



Applications de productivité mobiles

Contents

Calendrier de publication des applications de productivité mobiles	3
Prise en charge des applications de productivité mobiles	4
Tâches et considérations de l'administrateur	6
Fonctionnalités par plate-forme	16
Citrix Secure Hub	30
Présentation de Secure Mail	51
Citrix Secure Web	52
Citrix QuickEdit pour applications de productivité mobiles	66
ShareConnect	69
Citrix ShareFile Workflows	81
Citrix Files pour Endpoint Management	82
Applications en fin de vie et obsolètes	90
Autoriser l'interaction sécurisée avec les applications Office 365	91

Calendrier de publication des applications de productivité mobiles

December 10, 2018

Les applications de productivité mobiles sont publiées toutes les deux semaines. Bien que les dates exactes puissent changer, nous souhaitons vous aider à planifier à l'avance en vous faisant part de la fréquence de publication. Nous voulons également faciliter la gestion des mises à jour et des déploiements d'applications.

À propos du processus de publication par étapes de Secure Mail et Secure Web

Lorsque de nouvelles versions de Secure Mail et de Secure Web sont disponibles, les versions sont déployées en plusieurs étapes comme indiqué ci-après.

- Pour les utilisateurs d'iOS et d'Android, les mises à jour de Secure Mail et de Secure Web sont disponibles dans l'App Store et Google Play Store pour un pourcentage croissant d'utilisateurs au cours d'une semaine (sept jours).
- Les nouveaux téléchargements de Secure Mail et de Secure Web pour iOS obtiennent la nouvelle version pendant cette semaine. Les nouveaux téléchargements de Secure Mail et de Secure Web pour Android exécuteront la version précédente pendant la semaine, jusqu'à ce que le déploiement de la nouvelle version atteigne 100 % de tous les utilisateurs.
- Certaines fonctionnalités sont déployées pendant cinq jours après la mise en service progressive initiale de sept jours.

Conditions requises pour la gestion des commutateurs de fonctionnalité

Si un problème se produit avec Secure Hub ou Secure Mail en production, nous pouvons désactiver une fonctionnalité affectée dans le code de l'application. Pour ce faire, nous utilisons des commutateurs de fonctionnalité et un service tiers appelé Launch Darkly. Vous n'avez pas besoin d'effectuer des configurations pour activer le trafic vers Launch Darkly, sauf si un pare-feu ou un proxy bloque le trafic sortant. Dans ce cas, vous activez le trafic vers Launch Darkly via des URL ou adresses IP spécifiques, en fonction des exigences de votre stratégie. Pour de plus amples informations sur la prise en charge dans MDX depuis les applications de productivité mobiles 10.6.15 pour l'exclusion des domaines de la tunnellation, consultez la [documentation de MDX Toolkit](#). Pour afficher la liste des questions fréquemment posées sur les commutateurs de fonctionnalité et Launch Darkly, consultez cet [article du centre de connaissances](#).

Important :

Citrix a mis fin à la prise en charge de la distribution d'entreprise des applications de productivité mobiles le 31 décembre 2017. Consultez le [tableau des produits Citrix](#) pour plus d'informations.

Désormais, seule la distribution sur des magasins d'applications publics est prise en charge. Le MDX Toolkit continue à prendre en charge l'encapsulation d'applications d'entreprise tierces pour les développeurs d'applications.

Prise en charge des applications de productivité mobiles

March 1, 2019

Citrix prend en charge les mises à niveau à partir des deux dernières versions des applications de productivité mobiles. Les utilisateurs qui ont activé les mises à jour automatiques recevront la dernière version depuis le magasin d'applications.

Dernières versions de Secure Hub, Secure Mail et Secure Web pour iOS et Android :

- 19.2.0
- 19.1.5

Important :

La version 19.1.6 de Secure Mail est disponible uniquement pour iOS.

- 19.1.0

Systèmes d'exploitation pris en charge

Les dernières versions de Secure Hub, du MDX Toolkit et des applications de productivité mobiles sont compatibles avec la dernière version et les deux versions précédentes de Endpoint Management. Pour plus d'informations, consultez la section [Systèmes d'exploitation pris en charge](#).

La dernière version des applications de productivité mobiles requiert la dernière version de Secure Hub. Assurez-vous de garder Secure Hub à jour.

Appareils pris en charge pour le cryptage MDX

Citrix prend en charge le cryptage MDX avec les marques d'appareils suivantes.

Android

- Note Samsung
- Samsung Galaxy
- Google Pixel
- Motorola

iOS

- Tous les appareils iOS avec une version de système d'exploitation prise en charge dans la liste précédente sont pris en charge pour le cryptage MDX.

Autres considérations et limitations

Secure Mail

- Endpoint Management ne prend pas en charge NetScaler 12.0.41.16 en raison d'un problème avec Secure Ticket Authority (STA) et Secure Mail. Le problème est résolu dans NetScaler 12.0 build 41.22. Pour de plus amples informations et des mises à jour, consultez cet [article du centre de connaissances](#).
- La prise en charge de Secure Mail pour Exchange 2007 et Lotus Notes 8.5.3 a atteint la fin de vie (EOL) le 30 septembre 2017.
- Pour de meilleures performances lors de l'envoi de pièces jointes Citrix Files, les dernières versions de Citrix Files sont recommandées. Citrix Files n'est pas pris en charge pour Windows.
- Pour les environnements IBM Notes, vous devez configurer le serveur IBM Domino Traveler, version 9.0. Pour de plus amples informations, consultez la section Intégration à un serveur Exchange ou un serveur IBM Notes Traveler.

Secure Web

La dernière version d'Android WebView doit être installée sur les appareils. Les utilisateurs peuvent télécharger Android WebView à partir du Google Play Store.

QuickEdit

QuickEdit restera disponible en tant qu'application de productivité mobile. L'état de fin de vie (EOL) ne sera pas appliqué le 1er septembre 2018 comme indiqué précédemment.

Citrix Files

Les utilisateurs accèdent à Citrix Files pour Endpoint Management à partir des magasins d'applications publics après la version 6.5.

ShareConnect

Une condition préalable pour ShareConnect est un ordinateur hôte exécutant Windows 7 (version minimale).

Secure Notes et Secure Tasks

Important :

Secure Notes et Secure Tasks ont atteint la fin de leur cycle de vie le 31 décembre 2018. Pour plus d'informations, voir [Applications en fin de vie et obsolètes](#).

Tâches et considérations de l'administrateur

February 19, 2019

Cet article discute des tâches et des considérations pertinentes pour les administrateurs des applications de productivité mobiles.

Gestion des feature flag

Si un problème se produit avec Secure Hub, Secure Mail ou Secure Web pour iOS et Android en production, nous pouvons désactiver une fonctionnalité affectée dans le code de l'application. Pour ce faire, nous utilisons des commutateurs de fonctionnalité et un service tiers appelé Launch Darkly. Vous n'avez pas besoin d'effectuer des configurations pour activer le trafic vers Launch Darkly, sauf si un pare-feu ou un proxy bloque le trafic sortant. Dans ce cas, vous activez le trafic vers Launch Darkly via des URL ou adresses IP spécifiques, en fonction des exigences de votre stratégie. Pour de plus amples informations sur la prise en charge dans MDX depuis les applications de productivité mobiles 10.6.15 pour l'exclusion des domaines de la tunnellation, consultez la [documentation de MDX Toolkit](#).

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

Activer le trafic vers les URL suivantes

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- firehose.launchdarkly.com

Créer une liste blanche par domaine

Auparavant, nous proposons une liste d'adresses IP à utiliser lorsque les stratégies internes ne requièrent que la liste des adresses IP. Maintenant que Citrix a apporté des améliorations à l'infrastructure, nous supprimons progressivement les adresses IP publiques à compter du 16 juillet. Nous vous recommandons de créer une liste blanche par domaine si possible.

Répertorier les adresses IP dans une liste blanche

Si vous devez répertorier les adresses IP dans la liste blanche, consultez la [liste des adresses IP publiques de Launch Darkly](#) 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, consultez la page de [ressource racine de Launch Darkly](#). Pour plus d'informations sur l'état actuel des modifications de l'infrastructure, consultez la [page d'état de Launch Darkly](#).

Remarque :

Les applications provenant de magasins d'applications publics requièrent une nouvelle installation la première fois que vous les déployez. Il n'est pas possible de mettre à niveau la version encapsulée d'entreprise de l'application vers la version du magasin public.

Grâce à la distribution sur magasins d'applications publics, vous n'avez pas besoin de signer et d'encapsuler des applications développées par Citrix avec le MDX Toolkit. Cela optimise considérablement le processus de déploiement d'applications. Vous pouvez utiliser l'outil MDX Toolkit pour encapsuler des applications tierces ou d'entreprise.

Configuration système requise pour Launch Darkly

- Endpoint Management 10.7 ou version ultérieure.
- Assurez-vous que les applications peuvent communiquer avec les services suivants si le split tunneling sur Citrix ADC est **désactivé** :
 - Lancez le service Darkly. Pour de plus amples informations, consultez cet [article du centre de connaissances](#).
 - Service d'écoute APNs

Magasins d'applications pris en charge

Les applications de productivité mobiles sont disponibles sur l'App Store d'Apple et Google Play. Pour sécuriser et déployer les applications de productivité natives sur les appareils Windows, consultez la section [Stratégie Protection des informations Windows \(WIP\)](#).

En Chine, où Google Play n'est pas disponible, Secure Hub pour Android est disponible sur les magasins d'applications suivants :

- <https://shouji.baidu.com>
- <https://apk.hiapk.com>
- <https://apk.91.com>

Activation de la distribution sur des magasins d'applications publics

1. Téléchargez les fichiers .mdx du magasin public pour iOS et Android depuis la [page de téléchargements de Endpoint Management](#).
2. Chargez les fichiers .mdx sur la console XenMobile. Les versions de magasin public des applications de productivité mobiles sont toujours chargées en tant qu'applications MDX. Ne les chargez pas en tant qu'applications de magasin public sur le serveur. Pour les étapes, voir [Ajouter des applications](#).
3. Modifiez les valeurs par défaut des stratégies en fonction de vos stratégies de sécurité (facultatif).
4. Distribuez ces applications en tant qu'applications requises (facultatif). Cette étape nécessite que votre environnement soit activé pour la gestion des appareils mobiles.
5. Installez les applications sur l'appareil à partir de l'App Store, Google Play ou du magasin d'applications Endpoint Management.
 - Sur Android, l'utilisateur est dirigé vers le Play Store pour installer l'application. Sur iOS, dans les déploiements MDM, l'application s'installe sans que l'utilisateur soit dirigé vers l'App Store.
 - Lorsque l'application est installée à partir de l'App Store ou du Play Store, elle est convertie en application gérée tant que le fichier .mdx correspondant a été chargé sur le serveur. Lors de la transition vers une application gérée, l'application requiert la saisie d'un code PIN Citrix. Lorsque les utilisateurs entrent le code PIN Citrix, Secure Mail affiche l'écran de configuration du compte.
6. Les applications sont accessibles uniquement si vous vous êtes inscrit auprès de Secure Hub et que le fichier .mdx correspondant se trouve sur le serveur. Si l'une de ces conditions n'est pas remplie, les utilisateurs peuvent installer l'application, mais son utilisation sera bloquée.

Si vous utilisez actuellement des applications provenant de Citrix Ready Marketplace sur des magasins d'applications publics, le processus de déploiement vous est déjà familier. Les applications de productivité mobiles adoptent la même approche que la plupart des éditeurs de logiciels. Incorporez le SDK MDX dans l'application pour la préparer à être utilisée dans un magasin public.

Remarque :

Les versions de magasin public de l'application Citrix Files pour iOS et Android sont maintenant universelles. L'application Citrix Files est la même pour les téléphones et les tablettes.

Notifications push Apple

Pour de plus amples informations sur la configuration des notifications push, consultez la section [Configuration de Secure Mail pour les notifications push](#).

Questions fréquemment posées sur les magasins d'applications publics

- Puis-je déployer plusieurs copies de l'application de magasin public à différents groupes d'utilisateurs ? Par exemple, je souhaite déployer des stratégies différentes à différents groupes d'utilisateurs.

Vous devrez charger un fichier .mdx différent pour chaque groupe d'utilisateurs. Toutefois, dans ce cas, un utilisateur ne peut pas appartenir à plusieurs groupes. Si les utilisateurs appartiennent à plusieurs groupes, plusieurs copies de la même application sont attribuées à cet utilisateur. Plusieurs copies d'une application de magasin public ne peuvent pas être déployées sur le même appareil, car l'ID d'application ne peut pas être modifié.

- Puis-je distribuer des applications de magasin public en tant qu'applications requises ?

Oui. La distribution d'applications sur des appareils requiert MDM ; elle n'est pas prise en charge pour les déploiements MAM exclusif.

- Dois-je mettre à jour les stratégies de trafic ou les règles Exchange Server qui sont basées sur l'agent utilisateur ?

Chaînes pour stratégies et règles basées sur l'agent utilisateur par plate-forme :

Important :

Secure Notes et Secure Tasks ont atteint la fin de leur cycle de vie le 31 décembre 2018. Pour plus d'informations, voir [Applications en fin de vie et obsolètes](#).

Android

Application	Serveur	Chaîne agent-utilisateur
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		WorxMail
Citrix Secure Tasks	Exchange	WorxMail
Citrix Secure Notes	Exchange	WorxMail
	Citrix Files	Secure Notes

iOS

Application	Serveur	Chaîne agent-utilisateur
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		com.citrix.browser
Citrix Secure Tasks	Exchange	WorxTasks
Citrix Secure Notes	Exchange	WorxNotes
	Citrix Files	Secure Notes

- Puis-je empêcher la mise à niveau des applications ?

Non. Lorsqu'une mise à jour est publiée sur le magasin d'applications public, les utilisateurs qui ont activé les mises à jour automatiques recevront la mise à jour.

- Puis-je imposer la mise à jour des applications ?

Oui, les mises à niveau sont appliquées par le biais de la stratégie de période de grâce de mise à jour. Cette stratégie est définie lorsque le nouveau fichier .mdx correspondant à la version mise à jour de l'application est chargé sur le serveur Endpoint Management.

- Comment faire pour tester les applications avant de distribuer la mise à jour aux utilisateurs si je ne peux pas contrôler l'échéancier des mises à jour ?

À l'instar du processus pour Secure Hub, les applications sont disponibles à des fins de test sur TestFlight pour iOS durant la période EAR. Pour Android, les applications sont disponibles via le programme bêta Google Play durant la période EAR. Vous pouvez tester les mises à jour d'applications au cours de cette période.

- Que se passe-t-il si je ne mets pas à jour le nouveau fichier .mdx avant que la mise à jour automatique ne soit appliquée aux appareils des utilisateurs ?

L'application mise à jour continue de fonctionner avec l'ancien fichier .mdx. Les nouvelles fonctionnalités qui dépendent d'une nouvelle stratégie ne seront pas activées.

- L'application passera-t-elle en mode géré si Secure Hub est installé ou doit-elle être inscrite ?

Les utilisateurs doivent être inscrits auprès de Secure Hub pour que l'application du magasin public soit activée en tant qu'application gérée (sécurisée par MDX) et utilisable. Si Secure Hub est installé mais que l'utilisateur n'y est pas inscrit, il ne peut pas utiliser l'application de magasin public.

- Ai-je besoin d'un compte de développeur Apple Enterprise pour les applications d'un magasin public ?

Non. Étant donné que Citrix est maintenant responsable de la gestion des certificats et des profils de provisioning pour les applications de productivité mobiles, un compte de développeur Apple Enterprise n'est pas requis pour déployer des applications auprès d'utilisateurs.

- La fin de la distribution d'entreprise s'applique-t-elle à toute application encapsulée que j'ai déployée ?

Non, elle s'applique uniquement aux applications de productivité mobiles : Secure Mail, Secure Web et Citrix Files pour Endpoint Management, QuickEdit et ShareConnect. Toutes les autres applications d'entreprise encapsulées que vous avez déployées qui ont été développées en interne ou par des tiers peuvent continuer à utiliser l'encapsulation d'entreprise. Le MDX Toolkit continuera à prendre en charge l'encapsulation d'applications d'entreprise pour les développeurs d'applications.

- Lors de l'installation d'une application à partir de Google Play, je reçois une erreur Android avec le code d'erreur 505.

Remarque :

La prise en charge d'Android 5.x s'est terminée le 31 décembre 2018.

Il s'agit d'un problème connu avec Google Play et les versions 5.x. d'Android. Si cette erreur se produit, vous pouvez suivre ces étapes pour effacer toute date obsolète sur l'appareil qui empêche l'installation de l'application :

1. Redémarrez la machine.
2. Effacez le cache et les données relatives à Google Play dans les paramètres de l'appareil.
3. En dernier recours, supprimez et rajoutez le compte Google sur votre appareil.

Pour plus d'informations, effectuez une recherche sur ce [site](#) à l'aide des mots clés suivants « Fix Google Play Store Error 505 in Android: Unknown Error Code »

- Bien que l'application soit disponible en production sur Google Play et qu'il n'existe pas de version bêta, pourquoi Bêta s'affiche-t-il toujours après le titre de l'application sur Google Play ?

Si vous faites partie de notre programme Early Access Release, vous verrez toujours cette mention en regard du titre de l'application. Ce nom sert simplement à indiquer le niveau d'accès d'un utilisateur à une application spécifique. La mention Bêta indique que les utilisateurs reçoivent la version la plus récente de l'application disponible. La version la plus récente peut être la dernière version publiée dans un environnement de production ou bêta.

- Après l'installation et l'ouverture de l'application, les utilisateurs voient le message « Application non autorisée », même si le fichier .mdx est présent dans la console Endpoint Management.

Ce problème peut se produire si les utilisateurs installent l'application directement à partir de l'App Store ou de Google Play et que Secure Hub n'a pas été actualisé. Secure Hub doit être actualisé lorsque le délai d'inactivité a expiré. Actualisez les stratégies lorsque les utilisateurs

ouvrent Secure Hub et se réauthentifient. L'application est autorisée la prochaine fois qu'elle est ouverte par les utilisateurs.

- Ai-je besoin d'un code d'accès pour utiliser l'application ? Un message m'invite à entrer un code d'accès lors de l'installation de l'application à partir de l'App Store ou du Play Store.

Si vous êtes invité à entrer un code d'accès, c'est que vous ne vous êtes pas inscrit auprès de Endpoint Management via Secure Hub. Inscrivez-vous avec Secure Hub et assurez-vous que le fichier .mdx pour l'application est déployé sur le serveur. Assurez-vous également que l'application peut être utilisée. Le code d'accès est limité à un usage interne Citrix. Les applications requièrent un déploiement Endpoint Management pour être activées.

- Puis-je déployer les applications d'un magasin public iOS via le programme VPP ou DEP ?

Endpoint Management est optimisé pour la distribution VPP d'applications de magasin public non MDX. Bien que vous puissiez distribuer les applications du magasin public Endpoint Management avec VPP, le déploiement ne sera pas optimal tant que nous n'aurons pas apporté d'améliorations à Endpoint Management et au magasin Secure Hub pour résoudre les limites. Pour obtenir une liste des problèmes connus avec le déploiement d'applications du magasin public Endpoint Management via VPP et leurs solutions potentielles, consultez cet article dans le [Centre de connaissances Citrix](#).

Stratégies MDX pour les applications de productivité mobiles

Les stratégies MDX vous permettent de configurer les paramètres que Endpoint Management applique. Les stratégies couvrent les paramètres d'authentification, de sécurité sur l'appareil, d'exigences de réseau et d'accès, de cryptage, d'interaction avec l'application, de restrictions applicatives et plus. De nombreuses stratégies MDX s'appliquent à toutes les applications de productivité mobiles ; certaines stratégies sont spécifiques à l'application.

Les fichiers de stratégie sont fournis en tant que fichiers .mdx pour les versions de magasin public des applications de productivité mobiles. Vous pouvez également configurer des stratégies dans la console Endpoint Management lorsque vous ajoutez une application.

Pour obtenir une description complète des stratégies MDX, consultez les articles suivants de cette section :

- [Synopsis des stratégies MDX pour les applications de productivité mobiles](#)
- [Stratégies MDX pour les applications de productivité mobiles pour Android](#)
- [Stratégies MDX pour les applications de productivité mobiles pour iOS](#)

Les sections suivantes décrivent les stratégies MDX liées aux connexions utilisateur.

Connexions utilisateur au réseau interne

Les connexions qui sont tunnelisées sur le réseau interne peuvent utiliser un tunnel VPN complet ou une variante d'un VPN sans client, appelé *Navigation sécurisée*. La stratégie Mode VPN préféré contrôle ce comportement. Par défaut, les connexions utilisent la navigation sécurisée, ce qui est recommandé pour les connexions qui nécessitent l'authentification unique (SSO). Le paramètre Tunnel VPN complet est recommandé pour les connexions qui utilisent des certificats clients ou SSL de bout en bout pour une ressource dans le réseau interne ; il gère les protocoles faisant appel à TCP et peut être utilisé avec des ordinateurs Windows et Mac, ainsi qu'avec des appareils iOS et Android.

Secure Web pour iOS et Android prend en charge l'utilisation d'un fichier PAC avec un déploiement de tunnel VPN complet, si vous utilisez Citrix ADC pour l'authentification proxy.

La stratégie Autoriser le basculement vers le mode VPN permet le basculement automatique entre les modes de tunnel VPN complet et de navigation sécurisée si nécessaire. Cette stratégie est désactivée par défaut. Lorsque cette stratégie est activée, une demande réseau qui a échoué en raison d'une demande d'authentification qui ne peut pas être traitée dans le mode VPN préféré est de nouveau tentée dans un autre mode. Par exemple, les contestations de serveur pour les certificats clients peuvent utiliser le mode Tunnel VPN complet, mais pas le mode Navigation sécurisée. De même, les demandes d'authentification HTTP sont plus susceptibles d'être traitées avec l'authentification unique (SSO) lorsqu'elles utilisent le mode Navigation sécurisée.

Restrictions d'accès réseau

La stratégie Accès réseau spécifie si des restrictions sont imposées sur l'accès réseau. Par défaut, l'accès à Secure Mail est illimité, ce qui signifie qu'aucune restriction n'est imposée sur l'accès réseau ; les applications ont un accès illimité aux réseaux auxquels l'appareil est connecté. Par défaut, l'accès à Secure Web est tunnelisé vers le réseau interne, ce qui signifie qu'un tunnel VPN par application vers le réseau interne est utilisé pour tous les accès réseau et que les paramètres de split tunneling de Citrix ADC sont utilisés. Vous pouvez également spécifier un accès bloqué pour que l'application fonctionne comme si l'appareil n'avait pas de connexion réseau.

Ne bloquez pas la stratégie Accès réseau si vous voulez autoriser les fonctionnalités telles que AirPrint, iCloud et Facebook et les API Twitter.

La stratégie Accès réseau interagit avec la stratégie Services réseau d'arrière-plan. Pour de plus amples informations, consultez la section [Intégration à un serveur Exchange ou un serveur IBM Notes Traveler](#).

Propriétés du client Endpoint Management

Les propriétés du client contiennent des informations qui sont fournies directement à Secure Hub sur les appareils des utilisateurs. Les propriétés du client sont situées dans la console Endpoint Manage-

ment dans **Paramètres > Client > Propriétés du client**.

Les propriétés du client sont utilisées pour configurer des paramètres tels que ceux qui suivent :

Mise en cache du mot de passe utilisateur

La mise en cache du mot de passe de l'utilisateur permet la mise en cache locale du mot de passe Active Directory de l'utilisateur sur l'appareil mobile. Lorsque vous activez la mise en cache du mot de passe de l'utilisateur, les utilisateurs sont invités à créer un code PIN ou code secret Citrix.

Délai d'inactivité

Le délai d'inactivité définit la durée en minutes pendant laquelle les utilisateurs peuvent laisser leurs appareils inactifs et accéder à une application sans être invité à entrer un code PIN ou code secret Citrix. Pour activer ce paramètre pour une application MDX, vous devez définir la stratégie Code secret d'application sur **Activé**. Si la stratégie Code secret d'application est définie sur **Désactivé**, les utilisateurs sont redirigés vers Secure Hub pour effectuer une authentification complète. Lorsque vous modifiez ce paramètre, la valeur prend effet la prochaine fois que les utilisateurs sont invités à s'authentifier.

Authentification par code PIN Citrix

Le code PIN Citrix simplifie l'expérience d'authentification pour l'utilisateur. Le code PIN est utilisé pour sécuriser un certificat client ou enregistrement des informations d'identification Active Directory localement sur leur appareil. Si vous configurez des paramètres de code PIN, l'expérience de connexion de l'utilisateur est la suivante :

1. Lorsque les utilisateurs démarrent Secure Hub pour la première fois, ils sont invités à entrer un code PIN, qui place les informations d'identification Active Directory en mémoire cache.
2. Lorsque les utilisateurs démarrent ensuite une application de productivité mobile telle que Secure Mail, ils entrent le code PIN et se connectent.

Vous pouvez utiliser les propriétés du client pour activer l'authentification par code PIN, spécifier le type de code PIN, et spécifier les exigences en matière de force, longueur et modification du code PIN.

Authentification par empreinte digitale ou Touch ID

L'authentification par empreinte digitale, également connue sous le nom d'authentification Touch ID, pour les appareils iOS est une alternative à l'utilisation d'un code PIN Citrix. Cette fonctionnalité est

utile lorsque des applications encapsulées (à l'exception de Secure Hub) requièrent une authentification hors connexion, par exemple après expiration du délai d'inactivité. Vous pouvez activer cette fonction dans les scénarios d'authentification suivants :

- Code PIN Citrix + certificat client
- Code PIN Citrix + mot de passe Active Directory mis en cache
- Code PIN Citrix + certificat client et mot de passe Active Directory mis en cache
- Le code PIN Citrix est désactivé

Si l'authentification par empreinte digitale échoue ou si l'utilisateur annule l'invite d'authentification par empreinte digitale, les applications encapsulées utilisent l'authentification par code PIN Citrix ou par mot de passe Active Directory.

Exigences requises par l'authentification par empreinte digitale

- Appareils iOS (version minimum 8.1) prenant en charge l'authentification par empreinte digitale et disposant d'au moins une empreinte digitale configurée.
- L'entropie utilisateur doit être désactivée.

Pour configurer l'authentification par empreinte digitale

Important :

Si l'entropie utilisateur est activée, la propriété Enable Touch ID Authentication est ignorée. L'entropie utilisateur est activée à l'aide de la clé Encrypt secrets using Passcode.

1. Dans la console Endpoint Management, accédez à **Paramètres > Client > Propriétés du client**.
2. Cliquez sur **Ajouter**.

3. Ajoutez la clé **ENABLE_TOUCH_ID_AUTH**, définissez sa **valeur** sur **Vrai**, et définissez le nom de la stratégie sur **Activer l'authentification par empreinte digitale**.

Après avoir configuré l'authentification par empreinte digitale, les utilisateurs n'ont pas besoin de réinscrire leurs appareils.

Pour plus d'informations sur la clé Encrypt secrets using Passcode et les propriétés client en général, consultez l'article Endpoint Management sur les [propriétés du client](#).

Fonctionnalités par plate-forme

February 19, 2019

Les tableaux suivants dressent la liste des fonctionnalités des applications de productivité mobiles Citrix. **X** indique que la fonctionnalité est disponible pour cette plate-forme. Pour les fonctionnalités dans QuickEdit, consultez [l'article Citrix QuickEdit](#).

Citrix Secure Hub

Fonctionnalité	iOS	Android
Connexion pour s'authentifier	X	X
Surveiller le respect des stratégies	X	X

Applications de productivité mobiles

Fonctionnalité	iOS	Android
Accéder aux applications et bureaux	X	X
Applications et bureaux HDX	X	X
Créer et envoyer des journaux des problèmes	X	X
Joindre des pièces jointes à des journaux	X	X
Contacteur le bureau d'assistance directement depuis l'application	X	X
Contacteur l'assistance Citrix depuis l'application	X	X
Collecte et analyse des échecs	X	X
Authentification en mode hors connexion	X	X
Envoyer les journaux avec Citrix Secure Mail	X	X
Google Analytics	X	X
Mode portrait et paysage	X	X
Guide intégré sur l'approbation des applications	X	X
Si inscrit avec e-mail, inscription automatique dans Secure Mail (MAM uniquement)	X	X
Authentification hors connexion Touch ID	X	X
S'inscrire avec des informations d'identification dérivées	X	
Authentification biométrique		X

Applications de productivité mobiles

Fonctionnalité	iOS	Android
Utilisation du magasin d'applications Workspace	X	X

Citrix Secure Mail

Fonctionnalité	iOS	Android
Productivité de la messagerie		
Envoyer, recevoir, répondre, répondre à tous, transférer un e-mail	X	X
Créer, modifier, supprimer les brouillons	X	X
Marquer les messages	X	X
Marquer comme non lu	X	X
Afficher tous les dossiers et sous-dossiers	X	X
Enregistrer automatiquement les brouillons lorsque l'application est placée en arrière-plan	X	X
Envoyer un courrier vers une note avec Citrix Secure Notes	X	X
Important : Secure Notes a atteint la fin de son cycle de vie le 31 décembre 2018. Pour plus d'informations, voir Applications en fin de vie et obsolètes .		
Rechercher le courrier (localement et sur le serveur)	X	X

Fonctionnalité	iOS	Android
Sélectionner une période de synchronisation des messages (jusqu'à 1 mois ou Tous les messages)	X	X
Visualiser les messages non lus	X	X
Sécuriser l'affichage/la lecture des images, de la vidéo et de l'audio (dans les pièces jointes)	X	X
Pièces jointes multiples	X	X
Répondre et transférer les pièces jointes	X	X
Joindre des fichiers à partir de Citrix Files	X	X
Joindre des fichiers à partir de zones restreintes Citrix Files et de connecteurs	X	X
Référentiel de pièces jointes	X	X
Édition de texte enrichi	X	X
Notification par e-mail avec l'objet et l'aperçu sur l'écran de verrouillage	X	X
Répondre à et supprimer des messages et des invitations depuis l'écran de notification	X	
Attacher ou prendre une photo	X	X
Sélectionner plusieurs messages	X	X
Télécharger les pièces jointes	X	X
Charger des images en ligne	X	X
Triage rapide	X	X

Applications de productivité mobiles

Fonctionnalité	iOS	Android
Envoyer, recevoir, ouvrir et enregistrer les pièces jointes au format .zip	X	X
Modes portrait et paysage	X ; pour les vues de diffusion, de lecture de messages, de composition, de calendrier et de contacts	X : pour les vues de lecture de messages et de composition uniquement
Texte collé conserve la mise en forme	X	X
SMS depuis les contacts	X	X
FaceTime depuis les contacts	X	
Messages non envoyés en raison de problèmes de connectivité ou d'une boîte aux lettres saturée dans la boîte d'envoi	X	X
Bulle de dossiers récents		X
Tirer vers le bas pour actualiser la messagerie	X	X
Horodatage de la dernière actualisation	X	X
Balayage vers la gauche pour les actions sur les messages	X	X
Prise en charge de Microsoft Exchange et IBM Notes Traveler	X	X
Toucher pour actualiser la messagerie, le calendrier et les contacts	X	X
Respecter l'accessibilité à l'appareil/les paramètres de taille de police dans l'affichage des messages	X	X
Signature et cryptage S/MIME	X	X

Applications de productivité mobiles

Fonctionnalité	iOS	Android
Importation de certificats S/MIME par e-mail	X	X
S/MIME, intégration d'Intercede	X	
S/MIME, intégration d'Entrust	X	
Protection IRM Microsoft pour le corps du message	X	X
Notifications Push	X	X
Les notifications Push vers la boîte de réception mettent automatiquement à jour tous les dossiers, y compris le calendrier	X	
Ouvrir des documents Office 365	X	X
Actions tactiles 3D	X	
Icônes contextuelles sur l'écran de verrouillage	X	X
Rechercher des dossiers	X	X
Dossier de messagerie VIP	X	X
Prise en charge du type dynamique	X	X
Conserver les dossiers développés	X	X
Marqueurs de classification de message	X	X
Vérification de l'orthographe	X	
Attacher la dernière photo prise	X	X
Aperçu des URL	X	X
Ouvrir les liens Citrix Files dans Citrix Files	X	X

Applications de productivité mobiles

Fonctionnalité	iOS	Android
Prise en charge des fichiers .pass	X	
Sélectionner plusieurs e-mails en mode de recherche	X	X
Insérer des images	X	X
Mise à niveau vers Exchange ActiveSync (EAS) version 16	X	X
Empêcher les utilisateurs d'utiliser des domaines inconnus ou personnels	X	
Prise en charge des écrans extra-large		X
Configurer plusieurs comptes Exchange	X	X
Balayer vers la gauche ou la droite pour plus d'actions	X	X
Crypter les réponses à ou les transferts d'e-mails cryptés	X	
Imprimer des e-mails et des images insérées	X	
Vous pouvez utiliser Lignes d'aperçu dans les paramètres pour configurer le nombre de lignes qui s'affichent en tant qu'aperçu dans le corps d'un e-mail dans la vue de la boîte aux lettres.	X	
Prise en charge des e-mails « responsive ».	X	X
Aperçu des pièces jointes dans l'application (MS Office ou images).	X	X
Groupes de contacts personnels	X	X

Fonctionnalité	iOS	Android
Migrer des noms d'utilisateur vers des adresses e-mail (UPN)	X	X
Signaler les e-mails de phishing	X	X
Authentification moderne (OAuth)	X	X
Imprimer les pièces jointes	X	
Android Enterprise (Android for Work)	X	
Signatures au format RTF	X	X
Notifications push enrichies	X	
Flux	X	X
Améliorations au niveau de la pièce jointe photo	X	X
Notifications de groupe	X	
Intégration de Slack (Aperçu)	X	X
Flux de manager	X	
Calendrier		
Vues du jour, de la semaine, du mois et de l'agenda	X	X
Rappels détaillés sur l'écran de verrouillage	X	X
Synchronisation pour six mois	X	X
Définir des événements comme privés	X	X
Accéder à l'heure avant le premier événement	X	
Options d'actualisation manuelles	X	X
Définir des rappels	X	X

Fonctionnalité	iOS	Android
Tapoter pour mapper l'adresse	X	X
Jours de la semaine	X	X
Prise en charge du type dynamique	X	X
Marqueurs classification de sécurité	X	X
Appuis longs sur les adresses	X	
Définir le jour de début de la semaine	X	X
Focus sur la semaine de la date sélectionnée	X	
Date actuelle toujours mise en surbrillance	X	X
Pièces jointes au calendrier à partir du référentiel de pièces jointes	X	X
Prise en charge des calendriers personnels	X	X
Afficher les conflits avec les événements de calendrier personnel		X
Imprimer des événements de calendrier	X	
Appuyer sur des numéros de téléphone et des adresses Web dans une ligne d'objet de calendrier	X	
Rechercher dans le calendrier	X	
Réunions		
Répondre, répondre à tous, transférer les réunions	X	X
Vue de l'organisateur des réponses aux invitations	X	X

Fonctionnalité	iOS	Android
Vue de l'organisateur de la disponibilité des invités avec suggestions de disponibilité	X	X
Toucher pour participer à des réunions en ligne. Remarque : pour WebEx et Lync, vous devez configurer des stratégies dans Citrix Endpoint Management pour activer ces applications.	X	X
Toucher pour participer à des conférences audio	X	X
Planifier une réunion en ligne, une conférence audio dans une nouvelle invitation	X	X
Ajouter des liens ShareFile aux nouvelles invitations	X	X
Transférer les invitations avec pièces jointes	X	X
Toucher pour envoyer un e-mail « en retard »	X	X
Toucher pour répondre à l'organisateur d'une réunion	X	X
Toucher pour répondre à toutes les invitations à une réunion	X	X
Toucher pour répondre à tous les invités à une réunion	X	X
Toucher pour répondre à tous les invités à une réunion avec pièces jointes	X	X
Se connecter à GoToMeeting	X	X
Répondre à des invitations depuis l'écran de notification ou de verrouillage	X	X

Applications de productivité mobiles

Fonctionnalité	iOS	Android
Se connecter à des réunions WebEx ou Lync	X	X
Masquer les événements déclinés	X	X
Afficher plus de 3 événements à la fois	X	X
Aperçu rapide de l'état des invités	X	X
Supprimer, répondre, répondre à tous, ajouter des commentaires pour les événements annulés	X	X
Afficher le nom de l'organisateur sur les invitations transférées	X	X
Appareils partagés	X	X
Rejoindre les réunions Skype Entreprise	X	X
Répondre aux notifications de réunion avec les options Accepter, Décliner et Provisoire	X	X
Répondre aux notifications de message avec les options Répondre et Supprimer	X	
Contacts		
Informations de contact détaillées (recherche GAL)	X	X
Exporter et synchroniser les contacts Secure Mail vers les contacts locaux	X	X
Contacts : favori et catégorie		X
Contrôler quels champs des contacts sont exportés	X	X

Fonctionnalité	iOS	Android
Informations de contact non Secure Mail	X	X
Prise en charge du type dynamique	X	X
Marquer les contacts comme VIP	X	X
Partager des contacts avec .vcards	X	X
Afficher les contacts avec pression longue		X
Exporter les contacts, même si le compte de messagerie native existe	X	X
Afficher les dossiers et sous-dossiers	X	
Paramètres configurés sur l'appareil		
Prise en charge iMessage	X	
Options avancées pour contrôler les notifications	X	X
Contrôle de notification de verrouillage	X	X
Sons de notification de la messagerie et du calendrier	X	X
Actualiser automatiquement les dossiers	X	X
Définir les notifications d'absence du bureau internes et externes	X	X
Demander avant de supprimer	X	X
Conversation en thread ou vues chronologiques	X	X

Applications de productivité mobiles

Fonctionnalité	iOS	Android
Charger des pièces jointes via le Wi-Fi	X	X
Donner la valeur par défaut aux pièces jointes de charge sur un réseau Wi-Fi	X	X
Définir la période de synchronisation des e-mails	X	X
Synchronisation illimitée/synchroniser tous les e-mails		X
Définir la signature électronique	X	X
Liste des contacts par prénom ou nom	X	X
Avance automatique		X
Mon fuseau horaire		X
Modèles de réponse rapide		X
Fréquence de configuration de push des e-mails		X
Exporter/importer les paramètres	X	X
Toucher le bouton de retour de l'appareil pour ignorer les options du bouton d'action flottant		X

Citrix Secure Web

Fonctionnalité	iOS	Android
Télécharger un fichier	X	X
Ajouter des favoris	X	X
Effacer les noms et mots de passe utilisateur enregistrés	X	X

Applications de productivité mobiles

Fonctionnalité	iOS	Android
Supprimer le cache/l'historique/les cookies	X	X
Bloquer les fenêtres contextuelles	X	X
Enregistrer les pages hors connexion	X	X
Rechercher dans la barre d'adresses	X	X
Ouvrir les éléments téléchargés à partir des notifications	X	X
Mots de passe enregistrés automatiquement	X	X
Prise en charge des proxys		
Proxies d'entreprise	X	X
Adresse URL des listes noires et blanches	X	X
Historique	X	X
Page d'accueil par défaut	X	X
Onglets	X	X
Push des signets	X	X
Bloquer capture d'écran		X
Rechercher dans la page actuelle	X	X
Actions tactiles 3D	X	
Appareils partagés	X	X
Protection contre la falsification des fichiers sur les appareils partagés	X	
Exporter/importer les paramètres	X	X
Mode portrait et paysage	X	X

Fonctionnalité	iOS	Android
Android Enterprise (Android for Work)		X
Tirer vers le bas pour actualiser le contenu sur l'écran	X	X

Citrix Secure Hub

March 1, 2019

Citrix Secure Hub est le panneau de lancement des applications de productivité mobiles. Les utilisateurs inscrivent leurs appareils dans Secure Hub pour accéder à l'App Store. Depuis l'App Store, ils peuvent ajouter des applications de productivité mobiles développées par Citrix ainsi que des applications tierces.

Vous pouvez télécharger Secure Hub et d'autres composants depuis la [page des téléchargements de Citrix Endpoint Management](#).

Pour connaître la configuration système requise pour Secure Hub et pour les applications de productivité mobiles, consultez la section [Configuration système requise](#).

Nouveautés de cette version

Secure Hub 19.2.0

Cette version inclut des améliorations de performance et des corrections de bogues.

Nouveautés dans les versions précédentes

Secure Hub 19.1.5

Secure Hub pour Android Enterprise prend désormais en charge les stratégies suivantes :

- **Stratégie Wi-Fi.** La stratégie Wi-Fi prend en charge Android Enterprise désormais. Pour de plus amples informations sur cette stratégie, consultez la section [Stratégie d'appareil Wi-Fi].(/fr-fr/citrix-endpoint-management/policies/wifi-policy.html)
- **Stratégie XML personnalisé.** La stratégie XML personnalisé prend en charge Android Enterprise désormais. Pour plus d'informations sur cette stratégie, consultez [Stratégie XML personnalisé].(/fr-fr/citrix-endpoint-management/policies/custom-xml-policy.html)

- **Stratégie de fichiers.** Vous pouvez ajouter des fichiers de script dans Citrix Endpoint Management pour exécuter des fonctions sur les appareils Android Enterprise. Pour de plus amples informations sur cette stratégie, consultez la section [Stratégie de fichiers].(/fr-fr/citrix-endpoint-management/policies/files-policy.html)

Secure Hub 19.1.0

Secure Hub présente de nouvelles polices et couleurs ainsi que d'autres améliorations de l'interface utilisateur. Cette nouvelle mise en forme vous offre une expérience utilisateur enrichie tout en s'alignant étroitement sur l'esthétique de la marque Citrix à travers notre suite complète d'applications de productivité mobile.

Secure Hub 18.12.0

Cette version inclut des améliorations de performance et des corrections de bogues.

Secure Hub 18.11.5

- **Paramètres de stratégie de restrictions pour Android Enterprise.** Les nouveaux paramètres de la stratégie Restrictions permettent aux utilisateurs d'accéder aux fonctionnalités suivantes sur les appareils Android Enterprise : barre d'état, Keyguard sur l'écran de verrouillage, gestion de compte, partage d'emplacement et maintien de l'écran allumé pour les appareils Android Enterprise. Pour plus d'informations, consultez la section [Stratégies de restrictions](#).

Secure Hub 18.10.5 à 18.11.0 inclut des corrections de bugs et des améliorations des performances.

Secure Hub 18.10.0

- **Prise en charge du mode Samsung DeX :** Samsung DeX permet aux utilisateurs de connecter des appareils compatibles KNOX à un écran externe pour utiliser des applications, consulter des documents et regarder des vidéos sur une interface de type PC. Pour plus d'informations sur la configuration matérielle et logicielle requise pour Samsung DeX et la configuration de Samsung DeX, voir [Comment fonctionne Samsung DeX](#).

Pour configurer les fonctionnalités du mode Samsung DeX dans Citrix Endpoint Management, mettez à jour la stratégie Restrictions pour Samsung KNOX. Pour plus d'informations, voir **Paramètres Samsung KNOX** dans [Stratégie de restrictions](#).

- **Prise en charge d'Android SafetyNet :** vous pouvez configurer Endpoint Management pour utiliser la fonctionnalité **Android SafetyNet** permettant d'évaluer la compatibilité et la sécurité

des appareils Android sur lesquels Secure Hub est installé. Les résultats peuvent être utilisés pour déclencher des actions automatisées sur les appareils. Pour plus d'informations, voir [Android SafetyNet](#).

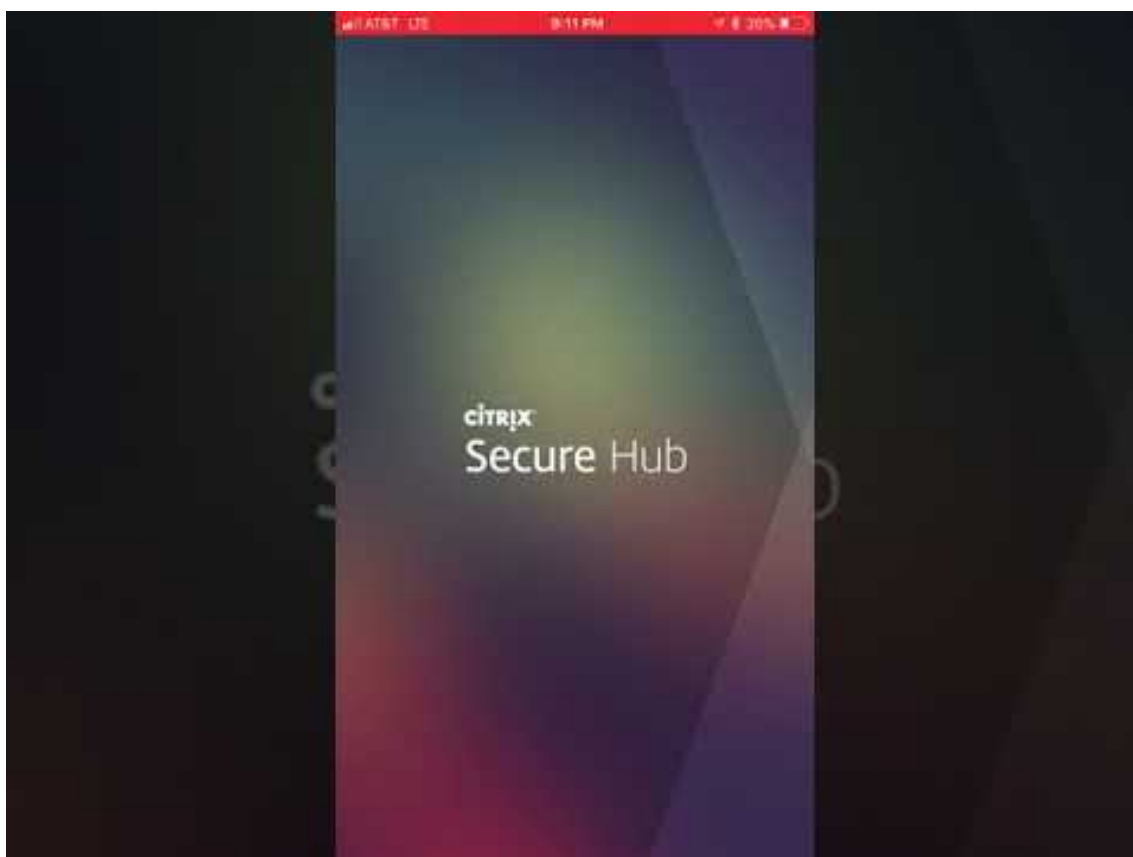
- **Empêcher l'utilisation de l'appareil photo pour les appareils Android Enterprise** : le nouveau paramètre **Autoriser l'utilisation de l'appareil photo** de la stratégie de restrictions vous permet d'empêcher les utilisateurs d'utiliser l'appareil photo sur leurs appareils Android Enterprise. Pour plus d'informations, consultez la section [Stratégies de restrictions](#).

Secure Hub 10.8.60 à 18.9.0

Corrections de bugs et améliorations des performances.

Secure Hub 10.8.60

- Prise en charge de la langue polonaise.
- Prise en charge de Android P.
- Prise en charge de l'utilisation du magasin d'applications Workspace.
Lors de l'ouverture de Secure Hub, les utilisateurs ne voient plus le magasin Secure Hub. Un bouton **Ajouter des applications** permet aux utilisateurs d'accéder au magasin d'applications Workspace. La vidéo suivante montre un appareil iOS effectuant une inscription à Citrix Endpoint Management à l'aide de l'application Citrix Workspace.



Important :

cette fonctionnalité est disponible uniquement pour les nouveaux clients. Nous ne prenons pas en charge la migration des clients existants pour le moment.

Pour utiliser cette fonctionnalité, configurez les éléments suivants :

- Activez les stratégies Mise en cache du mot de passe et Authentification par mot de passe. Pour de plus amples informations sur la configuration de ces stratégies, veuillez consulter la section [Synopsis des stratégies MDX pour les applications de productivité mobiles](#).
- Configurez l'authentification Active Directory en tant qu'AD ou AD+Cert. Nous prenons en charge ces deux modes. Pour plus d'informations sur la configuration de l'authentification, consultez [Authentification domaine ou domaine + jeton de sécurité](#).
- Activez l'intégration de Workspace pour Endpoint Management. Pour plus d'informations sur l'intégration de Workspace, consultez la section [Configuration de l'espace de travail](#).

Important :

Une fois cette fonctionnalité activée, le SSO Citrix Files se produit via Workspace et non Endpoint Management (anciennement XenMobile). Nous vous recommandons de désactiver l'intégration de Citrix Files dans la console Endpoint Management avant d'activer l'intégration de Workspace.

Secure Hub 10.8.55

- Possibilité de transmettre un nom d'utilisateur et un mot de passe aux portails Google Zero Touch et Samsung KNOX Mobile Environment (KME) à l'aide du fichier JSON de configuration. Pour de plus amples informations, consultez la section [Inscription en bloc Samsung KNOX](#).
- Lorsque vous activez le certificate pinning, les utilisateurs ne peuvent pas s'inscrire auprès de Endpoint Management avec un certificat auto-signé. Si les utilisateurs tentent de s'inscrire auprès de Endpoint Management avec un certificat auto-signé, ils sont avertis que le certificat n'est pas approuvé.

Secure Hub 10.8.25 : Secure Hub pour Android prend en charge les périphériques Android P.

Remarque :

Avant la mise à niveau vers la plateforme Android P : assurez-vous que votre infrastructure de serveurs est conforme aux certificats de sécurité ayant un nom d'hôte correspondant dans l'extension SAN (autre nom de l'objet). Pour vérifier un nom d'hôte, le serveur doit présenter un certificat avec un SAN correspondant. Les certificats qui ne contiennent pas de SAN correspondant au nom d'hôte ne sont plus approuvés. Pour plus de détails, consultez l'article du site Android Developer sur les [modifications de comportement d'Android P](#).

Mise à jour de Secure Hub pour iOS le 19 mars 2018 : Secure Hub version 10.8.6 pour iOS est disponible pour résoudre un problème avec la stratégie d'application VPP. Pour de plus amples informations, consultez cet [article du centre de connaissances Citrix](#).

Secure Hub 10.8.5 : prise en charge de Secure Hub pour Android en mode COSU pour Android Work (Android for Work). Pour de plus amples informations, consultez la [documentation Citrix Endpoint Management](#).

Administration de Secure Hub

Vous pouvez effectuer la plupart des tâches d'administration liées à Secure Hub lors de la configuration initiale de Endpoint Management. Pour mettre Secure Hub à la disposition des utilisateurs, pour iOS et Android, chargez Secure Hub sur l'App Store iOS et sur le Google Play Store.

Secure Hub actualise aussi la plupart des stratégies MDX stockées dans Endpoint Management pour les applications installées lorsque la session Citrix Gateway d'un utilisateur se renouvelle après l'authentification auprès de Citrix Gateway.

Important :

Les modifications apportées aux stratégies suivantes requièrent qu'un utilisateur supprime et réinstalle l'application pour appliquer la stratégie mise à jour : Groupe de sécurité, Activer le cryptage et Serveur Exchange Secure Mail.

Code PIN Citrix

Vous pouvez configurer l'application Secure Hub pour utiliser le code PIN Citrix, une fonctionnalité de sécurité activée dans la console Endpoint Management dans **Paramètres > Propriétés du client**. Le paramètre nécessite que les utilisateurs d'appareils mobiles inscrits se connectent à Secure Hub et activent les applications MDX encapsulées à l'aide d'un numéro d'identification personnel (PIN).

Cette fonctionnalité de code PIN Citrix simplifie l'expérience d'authentification utilisateur lors de la connexion à des applications encapsulées sécurisées. Les utilisateurs n'ont pas besoin d'entrer d'autres informations d'identification de manière répétée telles que leur nom d'utilisateur et mot de passe Active Directory.

Les utilisateurs qui se connectent à Secure Hub pour la première fois doivent entrer leur nom d'utilisateur et mot de passe Active Directory. Lors de la connexion, Secure Hub enregistre les informations d'identification Active Directory ou un certificat client sur la machine utilisateur et invite l'utilisateur à entrer un code PIN. Lorsque les utilisateurs se connectent de nouveau, ils entrent le code PIN pour accéder à leurs applications Citrix et au magasin en toute sécurité, jusqu'à ce que la prochaine période d'inactivité prenne fin pour la session utilisateur active. Les propriétés client associées vous permettent de crypter des secrets à l'aide du code PIN, de spécifier le type de code secret pour le code PIN et de spécifier les exigences en matière de force et longueur du code PIN. Pour de plus amples informations, consultez [Propriétés du client](#).

Lorsque l'authentification par empreinte digitale est activée, les utilisateurs peuvent se connecter à l'aide d'une empreinte digitale lorsque l'authentification hors connexion est requise en raison de l'inactivité de l'application. Les utilisateurs doivent toujours entrer un code PIN lorsqu'ils se connectent pour la première fois à Secure Hub, qu'ils redémarrent l'appareil et après l'expiration du délai d'inactivité. Pour plus d'informations sur l'activation de l'authentification par empreinte digitale, voir [Authentification par empreinte digitale ou Touch ID](#).

Certificate pinning

Secure Hub pour iOS et Android prend en charge le certificate pinning ou SSL pinning. Cette fonctionnalité s'assure que le certificat signé par votre entreprise est utilisé lorsque les clients Citrix communiquent avec Endpoint Management, ce qui empêche les connexions provenant de clients vers Endpoint Management lorsque l'installation d'un certificat racine sur l'appareil compromet la session SSL. Lorsque Secure Hub détecte que des modifications ont été apportées à la clé publique du serveur, Secure Hub refuse la connexion.

À partir d'Android N, le système d'exploitation n'autorise plus les autorités de certification (CA) ajoutées par l'utilisateur. Citrix recommande d'utiliser une autorité de certification racine publique à la place d'une autorité de certification ajoutée par un utilisateur.

Les utilisateurs qui effectuent une mise à niveau vers Android N peuvent rencontrer des problèmes s'ils utilisent des autorités de certification privées ou auto-signées. Les connexions sur les appareils Android N s'interrompent dans les cas suivants :

- Autorités de certification privées/auto-signées et l'option Autorité de certification de confiance requise pour l'option Endpoint Management est **activée**. Pour de plus amples informations, consultez la section [Détection automatique Endpoint Management](#).
- Autorités de certification privées/auto-signées et le service de découverte automatique (ADS) ne sont pas accessibles. En raison de problèmes de sécurité, lorsque le service ADS n'est pas accessible, l'option Autorité de certificat de confiance est **activée** même si elle a été **désactivée** initialement.

Avant d'inscrire des périphériques ou de mettre à niveau Secure Hub, envisagez d'activer le certificate pinning. L'option est **désactivée** par défaut et gérée par le service ADS (Endpoint Management Auto Discovery Service). Lorsque vous activez le certificate pinning, les utilisateurs ne peuvent pas s'inscrire auprès de Endpoint Management avec un certificat auto-signé. Si les utilisateurs tentent de s'inscrire auprès avec un certificat auto-signé, ils sont avertis que le certificat n'est pas approuvé. L'inscription échoue si les utilisateurs n'acceptent pas le certificat.

Pour utiliser le certificate pinning, demandez à Citrix de charger les certificats sur le serveur ADS Citrix. Ouvrez un ticket de support technique à l'aide du [portail d'assistance Citrix](#). Fournissez ensuite les informations suivantes :

- Le domaine contenant les comptes avec les utilisateurs s'inscrivent.
- Le nom de domaine complet (FQDN) de Endpoint Management.
- Le nom de l'instance Endpoint Management. Par défaut, le nom de l'instance est zdm et est sensible à la casse.
- Le type d'ID utilisateur, qui peut être UPN ou E-mail. Le paramètre par défaut est UPN.
- Le port utilisé pour l'inscription iOS si vous avez modifié le numéro de port par défaut 8443.
- Le port sur lequel le serveur Endpoint Management accepte les connexions si vous avez modifié le numéro de port par défaut 443.
- L'adresse URL complète de votre boîtier Citrix Gateway.
- Si vous le souhaitez, une adresse e-mail pour votre administrateur.
- Les certificats au format .pem que vous voulez ajouter au domaine.
- Comment gérer les certificats de serveur existants : faut-il supprimer l'ancien certificat de serveur immédiatement (car il est compromis) ou continuer à prendre en charge l'ancien certificat de serveur jusqu'à son expiration.

Votre ticket de support technique est mis à jour lorsque vos informations et votre certificat sont ajoutés aux serveurs Citrix.

Configuration de l'authentification par certificat + mot de passe à usage unique pour Secure Hub

Vous pouvez configurer Citrix ADC afin que Secure Hub s'authentifie à l'aide d'un certificat et d'un jeton de sécurité qui est utilisé en tant que mot de passe à usage unique. Cette configuration fournit une option de sécurité renforcée qui ne laisse aucune trace Active Directory sur les appareils.

Pour permettre à Secure Hub d'utiliser ce type d'authentification, procédez comme suit : ajoutez une action de réécriture ainsi qu'une stratégie de réécriture dans Citrix ADC qui insère un en-tête de réponse personnalisé au format **X-Citrix-AM-GatewayAuthType: CertAndRSA** pour indiquer le type d'ouverture de session Citrix Gateway.

D'ordinaire, Secure Hub utilise le type d'ouverture de session Citrix Gateway configuré dans la console Endpoint Management. Toutefois, Secure Hub n'a pas accès à ces informations tant qu'il n'a pas ouvert de session pour la première fois. Par conséquent l'en-tête personnalisé est requis.

Remarque :

Si différents types d'ouverture de session sont définis dans Endpoint Management et Citrix ADC, la configuration de Citrix ADC a priorité. Pour de plus amples informations, consultez la section [Citrix Gateway et Endpoint Management](#).

1. Dans Citrix ADC, accédez à **Configuration > AppExpert > Rewrite > Actions**.
2. Cliquez sur **Ajouter**.
L'écran **Create Rewrite Action** s'affiche.
3. Remplissez chaque champ, comme illustré dans la figure suivante et cliquez sur **Create**.

The screenshot shows the 'Create Rewrite Action' form with the following details:

- Name***: InsertGatewayAuthTypeHeader
- Type***: INSERT_HTTP_HEADER
- Use this action type to insert a header.**
- Header Name***: X-Citrix-AM-GatewayAuthType
- Expression**: "CertAndRSA"
- Buttons**: Create, Close

Le résultat suivant s'affiche sur l'écran principal **Rewrite Actions**.

Name	Type	Target Expression	Expression	Pattern
ns_cvpn_sp_js_checkout_rw_act	insert_after_all	TEXT	"\\'+window.location.pathname.split('\\')[1]+'\\'+wi...	re~a.substr(0,3).toLowerCase(\\)=\\'%2f\\)=a-
InsertGatewayAuthTypeHeader	insert_http_header	X-Citrix-AM-GatewayAuthType	"CertAndRSA"	

4. Liez l'action de réécriture au serveur virtuel en tant que stratégie de réécriture. Accédez à **Configuration > NetScaler Gateway > Virtual Servers** et sélectionnez votre serveur virtuel.

Name	State	IP Address	Port	Protocol	Maximum Users	Current Users	Total Connected Users
_XM_gwcamamappc8	Up	10.71.12.30	443	SSL	0	3	3
SessionTransfer	Up	10.71.12.30	500	SSL	0	0	0

5. Cliquez sur **Edit**.
6. Sur l'écran **Virtual Servers configuration**, faites défiler jusqu'à **Policies**.
7. Cliquez sur **+** pour ajouter une stratégie.

The screenshot displays the Citrix NetScaler configuration interface. It is divided into several sections:

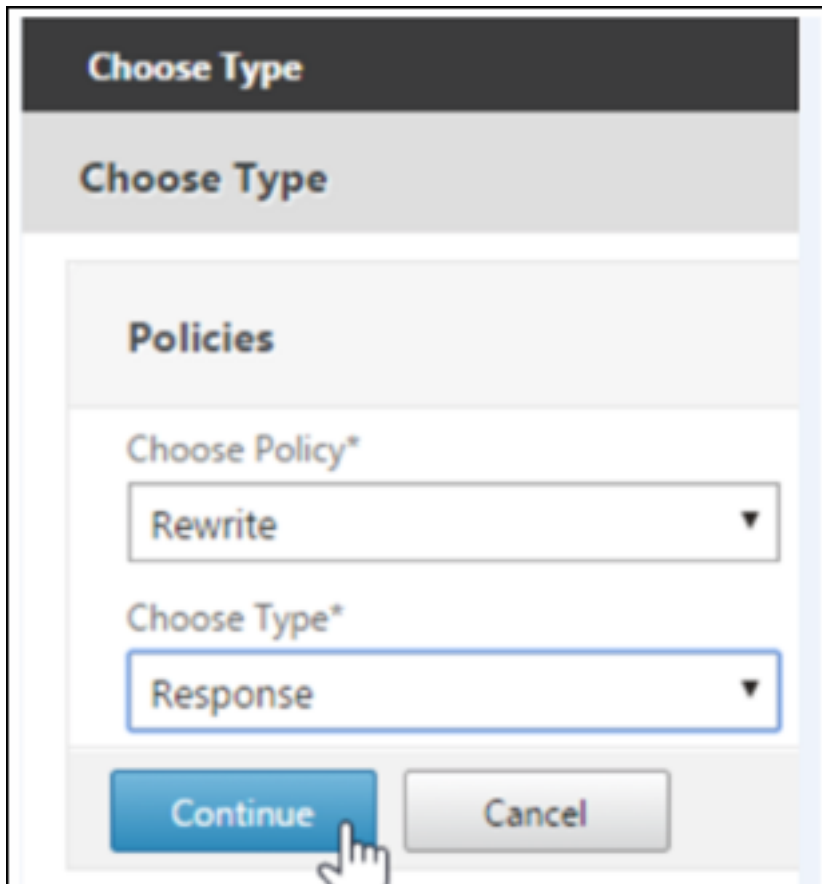
- Profiles:** Shows configuration for Net Profile, TCP Profile, and HTTP Profile (set to `nshhttp_default_strict_validation`).
- Published Applications:** Lists `No` Next HOP Server, `1` STA Server, and `No` Url.
- Other Settings:** A table of various settings:

ICMP Virtual Server Response	Passive	Listen Priority	
RHI State	Passive	Listen Policy Expression	NONE
Redirect to Home page	true	ShareFile	
		AppController	https://camamappc8.camam.net:8443
		L2 Connection	false
- Policies:** A list of policy categories: Request Policies, 3 Session Policies, 2 ClientlessAccess Policies, and 5 Cache Policies. A hand cursor is pointing to the '+' icon in the top right corner of this section.

On the right side, there is a 'Help' button and an 'Advanced Settings' menu with options like Content Switching Policies, SSL Profile, SSL Policies, Intranet IP Addresses, Intranet Applications, Portal Themes, and EULA.

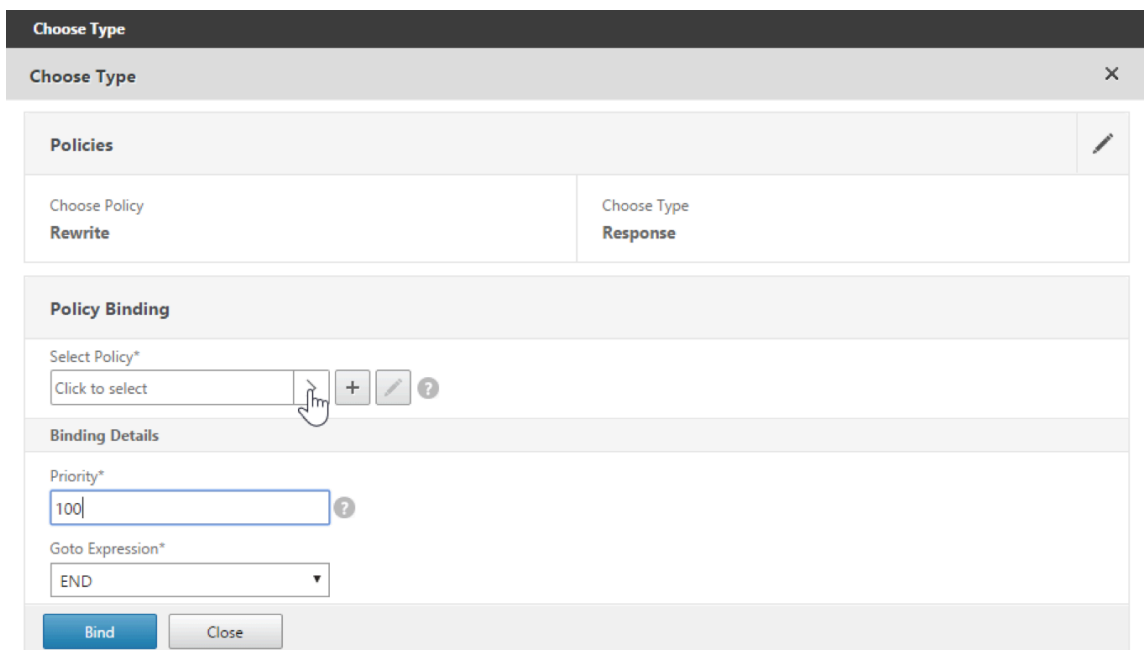
A 'Done' button is located at the bottom left of the configuration area.

8. Dans le champ **Choose Policy**, choisissez **Rewrite**.
9. Dans le champ **Choose Type**, choisissez **Response**.



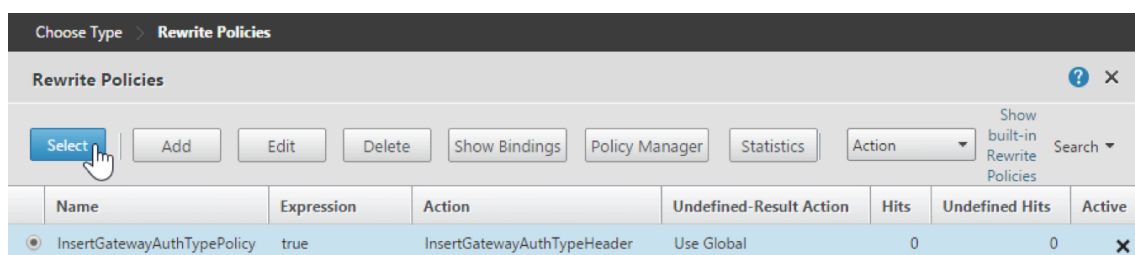
10. Cliquez sur **Continuer**.

La section **Policy Binding** va se développer.

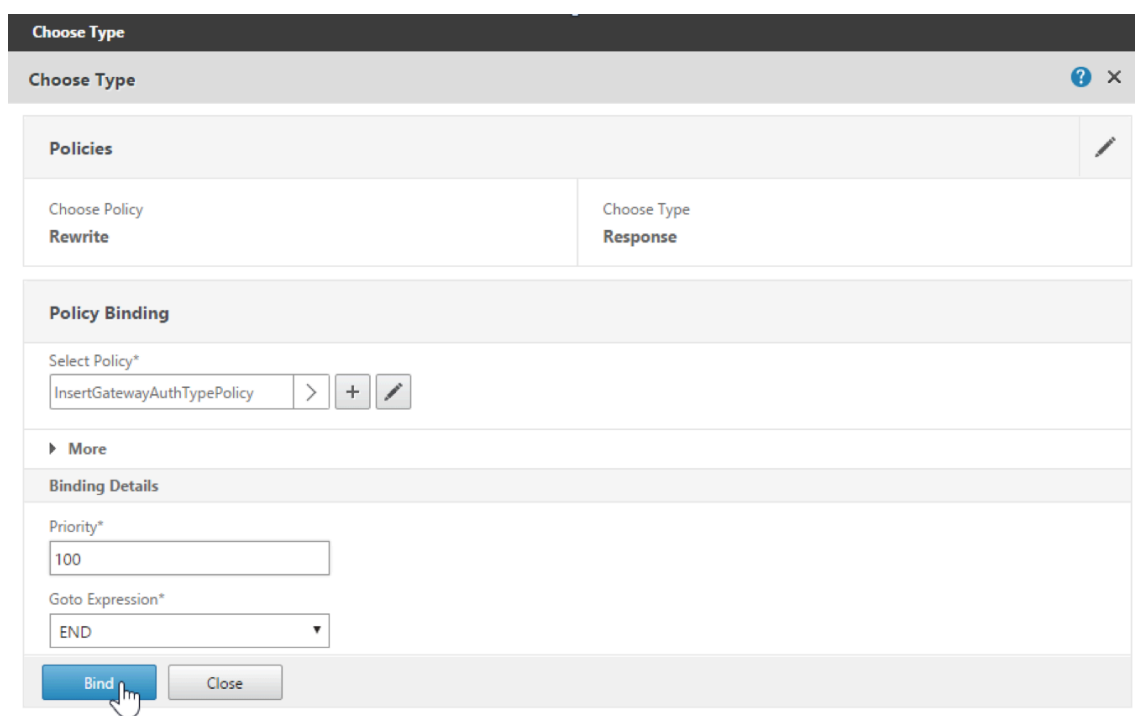


11. Cliquez sur **Select Policy**.

Un écran répertoriant les stratégies disponibles s'affiche.



12. Cliquez sur la ligne de la stratégie que vous avez créé, puis cliquez sur **Sélectionner**. L'écran **Policy Binding** s'affiche de nouveau, avec la stratégie sélectionnée renseignée.



13. Cliquez sur **Bind**.

Si la liaison réussie, l'écran de configuration principal s'affiche avec la stratégie de réécriture.

The screenshot displays a configuration page for mobile productivity applications. It is divided into several sections:

- SSL Settings:** Includes parameters like 'Enable DH Param' (DISABLED), 'Enable Ephemeral RSA' (ENABLED), 'Refresh Count' (0), 'Enable Session Reuse' (ENABLED), 'Time-out' (120), and 'SSL Redirect' (DISABLED). Other SSL-related settings include 'Clear Text Port' (0), 'Enable Cipher Redirect' (DISABLED), 'Client Authentication' (ENABLED), 'Client Certificate' (Mandatory), 'Send Close-Notify' (YES), 'PUSH Encryption Trigger' (Always), and 'SNI Enable' (DISABLED). There are also 'SSLv2 Redirect' (DISABLED) and 'SSLv2' (DISABLED) settings.
- Published Applications:** A list showing 'No Next HOP Server', '1 STA Server', and 'No Url'.
- Other Settings:** Includes 'ICMP Virtual Server Response' (Passive), 'RHI State' (Passive), 'Redirect to Home page' (true), 'Listen Priority', 'Listen Policy Expression' (None), 'ShareFile', 'AppController' (https://xms3.dm.com:8443), and 'L2 Connection' (false).
- Policies:** A list of policy categories: 'Request Policies', '3 Session Policies', '2 ClientlessAccess Policies', '4 Cache Policies', 'Response Policies', and '1 Rewrite Policy'. The 'Response Policies' and '1 Rewrite Policy' items are highlighted with a red border.

14. Pour afficher les détails de la stratégie, cliquez sur **Rewrite Policy**.

The screenshot shows the 'VPN Virtual Server Rewrite Policy Binding' configuration window. At the top, there are buttons for 'Add Binding', 'Unbind', and 'Edit'. Below is a table with the following columns: Priority, Policy Name, Expression, Action, and Goto Expression.

Priority	Policy Name	Expression	Action	Goto Expression
100	InsertGatewayAuthTypeHeaderPolicy	true	InsertGatewayAuthTypeHeader	END

At the bottom of the window, there is a 'Close' button.

Exigence en matière de port pour la connectivité ADS pour les appareils Android

La configuration d'un port permet de s'assurer que les appareils Android qui se connectent à partir de Secure Hub peuvent accéder au service ADS de Citrix depuis le réseau d'entreprise. L'accès au service ADS est important lors du téléchargement de mises à jour de sécurité mises à disposition via ADS. Les connexions ADS peuvent ne pas être compatibles avec votre serveur proxy. Dans ce scénario, autorisez la connexion ADS à contourner le serveur proxy.

Important :

Secure Hub pour Android et iOS nécessitent que vous autorisiez les appareils Android à accéder au service ADS (service de découverte automatique). Pour de plus amples informations, consultez la section [Configuration requise pour les ports](#) dans la documentation Citrix Endpoint Management. Cette communication se fait sur le port 443. Il est très probable que votre envi-

ronnement soit conçu pour autoriser cet accès. Nous déconseillons aux clients qui ne peuvent pas garantir cette communication de mettre à niveau vers Secure Hub 10.2. Si vous avez des questions, contactez l'assistance Citrix.

Les clients souhaitant activer le certificate pinning doivent effectuer ce qui suit :

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

Les nouvelles améliorations apportées au certificat pinning nécessitent que les appareils se connectent à ADS avant l'inscription de l'appareil. Cela garantit que Secure Hub dispose des dernières informations de sécurité pour l'environnement dans lequel l'appareil s'inscrit. Si les appareils ne peuvent pas contacter ADS, Secure Hub n'autorise pas l'inscription de l'appareil. Par conséquent, il est primordial d'autoriser l'accès à ADS dans le réseau interne pour permettre aux appareils de s'inscrire.

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

Nom de domaine complet	Adresse IP	Port	Utilisation adresse IP et port
discovery.mdm.zenprise.com	52.5.138.94	443	Secure Hub - Communication ADS
discovery.mdm.zenprise.com	52.1.30.122	443	Secure Hub - Communication ADS
ads.xm.cloud.com : veuillez noter que Secure Hub version 10.6.15 et versions ultérieures utilise ads.xm.cloud.com .	34.194.83.188	443	Secure Hub - Communication ADS
ads.xm.cloud.com : veuillez noter que Secure Hub version 10.6.15 et versions ultérieures utilise ads.xm.cloud.com .	34.193.202.23	443	Secure Hub - Communication ADS

Si le certificate pinning est activé :

- Secure Hub épingle votre certificat d'entreprise lors de l'inscription de l'appareil.
- Lors d'une mise à niveau, Secure Hub supprime tout certificate pinning en cours et épingle le certificat de serveur sur la première connexion des utilisateurs inscrits.

Remarque :

Si vous activez le certificate pinning après une mise à niveau, les utilisateurs doivent se réinscrire.

- Le renouvellement du certificat ne nécessite pas de réinscription, si la clé publique du certificat soit inchangée.

Le certificate pinning prend en charge les certificats feuille, mais pas les certificats intermédiaires ou les certificats d'émetteur. Le certificate pinning s'applique aux serveurs Citrix, tels que Endpoint Management et Citrix Gateway, et non aux serveurs tiers.

Fonctionnalités Secure Hub

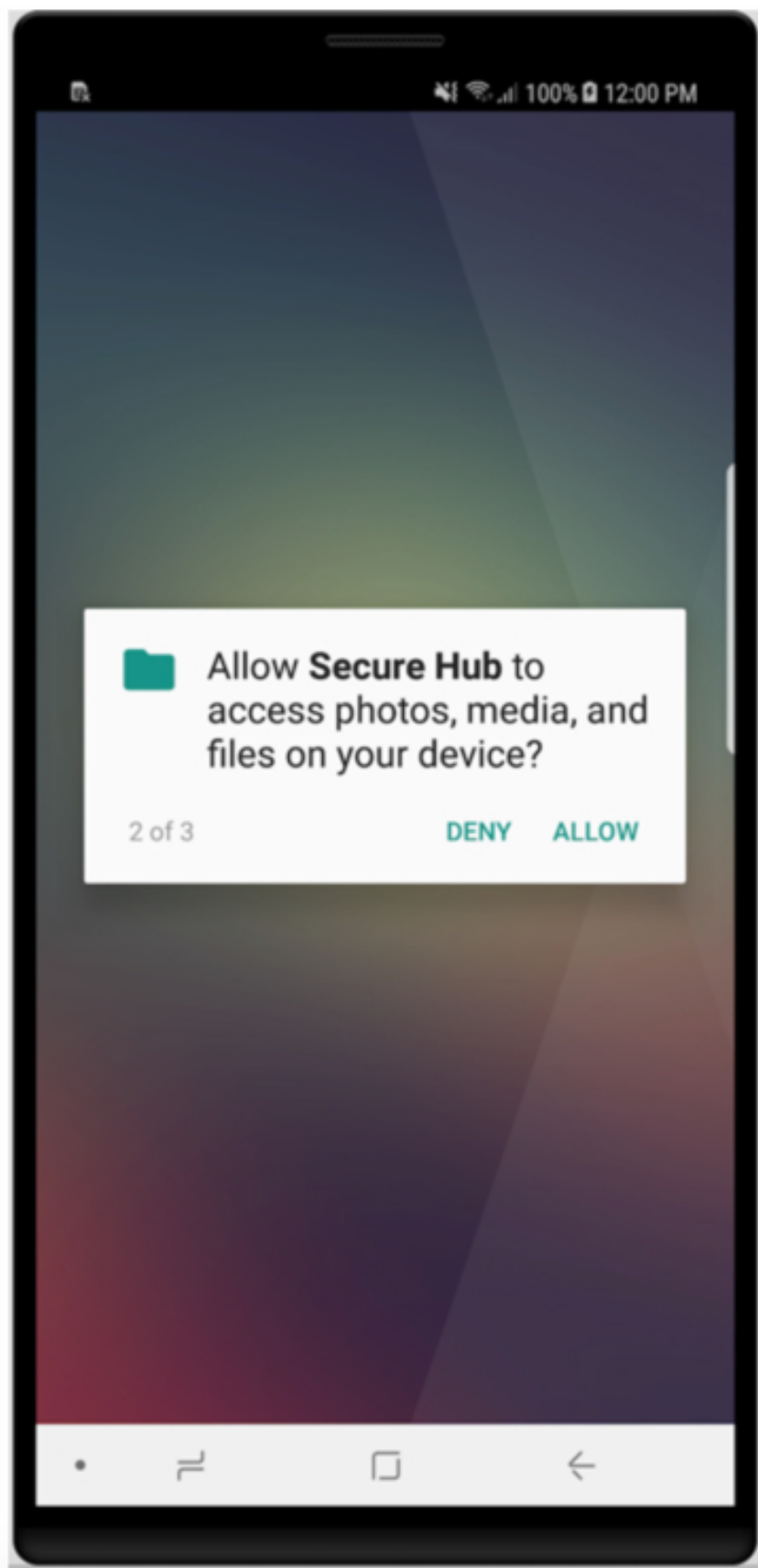
Secure Hub vous permet de contrôler et d'appliquer des stratégies mobiles tout en offrant un accès au magasin et une assistance en direct. Les utilisateurs commencent par télécharger Secure Hub sur leurs appareils depuis les magasins d'applications Apple, Android ou Windows.

Lorsque Secure Hub s'ouvre, les utilisateurs entrent les informations d'identification fournies par leurs sociétés pour inscrire leurs périphériques dans Secure Hub. Pour plus de détails sur l'inscription d'appareils, voir [Comptes utilisateur, rôles et inscription](#).

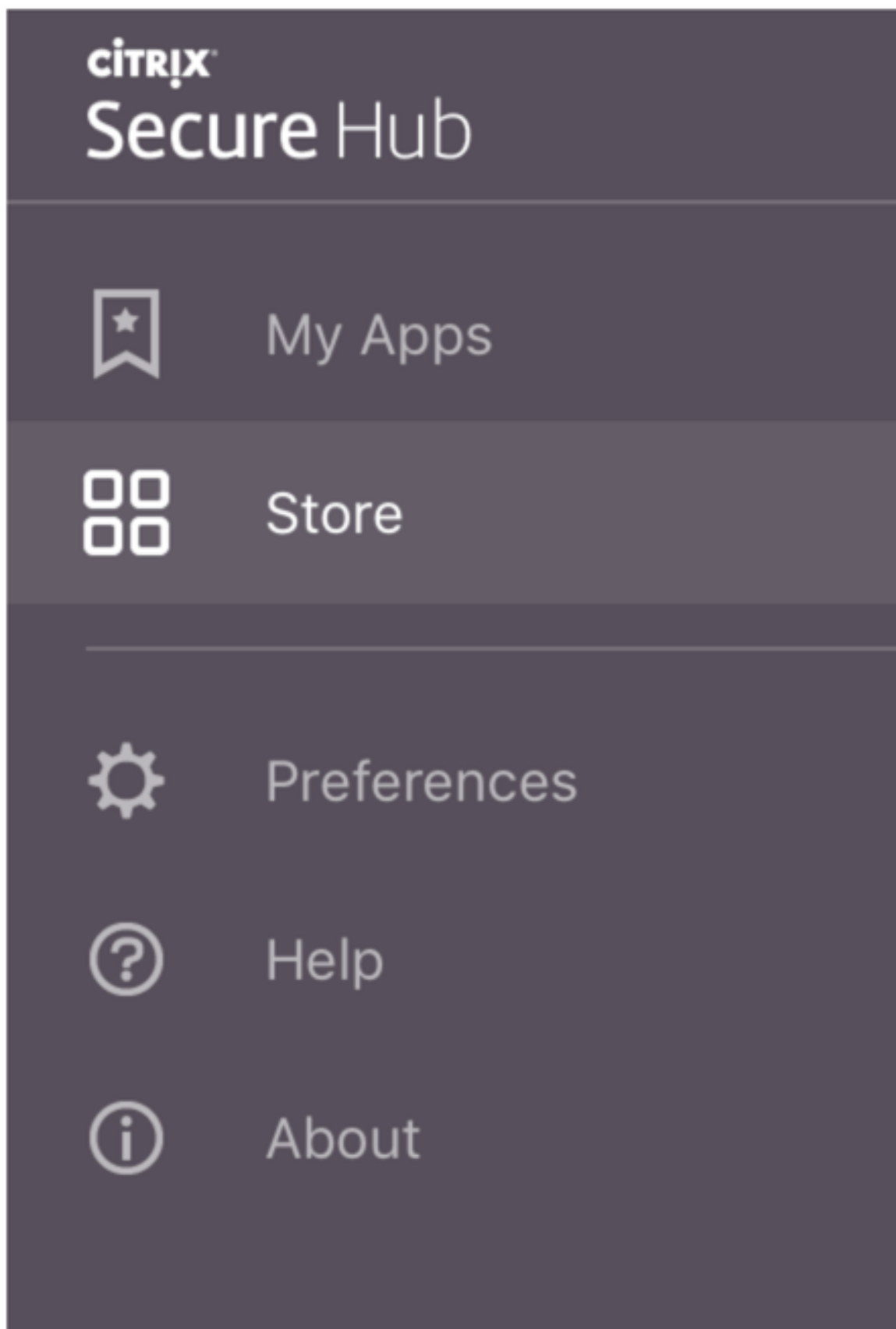
Sur Secure Hub pour Android, lors de l'installation et de l'inscription initiales, le message suivant s'affiche : Autoriser Secure Hub à accéder aux photos, médias et fichiers sur votre périphérique ?

Ce message provient du système d'exploitation Android et non de Citrix. Lorsque vous appuyez sur **Autoriser**, Citrix et les administrateurs qui gèrent Secure Hub n'ont jamais accès à vos données personnelles. Toutefois, si vous menez une session de support à distance avec votre administrateur, l'administrateur peut voir vos fichiers personnels dans la session.

Une fois inscrits, les utilisateurs verront les applications et bureaux que vous avez mis à disposition dans leur onglet **Mes applications**. Les utilisateurs peuvent ajouter davantage d'applications à partir du magasin. Sur les téléphones, le lien du magasin est disponible sous l'icône d'hamburger **Paramètres** dans le coin supérieur gauche :



Sur les tablettes, le magasin est un onglet séparé.



Lorsque les utilisateurs d'iPhone exécutant iOS 9 ou une version ultérieure installent des applications de productivité mobiles à partir du magasin, ils voient un message. Le message indique que le développeur d'entreprise, Citrix, n'est pas approuvé sur cet iPhone. Le message indique que l'application ne sera pas disponible tant que le développeur ne sera pas approuvé. Lorsque ce message s'affiche, Secure Hub invite les utilisateurs à afficher des instructions qui les guident dans le processus d'approbation des applications d'entreprise Citrix pour leur iPhone.

Pour les déploiements MAM exclusif, vous pouvez configurer Endpoint Management de manière à ce que les utilisateurs d'appareils Android ou iOS qui s'inscrivent dans Secure Hub avec des informations d'identification de messagerie soient automatiquement inscrits dans Secure Mail. Les utilisateurs n'ont pas à entrer d'informations supplémentaires ou à effectuer des étapes supplémentaires pour s'inscrire dans Secure Mail.

À la première utilisation de Secure Mail, Secure Mail obtient l'adresse e-mail de l'utilisateur, le domaine et l'ID utilisateur depuis Secure Hub. Secure Mail utilise l'adresse e-mail pour la détection automatique. Exchange Server est identifié par le domaine et l'ID utilisateur, ce qui permet à Secure Mail d'authentifier l'utilisateur automatiquement. L'utilisateur est invité à entrer un mot de passe si la stratégie est définie pour ne pas contourner le mot de passe. L'utilisateur n'est cependant pas invité à entrer des informations supplémentaires.

Pour activer cette fonctionnalité, créez trois propriétés :

- La propriété de serveur MAM_MACRO_SUPPORT. Pour obtenir des instructions, consultez la section [Propriétés de serveur](#).
- Les propriétés clientes ENABLE_CREDENTIAL_STORE et SEND_LDAP_ATTRIBUTES. Pour obtenir des instructions, consultez la section [Propriétés de client](#).

Si vous souhaitez personnaliser votre magasin, accédez à **Paramètres > Personnalisation du client** pour modifier le nom, ajouter un logo, et indiquer la façon dont les applications s'affichent.

XenMobile Analyze Manage Configure ⚙️ administrator ▾

Settings > Client Branding

Client Branding

You can set the way apps appear in the store and add a logo to brand Worx Home on mobile devices.

Store name* ⓘ

Default store view

Category

A-Z

Device

Phone

Tablet

Branding file Browse

Note:

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.
- A .zip file should be created from the files, not a folder with the files inside of it.

Cancel Save

Vous pouvez modifier la description des applications dans la console Endpoint Management. Cliquez sur **Configurer**, puis sur **Applications**. Sélectionnez l'application dans le tableau et cliquez sur **Modifier**. Sélectionnez les plates-formes de l'application dont vous modifiez la description et entrez le texte dans la case **Description**.

XenMobile Analyze Manage Configure

Device Policies Apps Actions ShareFile Delivery Groups

MDX

App Information

1 App Information

2 Platform

iOS

Android

Windows Phone

3 Approvals (optional)

4 Delivery Group Assignments (optional)

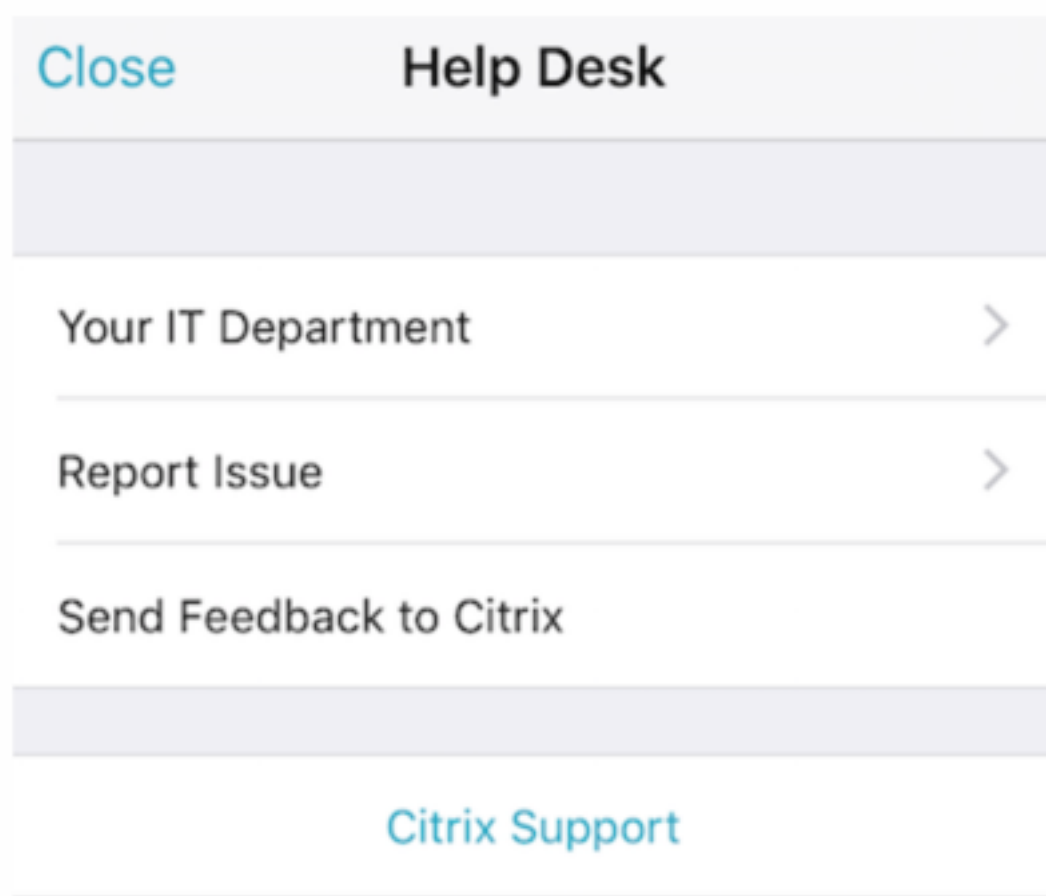
Name* ⓘ

Description

App category

Dans le magasin, les utilisateurs peuvent rechercher uniquement les applications et bureaux que vous avez configurés et sécurisés dans Endpoint Management. Pour ajouter l'application, les utilisateurs appuient sur **Détails** et sur **Ajouter**.

Secure Hub offre également aux utilisateurs plusieurs façons d'obtenir de l'aide. Sur les tablettes, il suffit de taper sur le point d'interrogation dans le coin supérieur droit pour afficher les options d'aide. Sur les téléphones, les utilisateurs appuient sur l'icône du menu hamburger dans le coin supérieur gauche et sur **Aide**.



Votre service informatique affiche le numéro de téléphone et l'adresse e-mail du service d'assistance de votre entreprise, auxquels les utilisateurs peuvent accéder directement depuis l'application. Vous entrez les numéros de téléphone et les adresses e-mail dans la console Endpoint Management. Cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche. Cliquez sur **Plus**, puis cliquez sur **Support client**. L'écran dans lequel vous entrez les informations s'affiche.

L'option **Signaler un problème** affiche une liste des applications. Les utilisateurs sélectionnent l'application qui présente un problème. Secure Hub génère automatiquement les journaux et ouvre un message dans Secure Mail avec les journaux attachés en tant que fichier zip. Les utilisateurs ajoutent un objet et une description du problème. Ils peuvent également joindre une copie d'écran.

L'option **Envoyer des commentaires à Citrix** ouvre un message dans Secure Mail dans lequel l'adresse de l'assistance Citrix est déjà renseignée. L'utilisateur peut entrer des suggestions visant à améliorer Secure Mail dans le corps du message. Si Secure Mail n'est pas installé sur l'appareil, le programme de messagerie natif s'ouvre.

Les utilisateurs peuvent également appuyer sur **Assistance Citrix**, ce qui ouvre le [centre de connaissances Citrix](#). De là, ils peuvent consulter les articles de support pour tous les produits Citrix.

Dans **Préférences**, les utilisateurs peuvent trouver des informations sur leurs comptes et leurs appareils.

Secure Hub offre également des stratégies de géolocalisation et de suivi géographique, par exemple, si vous voulez vous assurer qu'un appareil appartenant à l'entreprise ne sort pas d'un certain périmètre géographique. Pour plus de détails, consultez la section [Stratégie d'emplacement](#). Par ailleurs, Secure Hub collecte automatiquement et analyse les informations d'échec de façon à ce que vous puissiez découvrir la cause de l'échec. Le logiciel Crashlytics prend en charge cette fonction.

Présentation de Secure Mail

February 19, 2019

Citrix Secure Mail permet aux utilisateurs d'accéder à leurs e-mails, calendriers et contacts sur leurs téléphones mobiles et tablettes. Pour conserver la continuité des comptes Microsoft Outlook ou IBM Notes, Secure Mail est synchronisé avec le serveur Microsoft Exchange Server et le serveur IBM Notes Traveler.

En tant qu'application Citrix, Secure Mail tire parti de la compatibilité SSO avec Citrix Secure Hub. Une fois que les utilisateurs se sont connectés à Secure Hub, ils peuvent utiliser Secure Mail sans avoir à entrer de nouveau leur nom d'utilisateur et mot de passe. Vous pouvez configurer Secure Mail afin qu'il soit automatiquement distribué sur les appareils utilisateur lorsque ces derniers sont inscrits dans Secure Hub, ou les utilisateurs peuvent ajouter l'application depuis le magasin.

Secure Mail est compatible avec :

- Exchange Server 2016, mise à jour cumulative 11
- Exchange Server 2016, mise à jour cumulative 10
- Exchange Server 2016, mise à jour cumulative 9
- Exchange Server 2016, mise à jour cumulative 8
- Exchange Server 2013, mise à jour cumulative 21

- Exchange Server 2013, mise à jour cumulative 19
- Exchange Server 2010 SP3 Update Rollup 24
- Exchange Server 2010 SP3 Update Rollup 19
- Exchange Server 2010 SP3 Update Rollup 22
- Serveur de messagerie IBM Domino version 9.0.1 FP10 HF197
- Serveur de messagerie IBM Domino version 9.0.1 FP9
- IBM Lotus Notes Traveler version 9.0.1.21
- IBM Lotus Notes Traveler version 9.0.1.9
- Microsoft Office 365 (Exchange Online)

Pour commencer, téléchargez Secure Mail et d'autres composants Endpoint Management à partir de [Téléchargements de Citrix Endpoint Management](#).

Pour connaître la configuration système requise pour Secure Mail et pour d'autres applications de mobilité, consultez la section [Configuration système requise](#).

Pour plus d'informations sur les notifications dans Secure Mail pour iOS et Android lorsque l'application est exécutée en arrière-plan ou fermée, consultez la section [Notifications push pour Secure Mail](#).

Pour les fonctionnalités iOS prises en charge sur Secure Mail, voir les [fonctionnalités iOS pour Secure Mail](#).

Pour les fonctionnalités Android prises en charge sur Secure Mail, voir les [fonctionnalités Android pour Secure Mail](#).

Pour les fonctionnalités iOS et Android prises en charge sur Secure Mail, voir les [fonctionnalités iOS et Android pour Secure Mail](#).

Citrix Secure Web

March 1, 2019

Citrix Secure Web est un navigateur Web mobile qui offre un accès sécurisé à des sites internes et externes. Vous pouvez configurer Secure Web pour qu'il soit automatiquement poussé vers les appareils utilisateur lorsque ces derniers sont enrôlés dans Citrix Secure Hub, ou les utilisateurs peuvent ajouter l'application depuis le magasin d'applications Endpoint Management.

Pour connaître la configuration système requise pour Secure Web et pour d'autres applications de productivité mobiles, consultez la section [Configuration système requise](#).

Intégration et mise à disposition de Secure Web

Remarque :

Le MDX Toolkit 10.7.10 est la dernière version qui prend en charge l'encapsulation des applications de productivité mobiles. Les utilisateurs accèdent aux versions 10.7.5 et ultérieures des applications de productivité mobiles depuis des magasins d'applications publics.

Pour intégrer et délivrer Secure Web, suivez ces étapes :

1. Pour activer l'authentification unique (SSO) sur le réseau interne, configurez Citrix Gateway.

Pour le trafic HTTP, Citrix ADC peut fournir l'authentification unique (SSO) pour tous les types d'authentification proxy pris en charge par Citrix ADC. Pour le trafic HTTPS, la stratégie Activer la mise en cache du mot de passe Web permet à Secure Web de s'authentifier et de fournir l'authentification unique (SSO) au serveur proxy via MDX. MDX prend uniquement en charge l'authentification de proxy NTLM, Digest et de base. Le mot de passe est mis en cache à l'aide de MDX et stocké dans le coffre partagé Worx, une zone de stockage sécurisée pour les données applicatives sensibles. Pour plus d'informations sur la configuration de Citrix Gateway, consultez la section [Citrix Gateway](#).
2. Téléchargez Secure Web.
3. Déterminez la manière dont vous souhaitez configurer les connexions utilisateur au réseau interne.
4. Ajoutez Secure Web à Endpoint Management à l'aide des mêmes étapes que pour d'autres applications MDX et configurez des stratégies MDX. Pour de plus amples informations sur les stratégies spécifiques à Secure Web, veuillez consulter la section « À propos des stratégies Secure Web » de cet article.

Configuration des connexions utilisateur

Secure Web prend en charge les configurations suivantes pour les connexions utilisateur :

- **Navigation sécurisée** : les connexions qui sont tunnelisées sur le réseau interne peuvent utiliser une variante d'un VPN sans client, appelé Navigation sécurisée. Il s'agit de la configuration par défaut spécifiée pour la stratégie **Mode VPN préféré**. Navigation sécurisée est recommandé pour les connexions qui nécessitent l'authentification unique (SSO).
- **Tunnel VPN complet** : les connexions qui sont tunnelisées sur le réseau interne peuvent utiliser un tunnel VPN complet, configuré par la stratégie **Mode VPN préféré**. Un tunnel VPN complet est recommandé pour les connexions qui utilisent des certificats clients ou des connexions SSL de bout en bout vers une ressource dans le réseau interne. Le paramètre Tunnel VPN complet gère les protocoles faisant appel à TCP et peut être utilisé avec des ordinateurs Windows et Mac, ainsi qu'avec des appareils iOS et Android.

- La stratégie **Autoriser le basculement vers le mode VPN** permet le basculement automatique entre les modes de tunnel VPN complet et de navigation sécurisée si nécessaire. Cette stratégie est désactivée par défaut. Lorsque cette stratégie est activée, une demande réseau qui a échoué en raison d'une demande d'authentification qui ne peut pas être traitée dans le mode VPN préféré est de nouveau tentée dans un autre mode. Par exemple, les contestations de serveur pour les certificats clients peuvent utiliser le mode Tunnel VPN complet, mais pas le mode Navigation sécurisée. De même, les demandes d'authentification HTTP sont plus susceptibles d'être traitées avec l'authentification unique (SSO) lorsqu'elles utilisent le mode Navigation sécurisée.
- **Tunnel VPN complet avec PAC** : vous pouvez utiliser un fichier PAC (Proxy Automatic Configuration) avec un déploiement de tunnel VPN complet pour les appareils iOS. Un fichier PAC contient des règles qui définissent la manière dont les navigateurs Web sélectionnent un serveur proxy pour accéder à une URL spécifiée. Les règles du fichier PAC peuvent spécifier la procédure à suivre pour les sites internes et externes. Secure Web analyse les règles du fichier PAC et envoie les informations sur le serveur proxy à Citrix Gateway.
- Lorsqu'un fichier PAC est utilisé, les performances du tunnel VPN complet sont comparables au mode de navigation sécurisée. Pour de plus amples informations sur la configuration du fichier PAC, consultez la section [Tunnelisation VPN complète avec le fichier PAC](#).

Le tableau suivant indique si Secure Web invite l'utilisateur à entrer des informations d'identification, en fonction de la configuration et du type de site :

Mode de connexion	Type de site	Mise en cache du mot de passe	Authentification unique (SSO) configurée pour Citrix Gateway	Secure Web demande des identifiants lors du premier accès à un site Web	Secure Web demande des identifiants lors de l'accès ultérieur à un site Web	Secure Web demande des identifiants après le changement de mot de passe
Navigation sécurisée	http	Non	Oui	Non	Non	Non
Navigation sécurisée	https	Non	Oui	Non	Non	Non
VPN complet	http	Non	Oui	Non	Non	Non

Mode de connexion	Type de site	Mise en cache du mot de passe	Authentification unique (SSO) configurée pour Citrix Gateway	Secure Web demande des identifiants lors du premier accès à un site Web	Secure Web demande des identifiants lors de l'accès ultérieur à un site Web	Secure Web demande des identifiants après le changement de mot de passe
VPN complet	https	Oui ; si la stratégie MDX Secure Web Activer la mise en cache du mot de passe Web est définie sur Activé.	Non	Oui ; requis pour mettre en cache les informations d'identification dans Secure Web.	Non	Oui

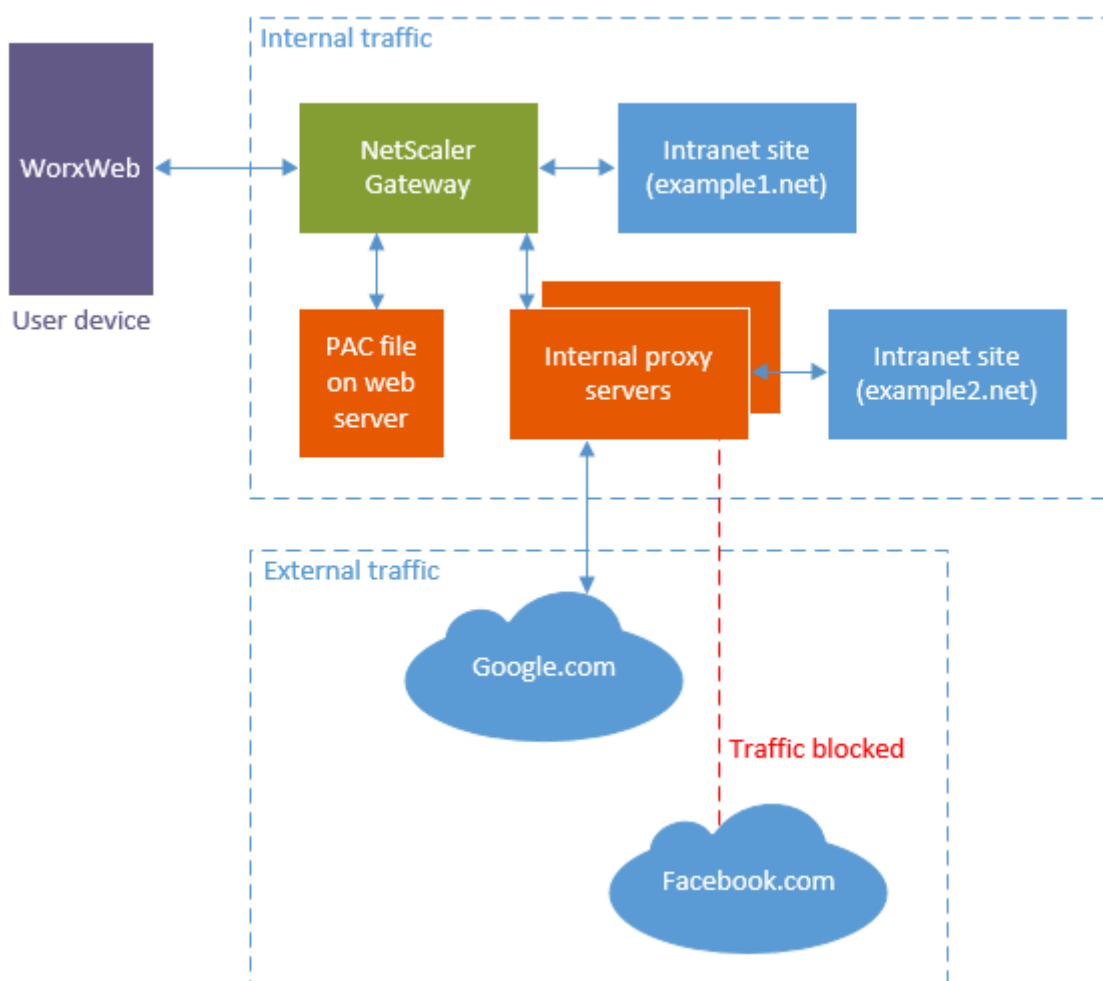
Tunnelisation VPN complète avec le fichier PAC

Important :

Si Secure Web est configuré avec un fichier PAC et que Citrix ADC est configuré pour utiliser un proxy, Secure Web expire. Vous devez supprimer les stratégies de trafic Citrix Gateway configurées pour le proxy avant d'utiliser le paramètre Tunnel VPN complet avec le fichier PAC.

Lorsque vous configurez Secure Web pour la tunnelisation VPN complète avec votre fichier PAC ou un serveur proxy, Secure Web envoie l'ensemble du trafic au proxy via Citrix Gateway, qui achemine ensuite le trafic en fonction des règles de configuration du proxy. Dans cette configuration, Citrix Gateway ignore le fichier PAC ou le serveur proxy. Le flux du trafic est le même que pour la tunnelisation VPN complète sans PAC.

Le diagramme suivant illustre le flux du trafic lorsque les utilisateurs Secure Web accèdent à un site Web :



Dans cet exemple, les règles de trafic spécifient ce qui suit :

- Citrix Gateway se connecte directement au site intranet `example1.net`.
- Le trafic vers le site intranet `example2.net` est transmis par proxy via des serveurs proxy internes.
- Le trafic externe est transmis par proxy via des serveurs proxy internes. Les règles de proxy bloquent le trafic externe vers `Facebook.com`.

Pour configurer un tunnel VPN complet avec PAC

1. Validez et testez le fichier PAC.

Remarque :

Pour de plus amples informations sur la création et l'utilisation de fichiers PAC, consultez <https://findproxyforurl.com/>.

Validez votre fichier PAC à l'aide d'un outil de validation PAC tel que [Pacparser](#). Lorsque vous lisez votre fichier PAC, assurez-vous que les résultats Pacparser sont conformes à vos attentes.

Si le fichier PAC contient une erreur de syntaxe, les appareils mobiles ignoreront le fichier PAC de manière silencieuse. (Un fichier PAC est uniquement stocké dans la mémoire des appareils mobiles.)

Un fichier PAC est traité de haut en bas et le traitement s'arrête lorsqu'une règle correspond à la requête actuelle.

Testez l'URL du fichier PAC avec un navigateur Web avant d'entrer une valeur dans le champ PAC/Proxy de Endpoint Management. Assurez-vous que l'ordinateur peut accéder au réseau sur lequel le fichier PAC est situé.

<https://webserver.local/GenericPAC.pac>

<https://webserver.local/GenericPAC.pac>

Les extensions du fichier PAC testé sont .txt ou .pac.

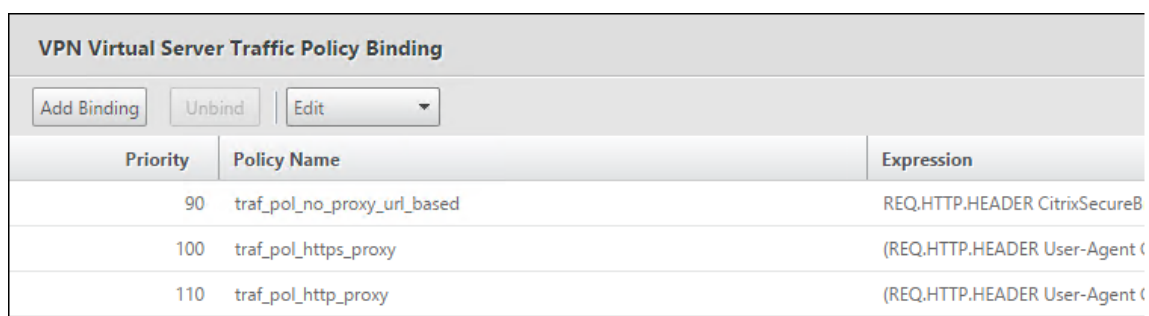
Le fichier PAC devrait afficher son contenu dans le navigateur Web.

Important :

Chaque fois que vous mettez à jour le fichier PAC utilisé avec Secure Web, informez les utilisateurs qu'ils doivent fermer et rouvrir Secure Web.

2. Configurez Citrix Gateway :

- Désactivez le split tunneling Citrix Gateway. Si le split tunneling est activé et qu'un fichier PAC est configuré, les règles du fichier PAC remplacent les règles de split tunneling de Citrix ADC. Un proxy ne remplace pas les règles de split tunneling de Citrix ADC.
- Supprimez les stratégies de trafic Citrix Gateway configurées pour le proxy. Ceci est requis pour assurer le bon fonctionnement de Secure Web. La figure suivante montre un exemple de règles de stratégie à supprimer.



Priority	Policy Name	Expression
90	traf_pol_no_proxy_url_based	REQ.HTTP.HEADER CitrixSecureB
100	traf_pol_https_proxy	(REQ.HTTP.HEADER User-Agent C
110	traf_pol_http_proxy	(REQ.HTTP.HEADER User-Agent C

3. Configurez les stratégies Secure Web :

- Définissez la stratégie Mode VPN préféré sur **Tunnel VPN complet**.
- Définissez la stratégie Autoriser le basculement vers le mode VPN sur **Désactivé**.
- Configurez la stratégie URL du fichier PAC ou serveur proxy. Secure Web prend en charge HTTP et HTTPS, ainsi que par les ports par défaut et les ports autres que ceux par défaut.

Pour HTTPS, l'autorité de certification racine doit être installée sur l'appareil si le certificat est auto-signé ou non fiable.

Veillez à tester l'adresse URL ou l'adresse du serveur proxy dans un navigateur Web avant de configurer la stratégie.

Exemple d'URL de fichier PAC :

```
http[s]://example.com/proxy.pac
```

```
http[s]://10.10.0.100/proxy.txt
```

Exemple de serveurs proxy (port obligatoire) :

```
myhost.example.com:port
```

```
10.10.0.100:port
```

Remarque :

si vous configurez un fichier PAC ou un serveur proxy, ne configurez pas PAC dans les paramètres de proxy du système pour le Wi-Fi.

- Définissez la stratégie Activer la mise en cache du mot de passe Web sur **Activé**. Cette dernière gère le SSO pour les sites HTTPS.

Citrix ADC peut effectuer l'authentification unique (SSO) pour les proxys internes si le proxy prend en charge la même infrastructure d'authentification.

Limitations de prise en charge de fichier PAC

Secure Web ne prend pas en charge :

- Le basculement d'un serveur proxy à une autre. L'évaluation du fichier PAC peut renvoyer plusieurs serveurs proxy pour un nom d'hôte. Secure Web utilise uniquement le premier serveur proxy renvoyé.
- Les protocoles tels que FTP et Gopher dans un fichier PAC.
- Les serveurs proxy SOCKS dans un fichier PAC.
- Le protocole WPAD.

Secure Web ignore la fonction alert du fichier PAC de façon à ce que Secure Web puisse analyser un fichier PAC ne contenant pas ces appels.

Stratégies Secure Web

Lors de l'ajout de Secure Web, tenez compte des stratégies MDX qui sont spécifiques à Secure Web. Pour tous les appareils mobiles pris en charge :

Sites Web autorisés ou bloqués

Secure Web ne filtre pas les liens Web. Vous pouvez utiliser cette stratégie pour configurer une liste spécifique de sites autorisés ou bloqués. Vous configurez des modèles d'adresse URL afin de limiter les sites Web que le navigateur est autorisé à ouvrir, sous forme de liste séparée par des virgules. Chaque modèle de la liste est précédé d'un signe Plus (+) ou Moins (-). Le navigateur compare une URL avec les modèles dans l'ordre indiqué jusqu'à ce qu'une correspondance soit trouvée. Lorsqu'une correspondance est trouvée, l'action exécutée est déterminée par le préfixe comme suit :

- Un préfixe - indique au navigateur de bloquer l'URL. Dans ce cas, l'URL est traitée comme si l'adresse du serveur Web ne pouvait pas être résolue.
- Un préfixe + autorise le traitement de l'URL.
- Si aucun préfixe (+ ou -) n'est fourni avec le modèle, + (autoriser) est la valeur par défaut.
- Si l'URL ne correspond à aucun modèle dans la liste, elle est autorisée.

Pour bloquer toutes les autres URL, ajoutez un signe moins suivi d'un astérisque (-*) à la fin de la liste. Par exemple :

- La valeur de stratégie `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` autorise les URL HTTP avec le domaine `mycorp.com`, mais bloque celles provenant d'un autre domaine, autorise les URL HTTPS et FTP de n'importe quel domaine, et bloque toutes les autres URL.
- La valeur de stratégie `+http://*.training.lab/*,+https://*.training.lab/*,-*` autorise les utilisateurs à ouvrir n'importe quel site dans le domaine Training.lab (intranet) via HTTP ou HTTPS, mais ne leur permet pas d'accéder à des URL publiques, telles que Facebook, Google, Hotmail, etc, quel que soit le protocole utilisé.

La valeur par défaut est vide (toutes les URL sont autorisées).

Bloquer les fenêtres contextuelles

Les fenêtres contextuelles sont de nouveaux onglets que les sites Web ouvrent sans votre autorisation. Cette stratégie détermine si Secure Web autorise les fenêtres contextuelles. Si ce paramètre est défini sur Activé, Secure Web empêche les sites Web d'ouvrir des fenêtres contextuelles. La valeur par défaut est Désactivé.

Signets pré-chargés

Définit un ensemble de signets préchargés pour le navigateur Secure Web. La stratégie est une liste séparée par des virgules de tuples contenant le nom du dossier, un nom convivial et une adresse Web. Chaque triplet doit être au format `dossier,nom,url` où dossier et nom peuvent éventuellement être entourés de guillemets (").

À titre d'exemple, les valeurs de stratégies , "Mycorp, Inc. home page", <https://www.mycorp.com>, "MyCorp Links", Account logon, <https://www.mycorp.com/Accounts> "MyCorp Links/Investor Relations", "Contact us", <https://www.mycorp.com/IR/Contactus.aspx> définissent trois signets. Le premier est un lien principal (aucun nom de dossier) appelé "Mycorp, Inc. home page". Le second lien sera placé dans un dossier "MyCorp Links" intitulé "Account logon". Le troisième sera placé dans le sous-dossier "Investor Relations" du dossier "MyCorp Links" et affiché en tant que "Contact us".

La valeur par défaut est vide.

URL de page d'accueil

Définit le site Web que Secure Web charge au démarrage. La valeur par défaut est vide (page de démarrage par défaut).

Pour les appareils Android et iOS pris en charge uniquement :

Interface utilisateur du navigateur

Spécifie le comportement et la visibilité des contrôles de l'interface utilisateur du navigateur pour Secure Web. Tous les contrôles de navigation sont normalement disponibles. Cela comprend les contrôles suivant, précédent, barre d'adresses et actualiser/arrêter. Vous pouvez configurer cette stratégie pour restreindre l'utilisation et la visibilité de certains de ces contrôles. La valeur par défaut est Toutes les commandes visibles.

Options :

- Toutes les commandes visibles. Toutes les commandes sont visibles et les utilisateurs sont autorisés à les utiliser.
- Barre d'adresses en lecture seule. Toutes les commandes sont visibles, mais les utilisateurs ne peuvent pas modifier le champ d'adresse du navigateur.
- Masquer la barre d'adresses. Masque la barre d'adresses, mais pas les autres commandes.
- Masquer toutes les commandes. Supprime la barre d'outils complète pour offrir une expérience de navigation sans cadre.

Activer la mise en cache du mot de passe Web

Lorsque les utilisateurs Secure Web entrent des informations d'identification lors de l'accès à une ressource Web ou la demande d'une ressource Web, cette stratégie détermine si Secure Web met en cache de façon silencieuse le mot de passe sur l'appareil. Cette stratégie s'applique aux mots de passe entrés dans les boîtes de dialogue d'authentification et non aux mots de passe entrés dans les formulaires Web.

Si l'option **Activé** est sélectionnée, Secure Web met en cache tous les mots de passe des utilisateurs lors de la demande d'une ressource Web. Si l'option **Désactivé** est sélectionnée, Secure Web ne met pas en cache les mots de passe et supprime les mots de passe en cache existants. La valeur par défaut est **Désactivé**.

Cette stratégie est activée uniquement lorsque vous définissez en parallèle la stratégie Mode VPN préféré sur Tunnel VPN complet pour cette application.

Serveurs proxy

Vous pouvez également configurer des serveurs proxy pour Secure Web lorsque vous utilisez le mode Navigation sécurisée. Pour plus d'informations, consultez ce [billet de blog](#).

Suffixes DNS

Sur Android, si aucun suffixe DNS n'est configuré, le VPN peut échouer. Pour de plus amples informations sur la configuration de suffixes DNS, reportez-vous à la section [Prise en charge de requêtes DNS à l'aide de suffixes DNS pour appareils Android](#).

Préparation des sites intranet pour Secure Web

Cette section est destinée aux développeurs de sites Web ayant besoin de configurer un site intranet pour utiliser Secure Web sous Android et iOS. Les sites intranet conçus pour des navigateurs de bureau devront être modifiés pour fonctionner correctement sur les appareils Android et iOS.

Secure Web dépend de Android WebView et iOS UIWebView pour prendre en charge la technologie Web. Certaines des technologies Web prises en charge par Secure Web sont :

- AngularJS
- ASP.NET
- JavaScript
- JQuery
- WebGL

Certaines des technologies Web non prises en charge par Secure Web sont :

- Flash
- Java

Le tableau suivant dresse la liste des fonctionnalités de rendu HTML et des technologies prises en charge par Secure Web. X indique si la fonction est disponible pour une combinaison plate-forme, navigateur et composant.

Technologie	iOS Secure Web	Android 6.x/7.x Secure Web
Moteur JavaScript	JavaScriptCore	V8
Stockage local	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
srcet	X	X
WebGL		X
requestAnimationFrame API		X
API Navigation Timing		X
API Resource Timing		X

Les technologies fonctionnent de la même façon sur tous les appareils ; cependant, Secure Web renvoie différentes chaînes d'agent utilisateur pour différents appareils. Pour déterminer la version de navigateur utilisée pour Secure Web, consultez la chaîne d'agent utilisateur. Depuis Secure Web, accédez à <https://whatsmyuseragent.com/>.

Dépannage des sites intranet

Pour résoudre les problèmes d'affichage lorsque votre intranet est affiché dans Secure Web, comparez les affichages entre Secure Web et d'autres navigateurs compatibles tiers.

Pour iOS, les navigateurs tiers compatibles à des fins de test sont Chrome et Dolphin.

Pour Android, le navigateur tiers compatible à des fins de test est Dolphin.

Remarque :

Chrome est un navigateur natif d'Android. Ne l'utilisez pas pour la comparaison.

Dans iOS, assurez-vous que les navigateurs prennent en charge le VPN au niveau de l'appareil. Vous pouvez configurer cette prise en charge sur l'appareil en accédant à **Réglages > VPN > Ajouter une configuration VPN**.

Vous pouvez également utiliser des clients VPN disponibles sur l'App Store, tels que [Citrix VPN](#), [Cisco AnyConnect](#) ou [Pulse Secure](#).

- Si l’affichage d’une même page Web est identique sur les deux navigateurs, le problème vient de votre site Web. Mettez à jour votre site et vérifiez qu’il fonctionne correctement avec le système d’exploitation.
- Si le problème d’affichage d’une page Web apparaît uniquement dans Secure Web, contactez le support technique Citrix pour ouvrir un ticket d’assistance. Veuillez indiquer les étapes de résolution des problèmes que vous avez suivies, y compris les navigateurs et types de systèmes d’exploitation testés. Si vous rencontrez des problèmes d’affichage avec Secure Web pour iOS, incluez une archive Web de la page, comme décrit dans les étapes suivantes. Ceci permet à Citrix de résoudre le problème plus rapidement.

Pour créer un fichier d’archive Web

À l’aide de Safari sur macOS 10.9 ou une version ultérieure, vous pouvez enregistrer une page Web en tant que fichier d’archive Web (aussi appelé liste de lecture) qui contient tous les fichiers liés, tels que les images, feuilles de style CSS et JavaScript.

1. Depuis Safari, videz le dossier de liste de lecture : dans le **Finder**, cliquez sur le menu **Aller** dans la barre des **menus**, cliquez sur **Aller au dossier**, tapez le nom du chemin d’accès ~/Bibliothèque/Safari/ReadingListArchives/, puis supprimez tous les dossiers dans cet emplacement.
2. Dans la barre des **menus**, accédez à **Safari > Préférences > Avancées** et activez **Afficher le menu Développement** dans la barre des menus.
3. Dans la barre des **menus**, accédez à **Développement > Agent d’utilisateur** et entrez l’agent d’utilisateur Secure Web : (Mozilla/5.0 (iPad; CPU OS 8_3 like macOS) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12F69 Secure Web/ 10.1.0(build 1.4.0) Safari/8536.25).
4. Dans Safari, ouvrez le site Web que vous allez enregistrer en tant que liste de lecture (fichier d’archive Web).
5. Dans la barre des **menus**, accédez à **Signets > Ajouter à la liste de lecture**. Cela peut prendre plusieurs minutes. L’archivage se produit en arrière-plan.
6. Recherchez la liste de lecture archivée : dans la barre des **menus**, cliquez sur **Présentation > Afficher la barre latérale de la liste de lecture**.
7. Vérifiez le fichier d’archive :
 - Désactivez la connectivité réseau sur votre Mac.
 - Ouvrez le site Web à partir de la liste de lecture.
Le site Web doit s’afficher complètement.
8. Comprimez le fichier d’archive : dans le **Finder**, cliquez sur le menu **Aller** dans la barre des **menus**, cliquez sur **Aller au dossier**, tapez le nom du chemin d’accès ~/Bibliothèque/Safari/ReadingListArchi

puis compressez le dossier contenant une chaîne hexadécimale aléatoire en tant que nom de fichier. Il s'agit du fichier que vous pouvez envoyer à l'assistance Citrix lorsque vous ouvrez un ticket d'assistance.

Fonctionnalités Secure Web

Secure Web utilise des technologies d'échange de données mobiles pour créer un tunnel VPN dédié aux utilisateurs pour accéder aux sites Web internes et externes et tous les autres sites Web (y compris les sites avec des informations confidentielles) dans un environnement sécurisé par les stratégies de votre organisation.

L'intégration de Secure Web avec Secure Mail et Citrix Files offre une expérience utilisateur transparente au sein du conteneur Endpoint Management sécurisé. Voici quelques exemples de fonctionnalités d'intégration :

- Lorsque les utilisateurs touchent des liens mailto, un nouveau message s'ouvre dans Citrix Secure Mail sans qu'aucune authentification supplémentaire ne soit requise.
- Dans iOS, les utilisateurs peuvent ouvrir un lien dans Secure Web à partir d'une application de messagerie native en insérant **ctxmobilebrowser://** au début de l'adresse URL. À titre d'exemple, pour ouvrir le lien example.com dans une application de messagerie native, utilisez l'adresse URL `ctxmobilebrowser://example.com`.
- Lorsque les utilisateurs cliquent sur un lien intranet dans un e-mail, Secure Web accède à ce site sans authentification supplémentaire requise.
- Les utilisateurs peuvent charger des fichiers dans Citrix Files qu'ils téléchargent à partir du Web dans Secure Web.

Les utilisateurs de Secure Web peuvent également effectuer les actions suivantes :

- Bloquer les fenêtres contextuelles.

Remarque :

La majorité de la mémoire de Secure Web est consommée par le rendu des fenêtres contextuelles, par conséquent le blocage des fenêtres publicitaires dans les paramètres permet d'améliorer les performances.

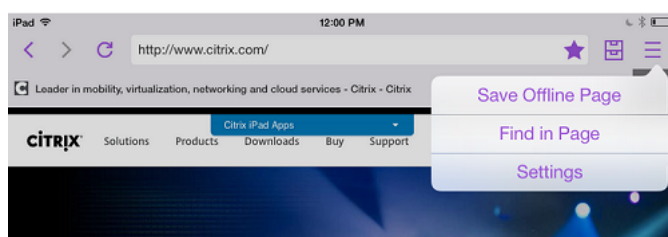
- Placer en signet leurs sites favoris.
- Télécharger des fichiers.
- Enregistrer des pages hors connexion.
- Enregistrer automatiquement des mots de passe.
- Effacer le cache/l'historique/les cookies.
- Désactiver les cookies et le stockage local HTML 5.

- Partager des appareils avec d'autres utilisateurs en toute sécurité.
- Effectuer des recherches dans la barre d'adresses.
- Autoriser les applications Web qu'ils exécutent dans Secure Web à déterminer leur position.
- Exporter et importer les paramètres.
- Ouvrir les fichiers directement dans Citrix Files sans avoir à les télécharger. Pour activer cette fonctionnalité, ajoutez **ctx-sf** à la stratégie URL autorisées dans Endpoint Management.
- Dans iOS, utilisez des actions tactiles 3D pour ouvrir un nouvel onglet et accéder aux pages en mode déconnecté, à des sites favoris et à des téléchargements directement à partir de l'écran d'accueil.
- Dans iOS, télécharger des fichiers de n'importe quelle taille et les ouvrir dans Citrix Files ou d'autres applications.

Remarque :

Si vous placez Secure Web en arrière-plan, le téléchargement s'arrêtera.

- Recherchez un terme dans la page affichée à l'aide de la fonction **Rechercher dans la page**.



Secure Web prend également en charge le texte dynamique, ce qui signifie qu'il affiche la police que les utilisateurs ont définie sur leurs appareils.

Formats de fichiers pris en charge

Remarque :

Secure Web ne prend en charge la lecture vidéo sur aucune plate-forme.

Les formats de fichiers suivants sont pris en charge sur iOS :

Audio	Image	Document
.aac	.jpeg	.txt
.mp3	.png	.pdf
.wav	.gif	.ppt
	Image Gif animée	.doc

Audio	Image	Document
		.docx
		.xls
		.xlsx

Les formats de fichiers suivants sont pris en charge sur Android :

Audio	Image	Document ; pour afficher un aperçu de documents sur Android, des applications d'entreprise, telles que QuickEdit, doivent être installées.
.flac	.jpeg	.txt
.aac	.png	.pdf ; Téléchargement uniquement. Ouvrez dans QuickEdit ou une autre application pour afficher un aperçu.
.m4a	.gif	.ppt
.3GP (AMR-NB)	Image .gif animée	.doc
.mp3		.docx
.wav		.xls
.wma		.xlsx

Citrix QuickEdit pour applications de productivité mobiles

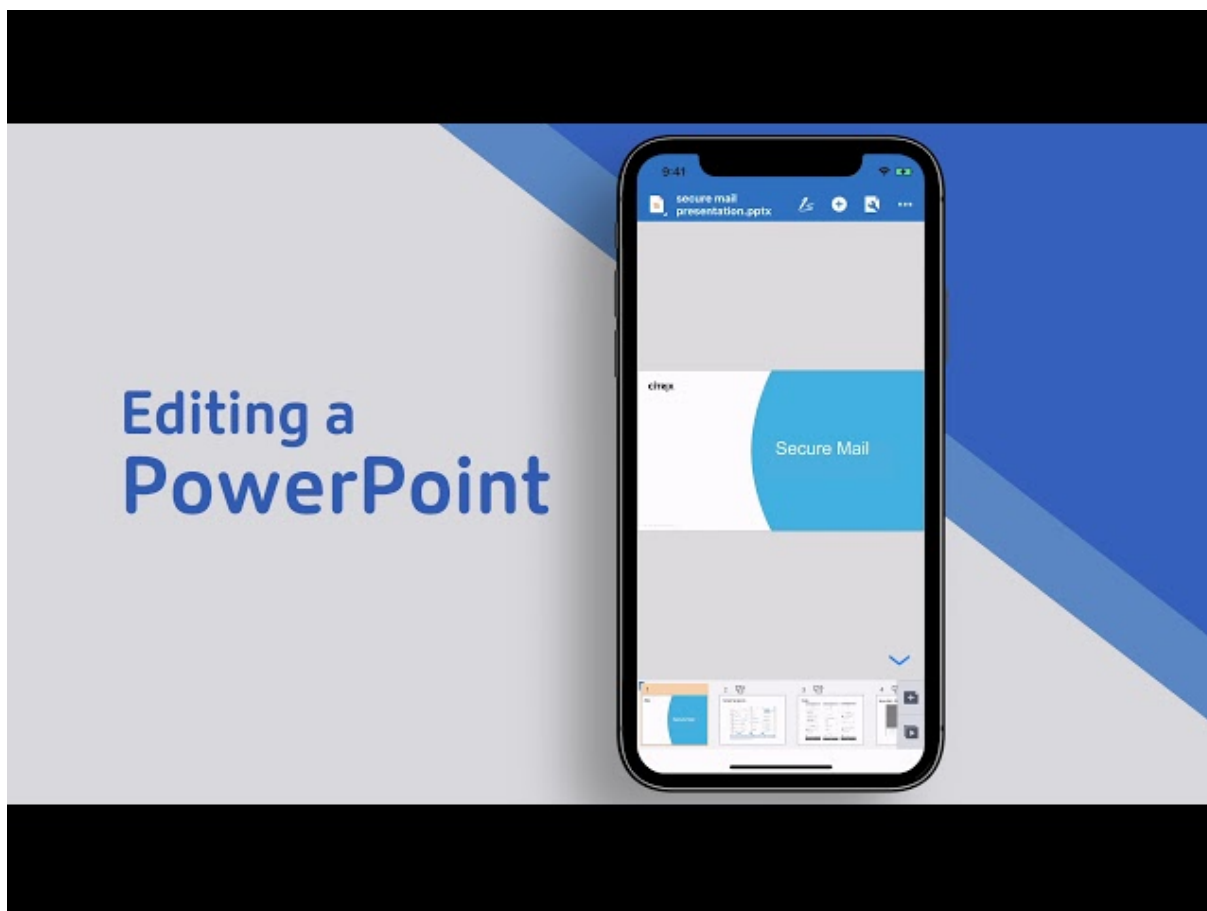
January 14, 2019

Citrix QuickEdit est l'outil de modification de choix pour les applications de productivité mobiles. Sa compatibilité avec Citrix Secure Mail et Citrix Files pour Endpoint Management permet un flux de travail transparent au sein de l'environnement Endpoint Management sécurisé.

Remarque :

Mise à jour le 2 juillet 2018 : QuickEdit restera disponible en tant qu'application de productivité mobile. L'état de fin de vie (EOL) ne sera pas appliqué le 1er septembre 2018 comme indiqué précédemment. Au lieu de cela, des mises à jour du composant de gestion de contenu de QuickEdit sont prévues.

Pour visionner une vidéo sur les fonctionnalités de Citrix QuickEdit, consultez la chaîne YouTube Citrix :



Pour connaître la configuration système requise pour QuickEdit et d'autres applications de productivité mobiles, consultez la section [Configuration système requise](#).

Vous pouvez configurer QuickEdit pour qu'il soit automatiquement poussé vers les appareils utilisateur lorsque ces derniers sont enrôlés dans Citrix Secure Hub, ou les utilisateurs peuvent ajouter l'application depuis le magasin d'applications.

QuickEdit est également compatible avec les programmes de messagerie natifs pour faciliter le partage ou le transfert de fichiers, en tant que pièce jointe ou un lien Citrix Files.

Types de fichiers pris en charge

- Microsoft Word (.doc, .docx)
- Microsoft Excel - .xls et .xlsx
- Microsoft PowerPoint (.pptx, .ppt)
- .csv, .txt
- .jpeg, .gif, .png, .svg, .bmp

Les types de fichiers suivants sont obsolètes depuis la dernière version : .docm, .xlsm, .pptm et .rft.

Intégration et mise à disposition de QuickEdit

Pour intégrer et délivrer QuickEdit avec Endpoint Management, suivez ces étapes :

1. Vous pouvez également activer l'authentification unique (SSO) à partir de Secure Hub. Pour ce faire, configurez les informations de compte Citrix Files dans Endpoint Management afin d'activer Endpoint Management en tant que fournisseur d'identité SAML pour Citrix Files.

La configuration des informations du compte Citrix Files dans Endpoint Management ne doit être effectuée qu'une seule fois pour tous les clients Endpoint Management, Citrix Files et Citrix Files non-MDX. Pour plus d'informations, voir [Intégration et mise à disposition des clients Citrix Files](#).

2. Téléchargez QuickEdit.
 - Vous pouvez télécharger QuickEdit depuis la [page de téléchargements de Endpoint Management](#).
 - QuickEdit est également disponible pour les nouveaux utilisateurs sur la plate-forme Citrix Workspace. Pour plus de détails, voir [Plate-forme Citrix Workspace](#).
3. Ajoutez QuickEdit à Endpoint Management à l'aide des mêmes étapes que pour d'autres applications MDX. Pour de plus amples informations, consultez la section [Ajouter des applications](#).

Problèmes résolus et connus dans la version actuelle

Les problèmes suivants sont connus ou résolus dans la dernière version.

Problèmes résolus

- Lorsque vous essayez d'envoyer des fichiers à Secure Mail à partir de QuickEdit pour iOS ou ScanDirect, le transfert échoue. Pour résoudre ce problème, ajoutez l'exclusion de cryptage de fichiers suivante aux paramètres de stratégie pour ces applications : "/tmp/.com.apple.Pasteboard". (Trouvé dans la version 6.14)

Problèmes connus

- Si la taille d'une page dépasse 10 000 points (hauteur ou largeur), les documents ne s'ouvrent pas afin d'éviter une erreur de mémoire potentielle.
- Les signatures numériques et les images en ligne ne sont pas prises en charge avec QuickEdit.
- Sur QuickEdit sur les appareils iOS 12, lorsque les utilisateurs créent un fichier, un problème de type "En raison d'une mémoire insuffisante" apparaît.
- Les utilisateurs ne peuvent pas voir les annotations dans les fichiers PDF à moins d'ouvrir le fichier en mode Édition, puis de sélectionner l'option Annotations.
- Lorsque les utilisateurs ouvrent un fichier PDF de plus de 150 Mo, un message d'erreur "Fichier non pris en charge" apparaît.
- Sur QuickEdit sur iPad, en mode Édition, le clavier ne s'affiche pas comme prévu.
- Les utilisateurs ne peuvent pas créer de fichier PowerPoint (.ppt) comprenant plusieurs photos.

Limitation connue

QuickEdit n'est pas pris en charge pour les appareils partagés. Si des utilisateurs disposaient d'une version plus ancienne de QuickEdit et sont connectés avec un utilisateur sur un appareil partagé, un problème sérieux peut survenir. S'ils tentent de mettre à jour QuickEdit pour iOS versions 7.4.0, les fichiers et dossiers existants gérés localement à partir de QuickEdit sont perdus. Les données de Citrix Files ne sont toutefois pas affectées.

ShareConnect

March 12, 2019

Avec ShareConnect, les utilisateurs peuvent se connecter à leurs ordinateurs en toute sécurité au travers d'iPads, de tablettes et de téléphones Android pour accéder à leurs fichiers et applications. Les utilisateurs peuvent effectuer les opérations suivantes :

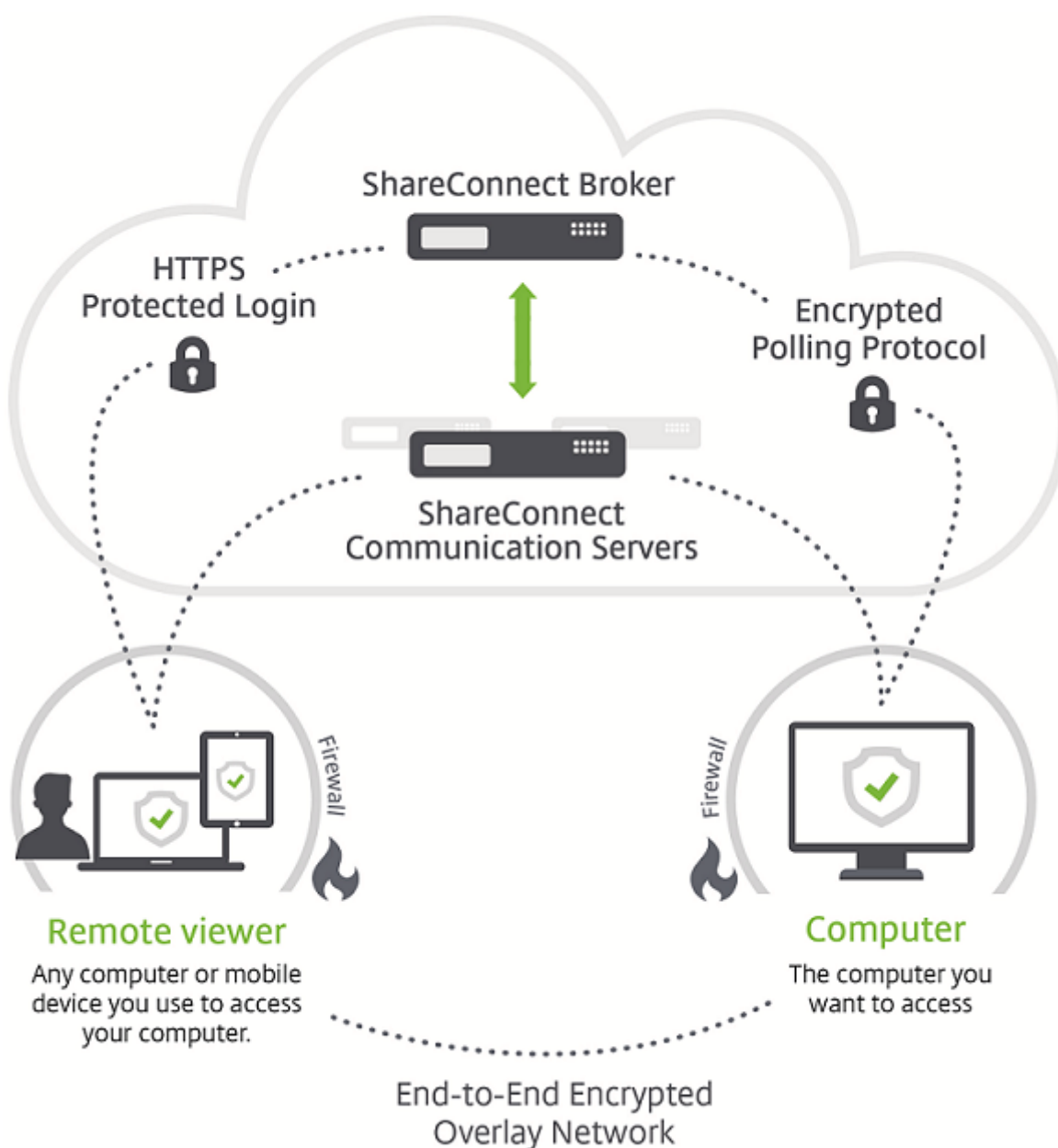
- Travailler sur des fichiers qui résident sur leur ordinateur et sur des lecteurs réseau connectés
- Exécuter des applications à partir de la machine cible dans ShareConnect.
- Avoir accès aux applications mobiles, sans qu'il soit nécessaire d'encapsuler d'autres applications de productivité mobiles.
- Exécuter ShareConnect sur Citrix Virtual Desktops pour bénéficier d'un accès optimisé.

Vous pouvez télécharger la version MDX de ShareConnect à partir de la page des [téléchargements de Endpoint Management](#).

Pour de plus amples informations sur la façon d'installer et utiliser ShareConnect, consultez le [centre de connaissances Citrix](#).

Aperçu de l'architecture

Les composants ShareConnect incluent le broker ShareConnect Citrix et les serveurs de communication ShareConnect, comme illustré dans la figure suivante. Le broker ShareConnect est une base de données et un serveur d'application qui mappent les utilisateurs sur les ordinateurs et leur indique si leur ordinateur hôte est en ligne ou déconnecté. Les serveurs de communication ShareConnect sont utilisés pour échanger des données entre les ordinateurs hôtes et les ordinateurs clients. Ces données peuvent transiter via un tunnel micro VPN sécurisé entre les ordinateurs hôtes et les ordinateurs clients ; cela dépend des paramètres Endpoint Management.



En outre, Citrix Files peut fournir l'authentification via SSO aux utilisateurs avec un fournisseur d'identité SAML (IdP), tel que Endpoint Management ou Active Directory Federation Services (ADFS). L'accès aux ressources en dehors du réseau est fourni via Citrix Gateway dans un déploiement Endpoint Management.

Fonctionnement des connexions dans ShareConnect

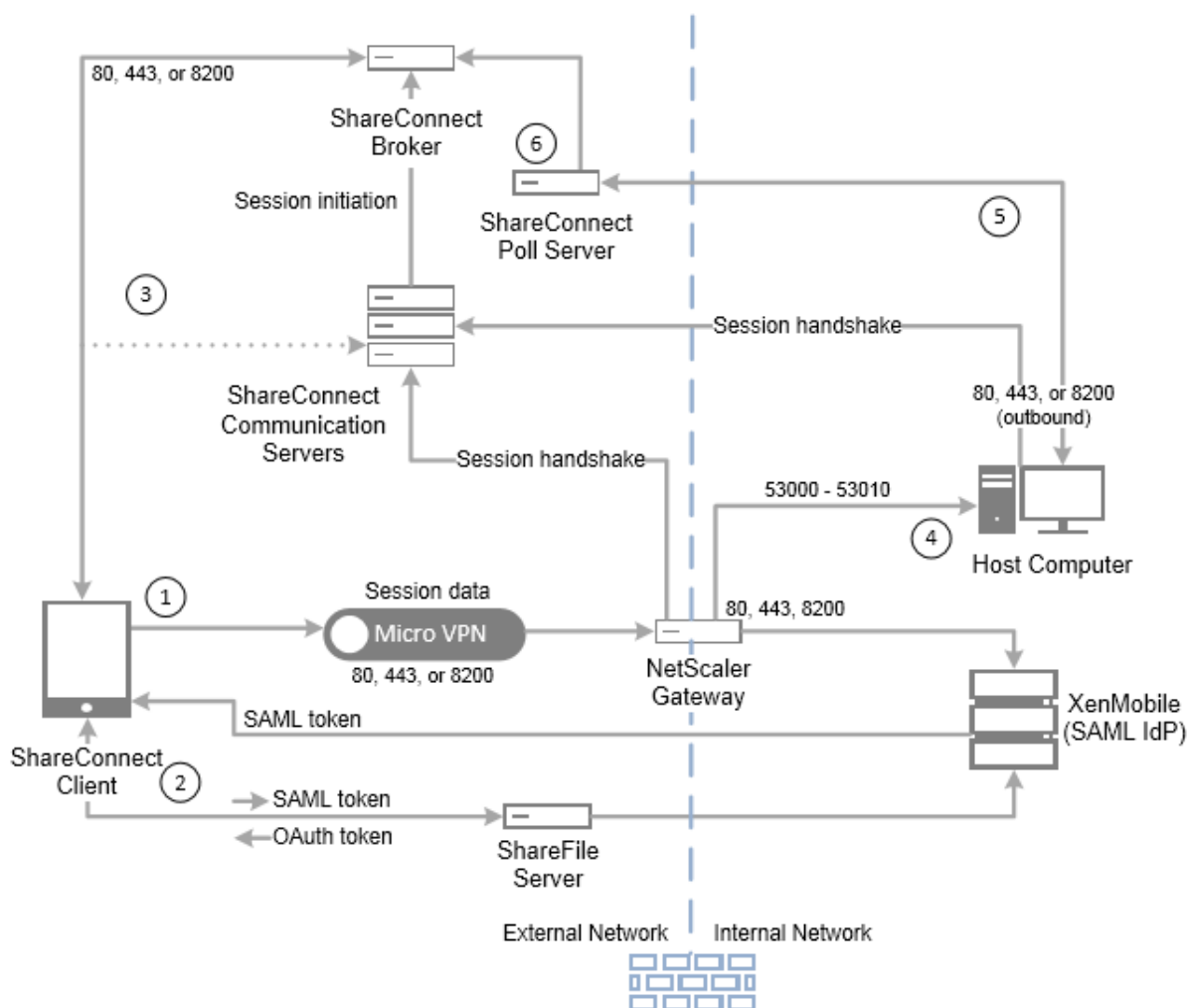
ShareConnect établit des connexions directes ou indirectes :

- **Connexions directes.** ShareConnect établit une connexion directe entre l'ordinateur client et

l'ordinateur hôte s'ils se trouvent sur le même réseau local ou réseau Wi-Fi. Dans ce scénario, les données transitent directement entre l'ordinateur client ou l'appareil mobile utilisé pour accéder à un ordinateur hôte. Les données ne circulent pas au travers des serveurs de communication ShareConnect, ce qui entraîne des performances optimales. Pour les connexions directes, Endpoint Management utilise Citrix Gateway pour sécuriser l'accès aux ressources en dehors du réseau local.

- **Connexions indirectes.** ShareConnect établit une connexion indirecte entre l'ordinateur client et l'ordinateur hôte s'ils ne sont pas directement accessibles. Dans ce scénario, les données circulent via les serveurs de communication ShareConnect.

La figure suivante illustre les connexions utilisées lorsque des utilisateurs accèdent à un ordinateur hôte à partir d'un ordinateur ou d'un appareil mobile exécutant ShareConnect à l'aide de connexions directes. Les étapes de connexion sont décrites après la figure.



☒ Dans ce scénario, Endpoint Management est configuré pour agir en tant que fournisseur d'identité SAML pour Citrix Files, afin de fournir l'authentification unique (SSO) à partir de Worx Home. Share-

Connect demande un jeton SAML auprès de Worx Home, qui à son tour transmet la demande à Endpoint Management via Citrix Gateway. Endpoint Management envoie ensuite le jeton SAML à ShareConnect.

☒ ShareConnect envoie le jeton SAML à Citrix Files à des fins de validation et pour échanger le jeton SAML avec un jeton OAuth.

☒ ShareConnect envoie le jeton OAuth au broker ShareConnect, qui envoie un jeton de session à ShareConnect.

☒ ShareConnect obtient une liste des ordinateurs hôtes depuis le broker ShareConnect et demande la saisie des informations d'identification de l'ordinateur hôte. ShareConnect établit ensuite une connexion directe au serveur de communication ShareConnect. Une fois que l'ordinateur hôte a validé les informations d'identification, ShareConnect obtient une liste des fichiers et applications depuis l'ordinateur hôte. Dès qu'un utilisateur ouvre un fichier ou une application, une connexion directe est établie entre ShareConnect et l'ordinateur hôte.

☒ L'agent ShareConnect sur l'ordinateur hôte envoie des messages d'état au serveur d'interrogation ShareConnect pour indiquer s'il est connecté ou déconnecté.

☒ Le serveur d'interrogation ShareConnect envoie des demandes de répartition de la charge depuis l'agent ShareConnect vers le broker ShareConnect et envoie des mises à jour de l'état au broker ShareConnect.

Sécurité ShareConnect

ShareConnect utilise un cryptage AES 128 bits de façon à crypter de bout en bout toutes les données envoyées entre le client ShareConnect et un ordinateur hôte exécutant l'agent ShareConnect. La clé de cryptage est unique à chaque connexion. Même les périphériques les plus sophistiqués ne peuvent pas intercepter les données requises pour décoder le cryptage.

Vous configurez généralement ShareConnect de manière à ce que les données soient acheminées directement entre le client ShareConnect et un ordinateur hôte. Les données ne transitent pas via les serveurs de communication ShareConnect sauf si vous configurez la stratégie Accès réseau afin de permettre un accès illimité. Pour plus d'informations sur les stratégies, voir [Ajouter ShareConnect à Endpoint Management](#) dans cet article.

Pour les connexions directes et indirectes, les métadonnées cryptées, telles que les adresses IP et les ports requis pour établir des connexions, sont envoyées aux serveurs ShareConnect.

Par ailleurs, l'encapsulation MDX de ShareConnect permet de crypter les données via le MDX Vault qui crypte les applications MDX encapsulées et les données stockées associées sur les appareils iOS (antérieurs à iOS 9) et Android à l'aide des modules cryptographiques certifiés FIPS fournis par OpenSSL.

Vous trouverez des informations sur les paramètres de sécurité et les commandes d'administration dans l'article technique dont le lien est fourni ci-dessous.

[Article technique sur la sécurité ShareConnect](#)

[Guide de l'administrateur ShareConnect](#)

Exigences requises par ShareConnect en matière de port

Vous devez ouvrir les ports suivants pour autoriser les communications ShareConnect. Les exigences en matière de port diffèrent selon le type de connexion, c-à-d des connexions directes (si les ordinateurs sont sur le même réseau LAN ou Wi-Fi) ou indirectes (si les ordinateurs hôtes et les ordinateurs clients ne peuvent pas communiquer directement entre eux).

Pour les connexions directes

Port TCP 80 - Utilisé pour les connexions sortantes depuis Citrix Gateway vers app.shareconnect.com.

Source - Citrix Gateway

Destination - app.shareconnect.com

Port TCP 80, 443, 8200 - Au moins un de ces ports est requis pour les connexions sortantes depuis Citrix Gateway vers le serveur de communication ShareConnect.

Source - Citrix Gateway

Destination - Serveurs de communication ShareConnect

Port TCP 80, 443, 8200 - Utilisé pour les connexions sortantes depuis les ordinateurs hôtes ShareConnect vers les serveurs Citrix.

Source - Ordinateurs hôtes ShareConnect

Destination - poll.shareconnect.com, Serveurs de communication ShareConnect

Port TCP 443 - Utilisé pour les connexions sortantes depuis Citrix Gateway vers les sites requis.

Source - Citrix Gateway

Destination - crashlytics.com, secure.sharefile.com, ShareFile_sub-domain.sharefile.com

Port TCP 53000 - 53010 - Utilisé pour les connexions sortantes depuis Citrix Gateway vers les ordinateurs hôtes ShareConnect.

Source - Citrix Gateway

Destination - Ordinateurs hôtes ShareConnect basés sur réseau local

Port TCP 53000 - 53010 - Utilisé pour les connexions entrantes depuis Citrix Gateway vers les ordinateurs hôtes ShareConnect.

Source - Citrix Gateway

Destination - Ordinateurs hôtes ShareConnect basés sur réseau local

Pour les connexions indirectes

Port TCP 80 - Utilisé pour les connexions sortantes depuis l'agent ShareConnect vers app.shareconnect.com.

Source - Agent ShareConnect

Destination - app.shareconnect.com

Port TCP 80, 443, 8200 - Au moins un de ces ports est requis pour les connexions sortantes depuis l'agent ShareConnect vers le serveur de communication ShareConnect.

Source - Agent ShareConnect

Destination - Serveurs de communication ShareConnect

Port TCP 80, 443, 8200 - Utilisé pour les connexions sortantes depuis les ordinateurs hôtes ShareConnect vers les serveurs Citrix.

Source - Ordinateurs hôtes ShareConnect

Destination - poll.shareconnect.com, Serveurs de communication ShareConnect

Port TCP 443 - Utilisé pour les connexions sortantes depuis l'agent ShareConnect vers les sites requis.

Source - Agent ShareConnect

Destination - crashlytics.com, secure.sharefile.com, ShareFile_sub-domain.sharefile.com

Intégration et mise à disposition de ShareConnect

Pour intégrer et délivrer ShareConnect avec Endpoint Management, suivez ces étapes :

1. Vous pouvez également activer l'authentification unique (SSO) à partir de Worx Home. Pour ce faire, vous configurez les informations de compte Citrix Files dans Endpoint Management afin d'activer Endpoint Management en tant que fournisseur d'identité SAML pour Citrix.

La configuration des informations du compte Citrix Files dans Endpoint Management ne doit être effectuée qu'une seule fois pour tous les clients d'applications de productivité mobiles, clients Citrix Files Worx et clients Citrix Files non-MDX.

2. [Téléchargez](#) et encapsulez ShareConnect. Pour de plus amples informations, consultez la section [À propos du MDX Toolkit](#).
3. Ajoutez ShareConnect à Endpoint Management et configurez les stratégies MDX.
4. Installez l'agent ShareConnect sur des ordinateurs hôtes. L'agent ShareConnect est un pack MSI, vous pouvez donc utiliser vos méthodes de déploiement de logiciels existantes pour distribuer et installer l'agent. Les utilisateurs doivent ensuite enregistrer l'ordinateur hôte en se connectant à l'agent à l'aide de leurs informations d'identification Citrix Files dans l'heure qui suit l'installation.

Les utilisateurs peuvent également installer l'agent ShareConnect sur l'ordinateur auquel ils se connecteront avec ShareConnect. Pour de plus amples informations, consultez la section « Pour installer l'agent ShareConnect sur un ordinateur » dans cet article.

Ajouter ShareConnect à Endpoint Management

Ajoutez ShareConnect à Endpoint Management à l'aide des mêmes étapes que pour d'autres applications MDX. Pour de plus amples informations, consultez la section [Ajouter une application MDX](#). Lors de l'ajout de ShareConnect, configurez les stratégies MDX comme indiqué dans le tableau suivant.

Stratégie	Valeur	Résultats
Accès réseau	Tunnélisé vers le réseau interne ou Non restreint	L'option Tunnélisé vers le réseau interne utilise un tunnel VPN par application vers le réseau interne pour tous les accès réseau. Cette configuration établit une configuration directe entre ShareConnect et un ordinateur hôte. L'option Non restreint utilise les serveurs de communication Citrix pour router les données cryptées entre un ordinateur hôte et l'agent ShareConnect. Veillez à tester votre installation avec un accès illimité pour vous assurer que tout fonctionne correctement, même si vous prévoyez d'utiliser l'option Tunnélisé vers le réseau interne pour l'accès réseau.
Mode VPN préféré	Navigation sécurisée	Définit le mode de connexion initiale de manière appropriée pour les connexions qui nécessitent une authentification unique (SSO).

Stratégie	Valeur	Résultats
Activer le chiffrement	Activé	Crypte les données stockées sur la tablette.
Couper et copier	Non restreint	Active les opérations couper/copier pour ShareConnect.
Coller	Non restreint	Active les opérations de collage pour ShareConnect.
Échange de documents (Ouvrir dans)	Non restreint	Autorise les utilisateurs à ouvrir un fichier sur l'ordinateur connecté ou un lecteur réseau connecté depuis ShareConnect.
Enregistrer le mot de passe	Désactivé	Exige que les utilisateurs entrent le nom d'utilisateur et le mot de passe de leur ordinateur chaque fois qu'ils se connectent à ShareConnect.

Pour installer l'agent ShareConnect sur un ordinateur

Les étapes suivantes décrivent comment un utilisateur installe l'agent ShareConnect sur chaque ordinateur physique ou virtuel auquel il souhaite se connecter à partir d'un appareil mobile pris en charge.

Avant d'effectuer ces étapes, l'utilisateur doit d'abord installer Worx Home et suivre les instructions pour autoriser l'installation d'applications de productivité mobiles sur l'appareil mobile pris en charge.

1. Connectez-vous à Worx Home sur la tablette.
2. Ouvrez ShareConnect.
3. Tapotez le lien de téléchargement de l'e-mail.
Citrix envoie un e-mail à no-reply@shareconnect.com.
4. À partir de l'ordinateur hôte auquel vous voulez accéder à partir de ShareConnect, ouvrez l'e-mail.
5. Dans l'e-mail, cliquez sur Set up this computer.

6. Double-cliquez sur **ShareConnect_Installer.exe** pour commencer l'installation.

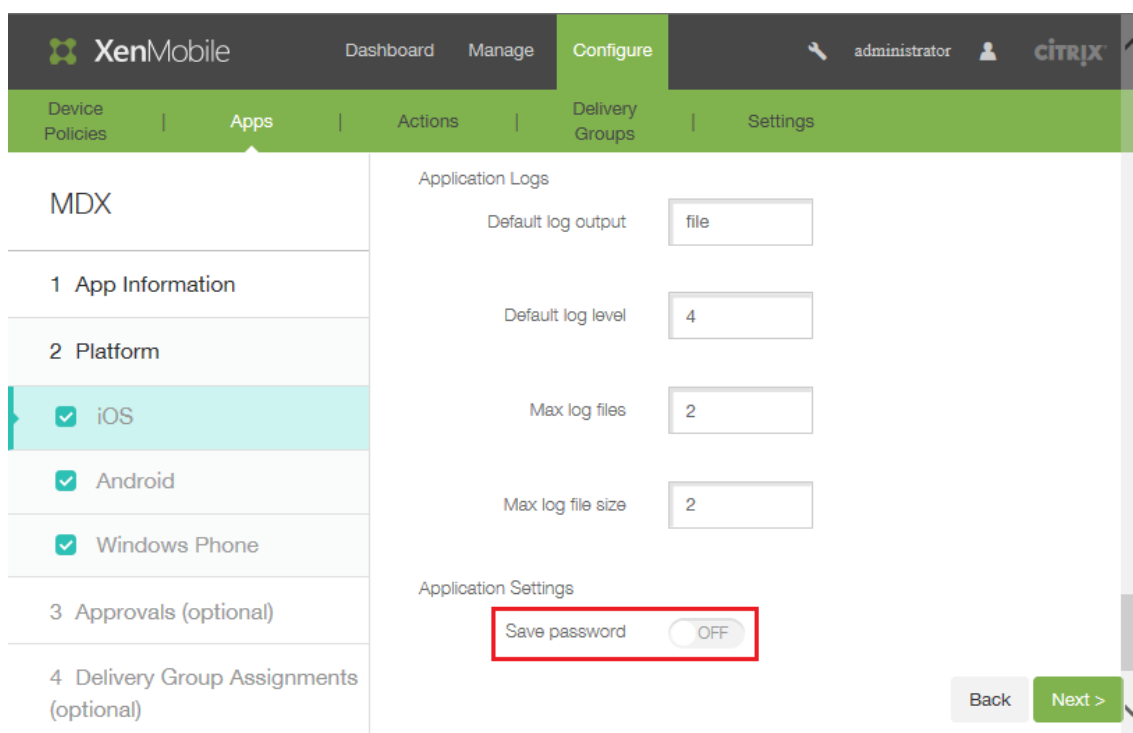
L'agent ShareConnect s'installe sur votre ordinateur hôte. Durant l'installation, ShareConnect invite les utilisateurs à saisir une adresse e-mail (si l'authentification unique à Citrix Files est configurée) ou les informations d'identification Citrix Files (si l'authentification unique à Citrix Files n'est pas configurée).

7. Suivez les instructions fournies dans les assistants ShareConnect et de mise en route.

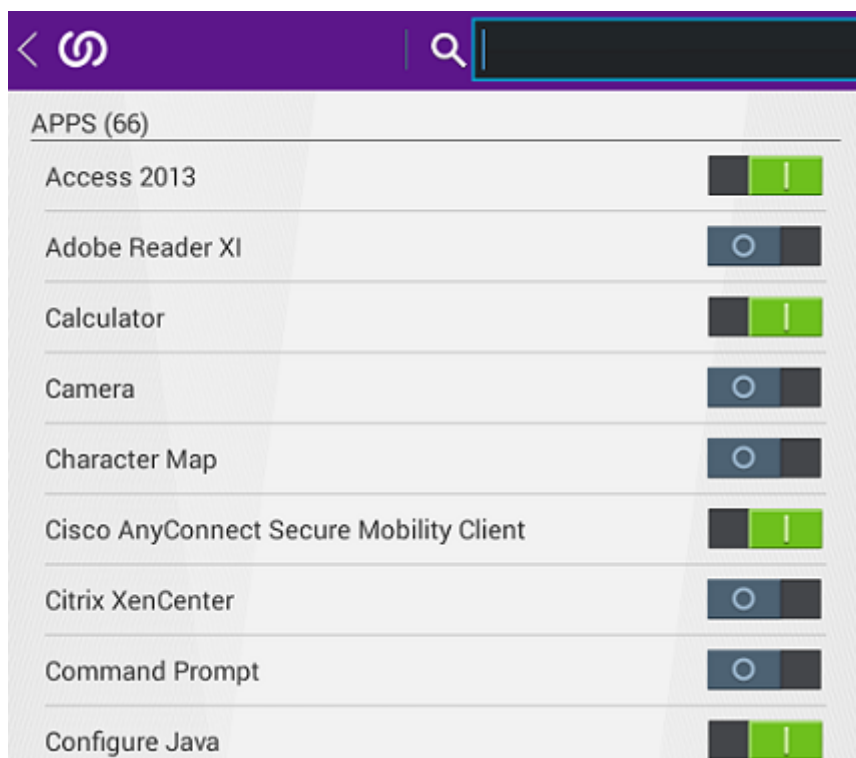
L'agent ShareConnect enregistre ensuite l'ordinateur hôte, qui peut se connecter à partir d'un client ShareConnect à condition que l'ordinateur hôte soit sous tension et qu'il puisse contacter poll.shareconnect.com sur au moins un port publié (80, 443 ou 8200).

Fonctionnalités ShareConnect

- **Ajouter des ordinateurs hôtes.** Les utilisateurs peuvent ajouter des ordinateurs hôtes distants et s'y connecter depuis des appareils mobiles pris en charge à l'aide de ShareConnect.
- **Accéder aux fichiers.** Les utilisateurs peuvent afficher une liste des fichiers récents et rechercher des fichiers sur leur ordinateur hôte et des lecteurs connectés.
- **Modifier les fichiers.** Depuis des tablettes, les utilisateurs peuvent accéder à des applications de bureau sur leurs ordinateurs hôtes pour modifier les fichiers. Les utilisateurs peuvent travailler avec les applications en plein écran.
- **Partage d'écran.** Au lieu de visualiser un seul fichier ou une seule application, les utilisateurs peuvent utiliser la fonctionnalité de partage d'écran pour afficher le bureau de leur ordinateur hôte.
- **Intégration de Citrix Files.** Les utilisateurs peuvent déplacer ou partager des fichiers entre l'ordinateur hôte et Citrix Files.
- **Clavier et souris.** ShareConnect prend en charge l'utilisation simultanée d'un clavier Bluetooth et du prototype de souris Citrix XI.
- **Ports restreints.** ShareConnect utilise les ports 53000 à 53010 uniquement.
- **Mots de passe obligatoires pour chaque connexion.** Pour une sécurité accrue, vous pouvez configurer cette option pour demander aux utilisateurs d'entrer leur mot de passe d'ordinateur chaque fois qu'ils ouvrent une session sur ShareConnect. Lorsque la stratégie Enregistrer le mot de passe est désactivée, comme illustré dans la figure suivante, les utilisateurs sont obligés d'entrer leurs informations d'identification à chaque connexion.



- **Ajouter ou supprimer des applications.** Les utilisateurs peuvent ajouter ou supprimer des applications à partir de la barre d'applications dans ShareConnect en basculant le commutateur en regard de chaque application pour la sélectionner ou la désélectionner.



- **Mettre en cache un aperçu des fichiers.** ShareConnect met en cache les fichiers qui ont déjà

été accédés de façon à ce que les fichiers n'aient pas à être téléchargés à nouveau si les utilisateurs affichent l'aperçu d'autres fichiers, puis reviennent à une version antérieure de ceux-ci. Cette fonctionnalité améliore le temps de chargement lorsque les utilisateurs accèdent à des fichiers ultérieurement.

Résolution des problèmes ShareConnect

Problèmes d'installation de l'agent ShareConnect

Problème	Description et résolution
Si un utilisateur télécharge l'agent ShareConnect et attend une heure ou plus avant de commencer l'installation, il doit entrer son nom et son mot de passe de compte Citrix Files pour enregistrer l'agent ShareConnect.	Le programme d'installation de l'agent ShareConnect contient un jeton qui expire une heure après le téléchargement. Si un utilisateur ne lance pas l'installation avant que le jeton n'expire, il doit se connecter à son compte Citrix Files à deux reprises, la première fois pour enregistrer l'agent ShareConnect et la deuxième fois pour se connecter à l'agent après la fin de l'installation. Si les utilisateurs téléchargent et installent l'agent ShareConnect dans l'heure qui suit, ils ne doivent se connecter qu'une seule fois.
Durant l'enregistrement de l'agent ShareConnect, l'agent ne se connecte pas et un message d'erreur du style « Vérifiez votre connexion et réessayez. » s'affiche.	Vérifiez que le port vers poll.shareconnect.com n'est pas bloqué. Pour de plus amples informations, consultez la section Configuration requise plus haut dans cet article.

Profils de connexion ShareConnect

Important :

Citrix recommande de tester ShareConnect en définissant la stratégie Accès réseau sur **Non restreint** pour exclure les problèmes liés aux ports et aux paramètres réseau. L'accès illimité oblige ShareConnect à se connecter via le serveur de communication ShareConnect, ce qui vous permet généralement de tester la connexion si l'appareil mobile ShareConnect et l'ordinateur hôte disposent d'un accès Internet.

Problème	Description et résolution
ShareConnect démarre, mais ne se connecte pas à l'ordinateur hôte et n'invite pas les utilisateurs à entrer leurs informations d'identification.	Vérifiez que votre installation répond aux conditions requises par les ports détaillés plus haut dans cet article sous Configuration requise.
Les utilisateurs ne peuvent pas se connecter à ShareConnect à l'aide de leurs informations d'identification au compte Citrix Files.	L'authentification unique à Citrix Files nécessite que votre compte ShareFile soit configuré avec un fournisseur d'identité SAML. Pour plus d'informations sur l'utilisation de Endpoint Management en tant que fournisseur d'identité SAML, voir Citrix Files pour Endpoint Management . Pour de plus amples informations sur la configuration d'autres fournisseurs d'identité, consultez cet article du centre de connaissances . Si l'authentification unique n'est pas configurée pour votre compte, ShareConnect pour iOS invite les utilisateurs à entrer leur nom d'utilisateur et mot de passe Citrix Files.
Une fois que les utilisateurs se sont connectés à ShareConnect, ShareConnect ne peut pas se connecter à l'ordinateur hôte.	Lorsque ShareConnect est configuré pour des connexions directes (en d'autres termes, la stratégie Accès réseau est définie sur Tunnélisé vers le réseau interne), des échecs de connexion peuvent se produire si des restrictions sont imposées dans les paramètres réseau, par exemple dans le cas où des pare-feu ou des serveurs proxy sont configurés.

Citrix ShareFile Workflows

October 30, 2018

Remarque :

Secure Forms a atteint la fin de son cycle de vie le 31 mars 2018. Nous vous recommandons d'utiliser ShareFile WorkFlows inclus avec les comptes Citrix Files Platinum et Premium.

ShareFile Workflows est le composant mobile de la fonctionnalité Workflows personnalisés de Citrix

Files. Cette fonctionnalité permet aux utilisateurs de créer des workflows personnalisés qui incluent plusieurs déclencheurs et actions. Des formulaires personnalisés peuvent être ajoutés à des modèles de workflow et affectés aux utilisateurs.

Lorsqu'un utilisateur est affecté à un formulaire, l'utilisateur peut compléter et envoyer le formulaire via l'application mobile ShareFile Workflows. Le stockage des données de formulaire est intégré en toute sécurité à Citrix Files, où sont stockés les fichiers de workflow pour consultation, référence et récupération.

Les modèles de formulaire et de workflow sont créés et gérés au sein de l'application Web Citrix Files.

Documentation utilisateur

La documentation utilisateur liée à la création et à la gestion des modèles de workflow et de formulaire est disponible dans le centre de connaissances Citrix :

- [Création d'un modèle de workflow](#)
- [Création d'un modèle de formulaire](#)
- [Envoi de formulaires via l'application mobile Workflows](#)

Citrix Files pour Endpoint Management

December 10, 2018

Citrix ShareFile pour Endpoint Management est maintenant Citrix Files pour Endpoint Management. Citrix Files est un service de partage et de synchronisation de fichiers d'entreprise qui permet aux utilisateurs d'échanger des documents de manière simple et sécurisée. Citrix Files offre aux utilisateurs plusieurs options d'accès, y compris des clients mobiles Citrix Files, tels que Citrix Files pour Android Phone et Citrix Files pour iPad.

Vous pouvez intégrer Citrix Files à Endpoint Management pour fournir l'ensemble des fonctionnalités de Citrix Files ou pour fournir un accès uniquement aux connecteurs de zones de stockage. Par défaut, la console Endpoint Management active uniquement la configuration de Citrix Files. Pour configurer Endpoint Management pour une utilisation avec les connecteurs de zones de stockage, consultez la section [Intégration de Citrix Files à Endpoint Management](#) dans la documentation de Citrix Endpoint Management.

Les clients Citrix Files pour Endpoint Management sont des versions compatibles MDX des clients mobiles Citrix Files. Ces clients fournissent un accès sécurisé et intégré aux données dans d'autres applications MDX encapsulées. Les clients Citrix Files pour Endpoint Management bénéficient également des fonctionnalités MDX, telles que le micro VPN, l'authentification unique (SSO) avec Secure Hub et l'authentification à deux facteurs.

Utilisez Endpoint Management, Citrix Files, le contrôleur de zones de stockage et Citrix ADC comme suit pour déployer et gérer les clients Citrix Files pour Endpoint Management :

- Lorsque Endpoint Management est configuré avec Citrix Files, Endpoint Management agit en tant que fournisseur d'identité SAML (IdP) et déploie Citrix Files pour les clients Endpoint Management. Citrix Files gère les données de Citrix Files. Aucune donnée de Citrix Files ne transite par Endpoint Management.
- Lorsque Endpoint Management est configuré avec Citrix Files ou avec des connecteurs de zones de stockage, le contrôleur de zones de stockage fournit la connectivité aux données dans les partages réseau et SharePoint. Les utilisateurs accèdent à vos données stockées via les applications de productivité mobiles Citrix Files. Les utilisateurs peuvent modifier des documents Microsoft Office, ainsi qu'afficher un aperçu et annoter des fichiers Adobe PDF depuis des appareils mobiles.
- Citrix ADC gère les demandes des utilisateurs externes, en sécurisant leurs connexions, en répartissant les demandes et en gérant la commutation de contenu des connecteurs de zones de stockage.

Pour télécharger les clients Citrix Files pour Endpoint Management, consultez la [page des téléchargements sur Citrix.com](#).

Pour connaître la configuration système requise pour Citrix Files pour Endpoint Management et pour d'autres applications de productivité mobiles, consultez la section [Prise en charge des applications de productivité mobiles](#).

Différences entre les clients Citrix Files pour Endpoint Management et les clients mobiles Citrix Files

La section suivante décrit les différences entre les clients Citrix Files pour Endpoint Management et les clients mobiles Citrix Files.

Accès des utilisateurs

Clients Citrix Files pour Endpoint Management :

Les utilisateurs obtiennent et ouvrent les clients Citrix Files pour Endpoint Management à partir de Secure Hub.

Clients mobiles Citrix Files :

Les utilisateurs obtiennent les clients mobiles Citrix Files à partir des magasins d'applications.

Authentification unique (SSO)

Clients Citrix Files pour Endpoint Management :

Pour l'intégration de Endpoint Management avec Citrix Files : vous pouvez configurer Endpoint Management en tant que fournisseur d'identité SAML pour Citrix Files. Dans cette configuration, Secure Hub obtient un jeton SAML pour le client Citrix Files pour Endpoint Management, en utilisant Endpoint Management comme fournisseur d'identité SAML. Un utilisateur qui démarre le client Citrix Files pour Endpoint Management, mais qui n'est pas connecté à Secure Hub, est invité à s'y connecter. L'utilisateur n'a pas besoin de connaître son domaine Citrix Files ou les informations de compte.

Clients mobiles Citrix Files :

Vous pouvez configurer Endpoint Management et Citrix Gateway en tant que fournisseur d'identité SAMP pour Citrix Files. Dans cette configuration, un utilisateur qui se connecte à Citrix Files à l'aide d'un navigateur Web ou d'autres clients Citrix Files est redirigé vers l'environnement Endpoint Management pour authentifier l'utilisateur. Une fois l'authentification par Endpoint Management réussie, l'utilisateur reçoit un jeton SAML valide pour la connexion à son compte Citrix Files.

Micro VPN

Clients Citrix Files pour Endpoint Management :

Les utilisateurs distants peuvent se connecter à l'aide d'un VPN ou d'une connexion micro VPN via Citrix Gateway pour accéder à des applications et des bureaux dans le réseau interne. Cette fonctionnalité, disponible au travers de l'intégration de Citrix ADC avec Endpoint Management, est transparente pour les utilisateurs.

Clients mobiles Citrix Files :

Sans objet.

Authentification à deux facteurs

Clients Citrix Files pour Endpoint Management :

L'intégration de Citrix ADC avec Endpoint Management prend également en charge l'authentification à l'aide d'une combinaison d'authentification du certificat client et d'un autre type d'authentification, telle que LDAP ou RADIUS.

Clients mobiles Citrix Files :

Sans objet.

Autorisations d'accès au dossier

Clients Citrix Files pour Endpoint Management et clients mobiles Citrix Files :

Pour l'intégration de Endpoint Management avec Citrix Files : déterminé par Citrix Files.

Protection d'accès aux documents

Clients Citrix Files pour Endpoint Management :

Les utilisateurs peuvent ouvrir des pièces jointes reçues dans Secure Mail ou téléchargées par une application MDX encapsulée. Seules les applications MDX encapsulées s'affichent lorsque l'utilisateur effectue une action Ouvrir dans. Les clients Citrix Files pour Endpoint Management n'ont pas accès aux données provenant d'une application non encapsulée. Les utilisateurs Secure Mail peuvent joindre des fichiers à partir de leur référentiel Citrix Files sans avoir à les télécharger sur l'appareil. Si un utilisateur dispose d'un client Citrix Files encapsulé et non encapsulé sur un appareil, le client Citrix Files encapsulé ne peut pas accéder aux fichiers dans le compte Citrix Files personnel de l'utilisateur. Le client Citrix Files encapsulé ne peut accéder qu'au sous-domaine Citrix Files configuré dans Endpoint Management.

Clients mobiles Citrix Files :

Les utilisateurs peuvent ouvrir des pièces jointes à partir de n'importe quelle application.

Accès au compte Citrix Files

Clients Citrix Files pour Endpoint Management :

Pour l'intégration de Endpoint Management à Citrix Files : pour accéder à un compte personnel Citrix Files ou à un compte tiers Citrix Files, les utilisateurs doivent utiliser une version non MDX de Citrix Files sur l'appareil.

Clients mobiles Citrix Files :

Pour l'intégration de Endpoint Management avec Citrix Files : disponible depuis les clients Citrix Files.

Stratégies d'appareil

Clients Citrix Files pour Endpoint Management et clients mobiles Citrix Files :

Les stratégies Endpoint Management et Citrix Files s'appliquent aux clients Citrix Files pour Endpoint Management. Par exemple, à partir de la console Endpoint Management, vous pouvez effectuer une réinitialisation de l'appareil. À partir de la console de Citrix Files, vous pouvez supprimer à distance l'application Citrix Files.

Stratégies MDX

Clients Citrix Files pour Endpoint Management :

Les stratégies MDX vous permettent de configurer les paramètres dans Citrix Endpoint Management que le magasin d'applications Endpoint Management applique. Les stratégies disponibles uniquement via MDX permettent de bloquer l'appareil photo, le micro, la composition d'e-mail, la capture d'écran et les opérations de couper, copier et coller dans le presse-papiers.

Clients mobiles Citrix Files :

Sans objet.

Cryptage des données

Clients Citrix Files pour Endpoint Management et clients mobiles Citrix Files :

Crypte toutes les données stockées avec AES-256 et protège les données en transit à l'aide de SSL 3.0 et un cryptage minimum de 128 bits.

Disponibilité

Clients Citrix Files pour Endpoint Management :

Les clients Citrix Files pour Endpoint Management sont inclus dans les éditions Endpoint Management Advanced et Enterprise.

Clients mobiles Citrix Files :

Toutes les éditions de Endpoint Management incluent toutes les fonctionnalités de Citrix Files. Vous pouvez intégrer Endpoint Management avec l'ensemble des fonctionnalités de Citrix Files ou uniquement avec les connecteurs de zones de stockage.

Intégration et mise à disposition des clients Citrix Files Endpoint Management

Pour intégrer et délivrer les clients Citrix Files avec Endpoint Management, suivez ces étapes :

1. Activez Endpoint Management en tant que fournisseur d'identité SAML pour Citrix Files, afin de fournir une authentification unique à partir de clients Citrix Files vers Citrix Files. Pour ce faire, vous devez configurer les informations de compte Citrix Files dans Endpoint Management, comme décrit dans cet article « Pour configurer des informations de compte Citrix Files dans Endpoint Management pour l'authentification unique (SSO) ».

Important :

Pour utiliser Endpoint Management comme fournisseur d'identité SAML pour les clients Citrix Files autres que MDX, tels que l'application Web Citrix Files et les clients Citrix Files Sync, une configuration supplémentaire est requise. Pour plus d'informations, consultez cet article sur le site de support de Citrix Files :

[Citrix Files \(ShareFile\) Single Sign-On SSO](#). Cet article contient un lien de téléchargement du guide de configuration de Endpoint Management.

2. Téléchargez les clients Citrix Files.
3. Ajoutez les clients Citrix Files à Endpoint Management. Pour plus de détails, voir "Pour ajouter Citrix Files à Endpoint Management" plus loin dans cet article.
4. Validez votre configuration. Pour de plus amples informations, consultez la section « Pour valider des clients Citrix Files » dans cet article.

The screenshot shows the 'ShareFile' configuration page in the Citrix Endpoint Management console. The page is titled 'ShareFile' and contains the following fields and controls:

- Domain ***: A text input field containing 'subdomain.sharefile.com'.
- Assign to delivery groups**: A search box with the placeholder text 'Type to search' and a magnifying glass icon. A blue 'Search' button is to the right of the search box. Below the search box is a list of delivery groups with checkboxes: AllUsers, Android, AFW, iOS, Mac, Windows, and win.
- ShareFile Administrator Account Logon**: A section with two text input fields: 'User name *' containing 'Enter User Name' and 'Password *' containing '*****'. Below these fields is a green 'Test Connection' button.
- User account provisioning**: A toggle switch currently set to 'OFF'.
- At the bottom right, there are 'Cancel' and 'Save' buttons.

À propos des paramètres :

- Domaine est le sous-domaine Citrix Files à utiliser pour les clients.
- Seuls les utilisateurs dans les groupes de mise à disposition sélectionnés pourront accéder en SSO à Citrix Files à partir des clients.

Si un utilisateur d'un groupe de mise à disposition ne possède pas de compte Citrix Files, Endpoint Management met l'utilisateur à disposition dans Citrix Files lorsque vous ajoutez le client

Citrix Files à Endpoint Management.

- Les informations d'identification du compte d'administrateur Citrix Files sont utilisées par Endpoint Management pour enregistrer les paramètres SAML dans le plan de contrôle Citrix Files.

Important :

La configuration qui permet l'authentification unique (SSO) à partir de clients Citrix Files vers Citrix Files n'authentifie pas les utilisateurs sur des partages réseau ou des bibliothèques de documents SharePoint. L'accès à ces sources de données de connecteur nécessite une authentification au domaine Active Directory dans lequel les partages réseau ou les serveurs SharePoint résident.

Pour configurer les informations de compte Citrix Files dans Endpoint Management pour SSO

Pour activer la connexion unique (SSO) à partir de Secure Hub vers les applications de productivité mobiles, vous devez spécifier les informations du compte Citrix Files et du service administrateur Citrix Files dans la console Endpoint Management. Avec cette configuration, Endpoint Management agit en tant que fournisseur d'identité SAML pour Citrix Files, pour les clients d'applications de productivité mobiles, les clients Citrix Files et les clients Citrix Files non-MDX. Lorsqu'un utilisateur démarre un client d'application de productivité mobile, Secure Hub obtient un jeton SAML pour l'utilisateur auprès d'Endpoint Management et l'envoie au client Citrix Files.

Dans la console Endpoint Management, cliquez sur **Configurer > Paramètres**, développez **Plus** et cliquez sur **ShareFile**, qui est l'ancien nom de Citrix Files.

Pour ajouter des clients Citrix Files pour Endpoint Management à Endpoint Management

Lorsque vous ajoutez des clients Citrix Files pour Endpoint Management à Endpoint Management, vous pouvez activer l'accès SSO aux sources de données du connecteur à partir des clients Citrix Files pour Endpoint Management. Pour ce faire, configurez la stratégie Accès réseau et la stratégie Mode VPN préféré comme décrit dans cette section.

Conditions préalables

- Endpoint Management doit pouvoir atteindre votre sous-domaine Citrix Files. Pour tester la connexion, envoyez une requête ping à votre sous-domaine Citrix Files à partir du serveur Endpoint Management.
- Le fuseau horaire de votre compte Citrix Files et celui de l'hyperviseur exécutant Endpoint Management doivent être identiques. Si les fuseaux horaires diffèrent, les demandes SSO peuvent

échouer car le jeton SAML ne peut pas accéder à Citrix Files dans le temps imparti. Pour configurer le serveur NTP pour Endpoint Management, utilisez l'interface de ligne de commande Endpoint Management.

Remarque :

N'oubliez pas que l'ordinateur hôte Hyper-V définit l'heure sur une VM Linux en fonction du fuseau horaire local et non de l'heure UTC.

- Connectez-vous à la console administrateur Citrix Files à l'aide d'un compte d'administrateur Citrix Files et vérifiez les paramètres SSO SAML dans **Admin > Configurer le Single Sign-On**.
- Téléchargez les clients Citrix Files pour Endpoint Management.

Étapes :

1. Dans la console Endpoint Management, cliquez sur **Configure > Apps**, puis cliquez sur **Add**.
2. Cliquez sur **MDX**.
3. Entrez un **nom** et, éventuellement une **description** et une **catégorie d'application** pour l'application.
4. Cliquez sur **Suivant** et chargez ensuite le fichier .mdx pour le client Citrix Files pour Endpoint Management.
5. Cliquez sur **Suivant** pour configurer les informations et stratégies applicatives.

La configuration qui permet l'authentification unique (SSO) à partir de clients Citrix Files pour Endpoint Management vers Citrix Files n'authentifie pas les utilisateurs sur des partages réseau ou des bibliothèques de documents SharePoint.

6. Pour activer l'authentification unique (SSO) entre le micro VPN Secure Hub et le contrôleur de zones de stockage, configurez les stratégies suivantes :

- Définissez la stratégie Accès réseau sur **Tunnélisé vers le réseau interne**.

Dans ce mode de fonctionnement, tout le trafic réseau en provenance du client Citrix Files pour Endpoint Management est intercepté par l'infrastructure MDX de Endpoint Manager et redirigé via Citrix Gateway à l'aide d'un micro VPN spécifique à l'application.

- Définissez la stratégie Mode VPN préféré sur **Navigation sécurisée**.

Dans ce mode de tunneling, le trafic SSL/HTTP en provenance d'une application MDX est arrêté par l'infrastructure MDX, ce qui initialise de nouvelles connexions aux connexions internes pour le compte de l'utilisateur. Ce paramètre de stratégie permet à l'infrastructure MDX de détecter et de répondre aux demandes d'authentification émises par des serveurs Web.

7. Complétez les approbations et les attributions de groupe de mise à disposition selon les besoins.

Seuls les utilisateurs dans les groupes de mise à disposition sélectionnés pourront accéder en SSO à Citrix Files à partir des clients Citrix Files pour Endpoint Management. Si un utilisateur d'un groupe de mise à disposition ne possède pas de compte Citrix Files, Endpoint Management met l'utilisateur à disposition dans Citrix Files lorsque vous ajoutez le client Citrix Files pour Endpoint Management à Endpoint Management.

Pour valider les clients Citrix Files pour Endpoint Management

1. Une fois la configuration décrite dans cet article terminée, démarrez le client Citrix Files pour Endpoint Management. Les fichiers Citrix Files ne doivent pas vous inviter à vous connecter.
2. Dans Secure Mail, composez un e-mail et ajoutez une pièce jointe depuis Citrix Files. Votre page d'accueil Citrix Files devrait s'ouvrir, sans vous inviter à ouvrir une session.

Applications en fin de vie et obsolètes

February 11, 2019

Les applications suivantes ont atteint leur fin de vie ou arrivent en fin de vie. Lorsqu'une version de produit atteint sa date de fin de cycle de vie, vous pouvez utiliser le produit selon les termes de votre contrat de licence de produit, mais les options de support disponibles sont limitées. Les archives sont disponibles dans le Centre de connaissances ou d'autres ressources en ligne. La documentation n'est plus mise à jour et elle est fournie telle quelle. Pour plus d'informations sur les étapes de cycle de vie des produits, consultez le [Tableau des produits](#).

Secure Notes : la date de fin du cycle de vie était le 31 décembre 2018.

Si vous avez besoin des fonctionnalités de Secure Notes et Secure Tasks, nous vous recommandons Notate for Citrix, une application tierce que vous pouvez sécuriser avec des stratégies MDX.

Si les utilisateurs de Secure Notes et de Secure Tasks ont stocké des données dans Outlook, ils peuvent accéder à ces données dans Notate. Si les utilisateurs ont stocké des données dans ShareFile, à présent Citrix Files, les données ne sont pas migrées.

Les utilisateurs peuvent continuer à exécuter Secure Notes au-delà de la date de fin de vie, jusqu'à ce que le système d'exploitation de leur plate-forme cesse de prendre en charge l'interface utilisateur. Toutefois, nous ne recommandons pas d'utiliser un produit non pris en charge.

Secure Tasks : la date de fin du cycle de vie était le 31 décembre 2018.

Secure Forms : la date de fin du cycle de vie était le 31 mars 2018. Nous encourageons nos clients à réaliser la transition vers Citrix ShareFile Workflows inclus avec les comptes Citrix Files Platinum et Premium. Pour plus d'informations, consultez [Citrix ShareFile Workflows](#).

ScanDirect : ScanDirect a atteint sa fin de vie le 1er septembre 2018.

Autoriser l'interaction sécurisée avec les applications Office 365

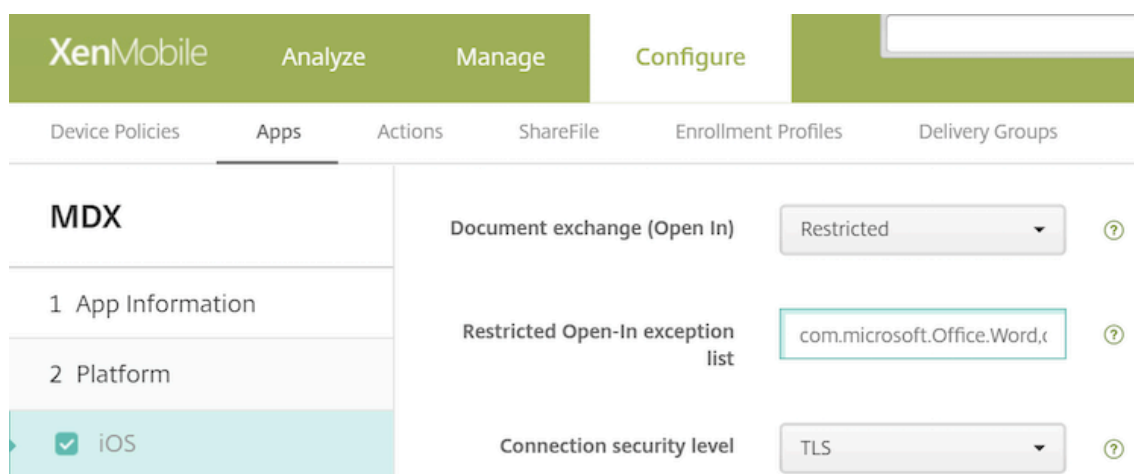
January 25, 2019

Citrix Secure Mail, Citrix Secure Web et Citrix Files proposent l'option d'ouvrir le conteneur MDX pour permettre aux utilisateurs de transférer des documents et des données vers les applications Microsoft Office 365. Vous pouvez gérer cette fonctionnalité pour les plates-formes iOS et Android via les stratégies d'ouverture disponibles sur la console Endpoint Management.

Une fois ouvertes dans une application Microsoft, les données ne sont plus sécurisées ou cryptées dans le conteneur MDX. Tenez compte des répercussions de cette fonctionnalité sur la sécurité. En particulier, les clients soucieux de prévenir la perte de données ou qui doivent se conformer aux strictes exigences de la réglementation HIPAA ou autre devraient peser le pour et le contre avant d'autoriser l'ouverture du conteneur.

Activation d'Office 365 dans iOS

1. Téléchargez la dernière version des applications Secure Mail, Secure Web ou Citrix Files à partir de la [page des téléchargements de Endpoint Management](#).
2. Chargez les fichiers sur la console Endpoint Management.
3. Recherchez la stratégie **Échange de documents (Ouvrir dans)** et définissez-la sur **Restreint**. Microsoft Word, Excel, PowerPoint, OneNote et Outlook figurent automatiquement dans la **Liste d'exceptions d'ouverture restreinte**. Par exemple : com.microsoft.Office.Word, com.microsoft.Office.Excel, com.microsoft.Office.Powerpoint, com.microsoft.onenote, com.microsoft.onenoteiPad, com.microsoft.Office.Outlook



Des contrôles supplémentaires pour les appareils iOS sont disponibles avec les inscriptions MDM.

Vous pouvez charger des applications iTunes sur la console Endpoint Management et les transférer sur des appareils. Si vous choisissez cette option, **activez** les stratégies suivantes :

- Supprimer l'application si le profil MDM est supprimé
- Empêcher la sauvegarde des données d'application
- Forcer l'application à être gérée (un effacement des données d'entreprise supprimera les applications et les données)

Pour empêcher que les documents et les données provenant des applications Microsoft soient transférés vers des applications non gérées sur l'appareil, accédez à **Configurer > Appareils > Restrictions > iOS** sur la console Endpoint Management, puis définissez **Documents provenant d'applications gérées dans les applications non gérées** et **Documents provenant d'applications non gérées dans les applications gérées** sur **OFF**.

Activation d'Office 365 dans Android

1. Téléchargez la dernière version des applications Secure Mail, Secure Web ou Citrix Files à partir de la [page des téléchargements de Endpoint Management](#).
2. Chargez les fichiers sur la console Endpoint Management.
3. Faites défiler vers le bas jusqu'à la stratégie **Échange de documents (Ouvrir dans)** et sélectionnez **Restreint**.
4. Dans **Liste d'exceptions d'ouverture restreinte**, ajoutez les ID de package suivants :

```
{ package=com.microsoft.office.word } { package=com.microsoft.office.powerpoint } { package=com.microsoft.office.excel }
```
5. Configurez les autres stratégies d'applications comme d'habitude et enregistrez les applications.

Les utilisateurs doivent enregistrer les fichiers provenant de Secure Mail, Secure Web ou Citrix Files sur leurs appareils et ouvrir les fichiers avec une application Office 365.

Pour iOS et Android, les utilisateurs peuvent ouvrir et modifier les types de fichiers suivants sur leurs appareils :

Formats de fichiers pris en charge

Pour les formats de fichiers pris en charge, consultez la [documentation de Microsoft Office](#).

**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2019 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).