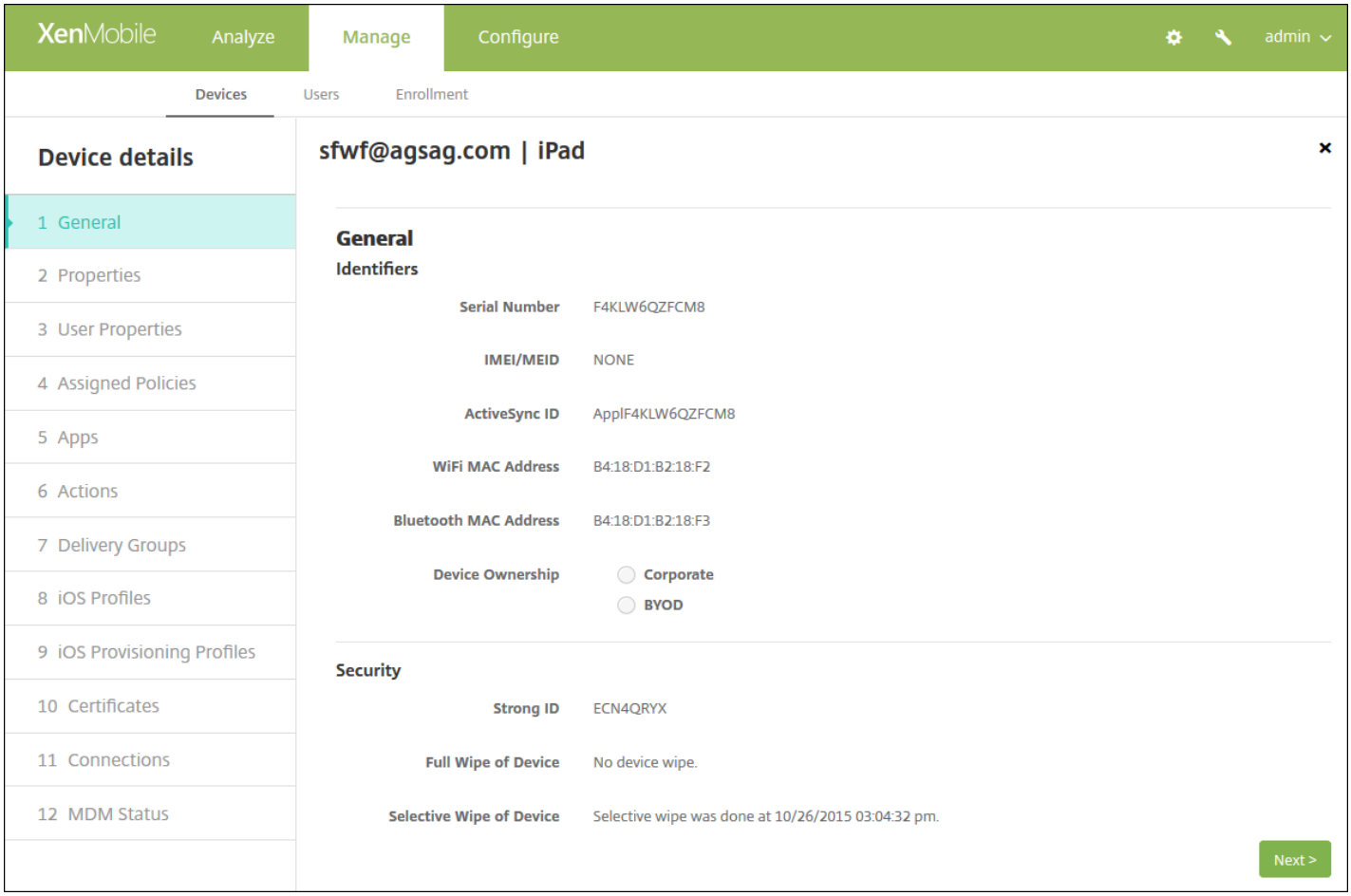


2. Sélectionnez le fichier à importer en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

3. Cliquez sur **Importer**. Les fichiers importés sont ajoutés au tableau **Appareils**.

Pour modifier des appareils

1. Sélectionnez l'appareil à modifier et cliquez sur Modifier. La page Détails de l'appareil s'affiche.



2. Sous **Général : identifiants**, le seul champ que vous pouvez modifier est **Propriétaire**, que vous pouvez définir sur **Entreprise** ou **BYOD**.

3. Cliquez sur **Suivant**. La page **Propriétés** s'affiche.

4. Sur la page **Propriétés**, vous pouvez ajouter, modifier ou supprimer des propriétés.

- Pour ajouter une propriété, cliquez sur Ajouter dans la catégorie dans laquelle vous souhaitez ajouter une propriété, cliquez sur la propriété dans la liste qui s'affiche, puis ajoutez la valeur de la propriété. Cliquez sur **Terminé**.
- Pour modifier une propriété, cliquez sur la propriété, modifiez ses paramètres, puis cliquez sur **Terminé** ou **Annuler**.
- Pour supprimer une propriété, placez le curseur sur la liste et cliquez sur le X sur le côté droit. L'élément est supprimé immédiatement.

5. Cliquez sur **Suivant**. La page qui s'affiche ensuite dépend de l'appareil sélectionné. Pour certains appareils, la page **Propriétés utilisateur** s'affichera, et pour d'autres, c'est la page **Propriétés attribuées** qui s'affichera.

6. Si la page **Propriétés utilisateur** s'affiche, vous pouvez ajouter, modifier ou supprimer des propriétés utilisateur comme suit ; sinon, les pages restantes contiennent des informations récapitulatives sur l'appareil. Pour obtenir une description détaillée de ces pages, reportez-vous à Pour ajouter des appareils manuellement.

Remarque : la partie supérieure de la page **Propriétés utilisateur** ne peut pas être modifiée.

- Pour chaque propriété d'utilisateur que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - Dans la liste qui s'affiche, cliquez sur la propriété que vous voulez ajouter, entrez la valeur pour la propriété, puis cliquez sur **Terminé** ou **Annuler**.
- Pour modifier une propriété, cliquez sur la propriété, modifiez ses paramètres, puis cliquez sur **Terminé** ou **Annuler**.
- Pour supprimer une propriété, placez le curseur sur la liste et cliquez sur le X sur le côté droit. L'élément est supprimé immédiatement.

7. Sur chacune des pages suivantes, vérifiez les informations récapitulatives, puis cliquez sur **Suivant**.

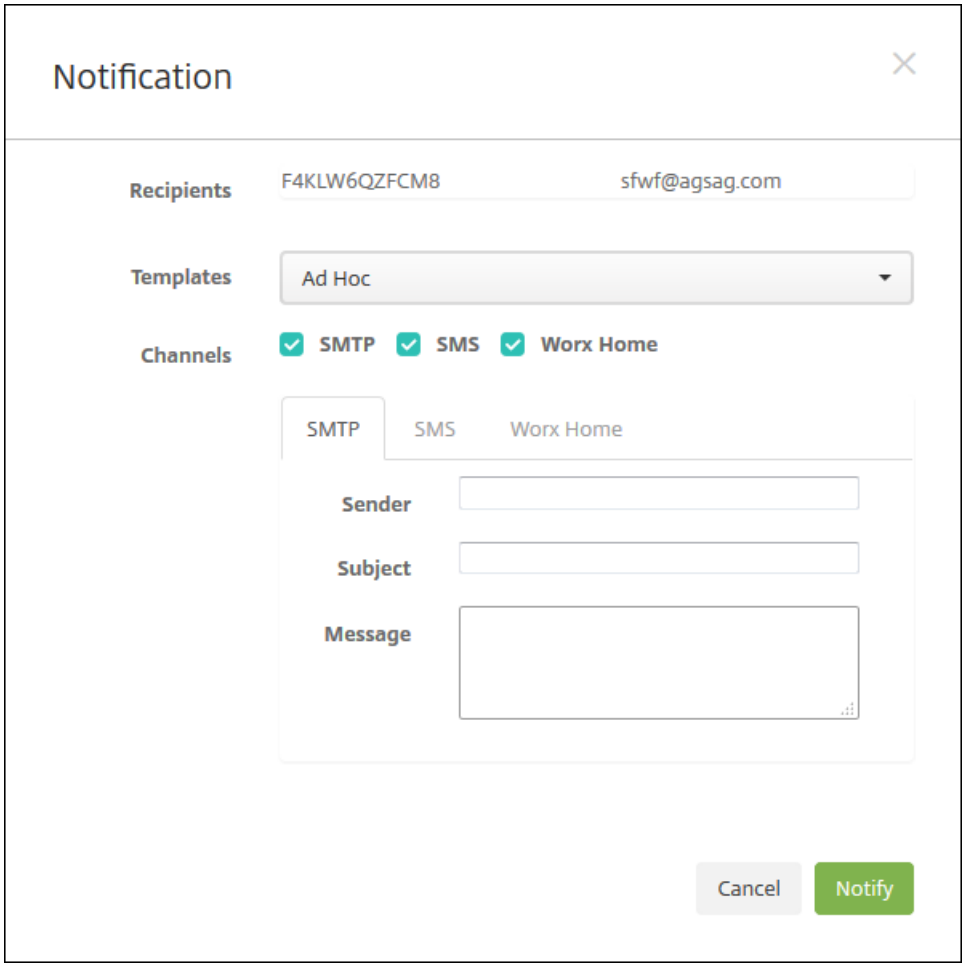
8. Sur la page finale, cliquez sur **Enregistrer** pour enregistrer les modifications sur l'appareil.

Pour envoyer une notification aux appareils

Vous pouvez envoyer des notifications aux appareils à partir de la page Appareils. Pour de plus amples informations sur les notifications, consultez la section Pour créer ou mettre à jour des modèles de notification dans XenMobile.

1. 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. Configurez les paramètres suivants :

- **Modèles** : dans la liste, cliquez sur le type de notification que vous souhaitez envoyer. Les champs **Sujet** et **Message** sont renseignés avec le texte configuré pour le modèle que vous avez choisi, sauf pour le modèle **Ad Hoc**.
- **Canaux** : sélectionnez la méthode à utiliser pour envoyer le message. La valeur par défaut est **SMTP**, **SMS** et **Worx Home**. Vous pouvez cliquer sur les onglets **SMTP**, **SMS** et **Worx Home** pour afficher le format du message pour chaque option.
- **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**.

Pour supprimer des appareils

1. Dans le tableau Appareils, sélectionnez l'appareil ou les appareils que vous voulez supprimer.
2. Cliquez sur Supprimer. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur Supprimer.
   Important : vous ne pouvez pas annuler cette opération.

Pour exporter le tableau Appareils

1. Cliquez sur le bouton **Exporter** au-dessus du tableau **Appareils**. XenMobile extrait les informations du tableau Appareils et les convertit en fichier .csv.

2. Ouvrez ou enregistrez le fichier .csv. Cette opération dépend du navigateur que vous utilisez. Vous pouvez également annuler l'opération.

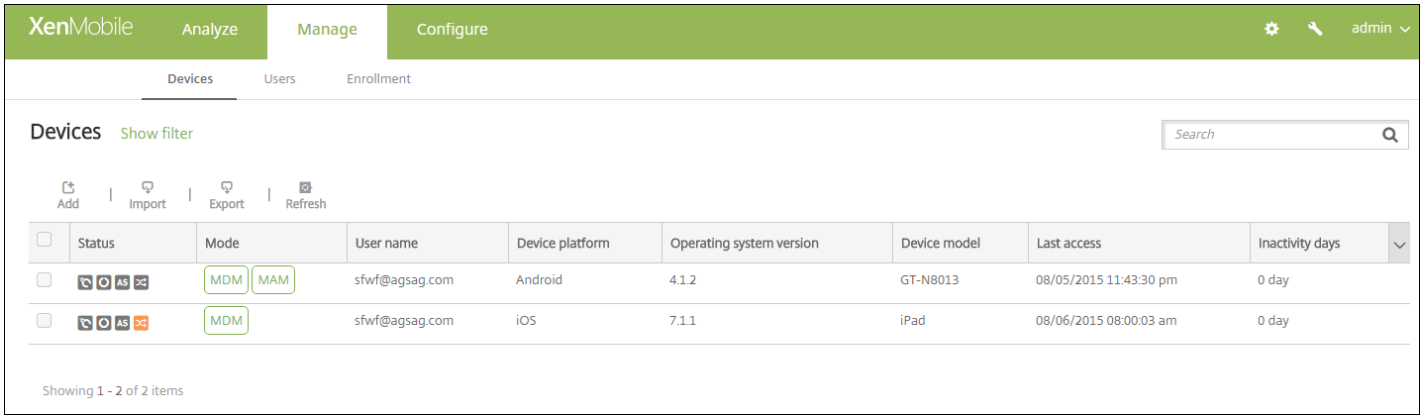
Verrouiller les appareils iOS

Jul 27, 2016

Vous pouvez verrouiller un appareil iOS avec l'affichage d'un message et d'un numéro de téléphone sur l'écran de verrouillage. Cette fonctionnalité est prise en charge sur iOS 7 et 8.

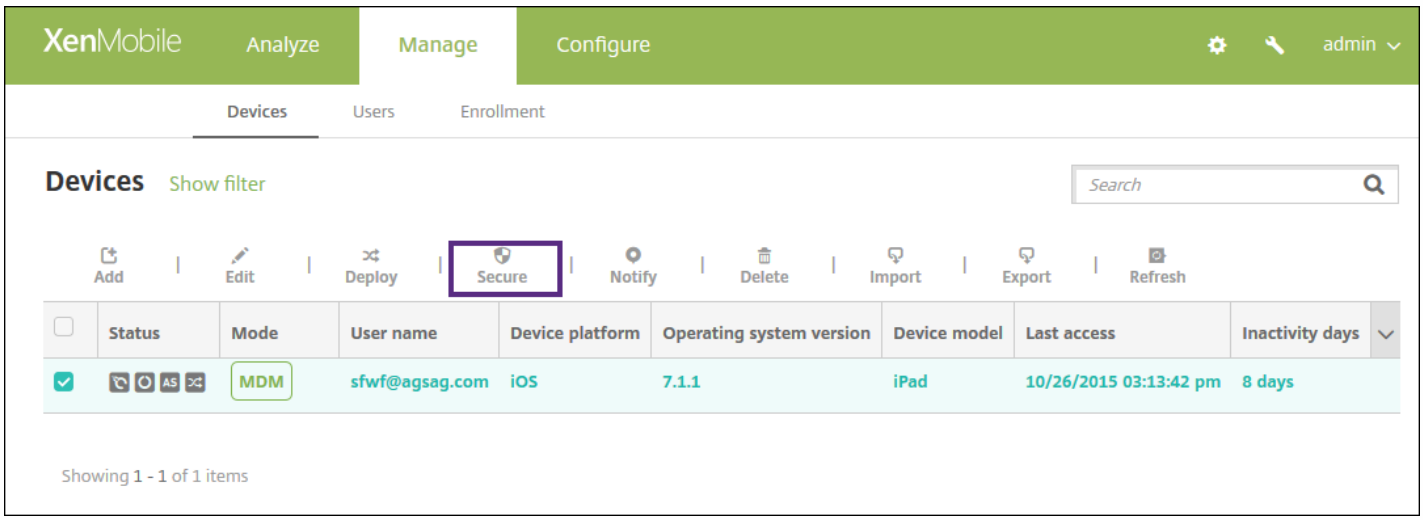
Si vous choisissez d'inclure un message et un numéro de téléphone sur l'écran de verrouillage, le message et le numéro de téléphone ne s'affichent sur un appareil verrouillé que si vous avez également défini la stratégie Code secret dans la console XenMobile, ou si les utilisateurs ont activé le code secret manuellement sur l'appareil.

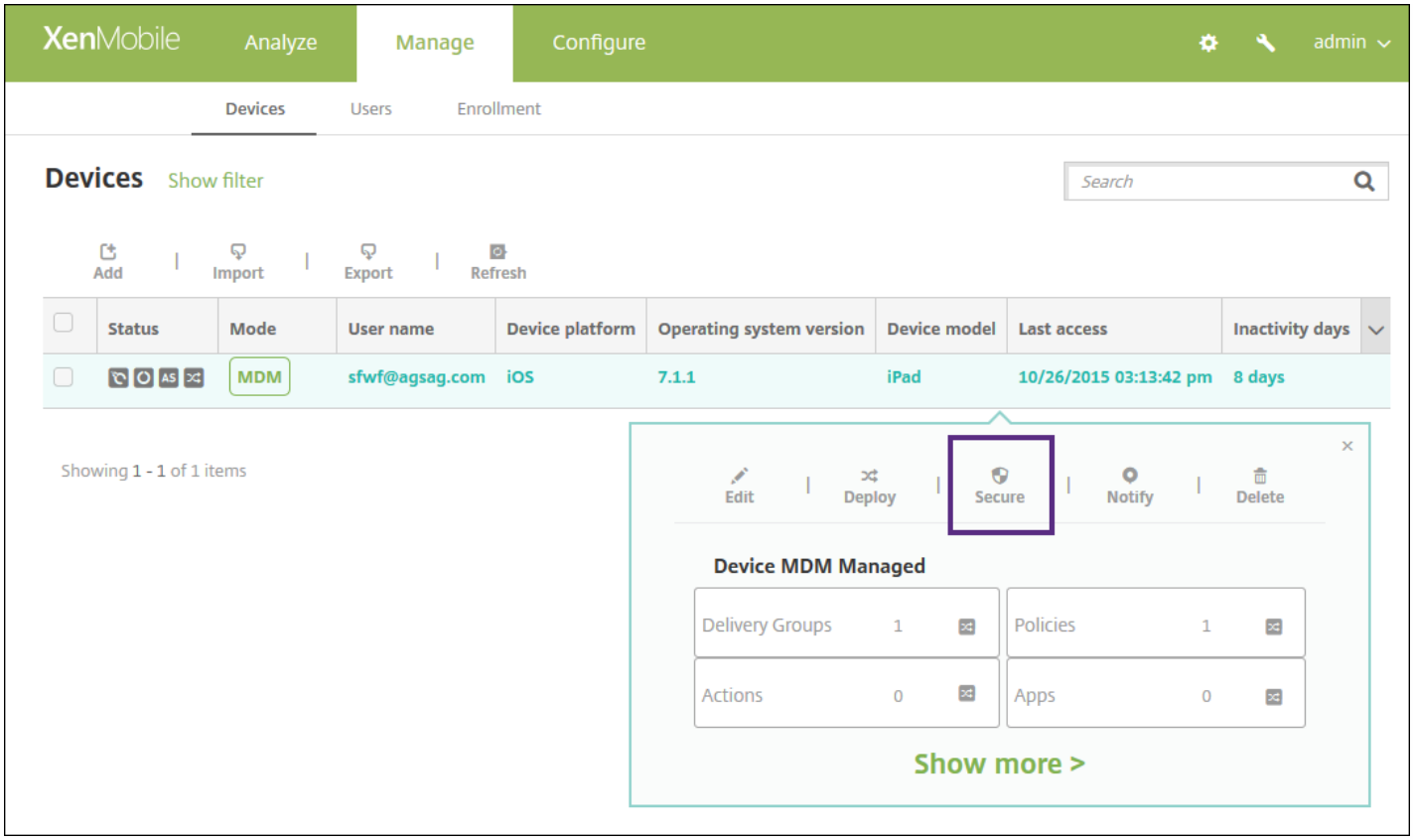
Dans la console XenMobile, cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.



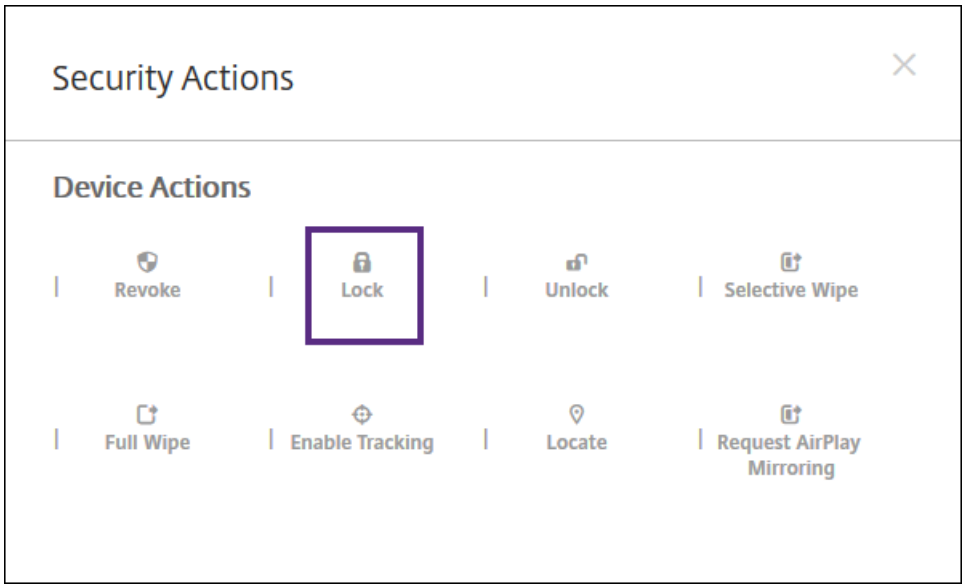
2. Sélectionnez l'appareil iOS que vous voulez verrouiller.

lorsque vous sélectionnez la case à cocher en regard d'un appareil, le menu d'options s'affiche au-dessus de la liste des appareils ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

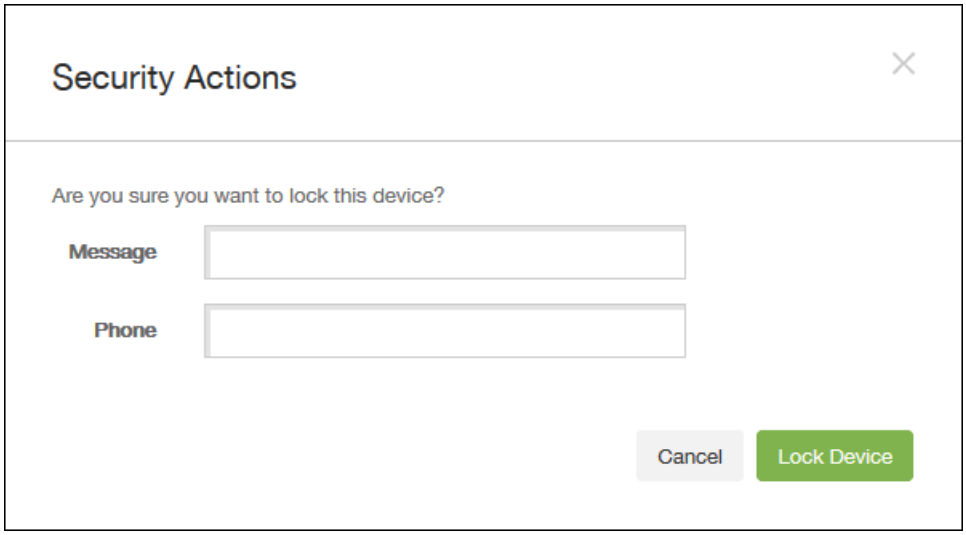




3. Dans le menu d'options, sélectionnez **Sécurité**. La boîte de dialogue **Actions de sécurisation** s'affiche.



4. Sélectionnez **Verrouiller**. La boîte de dialogue de confirmation **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.

6. Cliquez sur **Verrouiller un appareil**.

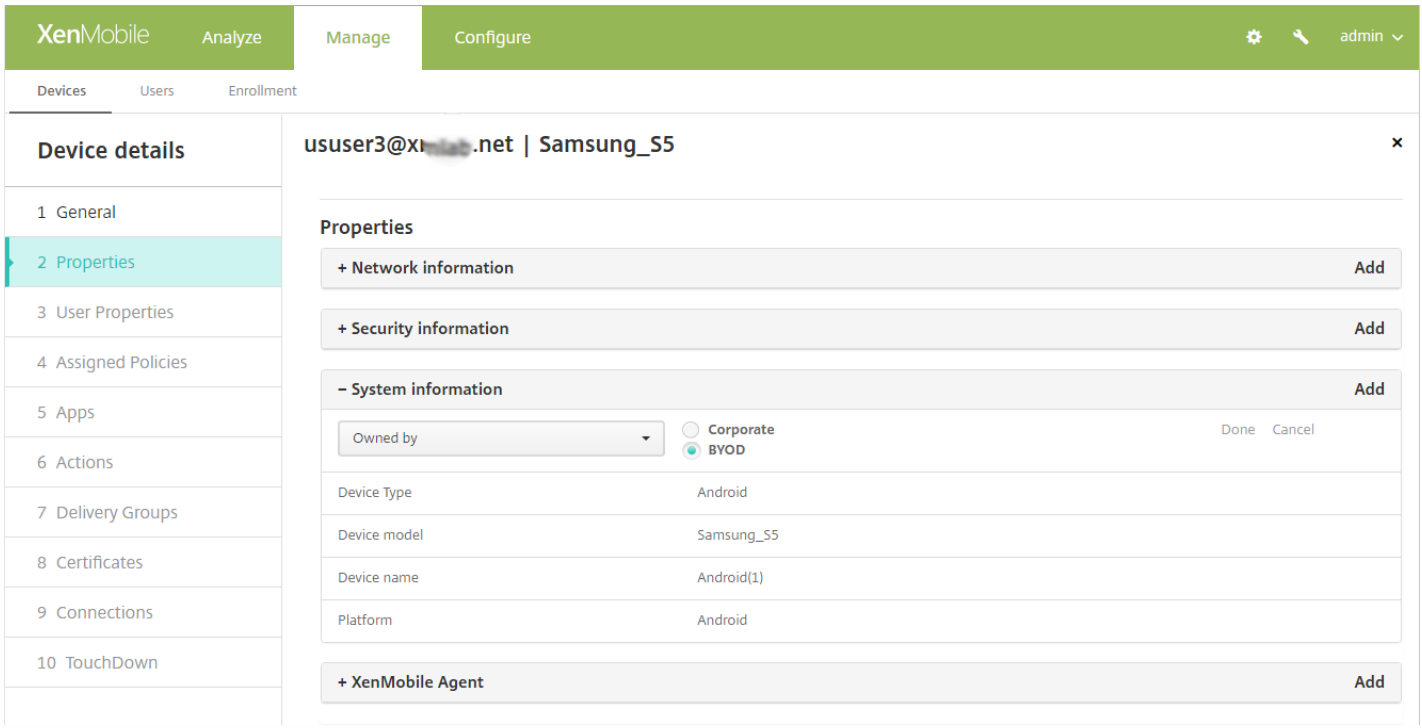
Identification manuelle des appareils utilisateur

Jul 27, 2016

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 également identifier l'appareil comme appartenant à la société ou à un employé. Comme indiqué dans la figure suivante, vous pouvez également identifier un appareil manuellement en ajoutant une propriété à l'appareil à partir de l'onglet **Appareils** dans la console XenMobile, en ajoutant la propriété appelée **Appartient à** et en choisissant **Société** ou **BYOD** (Appartient à l'employé).



Formats des fichiers de provisioning

Jul 27, 2016

La plupart des opérateurs mobiles ou des fournisseurs d'appareils fournissent des listes d'appareils mobiles autorisés que vous pouvez utiliser 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

Remarque :

- Le jeu de caractères du fichier doit être au format UTF-8.
- Les champs dans le fichier de provisioning sont séparés 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, la propriété propertyV;test;1;2 doit être saisie en tant que propertyV;1;test\;2 dans le fichier de provisioning.
- SerialNumber est requis si IMEI n'est pas spécifié.
- SerialNumber est requis pour les appareils iOS car le numéro de série est l'identifiant de l'appareil iOS.
- IMEI est requis si SerialNumber n'est pas spécifié.
- Les valeurs valides pour OperatingSystemFamily sont : WINDOWS, ANDROID ou iOS.

Exemple de fichier de provisioning d'appareil

Les lignes suivantes décrivent chacune un appareil dans un fichier de provisioning.

1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;propertyV$*&&éééétest

3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;

4050BF3F5173010816100655105903 93;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;

La première entrée signifie ce qui suit :

- SerialNumber : 1050BF3F51730108161006551059039 1
- IMEI : 15244201625379901
- OperatingSystemFamily : WINDOWS
- PropertyName : propertyN
- PropertyValue : propertyV\;test\;1\;2;prop 2

Stratégies applicatives

Oct 17, 2016

Vous pouvez configurer la façon dont XenMobile fonctionne 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 appareils iOS, Android et Windows et même entre différents fournisseurs d'appareils exécutant Android. Pour accéder à une liste des stratégies par plate-forme, consultez XenMobile Device Policies by Platform.

Avant de créer une nouvelle stratégie, vous devez effectuer les étapes suivantes :

- Créer les groupes de mise à disposition que vous voulez utiliser.
- Installer les certificats d'autorité de certification nécessaires.

Les étapes de base pour créer une stratégie sont les suivantes :

1. Fournissez un nom et une description pour la stratégie.
2. Configurez 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).

Vous pouvez configurer les stratégies d'appareil suivantes dans XenMobile.

Nom de la stratégie d'appareil	**Description de la stratégie d'appareil**
Mise en miroir AirPlay	Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin d'ajouter des appareils AirPlay spécifiques (tels que Apple TV ou un autre ordinateur Mac) aux appareils iOS des utilisateurs. Vous avez aussi la possibilité d'ajouter des appareils à une liste blanche d'appareils supervisés, ce qui limite l'accès des utilisateurs uniquement aux appareils AirPlay figurant sur la liste blanche.
AirPrint	Une stratégie AirPrint vous permet d'ajouter des imprimantes AirPrint à la liste des imprimantes AirPrint sur les appareils iOS des utilisateurs. Cette stratégie facilite la prise en charge d'environnements dans lesquels les imprimantes et les appareils figurent sur des sous-réseaux différents. Remarque : • Cette stratégie s'applique à iOS 7.0 et versions supérieures. • Vérifiez que vous disposez de l'adresse IP et du chemin d'accès à la ressource pour chaque imprimante.
Restrictions applicatives Android for Work	Cette stratégie vous permet de modifier les restrictions associées aux applications Android for Work, mais vous devez avant cela effectuer les actions suivantes :

	• Effectuer les tâches de configuration d'Android for Work sur Google. Pour de plus amples informations, consultez la section Gestion des appareils avec Android for Work. • Créer des informations d'identification Google Play. Pour de plus amples informations, consultez la section Identifiants Google Play. • Créer un compte Android for Work. Pour de plus amples informations, consultez la section Créer un compte Android for Work. • Ajouter des applications Android for Work à XenMobile. Pour de plus amples informations, consultez la section Ajout d'applications à XenMobile.
APN	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.
Accès applicatif	Une 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.
Attributs d'application	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.
Configuration de l'application	Grâce à cette stratégie, vous pouvez configurer à distance une application App Store qui prend en charge la configuration gérée en déployant un fichier de configuration XML (appelé une liste de propriétés, ou plist) sur les appareils iOS des utilisateurs pour configurer différents paramètres et comportements dans l'application.
Inventaire des applications	Une stratégie d'inventaire des applications vous permet d'établir un inventaire des applications sur les appareils gérés, puis l'inventaire est comparé aux stratégies d'accès aux applications déployées sur ces appareils. Vous pouvez ainsi détecter les applications figurant sur une liste noire (interdites dans une stratégie d'accès aux applications) ou blanche (requis dans une stratégie d'accès aux applications) et prendre les mesures qui s'imposent.
Mode kiosque	Vous pouvez créer une stratégie dans XenMobile afin 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. Remarque : 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 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.
Utilisation des réseaux	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 des applications 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 les applications déjà installées sur les appareils lorsqu'ils ont été inscrits dans XenMobile.
Restrictions applicatives	Grâce à cette stratégie, vous pouvez créer des listes noires d'applications dont vous souhaitez interdire l'installation sur les appareils Samsung KNOX, ainsi que des listes blanches d'applications que vous souhaitez autoriser les utilisateurs à installer.
Tunnel applicatif	Vous pouvez configurer la stratégie de tunnel applicatif pour augmenter la continuité du service et la fiabilité du transfert des données de 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. Remarque : 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.
Désinstallation d'applications	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 de vos 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.
Restriction de désinstallation d'applications	Grâce à cette stratégie, vous pouvez spécifier les applications que les utilisateurs peuvent ou ne peuvent pas désinstaller.
Navigateur	Vous pouvez créer des stratégies de navigateur afin de définir si les appareils peuvent utiliser

	le navigateur ou pour limiter les fonctions du navigateur auxquelles les appareils ont accès. 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. Sur les appareils Android for Work, vous pouvez placer sur liste noire ou blanche des adresses URL spécifiques, et ajouter des signets de navigateur sécurisés spécifiques.
Calendrier (CalDav)	Vous pouvez ajouter une stratégie dans XenMobile afin d'ajouter un compte de calendrier (CalDAV) sur des appareils iOS ou Mac OS X pour permettre à leurs utilisateurs de synchroniser les données de planification avec tout serveur qui prend en charge CalDAV.
Cellulaire	Cette stratégie vous permet de configurer des paramètres réseau cellulaire.
Gestionnaire de connexions	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.
Planification de connexion	Cette stratégie est 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 la stratégie. Si vous n'envoyez pas cette stratégie et que vous n'avez pas activé Google GCM, un appareil ne se reconnectera pas au serveur. Par conséquent, il est important de distribuer cette stratégie au paquetage de base pour l'inscription d'appareils.
Contacts (CardDAV)	Vous pouvez ajouter une stratégie dans XenMobile afin d'ajouter un compte de contacts iOS (CalDAV) sur des appareils iOS ou Mac OS X pour permettre à leurs utilisateurs de synchroniser les données de contact avec tout serveur qui prend en charge CalDAV.
Copier les applications sur le conteneur Samsung	Vous pouvez spécifier des applications déjà installées sur un appareil à copier vers un conteneur SEAMS ou un conteneur KNOX sur les appareils Samsung pris en charge. Les applications copiées sur le conteneur SEAMS sont disponibles sur les écrans d'accueil des utilisateurs ; les applications copiées sur le conteneur KNOX sont uniquement disponibles lorsque les utilisateurs se connectent au conteneur KNOX.
Informations d'identification	Vous pouvez créer des stratégies d'informations d'identification dans XenMobile afin d'intégrer l'authentification à votre configuration PKI dans XenMobile, comme une entité PKI, un keystore, un fournisseur d'informations d'identification ou un certificat de serveur. Pour plus d'informations sur les informations d'identification, veuillez consulter la section Certificats dans XenMobile. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans l'article Stratégie d'informations d'identification. 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.
Copier les applications sur le conteneur Samsung	Vous pouvez spécifier des applications déjà installées sur un appareil à copier vers un conteneur SEAMS ou un conteneur KNOX sur les appareils Samsung pris en charge. Pour de plus amples informations sur les appareils pris en charge, reportez-vous à la section Appareils Samsung KNOX pris en charge de Samsung. Les applications copiées sur le conteneur SEAMS sont disponibles sur les écrans d'accueil des utilisateurs ; les applications copiées sur le conteneur KNOX sont uniquement disponibles lorsque les utilisateurs se connectent au conteneur KNOX.
Informations d'identification	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.
XML personnalisé	Vous pouvez créer des stratégies XML personnalisées dans XenMobile pour personnaliser les fonctionnalités suivantes : • 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, ce qui comprend 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. 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 sur le site de Microsoft Developer Network.
Supprimer des fichiers et dossiers	Vous pouvez créer une stratégie dans XenMobile pour supprimer des fichiers ou dossiers spécifiques d'appareils Windows Mobile/CE.
Supprimer des clés et valeurs de registre	Vous pouvez créer une stratégie dans XenMobile pour supprimer des clés et valeurs de Registre spécifiques d'appareils Windows Mobile/CE.
Attestation de l'intégrité des appareils	Dans XenMobile, vous pouvez une stratégie qui nécessite que les appareils Windows 10 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 DEP • 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 HealthAttestation CSP de Microsoft.
Nom de l'appareil	Une stratégie de nom d'appareil vous permet de définir les noms sur des appareils iOS et Mac OS X, de façon à identifier facilement les appareils. Vous pouvez utiliser des macros et du texte, ou une combinaison des deux pour définir le nom de l'appareil. Pour de plus amples informations sur les macros, consultez la section Macros dans XenMobile.
Hub d'entreprise	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 Symantec • 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 Worx Home. Par exemple, pour télécharger Windows Phone Worx Home pour XenMobile Enterprise 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.
Exchange	XenMobile vous offre deux options pour distribuer des e-mails. Vous pouvez mettre à disposition la messagerie ActiveSync à l'aide de l'application WorxMail en conteneur, ou vous pouvez utiliser cette stratégie MDM Exchange pour activer la messagerie ActiveSync pour le client de messagerie natif sur l'appareil.
Fichiers	Grâce à cette stratégie, vous pouvez ajouter 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. Par exemple, si vous souhaitez que les utilisateurs Android reçoivent un document d'entreprise ou fichier .pdf, vous pouvez déployer le fichier sur l'appareil et informer les utilisateurs de son emplacement. 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
Police	Vous pouvez ajouter cette stratégie dans XenMobile pour ajouter des polices supplémentaires sur les appareils iOS et Mac OS X des utilisateurs. Les polices doivent être de type TrueType (.ttf) ou OpenType (.oft). Les collections de polices (.ttc ou.otc) ne sont pas prises en charge. Remarque : pour iOS, cette stratégie s'applique uniquement à iOS 7.0 et versions supérieures.
Importer le profil iOS et Mac OS X	Vous pouvez importer les fichiers XML de configuration d'appareil pour iOS et OS X dans XenMobile. Le fichier contient des stratégies de sécurité et des restrictions que vous préparez avec Apple Configurator. 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.
Kiosque	Lorsque vous créez une stratégie kiosque dans XenMobile, seules une ou des applications spécifiques peuvent être exécutées sur les appareils Samsung SAFE. 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. Remarque : • 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.
LDAP	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.
L'Emplacement	La stratégie d'emplacement peut être utilisée pour géo-localiser les appareils sur une carte, en supposant que le GPS est activé pour Worx Home sur l'appareil. Une fois cette stratégie transmise à l'appareil, les administrateurs peuvent envoyer une commande de localisation à partir du serveur XenMobile et l'appareil répondra avec ses coordonnées d'emplacement. Les stratégies de géofencing et de suivi sont également prises en charge.
Messagerie	Vous pouvez ajouter une stratégie de messagerie dans XenMobile pour configurer un compte de messagerie sur les appareils iOS ou Mac OS X des utilisateurs.
Domaines gérés	Vous pouvez définir des domaines gérés via cette stratégie 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. 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. Cette stratégie est uniquement prise en charge sur les appareils supervisés iOS 8 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. 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. Lorsqu'un utilisateur tente d'ouvrir un élément (document, pièce jointe ou téléchargement) 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.
Microsoft Exchange ActiveSync	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. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans l'article Microsoft Exchange ActiveSync de cette section.

Options MDM	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 des 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 ou Inscription en bloc iOS. Le verrouillage d'activation est une fonctionnalité de Localiser mon iPhone/iPad qui est conçue pour empêcher la réactivation des appareils perdus ou volés ; l'ID et le mot de passe Apple de l'utilisateur sont exigés pour désactiver la fonction Localiser mon iPhone, effacer l'appareil ou réactiver et utiliser l'appareil. Dans XenMobile, vous pouvez contourner l'obligation d'entrer ID et mot de passe en activant l'option Verrouillage d'activation dans la stratégie d'options MDM. Lorsqu'un utilisateur renvoie un appareil sur lequel la fonction Localiser mon iPhone est activée, vous pouvez gérer l'appareil à partir de la console XenMobile sans ses informations d'identification Apple.
Info organisation	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.
Code secret	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.
Personal Hotspot	Grâce à cette stratégie, 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.
Suppression de profil	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 Mac OS X des utilisateurs.
Profil de provisioning	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.
Suppression du profil de provisioning	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 Ajout d'un profil de provisioning.
Proxy	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. Remarque : 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 de plus amples informations, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.
Registre	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.
Remote Support	Vous créez une stratégie d'assistance à distance dans XenMobile pour vous permettre d'accéder à distance aux appareils Samsung KNOX des utilisateurs. 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, y compris le contrôle des couleurs (dans la fenêtre principale ou dans une fenêtre distincte flottante), d'établir une session Voix-sur-IP (VoIP) entre le bureau d'assistance et l'utilisateur, de configurer des paramètres et d'établir une session de chat entre le bureau d'assistance et l'utilisateur.
Restrictions	La stratégie de restriction offre aux administrateurs plusieurs façons de verrouiller et contrôler les fonctionnalités sur l'appareil géré. Il existe des centaines d'options de restriction, 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.

	Vous pouvez ajouter une stratégie d'appareil dans XenMobile pour limiter l'accès des utilisateurs à certaines fonctionnalités sur leurs appareils, téléphones, tablettes, etc. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article. Cette stratégie permet ou empêche les utilisateurs d'utiliser certaines fonctionnalités sur leurs appareils, 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 ON ou sont autorisés. Les principales exceptions sont la fonctionnalité Sécuriser - Forcer dans iOS et toutes les fonctionnalités de Windows Tablet, lesquelles prennent par défaut la valeur OFF ou appliquent des restrictions. Conseil : toute option définie sur ON signifie que l'utilisateur peut effectuer l'opération ou utiliser la fonctionnalité. Par exemple : ● Appareil photo. Si l'option est réglée sur ON, l'utilisateur peut utiliser l'appareil photo sur son appareil. Si l'option est réglée sur OFF, l'utilisateur ne peut pas utiliser l'appareil photo sur son appareil. ● Captures d'écrans. Si l'option est réglée sur ON, l'utilisateur peut prendre des captures d'écrans sur son appareil. Si l'option est réglée sur OFF, l'utilisateur ne peut pas prendre de captures d'écrans sur son appareil.
Itinérance	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.
Pare-feu Samsung SAFE	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 auxquels vous souhaitez autoriser les appareils à accéder ou auxquels vous souhaitez empêcher les appareils d'accéder. Vous pouvez également configurer les paramètres de redirection de proxy et de proxy.
Clé de licence MDM Samsung	XenMobile prend en charge et étend les stratégies Samsung for Enterprise (SAFE) et Samsung KNOX. SAFE fait partie d'une famille de solutions qui fournit des améliorations de sécurité pour les entreprises via l'intégration à des solutions MDM. Samsung KNOX est une solution du programme SAFE destinée à une utilisation professionnelle conçue pour renforcer la sécurité sur la plate-forme Android. Vous devez activer les API SAFE en déployant la clé Samsung ELM (Enterprise License Management) intégrée sur un appareil avant de pouvoir déployer des stratégies et restrictions SAFE. Pour activer les API Samsung KNOX, vous devez acheter une licence Samsung KNOX à l'aide du Samsung KNOX License Management System (KLMS) en plus de déployer la clé Samsung ELM. Le KMLS Samsung provisionne des licences valides sur des

	solutions MDM afin d'activer les API Samsung KNOX sur les appareils mobiles. Vous devez vous procurer ces licences auprès de Samsung car elles ne sont pas fournies par Citrix. Vous devez déployer Worx Home en conjonction avec la clé Samsung ELM pour activer les API SAFE et Samsung KNOX. Vous pouvez vérifier que les API SAFE sont activés en consultant les propriétés de l'appareil. Lorsque la clé Samsung ELM est déployée, le paramètre API Samsung MDM disponible est défini sur True.
SCEP	Cette stratégie vous permet de configurer des appareils iOS et Mac OS X 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.
Clé de sideloading	Le sideloading dans XenMobile vous permet de déployer des applications sur des appareils Windows 8.1 qui n'ont pas été achetées à partir du Windows Store. Dans la plupart des cas, vous sideloadez les applications que vous développez pour une utilisation en entreprise que vous ne souhaitez pas rendre publiques dans le Windows Store. Pour sideloader des applications, vous devez configurer la clé de sideloading et l'activation de clés et déployer les applications sur les appareils des utilisateurs. Vous devez disposer des informations suivantes avant de pouvoir créer cette stratégie : • La clé de sideloading du produit, que vous pouvez obtenir en vous connectant au Centre de gestion des licences en volume Microsoft. • L'activation de clé, que vous créez via la ligne de commande après avoir obtenu la clé de sideloading du produit.
Certificat de signature	Vous pouvez ajouter une stratégie d'appareil dans XenMobile pour configurer les certificats de signature à utiliser pour signer les fichiers APPX. Vous avez besoin des certificats de signature si vous voulez distribuer des fichiers APPX aux utilisateurs pour les autoriser à installer des applications sur leurs tablettes Windows.
Compte SSO	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. Remarque : cette stratégie s'applique uniquement à iOS 7.0 et versions supérieures.
Chiffrement du	Vous pouvez créer des stratégies de chiffrement du stockage dans XenMobile pour chiffrer

stockage	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 Samsung SAFE, Windows Phone et Android Sony. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans l'article Stratégie de chiffrement du stockage de cette section.
Abonnements calendriers	Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin d'ajouter un abonnement calendrier à la liste des calendriers sur les appareils iOS des utilisateurs. La liste des calendriers publics auxquels vous pouvez vous abonner est disponible sur www.apple.com/downloads/macosx/calendars. Remarque : 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	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.
VPN	Pour les clients désirant fournir l'accès aux systèmes principaux à l'aide de l'ancienne technologie de passerelle VPN, cette stratégie VPN peut être utilisée pour distribuer les détails de connexion de la passerelle VPN à l'appareil. Un certain nombre de fournisseurs VPN sont pris en charge via la stratégie 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 (en supposant que la passerelle VPN prenne en charge cette option). Vous pouvez ajouter une stratégie dans XenMobile pour configurer des paramètres de réseau privé virtuel (VPN) permettant aux appareils de se connecter de manière sécurisée aux ressources d'entreprise. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans l'article VPN de cette section.
Fond d'écran	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 version ultérieure. 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.

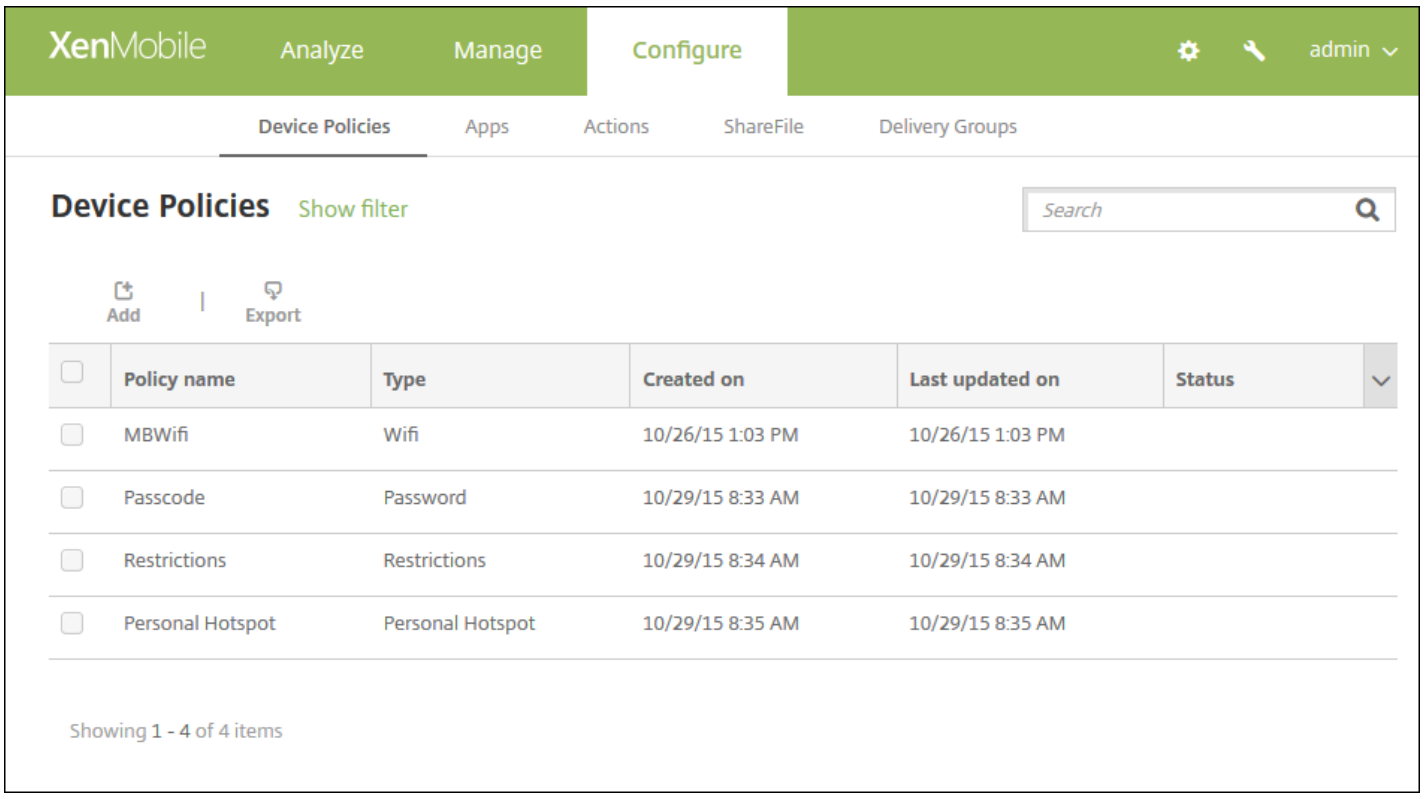
Filtre de contenu Web	Vous pouvez ajouter une stratégie dans XenMobile destinée à filtrer le contenu Web sur les appareils iOS à l'aide de la fonction de filtrage automatique d'Apple en conjonction avec les sites spécifiques que vous ajoutez aux listes blanches et listes noires. Cette stratégie est uniquement 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.
Clip Web	Grâce à cette stratégie, 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, Mac OS X et Android ; Windows Tablet requiert uniquement un nom et une adresse URL.
Wi-Fi	La stratégie Wi-Fi permet aux administrateurs de facilement distribuer les détails du routeur Wi-Fi : SSID, données de configuration et d'authentification sur un appareil géré. Les stratégies Wi-Fi vous permettent de gérer la manière dont les utilisateurs connectent leurs appareils à des réseaux sans fil en définissant ce qui suit : noms et types de réseau, stratégies d'authentification et de sécurité, serveurs proxy et d'autres détails liés à l'utilisation du Wi-Fi pour tous les utilisateurs sur les plates-formes que vous avez choisies. Vous pouvez configurer des paramètres Wi-Fi pour les utilisateurs des plates-formes associées répertoriées à gauche, mais chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans l'article Wi-Fi de cette section.
Certificat Windows CE	Ajoutez cette stratégie d'appareil 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.
Worx Store	Vous pouvez créer une stratégie dans XenMobile afin de spécifier si les appareils iOS, Android ou Windows Tablet affichent un clip Web Worx Store sur l'écran d'accueil des appareils.
Options XenMobile	Vous ajoutez une stratégie d'options XenMobile pour configurer le comportement de Worx Home lors de la connexion à XenMobile à partir d'appareils Android et Windows Mobile/CE.
Désinstallation de XenMobile	Vous pouvez ajouter cette 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.

Page Stratégies d'appareil dans la console

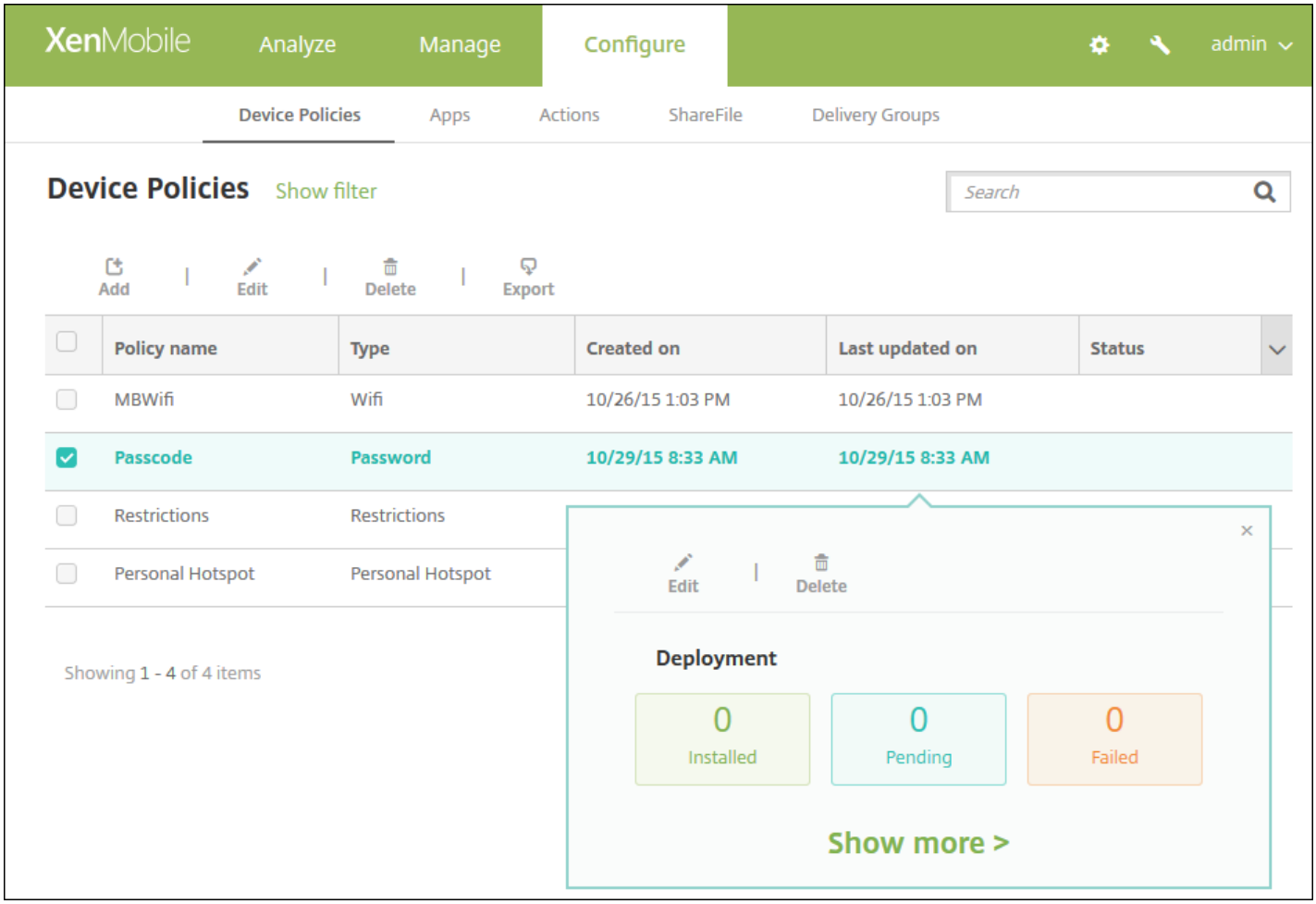
Les stratégies sont accessibles à partir de la page **Stratégies d'appareil** dans la console XenMobile. Pour accéder à la page

Stratégies d'appareil, cliquez sur **Configurer > Stratégies d'appareil**. À partir de cette fenêtre, vous pouvez ajouter de nouvelles stratégies, consulter l'état de stratégies existantes, et modifier ou supprimer des stratégies.

La page **Stratégies d'appareil** contient une table répertoriant toutes les stratégies actuelles.



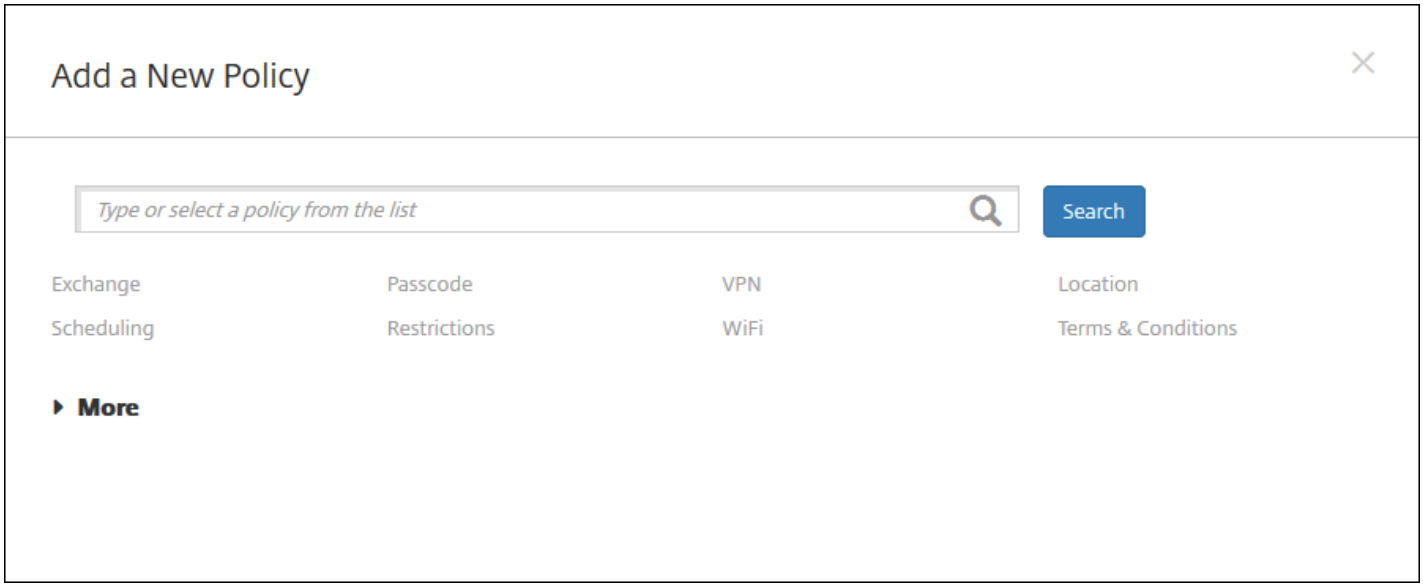
Pour modifier ou supprimer une stratégie sur la page **Stratégies d'appareil**, vous pouvez sélectionner la case à cocher en regard d'une stratégie pour afficher les options de menu au-dessus de la liste de stratégie, ou vous pouvez cliquer sur une stratégie dans la liste pour afficher le menu d'options sur le côté droit de la liste. Si vous cliquez sur **Afficher plus**, les détails de stratégie s'affichent.



Pour ajouter une stratégie d'appareil

1. Sur la page **Stratégies d'appareil**, cliquez sur **Ajouter**.

La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît. Vous pouvez développer **Plus** pour afficher d'autres stratégies.

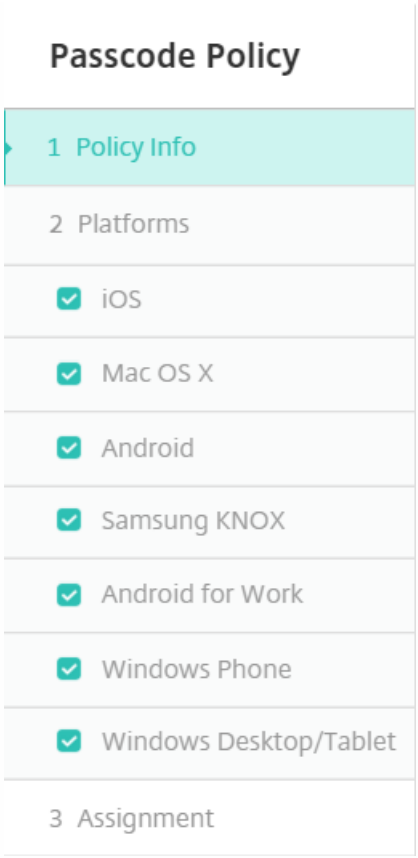


2. Pour trouver la stratégie que vous souhaitez ajouter, effectuez l'une des opérations suivantes :

- Cliquez sur la stratégie.
  La page **Informations sur la stratégie** pour la stratégie sélectionnée s'affiche.
- Entrez 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 la boîte de dialogue. Cliquez dessus pour ouvrir la page **Informations de stratégie** pour cette stratégie.
  Important : si votre stratégie sélectionnée figure dans la zone **Plus**, elle est uniquement visible si vous développez **Plus**.

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.

Remarque : seules les plates-formes prises en charge par la stratégie sont répertoriées.

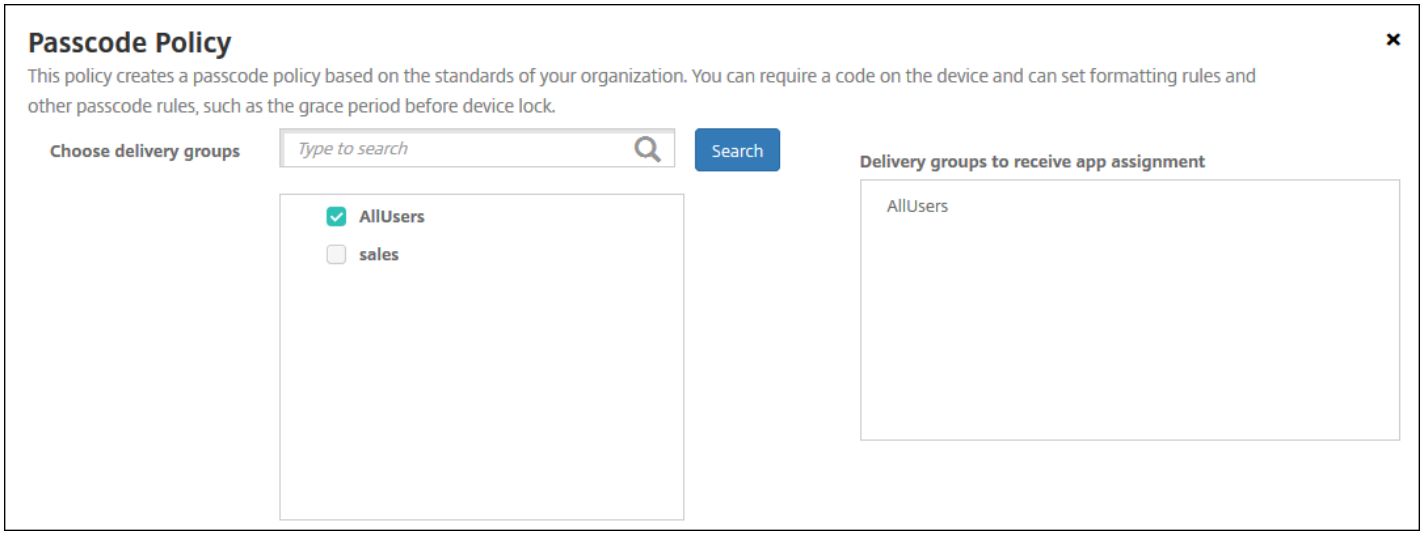


4. Remplissez la page **Informations de stratégie** puis cliquez sur **Suivant**. La page **Informations de stratégie** collecte des informations, comme le nom de la stratégie, pour vous aider à identifier et à suivre vos stratégies. Cette page est identique pour toutes les stratégies.

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. Chaque stratégie peut être différente entre les plates-formes. Les stratégies ne sont pas toutes prises en charge par toutes les plates-formes. 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 **Attribution**.

6. Sur la page **Attribution**, sélectionnez les groupes de mise à disposition auxquels vous voulez appliquer la stratégie. Lorsque 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**.

Remarque : 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.



7. Cliquez sur **Enregistrer**.

La stratégie est ajoutée au tableau **Stratégies d'appareil**.

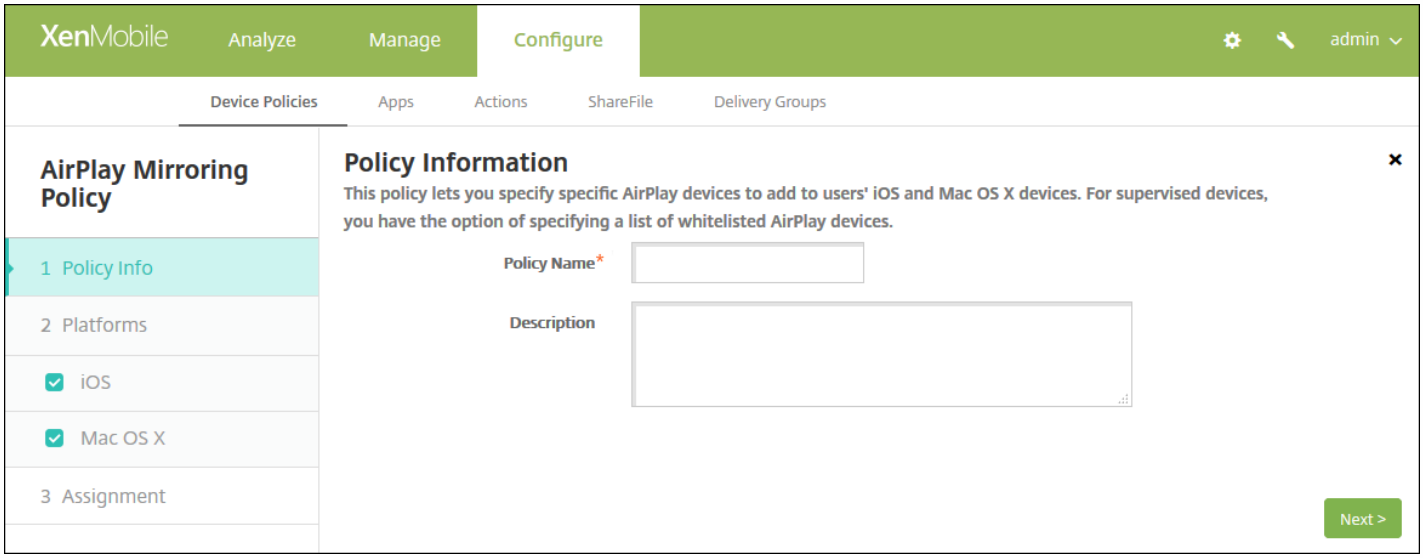
Pour modifier ou supprimer une stratégie d'appareil

1. Dans le tableau **Stratégies d'appareil**, sélectionnez la case à cocher en regard de la stratégie que vous souhaitez modifier ou supprimer.

2. Cliquez sur **Modifier** ou **Supprimer**.

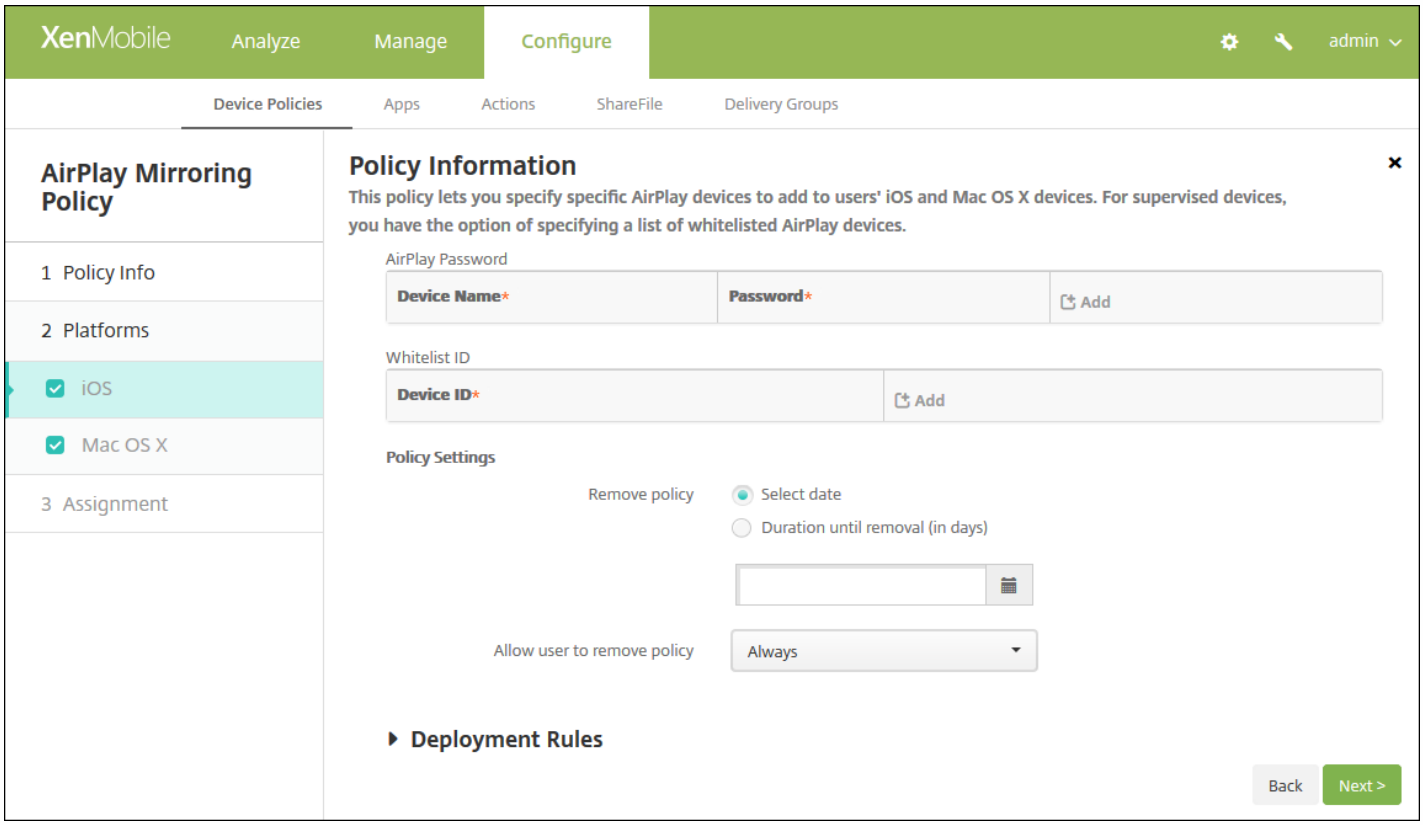
- Si vous cliquez sur **Modifier**, vous pouvez modifier tous les paramètres.
- Si vous cliquez sur le bouton **Supprimer**, dans la boîte de dialogue de confirmation, cliquez de nouveau sur **Supprimer**.

-
-
-
-
-
-
-
-
-
-
-



-
-

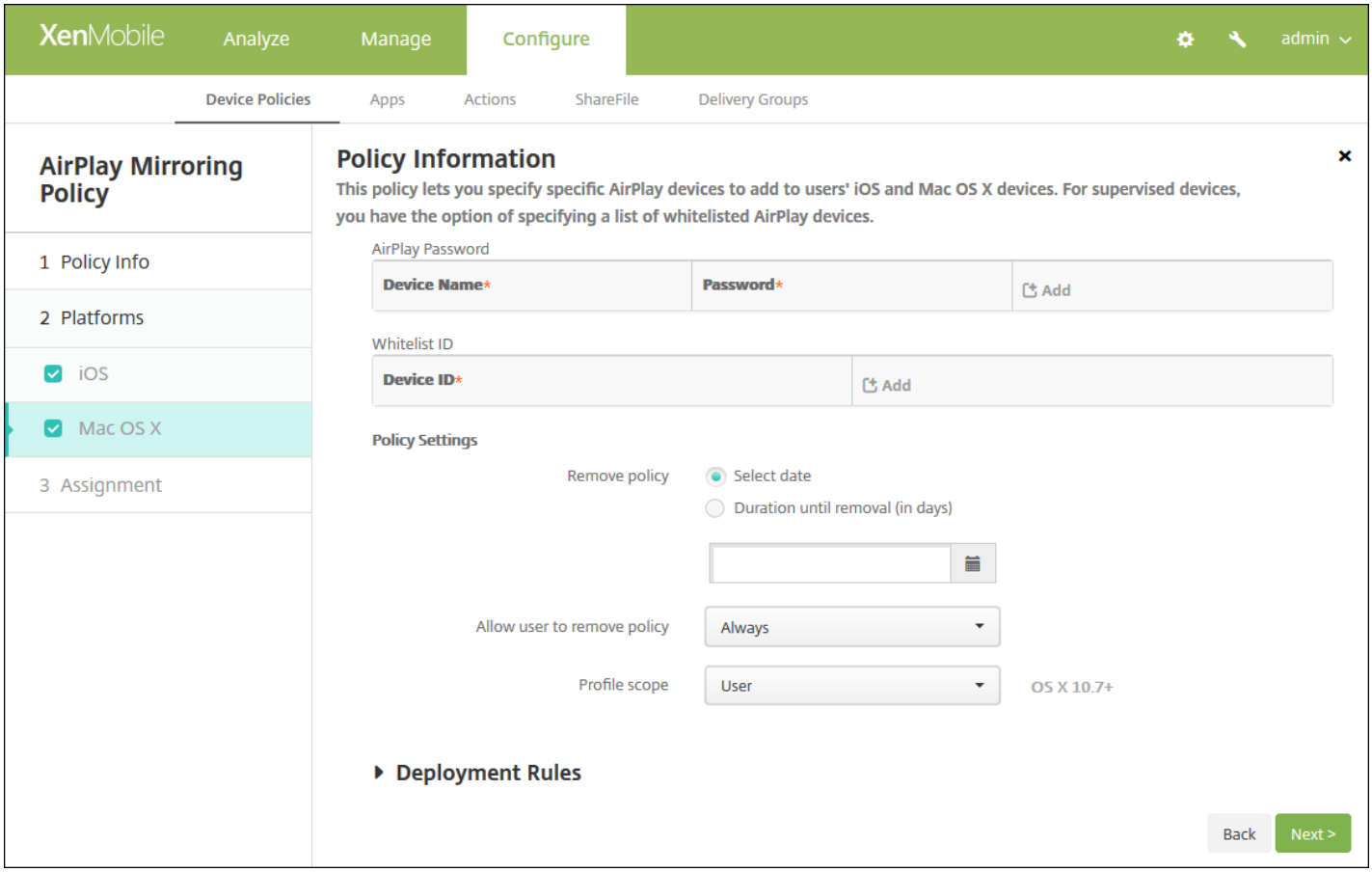
Configurer les paramètres pour iOS



-
  -
  -
  -
-
  -
  -

-
  -
  -
  -
  -

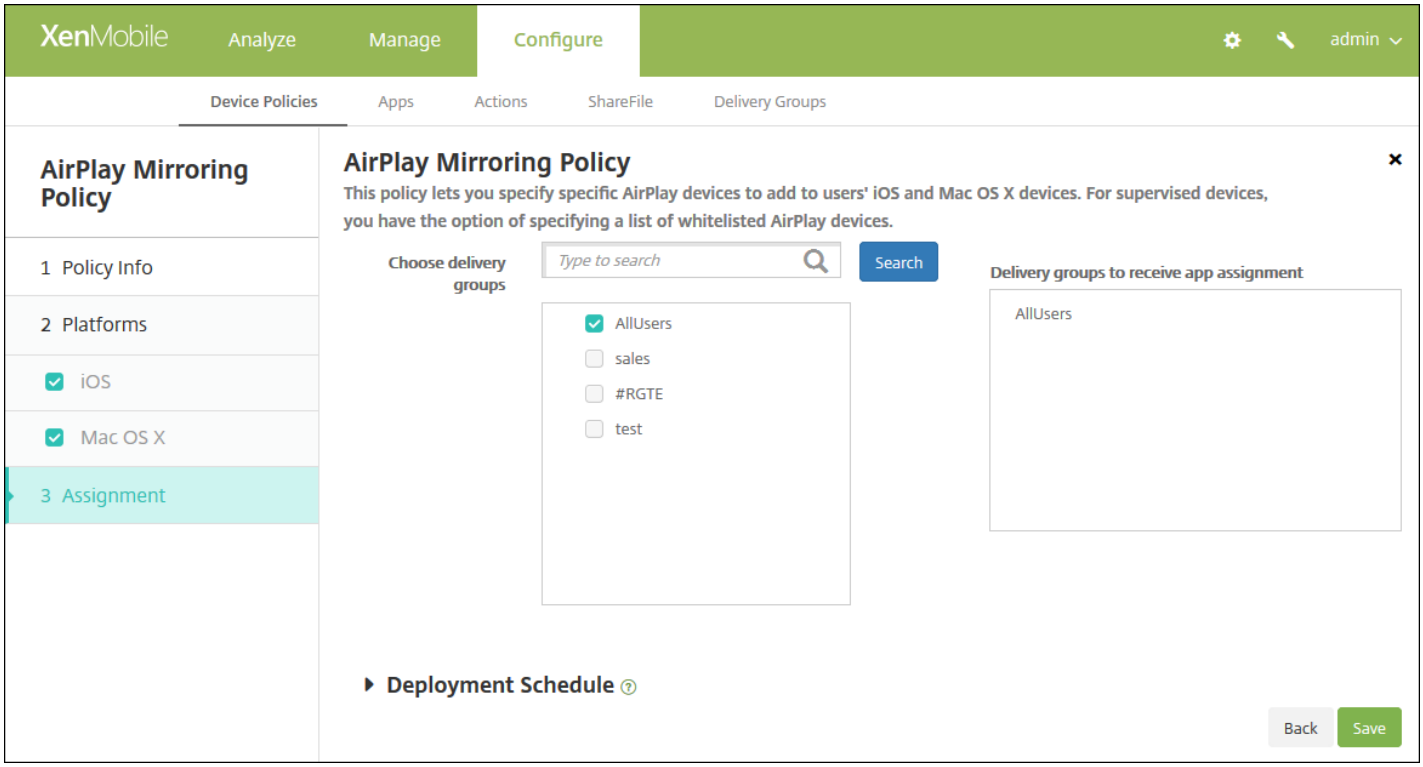
Configurer les paramètres pour Mac OS X



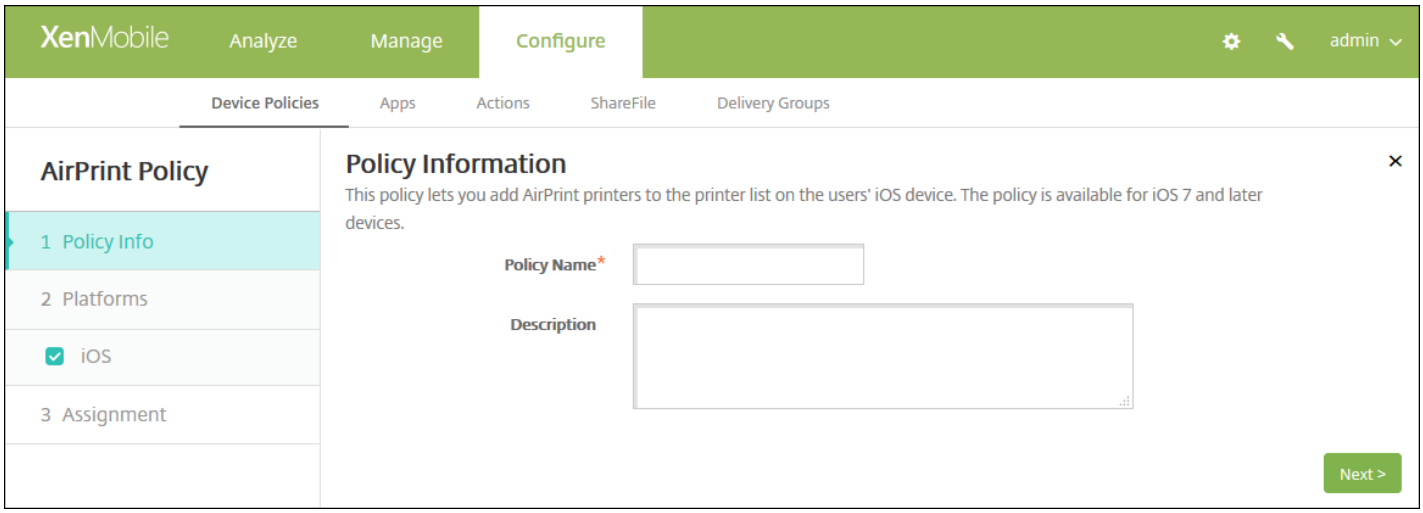
-
  -
  -
  -
-

-
-
-
  -
  -
  -
  -
  -

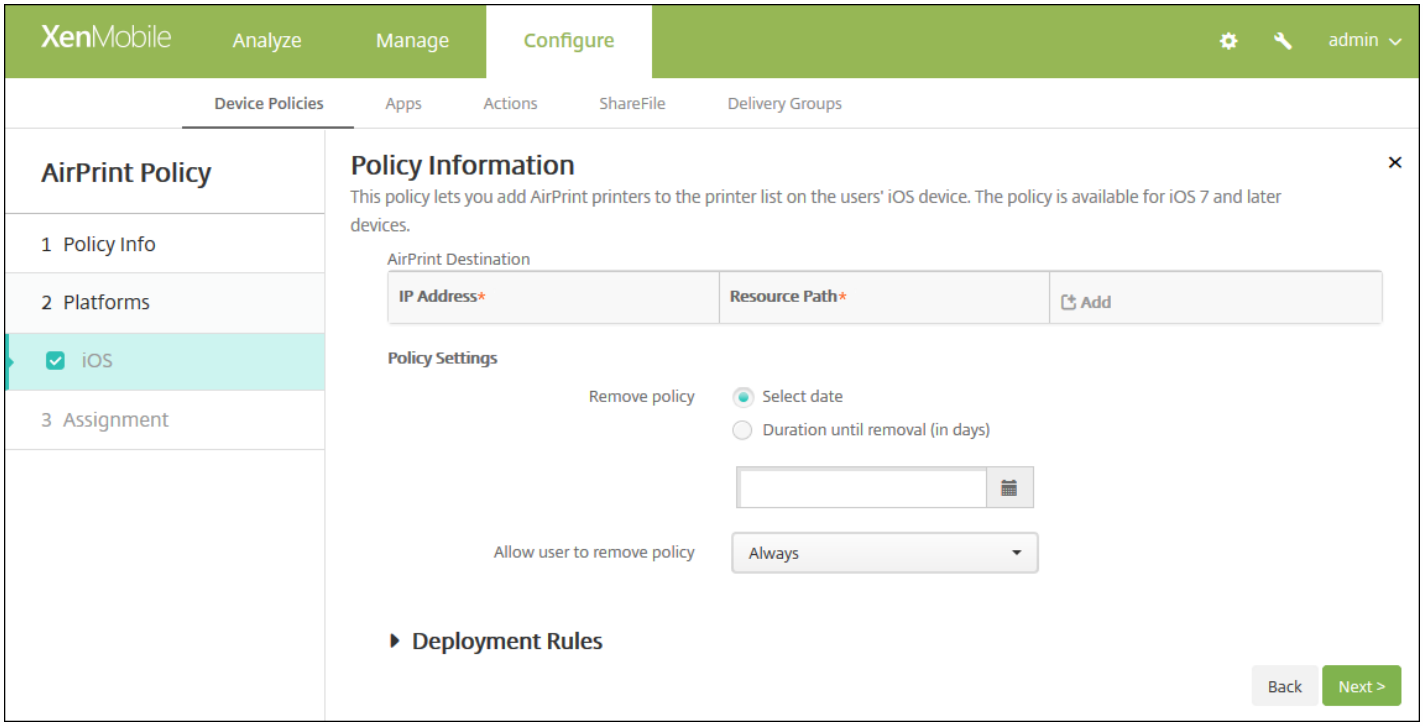
7. Configurez les règles de déploiement.



-
-

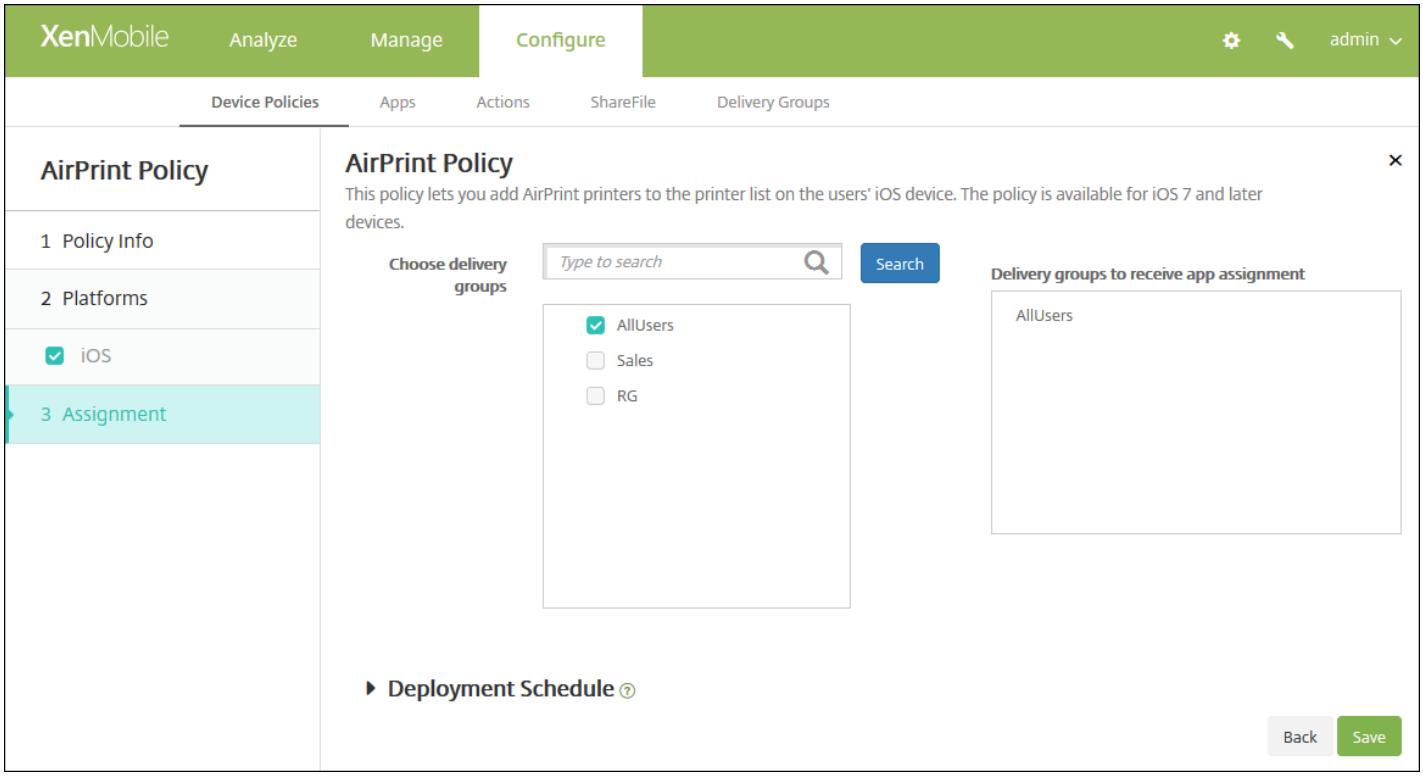


-
-



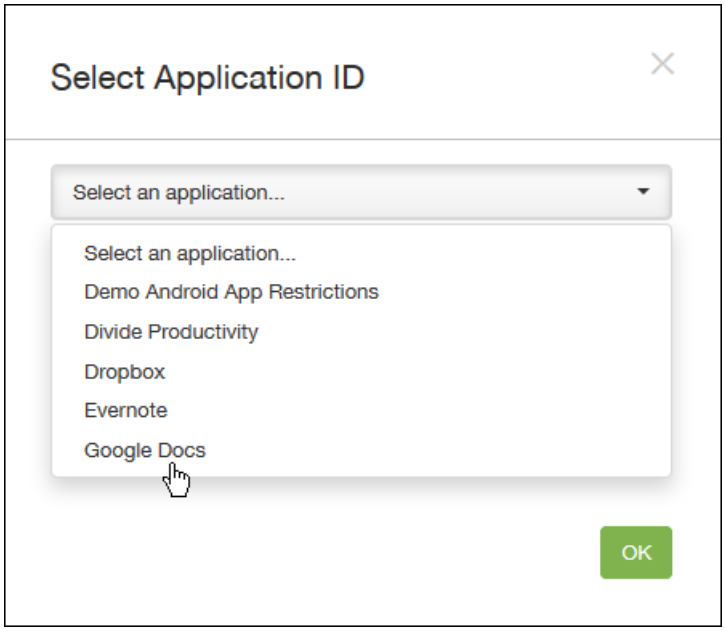
-
  -
  -
  -
-
  -
  -
  -
  -

7. Configurez les règles de déploiement.



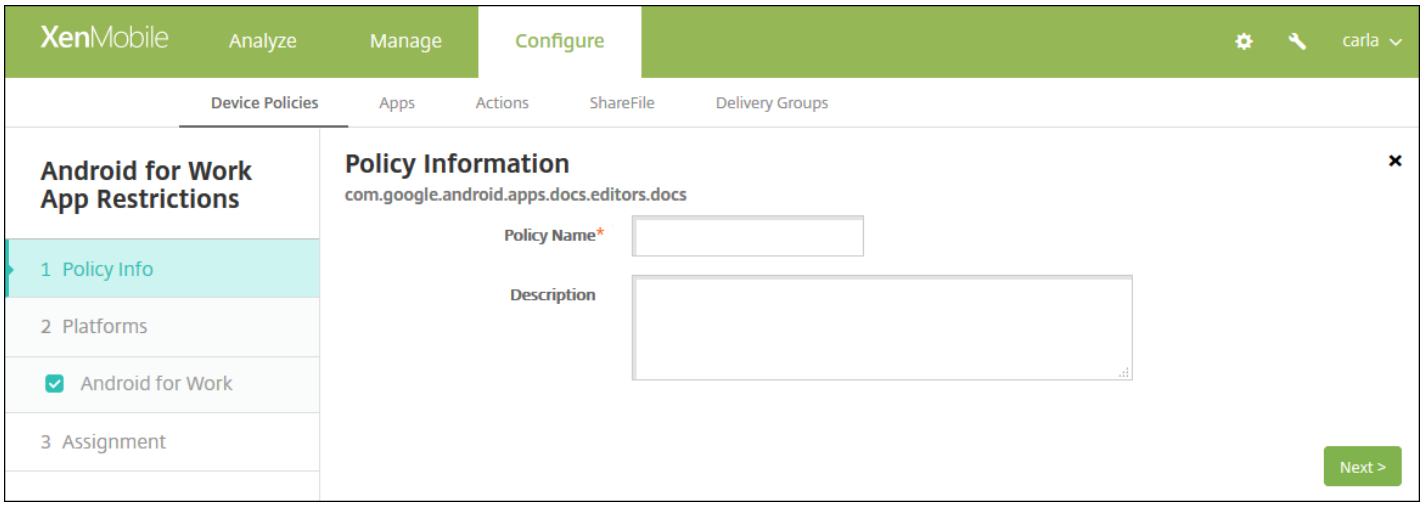
-

-
-
-
-

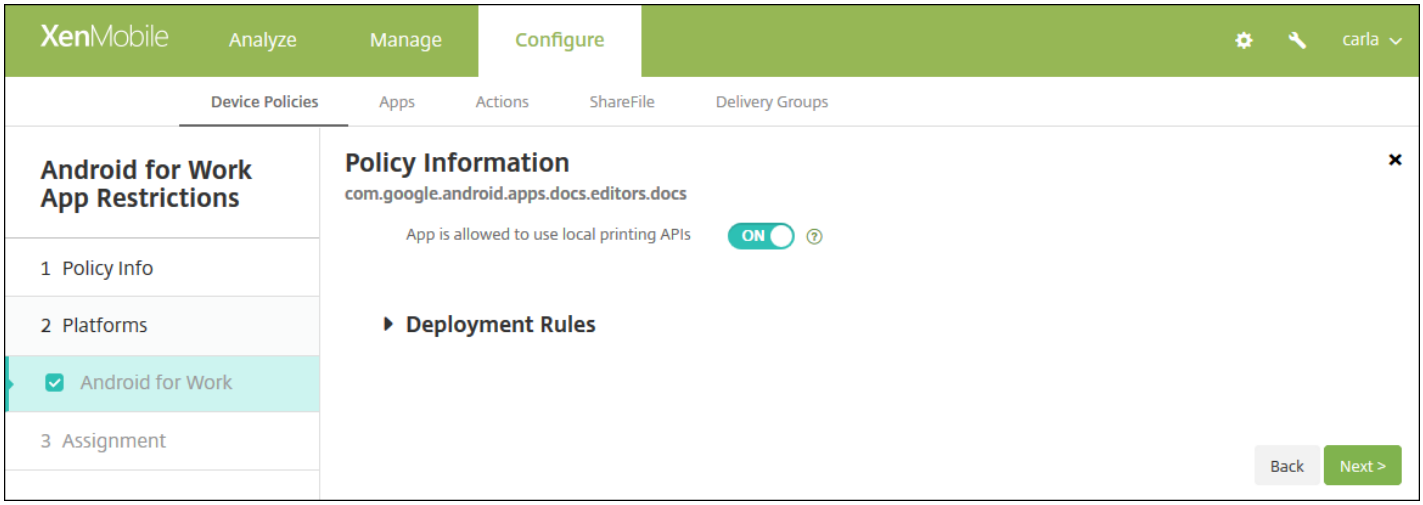


-

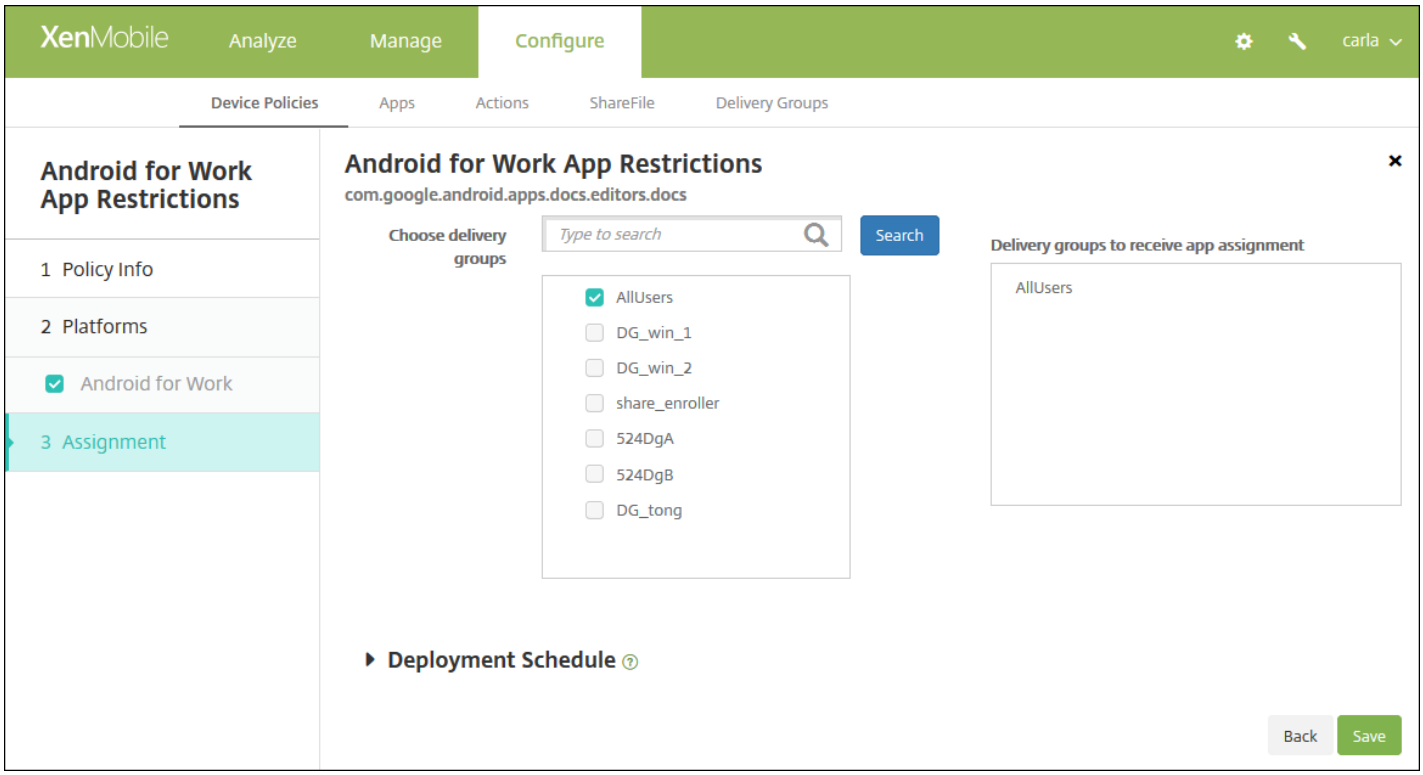
-
-



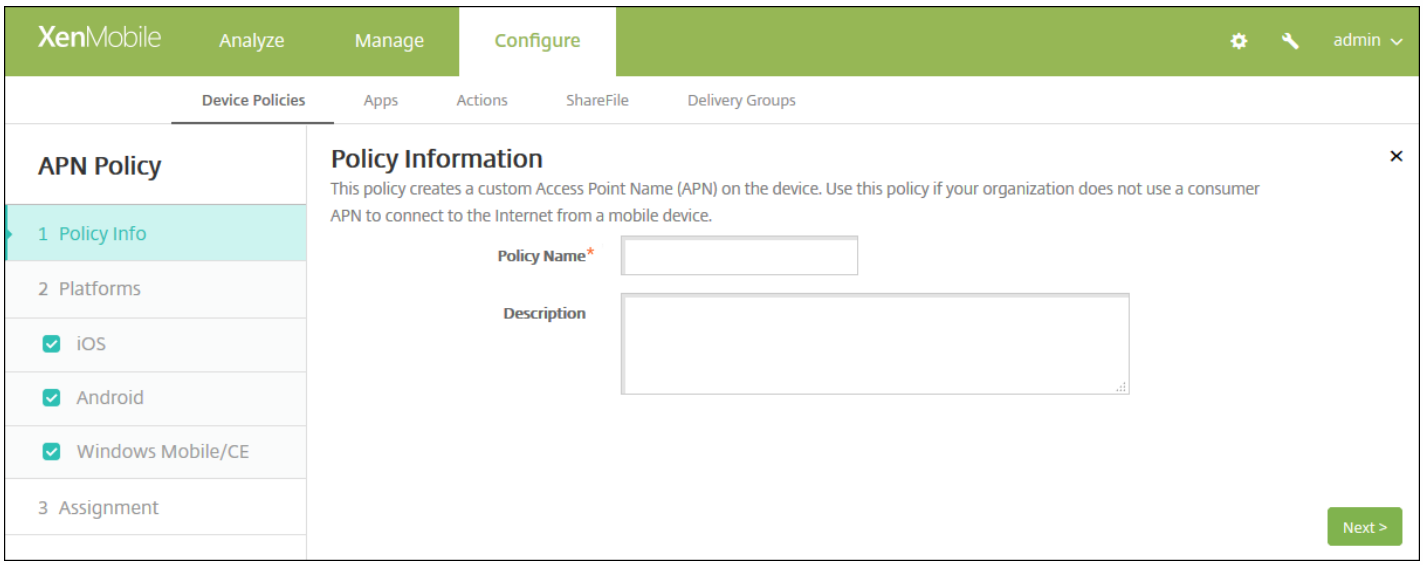
-
-



8. Configurez les règles de déploiement.

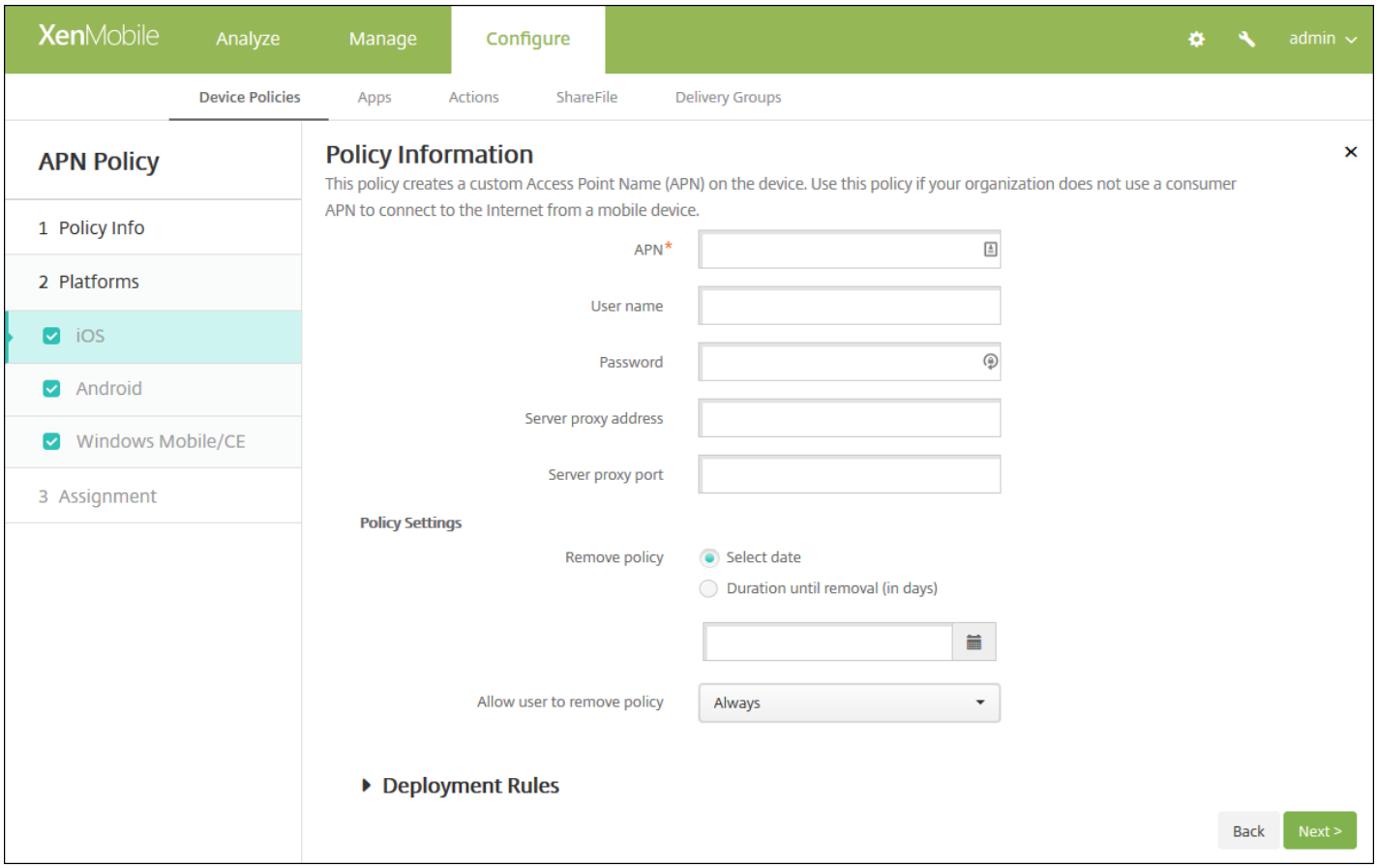


-
-
-
-
-
-
-



-
-

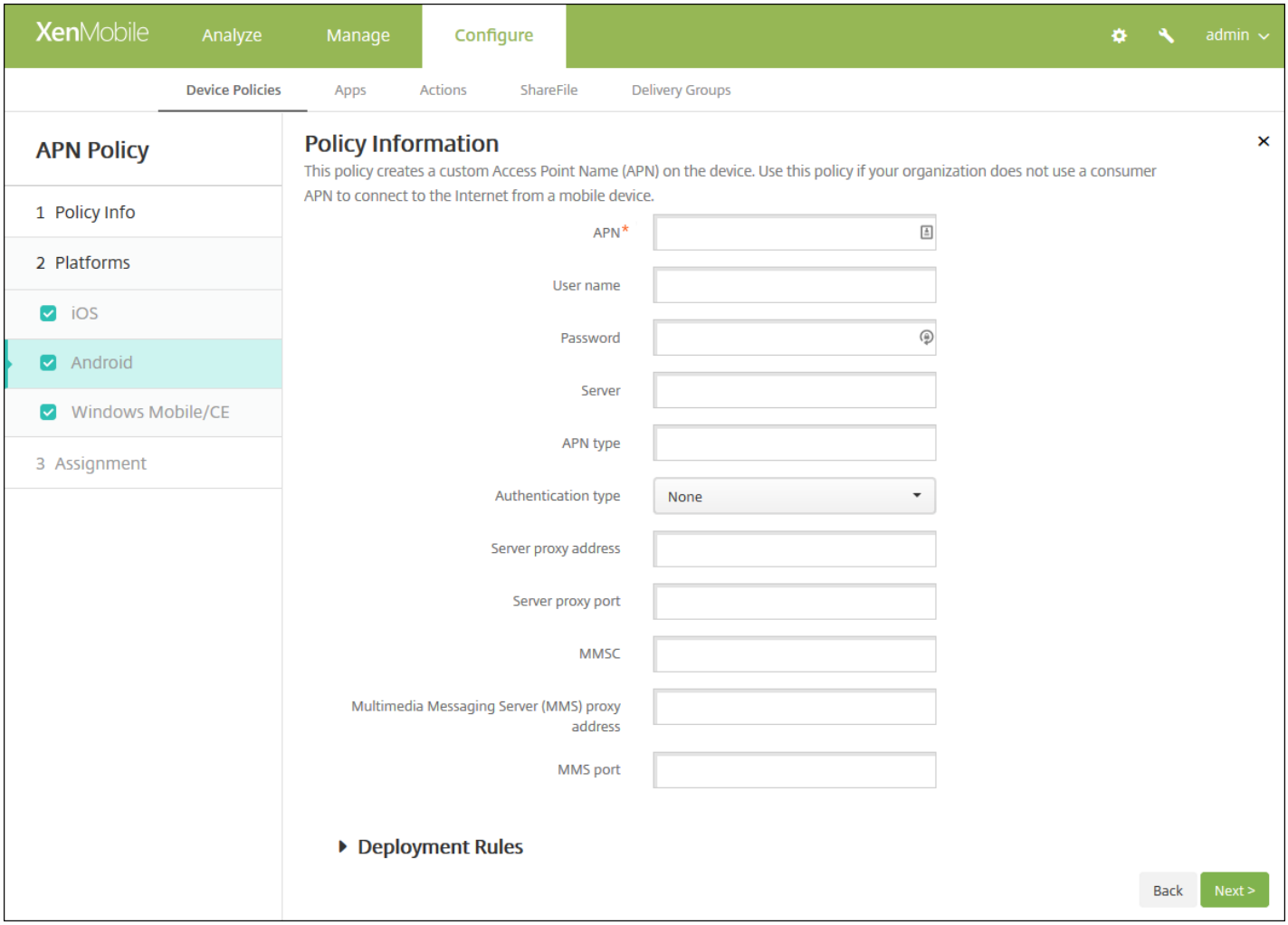
Configurer les paramètres pour iOS



-
-
-
-
-
-
  -
  -

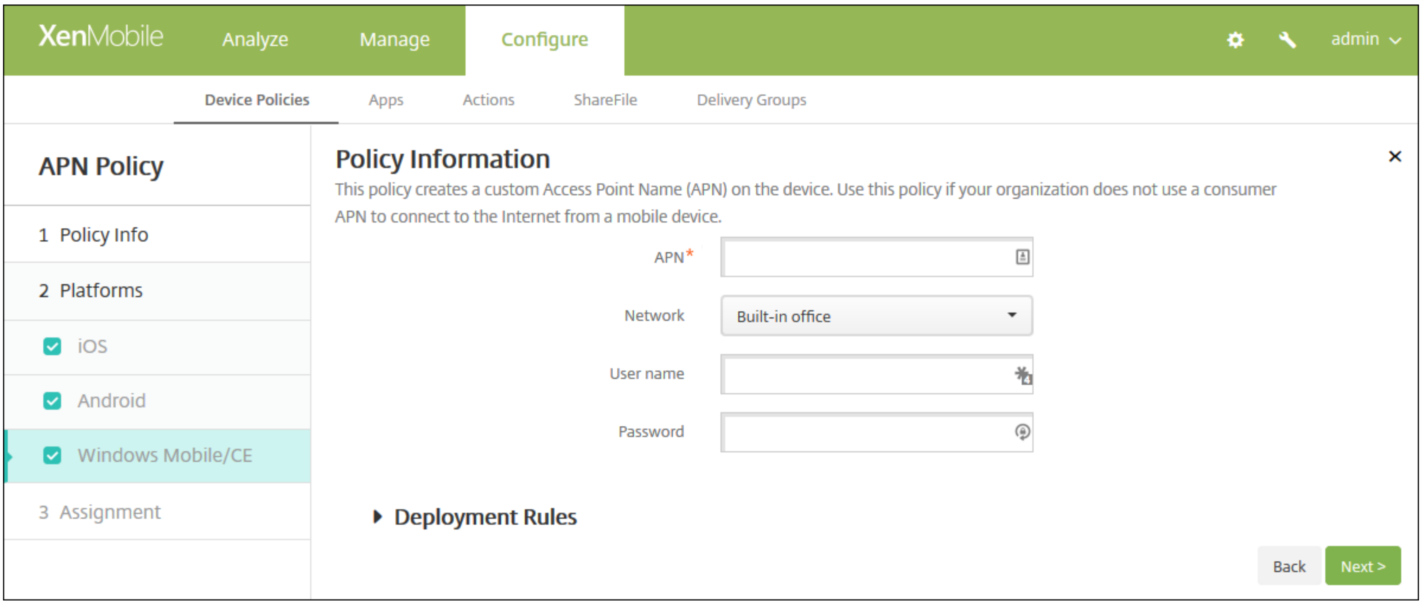
-

Configurer les paramètres pour Android

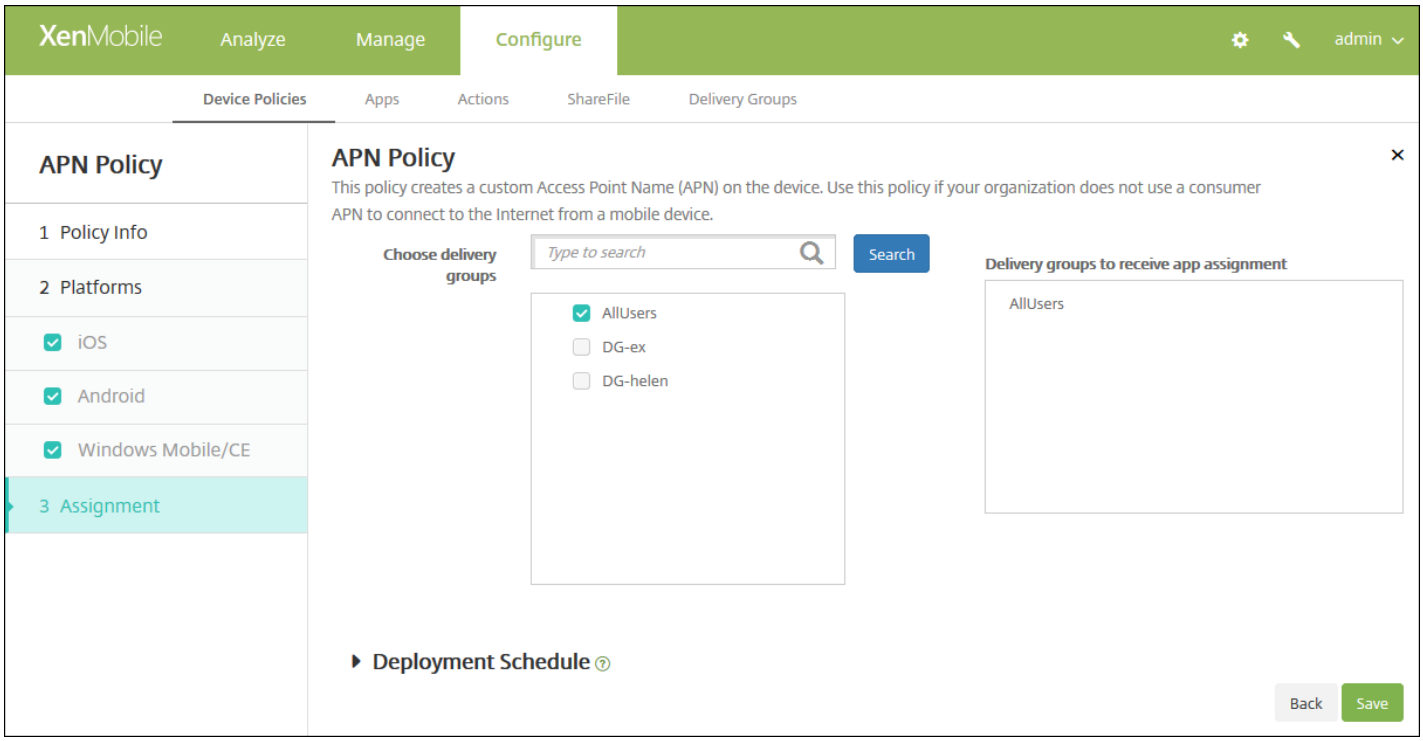


-
-
-
-
-

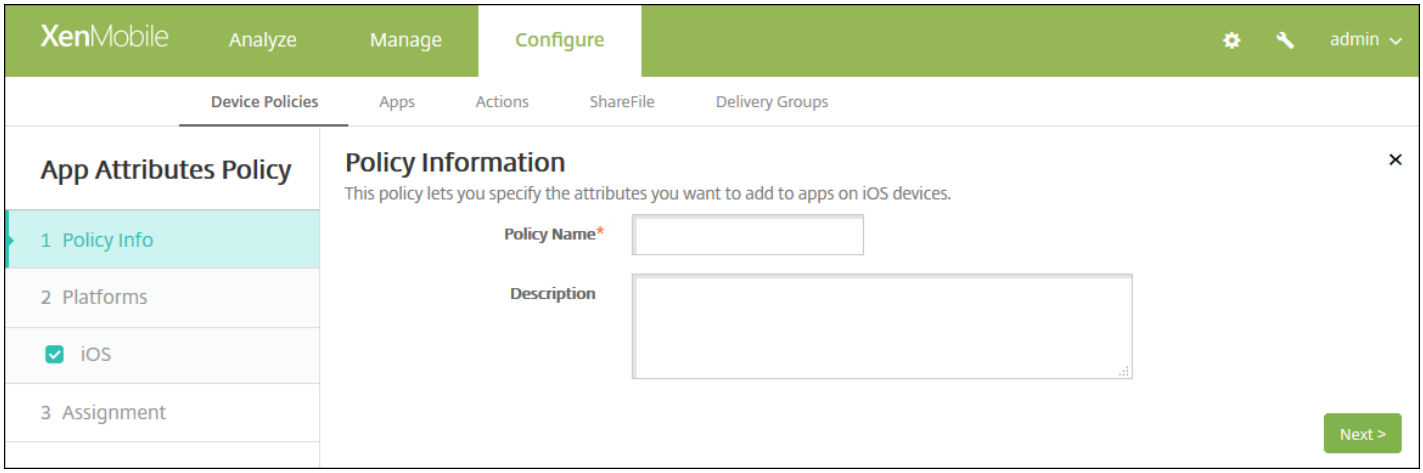
Configurer les paramètres Windows Mobile/CE



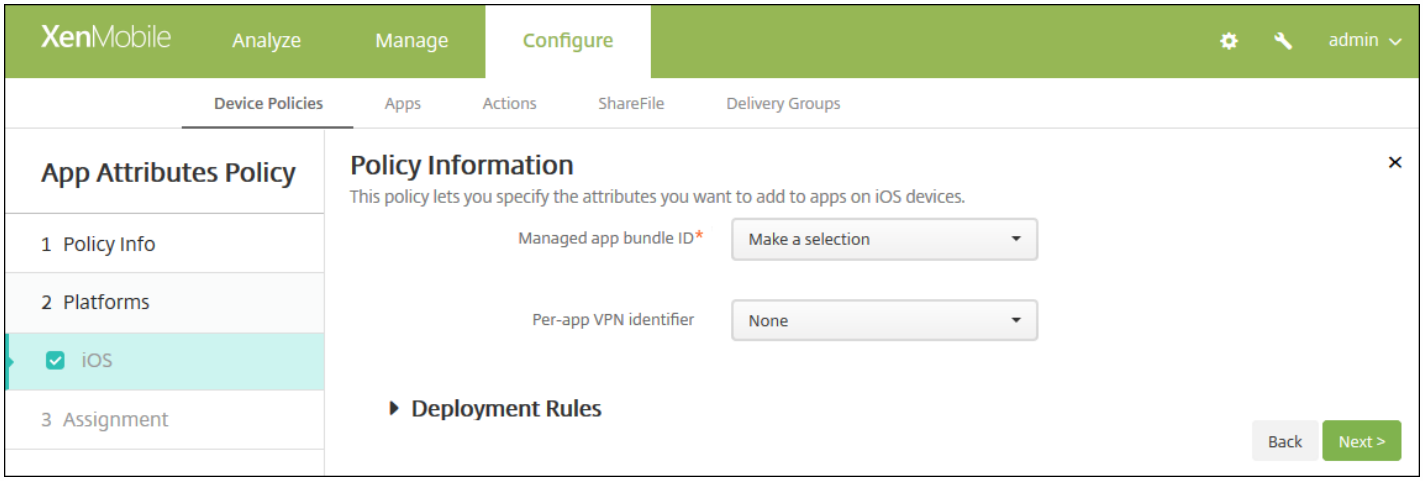
7. Configurez les règles de déploiement.



-

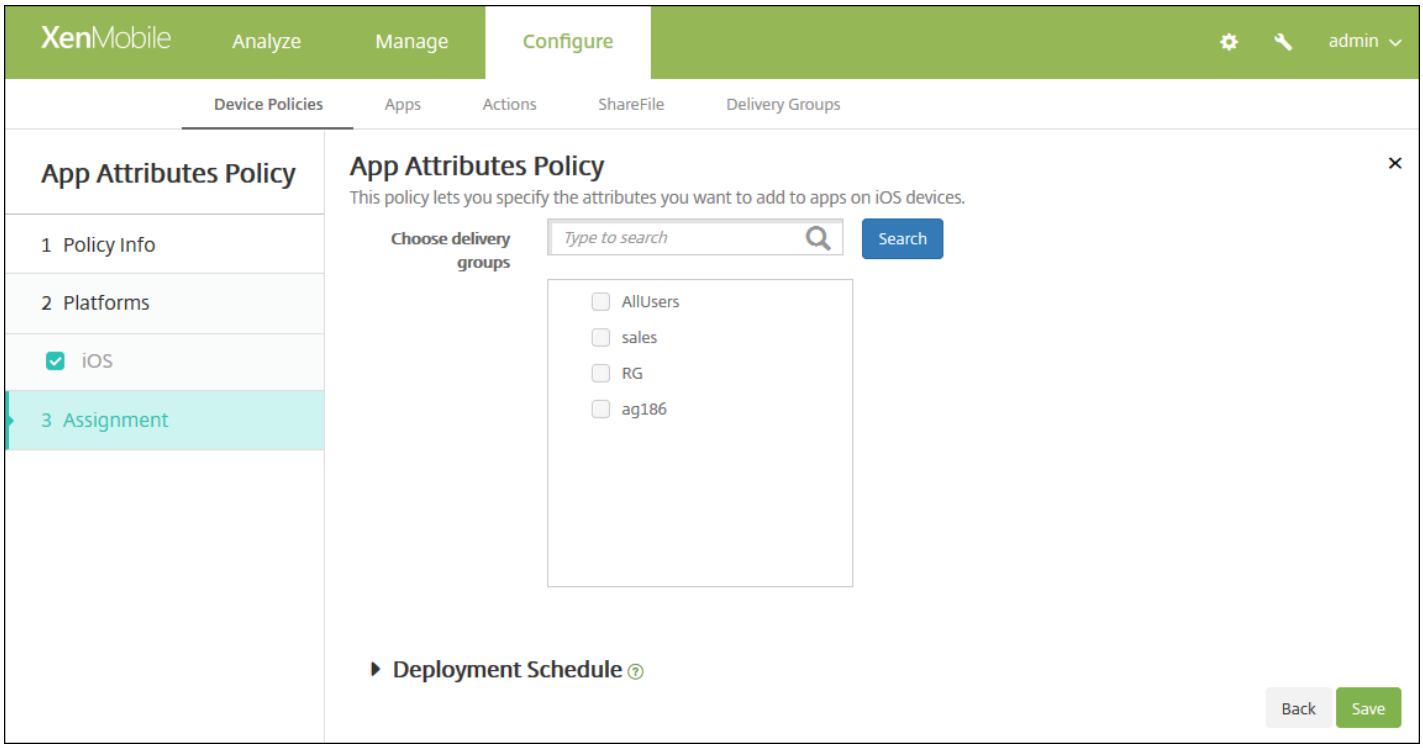


-
-

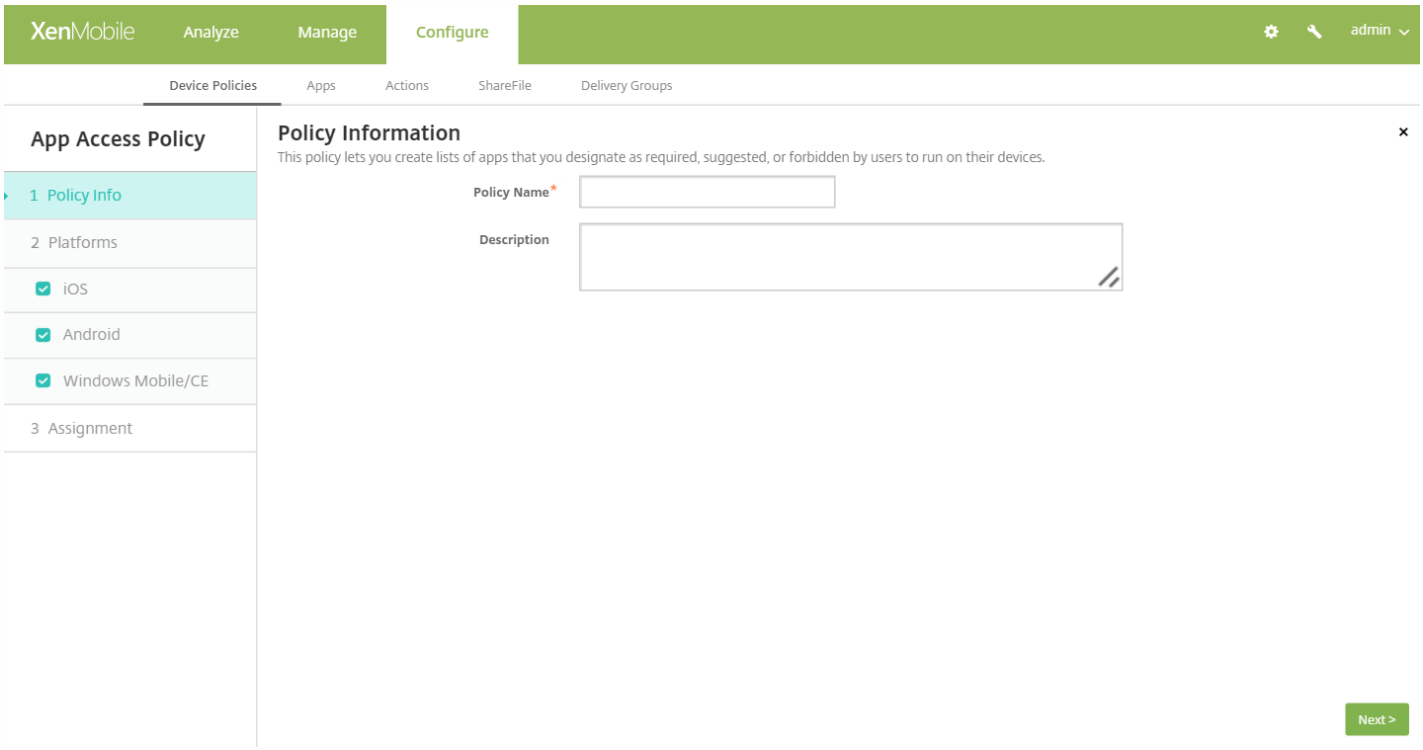


-
-
-

7. Configurez les règles de déploiement.



-
-
-
-
-
-
-



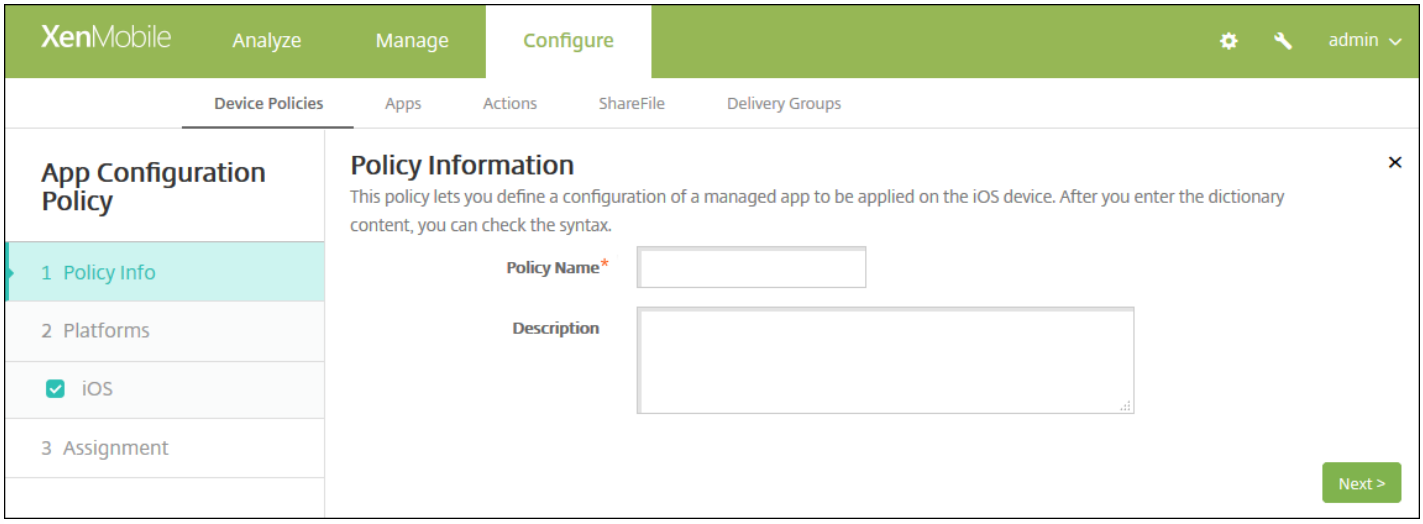
-
-

-
-
  -
  -
  -
  -

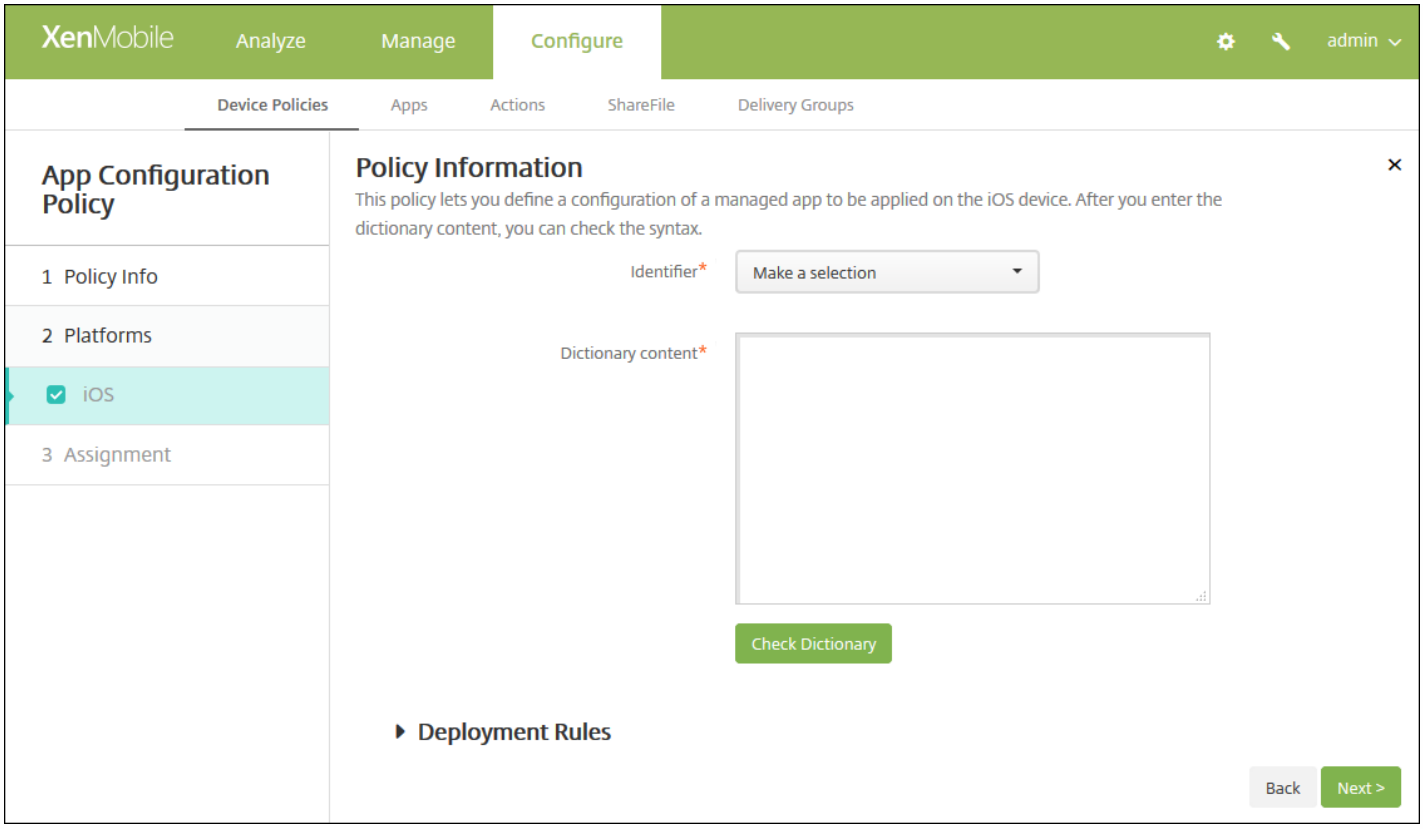
7. Configurez les règles de déploiement.

-
-
-
-
-

-
-

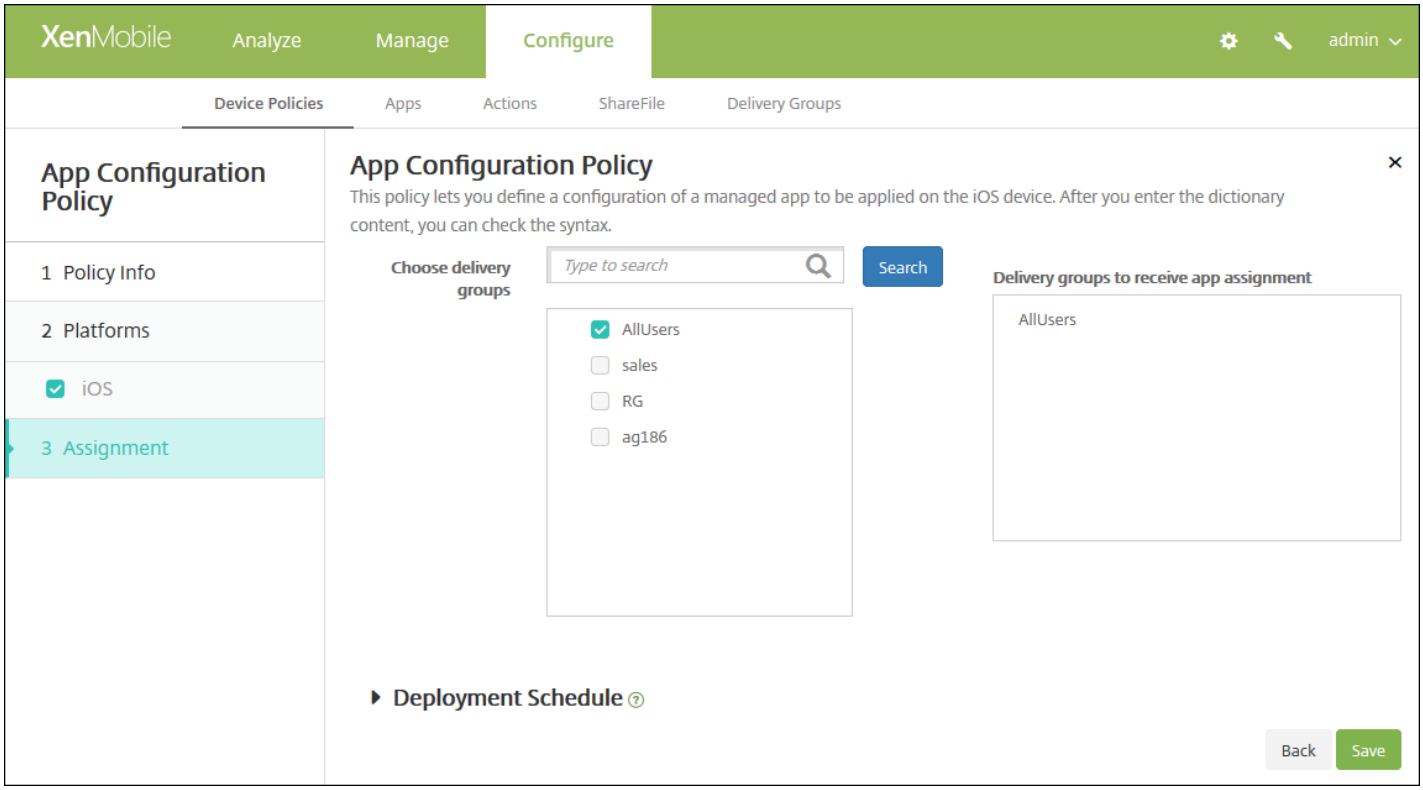


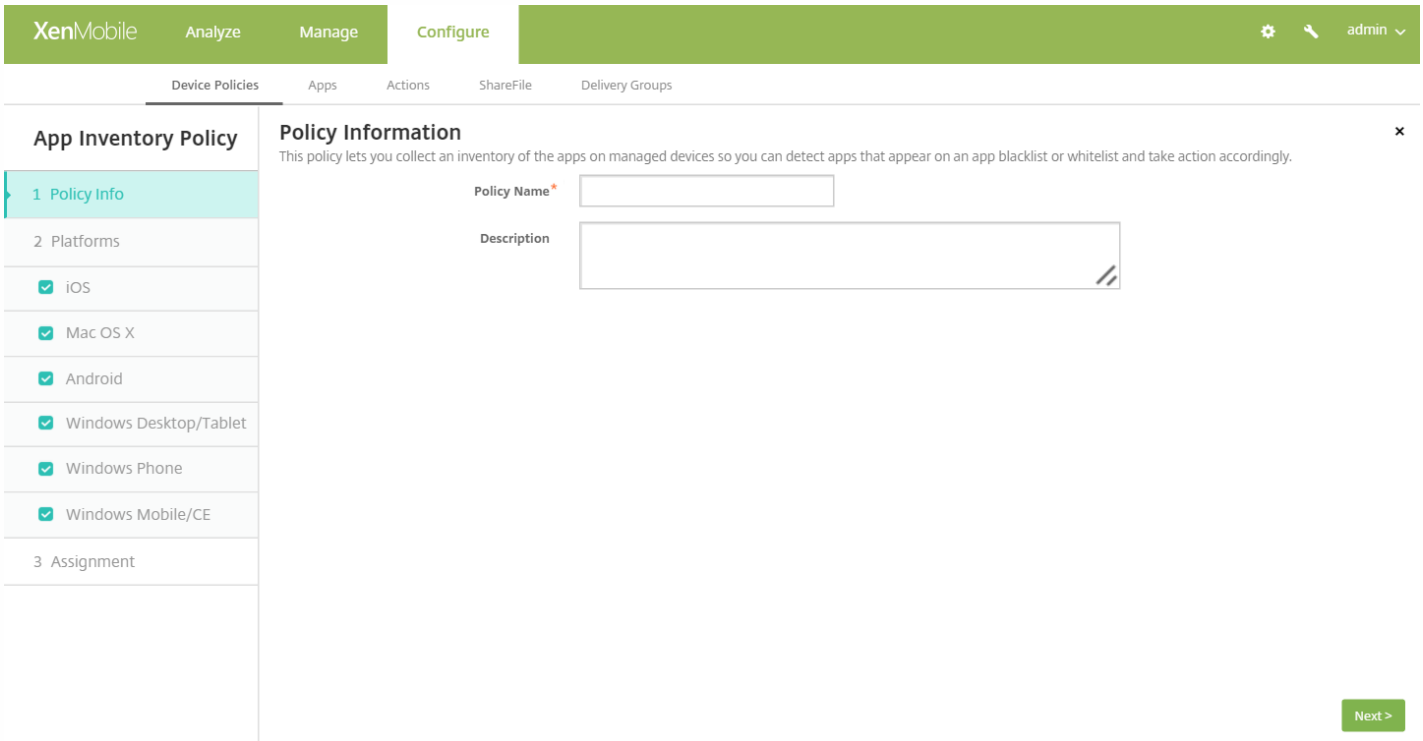
-
-



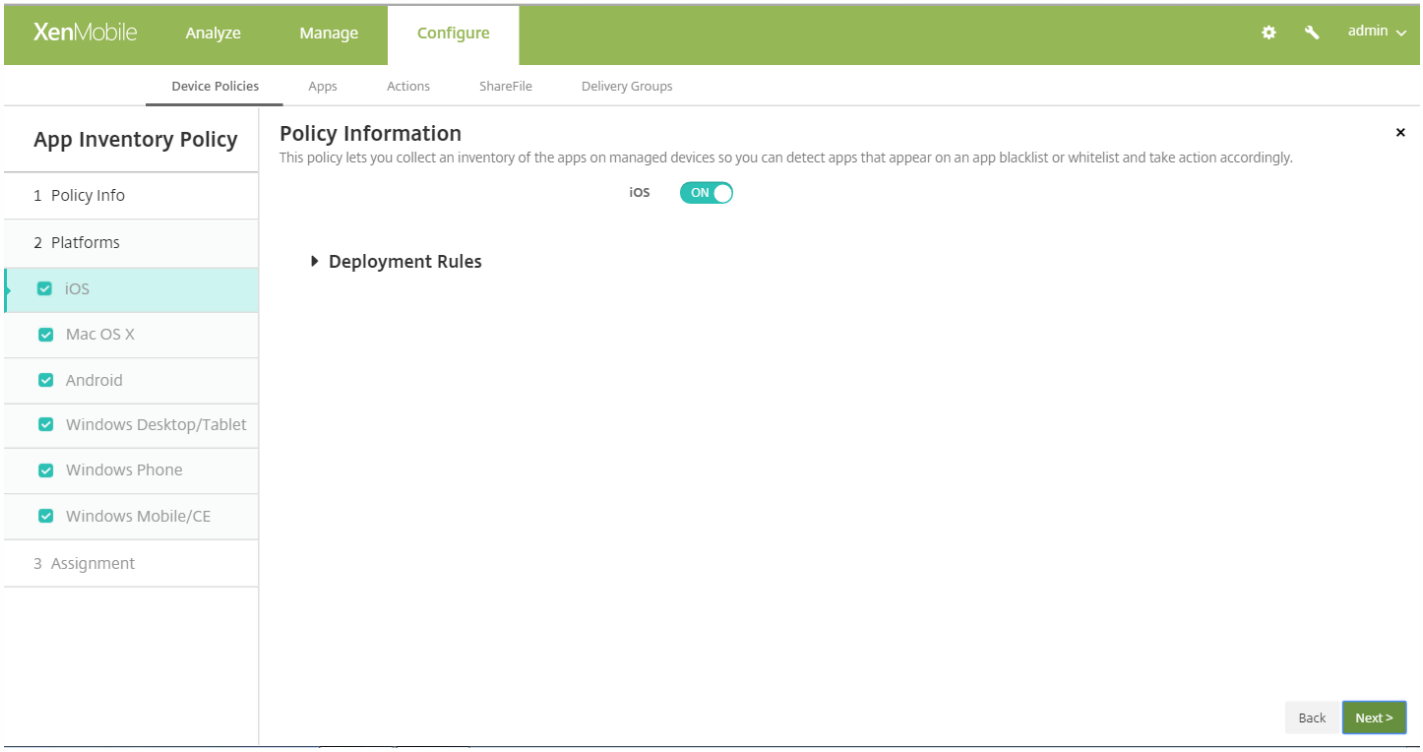
-
  -
-
-

7. Configurez les règles de déploiement.

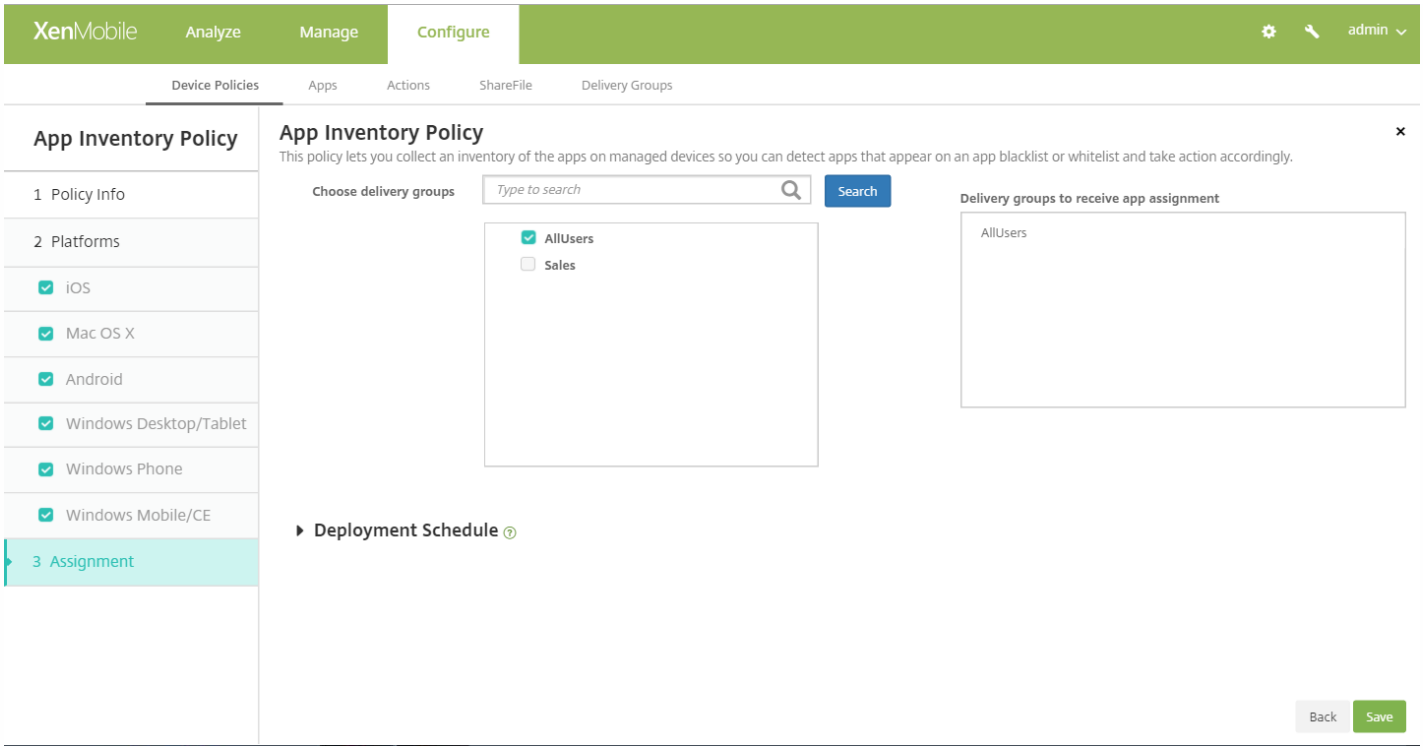




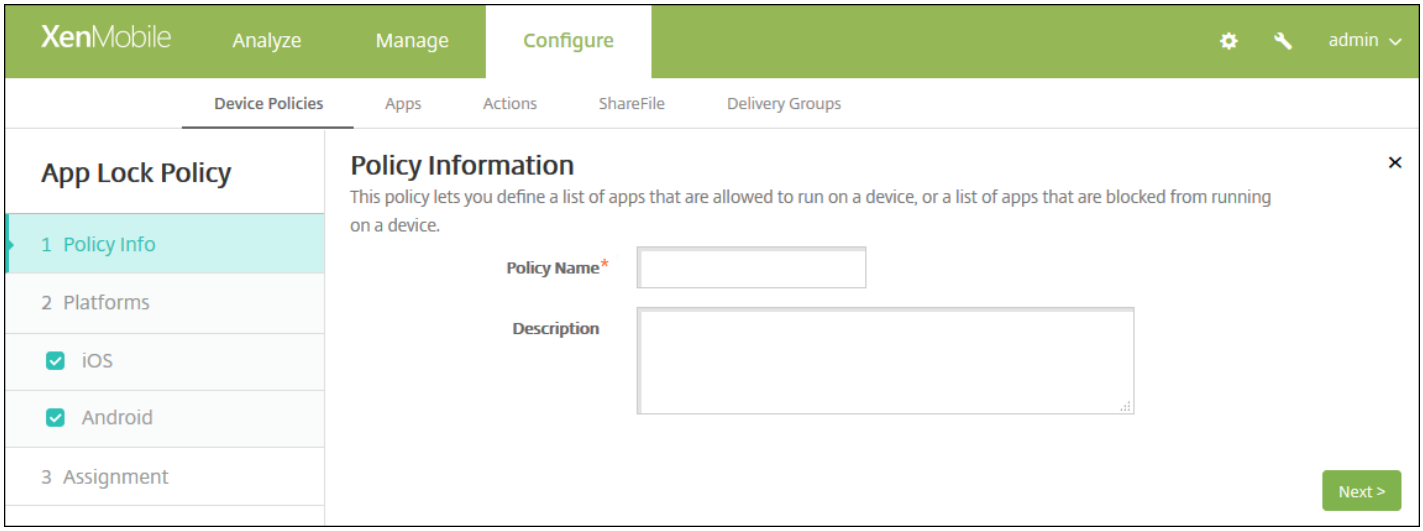
-
-



7. Configurez les règles de déploiement.

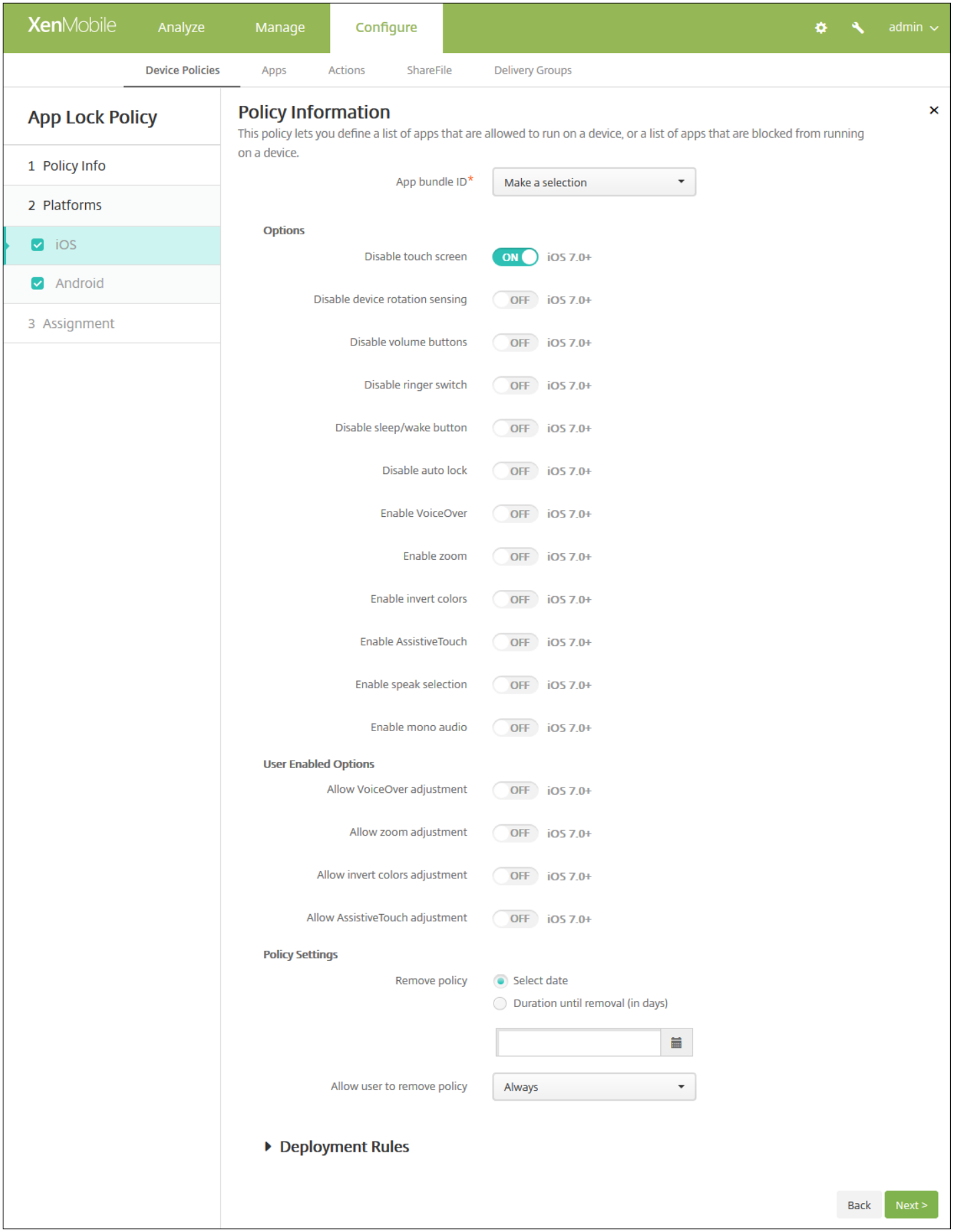


-
-
-
-
-
-
-



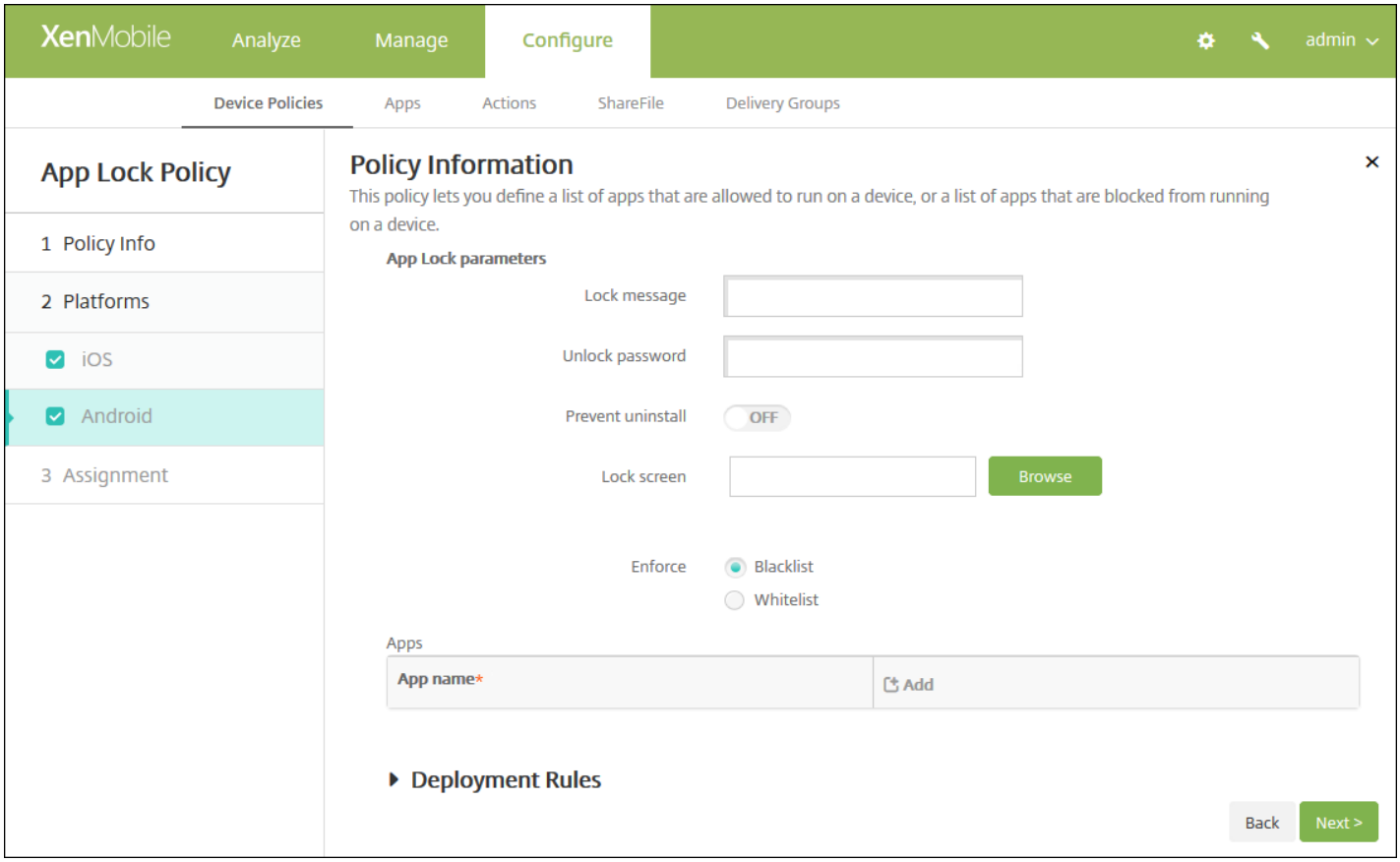
-
-

Configurer les paramètres pour iOS



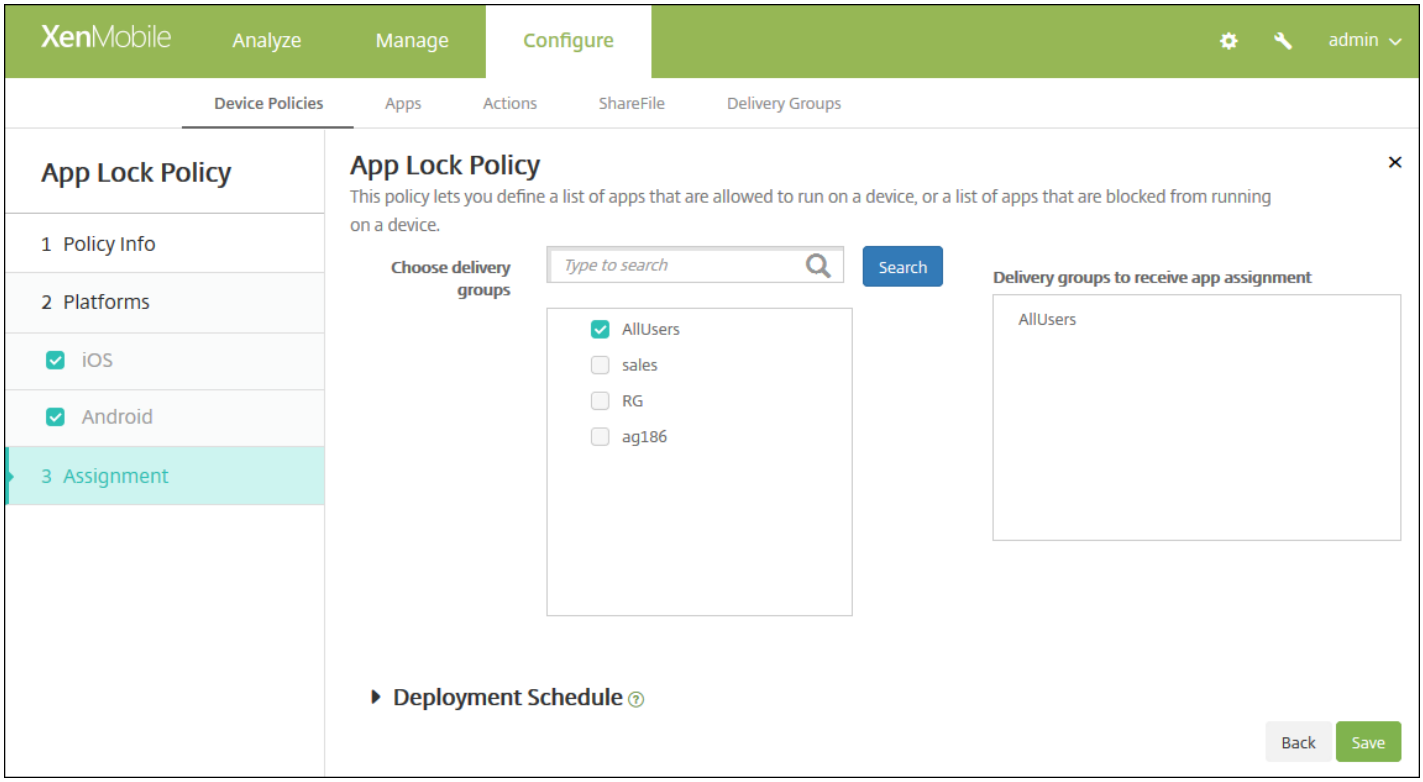
-
-
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -
-
  -
  -
  -
  -
-
  -
    -
    -
    -
    -

Configurer les paramètres pour Android

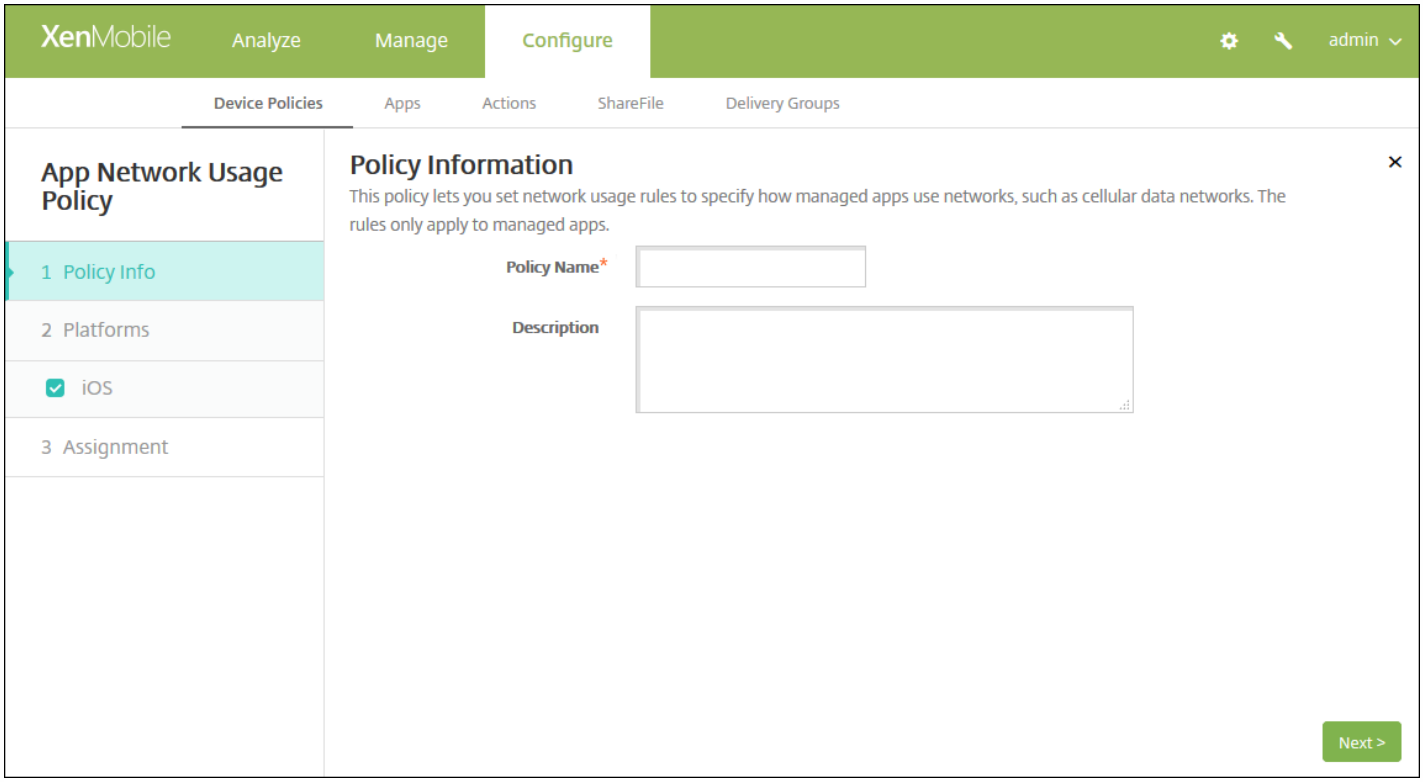


-
  -
  -
  -
  -
  -
-
  -
  -
  -
  -

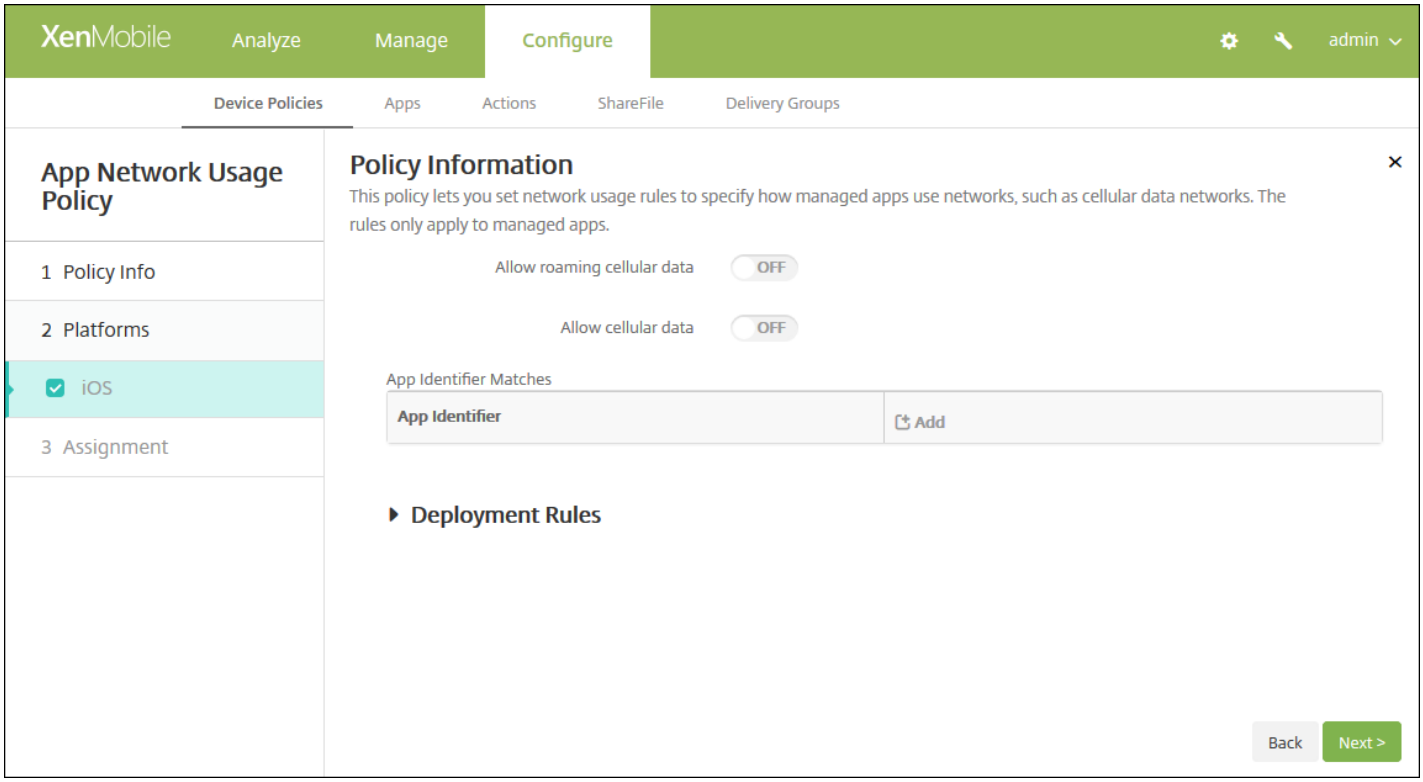
7. Configurez les règles de déploiement.



-
-
-

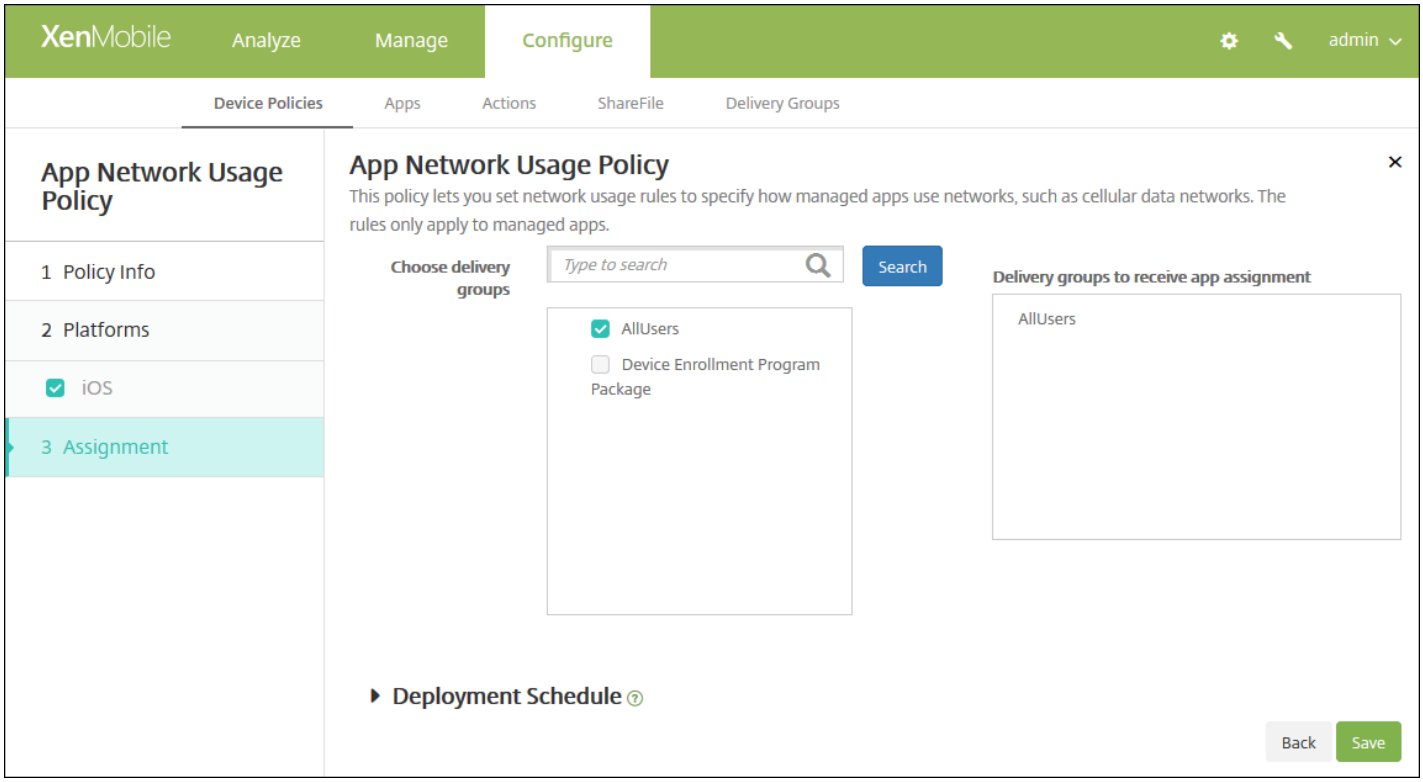


-
-

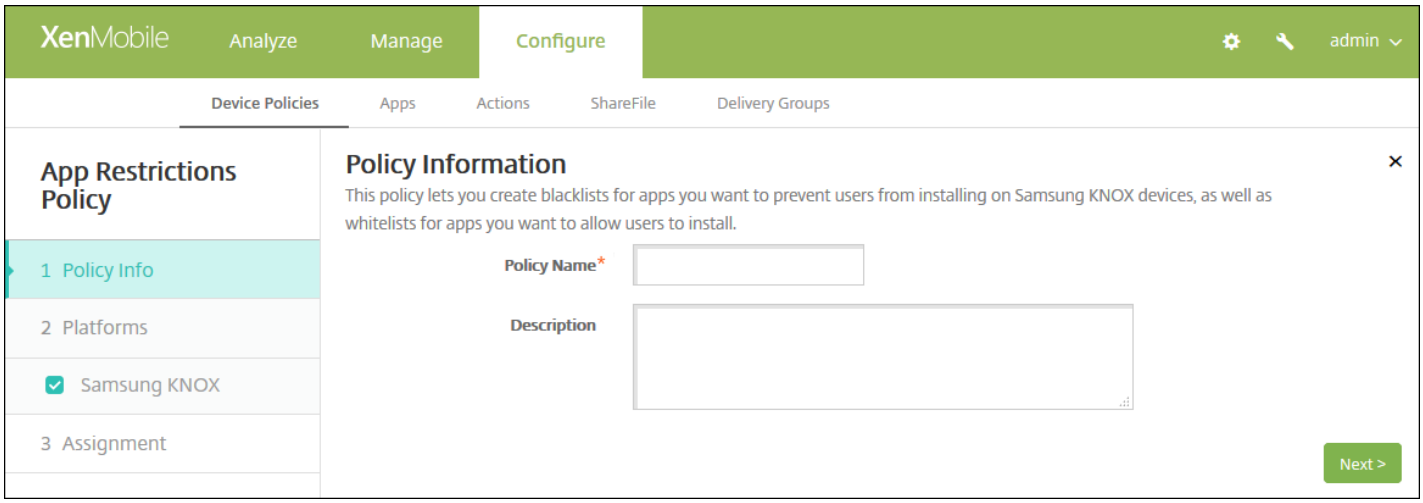


-
-
-
  -
  -

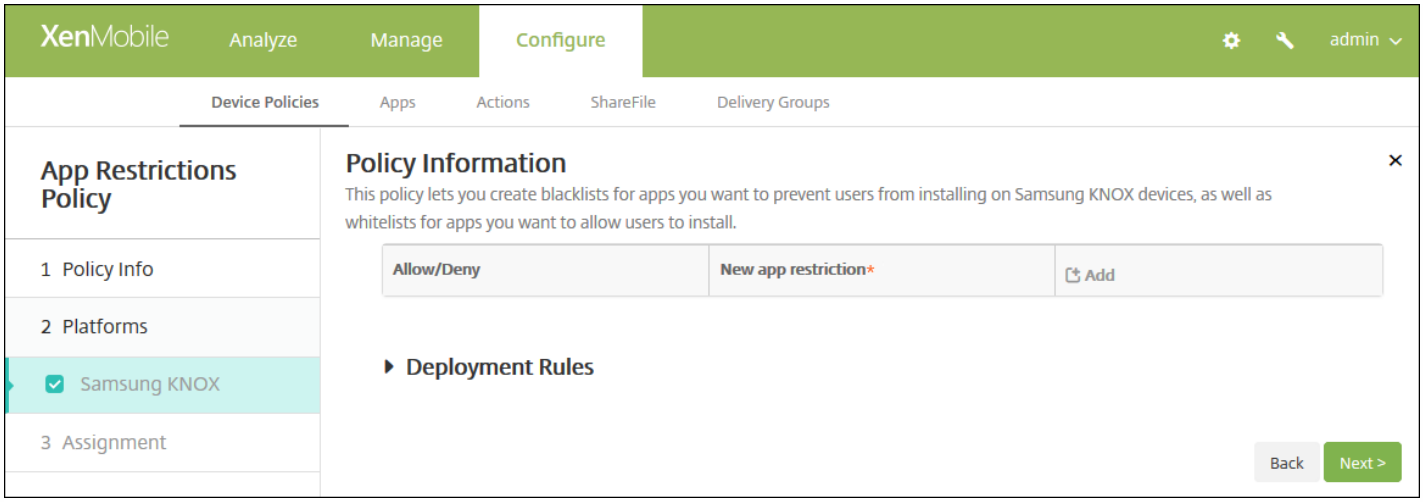
7. Configurez les règles de déploiement.



-
-
-
-
-
-
-

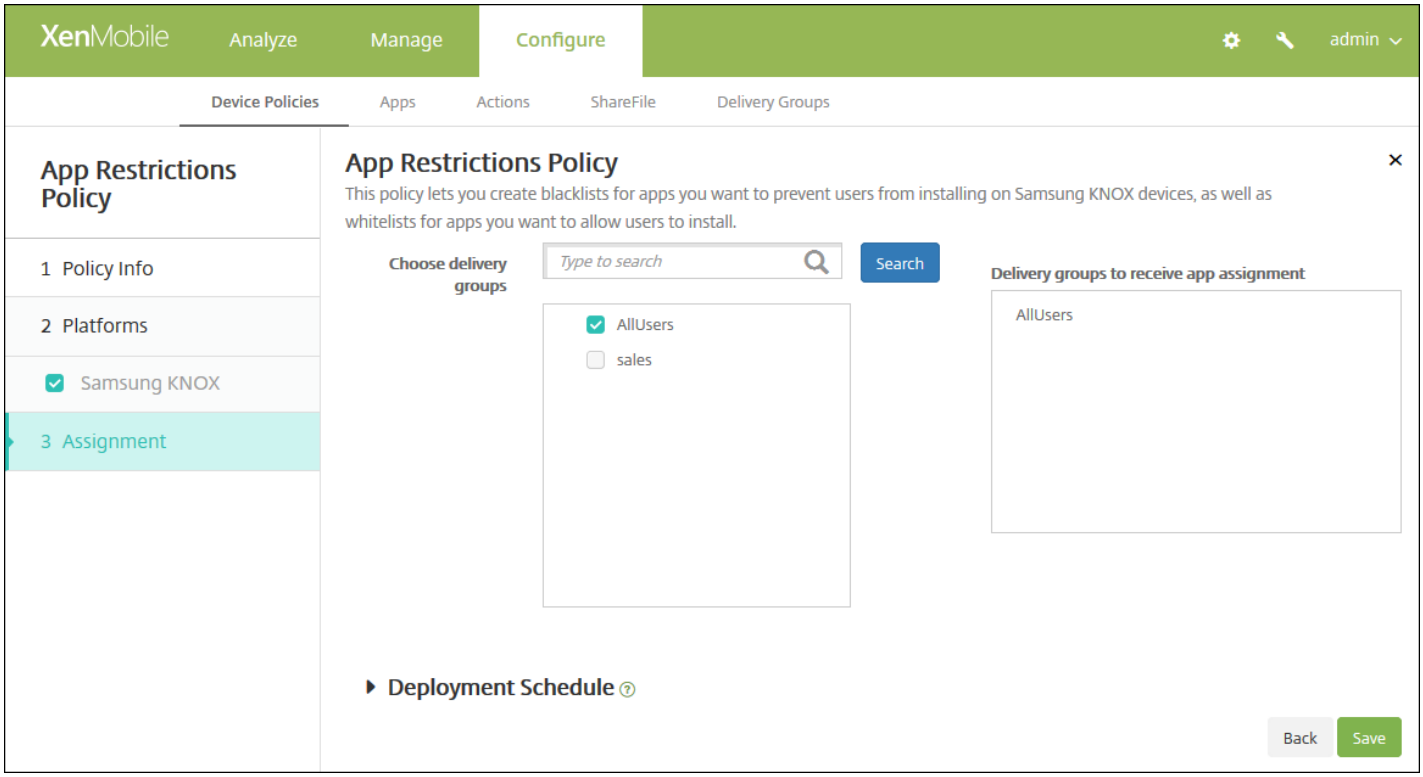


-
-

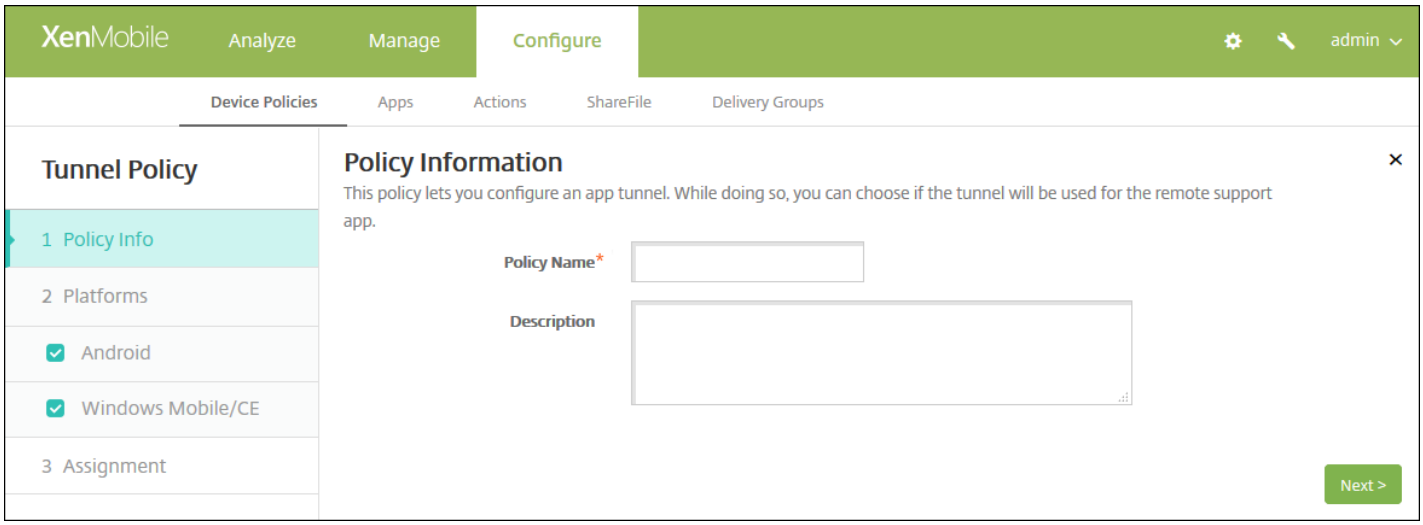


-
-
-

7. Configurez les règles de déploiement.

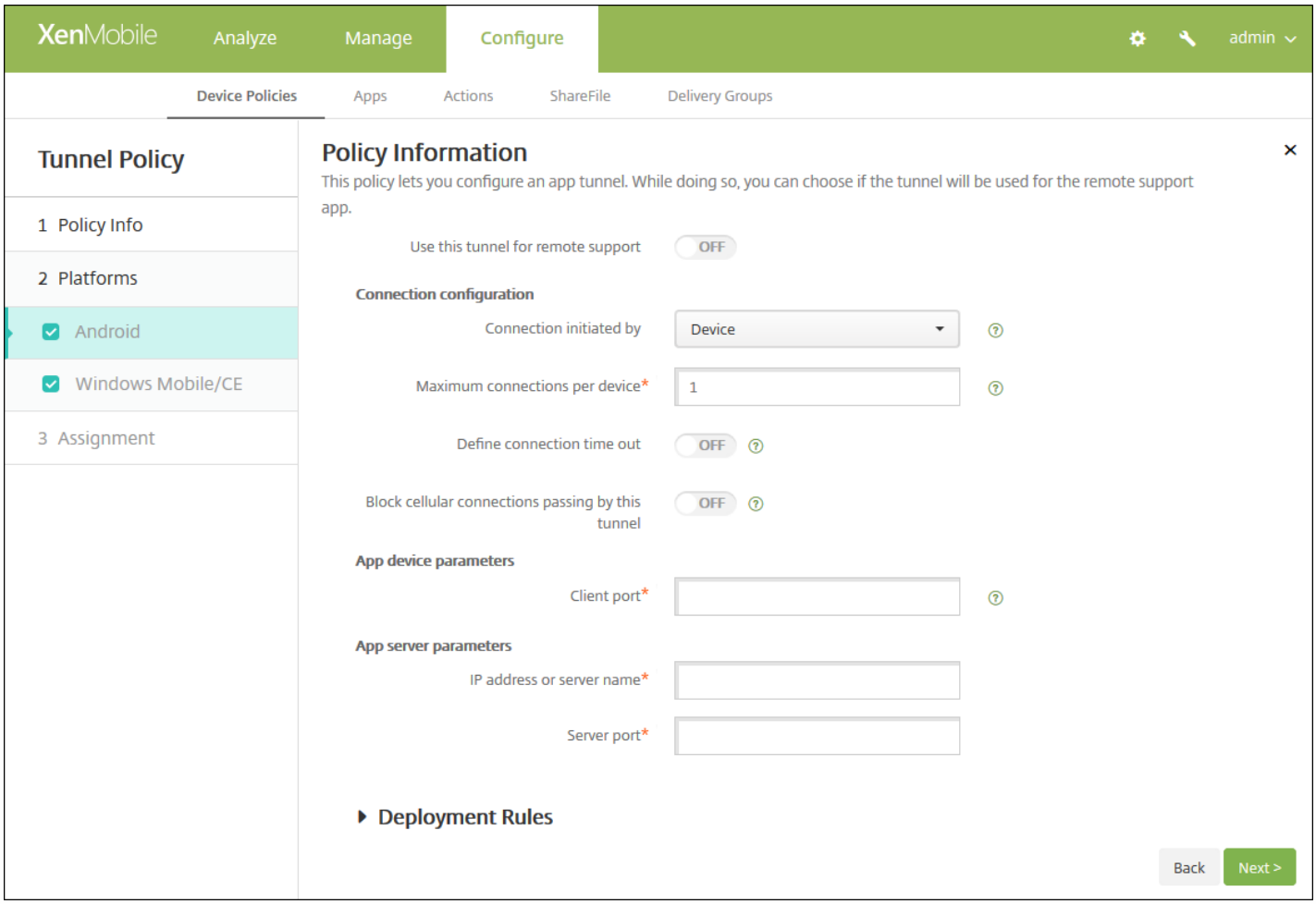


-
-
-
-
-
-
-



-
-

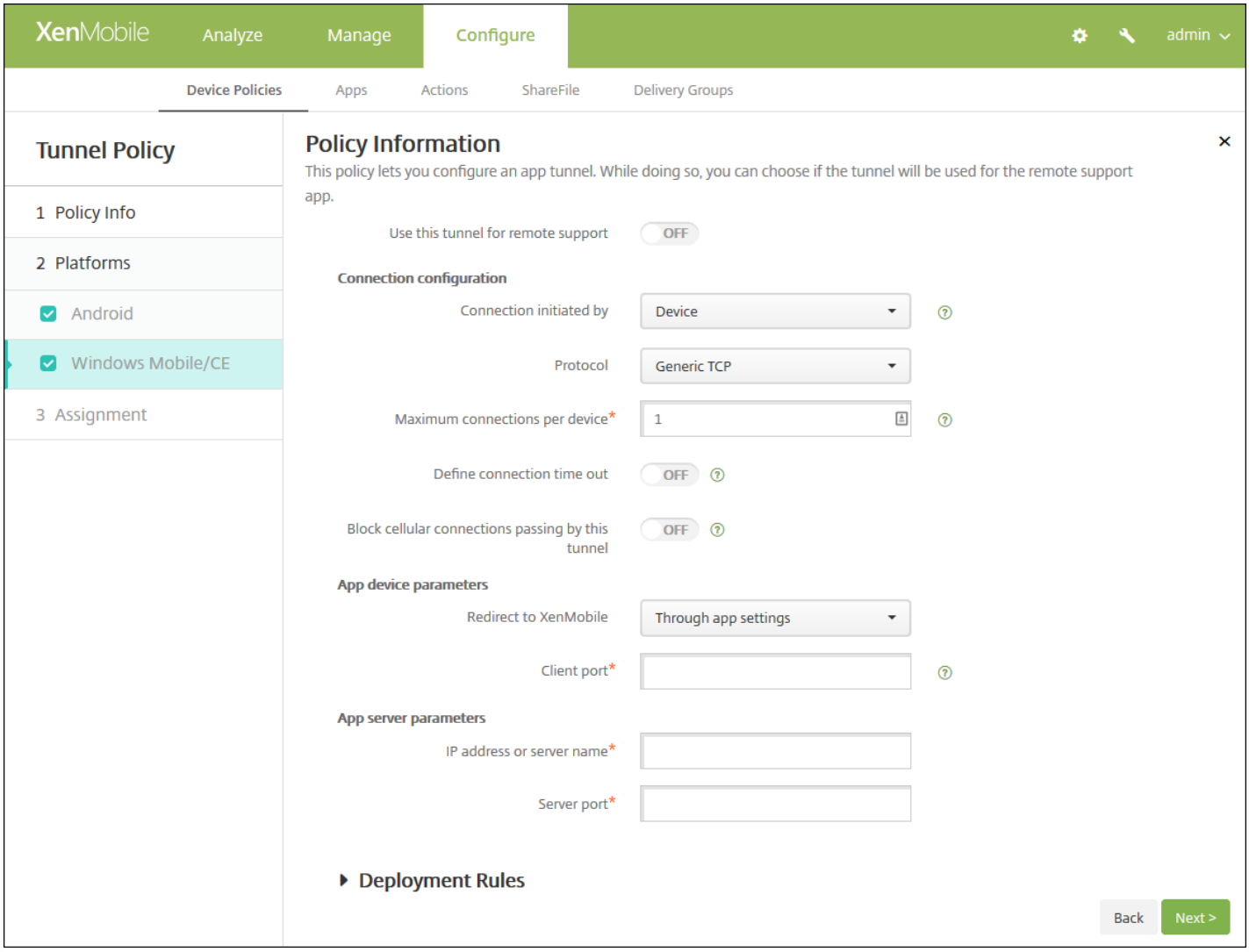
Configurer les paramètres pour Android



-
-
  -
  -
  -
    -

-
-
-
-
-
-
-
-
-
-

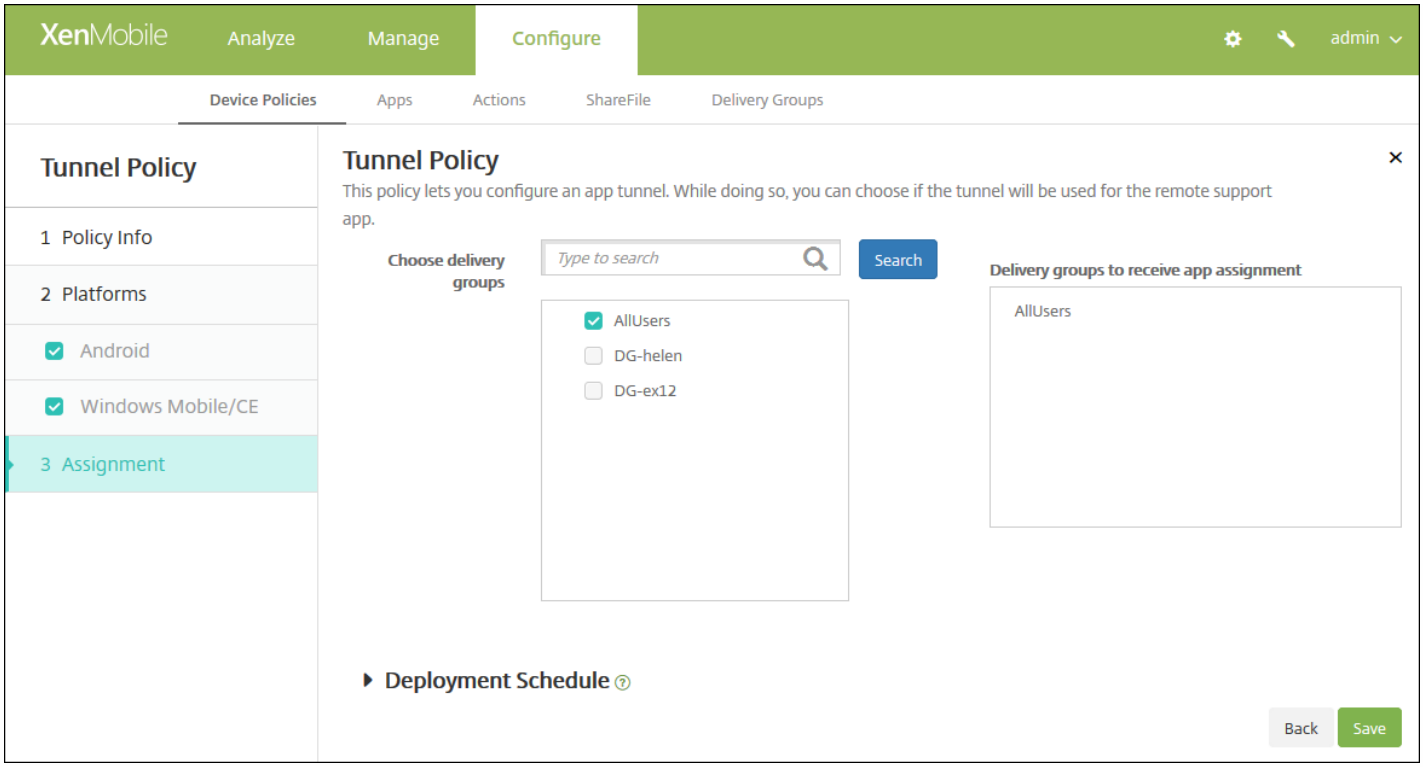
Configurer les paramètres pour Windows Mobile/CE

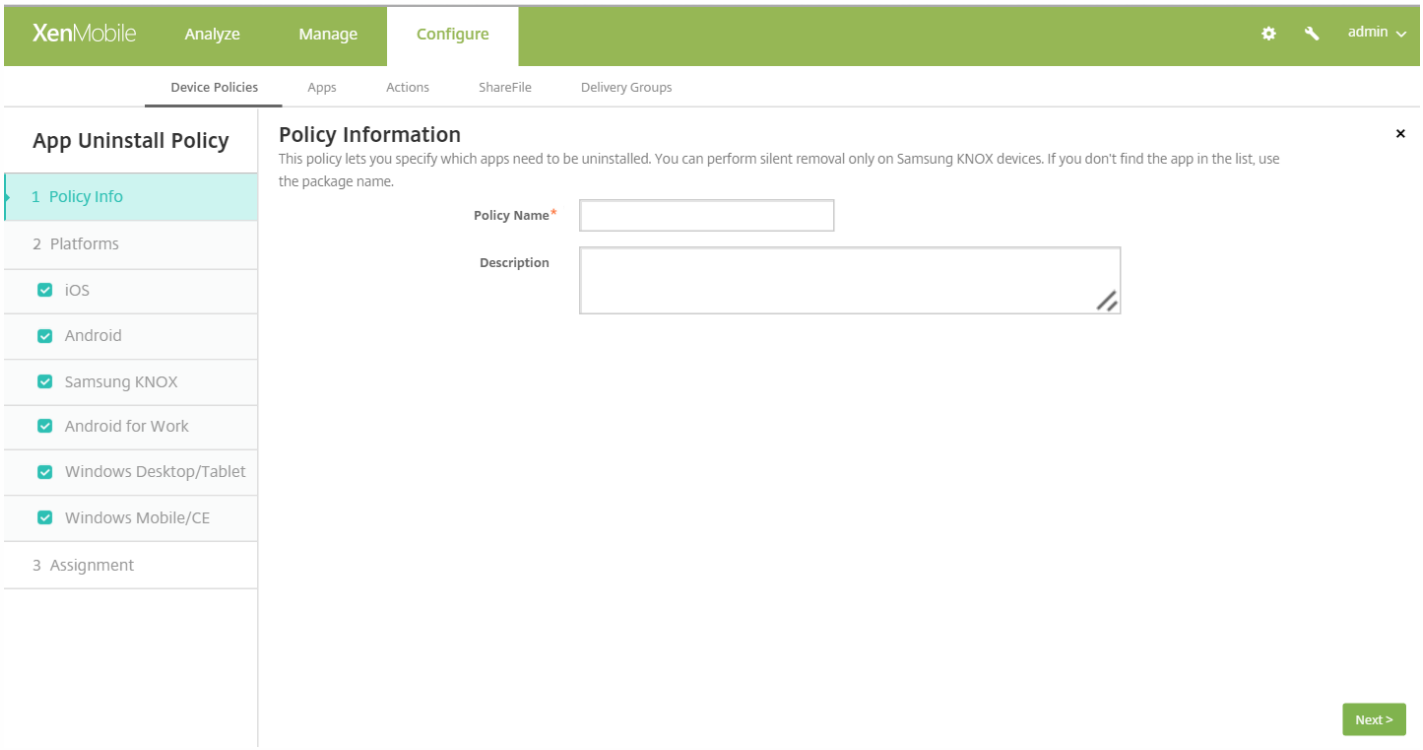


-
-
  -
  -
  -
  -
    -

-
-
  -
  -
-
-
-
-
-
-
-
-
-

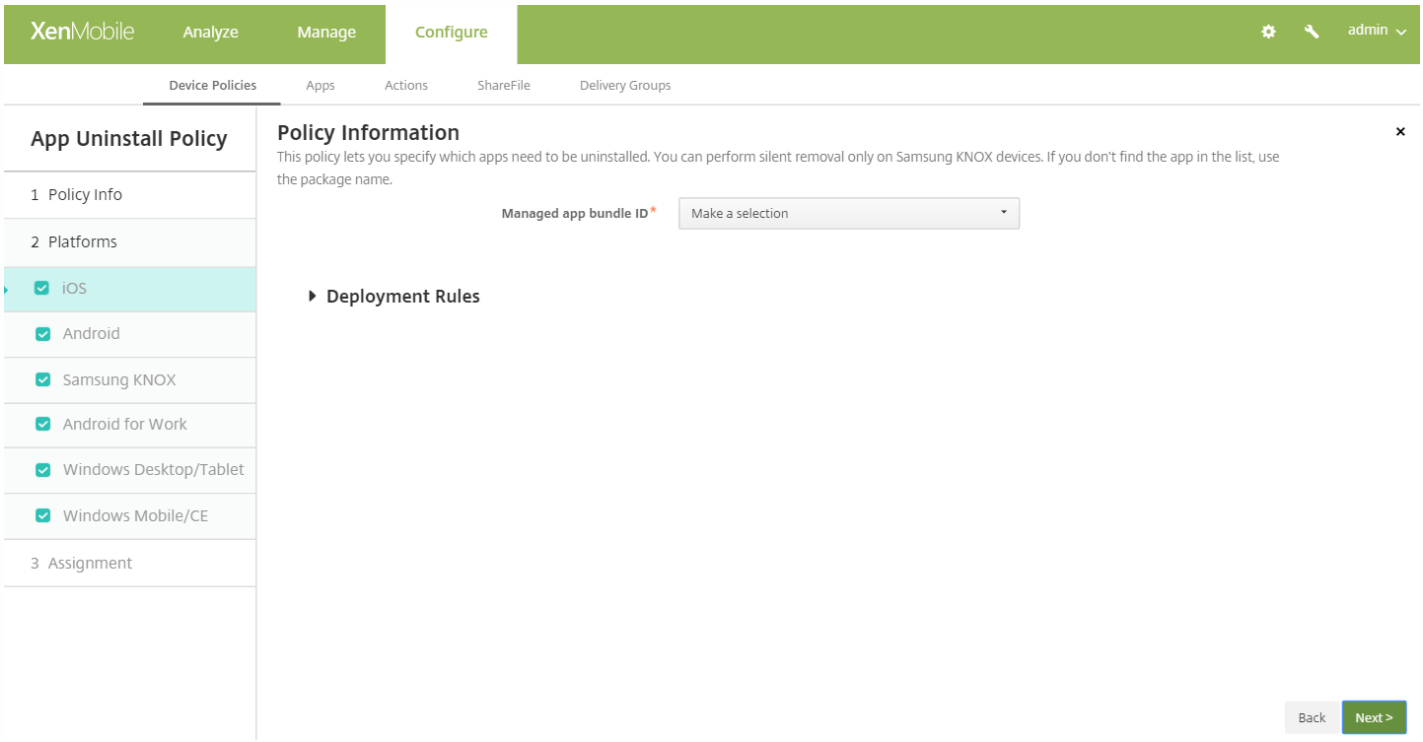
7. Configurez les règles de déploiement.





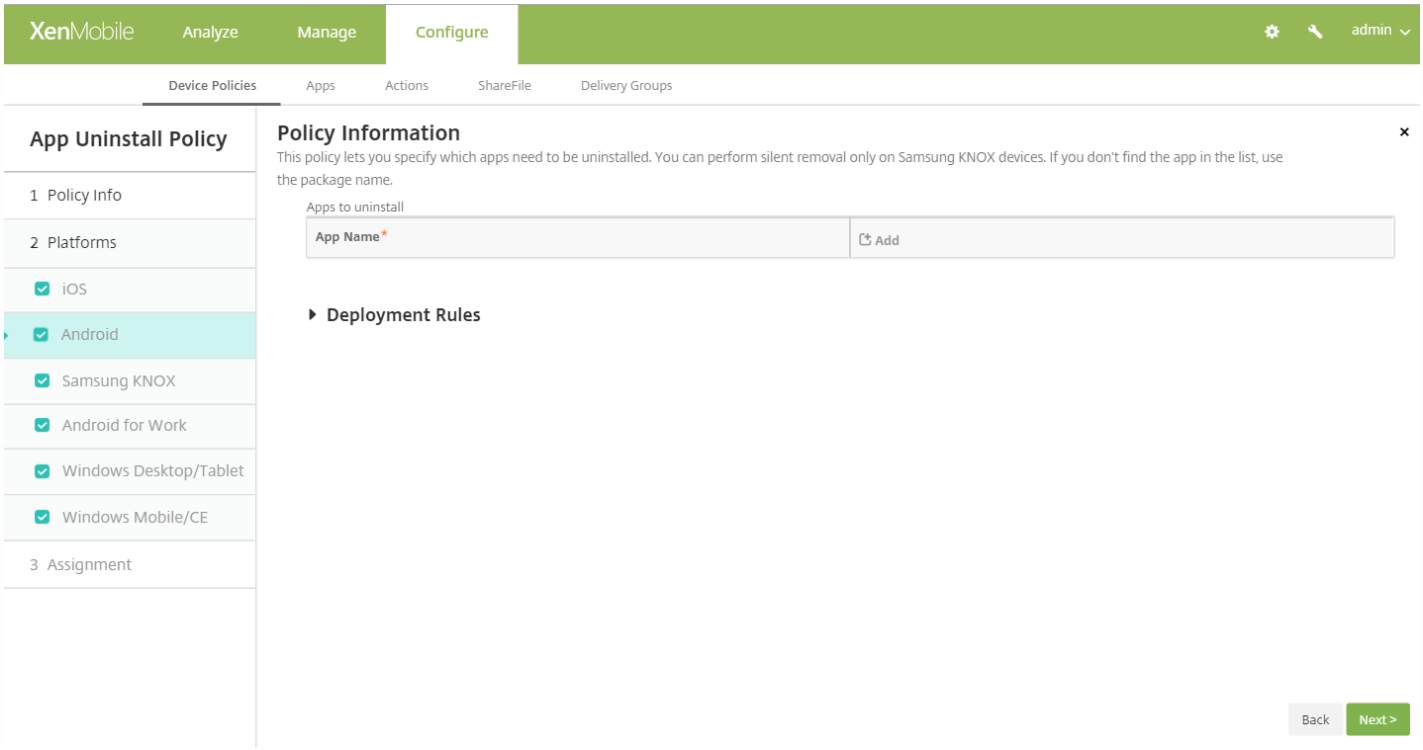
-
-

Configurer les paramètres pour iOS



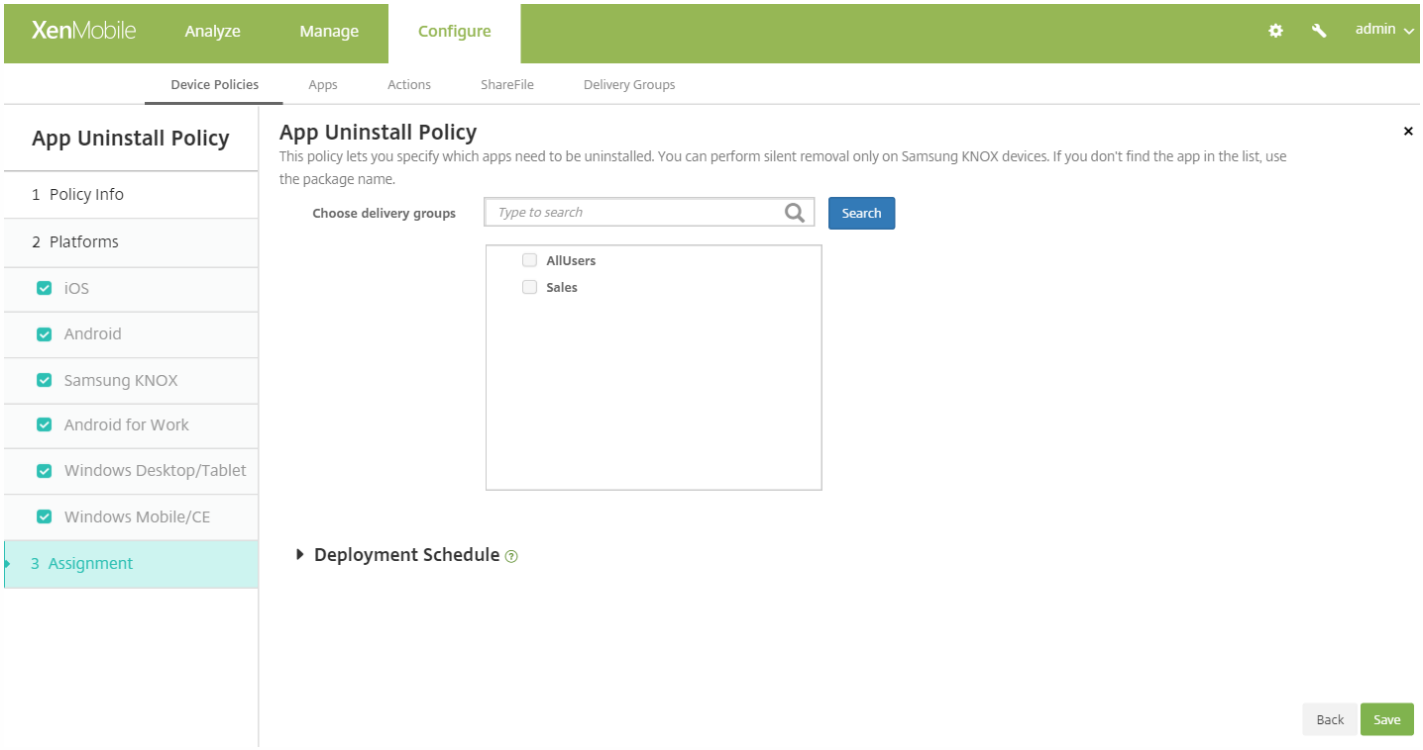
-
  -

Configurer tous les autres paramètres de plate-forme

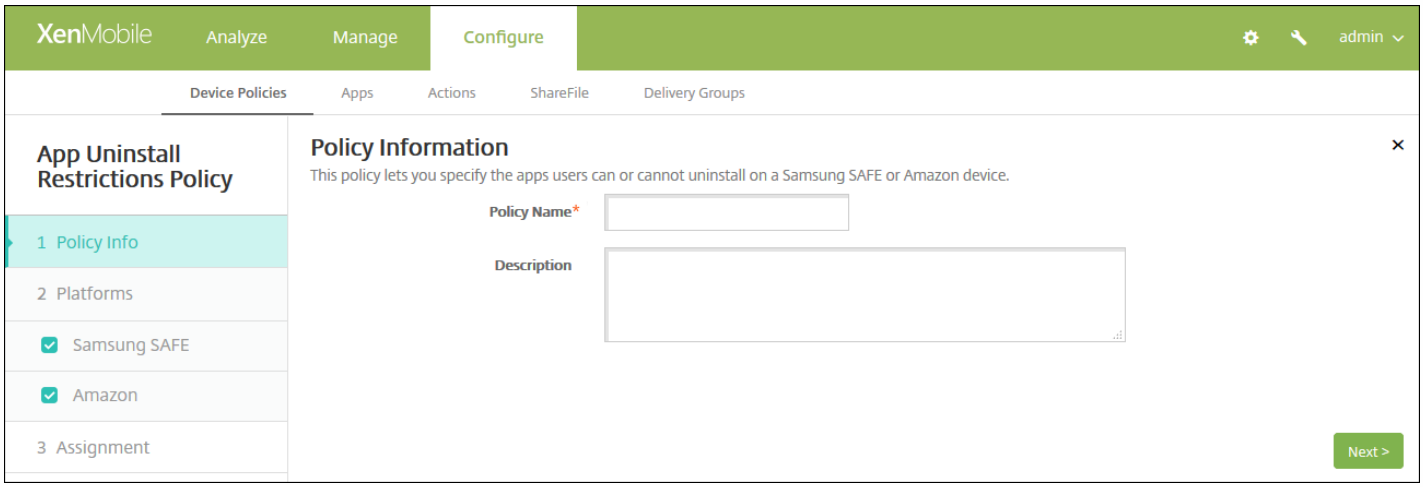


-
  -
  -

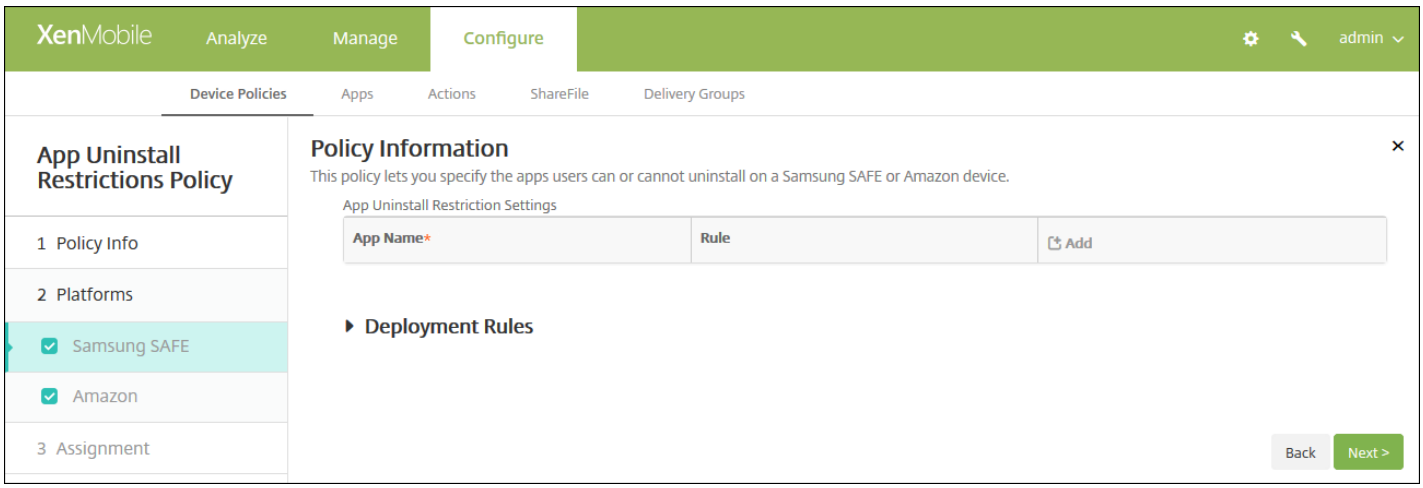
7. Configurez les règles de déploiement.



-
-
-
-
-
-
-
-

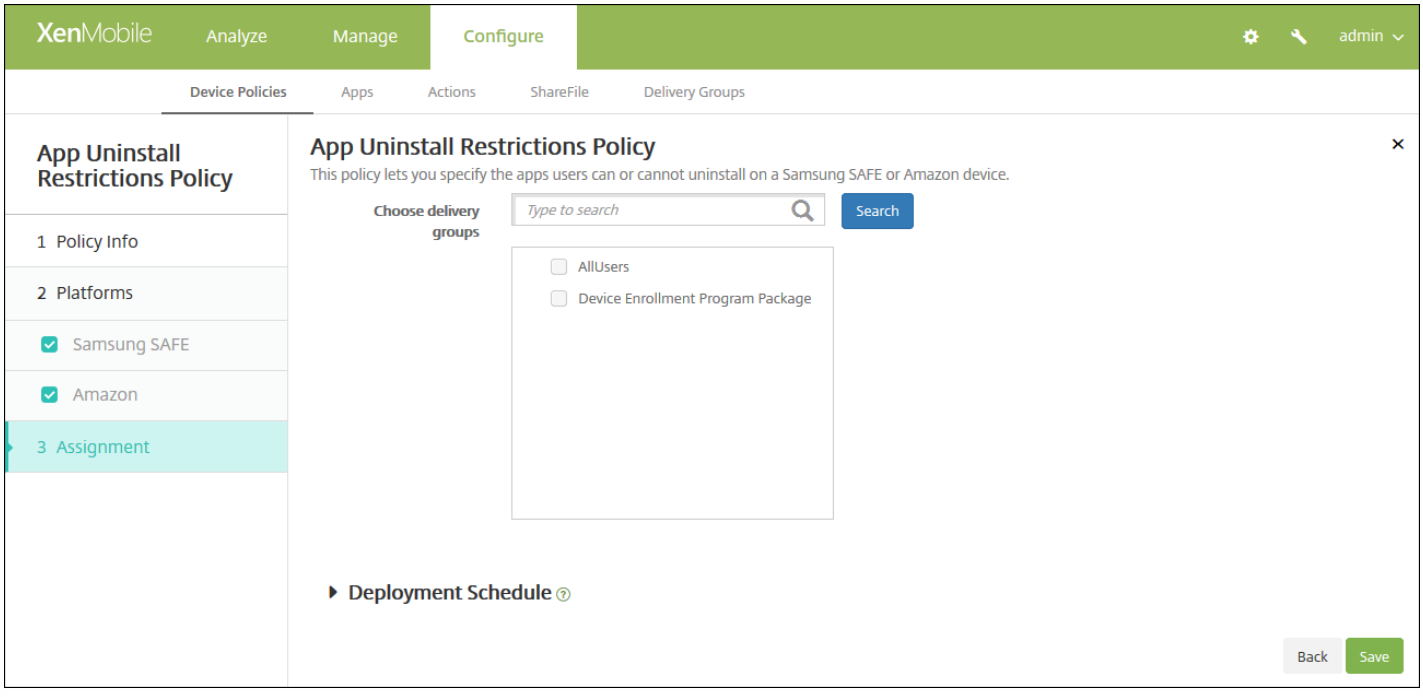


-
-

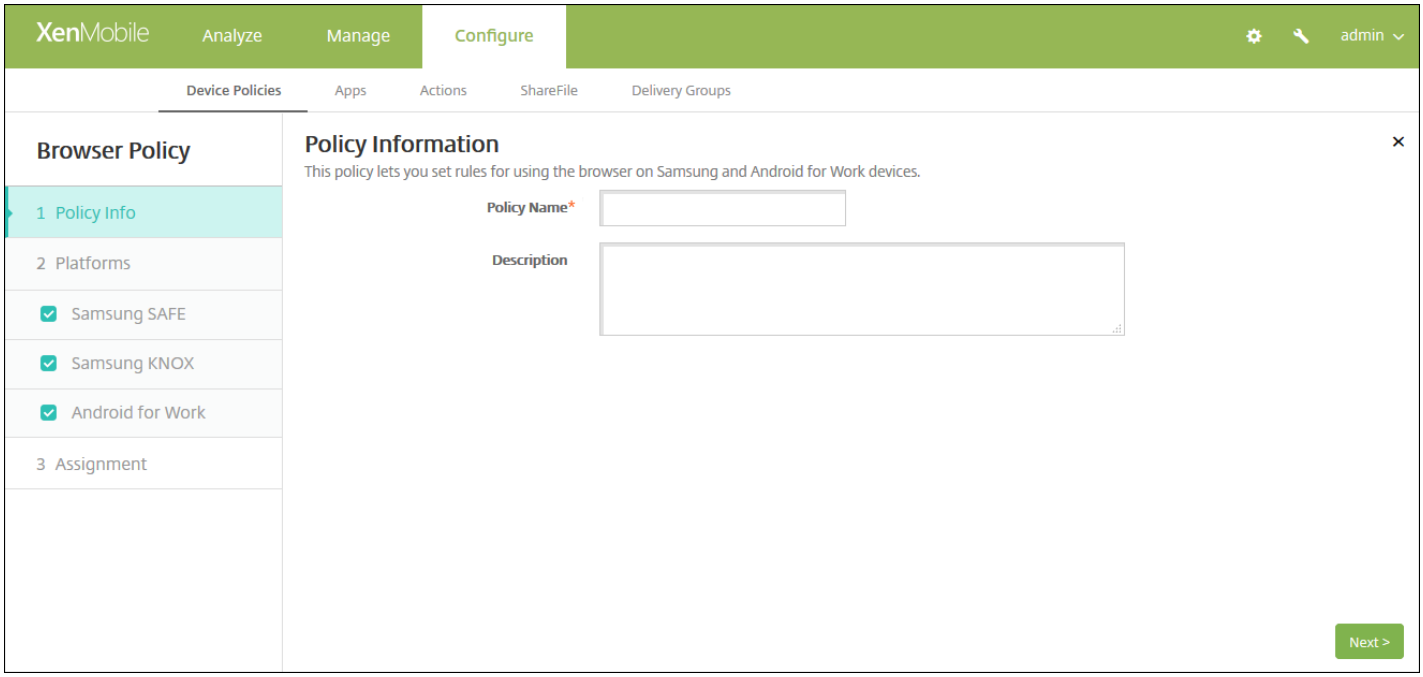


-
  -
  -
  -

8. Configurez les règles de déploiement.

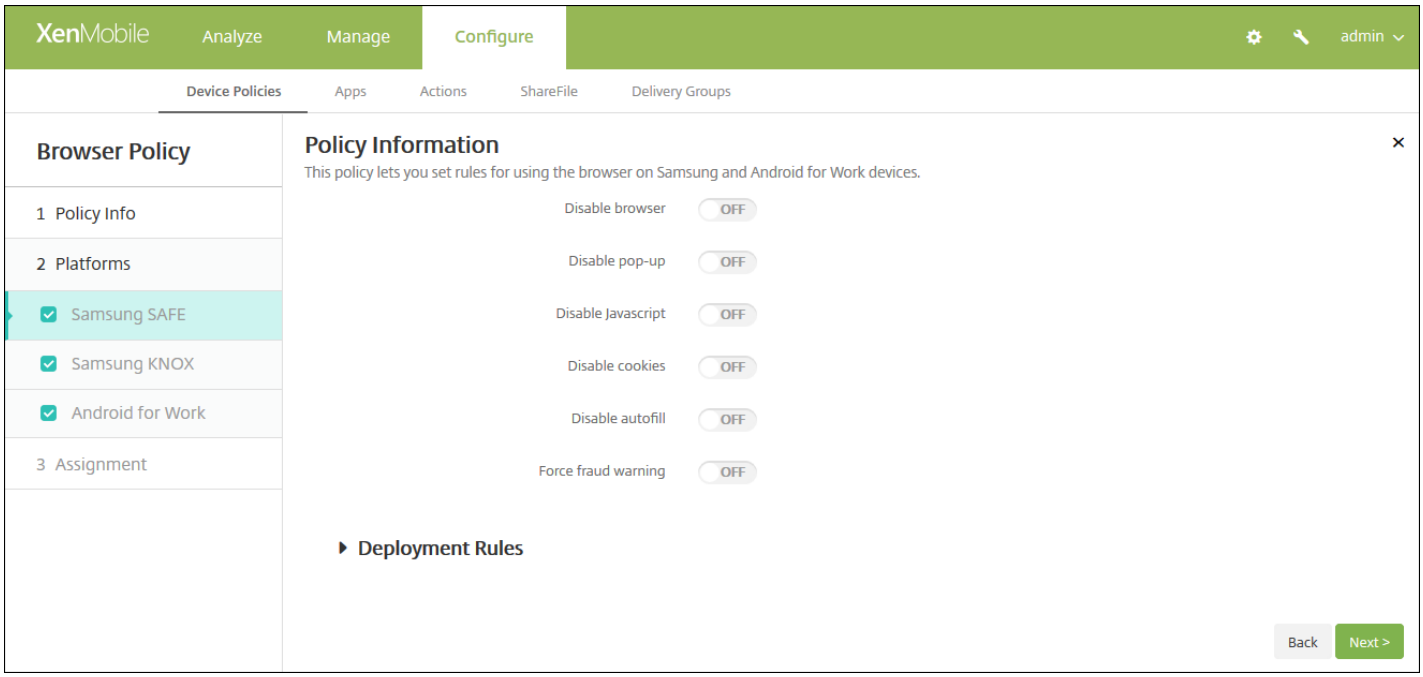


-
-
-
-
-
-
-



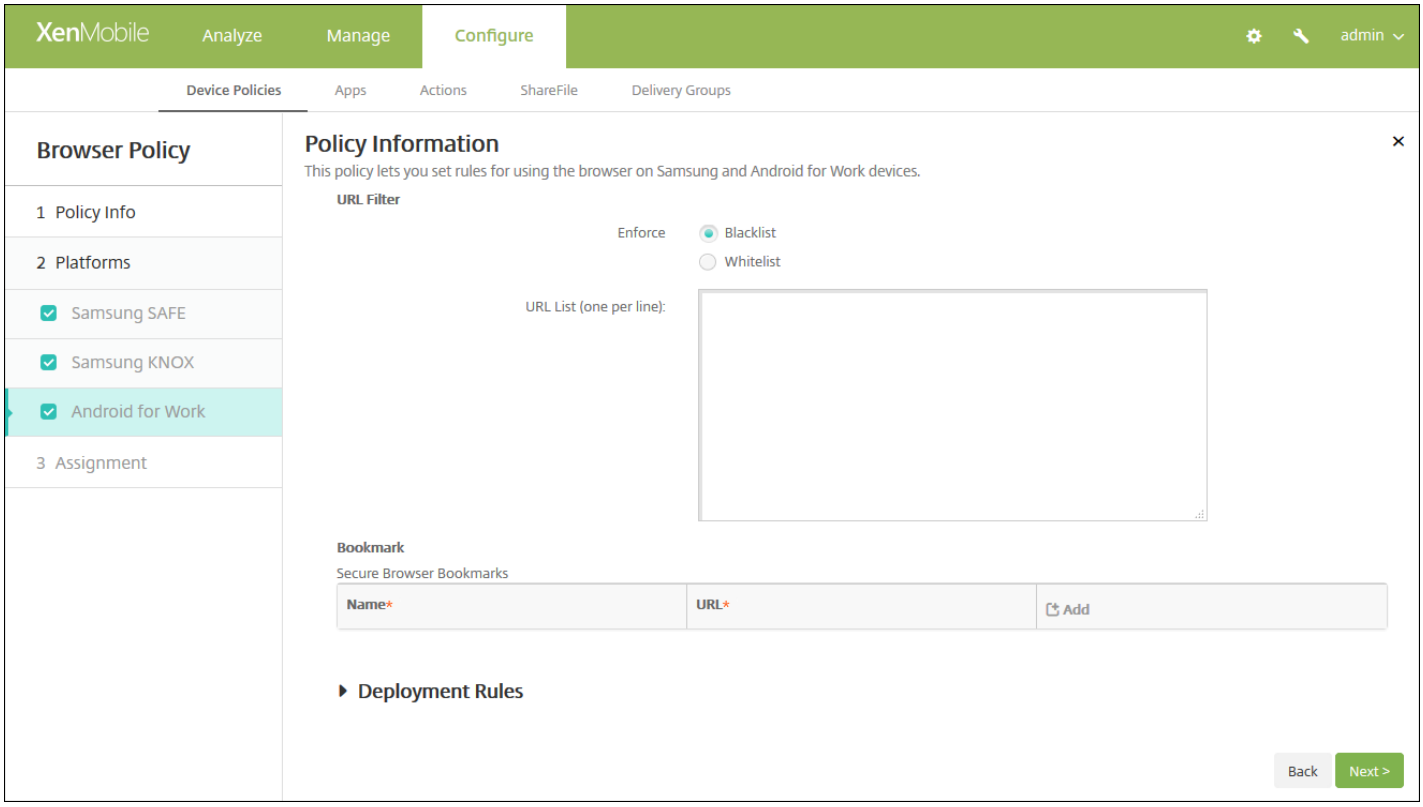
-
-

Configurer les paramètres Samsung SAFE et Samsung KNOX



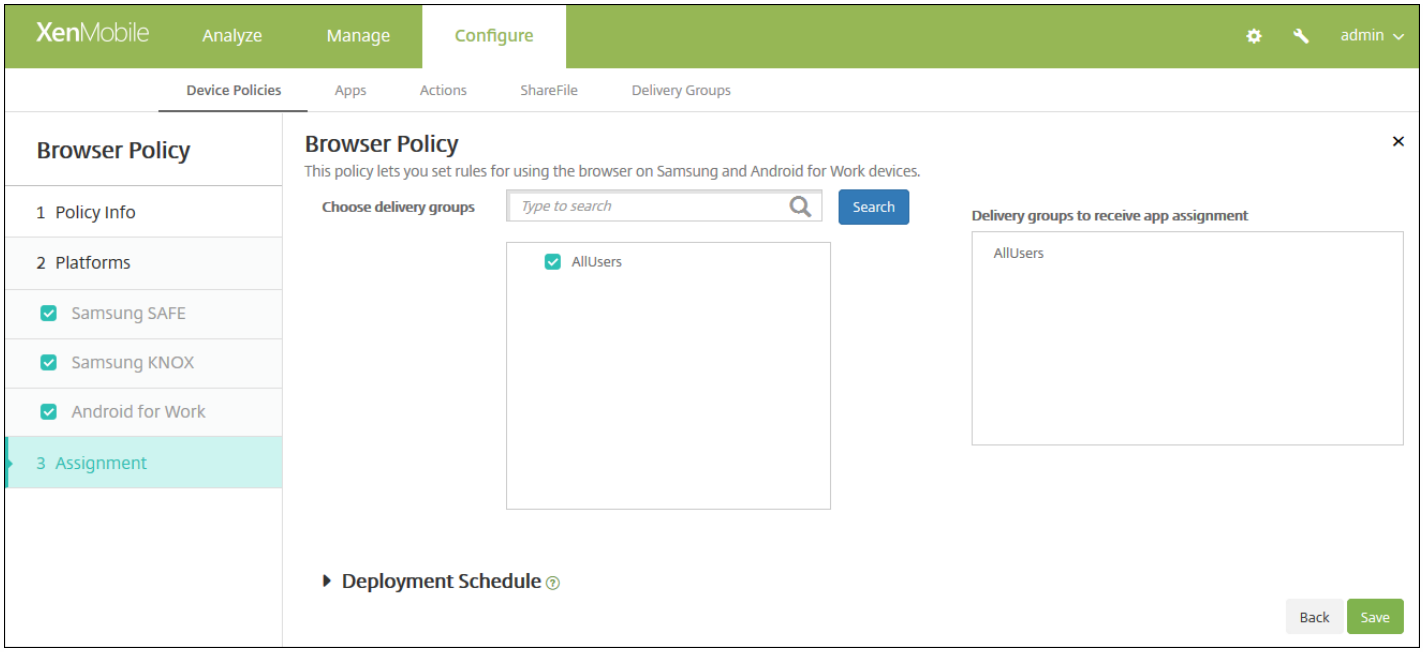
-
-
-
-
-
-

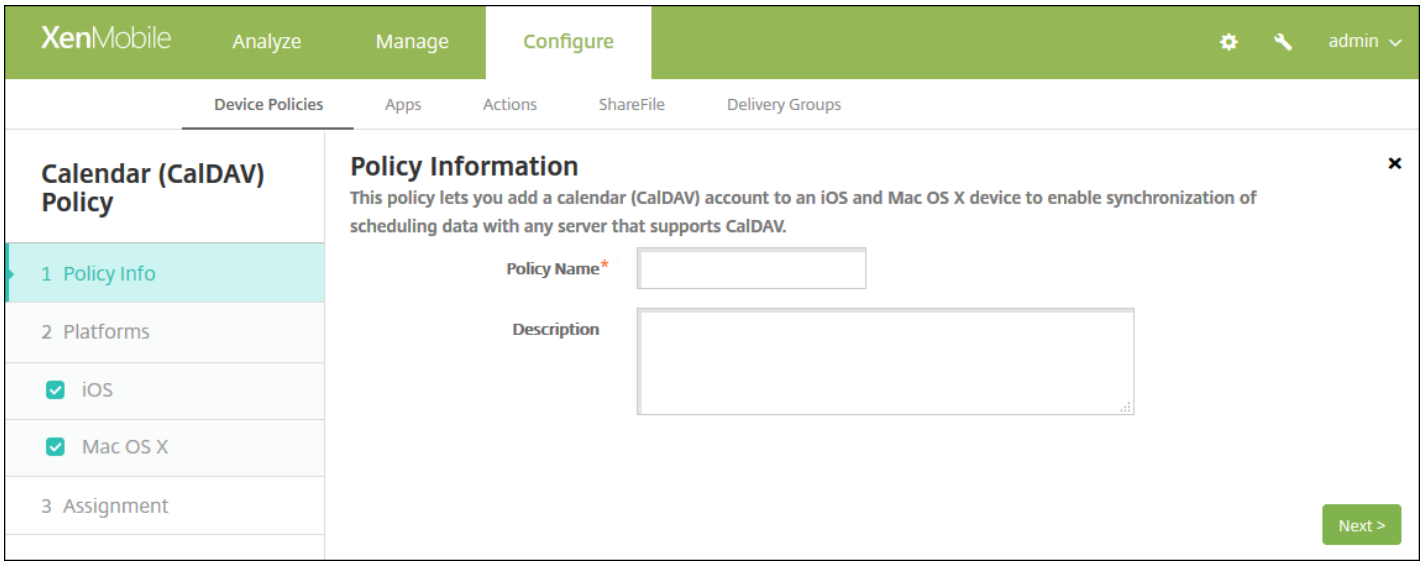
Configurer les paramètres Amazon pour Work



-
  -
  -
-

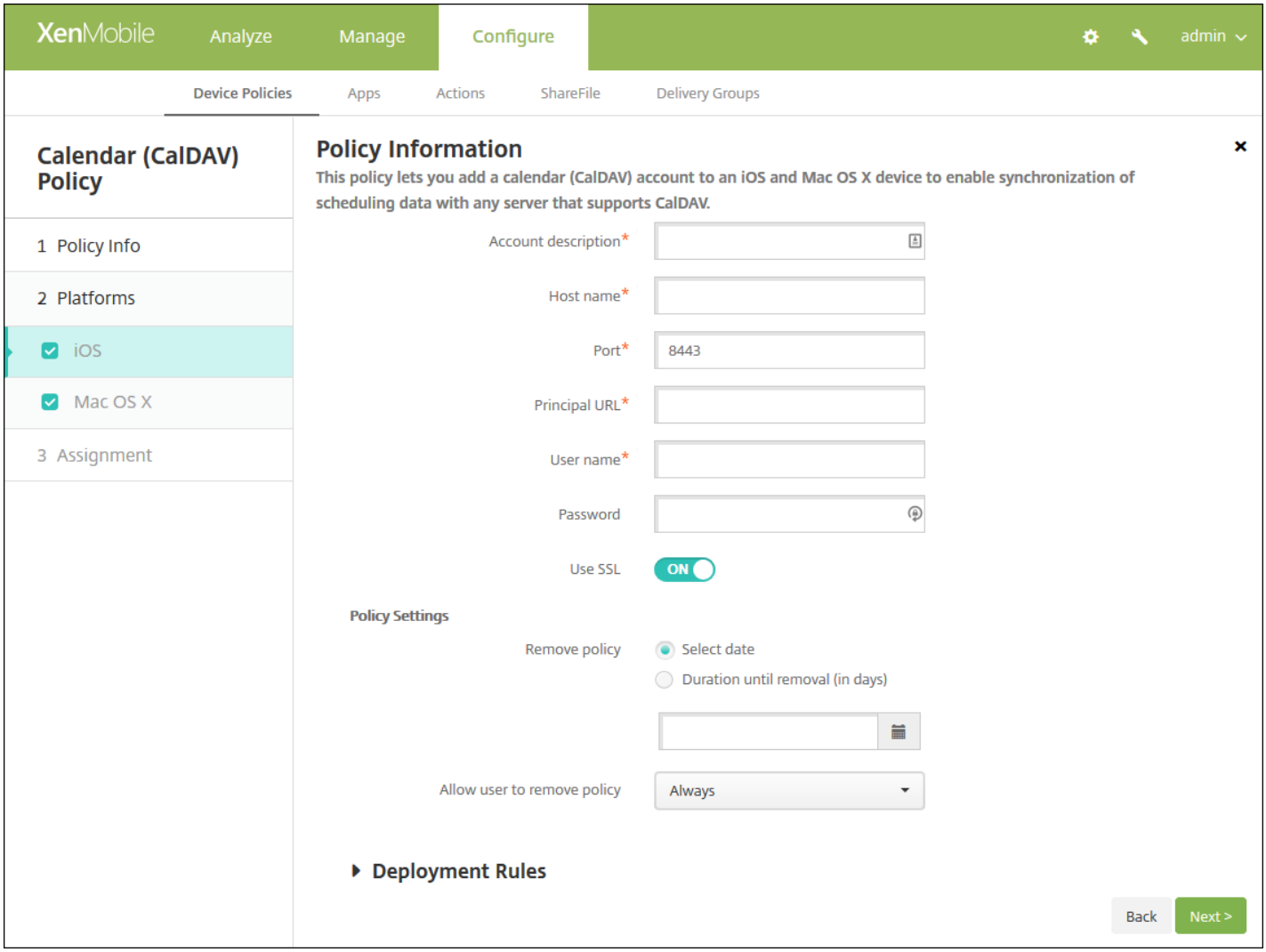
7. Configurez les règles de déploiement.





-
-

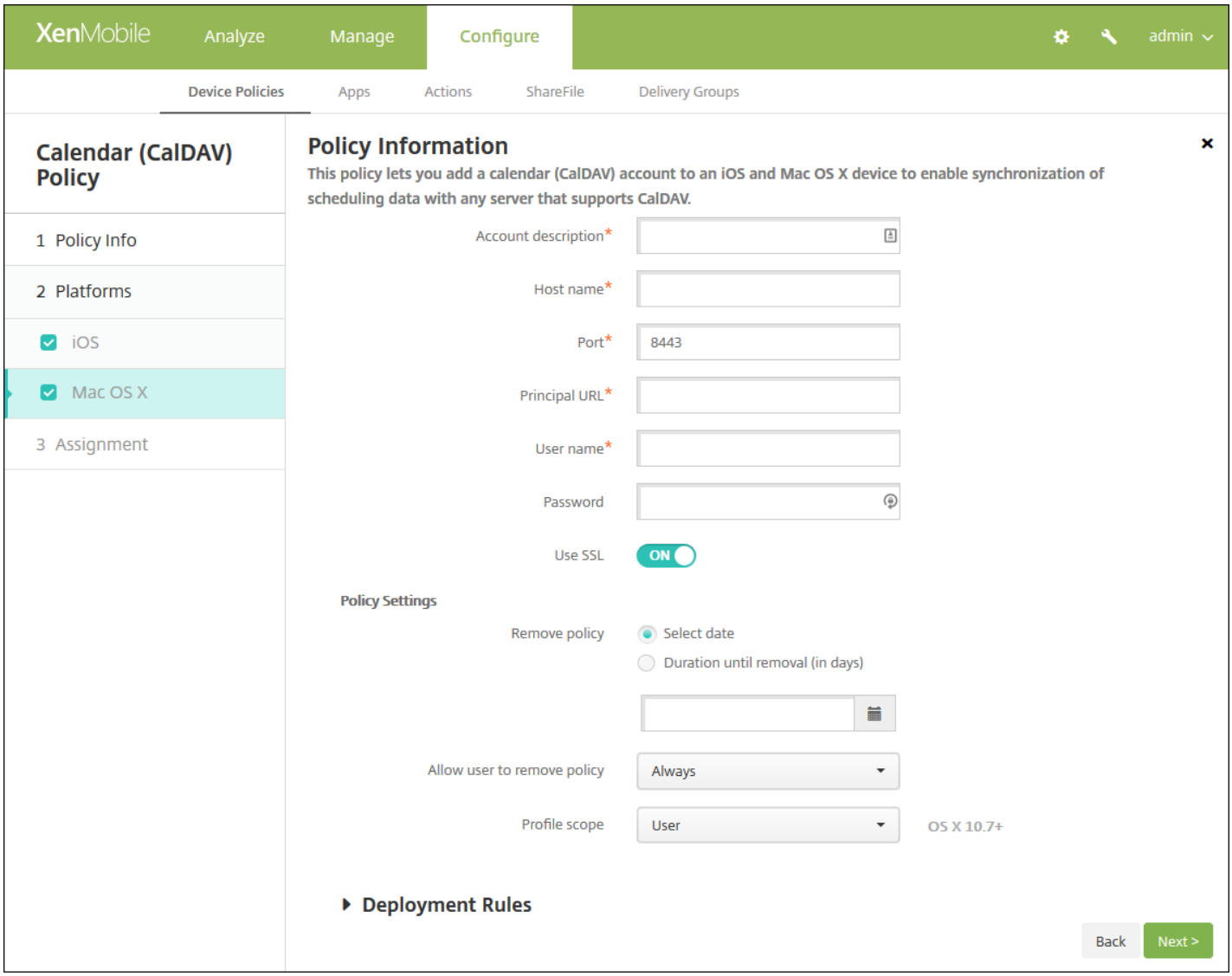
Configurer les paramètres pour iOS



-
-
-
-
-
-
-
-
  -
  -
  -

-

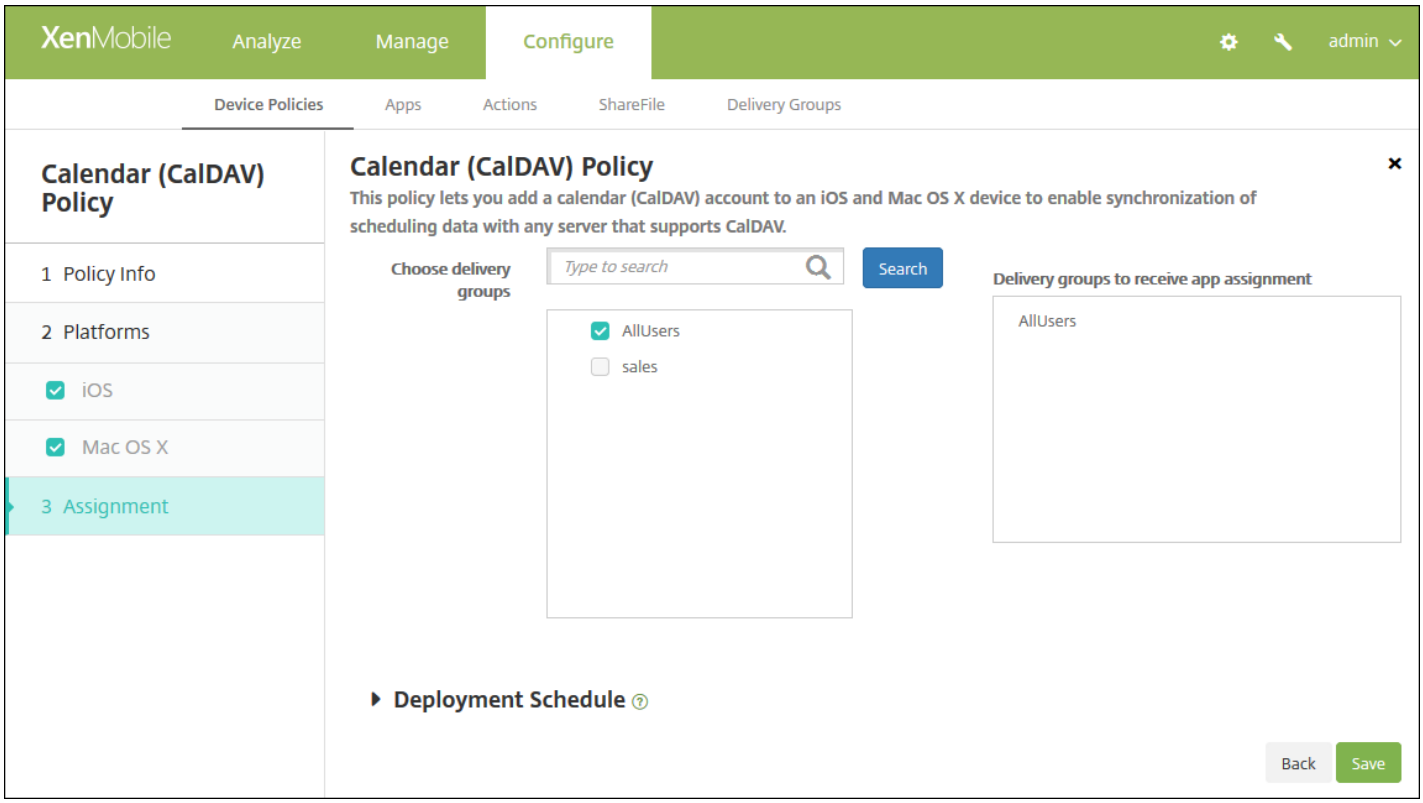
Configurer les paramètres pour Mac OS X



-
-
-
-
-
-
-
-

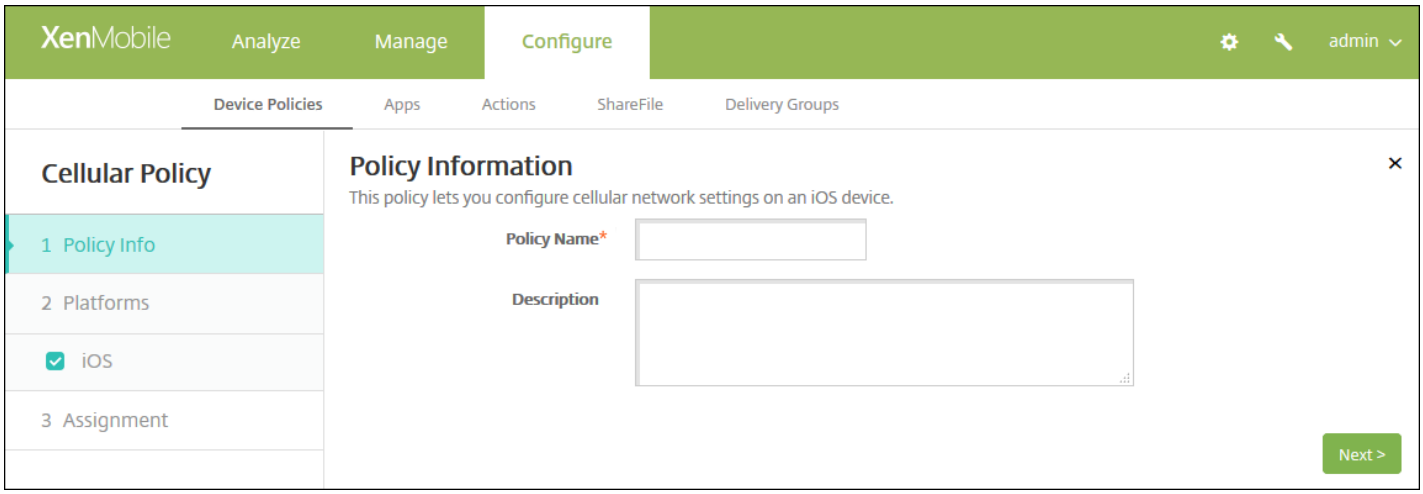
-
-
-
-

7. Configurez les règles de déploiement.

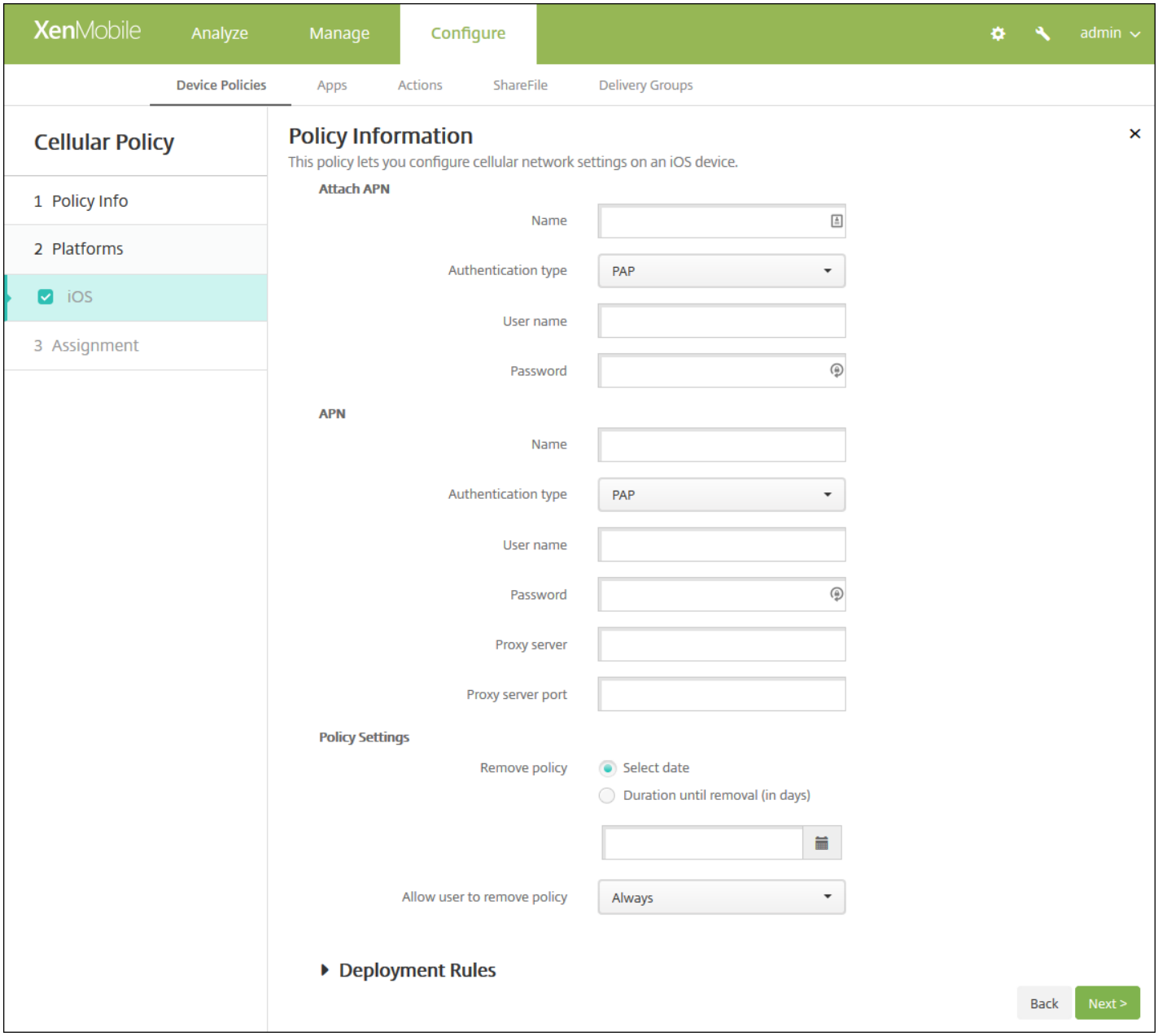


-
-

-
-
-
-
-



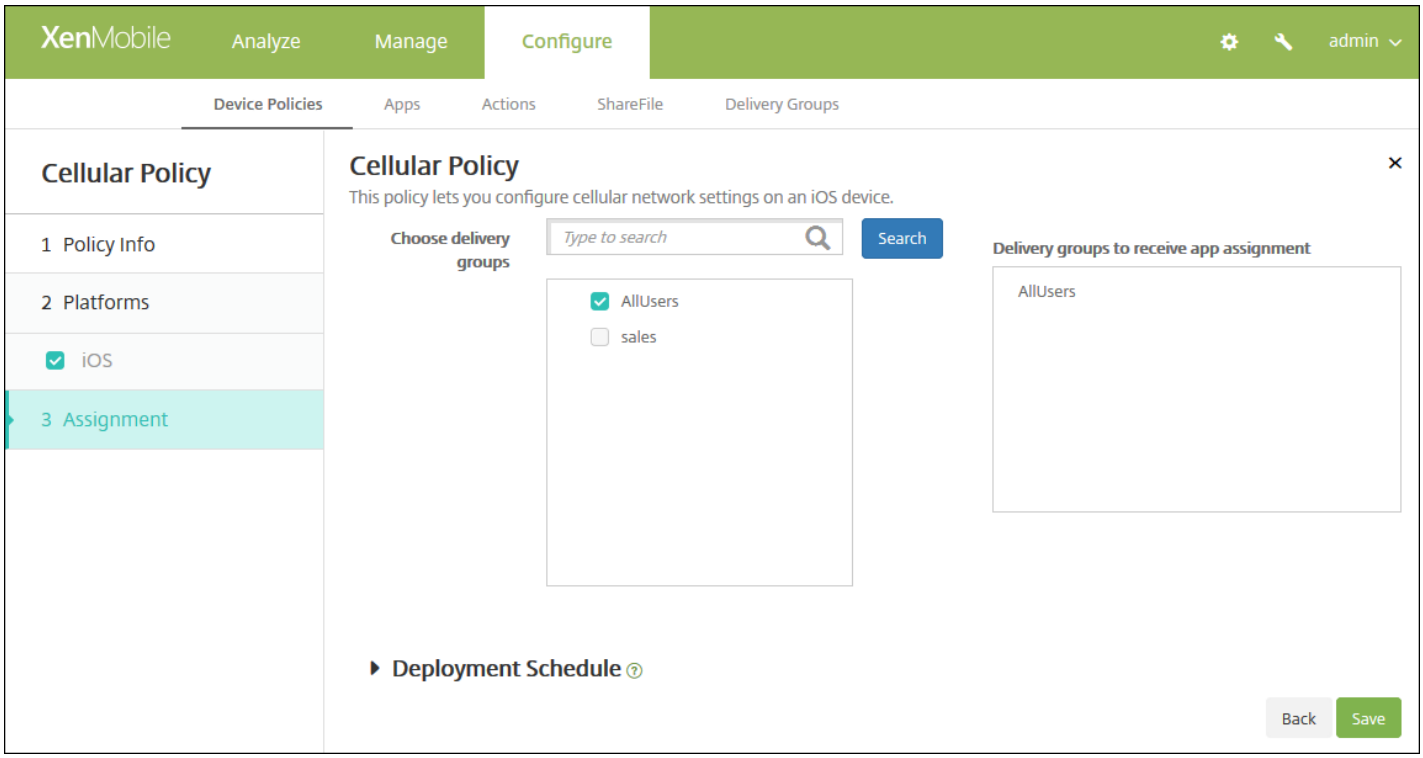
-
-



-
  -
  -
  -
-
  -
  -
  -
  -
  -

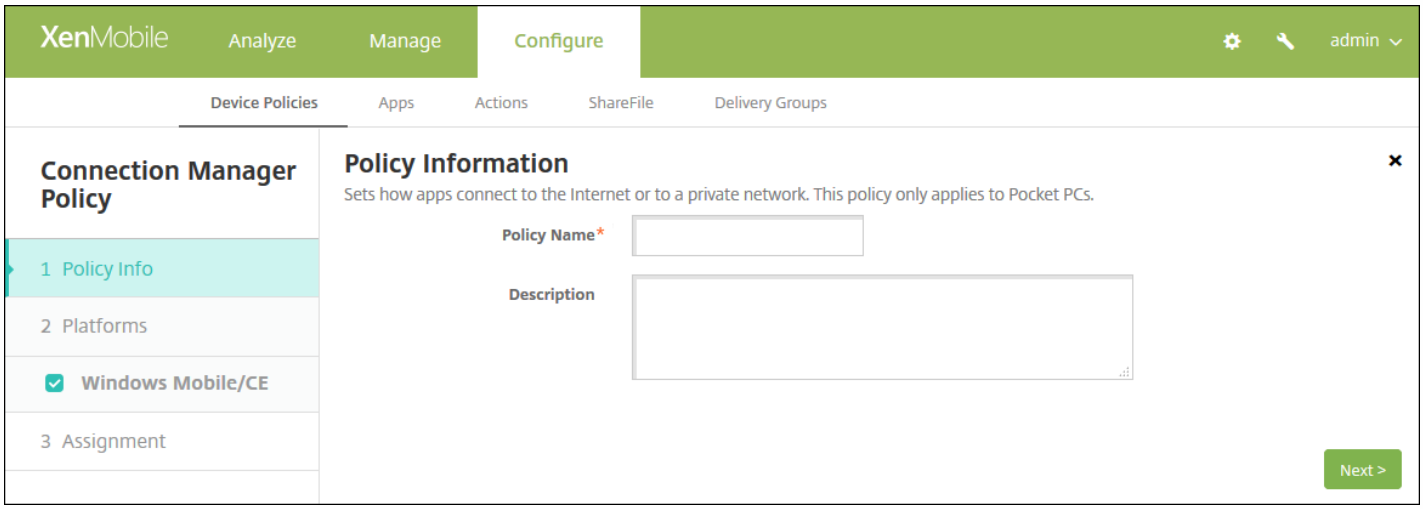
-
  -
  -
  -
  -

7. Configurez les règles de déploiement.

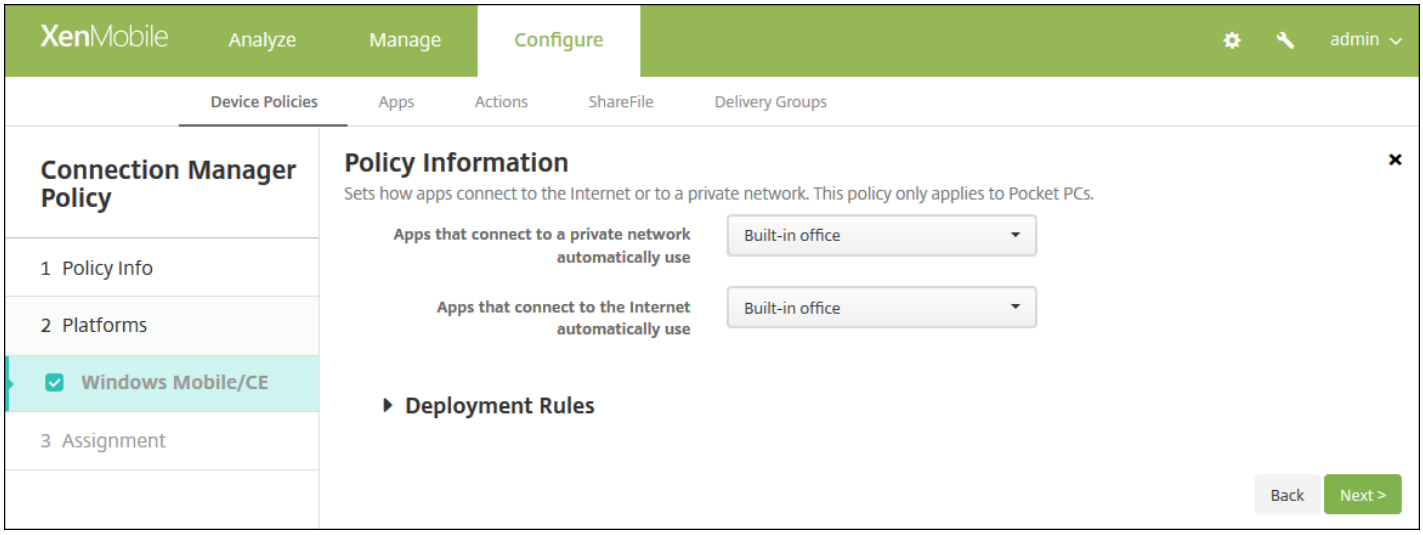


-
-
-

-
-
-
-

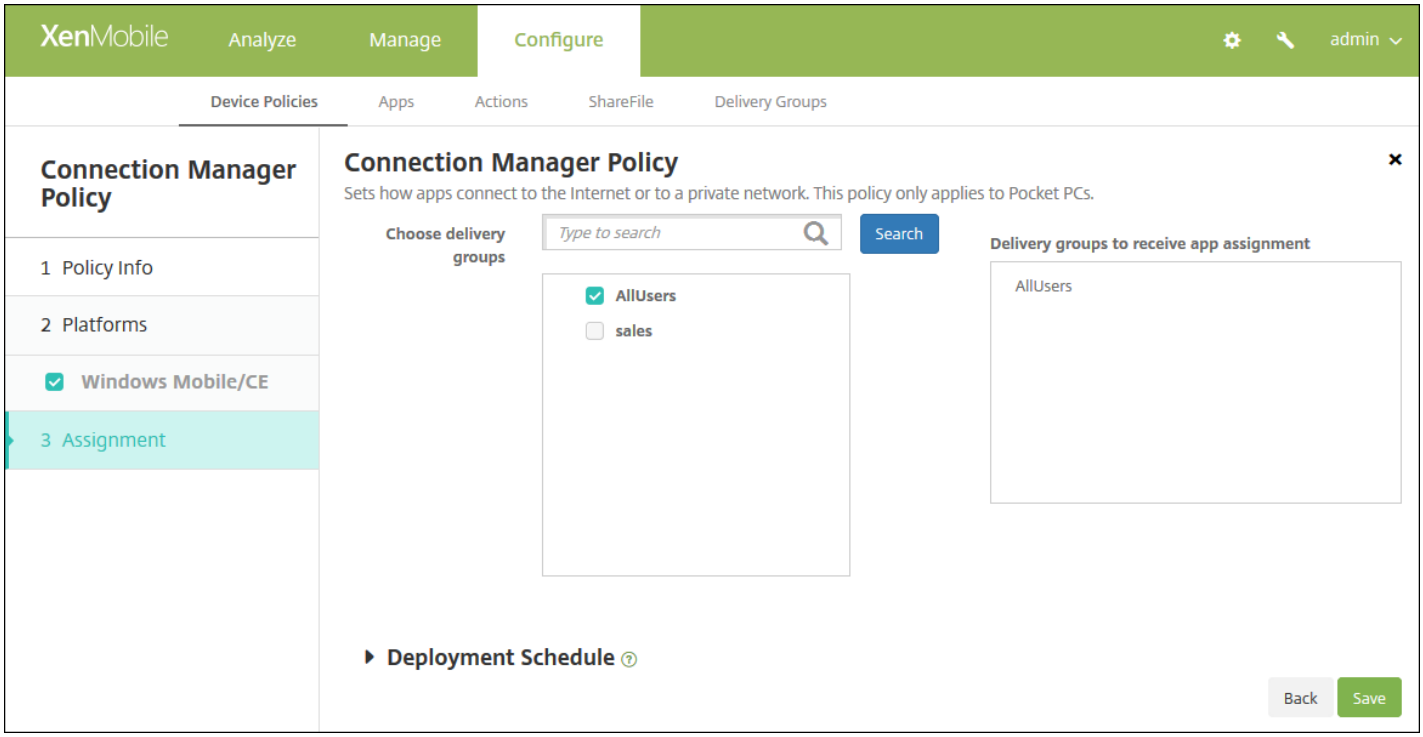


-
-

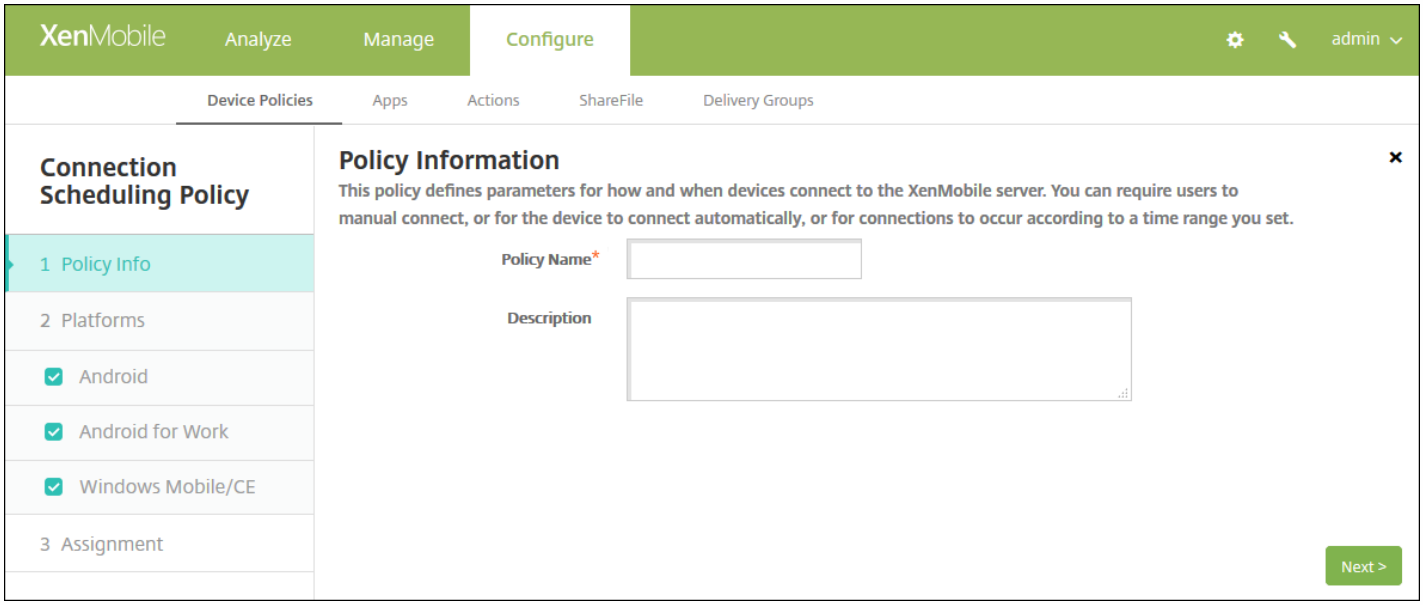


-
-

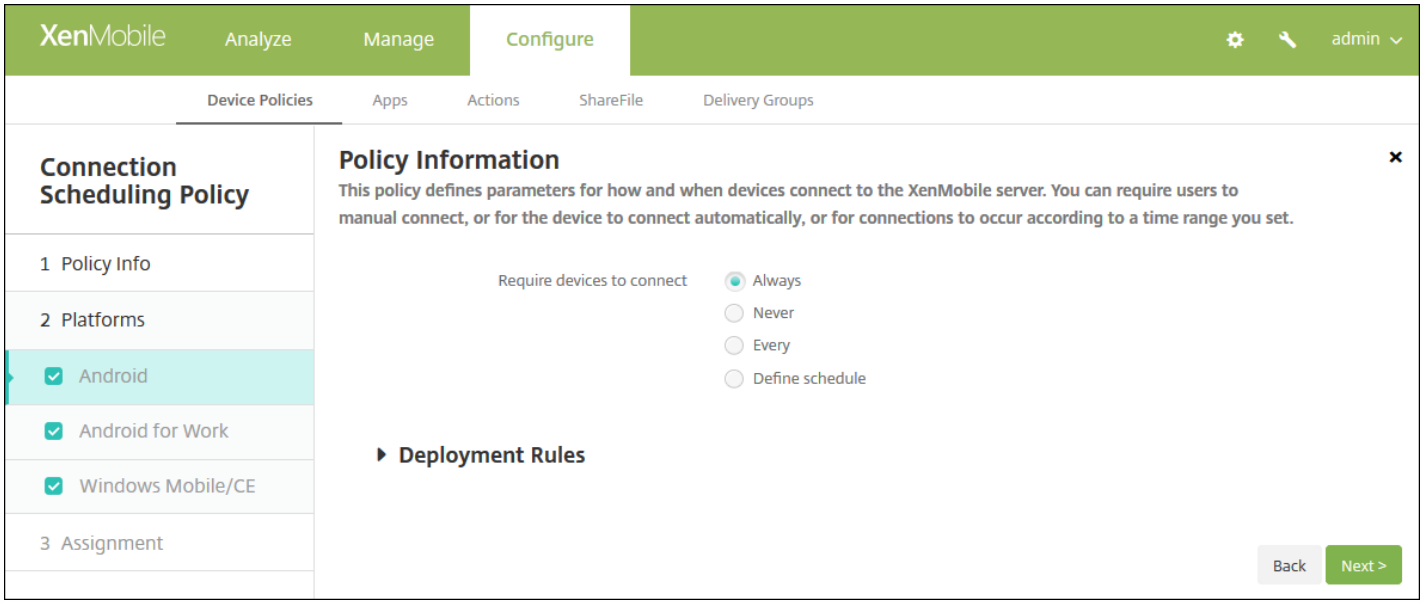
7. Configurez les règles de déploiement.



-
-
-
-
-
-
-

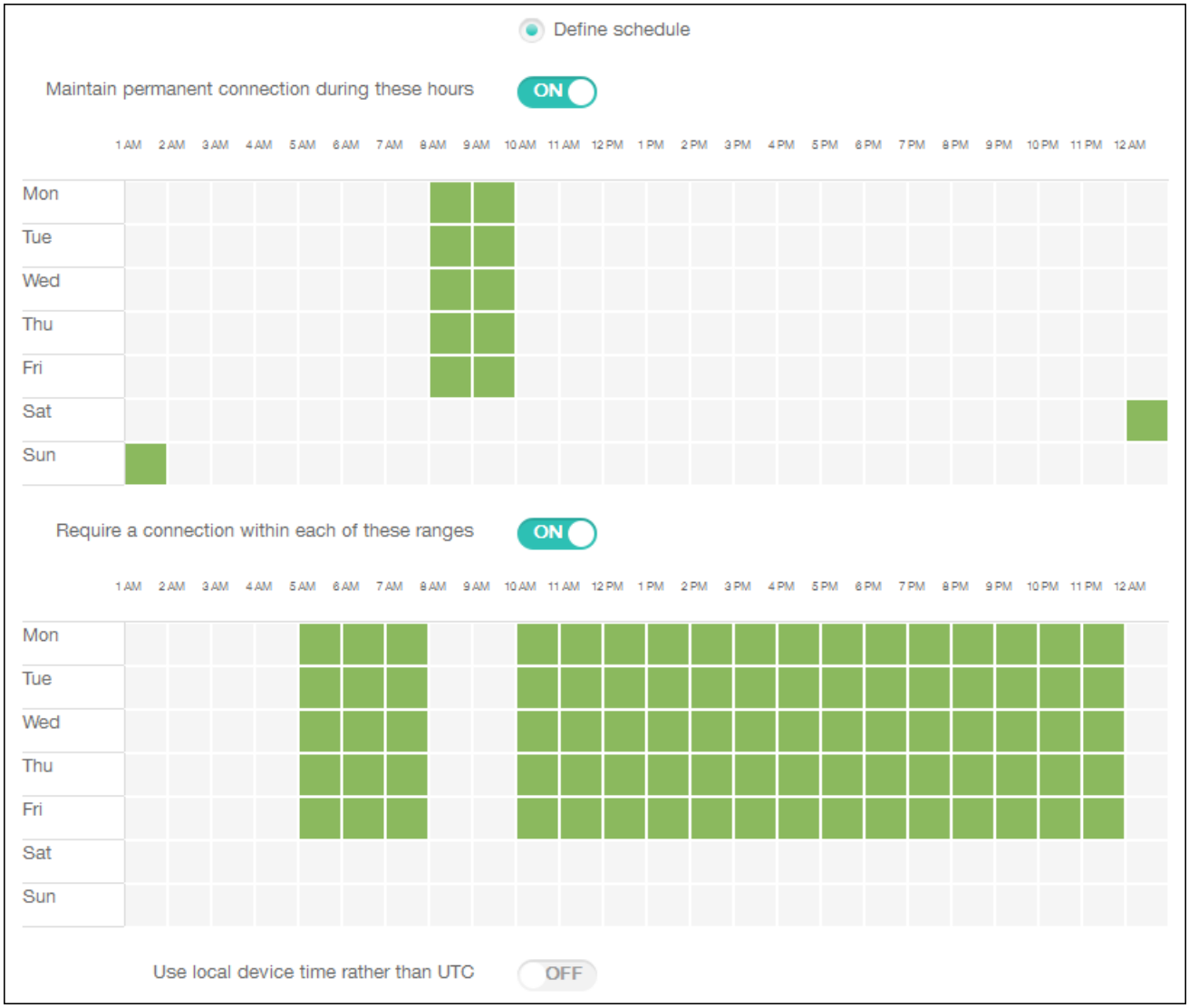


-
-

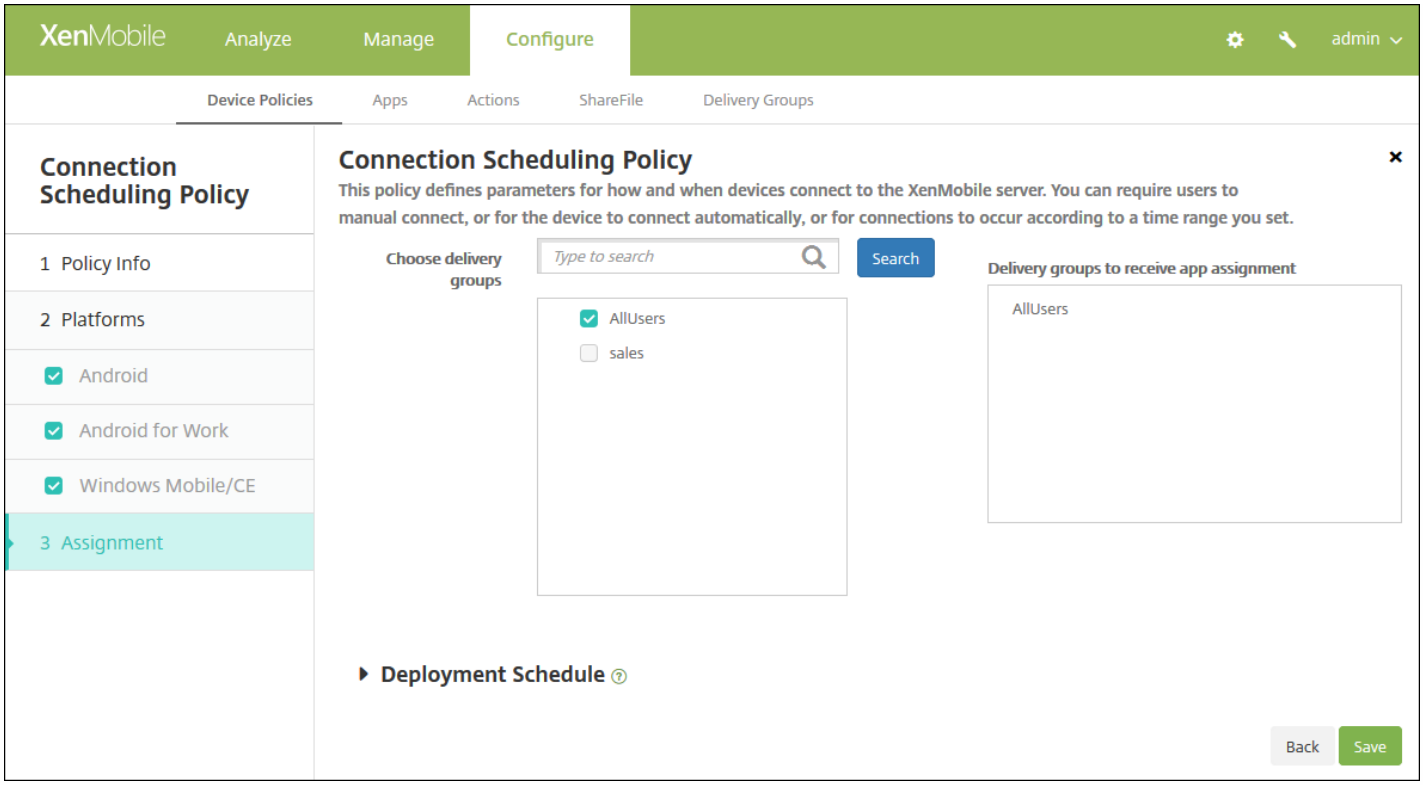


-
  -
  -
  -
  -

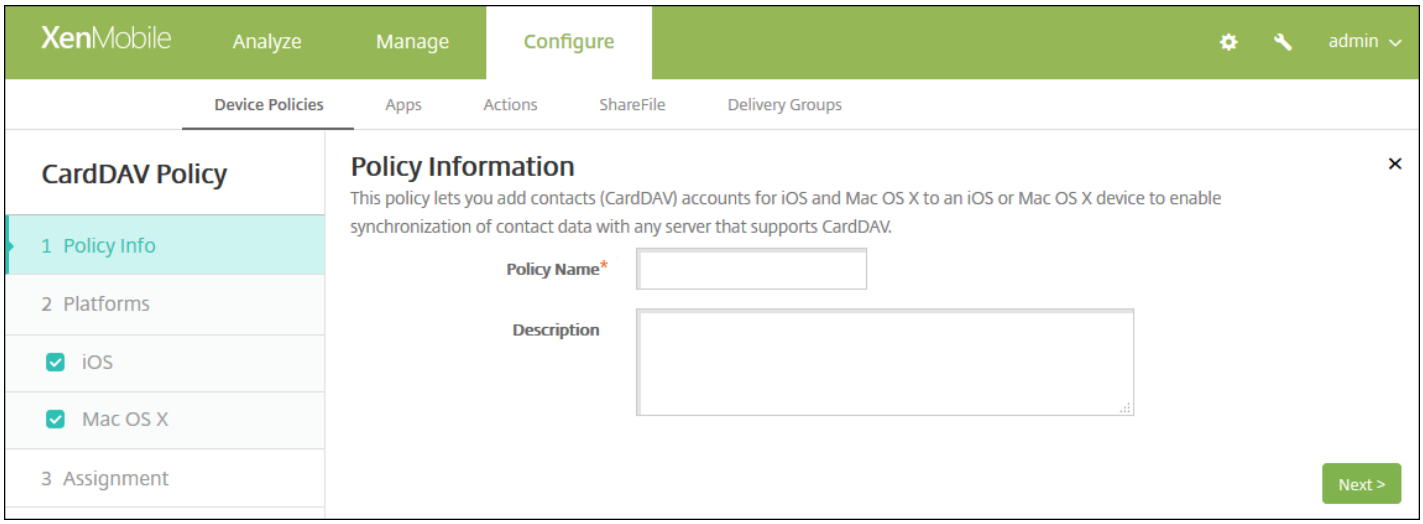
-
-
-



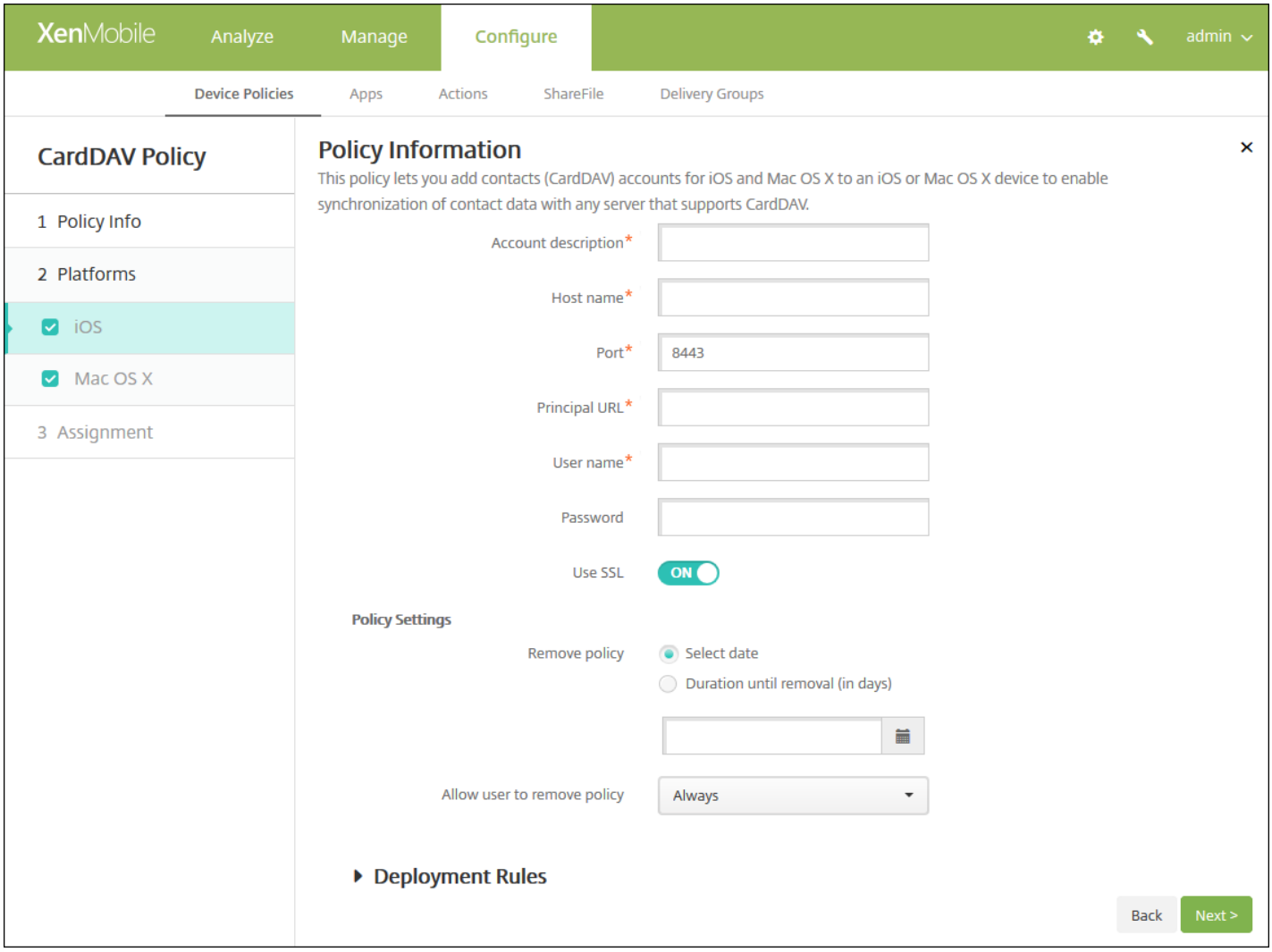
8. Configurez les règles de déploiement.



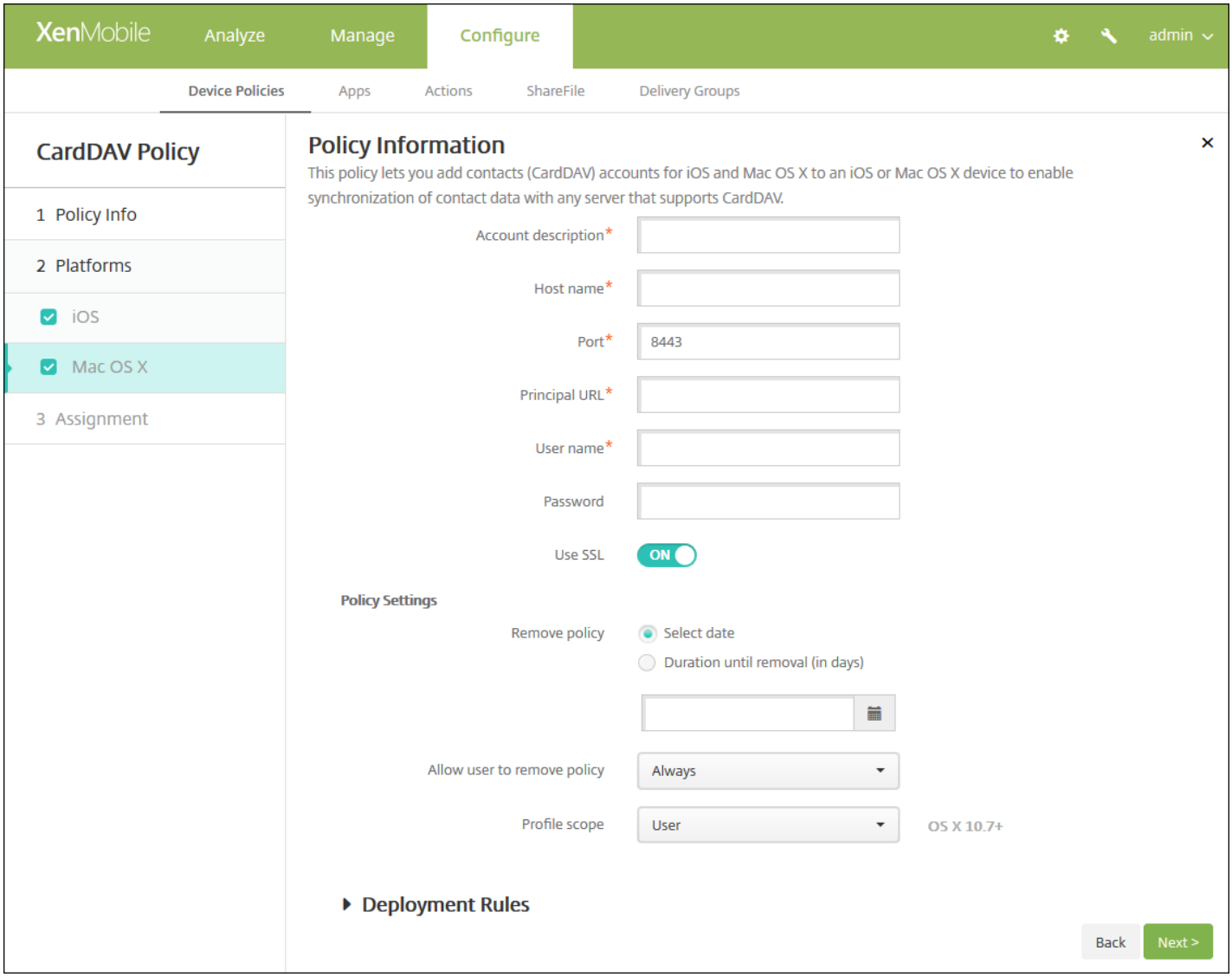
-
-
-
-
-
-
-



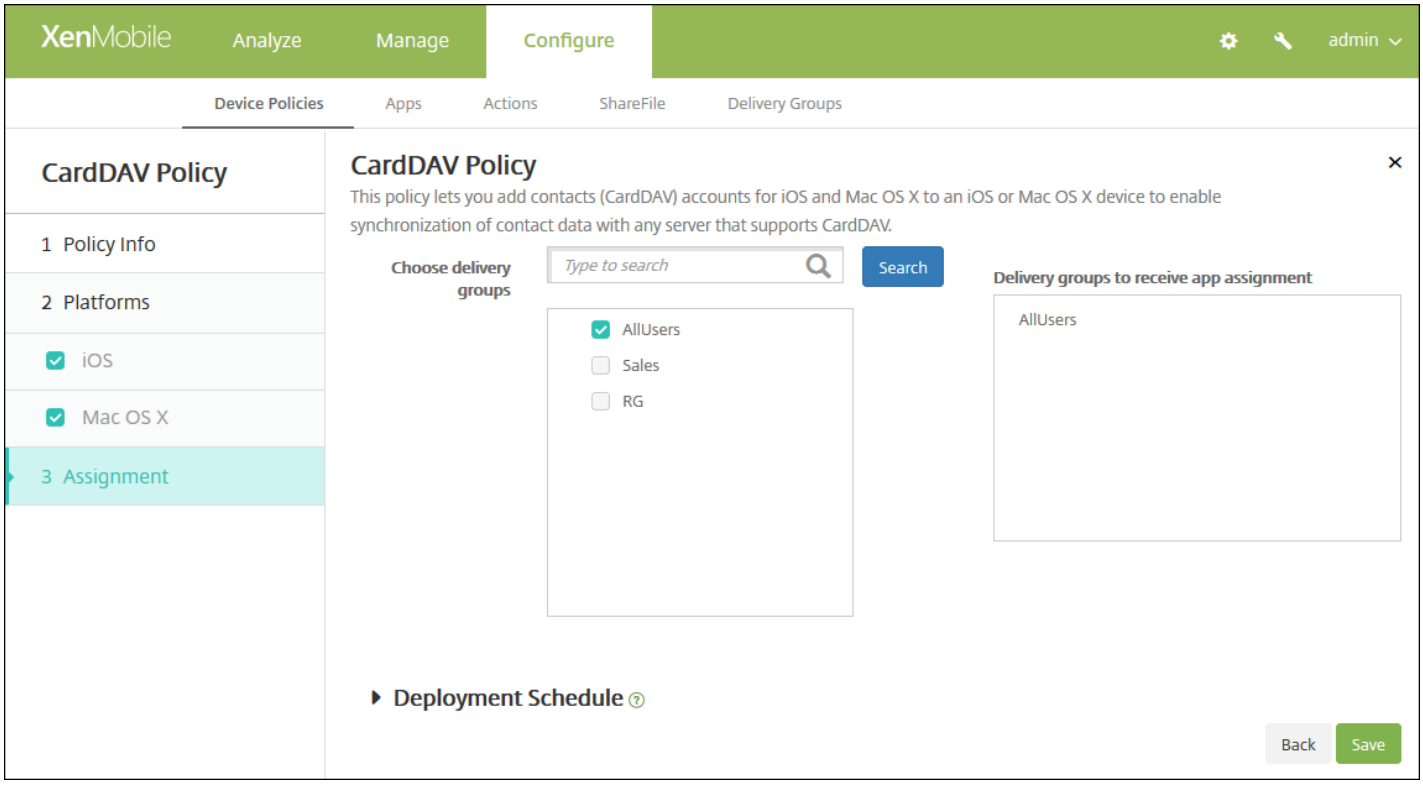
-
-



-
-
-
-
-
-
-
-
  -
  -
  -
  -

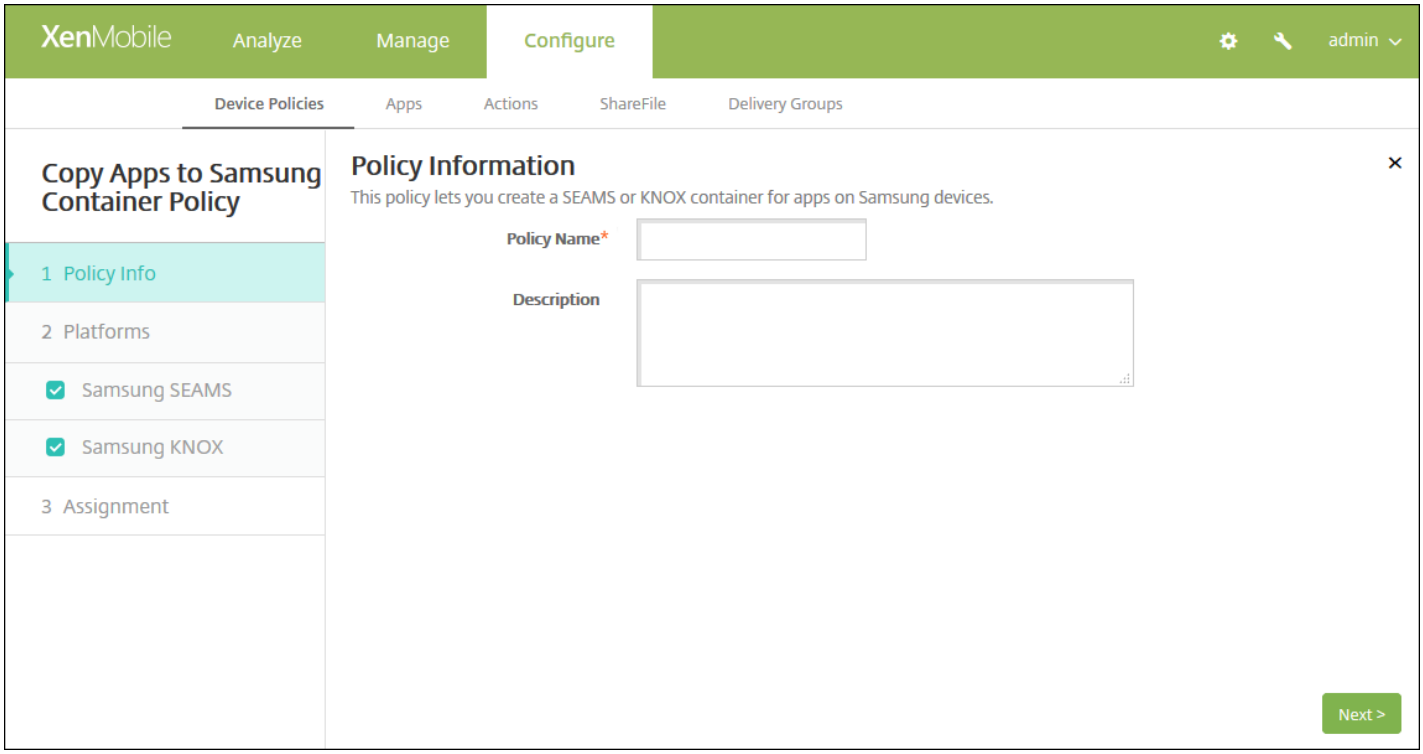


-
-
-
-
-
-
-
-
-

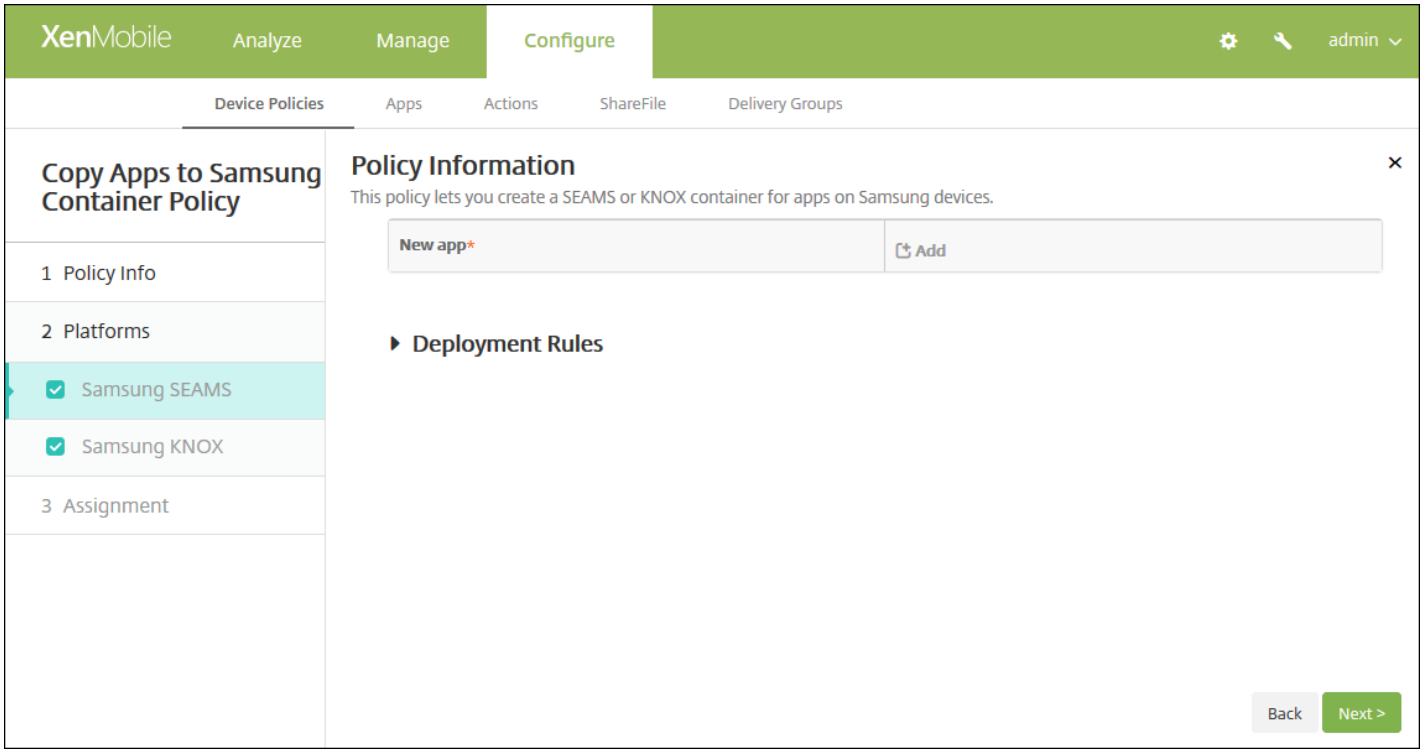


-
-
-
-

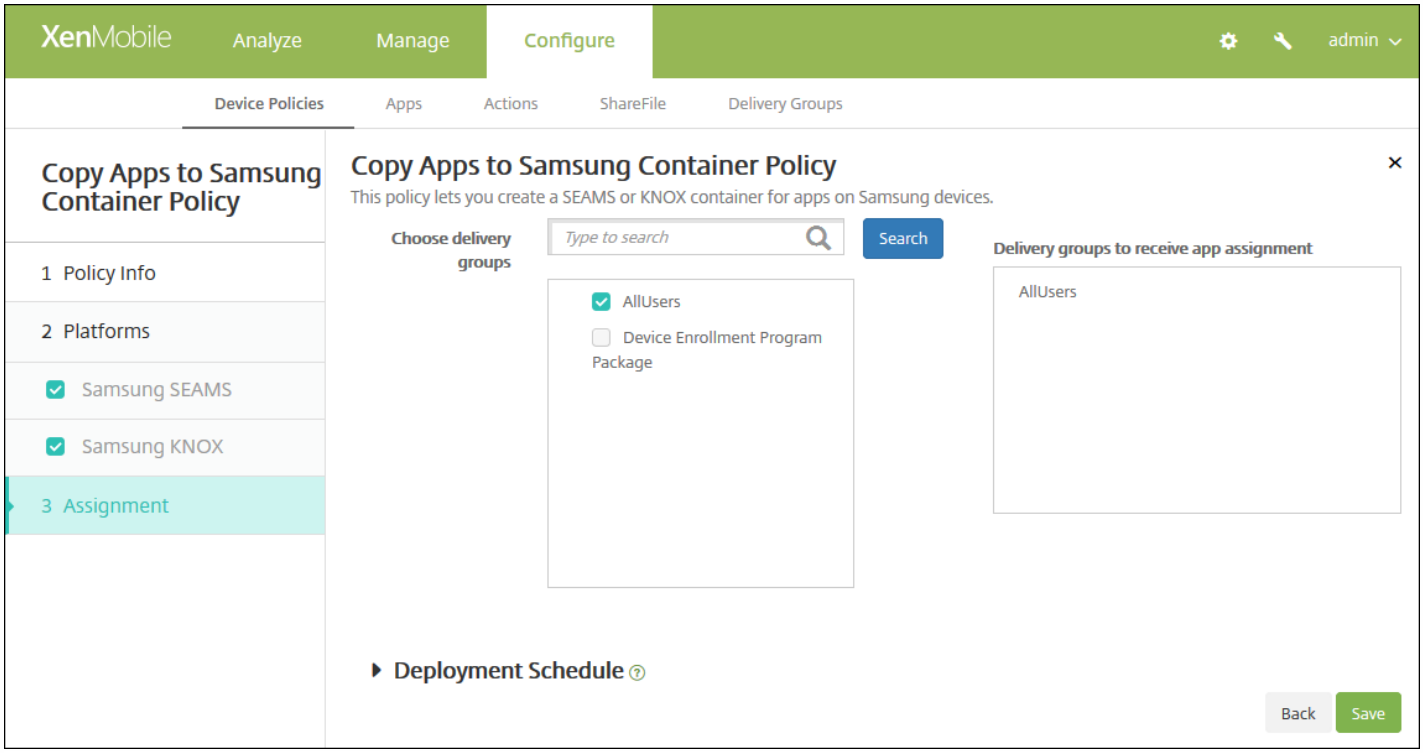
-
-
-
-



-
-

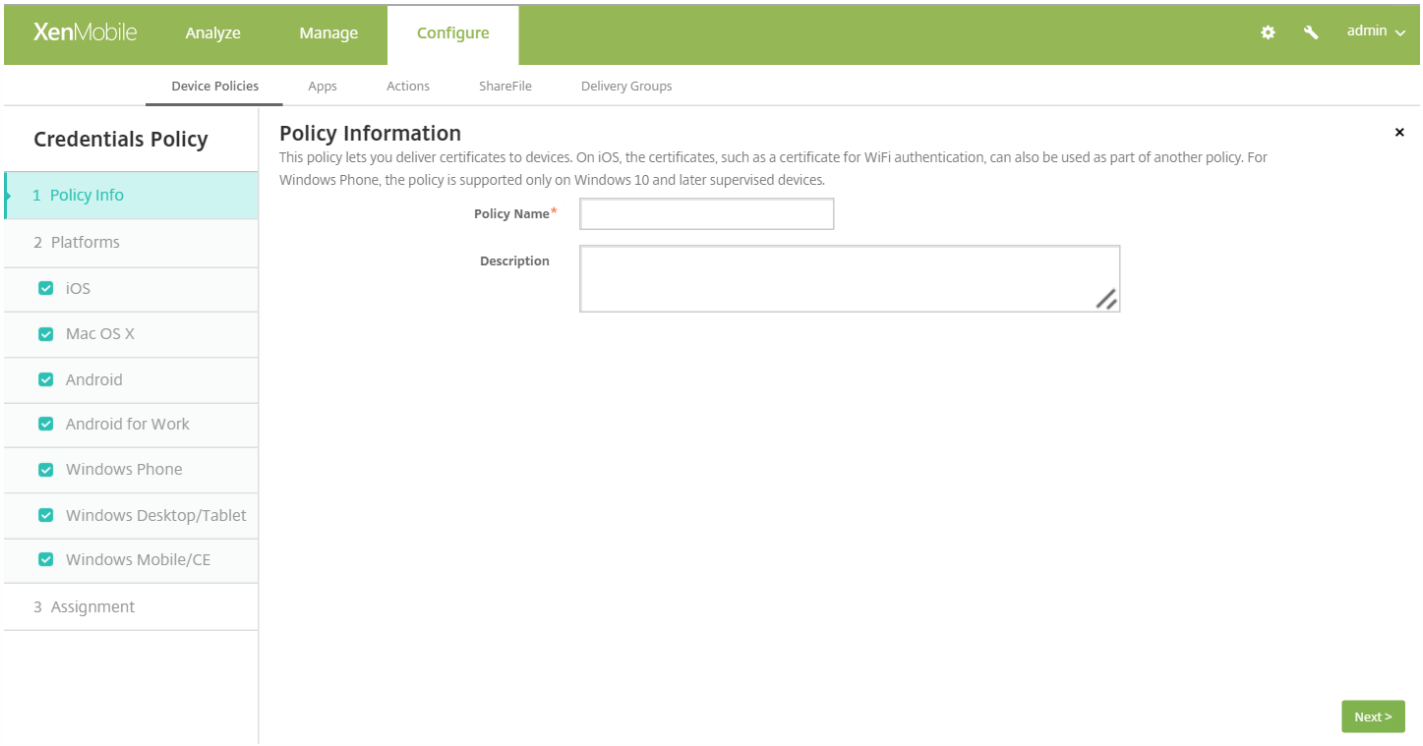


-
  -
  -

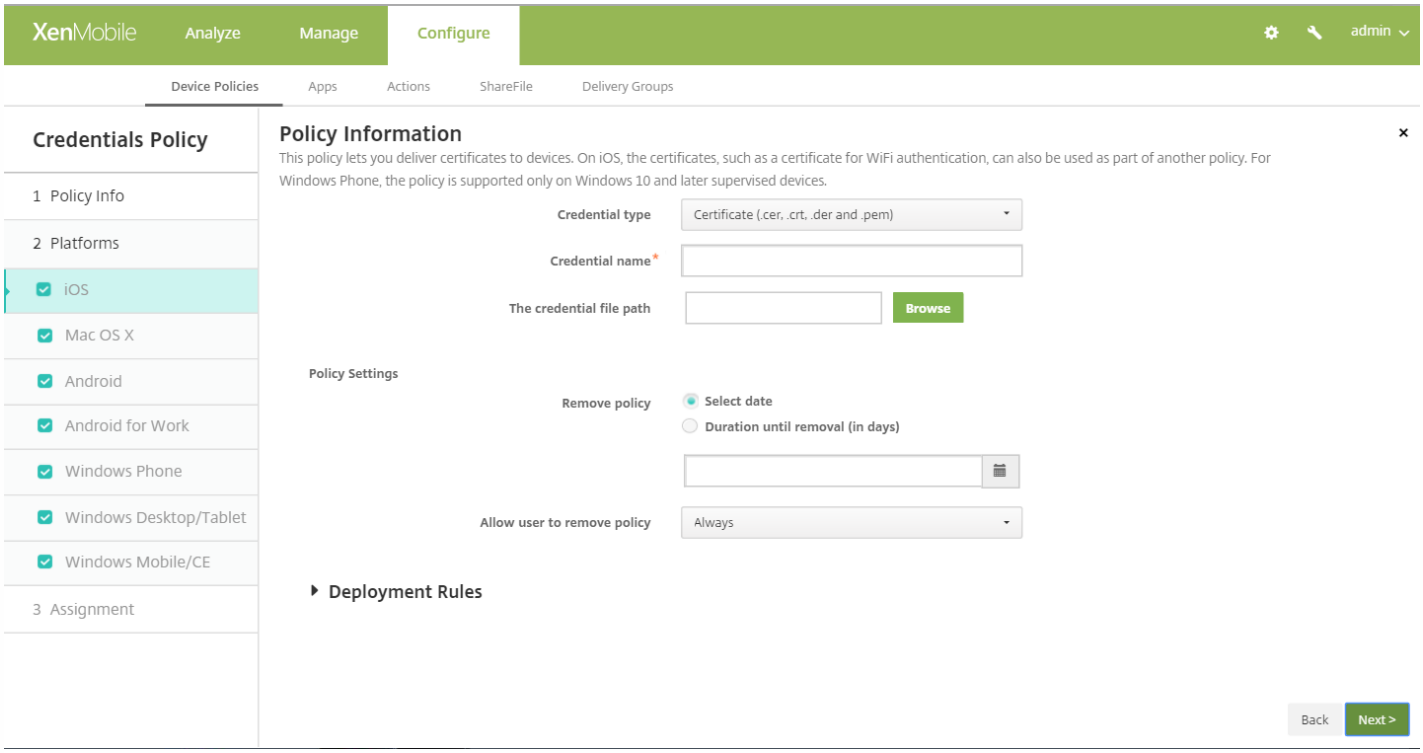


-
-
-
-
-
-

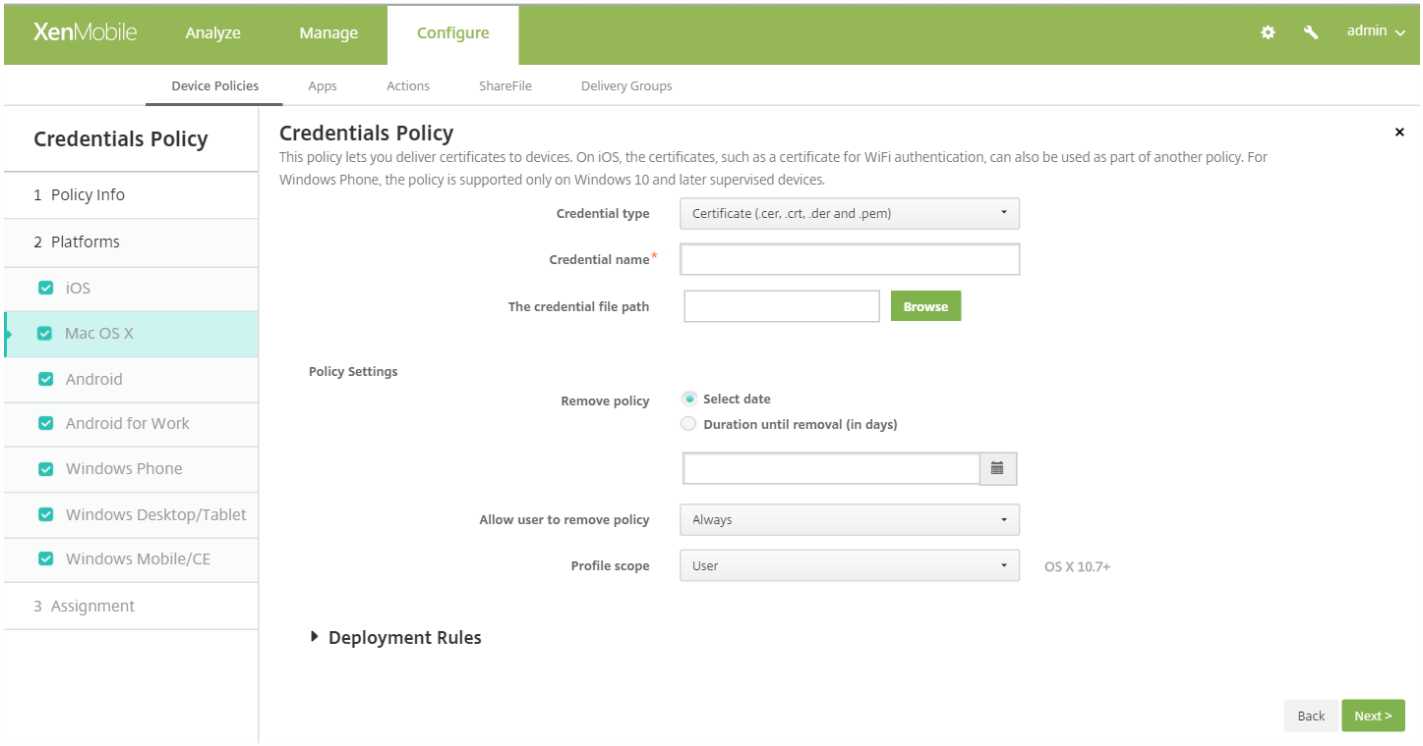
-



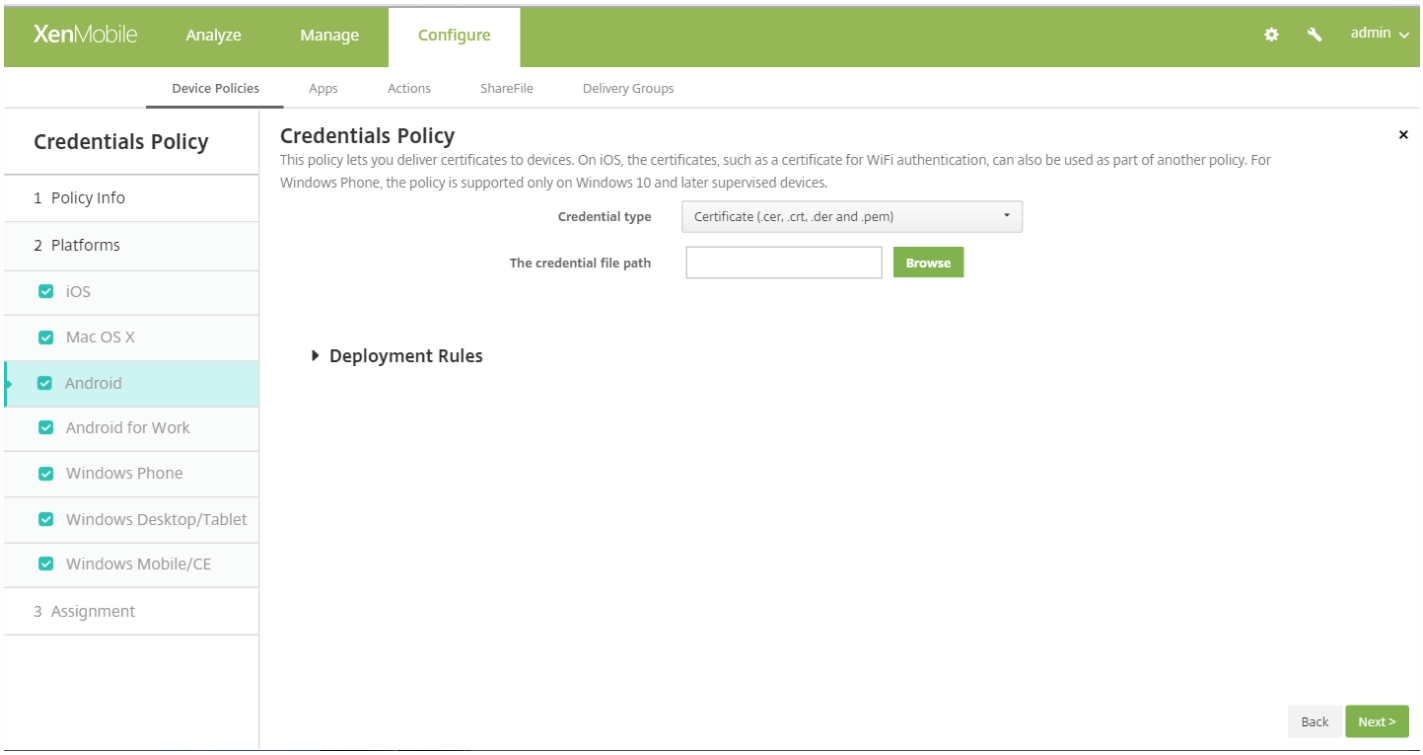
-
-

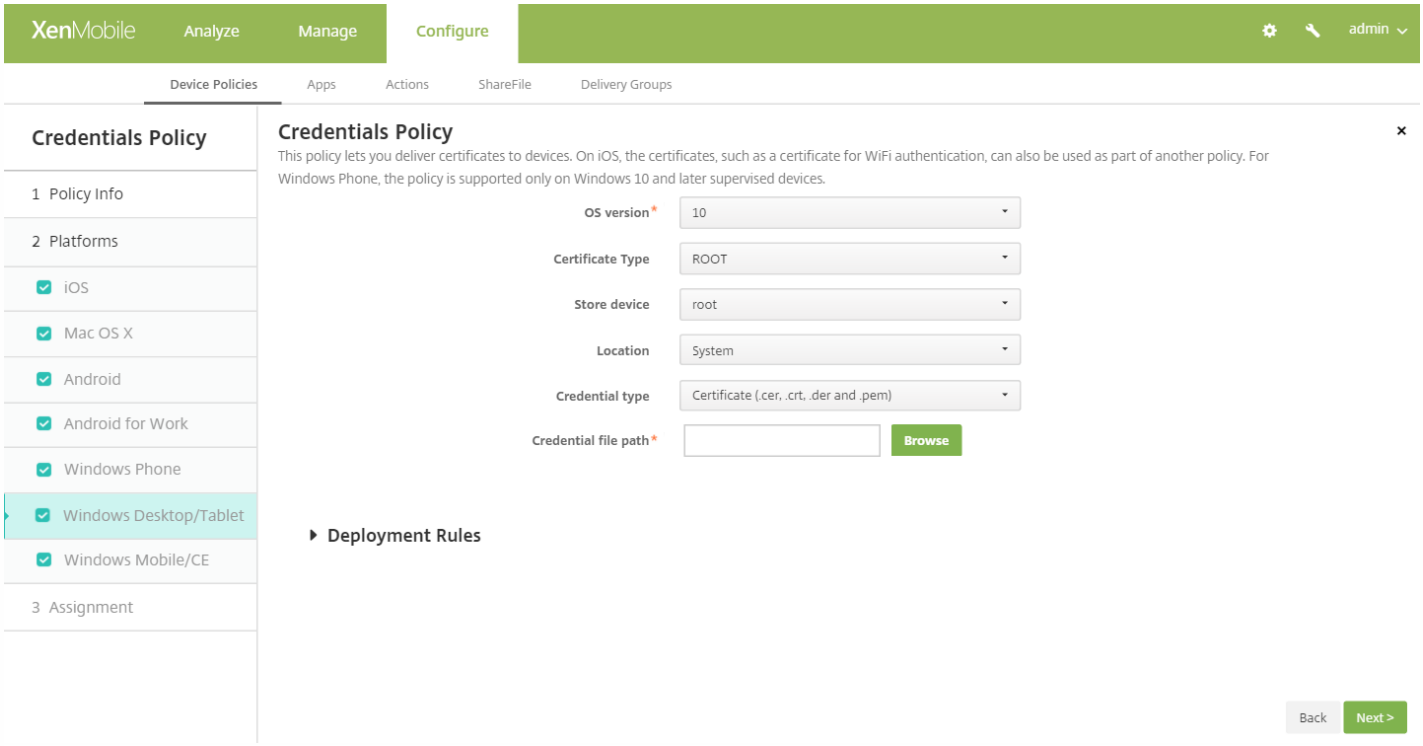


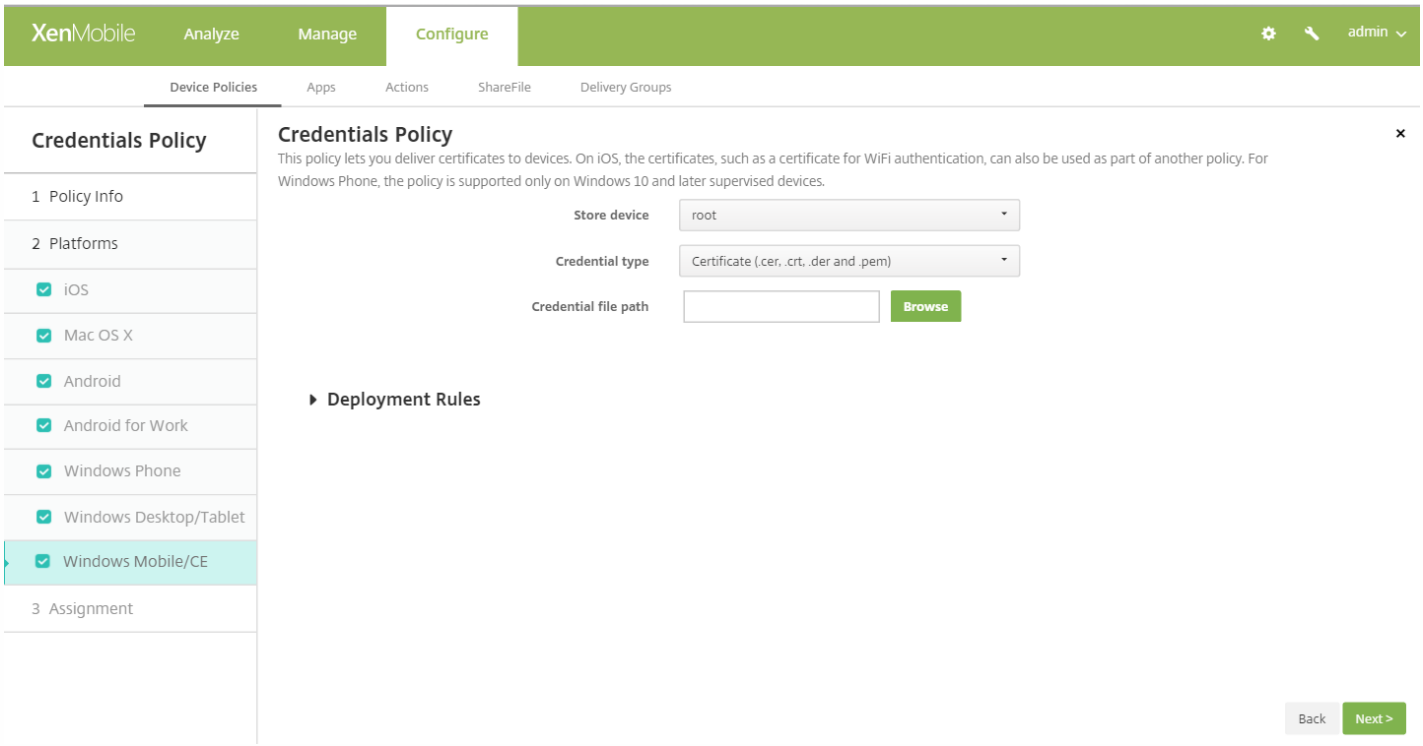
-
  -
    -
    -
  -
    -
    -
    -
  -
    -
  -
    -
-
  -
  -
  -
  -



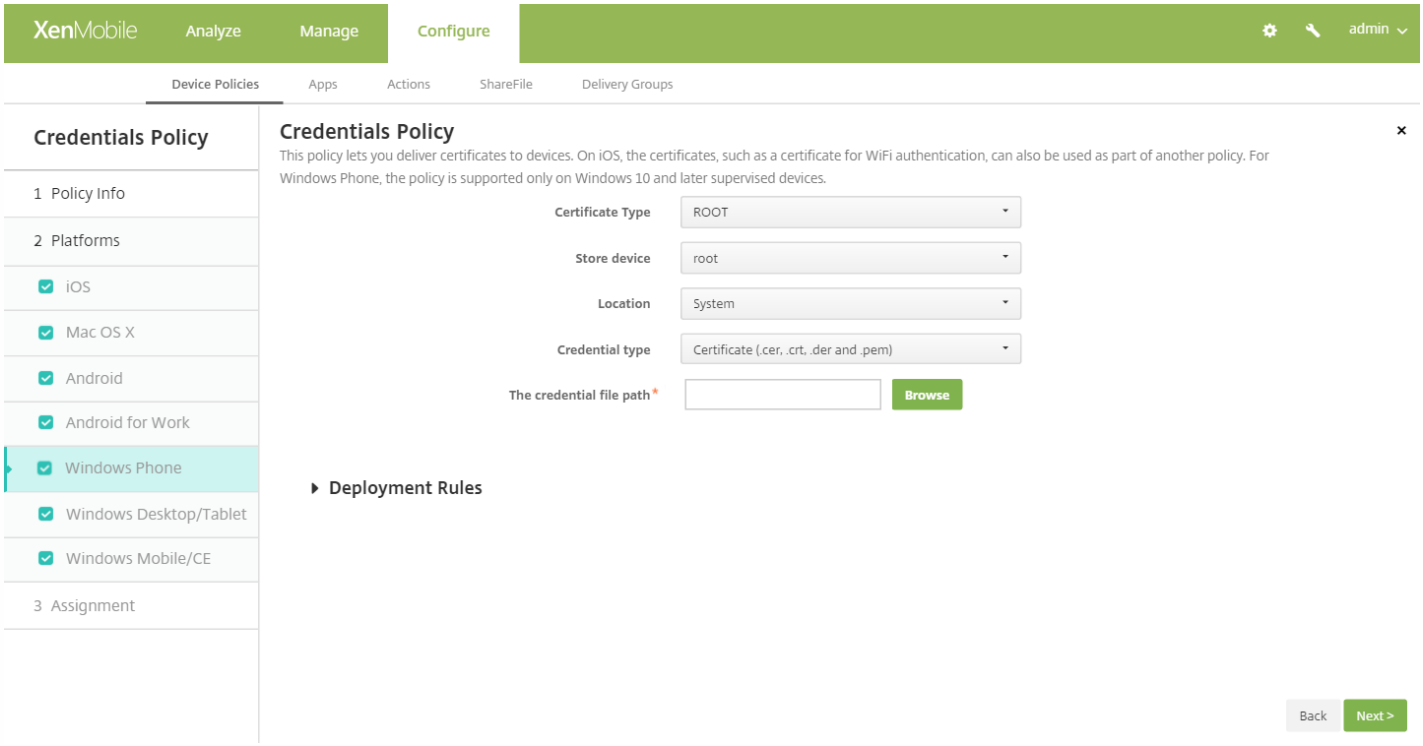
-
  -
    -
    -
  -
    -
    -
    -
  -
    -
  -
    -
-
  -
  -
  -
  -



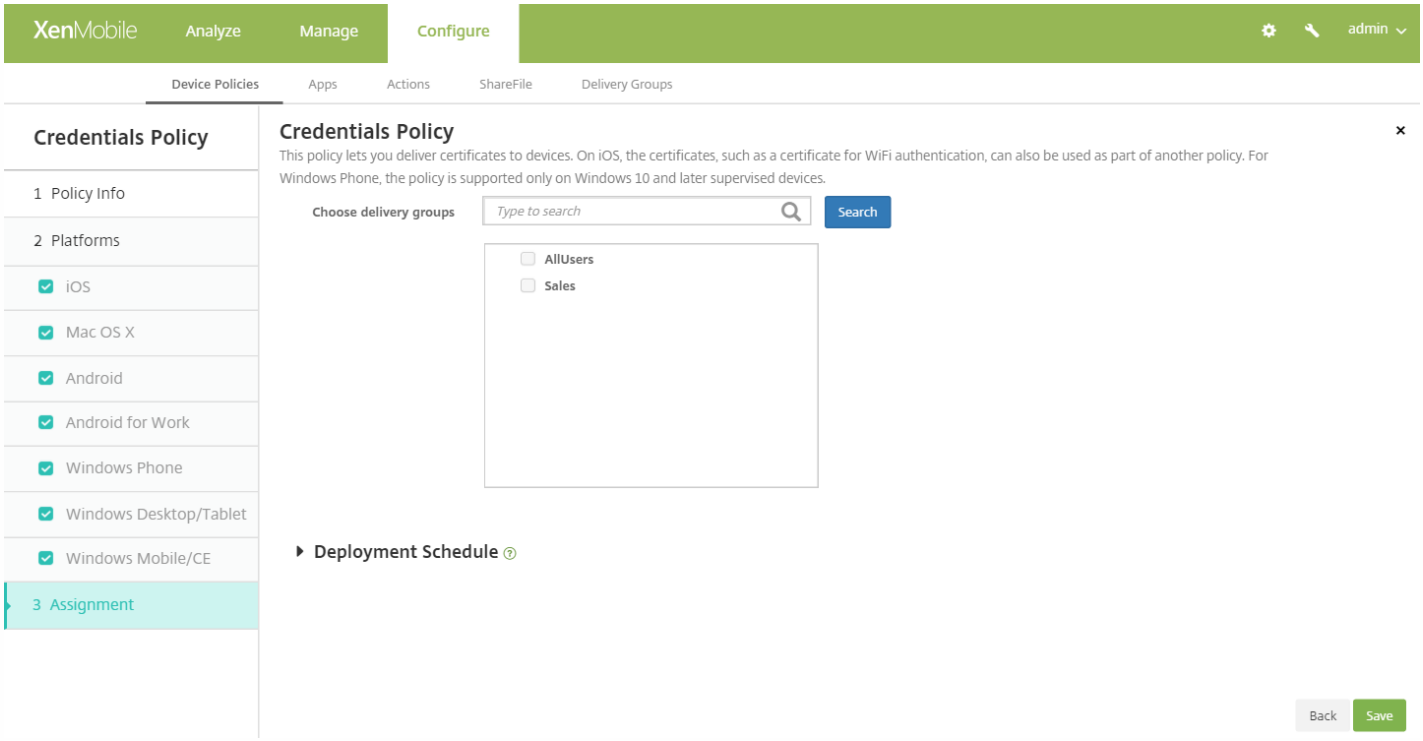




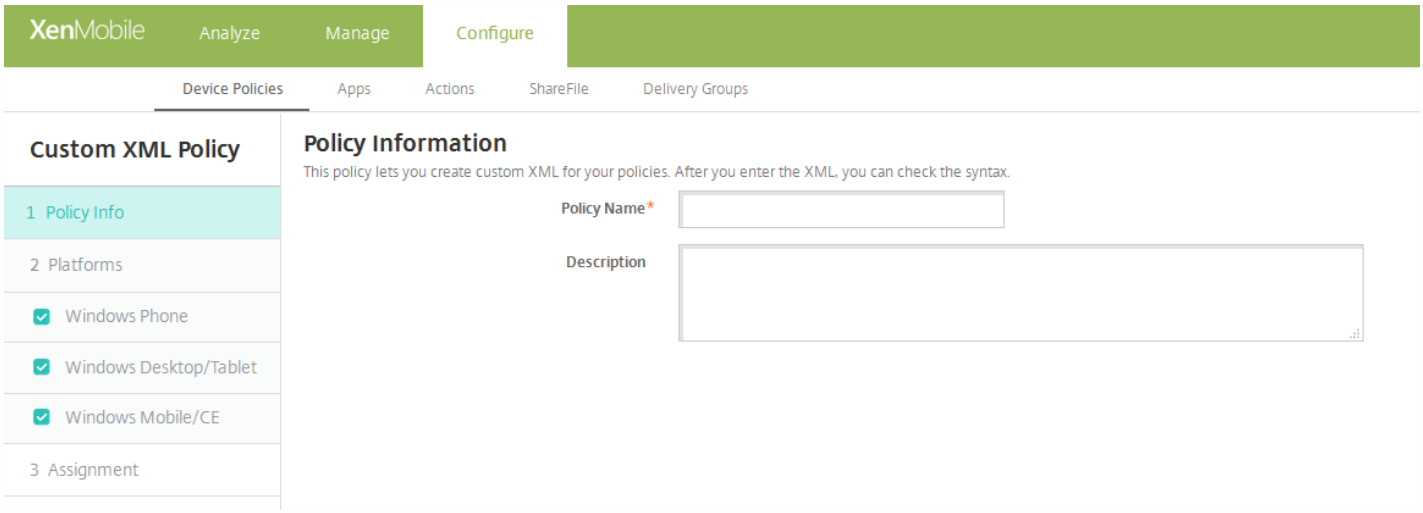
-
  -
  -
  -
  -
  -
-
-



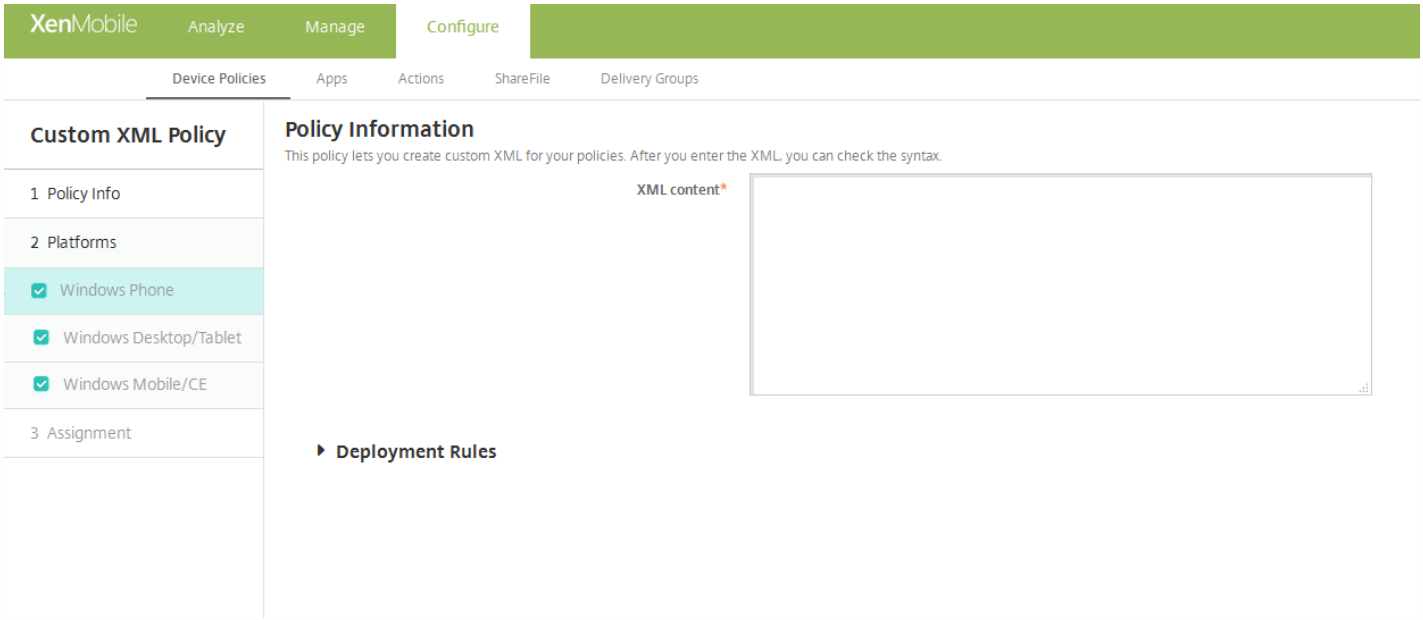
-
-
  -
    -
    -
    -
  -
    -
    -
    -
    -
    -



-
-
-
-



-
-



-

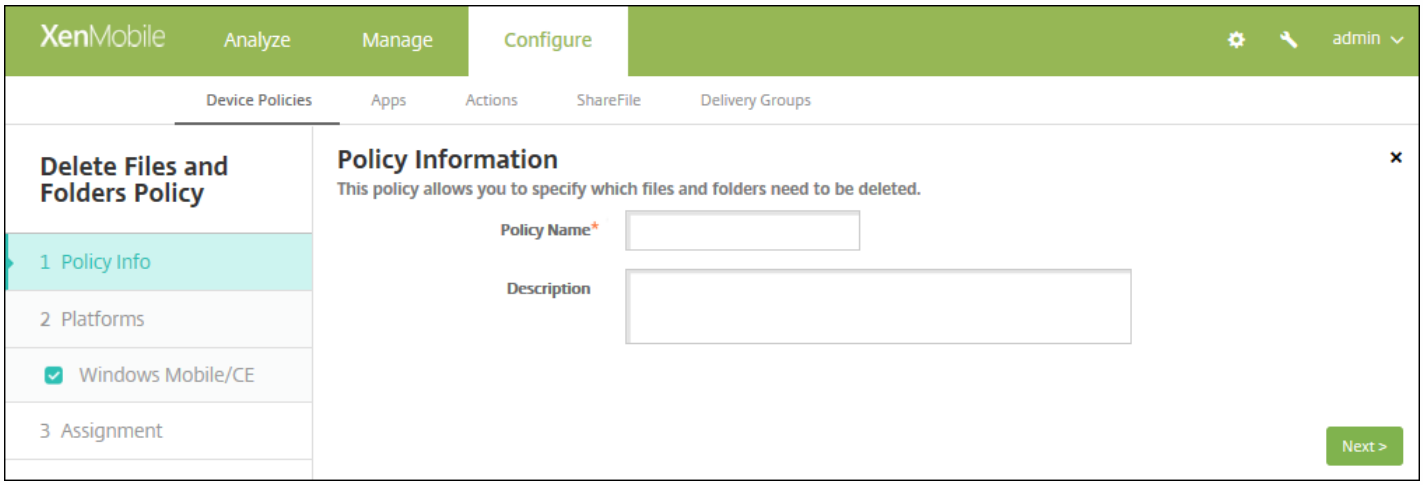
-

-

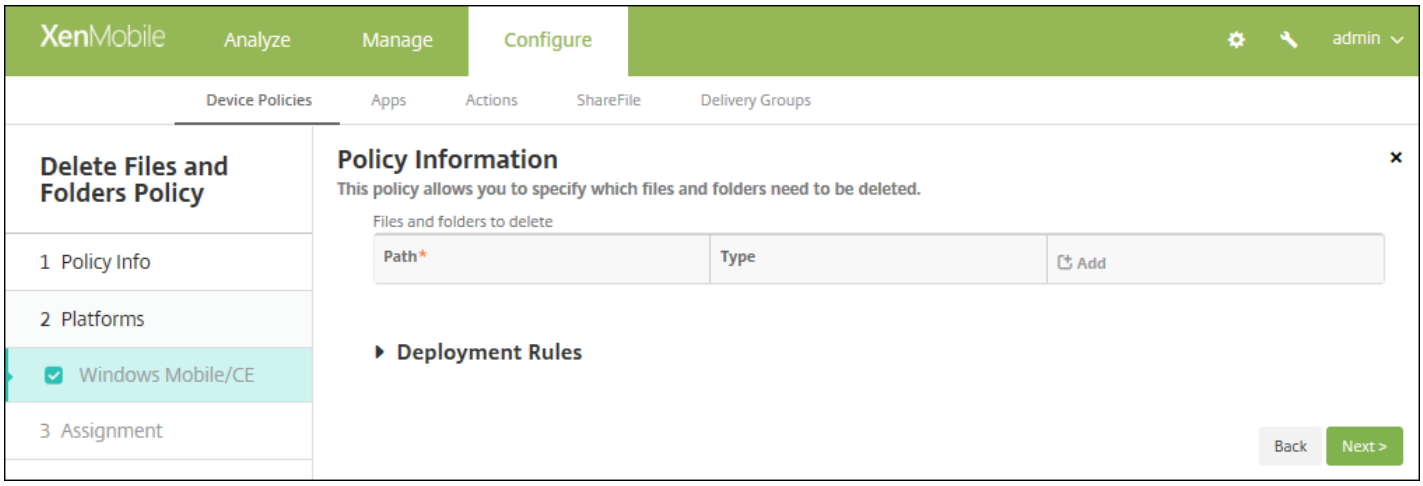
-

-

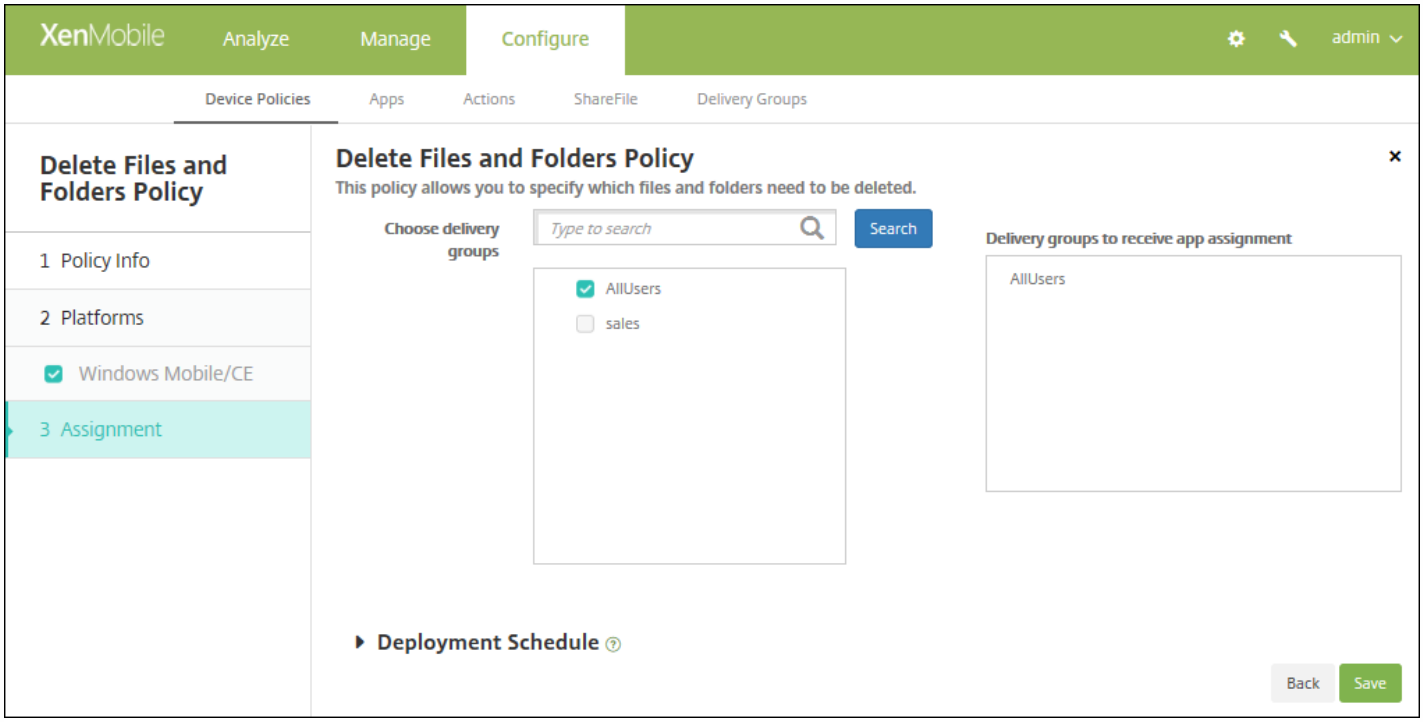
-
-
-



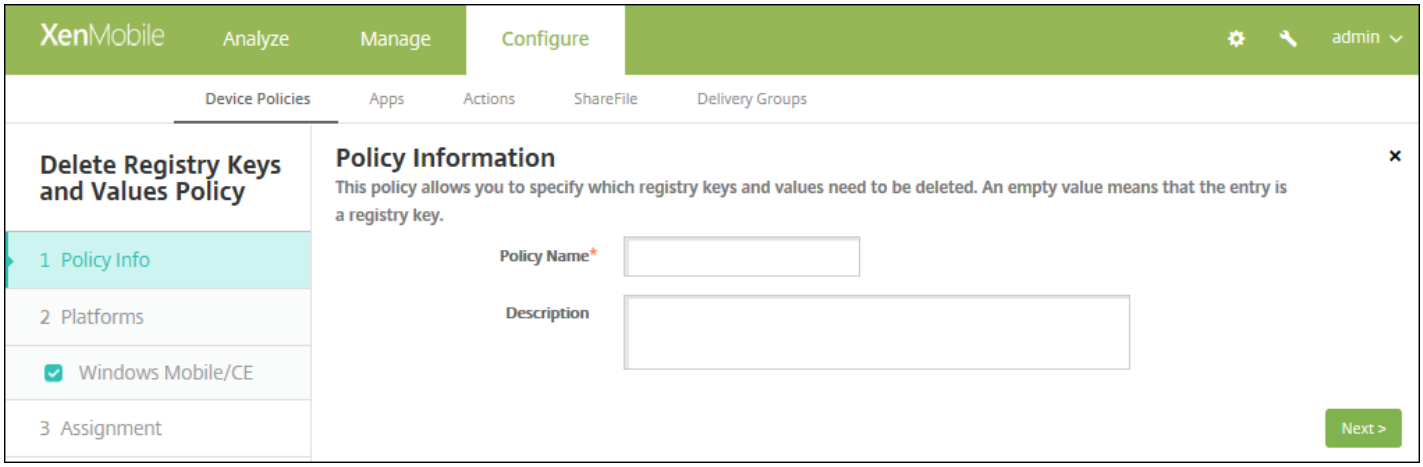
-
-



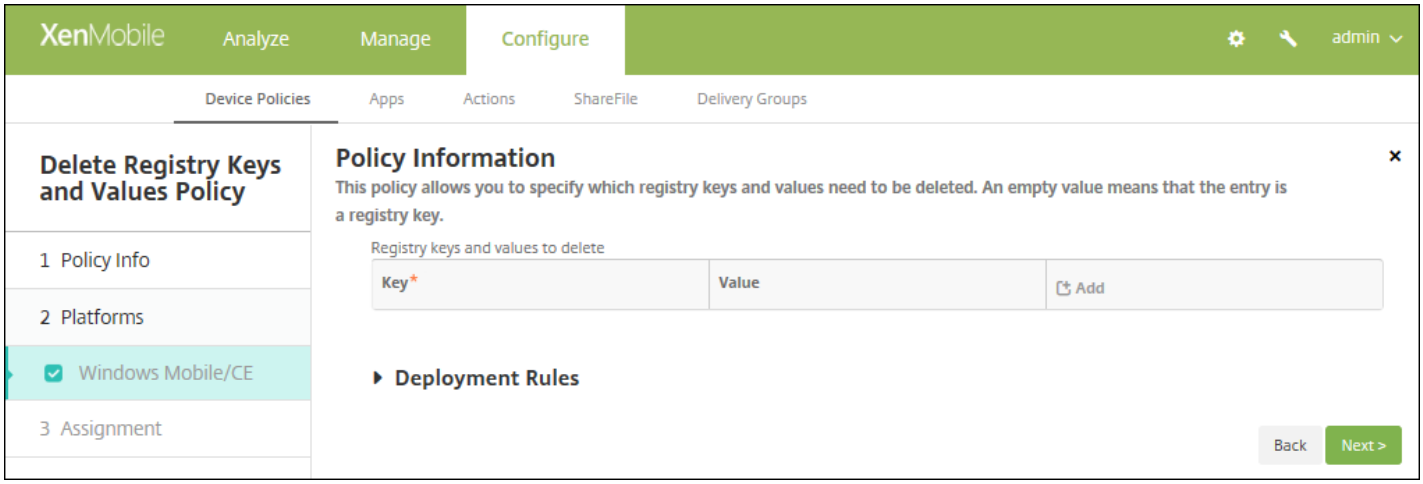
-
  -
  -
  -



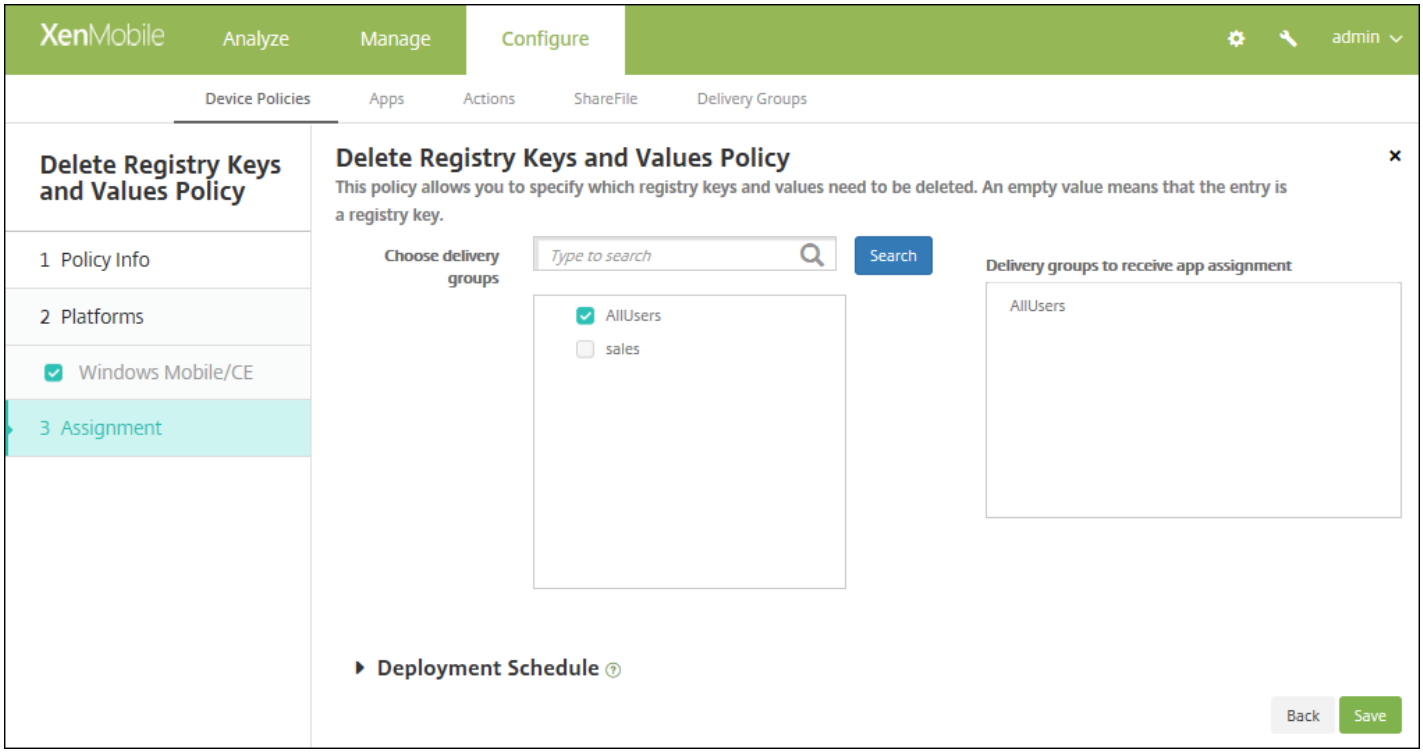
-
-
-
-
-
-
-



-
-

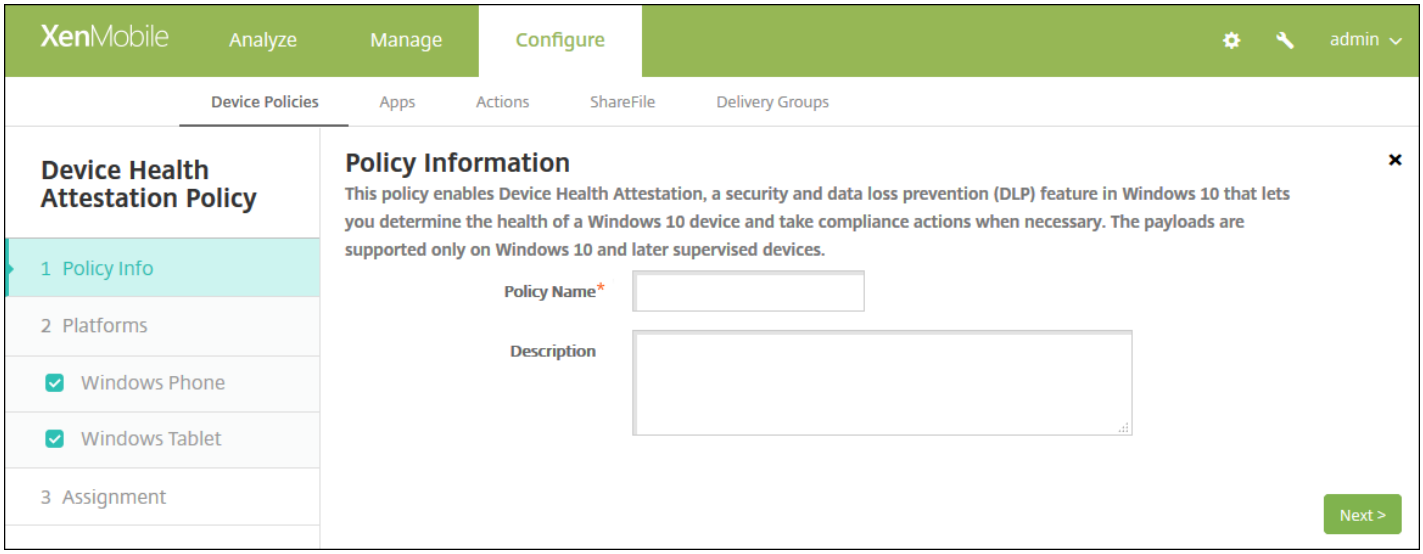


-
  -
  -
  -

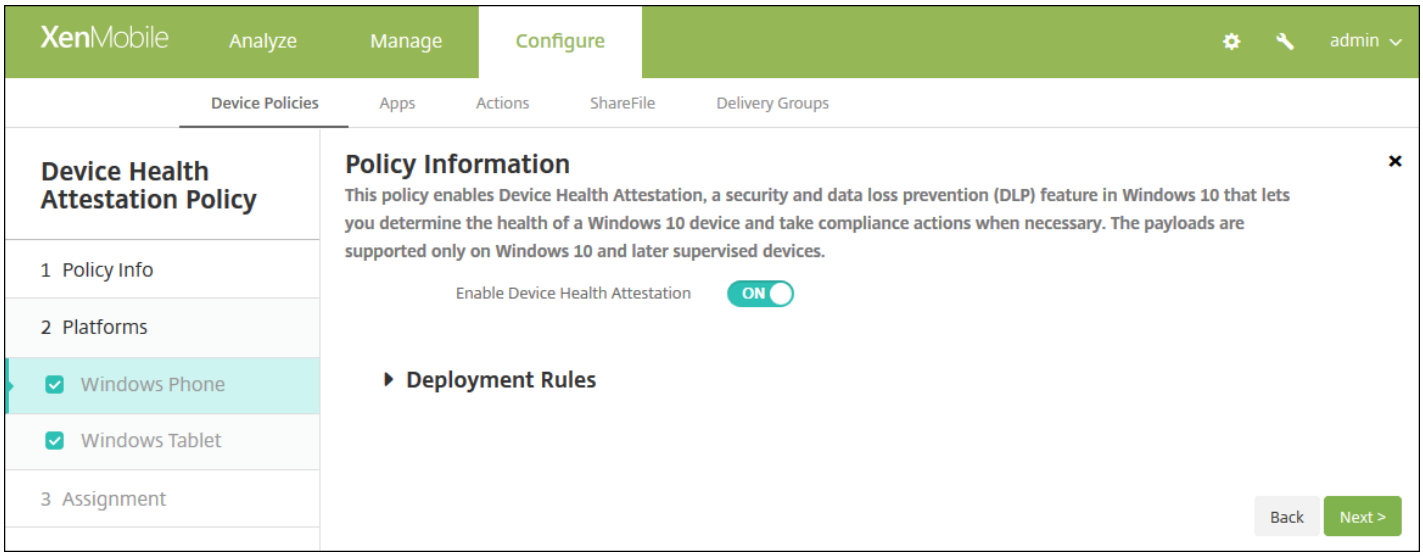


-
-
-
-
-
-
-

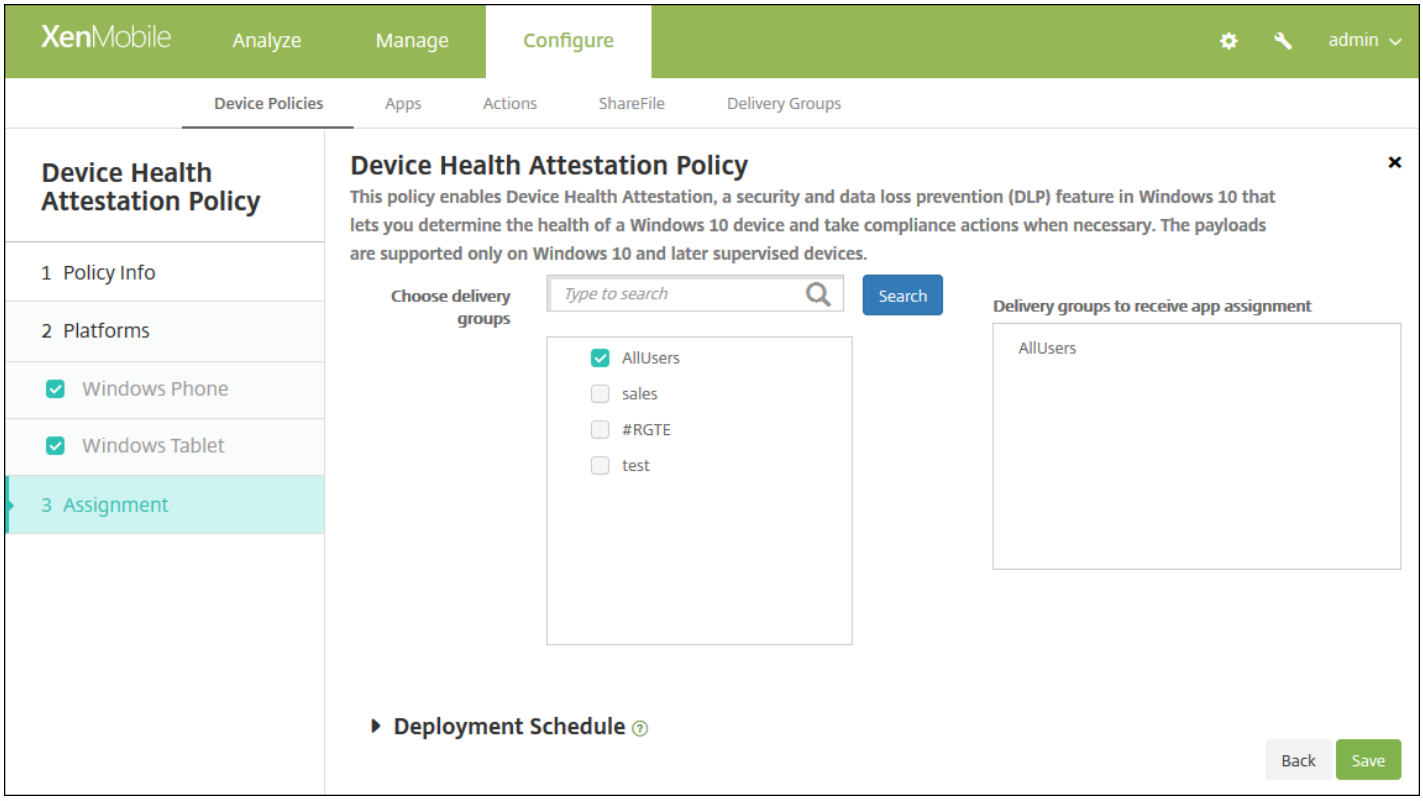
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-



-
-

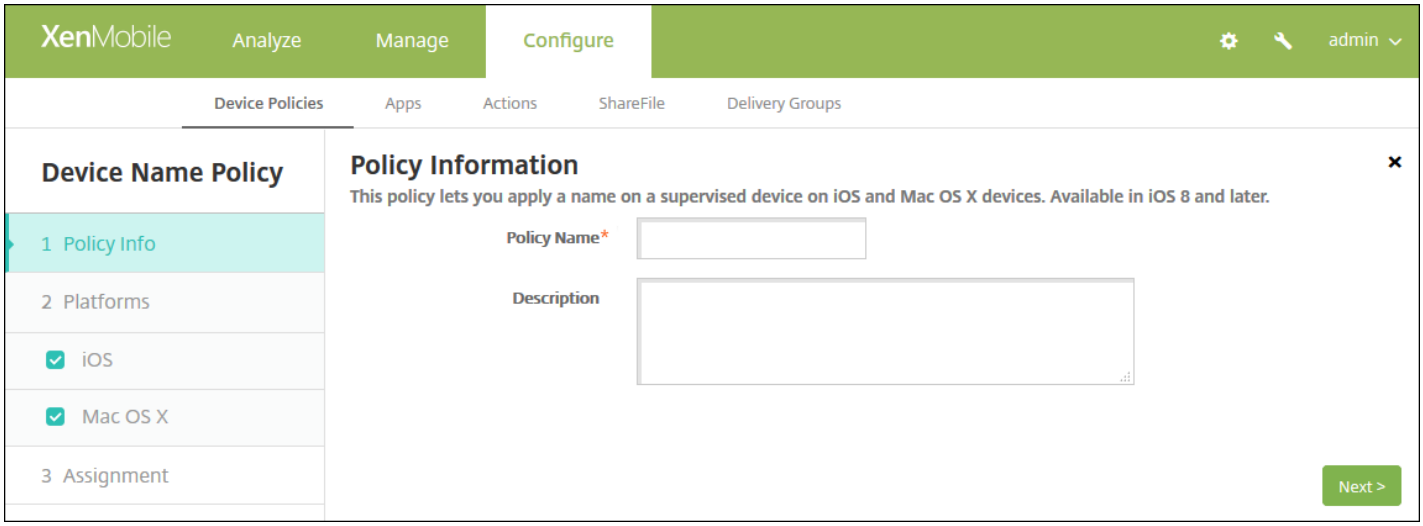


-

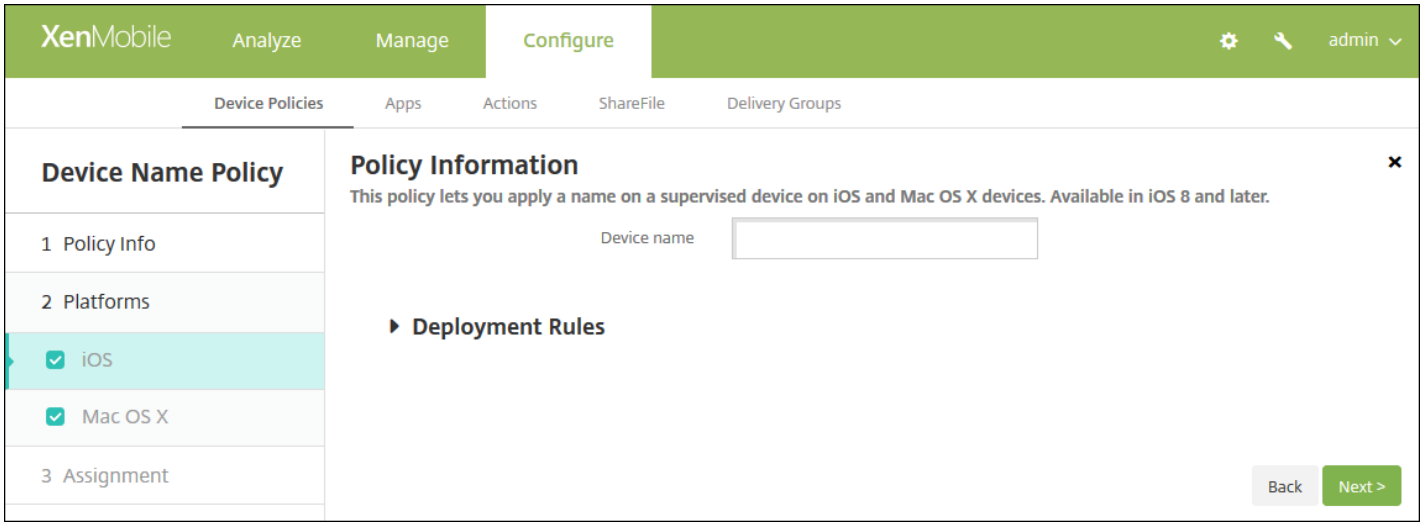


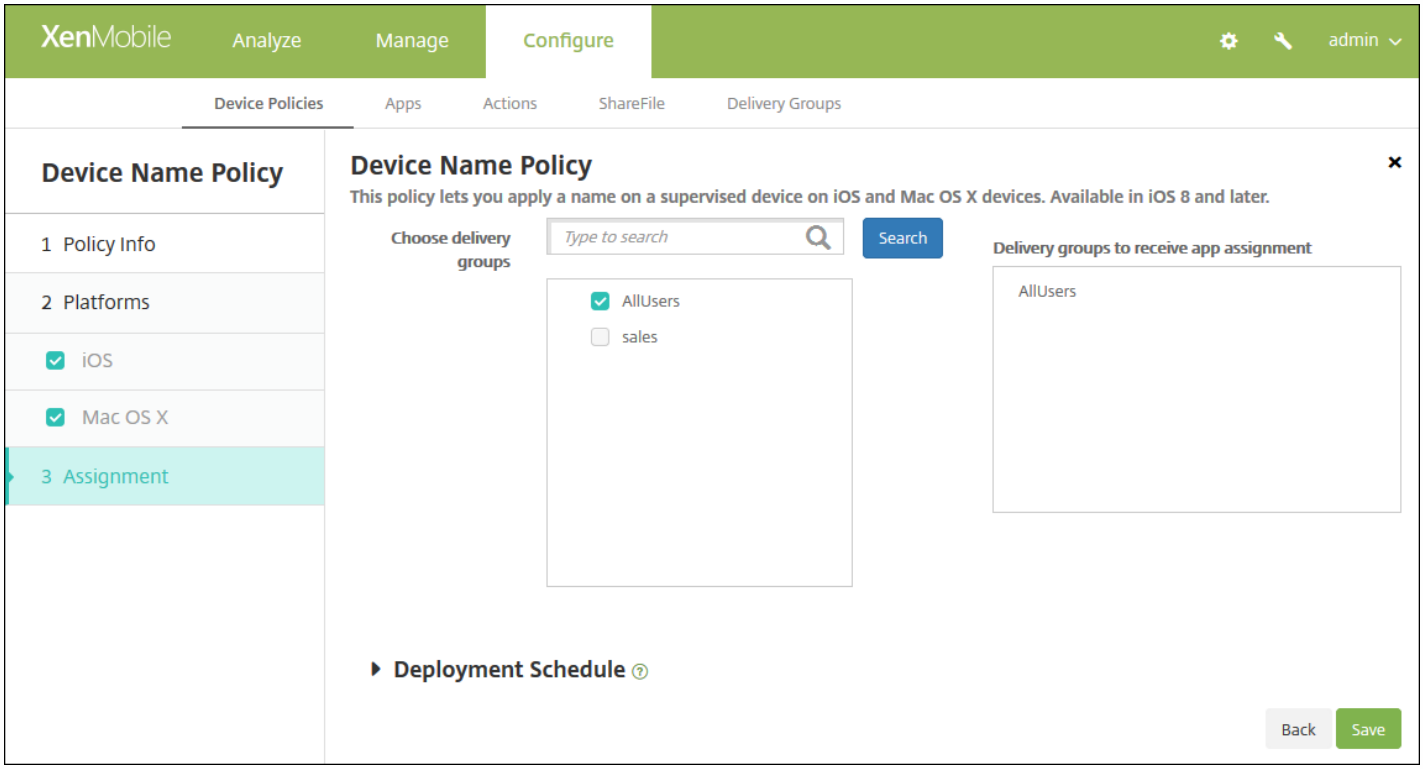
-
-
-
-
-

-
-



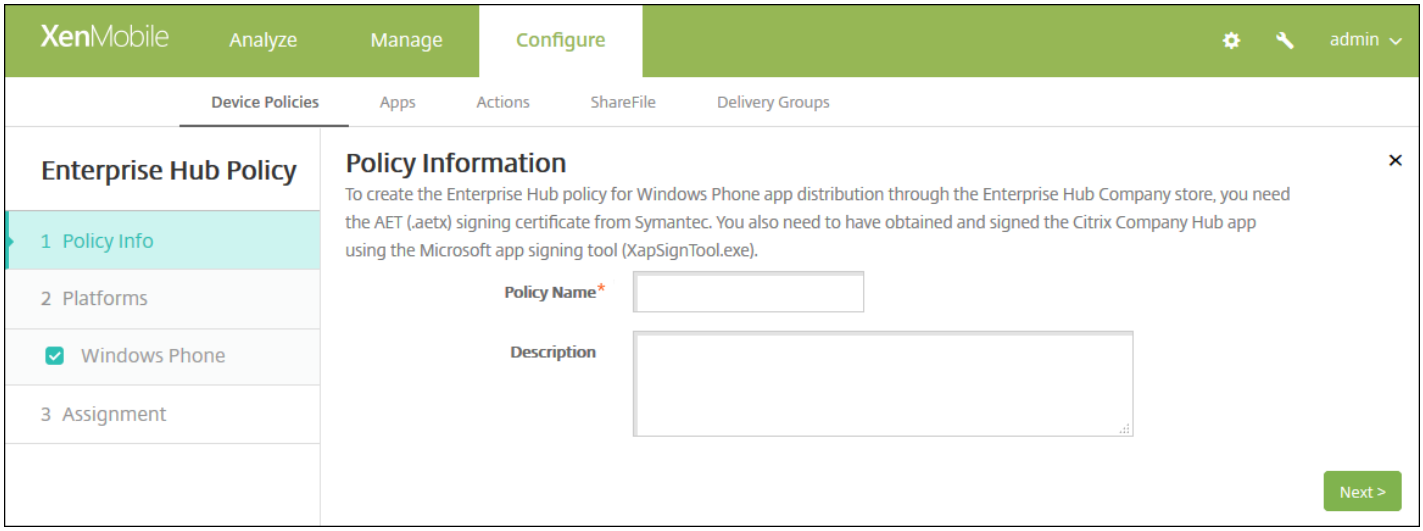
-
-



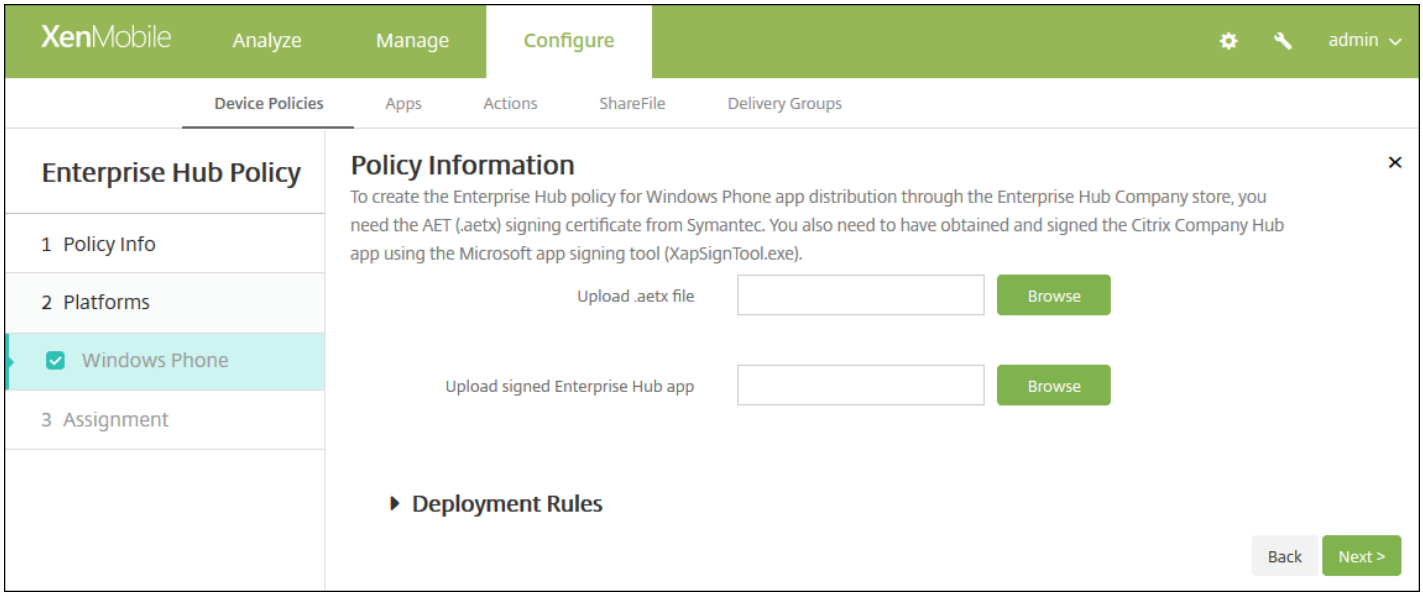


-
-
-
-
-
-
-

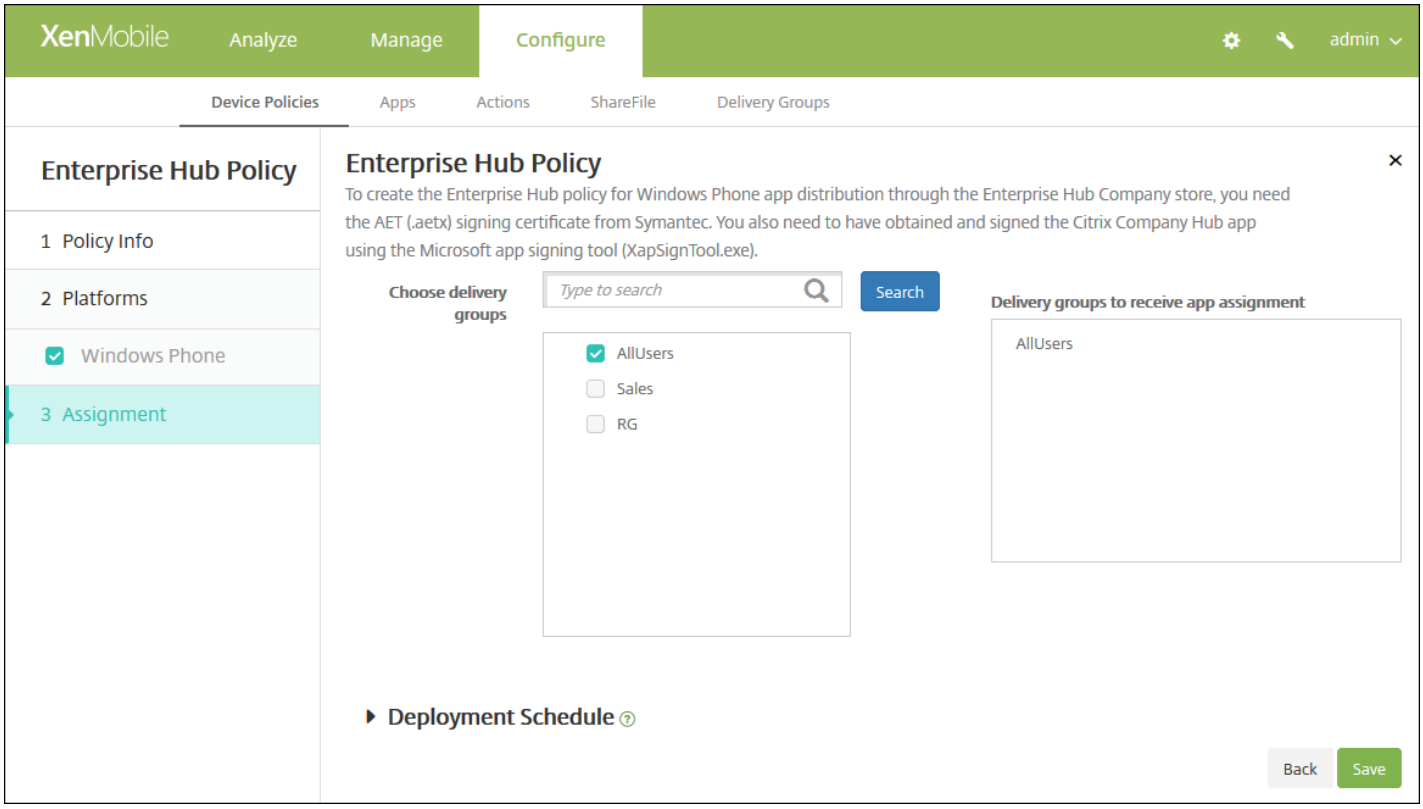
-
-



-
-

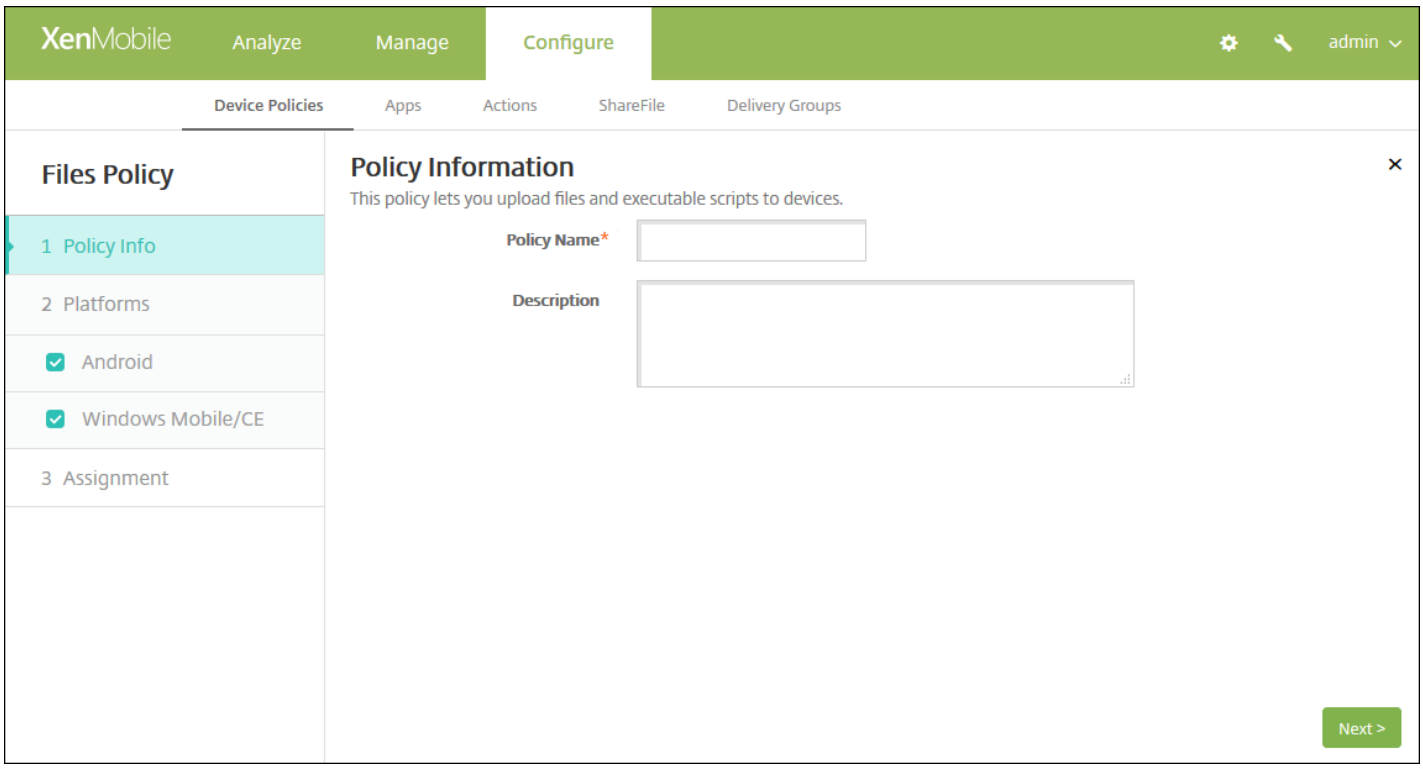


-
-

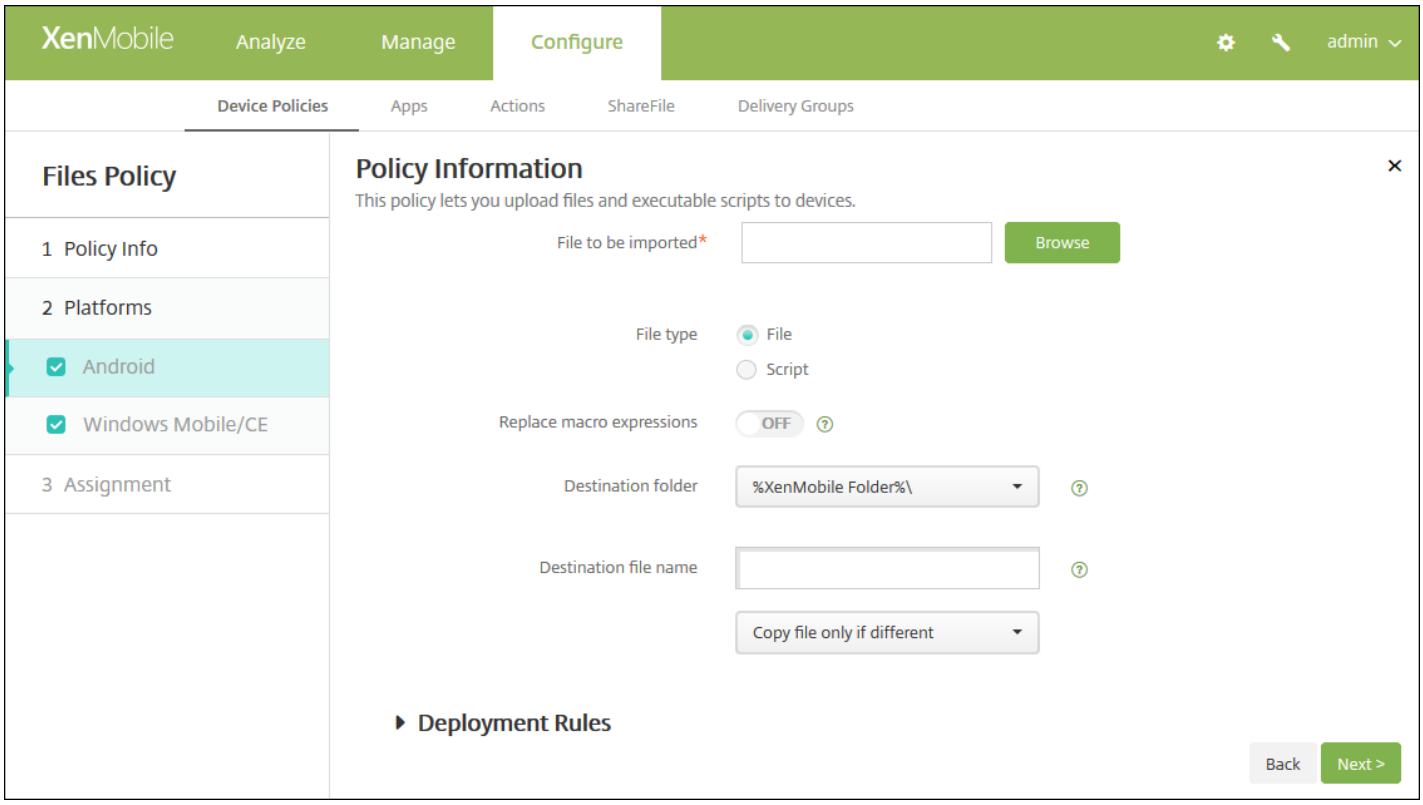


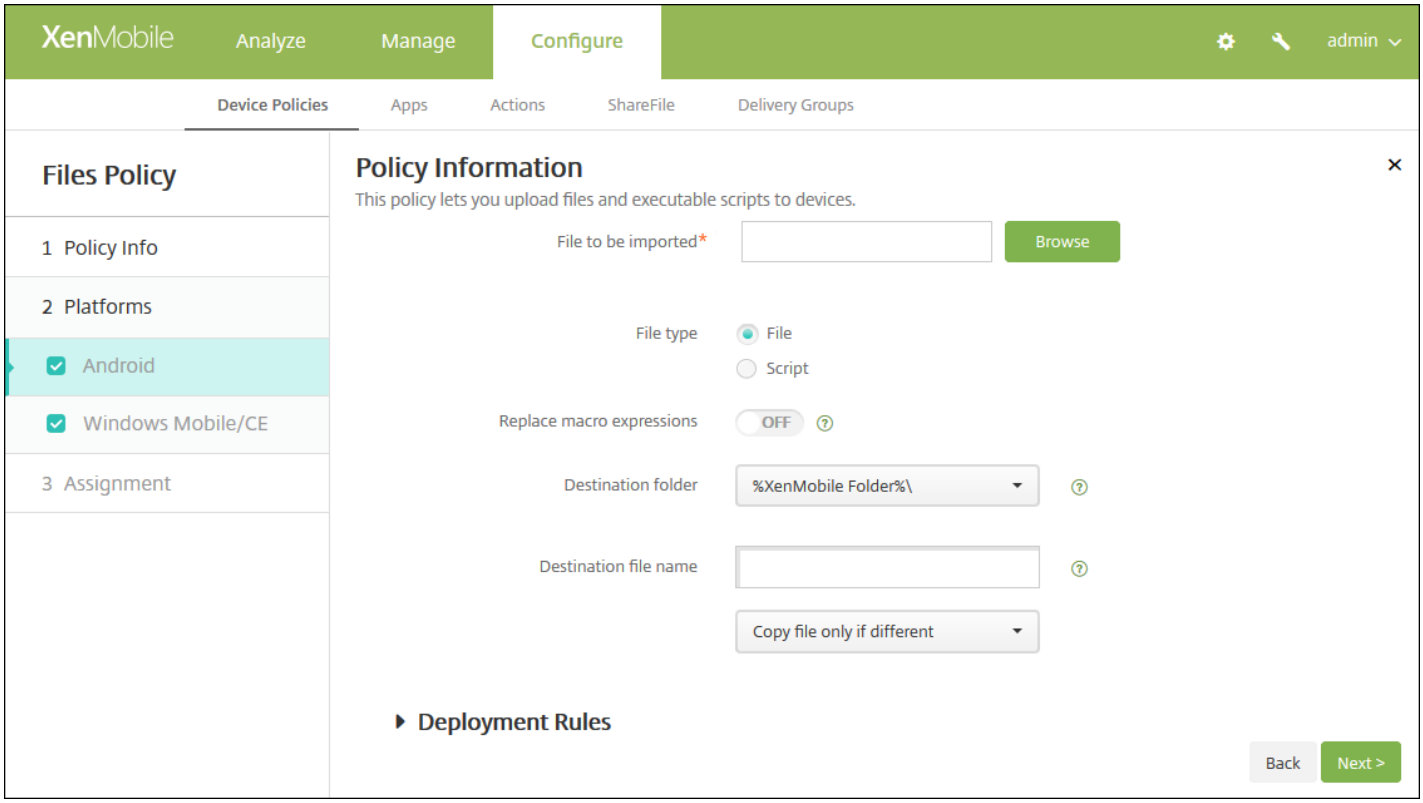
-
-
-
-
-
-
-

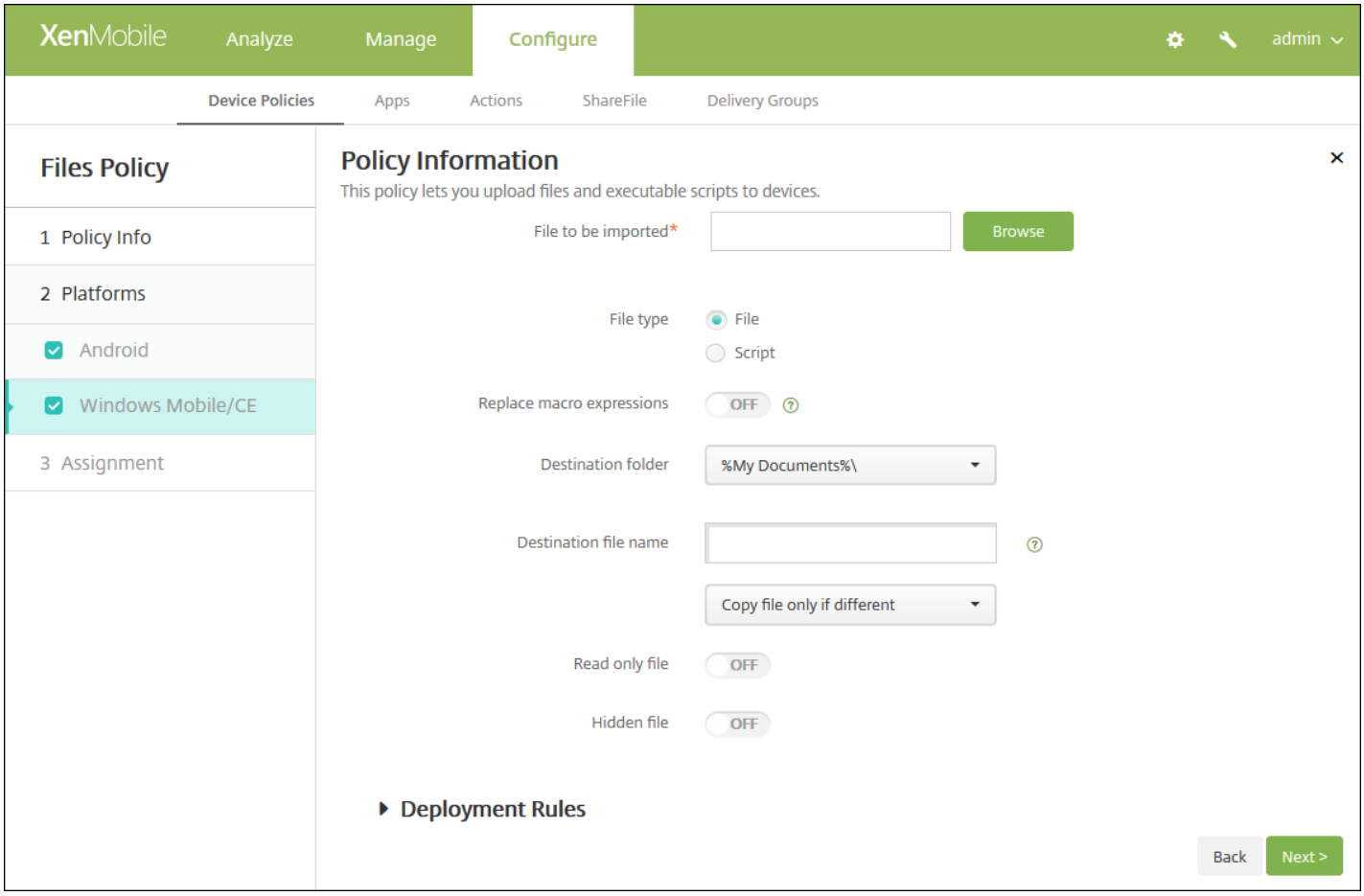
-
-
-



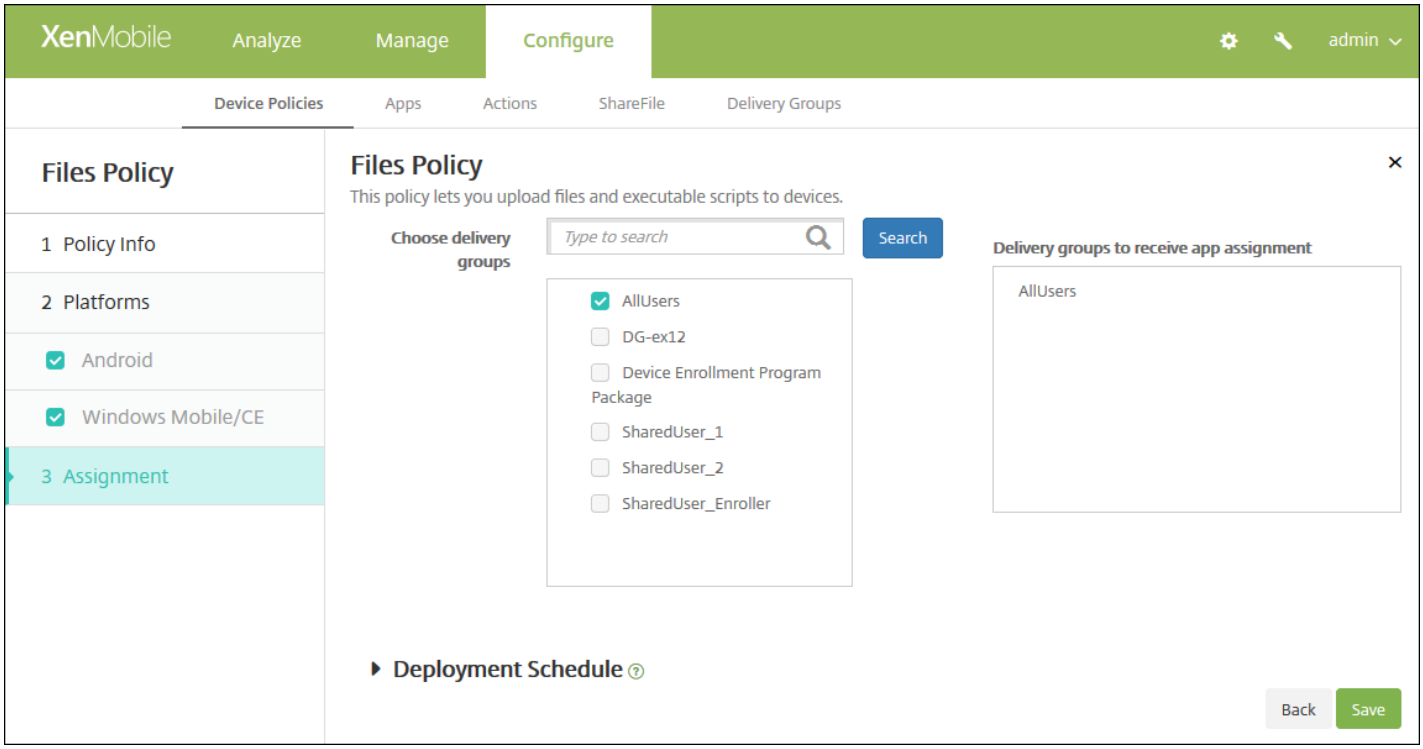
-
-



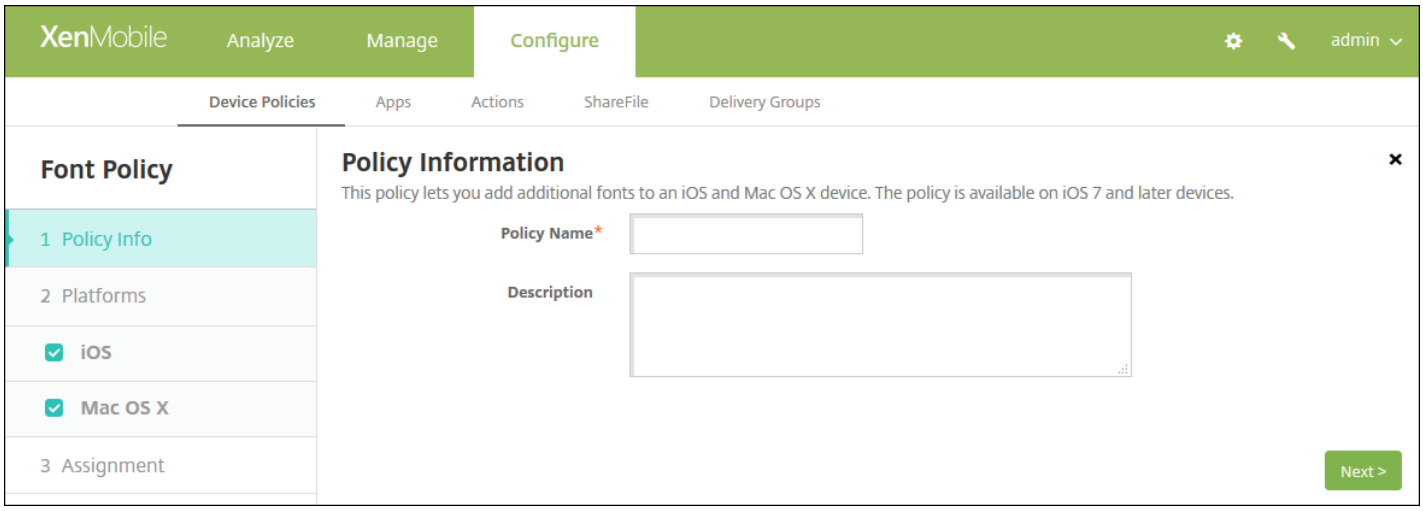




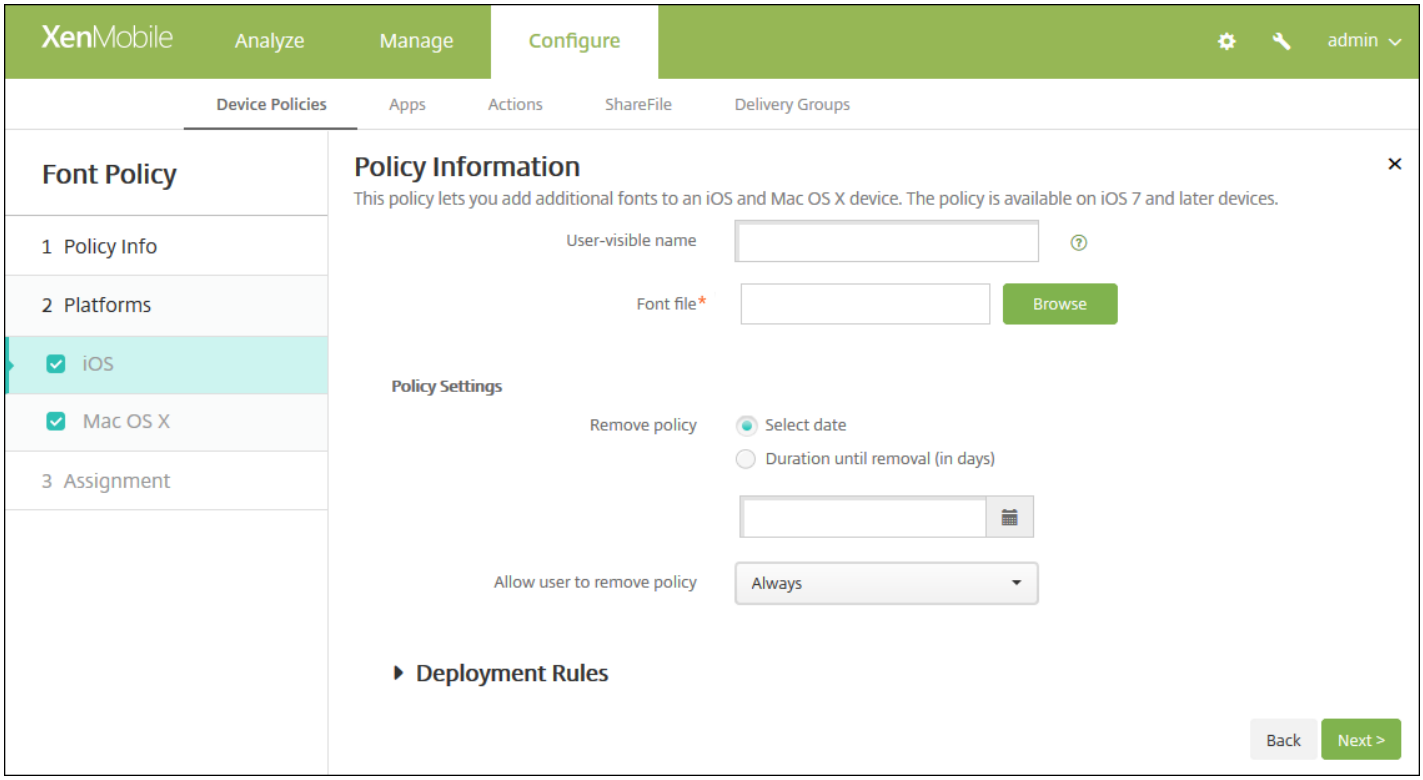
-
-
-
-
  -
  -
  -
  -
  -
-
-
-



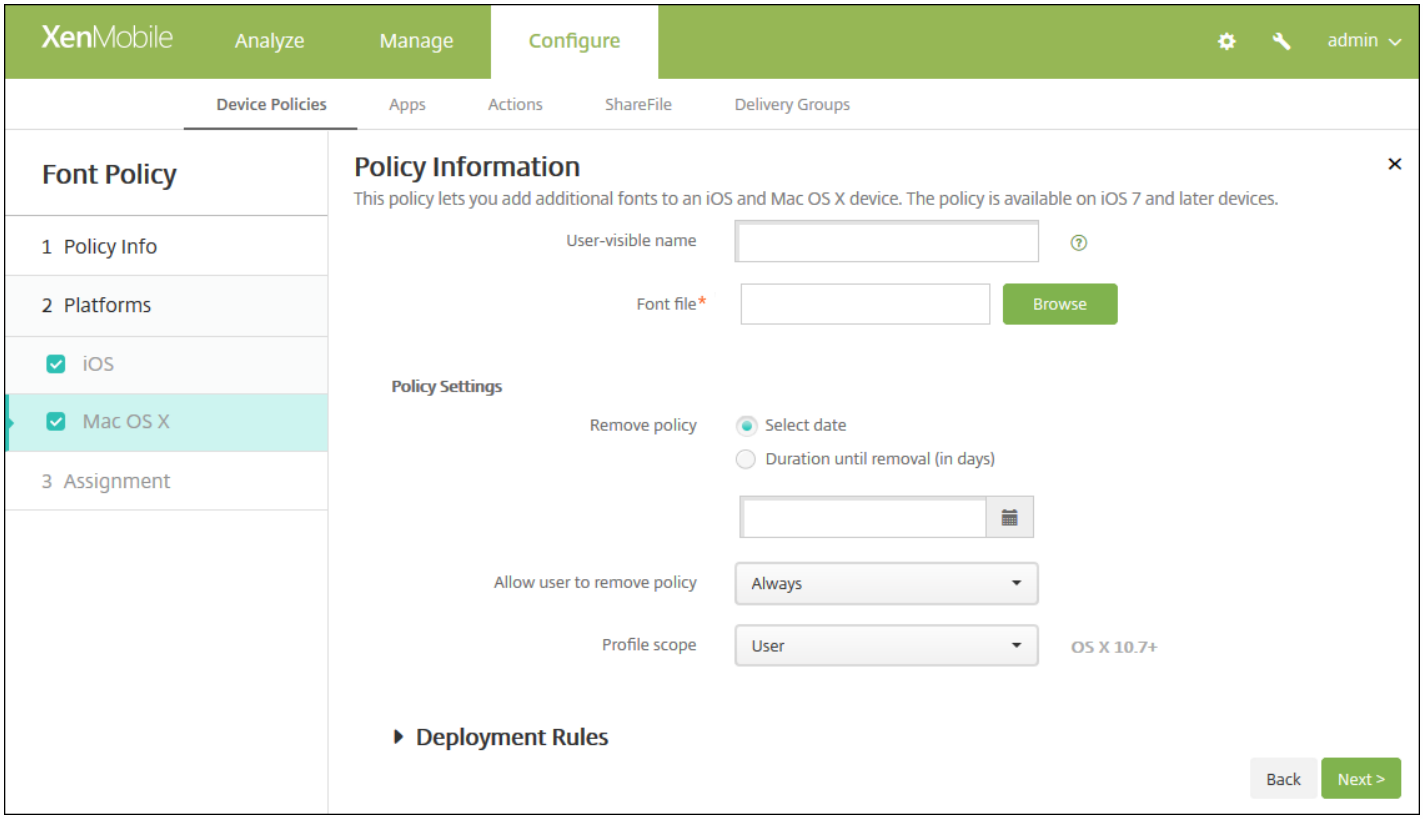
-
-



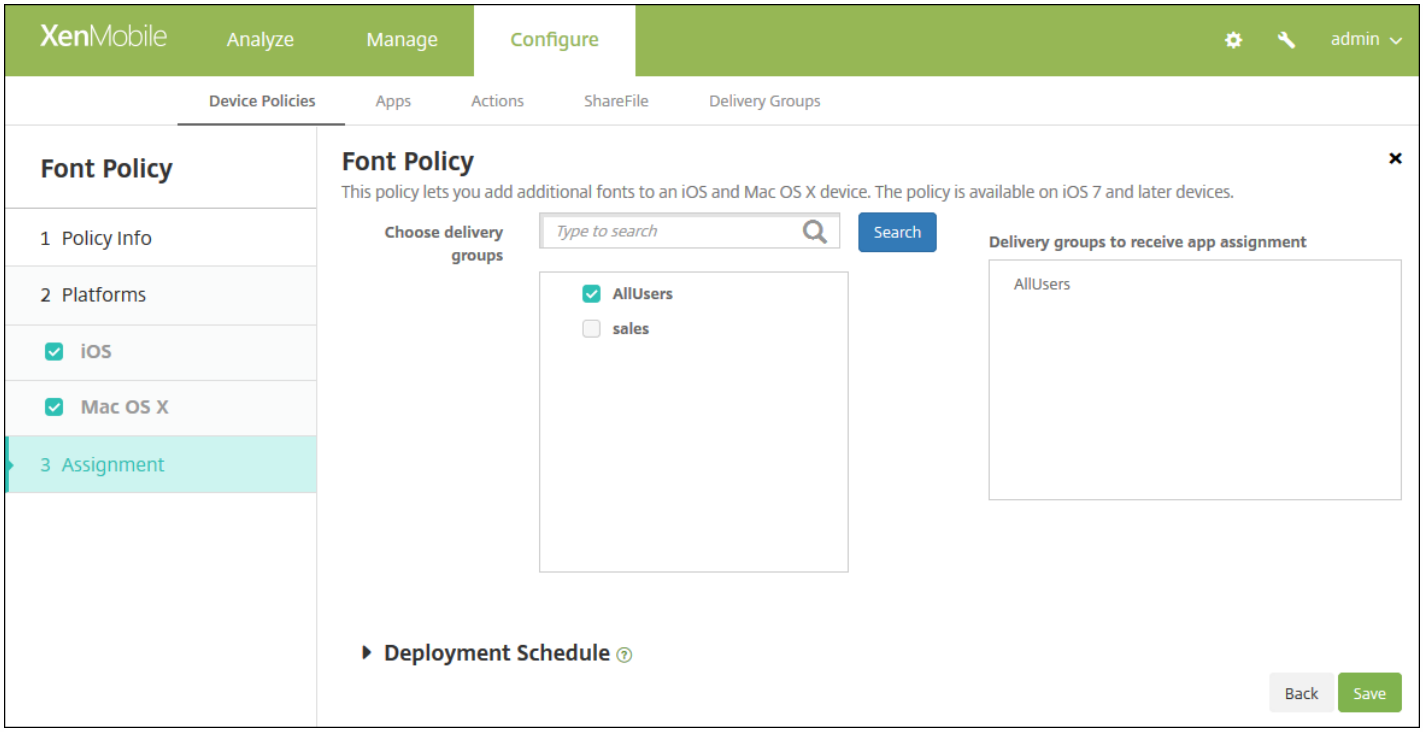
-
-

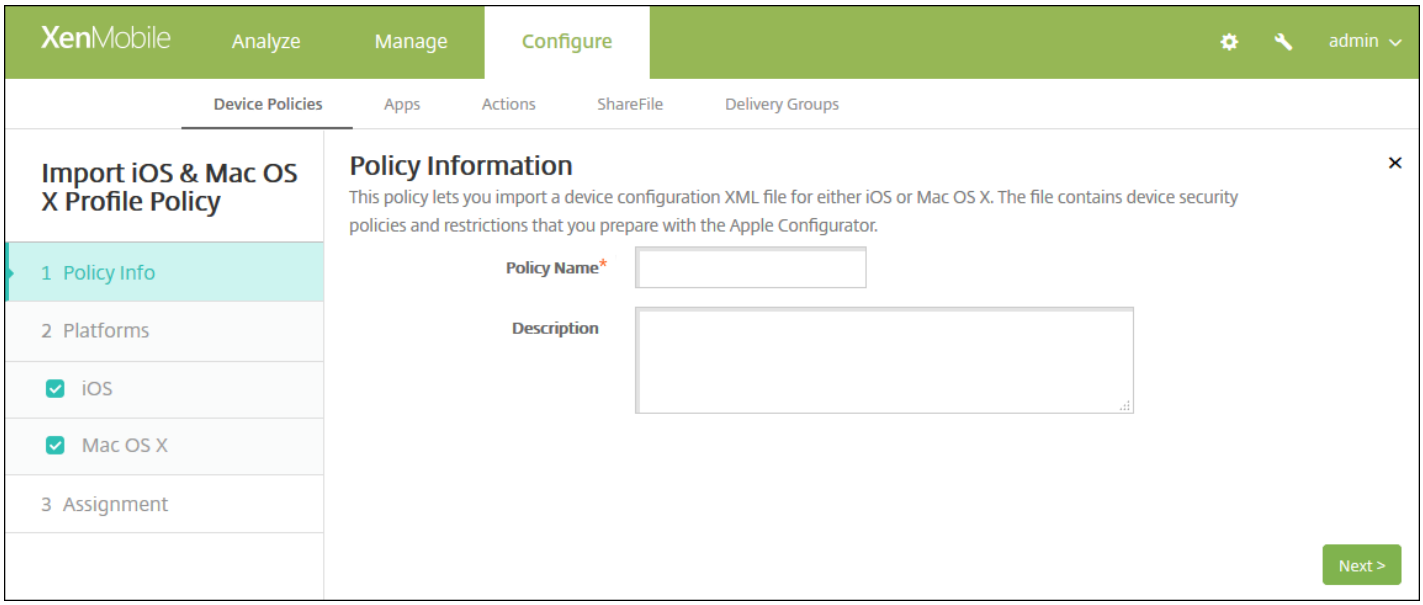


-
-
-
  -
  -
  -
  -

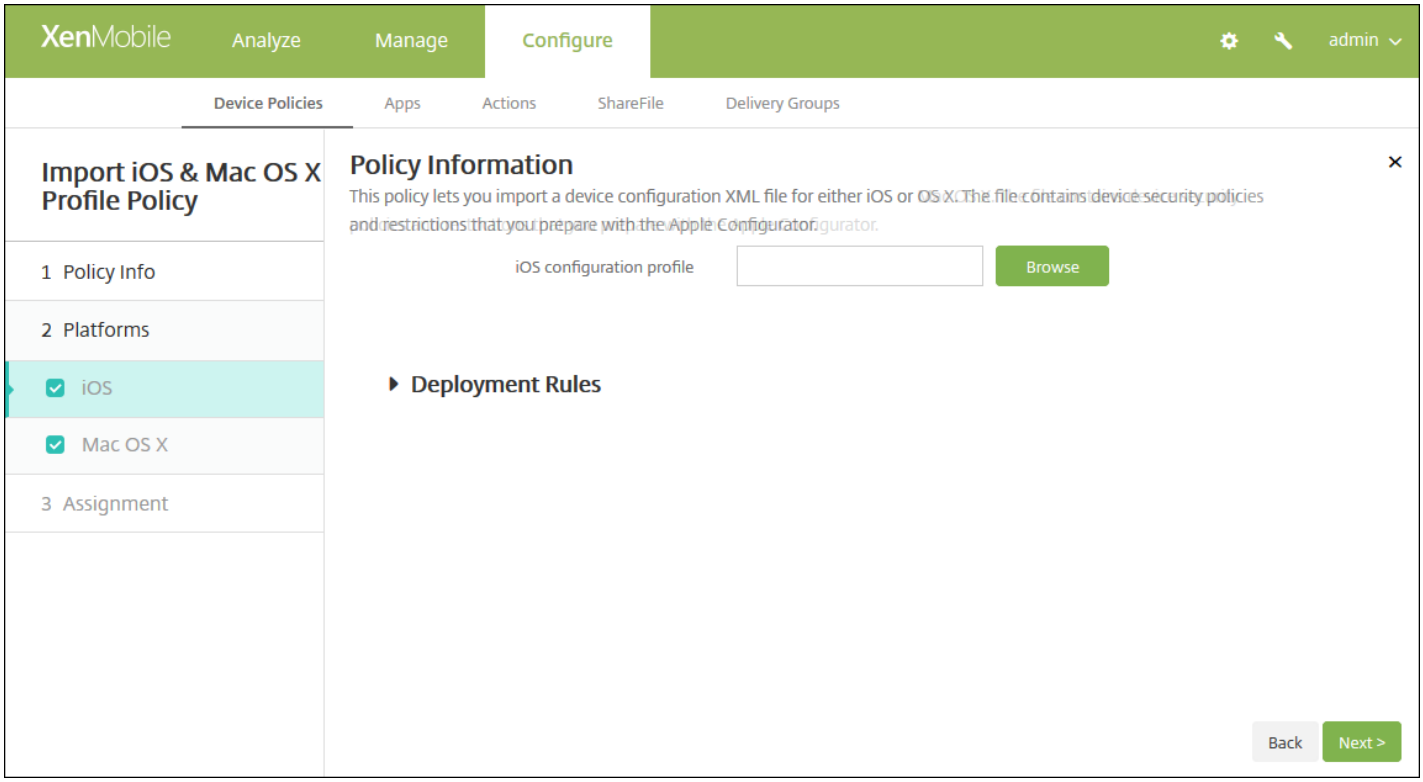


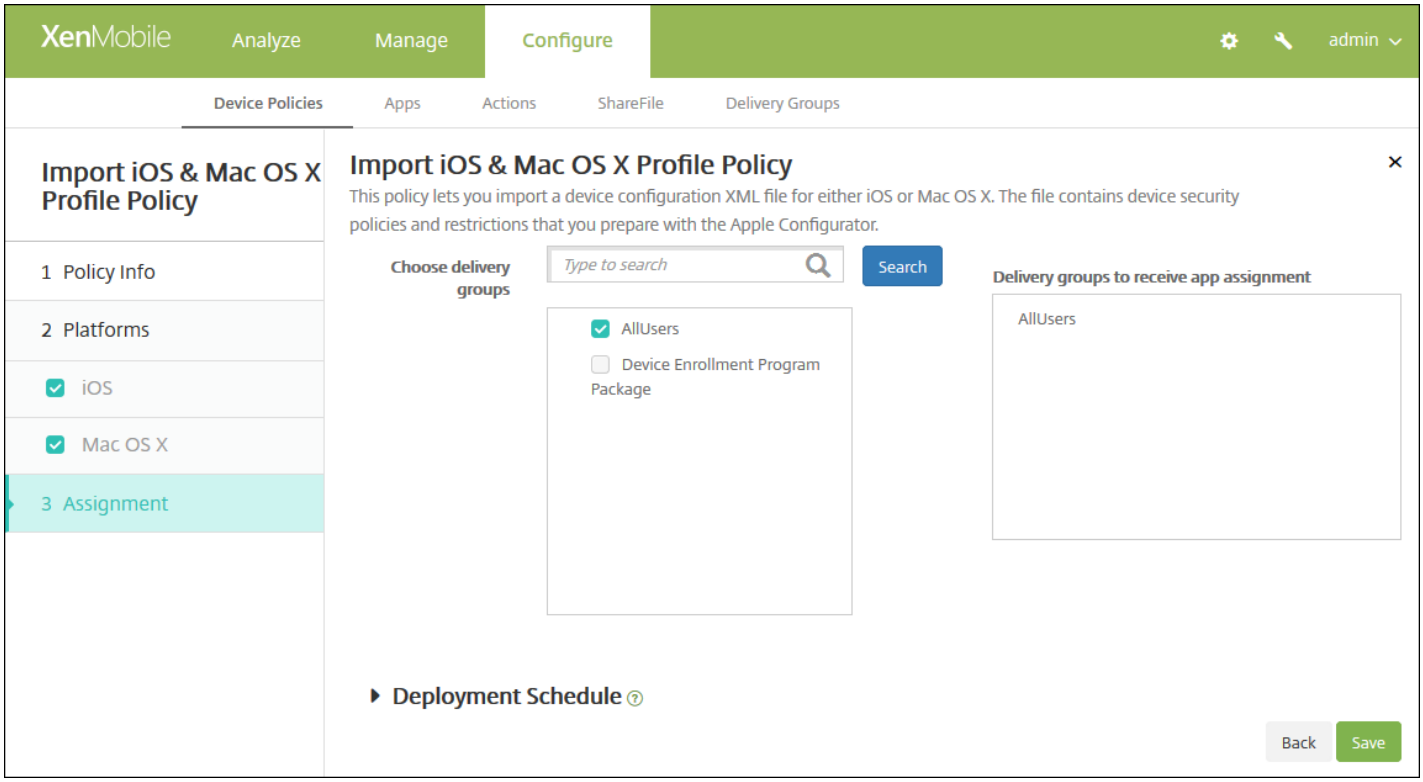
-
-
-
  -
  -
  -
  -
  -



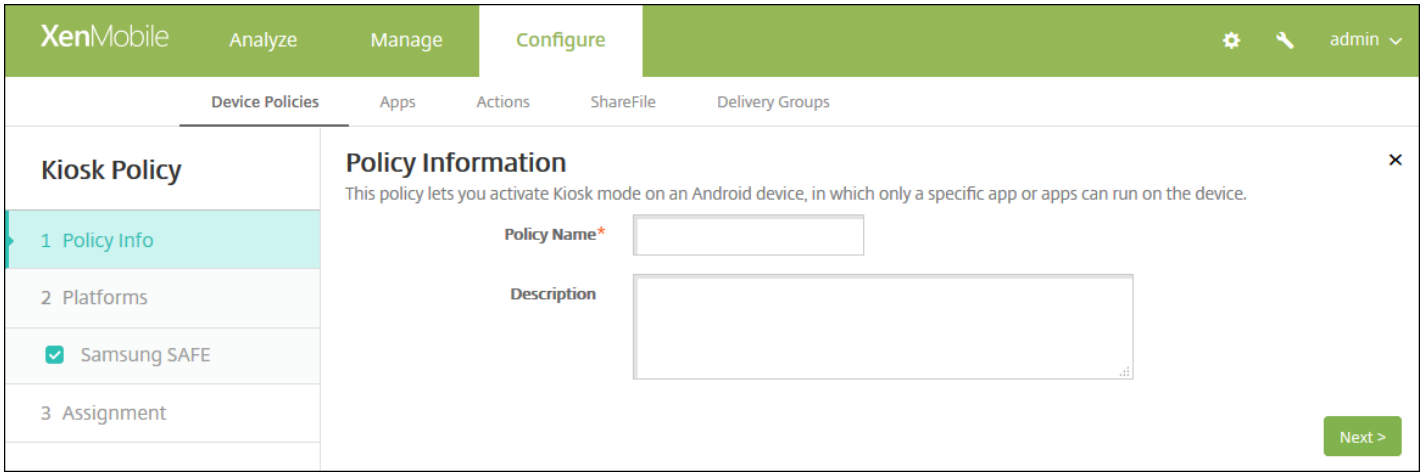


-
-

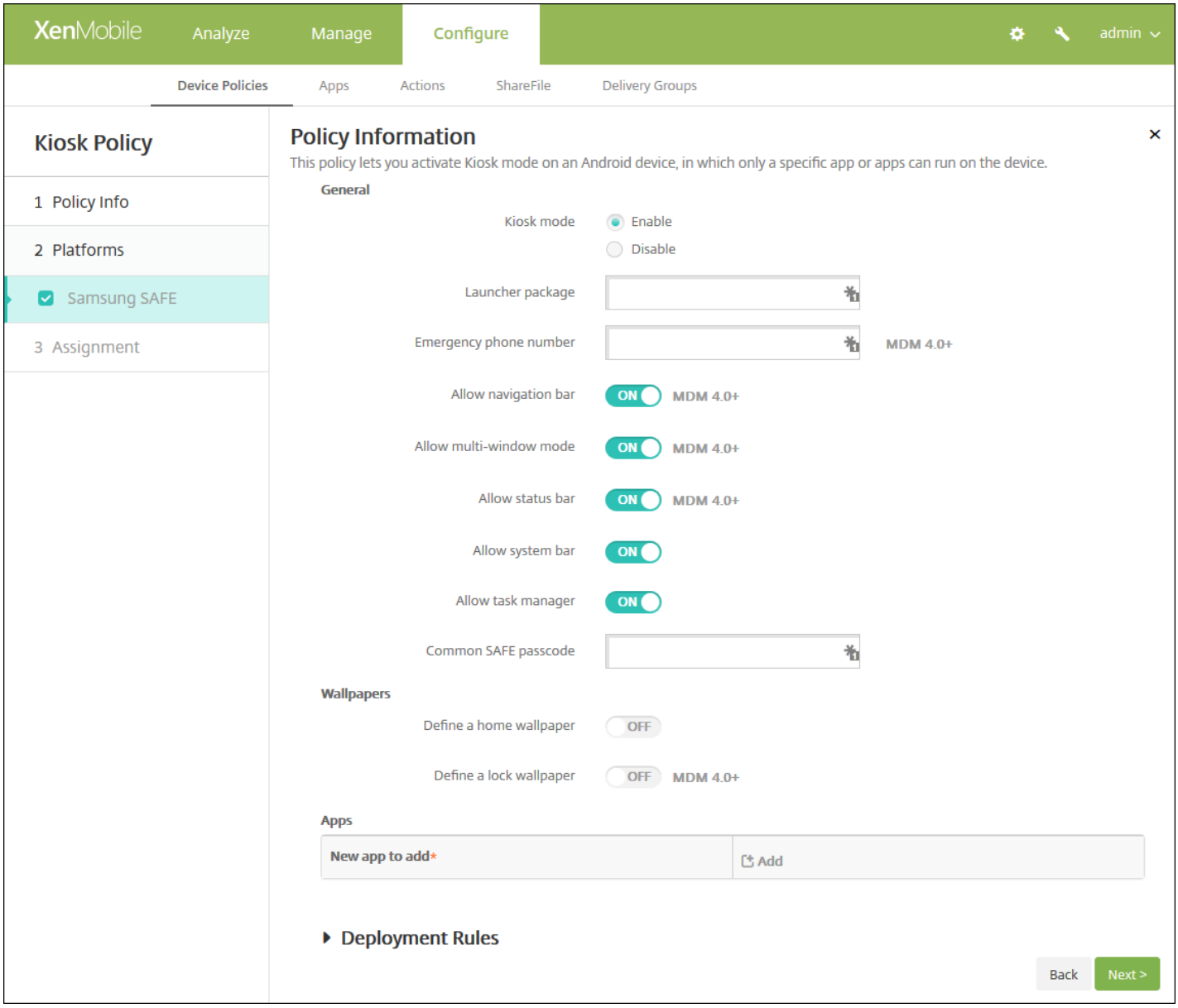




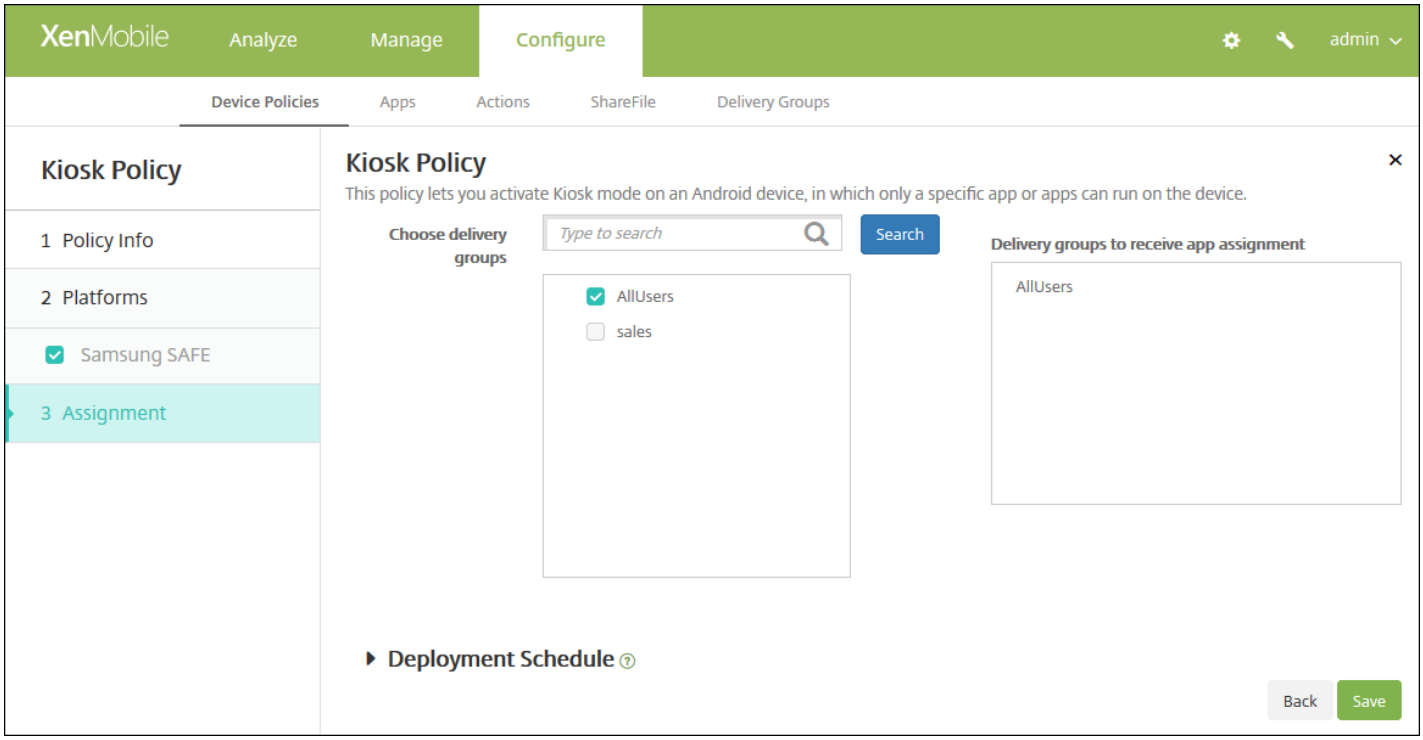
-
-



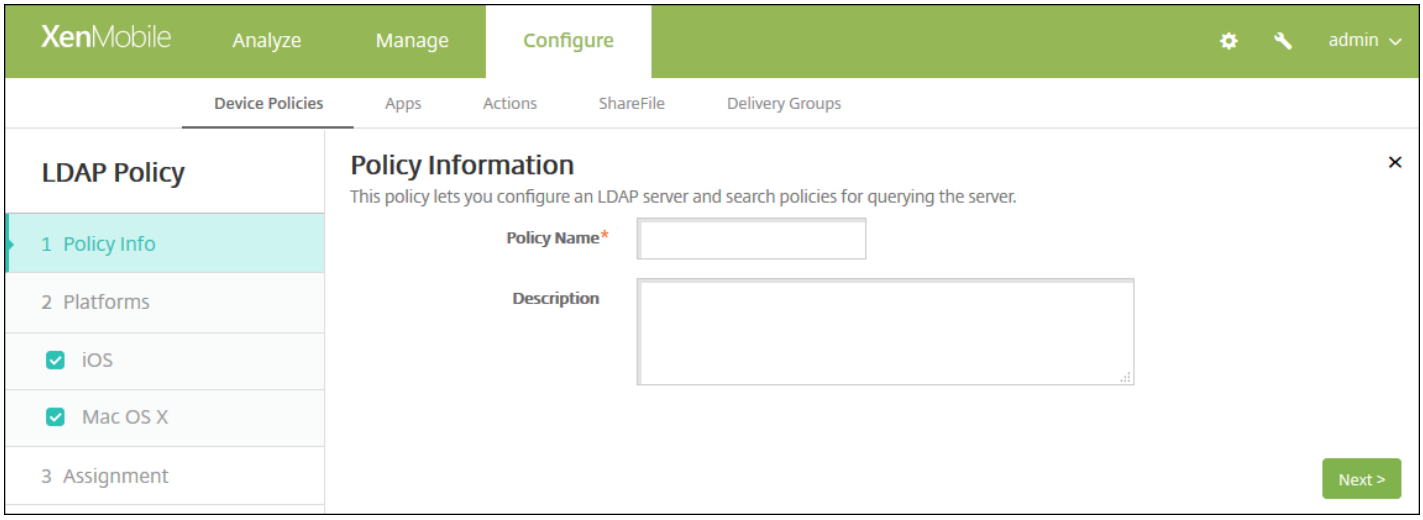
-
-



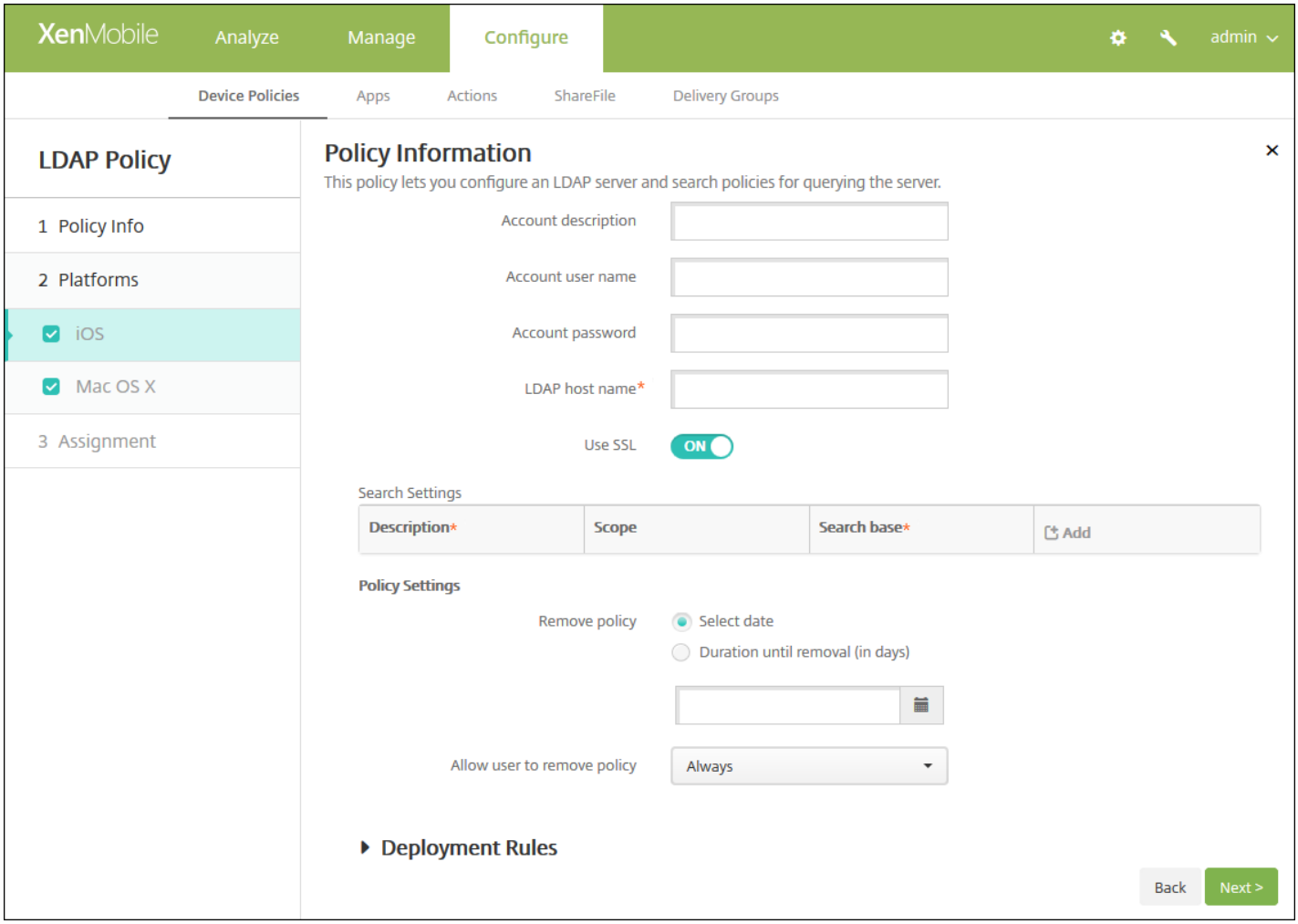
-
-
-
-
-



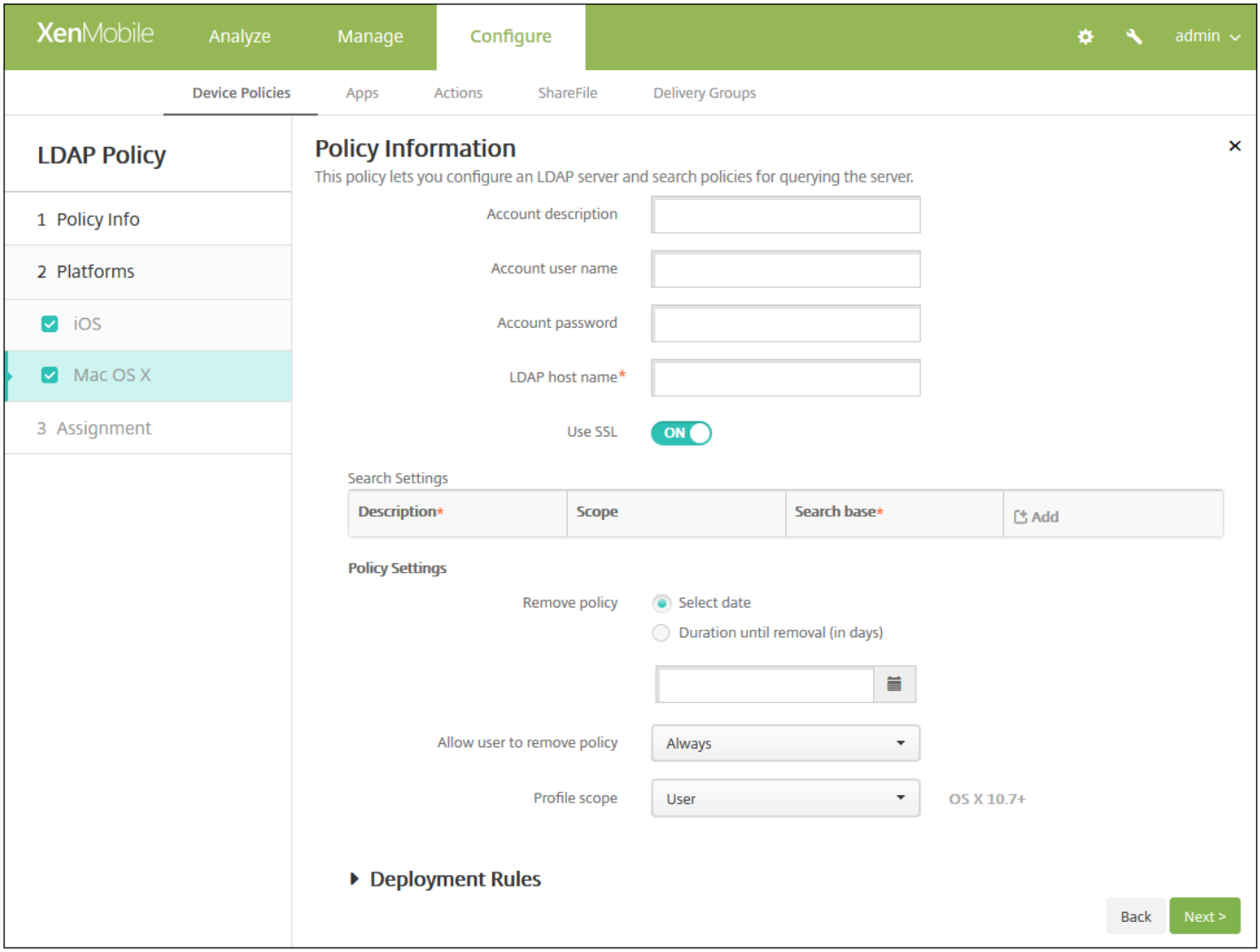
-
-
-
-
-
-
-



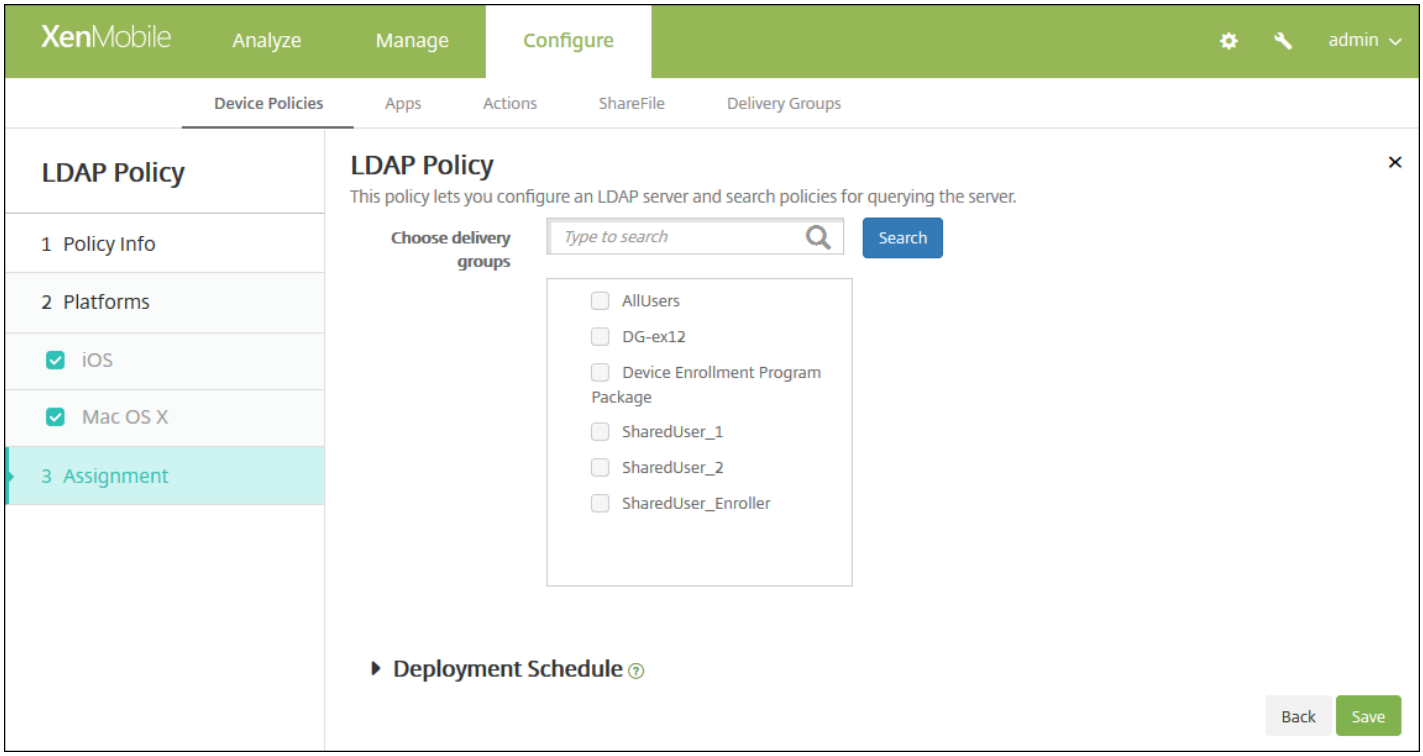
-
-



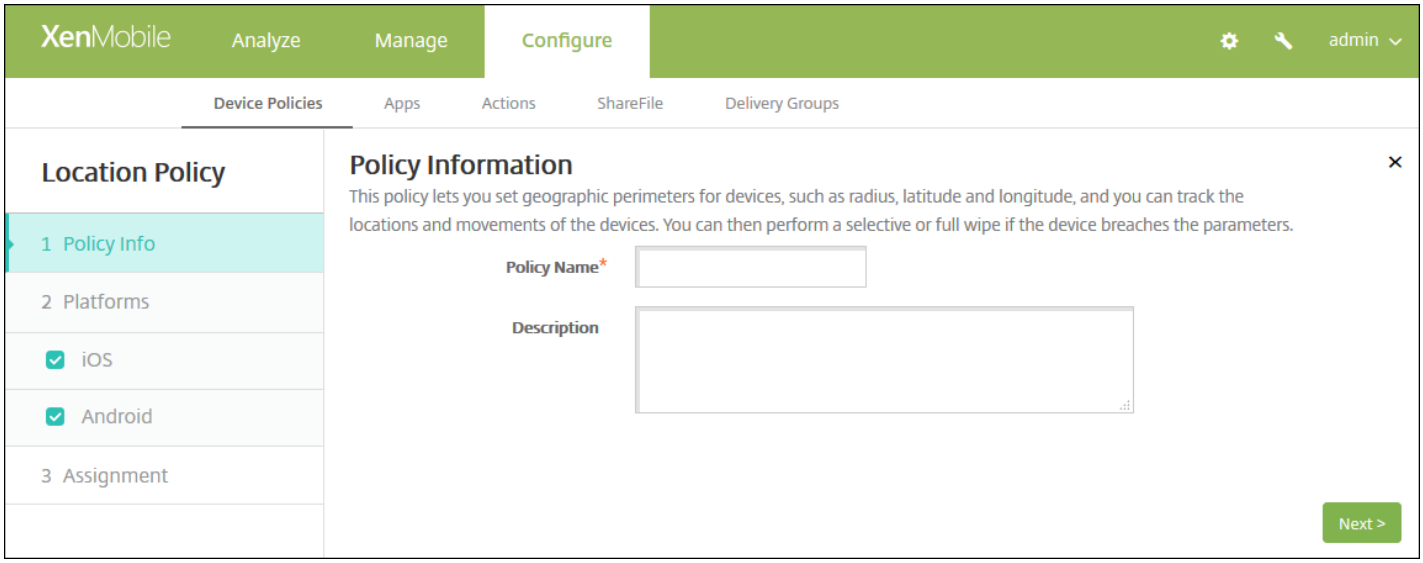
-
-
-
-
-
-
  -
  -
    -
    -



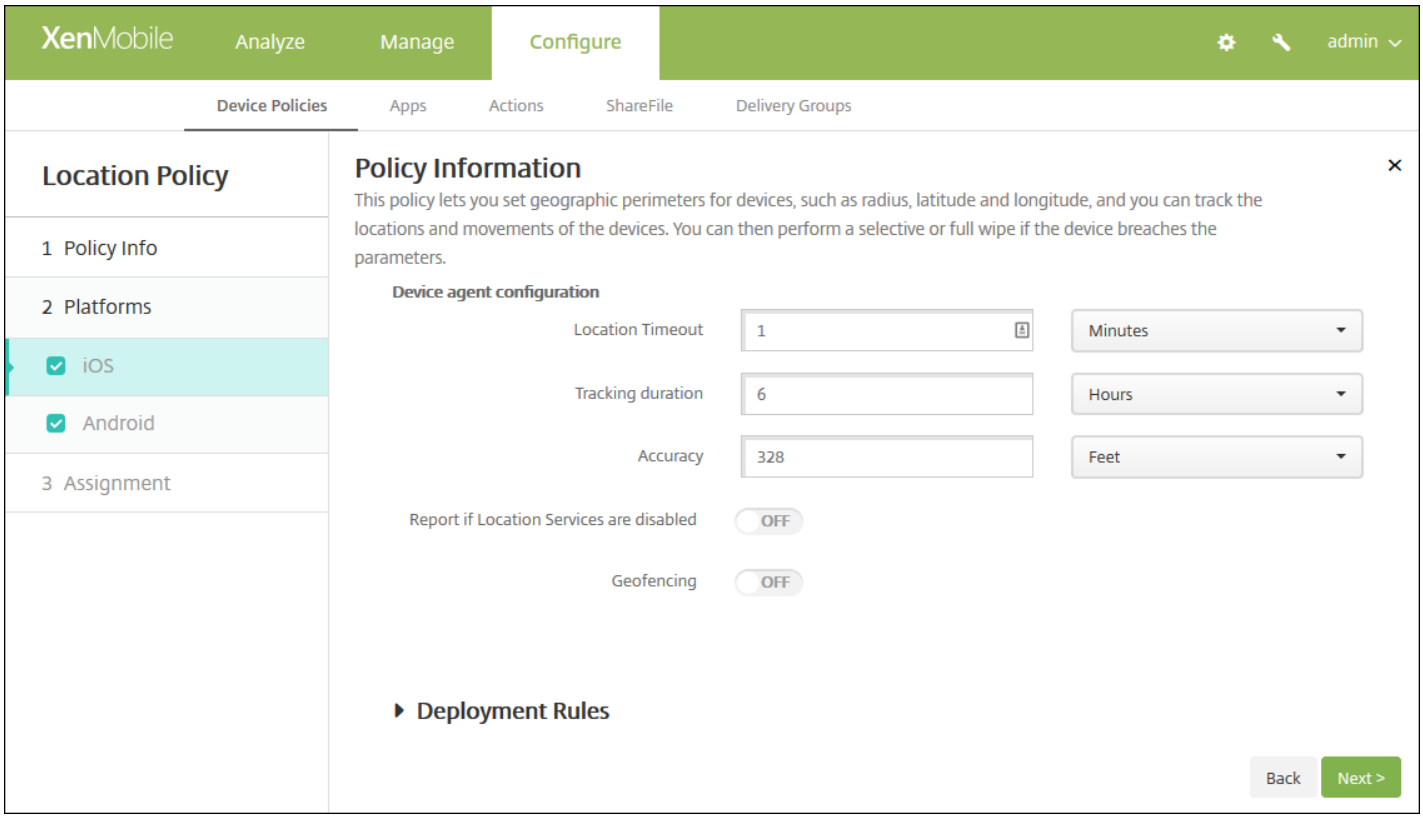
-
-
-
-
-
-
  -
  -
    -
    -

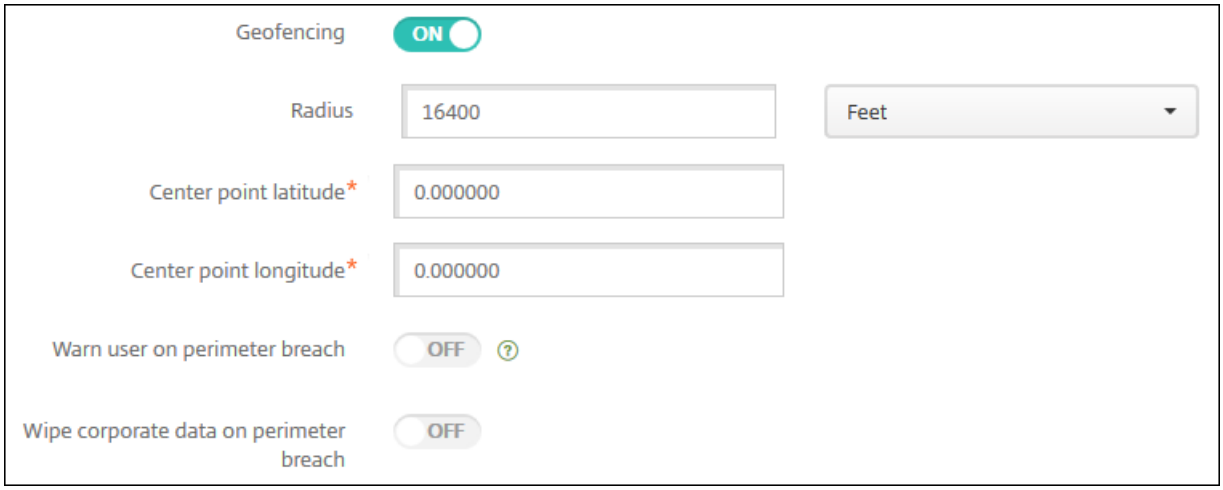


-
-
-
-
-
-
-

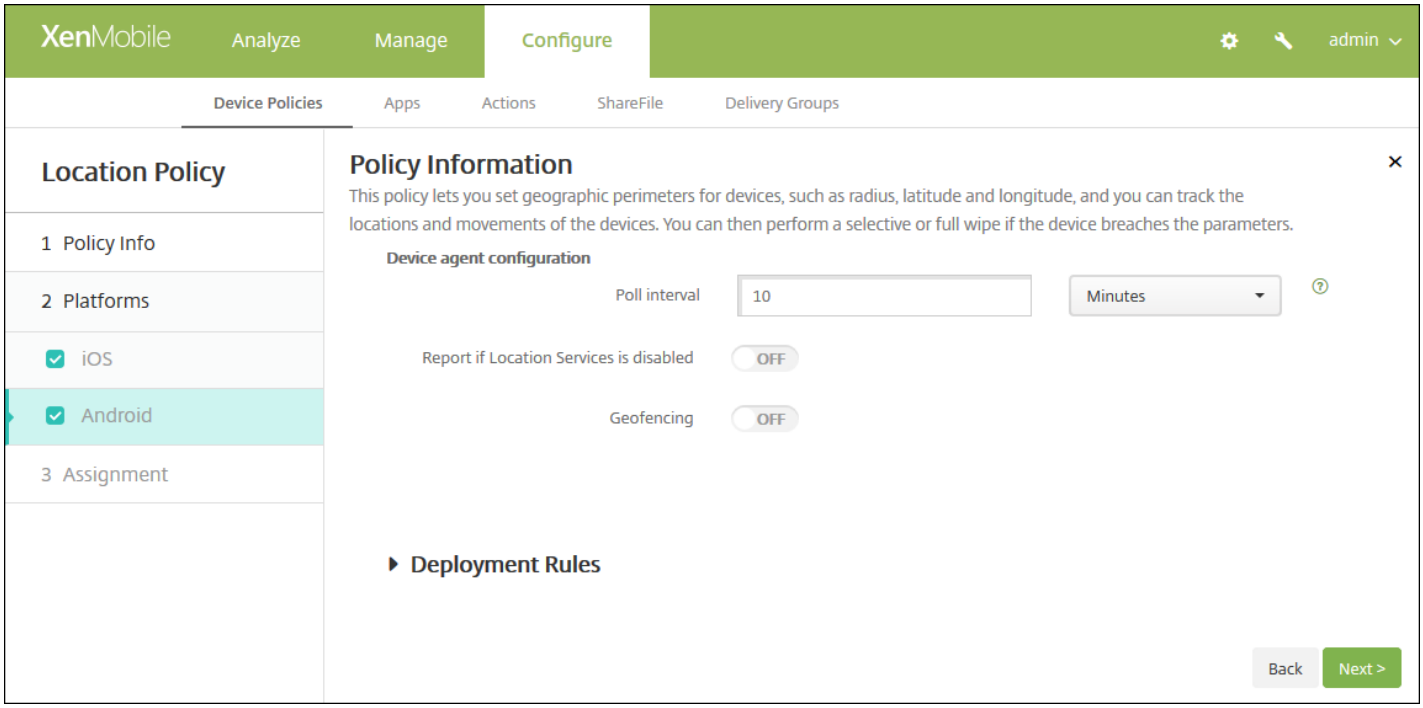


-
-





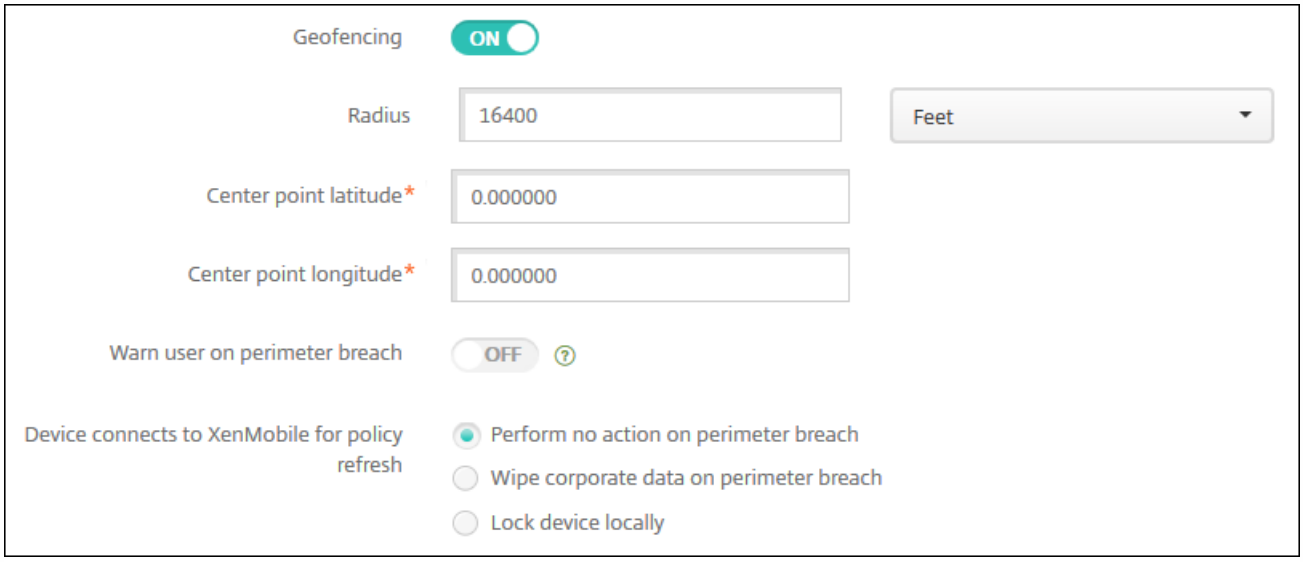
-
  -
  -
  -
  -
-
-
-
-
  -

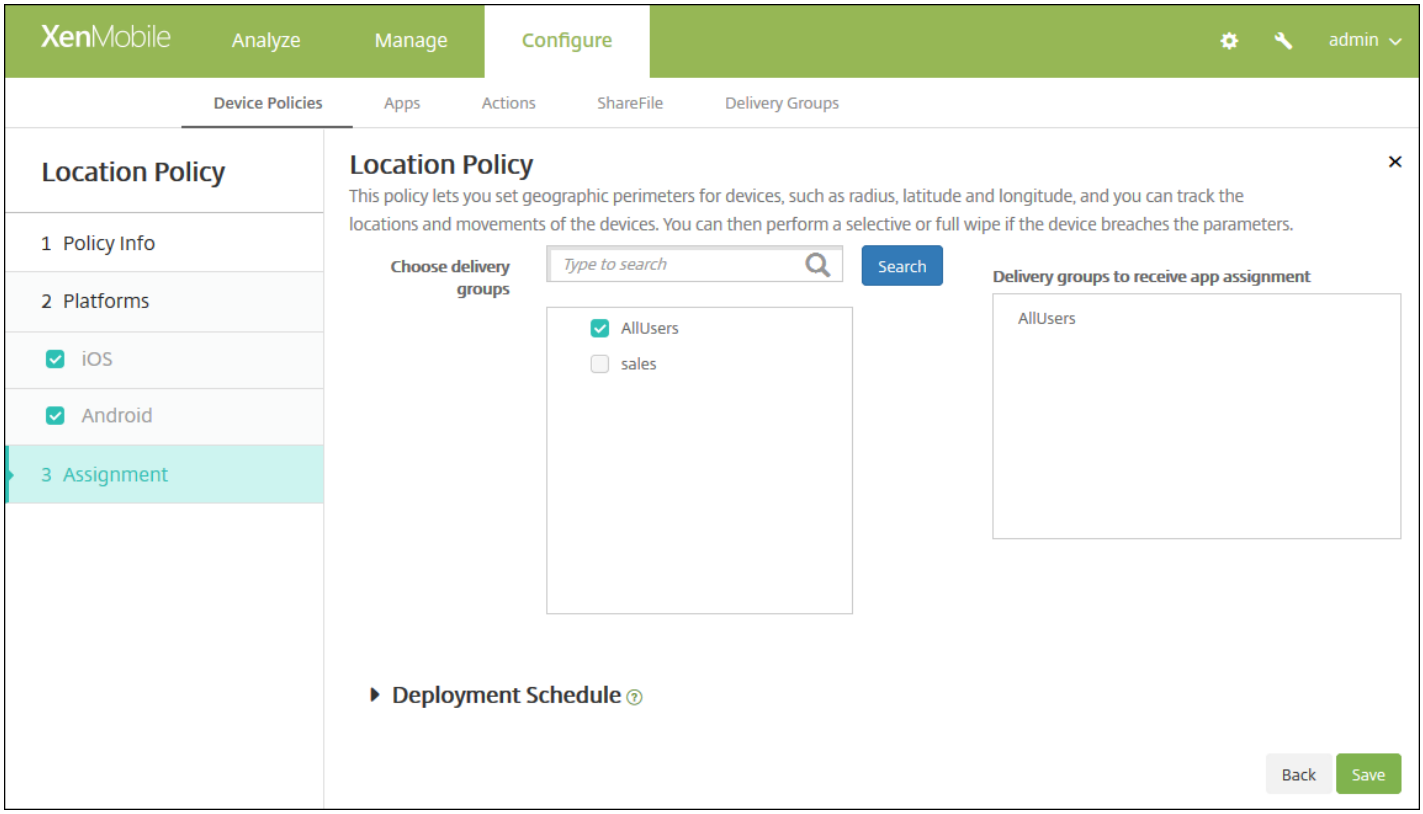


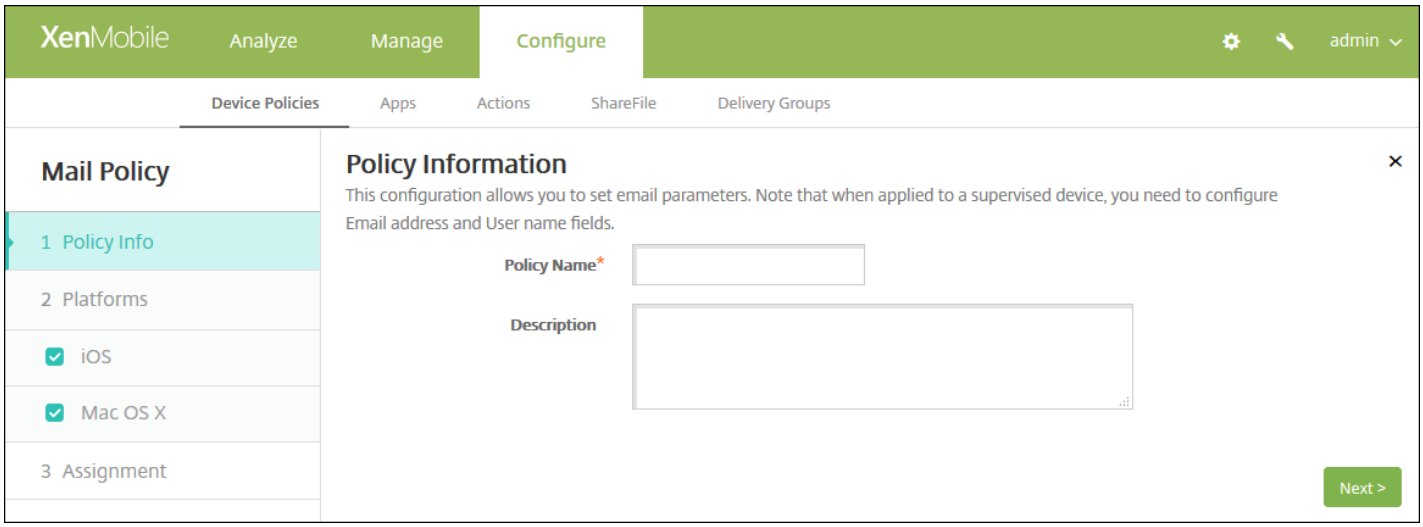
-

-

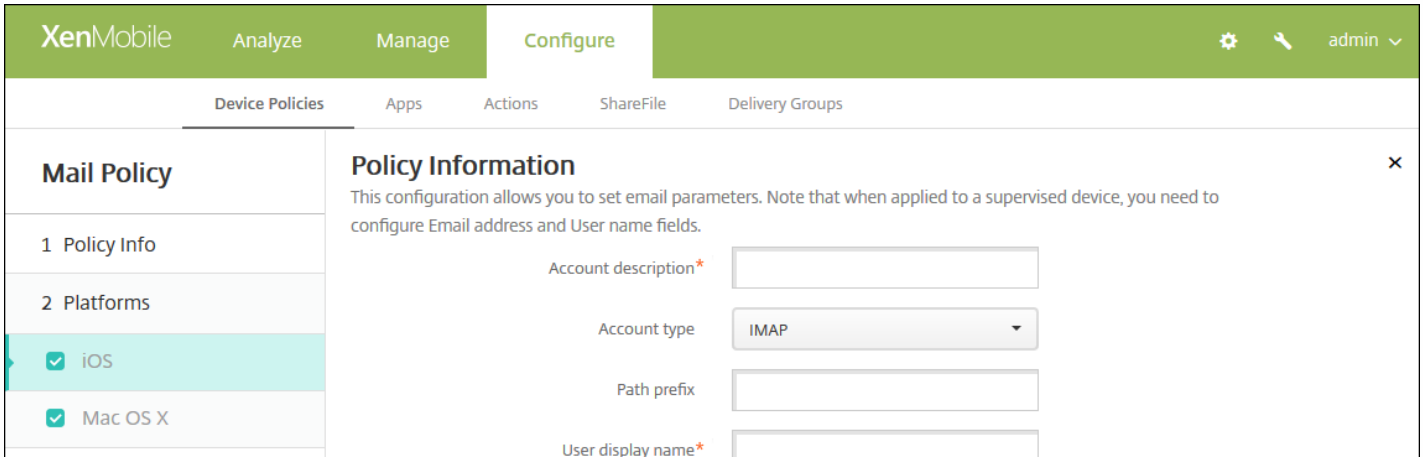
-

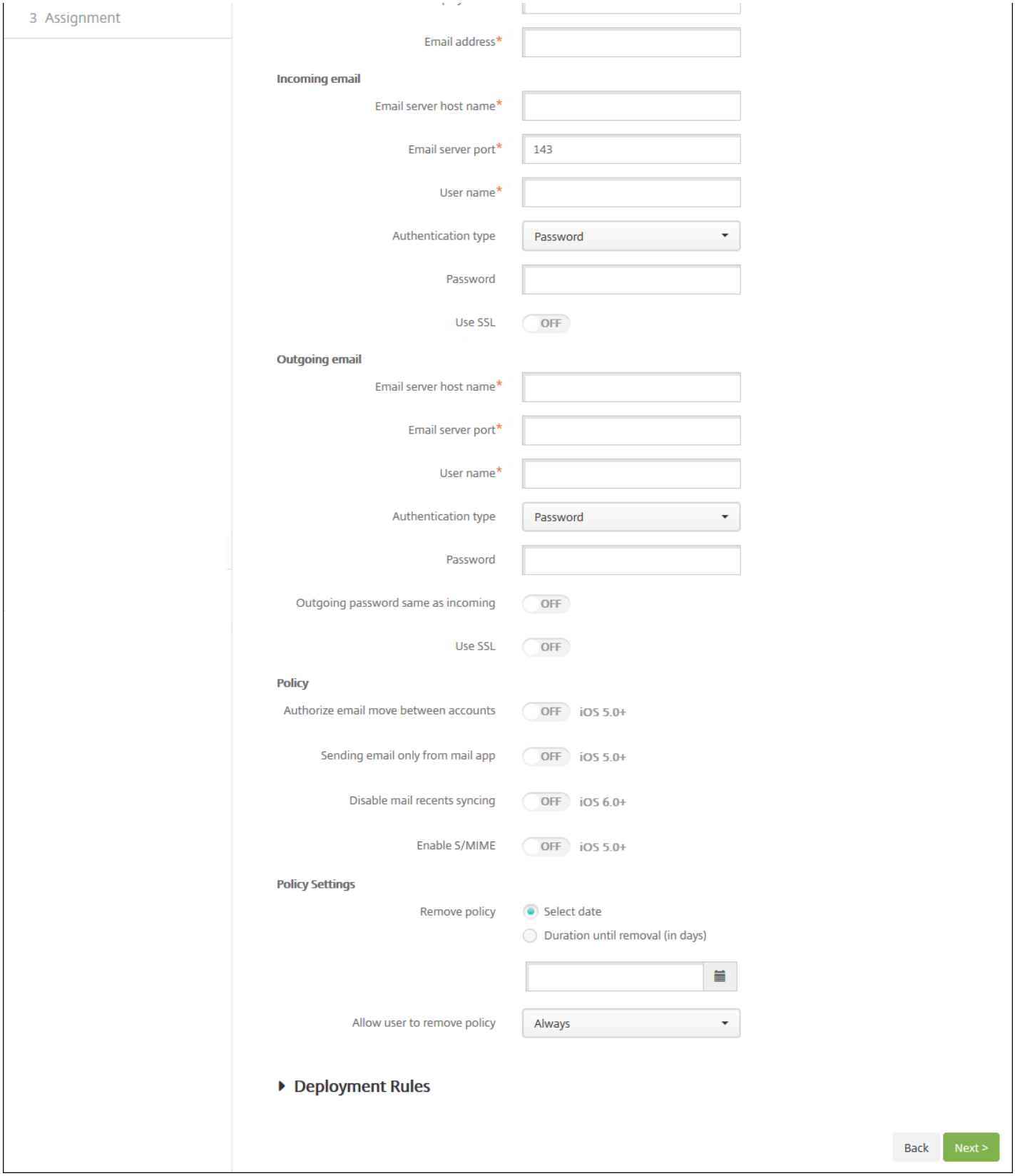






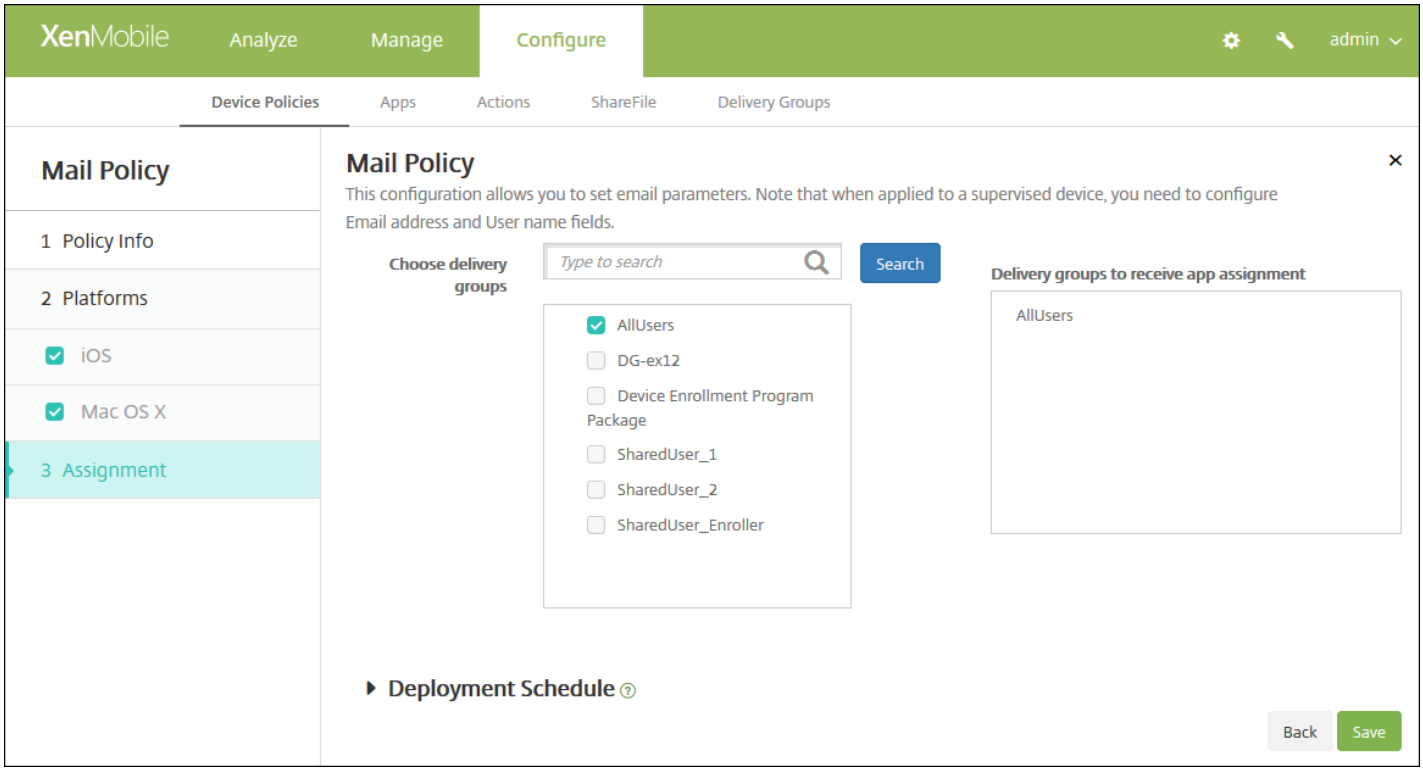
-
-



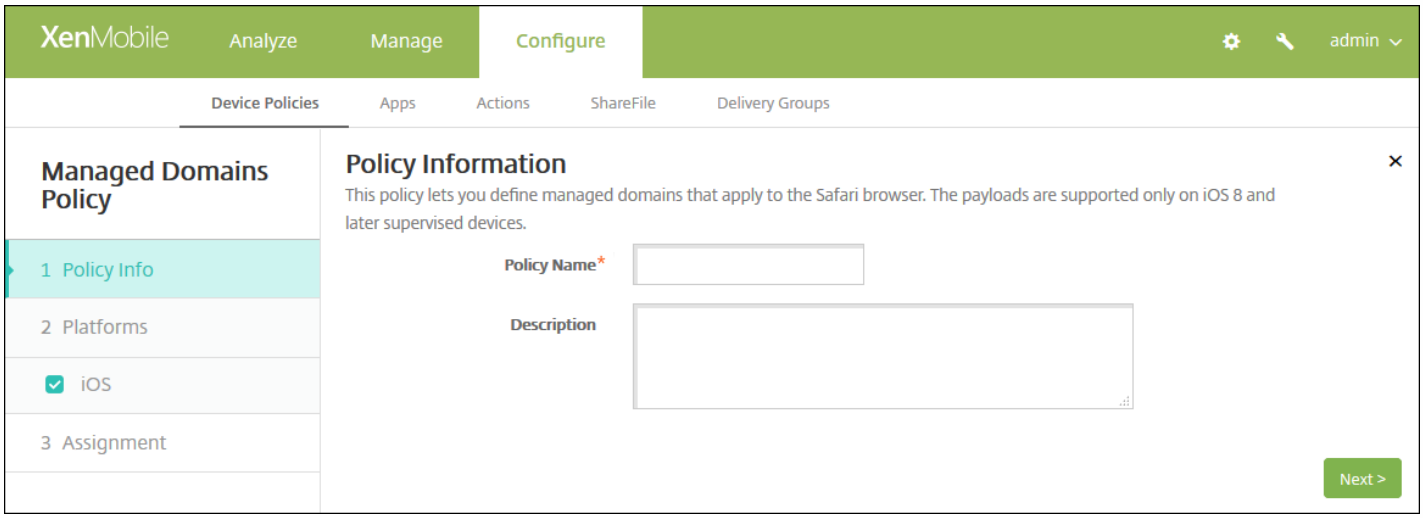


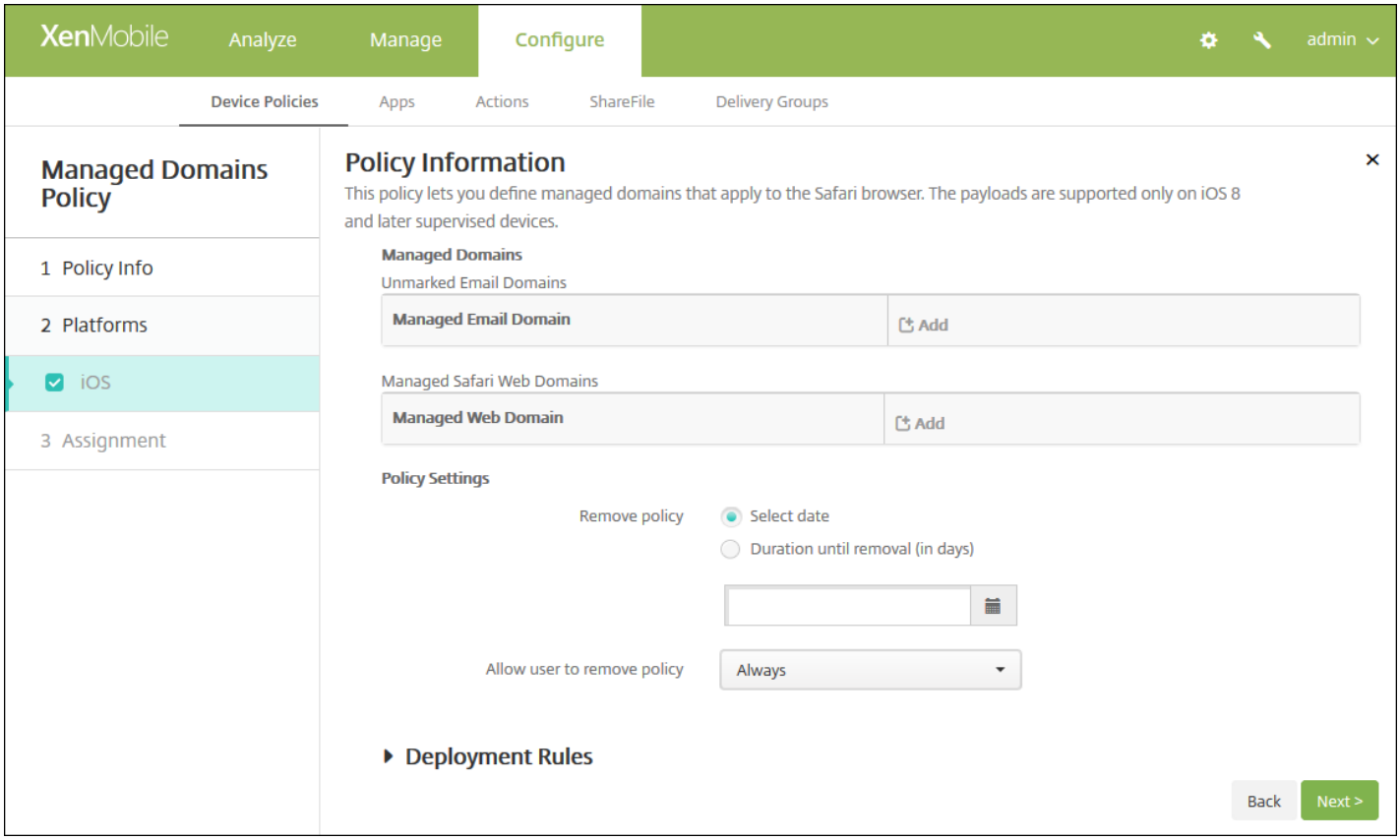
-
-
-
-
-
-
-
  -
  -
  -
  -
  -
  -
-
  -
  -
  -
  -
  -
  -
-
  -

-
-
-
-
-
-
-
  -
  -
  -
  -
  -
  -

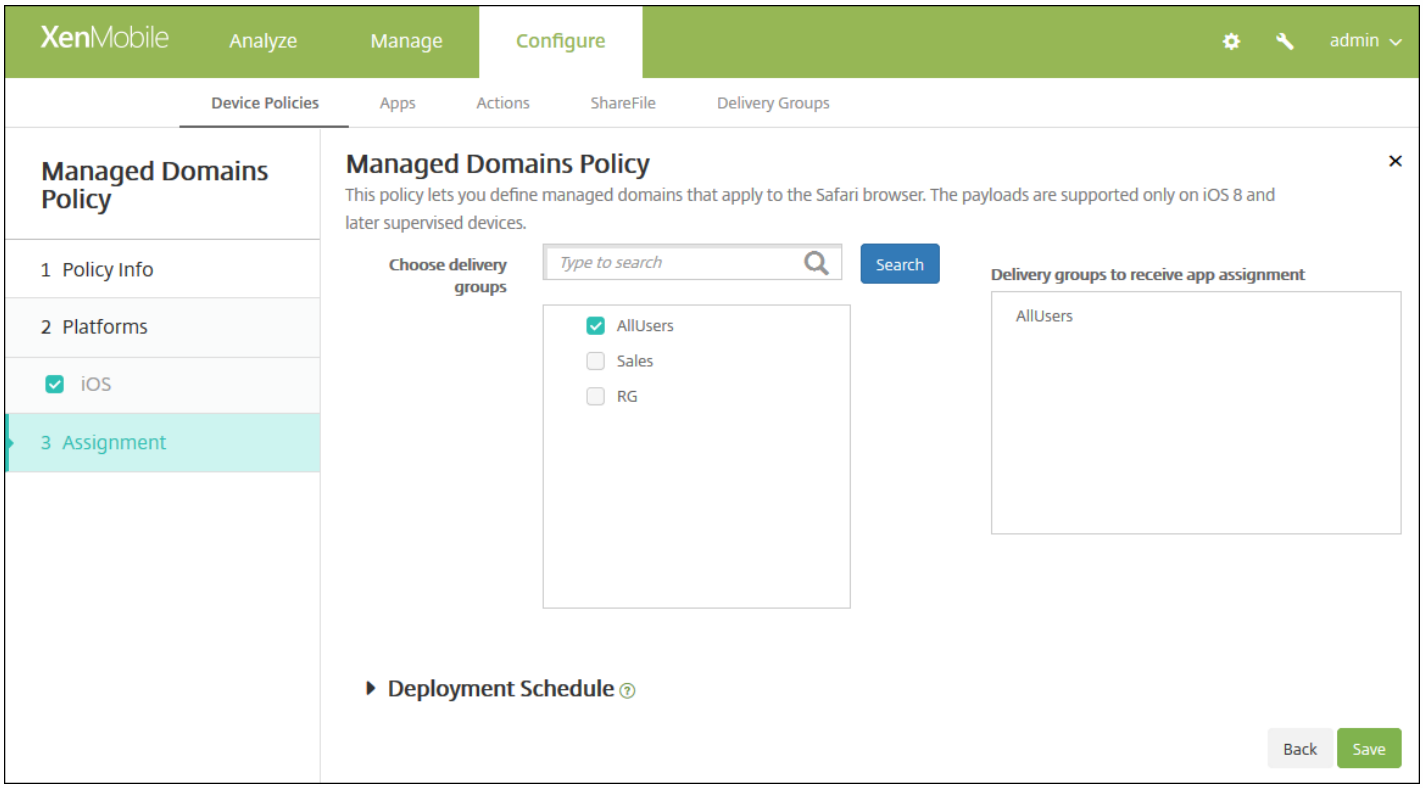


-
-
-
-
-
-
-



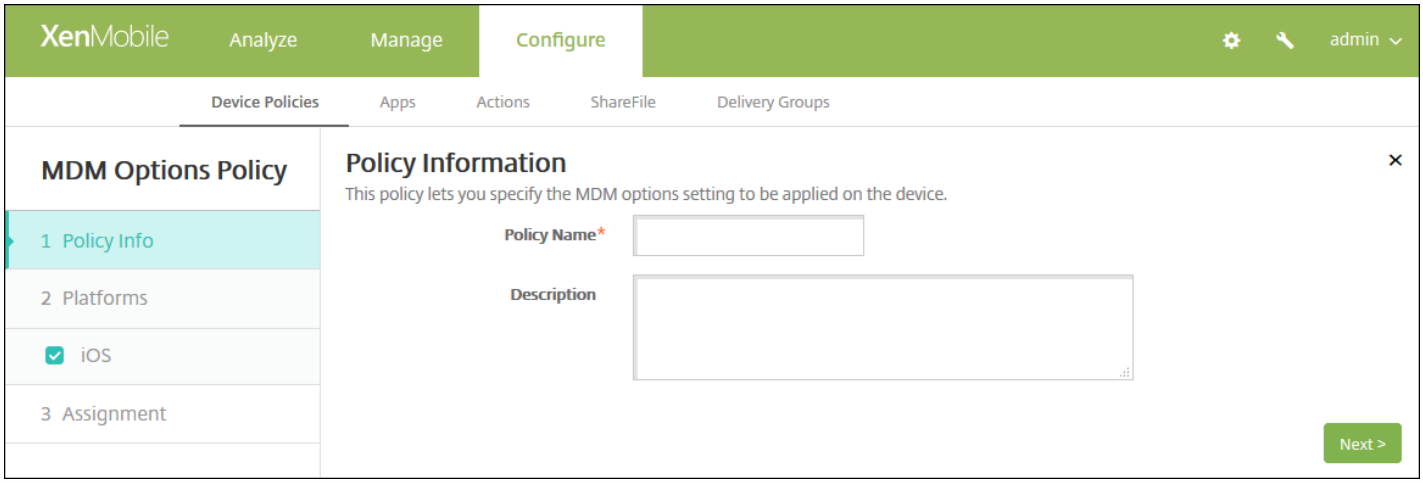


-
  -
  -
  -
  -

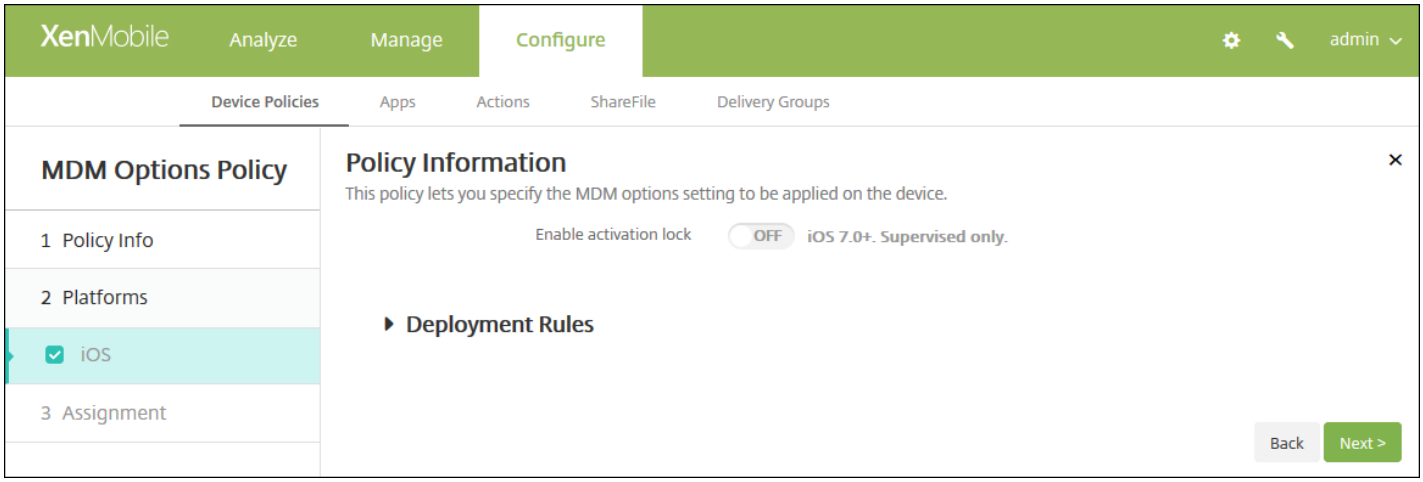


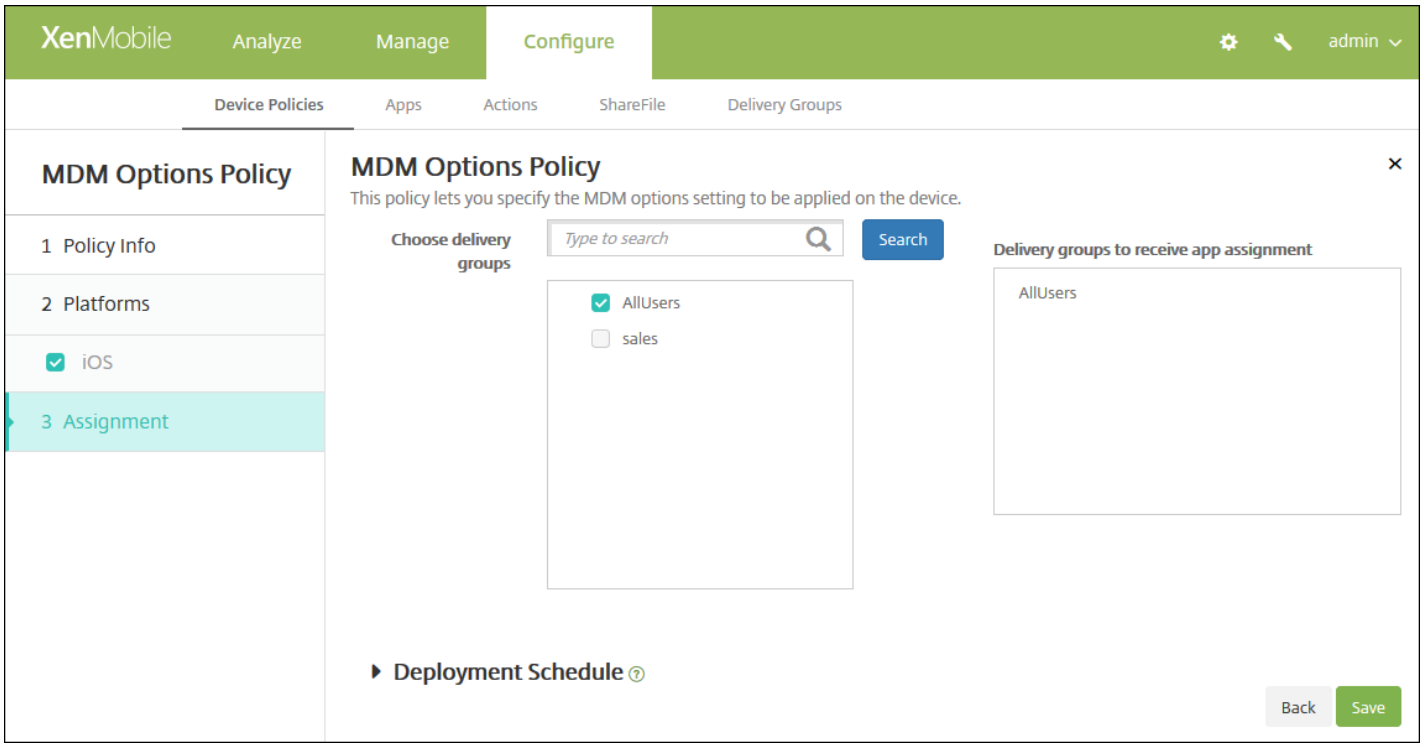
-

-
-
-
-
-
-

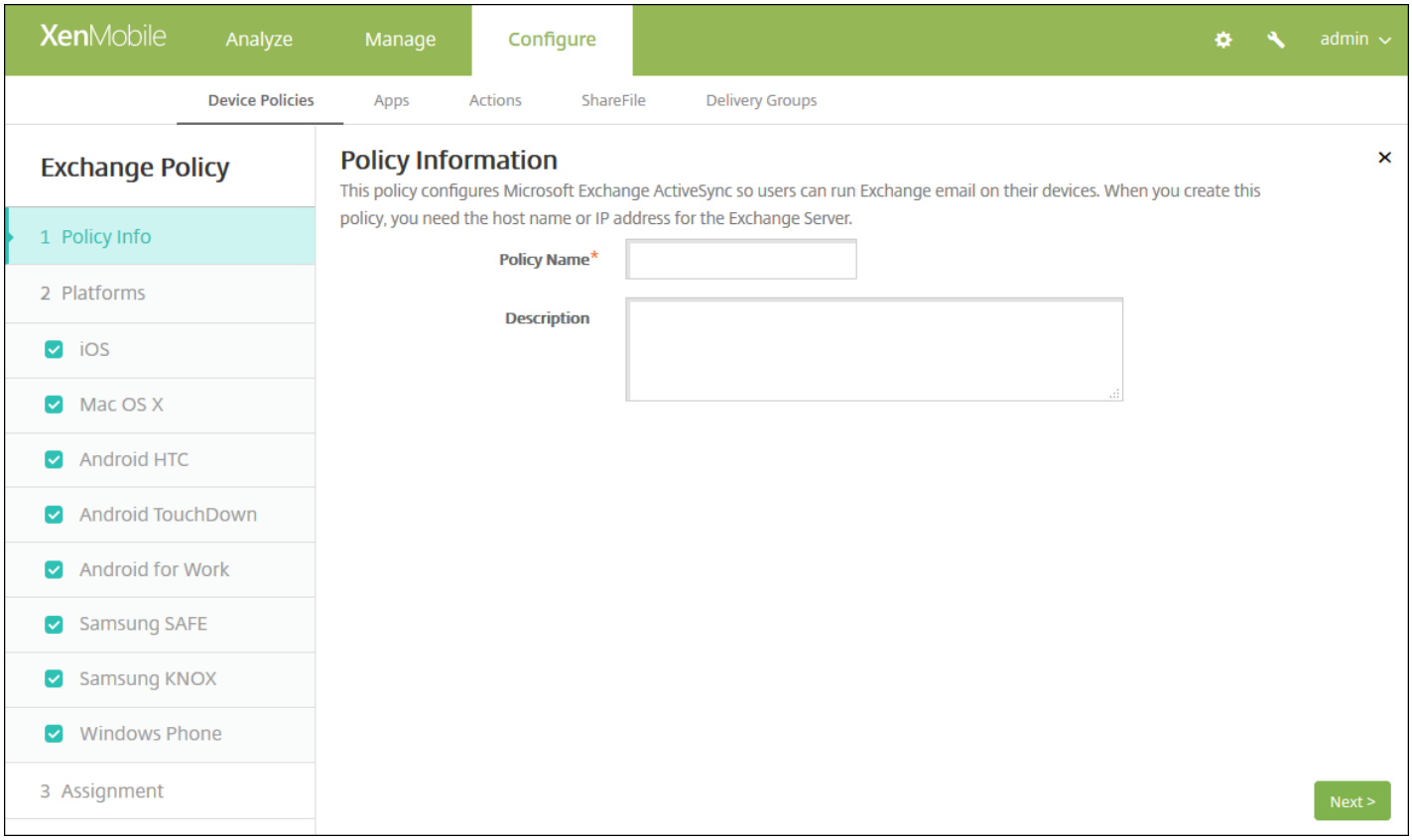


-
-

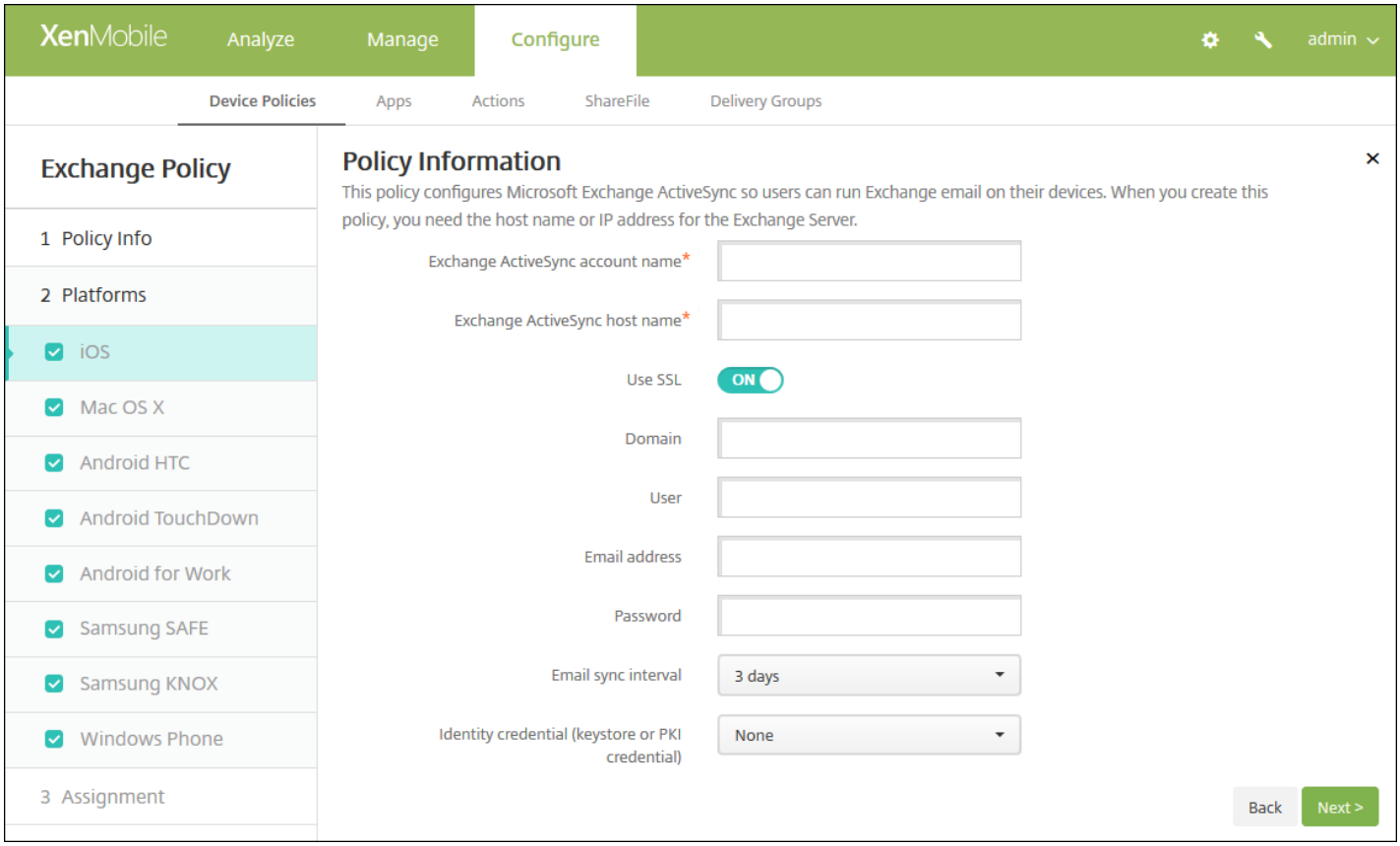




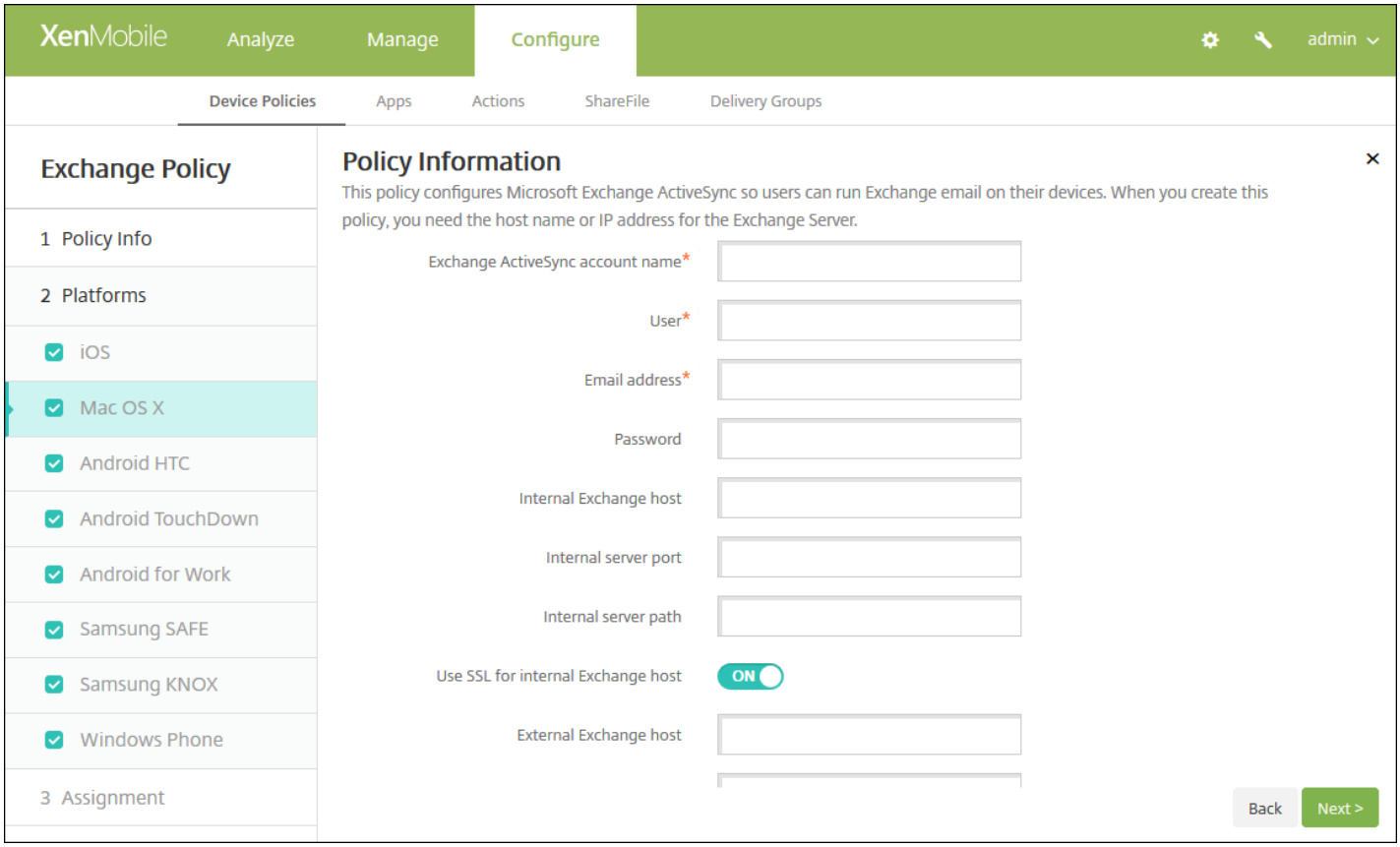
-
-
-
-
-
-
-



-
-

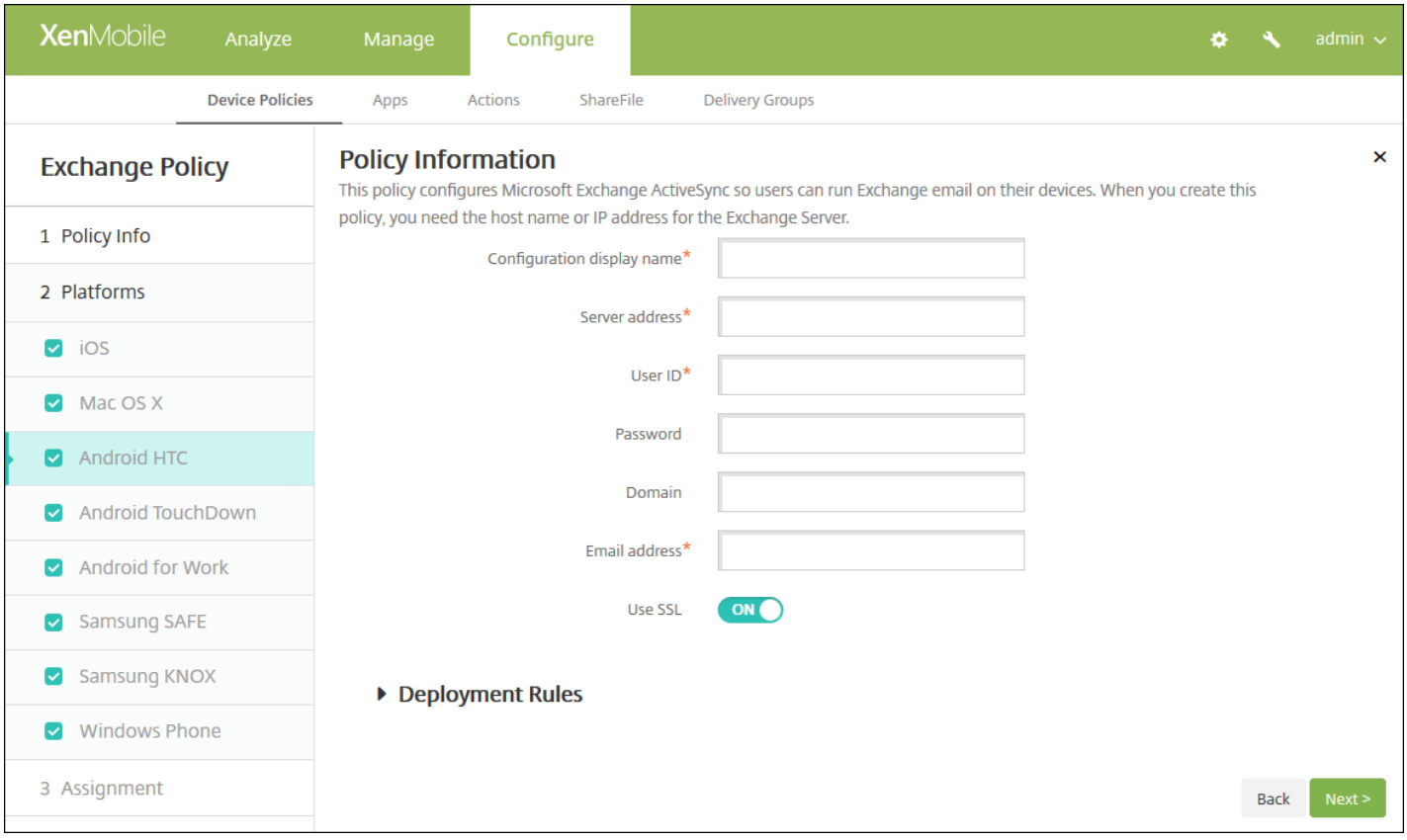


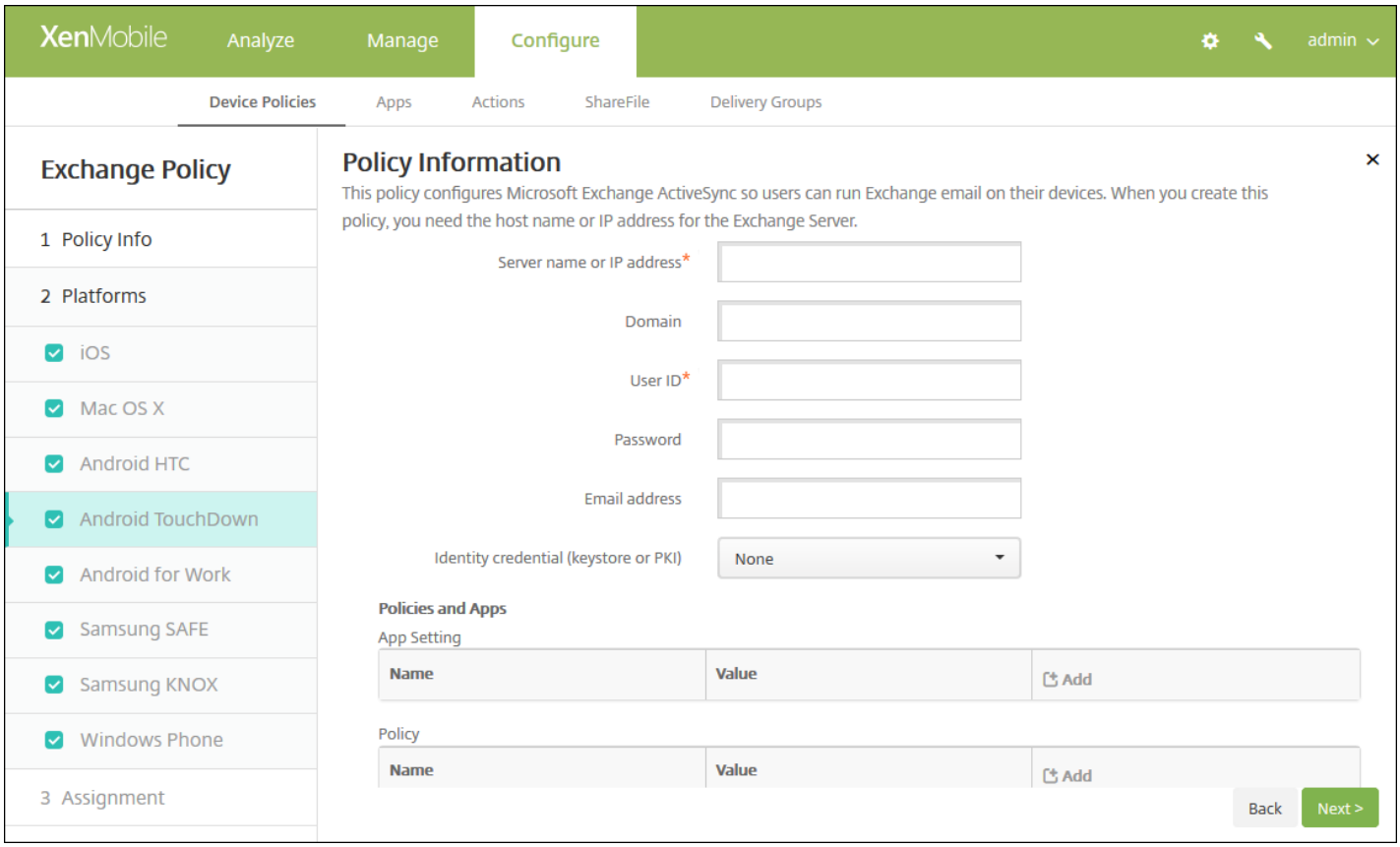
-
-
  -
  -
-

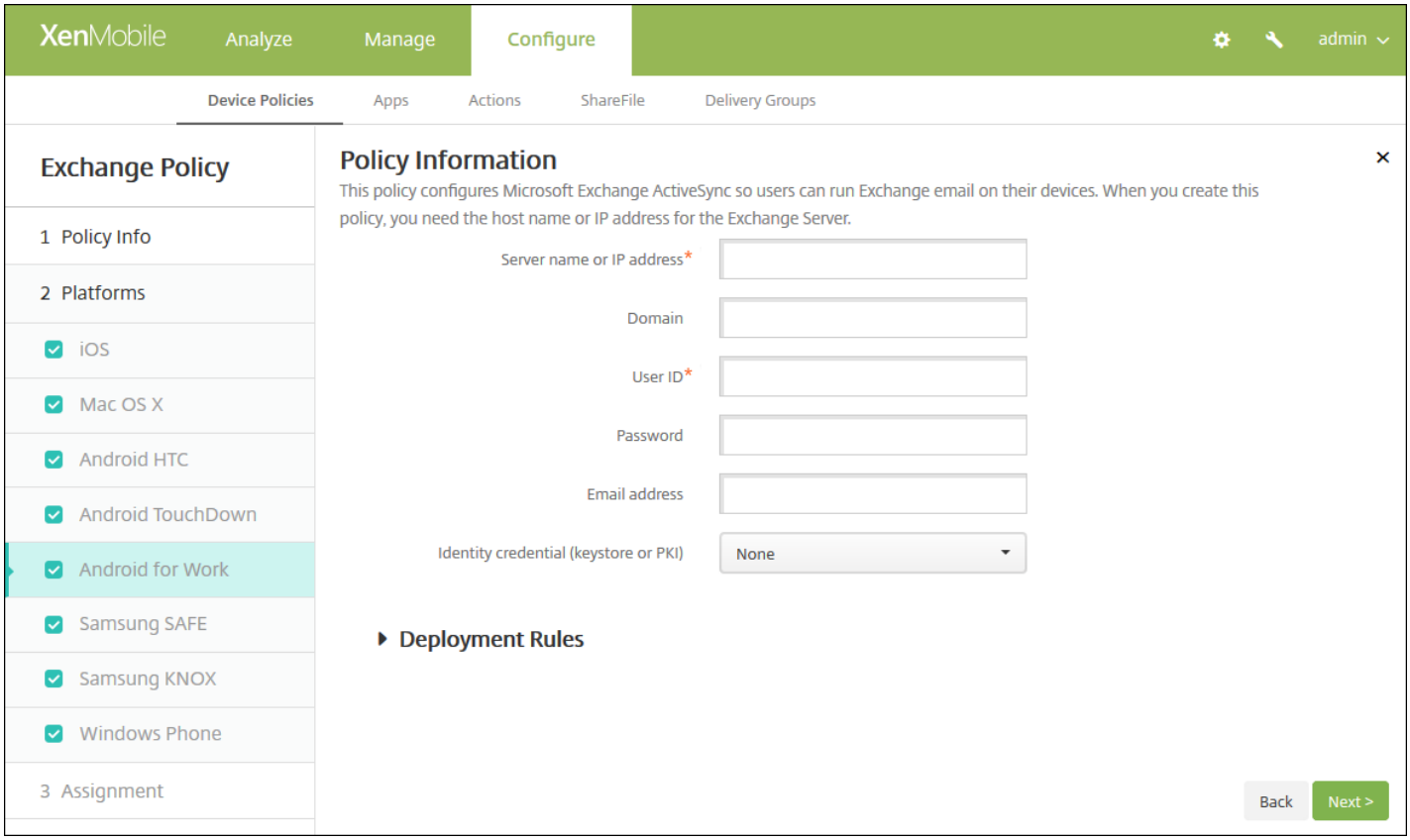


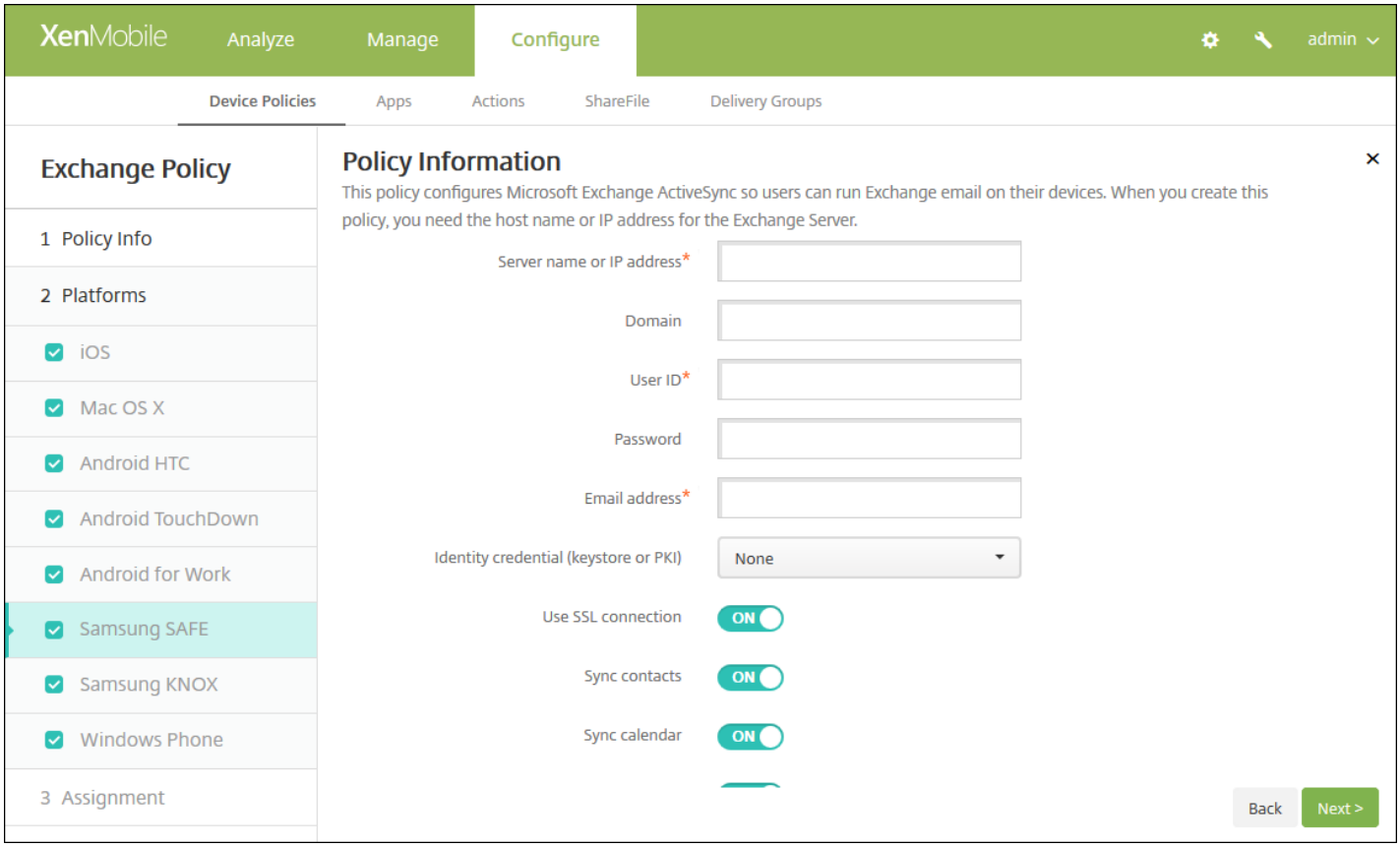
-
-
-

-
-
-
-
-
-
-
-
-
-

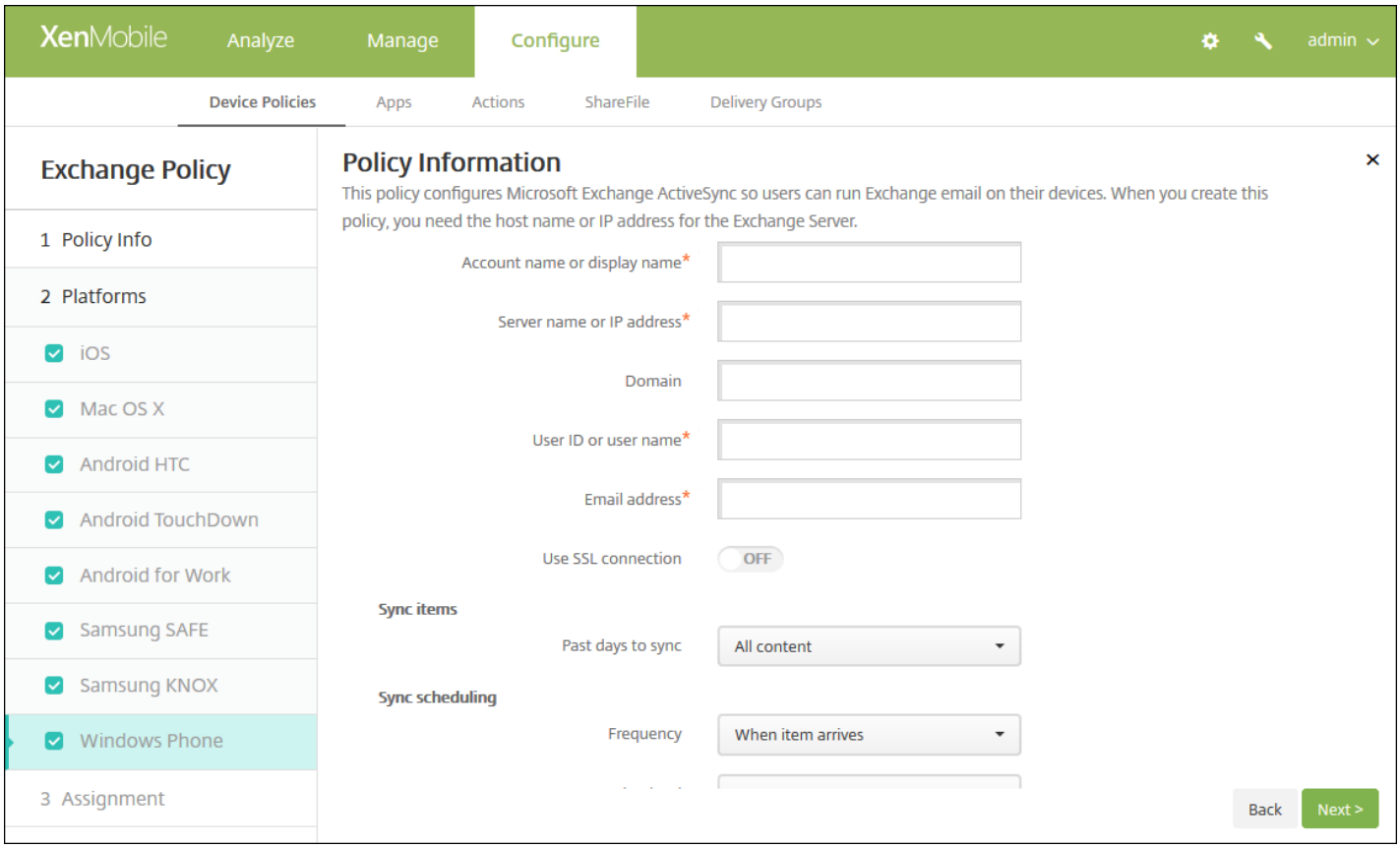






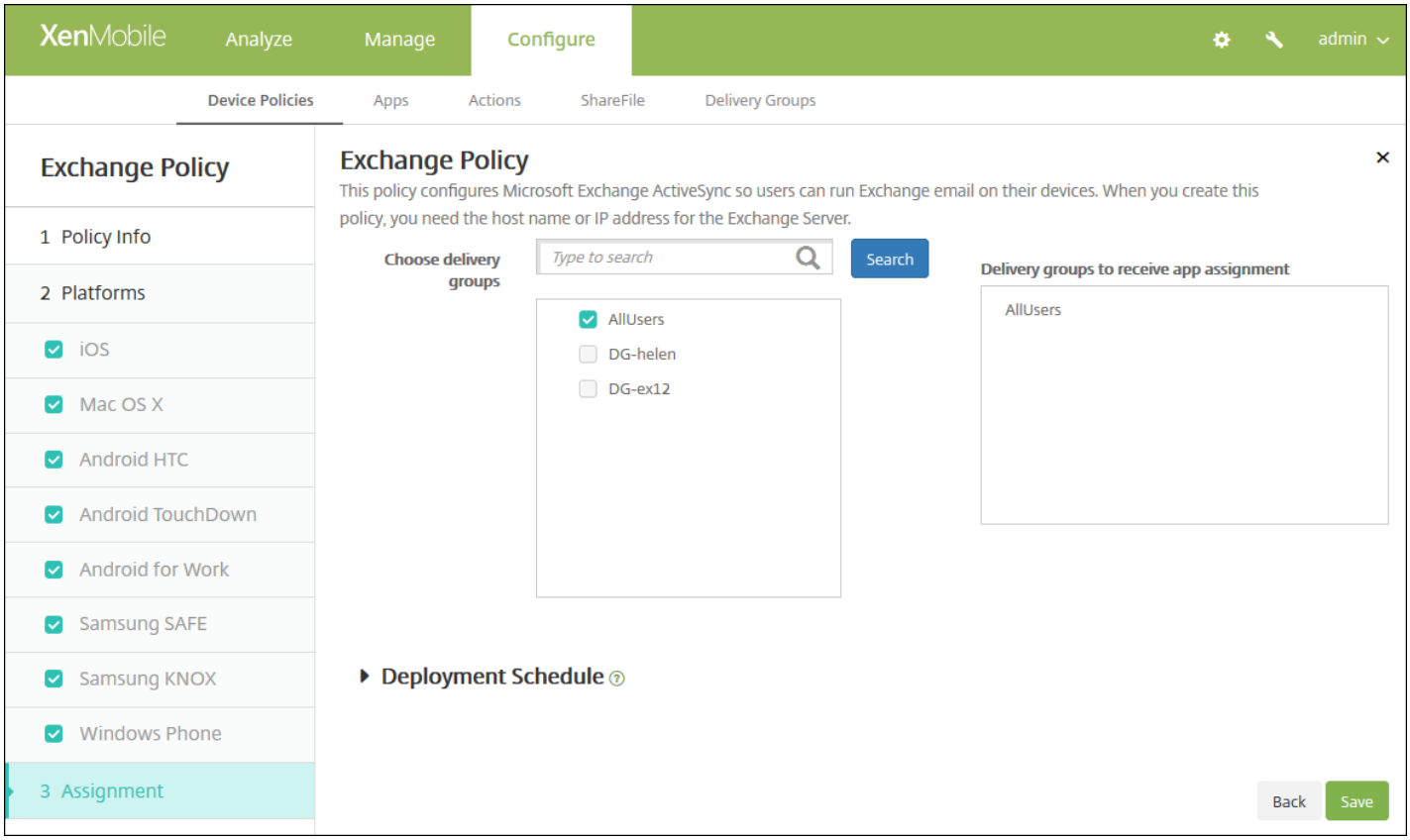


-
-
-
-

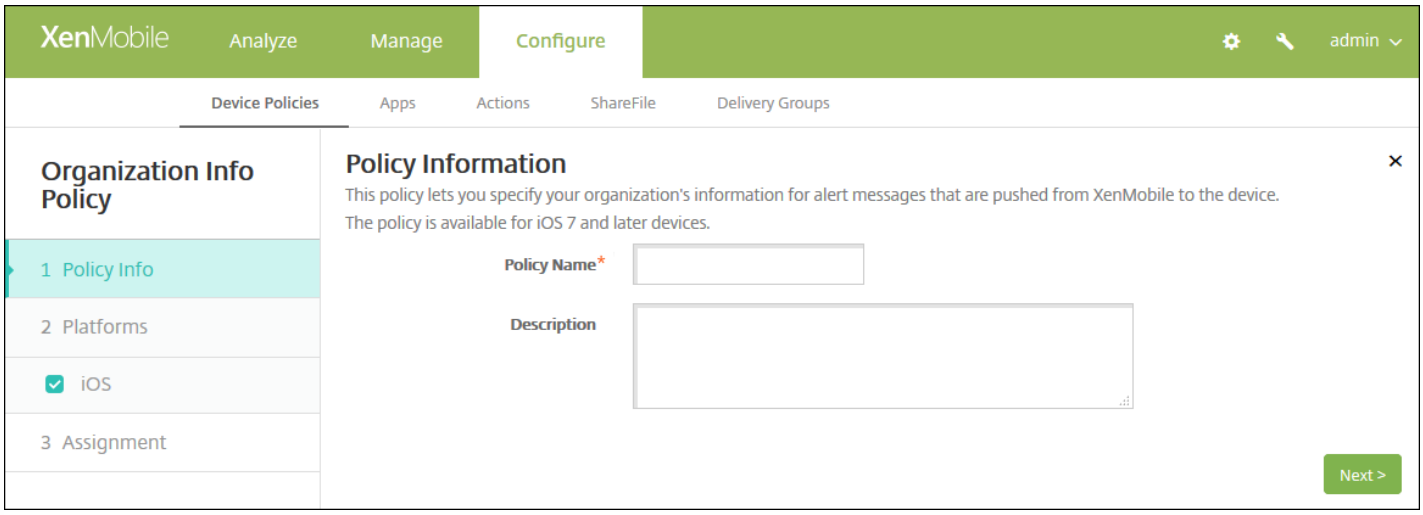


-
-
-
-

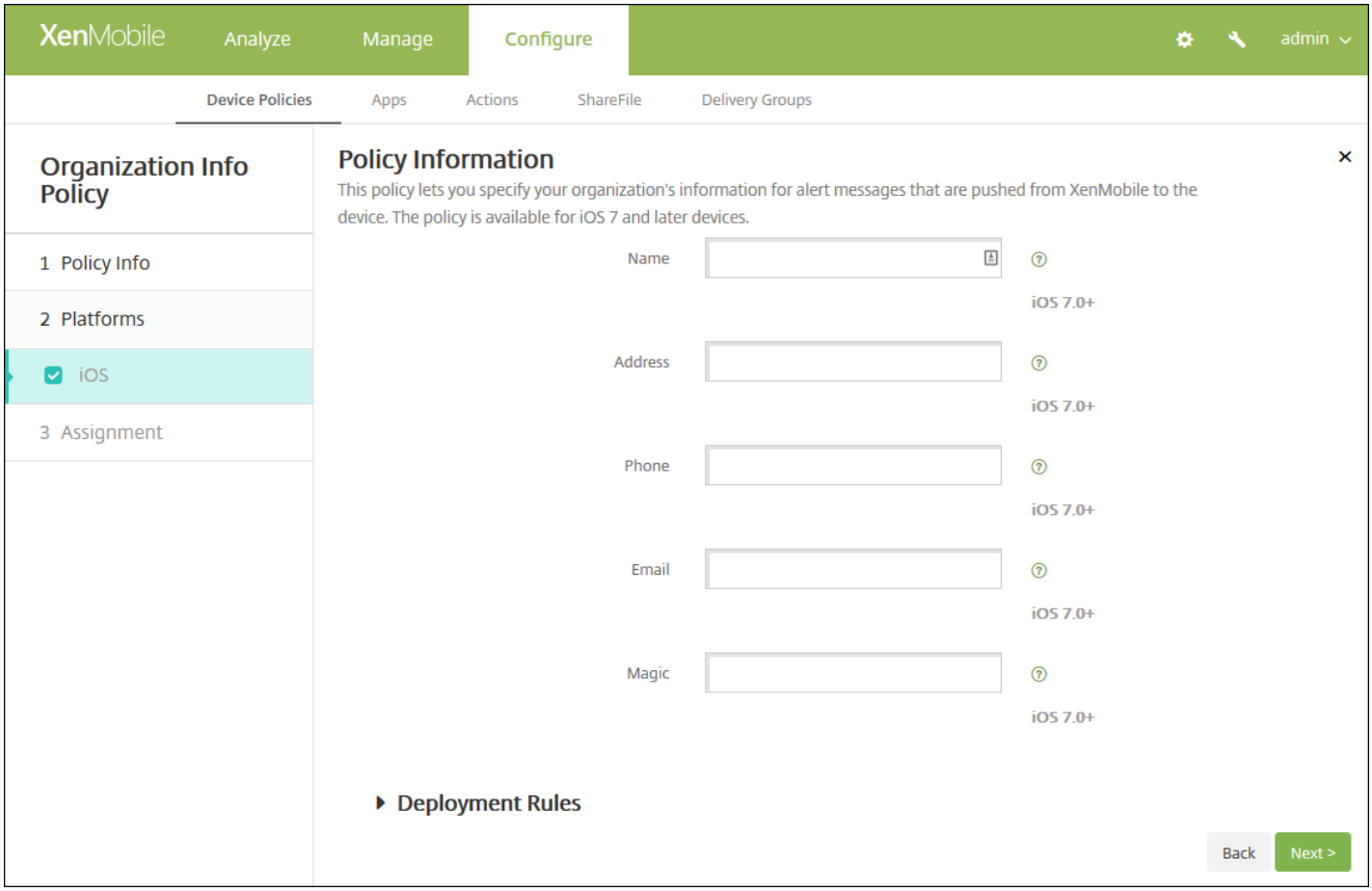
-
-
-
-
-



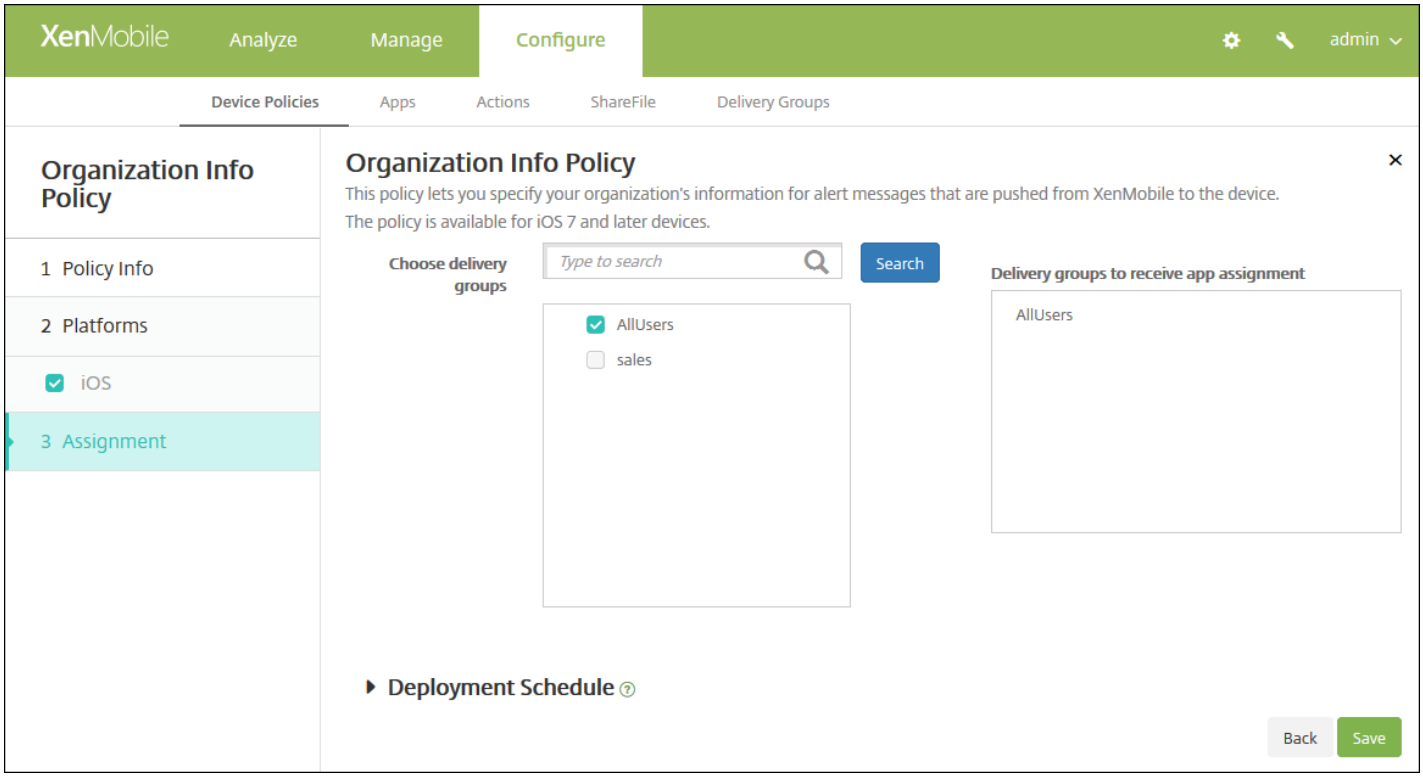
-
-
-
-
-
-
-



-
-



-
-
-
-
-



Stratégies de code secret

Jul 27, 2016

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, Mac OS X, Android, Samsung KNOX, Android for Work, Windows Phone et Windows Desktop/Tablet. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

Paramètres iOS

Paramètres Mac OS X

Paramètres Android

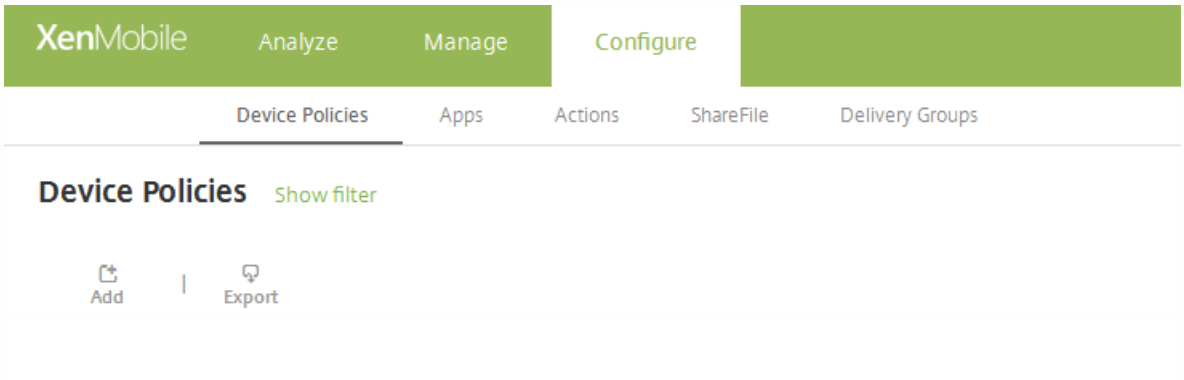
Paramètres Samsung KNOX

Paramètres Android for Work

Paramètres Windows Phone

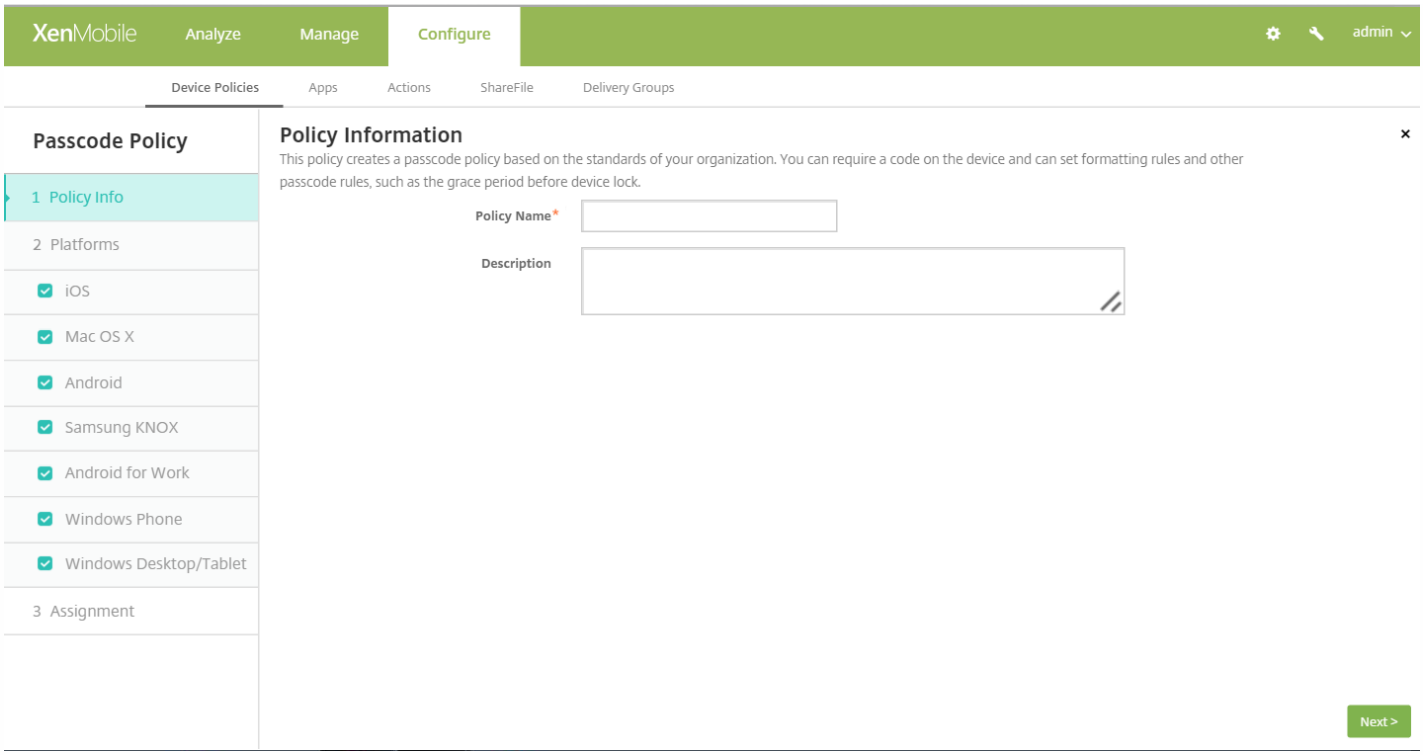
Paramètres Windows Desktop/Tablet

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.



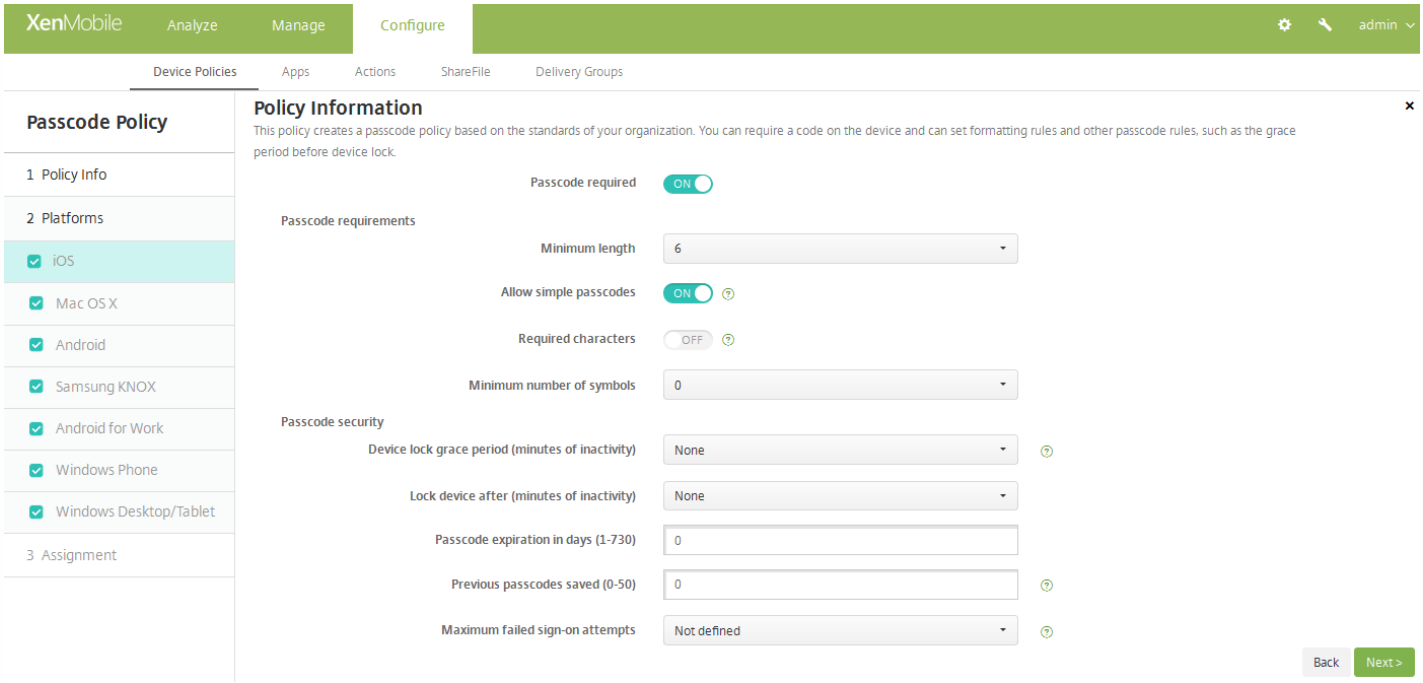
4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

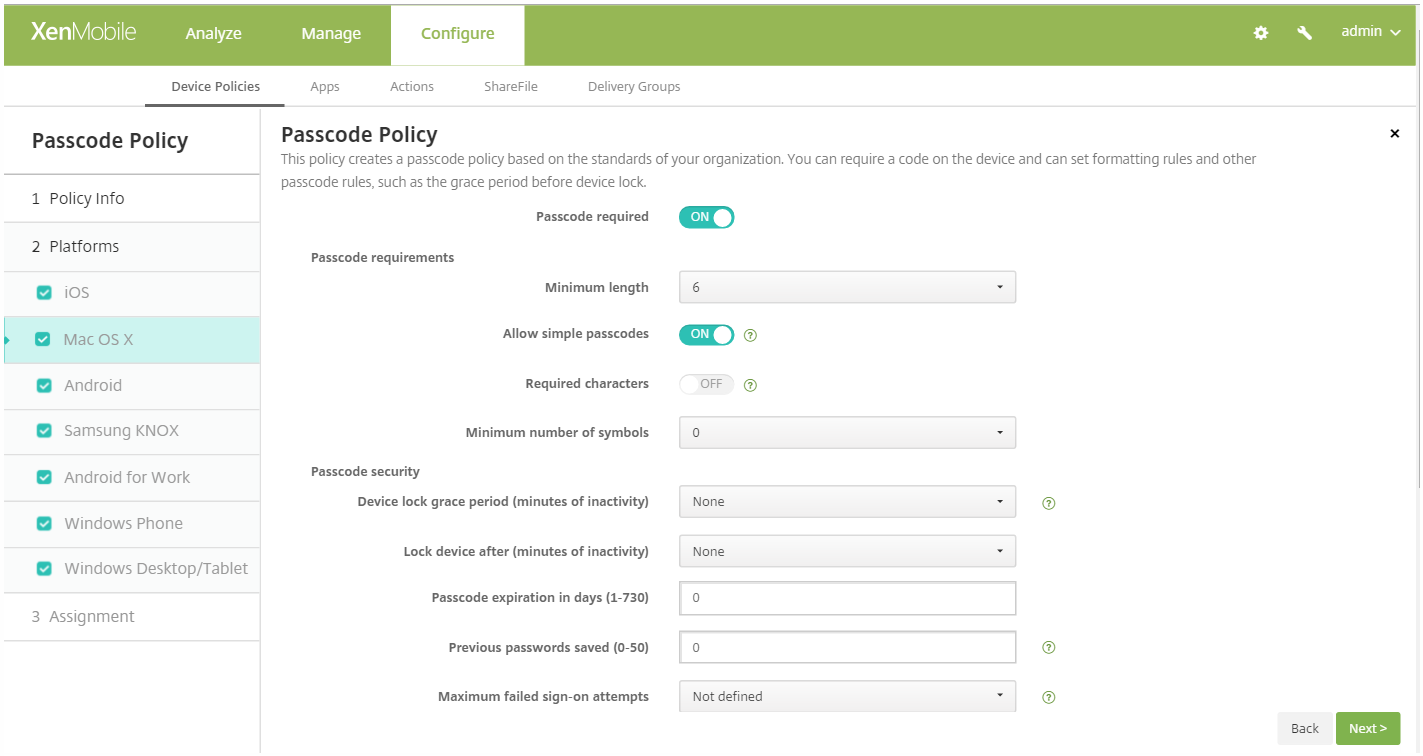
Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.



Configurez les paramètres suivants :

- **Code secret requis** : sélectionnez cette option pour exiger la saisie d'un code secret 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.
- **Conditions requises pour les codes secrets**
  - **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 **ON**.
  - **Caractères requis** : sélectionnez cette option pour exiger que les codes secrets contiennent au moins une lettre. La valeur par défaut est **OFF**.
  - **Nombre minimum de symboles** : dans la liste, cliquez sur le nombre de symboles que le code secret doit contenir. La valeur par défaut est de **0**.
- **Sécurité des codes secrets**
  - **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 **Aucune**.
  - **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 subit un effacement complet. La valeur par défaut est **Aucun nombre défini**.
- **Paramètres de stratégie**

- En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
- 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.



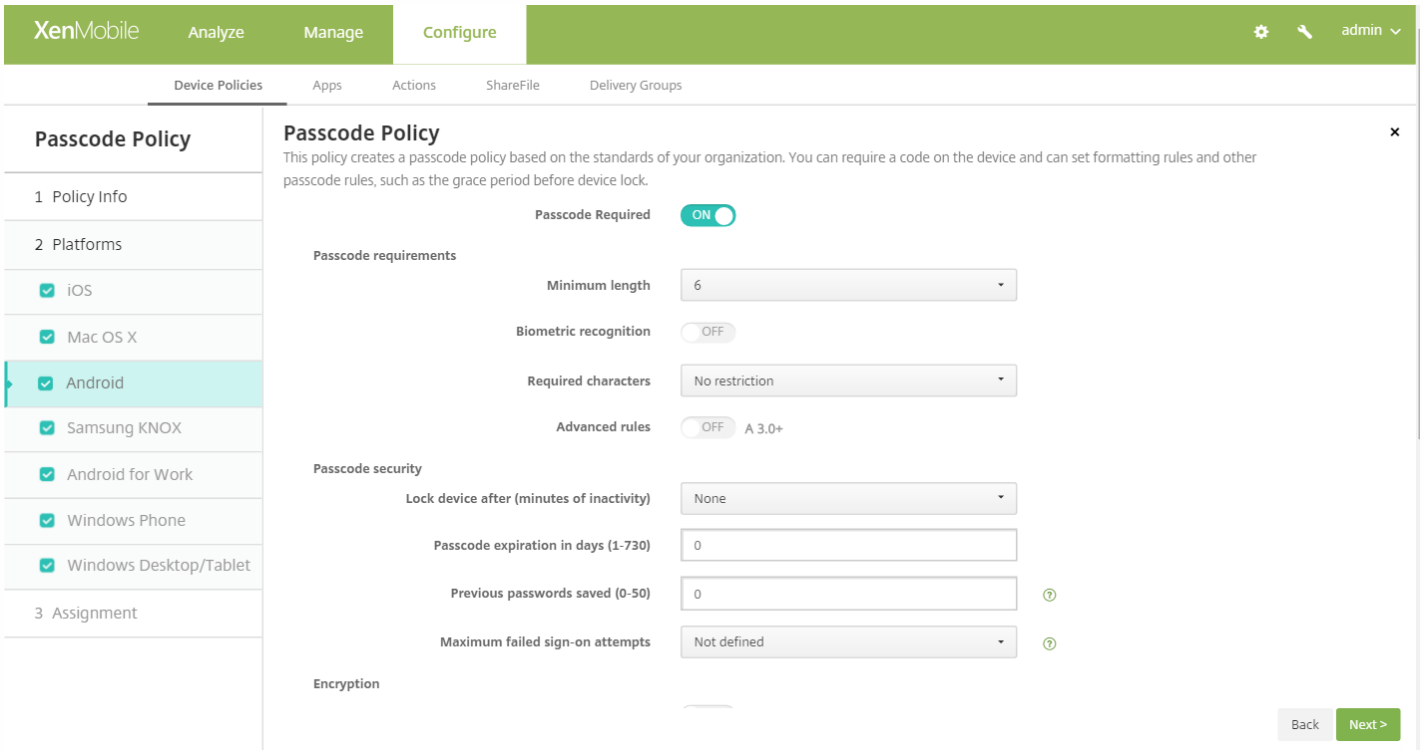
Pour configurer ces paramètres :

- **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 :
- **Conditions requises pour les codes secrets**
  - **Longueur minimale** : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de **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 **ON**.
  - **Caractères requis** : sélectionnez cette option pour exiger que les codes secrets contiennent au moins une lettre. La valeur par défaut est **OFF**.
  - **Nombre minimum de symboles** : dans la liste, cliquez sur le nombre de symboles que le code secret doit contenir. La valeur par défaut est de **0**.
- **Sécurité des codes secrets**
  - **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

Aucune.

- **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 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.

- Paramètres de stratégie
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - 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.
  - En regard de **Étendue du profil**, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur OS X 10.7 et versions ultérieures.



Pour configurer ces paramètres :

Remarque : le paramètre par défaut pour Android est **OFF**.

- **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, chiffrement et Samsung SAFE.
- **Conditions requises pour les codes secrets**
  - **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 **OFF**.
  - **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 **OFF**.
  - 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 des codes secrets**
  - **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**.
- **Chiffrement**
  - **Activer le chiffrement** : sélectionnez cette option si vous souhaitez activer le cryptage. 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.

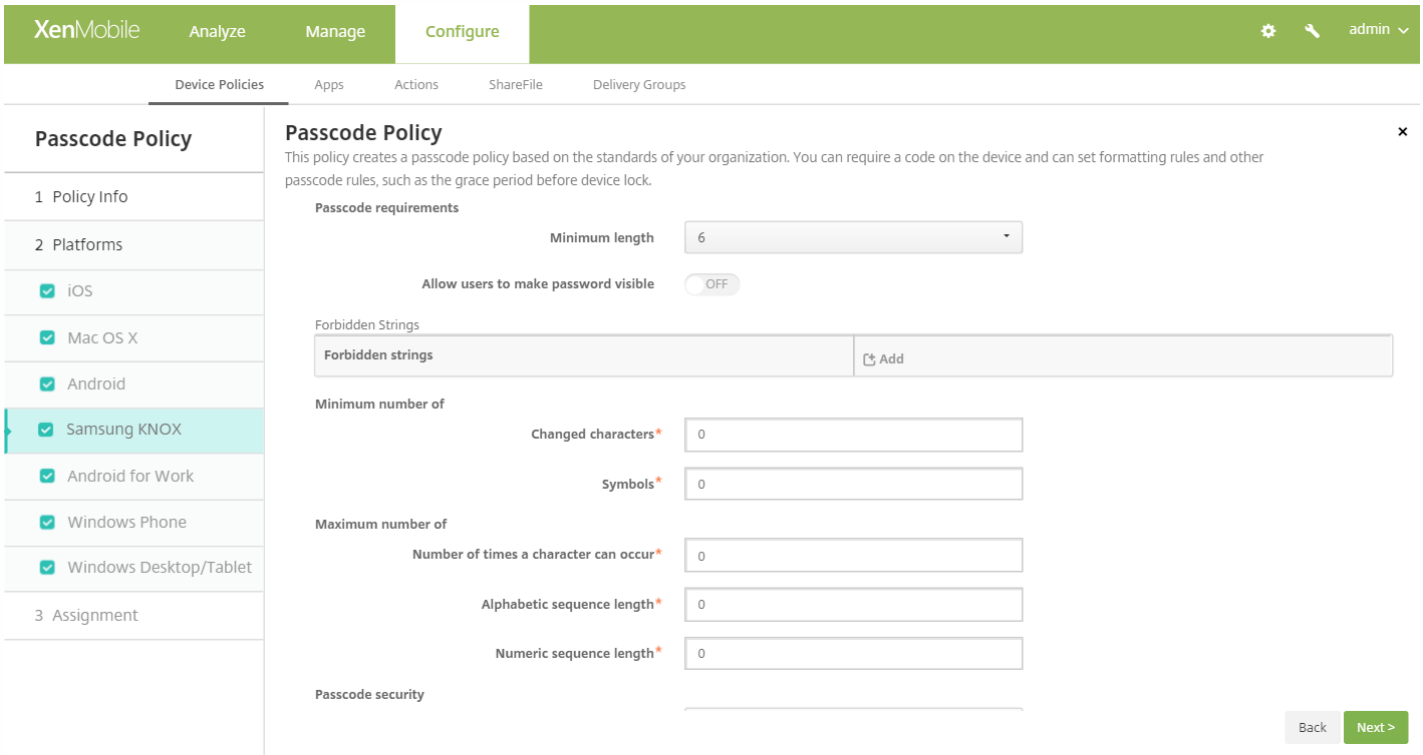
    Remarque : pour crypter leurs appareils, les utilisateurs doivent commencer avec une batterie chargée et laisser l'appareil branché pendant le délai nécessaire au cryptage, une heure au minimum. Si le processus de cryptage est interrompu, les utilisateurs risquent de perdre certaines ou toutes les données 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**
  - **Utilisez 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 **OFF**. 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 de **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 de **0**.
  - **Longueur des séquences alphabétiques** : entrez la longueur maximale d'une séquence alphabétique dans un code secret. La valeur par défaut est de **0**.
  - **Longueur des séquences numériques** : entrez la longueur maximale d'une séquence numérique dans un code secret. La valeur par défaut est de **0**.
  - **Autoriser les utilisateurs à afficher les mots de passe** : sélectionnez cette option pour autoriser les utilisateurs à afficher le mot de passe. La valeur par défaut est **ON**.
  - **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.

      Remarque : pour supprimer une chaîne existante, 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 une chaîne existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.



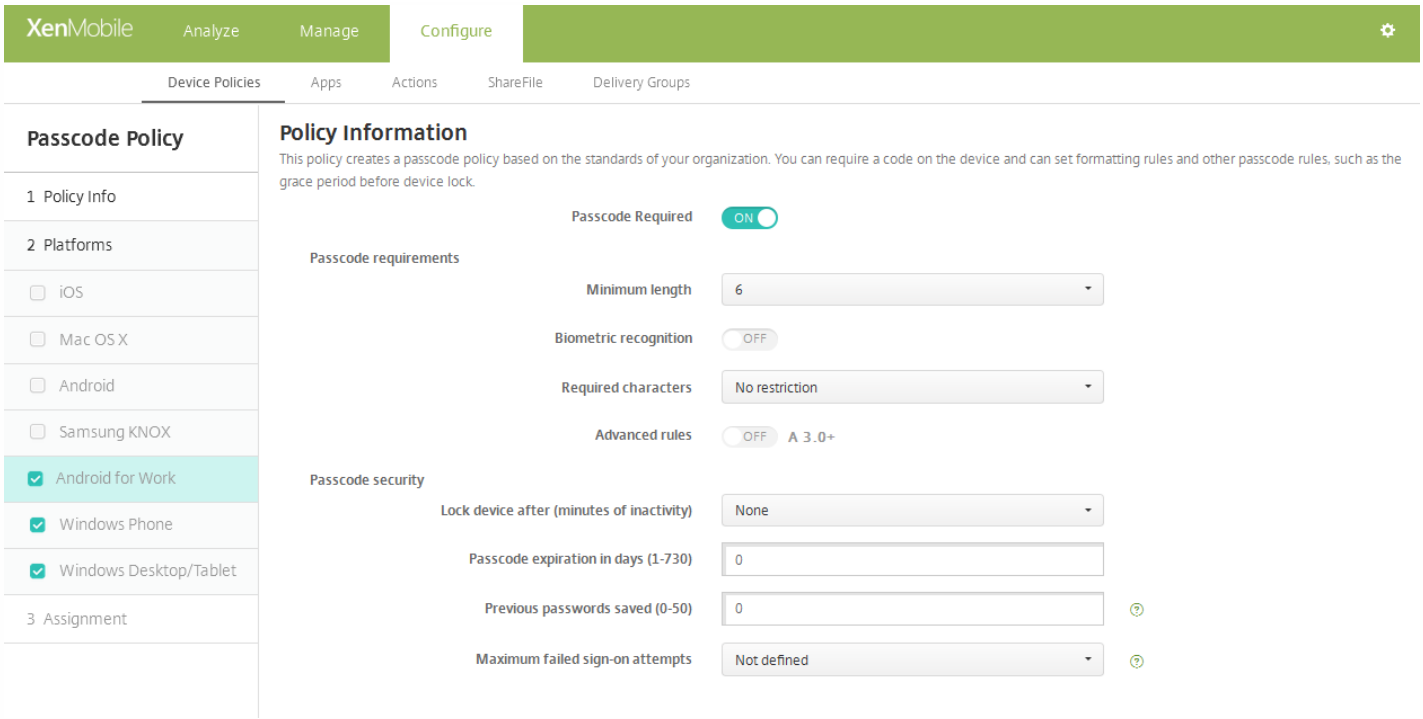
Pour configurer ces paramètres :

- **Conditions requises pour les codes secrets**
  - **Longueur minimale** : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de **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 refuser, 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.

      Remarque : pour supprimer une chaîne existante, 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 une chaîne existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

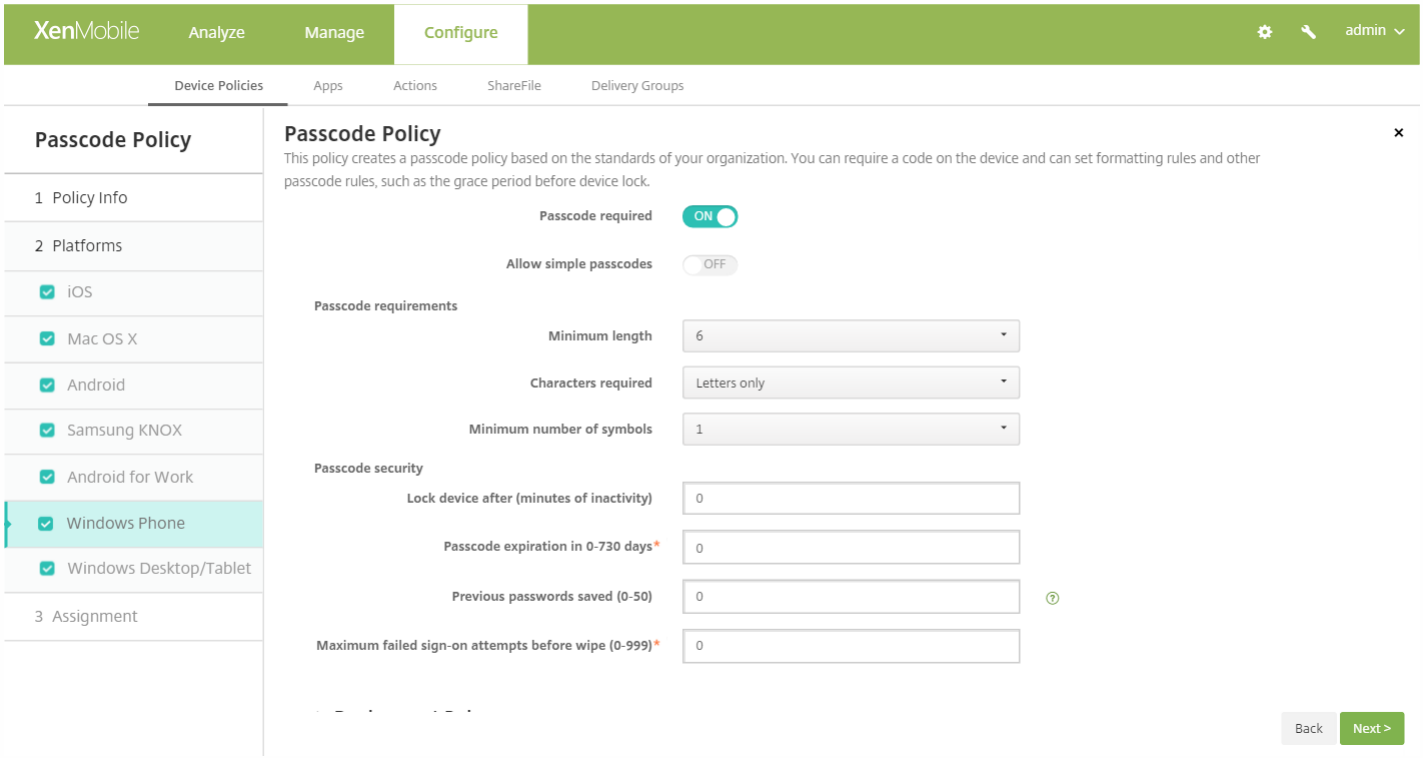
- **Nombre minimum de**
  - **Caractères modifiés** : entrez le nombre de caractères que les utilisateurs doivent changer par rapport à leur code secret précédent. La valeur par défaut est de **0**.
  - **Symboles** : entrez le nombre minimum de symboles requis dans un code secret. La valeur par défaut est de **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 de **0**.
  - **Longueur des séquences alphabétiques** : entrez la longueur maximale d'une séquence alphabétique dans un code secret. La valeur par défaut est de **0**.
  - **Longueur des séquences numériques** : entrez la longueur maximale d'une séquence numérique dans un code secret. La valeur par défaut est de **0**.
- **Sécurité des codes secrets**
  - **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 **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.
  - **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**.



Pour configurer ces paramètres :

- **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 for Work. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret et à la sécurité du code secret.
- **Conditions requises pour les codes secrets**
  - **Longueur minimale** : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de **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 **OFF**. Notez que cette fonctionnalité n'est pas prise en charge.
  - **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 n'est pas disponible pour les appareils Android de versions antérieures à Android 5.0. La valeur par défaut est **OFF**.
  - 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 des codes secrets**
  - **Verrouiller l'appareil après (minutes d'inactivité)** : dans la liste, cliquez sur le nombre de minutes pendant lesquelles un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est **Aucune**.

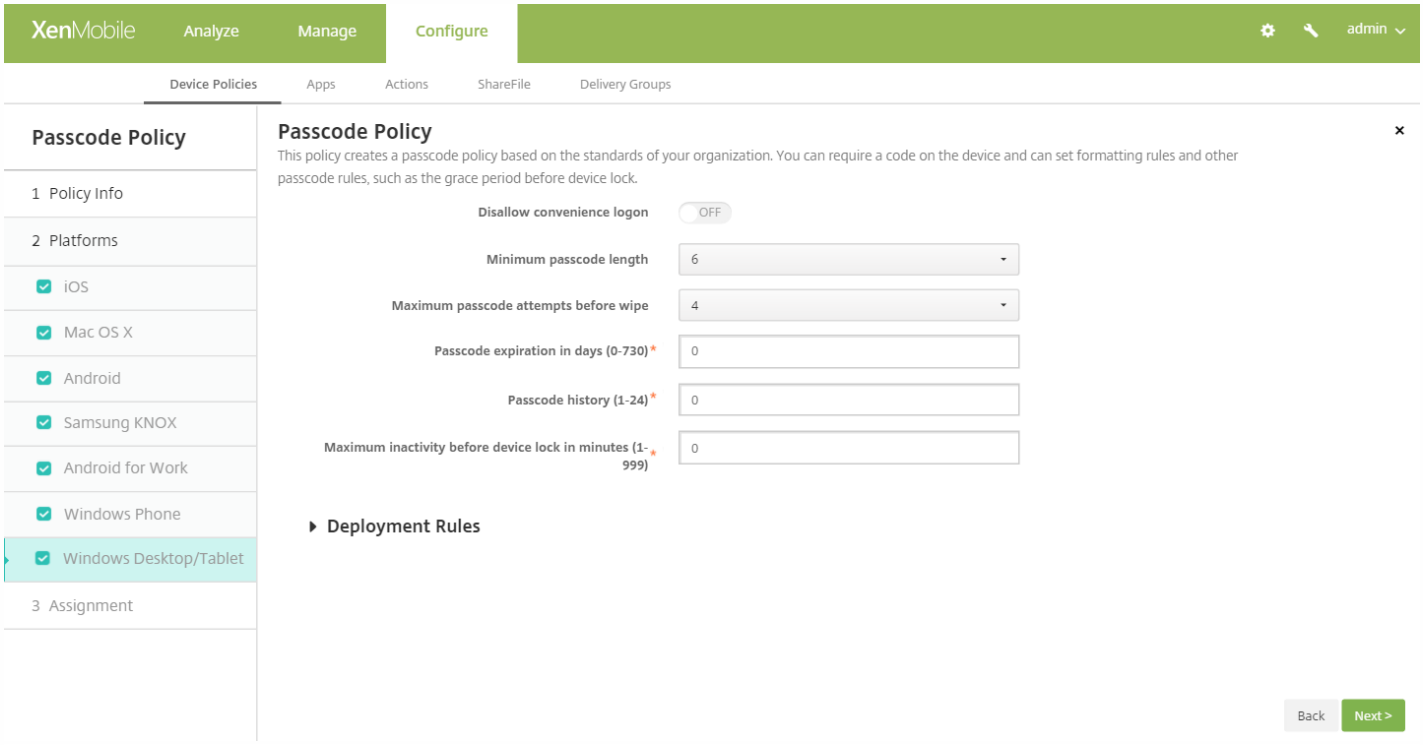
- **Expiration du code secret en jours (1 - 730)** : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
- **Mots de passe précédents enregistrés (0-50)** : entrez le nombre de 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 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**.



Pour configurer ces paramètres :

- **Code secret requis** : sélectionnez cette option pour ne pas exiger de code secret sur les appareils Windows Phone. Le paramètre par défaut est **ON**, ce qui nécessite un mot de passe. 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 OFF.
- **Conditions requises pour les codes secrets**
  - **Longueur minimale** : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de **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 de **1**.
- **Sécurité des codes secrets**

- **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 de **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 de **0**.



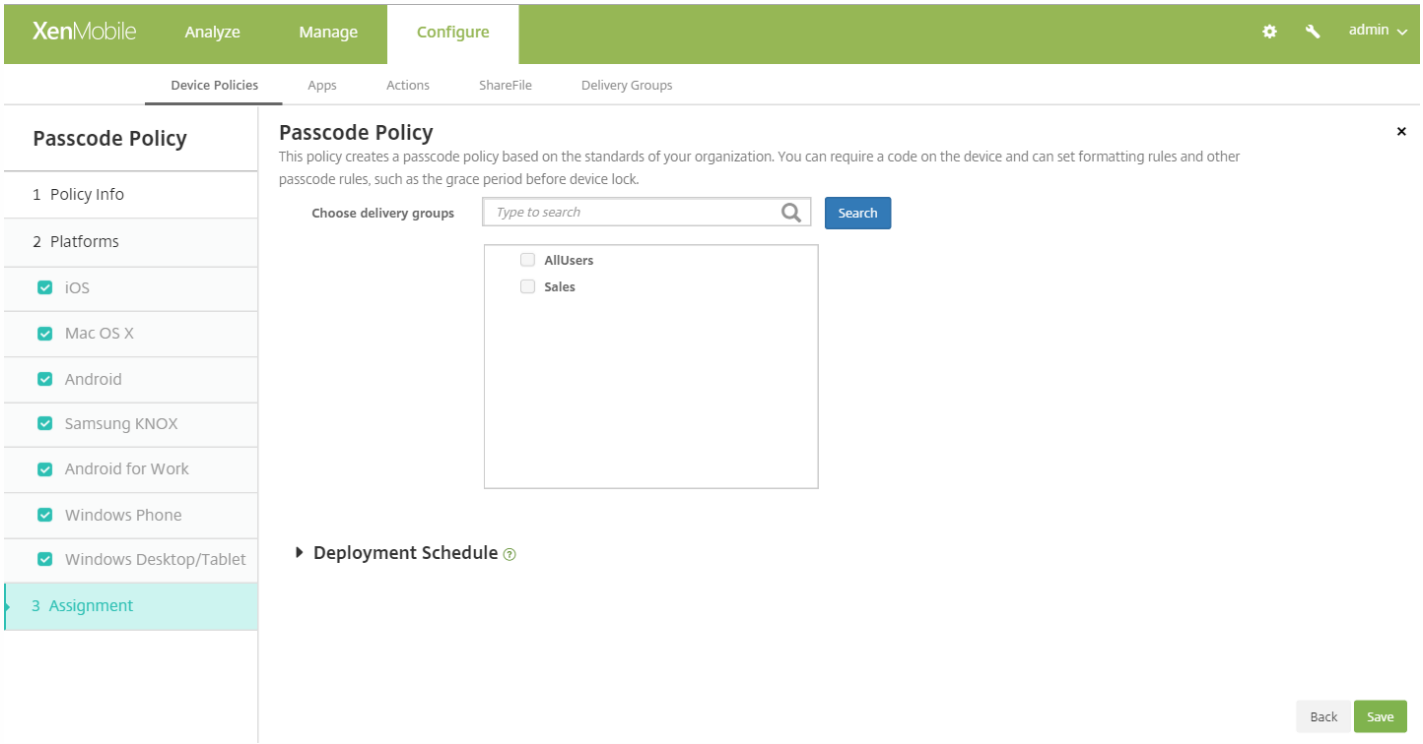
Pour configurer ces paramètres :

- **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 **OFF**.
- **Longueur minimum du code secret** : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de **6**.
- **Nombre maximum de tentatives de saisie du code secret avant effacement (0 - 999)** : 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 de **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 valides sont 1-24. Vous devez entrer un nombre compris entre 1 et 24. La valeur par défaut est de **0**.

- **Période d'inactivité maximale avant verrouillage de l'appareil en minutes (0 - 999)** : entrez la durée en minutes pendant laquelle un appareil peut rester inactif avant d'être verrouillé. Les valeurs valides sont 1-999. Vous devez entrer un nombre compris entre 1 et 999. La valeur par défaut est de **0**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie de code secret** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégie Personal Hotspot

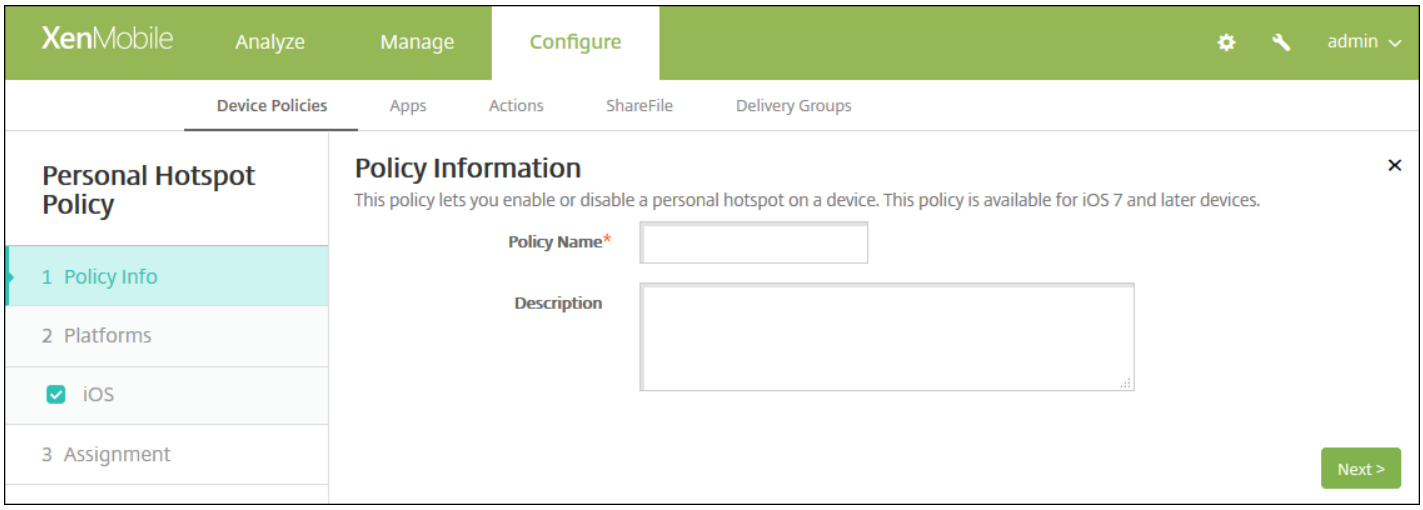
Jul 27, 2016

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.

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.

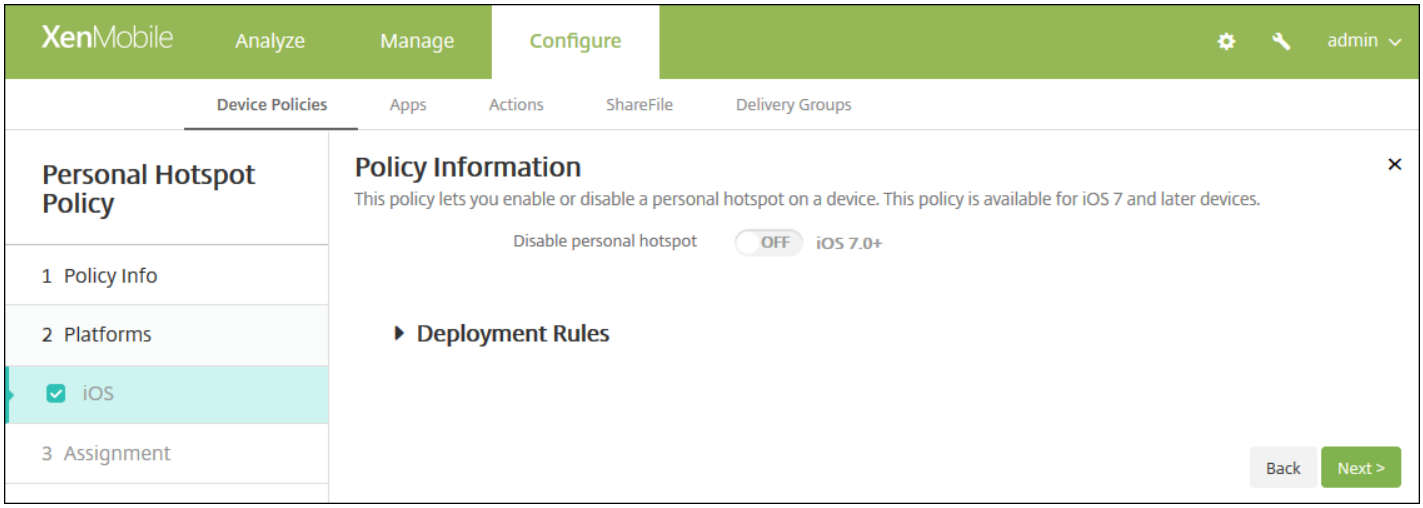
3. Développez **Plus**, puis, sous **Accès réseau**, cliquez sur **Personal Hotspot**. La page d'informations sur la **Stratégie Personal Hotspot** s'affiche.



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 **Next**. La page d'informations **Plate-forme iOS** s'affiche.

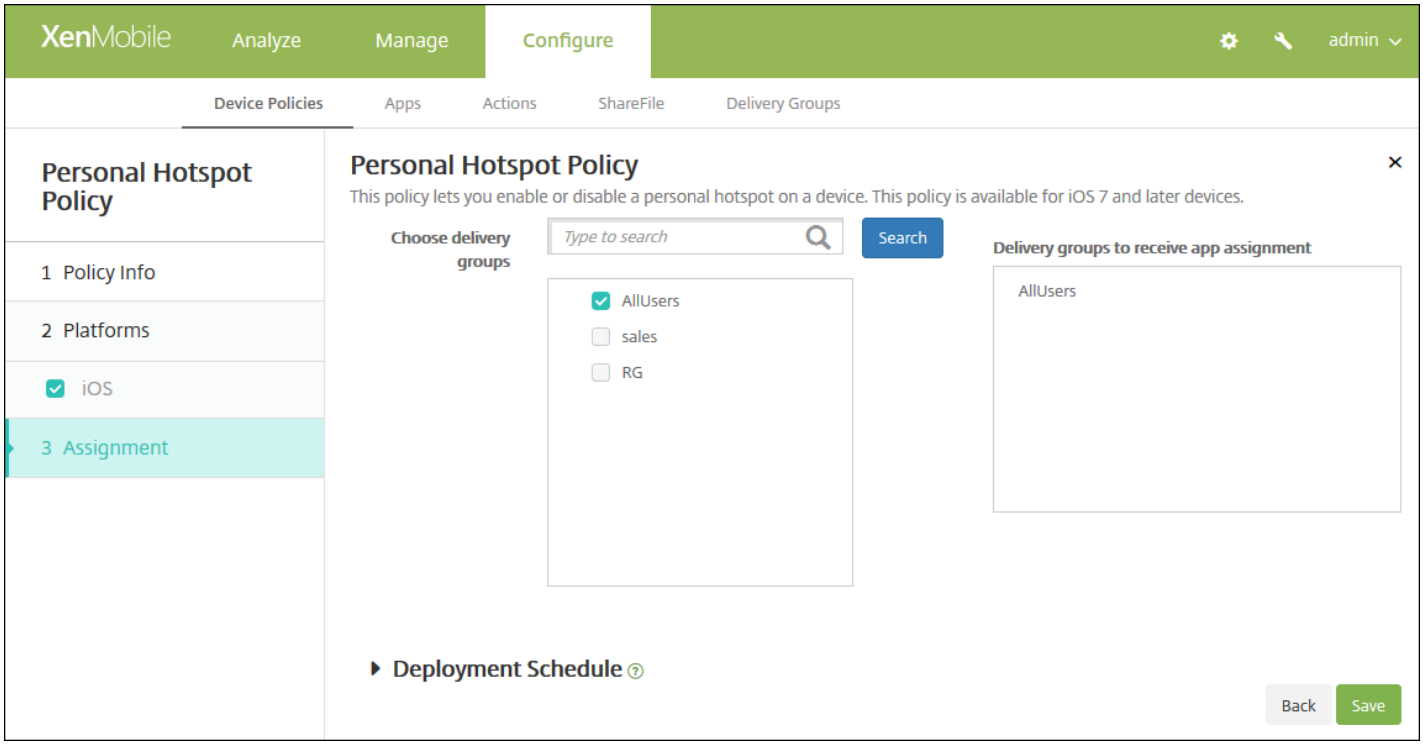


6. Configurez ce paramètre :

- **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 **OFF**, 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.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie Personal Hotspot** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 lorsque le déploiement précédent a échoué.** L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégies de suppression de profil

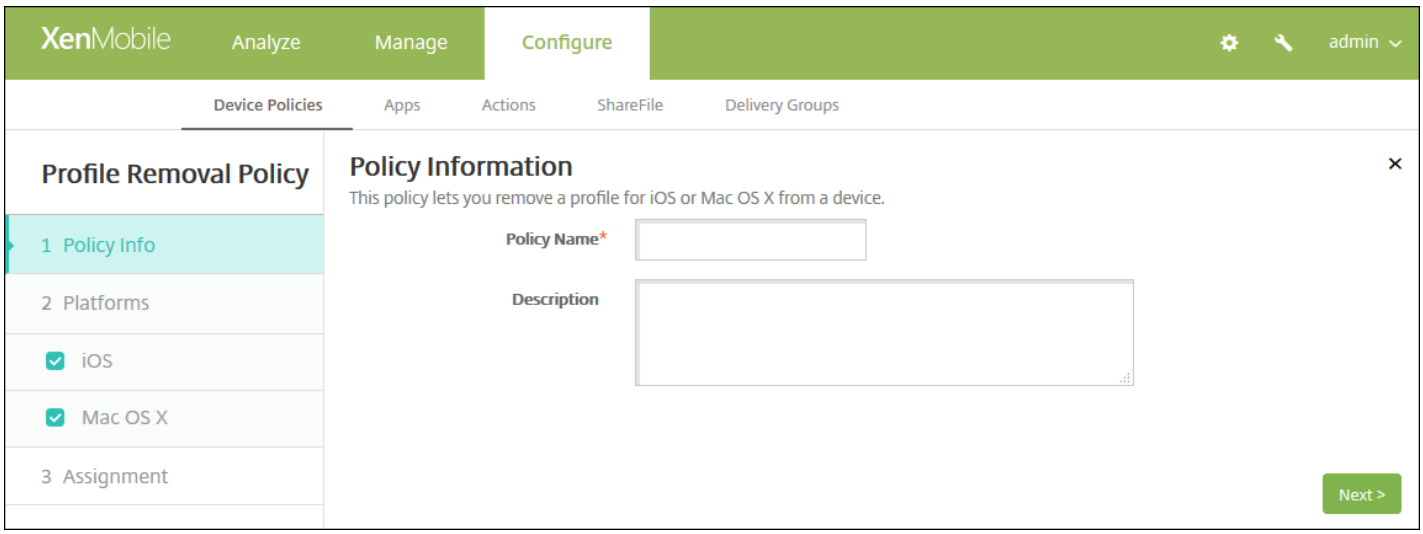
Jul 27, 2016

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 Mac OS X des utilisateurs.

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 **Suppression**, cliquez sur **Suppression du profil**. La page d'informations **Stratégie de suppression du profil** s'affiche.



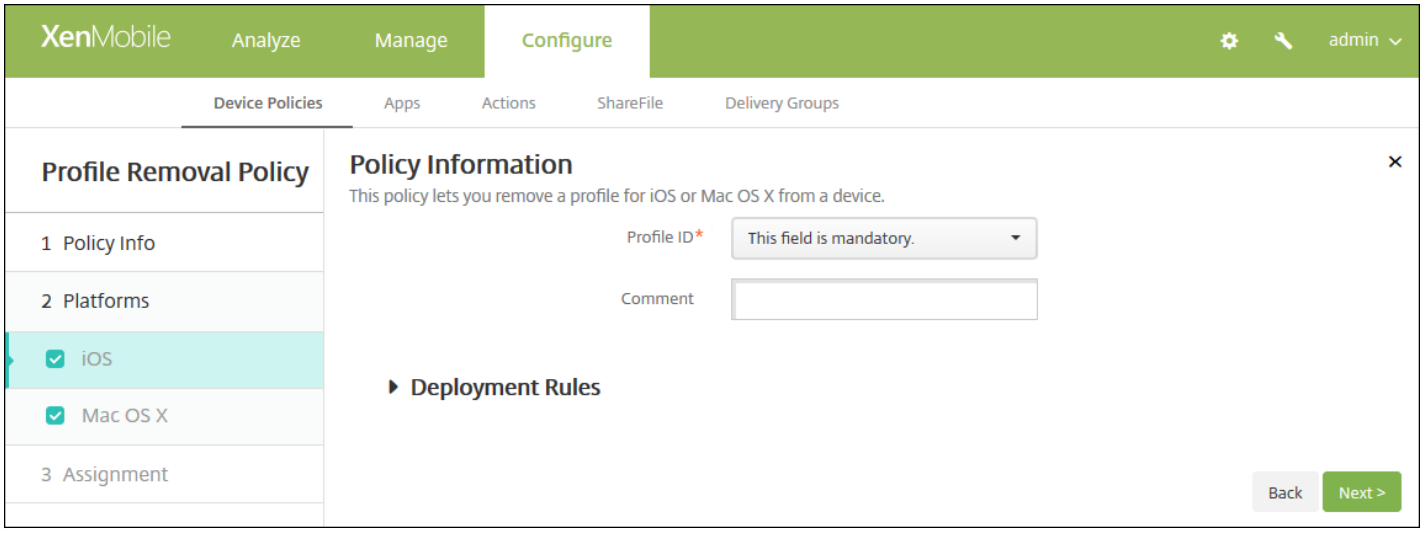
4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

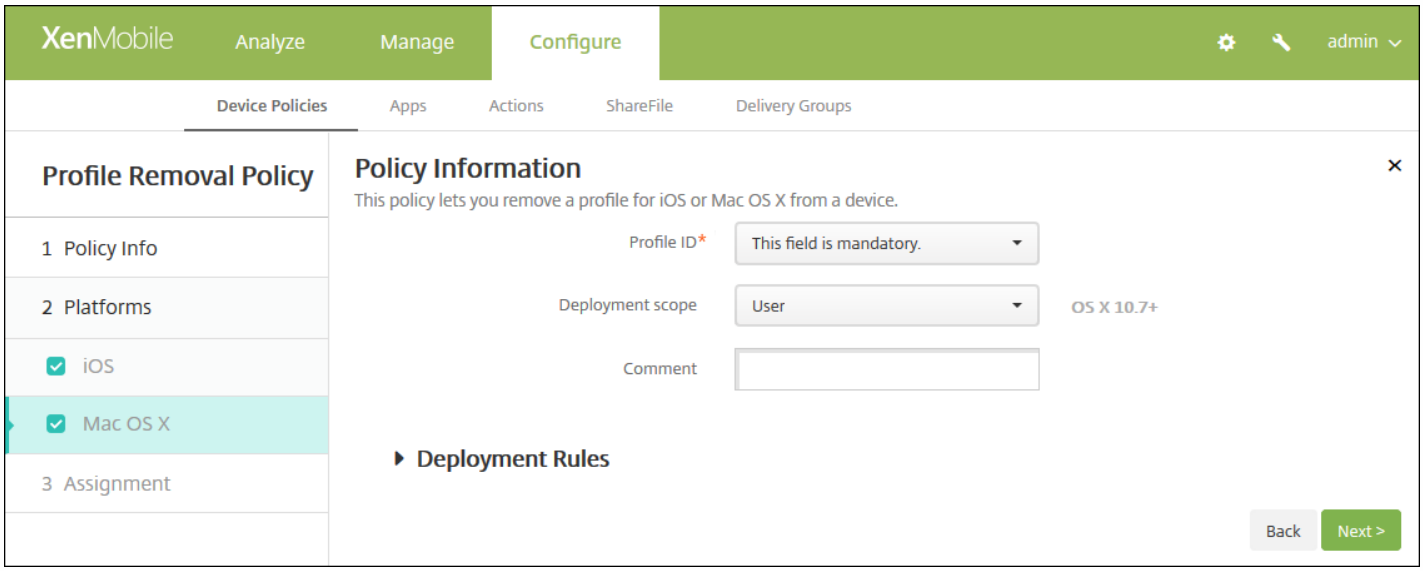
6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.



Pour configurer ces paramètres :

- **ID du profil** : dans la liste, cliquez sur l'ID du profil d'application. Ce champ est obligatoire.
- **Commentaires** : entrez un commentaire (facultatif).

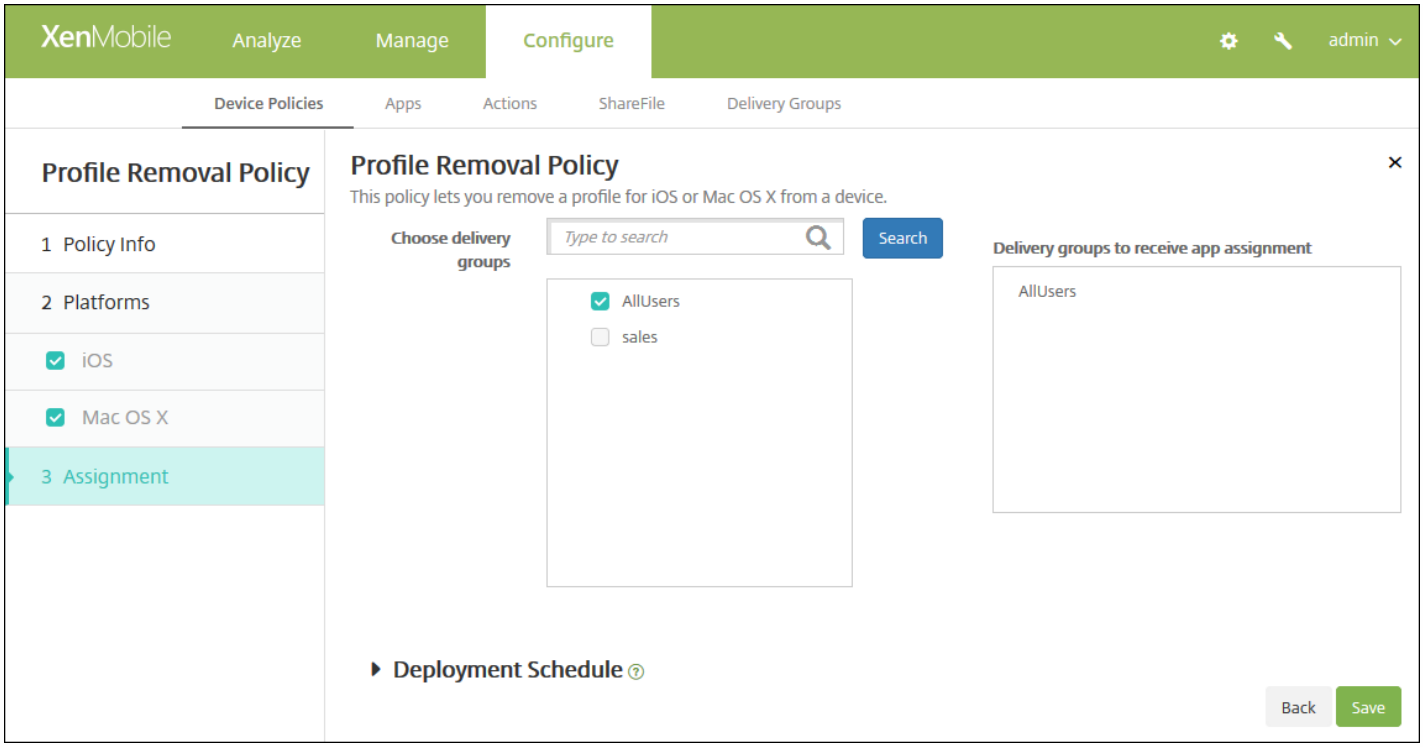


Pour configurer ces paramètres :

- **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 OS X 10.7 et versions ultérieures.
- **Commentaires** : entrez un commentaire (facultatif).

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie de suppression du profil** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 lorsque le déploiement précédent a échoué.** L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégie de profil de provisioning

Jul 27, 2016

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.

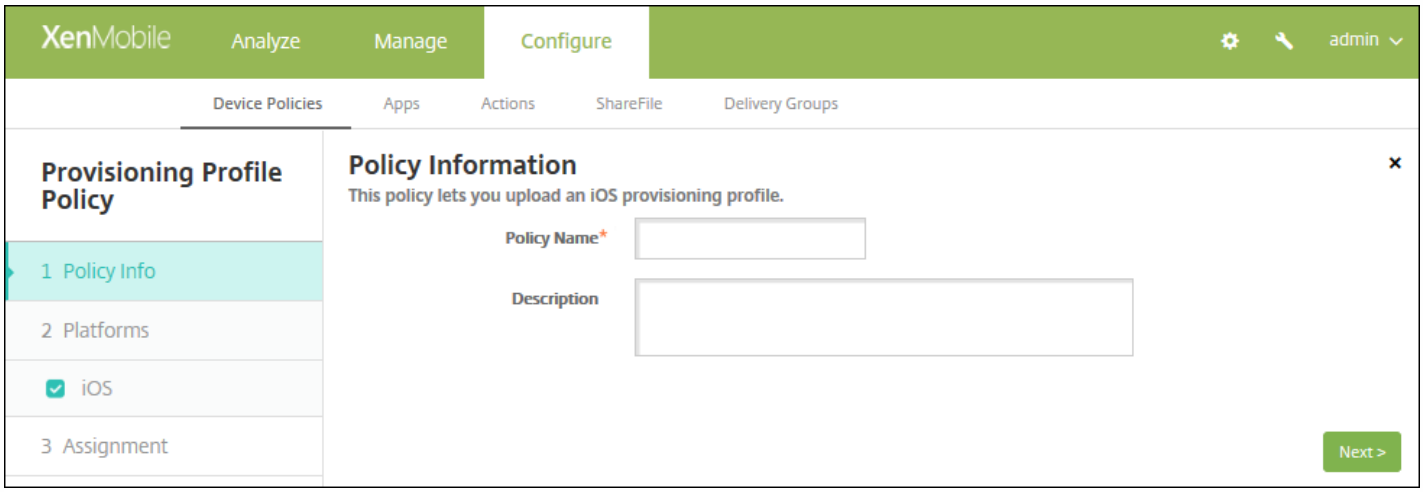
Pour effectuer cette opération de façon transparente pour les utilisateurs, dans XenMobile, vous pouvez installer et supprimer les profils de provisioning avec les stratégies d'appareil. Les profils manquants ou arrivés à expiration sont supprimés si nécessaire et des profils à jour sont installés sur 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, veuillez consulter la section Création de profils de provisioning sur le site Apple Developer.

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.

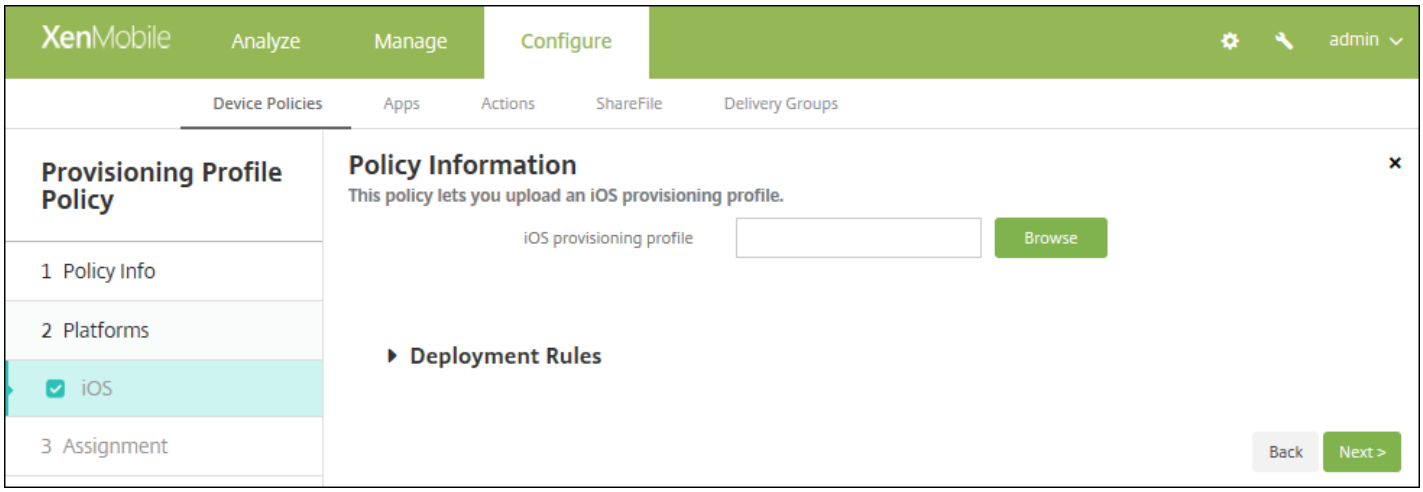
3. Développez **Plus** puis, sous **Applications**, cliquez sur **Profil de provisioning**. La page d'informations **Stratégie de profil de provisioning** s'affiche.



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 d'informations **Plate-forme iOS** s'affiche.

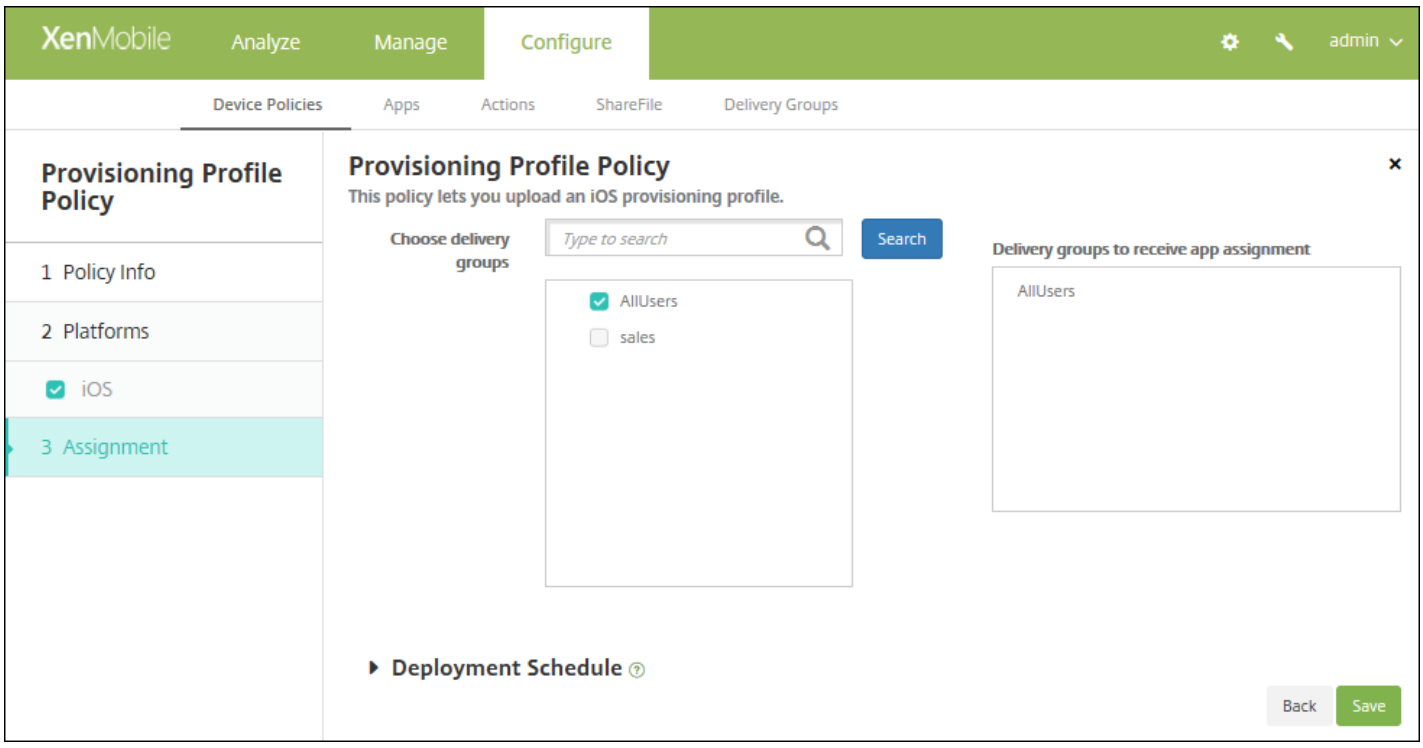


6. Configurez ce paramètre:

- **Profil de provisioning iOS** : sélectionnez le fichier de profil de provisioning à importer en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution **Stratégie de profil de provisioning** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégie de suppression de profil de provisioning

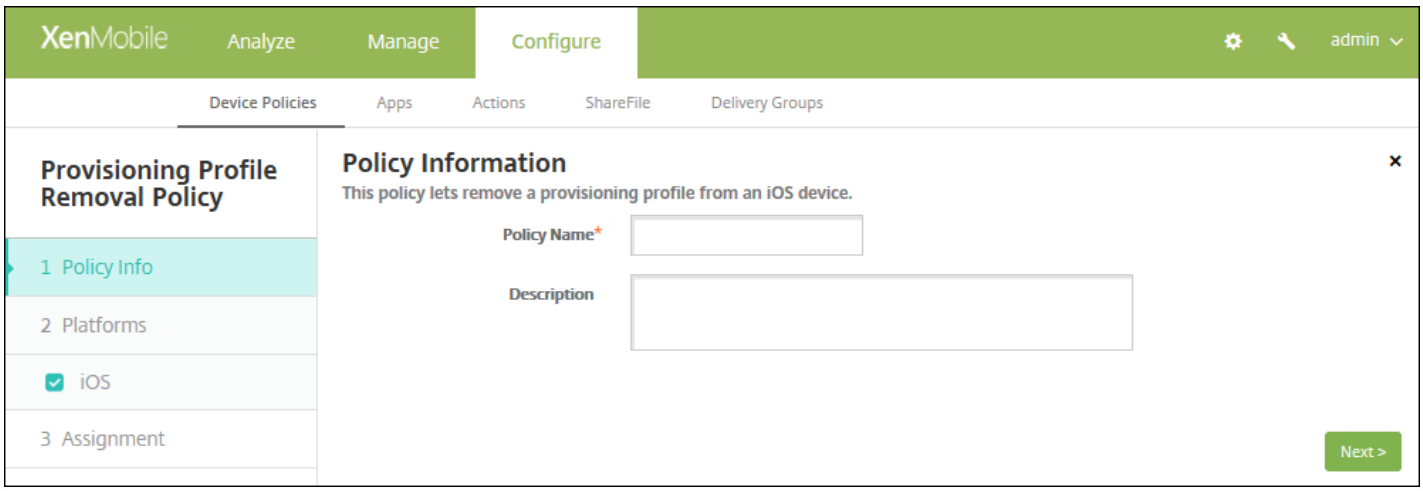
Jul 27, 2016

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 Ajout d'un profil de provisioning.

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.

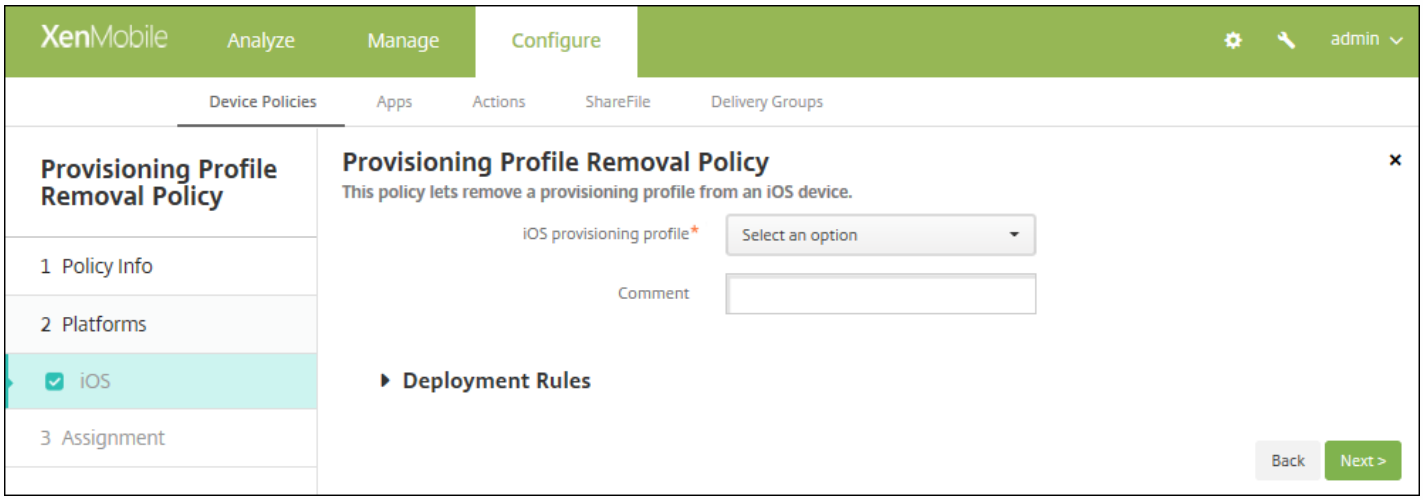
3. Développez **Plus** puis, sous **Suppression**, cliquez sur **Suppression du profil de provisioning**. La page d'informations **Stratégie de suppression du profil de provisioning** s'affiche.



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 **Next**. La page **Plate-forme iOS** s'affiche.

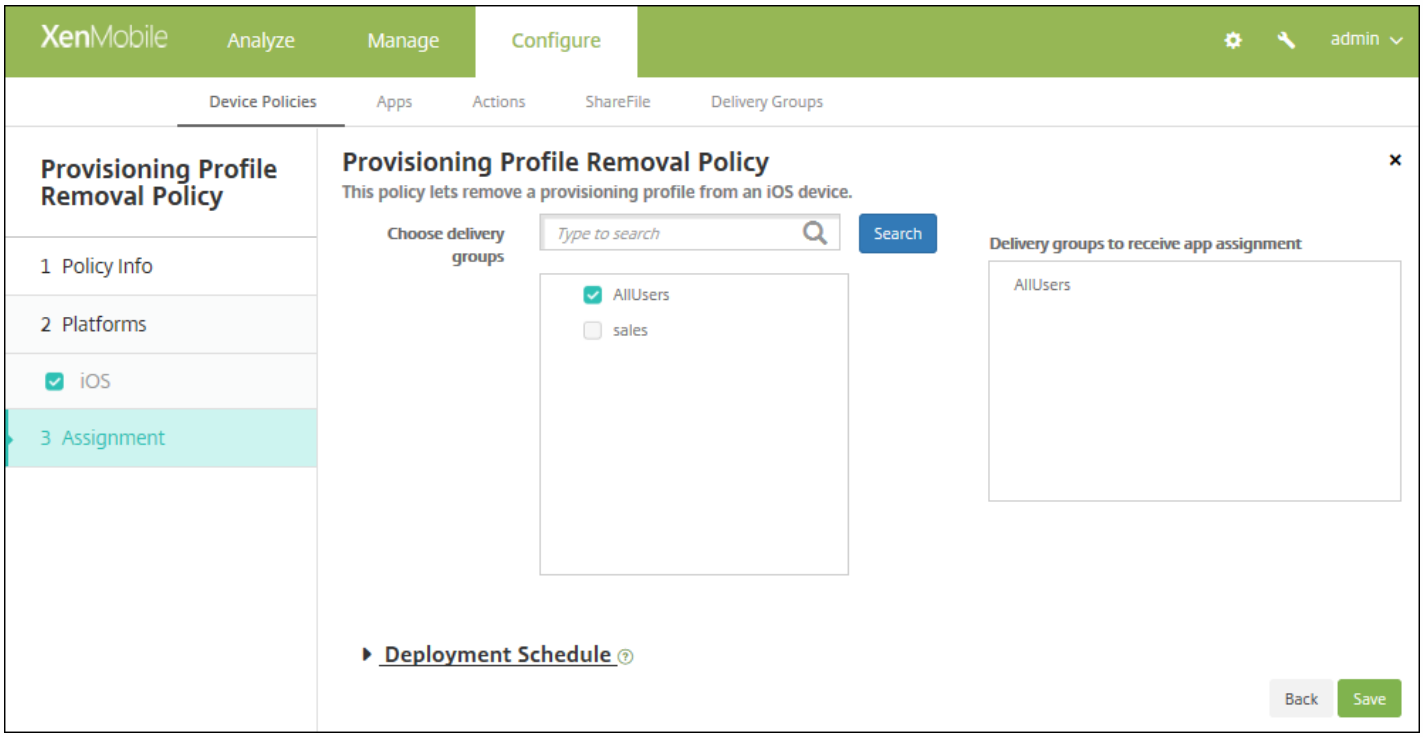


6. Configurez les paramètres suivants :

- **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.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie de suppression du profil de provisioning** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 lorsque le déploiement précédent a échoué.** L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégies de proxy

Jul 27, 2016

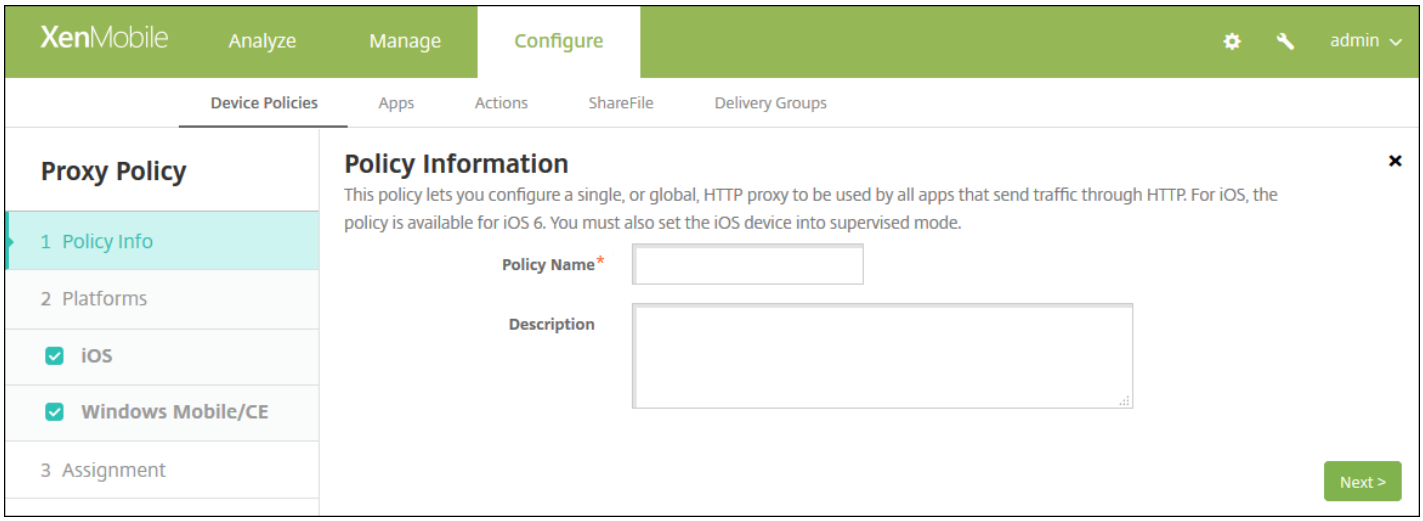
Vous pouvez ajouter une stratégie dans XenMobile pour spécifier les paramètres de proxy HTTP globaux pour les appareils exécutant Windows Mobile/CE et iOS 6.0 ou version ultérieure. Vous ne pouvez déployer qu'une stratégie de proxy HTTP globale par appareil.

Remarque : 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 de plus amples informations, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

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. Cliquez sur **Plus**, puis, sous **Accès réseau**, cliquez sur **Proxy**. La page **Stratégie de proxy** s'affiche.



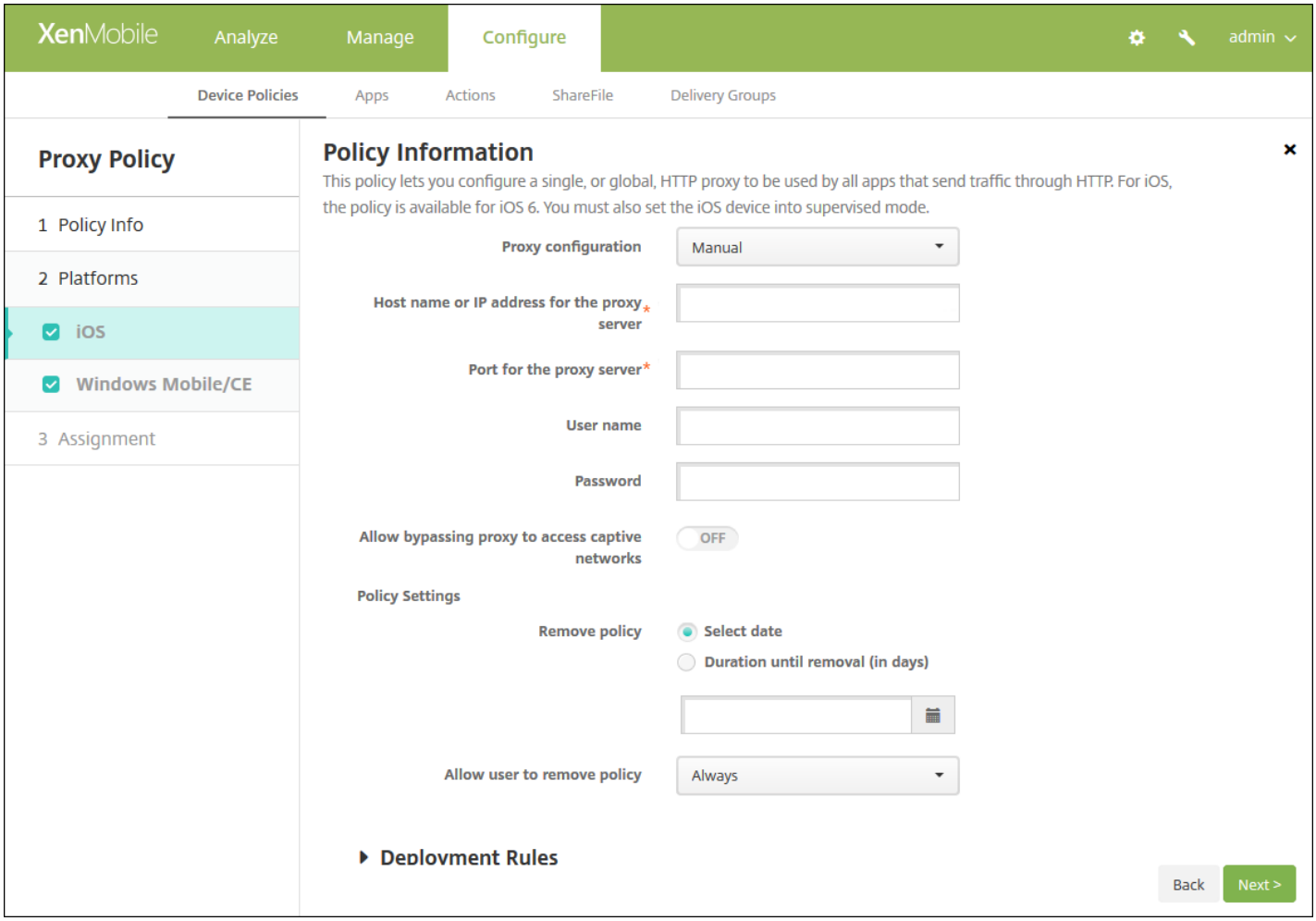
4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

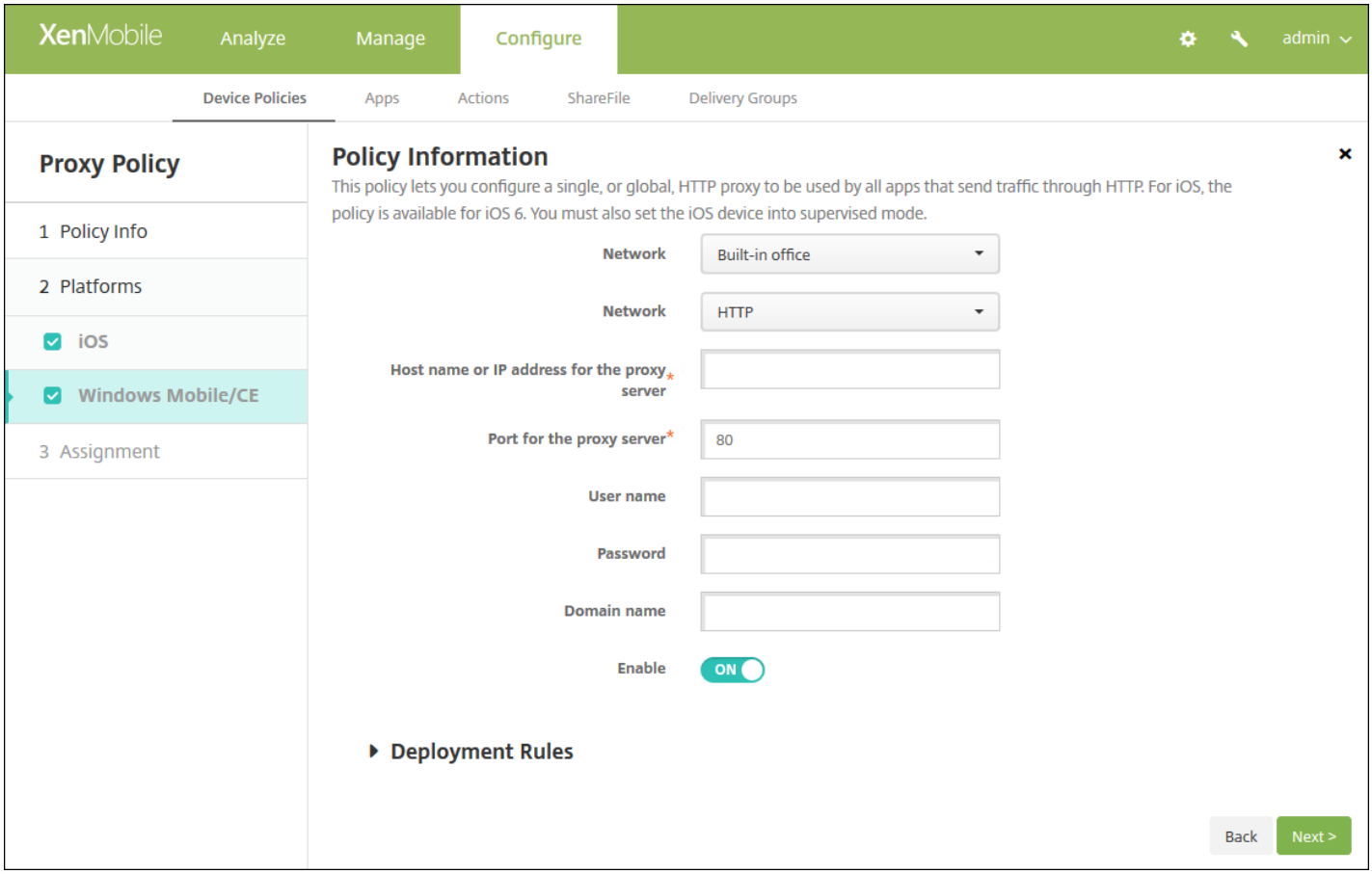
Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.



Pour configurer ces paramètres :

- **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 **ON**. 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 **OFF**.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.

- 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.



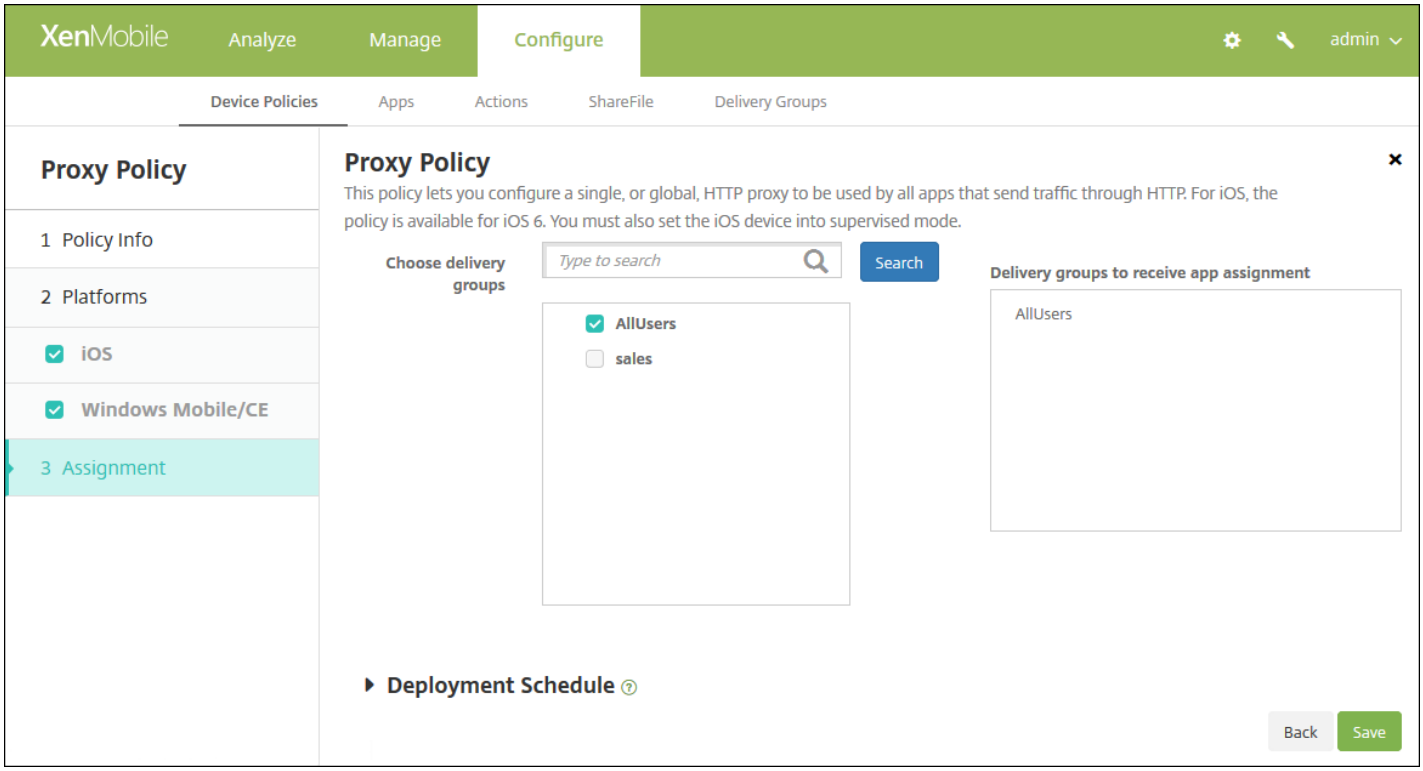
Pour configurer ces paramètres :

- **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 de **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 **ON**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie de proxy** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégie de Registre

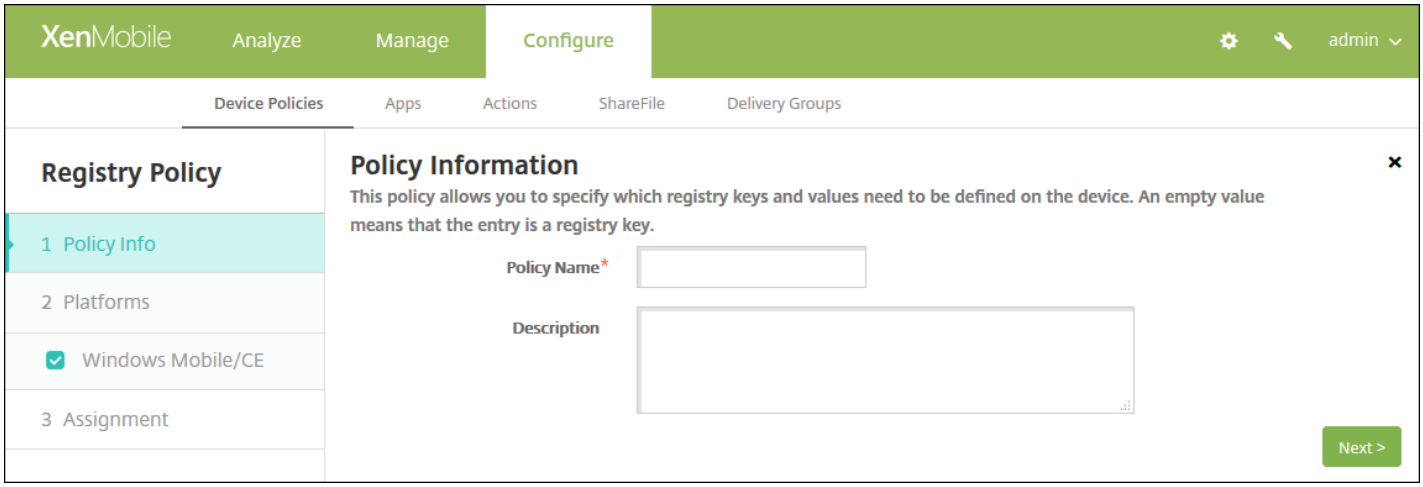
Jul 27, 2016

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.

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.

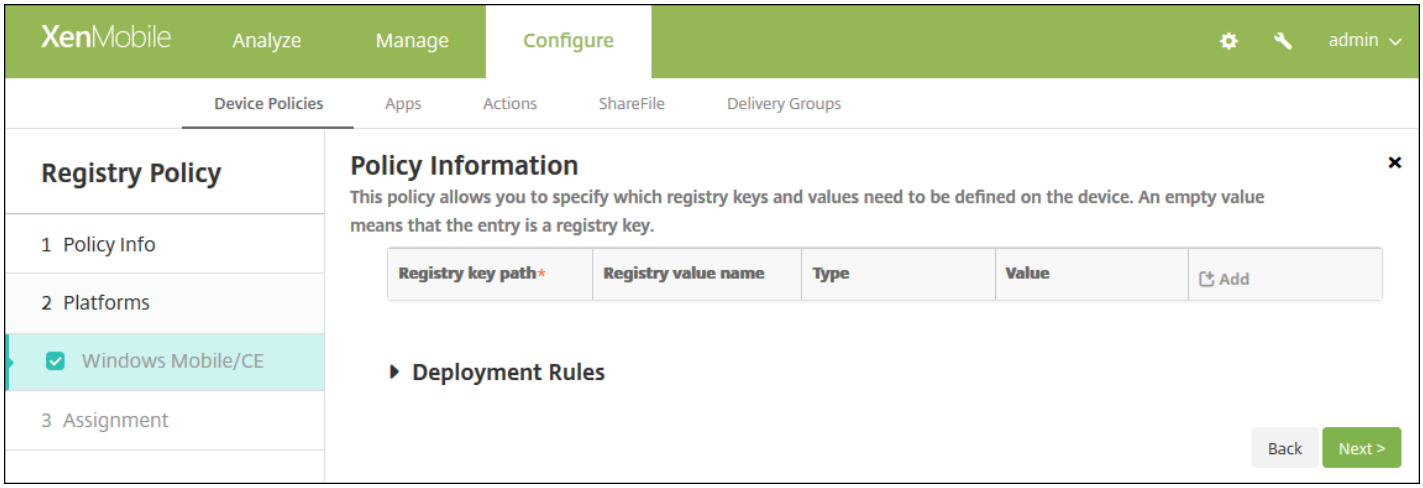
3. Développez **Plus** puis, sous **Personnalisé**, cliquez sur **Registre**. La page d'informations **Stratégie de Registre** s'affiche.



4. Dans le panneau **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 **Next**. La page d'informations sur la plate-forme **Plate-forme : Windows Mobile/CE** s'affiche.



6. Configurez les paramètres suivants :

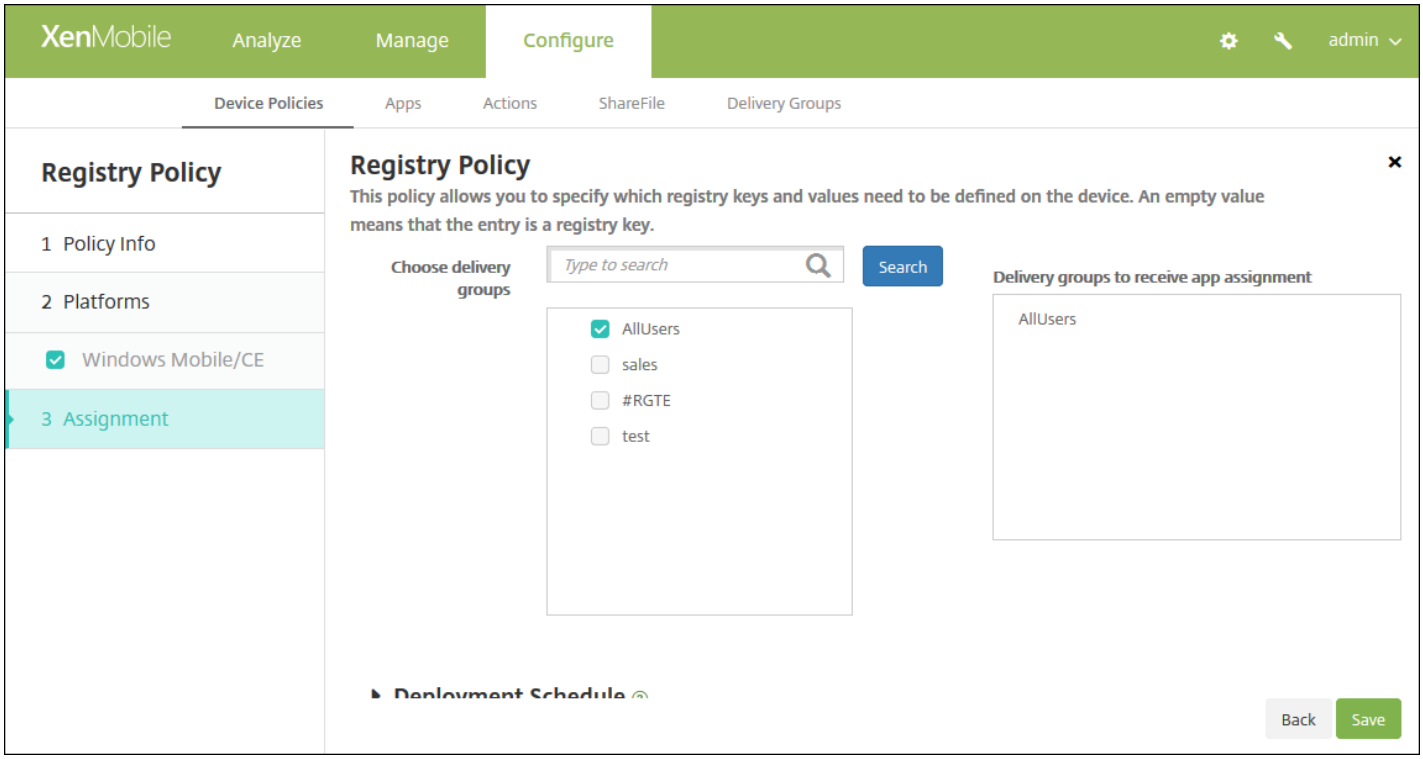
- Pour chaque clé de registre ou paire de clé/valeur de registre que vous souhaitez ajouter, cliquez sur **Ajouter** et procédez comme suit :
- **Chemin d'accès à la clé de Registre** : entrez le chemin d'accès complet pour la clé de registre. Par exemple, tapez *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows* 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.

  Remarque : pour supprimer une clé de registre existante, 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 une clé de registre, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie de Registre** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 lorsque le déploiement précédent a échoué.** L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégie d'assistance à distance

Jul 27, 2016

Vous créez une stratégie d'assistance à distance dans XenMobile pour vous permettre d'accéder à distance aux appareils Samsung KNOX des utilisateurs. 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, y compris le contrôle des couleurs (dans la fenêtre principale ou dans une fenêtre distincte flottante), d'établir une session Voix-sur-IP (VoIP) entre le bureau d'assistance et l'utilisateur, de configurer des paramètres et d'établir une session de chat entre le bureau d'assistance et l'utilisateur.

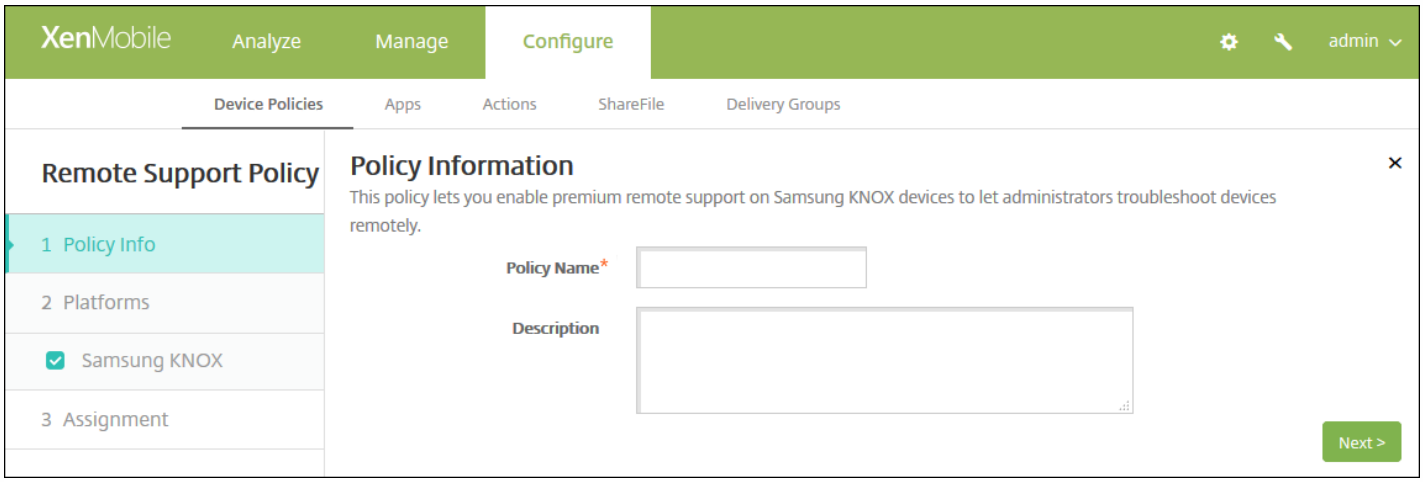
Remarque : pour implémenter cette stratégie, vous devez effectuer les tâches suivantes :

- 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 de tunnel applicatif à utiliser pour l'assistance à distance et la stratégie d'assistance à distance Samsung KNOX sur les appareils des utilisateurs.

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.

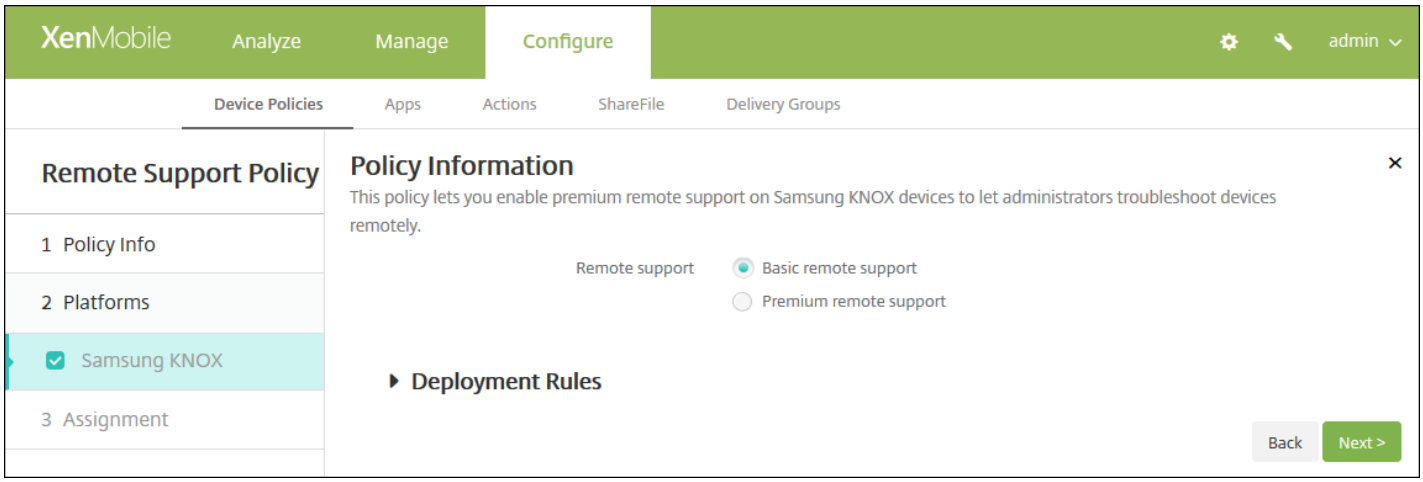
3. Développez **Plus**, puis, sous **Accès réseau**, cliquez sur **Assistance à distance**. La page **Stratégie d'assistance à distance** s'affiche.



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 **Next**. La page d'informations sur la plate-forme **Samsung KNOX** s'affiche.

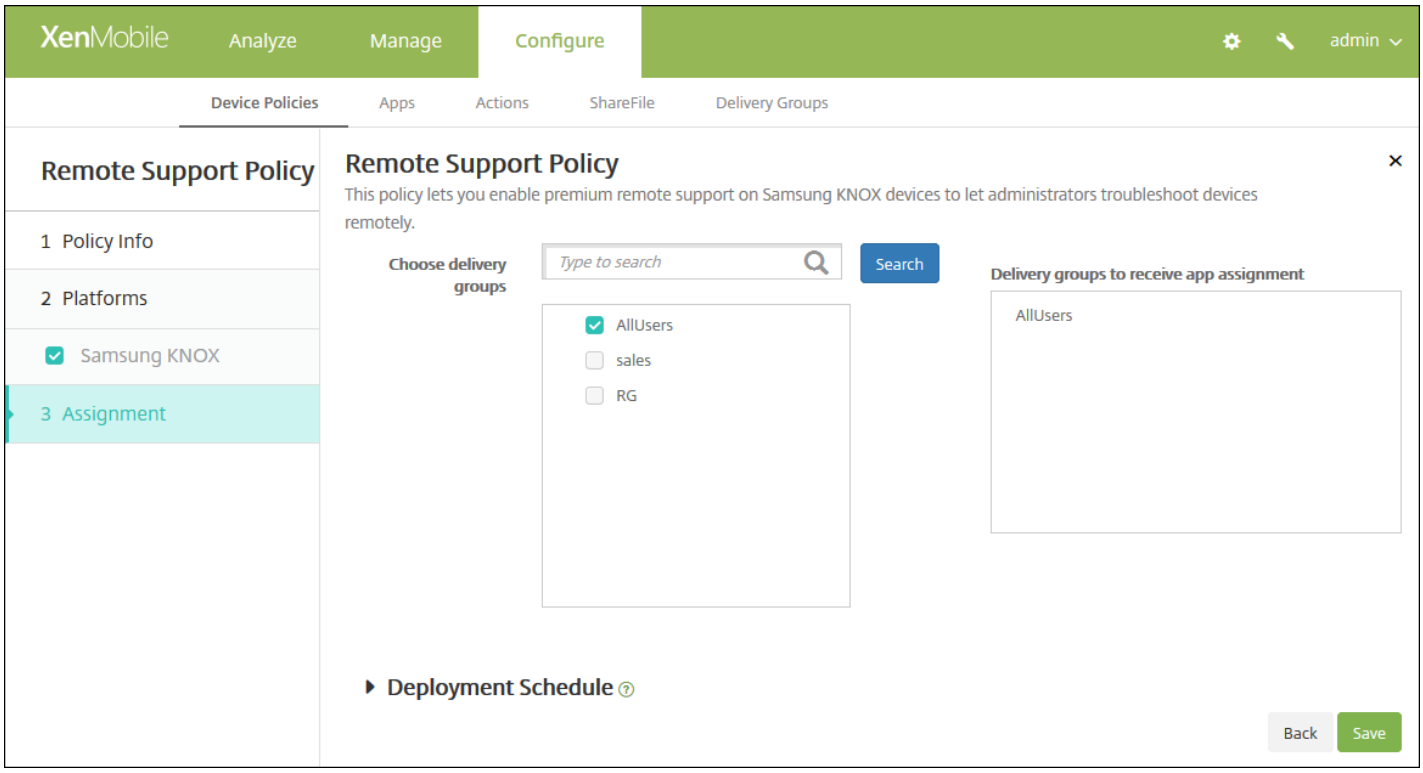


6. Configurez ce paramètre :

- **Assistance à distance** : sélectionnez **Assistance à distance de base** ou **Assistance à distance premium**. La valeur par défaut est **Assistance à distance de base**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie d'assistance à distance** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 lorsque le déploiement précédent a échoué.** L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégies de restrictions

Jul 27, 2016

Vous pouvez ajouter une stratégie d'appareil dans XenMobile pour limiter l'accès des utilisateurs à certaines fonctionnalités sur leurs appareils, téléphones, tablettes, etc. Vous pouvez configurer la stratégie de restrictions pour les plates-formes suivantes : iOS, Mac OS X, Samsung SAFE, Samsung KNOX, tablettes Windows, Windows Phone, Amazon et Windows Mobile/CE. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

Cette stratégie permet ou empêche les utilisateurs d'utiliser certaines fonctionnalités sur leurs appareils, 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 **ON** 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 **OFF** ou appliquent des *restrictions*.

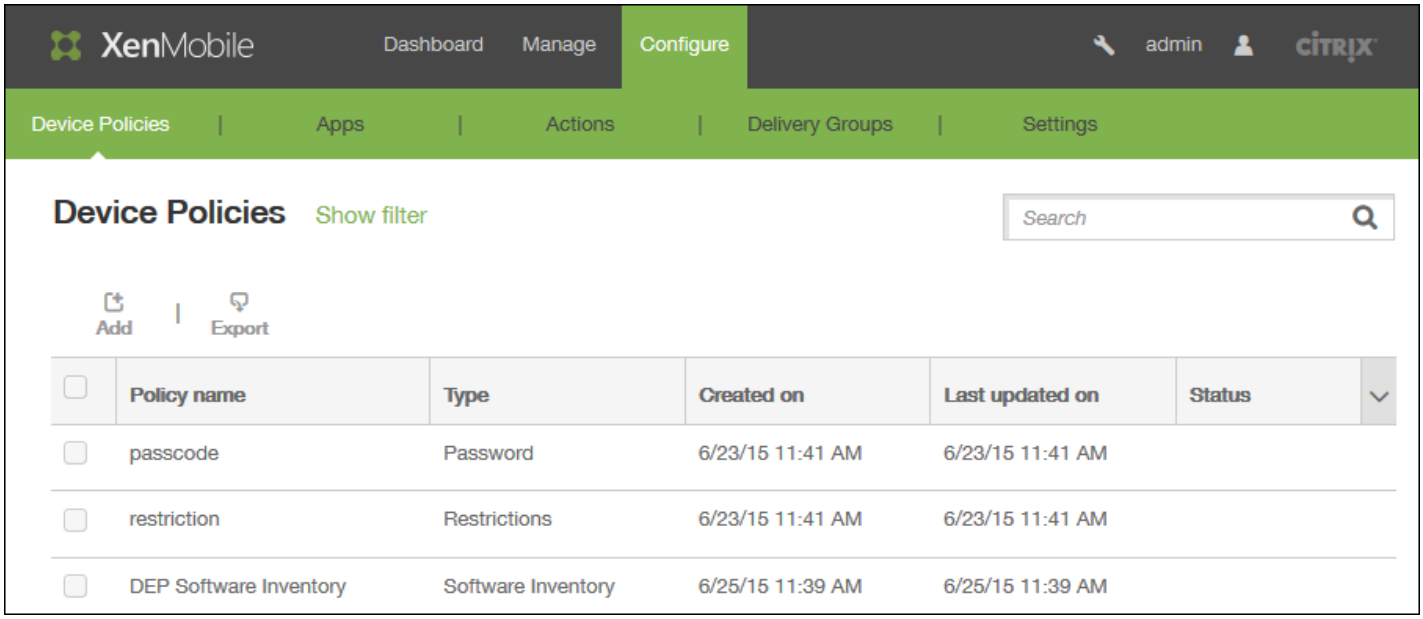
Conseil : toute option définie sur **ON** signifie que l'utilisateur

— peut

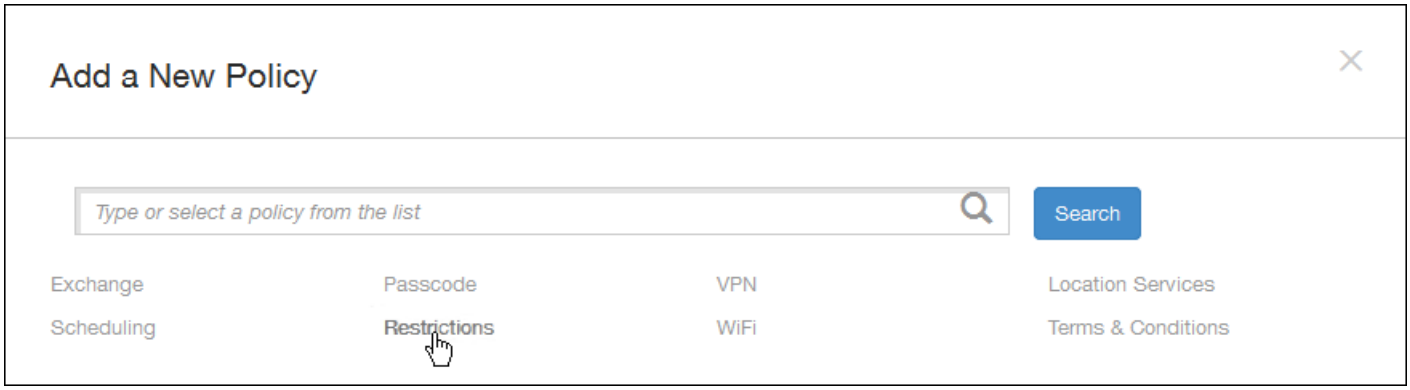
effectuer l'opération ou utiliser la fonctionnalité. Par exemple :

- **Appareil photo**. Si l'option est réglée sur **ON**, l'utilisateur peut utiliser l'appareil photo sur son appareil. Si l'option est réglée sur **OFF**, l'utilisateur ne peut pas utiliser l'appareil photo sur son appareil.
- **Captures d'écrans**. Si l'option est réglée sur **ON**, l'utilisateur peut prendre des captures d'écrans sur son appareil. Si l'option est réglée sur **OFF**, l'utilisateur ne peut pas prendre de captures d'écrans sur son appareil.

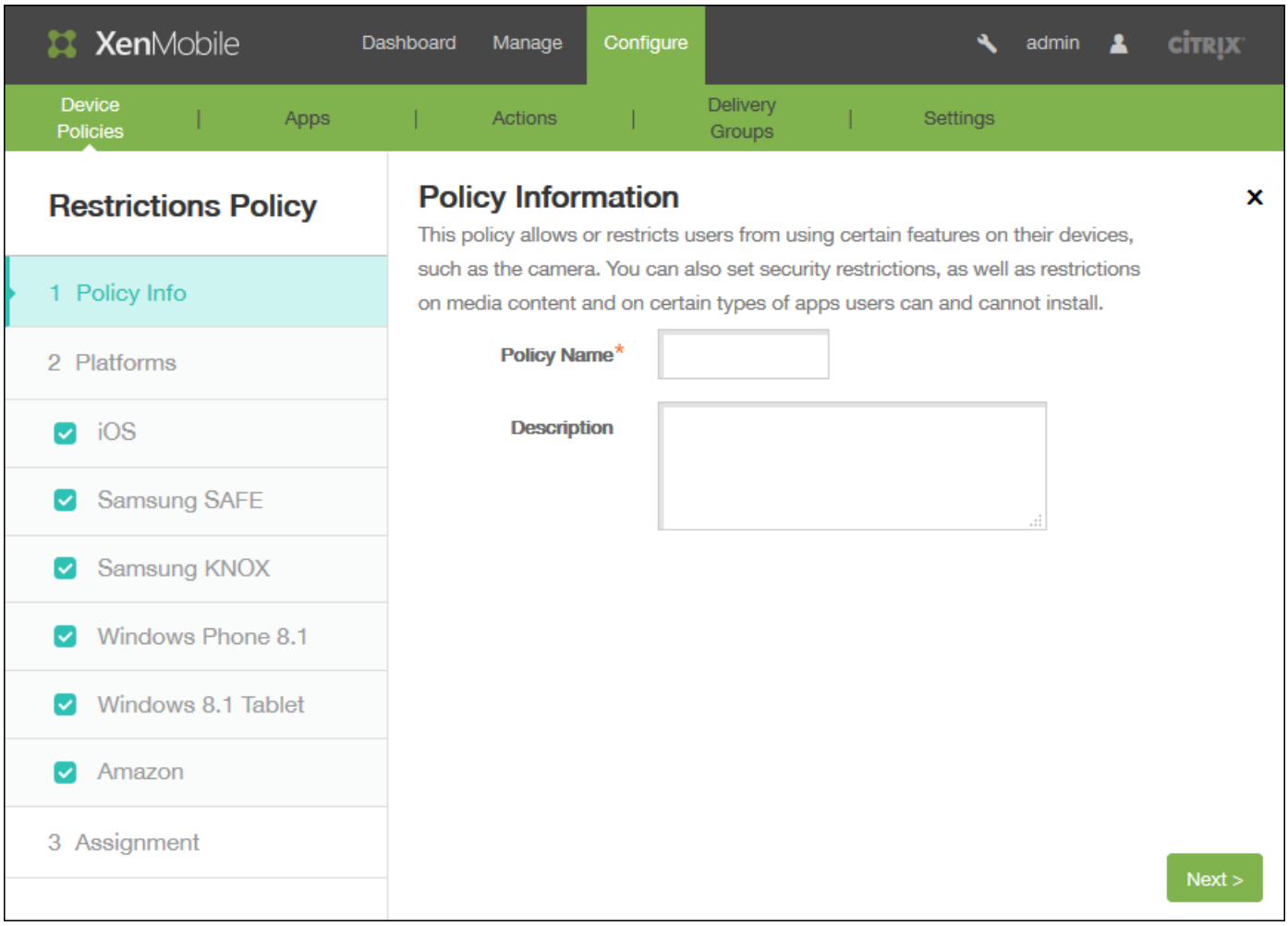
1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.



2. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** s'affiche.



3. Cliquez sur **Restrictions**. La page **Informations sur la stratégie** s'affiche.



4. Dans le panneau **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).

4. Cliquez sur **Suivant**. La page **Stratégie par plate-forme** s'affiche.

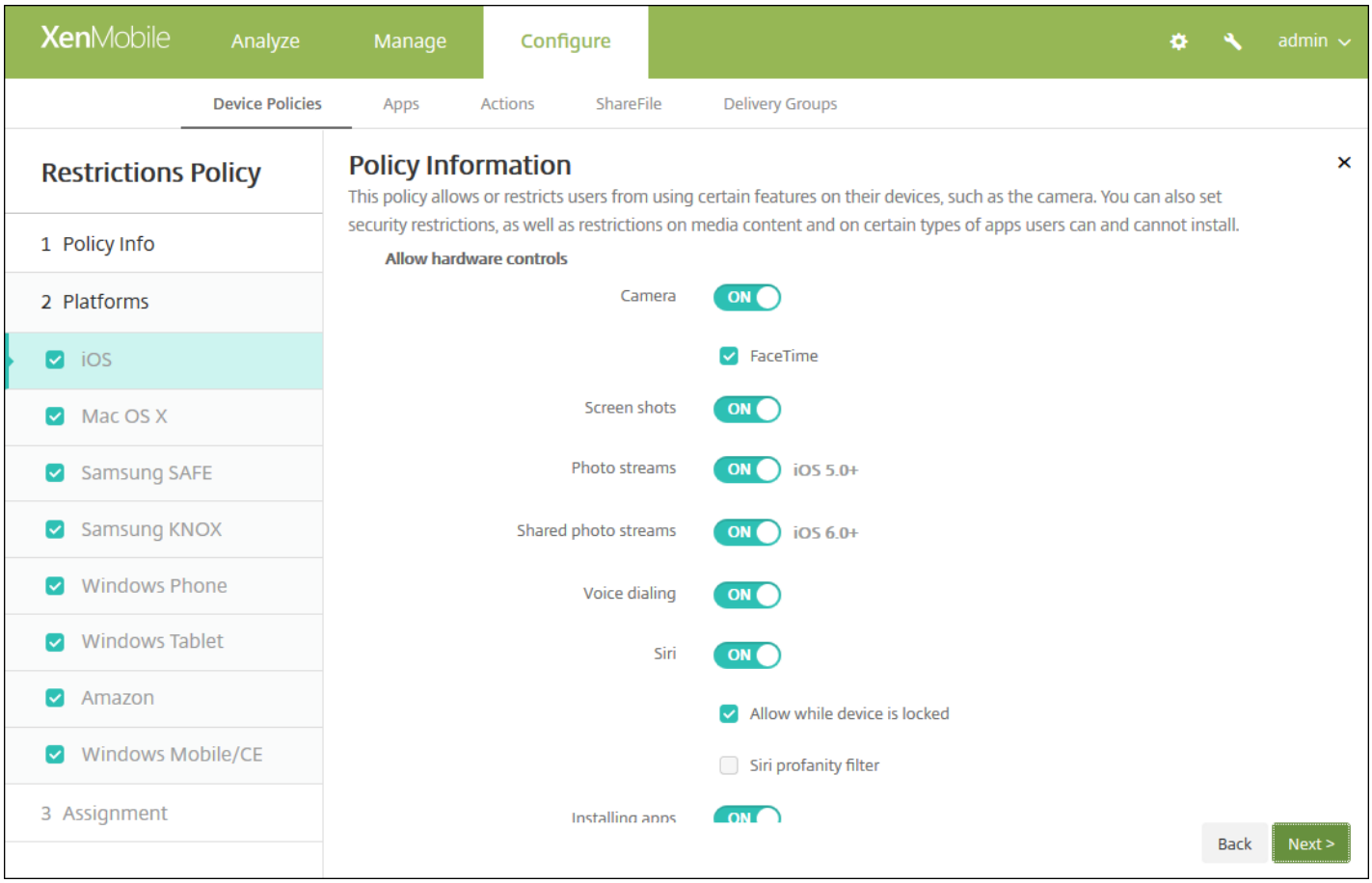
5. Sous **Plates-formes**, sélectionnez la ou les plates-formes que vous souhaitez ajouter. Vous pouvez ensuite modifier les

informations de stratégie pour chaque plate-forme que vous avez sélectionnée. Cliquez pour limiter les fonctionnalités dans les sections suivantes, ce qui désactive le paramètre (**OFF**). Sauf spécification contraire, la fonctionnalité est activée par défaut.

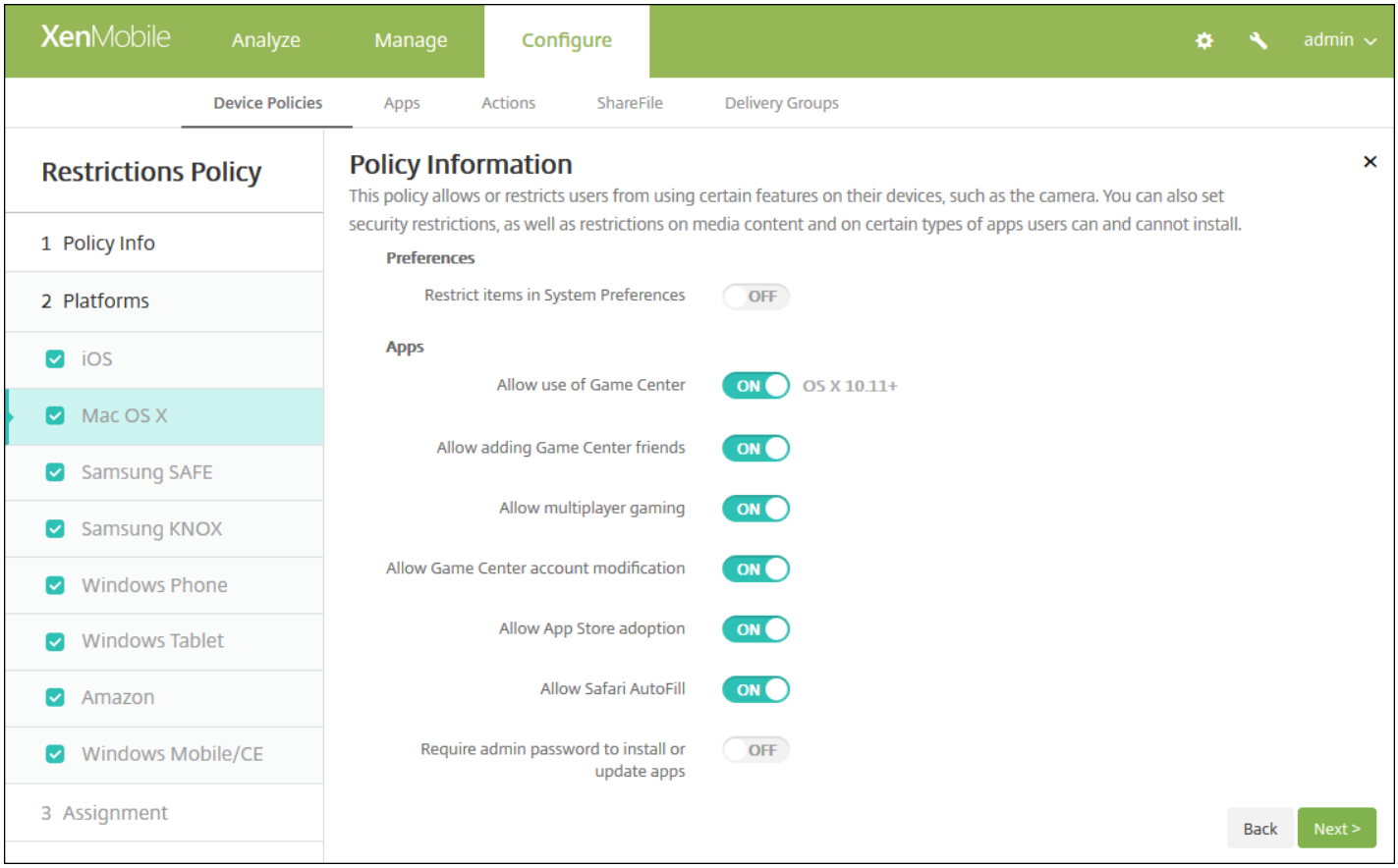
Si vous avez sélectionné :

iOS, configurez ces paramètres
Mac OS X, configurez ces paramètres
Samsung SAFE, configurez ces paramètres
Samsung KNOX, configurez ces paramètres
Windows Phone, configurez ces paramètres
Windows Tablet, configurez ces paramètres
Amazon, configurez ces paramètres
Windows Mobile/CE, configurez ces paramètres

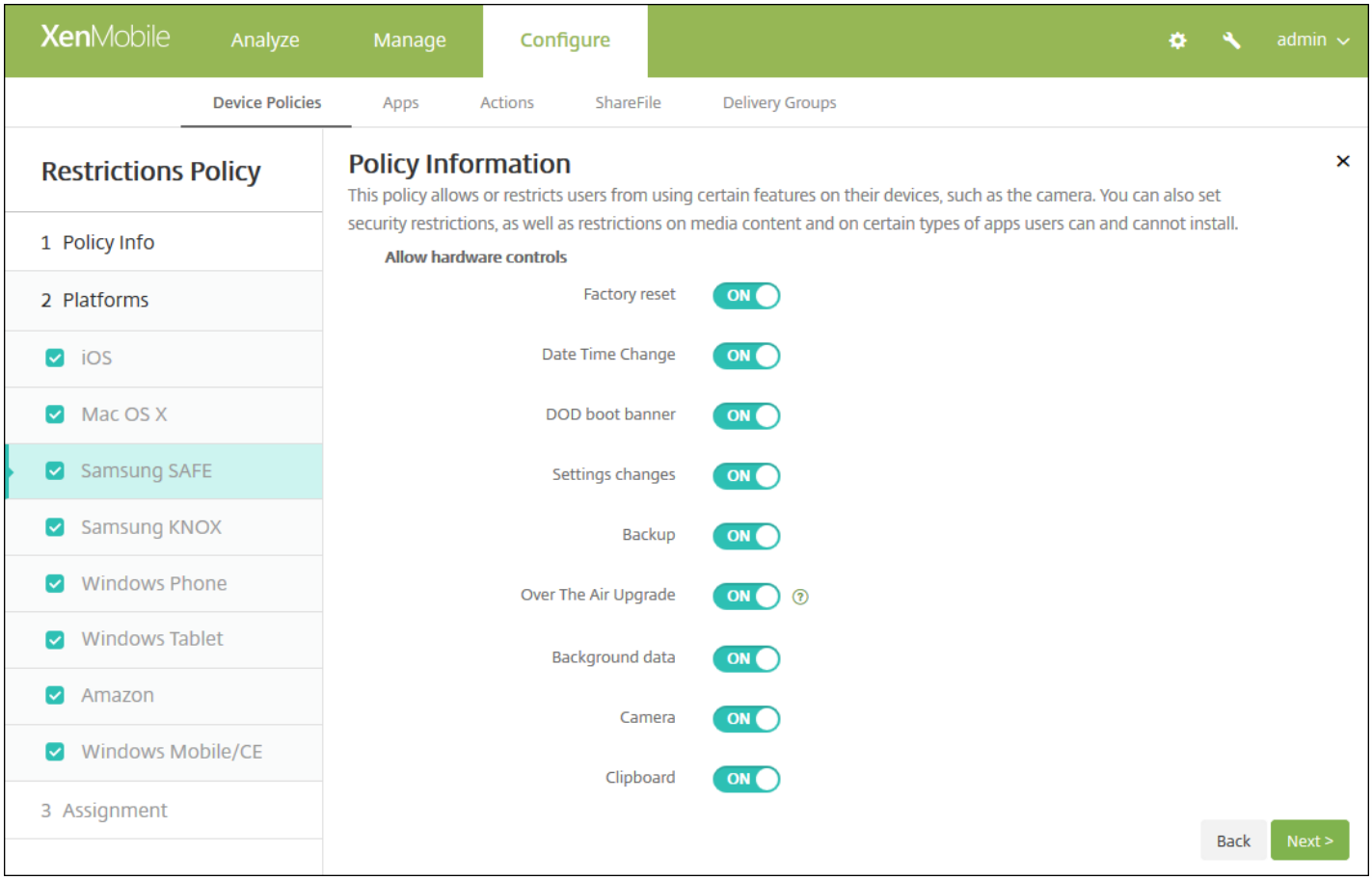
Une fois que vous avez fini de définir des restrictions pour une plate-forme, reportez-vous à l'étape 7 plus loin dans cet article pour savoir comment configurer les règles de déploiement de cette plate-forme.



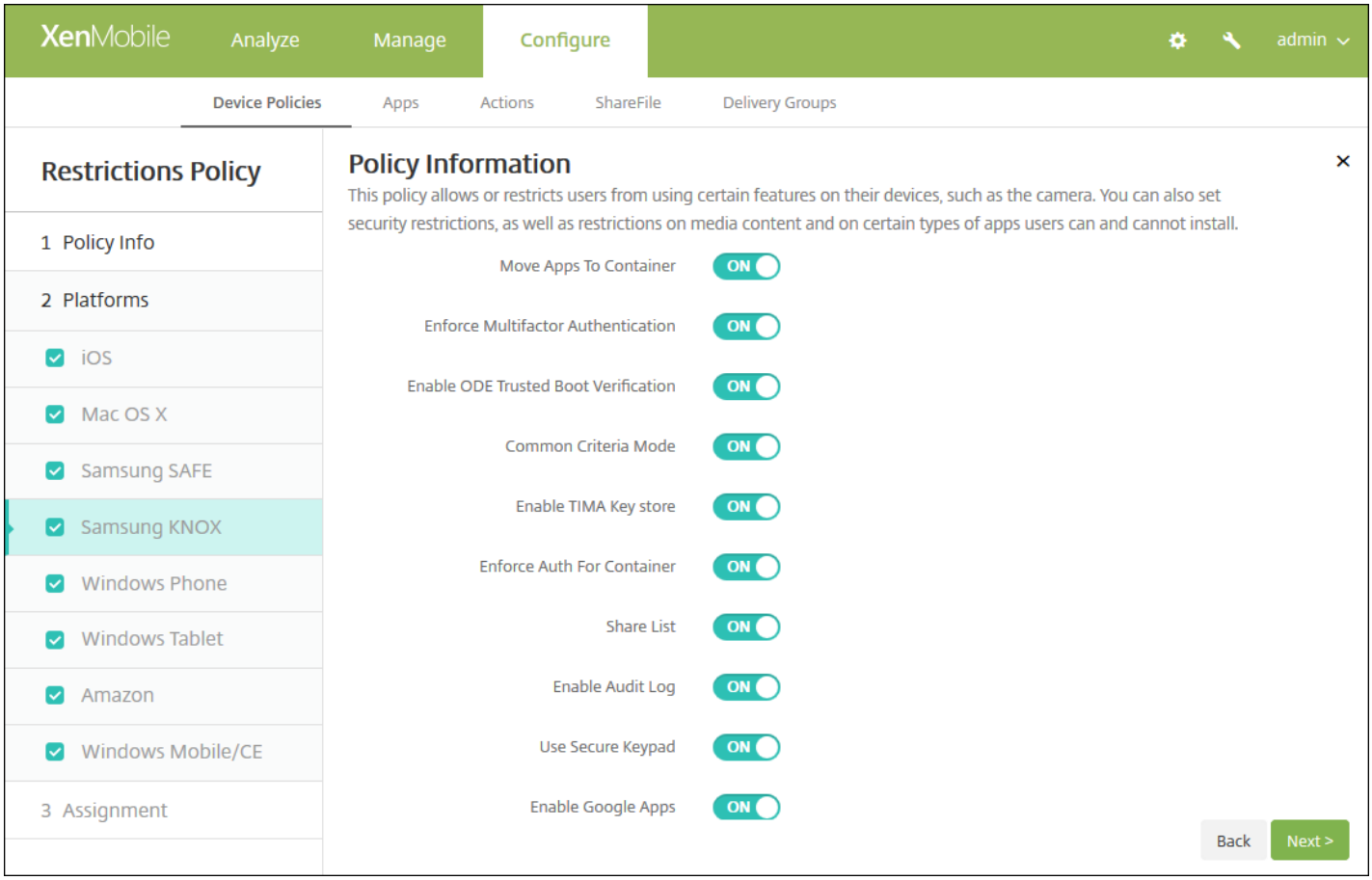
Paramètres iOS



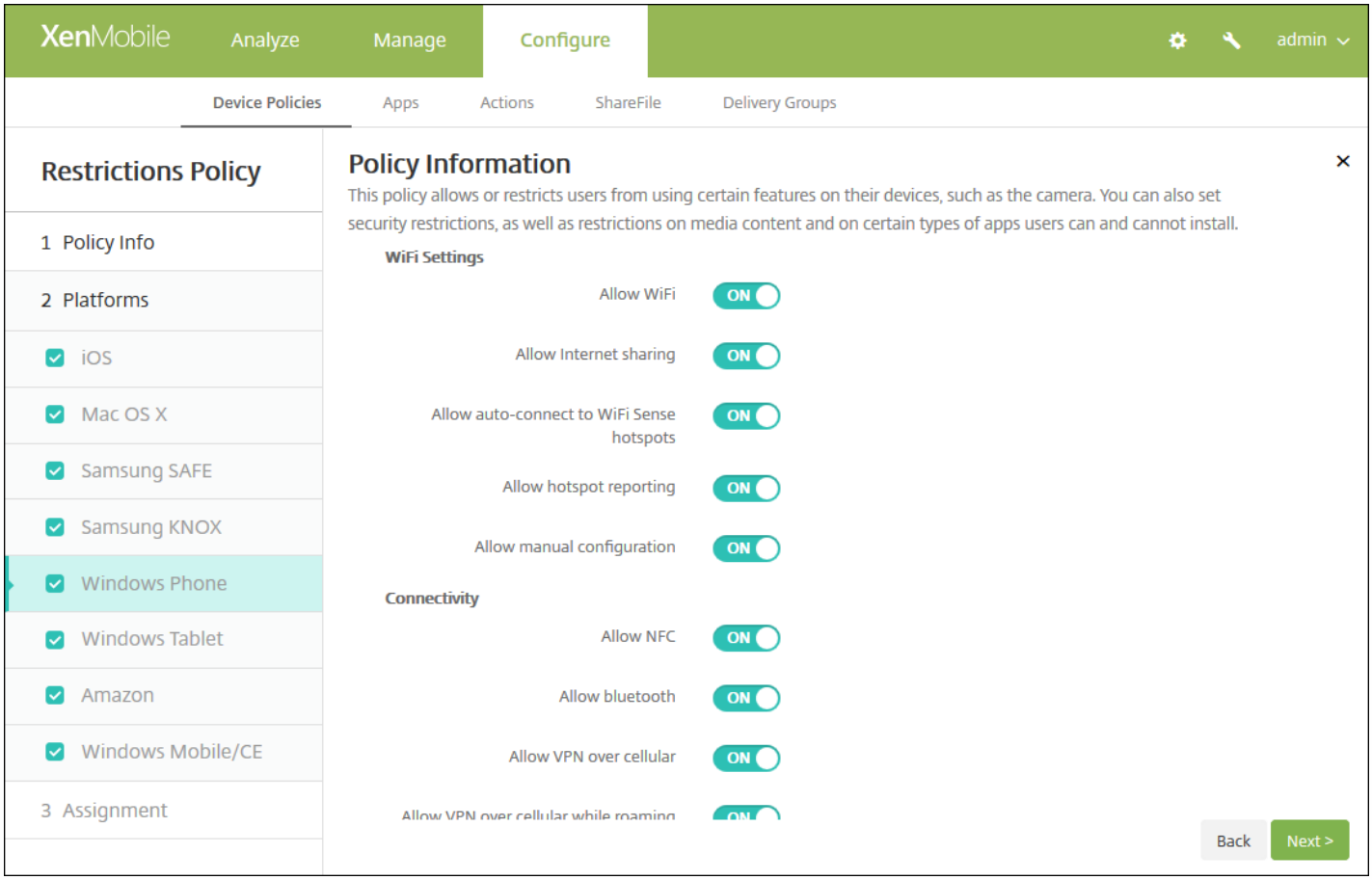
Paramètres Mac OS X



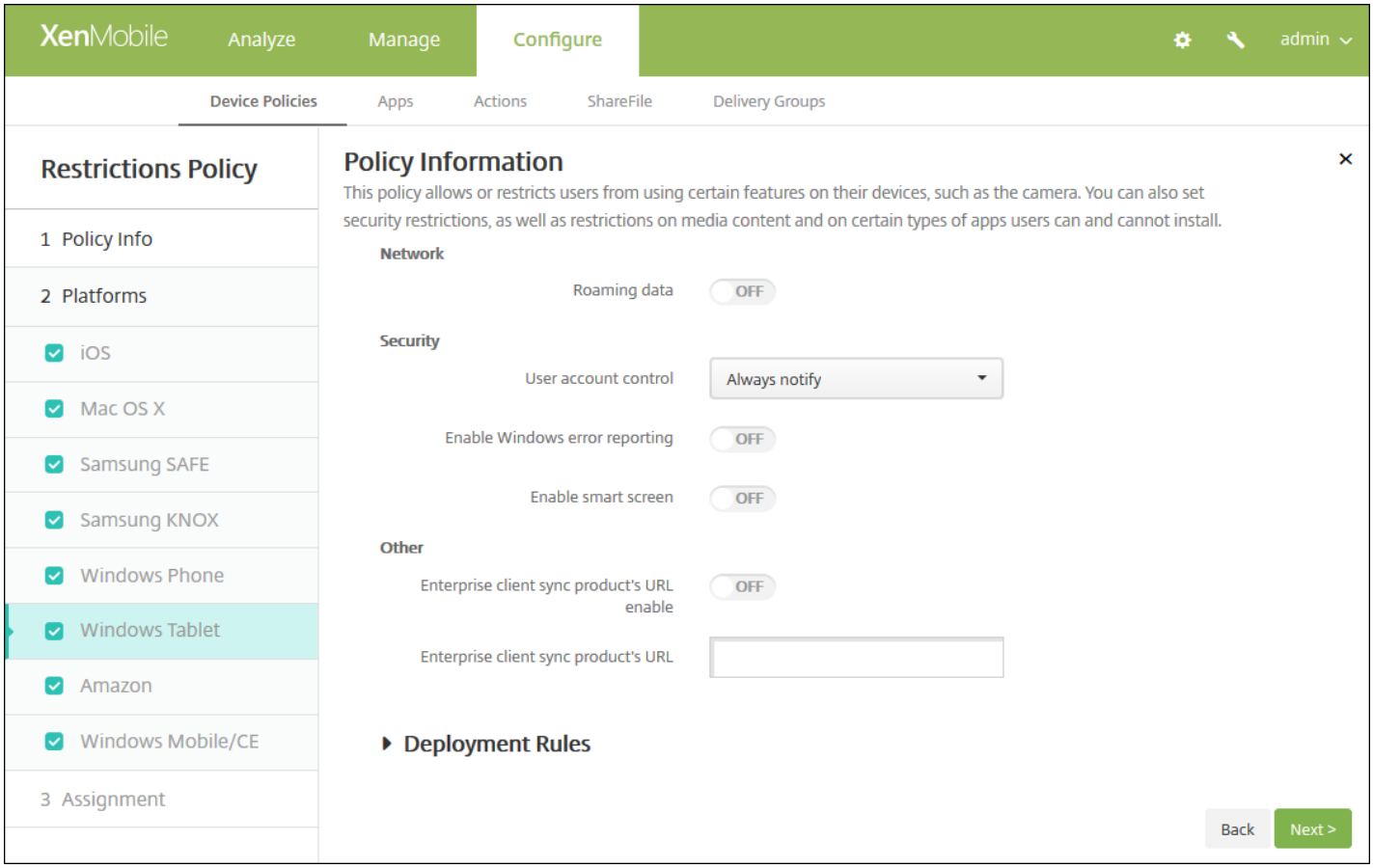
Paramètres Samsung SAFE



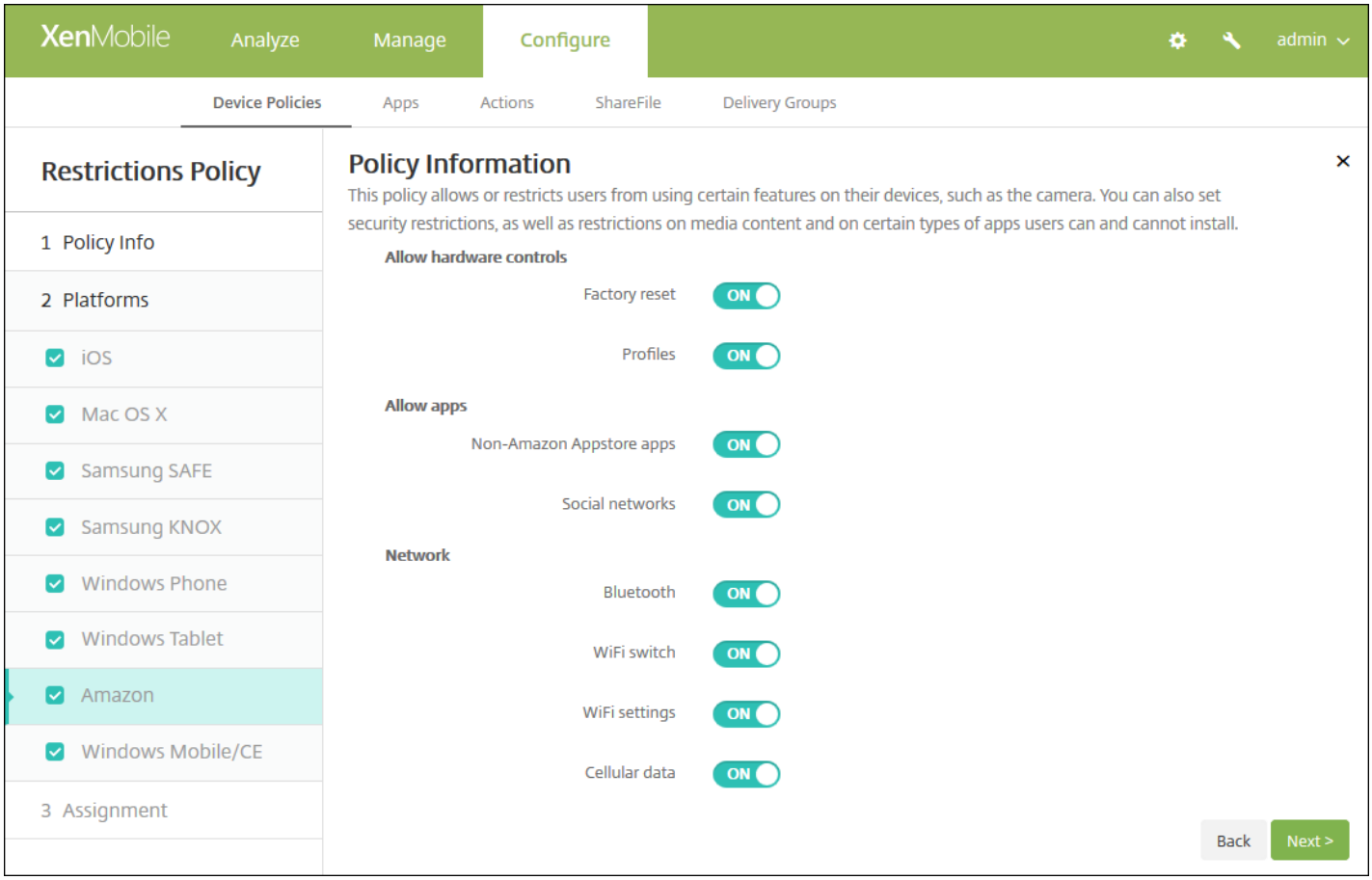
Paramètres Samsung KNOX



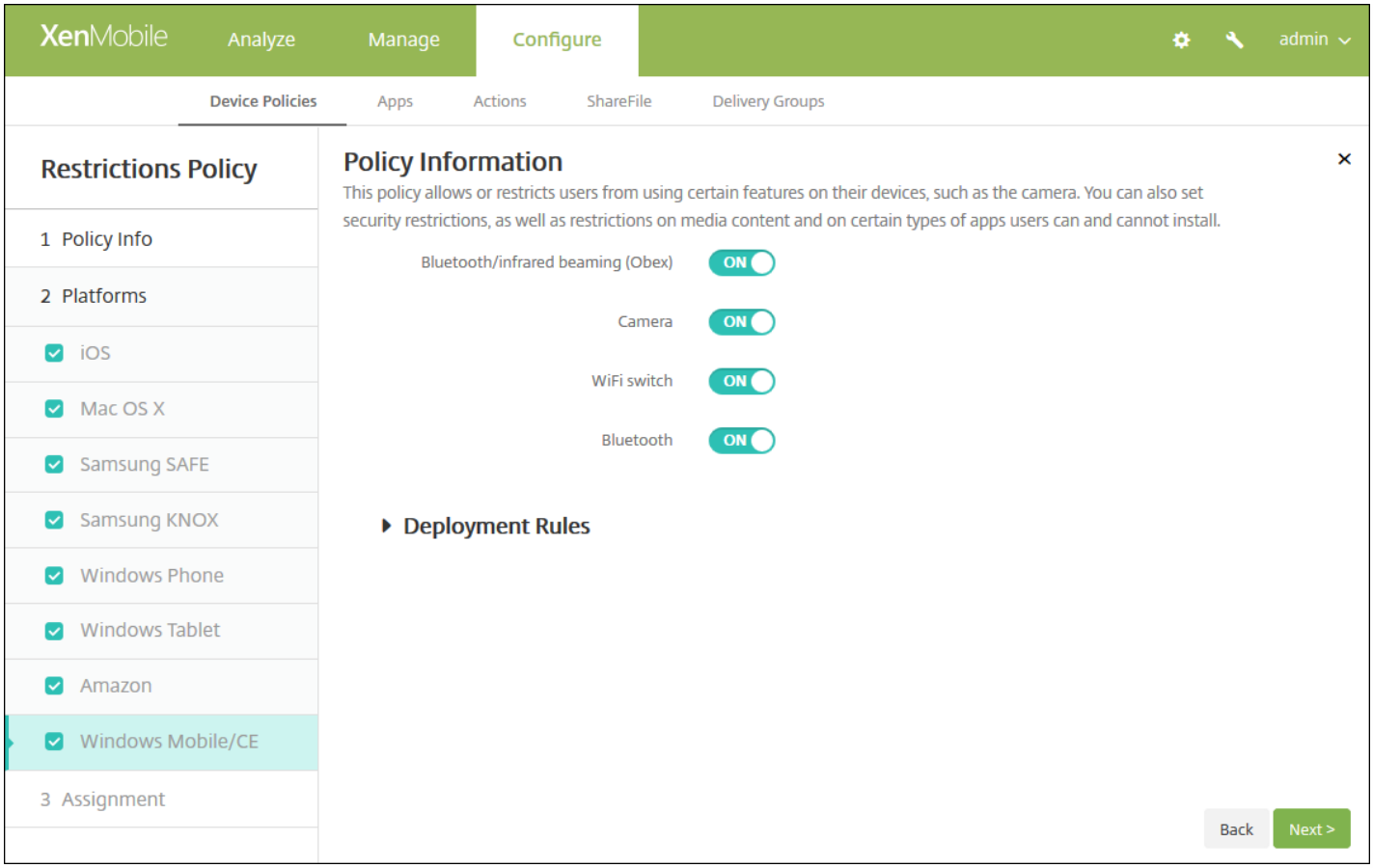
Paramètres Windows Phone



Paramètres Windows Tablet



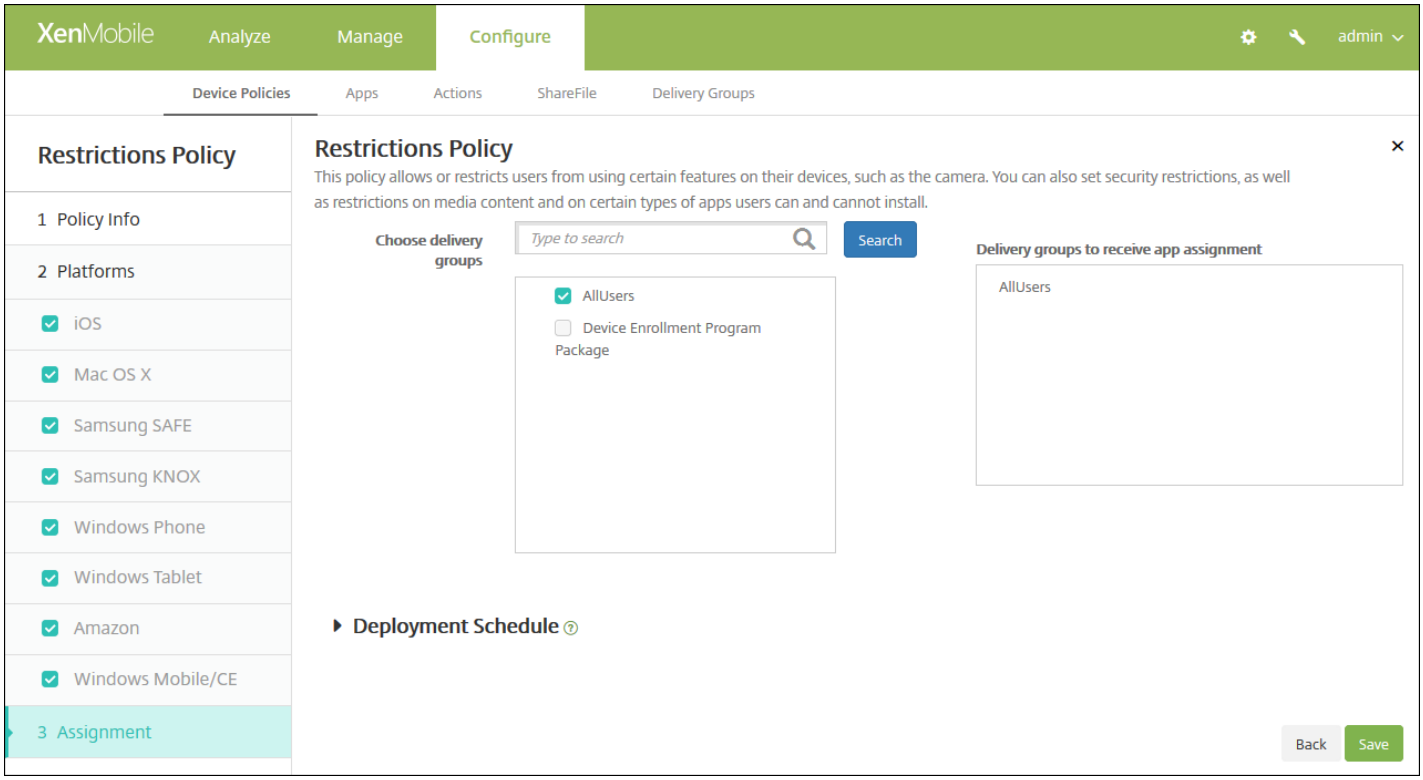
Paramètres Amazon



Paramètres Windows Mobile/CE

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**, la page d'attribution de **Stratégie de restrictions** s'affiche.



9. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

10. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

Stratégie d'itinérance

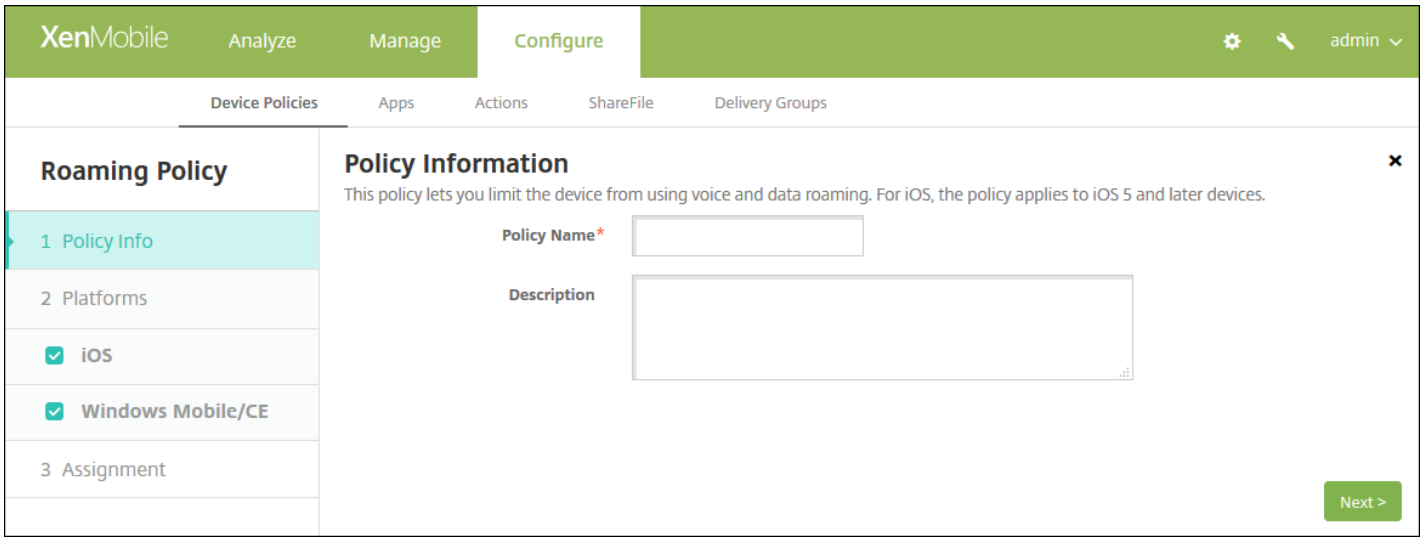
Jul 27, 2016

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.

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. Cliquez sur **Plus**, puis, sous **Accès réseau**, cliquez sur **Itinérance**. La page d'informations **Stratégie d'itinérance** s'affiche.



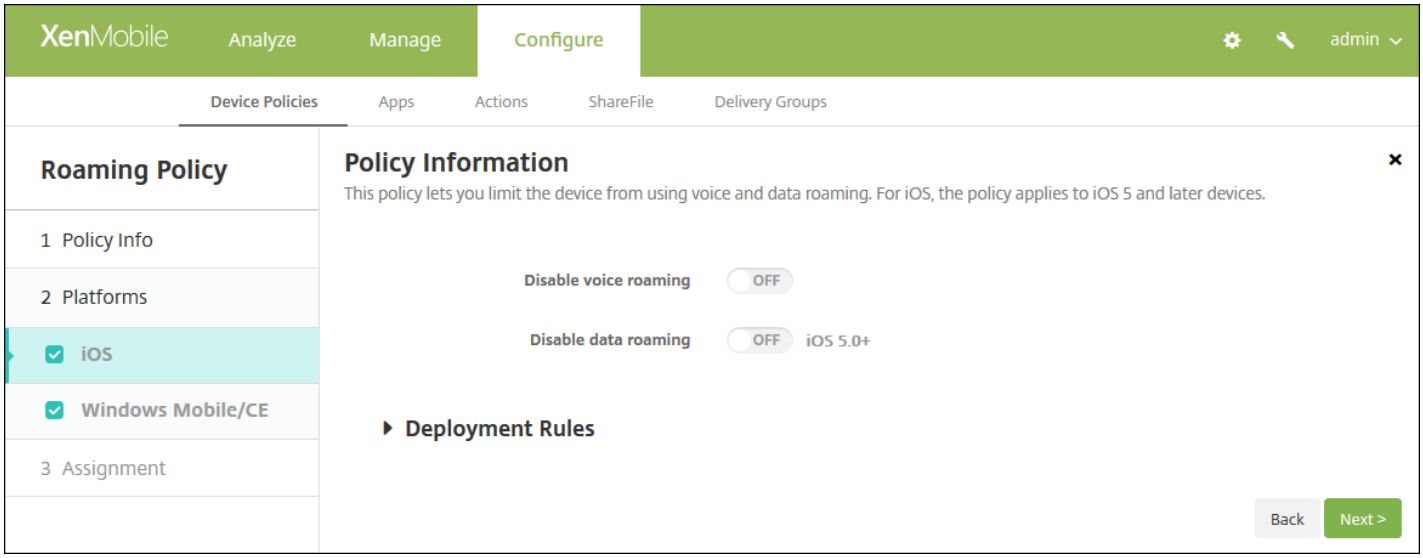
4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

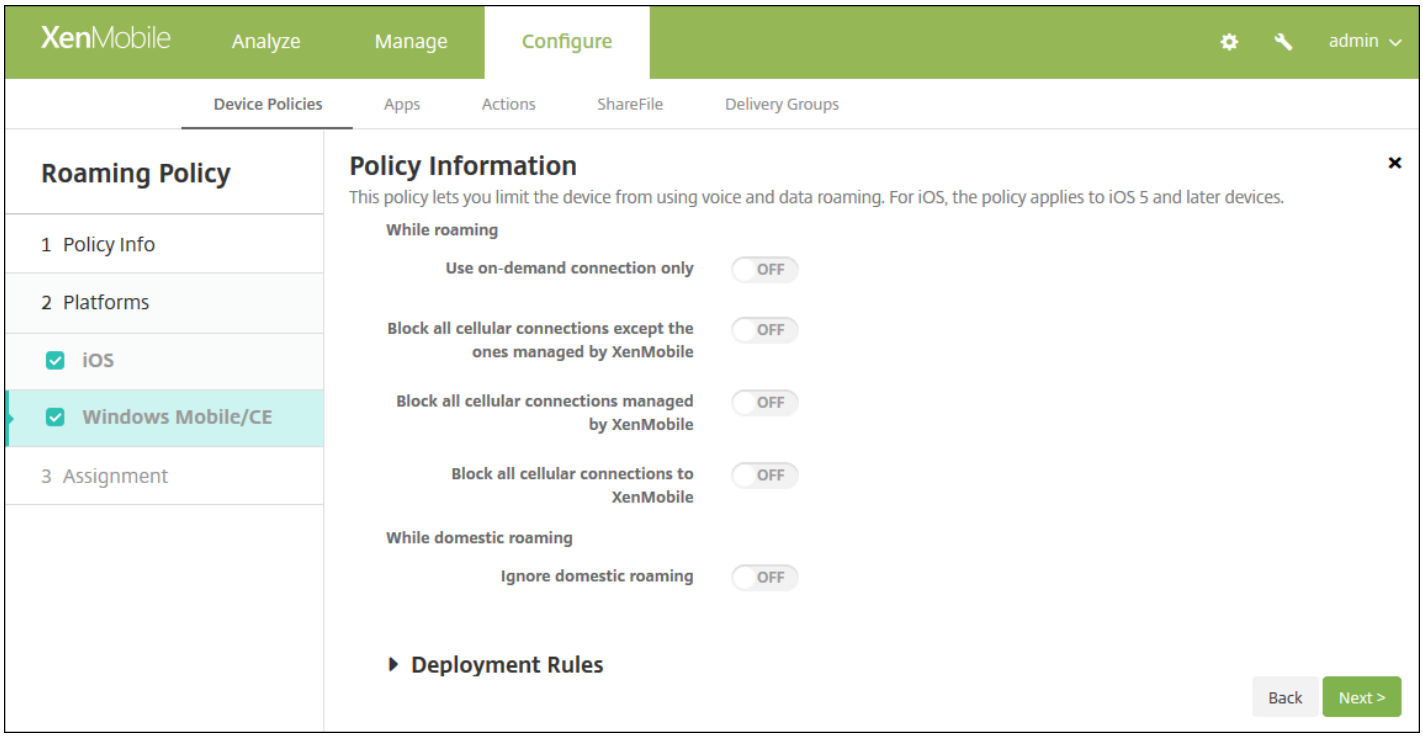
6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.



Pour configurer ces paramètres :

- **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 désactivée. La valeur par défaut est **OFF**, 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 **OFF**, ce qui active l'itinérance des données.

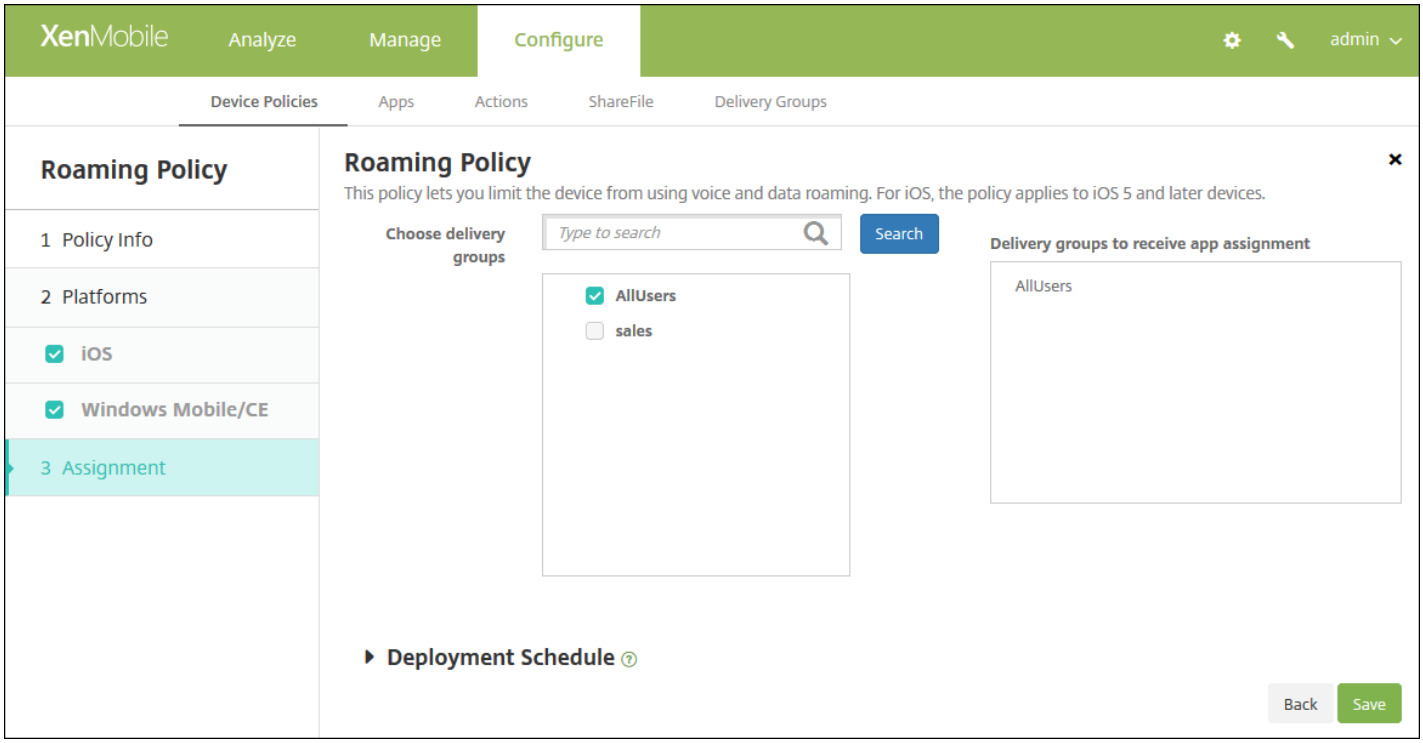


Pour configurer ces paramètres :

- 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.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie d'itinérance** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement.

L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.

- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégies de clé de licence MDM Samsung

Jul 27, 2016

XenMobile prend en charge et étend les stratégies Samsung for Enterprise (SAFE) et Samsung KNOX. SAFE fait partie d'une famille de solutions qui fournit des améliorations de sécurité pour les entreprises via l'intégration à des solutions MDM. Samsung KNOX est une solution du programme SAFE destinée à une utilisation professionnelle conçue pour renforcer la sécurité sur la plate-forme Android.

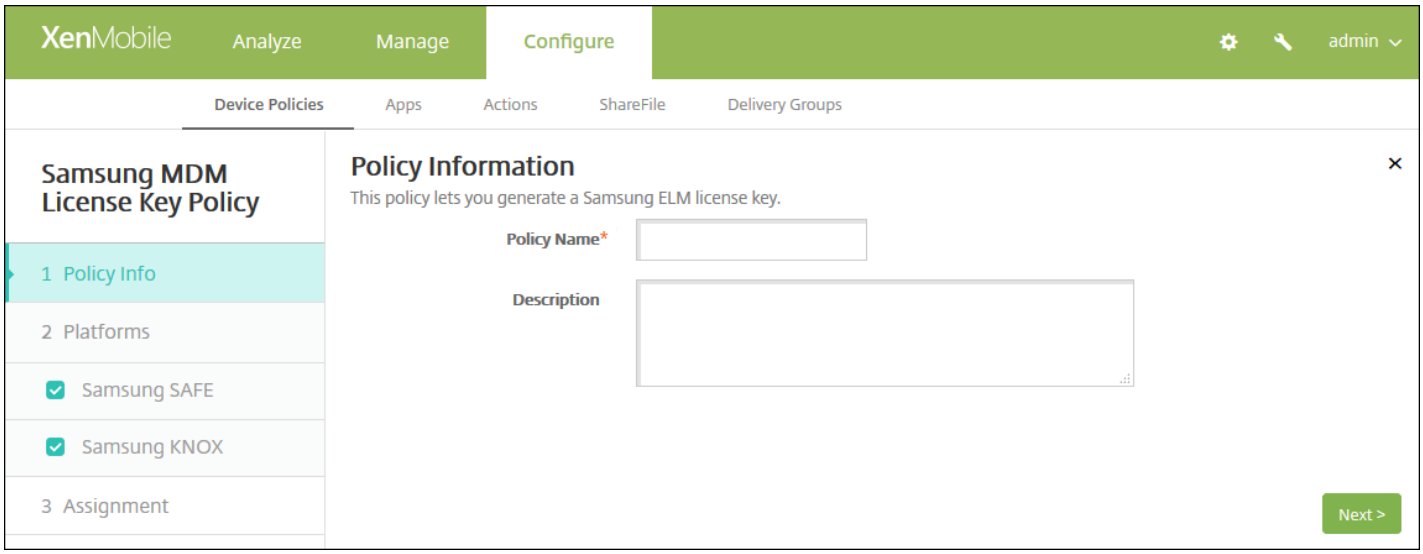
Vous devez activer les API SAFE en déployant la clé Samsung ELM (Enterprise License Management) intégrée sur un appareil avant de pouvoir déployer des stratégies et restrictions SAFE. Pour activer les API Samsung KNOX, vous devez acheter une licence Samsung KNOX Workspace à l'aide du Samsung KNOX License Management System (KLMS) en plus de déployer la clé Samsung ELM. Le KMLS Samsung provisionne des licences valides sur des solutions MDM afin d'activer les API Samsung KNOX sur les appareils mobiles. Vous devez vous procurer ces licences auprès de Samsung car elles ne sont pas fournies par Citrix.

Vous devez déployer Worx Home en conjonction avec la clé Samsung ELM pour activer les API SAFE et Samsung KNOX. Vous pouvez vérifier que les API SAFE sont activés en consultant les propriétés de l'appareil. Lorsque la clé Samsung ELM est déployée, le paramètre API Samsung MDM disponible est défini sur **True**.

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. Cliquez sur **Plus**, puis sous **Sécurité**, cliquez sur **Clé de licence MDM Samsung**. La page d'informations **Stratégie de clé de licence MDM Samsung** s'affiche.



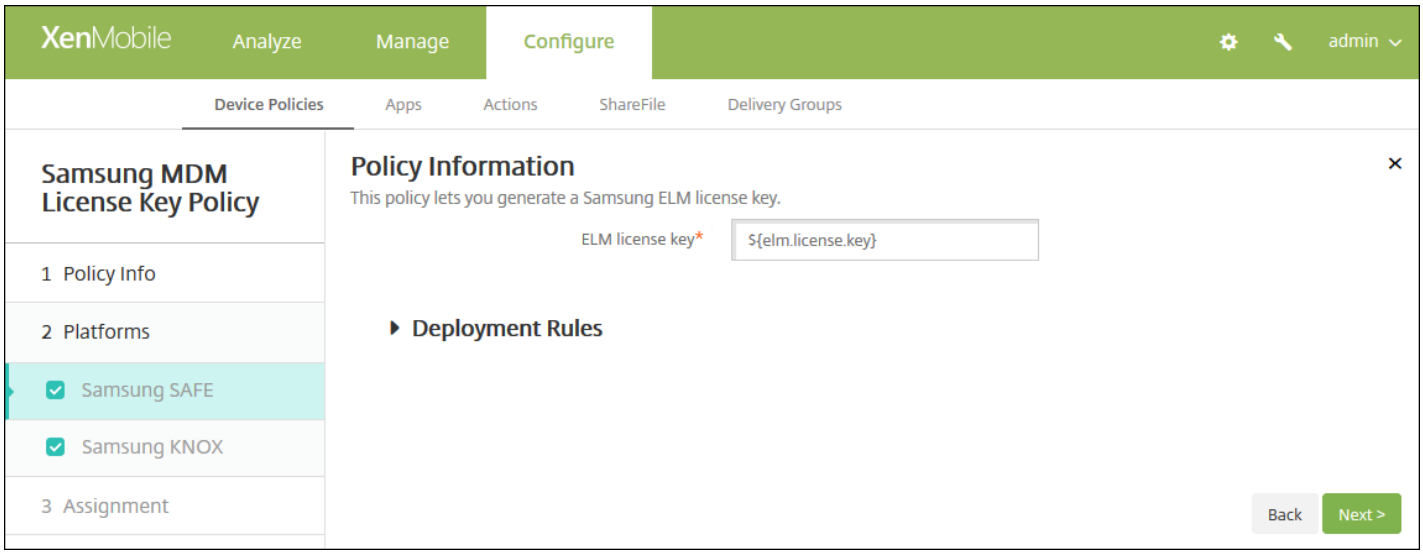
4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

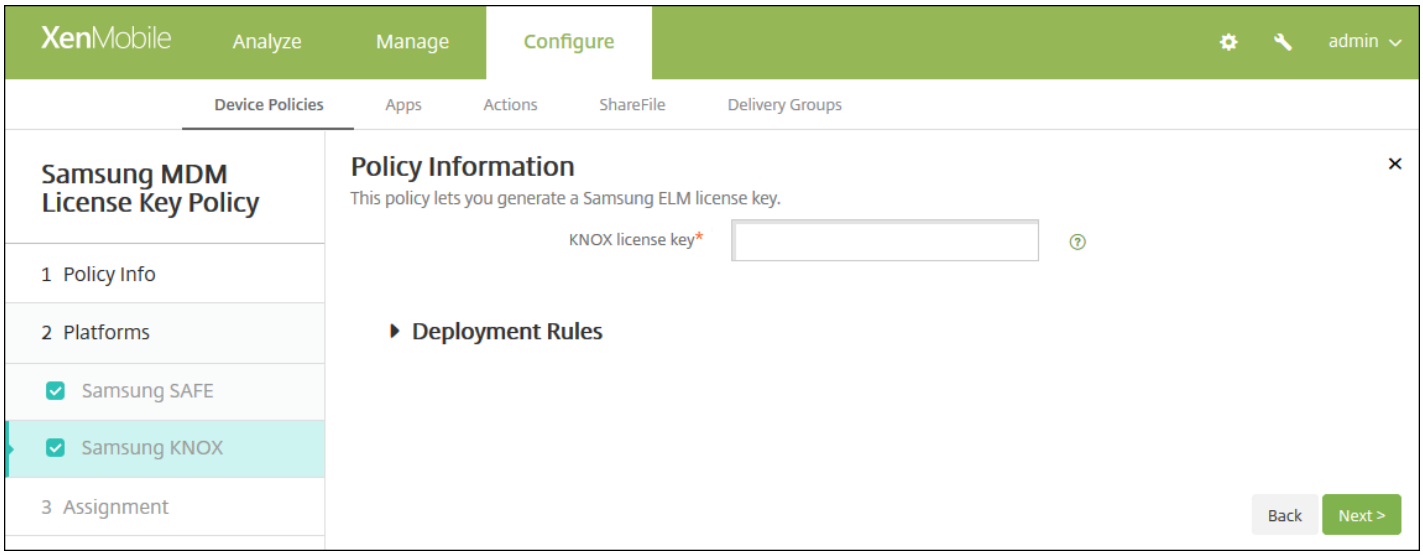
6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.



Configurez ce paramètre :

- **Clé de licence ELM** : ce champ doit déjà contenir la macro qui génère la clé de licence ELM. Si le champ est vide, entrez la macro ${elm.license.key}.

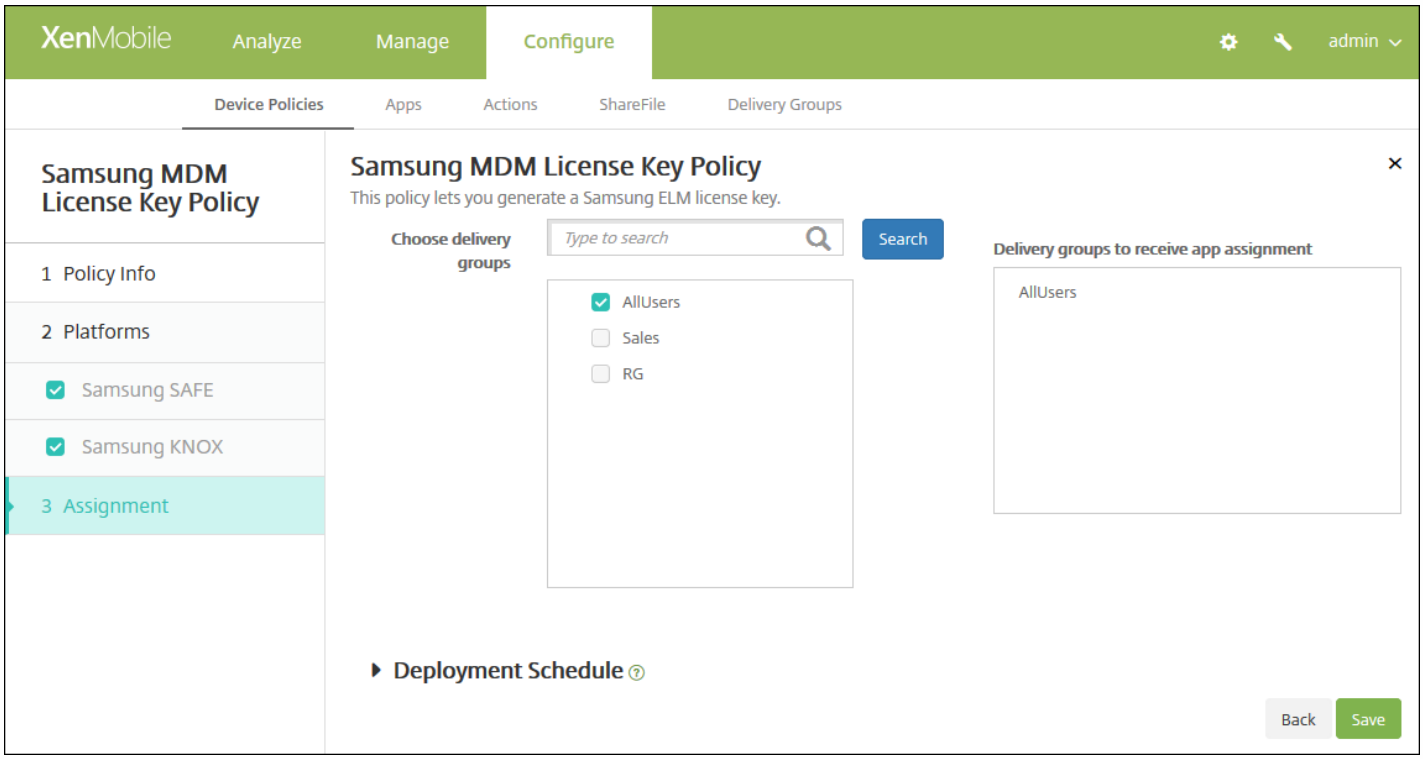


Configurez ce paramètre :

- **Clé de licence KNOX** : entrez la clé de licence KNOX à 25 chiffres que vous avez obtenue auprès de Samsung.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de **Stratégie de clé de licence MDM Samsung** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégie de pare-feu Samsung SAFE

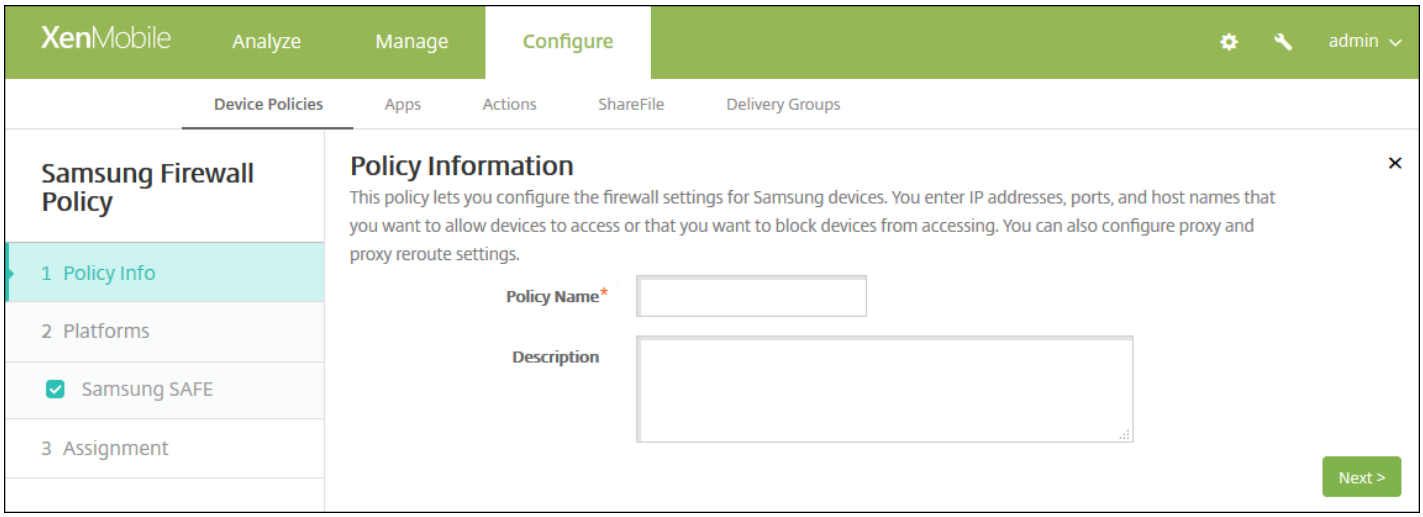
Jul 27, 2016

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 auxquels vous souhaitez autoriser les appareils à accéder ou auxquels vous souhaitez empêcher les appareils d'accéder. Vous pouvez également configurer les paramètres de redirection de proxy et de proxy.

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.

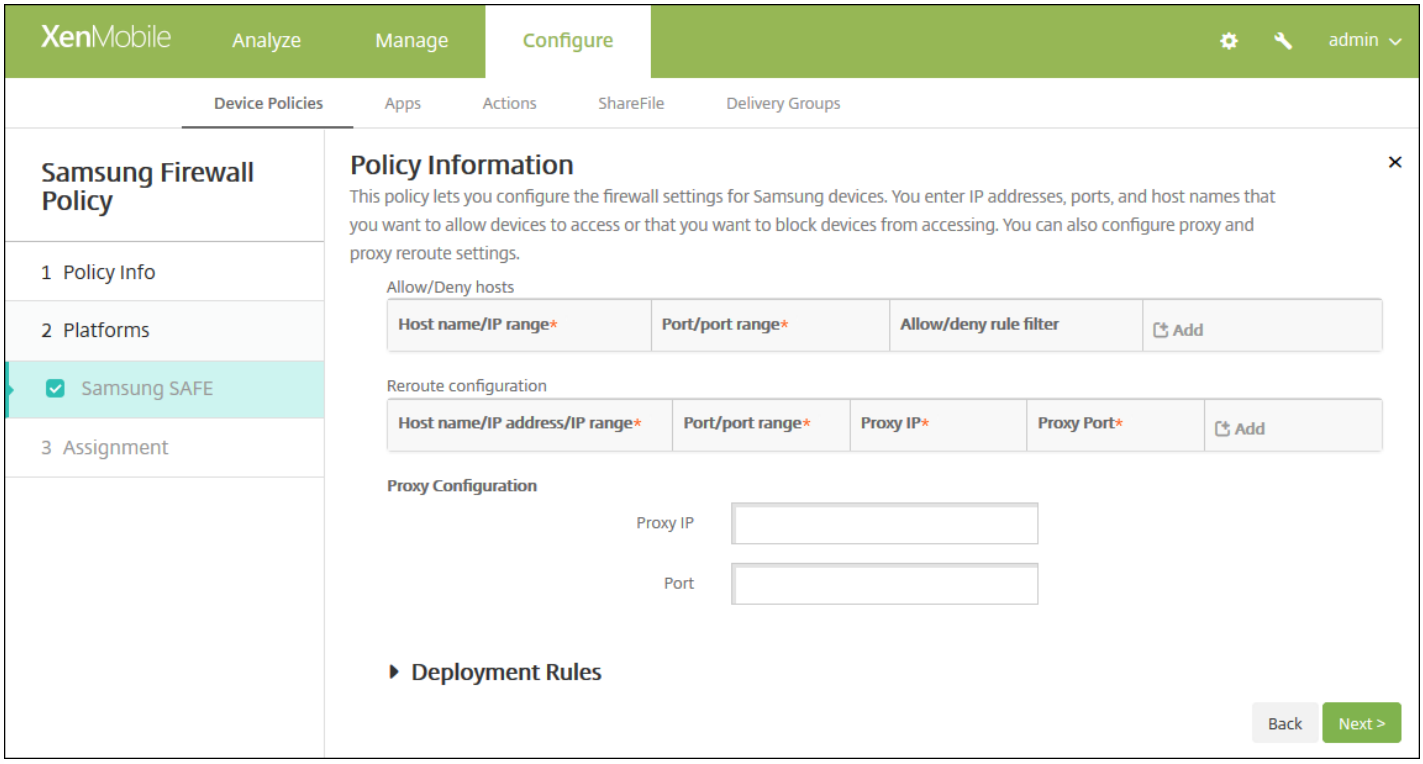
3. Développez **Plus**, puis, sous **Accès réseau**, cliquez sur **Pare-feu Samsung**. La page **Stratégie de pare-feu Samsung** s'affiche.



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 **Next**. La page d'informations sur la plate-forme **Samsung SAFE** s'affiche.



6. Configurez les paramètres suivants :

- **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** : entrez le nom d'hôte ou une plage d'adresses IP pour le site concerné.
    - **Port/Plage de ports** : entrez le port ou la 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.
    - Cliquez sur **Enregistrer** ou sur **Annuler**.
- **Configuration de redirection**
  - Pour chaque serveur proxy que vous souhaitez configurer, cliquez sur **Ajouter** et procédez comme suit :
    - **Nom d'hôte/adresse IP** : entrez le nom d'hôte ou la plage d'adresses IP pour la redirection proxy.
    - **Port/Plage de ports** : entrez le port ou la plage de ports.
    - **IP proxy** : entrez l'adresse IP du serveur proxy.
    - **Port proxy** : entrez le port du serveur proxy.
    - Cliquez sur **Enregistrer** ou sur **Annuler**.

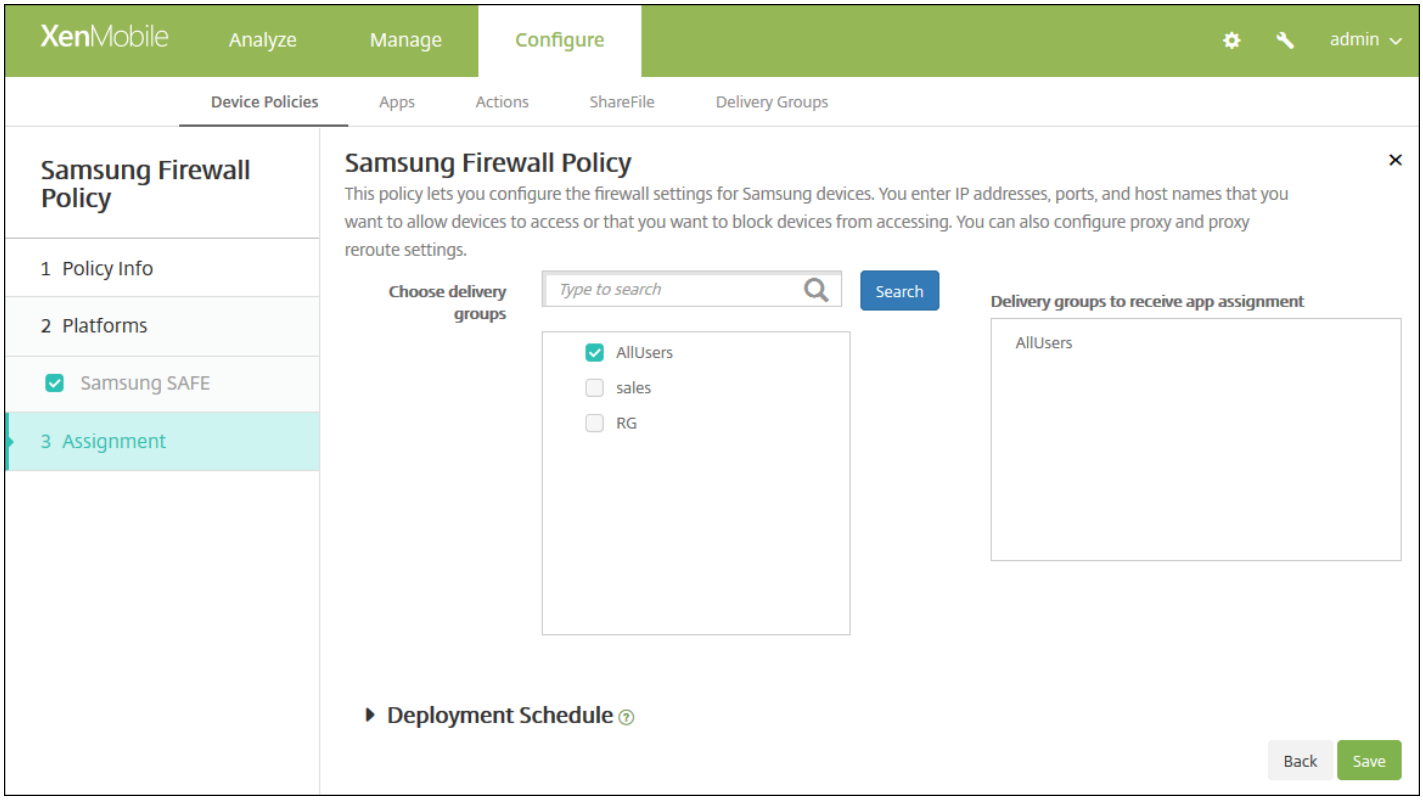
    Remarque : pour supprimer un élément existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

    Pour modifier un élément, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.
- **Configuration du proxy**
  - **IP Proxy** : saisissez l'adresse IP du serveur proxy.

- **Port** : entrez le port du serveur proxy.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie de pare-feu Samsung** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 lorsque le déploiement précédent a échoué.** L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégies SCEP

Jul 27, 2016

Cette stratégie vous permet de configurer des appareils iOS et Mac OS X 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.

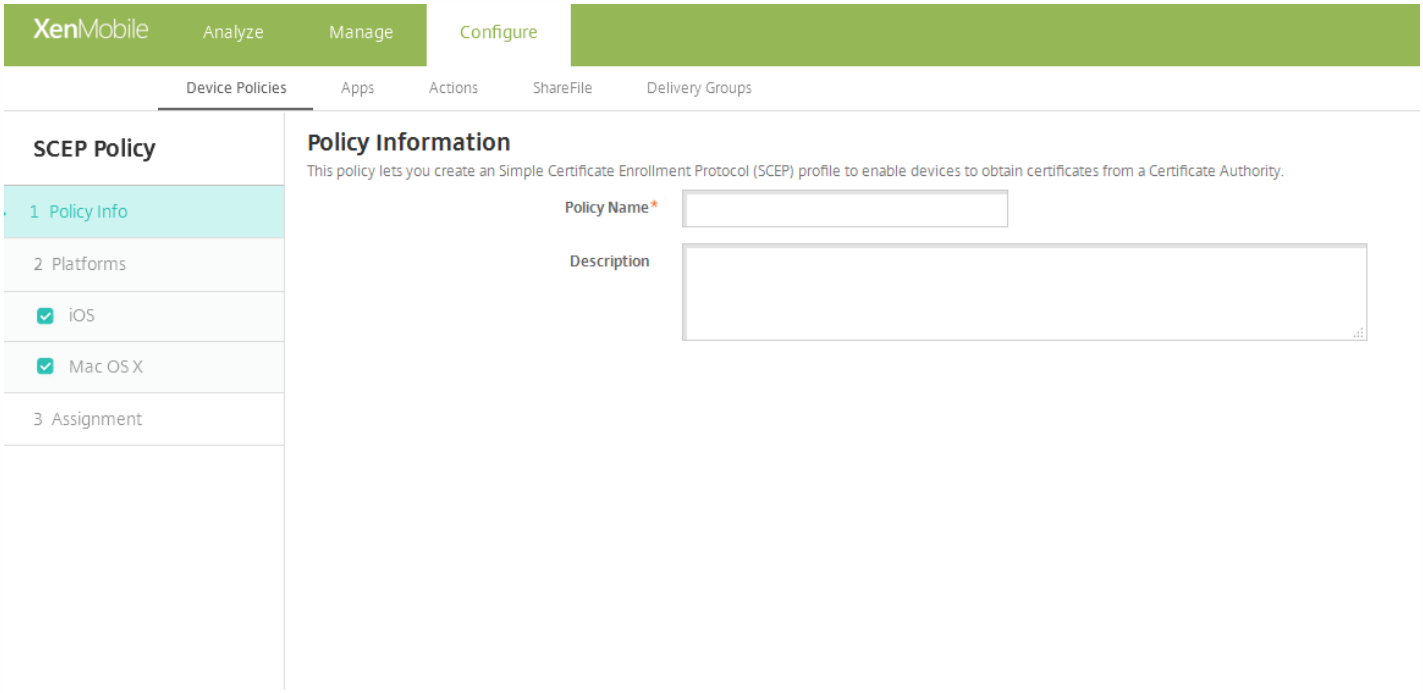
Paramètres iOS

Paramètres Mac OS X

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 **SCEP**. La page d'informations **Stratégie SCEP** s'affiche.



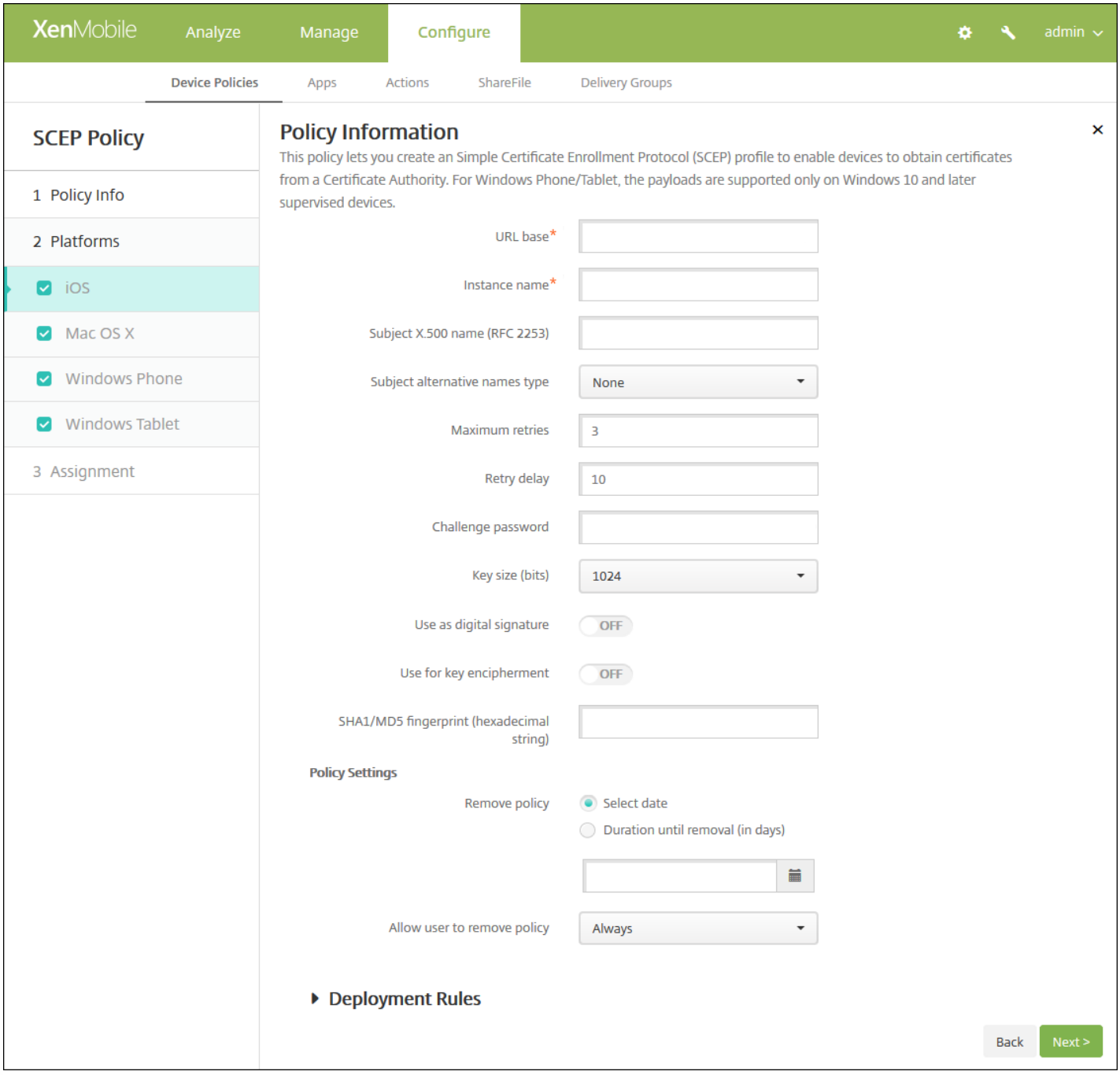
4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

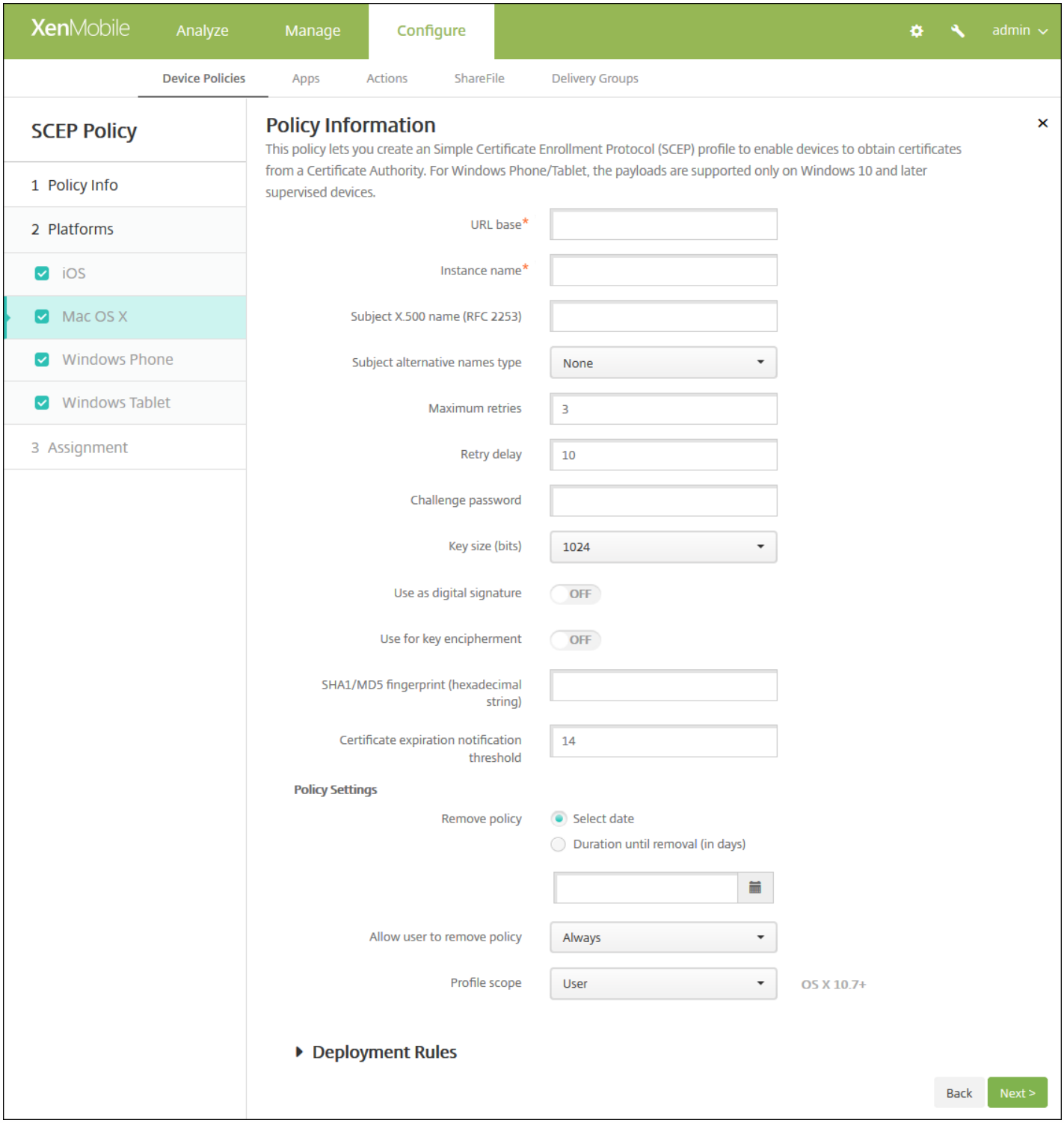
Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.



Pour configurer ces paramètres :

- **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 de **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 de **10**.
- **Vérifier le mot de passe** : entrez un secret pré-partagé.
- **Taille de la clé (bits)** : dans la liste, cliquez sur la taille de la clé en bits, **1024** ou **2048**. La valeur par défaut est de **1024**.
- **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**
  - Sous **Paramètres de stratégie**, à côté de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  - 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.



Pour configurer ces paramètres :

- **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 de **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 de **10**.
- **Vérifier le mot de passe** : entrez un secret pré-partagé.
- **Taille de la clé (bits)** : dans la liste, cliquez sur la taille de la clé en bits, **1024** ou **2048**. La valeur par défaut est de **1024**.
- **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**
  - Sous **Paramètres de stratégie**, à côté de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  - 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.
  - En regard de **Étendue du profil**, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur OS X 10.7 et versions ultérieures.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie SCEP** s'affiche.

9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement.

L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.

- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

Stratégie de clé de sideloading

Jul 27, 2016

Le sideloading dans XenMobile vous permet de déployer des applications sur des appareils Windows 8.1 qui n'ont pas été achetées à partir du Windows Store. Dans la plupart des cas, vous sideloadez les applications que vous développez pour une utilisation en entreprise que vous ne souhaitez pas rendre publiques dans le Windows Store. Pour sideloader des applications, vous devez configurer la clé de sideloading et l'activation de clés et déployer les applications sur les appareils des utilisateurs.

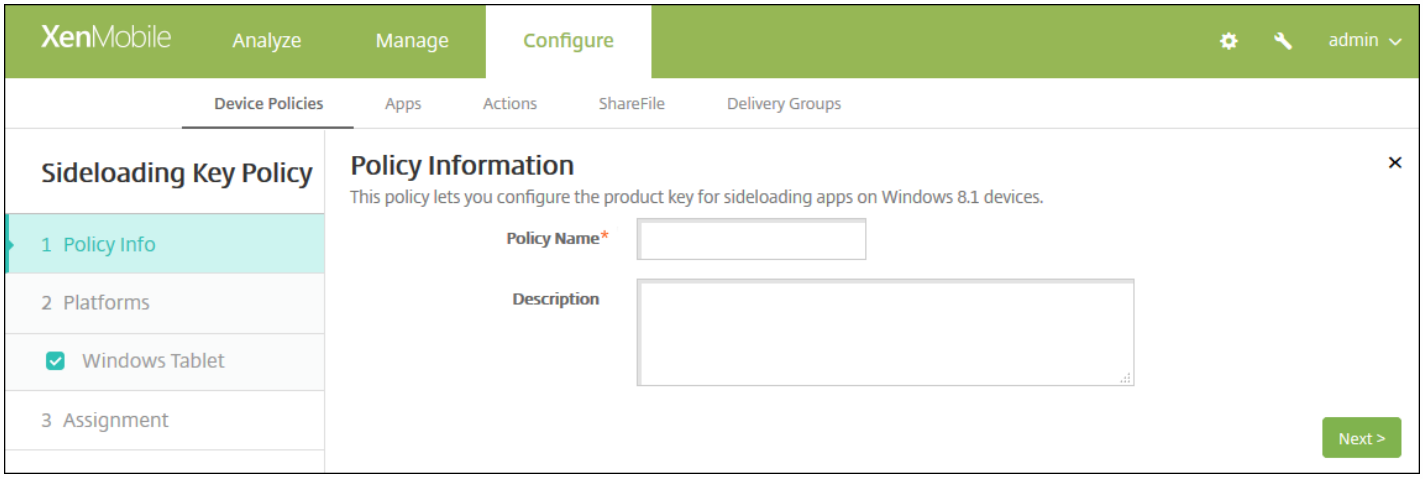
Vous devez disposer des informations suivantes avant de pouvoir créer cette stratégie :

- La clé de sideloading du produit, que vous pouvez obtenir en vous connectant au Centre de gestion des licences en volume Microsoft.
- L'activation de clé, que vous créez via la ligne de commande après avoir obtenu la clé de sideloading du produit.

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.

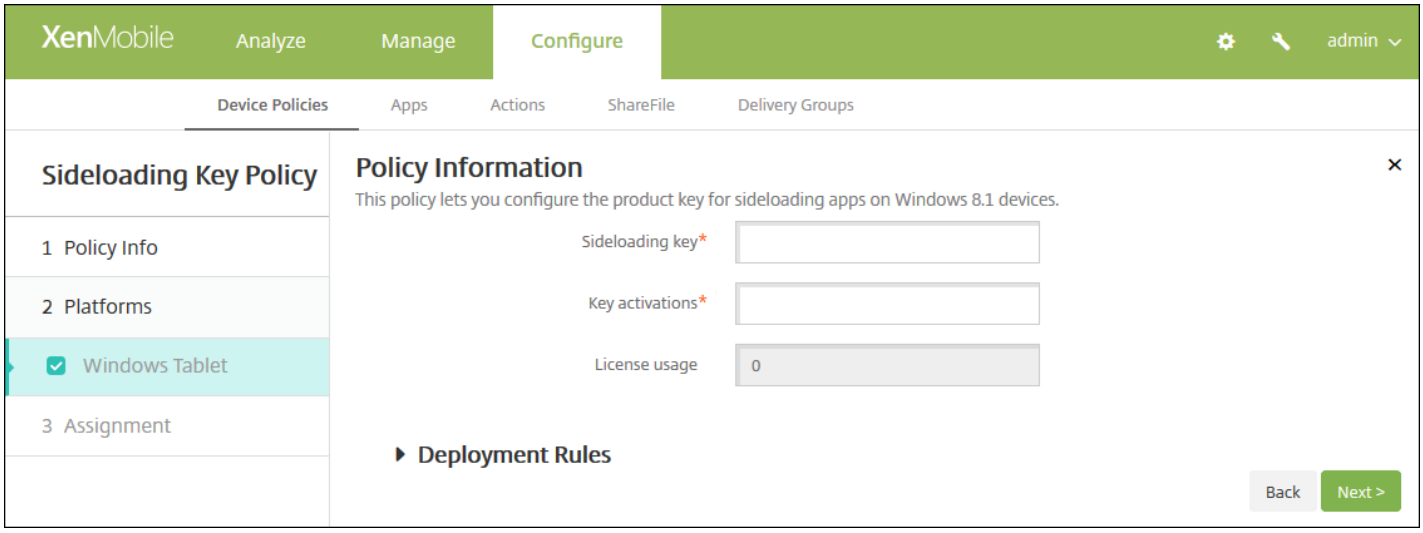
3. Développez **Plus** puis, sous **Applications**, cliquez sur **Clé de sideloading**. La page **Stratégie de clé de sideloading** s'affiche.



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 **Next**. La page d'informations **Windows Tablet** s'affiche.

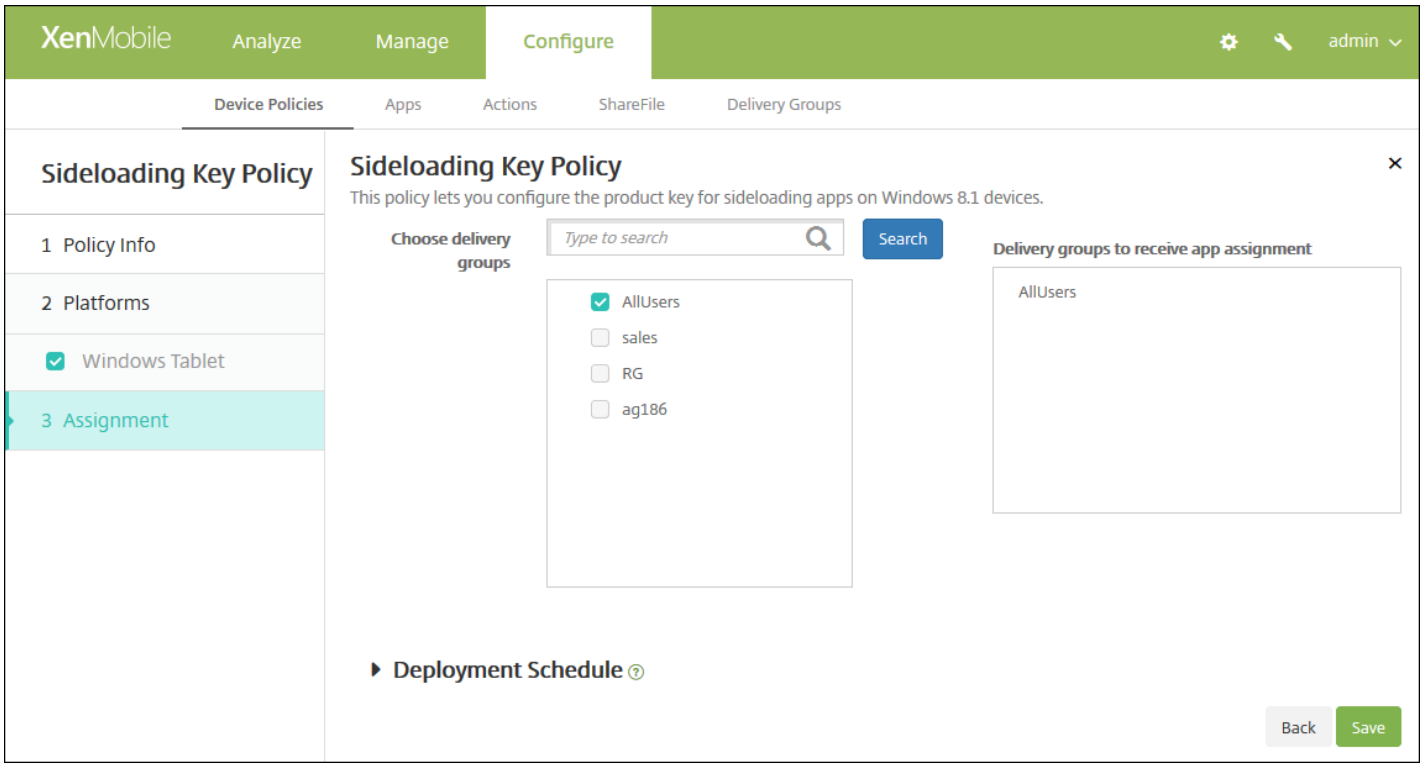


6. Configurez les paramètres suivants :

- **Clé de sideloading** : entrez la clé de sideloading que vous avez obtenue à partir du Centre de gestion des licences en volume Microsoft.
- **Activation de clés** : entrez l'activation de clé que vous avez créée pour la clé de sideloading.
- **Utilisation des licences** : XenMobile calcule cette valeur en fonction du nombre de tablettes inscrites. Vous ne pouvez pas modifier ce champ.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'assignation de la **Stratégie de clé de sideloading** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez Calendrier de déploiement et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 lorsque le déploiement précédent a échoué.** L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégie de certificat de signature

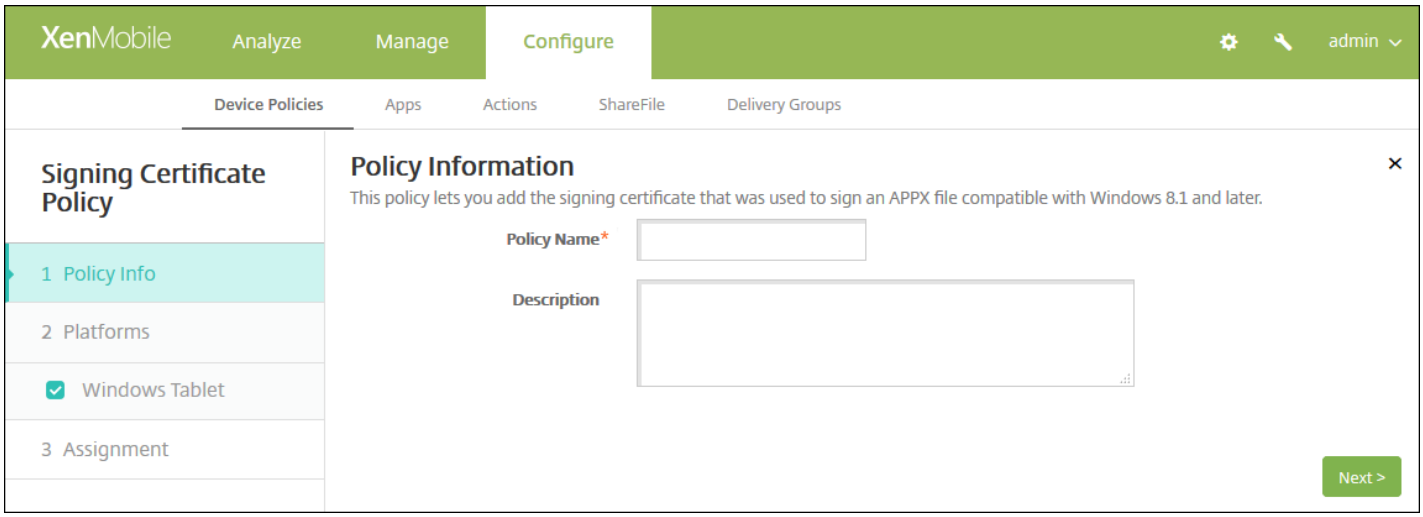
Jul 27, 2016

Vous pouvez ajouter une stratégie d'appareil dans XenMobile pour configurer les certificats de signature à utiliser pour signer les fichiers APPX. Vous avez besoin des certificats de signature si vous voulez distribuer des fichiers APPX aux utilisateurs pour les autoriser à installer des applications sur leurs tablettes Windows.

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.

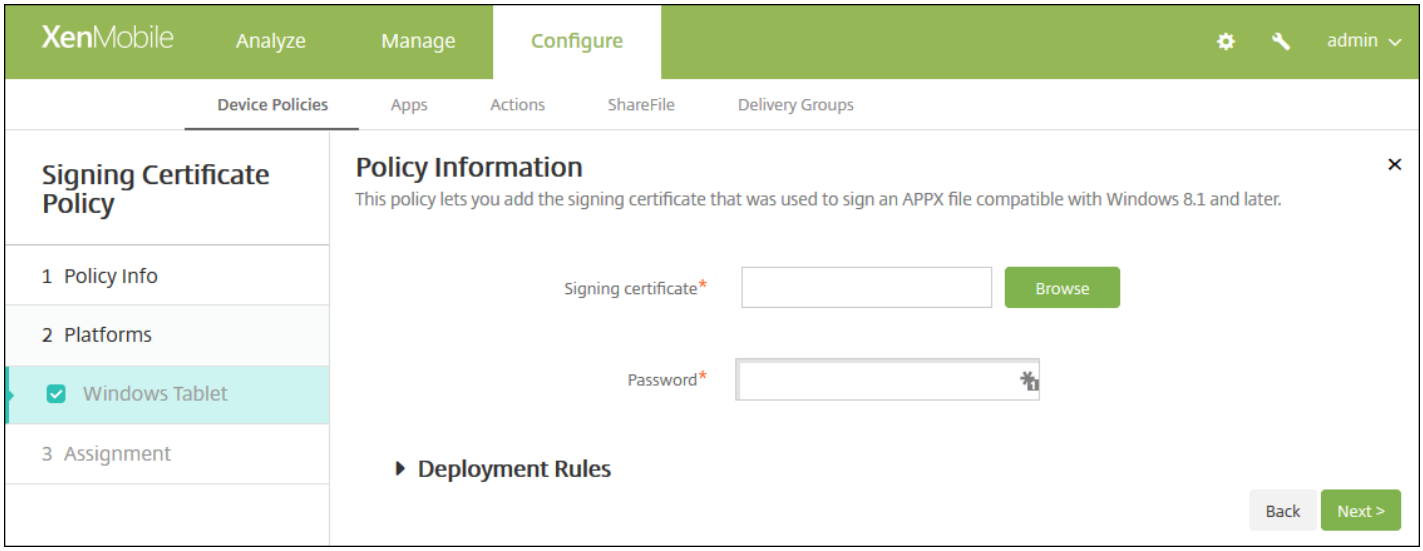
3. Cliquez sur **Plus** puis, sous **Applications**, cliquez sur **Certificat de signature**. La page **Stratégie de certificat de signature** s'affiche.



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 **Next**. La page **Windows Tablet** s'affiche.

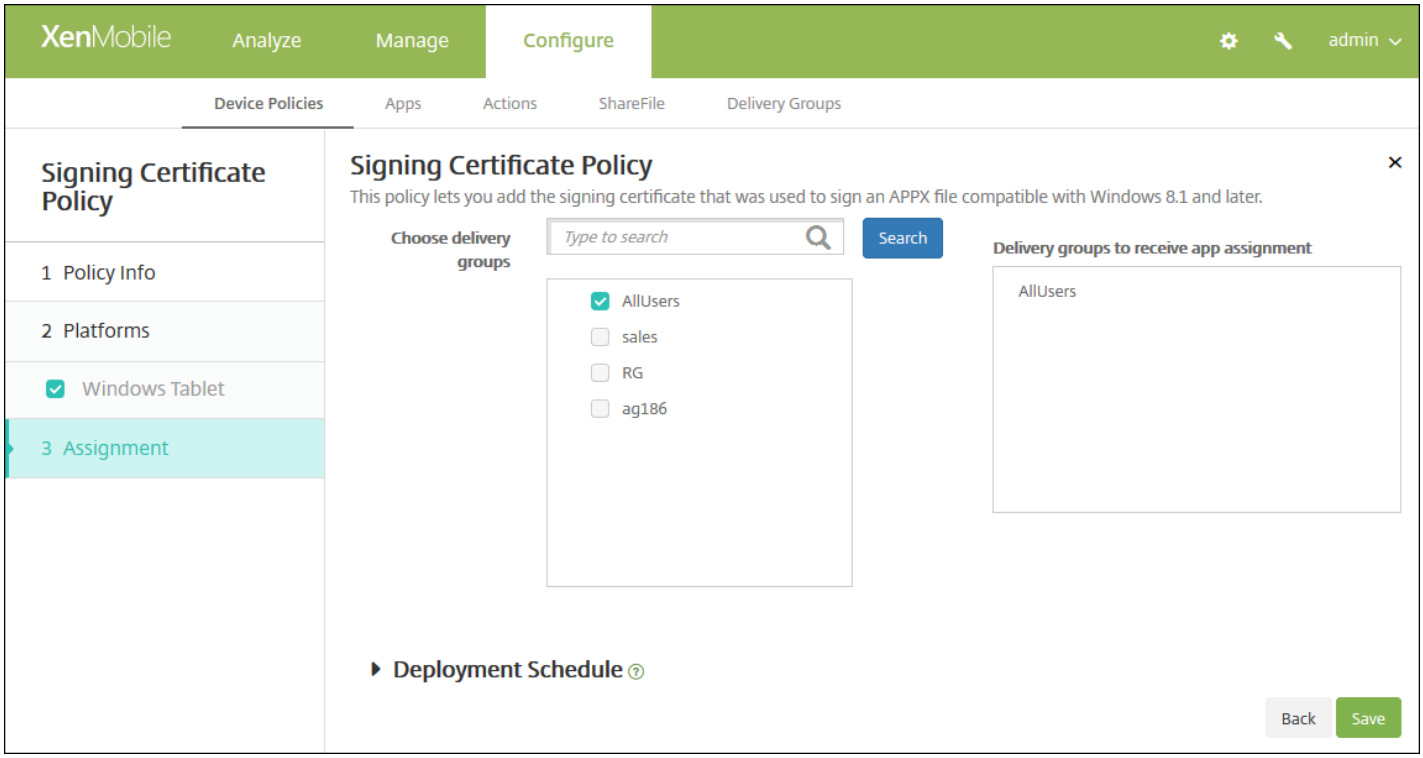


6. Configurez les paramètres suivants :

- **Certificat de signature** : sélectionnez le certificat qui a été utilisé pour signer le fichier APPX en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
- **Mot de passe** : entrez le mot de passe requis pour accéder au certificat de signature.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution **Stratégie de certificat de signature** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous

sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégie de compte SSO

Jul 27, 2016

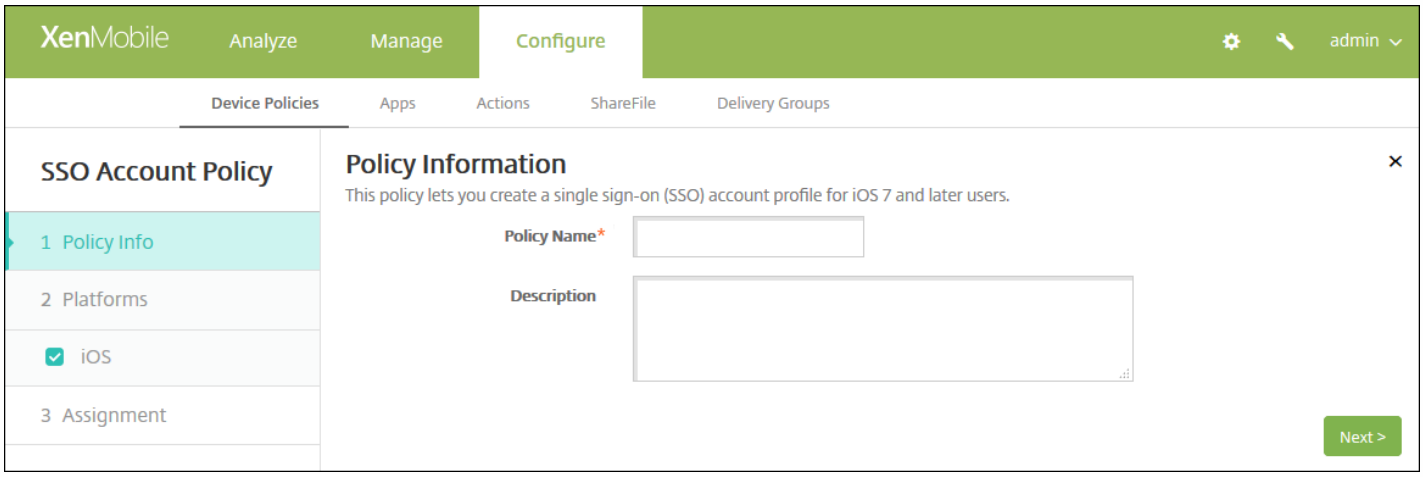
Vous créez des comptes SSO dans XenMobile pour permettre aux utilisateurs de s'authentifier une seule fois pour accéder à XenMobile et à vos ressources d'entreprise internes à partir de différentes applications. Les utilisateurs n'ont pas à stocker d'informations d'identification sur l'appareil. Les 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.

Remarque : cette stratégie s'applique uniquement à iOS 7.0 et versions supérieures.

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.

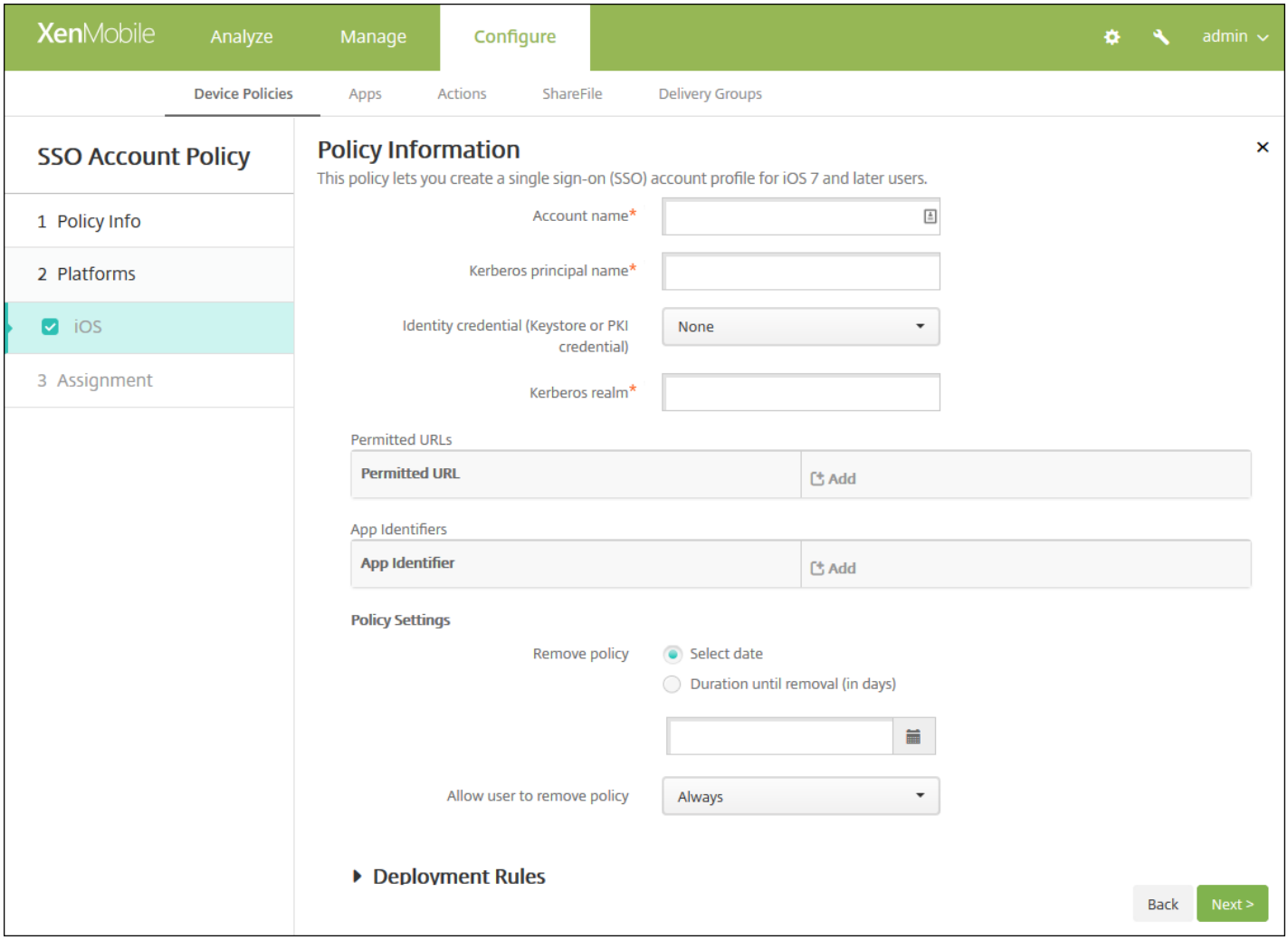
3. Cliquez sur **Plus**, puis, sous **Utilisateur final**, cliquez sur **Compte SSO**. La page **Stratégie de compte SSO** s'affiche.



4. Dans le panneau d'informations **Stratégie de compte SSO**, 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 **Next**. La page d'informations **Plate-forme iOS** s'affiche.



6. Configurez les paramètres suivants :

- **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. d'ouverture de session. La correspondance doit être exacte sur la partie hôte de l'URL, par exemple : http://shopping.apple.com est valide, mais http://*.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.

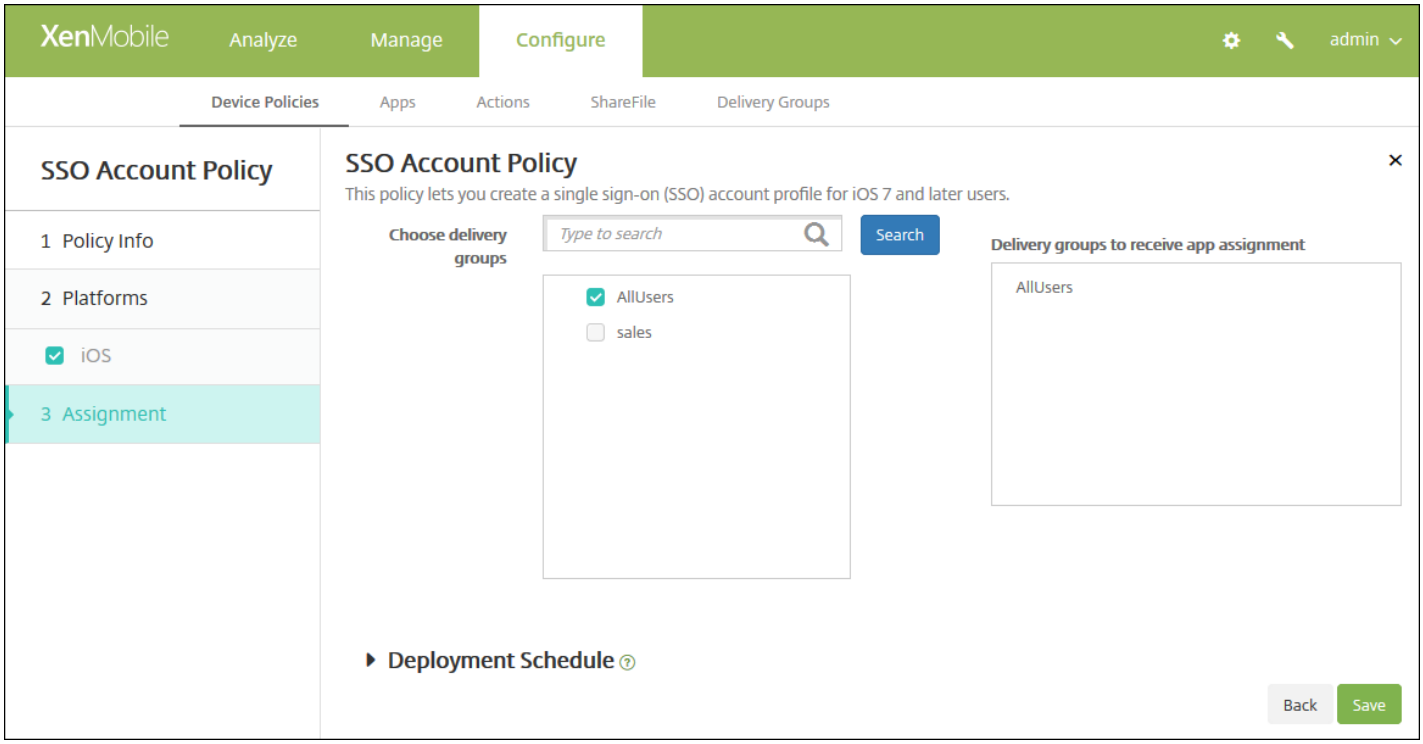
      Remarque : pour supprimer une URL ou un identifiant d'application, placez le curseur sur la ligne contenant la liste, puis cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur Supprimer pour supprimer la liste ou sur Annuler pour conserver la liste.

      Pour modifier une URL ou un identifiant d'application, placez le curseur sur la ligne contenant la liste, puis cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur Enregistrer pour enregistrer la nouvelle liste ou sur Annuler pour laisser la liste inchangée.

- **Paramètres de stratégie**
    - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
    - 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.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie de compte SSO** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

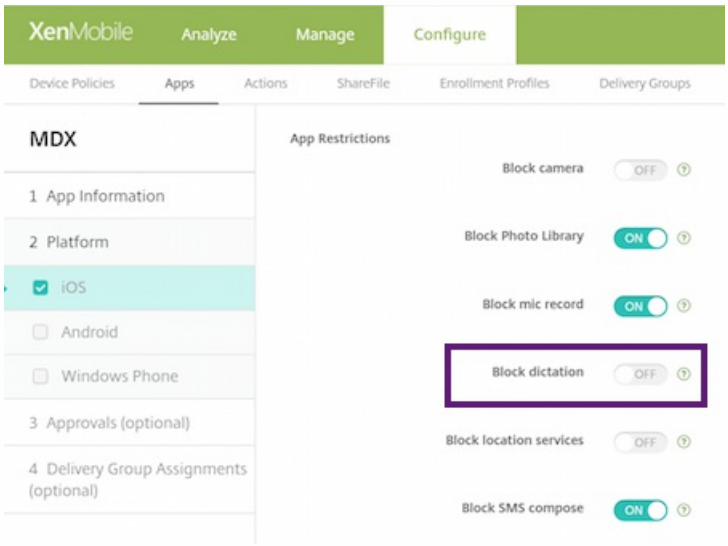
Stratégies de dictée et Siri

Jul 27, 2016

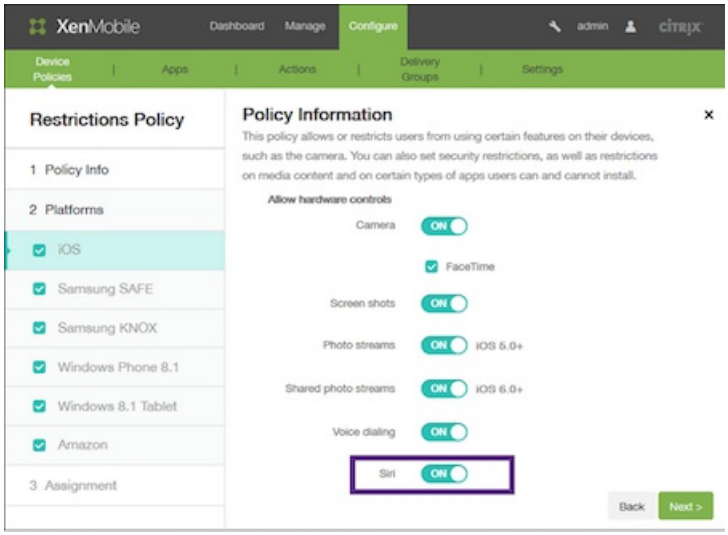
Lorsque les utilisateurs posent une question à Siri ou qu'ils dictent du texte sur des appareils iOS gérés, Apple collecte les données vocales à des fins d'amélioration de Siri. Les données vocales transitent via les services de cloud d'Apple et par conséquent elles existent en dehors du conteneur XenMobile 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 > Stratégie de restrictions > iOS**. 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**.

Stratégies de chiffrement du stockage

Jul 27, 2016

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 Samsung SAFE, Windows Phone et Android Sony. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans cet article.

Paramètres Samsung SAFE

Paramètres Windows Phone

Paramètres Android Sony

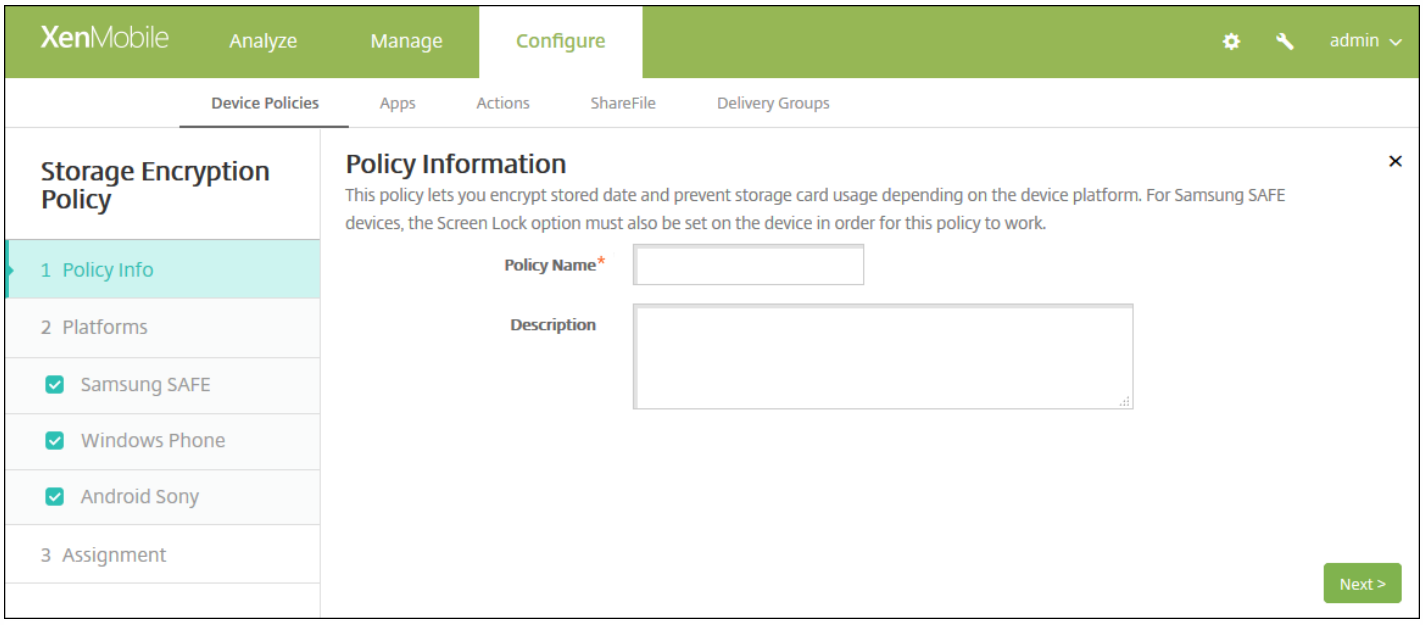
Remarque : pour les appareils Samsung SAFE, vérifiez que les conditions suivantes soient remplies avant de configurer cette stratégie :

- Vous devez définir l'option de verrouillage d'écran sur les appareils des utilisateurs.
- Les appareils doivent être branchés et chargés à 80 %.
- L'appareil doit exiger un mot de passe contenant des chiffres et des lettres ou des symboles.

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. Cliquez sur **Plus** puis, sous **Sécurité**, cliquez sur **Chiffrement du stockage**. La page d'informations sur la **Stratégie de chiffrement du stockage** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

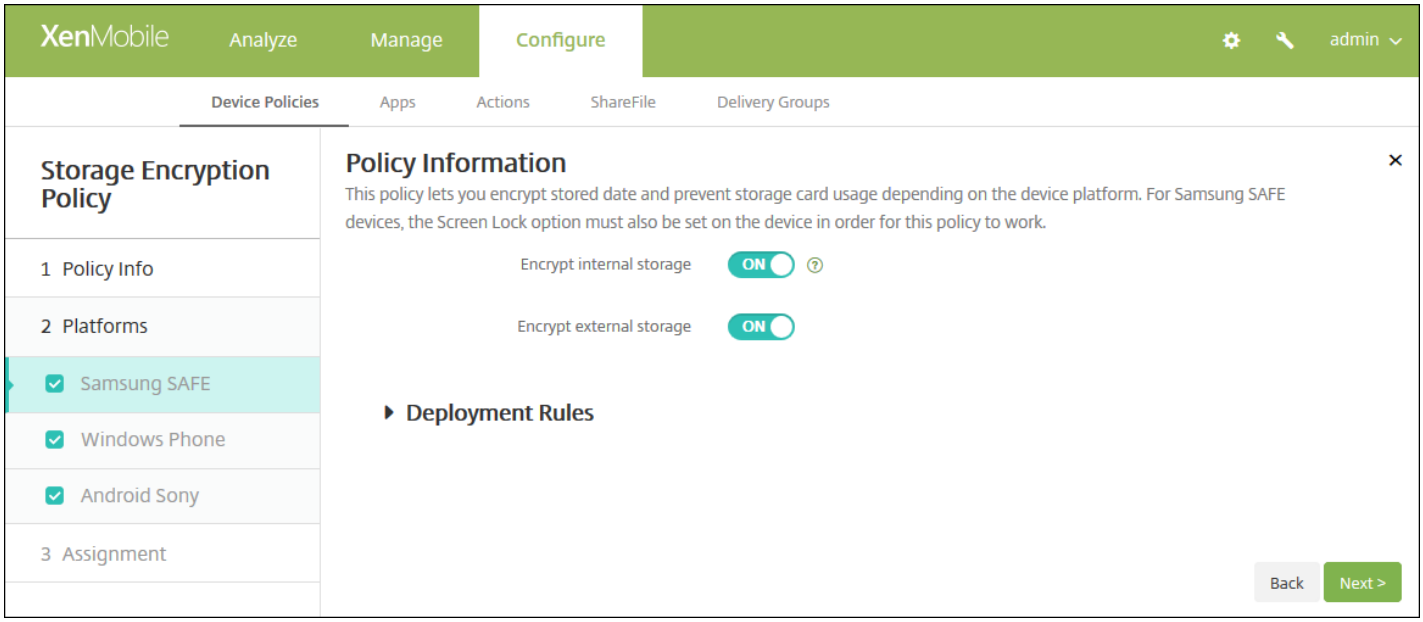
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.

- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.

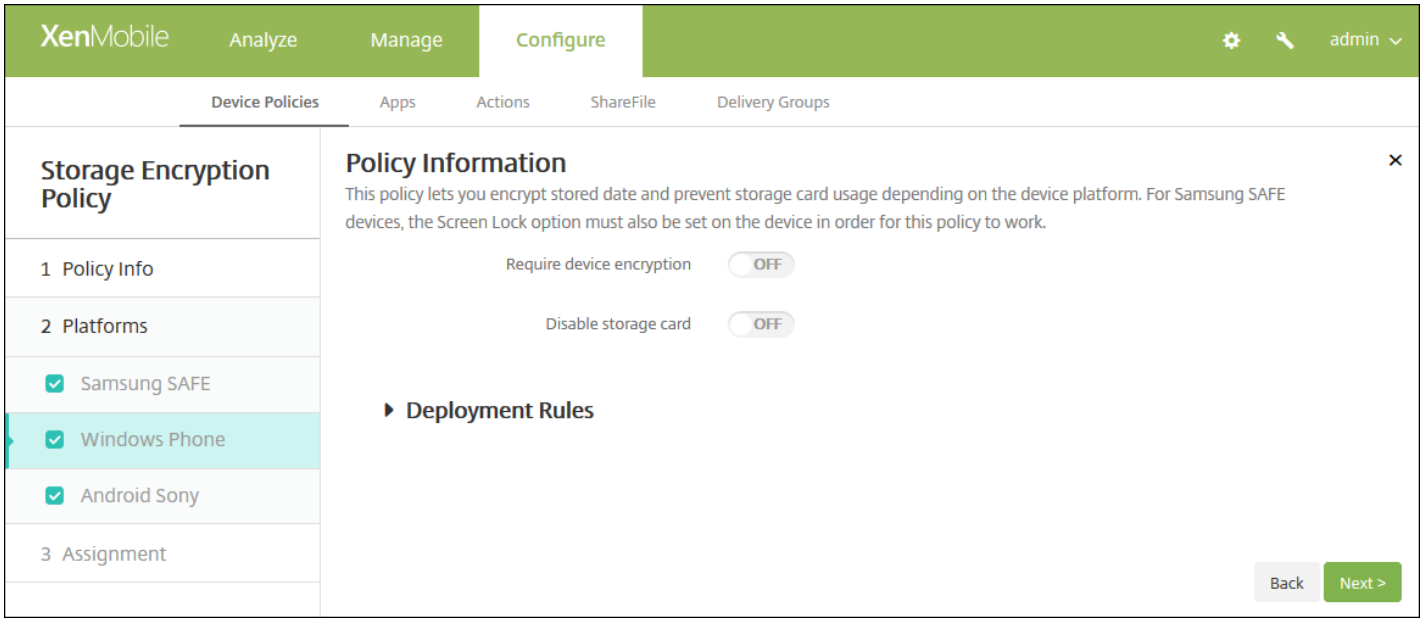
6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.



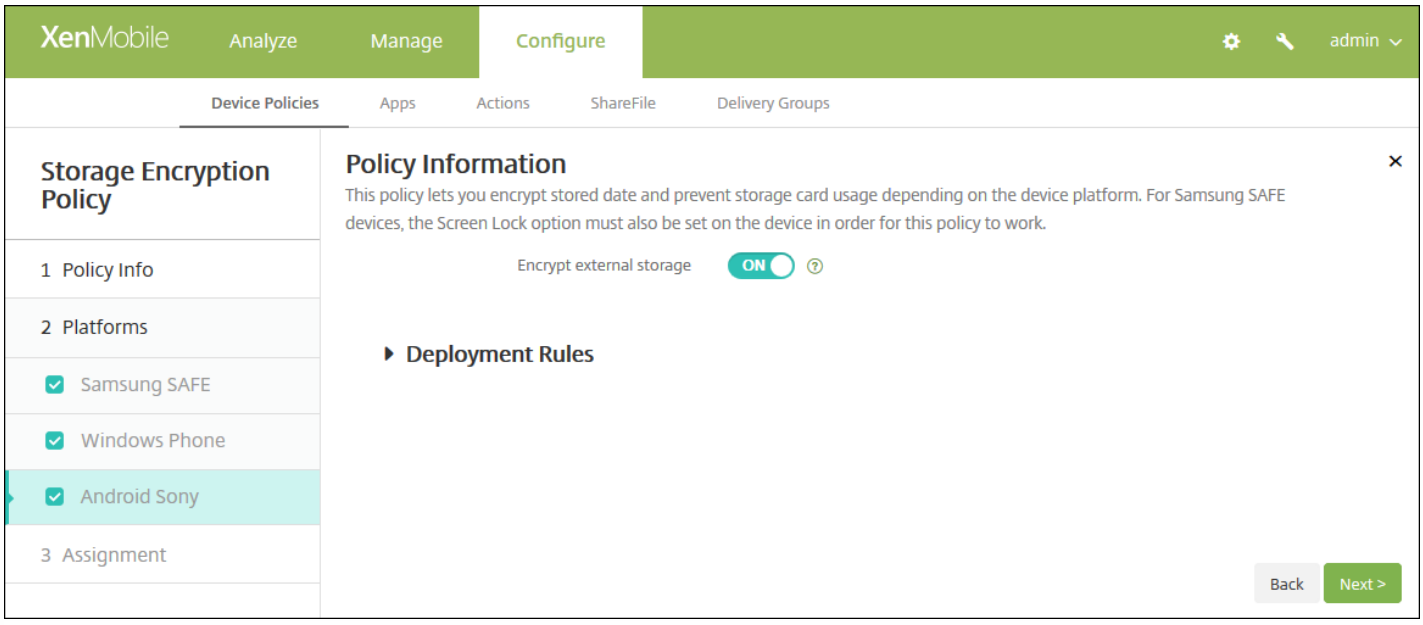
Pour configurer ces paramètres :

- **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 **ON**.
- **Chiffrer le stockage externe** : sélectionnez cette option pour chiffrer le stockage externe sur les appareils des utilisateurs. La valeur par défaut est **ON**.



Pour configurer ces paramètres :

- **Activer le chiffrement de l'appareil** : sélectionnez cette option pour chiffrer les appareils des utilisateurs. La valeur par défaut est **OFF**.
- **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 **OFF**.

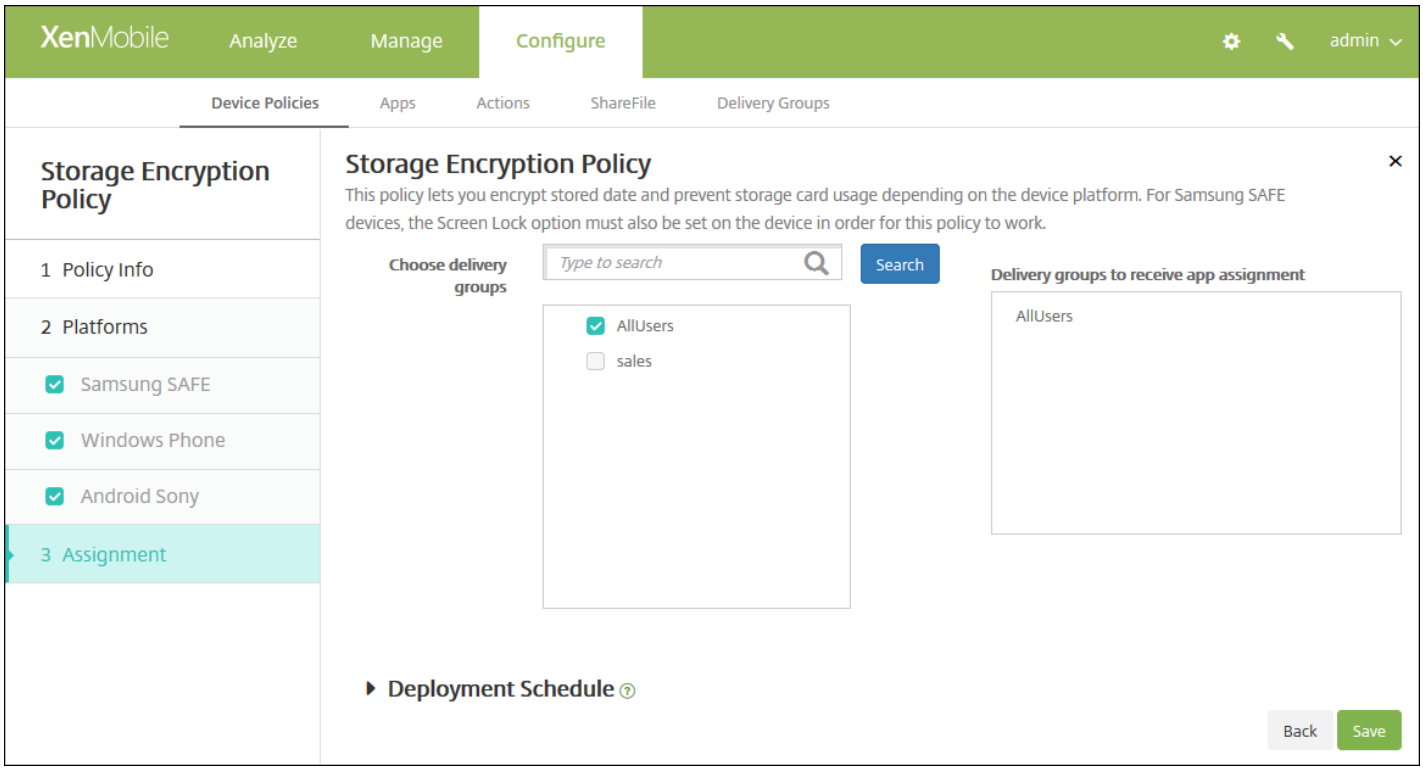


Configurez ce paramètre :

- **Chiffrer le stockage externe** : sélectionnez cette option pour chiffrer le stockage externe sur les appareils des utilisateurs. L'appareil doit exiger un mot de passe contenant des chiffres et des lettres ou des symboles. La valeur par défaut est **ON**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie de chiffrement du stockage** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégie d'abonnements calendriers

Jul 27, 2016

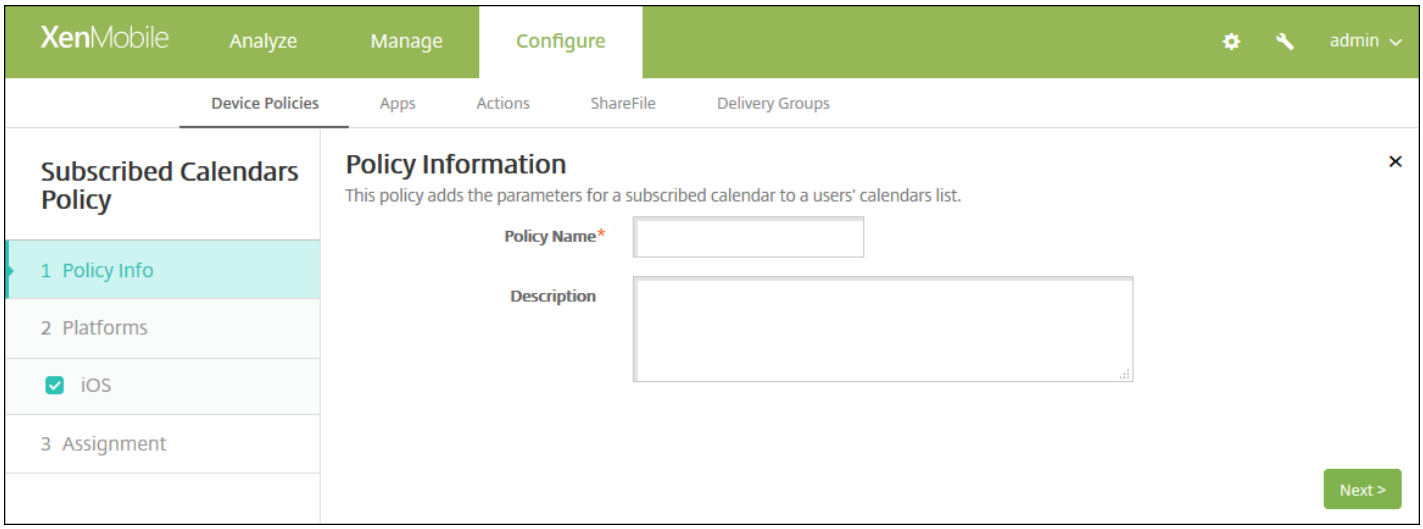
Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin d'ajouter un abonnement calendrier à la liste des calendriers sur les appareils iOS des utilisateurs. La liste des calendriers publics auxquels vous pouvez vous abonner est disponible sur www.apple.com/downloads/macosx/calendars.

Remarque : vous devez être abonné à un calendrier avant de pouvoir l'ajouter à la liste des abonnements calendriers sur les appareils des utilisateurs.

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.

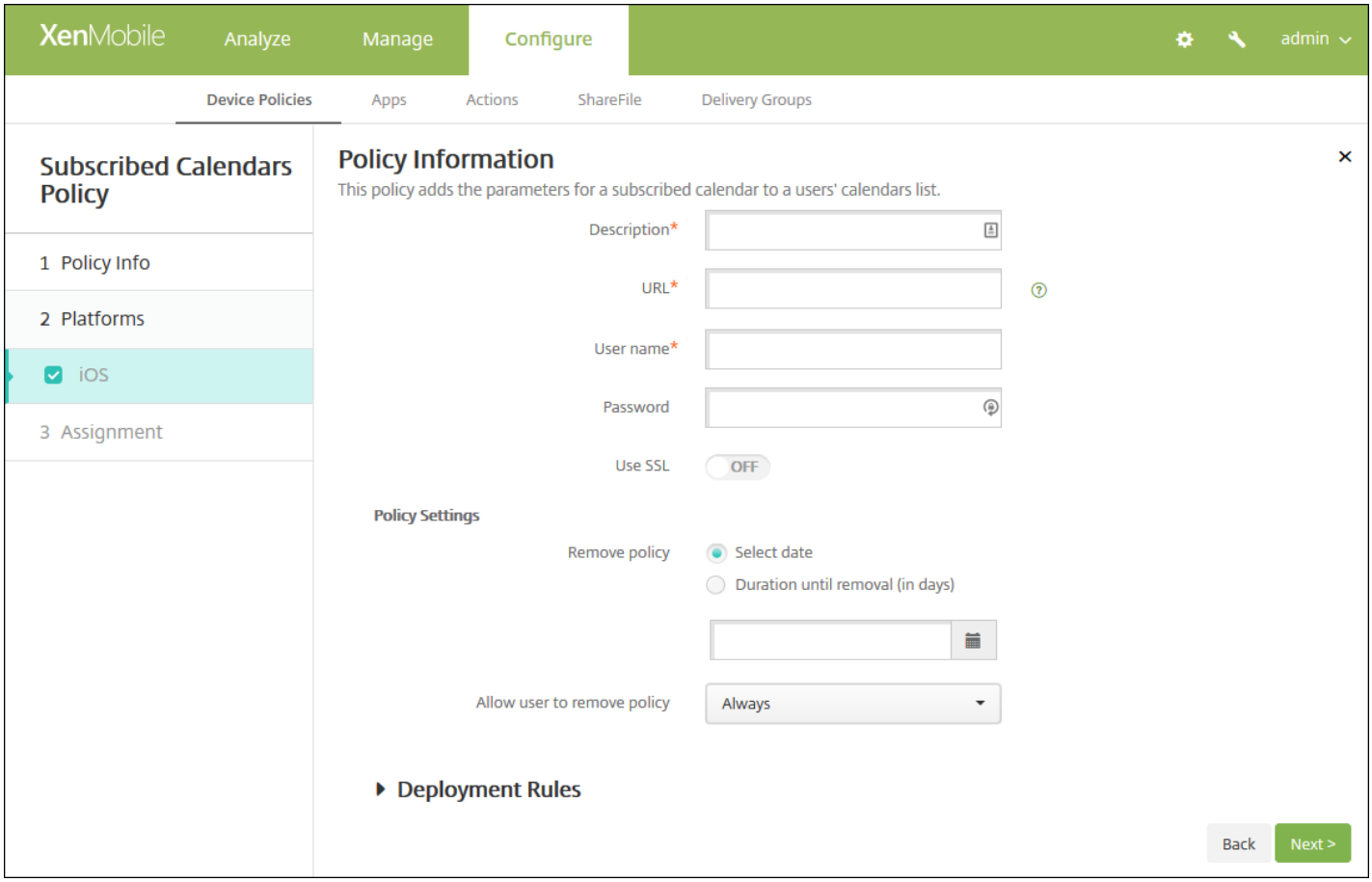
3. Cliquez sur **Plus**, puis, sous **Utilisateur final**, cliquez sur **Abonnements calendriers**. La page **Stratégie d'abonnements calendriers** s'affiche.



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 **Next**. La page **Informations sur la plate-forme iOS** s'affiche.

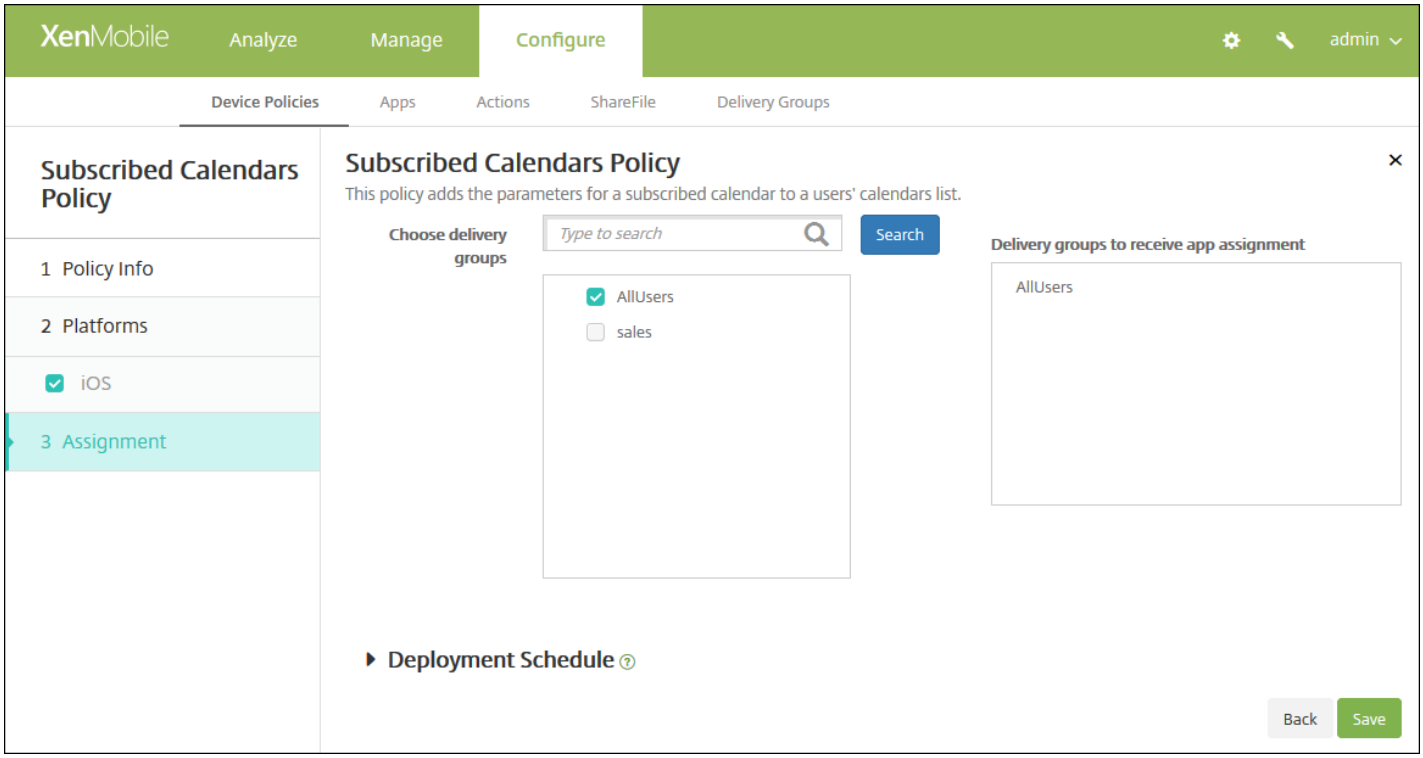


6. Configurez les paramètres suivants :

- **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 http:// 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 Off.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  - 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.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie d'abonnements calendriers** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégies termes et conditions.

Jul 27, 2016

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.

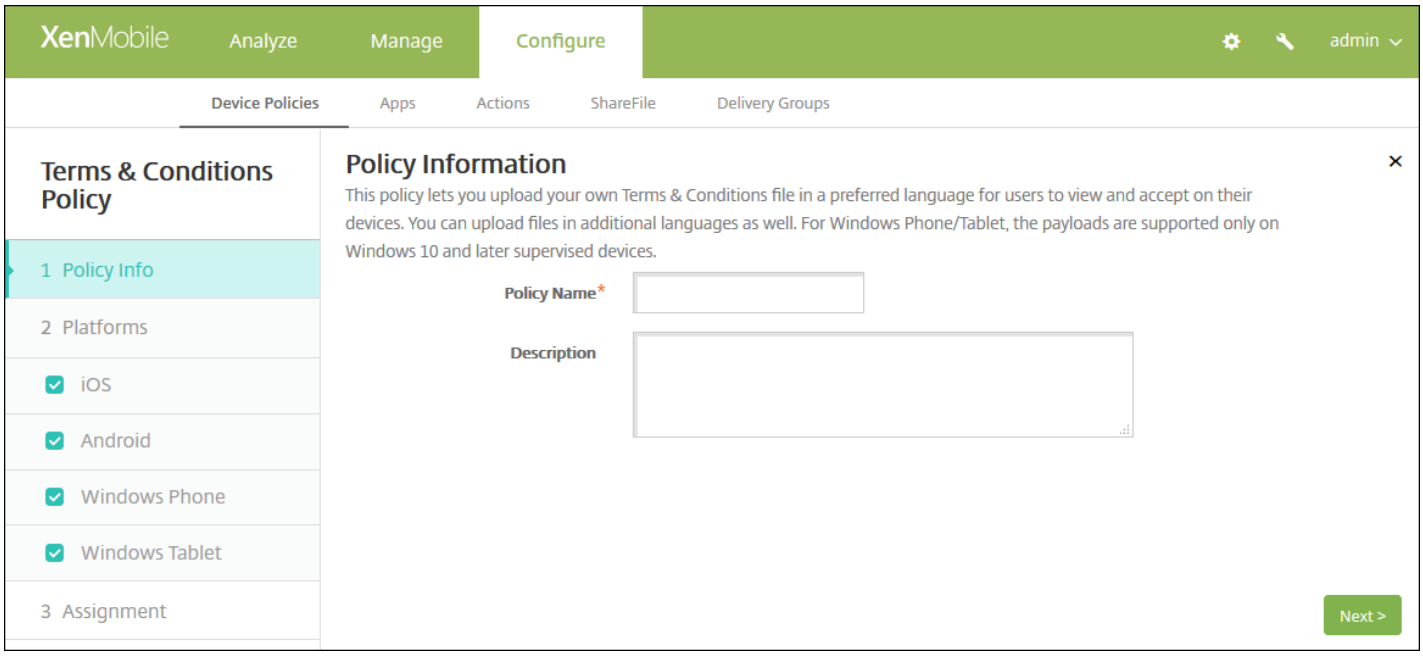
Paramètres iOS et Android.

Paramètres Windows Phone et Windows Tablet

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.

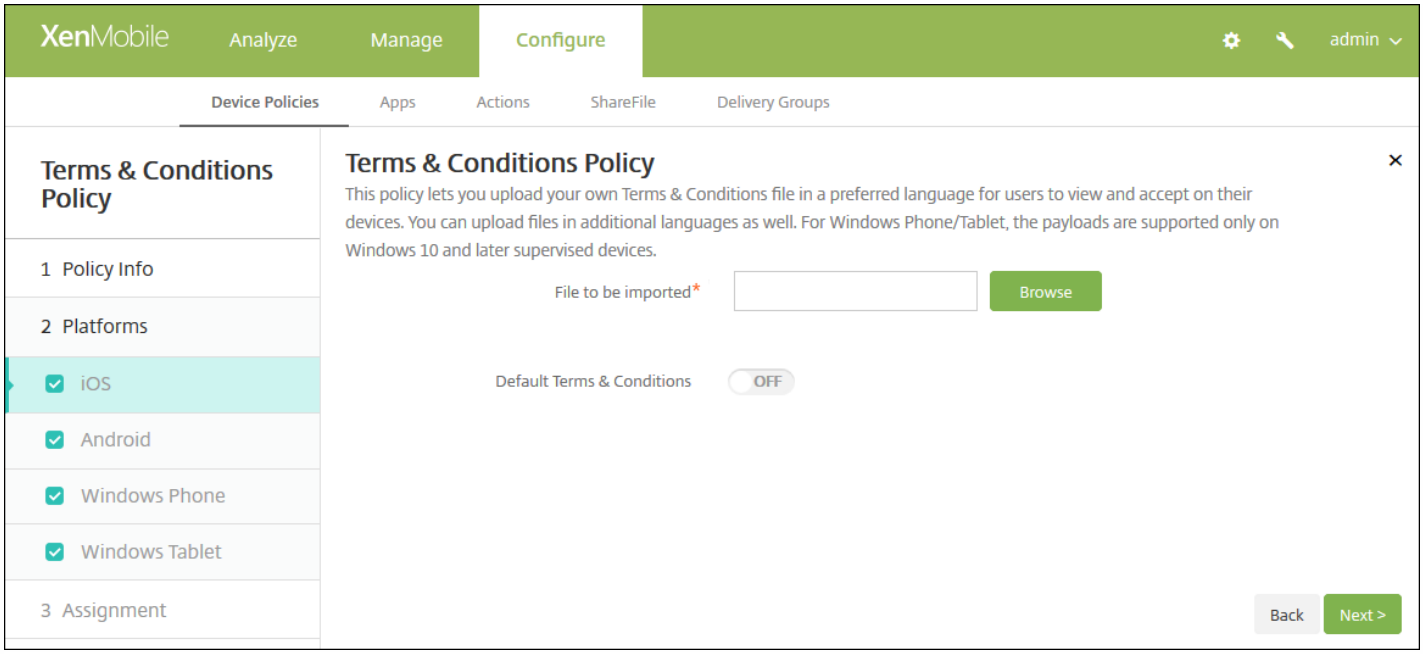
3. Cliquez sur **Termes et conditions**. La page **Stratégie termes et conditions** s'affiche.

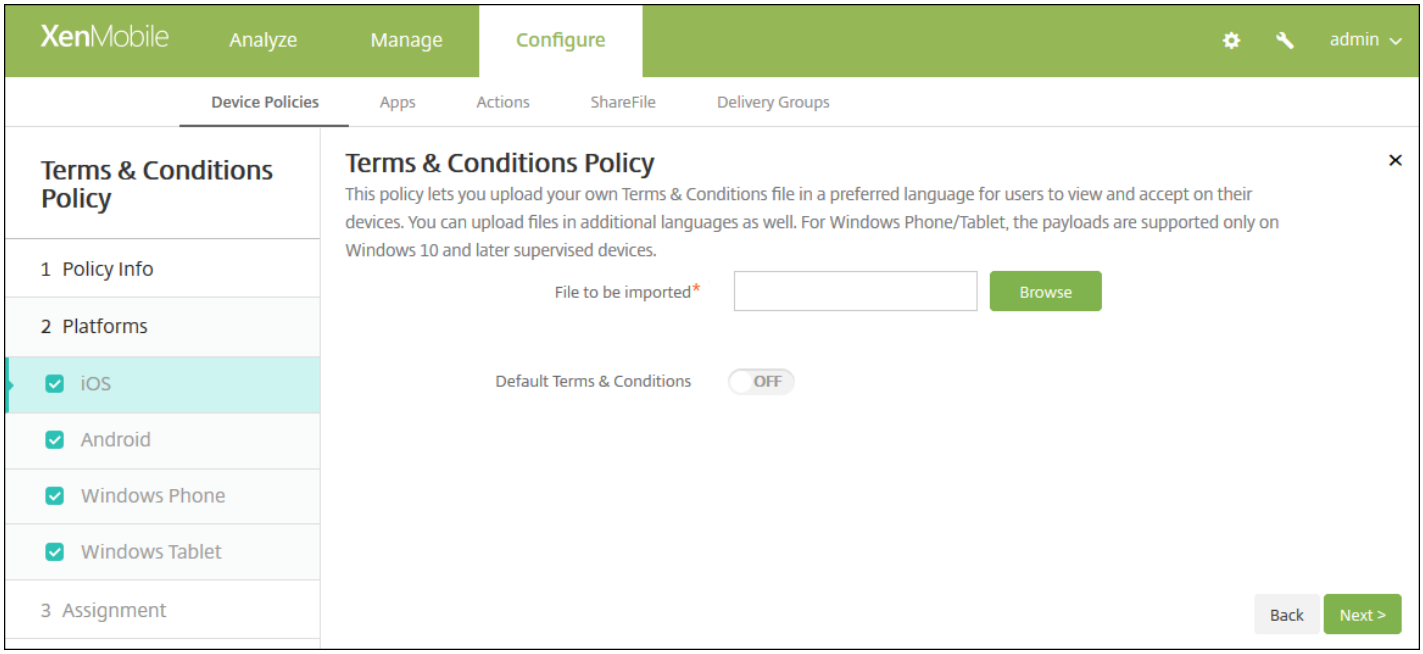


4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

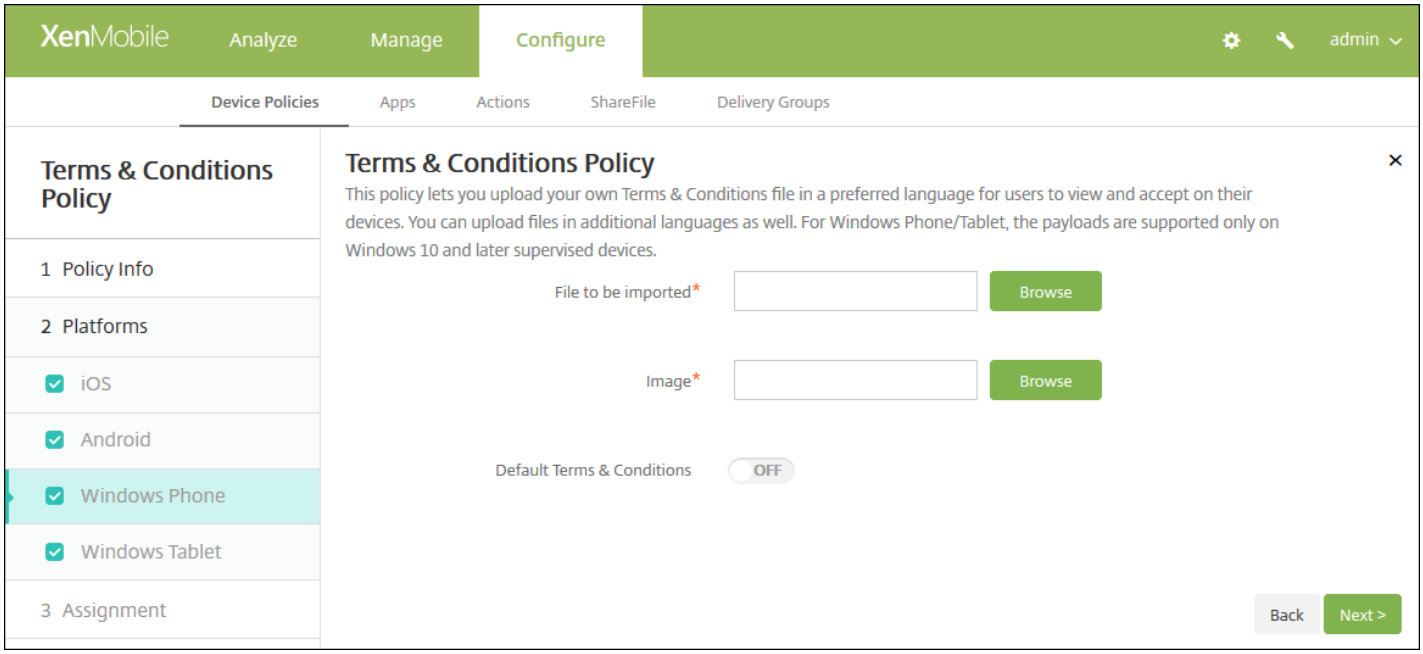
5. **Cliquez sur** Suivant. La page d'informations **Stratégie par plate-forme des termes et conditions** s'affiche.





Pour configurer ces paramètres :

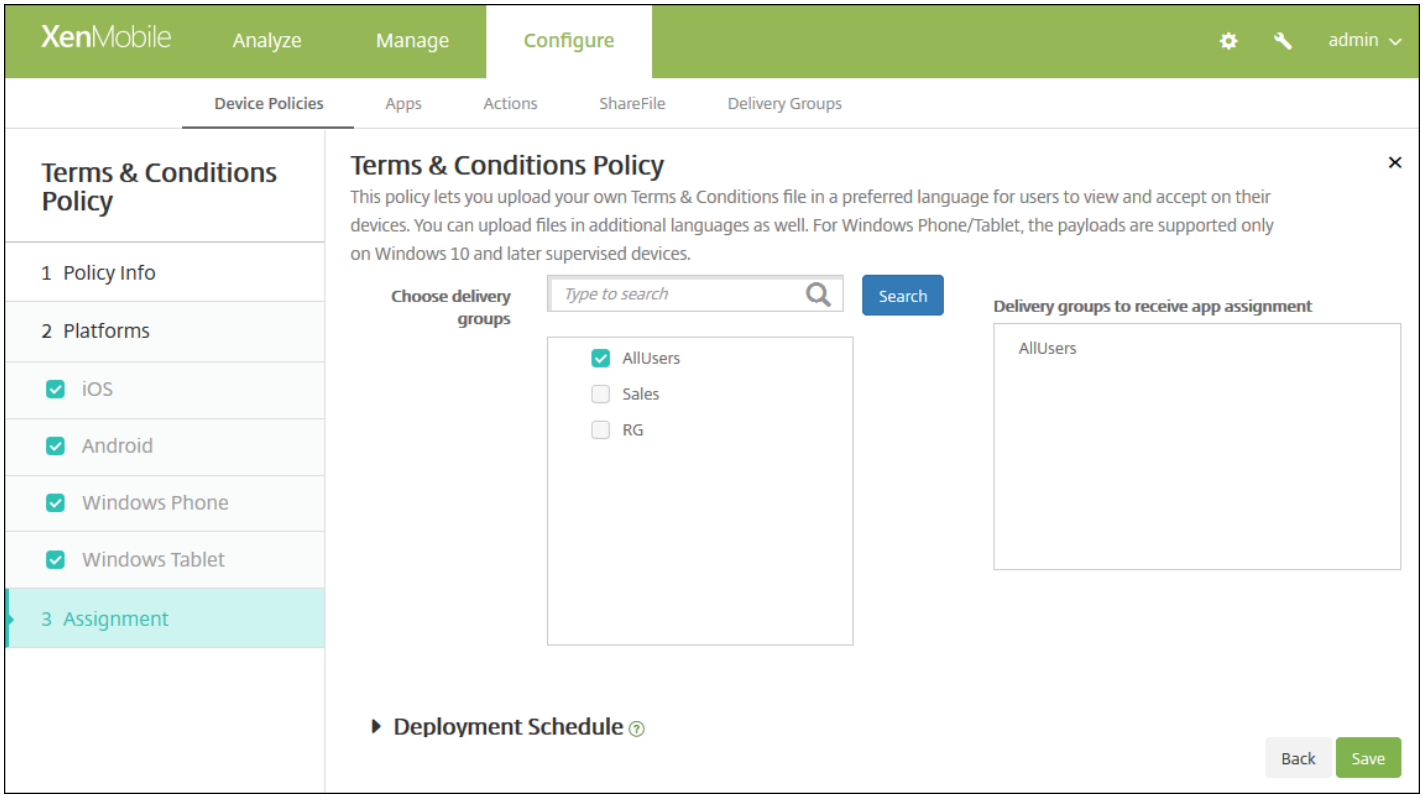
- **Fichier à importer** : sélectionnez le fichier de termes et conditions à importer en cliquant sur **Parcourir**, puis accédez à l'emplacement du fichier.
- **Termes et conditions par défaut** : sélectionnez cette option pour désigner ce fichier comme le document par défaut pour les utilisateurs qui sont membres de plusieurs groupes avec différents termes et conditions. La valeur par défaut est **OFF**.



Pour configurer ces paramètres :

- **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 **OFF**.

6. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie termes et conditions** s'affiche.



7. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

8. Cliquez sur **Enregistrer**.

Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator

Jul 27, 2016

Pour utiliser Apple Configurator, vous avez besoin d'un ordinateur Apple exécutant OS X 10.7.2 ou version ultérieure.

> **Important**
>
> le fait de placer un appareil en mode supervisé installera 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 le configurateur d'Apple. Le Configurateur indique que vous possédez un appareil à préparer pour la supervision.
4. Pour préparer l'appareil à des fins de supervision :
   1. 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.
   2. Si vous le souhaitez, entrez un nom pour l'appareil.
   3. 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.

Stratégies VPN

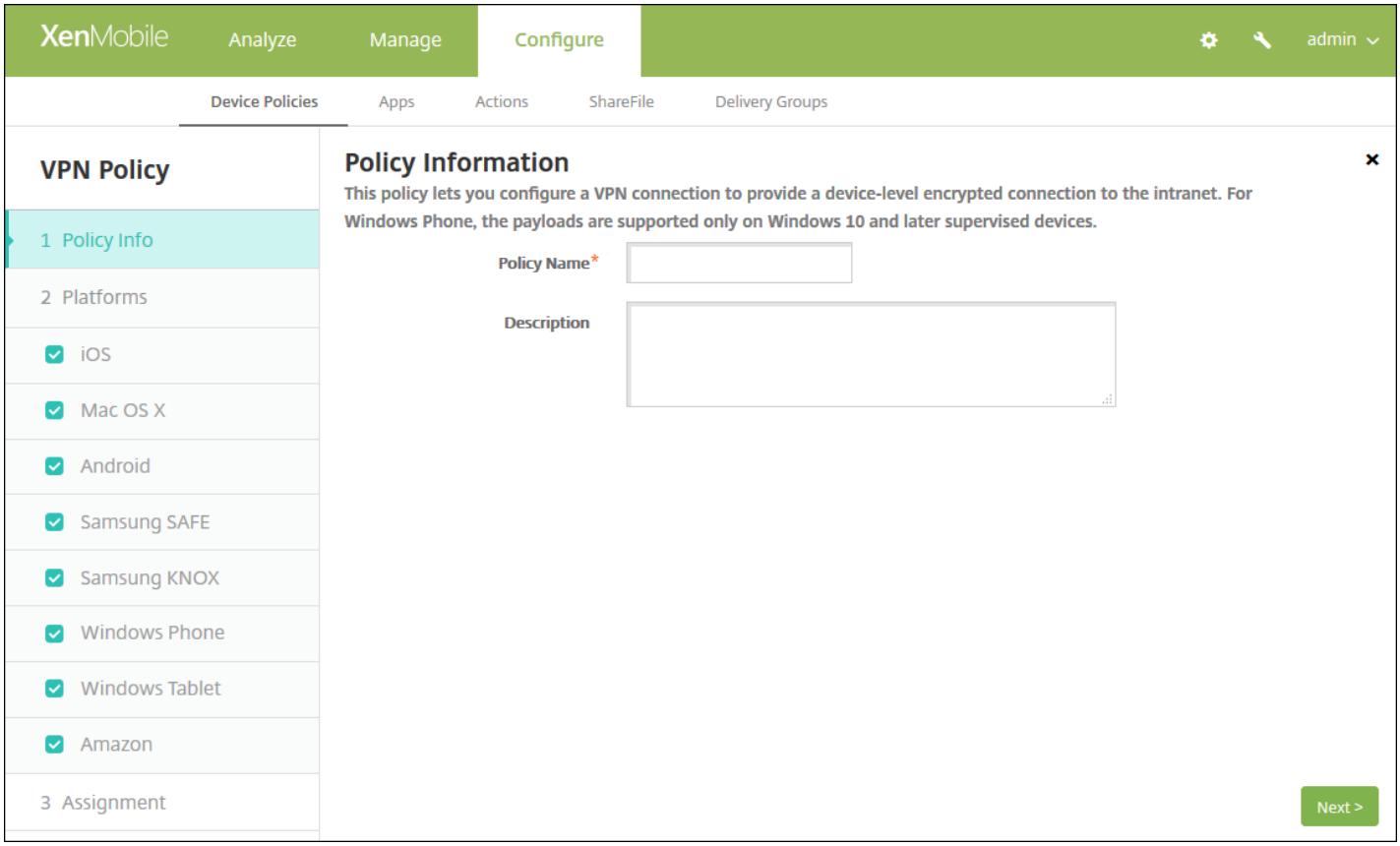
Oct 17, 2016

Vous pouvez ajouter une stratégie dans XenMobile pour configurer des 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 : iOS, Android (y compris les appareils activés pour Android for Work), Samsung SAFE, Samsung KNOX, Windows Tablet, Windows Phone et Amazon. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans cet article.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Add**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Cliquez sur **VPN**. La page **Stratégie VPN** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

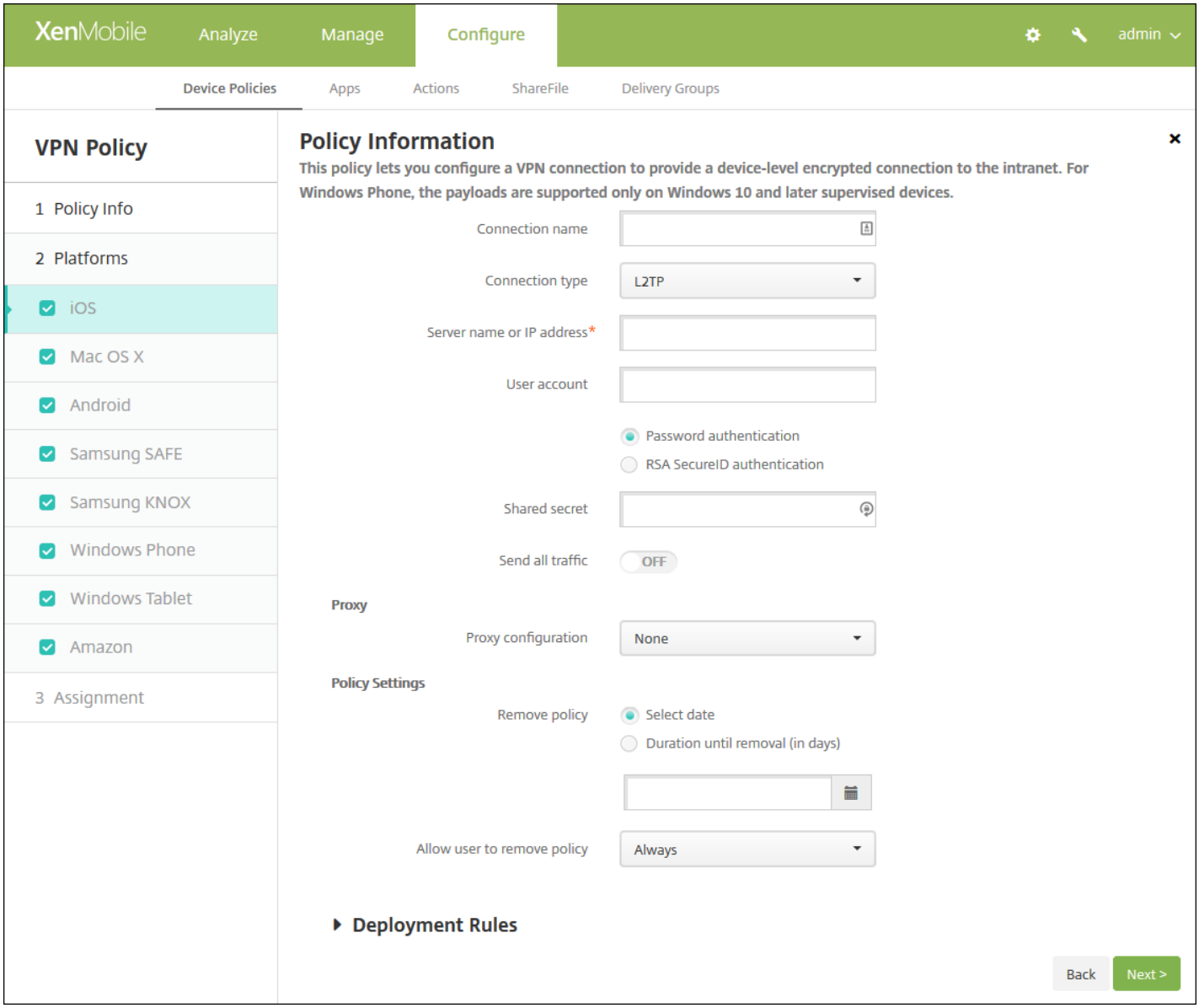
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche. lorsque la page **Stratégie par plate-forme** s'affiche, toutes les plates-formes sont sélectionnées et la plate-forme iOS s'affiche en premier.

6. Sous **Plates-formes**, sélectionnez la plate-forme ou les plates-formes que vous souhaitez ajouter. Désélectionnez les plates-formes que vous ne souhaitez pas configurer.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour iOS



Configurer ces paramètres

- **Nom de la connexion** : entrez un nom pour la connexion.
- **Type de connexion** : dans la liste, cliquez sur 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.
  - **IKEv2 (iOS uniquement)** : Internet Key Exchange version 2 pour iOS uniquement.
  - **Citrix VPN** : client Citrix VPN pour iOS.
  - **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

Configurer le protocole PPTP

Configurer le protocole IPSec

Configurer le protocole Cisco AnyConnect

Configurer le protocole SSL Juniper

Configurer le protocole F5 SSL

Configurer le protocole SonicWALL

Configurer le protocole Ariba VIA

Configurer le protocole IKEv2

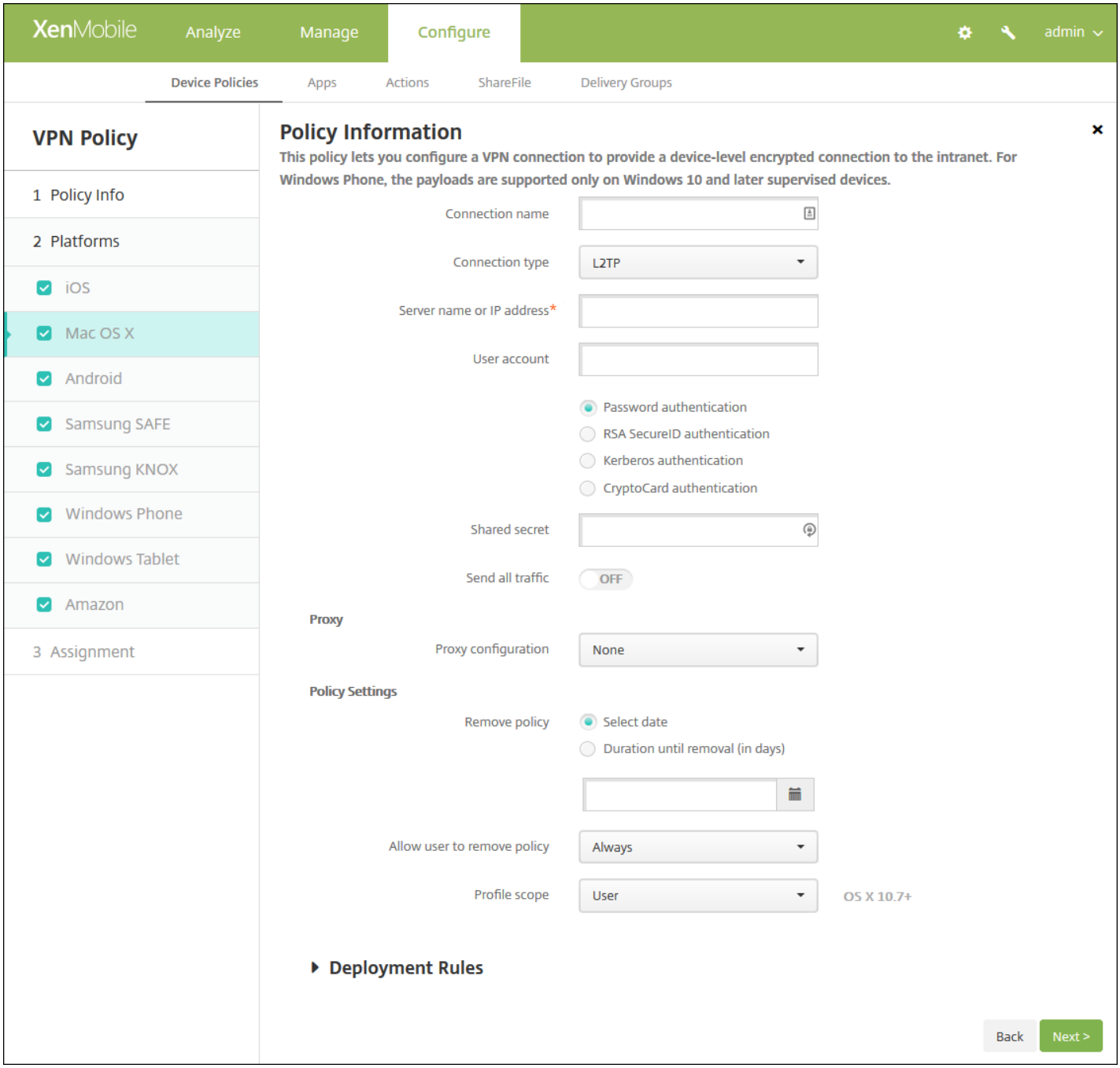
Configurer le protocole Citrix VPN

Configurer le protocole SSL personnalisé

Configurer les options de l'activation VPN sur demande

- **Proxy**
  - **Configuration du proxy** : dans la liste, cliquez sur la façon dont la connexion VPN transite via un serveur proxy. La valeur par défaut est **Aucune**.
    - 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**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  - 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.

Configurer les paramètres pour Mac OS X



Pour configurer ces paramètres :

- **Nom de la connexion** : entrez un nom pour la connexion.
- **Type de connexion** : dans la liste, cliquez sur 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

Configurer le protocole PPTP

Configurer le protocole IPSec

Configurer le protocole Cisco AnyConnect

Configurer le protocole SSL Juniper

Configurer le protocole F5 SSL

Configurer le protocole SonicWALL

Configurer le protocole Ariba VIA

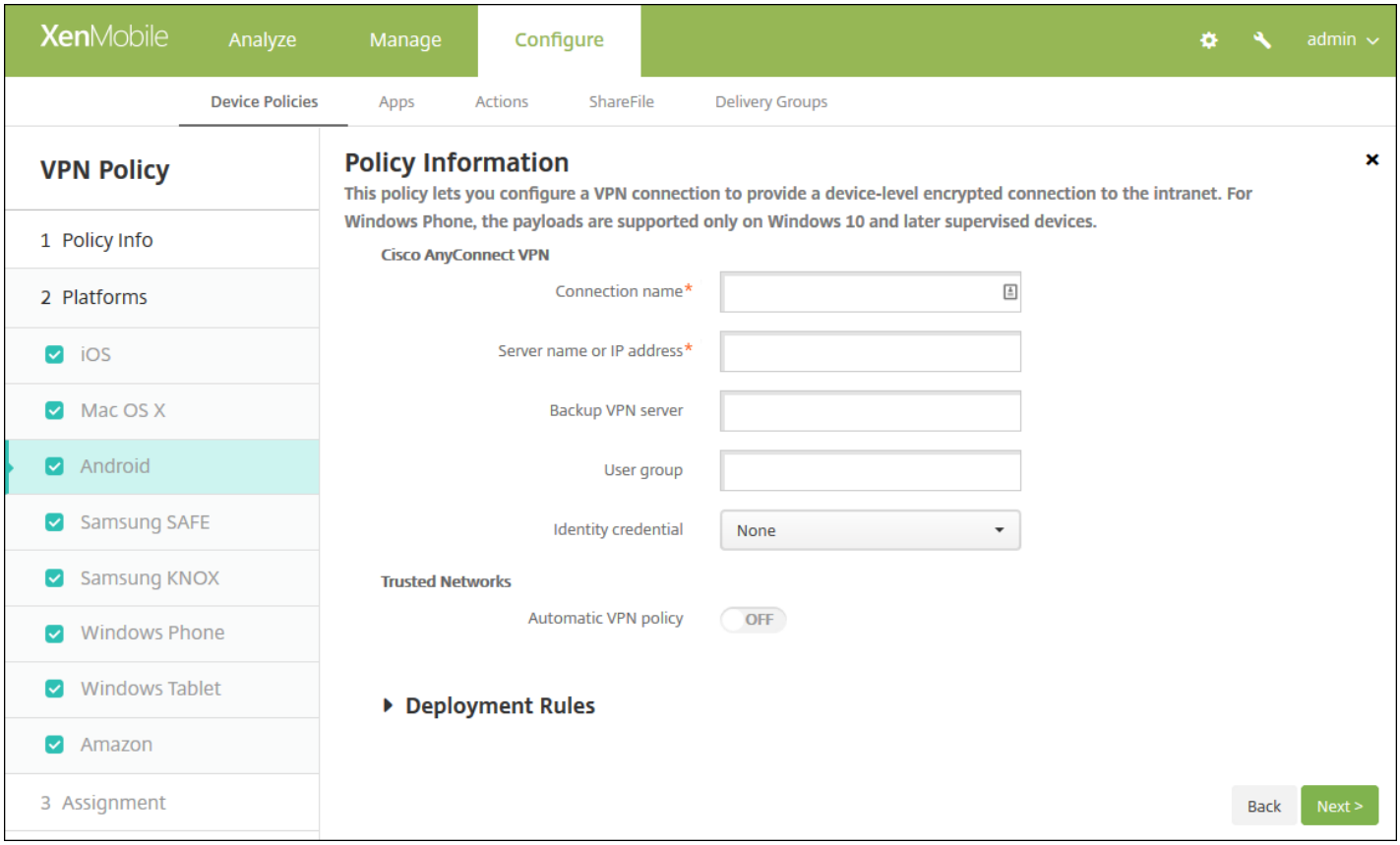
Configurer le protocole Citrix VPN

Configurer le protocole SSL personnalisé

Configurer les options de l'activation VPN sur demande

- **Proxy**
  - **Configuration du proxy** : dans la liste, cliquez sur la façon dont la connexion VPN transite via un serveur proxy. La valeur par défaut est **Aucune**.
    - 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**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  - 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.
  - En regard de **Étendue du profil**, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur OS X 10.7 et versions ultérieures.

Configurer les paramètres pour Android



Pour configurer ces paramètres :

- **VPN Cisco AnyConnect**
  - **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.
  - **Serveur VPN de sauvegarde** : entrez les informations du serveur VPN de sauvegarde.
  - **Groupe d'utilisateurs** : entrez les informations relatives au groupe d'utilisateurs.
  - **Infos d'identification de l'identité** : dans la liste, sélectionnez des Informations d'identification de l'identité.
- **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, cliquez sur 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 de l'option 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 (plutôt que de la déconnecter) 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. Cela élimine le besoin de créer une nouvelle session VPN après avoir quitté un réseau approuvé.
    - **Stratégie pour réseau non fiable** : dans la liste, cliquez sur la stratégie souhaitée. La valeur par défaut est **Connecter**. Les options possibles sont les suivantes :

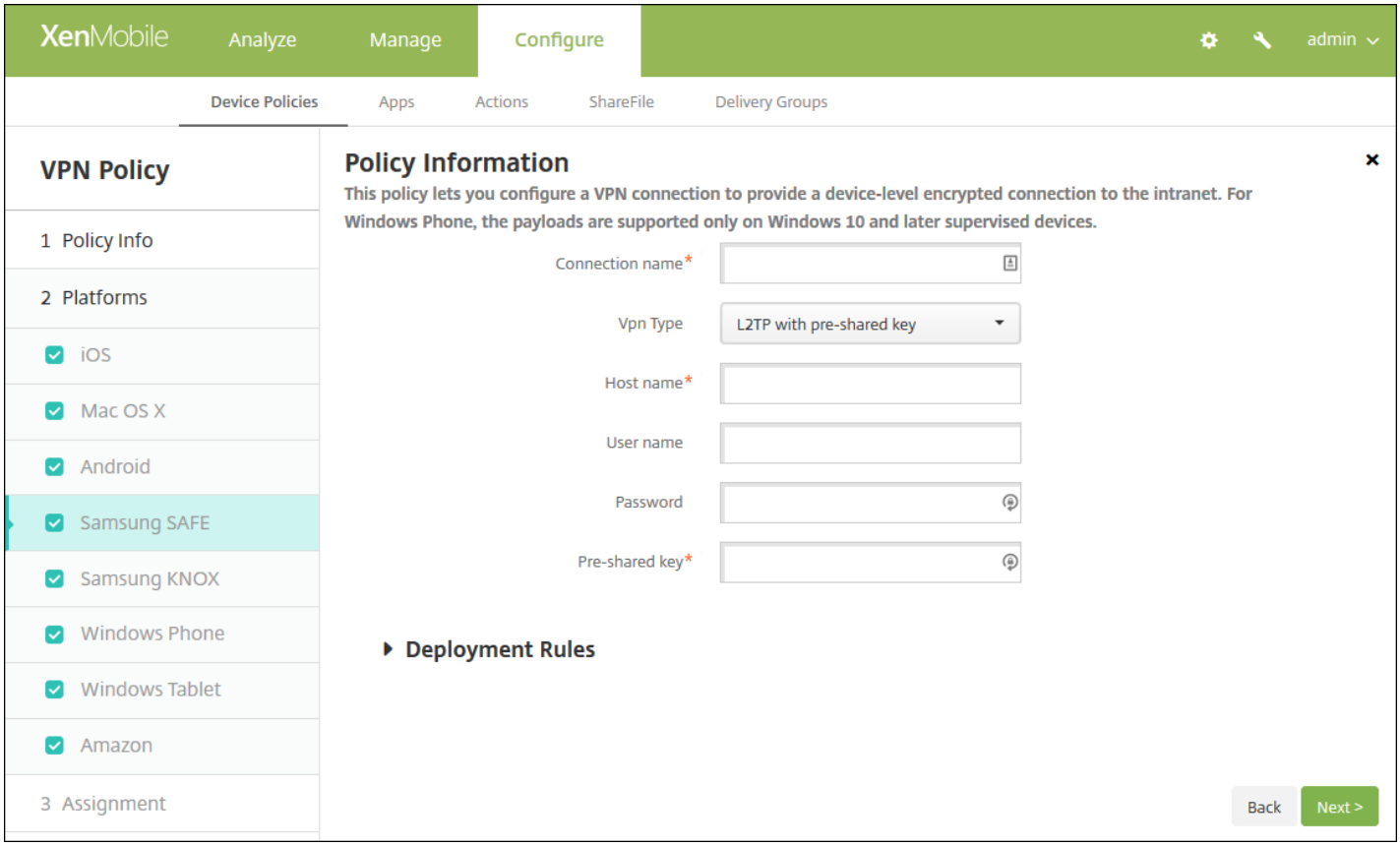
- **Connecter** : le client initie une connexion VPN dans le réseau non approuvé.
- **Ne rien faire** : le client démarre une connexion VPN dans le réseau non approuvé. Cette option désactive le VPN permanent.

- **Domaines approuvés** : pour chaque suffixe de domaine que l'interface réseau peut avoir 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 peut avoir 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.

    Remarque : pour supprimer un serveur, 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 serveur, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

Configurer les paramètres pour Samsung SAFE



Pour configurer ces paramètres :

- **Nom de la connexion** : entrez un nom pour la connexion.

- **Type de VPN** : dans la liste, cliquez sur 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. C'est le réglage par défaut.
  - **L2TP avec certificat** : Layer 2 Tunneling Protocol avec certificat.
  - **PPTP** : protocole PPTP.
  - **Entreprise** : votre connexion VPN d'entreprise. S'applique aux versions SAFE antérieures à 2.0.
  - **Générique** : connexion VPN générique. S'applique aux versions SAFE 2.0 ou supérieures.

Les sections suivantes répertorient les options de configuration pour chacun des types de VPN précédents.

Configurer le protocole L2TP avec clé prépartagée

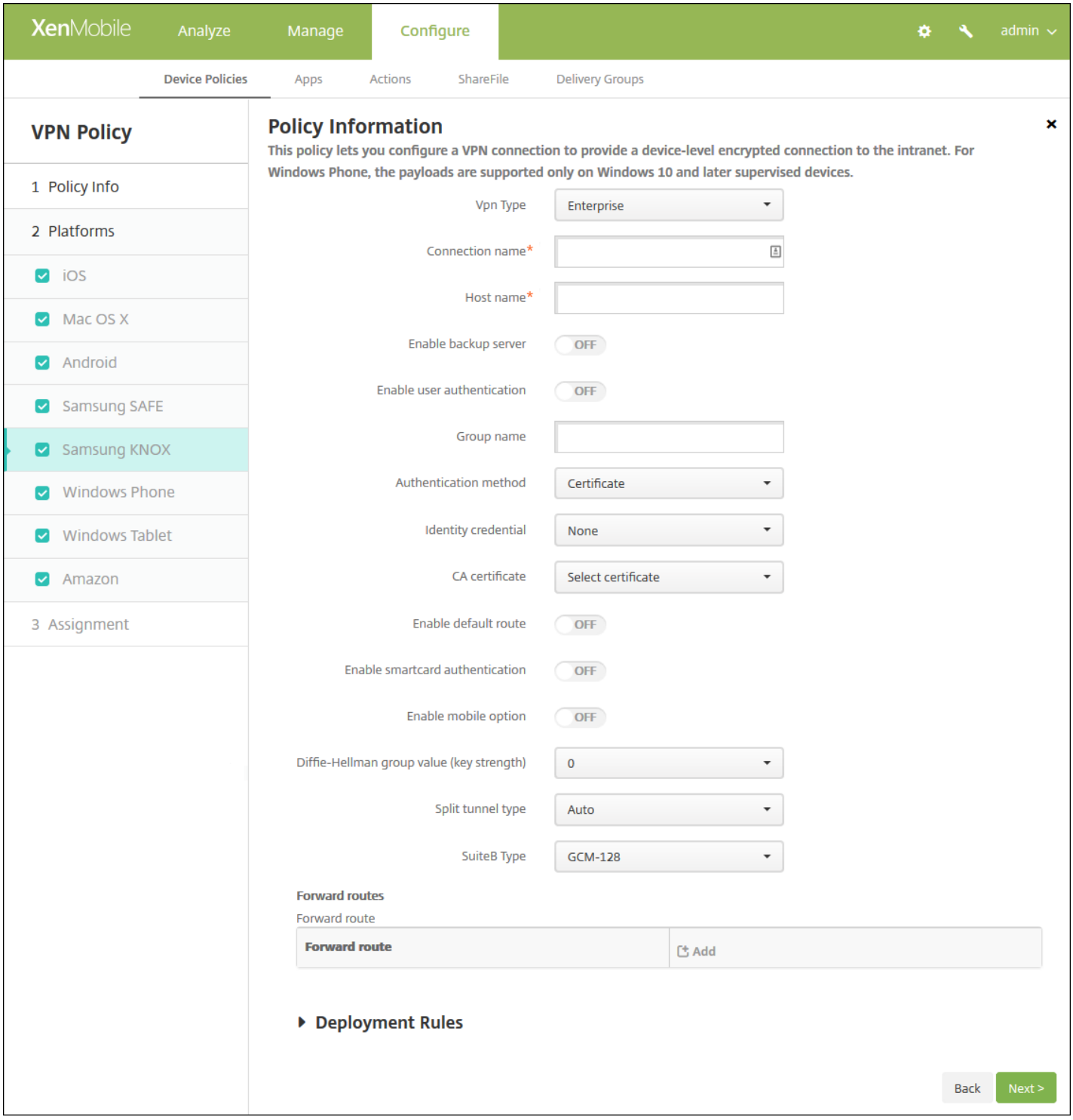
Configurer le protocole L2TP avec certificat

Configurer le protocole PPTP

Configurer le protocole Enterprise

Configurer le protocole générique

Configurer les paramètres pour Samsung KNOX



Remarque : lorsque vous configurez une stratégie pour Samsung KNOX, elle s'applique uniquement à l'intérieur du conteneur Samsung KNOX.

Pour configurer ces paramètres :

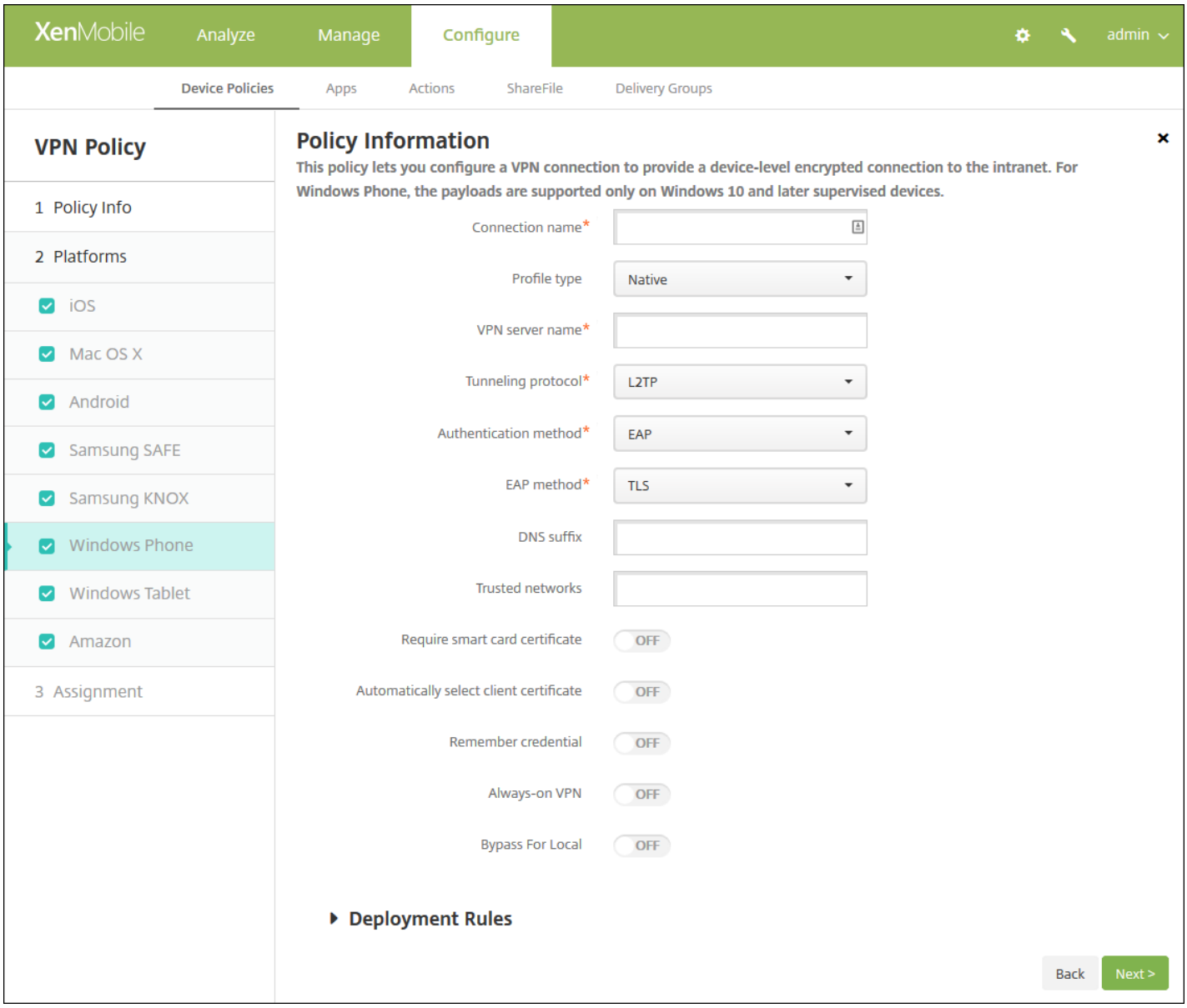
- **Type de VPN** : dans la liste, cliquez sur **Entreprise** (s'applique aux versions KNOX antérieures à 2.0) ou **Générique** (s'applique aux versions KNOX 2.0 ou supérieures) pour le type de connexion VPN à configurer. La valeur par défaut est **Entreprise**.

Les sections suivantes répertorient les options de configuration pour chacun des types de connexion précédents.

Configurer le protocole Enterprise

Configurer le protocole générique

Configurer les paramètres pour Windows Phone



Remarque : ces paramètres sont uniquement pris en charge sur les téléphones supervisés Windows 10 et versions ultérieures.

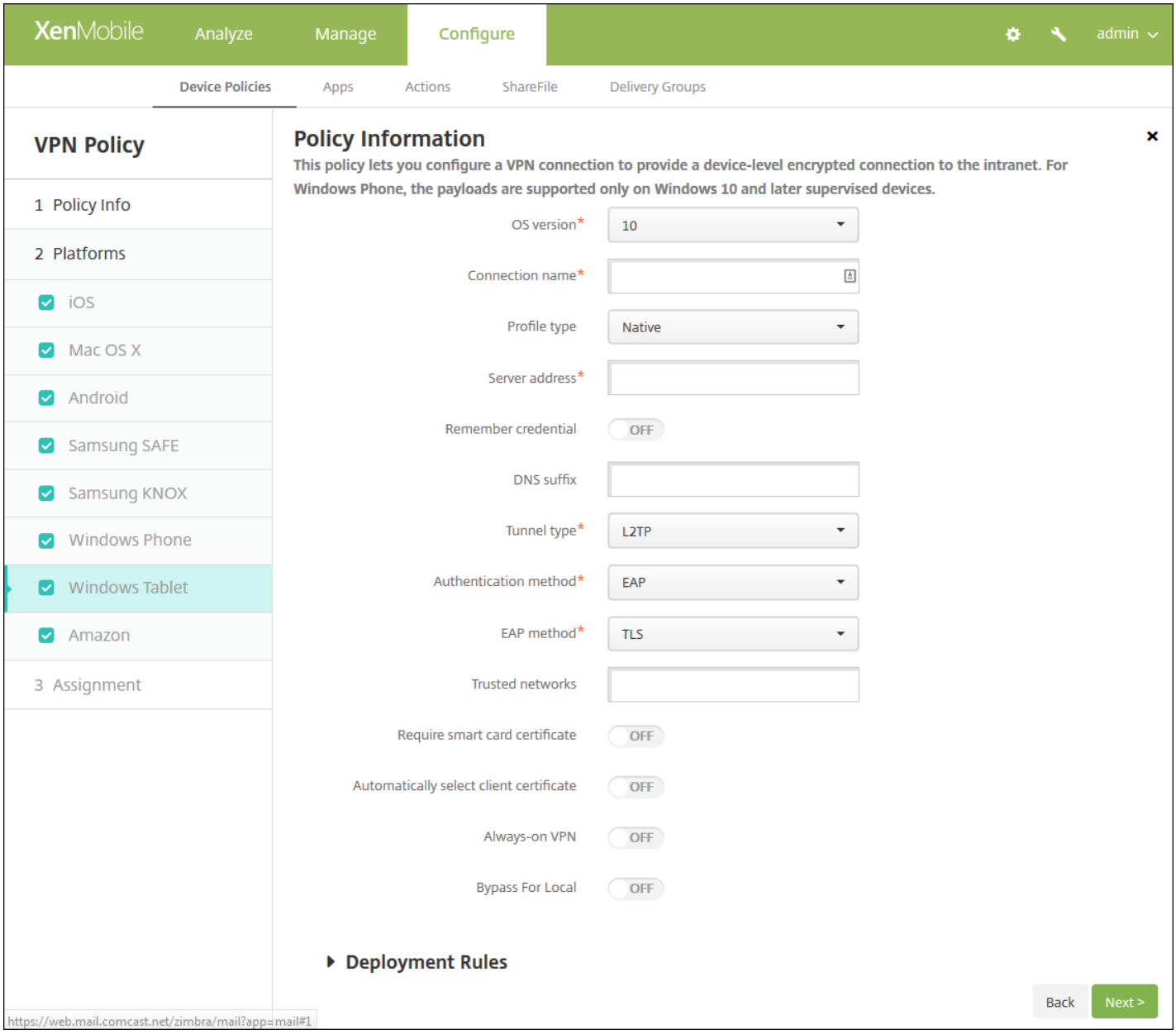
Pour configurer ces paramètres :

- **Nom de la connexion** : entrez un nom pour la connexion Ce champ est obligatoire.
- **Type de profil** : dans la liste, cliquez sur **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, cliquez sur 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, cliquez sur la méthode d'authentification à utiliser. La valeur par défaut est **EAP**. Les options possibles sont les suivantes :
    - **EAP** : protocole d'authentification étendue.
    - **MSChapV2** : utiliser 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 **OFF**.
  - **Méthode EAP** : dans la liste, cliquez sur 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 OFF.
  - **Sélectionner automatiquement le certificat client** : sélectionnez cette option pour choisir automatiquement le certificat client à utiliser pour l'authentification. La valeur par défaut est OFF. 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 OFF. 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 OFF. 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 de 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'adresse URL, le nom d'hôteou 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 OFF. 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 OFF. 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 pour Windows Tablet



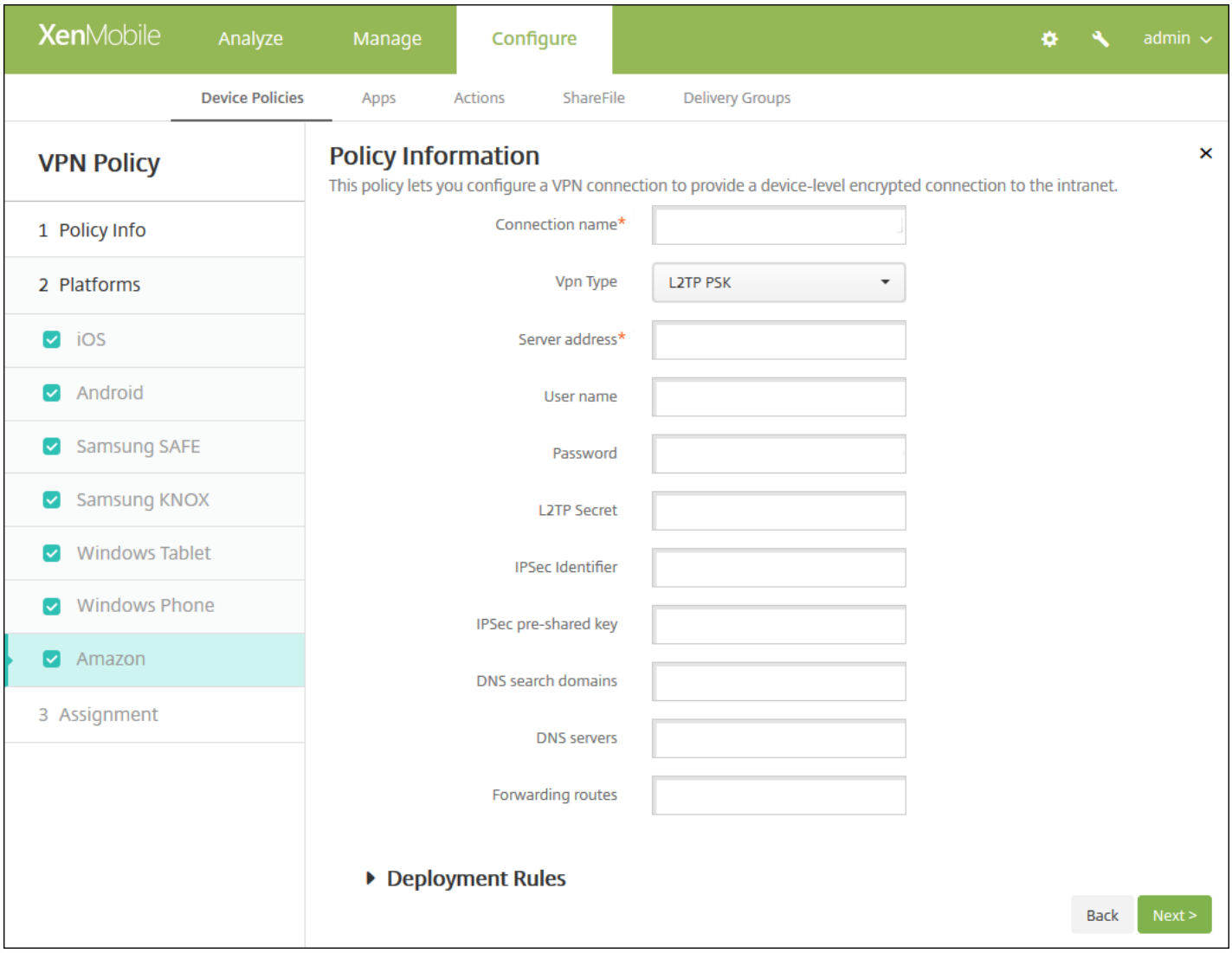
Pour configurer ces paramètres :

- **Version de l'OS** : dans la liste, cliquez sur **8.1** pour Windows 8.1 ou **10** pour Windows 10. La valeur par défaut est **10**

Configurer les paramètres pour Windows 10

Configurer les paramètres pour Windows 8,1

Configurer les paramètres pour Amazon



Pour configurer ces paramètres :

- **Nom de la connexion** : entrez un nom pour la connexion
- **Type de VPN** : cliquez sur 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 de l'option 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

Configurer les paramètres L2TP RSA

Configurer les paramètres IPSEC XAUTH PSK

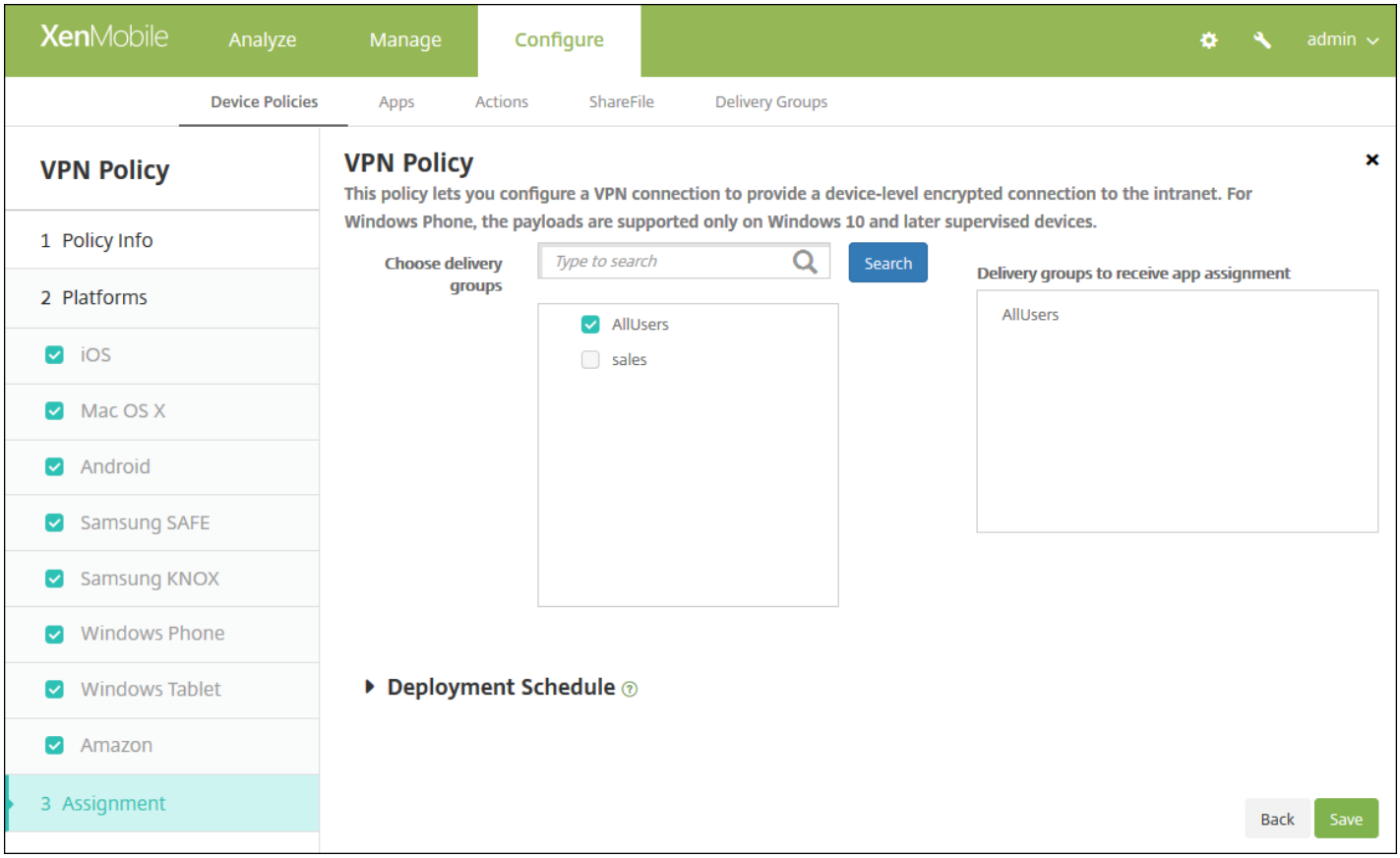
Configurer les paramètres IPSEC AUTH RSA

Configurer les paramètres IPSEC HYBRID RSA

Configurer les paramètres PPTP

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**, la page d'attribution **Stratégie VPN** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.

- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**. 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.

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.

11. Cliquez sur **Enregistrer**.

Stratégie de fond d'écran

Jul 27, 2016

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 version ultérieure. 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.

Appareil		**Dimensions d'image en pixels**
iPhone	**iPad**	
4, 4s		640 x 960
5, 5c et 5s		640 x 1136
6, 6s		750 x 1334
6 Plus		1080 x 1920
	Air, 2	1536 x 2048
	4, 3	1536 x 2048
	Mini 2, 3	1536 x 2048
	Mini	768 x 1024

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

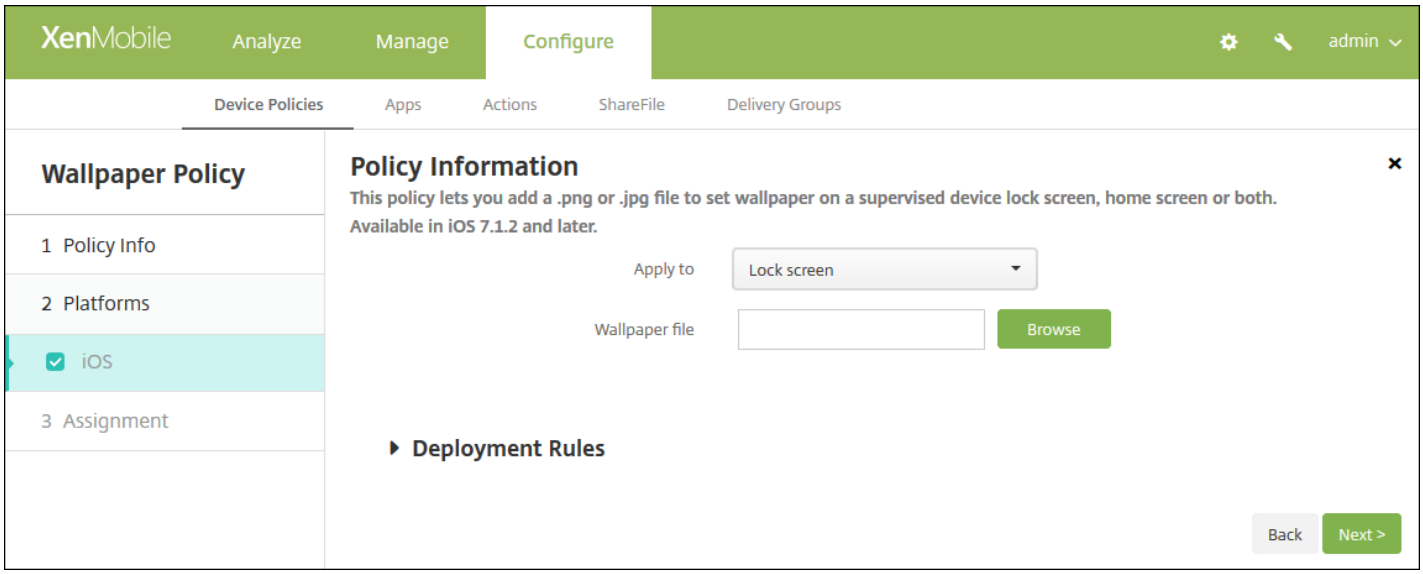
2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus**, puis, sous **Utilisateur final**, cliquez sur **Fond d'écran**. La page **Stratégie de fond d'écran** 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 **Next**. La page **Stratégie par plate-forme** s'affiche.

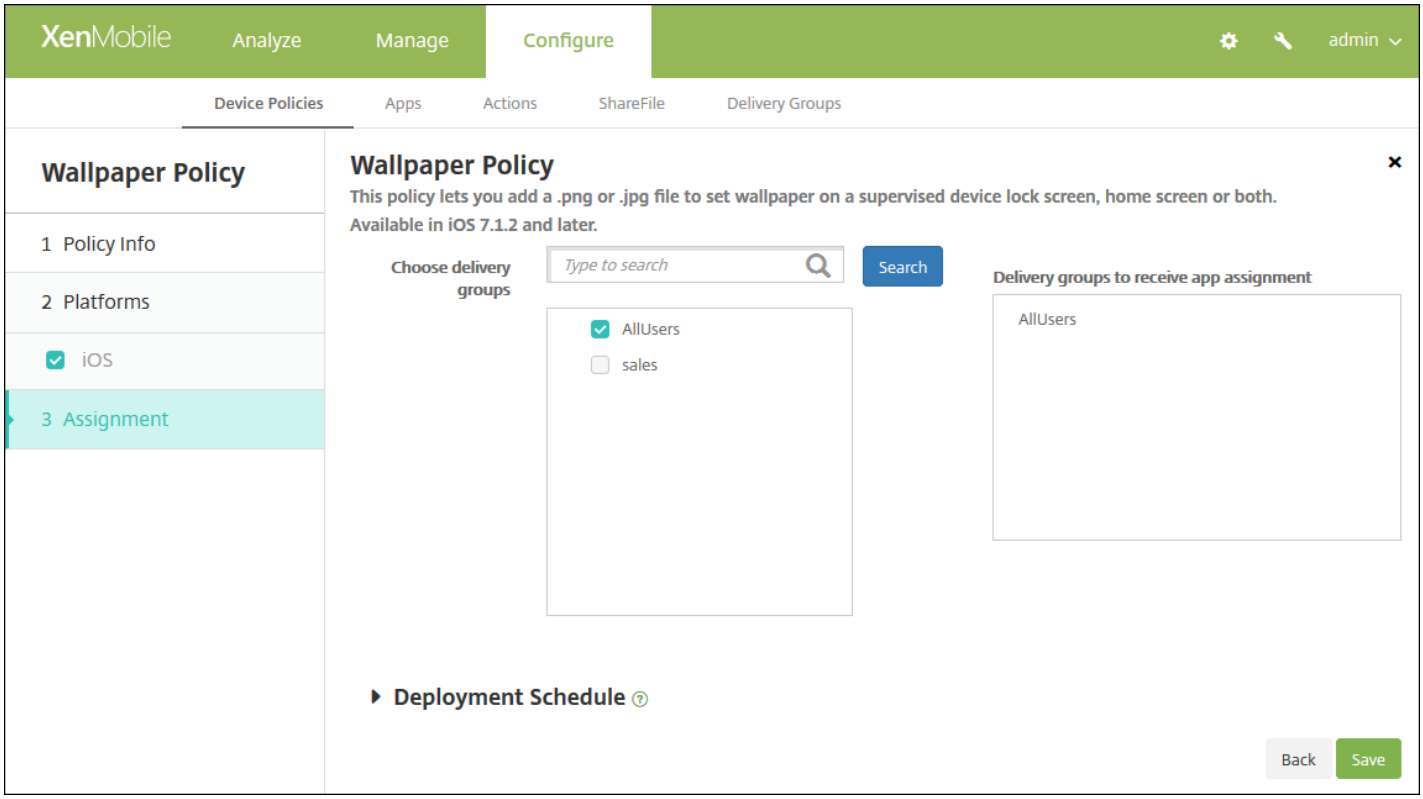


Pour configurer ces paramètres :

- **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.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie de fond d'écran** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 lorsque le déploiement précédent a échoué.** L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégie de filtre de contenu Web

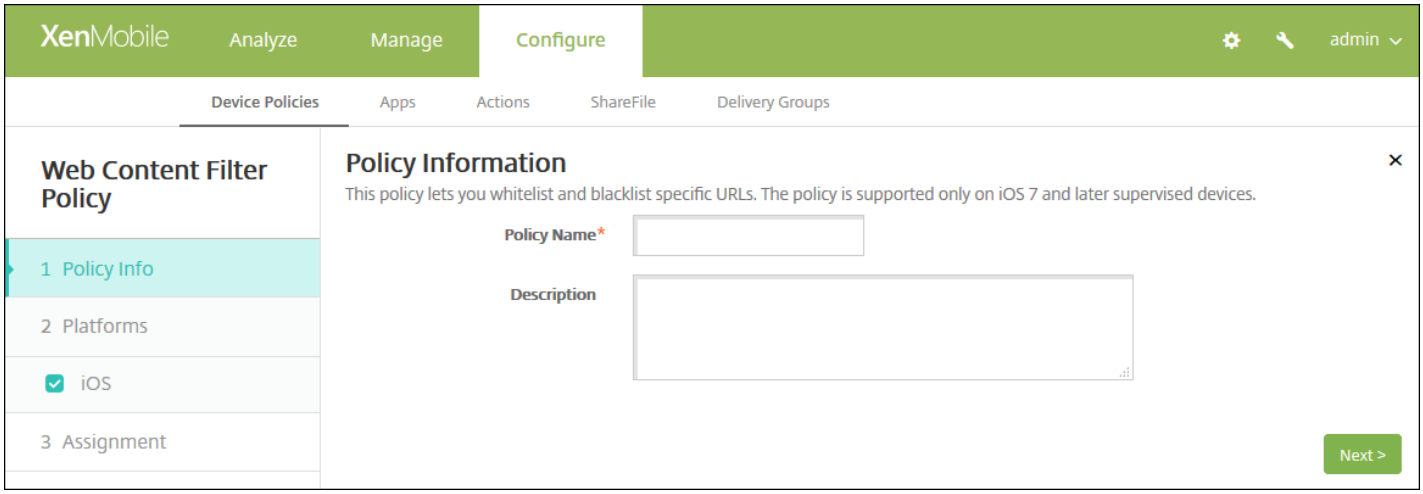
Jul 27, 2016

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 blanches et listes noires. 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.

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.

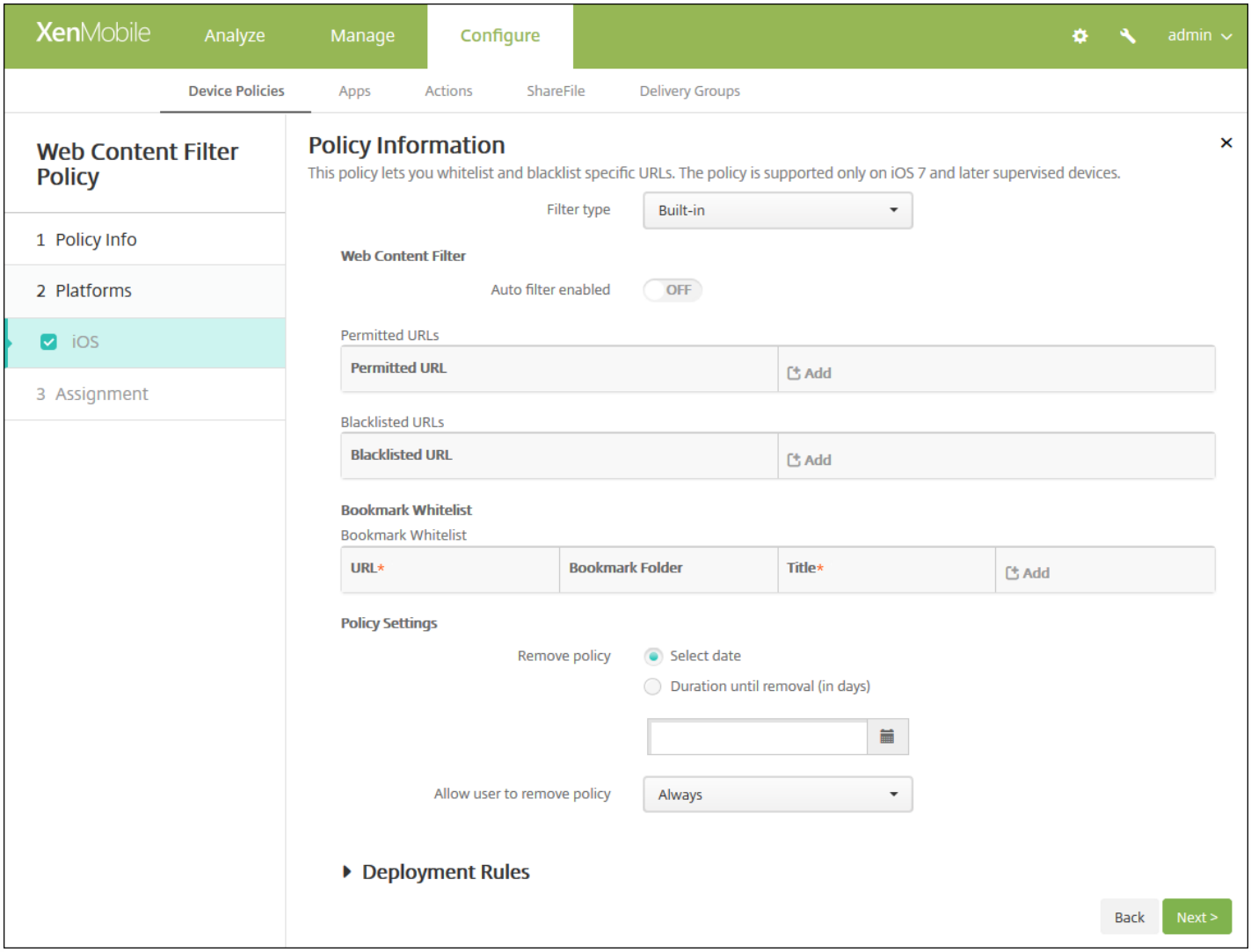
3. Cliquez sur **Plus** puis, sous **Sécurité**, cliquez sur **Filtre de contenu Web**. La page **Stratégie de filtre de contenu Web** s'affiche.



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 **Next**. La page d'informations **Plate-forme iOS** s'affiche.



6. Configurez les paramètres suivants :

- **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**.

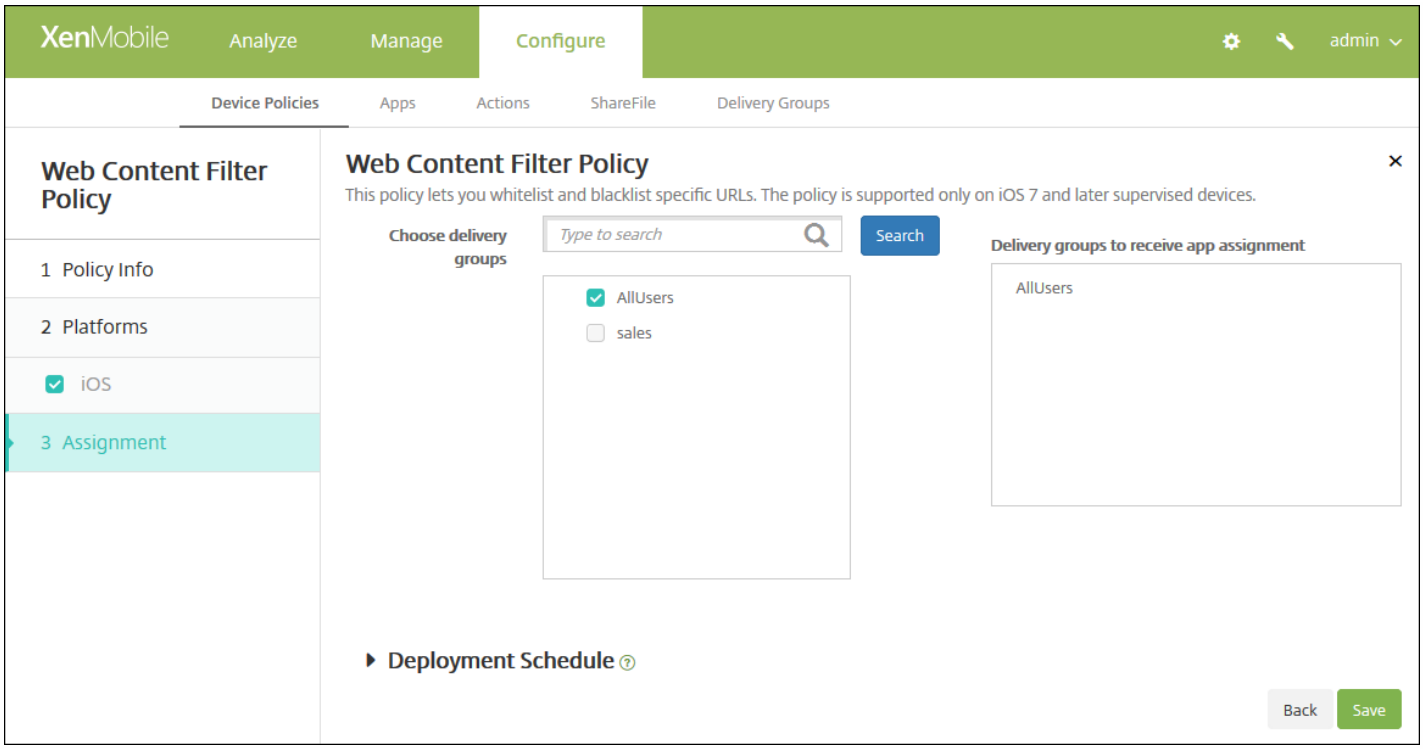
Paramètres du type de filtre Intégré

Paramètres du type de filtre Plug-in

- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  - 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.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie de filtre de contenu Web** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 ON ou OFF. L'option par défaut est OFF.**

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.

11. Cliquez sur **Enregistrer**.

Stratégies Webclip

Jul 27, 2016

Vous pouvez placer des raccourcis ou clips Websur des sites Web. Ils apparaissent à côté des applications sur les appareils. Vous pouvez spécifier vos propres icônes pour représenter les clips Web pour les appareils iOS, Mac OS X et Android ; Windows Tablet requiert uniquement une étiquette et une adresse URL.

Paramètres iOS

Paramètres Mac OS X

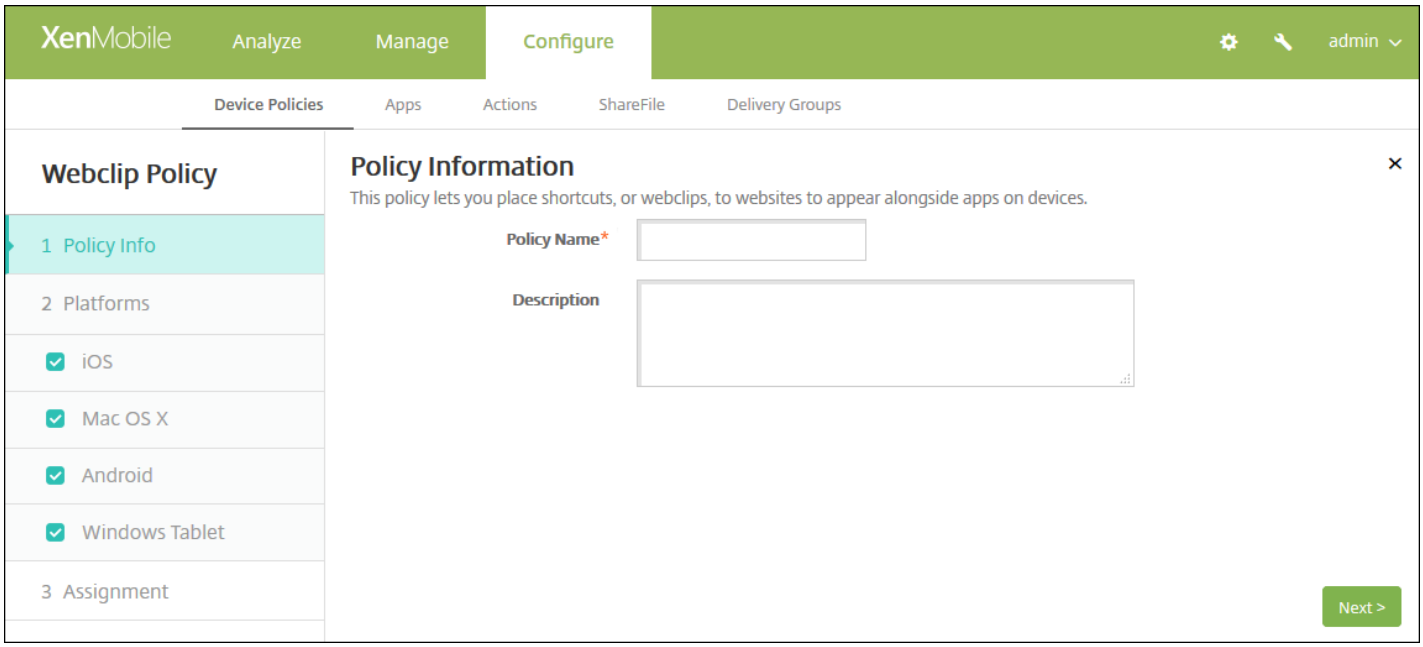
Paramètres Android

Paramètres Windows Tablet

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.

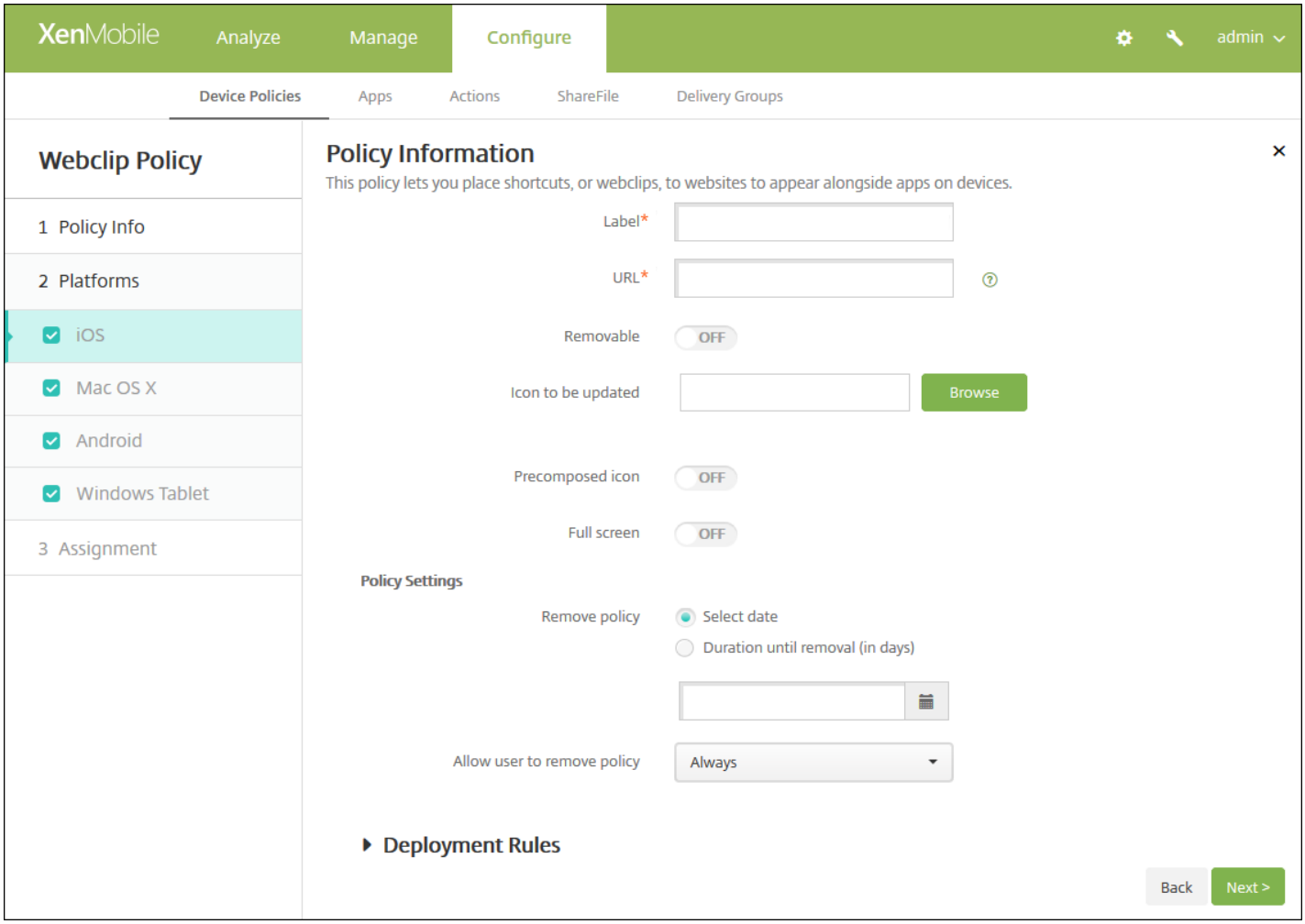
3. Développez **Plus** puis, sous **Applications**, cliquez sur **Clip Web**. La page Stratégie de **clip Web** s'affiche.



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).

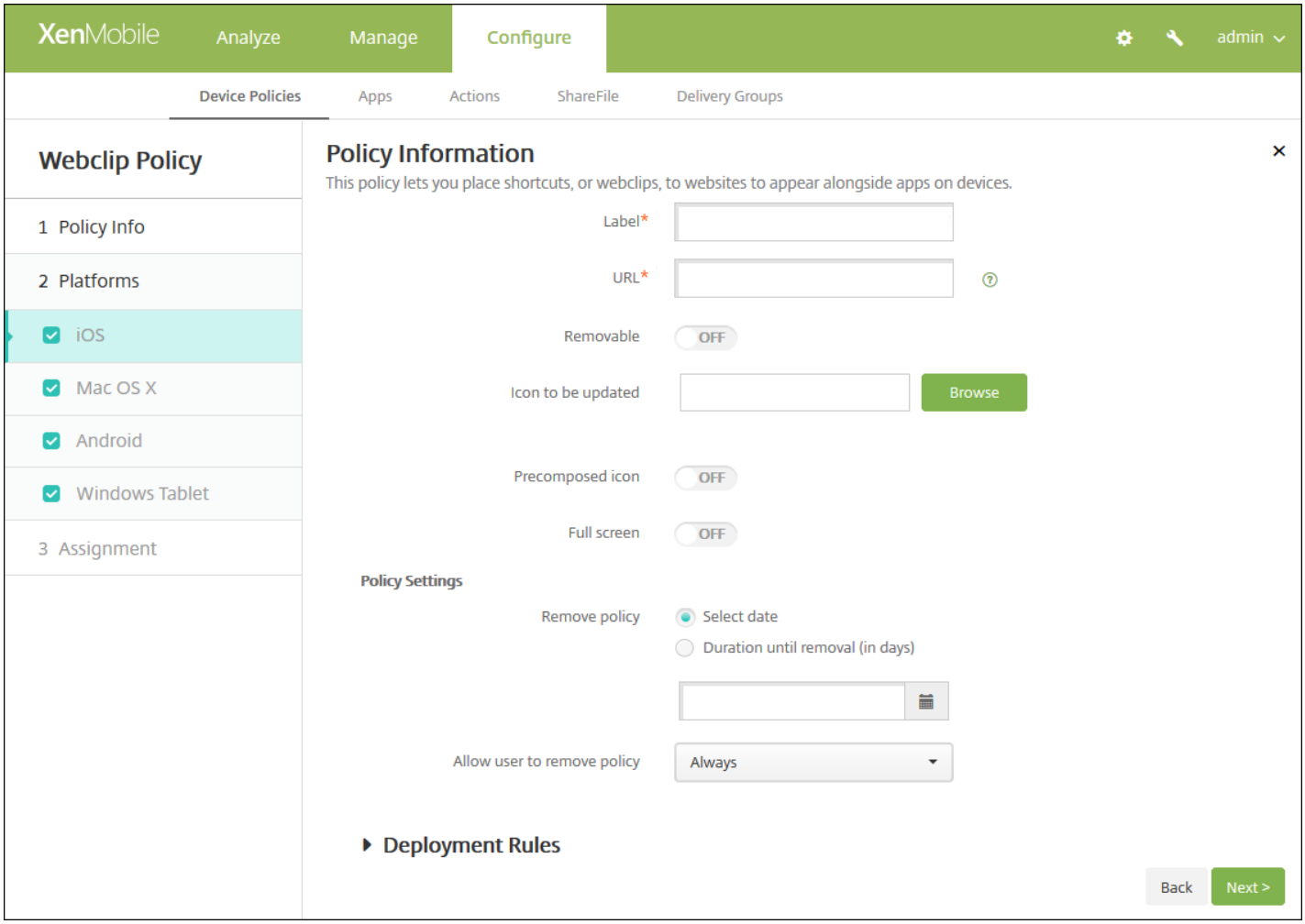
5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.



6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

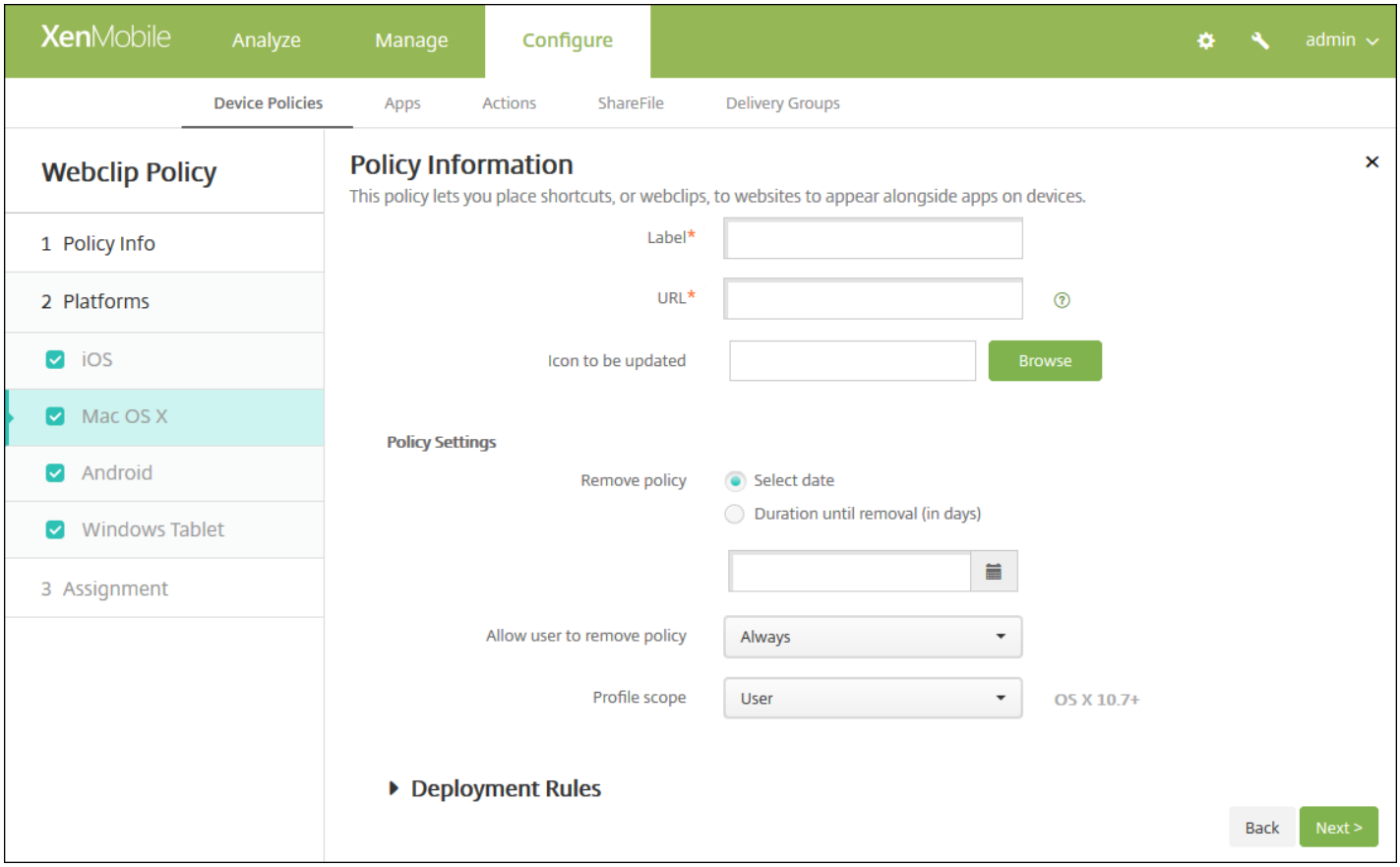
Configurer les paramètres pour iOS



Pour configurer ces paramètres :

- **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, http://serveur.
- **Amovible** : indiquez si les utilisateurs peuvent supprimer le clip Web. La valeur par défaut est **OFF**.
- **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 **OFF**, ce qui ajoute des effets.
- **Plein écran**: indiquez si la page Web associée s'ouvre en mode plein écran. La valeur par défaut est **OFF**.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  - 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.

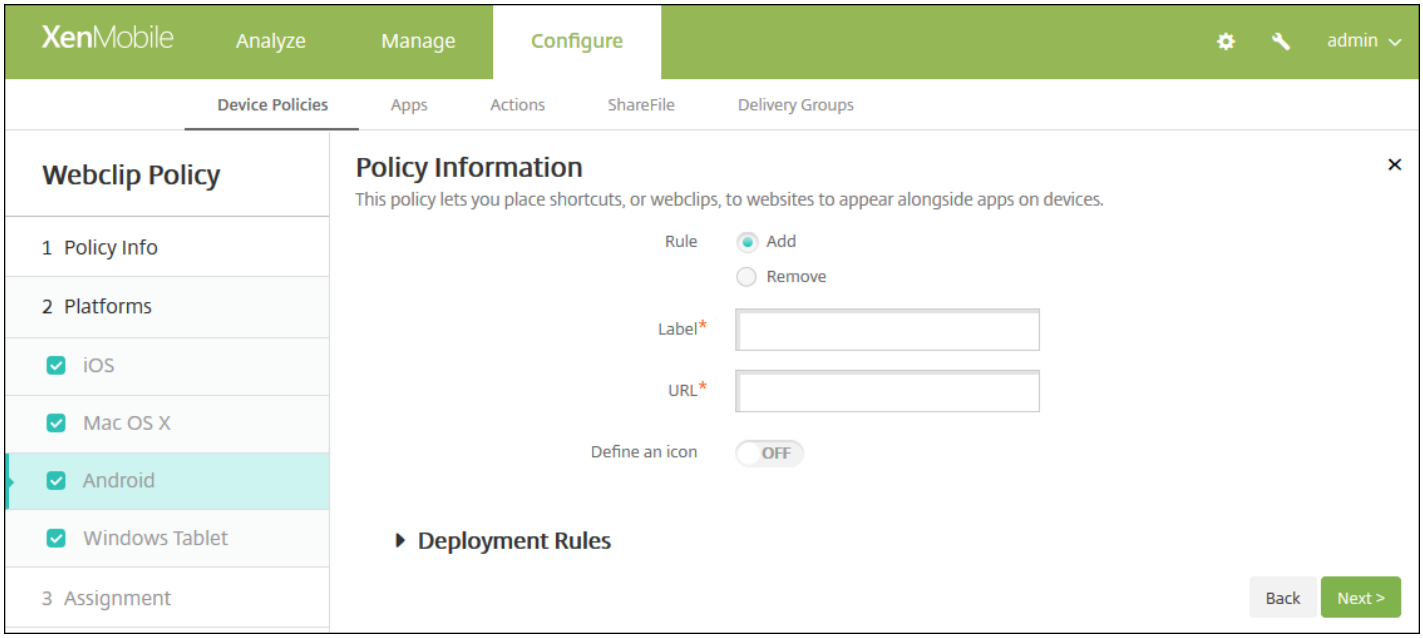
Configurer les paramètres pour Mac OS X



Pour configurer ces paramètres :

- **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, http://serveur.
- **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 de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  - 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.
  - Dans la liste **Étendue du profil**, cliquez sur **Utilisateur** ou **Système**. Cette option est disponible sur OS X 10.7 et versions ultérieures.

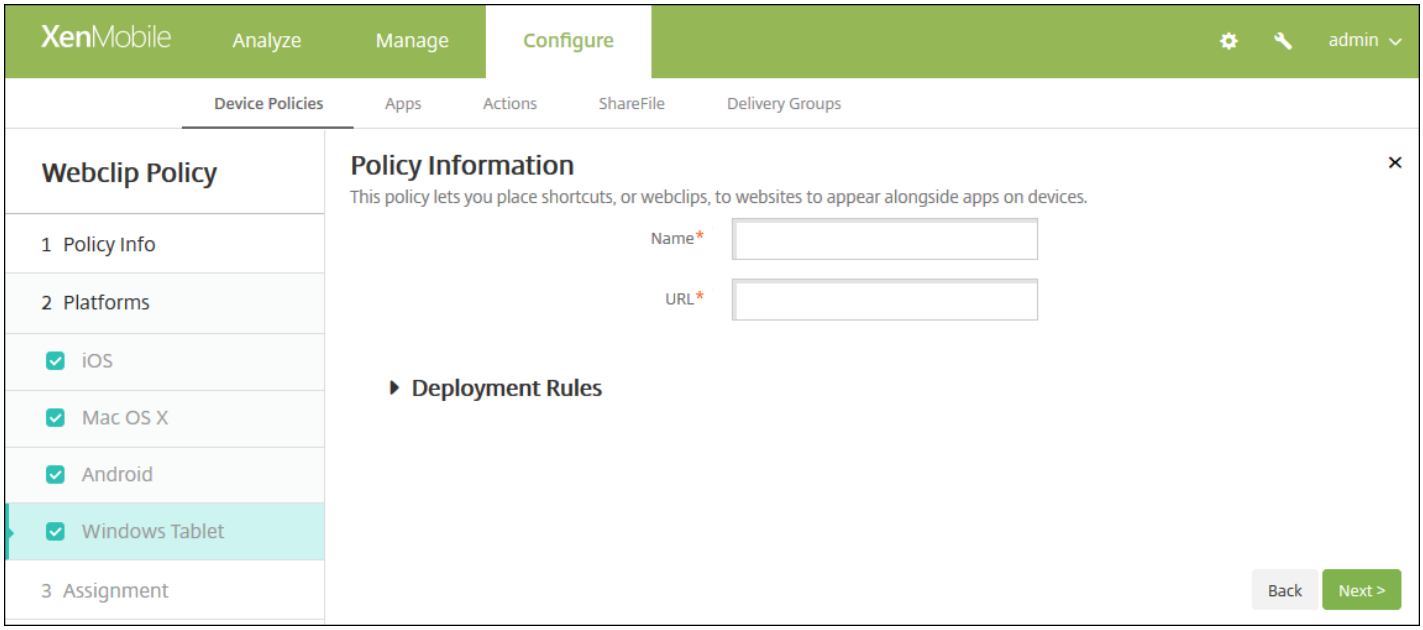
Configurer les paramètres pour Android



Pour configurer ces paramètres :

- **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 **OFF**.
- **Fichier icône** : si **Définir une icône** est réglé sur **ON**, sélectionnez le fichier d'icône à utiliser en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.

Configurer les paramètres pour Windows Tablet

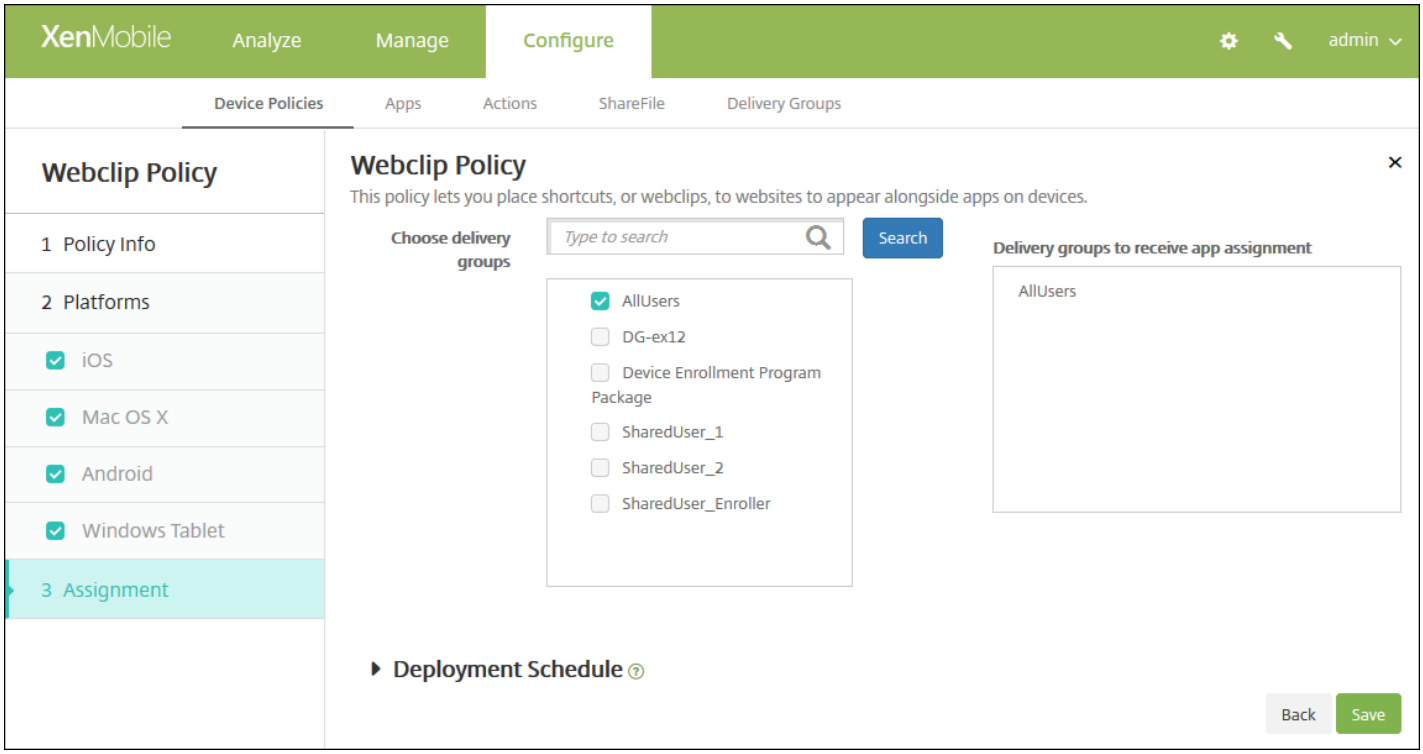


Pour configurer ces paramètres :

- **Nom** : entrez l'étiquette qui s'affichera avec le clip Web.
- **URL** : entrez l'adresse URL associée avec le clip Web.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie de clip Web** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

Stratégies WiFi

Jul 27, 2016

Vous pouvez créer ou modifier des stratégies Wi-Fi dans XenMobile sur la page Stratégies d'appareil de la console XenMobile. Les stratégies Wi-Fi vous permettent de gérer la manière dont les utilisateurs connectent leurs appareils à des réseaux sans fil en définissant ce qui suit : noms et types de réseau, stratégies d'authentification et de sécurité, serveurs proxy et d'autres détails liés à l'utilisation du Wi-Fi pour tous les utilisateurs d'une plate-forme particulière.

Vous pouvez configurer des paramètres Wi-Fi pour les utilisateurs pour les plates-formes suivantes : iOS, Mac OS X, Android (comprend les appareils activés pour Android for Work), Windows Phone et Windows Tablet. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans cet article.

Paramètres iOS

Paramètres Mac OS X

Paramètres Android

Paramètres Windows Phone

Paramètres Windows Tablet

Important

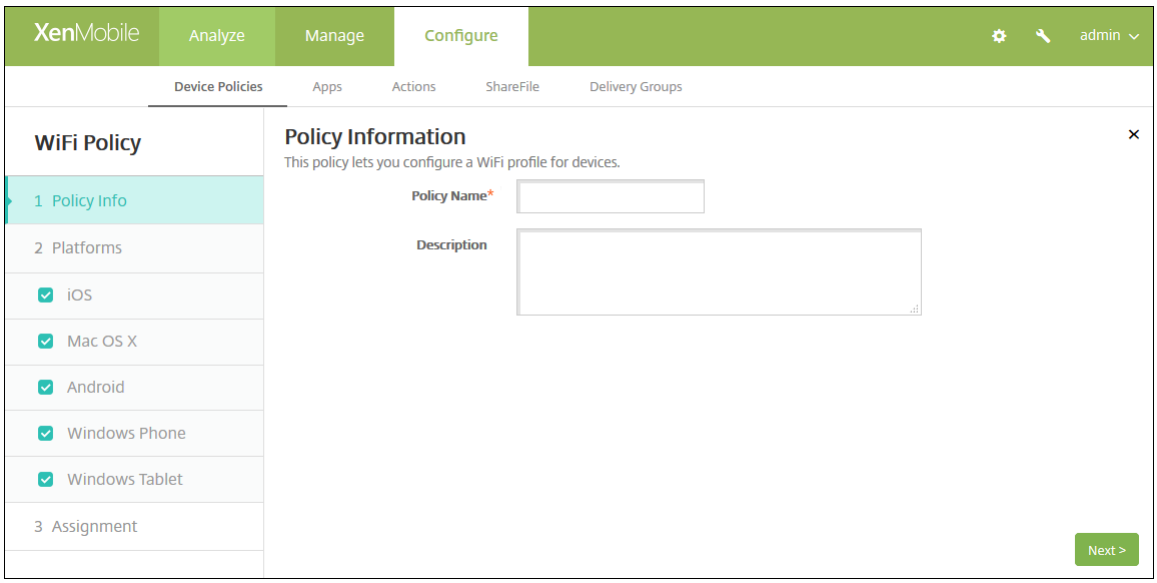
Avant de créer une nouvelle stratégie, vous devez effectuer les étapes suivantes :

- Créez les groupes de déploiement 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.

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. Cliquez sur **Wi-Fi**. La page **Stratégie WiFi** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

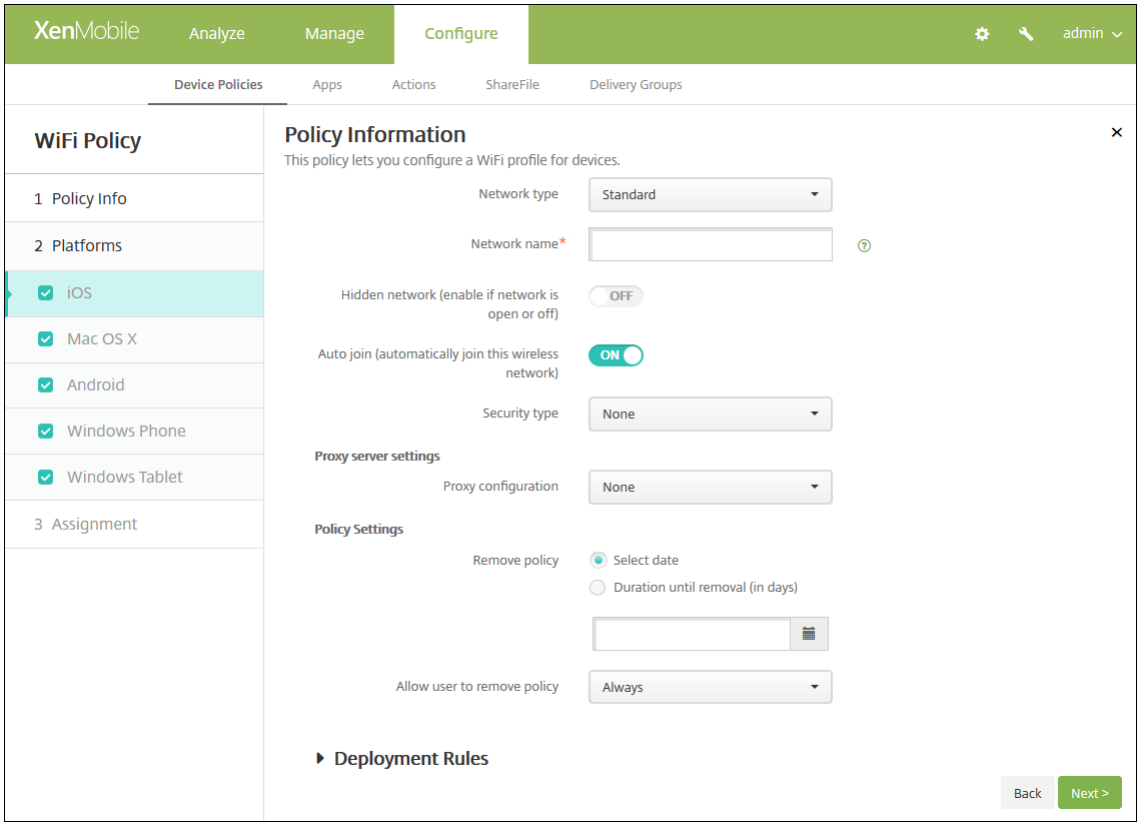
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour iOS



Pour configurer ces paramètres :

- **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 sur 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. La valeur par défaut est **ON**.
- **Type de sécurité** : dans la liste, cliquez sur 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.

WPA, WPA Personnel, Tous (Personnel)

WEP Entreprise, WPA Entreprise, WPA2 Entreprise, Tous (Entreprise)

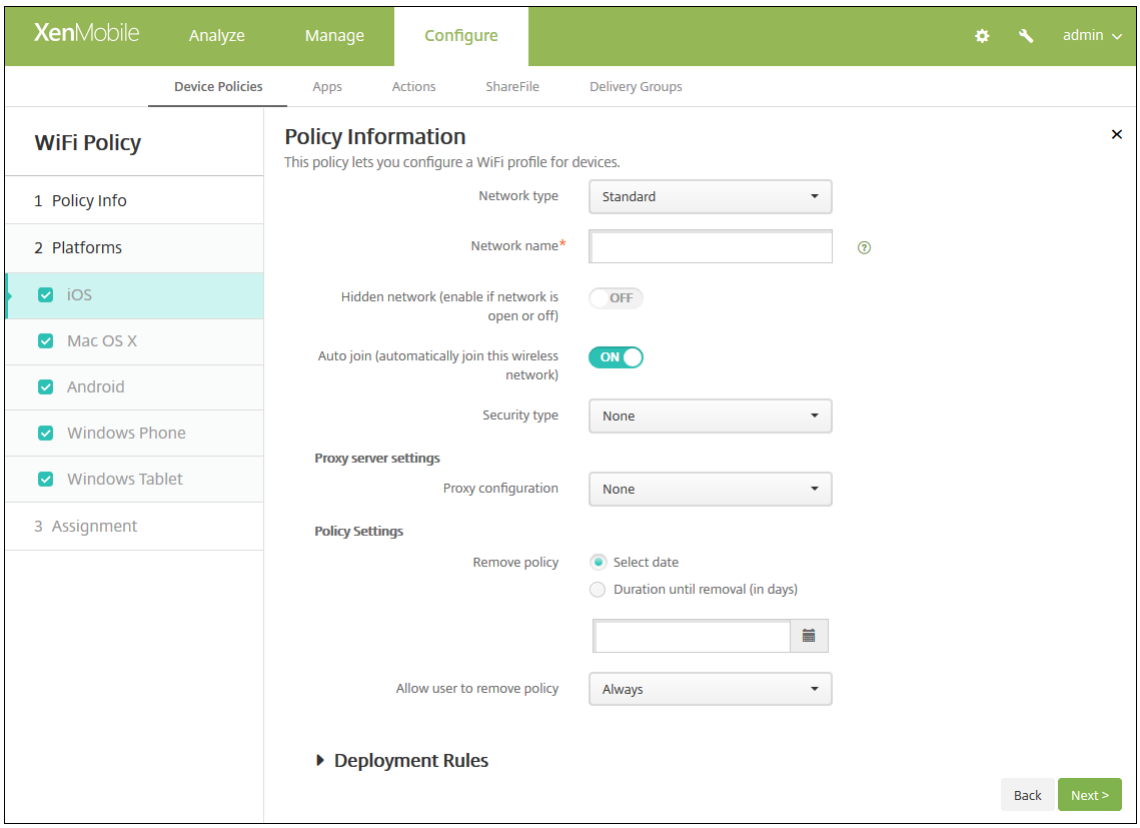
- **les paramètres du serveur proxy ;**
  - **Configuration du proxy** : dans la liste, cliquez sur Aucun, Manuel ou Automatique pour définir la façon dont la connexion VPN transite via un serveur proxy et configurez des options supplémentaires. La valeur par défaut est Aucun, ce qui n'exige aucune configuration 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 **ON**. Cette option est disponible uniquement sur iOS 7.0 et versions ultérieures.
- **Hotspot 2.0**
  - **Nom d'opérateur affiché** : entrez le nom d'opérateur à afficher. S'applique à iOS 7.0 et versions ultérieures.
  - **Nom de domaine** : entrez le nom de domaine utilisé pour la négociation Wi-Fi Hotspot 2.0. S'applique à iOS 7.0 et versions ultérieures.
  - **Autoriser la connexion aux réseaux partenaires itinérants** : sélectionnez cette option si vous voulez autoriser les appareils à se connecter à des réseaux partenaires itinérants. S'applique à iOS 7.0 et versions ultérieures.
  - **Identificateurs d'organisations (OI) du consortium d'itinérance** : ajoutez des identificateurs d'organisations du consortium d'itinérance utilisés pour la négociation Wi-Fi Hotspot 2.0 (facultatif).
  - **Noms de royaumes d'identificateur d'accès réseau (NAI)** : ajoutez des noms de domaines d'identificateur d'accès réseau utilisés pour la négociation Wi-Fi Hotspot 2.0 (facultatif).

- **Codes de pays mobiles (MCCs) et configurations de réseaux mobiles (MNCs)** : ajoutez des paires codes de pays mobiles et configurations de réseaux mobiles utilisées pour la négociation Wi-Fi Hotspot 2.0 (facultatif). Chaque chaîne doit contenir exactement six chiffres.

  Reportez-vous aux sections précédentes pour obtenir des informations sur les paramètres **Protocoles, types EAP acceptés**, **Protocoles, EAP-FAST** et **Authentification**.

- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  - 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.

Configurer les paramètres pour Mac OS X



Pour configurer ces paramètres :

- **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 sur 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. La valeur par défaut est **ON**.
- **Type de sécurité** : dans la liste, cliquez sur 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.

WPA, WPA Personnel, WPA 2 Personnel, Tous (Personnel)

WEP Entreprise, WPA Entreprise, WPA2 Entreprise, Tous (Entreprise)

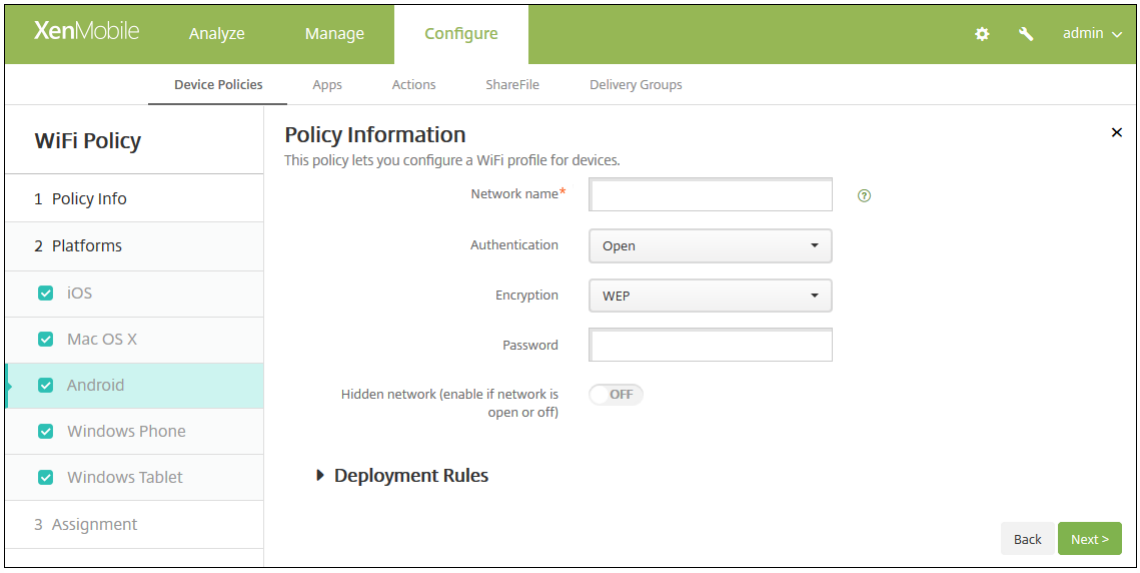
- **Utiliser comme configuration de fenêtre de connexion** : indiquez si vous souhaitez utiliser les informations d'identification saisies dans la fenêtre d'ouverture de session pour l'authentification de l'utilisateur.
- **les paramètres du serveur proxy ;**
  - **Configuration du proxy** : dans la 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 **ON**. Cette option est disponible uniquement sur iOS 7.0 et versions ultérieures.
- **Hotspot 2.0**
  - **Nom d'opérateur affiché** : entrez le nom d'opérateur à afficher. S'applique à iOS 7.0 et versions ultérieures.
  - **Nom de domaine** : entrez le nom de domaine utilisé pour la négociation Wi-Fi Hotspot 2.0. S'applique à iOS 7.0 et versions ultérieures.
  - **Autoriser la connexion aux réseaux partenaires itinérants** : sélectionnez cette option si vous voulez autoriser les appareils à se connecter à des réseaux partenaires itinérants. S'applique à iOS 7.0 et versions ultérieures.
  - **Identificateurs d'organisations (OI) du consortium d'itinérance** : ajoutez des identificateurs d'organisations du consortium d'itinérance utilisés pour la négociation Wi-Fi Hotspot 2.0 (facultatif).
  - **Noms de royaumes d'identificateur d'accès réseau (NAI)** : ajoutez des noms de domaines d'identificateur d'accès réseau utilisés pour la négociation Wi-Fi Hotspot 2.0 (facultatif).
  - **Codes de pays mobiles (MCCs) et configurations de réseaux mobiles (MNCs)** : ajoutez des paires codes de pays mobiles et configurations de réseaux mobiles utilisées pour la négociation Wi-Fi Hotspot 2.0 (facultatif). Chaque chaîne doit contenir exactement six chiffres.

    Reportez-vous aux sections précédentes pour obtenir des informations sur les paramètres **Protocoles, types EAP acceptés**, **Protocoles, EAP-FAST** et **Authentification**.

- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  - 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.
  - En regard de **Étendue du profil**, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement pour OS X 10.7 et versions ultérieures.

Configurer les paramètres pour Android



Pour configurer ces paramètres :

- **Nom du réseau** : entrez le SSID qui est affiché dans la liste des réseaux disponibles sur l'appareil de l'utilisateur.
- **Authentification** : dans la liste, cliquez sur 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.

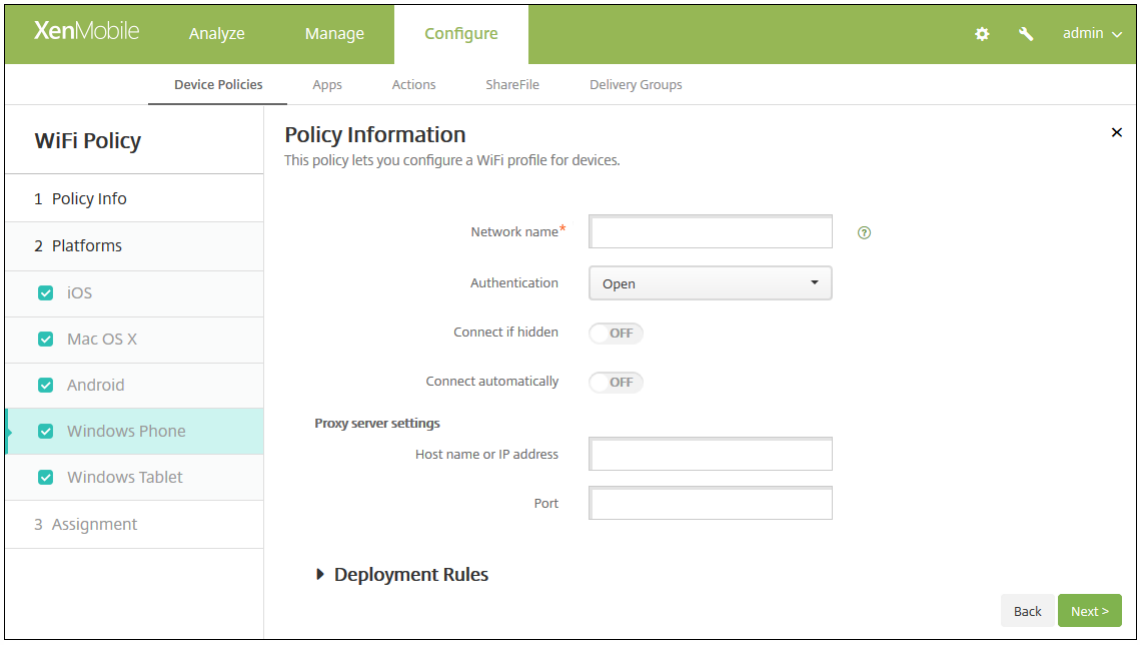
Ouvert, partagé

WPA, WPA-PSK, WPA2, WPA2-PSK

802.1x

- **Réseau masqué (activer si le réseau est ouvert ou désactivé)** : sélectionnez cette option pour spécifier si le réseau est masqué.

Configurer les paramètres pour Windows Phone



Pour configurer ces paramètres :

- **Nom du réseau** : entrez le SSID qui est affiché dans la liste des réseaux disponibles sur l'appareil de l'utilisateur.
- **Authentification** : dans la liste, cliquez sur le type de sécurité à utiliser avec la connexion Wi-Fi.
  - Ouverte
  - WPA Personnel
  - WPA-2 Personnel
  - WPA-2 Enterprise

  Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.

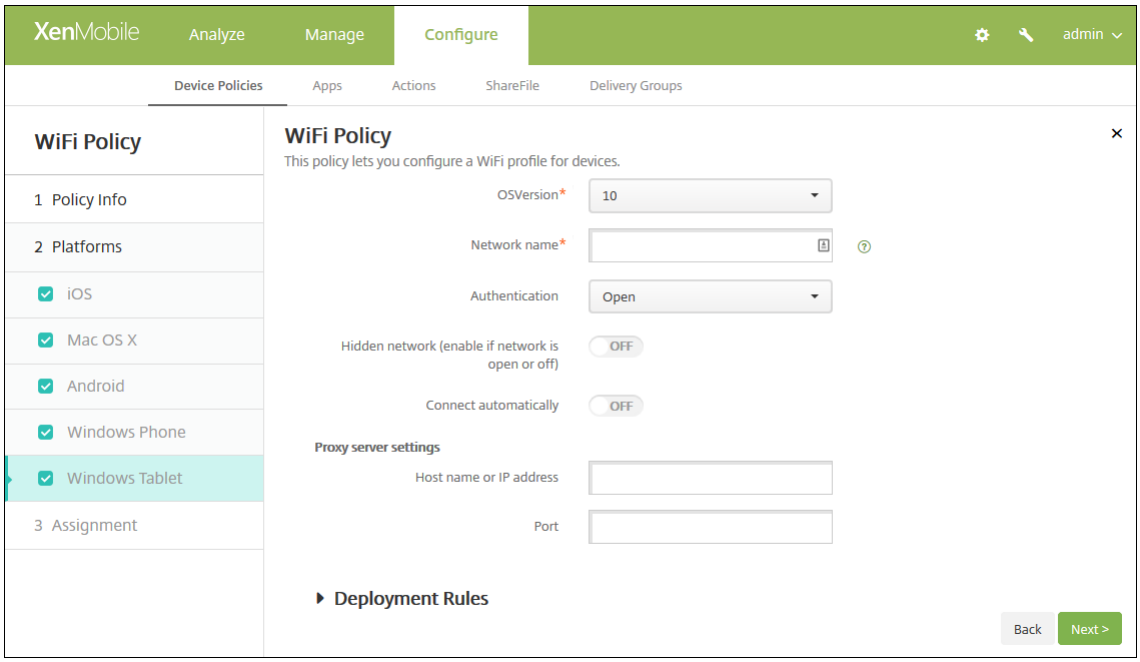
Ouverte

WPA Personnel, WPA-2 Personnel

WPA-2 Enterprise

- **les paramètres du serveur proxy ;**
  - **Nom d'hôte ou adresse IP** : entrez le nom ou l'adresse IP du serveur VPN.
  - **Port** : entrez le numéro de port du serveur proxy.

Configurer les paramètres pour Windows Tablet



Configurez les paramètres suivants :

- **Version de l'OS** : dans la liste, cliquez sur **8.1** pour Windows 8.1 ou **10** pour Windows 10. La valeur par défaut est de **10**.

Paramètres pour Windows 10

- **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

  Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.

Ouverte

WPA Personnel, WPA-2 Personnel

WPA-2 Enterprise

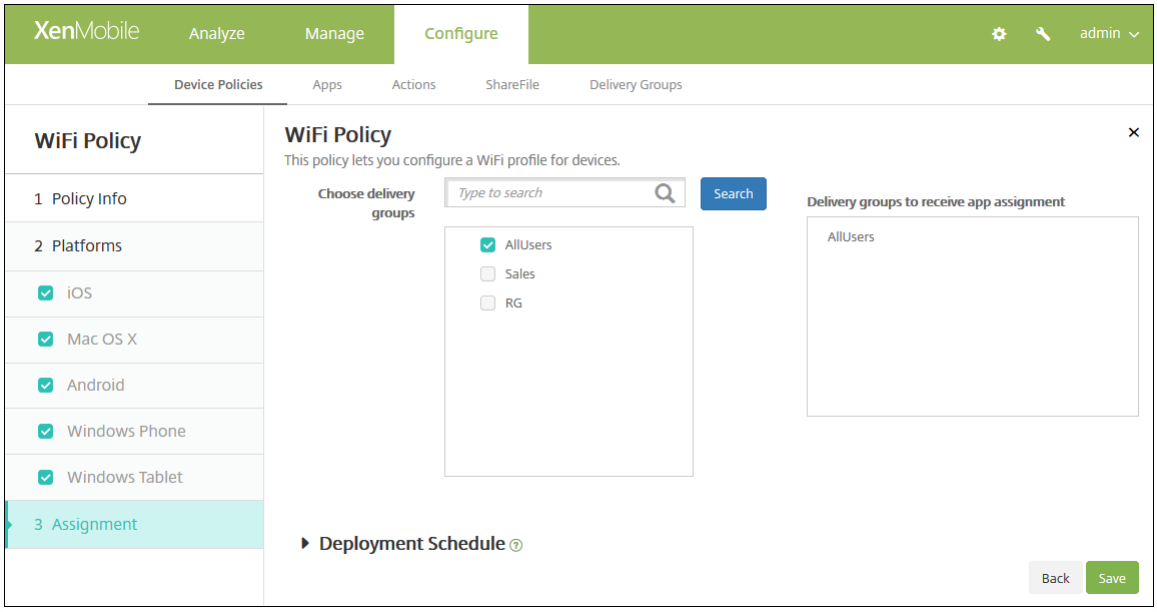
Paramètres pour Windows 8,1

- **Nom du réseau** : entrez le SSID qui est affiché dans la liste des réseaux disponibles sur l'appareil de l'utilisateur.
- **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
- **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.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'**attribution** de la **Stratégie WiFi** s'affiche.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie WiFi** s'affiche.
8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie WiFi** s'affiche.
8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie WiFi** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 lorsque le déploiement précédent a échoué.** L'option par défaut est **À chaque connexion**.

- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégie de certificat Windows CE

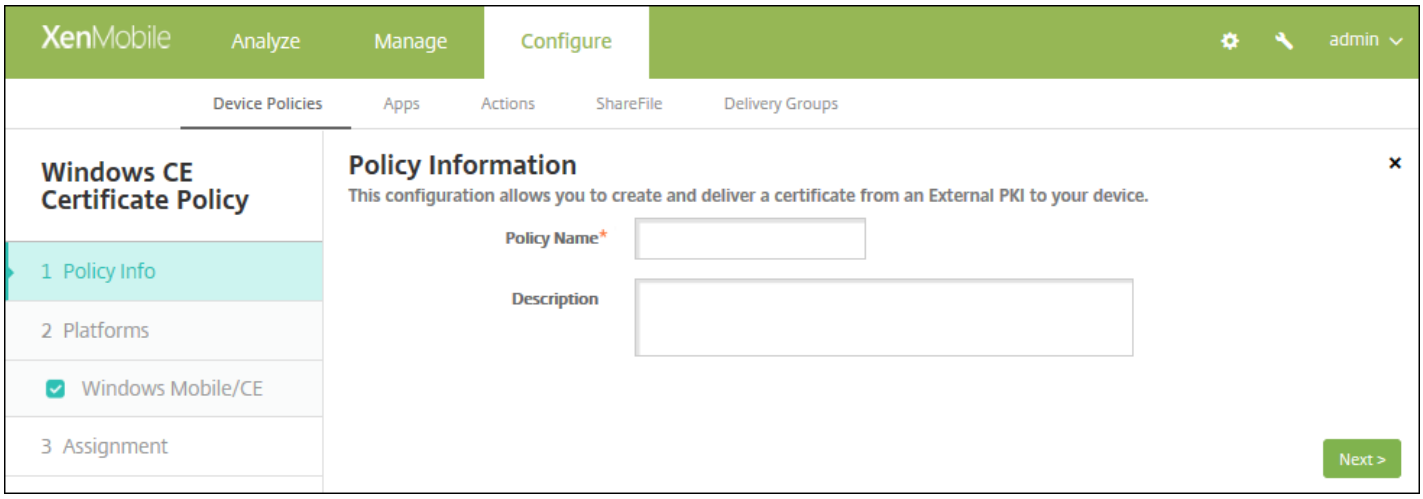
Jul 27, 2016

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. Consultez la section Certificats pour de plus amples informations sur les certificats et les entités PKI.

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.

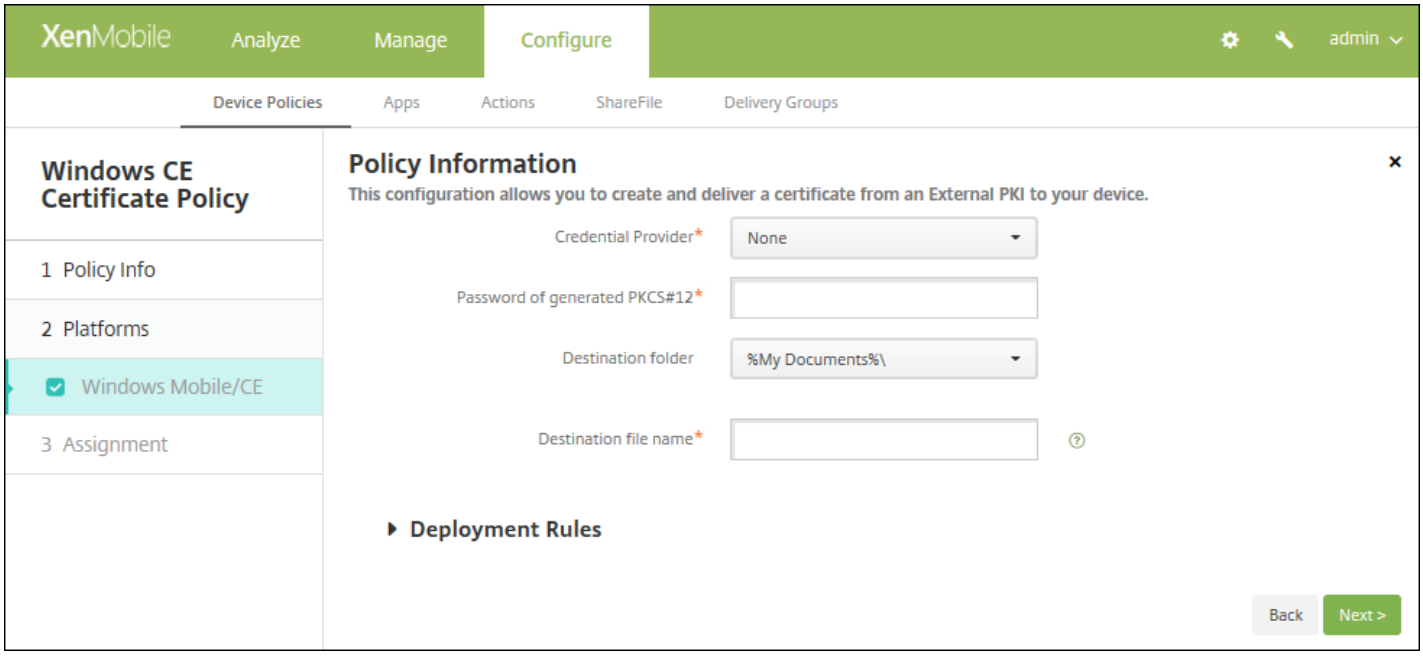
3. Développez **Plus** puis, sous **Sécurité**, cliquez sur **Certificats Windows CE**. La page d'informations **Stratégie de certificat Windows CE** s'affiche.



4. Dans le panneau **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 **Next**. La page d'informations **Stratégie de certificat Windows CE** s'affiche.

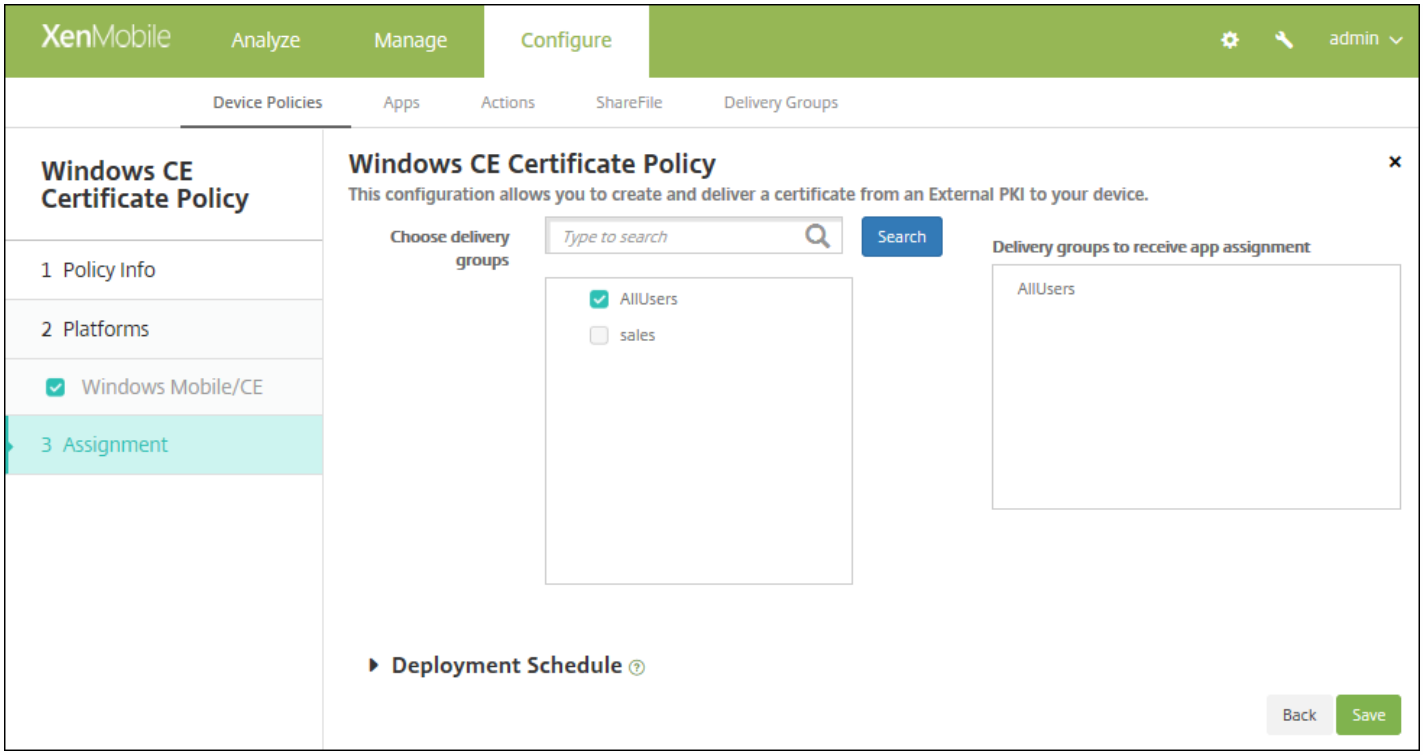


6. Configurez les paramètres suivants :

- **Fournisseur d'identités** : dans la liste, cliquez sur le fournisseur d'identités. La valeur par défaut est **Aucune**.
- **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%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %Mes Documents%\
  - %Windows%\
- **Nom du fichier de destination** : entrez le nom du fichier de certificat.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie de certificat Windows CE** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 lorsque le déploiement précédent a échoué.** L'option par défaut est À chaque connexion.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est OFF.

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.

11. Cliquez sur **Enregistrer**.

Stratégie Worx Store

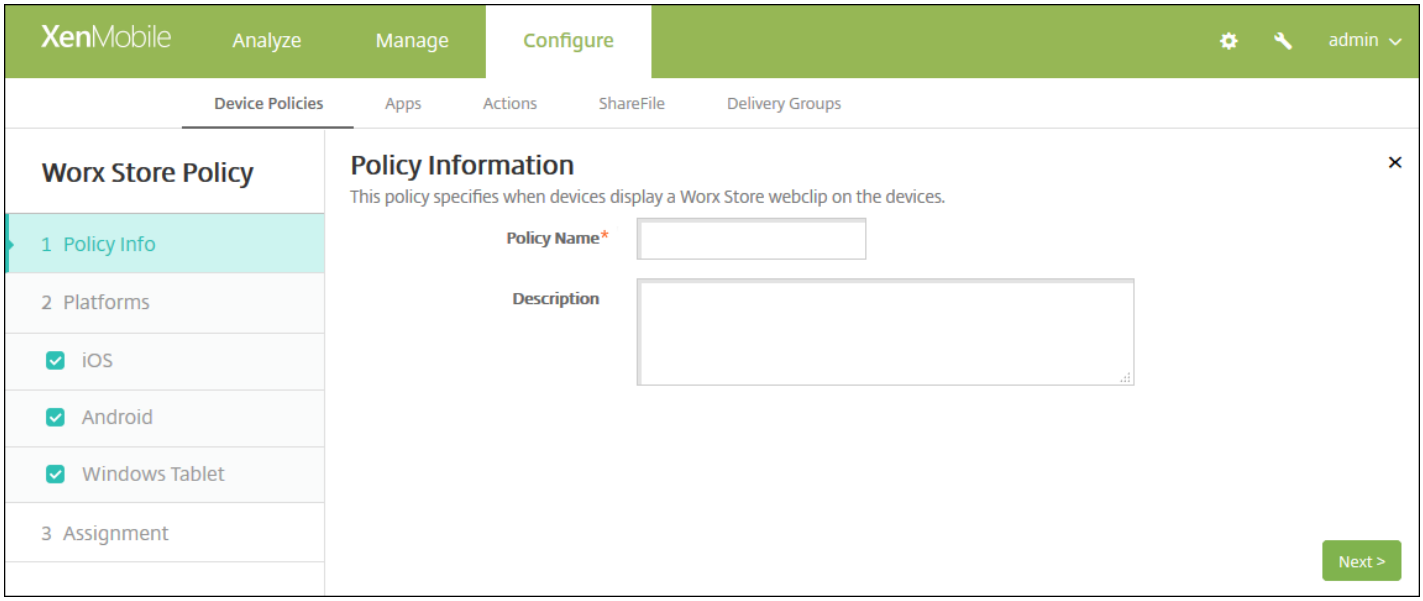
Jul 27, 2016

Vous pouvez créer une stratégie dans XenMobile afin de spécifier si les appareils iOS, Android ou Windows Tablet affichent un clip Web Worx Store sur l'écran d'accueil des appareils.

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.

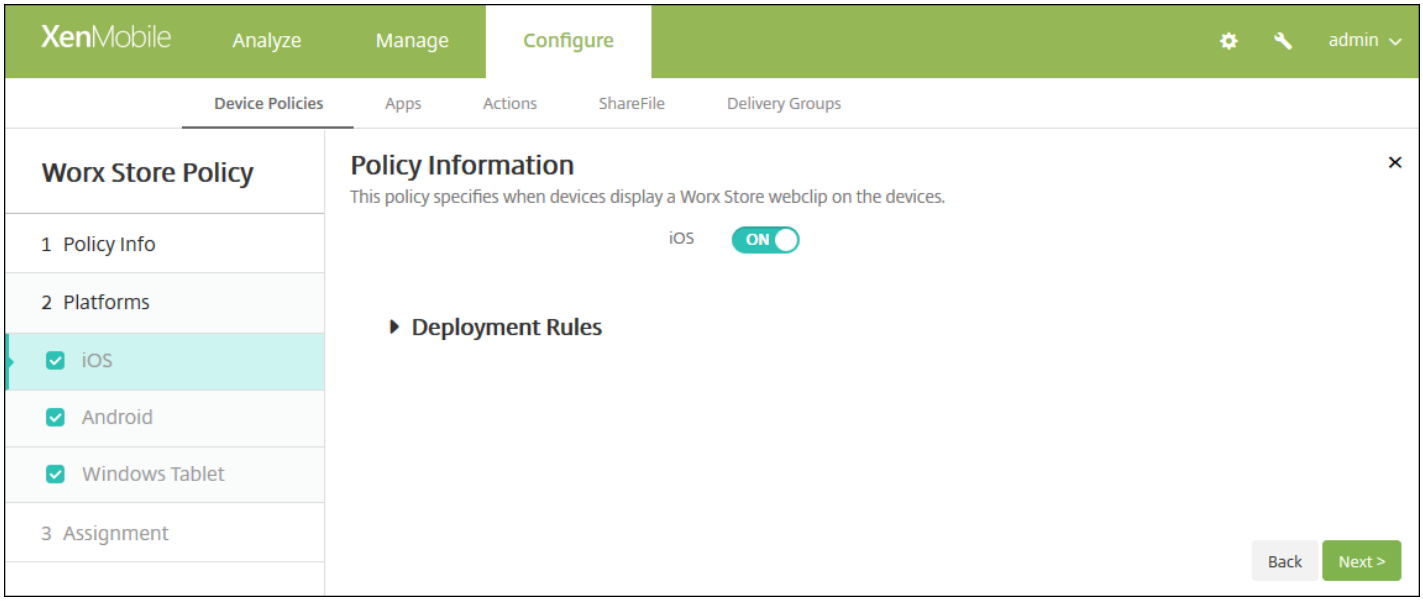
3. Développez **Plus** puis, sous **Applications**, cliquez sur **Worx Store**. La page **Stratégie Worx Store** s'affiche.



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 **Next**. La page **Plates-formes** s'affiche.



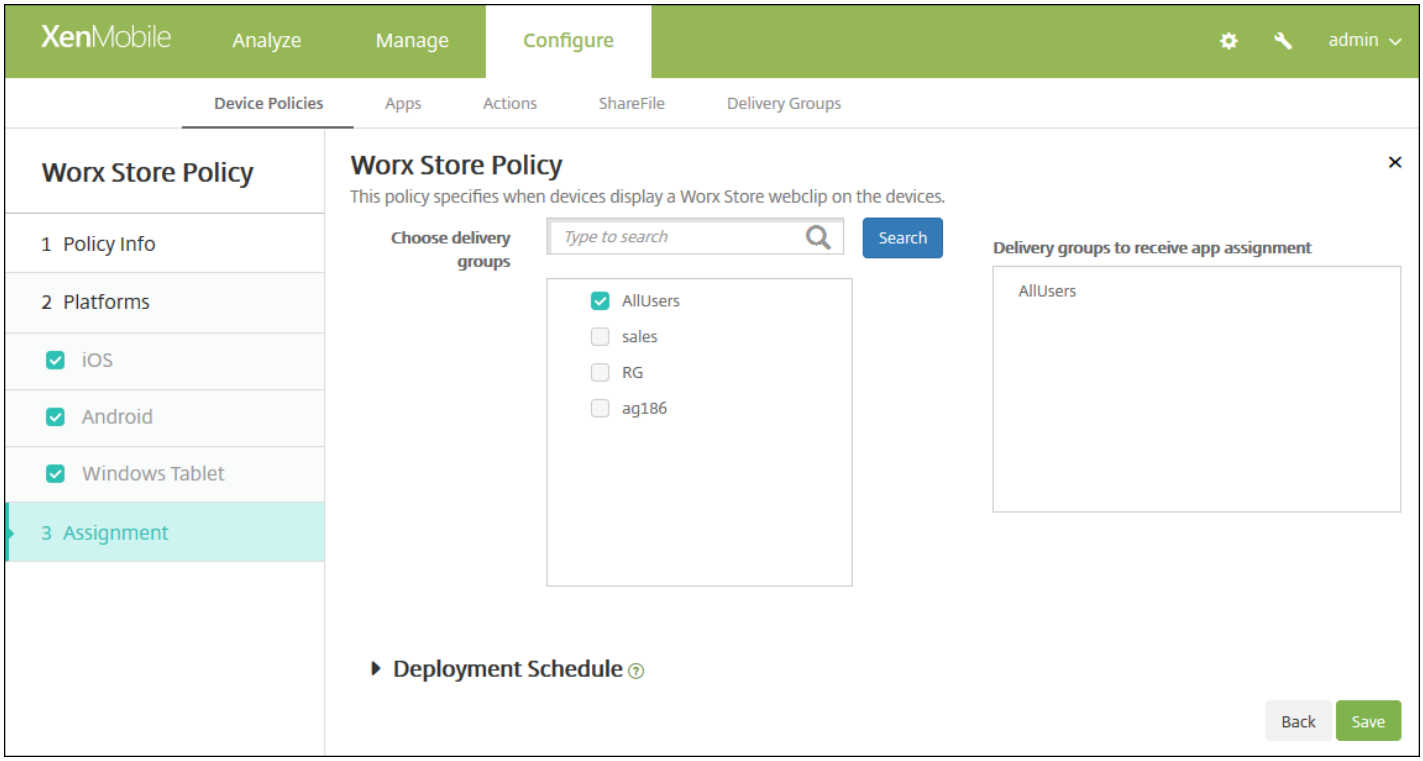
6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

7. Pour chaque plate-forme que vous configurez, sélectionnez si un clip Web Worx Store doit s'afficher sur les appareils des utilisateurs. La valeur par défaut est **ON**.

Pour chaque plate-forme que vous configurez, référez-vous à l'étape 8 pour savoir comment définir les règles de déploiement de cette plate-forme.

8. Configurez les règles de déploiement.

9. Cliquez sur **Suivant**, la page d'attribution de **Stratégie Work Store** 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 plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

12. Cliquez sur **Enregistrer**.

Stratégies d'options XenMobile

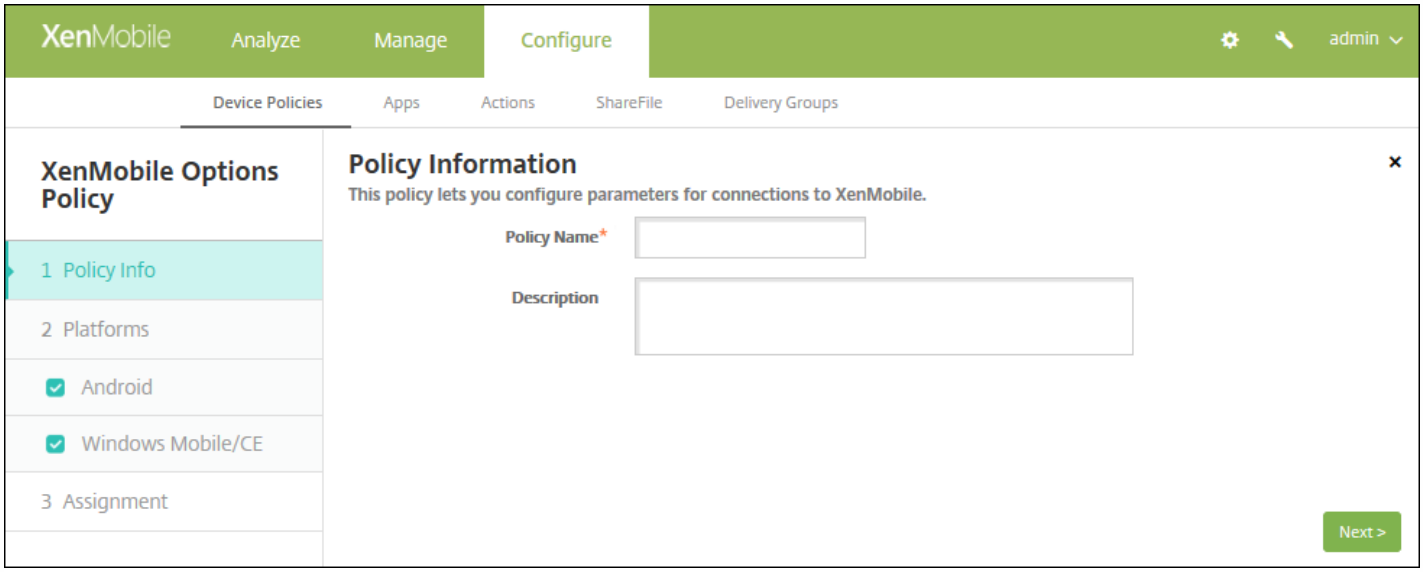
Jul 27, 2016

Vous ajoutez une stratégie d'options XenMobile pour configurer le comportement de Worx Home lors de la connexion à XenMobile à partir d'appareils Android et Windows Mobile/CE.

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 **Agent XenMobile**, cliquez sur **Options XenMobile**. La page **Stratégie d'options XenMobile** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

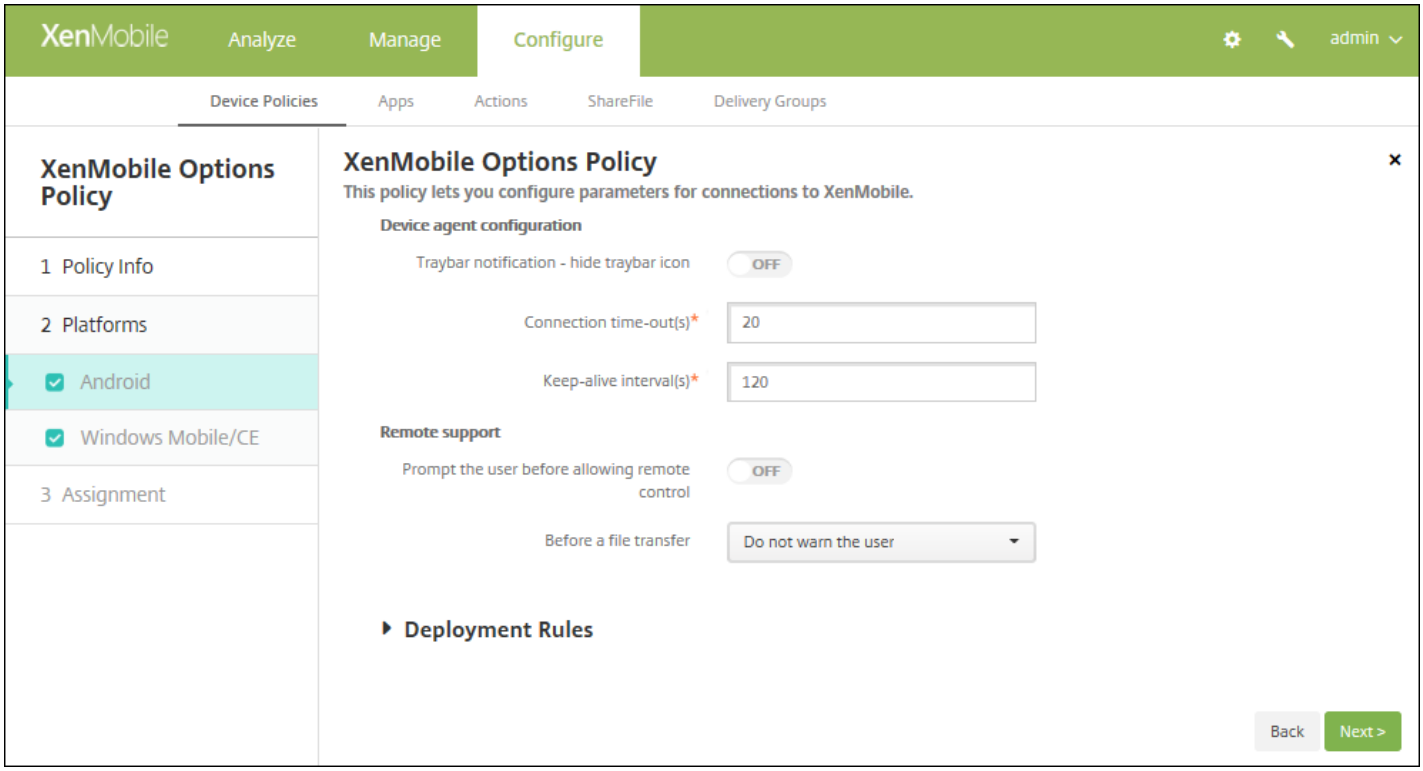
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

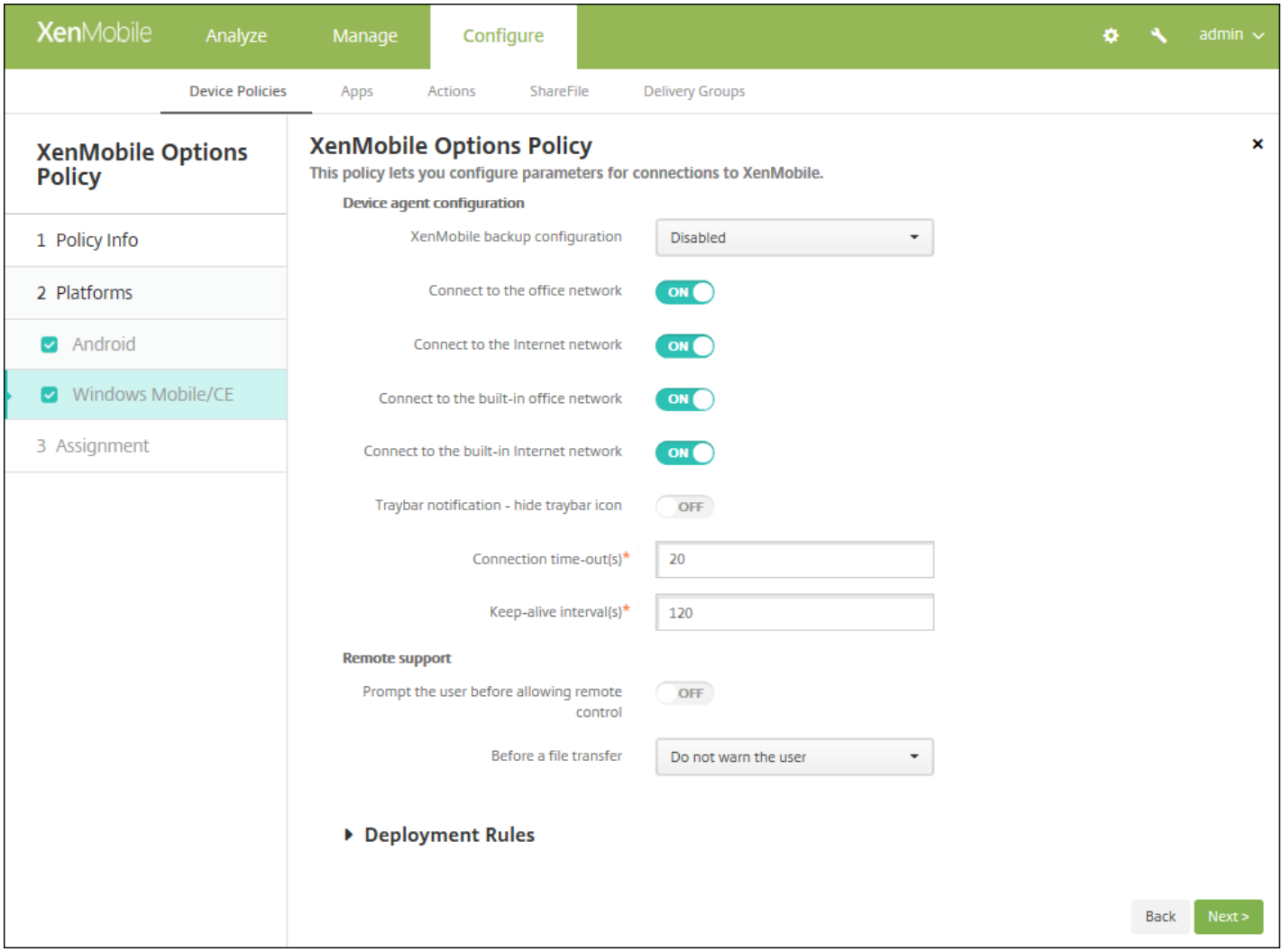
Configurer les paramètres pour Android



Pour configurer ces paramètres :

- **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 **OFF**.
- **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 **OFF**.
- **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**.

Configurer les paramètres pour Windows Mobile/CE



Pour configurer ces paramètres :

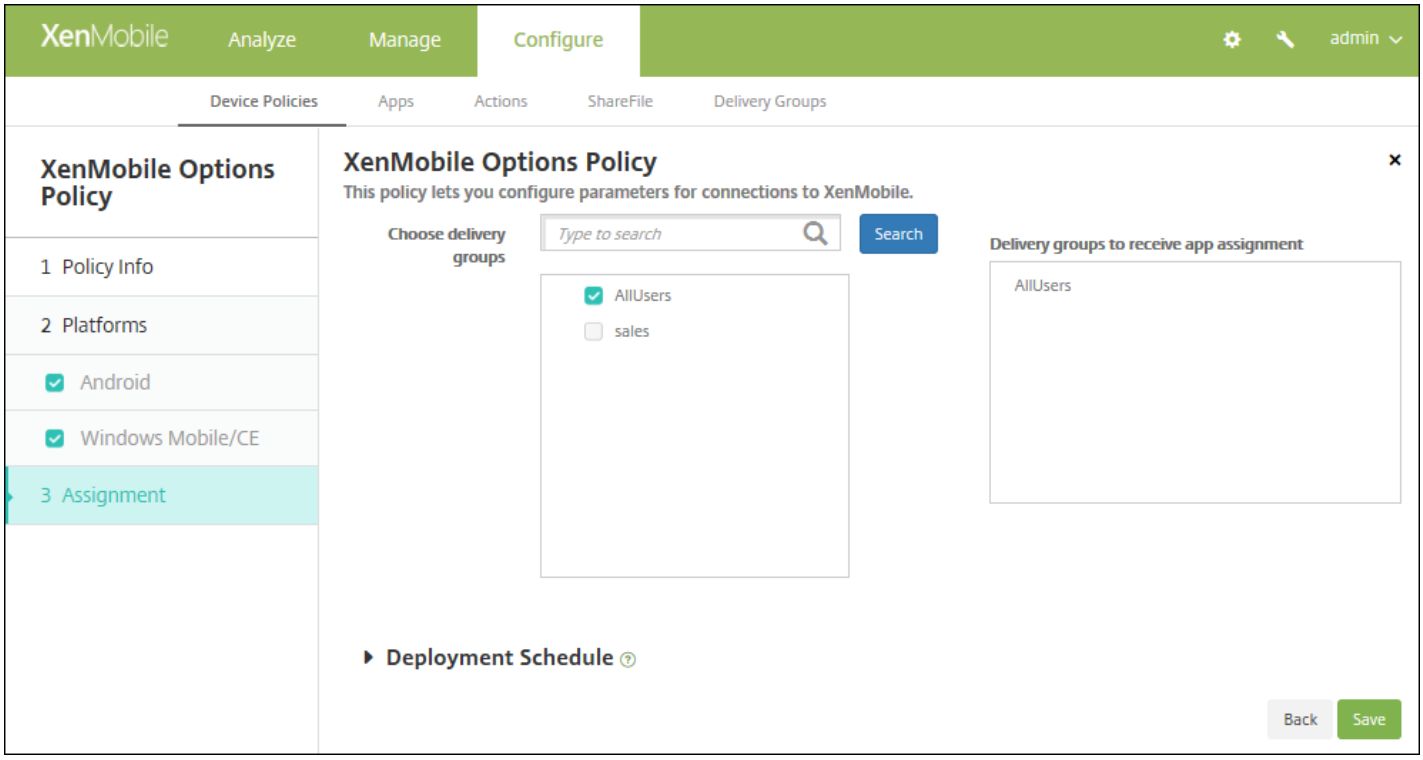
- **Configuration de l'agent sur l'appareil**
  - **Configuration de la sauvegarde XenMobile** : dans la liste, cliquez sur une option pour sauvegarder la configuration XenMobile sur les appareils des utilisateurs. La valeur par défaut est **Désactivée**. Les options disponibles sont les suivantes :
    - Désactivée
    - 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 **ON**, XenMobile détecte automatiquement le réseau.
  - **Se connecter au réseau Internet intégré** : lorsque cette valeur est définie sur **ON**, 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 **OFF**.
  - **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 **OFF**.
  - **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**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie d'options XenMobile** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 lorsque le déploiement précédent a échoué.** L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Stratégie de désinstallation de XenMobile

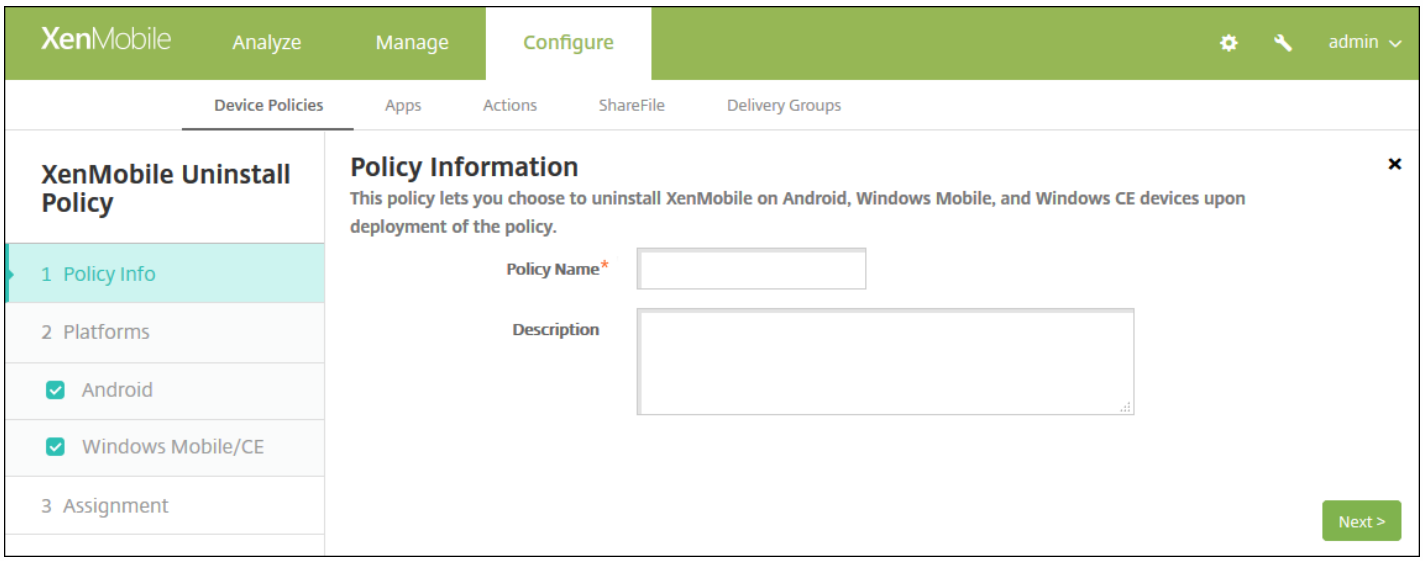
Jul 27, 2016

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.

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 **Agent XenMobile**, cliquez sur **Désinstallation de XenMobile**. La page **Stratégie de désinstallation de XenMobile** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

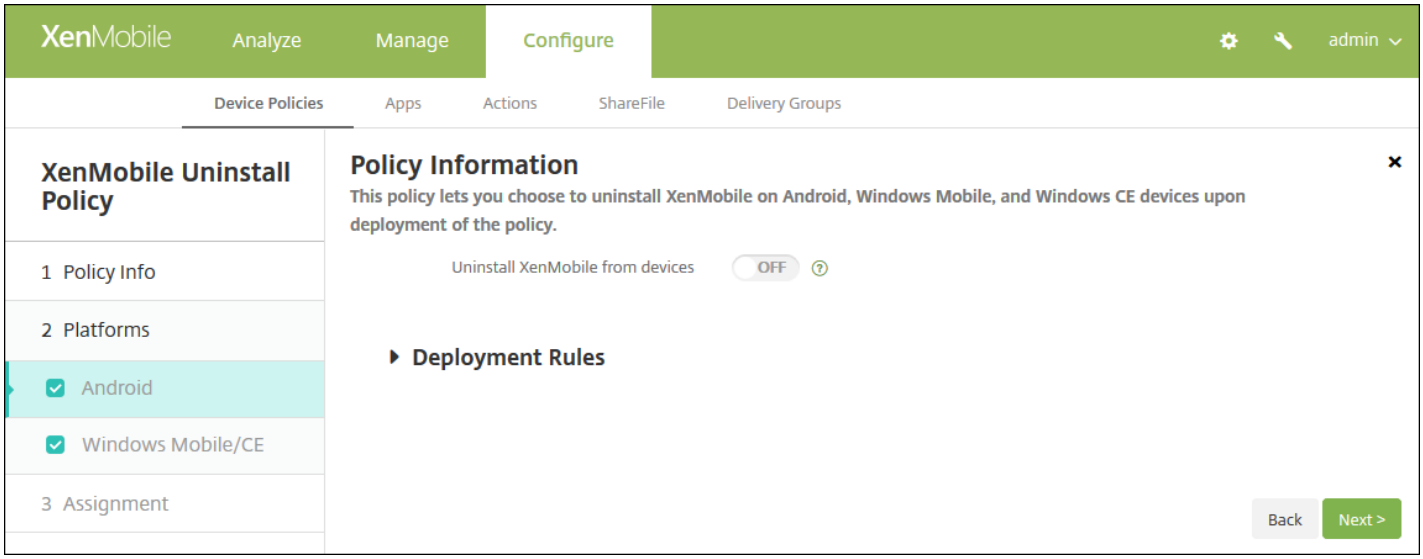
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour Android et Windows Mobile/CE

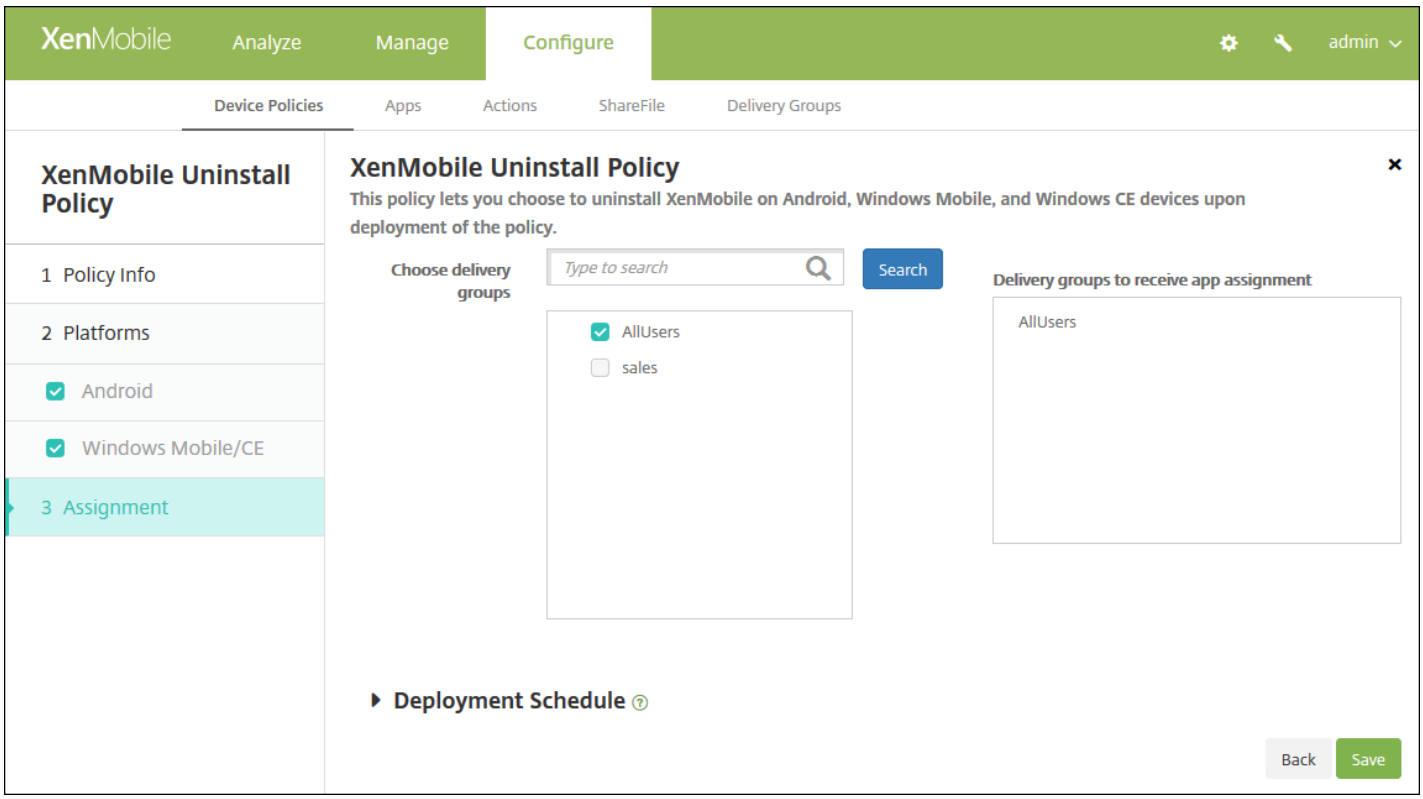


Configurez ce paramètre pour chaque plate-forme que vous sélectionnez :

- **Désinstaller XenMobile des appareils** : sélectionnez cette option pour désinstaller XenMobile de chaque appareil sur lequel vous déployez cette stratégie. La valeur par défaut est **OFF**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie de désinstallation de XenMobile** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou

sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Ajout d'applications à XenMobile

Jul 27, 2016

Vous pouvez ajouter des applications à XenMobile pour en assurer la gestion. Vous ajoutez les applications à la console XenMobile, où vous pouvez organiser les applications par catégorie et les déployer auprès des utilisateurs.

Vous pouvez ajouter les types suivants d'applications à XenMobile :

- **MDX**. Ce sont des applications wrappées avec le MDX Toolkit (et les stratégies associées). Vous déployez des applications MDX que vous avez obtenues depuis des magasins internes et publics. Par exemple : WorxMail.
- **Magasin d'applications public**. Ces applications peuvent être gratuites ou payantes et sont disponibles dans un magasin d'applications public, tel que iTunes ou Google Play. Par exemple : GoToMeeting. Les applications Android for Work sont comprises dans cette catégorie.
- **Web et SaaS**. Ces applications comprennent les applications accessibles à partir d'un réseau interne (applications web) ou sur un réseau public (SaaS). Vous pouvez créer vos propres applications, ou faire votre choix parmi un ensemble de connecteurs d'applications pour l'authentification unique aux applications Web existantes. Par exemple : GoogleApps_SAML.
- **Entreprise**. Ces applications sont des applications natives qui ne sont pas wrappées avec le MDX Toolkit et qui ne contiennent aucune des stratégies associées aux applications MDX.
- **Lien Web**. Il s'agit d'une adresse Web (URL) à un site public ou privé, ou à une application Web qui ne requiert pas d'authentification unique (SSO).

> ## Remarque
>
> Citrix prend en charge l'installation silencieuse d'applications iOS et Samsung Android. Une installation silencieuse signifie que les utilisateurs ne sont pas invités à installer les applications que vous déployez sur l'appareil ; les applications sont installées de manière silencieuse en arrière-plan. Vous devez remplir les conditions suivantes pour pouvoir effectuer une installation silencieuse :
>
> - Pour les applications iOS, l'appareil iOS géré doit être en mode supervisé. Pour de plus amples informations, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.
> - Pour les applications Android, des stratégies Samsung for Enterprise (SAFE) ou KNOX doivent être activées 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.

Fonctionnement des applications mobiles et MDX

XenMobile prend en charge les applications iOS, Mac OS X, Android et Windows, y compris les applications Worx, telles que Worx Home, WorxMail et WorxWeb, ainsi que l'utilisation de stratégies MDX. Grâce à la console XenMobile, vous pouvez charger des applications et les mettre à disposition sur les appareils des utilisateurs. En plus des applications Worx, vous pouvez ajouter les types suivants d'applications :

- Applications que vous développez pour vos utilisateurs.
- Applications dans lesquelles vous souhaitez autoriser ou interdire des fonctionnalités d'appareils à l'aide de stratégies MDX.

Citrix fournit le MDX Toolkit qui wrappe les applications pour iOS, Mac OS X, Android et Windows avec une logique et des

stratégies Citrix. L'outil peut wrapper une application qui a été créée au sein de votre organisation ou une application créée par des tiers de manière sécurisée.

Fonctionnement des applications Web et SaaS

XenMobile est fourni avec un ensemble de connecteurs d'applications constituant des modèles qu'il est possible de configurer en vue de l'authentification unique (SSO) pour des applications Web et Software as a Service (SaaS) et, dans certains cas, pour la création et la gestion de comptes d'utilisateur. XenMobile inclut des connecteurs SAML (Security Assertion Markup Language). Les connecteurs SAML sont prévus pour les applications Web qui prennent en charge le protocole SAML en vue de l'authentification unique et de la gestion des comptes d'utilisateur. XenMobile prend en charge les protocoles SAML 1.1 et SAML 2.0.

Vous pouvez également construire vos propres connecteurs SAML d'entreprise.

Fonctionnement des applications d'entreprise

Vous pouvez créer votre propre connecteur d'application et charger une application Android for Work dans XenMobile. Ce type d'application réside généralement dans votre réseau interne. Les utilisateurs peuvent se connecter aux applications à l'aide de Worx Home. Lorsque vous ajoutez une application d'entreprise, vous créez le connecteur d'application en même temps.

Fonctionnement du magasin d'applications public

Vous pouvez configurer des paramètres afin de récupérer les noms et descriptions des applications depuis l'App Store d'Apple, Google Play et Windows Store. Lorsque vous récupérez les informations d'application dans le magasin, XenMobile remplace le nom et la description existants.

Fonctionnement des liens 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 Worx Store. Lorsque les utilisateurs ouvrent une session avec Worx Home, le lien s'affiche avec la liste des applications et bureaux disponibles.

L'ajout d'une application à l'aide de la console comprend les étapes suivantes :

- Ajout d'informations sur l'application.
- Sélection et configuration de l'application pour chaque plate-forme prise en charge, telle que iOS ou Android.
- Définition d'une méthode d'approbation facultative.
- Définition d'attributions facultatives de groupes de mise à disposition.

1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'affiche.

Remarque : lorsque vous vous connectez à la console XenMobile pour la première fois, le tableau **Applications** est vide ; les seules options disponibles sont **Ajouter** et **Catégorie**.

2. Cliquez sur **Ajouter**, puis suivez les étapes de ces articles qui correspondent au type que vous voulez ajouter :

- Ajout d'une application MDX à XenMobile
- Ajout d'un magasin d'applications public à XenMobile
- Ajout d'une application Web et SaaS à XenMobile
- Ajout d'une application d'entreprise à XenMobile

- Ajout d'un lien Web applicatif à XenMobile

Lorsque vous ajoutez une application, l'application s'affiche dans le tableau sur la page **Applications**, dans laquelle vous pouvez modifier ou catégoriser l'application à tout moment.

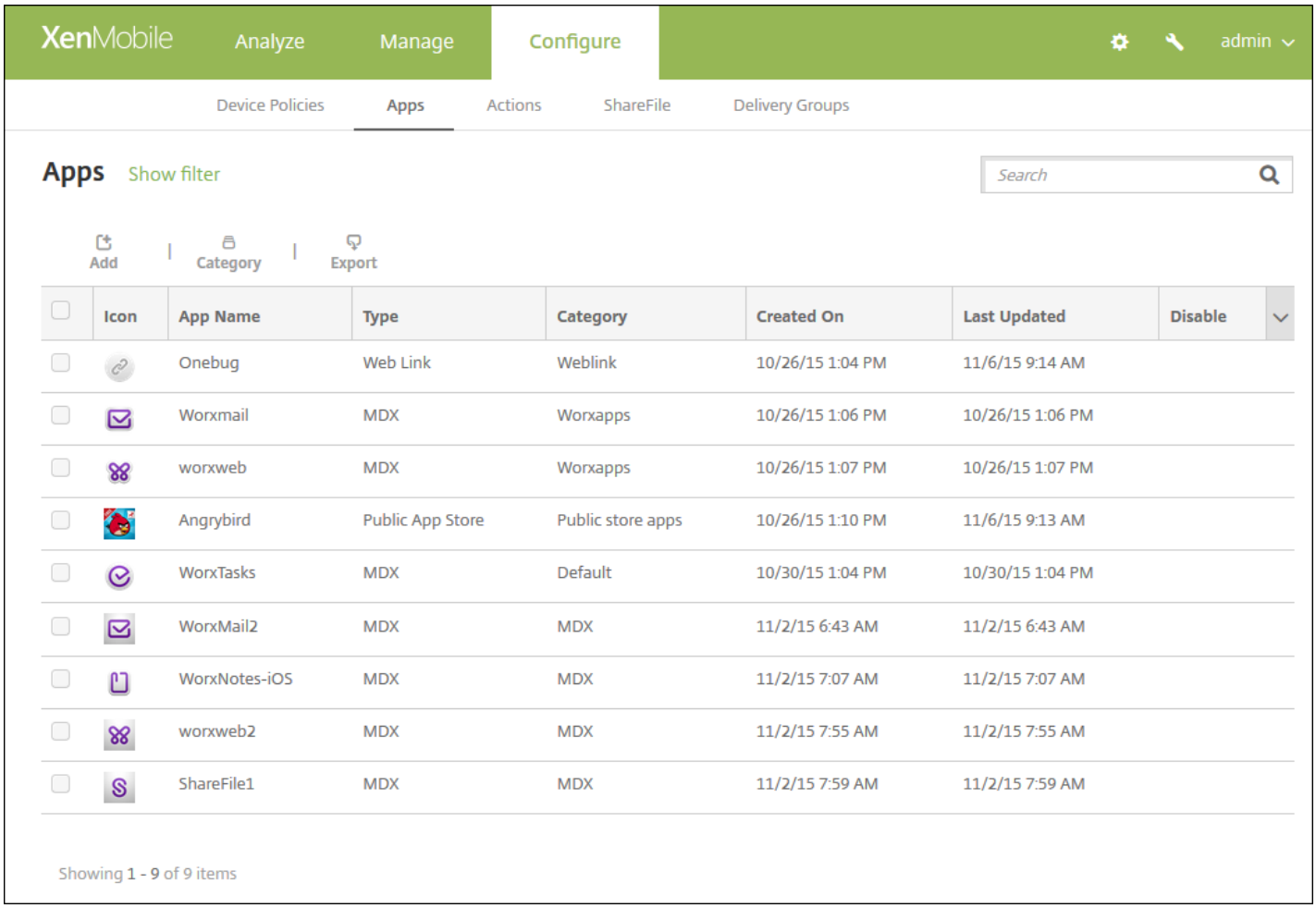
> ## Remarque
>
> Après la mise à niveau vers XenMobile 10.3, lorsque vous mettez à jour dans XenMobile 10.3 les applications mobiles Worx que vous avez configurées dans une version antérieure, les paramètres des applications ne s'affichent plus dans la console XenMobile. Vous devez modifier et configurer à nouveau les paramètres de ces applications. Il est cependant inutile de les réinstaller. Vous ne devez effectuer cette opération qu'une seule fois ; les valeurs seront conservées lors des prochaines mises à jour de l'application ou du serveur.

Ajout d'une application MDX à XenMobile

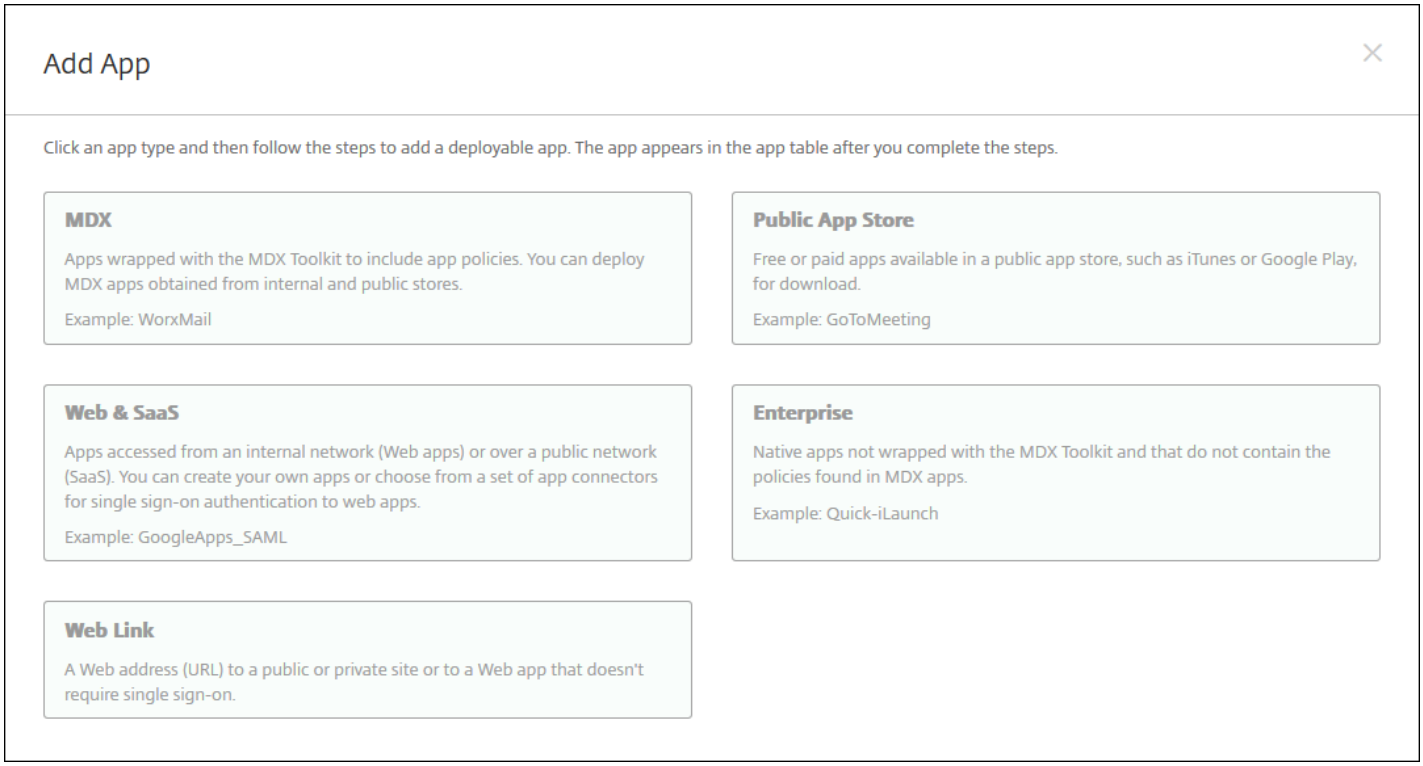
Jul 27, 2016

Lorsque vous recevez une application mobile MDX wrappée pour iOS, Android, ou Windows Phone, vous pouvez charger l'application sur XenMobile. Après le chargement de l'application, vous pouvez configurer les détails de l'application et les paramètres de stratégie. Pour de plus amples informations sur les stratégies applicatives disponibles pour chaque type de plate-forme, consultez la section Synopsis des stratégies MDX pour iOS, Android, et Windows Phone. Des descriptions détaillées des stratégies sont également proposées dans cette section.

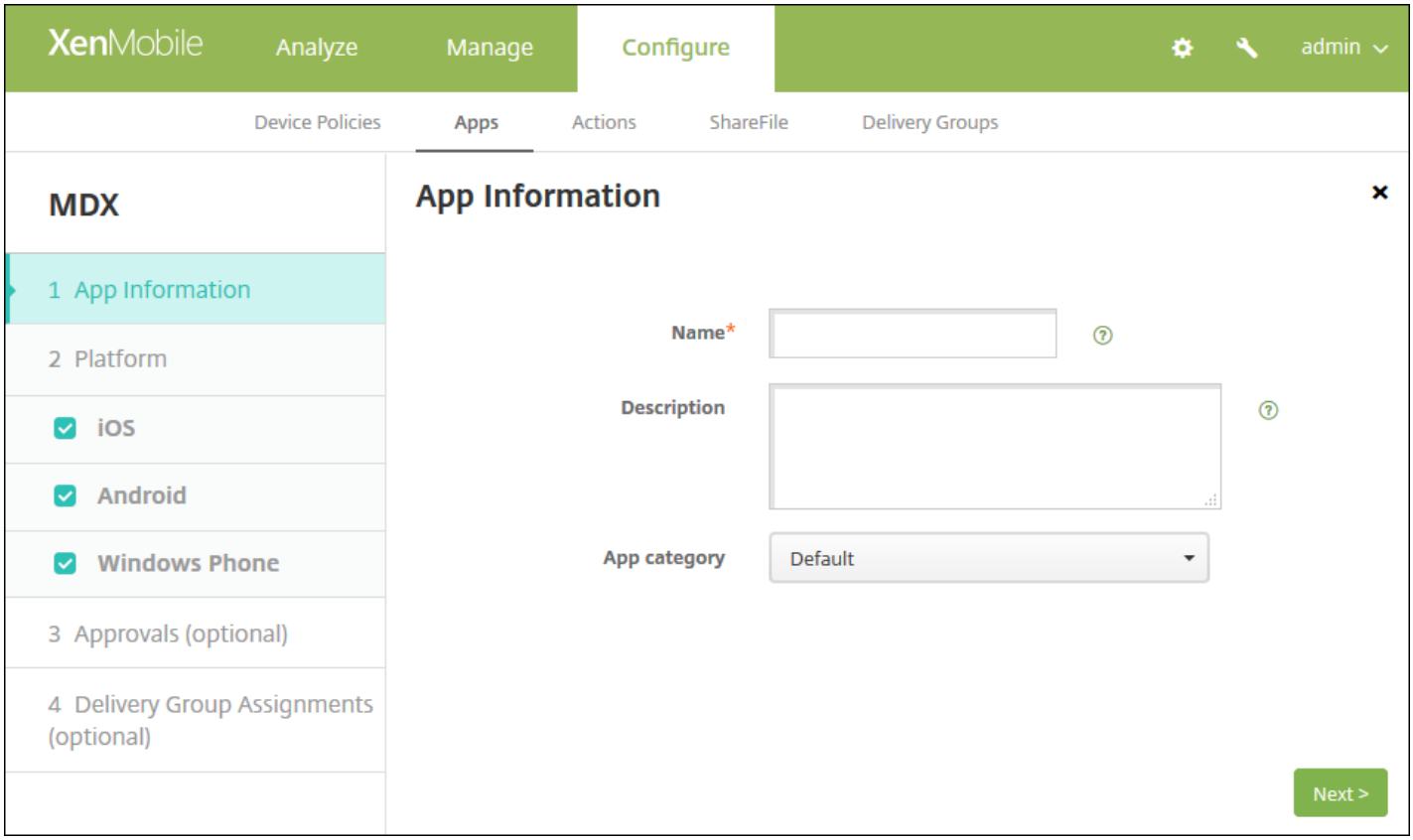
1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'affiche.



2. Cliquez sur **Add**. La boîte de dialogue **Ajouter une application** s'affiche.



3. Cliquez sur **MDX**. La page **Informations sur l'application** s'affiche.



4. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :

- **Nom** : entrez un nom descriptif pour l'application. Il est répertorié 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, consultez la section Création de catégories d'applications dans XenMobile.

5. Cliquez sur **Next**. 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.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 11 pour savoir comment définir les règles de déploiement de cette plate-forme.

7. Sélectionnez un fichier .mdx à charger en cliquant sur le bouton **Charger** et en accédant à l'emplacement du fichier.

- Si vous ajoutez une application VPP B2B iOS, cliquez sur **Votre application est-elle une application VPP B2B ?** et, dans la liste, cliquez sur le compte VPP B2B à utiliser.

8. Cliquez sur **Next**. La page sur les détails de l'application s'affiche.

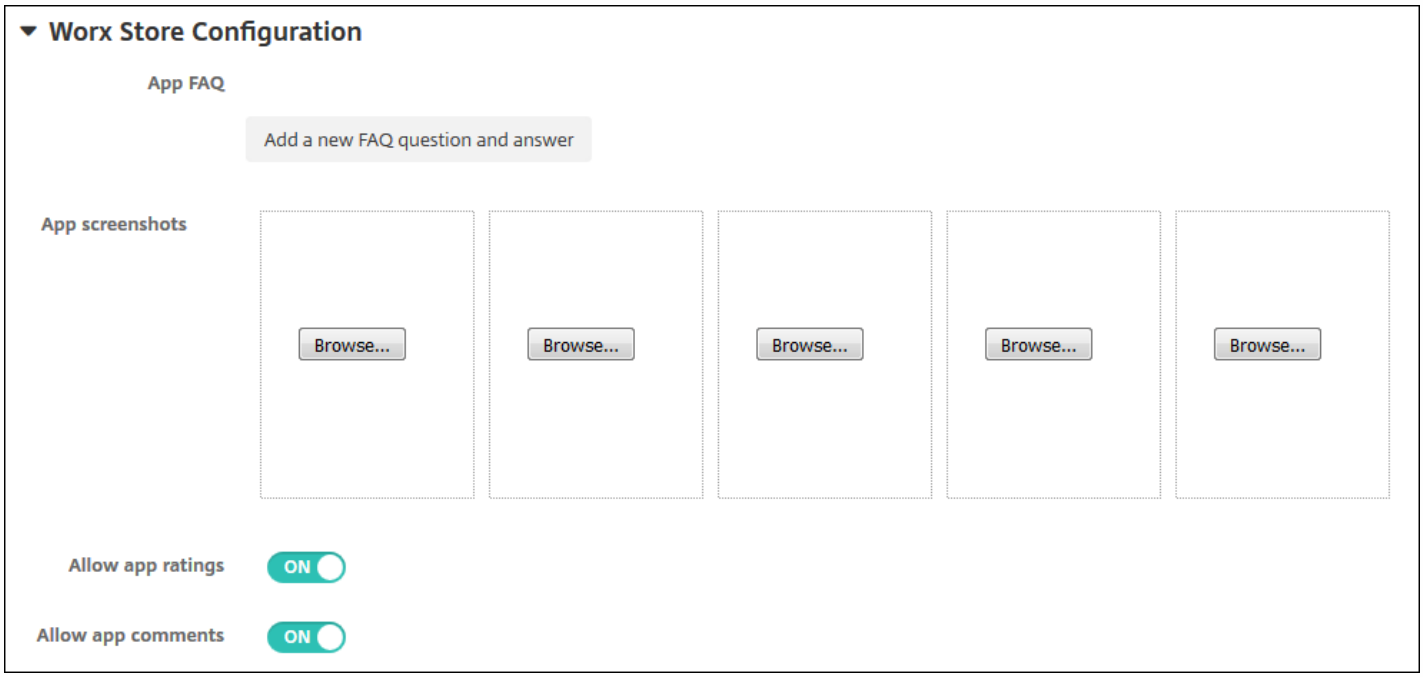
9. Configurez les paramètres suivants :

- **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.
- **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**.
- **Empêcher la sauvegarde des données d'application** : sélectionnez cette option si vous souhaitez empêcher les utilisateurs de sauvegarder les données de l'application. La valeur par défaut est **ON**.
- **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 **ON**. Disponible dans iOS 9.0 et version ultérieure.

10. 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, la configuration réseau requise, l'accès divers, le cryptage, l'interaction de l'application, les restrictions applicatives, l'accès au réseau d'entreprise, les journaux d'applications et le géofencing. Dans la console, les stratégies ont une info-bulle qui décrit chacune d'entre elles. Pour de plus amples informations sur les stratégies applicatives pour les applications MDX, telles qu'un tableau répertoriant les stratégies s'appliquant à chaque type de plate-forme, consultez la section Synopsis des stratégies MDX pour iOS, Android et Windows Phone.

11. Configurez les règles de déploiement.

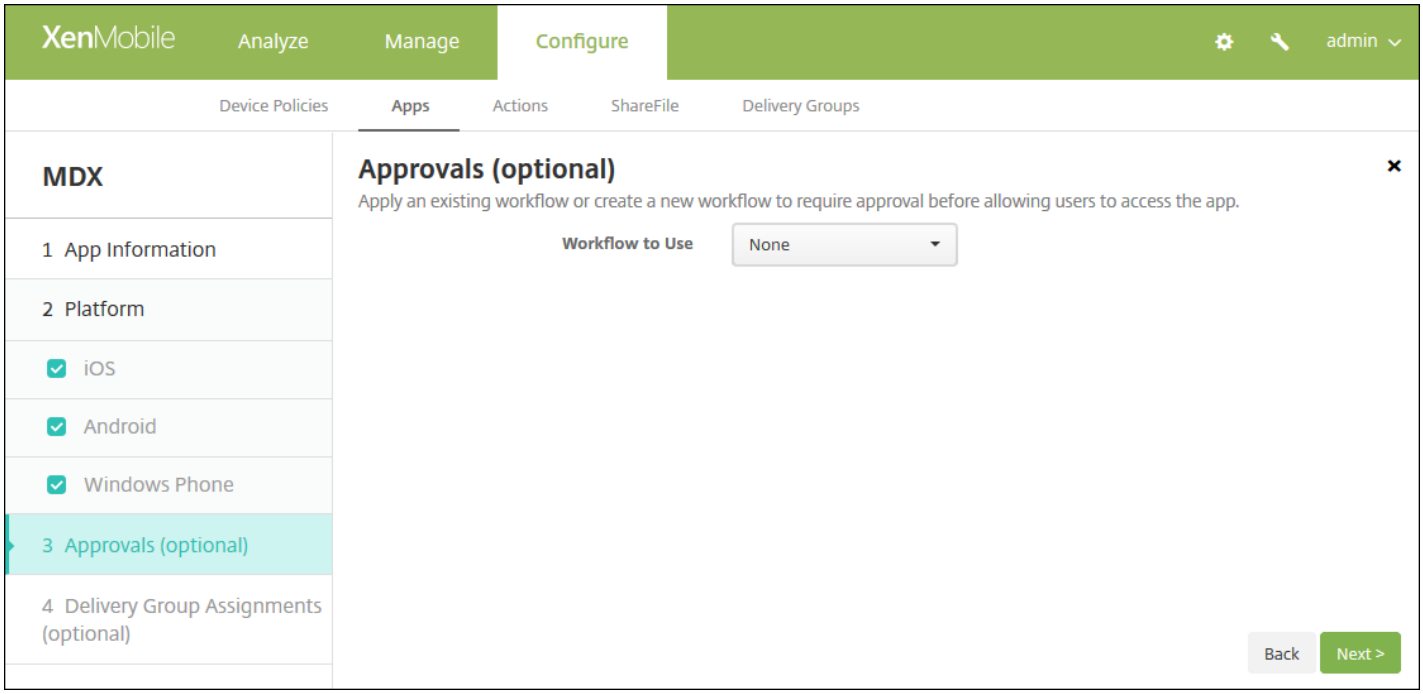
12. Développez **Configuration de Worx Store**.



Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le Worx Store. 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 Worx Store. 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 **ON**.
  - **Autoriser commentaires sur les applications** : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée. La valeur par défaut est **ON**.

13. Cliquez sur **Suivant**. La page **Approbations** s'affiche.



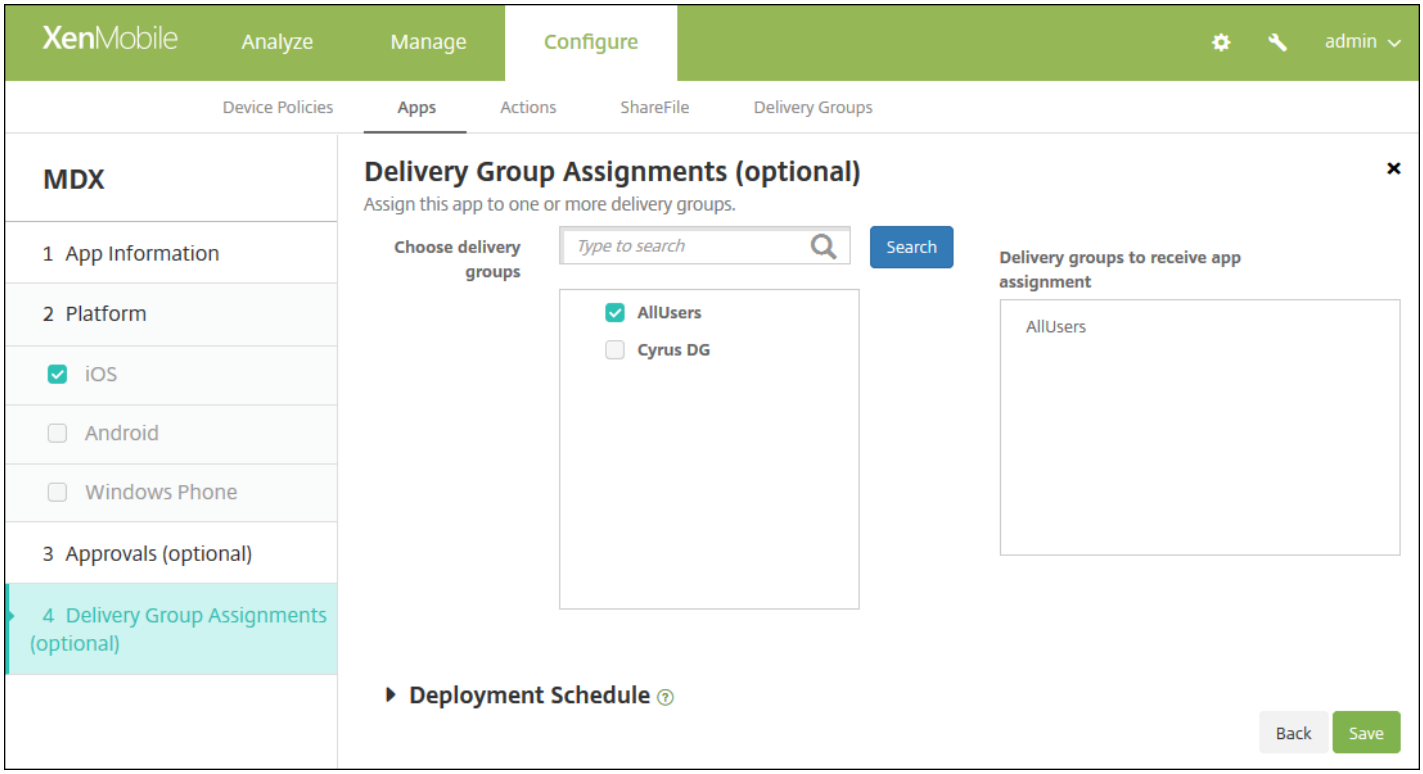
Vous utilisez des workflows lorsque vous avez besoin d'une approbation pour créer des comptes d'utilisateur. S'il n'est pas nécessaire de configurer des workflows d'approbation, vous pouvez passer à l'étape 15.

Configurez ce paramètre si vous devez 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 **Aucune**.
- 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 de la personne s'affiche dans le champ, sélectionnez la case à cocher en regard de son nom. Le nom et l'adresse e-mail de cette personne 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.

14. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.



15. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer l'application. 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 **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

17. Cliquez sur **Enregistrer**.

Création de catégories d'applications dans XenMobile

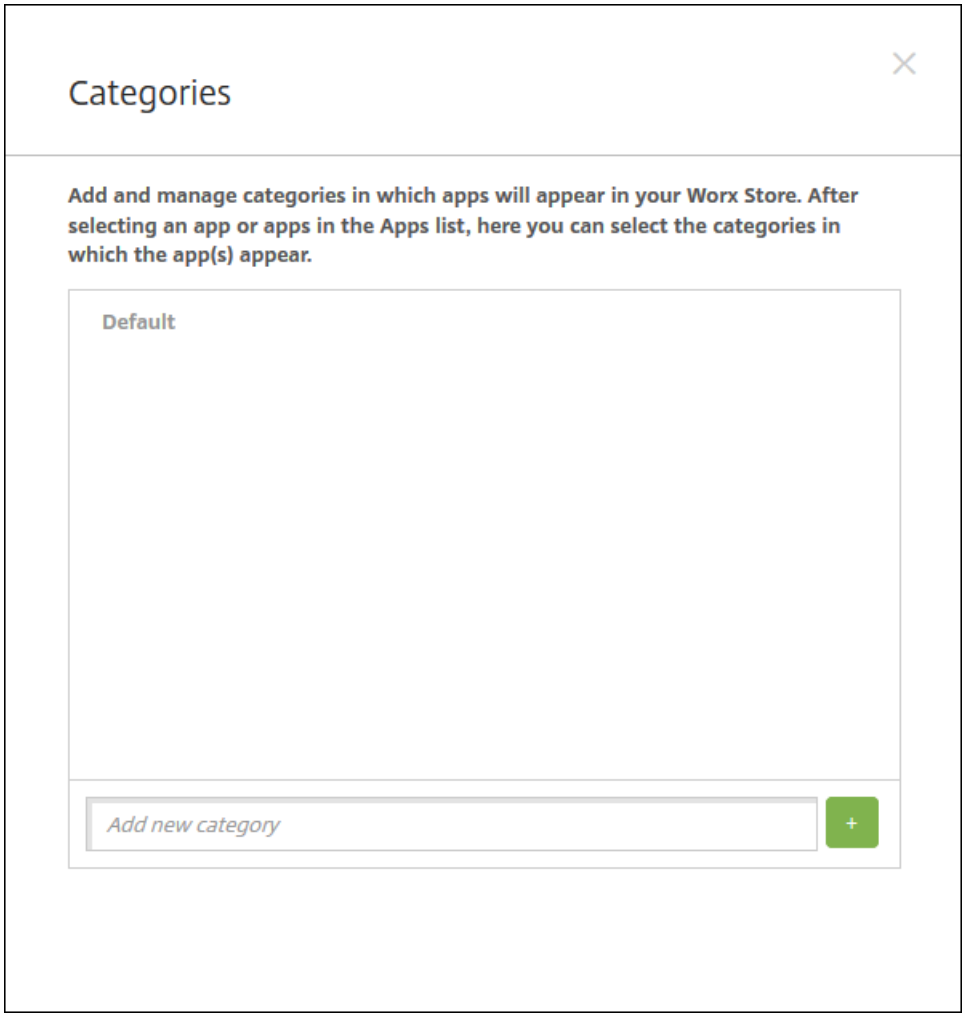
Jul 27, 2016

Lorsque les utilisateurs se connectent à Worx Home, ils obtiennent une liste des applications, des liens Web et des magasins que vous avez ajoutés et configurés dans XenMobile. Vous pouvez utiliser les catégories d'applications pour permettre aux utilisateurs d'accéder uniquement aux applications, liens Web ou magasins auxquels vous souhaitez autoriser l'accès. 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.

Vous configurez les catégories sur la page **Applications** dans la console XenMobile. Ensuite, 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 que vous avez configurées.

1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'affiche.

2. Cliquez sur **Catégorie**. La boîte de dialogue **Catégories** s'affiche.

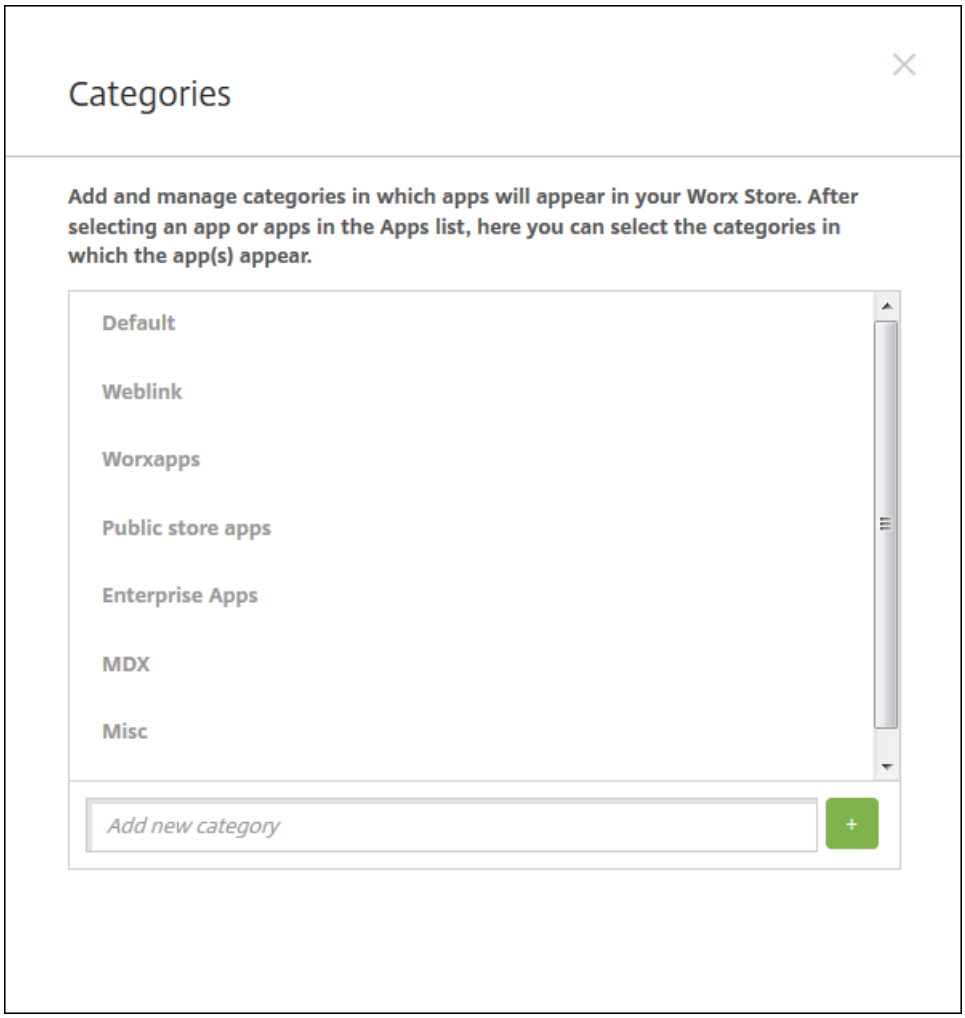


3. Pour chaque catégorie que vous voulez ajouter, procédez comme suit :

- 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**.



4. Lorsque vous avez terminé d'ajouter des catégories, fermez la boîte de dialogue **Catégories**.

5. Sur la page **Applications**, vous pouvez placer une application existante dans une nouvelle catégorie.

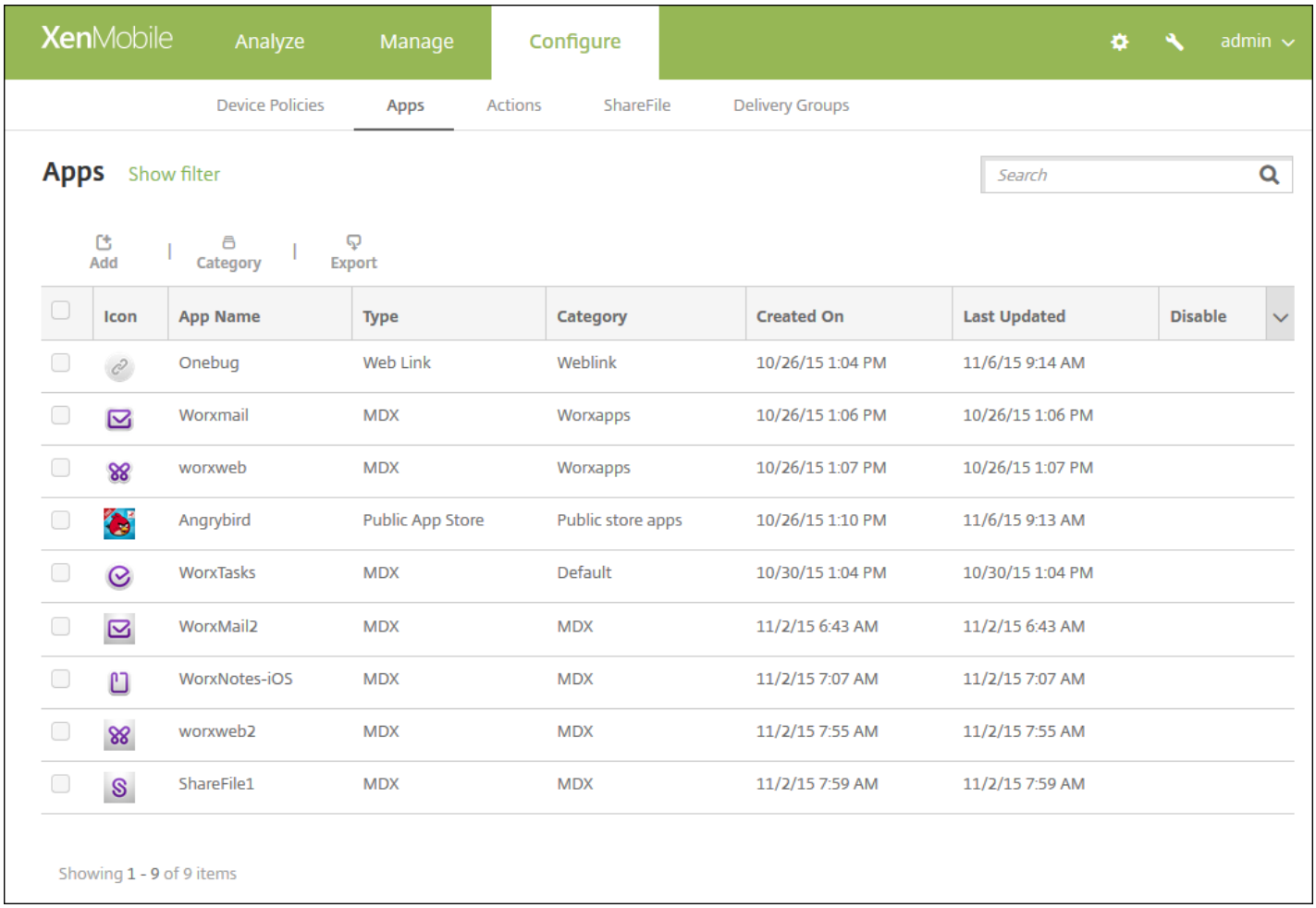
- Sélectionnez l'application que vous souhaitez classer.
- Cliquez sur **Modifier**. La page **Informations sur l'application** s'affiche.
- Dans la liste **Catégorie d'application**, appliquez la nouvelle catégorie en sélectionnant la case à cocher appropriée. Désélectionnez les cases à cocher pour 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**.

Ajout d'un magasin d'applications public à XenMobile

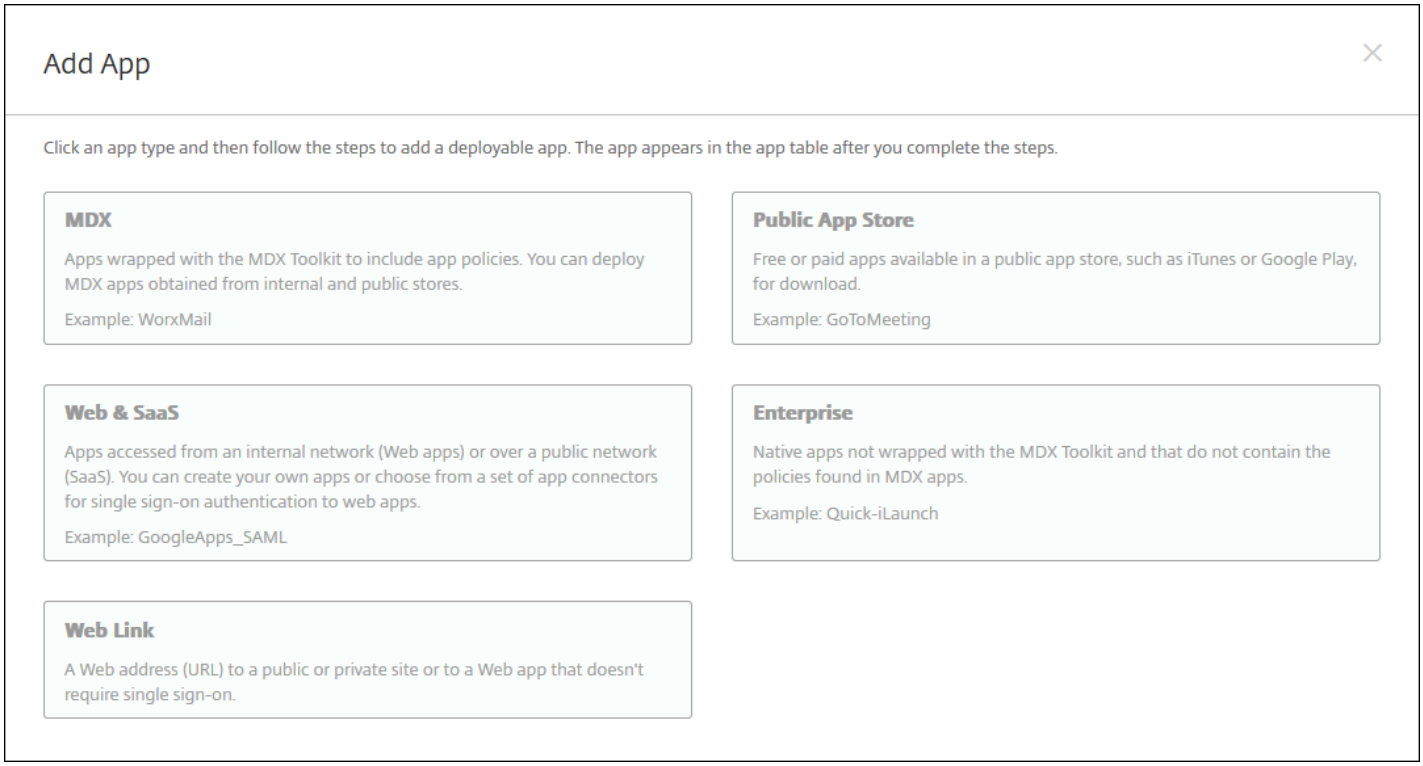
Oct 17, 2016

Vous pouvez ajouter des applications gratuites ou payantes à XenMobile qui sont disponibles dans un magasin d'applications public, tel que iTunes où GooglePlay. Par exemple : GoToMeeting. Également, lorsque vous ajoutez une application payante provenant d'un magasin d'applications public pour un Android for Work, vous pouvez vérifier l'état de la licence d'achat groupé : le nombre total de licences disponibles, ainsi que l'adresse e-mail de chaque utilisateur qui consomme les licences. Le plan Achat groupé pour Android for Work simplifie la recherche, l'achat et la distribution d'applications et d'autres données en bloc pour une organisation.

1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'affiche.



2. Cliquez sur **Add**. La boîte de dialogue **Ajouter une application** s'affiche.



3. Cliquez sur **Magasin d'applications public**. La page **Informations sur l'application** s'affiche.

4. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :

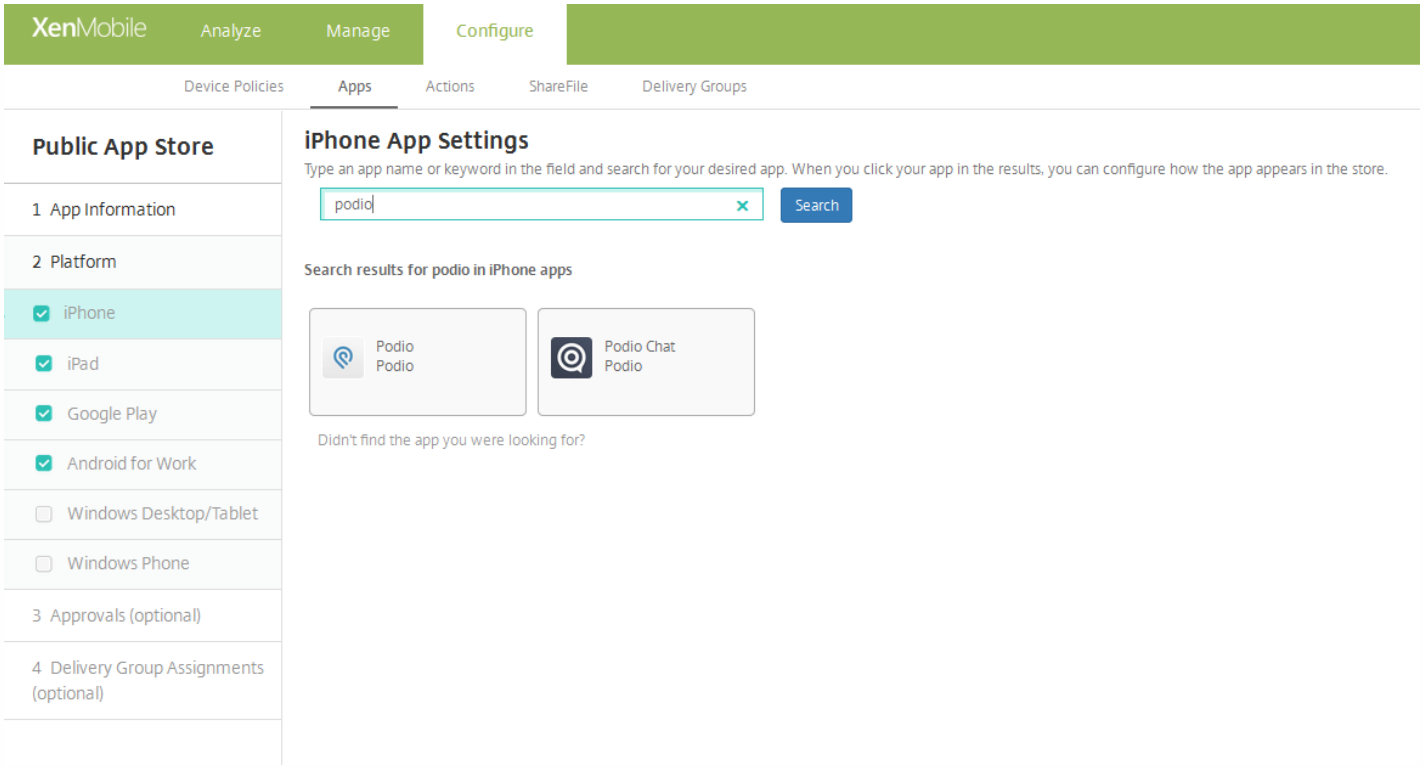
- **Nom** : entrez un nom descriptif pour l'application. Il est répertorié sous Nom de l'application dans le tableau Applications.
- **Description** : entrez une description pour l'application (facultatif).
- **Catégorie d'application** : si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section Création de catégories d'applications dans XenMobile.

5. Cliquez sur **Next**. La page **Plates-formes d'applications** s'affiche.

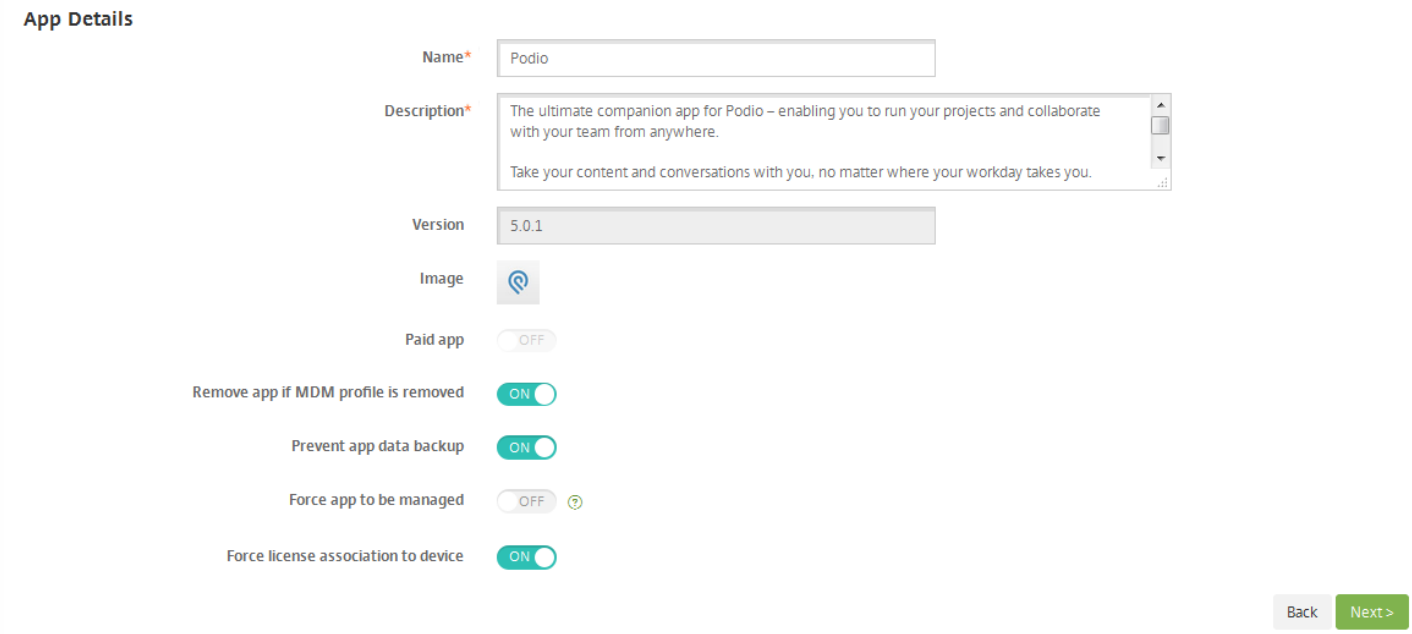
6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 10 pour savoir comment définir les règles de déploiement de cette plate-forme.

7. Sélectionnez une application à ajouter en tapant le nom de l'application dans la zone de recherche et en cliquant sur **Rechercher**. Les applications correspondant aux critères de recherche s'affichent. La figure suivante illustre le résultat de la recherche pour *podio*.



8. Cliquez sur chaque application que vous souhaitez ajouter. Les champs **Détails sur l'application** sont pré-remplis avec les informations relatives à l'application choisie (y compris le nom, la description, le numéro de version et l'image).



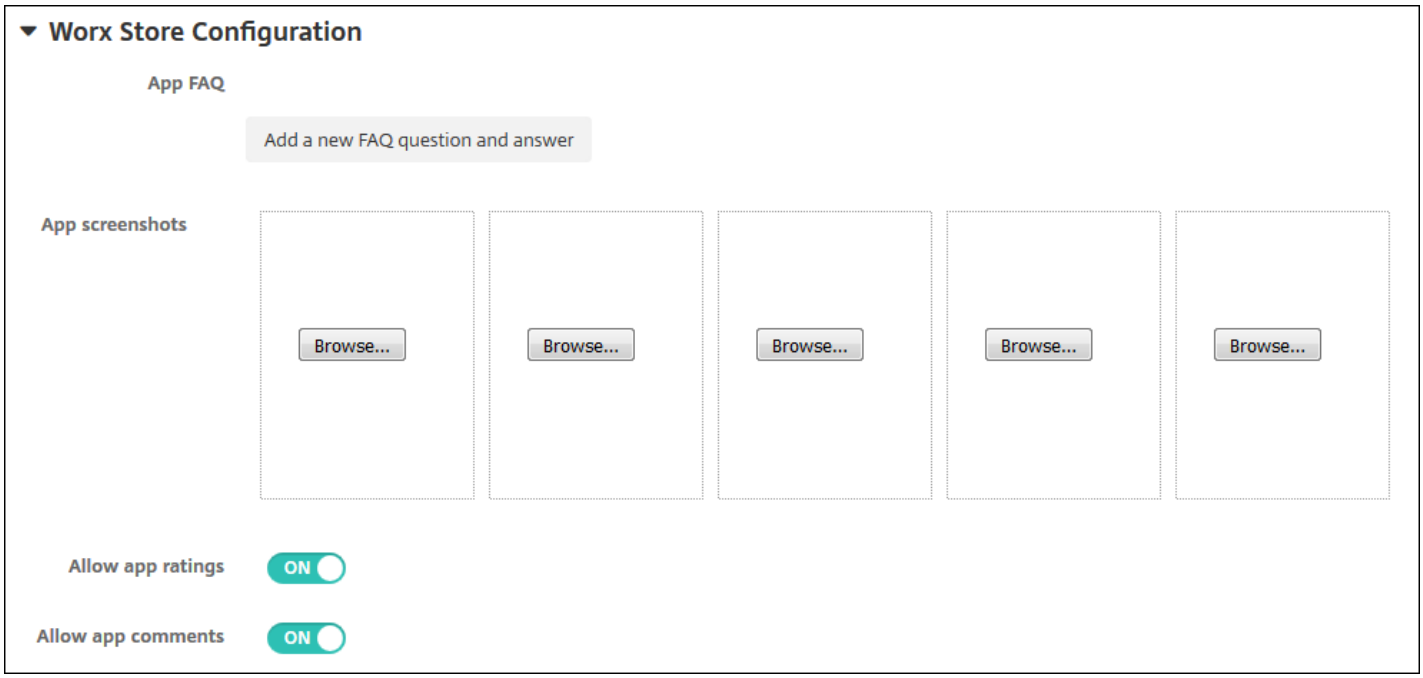
9. Configurez les paramètres suivants :

- 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 **ON**.
- **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**.
- **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 **OFF**. Disponible dans iOS 9.0 et version ultérieure.
- **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.

10. Configurez les règles de déploiement.

11. Développez **Configuration de Worx Store**.

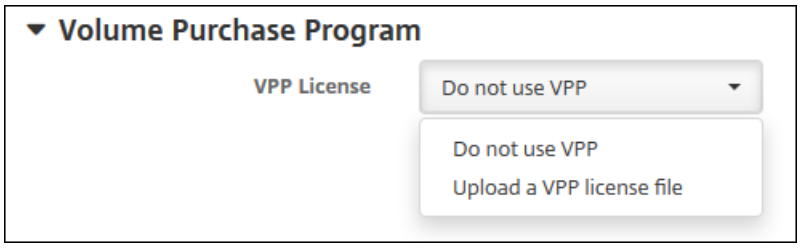


Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le Worx Store. Vous pouvez également indiquer si les utilisateurs peuvent évaluer ou ajouter des commentaires sur l'application.

- 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 Worx Store. 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 ON.
  - **Autoriser commentaires sur les applications** : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée.

12. Développez **Programme d'achat en volume** ou dans le cas d'Android for Work, développez **Achat groupé**.

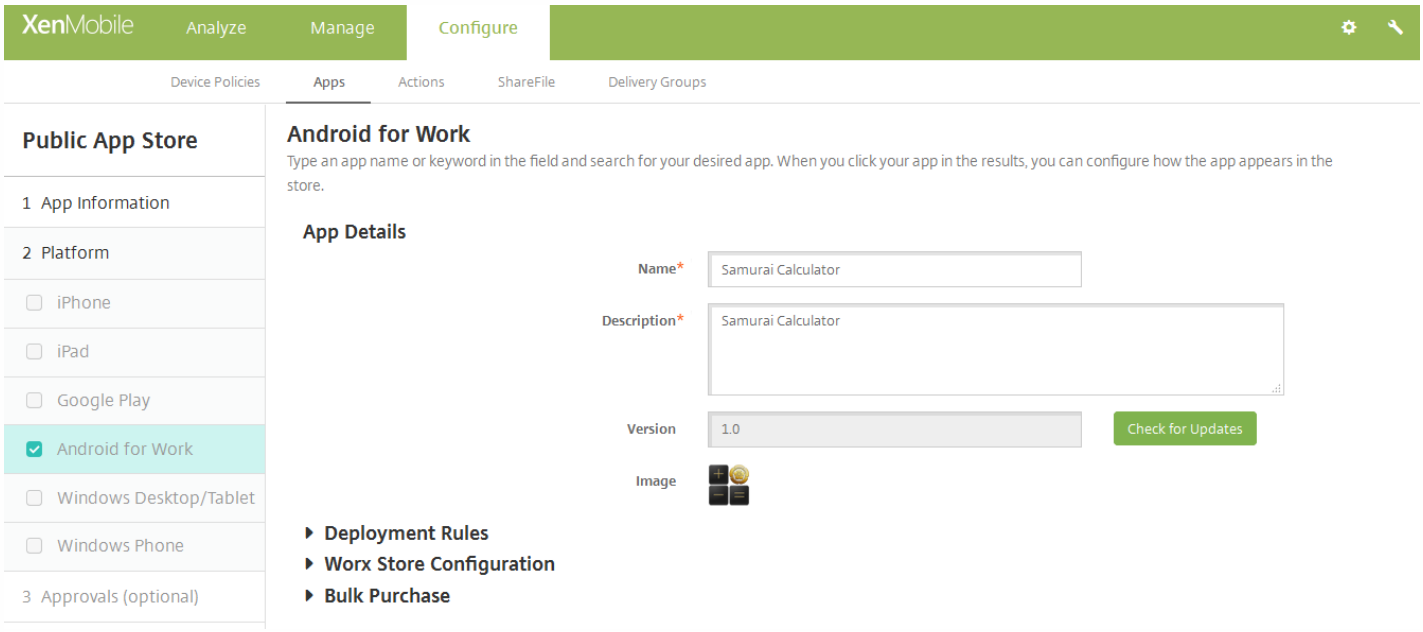
Pour le Programme d'achat en volume, suivez les étapes suivantes.



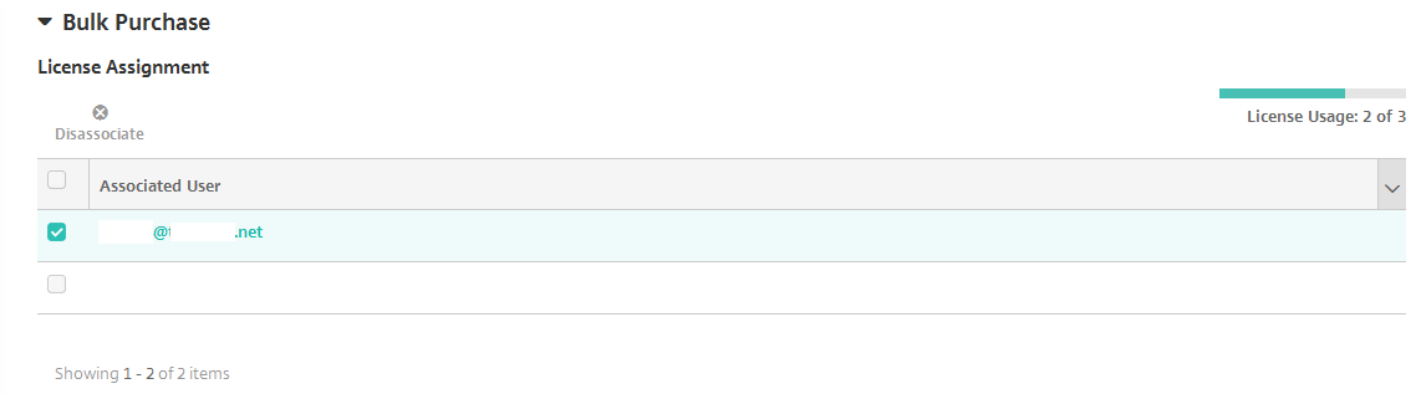
a. 9. Dans la liste **Licences VPP**, cliquez sur **Charger un fichier de licences VPP** si vous voulez autoriser XenMobile à appliquer une licence VPP pour l'application.

b. Dans la boîte de dialogue qui s'affiche, importez la licence.

Pour les achats groupés Android for Work, développez la section **Achat groupé**.



Le tableau Attribution de licences affiche le nombre de licences actuellement en cours d'utilisation pour l'application par rapport au nombre total disponible. 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.



13. 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. S'il n'est pas nécessaire de configurer des workflows d'approbation, vous pouvez passer à l'étape suivante.

Configurez ce paramètre si vous devez 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 **Aucune**.
- 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 de la personne s'affiche dans le champ, sélectionnez la case à cocher en regard de son nom. Le nom et l'adresse e-mail de cette personne 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.

14. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.

15. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer l'application. 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 **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

17. Cliquez sur **Enregistrer**.

Ajout d'une application Web et SaaS à XenMobile

Jul 27, 2016

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 Liste des types de connecteur d'applications. Vous pouvez également créer votre propre connecteur dans XenMobile.

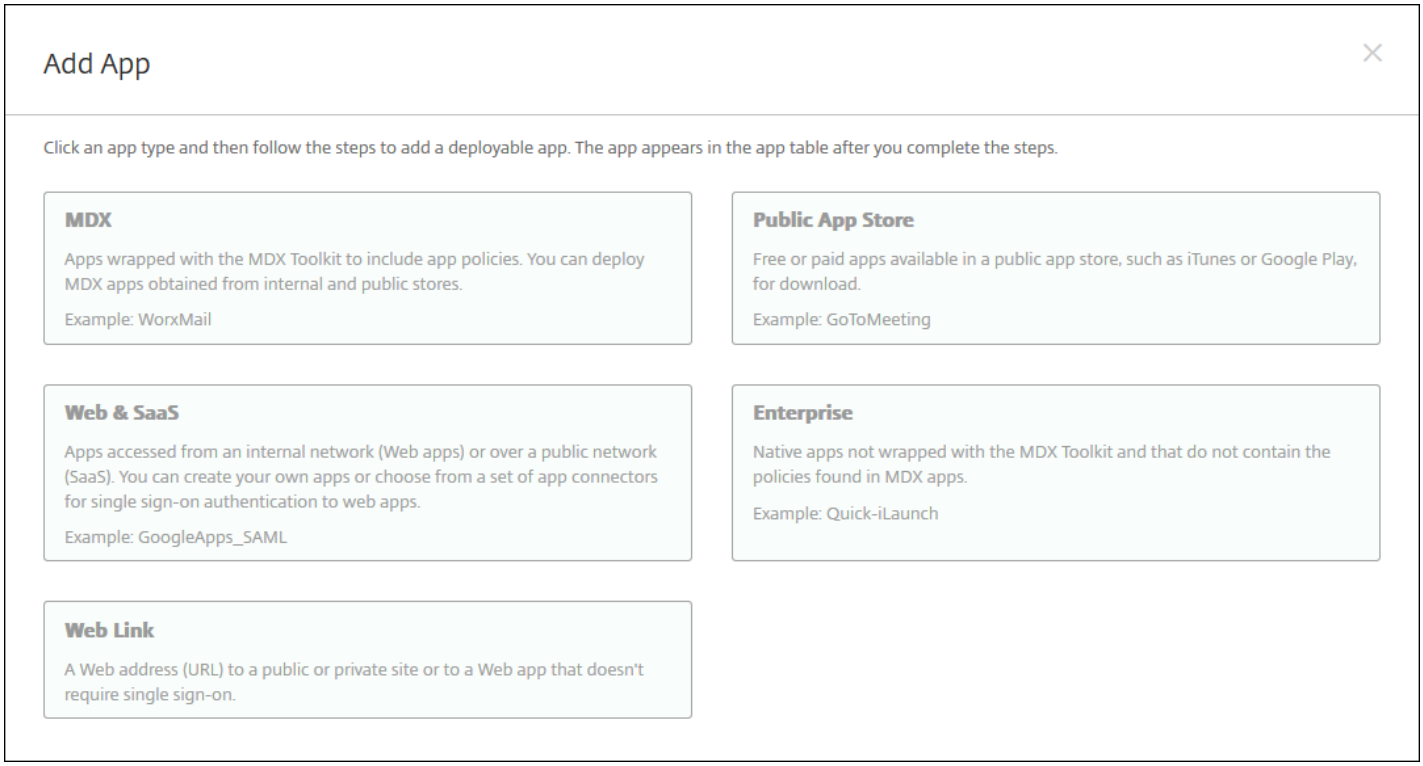
Pour configurer un connecteur, spécifiez les paramètres suivants :

- Noms différents (facultatif). Utilisez tout connecteur affiché dans la console. Le connecteur de zone n'est plus pris en charge.
- Description de l'application.
- Adresse Web en utilisant le nom de domaine complet (FQDN). Par exemple, si vous voulez ajouter LinkedIn à votre liste d'applications, vous accédez à http://www.linkedin.com, puis vous cliquez sur Sign in (Se connecter). Lorsque la page d'ouverture de session s'affiche, vous utilisez l'adresse Web https://www.linkedin.com lors de la configuration de l'application.
- Emplacement de l'application (Internet où votre réseau interne).
- Informations d'identification pour l'authentification unique. Les utilisateurs peuvent utiliser les informations d'identification de l'application.
- Catégorie à laquelle l'application appartient. Les catégories vous permettent d'organiser les applications dans Worx Home.
- Stratégies d'application pour chaque application que vous configurez dans XenMobile.
- Paramètres d'approbation du workflow pour toutes les applications. Spécifiez les personnes qui peuvent approuver le groupe de mise à disposition d'utilisateurs auquel vous voulez attribuer l'application.

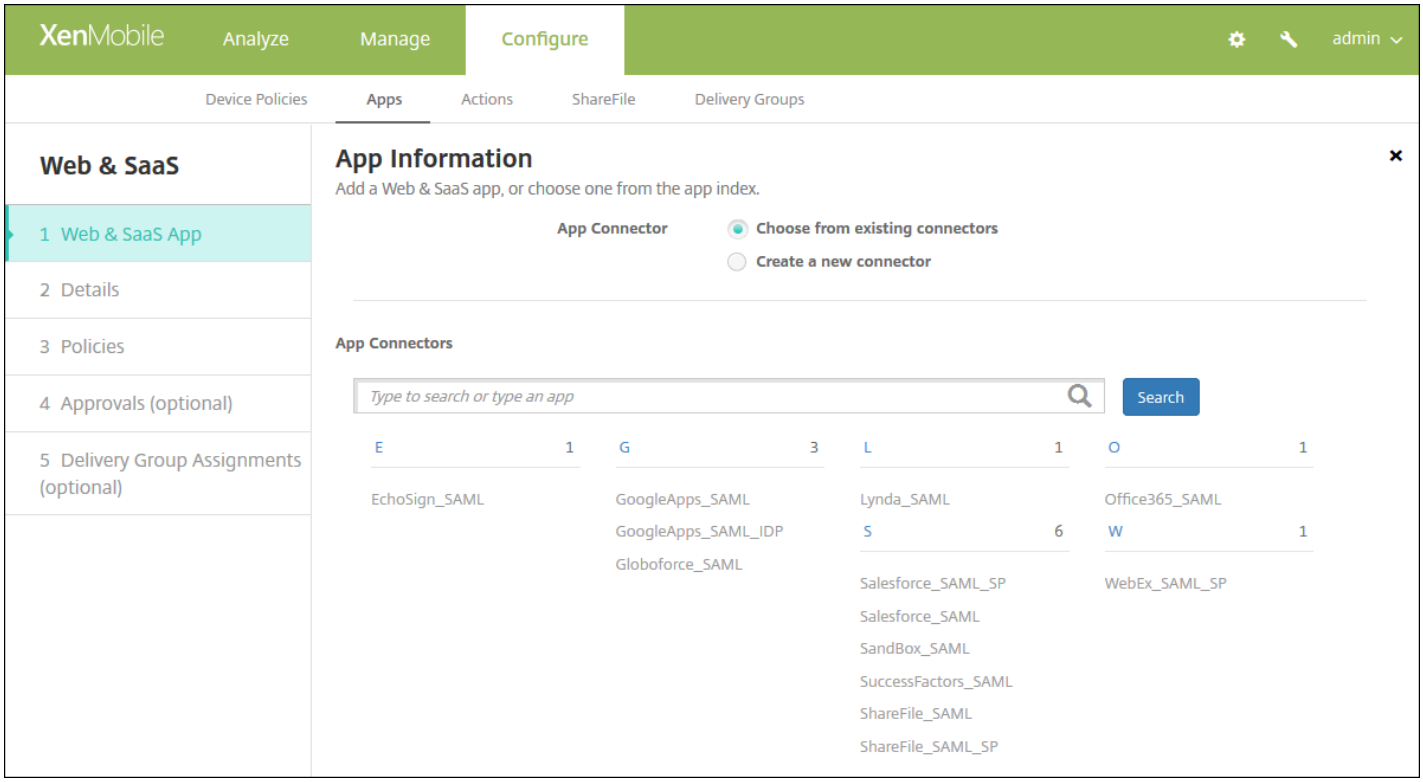
Si une application est uniquement disponible en authentification unique, enregistrez les paramètres lorsque vous terminez la configuration des paramètres précédents ; l'application s'affiche alors dans l'onglet **Applications** de la console XenMobile.

1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'ouvre.

2. Cliquez sur **Add**. La boîte de dialogue **Ajouter une application** s'affiche.



3. Cliquez sur **Web et SaaS**. La page **Informations sur l'application** s'affiche.



4. Configurez les paramètres suivants :

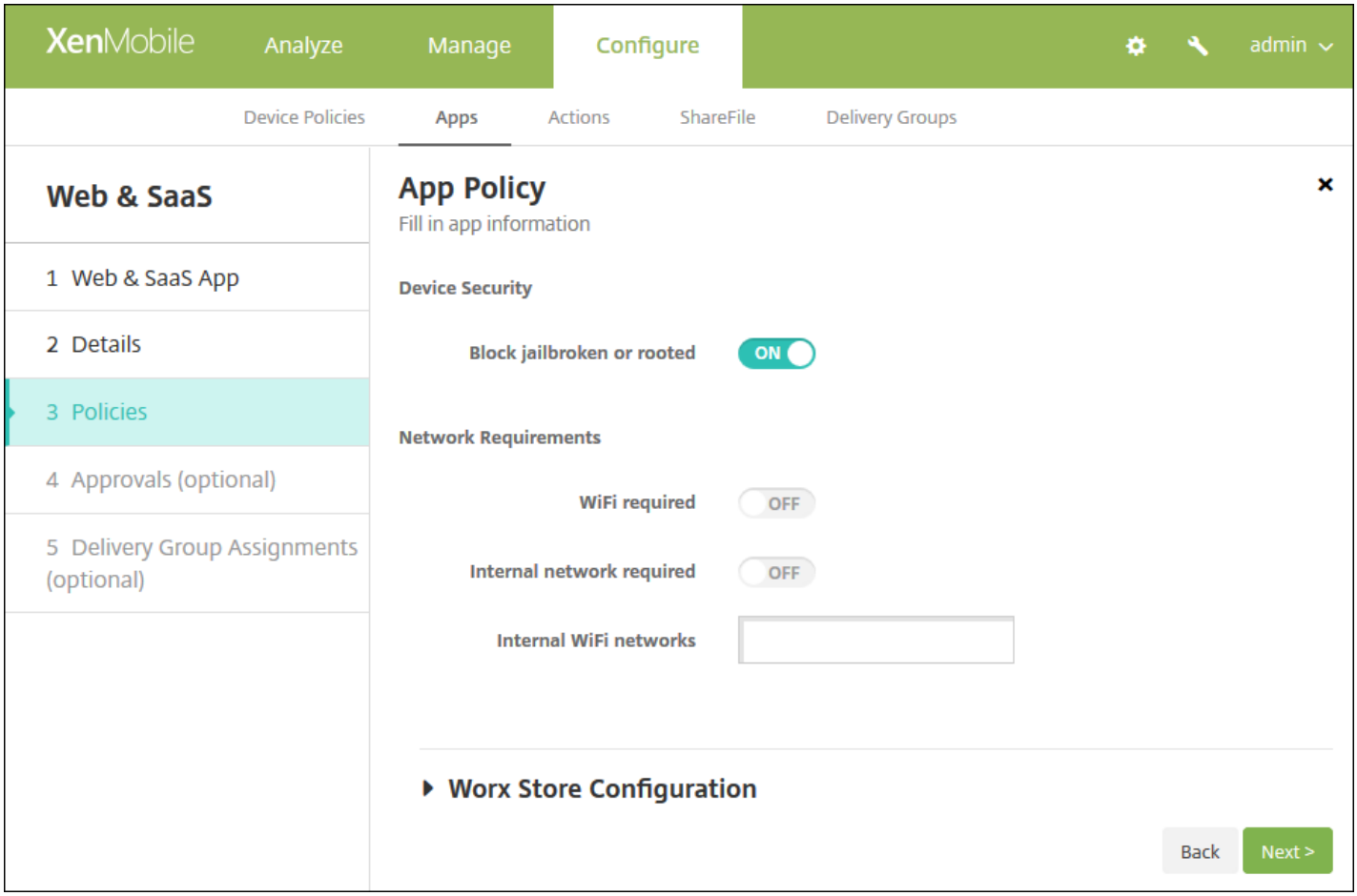
- **Connecteur d'application** : cliquez sur **Choisir parmi les connecteurs existants** ou **Créer un nouveau connecteur**.

La valeur par défaut est **Choisir parmi les connecteurs existants**.

- Si vous cliquez sur **Créer un nouveau connecteur**, des champs s'affichent pour vous permettre de définir le nouveau connecteur.
  - 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. Ce champ est obligatoire.
    - **Version SAML** : sélectionnez 1.1 ou 2.0. La valeur par défaut est de **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 **Email Address**.
    - **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.
      - Si vous souhaitez télécharger votre propre image, sélectionnez-la en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier. Le fichier doit être un fichier .PNG ; vous ne pouvez pas charger une image GIF ou JPEG. Lorsque vous ajoutez un graphique personnalisé, vous ne pouvez pas le modifier ultérieurement.
  - Cliquez sur **Ajouter**. La page **Détails** s'affiche.
- Si vous cliquez sur **Choisir parmi les connecteurs existants** ou sur **Ajouter** après la création d'un nouveau connecteur, la page **Détails** s'affiche.
- 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 NetScaler Gateway. En réglant cette option sur **ON**, le mot-clé VPN est ajouté à l'application et permet aux utilisateurs de se connecter via NetScaler Gateway. La valeur par défaut est **OFF**.
  - **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 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**. Les options possibles sont les suivantes :
        - Désactiver le compte

        - Conserver le compte
        - Supprimer 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 de **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 de **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 **OFF**. Si vous n'activez pas ce champ, lorsque les mots de passe des utilisateurs expirent, ils ne peuvent plus ouvrir l'application.

5. Cliquez sur **Next**. La page **Stratégie d'application** s'affiche.

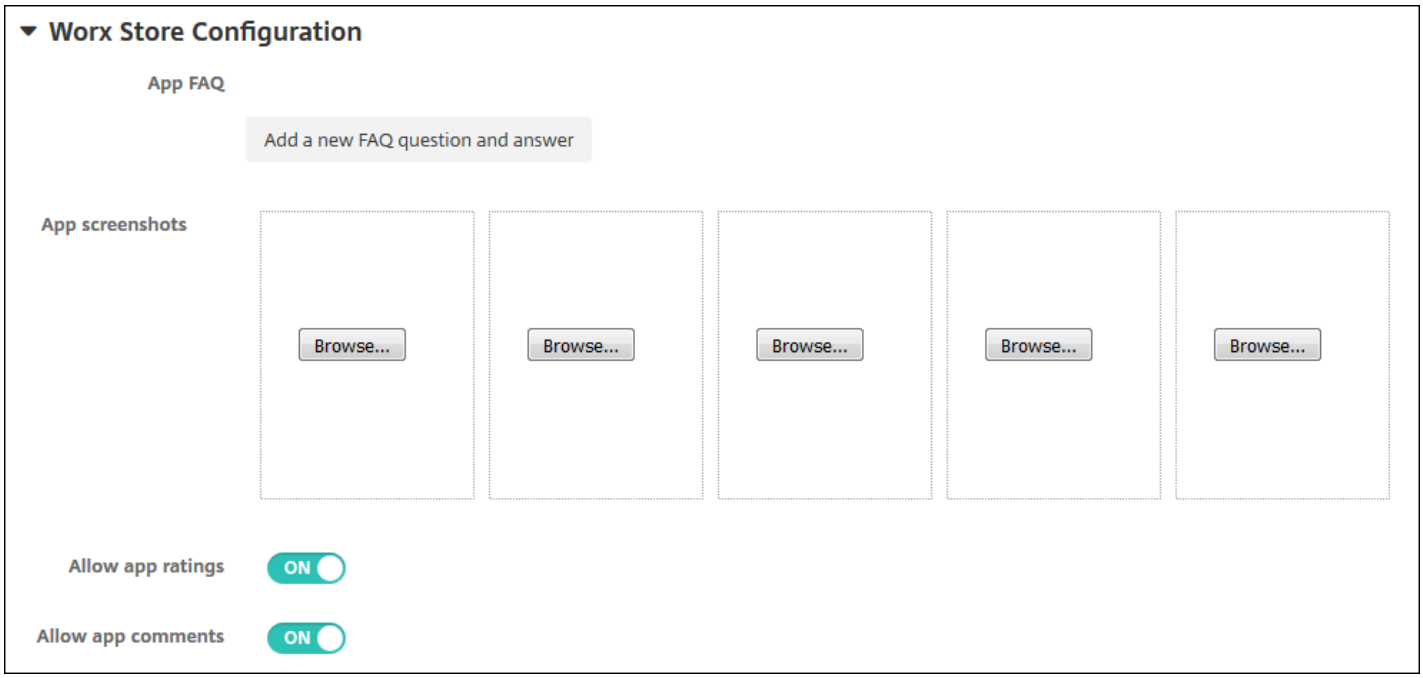


- Pour configurer ces paramètres :
    - **Sécurité de l'appareil**

- **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 **ON**.

- **Configuration réseau requise**
  - **Wi-Fi requis** : sélectionnez cette option pour spécifier qu'une connexion WiFi est requise pour exécuter l'application. La valeur par défaut est **OFF**.
  - **Réseau interne requis** : sélectionnez cette option si un réseau interne est requis pour exécuter l'application. La valeur par défaut est **OFF**.
  - **Réseaux Wi-Fi internes**: si vous avez activé **Wi-Fi requis**, saisissez les réseaux Wi-Fi internes à utiliser.

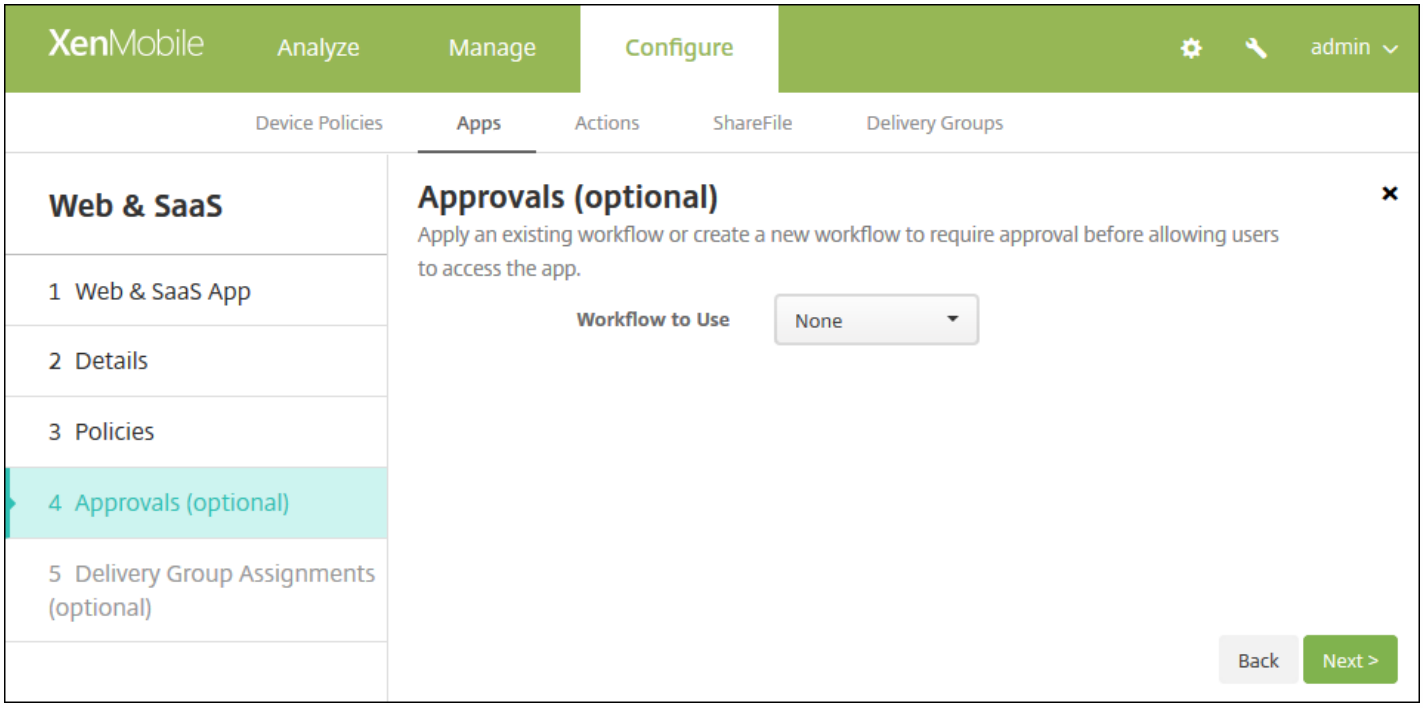
6. Développez **Configuration de Worx Store**.



Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le Worx Store. 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 Worx Store. 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 **ON**.
  - **Autoriser commentaires sur les applications** : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée. La valeur par défaut est **ON**.

7. Cliquez sur **Suivant**. La page **Approbations** s'affiche.



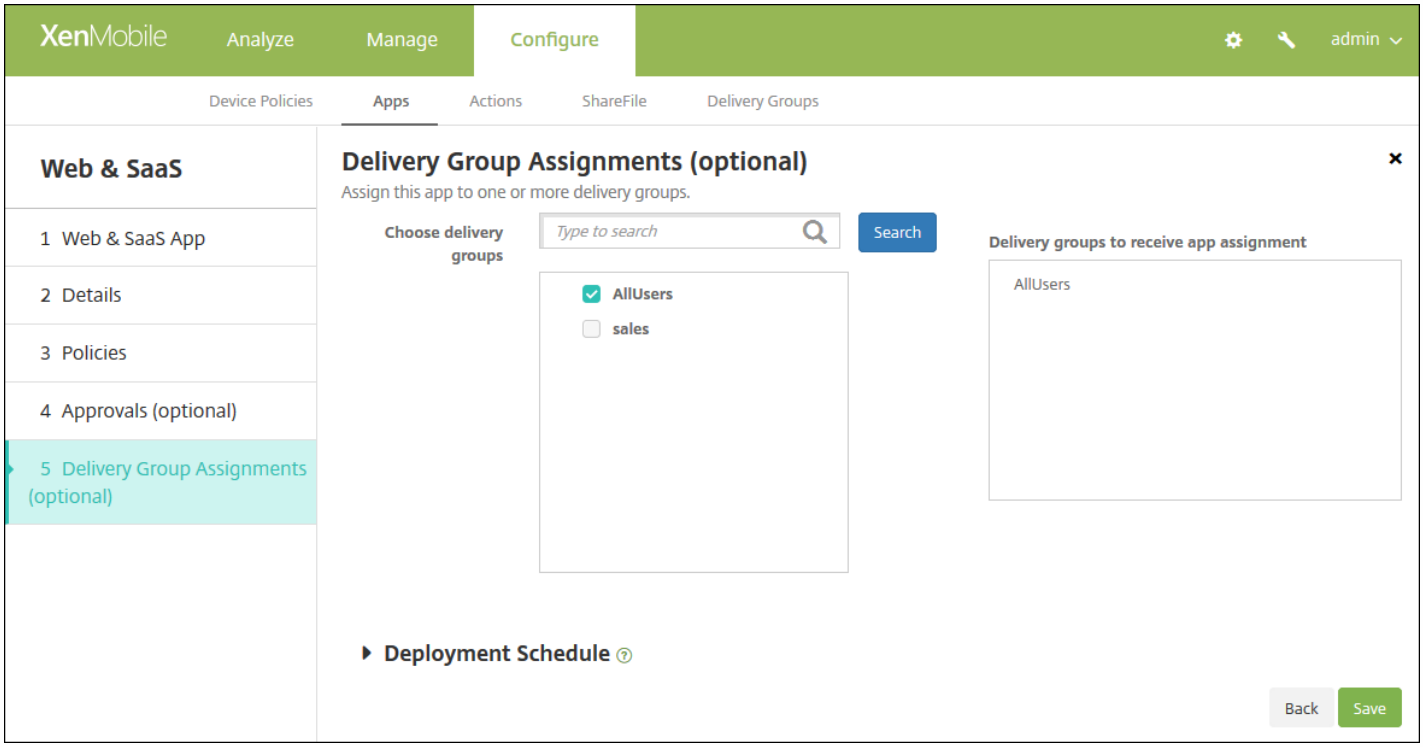
Vous utilisez des workflows lorsque vous avez besoin d'une approbation pour créer des comptes d'utilisateur. S'il n'est pas nécessaire de configurer des workflows d'approbation, vous pouvez passer à l'étape 8.

Configurez ce paramètre si vous devez 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 **Aucune**.
- 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 de la personne s'affiche dans le champ, sélectionnez la case à cocher en regard de son nom. Le nom et l'adresse e-mail de cette personne 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.

8. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer l'application. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

11. Cliquez sur **Enregistrer**.

Liste des types de connecteur d'applications

Jul 27, 2016

Le tableau suivant dresse la liste des connecteurs et des types de connecteurs disponibles avec XenMobile. Il indique également 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

Ajout d'une application d'entreprise à XenMobile

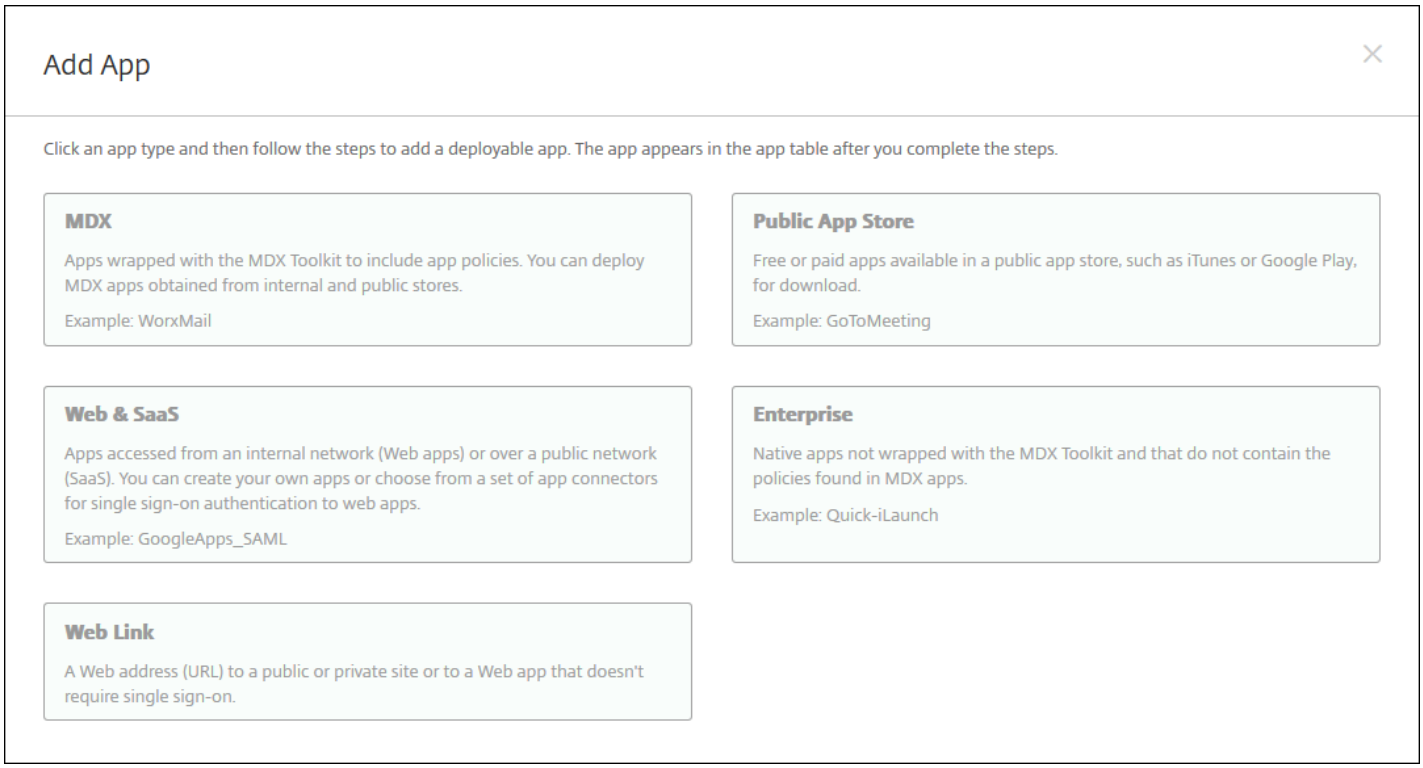
Jul 27, 2016

Les applications d'entreprise dans XenMobile représentent des applications natives qui ne sont pas wrappées avec le MDX Toolkit et qui ne contiennent aucune des 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) :

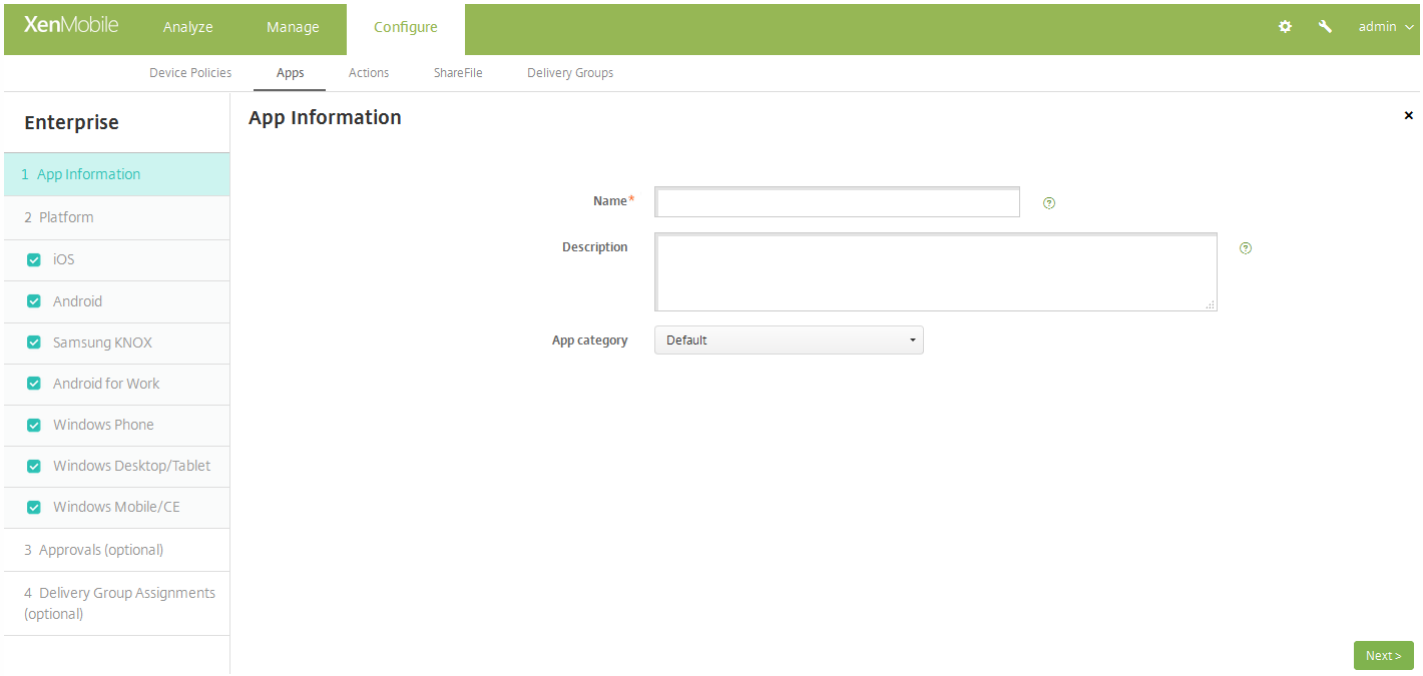
- iOS (fichier .ipa)
- Android (fichier .apk)
- Samsung KNOX (fichier .apk)
- Android for Work (fichier .apk)
- Windows Phone (fichier .xap ou .appx)
- Windows Tablet (fichier .appx)
- Windows Mobile/CE (fichier .cab)

1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'ouvre.

2. Cliquez sur **Add**. La boîte de dialogue **Ajouter une application** s'affiche.



3. Cliquez sur **Enterprise**. La page **Informations sur l'application** s'affiche.



4. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :

- **Nom** : entrez un nom descriptif pour l'application. Il est répertorié sous Nom de l'application dans le tableau des 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 Création de catégories d'applications dans XenMobile.

5. Cliquez sur **Next**. 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.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 10 pour savoir comment définir les règles de déploiement de cette plate-forme.

7. Pour chaque plate-forme que vous avez choisie, sélectionnez le fichier à charger en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

8. Cliquez sur **Next**. La page d'informations sur l'application pour la plate-forme s'affiche.

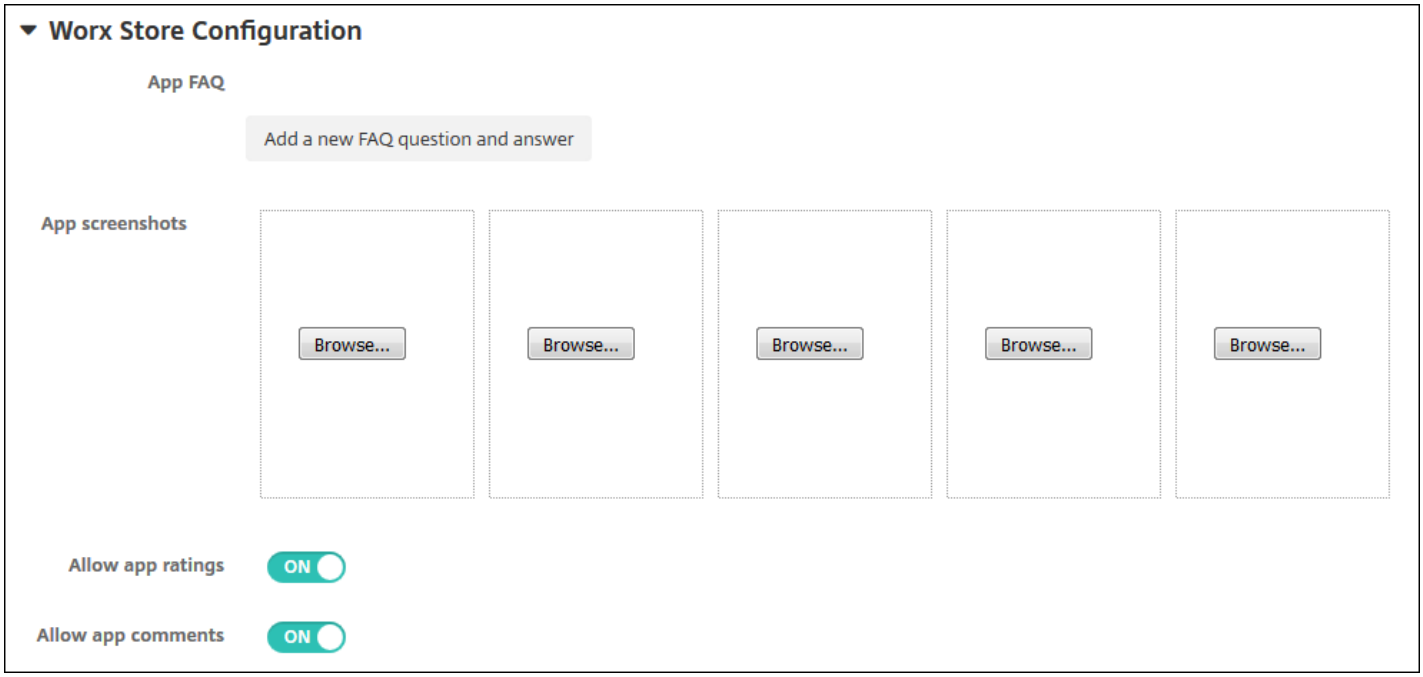
9. Configurez les paramètres pour le type de plate-forme, notamment :

- **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** :
- **Version d'OS maximum** :
- **Appareils exclus** :

- **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**.
- **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**.
- **Forcer l'application à être gérée** : si vous installez une application non gérée, sélectionnez ON 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. Ce paramètre s'applique aux appareils iOS 9.x.

10. Configurez les règles de déploiement.

11. Développez **Configuration de Worx Store**.



Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le Worx Store. 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 Worx Store. 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 **ON**.
  - **Autoriser commentaires sur les applications** : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée. La valeur par défaut est **ON**.

12. 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. S'il n'est pas nécessaire de configurer des workflows d'approbation, vous pouvez passer à l'étape 13.

Configurez ce paramètre si vous devez 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 **Aucune**.
- 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 de la personne s'affiche dans le champ, sélectionnez la case à cocher en regard de son nom. Le nom et l'adresse e-mail de cette personne 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.

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 plusieurs groupes dans la liste auxquels vous souhaitez attribuer l'application. 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 :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

16. Cliquez sur **Enregistrer**.

Ajout d'un lien Web applicatif à XenMobile

Jul 27, 2016

Dans XenMobile, vous pouvez créer une adresse Web (URL) à un site public ou privé, ou à une application Web qui ne requiert pas d'authentification unique (SSO).

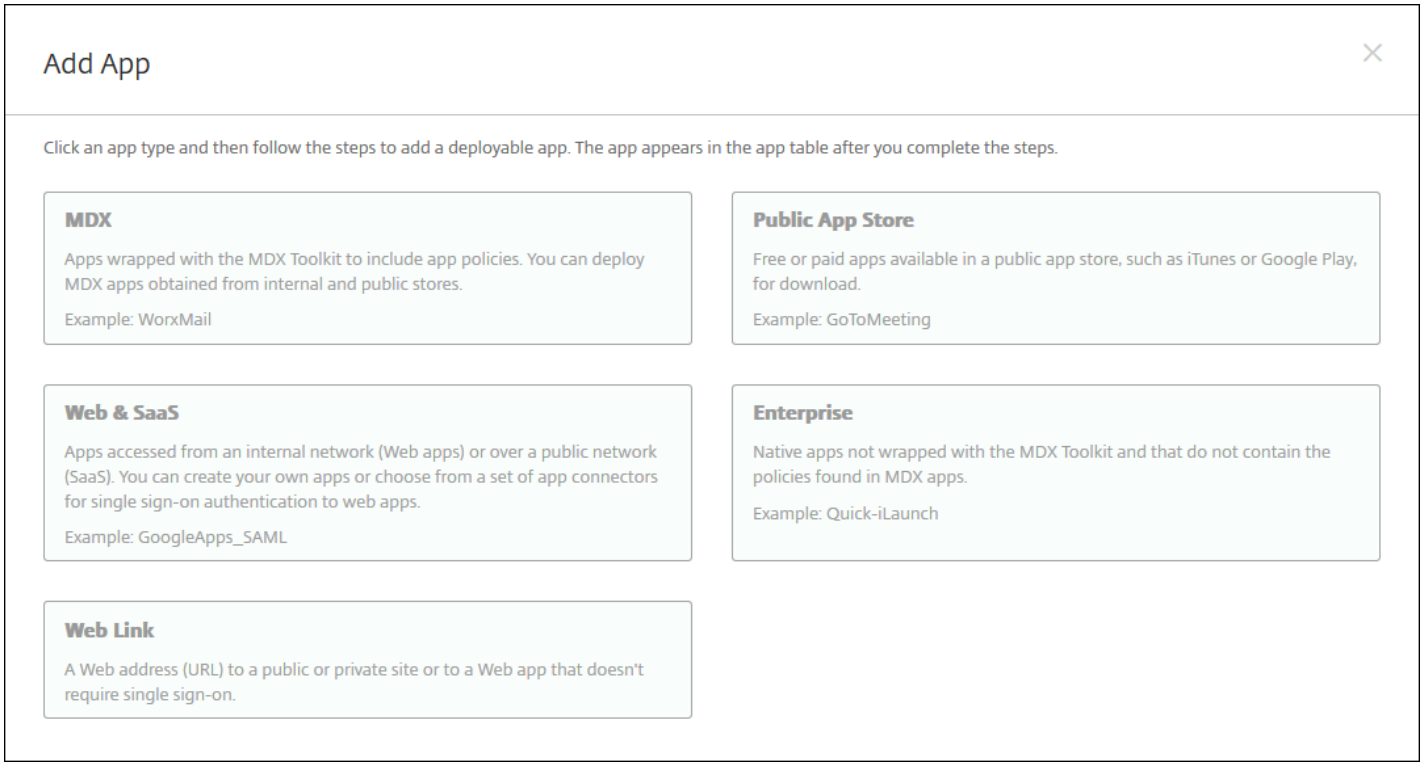
Vous pouvez configurer des liens Web dans l'onglet **Applications** de la console XenMobile. Une fois que vous avez terminé de configurer le lien Web, celui-ci s'affiche sous forme d'icône dans le tableau **Applications**. Lorsque les utilisateurs ouvrent une session avec Worx Home, le lien s'affiche avec la liste des applications et bureaux disponibles.

Pour ajouter le lien, vous devez fournir les informations suivantes :

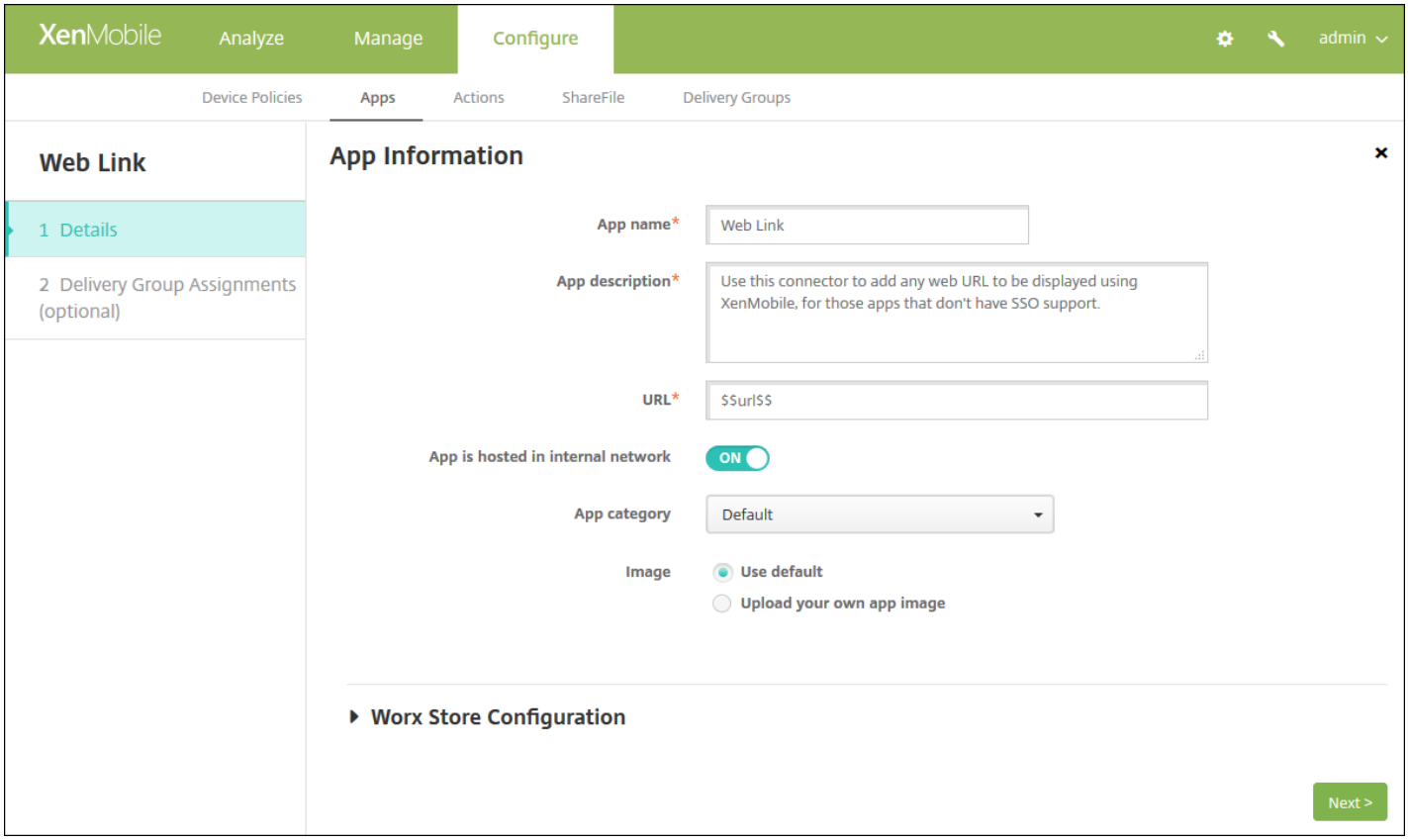
- Nom du lien
- Description du lien
- Adresse Web (URL)
- Catégorie
- Rôle
- Image au format .png (facultatif)

1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'affiche.

2. Cliquez sur **Add**. La boîte de dialogue **Ajouter une application** s'affiche.



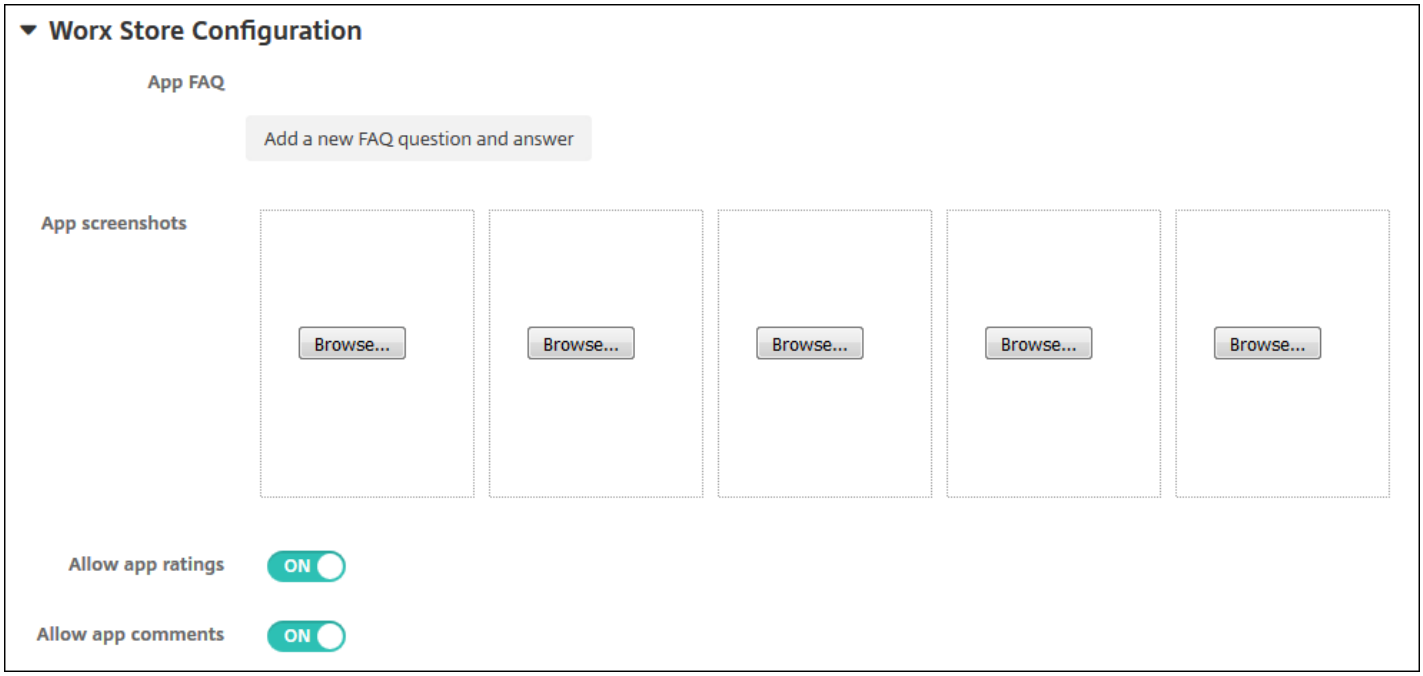
3. Cliquez sur **Lien Web**. La page **Informations sur l'application** s'affiche.



4. 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 NetScaler Gateway. En réglant cette option sur **ON**, le mot-clé VPN est ajouté à l'application et permet aux utilisateurs de se connecter via NetScaler Gateway. La valeur par défaut est **OFF**.
- **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.
  - Si vous souhaitez télécharger votre propre image, sélectionnez-la en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier. Le fichier doit être un fichier .PNG ; vous ne pouvez pas charger une image GIF ou JPEG. Lorsque vous ajoutez un graphique personnalisé, vous ne pouvez pas le modifier ultérieurement.

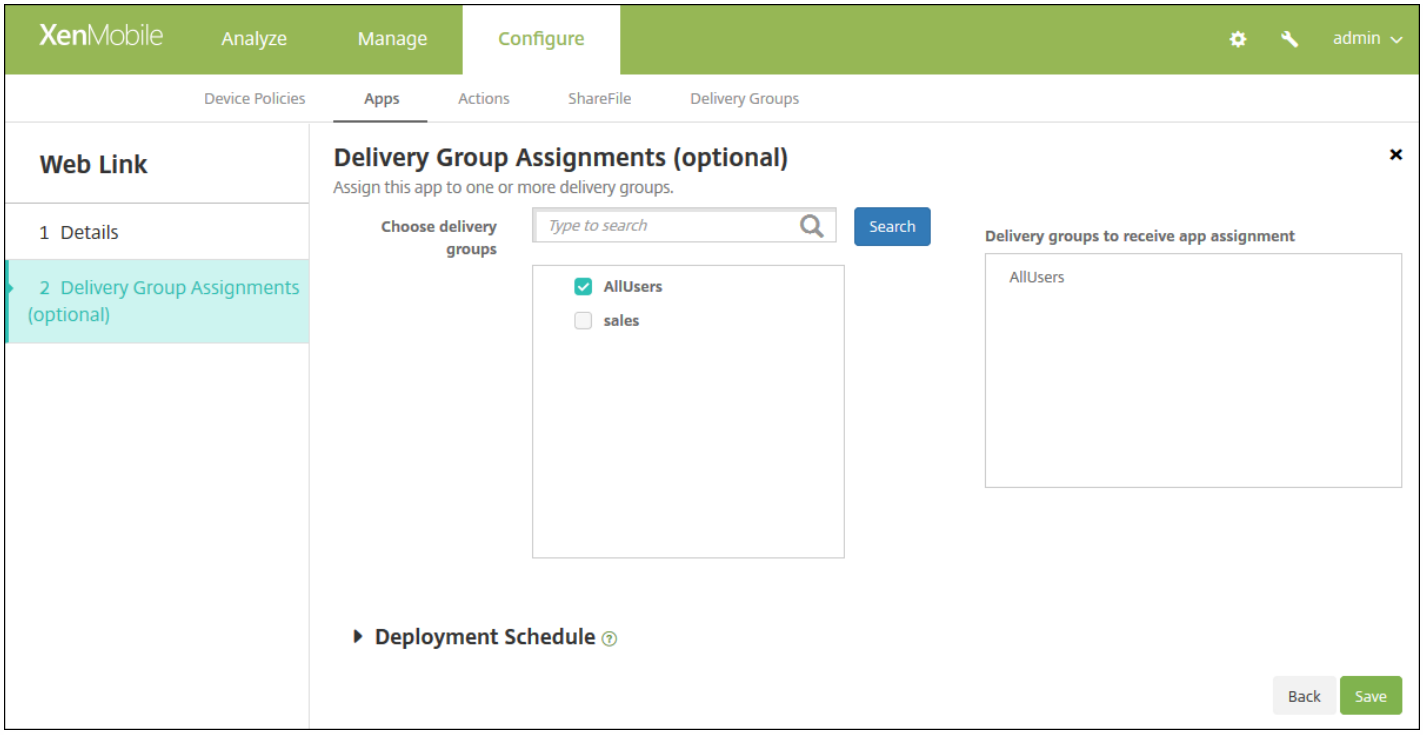
5. Développez **Configuration de Worx Store**.



Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le Worx Store. 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 Worx Store. 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 ON.
  - **Autoriser commentaires sur les applications** : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée. La valeur par défaut est ON.

6. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.



7. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer l'application. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

8. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 **ON** ou **OFF**. L'option par défaut est **OFF**.

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.

9. Cliquez sur **Enregistrer**.

Création et gestion des workflows dans XenMobile

Oct 17, 2016

Vous pouvez appliquer des workflows pour gérer la création et la suppression des comptes d'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.

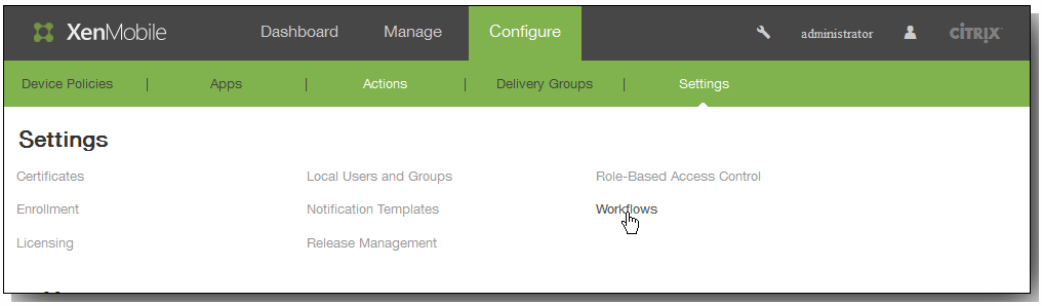
Lorsque vous configurez XenMobile pour la première fois, vous configurez les paramètres de messagerie de workflow. Il est indispensable de configurer les paramètres de messagerie de workflow pour utiliser les workflows. Vous pouvez modifier les paramètres de messagerie de workflow à tout moment. Ces paramètres incluent le serveur de messagerie, le port, l'adresse e-mail et si la demande de création du compte utilisateur requiert ou non une approbation.

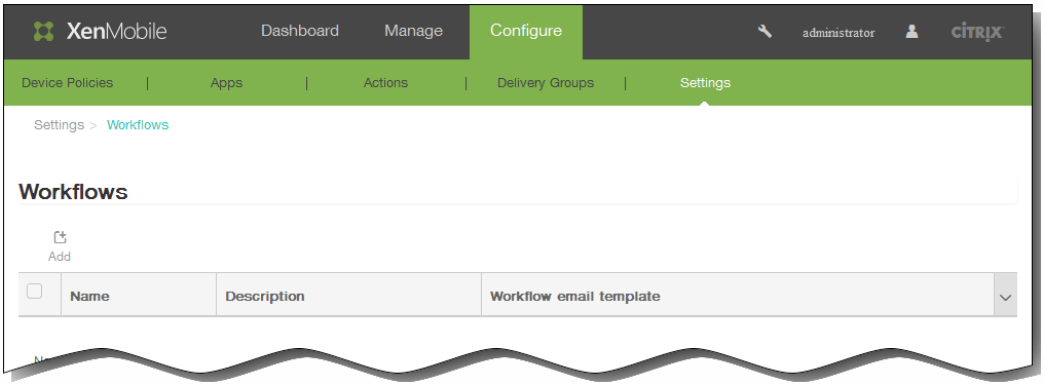
Vous pouvez configurer des workflows à deux emplacements dans XenMobile :

- Dans 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. Voir 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 utiliser leur nom ou adresse e-mail pour les rechercher et les sélectionner. 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.

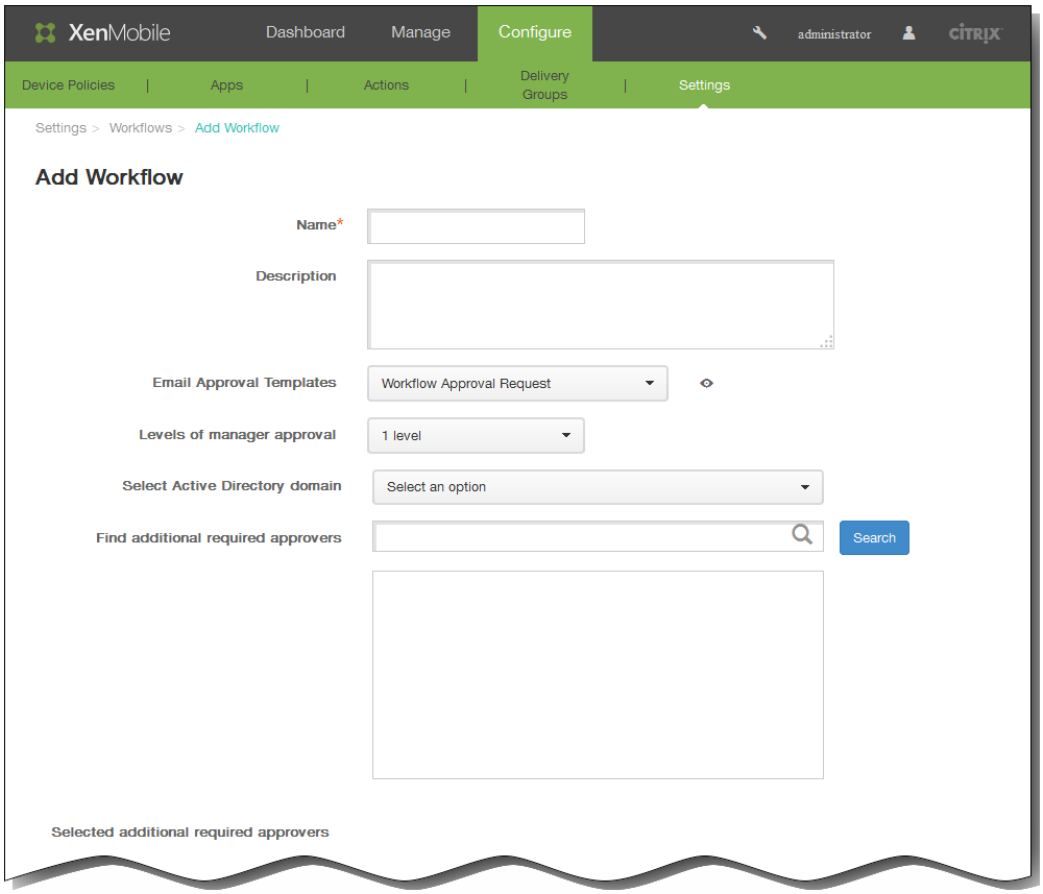
1. Dans la console XenMobile, cliquez sur Configurer > Paramètres > Workflows.





La page Workflows s'affiche.

2. Sur la page Workflows, cliquez sur Ajouter. La page Ajouter un workflow s'affiche.



3. Sur la page Ajouter un workflow, dans le champ Nom, entrez un nom unique pour le workflow.
4. Dans le champ Description, entrez une description pour le workflow (facultatif).
5. Dans la liste Modèles d'approbation d'e-mail, 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, le conseil suivant s'affiche.

6. Dans la liste Niveaux d'approbation par un responsable, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow.
7. Dans la liste Sélectionner un domaine Active Directory, sélectionnez le domaine Active Directory à utiliser pour le workflow.
8. En regard de 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.
9. Lorsque le nom de la personne s'affiche dans le champ, sélectionnez la case à cocher en regard de son nom. Le nom et l'adresse e-mail de cette personne 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.
10. Cliquez sur Save.
    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, vous devez créer un nouveau workflow.

Pour afficher les détails d'un workflow et le supprimer

1. Sur la page Workflows, dans la liste des workflows, sélectionnez un workflow en cliquant sur la ligne dans le tableau ou en cochant 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.

Mise à niveau d'une application MDX ou Enterprise dans XenMobile

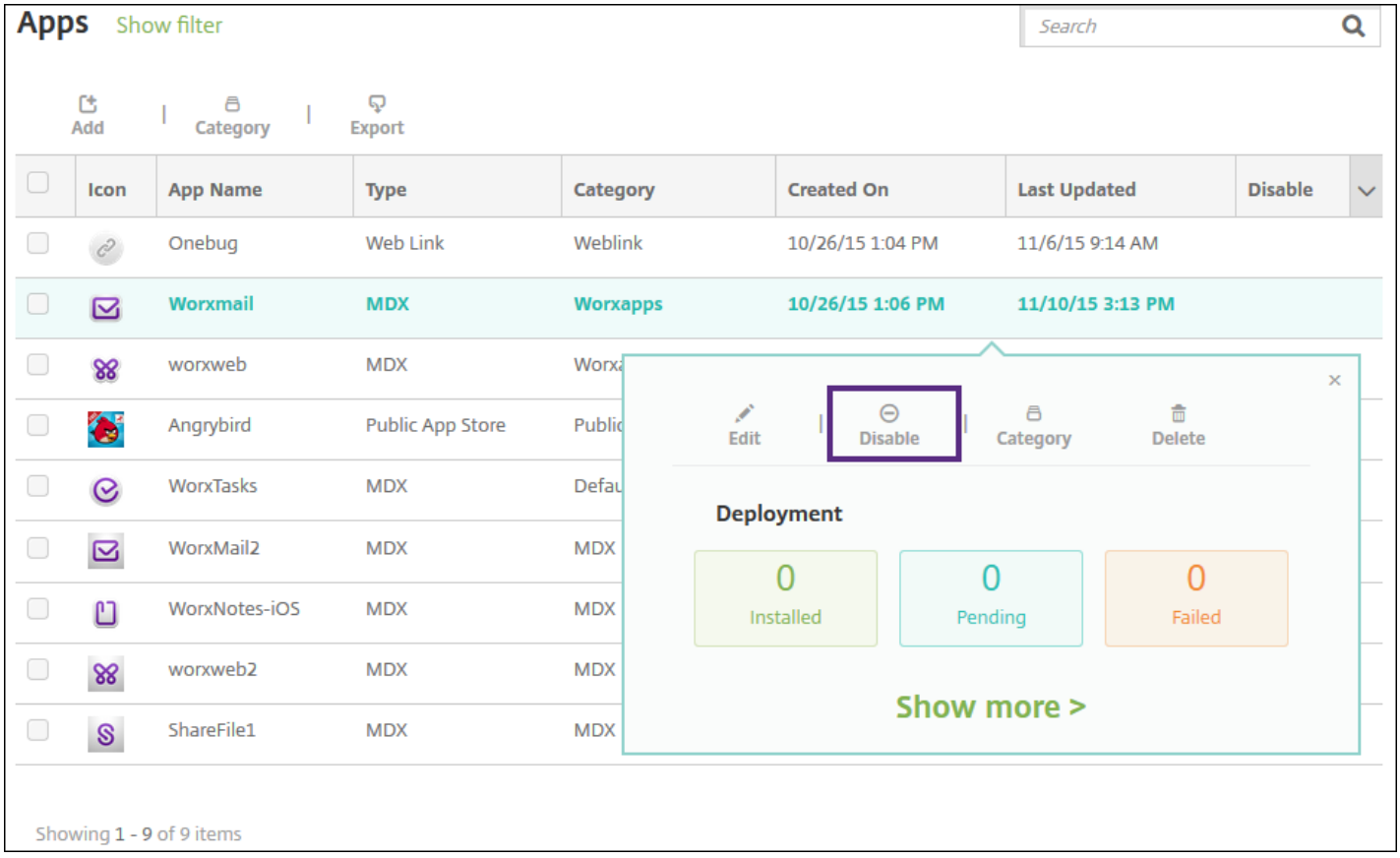
Jul 27, 2016

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.

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 4. Pour les appareils non gérés (appareils inscrits dans XenMobile uniquement à des fins de gestion des applications d'entreprise), procédez comme suit :

- 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.
- Cliquez sur **Désactiver** dans le menu qui s'affiche. La boîte de dialogue **Désactiver** apparaît.



- Cliquez sur **Désactiver** dans la boîte de dialogue. *Désactivé* s'affiche dans la colonne **Désactiver** pour l'application.

Icon	App Name	Type	Category	Created On	Last Updated	Disable
	Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM	
	Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/11/15 8:55 AM	Disabled

Remarque : l'application désactivée passe en mode de maintenance. 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. Les problèmes peuvent survenir en raison des mises à jour de stratégies, par exemple, ou si des utilisateurs effectuent une requête de téléchargement en même temps que vous chargez l'application sur XenMobile.

4. 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.

5. 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.

6. Configurez les paramètres suivants :

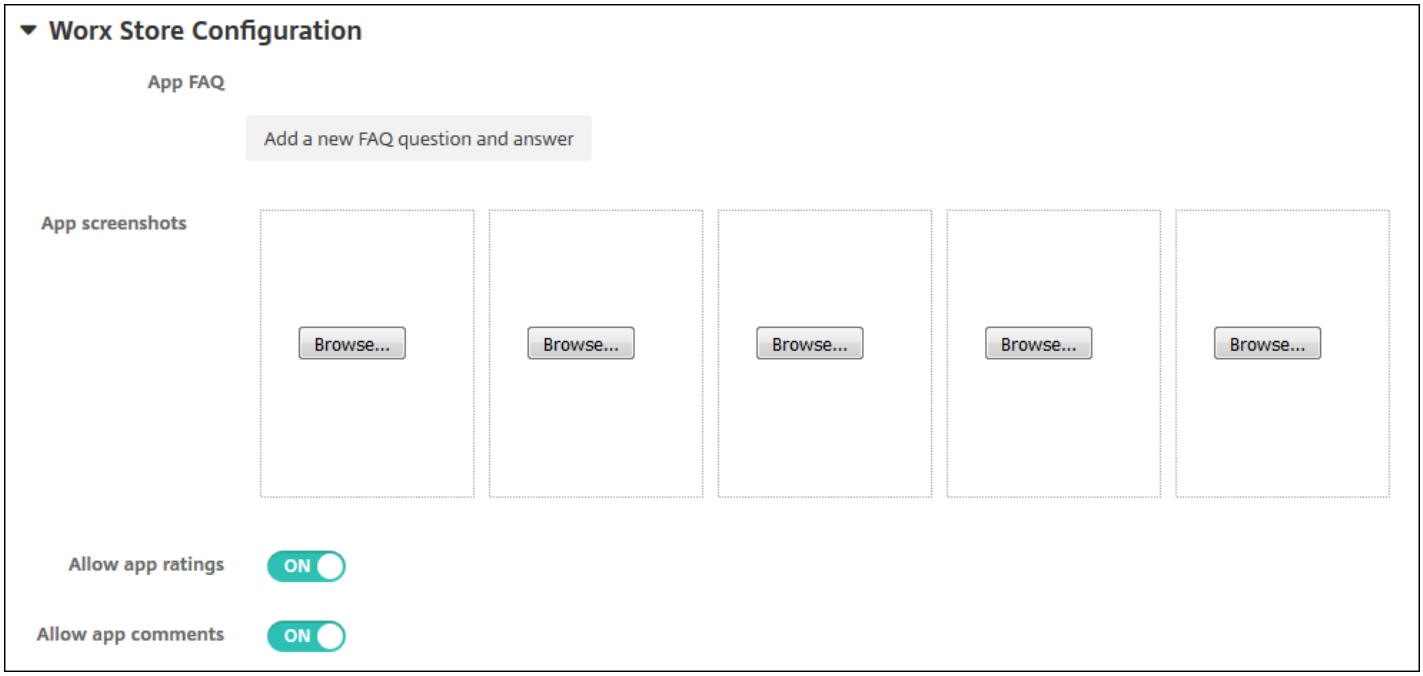
- **Nom** : si vous le souhaitez, vous pouvez modifier le nom de l'application.
- **Description** : si vous le souhaitez, vous pouvez modifier la description de l'application.
- **Catégorie d'application** : si vous le souhaitez, vous pouvez modifier la catégorie.

7. Cliquez sur **Next**. La première page de plate-forme sélectionnée s'affiche. Effectuez les opérations suivantes pour chaque plate-forme sélectionnée :

- 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 le souhaitez, vous pouvez modifier les détails de l'application et les paramètres de stratégie pour la plate-forme.
- Si vous le souhaitez, vous pouvez configurer des règles de déploiement (voir l'étape 7) et Worx Store (voir l'étape 8).

8. Configurez les règles de déploiement.

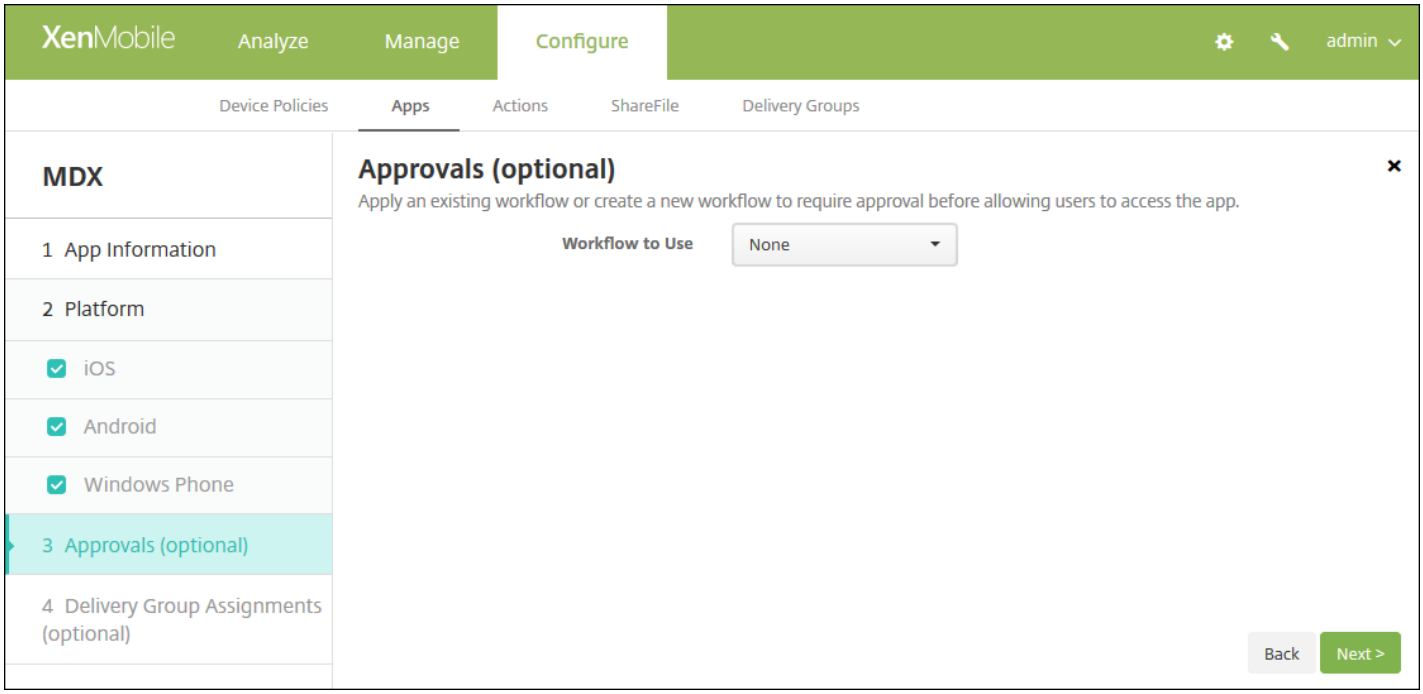
9. Développez **Configuration de Worx Store**.



Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le Worx Store. 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 Worx Store. 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 **ON**.
  - **Autoriser commentaires sur les applications** : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée. La valeur par défaut est **ON**.

10. Cliquez sur **Suivant**. La page **Approbations** s'affiche.



11. Vous utilisez des workflows lorsque vous avez besoin d'une approbation pour créer des comptes d'utilisateur. S'il n'est pas nécessaire de configurer des workflows d'approbation, vous pouvez passer à l'étape 12.

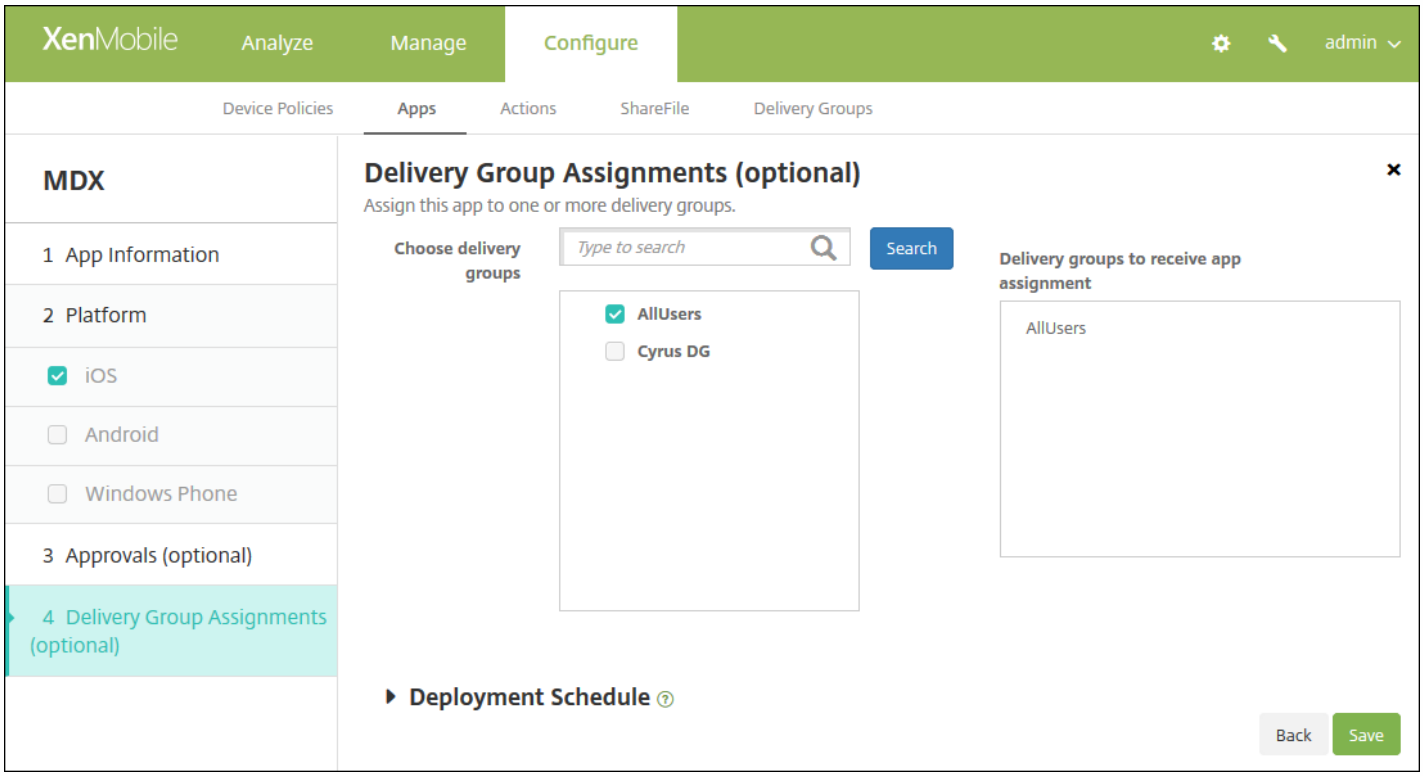
Configurez ce paramètre si vous devez attribuer ou créer un workflow :

- **Workflow à utiliser** : dans la liste, cliquez sur un workflow existant ou cliquez sur **Créer un nouveau workflow**. La valeur par défaut est None.
- 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 de la personne s'affiche dans le champ, sélectionnez la case à cocher en regard de son nom. Le nom et l'adresse e-mail de cette personne 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.

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 plusieurs groupes dans la liste auxquels vous souhaitez attribuer l'application. 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 :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 ON ou OFF. L'option par défaut est OFF.

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.

15. Cliquez sur **Enregistrer**. La page **Applications** s'affiche.

16. Si vous avez désactivé l'application à l'étape 2, effectuez les opérations suivantes :

- Dans le tableau des **Applications**, choisissez l'application que vous avez mis à jour puis dans le menu qui s'affiche, cliquez sur **Activer**.
- 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.

Activation des applications Microsoft Office 365

Aug 22, 2016

Vous pouvez ouvrir le conteneur MDX pour autoriser WorxMail, WorxWeb et ShareFile à transférer des documents et données à des applications Microsoft Office 365. Pour de plus amples informations, consultez la section Activation de l'intégration à Office 365 avec WorxMail, WorxWeb et ShareFile.

Synopsis des stratégies applicatives MDX

Jul 27, 2016

Pour consulter une liste des stratégies applicatives MDX pour iOS, Android et Windows Phone accompagnée de notes sur les restrictions et des recommandations de Citrix, consultez la section Synopsis des stratégies applicatives MDX dans la documentation du MDX Toolkit.

Configuration de XenMobile et de l'application ShareFile pour l'authentification unique à l'aide de SAML

Oct 17, 2016

Vous pouvez configurer XenMobile et ShareFile pour utiliser Security Assertion Markup Language (SAML) afin de fournir un accès SSO (authentification unique) aux applications mobiles ShareFile qui sont wrappées avec le MDX Toolkit, ainsi qu'aux clients ShareFile non wrappés, tel que le site Web, le plug-in Outlook ou les clients de synchronisation.

- **Pour les applications ShareFile wrappées**. Les utilisateurs qui ouvrent une session sur ShareFile via l'application mobile ShareFile sont redirigés vers Worx Home pour l'authentification utilisateur et pour acquérir un jeton SAML. Une fois l'authentification réussie, l'application mobile ShareFile envoie le jeton SAML à ShareFile. Après la première ouverture de session, les utilisateurs peuvent accéder à l'application mobile ShareFile via l'authentification unique et peuvent joindre des documents provenant de ShareFile à des e-mails WorxMail sans ouvrir une session à chaque fois.
- **Pour les clients ShareFile non wrappés**. Les utilisateurs qui ouvrent une session sur ShareFile à l'aide d'un navigateur Web ou d'un autre client ShareFile sont redirigés vers XenMobile pour l'authentification utilisateur et pour acquérir un jeton SAML. Une fois l'authentification réussie, le jeton SAML est envoyé à ShareFile. Après la première ouverture de session, les utilisateurs peuvent accéder aux clients ShareFile via l'authentification unique sans ouvrir une session à chaque fois.

Pour accéder à un diagramme d'architecture de référence détaillé, consultez l'article Reference Architecture for On-Premises Deployments du Manuel de déploiement de XenMobile.

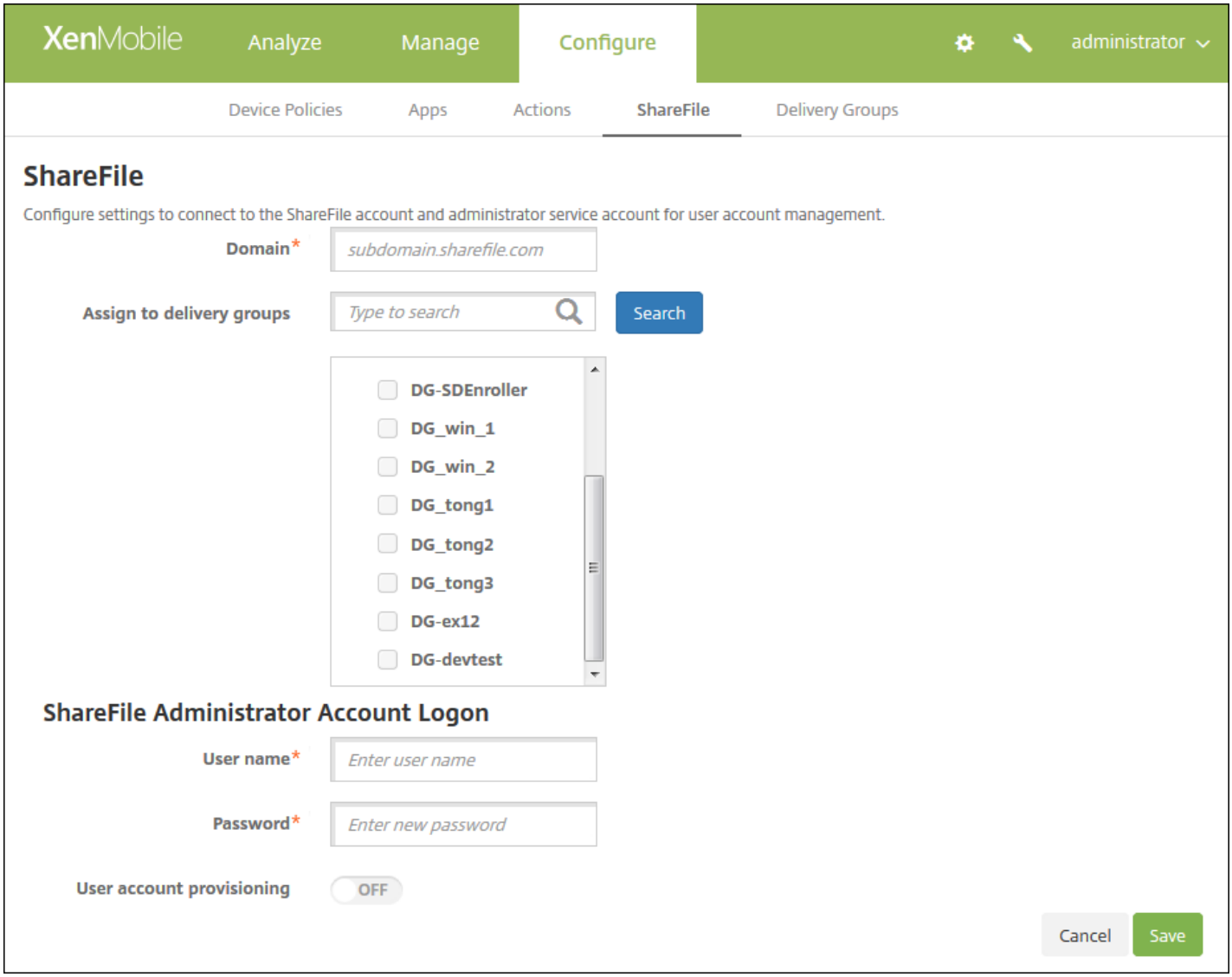
Vous devez remplir les conditions suivantes pour pouvoir configurer l'authentification unique avec les applications XenMobile et ShareFile :

- MDX Toolkit version 9.0.4 ou version ultérieure (pour les applications mobiles ShareFile)
- Applications mobiles ShareFile appropriées :
  - ShareFile pour iPhone version 3.0.x
  - ShareFile pour iPad version 2.2.x
  - ShareFile pour Android version 3.2.x
- Worx Home 9.0 (pour les applications mobiles ShareFile) : installez la version iOS ou Android.
- Compte d'administrateur ShareFile

Assurez-vous que XenMobile et ShareFile peuvent se connecter.

Avant de configurer SAML pour ShareFile, indiquez les informations d'accès à ShareFile comme suit :

1. Dans la console Web XenMobile, cliquez sur **Configurer > ShareFile**. La page de configuration de **ShareFile** s'affiche.



2. Configurez les paramètres suivants :

- **Domaine** : tapez votre nom de sous-domaine ShareFile, par exemple exemple.sharefile.com.
- **Attribuer aux groupes de mise à disposition** : sélectionnez ou recherchez les groupes de mise à disposition dont vous souhaitez qu'ils puissent utiliser l'authentification unique avec ShareFile.
- **Connexion au compte administrateur ShareFile**
  - **Nom d'utilisateur** : tapez le nom d'utilisateur administrateur ShareFile. Cet utilisateur doit disposer des privilèges d'administrateur.
  - **Mot de passe** : tapez le mot de passe d'administrateur ShareFile.
  - **Provisioning du compte utilisateur** : activez cette option si vous souhaitez activer le provisioning des utilisateurs dans XenMobile ; laissez-la désactivée si vous envisagez d'utiliser ShareFile User Management Tool.

    Remarque : si un utilisateur sans compte ShareFile est inclus dans les rôles sélectionnés, XenMobile provisionne automatiquement un compte ShareFile pour cet utilisateur si vous activez le Provisioning du compte utilisateur. Citrix vous recommande d'utiliser un rôle contenant peu de membres pour tester la configuration. Cela permet d'éviter qu'un grand nombre d'utilisateurs ne disposent pas d'un compte ShareFile.

3. Cliquez sur **Enregistrer**.

Les étapes suivantes s'appliquent aux applications et appareils iOS et Android.

1. À l'aide du MDX Toolkit, wrappez l'application mobile ShareFile. Pour de plus amples informations sur le wrapping d'applications avec le MDX Toolkit, consultez la section Wrapping d'applications avec le MDX Toolkit.

2. Dans la console XenMobile, chargez l'application mobile ShareFile wrappée. 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 en ouvrant une session sur ShareFile avec le nom d'utilisateur et le mot de passe administrateur que vous avez configurés dans Configurer l'accès à ShareFile.

4. Assurez-vous que le même fuseau horaire est configuré pour ShareFile et XenMobile.

Remarque : assurez-vous que XenMobile indique l'heure appropriée par rapport au fuseau horaire configuré. Si ce n'est pas le cas, la fonctionnalité SSO peut échouer.

Valider l'application mobile ShareFile

1. Sur la machine utilisateur, si cela n'a pas déjà été fait, installez et configurez Worx Home.

2. À partir de Worx Store, téléchargez et installez l'application mobile ShareFile.

3. Démarrez l'application mobile ShareFile. ShareFile démarre sans vous inviter à saisir un nom d'utilisateur ou un mot de passe.

Valider avec WorxMail

1. Sur la machine utilisateur, si cela n'a pas déjà été fait, installez et configurez Worx Home.

2. À partir de Worx Store, téléchargez, installez et configurez WorxMail.

3. Ouvrez un nouveau formulaire électronique et appuyez sur **Joindre à partir de ShareFile**. 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.

Si vous voulez configurer l'accès des clients ShareFile non wrappés, tels que le site Web, le plug-in Outlook ou les clients de synchronisation, vous devez configurer NetScaler Gateway pour prendre en charge l'utilisation de XenMobile en tant que fournisseur d'identité SAML de la manière suivante :

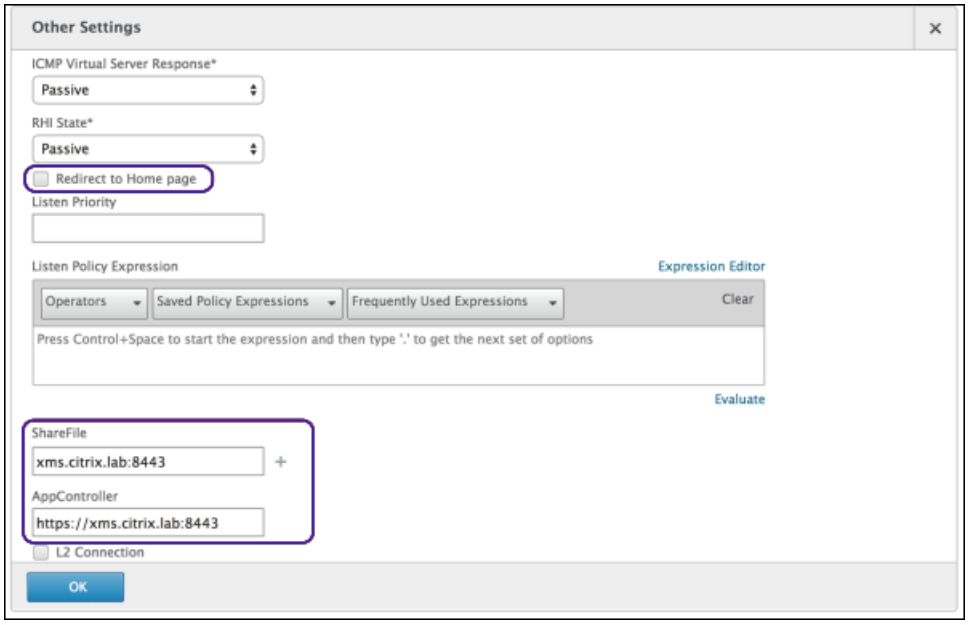
- Désactivez la redirection vers la page d'accueil.
- Créez une stratégie et un profil de session ShareFile.
- Configurez des stratégies sur le serveur virtuel NetScaler Gateway.

Désactiver la redirection vers la page d'accueil

Vous devez désactiver le comportement par défaut pour les demandes qui passent par le chemin d'accès /cginfra de manière à ce que l'utilisateur accède à l'URL interne demandée au lieu de la page d'accueil configurée.

1. Modifiez les paramètres du serveur virtuel NetScaler Gateway qui est utilisé pour les ouvertures de session XenMobile.

Dans NetScaler 10.5, cliquez sur **Other Settings**, puis désactivez la case à cocher intitulée **Redirect to Home Page**.



2. Sous **ShareFile**, tapez le nom de votre serveur interne XenMobile et le numéro de port.

3. Sous **AppController**, tapez l'URL de votre serveur XenMobile.

Cette configuration autorise les demandes pour l'URL indiquée via le chemin d'accès /cginfra.

Créer une stratégie et un profil de demande de session ShareFile

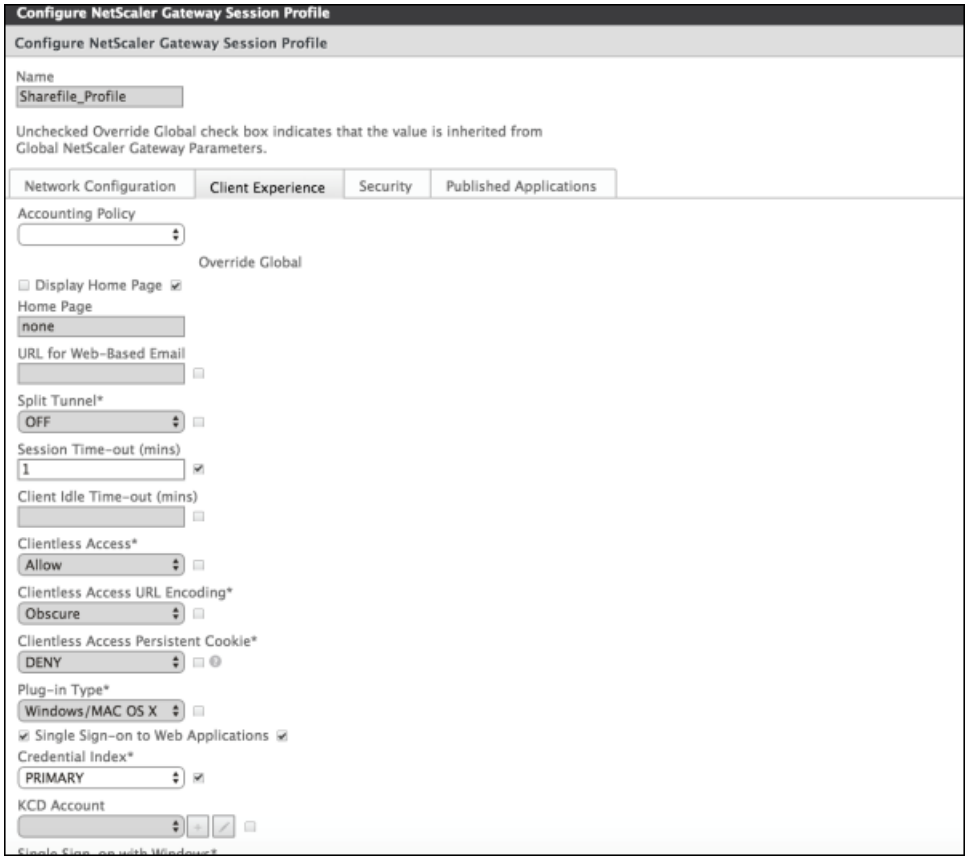
Configurez ces paramètres pour créer une stratégie et un profil de demande de session ShareFile :

1. Dans l'utilitaire de configuration de NetScaler Gateway, dans le volet de navigation de gauche, cliquez sur **NetScaler Gateway > Policies > Session**.

2. Créez une stratégie de session. Dans l'onglet **Policies**, cliquez sur **Add**.

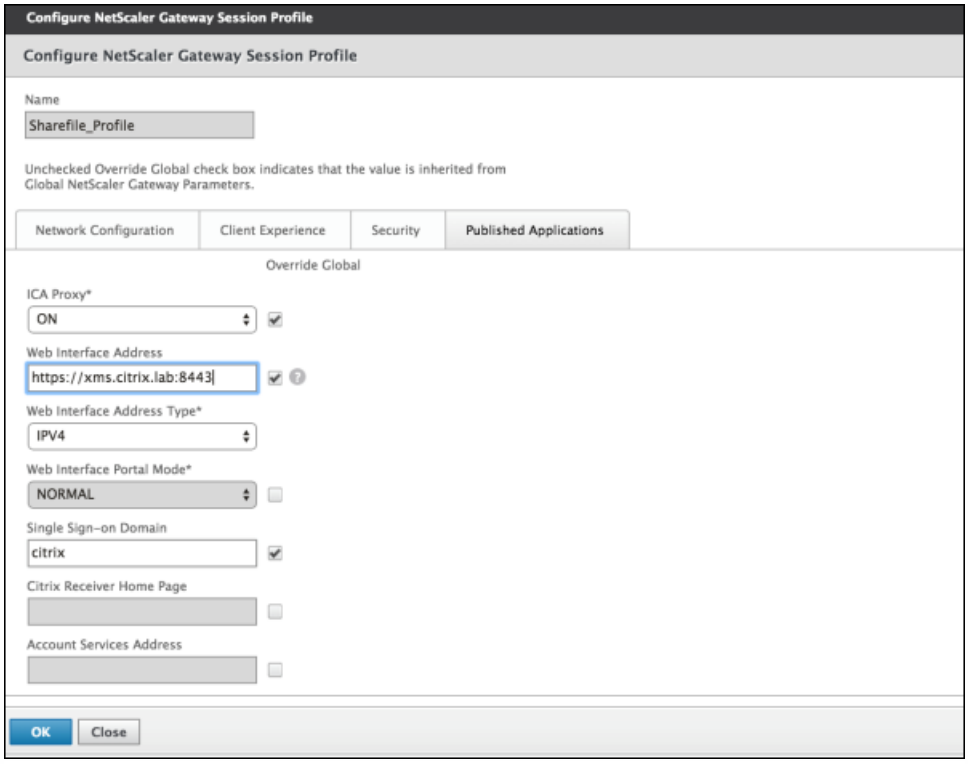
3. Dans le champ **Name**, tapez **ShareFile_Policy**.

4. Créez une action en cliquant sur le bouton **+**. La page **Create NetScaler Gateway 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**.



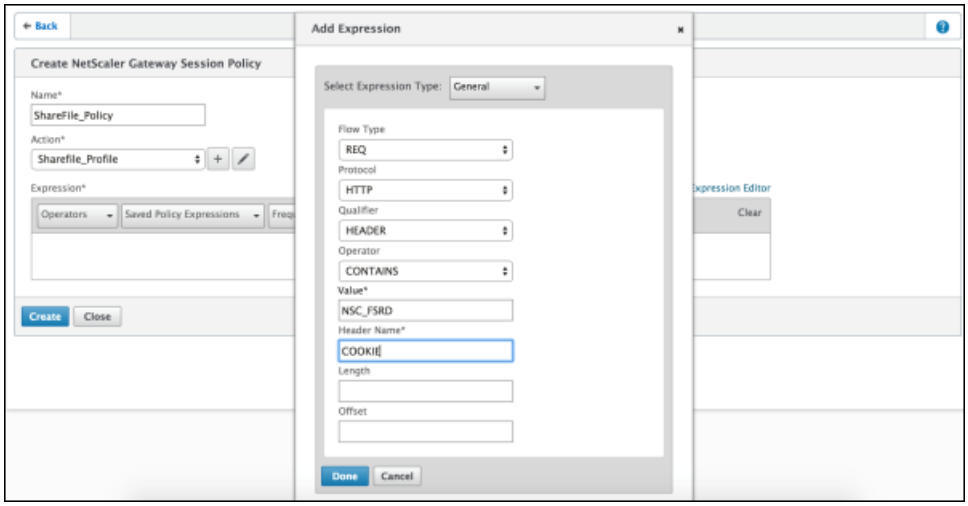
Pour configurer ces paramètres :

- o **Proxy ICA** : dans la liste, cliquez sur **ON**.
- o **Web Interface Address** : entrez l'URL de votre serveur XenMobile.
- o **Single Sign-on Domain** : tapez votre nom de domaine Active Directory.

Remarque : lors de la configuration du profil de session de NetScaler 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.
- Cliquez sur **Done**.

7. Cliquez sur **Create**, puis cliquez sur **Close**.

Configurer des stratégies sur le serveur virtuel NetScaler Gateway

Configurez les paramètres suivants sur le serveur virtuel NetScaler Gateway.

1. Dans l'utilitaire de configuration de NetScaler Gateway, dans le volet de navigation de gauche, cliquez sur **NetScaler Gateway > Virtual Servers**.

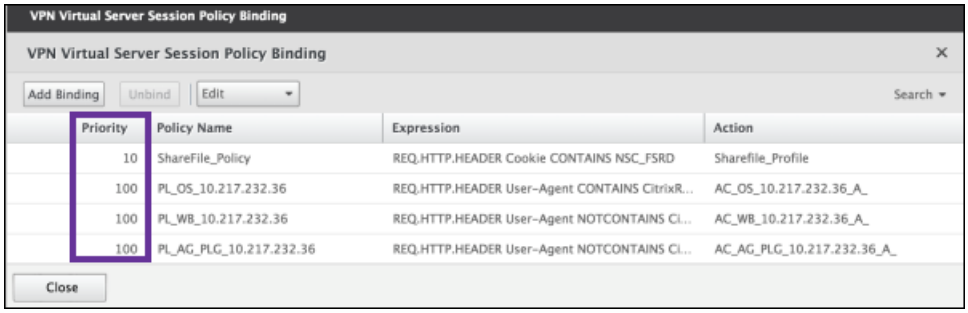
2. Dans le panneau **Details**, cliquez sur votre serveur virtuel NetScaler Gateway.

3. Cliquez sur **Edit**.

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, comme illustré sur la figure suivante.



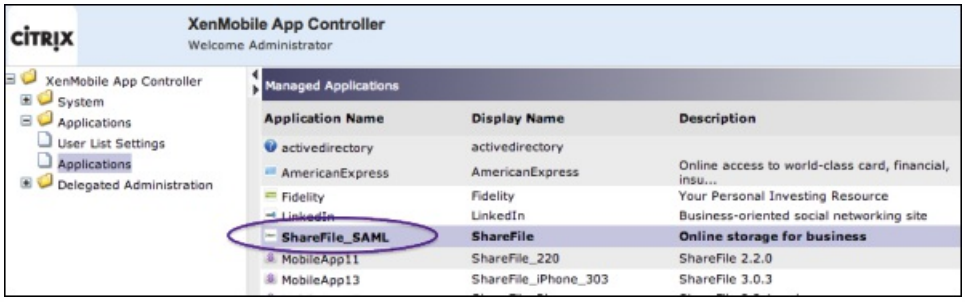
7. Cliquez sur **Terminé**, puis enregistrez la configuration NetScaler actuelle.

Procédez comme suit pour trouver le nom d'application interne pour votre configuration de ShareFile.

1. Ouvrez une session sur l'outil d'administration de XenMobile en accédant à la page suivante : **https://:4443/OCA/admin/**. Assurez-vous de saisir « OCA » en majuscules.

2. Dans la liste **View**, cliquez sur **Configuration**.

3. Cliquez sur **Applications** > Applications et notez le **nom de l'application (Application Name)** correspondant à l'application avec le **nom d'affichage (Display Name)** « ShareFile ».



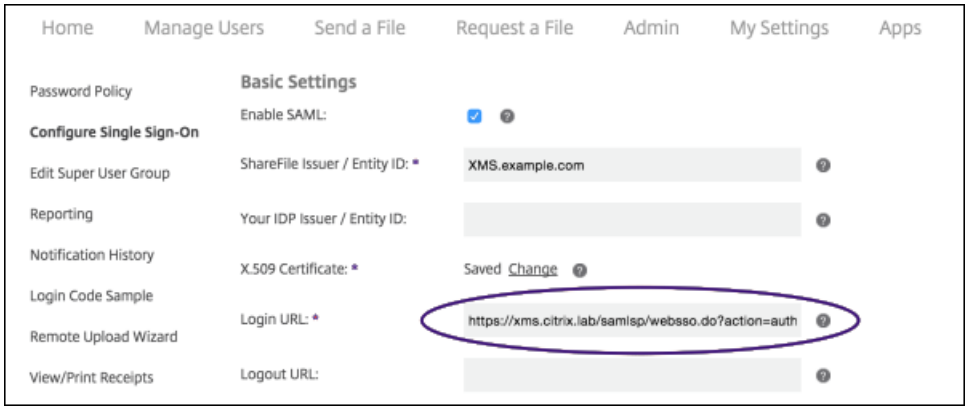
Modifier les paramètres d'authentification unique de ShareFile.com

1. Ouvrez une session sur votre compte ShareFile (https://.sharefile.com) en tant qu'administrateur.

2. Dans l'interface Web ShareFile, cliquez sur **Admin**, puis sélectionnez **Configurer le Single Sign-On**.

3. Modifiez **URL de connexion** comme suit :

URL de connexion doit ressembler à ceci : 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 NetScaler Gateway et « /cginfra/https/ » devant le nom de domaine complet du serveur XenMobile, puis ajoutez « 8443 » après le nom de domaine complet de XenMobile.

  L'URL doit maintenant ressembler à ce qui suit :
  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 interne de l'application ShareFile indiqué à l'étape 3 dans Configurer SAML pour les applications ShareFile non MDX. Le nom interne est **ShareFile_SAML** par défaut ; cependant, chaque fois que vous modifiez votre configuration, un nombre est ajouté au nom interne (ShareFile_SAML_2, ShareFile_SAML_3, etc.).

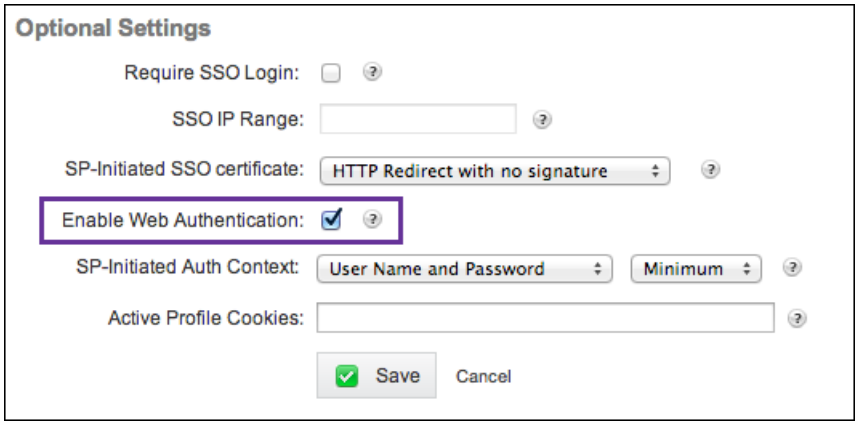
  L'URL doit maintenant ressembler à ce qui suit :
  https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser**&app=ShareFile_SAML**&reqtype=1

- Ajoutez « &nssso=true » à la fin de l'URL.

  L'URL modifiée doit maintenant ressembler à ce qui suit :
  https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1**&nssso=true**.

  Important : chaque fois que vous modifiez ou recréez l'application ShareFile ou que vous modifiez les paramètres ShareFile dans la console XenMobile, un nombre est ajouté au nom d'application interne, ce qui signifie que vous devez également mettre à jour l'URL de connexion sur le site Web de ShareFile pour tenir compte du nouveau nom de l'application.

4. Sous **Paramètres facultatifs**, sélectionnez la case à cocher **Activer l'authentification Web**.



Procédez comme suit pour valider la configuration.

1. Dans votre navigateur, accédez à https://sharefile.com/saml/login.

Vous êtes redirigé vers l'écran d'ouverture de session de NetScaler 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 NetScaler Gateway et XenMobile que vous avez configuré.

Vos dossiers ShareFile à l'adresse .ShareFile.com s'affichent. Si vos dossiers ShareFile n'apparaissent pas, assurez-vous que les informations d'identification saisies pour l'ouverture de session sont correctes.

Actions automatisées

Oct 17, 2016

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, vous devez définir son effet sur l'appareil de l'utilisateur lorsqu'il est connecté à XenMobile en fonction de déclencheurs. 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.

Par exemple, si vous souhaitez détecter une application que vous avez déjà mise dans une liste noire (par exemple, Scrabble), vous pouvez spécifier un déclencheur qui rend l'appareil utilisateur non-conforme lorsque l'application Scrabble est détectée sur leur appareil. L'action les avertit qu'ils doivent supprimer l'application pour que leurs appareils soient à nouveau conformes. Vous pouvez définir un délai au cours duquel l'utilisateur doit se conformer aux exigences avant d'entreprendre d'autres actions plus sérieuses, comme l'effacement des données d'entreprise de l'appareil.

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.

Remarque : 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 la section Notifications dans XenMobile. 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 Pour créer ou mettre à jour des modèles de notification dans XenMobile.

Cette rubrique explique comment ajouter, modifier et filtrer des actions automatisées dans XenMobile.

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 nouvelle action.
- Sélectionnez une action existante à modifier ou à supprimer. Cliquez sur l'option que vous voulez utiliser.

Remarque : lorsque vous activez la case à cocher en regard d'une action, le menu d'options s'affiche au-dessus de la liste d'actions ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

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 de façon unique 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.

Remarque : 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 en mode MDM et y réagit.
  - **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. Les actions disponibles sont les suivantes :

- **Effacer les données d'entreprise de l'appareil** : permet d'effacer toutes les données et applications d'entreprise d'un appareil, sans toucher aux données et applications personnelles.
- **Effacer toutes les données de l'appareil** : permet d'effacer toutes les données et applications d'un appareil, y compris des cartes mémoire si l'appareil en est doté.
- **Révoquer l'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 pourront pas se connecter à XenMobile. Sur iOS, les utilisateurs pourront se connecter, mais ils ne pourront pas accéder aux applications.
- **Effacement des applications** : sur Android, cette option supprime le compte XenMobile de l'utilisateur. Sur iOS, cette option supprime les clés de cryptage dont les utilisateurs ont besoin pour pouvoir accéder aux fonctionnalités de XenMobile.
- **Marquer l'appareil comme non conforme** : permet de définir l'appareil comme non conforme.
- **Envoyer une notification** : permet d'envoyer un message à l'utilisateur.

Le reste de cette procédure décrit comment 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.

Remarque : 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 la section Notifications dans XenMobile. 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 Pour créer ou mettre à jour des modèles de notification dans XenMobile.

Remarque : 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 une action et l'intervalle auquel l'action doit se répéter jusqu'à ce que l'utilisateur résolve le problème ayant activé le 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.

14. Lorsque vous avez terminé de configurer les règles de déploiement par plate-forme pour l'action, cliquez sur **Suivant**. La page d'attribution **Actions** s'affiche, où vous attribuez l'action à un groupe ou des 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 un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **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 **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- 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 sur **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 **ON** ou **OFF**. L'option par défaut est **OFF**. **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.

Remarque : 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.

Macros dans XenMobile

Jul 27, 2016

XenMobile fournit des macros puissantes qui permettent de renseigner les données de propriété d'utilisateur ou d'appareil dans le champ de texte d'un profil, d'une stratégie, d'une notification, ou d'un modèle d'inscription (pour certaines actions), pour ne citer que quelques exemples d'utilisations. Grâce aux macros, vous pouvez configurer une stratégie et la déployer 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. Par exemple, vous pouvez pré-remplir la valeur boîte aux lettres pour un utilisateur dans un profil Exchange pour des milliers d'utilisateurs.

Cette fonctionnalité est disponible uniquement dans le contexte de configurations et de modèles pour iOS et Android.

Les macros utilisateur suivantes sont toujours disponibles :

- nom d'ouverture de session (nom d'utilisateur + domainname)
- username (nom d'ouverture de session moins le domaine, si présent)
- domainname (nom de domaine, ou domaine par défaut)

Il se peut que les propriétés suivantes définies par l'administrateur soient disponibles :

- c
- cn
- company
- companyname
- department
- description
- displayname
- distinguishedname
- facsimiletelephonenumber
- givenname
- homecity
- homecountry
- homefax
- homephone
- homestate
- homestreetaddress
- homezip
- ipphone
- l
- mail
- middleinitial
- mobile
- officestreetaddress
- pager
- physicaldeliveryofficename

- postalcode
- postofficebox
- telephonenumber
- samaccountname
- sn
- st
- streetaddress
- title
- userprincipalname
- domainname (remplace la propriété décrite ci-dessus)

En outre, si l'utilisateur est authentifié à l'aide d'un serveur d'authentification, tel que LDAP, toutes les propriétés associées à l'utilisateur dans le magasin sont disponibles.

Une macro pouvez prendre la forme suivante :

- ${type.PROPERTYNAME}
- ${type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]}

De manière générale, toute syntaxe suivie du symbole dollar ($) doit être placée 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.")}.

Par exemple,${user.username} remplit la valeur de nom d'utilisateur dans le champ de texte d'une stratégie. Ceci est utile pour la configuration des profils Exchange ActiveSync et d'autres profils utilisés par plusieurs utilisateurs.

Pour les macros personnalisées (propriétés que vous définissez), le préfixe est ${custom}. Vous pouvez ignorer le préfixe.

Remarque : les noms de propriétés sont sensibles à la casse.

Paramètres du client XenMobile

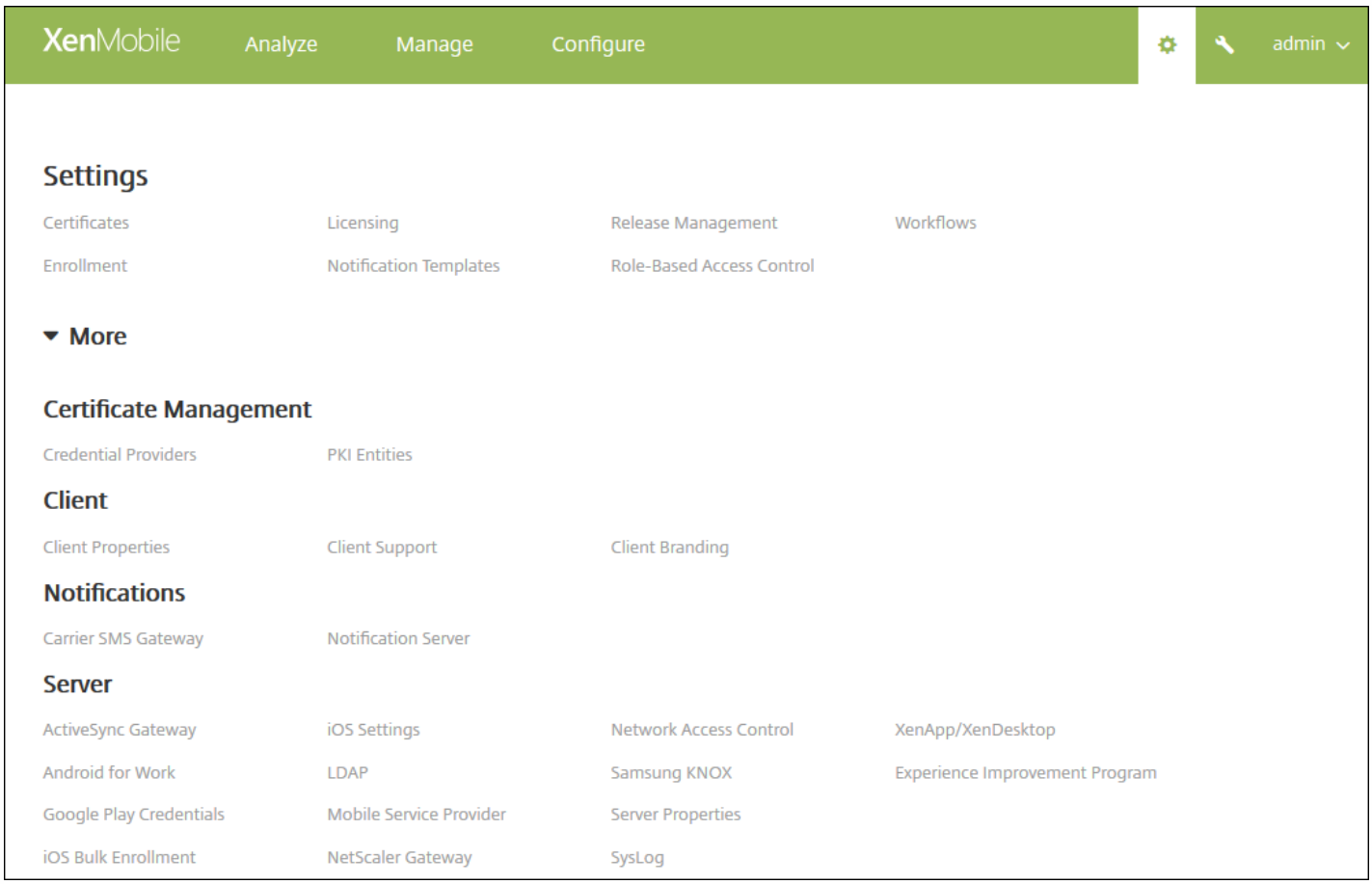
Jul 27, 2016

Les paramètres du client XenMobile que vous configurez dans la console Web XenMobile comprennent :

- Propriétés de client
- Support client
- Personnalisation du client

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

3. Sous **Client**, cliquez sur l'option que vous souhaitez configurer.



Personnalisation du Worx Store pour appareils iOS

Oct 17, 2016

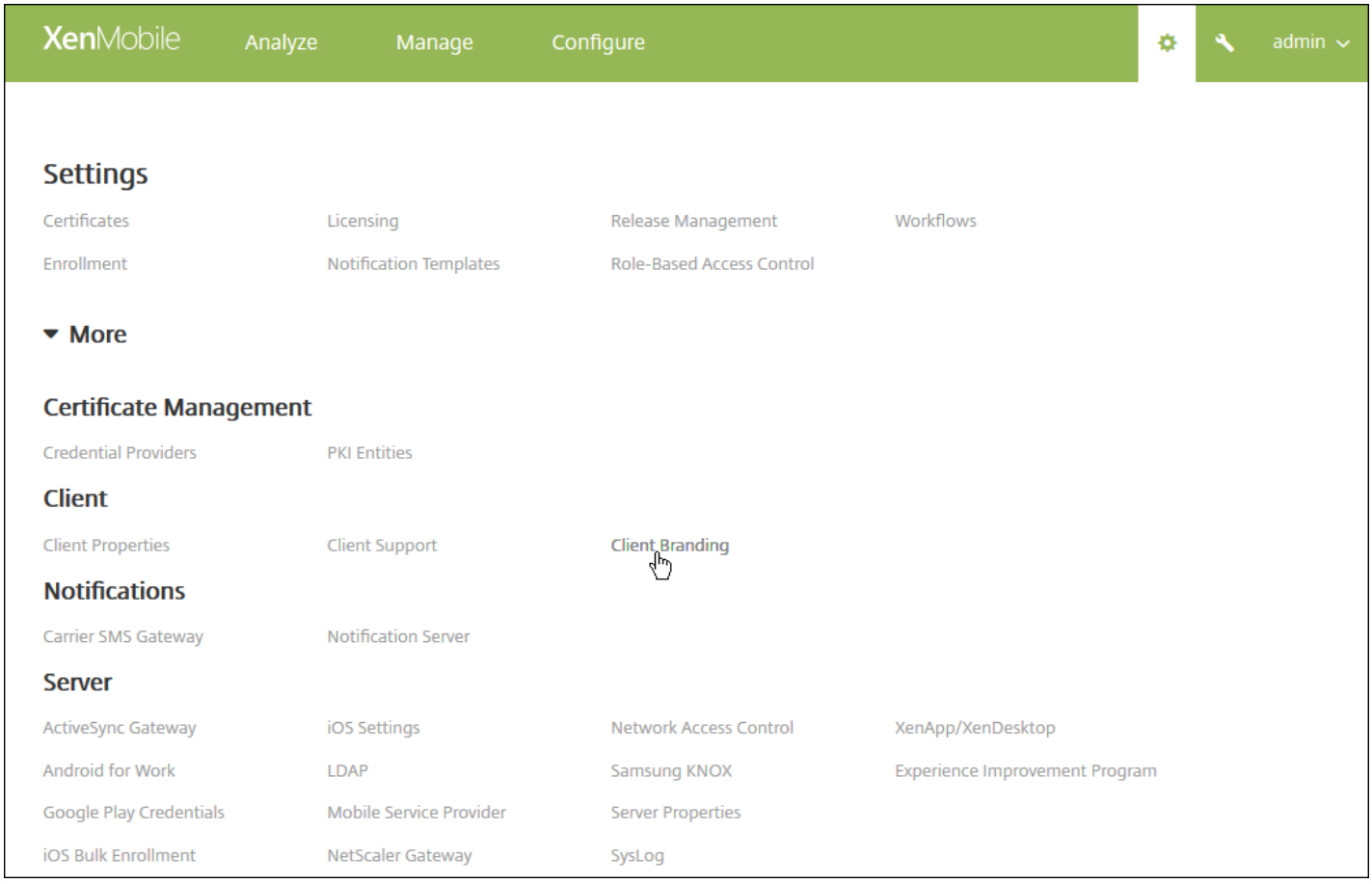
Vous pouvez configurer la manière dont les applications s'affichent dans le magasin et ajouter un logo pour personnaliser Secure Hub et XenMobile sur les appareils mobiles iOS et Android.

Remarque : avant de commencer, assurez-vous que votre image personnalisée est prête et accessible.

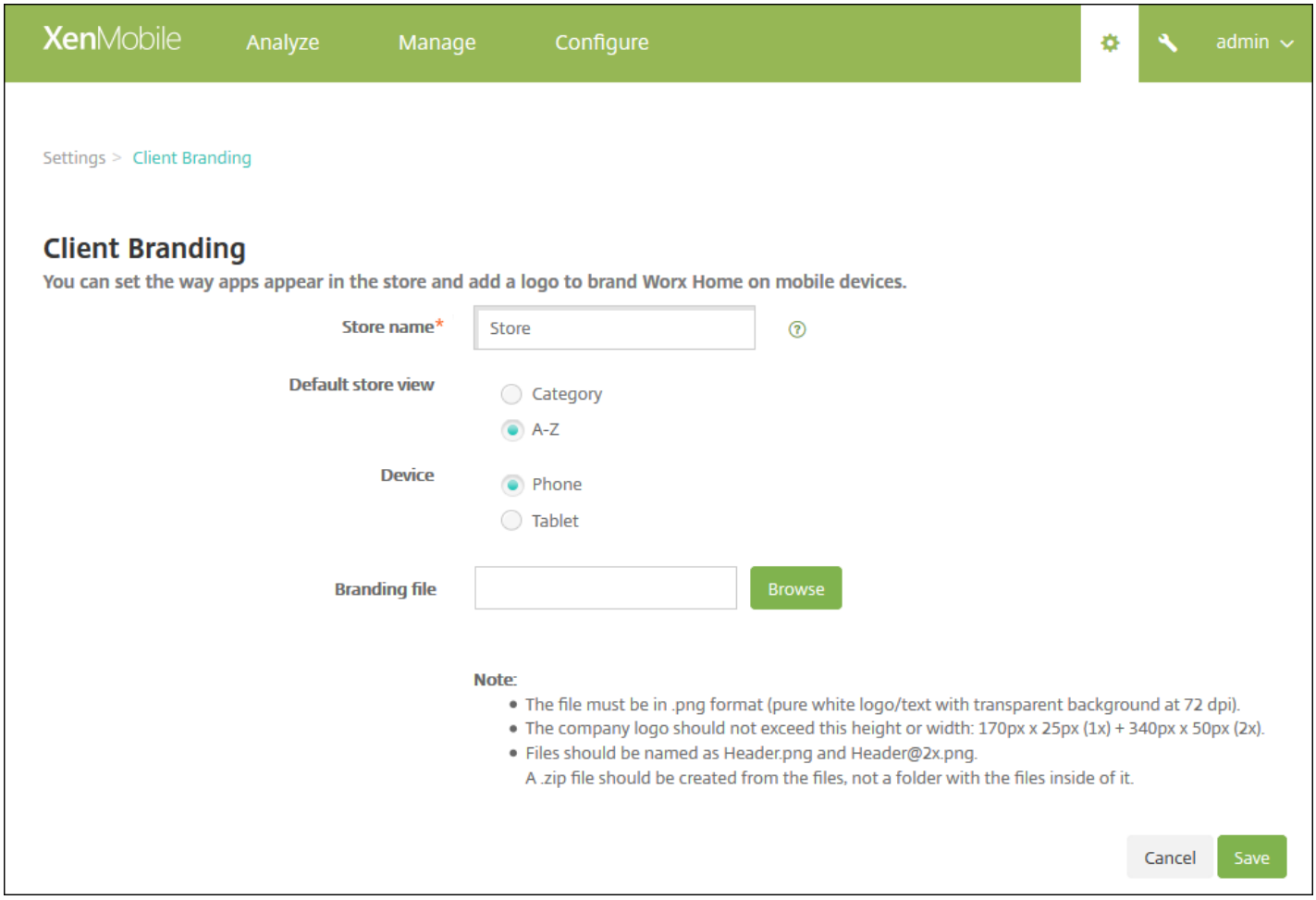
L'image personnalisée doit répondre à ces exigences :

- 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, 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.
- **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**.

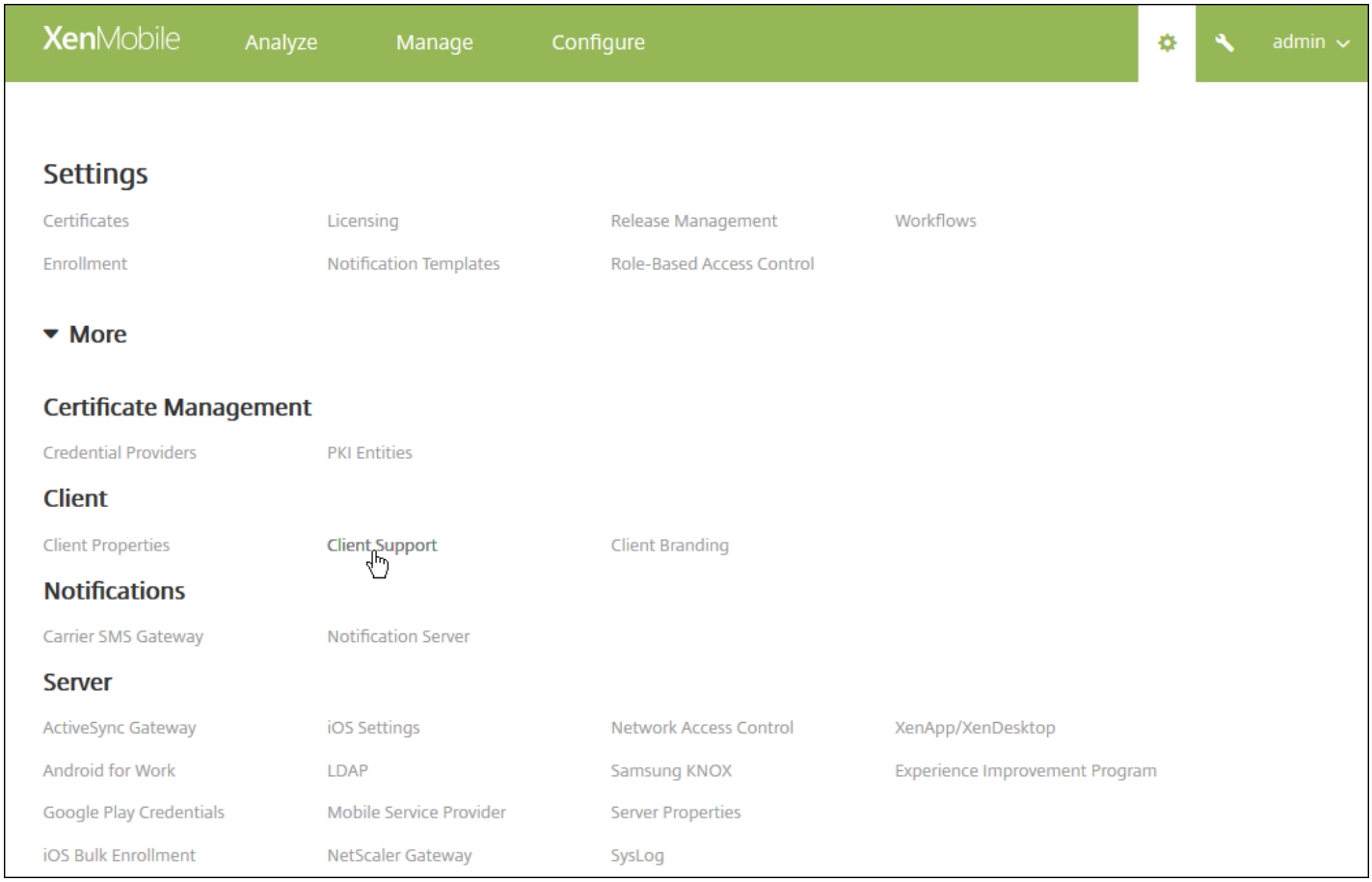
Pour déployer ce paquetage auprès des appareils de vos utilisateurs, vous devez créer un paquetage de déploiement et le déployer sur les appareils des utilisateurs.

Création d'options d'assistance Worx Home et GoToAssist

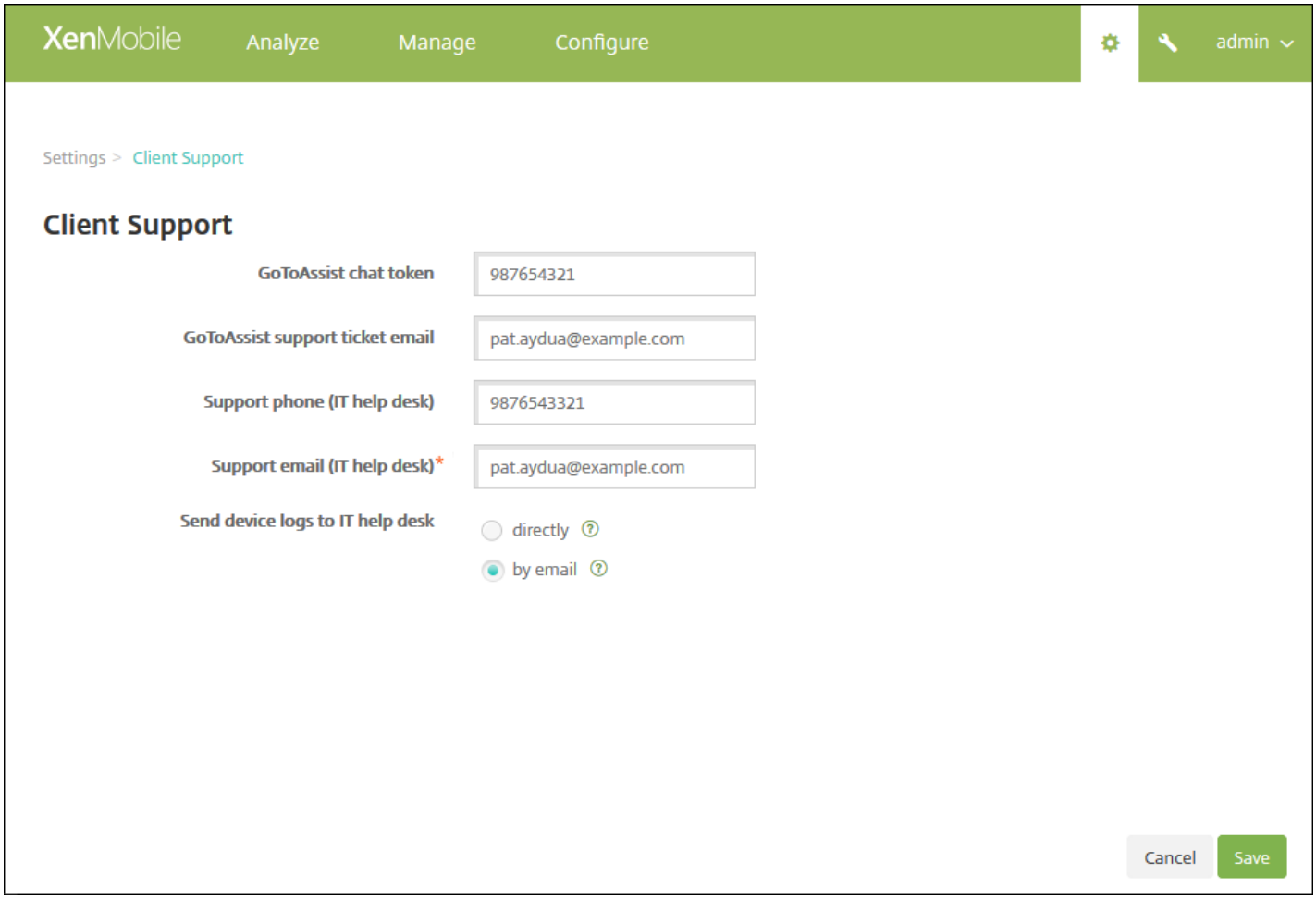
Oct 17, 2016

Vous pouvez fournir à vos utilisateurs différentes méthodes pour contacter le personnel d'assistance : adresses e-mail, numéros de téléphone, jetons et GoToAssist. Lorsque des utilisateurs demandent une assistance depuis leurs appareils, ils voient les options que vous avez définies.

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 :

- **Jeton de chat GoToAssist** : entrez le jeton que les utilisateurs reçoivent pour initier une session GoToAssist.
- **E-mail de ticket d'assistance GoToAssist** : entrez l'adresse e-mail utilisée par les utilisateurs pour les tickets d'assistance GoToAssist.
- **Téléphone de l'assistance (support technique)** : entrez le numéro de téléphone pour votre service d'assistance.
- **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 s'affichent. Si vous activez Stocker les journaux sur ShareFile, les journaux sont envoyés directement à ShareFile ; sinon, ils sont transmis à XenMobile puis envoyés par e-mail au service d'assistance. 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'il existe un problème de serveur, 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**.

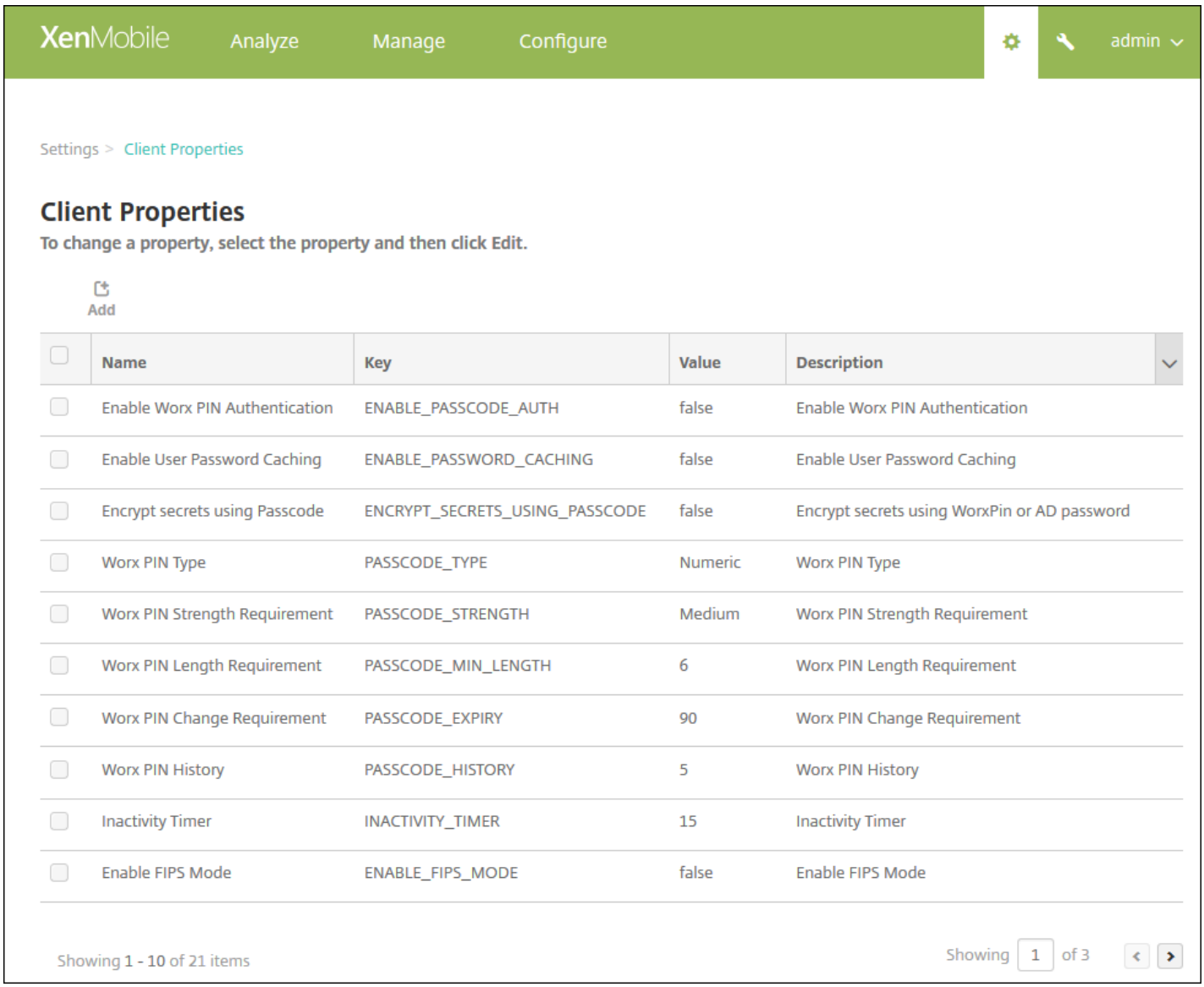
Pour ajouter, modifier ou supprimer des propriétés de client

Jul 27, 2016

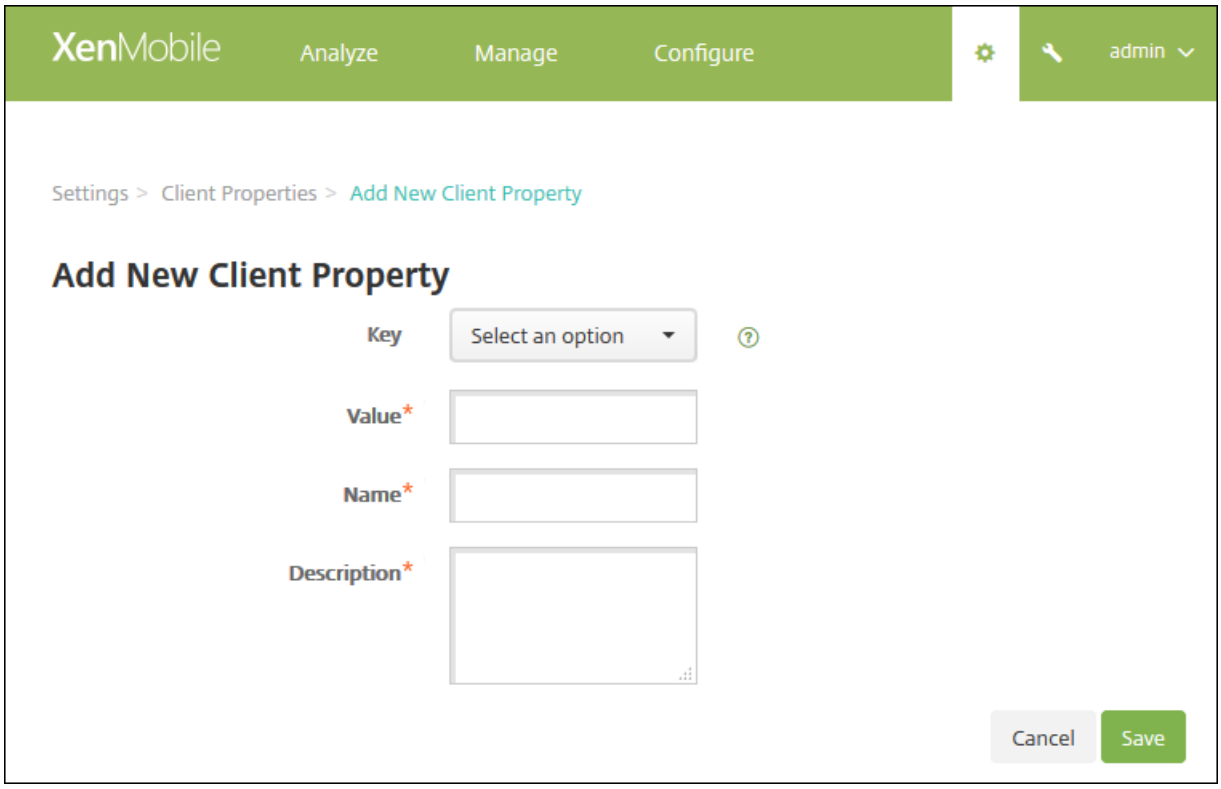
Les propriétés du client contiennent des informations qui sont fournies directement à Worx Home sur les appareils des utilisateurs. Vous pouvez utiliser ces propriétés pour configurer des paramètres avancés tels que le code PIN Worx. Vous obtenez les propriétés du client à partir du support de Citrix.

les propriétés du client sont susceptibles d'être modifiées avec chaque nouvelle version des applications clientes, et plus particulièrement Worx Home. Pour de plus amples informations sur les propriétés du client, consultez la section Propriété client.

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 boîte de dialogue **Propriétés du client** s'affiche. Vous pouvez ajouter, modifier et supprimer des propriétés de client à partir de cette page.



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



2. Configurez les paramètres suivants :

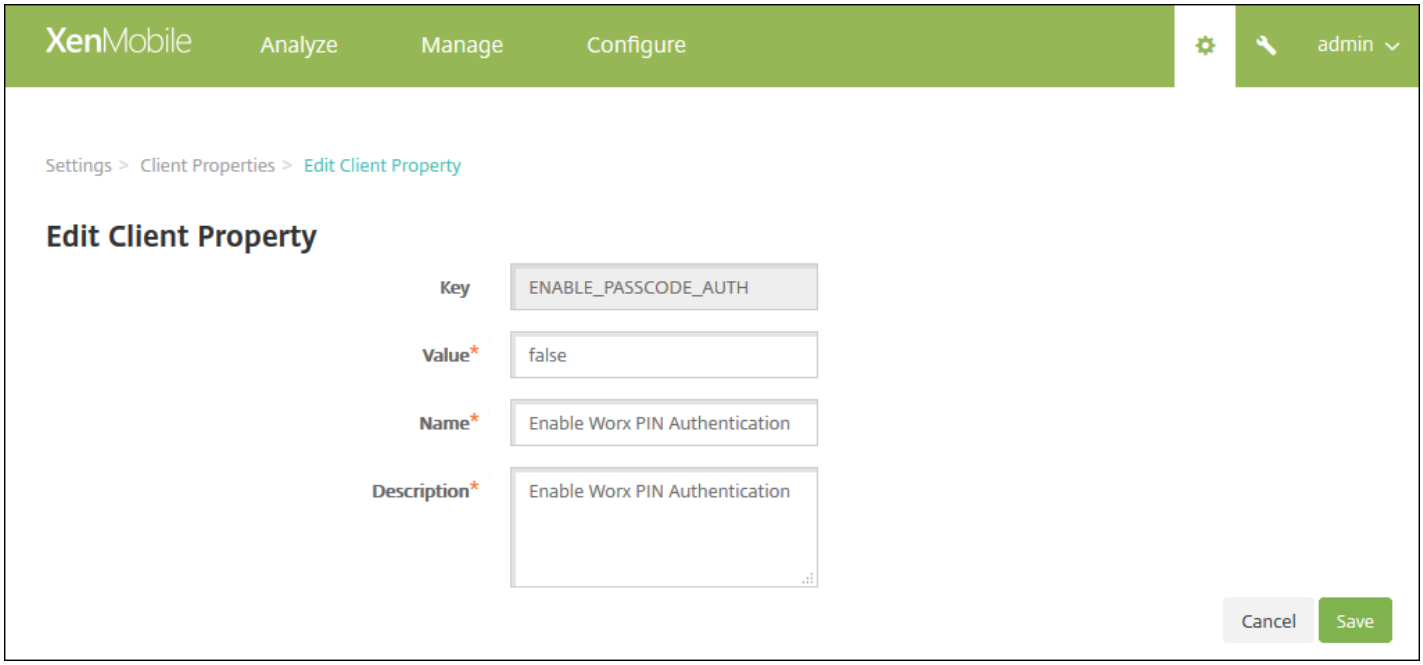
- **Clé** : dans la liste, cliquez sur la clé de propriété que vous souhaitez ajouter. **Important :** contactez le support Citrix avant d'apporter des modifications ou pour demander une clé spéciale pour effectuer une modification.
- **Valeur** : entrez la valeur de la propriété sélectionnée.
- **Nom** : entrez un nom pour la propriété.
- **Description** : entrez une description pour la propriété.

3. Cliquez sur **Enregistrer**.

1. Dans le tableau **Propriétés du client**, sélectionnez la propriété de client que vous voulez modifier.

Remarque : 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 ailleurs 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.

1. Dans le tableau **Propriétés du client**, sélectionnez la propriété de client que vous voulez supprimer.

   Remarque : 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

Jul 27, 2016

Les propriétés client prédéfinies de XenMobile et leurs paramètres par défaut sont comme suit.

CONTAINER_SELF_DESTRUCT_PERIOD

Nom d'affichage : Auto-destruction

La fonction d'auto-destruction empêche l'accès à WorxHome et aux applications gérées, après un certain nombre de jours d'inactivité. Après ce délai, les applications ne sont plus utilisables et l'utilisateur de l'appareil est désinscrit du serveur XenMobile. 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 vous définissez un délai de 30 jours pour la stratégie et que l'utilisateur n'utilise pas Worx Home ou d'autres 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.

ENABLE_WORXHOME_CEIP

Nom d'affichage : activer le programme CEIP de Worx Home

Cette touche active le Programme d'amélioration de l'expérience utilisateur. Ce dernier va envoyer périodiquement des données de configuration et d'utilisation anonymes à Citrix. Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de XenMobile.

Valeur : true ou false

Valeur par défaut : false

ENABLE_PASSCODE_AUTH

Nom complet : Activer l'authentification du code PIN Worx

Cette clé permet d'activer la fonctionnalité de code PIN Worx. Avec le code PIN ou code secret Worx, 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.

Si les utilisateurs s'authentifient en mode hors connexion, le code PIN Worx est validé localement et les utilisateurs sont autorisés à accéder à l'application ou au contenu demandé. Si les utilisateurs s'authentifient en ligne, le code PIN ou code secret Worx est utilisé pour déverrouiller le mot de passe Active Directory ou le certificat qui est ensuite envoyé à des fins d'authentification auprès de XenMobile.

Valeurs possibles : true ou false

Valeur par défaut : false

ENABLE_PASSWORD_CACHING

Nom complet : 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 Worx. 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

ENCRYPT_SECRETS_USING_PASSCODE

Nom complet : 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).

Citrix vous recommande d'activer cette clé de manière à fournir une sécurité plus élevée sur les appareils des utilisateurs.

Remarque : l'activation de cette clé affecte l'expérience utilisateur car le nombre d'invites de saisie du code PIN Worx est plus important.

Valeurs possibles : true ou false

Valeur par défaut : false

PASSCODE_TYPE

Nom complet : Type de code PIN Worx

Cette clé définit si les utilisateurs peuvent définir un code PIN Worx numérique ou un code secret Worx alphanumérique. Lorsque vous sélectionnez la valeur Numérique, l'utilisateur peut définir uniquement un code PIN Worx numérique. Lorsque vous sélectionnez la valeur Alphanumérique, l'utilisateur peut utiliser une combinaison de lettres et de chiffres pour le code secret Worx.

Remarque : lorsque vous modifiez le paramètre, les utilisateurs sont invités à créer un nouveau code PIN ou code secret Worx la prochaine fois qu'ils sont invités à s'authentifier.

Valeurs possibles : Numeric ou Alphanumeric

Valeur par défaut : Numeric

PASSCODE_STRENGTH

Nom complet : Exigences en matière de sûreté du code PIN Worx

Cette clé définit le niveau de sécurité du code PIN ou code secret Worx. Lorsque vous modifiez ce paramètre, les utilisateurs sont invités à définir un nouveau code PIN ou code secret Worx la prochaine fois qu'ils sont invités à s'authentifier.

Valeurs possibles : Low, Medium ou Strong

Valeur par défaut : Medium

Le tableau suivant décrit les règles de mot de passe pour chaque paramètre de sécurité en fonction du paramètre que vous sélectionnez pour PASSCODE_TYPE :

Sécurité du code secret	Règles pour code secret numérique	Règles pour code secret alphanumérique
Faible	Sont autorisés tous les nombres et toute séquence	Doit contenir au moins un nombre et une lettre. Non autorisé : AAAaaa, aaaaaa, abcdef Autorisé : aa11b1, Abcd1 Ab123 ~#,,, aa11aa aaaa11
Taille moyenne (Valeur par défaut)	1. Tous les nombres ne peuvent pas être identiques. Par exemple, 444444 n'est pas autorisé. 2. Tous les nombres ne peuvent pas être consécutifs. Par exemple, 123456 ou 654321 n'est pas autorisé. Autorisé : 444333, 124567, 136790, 555556, 788888	En plus des règles de sécurité de niveau Low pour un code secret : 1. Les lettres et tous les nombres ne peuvent pas être identiques. Par exemple, aaaa11, aa11aa ou aaa111 ne sont pas autorisés. 2. Les lettres et les nombres ne peuvent pas être consécutifs. Par exemple, abcd12, bcd123, 123abc, xy1234, xyz345 ou cba123 ne sont pas autorisés. Autorisé : aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~
Strong	Identique au niveau de sécurité Medium du code secret Worx.	Le code secret doit contenir au moins un nombre, un symbole spécial, une lettre majuscule et une lettre minuscule. Non autorisé : abcd12, Abcd12, dfgh12, jkrtA2 Autorisé : Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#

PASSCODE_MIN_LENGTH

Nom complet : Exigences en matière de longueur du code PIN Worx

Cette clé définit la longueur minimum des codes secrets Worx.

Valeurs possibles : 1-99

Valeur par défaut : 6

PASSCODE_EXPIRY

Nom complet : Exigences en matière d'expiration du code PIN Worx

Cette clé définit la durée (en jours) pendant laquelle le code PIN ou code secret Worx est valide, et après laquelle l'utilisateur est obligé de modifier son code PIN ou code secret Worx. Lorsque vous modifiez ce paramètre, la nouvelle valeur est définie uniquement lorsque le code PIN ou code secret Worx de l'utilisateur expire.

Valeurs possibles : 1 ou supérieure, mais la plage 1-99 est recommandée

Valeur par défaut : 90

Remarque : si vous voulez que les utilisateurs n'aient jamais à réinitialiser leur 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 expireront toujours à la fin de la période initiale mais plus jamais après.

PASSCODE_HISTORY

Nom complet : Historique du code PIN Worx

Cette clé définit le nombre de codes PIN ou codes secrets Worx précédemment utilisés que les utilisateurs ne sont pas autorisés à réutiliser lorsqu'ils changent leur code PIN ou code secret Worx. Lorsque vous modifiez ce paramètre, la nouvelle valeur est définie la prochaine fois que les utilisateurs réinitialisent leur code PIN ou code secret Worx.

Valeurs possibles : 1-99

Valeur par défaut : 5

INACTIVITY_TIMER

Nom complet : 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 Worx. Pour activer ce paramètre pour une application MDX, vous devez définir le paramètre App Passcode sur On. Si le paramètre App Passcode est défini sur Off, les utilisateurs sont redirigés vers Worx Home 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.

Remarque : sur iOS, le délai d'inactivité gère également l'accès à Worx Home et pas seulement aux applications MDX.

Valeurs possibles : tout entier positif

Valeur par défaut : 15

DISABLE_LOGGING

Nom d'affichage : Disable logging

Cette clé vous permet de désactiver la possibilité pour les utilisateurs de collecter et de télécharger des journaux à partir de leurs appareils. La journalisation est désactivée pour Worx Home et pour toutes les applications MDX installées. Les utilisateurs ne peuvent pas envoyer de journaux d'application à partir de la page Support ; bien que la boîte de dialogue de composition d'un message s'affiche, les journaux ne sont pas joints et un message indique que la journalisation est désactivée. Outre l'incidence de cette clé sur les appareils des utilisateurs, vous ne pouvez pas modifier les paramètres de journal dans la console XenMobile pour les applications Worx Home et MDX.

Lorsque cette clé est définie sur true, Worx Home définit la stratégie Bloquer les journaux d'application sur true afin que 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

Cette clé active ou désactive les rapports de plantage à l'aide des applications Crashlytics for Worx.

Valeurs possibles : true ou false

Valeur par défaut : true

DEVICE_LOGS_TO_IT_HELP_DESK

Nom d'affichage : envoyer les journaux de l'appareil au service d'assistance

Cette clé active ou désactive la possibilité d'envoyer des journaux au service d'assistance informatique.

Valeurs possibles : true ou false

Valeur par défaut : false

ON_FAILURE_USE_EMAIL

Nom d'affichage : En cas d'échec, utiliser la messagerie pour envoyer les journaux de l'appareil au service d'assistance

Cette clé 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_MAX_ATTEMPTS

Nom complet : Nombre maximal de tentatives de saisie du code PIN Worx

Cette clé définit le nombre de tentatives de saisie infructueuses du code PIN ou code secret Worx que les utilisateurs peuvent effectuer avant d'être invités à fournir une authentification complète. Une fois que les utilisateurs ont effectué une authentification complète, ils sont invités à créer un nouveau code PIN ou code secret Worx.

Valeurs possibles : tout entier positif

Valeur par défaut : 15

ENABLE_TOUCH_ID_AUTH

Nom complet : Activer l'authentification TouchID

Cette clé active ou désactive la possibilité des appareils (équipés de la fonctionnalité) d'utiliser la fonction d'authentification TouchID. Les appareils des utilisateurs doivent disposer d'un code PIN Worx activé et l'entropie utilisateur doit être définie sur false afin qu'ils soient invités à utiliser TouchID lorsqu'ils lancent une application.

Valeurs possibles : true ou false

Valeur par défaut : false

ENABLE_WORXHOME_GA

Nom d'affichage : activer Google Analytics dans WorxHome

Cette clé active ou désactive la possibilité de collecter des données à l'aide de Google Analytics dans Worx Home. Lorsque vous modifiez ce paramètre, la nouvelle valeur est appliquée la prochaine fois que l'utilisateur se connecte à WorxHome.

Valeurs possibles : true ou false

Valeur par défaut : true

Paramètres du serveur XenMobile

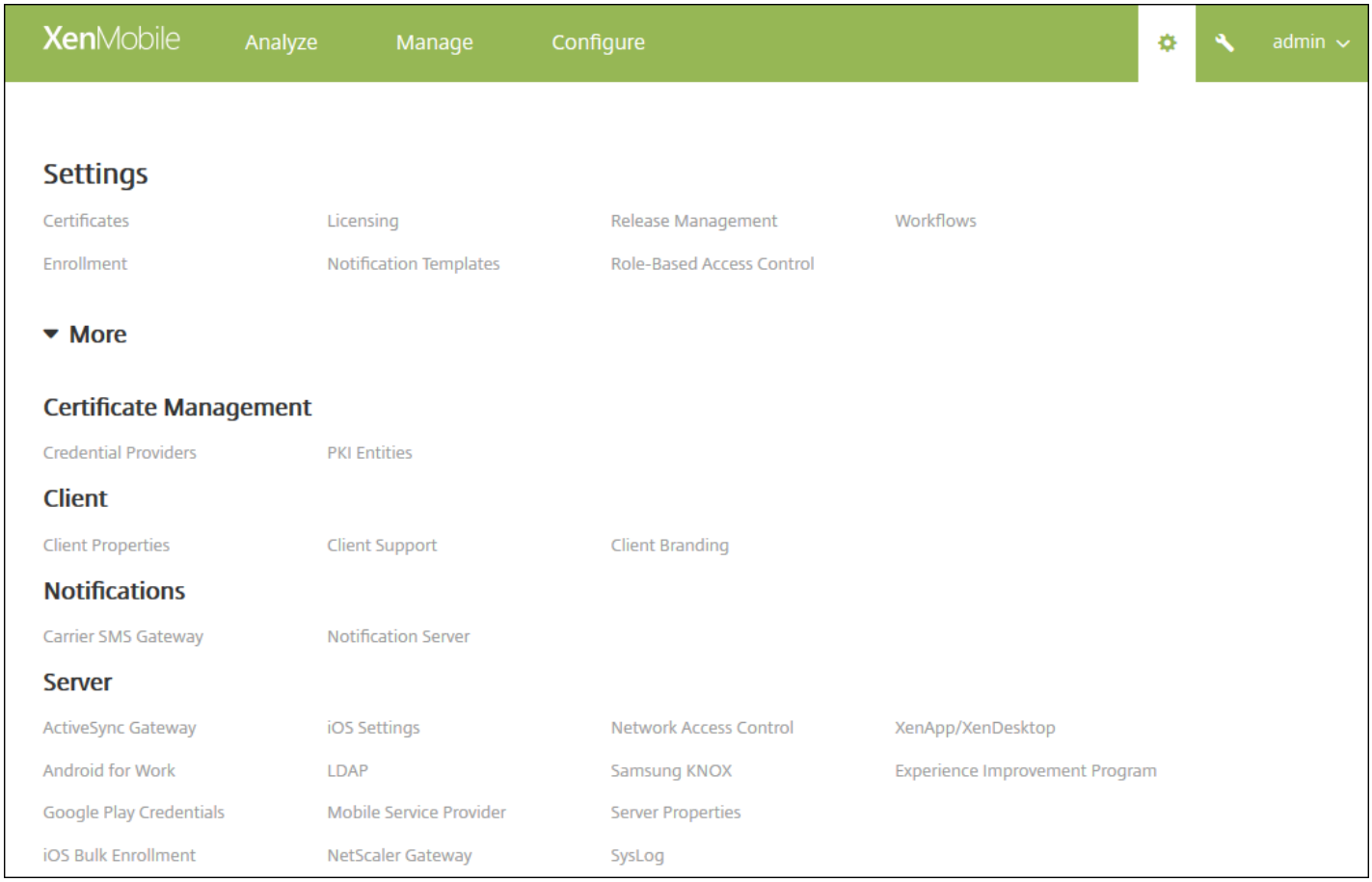
Jul 27, 2016

Les paramètres du serveur XenMobile que vous configurez dans la console XenMobile comprennent :

- ActiveSync Gateway
- Android for Work
- Programme d'amélioration de l'expérience
- Informations d'identification Google Play
- Inscription en bloc iOS
- Paramètres iOS
- LDAP
- Microsoft Azure
- Fournisseur de services mobiles
- NetScaler Gateway
- Contrôle d'accès réseau
- Samsung KNOX
- Propriétés du serveur
- SysLog
- XenApp/XenDesktop

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 l'option que vous souhaitez configurer.



ActiveSync Gateway dans XenMobile

Jul 27, 2016

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. En fonction de ces règles, des appareils peuvent être autorisés ou non 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.

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 : il s'agit de l'action par défaut pour ActiveSync Gateway. Elle crée une liste de tous les appareils qui ne répondent à aucun des autres 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.

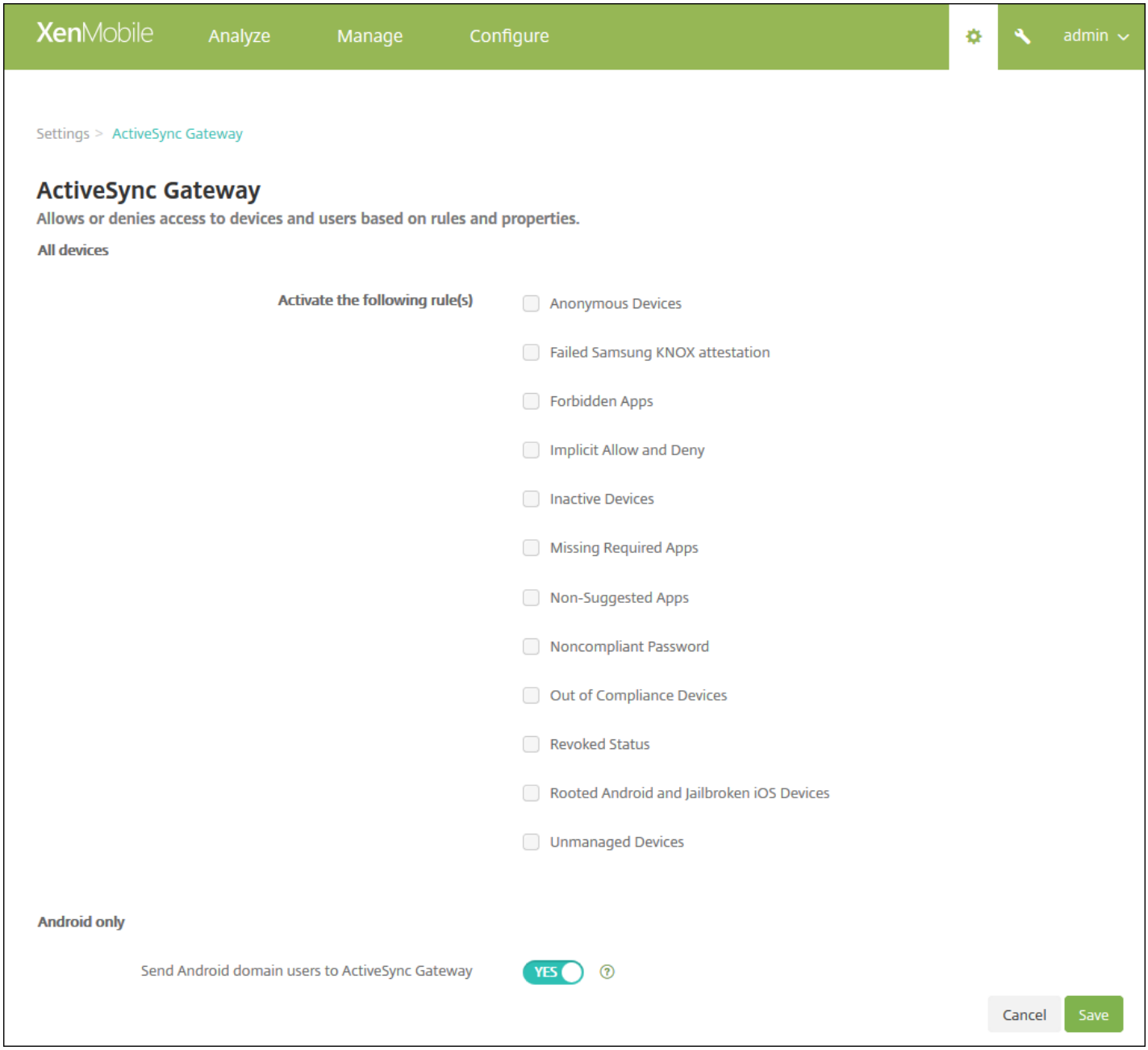
Appareils non gérés : vérifie si un appareil est toujours dans un état géré, sous le contrôle de XenMobile. Par exemple, un appareil exécuté en mode MAM ou un appareil désinscrit n'est pas géré.

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. Lorsque cette option est activée, elle garantit que XenMobile envoie les informations de l'appareil Android à ActiveSync Gateway au cas où XenMobile ne disposerait pas de l'identificateur ActiveSync de l'utilisateur de cet appareil Android.

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.



3. Dans **Activer la ou les règles suivantes**, sélectionnez une ou plusieurs règles à activer.

4. 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.

5. Cliquez sur **Enregistrer**.

Informations d'identification Google Play

Aug 22, 2016

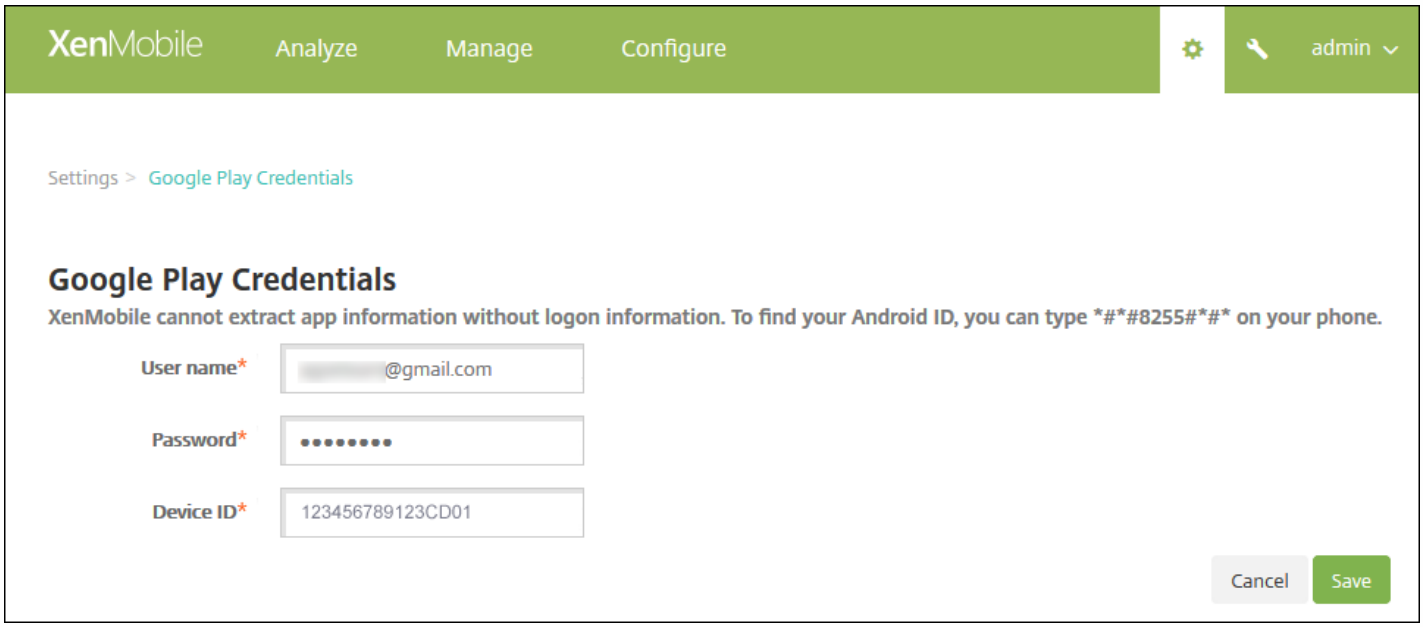
XenMobile utilise les informations d'identification Google Play pour extraire les informations applicatives pour l'appareil.

Remarque : pour trouver votre ID Android, entrez *#*#8255#*#*sur votre téléphone. Si le code ne révèle pas l'ID de l'appareil sur votre type d'appareil, il est possible d'utiliser une application tierce d'ID d'appareil pour obtenir l'ID d'appareil. L'ID que vous devez obtenir est l'ID Google Services Framework portant le label GSF ID.

Important : pour permettre à XenMobile d'extraire les informations de l'application, vous devrez peut-être configurer votre compte Gmail pour autoriser les connexions non sécurisées. Pour obtenir des instructions détaillées, consultez le site de support de Google .

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 **Identifiants Google Play**. La page **Identifiants Google Play** s'affiche.



3. Configurez les paramètres suivants :

- **Nom d'utilisateur**: entrez le nom associé au compte Google Play.
- **Mot de passe** : entrez le mot de passe de l'utilisateur.
- **ID de l'appareil** : entrez votre ID Android.
  Entrez *#*#8255#*#*sur votre téléphone pour déterminer l'ID Android.

3. Cliquez sur **Enregistrer**.

Inscription en bloc d'appareils iOS

Jul 27, 2016

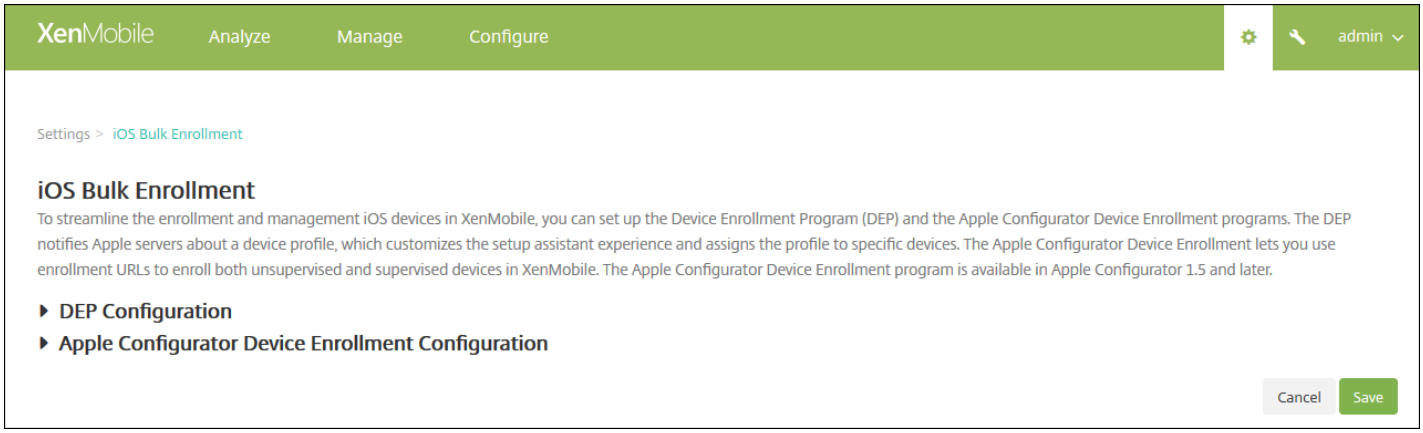
Vous pouvez inscrire un grand nombre d'appareils iOS dans XenMobile de deux façons. Vous pouvez utiliser le Device Enrollment Program (DEP) d'Apple pour inscrire les appareils que vous achetez directement auprès d'Apple ou d'un revendeur ou opérateur agréé Apple, ou vous pouvez utiliser Apple Configurator pour inscrire des appareils qu'ils aient été achetés ou non directement auprès d'Apple.

Avec le programme DEP, vous n'avez aucune tâche de préparation à effectuer sur les appareils ; vous envoyez les numéros de série des appareils ou les numéros de commande via le programme DEP et les appareils sont configurés et inscrits dans XenMobile. Une fois les appareils inscrits, ils sont prêts à l'emploi et peuvent être distribués aux utilisateurs. Par ailleurs, lorsque vous configurez des appareils avec le programme DEP, 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 de plus amples informations sur la configuration du programme DEP, reportez-vous à la page Device Enrollment Program d'Apple.

Avec Apple Configurator, vous associez des appareils à un ordinateur Apple exécutant OS X 10.7.2 ou version ultérieure et à l'application Apple Configurator. Vous préparez les appareils et configurez des stratégies à l'aide de Apple Configurator. Après avoir provisionné les appareils avec les stratégies requises, la première fois que les appareils se connectent à XenMobile, les stratégies sont appliquées et vous pouvez commencer à gérer les appareils. Pour de plus amples informations sur l'aide de Apple Configurator, consultez la page Apple Configurator d'Apple.

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 **Inscription en bloc iOS**. La page **Inscription en bloc iOS** s'affiche.



Si vous configurez les paramètres du programme DEP, veuillez consulter la section Configuration des paramètres du programme DEP ; si vous configurez les paramètres d'Apple Configurator, veuillez consulter la section Configuration des paramètres d'Apple Configurator.

Avant de continuer, vous devez avoir créé un compte Apple DEP sur deploy.apple.com. Après avoir créé un compte DEP, configurez un serveur MDM virtuel pour autoriser les communications entre XenMobile et Apple. Pour ce faire, vous devez charger une clé publique XenMobile sur le site d'Apple. Lorsque Apple reçoit la clé publique, il renvoie un jeton de serveur que vous importez dans XenMobile. Suivez ces étapes pour établir la connexion entre XenMobile et Apple.

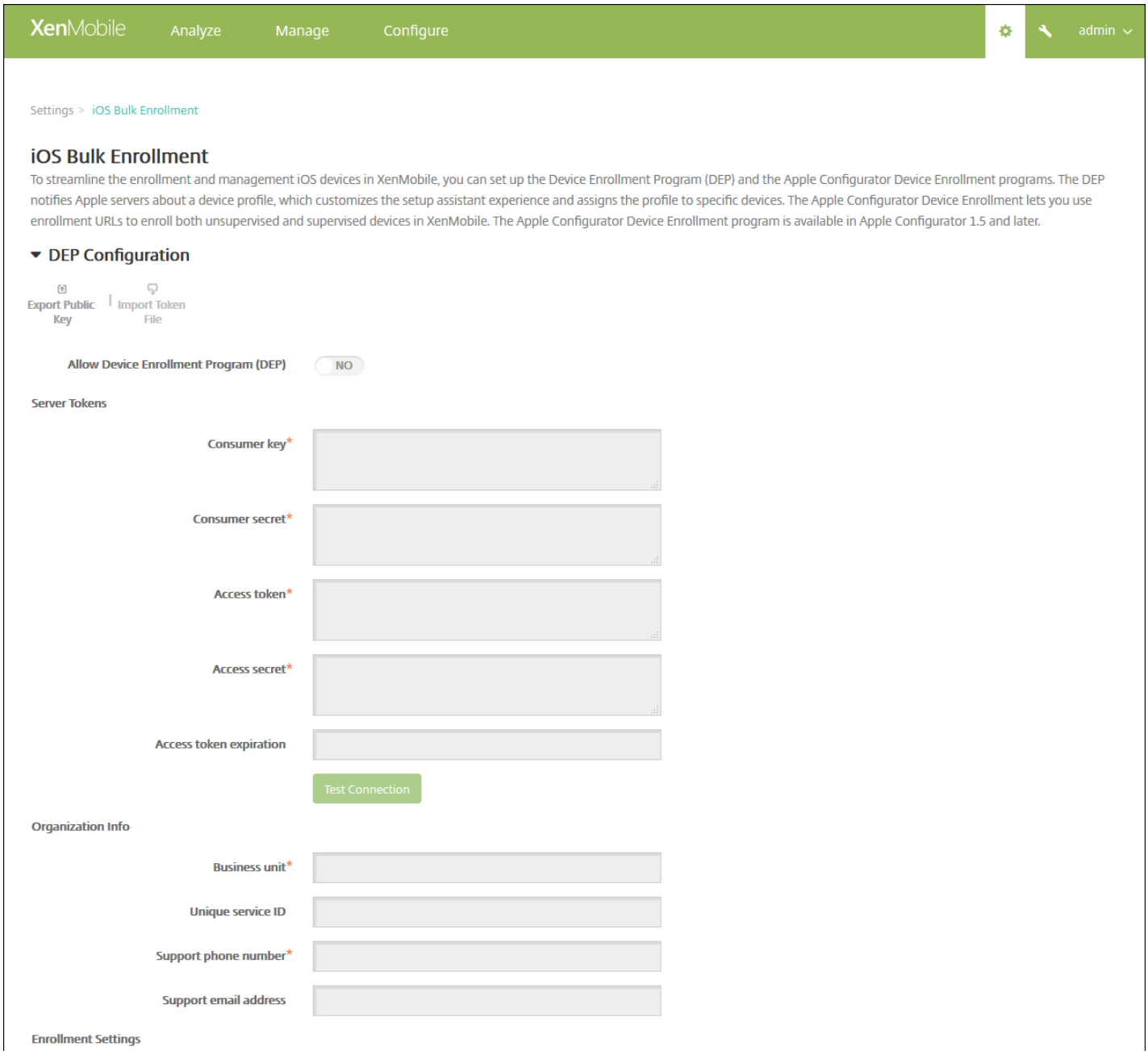
1. Pour obtenir la clé publique à charger sur Apple, sur la page **Inscription en bloc iOS**, développez **Configuration DEP**, cliquez sur **Exporter la clé publique** et enregistrez le fichier sur votre ordinateur.

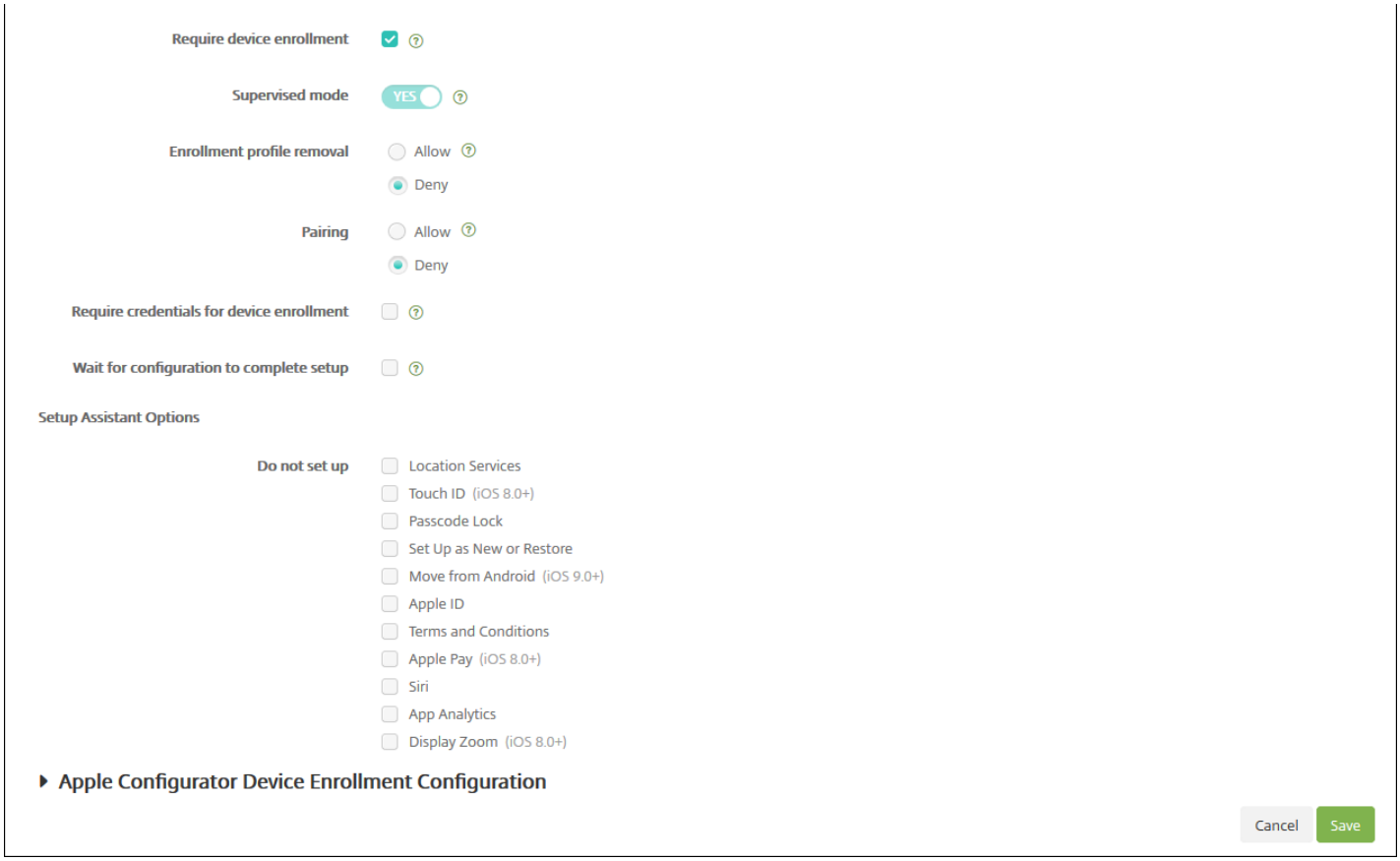
2. Accédez à deploy.apple.com, connectez-vous à votre compte DEP et suivez les instructions pour configurer un serveur MDM. Dans le cadre de ce processus, Apple fournit un jeton de serveur.

3. Sur la page **Inscription en bloc iOS**, cliquez sur **Importer un fichier jeton** pour ajouter le jeton de serveur Apple à XenMobile.

4. Le champ **Jetons de serveur** est renseigné automatiquement dès que le fichier de jeton est chargé sur XenMobile.

5. Cliquez sur **Tester la connectivité** pour confirmer que XenMobile et Apple peuvent communiquer. Si le test de la connexion échoue, vérifiez que vous avez bien ouvert tous les ports requis car ce type de problème est à l'origine de la plupart des échecs. Pour de plus amples informations sur les ports qui doivent être ouverts dans XenMobile, consultez la section Configuration requise pour les ports.





6. Configurez les paramètres suivants pour terminer la configuration DEP :

Informations sur l'organisation

- **Division** : entrez la division ou le département à laquelle ou auquel l'appareil est attribué. Ce champ est obligatoire.
- **ID de service unique** : entrez un ID unique (facultatif).
- **Numéro de téléphone de l'assistance** : entrez un 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** : entrez une adresse e-mail d'assistance (facultatif).

Paramètres d'inscription

- **Exiger l'inscription des appareils** : sélectionnez cette option pour obliger les utilisateurs à inscrire leurs appareils. Par défaut, l'inscription est exigée.
- **Mode supervisé** : doit être défini sur **Oui** si vous utilisez Apple Configurator pour gérer les appareils inscrits à DEP ou lorsque **Attendre la fin de l'installation** est activé. 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.
- **Suppression du profil d'inscription** : indiquez si vous souhaitez autoriser les appareils à utiliser un profil qui peut être supprimé à distance. La valeur par défaut est **Refuser**.
- **Couplage** : sélectionnez cette option pour autoriser les appareils inscrits par le biais du programme DEP à être gérés via iTunes et Apple Configurator. La valeur par défaut est **Refuser**.
- **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 de DEP. Cette option est disponible pour

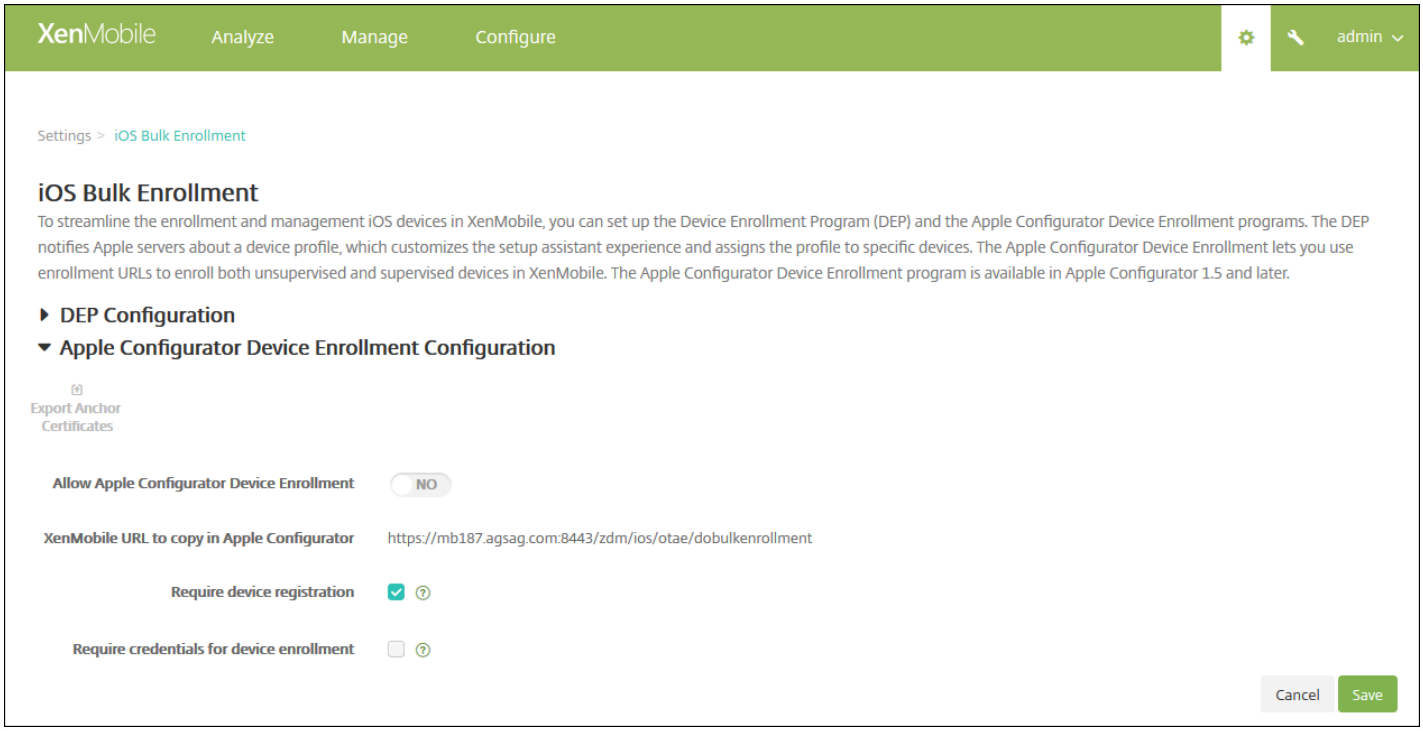
iOS 7.1 et version supérieure. **Remarque** : lorsque DEP est activé lors de la première configuration et que vous ne sélectionnez pas cette option, les composants DEP, tels que l'utilisateur DEP, Worx Home, l'inventaire logiciel et le groupe de déploiement DEP sont créés dès le début. Si vous sélectionnez cette option, les composants ne sont pas créés tant que l'utilisateur n'a pas entré ses informations d'identification. Par conséquent, si vous désactivez cette option ultérieurement, les utilisateurs qui n'ont pas entré leurs informations d'identification ne peuvent pas s'inscrire au programme DEP, car ces composants DEP n'existent pas. Pour ajouter les composants DEP, dans ce cas, il est conseillé de désactiver et d'activer le compte DEP.

- **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. Cette option est disponible sur les appareils iOS 9.0 et versions ultérieures en mode supervisé.
  - **Remarque** : 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

Installation

Sélectionnez les étapes de l'Assistant d'installation iOS que vos utilisateurs ne devront *pas* utiliser (étapes à ignorer) lorsqu'ils démarreront leurs appareils pour la première fois.

- **Services de localisation** : configurez le service de localisation sur l'appareil.
- **Touch ID** : configurez Touch ID dans iOS 8.0 et versions ultérieures.
- **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 copie de sauvegarde d'iCloud ou d'iTunes.
- **Déplacer depuis Android** : activez le transfert des données à partir d'un appareil Android vers un appareil iOS 9 ou version ultérieure. 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.
- **Termes et conditions** : exigez que l'utilisateur accepte les termes et conditions pour utiliser l'appareil.
- **Apple Pay** : configurez Apple Pay dans iOS 8.0 et versions ultérieures.
- **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 8.0 et versions ultérieures.



1. Développez **Configuration du DEP Apple Configurator**.

2. Définissez **Activer l'inscription d'appareils dans Apple Configurator** sur **Oui**.

3. Notez et configurez les paramètres suivants :

- **URL XenMobile à copier dans Apple Configurator** : ce champ en lecture seule est l'adresse URL du serveur XenMobile qui communique avec Apple, et que vous copiez et collez dans Apple Configurator ultérieurement. Dans Apple Configurator 2, l'adresse URL d'inscription est le nom de domaine complet (FQDN) ou l'adresse IP du serveur XenMobile, comme mdm.server.url.com.
- **Exiger l'inscription de l'appareil** : la sélection de ce paramètre nécessite que vous ajoutiez les appareils configurés sur l'onglet **Appareils** dans XenMobile manuellement ou via un fichier CSV avant de pouvoir les inscrire. Cela permet de garantir qu'aucun appareil inconnu ne peut s'inscrire. La valeur par défaut est de demander l'ajout d'appareils.
- **Exiger des informations d'identification pour l'inscription de l'appareil** : exigez que les utilisateurs d'appareils iOS 7.1 et versions ultérieures entrent leurs informations d'identification lors de l'inscription. Par défaut, les informations d'identification ne sont pas exigées.

> ## Remarque
>
> Si le serveur XenMobile utilise un certificat SSL approuvé, passez à l'étape suivante.

4. Cliquez sur **Exporter les certificats d'ancrage** et enregistrez le fichier certchain.pem dans le trousseau OS X (connexion ou System).

5. Démarrez Apple Configurator et accédez à **Prepare -> Setup -> Configure Settings.**

6. Dans le paramètre **Device Enrollment**, collez l'URL du serveur MDM de l'étape 4 dans le champ **MDM server URL** du

Configurator.

7. Dans le paramètre **Device Enrollment**, copiez l'autorité de certification racine et l'autorité de certification des serveurs SSL sur les certificats **Anchor**, si XenMobile n'utilise pas un certificat SSL approuvé.

8. Utilisez un câble Dock Connector vers USB pour connecter des appareils au Mac exécutant Apple Configurator pour 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.

9. Cliquez sur **Prepare**. Pour plus d'informations sur la préparation d'appareils avec Apple Configurator, consultez la page d'aide d'Apple Configurator Prepare devices.

10. Dans Apple Configurator, configurez les stratégies dont vous avez besoin.

11. À mesure que chaque appareil est préparé, activez-le pour démarrer l'Assistant d'installation iOS, qui prépare l'appareil pour la première utilisation.

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 DEP d'Apple et XenMobile lorsque vous renouvelez ou mettez à jour le certificat SSL. Vous pouvez, cependant, reconfigurer vos paramètres DEP à tout moment en suivant les étapes précédentes dans cet article.

Pour plus d'informations sur le programme DEP d'Apple, consultez la documentation Apple.

Pour plus d'informations sur un problème connu et la solution de contournement associée à cette configuration, consultez la section Problèmes connus de XenMobile Server 10.3.

Déploiement d'appareils iOS via le programme DEP d'Apple

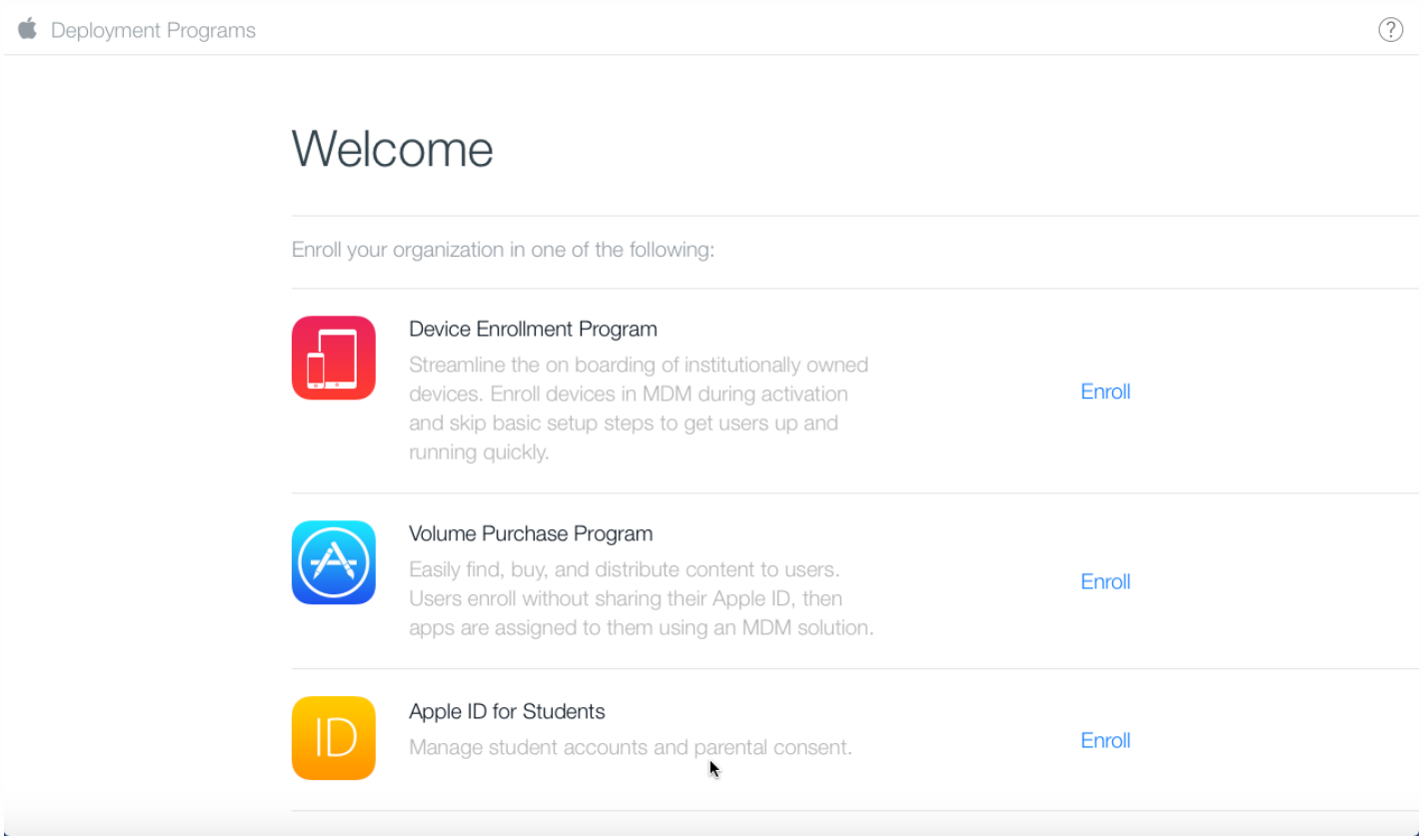
Jul 27, 2016

Vous avez besoin d'un compte Apple Developer Enterprise Program (DEP) pour bénéficier du programme DEP d'Apple pour inscrire et gérer des appareils iOS dans XenMobile. Les conditions principales que les organisations doivent respecter pour s'inscrire au programme DEP d'Apple sont les suivantes.

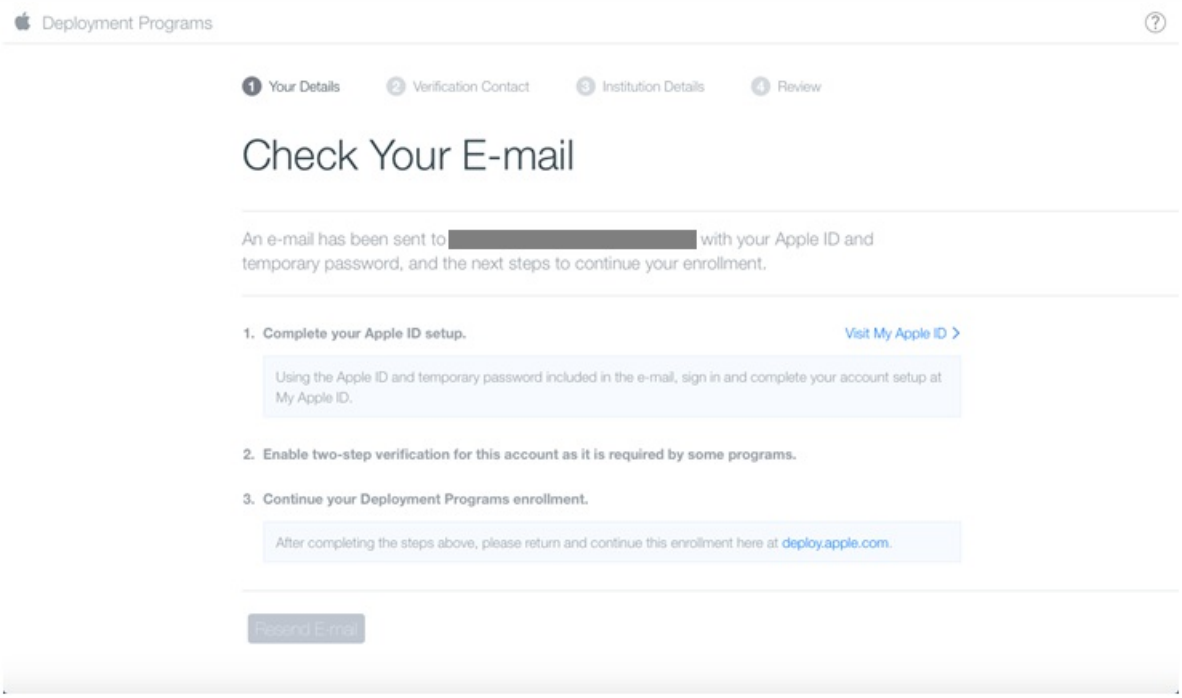
- Coordonnées professionnelles (adresse e-mail et numéro de téléphone)
- Contact pour validation
- Informations sur l'établissement (numéro DUNS / d'immatriculation fiscale)
- Numéro de client Apple

Pour de plus amples informations sur les détails du programme DEP d'Apple, consultez ce PDF d'Apple. Il est important de souligner que le programme DEP d'Apple est uniquement destiné aux organisations et non aux individus. Il est tout aussi important de savoir qu'un certain nombre de détails sur l'entreprise sont nécessaires pour créer un compte Apple DEP, par conséquent il peut s'écouler un certain temps entre la demande d'ouverture d'un compte et son approbation.

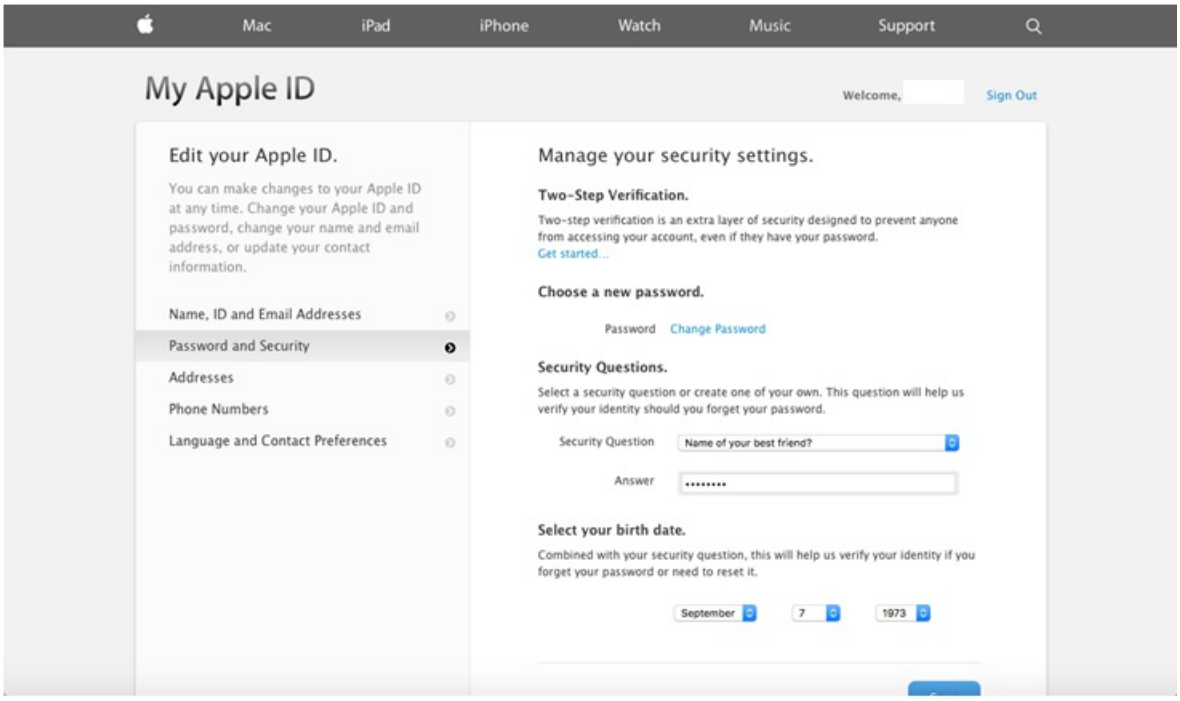
Lors de la demande d'ouverture d'un compte DEP, il est préconisé d'utiliser une adresse e-mail liée à l'organisation, telle que dep@société.com.



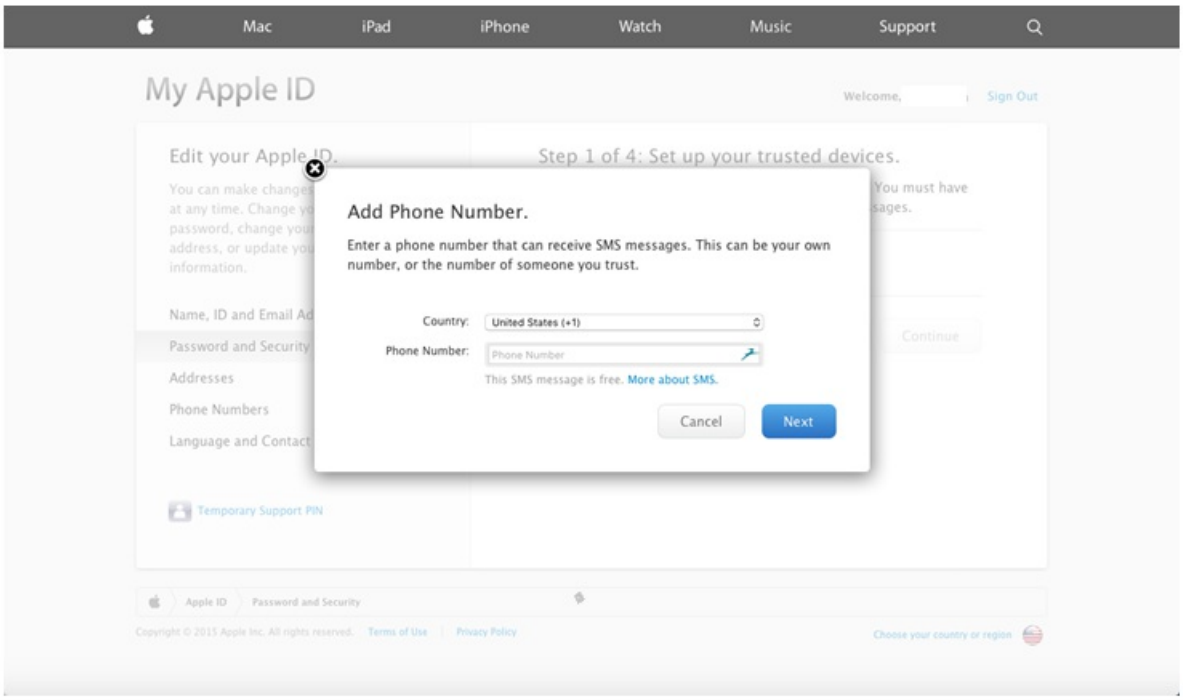
1. Après avoir entré les informations sur votre entreprise, vous allez recevoir par e-mail votre mot de passe temporaire ainsi qu'un nouvel identifiant Apple.



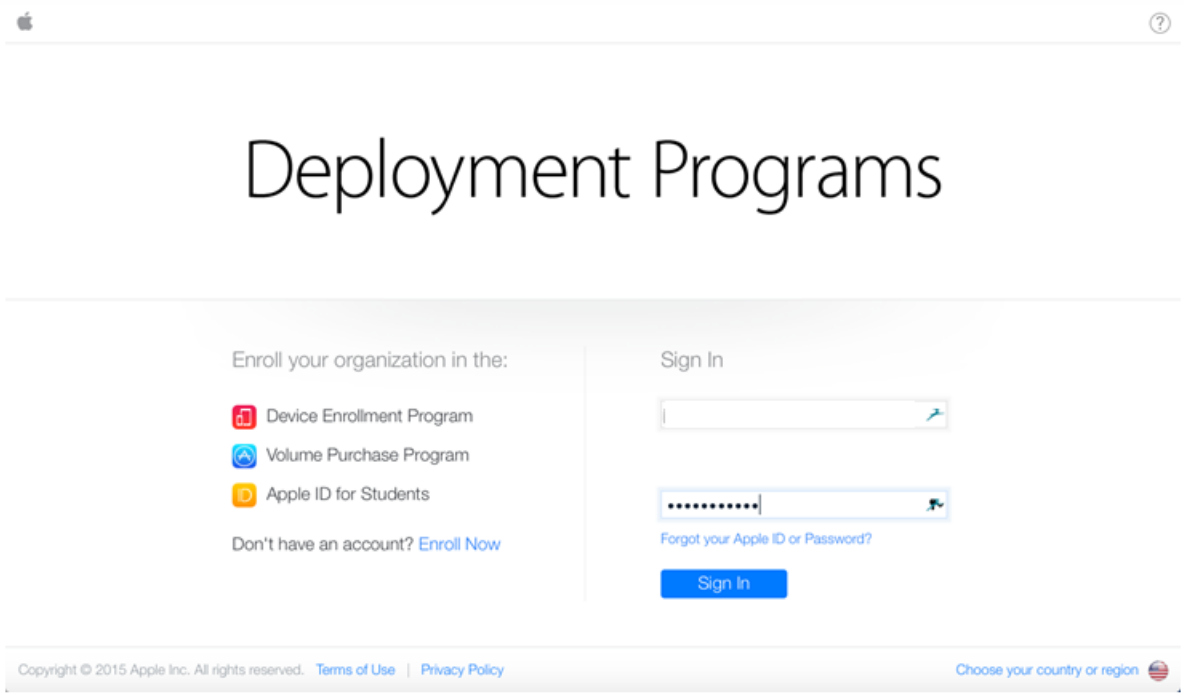
2. Connectez-vous à l'aide de cet identifiant Apple et configurez les paramètres de sécurité du compte.



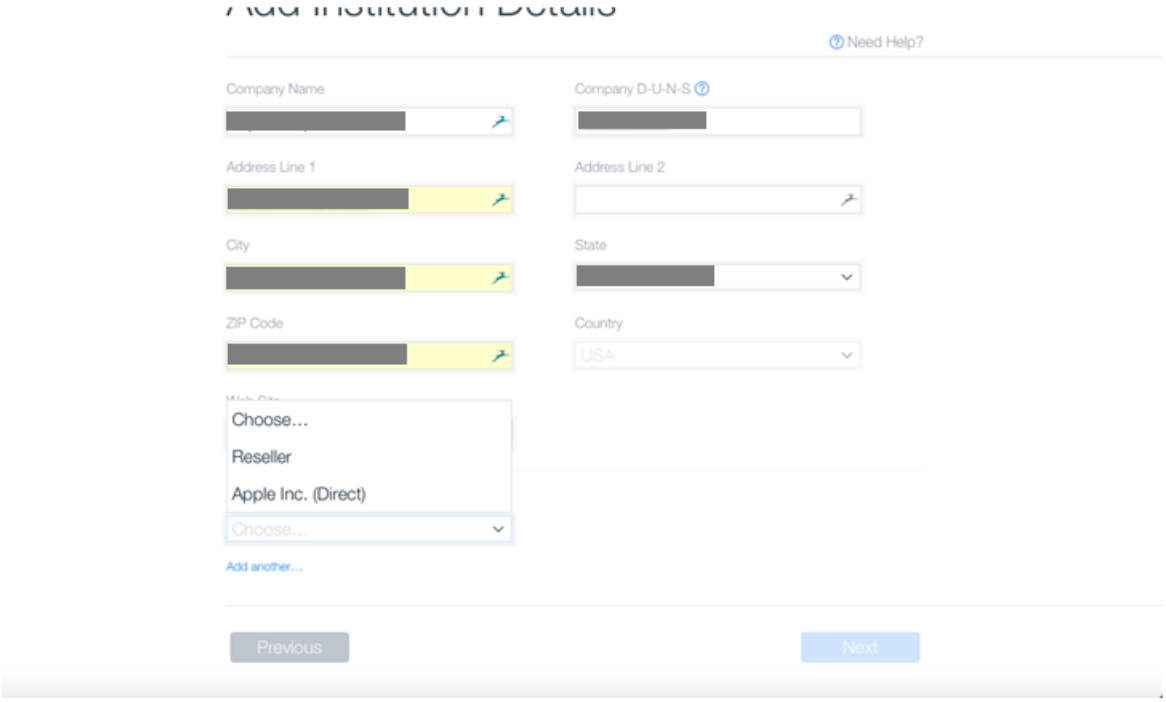
3. Configurez et activez la validation en deux étapes, ce qui est nécessaire pour utiliser le portail DEP. Durant ces étapes, vous ajoutez un numéro de téléphone par le biais duquel vous recevrez le code PIN à 4 chiffres requis pour la validation en deux étapes.



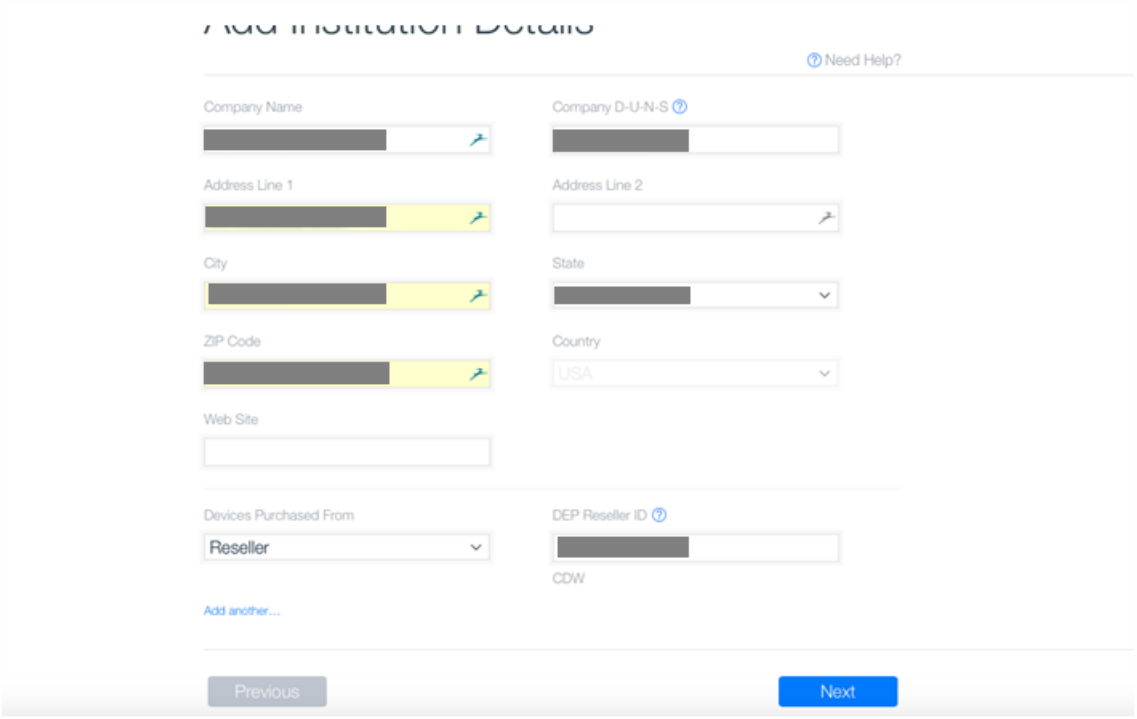
4. Connectez-vous au portail DEP pour terminer la configuration du compte à l'aide de la validation en deux étapes que vous venez de configurer.

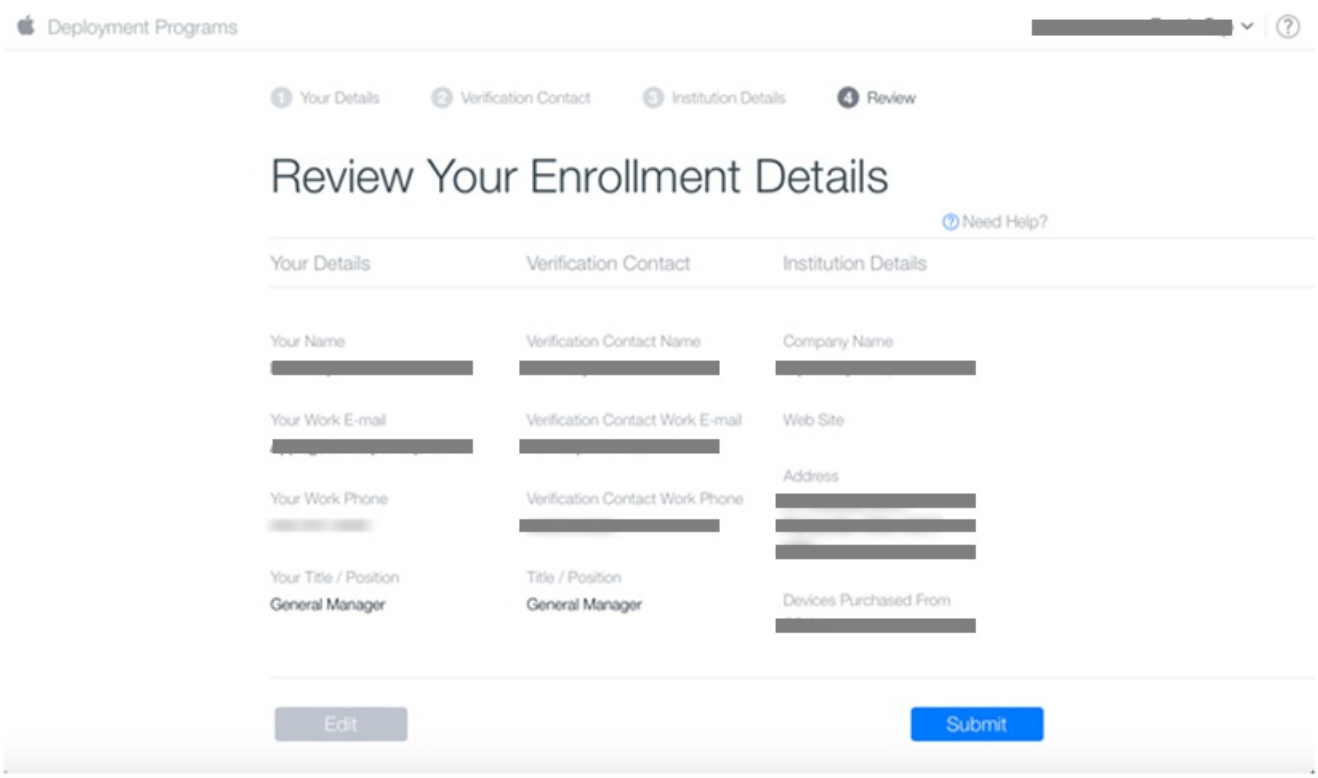


5. Ajoutez les détails de votre entreprise et sélectionnez là où vous avez acheté vos appareils. Pour de plus amples informations sur les options, consultez la section suivante, Commander des appareils compatibles avec le programme DEP.

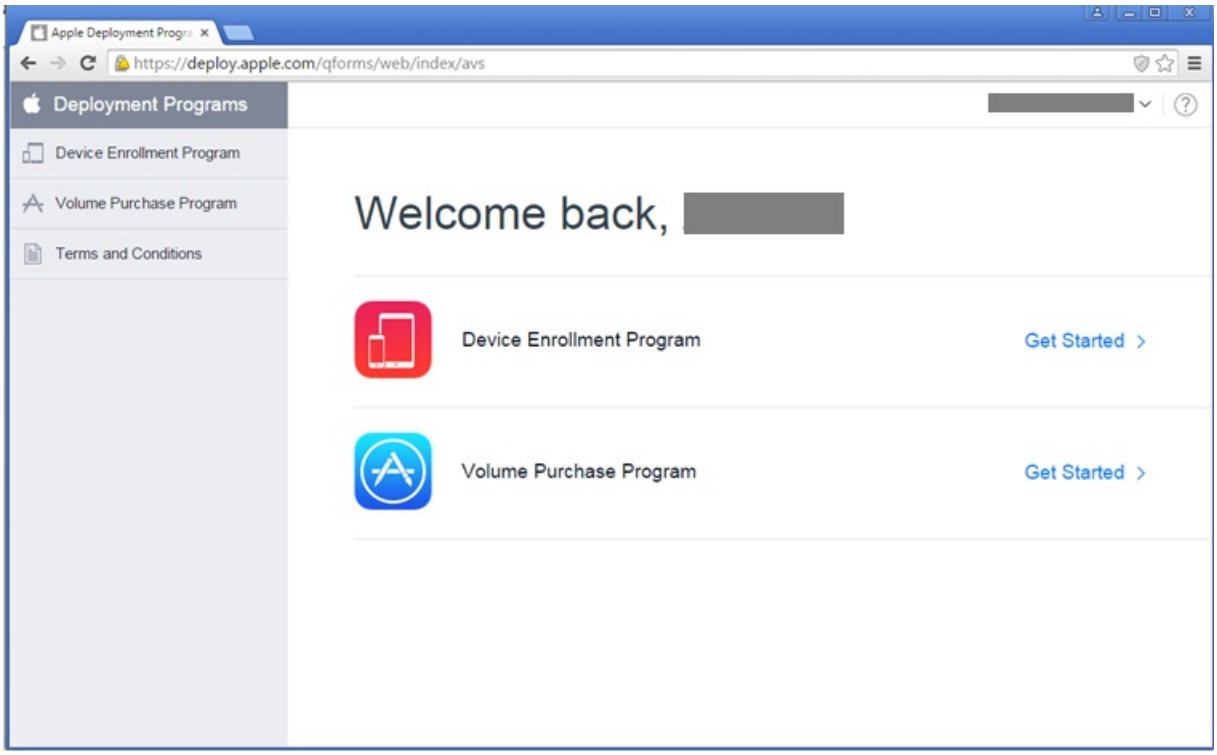


6. Ajoutez le numéro de client Apple ou l'ID du revendeur DEP, vérifiez vos détails d'inscription et attendez que Apple approuve votre compte.



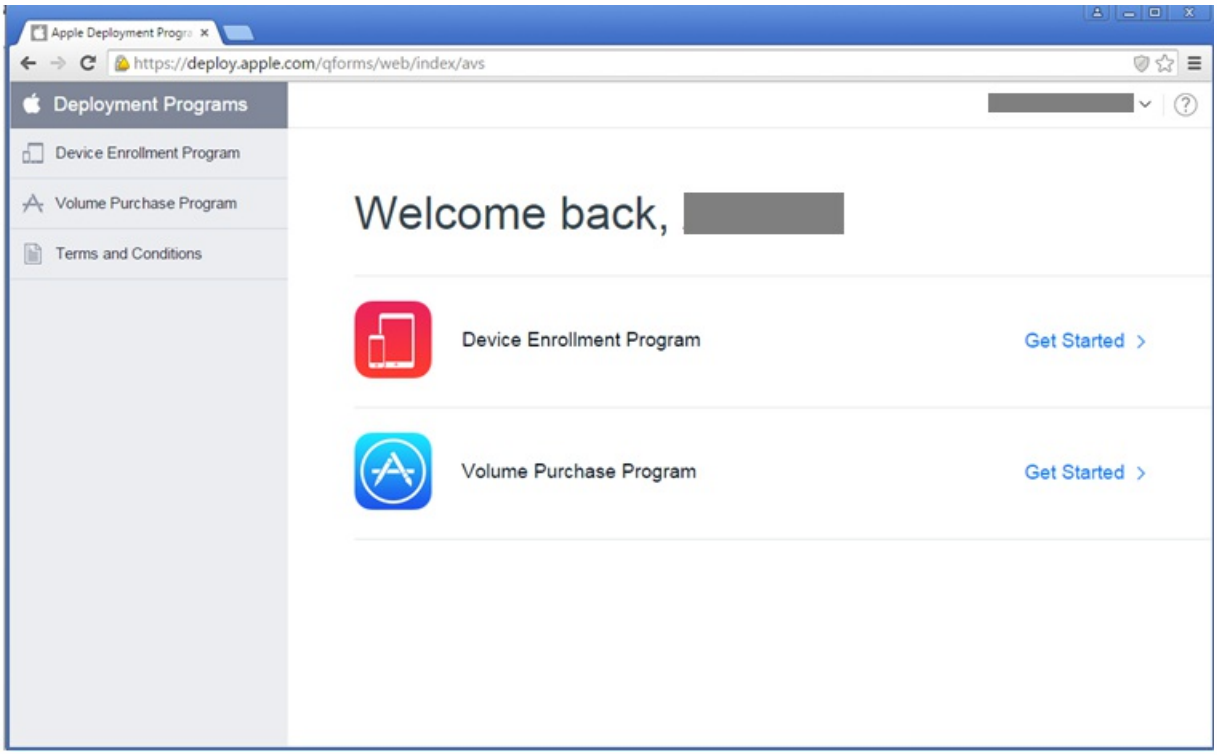


7. Après avoir reçu vos identifiants de connexion d'Apple, connectez-vous au portail DEP d'Apple. Suivez ensuite les étapes de la section suivante pour connecter votre compte avec XenMobile.

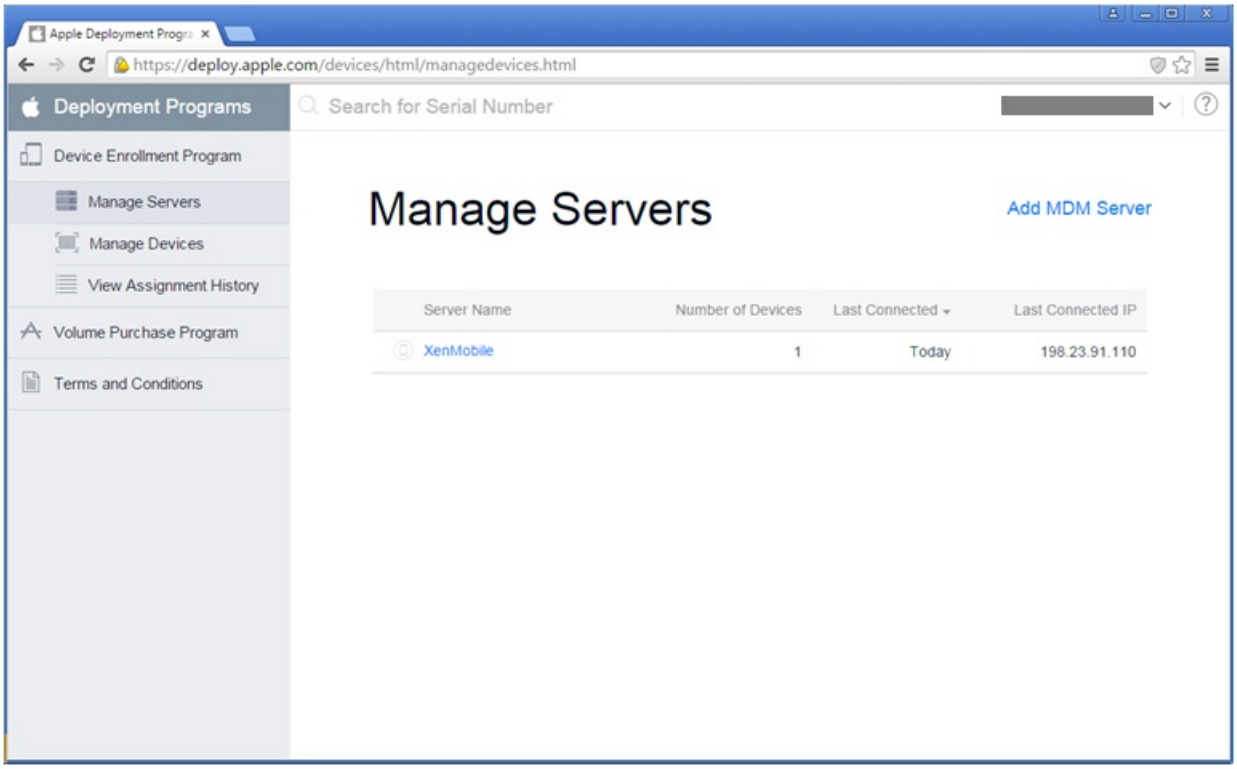


Suivez les étapes dans cette section pour connecter votre compte Apple DEP avec votre déploiement du serveur XenMobile.

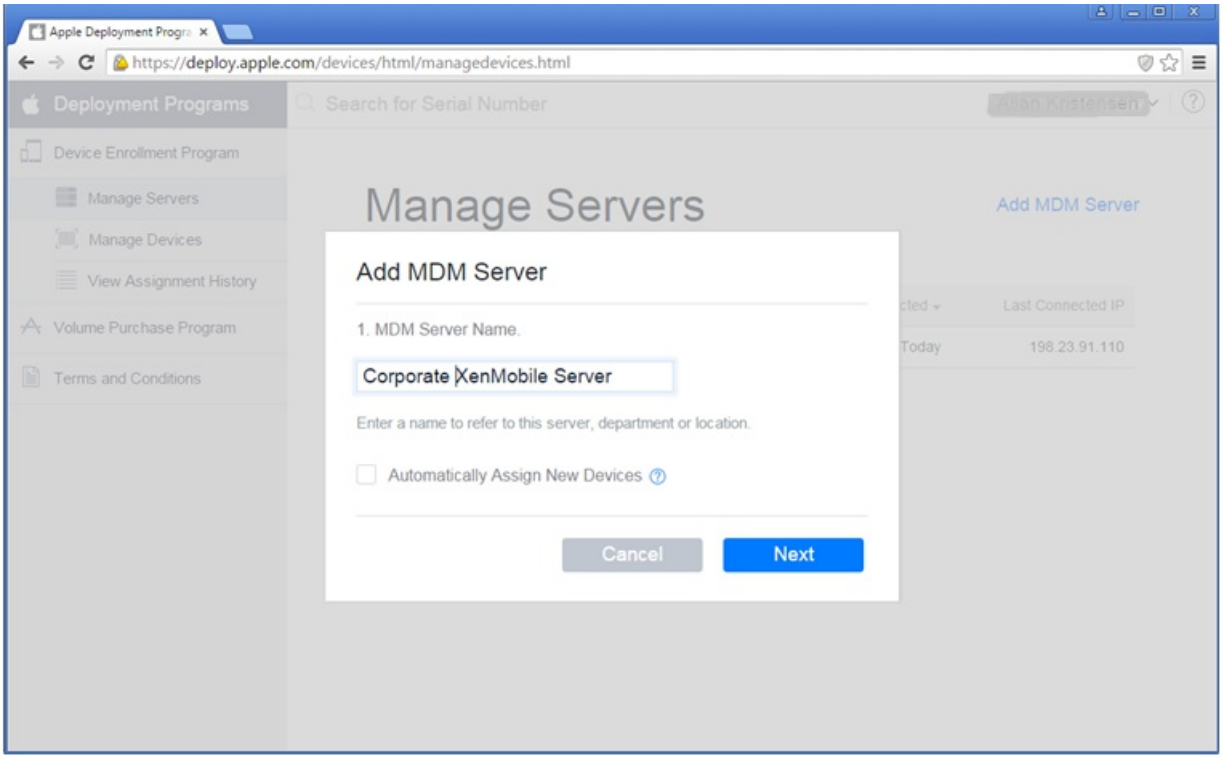
1. Sur le côté gauche du portail Apple DEP, cliquez sur **Programme d'inscription d'appareils**.



2. Cliquez sur **Gérer les serveurs** et sur le côté droit, cliquez sur **Ajouter un serveur MDM**.



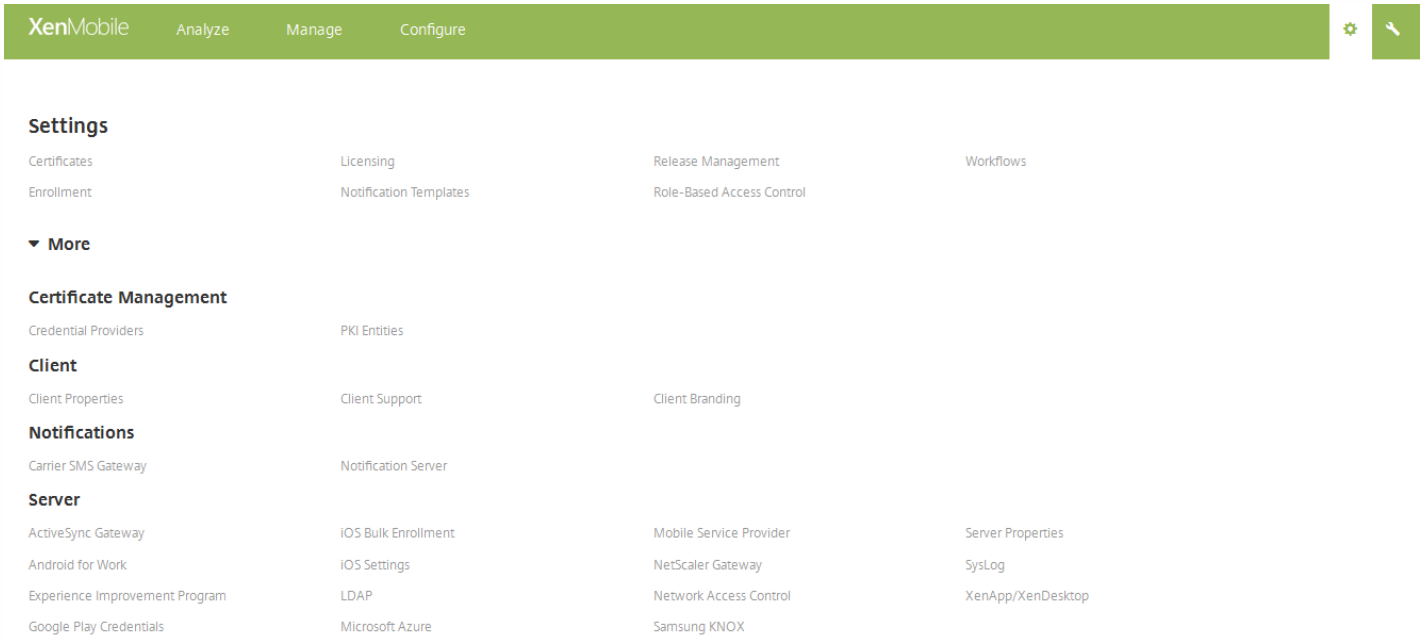
3. Dans **Ajouter un serveur MDM**, entrez un nom pour votre serveur XenMobile et cliquez sur **Suivant**.



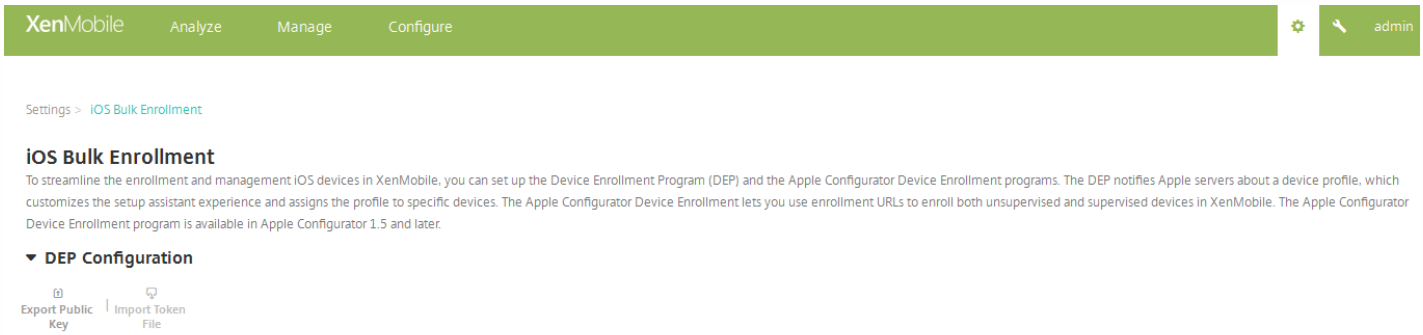
4. Chargez une clé publique depuis votre serveur XenMobile. Pour générer la clé depuis XenMobile, procédez comme suit :

    a. Connectez-vous à la console XenMobile et cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

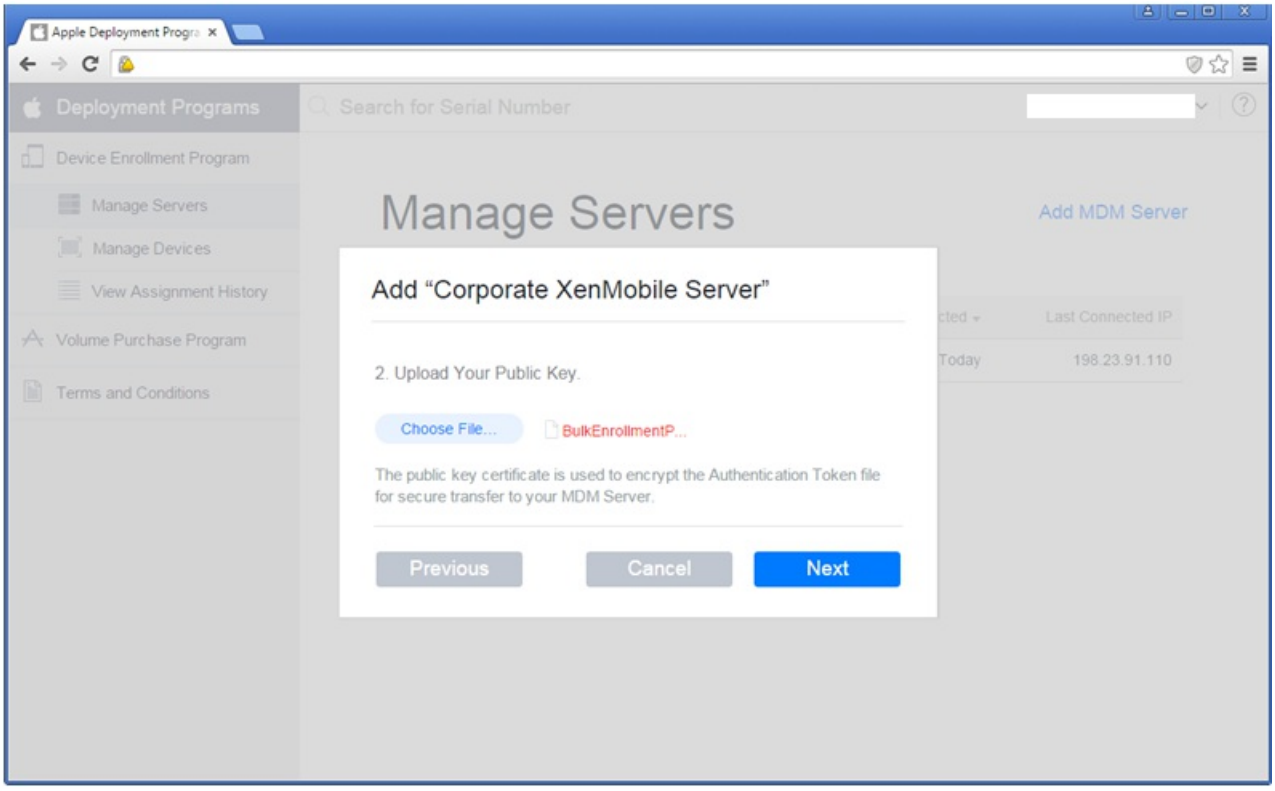
    b. Sous **Plus**, cliquez sur **Inscription en bloc iOS**.



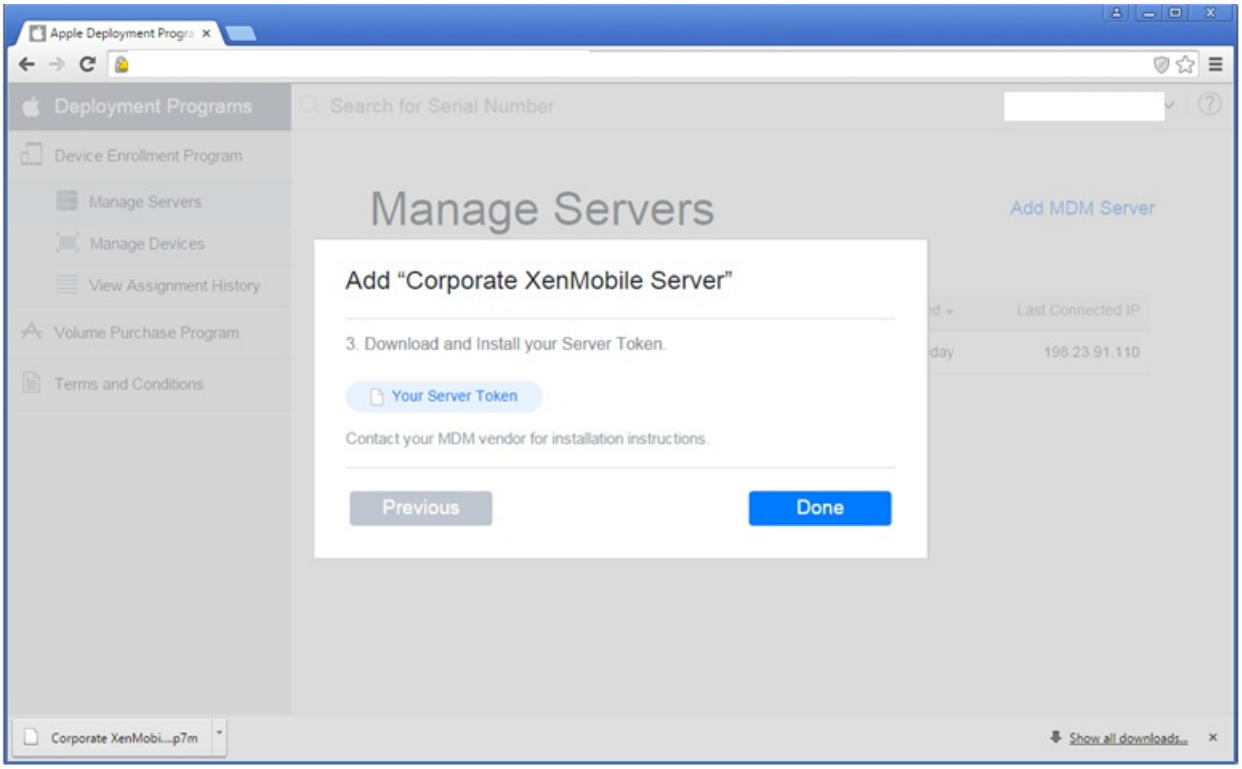
b. Sur la page **Inscription en bloc iOS**, développez **Configuration DEP** et cliquez sur **Exporter la clé publique**. La clé publique est téléchargée.



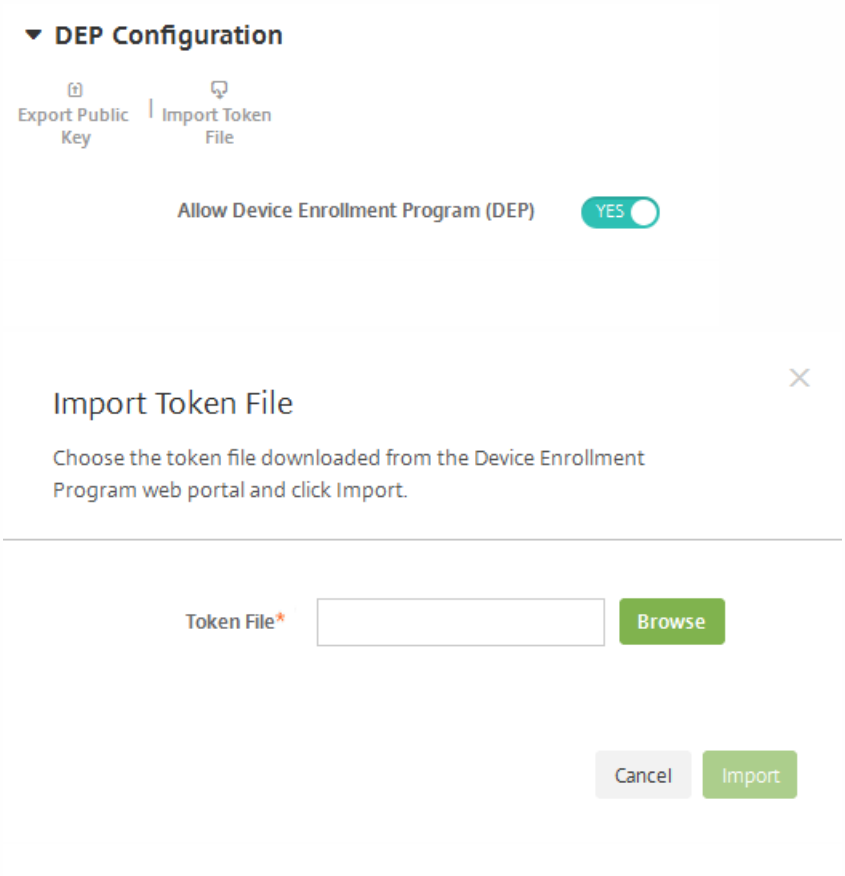
5. Sur le portail Apple DEP, cliquez **Choisir un fichier**, sélectionnez la clé publique que vous venez de télécharger et cliquez sur **Suivant**.



6. Cliquez sur **Votre jeton de serveur** pour générer un jeton de serveur, lequel est téléchargé depuis le navigateur, et cliquez sur **Terminé**.

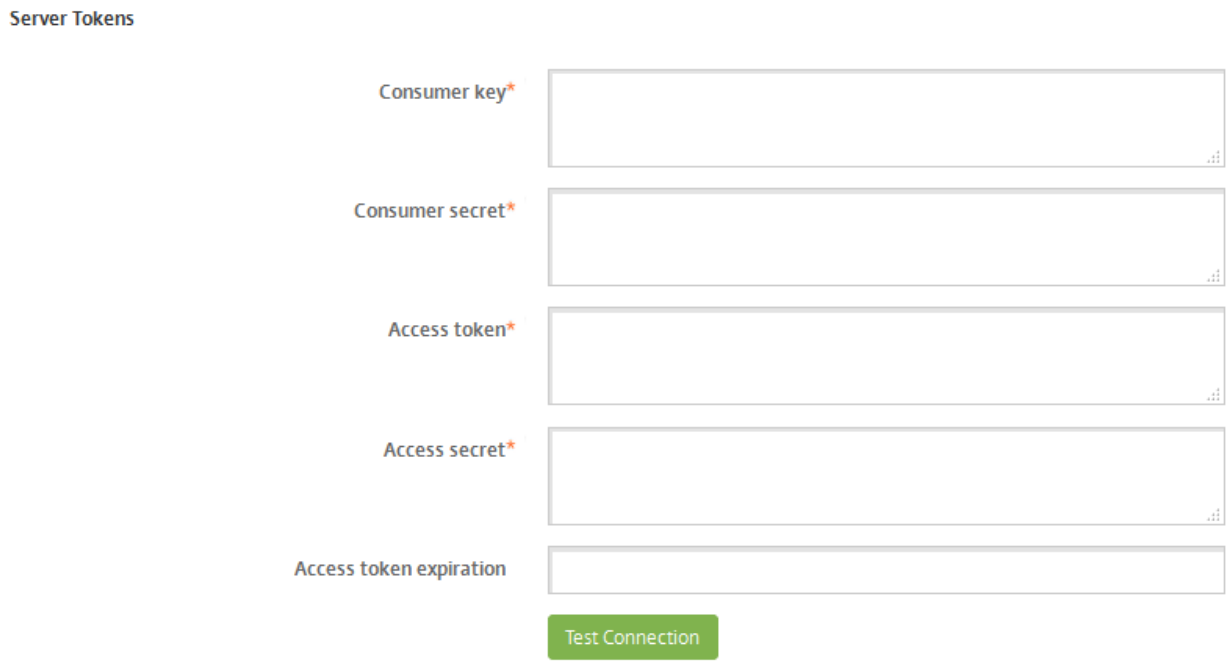


7. Sur la page **Inscription en bloc iOS** de la console XenMobile, en regard de **Autoriser Device Enrollment Program (DEP)**, cliquez sur OUI, cliquez sur **Importer un fichier jeton** et chargez le fichier jeton que vous avez téléchargé dans l'étape précédente.



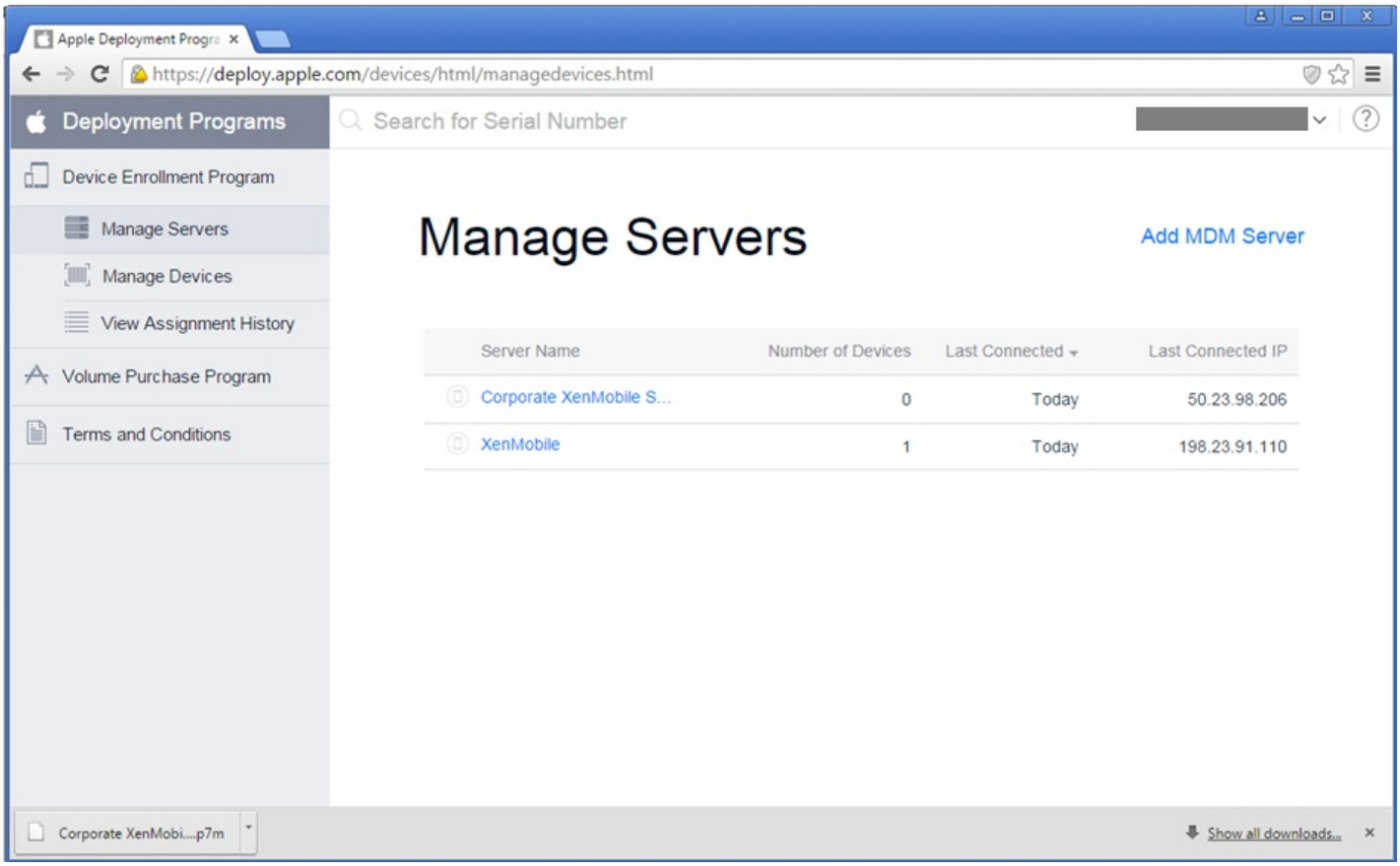
Les informations de votre jeton Apple DEP s'affichent dans la console XenMobile après l'importation du fichier de jeton.

8. Cliquez sur **Tester la connexion** pour vérifier la connexion du programme DEP d'Apple avec XenMobile.



9. Sur la page **Inscription en bloc iOS**, finalisez les paramètres supplémentaires, sélectionnez les contrôles et stratégies du programme DEP d'Apple que vous voulez implémenter sur les appareils inscrits auprès du programme DEP et cliquez sur **Enregistrer**.

Le serveur XenMobile s'affiche dans le portail DEP d'Apple.



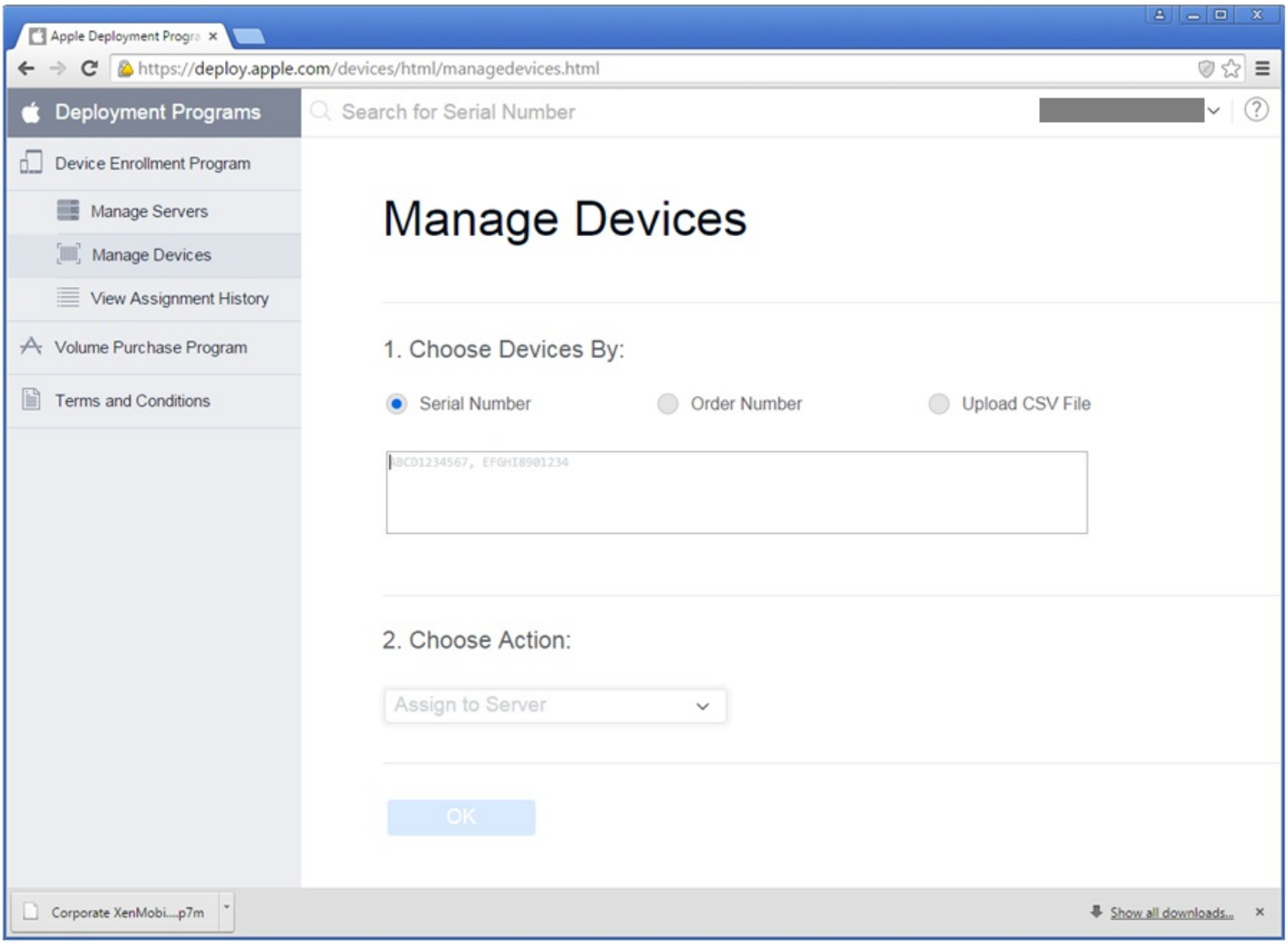
Vous pouvez commander des appareils compatibles avec le programme DEP directement auprès d'Apple ou de revendeurs ou opérateurs agrées. Pour commander directement auprès d'Apple, vous devez fournir votre numéro de client Apple dans le portail DEP pour permettre à Apple d'associer l'appareil acheté avec votre compte DEP Apple.

Pour commander auprès de votre revendeur ou d'un opérateur, contactez votre revendeur Apple ou opérateur pour savoir s'ils participent au programme DEP d'Apple. Lorsque vous achetez des appareils, demandez l'ID du programme DEP des revendeurs. Vous aurez besoin de ces informations pour ajouter votre revendeur DEP à votre compte Apple DEP. Une fois l'approbation obtenue, vous recevrez un ID de client DEP après avoir ajouté l'ID DEP Apple des revendeurs. Fournissez l'ID de client DEP au revendeur, qui utilisera l'ID pour soumettre les informations à propos des appareils que vous avez achetés à Apple. Pour plus d'informations, veuillez consulter ce site Web Apple.

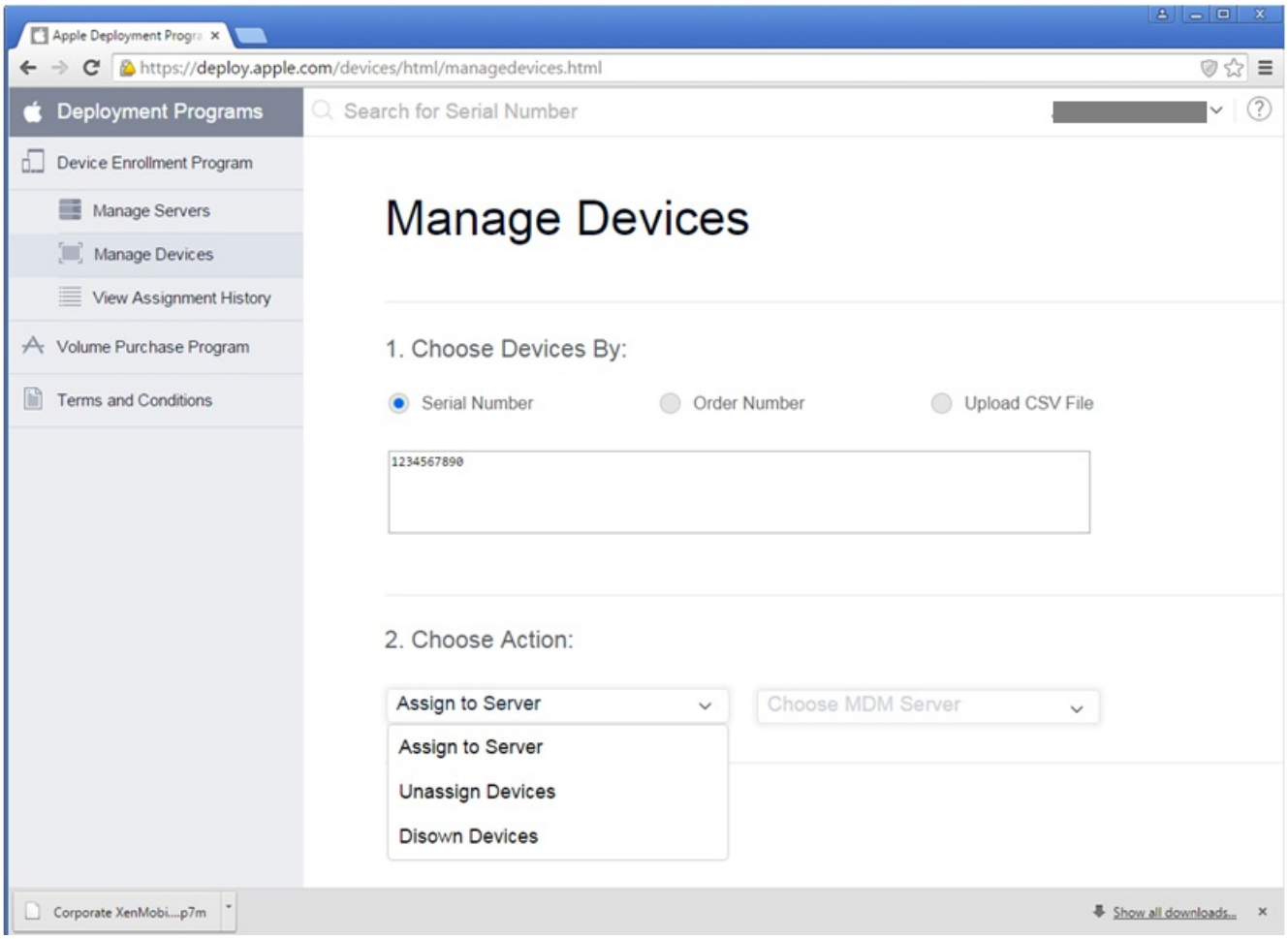
Suivez ces étapes pour associer des appareils avec votre serveur XenMobile dans votre compte Apple DEP via le portail DEP.

1. Connectez-vous au portail Apple DEP.

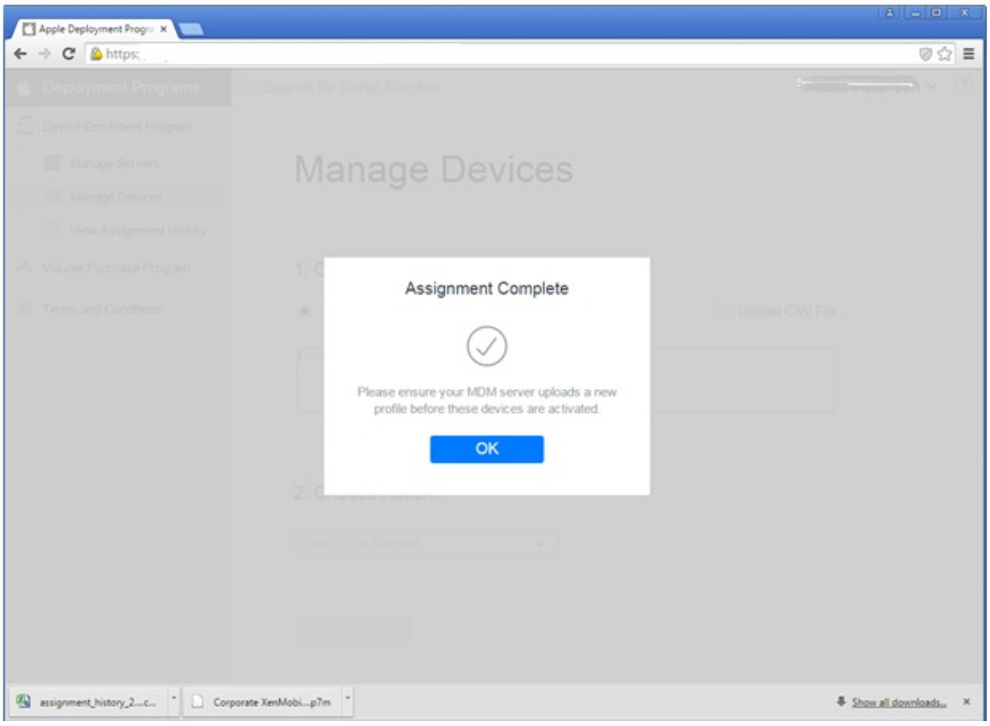
2. Cliquez sur **Programme d'inscription d'appareils**, sur **Gérer les appareils** et dans **Choisir des appareils**, sélectionnez l'option à utiliser pour charger et définir les appareils compatibles avec le programme DEP : **Numéro de série**, **Numéro de commande** ou **Télécharger un fichier CSV**.



3. Sous **Choisir une action**, pour attribuer vos appareils à un serveur XenMobile, cliquez sur **Attribuer au serveur**, et dans la liste, cliquez sur le nom de votre serveur XenMobile et cliquez sur **OK**.



Vos appareils DEP sont maintenant associés au serveur XenMobile sélectionné.



Lorsque les utilisateurs inscrivent un appareil au programme DEP d'Apple, ils suivent la procédure suivante.

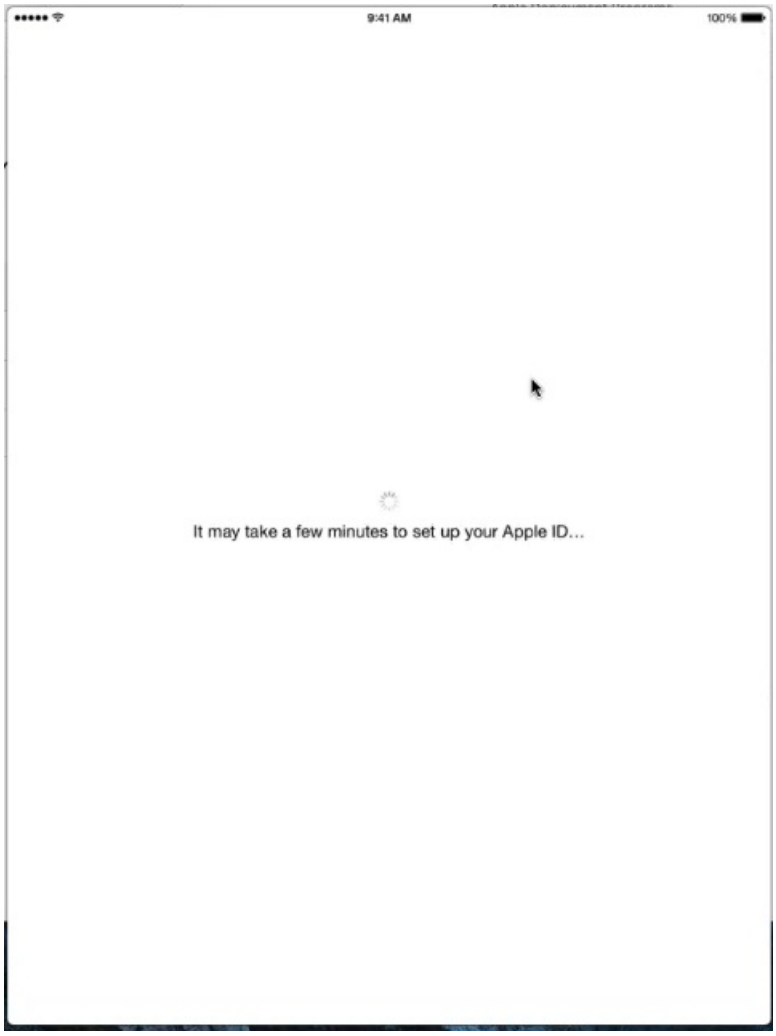
1. Ils démarrent leur appareil.

2. Ils utilisent l'assistant de configuration pour configurer les paramètres initiaux sur leur appareil iOS.

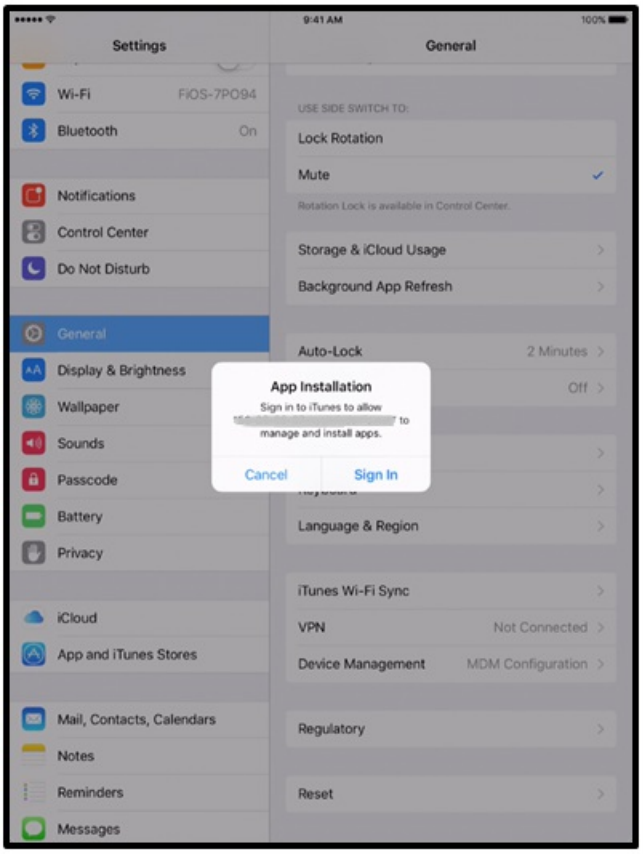
3. L'appareil démarre automatiquement le processus d'inscription d'appareils de XenMobile. Ils suivent l'assistant pour inscrire l'appareil auprès du serveur XenMobile associé à l'appareil compatible avec le programme DEP.

Le processus d'inscription auprès du programme DEP d'Apple démarre automatiquement dans le cadre du processus de configuration iOS initial des appareils compatibles avec le programme DEP.

4. La configuration DEP que vous avez configurée dans la console XenMobile est transmise à l'appareil. Les utilisateurs suivent l'assistant pour configurer l'appareil.



5. Il est possible qu'ils soient invités à se connecter à iTunes de façon à ce que Worx Home puisse être téléchargé.



6. Ils ouvrent Worx Home 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 Worx.

Le reste des applications requises est transmis à l'appareil.

Paramètres Programme d'achat en volume iOS

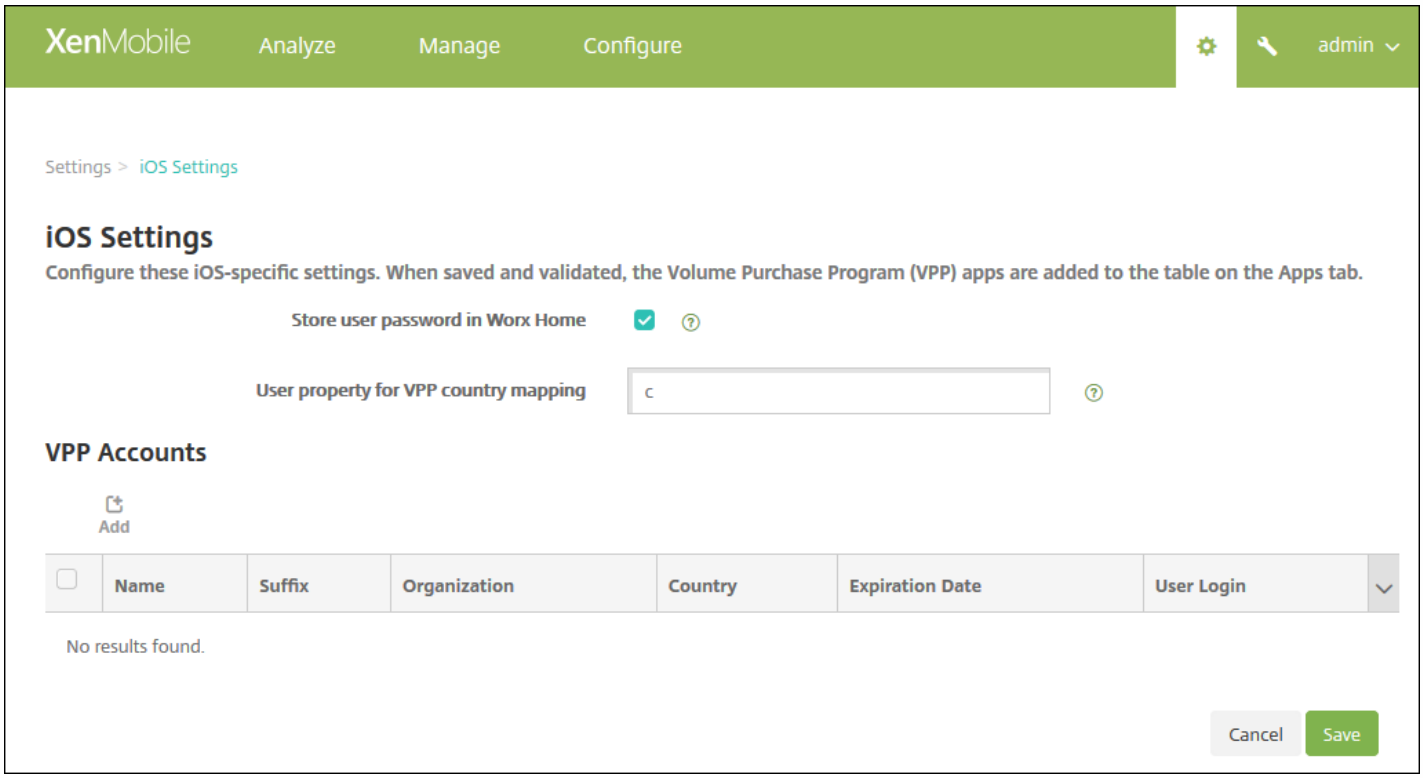
Jul 27, 2016

Vous pouvez configurer des paramètres spécifiques au Programme d'achat en volume iOS (VPP) dans XenMobile. Le programme VPP iOS simplifie la recherche, l'achat et la distribution d'applications en bloc pour une organisation. Le programme VPP fournit une solution simple et évolutive destinée à gérer les besoins en contenu de l'organisation.

Après avoir enregistré et validé les paramètres VPP iOS dans XenMobile, les applications achetées sont ajoutées au tableau de l'onglet Applications dans la console XenMobile.

1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Serveur**, cliquez sur **Paramètres iOS**. La page de configuration **Paramètres iOS** s'affiche.



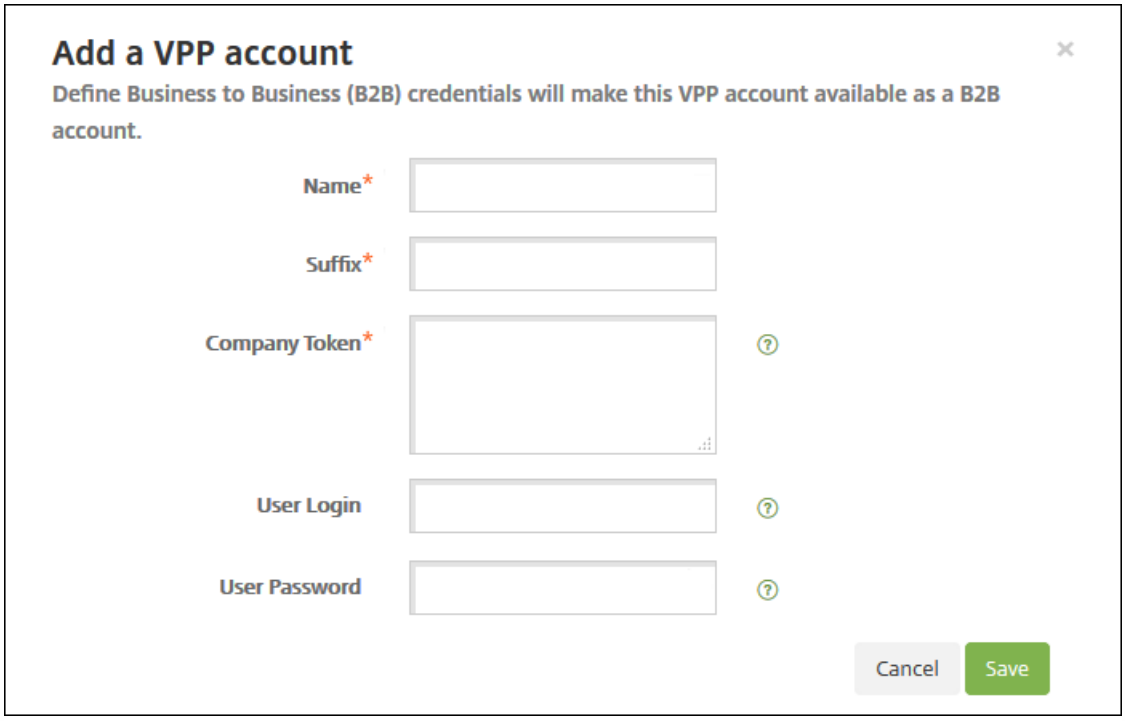
3. Configurez les paramètres suivants :

- **Stocker le mot de passe utilisateur dans Worx Home** : indiquez si un nom d'utilisateur et un mot de passe doivent être stockés de façon sécurisée dans Worx Home en vue de l'authentification sur XenMobile. Par défaut, les informations sont stockées.
- **Propriété utilisateur du choix de pays pour le Volume Purchasing Program (VPP)** : entrez un code pour autoriser les utilisateurs à télécharger des applications à partir de magasins d'applications spécifiques à un pays.

  Ce mappage est utilisé pour choisir le pool de propriété du code VPP. Par exemple, si la propriété de l'utilisateur est États-Unis, l'utilisateur ne peut pas télécharger d'applications si le code VPP de l'application est distribué au Royaume-Uni. Contactez votre administrateur de plan VPP pour plus d'informations sur le choix du code de pays.

Comptes VPP

- Pour chaque compte VPP que vous souhaitez ajouter, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un compte VPP** apparaît.



Configurez ces paramètres pour chaque compte à ajouter :

- **Nom** : entrez le nom du compte VPP.
- **Suffixe** : entrez le suffixe qui s'affiche sur les applications obtenues via le compte VPP.
- **Jeton d'entreprise** : entrez, ou copiez-collez, le jeton de service VPP obtenu auprès de Apple. Pour obtenir le jeton, dans la page de résumé de compte du portail Apple VPP, cliquez sur le bouton Télécharger pour générer et télécharger le fichier VPP. 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'utilisateurde compte VPP autorisé (facultatif).
- **Mot de passe utilisateur** : entrez un mot de passe utilisateur de compte VPP (facultatif).

5. Cliquez sur **Enregistrer** pour fermer la boîte de dialogue.

6. Cliquez sur **Enregistrer** pour enregistrer les paramètres iOS.

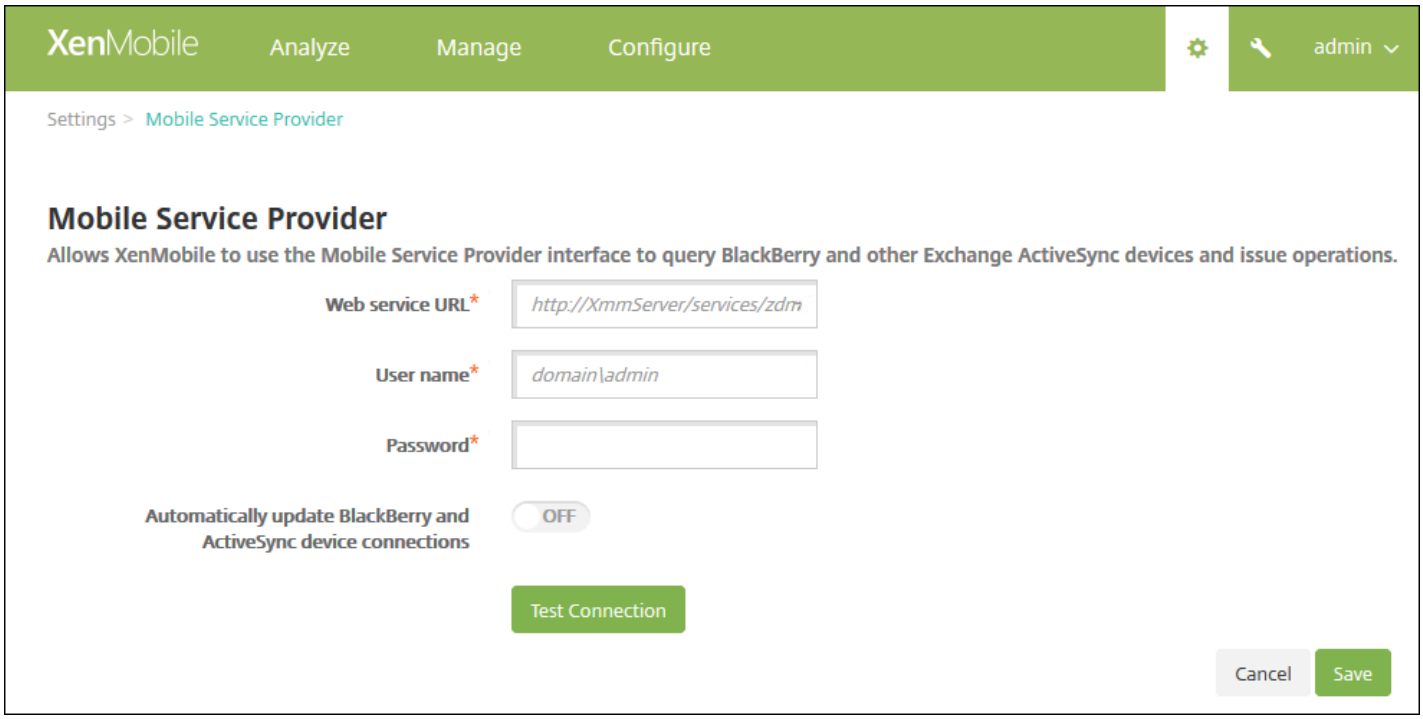
Fournisseur de services mobiles

Jul 27, 2016

Vous pouvez configurer XenMobile de manière à ce qu'il utilise l'interface du fournisseur de services mobiles pour interroger les appareils BlackBerry et d'autres appareils Exchange ActiveSync et effectuer des opérations.

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. Configurez les paramètres suivants :

- **URL du service Web** : entrez l'adresse URL du service Web, par exemple, http://ServeurXmm/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 **OFF**.
- Cliquez sur **Tester la connexion** pour vérifier la connexion.

4. Cliquez sur **Enregistrer**.

Contrôle d'accès réseau

Jul 27, 2016

Si vous disposez d'un boîtier de contrôle d'accès réseau (NAC) sur votre réseau (tel qu'un réseau Cisco ISE), dans XenMobile, vous pouvez activer des filtres pour définir les appareils comme conformes ou non conformes au NAC, en vous basant sur des règles ou des propriétés. Si un appareil géré dans XenMobile ne répond pas aux critères spécifiés, et qu'il est par conséquent marqué comme non conforme, le boîtier NAC bloque l'appareil sur votre réseau.

Dans la console XenMobile, sélectionnez les critères dans la liste en fonction desquels un appareil est jugé comme non conforme.

XenMobile prend en charge les filtres de conformité 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.

Autorisation et refus implicites : il s'agit de l'action par défaut pour ActiveSync Gateway. Elle crée une liste de tous les appareils qui ne répondent à aucun des autres 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 exécuté en mode MAM ou un appareil désinscrit n'est pas géré.

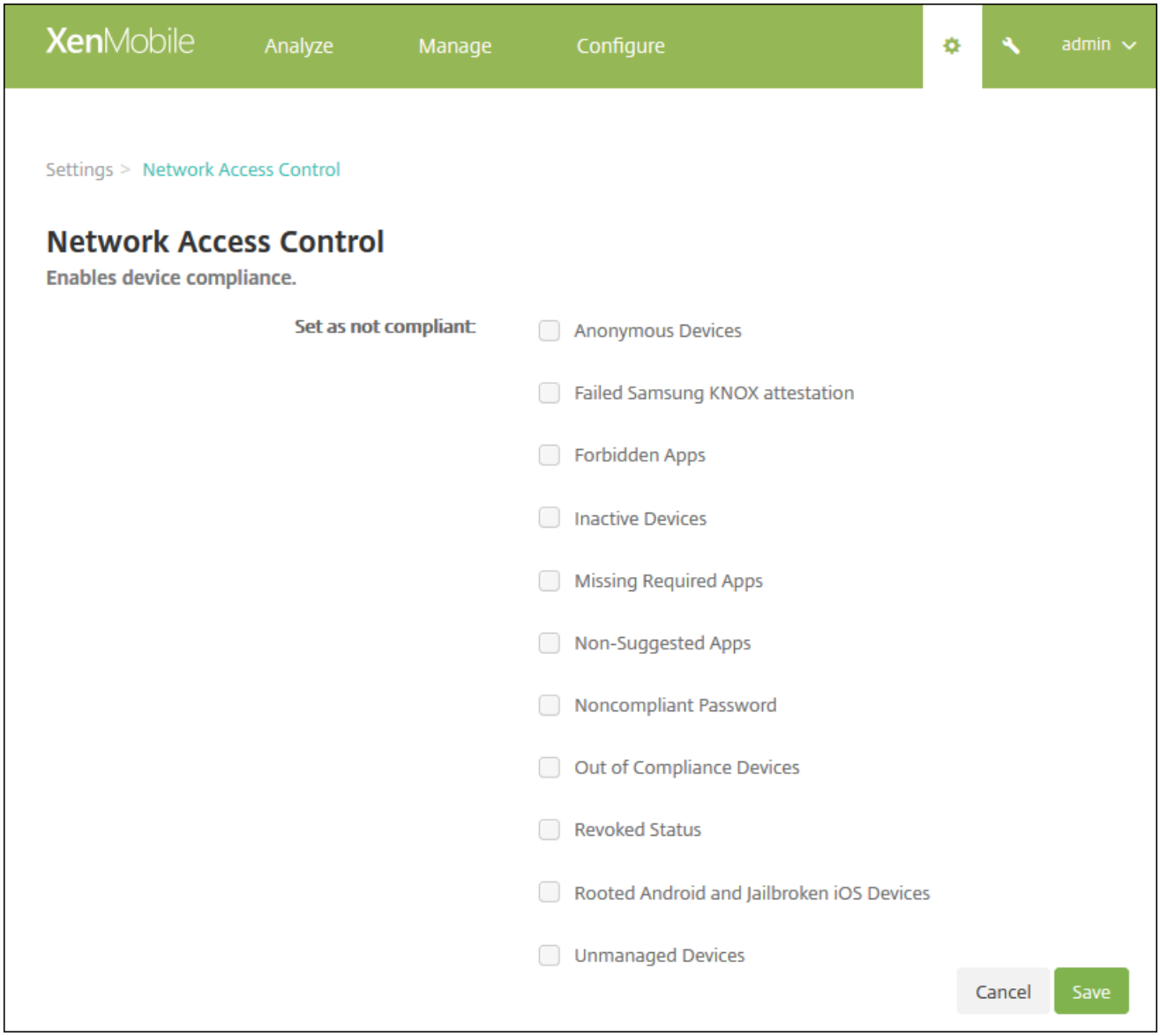
Envoyer les utilisateurs Android à ActiveSync Gateway : cliquez sur **OUI** pour vous assurer que XenMobile envoie des informations de l'appareil Android à ActiveSync Gateway. Lorsque cette option est activée, elle garantit que XenMobile envoie les informations de l'appareil Android à ActiveSync Gateway au cas où XenMobile ne disposerait pas de l'identificateur ActiveSync de l'utilisateur de cet appareil Android.

> ### Remarque
>
> le filtre Conformité/non conformité implicite définit la valeur par défaut uniquement sur les appareils qui sont gérés par XenMobile. Par exemple, les appareils sur lesquels une application en liste noire est installée ou qui ne sont pas inscrits sont marqués comme Non conformes et seront bloqués sur votre réseau par le boîtier NAC.

Configurer le contrôle d'accès réseau

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 **Contrôle d'accès réseau**. La page **Contrôle d'accès réseau** s'affiche.



3. Cochez les cases correspondant aux filtres **Définir comme non conforme** que vous souhaitez activer.

4. Cliquez sur **Enregistrer**.

Samsung KNOX

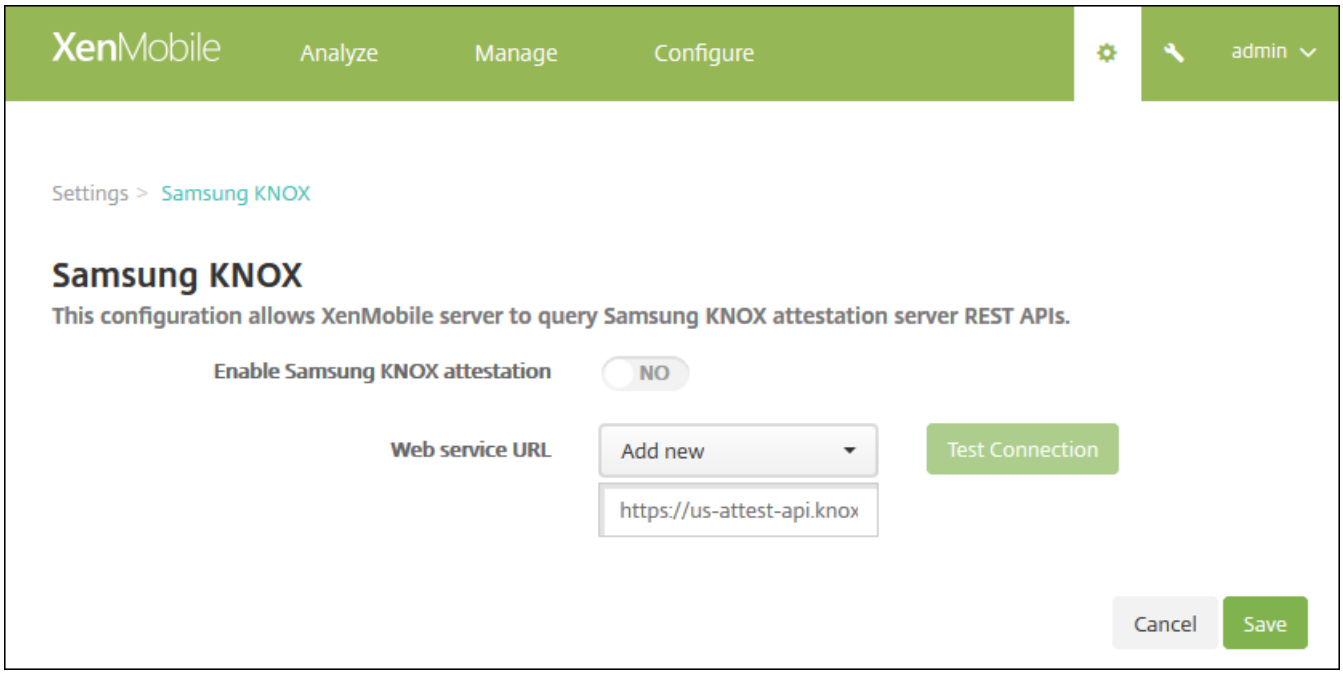
Jul 27, 2016

Vous pouvez configurer XenMobile pour interroger les API REST du serveur d'attestation Samsung KNOX.

Samsung KNOX tire profit 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) au moment de l'exécution en fonction des données collectées au cours du démarrage sécurisé.

1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Serveur**, cliquez sur **Samsung KNOX**. La page **Samsung KNOX** s'affiche.



3. Configurez les paramètres suivants :

- **Activer la certification Samsung KNOX** : sélectionnez cette option si vous souhaitez activer la certification Samsung KNOX. La valeur par défaut est **NO**. Lorsque vous activez le paramètre **Activer la certification Samsung KNOX**, l'option **URL du service Web** est activée.
- Dans la liste, cliquez sur le serveur d'attestation approprié.

4. Cliquez sur **Tester la connexion** pour vérifier la connexion.

5. Cliquez sur **Enregistrer**.

Remarque

Vous pouvez utiliser SamSung KNOX Mobile Enrollment pour inscrire plusieurs appareils Samsung KNOX dans XenMobile (ou Mobile Device Manager) sans avoir à configurer manuellement chaque appareil. Pour de plus amples informations, consultez la

section Inscription en bloc Samsung KNOX.

Pour ajouter, modifier ou supprimer des propriétés de serveur

Jul 27, 2016

XenMobile dispose de plus de 100 propriétés qui s'appliquent aux opérations du serveur. Cet article décrit certaines des propriétés de serveur les plus importantes et décrit en détail comment ajouter, modifier ou supprimer des propriétés de serveur.

Définitions des propriétés du serveur

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 le serveur XenMobile doit conserver 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 le serveur XenMobile doit conserver le journal d'audit. La valeur par défaut est **7**.

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 de serveur SSL

Si la valeur est **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 votre serveur XenMobile, le serveur d'autorité de certification Microsoft est l'émetteur du certificat et votre certificat a été signé par une autorité de certification racine interne dont la racine n'est pas approuvée par le serveur XenMobile. La valeur par défaut est **True**.

Délai d'inactivité en minutes

Nombre de minutes après lequel un administrateur inactif qui utilise l'API publique du serveur XenMobile pour accéder à la console XenMobile ou une application tierce, est déconnecté. Un délai d'expiration de **0** signifie qu'un utilisateur inactif reste connecté. La valeur par défaut est **5**.

Single Sign-On à NetScaler

Si la valeur est **False**, elle désactive la fonctionnalité de rappel de XenMobile durant le Single Sign-On depuis NetScaler vers le serveur XenMobile. La fonctionnalité de rappel est utilisée pour vérifier l'ID de session NetScaler Gateway, si la

configuration de NetScaler Gateway comprend une adresse URL de rappel. La valeur par défaut est **False**.

Nettoyage du journal de session (en jours)

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

Téléchargement d'applications non authentifiées pour appareils Android

Si la valeur est **True**, vous pouvez télécharger des applications auto-hébergées sur des appareils Android exécutant Android for Work. Cette propriété est nécessaire si l'option Android for Work 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 appareils Windows

Utilisé uniquement pour les anciennes versions de Worx Home 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**.

Ticket à usage unique XAM

Nombre de millisecondes pendant lequel un jeton d'authentification à usage unique (OTT) est valide pour le téléchargement d'une application. Cette propriété fonctionne en conjonction avec les propriétés **Téléchargement d'applications non authentifiées pour Android** et **Téléchargement d'applications non authentifiées pour Windows**, qui spécifient si le téléchargement d'applications non authentifiées est autorisé. La valeur par défaut est **3600000**.

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

Nombre de minutes après lequel un utilisateur inactif est déconnecté du 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**.

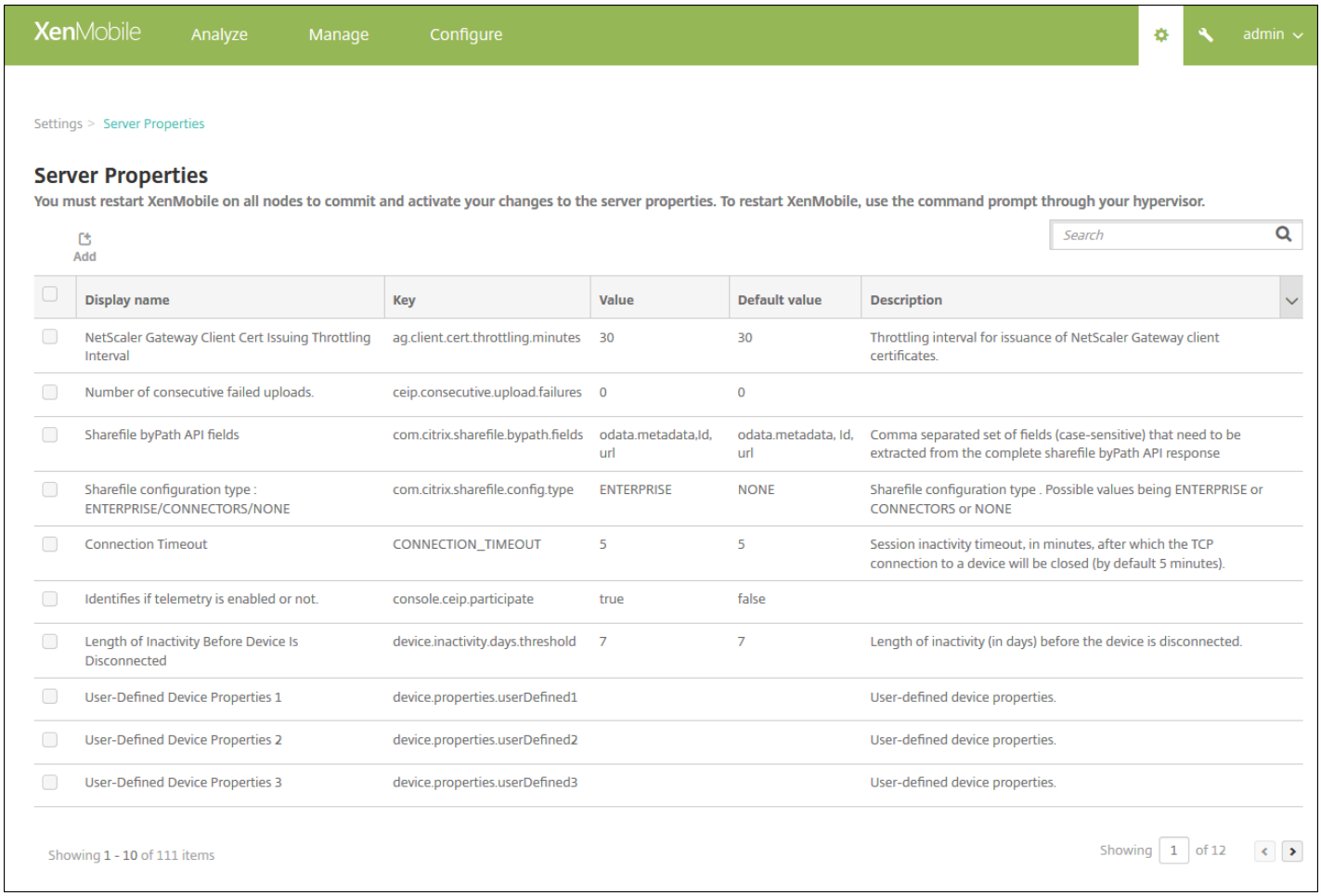
Ajout, modification ou suppression de propriétés de serveur

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.

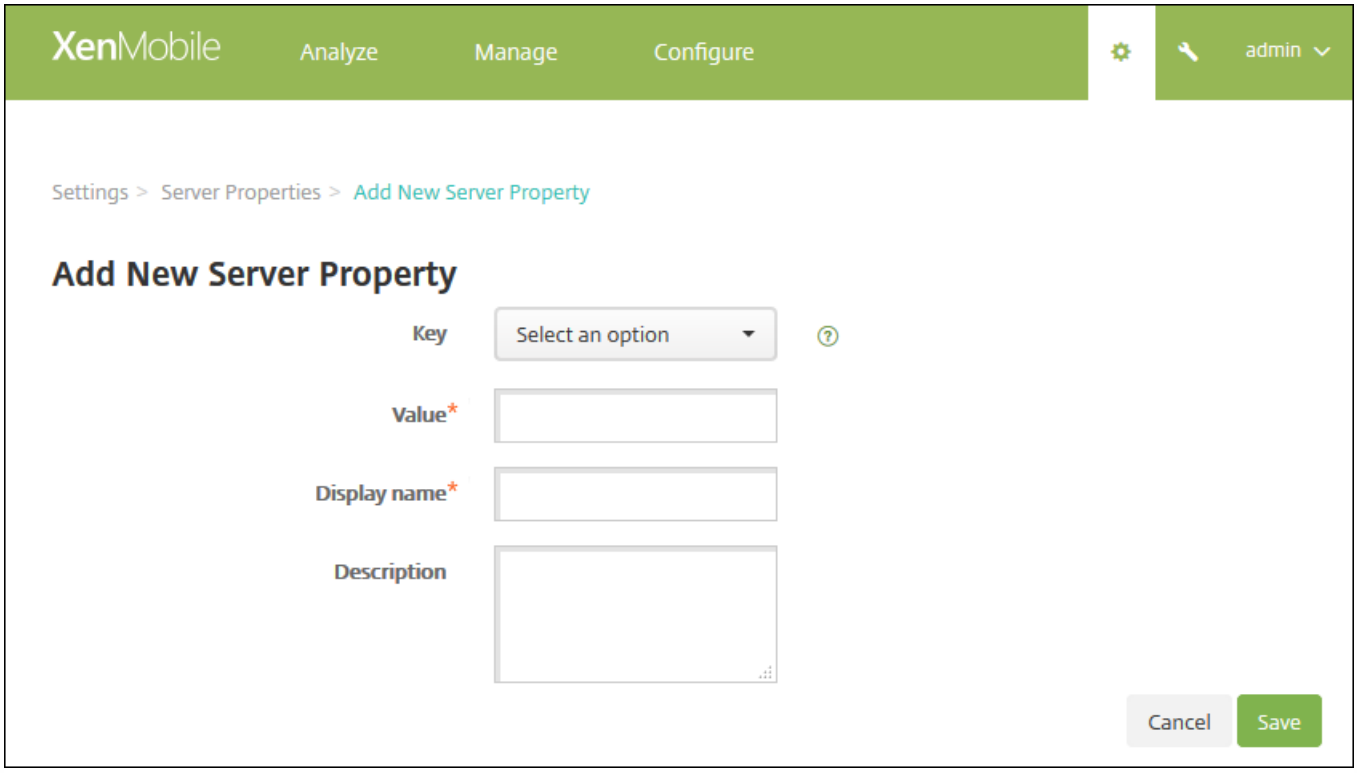
> ## Remarque
>
> Pour redémarrer XenMobile, utilisez l'invite de commande par le biais de votre hyperviseur.

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.



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



2. Configurez les paramètres suivants :

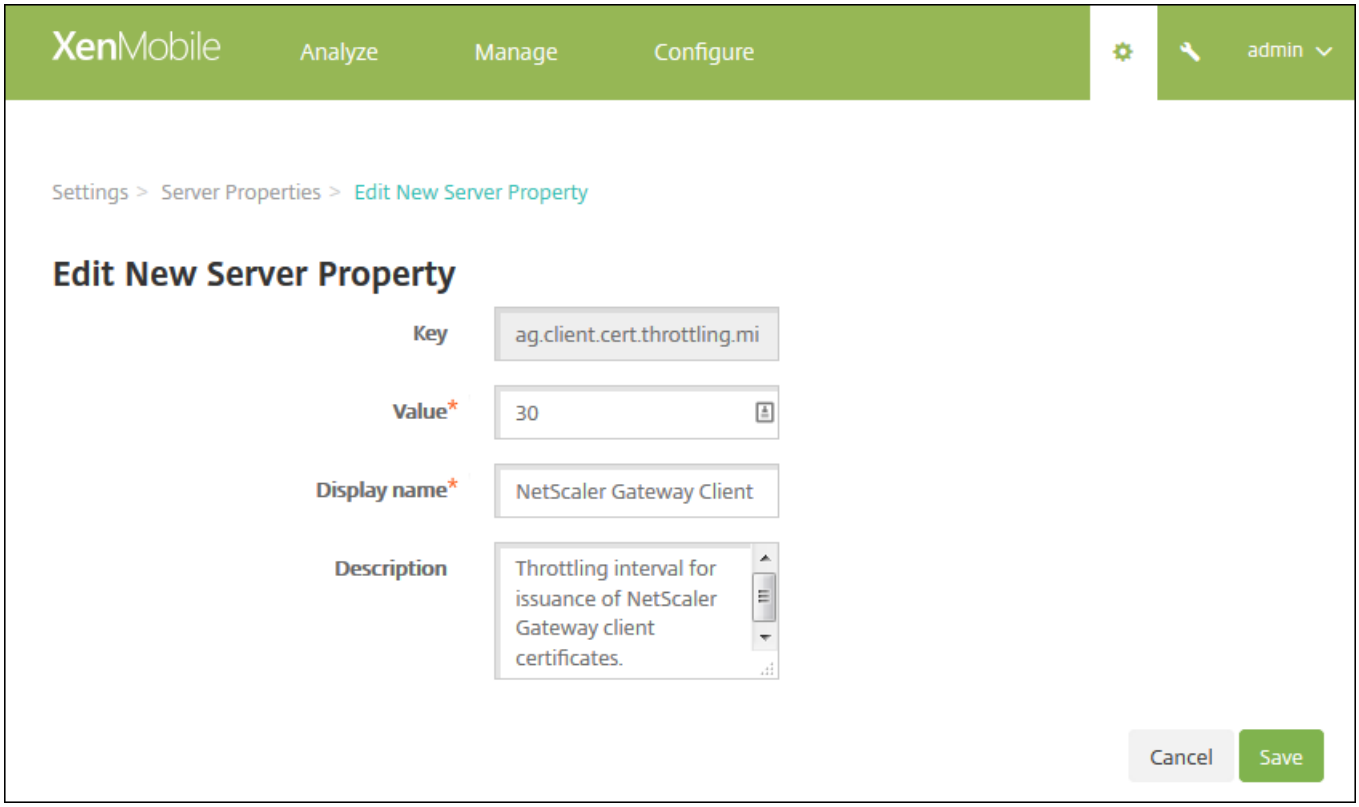
- **Clé** : dans la liste, sélectionnez la clé appropriée. les clés sont sensibles à la casse Vous devez contacter le support technique Citrix avant d'apporter des modifications, ou pour demander une clé spéciale.
- **Valeur** : entrez une valeur, en fonction de la clé que vous avez sélectionnée.
- **Nom 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**.

1. Dans le tableau **Propriétés du serveur**, sélectionnez la propriété de serveur que vous voulez modifier.

> **Remarque :** 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 ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

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.

1. Dans le tableau **Propriétés du serveur**, sélectionnez la propriété de serveur que vous voulez supprimer.

   Remarque : 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 du mode de serveur efficace XenMobile

Jul 27, 2016

Le mode de serveur XenMobile est une valeur définie dans les propriétés de serveur. Vous pouvez définir la valeur sur MAM, MDM ou ENT 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. La valeur par défaut du mode de serveur est ENT, quel que soit le type de licence.

Pour plus d'informations sur la configuration du mode de serveur, veuillez consulter la section Pour ajouter, modifier ou supprimer des propriétés de serveur.

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
ENT/ADV/MDM	Mode MDM	MDM
ENT/ADV	Mode MAM (également appelé mode MAM exclusif)	MAM
ENT/ADV	Mode MDM+MAM	ENT Les utilisateurs qui ont choisi de ne pas utiliser la gestion des appareils utiliseront l'ancien mode MAM.

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. 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. Pour les licences Enterprise et Advanced, le mode de serveur efficace correspond au mode du serveur.

Le mode de serveur est ajouté au journal du serveur à chaque fois qu'une licence est activée ou supprimée et lorsque le mode du serveur est modifié dans les propriétés du serveur. Pour de plus amples informations sur la création et l'affichage des fichiers journaux, consultez la section Support et maintenance de XenMobile.

SysLog

Jul 27, 2016

Vous pouvez configurer XenMobile de manière à envoyer les fichiers journaux à unserveur 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 le boîtier) 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 d'XenMobile.

Les informations de journal collectées par un serveur syslog à partir d'un boîtier sont stockées dans un fichier journal sous forme de messages. Ces messages contiennent généralement les informations suivantes :

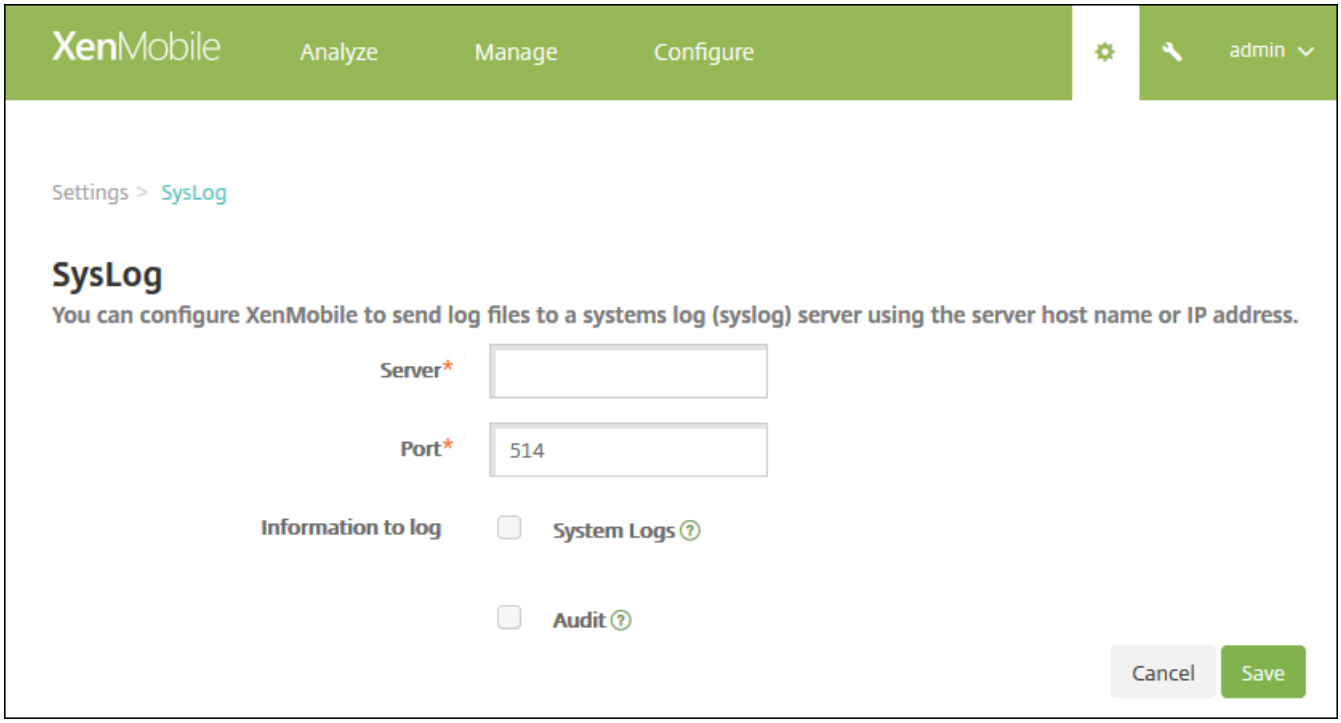
- L'adresse IP du boîtier qui a généré le message de journal
- Un horodatage
- Le type de message
- Le niveau de journalisation associé à un événement (critique, erreur, remarque, avertissement, informatif, débogage, alerte ou urgence)
- Les informations de message

Vous pouvez utiliser ces informations pour analyser la source de l'alerte et prendre des mesures correctives si nécessaire.

> ## Remarque
>
> Dans les déploiements XenMobile Cloud, Citrix ne prend pas en charge l'intégration syslog avec un serveur syslog local. Au lieu de cela, vous pouvez télécharger les journaux à partir de la page de support dans la console XenMobile. Ce faisant, vous devez cliquer sur **Tout télécharger** pour obtenir les journaux système. Pour de plus amples informations, consultez la section Visualisation et analyse des fichiers journaux dans 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 **Syslog**. La page **Syslog** s'affiche.



3. Configurez les paramètres suivants :

- **Nom** : 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 d'XenMobile.

4. Cliquez sur **Enregistrer**.

Pour configurer XenApp et XenDesktop

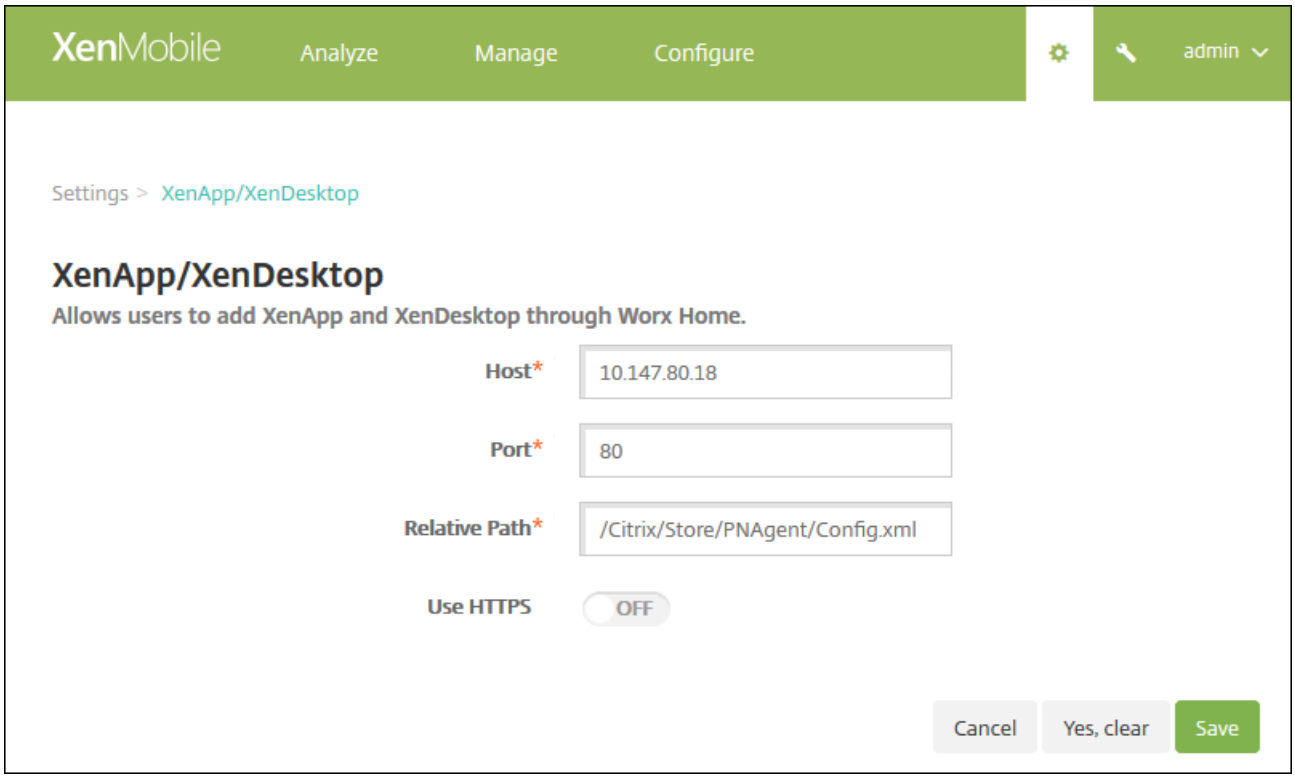
Jul 27, 2016

XenMobile peut collecter des applications depuis XenApp et XenDesktop et les rendre disponibles aux utilisateurs d'appareils mobiles dans Worx Store. Les utilisateurs s'abonnent directement aux applications dans Worx Store et les lancent depuis WorxHome. 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 XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Cliquez sur **XenApp/XenDesktop**. La page **XenApp/XenDesktop** s'affiche.



3. Configurez les paramètres suivants :

- **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 **OFF**.

4. Cliquez sur **Enregistrer**.

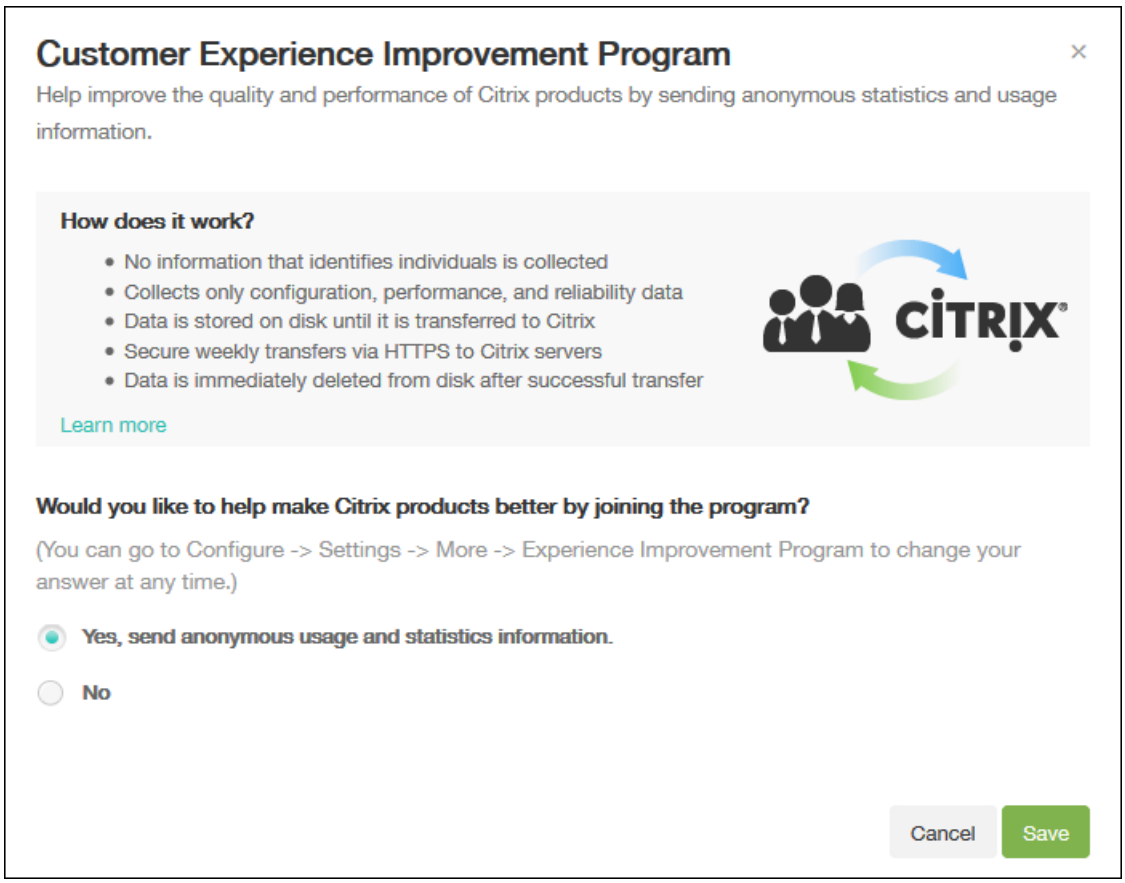
Programme d'amélioration de l'expérience utilisateur

Jul 27, 2016

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).

CEIP lors de l'installation ou la mise à niveau de XenMobile

La première fois que vous installez XenMobile ou lorsque vous effectuez une mise à jour, vous pouvez voir la boîte de dialogue suivante, dans laquelle vous devez indiquer si vous voulez participer, puis cliquez sur **Enregistrer**.

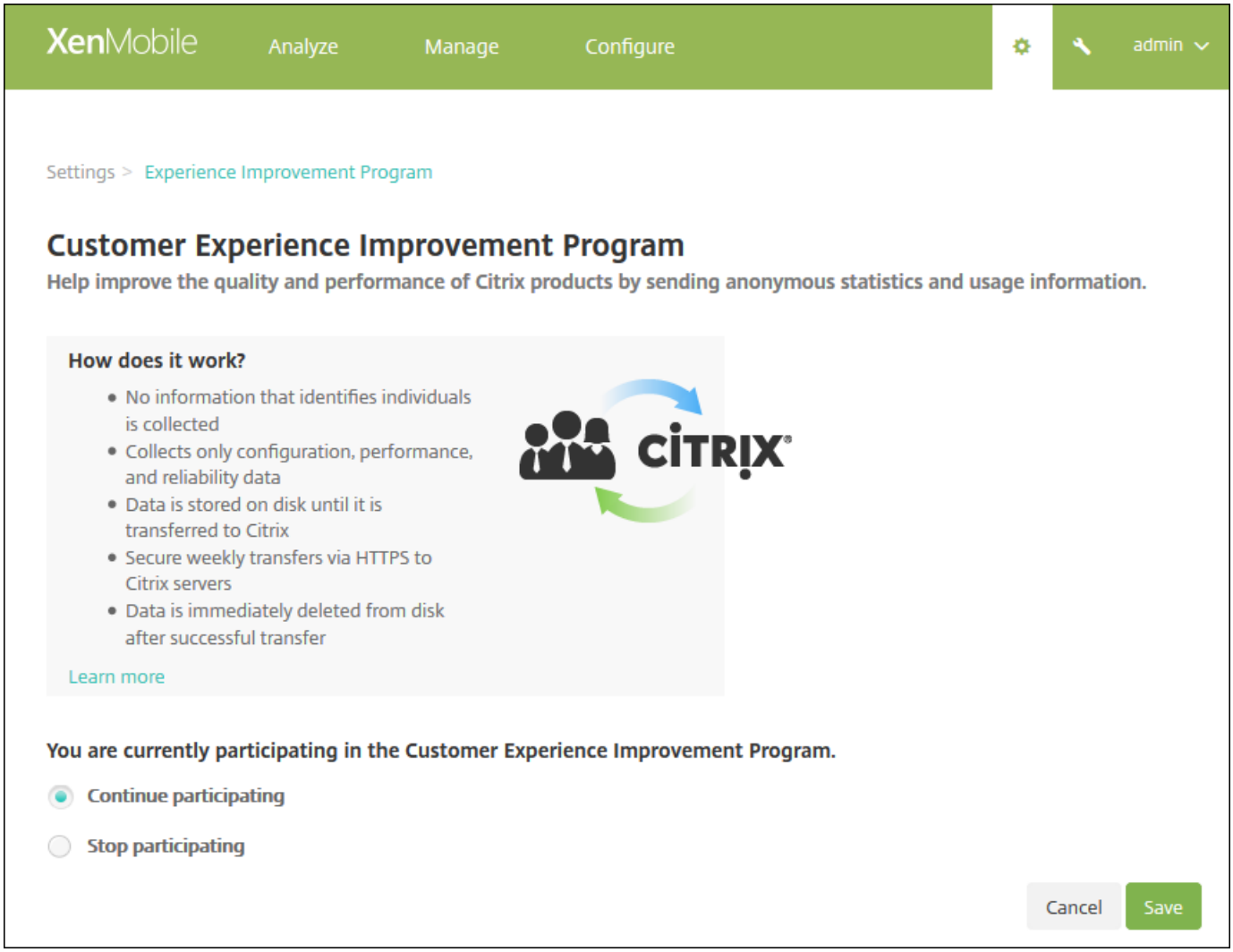


Modification de votre paramètre de participation au programme CEIP

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**.

Paramètres Microsoft Azure

Jul 27, 2016

Les appareils exécutant Windows 10 s'inscrivent à Azure afin de fédérer l'authentification Active Directory. Vous pouvez associer les appareils Windows 10 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 avez besoin d'une licence premium Active Directory Microsoft Azure avant de pouvoir intégrer XenMobile avec Microsoft Azure. La licence est requise pour activer l'intégration MDM avec Azure Active Directory de façon à ce que les utilisateurs avec des appareils Windows 10 puissent s'inscrire à l'aide d'Active Directory. Consultez Microsoft Azure pour de plus amples informations sur l'obtention de la licence premium. Pour plus d'informations sur les tarifs, veuillez consulter la section Tarifs Azure Active Directory.

Avant que les utilisateurs d'appareils Windows puissent s'inscrire à Azure, vous devez configurer les paramètres du serveur Microsoft Azure dans XenMobile, et configurer une stratégie termes et conditions pour les appareils Windows. Cet article explique comment configurer les paramètres Microsoft Azure. Pour de plus amples informations sur la configuration d'une stratégie termes et conditions pour les appareils Windows, consultez la section Stratégies termes et conditions.

Avant de pouvoir configurer les paramètres du serveur Microsoft Azure dans XenMobile, vous devez ouvrir une session sur le portail Azure AD et effectuez les opérations suivantes :

1. Enregistrez votre domaine personnalisé et vérifiez le domaine. Pour de plus amples informations, consultez la section Ajout de votre propre domaine à Azure Active Directory.

2. Étendez votre annuaire local à Azure Active Directory à l'aide des outils d'intégration d'annuaire. Pour de plus amples informations, consultez la section Intégration d'annuaire.

3. Faites du MDM une partie de confiance de Azure Active Directory. Pour ce faire, cliquez sur **Azure Active Directory** > **Applications**, puis sur **Ajouter**. Sélectionnez **Ajouter une application** à partir de la galerie. Accédez à **MOBILE DEVICE MANAGEMENT**, sélectionnez **On-premise MDM application**, puis enregistrez les paramètres.

4. Dans l'application, configurez la découverte du serveur XenMobile, les points de terminaison des conditions d'utilisation et l'URI d'ID de l'application comme suit :

- URL de découverte MDM : https://:8443/zdm/wpe
- URL des conditions d'utilisation MDM : https://:8443/zdm/wpe/tou
- URI d'ID de l'application : https://:8443/

5. Sélectionnez l'application MDM locale que vous avez créée à l'étape 3 et activez l'option **Manage devices for these users** pour activer la gestion MDM pour tous les utilisateurs ou un groupe d'utilisateurs spécifique.

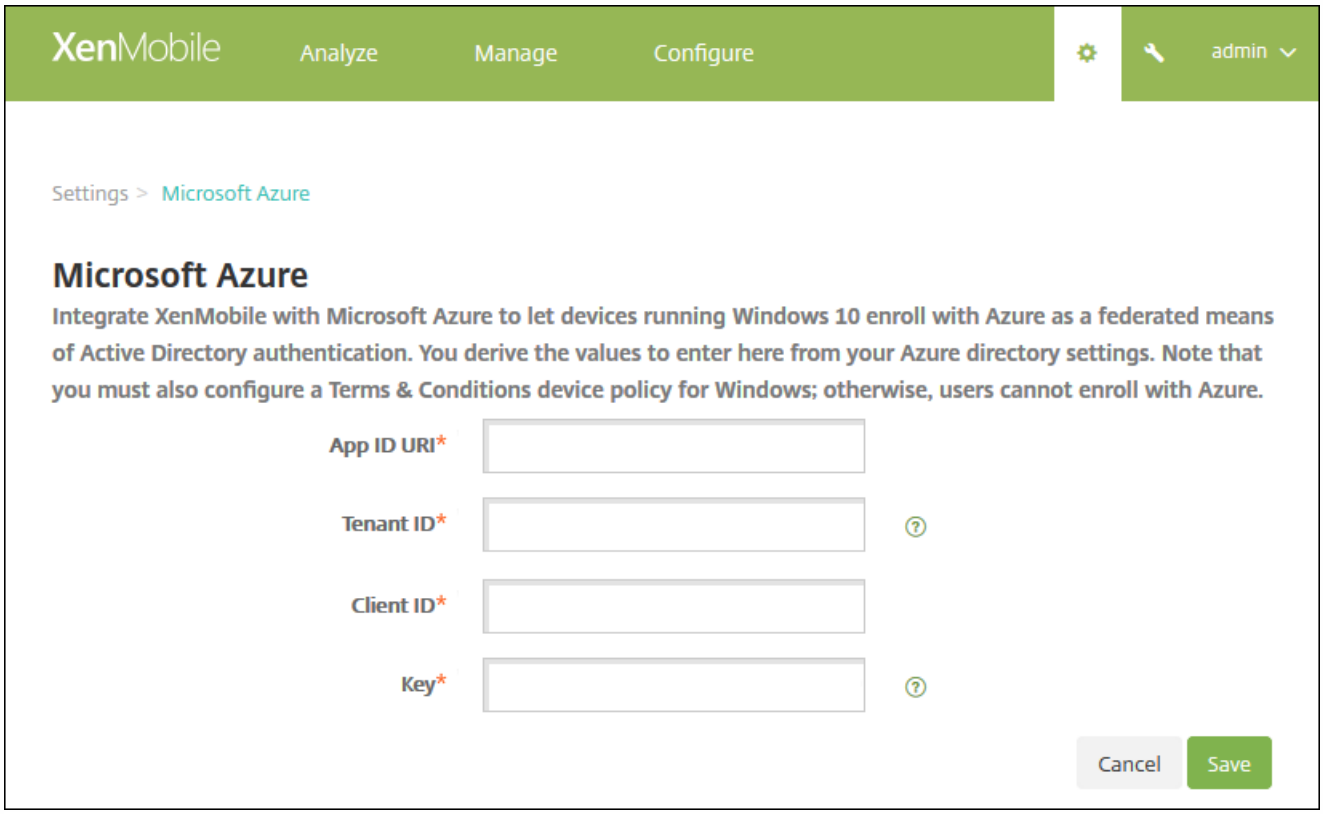
Vous devez également noter les informations suivantes à partir de votre compte Microsoft Azure afin de configurer les paramètres dans la console XenMobile.

- URI ID application : adresse URL du serveur exécutant XenMobile.
- ID du locataire : à partir de la page des paramètres d'application Azure.
- ID du client : identificateur unique pour votre application.

- Clé : dans la page des paramètres d'application Azure.

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 **Microsoft Azure**. La page **Microsoft Azure** s'affiche.



3. Configurez les paramètres suivants :

- **URI ID application** : entrez l'adresse URL du serveur exécutant XenMobile que vous avez entrée lorsque vous avez configuré vos paramètres Azure.
- **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*.
- **ID du client** : copiez et collez cette valeur depuis la page de configuration Azure. Il s'agit de 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.

4. Cliquez sur **Enregistrer**.

> ## Important
>
> Lorsque les utilisateurs se connectent à Azure AD sur leurs appareils Windows, les stratégies d'appareils Worx Store et Weblink que vous avez configurées dans XenMobile sont uniquement disponibles pour les utilisateurs AD Azure, mais pas pour les utilisateurs

locaux. Pour que les utilisateurs locaux puissent utiliser ces stratégies, ils doivent effectuer les opérations suivantes :

1. Se connecter à Azure Active Directory pour le compte d'un utilisateur Azure dans **Paramètres** > **À propos** > **Connecter à Azure AD**.
2. Fermer leur session Windows, puis se reconnecter avec un compte Azure AD.

Google Cloud Messaging

Jul 27, 2016

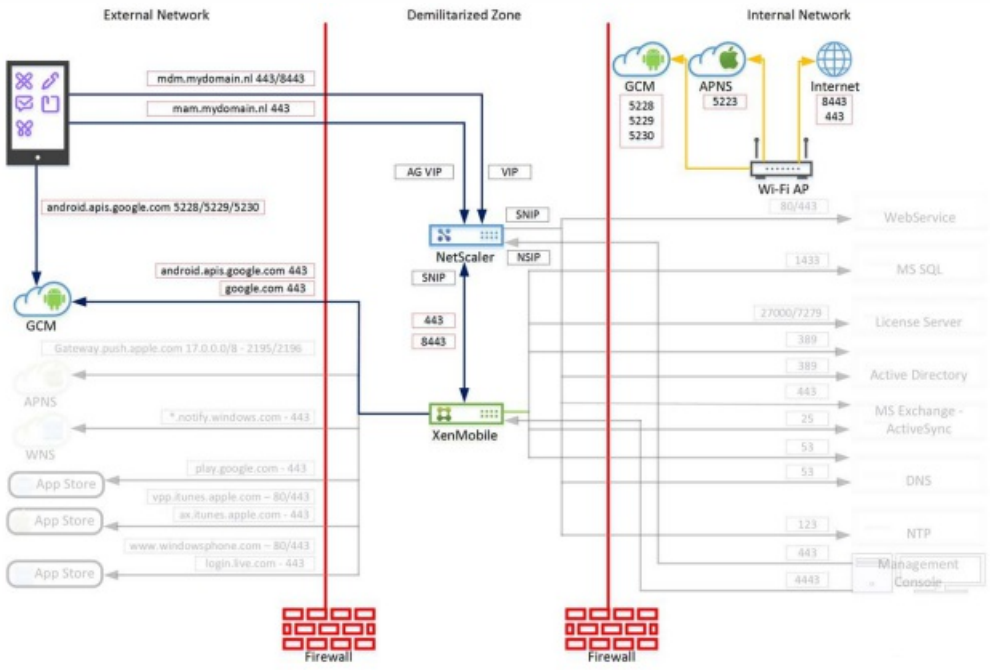
Une alternative à la stratégie MDX **Période d'interrogation active** consiste à utiliser Google Cloud Messaging (GCM) pour contrôler quand et comment les appareils Android doivent se connecter à XenMobile. Avec la configuration décrite dans cet article, toute action de sécurité ou commande de déploiement déclenche une notification push à Worx Home afin d'inviter l'utilisateur à se reconnecter au serveur XenMobile.

Conditions préalables

- XenMobile 10.3.x
- Dernier client Worx Home
- Informations d'identification du compte Google Developer
- Ouvrez le port 443 sur XenMobile pour Android.apis.google.com et Google.com

Architecture

Ce diagramme illustre le flux de communication pour GCM dans le réseau interne et externe.

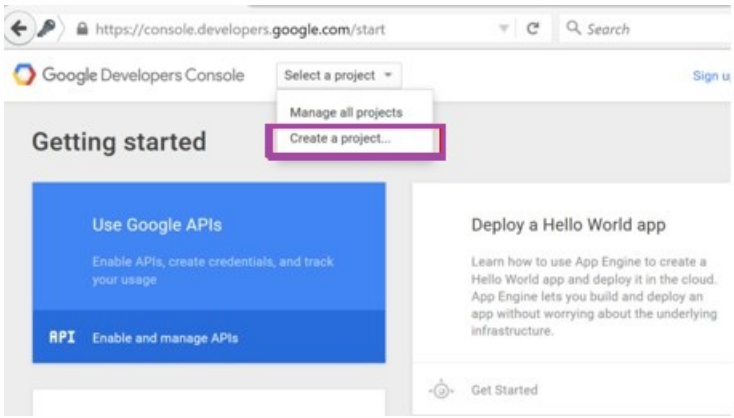


Pour configurer votre compte Google pour GCM

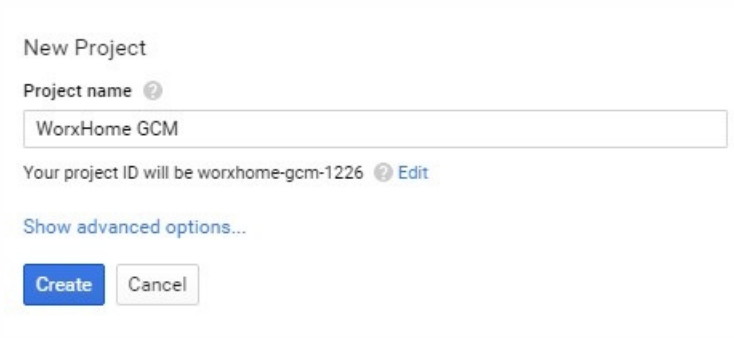
1. Connectez-vous à l'adresse URL suivante à l'aide des informations d'identification de votre compte Google Developer :

   https://console.developers.google.com

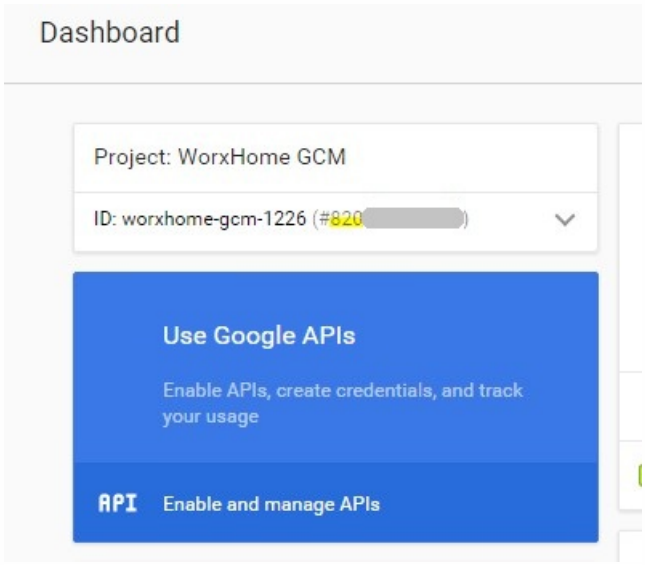
2. Dans **Sélectionner un projet**, choisissez **Créer un projet**.



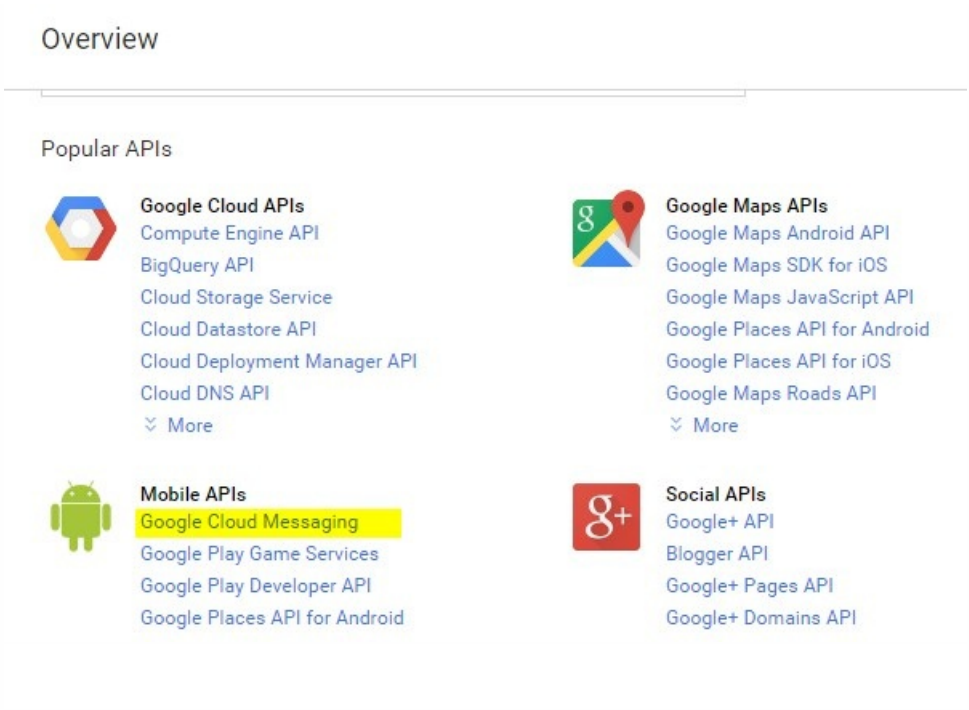
3. Entrez un **nom de projet** et cliquez sur **Créer**.



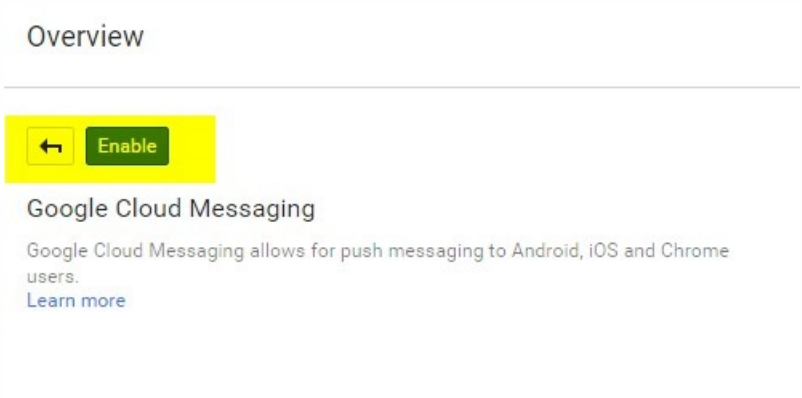
4. Dans le tableau de bord, votre ID d'expéditeur (en surbrillance ci-dessous) est affiché en regard de votre ID de projet. Enregistrez votre ID d'expéditeur ; vous devez l'entrer plus tard dans les paramètres du serveur XenMobile. Cliquez sur **Utiliser les API de Google**.



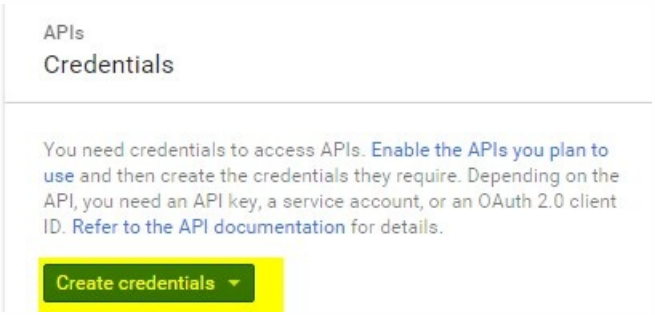
5. Dans la section **API pour mobile**, cliquez sur **Google Cloud Messaging**.



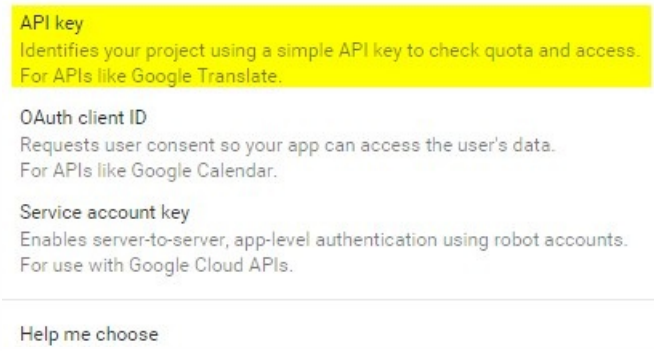
6. Cliquez sur **Activer**.



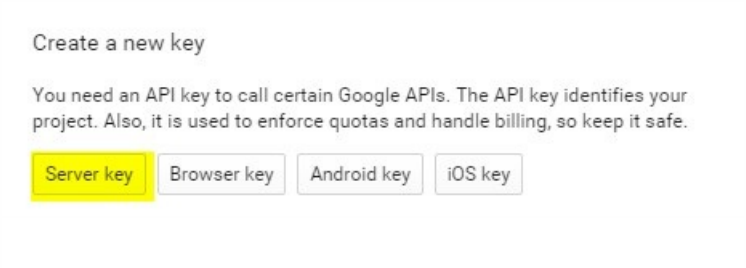
7 Sous **Identifiants**, cliquez sur **Créer des identifiants**.



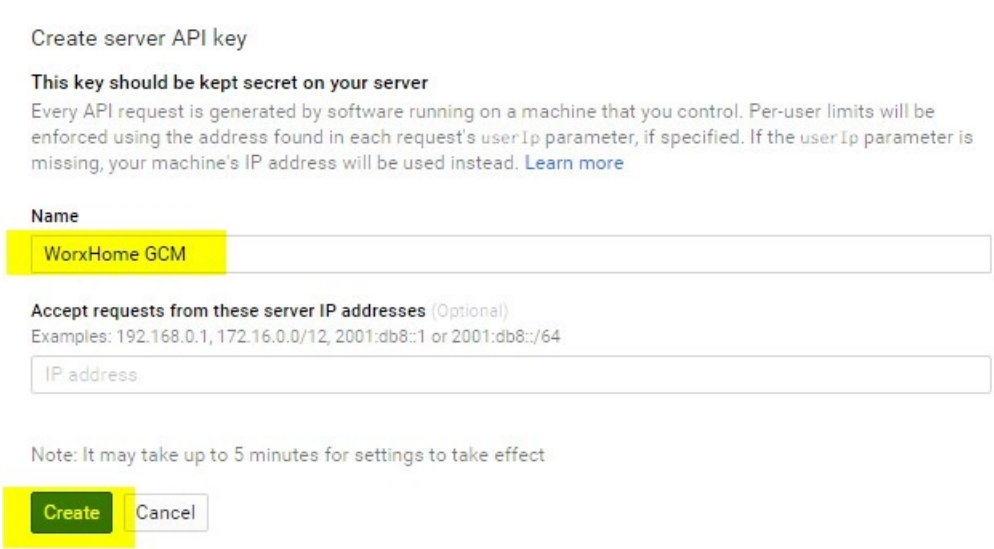
8. Cliquez sur **Clé API**.



9. Sous **Créer une clé**, cliquez sur **Clé serveur**.



10. Dans **Créer une clé pour l'API du serveur**, entrez un **nom** (par exemple, nous avons utilisé le nom du projet), puis cliquez sur **Créer**.



11. Enregistrez la clé d'API. Vous en aurez besoin pour configurer XenMobile.

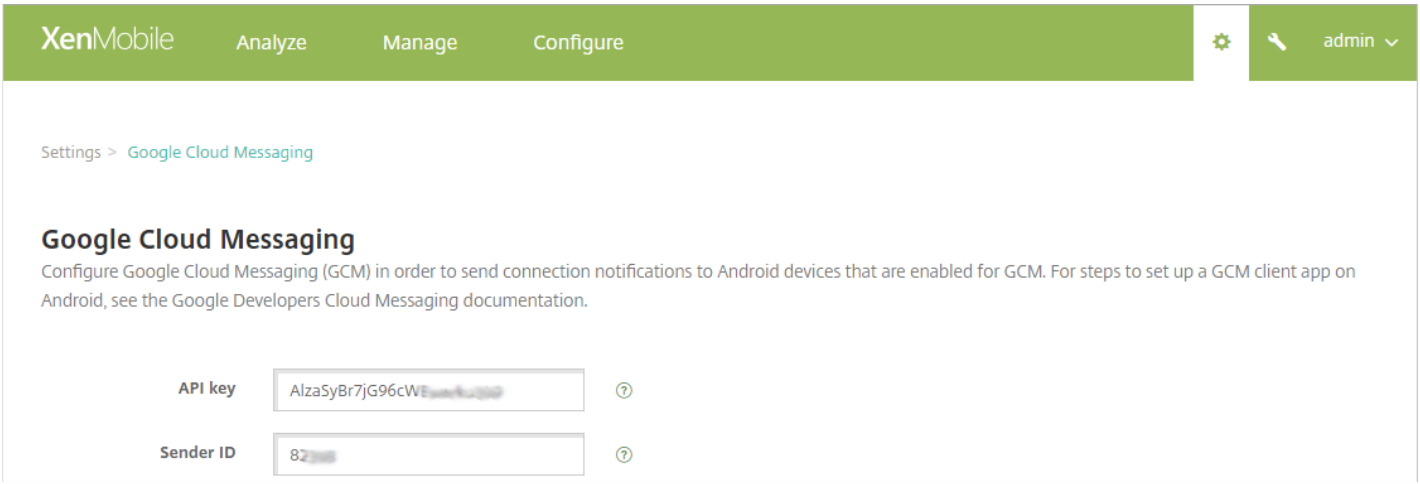
Pour configurer XenMobile pour GCM

1. Connectez-vous à la console d'administration XenMobile, puis cliquez sur **Paramètres > Google Cloud Messaging**.

   a. Dans **Clé API**, entrez la clé d'API GCM que vous avez copiée dans la dernière étape de la configuration de GCM.

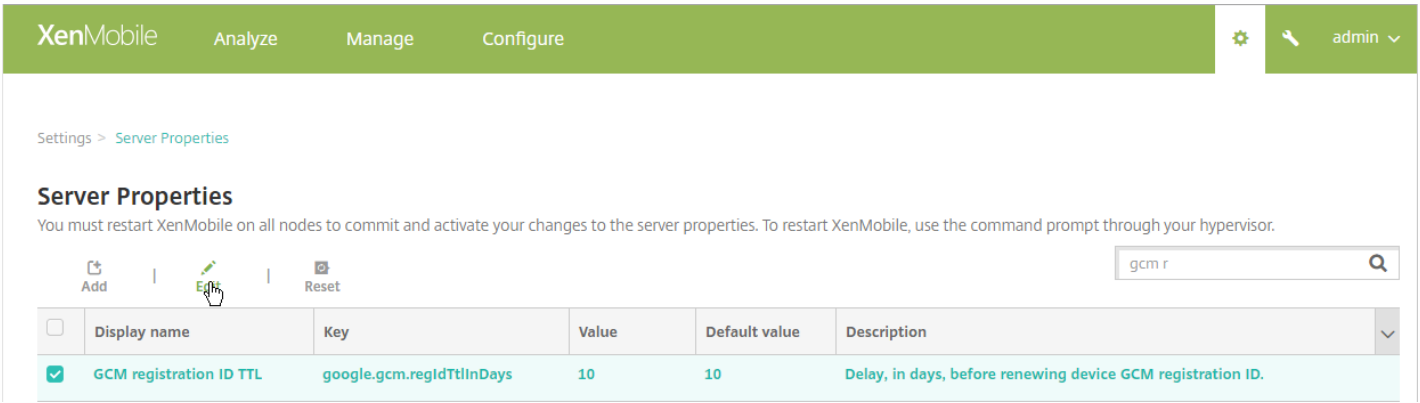
   b. Dans **ID d'expéditeur**, copiez la valeur de l'ID d'expéditeur que vous avez indiquée dans la procédure précédente, puis cliquez sur **Enregistrer**.

   Remarque : la page **Paramètres > Google Cloud Messaging** est nouvelle dans XenMobile 10.3.6. Si vous n'utilisez pas la dernière version de XenMobile, accédez à **Paramètres > Serveur** pour mettre à jour la **clé API** (google.gcm.apiKey) et l'**ID d'expéditeur** (google.gcm.senderid).



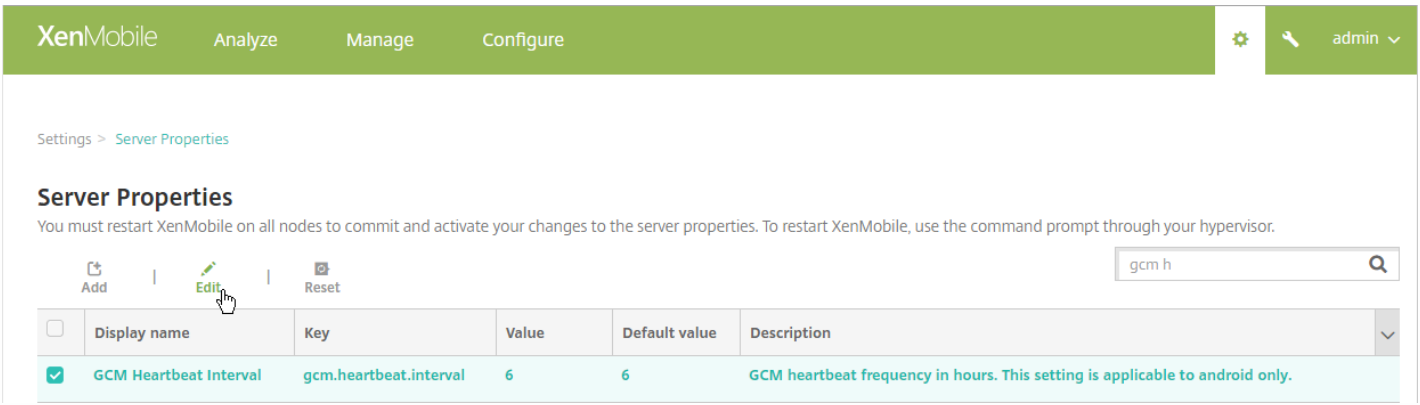
2. Si vous avez besoin de modifier les paramètres par défaut pour l'une des propriétés suivantes, cliquez sur **Paramètres > Propriétés du serveur**.

- **Durée de vie de l'ID d'enregistrement de GCM :** la valeur par défaut du délai après lequel l'ID d'enregistrement de GCM doit être renouvelé est de **10** jours. Pour modifier cette valeur, entrez **gcm r** dans la zone de recherche, cliquez sur **Durée de vie de l'ID d'enregistrement de GCM**, puis cliquez sur **Modifier**.



- **Intervalle d'interrogation de GCM par défaut :** la fréquence par défaut à laquelle XenMobile communique avec le serveur GCM est de **6** heures. Pour modifier cette valeur, entrez **gcm h** dans la zone de recherche, cliquez sur **Intervalle**

d'interrogation GCM et sur **Modifier**.

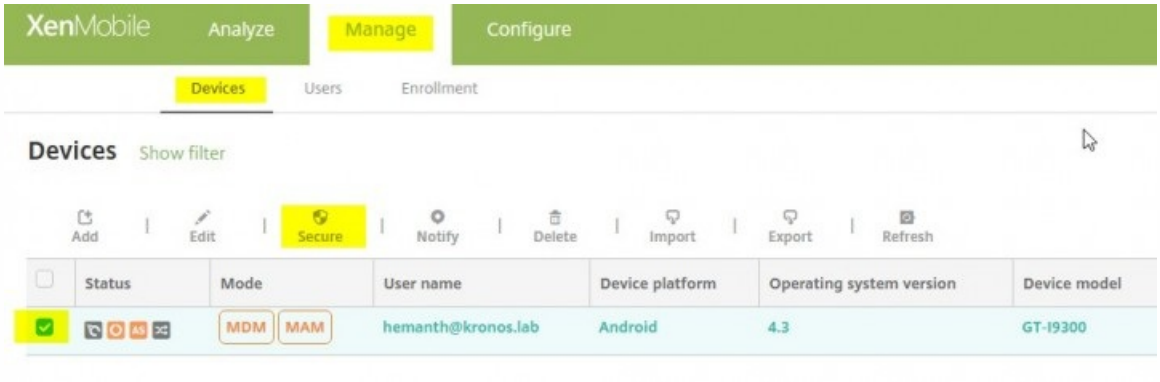


Pour tester votre configuration

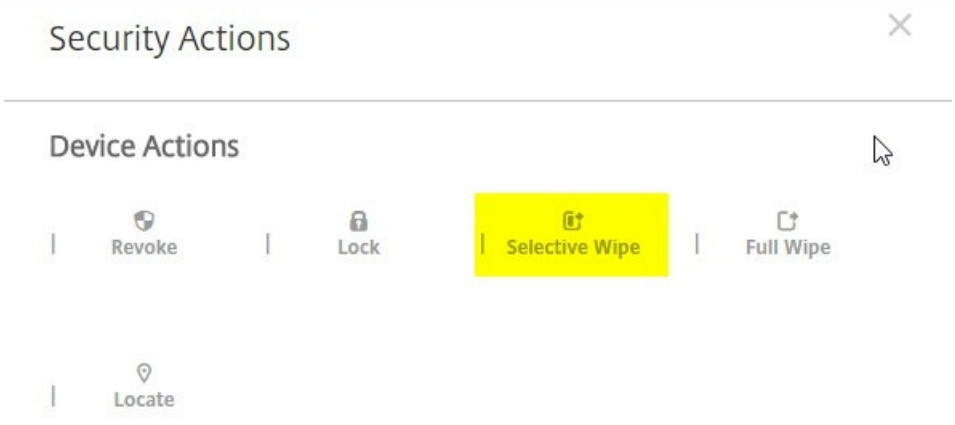
1. Inscrivez un appareil Android.

2. Laissez l'appareil inactif pendant un certain temps, de façon à ce qu'il se déconnecte du serveur XenMobile.

3. Ouvrez une session sur la console d'administration 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, l'effacement des données d'entreprise a lieu sur l'appareil sans qu'une reconnexion à XenMobile soit nécessaire.

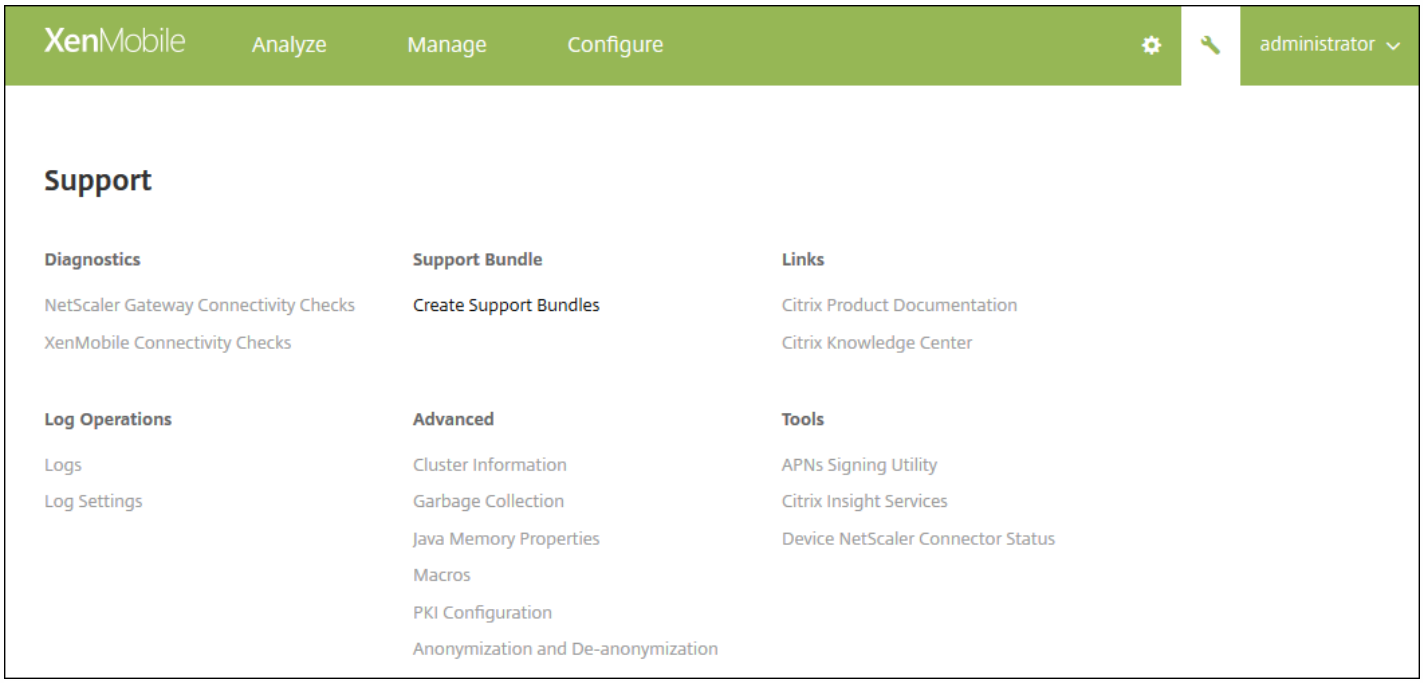
Support et maintenance de XenMobile

Jul 27, 2016

Utilisez la page Support de XenMobile pour accéder à des informations et outils de support. Vous pouvez également effectuer des actions à partir de l'interface de ligne de commande. Pour de plus amples informations, consultez la section Options d'interface de ligne de commande XenMobile.

Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit.

La page Support s'affiche.



Utilisez la page **Support** de XenMobile pour :

- Accéder aux diagnostics.
- Créer des packs d'assistance.
- Accéder aux liens de la documentation produit et du centre de connaissances Citrix.
- Accéder au journal des opérations.
- Sélectionner un ensemble d'options de configuration et d'informations avancées.
- Accéder à un ensemble d'outils et d'utilitaires.

Réalisation de contrôles de connectivité

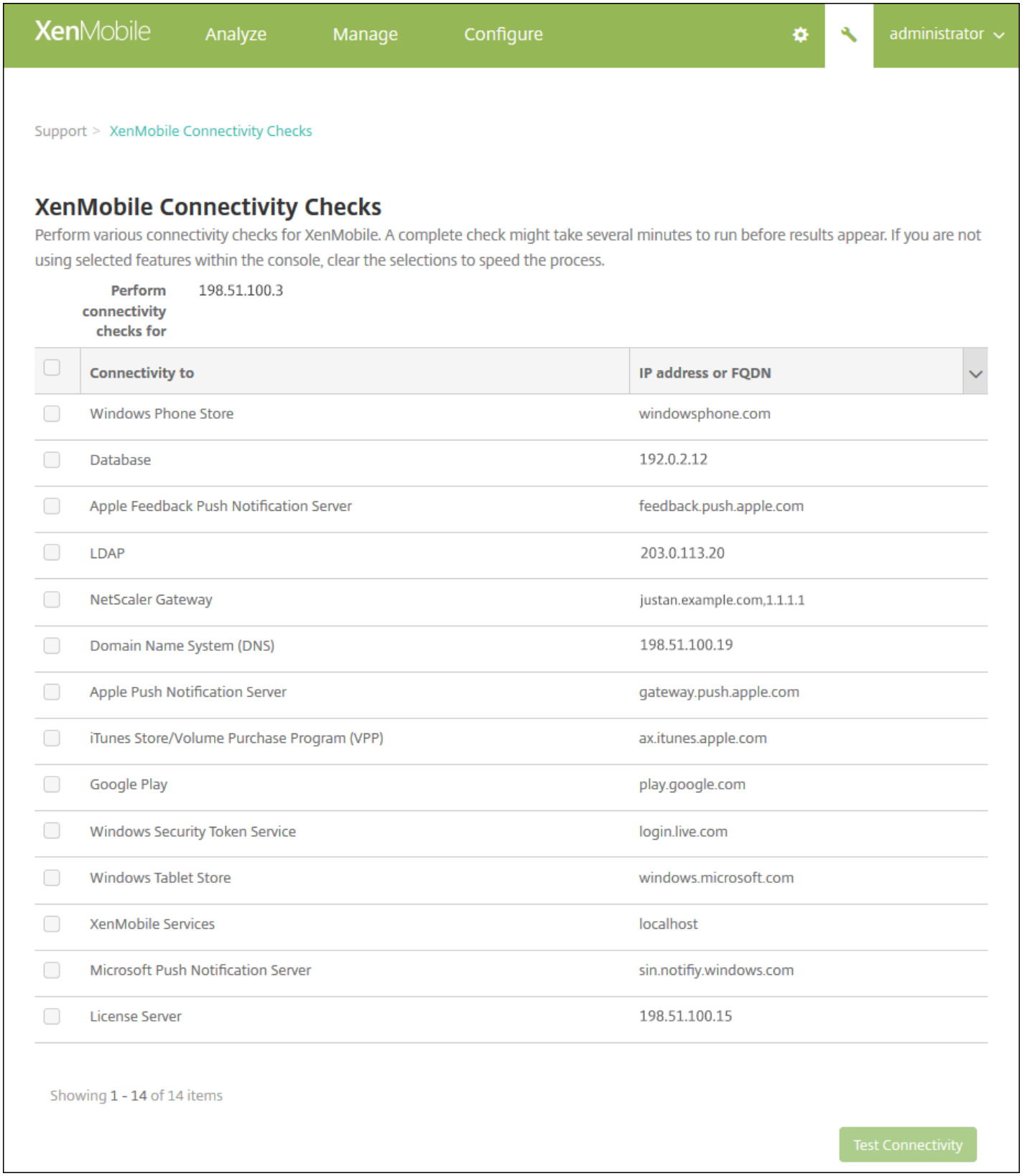
Jul 27, 2016

Depuis la page **Support** de XenMobile, vous pouvez vérifier la connexion de XenMobile à NetScaler Gateway et à d'autres serveurs et emplacements.

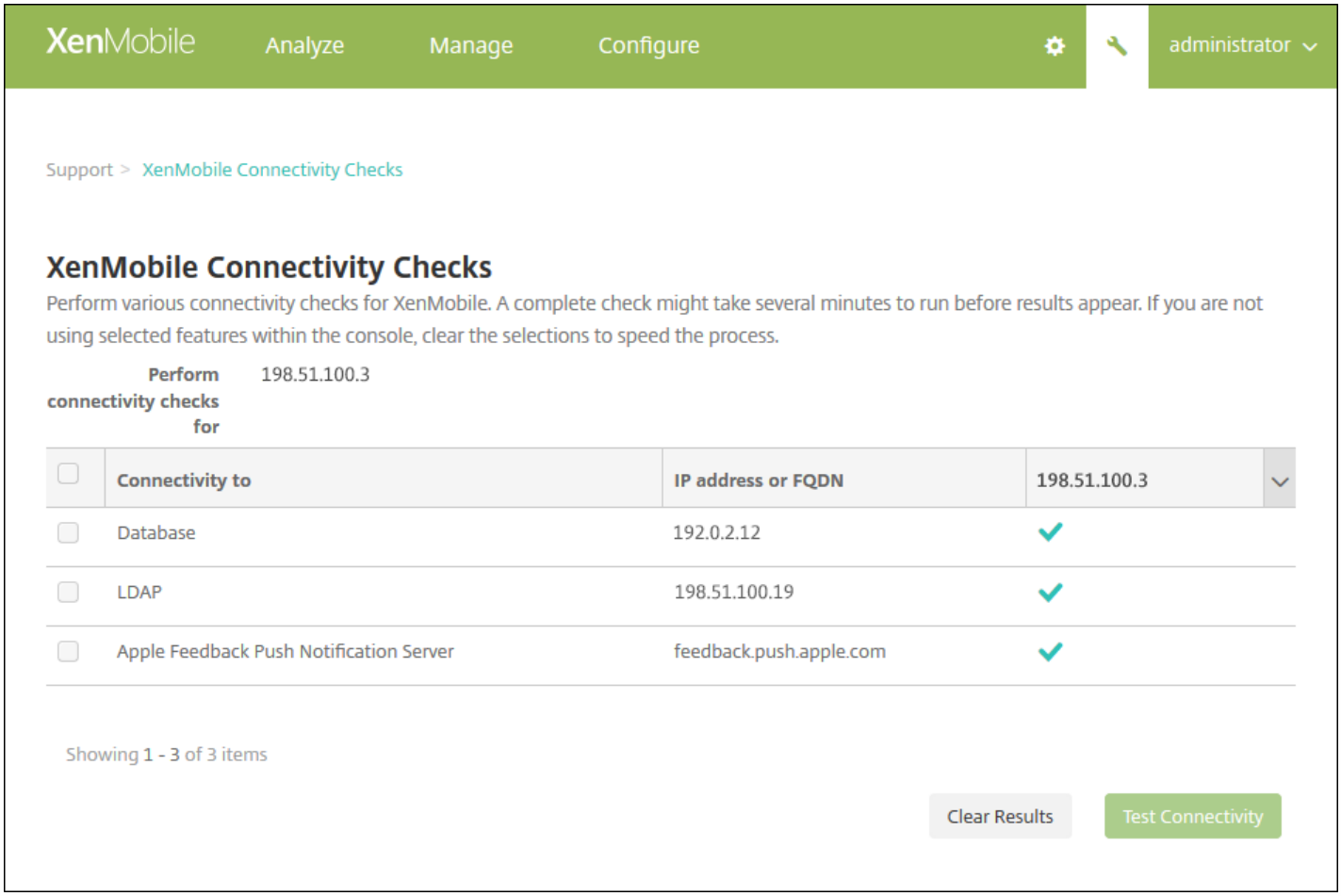
Réalisation de contrôles de connectivité dans XenMobile

1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Support** s'affiche.

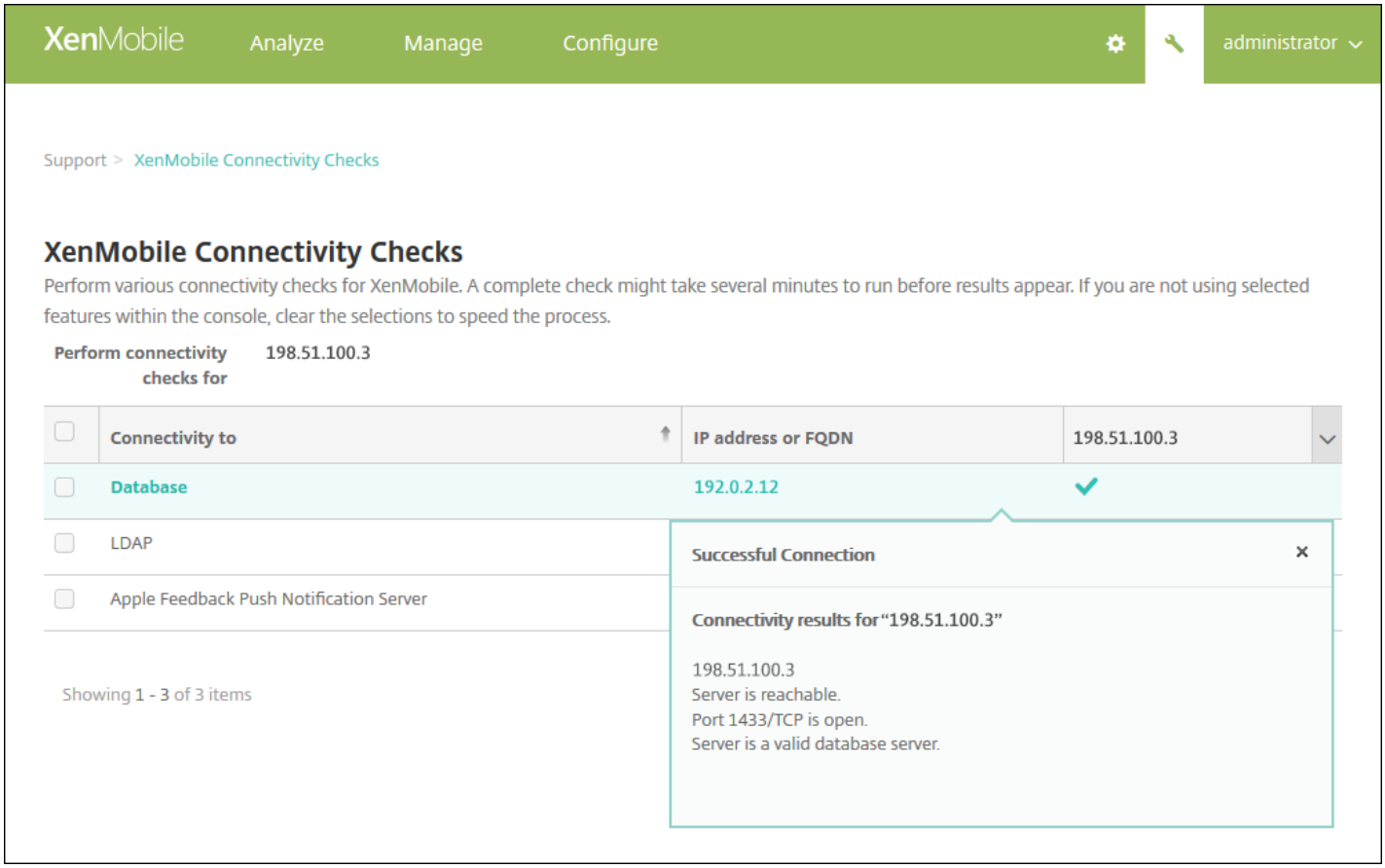
2. Sous **Diagnostics**, cliquez sur **Test de la connectivité XenMobile**. La page **Test de la connectivité XenMobile** s'affiche. Si votre environnement XenMobile contient des nœuds en cluster, tous les nœuds sont affichés.



2. 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.

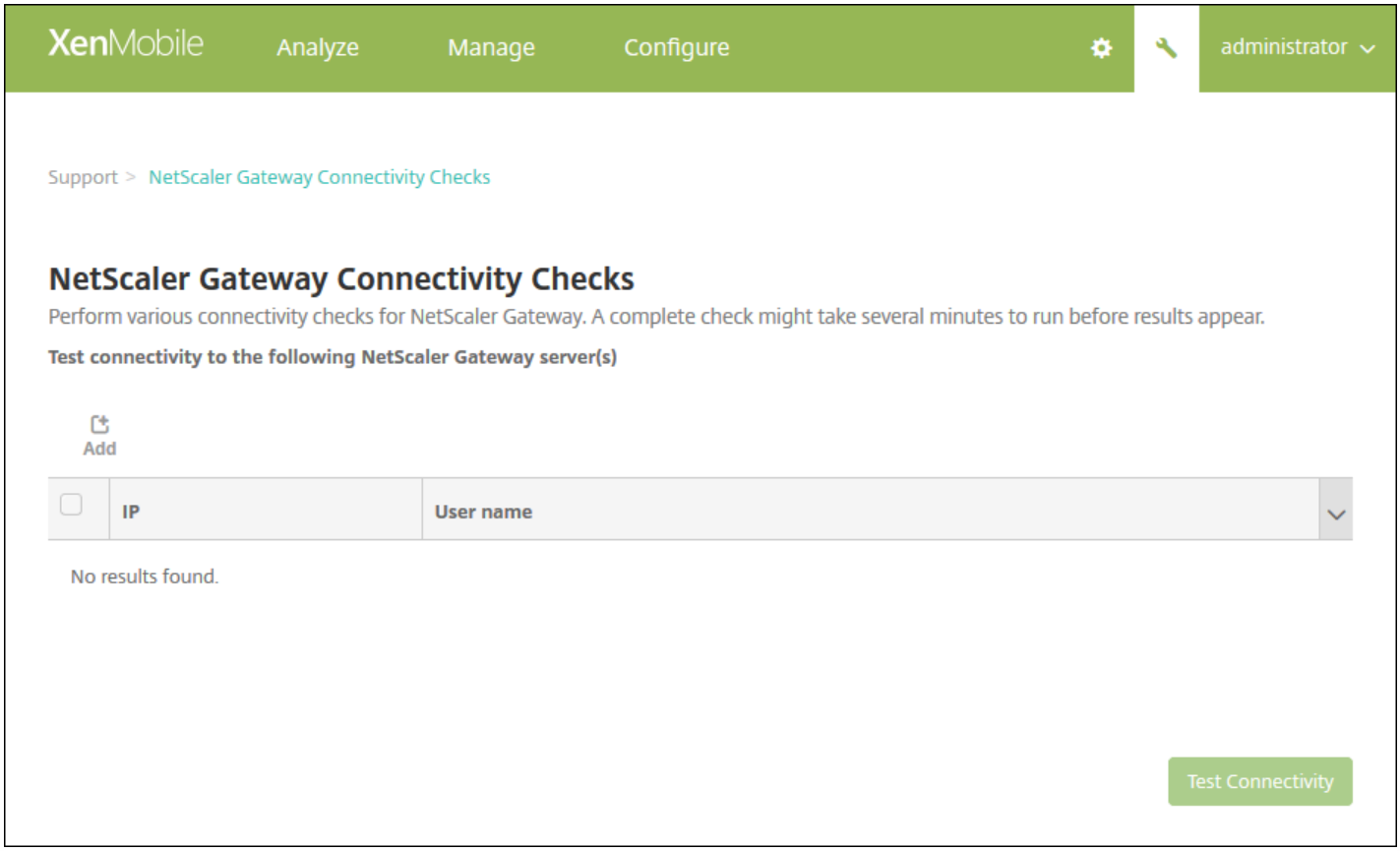


3. Sélectionnez un serveur dans la table Résultats du test pour afficher les résultats détaillés pour ce serveur.

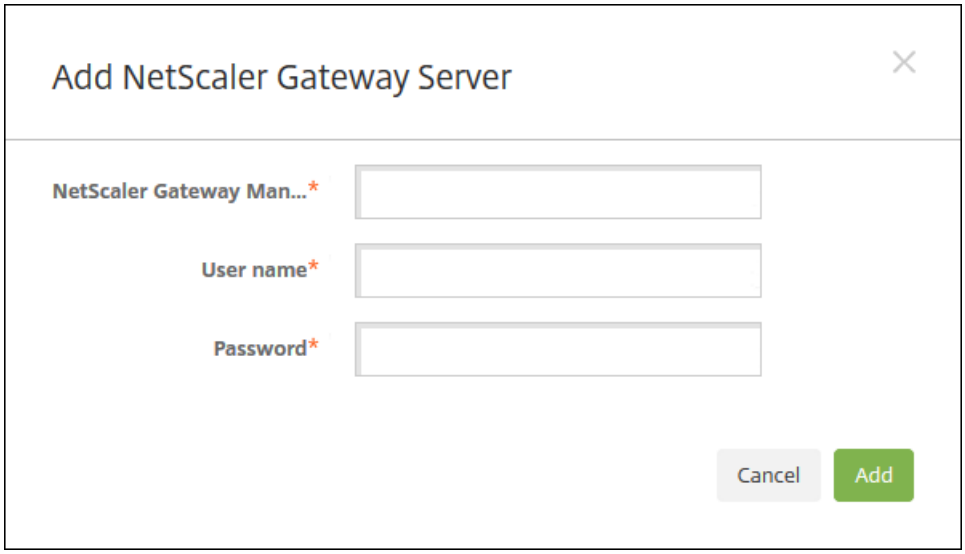


Réalisation de contrôles de connectivité pour NetScaler Gateway

1. Sur la page **Support**, sous **Diagnostics**, cliquez sur **Test de la connectivité NetScaler Gateway**. La page **Test de la connectivité NetScaler Gateway** s'affiche. Le tableau est vide si vous n'avez pas ajouté de serveurs NetScaler Gateway.



2. Cliquez sur **Add**. La boîte de dialogue **Ajouter un serveur NetScaler Gateway** s'affiche.



3. Dans **Adresse IP de gestion de NetScaler Gateway**, entrez l'adresse IP du serveur exécutant NetScaler Gateway que vous voulez tester.

Remarque : si vous effectuez un contrôle de connectivité pour un serveur NetScaler Gateway qui est déjà ajouté, l'adresse IP est renseignée.

4. Tapez vos informations d'identification d'administrateur pour ce NetScaler Gateway.

Remarque : si vous effectuez un contrôle de connectivité pour un serveur NetScaler Gateway qui est déjà ajouté, le nom d'utilisateur est renseigné.

5. Cliquez sur **Add**. La passerelle NetScaler Gateway est ajoutée au tableau sur la page **Test de la connectivité NetScaler Gateway**.

6. Cliquez sur **Tester la connectivité**. Les résultats s'affichent dans la table Résultats du test.

7. Sélectionnez un serveur dans la table Résultats du test pour afficher les résultats détaillés pour ce serveur.

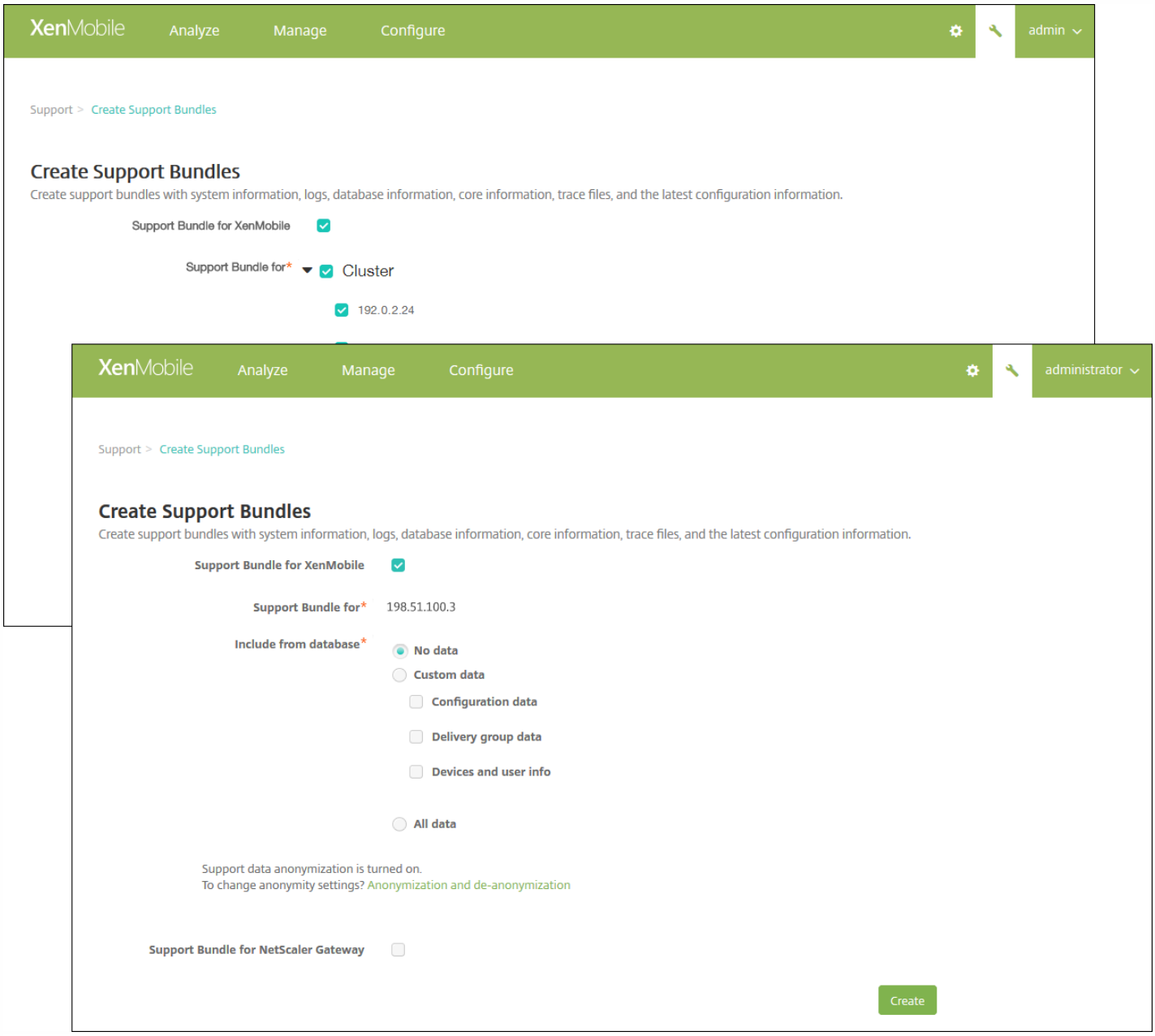
Création de packs d'assistance dans XenMobile

Jul 27, 2016

Si vous voulez signaler un problème à Citrix ou résoudre un problème, vous pouvez créer un pack d'assistance, puis le charger sur Citrix Insight Services (CIS).

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.



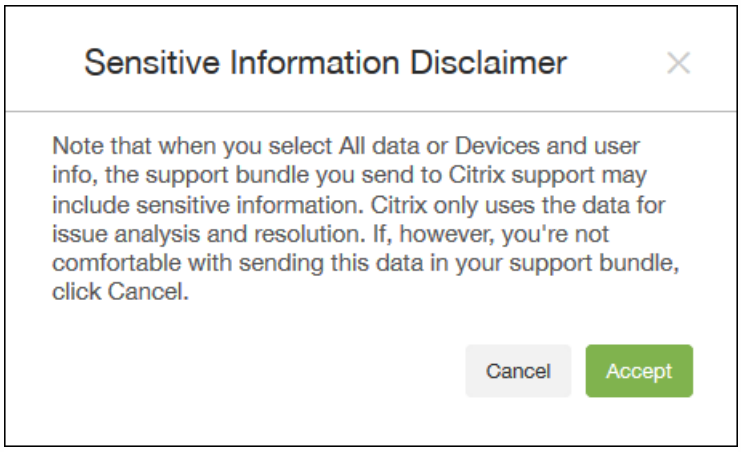
3. Assurez-vous que la case à cocher **Pack d'assistance pour XenMobile** est sélectionnée.

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**, puis sélectionnez tout ou partie des éléments suivants :
  - **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**.

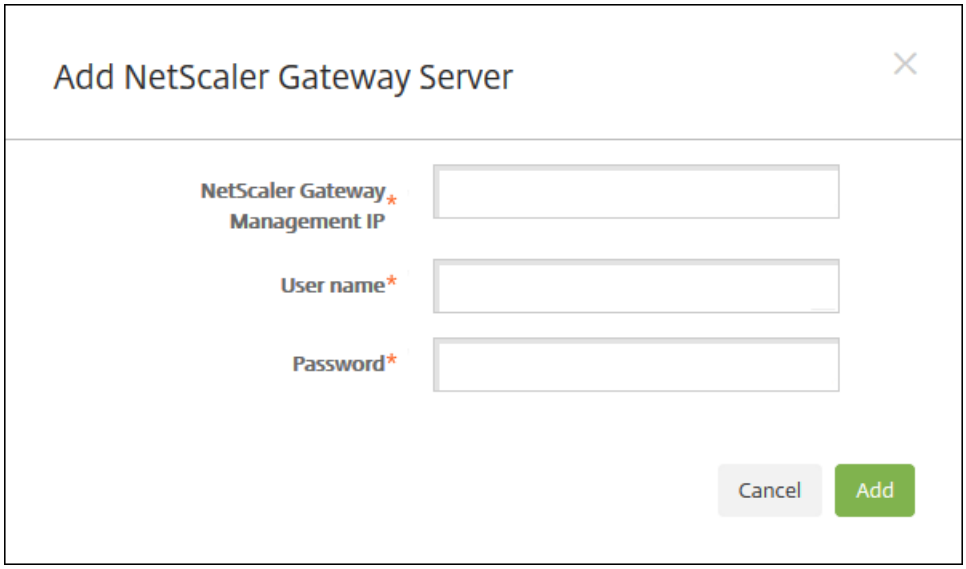
Remarque : si vous choisissez **Infos sur l'utilisateur et les appareils** ou **Toutes les données**, et s'il s'agit du premier pack d'assistance que vous créez, la boîte de dialogue **Avis de non-responsabilité : données sensibles** s'affiche. Lisez l'avis, puis cliquez sur **Accepter** ou **Annuler**. 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. Sous **Inclure depuis la base de données** est affichée une notification indiquant si les informations liées à l'utilisateur, au serveur ou au réseau sont rendues anonymes dans les packs d'assistance. Par défaut, les données sont rendues anonymes. Vous pouvez modifier ce paramètre en cliquant sur le lien **Anonymisation et réidentification**. VoirAnonymisation des données dans les packs d'assistance pour de plus amples informations sur l'anonymisation des données.

6. Sélectionnez le **Pack d'assistance pour NetScaler Gateway** si vous souhaitez inclure des packs d'assistance NetScaler Gateway, puis procédez comme suit :

- Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un serveur NetScaler Gateway** s'affiche.



- Dans **Adresse IP de gestion de NetScaler Gateway**, entrez l'adresse IP de gestion de NetScaler 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 NetScaler Gateway qui est déjà ajouté, l'adresse IP est renseignée.

- Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification utilisateur requises pour accéder au serveur exécutant NetScaler Gateway.

  Remarque : si vous créez un pack à partir d'un serveur NetScaler Gateway qui est déjà ajouté, le nom d'utilisateur est renseigné.

7. Cliquez sur **Add**. Le nouveau pack d'assistance NetScaler Gateway est ajouté au tableau.

8. Répétez l'étape 7 pour ajouter des packs d'assistance NetScaler Gateway supplémentaires.

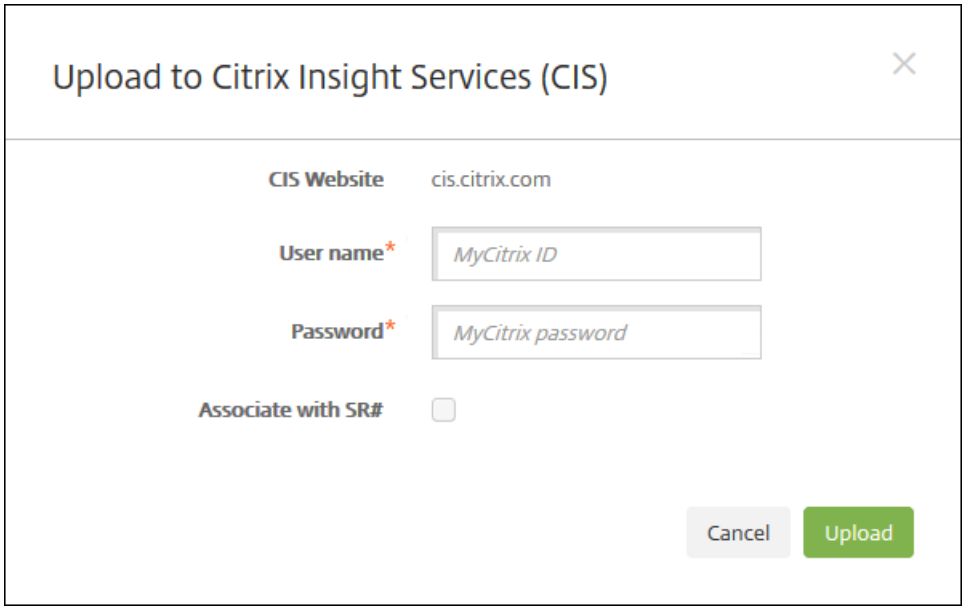
9. Cliquez sur **Créer**. Le pack d'assistance est créé et deux nouveaux boutons, **Charger sur CIS** et **Télécharger sur le client** s'affichent.

Passez à Chargement de packs d'assistance sur Citrix Insight Services ou Téléchargement de packs d'assistance sur un client.

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. Ces étapes vous montrent comment charger le pack sur CIS. Vous avez besoin d'un ID et d'un mot de passe MyCitrix pour charger 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 MyCitrix.

3. Dans le champ **Mot de passe**, entrez votre mot de passe MyCitrix.

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**, entrez le numéro de demande de service à huit chiffres que vous souhaitez associer à ce pack.
- 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.

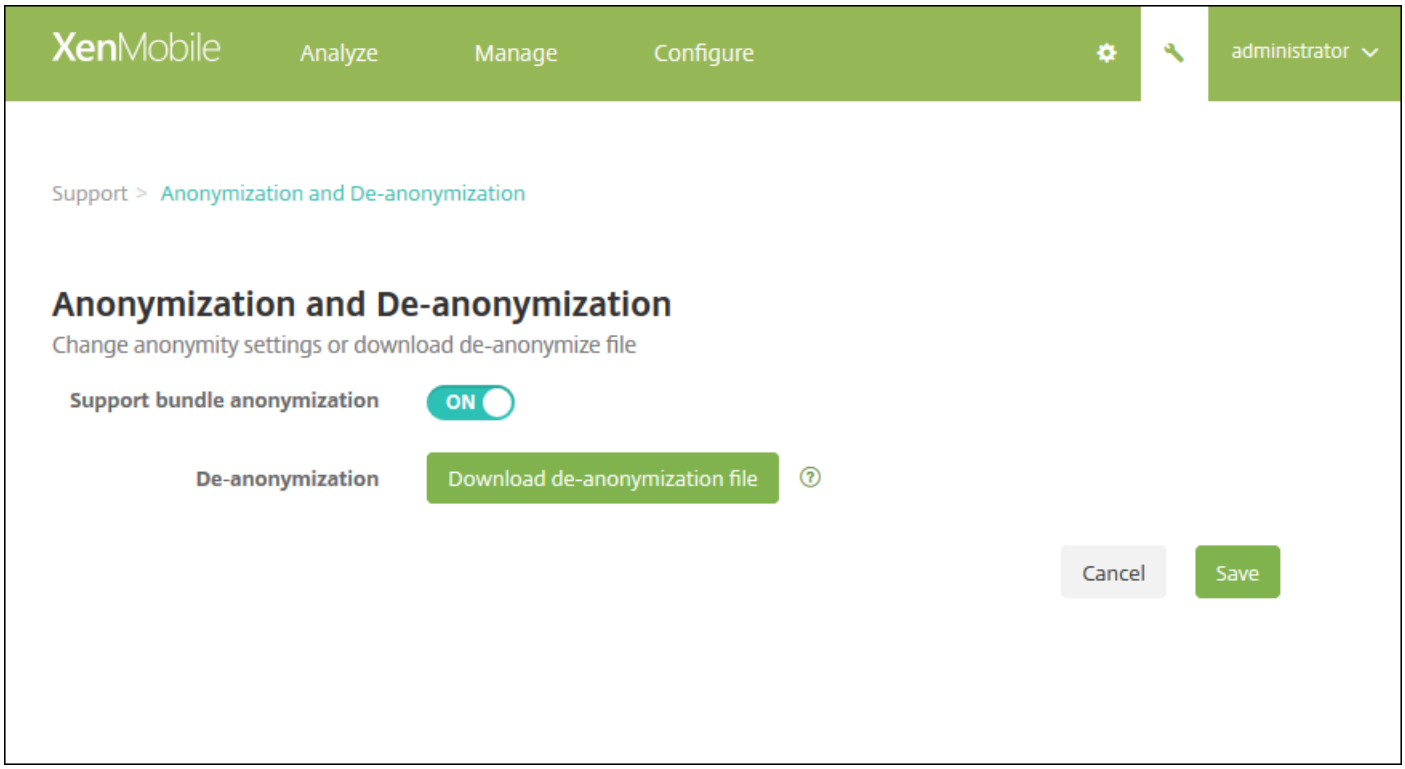
Anonymisation des données dans les packs d'assistance

Jul 27, 2016

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 **ON**.

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.

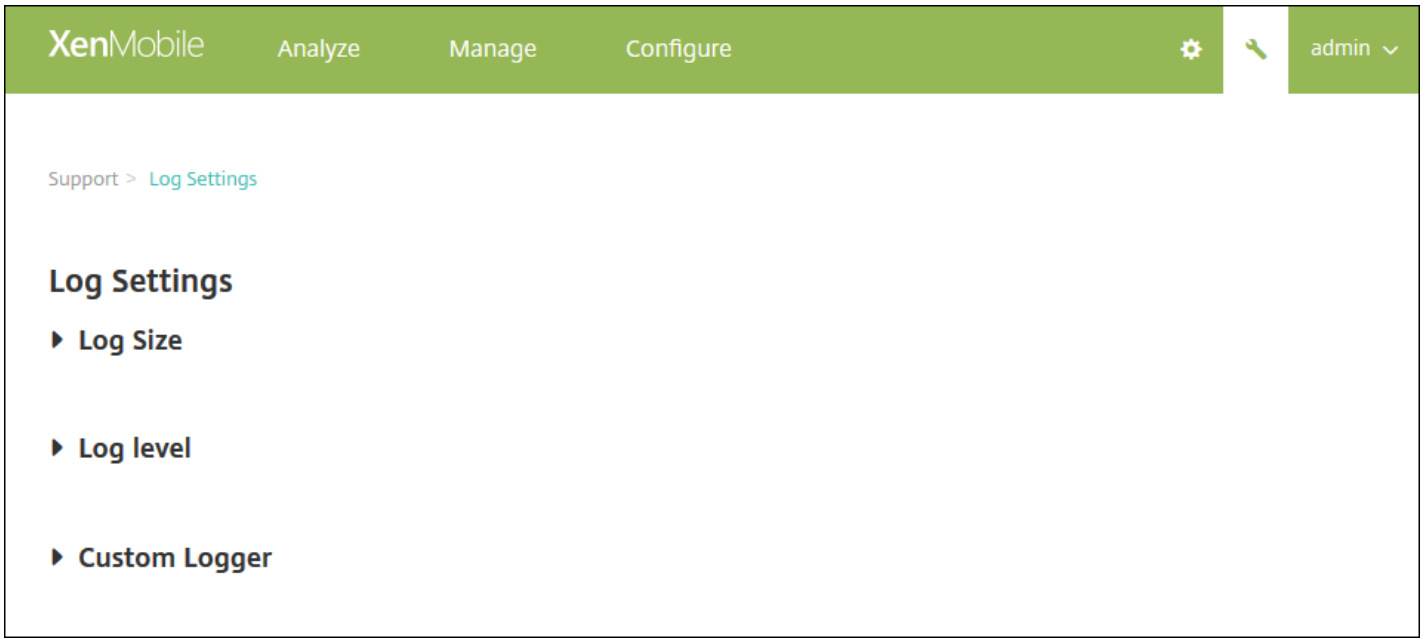
Configuration des paramètres du journal

Jul 27, 2016

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.

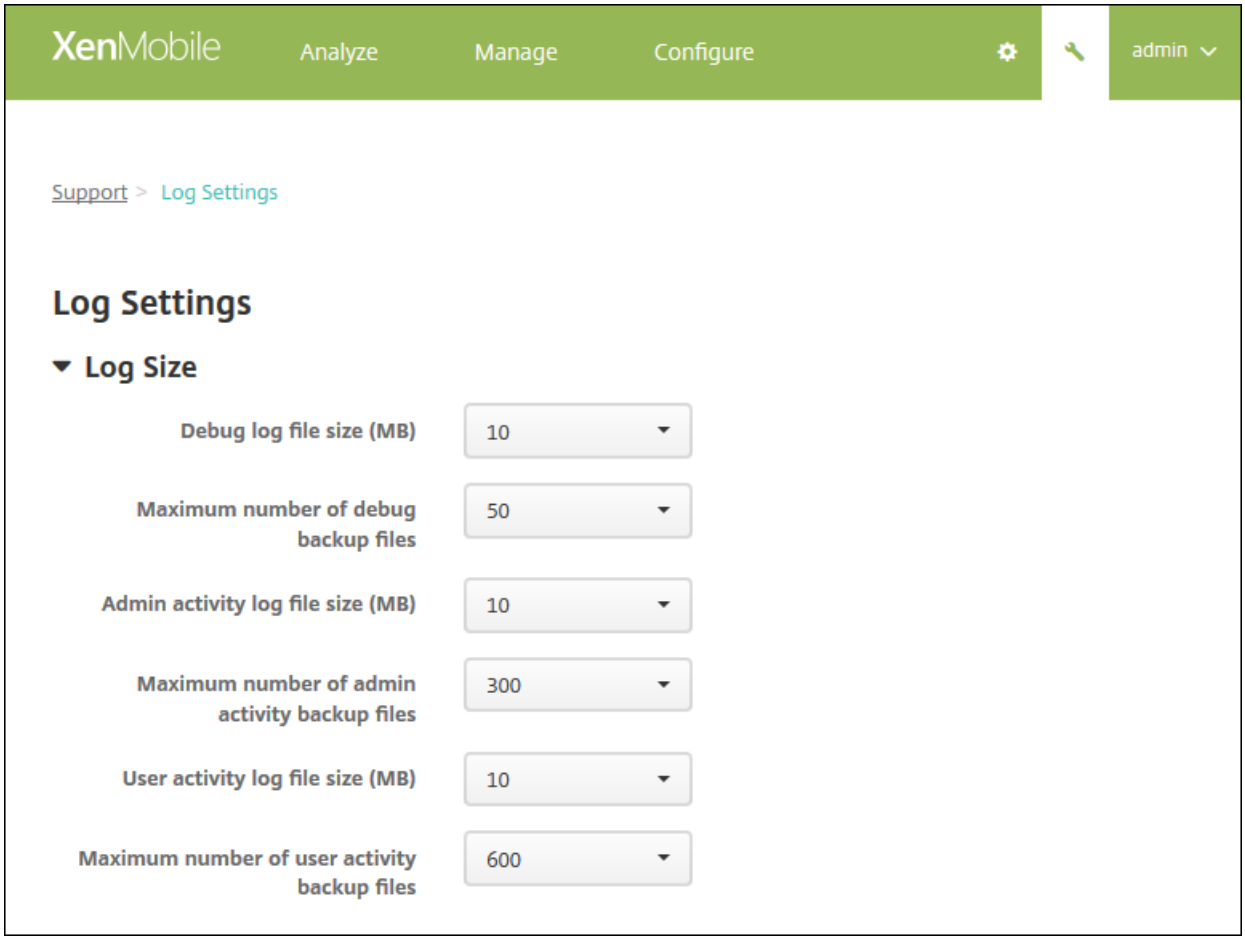


Sur la page **Paramètres du journal**, vous pouvez accéder aux options suivantes :

- **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. Configurez les paramètres suivants :

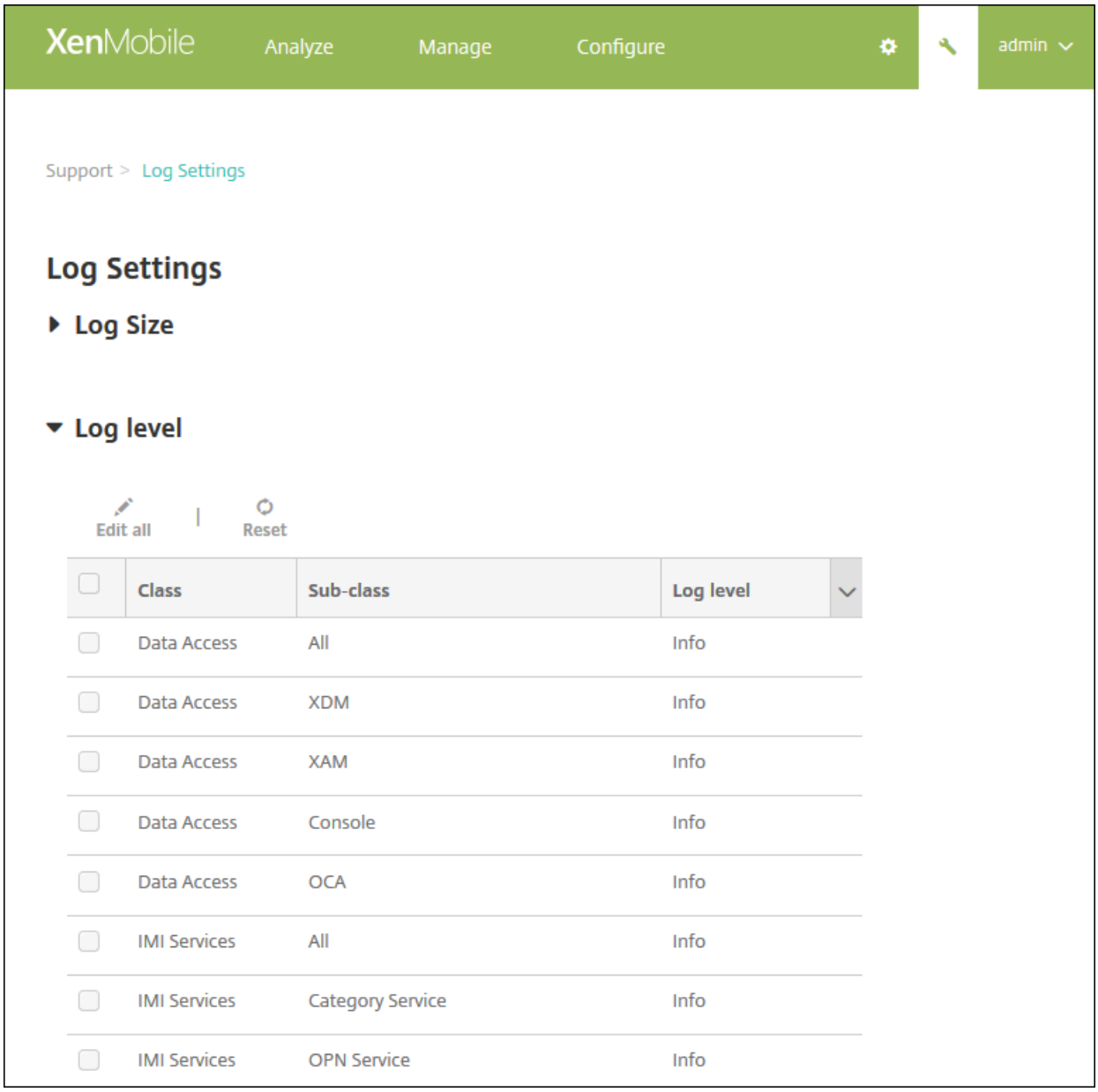
- **Taille du fichier journal de débogage (Mo)**: dans la liste, sélectionnez une taille comprise entre 5 et 20 Mo pour modifier la taille maximale du fichier de débogage. La valeur par défaut de la taille du fichier est de **10 Mo**.
- **Nombre maximum de fichiers de sauvegarde de débogage** : dans 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.

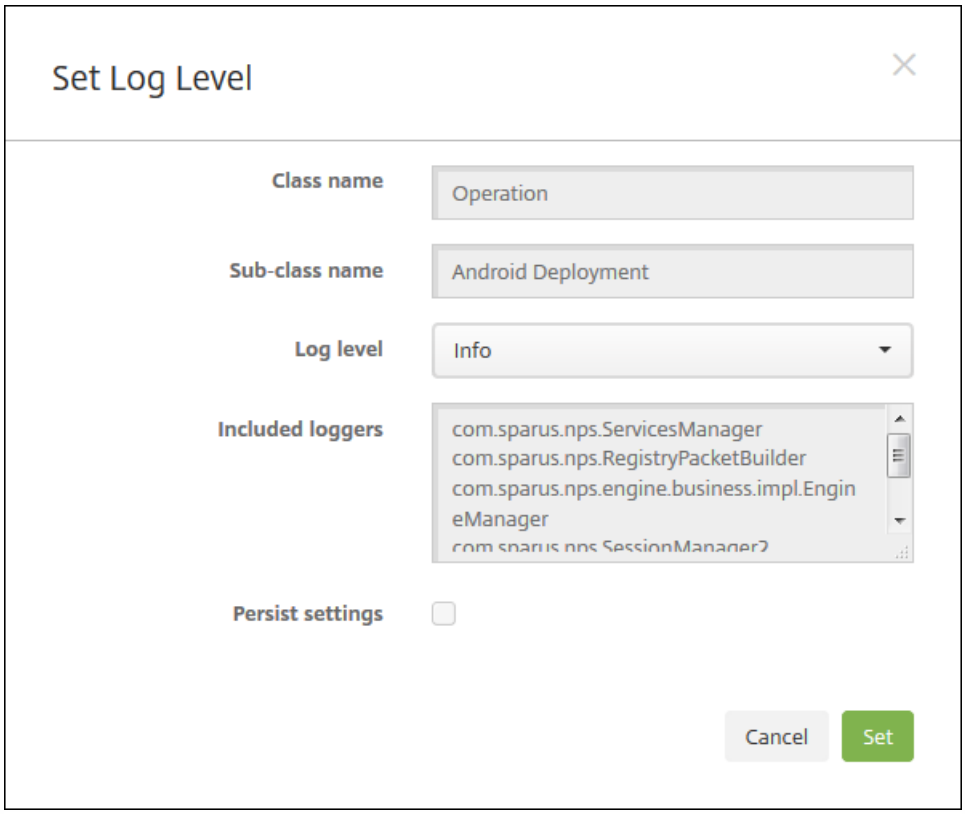
1. Sur la page **Paramètres du journal**, développez **Niveau de journalisation**. Un tableau de toutes les classes de journal s'affiche.



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** s'affiche ; vous pouvez y définir le niveau de journalisation et indiquer si les paramètres de niveau de journalisation persistent lorsque vous redémarrez le serveur XenMobile.



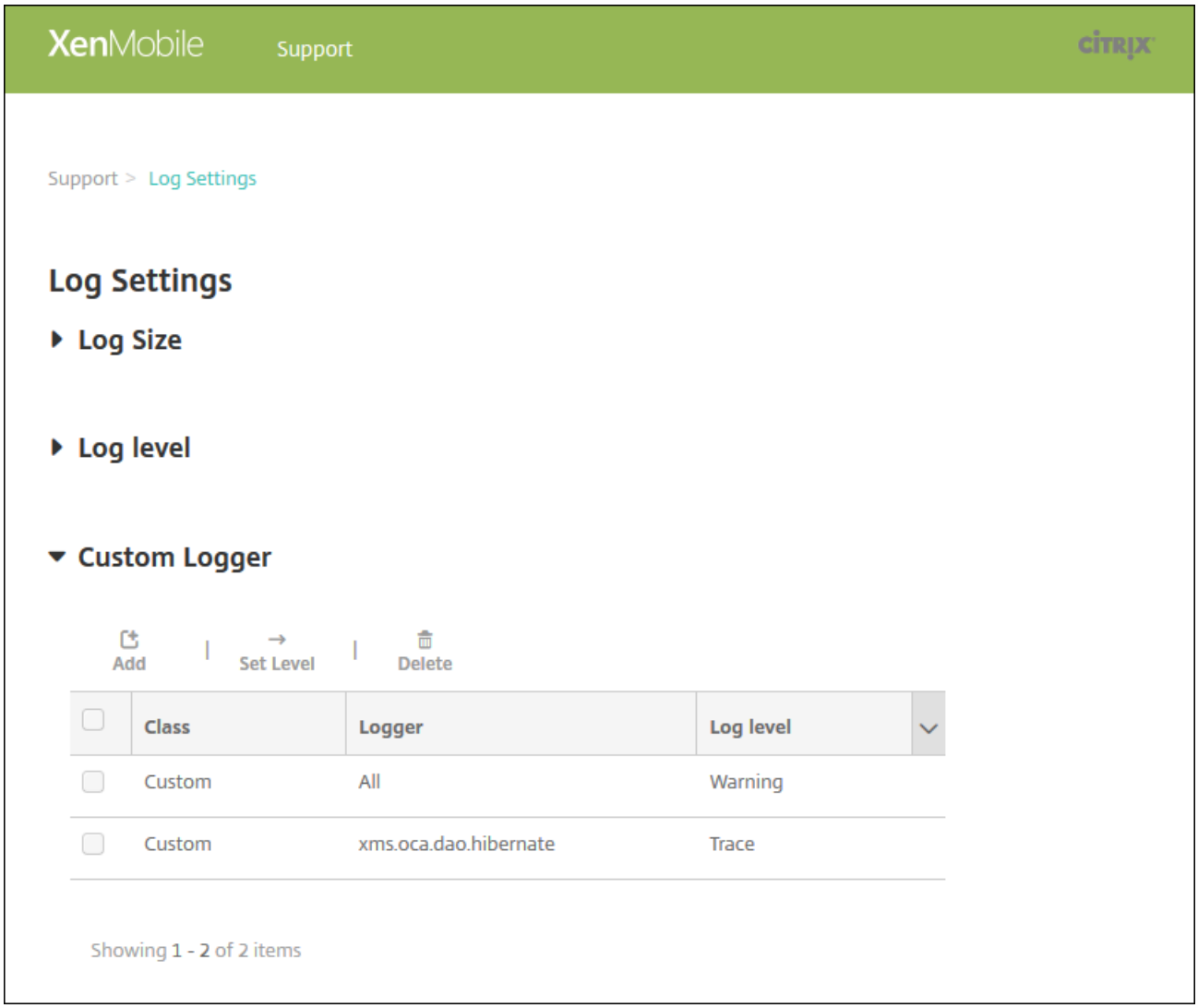
- **Nom de la classe** : ce champ affiche Tout lorsque vous modifiez le niveau de journalisation pour toutes les classes ou il affiche le nom de la classe individuelle ; il n'est pas modifiable.
- **Nom de la sous-classe** : ce champ affiche Tout lorsque vous modifiez le niveau de journalisation pour 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
  - Erreur
  - Avertissement
  - Info
  - Débogage
  - Trace
  - Off
- **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 à cocher. 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.

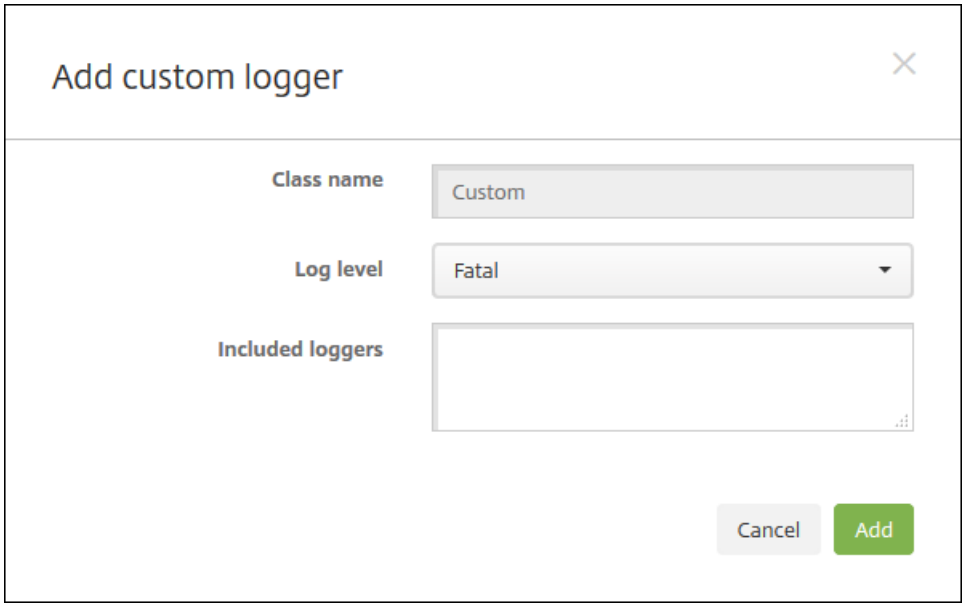
Pour ajouter un enregistreur d'événements personnalisé

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.



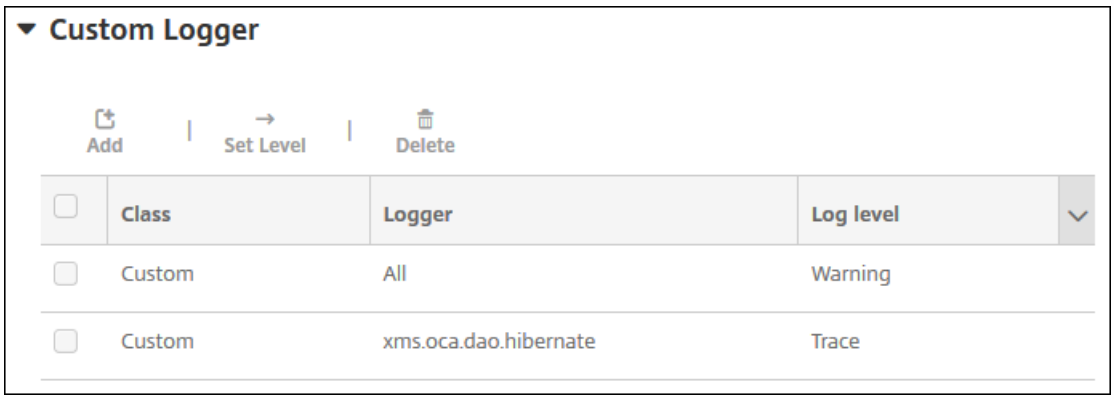
2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un enregistreur d'événements personnalisé** apparaît.



3. Configurez les paramètres suivants :

- **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
  - Erreur
  - Avertissement
  - Info
  - Débogage
  - Trace
  - Off
- **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**.

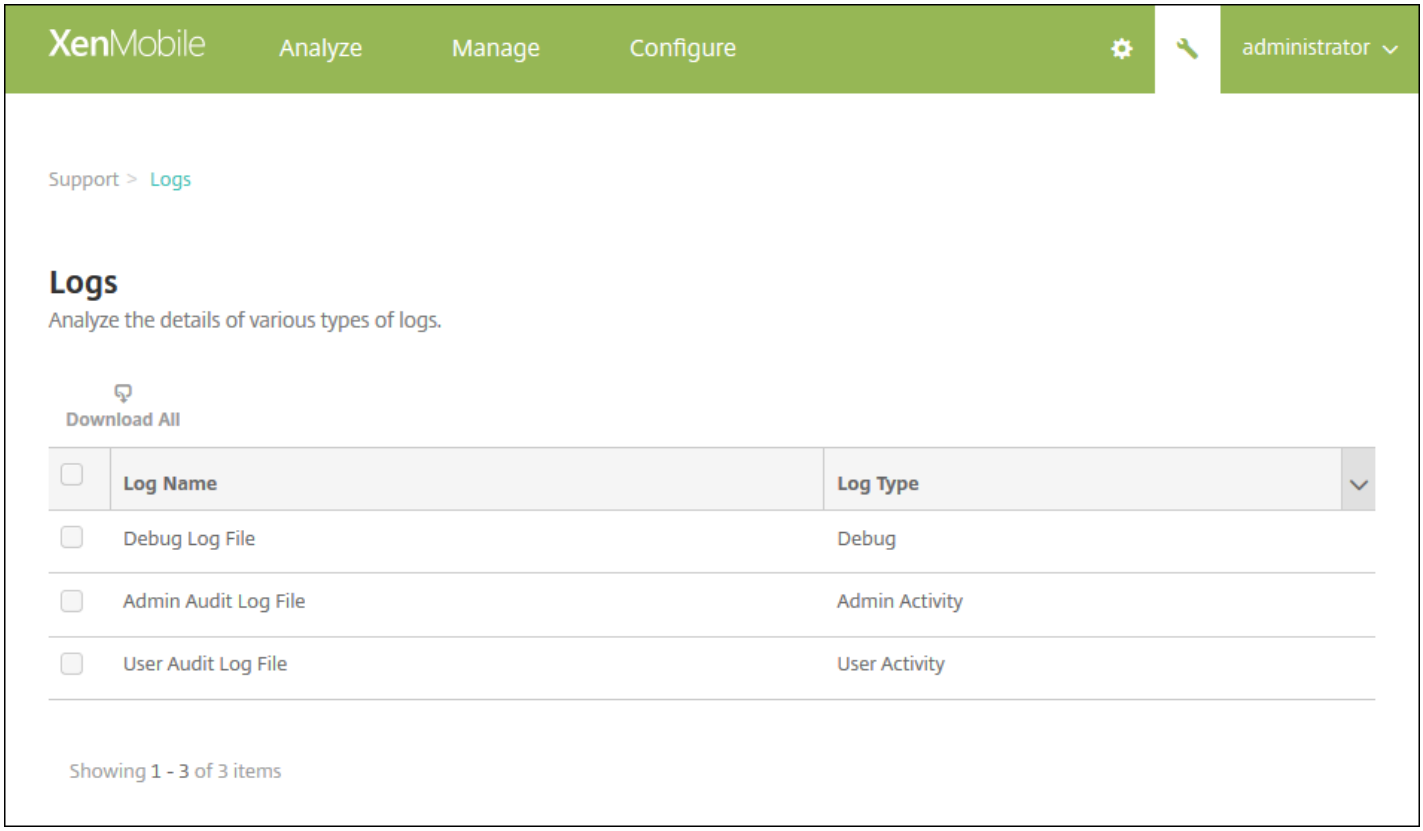
Important : vous ne pouvez pas annuler cette opération.

Visualisation et analyse des fichiers journaux dans XenMobile

Jul 27, 2016

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.

4. Utilisez les actions en haut du tableau pour télécharger tout, afficher, alterner, télécharger un journal ou supprimer le journal sélectionné.

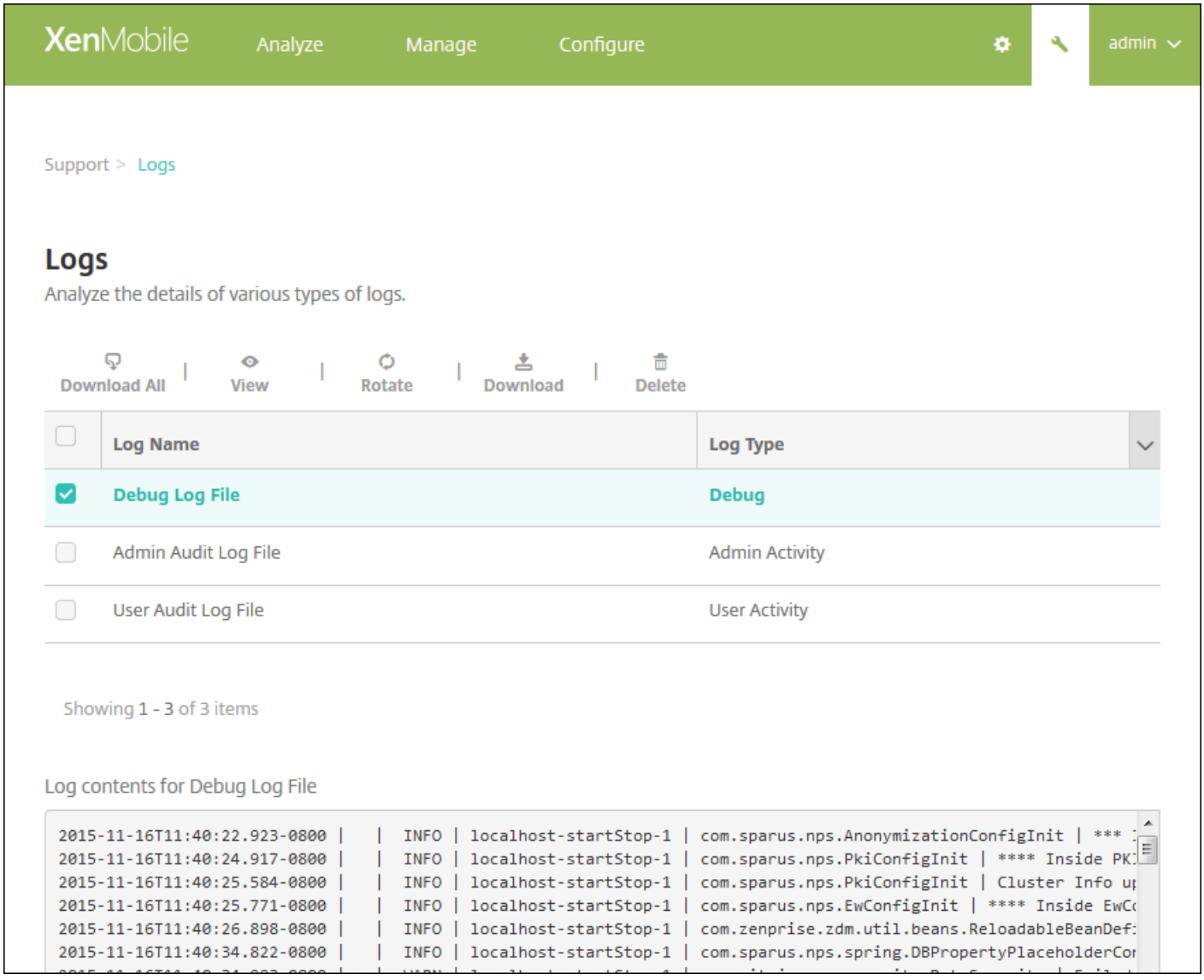
Remarque :

- Si vous sélectionnez plus d'un fichier journal, seules les options **Tout télécharger** et **Supprimer** 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.



Remote Support

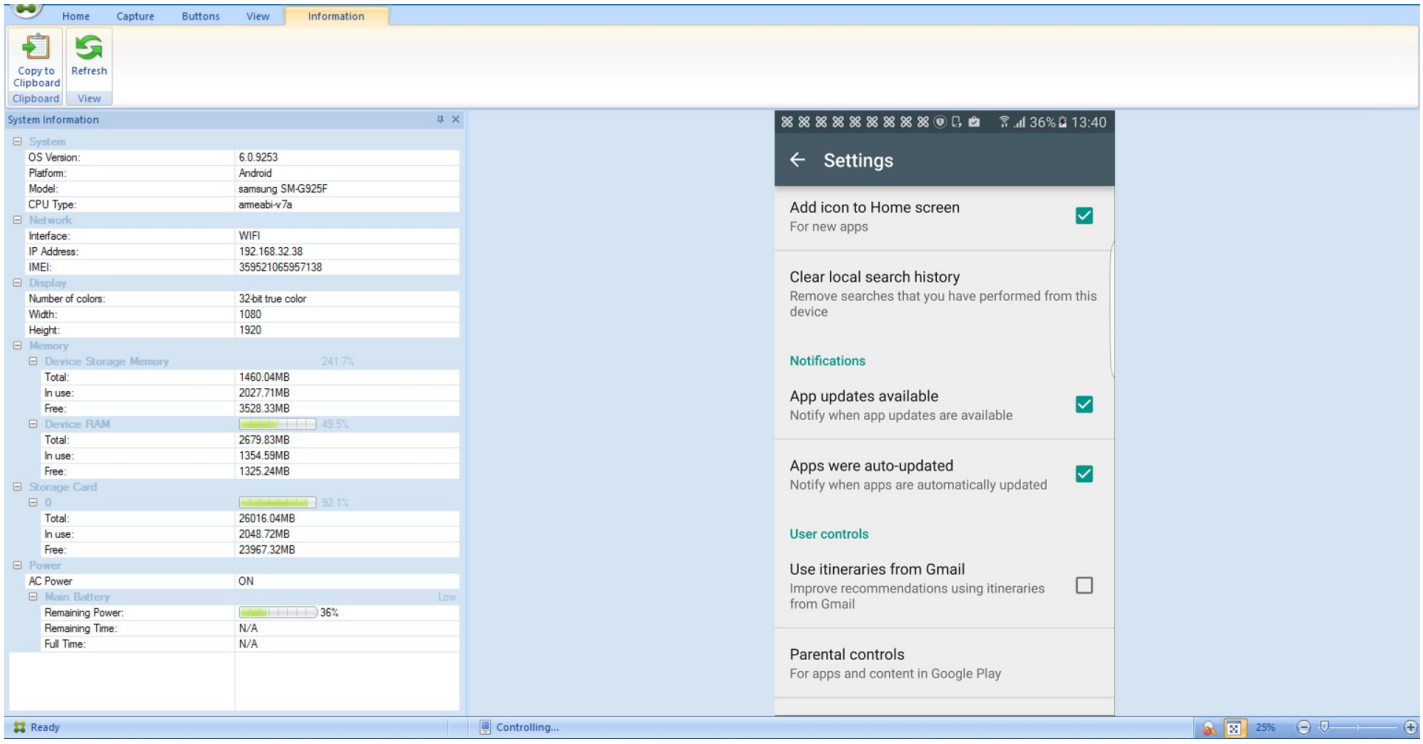
Jul 27, 2016

Remote Support permet aux représentants du service d'assistance de contrôler à distance des appareils mobiles Windows et Android gérés. L'application Remote Support est disponible sur tous les appareils mobiles Windows et sur les appareils Android Samsung SAFE. Le contrôle à distance des appareils iOS n'est pas pris en charge.

> ## Remarque
>
> XenMobile Remote Support n'est pas disponible dans les versions 10.x. de XenMobile Cloud.

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 de Remote Support voient la fenêtre de l'application Remote Support et une fenêtre Remote Control avec un rendu de l'appareil contrôlé.



Remote Support permet d'effectuer ce qui suit :

- Se connecter à distance à l'appareil mobile d'un utilisateur et contrôler l'écran de l'utilisateur. 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.

Remote Support permet également au personnel du service d'assistance technique d'effectuer ce qui suit :

- Afficher une liste de tous les appareils connectés à un ou plusieurs serveurs 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 du serveur XenMobile.
- Exécuter le gestionnaire des tâches de l'appareil afin de pouvoir afficher et mettre fin à des processus 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 Remote Support

Le logiciel Remote Support 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 de RAM minimum
- 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
- Microsoft Windows 8
- Microsoft Windows 7

Pour installer le logiciel Remote Support

1. Pour télécharger le programme d'installation de Remote Support, accédez à la page de téléchargement de XenMobile 10 et connectez-vous à votre compte.
2. Développez **Tools** et téléchargez XenMobile Remote Support v9.
   Le nom du fichier Remote Support est XenMobileRemoteSupport-9.0.0.35265.exe.
3. Cliquez deux fois sur le programme d'installation de Remote Support et suivez les instructions de l'assistant d'installation.

Pour installer Remote Support à partir de la ligne de commande :

Exécutez la commande suivante :

RemoteSupport.exe /S

où *RemoteSupport* correspond au nom du programme d'installation. Par exemple :

XenMobileRemoteSupport-9.0.0.35265.exe/S

Vous pouvez utiliser les variables suivantes lors de l'installation du logiciel Remote Support :

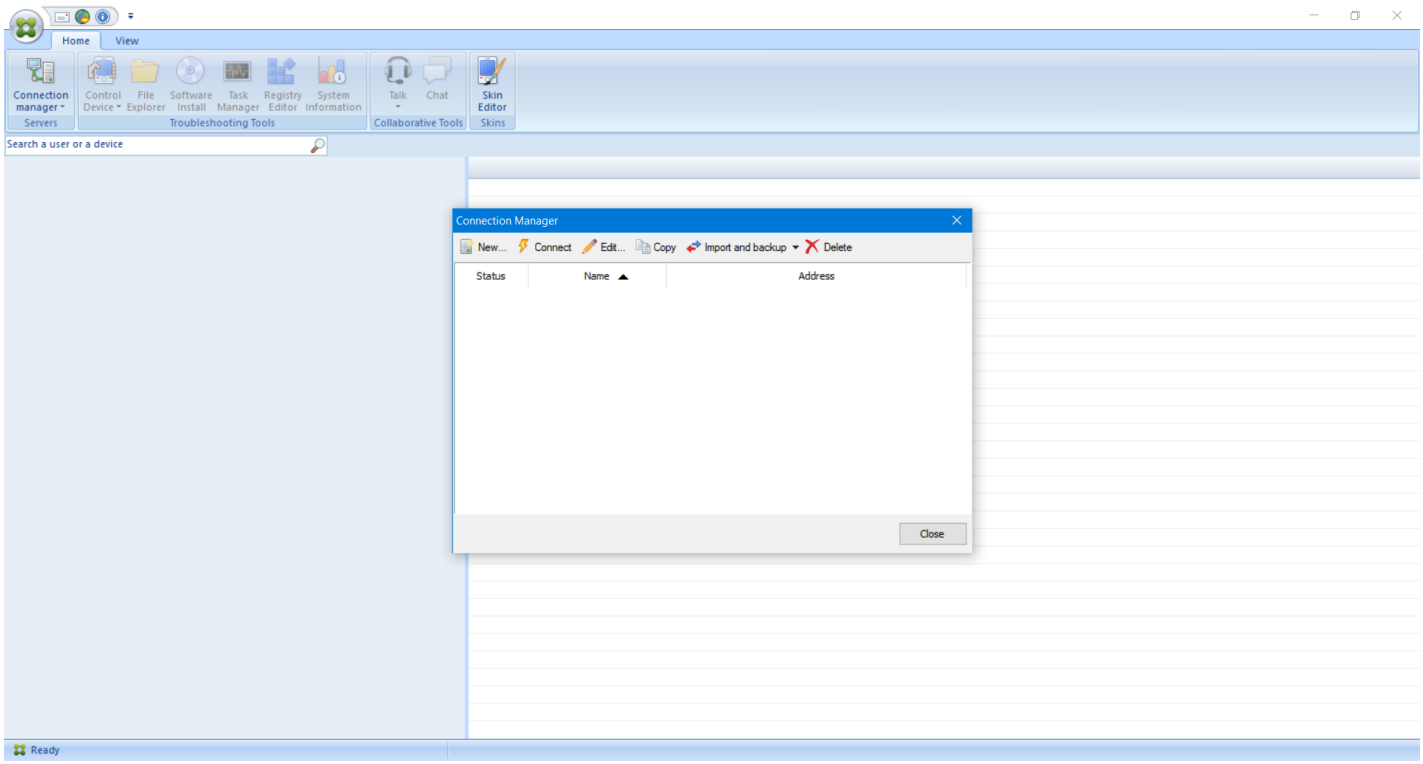
- /S: pour installer de manière silencieuse le logiciel Remote Support avec les paramètres par défaut.
- /D=dir: pour spécifier un répertoire d'installation personnalisé.

Pour connecter Remote Support à XenMobile

Pour établir des connexions d'assistance à distance avec des appareils gérés, vous devez ajouter une connexion depuis Remote Support vers le ou les serveurs XenMobile qui gèrent les appareils. Cette connexion s'exécute sur un tunnel applicatif défini dans la stratégie de tunnel, une stratégie pour les appareils Android et Windows Mobile/CE. Le tunnel applicatif doit être défini comme décrit dans la section Stratégies de tunnel applicatif avant de pouvoir connecter Remote Support à XenMobile.

1. Démarrez le logiciel Remote Support 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 :

   Dans **Configuration name**, entrez un nom pour l'entrée de configuration.

   Dans **Server IP address or name**, entrez l'adresse IP ou le nom DNS du serveur XenMobile.

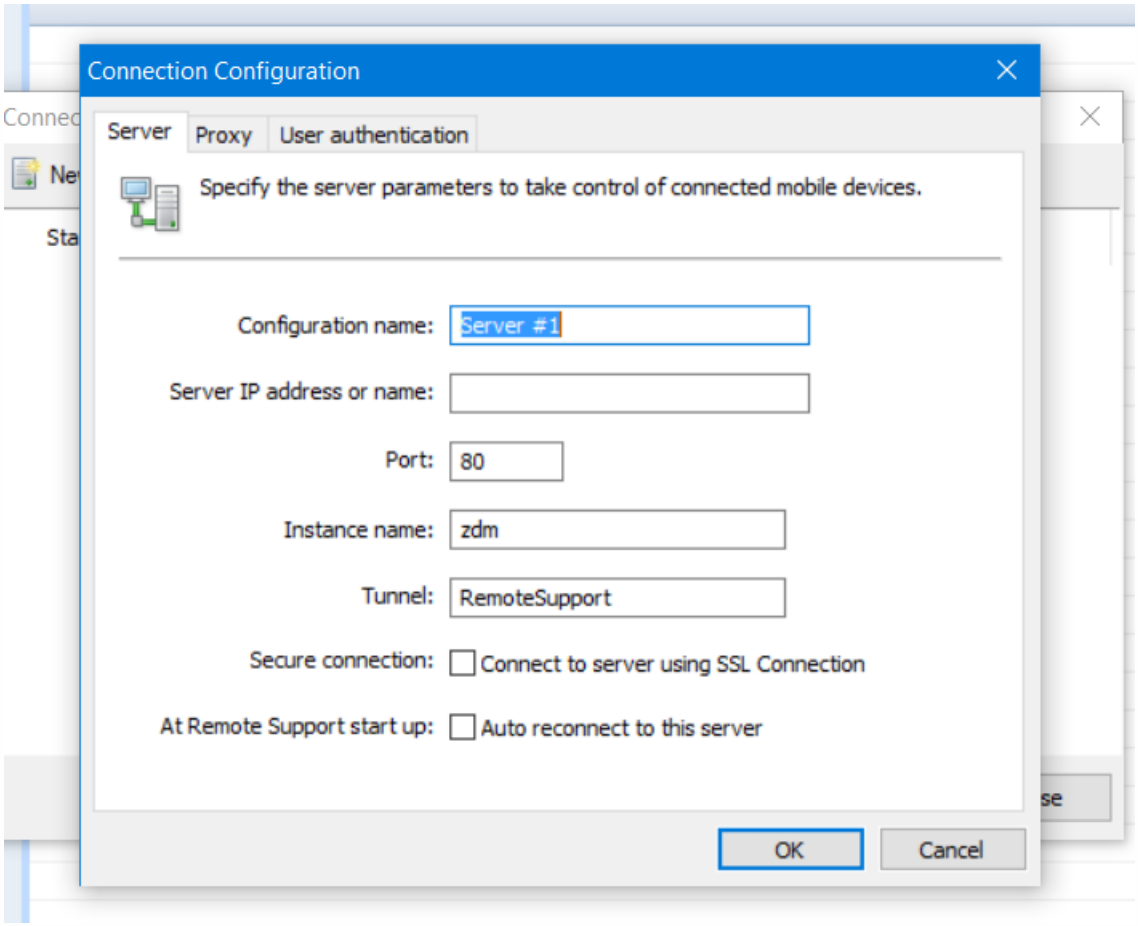
   Dans **Port**, entrez un numéro de port TCP, comme défini dans la configuration du serveur XenMobile.

   Dans **Instance name**, si XenMobile fait partie d'un déploiement Multi-Tenant, entrez un nom d'instance.

   Dans **Tunnel**, entrez le nom de la Stratégie de tunnel.

   Sélectionnez la case **Connect to server using SSL Connection**.

   Sélectionnez la case **Auto reconnect to this server** pour vous connecter au serveur XenMobile configuré chaque fois que l'application Remote Support démarre.



4. Sur l'onglet **Proxy**, sélectionnez **Use a http proxy server** et entrez les informations suivantes :

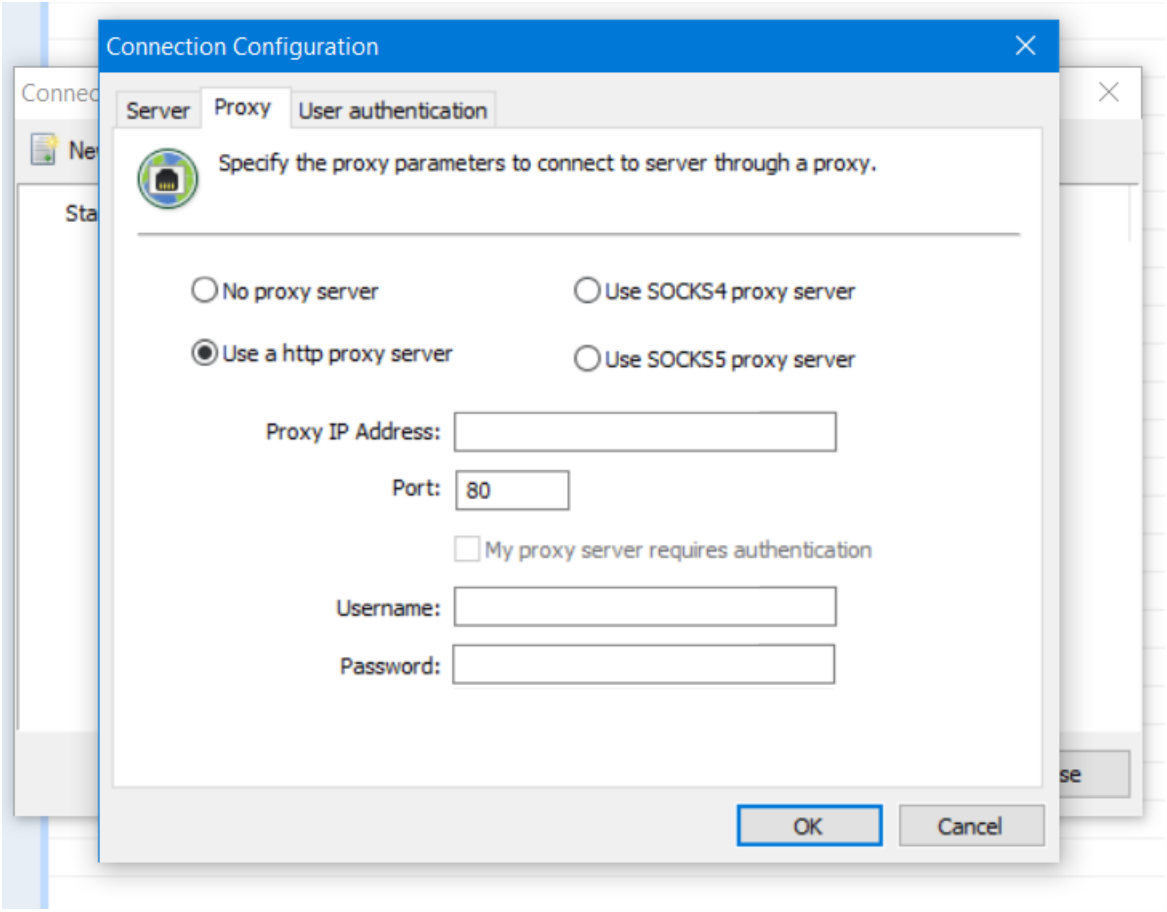
   Dans **Proxy IP Address**, saisissez l'adresse IP du serveur proxy.

   Dans **Port**, saisissez le numéro de port TCP utilisé par le proxy.

   Sélectionnez la case **My proxy server requires authentication** si le serveur proxy requiert une authentification pour autoriser le trafic.

   Dans **Username**, saisissez le nom de l'utilisateur qui doit être authentifié sur le serveur proxy.

   Dans **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 pouvez créer 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 : 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, y compris le contrôle des couleurs (dans la fenêtre principale ou dans une fenêtre distincte flottante), d'établir une session Voix-sur-

IP (VoIP) entre le bureau d'assistance et l'utilisateur, de configurer des paramètres et d'établir une session de chat entre le bureau d'assistance et l'utilisateur.

Pour de plus amples informations sur la configuration de la stratégie Assistance à distance, consultez la Stratégie d'assistance à distance.

Pour utiliser une session Remote Support

Lorsque vous démarrez Remote Support, la partie gauche de la fenêtre de l'application Remote Support présente des groupes d'utilisateurs XenMobile, comme défini dans la console d'administration 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 plusieurs façons :

- Contrôler l'écran de l'appareil, y compris 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 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.

Options d'interface de ligne de commande XenMobile

Jul 27, 2016

Vous pouvez accéder à tout moment aux options d'interface de ligne de commande suivantes (CLI) sur l'hyperviseur sur lequel vous avez installé XenMobile : Citrix XenServer, Microsoft Hyper-V ou VMware ESXi.

Vous trouverez ci-après les choix que vous pouvez effectuer dans le menu principal et les menus qui s'affichent pour chacune des quatre premières options : Configuration, Mise en cluster, Système, et Dépannage.

Menu principal

---

[0] Configuration

[1] Mise en cluster

[2] Système

[3] Dépannage

[4] Aide

[5] Fermer la session

Choix : [0 - 5]

Options du menu de configuration

À partir du menu principal, lorsque vous sélectionnez l'option Configuration, les menus suivants s'affichent :

[0] Retour au menu principal

[1] Réseau

[2] Pare-feu

[3] Base de données

[4] Ports d'écoute

Choix : [0 - 4]

Lorsque vous choisissez l'option Réseau, vous êtes invité à redémarrer pour enregistrer les modifications.

Lorsque vous choisissez l'option Pare-feu, vous êtes invité à effectuer ce qui suit :

Configurer les services qui sont activés via le pare-feu.

Possibilité de configurer l'accès aux listes blanches :

- liste séparée par des virgules d'hôtes ou de réseaux

- par exemple 10.20.5.3, 10.20.6.0/24

- une valeur vide signifie aucune restriction d'accès

- entrez la valeur c pour effacer la liste

Service HTTP

Port : 80

Activer l'accès (y/n) [Y]:

Service HTTPS de gestion

Port : 4443

Activer l'accès (y/n) [Y]:

Service SSH

Port [22]:

Activer l'accès (y/n) [Y]:

Accès liste blanche []:

Service HTTPS de l'API de gestion (pour la gestion intermédiaire)

Port [30001]:

Activer l'accès (y/n) [Y]:

Accès liste blanche []:

Tunnel d'assistance à distance

Port [8081]:

Activer l'accès (y/n) [n]:

Lorsque vous choisissez l'option Base de données, vous êtes invité à effectuer ce qui suit :

Type: [mi]

Utiliser SSL (y/n) [y]:

Charger le certificat racine (y/n) [y]:

Copier ou Importer (c/i) [c]:

Options du menu de mise en cluster

À partir du menu principal, lorsque vous sélectionnez l'option Mise en cluster, les menus suivants s'affichent :

[0] Retour au menu principal

[1] Afficher l'état du cluster

[2] Activer/désactiver le cluster

[3] Liste blanche des membres du cluster

[4] Activer ou désactiver le déchargement SSL

[5] Afficher le cluster Hazelcast

Choix : [0 - 5]

Lorsque vous choisissez d'activer la mise en cluster, le message suivant s'affiche :

Pour activer la communication en temps réel entre membres du cluster, ouvrez le port 80 à l'aide de l'option du menu Pare-feu du menu CLI. Vous pouvez également configurer la liste blanche d'accès dans les paramètres du pare-feu pour limiter l'accès.

Lorsque vous choisissez de désactiver la mise en cluster, le message suivant s'affiche :

Vous avez choisi de désactiver la mise en cluster. L'accès au port 80 n'est pas nécessaire. Veuillez le désactiver.

Lorsque vous sélectionnez la liste blanche de membre du cluster, et que vous avez désactivé la mise en cluster, le message suivant s'affiche :

Le cluster est désactivé. Veuillez l'activer.

Si la mise en cluster est activée, les options suivantes s'affichent :

Liste blanche actuelle :

- liste séparée par des virgules d'hôtes ou de réseaux

- par exemple 10.20.5.3, 10.20.6.0/24

- une valeur vide signifie aucune restriction d'accès

Veuillez entrer les hôtes ou réseaux à mettre sur liste blanche :

Si vous choisissez d'activer ou de désactiver le déchargement SSL, le message suivant s'affiche :

L'activation du déchargement SSL ouvrira le port 80 pour tout le monde. Veuillez configurer l'accès à la liste blanche dans les paramètres du pare-feu pour un accès limité.

Lorsque vous sélectionnez d'afficher le cluster Hazelcast, les options suivantes s'affichent :

Membres du cluster Hazlecast :

[Adresse IP répertoriée]

REMARQUE : si un nœud configuré ne fait pas partie du cluster, veuillez redémarrer ce nœud.

Options du menu Système

À partir du menu principal, lorsque vous sélectionnez l'option Système, les menus suivants s'affichent :

---

[0] Retour au menu principal

[1] Afficher la date système

[2] Définir le fuseau horaire

[3] Afficher l'utilisation du disque système

[4] Mettre à jour le fichier d'hôtes

[5] Serveur proxy

[6] Mot de passe (CLI) administrateur

[7] Redémarrer le serveur

[8] Arrêter le serveur

[9] Paramètres avancés

Choix : [0 - 9]

Options du menu Dépannage

À partir du menu principal, lorsque vous sélectionnez l'option Dépannage, les menus suivants s'affichent :

---

[0] Retour au menu principal

[1] Utilitaires de réseau

[2] Journaux

[3] Pack d'assistance

Choix : [0 - 3]

Lorsque vous sélectionnez l'option Utilitaires de réseau, le menu suivant s'affiche :

---

[0] Retour au menu de dépannage

[1] Informations réseau

[2] Afficher la table de routage

[3] Afficher la table ARP (Protocole de résolution d'adresse)

[4] PING

[5] Détermination d'itinéraire

[6] Recherche DNS

[7] Trace réseau

Choix : [0 - 7]

Lorsque vous sélectionnez l'option Journaux, le menu suivant s'affiche :

Menu Journaux

---

[0] Retour au menu de dépannage

[1] Afficher le fichier journal

Choix : [0 - 1]

XenMobile Analyzer Tool

Oct 17, 2016

XenMobile Analyzer est un outil sur cloud que vous pouvez utiliser pour diagnostiquer et résoudre les problèmes d'installation 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.

Pour activer la vérification, vous devez configurer l'outil afin qu'il pointe vers votre serveur XenMobile et fournir des informations, telles que le type de déploiement de serveur, la plate-forme mobile, le type d'authentification et les informations d'identification utilisateur à utiliser pour le test. 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.

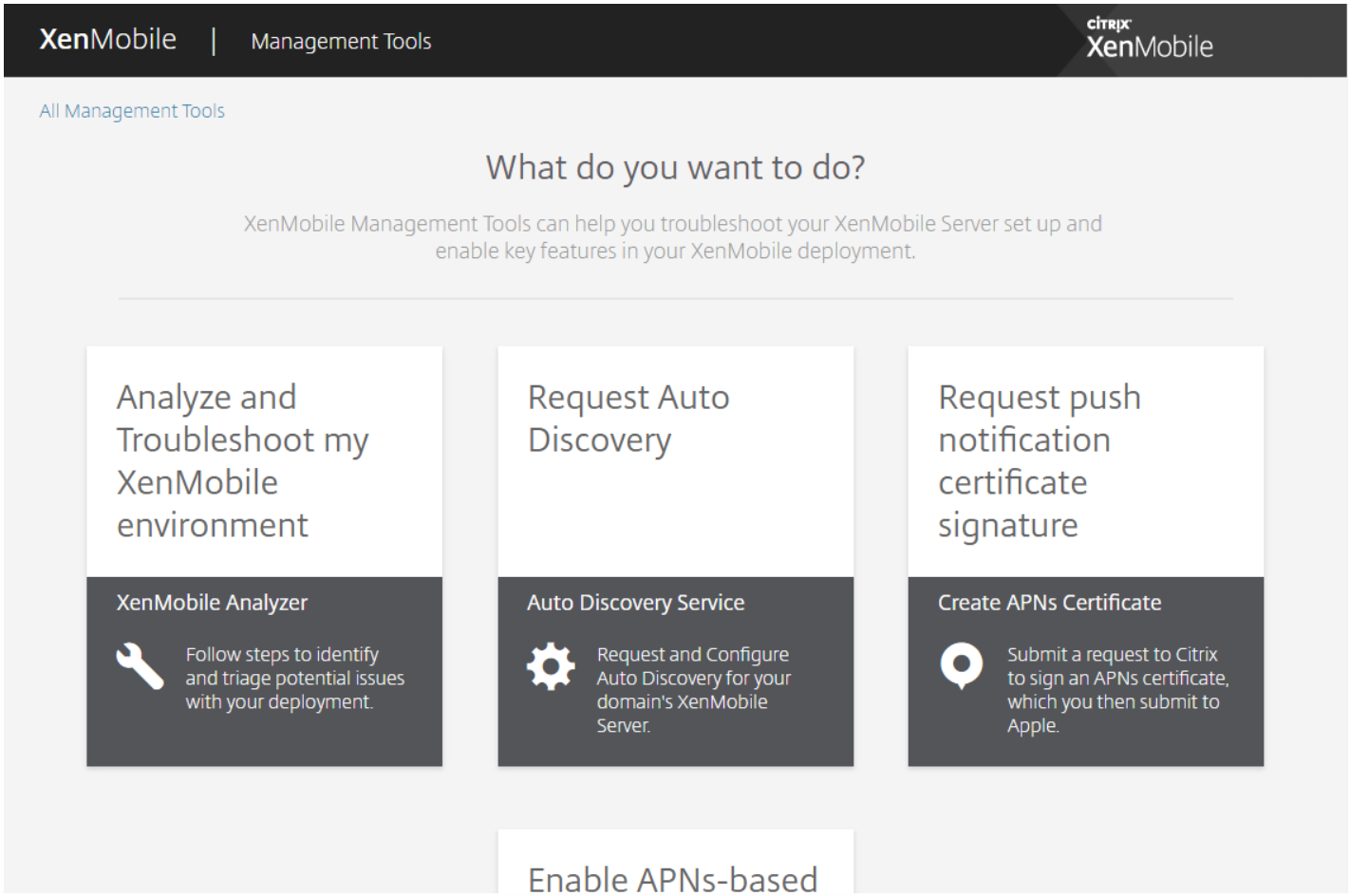
Fonctionnalités principales de XenMobile Analyzer

- Offre un micro-service sécurisé dans le cloud permettant de dépanner tous les problèmes liés à XenMobile.
- Fournit des recommandations précises en cas de problème avec la configuration de XenMobile.
- Réduit le nombre d'appels à l'assistance et accélère le dépannage des environnements XenMobile.
- Offre une assistance le jour même pour les versions du serveur XenMobile.
- Permet l'inscription personnalisée sur iOS : prise en charge de ports personnalisés pour XenMobile (sur les ports autres que le port 8443).
- Affiche une boîte de dialogue d'acceptation du certificat pour les certificats de serveur non approuvés ou incomplets.
- Détecte automatiquement les scénarios d'authentification à deux facteurs.
- Tests WorxWeb d'accessibilité aux sites intranet.
- Vérification du service de détection automatique de WorxMail.
- Vérification de l'authentification unique ShareFile.
- Permet la prise en charge de ports personnalisés pour NetScaler.
- Prend en charge les navigateurs autres que ceux en langue anglaise.

Conditions préalables

Produit	Version prise en charge
Serveur XenMobile	10.3.0 - 10.3.6
NetScaler Gateway	10.5 - 11.1
Simulation d'inscription de client	iOS et Android

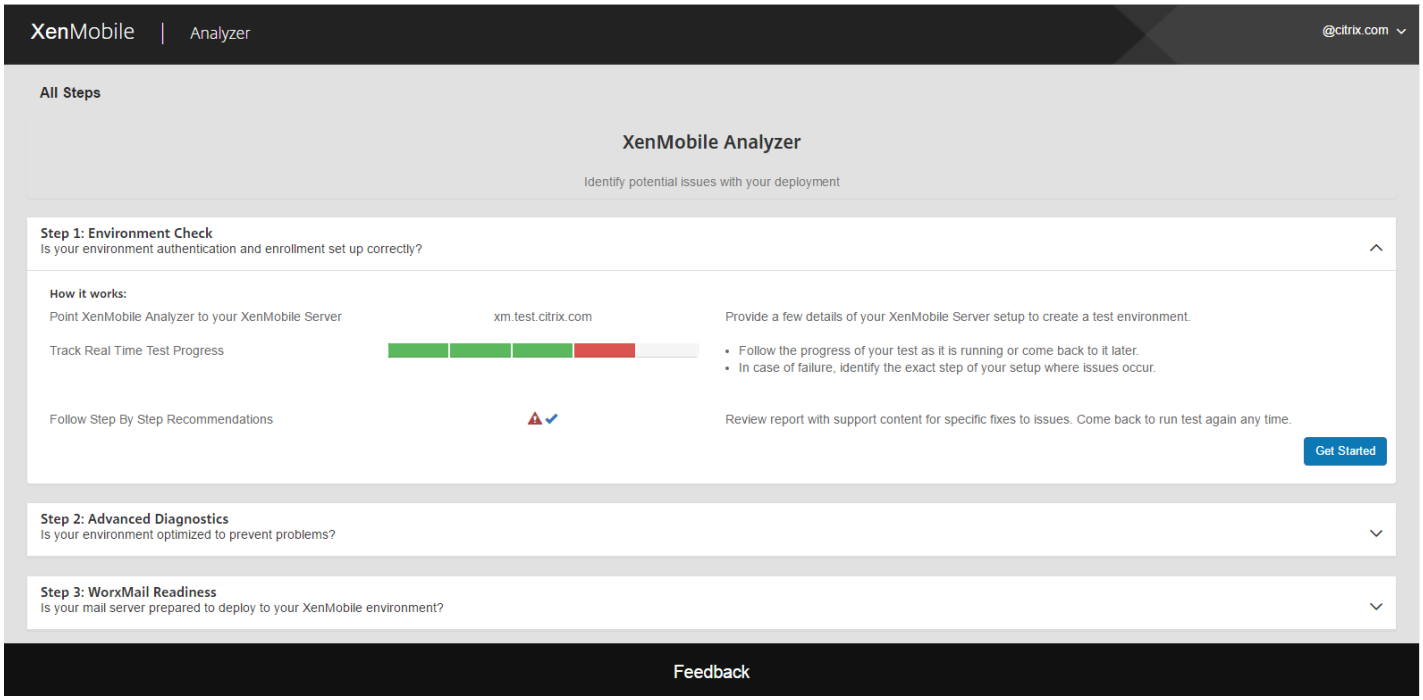
Vous pouvez utiliser les informations d'identification MyCitrix pour accéder à l'outil depuis https://xenmobiletools.citrix.com. Sur la page XenMobile Management Tools qui s'ouvre, pour démarrer XenMobile Analyzer, cliquez sur **Analyze and Troubleshoot my XenMobile Environment**.



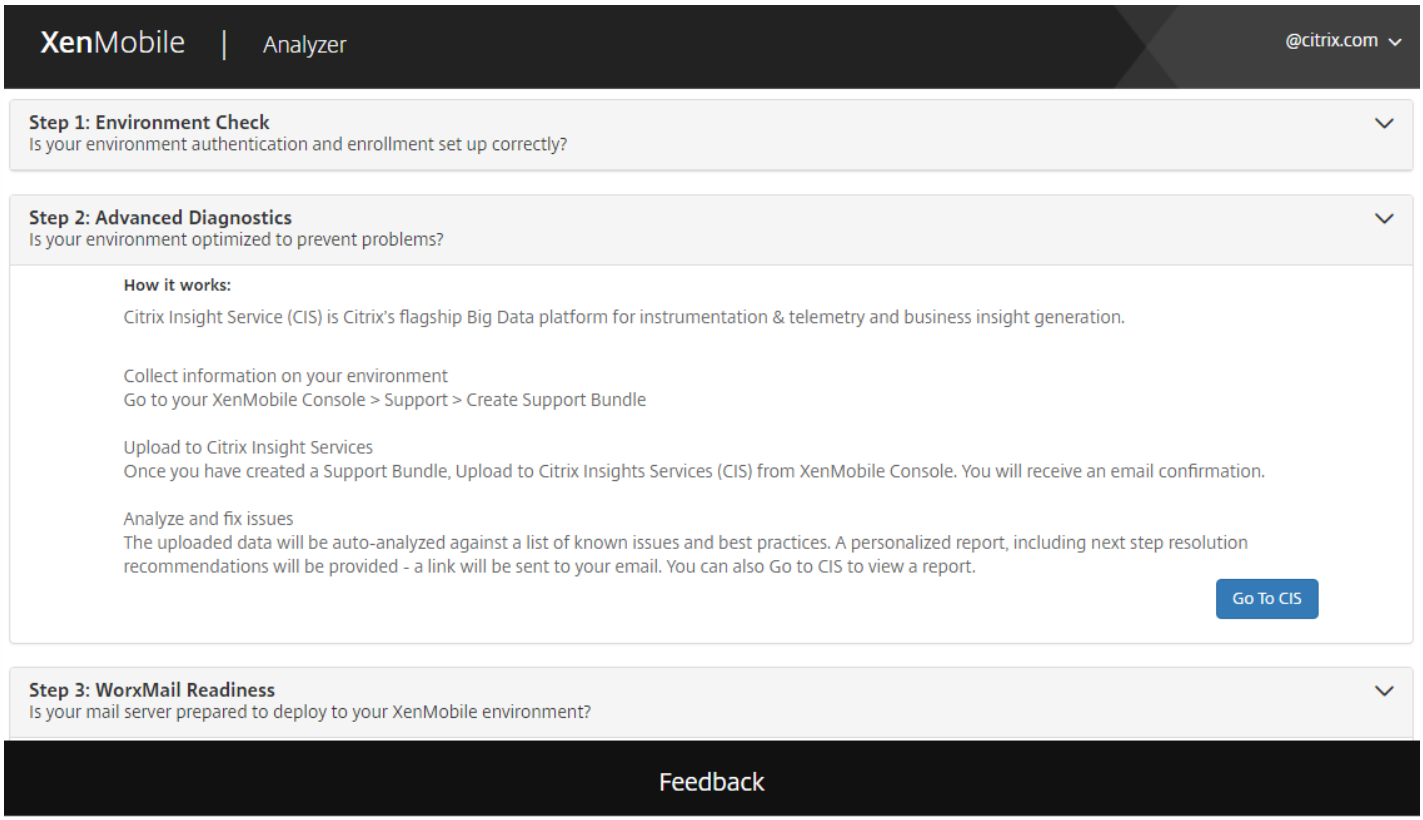
XenMobile Analyzer contient cinq étapes conçues pour vous guider à travers le processus de triage et réduire le nombre de tickets d'assistance, ce qui permet de réduire les coûts.

Les étapes sont les suivantes :

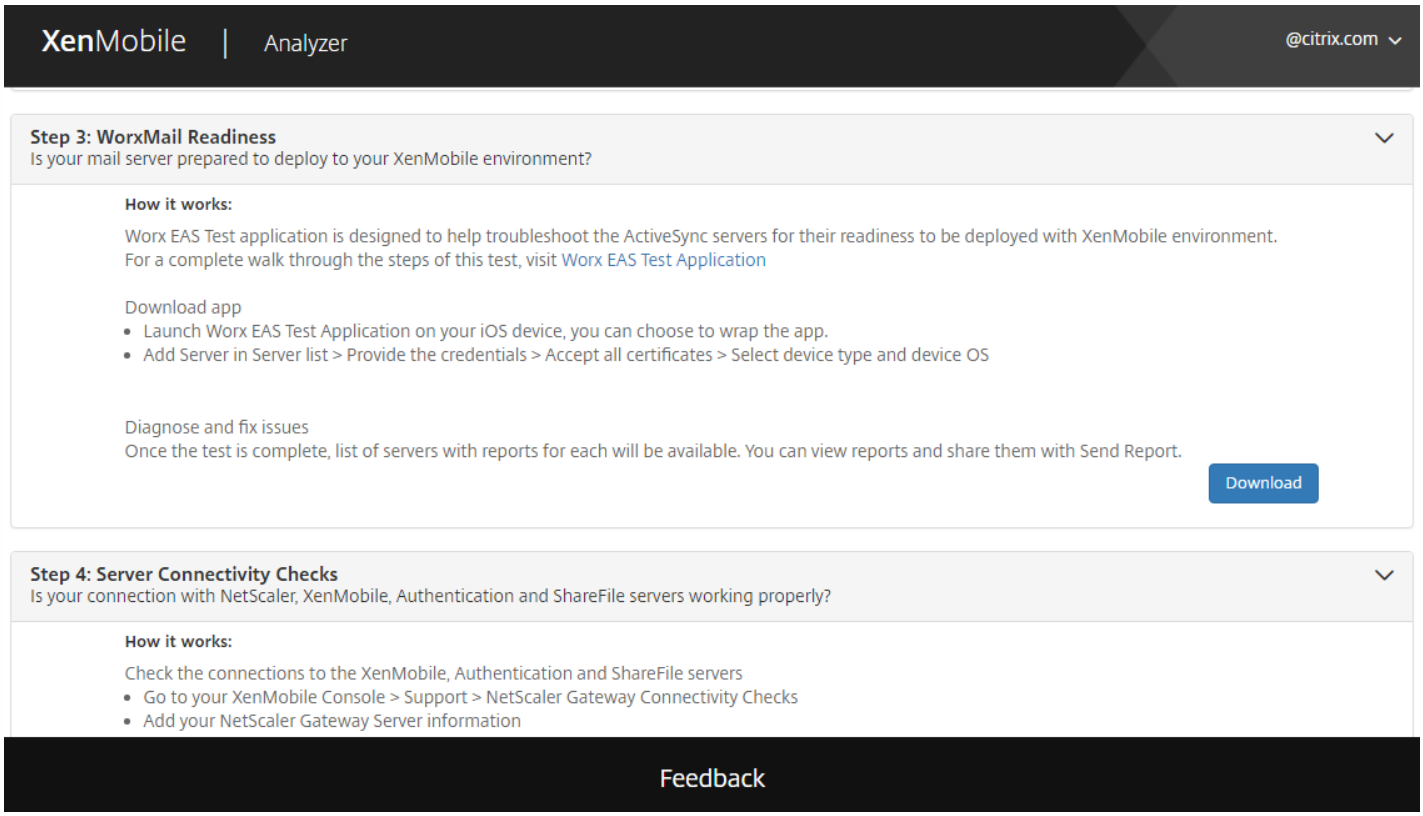
1. **Environment Check** (Vérification de l'environnement) : cette étape vous guide dans la configuration de tests destinés à détecter les problèmes d'installation. L'étape propose également des recommandations et des solutions permettant des régler les problèmes d'appareil, d'inscription d'utilisateur et d'authentification.



2. **Advanced Diagnostics** (Diagnostics avancés) : 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.

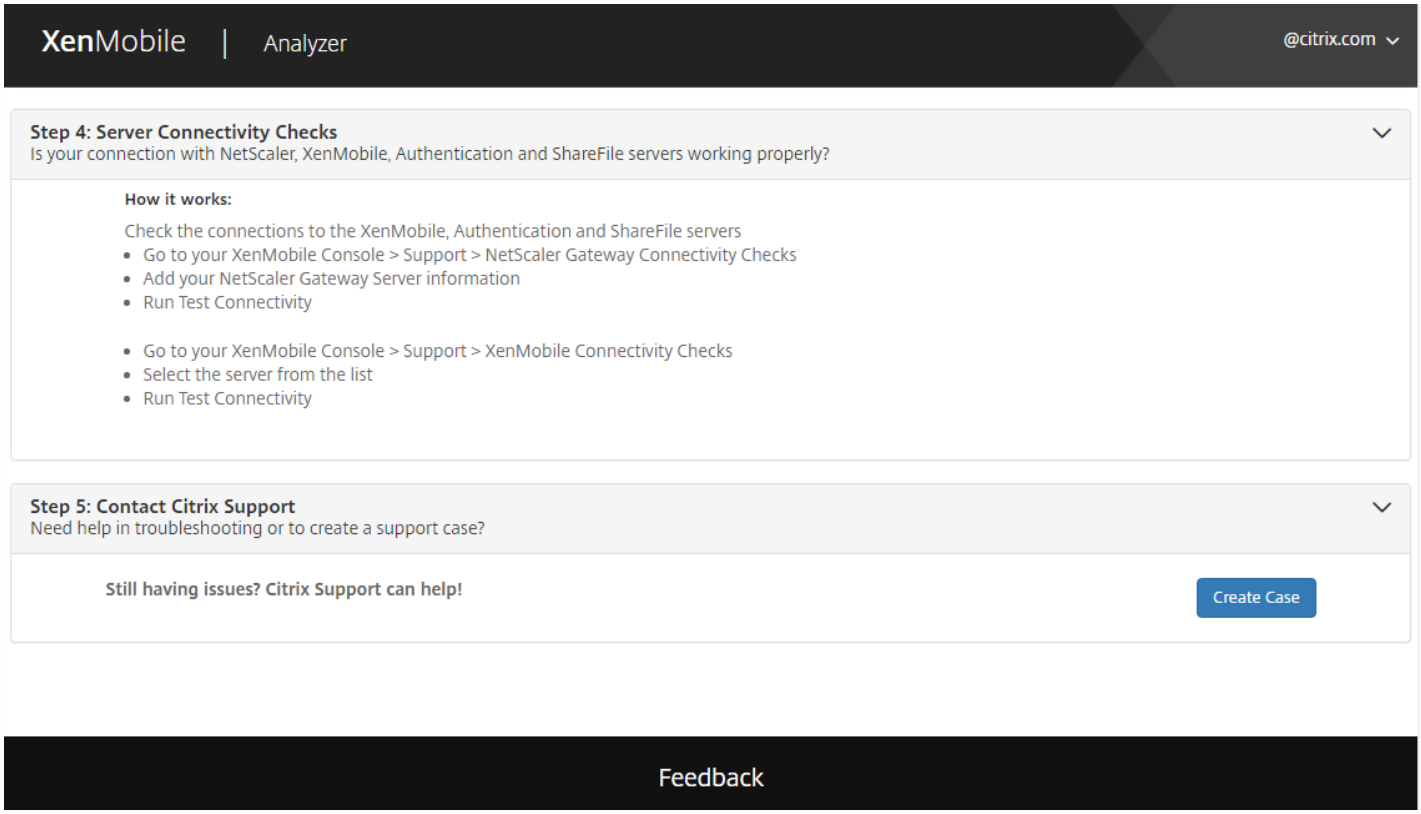


3. **WorxMail Readiness** (Disponibilité de WorxMail) : cette étape vous invite à télécharger l'application Worx Exchange ActiveSync Test, qui permet de résoudre les problèmes liés aux serveurs ActiveSync en vue de leur déploiement dans un environnement XenMobile.



4. **Server Connectivity Checks** (Vérification de la connectivité du serveur) : cette étape vous invite à tester la connectivité de vos serveurs.

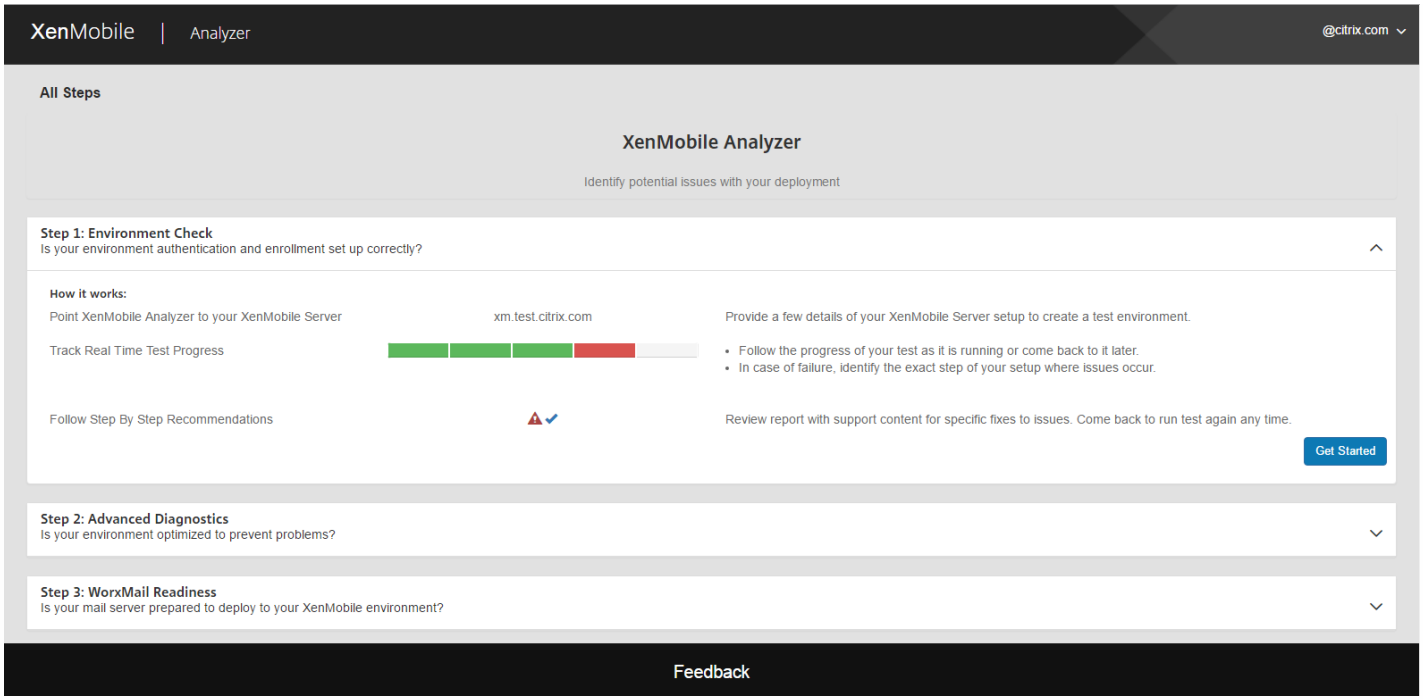
5. **Contact Citrix Support** (Contacter le support Citrix) : cette étape vous dirige vers le site à partir duquel vous pouvez créer un ticket de support technique Citrix si vous rencontrez toujours des problèmes.



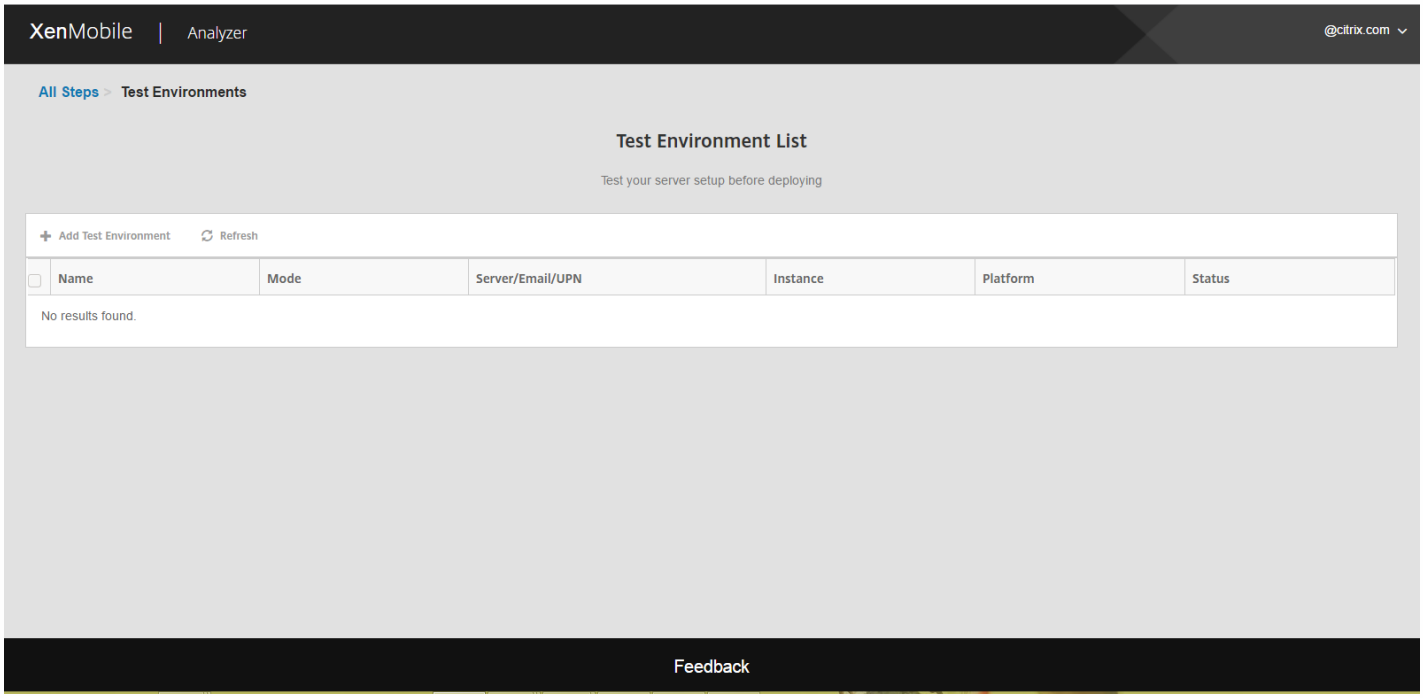
Les sections suivantes décrivent chaque étape de façon plus détaillée.

Vérification de l'environnement

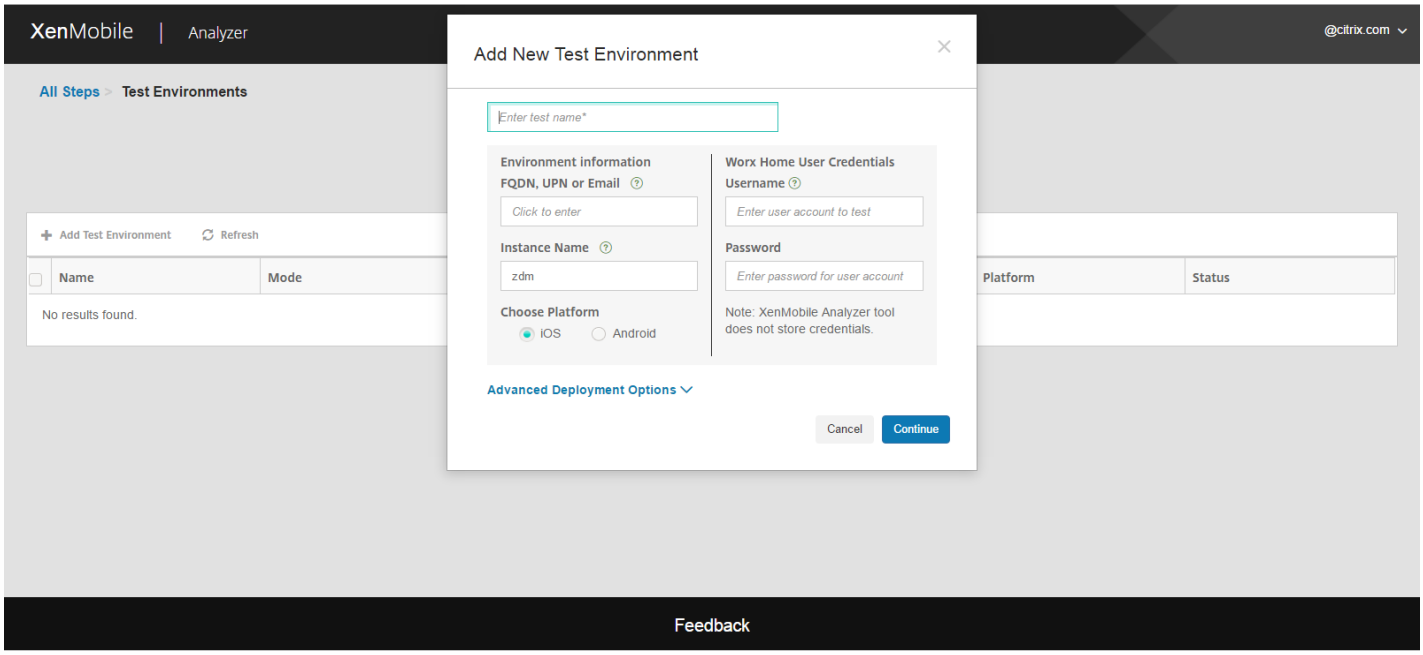
1. Ouvrez une session sur XenMobile Analyzer et cliquez sur **Step 1: Environment Checks**.
2. Cliquez sur **Get Started**.



3. Cliquez sur **Add Test Environment**.



4. Dans la nouvelle 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. Si vous disposez d'une URL d'invitation pour l'inscription, cliquez sur **Advanced Deployment Options**. Cochez la case **Do you have invitation URL** et fournissez l'URL. Si vous laissez le champ vide, l'outil détectera automatiquement le serveur XenMobile, le nom d'utilisateur et d'autres informations.

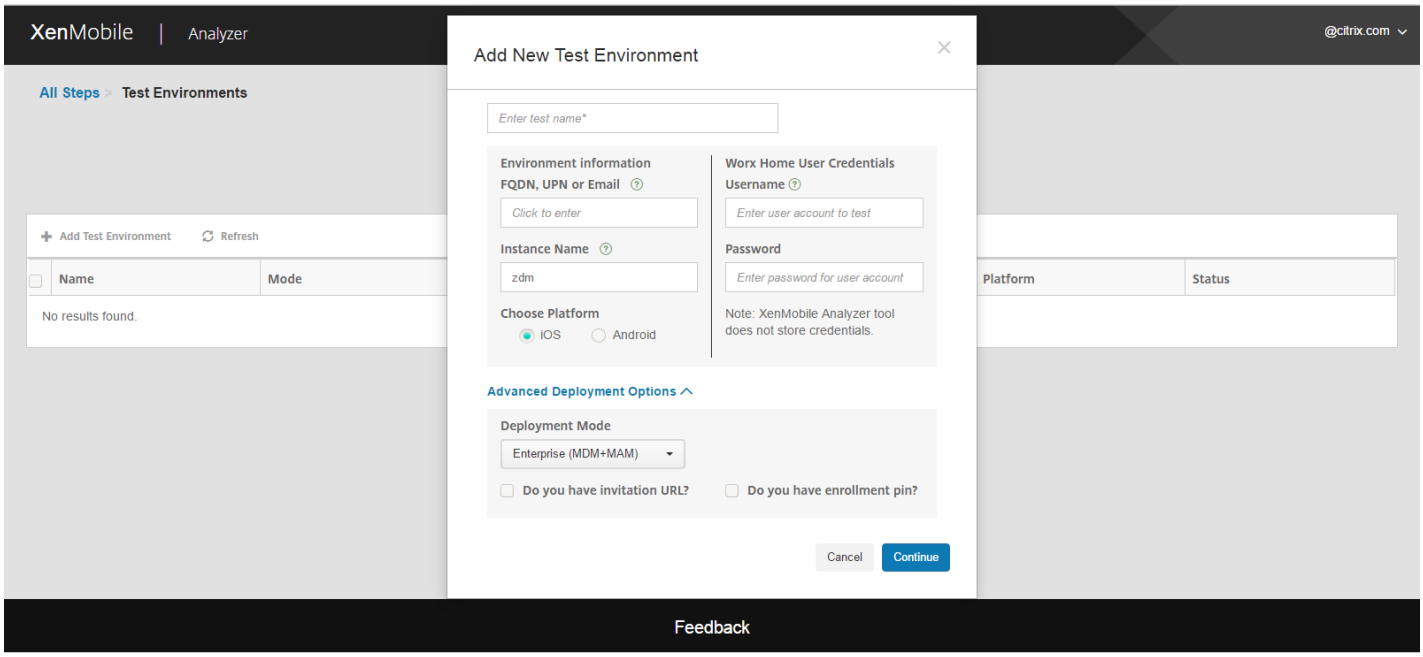
c. Si vous ne disposez pas d'une URL d'invitation, vous pouvez entrer les informations du serveur manuellement.

d. Dans la liste **Deployment Mode**, sélectionnez votre mode de déploiement XenMobile.

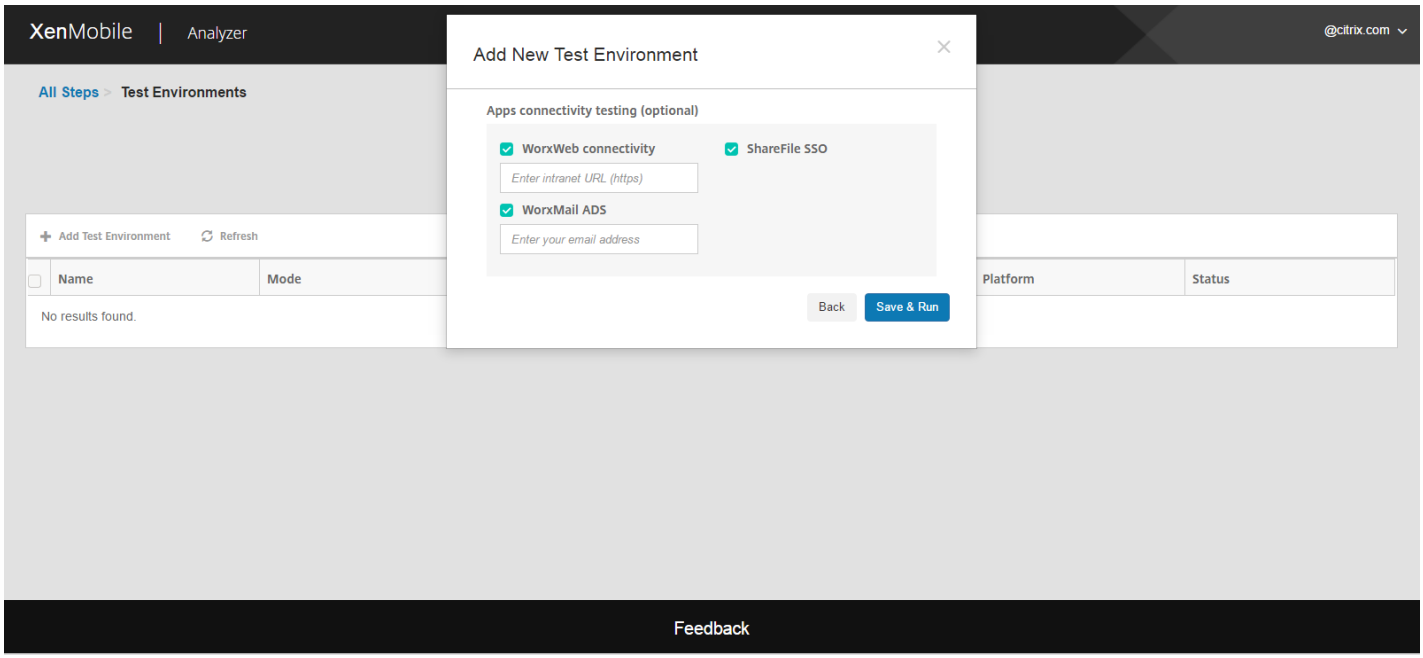
e. Dans **Instance Name**, si vous utilisez une instance personnalisée, vous pouvez fournir cette valeur.

f. Dans **Choose Platform**, sélectionnez **iOS** ou **Android** en tant que plate-forme pour le test.

g. Dans **Username** et **Password**, entrez le nom d'utilisateur et mot de passe à utiliser pour l'authentification. Si votre environnement est configuré pour l'authentification à deux facteurs, sélectionnez la case à cocher **Two Factor Authentication** et fournissez le second mot de passe.



5. Cliquez sur **Continue**.



6. Vous pouvez choisir les tests à exécuter au niveau de l'application. Vous pouvez choisir un ou plusieurs des tests suivants.

a. WorxWeb Connectivity. Fournissez une URL intranet. L'outil va tester l'accessibilité de l'URL. Il va détecter la présence de problèmes de connectivité susceptibles de se produire dans l'application WorxWeb lors de la tentative d'accès aux URL intranet.

b. WorxMail ADS. Fournissez un ID d'e-mail utilisateur. Cet ID sera utilisé pour tester la détection automatique de Microsoft Exchange Server dans votre environnement XenMobile. Il détectera s'il existe des problèmes liés à la

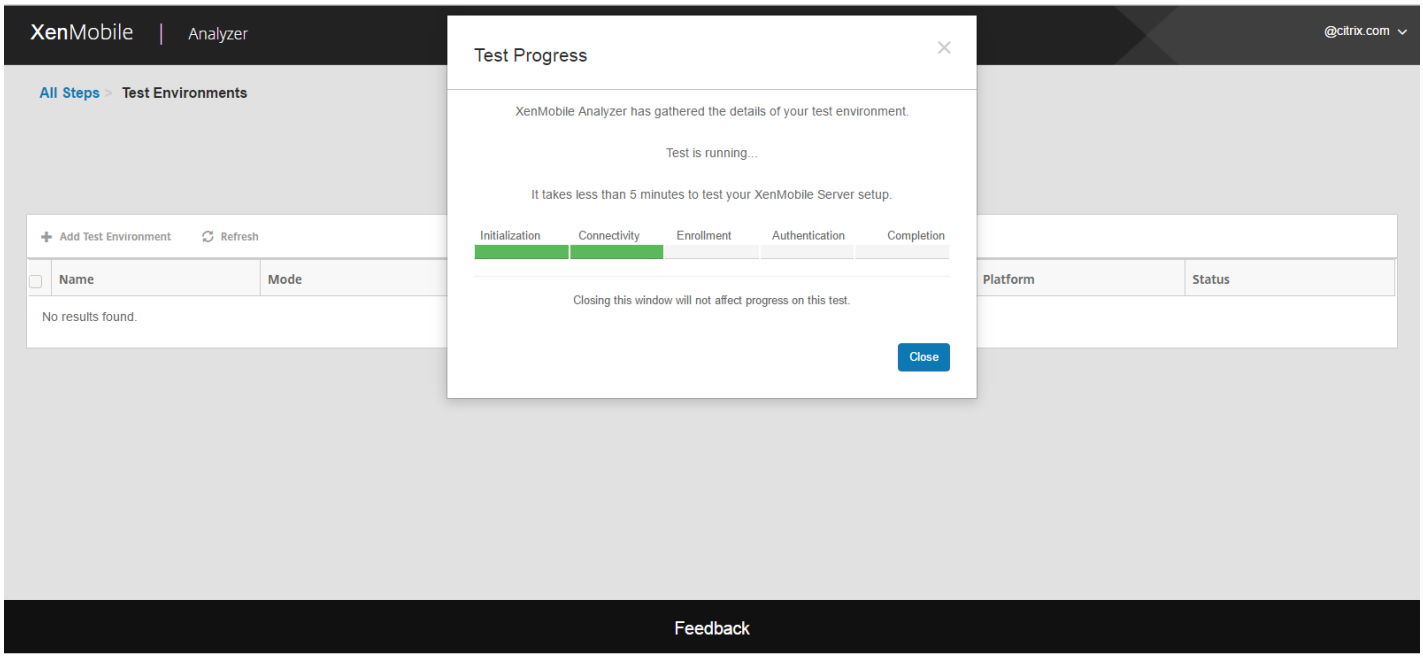
détection automatique de WorxMail.

c. ShareFile SSO. Si cette option est sélectionnée, XenMobile Analyzer testera si la résolution DNS ShareFile se déroule avec succès et si l'authentification unique à ShareFile (SSO) fonctionne avec les informations d'identification utilisateur fournies.

7. Cliquez sur **Save & Run** pour démarrer les tests.

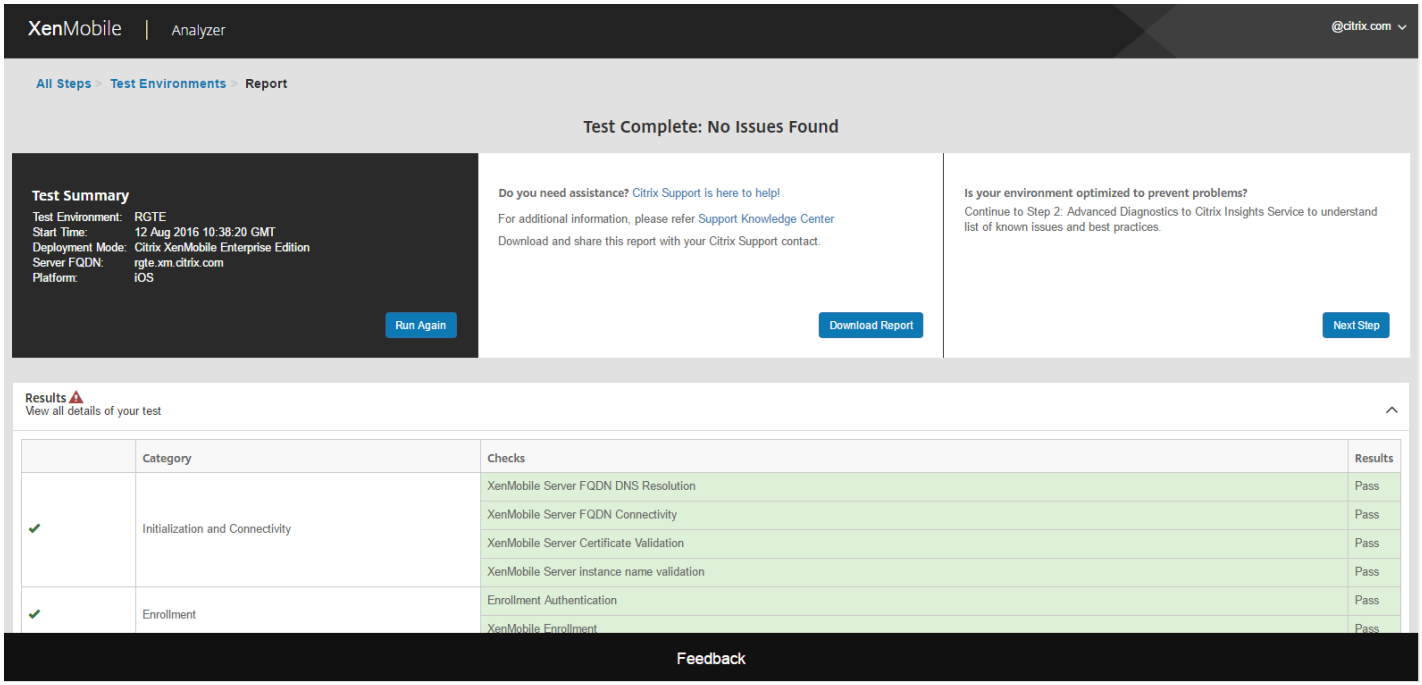
Une notification de progression s'affiche. Vous pouvez laisser la boîte de dialogue de progression ouverte ou la fermer et les tests continueront à s'exécuter.

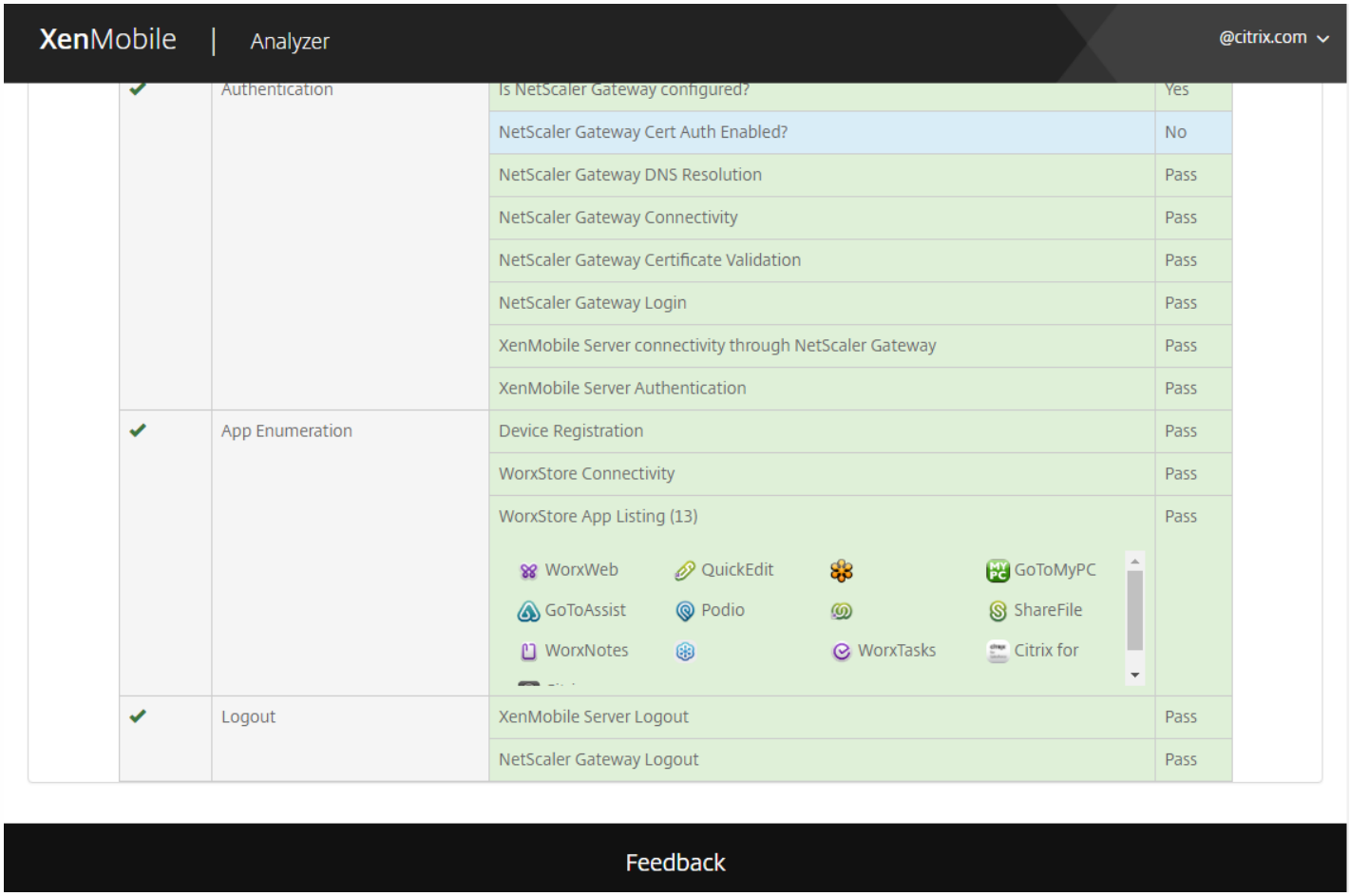
Les tests qui ont réussi s'affichent en vert. Ceux qui ont échoué s'affichent en rouge.



8. À tout moment après fermeture de la boîte de dialogue de progression, vous pouvez revenir à la page **Test Environments List**, puis cliquer sur l'icône **View Report** pour afficher les résultats du test.

La page **Results** affiche les détails du test, des recommandations ainsi que les résultats.





Si les recommandations s'accompagnent d'articles de la base de connaissances Citrix, les articles sont répertoriés sur cette page.

9. Cliquez sur l'onglet **Results** pour afficher la catégorie et les tests individuels effectués par l'outil, avec leurs résultats.

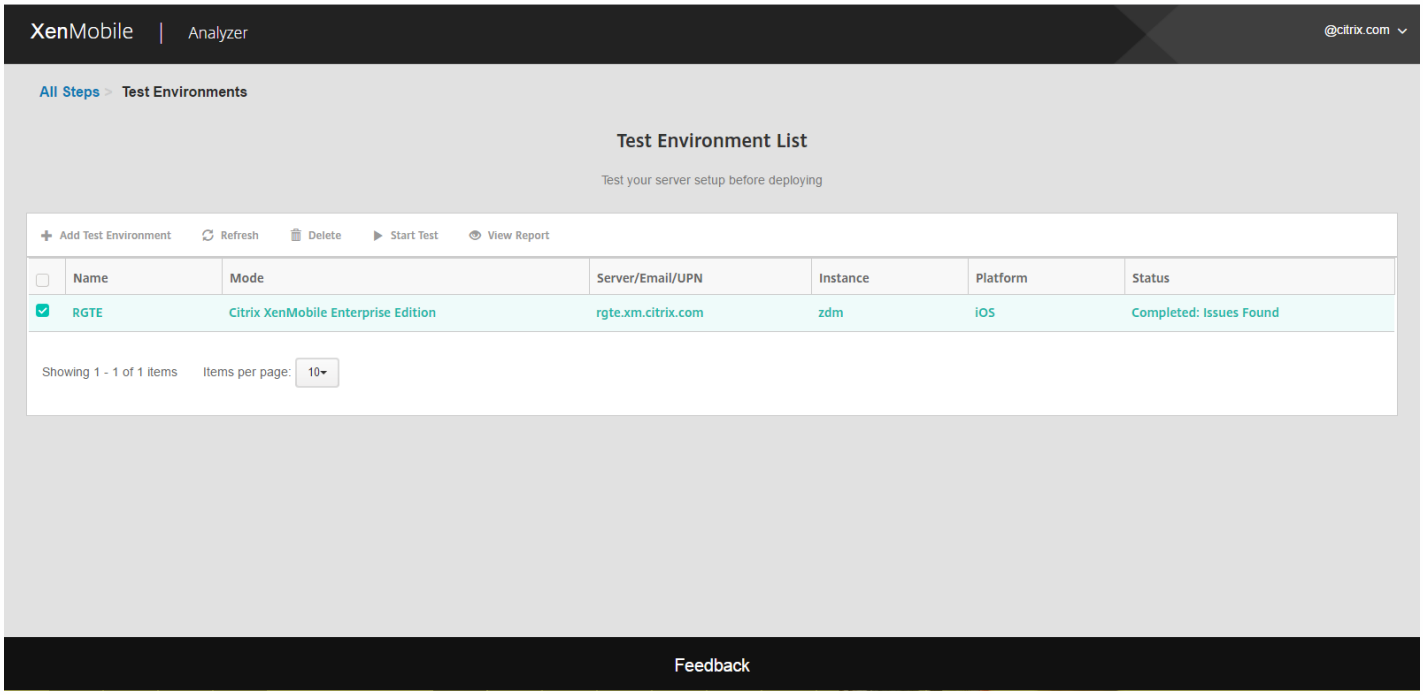
    a. Pour télécharger le rapport, cliquez sur **Download Report**.

    b. Pour revenir à la liste des environnements de test, cliquez sur **Test Environments**.

    c. Pour exécuter de nouveau le même test, cliquez sur **Run Again**.

    d. Si vous voulez réexécuter un autre test, revenez sur **Test Environments**, sélectionnez le test et cliquez sur **Start Test**.

    e. Pour accéder à l'étape suivante de XenMobile Analyzer, cliquez sur **Next Step**.



Exécution des étapes 2 à 5 de XenMobile Analyzer

Vous pouvez interagir directement avec l'étape Environment Check de XenMobile Analyzer pour effectuer des tests, alors que les étapes 2 à 5 sont purement informatives. Chacune de ces étapes fournit des informations concernant d'autres outils de support que vous pouvez utiliser pour vous assurer que votre environnement XenMobile est configuré correctement.

- **Step 2 - Advanced Diagnostics**: cette étape 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.
- **Step 3 - WorxMail Readiness:** cette étape vous invite à télécharger et exécuter l'application Worx 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.
- **Step 4 - Server Connectivity Checks:** cette étape vous fournit des instructions sur la vérification de vos connexions à

XenMobile, de l'authentification et des serveurs ShareFile.

- **Step 5 - 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 :

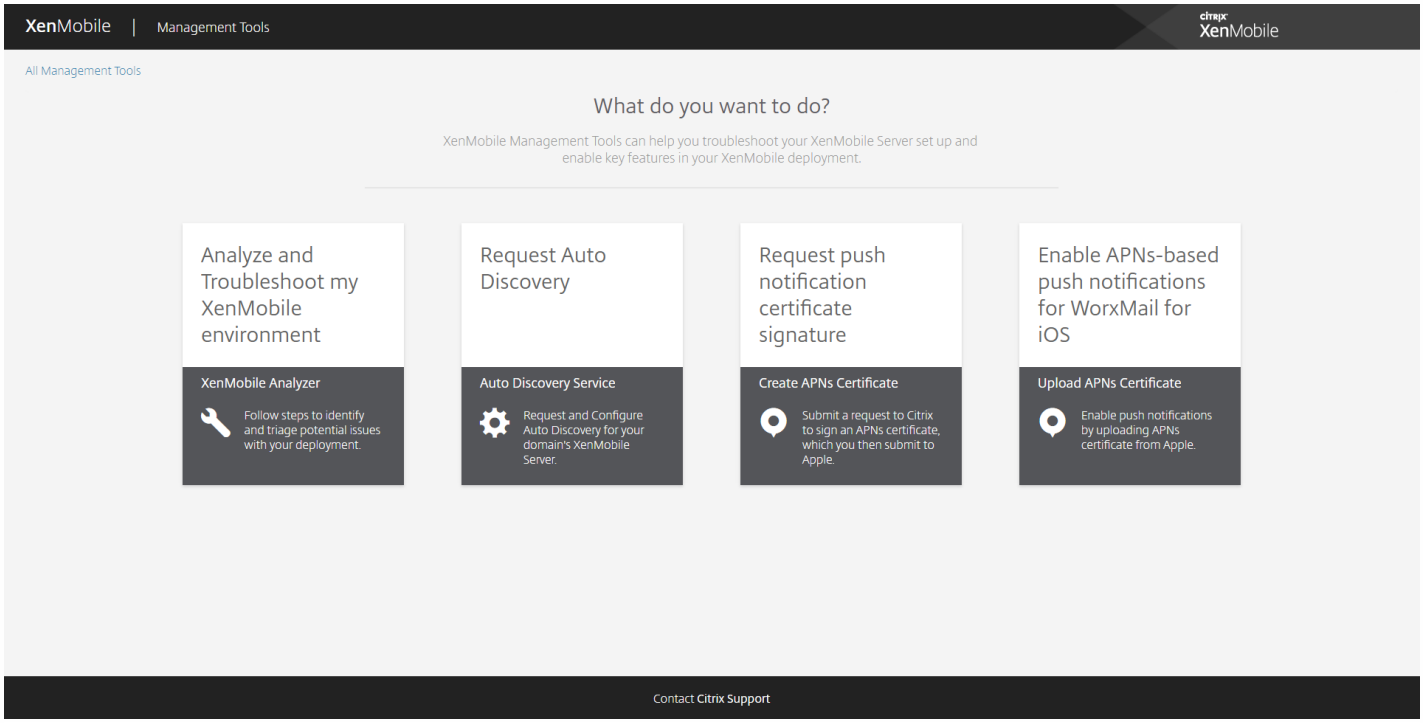
- Le nombre d'applications répertoriées peut varier en fonction du client si la stratégie de restriction de plate-forme est définie sur le serveur XenMobile.
- Lors de la vérification de la connectivité intranet de WorxWeb, la saisie d'URL multiples dans la zone de texte n'est pas prise en charge.
- La fonctionnalité d'authentification des appareils partagés de WorxHome n'est pas prise en charge.

XenMobile AutoDiscovery Service

Jul 27, 2016

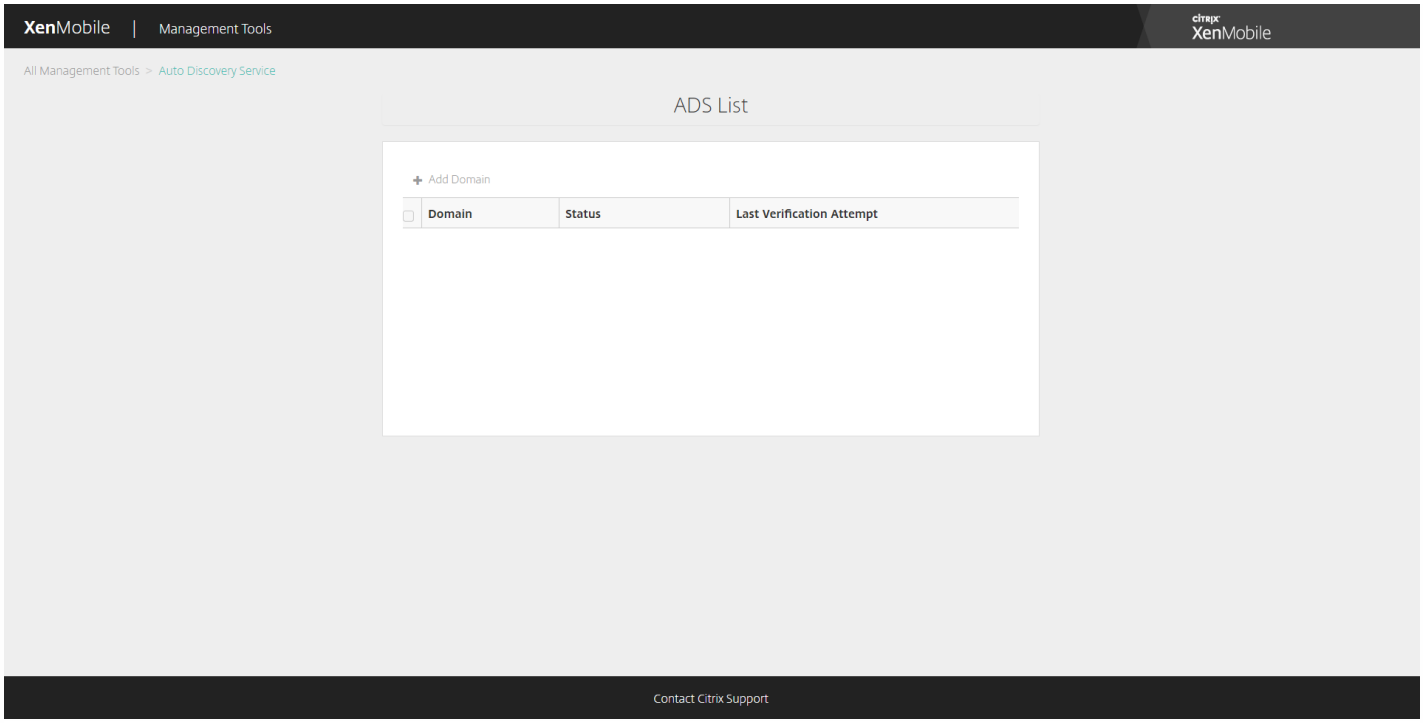
La détection automatique jour un rôle important dans la plupart des déploiements XenMobile. La découverte automatique simplifie le processus d'inscription pour les utilisateurs. Ils peuvent utiliser leurs noms d'utilisateur réseau et leurs mots de passe Active Directory pour inscrire leurs appareils, et n'ont pas besoin d'entrer ces détails sur le serveur XenMobile. Le nom d'utilisateur doit être entré au format UPN (nom d'utilisateur principal) ; par exemple, utilisateur@monentreprise.com. XenMobile AutoDiscovery Service vous permet de créer ou de modifier un enregistrement de détection automatique sans l'aide de l'assistance Citrix.

Pour accéder à XenMobile AutoDiscovery Service, accédez à https://xenmobiletools.citrix.com et cliquez sur **Request Auto Discovery**.

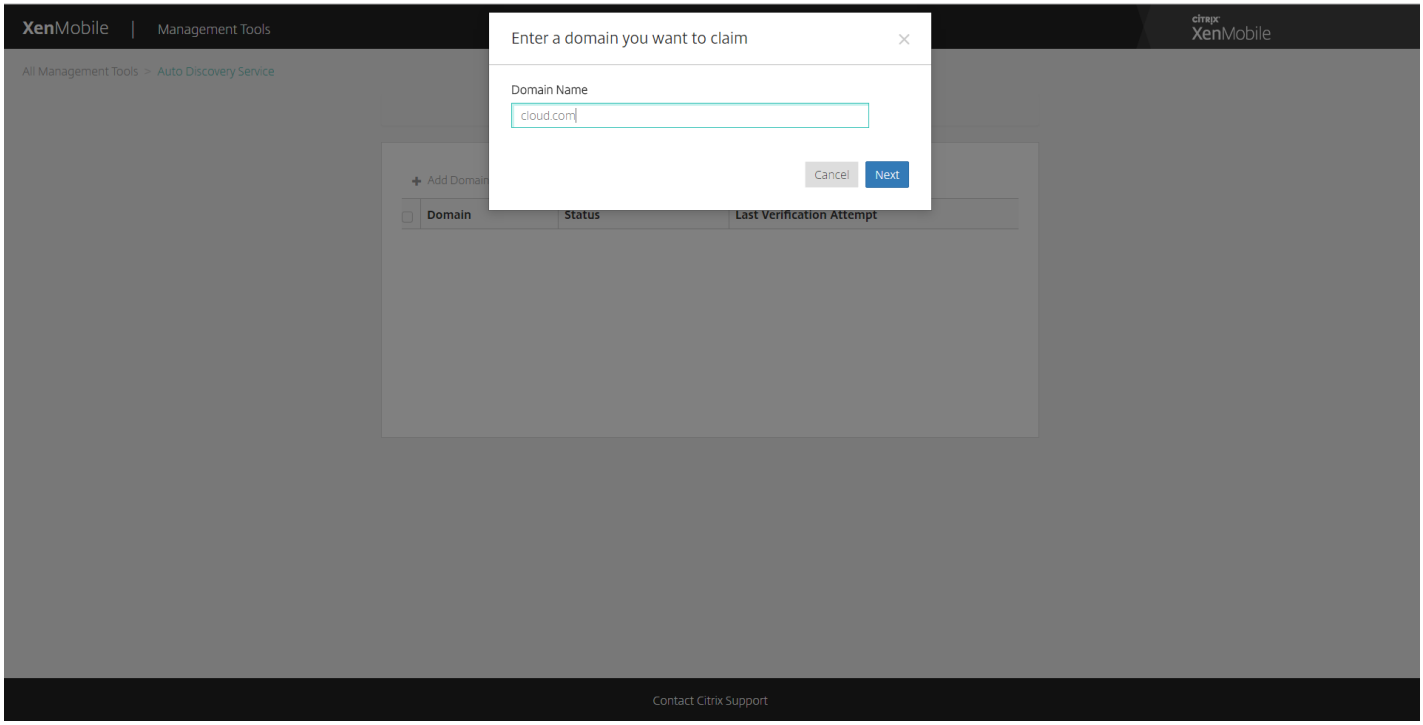


Faire une demande de détection automatique

1. Sur la page AutoDiscovery Service, vous devez d'abord revendiquer un domaine. Cliquez sur **Add Domain**.



2. Dans la boîte de dialogue qui s'affiche, entrez le nom de domaine de votre environnement XenMobile et cliquez sur **Next**.



3. L'étape suivante vous explique comment vérifier que vous êtes le propriétaire du domaine.

a. Copiez le jeton DNS fourni dans le XenMobile Tools Portal.

b. Créez un enregistrement TXT DNS dans le fichier de zone de votre domaine dans le portail Domain Hosting Provider.

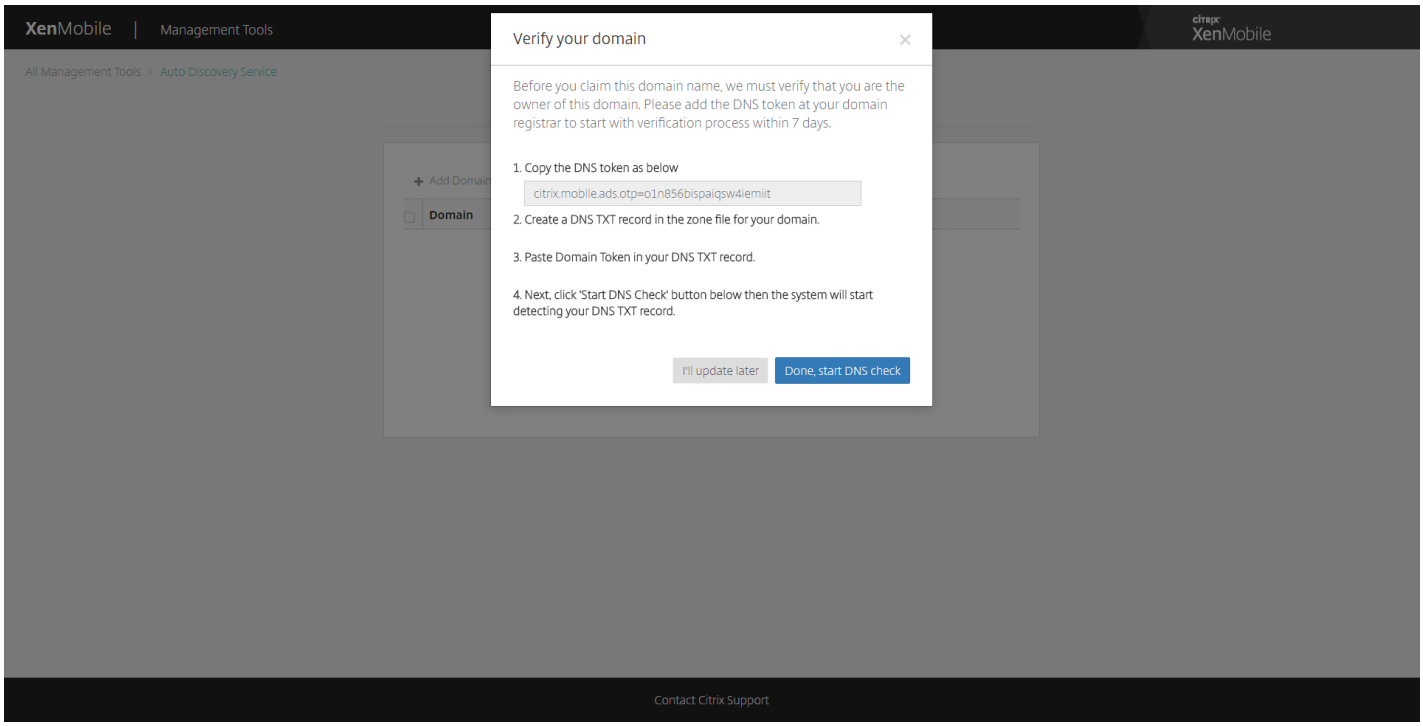
Pour créer un enregistrement TXT DNS, vous devez vous connecter au portail Domain Hosting Provider pour le domaine que vous avez ajouté à l'étape 2 ci-dessus. Dans le portail Domain Hosting, vous pouvez modifier vos enregistrements DNS et ajouter un enregistrement TXT personnalisé. Vous trouverez ci-dessous un exemple d'ajout d'une entrée TXT DNS dans un portail d'hébergement pour le domaine domaine.com.

c. Collez le jeton de domaine dans votre enregistrement TXT DNS et enregistrez votre enregistrement DNS.

d. De retour dans XenMobile Tools Portal, cliquez sur Done et démarrez la vérification du DNS.

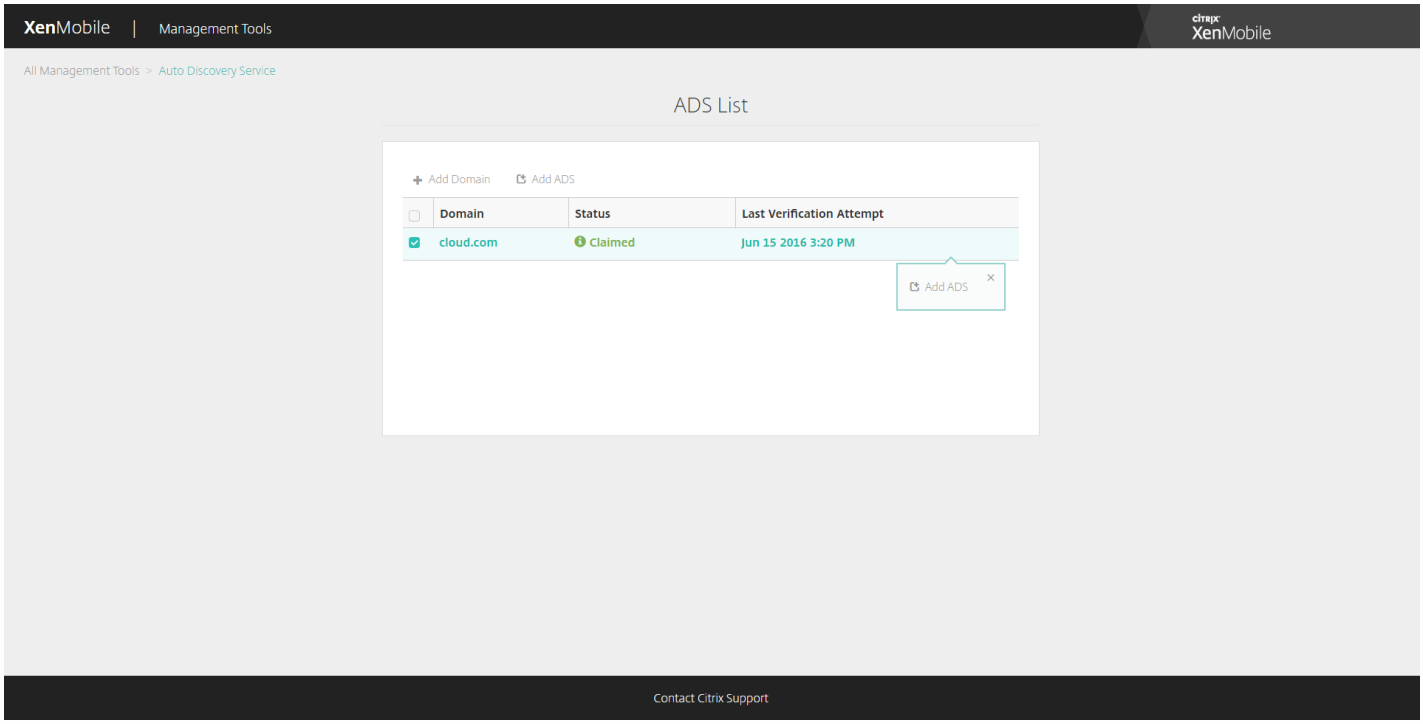
Le système détecte votre enregistrement TXT DNS. Vous pouvez éventuellement cliquer sur I'll update later et l'enregistrement est enregistré. La vérification du DNS ne démarrera pas tant que vous n'avez pas sélectionné l'enregistrement Waiting et cliqué sur DNS Check.

Cette vérification prend généralement une heure, mais le renvoi d'une réponse peut prendre jusqu'à deux jours. En outre, vous devrez peut-être quitter le portail et y retourner pour actualiser l'état.

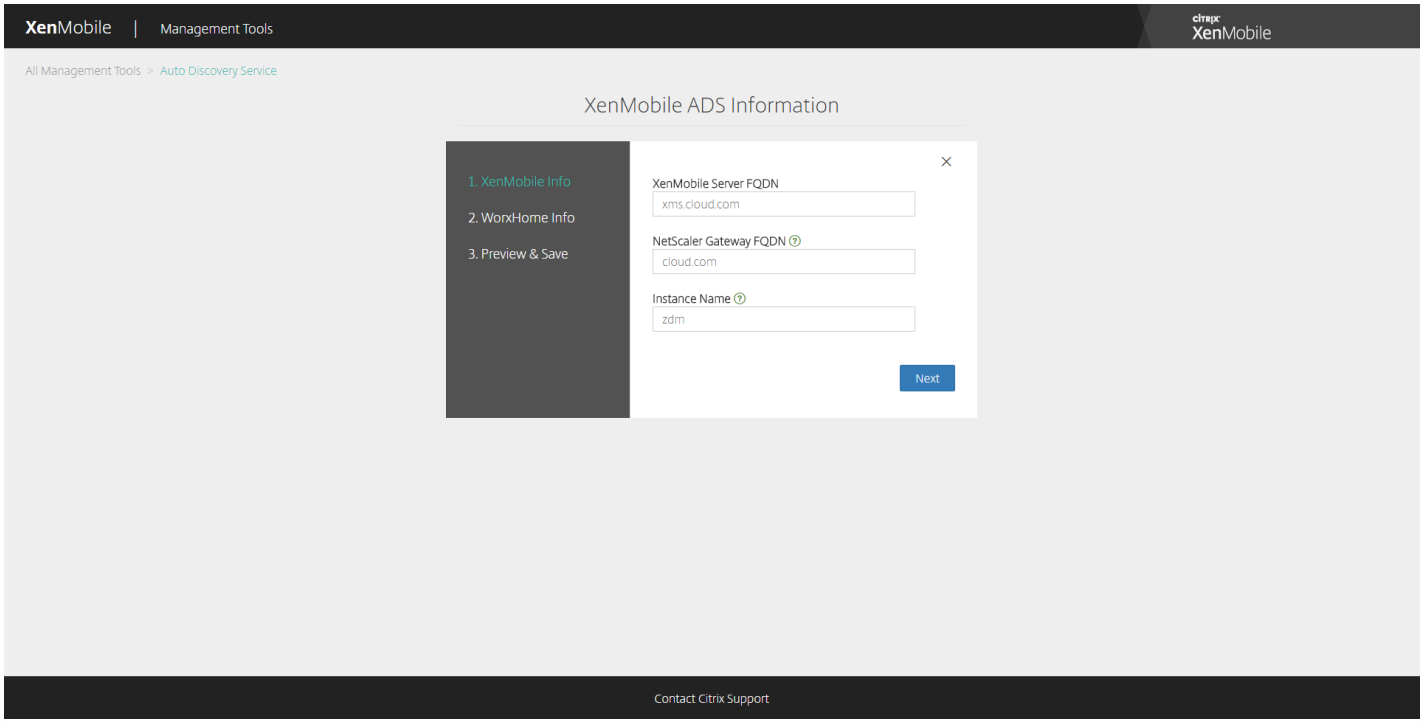


4. Après avoir revendiqué votre domaine, vous pouvez entrer les informations relatives au AutoDiscovery Service. Cliquez avec le bouton droit sur l'enregistrement de domaine pour lequel vous souhaitez faire une demande de détection automatique, puis cliquez sur **Add ADS**.

Si votre domaine dispose déjà d'un enregistrement AutoDiscovery, ouvrez un ticket auprès de l'assistance technique Citrix pour modifier les détails en fonction de vos besoins.



5. Entrez votre **XenMobile Server FQDN**, **NetScaler Gateway FQDN**, et **Instance Name** et cliquez sur **Next**. Si vous le souhaitez, ajoutez une instance par défaut de « zdm ».



6. Entrez les informations suivantes pour Worx Home et cliquez sur **Next**.

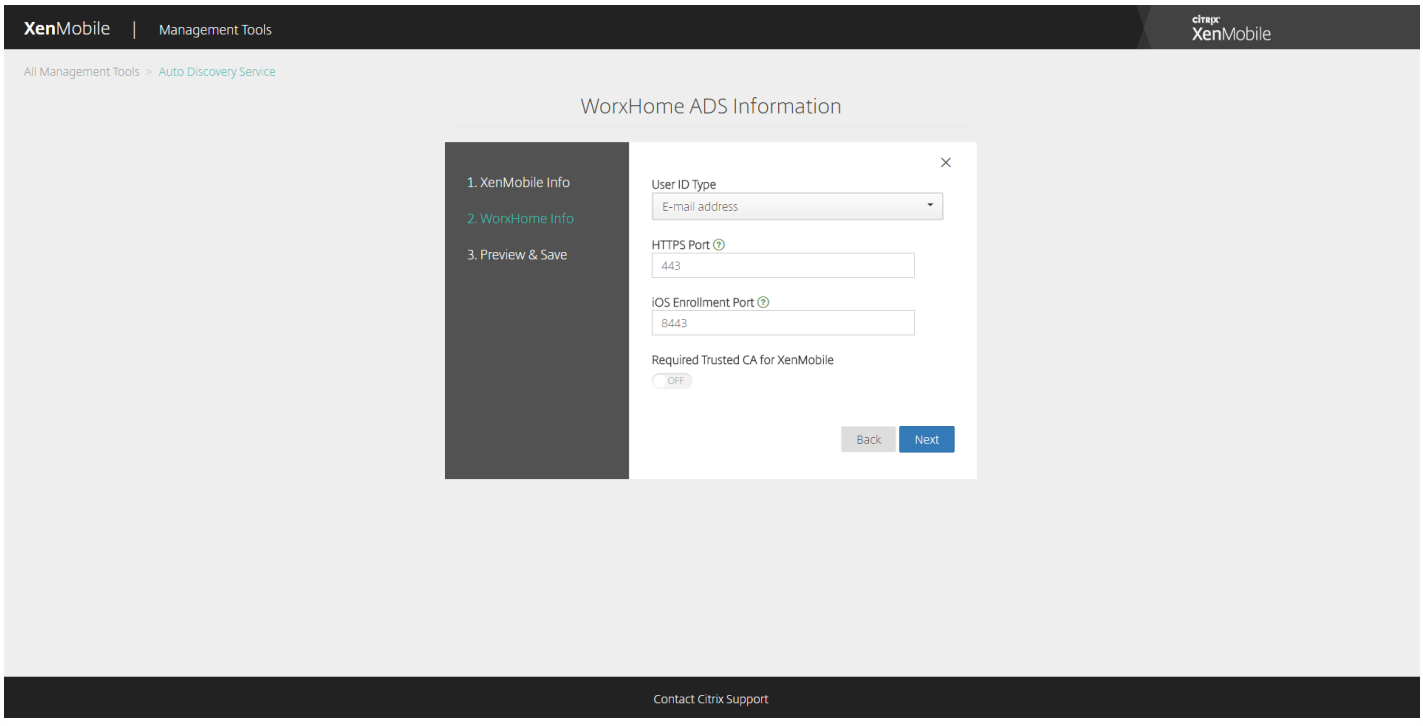
   a. **User ID Type** : sélectionnez le type d'ID avec lequel les utilisateurs se connectent, soit **l'adresse e-mail** soit le nom **UPN**.

UPN est utilisé lorsque l'UPN (nom d'utilisateur principal) de l'utilisateur est le même que son adresse e-mail. Les deux méthodes utilisent le domaine entré pour trouver l'adresse du serveur. Avec **E-mail address** , les utilisateurs seront invités à entrer leur nom d'utilisateur et mot de passe, et avec **UPN**, ils seront invités à entrer leur mot de passe.

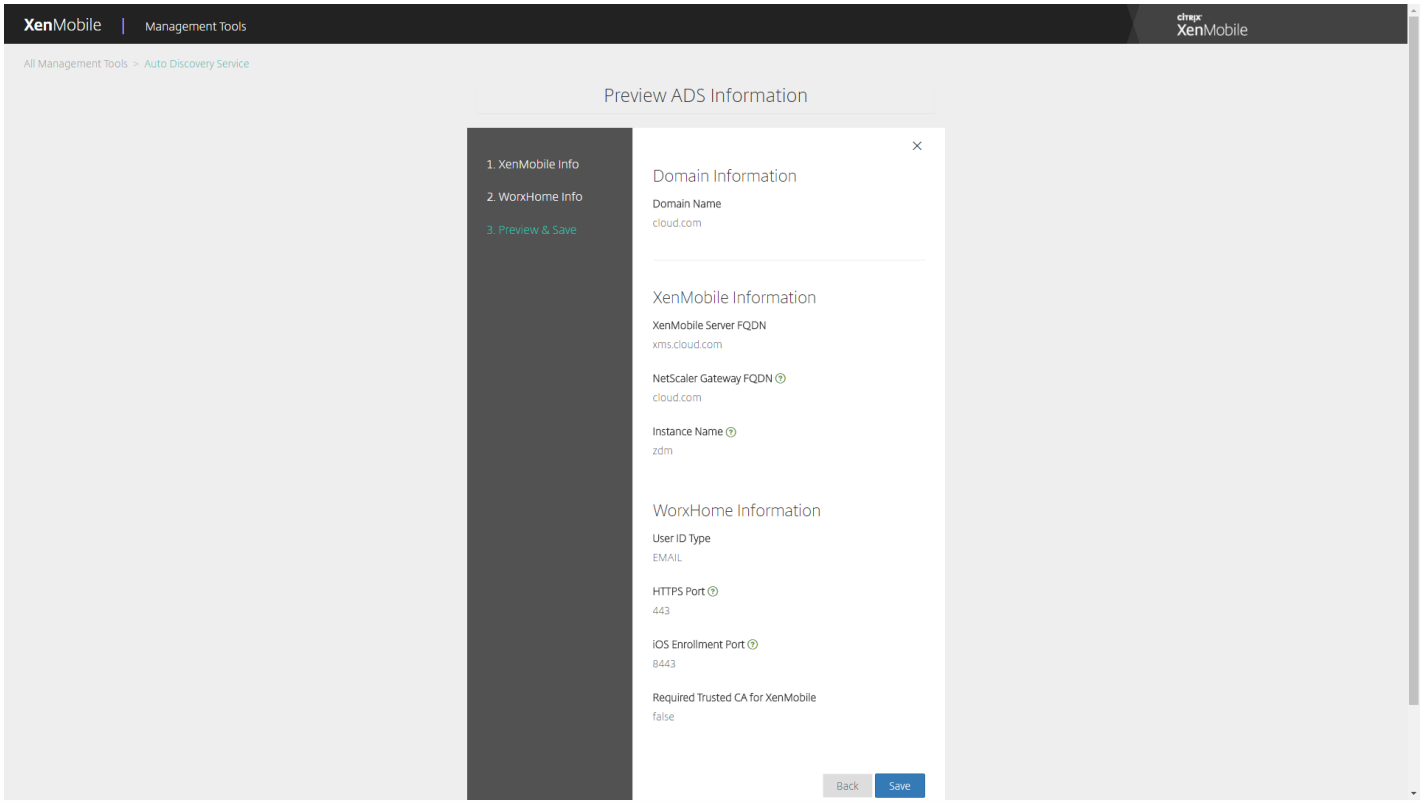
b. **HTTPS Port** : entrez le numéro de port utilisé pour accéder à Worx Home sur HTTPS. En règle générale, il s'agit du port 443.

c. **iOS Enrollment Port** : entrez le numéro de port utilisé pour accéder à Worx Home pour l'inscription iOS. En règle générale, il s'agit du port 8443.

d. **Required Trusted CA for XenMobile** : indiquez si un certificat approuvé est nécessaire pour accéder à XenMobile. Cette option peut être **OFF** ou **ON**. La possibilité de charger un certificat pour cette fonctionnalité n'est pas actuellement disponible. Si vous souhaitez utiliser cette fonctionnalité, vous devez appeler le support Citrix pour qu'ils configurent la détection automatique pour vous. Pour en savoir plus sur le certificate pinning, consultez la section sur le certificate pinning dans la rubrique Worx Home. Pour en savoir plus sur les ports requis pour assurer le fonctionnement du certificate pinning, consultez l'article Exigences requises par XenMobile en matière de port pour la connectivité ADS.



7. Une page de résumé affiche les informations que vous avez entrées dans les étapes précédentes. Vérifiez que les données sont correctes et cliquez sur **Save**.



API REST XenMobile : références

Jul 27, 2016

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 API REST XenMobile : références. Cet article ne couvre pas l'ensemble des API.

Autorisations requises pour accéder à l'API REST

Vous devez utiliser l'une des autorisations suivantes pour accéder à l'API REST :

- Autorisation d'accès à l'API publique définie dans le cadre de la configuration d'accès basé sur un rôle (pour plus d'informations sur la configuration d'accès basé sur un rôle, consultez 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.

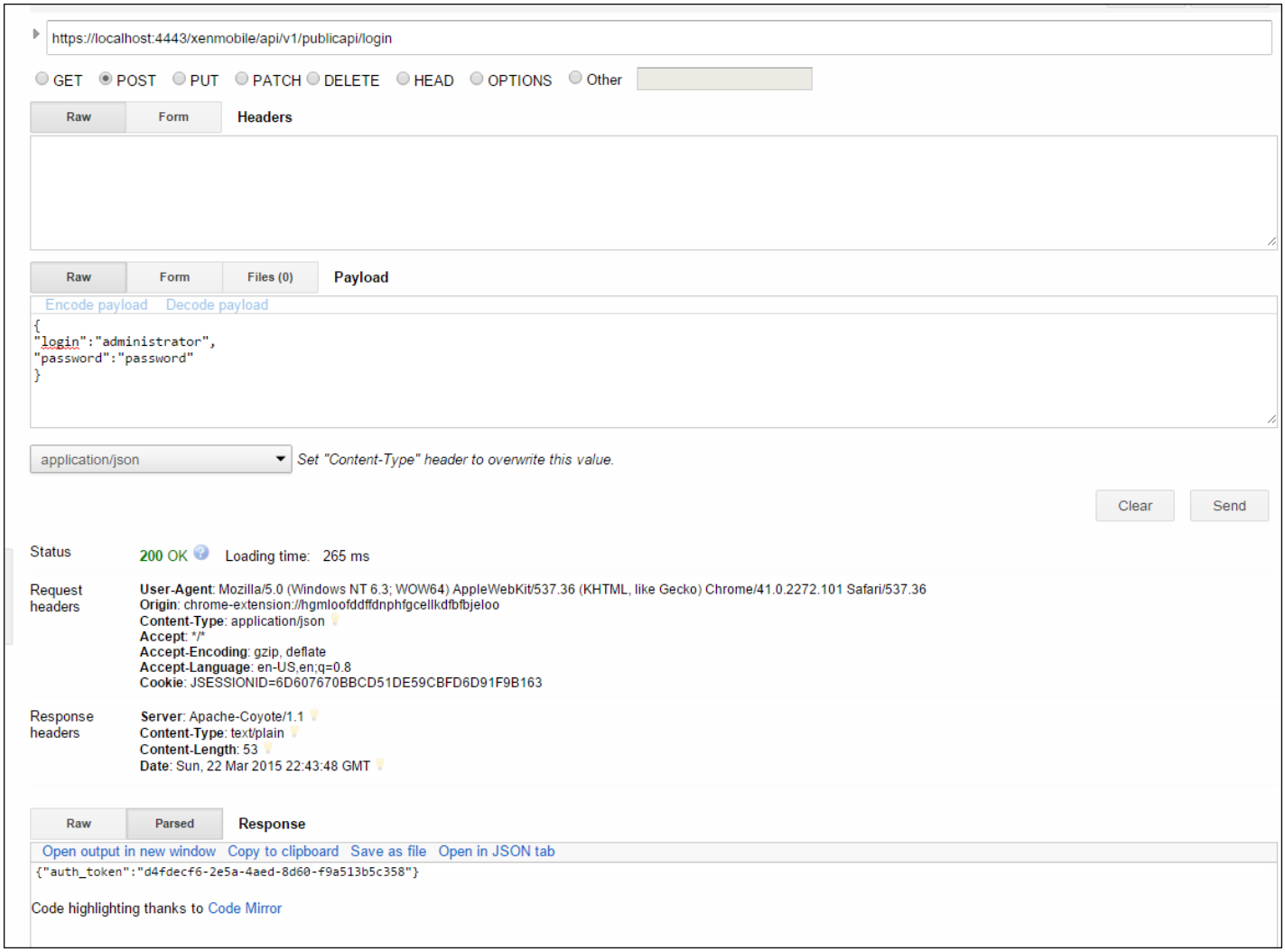
Connexion

URL : https://:/xenmobile/api/v1/authentication/login

Requête : { "login":"administrator", "password":"password" }

Type de méthode : POST

Content-type : application/json



Obtenir les groupes de mise à disposition par filtre

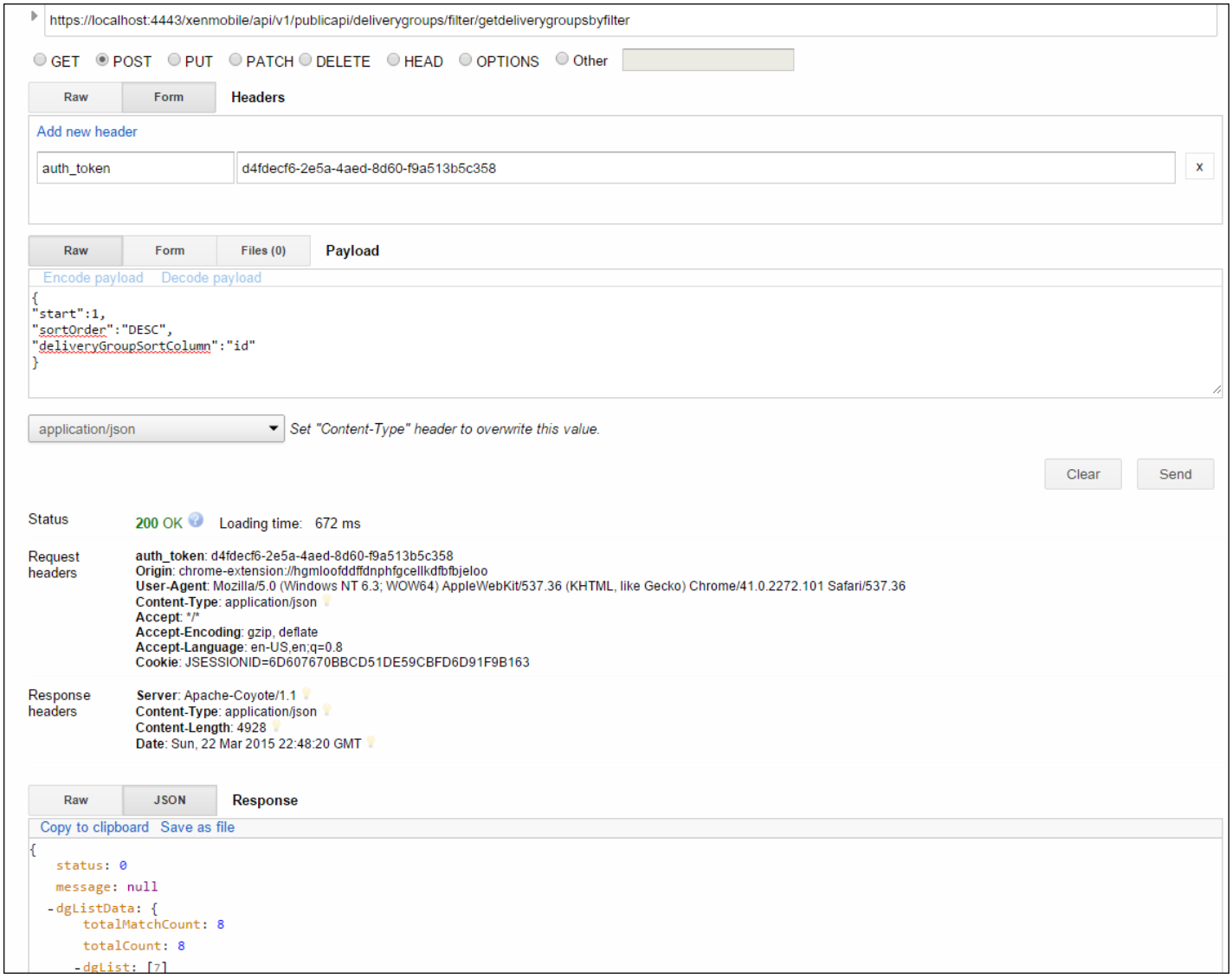
URL : /xenmobile/api/v1/deliverygroups/filter

Requête COPIER

```
{

    "start": 1,

    "sortOrder": "DESC",

    "deliveryGroupSortColumn":"id",

    "search":"add"

}
```

Type de méthode : POST

Content-type : application/json



Définition des API REST

Les sections suivantes abordent certaines des API disponibles dans le PDF. Reportez-vous au PDF pour consulter l'ensemble des API.

Rappel : dans les exemples suivants, modifiez le nom de l'hôte et le numéro de port afin qu'ils correspondent à votre environnement.

Pour ouvrir une session sur l'API publique

Accepte les informations d'identification de l'utilisateur et utilise l'AuthenticationManager existant pour authentifier l'utilisateur. La première fois que AuthenticationManager authentifie un utilisateur, il génère un jeton d'authentification qui est placé dans l'en-tête de la requête.

URL : https://:4443/xenmobile/api/v1/authentication/login

Type de requête : POST

Paramètres de requête COPIER

```
{ "login":"administrator", "password":"password" }
```

Exemple de réponse COPIER

```
{

    "auth-token":"q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"

}
```

Pour ouvrir une session sur l'API publique via la console Citrix Web Console

Accepte les informations d'identification de l'utilisateur et utilise l'AuthenticationManager existant pour authentifier l'utilisateur. La première fois que AuthenticationManager authentifie un utilisateur, il génère un jeton d'authentification qui est placé dans l'en-tête de la requête.

URL : https://:/xenmobile/api/v1/authentication/cwclogin

Type de requête : POST

En-tête de requête : Authorization – CWSAuth service=

Paramètres de requête COPIER

```
{“context”:”customer or cloud”, “customerId”:”customer ID”}
```

Exemple de réponse COPIER

```
{

    "auth-token":"authentication token"

}
```

Pour se déconnecter de l'API publique

Supprime le jeton d'authentification émis lorsque l'utilisateur se connecte et déconnecte l'utilisateur actuel. Nécessite le nom d'utilisateur et le jeton d'authentification.

URL : https://:/xenmobile/api/v1/authentication/logout

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Paramètres de requête COPIER

```
{“login”:”administrator”}
```

Exemple de réponse COPIER

```
{"Status":"user administrator logged out successfully."}
```

Pour gérer les certificats

Les opérations de gestion des certificats vous permettent d'afficher, de supprimer, d'importer et d'ajouter des certificats via l'API publique.

Obtenir tous les certificats

Retourne tous les certificats dans la base de données.

URL : https://:/xenmobile/api/v1/certificates

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Paramètres de requête : None

Exemple de réponse COPIER


```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": null,
    "certificate": [
        {
            "name": "ent-root-ca",
            "description": "test description server 1",
            "validFrom": "2012-02-22",
            "validTo": "2017-02-21",
            "type": "chain",
            "isActive": false,
            "privateKey": "false",
            "ca": null,
            "id": 4656,
            "certDetails": {
```



```
"signatureAlgo": "SHA1WithRSAEncryption",

"version": null,

"serialNum": "348237881800118418457268346483687164l3",

"issuerName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,

    "locality": null,

    "state": null,

    "country": null,

    "description": null

},

"subjectName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,
```



```
                    "locality": null,

                    "state": null,

                    "country": null,

                    "description": null

                }

            }

        }

    ],

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```


Supprimer les certificats

Supprime les certificats spécifiés. Requiert l'ID du certificat pour chaque certificat à supprimer.

URL : https://:/xenmobile/api/v1/publicapi/certificates

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Paramètres de requête COPIER

```
{“certificateIds”:[“<certificate_id_1>”,”<certificate_id_2>”, ..., "<certificate_id_n>"]}
```

Importer le certificat en tant que certificat SAML

Importe le certificat spécifié en tant que certificat SAML.

URL : https://:/xenmobile/api/v1/certificates/import/certificate/saml

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'saml',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {
```

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

    }
```

Importer le certificat en tant que certificat de serveur

Importe le certificat spécifié en tant que certificat de serveur.

URL : https://:/xenmobile/api/v1/certificates/import/certificate/server

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'none',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {
```

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

    }
```

Importer le certificat en tant que certificat d'écoute

Importe le certificat spécifié en tant que certificat d'écoute SSL.

URL : https://:/xenmobile/api/v1/certificates/import/certificate/listener

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'listener',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,
```

```
    "apnsCheck": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```

Créer un certificat

Crée un certificat auto-signé ou une demande de signature de certificat (CSR) qui requiert une signature de l'autorité de certification.

URL : https://:/xenmobile/api/v1/certificates/csr

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Application/form_url_encoded

Paramètres de requête COPIER

```
{
    "isSelfSign":true,
    "csrRequest":{
    "commonName":"your certificate name",
    "description":"certificate description",
    "org":"organization",
    "orgUnit":"organization unit",
    "locality":"location",
    "state":"CA",
    "country":"US",
    "isSelfSign":true
    },
"validDays":"60",
"keyLength":"1024",
"useAs":"none"
}
```

Exemple de réponse COPIER

```
{
    status: 0
    message: "Success"
    csrRequest: ""
    apnsCheck: null
    certificate: null
    apnsCheckObj:
    {
    topicNameMismatch: false
    certExpired: false
    certNotYetValid: false
    malformed: false
    }
}
```

Exporter un certificat

Télécharge le certificat spécifié. Le tableau suivant dresse la liste des paramètres pour cette opération.

Paramètre	Requis	Description

id	Oui	ID du certificat numérique
mot de passe		Mot de passe associé au certificat exporté.
exportPrivateKey		Indicateur qui spécifie si la clé privée doit être exportée.

URL : https://:/xenmobile/api/v1/certificates/export

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{
    "id": "300",
    "password": "1111",
    "exportPrivateKey": true
}
```

Exemple de réponse : affiche la chaîne de certificat suite à une requête fructueuse.

Pour gérer les keystores

Vous pouvez importer des keystores par le biais de l'API publique

Importer un keystore serveur

Importe un keystore serveur.

URL : https://:/xenmobile/api/v1/certificates/import/keystore/server

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
```

```
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Importer un keystore SAML

Importe un keystore SAML.

URL : https://:/xenmobile/api/v1/certificates/import/keystore/saml

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
}
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Exemple de réponse COPIER

```
{
    "status": 0,
```

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Importer un keystore APNS

Importe un keystore APNS.

URL : https://:/xenmobile/api/v1/certificates/import/keystore/apns

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':apns,
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

Exemple de réponse COPIER

```
{
    "status": 0,
```

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
            "topicNameMismatch": false,
            "certExpired": false,
            "certNotYetValid": false,
            "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Importer un keystore d'écoute SSL

Importe un keystore d'écoute SSL.

URL : https://:/xenmobile/api/v1/certificates/import/keystore/listener

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':"listener",
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

Exemple de réponse COPIER

```
{
```

```
    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

"certificate": null,

"apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```


Pour gérer les licences

Vous permet de gérer les licences par le biais de l'API publique.

Obtenir les informations de licences

Affiche des informations sur les licences.

URL : https://:/xenmobile/api/v1/licenses

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{
    status: 0
    message: "Success"
    cpLicenseServer: {
        serverAddress: "192.0.2.20"
        localPort: 0
        remotePort: 27000
        serverType: "remote"
        licenseType: "none"
        isServerConfigured: true
        gracePeriodLeft: 0
        isRestartLpeNeeded: null
        isScheduleNotificationNeeded: null
            licenseList: []
```

```
{
    sadate: "2015.1210"
    notice: "Example Systems Inc."
    vendorString: ";LT=Retail;GP=720;UDM=U;LP=90;CL=STD,ADV,ENT;SA=1;ODP=0"
    licensesInUse: 0
    licensesAvailable: 102
    overdraftLicenseCount: 2
    p_E_M: "CXM_ENTU_UD"
    serialNumber: "cxmretailent1000user"
    licenseType: "Retail"
    expirationDate: "01-DEC-2015"
}
licenseNotification:
{
    id: 1
    notificationEnabled: false
    notifyFrequency: 7
    notifyNumberDaysBeforeExpire: 60
    recepientList: ""
```

```
            emailContent: "License expiry notice"

        }

    }

}
```

Enregistrer les informations de licences

Enregistre toutes les informations sur les licences.

URL : https://:/xenmobile/api/v1/licenses

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "serverAddress": "192.0.2.20",

    "localPort": 0,

    "remotePort": 27000,

    "serverType": "remote",

    "licenseType": "none",

    "isServerConfigured": true,

    "gracePeriodLeft": 0,

    "isRestartLpeNeeded": true,
```

```
    "isScheduleNotificationNeeded": true,
    "licenseList": [],
    "licenseNotification": {
        "id": 1,
        "notificationEnabled": true,
        "notifyFrequency": 20,
        "notifyNumberDaysBeforeExpire": 60,
        "recepientList": "justa.name123@example.com",
        "emailContent": "Licenseexpirynotice"
    }
}
```


Exemple de réponse COPIER


```
{
    "status": 0,
    "message": "Success"
}
```


Charger le fichier de licences

Charge le fichier de licences spécifié.

URL : https://:/xenmobile/api/v1/licenses/upload

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête : uploadFile =

Exemple de réponse COPIER

```
{

   "status": 0,

   "message": "Success"

}
```

Activer une licence

Active la licence spécifiée.

URL : https://:/xenmobile/api/v1/licenses/activate/{type de licence}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête : ajoutez le type de licence pour activer l'URL de la licence.

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success"

    "cpLicenseServer": null

}
```

Supprimer toutes les licences

Supprime toutes les licences.

URL : https://:/xenmobile/api/v1/licenses/remove

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "isConnected": null

}
```

Tester le serveur de licences

Vérifie la connectivité sur le serveur de licences.

URL : https://:/xenmobile/api/v1/licenses/testserver/

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{
    "serverAddress": "192.0.2.7",
    "localPort": 0,
    "remotePort": 27000,
    "serverType": null,
    "licenseType": null,
    "isServerConfigured": null,
    "gracePeriodLeft": 0,
    "isRestartLpeNeeded": null,
    "isScheduleNotificationNeeded": null,
    "licenseList": [],
    "licenseNotification": null
}
```


Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "isConnected": true

}
```

Obtenir la première date d'expiration

Trouve la licence avec la première date d'expiration.

URL : https://:/xenmobile/api/v1/licenses/getexpirationdate

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
    "expiredDate": 1448956800000,
    "daysBeforeExpire": 229,
    "daysInPOC": 0
}
```

Pour gérer les configurations LDAP

Le tableau suivant dresse la liste des paramètres utilisés dans les opérations de configuration LDAP.

Paramètre	Requis	Description
primaryHost	Oui	Adresse IP ou nom d'hôte du serveur LDAP principal. Entrez en tant qu'Adresse IP ou FQDN.
secondaryHost	Non	Adresse IP ou nom d'hôte du serveur LDAP secondaire. Entrez en tant qu'Adresse IP ou FQDN.
port	Oui	Numéro de port du serveur LDAP
username	Oui	Nom d'utilisateur d'un serveur LDAP valide
mot de passe	Oui	Mot de passe pour le nom d'utilisateur
userBaseDN	Oui	
lockoutLimit	Non	

lockoutTime	Non	
useSecure	Non	
userSearchBy	Oui	Recherche d'utilisateurs par upn ou samaccount
domaine	Oui	Nom de domaine unique du serveur LDAP
domainAlias	Oui	Alias pour le domaine LDAP
globalCatalogPort	Non	
gcRootContext	Non	
groupBaseDN	Oui	
isDefault	Non	Partie de la réponse GET qui indique si la configuration LDAP est la configuration par défaut.
name	Non	Partie de la réponse GET qui est un identificateur unique utilisé pour mettre à jour ou supprimer la configuration LDAP.

Répertorier la configuration LDAP

Répertorie la configuration LDAP entière dans XenMobile.

URL : https://:/xenmobile/api/v1/ldap

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

    “result”: [

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"aaa@example.com","password":"1.pwd","userB

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"test@xmexample.com","password":"1.pwd","us

    ]

}
```

Ajouter une nouvelle configuration LDAP

Ajoute une nouvelle configuration LDAP. Le nom de domaine doit être unique et ne peut pas être le même qu'une autre configuration LDAP.

URL : https://:/xenmobile/api/v1/ldap/msactivedirectory

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```

Exemple de réponse COPIER

```
{

    “status”: 0,

    “message”: “LDAP configuration created”

}
```

Modifier une configuration LDAP

Modifie une configuration LDAP, mais vous ne pouvez pas modifier le domaine avec l'opération de modification.

URL : https://:/xenmobile/api/v1/ldap/msactivedirectory/{nom}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```


Définir la configuration LDAP par défaut

Définit la configuration LDAP spécifiée en tant que configuration par défaut.

URL : https://:/xenmobile/api/v1/ldap/default/{nom}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Supprimer une configuration LDAP

Supprime la configuration LDAP spécifiée.

URL : https://:/xenmobile/api/v1/ldap/{nom}

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Pour gérer les configurations NetScaler Gateway

Vous permet de gérer les configurations de NetScaler Gateway. Le tableau suivant dresse la liste des paramètres utilisés dans les opérations NetScaler Gateway.

Paramètre	Requis	Description
name	Oui	Nom unique de NetScaler Gateway
alias	Non	
url	Oui	URL publiquement accessible pour NetScaler Gateway
passwordRequired	Oui	
logonType	Oui	Valeurs valides : domain-only, domain-token, domain-certificate, certificate-only, certificate-token et token-only
callback	Non	
default,	Oui	Définissez ce paramètre sur true ou false lors de l'ajout ou de la modification d'une configuration de NetScaler Gateway. Si ce paramètre n'est pas transmis, la valeur par défaut est false.

id	Non	Partie de la réponse GET qui est un identificateur unique utilisé pour mettre à jour ou supprimer la configuration NetScaler Gateway.

Répertorier toutes les configurations NetScaler Gateway

Répertorie la configuration NetScaler Gateway entière dans XenMobile.

URL : https://:/xenmobile/api/v1/netscaler

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

    “result”: [

        { "name":"displayName",

        "alias":"",

        "url":"https://externalURl.com",

        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false","id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        },

        { "name":"displayName",

        "alias":"",
```

```
            "url":"https://externalURl.com",

            "passwordRequired":"false",

            "logonType":"domain",

            "default":"false",

            "id":"",

            “callback”: [{“callbackUrl”:http://example.com,

            “ip”:”192.0.2.8”}]

            }

      ]

}
```

Ajouter une nouvelle configuration NetScaler Gateway

Ajoute une nouvelle configuration NetScaler Gateway.

URL : https://:/xenmobile/api/v1/netscaler

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "name":"displayName",

    "alias":"",

    “default”:true, "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “callback”: [{“callbackUrl”:http://example.com,

    “ip”:”192.0.2.8”}]

}
```

Modifier une configuration NetScaler Gateway

Modifie la configuration NetScaler Gateway spécifiée.

URL : https://:/xenmobile/api/v1/netscaler/{id}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "name":"displayName",

    "alias":"",

    "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “default”: true,

    “callback”: [{“callbackUrl”:http://ag.com,

    “ip”:”192.0.2.8”}]

}
```

Supprimer une configuration NetScaler Gateway

Supprime la configuration NetScaler Gateway spécifiée.

URL : https://:/xenmobile/api/v1/netscaler/{id}

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Définir la configuration NetScaler Gateway par défaut

Définit la configuration NetScaler Gateway spécifiée en tant que configuration par défaut.

URL : https://:/xenmobile/api/v1/netscaler/default/{id}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Pour gérer les configurations du serveur de notifications SMS et SMTP

Vous pouvez ajouter, modifier, activer (définir comme valeur par défaut) et supprimer les configurations du serveur SMS et SMTP. Le tableau suivant dresse la liste des paramètres utilisés dans les opérations de configuration du serveur SMS et SMTP.

Paramètre	Requis	Description
name	Oui	Nom unique de configuration SMS/SMTP.
serverType	Non	Type de serveur de notification (SMS ou SMTP) envoyé par le serveur dans la requête GET.
active	Non	Indique si le serveur est utilisé pour les notifications. Un seul serveur peut être actif pour chaque type.
id	Non	Identificateur unique utilisé pour mettre à jour, supprimer et activer le serveur.
description	Non	Description du serveur.
Paramètres SMS		
key	Oui	
secret	Oui	
virtualPhoneNumber	Oui	Doit utiliser un format de numéro de téléphone.
https	Oui	La valeur par défaut est false
country	Oui	
carrierGateway	Oui	La valeur par défaut est false
Paramètres SMTP		
secureChannelProtocol	Oui	Type de protocole de sécurité à utiliser. Les valeurs valides sont : None,

		SSL et TLS. La valeur par défaut est none.
port	Oui	
authentication	Oui	Indique s'il faut utiliser l'authentification. Les valeurs valides sont true et false.
username	Oui, si l'authentification est true.	
mot de passe	Oui, si l'authentification est true.	
msSecurePasswordAuth	Oui	La valeur par défaut est false
fromName	Oui	
fromEmail	Oui	
numOfRetries	Non	Un nombre entier. La valeur par défaut est 5.
timeout	Non	Un nombre entier. La valeur par défaut est 30.
maxRecipients	Non	Un nombre entier. La valeur par défaut est 100.

Répertorier tous les serveurs SMS et SMTP

Répertorie tous les serveurs SMS et SMTP dans XenMobile.

URL : https://:/xenmobile/api/v1/notificationserver

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Accept : application/json

Exemple de réponse COPIER

```
{

    “result”: [

        { "name":"serverName","serverType":"SMS,"active":"true","id":"10"},

        { "name":"serverName2","serverType":"SMTP,"active":"true","id":"10"},

        { "name":"serverName3","serverType":"SMS,"active":"false","id":"10"}

    ]

}
```

Obtenir les détails du serveur

Obtient des informations sur le serveur par ID de serveur.

URL : https://:/xenmobile/api/v1/notificationserver/{id}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Accept : application/json

Exemple de réponse SMS COPIER

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Exemple de réponse SMTP COPIER

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.12",

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Ajouter une configuration de serveur SMS

Ajoute une configuration de serveur SMS.

URL : https://:/xenmobile/api/v1/notificationserver/sms

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Modifier la configuration du serveur SMS

Modifie la configuration du serveur SMS spécifié.

URL : https://:/xenmobile/api/v1/notificationserver/sms/{id}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Ajouter une configuration de serveur SMTP

Ajoute une configuration de serveur SMTP.

URL : https://:/xenmobile/api/v1/notificationserver/smtp

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Modifier une configuration SMTP

Modifie la configuration SMTP spécifiée.

URL : https://:/xenmobile/api/v1/notificationserver/smtp/{id}

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    name":"displayName",

    "description":"Edited description",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Supprimer la configuration du serveur

Supprime la configuration du serveur SMS ou SMTP spécifié.

URL : https://:/xenmobile/api/v1/notificationserver/{id}

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Définir la configuration SMS par défaut

Définit la configuration du serveur SMS spécifié en tant que configuration par défaut.

URL : https://:/xenmobile/api/v1/notificationserver/activate/sms/{id}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Définir la configuration SMTP par défaut

Définit la configuration du serveur SMTP spécifié en tant que configuration par défaut.

URL : https://:/xenmobile/api/v1/notificationserver/activate/smtp/{id}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Pour gérer les utilisateurs et groupes locaux

Vous pouvez gérer les utilisateurs et groupes locaux en utilisant les services suivants.

Obtenir tous les utilisateurs

Obtient tous les utilisateurs locaux.

URL : https://:/xenmobile/api/v1/localusersgroups

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{
```

```
"status": 0,

"message": "Success",

"result": [

    {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"

        },

        "role": "ADMIN",

        "roles": null,

        "createdOn": "1/10/15 11:42 AM",

        "lastAuthenticated": "1/10/15 11:42 AM",

        "domainName": null,

        "adUser": false,

        "vppUser": false

    }
```



```
    ]

}
```

Obtenir un utilisateur

Obtient l'utilisateur local spécifié.

URL : https://:/xenmobile/api/v1/localusersgroups/{nom}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "result": {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"
```

```
            company": "Example"
        },
        "role": "ADMIN",
        "roles": null,
        "createdOn": "1/10/15 11:42 AM",
        "lastAuthenticated": "1/10/15 11:42 AM",
        "domainName": null,
        "adUser": false,
        "vppUser": false
    }
}
```

Ajouter un utilisateur

Ajoute un utilisateur avec les attributs spécifiés.

URL : https://:/xenmobile/api/v1/localusersgroups

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
        },
    "groups": [
        "MSP"
        ],
    "role": "USER",
    "username": "justaname_XX",
    "password": "password"
}
```

Exemple de réponse COPIER

```
{
    "status": 0,
```

```
"message": "Success",

"user": {

    "userid": 0,

    "username": "justaname_XX",

    "password": "password",

    "confirmPassword": null,

    "groups": [

        "MSP"

    ],

    "attributes": {

        "badpwdcount": "4",

        "asuseremail": "justa.name@example.com",

        "company": "example",

        "mobile": "4695557854"

    },

    "role": "USER",

    "roles": null,

    "createdOn": null,

    "lastAuthenticated": null,

    "domainName": null,
```



```
        "adUser": false,

        "vppUser": false

    }

}
```

Mettre à jour un utilisateur

Met à jour les attributs utilisateur.

URL : https://:/xenmobile/api/v1/localusersgroups

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "attributes": {

          "badpwdcount": "4",

          "asuseremail": "justa.name@example.com",

          "company": "example",

          "mobile": "4695557854"

          },

    "groups": [

          "MSP"

          ],

    "role": "USER",

    "username": "justaname_XX",

    "password": "password"

}
```

Exemple de réponse COPIER

```
{

    "status": 0,
```

```
"message": "Success",

"user": {

    "userid": 108,

    "username": "justaname_XX",

    "password": null,

    "confirmPassword": null,

    "groups": [

        "MSP"

    ],

    "attributes": {

        "badpwdcount": "4",

        "asuseremail": "justa.name@example.com",

        "company": "example",

        "mobile": "4695557854"

    },

    "role": "USER",

    "roles": null,

    "createdOn": "3/27/15 1:10 PM",

    "lastAuthenticated": "3/27/15 1:10 PM",

    "domainName": null,
```



```
        "adUser": false,

        "vppUser": false

    }

}
```

Changer le mot de passe utilisateur

Réinitialise le mot de passe d'un utilisateur ; vous pouvez également modifier le mot de passe d'un utilisateur dans l'appel « update local user ».

URL : https://:/xenmobile/api/v1/localusersgroups/resetpassword

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "username": “administrator”,

    “password”: “newPassword”

}
```

Exemple de réponse COPIER

```
Response Errors:

1250 – User id not found

1252 – Failed to reset the password

Password can also be changed in the update local user call.
```

Supprimer des utilisateurs

Supprime les utilisateurs spécifiés.

URL : https://:/xenmobile/api/v1/localusersgroups/resetpassword

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{ justaname XX }
```

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

Supprimer un utilisateur

Supprime l'utilisateur spécifié.

URL : https://:/xenmobile/api/v1/localusersgroups/

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

Importer un fichier de provisioning

Charge un fichier contenant les données de l'utilisateur local. Le fichier à charger doit être au format .csv. Pour de plus amples informations sur les fichiers de provisioning, consultez la section Formats des fichiers de provisioning.

URL : https://:/xenmobile/api/v1/localusersgroups/importprovisioningfile

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
importdata={"fileType:"user"}

uploadfile=<file to be uploaded.csv>
```

Exemple de réponse COPIER

```
{

   "status": 0,

   "message": "Success",

   "user": null

}
```

Pour gérer les applications

Vous pouvez gérer les applications avec les services suivants.

Obtenir toutes les applications par filtre

Obtient les applications en fonction des paramètres de filtre spécifiés.

URL : https://:/xenmobile/api/v1/application/filter

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté
Content type – application/json

Exemple de données de requête COPIER

```
{
    "start": 0,
    "limit": 10,

    "applicationSortColumn": "name",
    "sortOrder": "DESC",
    "enableCount": false,
    "search": "Worx",
    "filterIds":"['application.deliverygroup#<DG_Name>@_fn_@app.dg','application.deliverygroup#<DG_Name>@_fn_@app.d
}
```

Exemple de données de réponse COPIER

```
{

  "status": 0,

  "message": "Success",

  "applicationListData": {

    "totalMatchCount": 2,

    "totalCount": 2,

    "appList": [{

      "id": 2,

      "name": "WorxNotes",

      "description": "Worx Notes Application",

      "createdOn": "6/7/16 3:55 PM",

      "lastUpdated": "6/7/16 5:11 PM",

      "disabled": false,

      "nbSuccess": 0,

      "nbFailure": 0,

      "nbPending": 0,

      "schedule": null,

      "permitAsRequired": true,

      "iconData": "iVBORw0KGgoAAAANSUhEUgAAAHgAAAB4CAYAAAA5ZDbSAAA.....",

      "appType": "MDX",
```



```
    "categories": ["Default"],
    "roles": null,
    "workflow": null,
    "vppAccount": null
  }, {
    "id": 1,
    "name": "Angry Bird",
    "description": "",
    "createdOn": "6/7/16 3:53 PM",
    "lastUpdated": "6/7/16 3:54 PM",
    "disabled": false,
    "nbSuccess": 0,
    "nbFailure": 0,
    "nbPending": 0,
    "schedule": null,
    "permitAsRequired": true,
    "iconData": "/9j/4AAQSkZJRgABAQEAAQABAAD/2wBDAAYEBQYFBAYGBQYHBwYIChA...",
    "appType": "App Store App",
    "categories": ["Default"],
    "roles": null,
```



```
        "workflow": null,
        "vppAccount": null
      }]
    }
}
```

Obtenir des applications mobiles par conteneur

Obtient des applications mobiles dans le conteneur spécifié.

URL : https://:/xenmobile/api/v1/application/mobile/{Idconteneur}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
    "result": {
        "id": 14,
        "name": "testApp",
        "description": "",
```

```
"createdOn": null,

"lastUpdated": null,

"disabled": false,

"nbSuccess": 0,

"nbFailure": 0,

"nbPending": 0,

"schedule": {

    "enableDeployment": true,

    "deploySchedule": "NOW",

    "deployScheduleCondition": "EVERYTIME",

    "deployDate": null,

    "deployTime": null,

    "deployInBackground": false

},

"iconData": "",

"appType": "MDX",

"categories": [

    "Default"

],

"roles": [],
```



```
"workflow": null,
"ios": {
"displayName": "GoToMeeting",
"description": "G2MW_IOS_5.3.3_075_01",
"paid": false,
"removeWithMdm": true,
"preventBackup": true,
"appVersion": "5.3.3.075",
"minOsVersion": "",
"maxOsVersion": "",
"excludedDevices": "",
"avppParams": null,
"avppTokenParams": null,
"rules": null,
"appType": "mobile_ios",
"uuid": "8e69d397-48bb-4f29-a95c-dd7b16665c1c",
"id": 0,
"store": {
"rating": {
"rating": 0,
```



```
            "reviewerCount": 0
        },
        "screenshots": [],
        "faqs": [],
        "storeSettings": {
            "rate": true,
            "review": true
        }
    },
    "policies": [
        {
            "policyName": "ReauthenticationPeriod",
            "policyValue": "480",
            "policyType": "integer",
            "policyCategory": "Authentication",
            "title": "Reauthentication period (minutes)",
            "description": "\nDefines the period before a user is challenged to authenticate again. ",
            "units": "minutes",
            "explanation": null
        }
```



```
},
{
    "policyName": "BlockJailbrokenDevices",
    "policyValue": "true",
    "policyType": "boolean",
    "policyCategory": "Device Security",
    "title": "Block jailbroken or rooted",
    "description": "\nIf On, the application is locked when the device is jailbroken or rooted.",
    "units": null,
    "explanation": null
},
{
    "policyName": "CertificateLabel",
    "policyValue": "",
    "policyType": "string",
    "policyCategory": "Network Access",
    "title": "Certificate label",
    "description": "\nThe label for the certificate.\n                                                    Default value is er
    "units": null,
    "explanation": null
```



```
                }

            ]

        },

        "android": null,

        "android_knox": null,

        "android_work": null,

        "windows": null,

        "windows_tab": null

    }

}
```

Obtenir applications d'un magasin public par conteneur

Obtient les applications d'un magasin public depuis le conteneur spécifié.

URL : https://:/xenmobile/api/v1/application/mobile/appstore/{Idconteneur}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Supprimer un conteneur d'application

Supprime le conteneur d'application spécifié.

URL: https://:/xenmobile/api/v1/application/{Idconteneur}

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Pour gérer les configurations de groupe de mise à disposition

Vous pouvez gérer les configurations de groupe de mise à disposition avec les services suivants.

Obtenir des groupes de mise à disposition par filtre

Utilise les paramètres de filtre spécifiés pour obtenir les groupes de mise à disposition.

URL : https://:/xenmobile/api/v1/deliverygroups/filter

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
{

  "start": 1,

  "sortOrder": "DESC",

  "deliveryGroupSortColumn": "id",

  “limit”:10,

  "search": "add"

}
```

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",
```

```
"dgListData": {

"totalMatchCount": 7,

"totalCount": 10,

"dgList": [

{

"id": null,

"name": "add delivery group 6.0",

"description": "testing add delivery group 6.0",

"groups": [[{

{

"id": 1null,

"userListId": 1null,

"name": "MSPTESTLOCALGROUP",

"uniqueName": "MSPTESTLOCALGROUP",

"uniqueId": "MSPTESTLOCALGROUP",

"domainName": "local",

"primaryToken": 0null,

}"objectSid": null

],},

{
```



```
        "id": null,
        "userListId": null,
        "name": "AC08EP61S75",
        "uniqueName": "AC08EP61S75",
        "uniqueId": "AC08EP61S75",
        "domainName": "local",
        "primaryToken": null,
        "objectSid": null
    }],
    "users": [{
        "uniqueName": null,
        "domainName": "local",
        "name": null,
        "objectId": "shankar",
        "customProperties": {
            "name": "value",
            "name1": "value1"
        },
        "uniqueId": "shankar"
    }],
```



```
"zoneId": null,

"zoneDomain": null,

"rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId

"disabled": false,

"lastUpdated": 1427144713353,

"anonymousUser": true,

"roledefLangVersionId": 1,

"applications": [

    {

        "name": "Web Link",

        "required": false

    },

    {

        "name": "GoogleApps_SAML",

        "required": true

    }

],

"devicePolicies": [

    "test terms conditions"

]
```



```
        ],
        "smartActions": [
            "shankar ganesh"
        ],
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0
    },
    {
        "id": null,
        "name": "add delivery group 5.0",
        "description": "testing add delivery group 5.0",
        "groups": [
            {
                "id": 1,
                "userListId": 1,
                "name": "MSP",
                "uniqueName": "MSP",
                "uniqueId": "MSP",
                "domainName": "local",
```



```
                "primaryToken": 0

            }

        ],

        "zoneId": null,

        "zoneDomain": null,

        "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId

        "disabled": false,

        "lastUpdated": 1426891345698,

        "anonymousUser": true,

        "roledefLangVersionId": 1,

        "applications": [

            {

                "name": "GoogleApps_SAML",

                "required": true

            },

            {

                "name": "Web Link",

                "required": false

            }

        ],
```



```
                    "devicePolicies": [

                        "test terms conditions"

                    ],

                    "smartActions": [

                        "shankar ganesh"

                    ],

                    "nbSuccess": 0,

                    "nbFailure": 0,

                    "nbPending": 0

                }

            ]

        }



}
```


Obtenir un groupe de mise à disposition par nom

URL : https://:/xenmobile/api/v1/deliverygroups/{nom}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
    "role": {
        "id": null,
        "name": "AllUsers",
        "description": "default role",
        "groups": [],
        "zoneId": null,
        "zoneDomain": null,
        "rules": null,
        "disabled": false,
        "lastUpdated": null,
        "anonymousUser": false,
        "roledefLangVersionId": 1,
        "applications": [
            {
                "name": "test mdx",
                "required": false
            },
```



```
        {
            "name": "test all",
            "required": false
        },
        {
            "name": "justa test",
            "required": false
        },
        {
            "name": "test enterprise",
            "required": false
        },
        {
            "name": "name test",
            "required": false
        }
    ],
    "devicePolicies": [
        "test terms conditions"
    ],
```



```
        ],
        "smartActions": [
            "justa name"
        ],
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0
    }
}
```

Modifier un groupe de mise à disposition

URL : https://:/xenmobile/api/v1/deliverygroups

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
{
  "name": "temp3",
  "description": "temp3 desc",
  "applications": [
```

```
{

            "name": "TESTAPP",

             "priority": -1,

             "required": false

                    }     ],

    "devicePolicies": [

        {

             "name":"test terms conditions",

             "priority":-1

         }

      ],

    "smartActions": [

        {

           "name":"Smart Action Name 1",

           "priority":-1

         }

      ],

  "groups": [

     {

  "uniqueName": "AC08EP61S75",

       "domainName": "local",

       "name": "AC08EP61S75",

       "objectSid": "AC08EP61S75",
```

```
"uniqueId": "AC08EP61S75",

"customProperties": {

    "gr1": "gr1",

    "gr2": "gr2"

  }

    }

  ],

  "users": [

    {

      "uniqueName": "testuser",

      "domainName": "local",

      "name": " testuser ",

      "objectId": " testuser "

    }

  ],

  "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\" te

}
```


Exemple de réponse COPIER


```
{

      "status": 0,

      "message": "Success",

"role": {

            "id": null,

            "name": "temp4",

            "description": "temp4 desc",

            "zoneId": null,

            "zoneDomain": null,

            "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value

            "disabled": false,

            "lastUpdated": null,

            "anonymousUser": false,

            "roledefLangVersionId": null,

            "applications": [

                  {

                  "name": "TESTAPP2",

                  "priority": -1,
```



```
                "required": false

            },

{

                "name": "TESTAPP2",

                "priority": -1,

                "required": false

            }

            ],

            "devicePolicies": [

                {

                "name": "TestPolicy1",

                "priority": -1

            },

{

                "name": "TestPolicy",

                "priority": -1

            }

            ],

            "smartActions": [

{
```

```
                "name": "TestAction2",

                "priority": -1

            },

{

                "name": "TestAction3",

                "priority": -1

            }

        ],

            "nbSuccess": 0,

            "nbFailure": 0,

            "nbPending": 0,

            "groups": [{

                  "uniqueName": "AC08EP61S75",

                 "domainName": "local",

                "name": "AC08EP61S75",

                 "objectSid": "AC08EP61S75",

                "uniqueId": "AC08EP61S75",

                "customProperties": {

                  "gr1": "gr1",

                    "gr2": "gr2"
```



```
            }

        }],

        "users": [{

            "uniqueName": " tempuser ",

            "domainName": "local",

            "name": " tempuser ",

            "objectId": " tempuser ",

            "customProperties": null,

            "uniqueId": " tempuser "

        }]


    }
```

Ajouter un groupe de mise à disposition

Ajoute un groupe de mise à disposition.

URL : https://:/xenmobile/api/v1/deliverygroups

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
{

  "name": "temp3",

  "description": "temp3 desc",

  "applications": [

{

            "name": "TESTAPP",

             "priority": -1,

             "required": false

                    }     ],

    "devicePolicies": [

        {

            "name":"test terms conditions",

            "priority":-1

         }

      ],

    "smartActions": [

        {

           "name":"Smart Action Name 1",

           "priority":-1

         }

      ],

  "groups": [

    {

  "uniqueName": "AC08EP61S75",
```



```
        "domainName": "local",

        "name": "AC08EP61S75",

        "objectSid": "AC08EP61S75",

"uniqueId": "AC08EP61S75",

"customProperties": {

     "gr1": "gr1",

     "gr2": "gr2"

  }}

  ],

  "users": [

    {

      "uniqueName": "testuser",

      "domainName": "local",

      "name": "testuser",

      "objectId": "testuser"

    }

  ],

  "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\"te

}
```


Exemple de réponse COPIER


```
{
      "status": 0,
      "message": "Success",
"role": {
            "id": null,
            "name": "temp4",
            "description": "temp4 desc",
            "zoneId": null,
            "zoneDomain": null,
            "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value
            "disabled": false,
            "lastUpdated": null,
            "anonymousUser": false,
            "roledefLangVersionId": null,
            "applications": [
                  {
                  "name": "TESTAPP2",
                  "priority": -1,
```



```
                "required": false
            },
{
                "name": "TESTAPP2",
                "priority": -1,
                "required": false
            }
            ],
            "devicePolicies": [
                {
                "name": "TestPolicy1",
                "priority": -1
            },
{
                "name": "TestPolicy",
                "priority": -1
            }
            ],
            "smartActions": [
{
```

```
{
                "name": "TestAction2",
                "priority": -1
            },
{
                "name": "TestAction3",
                "priority": -1
            }
        ],
            "nbSuccess": 0,
            "nbFailure": 0,
            "nbPending": 0,
            "groups": [{
                  "uniqueName": "AC08EP61S75",
          "domainName": "local",
          "name": "AC08EP61S75",
          "objectSid": "AC08EP61S75",
"uniqueId": "AC08EP61S75",
"customProperties": {
      "gr1": "gr1",
```



```
        "gr2": "gr2"

    }        }],

            "users": [{

                "uniqueName": " tempuser ",

                "domainName": "local",

                "name": " tempuser ",

                "objectId": " tempuser ",

                "customProperties": null,

                "uniqueId": " tempuser "

            }]


      }
```

Supprimer un groupe de mise à disposition

Supprime les groupes de mise à disposition spécifiés.

URL : https://:/xenmobile/api/v1/deliverygroups

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
[ "add delivery group 11.0" ]
```

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
    "roleNames": [
        "add delivery group 11.0"
    ]
}
```

Activer ou désactiver un groupe de mise à disposition

Activez ou désactivez les groupes de mise à disposition spécifiés.

URL : https://:/xenmobile/api/v1/deliverygroups/{groupe mise à disposition}/{enable/disable}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "roleName": "AllUsers"

}
```

Pour gérer les propriétés du serveur

Vous pouvez gérer les propriétés du serveur XenMobile à l'aide des services suivants.

Obtenir toutes les propriétés du serveur

Obtient tous les propriétés du serveur XenMobile.

URL : https://:/xenmobile/api/v1/serverproperties

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": [

        {

            "id": 1,

            "name": "ios.mdm.pki.ca-root.certificatefile",
```



```
        "value": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",
        "displayName": "ios.mdm.pki.ca-root.certificatefile",
        "description": "",
        "defaultValue": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",
        "displayFlag": false,
        "editFlag": true,
        "deleteFlag": false,
        "markDeleted": false
    } ,
    {
        "id": 2,
        "name": "ios.mdm.https.host",
        "value": "192.0.2.4",
        "displayName": "ios.mdm.https.host",
        "description": "",
        "defaultValue": "192.0.2.4",
        "displayFlag": false,
        "editFlag": false,
        "deleteFlag": false,
```



```
            "markDeleted": false

        },

        {

            "id": 3,

            "name": "ios.mdm.enrolment.checkRemoteAddress",

            "value": "false",

            "displayName": "iOS Device Management Enrollment - Check Remote Address",

            "description": "",

            "defaultValue": "false",

            "displayFlag": true,

            "editFlag": true,

            "deleteFlag": false,

            "markDeleted": false

        },

    ]

}
```


Obtenir les propriétés du serveur par filtre

Obtient les propriétés du serveur à l'aide des paramètres de filtre spécifiés.

URL : https://:/xenmobile/api/v1/serverproperties/filter

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{
    "start": 0,
    "limit": 1000,
    "orderBy": "name",
    "sortOrder": "desc",
    "searchStr": "justaserver1"
}
```

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": [
        {
            "id": 154,
            "name": "justaserver123",
```

```
            "value": "justaserver1",

            "displayName": "justarserver display name",

            "description": "justaserver description",

            "defaultValue": "justaserver1",

            "displayFlag": true,

            "editFlag": true,

            "deleteFlag": true,

            "markDeleted": false

        }

    ]

}
```

Ajouter une propriété de serveur

Ajoute la propriété de serveur spécifiée.

URL : https://:/xenmobile/api/v1/serverproperties

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 1",
    "description": "Description 1"
}
```

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": null
}
```

Modifier des propriétés de serveur

Modifie la propriété de serveur spécifiée.

URL : https://:/xenmobile/api/v1/serverproperties

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 2",
    "description": "Description 2"
}
```

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Réinitialiser des propriétés de serveur

Réinitialise les propriétés de serveur spécifiées.

URL : https://:/xenmobile/api/v1/serverproperties/reset

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "names": [,

        "justaname7"

        ]

}
```

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": null

}
```

Supprimer des propriétés de serveur

URL : https://:/xenmobile/api/v1/serverproperties

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "justaname3",

    "justaname4"

}
```

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

Pour gérer les appareils

Vous pouvez gérer les appareils dans XenMobile à l'aide des services suivants.

Obtenir des appareils par filtre

URL : https://:/xenmobile/api/v1/device/filter

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Tous les **paramètres de requête** sont facultatifs.

Valeurs valides pour **sortOrder** : ASC, DSC et DESC.

Valeurs valides pour **sortColumn** : ID, SERIAL, IMEI, ACTIVESYNCID, WIFIMAC, BLUETOOTHMAC, OSFAMILY, SYSTEM_OEM, SYSTEM_PLATFORM, SYSTEM_OS_VERSION, DEVICE_PROPERTY, LASTAUTHDATE, INACTIVITYDAYS,ISACTIVE, LASTUSER, BLCOMPLIANT, WLCOMPLIANT, RLCOMPLIANT, MANAGED, SHAREABLE et BULKPROFILESTATUS.

Paramètres de requête COPIER


```
{
  "start": "0-999",
  "limit": "0-999",
  "sortOrder": "ASC",
  "sortColumn": "ID",
  "search": "Any search term",
  "enableCount": "false",
  "constraints": "{'constraintList':[{'constraint':'DEVICE_OS_FAMILY','parameters':[{'name':'osFamily','type':'STRING','value':'iO
  "filterIds": "['group#/group/MSP@_fn_@normal']"
}
```


Exemple de réponse COPIER


```
{
```



```
"id": "1-9999999",

"jailBroken": "true/false",

"managed": "true/false",

"gatewayBlocked": "true/false",

"deployFailed": "1-999",

"deployPending": "1-999",

"deploySuccess": "1-999",

"mdmKnown": "true/false",

"mamRegistered": "true/false",

"mamKnown": "true/false",

"userName": "user name",

"serialNumber": "serial number",

"imeiOrMeid": "IMEI/MEID",

"activeSyncId": "Active sync ID",

"wifiMacAddress": "WiFi MAC address",

"blueToothMacAccress": "Bluetoothi MAC address",

"devicePlatform": "Device platform",

"osVersion": "Operating system version of the device",

"deviceModel": "Device model information",

"lastAccess": "Timestamp when the device was last accessed",
```

```
    "inactivityDays": "Number of days device has been inactive",

    "shareable": "Flag indicating if the device is shareable",

    "sharedStatus": "Get shareable status of the device",

    "depRegistered": "Flag indicating if the device is DEP registered",

    "deviceName": "Name of the device",

    "deviceType": "Phone/Tablet",

    "productName": "Product name",

    "platform": "Platform of the device"

}
```

Obtenir des appareils par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/{ID_appareil}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "device": {

  "htcMdm": true,
```

```
"managedByZMSP": true,

"serialNumber": "string",

"id": 0,

"applications": [

 {

  "resourceType": "APP_NATIVE",

  "resourceTypeLabel": "string",

  "packageInfo": "string",

  "statusLabel": "string",

  "lastUpdate": 0,

  "status": "SUCCESS",

  "name": "string"

 }

],

"smartActions": [

 {

  "resourceType": "APP_NATIVE",

  "resourceTypeLabel": "string",

  "packageInfo": "string",

  "statusLabel": "string",
```



```
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
  }
],
"platform": "string",
"osFamily": "WINDOWS",
"nbSuccess": 0,
"nbFailure": 0,
"nbPending": 0,
"deliveryGroups": [
  {
    "statusLabel": "string",
    "linkey": "string",
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
  }
],
"lastAuthDate": 0,
```



```
"sharedStatus": "INACTIVE",
"managed": true,
"smgStatus": "ACCESS_ALLOWED",
"mdmKnown": true,
"mamKnown": true,
"mamRegistered": true,
"lastUsername": "string",
"imei": "string",
"activesyncid": "string",
"wifimac": "string",
"bluetoothmac": "string",
"inactivityDays": 0,
"shareable": true,
"bulkProfileStatus": "NO_BULK",
"deviceType": "string",
"softwareInventory": [
 {
  "version": "string",
  "blacklistCompliant": true,
```



```
    "suggestedListCompliant": true,
    "packageInfo": "string",
    "installCount": 0,
    "installTimeStamp": 0,
    "author": "string",
    "container": 0,
    "name": "string",
    "size": 0
  }
],
"deviceActions": [
  {
    "actionType": "WIPE",
    "failedTime": 0,
    "doneTime": 0,
    "askedTime": 0
  }
],
"managedSoftwareInventory": [
  {
```



```
    "version": "string",
    "blacklistCompliant": true,
    "suggestedListCompliant": true,
    "packageInfo": "string",
    "installCount": 0,
    "installTimeStamp": 0,
    "author": "string",
    "container": 0,
    "name": "string",
    "size": 0
  }
],
"policies": [
  {
    "resourceType": "APP_NATIVE",
    "resourceTypeLabel": "string",
    "packageInfo": "string",
    "statusLabel": "string",
    "lastUpdate": 0,
    "status": "SUCCESS",
```



```
    "name": "string"

  }

],

"active": true,

"xmlId": "string",

"deviceUsers": [

 {

   "user": {

     "displayName": "string",

     "id": 0,

     "xmlId": "string",

     "properties": [

       {

         "displayName": "string",

         "id": 0,

         "b64": true,

         "group": "string",

         "name": "string",

         "value": "string"

       }
```



```
    ]

   },

   "lastAuthDate": 0,

   "prevAuthDate": 0,

   "userLogin": "string"

  }

 ],

 "packageStates": [

  {

   "packageName": "string",

   "packageId": 0,

   "statusLabel": "string",

   "date": 0,

   "status": "PENDING"

  }

 ],

 "pushState": "ENQUEUED",

 "pushStateLabel": "string",

 "lastPushDate": 0,

 "lastSentNotification": 0
```



```
 "lastSentNotification": 0,
"lastRepliedNotification": 0,
"strongId": "string",
"lastSoftwareInventoryTime": 0,
"firstConnectionDate": 0,
"lastIOSProfileInventoryTime": 0,
"lastUser": {
 "displayName": "string",
 "id": 0,
 "xmlId": "string",
 "properties": [
  {
   "displayName": "string",
   "id": 0,
   "b64": true,
   "group": "string",
   "name": "string",
   "value": "string"
  }
 ]
```



```
  },
  "blacklistCompliant": true,
  "suggestedListCompliant": true,
  "requiredListCompliant": true,
  "devicePropertiesTimestamp": 0,
  "revoked": true,
  "mamDeviceId": "string",
  "deviceToken": "string",
  "typeInst": 0,
  "appLock": true,
  "appWipe": true,
  "mamReady": true,
  "validCertificates": [
   {
    "credentialProviderId": "string",
    "type": "string",
    "issuerName": "string",
    "startDate": 0,
    "endDate": 0,
    "revoked": true,
```

```
    "certificateNumber": "string"
  }
],
"revokedCertificates": [
  {
    "credentialProviderId": "string",
    "type": "string",
    "issuerName": "string",
    "startDate": 0,
    "endDate": 0,
    "revoked": true,
    "certificateNumber": "string"
  }
],
"authorizeEnabled": true,
"revokeEnabled": true,
"lockEnabled": true,
"cancelLockEnabled": true,
"unlockEnabled": true,
"cancelUnlockEnabled": true,
```



```
"containerLockEnabled": true,

"cancelContainerLockEnabled": true,

"containerUnlockEnabled": true,

"cancelContainerUnlockEnabled": true,

"containerPwdResetEnabled": true,

"cancelContainerPwdResetEnabled": true,

"wipeEnabled": true,

"cancelWipeEnabled": true,

"clearRestrictionsEnabled": true,

"cancelClearRestrictionsEnabled": true,

"corpWipeEnabled": true,

"cancelCorpWipeEnabled": true,

"sdCardWipeEnabled": true,

"cancelSdCardWipeEnabled": true,

"locateEnabled": true,

"cancelLocateEnabled": true,

"enableTrackingEnabled": true,

"disableTrackingEnabled": true,

"disownEnabled": true,

"activationLockBypassEnabled": true,
```



```
"ringEnabled": true,
"cancelRingEnabled": true,
"newPinCode": "string",
"oldPinCode": "string",
"lockMessage": "string",
"resetPinCode": true,
"scanTime": "string",
"screenSharingPwd": "string",
"iosprofileInventory": [
 {
  "iosConfigInventories": [
   {
    "description": "string",
    "type": "string",
    "organization": "string",
    "identifier": "string",
    "name": "string"
   }
  ],
```



```
    "description": "string",
    "organization": "string",
    "managed": true,
    "identifier": "string",
    "receivedDate": 0,
    "encrypted": true,
    "name": "string"
   }
  ],
  "iosprovisioningProfileInventory": [
   {
    "managed": true,
    "uuid": "string",
    "expiryDate": 0,
    "name": "string"
   }
  ],
  "erasedMemoryCard": true,
  "gpsCoordinates": [
   {
```



```
    "gpsTimestamp": 0

   }

],

"lastGpsCoordinate": {

  "gpsTimestamp": 0

},

"gpsFilterStartDate": 0,

"gpsFilterEndDate": 0,

"wipePinCode": "string",

"lockPhoneNumber": "string",

"dstDevIdUsed": true,

"dstValue": "string",

"smartActionsFailure": true,

"policiesFailure": true,

"applicationsFailure": true,

"touchdownProperties": [

  {

    "category": "string",

    "name": "string",

    "value": "string"
```



```
  }

],

"appUnwipeEnabled": true,

"requestMirroringEnabled": true,

"cancelRequestMirroringEnabled": true,

"stopMirroringEnabled": true,

"cancelStopMirroringEnabled": true,

"knownByZMSP": true,

"wipeDeviceFlag": true,

"lockDeviceFlag": true,

"appWipeEnabled": true,

"appLockEnabled": true,

"appUnlockEnabled": true,

"bulkEnrolled": true,

"nbAvailable": 0,

"hasContainer": true,

"connected": true,

"properties": [

  {

    "displayName": "string",
```



```
      "id": 0,
      "b64": true,
      "group": "string",
      "name": "string",
      "value": "string"
    }
  ]
 }
}
```


Obtenir les applications d'un appareil par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/{ID_appareil}/apps

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "applications": [

  {

   "resourceType": "APP_NATIVE",

   "resourceTypeLabel": "string",

   "packageInfo": "string",

   "statusLabel": "string",

   "lastUpdate": 0,

   "status": "SUCCESS",

   "name": "string"

  }

 ]

}
```


Obtenir les actions d'un appareil par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/{ID_appareil}/actions

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "actions": [
  {
   "resourceType": "APP_NATIVE",
   "resourceTypeLabel": "string",
   "packageInfo": "string",
   "statusLabel": "string",
   "lastUpdate": 0,
   "status": "SUCCESS",
   "name": "string"
  }
 ]
}
```

Obtenir les groupes de mise à disposition d'un appareil par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/{ID_appareil}/deliverygroups

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deliveryGroups": [

  {

   "statusLabel": "string",

   "linkey": "string",

   "lastUpdate": 0,

   "status": "SUCCESS",

   "name": "string"

  }

 ]

}
```

Obtenir l'inventaire logiciel géré par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/{ID_appareil}/managedswinventory

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER


```
{
 "status": 0,
 "message": "string",
 "softwareInventory": [
  {
   "version": "string",
   "blacklistCompliant": true,
   "suggestedListCompliant": true,
   "packageInfo": "string",
   "installCount": 0,
   "installTimeStamp": 0,
   "author": "string",
   "container": 0,
   "name": "string",
   "size": 0
  }
 ]
}
```


Obtenir les stratégies par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/{ID_appareil}/policies

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "policies": [

  {

   "resourceType": "APP_NATIVE",

   "resourceTypeLabel": "string",

   "packageInfo": "string",

   "statusLabel": "string",

   "lastUpdate": 0,

   "status": "SUCCESS",

   "name": "string"

  }

 ]

}
```


Obtenir l'inventaire logiciel par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/{ID_appareil}/softwareinventory

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER


```
{
 "status": 0,
 "message": "string",
 "softwareInventory": [
  {
   "version": "string",
   "blacklistCompliant": true,
   "suggestedListCompliant": true,
   "packageInfo": "string",
   "installCount": 0,
   "installTimeStamp": 0,
   "author": "string",
   "container": 0,
   "name": "string",
   "size": 0
  }
 ]
}
```


Obtenir les coordonnées GPS par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/locations/{id_appareil}

Paramètres de requête :

startDate : date de début du filtre de coordonnées
endDate : date de fin du filtre de coordonnées

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceCoordinates": {

  "deviceCoordinateList": {

   "deviceCoordinateList": [

    {

     "gpsTimestamp": 0

    }

   ],

   "startDate": 0,

   "endDate": 0

  }

}
```

Envoyer une notification à une liste d'appareils ou d'utilisateurs

URL : https://:/xenmobile/api/v1/device/notify

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
{
 "smtpFrom": "Test",
 "to": [
  {
   "deviceId": "1",
   "email": "user@test.com",
   "osFamily": "iOS",
   "serialNumber": "F7NLX6WDF196",
   "smsTo": "+123456676",
   "token": {
    "type": "apns",
     "value": "dfb2fb351a4fb068e40858ecad572e317e6c39b4fa7de6fb29ea1ad7e2254499"
   }
  }
 ],
 "smtpSubject": "This is test subject",
 "smtpMessage": "This is test message",
 "smsMessage": "This is test message",
 "agentMessage": "This is test message",
 "sendAsBCC": "true",
```



```
"smtp": "true",

"sms": "true",

"agent": "true",

"templateId": "-1",

"agentCustomProps": {

 "sound": "Casino.wav"

}
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "notificationRequests": {

  "smtpNotifRequestId": 0,

  "smsNotifRequestId": 0,

  "smsGatewayNotifRequestId": 0,

  "apnsAgentNotifRequestId": 0,

  "shtpAgentNotifRequestId": 0

 }

}
```

Autoriser une liste d'appareils

URL : https://:/xenmobile/api/v1/device/authorize

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```


Appliquer la non utilisation du verrouillage d'activation sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/activationLockBypass

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Appliquer le mode kiosque sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/appLock

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Appliquer l'effacement de l'application sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/appWipe

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Appliquer le verrouillage du conteneur sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/containerLock

Paramètres de requête : newPinCode - code PIN pour le conteneur Android

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Annuler le verrouillage du conteneur sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/containerLock/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Appliquer le déverrouillage du conteneur sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/containerUnlock

Paramètres de requête : newPinCode - code PIN pour le conteneur Android

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Annuler le déverrouillage du conteneur sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/containerUnlock/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Réinitialiser le mot de passe du conteneur sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/containerPwdReset

Paramètres de requête : newPinCode - code PIN pour le conteneur Android

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Annuler la réinitialisation du mot de passe du conteneur sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/containerPwdReset/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Exclure une liste d'appareils

URL : https://:/xenmobile/api/v1/device/disown

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Rechercher une liste d'appareils

URL : https://:/xenmobile/api/v1/device/locate

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Annuler la recherche d'une liste d'appareils

URL : https://:/xenmobile/api/v1/device/locate/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Activer le suivi GPS sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/track

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Annuler le suivi GPS sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/track/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Verrouiller une liste d'appareils

URL : https://:/xenmobile/api/v1/device/lock

Paramètres de requête :

newPinCode : le code PIN doit être compris entre 4 et 16 caractères pour les appareils Android et Symbian. Le code PIN doit comporter 4 chiffres pour les appareils Windows

resetPinCode : permet d'ajouter une demande de réinitialisation du code PIN à la demande de verrouillage. Uniquement disponible pour Windows Phone 8.1
lockMessage : permet d'ajouter un message à la demande de verrouillage. Disponible uniquement pour iOS 7 et versions ultérieures
phoneNumber : permet d'ajouter un numéro de téléphone à la demande de verrouillage. Disponible uniquement pour iOS 7 et versions ultérieures

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Annuler le verrouillage d'une liste d'appareils

URL : https://:/xenmobile/api/v1/device/lock/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Déverrouiller une liste d'appareils

URL : https://:/xenmobile/api/v1/device/unlock

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Annuler le déverrouillage d'une liste d'appareils

URL : https://:/xenmobile/api/v1/device/unlock/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Déployer une liste d'appareils

URL : https://:/xenmobile/api/v1/device/refresh

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Demander une mise en miroir AirPlay sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/requestMirroring

Paramètres de requête :

dstName : nom de destination, en tant que nom de destination ou ID d'appareil de destination
dstDevId : adresse MAC de l'appareil de destination, en tant que nom de destination ou ID d'appareil de destination

scanTime : durée de l’analyse en nombre de secondes
screenSharingPwd : mot de passe pour le partage d’écran

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Annuler la demande de mise en miroir AirPlay sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/requestMirroring/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Arrêter la mise en miroir AirPlay sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/stopMirroring

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```


Annuler l'arrêt de la mise en miroir AirPlay sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/stopMirroring/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Effacer toutes les restrictions sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/restrictions/clear

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```


Annuler l'effacement de toutes les restrictions sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/restrictions/clear/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Révoquer une liste d'appareils

URL : https://:/xenmobile/api/v1/device/revoke

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Appeler une liste d'appareils

URL : https://:/xenmobile/api/v1/device/ring

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Annuler l'appel d'une liste d'appareils

URL : https://:/xenmobile/api/v1/device/ring/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Effacer une liste d'appareils

URL : https://:/xenmobile/api/v1/device/wipe

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Annuler l'effacement d'une liste d'appareils

URL : https://:/xenmobile/api/v1/device/wipe/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Effacer les données d'entreprise d'une liste d'appareils

URL : https://:/xenmobile/api/v1/device/selwipe

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Annuler l'effacement des données d'entreprise d'une liste d'appareils

URL : https://:/xenmobile/api/v1/device/selwipe/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Effacer les cartes SD sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/sdcardwipe

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Annuler l'effacement des cartes SD sur une liste d'appareils

URL : https://:/xenmobile/api/v1/device/sdcardwipe/cancel

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
[1,2]
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Obtenir toutes les propriétés connues sur un appareil

URL : https://:/xenmobile/api/v1/device/knownProperties

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER


```
{
 "status": 0,
 "message": "string",
 "knownProperties": {
  "knownProperties": {
   "knownPropertyList": [
    {
     "name": "string",
     "type": "STRING",
     "displayName": "string",
     "group": "EVERYWAN",
     "groupLabel": "string"
    }
   ]
  }
}
```


Obtenir toutes les propriétés utilisées sur un appareil

URL : https://:/xenmobile/api/v1/device/usedProperties

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{
 "status": 0,
 "message": "string",
 "deviceUsedPropertiesList": {
  "deviceUsedProperties": {
   "deviceUsedPropertiesParameters": [
    {
     "name": "string",
     "type": "STRING",
     "displayName": "string"
    }
   ]
  }
 }
}
```

Obtenir toutes les propriétés d'un appareil par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/properties/{id_appareil}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER


```
{
 "status": 0,
 "message": "string",
 "devicePropertiesList": {
  "deviceProperties": {
   "startIndex": 0,
   "devicePropertyParameters": [
    {
     "name": "string",
     "value": "string",
     "id": 0,
     "displayName": "string",
     "group": "string",
     "b64": true
    }
   ],
```



```
    "totalCount": 0

  }

 }

}
```

Mettre à jour toutes les propriétés d'un appareil par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/properties/{id_appareil}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
{

  "properties": [

    {

      "name": "ACTIVE_ITUNES",

      "value": "0"

    }

  ]

}
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string"

}
```

Ajouter ou mettre à jour une propriété d'appareil par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/properties/{id_appareil}

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de requête COPIER

```
{

 "name": "PROPERTY_NAME",

 "value": "PROPERTY_VALUE"

}
```

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string"

}
```

Supprimer une propriété d'appareil par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/properties/{id_appareil}

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string"

}
```

Obtenir l'état du MDM d'un appareil iOS par ID de l'appareil

URL : https://:/xenmobile/api/v1/device/mdmStatus/{id_appareil}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "deviceMdmStatus": {

  "deviceMdmStatusParameters": {

     "pushState": "ENQUEUED",

     "lastPushDate": 0,

     "lastRepliedNotification": 0,

     "lastSentNotification": 0,

     "pushStateLabel": "string"

   }

 }

}
```

Générer un code PIN

URL : https://:/xenmobile/api/v1/device/pincode/generate

Paramètres de requête: pinCodeLength - longueur du code PIN requis

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

 "status": 0,

 "message": "string",

 "pinCode": {

  "answer": "string"

 }

}
```

API SOAP XenMobile

Aug 22, 2016

Vous pouvez utiliser les API des services Web SOAP suivants dans XenMobile pour gérer votre flotte mobile. Vous pouvez télécharger les API et les kits de développement pour XenMobile depuis le site XenMobile Developer Community.

Nom WSDL (Service Web Definition Language)	Appels
EveryWanDevice	addDevice
	addDevice
	authenticateUser
	authorize
	canCreateUser
	clearDeploymentHisto
	corporateDataWipeDevice
	createUser
	deploy
	deviceExists
	disableTrackingDevice
	enableTrackingDevice
	findDeviceByUdid
	getAllDevices
	getDeploymentHisto
	getDeploymentHisto

getDeviceInfo

getDeviceInformationForUser

getDeviceProperties

getLastUser

getManagedStatus

getMasterKeyList

getSoftwareInventory

getStrongID

getUserDevices

isEnforceSSL

isEnforceStrongAuthentication

locateDevice

lockDevice

putDeviceProperties

registerDeviceForUser

removeDevice

resetDeploymentState

revoke

unlockDevice

wipeDevice

	addDevice
CiscoISE/NAC	action/pinlock
	/mdminfo
	/devices/0/all
	/devices/0/macaddress/
	/batchdevices/0/macaddress/all
OTPServices	browseOtp
	createOtp
	getAvailableEnrollmentModes
	getOtpInfo
	revokeOtp
	triggerNotification

XenMobile Mail Manager 10

Oct 17, 2016

XenMobile Mail Manager permet d'étendre 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 EAS sur un appareil mobile.
- 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/ou la réinitialisation du mot de passe (ResetPassword).

Pour télécharger XenMobile Mail Manager, consultez la section Server Components (Composants serveur) dans la rubrique XenMobile 10 Server sur Citrix.com.

Nouveautés dans XenMobile Mail Manager 10.1

Règles d'accès

La fenêtre Rule Analysis contient une case qui, lorsqu'elle est sélectionnée, affiche uniquement les conflits, remplacements, redondances ou compléments.

L'accès par défaut (Allow, Block ou Unchanged) et les modes de commande ActiveSync (PowerShell ou Simulation) sont définis séparément pour chaque environnement Microsoft Exchange configuré dans votre déploiement XenMobile.

Instantanés

Vous pouvez configurer le nombre maximal d'instantanés affichés dans l'historique des instantanés.

Vous pouvez configurer les erreurs à ignorer lors d'un instantané principal. Lorsqu'un instantané principal renvoie des erreurs qui ne sont pas configurées comme pouvant être ignorées, les résultats des instantanés sont ignorés.

Pour configurer des erreurs pouvant être ignorées, modifiez le fichier config.xml à l'aide d'un éditeur XML :

- Si le serveur Exchange Server est Office 365, accédez au nœud /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrors et ajoutez le texte représentant un élément enfant au même format que l'élément enfant Error existant. Les expressions régulières sont prises en charge.
- Si le serveur Exchange Server est local, accédez au nœud /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrors et ajoutez le texte représentant un élément enfant au même format que l'élément enfant Error existant. Les expressions régulières sont prises en charge.
- Si plusieurs environnements Exchange sont configurés, accédez au nœud /ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='ID correspondant au nœud Exchange environment']/ExchangeServer/Specialists/PowerShell souhaité. Ajoutez un nœud enfant IgnorableErrors au nœud PowerShell et pour chaque erreur à ignorer. Ajoutez un nœud enfant Error au nœud IgnorableErrors avec le texte correspondant contenu dans une section CDATA. Les expressions régulières sont prises en charge.

Enregistrez le fichier config.xml et redémarrez le service XenMobile Mail Manager.

PowerShell et Exchange

XenMobile Mail Manager détermine maintenant de manière dynamique les applets de commande à utiliser en fonction de la version d'Exchange à laquelle il est connecté. À titre d'exemple, il utilise Get-ActiveSyncDevice pour Exchange 2010 mais Get-MobileDevice pour

Exchange 2013 et Exchange 2016.

Configuration d'Exchange

Les configurations d'Exchange Server peuvent être modifiées et mises à jour sans redémarrer le service XenMobile Mail Manager.

Deux nouvelles colonnes ajoutées à l'onglet de synthèse de l'environnement Exchange affichent le mode de commande (PowerShell ou Simulation) de chaque environnement et le mode d'accès (Allow, Block ou Unchanged).

Dépannage et diagnostics

Des utilitaires PowerShell destinés au dépannage sont disponibles dans le dossier Support\PowerShell.

Le test de la connectivité au service Exchange à l'aide du bouton Test Connectivity disponible dans la fenêtre Configuration de la console exécute chaque applet de commande en lecture seule utilisée par le service, exécute des tests des autorisations RBAC sur le serveur Exchange Server pour l'utilisateur configuré, et affiche les erreurs ou avertissements à l'aide de couleurs (bleu-jaune pour les avertissements, rouge-orange pour les erreurs).

Un nouvel 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.

Dans les scénarios de support, toutes les propriétés de toutes les boîtes aux lettres sur tous les appareils gérés par XenMobile Mail Manager peuvent être enregistrées en sélectionnant une case à cocher de diagnostic dans la console.

La journalisation des traces est maintenant prise en charge dans les scénarios de support.

Authentification

XenMobile Mail Manager prend en charge l'authentification de base pour les déploiements locaux. Cela permet à XenMobile Mail Manager d'être utilisé lorsque le serveur XenMobile Mail Manager n'est pas membre du domaine dans lequel le serveur Exchange Server réside.

Problèmes résolus

Règles d'accès

XenMobile Mail Manager applique des règles de contrôle d'accès local à tous les utilisateurs des groupes Active Directory (AD), même si un groupe AD contient plus de 1000 utilisateurs. Précédemment, XenMobile Mail Manager appliquait des règles de contrôle d'accès local uniquement aux premiers 1000 utilisateurs d'un groupe AD. [#548705]

Il arrive parfois que la console XenMobile Mail Manager ne réponde pas lors de l'interrogation de groupes Active Directory contenant 1000 utilisateurs ou plus. [CXM-11729]

La fenêtre LDAP Configuration n'affiche plus un mode d'authentification incorrect. [CXM-5556]

Instantanés

Les noms d'utilisateurs contenant des apostrophes n'entraînent pus l'échec des instantanés secondaires. [#617549]

Dans les scénarios de support dans lesquels le pipelining est désactivé (l'option Disable Pipelining est sélectionnée dans la fenêtre Configuration de la console XenMobile Mail Manager), les instantanés principaux n'échouent plus dans les environnements Exchange locaux. [#586083]

Dans les scénarios de support dans lesquels le pipelining est désactivé (l'option Disable Pipelining est sélectionnée dans la fenêtre Configuration de la console XenMobile Mail Manager), les données des instantanés complets ne sont plus collectées, que l'environnement ait été configuré pour des instantanés complets (deep) ou superficiels (shallow). Désormais, les données des instantanés complets sont

collectées uniquement lorsque l'environnement est configuré pour des instantanés complets. [#586092]

Le premier instantané principal après l'installation initiale rencontrait parfois une erreur qui empêchait XenMobile Mail Manager d'exécuter un autre instantané principal tant que le service XenMobile Mail Manager n'était pas redémarré. Cela ne se produit plus. [CXM-5536]

À propos de XenMobile Mail Manager 10

À propos de XenMobile Mail Manager 10.1

Oct 17, 2016

Les fonctionnalités suivantes sont nouvelles dans XenMobile Mail Manager 10.1 :

Règles d'accès

La fenêtre Rule Analysis contient une case qui, lorsqu'elle est sélectionnée, affiche uniquement les conflits, remplacements, redondances ou compléments.

L'accès par défaut (Allow, Block ou Unchanged) et les modes de commande ActiveSync (PowerShell ou Simulation) sont définis séparément pour chaque environnement Microsoft Exchange configuré dans votre déploiement XenMobile.

Instantanés

Vous pouvez configurer le nombre maximal d'instantanés affichés dans l'historique des instantanés.

Vous pouvez configurer les erreurs à ignorer lors d'un instantané principal. Lorsqu'un instantané principal renvoie des erreurs qui ne sont pas configurées comme pouvant être ignorées, les résultats des instantanés sont ignorés.

Pour configurer des erreurs pouvant être ignorées, modifiez le fichier config.xml à l'aide d'un éditeur XML :

- Si le serveur Exchange Server est Office 365, accédez au nœud /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrors et ajoutez le texte représentant un élément enfant au même format que l'élément enfant Error existant. Les expressions régulières sont prises en charge. Passez à l'étape 7.
- Si le serveur Exchange Server est local, accédez au nœud /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrors et ajoutez le texte représentant un élément enfant au même format que l'élément enfant Error existant. Les expressions régulières sont prises en charge. Passez à l'étape 7.
- Si plusieurs environnements Exchange sont configurés, accédez au nœud /ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='ID correspondant au nœud Exchange environment']/ExchangeServer/Specialists/PowerShell souhaité. Ajoutez un nœud enfant IgnorableErrors au nœud PowerShell et pour chaque erreur à ignorer, ajoutez un nœud enfant Error au nœud IgnorableErrors avec le texte correspondant contenu dans une section CDATA. Les expressions régulières sont prises en charge.

Enregistrez le fichier config.xml et redémarrez le service XenMobile Mail Manager.

PowerShell et Exchange

XenMobile Mail Manager détermine maintenant de manière dynamique les applets de commande à utiliser en fonction de la version d'Exchange à laquelle il est connecté. À titre d'exemple, il utilise **Get-ActiveSyncDevice** pour Exchange 2010 mais **Get-MobileDevice** pour Exchange 2013 et Exchange 2016.

Configuration d'Exchange

Les configurations d'Exchange Server peuvent être modifiées et mises à jour sans redémarrer le service XenMobile Mail Manager.

Deux nouvelles colonnes ajoutées à l'onglet de synthèse de l'environnement Exchange affichent le mode de commande (PowerShell ou Simulation) de chaque environnement et le mode d'accès (Allow, Block ou Unchanged).

Dépannage et diagnostics

Des utilitaires PowerShell destinés au dépannage sont disponibles dans le dossier Support\PowerShell.

Le test de la connectivité au service Exchange à l'aide du bouton **Test Connectivity** disponible dans la fenêtre Configuration de la

console exécute chaque applet de commande en **lecture seule** utilisée par le service, exécute des tests des autorisations RBAC sur le serveur Exchange Server pour l'utilisateur configuré, et affiche les erreurs ou avertissements à l'aide de couleurs (bleu-jaune pour les avertissements, rouge-orange pour les erreurs).

Un nouvel 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.

Dans les scénarios de support, toutes les propriétés de toutes les boîtes aux lettres sur tous les appareils gérés par XenMobile Mail Manager peuvent être enregistrées en sélectionnant une case à cocher de diagnostic dans la console.

La journalisation des traces est maintenant prise en charge dans les scénarios de support.

Authentification

XenMobile Mail Manager prend en charge l'authentification de base pour les déploiements locaux. Cela permet à XenMobile Mail Manager d'être utilisé lorsque le serveur XenMobile Mail Manager n'est pas membre du domaine dans lequel le serveur Exchange Server réside.

Problèmes résolus

Règles d'accès

XenMobile Mail Manager applique des règles de contrôle d'accès local à tous les utilisateurs des groupes Active Directory, même si un groupe Active Directory contient plus de 1 000 utilisateurs. Précédemment, XenMobile Mail Manager appliquait des règles de contrôle d'accès local uniquement aux premiers 1 000 utilisateurs d'un groupe Active Directory. [#548705]

Il arrive parfois que la console XenMobile Mail Manager ne réponde pas lors de l'interrogation de groupes Active Directory contenant 1 000 utilisateurs ou plus. [CXM-11729]

La fenêtre LDAP Configuration n'affiche plus un mode d'authentification incorrect. [CXM-5556]

Instantanés

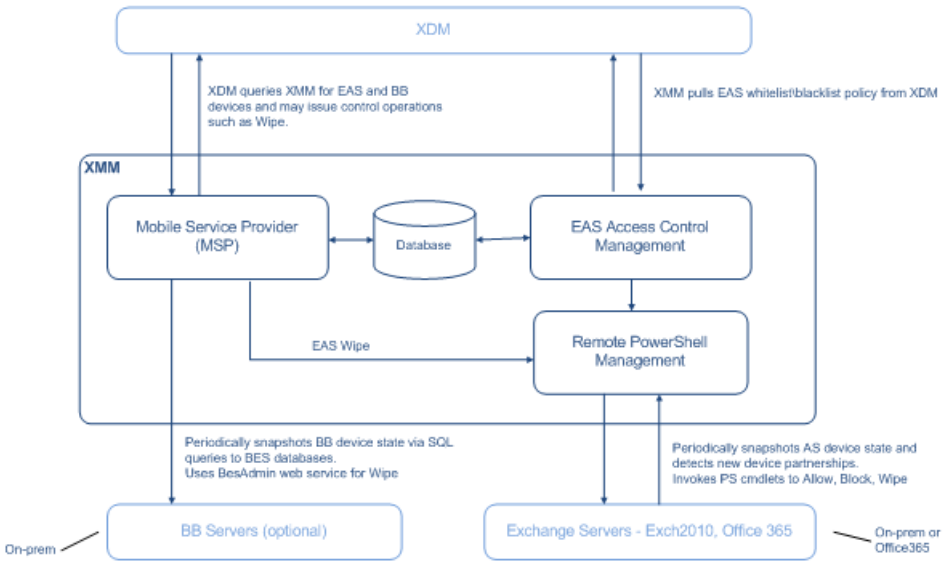
Les noms d'utilisateurs contenant des apostrophes n'entraînent pus l'échec des instantanés secondaires. [#617549]

Dans les scénarios de support dans lesquels le pipelining est désactivé (l'option **Disable Pipelining** est sélectionnée dans la fenêtre Configuration de la console XenMobile Mail Manager), les instantanés principaux n'échouent plus dans les environnements Exchange locaux. [#586083]

Dans les scénarios de support dans lesquels le pipelining est désactivé (l'option **Disable Pipelining** est sélectionnée dans la fenêtre Configuration de la console XenMobile Mail Manager), les données des instantanés complets ne sont plus collectées, que l'environnement ait été configuré pour des instantanés complets (deep) ou superficiels (shallow). Désormais, les données des instantanés complets sont collectées uniquement lorsque l'environnement est configuré pour des instantanés complets. [#586092]

Le premier instantané principal après l'installation initiale rencontrait parfois une erreur qui empêchait XenMobile Mail Manager d'exécuter un autre instantané principal tant que le service XenMobile Mail Manager n'était pas redémarré. Cela ne se produit plus. [CXM-5536]

-
-
-



-
-
-

Autorisations. 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

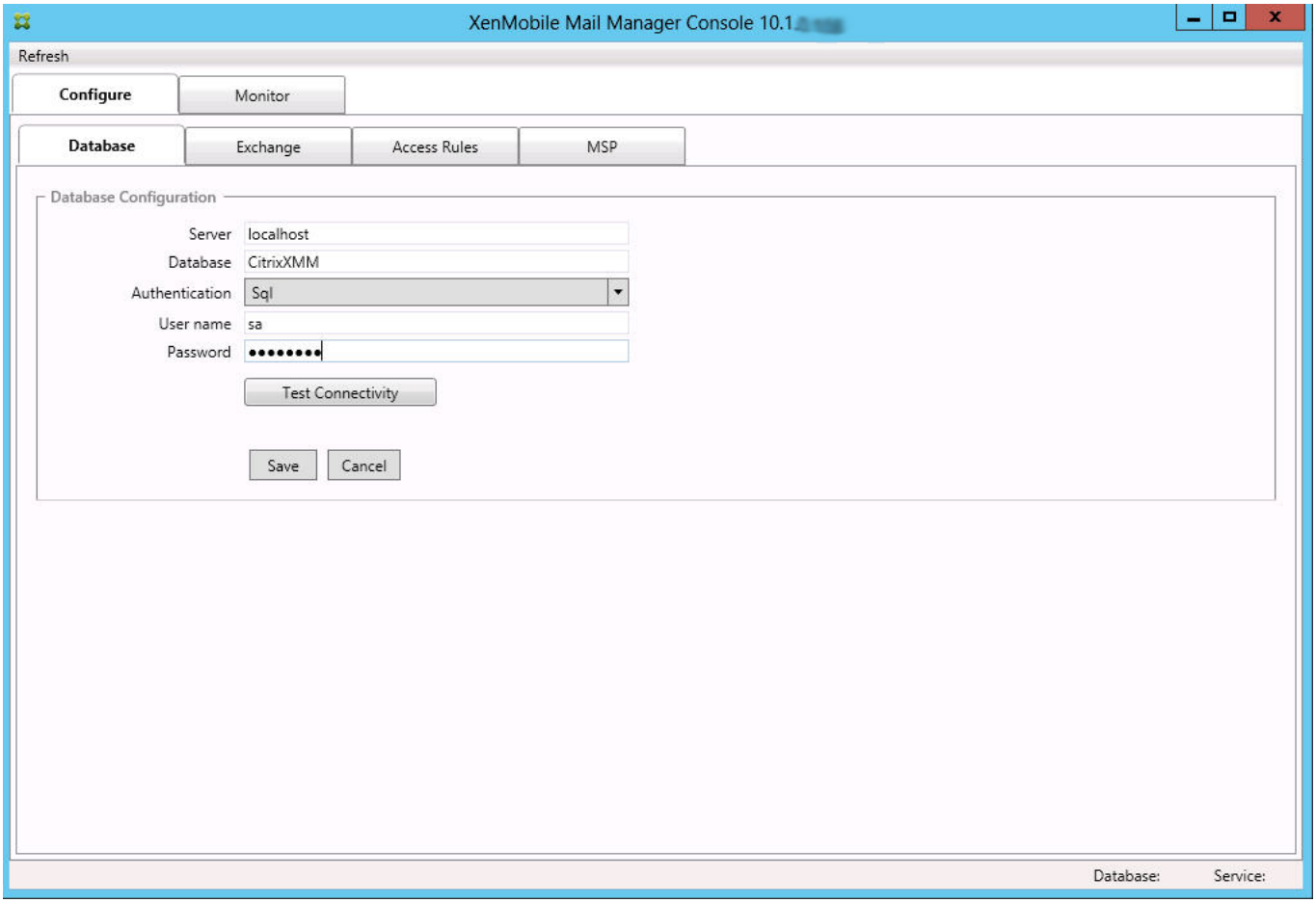
  - Get-ManagementRole
  - Get-ManagementRoleAssignment

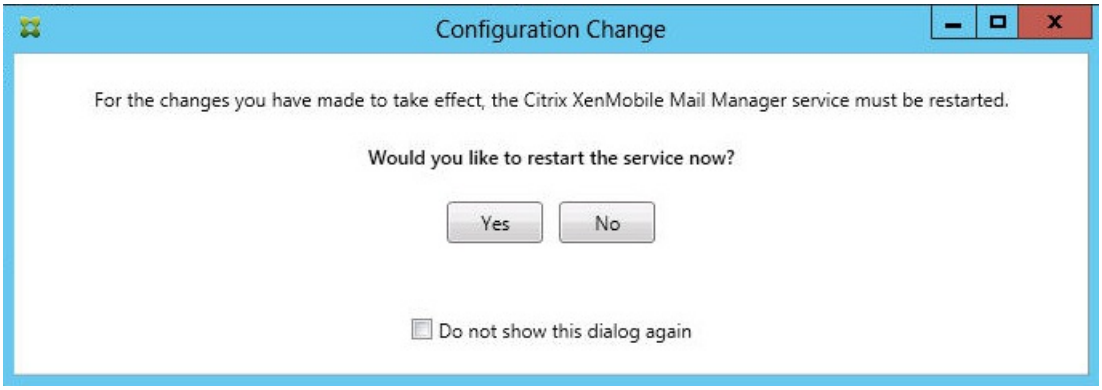
- Si XenMobile Mail Manager est configuré pour afficher l'ensemble de la forêt, l'autorisation doit avoir été accordée pour exécuter : Set-AdServerSettings -ViewEntireForest $true
- Les informations d'identification fournies doivent avoir été autorisées à se connecter au serveur Exchange Server via le Shell distant. Par défaut, l'utilisateur qui a installé Exchange possède ce droit.
- Conformément à l'article Microsoft TechNet about_Remote_Requirements, 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. Conformément à ce billet de blog, You Don't Have to Be An Administrator to Run Remote PowerShell Commands, Set-PSSessionConfiguration peut être utilisé pour éliminer les exigences d'administration, mais le support et les discussions spécifiques à cette commande sont hors de portée de ce document.
- 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 d'entre elles 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. Une fois la limite de connexion atteinte, XenMobile Mail Manager ne sera plus en mesure de 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.

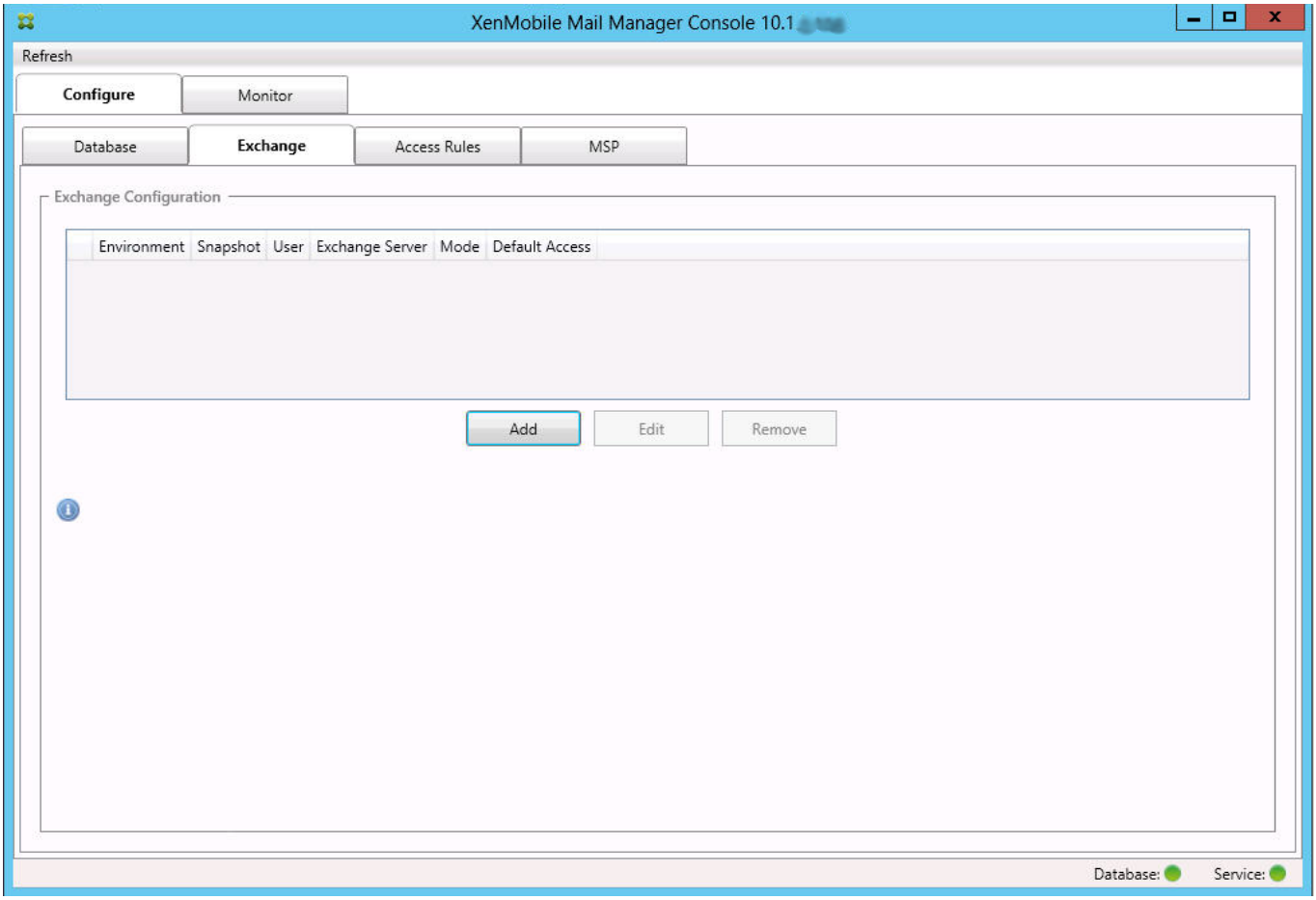
Configuration requise pour Office 365 Exchange

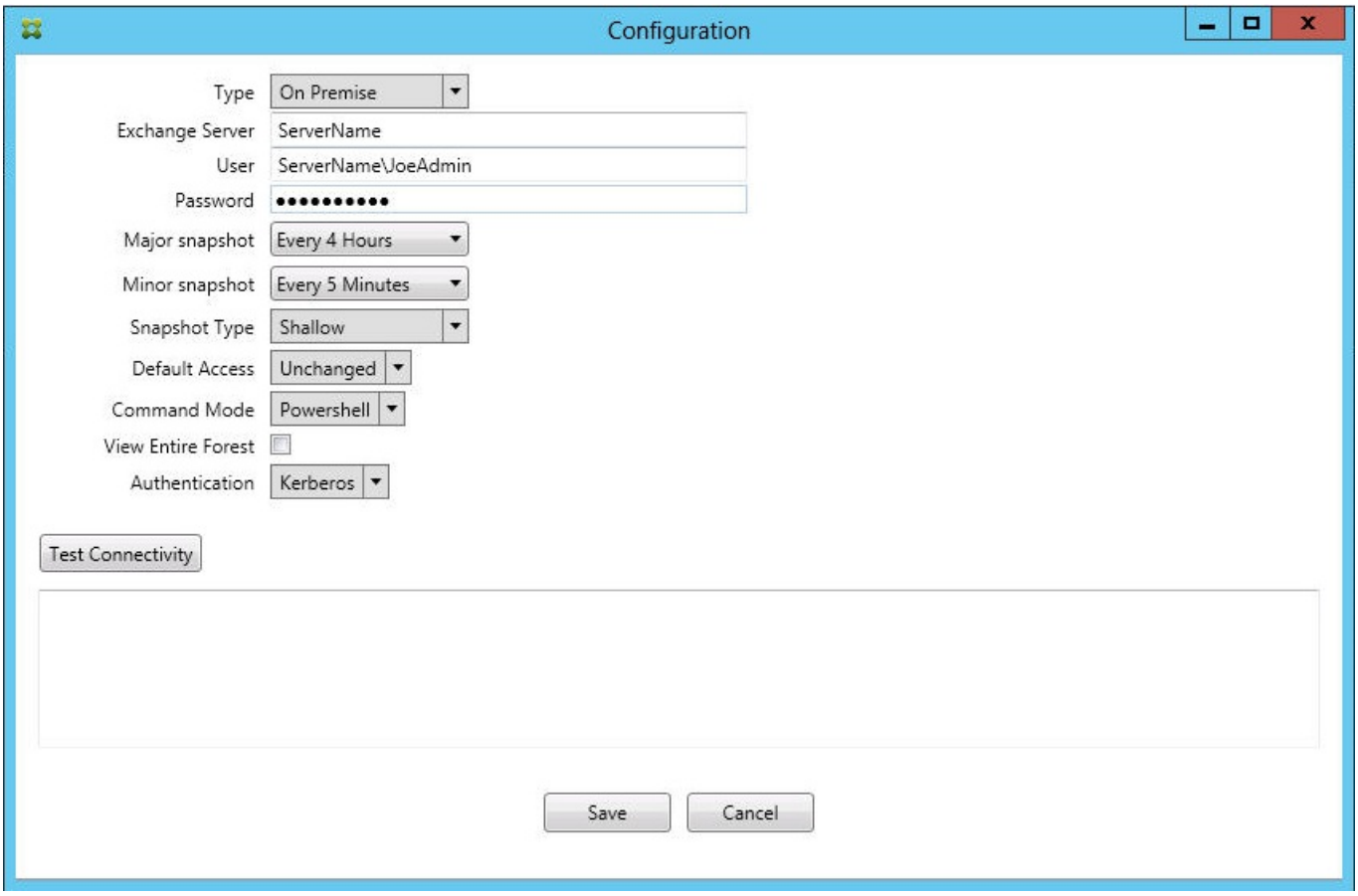
- **Autorisations**. Les informations d'identification spécifiées dans l'interface utilisateur de la console Exchange Configuration doivent être en mesure de se connecter à Office 365 et bénéficier d'un accès complet pour exécuter les applets de commande PowerShell spécifiques à Exchange suivantes :
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- Les informations d'identification fournies doit avoir été autorisées à se connecter au serveur Office 365 via le Shell distant. Par défaut, l'administrateur en ligne d'Office 365 possède les privilèges requis.
- Exchange possède de nombreuses stratégies de limitation. L'une d'entre elles contrôle combien de connexions PowerShell simultanées sont autorisées par utilisateur. Par défaut, le nombre de connexions simultanées autorisées pour un utilisateur est de 3 sur Office 365. Une fois la limite de connexion atteinte, XenMobile Mail Manager ne sera plus en mesure de 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.

-
-

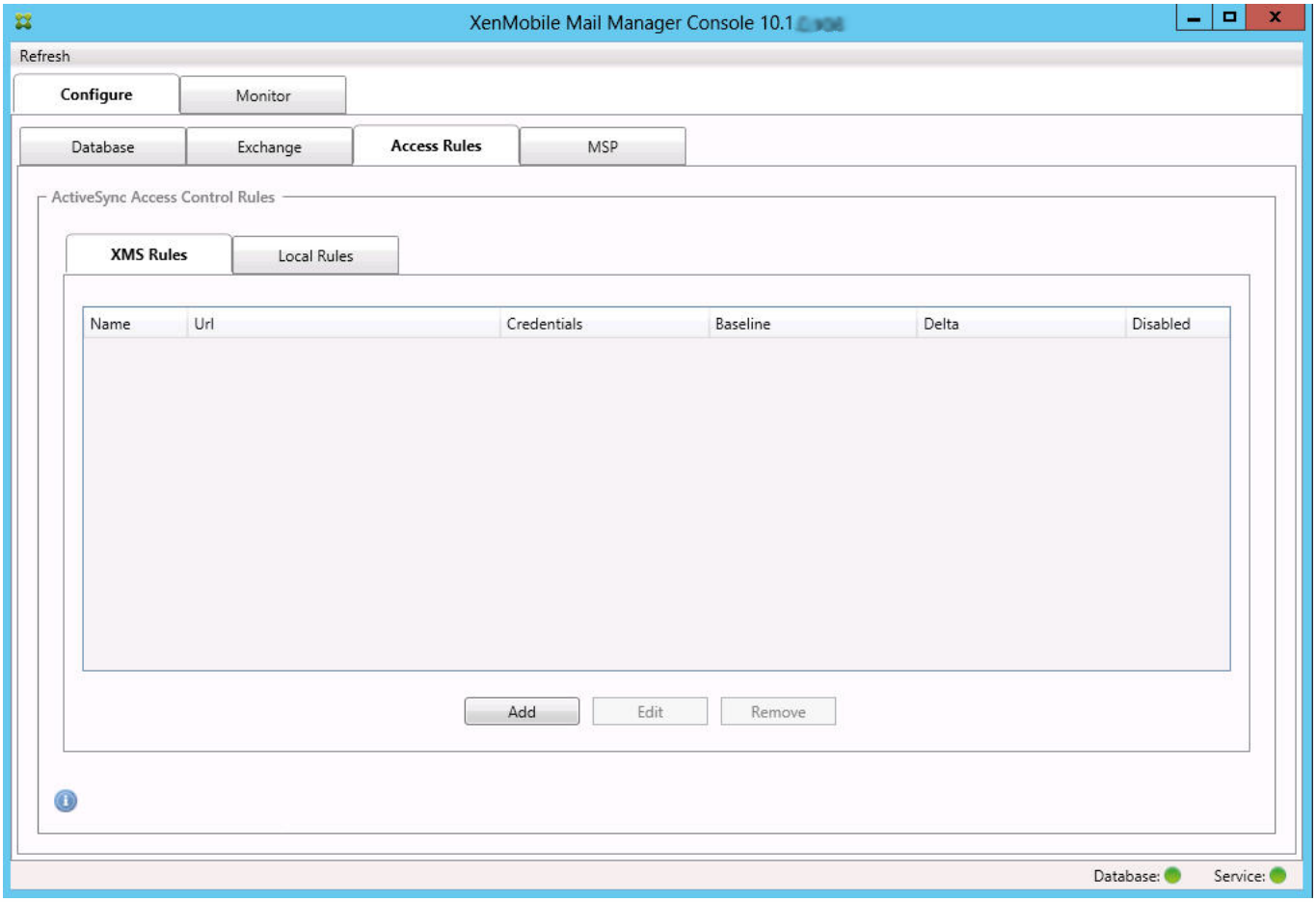


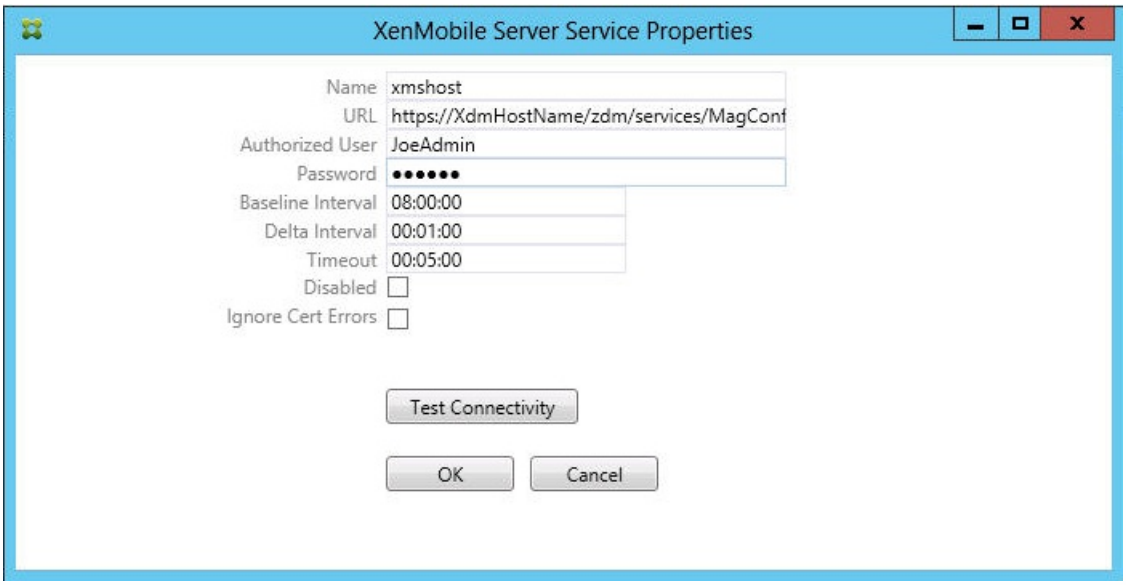


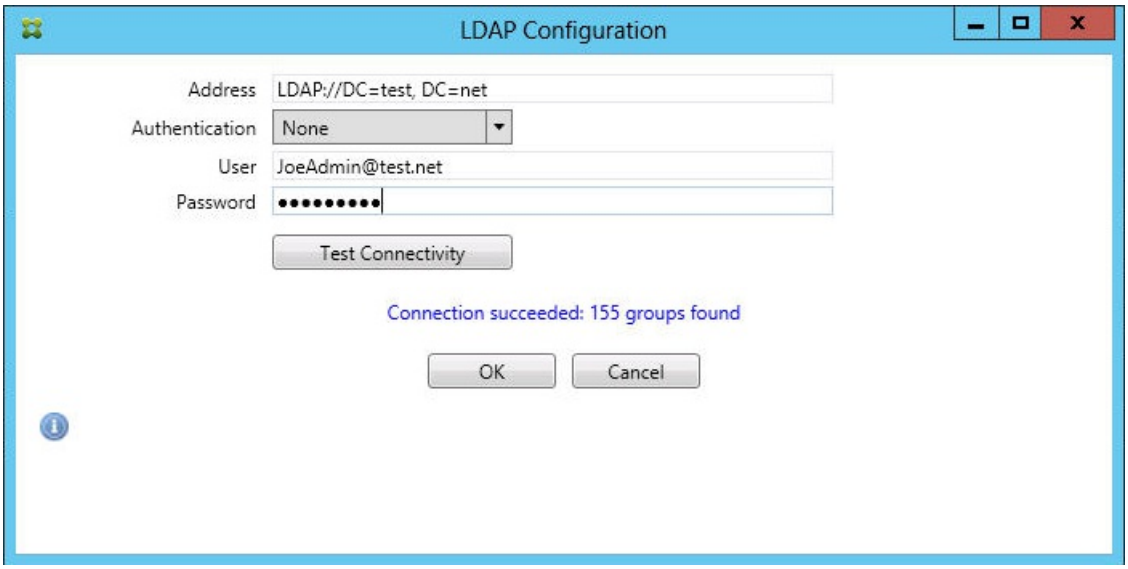


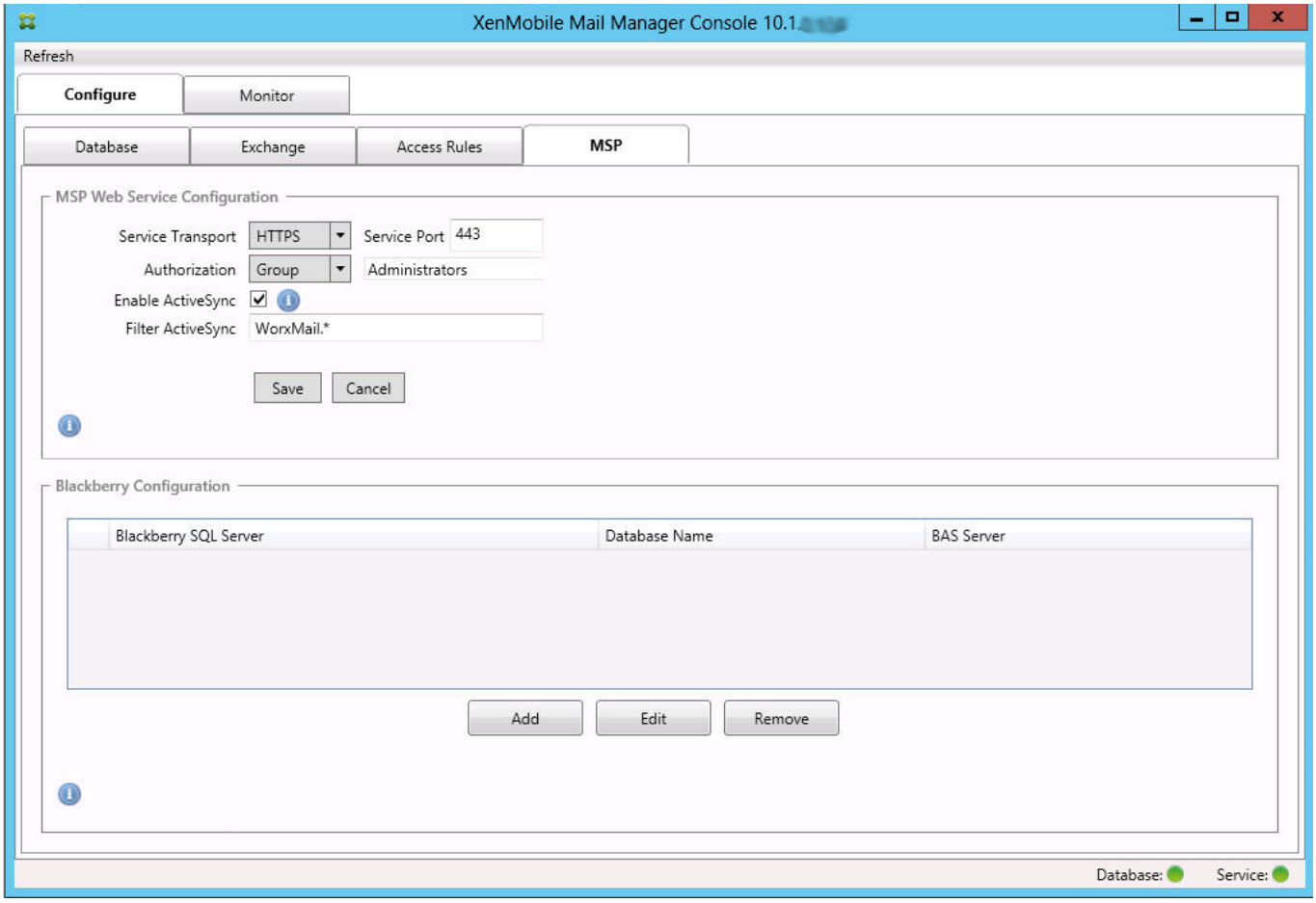


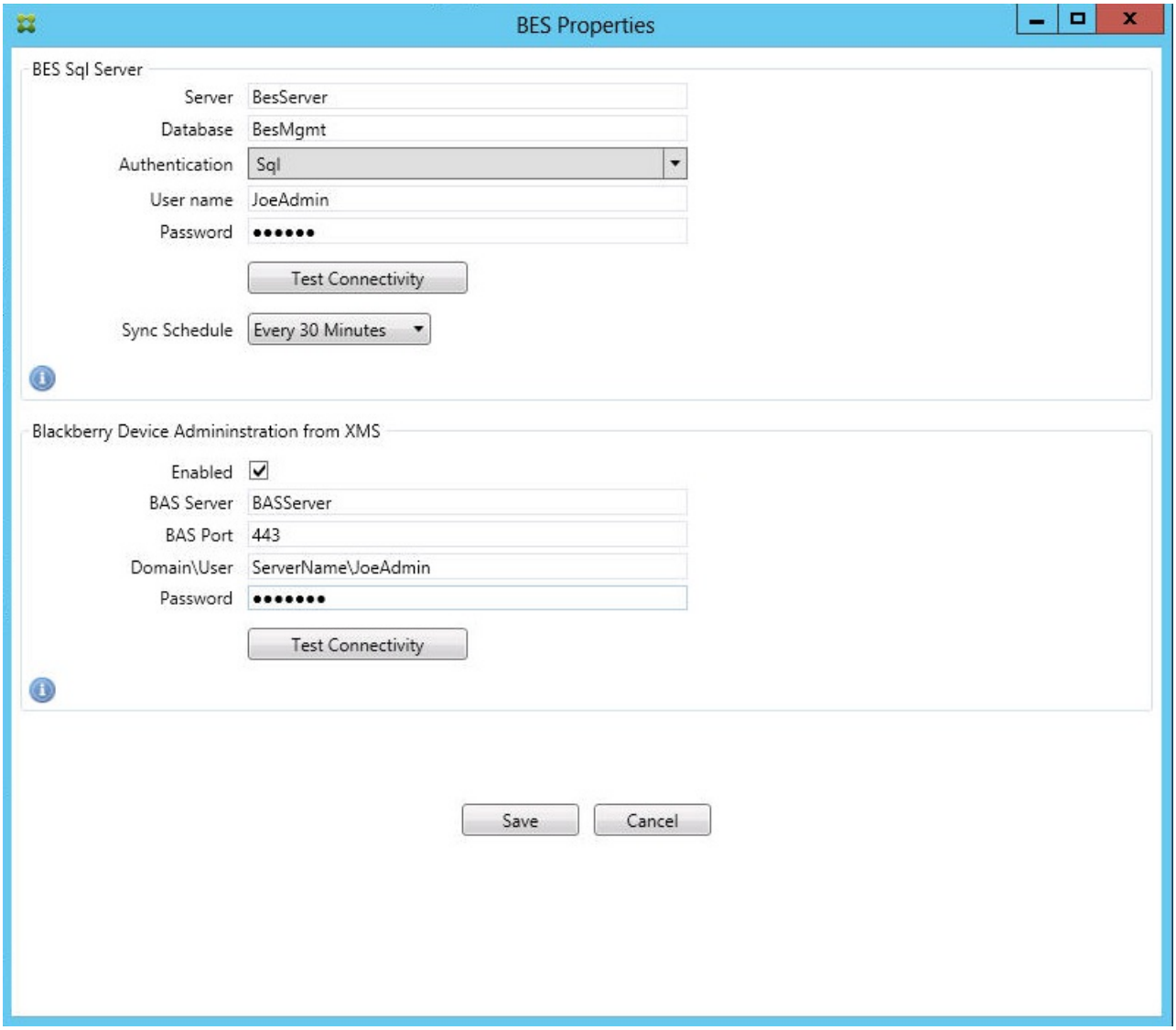
-
-

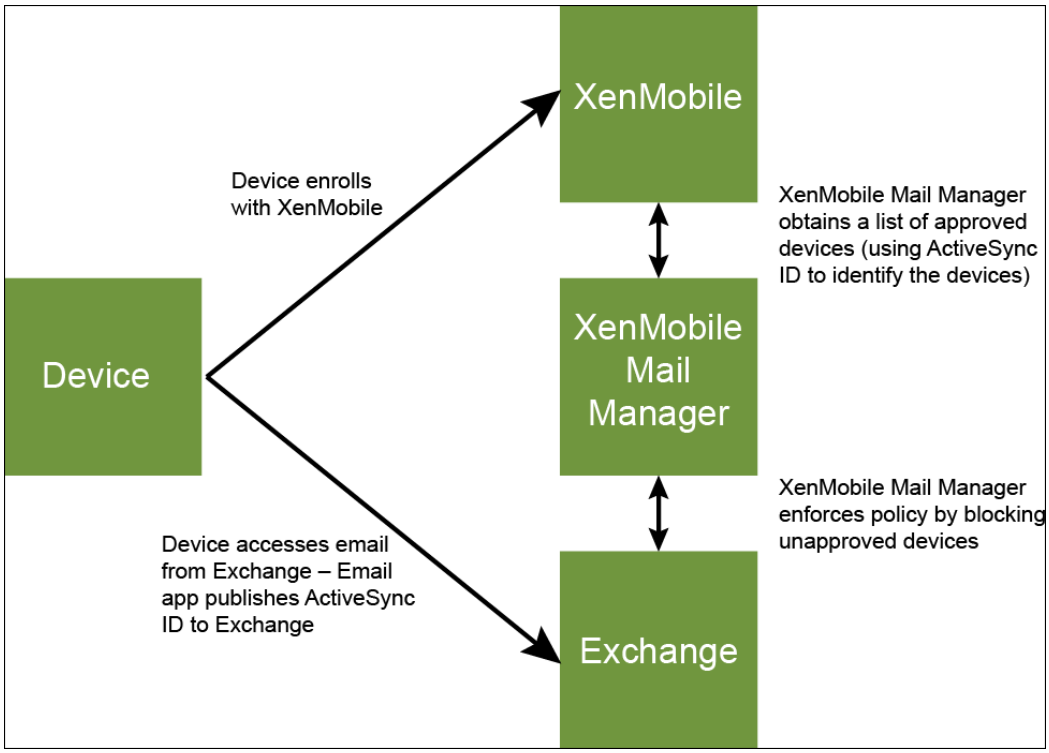










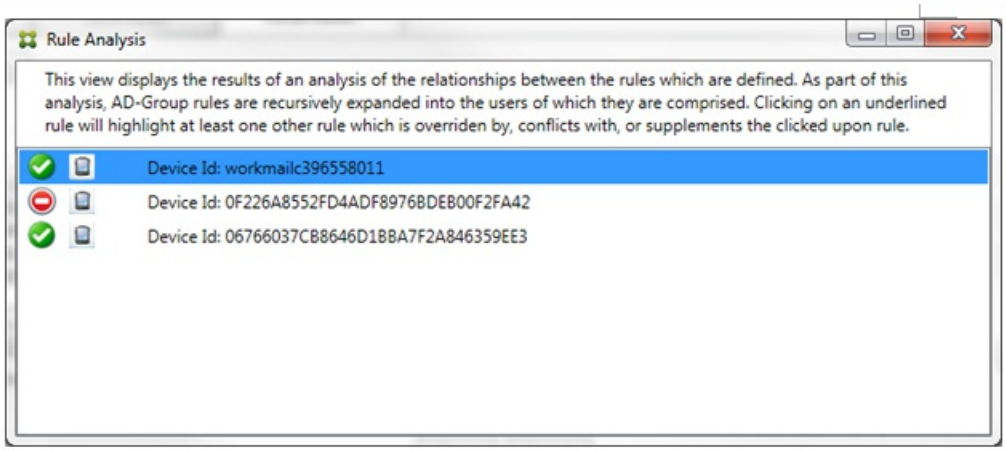


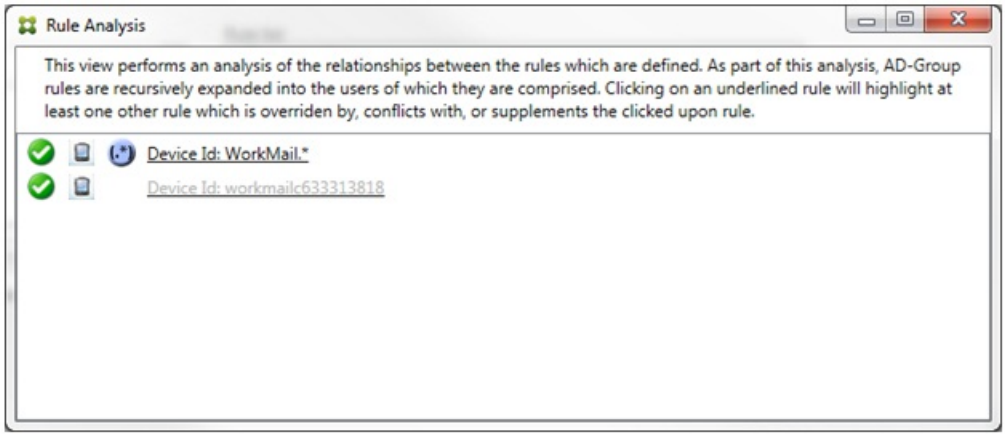
-
-

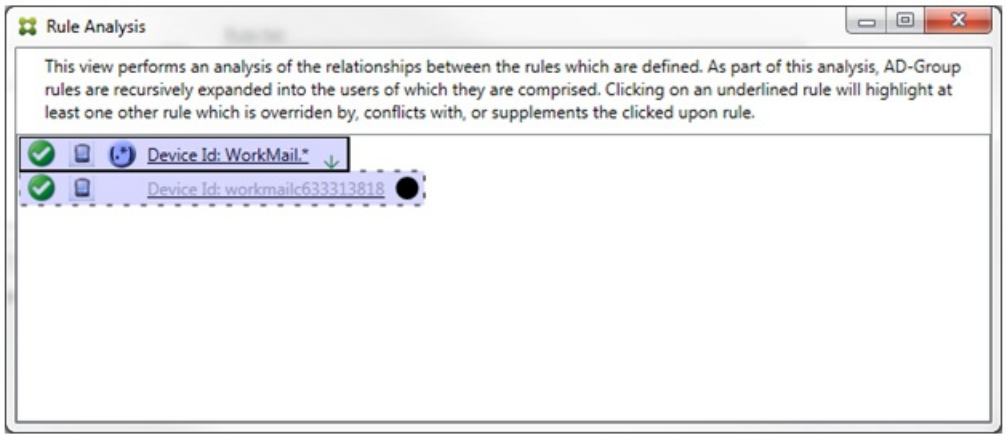
-
-
-
-

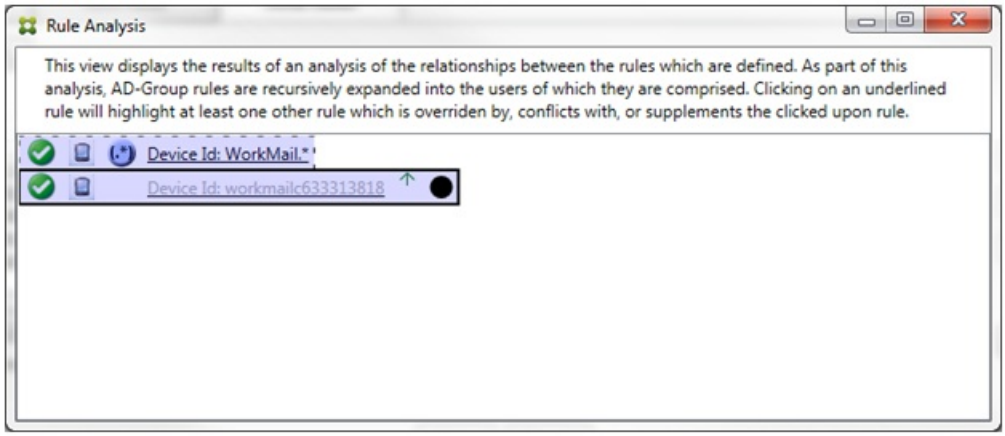
-
-
-
-
-
-
-

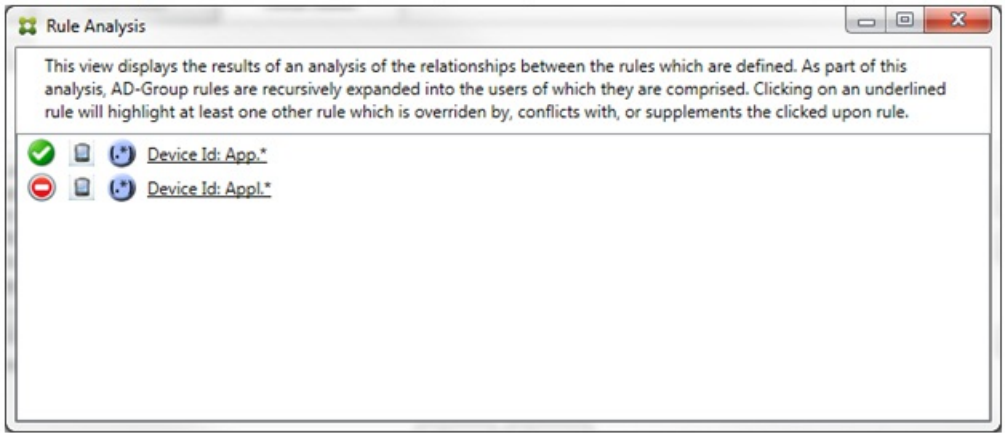
-
-
-
-

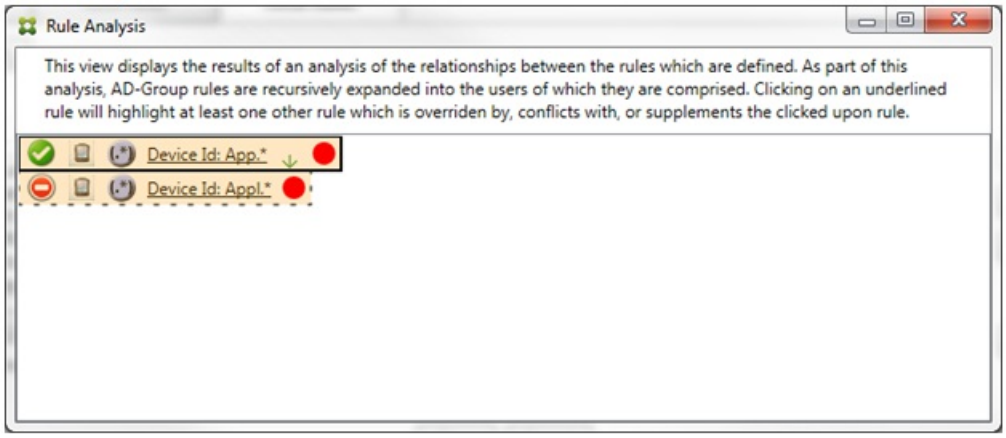


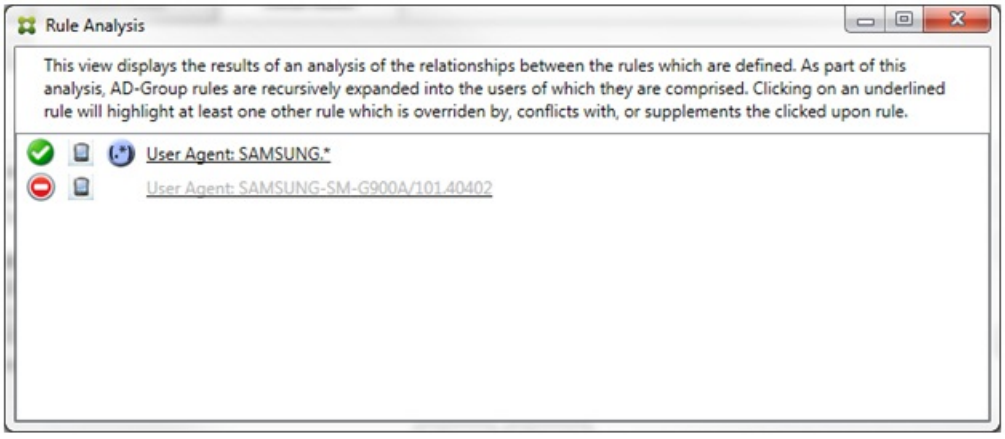


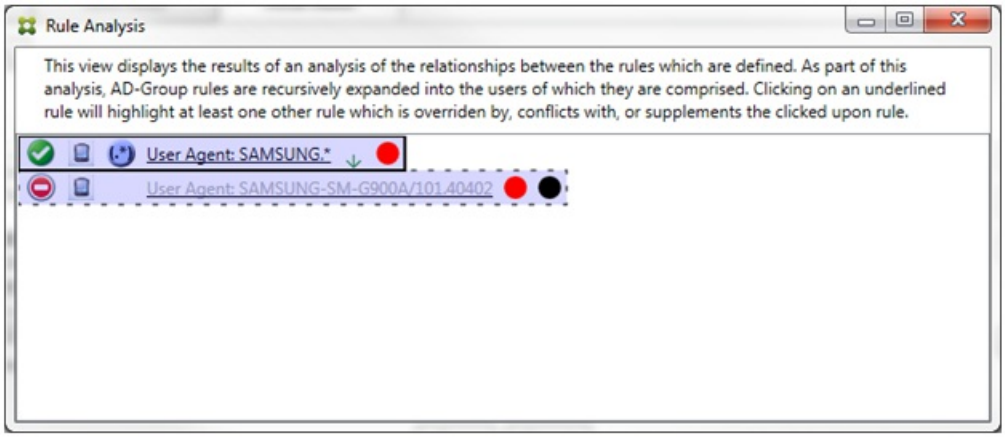


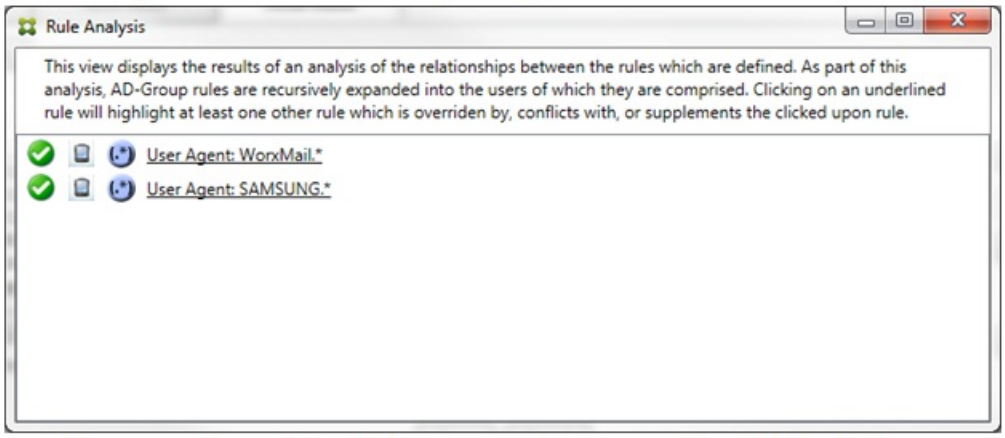


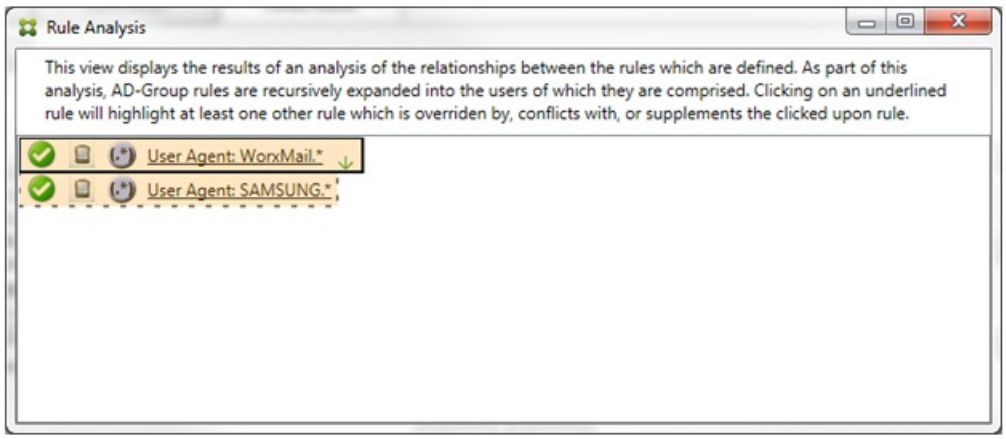


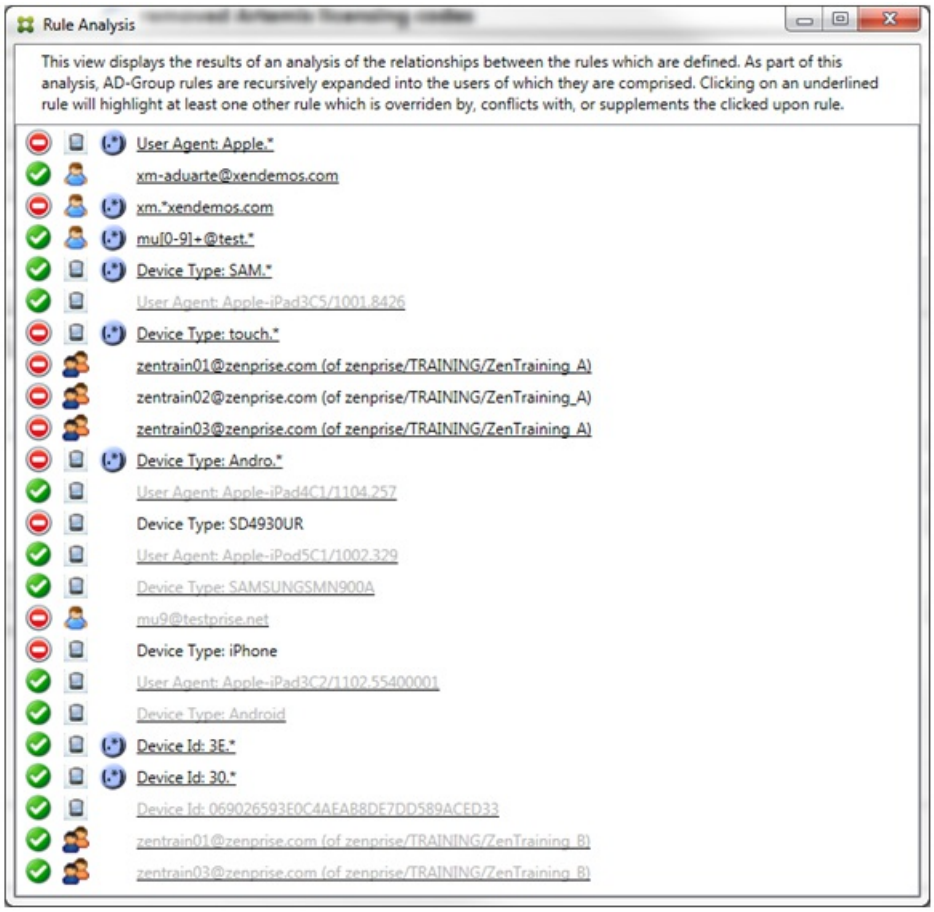


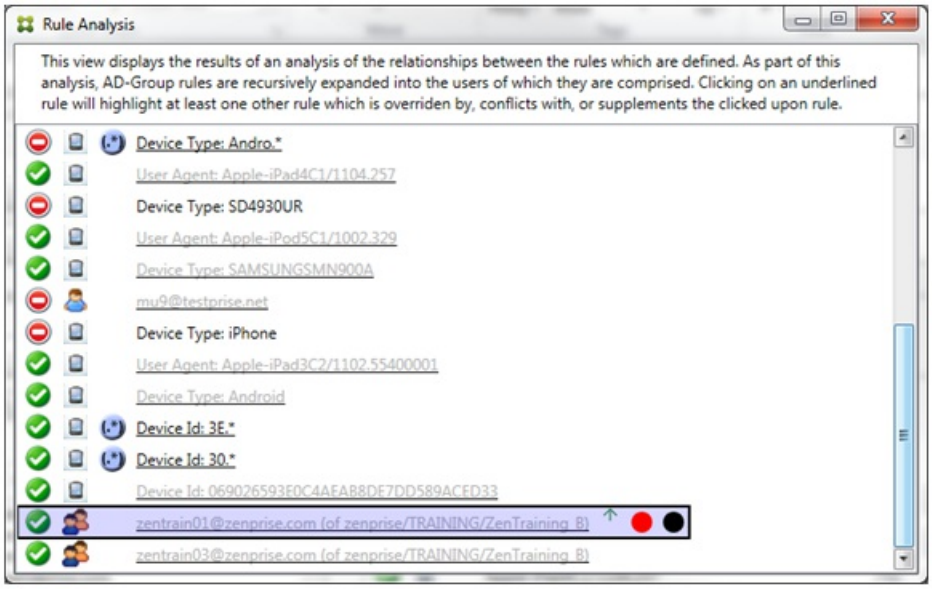




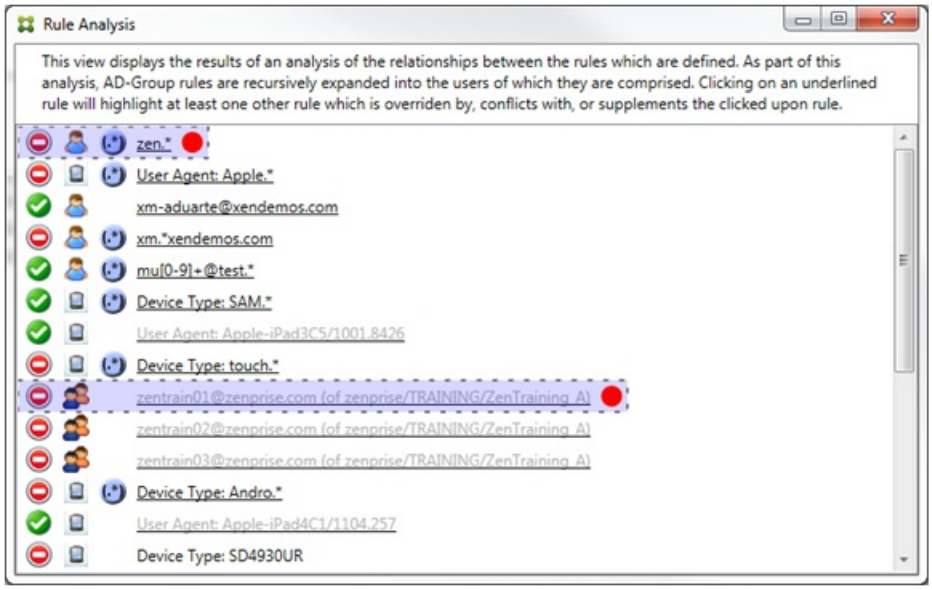


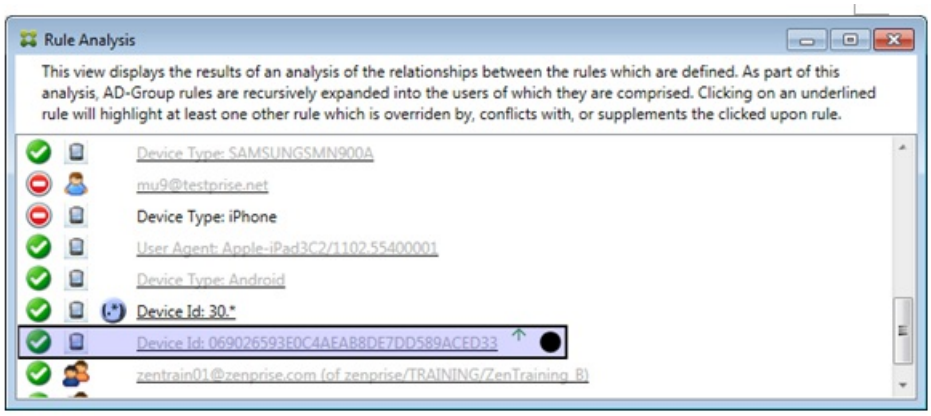




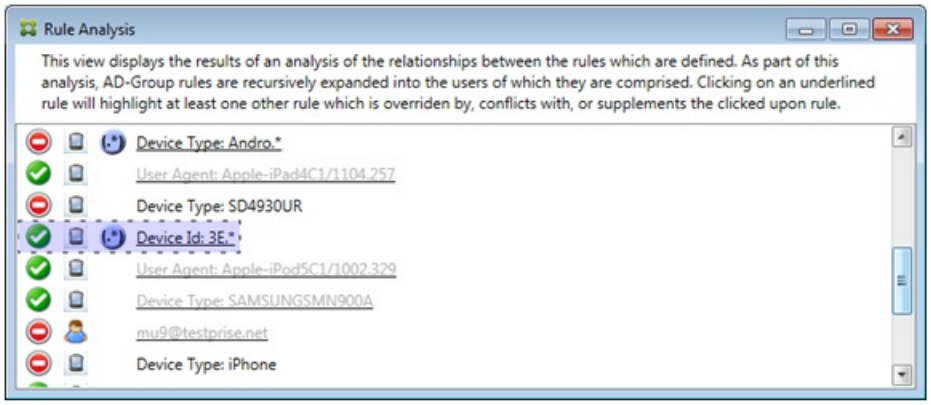


-
-
-



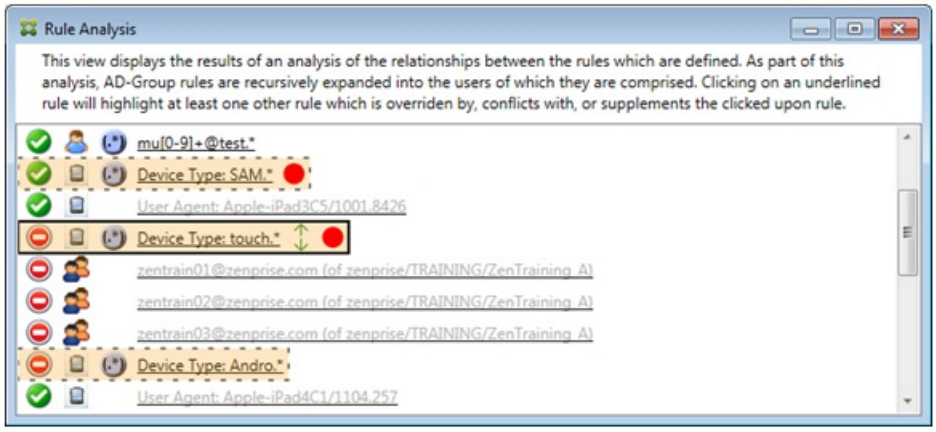


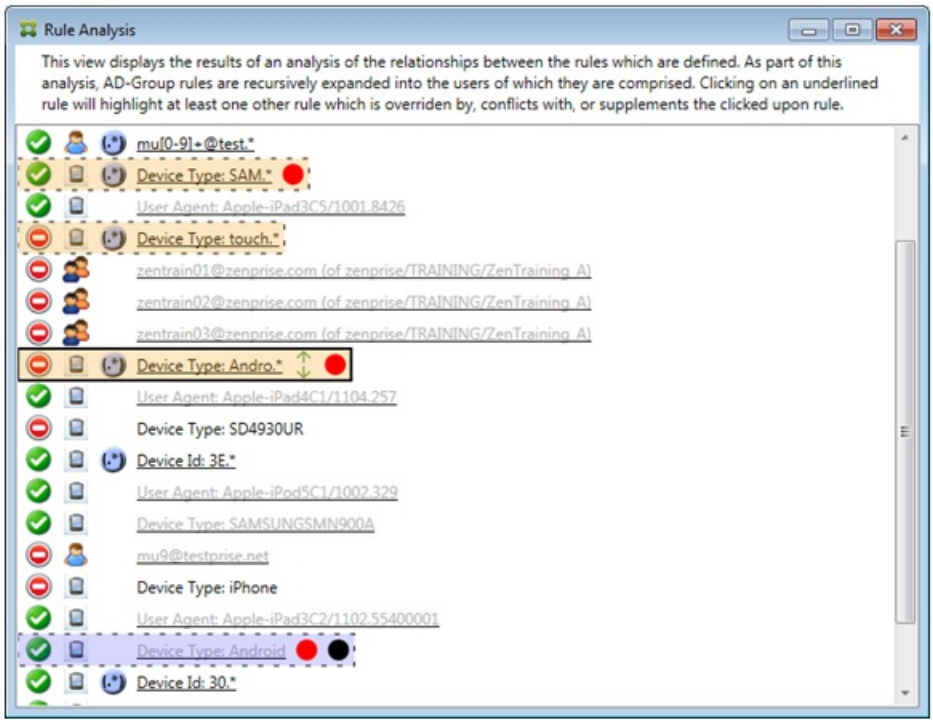
-
-
-

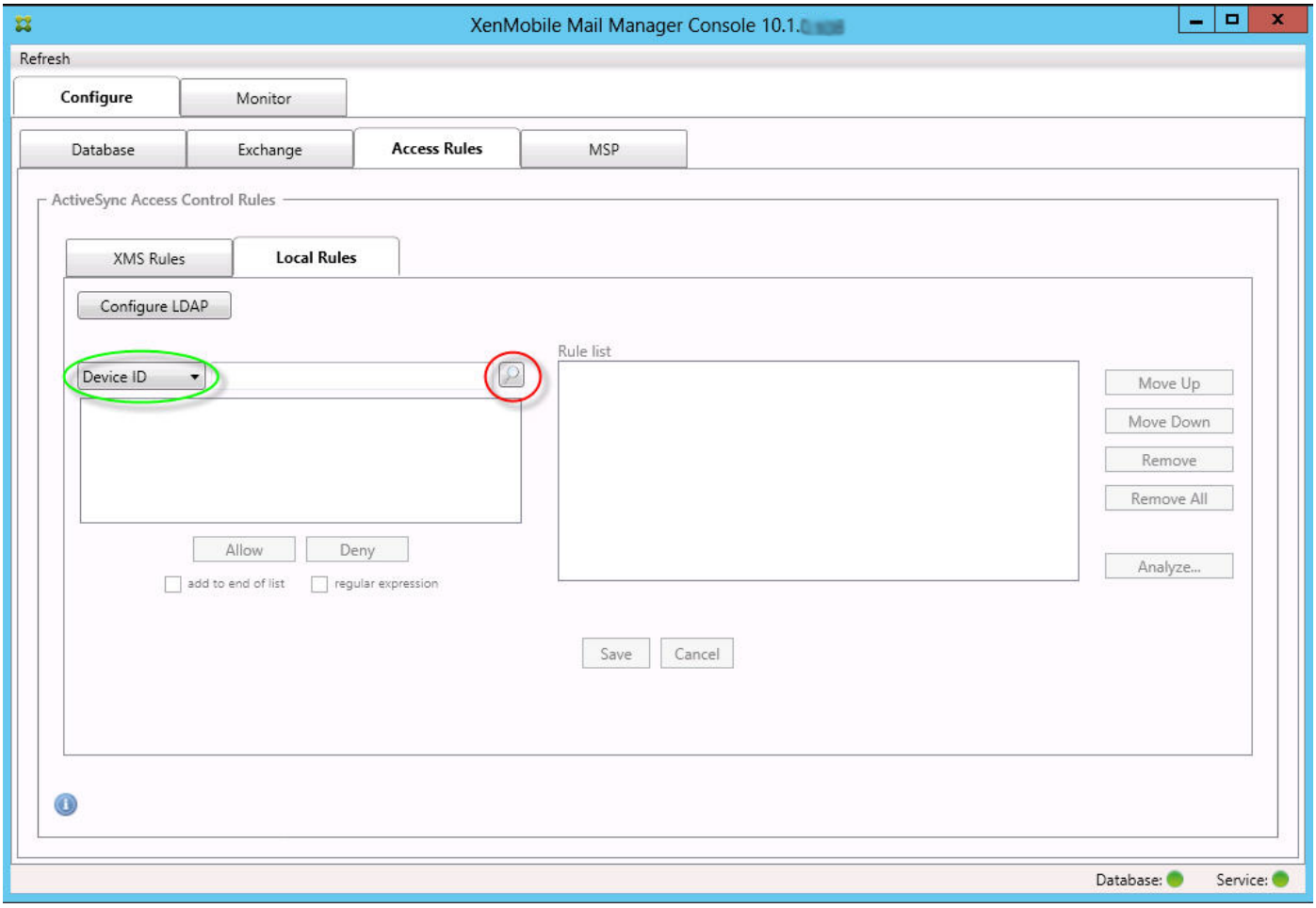


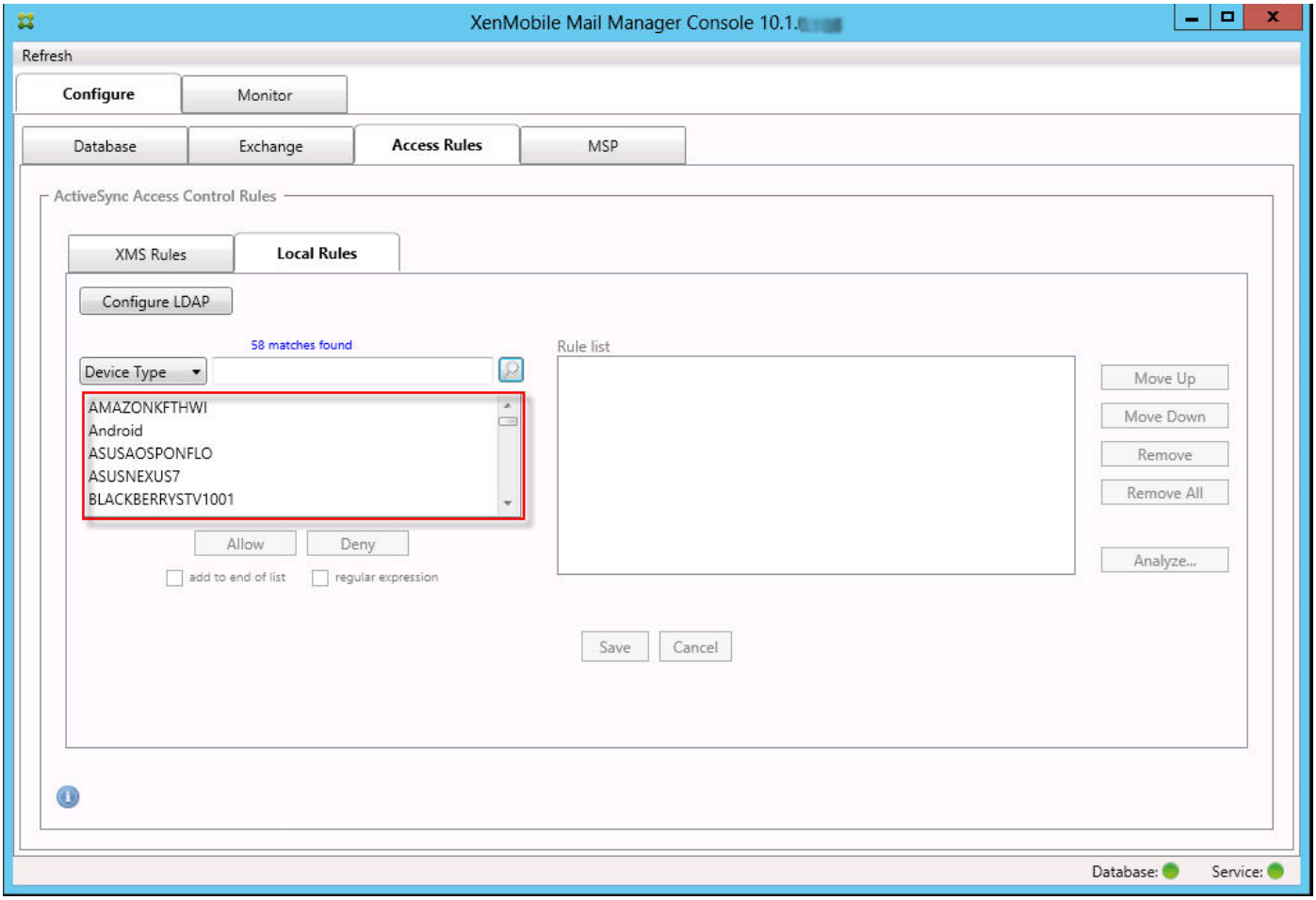
-
-

-
-
-
-
-

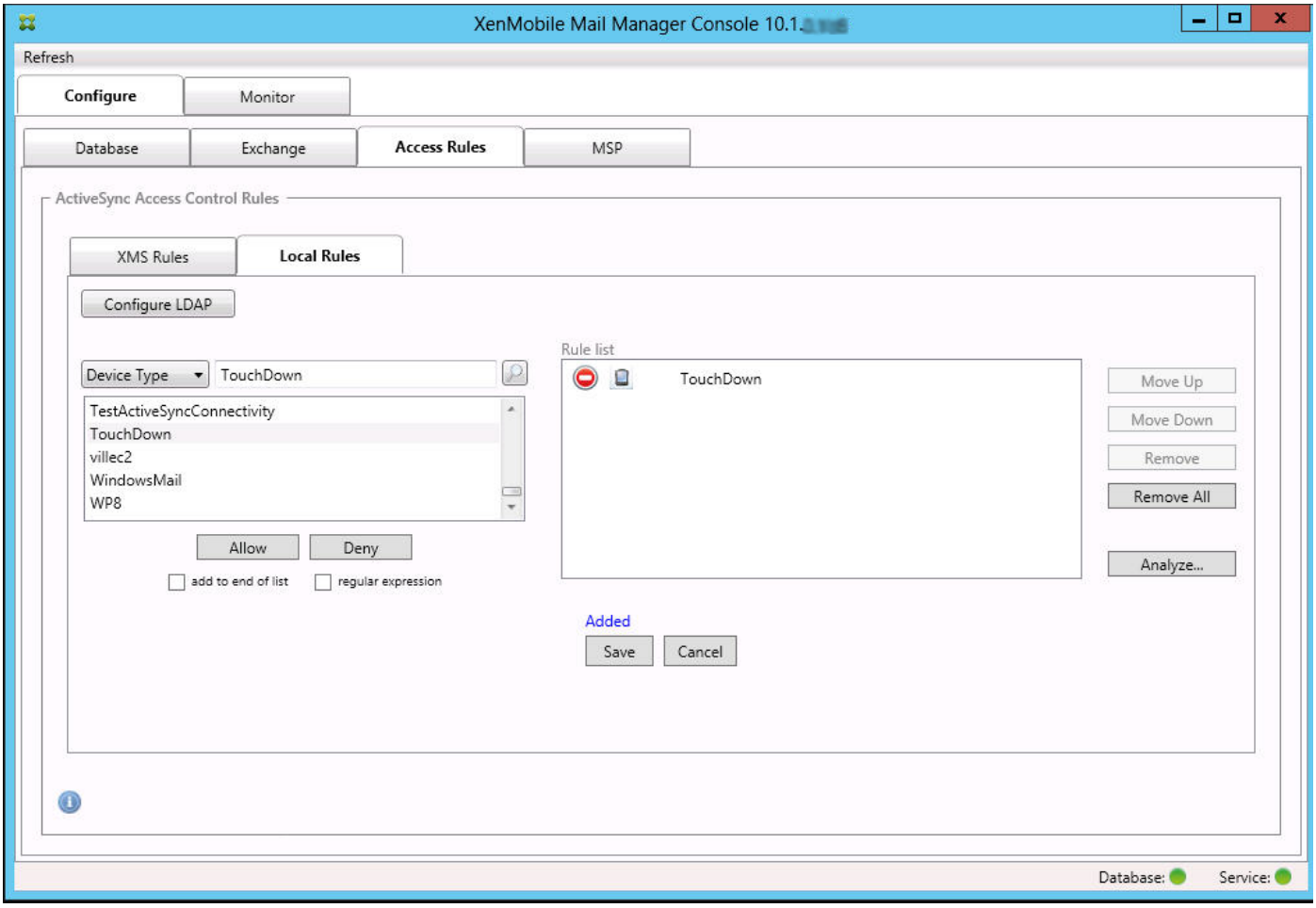


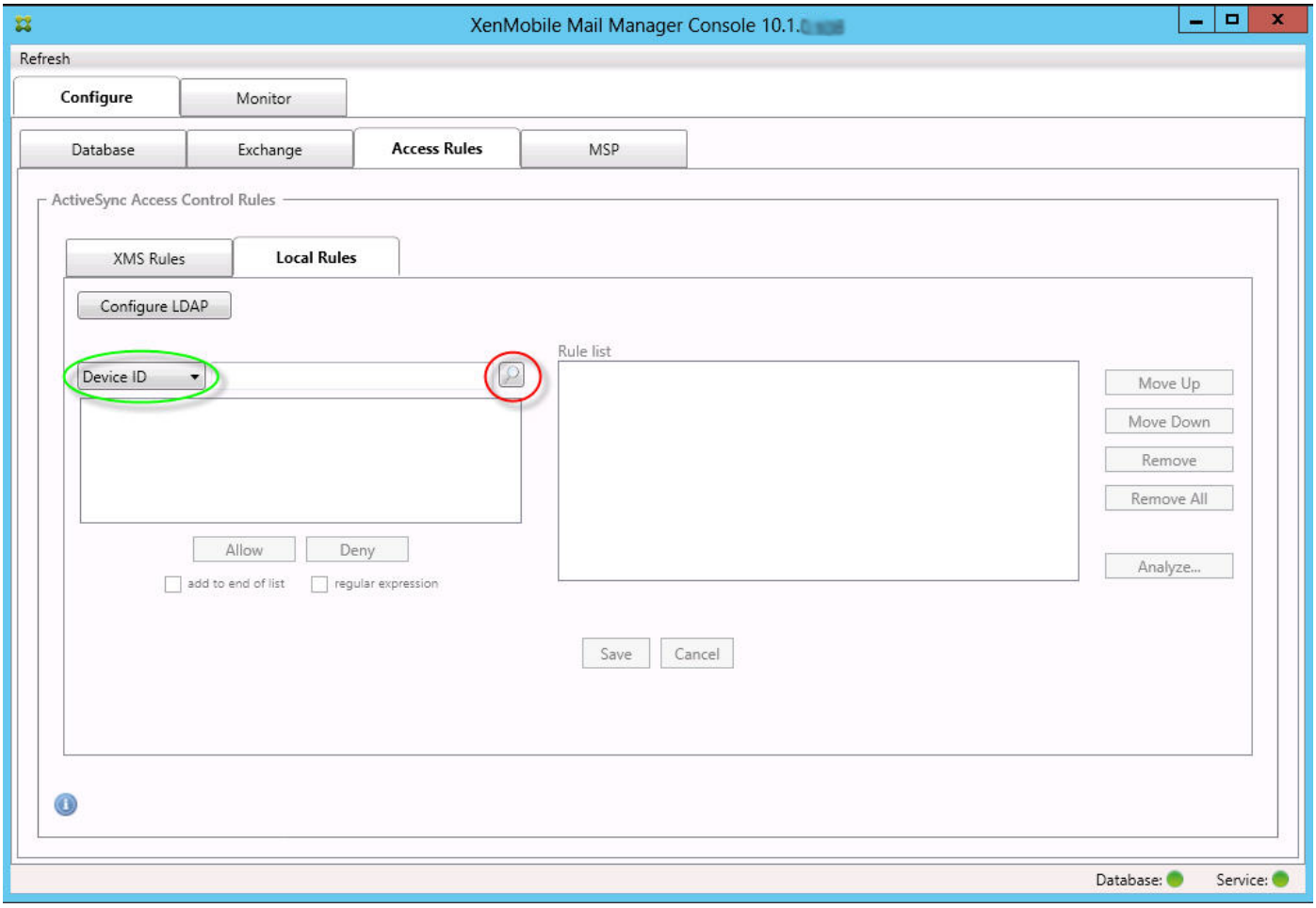


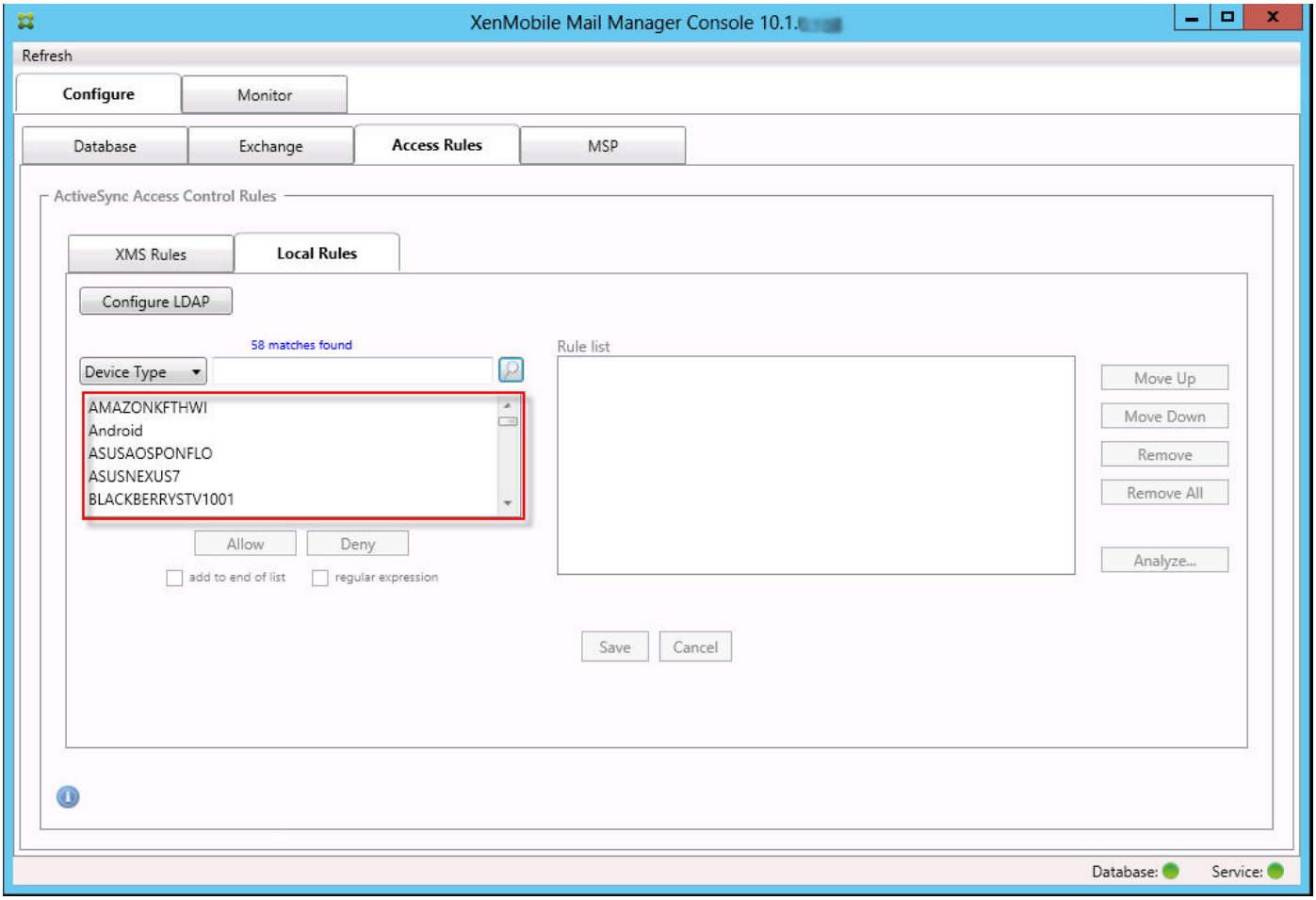


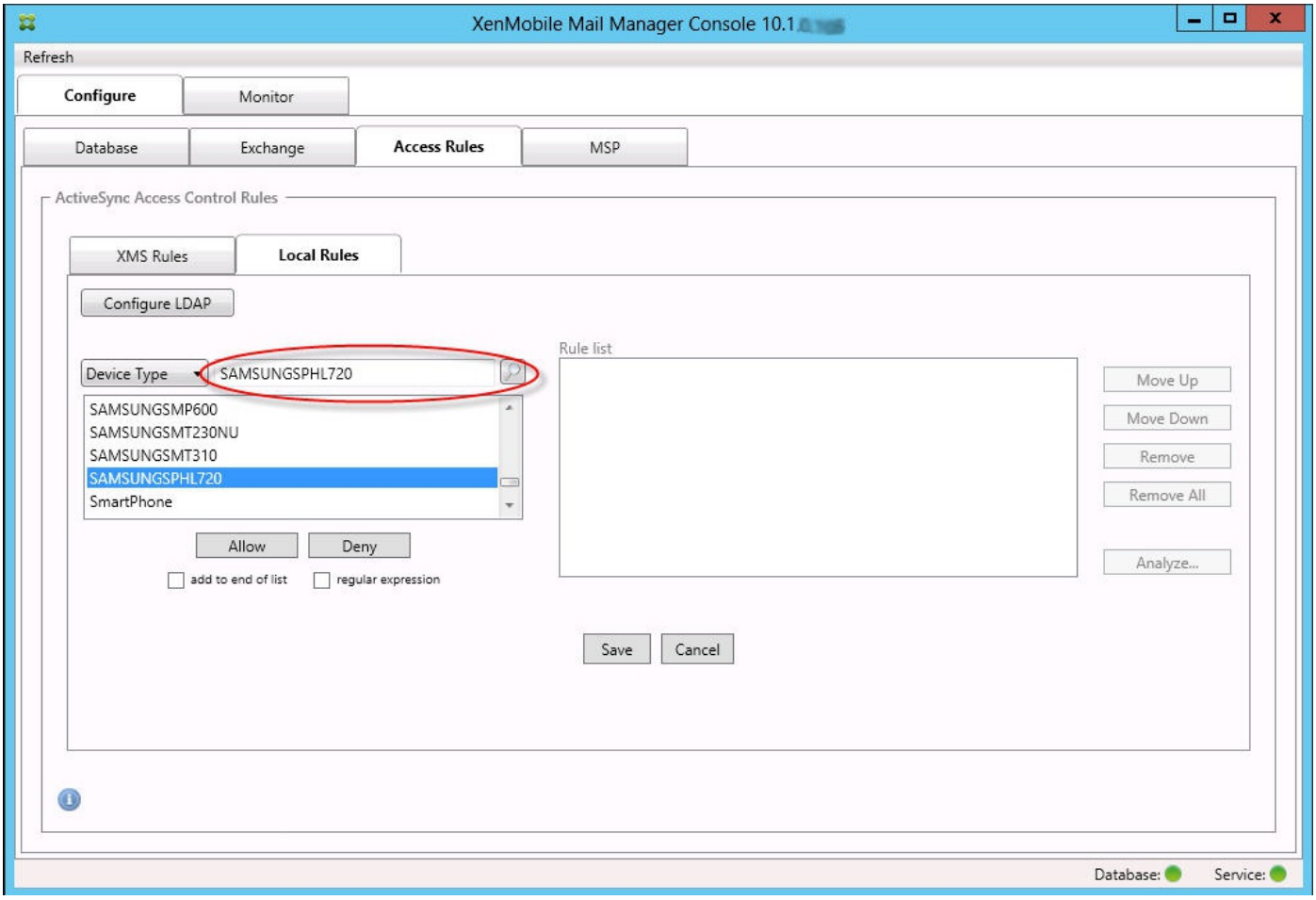


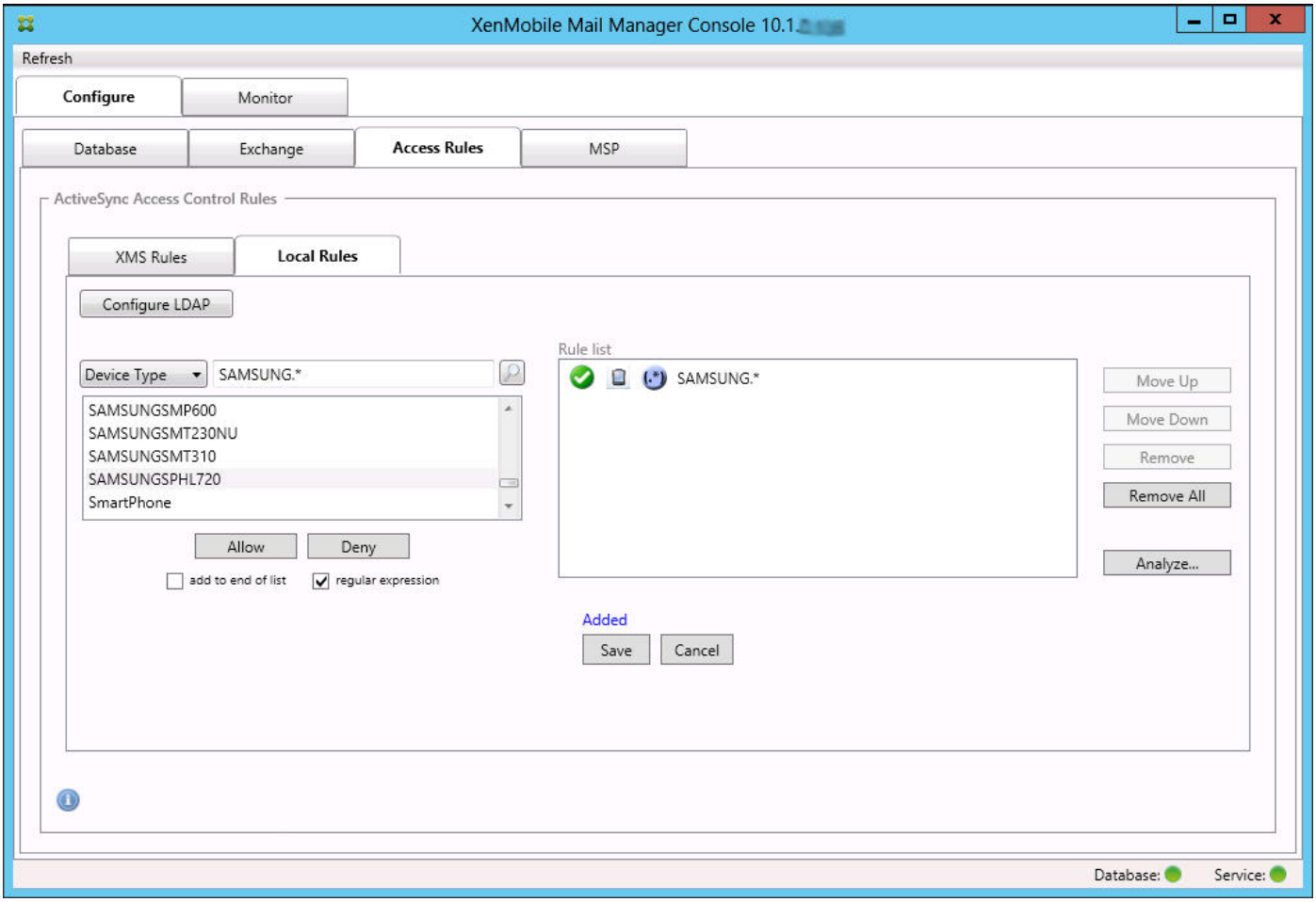
-
-

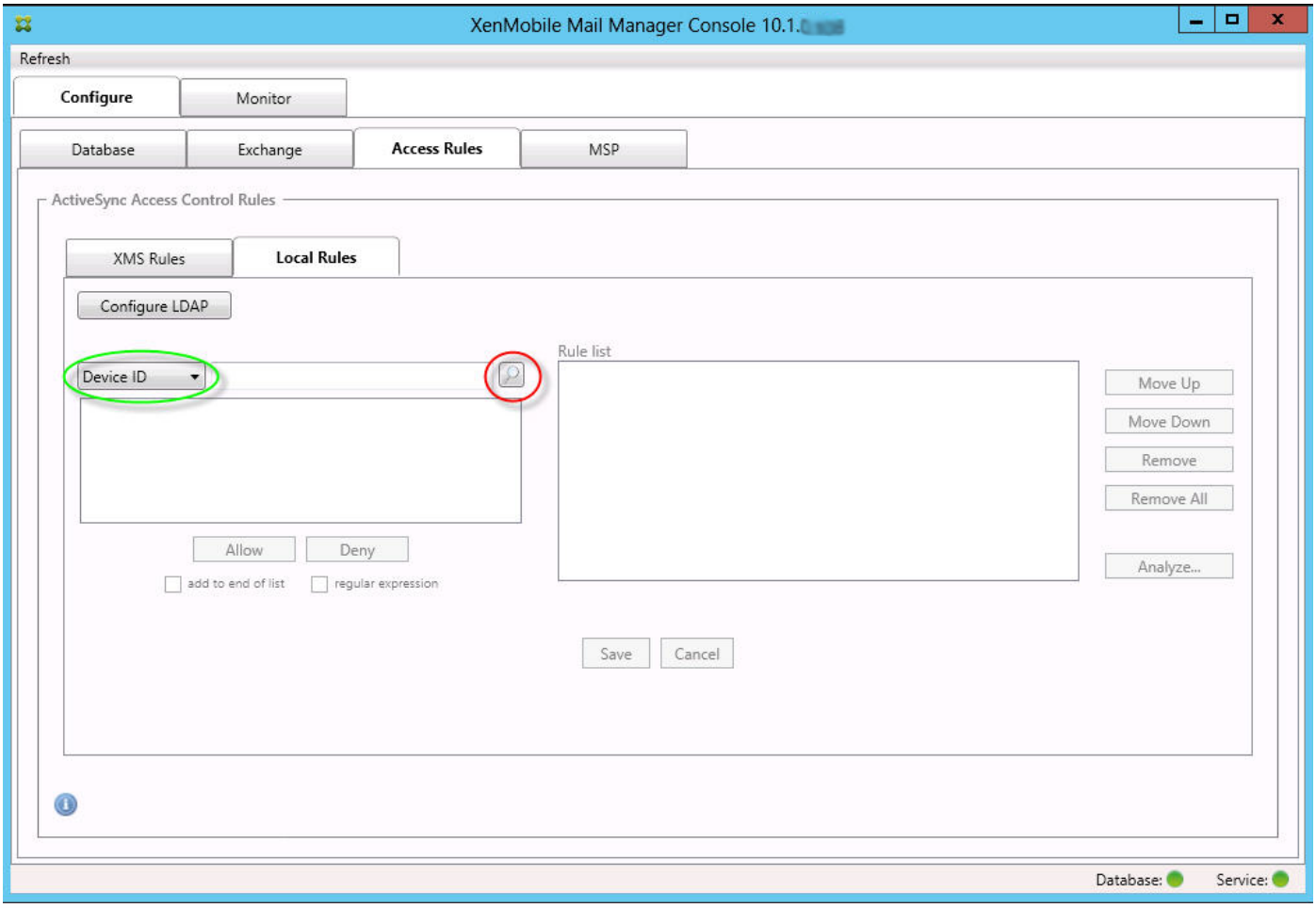


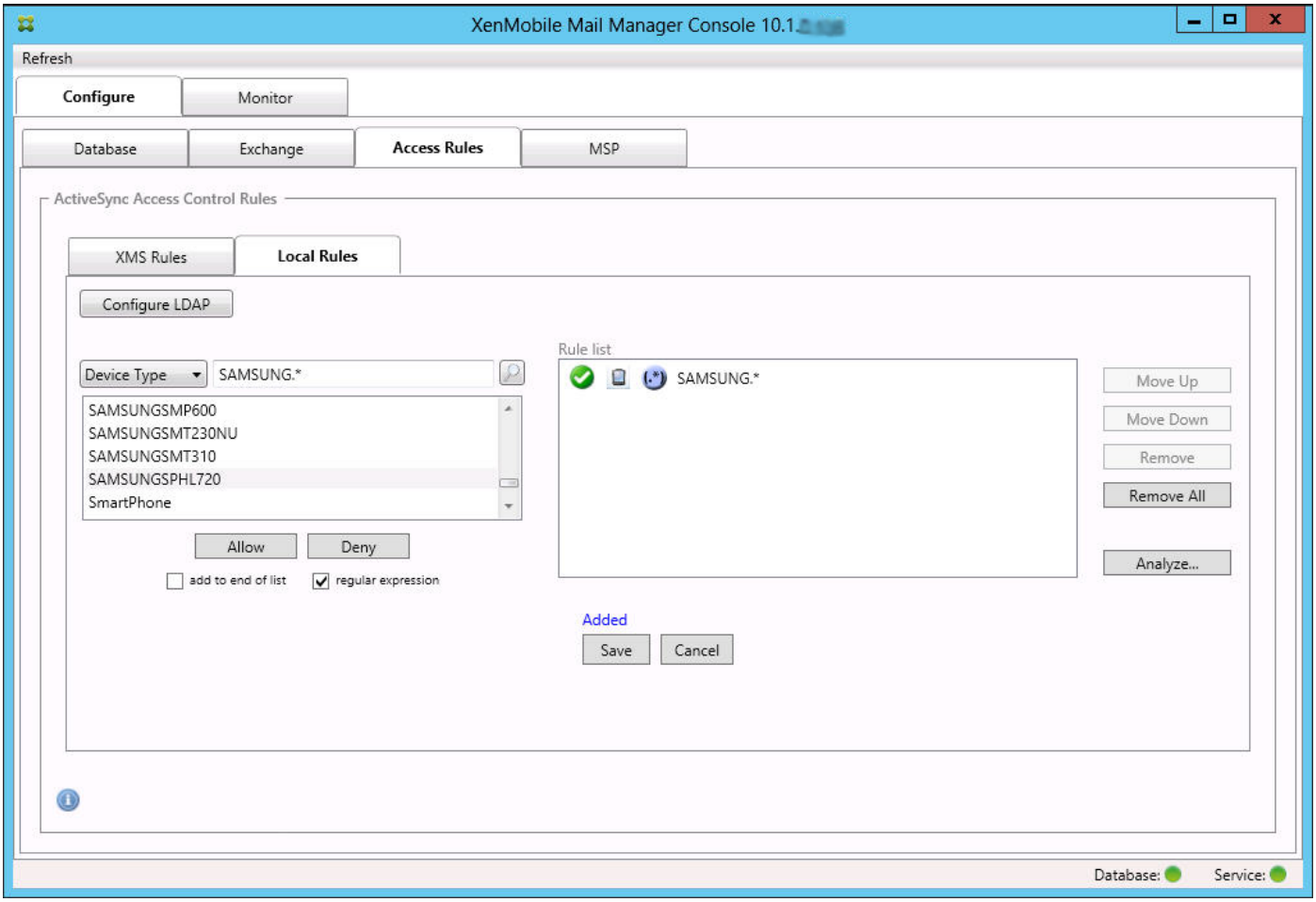


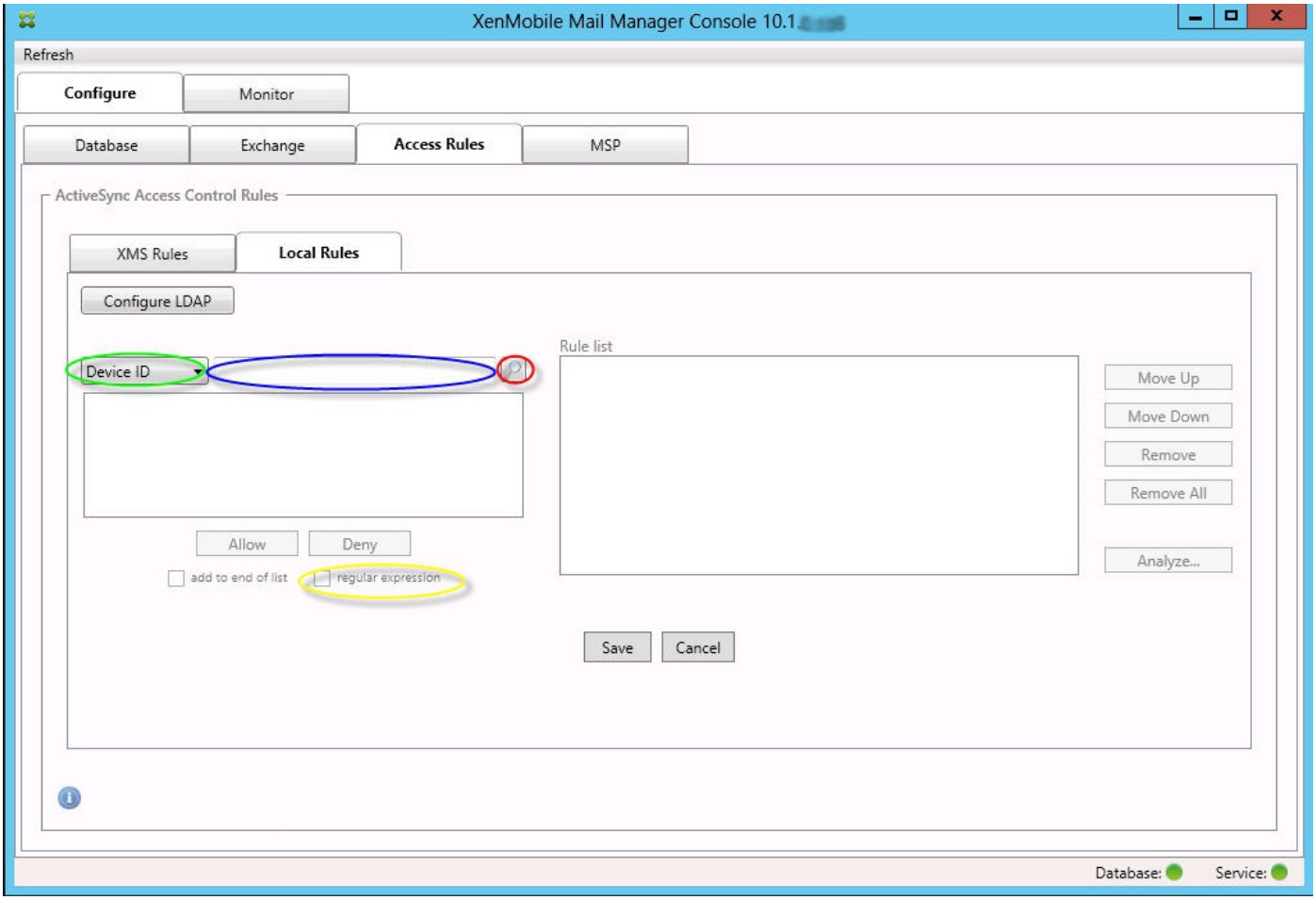


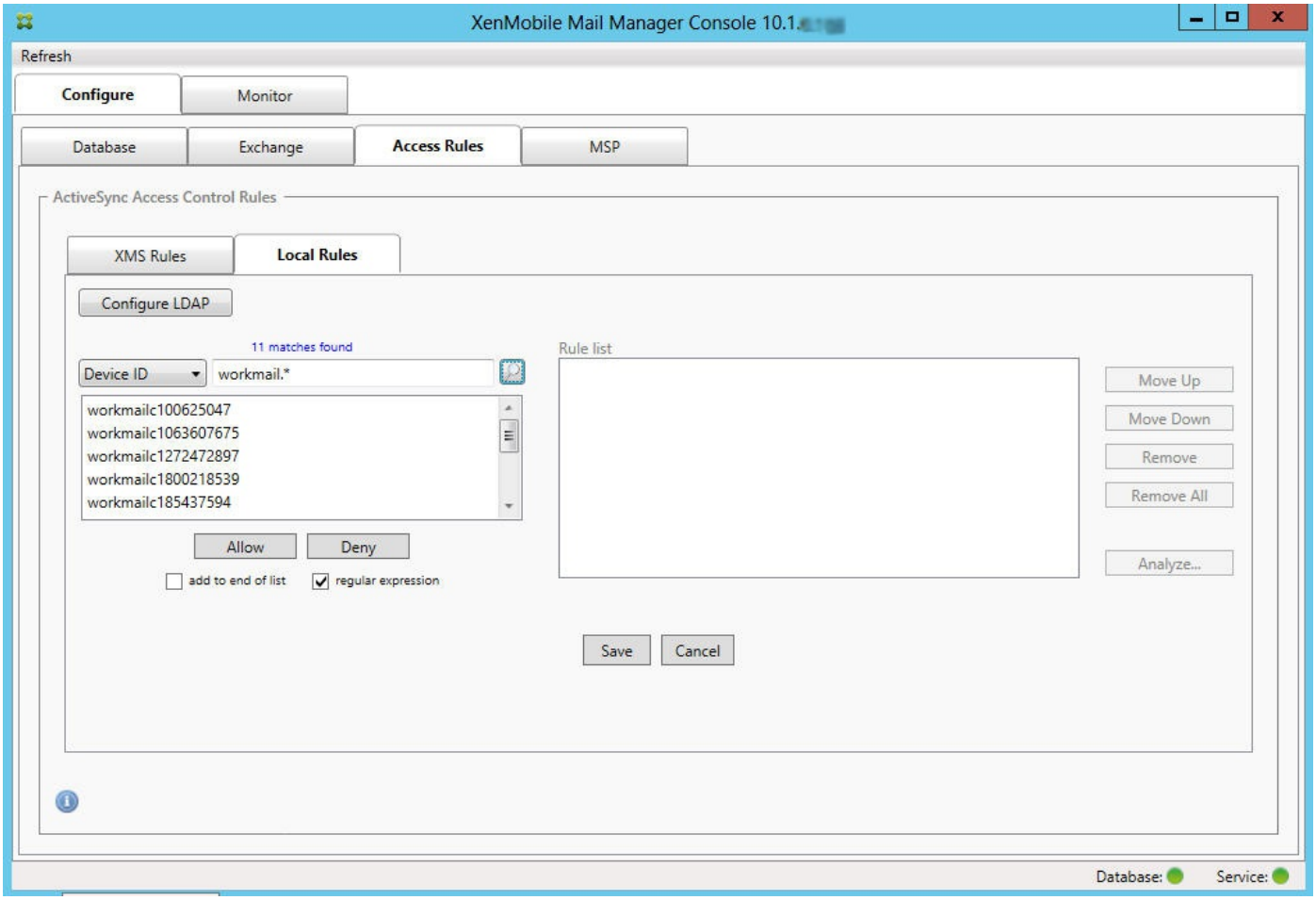


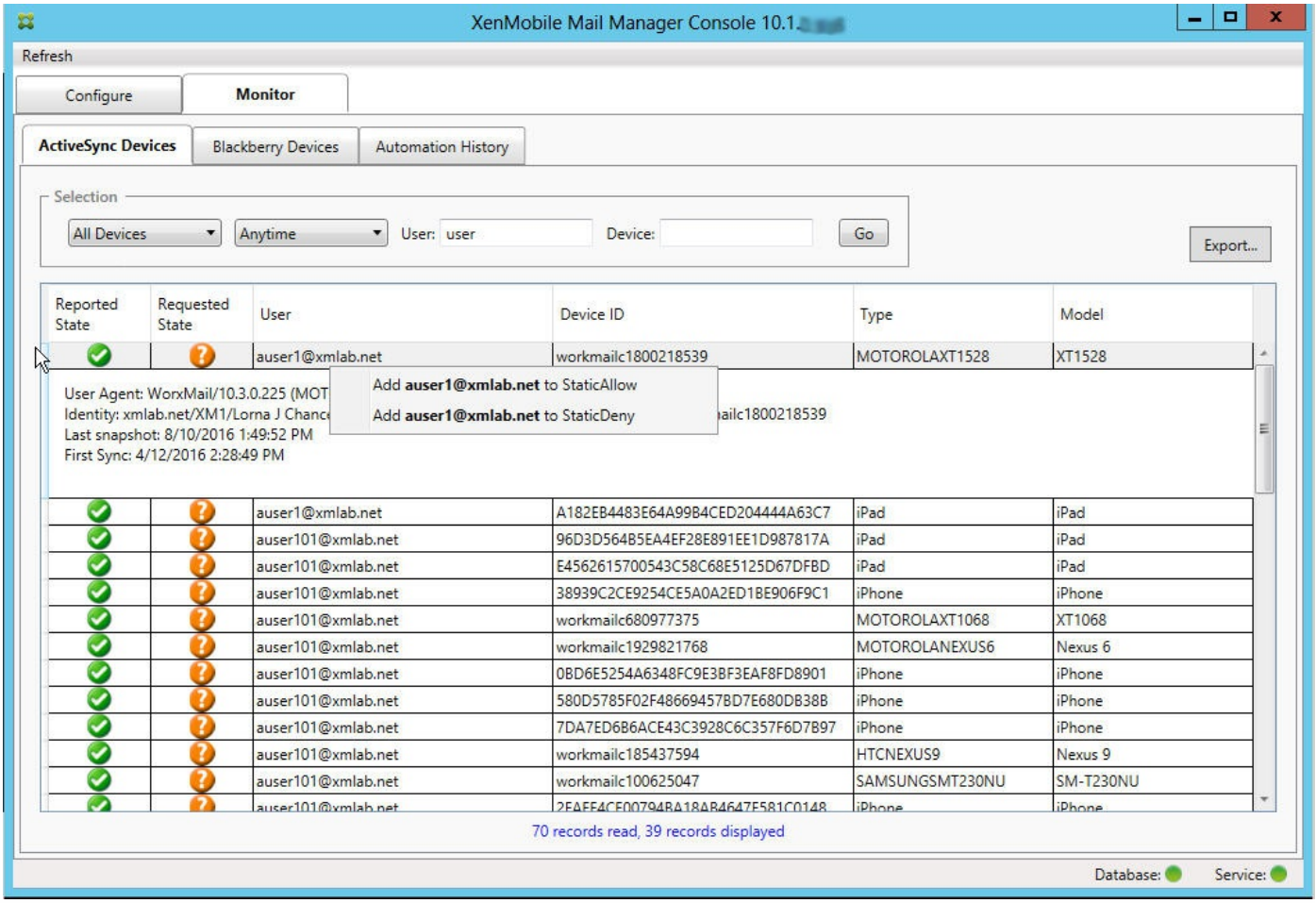






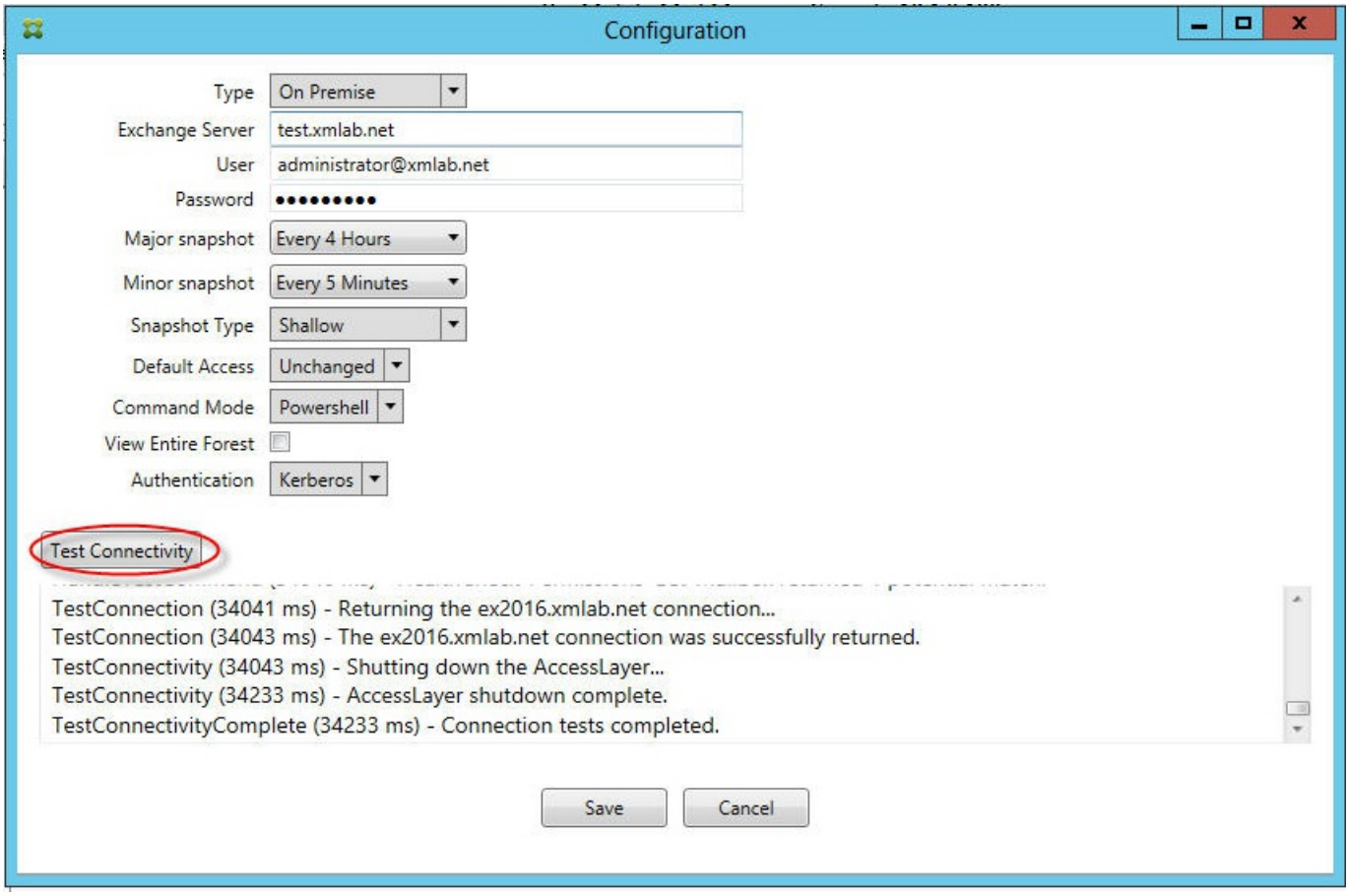






-
  -
  -
  -
-
-
-
-

-
  -
  -
-



-
-