Application Citrix Workspace pour iOS

Contents

Application Citrix Workspace pour iOS

July 1, 2024

L'application Citrix Workspace pour iOS est un logiciel client pouvant être téléchargé depuis l'App Store. Il vous permet d'accéder et d'exécuter des bureaux virtuels et des applications hébergées mis à disposition par Citrix Virtual Apps and Desktops.

iOS est le système d'exploitation des appareils mobiles Apple tels qu'iPad et iPhone. L'application Citrix Workspace pour iOS s'exécute sur les appareils utilisant le système d'exploitation iOS, tels qu'iPhone X, iPad mini et iPad Pro.

Pour obtenir des informations détaillées sur les fonctionnalités, les problèmes résolus et les problèmes connus, consultez la page À propos de cette version.

Pour plus d'informations sur les éléments obsolètes, consultez la page Fin de prise en charge.

Langues prises en charge

L'application Citrix Workspace pour iOS a été conçue pour être utilisée dans des langues autres que l'anglais. Pour obtenir la liste des langues prises en charge par l'application Citrix Workspace pour iOS, consultez la section Langues prises en charge.

Articles de référence

- Fiche technique : Citrix Workspace
- Service Global App Configuration
- Interface utilisateur de Workspace
- Optimisation de Microsoft Teams dans les environnements Citrix Virtual Apps and Desktops
- Calendrier de publication de l'application Citrix Workspace
- Documentation du développeur

Nouveautés dans les produits associés

- Citrix Workspace
- Citrix DaaS
- StoreFront
- Secure Private Access
- Application Citrix Workspace pour Mac

Ancienne documentation

Pour les versions de produits qui ont atteint leur fin de vie, consultez la section Ancienne documentation.

À propos de cette version

July 1, 2024

Découvrez les nouvelles fonctionnalités, les améliorations, les problèmes résolus et les problèmes connus.

> **Remarque :**
>
> Vous recherchez une fonctionnalité en version Technical Preview ? Nous avons rassemblé ces fonctionnalités dans une liste afin que vous puissiez les trouver en un seul endroit. Découvrez notre page Fonctionnalités de la version Technical Preview et partagez vos commentaires en utilisant le lien vers le formulaire Podio ci-joint.

Nouveautés de la version 24.5.0

Prise en charge de l'authentification à l'aide de FIDO2 lors de la connexion à un magasin cloud

À partir de la version 24.5.0, les utilisateurs peuvent s'authentifier auprès de l'application Citrix Workspace à l'aide de l'authentification sans mot de passe basée sur FIDO2 lors de la connexion à un magasin cloud. Le protocole FIDO2 offre une méthode d'authentification transparente, permettant aux employés de l'entreprise d'accéder aux applications et bureaux pendant les sessions virtuelles sans avoir à saisir de nom d'utilisateur ni de mot de passe. Cette fonctionnalité prend en charge à la fois l'itinérance (USB uniquement) et les authentificateurs de plateforme (code PIN, Touch ID et Face ID uniquement). Cette fonctionnalité est activée par défaut. Pour plus d'informations, consultez la section Prise en charge de l'authentification à l'aide de FIDO2 lors de la connexion à un magasin cloud.

> **Remarque :**
>
> L'authentification FIDO2 est prise en charge par défaut avec les onglets personnalisés de Chrome. Si vous souhaitez utiliser l'authentification FIDO2 avec WebView, signalez-le à l'aide du formulaire Podio.

Prise en charge des scanners de documents

À partir de la version 24.5.0, l'application Citrix Workspace pour iOS prend en charge la fonctionnalité de numérisation de documents. Grâce à cette fonctionnalité, vous pouvez désormais numériser et enregistrer plusieurs documents, le tout dans la session de bureau. Cette fonctionnalité est activée par défaut. Pour plus d'informations, consultez Prise en charge des scanners de documents.

Annonce de l'obsolescence du protocole DTLS 1.0 Citrix prévoit de rendre obsolète la prise en charge du protocole DTLS 1.0 dans les prochaines versions. Le protocole recommandé est DTLS 1.2. Pour plus d'informations, consultez Fin de prise en charge.

Technical Preview

- Prise en charge de l'authentification unique pour les machines virtuelles associées à Microsoft Entra ID
- Prise en charge de l'application de l'authentification biométrique pour accéder à l'application Citrix Workspace

Pour obtenir la liste complète des fonctionnalités préliminaires (version Technical Preview), consultez la page Fonctionnalités de la version Technical Preview.

Problèmes résolus dans la version 24.5.0

- Vous remarquerez peut-être que lorsque vous utilisez le lecteur de codes-barres dans la session virtuelle, le texte ne peut pas être numérisé correctement. [HDX-63675]

Problèmes connus dans la version 24.5.0

Vous remarquerez peut-être que le trackpad du Magic Keyboard ne fonctionne pas correctement lors de la session virtuelle sur un appareil iPad Pro M4. Pour contourner le problème, vous pouvez utiliser une souris externe (connecteur USB de type C filaire ou Bluetooth) pour naviguer sur l'écran lors de la session virtuelle. [HDX-66083]

Versions précédentes

Cette section fournit des informations sur les nouvelles fonctionnalités et les problèmes résolus dans les versions précédentes que nous prenons en charge. Pour plus d'informations sur le cycle de vie de ces versions, consultez la section Étapes clés du cycle de vie de l'application Citrix Workspace et de Citrix Receiver.

24.4.0

Nouveautés

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Annonce de l'obsolescence des protocoles TLS 1.0 et TLS 1.1 Citrix prévoit de rendre obsolète la prise en charge des protocoles TLS 1.0 et TLS 1.1 dans les prochaines versions. Le protocole recommandé est TLS 1.2 ou TLS 1.3. Pour plus d'informations, consultez Fin de prise en charge.

Problèmes résolus

- Lorsque vous ouvrez la caméra de l'appareil depuis la session de l'application virtuelle, l'application Citrix Workspace pour iOS peut se fermer de manière inattendue. [CVADHELP-24825]

Problèmes connus

Il n'y a aucun nouveau problème connu.

24.3.5

Nouveautés

Prise en charge du lecteur utilitaire de carte à puce Twocanoes À partir de la version 24.3.5, l'application Citrix Workspace pour iOS prend en charge les lecteurs utilitaires de cartes à puce Twocanoes. Pour plus d'informations sur les lecteurs de cartes à puce pris en charge et les détails de configuration, consultez la section Cartes à puce.

> **Remarque :**
>
> Le lecteur USB-C de l'utilitaire de carte à puce Twocanoes est pris en charge à la fois pour la connexion à l'application Citrix Workspace et pour la connexion à une session virtuelle. Cependant, le lecteur Bluetooth de l'utilitaire de cartes à puce Twocanoes n'est pris en charge que pour la connexion à l'application Citrix Workspace et non pour la connexion à une session virtuelle.

Prise en charge de la configuration du nom de l'appareil via UEM À partir de la version 24.3.5, l'application Citrix Workspace pour iOS permet aux administrateurs d'attribuer et d'identifier des

noms d'appareils en fonction de groupes d'utilisateurs via une solution Unified Endpoint Management (UEM). Pour plus d'informations, consultez la section Prise en charge de la configuration du nom de l'appareil via UEM.

Technical Preview

- Prise en charge de la configuration des paramètres de l'application Citrix Workspace via UEM

Pour plus d'informations sur cette version Technical Preview, consultez la section Fonctionnalités de la version Technical Preview.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes connus

Il n'y a aucun nouveau problème connu.

24.3.0

Nouveautés

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Technical Preview

- Prise en charge de l'audio adaptatif

Pour plus d'informations sur cette version Technical Preview, consultez la section Fonctionnalités de la version Technical Preview.

Problèmes résolus

Après la mise à niveau de l'application Citrix Workspace pour iOS avec la version 24.1.0, la saisie à l'aide du clavier virtuel au cours de la session peut échouer pour les applications basées sur le logiciel Oracle Java Web Start. [CVADHELP-24645]

Problèmes connus

Il n'y a aucun nouveau problème connu.

24.2.0

Nouveautés

Possibilité de supprimer plusieurs magasins à la fois À partir de la version 24.2.0, l'application Citrix Workspace pour iOS permet de sélectionner plusieurs magasins et de les supprimer. Cette fonctionnalité améliore l'expérience utilisateur lors de l'utilisation de plusieurs magasins. Cette fonctionnalité est activée par défaut. Pour plus d'informations, consultez la section Possibilité de supprimer plusieurs magasins à la fois.

Possibilité pour les administrateurs d'empêcher les utilisateurs de modifier le nom d'un magasin Auparavant, les utilisateurs pouvaient modifier le nom d'un magasin en utilisant l'option **Modifier le compte**.

À partir de la version 24.2.0, l'application Citrix Workspace pour iOS offre aux administrateurs la possibilité d'empêcher les utilisateurs de modifier le nom d'un magasin. Grâce à cette fonctionnalité, les administrateurs peuvent facilement identifier et maintenir la cohérence des noms de magasin. Pour plus d'informations, consultez Possibilité pour les administrateurs d'empêcher les utilisateurs de modifier le nom d'un magasin.

Remplissage automatique du nom du magasin À partir de la version 24.2.0, l'application Citrix Workspace pour iOS permet aux administrateurs de mettre à jour les noms de magasin et de les transmettre automatiquement aux utilisateurs. Cette fonctionnalité améliore l'expérience utilisateur, car il n'est plus nécessaire de recourir à une intervention manuelle pour mettre à jour le nom d'un magasin. Pour plus d'informations, consultez la section Remplissage automatique du nom du magasin.

> **Remarque :**
>
> cette fonctionnalité ne peut prendre effet que si les administrateurs ont désactivé l'option permettant d'empêcher les utilisateurs de modifier le nom du magasin.

Technical Preview

- Prise en charge des fonctionnalités d'accessibilité et VoiceOver

Pour plus d'informations sur cette version Technical Preview, consultez la section Fonctionnalités de la version Technical Preview.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes connus

Il n'y a aucun nouveau problème connu.

24.1.0

Nouveautés

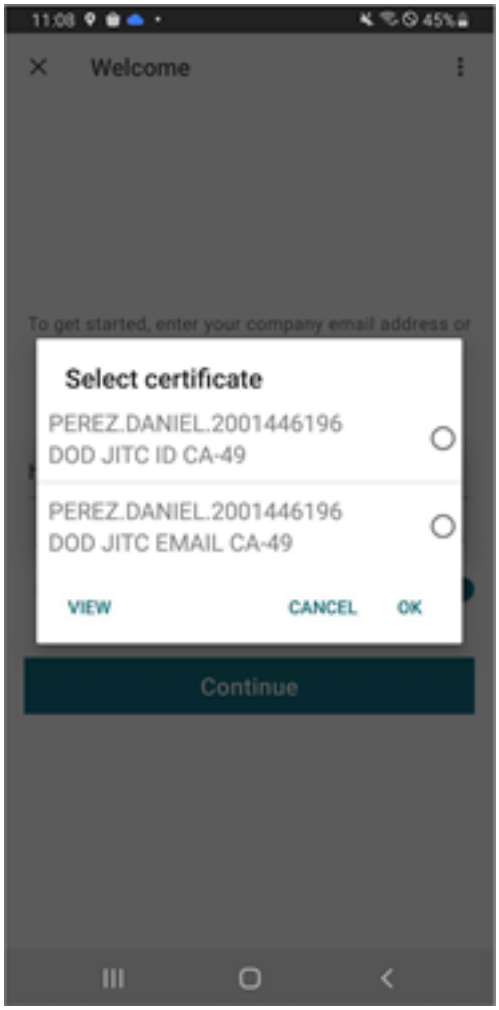
Mise à jour de sécurité Cette version contient des mises à jour de sécurité critiques et des correctifs pour les problèmes de sécurité.

Prise en charge de la configuration du stockage des jetons d'authentification lors du déploiement local L'application Citrix Workspace pour iOS propose désormais une option permettant de configurer le stockage des jetons d'authentification sur le disque local, pour les magasins locaux. Grâce à cette fonctionnalité, vous pouvez désactiver le stockage du jeton d'authentification pour renforcer la sécurité. Après la désactivation, lorsque le système ou la session redémarre, vous devez vous authentifier à nouveau pour accéder à la session. Pour plus d'informations, consultez la section Prise en charge de la configuration du stockage des jetons d'authentification lors du déploiement local.

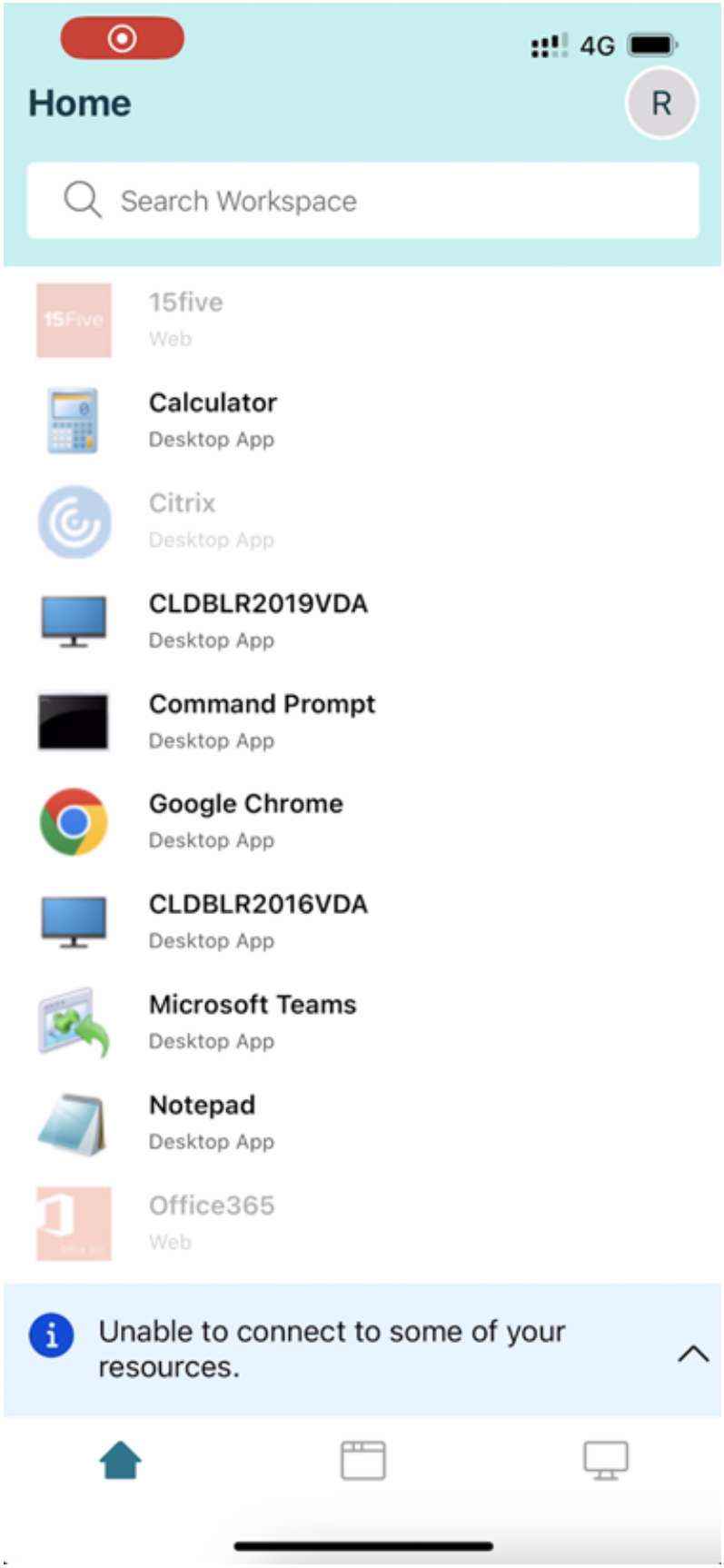
Prise en charge de magasins cloud multiples À partir de la version 24.1.0, vous pouvez ajouter plusieurs comptes de magasin cloud à l'application Citrix Workspace pour iOS et iPadOS. Désormais, les utilisateurs finaux peuvent facilement ajouter plusieurs magasins et passer d'un magasin à l'autre. Cette fonctionnalité améliore l'expérience utilisateur lors de l'accès à plusieurs magasins. Pour plus d'informations, consultez la section Prise en charge de plusieurs magasins cloud.

Prise en charge de plusieurs certificats dans l'authentification par carte à puce Auparavant, l'application Citrix Workspace pour iOS affichait le certificat disponible sur le premier emplacement de la carte à puce connectée.

À compter de la version 24.1.0, l'application Citrix Workspace pour iOS affiche tous les certificats disponibles sur la carte à puce et vous permet de sélectionner le certificat requis lors de l'authentification par carte à puce. Pour plus d'informations, consultez la section Prise en charge de plusieurs certificats dans l'authentification par carte à puce.



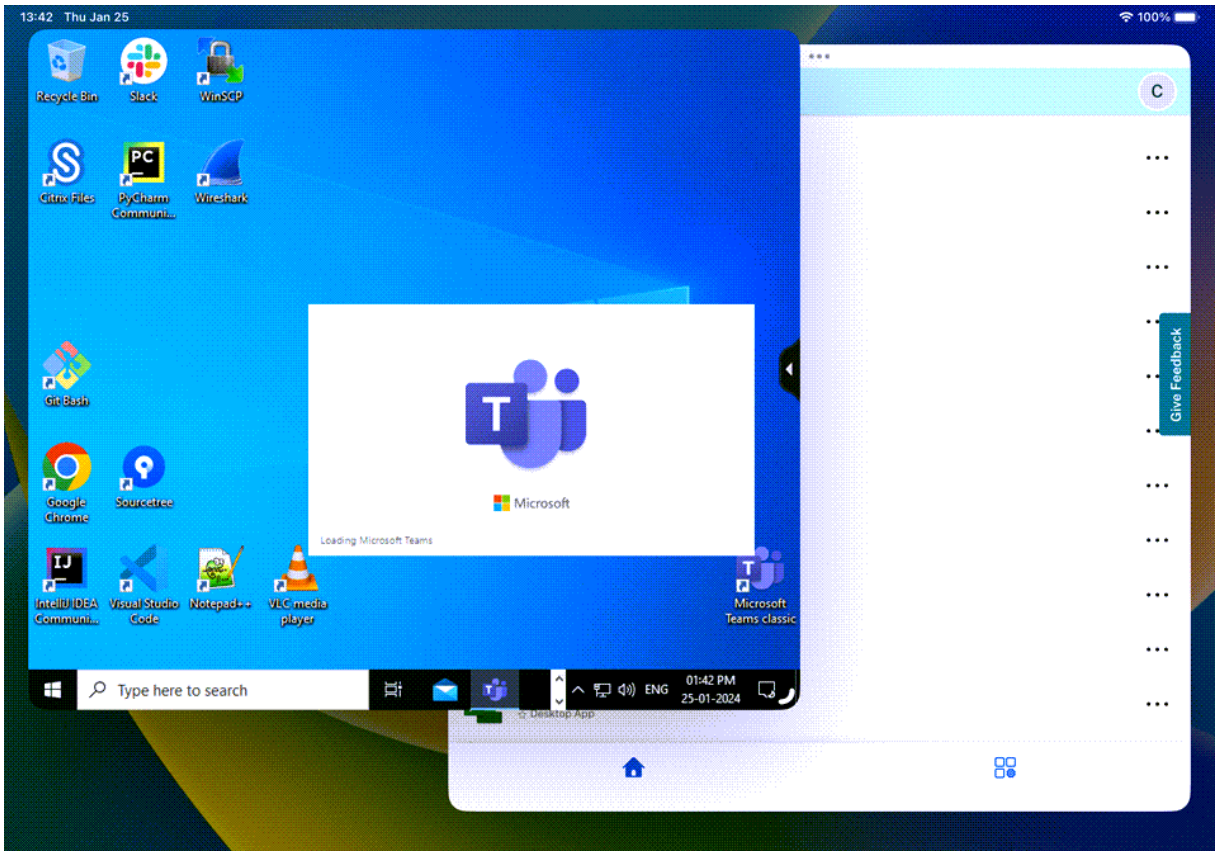
Amélioration de l'interface utilisateur pour le mode hors ligne de continuité du service À compter de la version 24.1.0, l'interface utilisateur de l'application Citrix Workspace pour iOS a été améliorée pour être plus informative, plus moderne et offrir une expérience conviviale lors des pannes de Citrix Workspace. La fonctionnalité de recherche analogique est également incluse pour le mode hors ligne. Grâce à cette fonctionnalité, vous pouvez trouver des résultats pour des applications ou des bureaux avec du texte proche et des termes de recherche mal orthographiés. Pour plus d'informations sur la continuité de service, consultez la section Continuité de service.



Prise en charge d'une fenêtre de session distincte de celle de l'application Citrix Workspace À partir de la version 24.1.0, l'application Citrix Workspace pour iOS introduit une fenêtre de session distincte qui rend le multitâche plus efficace et convivial. Grâce à cette fonctionnalité, vous pouvez profiter d'une expérience similaire à celle d'un ordinateur de bureau. Lorsque la fonctionnalité "Fenêtre de session distincte"est activée, vous pouvez simplement glisser-déposer les sessions sur les moniteurs externes connectés. Par conséquent, le moniteur principal de l'iPad peut être utilisé pour effectuer plusieurs tâches à la fois avec d'autres applications.

> **Remarque :**
>
> Cette fonctionnalité n'est prise en charge que sur les appareils qui prennent en charge la fonctionnalité Stage Manager. Les appareils iPhone et iPad ne prennent pas tous en charge cette fonctionnalité. Pour plus d'informations sur la fonctionnalité State Manager, consultez la section Activer ou désactiver Stage Manager sur votre iPad dans la documentation d'assistance Apple.

Pour plus d'informations, consultez la section Prise en charge d'une fenêtre de session distincte de celle de l'application Citrix Workspace.



Prise en charge du mode de saisie Scancode À partir de la version 24.1.0, vous pouvez sélectionner **Scancode** comme mode de saisie au clavier lorsque vous utilisez un clavier physique externe. Cette

fonctionnalité est utile lorsque vous utilisez des appareils iOS dotés du clavier standard d'un PC Windows externe. Avec **Scancode**, vous pouvez utiliser la disposition du clavier du VDA au lieu de celle du clavier d'iOS. De cette façon, vous pouvez suivre complètement le style de saisie du clavier Windows externe au lieu de celui d'iOS. C'est utile lorsque vous effectuez des saisies dans des langues d'Asie de l'Est, car cela améliore considérablement l'expérience utilisateur globale. L'utilisateur final peut se retrouver à utiliser la disposition du clavier du serveur au lieu de celle du client. Pour plus d'informations, consultez la section Prise en charge du mode de saisie Scancode.

Amélioration de la prise en charge des raccourcis clavier externes L'application Citrix Workspace pour iOS vous permet désormais d'utiliser davantage de raccourcis depuis des claviers externes lors d'une session d'application ou de bureau à distance. Voici quelques-unes des améliorations importantes apportées aux raccourcis clavier externes :

- Prise en charge des touches propres au clavier Windows, telles que `Insert`, `Delete` et le pavé numérique.
- Lorsque vous maintenez une touche enfoncée sans la relâcher, l'application/le bureau à distance répond correctement.
- Prise en charge de raccourcis avec plus de trois touches.

En outre, vous pouvez désormais configurer la touche spécifique pour `Alt` en utilisant les options suivantes via **Paramètres > Options du clavier > Attribuer une touche spécifique pour Alt** :

- `Option or Alt (left)` : envoie `Alt` avec `Option (left)` `or Alt (left)`.
- `Command or Windows (left)` : envoie `Alt` à l'aide des touches `Command (left)` `or Windows (left)`.
- `Option or Alt (left and right)` : envoie `Alt` à l'aide de la touche `Option or Alt (left and right)`.

L'option **Attribuer une touche spécifique pour Alt** permet d'éviter les conflits entre la touche `Option` macOS et la touche `Alt` Windows.

Pour plus d'informations, consultez la section Amélioration de la prise en charge des raccourcis clavier externes.

Performances graphiques améliorées À partir de la version 24.1.0, l'application Citrix Workspace pour iOS prend en charge le codage ou le décodage vidéo H.264 avec accélération matérielle. Le moteur multimédia de Citrix HDX utilise désormais l'infrastructure Video Toolbox d'Apple pour le codage et le décodage. Cette infrastructure compresse et décompresse la vidéo plus rapidement et en temps réel. Cette amélioration réduit la charge sur l'unité centrale lors de l'utilisation du multimédia. Pour plus d'informations, consultez la section Performances graphiques améliorées.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes connus

- Après la mise à niveau de l'application Citrix Workspace pour iOS avec la version 24.1.0, la saisie à l'aide du clavier virtuel au cours de la session peut échouer pour les applications basées sur le logiciel Oracle Java Web Start. [CVADHELP-24645]

23.12.1

Nouveautés

Prise en charge de la clé YubiKey pour l'authentification par carte à puce Vous pouvez désormais effectuer une authentification par carte à puce à l'aide d'une clé YubiKey. Cette fonctionnalité fournit une expérience d'authentification sur un seul appareil pour l'application Citrix Workspace, les sessions virtuelles et les applications publiées dans la session VDA. Il n'est plus nécessaire de connecter des lecteurs de carte à puce ou d'autres authentificateurs externes. Cela simplifie l'expérience utilisateur, car la clé YubiKey prend en charge une grande variété de protocoles, tels que OTP, FIDO et bien d'autres encore.

Pour vous connecter à l'application Citrix Workspace, insérez la clé YubiKey dans votre iPhone ou iPad, activez le bouton de la carte à puce et indiquez l'URL de votre magasin.

> **Remarque :**
>
> L'application Citrix Workspace pour iOS ne prend en charge que la série YubiKey 5. Pour plus d'informations sur les clés YubiKey, consultez la page série YubiKey 5.

Prise en charge des lecteurs génériques de type C L'application Citrix Workspace pour iOS prend désormais en charge les lecteurs compatibles CCID de type C pour l'authentification par carte à puce. Auparavant, seuls les lecteurs basés sur des ports Lightning étaient pris en charge. L'inclusion de lecteurs de cartes à puce de type C dans l'application Citrix Workspace présente un double avantage : les utilisateurs peuvent s'authentifier via l'application Citrix Workspace et utiliser facilement la carte à puce lors de leurs sessions de bureau virtuel.

Configurer le nom de l'appareil via UEM Avec cette version, un nouveau paramètre appelé deviceName est désormais disponible pour la configuration via Unified Endpoint Management (UEM).

Cet attribut aide les administrateurs à attribuer et à identifier les noms des appareils en fonction des groupes d'utilisateurs.

Clé de configuration	Type de valeur	Valeur de configuration
deviceName	Chaîne	name_of_the _device

Fin de prise en charge pour iOS version 14 L'application Citrix Workspace pour iOS ne prend pas en charge la version iOS 14 ou antérieure à partir de la version 23.12.0. Vous pouvez passer à la dernière version d'iOS depuis l'App Store. Pour plus d'informations, consultez le tableau de fin de prise en charge.

Technical Preview

- Prise en charge de la webcam externe

Pour plus d'informations sur cette version Technical Preview, consultez la section Fonctionnalités de la version Technical Preview.

Problèmes résolus

- L'ouverture d'une session de bureau échoue lorsque la langue de l'application Citrix Workspace est définie sur l'italien.

23.12.0

Nouveautés

Prise en charge de la clé YubiKey pour l'authentification par carte à puce Vous pouvez désormais effectuer une authentification par carte à puce à l'aide d'une clé YubiKey. Cette fonctionnalité fournit une expérience d'authentification sur un seul appareil pour l'application Citrix Workspace, les sessions virtuelles et les applications publiées dans la session VDA. Il n'est plus nécessaire de connecter des lecteurs de carte à puce ou d'autres authentificateurs externes. Cela simplifie l'expérience utilisateur, car la clé YubiKey prend en charge une grande variété de protocoles, tels que OTP, FIDO et bien d'autres encore.

Pour vous connecter à l'application Citrix Workspace, insérez la clé YubiKey dans votre iPhone ou iPad, activez le bouton de la carte à puce et indiquez l'URL de votre magasin.

> **Remarque :**
>
> L'application Citrix Workspace pour iOS ne prend en charge que la série YubiKey 5. Pour plus d'informations sur les clés YubiKey, consultez la page série YubiKey 5.

Prise en charge des lecteurs génériques de type C L'application Citrix Workspace pour iOS prend désormais en charge les lecteurs compatibles CCID de type C pour l'authentification par carte à puce. Auparavant, seuls les lecteurs basés sur des ports Lightning étaient pris en charge. L'inclusion de lecteurs de cartes à puce de type C dans l'application Citrix Workspace présente un double avantage : les utilisateurs peuvent s'authentifier via l'application Citrix Workspace et utiliser facilement la carte à puce lors de leurs sessions de bureau virtuel.

Configurer le nom de l'appareil via UEM Avec cette version, un nouveau paramètre appelé deviceName est désormais disponible pour la configuration via Unified Endpoint Management (UEM). Cet attribut aide les administrateurs à attribuer et à identifier les noms des appareils en fonction des groupes d'utilisateurs.

Clé de configuration	Type de valeur	Valeur de configuration
deviceName	Chaîne	name_of_the _device

Fin de prise en charge pour iOS version 14 L'application Citrix Workspace pour iOS ne prend pas en charge la version iOS 14 ou antérieure à partir de la version 23.12.0. Vous pouvez passer à la dernière version d'iOS depuis l'App Store. Pour plus d'informations, consultez le tableau de fin de prise en charge.

Technical Preview

- Prise en charge de la webcam externe

Pour plus d'informations sur cette version Technical Preview, consultez la section Fonctionnalités de la version Technical Preview.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.12.0

Nouveautés

Prise en charge de la clé YubiKey pour l'authentification par carte à puce Vous pouvez désormais effectuer une authentification par carte à puce à l'aide d'une clé YubiKey. Les utilisateurs s'authentifient sur un seul appareil pour les applications Web et SaaS, ainsi que pour les sessions virtuelles, sans avoir besoin de connecter des lecteurs de cartes à puce ou d'autres authentificateurs externes. Cela simplifie l'expérience utilisateur, car la clé YubiKey prend en charge une grande variété de protocoles, tels que OTP, FIDO et bien d'autres encore.

Pour vous connecter à l'application Citrix Workspace, insérez la clé YubiKey dans votre iPhone ou iPad, activez le bouton de la carte à puce et indiquez l'URL de votre magasin.

> **Remarque :**
>
> L'application Citrix Workspace pour iOS ne prend en charge que la série YubiKey 5. Pour plus d'informations sur les clés YubiKey, consultez la page série YubiKey 5.

Prise en charge des lecteurs génériques de type C L'application Citrix Workspace pour iOS prend désormais en charge les lecteurs compatibles CCID de type C pour l'authentification par carte à puce. Auparavant, seuls les lecteurs basés sur des ports Lightning étaient pris en charge. L'inclusion de lecteurs de cartes à puce de type C dans l'application Citrix Workspace présente un double avantage : les utilisateurs peuvent s'authentifier via l'application Citrix Workspace et utiliser facilement la carte à puce lors de leurs sessions de bureau virtuel.

Configurer le nom de l'appareil via UEM Avec cette version, un nouveau paramètre appelé deviceName est désormais disponible pour la configuration via Unified Endpoint Management (UEM). Cet attribut aide les administrateurs à attribuer et à identifier les noms des appareils en fonction des groupes d'utilisateurs.

Clé de configuration	Type de valeur	Valeur de configuration
deviceName	Chaîne	name_of_the _device

Fin de prise en charge pour iOS version 14 L'application Citrix Workspace pour iOS ne prend pas en charge la version iOS 14 ou antérieure à partir de la version 23.12.0. Vous pouvez passer à la dernière version d'iOS depuis l'App Store. Pour plus d'informations, consultez le tableau de fin de prise en charge.

Technical Preview

- Prise en charge de la webcam externe

Pour plus d'informations sur cette version Technical Preview, consultez la section Fonctionnalités de la version Technical Preview.

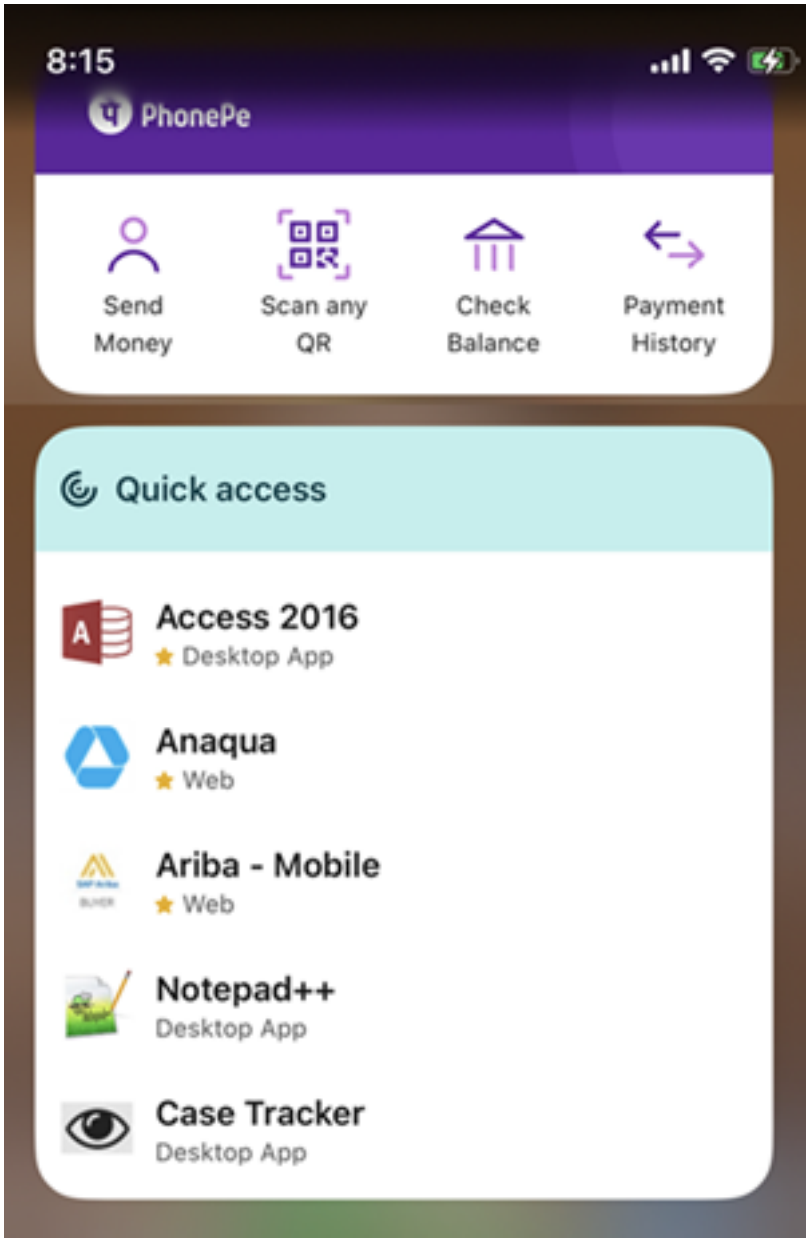
Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.11.0

Afficher les applications et les bureaux sous forme de widgets

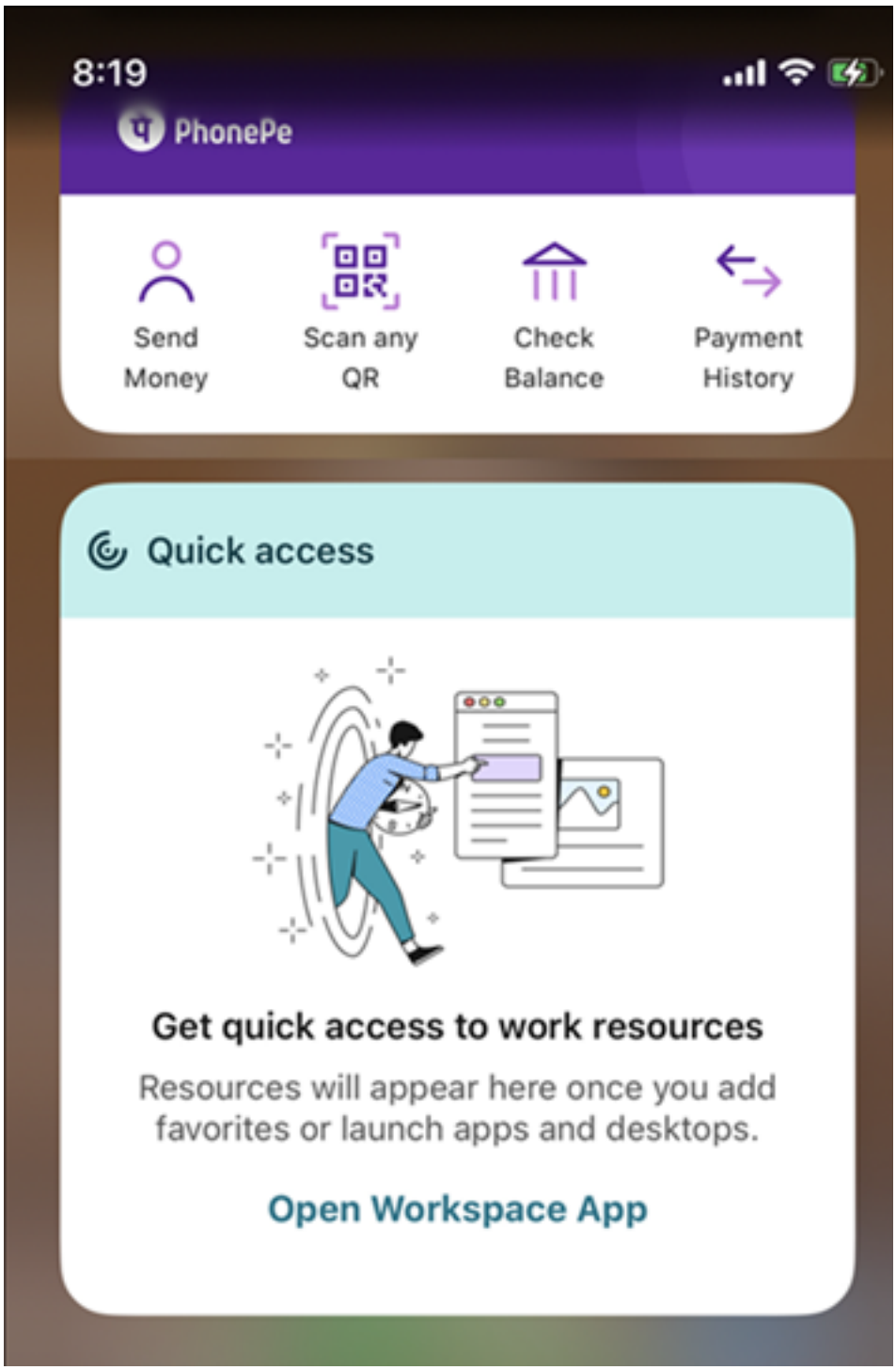
Les utilisateurs finaux peuvent désormais lancer leurs applications et bureaux virtuels directement depuis leur iPhone et iPad. Ils n'ont pas besoin d'ouvrir l'application Citrix Workspace pour démarrer une session d'application ou de bureau. Un utilisateur peut disposer d'un maximum de cinq applications et bureaux virtuels sous forme de widgets.



Les widgets sont créés automatiquement selon les critères suivants :

- Trois applications ou bureaux favoris et deux récemment ouverts sont affichés sous forme de widgets
- S'il n'y a pas d'applications ou de bureaux favoris, jusqu'à cinq applications et bureaux récemment ouverts sont affichés sous forme de widgets
- S'il n'y a pas d'applications ou de bureaux récemment ouverts, jusqu'à cinq applications ou bureaux favoris sont affichés sous forme de widgets
- Si aucune application ni aucun bureau n'a encore été ajouté aux favoris et qu'aucune application ou bureau n'a été ouvert récemment, les utilisateurs sont invités à ouvrir l'application Citrix Workspace pour iOS. Ils peuvent ensuite marquer certaines applications ou certains bureaux

comme favoris.



Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.10.1

Nouveautés

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.10.0

Nouveautés

Annonce de fin de prise en charge de la version 14 d'iOS L'application Citrix Workspace ne prendra plus en charge la version 14 d'iOS ou les versions antérieures à partir de version 23.12.0. Vous pouvez passer à la dernière version d'iOS depuis l'App Store. Pour plus d'informations, consultez le tableau de fin de prise en charge.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.9.0

Nouveautés

Prise en charge du protocole TLS 1.3 L'application Citrix Workspace pour iOS prend désormais en charge le protocole TLS 1.3 qui améliore les performances et l'efficacité. Le protocole TLS 1.3 garantit une sécurité de haut niveau grâce à ses suites de chiffrement complexes et à ses clés de session uniques.

Les utilisateurs peuvent l'activer sur l'application Citrix Workspace pour iOS comme suit :

1. Accédez à **Paramètres avancés** > **Versions TLS**.
2. Sélectionnez la **version TLS 1.3**.

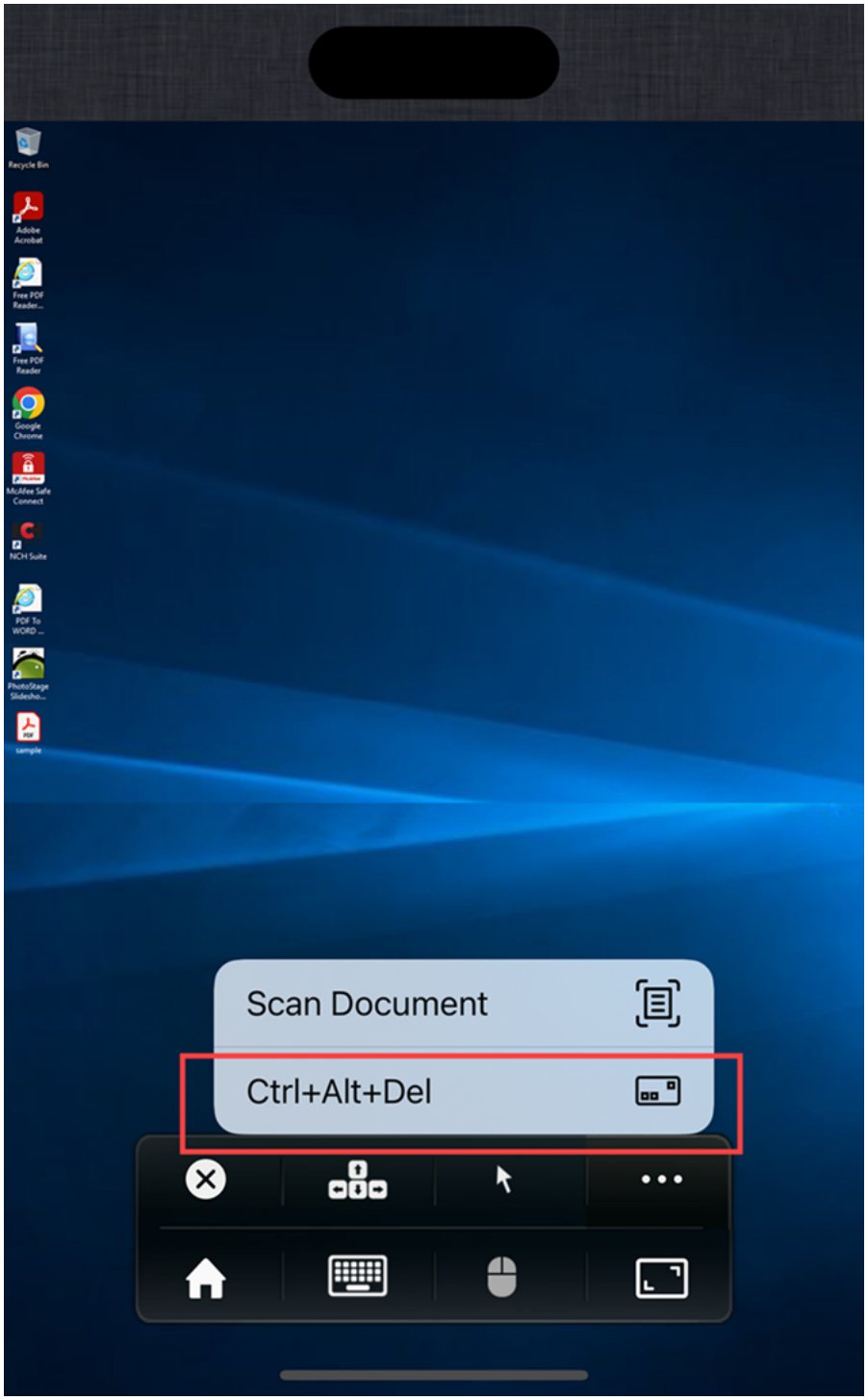
Prise en charge des imprimantes compatibles AirPrint Grâce aux imprimantes compatibles avec la technologie AirPrint, les utilisateurs peuvent désormais imprimer des documents à partir de leurs sessions actives sur des appareils iOS. Il n'est donc plus nécessaire de connecter les imprimantes via un câble ou un réseau. Les imprimantes compatibles AirPrint sont répertoriées avec les autres imprimantes disponibles une fois que les utilisateurs ont lancé une commande d'impression.

Pour imprimer à l'aide d'une imprimante compatible AirPrint, les utilisateurs doivent s'assurer des points suivants.

- L'imprimante requise doit être compatible avec la technologie AirPrint.
- L'appareil de l'utilisateur doit être connecté au même réseau Wi-Fi que l'imprimante compatible AirPrint.

Cette fonctionnalité est disponible pour les plateformes iOS dans les environnements cloud et sur site.

Ajout du raccourci Ctrl+Alt+Suppr à la barre d'outils de la session La barre d'outils de la session dispose désormais d'une option permettant d'exécuter la fonction **Ctrl+Alt+Suppr** en appuyant simplement sur un bouton. Cette option permet aux utilisateurs de se déconnecter, de changer d'utilisateur, de verrouiller le système ou d'accéder au Gestionnaire des tâches.



Authentification basée sur FIDO2 L'application Citrix Workspace pour iOS prend désormais en charge l'authentification sans mot de passe au sein d'une session Citrix Virtual Apps and Desktops à l'aide de méthodes d'authentification basées sur FIDO2. Cela permet aux utilisateurs de se connecter à un site Web compatible avec WebAuthn avec des navigateurs tels que Google Chrome ou Microsoft

Edge à l'aide de clés de sécurité Yubico compatibles avec FIDO2. Le simple fait d'ouvrir un site Web compatible avec WebAuthn déclenche une authentification sans mot de passe.

Seuls les appareils dotés de ports Lightning sont pris en charge (les appareils dotés de ports USB-C ou USB 4 ne sont pas pris en charge). La connexion à l'application Citrix Workspace ou à une session de bureau à l'aide d'une authentification sans mot de passe n'est pas prise en charge.

Pour plus d'informations sur les conditions requises pour cette fonctionnalité, consultez la section Autorisation locale et authentification virtuelle à l'aide de FIDO2 dans la documentation de Citrix Virtual Apps and Desktops.

Technical Preview

- Ajouter plusieurs magasins à l'aide de solutions Unified Endpoint Management (UEM)
- Supprimer plusieurs magasins à l'aide de solutions Unified Endpoint Management (UEM)

Pour obtenir la liste complète des fonctionnalités Technical Preview, consultez la page Fonctionnalités de la version Technical Preview.

Problèmes résolus

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

23.7.5

Nouveautés

Affichage de tous les certificats disponibles sur la carte à puce

L'application Citrix Workspace pour iOS affiche désormais plusieurs certificats disponibles sur la carte à puce et vous permet de sélectionner le certificat à utiliser pour l'authentification par carte à puce. Le certificat requis peut être sélectionné sur la page **Sélectionner un certificat** une fois que le bouton de la carte à puce a été activé.

Accès aux magasins Web compatibles avec Global App Configuration Service

Les administrateurs peuvent désormais configurer un magasin Web (interface Web) pour la découverte de magasins basée sur une adresse e-mail. Sur la base de l'adresse e-mail saisie par les utilisateurs lors de l'ajout d'un magasin (sur l'écran de bienvenue), Global App Configuration Service permet d'identifier l'URL Web (interface Web) personnalisée définie par l'administrateur. L'utilisateur est ensuite automatiquement dirigé vers le magasin Web configuré par l'administrateur.
Pour en savoir plus sur la configuration des URL des magasins Web pour les utilisateurs, consultez Allowed Custom Web Portal.

Annonce de fin de prise en charge de PNAgent

La fin de prise en charge du magasin PNA a été annoncée pour l'application Citrix Workspace pour iOS avec la version 23.7.5. Citrix ne prend pas en charge les corrections de bogues ni les correctifs de sécurité pour la fonctionnalité de magasin PNA après la version 23.7.5.

Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.6.5

Nouveautés

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.6.0

Nouveautés

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.5.0

Nouveautés

Améliorations apportées au clavier étendu À partir de la version 23.5.0, la fonctionnalité de clavier étendu a été améliorée pour offrir une meilleure expérience utilisateur. Les améliorations sont les suivantes :

- Possibilité d'épingler ou de détacher l'interface utilisateur de la barre d'outils étendue
- Possibilité de faire pivoter la barre d'outils étendue en phase avec la rotation de l'écran
- Prise en charge des raccourcis clavier Windows et des raccourcis utilisant une combinaison de 3 touches.
- Amélioration de l'expérience dans les scénarios dans lesquels plusieurs écrans sont utilisés
- Possibilité d'ouvrir ou de réduire automatiquement l'interface utilisateur de la barre d'outils étendue
- Amélioration de l'expérience du mode Stage Manager (sur iPad avec puce M1)

Problèmes résolus dans la version 23.5.0 Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.4.5

Nouveautés

Prise en charge des canaux de Global App Configuration Service À partir de la version 23.4.5, les administrateurs peuvent maintenant utiliser le Global App Configuration Service pour définir les paramètres et les tester avant de déployer la configuration auprès de tous les utilisateurs finaux. Ce processus garantit que les fonctionnalités ont été testées et validées avant le déploiement dans un environnement de production.

> **Remarque :**
>
> - L'application Citrix Workspace pour iOS prend en charge les configurations **Valeur par défaut** et **Canal de test**. Par défaut, tous les utilisateurs utilisent le canal **Valeur par défaut**.

Pour plus d'informations, consultez la documentation Global App Configuration Service.

Pour plus d'informations sur la configuration, consultez Prise en charge des canaux de Global App Configuration Service.

Prise en charge de la configuration du magasin à l'aide de solutions MDM L'application Citrix Workspace pour iOS prend désormais en charge la configuration à distance de l'URL de votre Workspace Store à l'aide de solutions de gestion des appareils mobiles (MDM). Pour plus d'informations, voir Configurer l'application Workspace à l'aide de solutions MDM.

Améliorations apportées aux solutions MDM L'application Citrix Workspace pour iOS prend en charge quelques configurations supplémentaires à l'aide de paires clé-valeur basées sur AppConfig pour configurer l'application Citrix Workspace. Auparavant, les administrateurs pouvaient configurer les URL des magasins. Les administrateurs peuvent désormais empêcher les utilisateurs finaux de modifier les URL des magasins et contrôler comment s'affiche l'application.

Configuration key	Value type	Configuration value
url	String	myworkprod0.cloud.com
restrict_user_store_modification	Boolean	true
storeType	Integer	1

Les détails sont les suivants :

Clé de configuration	Type de valeur	Valeur de configuration
`url`	`String`	URL du magasin. Par exemple, `prodcwa.cloud.com`
`storeType`	`Integer`	• (défaut) Si ce paramètre est défini sur 1, les utilisateurs peuvent voir le magasin natif ou par défaut. - Si ce paramètre est défini sur 2, les utilisateurs peuvent voir le magasin dans une interface Web.

Clé de configuration	Type de valeur	Valeur de configuration
restrict_user_store_modification	Booléen	• Si ce paramètre est défini sur **true**, les utilisateurs ne peuvent pas modifier le magasin (ajouter/supprimer/modifier). - Si ce paramètre est défini sur **false**, les utilisateurs peuvent modifier le magasin. **Remarque :** si l'indicateur est défini sur true, tous les magasins existants sont supprimés avant l'ajout d'un nouveau magasin configuré avec MDM.

Technical Preview

- Prise en charge de l'authentification FIDO2

Pour obtenir la liste complète des fonctionnalités préliminaires (version Technical Preview), consultez la page Fonctionnalités de la version Technical Preview.

Problèmes résolus dans la version 23.4.5

- Lorsque vous activez le mode de défilement naturel et que vous déplacez vos doigts du haut vers le bas de l'iPad, la page se déplace vers le bas. Le même comportement est observé même lorsque vous désactivez le défilement naturel. Ce comportement se produit également avec la Magic Mouse. [HDX-49267]
- En mode Étendre, lorsque vous utilisez les résolutions Ajustement automatique - Moyen ou Ajustement automatique - Élevé, la résolution de l'écran est redimensionnée automatiquement et l'affichage est tronqué. Ce problème se produit lorsque l'application Citrix Workspace passe de l'arrière-plan au premier plan. [CVADHELP-19169]

23.3.5

Nouveautés

Chaîne agent-utilisateur Par défaut, la chaîne agent-utilisateur utilisée lors de certaines requêtes réseau initiées via WKWebView inclut désormais l'identifiant de l'application Citrix Workspace.

Par conséquent, elle est passée de :
`Mozilla/5.0 (iPhone; CPU iPhone OS 15_2 like Mac OS X)AppleWebKit /605.1.15 (KHTML, like Gecko)Mobile/15E148 AuthManager/3.2.4.0`

À :

`Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X)AppleWebKit /605.1.15 (KHTML, like Gecko)Mobile/15E148 CWA/23.3.0 iOS/15.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone`
(Exemple d'iPhone)

Ou

`Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X)AppleWebKit /605.1.15 (KHTML, like Gecko)Mobile/15E148 CWA/23.3.0 iOS/15.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad`
(Exemple d'iPad)

Technical Previews

- Numérisation rapide

Pour obtenir la liste complète des fonctionnalités préliminaires (version Technical Preview), consultez la page Fonctionnalités de la version Technical Preview.

Problèmes résolus dans la version 23.3.5

Après la mise à niveau de l'application Citrix Workspace pour iOS vers la version 23.3.0, vous ne pouvez pas vous authentifier auprès de votre magasin si celui-ci est configuré à l'aide de l'adresse complète du magasin via une solution MDM.

23.3.0

Nouveautés

Prise en charge de la configuration du magasin à l'aide de solutions MDM [version Technical Preview]

> **Remarque :**
>
> Cette fonctionnalité est disponible en version préliminaire publique.

L'application Citrix Workspace pour iOS prend désormais en charge la configuration à distance de l'URL de votre Workspace Store à l'aide de solutions de gestion des appareils mobiles (MDM). Pour plus d'informations, voir Configurer l'application Workspace à l'aide de solutions MDM.

Réauthentification après expiration de la session Dans cette version, vous êtes désormais invité à vous réauthentifier auprès de l'application Citrix Workspace si votre session a expiré depuis votre dernière connexion. Vous êtes invité à utiliser une authentification à deux facteurs ou un nom d'utilisateur et un mot de passe lorsque vous vous connectez à l'application Citrix Workspace à partir du Web ou d'un client natif.

Technical Preview

- Scanner de documents
- Prise en charge du mode d'image en incrustation (PiP)

Pour obtenir la liste complète des fonctionnalités préliminaires (version Technical Preview), consultez la page Fonctionnalités de la version Technical Preview.

Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.2.1

Nouveautés

Support de caméra arrière L'application Citrix Workspace pour iOS permet désormais de changer la position de la caméra de l'avant vers l'arrière et inversement au cours d'une session HDX.

Lorsque vous invoquez la caméra dans la session virtuelle, un bouton flottant s'affiche à l'écran pour permettre le changement de position de la caméra. Vous pouvez également déplacer librement le bouton flottant sur l'écran et le placer n'importe où.

Pour changer la position de la caméra de l'avant vers l'arrière au cours d'une session virtuelle, procédez comme suit :

1. Ouvrez une application cliente qui capture des vidéos.
2. Démarrez l'enregistrement vidéo.
3. Touchez le bouton flottant de la caméra qui s'affiche à l'écran pour changer la position de la caméra de l'avant vers l'arrière.

> **Remarque :**
>
> les paramètres de l'application cliente n'ont aucun effet sur la caméra au cours d'une session HDX. Pour changer la position de la caméra, vous devez utiliser le bouton flottant de la caméra activé par Citrix.

Problèmes connus :

Le bouton flottant est partiellement ou totalement obstrué lorsque la fonction de casting ou de numérisation de documents est activée.

Prise en charge du remplissage automatique de l'URL du magasin Lorsque vous accédez à l'application Citrix Workspace pour iOS rebaptisée, vous pouvez choisir de renseigner automatiquement l'URL du magasin. Cette fonctionnalité réduit les interventions manuelles et offre un accès rapide à l'application. Pour plus d'informations sur la personnalisation des applications, consultez la section Personnalisation des applications.

Possibilité de changer de navigateur Web pour l'authentification Sur les appareils iOS ou iPad, les administrateurs peuvent maintenant changer le navigateur utilisé pour le processus d'authentification du navigateur intégré au navigateur système, lorsqu'une stratégie d'authentification avancée est configurée sur le déploiement local de Citrix Gateway et StoreFront. Pour plus d'informations, consultez Configurer une stratégie de réécriture pour le processus d'authentification.

Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

23.2.0

Nouveautés

Support de caméra arrière L'application Citrix Workspace pour iOS permet désormais de changer la position de la caméra de l'avant vers l'arrière et inversement au cours d'une session HDX.

Lorsque vous invoquez la caméra dans la session virtuelle, un bouton flottant s'affiche à l'écran pour permettre le changement de position de la caméra. Vous pouvez également déplacer librement le bouton flottant sur l'écran et le placer n'importe où.

Pour changer la position de la caméra de l'avant vers l'arrière au cours d'une session virtuelle, procédez comme suit :

1. Ouvrez une application cliente qui capture des vidéos.
2. Démarrez l'enregistrement vidéo.
3. Touchez le bouton flottant de la caméra qui s'affiche à l'écran pour changer la position de la caméra de l'avant vers l'arrière.

> **Remarque :**
>
> les paramètres de l'application cliente n'ont aucun effet sur la caméra au cours d'une session HDX. Pour changer la position de la caméra, vous devez utiliser le bouton flottant de la caméra activé par Citrix.

Problèmes connus :

Le bouton flottant est partiellement ou totalement obstrué lorsque la fonction de casting ou de numérisation de documents est activée.

Prise en charge du remplissage automatique de l'URL du magasin Lorsque vous accédez à l'application Citrix Workspace pour iOS rebaptisée, vous pouvez choisir de renseigner automatiquement l'URL du magasin. Cette fonctionnalité réduit les interventions manuelles et offre un accès rapide à l'application. Pour plus d'informations sur la personnalisation des applications, consultez la section Personnalisation des applications.

Possibilité de changer de navigateur Web pour l'authentification Sur les appareils iOS ou iPad, les administrateurs peuvent maintenant changer le navigateur utilisé pour le processus d'authentification du navigateur intégré au navigateur système, lorsqu'une stratégie d'authentification avancée est configurée sur le déploiement local de Citrix Gateway et StoreFront. Pour plus d'informations, consultez Configurer une stratégie de réécriture pour le processus d'authentification.

Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

Limitations

- Nous vous recommandons d'utiliser les touches **Ctrl+C** et **Ctrl+V** du clavier logiciel de votre appareil pour copier et coller. Les touches **Command+C** et **Command+V** sur un clavier externe peuvent ne pas fonctionner. [HDX-32431]

- Les tentatives de lancement d'une application en appuyant sur le fichier ICA dans le gestionnaire de téléchargement échouent lors de l'utilisation du navigateur Web Safari.
  Pour garantir le succès du lancement d'une application à partir de Safari, assurez-vous que la dernière version de l'application Citrix Workspace ou de Citrix Receiver pour iOS (mais pas les deux) est présente sur l'appareil. [RFIOS-5502]
- Après la migration vers Citrix Workspace depuis StoreFront, l'écran clignote momentanément lorsque vous appuyez sur le bouton **Suivant** dans le guide Pendo.
- Lors du démarrage d'applications Web et SaaS depuis l'application Citrix Workspace, si l'application utilise Google IdP et nécessite que l'utilisateur se connecte, l'authentification échouera et le message d'erreur « Accès refusé » s'affichera. [RFIOS-11904]

Fin de prise en charge

Pour plus d'informations sur les éléments obsolètes, consultez la page Fin de prise en charge.

Fonctionnalités de la version Technical Preview

July 1, 2024

Les fonctionnalités présentées dans les versions Technical Preview sont disponibles à des fins d'utilisation dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités présentées dans les versions Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut prendre en considération les commentaires en fonction de leur gravité, criticité et importance.

Liste des fonctionnalités de la version Technical Preview

Le tableau suivant répertorie les fonctionnalités de la version Technical Preview. Ces fonctionnalités sont des fonctionnalités de prévisualisation sur demande uniquement. Pour activer l'une de ces fonctionnalités et fournir des commentaires sur celles-ci, remplissez les formulaires correspondants.

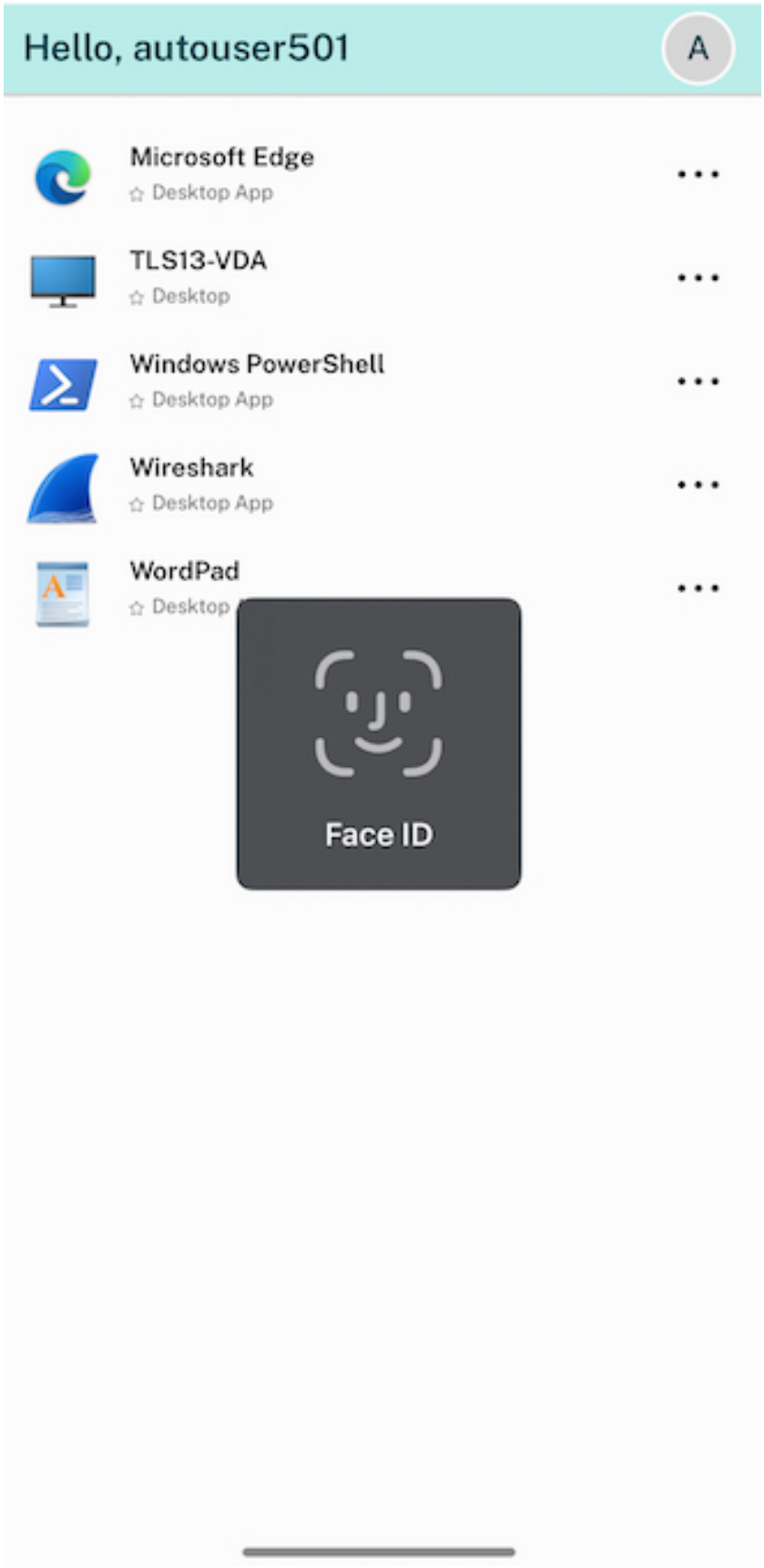
Titre	Disponible à partir de la version	Formulaire d'activation (cliquez sur l'icône)	Formulaire de commentaires (cliquez sur l'icône)
Prise en charge de l'application de l'authentification biométrique pour accéder à l'application Citrix Workspace	2405		
Prise en charge de l'authentification unique pour les machines virtuelles associées à Microsoft Entra ID	2405		
Prise en charge de la configuration des paramètres de l'application Citrix Workspace via UEM	24.3.5		
Prise en charge de l'audio adaptatif	24.3.0		
Prise en charge des fonctionnalités d'accessibilité et VoiceOver	24.2.0		
Prise en charge de la webcam externe	23.12.0		

Titre	Disponible à partir de la version	Formulaire d'activation (cliquez sur l'icône)	Formulaire de commentaires (cliquez sur l'icône)
Ajouter plusieurs magasins à l'aide de solutions Unified Endpoint Management (UEM)	23.9.0		
Supprimer plusieurs magasins à l'aide de solutions Unified Endpoint Management (UEM)	23.9.0		
Numérisation rapide	23.3.5		
Prise en charge du mode d'image en incrustation (PiP)	23.3.0		
Prise en charge du mode non-miroir natif d'Apple	23.3.0		
Prise en charge d'une expérience d'authentification unique (SSO) améliorée pour les applications Web et SaaS	23.3.0		

Prise en charge de l'application de l'authentification biométrique pour accéder à l'application Citrix Workspace

Technical Preview de la version 2405	Formulaire d'activation	Formulaire de commentaires

À partir de la version 24.5.0, les administrateurs peuvent désormais appliquer l'authentification biométrique d'un appareil pour accéder à l'application Citrix Workspace pour leurs utilisateurs. Grâce à cette fonctionnalité, lorsque vous ouvrez l'application Citrix Workspace après l'avoir supprimée ou que vous la mettez au premier plan après l'avoir réduite, une invite de vérification par Face ID ou Touch ID apparaît pour déverrouiller et vous connecter. Si l'appareil ne prend pas en charge l'authentification biométrique, la méthode d'authentification par mot de passe ou code secret est utilisée pour accéder à l'application. Si le code secret n'est pas activé sur l'appareil, le compte est déconnecté, ce qui oblige l'utilisateur à se reconnecter pour accéder à l'application Citrix Workspace.



Les administrateurs peuvent configurer cette fonctionnalité à l'aide de la solution Unified Endpoint Management avec les paires clé-valeur suivantes :

- **clé**: verify_biometric_on_app_foreground_transition
- **type de valeur :** booléen
- **valeur :** true ou false
  - Si ce paramètre est défini sur **true**, l'authentification biométrique est requise pour que les utilisateurs finaux puissent accéder à l'application Citrix Workspace.
  - Si ce paramètre est défini sur **false**, l'authentification biométrique n'est pas appliquée pour accéder à l'application Citrix Workspace. Les utilisateurs ont la possibilité de désactiver l'authentification biométrique.

Prise en charge de l'authentification unique pour les machines virtuelles associées à Microsoft Entra ID

Technical Preview de la version 2405	Formulaire d'activation	Formulaire de commentaires

À partir de la version 24.5.0, l'application Citrix Workspace pour iOS permet aux utilisateurs de se connecter à des machines virtuelles jointes à Azure AD à l'aide de l'authentification unique. Vous devez fournir des informations d'identification Microsoft lorsque vous vous connectez à une machine virtuelle jointe à Azure AD pour la première fois. Pour les connexions suivantes, les informations d'identification ne sont pas requises avant l'expiration du jeton.

> **Remarque :**
>
> - Si l'utilisateur n'utilise pas **WKwebview** pour l'authentification, les informations d'identification doivent être saisies pour la première fois.
> - Cette fonctionnalité s'applique uniquement aux magasins cloud.

Prise en charge de la configuration des paramètres de l'application Citrix Workspace via UEM

Technical Preview de la version 24.3.5	Formulaire d'activation	Formulaire de commentaires

Auparavant, vous ne pouviez configurer l'URL du magasin dans l'application Citrix Workspace qu'à l'aide d'une solution Unified Endpoint Management (UEM).

À partir de la version 24.3.5, vous pouvez également configurer les paramètres de l'application Citrix Workspace sur les appareils gérés à l'aide de n'importe quelle solution UEM déployée dans votre infrastructure.

> **Remarque :**
>
> En tant qu'administrateur, si vous avez la possibilité de configurer les paramètres de l'application Citrix Workspace à l'aide d'UEM et du Global App Configuration Service (GACS), UEM a toujours la préférence sur GACS.

Voici un exemple de fichier JSON permettant de configurer les paramètres de l'application Citrix Workspace :

```
<dict>
    <key>stores</key>
    <array>
        <dict>
            <key>url</key>
            <string>https://teststore.cloud.com</string>
            <key>storeType</key>
            <integer>1</integer>
            <key>displayName</key>
            <string>Cloud Store 1</string>
            <key>appSettings</key>
            <array>
                <dict>
                    <key>category</key>
                    <string>audio</string>
                    <key>userOverride</key>
                    <false/>
                    <key>settings</key>
                    <array>
                        <dict>
                            <key>name</key>
                            <string>settings_audio_stream</string>
                            <key>value</key>
                            <true/>
                        </dict>
                    </array>
                </dict>
                <dict>
                    <key>category</key>
                    <string>authentication</string>
                    <key>userOverride</key>
                    <false/>
                    <key>settings</key>
                    <array>
                        <dict>
                            <key>name</key>
                            <string>settings_auth_web_browser</string>
                            <key>value</key>
                            <string>embedded</string>
```



```
                        </dict>
                    </array>
                </dict>
            </array>
        </dict>
        <dict>
            <key>url</key>
            <string>https://teststore.cloud.com</string>
            <key>storeType</key>
            <integer>1</integer>
            <key>displayName</key>
            <string>StoreFront1</string>
            <key>appSettings</key>
            <array>
                <dict>
                    <key>category</key>
                    <string>audio</string>
                    <key>userOverride</key>
                    <false/>
                    <key>settings</key>
                    <array>
                        <dict>
                            <key>name</key>
                            <string>settings_audio_stream</string>
                            <key>value</key>
                            <false/>
                        </dict>
                    </array>
                </dict>
                <dict>
                    <key>category</key>
                    <string>authentication</string>
                    <key>userOverride</key>
                    <false/>
                    <key>settings</key>
                    <array>
                        <dict>
                            <key>name</key>
                            <string>settings_auth_web_browser</string>
                            <key>value</key>
                            <string>system</string>
                        </dict>
                    </array>
                </dict>
            </array>
        </dict>
    </array>
    <key>storesToDelete</key>
    <array>
        <string>test.cldblr.com</string>
        <string>test.cloud.com</string>
    </array>
    <key>restrict_user_store_modification</key>
```



```
93      <false/>
94  </dict>
95  <!--NeedCopy-->
```

> **Remarque :**
>
> L'indicateur `userOverride` permet à l'utilisateur de modifier les paramètres de l'application Citrix Workspace. Si l'indicateur `userOverride` est défini sur true, l'utilisateur peut modifier les paramètres. Si l'indicateur `userOverride` est défini sur false pour tous les paramètres, l'utilisateur ne peut pas le modifier dans les paramètres de l'application Citrix Workspace.

Tableau des paires clé-valeur

Le tableau suivant fournit des informations sur les paires clé-valeur :

> **Remarque :**
>
> Vous devez ajouter des paramètres spécifiques à une catégorie dans un bloc unique sous cette catégorie.

Catégorie	Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut
Audio	Audio	Permet aux utilisateurs d'activer ou de désactiver le son depuis l'application ou le bureau virtuel.	settings_audio_state	true/false	Booléen	TRUE
Clavier	Utiliser clavier Unicode	Permet aux utilisateurs d'utiliser un clavier Unicode standard.	settings_use_unicode_keyboard	true/false	Booléen	TRUE

Catégorie	Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut
Clavier	Clavier automatique	Active ou désactive l'affichage automatique du clavier dans la session.	settings_automatic_keyboard	true/false	Booléen	TRUE
Clavier	Synchronisation de la disposition du clavier	Permet aux utilisateurs de basculer vers une disposition de clavier préférée sur l'appareil.	settings_keyboard_layout_sync	true/false	Booléen	FAUX
Clavier	Utiliser des claviers personnalisés	Permet aux utilisateurs d'utiliser des claviers tiers téléchargés dans une session virtuelle.	settings_allow_keyboard_extensions	true/false	Booléen	FAUX
display	Résolution de la session	Permet aux utilisateurs de sélectionner la résolution d'écran.	settings_resolution	0–9	Entier	5 (iPad) 3 (iPhone)

Catégorie	Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut
display	Mode de présentation	Permet d'utiliser votre appareil iOS comme trackpad pour contrôler la session tout en utilisant un écran externe.	settings_presentationMode	true/false	Booléen	FAUX
display	Affichage externe	Connectez un écran externe à l'appareil.	settings_externalDisplay	true/false	Booléen	TRUE
advanced	Validation stricte des certificats	Applique un contrôle plus strict de la validation du certificat de serveur.	settings_strictCertValidation	True/False	Booléen	FAUX
advanced	Versions TLS	Permet aux utilisateurs de modifier leurs paramètres TLS à des fins de dépannage.	settings_tlsVersion	0–3	Entier	0

Catégorie	Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut
advanced	Utiliser liste déroulante native	Permet d'utiliser la fonctionnalité de sélection native iOS.	settings_native_combobox	true/false	Booléen	TRUE
advanced	Tactile (iPad uniquement)	Active la fonctionnalité tactile pour toutes les applications et tous les bureaux, y compris ceux pour lesquels l'option tactile n'est pas activée en mode natif.	settings_multitouch	true/false	Booléen	true (iPad) false (iPhone)
advanced	Affichage plein écran	Permet d'afficher vos applications et vos postes de travail en plein écran.	settings_mobile_view_full_screen	true/false	Booléen	true (iPad) false (iPhone)

Catégorie	Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut
advanced	Reconnecter lors de la connexion	Permet à une session de se reconnecter automatiquement lorsqu'un nouveau compte est ajouté ou lors de la connexion.	settings_reconnect_logon	true/false	Booléen	FAUX
advanced	Reconnecter lors de l'actualisation	Se reconnecte automatiquement à une session lancée à partir d'un autre appareil lors de l'actualisation des applications ou des bureaux sur le deuxième appareil.	settings_reconnect_refresh	true/false	Booléen	FAUX
advanced	Activer le proxy HTTP	Permet d'utiliser le proxy HTTP pour une session.	settings_use_local_proxy	true/false	Booléen	TRUE

Catégorie	Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut
advanced	Utiliser informations d'identification dérivées	Permet d'utiliser des informations d'identification dérivées.	setting_useDerivedCredentials	true/false	Booléen	FAUX
advanced	Carte à puce dans une session	Permet l'utilisation d'une carte à puce au cours d'une session. Ce paramètre n'autorise pas les utilisateurs à s'authentifier auprès de la session.	settings_usesSmartCardInSession	true/false	Booléen	FAUX
advanced	Autoriser EDT	Active la prise en charge du transport adaptatif.	settings_allowUdp	true/false	Booléen	TRUE

Catégorie	Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut
advanced	Mode tablette automatique	Permet de lancer la session virtuelle en mode tablette, lorsqu'aucun clavier ou souris externe n'est détecté.	settings_enableTabletModeSwitch	true/false	Booléen	TRUE
advanced	Garder l'écran activé	Maintient l'écran allumé.	settings_stay_awake	true/false	Booléen	FAUX
advanced	Utiliser stockage de l'iPad	Permet d'accéder aux lecteurs locaux de votre appareil.	settings_clienttdrive	true/false	Booléen	false
Souris X1	Autoriser la souris X1	Permet de basculer vers votre souris Citrix X1.	settings_allowtX1e_mouse	true/false	Booléen	FAUX
Souris X1	Vitesse de la souris Citrix X1	Permet aux utilisateurs de contrôler la vitesse du curseur de la souris dans la session virtuelle.	settings_x1MouseSpeed	1,2	Entier	200 (iPadPro) 100 (tous les autres appareils)

Catégorie	Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut
Souris X1	Utiliser l'image du curseur distant pour la souris Citrix X1	Fait correspondre le curseur à l'application ou au bureau dans une session. Par exemple, si le curseur se trouve sur une zone de texte, il change pour correspondre à la zone de texte.	settings_X1_mouse_server_side_cursor	true/false	Booléen	TRUE
authentication	Navigateur Web pour l'authentification	Permet d'identifier l'utilisation de SafariViewController au lieu de WKWeb sur l'appareil.	settings_auth_system_browser	embedded/system	Chaîne	Embedded

Catégorie	Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut
thirdPartyServices	LaunchDarkly	Active l'indicateur Launch-Darkly sur les fonc-tionnalités de l'application Citrix Workspace.	enableLaunchDarkly	true/false	Booléen	true (régions hors UE)

Prise en charge de l'audio adaptatif

Technical Preview de la version 24.3.0	Formulaire d'activation	Formulaire de commentaires

À partir de la version 24.3.0, l'application Citrix Workspace pour iOS prend en charge l'audio adaptatif HDX. Cette fonctionnalité améliore l'expérience utilisateur en fournissant une meilleure qualité audio et une faible latence.

Pour plus d'informations, consultez l'article sur les Paramètres de stratégie audio dans la documentation Citrix Virtual Apps and Desktops.

Prise en charge des fonctionnalités d'accessibilité et VoiceOver

Technical Preview de la version 24.2.0	Formulaire d'activation	Formulaire de commentaires

À partir de la version 24.2.0, l'application Citrix Workspace pour iOS prend en charge les fonctionnalités d'accessibilité et VoiceOver. Ces fonctionnalités améliorent l'expérience des utilisateurs qui ont des difficultés à voir l'écran. Lorsque vous utilisez Citrix Workspace et l'interface utilisateur des sessions virtuelles, le narrateur lit les éléments de l'écran à haute voix.

Pour activer la fonctionnalité VoiceOver, accédez à **Paramètres iOS > Accessibilité > VoiceOver**.

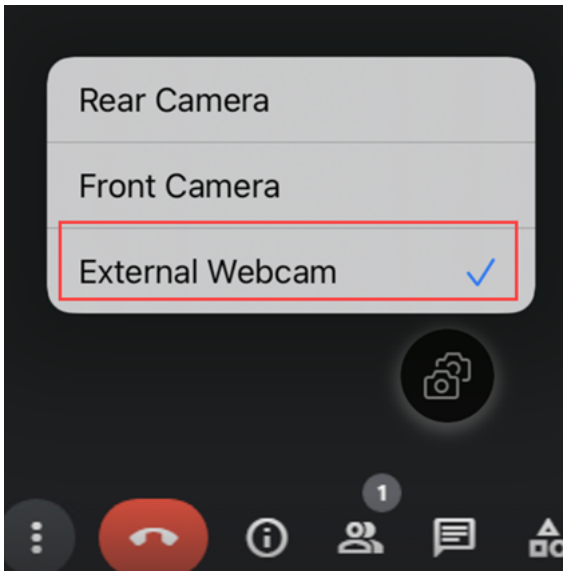
Pour interagir avec l'application Citrix Workspace, vous devez utiliser les gestes standards d'accessibilité fournis par iOS. Par exemple, vous pouvez balayer l'écran vers la gauche et la droite afin de naviguer entre les menus pendant la narration en voix-off de chaque élément. Pour plus d'informations, consultez les pages Premiers pas avec les fonctionnalités d'accessibilité sur l'iPhone et Premiers pas avec les fonctionnalités d'accessibilité sur l'iPad dans la documentation d'assistance Apple.

Prise en charge de la webcam externe

Technical Preview de la version 23.12.0	Formulaire d'activation	Formulaire de commentaires

L'application Citrix Workspace pour iOS prend désormais en charge les webcams connectées en externe lors de vos sessions DaaS. Connectez une webcam via USB et utilisez-la pour la visioconférence en cliquant sur l'icône de la caméra, puis en sélectionnant l'option **Webcam externe**. Cela améliore l'expérience de session des utilisateurs en utilisant des ressources qui leur sont disponibles.

> **Remarque :**
>
> - La webcam externe n'est compatible qu'avec les iPad exécutant iOS 17 ou une version ultérieure et dotés d'un connecteur USB-C.
> - L'option Webcam externe ne s'affiche que lorsqu'une caméra externe est détectée.
> - Au cours d'une session HDX, les paramètres de l'application cliente n'ont aucun effet sur la caméra. Pour changer la position de la caméra, vous devez utiliser le bouton flottant de la caméra activé par Citrix.



La prochaine fois que vous utiliserez une application de visioconférence, le système mémorisera et appliquera les préférences d'utilisation de la caméra. Par exemple, si vous avez effectué votre dernier appel vidéo avec la préférence **Webcam externe**, la prochaine fois, la Webcam externe sera sélectionnée par défaut.

Vous pouvez modifier vos préférences de caméra en appuyant sur l'icône de la caméra affichée sur votre écran. Il est également possible de modifier les préférences de caméra pendant les appels.

Cette fonctionnalité est disponible pour les clients dans les magasins cloud et locaux.

Ajouter plusieurs magasins à l'aide de solutions Unified Endpoint Management (UEM)

Technical Preview de la version 23.12.0	Formulaire d'activation	Formulaire de commentaires

Les administrateurs peuvent utiliser les solutions Unified Endpoint Management (UEM) pour configurer et ajouter plusieurs magasins pour les appareils iOS gérés. Les informations de chaque magasin peuvent être ajoutées à un fichier XML. Ce fichier XML peut ensuite être chargé lors de la configuration de la stratégie de configuration de l'application.

> **Remarque :**
>
> Le fichier XML doit être au format clé-valeur.

Clé de configuration	Type de valeur	Description
url	Chaîne	URL du magasin. Par exemple, exemple.cloud.com
storeType (facultatif)	Entier	Si ce paramètre est défini sur **1**, les utilisateurs peuvent voir le magasin natif ou par défaut. Si ce paramètre est défini sur **2**, les utilisateurs peuvent voir le magasin dans une interface Web.
displayName (facultatif)	Chaîne	Nom du magasin.

Clé de configuration	Type de valeur	Description
restrict_user_store_modification (facultatif)	Booléen	Si ce paramètre est défini sur **true**, les utilisateurs ne peuvent pas modifier le magasin (ajouter/supprimer/modifier). Si ce paramètre est défini sur **false**, les utilisateurs peuvent modifier le magasin (ajouter/supprimer/modifier).

> **Important**
>
> - Si le paramètre **restrict_user_store_modification** est défini sur **true**, tous les magasins existants sont supprimés avant l'ajout d'un nouveau magasin configuré pour la gestion unifiée des terminaux.
> - Si le paramètre storeType n'est pas fourni, l'interface par défaut est considérée comme native.

Exemple de configuration XML pour ajouter des magasins

Reportez-vous à cet exemple de fichier XML pour plus d'informations.

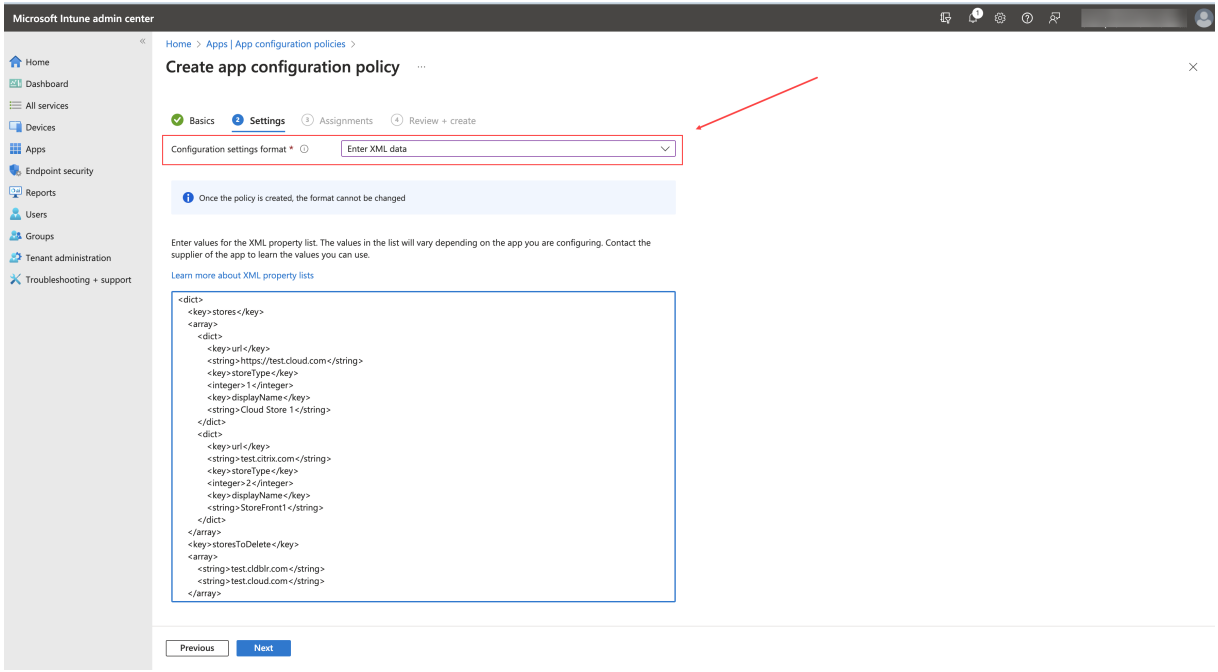
```
<dict>
    <key>stores</key>
    <array>
        <dict>
            <key>url</key>
            <string>test.cloud.com</string>
            <key>storeType</key>
            <integer>1</integer>
            <key>displayName</key>
            <string>Cloud Store </string>
        </dict>
        <dict>
            <key>url</key>
            <string>test.citrix.com</string>
            <key>storeType</key>
            <integer>2</integer>
            <key>displayName</key>
            <string>StoreFront</string>
        </dict>
    </array>
        <key>restrict_user_store_modification</key>
    <true/>
```



```
    </dict>

<!--NeedCopy-->
```

Une fois que le fichier XML est prêt avec la configuration du magasin, les administrateurs peuvent le charger sur la page **Créer une stratégie de configuration d'application**. Par exemple, dans Microsoft Intune, les administrateurs doivent sélectionner l'option **Entrer des données XML** dans la liste déroulante **Format des paramètres de configuration**.



Supprimer plusieurs magasins à l'aide de solutions Unified Endpoint Management (UEM)

Technical Preview de la version 23.12.0	Formulaire d'activation	Formulaire de commentaires

Les administrateurs doivent ajouter une liste de magasins à supprimer dans un fichier XML portant le nom de clé **storesToDelete** pour supprimer un ou plusieurs magasins.

Exemple de configuration XML pour supprimer des magasins

Reportez-vous à cet exemple de fichier XML pour plus d'informations.

```
    <dict>
        <key>storesToDelete</key>
```



```
    <array>
        <string>test.cldblr.com</string>
        <string>test.onprem.com</string>
    </array>
   </dict>

<!--NeedCopy-->
```

Vous trouverez ci-dessous un exemple de fichier de configuration XML contenant la configuration pour l'ajout et la suppression de magasins.

```
        <dict>
        <key>stores</key>
        <array>
            <dict>
                <key>url</key>
                <string>test.cloud.com</string>
                <key>storeType</key>
                <integer>1</integer>
                <key>displayName</key>
                <string>Cloud Store </string>
            </dict>
            <dict>
                <key>url</key>
                <string>test.citrix.com</string>
                <key>storeType</key>
                <integer>2</integer>
                <key>displayName</key>
                <string>StoreFront</string>
            </dict>
        </array>
        <key>storesToDelete</key>
        <array>
            <string>test.cldblr.com</string>
            <string>test.onprem.com</string>
        </array>
        <key>restrict_user_store_modification</key>
        <true/>
    </dict>

<!--NeedCopy-->
```

Numérisation rapide

Technical Preview de la version 23.3.5	Formulaire d'activation	Formulaire de commentaires

Si vous êtes connecté à l'application Citrix Workspace sur plusieurs appareils, vous pouvez utiliser

la fonctionnalité de numérisation rapide pour numériser plusieurs documents à l'aide d'un appareil iOS. Transférez ensuite ces documents numérisés vers un appareil iOS.

Pour obtenir des instructions sur l'utilisation de la fonction Numérisation rapide pour numériser des documents, procédez comme suit :

1. Sur votre Mac, cliquez avec le bouton droit sur l'icône de l'application Citrix Workspace dans votre session de bureau et cliquez sur **Numérisation rapide**. Un code QR s'affiche.
2. Sur votre appareil iOS, cliquez sur **Réglages** > **Numérisation rapide**.
3. Scannez le code QR affiché sur votre Mac pour établir la connexion entre votre Mac et les appareils iOS.
4. Numérisez n'importe quel document et envoyez-le sur votre Mac.
5. Dans votre session de bureau sur Mac, vous pouvez localiser les documents que vous avez numérisés dans le Finder.

Logiciels requis

- Le mappage des lecteurs clients (CDM) doit être activé pour le magasin.
- Vous devez être connecté au même compte dans l'application Citrix Workspace sur votre appareil iOS et votre Mac.
- Vous devez être connecté au même réseau Wi-Fi.
- La version minimale requise de l'application Citrix Workspace pour Mac est 2304.
- La numérisation rapide nécessite un accès en lecture et en écriture sur votre appareil. Pour donner accès, procédez comme suit :

    1. Dans votre profil, cliquez sur **Paramètres de l'application** > **Paramètres du magasin**.
    2. Cliquez sur votre magasin actuel.
    3. Cliquez sur **Stockage de l'appareil** et sélectionnez **Accès en lecture et en écriture**.

Prise en charge du mode d'image en incrustation (PiP)

Technical Preview de la version 23.3.0	Formulaire d'activation	Formulaire de commentaires

L'application Citrix Workspace pour iOS prend en charge le mode d'image en incrustation (Picture-in-Picture, PiP), qui vous permet de réduire votre session de bureau, votre application SaaS ou votre application Web à une fenêtre flottante. Vous pouvez déplacer cette fenêtre librement sur l'écran et la placer n'importe où. Le mode PiP libère l'écran d'accueil de l'application Citrix Workspace pour que vous puissiez effectuer d'autres tâches. Cliquez sur le bouton **Accueil** dans la barre d'outils de votre session de bureau, ou sur le **menu à points de suspension (…)** > **Réduire** dans votre application SaaS

ou Web pour réduire l'écran. Cliquez sur la fenêtre flottante pour afficher l'application en plein écran et fermez l'application en cliquant sur l'icône **X** de la fenêtre flottante. La fenêtre flottante apparaît automatiquement en plein écran lorsque vous réduisez une autre application.

Cette fonctionnalité est prise en charge à la fois pour les déploiements sur site et dans le cloud. Toutefois, pour les déploiements dans le cloud, les applications Web peuvent être réduites à une image en incrustation. Vous pouvez également basculer entre une session de bureau et une application Web en cliquant sur la fenêtre flottante.

> **Remarque :**
>
> Vous ne pouvez garder que deux applications actives à la fois. L'une en mode plein écran et l'autre réduite en PiP :
>
> - 2 applications Web ou SaaS
> - 1 application Web ou SaaS et 1 session de bureau ou application virtuelle

Limitations connues :

- Le mode PiP n'est pas disponible lorsque des périphériques externes sont connectés, tels qu'une souris, un clavier ou un moniteur externe.
- Si le mode PiP est activé et que votre appareil est connecté à un moniteur externe, l'application Citrix Workspace ne répond pas et le bouton de retour n'est pas disponible dans les **paramètres d'affichage** de la session de bureau.

Compatibilité avec le mode non-miroir natif d'Apple

Technical Preview de la version 22.12.0	Formulaire d'activation	Formulaire de commentaires

Vous pouvez désormais étendre l'affichage à l'aide du mode non-miroir d'Apple, disponible avec iPad OS 16.2. Vous pouvez effectuer plusieurs tâches à la fois en exécutant l'application Citrix Workspace, des applications virtuelles et des bureaux virtuels sur le moniteur externe et en laissant l'écran de l'iPad libre pour exécuter d'autres applications natives.

> **Remarque :**
>
> La prise en charge de l'affichage étendu en mode non-miroir d'Apple n'est disponible que sur certains modèles d'iPad. Pour plus d'informations, consultez la documentation Apple.

Si vous ne souhaitez pas utiliser cette fonctionnalité de Technical Preview, vous pouvez toujours utiliser l'application Citrix Workspace en mode plein écran.

Prise en charge d'une expérience d'authentification unique (SSO) améliorée pour les applications Web et SaaS

Technical Preview de la version 22.3.5	Formulaire d'activation	Formulaire de commentaires

Cette fonctionnalité simplifie la configuration du SSO pour les applications Web internes et les applications SaaS lors de l'utilisation de fournisseurs d'identité tiers (IdP). L'expérience SSO améliorée réduit l'ensemble du processus à quelques commandes. Elle élimine le besoin de configurer Citrix Secure Private Access dans la chaîne du fournisseur d'identité pour configurer SSO. Cela améliore également l'expérience utilisateur, à condition que le même IdP soit utilisé pour l'authentification à la fois auprès de l'application Workspace et de l'application Web ou SaaS qui est lancée.

De la version préliminaire (version Technical Preview) à la disponibilité générale (GA)

Service ou fonctionnalité	Version en disponibilité générale
Prise en charge des scanners de documents	24.5.0
Prise en charge de l'authentification FIDO2	23.9.0

Configuration système requise et compatibilité

March 29, 2024

Configuration requise par l'appareil

- L'application Citrix Workspace pour iOS version 23.9.0 ou versions supérieures prend en charge iOS 17 et iPadOS 17.
- L'application Citrix Workspace pour iOS version 22.9.0 ou versions supérieures prend en charge iOS 16 et iPadOS 16.
- L'application Citrix Workspace pour iOS version 21.9.1 ou versions supérieures prend en charge iOS 15 et iPadOS 15.
- L'application Citrix Workspace pour iOS version 20.9.0 ou versions supérieures prend en charge iOS 14 et iPadOS 14.

- Cette mise à jour logicielle a été validée sur les appareils suivants :
  - Modèles iPhone 7x, modèles iPhone 8x et modèle iPhone X uniquement.
  - Tous les modèles d'iPad (y compris l'iPad Pro) à l'exception de l'iPad 1 et iPad 2 qui ne sont pas pris en charge.
- Prise en charge de moniteurs externes
  - iPhone - même prise en charge que iOS.
  - iPad - si pris en charge par iOS (n'utilise pas l'écran entier).

Éléments requis sur les serveurs

Vérifiez que vous avez installé tous les derniers correctifs logiciels pour vos serveurs.

- Pour les connexions aux applications et bureaux virtuels, l'application Citrix Workspace prend en charge Citrix StoreFront et l'Interface Web.

  StoreFront :

  - StoreFront 3.6 ou versions ultérieures (recommandé). L'application Citrix Workspace a été validée avec la dernière version de StoreFront ; les versions précédentes prises en charge comprennent StoreFront 2.6 ou versions supérieures.

    Permet d'accéder directement aux magasins StoreFront. L'application Citrix Workspace prend également en charge les versions antérieures de StoreFront.

    > **Remarque :**
    >
    > Avec XenApp et XenDesktop 7.8, Citrix a introduit la prise en charge du canal virtuel Framehawk et de 3D Pro. Cette fonctionnalité a été étendue à l'application Citrix Workspace.

  - StoreFront configuré avec un site Workspace pour Web.

    Permet d'accéder aux magasins StoreFront à partir d'un navigateur Web Safari. Les utilisateurs doivent ouvrir le fichier ICA manuellement à l'aide du navigateur. Pour prendre connaissance des limitations de ce déploiement, consultez la documentation de StoreFront.

  Interface Web :

  - Interface Web 5.4 avec des sites Interface Web
  - Interface Web 5.4 avec sites XenApp et XenDesktop
  - Interface Web sur Citrix Gateway (accès par navigateur Safari uniquement)

    Activez les stratégies de réécriture fournies par Citrix Gateway.

- **Citrix Virtual Apps and Desktops**, **XenApp** et **XenDesktop** (l'un des produits suivants) :
  - Citrix Virtual Apps and Desktops 7 1808 ou version ultérieure
  - Citrix XenDesktop 7.x ou version ultérieure
  - Citrix XenApp 7.5 ou version ultérieure

Connexions, certificats et authentification

Pour les connexions à StoreFront, l'application Citrix Workspace prend en charge les méthodes d'authentification suivantes :

	Workspace pour Web utilisant des navigateurs	Site StoreFront Services (natif)	Site StoreFront XenApp et XenDesktop (natif)	Citrix Gateway auprès de Workspace pour Web (navigateur)	Citrix Gateway auprès du site StoreFront Services (natif)
Anonyme	Oui	Oui			
Domaine	Oui	Oui	Oui	Oui*	Oui*
Authentification pass-through au domaine	Oui	Oui	Oui		
Jeton de sécurité				Oui*	Oui*
Authentification à deux facteurs (domaine avec jeton de sécurité)				Oui*	Oui*
SMS				Oui*	Non
Carte à puce		Oui		Oui*	Oui*
Certificat utilisateur				Oui (Citrix Gateway Plug-in)	Oui (Citrix Gateway Plug-in)

*Disponible uniquement pour :

- Workspace pour sites Web.

- Déploiements incluant Citrix Gateway, avec ou sans l'installation du plug-in associé installé sur la machine.

> **Remarque :**
>
> Le plug-in EPA (End-Point Analysis) de Citrix Gateway est pris en charge sur Citrix Workspace. Sur l'application Citrix Workspace native, il n'est pris en charge que si l'authentification nFactor est utilisée. Pour plus d'informations, consultez Configurer l'analyse EPA pré-authentification et post-authentification en tant que facteur dans l'authentification nFactor dans la documentation Citrix ADC.

Pour les connexions à l'Interface Web 5.4, l'application Citrix Workspace prend en charge les méthodes d'authentification suivantes :

> **Remarque :**
>
> L'Interface Web utilise le terme Explicite pour représenter l'authentification par jeton de sécurité et domaine.

	Interface Web (navigateurs)	Site Interface Web XenApp et XenDesktop	Citrix Gateway vers Interface Web (navigateur)	Citrix Gateway vers site Interface Web XenApp et XenDesktop
Anonyme	Oui			
Domaine	Oui	Oui	Oui*	
Authentification pass-through au domaine	Oui			
Jeton de sécurité			Oui*	
Authentification à deux facteurs (domaine avec jeton de sécurité)			Oui*	
SMS			Oui*	
Carte à puce				
Certificat utilisateur			Oui (requiert Citrix Gateway Plug-in)	

Certificats

Certificats privés (auto-signés) Vous pouvez accéder aux ressources Citrix à l'aide de l'application Citrix Workspace :

- lorsqu'un certificat privé est installé sur la passerelle distante ;
- lorsque le certificat racine de l'autorité de certification de l'organisation est installé sur l'appareil.

> **Remarque :**
>
> Un avertissement de certificat non approuvé s'affiche si le certificat de la passerelle distante ne peut pas être vérifié lors de la connexion. Ce problème est dû au fait que le certificat racine n'est pas inclus dans le keystore local. Si un utilisateur choisit d'ignorer l'avertissement, une liste des applications s'affiche ; toutefois, les applications ne démarrent pas.

Certificats installés manuellement Dans iOS 10.3 et versions ultérieures, un certificat inclus dans un profil que vous installez manuellement n'est pas automatiquement approuvé pour SSL. Pour faire confiance aux profils de certificat installés manuellement dans iOS :

1. Assurez-vous que vous avez installé le profil de certificat sur l'appareil.
2. Accédez à **Réglages** > **Général** > **Informations** > **Réglages des certificats**.

   Chaque racine installée via un profil apparaît sous **Activer la confiance totale pour les certificats racine**.
3. Vous pouvez activer ou désactiver la confiance pour chaque racine.

Importation de certificats racine sur iPad et iPhone Obtenez le certificat racine auprès de l'émetteur du certificat et envoyez-le par e-mail à un compte de messagerie configuré sur votre appareil. Lorsque vous cliquez sur la pièce jointe, vous êtes invité à importer le certificat racine.

Certificats génériques Les certificats génériques remplacent les certificats de serveur individuel pour n'importe quel serveur situé dans le même domaine. L'application Citrix Workspace prend en charge les certificats génériques.

Certificats intermédiaires et Citrix Gateway Si votre chaîne de certificat contient un certificat intermédiaire, ce dernier doit être ajouté au certificat du serveur Citrix Gateway (ou Access Gateway). En outre, pour les installations d'Access Gateway, consultez la section Installer, lier et mettre à jour des certificats correspondant à vos exigences dans la documentation de Citrix ADC.

L'authentification RSA SecurID est prise en charge pour les configurations Secure Gateway (via l'Interface Web uniquement) et toutes les configurations Access Gateway prises en charge.

L'application Citrix Workspace prend en charge toutes les méthodes d'authentification prises en charge par Access Gateway.

Stratégie de validation des certificats de serveur Les versions de l'application Citrix Workspace disposent d'une stratégie de validation des certificats de serveur plus stricte.

> **Important**
>
> Avant d'installer l'application Citrix Workspace, vérifiez que les certificats sur le serveur ou la passerelle sont correctement configurés comme indiqué ci-dessous. Les connexions peuvent échouer si :
>
> - la configuration du serveur ou de la passerelle inclut un certificat racine incorrect ;
> - la configuration du serveur ou de la passerelle n'inclut pas tous les certificats intermédiaires ;
> - la configuration du serveur ou de la passerelle inclut un certificat intermédiaire expiré ou non valide ;
> - la configuration du serveur ou de la passerelle inclut un certificat intermédiaire avec signature croisée.

Lors de la validation d'un certificat de serveur, l'application Citrix Workspace utilise maintenant **tous** les certificats fournis par le serveur (ou la passerelle). Comme dans les versions précédentes, l'application Citrix Workspace vérifie également que les certificats sont approuvés. Si les certificats ne sont pas tous approuvés, la connexion échoue.

Cette stratégie est plus stricte que la stratégie de certificat des navigateurs web. De nombreux navigateurs Web comprennent un grand nombre de certificats racine auxquels ils font confiance.

Le serveur (ou la passerelle) doit être configuré avec le jeu correct de certificats. Un jeu incorrect de certificats peut entraîner l'échec de la connexion de l'application Citrix Workspace.

Supposons qu'une passerelle soit configurée avec ces certificats valides. Cette configuration est recommandée pour les clients qui requièrent une validation stricte, en déterminant précisément quel certificat racine est utilisé par l'application Citrix Workspace :

- Certificat de serveur exemple
- Certificat intermédiaire exemple
- Certificat racine exemple

L'application Citrix Workspace vérifie ensuite que tous ces certificats sont valides. L'application Citrix Workspace vérifie également si le **certificat racine exemple** est déjà approuvé.

> **Remarques :**
>
> - Si l'application Citrix Workspace ne fait pas confiance à **Certificat racine exemple**, la connexion échoue.
> - Certaines autorités de certification disposent de plus d'un certificat racine. Si vous avez besoin d'une validation plus stricte, assurez-vous que votre configuration utilise le certificat racine approprié.

Par exemple, il existe actuellement deux certificats :

- DigiCert ou GTE CyberTrust Global Root
- DigiCert Baltimore Root ou Baltimore CyberTrust Root

Ces certificats peuvent valider les mêmes certificats de serveur. Sur certaines machines utilisateur, les deux certificats racine sont disponibles. Sur les autres machines, seul (**DigiCert Baltimore Root** ou **Baltimore CyberTrust Root**) est disponible.

Si vous configurez **GTE CyberTrust Global Root** sur la passerelle, les connexions de l'application Citrix Workspace sur ces machines utilisateur échouent. Consultez la documentation de l'autorité de certification pour déterminer quel certificat racine doit être utilisé. Notez également que les certificats racine finissent par expirer, comme tous les certificats.

L'application Citrix Workspace utilise ensuite ces deux certificats. Elle recherche un certificat racine sur la machine utilisateur. Si elle en trouve un qui est validé et également approuvé (tel que **Certificat racine exemple**), la connexion réussit. Sinon, la connexion échoue.

Cette configuration fournit le certificat intermédiaire dont l'application Citrix Workspace a besoin, mais permet également à l'application Citrix Workspace de choisir un quelconque certificat racine valide et approuvé.

Supposons maintenant qu'une passerelle soit configurée avec ces certificats :

- Certificat de serveur exemple
- Certificat intermédiaire exemple
- Certificat racine incorrect

Un navigateur Web peut ignorer le certificat racine incorrect. Toutefois, l'application Citrix Workspace n'ignore pas le certificat racine incorrect et la connexion échoue.

Certaines autorités de certification disposent de plus d'un certificat intermédiaire. Dans ce cas, la passerelle est généralement configurée avec tous les certificats intermédiaires (mais pas le certificat racine) tels que :

- Certificat de serveur exemple
- Certificat intermédiaire exemple 1

- Certificat intermédiaire exemple 2

> **Important**
>
> Certaines autorités de certification utilisent un certificat intermédiaire avec signature croisée. De tels certificats sont destinés aux situations dans lesquelles il existe plus d'un certificat racine, et qu'un certificat racine antérieur est toujours en cours d'utilisation en même temps qu'un certificat racine plus récent. Dans de tels cas, il existe au moins deux certificats intermédiaires.

Par exemple, le certificat racine antérieur **Class 3 Public Primary Certification Authority** et le certificat intermédiaire avec signature croisée **Verisign Class 3 Public Primary Certification Authority - G5** correspondant. Toutefois, un certificat racine antérieur **Verisign Class 3 Public Primary Certification Authority - G5** correspondant est également disponible, et il remplace **Class 3 Public Primary Certification Authority**. Le certificat racine antérieur n'utilise pas de certificat intermédiaire avec signature croisée.

> **Remarque :**
>
> Le certificat intermédiaire avec signature croisée et le certificat racine ont le même nom d'objet (délivré à), mais le certificat intermédiaire avec signature croisée a un nom d'émetteur différent (émis par). Le nom de l'émetteur permet de différencier le certificat intermédiaire avec signature croisée d'un certificat intermédiaire ordinaire (tel **Certificat intermédiaire exemple 2**).

Cette configuration, qui ignore le certificat racine et le certificat intermédiaire avec signature croisée, est généralement recommandée :

- Certificat de serveur exemple
- Certificat intermédiaire exemple

Évitez de configurer la passerelle de manière à utiliser le certificat intermédiaire avec signature croisée, car l'application Citrix Workspace sélectionnera le certificat racine antérieur :

- Certificat de serveur exemple
- Certificat intermédiaire exemple
- Certificat intermédiaire croisé exemple [non recommandé]

Il n'est pas recommandé de configurer la passerelle avec le certificat de serveur uniquement :

- Certificat de serveur exemple

Dans de tels cas, si l'application Citrix Workspace ne peut pas trouver tous les certificats intermédiaires, la connexion échoue.

Installation et mise à niveau

November 10, 2023

Vous pouvez télécharger ou passer à la dernière version de l'application Citrix Workspace depuis l'Apple Store.

- Les nouveaux utilisateurs peuvent télécharger l'application Citrix Workspace depuis l'Apple Store et l'installer sur leur appareil.
- Les utilisateurs existants peuvent passer à la dernière version de l'application Citrix Workspace depuis l'Apple Store.

Pour plus d'informations sur la configuration de l'application Citrix Workspace, consultez la section Configurer.

Pour plus d'informations sur les fonctionnalités disponibles dans l'application Citrix Workspace pour iOS, consultez Tableau des fonctionnalités de l'application Citrix Workspace.

Prise en main

March 29, 2024

Installation

L'application Citrix Workspace pour iOS prend en charge la configuration de l'Interface Web pour votre déploiement Citrix Virtual Apps. Il existe deux types de sites d'Interface Web :

- Sites XenApp et XenDesktop
- Sites Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).

Les sites Interface Web permettent aux machines clientes de se connecter à la batterie de serveurs. Plusieurs solutions permettent d'assurer l'authentification entre l'application Citrix Workspace pour iOS et un site Interface Web, notamment Citrix Secure Web Gateway.

Vous pouvez également configurer StoreFront de manière à fournir des services d'authentification et de mise à disposition de ressources pour l'application Citrix Workspace. Cette configuration vous permet de créer de façon centralisée des magasins d'entreprise destinés à mettre à disposition des bureaux, des applications, ainsi que d'autres ressources aux utilisateurs.

Pour plus d'informations sur la configuration des connexions, y compris des vidéos, des blogs et un forum d'assistance, référez-vous à http://community.citrix.com.

Avant d'autoriser vos utilisateurs à accéder aux applications hébergées sur votre déploiement Citrix Virtual Apps and Desktops et Citrix DaaS, configurez les composants suivants dans votre déploiement comme indiqué ci-dessous.

- Lors de la publication d'applications sur vos batteries ou sites, envisagez les options suivantes pour améliorer l'expérience des utilisateurs qui accèdent aux applications par le biais des magasins StoreFront.
  - Veillez à inclure des descriptions claires des applications publiées, car ces descriptions sont consultées par les utilisateurs dans l'application Citrix Workspace.
  - Vous pouvez augmenter la visibilité des applications publiées auprès des utilisateurs d'appareils mobiles. Vous pouvez répertorier les applications dans la liste Sélection. Pour renseigner cette liste dans l'application Citrix Workspace, modifiez les propriétés des applications publiées sur vos serveurs. Vous pouvez maintenant ajouter la chaîne « KEYWORDS: Featured » au champ **Description de l'application**.
  - Le mode d'adaptation de l'écran ajuste l'application à la taille de l'écran des appareils mobiles. Pour activer ce mode, modifiez les propriétés des applications publiées sur vos serveurs et ajoutez la chaîne « KEYWORDS: mobile » à la valeur du champ Description de l'application. Ce mot-clé active également la fonctionnalité de défilement automatique pour l'application.
  - Pour abonner automatiquement tous les utilisateurs d'un magasin à une application, ajoutez la chaîne « KEYWORDS: Auto » à la description lors de la publication de l'application dans Citrix Virtual Apps. Lorsque les utilisateurs ouvrent une session dans le magasin, l'application est automatiquement provisionnée sans qu'ils aient à y souscrire manuellement.
- Si l'Interface Web de votre déploiement Citrix Virtual Apps and Desktops et Citrix DaaS ne dispose pas d'un site, créez-en un. Le nom du site et sa méthode de création dépendent de la version de l'Interface Web que vous avez installée.

Configuration manuelle

En général, lorsque l'application Citrix Workspace se connecte à Citrix Gateway, l'application Citrix Workspace tente de localiser un site XenApp et XenDesktop ou un site Web Citrix Virtual Apps après l'authentification. Si aucun site n'est détecté, l'application Citrix Workspace pour iOS affiche une erreur. Pour éviter ce problème, vous pouvez configurer un compte manuellement pour faire en sorte que l'application Citrix Workspace pour iOS se connecte à Citrix Gateway.

1. Touchez l'icône **Comptes**, et dans l'écran **Comptes** touchez le signe **Plus (+)**. L'écran Nouveau compte s'affiche.
2. Dans le coin inférieur gauche, touchez l'icône à gauche de **Options** et touchez **Installation manuelle**. Des champs supplémentaires s'affichent sur l'écran.
3. Dans le champ **Adresse**, entrez l'adresse URL sécurisée du site ou de Citrix Gateway (par exemple, `agee.mycompany.com`).
4. Sélectionnez l'une des options de connexion suivantes. Les autres champs sur l'écran changent, en fonction de votre sélection.

    - **Interface Web** : permet à l'application Citrix Workspace d'afficher un site Web Citrix Virtual Apps similaire à un navigateur Web. Également appelé Affichage Web.
    - **XenApp Services** : permet à l'application Citrix Workspace pour iOS de localiser un site XenApp et XenDesktop spécifique pour lequel l'authentification via Citrix Gateway n'est pas configurée. Dans les options supplémentaires qui s'affichent à l'écran, saisissez les informations d'identification d'ouverture de session au site.
        - <StoreFront FQDN> : s'il existe plusieurs magasins, une liste s'affiche et l'utilisateur peut choisir le magasin à ajouter.
        - <StoreFront FQDN>/citrix/<Store Name> : cela ajoute le magasin StoreFront <Store Name>.
        - <StoreFront FQDN>/citrix/PnAgent/config.xml : cela ajoute le magasin PNAgent d'ancienne génération par défaut.
        - <StoreFront FQDN>/citrix/<Store Name>/PnAgent/config.xml : cela ajoute le magasin PNAgent d'ancienne génération associé à <Store Name>.
    - Citrix Gateway : permet à l'application Citrix Workspace pour iOS de se connecter à un site XenApp et XenDesktop via un Citrix Gateway spécifique. Dans les options supplémentaires qui s'affichent à l'écran, sélectionnez l'édition de serveur et ses informations d'identification d'ouverture de session, y compris si un jeton de sécurité est requis pour l'authentification.

5. Pour le certificat de sécurité, utilisez le paramètre dans le champ Ignorer les avertissements de certificat pour spécifier si vous voulez vous connecter au serveur même s'il dispose d'un certificat non valide, auto-signé ou expiré. Le paramètre par défaut est Désactivé.
   Important : si vous activez cette option, vous devez vous assurer que vous vous connectez au serveur correct. Citrix recommande fortement que tous les serveurs possèdent un certificat valide afin de protéger les machines utilisateur des attaques de sécurité en ligne. Un serveur sécurisé utilise un certificat SSL délivré depuis une autorité de certification. Citrix ne prend pas en charge les certificats auto-signés et ne recommande pas d'ignorer le certificat de sécurité.
6. Appuyer sur Enregistrer.
7. Entrez votre nom d'utilisateur et mot de passe (ou jeton, si vous avez sélectionné l'authentification à deux facteurs) et touchez Ouvrir session. L'écran de l'application Citrix Workspace pour

iOS s'affiche, dans lequel vous pouvez accéder à vos bureaux et ajouter et ouvrir vos applications.

StoreFront

> **Important :**
>
> - Lors de l'utilisation de StoreFront, l'application Citrix Workspace pour iOS prend en charge Citrix Access Gateway Enterprise Edition à partir de la version 9.3, et Citrix Gateway jusqu'à la version 13.
> - L'application Citrix Workspace pour iOS prend uniquement en charge les sites XenApp et XenDesktop sur l'Interface Web.
> - L'application Citrix Workspace pour iOS prend en charge le lancement de sessions à partir de Workspace pour Web, à condition que le navigateur Web fonctionne avec Workspace pour Web. Si le lancement échoue, configurez votre compte directement via l'application Citrix Workspace pour iOS. Les utilisateurs doivent ouvrir le fichier ICA manuellement à l'aide de la fonction « Ouvrir dans Workspace » du navigateur. Pour prendre connaissance des limitations de ce déploiement, consultez la documentation de StoreFront.

Les magasins que vous créez dans StoreFront se composent de services destinés à fournir une infrastructure d'authentification et de mise à disposition de ressources pour l'application Citrix Workspace pour iOS. Créez des magasins qui comptent et additionnent les bureaux et les applications à partir des éléments suivants :

- Sites Citrix Virtual Apps and Desktops et Citrix DaaS
- Batteries Citrix Virtual Apps

1. Installez et configurez StoreFront. Pour plus de détails, consultez la documentation produit de StoreFront. Pour les administrateurs soucieux d'exercer un contrôle plus rigoureux, Citrix fournit un modèle que vous pouvez utiliser pour créer un site de téléchargement pour l'application Citrix Workspace pour iOS.
2. Configurez des magasins pour StoreFront comme vous le faites pour toute autre application Citrix Virtual Apps and Desktops et Citrix DaaS. Aucune configuration spéciale n'est nécessaire pour les appareils mobiles. Pour plus de détails, consultez la section Options d'accès utilisateur dans la section StoreFront de la documentation Produit. Pour les appareils mobiles, utilisez l'une de ces méthodes :

    - Fichier de provisioning. Vous pouvez fournir aux utilisateurs des fichiers de provisioning (.cr) contenant les informations nécessaires pour se connecter aux magasins. Après l'installation, les utilisateurs ouvrent le fichier sur leur appareil pour configurer automatiquement l'application Citrix Workspace pour iOS. Par défaut, les sites Workspace pour Web offrent aux utilisateurs un fichier de provisioning destiné au magasin pour lequel le site

est configuré. Vous pouvez également utiliser la console de gestion Citrix StoreFront pour générer des fichiers de provisioning pour des magasins uniques ou multiples que vous distribuez manuellement à vos utilisateurs.

- Configuration manuelle. Vous pouvez informer directement les utilisateurs des adresses URL de Citrix Gateway ou de magasin nécessaires à l'accès à leurs bureaux ou applications. Pour les connexions via Citrix Gateway, les utilisateurs doivent également connaître l'édition du produit et la méthode d'authentification requise. Après installation, les utilisateurs entrent ces détails dans l'application Citrix Workspace qui tente de vérifier la connexion et, en cas de réussite, invite les utilisateurs à se connecter.
- Configuration automatique. Appuyez sur **Ajouter un compte** sur l'écran de bienvenue et entrez l'URL du serveur StoreFront dans le champ d'adresse. Le compte est configuré lorsqu'il est ajouté.

Pour configurer Citrix Gateway

Si certains utilisateurs se connectent depuis l'extérieur du réseau interne, configurez l'authentification via Citrix Gateway. Par exemple, les utilisateurs qui se connectent via Internet à partir d'emplacements distants.

- Lors de l'utilisation de StoreFront, l'application Citrix Workspace pour iOS prend en charge Citrix Access Gateway Enterprise Edition à partir de la version 9.3, et Citrix Gateway jusqu'à la version 13.

Interface Web

Pour configurer le site Interface Web, les utilisateurs d'iPhone et d'iPad peuvent lancer des applications via votre site Interface Web et le navigateur Safari intégré à leur appareil mobile. Configurez le site Interface Web comme vous le faites pour toute autre application Citrix Virtual Apps. Si aucun site XenApp et XenDesktop n'est configuré pour l'appareil mobile, l'application Citrix Workspace pour iOS utilise automatiquement votre site Interface Web. Aucune configuration spéciale n'est nécessaire pour les appareils mobiles.

Le navigateur Safari intégré prend en charge l'Interface Web 5.x.

Pour lancer des applications sur l'appareil iOS

Sur l'appareil mobile, les utilisateurs peuvent se connecter au site Interface Web à l'aide de leur nom de connexion et mot de passe.

Provisionnement automatique pour appareils mobiles

Dans StoreFront, utilisez les tâches **Exporter le fichier de provisioning multi-magasins** et **Exporter le fichier de provisioning** pour générer des fichiers contenant les détails de connexion des magasins, y compris les déploiements Citrix Gateway et les balises configurées pour les magasins. Mettez ces fichiers à la disposition des utilisateurs pour leur permettre de configurer l'application Citrix Workspace pour iOS automatiquement avec les détails relatifs aux magasins. Les utilisateurs peuvent également obtenir les fichiers de provisioning de l'application Citrix Workspace pour iOS à partir de Workspace pour sites Web.

> **Important :**
>
> Dans les déploiements faisant appel à de multiples serveurs, n'utilisez qu'un serveur à la fois pour modifier la configuration du groupe de serveurs. Vérifiez que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois les modifications terminées, propagez les modifications que vous avez apportées à la configuration du groupe de serveurs de façon à mettre à jour les autres serveurs dans le déploiement.

1. Sur l'écran Démarrer de Windows ou l'écran Applications, accédez à la vignette Citrix StoreFront et cliquez dessus. Sélectionnez le nœud Magasins dans le volet gauche de la console de gestion Citrix StoreFront.
2. Pour générer un fichier de provisioning contenant les détails relatifs à plusieurs magasins, dans le panneau Actions, cliquez sur Exporter le fichier de provisioning multi-magasins, puis sélectionnez les magasins que vous souhaitez inclure dans ce fichier.
3. Cliquez sur Exporter et Enregistrer pour enregistrer le fichier de provisioning avec une extension `.cr` sur un emplacement approprié de votre réseau.

Informations d'accès utilisateur

Vous devez fournir aux utilisateurs les informations de compte de l'application Citrix Workspace pour iOS dont ils ont besoin pour accéder à leurs applications, données et bureaux hébergés. Vous pouvez leur fournir ces informations de la façon suivante :

- En configurant la découverte de compte basée sur une adresse e-mail
- En fournissant un fichier de provisioning aux utilisateurs
- En fournissant aux utilisateurs des informations de compte à entrer manuellement

Configurer la découverte de compte basée sur une adresse e-mail

Vous pouvez configurer l'application Citrix Workspace pour iOS de manière à utiliser la découverte de compte basée sur e-mail. Une fois configurée, plutôt que d'entrer une adresse URL de serveur, les

utilisateurs entrent leur adresse e-mail durant l'installation et la configuration de l'application Citrix Workspace pour iOS. L'application Citrix Workspace identifie le serveur Access Gateway ou StoreFront, ou l'appliance virtuelle Endpoint Management associés à l'adresse e-mail en se basant sur les enregistrements SRV de DNS et invite les utilisateurs à ouvrir une session pour accéder à leurs applications, données et bureaux publiés.

> **Remarque :**
>
> La découverte de compte basée sur l'adresse e-mail n'est pas prise en charge si l'application Citrix Workspace pour iOS se connecte à un déploiement Interface Web.

Ajouter un enregistrement d'emplacement du service DNS (SRV) pour activer la découverte par e-mail Lors de la configuration initiale, l'application Citrix Workspace peut contacter les serveurs DNS Active Directory pour obtenir des détails sur les magasins auxquels les utilisateurs ont accès. Cela signifie que les utilisateurs n'ont pas besoin de connaître les détails d'accès de leurs magasins lorsqu'ils installent et configurent l'application Citrix Workspace pour iOS. Au lieu de cela, les utilisateurs saisissent leur adresse e-mail et l'application Citrix Workspace contacte le serveur DNS. Vous pouvez collecter les détails du domaine à partir de l'adresse e-mail.

Pour permettre à l'application Citrix Workspace de localiser les magasins disponibles en fonction des adresses e-mail des utilisateurs :

- Configurez des enregistrements de ressources de localisation de l'emplacement du service (SRV) pour Access Gateway.
- Configurez les connexions StoreFront ou AppController sur votre serveur DNS.

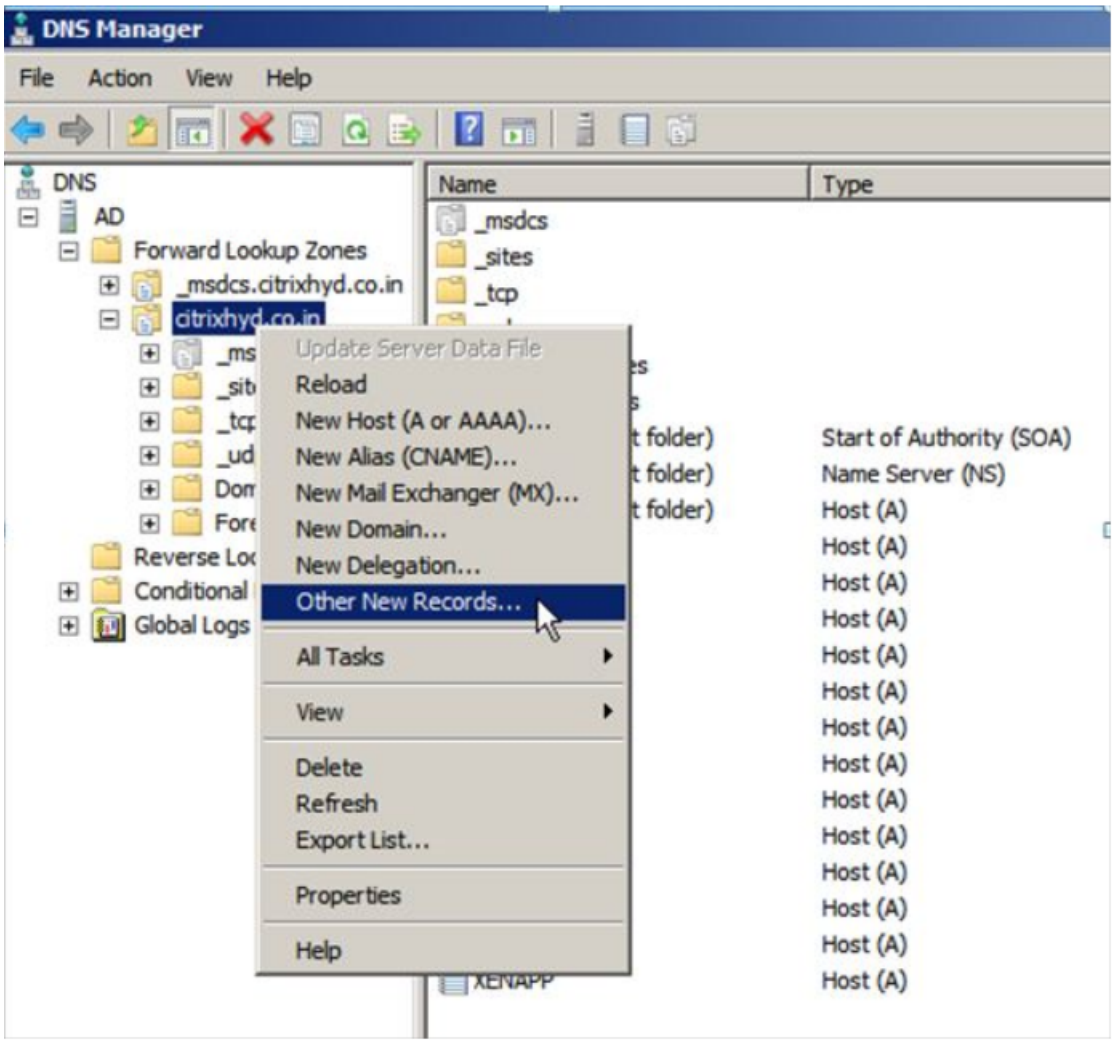
Vous devez installer un certificat de serveur valide sur l'appliance Access Gateway et le serveur StoreFront ou AppController pour activer la découverte de compte par e-mail. La chaîne complète du certificat racine doit également être valide. Pour garantir une expérience utilisateur optimale, installez un certificat avec :

- une entrée Objet ;
- une entrée Autre nom de l'objet définie sur *discoverReceiver.domain* ;
- un certificat générique pour le domaine contenant les comptes de messagerie de vos utilisateurs.

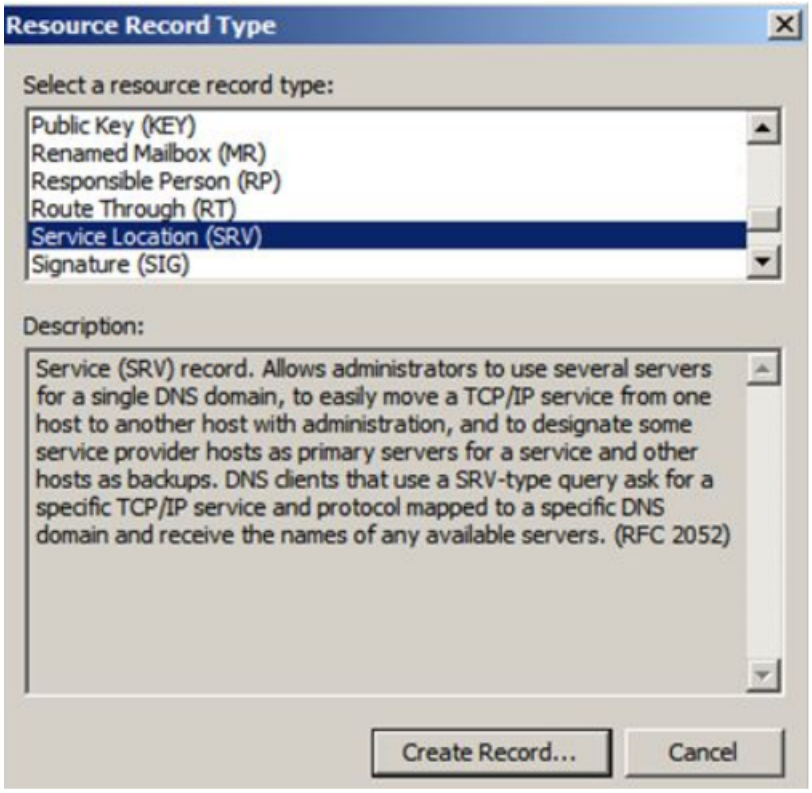
Pour permettre aux utilisateurs de configurer l'application Citrix Workspace pour iOS à l'aide d'une adresse e-mail, ajoutez un enregistrement SRV à votre zone DNS comme suit :

1. Connectez-vous à votre serveur DNS.
2. Dans DNS, cliquez avec le bouton droit de la souris sur votre zone de recherche directe.

3. Cliquez sur **Nouveaux enregistrements.**



4. La boîte de dialogue **Type d'enregistrement de ressource** apparaît.
5. Sous **Choisissez un type d'enregistrement de ressource**, sélectionnez **Emplacement du service (SRV).**
6. Sélectionnez **Créer un enregistrement.**



7. La boîte de dialogue Propriétés apparaît.
8. Sélectionnez l'onglet **Emplacement du service**.
9. Sous **Service**, entrez la valeur d'hôte _citrixreceiver.
10. Sous **Protocole**, entrez la valeur _tcp.
11. Sous **Hôte offrant ce service**, spécifiez le nom de domaine complet (FQDN) et le port de votre appliance Access Gateway (pour prendre en charge les utilisateurs locaux et distants) ou le serveur StoreFront ou AppController (pour prendre en charge les utilisateurs sur le réseau local uniquement).
12. Cliquez sur OK.

> **Remarque :**
>
> Votre nom de domaine complet StoreFront doit être unique et différent du nom de domaine complet du serveur virtuel Access Gateway. L'utilisation d'un même nom de domaine complet pour StoreFront et le serveur virtuel Access Gateway n'est pas prise en charge. L'application Citrix Workspace nécessite que le nom de domaine complet de StoreFront soit une adresse unique qui ne peut être résolue qu'à partir des machines utilisateur connectées au réseau interne. Sinon, les utilisateurs de l'application Citrix Workspace ne peuvent pas utiliser la découverte de comptes basée sur une adresse e-mail.

Fournir un fichier de provisioning aux utilisateurs

Vous pouvez utiliser StoreFront pour créer des fichiers de provisioning contenant les détails des comptes. Vous pouvez mettre ces fichiers à la disposition de vos utilisateurs pour leur permettre de configurer l'application Citrix Workspace pour iOS automatiquement. Après l'installation de l'application Citrix Workspace pour iOS, il leur suffit d'ouvrir le fichier `.cr` sur l'appareil pour configurer l'application Citrix Workspace pour iOS. Si vous configurez Workspace pour des sites Web, les utilisateurs peuvent également obtenir les fichiers de provisioning de l'application Citrix Workspace pour iOS à partir de ces sites.

Pour plus d'informations, veuillez consulter la documentation de StoreFront.

Fournir aux utilisateurs des informations de compte à entrer manuellement

Si vous fournissez aux utilisateurs des informations de compte à entrer manuellement, vous devez leur communiquer les informations suivantes afin de leur permettre de se connecter à leurs bureaux hébergés avec succès :

- L'adresse URL de StoreFront ou du site XenApp et XenDesktop hébergeant les ressources ; par exemple : `servername.company.com`.
- Pour permettre l'accès à l'aide de Citrix Gateway, fournissez l'adresse de Citrix Gateway et la méthode d'authentification requise.

Lorsqu'un utilisateur entre les détails d'un nouveau compte, l'application Citrix Workspace tente de vérifier la connexion. En cas de réussite, l'application Citrix Workspace pour iOS invite l'utilisateur à se connecter au compte.

Configurer l'application Citrix Workspace

March 29, 2024

Cet article répertorie les tâches qui vous aident à configurer l'application Citrix Workspace pour iOS.

Gestion des feature flag

Si un problème survient avec l'application Citrix Workspace en production, la fonctionnalité affectée peut être désactivée dynamiquement dans l'application Citrix Workspace, même après la livraison de la fonctionnalité. Nous utilisons des commutateurs de fonctionnalité et un service tiers appelé LaunchDarkly. Vous n'avez pas besoin d'effectuer des configurations pour activer le trafic vers

LaunchDarkly, sauf si un pare-feu ou un proxy bloque le trafic sortant. Dans ce cas, vous activez le trafic vers LaunchDarkly via des URL ou adresses IP spécifiques, en fonction des exigences de votre stratégie.

Vous pouvez activer le trafic et la communication vers LaunchDarkly des manières suivantes :

Activer le trafic vers les URL suivantes

- `app.launchdarkly.com`
- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `Firehose.launchdarkly.com`
- `mobile.launchdarkly.com`

Répertorier les adresses IP dans une liste verte

Si vous devez répertorier les adresses IP dans la liste verte, consultez la liste des adresses IP publiques de LaunchDarkly pour obtenir une liste de toutes les plages d'adresses IP actuelles. Vous pouvez utiliser cette liste pour vous assurer que les configurations du pare-feu sont mises à jour automatiquement en fonction des mises à jour de l'infrastructure. Pour plus d'informations sur l'état des modifications de l'infrastructure, consultez la page LaunchDarkly Status.

Configuration système requise pour LaunchDarkly

Vous devez vérifier si les applications peuvent communiquer avec les services suivants si le split tunneling sur Citrix ADC est **désactivé** :

- Service LaunchDarkly
- Service d'écoute APNs

Disposition pour désactiver le service LaunchDarkly :

Vous pouvez désactiver le service LaunchDarkly sur les magasins sur site et dans le cloud.

Dans la configuration cloud, vous pouvez désactiver le service LaunchDarkly en définissant l'attribut enableLaunchDarkly sur False. Vous pouvez y parvenir à partir de l'interface utilisateur de Global App Configuration service.

```
{

    "assignedTo": [
        "AllUsersNoAuthentication"
```



```
    ],
    "category": "Third Party Services",
    "settings": [
        {

        "name": "Enable Launch Darkly",
        "value": "true"
         }

    ],
    "userOverride": false
 }

<!--NeedCopy-->
```

Pour plus d'informations, consultez la documentation Global App Configuration Service.

Lors du déploiement local, procédez comme suit :

1. Dans un éditeur de texte, ouvrez le fichier web.config qui se trouve en général dans le répertoire `C:\inetpub\wwwroot\Citrix\Roaming`.
2. Recherchez l'élément de compte d'utilisateur dans le fichier (Store est le nom du compte de votre déploiement).

   Par exemple, `<account id=... name="Store">`

   Avant la balise, accédez aux propriétés de ce compte utilisateur :

   ```
   <properties>
   <clear/>
   </properties>
   <!--NeedCopy-->
   ```

3. Ajoutez la balise enableLaunchDarkly et définissez la valeur sur false.
4. Ajoutez la balise enableLaunchDarkly et définissez la valeur sur false.

   `<property name="enableLaunchDarkly"value="false"/>`

> **Remarque :**
>
> La plupart des fonctionnalités se trouvent derrière un indicateur de fonctionnalité contrôlé par LaunchDarkly. Dans les environnements où elle est désactivée, vous devez attendre au moins 90 jours.

Délai d'inactivité pour l'application Citrix Workspace

Les administrateurs peuvent spécifier la durée d'inactivité autorisée. Après expiration du délai d'inactivité, une invite d'authentification s'affiche.

La valeur du délai d'inactivité définie doit être comprise entre 1 et 24 heures. Par défaut, le délai d'inactivité n'est pas configuré. Les administrateurs peuvent configurer la propriété inactivityTimeoutInMinutesMobile à l'aide d'un module PowerShell. Cliquez ici pour télécharger les modules PowerShell pour la configuration de l'application Citrix Workspace.

Lorsque vous atteignez la valeur du délai d'inactivité spécifiée, l'expérience utilisateur est la suivante en fonction du type d'authentification configuré :

- Une fois le délai d'inactivité dépassé, vous serez invité à fournir une authentification biométrique pour accéder à nouveau à l'application Citrix Workspace.
- Si vous pouvez annuler l'invite d'authentification biométrique, le message suivant s'affiche :

  L'application Citrix Workspace est verrouillée.

  Vous devez vous authentifier pour continuer à utiliser l'application Workspace.

Si le code d'accès n'est pas configuré sur iOS, vous devez vous connecter avec des informations d'identification après l'expiration du délai d'inactivité.

> **Remarque :**
>
> Cette fonctionnalité s'applique uniquement aux clients de Workspace (Cloud).

CEIP (programme d'amélioration de l'expérience du client)

Données collectées	Description	Quel usage faisons-nous de ces données
Données de configuration et d'utilisation	Le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) rassemble des données de configuration et d'utilisation à partir de l'application Citrix Workspace pour iOS et les envoie automatiquement à Google Firebase.	Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de Workspace.

Informations supplémentaires

Citrix traite vos données conformément aux termes de votre contrat avec Citrix et les protège comme indiqué dans l'Annexe sur la sécurité des Services Citrix. Pour plus d'informations, consultez Citrix Trust Center.

Citrix utilise Google Firebase pour collecter certaines données à partir de l'application Citrix Workspace dans le cadre du programme CEIP. Informez-vous sur la manière dont Google gère les données collectées pour Google Firebase.

Pour arrêter l'envoi de données via le programme CEIP à Citrix et Google Firebase :

1. Ouvrez l'application Citrix Workspace pour iOS.
2. Appuyez sur **Accueil** > **Paramètres**.
3. Accédez à la section **Général**.
4. Désactivez l'option **Envoyer statistiques d'utilisation**.

> **Remarque :**
>
> Aucune donnée n'est collectée pour les utilisateurs de l'Union européenne (UE), de l'Espace économique européen (EEE), de la Suisse et du Royaume-Uni (UK).

Les données spécifiques à CEIP collectées par Google Firebase sont les suivantes :

Informations sur la session et la méthode de lancement de session	Configuration de magasins et des magasins Citrix	Type d'authentification et configuration de l'authentification	Connexions ICA
Lancement de session HDX	Session d'application de magasin	Ouverture d'action WebView	Copie d'action WebView
Partage d'action WebView	Contrôle de l'application Workspace	État de la connexion, erreur de connexion, utilisation du centre de connexion	Affichage externe
État de la socket	Durée de la session	HDX sur UDP	Heure de lancement de la session
Informations sur l'appareil	Informations sur le modèle d'appareil	Envoyer statistiques d'utilisation	Langue de l'application, langue de l'application Workspace
Langue du clavier	Type de magasin Citrix	Combinaison de magasins Citrix	Type de protocole de stockage
Nombre de magasins	État HDX UDP	Installations de jetons RSA	

Limitations connues

- Sur les VDA 7.18 ou versions antérieures, la diffusion vers un Workspace Hub nécessite que la stratégie plein écran h.264 soit activée et que la stratégie de graphiques d'ancienne génération soit désactivée sur le bureau ou toute autre ressource que vous utilisez.

Partage de session

Si les utilisateurs se déconnectent d'un compte de l'application Citrix Workspace, ils peuvent toujours se déconnecter ou fermer les sessions à distance.

- **Déconnexion** : se déconnecte du compte mais laisse l'application ou le bureau Windows en cours d'exécution sur le serveur. L'utilisateur peut démarrer un autre appareil, lancer l'application Citrix Workspace pour iOS et se reconnecter au dernier état avant la déconnexion de l'appareil iOS. Cette option permet aux utilisateurs de se reconnecter à partir d'un autre appareil et de reprendre le travail dans les applications en cours d'exécution.
- **Fermer la session** : déconnecte le compte et ferme l'application Windows. Déconnecte également du serveur Citrix Virtual Apps and Desktops et du serveur Citrix DaaS. Cette option permet aux utilisateurs de se déconnecter du serveur et de fermer la session du compte. Lorsqu'ils lancent à nouveau l'application Citrix Workspace pour iOS, elle s'ouvre dans l'état par défaut.

Magasins Cloud

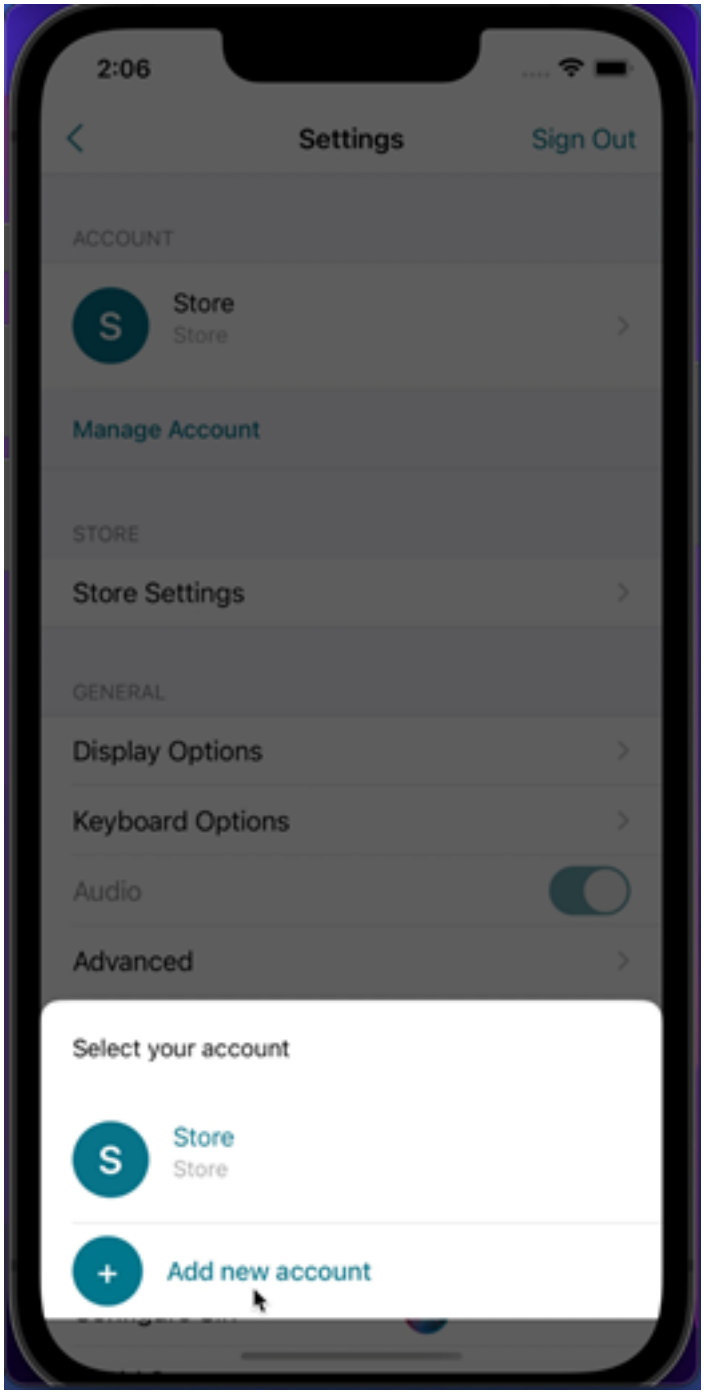
Vous pouvez accéder aux applications Web, SaaS et aux sites Web hébergés par votre organisation, quel que soit votre emplacement d'accès. Cette fonctionnalité n'est disponible que pour les clients de magasins dans le cloud.

Prise en charge de magasins cloud multiples

À partir de la version 24.1.0, vous pouvez ajouter plusieurs comptes de magasin cloud à l'application Citrix Workspace pour iOS et iPadOS. Désormais, les utilisateurs finaux peuvent facilement ajouter plusieurs magasins et passer d'un magasin à l'autre. Cette fonctionnalité améliore l'expérience utilisateur lors de l'accès à plusieurs magasins.

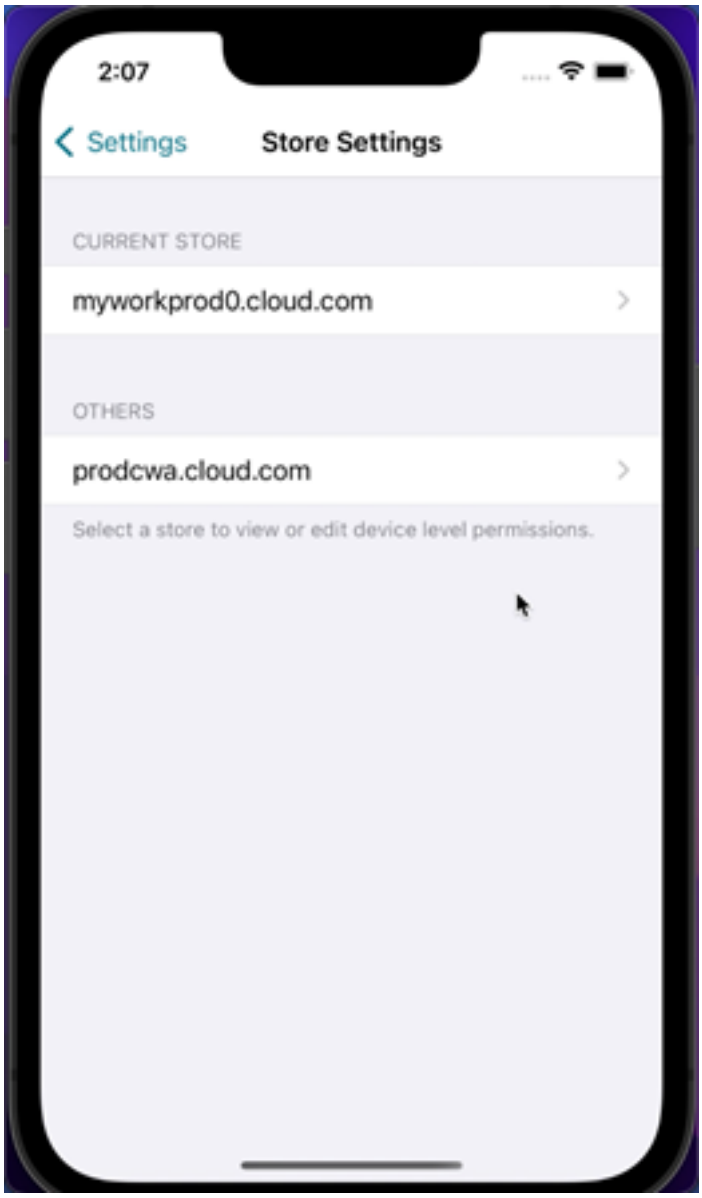
Pour ajouter un autre compte, procédez comme suit :

1. Accédez à **Paramètres > Gérer le compte**. Une boîte de dialogue apparaît en bas de l'écran avec la liste de vos comptes.
2. Touchez **Ajouter nouveau compte**.



3. Tapez l'URL ou l'adresse e-mail fournie par votre administrateur informatique. Pour utiliser une carte à puce pour ouvrir une session, touchez **Utiliser carte à puce**.
4. Touchez **Continuer**. La boîte de dialogue **Connexion** s'affiche avec les champs correspondant à votre nom d'utilisateur, mot de passe, domaine et code secret.
5. Saisissez les informations requises. Pour plus d'informations sur les champs, contactez votre administrateur informatique.

6. Touchez **Se connecter**. Votre nouveau compte est maintenant configuré.



Remplir automatiquement l'URL du magasin

Lorsque vous accédez à l'application Citrix Workspace pour iOS rebaptisée, vous pouvez choisir de renseigner automatiquement l'URL du magasin. Cette fonctionnalité réduit les interventions manuelles et offre un accès rapide à l'application. Pour plus d'informations sur la personnalisation des applications, consultez la section Personnalisation des applications.

Possibilité de supprimer plusieurs magasins à la fois

À partir de la version 24.2.0, l'application Citrix Workspace pour iOS permet de sélectionner plusieurs magasins et de les supprimer. Cette fonctionnalité améliore l'expérience utilisateur lors de l'utilisation de plusieurs magasins. Cette fonctionnalité est activée par défaut.

Pour supprimer plusieurs magasins à la fois depuis l'écran **Magasins**, procédez comme suit :

1. Sur l'écran **Magasins**, touchez **Sélectionner**.
2. Sélectionnez les magasins à supprimer. Pour supprimer tous les magasins, touchez **Tout sélectionner**.
3. Touchez **Supprimer**.

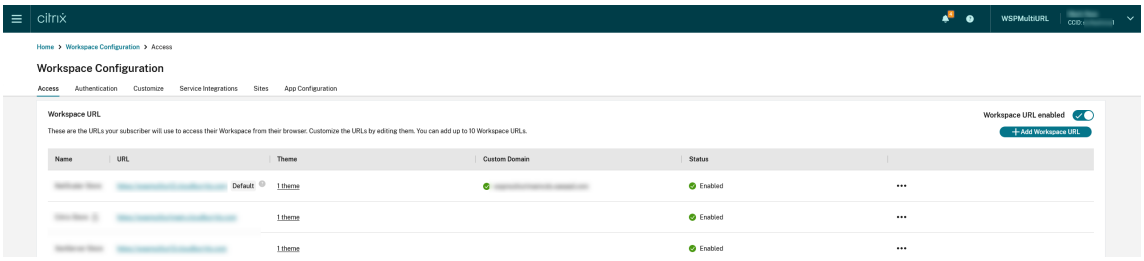
Possibilité pour les administrateurs d'empêcher les utilisateurs de modifier le nom d'un magasin

Auparavant, les utilisateurs pouvaient modifier le nom d'un magasin en utilisant l'option **Modifier le compte**.

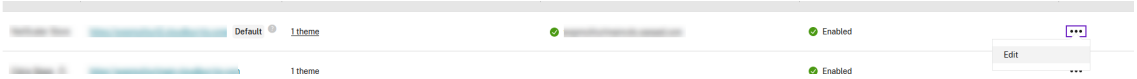
À partir de la version 24.2.0, l'application Citrix Workspace pour iOS offre aux administrateurs la possibilité d'empêcher les utilisateurs de modifier le nom d'un magasin. Grâce à cette fonctionnalité, les administrateurs peuvent facilement identifier et maintenir la cohérence des noms de magasin.

Pour autoriser les utilisateurs à modifier le nom d'un magasin, procédez comme suit :

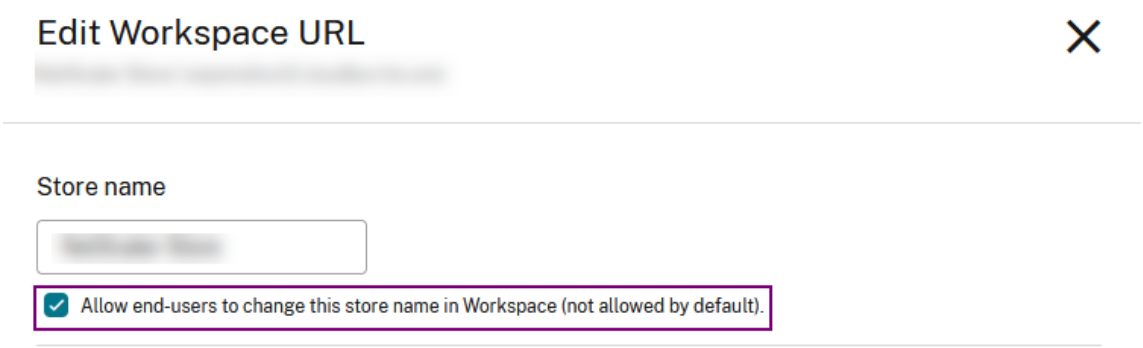
1. Connectez-vous à Citrix Cloud avec vos informations d'identification.
2. Accédez à **Configuration de l'espace de travail > Accès**. Sous **URL de l'espace de travail**, vous trouverez une liste des URL de magasin existantes.



3. Cliquez sur le menu des points de suspension du magasin pour lequel vous souhaitez autoriser les utilisateurs à en modifier le nom.
4. Sélectionnez **Modifier**.



5. Dans la boîte de dialogue **Modifier l'URL de l'espace de travail**, sélectionnez **Autoriser les utilisateurs à modifier le nom de ce magasin dans Workspace (non autorisé par défaut)**.



6. Cliquez sur **Enregistrer**.

Remplissage automatique du nom du magasin

À partir de la version 24.2.0, l'application Citrix Workspace pour iOS permet aux administrateurs de mettre à jour les noms de magasin et de les transmettre automatiquement aux utilisateurs. Cette fonctionnalité améliore l'expérience utilisateur, car il n'est plus nécessaire de recourir à une intervention manuelle pour mettre à jour le nom d'un magasin.

> **Remarque :**
>
> cette fonctionnalité ne peut prendre effet que si les administrateurs ont désactivé l'option permettant d'empêcher les utilisateurs de modifier le nom du magasin.

Amélioration de la surveillance de l'expérience utilisateur final

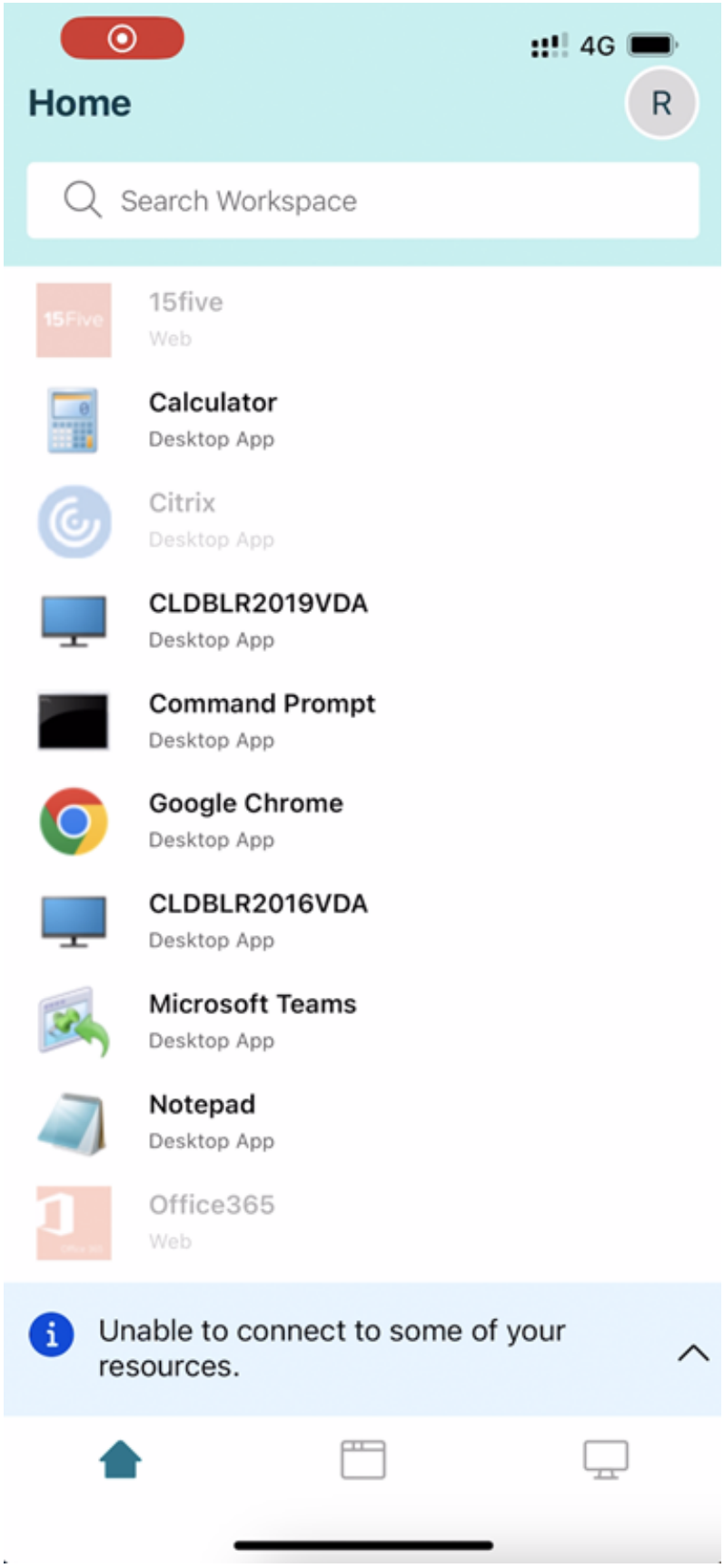
Nous prenons désormais en charge les mesures de démarrage du client EUEM (Suivi de l'expérience utilisateur). EUEM permet de collecter des données de surveillance de l'expérience de session très granulaires en temps réel. Il envoie les données au tableau de bord Director, afin que l'administrateur puisse surveiller l'expérience utilisateur. Les données sont collectées via le service SEMS (Session Experience Monitoring Service) présent sur le VDA. Les données de mesure de démarrage du client disponibles pour la surveillance sur le tableau de bord incluent :

- Durée de téléchargement du fichier ICA.
- Durée de création de sessions sur le client. La durée de création de sessions sur le client représente le temps nécessaire à la création d'une session. Elle est calculée à partir du moment où un fichier ICA est lancé jusqu'à ce que la connexion soit établie.

- Durée de recherche de sessions sur le client. La durée de recherche de sessions sur le client représente le temps nécessaire pour interroger chaque session pour héberger l'application publiée demandée. La vérification est effectuée sur le client pour déterminer si une session existante peut gérer la demande de lancement de l'application.
- Enregistrement en temps réel par Citrix des boucles ICA, également connu sous le nom de ICA RTT. ICA RTT est le temps qui s'écoule entre le moment où l'utilisateur appuie sur une touche et l'affichage de la réponse sur le point de terminaison.

Amélioration de l'interface utilisateur pour le mode hors ligne de continuité du service

À compter de la version 24.1.0, l'interface utilisateur de l'application Citrix Workspace pour iOS a été améliorée pour être plus informative, plus moderne et offrir une expérience conviviale lors des pannes de Citrix Workspace. La fonctionnalité de recherche analogique est également incluse pour le mode hors ligne. Grâce à cette fonctionnalité, vous pouvez trouver des résultats pour des applications ou des bureaux avec du texte proche et des termes de recherche mal orthographiés. Pour plus d'informations sur la continuité de service, consultez la section Continuité de service.



Configurer l'application Workspace à l'aide des solutions Unified Endpoint Management

April 17, 2024

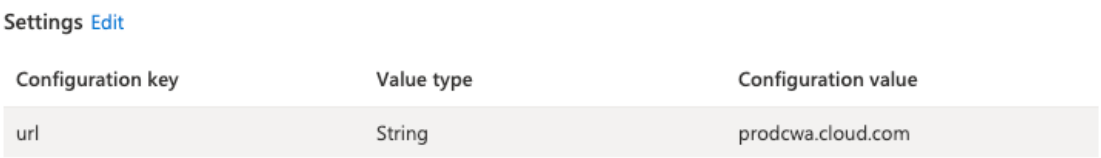
L'application Citrix Workspace pour iOS prend en charge la configuration administrative de l'application Workspace avec des paires clé-valeur basées sur AppConfig à l'aide de solutions Unified Endpoint Management (UEM).

Comment configurer

Pour configurer l'URL de votre Workspace Store à l'aide de solutions Unified Endpoint Management, procédez comme suit :

> **Remarque :**
>
> À des fins de démonstration, Microsoft Intune est utilisé comme solution UEM dans cet exemple. Les étapes ci-dessous et l'interface utilisateur affichée varient en fonction de votre fournisseur UEM.

1. Connectez-vous à votre fournisseur de solutions Unified Endpoint Management (UEM).
2. Ajoutez l'application Citrix Workspace que vous souhaitez gérer par votre fournisseur UEM. Vous pouvez télécharger l'application en utilisant le portail de votre fournisseur UEM pour permettre la gestion par votre fournisseur UEM. Vous pouvez également créer un lien vers l'application dans l'App Store.
3. Créez une stratégie de configuration pour votre application.
4. Ajoutez une nouvelle paire clé-valeur à la liste des propriétés XML et renseignez les valeurs suivantes :
   - **Clé** : `url`
   - **Type de valeur** : `String`
   - **Valeur** : URL de votre magasin (par exemple, `prodcwa.cloud.com`)



Limitations

- Si un magasin cloud est déjà configuré et que l'administrateur en configure un nouveau, votre magasin cloud existant est supprimé. Cela supprime également l'ensemble des données ou paramètres associés du magasin cloud existant. Vous recevez une notification dans Citrix Workspace. Vous devez ensuite vous reconnecter pour que le nouveau magasin cloud soit ajouté à Citrix Workspace.
  - L'information ci-dessus ne s'applique qu'aux magasins cloud existants. Si un magasin sur site est déjà configuré et que l'administrateur configure un nouveau magasin cloud ou local, le nouveau magasin est ajouté et aucune suppression ne se produit.
- Pour appliquer de nouvelles configurations, vous devez forcer l'arrêt et redémarrer l'application Citrix Workspace.

Améliorations apportées aux solutions Unified Endpoint Management

L'application Citrix Workspace pour iOS prend en charge quelques configurations supplémentaires à l'aide de paires clé-valeur basées sur AppConfig pour configurer l'application Citrix Workspace. Auparavant, les administrateurs pouvaient configurer les URL des magasins. Les administrateurs peuvent désormais empêcher les utilisateurs finaux de modifier les URL des magasins et contrôler comment s'affiche l'application.

Configuration key	Value type	Configuration value
url	String	myworkprod0.cloud.com
restrict_user_store_modification	Boolean	true
storeType	Integer	1

Les détails sont les suivants :

Clé de configuration	Type de valeur	Valeur de configuration
`url`	`String`	URL du magasin. Par exemple, `prodcwa.cloud.com`

Clé de configuration	Type de valeur	Valeur de configuration
storeType	Integer	• (défaut) Si ce paramètre est défini sur 1, les utilisateurs peuvent voir le magasin natif ou par défaut. - Si ce paramètre est défini sur 2, les utilisateurs peuvent voir le magasin dans une interface Web.
restrict_user_store_modification	Boolean	• Si ce paramètre est défini sur **true**, les utilisateurs ne peuvent pas modifier le magasin (ajouter/supprimer/modifier). - Si ce paramètre est défini sur **false**, les utilisateurs peuvent modifier le magasin. **Remarque :** si l'indicateur est défini sur true, tous les magasins existants sont supprimés avant l'ajout d'un magasin configuré avec UEM.

Prise en charge de la configuration du nom de l'appareil via UEM

À partir de la version 24.3.5, l'application Citrix Workspace pour iOS permet aux administrateurs d'attribuer et d'identifier des noms d'appareils en fonction de groupes d'utilisateurs via une solution Unified Endpoint Management (UEM).

Pour configurer le nom du périphérique à l'aide d'UEM, procédez comme suit :

> **Remarque :**
>
> À des fins de démonstration, Microsoft Intune est utilisé comme solution UEM dans cet exemple. Les étapes ci-dessous et l'interface utilisateur affichée varient en fonction de votre fournisseur UEM.

1. Connectez-vous à votre fournisseur UEM.

2. Ajoutez l'application Citrix Workspace que vous souhaitez gérer à l'aide du fournisseur UEM. Vous pouvez télécharger l'application en utilisant le portail de votre fournisseur UEM pour permettre la gestion par votre fournisseur UEM. Vous pouvez également créer un lien vers l'application dans l'App Store.
3. Créez une stratégie de configuration pour votre application.
4. Ajoutez une nouvelle paire clé-valeur à la liste des propriétés XML et renseignez les valeurs suivantes :

    - clé : deviceName
    - type de valeur : chaîne
    - valeur : nom de l'appareil (par exemple, MY_IPHONE_Device)

Périphériques

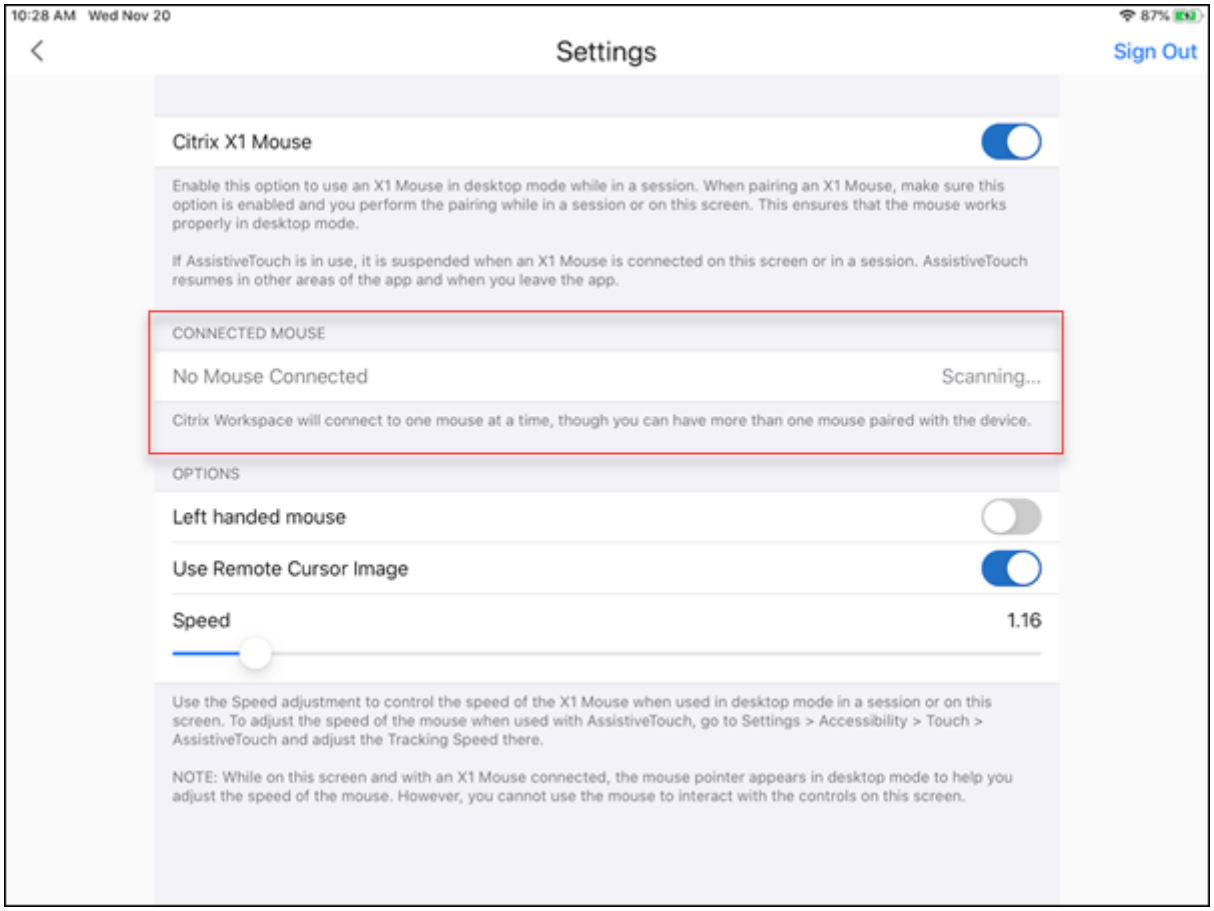
July 1, 2024

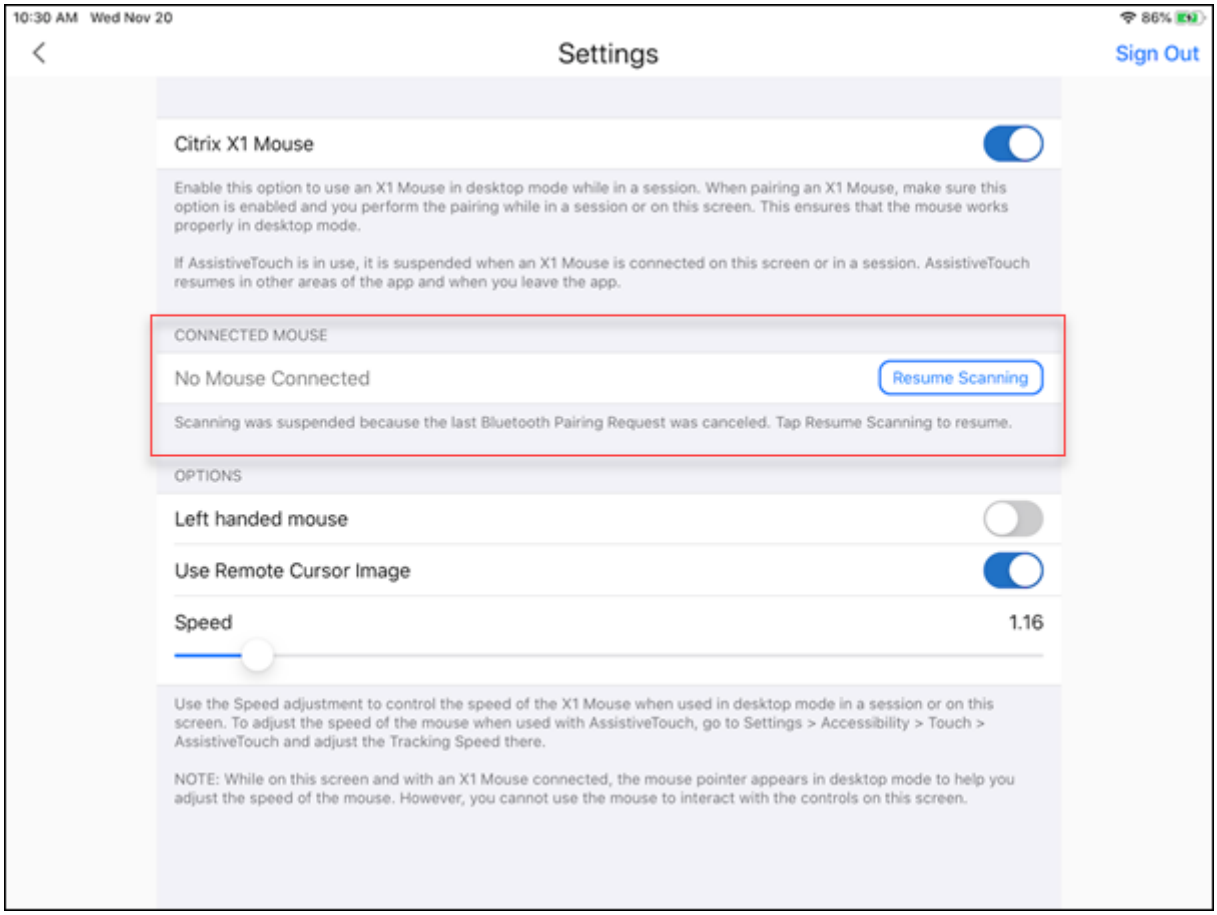
Souris Citrix X1

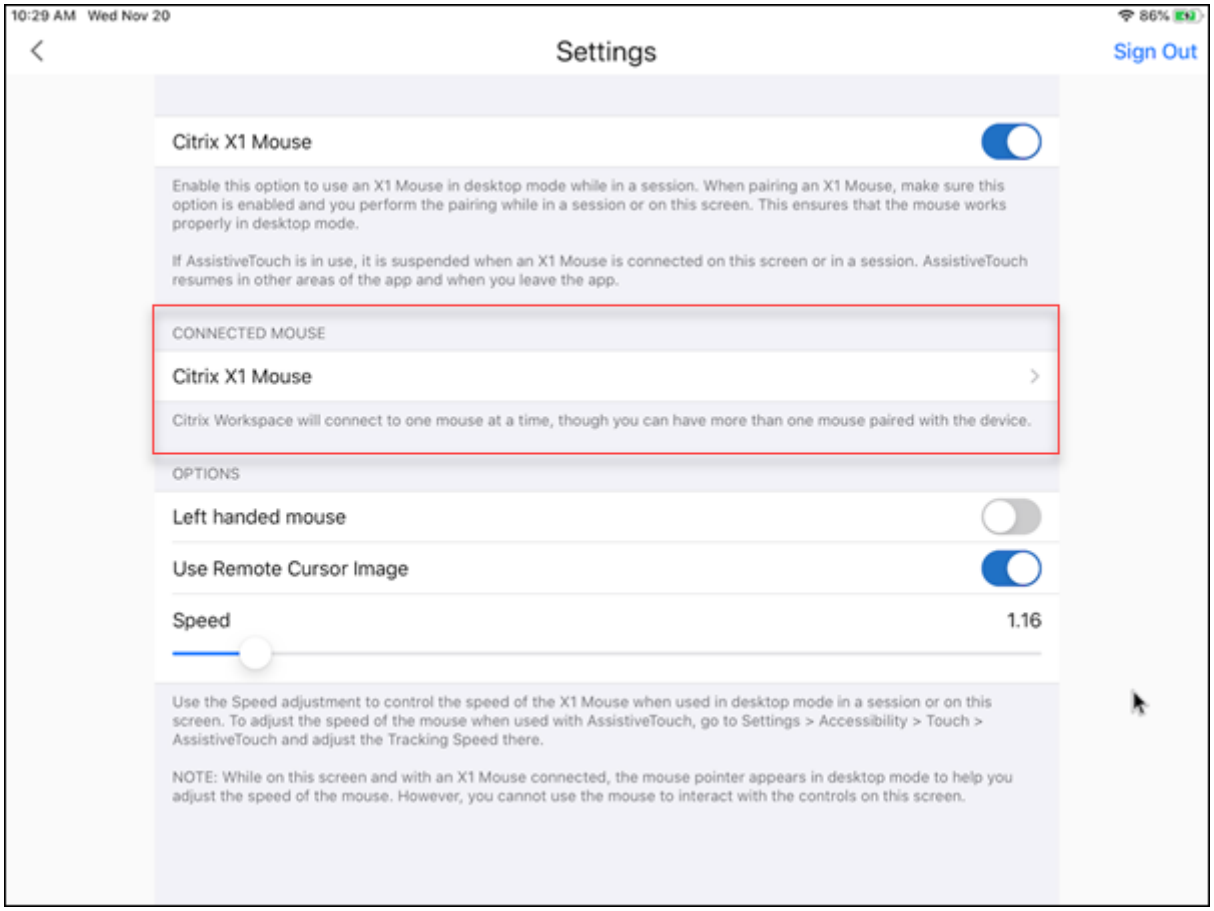
Couplage de la souris Citrix X1 et état de la connexion

Cette fonctionnalité vous permet d'avoir plus de contrôle sur le processus de couplage de la souris Citrix X1. Sur l'écran **Paramètres**, vous pouvez :

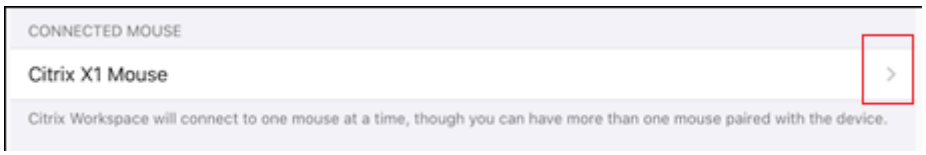
- Coupler la souris Citrix X1. Vous pouvez également coupler une souris X1 lorsque vous êtes dans une session.
- Afficher l'état de la connexion.







- Afficher les propriétés de la souris Citrix X1, telles que **Nom**, **UUID**, **Révision du firmware** et **Niveau de la batterie**. Pour ce faire, appuyez sur l'entrée de la souris Citrix X1 sous **SOURIS CONNECTÉE**.



Propriétés de la souris connectée :

AssistiveTouch Avec l'activation de la fonctionnalité AssistiveTouch sur iOS 13 ou version ultérieure, vous pouvez voir le curseur AssistiveTouch si vous basculez entre le mode souris de bureau et le mode AssistiveTouch.

> **Remarque :**
>
> En mode de souris du bureau, le curseur du pointeur s'affiche. En mode AssistiveTouch, le curseur arrondi s'affiche.

Le curseur AssistiveTouch apparaît dans les cas suivants :

- Quittez une session
- Accédez à l'écran iOS App Switcher
- Accédez à l'écran d'accueil iOS ou à une autre application

Le mode Bureau reprend lorsque vous revenez à l'application Citrix Workspace et lorsque vous êtes dans une session.

Prise en charge d'un moniteur externe et de la barre d'outils

Vous pouvez utiliser la souris Citrix X1 pour utiliser la barre d'outils sur un moniteur externe. Vous pouvez déplacer l'encoche de la barre d'outils horizontalement même lorsque la barre d'outils est fermée. Lorsque vous connectez votre appareil iOS au moniteur externe, l'application Citrix Workspace détecte automatiquement la résolution d'écran du moniteur externe. Vous pouvez utiliser le bouton **Affichage** de la barre d'outils pour sélectionner une résolution d'écran particulière. Vous pouvez accéder à l'option **Affichage** sans avoir à ajouter de compte ou à vous connecter.

Souris générique

Prise en charge de la souris et du trackpad génériques

Vous pouvez utiliser une souris ou un trackpad générique pour cliquer avec le bouton droit de la souris, faire défiler et survoler dans les sessions HDX. Les actions sont similaires à celles de la souris Citrix X1. Le style du curseur local de la souris change pour correspondre à celui du curseur distant.

> **Remarques :**
>
> - Cette fonctionnalité est disponible sur iPadOS 13.4 et versions ultérieures.
> - Cette fonctionnalité n'est pas prise en charge sur les iPhones.

Limitation Si un moniteur externe est connecté pendant une session, le curseur de la souris générique reste sur le périphérique natif en raison d'une limitation iOS.

Prise en charge de la souris générique sur les moniteurs externes

Vous pouvez utiliser une souris générique sur des moniteurs externes connectés à un iPad. La souris générique est prise en charge sur les appareils exécutant iOS 13.4 ou version ultérieure.

> **Important :**
>
> Pour utiliser une souris générique avec des moniteurs externes, vérifiez que le mode **Présentation** est désactivé dans votre application Citrix Workspace en accédant à **Paramètres** > **Options d'affichage**.

La barre d'outils du moniteur externe est masquée lorsque vous utilisez une souris générique. En outre, le pointeur de la souris est mis en miroir sur le moniteur externe et apparaît simultanément sur l'écran de votre iPad et sur le moniteur externe.

Prise en charge de plusieurs moniteurs étendue avec la souris générique pour iPad

Vous pouvez étendre la session de bureau sur un moniteur externe lorsque vous connectez une souris générique à votre iPad. Cette fonctionnalité prend en charge les versions 14.0 et ultérieures d'iPadOS.

> **Remarque :**
>
> - Cette fonctionnalité peut être partiellement disponible dans les versions antérieures. Pour utiliser la fonctionnalité complète, effectuez une mise à niveau vers la version 22.1.0.
> - Désactivez AssistiveTouch dans **Réglages** iOS > **Accessibilité** > **Toucher** > **AssistiveTouch** pour que l'application Citrix Workspace reçoive les clics gauche de la souris.

Configurer le mode Étendre Pour activer le mode **Étendre** :

1. Connectez le moniteur externe à l'iPad à l'aide du câble HDMI et des adaptateurs requis.

   > **Remarque :**
   >
   > La configuration fonctionne mieux avec un adaptateur USB-C vers Digital AV Multiport d'Apple ou un adaptateur Lightning Digital AV.

2. Accédez aux **Paramètres** > **Options d'affichage** de l'application et **activez** l'option **Affichage externe**. Différents modes d'affichage apparaissent. Les modes Miroir et Présentation utilisent également la souris générique, si la version iPadOS est 14.0 ou ultérieure.
3. Sélectionnez l'option **Étendre**.

   Vous pouvez sélectionner l'un des modes d'affichage suivants :

   - Miroir : vous permet de dupliquer l'affichage sur le moniteur externe connecté à l'iPad.
   - Présentation : vous permet de passer de votre moniteur externe à un trackpad.
   - Étendre : vous permet d'afficher des vues ou des écrans différents sur chaque affichage.

> **Remarque :**
>
> - Définissez le mode **Étendre** avant de lancer et d'étendre la session de bureau.
> - Le mode **Étendre** n'est pas pris en charge sur l'iPhone tant que cela n'a pas été officialisé.

Configurer la disposition de l'affichage Pour configurer la disposition de l'affichage :

1. Sélectionnez le mode **Étendre**, l'option **Disposition de l'affichage** apparaît.
2. Repositionnez la vignette **Affichage externe** à gauche, en haut, à droite ou en bas sur l'écran de l'iPad.

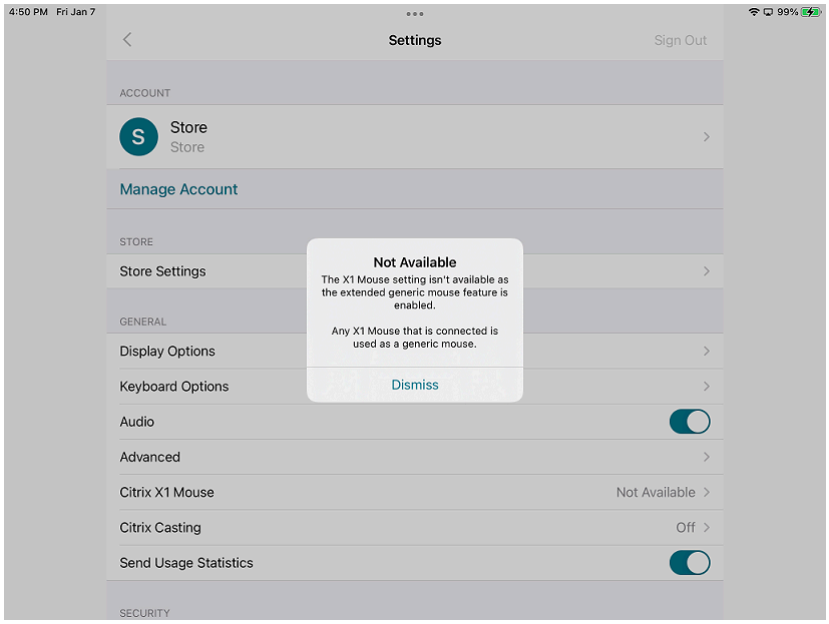
> **Remarque :**
>
> Vous pouvez ajuster la disposition de l'affichage lorsque vous êtes dans une session à l'aide de la barre d'outils de session > icône du paramètre **Affichage**.

> **Remarque :**
>
> La résolution de l'écran externe dépend des éléments suivants :
>
> - Adaptateurs
> - iPad
> - Autre matériel utilisé

Mode de souris générique par rapport au mode de souris Citrix X1

Le mode de souris générique a priorité sur le mode de souris Citrix X1. Si une souris X1 est connectée, elle est utilisée comme souris générique. Par conséquent, la page des paramètres de la souris X1 n'est pas accessible lorsque l'indicateur de fonctionnalité Souris générique est activé.

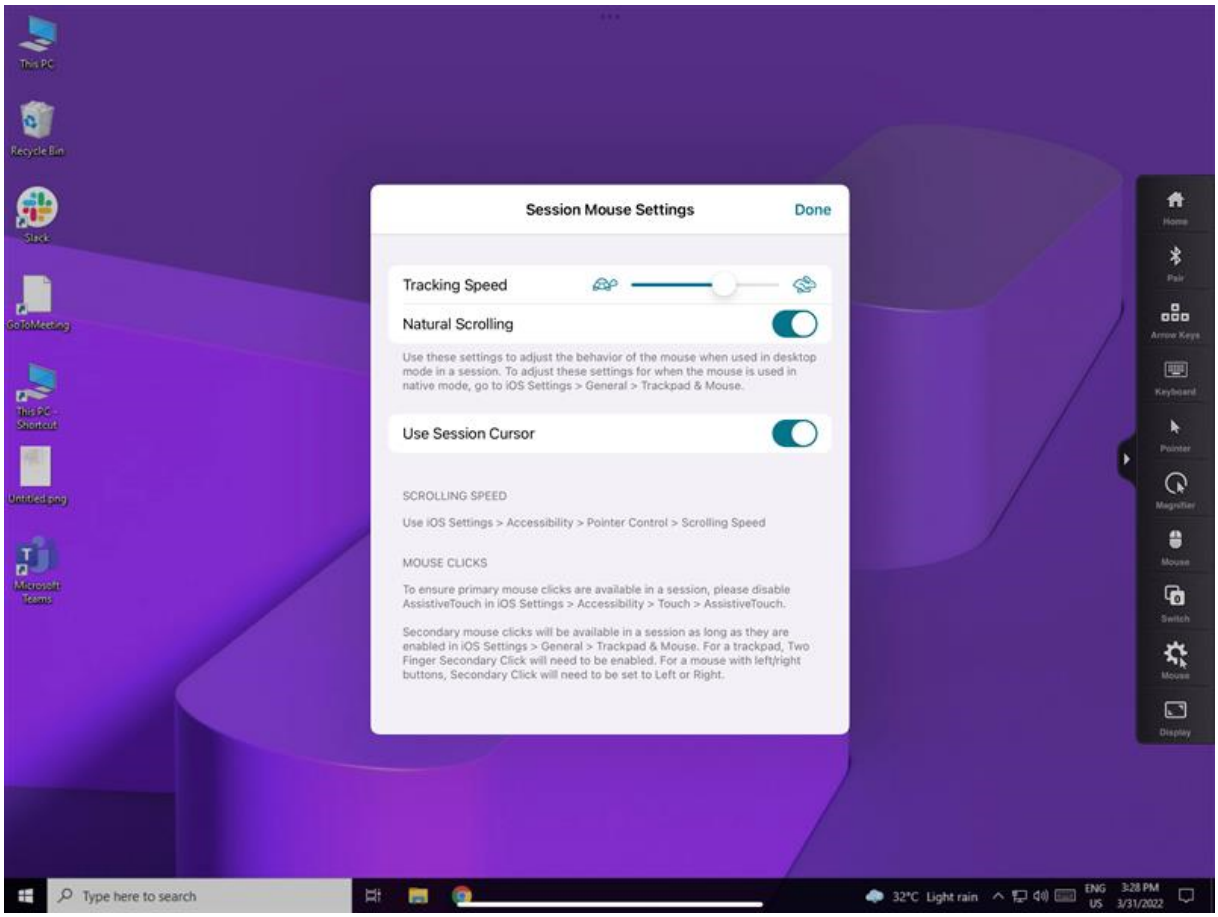
> **Remarque :**
>
> Pour les versions 14.0 et ultérieures d'iPadOS, toute souris X1 connectée à l'iPad se comporte comme une souris Bluetooth.



Icône de souris générique

L'icône des paramètres de la **souris** est ajoutée dans la barre d'outils de session en regard de l'icône des paramètres **d'affichage**. Utilisez les paramètres de la **souris** pour régler la vitesse de déplacement de la souris générique lorsque vous êtes dans une session. Vous pouvez également l'activer/la désactiver à l'aide de l'image du curseur distant.

> **Remarque :**
>
> Vous pouvez régler la vitesse de déplacement de la souris native à partir des réglages iOS.



Limitations de la fonctionnalité

- Pour vous assurer que les clics de souris principaux sont disponibles dans l'application Citrix Workspace, désactivez AssistiveTouch dans **Paramètres iOS** > **Accessibilité** > **Toucher** > **AssistiveTouch**.
- Les options Vitesse de suivi et Défilement naturel des paramètres iOS n'affectent pas la souris générique au sein de la session. Toutefois, la vitesse de défilement peut être contrôlée à partir des **paramètres iOS**.

Vous pouvez accéder aux options Vitesse de suivi et Défilement naturel depuis l'écran **Paramètres de la souris** de la barre d'outils de la session.

- Lorsqu'un iPad est utilisé en mode partagé et que le moniteur est connecté, la souris générique fonctionne uniquement en mode miroir dans une session de bureau.
- Si le curseur natif se trouve sur le menu multitâche avant que l'application obtienne le verrouillage du pointeur, c'est-à-dire avant le lancement de la session, les événements de souris ne sont pas reçus.
  Pour contourner le problème, déplacez le Centre de notifications vers le bas, déplacez le pointeur natif vers un autre emplacement et quittez le Centre de notifications.
- La redirection audio échoue lorsque vous connectez un iPad à un moniteur externe. Le son est diffusé via les haut-parleurs de l'iPad. [HDX-39159]

Problèmes connus liés à cette fonctionnalité

- Lorsque la session est active, l'image du bureau qui apparaît sur un iPad ou un moniteur externe est altérée lorsque vous modifiez ce qui suit :
  - Disposition de l'affichage
  - Résolution
  - Orientation ou
  - Modes d'affichage

  Pour contourner le problème, déconnectez et reconnectez le moniteur. Si le problème persiste, déconnectez et relancez la session. [HDX-37038] [HDX-36979] [HDX-36925] [HDX-36924].
- Dans de rares cas, vous pouvez observer un décalage de quelques secondes dans l'audio lorsque la vidéo est lue sur le moniteur externe. [HDX-39159]
- Dans de rares cas, l'affichage du VDA est tronqué sur un iPad et sur le moniteur externe. Pour contourner le problème, déconnectez et reconnectez le moniteur. Si le problème persiste, déconnectez et relancez la session. [HDX-37100]
- Lorsque vous agrandissez la vidéo en plein écran sur le moniteur externe, vous pouvez observer des problèmes de qualité vidéo. [HDX-39159]
- Dans de rares cas, au cours d'une session de bureau, une tentative de déplacement des applications d'un iPad vers le moniteur externe échoue. Pour contourner le problème, déconnectez et reconnectez le moniteur. Si le problème persiste, déconnectez et relancez la session. [HDX-36981]
- Dans de rares cas, lorsque vous connectez un iPad à un moniteur externe à l'aide d'adaptateurs tiers, les modes d'affichage ne sont pas visibles sous les options d'affichage. [HDX-39713]
- Parfois, une ligne est observée sous le pointeur de la souris dans la session VDA. [RFIOS-9569]

Prise en charge du clavier

Synchronisation de la disposition du clavier

La synchronisation de la disposition du clavier permet aux utilisateurs de basculer entre leurs dispositions de clavier préférées sur la machine cliente. Cette fonction est désactivée par défaut.

Pour activer la synchronisation de la disposition du clavier, accédez à **Paramètres** > **Options du clavier** et activez l'option **Synchronisation de la disposition du clavier**.

> **Remarque :**
>
> L'utilisation de l'option de disposition du clavier local active l'éditeur IME (Éditeur de méthode d'entrée) du client. Si vous travaillez en japonais, chinois simplifié ou coréen et que vous préférez utiliser l'éditeur IME du serveur, désactivez l'option de disposition du clavier local en désélectionnant l'option dans **Préférences** > **Clavier**.

Logiciels requis

- Pour Linux VDA, activez la stratégie Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME.
- Pour les VDA Windows, activez les stratégies Mappage de disposition du clavier Unicode, Synchronisation de la disposition du clavier client et Améliorations apportées à l'éditeur IME.
- Le VDA doit être la version 7.16 ou ultérieure.

Prise en charge de la disposition du clavier pour VDA Windows et VDA Linux

Disposition du clavier sur iOS	Langue du clavier	Disposition du clavier sur Windows	Disposition du clavier sur Linux
Biélorusse (Biélorussie)	Biélorusse (Biélorussie)	Clavier biélorusse (Biélorussie)	by
Bulgare	Bulgare	Clavier bulgare (machine à écrire)	bg
Chinois (Simplifié)	Chinois (simplifié, Chine)	Citrix IME - Chinois (simplifié, Chine)	zh
Chinois (traditionnel)	Chinois (traditionnel, Taïwan)	Citrix IME - Chinois (traditionnel, Taïwan)	tw
Croate	Croate (Croatie)	Clavier croate	hr
Tchèque	Tchèque	Clavier tchèque	cz
Danois	Danois	Clavier danois	df

Disposition du clavier sur iOS	Langue du clavier	Disposition du clavier sur Windows	Disposition du clavier sur Linux
Néerlandais	Néerlandais (Pays-Bas)	Clavier américain - international	us
Néerlandais (Belgique)	Néerlandais	Clavier belge (d' époque)	be
Anglais (Australie)	Anglais (Australie)	Clavier américain	us
Anglais (Canada)	Anglais (Canada)	Clavier américain	us
Anglais (Royaume-Uni)	Anglais (Royaume-Uni)	Clavier britannique	gb
Anglais (États-Unis)	Anglais (États-Unis)	Clavier américain	us
Estonien	Estonien	Clavier estonien	ee
Finnois	Finnois	Clavier finnois	fi
Français (Canada)	Français (Canada)	Clavier français	fr
Français (Suisse)	Français (France)	Clavier français de Suisse	ch
Français (français)	Français (France)	Clavier français	fr
Allemand (Autriche)	Allemand (Autriche)	Clavier allemand	at
Allemand (Suisse)	Allemand (Suisse)	Clavier suisse allemand	ch
Allemand (Allemagne)	Allemand (Allemagne)	Clavier allemand	at
Grec	Grec	Clavier grec	gr
Hongrois	Hongrois	Clavier hongrois	hu
Islandais	Islandais	Clavier islandais	is
Irlandais	Irlandais		ie
Italien	Italien (Italie)	Clavier italien	it
Japonais	Japonais	Citrix IME - japonais	jp
Coréen	Coréen	Citrix IME - Coréen	kr
Letton	Letton	Clavier letton	lv
Norvégien	Norvégien (Bokmål)	Clavier norvégien	non
Polonais	Polonais	Clavier polonais (programmeurs)	pl
Portugais (Brésil)	Portugais (Brésil)	Clavier portugais (ABNT du Brésil)	br

Disposition du clavier sur iOS	Langue du clavier	Disposition du clavier sur Windows	Disposition du clavier sur Linux
Portugais (Portugal)	Portugais (Portugal)	Clavier portugais	pt
Roumain	Roumain (Roumanie)	Clavier roumain (ancien)	ro
Russe (Russie)	Russe	Clavier russe	ru
Slovaque	Slovaque	Clavier slovaque	sk
Slovène	Slovène	Clavier slovène	si
Espagnol (Mexique)	Espagnol (Mexique)	Clavier latino-américain	latam
Espagnol (Espagne)	Espagnol (Espagne)	Clavier espagnol	es
Suédois (Suède)	Suédois (Suède)	Clavier suédois	se
Turc	Turc	Clavier turc F	tr
Ukrainien	Ukrainien	Clavier ukrainien	ua

Prise en charge des touches spéciales

Prise en charge des touches simples suivantes sur un clavier externe avec iOS 13.4 et versions ultérieures :

- Pg Préc.
- Pg Suiv.
- Accueil
- Fin
- F1
- F2
- F3
- F4
- F5
- F6
- F7
- F8
- F9
- F10
- F11
- F12

Prise en charge de combinaisons de touches spéciales

Cette version prend en charge les combinaisons de touches suivantes sur les claviers externes iOS :

- Windows + R
- Windows + D
- Windows + E
- Windows + L
- Windows + M
- Windows + S
- Windows + CTRL+ S
- Windows + T
- Windows + U
- Windows + numéro
- Windows + Haut
- Windows + Bas
- Windows + Gauche
- Windows + Droite
- Windows + X
- Windows + K
- CTRL + ÉCHAP

Améliorations apportées au clavier étendu

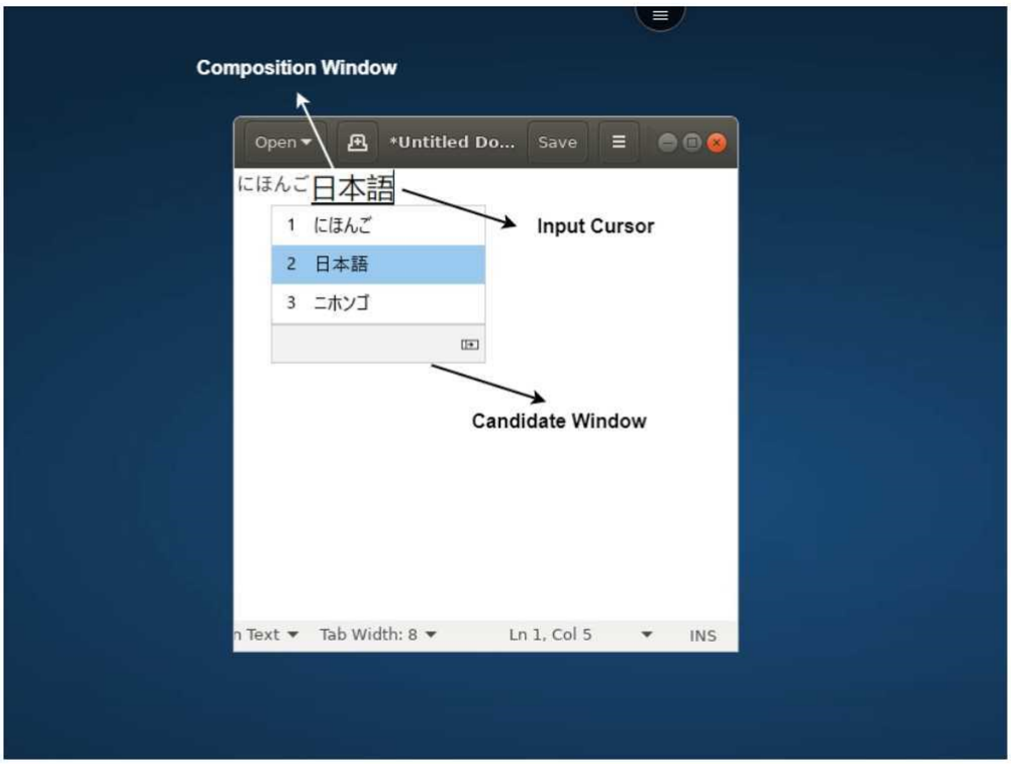
À partir de la version 23.5.0, la fonctionnalité de clavier étendu a été améliorée pour offrir une meilleure expérience utilisateur. Les améliorations sont les suivantes :

- Possibilité d'épingler ou de détacher l'interface utilisateur de la barre d'outils étendue
- Possibilité de faire pivoter la barre d'outils étendue en phase avec la rotation de l'écran
- Prise en charge des raccourcis clavier Windows et des raccourcis utilisant une combinaison de 3 touches.
- Amélioration de l'expérience dans les scénarios dans lesquels plusieurs écrans sont utilisés
- Possibilité d'ouvrir ou de réduire automatiquement l'interface utilisateur de la barre d'outils étendue
- Amélioration de l'expérience du mode Stage Manager (sur iPad avec puce M1)

Interface utilisateur de l'éditeur IME

En général, l'éditeur IME fournit des composants d'interface utilisateur tels que la fenêtre candidate et la fenêtre de composition. La fenêtre de composition contient les caractères de composition et

les éléments de l'interface utilisateur de composition, par exemple le soulignement et la couleur d'arrière-plan. La fenêtre candidate affiche la liste des candidats.



La fenêtre de composition permet de distinguer les caractères confirmés des caractères de composition. La fenêtre de composition et la fenêtre candidate se déplacent avec le curseur de saisie.

Par conséquent, la fonctionnalité fournit :

- Une saisie améliorée des caractères à l'emplacement du curseur dans la fenêtre de composition.
- Un affichage amélioré dans la fenêtre candidate et de composition.

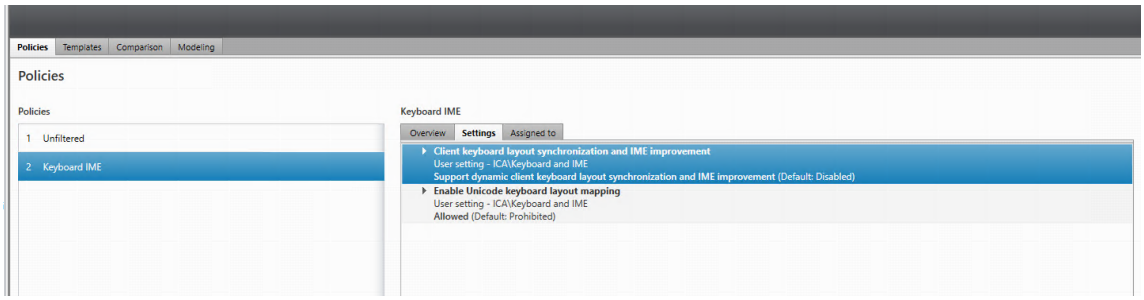
Vous pouvez actuellement utiliser cette fonctionnalité sur les sessions hébergées sur des VDA Windows ; elle prend en charge à la fois les claviers logiciels et les claviers physiques externes.

Éditeur IME client générique pour les langues d'Asie orientale

La fonctionnalité d'éditeur IME client générique (IME) améliore l'expérience de saisie et d'affichage des caractères chinois, japonais et coréen (CJK) sur les appareils iOS. Cette fonctionnalité vous permet de composer des caractères CJK à la position du curseur à l'aide de vos éditeurs IME client lorsque vous êtes dans une session. La fonctionnalité est disponible pour les environnements VDA Windows. Il est recommandé d'utiliser l'éditeur IME client au lieu de l'éditeur IME côté VDA pour une meilleure expérience utilisateur.

Logiciels requis

- Activez la synchronisation de la disposition du clavier client et l'amélioration de l'éditeur IME et activez le mappage du clavier Unicode sur votre VDA Windows via la stratégie de groupe.



Pour obtenir davantage d'informations, veuillez consulter l'article CTX312404 du centre de connaissances.

Vous pouvez également activer les options à l'aide des registres suivants sur votre VDA Windows :

```
- HKLM\Software\Citrix\ICA\IcaIme\DisableKeyboardSync value = DWORD 0
- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\EnableKlMap value =
  DWORD 1
- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\DisableWindowHook value
  = DWORD 1
```

- Activez l'option **Paramètres** > **Options du clavier** > **Synchronisation de la disposition du clavier** dans l'application Citrix Workspace.

Prise en charge du mode de saisie Scancode

À partir de la version 24.1.0, vous pouvez sélectionner **Scancode** comme mode de saisie au clavier lorsque vous utilisez un clavier physique externe. Cette fonctionnalité est utile lorsque vous utilisez des appareils iOS dotés du clavier standard d'un PC Windows externe. Avec **Scancode**, vous pouvez utiliser la disposition du clavier du VDA au lieu de celle du clavier d'iOS. De cette façon, vous pouvez suivre complètement le style de saisie du clavier Windows externe au lieu de celui d'iOS. C'est utile lorsque vous effectuez des saisies dans des langues d'Asie de l'Est, car cela améliore considérablement l'expérience utilisateur globale. L'utilisateur final peut se retrouver à utiliser la disposition du clavier du serveur au lieu de celle du client. Pour en savoir plus, consultez la section Cas d'utilisation de cet article.

Pour utiliser la fonctionnalité **Scancode**, procédez comme suit :

1. Ouvrez l'application Citrix Workspace pour iOS et accédez à **Paramètres > Options du clavier**.
2. Appuyez sur **Mode de saisie du clavier externe**.

3. Sélectionnez l'une des options suivantes :

    - **Scancode :** la position des touches du clavier côté client est envoyée au VDA et le VDA génère le caractère correspondant. Applique la disposition du clavier côté serveur.
    - **Unicode :** la touche du clavier côté client est envoyée au VDA et le VDA génère le même caractère dans le VDA. Applique la disposition du clavier côté client.

    Par défaut, **Unicode** est sélectionné comme mode de saisie à la fois pour le clavier logiciel ou tactile et pour le clavier externe.

4. Appuyez sur **Scancode**.

    En cours de session, vous pouvez changer la disposition du clavier distant, du clavier du serveur ou du clavier du VDA et effectuer des saisies suite à ce changement.

Cas d'utilisation Par exemple, imaginez un scénario dans lequel vous utilisez une disposition de clavier internationale américaine connectée à votre appareil iOS.
Lorsque vous choisissez **Scancode** et que vous appuyez sur la touche à côté de Verr Maj sur votre clavier externe, le **Scancode 1E** est envoyé au VDA. Le VDA utilise ensuite **1E** pour afficher le caractère **a**.
Si vous choisissez **Unicode** et que vous appuyez sur la touche à côté de Verr Maj sur votre clavier externe, le caractère **a** est envoyé au VDA. Ainsi, même si le VDA utilise une autre disposition de clavier comportant un caractère différent à la même position, le caractère **a** s'affiche à l'écran.

> **Remarque :**
>
> **Unicode** est le mode de saisie à privilégier lorsque vous utilisez un clavier tactile sur vos appareils mobiles. En effet, les touches d'un clavier tactile ne génèrent généralement pas de Scancode.

Améliorations de la prise en charge des raccourcis clavier externes

L'application Citrix Workspace pour iOS vous permet désormais d'utiliser davantage de raccourcis depuis des claviers externes lors d'une session d'application ou de bureau à distance. Voici quelques-unes des améliorations importantes apportées aux raccourcis clavier externes :

- Prise en charge des touches propres au clavier Windows, telles que **Inser** et **Suppr**, et du pavé numérique.
- Lorsque vous maintenez une touche enfoncée sans la relâcher, l'application/le bureau à distance répond correctement.
- Prise en charge de raccourcis avec plus de trois touches.

En outre, vous pouvez désormais configurer la touche spécifique pour **Alt** en utilisant les options suivantes via **Paramètres > Options du clavier > Attribuer une touche spécifique pour Alt** :

- **Option ou Alt (gauche)** : envoie **Alt** en utilisant **Option (gauche) ou Alt (gauche)**.
- **Commande ou Windows (gauche)** : envoie **Alt** en utilisant les touches **Commande (gauche) ou Windows (gauche)**.
- **Option ou Alt (gauche et droite)** : envoie **Alt** en utilisant la touche **Option ou Alt (gauche et droite)** .

L'option **Attribuer une touche spécifique pour Alt** permet d'éviter les conflits entre la touche macOS **Option** et la touche Windows **Alt**.

Limitations Les raccourcis système iOS suivants ne sont actuellement pas pris en charge :

- **Commande (Windows)-H** : permet d'accéder à l'écran d'accueil.
- **Commande (Windows)-Barre d'espace** : affiche ou masque le champ de recherche.
- **Commande (Windows)-Tab** : passe à l'application la plus récemment utilisée parmi les applications ouvertes.
- **Commande (Windows)-Maj-3** : prend une capture d'écran.
- **Commande (Windows)-Maj-4** : prend une capture d'écran et ouvre immédiatement Markup pour l'afficher ou la modifier.
- **Commande (Windows)-Option (Alt)-D** : affiche ou masque le Dock.
- **Commande (Windows)-Ctrl-Q** : verrouille l'appareil.
- La touche **AltGr** du clavier européen n'est pas prise en charge. Si vous souhaitez saisir des caractères spéciaux avec **AltGr**, utilisez plutôt les raccourcis suivants :
  - Raccourci macOS **Option+*** ou
  - Raccourci OS Windows **Alt + pavé numérique**.

Accès au microphone et à la caméra

Vous pouvez maintenant accéder à votre microphone et à votre caméra pour des conférences audio-vidéo via une session VDA. L'application Citrix Workspace requiert votre autorisation pour accéder au microphone ou à la caméra, ce qui peut être fourni en accédant aux **paramètres** de votre appareil et en activant la caméra ou le microphone.

En outre, l'accès au microphone et à la caméra par magasin dans le cadre de la fonctionnalité Client Selective Trust a été inclus pour permettre à l'application Citrix Workspace d'approuver l'accès à partir d'une session VDA.

L'application Citrix Workspace requiert l'autorisation de l'utilisateur pour accéder au microphone ou à la caméra.

Vous pouvez configurer les niveaux d'accès en accédant à **Paramètres > Paramètres du magasin**. Dans le menu **Paramètres du magasin**, cliquez sur un magasin pour activer l'accès au microphone

ou à la caméra. Le paramètre sélectionné pour l'accès au microphone où à la caméra est appliqué par magasin.

Support de caméra arrière

L'application Citrix Workspace pour iOS vous permet désormais de changer la position de la caméra de l'avant vers l'arrière et inversement, au cours de la session de VDA.

Un bouton flottant apparaît lorsque vous appelez la caméra. Appuyez une fois sur le bouton flottant pour basculer entre les positions avant et arrière de la caméra.

Vous pouvez également déplacer librement le bouton flottant sur l'écran et le placer n'importe où.

Problèmes connus :

Le bouton flottant est partiellement ou totalement obstrué lorsque la fonction de casting ou de numérisation de documents est activée.

Graphisme et affichage

Performances graphiques améliorées

À partir de la version 24.1.0, l'application Citrix Workspace pour iOS prend en charge le codage ou le décodage vidéo H.264 avec accélération matérielle. Le moteur multimédia de Citrix HDX utilise désormais l'infrastructure Video Toolbox d'Apple pour le codage et le décodage. Cette infrastructure compresse et décompresse la vidéo plus rapidement et en temps réel. Cette amélioration réduit la charge sur l'unité centrale lors de l'utilisation du multimédia.

Mappage des lecteurs clients (CDM)

Vous pouvez sélectionner un accès au stockage de périphérique spécifique pour chaque magasin configuré. L'accès au stockage de périphérique comporte les options suivantes.

- Aucun accès
- Accès en lecture seule
- Accès en lecture et en écriture
- Toujours me demander

Si vous sélectionnez **Toujours me demander**, une invite s'affiche, vous demandant de sélectionner le type d'accès au stockage du périphérique à chaque lancement. Par défaut, l'option **Aucun accès** est sélectionnée.

> **Remarque :**
>
> Cette fonctionnalité s'applique uniquement aux lancements ICA directs et aux magasins configurés pour Citrix Gateway. Les magasins sans configuration SSL de bout en bout ne sont pas pris en charge.

Les paramètres **Stockage de l'appareil** sont disponibles dans une nouvelle section des paramètres appelée **Paramètres du magasin**. Pour afficher le **Stockage de l'appareil**, accédez à **Paramètres** > **Paramètres du magasin**.

Citrix Ready Workspace Hub

Citrix Ready Workspace Hub combine des environnements numériques et physiques pour fournir des applications et des données dans un espace intelligent sécurisé. Le système complet connecte des appareils (ou objets), comme des applications mobiles et des capteurs, pour créer un environnement intelligent et réactif.

Citrix Ready Workspace Hub est basé sur la plate-forme Raspberry Pi 3. L'appareil exécutant l'application Citrix Workspace se connecte au Citrix Ready Workspace Hub et diffuse les applications ou les bureaux sur un écran plus grand.

Pour plus d'informations sur Citrix Ready Workspace Hub, consultez la documentation relative à Citrix Ready Workspace Hub.

Citrix Ready Workspace Hub prend en charge une connexion SSL entre les appareils mobiles et le hub à des fins de sécurité. Définissez un nom de domaine complet (FQDN) manuellement ou automatiquement pour identifier de manière unique chaque appareil. Pour plus d'informations, consultez Connexion sécurisée dans la documentation relative à Citrix Ready Workspace Hub.

Citrix Ready Workspace Hub est activé sur l'application Citrix Workspace lorsque toutes les conditions suivantes sont remplies :

- Application Citrix Workspace 1810.1 pour iOS ou version ultérieure
- Bluetooth activé
- Appareil mobile et hub d'espace de travail utilisant le même réseau Wi-Fi

Configurer Citrix Ready Workspace Hub

Pour activer les fonctionnalités de Citrix Ready Workspace Hub, accédez à **Paramètres** et touchez **Citrix Casting** pour activer la fonctionnalité sur votre appareil. Pour plus d'informations, consultez la documentation d'aide pour les appareils iOS.

L'application Citrix Workspace intègre une nouvelle procédure permettant d'ajouter ou de supprimer un Workspace Hub de la liste de confiance sur les appareils iOS. Pour plus d'informations, consultez la section Connexion sécurisée.

Prise en charge des scanners de documents

À partir de la version 24.5.0, l'application Citrix Workspace pour iOS prend en charge la fonctionnalité de numérisation de documents. Grâce à cette fonctionnalité, vous pouvez désormais numériser et enregistrer plusieurs documents, le tout dans la session de bureau. Cette fonctionnalité est activée par défaut.

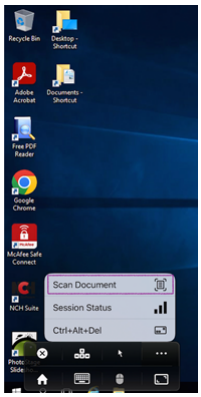
Logiciels requis

- Le mappage des lecteurs clients (CDM) doit être activé pour le magasin.
- La fonction de scanner de documents nécessite un accès en lecture et en écriture sur votre appareil. Pour donner accès, procédez comme suit :

    1. Depuis votre profil, touchez Paramètres de **l'application > Paramètres du magasin**.
    2. Appuyez sur votre magasin actuel.
    3. Touchez **Stockage de l'appareil** et sélectionnez **Accès complet**.

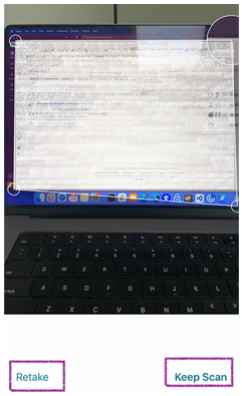
Pour numériser des documents à l'aide du scanner de documents, procédez comme suit :

1. Dans la barre d'outils de la session, touchez le menu des points de suspension et sélectionnez **Scanner document**. L'application de la caméra s'ouvre.

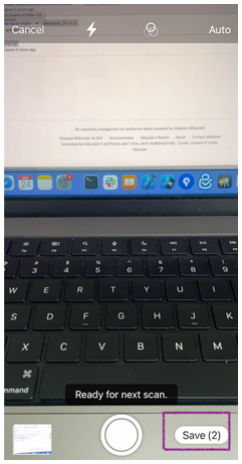


2. Touchez le déclencheur pour prendre la photo. Si vous choisissez de reprendre la photo, touchez **Reprendre**.

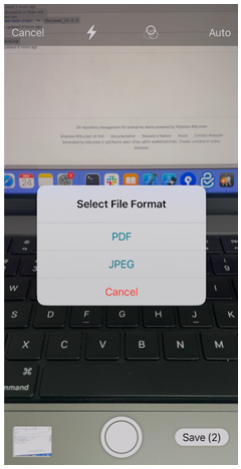
3. Facultatif : recadrez le document numérisé. Après avoir recadré à la taille requise, touchez **Continuer à numériser**. L'application de la caméra s'ouvre à nouveau pour vous permettre de capturer plus d'images.



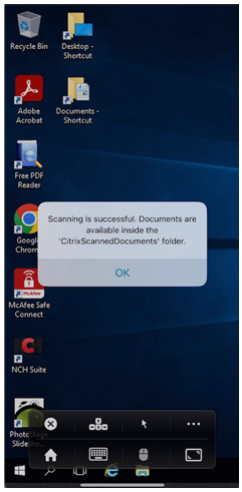
4. Après avoir capturé les images requises, touchez **Enregistrer**.



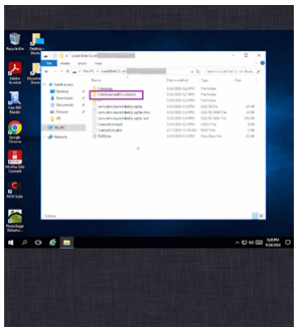
5. Sélectionnez l'option de format de fichier pour enregistrer le document numérisé dans le format requis.



6. Touchez **OK**.



Tous les documents numérisés sont accessibles dans le dossier **CitrixScannedDocuments** du stockage local de l'appareil. Vous pouvez également accéder aux documents **CitrixScannedDocuments** dans le gestionnaire de fichiers de session.

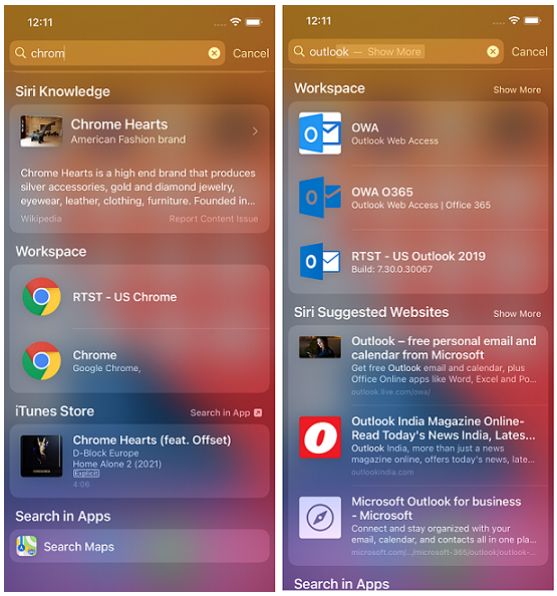


Expérience utilisateur

May 9, 2024

Amélioration de la recherche dans Spotlight

L'icône de l'application correspond à la recherche d'application correspondante. Auparavant, l'icône de l'application Citrix Workspace était affichée pour toutes les recherches.



Accès aux applications récentes à l'aide des gestes 3D-Touch

Vous pouvez accéder à la liste des applications récemment lancées pour y accéder rapidement lorsque vous utilisez le geste 3D-Touch (appui long) sur l'icône de l'**application Citrix Workspace**.

Indicateur d'état de la batterie

L'état de la batterie de l'appareil s'affiche désormais dans la zone de notification d'une session de bureau virtuel.

Cette fonctionnalité est prise en charge uniquement sur les versions 7.18 et ultérieures du VDA.

> **Remarque :**
>
> Dans les sessions exécutées sur des VDA Microsoft Windows 10, l'indicateur d'état de la batterie peut prendre environ 1 à 2 minutes avant d'apparaître.

Fonctionnalité Appuyer de manière prolongée pour accéder à la ressource

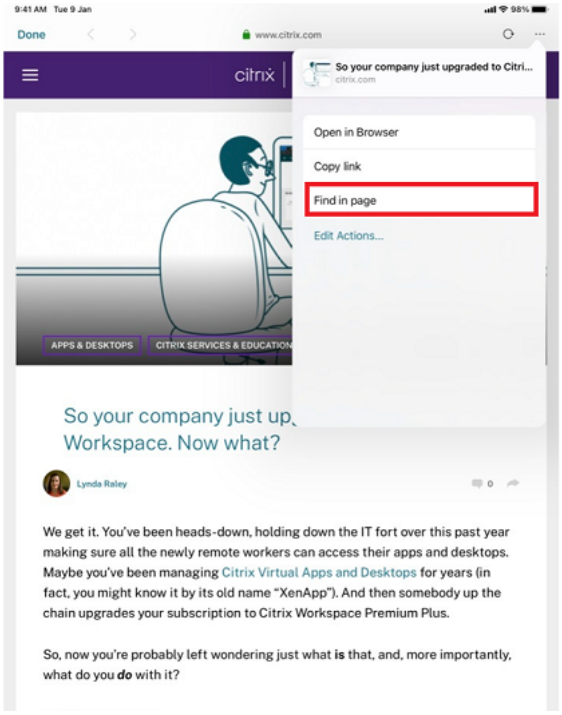
Vous pouvez maintenant appuyer de manière prolongée sur l'icône de l'application Citrix Workspace pour accéder à votre dernière ressource lancée. Vous pouvez désormais quitter l'application Citrix Workspace et accéder à votre dernière ressource lancée.

Amélioration de la recherche dans la page

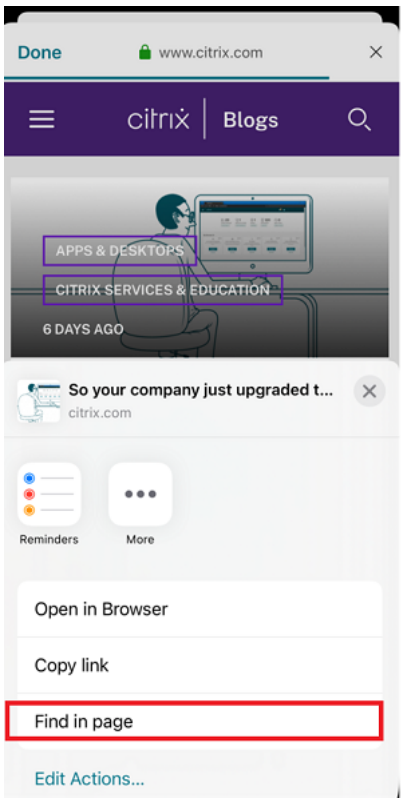
L'amélioration de la recherche dans la page vous permet de rechercher des mots ou des expressions. Cette amélioration au niveau de la convivialité est disponible dans vos applications Web et SaaS (Software-as-a-Service).

Pour effectuer une recherche :

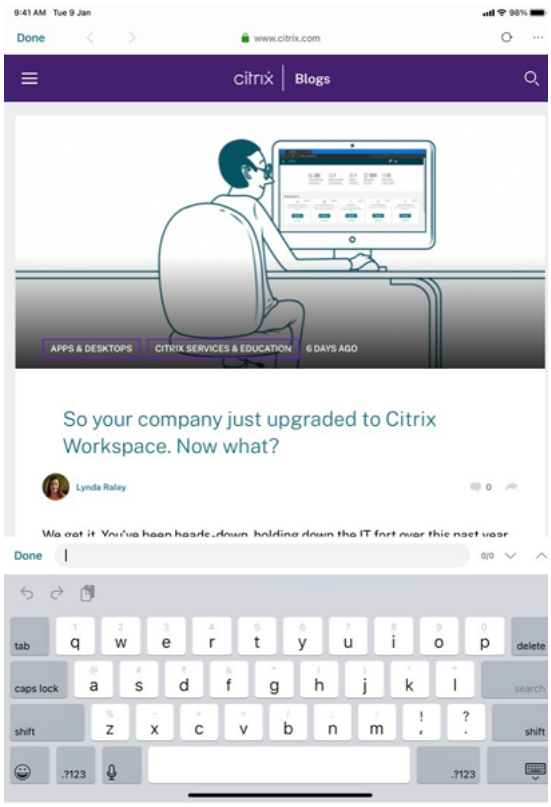
1. Sur votre iPad, appuyez sur le bouton représentant des points de suspension (…) dans le coin supérieur droit, puis sélectionnez **Rechercher dans la page**.



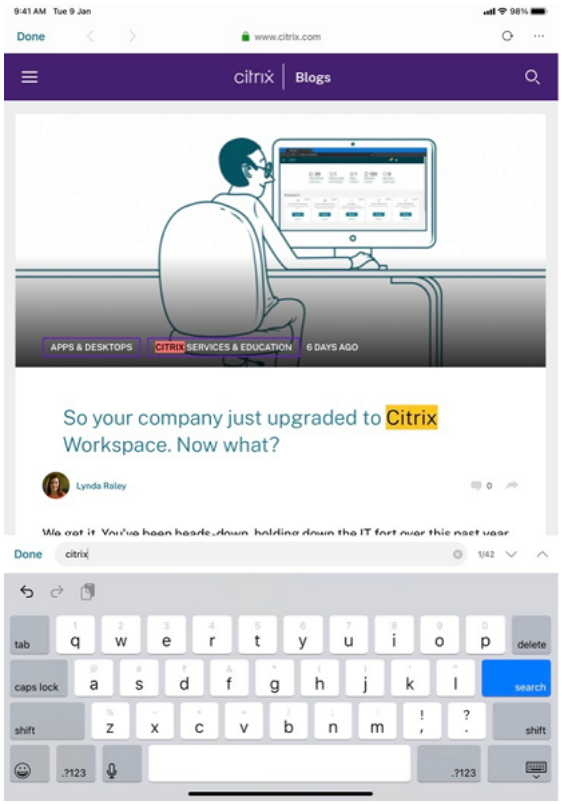
Sur votre iPhone, appuyez sur le bouton représentant des points de suspension (…) dans le coin inférieur droit, puis sélectionnez **Rechercher dans la page**.



Le clavier apparaît à l'écran.



1. Tapez le texte que vous souhaitez rechercher dans la zone de texte (par exemple, tapez le mot « Citrix »). Les résultats de la recherche s'affichent.



Repositionnement de la barre d'outils de session

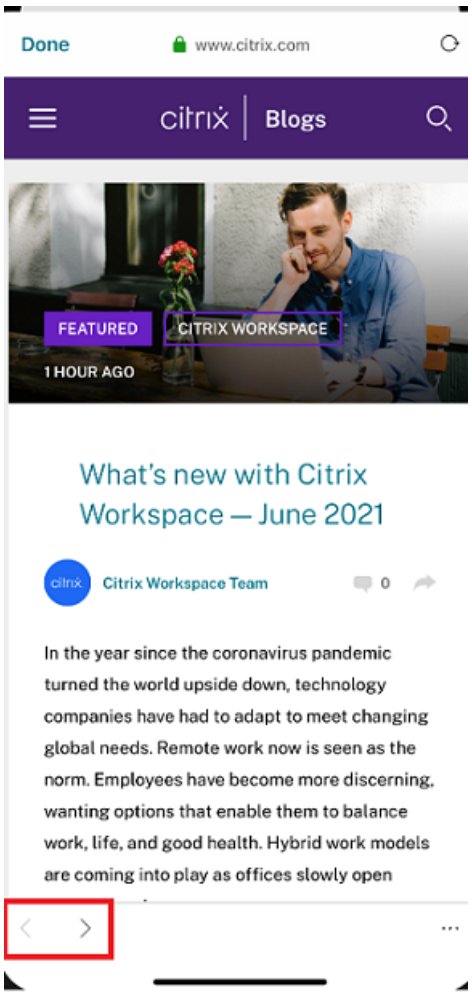
Vous pouvez repositionner la barre d'outils de session en haut ou à droite de l'écran. Lorsque vous éloignez l'encoche de la barre d'outils du bord de la barre d'outils, l'indicateur de déplacement en forme de rectangle et la cible de déplacement apparaissent. Déplacez l'indicateur de déplacement sur la cible de déplacement pour repositionner la barre d'outils.

> **Remarques :**
>
> - La fonctionnalité s'applique uniquement aux utilisateurs d'iPad.
> - La fonction fonctionne avec écran tactile ou souris.
> - La fonction fonctionne avec un iPad ou sur un écran externe.
> - La dernière position de la barre d'outils est conservée lors de la prochaine session ou du prochain lancement de l'application.

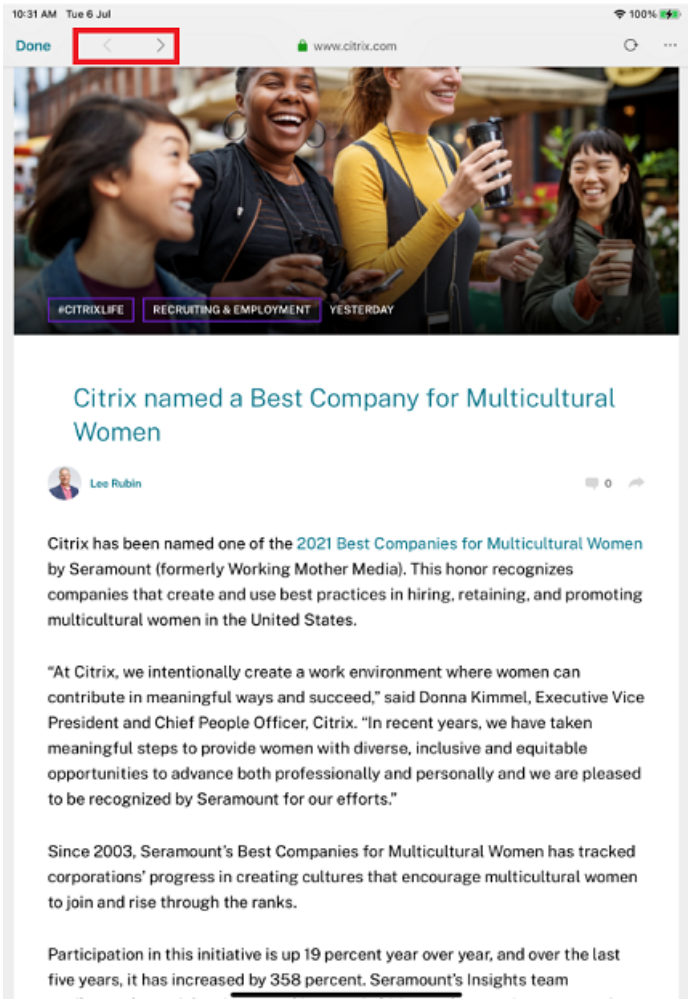
Basculer entre les applications SaaS et les applications Web

Cette amélioration de la convivialité vous permet de naviguer dans les applications Web et SaaS (Software-as-a-Service).

Les boutons de navigation s'affichent en bas à gauche des sessions d'application SaaS et Workspace pour Web sur votre iPhone.



Les boutons de navigation s'affichent en haut à gauche des sessions d'application SaaS et Workspace pour Web sur votre iPad.



Migration d'un compte local vers un compte cloud

Les administrateurs peuvent migrer en toute transparence les utilisateurs d'une URL de magasin StoreFront local vers une URL Workspace. Les administrateurs peuvent effectuer la migration avec un minimum d'interaction de l'utilisateur à l'aide du Global App Configuration Service.

Pour configurer :

1. Accédez à l'URL de l'API des paramètres de Global App Configuration Store et saisissez l'URL du magasin cloud.
   Par exemple, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.
2. Accédez à **API Exploration** > **SettingsController** > **postDiscoveryApiUsingPOST** > cliquez sur **POST**.
3. Cliquez sur **INVOKE API**.

4. Entrez et chargez les détails de la charge utile. Entrez la date d'expiration du magasin Store-Front dans l'horodatage en millisecondes.

   Par exemple,

```
"migrationUrl": [
{


"url": "<cloud store url>"
"StoreFrontValidUntil": "<epoch timestamp in milliseconds>",
 }

]   ,
<!--NeedCopy-->
```

5. Cliquez sur **EXECUTE** pour envoyer le service.

Expérience utilisateur final

En tant qu'utilisateur final, si vous utilisez l'application Citrix Workspace pour la première fois, après une authentification réussie, l'écran de migration **Présentation du nouveau Citrix Workspace** s'affiche (s'il est éligible). Après avoir cliqué sur l'option **Essayez le nouveau Citrix Workspace**, la migration commence. Une fois la migration réussie, vous pouvez accéder au magasin Workspace (magasin cloud).

> **Remarque :**
>
> Vous pouvez ignorer la migration à trois reprises. Au-delà, la migration est forcée sans possibilité de l'ignorer.

Après avoir migré vers le magasin Workspace (cloud), vous pouvez afficher à la fois le magasin StoreFront et le magasin Workspace sous **Paramètres**. Lorsque vous passez d'un magasin cloud au magasin StoreFront local, un écran de commentaires s'affiche pour recueillir vos impressions.

> **Remarque :**
>
> Le magasin StoreFront a une date d'expiration. Après la date d'expiration, le magasin est supprimé.

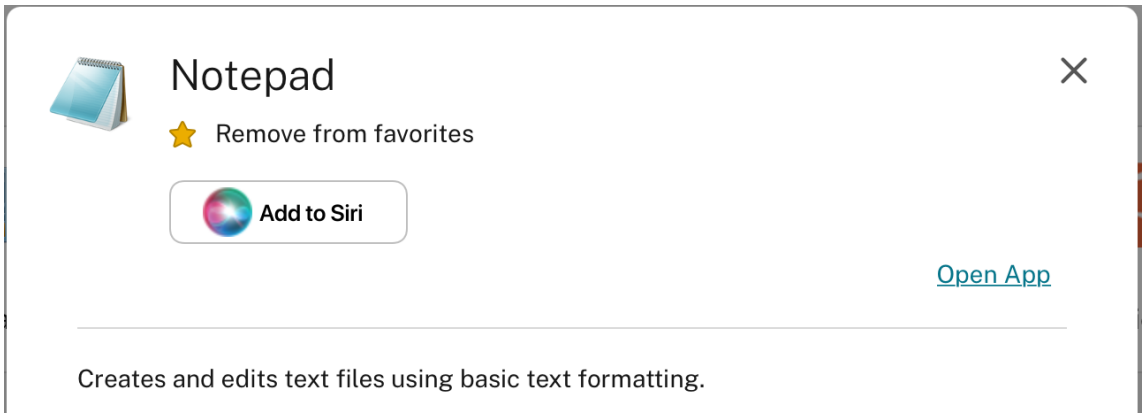
Intégration Siri

Vous pouvez interagir avec Siri pour lancer des ressources telles que des applications et des bureaux sans lancer l'application Citrix Workspace à chaque fois.

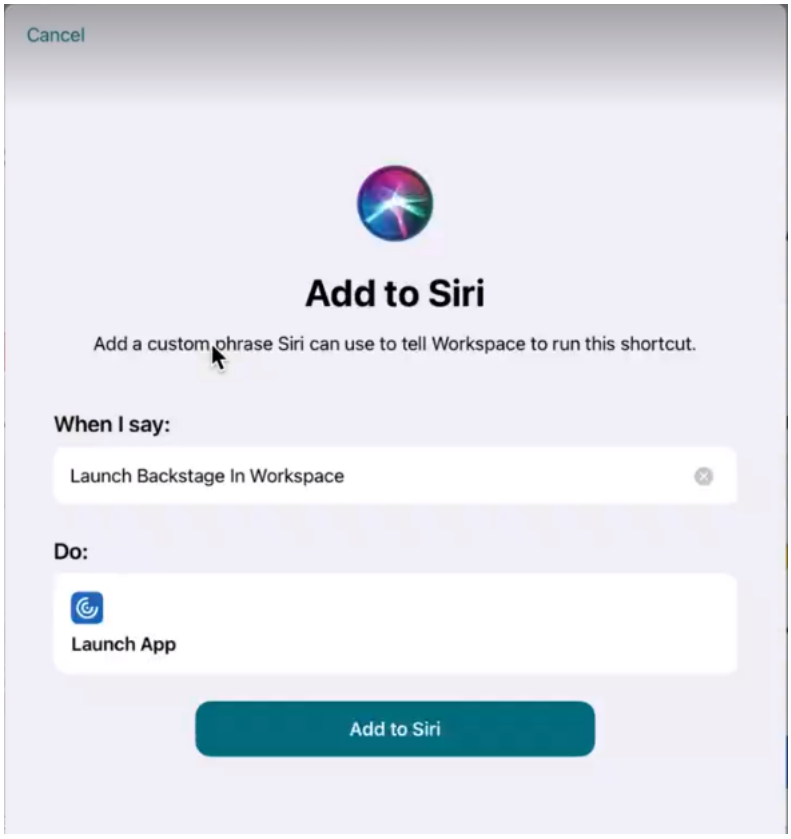
Configuration

1. Lancez l'application Citrix Workspace et appuyez sur **Applications** ou **Bureaux**. Sélectionnez la ressource que vous souhaitez ajouter au raccourci Siri.
2. Appuyez sur points de suspension (…). Une boîte de dialogue apparaît.

   > **Remarque :**
   >
   > Si vous utilisez un iPhone ou un iPad, appuyez sur les **points de suspension** (…) > écran **Détails sur l'application** > **Afficher les détails**. Une boîte de dialogue apparaît. Continuez avec l'étape 3.

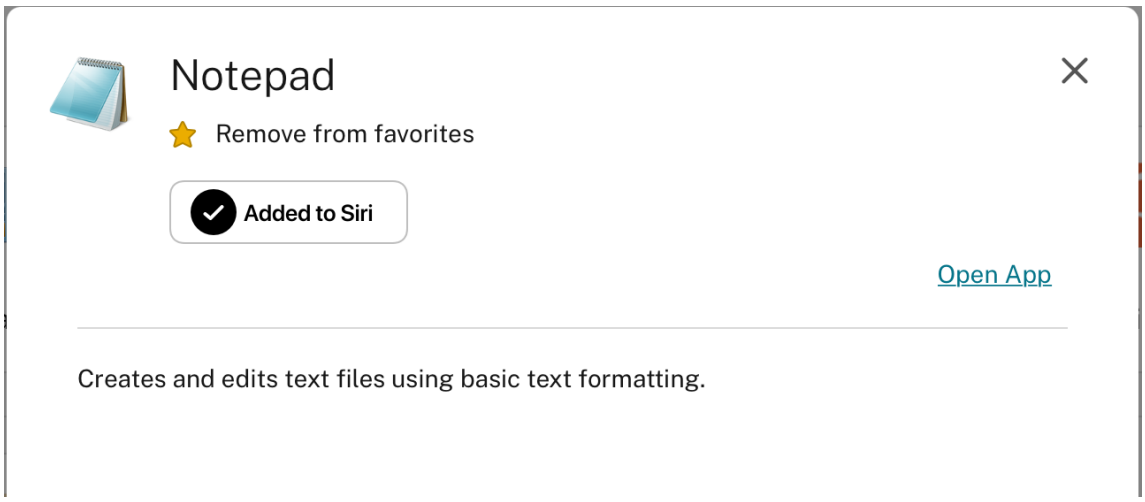
   

3. Appuyez sur **Ajouter à Siri**. La boîte de dialogue **Ajouter à Siri** apparaît.



4. (Facultatif) Modifiez la phrase personnalisée pour appeler Siri. Appuyez sur **Ajouter à Siri**. La ressource est maintenant ajoutée au raccourci Siri. Fermez la boîte de dialogue.

> **Remarque :**
>
> Quelques appareils prennent en charge l'enregistrement de la phrase personnalisée pour appeler Siri.



Paramètres de l'application

Lancez l'application Citrix Workspace et appuyez sur l'icône de votre profil, puis sur **Paramètres de l'application** > **Configurer Siri**. Pour activer cette fonctionnalité, appuyez sur **Ajouter à Siri**.

Vous pouvez désormais utiliser votre voix pour lancer la ressource.

Pour modifier ou supprimer le raccourci

1. Sélectionnez la ressource.
2. Appuyez sur points de suspension (...). Une boîte de dialogue apparaît.
3. Appuyez sur **Ajouté à Siri**. La boîte de dialogue **Modifier le raccourci** apparaît.

Prise en charge d'une fenêtre de session distincte de celle de l'application Citrix Workspace

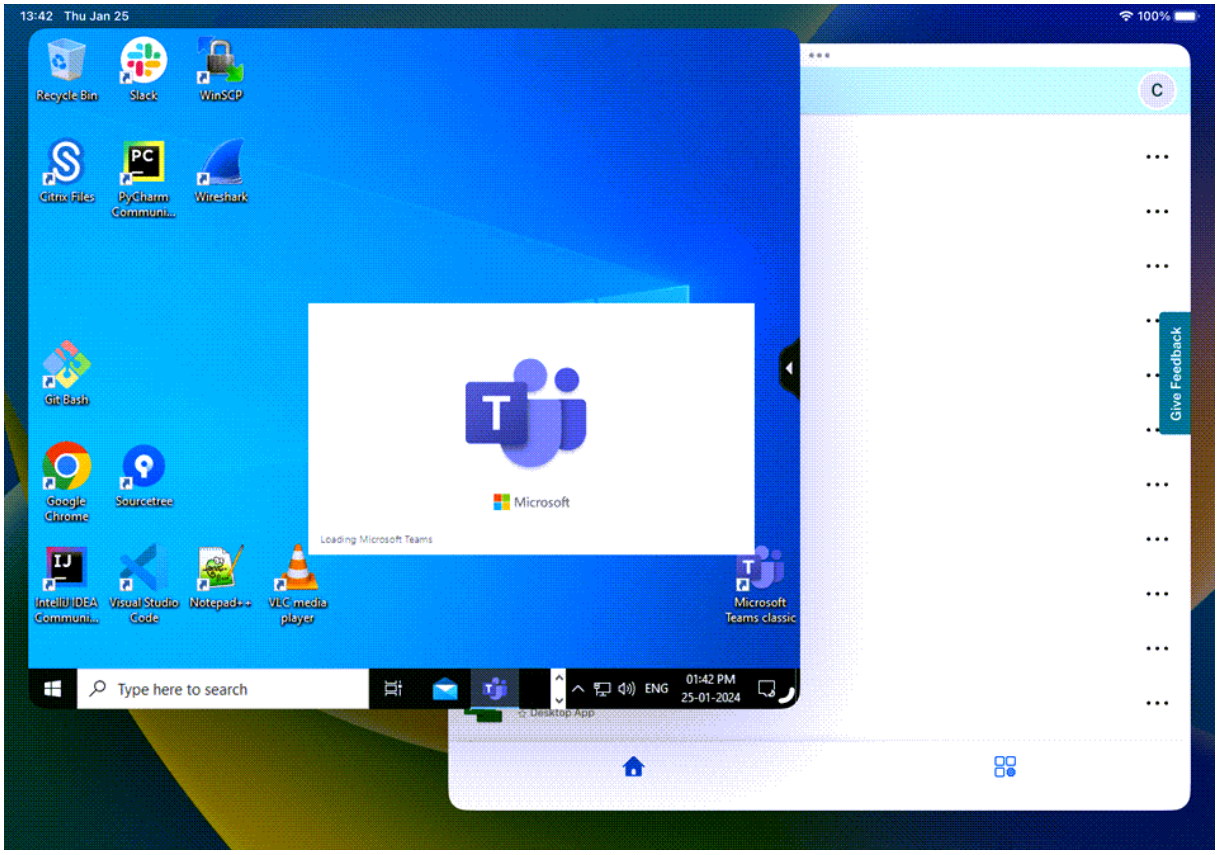
À partir de la version 24.1.0, l'application Citrix Workspace pour iOS introduit une fenêtre de session distincte qui rend le multitâche plus efficace et convivial. Grâce à cette fonctionnalité, vous pouvez profiter d'une expérience similaire à celle d'un ordinateur de bureau. Lorsque la fonctionnalité Fenêtre de session distincte est activée, vous pouvez simplement glisser-déposer les sessions sur les moniteurs externes connectés. Par conséquent, le moniteur principal de l'iPad peut être utilisé pour effectuer plusieurs tâches à la fois avec d'autres applications.

Les améliorations suivantes sont incluses dans cette fonctionnalité :

- Lorsque vous cliquez sur le bouton **Accueil** dans la barre de menu de la session, la fenêtre de l'interface utilisateur Citrix Workspace s'ouvre au lieu de fermer la fenêtre de session HDX. Cette amélioration vous permet d'utiliser simultanément l'interface utilisateur de Citrix Workspace et la session HDX. Si vous démarrez une nouvelle session depuis l'interface utilisateur de Citrix Workspace, la session existante est automatiquement déconnectée.
- Lorsque vous cliquez sur le bouton **Options d'affichage** de la barre de menu de la session, une fenêtre de configuration apparaît en haut de la session HDX. Cette fenêtre vous permet d'ajuster la résolution de la session plutôt que les paramètres de l'interface utilisateur Citrix Workspace.

> **Remarque :**
>
> Cette fonctionnalité n'est prise en charge que sur les appareils qui prennent en charge la fonctionnalité Stage Manager. Les appareils iPhone et iPad ne prennent pas tous en charge cette fonctionnalité. Pour plus d'informations sur la fonctionnalité State Manager, consultez la section Activer ou désactiver Stage Manager sur votre iPad dans la documentation d'assistance Apple.

Pour configurer la fonctionnalité de fenêtre de session distincte, accédez à **Paramètres -> Avancé -> Multitâche** et sélectionnez **Fenêtre de session distincte**.



Affichage Web pour les applications Web et SaaS

December 12, 2023

Page Web

Partage externe de pages Web

Vous pouvez partager les pages Web que vous ouvrez à partir de l'application Citrix Workspace avec d'autres utilisateurs. Vous pouvez :

- copier un lien à partir d'un affichage Web
- ouvrir directement une page Web dans Safari
- envoyer des liens directement à des personnes ou des applications

Pour ce faire, appuyez sur l'icône **...** en haut à droite de l'affichage Web ou appuyez longuement sur n'importe quel lien dans l'affichage Web et appuyez sur l'option dont vous avez besoin.

Affichage Web

Affichage Web amélioré avec contrôles natifs pour les applications SaaS

Vous pouvez disposer d'un affichage Web amélioré avec des contrôles natifs pour les applications SaaS. Cette amélioration vous permet de :

- Afficher l'URL de vos applications.
- Afficher les informations de sécurité de vos applications.
- Partager vos applications.

En outre, vous pouvez maintenant balayer vos applications vers la gauche et la droite pour aller de l'avant et vers l'arrière, respectivement.

Visionneuse Web de l'application mobile Citrix Workspace

La visionneuse Web est une solution de navigation intégrée exécutée dans l'application Citrix Workspace. Elle permet aux utilisateurs d'ouvrir des applications Web ou SaaS à partir de l'application Citrix Workspace de manière sécurisée. La visionneuse Web garantit une interface utilisateur cohérente lors de l'accès à diverses applications Web ou SaaS. Cela améliore la productivité et donne de meilleures performances dans le rendu des applications.

Nos efforts continus pour enrichir l'expérience utilisateur se traduisent par cette nouvelle visionneuse Web qui vous offre une expérience améliorée et native, ainsi que les fonctionnalités suivantes :

- Accès sans VPN aux pages Web internes
- SSO pour le Web et SaaS avec stratégies d'accès adaptatives
- Téléchargement de fichiers avec prévisualisation
- Navigation fluide entre les pages et les sites
- Possibilité de partager des URL
- Rechercher dans la page
- Affichage cohérent lors de l'accès aux liens via le flux d'activités

Les administrateurs peuvent activer Secure Private Access (SPA), y compris des restrictions de téléchargement, de presse-papiers, de navigation, de chargement de fichiers, ainsi que l'utilisation de filigrane dans différentes combinaisons pour chaque URL.

Gestion du mot de passe

March 29, 2024

Enregistrer des mots de passe

À l'aide de la console de gestion de l'Interface Web Citrix, vous pouvez configurer la méthode d'authentification afin d'autoriser les utilisateurs à enregistrer leurs mots de passe. Lorsque vous configurez le compte utilisateur, le mot de passe chiffré est enregistré jusqu'à ce que l'utilisateur se connecte. Tenez compte des considérations suivantes :

- Si vous activez l'enregistrement du mot de passe, l'application Citrix Workspace pour iOS stocke ce dernier et n'invite pas les utilisateurs à le saisir à nouveau pour se connecter à des applications.

  > **Remarque :**
  >
  > Le mot de passe est uniquement stocké si les utilisateurs entrent un mot de passe lors de la création de compte. Si aucun mot de passe n'est entré pour le compte, aucun mot de passe n'est enregistré, quel que soit le paramètre du serveur.

- Si vous désactivez l'enregistrement du mot de passe (paramètre par défaut), l'application Citrix Workspace pour iOS invite les utilisateurs à entrer leur mot de passe chaque fois qu'ils se connectent.

> **Remarque :**
>
> L'enregistrement du mot de passe n'est pas disponible avec les connexions directes à StoreFront.

Pour annuler l'enregistrement des mots de passe

Si vous configurez le serveur de manière à enregistrer les mots de passe, les utilisateurs qui préfèrent demander des mots de passe à l'ouverture de session peuvent ignorer l'enregistrement des mots de passe :

- Lors de la création du compte, laissez le champ de mot de passe vide.
- Lors de la modification d'un compte, supprimez le mot de passe et enregistrez le compte.

Utilisation

L'application Citrix Workspace dispose d'une fonctionnalité qui optimise le processus de connexion en vous permettant d'enregistrer votre mot de passe, ce qui élimine le besoin de vous authentifier chaque fois que vous ouvrez l'application Citrix Workspace.

> **Remarque :**
>
> La fonctionnalité d'**enregistrement de mot de passe** prend actuellement en charge le protocole PNA. Elle ne prend pas en charge le mode *natif* de StoreFront. Toutefois, elle fonctionne lorsque StoreFront active le mode *d'ancienne génération* PNA.

Configurer StoreFront pour enregistrer le mot de passe

Pour configurer StoreFront afin d'activer la fonctionnalité d'**enregistrement de mot de passe** :

1. Si vous configurez un magasin existant, passez à l'étape 3.
2. Pour configurer un nouveau déploiement StoreFront, suivez les recommandations détaillées dans Installer, configurer, mettre à niveau et désinstaller.
3. Ouvrez la console de gestion Citrix StoreFront. Assurez-vous que l'URL de base utilise HTTPS et qu'elle est identique au nom commun spécifié lors de la génération de votre certificat SSL.
4. Sélectionnez le magasin à configurer.
5. Cliquez sur **Configurer la prise en charge de XenApp Services**.
6. Activez la **prise en charge de XenApp Services**, sélectionnez le **magasin par défaut**(facultatif) et cliquez sur **OK**.
7. Accédez au fichier de configuration de modèle sur c:\inetpub\wwwroot\Citrix\<store name>\Views\PnaConfig\.
8. Effectuez une copie de sauvegarde de Config.aspx.
9. Ouvrez le fichier d'origine Config.aspx.
10. Modifiez la ligne <EnableSavePassword>**false**</EnableSavePassword> et changez la valeur **false** sur **true**.
11. Enregistrez le fichier Config.aspx.
12. Sur le serveur StoreFront, exécutez PowerShell avec des droits d'administration.
13. Dans la console PowerShell :

    a. `cd "c:\\Program Files\\Citrix\\Receiver StoreFront\\Scripts"`

    b. Tapez "Set-ExecutionPolicy RemoteSigned"

    c. Tapez ".\ImportModules.ps1"

    d. Tapez "Set-DSServiceMonitorFeature –ServiceUrl"`https://localhost:443/StoreFrontMonitor`

14. Si vous disposez d'un groupe StoreFront, exécutez les mêmes commandes sur tous les membres du groupe.

Configurer Citrix Gateway pour enregistrer les mots de passe

> **Remarque :**
>
> Cette configuration utilise des serveurs d'équilibrage de charge Citrix Gateway.

Pour configurer Citrix Gateway afin de prendre en charge la fonctionnalité d'enregistrement de mot de passe :

1. Connectez-vous à la console de gestion Citrix Gateway.
2. Suivez les recommandations de Citrix pour créer un certificat pour vos serveurs d'équilibrage de charge.
3. Sur l'onglet de configuration, accédez à **Traffic Management** > **Load Balancing** > **Servers** et cliquez sur **Add**.
4. Entrez le nom et l'adresse IP du serveur StoreFront.
5. Cliquez sur **Créer**. Si vous disposez d'un groupe StoreFront, répétez l'étape 5 pour tous les serveurs du groupe.
6. Sur l'onglet de configuration, accédez à **Traffic Management** -> **Load Balancing** -> **Monitor** et cliquez sur **Add**.
7. Entrez un nom pour le moniteur. Sélectionnez le type **StoreFront**. En bas de la page, sélectionnez **Secure** (requis car le serveur StoreFront utilise HTTPS).
8. Cliquez sur l'onglet **Special Parameters**. Entrez le nom du StoreFront configuré précédemment, sélectionnez **Check Backed Services** et cliquez sur **Create**.
9. Sur l'onglet **Configuration**, accédez à **Traffic Management** -> **Load Balancing** -> **Service Groups** et cliquez sur **Add**.
10. Entrez un nom pour votre groupe de services et définissez le protocole sur **SSL** et cliquez sur **OK**.
11. Sur le côté droit de l'écran, sous Advanced Settings, sélectionnez **Settings**.
12. Activez l'option Client IP et entrez ce qui suit pour la valeur Header : **X-Forwarded-For** et cliquez sur **OK**.
13. Sur le côté droit de l'écran, sous Advanced Settings, sélectionnez **Monitors**. Cliquez sur la flèche pour ajouter de nouveaux moniteurs.
14. Cliquez sur le bouton **Add**, puis sélectionnez le menu déroulant **Select Monitor**. Une liste des moniteurs (configurés sur Citrix Gateway) s'affiche.
15. Cliquez sur le bouton radio en regard du moniteur que vous avez créé précédemment et cliquez sur **Select**, puis sur **Bind**.

16. Sur le côté droit de l'écran (sous Advanced Settings), sélectionnez **Members**. Cliquez sur la flèche pour ajouter de nouveaux membres au groupe de services.
17. Cliquez sur le bouton **Add** et sélectionnez le menu déroulant **Select Member**.
18. Sélectionnez le bouton radio **Server Based**. Une liste des membres du serveur (configurés sur Citrix Gateway) s'affiche. Cliquez sur le bouton radio en regard du serveur StoreFront que vous avez créé précédemment.
19. Entrez 443 pour le numéro de port et spécifiez un numéro Hash ID unique, puis cliquez sur **Create** et **Done**. Si tout a été configuré correctement, **Effective State** doit afficher un voyant vert, ce qui indique que la surveillance fonctionne correctement.
20. Accédez à **Traffic Management -> Load Balancing -> Virtual Servers** et cliquez sur **Add**. Entrez un nom pour le serveur et sélectionnez **SSL** en tant que protocole.
21. Entrez l'adresse IP du serveur d'équilibrage de charge StoreFront et cliquez sur **OK**.
22. Sélectionnez la liaison **Load Balancing Virtual Server Service Group**, cliquez sur la flèche et ajoutez le groupe de services créé précédemment. Cliquez sur **OK** deux fois.
23. Allouez le certificat SSL créé pour le serveur virtuel d'équilibrage de charge. Sélectionnez **No Server Certificate**.
24. Sélectionnez le certificat du serveur d'équilibrage de charge dans la liste et cliquez sur **Bind**.
25. Ajoutez le certificat de domaine au serveur d'équilibrage de charge. Cliquez sur **No CA certificate**.
26. Sélectionnez le certificat de domaine et cliquez sur **Bind**.
27. Sur le côté droit de l'écran, sélectionnez **Persistence**.
28. Changez l'option Persistence sur **SOURCEIP** et définissez le délai d'expiration sur **20**. Cliquez sur **Save**, puis sur **Done**.
29. Sur votre serveur DNS de domaine, ajoutez le serveur d'équilibrage de charge (s'il n'a pas déjà été créé).
30. Lancez l'application Citrix Workspace pour iOS sur votre appareil iOS et entrez l'URL complète de XenApp.

Authentification

July 1, 2024

Authentification du certificat client

> **Important :**
>
> - Lorsque StoreFront est utilisé, l'application Citrix Workspace prend en charge :
>   - Citrix Access Gateway Enterprise Edition version 9.3
>   - NetScaler Gateway versions 10.x à 11.0
>   - Citrix Gateway version 11.1 et versions ultérieures
> - L'application Citrix Workspace pour iOS prend en charge l'authentification du certificat client.
> - Seules les éditions 9.x et 10.x (et les versions ultérieures) d'Access Gateway Enterprise prennent en charge l'authentification du certificat client.
> - Les types d'authentification double doivent être CERT et LDAP.
> - L'application Citrix Workspace prend également en charge l'authentification facultative du certificat client.
> - Seuls les certificats P12 sont pris en charge.

Les utilisateurs qui se connectent sur un serveur virtuel Citrix Gateway peuvent également être authentifiés en fonction des attributs du certificat client qui est présenté au serveur virtuel. L'authentification du certificat client peut également être utilisée avec un autre type d'authentification, à savoir LDAP, afin de fournir une authentification double.

Les administrateurs peuvent authentifier les utilisateurs en fonction des attributs de certificat côté client comme suit :

- L'authentification du client est activée sur le serveur virtuel.
- Le serveur virtuel demande un certificat client.
- Vous devez lier un certificat racine au serveur virtuel sur Citrix Gateway.

Lorsque les utilisateurs se connectent au serveur virtuel Citrix Gateway, après l'authentification, ils peuvent extraire le nom d'utilisateur et les informations sur le domaine à partir du champ **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** du certificat. Ils sont au format `username@domain`.

L'authentification est terminée lorsque l'utilisateur extrait le nom d'utilisateur et le domaine et fournit les informations requises (telles que le mot de passe). Si l'utilisateur ne fournit pas un certificat et des informations d'identification valides, ou si l'extraction du nom d'utilisateur/domaine échoue, l'authentification échoue.

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.

Pour configurer la batterie XenApp

Créez une batterie XenApp pour appareils mobiles dans la console Citrix Virtual Apps ou la console Interface Web. La console dépend de la version de Citrix Virtual Apps que vous avez installée.

L'application Citrix Workspace utilise une batterie XenApp pour obtenir des informations sur les applications auxquelles un utilisateur est autorisé à accéder. Les mêmes informations sont partagées avec les applications qui s'exécutent sur l'appareil. Cette méthode est similaire à la manière dont vous utilisez l'Interface Web pour les connexions Citrix Virtual Apps SSL traditionnelles pour lesquelles vous pouvez configurer l'instance Citrix Gateway.

Configurez la batterie XenApp pour l'application Citrix Workspace pour appareils mobiles afin de prendre en charge les connexions en provenance de Citrix Gateway comme suit :

1. Dans la batterie XenApp, sélectionnez **Gérer l'accès client sécurisé** > **Modifier les paramètres d'accès au client sécurisé**.
2. Dans Méthode d'accès, choisissez Passerelle directe.
3. Entrez le nom de domaine complet de l'appliance Citrix Gateway.
4. Entrez les informations de Secure Ticket Authority (STA).

Pour configurer l'appliance Citrix Gateway

Pour l'authentification du certificat client, configurez Citrix Gateway avec l'authentification à deux facteurs à l'aide des stratégies d'authentification Cert et LDAP. Pour configurer l'appliance Citrix Gateway :

1. Créez une stratégie de session sur Citrix Gateway de manière à autoriser les connexions Citrix Virtual Apps entrantes provenant de l'application Citrix Workspace. Spécifiez l'emplacement de la batterie XenApp que vous venez de créer.

    - Créez une stratégie de session pour identifier l'application Citrix Workspace comme étant à l'origine de la connexion. Lorsque vous créez la stratégie de session, configurez l'expression suivante et choisissez Match All Expressions comme opérateur pour l'expression :

      ```
      REQ.HTTP.HEADER User-Agent CONTAINS CitrixWorkspace
      ```

    - Dans la configuration de profil associé pour la stratégie de session, sur l'onglet **Security**, définissez **Default Authorization** sur **Allow**.

      Sur l'onglet **Published Applications**, s'il ne s'agit pas d'un paramètre global (vous avez coché la case Override Global), assurez-vous que le champ **ICA Proxy** est défini sur la valeur **ON**.

      Dans le champ **Address** de l'Interface Web, entrez l'URL, y compris le fichier config.xml de la batterie XenApp utilisée par les utilisateurs de l'appareil, par exemple :

  - /XenAppServerName/Citrix/PNAgent/config.xml
    ou
  - /XenAppServerName/CustomPath/config.xml.
- Associez la stratégie de session à un serveur virtuel.
- Créez des stratégies d'authentification pour Cert et LDAP.
- Associez les stratégies d'authentification au serveur virtuel.
- Configurez le serveur virtuel pour demander des certificats clients lors de la négociation TLS. Pour ce faire, accédez à **Certificate**, ouvrez **SSL Parameters** > **Client Authentication** et définissez **Client Certificate** sur **Mandatory**.

> **Important :**
>
> Si le certificat de serveur utilisé sur Citrix Gateway fait partie d'une chaîne de certificats, par exemple, s'il s'agit d'un certificat intermédiaire, installez les certificats sur Citrix Gateway. Pour de plus amples informations sur l'installation de certificats, consultez la documentation de Citrix Gateway.

Pour configurer l'appareil mobile

Si l'authentification du certificat client est activée sur Citrix Gateway, les utilisateurs sont authentifiés en fonction de certains attributs du certificat client. Après l'authentification, vous pouvez extraire le nom d'utilisateur et le domaine du certificat. Vous pouvez appliquer des stratégies spécifiques à chaque utilisateur.

1. À partir de l'application Citrix Workspace, ouvrez **Compte**, et dans le champ Serveur, entrez le nom de domaine complet de votre serveur Citrix Gateway. For example, GatewayClientCertificateServer.organization.com. L'application Citrix Workspace détecte automatiquement que le certificat client est requis.
2. Deux choix se présentent à l'utilisateur : il peut soit installer un nouveau certificat, soit en sélectionner un dans la liste des certificats déjà installés. Pour l'authentification par certificat client iOS, téléchargez et installez le certificat uniquement à partir de l'application Citrix Workspace.
3. Une fois que vous avez sélectionné un certificat valide, les champs de nom d'utilisateur et de domaine de l'écran de connexion sont préremplis à l'aide du nom d'utilisateur du certificat. L'utilisateur peut saisir d'autres informations, y compris le mot de passe.
4. Si l'authentification du certificat client est définie sur Facultative, les utilisateurs peuvent ignorer la sélection du certificat en appuyant sur Précédent dans la page des certificats. Dans ce cas, l'application Citrix Workspace établit la connexion et affiche l'écran d'ouverture de session.
5. Une fois la connexion initiale effectuée, les utilisateurs peuvent lancer des applications sans avoir à fournir de nouveau le certificat. L'application Citrix Workspace stocke le certificat du compte et l'utilise automatiquement lors des ouvertures de session suivantes.

Configurer une stratégie de réécriture pour le processus d'authentification

Les administrateurs peuvent faire passer le navigateur utilisé pour le processus d'authentification du navigateur intégré au navigateur système. Cela n'est possible que lorsqu'une stratégie d'authentification avancée est configurée sur le déploiement local de Citrix Gateway et StoreFront. Pour configurer une stratégie d'authentification avancée, configurez la stratégie de réécriture NetScaler à l'aide de la ligne de commande NetScaler :

1. `enable ns feature REWRITE`
2. `add rewrite action insert_auth_browser_type_hdr_act insert_http_header X-Auth-WebBrowser "\"System\""`
3. `add rewrite policy insert_auth_browser_type_hdr_pol "HTTP.REQ.URL.EQ(\"/cgi/authenticate\")"insert_auth_browser_type_hdr_act`
4. `bind vpn vserver <VPN-vserver-Name> -policy insert_auth_browser_type_hdr_p -priority 10 -gotoPriorityExpression END -type AAA_RESPONSE`

Le passage au navigateur du système offre quelques-unes des fonctionnalités supplémentaires suivantes :

- Meilleure expérience grâce à l'authentification basée sur des certificats.
- Possibilité d'utiliser un certificat utilisateur existant depuis le keystore de l'appareil pendant le processus d'authentification.
- Prise en charge d'autres authentificateurs tiers tels que SITHS eID.

Le navigateur intégré est utilisé comme navigateur par défaut pour l'authentification si l'administrateur n'a pas configuré la stratégie de réécriture ci-dessus.

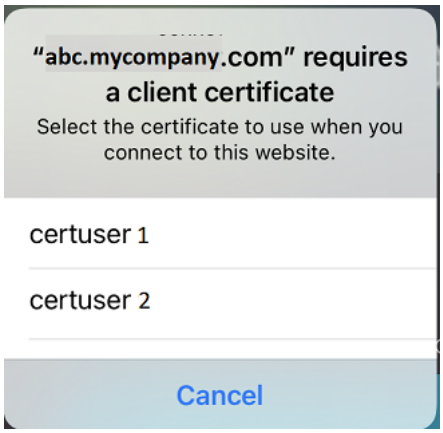
Ce tableau répertorie les navigateurs utilisés pour l'authentification en fonction de la configuration sur NetScaler Gateway et Global App Config Service :

NetScaler Gateway	Global App Configuration Service	Navigateur utilisé pour l'authentification
Système	Système	Système
Système	Embedded	Système
Embedded	Système	Système
Embedded	Embedded	Embedded
Aucune configuration	Système	Système
Aucune configuration	Embedded	Embedded

Prise en charge de l'authentification basée sur des certificats pour les magasins locaux

Les utilisateurs peuvent désormais gérer l'authentification basée sur les certificats où les certificats sont enregistrés dans le trousseau de l'appareil. Lors de la connexion, l'application Citrix Workspace détecte la liste des certificats sur votre appareil. Vous pouvez alors choisir un certificat pour l'authentification.

> **Important :**
>
> Une fois que vous avez choisi le certificat, la sélection est conservée pour le prochain lancement de l'application Citrix Workspace. Pour choisir un autre certificat, vous pouvez réinitialiser Safari dans les paramètres de l'appareil iOS ou réinstaller l'application Citrix Workspace.



> **Remarque :**
>
> Cette fonctionnalité prend en charge les déploiements sur site.

Pour configurer :

1. Accédez à l'URL de l'API des paramètres de Global App Configuration Store et saisissez l'URL du magasin cloud.
   Par exemple, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.
2. Accédez à **API Exploration** > **SettingsController** > **postDiscoveryApiUsingPOST** > cliquez sur **POST**.
3. Cliquez sur **INVOKE API**.
4. Entrez et chargez les détails de la charge utile. Sélectionnez l'une des valeurs suivantes :
   - « Embedded » : vous pouvez utiliser WKWebView. Cette option est définie par défaut.
   - « system » : vous pouvez utiliser le contrôleur d'affichage Safari.

   Par exemple,


```
"category": "Authentication",
"userOverride": false,
"settings": [
{
  "name": "Web Browser to use for Authentication", "value": "*
     Embedded*/*System*"  }
 ,
<!--NeedCopy-->
```

Sur les appareils iOS ou iPad, les administrateurs peuvent changer le navigateur utilisé pour le processus d'authentification. Vous pouvez passer du navigateur intégré au navigateur système lorsqu'une stratégie d'authentification avancée est configurée sur le déploiement local de Citrix Gateway et StoreFront. Pour plus d'informations, consultez Configurer une stratégie de réécriture pour le processus d'authentification.

5. Cliquez sur **EXECUTE** pour envoyer le service.

Cartes à puce

L'application Citrix Workspace prend en charge les cartes à puce SITHS pour les connexions dans les sessions uniquement.

Si vous utilisez des périphériques Citrix Gateway certifiés FIPS, configurez vos systèmes afin de refuser les renégociations SSL. Pour de plus amples informations, consultez l'article CTX123680 du centre de connaissances.

Les configurations et produits suivants sont pris en charge :

- Lecteurs pris en charge :
  - Precise Biometrics Tactivo pour iPad Mini Firmware version 3.8.0
  - Precise Biometrics Tactivo pour iPad (4ème génération) et Tactivo pour iPad (3ème génération) et iPad 2 Firmware version 3.8.0
  - Lecteurs de carte à puce BaiMobile® 301MP et 301MP-L
  - Lecteur USB Thursby PKard
  - Lecteur USB Feitian iR301
  - Lecteurs compatibles CCID de type C
  - Lecteur utilitaire de carte à puce Twocanoes
- Middleware de carte à puce VDA pris en charge
  - ActiveIdentity
- Cartes à puce prises en charge :
  - Cartes PIV

  - Cartes CAC

- Configurations prises en charge :
  - Authentification par carte à puce à Citrix Gateway avec StoreFront 2.x et XenDesktop 7.x ou versions supérieures ou XenApp 6.5 ou versions supérieures.

Pour configurer l'application Citrix Workspace pour accéder aux applications

1. Si vous souhaitez configurer l'application Citrix Workspace automatiquement pour accéder aux applications lors de la création d'un compte, dans le champ Adresse, entrez l'URL correspondante de votre magasin. Par exemple :
   - StoreFront.organization.com
   - netscalervserver.organization.com
2. Sélectionnez l'option **Utiliser carte à puce** si vous utilisez une carte à puce pour l'authentification.

> **Remarque :**
>
> Les ouvertures de session sur le magasin sont valides pour environ une heure. Une fois cette période écoulée, les utilisateurs doivent de nouveau ouvrir une session pour actualiser ou lancer d'autres applications.

Prise en charge du lecteur utilitaire de carte à puce Twocanoes

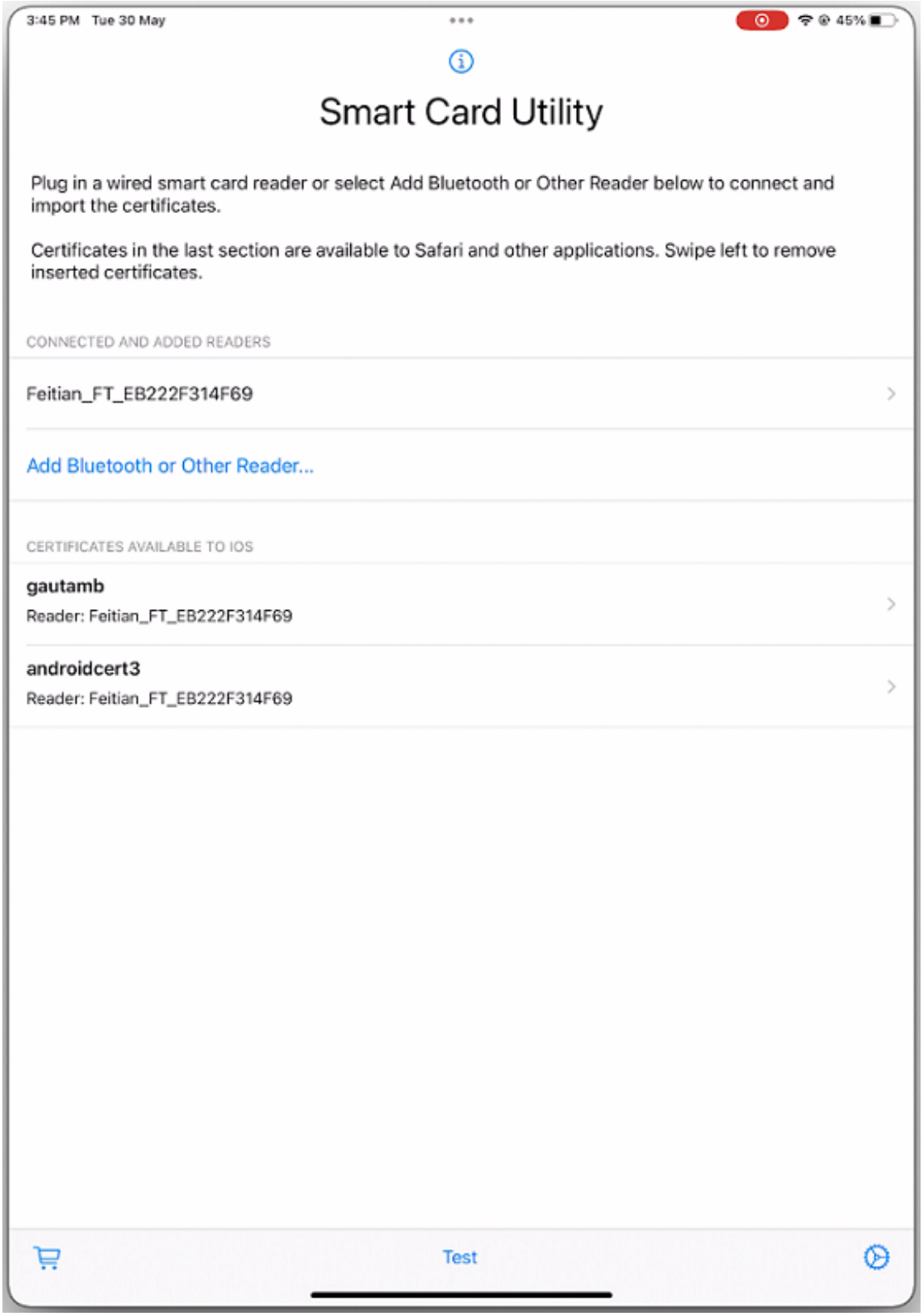
À partir de la version 24.3.5, l'application Citrix Workspace pour iOS prend en charge les lecteurs utilitaires de cartes à puce Twocanoes. Pour plus d'informations sur les lecteurs de cartes à puce pris en charge, consultez la section Cartes à puce.

> **Remarque :**
>
> Le lecteur USB-C de l'utilitaire de carte à puce Twocanoes est pris en charge à la fois pour la connexion à l'application Citrix Workspace et pour la connexion à une session virtuelle. Cependant, le lecteur Bluetooth de l'utilitaire de cartes à puce Twocanoes n'est pris en charge que pour la connexion à l'application Citrix Workspace et non pour la connexion à une session virtuelle.

Pour configurer le lecteur Bluetooth de l'utilitaire de cartes à puce Twocanoes, procédez comme suit :

1. Téléchargez et installez l'application Smart Card Utility depuis l'App Store. Pour plus d'informations, consultez Smart Card Utility Bluetooth Reader Quick Start dans la base de connaissances Twocanoes.

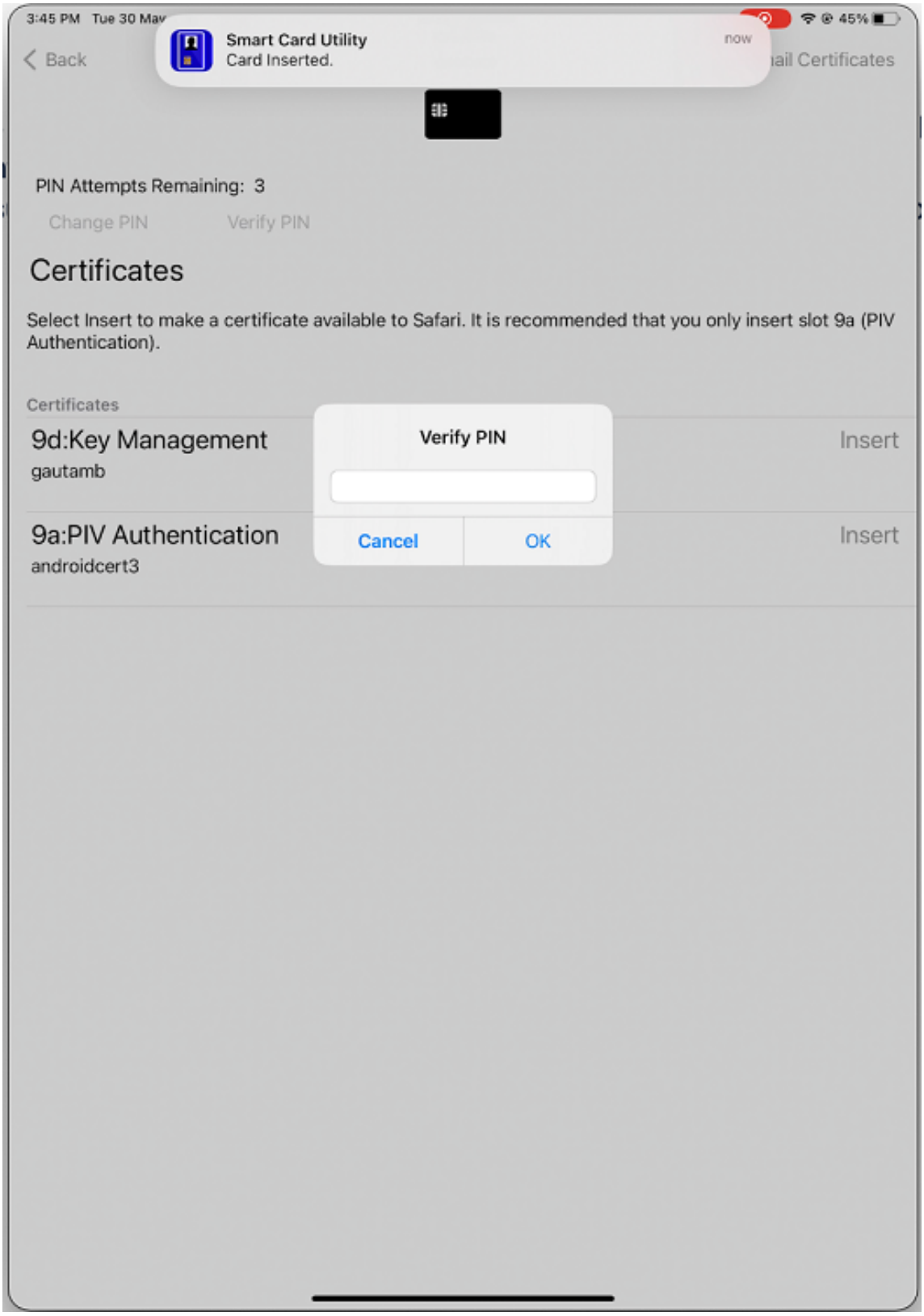
2. Assurez-vous que le Bluetooth de votre appareil est activé et que la carte à puce est insérée dans le lecteur.
3. Ouvrez l'application Smart Card Utility.



4. Si vous utilisez le lecteur Bluetooth, touchez **Add Bluetooth or Other Reader…** et sélectionnez

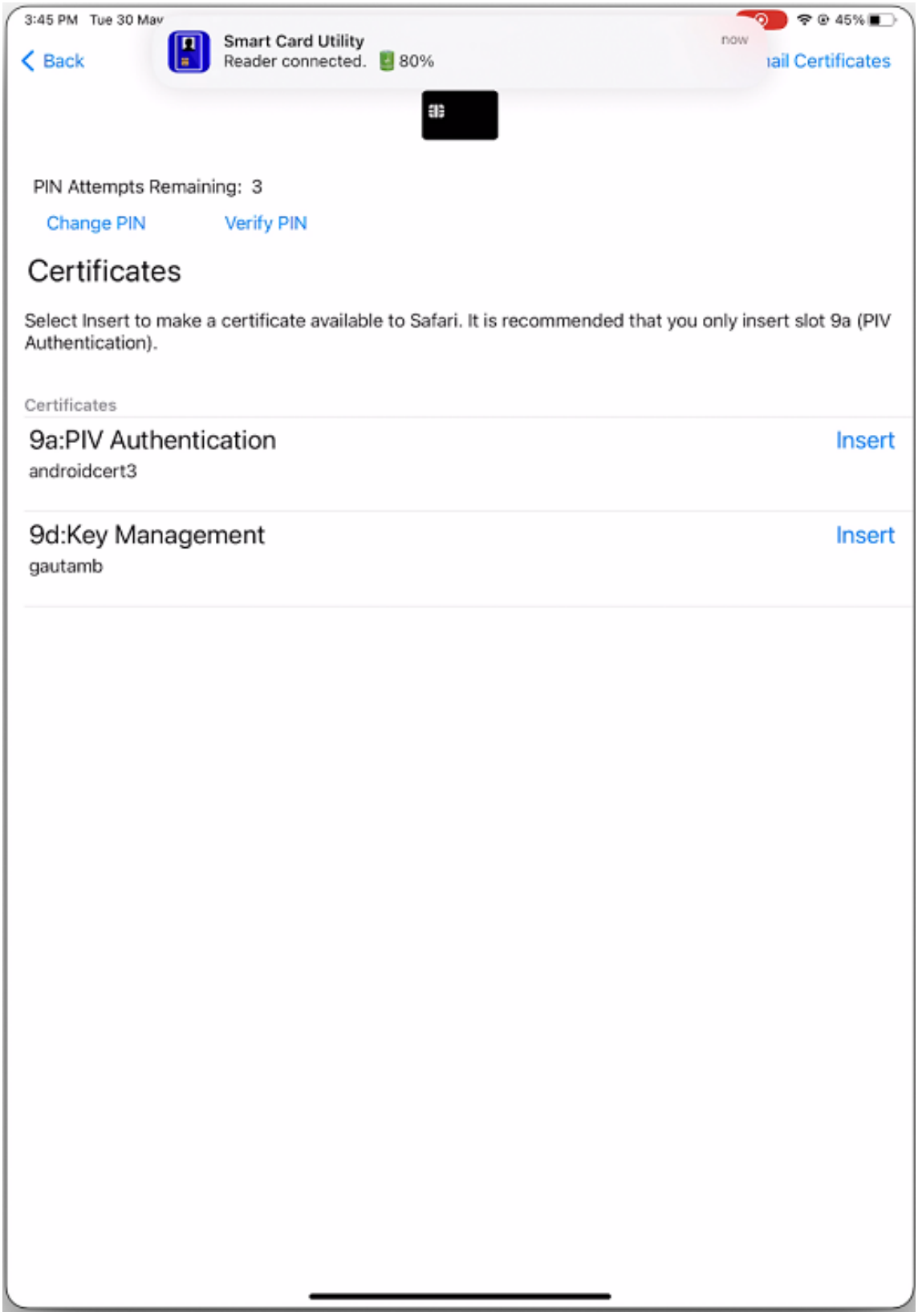
le lecteur à connecter.

> **Remarque :**
>
> Si le lecteur est activé avec le couplage des codes PIN, vous devez saisir le **code PIN** lorsque vous y êtes invité. Le **code PIN** est disponible à l'arrière du lecteur.



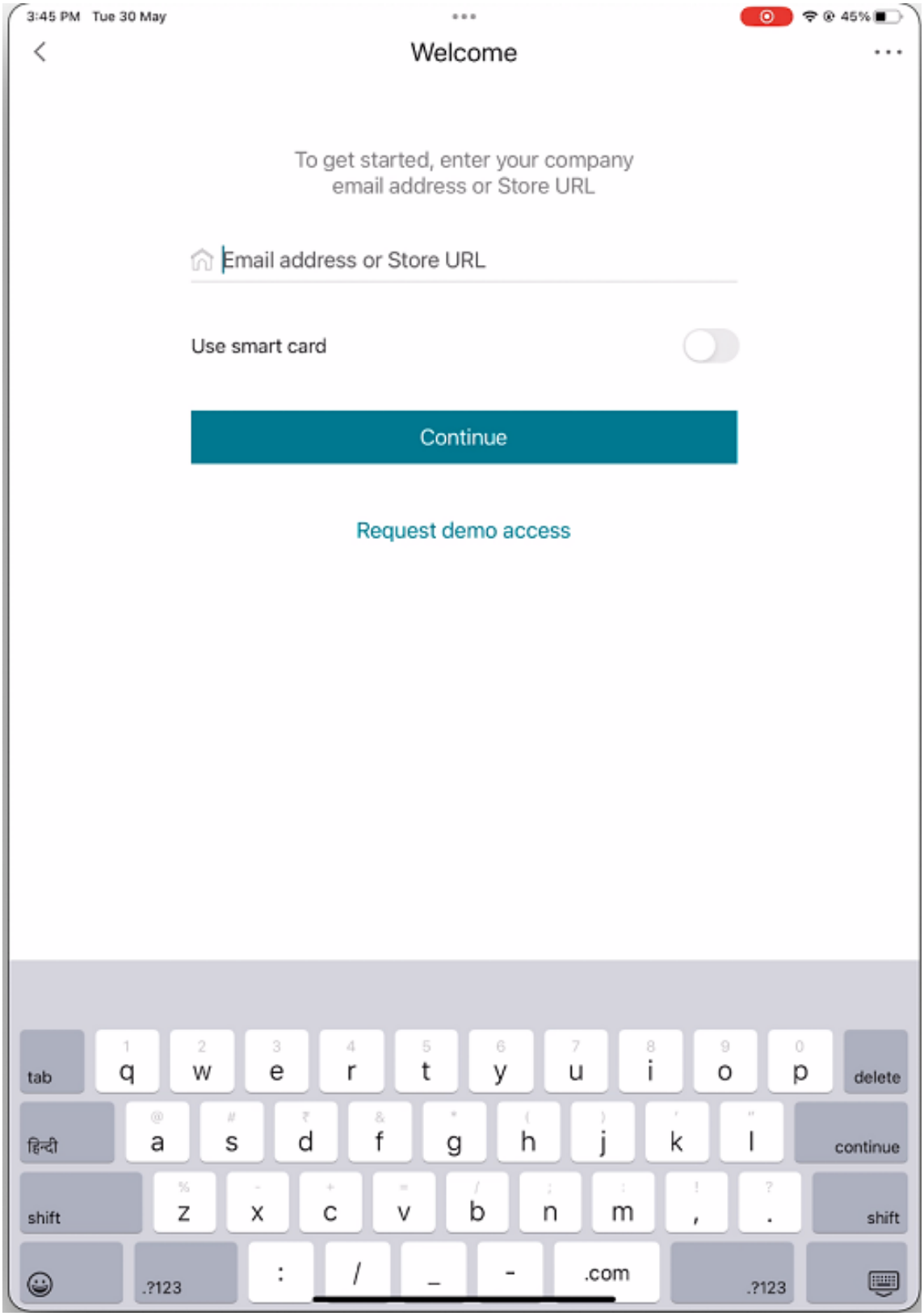
5. Touchez **Insérer** sur le certificat requis pour le copier dans l'interface du trousseau.

> **Remarque :**
>
> L'application Smart Card Utility a implémenté une extension Cryptokit fournie par Apple pour écrire des certificats sur l'interface du trousseau sous forme de jetons. Pour plus d'informations, consultez la page Configure Smart Card Authentication dans la documentation Apple destinée aux développeurs.

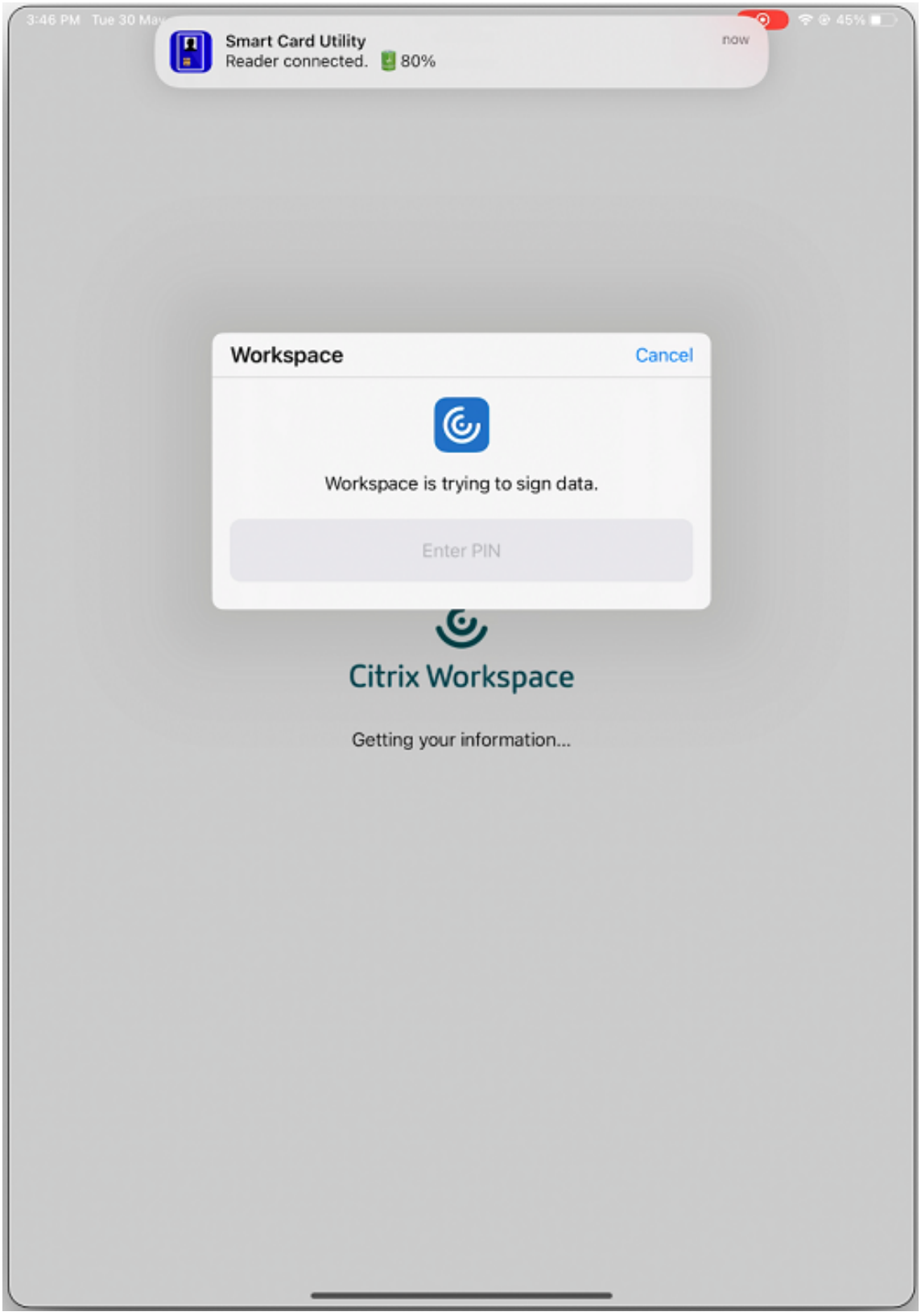


6. Assurez-vous que le lecteur reste connecté à l'appareil.

7. Ouvrez l'application Citrix Workspace et entrez l'URL du magasin configurée avec l'authentification par carte à puce.

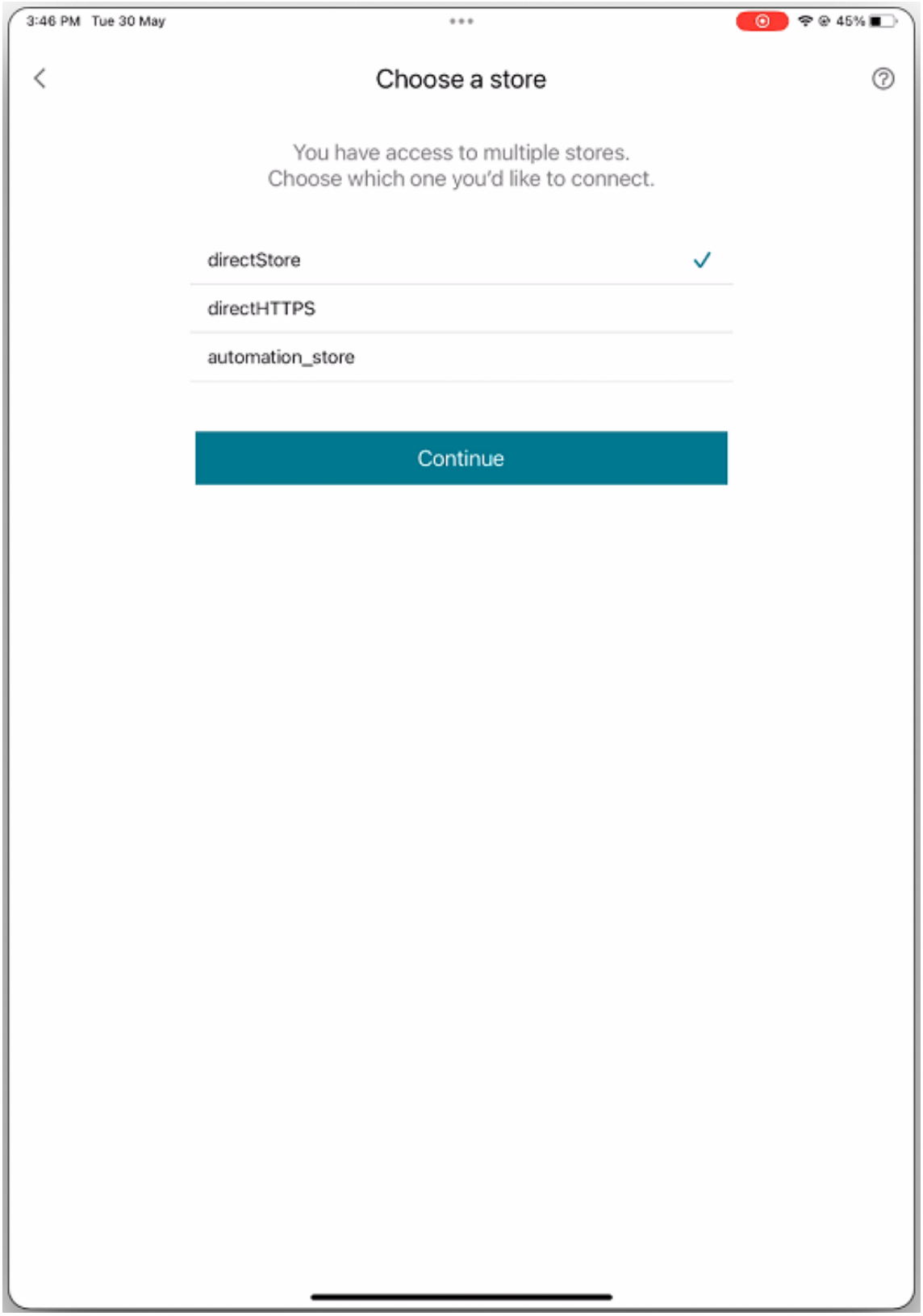


8. Sur l'écran Certificats, sélectionnez le certificat requis et saisissez le code PIN de la carte à puce fourni par votre administrateur informatique pour vous connecter.



9. Si vous avez accès à plusieurs magasins, sélectionnez le magasin requis, puis touchez **Contin-**

uer.



10. Une fois l'authentification réussie, vous êtes connecté à l'application Citrix Workspace.

Prise en charge de la clé YubiKey pour l'authentification par carte à puce

Vous pouvez désormais effectuer une authentification par carte à puce à l'aide d'une clé YubiKey. Cette fonctionnalité fournit une expérience d'authentification sur un seul appareil pour l'application Citrix Workspace, ainsi que pour les sessions virtuelles et les applications publiées dans la session VDA. Il n'est plus nécessaire de connecter des lecteurs de carte à puce ou d'autres authentificateurs externes. Cela simplifie l'expérience utilisateur, car la clé YubiKey prend en charge une grande variété de protocoles, tels que OTP, FIDO et bien d'autres encore.

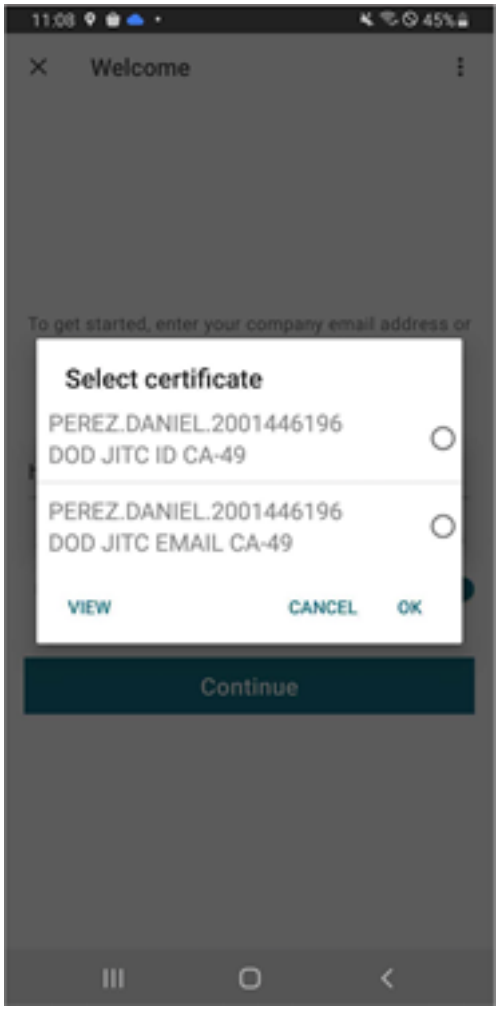
Pour se connecter à l'application Citrix Workspace, les utilisateurs insèrent la clé YubiKey dans leur iPhone ou iPad, activent le bouton de la carte à puce et indiquent l'URL de leur magasin.

> **Remarque :**
>
> Cette fonctionnalité ne prend en charge que la connexion directe à l'application Citrix Workspace sur les déploiements StoreFront, et non via Citrix Gateway. La prise en charge de YubiKey pour l'authentification par carte à puce via Citrix Gateway sera disponible dans la prochaine version. L'application Citrix Workspace pour iOS ne prend en charge que la série YubiKey 5. Pour plus d'informations sur les clés YubiKey, consultez la page série YubiKey 5.

Prise en charge de plusieurs certificats dans l'authentification par carte à puce

Auparavant, l'application Citrix Workspace pour iOS affichait le certificat disponible sur le premier emplacement de la carte à puce connectée.

À partir de la version 24.1.0, l'application Citrix Workspace pour iOS affiche tous les certificats disponibles sur la carte à puce. Cette fonctionnalité vous permet de sélectionner le certificat requis lors de l'authentification par carte à puce.



Authentification RSA SecurID

L'application Citrix Workspace prend en charge l'authentification RSA SecurID pour les configurations de Secure Web Gateway. Les configurations sont effectuées via l'Interface Web et sont appliquées à toutes les configurations Citrix Gateway.

Schéma d'URL requis pour le jeton logiciel sur l'application Citrix Workspace pour iOS : le jeton logiciel RSA SecurID utilisé par l'application Citrix Workspace enregistre uniquement le schéma d'URL com.citrix.securid.

Si les utilisateurs ont installé l'application Citrix Workspace et RSA SecurID sur leur appareil iOS, ils doivent sélectionner le schéma d'URL **com.citrix.securid** pour importer RSA SecurID Software Authenticator (jeton logiciel) sur l'application Citrix Workspace de leur appareil.

Pour importer un jeton logiciel RSA SecurID

Pour utiliser un jeton logiciel RSA avec l'application Citrix Workspace, en tant qu'administrateur, assurez-vous que les utilisateurs suivent :

- la stratégie concernant la longueur du code PIN ;
- le type de code PIN (numérique uniquement et alphanumérique) ;
- les limites liées à la réutilisation du code PIN.

Une fois que l'utilisateur s'est authentifié auprès du serveur RSA, il ne doit configurer le code PIN qu'une seule fois. Après la vérification du code PIN, il est également authentifié auprès du serveur StoreFront. Après toutes les vérifications, l'application Workspace affiche les applications et bureaux disponibles et publiés.

Pour utiliser un jeton logiciel RSA

1. Importez le jeton logiciel RSA qui vous a été fourni par votre organisation.
2. À partir de l'e-mail contenant votre fichier SecurID, sélectionnez **Ouvrir dans Workspace** en tant que destination d'importation. Une fois le jeton logiciel importé, l'application Citrix Workspace s'ouvre automatiquement.
3. Si votre organisation vous a fourni un mot de passe pour l'importation, entrez-le et cliquez sur **OK**. Après avoir cliqué sur **OK**, un message vous indiquera que le jeton a été importé avec succès.
4. Fermez le message d'importation et cliquez sur **Ajouter un compte** dans l'application Citrix Workspace.
5. Entrez l'adresse URL du magasin fournie par votre organisation et cliquez sur **Suivant**.
6. Sur l'écran Ouvrir session, entrez vos informations d'identification : nom d'utilisateur, mot de passe et domaine. Pour le champ de code PIN, entrez **0000**, sauf si votre organisation vous a fourni un code PIN par défaut différent. Le code PIN 0000 est le code RSA par défaut, mais il est possible que votre organisation l'ait modifié pour se conformer à ses stratégies de sécurité.
7. Dans le coin supérieur gauche, cliquez sur **Ouvrir session**. Un message apparaît pour créer un code PIN.
8. Entrez un code PIN composé de 4 à 8 chiffres et cliquez sur **OK**. Un message apparaît pour vérifier votre nouveau code PIN.
9. Entrez à nouveau votre code PIN et cliquez sur **OK**. Vous pouvez désormais accéder à vos applications et bureaux.

Code de jeton suivant

L'application Citrix Workspace prend en charge la fonctionnalité de code de jeton suivant lorsque vous configurez Citrix Gateway avec l'authentification RSA SecurID. Si vous entrez trois mots de passe incorrects, un message d'erreur s'affiche sur le plug-in Citrix Gateway. Pour vous connecter, attendez le jeton suivant. Le serveur RSA peut être configuré pour désactiver un compte utilisateur si un utilisateur se connecte un certain nombre de fois à l'aide d'un mot de passe incorrect.

Informations d'identification dérivées

La prise en charge des informations d'identification dérivées Purebred est disponible dans l'application Citrix Workspace. Lorsqu'ils se connectent à un magasin qui autorise les informations d'identification dérivées, les utilisateurs peuvent se connecter à l'application Citrix Workspace à l'aide d'une carte à puce virtuelle. Cette fonctionnalité est prise en charge uniquement sur les déploiements sur site.

> **Remarque :**
>
> Citrix Virtual Apps and Desktops 7 1808 ou version ultérieure est nécessaire pour utiliser cette fonctionnalité.

Pour activer les informations d'identification dérivées dans l'application Citrix Workspace :

1. Accédez à **Paramètres** > **Avancé** > **Informations d'identification dérivées**.
2. Appuyez sur **Utiliser informations d'identification dérivées**.

Pour créer une carte à puce virtuelle à utiliser avec les informations d'identification dérivées :

1. Dans **Paramètres** > **Avancé** > **Informations d'identification dérivées**, appuyez sur **Ajouter nouvelle carte à puce virtuelle**.
2. Modifiez le nom de la carte à puce virtuelle.
3. Entrez un code PIN à 8 chiffres uniquement et confirmez.
4. Appuyez sur **Suivant**.
5. Sous Certificat d'authentification, appuyez sur **Importer le certificat…**
6. Le sélecteur de documents s'affiche. Appuyez sur **Parcourir**.
7. Sous Emplacements, sélectionnez **Chaîne de clé Purebred**.
8. Sélectionnez le certificat d'authentification approprié dans la liste.
9. Appuyez sur **Importer la clé**.
10. Répétez les étapes 5 à 9 pour le certificat de signature numérique et le certificat de chiffrement, si vous le souhaitez.
11. Appuyer sur **Enregistrer**.

Vous pouvez importer jusqu'à trois certificats pour votre carte à puce virtuelle. Le certificat d'authentification est requis pour que la carte à puce virtuelle fonctionne correctement. Le certificat de chiffrement et le certificat de signature numérique peuvent être ajoutés pour une utilisation dans une session VDA.

> **Remarque :**
>
> Lors de la connexion à une session HDX, la carte à puce virtuelle créée est redirigée vers la session.

Limitations connues

- Les utilisateurs ne peuvent avoir qu'une seule carte active à la fois.
- Une fois qu'une carte à puce virtuelle est créée, elle ne peut pas être modifiée. Supprimez et créez une carte.
- Un code PIN peut être saisi incorrectement dix fois. S'il n'est pas valide après dix essais, la carte à puce virtuelle est supprimée.
- Lorsque vous sélectionnez des informations d'identification dérivées, la carte à puce virtuelle remplace une carte à puce physique.

Chaîne agent-utilisateur pour WKWebView

Par défaut, la chaîne agent-utilisateur utilisée lors de certaines requêtes réseau initiées via WKWebView inclut désormais l'identifiant de l'application Citrix Workspace.

Par conséquent, elle est passée de :

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_2 like Mac OS X)AppleWebKit
/605.1.15 (KHTML, like Gecko)Mobile/15E148 AuthManager/3.2.4.0
```

À :

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X)AppleWebKit
/605.1.15 (KHTML, like Gecko)Mobile/15E148 CWA/23.3.0 iOS/15.0
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone
```

(Exemple d'iPhone)

Ou

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X)AppleWebKit
/605.1.15 (KHTML, like Gecko)Mobile/15E148 CWA/23.3.0 iOS/15.0
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad
```

(Exemple d'iPad)

Authentification nFactor

Prise en charge de l'authentification multifacteur (nFactor)

L'authentification multifacteur améliore la sécurité d'une application en exigeant des utilisateurs qu'ils fournissent plusieurs preuves d'identification pour y accéder. L'authentification multifacteur rend les étapes d'authentification et les formulaires de collecte d'informations d'identification associés configurables par l'administrateur.

L'application Citrix Workspace native peut prendre en charge ce protocole en s'appuyant sur le support de formulaires de connexion déjà mis en œuvre pour StoreFront. La page de connexion Web pour les serveurs virtuels Citrix Gateway et Traffic Manager utilise également ce protocole.

Pour plus d'informations, consultez Authentification SAMLet Authentification multifacteur (nFactor).

Limitations :

- Lorsque nFactor est activé, vous ne pouvez pas utiliser d'authentification biométrique telle que Touch ID et Face ID.

Prise en charge de la stratégie d'authentification nFactor Advanced

Nous prenons désormais en charge l'authentification basée sur les certificats sur l'application Citrix Workspace lorsqu'elle est configurée via des stratégies d'authentification nFactor Advanced sur Citrix Gateway. L'authentification nFactor permet de configurer des schémas multifacteurs flexibles et agiles.

Chaîne agent-utilisateur :

Lors de l'authentification avancée (nFactor) pour l'application Citrix Workspace sur iPhone ou iPad, le processus d'authentification est redirigé vers un affichage Web intégré. La chaîne d'agent utilisateur qui en résulte peut varier légèrement en fonction de la version du système d'exploitation, de la version de compilation de CWA, du modèle d'appareil et de la version d'AuthManager. Par exemple, considérez les chaînes d'agent utilisateur suivantes pour iPhone et iPad.

Pour iPhone :

```
Mozilla/5.0 (iPhone; CPU iPhone OS 16_2 like Mac OS X)AppleWebKit
/605.1.15 (KHTML, like Gecko)Mobile/15E148 CWA/23.5.0 iOS/16.2
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone
AuthManager/3.3.0.0
```

Pour iPad :


```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6)AppleWebKit/605.1.15 (
KHTML, like Gecko)Mobile/15E148 CWA/23.5.0 iOS/15.0 X1Class CWACapable
 302RedirectionCapable CFNetwork Darwin CWA-iPad AuthManager/3.3.0.0
```

Cette fonctionnalité est disponible dans la Tech Preview. Elle peut être activée sur demande à l'aide du lien Podio ou en contactant le support technique de Citrix. Toutefois, elle sera eventuellement déployée auprès de tous les clients une fois la version préliminaire terminée.

> **Remarque :**
>
> - Les informations relatives à la version ou au modèle de l'appareil peuvent varier en fonction de l'environnement.
> - Pour appliquer les stratégies basées sur les agents utilisateur spécifiques à l'application Citrix Workspace pour iOS lors de l'authentification, utilisez les mots clés suivants :
>   - iOS
>   - CWA
>   - CWACapable

Prise en charge de l'authentification basée sur FIDO2 lors de la connexion à une session HDX

L'application Citrix Workspace pour iOS prend désormais en charge l'authentification sans mot de passe au sein d'une session Citrix Virtual Apps and Desktops à l'aide de méthodes d'authentification basées sur FIDO2. Cette fonctionnalité permet aux utilisateurs de se connecter à un site Web compatible avec WebAuthn avec des navigateurs tels que Google Chrome ou Microsoft Edge à l'aide de clés de sécurité Yubico compatibles avec FIDO2. Le simple fait d'ouvrir un site Web compatible avec WebAuthn déclenche une authentification sans mot de passe.
Seuls les appareils dotés de ports Lightning sont pris en charge (les appareils dotés de ports USB-C ou USB 4 ne sont pas pris en charge). La connexion à l'application Citrix Workspace ou à une session de bureau à l'aide d'une authentification sans mot de passe n'est pas prise en charge.

Pour plus d'informations sur les conditions requises, consultez la section Autorisation locale et authentification virtuelle à l'aide de FIDO2 dans la documentation de Citrix Virtual Apps and Desktops.

Prise en charge de l'authentification à l'aide de FIDO2 lors de la connexion à un magasin cloud

À partir de la version 24.5.0, les utilisateurs peuvent s'authentifier auprès de l'application Citrix Workspace à l'aide de l'authentification sans mot de passe basée sur FIDO2 lors de la connexion à un magasin cloud. Le protocole FIDO2 offre une méthode d'authentification transparente, permettant aux

employés de l'entreprise d'accéder aux applications et bureaux pendant les sessions virtuelles sans avoir à saisir de nom d'utilisateur ni de mot de passe. Cette fonctionnalité prend en charge à la fois l'itinérance (USB uniquement) et les authentificateurs de plateforme (code PIN, Touch ID et Face ID uniquement). Cette fonctionnalité est activée par défaut.

> **Remarque :**
>
> L'authentification FIDO2 est prise en charge par défaut avec les onglets personnalisés de Chrome. Si vous souhaitez utiliser l'authentification FIDO2 avec WebView, signalez-le à l'aide du formulaire Podio.

Prise en charge de la configuration du stockage des jetons d'authentification lors du déploiement local

L'application Citrix Workspace pour iOS propose désormais une option permettant de configurer le stockage des jetons d'authentification sur le disque local, pour les magasins locaux. Grâce à cette fonctionnalité, vous pouvez désactiver le stockage du jeton d'authentification pour renforcer la sécurité. Après la désactivation, lorsque le système ou la session redémarre, vous devez vous authentifier à nouveau pour accéder à la session.

Pour désactiver le stockage des jetons d'authentification sur le déploiement local à l'aide du fichier de configuration d'administration, procédez comme suit :

1. Utilisez un éditeur de texte pour ouvrir le fichier web.config, qui se trouve généralement dans `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Recherchez l'élément de compte d'utilisateur dans le fichier (Store est le nom de compte de votre déploiement).
   Par exemple : `<account id=... name="Store">`
3. Avant la balise `</account>`, accédez aux propriétés de ce compte utilisateur et ajoutez ce qui suit :

```
    <properties>
        <property name="TokenPersistence" value="false" />
    </properties>
<!--NeedCopy-->
```

Voici un exemple du fichier web.config :

```
    <account id="########################################" name="Store
        Service"
        description="" published="true" updaterType="None"
           remoteAccessType="StoresOnly">
        <annotatedServices>
            <clear />
            <annotatedServiceRecord serviceRef="1__Citrix_Store">
                <metadata>
```



```
                    <plugins>
                        <clear />
                    </plugins>
                    <trustSettings>
                        <clear />
                    </trustSettings>
                    <properties>
                        <clear />
                        <property name="TokenPersistence" value="false"
                            />
                     </properties>
                </metadata>
            </annotatedServiceRecord>
        </annotatedServices>
        <metadata>
        <plugins>
          <clear />
        </plugins>
        <trustSettings>
          <clear />
        </trustSettings>
        <properties>
        </properties>
     </metadata>
    </account>
<!--NeedCopy-->
```

Sécuriser

January 10, 2024

Pour sécuriser les communications entre votre batterie de serveurs et l'application Citrix Workspace, intégrez vos connexions à la batterie de serveurs grâce à un large choix de technologies de sécurité, y compris Citrix Gateway.

> **Remarque :**
>
> Citrix recommande d'utiliser Citrix Gateway pour sécuriser les communications entre les serveurs StoreFront et les appareils des utilisateurs.

- Un serveur proxy SOCKS ou serveur proxy sécurisé (également appelé serveur proxy ou serveur proxy HTTPS).

  Vous pouvez utiliser des serveurs proxy pour limiter l'accès à l'intérieur et à l'extérieur de votre réseau, et pour gérer les connexions entre l'application Citrix Workspace et les serveurs. L'application Citrix Workspace prend en charge les protocoles de proxy SOCKS et de proxy sécurisé.

- Secure Web Gateway.

Vous pouvez utiliser Secure Web Gateway avec l'Interface Web pour fournir un point d'accès Internet unique, sécurisé et chiffré aux serveurs des réseaux d'entreprise internes.

Vous pouvez utiliser Secure Web Gateway avec l'Interface Web pour fournir des données uniques, sécurisées et chiffrées. Les serveurs des réseaux d'entreprise internes peuvent accéder aux données sécurisées via Internet.

- Solutions de relais SSL avec protocoles TLS.
- Un pare-feu.

  Les pare-feu de réseau peuvent autoriser ou empêcher le passage des paquets de données en fonction de l'adresse et du port de destination.

  Si vous utilisez l'application Citrix Workspace avec un pare-feu de réseau qui mappe l'adresse IP interne du serveur sur une adresse Internet externe (c'est-à-dire, la traduction d'adresse de réseau, ou NAT), configurez l'adresse externe.

Citrix Gateway

Pour permettre aux utilisateurs distants de se connecter à votre déploiement Citrix Endpoint Management via Citrix Gateway, vous pouvez configurer les certificats de manière à fonctionner avec StoreFront. La méthode que vous allez choisir pour autoriser l'accès dépend de l'édition de Citrix Endpoint Management dans votre déploiement.

Si vous déployez Citrix Endpoint Management dans votre réseau, autorisez les connexions des utilisateurs internes ou distants à StoreFront via Citrix Gateway en intégrant Citrix Gateway et StoreFront. Cette fonctionnalité permet aux utilisateurs de se connecter à StoreFront pour accéder aux applications publiées XenApp et aux bureaux virtuels XenDesktop. Les utilisateurs se connectent via l'application Citrix Workspace.

Secure Web Gateway

Cette rubrique s'applique uniquement aux déploiements faisant appel à l'Interface Web.

Vous pouvez utiliser Secure Web Gateway en mode Normal ou en mode Relais afin de fournir un canal sécurisé de communication entre l'application Citrix Workspace et le serveur. Si vous utilisez Secure Web Gateway en mode **Normal**, l'application Citrix Workspace ne nécessite aucune configuration. Vérifiez que les utilisateurs se connectent via l'Interface Web.

L'application Citrix Workspace utilise les paramètres configurés à distance sur le serveur Interface Web pour se connecter aux serveurs exécutant Secure Web Gateway.

Si le proxy Secure Web Gateway est installé sur un serveur dans le réseau sécurisé, vous pouvez l'utiliser en mode Relais. Si vous utilisez le mode Relais, le serveur Secure Web Gateway fonctionne

comme un serveur proxy. Dans ce cas, vous devez configurer l'application Citrix Workspace pour qu'elle utilise :

- le nom de domaine complet du serveur Secure Web Gateway ;
- le numéro de port du serveur Secure Web Gateway.

> **Remarque :**
>
> Secure Web Gateway version 2.0 ne prend pas en charge le mode Relais.

Le nom de domaine complet (FQDN) doit contenir, dans l'ordre, les trois composants suivants :

- Nom d'hôte
- Domaine intermédiaire
- Domaine de tête

Par exemple : `my_computer.example.com` est un nom de domaine complet car il liste dans l'ordre un nom d'hôte (`my_computer`), un domaine intermédiaire (exemple) et un domaine de tête (`com`). La combinaison du domaine intermédiaire et du domaine de tête (`example. com`) est appelée nom de domaine.

Serveur proxy

Les serveurs proxy permettent de limiter l'accès vers et depuis votre réseau, et de gérer les connexions entre l'application Citrix Workspace et les serveurs. L'application Citrix Workspace prend en charge les protocoles de proxy SOCKS et de proxy sécurisé.

L'application Citrix Workspace utilise les paramètres de serveur proxy pour communiquer avec le serveur Citrix Virtual Apps and Desktops. Les paramètres du serveur proxy sont configurés à distance sur le serveur de l'Interface Web.

Lorsque l'application Citrix Workspace communique avec le serveur Web, l'application utilise les paramètres du serveur proxy. Configurez les paramètres du serveur proxy pour le navigateur Web par défaut sur la machine utilisateur.

Pare-feu

Les pare-feu de réseau peuvent autoriser ou empêcher le passage des paquets de données en fonction de l'adresse et du port de destination. Si vous utilisez un pare-feu dans votre déploiement, l'application Citrix Workspace doit pouvoir communiquer via le pare-feu avec le serveur Web et le serveur Citrix. Le pare-feu doit autoriser le trafic HTTP pour les communications entre les machines utilisateur et le serveur Web. Généralement, le trafic HTTP passe par le port HTTP standard 80 ou 443 si un serveur

Web sécurisé est utilisé. Pour les communications avec le serveur Citrix, le pare-feu doit autoriser le trafic ICA entrant sur les ports 1494 et 2598.

Si le pare-feu est configuré pour la traduction des adresses réseau, vous pouvez vous servir de l'Interface Web pour définir les mappages depuis les adresses internes vers les adresses externes et les ports. Par exemple, si votre serveur Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) n'est pas configuré avec une adresse secondaire, vous pouvez configurer l'Interface Web pour qu'elle fournisse une adresse secondaire à l'application Citrix Workspace pour iOS. L'application Citrix Workspace pour iOS se connecte ensuite au serveur à l'aide de l'adresse externe et du numéro de port.

TLS

L'application Citrix Workspace prend en charge TLS 1.0, 1.1 et 1.2 avec les suites de chiffrement suivantes pour les connexions TLS à XenApp et XenDesktop :

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **Remarque :**
>
> L'application Citrix Workspace exécutée sur iOS 9 et versions ultérieures ou la version 21.2.0 ne prend pas en charge les suites de chiffrement TLS suivantes :
>
> - TLS_RSA_WITH_RC4_128_SHA
> - TLS_RSA_WITH_RC4_128_MD5

TLS (Transport Layer Security) est la dernière version normalisée du protocole TSL. Le groupe de travail Internet Engineering Taskforce (IETF) l'a rebaptisé TLS lorsqu'il est devenu responsable du développement de TLS sous la forme d'une norme ouverte.

TLS garantit la sécurité des communications de données grâce à l'authentification des serveurs, au chiffrement du flux de données et aux contrôles d'intégrité des messages. Certaines organisations, notamment des organisations gouvernementales américaines, requièrent l'utilisation du protocole TLS pour la sécurisation de leurs communications de données. Ces organisations peuvent également exiger l'utilisation d'une cryptographie éprouvée, telle que FIPS 140. La norme FIPS 140 est une norme de cryptographie.

L'application Citrix Workspace prend en charge les clés RSA de longueur 1024, 2048 et 3072. Les certificats racine avec des clés RSA de longueur de 4 096 bits sont aussi pris en charge.

> **Remarque :**
>
> - L'application Citrix Workspace utilise la cryptographie de plate-forme (iOS) pour les connexions entre l'application Citrix Workspace pour iOS et StoreFront.

Configurer et activer TLS

Deux étapes principales permettent de configurer TLS :

1. Configurez le Relais SSL sur votre serveur Citrix Virtual Apps and Desktops et sur votre serveur Interface Web, procurez-vous le certificat serveur approprié et installez-le.
2. Installez le certificat racine équivalent sur la machine utilisateur.

Installer des certificats racine sur des machines utilisateur Pour sécuriser les communications entre l'application Citrix Workspace sur laquelle TLS est activé et Citrix Virtual Apps and Desktops, vous avez besoin d'un certificat racine sur la machine utilisateur. Le certificat vérifie la signature de l'autorité de certification sur le certificat du serveur.

iOS est fourni avec une centaine de certificats racine commerciaux préinstallés. Si vous souhaitez utiliser un certificat différent, vous pouvez en recevoir un auprès d'une autorité de certification et l'installer sur chaque machine utilisateur.

En fonction des procédures de sécurité de votre entreprise, vous pouvez installer le certificat racine sur chaque machine utilisateur plutôt que de demander aux utilisateurs de l'installer eux-mêmes. Le choix le plus sûr et le plus facile consiste à ajouter des certificats racine au trousseau iOS.

Pour ajouter un certificat racine au trousseau

1. Envoyez un e-mail à votre propre adresse avec le fichier de certificat.
2. Ouvrez le fichier de certificat sur l'appareil. Cette action démarre automatiquement l'application Trousseau d'accès.
3. Suivez les invites pour ajouter le certificat.
4. À compter d'iOS 10, vérifiez que le certificat est approuvé en accédant à **Réglages iOS** > **Informations** > **Réglages des certificats**.

   Sous Réglages des certificats, consultez la section « ACTIVER LA CONFIANCE TOTALE POUR LES CERTIFICATS RACINE. » Assurez-vous que votre certificat a été sélectionné pour une confiance totale.

Le certificat racine est installé. Les clients TLS et les autres applications utilisant TLS peuvent utiliser le certificat racine à l'aide de TLS.

Site XenApp et XenDesktop

Pour configurer le site XenApp et XenDesktop :

> **Important :**
>
> - L'application Citrix Workspace utilise les sites XenApp et XenDesktop qui prennent en charge Citrix Secure Gateway 3.x.
> - L'application Citrix Workspace utilise les sites Web Citrix Virtual Apps qui prennent en charge Citrix Secure Gateway 3.x.
> - Les sites XenApp et XenDesktop ne prennent en charge que l'authentification à un facteur.
> - Les sites Web Citrix Virtual Apps prennent en charge l'authentification à un facteur et à deux facteurs.
> - Tous les navigateurs intégrés prennent en charge l'Interface Web 5.4.

Avant de commencer la configuration, installez et configurez Citrix Gateway de sorte qu'il fonctionne avec l'Interface Web. Vous pouvez modifier ces instructions afin de les adapter à votre environnement spécifique.

Si vous utilisez une connexion Citrix Secure Gateway, ne configurez pas les paramètres Citrix Gateway sur l'application Citrix Workspace.

L'application Citrix Workspace utilise un site XenApp et XenDesktop pour obtenir des informations sur les applications auxquelles un utilisateur est autorisé à accéder. Au cours de ce processus, les informations sont présentées à l'application Citrix Workspace exécutée sur votre appareil. De même, vous pouvez utiliser l'Interface Web pour les connexions Citrix Virtual Apps traditionnelles basées sur SSL. Pour la même connexion basée sur SSL, vous pouvez configurer Citrix Gateway. Cette capacité de configuration est intégrée aux sites XenApp et XenDesktop exécutés sur l'Interface Web 5.x.

Configurez le site XenApp et XenDesktop pour prendre en charge des connexions provenant d'une connexion Citrix Secure Gateway :

1. Dans le site XenApp et XenDesktop, sélectionnez **Gérer l'accès client sécurisé** > **Modifier les paramètres d'accès au client sécurisé**.
2. Dans Méthode d'accès, choisissez **Passerelle directe**.
3. Entrez le nom de domaine complet de l'appliance Secure Web Gateway.
4. Entrez les informations de Secure Ticket Authority (STA).

> **Remarque :**
>
> Pour Citrix Secure Gateway, Citrix recommande d'utiliser le chemin d'accès par défaut Citrix (//NomServeurXenApp/Citrix/PNAgent). Le chemin par défaut permet aux utilisateurs de spécifier le nom de domaine complet de la passerelle Secure Web Gateway à laquelle ils se connectent. N'utilisez pas le chemin d'accès complet au fichier config.xml qui se trouve sur le site XenApp et XenDesktop. Par exemple, //XenAppServerName/CustomPath/config.xml).

Pour configurer Citrix Secure Gateway

1. Utilisez l'assistant de configuration Citrix Secure Gateway pour configurer la passerelle.

   Citrix Secure Gateway prend en charge le serveur dans le réseau sécurisé qui héberge le site XenApp Service.

   Après avoir sélectionné l'option **Indirect**, entrez le chemin d'accès du nom de domaine complet de votre serveur passerelle Secure Web Gateway et complétez les étapes suivantes de l'assistant.

2. Testez une connexion à partir d'une machine utilisateur pour vous assurer que Secure Web Gateway est correctement configuré en termes de réseau et d'allocation de certificat.

Pour configurer l'appareil mobile

1. Lors de l'ajout d'un compte Citrix Secure Gateway, entrez le nom de domaine complet correspondant de votre serveur Citrix Secure Gateway dans le champ **Adresse** :

   - Si vous avez créé les sites XenApp et XenDesktop à l'aide du chemin d'accès par défaut (/Citrix/PNAgent), entrez le FQDN de Secure Web Gateway : FQDNofSecureGateway.companyName.com
   - Si vous avez personnalisé le chemin d'accès aux sites XenApp et XenDesktop, entrez le chemin d'accès complet au fichier config.xml, tel que : FQDNofSecureGateway.companyName.com/CustomPath/config.xml

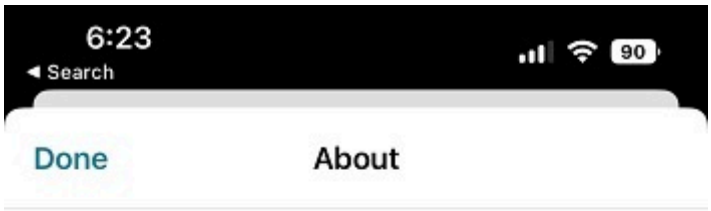
2. Si vous configurez manuellement le compte, désactivez l'option Citrix Gateway **Nouveau compte**.

Dépannage

May 9, 2024

Comment vérifier la version de l'application

Pour vérifier la version de votre application Citrix Workspace, ouvrez-la, puis appuyez sur **Paramètres** > **À propos de**. Les informations de version s'affichent sur votre écran.



Comment mettre à niveau l'application Citrix Workspace vers la dernière version

Vous pouvez mettre à niveau l'application Citrix Workspace vers la dernière version depuis l'App Store. Recherchez l'application Citrix Workspace et appuyez sur le bouton **Mettre à niveau**.

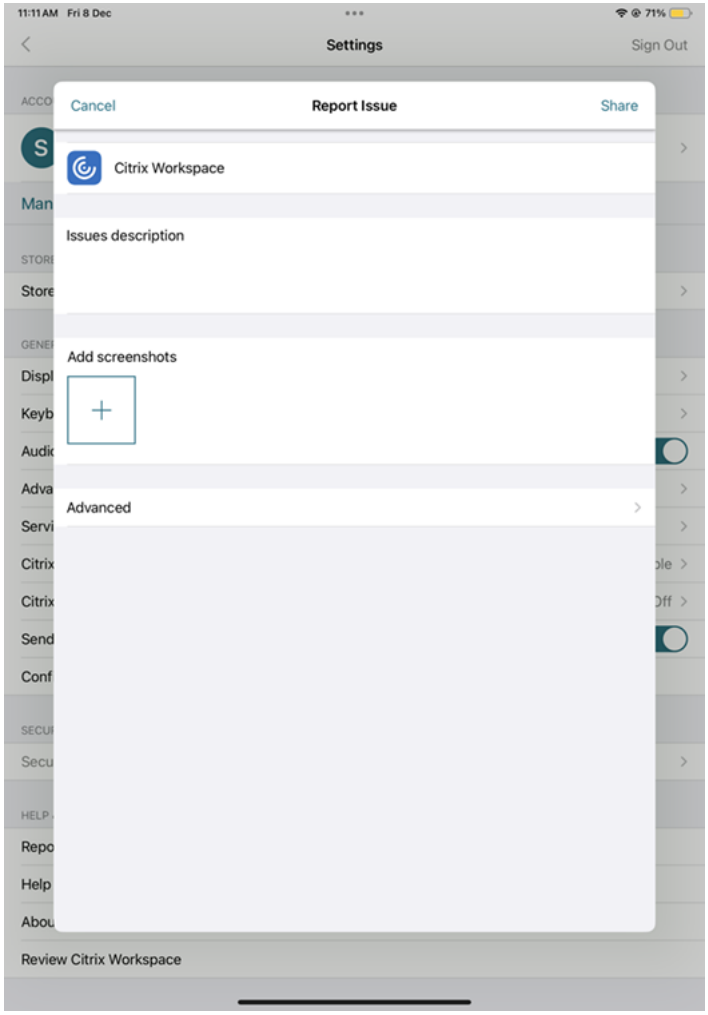
Comment réinitialiser l'application Citrix Workspace

Vous pouvez réinitialiser votre application Citrix Workspace à l'aide de l'une des méthodes suivantes :

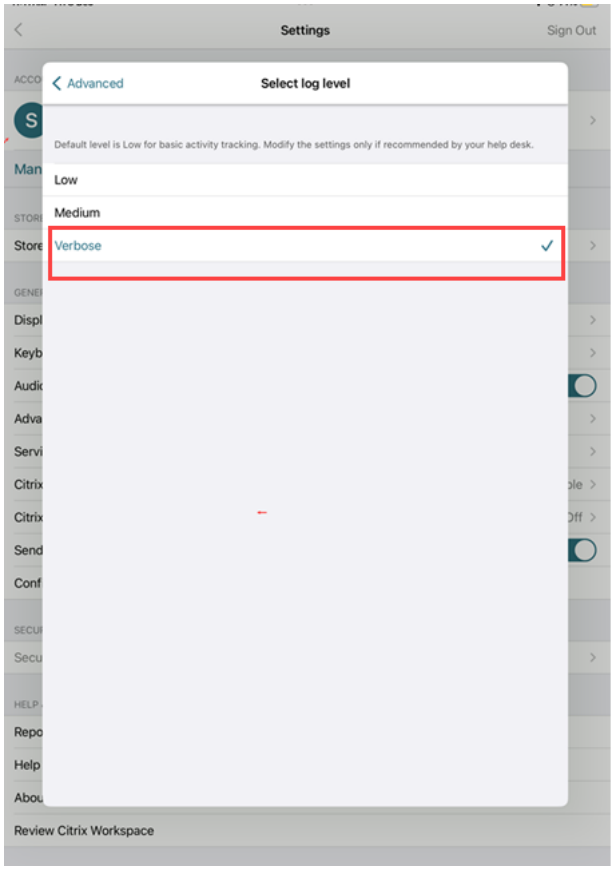
- Supprimer tous les comptes existants de l'application Citrix Workspace
- Effacer les données de stockage de l'application Citrix Workspace
- Désinstaller l'application Citrix Workspace actuelle et installer la dernière version de l'application Citrix Workspace pour iOS qui contient le dernier correctif.

Comment collecter des journaux

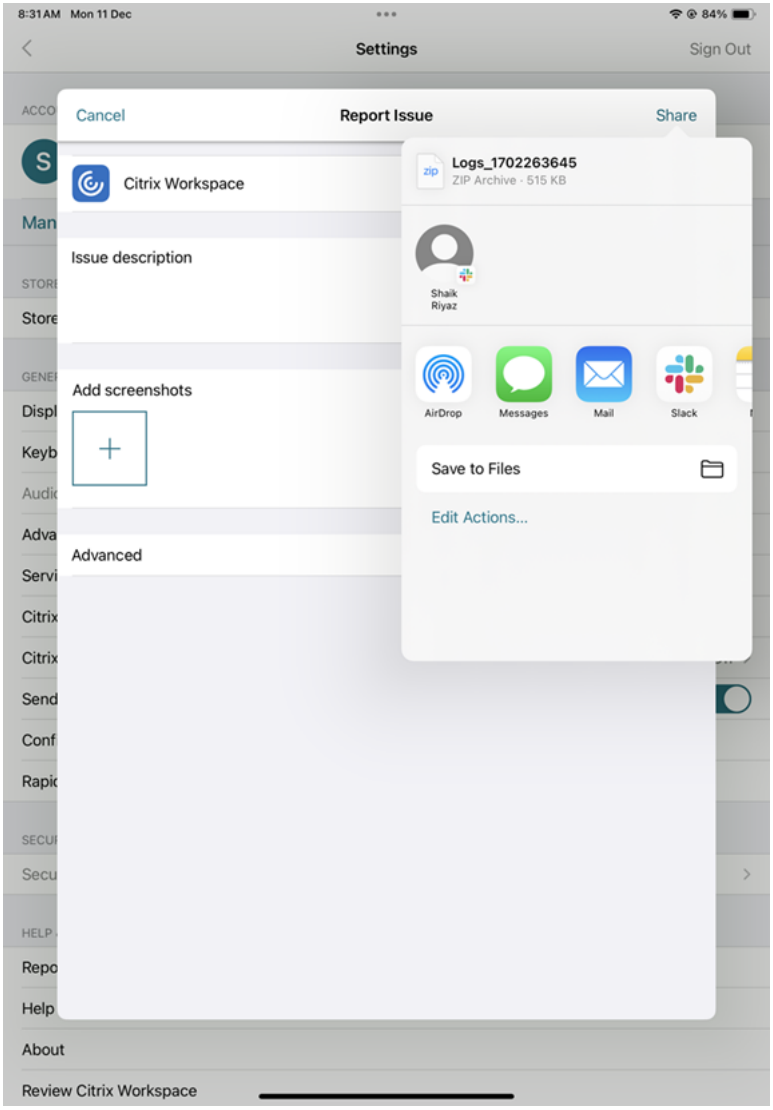
1. Ouvrez l'application Citrix Workspace et accédez à **Paramètres**.
2. Dans **Aide et support**, sélectionnez **Signaler un problème**.



3. Reproduisez le problème.
4. Sur la page Sélectionnez le niveau de journalisation, sélectionnez **Détaillé**.



5. Sur la page **Sélectionnez l'emplacement du journal**, sélectionnez **Console et Fichier**.
6. Partagez le fichier ZIP avec Citrix.



Comment demander des améliorations

Vous pouvez envoyer vos demandes d'améliorations en remplissant ce formulaire.

Comment accéder aux fonctionnalités de version Technical Preview

Vous pouvez demander des fonctionnalités en version Technical Preview à l'aide d'un formulaire Podio propre à chaque fonctionnalité. Vous trouverez ce formulaire joint à l'annonce de version Technical Preview dans la documentation du produit.

Comment fournir des commentaires sur la version EAR

Pour nous faire part de vos commentaires sur la version EAR, appuyez ici.

Problèmes courants et conseils de dépannage

Sessions déconnectées

Les utilisateurs peuvent se déconnecter (mais pas fermer de session) d'une session d'application Citrix Workspace pour iOS des manières suivantes :

- Lors de l'affichage d'une application ou d'un bureau publié dans une session :
  - appuyez sur la flèche en haut de l'écran pour afficher le menu déroulant de la session.
  - appuyez sur le bouton **Accueil** pour revenir à votre point de départ.
  - remarquez l'ombre blanche sous l'icône de l'une des applications publiées toujours dans une session active ; appuyez sur l'icône.
  - appuyez sur Déconnecter.
- Fermer l'application Citrix Workspace pour iOS :
  - appuyez deux fois sur le bouton **Accueil** de l'appareil.
  - Localisez l'application Citrix Workspace pour iOS dans la vue du sélecteur d'application iOS.
  - appuyez sur Déconnecter dans la boîte de dialogue qui s'affiche.
- En appuyant sur le bouton d'accueil sur leur appareil mobile.
- En tapant sur Accueil ou Basculer dans le menu déroulant de l'application.

La session affiche un état déconnecté. Bien que l'utilisateur puisse se reconnecter ultérieurement, vous pouvez vérifier que les sessions déconnectées s'affichent comme inactives après un certain laps de temps.

Pour afficher l'application en mode inactif, configurez un délai d'expiration de session pour la connexion ICA-TCP dans la configuration d'hôte de session Bureau à distance (anciennement appelée « Configuration des services Terminal Server »).

Pour de plus amples informations sur la configuration de Services Bureau à distance (anciennement appelée « Services Terminal Server »), reportez-vous à la documentation produit Microsoft Windows Server.

Mots de passe expirés

L'application Citrix Workspace pour iOS permet aux utilisateurs de modifier leurs mots de passe quand ils ont expiré. Ils sont invités à entrer les informations requises.

Appareils jailbreakés

Vos utilisateurs peuvent compromettre la sécurité de votre déploiement en se connectant à l'aide d'appareils iOS jailbreakés. Les appareils jailbreakés sont des appareils qui ont été modifiés par leurs propriétaires, généralement dans le but de contourner certaines mesures de sécurité.

Lorsque l'application Citrix Workspace pour iOS détecte un appareil iOS jailbreaké, elle affiche une alerte.

Pour sécuriser davantage votre environnement, vous pouvez configurer StoreFront ou l'Interface Web de manière à empêcher les appareils jailbreakés d'exécuter des applications.

Exigences

- Citrix Receiver pour iOS 6.1 ou version ultérieure
- StoreFront 3.0 ou Interface Web 5.4 ou version ultérieure
- Accès à StoreFront ou l'Interface Web via un compte d'administrateur

Pour empêcher les appareils jailbreakés d'exécuter des applications

1. Ouvrez une session sur le serveur StoreFront ou Interface Web en tant qu'utilisateur doté de privilèges d'administrateur.
2. Recherchez le fichier **`default`**`.ica`, qui se trouve dans l'un des emplacements suivants :
    - `C:\\inetpub\\wwwroot\\Citrix\\*storename*\\conf` (Microsoft Internet Information Services)
    - `C:\\inetpub\\wwwroot\\Citrix\\*storename*\\App\\_Data` (Microsoft Internet Information Services)
    - `./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF` (Apache Tomcat)
3. Sous la section **[Application]** ajoutez ce qui suit : **AllowJailBrokenDevices=OFF**
4. Enregistrez le fichier et redémarrez votre serveur StoreFront ou Interface Web.

Après avoir redémarré le serveur StoreFront, les utilisateurs qui ont vu l'alerte à propos des appareils jailbreakés ne peuvent pas lancer d'applications depuis votre serveur StoreFront ou Interface Web.

Pour autoriser les appareils jailbreakés à exécuter des applications Si vous ne définissez pas AllowJailBrokenDevices, l'alerte est affichée par défaut aux utilisateurs d'appareils jailbreakés mais ils sont quand même autorisés à lancer des applications.

Si vous voulez spécifiquement autoriser vos utilisateurs à exécuter des applications sur des appareils jailbreakés :

1. Ouvrez une session sur le serveur StoreFront ou Interface Web en tant qu'utilisateur doté de privilèges d'administrateur.
2. Accédez au fichier default.ica, qui se trouve dans l'un des emplacements suivants :
    - `C:\\inetpub\\wwwroot\\Citrix\\*storename*\\conf` (Microsoft Internet Information Services)
    - `C:\\inetpub\\wwwroot\\Citrix\\*storename*\\App\\_Data` (Microsoft Internet Information Services)
    - `./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF` (Apache Tomcat)
3. Sous la section **[Application]** ajoutez ce qui suit : **AllowJailBrokenDevices=ON**
4. Enregistrez le fichier et redémarrez votre serveur StoreFront ou Interface Web.

Lorsque vous définissez AllowJailBrokenDevices sur ON, vos utilisateurs voient l'alerte relative à l'utilisation d'un appareil jailbreaké, mais ils peuvent exécuter des applications depuis StoreFront où l'Interface Web.

Perte de qualité audio HDX

Depuis Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), il se peut que la qualité de l'audio HDX vers l'application Citrix Workspace pour iOS se détériore. Le problème se produit lorsque vous utilisez simultanément l'audio et la vidéo.

Le problème se produit lorsque les stratégies HDX Citrix Virtual Apps and Desktops et Citrix DaaS ne peuvent pas gérer la quantité de données audio avec les données vidéo.

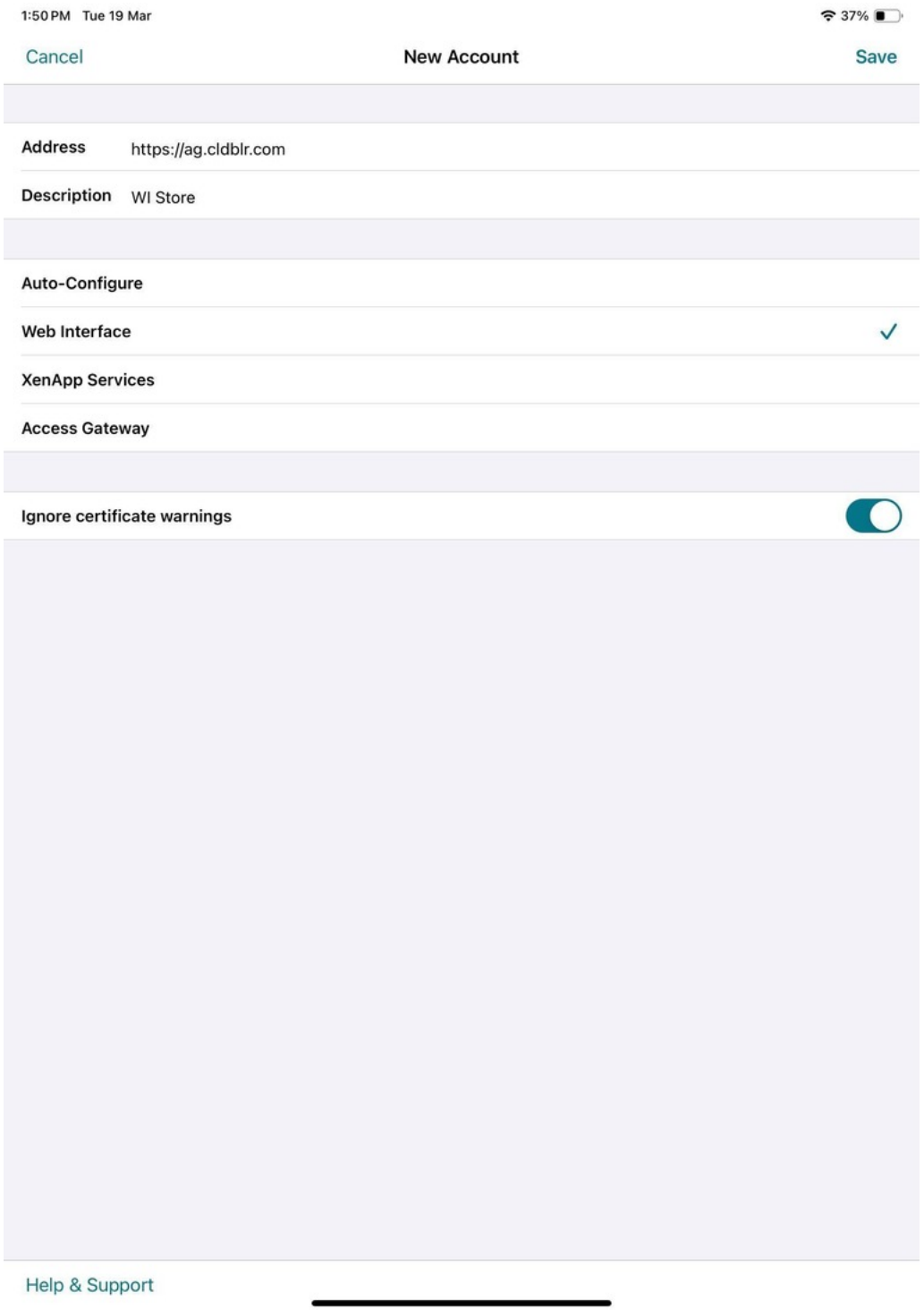
Pour des suggestions sur la création de stratégies destinées à améliorer la qualité audio, consultez l'article CTX123543 du centre de connaissances.

Impossible de lancer les sessions de bureau et d'application pour une expérience de magasin personnalisée

Il se peut que vous ne parveniez pas à lancer des sessions de bureau et d'application à partir de l'application Citrix Workspace si vous disposez d'une expérience de magasin personnalisée. La découverte automatique du type de magasin est prise en charge uniquement pour les adresses e-mail et non pour les URL des magasins. Il est recommandé d'utiliser l'adresse e-mail ou le mode de connexion par l'interface Web si vous avez une magasin personnalisé. Pour plus d'informations, consultez Configuration manuelle et Configuration de la découverte de compte basée sur une adresse e-mail.

Pour configurer un compte manuellement via le mode de connexion par l'interface Web, procédez comme suit :

1. Touchez **l'icône Comptes, la fenêtre Comptes, puis le signe Plus (+)**. La fenêtre **Nouveau compte** s'affiche.
2. Dans le coin inférieur gauche, touchez l'icône à gauche de **Options** et touchez **Installation manuelle**. Des champs supplémentaires s'affichent sur l'écran.
3. Dans le champ **Adresse**, entrez l'adresse URL sécurisée du site ou de Citrix Gateway (par exemple, agee.mycompany.com).
4. Sélectionnez la connexion par l'**interface Web**. Ce mode de connexion affiche un site Web Citrix Virtual Apps semblable à un navigateur Web. Également appelé Affichage Web.



5. Pour le certificat de sécurité, utilisez le paramètre dans le champ **Ignorer les avertissements de certificat** pour spécifier si vous voulez vous connecter au serveur même s'il dispose d'un certificat non valide, auto-signé ou expiré. Le paramètre par défaut est Désactivé.

> **Important :**
>
> Si vous activez cette option, assurez-vous que vous vous connectez au serveur approprié. Citrix recommande fortement que tous les serveurs possèdent un certificat valide afin de protéger les machines utilisateur des attaques de sécurité en ligne. Un serveur sécurisé utilise un certificat SSL émis par une autorité de certification. Citrix ne prend pas en charge les certificats auto-signés et ne recommande pas d'ignorer le certificat de sécurité.

6. Appuyer sur **Enregistrer**.
7. Entrez votre nom d'utilisateur et mot de passe (ou jeton, si vous avez sélectionné l'authentification à deux facteurs) et touchez Ouvrir session. L'écran de l'application Citrix Workspace pour iOS s'affiche, dans lequel vous pouvez accéder à vos bureaux et ajouter et ouvrir vos applications.

> **Remarque :**
>
> Vous devez saisir les informations d'identification de l'utilisateur pour chaque connexion, car elles ne sont pas enregistrées dans le mode de connexion de l'interface Web.

FAQ

Comment améliorer les performances vidéo d'une application et d'un bureau virtuels sur les appareils mobiles ou à faible consommation

Pour plus d'informations sur la configuration des bureaux virtuels et l'amélioration des performances vidéo à l'aide de la valeur de registre "MaxFramesPerSecond"ou des stratégies HDX selon votre version de Citrix Virtual Apps and Desktops, consultez l'article CTX123543 du centre de connaissances.

Mes applications ou bureaux ne s'affichent pas après m'être connecté à l'application Citrix Workspace

Contactez le service d'assistance de votre entreprise ou l'administrateur de votre équipe de support informatique pour obtenir de l'aide.

Comment dépanner les problèmes de connexion lente ?

Si vous rencontrez l'un des problèmes suivants, suivez les étapes décrites dans la section **Solution** suivante.

- Connexions lentes au site Citrix Virtual Apps and Desktops
- Icônes d'application manquantes
- Messages Erreur de pilote de protocole récurrents

Solution Désactivez les propriétés de l'adaptateur Ethernet Citrix PV pour l'interface réseau sur le serveur Citrix Virtual Apps, Citrix Secure Web Gateway et le serveur d'interface Web.
Les propriétés de l'adaptateur Ethernet Citrix PV incluent les propriétés suivantes qui sont activées par défaut. Vous devez désactiver toutes ces propriétés.

- Large Send Offload
- Offload IP Checksum
- Offload TCP Checksum
- Offload UDP Checksum

> **Remarque :**
>
> Le redémarrage du serveur n'est pas nécessaire. Cette solution s'applique à Windows Server 2003 et 2008 32 bits. Ce problème n'affecte pas Windows Server 2008 R2.

Dépanner les problèmes liés aux touches numériques et aux caractères spéciaux

Si les touches numériques ou les caractères chinois IME ne fonctionnent pas comme prévu, vous devez désactiver l'option de clavier Unicode.
Pour désactiver l'option de clavier Unicode :

1. Accédez à **Paramètres** > **Options du clavier**.
2. Définissez **Utiliser clavier Unicode** sur **Désactivé**.

Application Citrix Workspace pour iOS

July 1, 2024

L'application Citrix Workspace pour iOS est un logiciel client pouvant être téléchargé depuis l'App Store. Il vous permet d'accéder et d'exécuter des bureaux virtuels et des applications hébergées mis à disposition par Citrix Virtual Apps and Desktops.

iOS est le système d'exploitation des appareils mobiles Apple tels qu'iPad et iPhone. L'application Citrix Workspace pour iOS s'exécute sur les appareils utilisant le système d'exploitation iOS, tels qu'iPhone X, iPad mini et iPad Pro.

Langues prises en charge

L'application Citrix Workspace pour iOS a été conçue pour être utilisée dans des langues autres que l'anglais. Pour obtenir la liste des langues prises en charge par l'application Citrix Workspace pour iOS, consultez la section Langues prises en charge.

Fin de prise en charge

Les annonces de cet article visent à vous avertir des plates-formes, des produits Citrix et des fonctionnalités qui vont disparaître pour que vous puissiez prendre les décisions appropriées. Citrix surveille l'utilisation des clients et leurs commentaires pour déterminer quand les retirer. Les annonces peuvent être modifiées dans les versions ultérieures et peuvent ne pas contenir chaque fonctionnalité amenée à disparaître.

Les éléments obsolètes ne sont pas retirés immédiatement. Citrix continue de les prendre en charge dans cette version, mais ils seront retirés à l'avenir.

Élément	Abandon annoncé	Supprimé dans	Solution alternative
Prise en charge du protocole DTLS 1.0	Application Citrix Workspace pour iOS version 24.5.0	-	Protocole DTLS 1.2
Prise en charge des protocoles TLS 1.0 et TLS 1.1	Application Citrix Workspace pour iOS version 24.4.0	-	Protocole TLS 1.2 ou TLS 1.3
XenApp Services (également connus sous le nom de PNAgent)	Application Citrix Workspace pour iOS version 23.7.5	-	Dans l'application Citrix Workspace, connectez-vous aux magasins à l'aide de l'URL du magasin plutôt que de l'URL de XenApp Services.
Système d'exploitation iOS version 14	Application Citrix Workspace pour iOS version 23.10.0	Cible : application Citrix Workspace pour iOS 23.12.0	Effectuez la mise à niveau vers la dernière version disponible d'iOS
Système d'exploitation iOS version 13.x	Application Citrix Workspace pour iOS version 22.9.5	Objectif : décembre 2022 et version 22.12.0	Effectuez la mise à niveau vers la dernière version disponible d'iOS
Système d'exploitation iOS versions 11.x et 12.x	Application Citrix Workspace pour iOS version 21.12.0	Objectif : août 2022 et version 22.8.0	Effectuez la mise à niveau vers la dernière version disponible d'iOS

Élément	Abandon annoncé	Supprimé dans	Solution alternative
Système d'exploitation iOS version 10.x	Application Citrix Workspace pour iOS version 21.1.5	Version suivant 21.1.5	Utilisez l'application Citrix Workspace pour iOS version 21.1.5 ou antérieure.

Remarques :

- Les utilisateurs existants de l'application Citrix Workspace sur des versions de plate-forme obsolètes ne peuvent pas effectuer la mise à niveau vers la dernière version (à partir de l'App Store) de l'application Citrix Workspace.
- Les nouveaux utilisateurs de l'application Citrix Workspace sur des versions de plate-forme obsolètes peuvent uniquement télécharger une ancienne version compatible à partir de l'App Store.
- Les utilisateurs de versions de plate-forme obsolètes ne bénéficient pas des nouvelles fonctionnalités ou des correctifs de sécurité fournis avec chaque nouvelle version de l'application Citrix Workspace.