Citrix Endpoint Management

Contents

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Endpoint Management

March 1, 2024

Solution de gestion des points de terminaison, Citrix Endpoint Management offre des fonctionnalités de gestion d'appareils mobiles (MDM) et de gestion d'applications mobiles (MAM). Citrix Endpoint Management vous permet de gérer les stratégies d'appareil et d'application, ainsi que de fournir des applications aux utilisateurs. Les informations de votre entreprise restent protégées grâce à des mesures de sécurité strictes pour l'identité, les appareils, les applications, les données et les réseaux.

Responsabilités des clients et de Citrix

Citrix Cloud Operations gère diverses infrastructures et tâches de monitoring. Par conséquent, vous pouvez vous focaliser sur l'expérience utilisateur et sur la gestion des appareils, des applications et des stratégies.

Responsabilités de Citrix :

- Nœuds de serveur Citrix Endpoint Management
- Intégration et configuration initiales de NetScaler Gateway (service ou sur site)
- Équilibreur de charge NetScaler Gateway
- Base de données
- Configuration logicielle de Cloud Connector
- Intégration de l'authentification SAML à ShareFile
- Surveillance du site Citrix Endpoint Management : instance, base de données, connectivité d'entreprise (LDAP), tunnel VPN (le cas échéant), certificat SSL public, licence Citrix Endpoint Management

Responsabilités du client :

- Gestion et mises à jour de NetScaler Gateway (sur site)
- Machines sur lesquelles Cloud Connector et Gateway Connector (pour le service Citrix Gateway) sont installés
- LDAP/Active Directory
- DNS
- ShareFile : configuration initiale de ShareFile, installation locale du contrôleur de zones de stockage, mises à jour de Citrix Files
- Configuration de Citrix Endpoint Management : appareils, stratégies, applications, actions, groupes de mise à disposition et certificats client

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Intégration à Microsoft Endpoint Manager

Citrix Endpoint Management peut être intégré à Microsoft Endpoint Manager (MEM). Cette intégration ajoute la valeur du micro VPN de Citrix Endpoint Management aux applications compatibles Microsoft Intune, telles que le navigateur Microsoft Edge. Avec l'intégration, vous pouvez :

- Sécuriser les applications Office 365 par accès conditionnel via Azure AD. Pour de plus amples informations, consultez Intégrer avec l'accès conditionnel Azure AD.
- Encapsuler vos propres applications métier avec Intune et Citrix pour fournir des fonctionnalités de micro-VPN à l'intérieur d'un conteneur de gestion des applications mobiles (MAM) Intune
- Effectuer la gestion et la mise à disposition des applications Office 365, des applications métier et de Citrix Secure Mail dans un même conteneur Cette méthode de gestion offre une sécurité et une productivité optimales. Par exemple, vous pouvez :
  - Bloquer des appareils ou des systèmes d'exploitation individuels
  - Personnaliser les stratégies ActiveSync en fonction des appareils, des utilisateurs ou des groupes d'utilisateurs
  - Mettre en quarantaine au niveau de l'appareil
  - Surveiller des connexions ou des appareils individuels
  - Éviter les risques de sécurité liés aux informations d'identification et à la mise en cache des données

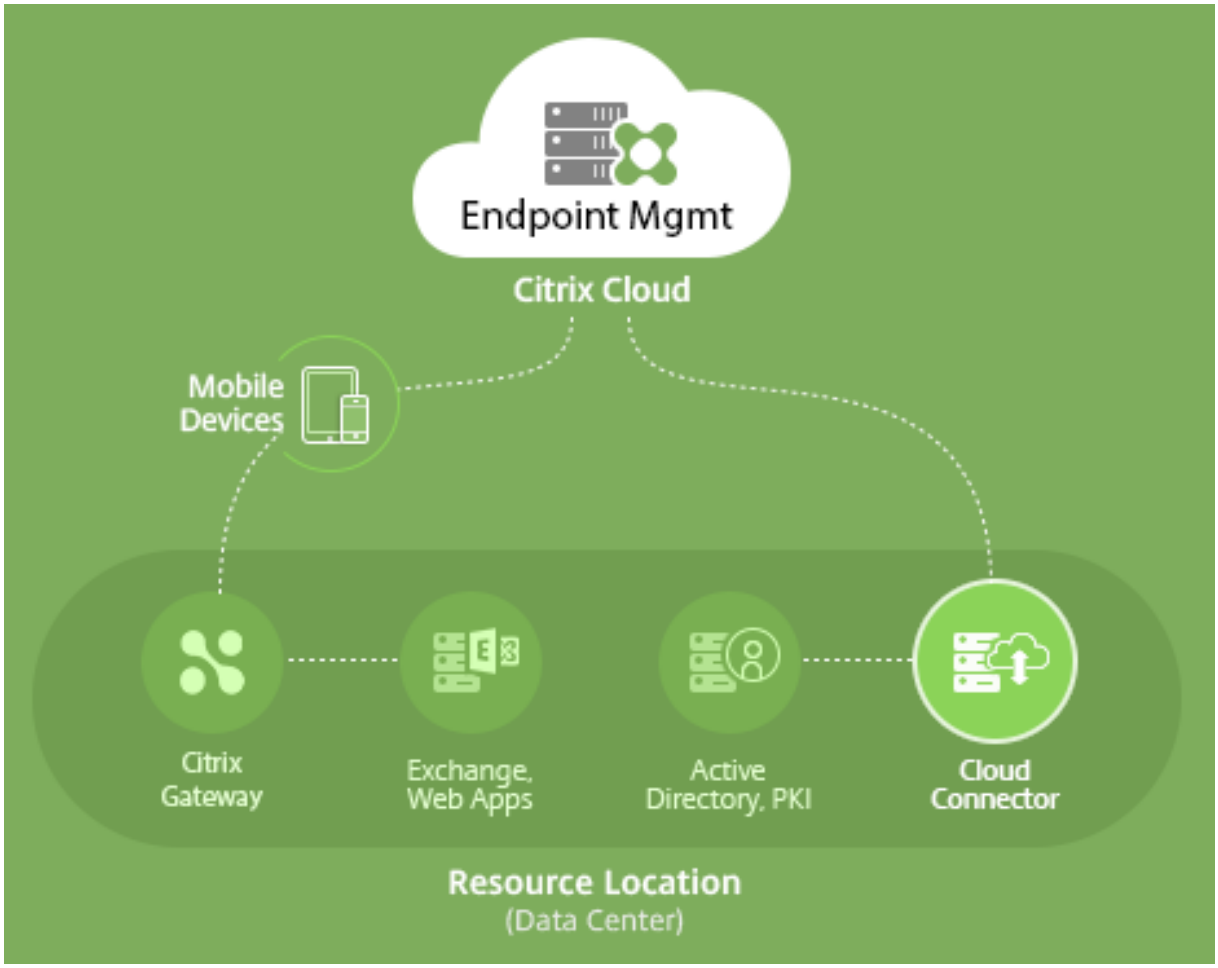
Utilisez Citrix Endpoint Management MDM+MAM ou Intune MDM pour gérer les appareils. Pour plus d'informations, consultez la section Intégration de Citrix Endpoint Management avec Microsoft Endpoint Manager.

Cloud Connector et emplacements de ressources

Vous vous connectez à Citrix Endpoint Management via Cloud Connector. Cloud Connector sert de canal de communication entre Citrix Cloud et les emplacements de vos emplacements de ressources. Cloud Connector permet d'administrer le cloud sans nécessiter de configuration de réseau ou d'infrastructure complexe telle que des VPN ou des tunnels IPsec.

Les emplacements de ressources contiennent les ressources requises pour fournir des services à vos abonnés. Pour Citrix Endpoint Management, les emplacements des ressources sont vos serveurs NetScaler Gateway, LDAP, DNS et PKI.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pour de plus amples informations sur Cloud Connector et les emplacements de ressources, consultez la section À propos de Citrix Endpoint Management.

Mise en route de Citrix Endpoint Management

> **Conseil :**
>
> service de migration de XenMobile
>
> Si vous utilisez une installation locale de XenMobile Server, notre service de migration de XenMobile (XenMobile Migration Service) peut vous aider à démarrer avec Citrix Endpoint Management. La migration de XenMobile Server vers Citrix Endpoint Management ne nécessite pas de réinscrire les appareils.
>
> Pour plus d'informations, contactez votre représentant Citrix, votre ingénieur système ou votre partenaire Citrix local.
>
> Pour en savoir plus sur notre service de migration, consultez 3 raisons pour passer au service Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Pour découvrir pourquoi effectuer la migration, comment effectuer la migration et les avantages de la migration vers Citrix Endpoint Management, visitez le catalogue de cours du service de migration CEM ou consultez le guide du service de migration Citrix Endpoint Management (CEM) .

Lorsque vous évaluez ou achetez Citrix Endpoint Management, l'équipe Citrix Endpoint Management Operations fournit une aide continue pour l'intégration. L'équipe Operations communique également avec vous pour s'assurer que les principaux services de Citrix Endpoint Management sont exécutés et configurés correctement. Cette figure présente les étapes d'intégration.

Pour ouvrir un compte Citrix et demander une version d'évaluation de Citrix Endpoint Management, contactez votre représentant Citrix. Lorsque vous êtes prêt à continuer, accédez à https://onboarding.cloud.com.

Pour un aperçu rapide de l'intégration et de la configuration de Citrix Endpoint Management, visionnez cette vidéo.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Vous souhaitez en savoir plus avant de commencer ? Essayez ces ressources :

Documentation Citrix Endpoint Management : fournit une documentation complète sur Citrix Endpoint Management, de l'intégration à la configuration initiale, en passant par la configuration avancée. Un article « Nouveautés » décrit les nouvelles fonctionnalités et corrections. Citrix vous avertit lorsque cet article est disponible pour une nouvelle version.

Citrix Cloud Citrix Endpoint Management Onboarding Handbook : regroupe toutes les informations disponibles autour de Citrix Endpoint Management afin que vous puissiez procéder à une activation et une intégration sans accroc de Citrix Endpoint Management. Vous pouvez utiliser ce document pour enregistrer les modifications apportées à vos processus internes et documenter vos conceptions de haut niveau et fonctionnelles.

Citrix Endpoint Management Deployment Handbook : de nombreuses considérations sont à prendre en compte lors de la planification d'un déploiement Citrix Endpoint Management. Vous trouverez dans ce manuel des conseils, des questions fréquemment posées et des cas d'utilisation relatifs à votre environnement Citrix Endpoint Management.

SalesIQ : plus de ressources pour nos partenaires Citrix.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Étapes suivantes

Pour plus d'informations sur le processus d'intégration de Citrix Endpoint Management, consultez la section Intégration et configuration des ressources.

Une fois l'intégration effectuée, consultez la section Préparation à l'inscription d'appareils et à la mise à disposition de ressources.

Annonces de fin de prise en charge

Pour plus d'informations sur les fonctionnalités de Citrix Endpoint Management qui seront progressivement supprimées, reportez-vous à la section Fin de prise en charge.

Prise en charge de Citrix Endpoint Management

Pour de plus amples informations sur la manière d'accéder à des informations et outils de support dans la console Citrix Endpoint Management, consultez la section Surveillance et support.

Des mises à jour sont déployées sur Citrix Endpoint Management environ toutes les 2 semaines. Pour vous, en tant que client, ce processus est transparent. Les mises à jour initiales sont uniquement appliquées aux sites Citrix internes pour être ensuite graduellement appliquées aux environnements des clients. La mise à disposition des mises à jour de façon incrémentielle permet de garantir la qualité des produits et de maximiser la disponibilité.

Les clients Citrix Endpoint Management reçoivent les mises à jour et les communications directement depuis l'équipe Citrix Endpoint Management Cloud Operations. Ces mises à jour vous tiennent au courant des nouvelles fonctionnalités, des problèmes connus, des problèmes résolus, etc.

L'équipe Citrix Cloud Operations gère les environnements Citrix Endpoint Management avec les dernières mises à jour Citrix Endpoint Management. Pour obtenir des correctifs spécifiques ou qui sont requis avant le correctif, contactez le support technique Citrix.

Si vous rencontrez des problèmes avec votre environnement, contactez le support technique de Citrix ou votre équipe de compte Citrix. Ces problèmes peuvent inclure l'inscription d'appareil mobile, l'accès à la console Citrix Endpoint Management ou des problèmes liés à Citrix Secure Mail.

Si vous avez besoin d'une intégration ou de modifications de NetScaler Gateway dans le Cloud ou Citrix Endpoint Management, envoyez une demande via le support technique de Citrix.

Les exemples de modifications que vous pourriez demander sont :

- Intégration de Citrix Files à NetScaler Gateway dans le cloud
- Changer le type d'authentification NetScaler Gateway
- Vérifier la connectivité aux ressources du datacenter du client

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Changer la configuration de split tunneling pour un Micro VPN
- Redémarrer les composants Citrix Endpoint Management en raison de la modification de la configuration

Accord de niveau de service

Citrix Endpoint Management utilise les meilleures pratiques de l'industrie afin de garantir la scalabilité du cloud et un haut degré de disponibilité du service.

Pour plus d'informations sur l'engagement de Citrix concernant la disponibilité des services Citrix Cloud, consultez le contrat de niveau de service.

Nouveautés

March 1, 2024

L'objectif de Citrix est d'offrir de nouvelles fonctionnalités et des mises à jour de produits aux clients de Citrix Endpoint Management lorsqu'elles sont disponibles. Les nouvelles versions étant plus avantageuses, il est important que vous en profitiez le plus rapidement possible.

- Des mises à jour sont déployées sur Citrix Endpoint Management environ toutes les 2 semaines.
- Ces mises à jour n'entraînent pas de temps d'arrêt pour les utilisateurs de votre instance ou de votre appareil.
- Toutes les versions ne disposent pas de nouvelles fonctionnalités et certaines mises à jour incluent des correctifs et des améliorations de performances.

Pour vous, en tant que client, ce processus est transparent. Nous appliquons les mises à jour initiales aux sites internes Citrix uniquement, puis graduellement aux environnements des clients. La mise à disposition des mises à jour de façon incrémentielle permet d'assurer la qualité des produits et de maximiser la disponibilité.

Vous recevez également les mises à jour et les communications Citrix Endpoint Management directement depuis l'équipe Citrix Endpoint Management Cloud Operations. Ces mises à jour vous tiennent au courant des nouvelles fonctionnalités, des problèmes connus, des problèmes résolus, etc.

Pour plus d'informations sur l'évolutivité et la disponibilité des services dans le cloud, consultez l'Accord de niveau de service de Citrix Endpoint Management. Pour contrôler les interruptions de service et la maintenance planifiée, consultez le tableau de bord de l'état de service.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Prise en charge continue des stratégies classiques obsolètes de Citrix ADC

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

Avant de mettre à niveau les terminaux vers iOS 14.5

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

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

Avant la mise à niveau d'une instance Citrix ADC locale vers 13.0-64.35+

Si vous utilisez la version locale de Citrix ADC et effectuez une mise à niveau vers la version 13.0-64.35+ : suivez les étapes de la solution décrite à la section Problèmes connus dans Citrix Endpoint Management 20.10.1.

Citrix Endpoint Management 24.1.0

Cette version résout également plusieurs problèmes afin d'améliorer la stabilité et les performances générales. Aucune nouvelle fonctionnalité n'a été ajoutée.

Citrix Endpoint Management 23.12.0

Ajout d'un nouveau champ obligatoire « Domaine » dans les paramètres 802.1x pour Android : un nouveau champ **Domaine** est ajouté sur la page des paramètres de **stratégie réseau de la plateforme Android Enterprise** pour le type d'authentification **EAP 802.1x**. Pour plus d'informations, consultez la section Paramètres 802.1x pour Android.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Endpoint Management 23.9.0

> **Remarque :**
>
> Les mises à jour de la documentation pour Citrix Endpoint Management 23.9.0 ont été annulées en raison de l'annulation de la publication du produit.

Problèmes connus actuels

Problèmes connus dans Citrix Endpoint Management 22.6.0

La sélection des trois types de journaux (**Débogage**, **Audit administrateur**, **Audit utilisateur**) à télécharger sous **Dépannage et support > Journaux** ne fonctionne pas par intermittence. Seuls les journaux de débogage sont téléchargés. Pour contourner le problème, vous pouvez télécharger chaque journal séparément ou ouvrir votre navigateur en mode navigation privée pour télécharger tous les journaux en cochant les trois cases. [CXM-105334]

Lors de la création d'un lien Web dans Android Enterprise, une erreur se produit lors de la tentative d'enregistrement de l'application avec une icône. Cette erreur est lié aux services Google. Pour contourner le problème, enregistrez l'application sans télécharger d'icône. [CXM-105395]

Les stratégies Samsung Knox/SAFE restent actives sur les appareils inscrits, même après la fin de leur prise en charge, et ne peuvent pas être désactivées ni configurées. Pour contourner le problème, désinscrivez et réinscrivez l'appareil. [CXM-104303]

Problèmes connus dans Citrix Endpoint Management 22.4.0

Lorsque vous recherchez un utilisateur Active Directory inscrit dans l'onglet **Surveiller**, aucun appareil inscrit n'est affiché pour cet utilisateur. Vous pouvez toujours afficher les stratégies et les applications attribuées à l'utilisateur et effectuer toutes les actions de sécurité dans **Gérer > Appareils**. Les appareils enregistrés sous iOS et Android sont affectés. [CXM-104283]

Les applications privées ne peuvent pas être publiées à l'aide d'Android Enterprise en raison d'un problème dans les services Google. Nous mettrons à jour notre documentation lorsque le problème sera résolu. [CXM-103690]

Problèmes connus dans Citrix Endpoint Management 21.12.0

Après la migration vers le RBAC basé sur Citrix Cloud, les utilisateurs administrateurs disposant d'une autorisation d'accès complet dans Citrix Cloud obtiendront également une autorisation d'accès complet dans CEM, même s'ils disposaient d'une autorisation personnalisée avant la migration. Pour

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

contourner le problème, vous pouvez mettre à jour les autorisations d'administrateur sur la page Gestion des identités et des accès Citrix Cloud avec l'accès souhaité. [CXM-102765]

Les clients intégrés avant 2018 disposent d'un accès administrateur local à la console. Les utilisateurs administrateurs CEM disposant d'autorisations permettant d'ajouter ou de modifier des utilisateurs locaux peuvent également ajouter ou modifier des utilisateurs locaux dans Citrix Cloud. Ces autorisations incluent la modification des mots de passe des utilisateurs locaux. Pour résoudre ce problème, vous pouvez appeler le support pour bloquer l'accès administrateur local direct à la console, ce qui autorise uniquement l'accès administrateur à Citrix Cloud. [CXM-102780]

Problèmes connus dans Citrix Endpoint Management 21.11.0

Sur les appareils iOS inscrits uniquement dans MAM, l'installation des applications d'entreprise échoue. [CXM-101852]

L'utilisation de la stratégie **Mise à jour automatique des applications gérées** pour Android Enterprise ne s'applique pas aux appareils lorsque le serveur CEM est mis à niveau vers la version 21.11.0. L'échec de la stratégie affecte les mises à jour des applications sur l'appareil. Pour contourner le problème, un administrateur peut modifier et enregistrer la stratégie pour actualiser les valeurs par défaut. [CXM-102446]

Problèmes connus dans Citrix Endpoint Management 21.10.0

La stratégie VPN ne fonctionne pas correctement sur les appareils Windows 11 gérés. Nous avons signalé ce problème à Microsoft et nous travaillons avec Microsoft pour le résoudre. Nous apporterons des informations sur toute progression.

Problèmes connus dans Citrix Endpoint Management 21.9.1

Sur les appareils Android inscrits en mode Profil de travail sur appareil appartenant à l'entreprise : les utilisateurs peuvent voir des erreurs indiquant qu'ils ne peuvent pas installer ou rechercher des applications sur leur profil personnel. Si ces erreurs s'affichent, mettez à jour l'application Google Play Store et réessayez. [CXM-100678]

Problèmes connus dans Citrix Endpoint Management 21.5.0

Les utilisateurs ne peuvent pas s'authentifier auprès d'Azure Active Directory (AAD) s'ils :

1. Inscrivent leur appareil dans Citrix Endpoint Management à l'aide des informations d'identification AAD.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Lancent une application Office 365 et complètent l'enregistrement AAD.
3. Suppriment leur compte de l'application Microsoft Authenticator.
4. Lancent une application Office 365 et se déconnectent.

Pour contourner le problème, désinscrivez l'appareil de Citrix Endpoint Management et réinscrivez-le. [CXM-90235]

Problèmes connus dans Citrix Endpoint Management 21.4.0

La réinscription échoue sur les appareils iOS si l'utilisateur qui tente de se réinscrire est un utilisateur Azure Active Directory différent de l'utilisateur initialement inscrit sur l'appareil. Pour contourner le problème, annulez l'inscription de l'utilisateur d'origine sur l'application Microsoft Authenticator de l'appareil avant la réinscription. [CXM-90218]

Problèmes connus dans Citrix Endpoint Management 21.2.0

Lorsque vous ajoutez Citrix Secure Web en tant qu'application MDX pour Android Enterprise, Google Play d'entreprise ne peut pas trouver l'application à l'aide de l'identifiant de l'application. Si vous recherchez « Citrix Secure Web » au lieu de l'identifiant de l'application, Google Play d'entreprise peut trouver l'application. Ce problème est un bug Google. [CXM-91991]

L'importation du certificat d'écoute SSL peut échouer. Reconditionnez le keystore de certificat en suivant les étapes décrites dans CTX-297153. [XMHELP-3346]

Problèmes connus dans Citrix Endpoint Management 20.10.1

Si vous effectuez une mise à niveau de la version Citrix ADC locale vers 13.0-64.35 ou version ultérieure, et que Citrix Endpoint Management n'est pas compatible avec Workspace : une erreur se produit lors de l'authentification unique (Single Sign-On) avec Citrix Files ou lors de l'utilisation de l'URL du domaine ShareFile. L'utilisateur ne peut pas se connecter. Cette erreur se produit uniquement dans un navigateur avec l'option **Connexion employés**.

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

```
set vpn parameter SSO ON
```

```
bind vpn vs <vsName> -portalTheme X1
```

Pour plus d'informations, consultez :

- Version Citrix ADC

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Configurations SSO affectées

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

Problèmes connus dans Citrix Endpoint Management 20.2.1

Après avoir configuré ShareFile avec une adresse URL ShareFile dans la console Citrix Endpoint Management, lorsque vous cliquez sur le bouton **Tester la connexion**, une erreur est générée. Pour résoudre ce problème, désactivez l'authentification multifacteur pour ShareFile. Pour en savoir plus sur ce problème et sa solution, consultez cette page d'assistance. [CXM-79240]

Problèmes connus dans Citrix Endpoint Management 20.1.0

Lorsque vous ajoutez des utilisateurs à une bibliothèque dans Citrix Cloud, Citrix Endpoint Management signale un succès, mais les utilisateurs ne sont pas ajoutés. [CXM-73726]

Problèmes connus dans Citrix Endpoint Management 19.11.0

Les applications MDX et publiques ne peuvent pas être supprimées de la console. Pour contourner le problème, sélectionnez l'application à supprimer, puis cliquez sur **Modifier**. Désélectionnez **Android Enterprise** et sélectionnez d'autres plates-formes dans la liste des plates-formes. Enregistrez l'application. Vous pouvez à présent supprimer l'application. [CXM-74468]

Problèmes connus dans Citrix Endpoint Management 19.5.0

Lors de l'inscription d'un appareil Citrix Ready Workspace Hub, définissez l'adresse MAC Ethernet (eth0) dans la liste d'autorisation pour éviter l'échec de l'inscription. [CXM-43141]

Problèmes connus dans Citrix Endpoint Management 19.4.1

Lorsque vous utilisez des tabulations pour parcourir les options de stratégie de GPO Windows, les boutons radio et les cases à cocher sont ignorés. [CXM-58277]

Problèmes connus dans Citrix Endpoint Management 19.2.1

Si vous désinscrivez une entreprise Android Enterprise en la supprimant via la console d'administration Google, les tentatives de réinscription de l'entreprise risquent d'échouer. Utilisez toujours la

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

console Citrix Endpoint Management pour annuler l'inscription d'une entreprise Android Enterprise, comme décrit dans la section Désinscription d'une entreprise Android Entreprise. Pour les clients Google Workspace, suivez les instructions de la section Désinscription d'une entreprise Android Entreprise. [CXM-62709] [CXM-62950]

Problèmes connus dans Citrix Endpoint Management 19.2.0

Lors de la création d'une application de magasin public dans Citrix Endpoint Management 10.18.3 : sur la page Réglages de l'app de l'iPad, si vous cliquez sur **Retour** sans rechercher d'applications, puis cliquez sur **Suivant**, le problème suivant se produit. Les boutons de navigation ne répondent pas et ne vous permettent pas de rechercher des applications. Le problème se produit lors de la création d'applications de magasin public pour iOS ou Android. [CXM-46820]

Problèmes connus dans Citrix Endpoint Management 10.19.1

Après avoir terminé le processus d'inscription sur la page **Paramètres > Android Enterprise**, le message d'erreur suivant s'affiche : `A configuration error occurred. Please try again`. Lorsque vous fermez le message d'erreur, votre configuration Android Entreprise est enregistrée, mais **Activer Android Entreprise** est **désactivé**. Pour contourner ce problème, réduisez le nombre de catégories d'application à 30 ou moins. [CXM-60899]

Problèmes connus dans Citrix Endpoint Management 10.18.5

Lorsqu'une application Chrome est configurée comme application requise pour les appareils Chrome OS, les utilisateurs devront peut-être se déconnecter et se reconnecter pour installer l'application. Ce problème externe est associé à l'ID de bogue Google 76022819. [CXM-48060]

Problèmes connus dans Citrix Endpoint Management 10.18.3

Après suppression d'un administrateur Citrix Cloud dont un appareil est inscrit : Citrix Endpoint Management ne met pas à jour le rôle utilisateur dans la console Citrix Endpoint Management tant que l'administrateur ne se reconnecte pas à partir de l'app Citrix Secure Hub ou du portail en libre-service. [CXM-45730]

Problèmes connus dans Citrix Endpoint Management 10.7.4

Si vous configurez Citrix Endpoint Management pour la connexion unique (SSO) à l'aide du fournisseur d'identité Citrix avec Azure Active Directory : lorsqu'un administrateur ou un utilisateur Citrix

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Endpoint Management est redirigé vers l'écran de **connexion Azure Active Directory**, l'écran affiche le message « Page de connexion pour Citrix Secure Hub.» Le message correct est « Page de connexion pour la console Citrix Endpoint Management ». [CXM-42309]

Avis de tiers

April 27, 2020

Citrix Endpoint Management peut inclure des logiciels tiers sous licence selon les conditions définies dans le document suivant :

Avis de tiers Citrix Endpoint Management

Fin de prise en charge

March 1, 2024

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

> **Important :**
>
> Merci d'avoir utilisé l'outil Citrix Endpoint Management Analyzer, nous vous en sommes reconnaissants. En raison de notre cadence de publication fréquente et stable, cet outil n'est plus nécessaire. Citrix a décidé de mettre fin à ce service à compter du 31 mars 2023. Nous vous recommandons d'utiliser les contrôles de connectivité disponibles dans la console Citrix Endpoint Management ou Citrix NetScaler Gateway. Pour plus d'informations, consultez la section Tests de connectivité.

Fins de prise en charge et retraits

La liste suivante présente les fonctionnalités Citrix Endpoint Management qui sont obsolètes ou ont été retirées.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Les éléments *retirés* sont retirés, ou ne sont plus pris en charge, dans Citrix Endpoint Management.

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

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Offre Citrix Endpoint Management Government	Fin de prise en charge pour l'offre Citrix Endpoint Management Government.	Janvier 2022	Juillet 2022	Citrix Endpoint Management Édition Standard
API SafetyNet Attestation	Fin de la prise en charge d'Android SafetyNet Attestation, conformément à l'annonce de Google disponible ici.	Juillet 2023	Novembre 2023	API Play Integrity
Chrome OS	Fin de la prise en charge de Chrome OS.	Juillet 2022	Mai 2023	Pas de solution alternative
tvOS	Fin de la prise en charge de tvOS.	Juillet 2022	Mai 2023	Pas de solution alternative
Protection des informations Windows (WIP)	Fin de la prise en charge de la Protection des informations Windows conformément à l'annonce de Microsoft ici.	Août 2022	Octobre 2022	Pas de solution alternative
Citrix Endpoint Management Analyzer	Fin de la prise en charge de l'outil Citrix Endpoint Management Analyzer.	Juillet 2022	Objectif : 31 mars 2023	Pas de solution alternative

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Gestion des appareils Workspace Hub	Fin de la prise en charge des appareils Citrix Ready Workspace Hub.	Janvier 2022	Juin 2022	Pas de solution alternative
Microsoft Store pour Entreprises	Microsoft Store pour Entreprises n'est plus pris en charge. Microsoft ne prend plus en charge cette plate-forme. Pour de plus amples informations, consultez la documentation de Microsoft.	Juillet 2021	Objectif : mars 2023	Pas de solution alternative
Samsung SAFE	Fin de la prise en charge de Samsung SAFE.	Janvier 2022	Juin 2022	Utilisez Android Enterprise.
XML personnalisé pour Zebra	Fin de la prise en charge de la stratégie XML personnalisé sur les appareils Zebra.	Janvier 2022	Juin 2022	Utilisez la configuration gérée par Android Entreprise
Identités PKI : génériques, Symantec PKI, DigiCert et Entrust	Prise en charge obsolète des entités PKI génériques, gérées par DigiCert et de l'adaptateur Entrust.	Juin 2021	Janvier 2022	Pas de solution alternative

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Android pour Workspace	Prise en charge d' Android pour Workspace abandonnée	Janvier 2022	Avril 2022	Pas de solution alternative
Passerelle SMS de l'opérateur	Fin de la prise en charge des notifications de passerelle SMS Nexmo	Janvier 2022	Avril 2022	Utiliser les notifications du serveur SMTP
Fournisseur de services mobiles (MSP)	Fin de la prise en charge de l' interface MSP pour interroger des appareils Blackberry et d' autres appareils Exchange ActiveSync et effectuer des opérations d' émission	Janvier 2022	Avril 2022	Pas de solution alternative

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
MDX Toolkit	Fin de prise en charge de MDX Toolkit en faveur du SDK MAM (Gestion d' applications mobiles). Pendant la période de transition, vous pouvez utiliser à la fois des applications encapsulées avec MDX et des applications développées par le SDK MAM.	Mars 2020	Juillet 2023	Pour continuer à gérer vos applications d' entreprise, utilisez le SDK MAM.
Rôle RBAC : inscription d' appareils partagés et inscription d' appareils COSU	Fin de la prise en charge des paramètres prédéfinis du contrôle d'accès basé sur rôle pour l'inscription d'appareils partagés et l' inscription d' appareils COSU	Juillet 2021	Décembre 2021	Configurez les appareils iOS via Apple School Manager ou Apple Business Manager. Configurez les appareils COSU (dédiés) Android via des profils d' inscription.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Autoriser la connexion automatique aux points d'accès Wi-Fi sense pour les appareils Windows.	Fin de prise en charge pour la restriction Autoriser la connexion automatique aux points d'accès Wi-Fi Sense pour les appareils Windows 10. Windows 10 ne prend plus en charge cette fonctionnalité. Pour de plus amples informations, veuillez consulter la documentation Microsoft.	Octobre 2021	Février 2022	Pas de solution alternative
MDX : Autre serveur de passerelle	Fin de prise en charge de l' authentification renforcée pour les appareils iOS et Android.	Mars 2020	Septembre 2021	Pas de solution alternative
MDX : Micro VPN (mode tunnel complet)	Fin de prise en charge du tunnel VPN complet pour les appareils iOS et Android.	Mars 2020	Septembre 2021	Utilisez le mode SSO Web du SDK MAM ou créez une stratégie Per App VPN avec le type de connexion Citrix SSO.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
MDX : prise en charge des fichiers PAC	Fin de prise en charge d'un fichier PAC (Proxy Automatic Configuration) avec un déploiement de tunnel VPN complet pour les appareils iOS et Android.	Mars 2020	Septembre 2021	Utilisez NetScaler Gateway pour vous connecter via un serveur proxy pour accéder aux réseaux internes.
Prise en charge des appareils partagés MDX	Fin de prise en charge des appareils partagés pour les applications MDX.	Mars 2020	Septembre 2021	Pour Android Enterprise, utilisez des appareils partagés inscrits en tant qu' appareils dédiés. Pour iOS, utilisez Apple School Manager ou GroundControl.
Android - Sony	Fin de la prise en charge des appareils Android Sony et des stratégies spécifiques à Sony.	Janvier 2021	Février 2022	Utiliser Android Enterprise
Android - HTC	Fin de la prise en charge des appareils Android HTC et des stratégies spécifiques à HTC.	Janvier 2021	Février 2022	Utiliser Android Enterprise

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Android - Amazon	Fin de la prise en charge des appareils Android Amazon et des stratégies spécifiques à Amazon.	Janvier 2021	Février 2022	Utiliser Android Enterprise
Inscription Knox Mobile Enrollment (ancien mode DA)	Fin de prise en charge de Knox Mobile Enrollment (KME) dans l'ancien mode Administrateur d'appareils (DA) sur toutes les versions Android.	4 mai 2021	Septembre 2021	Utilisez KME pour l'inscription au mode Android Enterprise. Android 8, 9, 10, 11 prend en charge Android Enterprise.
Mode d'inscription haute sécurité	Fin de la prise en charge de la génération d'invitations d'inscription avec le mode d'inscription sécurisée **Haute sécurité**.	Juillet 2021	Février 2022	Consultez Invitations d'inscription pour obtenir une liste des modes d'inscription sécurisée pris en charge.
Informations d'identification dérivées	Fin de la prise en charge des informations d'identification dérivées et de l'application Citrix Derived Credential Manager.	March 2021	Décembre 2021	Pour obtenir la liste des types d'authentification pris en charge pour iOS, consultez iOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Ports sortants APNs	La prise en charge par Apple du protocole binaire hérité du service Apple Push Notification prend fin le 31 mars 2021. Apple recommande d'utiliser à la place l'API du fournisseur APNs basé sur HTTP/2. Dans le cadre de ce changement, les ports 2195 et 2196, utilisés pour envoyer des notifications APNs à `*.push.apple.com` sont dépréciés.	Octobre 2020	March 2021	Utilisez le port 443 à la place. Consultez la section Configuration requise pour le réseau et le pare-feu.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
MDX Service	Fin de prise en charge de MDX Service en faveur du SDK MAM (Gestion d' applications mobiles). Pendant la période de transition, vous pouvez utiliser à la fois des applications encapsulées avec MDX à l'aide du MDX Toolkit et des applications développées par le SDK MAM.	Mars 2020	Septembre 2021	Pour continuer à encapsuler vos applications d' entreprise, utilisez l'outil MDX Toolkit.
Configuration de l'invitation d' inscription dans le portail en libre-service	Fin de la prise en charge de la génération d' invitations d' inscription pour les utilisateurs à partir du portail en libre-service.	Juillet 2021	Juillet 2021	Contactez votre administrateur pour générer des invitations d' inscription dans la console Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Configuration de l'invitation d' inscription	Fin de prise en charge pour l' utilisation du numéro IMEI, du numéro de série ou de l'UDID d'un appareil pour créer une invitation d' inscription.	Avril 2021	Juillet 2021	Lorsque vous créez une invitation d' inscription, configurez les paramètres disponibles sous **Gérer > Invitations d' inscription** dans la console Citrix Endpoint Management.
Algorithmes de signature d' authentification basés sur des certificats (non-FIPS et chiffrements faibles)	Fin de prise en charge des algorithmes de signature suivants : SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA, SHA1withDSA, RIPEMD160withRSA, RIPEMD128withRSA, RIPEMD256withRSA.	Mai 2020	Juin 2021	Lorsque vous créez un CSR pour un fournisseur d' informations d' identification dans la console Citrix Endpoint Management (**Paramètres > Fournisseurs d' identités > Demande de signature de certificat**), choisissez un chiffrement plus puissant.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Applications de mobilité Citrix et applications Workspace pour Android 7.x et iOS 12.x	Fin de prise en charge des versions Android 7.x et iOS 12.x de Citrix Secure Hub, Citrix Secure Mail, Citrix Secure Web et de l' application Citrix Workspace.	Avril 2021	Juin 2021	Utilisez, au minimum, la version actuelle et une version antérieure des principales plates-formes de système d' exploitation. Les appareils plus anciens restent inscrits. Toutefois, Citrix ne teste ni ne prend en charge les appareils d' ancienne génération.
Prise en charge des jetons logiciels RSA pour Android	Fin de prise en charge de l' importation directe des jetons logiciels RSA dans Citrix Secure Hub pour Android.	Janvier 2021	Février 2021	Vous pouvez importer le jeton logiciel RSA dans l'application RSA Secure ID disponible dans Google Play. Vous pouvez ensuite utiliser le jeton pour l' authentification NetScaler Gateway.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Internet Explorer 11	Fin de prise en charge de l' utilisation d' Internet Explorer avec la console Citrix Endpoint Management.	Janvier 2021	Janvier 2021	Utilisez la dernière version de ces navigateurs Web : Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari
Vérification de la configuration Gateway dans Citrix Endpoint Management Analyzer	Fin de la prise en charge de l' option de vérification de la configuration Gateway.	Novembre 2020	Novembre 2020	Utilisez la vérification Citrix Insight Services dans Analyzer pour vérifier que vos configurations Citrix ADC sont prêtes à déployer Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Applications publiées pour le mode Administrateur de l'appareil (DA) hérité sur les appareils Android Enterprise	Nous ne fournissons plus d'applications publiées pour la plate-forme en mode DA hérité aux appareils inscrits dans Android Enterprise.	Octobre 2020	Novembre 2020	Pour les appareils Android Enterprise, publiez des applications pour la plate-forme Android Enterprise. Pour continuer à publier des applications en mode DA hérité sur des appareils en mode DA, créez un groupe de mise à disposition distinct pour ces applications.
Mode Administrateur d'appareils (DA) hérité pour les appareils Android 10.	Google a mis fin à la prise en charge de certaines API d'administrateur d'appareils Citrix ne prend pas en charge les appareils Android 10 inscrits en mode Administrateur d'appareils après la mise à niveau de Citrix Secure Hub qui cible l'API Android niveau 29.	Février 2020	Novembre 2020	Migrez les appareils Android 10 vers Android Enterprise.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Android TouchDown	DigiCert a cessé de prendre en charge Android TouchDown. Citrix a supprimé la page de la plate-forme Android TouchDown de la stratégie Exchange.	Juillet 2018	Novembre 2020	Recommandation : Utiliser Citrix Secure Mail.
Nouvelles inscriptions d' administrateur d' appareils pour Android 10	Prise en charge obsolète des nouvelles inscriptions ou réinscriptions en mode Administrateur d' appareils (DA) hérité sur les appareils Android 10. Les appareils déjà inscrits continuent de fonctionner.	Février 2020	Septembre 2020	Inscrivez les nouveaux appareils Android 10+ dans Android Enterprise.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Cryptage MDX	Fin de prise en charge de la fonctionnalité de cryptage MDX dans la console Citrix Endpoint Management.	Octobre 2019	Septembre 2020	Activez le cryptage de plate-forme iOS ou Android à l'aide de notre fonctionnalité de gestion du cryptage avec contrôle de la conformité. Assurez-vous d'avoir testé et planifié la migration depuis le cryptage MDX d'ici juillet 2020.
Windows Mobile/CE	Fin de la prise en charge des périphériques Windows Mobile/CE.	Avril 2018	Septembre 2020	Utilisez Windows 10 Desktop et Laptop.
Conteneur Samsung SEAMS	Fin de la prise en charge du conteneur Samsung SEAMS.	Juin 2020	Août 2020	Utilisez Android Enterprise.
Assistance à distance	Fin de la prise en charge du client d'assistance à distance	Janvier 2019	Août 2020	Pas de solution alternative

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Applications de mobilité Citrix et applications Workspace pour Android 6.x et iOS 11.x	Fin de prise en charge des versions Android 6.x et iOS 11.x de Citrix Secure Hub, Citrix Secure Mail, Citrix Secure Web et Citrix Workspace.	Avril 2020	Juin 2020	Utilisez, au minimum, la version actuelle et une version antérieure des principales plates-formes de système d' exploitation. Les appareils plus anciens restent inscrits. Toutefois, Citrix ne teste ni ne prend en charge les appareils d' ancienne génération.
Extensions réseau Citrix Secure Hub pour iOS	Fin de prise en charge de l' infrastructure d' extension réseau qui permet de personnaliser les fonctionnalités de mise en réseau pour les appareils iOS. Citrix Secure Hub version 20.3.0.	Octobre 2018	Mars 2020	Pas de solution alternative

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Élément	Description	Fin de prise en charge annoncée	Supprimé	Solution alternative
Connexion à l'API à l'aide de comptes locaux	Les administrateurs ne peuvent plus se connecter à l' API REST à l'aide d'un compte local.	Octobre 2020		Les administrateurs peuvent se connecter à l' aide d'un compte Citrix Cloud. Consultez la section API REST.
Certificats SSL (Secure Sockets Layer) auto-signés	Fin de la prise en charge des certificats SSL auto-signés pour toutes les plates-formes d' appareil.	Mai 2020		Remplacez votre certificat auto-signé existant par un certificat SSL approuvé d'une autorité de certification connue.

Configuration système requise

March 1, 2024

En attendant la mise à disposition de Citrix Endpoint Management par Citrix, assurez-vous de préparer votre déploiement Citrix Endpoint Management en installant Cloud Connector. Si Citrix héberge et met à disposition votre solution Citrix Endpoint Management, il est nécessaire de configurer la communication et les ports. Cette configuration connecte l'infrastructure Citrix Endpoint Management aux services d'entreprise, tels que Active Directory.

Configuration requise pour Cloud Connector

Citrix utilise Cloud Connector pour intégrer l'architecture Citrix Endpoint Management dans votre infrastructure existante. Cloud Connector intègre en toute sécurité les emplacements de ressources suivants à Citrix Endpoint Management via le port 443 : LDAP, serveur PKI, requêtes DNS internes et énumération Citrix Workspace.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Au moins deux machines Windows Server dédiées appartenant à votre domaine Active Directory Les machines peuvent être physiques ou virtuelles. La machine sur laquelle vous installez le Connector doit être synchronisée avec l'heure UTC pour assurer une installation et un fonctionnement appropriés. Pour obtenir une liste complète des dernières exigences, consultez les documents de déploiement fournis par votre équipe de compte Citrix.

  L'assistant d'intégration vous guide à travers l'installation de Cloud Connector sur ces machines.

- Pour connaître la configuration système requise pour la plate-forme, consultez Citrix Cloud Connector.

Niveaux fonctionnels Active Directory pris en charge

Lorsque Citrix Cloud Connector est utilisé avec Citrix Endpoint Management, il prend en charge les niveaux fonctionnels de forêt et de domaine suivants dans Active Directory.

Niveau fonctionnel de la forêt	Niveau fonctionnel du domaine	Contrôleurs de domaine pris en charge
Windows Server 2016	Windows Server 2016	Windows Server 2016, Windows Server 2019
Windows Server 2016	Windows Server 2019	Windows Server 2019
Windows Server 2019	Windows Server 2019	Windows Server 2019

> **Remarque :**
>
> Les versions 2012 R2, 2012 et 2008 R2 de Windows Servers ne sont plus prises en charge car elles ont atteint leur fin de vie. Pour en savoir plus, consultez la documentation sur le cycle de vie des produits Microsoft.

Configuration requise pour NetScaler Gateway

Citrix Endpoint Management requiert l'installation d'une passerelle NetScaler Gateway dans votre emplacement de ressources pour les scénarios suivants :

- Vous avez besoin d'un micro VPN pour accéder aux ressources réseau internes pour les applications métier. Ces applications sont encapsulées avec la technologie Citrix MDX. Le micro-VPN a besoin de NetScaler Gateway pour se connecter aux infrastructures back-end internes.
- Vous envisagez d'utiliser des applications de productivité mobiles, telles que Citrix Secure Mail.
- Vous prévoyez d'intégrer Citrix Endpoint Management à Microsoft Endpoint Manager.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration requise :

- Authentification de domaine (LDAP)
- NetScaler Gateway 12.1 ou version ultérieure, avec une licence Platform ou Universal

Pour plus de détails, consultez la section Gestion des licences.

- Certificat SSL public.

Pour plus de détails, consultez la section Créer et utiliser des certificats SSL sur une appliance Citrix ADC.

- Adresse IP publique non utilisée pour le serveur virtuel NetScaler Gateway
- Nom de domaine complet (FQDN) pouvant être résolu publiquement pour le serveur virtuel NetScaler Gateway
- Certificats racine et intermédiaire Citrix Endpoint Management hébergés sur le cloud (fournis dans le bundle de script)
- Adresse IP privée interne non utilisée pour l'adresse IP d'équilibrage de charge du proxy
- Pour plus d'informations sur les ports, reportez-vous à la section Configuration requise pour les ports NetScaler Gateway, plus loin dans cet article.
- Intégration de Citrix Endpoint Management avec Microsoft Endpoint Manager
- Déployer l'instance Citrix ADC VPX sur Microsoft Azure

Pour obtenir des informations sur la configuration requise pour NetScaler Gateway, consultez les documents de déploiement fournis par votre équipe de compte Citrix.

Pour plus d'informations sur la configuration requise pour Android Enterprise, consultez la section Android Enterprise.

Configuration requise pour Citrix Files

Les services de synchronisation et de partage de fichiers Citrix Files sont disponibles dans l'offre Citrix Endpoint Management Premium Service. StorageZones Controller étend le stockage sur le cloud Citrix Files SaaS en fournissant à votre compte Citrix Files des zones de stockage privées.

Conditions requises pour StorageZones Controller :

- Une machine physique ou virtuelle dédiée
- Windows Server 2012 R2 (Datacenter, Standard ou Essentials), Windows Server 2016, Windows Server 2019 ou Windows Server 2022
- 2 processeurs virtuels
- 4 Go de RAM
- 50 Go d'espace disque

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

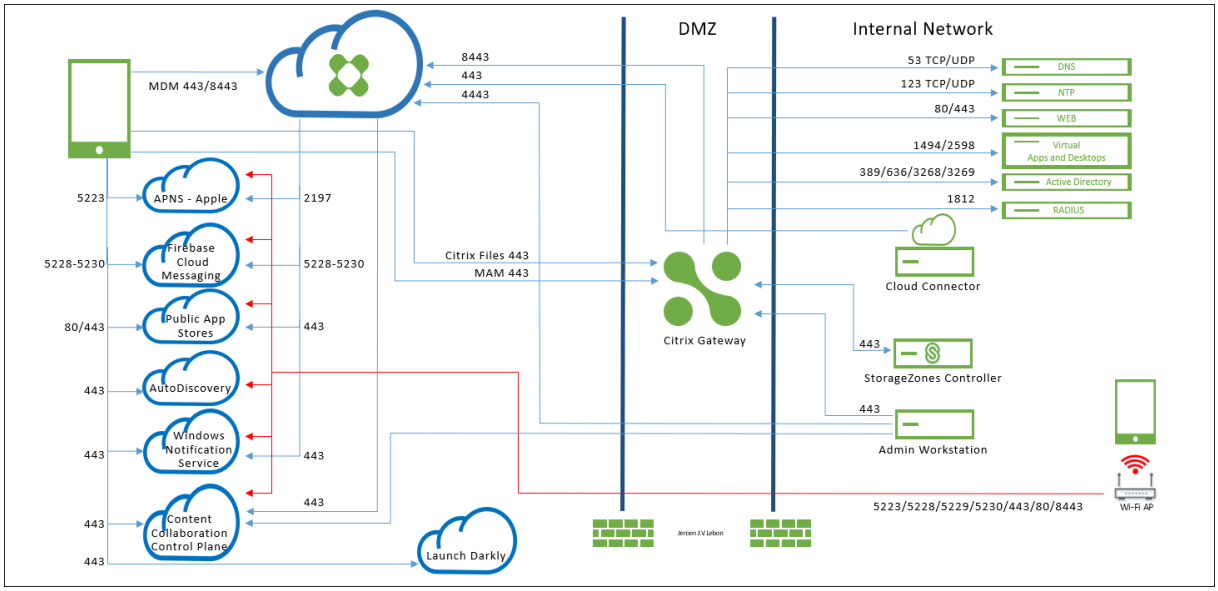
- Rôles de serveur pour le serveur Web (IIS) :
  - Développement d'applications : ASP. NET 4.5.2
  - Sécurité : authentification de base
  - Sécurité : authentification Windows

Configuration requise pour la plateforme Citrix Files :

- Le programme d'installation de Citrix Files requiert des privilèges d'administration sur Windows Server
- Nom d'utilisateur administrateur Citrix Files

Configuration requise pour les ports

Pour autoriser des appareils et des applications à communiquer avec Citrix Endpoint Management, vous devez ouvrir des ports spécifiques dans vos pare-feu. Le schéma suivant illustre le flux du trafic pour Citrix Endpoint Management.



Les sections suivantes répertorient les ports que vous devez ouvrir. Pour plus d'informations sur les URL utilisées par les applications de productivité mobiles, voir Gestion des feature flag.

Configuration requise pour les ports NetScaler Gateway

Ouvrez les ports pour autoriser les connexions utilisateur à partir de Citrix Secure Hub et Citrix Workspace via NetScaler Gateway pour :

- Citrix Endpoint Management
- StoreFront

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Autres ressources du réseau interne telles que les sites Web intranet

Pour plus d'informations sur NetScaler Gateway, consultez la section Configuration des paramètres de votre environnement Citrix Endpoint Management dans la documentation NetScaler Gateway. Pour plus d'informations sur les adresses IP, consultez la section Comment NetScaler Gateway utilise les adresses IP dans la documentation de NetScaler Gateway.

Port TCP	Description	Source	Destination
53 (TCP et UDP)	Utilisé pour les connexions DNS.	SNIP NetScaler Gateway	Serveur DNS
80/443	NetScaler Gateway transmet la connexion micro VPN à la ressource du réseau interne via le second pare-feu.	SNIP NetScaler Gateway	Sites Web intranet
123 (TCP et UDP)	Utilisé pour les services NTP (Network Time Protocol).	SNIP NetScaler Gateway	Serveur NTP
389	Utilisé pour les connexions LDAP non sécurisées.	NSIP NetScaler Gateway (ou SNIP, si un équilibreur de charge est utilisé)	Serveur d'authentification LDAP ou Microsoft Active Directory
443	Utilisé pour les connexions à StoreFront de Citrix Workspace vers Citrix Virtual Apps and Desktops.	Internet	NetScaler Gateway
443	Utilisé pour les connexions à Citrix Endpoint Management pour la mise à disposition d'applications Web, mobiles et SaaS.	Internet	NetScaler Gateway

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Port TCP	Description	Source	Destination
443	Utilisé pour la communication Cloud Connector - énumération LDAP, DNS, PKI et Citrix Workspace	Serveurs Cloud Connector	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.blob.core.windows.net/, https://*.servicebus.windows.net
443	Utilisé pour accéder au portail en libre-service de Citrix Endpoint Management, s'il est activé, via le navigateur.	Point d'accès (navigateur)	Citrix Endpoint Management (https://<sitename>/zdm/shp)
636	Utilisé pour les connexions LDAP sécurisées.	NSIP NetScaler Gateway (ou SNIP, si un équilibreur de charge est utilisé)	Serveur d'authentification LDAP ou Active Directory
1494	Utilisé pour les connexions ICA à des applications Windows dans le réseau interne. Citrix recommande de conserver ce port ouvert.	SNIP NetScaler Gateway	Citrix Virtual Apps and Desktops
1812	Utilisé pour les connexions RADIUS.	NSIP NetScaler Gateway	Serveur d'authentification RADIUS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Port TCP	Description	Source	Destination
2598	Utilisé pour les connexions aux applications Windows dans le réseau interne à l'aide de la fiabilité de session. Citrix recommande de conserver ce port ouvert.	SNIP NetScaler Gateway	Citrix Virtual Apps and Desktops
3269	Utilisé pour les connexions LDAP sécurisées au Microsoft Global Catalog.	NSIP NetScaler Gateway (ou SNIP, si un équilibreur de charge est utilisé)	Serveur d' authentification LDAP ou Active Directory
4443	Utilisé pour l'accès à la console Citrix Endpoint Management par un administrateur via le navigateur.	Point d'accès (navigateur)	Citrix Endpoint Management
8443	Utilisé pour l' inscription, le magasin d'applications et la gestion des applications mobiles (MAM).	SNIP NetScaler Gateway	Citrix Endpoint Management
8443	Port Secure Ticket Authority (STA) utilisé pour le jeton d' authentification de Citrix Secure Mail	SNIP NetScaler Gateway	Citrix Endpoint Management

Configuration requise pour le réseau et le pare-feu

Pour autoriser des appareils et des applications à communiquer avec Citrix Endpoint Management, vous devez ouvrir des ports spécifiques dans vos pare-feu. Les tableaux suivants répertorient ces ports.

Ports ouverts depuis le réseau interne vers Citrix Cloud :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Port TCP	IP source	Description	Destination	IP destination
443		Cloud Connector	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.sharefile.com, https://cwsproduction.blob.core.wind ows.net/downloads, https://*.servicebus.windows.net	
443		Console d' administration	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.citrix.com, https://cwsproduction.blob.core.windows.net/downloads	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Port TCP	IP source	Description	Destination	IP destination
443		Accès au portail en libre-service de Citrix Endpoint Management via un navigateur (si le portail est activé)	Citrix Endpoint Management	
4443		Accès à la console Citrix Endpoint Management via un navigateur	Citrix Endpoint Management	

Ports ouverts depuis Internet vers la DMZ :

Port TCP	Description	IP source	Destination	IP destination
443	Appareil client Citrix Endpoint Management		IP NetScaler Gateway	
443	Appareil client Citrix Endpoint Management		NetScaler Gateway VIP	
443	Adresse IP publique Citrix Files	CTX208318	NetScaler Gateway VIP	

Ports ouverts depuis la DMZ vers le réseau interne :

Port TCP	Description	IP source	Destination	IP destination
389 ou 636	NSIP NetScaler Gateway		IP Active Directory	
53 (UDP)	NSIP NetScaler Gateway		IP du serveur DNS	
443	SNIP NetScaler Gateway		IP serveur Exchange (EAS)	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Port TCP	Description	IP source	Destination	IP destination
443	SNIP NetScaler Gateway		Applications/Services Web internes	
443	SNIP NetScaler Gateway		IP StorageZones Controller	

Ports ouverts depuis le réseau interne vers la DMZ :

Port TCP	Description	IP source	Destination	IP destination
443	Client admin		NSIP NetScaler Gateway	

Ports ouverts depuis le réseau interne vers Internet :

Port TCP	Description	IP source	Destination	IP destination
443	IP serveur Exchange (EAS)		Écouteurs de notifications push Citrix Endpoint Management (1)	
443	IP StorageZones Controller		Plan de contrôle Citrix Files	CTX208318

(1)`us-east-1.mailboxlistener.xm.citrix.com`, `eu-west-1.mailboxlistener.xm.citrix.com`, `ap-southeast-1.mailboxlistener.xm.citrix.com`

Ports ouverts depuis le Wi-Fi de l'entreprise vers Internet :

Port TCP	Description	IP source	Destination	IP destination
8443 / 443	Appareil client Citrix Endpoint Management		Citrix Endpoint Management	
5223	Appareil client Citrix Endpoint Management		Serveurs APNS Apple	`17.0.0.0/8`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Port TCP	Description	IP source	Destination	IP destination
5228	Appareil client Citrix Endpoint Management		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
5229	Appareil client Citrix Endpoint Management		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
5230	Appareil client Citrix Endpoint Management		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
443	Appareil client Citrix Endpoint Management		Firebase Cloud Messaging	fcm.googleapis.com
443	Appareil client Citrix Endpoint Management		Windows Push Notification Service	*.notify.windows.com
443 / 80	Appareil client Citrix Endpoint Management		Apple iTunes App Store	ax.apps.apple.com, *.mzstatic.com, vpp.itunes.apple.com

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Port TCP	Description	IP source	Destination	IP destination
443 / 80	Appareil client Citrix Endpoint Management		Google Play	play.google.com, android.clients.google.com, android.l.google.com, android.com, google-analytics.com
443 / 80	Appareil client Citrix Endpoint Management		Microsoft App Store	login.live.com, *.notify.windows.com
443	Appareil client Citrix Endpoint Management		Détection automatique Citrix Endpoint Management pour iOS et Android	discovery.cem.cloud.us
443	Appareil client Citrix Endpoint Management		Détection automatique Citrix Endpoint Management pour Windows	enterpriseenrollment.mycompany.com, discovery.cem.cloud.us
443	IP StorageZones Controller		Plan de contrôle Citrix Files	CTX208318
443	Appareil client Citrix Endpoint Management		Gestion des appareils mobiles Google, API Google, API Google Play Store	*.googleapis.com

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Port TCP	Description	IP source	Destination	IP destination
443	Appareil client Citrix Endpoint Management		Vérifie la connectivité pour les versions CloudDPC antérieures à v470. La vérification de la connectivité Android commençant par N MR1 exige que `https://www.google.com/generate_204` soit joignable ou que le réseau Wi-Fi donné pointe vers un fichier PAC accessible	`connectivitycheck.android.com`, `www.google.com`

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

La configuration de ce port permet de s'assurer que les appareils Android qui se connectent à partir de Citrix Secure Hub pour Android peuvent accéder au service de détection automatique de Citrix Endpoint Management depuis le réseau interne. L'accès au service ADS est important lors du téléchargement de mises à jour de sécurité mises à disposition via ADS.

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

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

- **Collecter les certificats du serveur Citrix Endpoint Management et de NetScaler Gateway :** les certificats doivent être au format PEM et doivent être des certificats de clé publique et non de clé privée.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Contacter l'assistance Citrix et demander l'activation du certificate pinning :** lors de cette opération, vous êtes invité à fournir vos certificats.

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

Pour autoriser l'accès à ADS pour Citrix Secure Hub pour Android/iOS, ouvrez le port 443 pour les noms de domaine complets suivants :

Nom de domaine complet	Port	Utilisation adresse IP et port
`discovery.cem.cloud.us`	443	Citrix Secure Hub - Communication ADS via CloudFront

Pour plus d'informations sur les adresses IP prises en charge, consultez Cloud-based storage centers from AWS.

Configuration réseau requise pour Android Enterprise

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

Exigences relatives aux applications

Citrix Endpoint Management permet d'ajouter et de gérer jusqu'à 300 applications. Si vous dépassez cette limite, votre système devient instable.

Compatibilité Citrix Endpoint Management

November 29, 2023

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

  Le MDX Toolkit devrait atteindre la fin de son cycle de vie en juillet 2023. Pour continuer à gérer vos applications d'entreprise, vous devez incorporer le SDK MAM.

- Applications de productivité mobiles

Cet article décrit les versions des composants Citrix Endpoint Management pris en charge que vous pouvez intégrer.

Les dernières versions de Citrix Secure Hub, du MDX Toolkit et des applications de productivité mobiles sont compatibles avec la dernière version et les deux versions précédentes de Citrix Endpoint Management.

Applications de productivité mobiles

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

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

SDK MAM

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

MDX Toolkit

Le MDX Toolkit devrait atteindre la fin de son cycle de vie en juillet 2023. Pour continuer à gérer vos applications d'entreprise, vous devez incorporer le SDK MAM.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Prise en charge des navigateurs

La console Citrix Endpoint Management nécessite l'un des navigateurs Web pris en charge suivants :

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

Systèmes d'exploitation pris en charge

March 1, 2024

Cet article couvre les appareils pris en charge pour la gestion de la mobilité d'entreprise avec Citrix Endpoint Management. En raison de restrictions spécifiques à la plate-forme et de fonctionnalités de sécurité, Citrix Endpoint Management ne prend pas en charge toutes les fonctionnalités sur toutes les plates-formes.

Pour obtenir les dernières versions des applications de productivité mobiles, consultez la section Prise en charge des applications de productivité mobiles.

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

Liste des systèmes d'exploitation pris en charge

Citrix Endpoint Management prend en charge les systèmes d'exploitation suivants :

- **Android :** 10.x, 11.x, 12.x, 13.x, 14.x

  Citrix recommande de mettre à niveau vers Android 10 ou version supérieure avant d'utiliser Android Enterprise. Consultez la section Considérations relatives à Android pour de plus amples informations.

- **iOS :** 13.x, 14.x, 15.x, 16.x, 17.x

  Les applications mobiles Citrix Endpoint Management et Citrix ne prennent actuellement pas en charge toutes les nouvelles fonctionnalités iOS 14.x, iOS 15.x, iOS 16.x et iOS 17.x.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **iPadOS :** 13.x, 14.x, 15.x, 16.x, 17.x

  Les applications mobiles Citrix Endpoint Management et Citrix ne prennent actuellement pas en charge toutes les nouvelles fonctionnalités d'iPadOS 14.x, iPadOS 15.x, iPadOS 16.x et iPadOS 17.x.

- **macOS :** 11.x, 12.x, 13.x, 14.x

  Citrix Endpoint Management et les applications mobiles Citrix ne prennent pas actuellement en charge toutes les nouvelles fonctionnalités disponibles pour macOS 11, macOS 12, macOS 13 et macOS 14.

- **Ordinateurs et tablettes Windows 10 et Windows 11 :** (MDM uniquement)

  - Windows 10 Professionnel et Windows 11 Professionnel
  - Windows 10 Entreprise et Windows 11 Entreprise
  - Windows 10 Éducation et Windows 11 Éducation
  - Windows IoT Enterprise

  Consultez la documentation Microsoft pour connaître le niveau de prise en charge d'un système d'exploitation spécifique.

Considérations relatives à Android

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

- Google a mis fin à la prise en charge des API d'administration des appareils, ce qui a un impact sur les appareils fonctionnant sous Android 10+. L'inscription des appareils Android 10+ en mode hérité d'administration des appareils échoue. Citrix ne prend pas en charge l'inscription d'appareils Android en mode d'administration des appareils.
- Citrix recommande d'utiliser Android Entreprise pour les appareils Android. Pour plus d'informations, consultez la section Migrer de l'administration des appareils vers Android Enterprise.
- La modification de l'API Google n'affecte pas les appareils inscrits en mode MAM-uniquement.
- Consultez également ce blog Citrix.

Avant la mise à niveau :

- Assurez-vous que votre infrastructure de serveurs est conforme aux certificats de sécurité ayant un nom d'hôte correspondant dans l'extension SAN (autre nom de l'objet).
- Pour vérifier un nom d'hôte, le serveur doit présenter un certificat avec un SAN correspondant. Citrix approuve uniquement les certificats qui contiennent un SAN correspondant au nom d'hôte.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Langues prises en charge

November 29, 2023

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

Cet article dresse la liste des langues prises en charge dans la dernière version de Citrix Endpoint Management.

Console Citrix Endpoint Management et portail en libre-service

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

Applications de productivité mobiles Citrix

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

iOS et Android

Langue	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
Japonais	X	X	X	X	X	X
Chinois simplifié	X	X	X	X	X	X
Chinois traditionnel	X	X	X	X	X	X
Français	X	X	X	X	X	X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Langue	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
Allemand	X	X	X	X	X	X
Espagnol	X	X	X	X	X	X
Coréen	X	X	X	X	X	X
Portugais	X	X	X	X	X	X
Néerlandais	X	X	X	X	X	X
Italien	X	X	X	X	X	X
Danois	X	X	X	X	X	X
Suédois	X	X	X	X	X	X
Hébreu	X	X	X	X	X	iOS uniquement
Arabe	X	X	X	X	X	X
Russe	X	X	X	X	X	X
Turc	X	X	Android uniquement	-	-	-
Polonais	X	X	X	-	-	-

Prise en charge des langues de droite à gauche

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Conformité FIPS 140-2

March 1, 2024

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

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

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

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

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

À propos de Citrix Endpoint Management

March 1, 2024

Citrix Endpoint Management est une solution Unified Endpoint Management (UEM) qui regroupe chaque application et point de terminaison dans une vue unifiée pour augmenter la sécurité et améliorer la productivité. Pour obtenir une vue d'ensemble de l'UEM, consultez la fiche technique de Citrix Tech Zone, Citrix Endpoint Management..

Citrix Endpoint Management propose la gestion d'appareils mobiles (MDM) et la gestion d'applications mobiles (MAM).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Les fonctionnalités MDM de Citrix Endpoint Management vous permettent d'effectuer les opérations suivantes :

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

Les fonctionnalités MAM de Citrix Endpoint Management vous permettent d'effectuer les opérations suivantes :

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

En combinant les fonctionnalités MDM et MAM, vous pouvez effectuer les opérations suivantes :

- Gérer un appareil fourni par l'entreprise via MDM
- Déployer des applications et des stratégies d'appareil
- Récupérer un inventaire logiciel
- Effacer des appareils
- Mettre à disposition des applications mobiles d'entreprise
- Verrouiller des applications et effacer les données sur les appareils

Le tableau suivant récapitule les fonctionnalités de Citrix Endpoint Management prises en charge pour MDM, MAM ou MDM+MAM.

Fonctionnalité (par plate-forme)	MDM (1)	MAM (2)	MDM+MAM
Android Entreprise :			
Prise en charge de l'inscription d'appareils	Oui	Oui	Oui
Prise en charge de l'authentification de domaine	Oui	Non	Oui
Prise en charge de l'authentification domaine + jeton de sécurité	Non	Non	Oui
Prise en charge de l'authentification du certificat client	Non	Oui	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fonctionnalité (par plate-forme)	MDM (1)	MAM (2)	MDM+MAM
Prise en charge de l'authentification certificat + domaine	Non	Non	Oui
Prise en charge du certificat client + jeton de sécurité	Non	Non	Oui
Prise en charge du fournisseur d'identité Azure AD	Oui	Non	Oui
Prise en charge du fournisseur d'identité Okta	Oui	Non	Oui
Connexion unique aux applications SaaS natives	Oui	Non	Oui
Prise en charge du réseau de mise à disposition de contenu Citrix pour les applications d'entreprise	Oui	Oui	Oui
Prise en charge du réseau de mise à disposition de contenu Citrix pour les applications MDX	Oui	Oui	Oui
Prise en charge des appareils partagés en provisionnant des appareils Android Enterprise dédiés	Oui	Non	Oui
Android (ancien) :			
Prise en charge de l'inscription d'appareils	Oui	Oui	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fonctionnalité (par plate-forme)	MDM (1)	MAM (2)	MDM+MAM
Prise en charge de l' authentification domaine ou domaine + jeton de sécurité	Non	Non	Oui
Prise en charge de l' authentification du certificat client	Non	Oui	Oui
Prise en charge de l' authentification certificat + domaine	Non	Non	Oui
Prise en charge du certificat client + jeton de sécurité	Non	Non	Oui
Prise en charge des fournisseurs d'identité Azure AD et Citrix	Oui	Non	Oui
Prise en charge du fournisseur d'identité Okta	Oui	Non	Oui
Connexion unique aux applications SaaS natives	Oui	Non	Oui
Prise en charge du réseau de mise à disposition de contenu Citrix pour les applications d' entreprise	Oui	Oui	Oui
Prise en charge du réseau de mise à disposition de contenu Citrix pour les applications MDX	Oui	Oui	Oui
Chrome :			
Prise en charge de l' inscription d'appareils	Oui	Non	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fonctionnalité (par plate-forme)	MDM (1)	MAM (2)	MDM+MAM
Prise en charge de l'authentification par nom d'utilisateur et mot de passe	Oui	Non	Oui
iOS :			
Prise en charge de l'inscription d'appareils	Oui	Oui	Oui
Prise en charge de l'authentification domaine ou domaine + jeton de sécurité	Non	Non	Oui
Prise en charge de l'authentification du certificat client	Non	Oui	Oui
Prise en charge de l'authentification certificat + domaine	Non	Non	Oui
Prise en charge des fournisseurs d'identité Azure AD et Citrix	Oui	Non	Oui
Prise en charge du fournisseur d'identité Okta	Oui	Non	Oui
Connexion unique aux applications SaaS natives	Oui	Non	Oui
Prise en charge du réseau de mise à disposition de contenu Citrix pour les applications d'entreprise	Oui	Oui	Oui
Prise en charge du réseau de mise à disposition de contenu Citrix pour les applications MDX	Oui	Oui	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fonctionnalité (par plate-forme)	MDM (1)	MAM (2)	MDM+MAM
Intégration d'Apple Éducation	Oui	Non	Oui
macOS :			
Prise en charge de l' inscription d'appareils	Oui	Non	Non
Prise en charge du domaine ou domaine + mot de passe unique	Oui	Non	Non
Prise en charge de l' URL d'invitation + mot de passe unique	Oui	Non	Non
Windows :			
Prise en charge de l' inscription d'appareils	Oui	Non	Non
Inscription automatique des appareils Windows 10 et Windows 11 via l' application Citrix Workspace	Oui	Non	Non
Prise en charge de l' authentification domaine ou domaine + jeton de sécurité	Oui	Non	Non
Prise en charge de l' authentification du certificat client	Oui	Non	Non
Prise en charge de l' authentification certificat + domaine	Oui	Non	Non
Authentification fédérée via le fournisseur d'identités Azure AD ou Citrix	Oui	Non	Non

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fonctionnalité (par plate-forme)	MDM (1)	MAM (2)	MDM+MAM
Prise en charge du réseau de mise à disposition de contenu Citrix pour les applications d'entreprise	Oui	Non	Non
Intégration de Workspace Environment Management (3)	Oui	Non	Non

> **Remarques :**
>
> (1) L'ordre de déploiement s'applique uniquement aux appareils d'un groupe de mise à disposition dont le profil d'inscription est configuré pour MDM.
>
> (2) L'inscription MAM nécessite NetScaler Gateway.
>
> (3) L'intégration WEM (Workspace Environment Management) permet d'accéder aux fonctionnalités MDM sur un large éventail de systèmes d'exploitation Windows.

Pour de plus amples informations, consultez Modes de gestion.

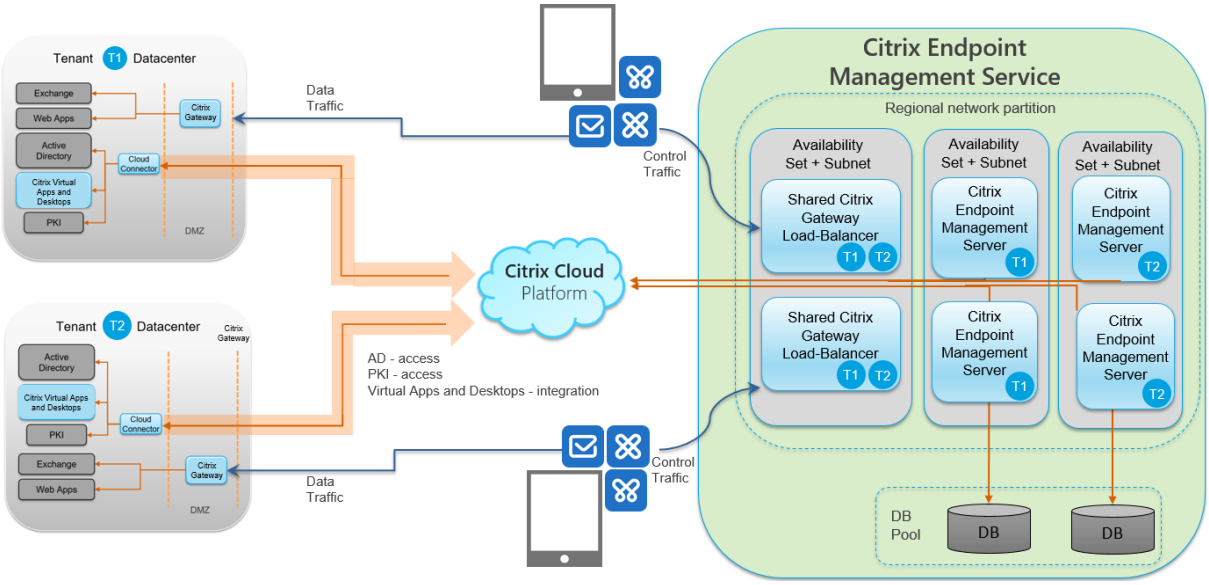
Architecture

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

- NetScaler Gateway permet aux utilisateurs d'accéder à distance à des applications mobiles et effectue le suivi des types d'appareils des utilisateurs.
- Citrix Endpoint Management est l'endroit où vous gérez ces applications et appareils.

Le schéma suivant illustre une architecture générale d'un déploiement cloud de Citrix Endpoint Management et son intégration avec votre data center.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Les sous-sections suivantes contiennent des diagrammes d'architecture de référence pour :

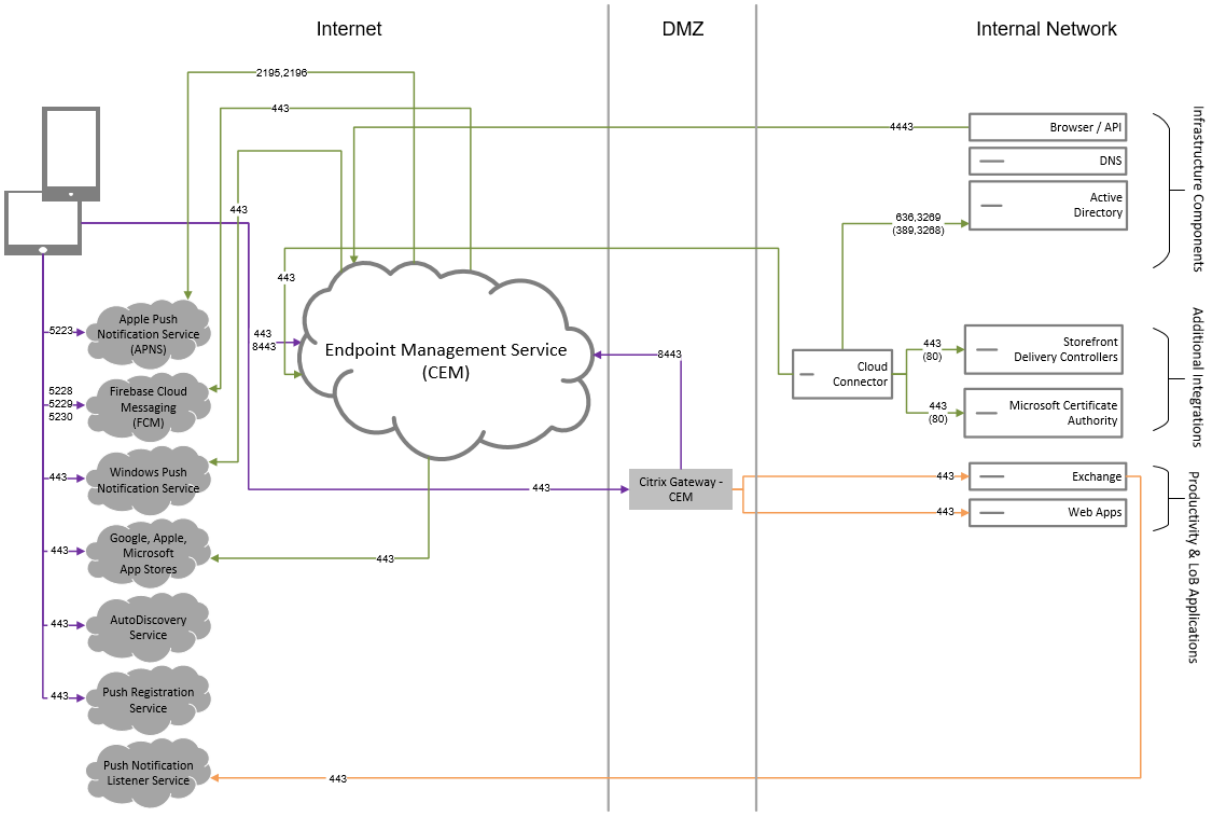
- Citrix Endpoint Management
- Des composants facultatifs tels qu'une autorité de certification externe, Citrix Endpoint Management Connector pour Exchange ActiveSync et le flux de trafic MDM+MAM Citrix Endpoint Management et MAM Intune.

Pour plus d'informations sur la configuration requise pour Citrix ADC et NetScaler Gateway, consultez la documentation du produit Citrix à l'adresse https://docs.citrix.com/.

Architecture de référence principale

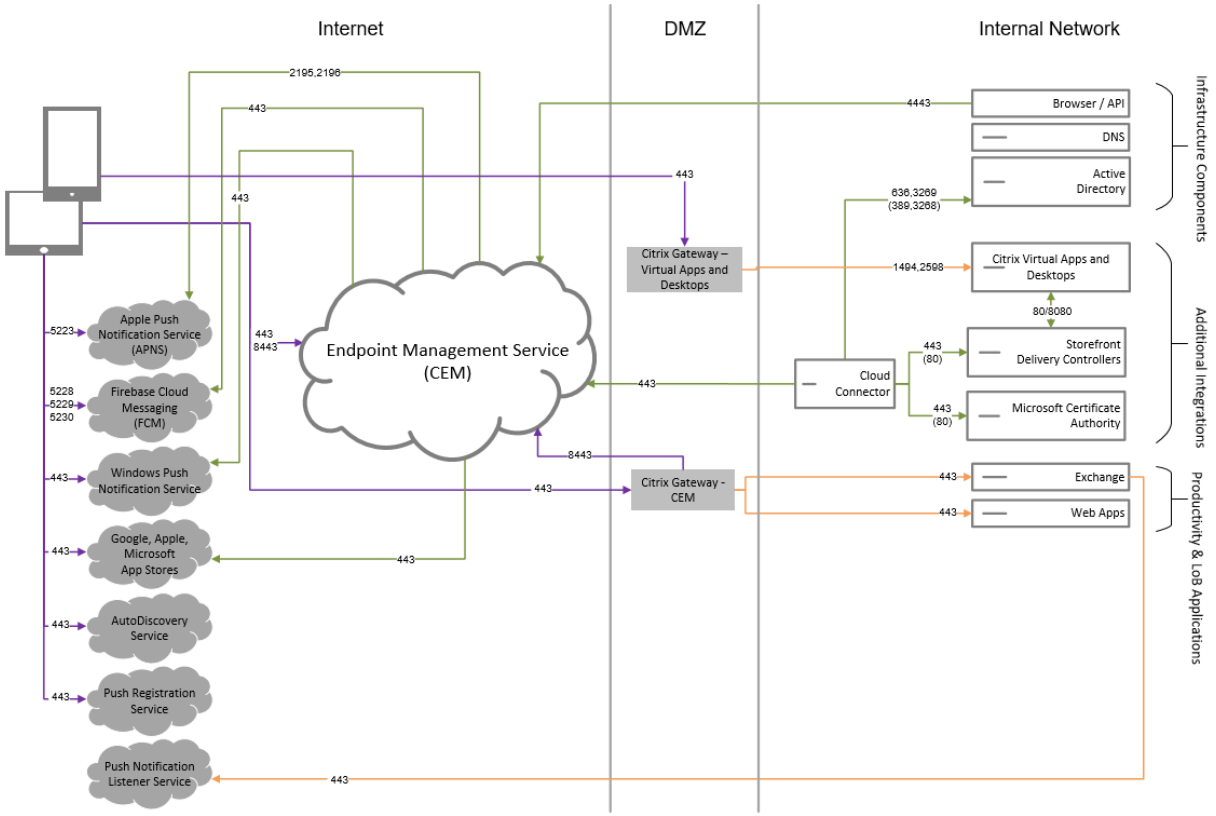
Pour les exigences en matière de port, consultez la section Configuration système requise.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



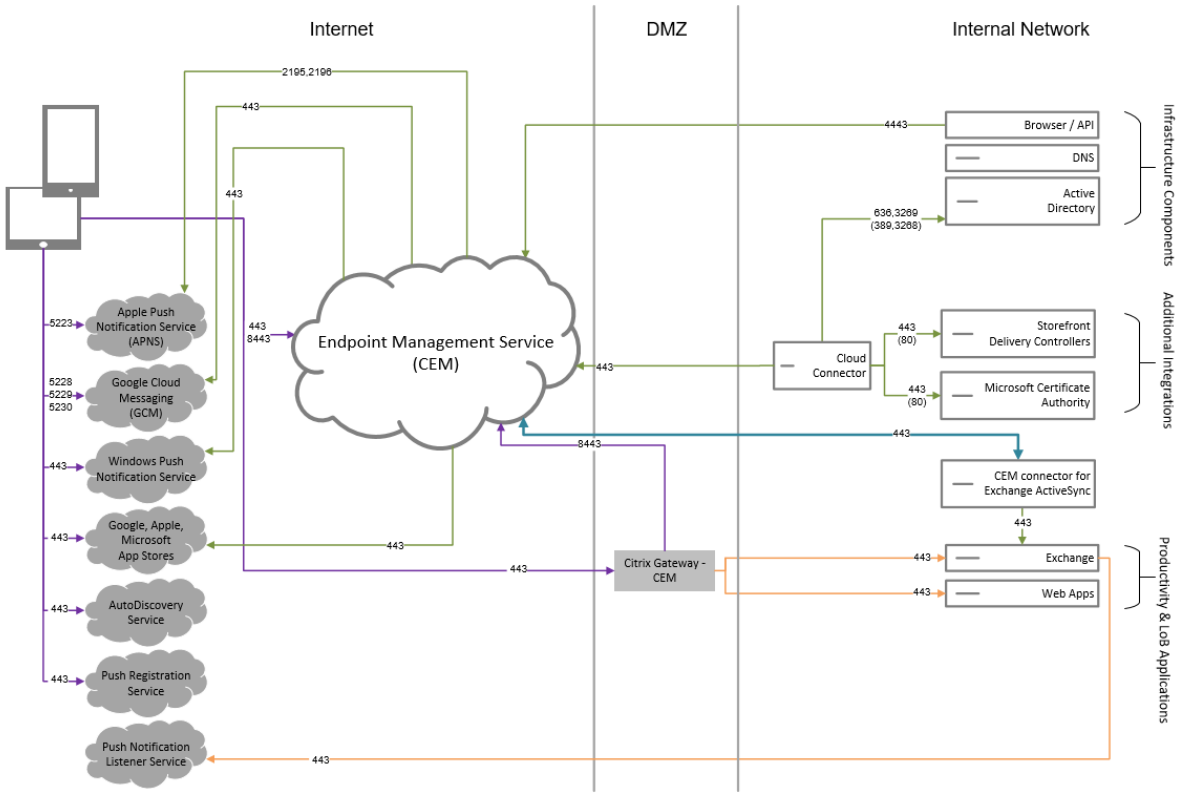
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Architecture de référence avec Citrix Virtual Apps and Desktops



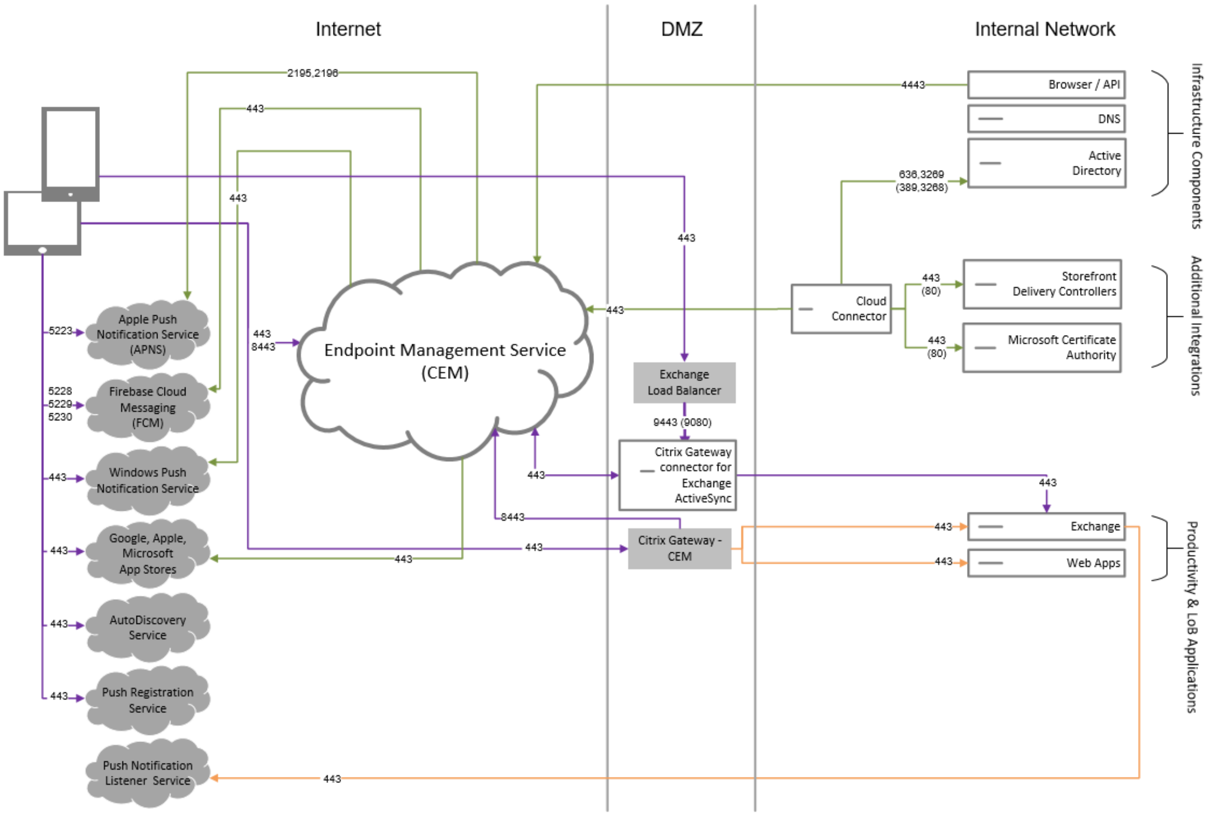
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Architecture de référence avec Citrix Endpoint Management Connector pour Exchange ActiveSync

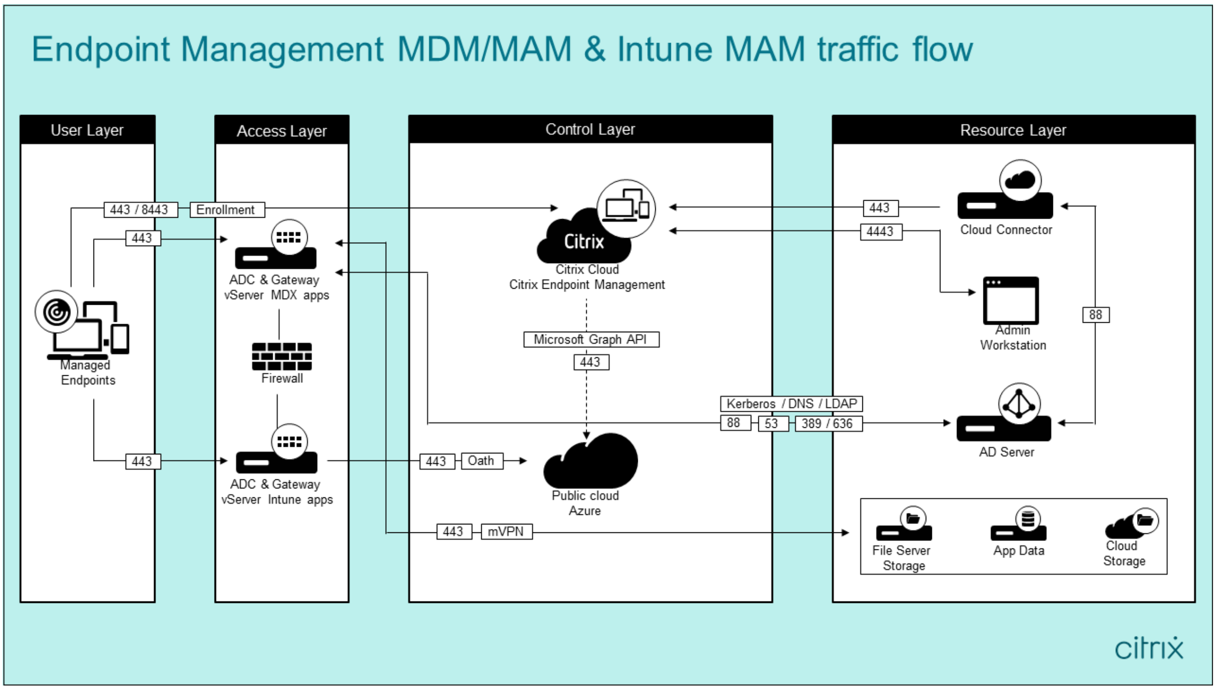


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Architecture de référence avec NetScaler Gateway Connector pour Exchange ActiveSync



Architecture de référence avec MDM+MAM Citrix Endpoint Management et MAM Intune



Emplacements des ressources

Placez les emplacements de ressources là où ils répondent le mieux aux besoins de votre entreprise. Par exemple : dans un cloud public, une succursale, un cloud privé ou un centre de données. Facteurs qui peuvent déterminer le choix de l'emplacement :

- Proximité des abonnés
- Proximité des données
- Exigences en matière de montée en charge
- Attributs de sécurité

Vous pouvez créer n'importe quel nombre d'emplacements de ressources. Par exemple, vous pouvez :

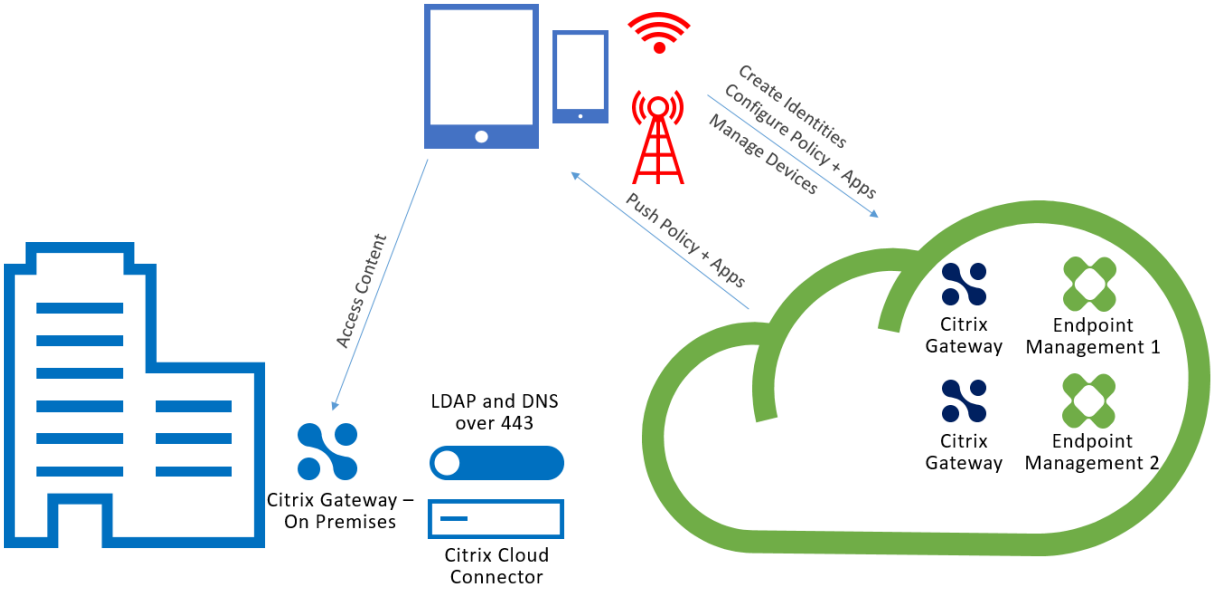
- Créer un emplacement de ressources dans votre centre de données pour le siège social en fonction des applications et des abonnés qui doivent être proches des données.
- Ajouter un emplacement de ressources distinct pour vos utilisateurs internationaux dans un cloud public. Ou créer des emplacements de ressources distincts dans les succursales pour fournir les applications les plus utilisées à proximité des employés de la succursale.
- Ajouter un autre emplacement de ressources sur un réseau distinct qui fournit des applications restreintes. Cette configuration offre une visibilité limitée aux autres ressources et abonnés sans avoir à ajuster les autres emplacements de ressources.

Cloud Connector

Cloud Connector authentifie et crypte toutes les communications entre Citrix Cloud et vos emplacements de ressources. Cloud Connector est nécessaire pour accéder aux services suivants : LDAP, fournisseurs d'identité, serveur PKI, requêtes DNS internes, Citrix Virtual Apps, NetScaler Gateway, Citrix Workspace et Microsoft Endpoint Manager.

Le schéma suivant illustre le flux du trafic pour Cloud Connector.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Cloud Connector établit les connexions avec Citrix Cloud. Cloud Connector n'accepte pas les connexions entrantes.

Cloud Connector est soumis à une charge élevée uniquement pendant l'inscription de l'appareil. Pour plus d'informations, consultez la section Considérations sur le dimensionnement et la scalabilité des Cloud Connector.

Une solution qui inclut la gestion des applications mobiles (MAM) nécessite un micro-VPN fourni par une passerelle NetScaler Gateway locale. Dans ce scénario :

- Les composants suivants résident dans votre centre de données :
  - Cloud Connector
  - NetScaler Gateway
  - Vos serveurs pour Exchange, applications Web, Active Directory et PKI
- Les appareils mobiles communiquent avec Citrix Endpoint Management et votre NetScaler Gateway sur site.

Composants Citrix Endpoint Management

Console Citrix Endpoint Management : Vous utilisez la console d'administration Citrix Endpoint Management pour configurer Citrix Endpoint Management. Pour de plus amples informations sur l'utilisation de la console Citrix Endpoint Management, consultez les articles sous Citrix Endpoint Management. Citrix vous avertit lorsque les articles Nouveautés Citrix Endpoint Management sont mis à jour pour une nouvelle version.

Tenez compte des différences suivantes entre le service Citrix Endpoint Management et les versions locales :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Le client d'assistance à distance n'est pas disponible dans Citrix Endpoint Management.
- Citrix ne prend pas en charge l'intégration de syslog dans Citrix Endpoint Management avec un serveur syslog sur site. Au lieu de cela, vous pouvez télécharger les journaux à partir de la page **Dépannage et support** dans la console Citrix Endpoint Management. Ce faisant, vous devez cliquer sur **Tout télécharger**.

SDK MAM : Le MDX Toolkit devrait atteindre la fin de son cycle de vie en juillet 2023. Pour continuer à gérer vos applications d'entreprise, vous devez incorporer le SDK MAM.

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

Applications de productivité mobiles : Les applications de productivité mobiles développées par Citrix offrent une suite d'outils de productivité et de communication au sein de l'environnement Citrix Endpoint Management. Ce sont vos politiques d'entreprise qui sécurisent ces applications. Pour de plus amples informations, consultez la section Applications de productivité mobiles.

Citrix Endpoint Management Connector pour Exchange ActiveSync : Citrix Endpoint Management Connector pour Exchange ActiveSync fournit un accès sécurisé à la messagerie aux utilisateurs qui utilisent des applications de messagerie mobile natives. Le connecteur pour Exchange ActiveSync fournit un filtrage ActiveSync au niveau du service Exchange. Par conséquent, le filtrage ne se produit qu'une fois que le courrier parvient au service Exchange, et non lorsqu'il entre dans l'environnement Citrix Endpoint Management. Le connecteur ne nécessite pas l'utilisation de NetScaler Gateway. Vous pouvez déployer le connecteur sans modifier le routage du trafic ActiveSync existant. Pour plus d'informations, consultez la section Citrix Endpoint Management Connector pour Exchange ActiveSync.

NetScaler Gateway Connector pour Exchange ActiveSync. NetScaler Gateway Connector pour Exchange ActiveSync fournit un accès sécurisé à la messagerie aux utilisateurs qui utilisent des applications de messagerie mobile natives. Le connecteur pour Exchange ActiveSync fournit un filtrage ActiveSync au niveau du périmètre. Le filtrage utilise NetScaler Gateway comme proxy pour le trafic ActiveSync. Le composant de filtrage se trouve donc sur le chemin du flux de trafic de messagerie, interceptant le courrier à l'entrée ou à la sortie de l'environnement. Le connecteur pour Exchange ActiveSync agit comme un intermédiaire entre NetScaler Gateway et Citrix Endpoint Management. Pour plus d'informations, consultez la section NetScaler Gateway Connector pour Exchange ActiveSync.

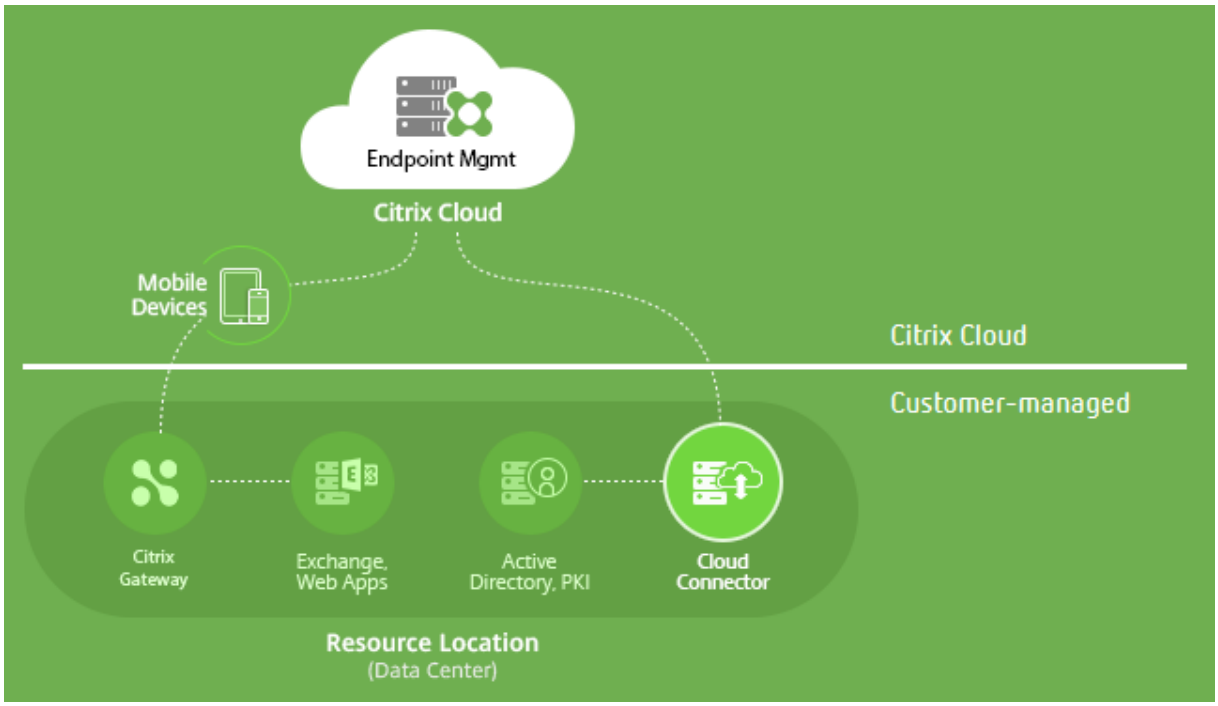
Vue d'ensemble de la sécurité technique de Citrix Endpoint Management

Citrix Cloud gère le plan de contrôle des environnements Citrix Endpoint Management. Le plan de contrôle comprend Citrix Endpoint Management Server, l'équilibrage de charge Citrix ADC et une base

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de données mono-locataire. Le service de cloud s'intègre à un data center client à l'aide de Citrix Cloud Connector. Les clients de Citrix Endpoint Management qui utilisent Cloud Connector gèrent généralement NetScaler Gateway dans leurs data centers.

La figure suivante illustre le service et ses limites de sécurité.



Les informations de cette section :

- fournissent une introduction aux fonctionnalités de sécurité de Citrix Cloud ;
- définissent la répartition des responsabilités entre Citrix et les clients pour la sécurisation du déploiement de Citrix Cloud ;
- ne constituent pas un guide de configuration et d'administration pour Citrix Cloud ou l'un de ses composants ou services.

Pour plus d'informations sur la technologie utilisée par Citrix Endpoint Management pour fournir une sécurité complète de bout en bout, consultez Security and Productivity for the Mobile Enterprise.

Flux de données

Le plan de contrôle dispose d'un accès en lecture limité aux objets utilisateur et groupe. Ces objets résident dans votre répertoire, DNS et services similaires. Le plan de contrôle accède à ces services via Citrix Cloud Connector via des connexions HTTPS sécurisées.

Les données de l'entreprise, telles que les e-mails, l'intranet et le trafic d'applications Web, circulent directement entre un appareil et les serveurs d'applications via NetScaler Gateway. NetScaler Gateway est déployé dans le data center du client.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Isolation des données

Le plan de contrôle stocke les métadonnées nécessaires à la gestion des appareils utilisateurs et de leurs applications mobiles. Le service lui-même consiste en une combinaison de composants multi-locataires et mono-locataires. Cependant, par l'architecture de service, les métadonnées client sont toujours stockées séparément pour chaque locataire et sécurisées à l'aide d'informations d'identification uniques.

Gestion des informations d'identification

Le service gère les types d'informations d'identification suivants :

- **Informations d'identification de l'utilisateur :** les informations d'identification de l'utilisateur sont transmises de l'appareil au plan de contrôle via une connexion HTTPS. Le plan de contrôle valide ces informations d'identification avec un répertoire dans le répertoire du client sur une connexion sécurisée.
- **Informations d'identification d'administrateur :** les administrateurs s'authentifient auprès de Citrix Cloud, qui utilise le système d'authentification de Citrix Online. Ce processus génère un jeton JWT (JSON Web Token) à usage unique, qui permet à l'administrateur d'accéder au service.
- **Informations d'identification Active Directory :** le plan de contrôle nécessite des informations d'identification de liaison pour lire les métadonnées d'utilisateur provenant d'Active Directory. Ces informations d'identification sont chiffrées à l'aide du chiffrement AES-256 et enregistrées dans une base de données par locataire.

Considérations de déploiement

Citrix vous recommande de consulter la documentation sur les meilleures pratiques publiées pour le déploiement de NetScaler Gateway dans vos environnements.

Plus de ressources

Les clients sont invités à consulter les bulletins de sécurité relatifs à leurs produits Citrix. Pour plus d'informations sur les bulletins de sécurité nouveaux et mis à jour, consultez Bulletins de sécurité Citrix. Pensez également à vous inscrire pour recevoir des alertes dans vos paramètres d'alerte.

Consultez les ressources suivantes pour de plus amples informations sur la sécurité :

- Site de sécurité de Citrix : https://www.citrix.com/security
- Documentation Citrix Cloud : Guide de déploiement sécurisé pour la plate-forme Citrix Cloud
- Guide de déploiement sécurisé pour Citrix ADC

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Intégration au logiciel Mobile Threat Defense

Le logiciel MTD (Mobile Threat Defense) détecte, analyse et permet d'empêcher les cyberattaques avancées contre les appareils mobiles d'entreprise. L'utilisation du logiciel MTD conjointement avec Citrix Endpoint Management unifié (UEM) augmente la sécurité et la visibilité de votre organisation.

Le logiciel MTD fournit des données sur les menaces utilisées par Citrix Endpoint Management pour :

- Protéger contre les logiciels malveillants, le phishing, les attaques réseau et les attaques « man-in-the-middle »
- Déterminer l'état de conformité des appareils
- Déterminer les niveaux de risque
- Prenez des mesures basées sur des stratégies pour protéger vos applications, vos données, vos appareils et votre réseau mobile

Citrix Endpoint Management s'intègre aux fournisseurs MTD suivants :

- Check Point
- Lookout
- Wandera
- Zimperium

Pour plus d'informations ou pour demander une démonstration, contactez nos partenaires MTD ou votre représentant commercial Citrix.

Intégration de Citrix Endpoint Management avec Microsoft Endpoint Manager

March 1, 2024

L'intégration de Citrix Endpoint Management avec Microsoft Endpoint Manager (MEM) ajoute la valeur du micro VPN de Citrix Endpoint Management aux applications compatibles Microsoft Intune, telles que le navigateur Microsoft Edge.

Pour activer l'intégration, contactez l'équipe Citrix Cloud Operations.

Cette version prend en charge les cas d'utilisation suivants :

- MAM Intune avec MDM+MAM Citrix Endpoint Management.

  Cet article se concentre sur le cas d'utilisation Intune MAM + Citrix Endpoint Management MDM+MAM. Après avoir ajouté Citrix en tant que fournisseur MDM, configurez les applications gérées Intune en vue de les déployer sur les appareils.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

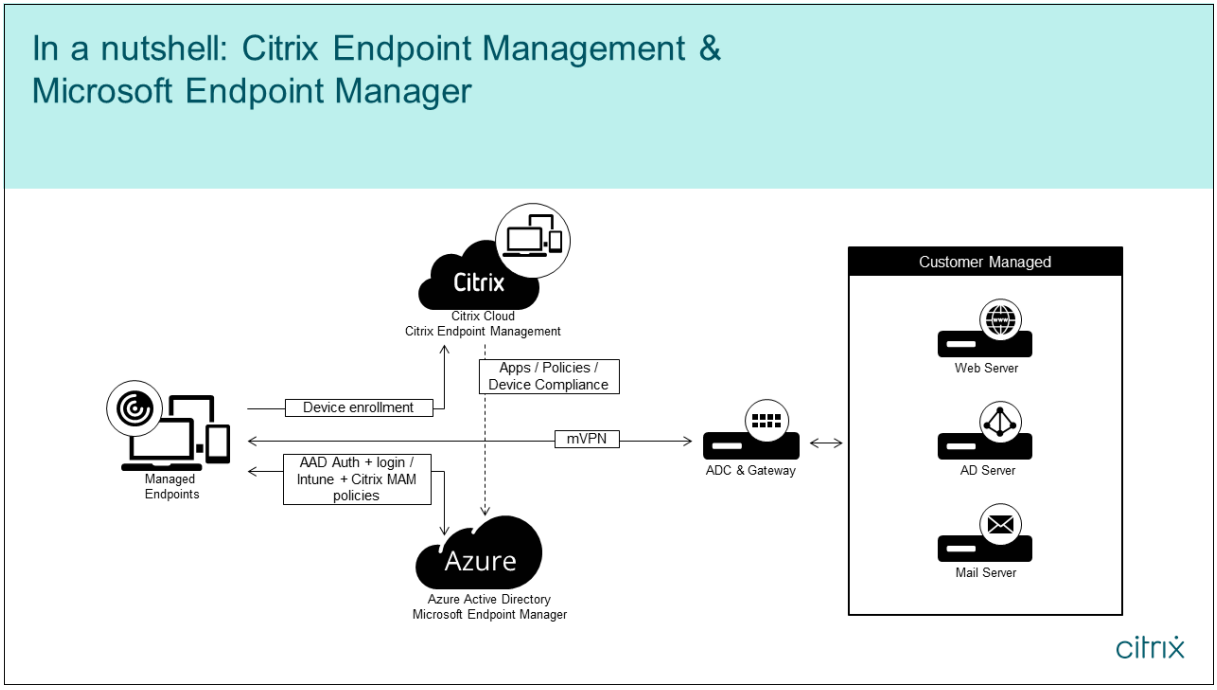
> **Important :**
>
> Pour ce cas d'utilisation, Citrix Secure Mail ne prend pas en charge l'intégration à Intune. Citrix Secure Mail ne fonctionne que pour les appareils inscrits en mode MDX.

- MAM Intune et MDM Citrix Endpoint Management.
- MAM Intune.
- MAM Intune et MDM Intune. Citrix Secure Mail pour iOS prend en charge l'authentification unique pour ce cas d'utilisation.

Pour obtenir un guide graphique facile à suivre pour configurer l'intégration de Citrix Endpoint Management avec MEM, consultez le Guide de mise en route.

Pour plus d'informations sur l'intégration avec l'accès conditionnel Azure AD, consultez la section Intégrer avec l'accès conditionnel Azure AD.

Le diagramme suivant fournit une vue d'ensemble de l'intégration de Citrix Endpoint Management avec Microsoft Endpoint Manager.



Configuration système requise

Activation MDX

- SDK MAM

  ou

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- MDX Toolkit

Microsoft

- Accès Azure Active Directory (AD) (avec privilèges d'administrateur de locataires)
- Locataire activé par Intune

Règle de pare-feu

- Activer une règle de pare-feu pour autoriser le trafic DNS et SSL à partir d'une adresse IP de sous-réseau NetScaler Gateway vers `*.manage.microsoft.com`, `https://login.microsoftonline.com` et `https://graph.windows.net` (ports 53 et 443)

Logiciels requis

- **Navigateur Microsoft Edge :** le SDK Applications mobiles est intégré à l'application de navigateur Microsoft Edge pour iOS et Android. Pour plus d'informations sur Microsoft Edge, veuillez consulter la documentation de Microsoft Edge.
- **Compte Citrix Cloud :** pour ouvrir un compte Citrix et demander une version d'évaluation de Citrix Endpoint Management, contactez votre représentant Citrix. Lorsque vous êtes prêt à continuer, accédez à https://onboarding.cloud.com. Pour plus d'informations sur la demande d'un compte Citrix Cloud, voir S'inscrire à Citrix Cloud.

  > **Remarque :**
  >
  > L'e-mail que vous fournissez doit être une adresse qui n'est pas associée à Azure AD. Vous pouvez utiliser n'importe quel service de messagerie gratuit.

- **Certificats APNs pour iOS :** assurez-vous de configurer le certificat APNs pour iOS. Pour en savoir plus sur la configuration de ces certificats, consultez cet article de blog Citrix : Creating and Importing APNs Certificates.
- **Azure AD Sync :** configurez la synchronisation entre Azure AD et le répertoire Active Directory local. N'installez pas l'outil de synchronisation AD sur la machine du contrôleur de domaine. Pour plus d'informations sur la configuration de cette synchronisation, consultez la documentation Microsoft sur Azure Active Directory.

Configuration de NetScaler Gateway

Si vous configurez un nouveau déploiement Citrix Endpoint Management, installez l'une des appliances NetScaler Gateway suivantes :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- NetScaler Gateway VPX 3000 ou version supérieure
- Instance NetScaler Gateway MPX ou SDX dédiée

Pour utiliser NetScaler Gateway avec l'intégration de Citrix Endpoint Management à MEM, procédez comme suit :

- Configurez NetScaler Gateway avec une interface de gestion et une adresse IP de sous-réseau.
- Utilisez TLS 1.2 pour toutes les communications client-serveur. Pour plus d'informations sur la configuration de TLS 1.2 pour NetScaler Gateway, consultez la section CTX247095.

Si vous utilisez l'intégration Citrix Endpoint Management à MEM avec un déploiement MDM+MAM Citrix Endpoint Management, configurez deux instances Citrix Gateway. Le trafic d'application MDX est acheminé via une instance NetScaler Gateway. Le trafic d'application Intune est acheminé via l'autre instance NetScaler Gateway. Configurez les éléments suivants :

- Deux adresses IP publiques.
- Éventuellement, une adresse IP définie via la traduction d'adresse réseau (NAT).
- Deux noms DNS. Exemple : `https://mam.company.com`.
- Deux certificats SSL publics. Configurez les certificats qui correspondent au nom DNS public réservé ou qui utilisent des certificats génériques.
- Un équilibreur de charge MAM avec une adresse IP RFC 1918 interne non routable.
- Un compte de service LDAP Active Directory.

Accepter les invites d'autorisations déléguées

Pour les applications gérées qui nécessitent l'authentification des utilisateurs, les applications demandent des autorisations d'applications exposées par Microsoft Graph. Lorsque les invites d'autorisation sont acceptées, l'application peut accéder aux ressources et API requises. Certaines applications nécessitent le consentement de l'administrateur global pour Microsoft Azure AD. Pour ces autorisations déléguées, l'administrateur global doit accorder à Citrix Cloud l'autorisation de demander des jetons. Les jetons activent ensuite les autorisations suivantes. Pour plus d'informations, consultez la référence des autorisations de Microsoft Graph.

- **Se connecter et lire le profil utilisateur :** cette autorisation permet aux utilisateurs de se connecter à Azure AD. Citrix ne peut pas afficher les informations d'identification de l'utilisateur.
- **Lire les profils de base de tous les utilisateurs :** l'application lit les propriétés du profil pour les utilisateurs de l'organisation. Les propriétés comprennent le nom d'affichage, le prénom et le nom, ainsi que l'adresse e-mail et la photo des utilisateurs de l'organisation.
- **Lire tous les groupes :** cette autorisation permet de spécifier les groupes Azure AD pour l'attribution d'applications et de stratégies.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Accéder au répertoire en tant qu'utilisateur connecté :** cette autorisation vérifie l'abonnement Intune et active les configurations NetScaler Gateway et VPN.
- **Lire et écrire des applications Microsoft Intune :** l'application peut lire et écrire les éléments suivants :
  - Propriétés gérées par Microsoft
  - Affectations de groupe et état des applications
  - Configurations d'applications
  - Stratégies de protection des applications

En outre, au cours de la configuration de NetScaler Gateway, l'administrateur global Azure AD doit :

- Approuver le répertoire Active Directory choisi pour le micro VPN. L'administrateur global doit également générer un secret client que NetScaler Gateway utilise pour communiquer avec Azure AD et Intune.
- Il ne doit pas avoir le rôle d'administrateur Citrix. L'administrateur Citrix attribue des comptes Azure AD aux utilisateurs dotés des privilèges d'administrateur d'application Intune appropriés. L'administrateur Intune a ensuite le rôle d'administrateur Citrix Cloud pour gérer Intune à partir de Citrix Cloud.

> **Remarque :**
>
> Citrix utilise uniquement le mot de passe de l'administrateur global Intune lors de l'installation et redirige l'authentification vers Microsoft. Citrix ne peut pas accéder au mot de passe.

Pour configurer l'intégration de Citrix Endpoint Management à MEM

1. Ouvrez une session sur le site Citrix Cloud et demandez une évaluation pour Citrix Endpoint Management.
2. Un ingénieur commercial planifie une réunion d'intégration avec vous. Faites-lui savoir que vous souhaitez intégrer Citrix Endpoint Management à MEM. Lorsque votre demande est approuvée, cliquez sur **Gérer**.
3. À partir de là, vous pouvez cliquer sur l'icône d'engrenage en haut à droite de votre site ou cliquer sur **Configurer le site**.
4. Suivez le lien vers la page **Gestion des identités et des accès** fourni à la première étape.
5. Cliquez sur **Connecter** pour connecter votre installation Azure AD.
6. Entrez une URL d'ouverture de session unique que l'administrateur Azure AD utilise pour ouvrir une session, puis cliquez sur **Confirmer**.
7. Ajoutez un compte administrateur global Azure AD, puis acceptez la demande d'autorisation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. Vérifiez que votre instance Azure AD se connecte correctement. Pour indiquer une connexion réussie, le texte **Non connecté** devient **Activé**.
9. Cliquez sur l'onglet **Administrateurs**, puis ajoutez votre administrateur Azure AD Intune en tant qu'administrateur Citrix Cloud. Sélectionnez Azure AD ou Citrix Identity dans le menu déroulant, puis recherchez le nom d'utilisateur que vous souhaitez ajouter. Cliquez sur **Inviter**, puis accordez à l'utilisateur un **accès complet** ou un **accès personnalisé** avant de cliquer sur **Envoyer une invitation**.

   > **Remarque :**
   >
   > Citrix Endpoint Management nécessite les règles suivantes pour l'**accès personnalisé** : Bibliothèque et Citrix Endpoint Management.

   L'administrateur Azure AD Intune reçoit alors une invitation par e-mail pour créer un mot de passe et se connecter à Citrix Cloud. Avant que l'administrateur ne se connecte, assurez-vous de vous déconnecter de tous les autres comptes.

   L'administrateur Azure AD Intune doit suivre les étapes restantes de cette procédure.
10. Une fois connecté avec le nouveau compte, sous **Citrix Endpoint Management**, cliquez sur **Gérer**. Si vous configurez tout correctement, la page indique que l'administrateur Azure AD est connecté et que votre abonnement Intune est valide.

Pour configurer NetScaler Gateway pour un micro VPN

Pour utiliser un micro VPN avec Intune, vous devez configurer NetScaler Gateway pour l'authentification auprès d'Azure AD. Un serveur virtuel NetScaler Gateway existant ne fonctionne pas pour ce cas d'utilisation.

Tout d'abord, configurez Azure AD pour qu'il se synchronise avec le répertoire Active Directory local. Cette étape est nécessaire pour s'assurer que l'authentification entre Intune et NetScaler Gateway se produit correctement.

1. Dans la console Citrix Cloud, sous **Citrix Endpoint Management**, cliquez sur **Manage**.
2. En regard de **Micro VPN**, cliquez sur **Configure Micro VPN**.
3. Entrez un nom pour le service micro VPN et l'URL externe de votre NetScaler Gateway, puis cliquez sur **Next**.

   Ce script configure NetScaler Gateway pour la prise en charge d'Azure AD et des applications Intune.
4. Cliquez sur **Download Script**. Le fichier .zip comprend un fichier readme avec des instructions pour implémenter le script. Même si vous pouvez enregistrer et quitter à partir de cette étape,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

le micro VPN n'est pas configuré tant que vous n'avez pas exécuté le script sur votre installation NetScaler Gateway.

> **Remarque :**
>
> Lorsque vous avez terminé le processus de configuration de NetScaler Gateway, si vous voyez un état OAuth autre que COMPLETE, reportez-vous à la section Dépannage.

Pour configurer la gestion des appareils

Si vous souhaitez gérer des appareils en plus des applications, choisissez une méthode de gestion des appareils. Vous pouvez utiliser Citrix Endpoint Management MDM+MAM ou Intune MDM.

> **Remarque :**
>
> La console est par défaut Intune MDM. Pour utiliser Intune en tant que fournisseur MDM, consultez la documentation Microsoft Intune.

1. Dans la console Citrix Cloud, sous « Citrix Endpoint Management integration with MEM », cliquez sur **Manage**. En regard de **Device Management - Optional**, cliquez sur **Configure MDM**.
2. Entrez un nom de site unique, sélectionnez la région cloud la plus proche de vous, puis cliquez sur **Request a Site**. Vous recevrez un e-mail dès que votre site est prêt.
3. Cliquez sur **OK** pour fermer l'invite. Sélectionnez un emplacement Active Directory à associer à votre site ou créez un emplacement de ressources, puis cliquez sur **Suivant**.
4. Cliquez sur **Download Cloud Connector** et suivez les instructions à l'écran pour installer le connecteur. Après l'installation, cliquez sur **Test Connection** pour vérifier la connexion entre Citrix Cloud et le Cloud Connector.
5. Cliquez sur **Save & Exit** pour terminer. Votre emplacement de ressources apparaît. Cliquez sur **Finish** pour revenir à l'écran des paramètres.
6. Vous pouvez désormais accéder à la console Citrix Endpoint Management à partir de la vignette de votre site. À partir de là, vous pouvez effectuer des tâches de gestion MDM et attribuer des stratégies d'appareil. Consultez la section Stratégies d'appareil pour de plus amples informations sur les stratégies d'appareil.

Configurer les applications gérées par Intune pour les distribuer sur les appareils

Pour configurer les applications gérées par Intune en vue de leur distribution :

- Ajouter les applications à la bibliothèque Citrix Cloud
- Créer des stratégies Citrix Endpoint Management pour contrôler le flux de données
- Créer un groupe de mise à disposition pour les applications et les stratégies

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ajouter des applications Microsoft Intune à la bibliothèque Citrix Cloud

Pour chaque application que vous souhaitez ajouter :

1. Dans la console Citrix Cloud, cliquez sur l'icône de menu, puis cliquez sur **Bibliothèque**.
2. Cliquez sur l'icône de signe plus en haut à droite, puis cliquez sur **Add a Mobile app**.
3. Si Android Enterprise est configuré dans la console Citrix Endpoint Management, sélectionnez **Applications Microsoft Intune** sous **Choisir une application**. Sélectionnez un modèle d'application à personnaliser ou cliquez sur **Upload my own App**.

   Citrix fournit les modèles d'application existants, chacun accompagné d'un ensemble de stratégies par défaut préconfigurées. Pour les applications que les clients chargent, les stratégies suivantes s'appliquent :

   - **Fichiers MDX :** inclut les applications pour lesquelles le SDK MAM est activé ou les applications encapsulées avec MDX, telles que :
     - Stratégies de protection des applications Intune et stratégies MDX par défaut contenues dans le package
     - Applications du magasin public, telles que les stratégies de protection des applications Intune et les stratégies MDX par défaut qui correspondent à l'ID du bundle ou de l'ID du package
   - **Fichiers IPA :** stratégies de protection des applications Intune.
   - **Fichiers APK :** stratégies de protection des applications Intune.

   > **Remarque :**
   >
   > Si l'application n'est pas encapsulée avec Intune, les stratégies de protection des applications Intune ne s'appliquent pas.

4. Cliquez sur **Upload my own App** et chargez votre fichier encapsulé .mdx ou Intune.
5. Entrez un nom et une description pour l'application, indiquez si l'application est facultative ou obligatoire, puis cliquez sur **Suivant**.
6. Configurez les paramètres de l'application. Les configurations suivantes permettent aux conteneurs Citrix Endpoint Management et Intune d'échanger des données.

   - **Autoriser les applications à recevoir des données provenant d'autres applications :** sélectionnez **Applications gérées par stratégie**.
   - **Autoriser l'application à transférer des données vers d'autres applications :** sélectionnez **Toutes les applications**.
   - **Restreindre les fonctions couper, copier et coller avec d'autres applications :** sélectionnez **Applications gérées par stratégie**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. Configurez les référentiels de stockage pour les données enregistrées. Pour **Select which storage services corporate data can be saved to** (Sélectionnez les services de stockage dans lesquels les données d'entreprise sont enregistrées), sélectionnez **LocalStorage**.
8. Facultatif : définissez les stratégies Réadressage des données, Accès et Code PIN pour l'application. Cliquez sur **Suivant**.
9. Consultez les informations récapitulatives de l'application, puis cliquez sur **Terminer**.

   Le processus de configuration de l'application peut prendre quelques minutes. Une fois le processus terminé, un message indique que l'application a été publiée dans la bibliothèque.
10. Pour affecter des groupes d'utilisateurs à l'application, cliquez sur **Attribuer des utilisateurs**.
11. Dans la zone de recherche, recherchez des groupes d'utilisateurs et cliquez pour les ajouter. Vous ne pouvez pas ajouter d'utilisateurs individuels.
12. Lorsque vous avez ajouté tous les groupes souhaités, fermez la fenêtre en cliquant sur le X.

    Vous pouvez rencontrer une erreur lors de l'ajout de groupes d'utilisateurs. Cette erreur se produit lorsque le groupe d'utilisateurs n'a pas été synchronisé avec le répertoire local Active Directory.

Ajouter des applications Android Enterprise à la bibliothèque Citrix Cloud

Pour ajouter des applications Android Enterprise à la bibliothèque Citrix Cloud et définir des stratégies de protection des applications Intune, configurez votre environnement cloud avec les éléments suivants :

- Fédérez Citrix Cloud avec votre compte Azure Active Directory (AAD). Voir Connecter Azure Active Directory à Citrix Cloud.
- Configurez LDAP et Cloud Connector dans Citrix Endpoint Management.
- Configurez Android Enterprise dans Citrix Endpoint Management. Assurez-vous que les appareils Android Enterprise s'inscrivent à MDM+MAM. Pour configurer Android Enterprise, consultez Android Enterprise.

Suivez cette procédure pour ajouter des applications Android Enterprise à la console Citrix Endpoint Management et à la console Intune simultanément. Pour chaque application Android Enterprise que vous souhaitez ajouter, procédez comme suit :

1. Dans la console Citrix Cloud, cliquez sur l'icône de menu, puis cliquez sur **Bibliothèque**.
2. Cliquez sur l'icône de signe plus en haut à droite, puis cliquez sur **Add a Mobile app**.
3. Sous **Choisir une application**, sélectionnez **Applications Android Enterprise**.
4. Recherchez une application et approuvez-la dans la fenêtre Google Play Store d'entreprise. Une fois la fenêtre Google fermée, cliquez sur **Suivant**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Ajoutez les détails de l'application, puis cliquez sur **Suivant**.
6. Si vous avez recherché et sélectionné une application de productivité mobile Citrix, vous pouvez configurer des stratégies Micro VPN. Après avoir configuré ces stratégies, cliquez sur **Suivant**.
7. Configurez les stratégies de protection des applications Intune. Cliquez sur **Suivant**.
8. Configurez les paramètres de l'application. Les configurations suivantes permettent aux conteneurs Citrix Endpoint Management et Intune d'échanger des données.
   - **Autoriser les applications à recevoir des données provenant d'autres applications :** sélectionnez **Applications gérées par stratégie**.
   - **Autoriser l'application à transférer des données vers d'autres applications :** sélectionnez **Toutes les applications**.
   - **Restreindre les fonctions couper, copier et coller avec d'autres applications :** sélectionnez **Applications gérées par stratégie**.
9. Configurez les référentiels de stockage pour les données enregistrées. Pour **Select which storage services corporate data can be saved to** (Sélectionnez les services de stockage dans lesquels les données d'entreprise sont enregistrées), sélectionnez **LocalStorage**.
10. Facultatif : définissez les stratégies Réadressage des données, Accès et Code PIN pour l'application. Cliquez sur **Suivant**.
11. Consultez les informations récapitulatives de l'application, puis cliquez sur **Terminer**.

    Le processus de configuration de l'application peut prendre quelques minutes. Une fois le processus terminé, un message indique que l'application a été publiée dans la bibliothèque. L'application est disponible sur les consoles Citrix Endpoint Management et Intune. Dans la console Citrix Endpoint Management, l'application fait partie d'un nouveau groupe de mise à disposition et est identifiée comme une application de magasin d'applications public.
12. Pour affecter des groupes d'utilisateurs à l'application, cliquez sur **Attribuer des utilisateurs**.
13. Dans la zone de recherche, recherchez des groupes d'utilisateurs et cliquez pour les ajouter. Vous ne pouvez pas ajouter d'utilisateurs individuels.
14. Lorsque vous avez ajouté tous les groupes souhaités, fermez la fenêtre en cliquant sur le X.

    Vous pouvez rencontrer une erreur lors de l'ajout de groupes d'utilisateurs. Cette erreur se produit lorsque le groupe d'utilisateurs n'a pas été synchronisé avec le répertoire local Active Directory.

Contrôler le type de données transférées entre les applications gérées

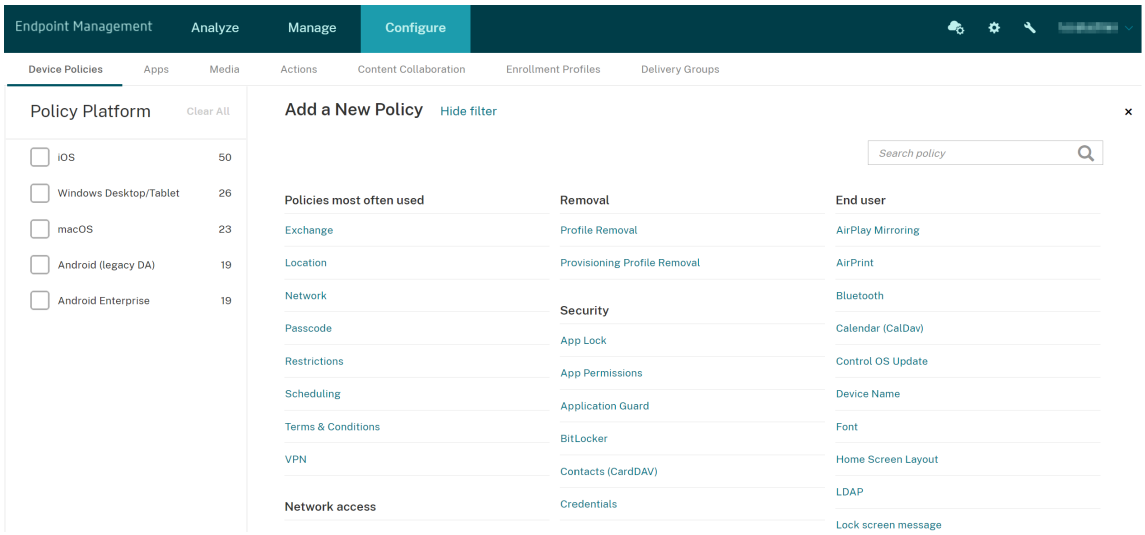
Contrôlez le type de données pouvant être transférées entre des applications gérées dans les conteneurs Citrix Endpoint Management ou Intune à l'aide des stratégies Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Vous pouvez configurer une stratégie Restrictions pour autoriser uniquement les données marquées comme « corporate » (entreprise). Configurez une stratégie Configuration de l'application pour baliser les données.

Pour configurer la stratégie Restrictions :

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Stratégies d'appareil**.
2. Sur la page **Stratégies d'appareil**, cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.



3. Cliquez sur **Restrictions** dans la liste des stratégies.
4. Sur la page **Informations sur la stratégie**, tapez un nom et (éventuellement) une description pour la stratégie. Cliquez sur **Suivant**.
5. Pour créer une stratégie pour les applications iOS, sélectionnez **iOS** dans le volet **Plates-formes**.
6. Sous **Sécurité - Autoriser**, définissez **Documents provenant d'applications gérées dans les applications non gérées** sur **Désactivé**. La valeur **Désactivé** définit également **Les applications non gérées lisent les contacts gérés** et **Les applications gérées écrivent sur les contacts non gérés** sur **Désactivé**. Cliquez sur **Suivant**.
7. Cliquez sur **Suivant** jusqu'à ce que le bouton **Enregistrer** s'affiche. Cliquez sur **Enregistrer**.

Configurez la stratégie Configuration de l'application pour chaque application :

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Stratégies d'appareil**.
2. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.
3. Cliquez sur **Configuration de l'application** dans la liste des stratégies.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Sur la page **Informations sur la stratégie**, tapez un nom et (éventuellement) une description pour la stratégie. Cliquez sur **Suivant**.
5. Pour créer une stratégie une application iOS, sélectionnez **iOS** dans le volet **Plates-formes**.
6. Sélectionnez l'identifiant de l'application à configurer.
7. Pour les applications iOS, ajoutez le texte suivant à **Contenu du dictionnaire** :

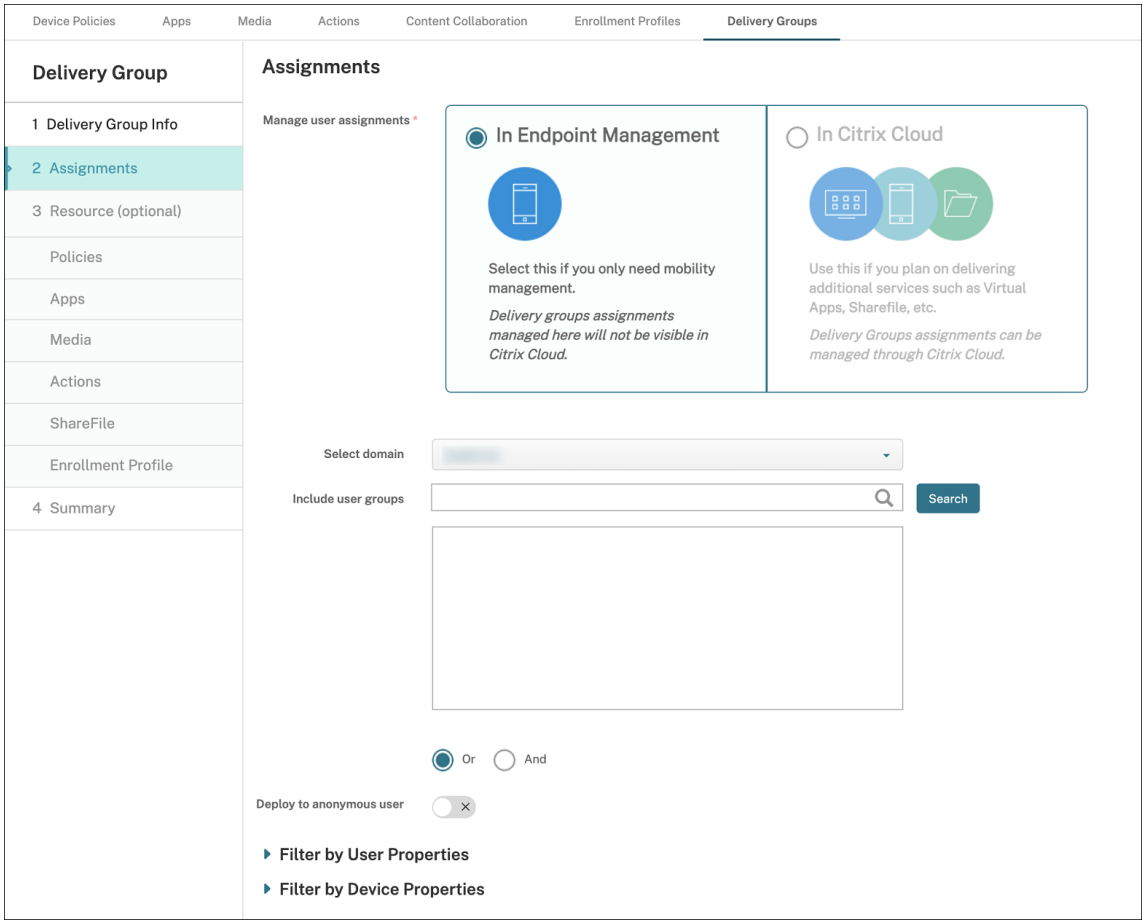
```
<dict>
    <key>IntuneMAMUPN</key>
    <string>${
 user.userprincipalname }
 </string>
</dict>
<!--NeedCopy-->
```

8. Cliquez sur **Vérifier le dictionnaire**.
9. Cliquez sur **Suivant**.
10. Cliquez sur **Enregistrer**.

Configurer des groupes de mise à disposition pour les applications et les stratégies

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Groupes de mise à disposition**.
2. Sur la page **Groupes de mise à disposition**, cliquez sur **Ajouter**. La page **Informations sur le groupe de mise à disposition** s'affiche.
3. Sur la page **Informations sur le groupe de mise à disposition**, tapez un nom et (éventuellement) une description pour le groupe de mise à disposition. Cliquez sur **Suivant**.
4. Sur la page **Attributions**, spécifiez le mode de déploiement du groupe de mise à disposition : choisissez **Dans Citrix Endpoint Management** ou **Dans Citrix Cloud**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Si vous avez choisi **Dans Citrix Endpoint Management** :

   - **Sélectionner un domaine :** sélectionnez le domaine à partir duquel choisir les utilisateurs dans la liste.
   - **Inclure des groupes d'utilisateurs :** effectuez l'une des opérations suivantes :
     - Dans la liste des groupes d'utilisateurs, cliquez sur les groupes que vous souhaitez ajouter. Les groupes sélectionnés s'affichent dans la liste **Groupes d'utilisateurs sélectionnés**.
     - Cliquez sur **Rechercher** pour afficher une liste de tous les groupes d'utilisateurs dans le domaine sélectionné.
     - Tapez un nom de groupe complet ou partiel dans la zone de recherche, puis cliquez sur **Rechercher** pour limiter la liste des groupes d'utilisateurs.

     Pour supprimer un groupe d'utilisateurs de la liste **Groupes d'utilisateurs sélectionnés**, effectuez l'une des opérations suivantes :

     - Dans la liste **Groupes d'utilisateurs sélectionnés**, cliquez sur le **X** en regard de chaque groupe que vous souhaitez supprimer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Cliquez sur **Rechercher** pour afficher une liste de tous les groupes d'utilisateurs dans le domaine sélectionné. Parcourez la liste et décochez la case à cocher en regard de chaque groupe à supprimer.
  - Tapez un nom de groupe complet ou partiel dans la zone de recherche, puis cliquez sur **Rechercher** pour limiter la liste des groupes d'utilisateurs. Parcourez la liste et décochez la case à cocher en regard de chaque groupe à supprimer.

6. Cliquez sur **Suivant**.
7. Sur la page **Stratégies**, faites glisser la stratégie Restrictions et la stratégie Configuration de l'application que vous créez de gauche à droite. Cliquez sur **Suivant**.
8. Sur la page **Applications**, faites glisser les applications que vous souhaitez distribuer du côté gauche de la page vers **Applications requises** ou **Applications facultatives**. Cliquez sur **Suivant**.
9. (Facultatif) Configurez les paramètres sur la page **Média**, la page **Actions** et la page **Inscriptions**. Ou acceptez les valeurs par défaut sur chaque page et cliquez sur **Suivant**.
10. Sur la page **Résumé**, passez en revue les paramètres du groupe de mise à disposition et cliquez sur **Enregistrer** pour créer le groupe de mise à disposition.

Lorsque vous publiez l'application dans la console Intune, sélectionnez **Forcer l'application à être gérée**. Les utilisateurs sur des appareils non supervisés sont invités à autoriser la gestion de l'application. Si les utilisateurs acceptent, l'application est gérée sur l'appareil. Si les utilisateurs refusent, l'application n'est pas disponible sur l'appareil.

Configurer Citrix Secure Mail

Citrix Secure Mail prend désormais en charge diverses configurations. Vous pouvez encapsuler Citrix Secure Mail dans un conteneur MAM Intune se connectant à un Exchange Server local. Vous pouvez connecter Citrix Secure Mail à des comptes Exchange ou Office 365 hébergés. Cependant, cette version ne prend pas en charge l'authentification basée sur les certificats, utilisez donc LDAP à la place.

> **Important :**
>
> Pour utiliser Citrix Secure Mail en mode MDX, vous devez utiliser le mode MDM+MAM de Citrix Endpoint Management.

Citrix Secure Mail remplit également automatiquement les noms d'utilisateur. Pour activer cette fonctionnalité, vous devez d'abord configurer les stratégies personnalisées suivantes :

1. Depuis votre console Citrix Endpoint Management, accédez à **Paramètres > Propriétés du serveur** puis cliquez sur **Ajouter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Dans la liste, cliquez sur **Clé personnalisée** puis dans le champ **Clé**, tapez `xms.store.idpuser_attrs`.
3. Définissez la valeur sur **vrai** puis dans **Nom d'affichage**, tapez `xms.store.idpuser_attrs`. Cliquez sur **Enregistrer**.
4. Cliquez sur **Propriétés du client** puis cliquez sur **Ajouter**.
5. Sélectionnez **Clé personnalisée** puis tapez **SEND_LDAP_ATTRIBUTES** dans le champ **Clé**.
6. Entrez `userPrincipalName=${ user.userprincipalname } ,email=${ user.mail } ,displayname=${ user.displayname } ,sAMAccountName=${ user.samaccountname } ,aadupn=${ user.id_token.upn } ,aadtid=${ user.id_token.tid }` dans le champ **Valeur**. Entrez une description, puis cliquez sur **Enregistrer**.

   Les étapes suivantes s'appliquent uniquement aux appareils iOS.

7. Accédez à **Configurer > Stratégies d'appareil**, cliquez sur Ajouter et sélectionnez la stratégie **Configuration d'applications**.
8. Entrez un nom de stratégie, puis cliquez sur **Suivant**.

   Dans la liste Identificateur, cliquez sur **Ajouter**. Dans la zone de texte qui apparaît, entrez le Bundle ID pour votre application Citrix Secure Mail.

9. Dans la zone de contenu **Dictionnaire**, tapez le texte suivant.

```
<dict>

<key>XenMobileUserAttributes</key>

<dict>

<key>userPrincipalName</key>

<string>${
 user.userprincipalname }
 </string>

<key>email</key>

<string>${
 user.mail }
 </string>

<key>displayname</key>

<string>${
 user.displayname }
 </string>

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
25 <key>sAMAccountName</key>
26
27 <string>${
28  user.samaccountname }
29  </string>
30
31 <key>aadupn</key>
32
33 <string>${
34  user.id_token.upn }
35  </string>
36
37 <key>aadtid</key>
38
39 <string>${
40  user.id_token.tid }
41  </string>
42
43 </dict>
44
45 <key>IntuneMAMUPN</key>
46
47 <string>${
48  user.id_token.upn }
49  </string>
50
51 </dict>
```

10. Désélectionnez la case **Windows Desktop/Tablet**, puis cliquez sur **Suivant**.
11. Sélectionnez les groupes d'utilisateurs sur lesquels vous souhaitez déployer la stratégie, puis cliquez sur **Enregistrer**.

Dépannage

Problèmes d'ordre général

Problème : lors de l'ouverture d'une application, le message d'erreur suivant s'affiche : Stratégie applicative requise.

Résolution : ajoutez des stratégies dans l'API Microsoft Graph.

Problème : vous rencontrez des conflits de stratégie.

Résolution : une seule stratégie par application est autorisée.

Problème : votre application ne peut pas se connecter aux ressources internes.

Résolution : assurez-vous que les ports de pare-feu appropriés sont ouverts, que l'ID du locataire est correct, etc.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problèmes liés à NetScaler Gateway

Le tableau suivant répertorie les problèmes courants liés aux configurations NetScaler Gateway et leurs solutions. Pour le dépannage, activez d'autres journaux et vérifiez-les en procédant comme suit :

1. Dans l'interface de ligne de commande, exécutez la commande suivante : `set audit syslogParams -logLevel ALL`
2. Vérifiez les journaux de l'interpréteur de commandes à l'aide de `tail -f /var/log/ns.log`

Problème	Solution
Les autorisations devant être configurées pour l'application de passerelle sur Azure ne sont pas disponibles.	Vérifiez si une licence Intune appropriée est disponible. Essayez d'utiliser le portail manage.windowsazure.com pour voir si l'autorisation peut être ajoutée. Contactez le support technique Microsoft si le problème persiste.
NetScaler Gateway ne peut pas atteindre `login.microsoftonline.com` et `graph.windows.net`.	À partir de NS Shell, vérifiez si vous êtes en mesure d'accéder au site Microsoft suivant : `curl -v -k https://login.microsoftonline.com`. Ensuite, vérifiez si DNS est configuré sur NetScaler Gateway et si les paramètres du pare-feu sont corrects (les demandes DNS pourraient rester derrière le pare-feu).
Une erreur apparaît dans ns.log après la configuration de OAuthAction.	Vérifiez si la licence Intune est activée et si l'application de passerelle Azure dispose des autorisations appropriées.
La commande Sh OAuthAction n'affiche pas l'état OAuth comme terminé.	Vérifiez les paramètres DNS et les autorisations configurées sur l'application de passerelle Azure.
L'appareil Android ou iOS n'affiche pas l'invite d'authentification double.	Vérifiez si l'ID d'appareil à double facteur LogonSchema est lié au serveur virtuel d'authentification.

Condition et état de l'erreur OAuth

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

État	Condition d'erreur
COMPLETE	Réussite
AADFORGRAPH	Secret non valide, URL non résolue, expiration de la connexion
MDMINFO	*manage.microsoft.com est en panne ou inaccessible
GRAPH	Le point de terminaison graphique est inaccessible
CERTFETCH	Communication impossible avec Token Endpoint: `https://login.microsoftonline.com` en raison d'une erreur DNS. Pour valider cette configuration, allez dans shell et tapez `curl https://login.microsoftonline.com`. Cette commande doit être validée.

Limitations

Les éléments suivants décrivent certaines limitations liées à l'utilisation de MEM avec Citrix Endpoint Management.

- Lorsque vous déployez des applications avec Citrix et Intune pour prendre en charge le micro VPN : lorsque les utilisateurs fournissent leur nom d'utilisateur et leur mot de passe pour accéder aux sites Digest, même si leurs informations d'identification sont valides, une erreur apparaît. [CXM-25227]
- Après avoir modifié le **split tunneling** de **On** à **Off** et en attente de l'expiration de la session de passerelle en cours : le trafic externe est transmis directement sans passer par NetScaler Gateway jusqu'à ce que l'utilisateur lance un site interne en mode VPN complet. [CXM-34922]
- Lorsque la stratégie d'ouverture passe de **Applications gérées** uniquement à **Toutes les applications**, les utilisateurs ne peuvent pas ouvrir de documents dans les applications non gérées jusqu'à ce qu'ils ferment et relancent Citrix Secure Mail. [CXM-34990]
- Lorsque le split tunneling est **activé** en mode VPN complet et que le Split DNS passe de local à distant, les sites internes ne parviennent pas à se charger. [CXM-35168]

Problèmes connus

Lorsque la stratégie mVPN **Activer la redirection http/https (avec SSO)** est désactivée, Citrix Secure Mail ne fonctionne pas. [CXM-58886]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problèmes tiers connus

Sur Citrix Secure Mail pour Android, lorsqu'un utilisateur appuie sur **Créer un nouvel événement**, la page de création d'un nouvel événement ne s'affiche pas. [CXM-23917]

Lorsque vous déployez Citrix Secure Mail pour iOS avec Citrix et Intune pour prendre en charge le micro VPN : la stratégie applicative qui obscurcit l'écran Citrix Secure Mail lorsque les utilisateurs déplacent l'application vers l'arrière-plan n'est pas appliquée. [CXM-25032]

Intégration et configuration des ressources

March 1, 2024

Si vous découvrez Citrix, Citrix Cloud ou Citrix Endpoint Management, cet article vous guidera tout au long de l'intégration. Découvrez le workflow et les détails dont vous avez besoin pour la mise en route.

- **Par où dois-je commencer ?**
  - Si vous n'avez pas acheté d'abonnement Citrix Endpoint Management, reportez-vous à la section Pour les nouveaux clients Citrix.
  - Si vous avez un abonnement à Citrix Endpoint Management, passez à Lorsque le bouton Gérer est disponible.
  - Si votre site Citrix Endpoint Management est provisionné, passez à Configurer l'authentification.
- **L'ordre de configuration est-il important ?** Cet article suit une séquence de configuration recommandée. Vous pouvez suivre un ordre différent. La console Citrix Endpoint Management vous permet de déterminer si des conditions préalables sont manquantes, via des messages tels que « Configurer après le provisioning ».
- **Que dois-je faire après l'intégration ?** Une fois la configuration d'intégration et de ressources décrite dans cet article terminée, poursuivez votre configuration dans la console Citrix Endpoint Management. Pour plus d'informations sur les étapes suivantes, consultez la section Préparation à l'inscription d'appareils et à la mise à disposition de ressources.

Pour les nouveaux clients Citrix

Pour les clients Citrix Cloud qui découvrent Citrix Endpoint Management :

Si vous avez déjà un abonnement à Citrix Endpoint Management, passez à Lorsque le bouton Gérer est disponible.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si vous n'avez pas configuré de compte Citrix Cloud, consultez la section Inscription à Citrix Cloud.

Si vous avez déjà configuré un compte Citrix Cloud, mais que vous n'avez pas acheté Citrix Endpoint Management, demandez une démo de service.

1. Utilisez vos informations d'identification d'administrateur Citrix Cloud pour vous connecter à votre compte Citrix Cloud. La page d'accueil de Citrix Cloud s'affiche.

   Tous les comptes administrateur Citrix Cloud sont créés comme suit :

   - Par défaut, les administrateurs de Citrix Cloud sont créés en tant qu'administrateurs de Citrix Endpoint Management.
   - Les administrateurs Citrix Cloud créés avec un accès client doivent avoir sélectionné Citrix Endpoint Management pour pouvoir administrer Citrix Endpoint Management.

2. Sur la page d'accueil de Citrix Cloud, recherchez la vignette des services Citrix Endpoint Management et cliquez sur **Demander une démo**.
3. Remplissez et envoyez le formulaire de demande de démonstration. Le bouton de la vignette des services Citrix Endpoint Management indique **Démo demandée**.

Si vous cliquez sur la vignette Citrix Endpoint Management Services avant que votre demande ne soit traitée, un écran s'affiche pour vous conseiller de contacter votre représentant ou votre partenaire. Un représentant commercial Citrix peut fournir des informations et des détails complémentaires sur le service.

En attendant la version d'évaluation, assurez-vous de préparer votre déploiement de Citrix Endpoint Management en consultant la section Configuration système requise. Si Citrix héberge et met à disposition votre solution Citrix Endpoint Management, certaines exigences doivent être respectées en matière de communication et de port.

Passez à la section suivante.

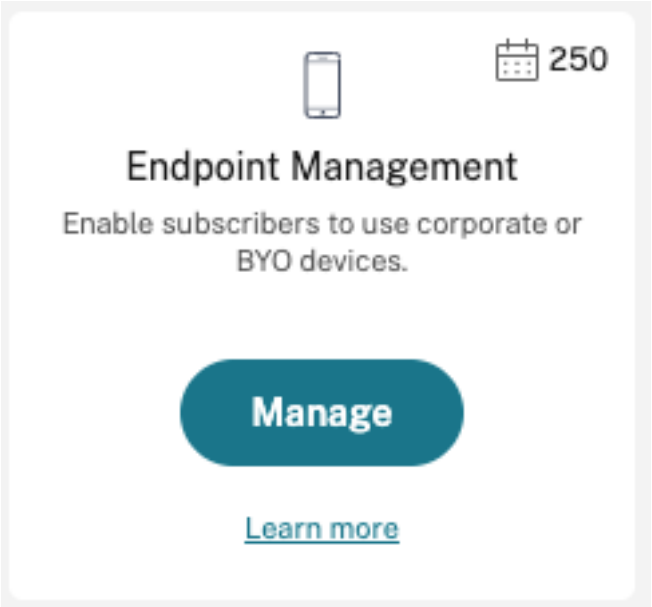
Lorsque le bouton Gérer est disponible

Cette vidéo vous guide tout au long de l'intégration :

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

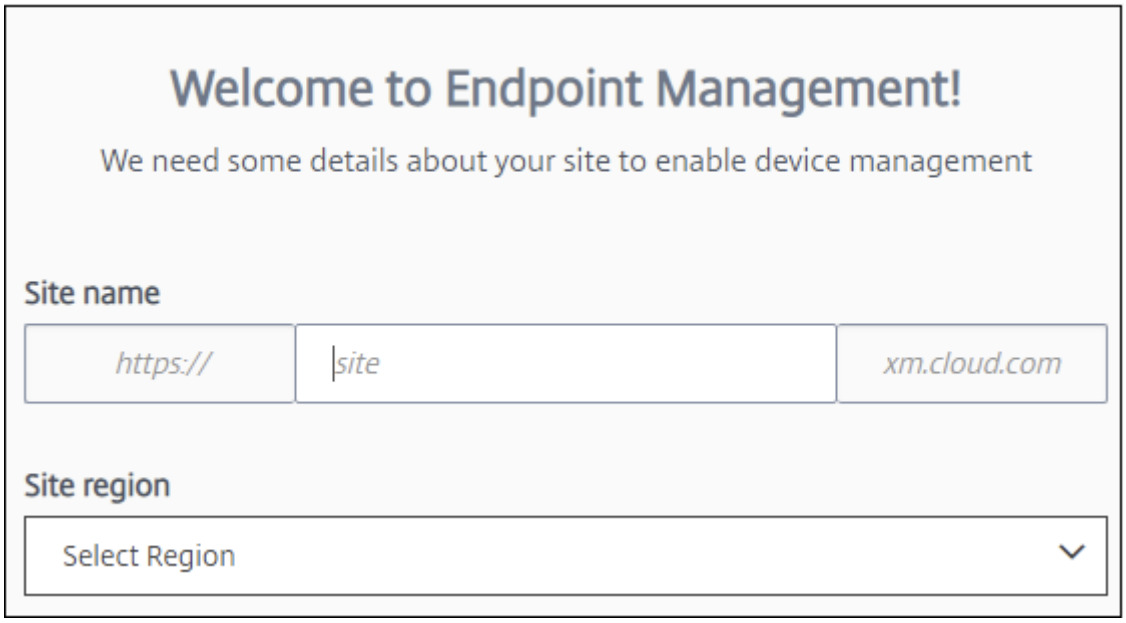
Lorsque votre service Citrix Endpoint Management est disponible, le bouton de la vignette des services Citrix Endpoint Management indique**Gérer**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pour démarrer la configuration :

1. Connectez-vous à votre compte Citrix Cloud à l'aide de vos informations d'identification d'administrateur Citrix Cloud.
2. Cliquez sur **Gérer** dans la vignette Citrix Endpoint Management pour accéder à la console Citrix Endpoint Management.
3. Entrez le nom de votre site et sélectionnez une région. Sélectionnez ensuite **Enregistrer et continuer**.

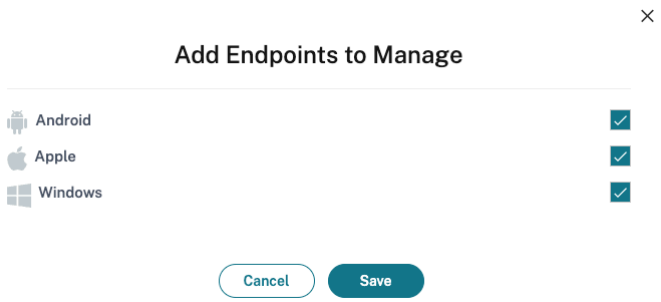


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Remarque :**
>
> Pour demander l'autorisation d'adresses IP, contactez le représentant de l'assistance Citrix.

La console Citrix Endpoint Management s'ouvre et affiche un message indiquant que votre suite est en cours de provisioning et que certaines fonctions Citrix Endpoint Management sont verrouillées.

1. Dans l'écran **Bienvenue**, cliquez sur **Démarrer la configuration** .
2. Sélectionnez les points de terminaison que vous souhaitez gérer, puis cliquez sur **Enregistrer**. Vous pouvez ajouter ou effacer des points de terminaison à tout moment pour les afficher ou les masquer dans la console. L'affichage et le masquage des points de terminaison n'affectent pas votre configuration.



Nous vous envoyons un e-mail lorsque le provisioning est terminé.

Centre de ressources


Cliquez sur l'icône **Centre de ressources** pour visionner des didacticiels vidéo sans quitter la console.

Pendant le provisioning

Pendant que nous provisionnons Citrix Endpoint Management, vous pouvez commencer la configuration.

Configurer les emplacements des ressources

Vous avez besoin d'emplacements de ressources pour pouvoir configurer des connexions LDAP (Lightweight Directory Access Protocol) pour Citrix Endpoint Management. Les emplacements de ressources contiennent les ressources requises pour fournir des services de cloud à vos abonnés.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Vous avez besoin d'un emplacement de ressources par domaine. Pour obtenir de l'aide, consultez l'article Citrix Cloud Emplacements des ressources.

En attendant la version d'évaluation, assurez-vous de préparer votre déploiement de Citrix Endpoint Management en consultant la section Configuration système requise. Si Citrix héberge et met à disposition votre solution Citrix Endpoint Management, il existe certaines exigences en matière de communication et de port. Cette configuration connecte l'infrastructure Citrix Endpoint Management aux services d'entreprise, tels que Active Directory. Les informations que vous devez fournir sont incluses dans le manuel Onboarding Handbook sous « Citrix Endpoint Management Trial Sales Engineer engagement ».

Une fois que vous êtes autorisé à accéder à la version d'évaluation, le bouton de **Citrix Endpoint Management** indique **Gérer**. Cliquez sur **Gérer** pour ouvrir la console Citrix Endpoint Management.

Configuration de l'authentification

Une fois votre site configuré, vous pouvez poursuivre la configuration. Nous vous recommandons de configurer un fournisseur d'identité (IdP) hébergé dans le cloud ou le protocole LDAP (Lightweight Directory Access Protocol) pour importer des groupes, des comptes utilisateur et les propriétés associées.

Pour configurer le fournisseur d'identité

Citrix Endpoint Management prend en charge l'authentification auprès de fournisseurs d'identité, tels que Azure Active Directory, Okta et NetScaler Gateway local.

Pour configurer un fournisseur d'identité dans Citrix Cloud et le configurer pour Citrix Endpoint Management :

- Authentification avec Azure Active Directory via Citrix Cloud
- Authentification avec Okta via Citrix Cloud
- Authentification avec une passerelle NetScaler Gateway locale via Citrix Cloud

Pour configurer LDAP

Vous pouvez configurer une connexion dans Citrix Endpoint Management à un ou plusieurs annuaires compatibles LDAP pour l'authentification basée sur domaine. Citrix Endpoint Management prend en charge les groupes imbriqués dans LDAP. Les groupes imbriqués sont synchronisés quotidiennement à 12 h, heure locale.

Dans le cadre de la configuration de LDAP, vous devez installer au moins un Cloud Connector.

Pour un aperçu rapide, visionnez cette vidéo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Pour configurer LDAP :

1. Sur la page **Paramètres**, faites défiler l'affichage jusqu'à la vignette **LDAP**, puis cliquez sur **Configurer**.
2. Suivez les instructions à l'écran pour télécharger et installer un Cloud Connector. Les composants Cloud Connector sont requis pour établir la communication entre Citrix Cloud et vos ressources. Pour obtenir de l'aide, veuillez consulter la section Citrix Cloud Connector.

Si vous disposez de la configuration LDAP et que vous ajoutez Azure AD ou Okta en tant que fournisseur d'identité, Citrix Endpoint Management synchronise les informations spécifiques au fournisseur d'identité pour vos groupes Active Directory dans la base de données Citrix Endpoint Management. Cette configuration n'affecte pas vos groupes de mise à disposition existants ni vos inscriptions utilisateur. Toutefois, vous ne pouvez pas ajouter de paramètres LDAP dans Citrix Endpoint Management ultérieurement. Pour plus d'informations, consultez Authentification par fournisseur d'identité.

Si vous modifiez les paramètres **Alias de domaine** et **Rechercher utilisateurs par** après l'inscription, les utilisateurs doivent s'inscrire à nouveau. Pour plus d'informations sur la configuration LDAP, consultez la section Authentification domaine ou domaine + jeton de sécurité.

Après avoir configuré LDAP, vous pouvez poursuivre la configuration de l'authentification ou configurer une plate-forme spécifique.

Configurer NetScaler Gateway

Lorsqu'il est intégré à Citrix Endpoint Management, NetScaler Gateway fournit un accès à distance à votre réseau interne et à vos ressources.

Citrix Endpoint Management requiert l'installation d'une passerelle NetScaler Gateway pour les scénarios suivants :

- Vous avez besoin d'un micro VPN pour accéder aux ressources réseau internes pour les applications métier. Ces applications sont encapsulées avec la technologie Citrix MDX. Le micro-VPN a besoin de NetScaler Gateway pour se connecter aux infrastructures back-end internes.
- Vous prévoyez d'utiliser Citrix Endpoint Management pour gérer les applications (MAM ou MDM + MAM). NetScaler Gateway n'est pas nécessaire pour gérer uniquement les appareils (MDM).
- Vous prévoyez d'intégrer Citrix Endpoint Management à Microsoft Endpoint Manager. (Nécessite une passerelle NetScaler Gateway locale.)

Pour un aperçu rapide, visionnez cette vidéo.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Le tableau suivant récapitule les fonctionnalités prises en charge par les solutions NetScaler Gateway basées sur site.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fonctionnalités prises en charge	NetScaler Gateway sur site
Citrix Secure Mail (STA)*	oui
Tunnel - SSO Web (authentification unique Web)	oui
VPN complet (non disponible pour les applications de productivité mobiles Citrix pour iOS)	oui
Per App VPN	oui
Authentification unique mobile (contrôle d'accès)	non
Haute disponibilité	oui**
Déploiement multi-POP	oui***
Prise en charge des proxys	oui
Split tunneling	oui
Split DNS	oui

* Configuration du service Citrix Cloud Secure Ticket Authority (STA)

** Configuration locale

*** Configuration de l'équilibrage de charge globale des serveurs

Cas d'utilisation d'une passerelle NetScaler Gateway locale

Utilisez une ou plusieurs appliances NetScaler Gateway sur site avec Citrix Endpoint Management lorsque :

- Vous avez besoin de fonctionnalités Per App VPN.
- Vous avez besoin d'un tunneling complet, d'un split tunneling, d'un split tunneling inversé ou d'un split DNS. 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.
- Vous utilisez l'intégration de Citrix Endpoint Management à Microsoft Endpoint Manager.

L'utilisation de la passerelle NetScaler Gateway locale implique une configuration et une maintenance importantes. Après avoir configuré LDAP et NetScaler Gateway dans la console Citrix Endpoint Management, vous exportez un script à partir de cette console. Vous exécutez ensuite le script sur NetScaler Gateway.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Sur la page **Paramètres**, faites défiler l'affichage jusqu'à la vignette **NetScaler Gateway**, puis cliquez sur **Démarrer la configuration**.
2. Sélectionnez **NetScaler Gateway (local)** comme type.
3. Suivez les instructions à l'écran. Pour plus d'informations, consultez Configurer une passerelle NetScaler Gateway locale pour une utilisation avec Citrix Endpoint Management.

Configurer le serveur de notification

Pour envoyer des notifications, vous devez configurer une passerelle et un serveur de notification. Un serveur de notification assure la connectivité et la possibilité de communication entre les utilisateurs et l'administrateur. Pour configurer un serveur de notifications dans Citrix Endpoint Management, reportez-vous à la section Notifications.

Configurer un certificat APNs (Apple Push Notification service) pour les appareils Apple

Pour inscrire et gérer des appareils Apple, Citrix Endpoint Management requiert un certificat APNs (Apple Push Notification service). Citrix Endpoint Management requiert également un certificat APNs si vous envisagez d'utiliser des notifications push pour Citrix Secure Mail pour Apple. Pour plus d'informations sur Citrix Endpoint Management et APNS, consultez Notifications push pour Citrix Secure Mail pour iOS.

L'obtention d'un certificat Apple nécessite un identifiant Apple ID et un compte de développeur. Pour de plus amples informations, consultez le site Web Apple Developer Program.

Pour un aperçu rapide, visionnez cette vidéo.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Pour configurer APNs avec une demande de signature de certificat Citrix :

1. Sur la page **Paramètres**, développez la vignette **Apple**.
2. Sur la vignette **Certificat APNs**, cliquez sur **Configurer**, puis suivez les instructions à l'écran.

Pour de plus amples informations, consultez Certificats et authentification.

Configurer Android Enterprise

Citrix Endpoint Management est entièrement configuré après la création de groupes de mise à disposition et l'affectation d'utilisateurs aux groupes de mise à disposition via la bibliothèque cloud. À partir de ce moment, l'administration de Citrix Endpoint Management se déroule au sein de Citrix Cloud. L'interface combinée simplifie le basculement entre Citrix Cloud et Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Vous pouvez configurer Android Enterprise pour Citrix Endpoint Management avec Google Play ou Google Workspace.

1. **Si votre organisation n'utilise pas Google Workspace :** vous pouvez utiliser Google Play pour enregistrer Citrix en tant que fournisseur EMM. Si vous utilisez un Google Play d'entreprise, vous provisionnez des comptes Google Play d'entreprise pour les appareils et les utilisateurs. Les comptes Google Play d'entreprise permettent d'accéder à la plate-forme Google Play d'entreprise, ce qui permet aux utilisateurs d'installer et d'utiliser les applications professionnelles que vous mettez à leur disposition. Si votre organisation utilise un service d'identité tiers, vous pouvez lier des comptes Google Play d'entreprise à vos comptes d'identité existants.

   Comme ce type d'entreprise n'est pas lié à un domaine, vous pouvez créer plusieurs entreprises pour une seule organisation. Par exemple, chaque département ou région d'une organisation peut s'inscrire en tant qu'entreprise différente. Cette configuration vous permet d'utiliser différentes entreprises pour gérer des ensembles distincts d'appareils et d'applications.

2. **Si votre organisation utilise déjà Google Workspace pour permettre aux utilisateurs d'accéder aux applications Google :** vous pouvez utiliser Google Workspace pour enregistrer Citrix comme fournisseur EMM. Si votre organisation utilise Google Workspace, elle dispose d'un identifiant d'entreprise et de comptes Google existants pour les utilisateurs. Pour utiliser Citrix Endpoint Management avec Google Workspace, vous synchronisez vos données avec votre annuaire LDAP et récupérez les informations de compte Google à partir de Google à l'aide de l'API Google Directory.

   Ce type d'entreprise est lié à un domaine existant. Par conséquent, chaque domaine ne peut créer qu'une seule entreprise. Pour inscrire un appareil dans Citrix Endpoint Management, chaque utilisateur doit se connecter manuellement avec son compte Google existant. Le compte permet aux utilisateurs d'accéder au Google Play d'entreprise et à d'autres services Google via votre abonnement Google Workspace.

Pour un aperçu rapide, visionnez cette vidéo.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Pour commencer :

1. Sur la page **Paramètres**, développez la vignette **Android**.
2. Sur la vignette **Android Enterprise**, cliquez sur **Configurer**.
3. Choisissez **Google Play** ou **G Suite**, en fonction de la façon dont vous accordez aux utilisateurs l'accès aux applications Google.
   Si vous avez précédemment configuré la plate-forme Android Enterprise avec Google Play, l'interface utilisateur vous dirige vers la boutique Google Play pour vous réinscrire. Cliquez sur **Réinscription**, revenez à la console CEM et actualisez la page.
4. Suivez les instructions à l'écran.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Consultez :

- Créer un compte Android Entreprise

Configurer Firebase Cloud Messaging

Citrix recommande d'utiliser Firebase Cloud Messaging (FCM) pour contrôler quand et comment les appareils Android se connectent à Citrix Endpoint Management. Citrix Endpoint Management envoie des notifications de connexion aux appareils Android activés pour FCM. Toute action de sécurité ou commande de déploiement déclenche une notification push afin d'inviter l'utilisateur à se reconnecter au serveur Citrix Endpoint Management. Consultez la section Firebase Cloud Messaging.

Intégration à Microsoft Endpoint Manager

L'intégration de Citrix Endpoint Management avec Microsoft Endpoint Manager ajoute la valeur du micro VPN de Citrix Endpoint Management aux applications compatibles Microsoft Intune, telles que le navigateur Microsoft Edge.

L'intégration de Citrix Endpoint Management à MEM permet également aux entreprises d'encapsuler leurs propres applications métier avec Intune et Citrix. L'encapsulation d'applications fournit des fonctionnalités de micro-VPN à l'intérieur d'un conteneur de gestion des applications mobiles (MAM) Intune. Le micro VPN de Citrix Endpoint Management permet à vos applications d'accéder aux ressources locales. Effectuez la gestion et la mise à disposition des applications Office 365, des applications métier et de Citrix Secure Mail dans un même conteneur. Un conteneur unique assure une sécurité et une productivité optimales.

- Par défaut, les administrateurs de Citrix Cloud sont créés en tant qu'administrateurs de Citrix Endpoint Management.
- Les administrateurs Citrix Cloud créés avec un accès client doivent avoir sélectionné Citrix Endpoint Management pour pouvoir administrer Citrix Endpoint Management.

Dans la console Citrix Endpoint Management, vous ne pouvez modifier que le rôle et l'appartenance d'un utilisateur. Pour modifier un rôle à tout moment, accédez à la console Citrix Endpoint Management à partir du tableau de bord Citrix Cloud. Accédez à l'onglet **Gérer** et cliquez sur **Utilisateurs**. Sélectionnez un utilisateur spécifique et cliquez sur **Modifier** pour modifier le rôle. Pour plus d'informations, veuillez consulter la section Configurer des rôles avec RBAC.

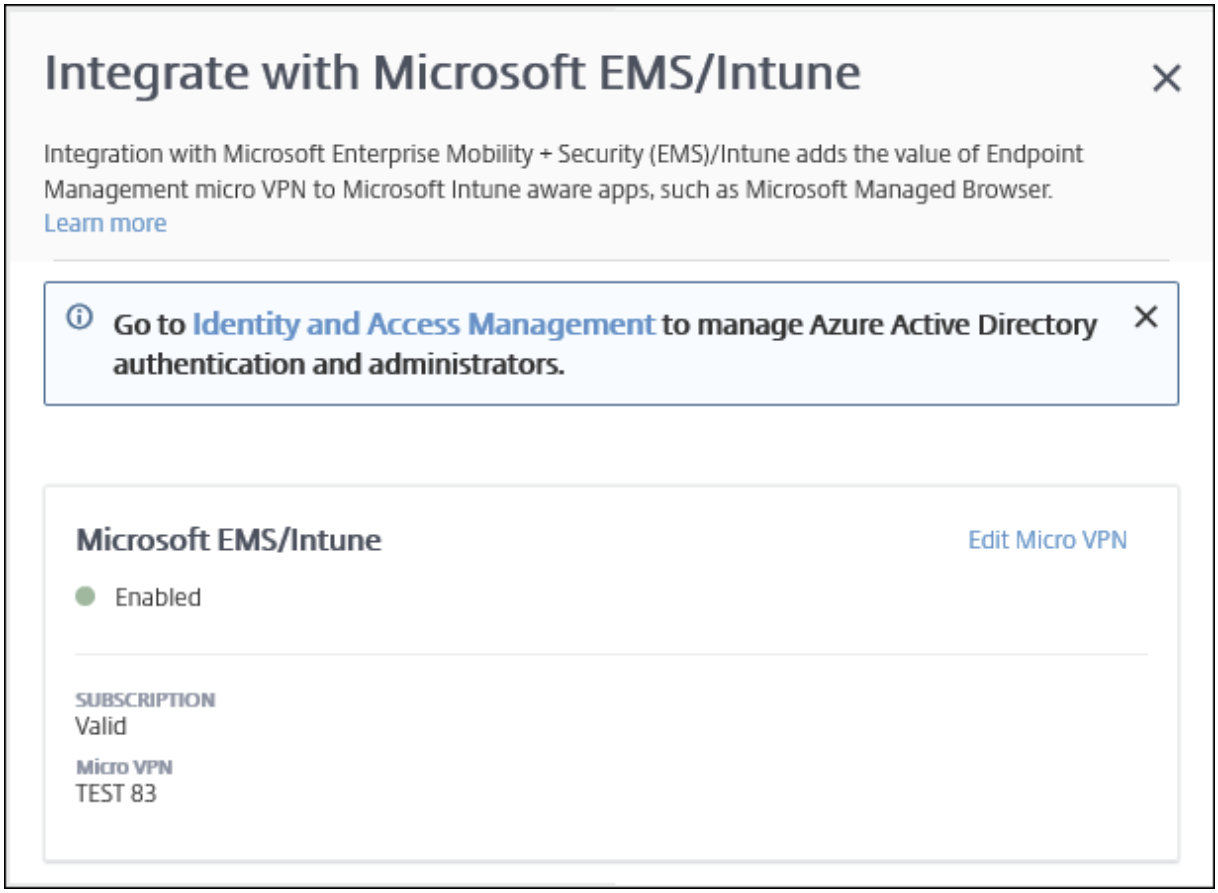
Pour intégrer MEM, consultez Intégration de Citrix Endpoint Management avec Microsoft Endpoint Manager.

Une fois la configuration dans Citrix Cloud terminée, revenez à la console Citrix Endpoint Management comme suit : accédez à la page d'**accueil** de Citrix Cloud, puis cliquez sur **Gérer** dans la vignette **Citrix**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Endpoint Management. Vous pouvez ensuite vérifier si vous vous êtes connecté à Citrix Endpoint Management avec votre compte Azure Active Directory.

1. Sur la page **Paramètres**, accédez à la vignette **Intégrer avec Microsoft EMS/Intune**.
2. Cliquez sur **En savoir plus**. L'interface utilisateur indique si la connexion a été activée.



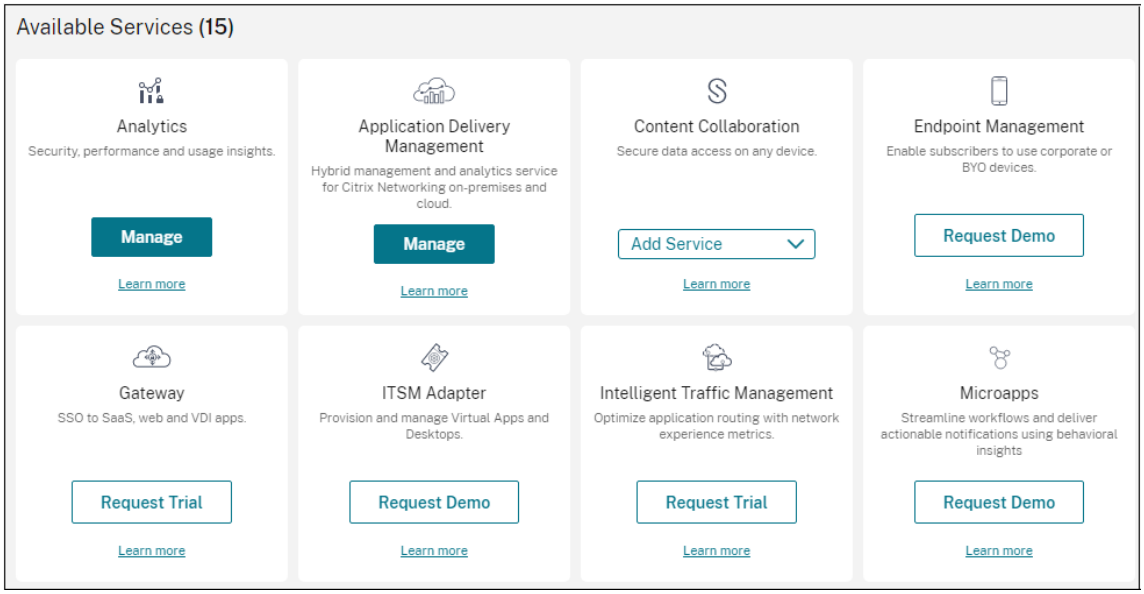
Dans la console Citrix Cloud, vous pouvez également modifier les noms d'utilisateur ou les mots de passe et supprimer ou modifier des utilisateurs locaux. Consultez la section Gestion des identités et des accès.

Associer un compte ShareFile existant à Citrix Cloud

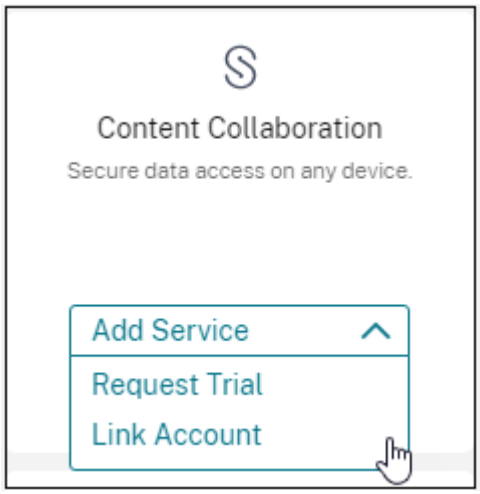
Si vous avez un compte ShareFile qui existait avant votre inscription à Citrix Cloud, vous devez associer ce compte à Citrix Cloud. Pour associer un compte, le propriétaire de l'adresse e-mail utilisée doit être un administrateur du compte ShareFile. Lorsque vous êtes prêt à continuer, accédez à https://onboarding.cloud.com.

1. Une fois que vous êtes connecté, un écran semblable au suivant apparaît :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

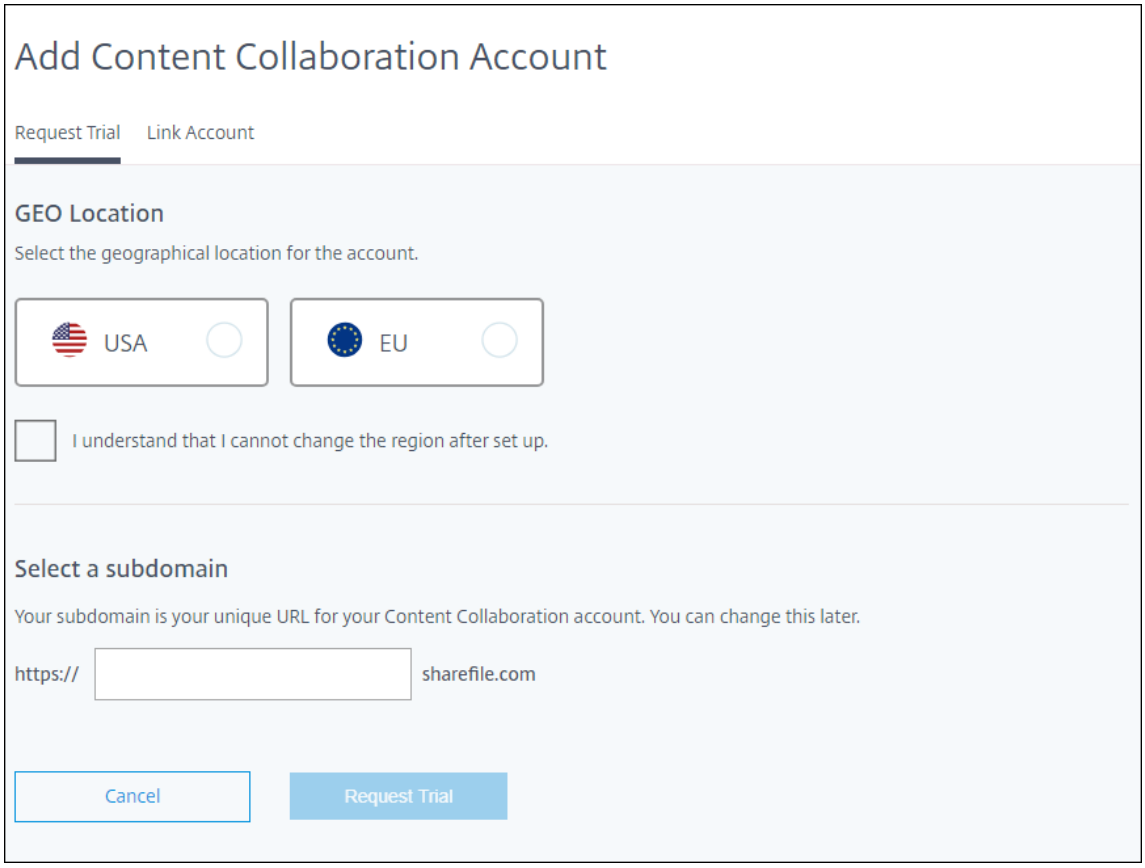


2. Dans la vignette **ShareFile**, choisissez **Lier le compte**.



3. Une fois que nous avons confirmé votre compte ShareFile, la page suivante s'affiche :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Cliquez sur **Associer compte** pour terminer le processus. Vous pouvez immédiatement gérer votre compte ShareFile à partir de Citrix Cloud.

Considérations sur le dimensionnement et la scalabilité des Cloud Connector

November 29, 2023

Lors de l'évaluation de la taille et de l'évolutivité du service Citrix Endpoint Management, effectuez des recherches et testez la configuration des Cloud Connector en fonction de vos besoins spécifiques. Cloud Connector est soumis à une charge élevée uniquement pendant l'inscription de l'appareil. Le sous-dimensionnement des machines peut avoir un impact négatif sur les performances du système.

Citrix nécessite deux Cloud Connector par emplacement de ressource. Installez Cloud Connector sur un serveur dédié qui ne partage aucune responsabilité avec d'autres composants ou produits. Lors de nos tests, les Cloud Connector ont été déployés dans des groupes à haute disponibilité (**leur charge n'est pas répartie**).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration de test

- Deux machines Windows Server 2019 dédiées, deux processeurs virtuels, 4 Go de mémoire
- Inscriptions d'appareils Android et iOS dans MDM+MAM, réparties uniformément sur une période de 8 heures
- Citrix Endpoint Management configuré pour inscrire 125 appareils par heure pour 1 000 appareils
  - 1 000 appareils (125 inscriptions d'appareils par heure)
  - 5 000 appareils (625 inscriptions d'appareils par heure)
  - 10 000 appareils (1 250 inscriptions d'appareils par heure)
  - 20 000 appareils (2 500 inscriptions d'appareils par heure)

Résultats des tests

Cloud Connector	1 000 appareils	5 000 appareils	10 000 appareils	20 000 appareils
Utilisation moyenne de l'UC	2 %	2 %	4 %	4 %
Utilisation maximale de l'UC	8 %	8 %	10 %	11 %
Utilisation moyenne de la mémoire	73 %	73 %	75 %	75 %
Utilisation maximale de la mémoire	76 %	76 %	76 %	79 %

Préparation à l'inscription d'appareils et à la mise à disposition de ressources

March 1, 2024

> **Important :**
>
> Avant de commencer, assurez-vous de terminer toutes les tâches décrites dans la section Intégration et configuration des ressources.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Tenez vos utilisateurs informés des changements à venir. Consultez Welcome to your Citrix User Adoption Kit.

Citrix Endpoint Management prend en charge diverses options d'inscription. Cet article traite de la configuration de base requise pour permettre l'inscription de tous les appareils pris en charge. Le diagramme suivant résume la configuration de base.

Pour obtenir une liste des appareils pris en charge, consultez la section Systèmes d'exploitation d'appareils pris en charge.

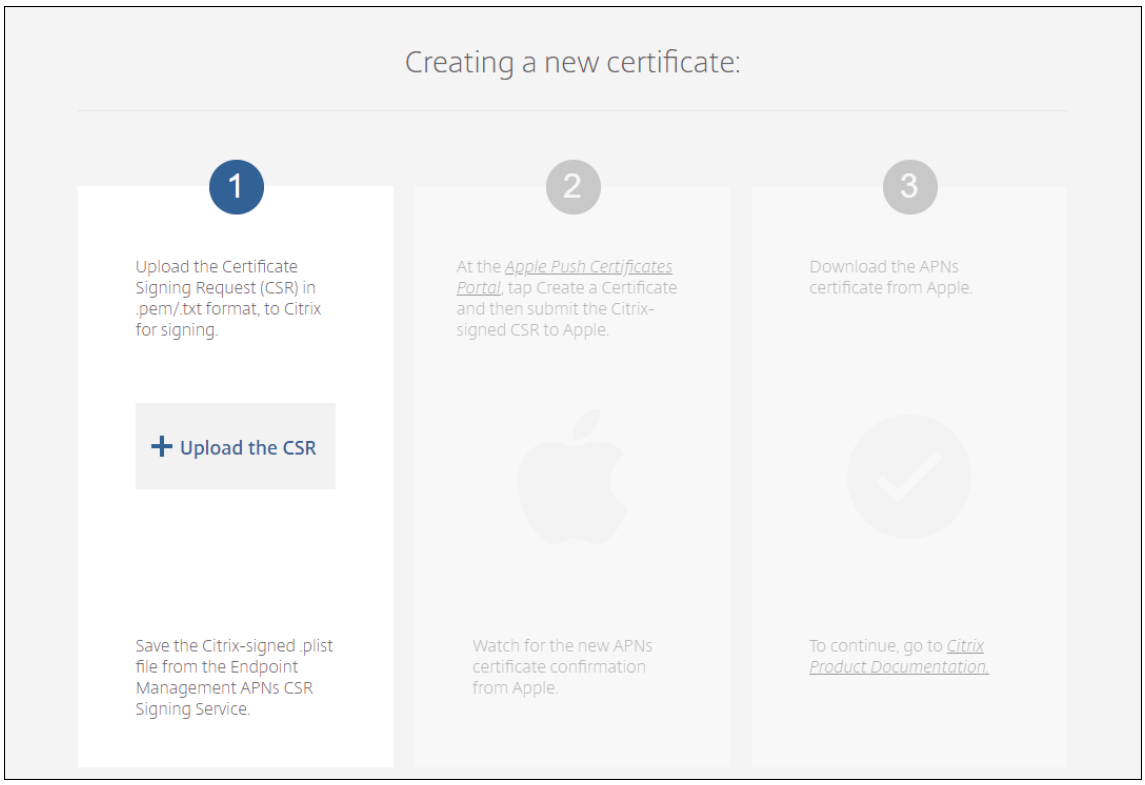
Configurer un certificat Apple Push Notification Service (APNS) pour les appareils iOS

> **Important :**
>
> La prise en charge par Apple du protocole binaire hérité du service Apple Push Notification prend fin le 31 mars 2021. Apple recommande d'utiliser à la place l'API du fournisseur APNs basé sur HTTP/2. À partir de la version 20.1.0, Citrix Endpoint Management prend en charge l'API HTTP/2. Pour plus d'informations, consultez « Apple Push Notification Service Update » dans https://developer.apple.com/. Pour obtenir de l'aide sur la vérification de la connectivité à APNs, consultez la section Tests de connectivité.

Pour inscrire et gérer des appareils iOS, Citrix Endpoint Management requiert un certificat Apple Push Notification Service (APNS). Citrix Endpoint Management requiert également un certificat APNS pour les notifications push pour Citrix Secure Mail pour iOS.

- L'obtention d'un certificat Apple nécessite un identifiant Apple ID et un compte de développeur. Pour de plus amples informations, consultez le site Web Apple Developer Program.
- Pour obtenir un certificat APNS et l'importer dans Citrix Endpoint Management, consultez la section Certificats APNS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Pour plus d'informations sur Citrix Endpoint Management et APNS, consultez Notifications push pour Citrix Secure Mail pour iOS.

Configurer Firebase Cloud Messaging (FCM) pour les appareils Android

Firebase Cloud Messaging (FCM) permet de contrôler quand et comment les appareils Android se connectent au service Citrix Endpoint Management. Toute action de sécurité ou commande de déploiement déclenche une notification push. La notification invite les utilisateurs à se reconnecter à Citrix Endpoint Management.

- La configuration de FCM nécessite la configuration de votre compte Google. Pour créer des informations d'identification Google Play, consultez la section Gérer les informations de votre compte développeur. Vous utilisez également Google Play pour ajouter, acheter et approuver des applications en vue de les déployer sur l'espace Android Entreprise d'un appareil. Vous pouvez utiliser Google Play pour déployer des applications Android privées, des applications tierces et publiques.
- Pour configurer FCM, consultez la section Firebase Cloud Messaging.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer la détection automatique Citrix Endpoint Management

Le service de détection automatique simplifie le processus d'inscription pour les utilisateurs via la détection d'URL basée sur une adresse e-mail. Le service de détection automatique fournit des fonctionnalités telles que la vérification de l'inscription, le certificate pinning, ainsi que des avantages supplémentaires pour les clients Citrix Workspace. Le service, hébergé dans Citrix Cloud, joue un rôle important dans la plupart des déploiements Citrix Endpoint Management.

Avec le service de détection automatique, les utilisateurs :

- Peuvent utiliser leurs informations d'identification de réseau d'entreprise pour inscrire leurs appareils.
- N'ont pas besoin d'entrer les détails sur l'adresse du serveur Citrix Endpoint Management.
- Entrent leur nom d'utilisateur au format UPN (nom d'utilisateur principal). Par exemple, `user@mycompany.com`.

Nous vous recommandons d'utiliser le service de détection automatique pour les environnements à haute sécurité. Le service de détection automatique prend en charge le certificate pinning de clé publique, qui empêche les attaques « man-in-the-middle ». Le certificate pinning garantit que le certificat signé par votre entreprise est utilisé lorsque les clients Citrix communiquent avec Citrix Endpoint Management. Pour configurer les certificate pinnings pour vos sites Citrix Endpoint Management, contactez le support Citrix. Pour plus d'informations, consultez la section Certificate pinning.

Pour accéder au service de détection automatique, accédez à https://adsui.cloud.com (commercial).

Logiciels requis

- Le nouveau service de détection automatique dans Citrix Cloud requiert la dernière version de Citrix Secure Hub :
  - Pour iOS, Citrix Secure Hub version 21.6.0 ou ultérieure
  - Pour Android, Citrix Secure Hub version 21.8.5 ou ultérieure

    Les appareils exécutés sur des versions antérieures de Citrix Secure Hub peuvent rencontrer des interruptions de service.
- Pour accéder au nouveau service de détection automatique, vous devez disposer d'un compte d'administrateur Citrix Cloud avec un accès complet. Le service de détection automatique ne prend pas en charge les comptes d'administrateur disposant d'un accès personnalisé. Si vous n'avez pas de compte, consultez Ouvrir un compte Citrix Cloud.

  Citrix a migré tous les enregistrements de détection automatique existants vers Citrix Cloud sans interruption de service. Les enregistrements migrés n'apparaissent pas automatiquement

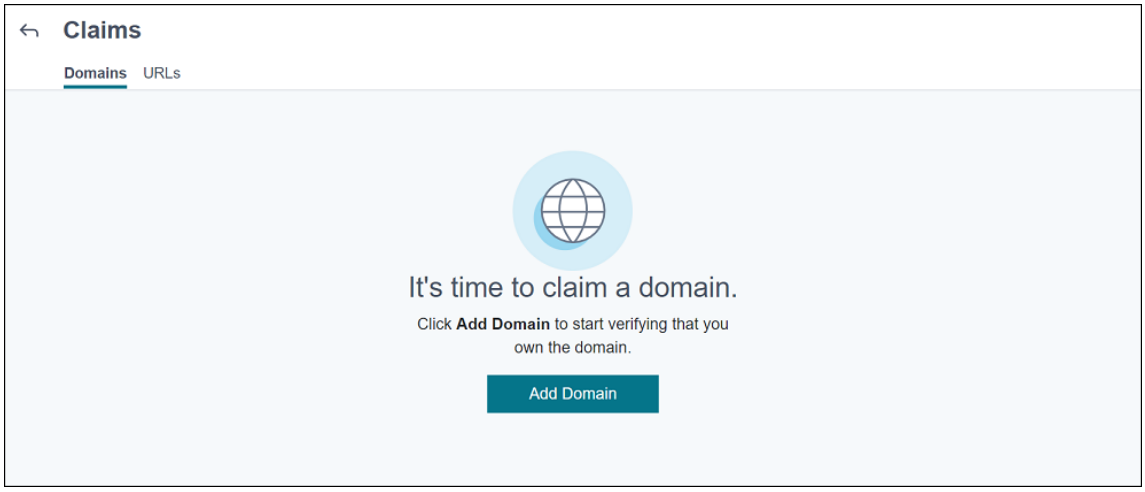
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

dans la nouvelle console. Vous devez récupérer les domaines dans le nouveau service de détection automatique pour prouver la propriété. Pour plus d'informations, consultez l'article CTX312339.

- Avant de commencer à utiliser le service de détection automatique pour vos déploiements Citrix Endpoint Management, vérifiez et revendiquez votre domaine. Vous pouvez revendiquer jusqu'à 10 domaines. La revendication associe le domaine vérifié au service de détection automatique. Pour revendiquer plus de 10 domaines, ouvrez un ticket SRE ou contactez le support technique Citrix.
- Utilisez le paramètre Port MAM au lieu de Nom de domaine complet NetScaler Gateway pour diriger le trafic MAM vers votre centre de données. Si vous entrez un nom de domaine complet avec le port de votre instance NetScaler Gateway, la machine client utilise la configuration du paramètre **Port MAM**.
- Si un bloqueur de publicités empêche l'ouverture du site, assurez-vous de désactiver le bloqueur de publicités pour l'ensemble du site Web.

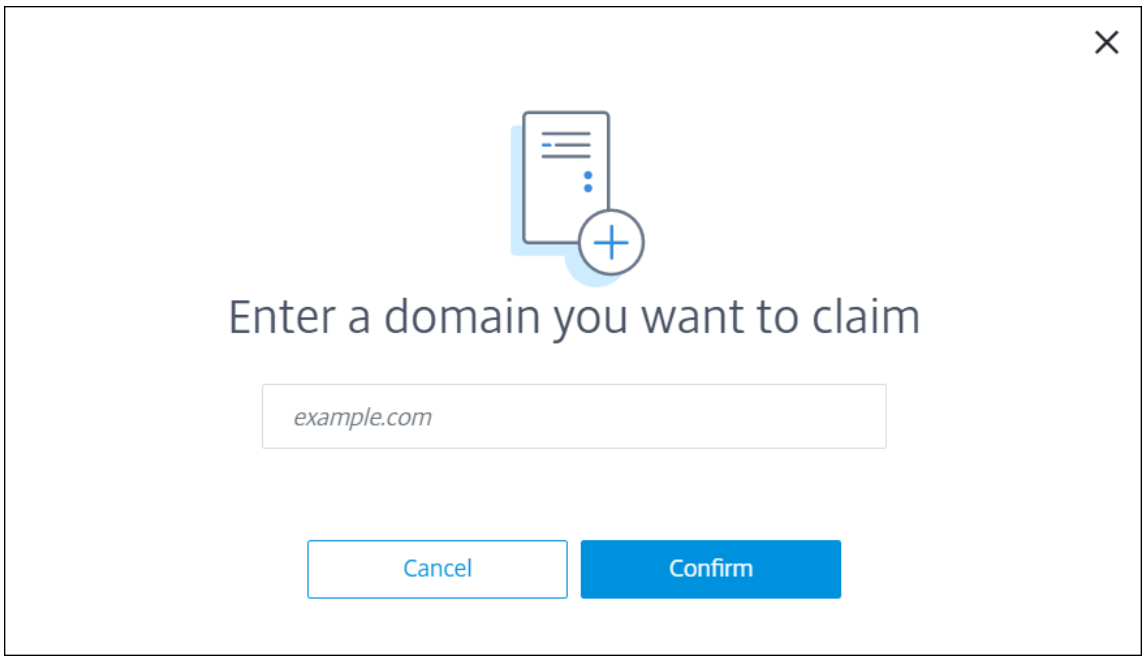
Revendiquer un domaine

1. Sous l'onglet **Revendications > Domaines**, cliquez sur **Ajouter un domaine**.

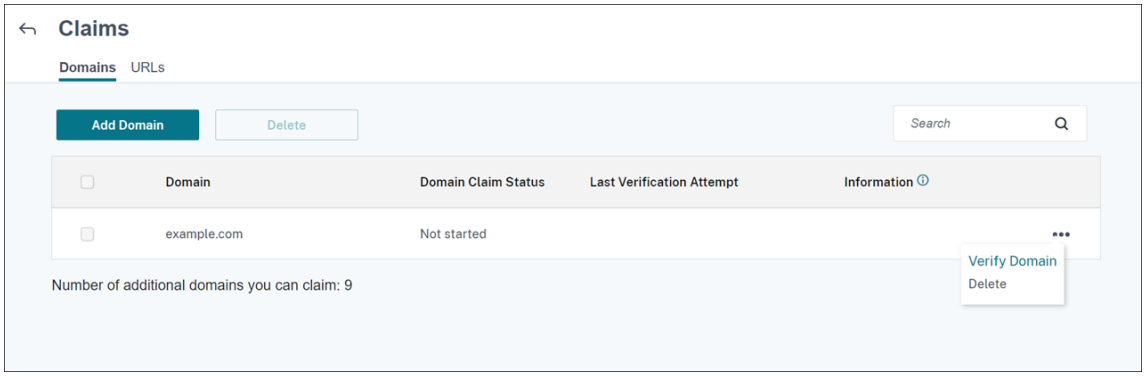


2. Dans la boîte de dialogue qui s'affiche, entrez le nom de domaine de votre environnement Citrix Endpoint Management et cliquez sur **Confirmer**. Votre domaine apparaît dans **Revendications > Domaines**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

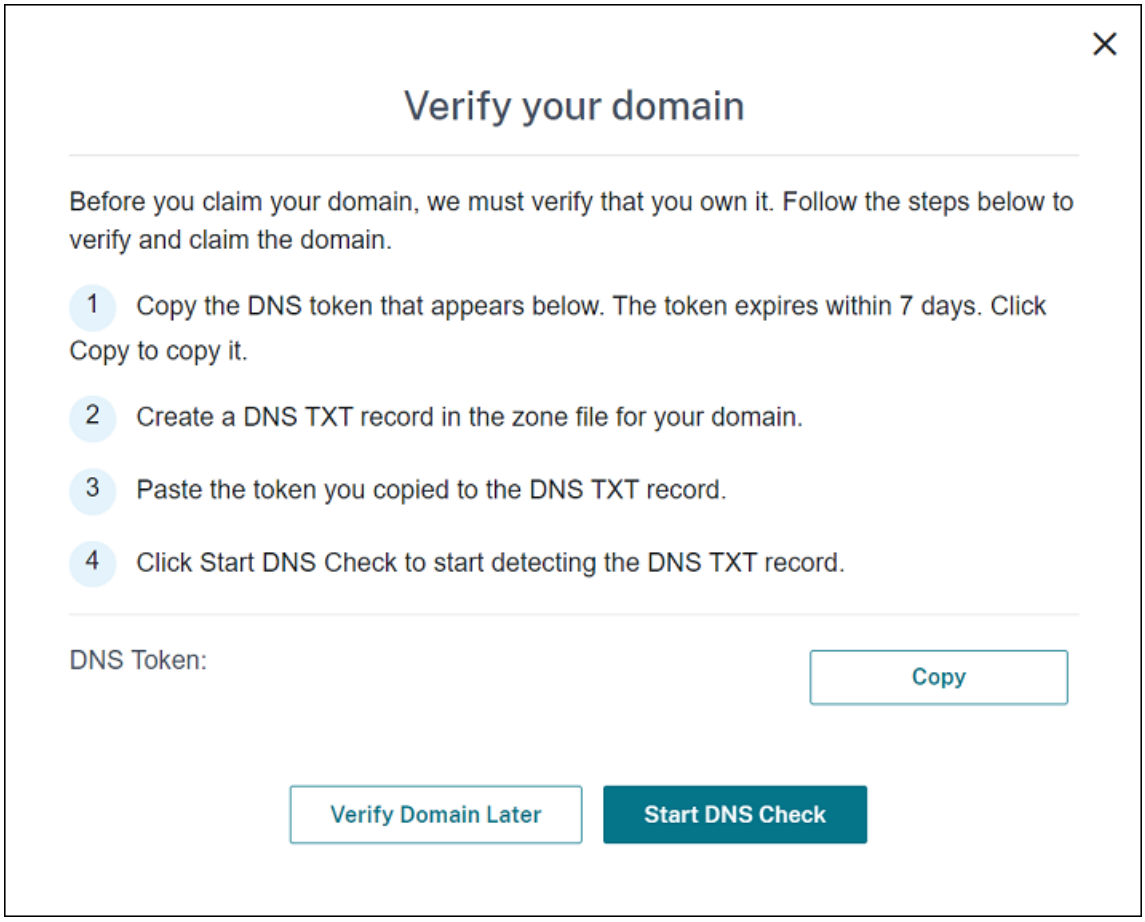


3. Dans le domaine que vous avez ajouté, cliquez sur le menu des points de suspension et sélectionnez **Vérifier le domaine** pour démarrer le processus de vérification. La page **Vérifier votre domaine** s'affiche.



4. Sur la page **Vérifier votre domaine**, suivez les instructions pour vérifier que vous êtes propriétaire du domaine.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

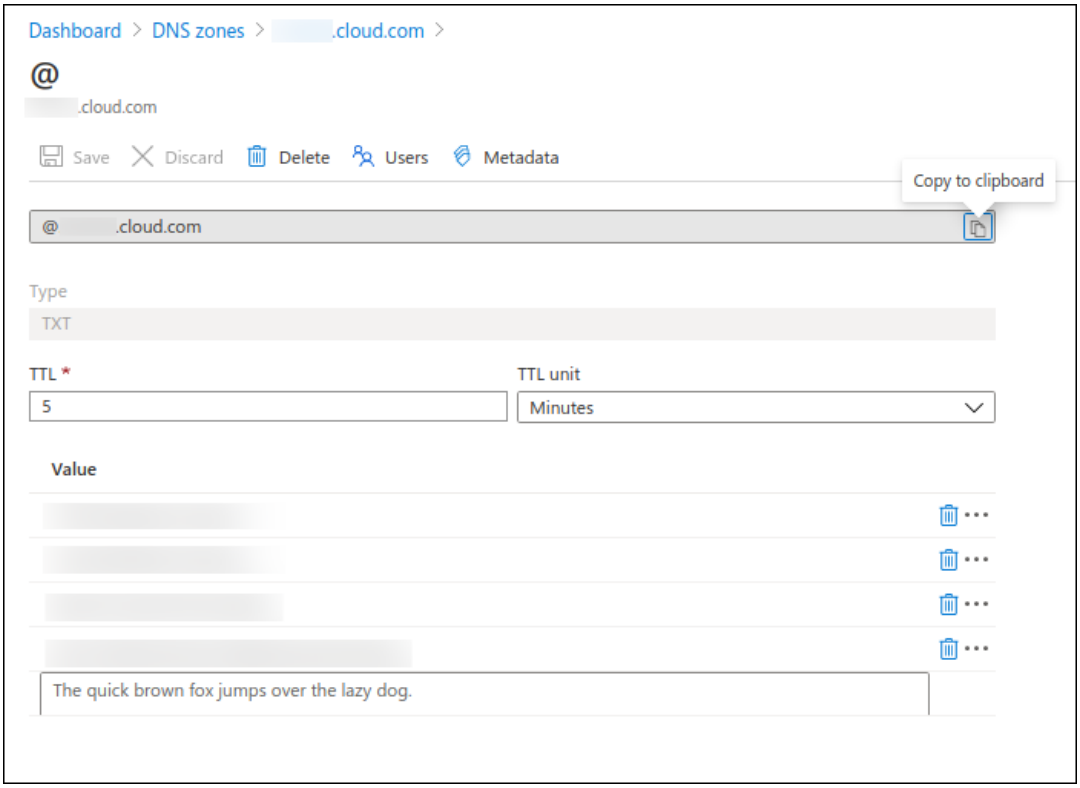


a) Cliquez sur **Copier** pour copier le jeton DNS dans le Presse-papiers.

b) Créez un enregistrement TXT DNS dans le fichier zone de votre domaine. Pour ce faire, accédez au portail hébergeur de domaine et ajoutez le jeton DNS que vous avez copié.

   La capture d'écran suivante montre un portail hébergeur de domaine. Votre portail peut sembler différent.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



c) Dans Citrix Cloud, sur la page **Vérifier votre domaine**, cliquez sur **Démarrer vérification de DNS** pour commencer à détecter votre enregistrement TXT DNS. Si vous souhaitez vérifier le domaine ultérieurement, cliquez sur **Vérifier le domaine ultérieurement**.

Le processus de vérification prend généralement environ une heure. Cependant, la réponse peut prendre jusqu'à deux jours. Vous pouvez vous déconnecter et vous reconnecter lors de la vérification de l'état.

Une fois la configuration terminée, l'état de votre domaine passe de **En attente** à **Vérifié**.

5. Après avoir revendiqué votre domaine, entrez les informations relatives au service de détection automatique. Cliquez sur le menu des points de suspension du domaine que vous avez ajouté, puis cliquez sur **Ajouter des informations sur Citrix Endpoint Management**. La page **Informations sur le service de détection automatique** s'affiche.

6. Entrez les informations suivantes, puis cliquez sur **Enregistrer**.

   - **Nom de domaine complet du serveur Citrix Endpoint Management :** entrez le nom de domaine complet du serveur Citrix Endpoint Management. Par exemple : `example.xm.cloud.com`. Ce paramètre est utilisé pour le trafic de contrôle MDM et MAM.
   - **Nom de domaine complet de NetScaler Gateway :** entrez le nom de domaine complet de NetScaler Gateway, sous la forme FQDN ou FQDN:port. Par exemple : `example.com`. Ce paramètre permet de diriger le trafic MAM vers votre centre de données. Pour les déploiements MDM exclusif, laissez ce champ vide.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Remarque :**
>
> Citrix vous recommande d'utiliser le paramètre **Port MAM** au lieu de **Nom de domaine complet de NetScaler Gateway** pour contrôler le trafic MAM. Si vous entrez un nom de domaine complet avec le port de votre instance NetScaler Gateway, la machine client utilise la configuration du paramètre **Port MAM**.

- **Nom de l'instance :** entrez le nom de l'instance du serveur Citrix Endpoint Management que vous avez configuré précédemment. Si vous ne connaissez pas le nom de votre instance, laissez la valeur par défaut **zdm**.
- **Port MDM :** entrez le port utilisé pour le trafic de contrôle MDM et l'inscription MDM. Pour les services basés sur le cloud, la valeur par défaut est 443.
- **Port MAM :** entrez le port utilisé pour le trafic de contrôle MAM, l'inscription MAM, l'inscription iOS et l'énumération des applications. Pour les services basés sur le cloud, la valeur par défaut est 8443.

Demander la détection automatique pour les appareils Windows

Si vous prévoyez d'inscrire des appareils Windows, procédez comme suit :

1. Contactez le support Citrix et créez une demande de support pour activer la détection automatique de Windows.
2. Obtenez un certificat SSL non générique, signé publiquement pour `enterpriseenrollment.mycompany.com`. La partie `mycompany.com` est le domaine qui contient les comptes que les utilisateurs utilisent pour s'inscrire. Joignez le certificat SSL au format .pfx et son mot de passe à la demande de support créée à l'étape précédente.

   Pour utiliser plusieurs domaines pour inscrire des appareils Windows, vous pouvez également utiliser un certificat multi-domaines avec la structure suivante :

   - Un SubjectDN avec un CN (nom commun) qui spécifie le domaine principal qu'il sert (par exemple, enterpriseenrollment.masociété1.com).
   - Les SAN appropriés pour les domaines restants (par exemple, enterpriseenrollment.masociété2.com, enterpriseenrollment.masociété3.com, etc).
3. Créez un nom canonique (CNAME) dans votre DNS et mappez l'adresse de votre certificat SSL (enterpriseenrollment.masociété.com) vers autodisc.xm.cloud.com.

   Lorsqu'un utilisateur d'appareil Windows s'inscrit à l'aide d'un UPN, le serveur d'inscription Citrix :

   - fournit les détails de votre serveur Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- indique à l'appareil de demander un certificat valide à Citrix Endpoint Management.

À ce stade, vous pouvez inscrire tous les appareils pris en charge. Passez à la section suivante pour préparer la mise à disposition de ressources aux appareils.

Intégrer avec l'accès conditionnel Azure AD

Vous pouvez configurer Citrix Endpoint Management pour appliquer la prise en charge de l'accès conditionnel Azure AD aux applications Office 365. Cette fonctionnalité vous permet de déployer la méthodologie Zero Trust pour les utilisateurs d'appareils lors du déploiement d'applications Office 365. Vous pouvez utiliser l'état de l'appareil, l'indice de risque, l'emplacement et les protections des appareils pour appliquer des actions automatisées et définir l'accès aux applications Office 365 sur les appareils Android Enterprise et iOS gérés.

Pour appliquer la conformité des appareils Azure AD, vous devez configurer des stratégies d'accès conditionnel pour les applications Office 365 individuelles. Vous pouvez restreindre l'accès des utilisateurs à des applications Office 365 spécifiques sur des appareils non gérés et non conformes et autoriser l'accès aux applications individuelles uniquement sur des appareils gérés et conformes.

Logiciels requis

- Pour cette intégration, vous devez disposer d'un abonnement Azure AD Premium valide, y compris les licences Intune et Microsoft Office 365.
- Citrix Secure Hub version 21.4.0 et ultérieure
- Configurez Azure AD en tant que fournisseur d'identité (IdP) dans Citrix Cloud, puis définissez l'identité Citrix comme type d'IdP pour Citrix Endpoint Management. Pour de plus amples informations, consultez la section Authentification avec Azure Active Directory via Citrix Cloud.
- Donnez votre consentement à l'application AAD multi-locataire Citrix pour permettre aux applications mobiles de s'authentifier auprès de l'application cliente AAD. Ceci est nécessaire uniquement si l'administrateur global Azure a défini la valeur **Les utilisateurs peuvent inscrire des applications** sur **Non**. Configurez ce paramètre dans le portail Azure sous **Azure Active Directory > Utilisateurs > Paramètres utilisateur**. Pour donner votre consentement, consultez la section Configurer Citrix Endpoint Management pour la gestion de la conformité Azure AD.
- Installez l'application Microsoft Authenticator sur l'appareil avant de démarrer le processus d'enregistrement d'appareil Azure AD.
- Pour la plate-forme Android Enterprise, configurez une application de navigateur Web comme application de magasin public requise.
- Désactivez les **paramètres de sécurité par défaut** dans la console Azure AD. Lorsque vous démarrez la configuration Azure AD, vous remplacez les paramètres de sécurité par défaut par

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

des stratégies d'accès conditionnel Azure AD plus granulaires. Pour plus d'informations sur les valeurs par défaut de sécurité, veuillez consulter la documentation Microsoft.

Configurer la conformité des appareils via des stratégies d'accès conditionnel Azure AD

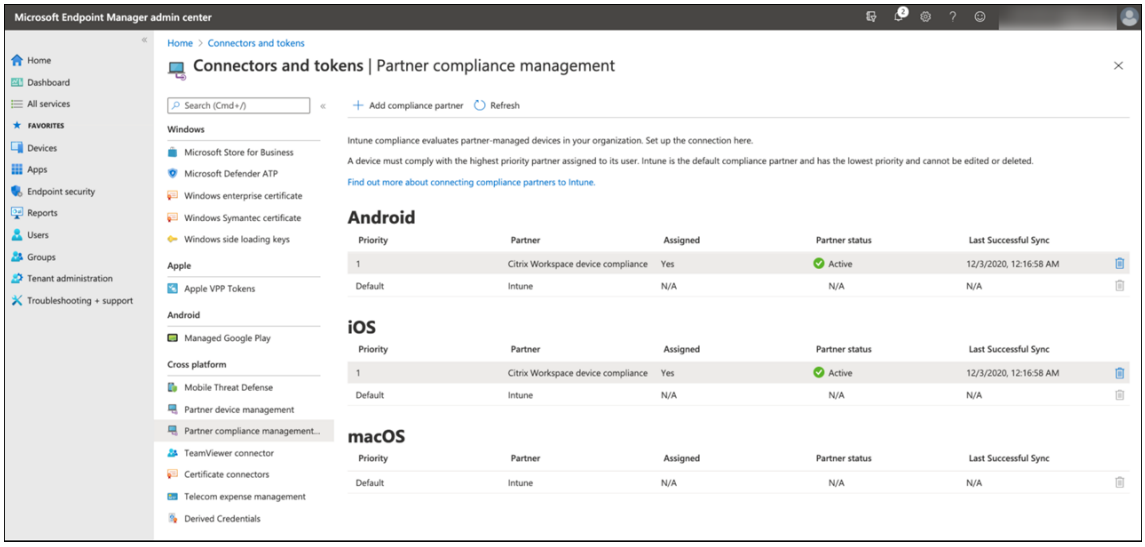
Les étapes générales pour configurer la conformité des appareils via les stratégies d'accès conditionnel Azure AD sont les suivantes :

1. **Configuration de Citrix Endpoint Management :**
   - Dans le centre d'administration Microsoft Endpoint Manager, ajoutez la **conformité des appareils Citrix Workspace** en tant que partenaire de conformité pour chaque plate-forme d'appareil et attribuez des groupes d'utilisateurs.
   - Dans Citrix Endpoint Management, synchronisez les informations à partir du centre d'administration Microsoft Endpoint Manager.
2. **Configuration Azure AD :** dans le portail Azure AD, définissez des stratégies d'accès conditionnel pour les applications Office 365 individuelles.
3. **Configuration de Citrix Endpoint Management :** après avoir configuré les stratégies d'accès conditionnel pour les applications Office 365, ajoutez l'application Microsoft Authenticator et les applications Office 365 en tant qu'applications de magasin d'applications public dans Citrix Endpoint Management. Attribuez ces applications publiques au groupe de mise à disposition et définissez-les comme applications requises.

Configurer Citrix Endpoint Management pour la gestion de la conformité Azure AD

1. Connectez-vous au centre d'administration Microsoft Endpoint Manager et accédez à **Tenant administration > Connectors and tokens > Device compliance management** (Administration des clients > Connecteurs et jetons > Gestion de la conformité des appareils). Cliquez sur **Add compliance partner** (Ajouter un partenaire de conformité) et choisissez **Citrix Workspace Device Compliance** (Conformité des appareils Citrix Workspace) comme partenaire de conformité pour chaque plate-forme d'appareil. Ensuite, attribuez des groupes d'utilisateurs.

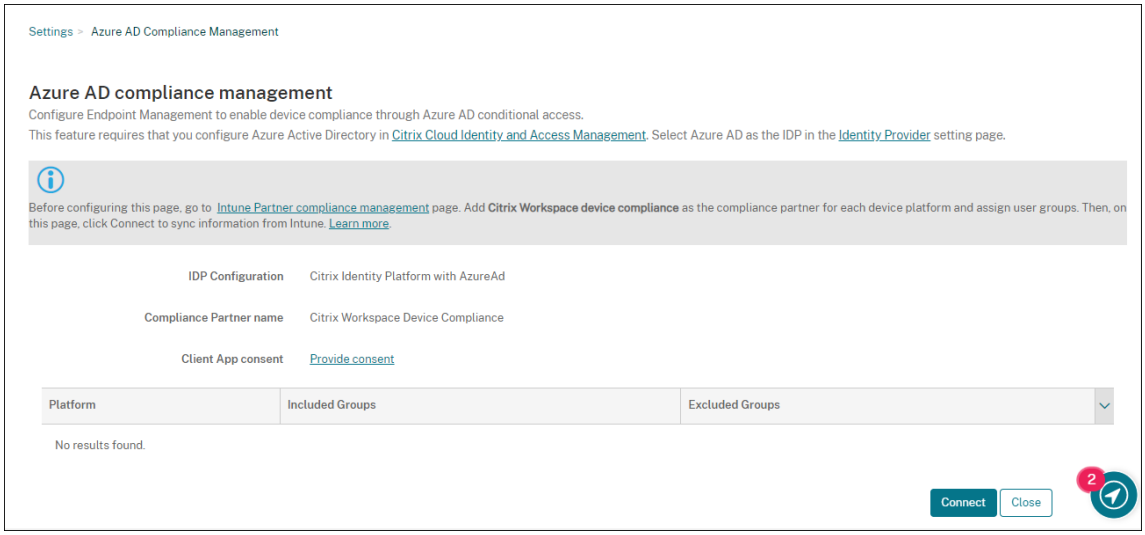
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Dans Citrix Endpoint Management, accédez à **Paramètres > Gestion de la conformité aux normes Azure AD**.

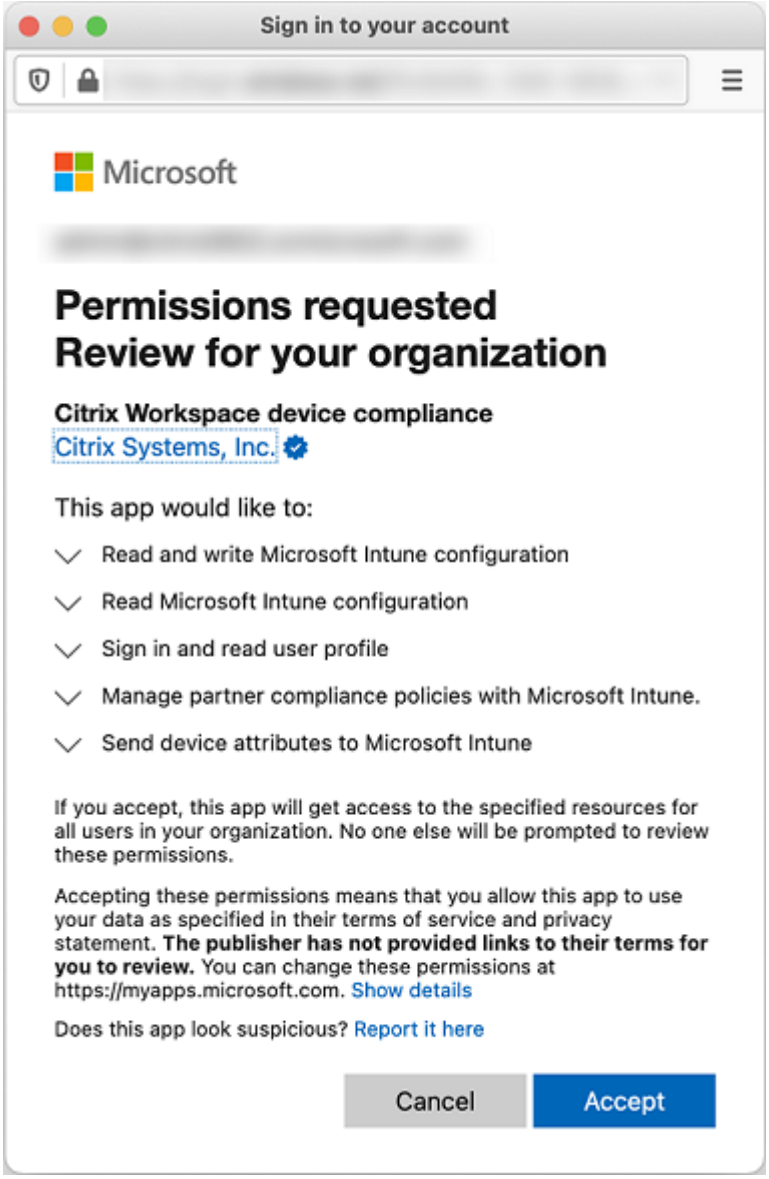
3. Si vous le souhaitez, vous pouvez définir un consentement global afin que les utilisateurs n'aient pas besoin de fournir leur consentement sur chaque appareil. En regard de l'**accord de l'application cliente**, cliquez sur **Donner mon accord**. Entrez vos informations d'identification d'administrateur général Azure AD et suivez les invites pour fournir un consentement global pour les applications clientes.

4. Cliquez sur **Se connecter** pour synchroniser les informations à partir du centre d'administration Microsoft Endpoint Manager.



Une boîte de dialogue vous invite à accepter les autorisations pour cette configuration. Cliquez sur **Accepter**. Une fois la configuration terminée, les plates-formes d'appareils synchronisées apparaissent dans la liste.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configurer les stratégies d'accès conditionnel dans Azure AD

Dans le portail Azure AD, configurez des stratégies d'accès conditionnel pour les applications Office 365 afin d'appliquer la conformité des appareils. Accédez à **Appareils > Accès conditionnel > Stratégies > Nouvelle stratégie**. Pour plus d'informations, consultez la documentation de Microsoft.

Pour configurer la conformité des appareils pour les applications gérées Intune :

- Configurer les applications gérées par Intune pour les distribuer sur les appareils
- Exiger des applications clientes approuvées
- Exiger une stratégie de protection des applications et une application cliente approuvée pour l'accès aux applications cloud

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer des applications dans Citrix Endpoint Management

Après avoir configuré les stratégies d'accès conditionnel pour les applications Office 365, ajoutez l'application Microsoft Authenticator et les applications Office 365 en tant qu'applications de magasin d'applications public dans Citrix Endpoint Management. Attribuez ces applications publiques au groupe de mise à disposition et définissez-les comme applications requises. Pour plus d'informations, consultez la section Ajouter une application d'un magasin d'applications public.

Workflow d'authentification utilisateur

1. Un nouvel utilisateur doit inscrire un appareil sur Citrix Endpoint Management à l'aide des informations d'identification Azure AD. Les utilisateurs qui étaient précédemment inscrits avec des informations d'identification Azure AD, n'ont pas besoin de réinscrire leurs appareils.
2. Citrix Endpoint Management envoie Microsoft Authenticator et les applications Office 365 configurées sur un appareil en tant qu'applications requises. Si vous avez configuré une application de navigateur Web comme application de magasin public requise pour la plate-forme Android, Citrix Endpoint Management l'envoie également sur la machine utilisateur.
3. Citrix Secure Hub installe et affiche automatiquement toutes les applications gérées via Citrix Endpoint Management.
4. Lorsqu'un utilisateur tente de se connecter à une application Office 365 disponible, l'appareil invite l'utilisateur à appuyer sur le lien **d'inscription Azure AD** pour démarrer le processus d'inscription.
5. Une fois que l'utilisateur appuie sur le lien d'inscription, l'application Microsoft Authenticator s'ouvre. L'utilisateur entre les informations d'identification Azure AD et accepte les conditions d'inscription de l'appareil. Ensuite, l'application Microsoft Authenticator se ferme et Citrix Secure Hub s'ouvre de nouveau.
6. Citrix Secure Hub affiche un message indiquant que l'inscription des appareils Azure AD est terminée. L'utilisateur peut désormais utiliser les applications Microsoft pour accéder à ses ressources cloud.

   Une fois l'inscription terminée, Azure AD marque l'appareil comme géré et conforme dans la console.

Stratégies d'appareil par défaut et applications de productivité mobiles

Si vous intégrez Citrix Endpoint Management à partir de la version 19.5.0 ou version ultérieure, nous préconfigurons quelques stratégies d'appareil et applications de productivité mobiles. Cette configuration vous permet de :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Déployer immédiatement des fonctionnalités de base sur les appareils
- Commencer par les configurations de base recommandées pour un espace de travail sécurisé

Pour les plates-formes Android, Android Enterprise, iOS, macOS et Windows Desktop/Tablet, votre site contient les stratégies d'appareil préconfigurées suivantes :

- **Stratégie de code secret :** la stratégie de code secret est définie sur **Activé** et tous les paramètres de code secret sont activés par défaut.
- **Stratégie d'inventaire des applications :** la stratégie d'inventaire des applications est définie sur **Activé**.
- **Stratégies de restrictions :** la stratégie de restrictions est définie sur **Activé** et tous les paramètres de restrictions sont activés par défaut.

Ces stratégies se trouvent dans le groupe de mise à disposition **AllUsers**, qui contient tous les utilisateurs Active Directory et locaux. Nous vous recommandons d'utiliser le groupe de mise à disposition AllUsers uniquement pour les tests initiaux. Ensuite, créez vos propres groupes de mise à disposition et désactivez le groupe de mise à disposition AllUsers. Vous pouvez réutiliser les stratégies et les applications préconfigurées dans vos groupes de mise à disposition.

Toutes les stratégies d'appareil Citrix Endpoint Management sont documentées sous Stratégies d'appareil. Cet article contient des informations sur l'utilisation de la console pour modifier les stratégies d'appareil. Pour plus d'informations sur certaines stratégies d'appareil couramment utilisées, consultez la section Stratégies d'appareil et cas d'utilisation.

Pour les plates-formes iOS et Android, votre site contient les applications de productivité mobiles préconfigurées suivantes :

- **Citrix Secure Mail**
- **Citrix Secure Web**
- **Citrix Files**

Ces applications se trouvent dans le groupe de mise à disposition **AllUsers**.

Pour de plus amples informations, consultez la section À propos des applications de productivité mobiles.

Poursuivre la configuration Citrix Endpoint Management

Une fois que vous avez terminé la configuration de base pour l'inscription de l'appareil, la manière dont vous configurez Citrix Endpoint Management varie considérablement en fonction de vos cas d'utilisation. Par exemple :

- Quelles sont vos exigences en matière de sécurité et comment souhaitez-vous équilibrer ces exigences avec l'expérience utilisateur ?

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Quelles plates-formes d'appareils prenez-vous en charge ?
- Les utilisateurs possèdent-ils leurs appareils ou utilisent-ils des appareils appartenant à l'entreprise ?
- Quelles stratégies souhaitez-vous transmettre aux appareils ?
- Quels types d'applications proposez-vous aux utilisateurs ?

Cette section vous aide à naviguer parmi les nombreux choix de configuration en vous dirigeant vers les articles de documentation.

Lorsque vous terminez la configuration sur des sites tiers, notez les informations et leur emplacement à des fins de référence lors de la configuration des paramètres de la console Citrix Endpoint Management.

- Sécurité et authentification. Citrix Endpoint Management utilise les certificats pour établir des connexions sécurisées et authentifier les utilisateurs. Citrix fournit des certificats génériques pour votre instance Citrix Endpoint Management.
  - Pour plus d'informations sur les composants d'authentification et les configurations recommandées par niveau de sécurité, consultez la section « Concepts avancés » dans l'article Authentification. Consultez également Sécurité et expérience utilisateur.
  - Pour une présentation des composants d'authentification utilisés lors des opérations Citrix Endpoint Management, consultez la section Certificats et authentification.
  - Vous pouvez choisir parmi les types d'authentification suivants. La configuration de l'authentification inclut des tâches dans les consoles Citrix Endpoint Management et NetScaler Gateway.
    * Authentification avec domaine ou domaine + jeton de sécurité
    * Authentification certificat client ou certificat + domaine
  - Pour la mise à disposition de certificats aux utilisateurs, configurez les éléments suivants :
    * Entités PKI
    * Fournisseur d'identités
  - Modes d'inscription sécurisée. Les modes d'inscription sécurisée des appareils spécifient les types d'informations d'identification et les étapes d'inscription des utilisateurs requis pour que les utilisateurs inscrivent leurs appareils dans Citrix Endpoint Management. Pour de plus amples informations, consultez la section Configurer les modes d'inscription sécurisée.
  - Pour permettre aux utilisateurs de s'authentifier à l'aide d'informations d'identification Azure Active Directory, consultez la section Authentification avec Azure Active Directory via Citrix Cloud.
- Inscription d'appareils

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Des programmes sont disponibles pour inscrire un grand nombre d'appareils :
    * Déployer des appareils via le programme de déploiement d'Apple
    * Inscription en bloc d'appareils Apple
    * Inscription en bloc d'appareils Windows
  - Pour inscrire des appareils Android, créez un compte d'administrateur Android Enterprise. Consultez Android Enterprise. Ou consultez Ancienne version d'Android Enterprise pour clients Google Workspace.
  - Vous pouvez utiliser des invitations d'inscription ou envoyer des notifications pour l'inscription.
    * Invitations d'inscription.
    * Notifications.
  - Pour plus d'informations sur l'inscription, consultez la section Gestion d'appareils et les articles associés.

- Stratégies et gestion d'appareil
  - Stratégies d'appareil (MDM). Toutes les stratégies d'appareil Citrix Endpoint Management sont documentées sous Stratégies d'appareil. Pour plus d'informations sur certaines stratégies d'appareil couramment utilisées, consultez la section Stratégies d'appareil et cas d'utilisation.
  - Propriétés du client. Les propriétés du client contiennent des informations qui sont fournies directement à Citrix Secure Hub sur les appareils des utilisateurs. Consultez Propriétés du client et Propriétés du client Citrix Endpoint Management.
  - Groupes de mise à disposition. Pour un exemple de cas d'utilisation lié à des groupes de mise à disposition, consultez les sections Communautés d'utilisateurs et Ajouter un groupe de mise à disposition.

- Préparer le déploiement d'application
  - Pour plus d'informations sur les applications prises en charge par Citrix Endpoint Management, consultez la section Ajouter des applications.
  - Vous pouvez gérer les licences d'applications iOS à l'aide de l'achat en volume d'Apple. Pour de plus amples informations, consultez la section Achat en volume d'Apple.
  - Vous pouvez utiliser Citrix Endpoint Management pour déployer des iBooks que vous obtenez via l'achat en volume d'Apple. Voir Ajouter un média.
  - Citrix fournit des applications de productivité mobiles, notamment Citrix Secure Mail et Citrix Secure Web. Consultez la section À propos des applications de productivité mobiles.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Au lieu de Citrix Secure Mail, vous pouvez mettre à disposition des appareils une messagerie native. Consultez :
    * Stratégie de messagerie
    * Citrix Endpoint Management Connector pour Exchange ActiveSync
    * NetScaler Gateway Connector pour Exchange ActiveSync
  - Pour permettre aux utilisateurs de transférer en toute sécurité des documents et des données vers les applications Microsoft Office 365, consultez les sections Autoriser l'interaction sécurisée avec les applications Office 365 et Stratégie Office.
  - Pour des informations générales sur les stratégies des applications, consultez la section Stratégies d'application et scénarios de cas d'utilisation.
  - Le MDX Toolkit est une technologie d'encapsulation d'application qui prépare les applications d'entreprise en vue de les déployer en toute sécurité avec Citrix Endpoint Management. Le SDK MAM remplace l'outil MDX Toolkit. Le MDX Toolkit devrait atteindre la fin de son cycle de vie en juillet 2023.

    Pour plus d'informations sur le SDK MAM, consultez la section Présentation du SDK MAM.
  - Pour plus d'informations sur les applications, consultez les autres articles sous Ajouter des applications.

- La fonctionnalité de contrôle d'accès basé sur rôle (RBAC) de Citrix Endpoint Management vous permet d'attribuer des rôles prédéfinis ou un ensemble d'autorisations aux utilisateurs et aux groupes. Ces autorisations contrôlent le niveau d'accès des utilisateurs aux fonctions du système. Pour plus d'informations, consultez la section Configurer des rôles avec RBAC.
- Vous créez des actions automatisées dans Citrix Endpoint Management pour spécifier des actions à prendre suite à des événements, à certaines propriétés ou à la présence d'applications sur les appareils utilisateur. Pour plus d'informations, consultez la section Actions automatisées.

Certificats et authentification

March 1, 2024

Plusieurs composants jouent un rôle dans le processus d'authentification lors des opérations Citrix Endpoint Management :

- **Citrix Endpoint Management :** le serveur Citrix Endpoint Management vous permet de définir la sécurité liée à l'inscription ainsi que l'expérience d'inscription. Les options d'intégration des utilisateurs comprennent :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Inscription ouverte à tous ou sur invitation seulement.
  - Authentification à deux facteurs ou à trois facteurs obligatoire. Les propriétés du client Citrix Endpoint Management vous permettent d'activer l'authentification par code PIN Citrix et de configurer la complexité et l'expiration du code PIN.

- **NetScaler Gateway :** NetScaler Gateway fournit un point de terminaison pour les sessions SSL micro VPN. NetScaler Gateway assure aussi la sécurité en transit sur le réseau et vous permet de définir l'expérience d'authentification utilisée chaque fois qu'un utilisateur accède à une application.

- **Citrix Secure Hub :** Citrix Secure Hub fonctionne avec Citrix Endpoint Management au cours des opérations d'inscription. Citrix Secure Hub est l'entité basée sur un appareil qui communique avec NetScaler Gateway : lorsqu'une session expire, Citrix Secure Hub obtient un ticket d'authentification de NetScaler Gateway et transmet le ticket aux applications MDX. Citrix vous recommande le certificate pinning, qui empêche les attaques « man-in-the-middle ». Pour de plus amples informations, consultez cette section dans l'article Citrix Secure Hub : Certificate pinning.

  Citrix Secure Hub gère également le conteneur de sécurité MDX : Citrix Secure Hub force les stratégies, crée une session avec NetScaler Gateway lors de l'expiration d'une application et définit le délai d'expiration MDX et l'authentification. Citrix Secure Hub est également responsable de la détection des appareils jailbreakés, des contrôles de géolocalisation et de toute autre stratégie que vous appliquez.

- **Stratégies MDX :** les stratégies MDX créent l'espace de stockage sécurisé sur l'appareil. Les stratégies MDX redirigent les connexions micro VPN vers NetScaler Gateway et appliquent les restrictions du mode déconnecté ainsi que les stratégies de client, telles que les délais d'expiration.

Citrix Endpoint Management authentifie les utilisateurs auprès de leurs ressources à l'aide des méthodes d'authentification suivantes :

- Gestion des appareils mobiles (MDM)
  - Fournisseurs d'identité (IdP) hébergés sur le cloud
  - LDAP (Lightweight Directory Access Protocol)
    - URL d'invitation + PIN
    - Authentification à deux facteurs
- Gestion des applications mobiles (MAM)
  - LDAP
  - Certificat
  - L'authentification MAM par jeton de sécurité requiert NetScaler Gateway.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour plus d'informations sur la configuration, consultez les articles suivants :

- Charger, mettre à jour et renouveler des certificats
- NetScaler Gateway et Citrix Endpoint Management
- Authentification avec domaine ou domaine + jeton de sécurité
- Authentification certificat client ou certificat + domaine
- Entités PKI
- Fournisseur d'identités
- Certificats APNs
- SAML pour l'authentification unique avec Citrix Files
- Authentification avec Azure Active Directory via Citrix Cloud
- Authentification avec Okta via Citrix Cloud
- Authentification avec une passerelle NetScaler Gateway locale via Citrix Cloud
- Pour l'authentification auprès d'un serveur Wi-Fi, envoyez un certificat aux appareils : Stratégie de réseau
- Pour envoyer un certificat unique non utilisé pour l'authentification, tel qu'un certificat d'autorité de certification racine interne ou une stratégie spécifique : Stratégie d'informations d'identification

Certificats

Citrix Endpoint Management génère un certificat SSL auto-signé lors de l'installation afin de sécuriser les communications sur le serveur. Remplacez le certificat SSL avec un certificat SSL approuvé provenant d'une autorité de certification reconnue.

Citrix Endpoint Management utilise également son propre service d'infrastructure de clé publique (PKI) ou obtient les certificats de l'autorité de certification pour les certificats clients. Tous les produits Citrix prennent en charge les caractères génériques et les certificats SAN. Pour la plupart des déploiements, vous n'aurez besoin que deux caractères génériques ou certificats SAN.

L'authentification du certificat client offre une couche de sécurité supplémentaire pour les applications mobiles et permet aux utilisateurs d'accéder de manière transparente aux applications HDX. Lorsque l'authentification du certificat client est configurée, les utilisateurs entrent leur code PIN Citrix pour accéder aux applications Citrix Endpoint Management avec l'authentification unique. Le code secret Citrix simplifie également l'expérience utilisateur pour l'authentification. Le code PIN Citrix est utilisé pour sécuriser un certificat client ou enregistrement des informations d'identification Active Directory localement sur leur appareil.

Pour inscrire et gérer des appareils iOS avec Citrix Endpoint Management, configurez et créez un certificat Apple Push Notification Service (APNS). Ces étapes sont décrites sous Certificats APNS.

Le tableau suivant illustre le format et le type du certificat pour chaque composant Citrix Endpoint Management :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Composant Citrix Endpoint Management	Format du certificat	Type de certificat requis
NetScaler Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Root (NetScaler Gateway convertit automatiquement un fichier PFX vers PEM.
Citrix Endpoint Management	.p12 (.pfx sur les ordinateurs Windows)	SSL, SAML, APN (Citrix Endpoint Management génère également une PKI complète au cours du processus d'installation.) **Important :** Citrix Endpoint Management ne prend pas en charge les certificats avec une extension .pem. Pour utiliser un certificat .pem, divisez le fichier .pem en un certificat et une clé et importez-les dans le serveur Citrix Endpoint Management.
StoreFront	PFX (PKCS #12)	SSL, racine

Citrix Endpoint Management prend en charge les certificats clients de 4096 et 2048 bits.

Pour NetScaler Gateway et Citrix Endpoint Management, il est recommandé d'obtenir les certificats de serveur à partir d'une autorité de certification publique, comme Verisign, Thawte ou DigiCert. Vous pouvez créer une demande de signature de certificat (CSR) à partir de NetScaler Gateway ou de l'utilitaire de configuration Citrix Endpoint Management. Lorsque vous créez la CSR, envoyez-la à l'autorité de certification pour signature. Lorsque l'autorité de certification renvoie le certificat signé, vous pouvez l'installer sur NetScaler Gateway ou Citrix Endpoint Management.

> **Important :**
>
> conditions requises pour les certificats de confiance dans iOS, iPadOS et macOS
>
> Apple a introduit de nouvelles exigences pour les certificats de serveur TLS. Vérifiez que tous les certificats respectent les exigences d'Apple. Consultez la publication Apple, https://support.apple.com/en-us/HT210176.
>
> Apple réduit la durée de vie maximale autorisée des certificats de serveur TLS. Cette modification concerne uniquement les certificats de serveur émis après septembre 2020. Consultez la publication Apple, https://support.apple.com/en-us/HT211025.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Authentification LDAP

Citrix Endpoint Management prend en charge l'authentification basée sur domaine pour un ou plusieurs annuaires, qui sont compatibles avec le protocole LDAP (Lightweight Directory Access Protocol). LDAP est un protocole logiciel qui permet d'accéder à des informations sur les groupes, les comptes utilisateur et les propriétés associées. Pour de plus amples informations, consultez la section Domaine ou domaine + authentification par jeton de sécurité.

Authentification par fournisseur d'identité

Vous pouvez configurer un fournisseur d'identité (IdP) via Citrix Cloud pour inscrire et gérer les machines utilisateur.

Cas d'utilisation pris en charge pour les fournisseurs d'identité :

- Azure Active Directory via Citrix Cloud
  - L'intégration de Workspace est facultative
  - NetScaler Gateway configuré pour l'authentification par certificat
  - Android Enterprise (version préliminaire. Prise en charge du BYOD, des appareils entièrement gérés et des profils d'inscription améliorés)
  - iOS pour les inscriptions MDM+MAM et MDM
  - iOS et macOS pour les inscriptions dans Apple Business Manager
  - Android ancienne version (DA)

  Les fonctionnalités d'inscription automatique telles que Apple School Manager ne sont actuellement pas prises en charge.
- Okta via Citrix Cloud
  - L'intégration de Workspace est facultative
  - NetScaler Gateway configuré pour l'authentification par certificat
  - Android Enterprise (version préliminaire. Prise en charge du BYOD, des appareils entièrement gérés et des profils d'inscription améliorés)
  - iOS pour les inscriptions MDM+MAM et MDM
  - iOS et macOS pour les inscriptions dans Apple Business Manager
  - Android ancienne version (DA)

  Les fonctionnalités d'inscription automatique telles que Apple School Manager ne sont actuellement pas prises en charge.
- Instance NetScaler Gateway locale via Citrix Cloud
  - NetScaler Gateway configuré pour l'authentification par certificat

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Android Enterprise (version préliminaire. Prise en charge du BYOD, des appareils entièrement gérés et des profils d'inscription améliorés)
  - iOS pour les inscriptions MDM+MAM et MDM
  - Android ancienne version (DA)
    Les fonctionnalités d'inscription automatique telles que le programme de déploiement Apple ne sont actuellement pas prises en charge

Charger, mettre à jour et renouveler des certificats

March 1, 2024

Nous vous recommandons de répertorier les certificats nécessaires à votre déploiement Citrix Endpoint Management. Utilisez la liste pour suivre les dates d'expiration du certificat et les mots de passe. Cet article vous aide à administrer les certificats tout au long de leur durée de vie.

Votre environnement peut inclure les certificats suivants :

- Serveur Citrix Endpoint Management
  - Certificat SSL pour nom de domaine complet MDM (nécessaire si vous avez migré de XenMobile Server vers Citrix Endpoint Management ; sinon, Citrix gère ce certificat)
  - Certificat SAML (pour Citrix Files)
  - Certificats d'autorité de certification racine et intermédiaire pour les certificats ci-dessus et toute autre ressource interne (StoreFront/Proxy, etc)
  - Certificat APNs pour la gestion des appareils iOS
  - Certificat utilisateur PKI pour la connectivité aux infrastructures de clé publique (PKI) (requis si votre environnement nécessite une authentification basée sur des certificats)
- MDX Toolkit
  - Certificat Apple Developer
  - Profil de provisioning Apple (par application)
  - Certificat APNs Apple (pour utilisation avec Citrix Secure Mail)
  - Fichier de keystore Android

  Le SDK MAM n'encapsulant pas les applications, il ne nécessite donc pas de certificat.
- NetScaler Gateway
  - Certificat SSL pour nom de domaine complet MDM
  - Certificat SSL pour nom de domaine complet Gateway
  - Certificat SSL pour nom de domaine complet ShareFile SZC

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Certificat SSL pour l'équilibrage de charge Exchange (configuration de déchargement)
  - Certificat SSL pour l'équilibrage de charge StoreFront
  - Certificats d'autorité de certification racine et intermédiaire pour les certificats ci-dessus

> **Remarque :**
>
> La machine cliente doit disposer du certificat racine/intermédiaire requis pour établir la confiance avec l'autorité de certification qui a émis le certificat de serveur. Sinon, il est possible que vous receviez l'erreur SSL 61. Pour résoudre ce problème :
>
> 1. Téléchargez ou obtenez le fichier de certificat racine/intermédiaire SSL (.crt ou .cer) émis par votre fournisseur de certificats SSL. En général, le certificat racine/intermédiaire/serveur se trouve dans le bundle de certificats fourni par votre fournisseur de services SSL.
> 2. Installez le certificat racine/intermédiaire sur la machine cliente.
> 3. Si un antivirus est installé sur la machine cliente, assurez-vous que l'antivirus fait confiance au certificat.

Charger des certificats

Chaque certificat que vous chargez est représenté par une entrée dans le tableau Certificats, qui résume son contenu. Lorsque vous configurez des composants d'intégration PKI qui nécessitent un certificat, choisissez un certificat de serveur répondant à ces critères. Par exemple, il se peut que vous souhaitiez configurer Citrix Endpoint Management pour s'intégrer à votre autorité de certification (CA) Microsoft. La connexion à Microsoft CA doit être authentifiée à l'aide d'un certificat client.

Citrix Endpoint Management peut ne pas posséder la clé privée d'un certificat donné. De même, Citrix Endpoint Management peut nécessiter une clé privée pour les certificats chargés.

Cette section explique comment charger des certificats. Pour de plus amples informations sur la création, le chargement et la configuration de certificats clients, consultez la section Authentification certificat client ou certificat + domaine.

Vous disposez de deux options pour charger des certificats :

- Chargez les certificats individuellement sur la console.
- Effectuez un chargement groupé de certificats à l'aide de l'API REST. Cette option est disponible uniquement pour les appareils iOS.

Pour télécharger des certificats sur la console :

- Importez un keystore. Vous identifiez ensuite l'entrée dans le référentiel de keystore dans lequel vous souhaitez l'installer, sauf si vous chargez un format PKCS #12.
- Importez un certificat.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

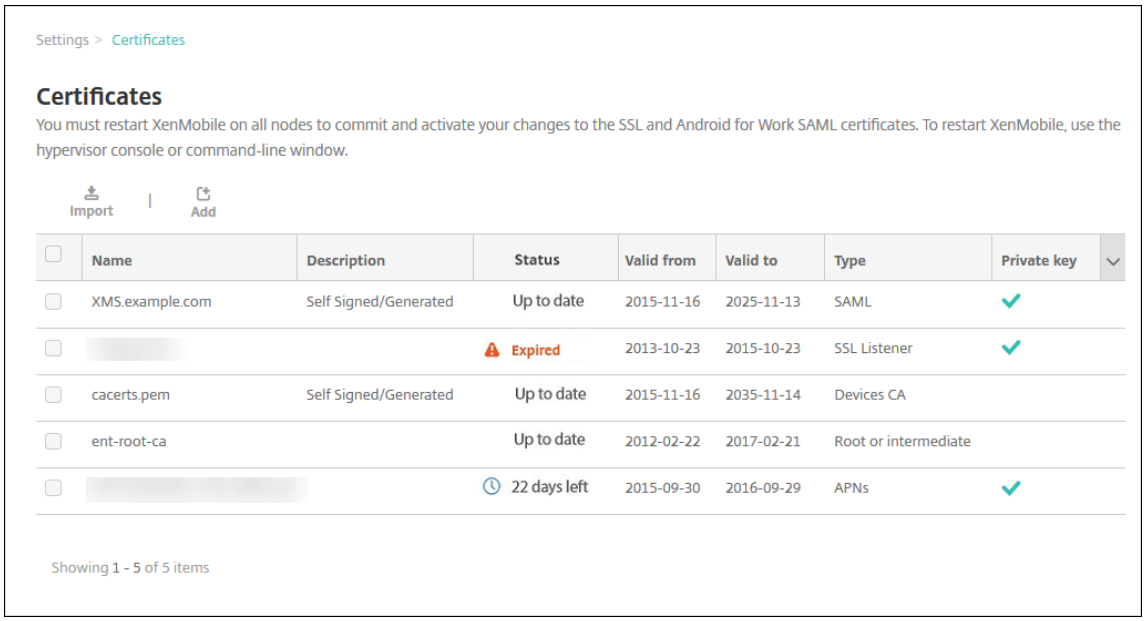
Vous pouvez charger le certificat d'autorité de certification (sans clé privée) que l'autorité de certification utilise pour signer les demandes. Vous pouvez également charger un certificat de client SSL (avec clé privée) pour l'authentification du client.

Lors de la configuration de l'entité Microsoft CA, vous spécifiez le certificat d'autorité de certification. Vous sélectionnez le certificat d'autorité de certification dans une liste de tous les certificats de serveur qui sont des certificats d'autorité de certification. De même, lorsque vous configurez l'authentification de client, vous pouvez faire votre choix dans une liste de tous les certificats de serveur pour lesquels Citrix Endpoint Management possède la clé privée.

Pour importer un keystore

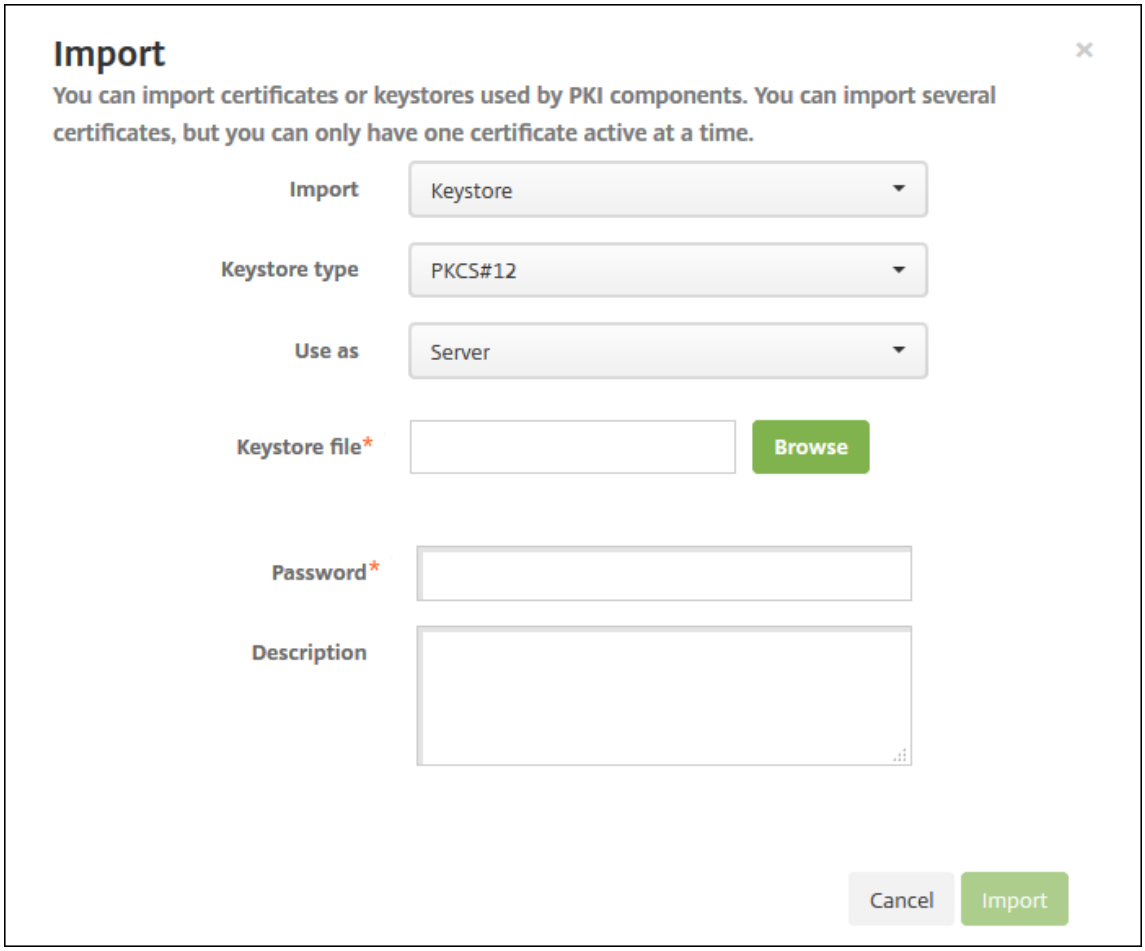
Un keystore (ou magasin de clés) est un référentiel de certificats de sécurité. Les keystores, de par leur conception, peuvent comporter plusieurs entrées. Lors du chargement à partir d'un keystore, vous devez indiquer l'alias d'entrée qui identifie l'entrée à charger. Si vous ne spécifiez pas d'alias, la première entrée du magasin est chargée. Étant donné que les fichiers PKCS #12 ne contiennent généralement qu'une seule entrée, le champ d'alias ne s'affiche pas lorsque vous sélectionnez PKCS #12 en tant que type de keystore.

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. Utilisez la barre de recherche pour rechercher et ouvrir le paramètre **Certificats**.



2. Cliquez sur **Importer**. La boîte de dialogue **Importer** apparaît.
3. Pour configurer ces paramètres :
   - **Importer :** sélectionnez **Keystore**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Type de keystore :** dans la liste, cliquez sur **PKCS #12**.
- **Utiliser en tant que :** dans la liste, cliquez pour spécifier la manière dont vous prévoyez d'utiliser le certificat. Les options disponibles sont :
  - **Serveurs :** les certificats de serveur sont des certificats utilisés par Citrix Endpoint Management. Vous téléchargez des certificats de serveur sur la console Web Citrix Endpoint Management. Ces certificats comprennent des certificats d'autorité de certification, des certificats d'autorité d'inscription et des certificats pour l'authentification des clients avec d'autres composants de votre infrastructure. En outre, vous pouvez utiliser les certificats de serveur en tant que stockage pour les certificats que vous voulez déployer vers des appareils. Cette utilisation s'applique particulièrement aux autorités de certification utilisées pour établir une relation de confiance sur l'appareil.
  - **SAML :** la certification SAML vous permet de fournir une authentification unique (SSO) aux serveurs, sites Web et applications.
  - **APNs :** les certificats APNS d'Apple permettent de gérer les appareils mobiles via le réseau Apple Push Network.
  - **Écouteur SSL :** l'écouteur SSL (Secure Sockets Layer) notifie Citrix Endpoint Manage-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ment de l'activité cryptographique SSL.

- **Fichier de keystore :** recherchez le keystore que vous souhaitez importer. Le keystore est un fichier .p12 ou .pfx. Sélectionnez le fichier et cliquez sur **Ouvrir**.
- **Mot de passe :** entrez le mot de passe affecté au certificat.
- **Description :** entrez une description vous permettant de distinguer le keystore de vos autres keystores (facultatif).

4. Cliquez sur **Importer**. Le keystore est ajouté au tableau Certificats.

Pour importer un certificat

Lors de l'importation d'un certificat, Citrix Endpoint Management tente de construire une chaîne de certificats à partir de l'entrée. Citrix Endpoint Management importe tous les certificats de cette chaîne pour créer une entrée de certificat de serveur pour chaque certificat. Cette opération fonctionne uniquement si les certificats du fichier ou l'entrée keystore forment réellement une chaîne. Chaque certificat suivant de la chaîne doit être l'émetteur du certificat précédent.

Vous pouvez ajouter une description facultative pour le certificat importé. La description est uniquement attachée au premier certificat dans la chaîne. Vous pouvez mettre à jour la description des certificats restants plus tard.

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. Utilisez la barre de recherche pour rechercher et ouvrir le paramètre **Certificats**.

2. Sur la page **Certificats**, cliquez sur **Importer**. La boîte de dialogue **Importer** apparaît. Configurez ce qui suit :

   - **Importer :** cliquez sur **Certificat**.
   - **Utiliser en tant que :** spécifiez la manière dont vous prévoyez d'utiliser le certificat. Les options disponibles sont :
     - **Serveurs :** les certificats de serveur sont des certificats utilisés par Citrix Endpoint Management. Vous téléchargez des certificats de serveur sur la console Web Citrix Endpoint Management. Ces certificats comprennent des certificats d'autorité de certification, des certificats d'autorité d'inscription et des certificats pour l'authentification des clients avec d'autres composants de votre infrastructure. En outre, vous pouvez utiliser les certificats de serveur en tant que stockage pour les certificats que vous voulez déployer vers des appareils. Cette option s'applique particulièrement aux autorités de certification utilisées pour établir une relation de confiance sur l'appareil.
     - **SAML :** la certification SAML vous permet de fournir une authentification unique (SSO) aux serveurs, sites Web et applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Écouteur SSL :** l'écouteur SSL (Secure Sockets Layer) notifie Citrix Endpoint Management de l'activité cryptographique SSL.
- **Importation de certificat :** recherchez le certificat que vous souhaitez importer. Sélectionnez le fichier et cliquez sur **Ouvrir**.
- **Fichier de clé privée :** recherchez le fichier de clé privée facultatif associé au certificat. La clé privée est utilisée pour le chiffrement et le déchiffrement en conjonction avec le certificat. Sélectionnez le fichier et cliquez sur **Ouvrir**.
- **Description :** (facultatif) entrez une description pour le certificat pour vous aider à le distinguer de vos autres certificats.

3. Cliquez sur **Importer**. Le certificat est ajouté au tableau Certificats.

Effectuer un chargement groupé de certificats avec l'API REST Il existe des situations où le chargement d'un seul certificat à la fois n'est pas pratique. Dans ce cas, effectuez un chargement groupé de certificats à l'aide de l'API REST. Cette méthode prend en charge les certificats au format .p12. Pour plus d'informations sur l'API REST, reportez-vous à la section API REST.

1. Renommez chacun des fichiers de certificat au format `device_identity_value.p12`. `device_identity_value` peut être l'IMEI, le numéro de série ou le MEID de chaque appareil.

   Par exemple, vous choisissez d'utiliser les numéros de série comme méthode d'identification. Le numéro de série de l'appareil est `A12BC3D4EFGH`, donc nommez le fichier de certificat que vous prévoyez d'installer sur cet appareil de la façon suivante : `A12BC3D4EFGH.p12`.

2. Créez un fichier texte pour stocker les mots de passe pour les certificats .p12. Dans ce fichier, tapez l'identifiant et le mot de passe de chaque appareil sur une nouvelle ligne. Utilisez le format `device_identity_value=password`. Consultez les pages suivantes :

```
A12BC3D4EFGH.p12=password1!
A12BC3D4EFIJ.p12=password2@
A12BC3D4EFKL.p12=password3#
<!--NeedCopy-->
```

3. Compressez tous les certificats et le fichier texte que vous avez créé dans un fichier .zip.

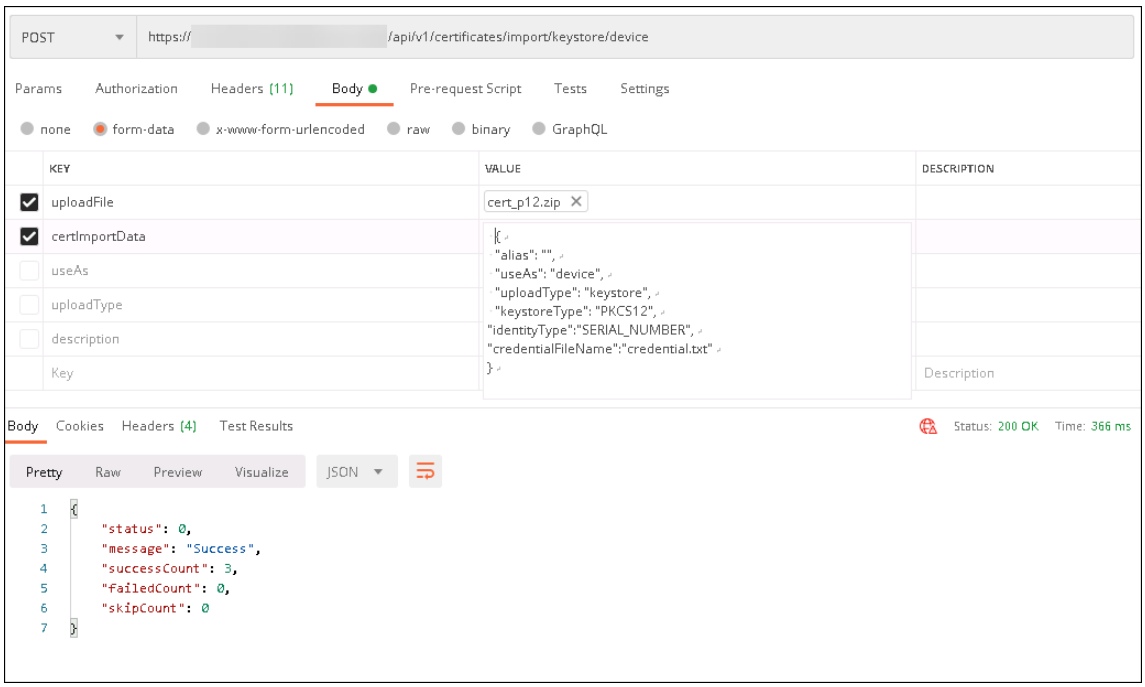
4. Lancez votre client d'API REST, connectez-vous à Citrix Endpoint Management et obtenez un jeton d'authentification.

5. Importez vos certificats, en vous assurant de placer les éléments suivants dans le corps du message :

```
{

    "alias": "",
    "useAs": "device",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

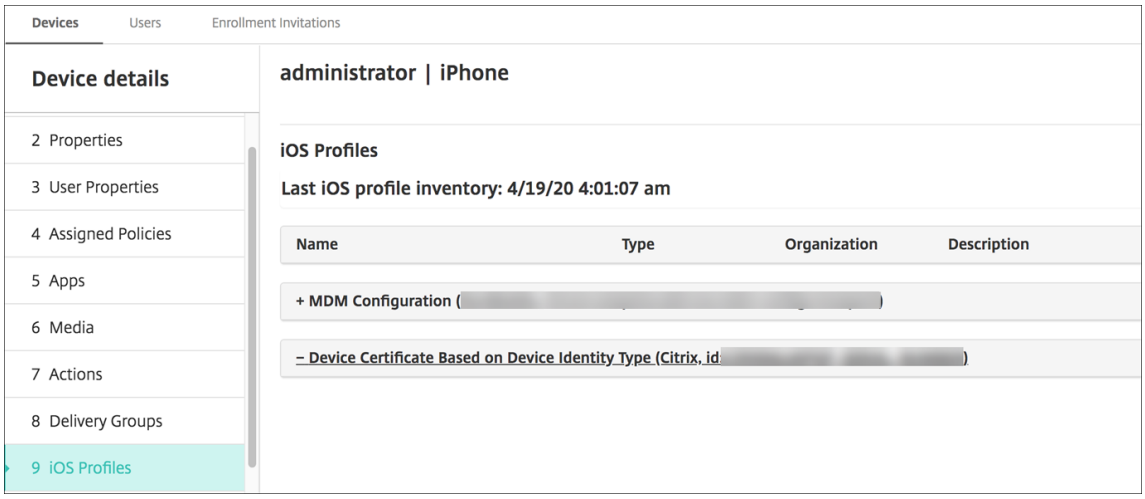
```
5       "uploadType": "keystore",
6       "keystoreType": "PKCS12",
7       "identityType":"SERIAL_NUMBER",        # identity type can be
            "SERIAL_NUMBER","IMEI","MEID"
8       "credentialFileName":"credential.txt"   # The credential file
            name in .zip
9   }
10
11  <!--NeedCopy-->
```



6. Créez une stratégie VPN avec le type d'informations d'identification **Always on IKEv2** (Toujours sur IKEv2) et la méthode d'authentification d'appareil **Certificat d'appareil basé sur l'identité de l'appareil**. Sélectionnez le **Type d'identité de l'appareil** que vous avez utilisé dans vos noms de fichiers de certificat. Consultez la section Stratégie VPN.

7. Inscrivez un appareil iOS et attendez le déploiement de la stratégie VPN. Confirmez l'installation du certificat en vérifiant la configuration MDM sur l'appareil. Vous pouvez également vérifier les détails de l'appareil dans la console Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

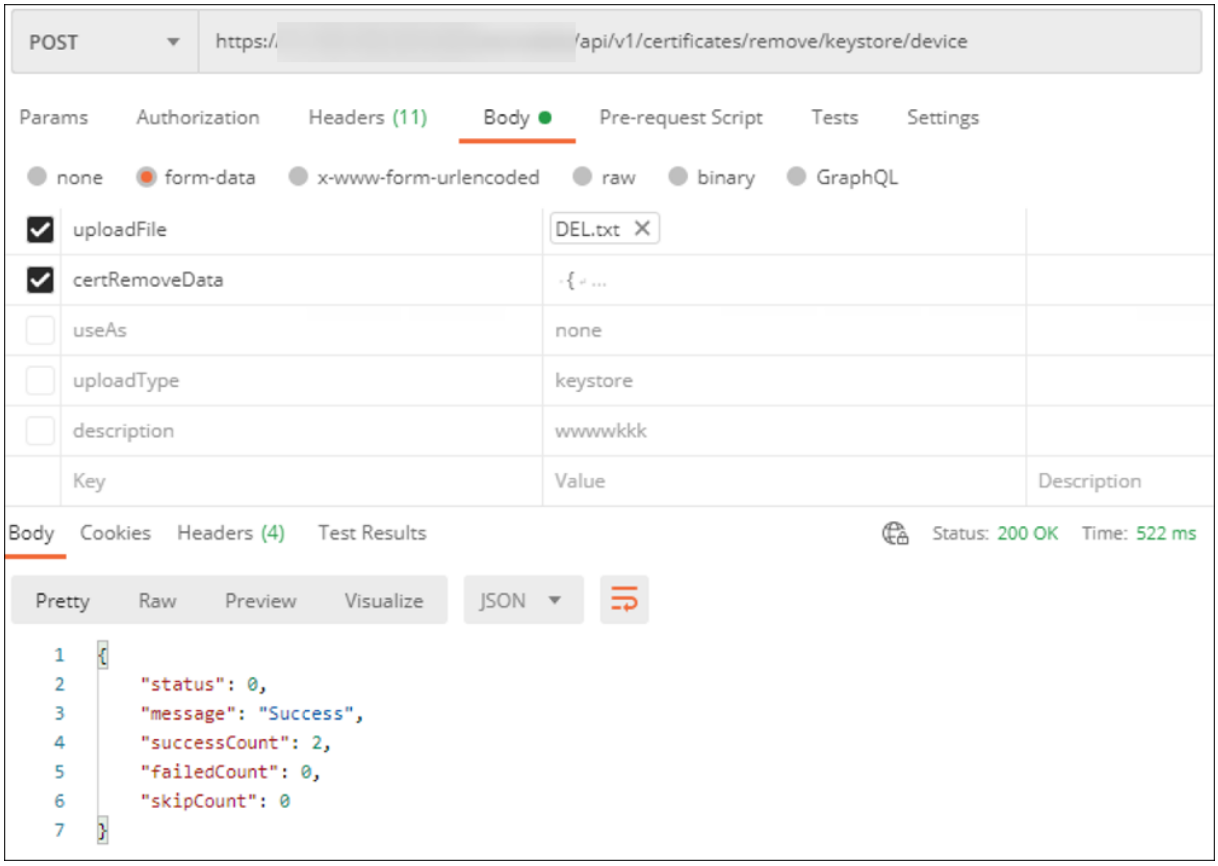


Vous pouvez également supprimer des certificats de façon groupée en créant un fichier texte avec la valeur `device_identity_value` répertoriée pour chaque certificat à supprimer. Dans l'API REST, appelez l'API delete et utilisez la requête suivante, en remplaçant `device_identity_value` par l'identifiant approprié :

```
```
{

    "identityType"="device_identity_value"
 }

<!--NeedCopy--> ```
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 
```



Mettre à jour un certificat

Citrix Endpoint Management n'autorise l'existence que d'un seul certificat par clé publique dans le système à tout moment. Si vous essayez d'importer un certificat pour la même paire de clés qu'un certificat déjà importé, vous pouvez :

- Remplacer l'entrée existante ;
- Supprimer l'entrée.

Une fois que vous avez téléchargé un nouveau certificat pour remplacer un ancien certificat, vous ne pouvez pas supprimer l'ancien certificat. Lorsque vous configurez le paramètre Entités PKI, les deux certificats existent dans le menu **Certificat SSL**. Le certificat le plus récent apparaît dans une position plus basse dans la liste que l'ancien certificat.

Pour mettre à jour vos certificats

1. Créez un certificat de remplacement en suivant les étapes de l'authentification certificat client ou certificat + domaine.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Important :**
>
> N'utilisez pas cette option pour créer un certificat avec la clé privée existante. Lorsque vous créez un certificat pour mettre à jour un certificat qui arrive à expiration, vous devez également utiliser une nouvelle clé privée.

2. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. Utilisez la barre de recherche pour rechercher et ouvrir le paramètre **Certificats**.
3. Dans la boîte de dialogue **Importer**, importez le nouveau certificat.

Lorsque vous mettez un certificat de serveur à jour, les composants qui utilisaient le certificat précédent utilisent automatiquement le nouveau certificat. De même, si vous avez déployé le certificat de serveur sur les appareils, il sera automatiquement mis à jour lors du prochain déploiement.

Pour renouveler un certificat APNs, procédez comme suit pour créer un certificat, puis accédez au portail Apple Push Certificates Portal. Pour de plus amples informations, consultez la section Renouveler un certificat APNS.

Si NetScaler Gateway est configuré pour la décharge SSL, assurez-vous de mettre à jour l'équilibrage de charge avec le nouveau certificat cacert.perm.

> **Remarque :**
>
> si vous avez migré de XenMobile sur site vers Citrix Endpoint Management et que vous mettez à jour votre certificat, contactez le support Citrix après avoir effectué les étapes précédentes. Vous devez leur fournir une copie du nouveau certificat (au format PFX), y compris le mot de passe du certificat. Le support Citrix mettra à jour NetScaler dans le cloud et redémarrera les nœuds cents pour finaliser le processus de mise à jour des certificats.

Pour mettre à jour une autorité de certification d'infrastructure de clé publique

Vous pouvez demander que Citrix Cloud Operations actualise ou régénère les autorités de certification d'infrastructure de clé publique interne dans votre déploiement Citrix Endpoint Management. Ouvrez un dossier d'assistance technique pour ces demandes.

```
When the new CAs are available, Cloud Operations lets you know that you
    can proceed with renewing the device certificates for your users.
```

Renouveler les certificats d'appareil

Si un certificat expire sur un appareil, il n'est plus valide. Vous ne pouvez plus exécuter de transactions sécurisées dans votre environnement et vous ne pouvez pas accéder aux ressources Citrix Endpoint

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Management. L'autorité de certification (CA) vous invite à renouveler votre certificat SSL avant la date d'expiration. Suivez les étapes décrites précédemment pour mettre à jour le certificat, puis lancez un renouvellement de certificat sur les appareils inscrits.

Pour les appareils iOS, macOS et Android pris en charge, vous pouvez lancer le renouvellement des certificats via l'action de sécurité Renouvellement de certificat. Vous renouvelez les certificats des appareils à partir de la console Citrix Endpoint Management ou de l'API REST publique. Pour les appareils Windows inscrits, les utilisateurs doivent réinscrire leurs appareils pour recevoir une nouvelle autorité de certification d'appareil.

Lors de la prochaine connexion d'appareils à Citrix Endpoint Management, Citrix Endpoint Management Server émet de nouveaux certificats d'appareils basés sur la nouvelle autorité de certification.

Pour renouveler les certificats d'appareils à l'aide de la console

1. Accédez à **Gérer > Appareils** et sélectionnez les appareils pour lesquels vous souhaitez renouveler les certificats.
2. Cliquez sur **Sécuriser**, puis cliquez sur **Renouvellement de certificat**.

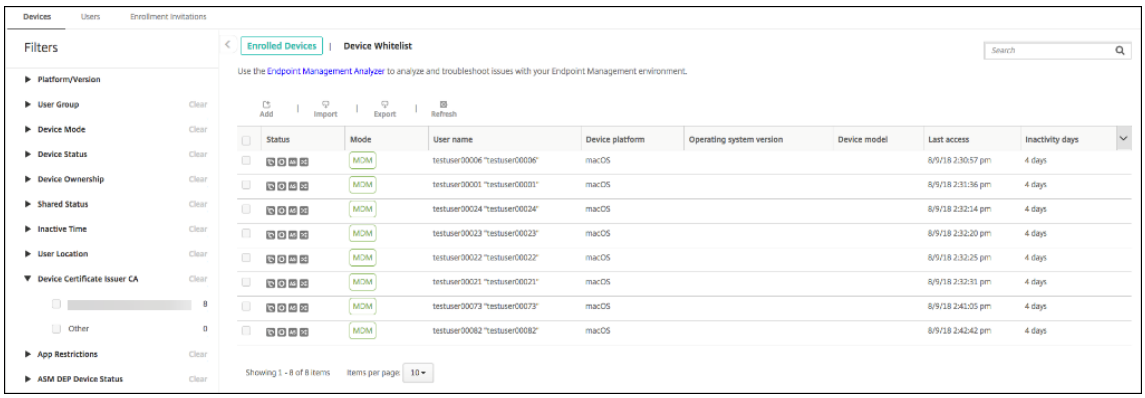
   Les appareils inscrits continuent de fonctionner sans interruption. Citrix Endpoint Management émet un certificat d'appareil lorsqu'un appareil se reconnecte au serveur.

Pour interroger les appareils appartenant à un groupe d'AC émettrice de certificat d'appareil spécifique, procédez comme suit :

1. Dans **Gérer > Appareils**, développez le panneau **Filtres**.
2. Dans le panneau **Filtres**, développez **AC émettrice du certificat d'appareil**, puis sélectionnez les autorités de certification émettrices que vous souhaitez renouveler.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dans le tableau des appareils, les appareils associés aux AC émettrices sélectionnées apparaissent.



Pour renouveler les certificats d'appareils à l'aide de l'API REST

Citrix Endpoint Management utilise les autorités de certification suivantes en interne pour l'infrastructure de clé publique (PKI) : autorité de certification racine, autorité de certification d'appareil et autorité de certification de serveur. Ces autorités de certification sont classées en tant que groupe logique et reçoivent un nom de groupe. Lors du provisioning de Citrix Endpoint Management, le serveur génère trois autorités de certification et leur attribue le nom de groupe "default".

Les API suivantes pour gérer et renouveler les certificats d'appareils sont émises par les autorités de certification. Les appareils déjà inscrits continuent de fonctionner sans interruption. Citrix Endpoint Management émet un certificat d'appareil lorsqu'un appareil se reconnecte au serveur. Pour plus d'informations, téléchargez le PDF API publique pour services REST.

- Renvoyer la liste des appareils utilisant toujours l'ancienne autorité de certification (voir la section 3.16.2 dans le PDF Public API for REST Services)
- Renouveler le certificat de l'appareil (voir la section 3.16.58)
- Obtenir tous les groupes d'autorité de certification (voir section 3.23.1)

Certificat APNS pour Citrix Secure Mail

Certificats Apple Push Notification Service (APNs) Veillez à créer un certificat SSL APNs et à le mettre à jour dans le portail Citrix avant l'expiration du certificat. Si le certificat expire, les utilisateurs rencontrent des problèmes avec les notifications push Citrix Secure Mail. De plus, vous ne pouvez plus envoyer de notifications push pour vos applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Certificat APNS pour la gestion des appareils iOS

Pour inscrire et gérer des appareils iOS avec Citrix Endpoint Management, configurez et créez un certificat APNS Apple. Si le certificat expire, les utilisateurs ne peuvent pas s'inscrire dans Citrix Endpoint Management et vous ne pouvez pas gérer leurs appareils iOS. Pour plus d'informations, consultez la section Certificats APNS.

Vous pouvez afficher l'état et la date d'expiration du certificat APNs en ouvrant une session sur le portail de certificats push Apple. Veillez à ouvrir une session avec les informations de l'utilisateur qui a créé le certificat.

Vous recevez également une notification par e-mail d'Apple 30 et 10 jours avant la date d'expiration. La notification inclut les informations suivantes :

```
1 The following Apple Push Notification Service certificate, created for
     Apple ID CustomerID will expire on Date. Revoking or allowing this
     certificate to expire will require existing devices to be re-
     enrolled with a new push certificate.
2
3 Please contact your vendor to generate a new request (a signed CSR),
     then visit https://identity.apple.com/pushcert to renew your Apple
     Push Notification Service certificate.
4
5 Thank You,
6
7 Apple Push Notification Service
8 <!--NeedCopy-->
```

MDX Toolkit (certificat de distribution iOS)

Toute application exécutée sur un appareil iOS physique (autres que des applications dans l'App Store d'Apple) présente les exigences de signature suivantes :

- Signer l'application avec un profil de provisioning.
- Signer l'application avec un certificat de distribution correspondant.

Pour vérifier que vous disposez d'un certificat de distribution iOS valide, procédez comme suit :

1. À partir du portail Apple Enterprise Developer, créez un ID d'application explicite pour chaque application que vous voulez encapsuler avec MDX. Exemple d'ID d'application acceptable : `com.CompanyName.ProductName`.
2. À partir du portail Apple Enterprise Developer, accédez à **Provisioning Profiles > Distribution** et créez un profil de provisioning interne. Répétez cette étape pour chaque ID d'application créé à l'étape précédente.
3. Téléchargez tous les profils de provisioning. Pour plus d'informations, consultez la section Encapsulation des applications mobiles iOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour vérifier si tous les certificats du serveur Citrix Endpoint Management sont valides, procédez comme suit :

1. Dans la console Citrix Endpoint Management, cliquez sur **Paramètres > Certificats**.
2. Assurez-vous que tous les certificats y compris les certificats APNs, d'écoute SSL, racine et intermédiaire sont valides.

Keystore Android

Le keystore est un fichier qui contient les certificats utilisés pour signer votre application Android. Lorsque la période de validité de votre clé expire, les utilisateurs ne peuvent plus mettre à niveau vers les nouvelles versions de votre application.

NetScaler Gateway

Pour plus d'informations sur la gestion de l'expiration de certificat pour NetScaler Gateway, consultez la section How to handle certificate expiry on NetScaler dans le centre de connaissances du support Citrix.

Un certificat NetScaler Gateway ayant expiré empêche les utilisateurs de s'inscrire et d'accéder au magasin. Le certificat expiré empêche également les utilisateurs de se connecter à Exchange Server lors de l'utilisation de Citrix Secure Mail. En outre, les utilisateurs ne peuvent pas énumérer ni ouvrir les applications HDX (en fonction de quel certificat a expiré).

Le Moniteur d'expiration et Command Center peuvent vous aider à effectuer le suivi de vos certificats NetScaler Gateway. Le Command Center vous informe de l'expiration du certificat. Ces outils permettent de surveiller les certificats NetScaler Gateway suivants :

- Certificat SSL pour nom de domaine complet MDM
- Certificat SSL pour nom de domaine complet Gateway
- Certificat SSL pour nom de domaine complet ShareFile SZC
- Certificat SSL pour l'équilibrage de charge Exchange (configuration de déchargement)
- Certificat SSL pour l'équilibrage de charge StoreFront
- Certificats d'autorité de certification racine et intermédiaire pour les certificats ci-dessus

NetScaler Gateway et Citrix Endpoint Management

March 1, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Lorsqu'il est intégré à Citrix Endpoint Management, NetScaler Gateway fournit un accès à distance à votre réseau interne et à vos ressources. Citrix Endpoint Management crée un micro VPN depuis les applications vers NetScaler Gateway sur l'appareil.

Vous pouvez utiliser le service Citrix Gateway (version préliminaire) ou une instance NetScaler Gateway locale, également appelée NetScaler Gateway. Pour obtenir une vue d'ensemble des deux solutions NetScaler Gateway, voir Configurer l'utilisation de NetScaler Gateway avec Citrix Endpoint Management.

Configurer l'authentification pour un accès à distance au réseau interne

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Serveur**, cliquez sur **NetScaler Gateway**. La page **NetScaler Gateway** s'affiche. Dans l'exemple suivant, il existe une instance NetScaler Gateway.

	Name	Default	External URL	Logon Type	# of Callback URLs
☑	testNS	✓	https://testns.domain.com	Domain	0

3. Pour configurer ces paramètres :
   - **Authentification :** sélectionnez cette option pour activer l'authentification. La valeur par défaut est **Activé**.
   - **Délivrer un certificat utilisateur pour l'authentification :** indiquez si vous voulez que Citrix Endpoint Management partage le certificat d'authentification avec Citrix Secure Hub. Le partage du certificat permet à NetScaler Gateway de gérer l'authentification du certificat client. La valeur par défaut est **Désactivé**.
   - **Fournisseur d'identités :** dans la liste, cliquez sur le fournisseur d'identités. Pour de plus amples informations, consultez la section Fournisseurs d'identités.
4. Cliquez sur **Enregistrer**.

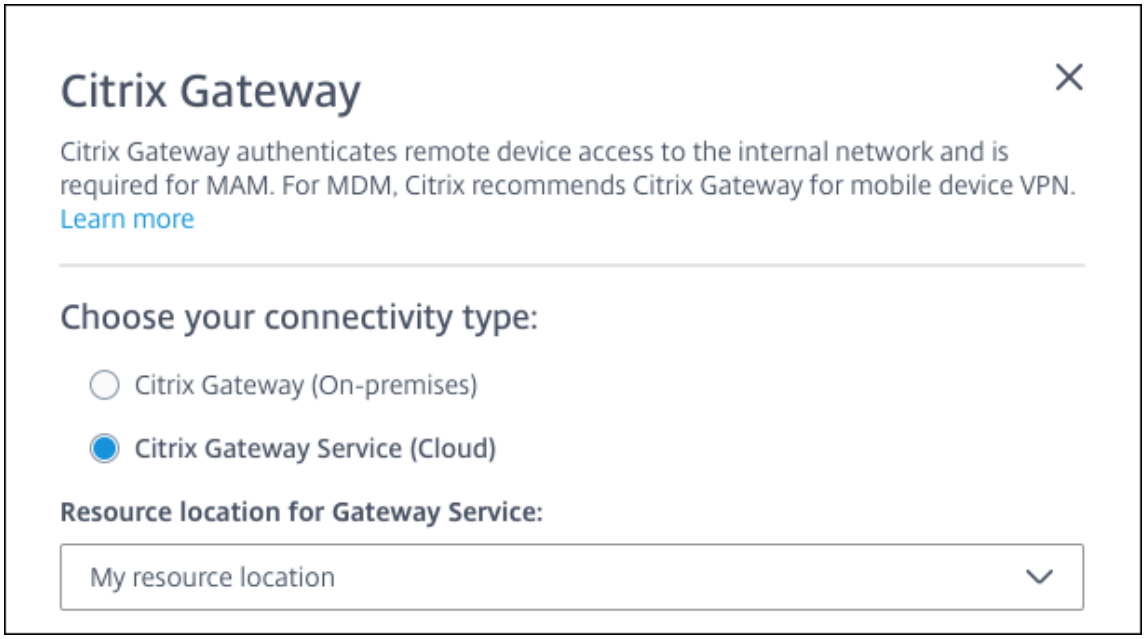
Ajouter une instance de service Citrix Gateway (version préliminaire)

Après avoir enregistré les paramètres d'authentification, vous ajoutez une instance NetScaler Gateway à Citrix Endpoint Management.

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'ouvre.
2. Sur la page **Paramètres**, faites défiler l'affichage jusqu'à la vignette NetScaler Gateway, puis cliquez sur **Démarrer la configuration**. La page **NetScaler Gateway** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Sélectionnez **Citrix Gateway Service (Cloud)** et spécifiez l'emplacement des ressources pour le service Gateway.



   - **Emplacement de ressources pour Citrix Gateway :** est requis si vous utilisez Citrix Secure Mail. Spécifiez l'emplacement des ressources pour le service STA. L'emplacement des ressources doit inclure une passerelle NetScaler Gateway configurée. Si vous devez ultérieurement supprimer un emplacement de ressources configuré pour le service Gateway, mettez ce paramètre à jour.

   Une fois ces paramètres terminés, cliquez sur **Connecter** pour établir la connexion. Le nouveau NetScaler Gateway est ajouté. La vignette **Citrix Gateway Service (Cloud)** apparaît sur la page **Paramètres**. Pour modifier une instance, cliquez sur **Voir plus**. Si des Gateway Connector ne sont pas disponibles dans l'emplacement de ressources sélectionné, cliquez sur **Ajouter Gateway Connector**. Suivez les instructions à l'écran pour installer les Gateway Connector. Vous pouvez également ajouter des Gateway Connector ultérieurement.

4. Cliquez sur **Enregistrer et exporter le script**.

   - **Enregistrer et exporter le script**. Cliquez sur le bouton pour enregistrer vos paramètres et exporter un bundle de configuration. Vous pouvez charger un script à partir du bundle vers NetScaler Gateway pour le configurer avec les paramètres de Citrix Endpoint Management. Pour plus d'informations, consultez « Configurer NetScaler Gateway pour une utilisation avec Citrix Endpoint Management » après cette procédure.

   Vous avez ajouté le nouveau NetScaler Gateway. La vignette **NetScaler Gateway** apparaît sur la page **Paramètres**. Pour modifier une instance, cliquez sur **Voir plus**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer un NetScaler Gateway sur site à utiliser avec Citrix Endpoint Management

Pour configurer une instance NetScaler Gateway locale pour une utilisation avec Citrix Endpoint Management, vous devez effectuer les étapes générales suivantes, détaillées dans les sections suivantes.

1. Vérifiez que votre environnement répond à la configuration requise.
2. Exportez le bundle de script à partir de la console Citrix Endpoint Management.
3. Extrayez les fichiers du bundle. Si vous utilisez uniquement des stratégies classiques sur NetScaler Gateway et que vous exécutez Citrix ADC 13.0 ou version antérieure, utilisez le script avec « Classic » dans le nom du fichier. Si vous utilisez des stratégies avancées ou si vous exécutez Citrix ADC 13.1 ou version ultérieure, utilisez le script avec « Advanced » dans le nom du fichier.
4. Exécutez le script approprié sur NetScaler Gateway. Pour plus d'informations, consultez le fichier Lisez-moi accompagnant les scripts pour accéder aux instructions détaillées les plus récentes.
5. Testez la configuration.

Les scripts configurent les paramètres NetScaler Gateway suivants requis par Citrix Endpoint Management :

- Serveurs virtuels NetScaler Gateway requis pour le mode MDM et MAM
- Stratégies de session pour les serveurs virtuels NetScaler Gateway
- Détails du serveur Citrix Endpoint Management
- Équilibrage de charge du proxy pour la validation du certificat
- Stratégies d'authentification et Actions pour le serveur virtuel NetScaler Gateway. Les scripts décrivent les paramètres de configuration LDAP.
- Actions et stratégies de trafic pour le serveur proxy
- Profil d'accès sans client
- Enregistrement DNS local statique sur NetScaler Gateway
- Autres liaisons : stratégie de service, certificat d'autorité de certification

Les scripts ne prennent pas en charge la configuration suivante :

- Équilibrage de charge Exchange
- Equilibrage de charge Citrix Files
- Configuration du proxy ICA
- Déchargement SSL

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Conditions préalables à l'utilisation des scripts de configuration de NetScaler Gateway

Configuration requise pour Citrix Endpoint Management :

- Effectuez la configuration LDAP et NetScaler Gateway dans Citrix Endpoint Management avant d'exporter le bundle de scripts. Si vous modifiez les paramètres, exportez à nouveau le bundle de scripts.

Configuration requise pour NetScaler Gateway :

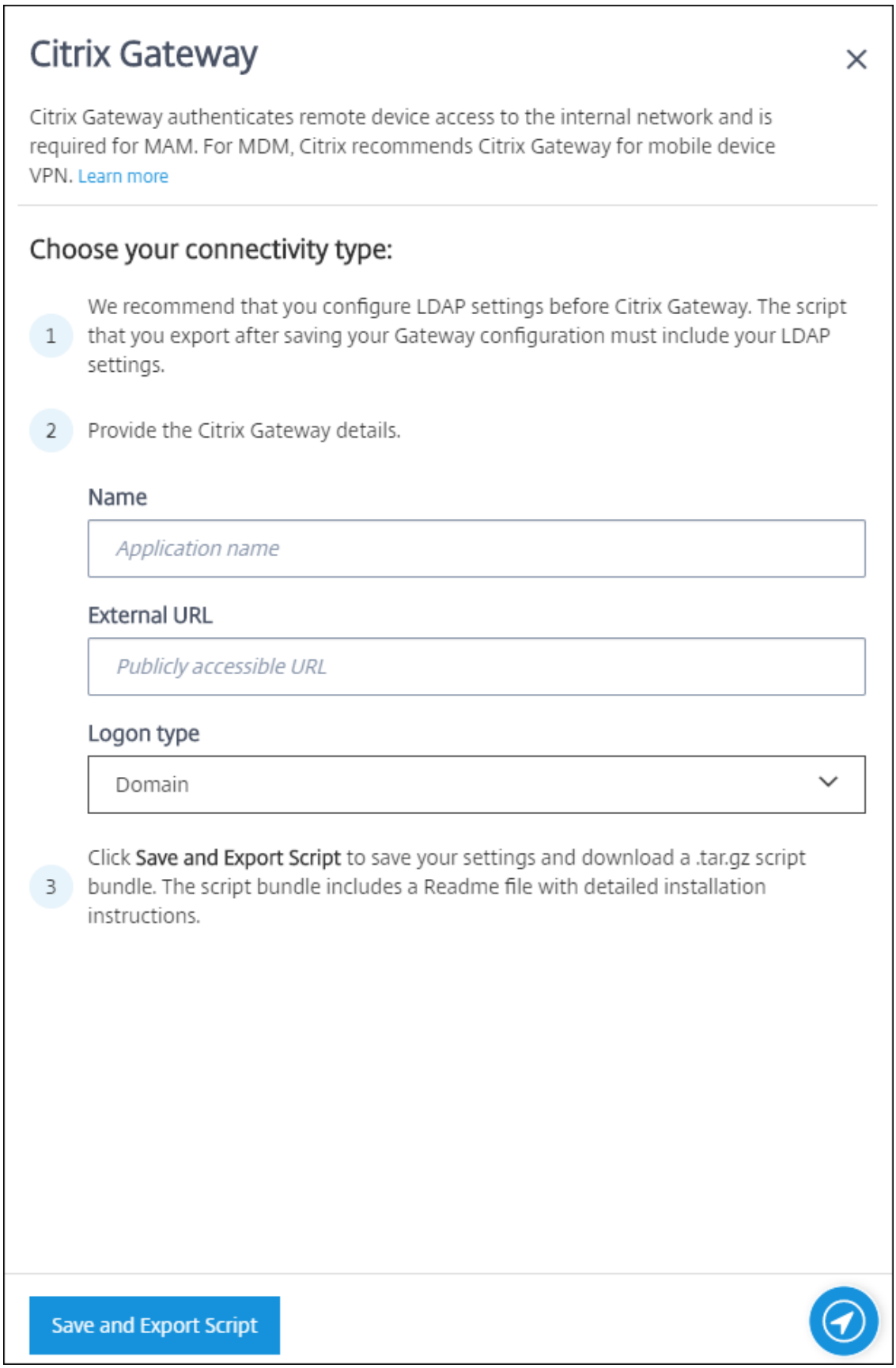
- Lorsque vous utilisez l'authentification basée sur les certificats sur NetScaler Gateway, vous devez créer des certificats SSL sur une appliance Citrix ADC. Voir Créer et utiliser des certificats SSL sur une appliance Citrix ADC.
- NetScaler Gateway (version minimum 11.0, Build 70.12).
- L'adresse IP NetScaler de Gateway est configurée et peut se connecter au serveur LDAP, à moins d'un équilibrage de charge de LDAP.
- L'adresse IP de sous-réseau de NetScaler Gateway (SNIP) est configurée, peut se connecter aux serveurs back-end nécessaires et dispose d'un accès réseau public sur le port 8443/TCP.
- DNS peut résoudre les domaines publics.
- NetScaler Gateway est utilisé sous licence Platform/Universal ou d'évaluation. Pour de plus amples informations, consultez https://support.citrix.com/article/CTX126049.

Exporter le bundle de script à partir de Citrix Endpoint Management

Après avoir enregistré les paramètres d'authentification, vous ajoutez une instance NetScaler Gateway à Citrix Endpoint Management.

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'ouvre.
2. Sur la page **Paramètres**, faites défiler l'affichage jusqu'à la vignette NetScaler Gateway, puis cliquez sur **Démarrer la configuration**. La page **NetScaler Gateway** s'affiche.
3. Sélectionnez **NetScaler Gateway (local)** et configurez les paramètres suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Nom :** entrez un nom pour l'instance NetScaler Gateway.
- **URL externe :** entrez l'adresse URL publiquement accessible de NetScaler Gateway. Par exemple, `https://receiver.com`.
- **Type d'ouverture de session :** choisissez un type d'ouverture de session. Les types disponibles sont les suivants : **Domaine**, **Jeton de sécurité uniquement**, **Domaine et jeton de sécurité**, **Certificat**, **Certificat et domaine** et **Certificat et jeton de sécurité**. La valeur par défaut est **Domaine**.

Si vous disposez de plusieurs domaines, utilisez **Certificat et domaine**. Pour plus d'informations, consultez Configuration de l'authentification multi-domaines.

L'authentification basée sur les certificats sur NetScaler Gateway nécessite une configuration supplémentaire. Par exemple, vous devez charger votre certificat d'autorité de certification racine sur votre appliance Citrix ADC. Voir Créer et utiliser des certificats SSL sur une appliance Citrix ADC.

Pour plus d'informations, consultez la section Authentification dans le manuel de déploiement.

4. Cliquez sur **Enregistrer et exporter le script**.

   - **Enregistrer et exporter le script**. Cliquez sur le bouton pour enregistrer vos paramètres et exporter un bundle de configuration. Vous pouvez charger un script à partir du bundle vers NetScaler Gateway pour le configurer avec les paramètres de Citrix Endpoint Management. Pour plus d'informations, consultez « Configurer NetScaler Gateway pour une utilisation avec Citrix Endpoint Management » après cette procédure.

   Vous avez ajouté le nouveau NetScaler Gateway. La vignette **NetScaler Gateway** apparaît sur la page **Paramètres**. Pour modifier une instance, cliquez sur **Voir plus**.

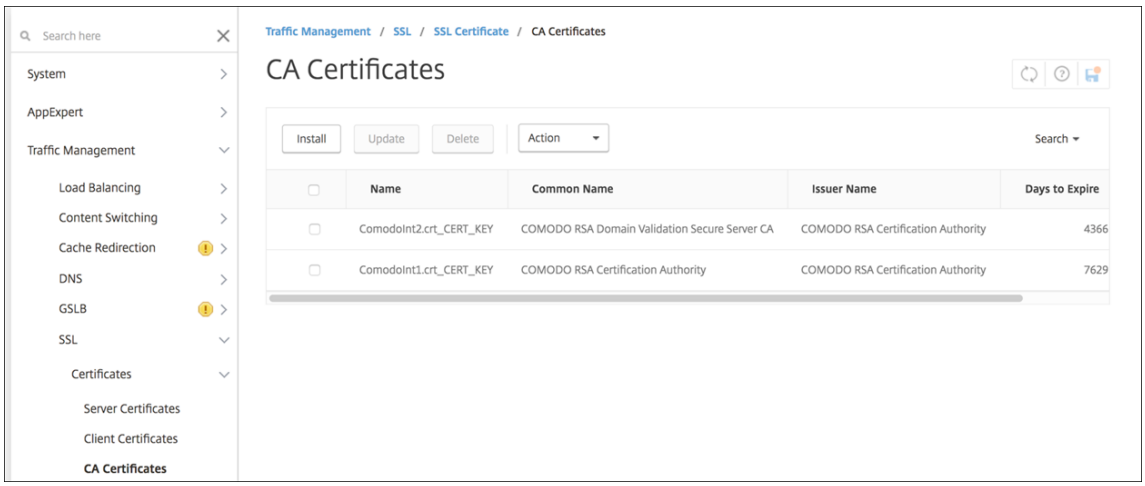
Installez le script dans votre environnement

Le bundle de scripts comprend ce qui suit.

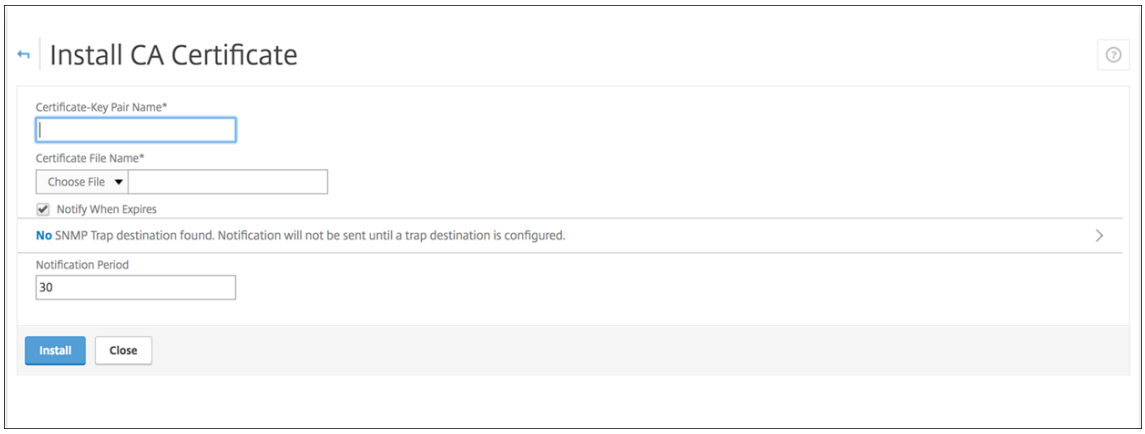
- Fichier Lisez-moi avec instructions détaillées
- Scripts contenant les commandes d'interface de ligne de commande NetScaler permettant de configurer les composants requis dans NetScaler
- Certificat d'autorité de certification racine public et certificat d'autorité de certification intermédiaire
- Scripts contenant les commandes d'interface de ligne de commande NetScaler permettant de supprimer la configuration de NetScaler

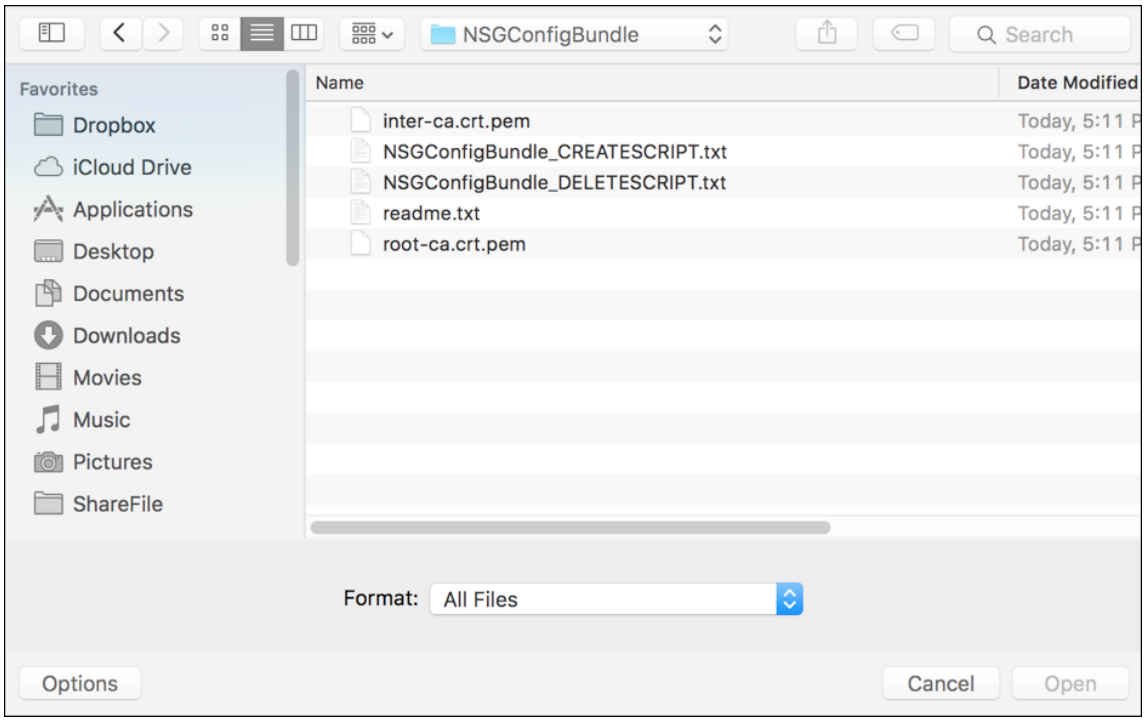
1. Chargez et installez les fichiers de certificat (fournis dans le bundle de script) sur le boîtier Citrix ADC sur le répertoire /nsconfig/ssl/. Voir Créer et utiliser des certificats SSL sur une appliance Citrix ADC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

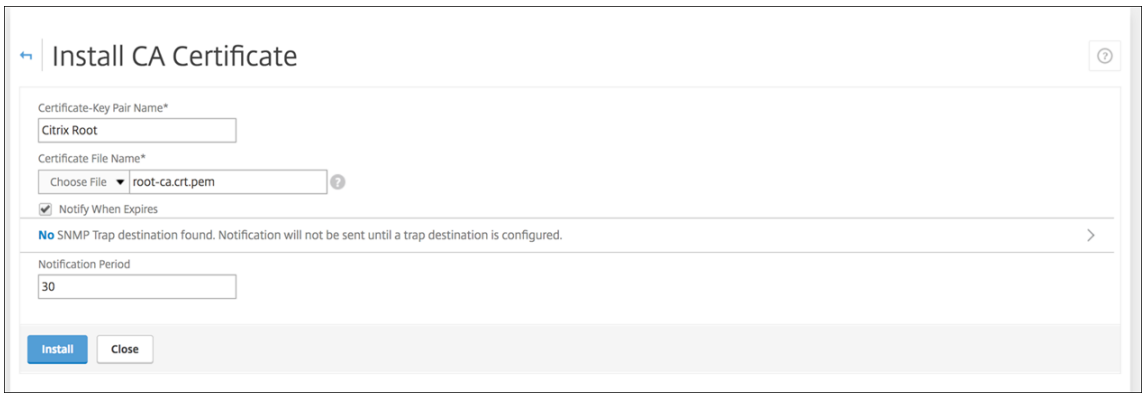


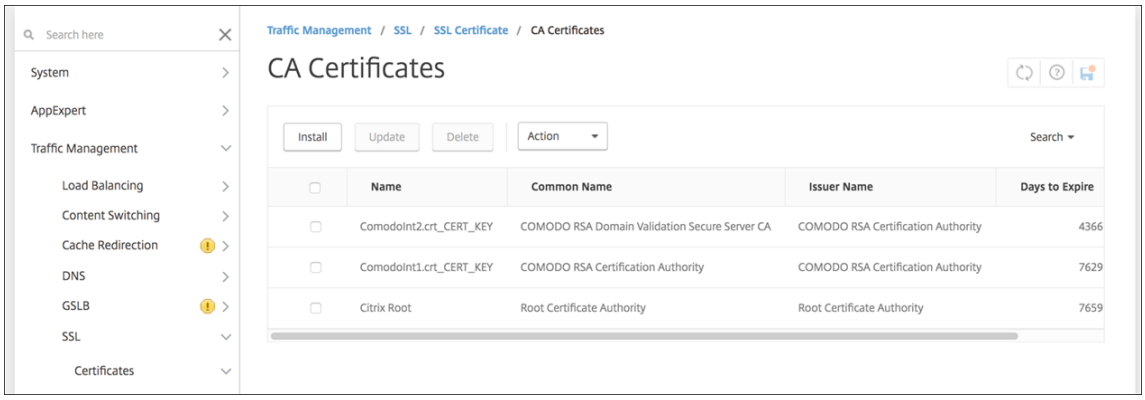
Les exemples suivants expliquent comment installer le certificat racine.





© 1999–2024 Cloud Software Group, Inc. All rights reserved.





Assurez-vous que vous installez à la fois les certificats racine et intermédiaire.

2. Modifiez le script (ConfigureCitrixGatewayScript_Classic.txt ou ConfigureCitrixGatewayScript_Advanced.txt) pour remplacer tous les espaces réservés par des détails de votre environnement.

```
#Important Note: Please update the following placeholders with valid values:
# <NSG_IP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reachable from your devices either directly or via a
NAT.
# <PROXY_LB_VIP> -- Virtual IP Address to be assigned to the proxy load-balancer configured on the NetScaler. This IP address must be a private address.
# <LDAP_SVC_USERNAME> -- LDAP Service Account Username.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <SERVER_CERT_NAME> -- Name of the server certificate file on the NetScaler. This certificate is bound to the NetScaler Gateway virtual server.
```

3. Exécutez le script modifié dans le shell bash NetScaler, comme décrit dans le fichier Lisez-moi accompagnant le bundle de script. Par exemple :

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler
Management Password> batch -f "/var/OfflineNSGConfigtBundle_CREATESCRIPT
.txt"
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
login as: nsroot
##############################################################################
#                                                                            #
#        WARNING: Access to this system is for authorized users only         #
#         Disconnect IMMEDIATELY if you are not an authorized user!          #
#                                                                            #
##############################################################################

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

Lorsque le script prend fin, les lignes suivantes s'affichent.

```
exec: save ns config
 Done
 Done
root@ns#
```

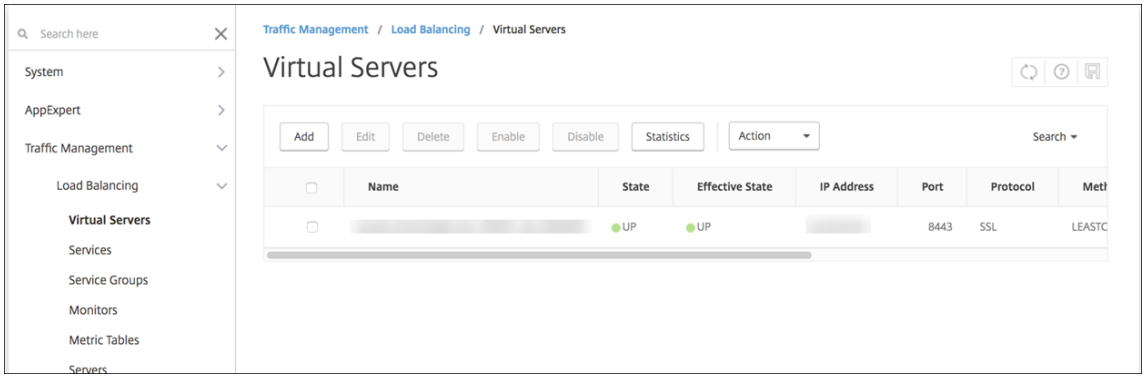
Tester la configuration

Pour valider la configuration :

1. Vérifiez que le serveur virtuel NetScaler Gateway affiche un état **Actif**.

2. Vérifiez que le serveur virtuel d'équilibrage de charge du proxy indique un état **Actif**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Ouvrez un navigateur Web, connectez-vous à l'adresse URL de NetScaler Gateway et essayez de vous authentifier. Si l'authentification réussit, vous serez redirigé vers un message « État HTTP 404 - Introuvable. »
4. Inscrivez un appareil et assurez-vous qu'il est inscrit auprès de MDM et MAM.

Configuration de l'authentification multi-domaines

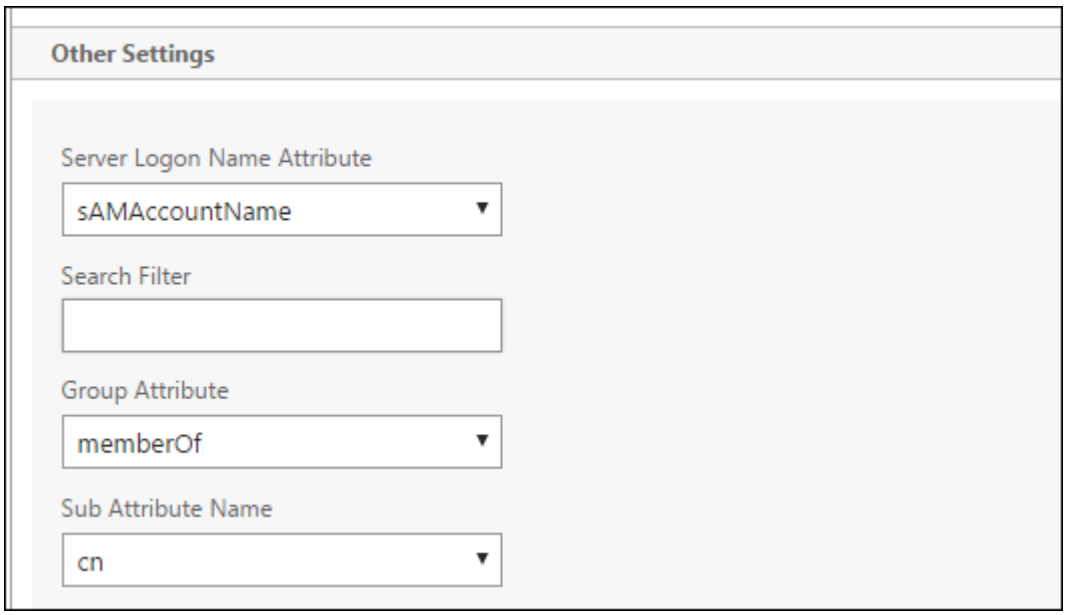
Si vous disposez de plusieurs instances Citrix Endpoint Management, telles que les environnements de test, de développement et de production, vous devez configurer manuellement NetScaler Gateway pour les environnements supplémentaires. Vous ne pouvez exécuter l'assistant NetScaler pour XenMobile qu'une seule fois.

Configuration de NetScaler Gateway

Pour configurer les stratégies d'authentification NetScaler Gateway et une stratégie de session pour un environnement multi-domaine :

1. Dans l'onglet **Configuration** de l'outil de configuration NetScaler Gateway, développez **NetScaler Gateway > Policies > Authentication**.
2. Dans le panneau de navigation, cliquez sur **LDAP**.
3. Cliquez pour modifier le profil LDAP. Définissez **Server Logon Name Attribute** sur **userPrincipalName** ou sur l'attribut que vous souhaitez utiliser pour vos recherches. Prenez note de l'attribut que vous spécifiez. Vous devez le fournir lorsque vous configurez les paramètres LDAP dans la console Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

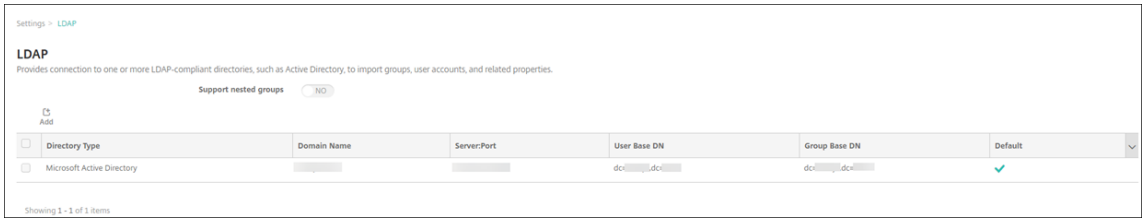


4. Répétez ces étapes pour chaque stratégie LDAP. Une stratégie LDAP distincte est requise pour chaque domaine.
5. Dans la stratégie de session liée au serveur virtuel NetScaler Gateway, accédez à **Edit session profile > Published Applications**. Assurez-vous que le champ **Single Sign-On Domain** est vide.

Configuration de Citrix Endpoint Management

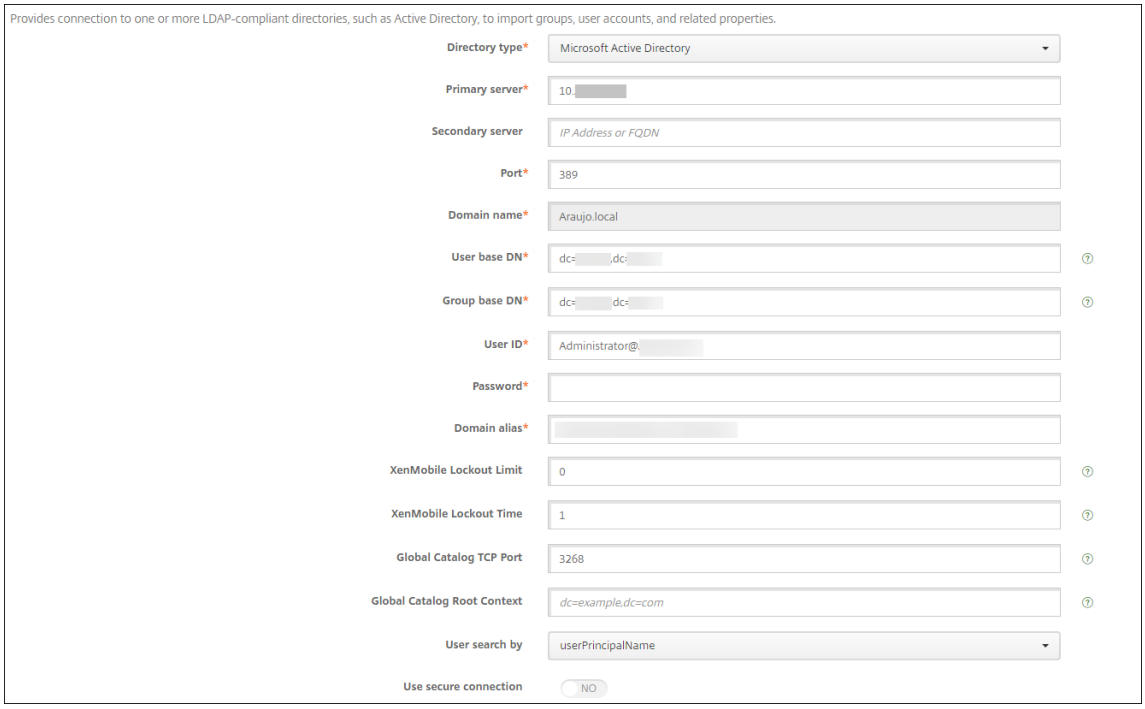
Pour configurer les paramètres LDAP de Citrix Endpoint Management pour un environnement multi-domaine :

1. Dans la console Citrix Endpoint Management, accédez à **Settings > LDAP** et ajoutez ou modifiez un répertoire.



2. Entrez les informations.
   - Sous **Alias de domaine**, spécifiez chaque domaine à utiliser pour l'authentification utilisateur. Séparez les domaines avec une virgule et n'insérez pas d'espaces entre les domaines. Par exemple : domain1.com,domain2.com,domain3.com
   - Assurez-vous que le champ **User search by** correspond à l'attribut **Server Logon Name Attribute** spécifié dans la stratégie LDAP NetScaler Gateway.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Supprimer les demandes de connexion entrante vers des adresses URL spécifiques

Dans votre environnement, si NetScaler Gateway est configuré pour le déchargement SSL, vous pouvez souhaiter que la passerelle supprime les demandes de connexion entrante pour des adresses URL spécifiques. Si vous préférez une sécurité supplémentaire, contactez Citrix Cloud Operations et demandez-leur d'autoriser votre adresse IP dans vos centres de données locaux.

Authentification avec domaine ou domaine + jeton de sécurité

March 1, 2024

Citrix Endpoint Management prend en charge l'authentification basée sur domaine auprès d'un ou plusieurs annuaires, qui sont compatibles avec le protocole LDAP (Lightweight Directory Access Protocol). Vous configurez une connexion dans Citrix Endpoint Management à un ou plusieurs répertoires. Citrix Endpoint Management utilise la configuration LDAP pour importer des groupes, des comptes d'utilisateurs et des propriétés associées.

> **Important :**
>
> Citrix Endpoint Management ne prend pas en charge le passage du mode d'authentification, d'un type de domaine d'authentification à un autre mode d'authentification, une fois que les

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> utilisateurs ont inscrit des appareils dans Citrix Endpoint Management. Par exemple, vous ne pouvez pas modifier le mode d'authentification de **Authentification de domaine** à **Domaine + Certificat** une fois que les utilisateurs se sont inscrits.

À propos de LDAP

LDAP est un protocole applicatif indépendant open source qui permet d'accéder et de gérer les services d'informations d'annuaire distribués sur un réseau IP (Internet Protocol). Les services d'informations d'annuaire sont utilisés pour partager des informations sur les utilisateurs, les systèmes, les réseaux, les services et les applications disponibles sur le réseau.

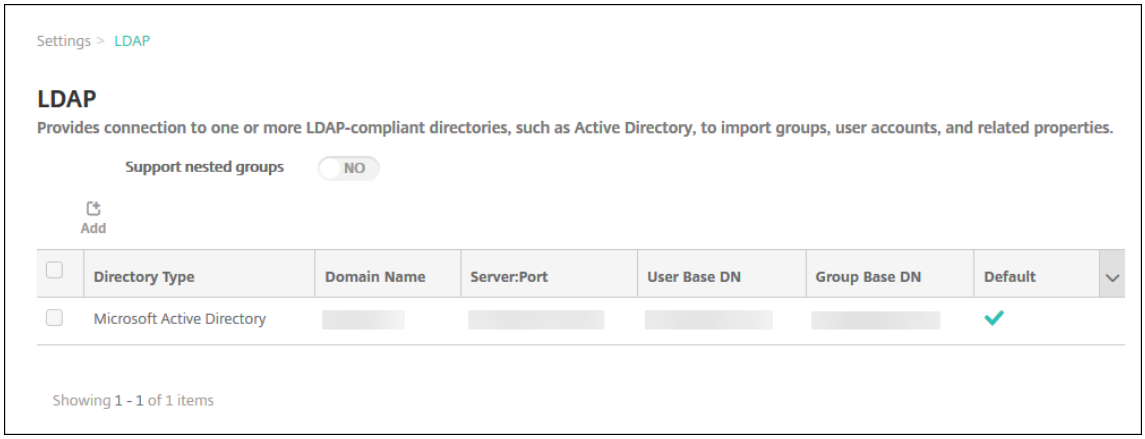
LDAP est couramment utilisé pour fournir une authentification unique (SSO) aux utilisateurs, avec laquelle un seul mot de passe (par utilisateur) est partagé entre plusieurs services. L'authentification unique permet à un utilisateur de se connecter une seule fois au site Web d'une entreprise, pour un accès authentifié à l'intranet de l'entreprise.

Un client démarre une session LDAP en se connectant à un serveur LDAP, appelé DSA (Agent système d'annuaire). Le client envoie une demande d'opération au serveur et le serveur répond avec l'authentification appropriée.

Pour ajouter ou modifier des connexions LDAP dans Citrix Endpoint Management

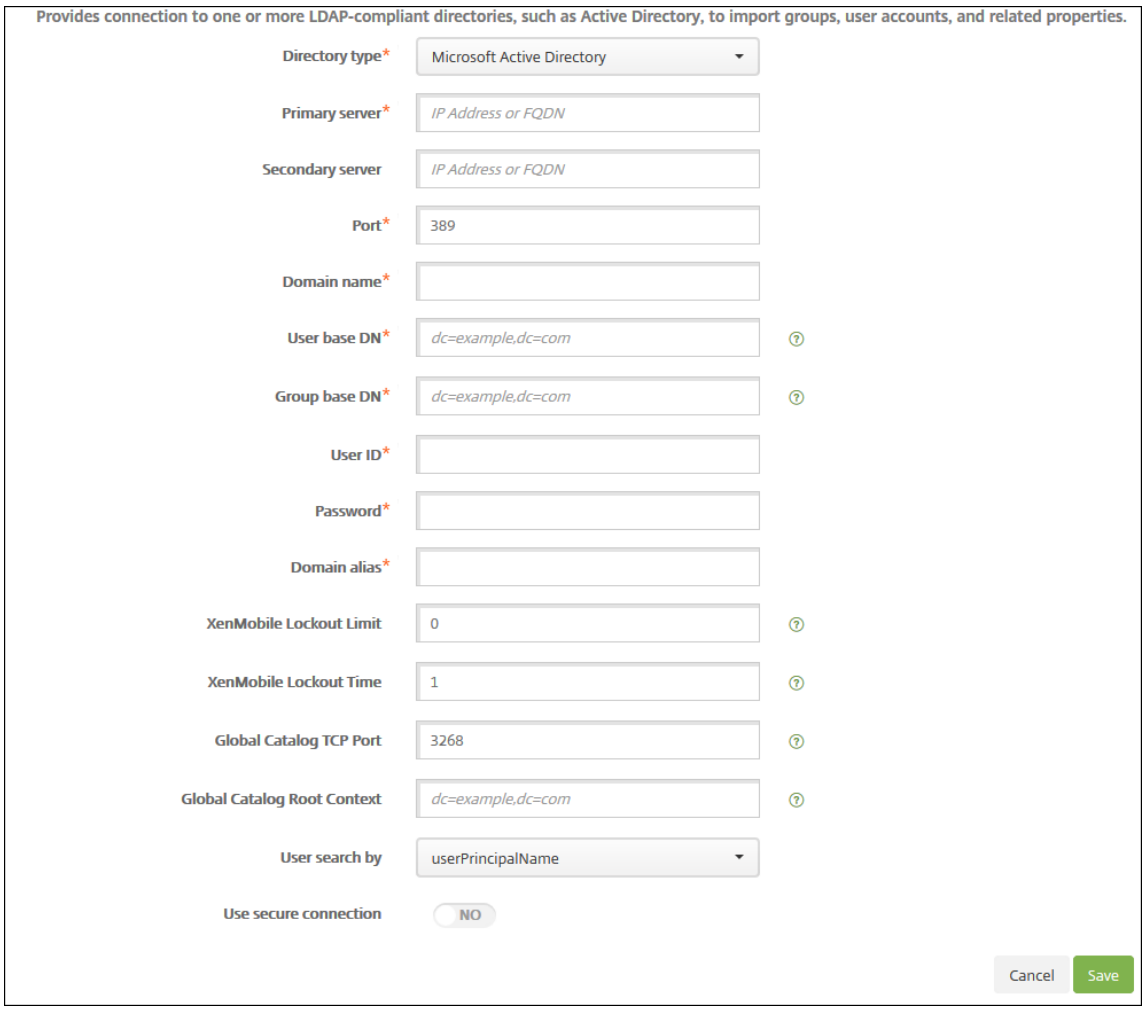
Vous configurez généralement des connexions LDAP lors de l'intégration à Citrix Endpoint Management, comme décrit à la section Pour configurer LDAP. Si vous avez procédé à l'intégration avant que les écrans affichés dans cette section ne soient disponibles, utilisez les informations de cette section pour ajouter des connexions LDAP.

1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > LDAP**.
2. Sous **Serveur**, cliquez sur **LDAP**. La page **LDAP** s'affiche.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Sur la page **LDAP**, cliquez sur **Ajouter** ou **Modifier**. La page **Ajouter un LDAP** ou **Modifier un LDAP** s'affiche.



4. Pour configurer ces paramètres :

   - **Type d'annuaire :** dans la liste, cliquez sur le type d'annuaire approprié. La valeur par défaut est **Microsoft Active Directory**.
   - **Serveur principal :** entrez le serveur principal utilisé pour LDAP ; vous pouvez entrer l'adresse IP ou le nom de domaine complet (FQDN).
   - **Serveur secondaire :** éventuellement, si un serveur secondaire a été configuré, entrez l'adresse IP ou le nom de domaine complet du serveur secondaire. Ce serveur est un serveur de basculement utilisé au cas où le serveur principal ne peut pas être contacté.
   - **Port :** entrez le numéro du port utilisé par le serveur LDAP. Par défaut, le numéro de port est défini sur **389** pour les connexions LDAP non sécurisées. Utilisez le numéro de port **636** pour les connexions LDAP sécurisées, **3268** pour les connexions LDAP non sécurisées Microsoft, ou **3269** pour les connexions LDAP sécurisées Microsoft.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Nom de domaine :** entrez le nom du domaine.
- **Nom unique de l'utilisateur de base :** entrez l'emplacement des utilisateurs dans Active Directory à l'aide d'un identificateur unique. Exemples de syntaxe : `ou=users`, `dc=example` ou `dc=com`.
- **Nom unique du groupe de base :** entrez l'emplacement des groupes dans Active Directory. Par exemple, `cn=users, dc=domain, dc=net` où `cn=users` représente le nom de conteneur des groupes et `dc` représente le composant de domaine d'Active Directory.
- **ID utilisateur :** entrez l'ID de l'utilisateur associé au compte Active Directory.
- **Mot de passe :** entrez le mot de passe associé à l'utilisateur.
- **Alias de domaine :** entrez un alias pour le nom de domaine. Si vous modifiez le paramètre **Alias de domaine** après l'inscription, les utilisateurs doivent s'inscrire à nouveau.
- **Limite de verrouillage de Citrix Endpoint Management :** entrez un nombre compris entre **0** et **999** pour le nombre d'échecs de tentatives d'ouverture de session. Si ce champ est défini sur **0**, Citrix Endpoint Management ne verrouillera jamais l'utilisateur quel que soit le nombre de tentatives d'ouverture de session infructueuses. La valeur par défaut est **0**.

  Envisagez de définir cette limite de verrouillage sur une valeur inférieure à votre stratégie de verrouillage LDAP. Cela permet d'éviter le verrouillage des utilisateurs si Citrix Endpoint Management ne parvient pas à s'authentifier auprès du serveur LDAP. Par exemple, si la stratégie de verrouillage LDAP est définie sur 5 tentatives, configurez cette limite de verrouillage sur **4** ou moins.
- **Durée de verrouillage de Citrix Endpoint Management :** entrez un nombre compris entre **0** et **99 999** représentant le nombre de minutes pendant lesquelles un utilisateur doit patienter après avoir dépassé la limite de verrouillage. Une valeur de **0** signifie que l'utilisateur n'est pas forcé d'attendre après un verrouillage. La valeur par défaut est **1**.
- **Port TCP du catalogue global :** entrez le numéro de port TCP du serveur du catalogue global. Par défaut, le numéro de port TCP est défini sur **3268** ; pour les connexions SSL, utilisez le numéro de port **3269**.
- **Base de recherche du catalogue global :** si vous le souhaitez, entrez la valeur de base de recherche globale utilisée pour activer une recherche du catalogue global dans Active Directory. Cette recherche est en supplément de la recherche LDAP standard, dans tout domaine sans avoir à spécifier le nom de domaine.
- **Recherche utilisateur par :** sélectionnez le format du nom d'utilisateur ou de l'ID utilisateur utilisé par Citrix Endpoint Management pour rechercher des utilisateurs dans ce répertoire. Les utilisateurs saisissent leur nom d'utilisateur ou leur ID d'utilisateur dans

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ce format lors de leur inscription. Si vous modifiez le paramètre **Rechercher utilisateurs par** après l'inscription, les utilisateurs doivent s'inscrire à nouveau.

Si vous choisissez **UserPrincipalName**, les utilisateurs saisissent un nom d'utilisateur principal (UPN) dans le format suivant :

- *nom d'utilisateur@domaine*

Si vous choisissez **SamAccountName**, les utilisateurs saisissent un nom SAM (Secure Account Manager) dans l'un des formats suivants :

- *nom d'utilisateur@domaine*
- *domaine\nom d'utilisateur*

- **Utiliser une connexion sécurisée :** indiquez si des connexions sécurisées doivent être utilisées. La valeur par défaut est **Non**.

5. Cliquez sur **Enregistrer**.

Pour supprimer un annuaire compatible LDAP

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

   Vous pouvez sélectionner plusieurs propriétés à supprimer en sélectionnant la case à cocher en regard de chaque propriété.

2. Cliquez sur **Delete**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer**.

Configurer l'authentification domaine + jeton de sécurité

Vous pouvez configurer Citrix Endpoint Management de manière à obliger les utilisateurs à s'authentifier avec leurs informations d'identification LDAP plus un mot de passe à usage unique, à l'aide du protocole RADIUS.

Pour une utilisabilité optimale, vous pouvez combiner cette configuration avec le code PIN Citrix et la mise en cache du mot de passe Active Directory. Avec cette configuration, les utilisateurs n'ont pas à entrer leurs noms d'utilisateur et mots de passe LDAP à plusieurs reprises. Les utilisateurs doivent entrer leurs noms et mots de passe lors de l'inscription, de l'expiration du mot de passe et du verrouillage du compte.

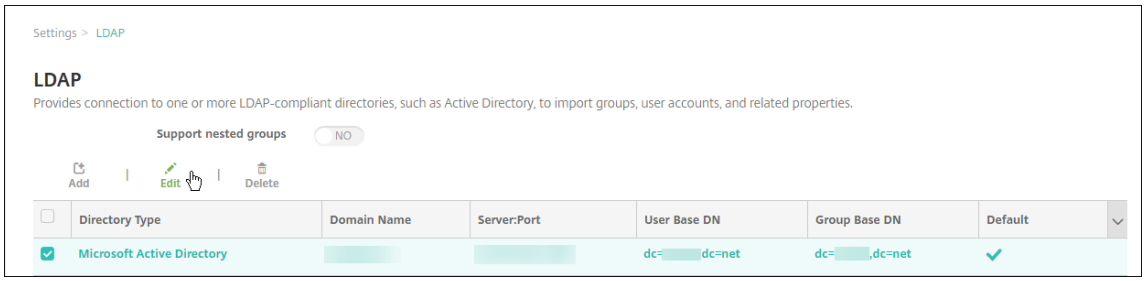
Configurer les paramètres LDAP

L'utilisation de LDAP pour l'authentification nécessite que vous installiez un certificat SSL d'une autorité de certification sur Citrix Endpoint Management. Pour de plus amples informations, consultez

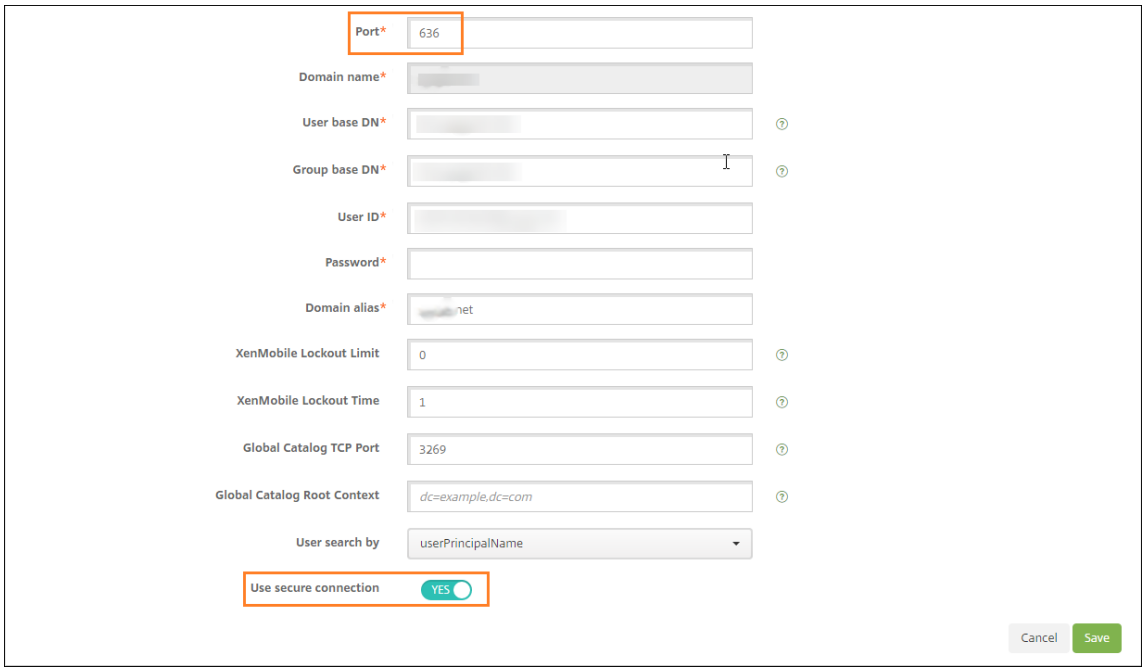
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

la section Charger des certificats.

1. Dans **Paramètres**, cliquez sur **LDAP**.
2. Sélectionnez **Microsoft Active Directory** et cliquez sur **Modifier**.



3. Vérifiez que le port Port est **636** pour les connexions LDAP sécurisées ou **3269** pour les connexions LDAP sécurisées Microsoft.
4. Changez **Utiliser une connexion sécurisée** sur **Oui**.



Configurer les paramètres de NetScaler Gateway

Les étapes suivantes supposent que vous avez déjà ajouté une instance NetScaler Gateway à Citrix Endpoint Management. Pour ajouter une instance de NetScaler Gateway, consultez NetScaler Gateway et Citrix Endpoint Management.

1. Dans **Paramètres**, cliquez sur **NetScaler Gateway**.
2. Sélectionnez le NetScaler Gateway et cliquez sur **Modifier**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Activer le code PIN Citrix et la mise en cache du mot de passe de l'utilisateur

Pour activer le code PIN Citrix et la mise en cache du mot de passe de l'utilisateur, accédez à **Paramètres > Propriétés du client** et sélectionnez ces cases : **Activer l'authentification par code PIN Citrix** et **Activer la mise en cache du mot de passe de l'utilisateur**. Pour de plus amples informations, consultez la section Propriétés du client.

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

Configurez des profils de sessions NetScaler Gateway et des stratégies pour les serveurs virtuels que vous utilisez avec Citrix Endpoint Management. Pour de plus amples informations, consultez la documentation de NetScaler Gateway.

Authentification certificat client ou certificat + domaine

March 1, 2024

La configuration par défaut pour Citrix Endpoint Management est l'authentification par nom d'utilisateur et mot de passe. Pour ajouter une autre couche de sécurité pour l'inscription et l'accès à l'environnement Citrix Endpoint Management, vous pouvez utiliser l'authentification basée sur certificats. Dans l'environnement Citrix Endpoint Management, cette configuration est la meilleure combinaison de sécurité et d'expérience utilisateur. L'authentification par certificat plus domaine offre les meilleures possibilités d'authentification unique associées à la sécurité fournie par l'authentification à deux facteurs sur NetScaler Gateway.

Pour une utilisabilité optimale, vous pouvez combiner l'authentification par certificat plus domaine avec le code PIN Citrix et la mise en cache du mot de passe Active Directory. Dans ce cas, les utilisateurs n'ont pas à entrer leurs noms d'utilisateur et mots de passe LDAP à plusieurs reprises. Les utilisateurs doivent entrer leurs noms et mots de passe lors de l'inscription, de l'expiration du mot de passe et du verrouillage du compte.

> **Important :**
>
> Citrix Endpoint Management ne prend pas en charge le passage du mode d'authentification, de l'authentification de domaine à un autre mode d'authentification, une fois que les utilisateurs ont inscrit des appareils dans Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si vous n'autorisez pas LDAP et utilisez des cartes à puce ou méthodes similaires, la configuration des certificats vous permet de représenter une carte à puce auprès de Citrix Endpoint Management. Les utilisateurs s'inscrivent alors à l'aide d'un code PIN unique généré par Citrix Endpoint Management. Une fois qu'un utilisateur a accès, Citrix Endpoint Management crée et déploie le certificat utilisé pour s'authentifier auprès de l'environnement Citrix Endpoint Management.

Vous pouvez utiliser l'assistant NetScaler pour XenMobile pour procéder à la configuration requise pour Citrix Endpoint Management lors de l'utilisation de l'authentification par certificat NetScaler Gateway ou certificat + domaine. Vous ne pouvez exécuter l'assistant NetScaler pour XenMobile qu'une seule fois.

Dans les environnements hautement sécurisés, l'utilisation d'informations d'identification LDAP en dehors d'une organisation dans des réseaux publics ou non sécurisés est considérée comme une menace de sécurité majeure pour l'entreprise. Pour les environnements hautement sécurisés, il est possible d'opter pour l'authentification à deux facteurs à l'aide d'un certificat client et d'un jeton de sécurité. Pour de plus amples informations, consultez la section Configuration de Citrix Endpoint Management pour l'authentification par certificat et jeton de sécurité.

L'authentification par certificat client est disponible pour les appareils inscrits à MAM et MDM+MAM. Pour utiliser l'authentification par certificat client pour ces appareils, vous devez configurer le serveur Microsoft, Citrix Endpoint Management et NetScaler Gateway. Suivez ces étapes générales, décrites dans cet article.

Sur le serveur Microsoft :

1. Ajoutez un composant logiciel enfichable pour les certificats dans la console Microsoft Management Console.
2. Ajoutez le modèle à l'autorité de certification (CA).
3. Créez un certificat PFX depuis le serveur CA.

Sur Citrix Endpoint Management :

1. Chargez le certificat sur Citrix Endpoint Management.
2. Créez l'entité PKI pour l'authentification par certificat.
3. Configurez les fournisseurs d'informations d'identification.
4. Configurez NetScaler Gateway afin de fournir un certificat utilisateur pour l'authentification.

Pour plus d'informations sur la configuration de NetScaler Gateway, consultez ces articles dans la documentation de Citrix ADC :

- Authentification client
- Infrastructure de profils SSL
- Configuration et liaison d'une stratégie d'authentification de certificat client.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

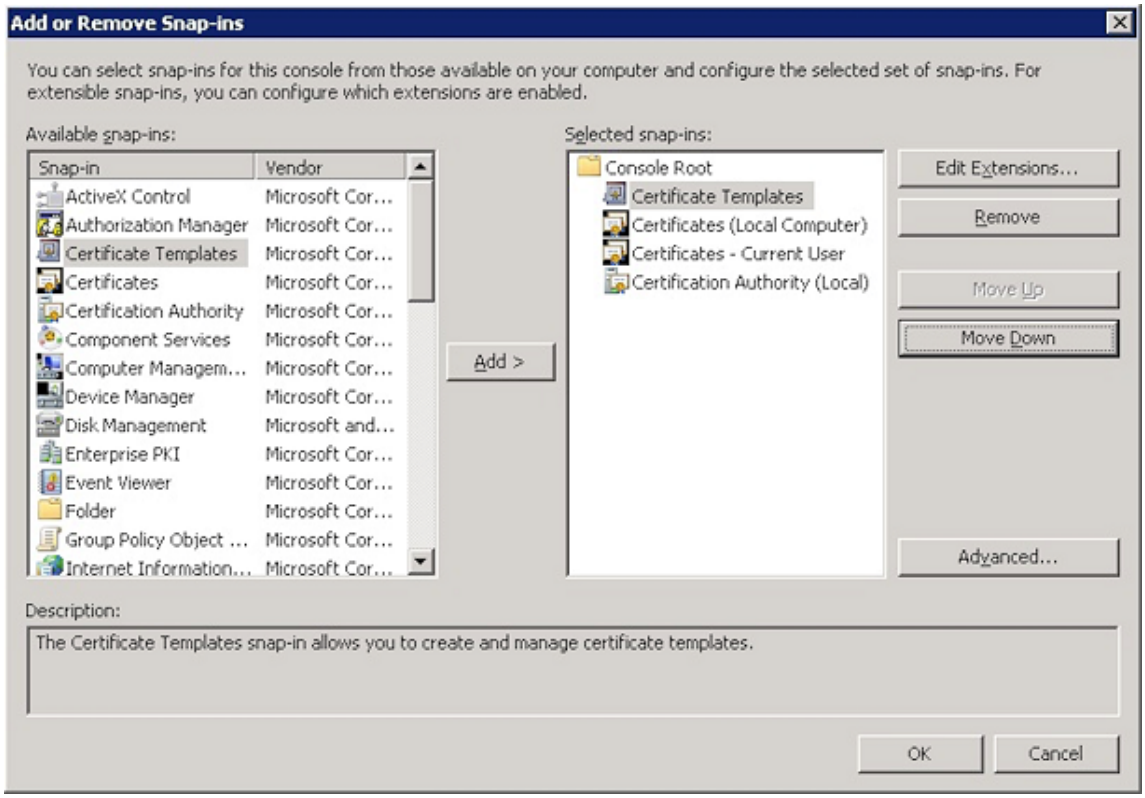
Logiciels requis

- Lorsque vous créez un modèle d'entité Services de certificats Microsoft, évitez les problèmes d'authentification possibles avec des appareils inscrits, en n'utilisant pas de caractères spéciaux. Par exemple, n'utilisez pas ces caractères dans le nom du modèle : `: ! $ ()# % + * ~ ? | { } []`
- Pour configurer l'authentification basée sur certificat pour Exchange ActiveSync, consultez la documentation Microsoft sur Exchange Server. Configurez le site de serveur d'autorité de certification (CA) pour Exchange ActiveSync pour exiger des certificats clients.
- Si vous utilisez des certificats de serveur privé pour sécuriser le trafic ActiveSync avec le serveur Exchange, assurez-vous que tous les certificats racine et intermédiaires ont été installés sur les appareils mobiles. Sinon, l'authentification basée sur certificat échoue lors de la configuration de la boîte aux lettres dans Citrix Secure Mail. Dans la console Exchange IIS, vous devez :
  - Ajouter un site Web à utiliser par Citrix Endpoint Management avec Exchange et lier le certificat de serveur Web.
  - Utiliser le port 9443.
  - Pour ce site Web, vous devez ajouter deux applications, une pour « Microsoft-Server-ActiveSync » et une pour « EWS ». Pour ces deux applications, sous **Paramètres SSL**, sélectionnez **Exiger SSL**.

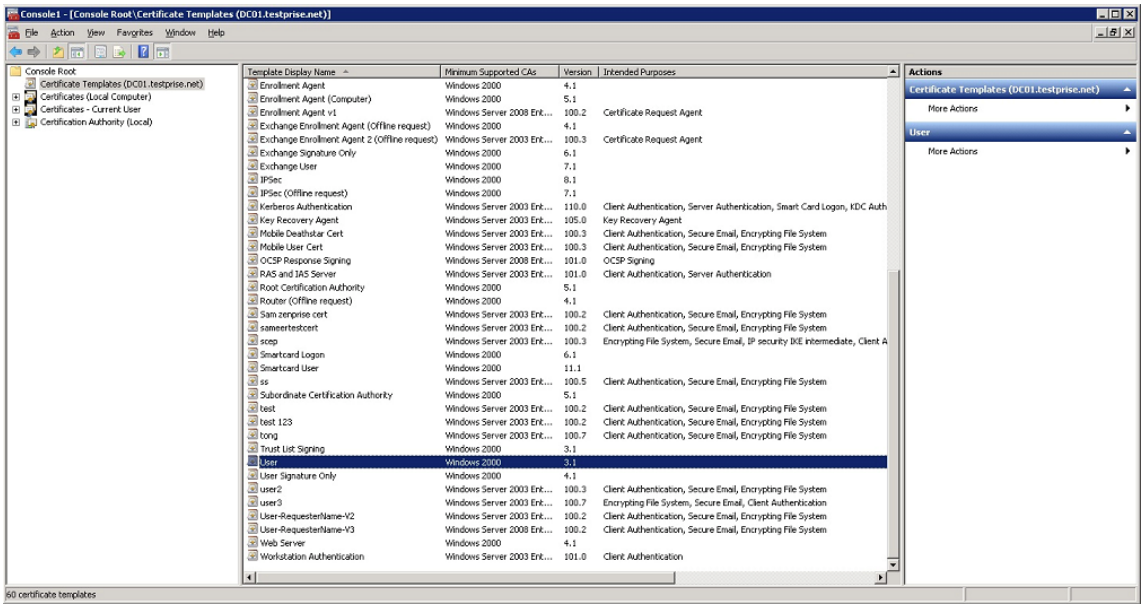
Ajoutez un composant logiciel enfichable pour les certificats dans la console Microsoft Management Console

1. Ouvrez la console et cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
2. Ajoutez les composants logiciels enfichables suivants :
   - Modèles de certificats
   - Certificats (ordinateur local)
   - Certificats - Utilisateur actuel
   - Autorité de certification (locale)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

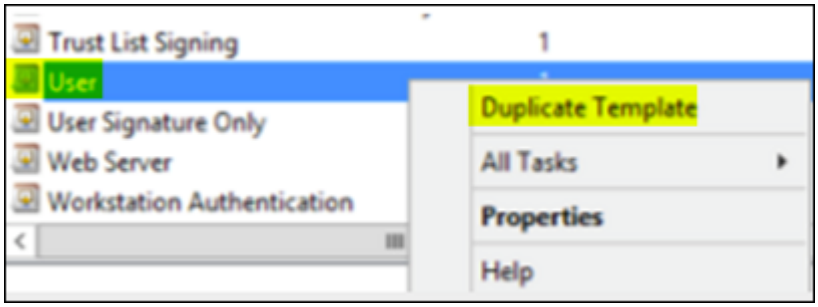


3. Développez **Modèles de certificats**.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Fournissez le nom du modèle.

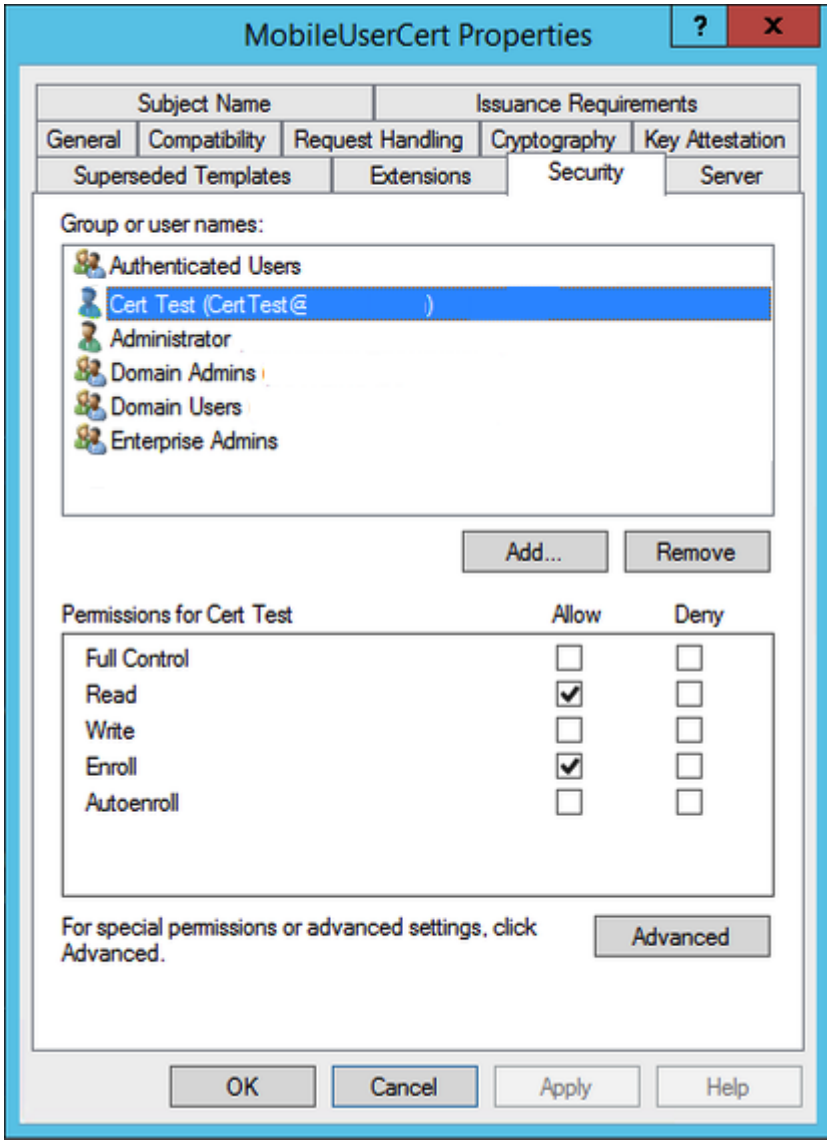
> **Important :**
>
> Sélectionnez la case **Publier le certificat dans Active Directory** uniquement si nécessaire. Si cette option est sélectionnée, tous les certificats client utilisateur sont créés dans Active Directory, ce qui pourrait encombrer votre base de données Active Directory.

6. Sélectionnez **Windows 2003 Server** comme type de modèle. Dans Windows 2012 R2 Server, sous **Compatibilité**, sélectionnez **Autorité de certification** et définissez le destinataire en tant que **Windows 2003**.
7. Sous **Sécurité**, cliquez sur **Ajouter**, puis sélectionnez le compte utilisateur AD que Citrix Endpoint Management utilisera pour générer des certificats.

> **Important :**
>
> ajoutez uniquement l'utilisateur du compte de service ici. Ajoutez l'autorisation **Inscrire** uniquement pour ce compte utilisateur AD.

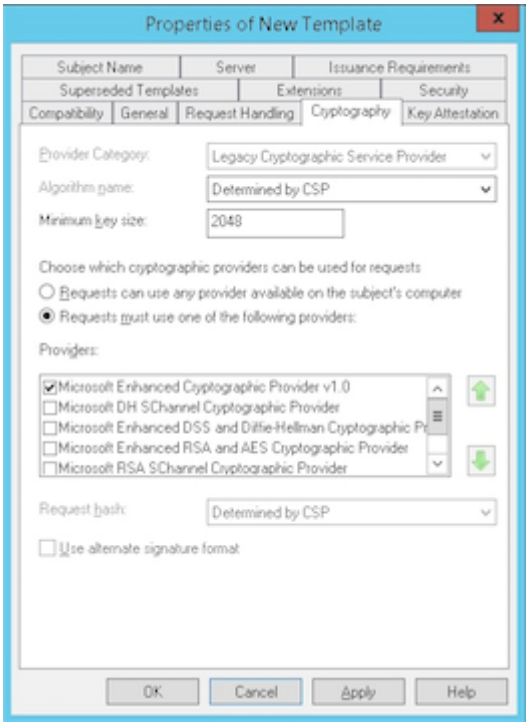
Comme décrit plus loin dans cet article, vous allez créer un certificat utilisateur .pfx à l'aide du compte de service. Pour plus d'informations, consultez la section Création d'un certificat PFX depuis le serveur CA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

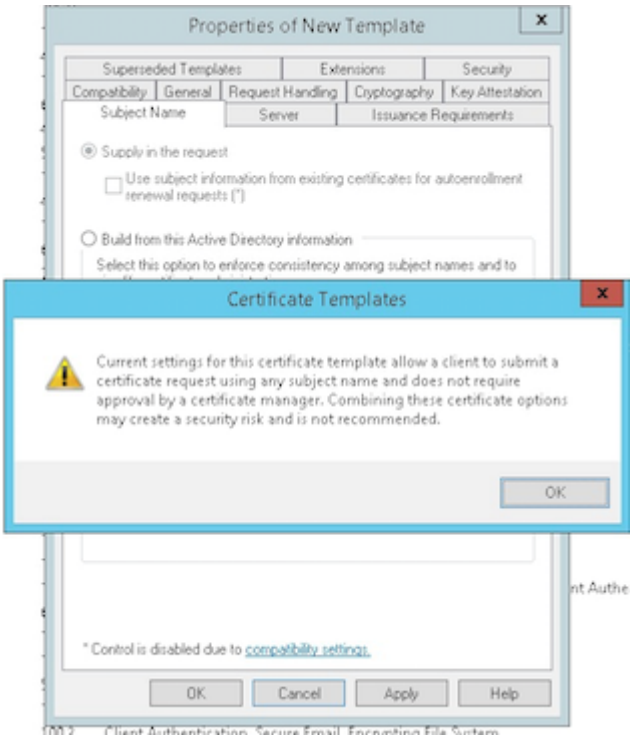


8. Sous **Cryptographie**, assurez-vous de fournir la taille de la clé. Vous entrerez plus tard la taille de la clé lors de la configuration de Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



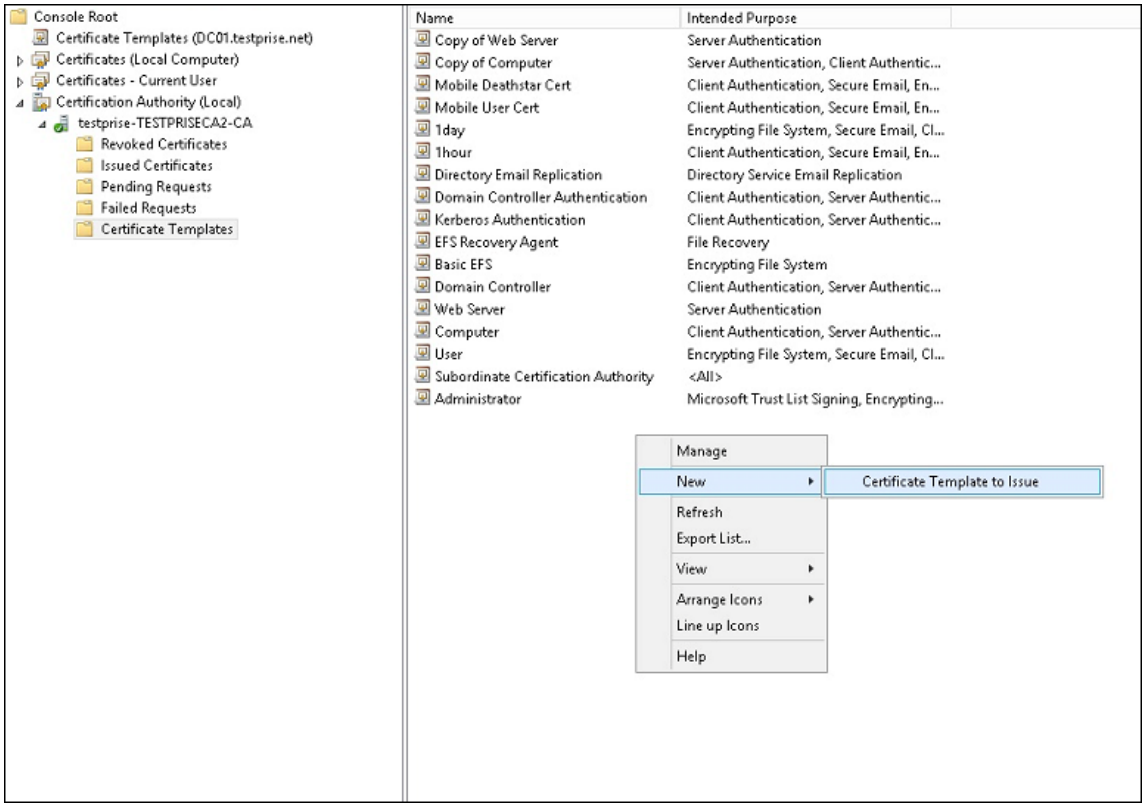
9. Sous **Nom du sujet**, sélectionnez **Fournir dans la demande**. Appliquez les modifications et enregistrez.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

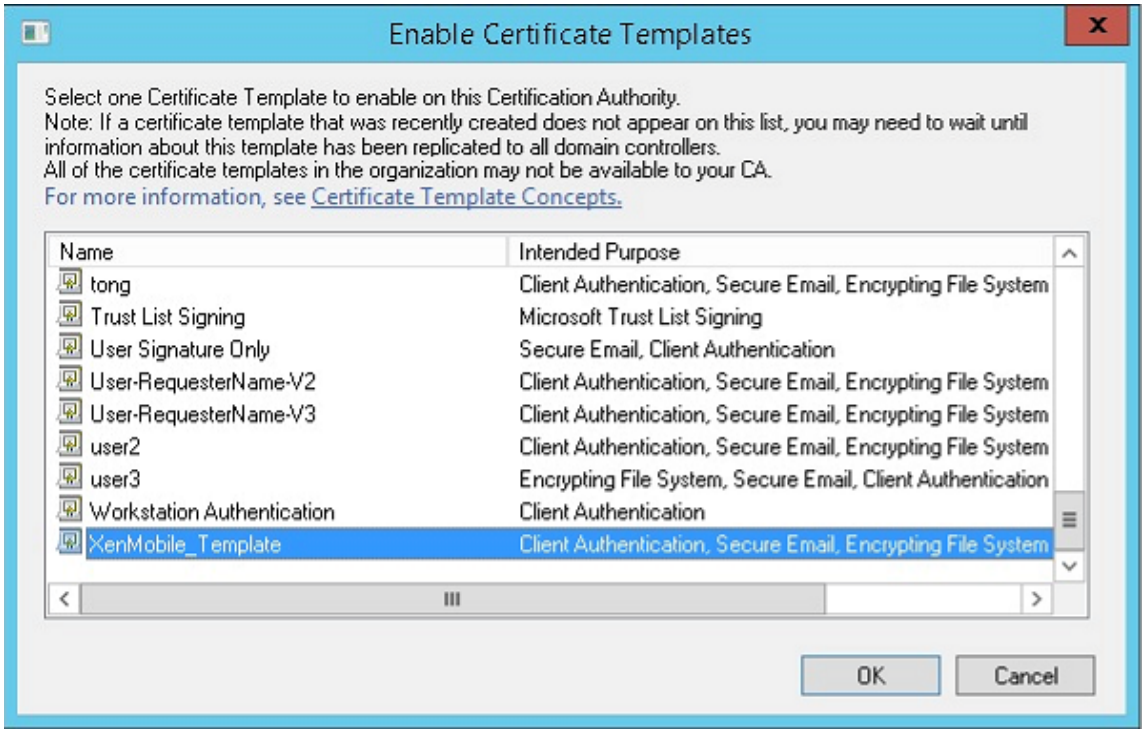
Ajout du modèle à l'autorité de certification (CA)

1. Accédez à **Autorité de certification** et sélectionnez **Modèles de certificats**.
2. Cliquez avec le bouton droit dans le panneau de droite et sélectionnez **Nouveau > Modèle de certificat à délivrer**.



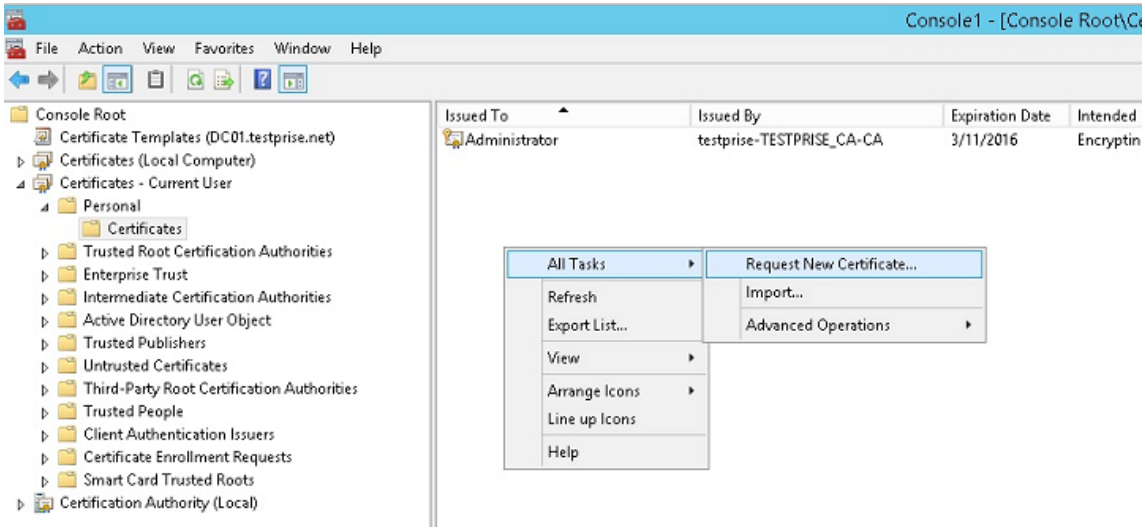
3. Sélectionnez le modèle que vous avez créé à l'étape précédente et cliquez sur **OK** pour l'ajouter à l'**autorité de certification**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



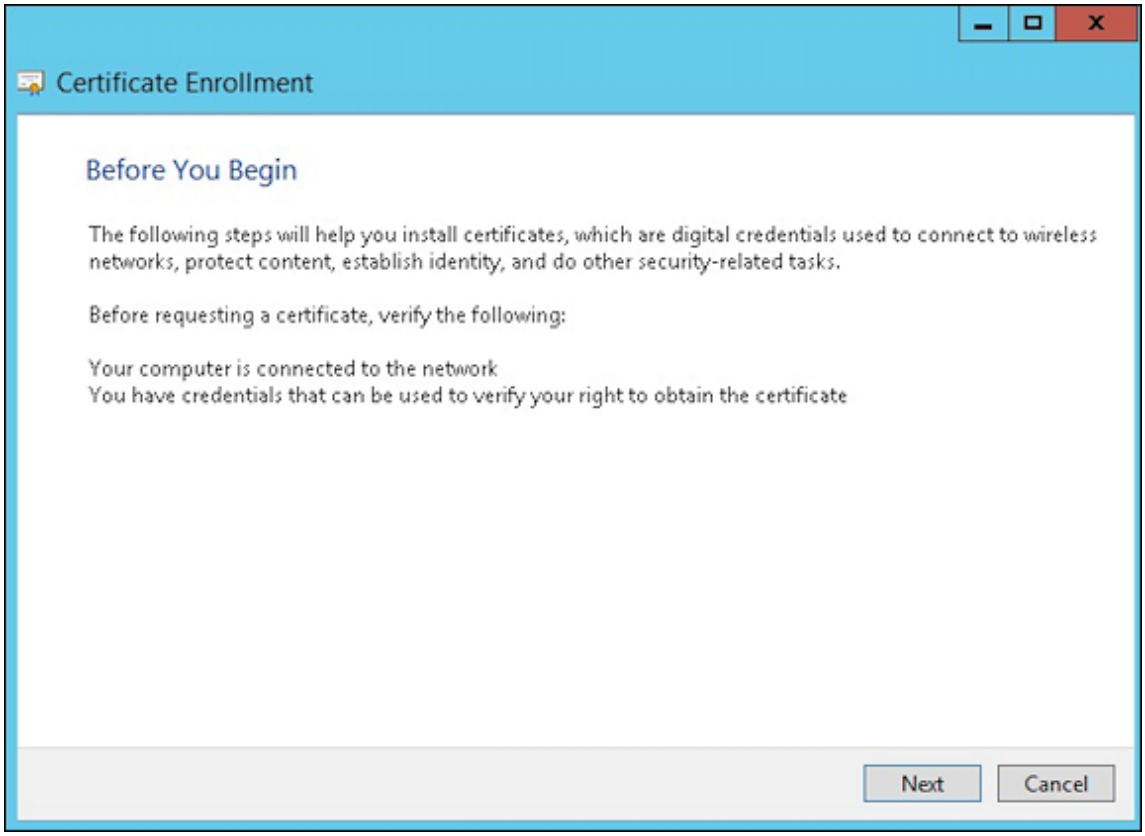
Création d'un certificat PFX depuis le serveur CA

1. Créez un certificat utilisateur .pfx à l'aide du compte de service avec lequel vous vous êtes connecté. Ce fichier .pfx est chargé dans Citrix Endpoint Management, qui demande ensuite un certificat utilisateur de la part des utilisateurs qui inscrivent leurs appareils.
2. Sous **Utilisateur actuel**, développez **Certificats**.
3. Cliquez avec le bouton droit dans le panneau de droite et cliquez sur **Demander un nouveau certificat**.



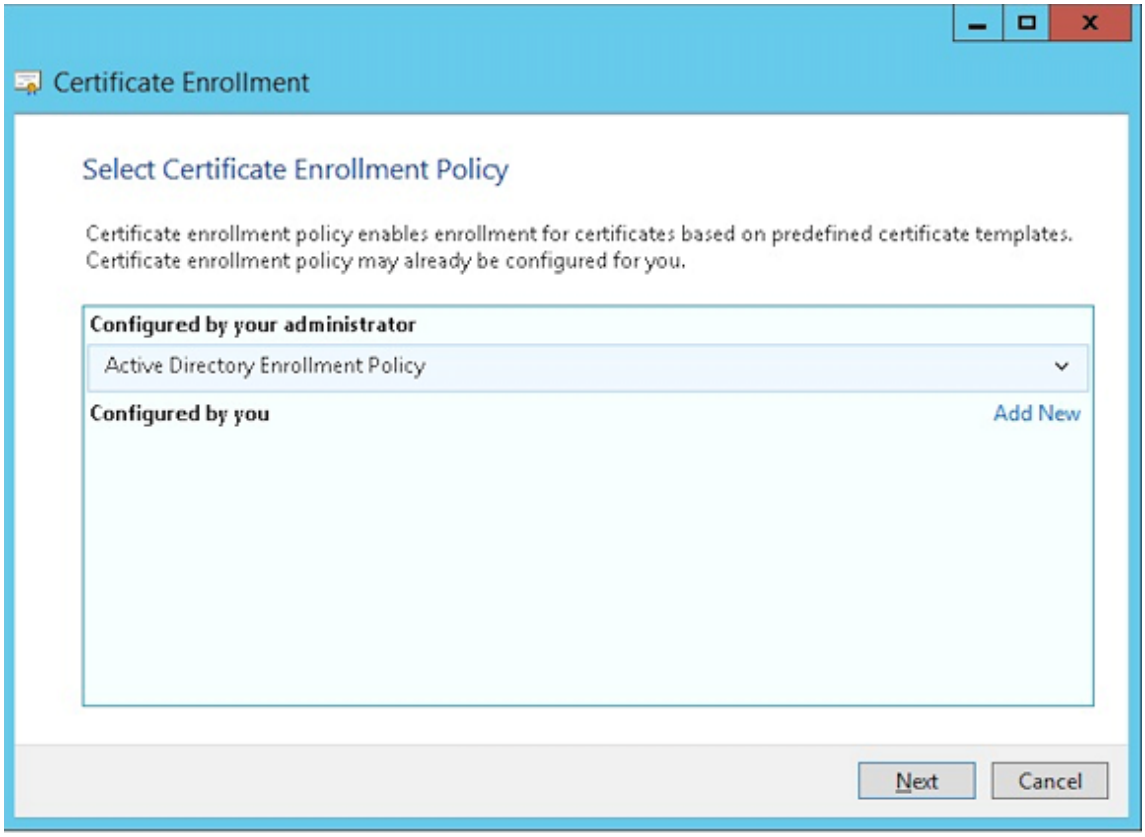
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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



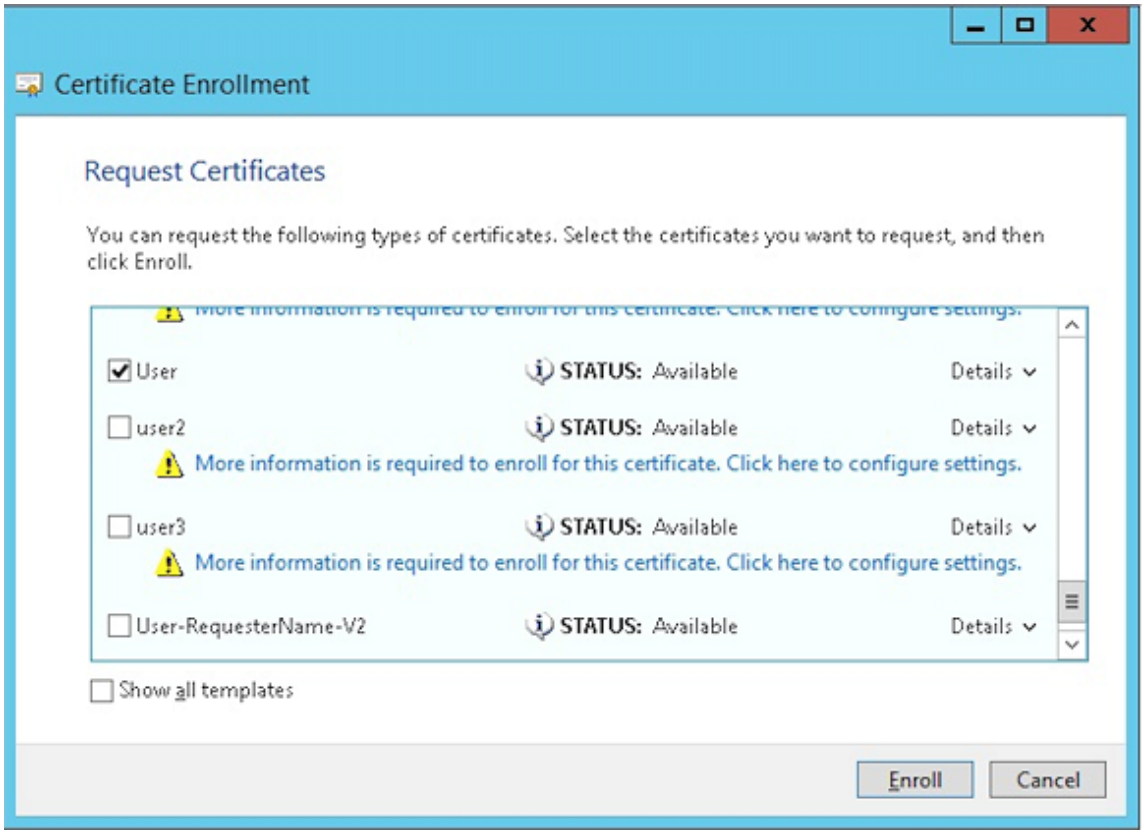
5. Sélectionnez **Stratégie d'inscription à Active Directory** et cliquez sur **Suivant**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

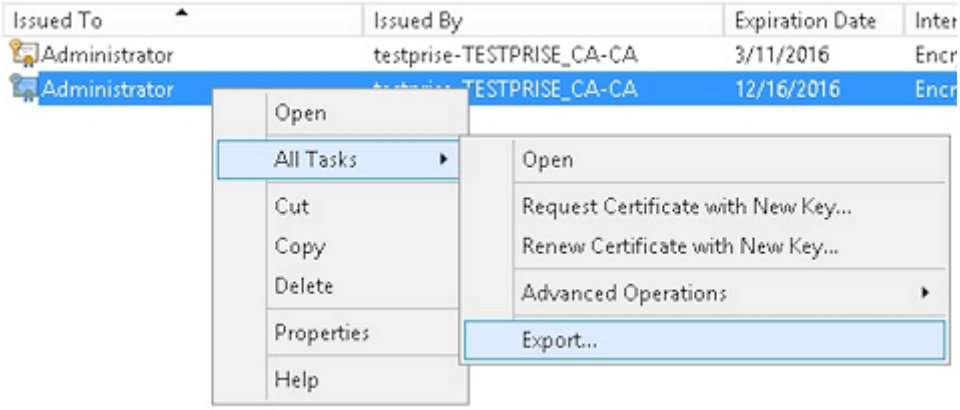


6. Sélectionnez le modèle **Utilisateur** et cliquez sur **Inscrire**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

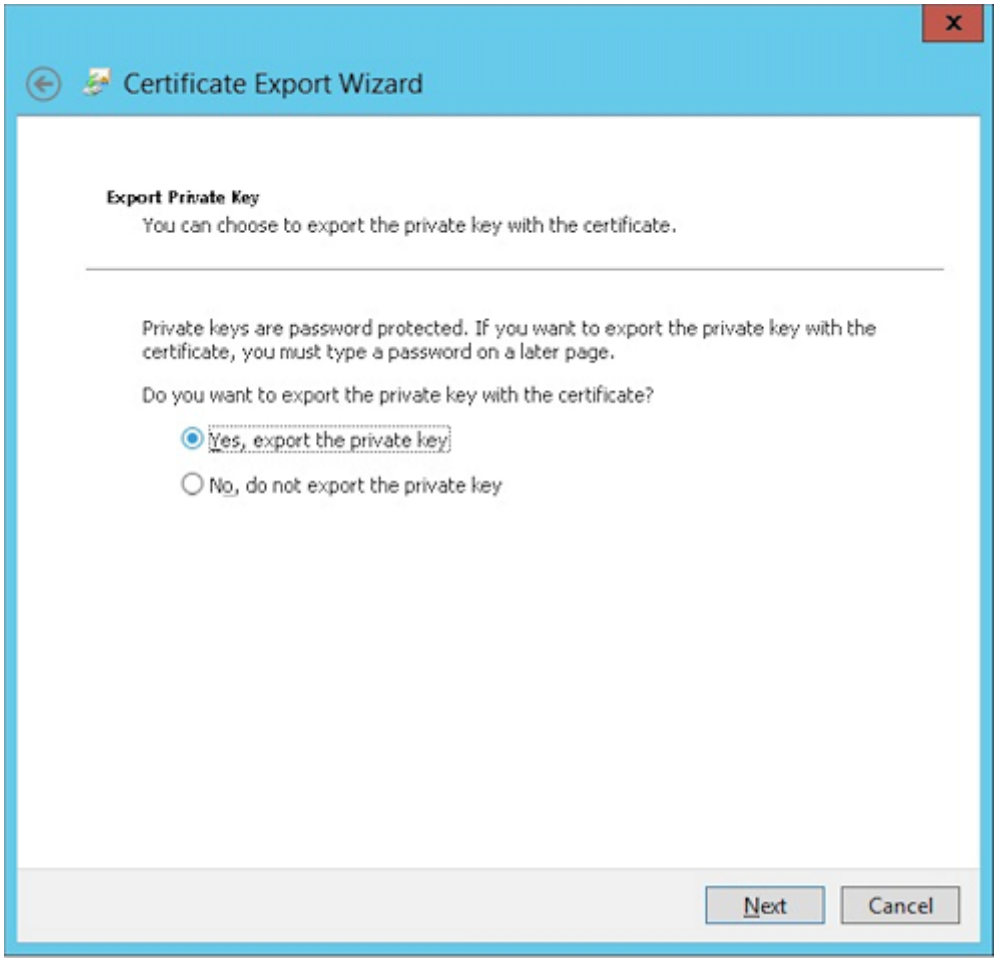


7. Exportez le fichier .pfx que vous avez créé à l'étape précédente.



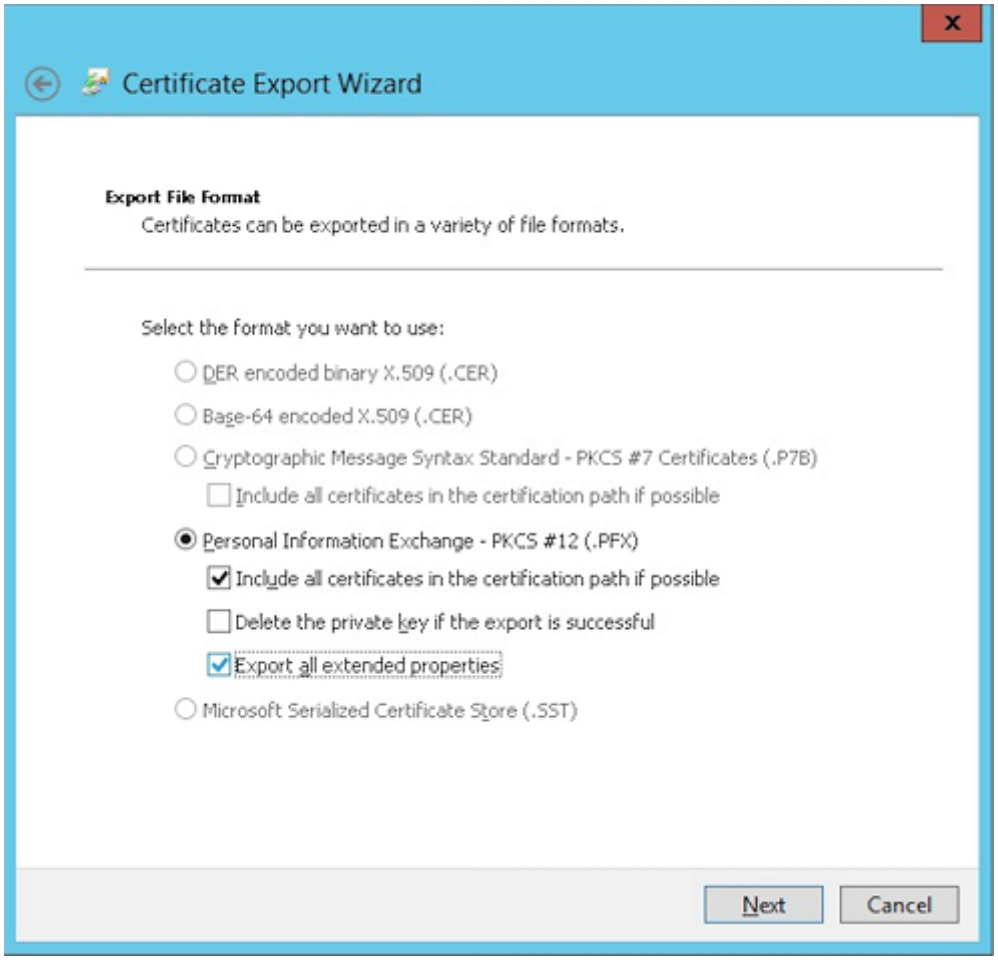
8. Cliquez sur **Oui, exporter la clé privée**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



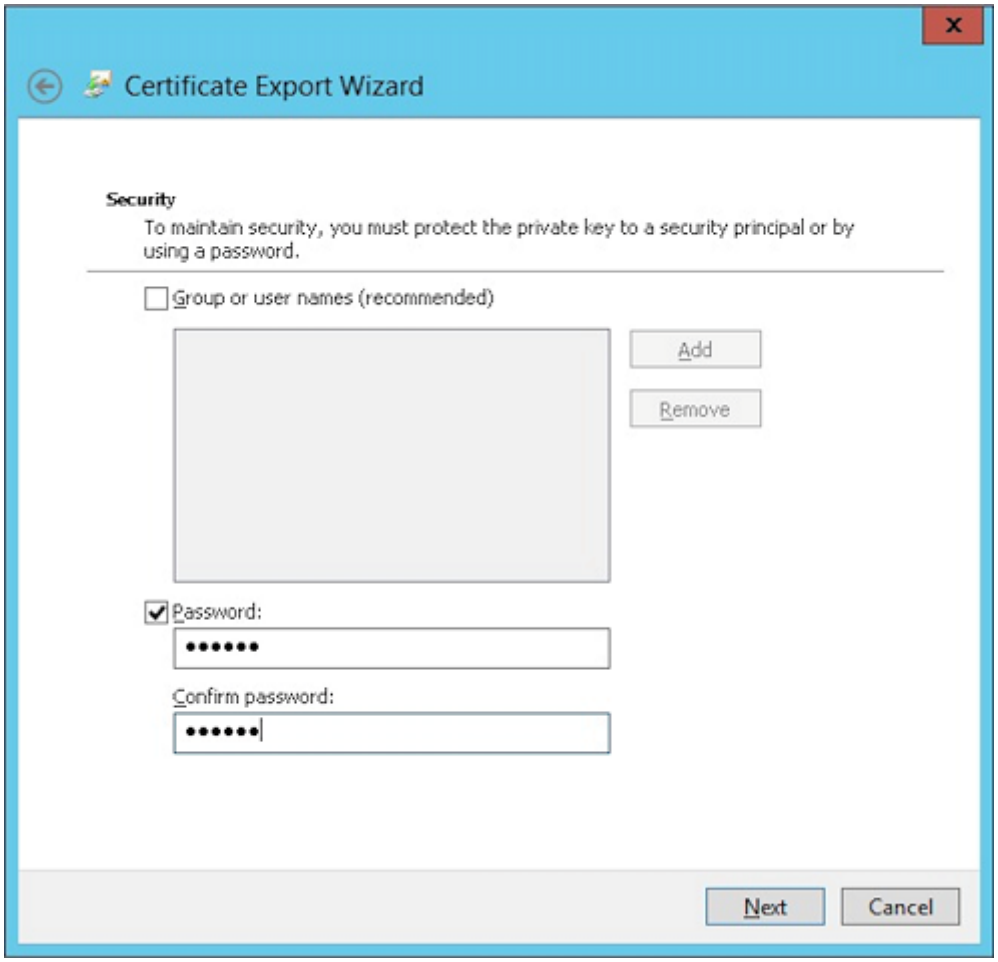
9. Sélectionnez **Si possible inclure tous les certificats dans le chemin d'accès de certification si possible** et la case **Exporter toutes les propriétés étendues**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



10. Définissez un mot de passe que vous utiliserez lors du chargement de ce certificat dans Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

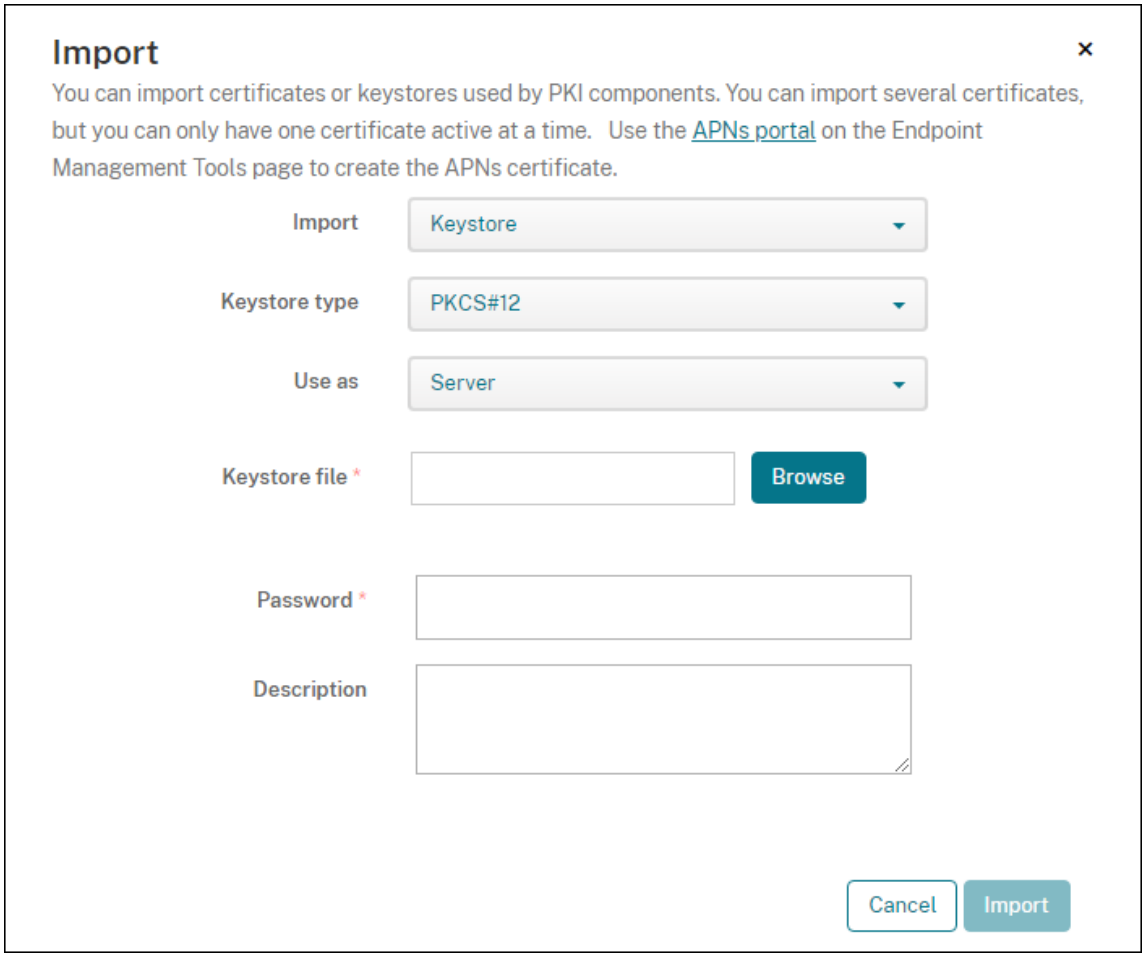


11. Enregistrez le certificat sur votre disque dur.

Chargement du certificat dans Citrix Endpoint Management

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. L'écran **Paramètres** s'affiche.
2. Cliquez sur **Certificats** et sur **Importer**.
3. Entrez les paramètres suivants :
   - **Importer :** Keystore
   - **Type de keystore :** PKCS # 12
   - **Utiliser en tant que :** Serveur
   - **Fichier de keystore :** cliquez sur Parcourir pour sélectionner le certificat .pfx que vous venez de créer.
   - **Mot de passe :** entrez le mot de passe que vous avez créé pour ce certificat.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



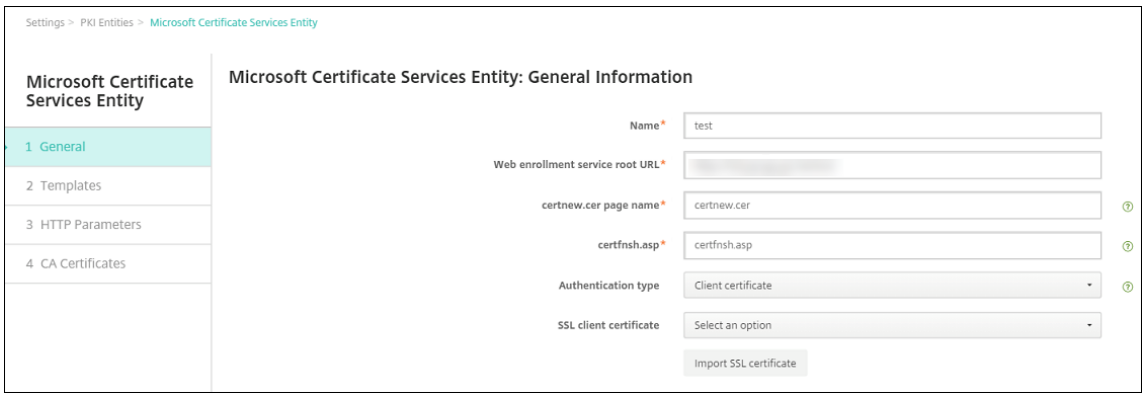
4. Cliquez sur **Importer**.
5. Vérifiez que le certificat a été installé correctement. Un certificat correctement installé s'affiche en tant que certificat utilisateur.

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

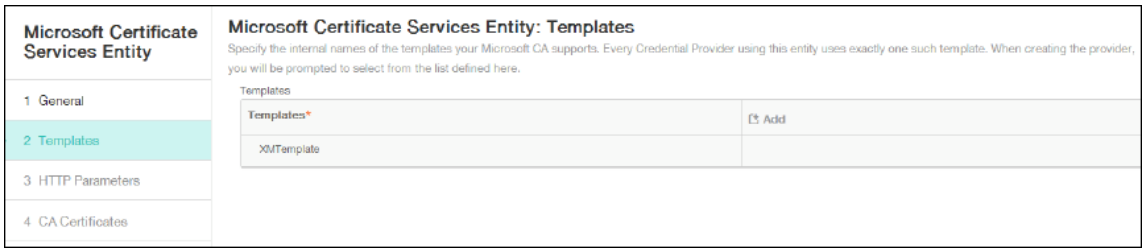
1. Dans **Paramètres**, accédez à **Plus > Gestion des certificats > Entités PKI**.
2. Cliquez sur **Ajouter** et sur **Entité Services de certificats Microsoft**. L'écran **Entité Services de certificats Microsoft : informations générales** s'affiche.
3. Entrez les paramètres suivants :
   - **Nom :** entrez un nom quelconque.
   - **URL racine du service d'inscription Web :** `https://RootCA-URL/certsrv/` (N'oubliez pas d'ajouter la dernière barre oblique (/) dans l'URL.)
   - **Nom de page certnew.cer :** certnew.cer (valeur par défaut)
   - **certfnsh.asp :** certfnsh.asp (valeur par défaut)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

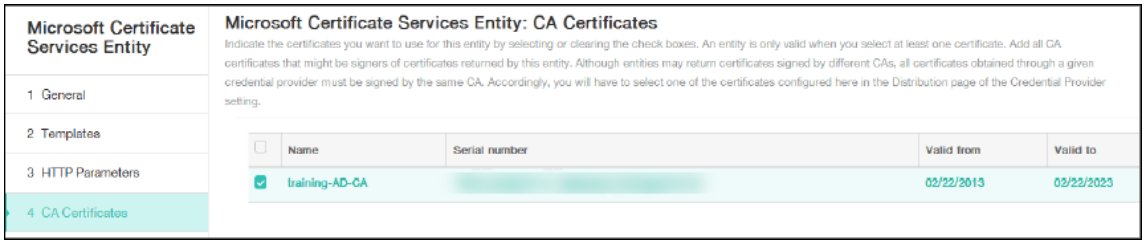
- **Type d'authentification :** certificat client
- **Certificat SSL :** sélectionnez le certificat utilisateur à utiliser pour émettre le certificat client Citrix Endpoint Management. Si aucun certificat n'existe, suivez la procédure décrite dans la section précédente pour télécharger des certificats.



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



5. Ignorez les paramètres HTTP et cliquez sur **Certificats CA**.
6. Sélectionnez le nom de l'autorité de certification racine qui correspond à votre environnement. L'autorité de certification racine fait partie de la chaîne importée depuis le certificat client Citrix Endpoint Management.



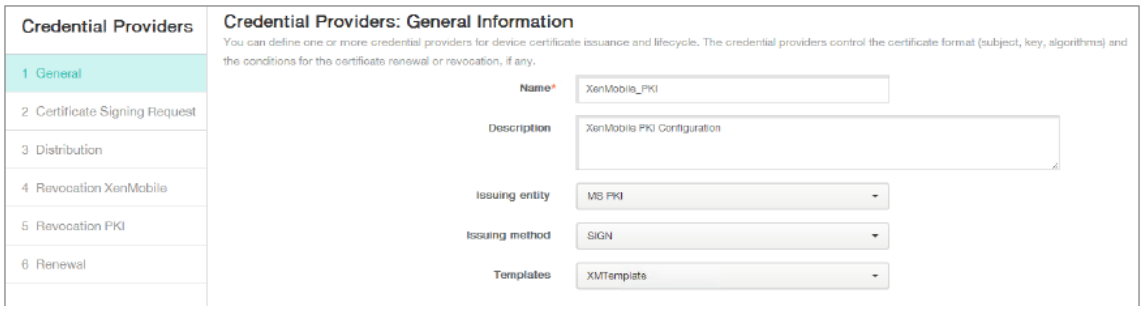
7. Cliquez sur **Enregistrer**.

Configuration des Fournisseurs d'informations d'identification

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Cliquez sur **Ajouter**.
3. Sous **Général**, entrez les paramètres suivants :
   - **Nom :** entrez un nom quelconque.
   - **Description :** entrez une description quelconque.
   - **Entité émettrice :** sélectionnez l'entité PKI créée précédemment.
   - **Méthode d'émission :** SIGNER
   - **Modèles :** sélectionnez le modèle ajouté sous l'entité PKI.



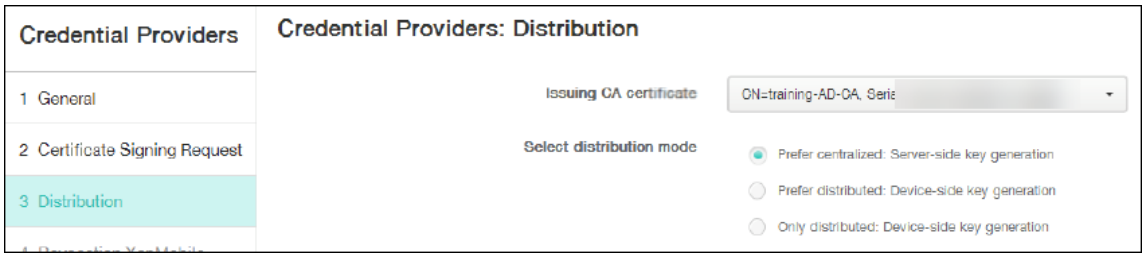
4. Cliquez sur **Demande de signature de certificat** et entrez les paramètres suivants :
   - **Algorithme de clé :** RSA
   - **Taille de la clé :** 2048
   - **Algorithme de signature :** SHA256withRSA
   - **Nom du sujet :** `cn=$user.username`

   Pour **Noms de sujet alternatifs**, cliquez sur **Ajouter** et entrez les paramètres suivants :
   - **Type :** nom principal de l'utilisateur
   - **Valeur :** `$user.userprincipalname`

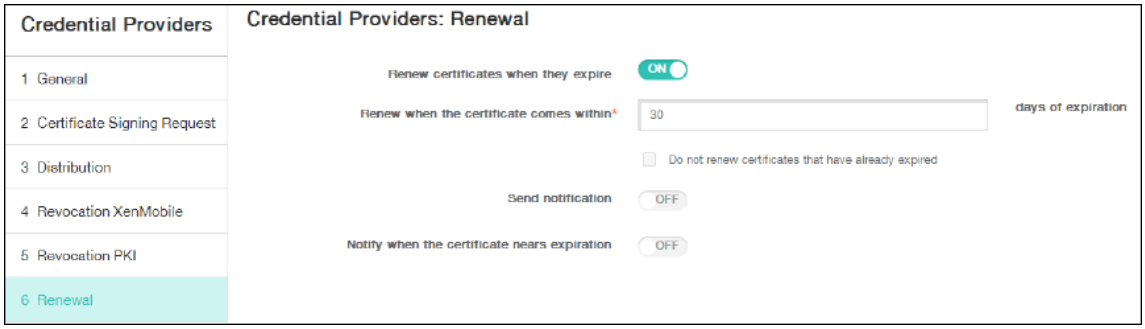
5. Cliquez sur **Distribution** et entrez les paramètres suivants :
   - **Certificat émis par l'autorité de certification :** sélectionnez l'autorité de certification émettrice qui a signé le certificat client Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Sélectionner le mode de distribution :** sélectionnez **Préférer mode centralisé : génération de la clé sur le serveur**.



6. Pour les deux prochaines sections, **Révocation Citrix Endpoint Management** et **Révocation PKI**, définissez les paramètres comme vous le souhaitez. Dans cet exemple, les deux options sont ignorées.
7. Cliquez sur **Renouvellement**.
8. Activez **Renouveler les certificats lorsqu'ils expirent**.
9. Laissez tous les autres paramètres par défaut ou modifiez-les comme vous le souhaitez.

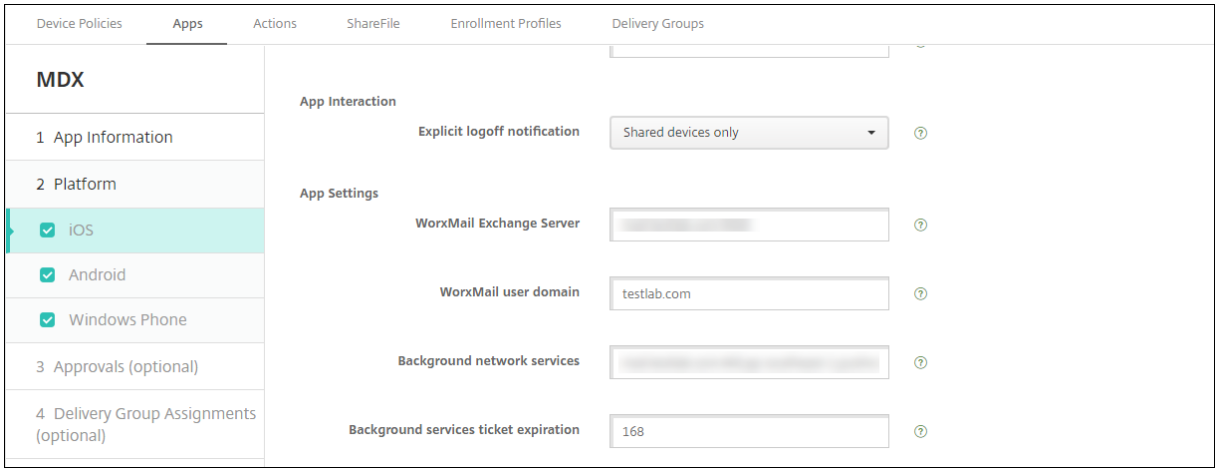


10. Cliquez sur **Enregistrer**.

Configuration de Citrix Secure Mail pour utiliser l'authentification basée sur certificat

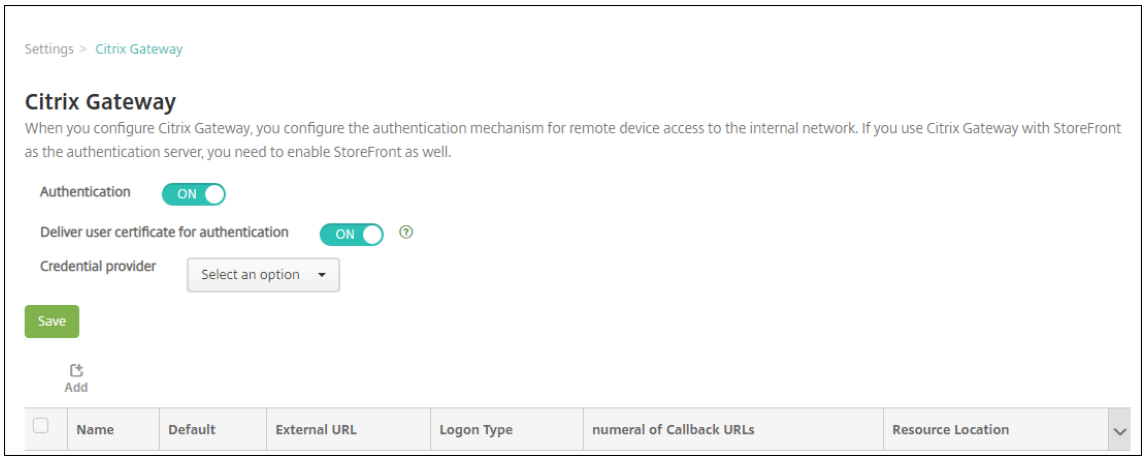
Lorsque vous ajoutez Citrix Secure Mail à Citrix Endpoint Management, n'oubliez pas de configurer les paramètres Exchange sous **Paramètres applicatifs**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



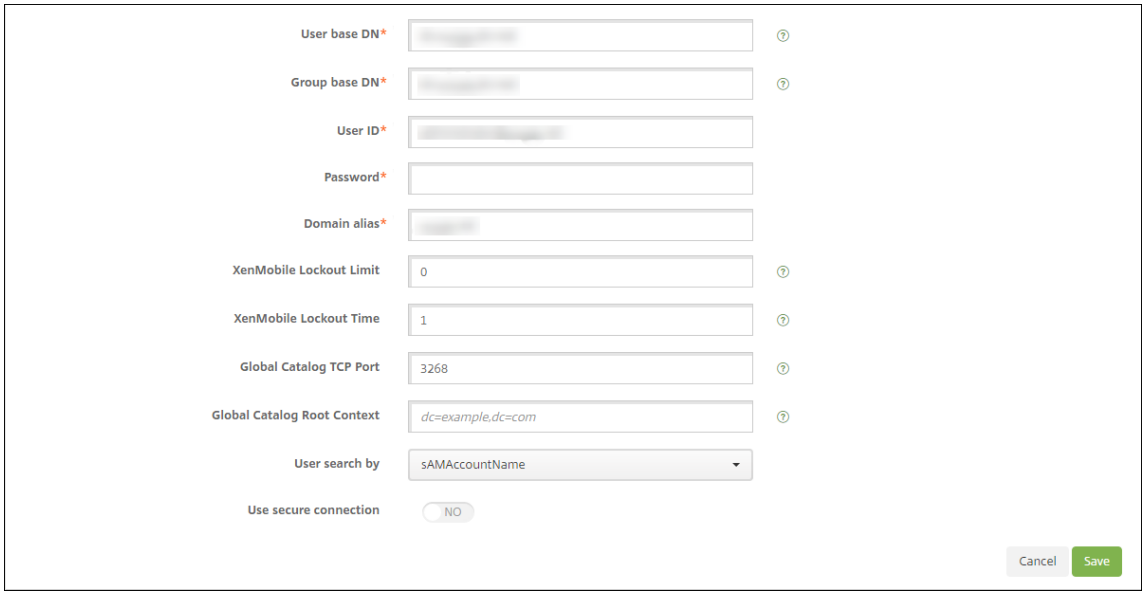
Configuration de la mise à disposition de certificats NetScaler Gateway dans Citrix Endpoint Management

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. L'écran **Paramètres** s'affiche.
2. Sous **Serveur**, cliquez sur **NetScaler Gateway**.
3. Si NetScaler Gateway n'est pas déjà ajouté, cliquez sur **Ajouter** et spécifiez les paramètres :
   - **Nom :** nom descriptif de l'appliance.
   - **Alias :** alias facultatif de l'appliance.
   - **URL externe :** `https://YourCitrixGatewayURL`
   - **Type d'ouverture de session :** sélectionnez **Certificat et domaine**
   - **Mot de passe requis :** Désactivé
   - **Définir par défaut :** Activé
4. Pour **Authentification** et **Délivrer un certificat utilisateur pour l'authentification**, sélectionnez **Activé**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Pour **Fournisseur d'identités**, sélectionnez un fournisseur et cliquez sur **Enregistrer**.
6. Pour utiliser des attributs sAMAccount dans les certificats utilisateur comme une alternative au nom d'utilisateur principal (UPN), configurez le connecteur LDAP dans Citrix Endpoint Management : accédez à **Paramètres > LDAP**, sélectionnez le répertoire et cliquez sur **Modifier**, puis sélectionnez **sAMAccountName** dans **Recherche utilisateur par**.



Activer le code PIN Citrix et la mise en cache du mot de passe de l'utilisateur

Pour activer le code PIN Citrix et la mise en cache du mot de passe de l'utilisateur, accédez à **Paramètres > Propriétés du client** et sélectionnez ces cases : **Activer l'authentification par code PIN Citrix** et **Activer la mise en cache du mot de passe de l'utilisateur**. Pour de plus amples informations, consultez la section Propriétés du client.

Résolution des problèmes de configuration du certificat client

Une fois la configuration précédente et la configuration NetScaler Gateway effectuées avec succès, le workflow de l'utilisateur est le suivant :

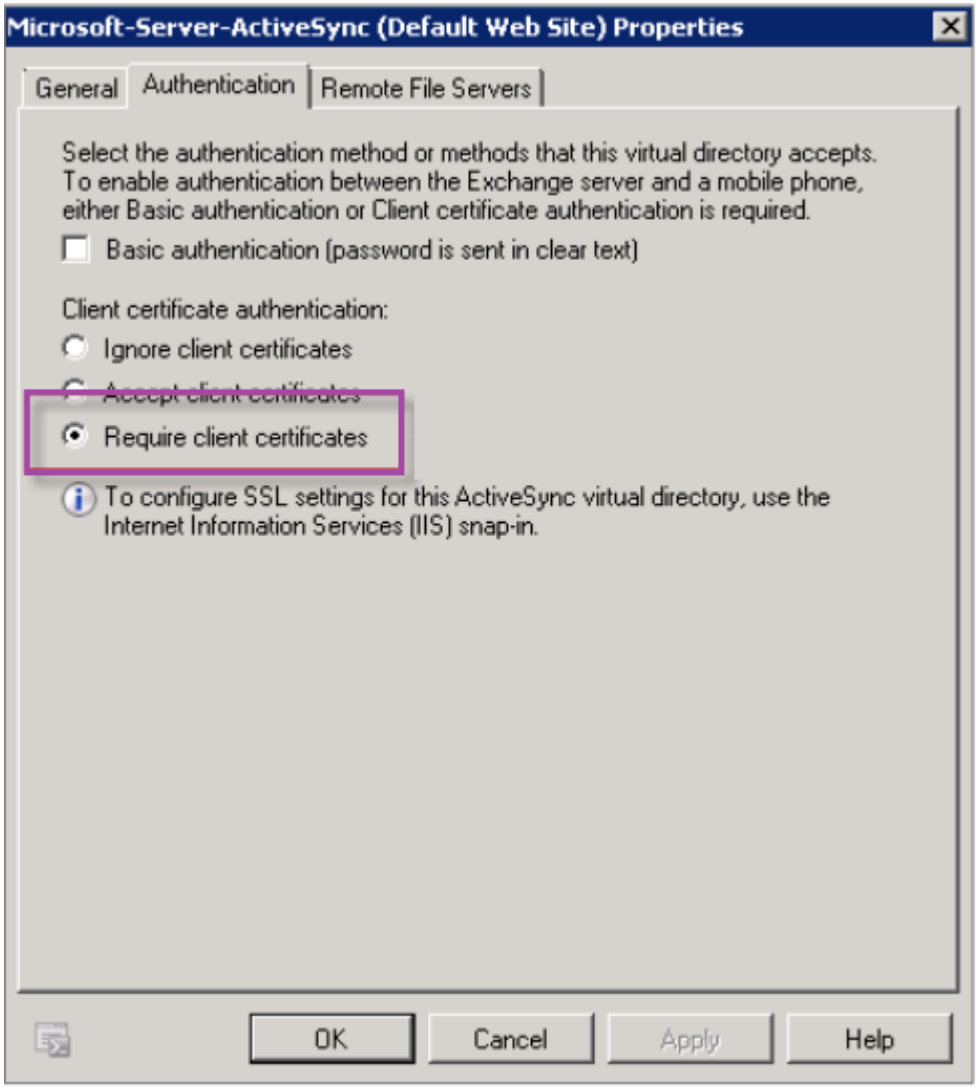
1. Les utilisateurs inscrivent leurs appareils mobiles.
2. Citrix Endpoint Management invite les utilisateurs à créer un code PIN Citrix.
3. Les utilisateurs sont redirigés vers le magasin d'applications.
4. Lorsque les utilisateurs démarrent Citrix Secure Mail, Citrix Endpoint Management ne les invite pas à entrer d'informations d'identification afin de configurer leurs boîtes aux lettres. Au lieu de cela, Citrix Secure Mail demande le certificat client de Citrix Secure Hub et l'envoie à Microsoft

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exchange Server pour authentification. Si Citrix Endpoint Management invite les utilisateurs à entrer des informations d'identification lorsqu'ils démarrent Citrix Secure Mail, vérifiez votre configuration.

Si les utilisateurs peuvent télécharger et installer Citrix Secure Mail, mais que Citrix Secure Mail ne termine pas la configuration durant la configuration de la boîte aux lettres :

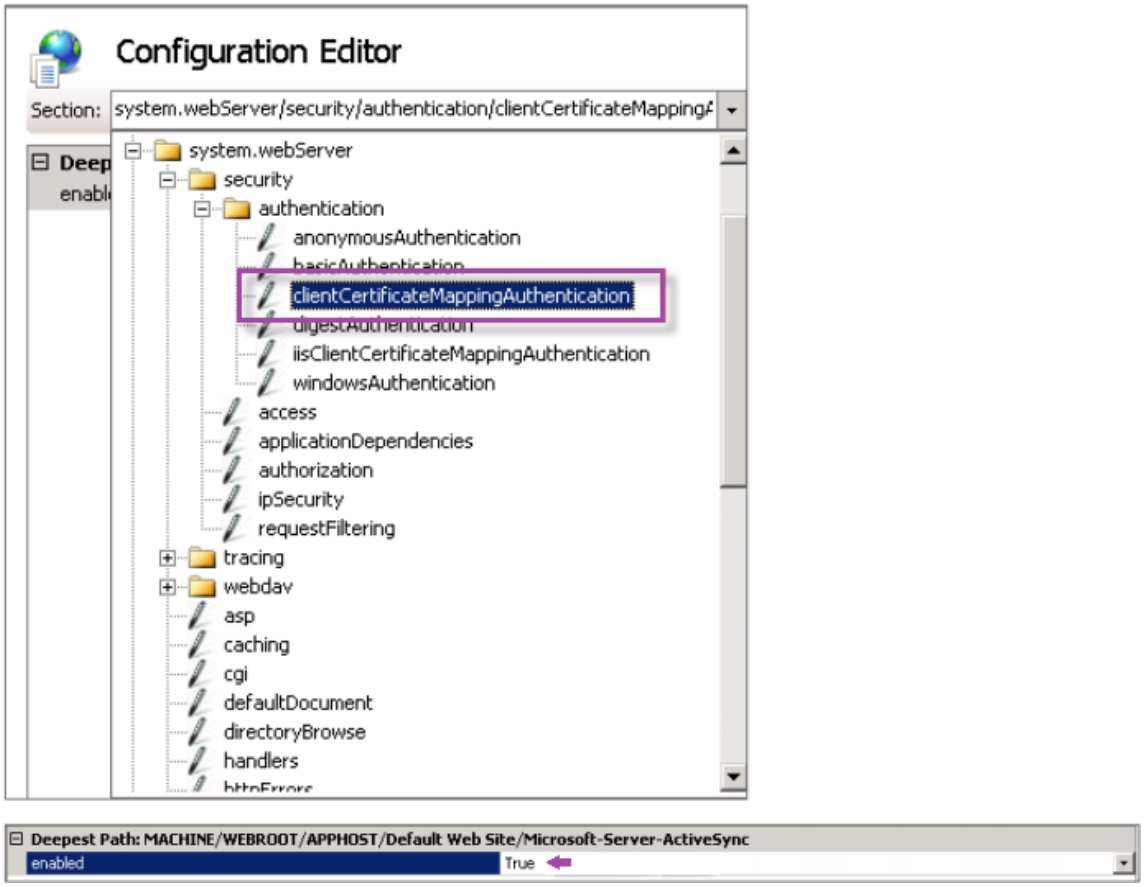
1. Si Microsoft Exchange Server ActiveSync utilise des certificats de serveur SSL privé pour sécuriser le trafic, vérifiez que les certificats racine/intermédiaire sont installés sur l'appareil mobile.
2. Vérifiez que le type d'authentification sélectionné pour ActiveSync est **Exiger les certificats clients**.



3. Sur Microsoft Exchange Server, sélectionnez le site **Microsoft-Server-ActiveSync** pour vérifier que l'authentification par mappage de certificat client est activée. Par défaut, l'authentification

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

par mappage de certificat client est désactivée. L'option figure sous **Éditeur de configuration > Sécurité > Authentification**.



Après avoir sélectionné **Vrai**, cliquez sur **Appliquer** pour que les modifications prennent effet.

4. Vérifiez les paramètres de NetScaler Gateway dans la console Citrix Endpoint Management : assurez-vous que **Délivrer un certificat utilisateur pour l'authentification** est défini sur **Activé** et que le profil correct est sélectionné pour **Fournisseur d'identités**.

Pour déterminer si le certificat client a été délivré à un appareil mobile

1. Dans la console Citrix Endpoint Management, accédez à **Gérer > Appareils** et sélectionnez l'appareil.
2. Cliquez sur **Modifier** ou **Afficher plus**.
3. Accédez à la section **Groupes de mise à disposition** et recherchez cette entrée :

   Informations d'identification NetScaler Gateway : Requested credential, CertId=

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour vérifier si la négociation du certificat client est activée

1. Exécutez cette commande `netsh` pour afficher la configuration du certificat SSL qui est liée sur le site Web IIS :

   ```
   netsh http show sslcert
   ```

2. Si la valeur **Négocier le certificat client** est **désactivée**, exécutez la commande suivante pour l'activer :

   ```
   netsh http delete sslcert ipport=0.0.0.0:443
   ```

   ```
   netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash
   appid={ app_id } certstorename=store_name verifyclientcertrevocation
   =Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck
   =Enable clientcertnegotiation=Enable
   ```

   Par exemple :

   ```
   netsh http add sslcert ipport=0.0.0.0:443 certhash=23498dfsdfhaf98rhkjqf98
    appid={ 123asd456jd-a12b-3c45-d678-123456lkjhgf } certstorename=
   ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWit
   =Disable UsageCheck=Enable clientcertnegotiation=Enable
   ```

Si vous ne pouvez pas délivrer de certificats racine/intermédiaire à un appareil Windows Phone 8.1 via Citrix Endpoint Management :

- Envoyez des fichiers de certificats racine/intermédiaire (.cer) par e-mail à l'appareil Windows Phone 8.1 et installez-les directement.

Si Citrix Secure Mail n'est pas installé correctement sur Windows Phone 8.1, vérifiez les points suivants :

- Le fichier de jeton d'inscription d'application (.AETX) est délivré via Citrix Endpoint Management à l'aide de la stratégie d'hub d'entreprise.
- Le jeton d'inscription d'application a été créé à l'aide du même certificat d'entreprise que celui du fournisseur de certificats utilisé pour encapsuler Citrix Secure Mail et signer les applications Citrix Secure Hub.
- Le même ID d'éditeur est utilisé pour signer et encapsuler Citrix Secure Hub, Citrix Secure Mail et le jeton d'inscription d'application.

Entités PKI

March 1, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Une configuration d'entité d'infrastructure de clé publique (PKI) Citrix Endpoint Management représente un composant réalisant des opérations PKI réelles (émission, révocation et informations d'état). Ces composants sont internes ou externes à Citrix Endpoint Management. Les composants internes sont appelés discrétionnaire. Les composants externes font partie de votre infrastructure d'entreprise.

Citrix Endpoint Management prend en charge les types d'entités PKI suivantes :

- Services de certificats Microsoft
- Autorités de certification discrétionnaires (CA)

Citrix Endpoint Management prend en charge les serveurs d'autorité de certification suivants :

- Windows Server 2016
- Windows Server 2019

> **Remarque :**
>
> Les versions 2012 R2, 2012 et 2008 R2 de Windows Servers ne sont plus prises en charge car elles ont atteint leur fin de vie. Pour en savoir plus, consultez la documentation sur le cycle de vie des produits Microsoft.

Concepts de PKI communs

Quel que soit son type, chaque entité PKI possède un sous-ensemble des fonctionnalités suivantes :

- **Signer :** émission d'un nouveau certificat, basé sur une demande de signature de certificat (CSR).
- **Récupérer :** récupération d'un certificat existant et d'une paire de clés.
- **Révoquer :** révocation d'un certificat client.

À propos des certificats CA

Lorsque vous configurez une entité PKI, informez Citrix Endpoint Management de la nature du certificat d'autorité de certification qui est le signataire des certificats émis par (ou récupérés depuis) cette entité. Cette entité PKI peut renvoyer des certificats signés (récupérés ou nouvellement signés) par un certain nombre d'autorités de certification différentes.

Fournissez le certificat de chacune de ces autorités dans le cadre de la configuration de l'entité PKI. Pour ce faire, chargez les certificats sur Citrix Endpoint Management puis référencez-les dans l'entité PKI. Pour les autorités de certification discrétionnaires, le certificat est implicitement le certificat de l'autorité de certification signataire. Pour les entités externes, vous devez spécifier le certificat manuellement.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Important :**
>
> Lorsque vous créez un modèle d'entité Services de certificats Microsoft, évitez les problèmes d'authentification possibles avec des appareils inscrits ; n'utilisez pas de caractères spéciaux dans le nom du modèle. Par exemple, n'utilisez pas : `! : $ ( )# % + * ~ ? | { } [ ]`

Services de certificats Microsoft

Citrix Endpoint Management se connecte avec Microsoft Certificate Services Web par le biais de son interface d'inscription Web. Citrix Endpoint Management prend uniquement en charge l'émission de nouveaux certificats via cette interface. Si l'autorité de certification Microsoft génère un certificat d'utilisateur NetScaler Gateway, NetScaler Gateway prend en charge le renouvellement et la révocation de ces certificats.

Pour créer une entité PKI Microsoft CA dans Citrix Endpoint Management, vous devez spécifier l'adresse URL de base de l'interface Web des services de certificats. Si vous le souhaitez, utilisez l'authentification de client SSL pour sécuriser la connexion entre Citrix Endpoint Management et l'interface Web des services de certificats.

Ajouter une entité Services de certificats Microsoft

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Entités PKI**.
2. Sur la page **Entités PKI**, cliquez sur **Ajouter**.

   Un menu des types d'entité PKI s'affiche.
3. Cliquez sur **Entité Services de certificats Microsoft**.

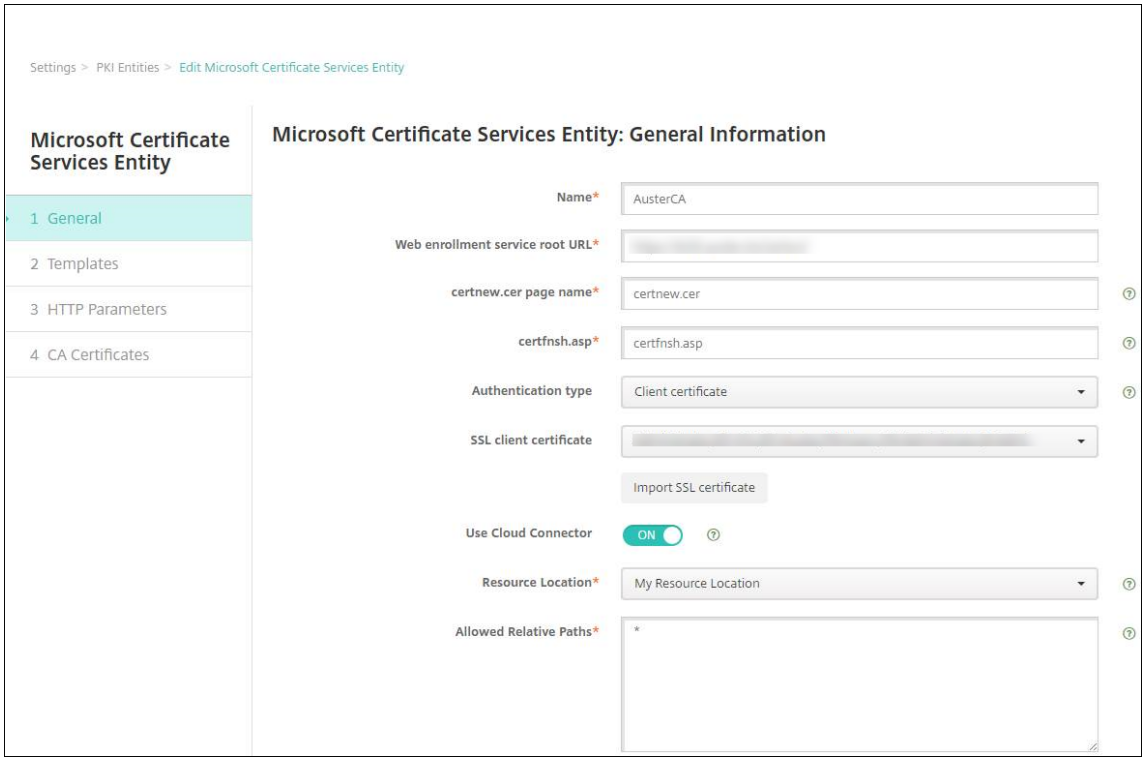
   La page **Entité Services de certificats Microsoft : informations générales** s'affiche.
4. Sur la page **Entité Services de certificats Microsoft : informations générales**, configurez ces paramètres :

   - **Nom :** entrez un nom pour votre nouvelle entité, qui sera utilisé plus tard pour faire référence à cette entité. Les noms de l'entité doivent être uniques.
   - **URL racine du service d'inscription Web :** entrez l'adresse URL de votre service d'inscription Web d'autorité de certification Microsoft. Par exemple : `https://192.0.0.1/certsrv/`. L'adresse URL peut utiliser un format HTTP ou HTTP-over-SSL.
   - **Nom de page certnew.cer :** nom de la page certnew.cer. Utilisez le nom par défaut sauf si vous l'avez renommé pour une raison quelconque.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **certfnsh.asp :** nom de la page certfnsh.asp. Utilisez le nom par défaut sauf si vous l'avez renommé pour une raison quelconque.
- **Type d'authentification :** choisissez la méthode d'authentification à utiliser.
  - **Aucune**
  - **HTTP basique :** entrez le nom d'utilisateur et mot de passe requis pour se connecter.
  - **Certificat client :** sélectionnez le certificat client SSL correct.
- **Utiliser Cloud Connector :** choisissez **Activé** pour utiliser Cloud Connector pour les connexions au serveur PKI. Ensuite, spécifiez un **emplacement de ressources** et des **chemins relatifs autorisés** pour la connexion.
  - **Emplacement des ressources :** choisissez parmi les emplacements de ressources définis dans Citrix Cloud Connector.
  - **Chemins relatifs autorisés :** chemins relatifs autorisés pour l'emplacement de ressources spécifié. Spécifiez un chemin d'accès par ligne. Vous pouvez utiliser le caractère générique astérisque (*).

    Si l'emplacement des ressources est `https://www.ServiceRoot/certsrv`. Pour fournir l'accès à toutes les adresses URL dans le chemin d'accès, entrez `/*` dans **Chemins relatifs autorisés**.



5. Cliquez sur **Tester la connexion** pour vous assurer que le serveur est accessible. S'il n'est pas accessible, un message s'affiche, indiquant que la connexion a échoué. Vérifiez vos paramètres

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de configuration.

6. Cliquez sur **Suivant**.

   La page **Entité Services de certificats Microsoft : modèles** s'affiche. Sur cette page, spécifiez le nom interne des modèles pris en charge par votre autorité de certification Microsoft. Lors de la création de Fournisseurs d'informations d'identification, vous devez sélectionner un modèle dans la liste définie ici. Chaque fournisseur d'identités utilisant cette entité utilise un seul modèle de ce type.

   Pour connaître la configuration requise pour les modèles Services de certificats Microsoft, veuillez consulter la documentation Microsoft relative à votre version de serveur Microsoft. Citrix Endpoint Management ne requiert pas de configuration particulière pour les certificats qu'il distribue autres que les formats de certificat indiqués dans Certificats.

7. Sur la page **Entité Services de certificats Microsoft : modèles**, cliquez sur **Ajouter**, entrez le nom du modèle et cliquez sur **Enregistrer**. Répétez cette étape pour chaque modèle à ajouter.

8. Cliquez sur **Suivant**.

   La page **Entité Services de certificats Microsoft : paramètres HTTP** s'affiche. Sur cette page, spécifiez des paramètres personnalisés que Citrix Endpoint Management doit ajouter à la requête HTTP auprès de l'interface d'inscription Web de Microsoft. Les paramètres personnalisés ne sont utiles que pour les scripts personnalisés exécutés sur l'autorité de certification.

9. Sur la page **Entité Services de certificats Microsoft : paramètres HTTP**, cliquez sur **Ajouter**, entrez le nom et la valeur des paramètres HTTP que vous souhaitez ajouter, puis cliquez sur **Suivant**.

   La page **Entité Services de certificats Microsoft : certificats CA** s'affiche. Sur cette page, vous devez informer Citrix Endpoint Management des signataires des certificats que le système obtient par le biais de cette entité. Lorsque votre certificat CA est renouvelé, mettez-le à jour dans Citrix Endpoint Management. Citrix Endpoint Management applique le changement à l'entité de manière transparente.

10. Sur la page **Entité Services de certificats Microsoft : certificats CA**, sélectionnez les certificats que vous voulez utiliser pour cette entité.

11. Cliquez sur **Enregistrer**.

    L'entité s'affiche sur le tableau Entités PKI.

Liste de révocation de certificats (CRL) NetScaler Gateway

Citrix Endpoint Management prend en charge la liste de révocation de certificats (CRL) uniquement pour une autorité de certification tierce. Si vous disposez d'une autorité de certification Microsoft configurée, Citrix Endpoint Management utilise NetScaler Gateway pour gérer la révocation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Lorsque vous configurez l'authentification basée sur un certificat client, vous devez décider si vous avez besoin de configurer le paramètre Liste de révocation de certificats (CRL) NetScaler Gateway, **Enable CRL Auto Refresh**. Cette étape garantit que l'utilisateur d'un appareil en mode MAM exclusif ne peut pas s'authentifier à l'aide d'un certificat existant sur l'appareil.

Citrix Endpoint Management émet un nouveau certificat, car il n'interdit pas à un utilisateur de générer un certificat utilisateur si un certificat est révoqué. Ce paramètre renforce la sécurité des entités PKI lorsque la CRL vérifie la présence d'entités PKI expirées.

Autorités de certification discrétionnaires

Une autorité de certification discrétionnaire est créée lorsque vous fournissez un certificat d'autorité de certification et la clé privée qui lui est associée à Citrix Endpoint Management. Citrix Endpoint Management gère l'émission, la révocation et les informations d'état en interne des certificats, selon les paramètres que vous spécifiez.

Lorsque vous configurez une autorité de certification discrétionnaire, vous pouvez activer la prise en charge du protocole OCSP pour cette autorité de certification. Si vous activez la prise en charge du protocole OCSP, l'autorité de certification ajoute une extension `id-pe-authorityInfoAccess` aux certificats qu'elle émet. L'extension pointe vers le répondeur OCSP interne de Citrix Endpoint Management à l'emplacement suivant :

```
https://<server>/<instance>/ocsp
```

Lors de la configuration du service OCSP, spécifiez un certificat de signature OCSP pour l'entité discrétionnaire en question. Vous pouvez utiliser le certificat d'autorité de certification lui-même en tant que signataire. Pour éviter la divulgation inutile de la clé privée de votre autorité de certification (recommandé), créez un certificat de signature OCSP délégué, signé par le certificat d'autorité de certification et incluez l'extension suivante : `id-kp-OCSPSigning extendedKeyUsage`.

Le service du répondeur OCSP de Citrix Endpoint Management prend en charge les réponses OCSP de base et les algorithmes de hash suivants utilisés dans les requêtes :

- SHA-256
- SHA-384
- SHA-512

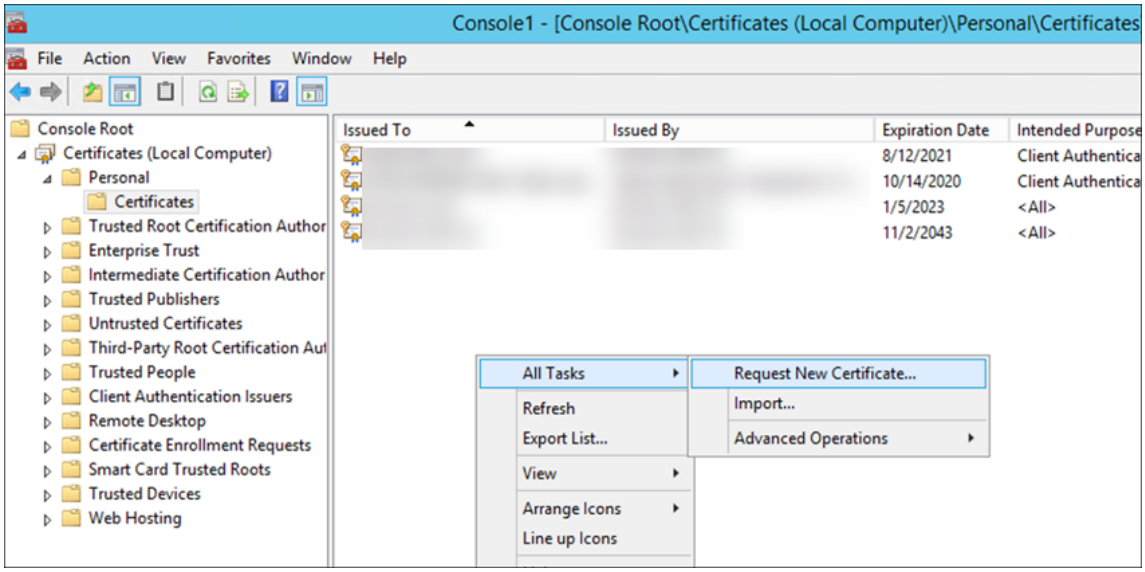
Les réponses sont signées avec SHA-256 et l'algorithme de clé du certificat de signature (DSA, RSA ou ECDSA).

Générer et importer un certificat pour votre autorité de certification

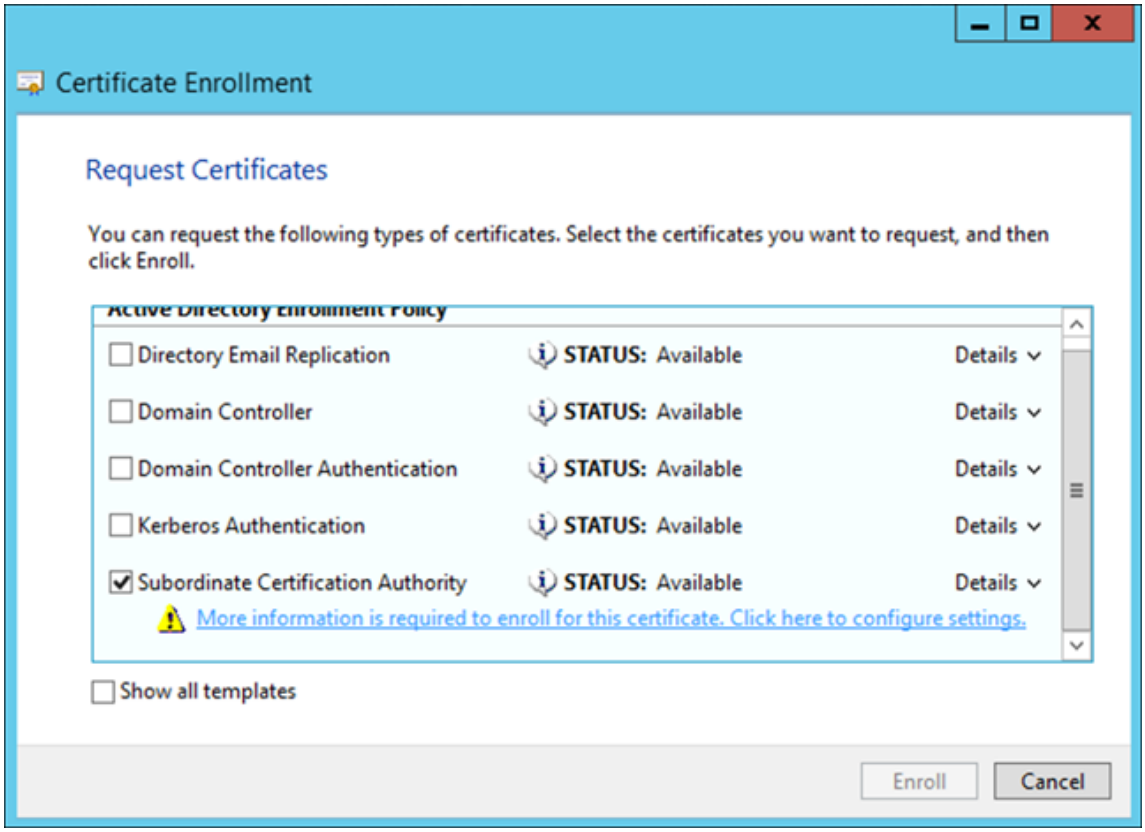
1. Sur votre serveur, ouvrez la console de gestion Microsoft (MMC) avec votre compte Système local et ouvrez le composant logiciel enfichable Certificats. Dans le volet de droite, cliquez avec le

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

bouton droit, puis cliquez sur **Toutes les tâches > Demander un nouveau certificat**.

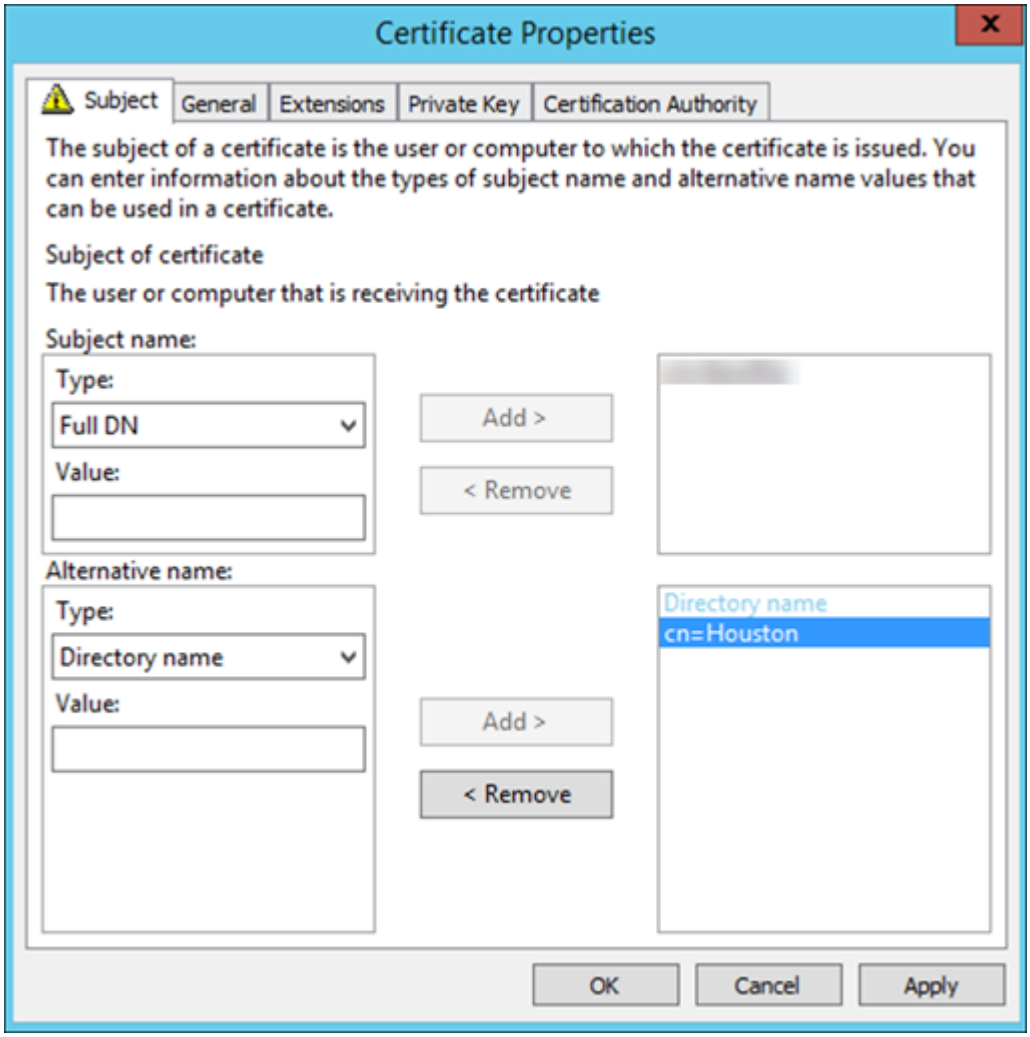


2. Dans l'assistant qui s'ouvre, cliquez deux fois sur **Suivant**. Dans la liste **Demander des certificats**, sélectionnez **Autorité de certification secondaire**, puis cliquez sur le lien **Plus d'informations**.



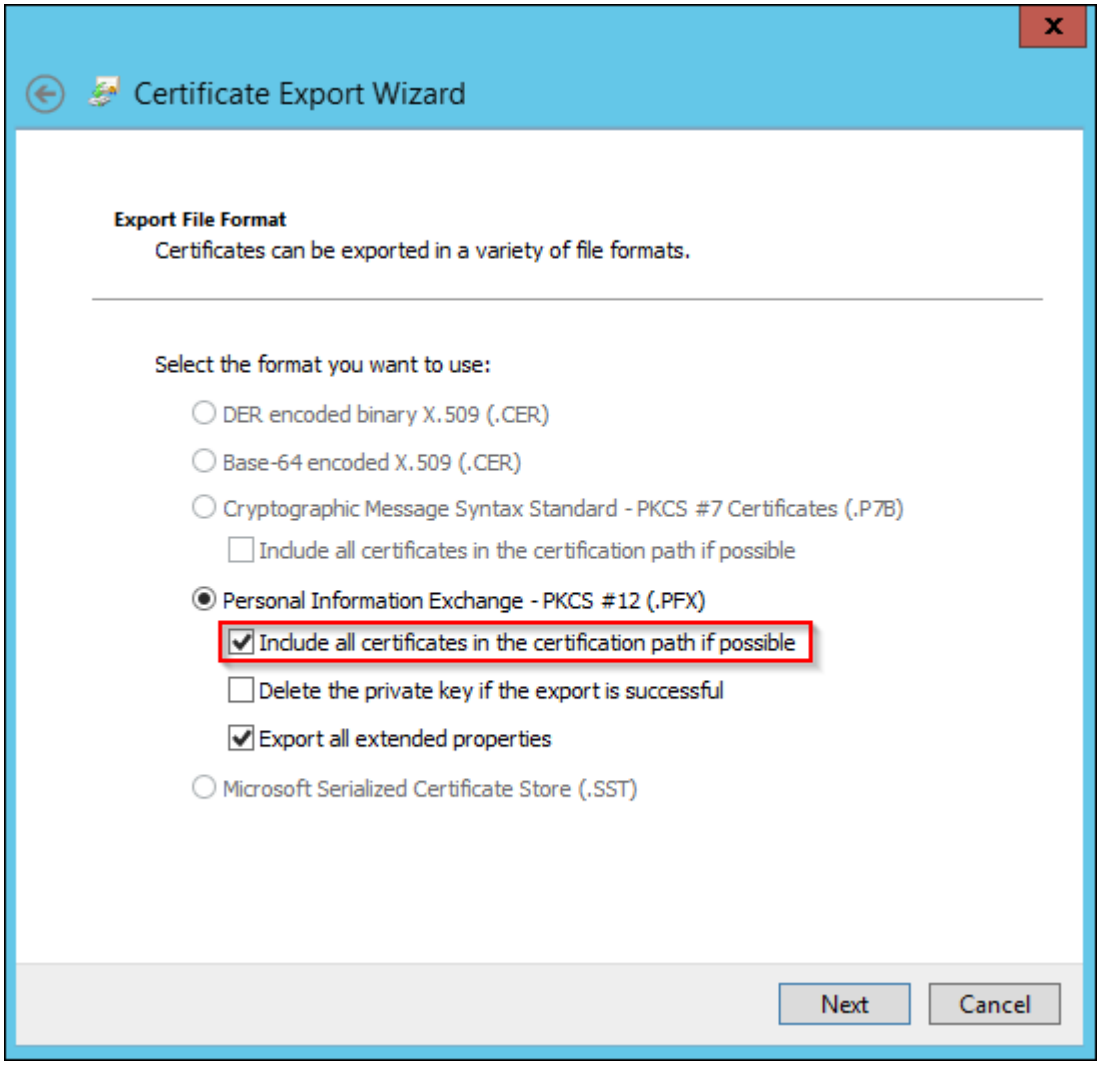
3. Dans la fenêtre, tapez un **nom de sujet** et un **autre nom**. Cliquez sur **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

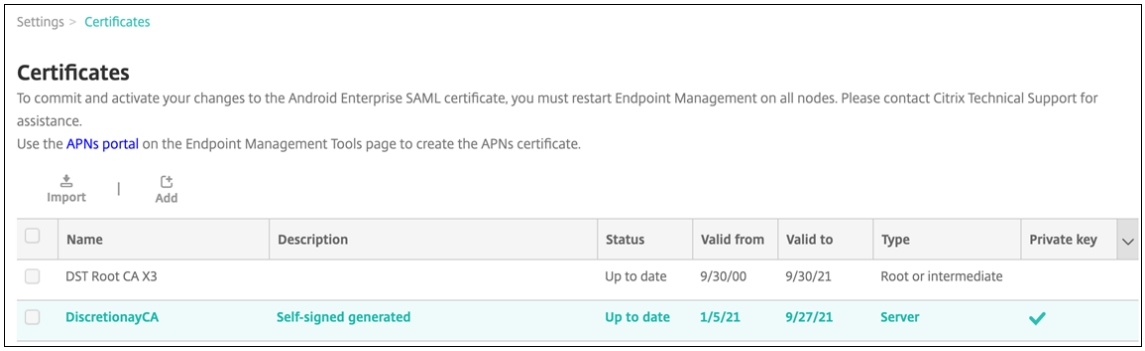


4. Cliquez sur **Inscrire**, puis sur **Terminer**.
5. Dans la console MMC, cliquez avec le bouton droit sur le certificat que vous avez créé. Cliquez sur **Toutes les tâches > Exporter**. Exportez le certificat en tant que fichier .pfx avec une clé privée. Sélectionnez l'option **Inclure tous les certificats dans le chemin d'accès de certification, si possible**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

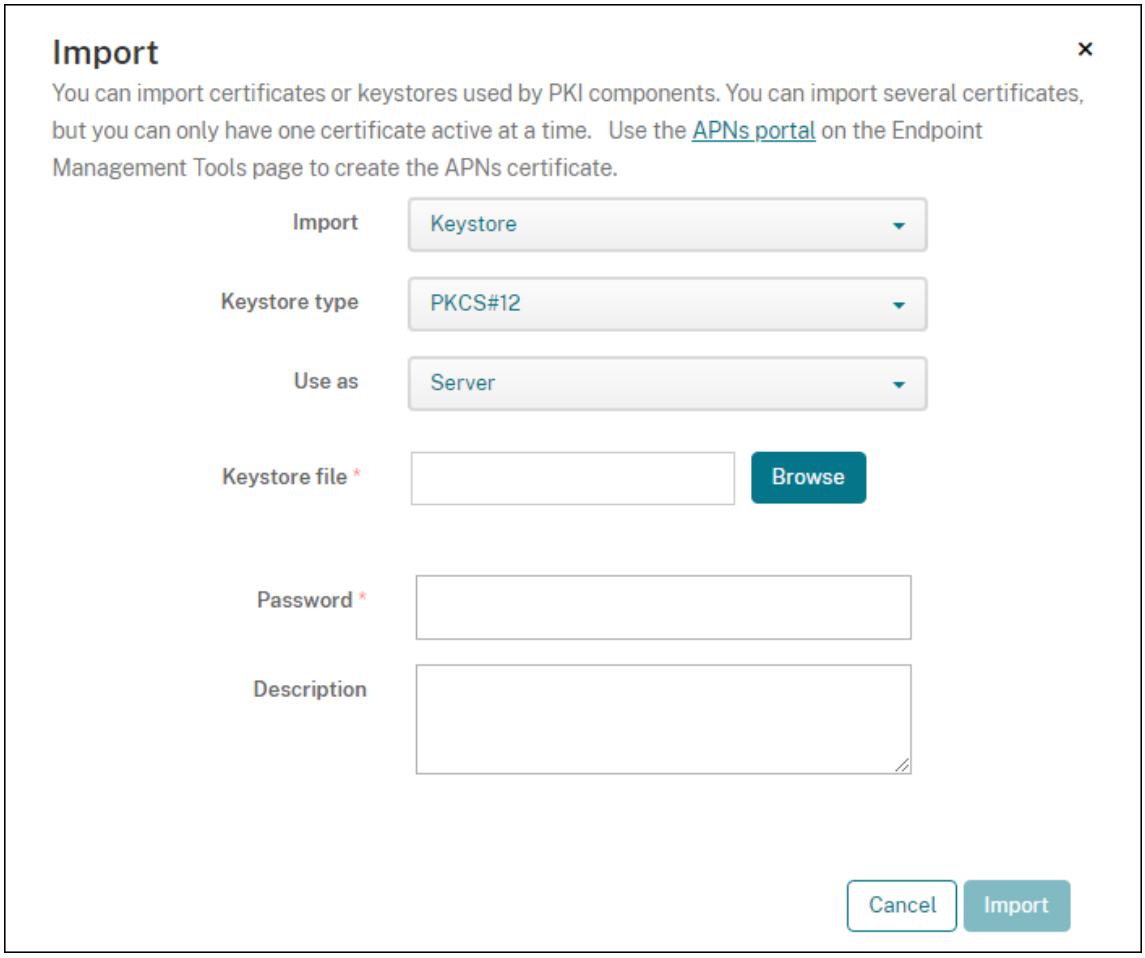


6. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Certificats**.



7. Cliquez sur **Importer**. Dans la fenêtre qui s'ouvre, recherchez les fichiers de certificat et de clé privée que vous avez exportés précédemment.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

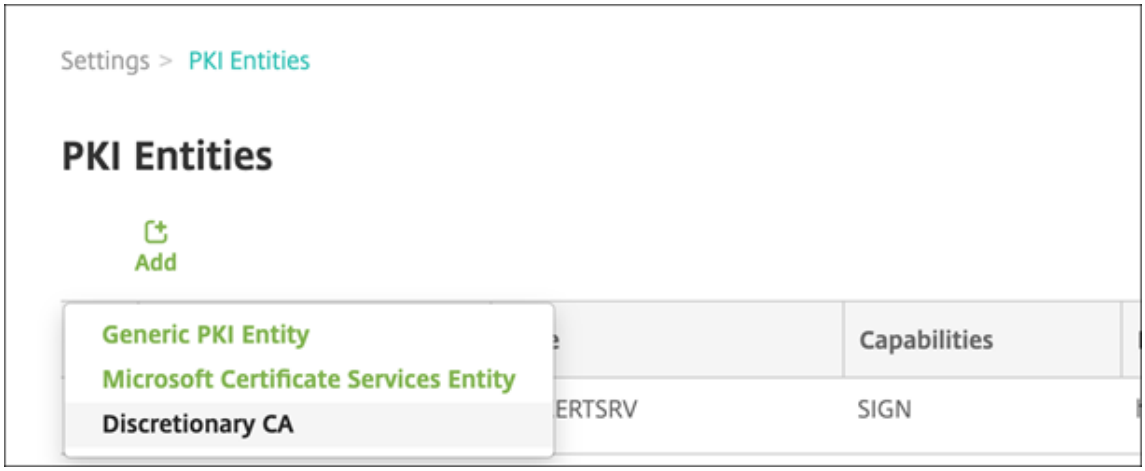


8. Cliquez sur **Importer**. Le certificat est ajouté au tableau.

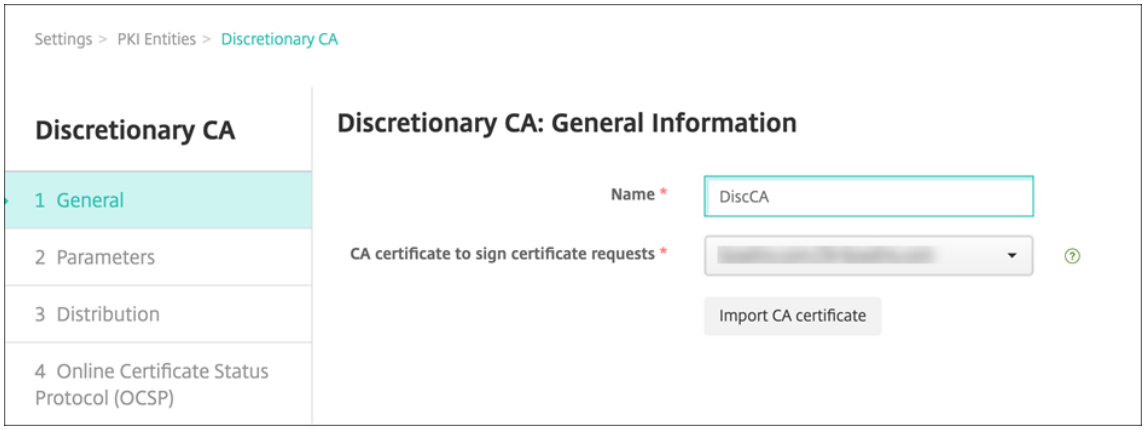
Ajouter des autorités de certification discrétionnaires

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Plus > Entités PKI**.
2. Sur la page **Entités PKI**, cliquez sur **Ajouter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Cliquez sur **CA discrétionnaire**.



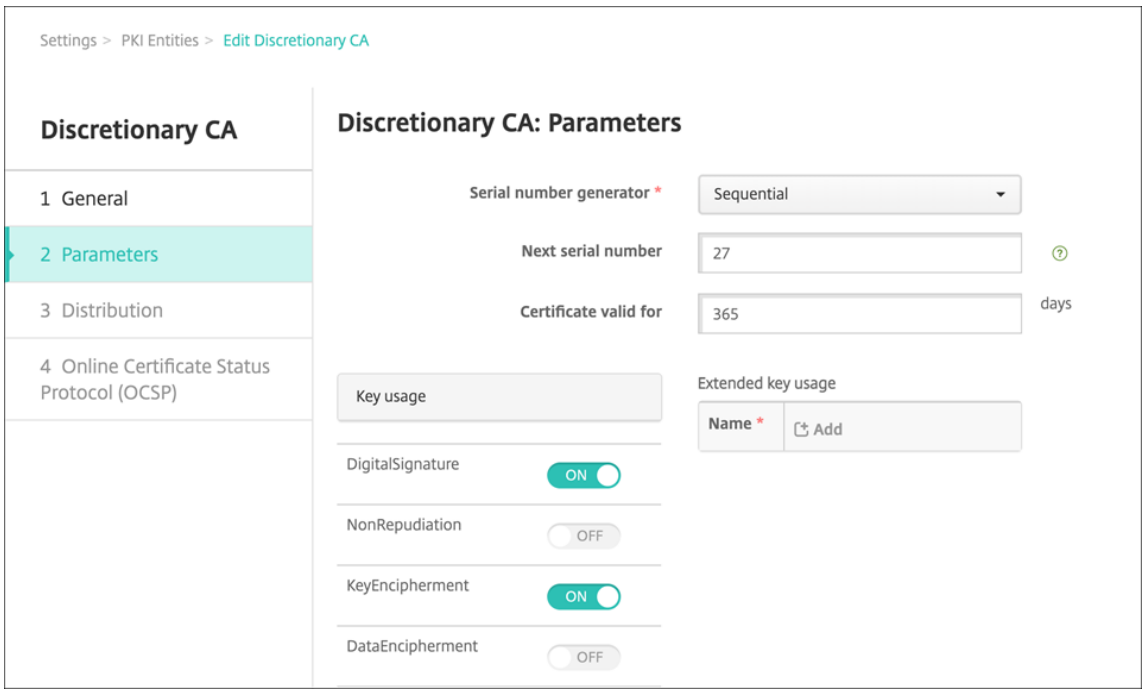
4. Sur la page **CA discrétionnaire : informations générales**, effectuez la configuration suivante :

   - **Nom :** entrez un nom descriptif pour la CA discrétionnaire.
   - **Certificat CA utilisé pour signer les demandes de certificat :** cliquez sur un certificat pour la CA discrétionnaire à utiliser pour signer les demandes de certificats.

     Cette liste de certificats est générée à partir des certificats CA avec des clés privées que vous avez chargées sur Citrix Endpoint Management dans **Configure > Paramètres > Certificats**.

5. Cliquez sur **Suivant**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

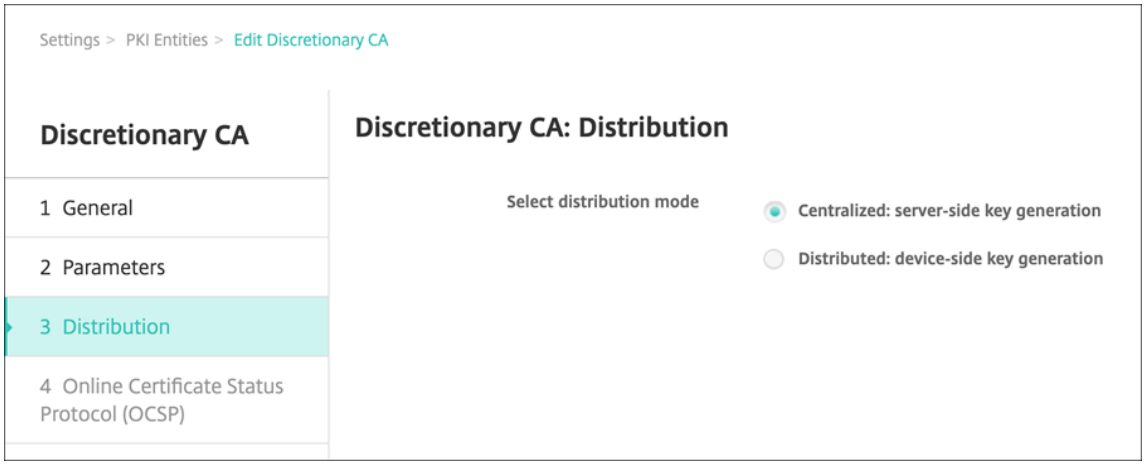


6. Sur la page **CA discrétionnaire : paramètres**, effectuez la configuration suivante :

   - **Générateur de numéro de série :** la CA discrétionnaire génère des numéros de série pour les certificats qu'elle émet. Dans cette liste, cliquez sur **Séquentiel** ou **Non-séquentiel** pour déterminer comment les numéros sont générés.
   - **Numéro de série suivant :** entrez une valeur pour déterminer le numéro suivant émis.
   - **Certificat valide pour :** entrez le nombre de jours pendant lesquels le certificat est valide.
   - **Utilisation de la clé :** identifiez la fonction des certificats émis par l'autorité de certification discrétionnaire en définissant les clés appropriées sur **Activé**. Une fois cette option définie, l'autorité de certification peut uniquement émettre des certificats aux fins susmentionnées.
   - **Utilisation de clé étendue :** pour ajouter d'autres paramètres, cliquez sur **Ajouter**, entrez le nom de clé, puis cliquez sur **Enregistrer**.

7. Cliquez sur **Suivant**.

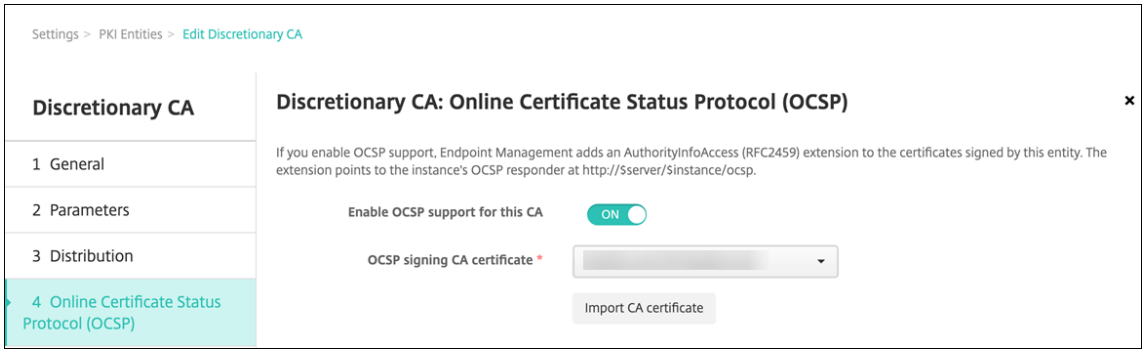
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. Sur la page **CA discrétionnaire : distribution**, sélectionnez un mode de distribution :

   - **Centralisé : génération de la clé sur le serveur**. Citrix recommande l'option centralisée. Les clés privées sont générées et stockées sur le serveur et distribuées sur les appareils des utilisateurs.
   - **Distribué : génération de la clé sur l'appareil**. Les clés privées sont générées sur les appareils des utilisateurs. Ce mode distribué utilise SCEP et requiert un certificat de chiffrement RA avec l'extension **keyUsage keyEncryption** et un certificat de signature RA avec l'extension **keyUsage digitalSignature**. Le même certificat peut être utilisé pour le chiffrement et la signature.

9. Cliquez sur **Suivant**.



10. Sur la page **CA discrétionnaire : protocole OCSP**, effectuez la configuration suivante :

    - Si vous souhaitez ajouter une extension `AuthorityInfoAccess` (RFC2459) pour les certificats signés par cette autorité de certification, définissez **Activer le support d'OCSP pour cette CA** sur **Activé**. Cette extension pointe vers le répondeur OCSP de l'autorité de certification sur `https://<server>/<instance>/ocsp`.
    - Si vous avez activé la prise en charge du protocole OCSP, sélectionnez un certificat d'autorité de certification de signature OSCP. Cette liste de certificats est générée à partir des

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

certificats d'autorité de certification que vous avez chargés sur Citrix Endpoint Management.

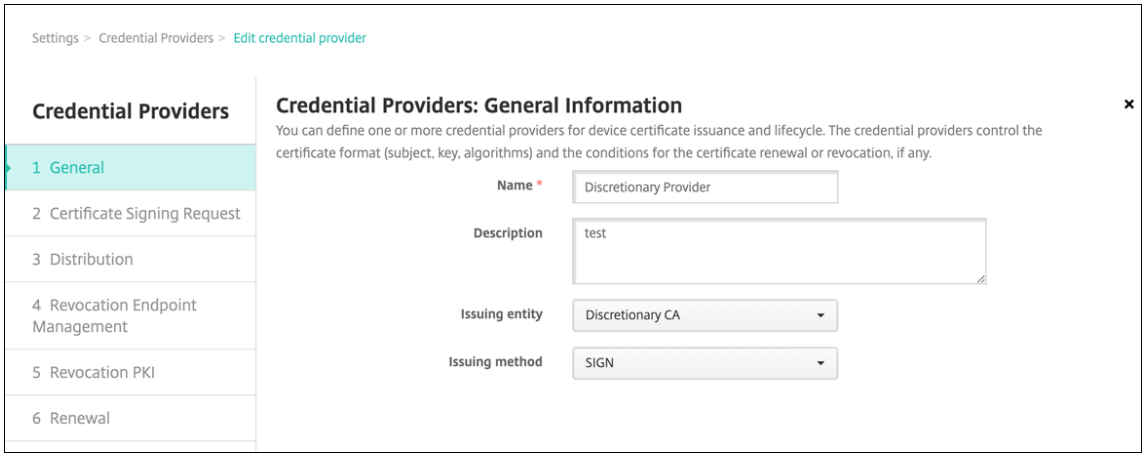
L'activation de la fonctionnalité donne à Citrix ADC la possibilité de vérifier l'état des certificats. Citrix vous recommande d'activer cette fonctionnalité.

11. Cliquez sur **Enregistrer**.

    L'autorité de certification discrétionnaire s'affiche sur le tableau Entités PKI.

Configurer un fournisseur d'informations d'identification

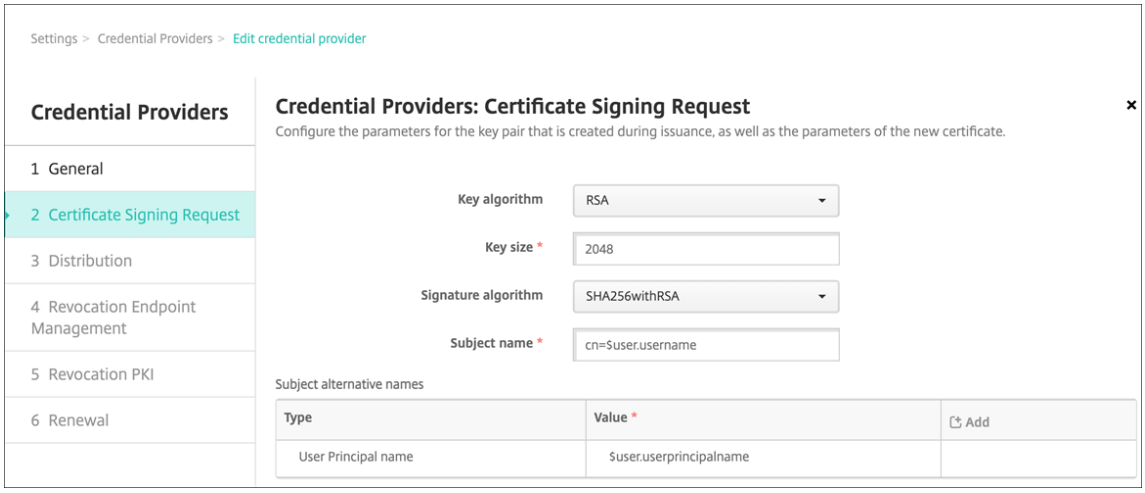
1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Fournisseur d'informations d'identification**, puis cliquez sur **Ajouter**.
2. Sur la page **Fournisseurs d'informations d'identification : informations générales**, effectuez la configuration suivante :



   - **Nom :** entrez un nom unique pour la nouvelle configuration du fournisseur. Ce nom sera utilisé par la suite pour faire référence à la configuration dans d'autres parties de la console Citrix Endpoint Management.
   - **Description :** décrivez le fournisseur d'identités. Bien que ce champ soit facultatif, une description peut être utile pour vous fournir des détails sur ce fournisseur d'identités.
   - **Entité émettrice :** sélectionnez **CA discrétionnaire**.
   - **Méthode d'émission :** cliquez sur **Signer** ou **Récupérer** pour choisir la méthode que le système utilise pour obtenir des certificats auprès de l'entité configurée. Pour l'authentification de certificat client, utilisez **Signer**.

3. Cliquez sur **Suivant**. Sur la page **Fournisseurs d'identités : demande de signature de certificat**, configurez les éléments suivants en fonction de votre configuration de certificat :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Algorithme de clé :** choisissez l'algorithme de clé pour la nouvelle paire de clés. Les valeurs disponibles sont **RSA**, **DSA** et **ECDSA**.
- **Taille de la clé :** entrez la taille en octets de la paire de clés. Ce champ est obligatoire. Citrix recommande d'utiliser **2048** bits.
- **Algorithme de signature :** cliquez sur une valeur pour le nouveau certificat. Les valeurs dépendent de l'algorithme de clé. Citrix recommande **SHA256WithRSA**.
- **Nom du sujet :** obligatoire. Tapez le nom unique (DN) du sujet du nouveau certificat. Utilisez `CN=${ user.username }` pour le nom d'utilisateur ou `CN=${ user.samaccountname }` pour utiliser sAMAccountName.
- Pour ajouter une entrée à la table **Noms de sujet alternatifs**, cliquez sur **Ajouter**. Sélectionnez le type de nom alternatif, puis tapez une valeur dans la deuxième colonne.

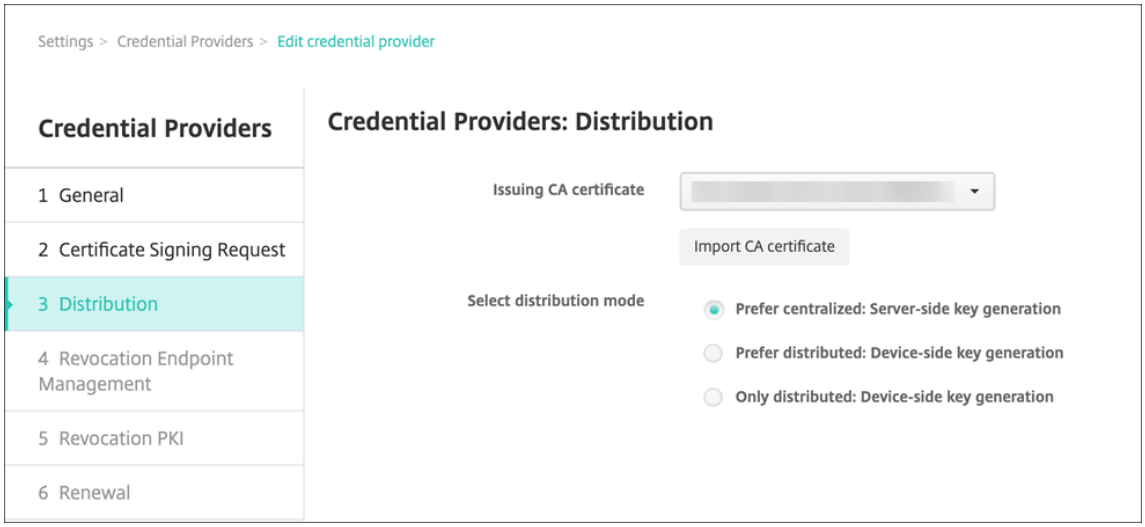
  Ajoutez ce qui suit :

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

  Comme avec le nom du sujet, vous pouvez utiliser les macros Citrix Endpoint Management dans le champ de valeur.

4. Cliquez sur **Suivant**. Sur la page **Fournisseurs d'informations d'identification : distribution**, effectuez la configuration suivante :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

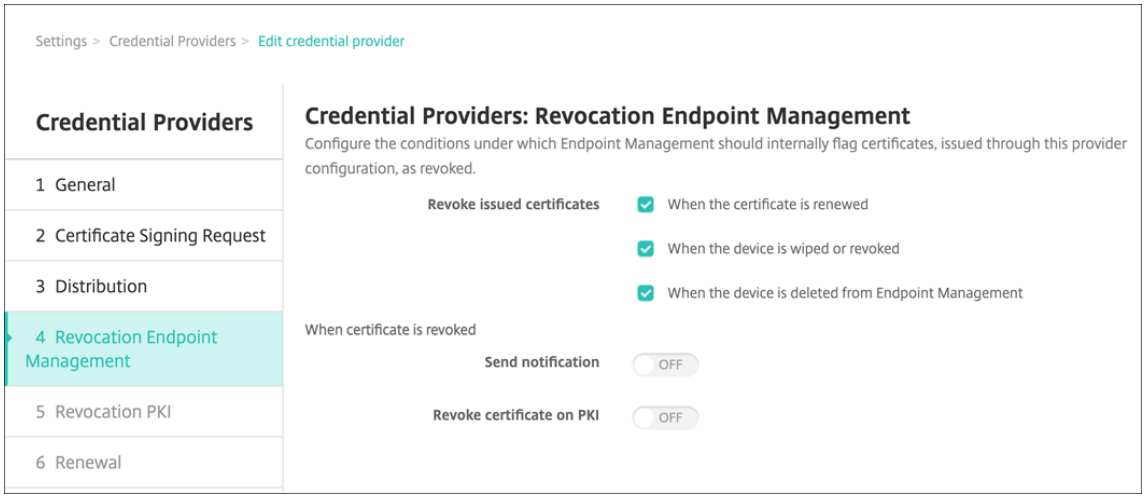


- **Certificat émis par l'autorité de certification :** sélectionnez le certificat d'autorité de certification discrétionnaire que vous avez ajouté précédemment.
- Dans **Sélectionner le mode de distribution**, sélectionnez l'une des méthodes de génération et de distribution de clés :
  - **Préférer mode centralisé : génération de la clé sur le serveur :** Citrix recommande cette option centralisée. Ce mode prend en charge toutes les plates-formes prises en charge par Citrix Endpoint Management et est requis lors de l'utilisation de l'authentification NetScaler Gateway. Les clés privées sont générées et stockées sur le serveur et distribuées sur les appareils des utilisateurs.
  - **Préférer mode distribué : génération de la clé sur l'appareil.** Les clés privées sont générées et stockées sur les appareils des utilisateurs. Ce mode distribué utilise SCEP et requiert un certificat de chiffrement RA avec le keyUsage keyEncryption et un certificat de signature RA avec le KeyUsage digitalSignature. Le même certificat peut être utilisé pour le chiffrement et la signature.
  - **Distribué uniquement : génération de la clé sur l'appareil :** cette option fonctionne de la même façon que **Préférer mode distribué : génération de la clé sur l'appareil**, sauf qu'aucune option n'est disponible si la génération de la clé sur l'appareil échoue.

Si vous avez sélectionné **Préférer mode distribué : génération de la clé sur l'appareil** ou **Distribué uniquement : génération de la clé sur l'appareil**, cliquez sur le certificat de signature RA et le certificat de chiffrement RA. Le même certificat peut être utilisé pour les deux modes. De nouveaux champs apparaissent pour ces certificats.

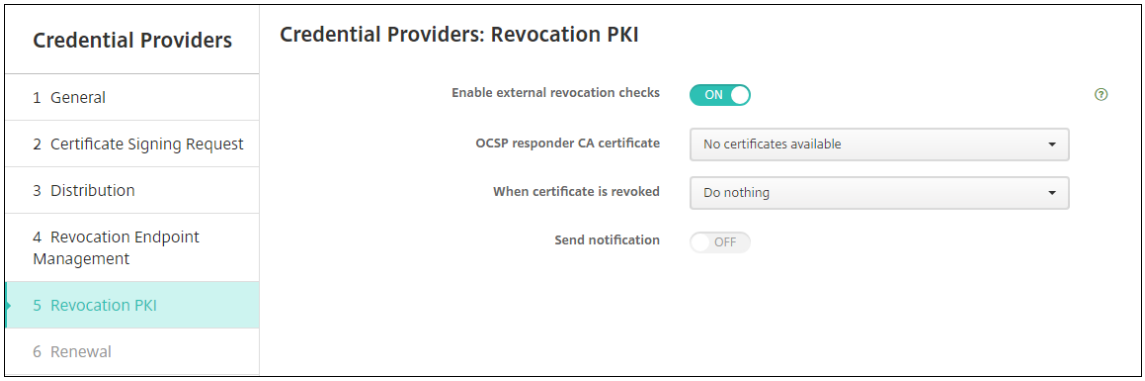
5. Cliquez sur **Suivant**. Sur la page **Fournisseurs d'informations d'identification : Révocation Citrix Endpoint Management**, vous configurez les conditions dans lesquelles Citrix Endpoint Management marque (en interne) comme révoqué les certificats émis au travers de cette configuration de fournisseur. Configurez ce qui suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Dans **Révoquer les certificats émis**, sélectionnez l'une des options qui indique quand les certificats doivent être révoqués.
- Si vous voulez que Citrix Endpoint Management envoie une notification lorsque le certificat est révoqué, définissez la valeur de **Envoyer une notification** sur **Activé** et choisissez un modèle de notification.
- L'option **Révoquer le certificat auprès de la PKI** ne fonctionne pas lorsque vous utilisez Citrix Endpoint Management en tant que PKI discrétionnaire.

6. Cliquez sur **Suivant**. Sur la page **Fournisseurs d'informations d'identification : PKI de révocation**, identifiez les actions à effectuer sur la PKI si le certificat est révoqué. Vous avez aussi la possibilité de créer un message de notification. Configurez ce qui suit :



- **Activer les vérifications de révocation externe :** définissez sur **Activer**. Des champs supplémentaires liés à la PKI de révocation apparaissent.
- Dans la liste **Certificat CA du répondeur OCSP**, sélectionnez le nom unique (DN) du sujet du certificat.

  Vous pouvez utiliser les macros Citrix Endpoint Management pour les valeurs de champ de nom unique. Pa exemple : `CN=${ user.username } , OU=${`

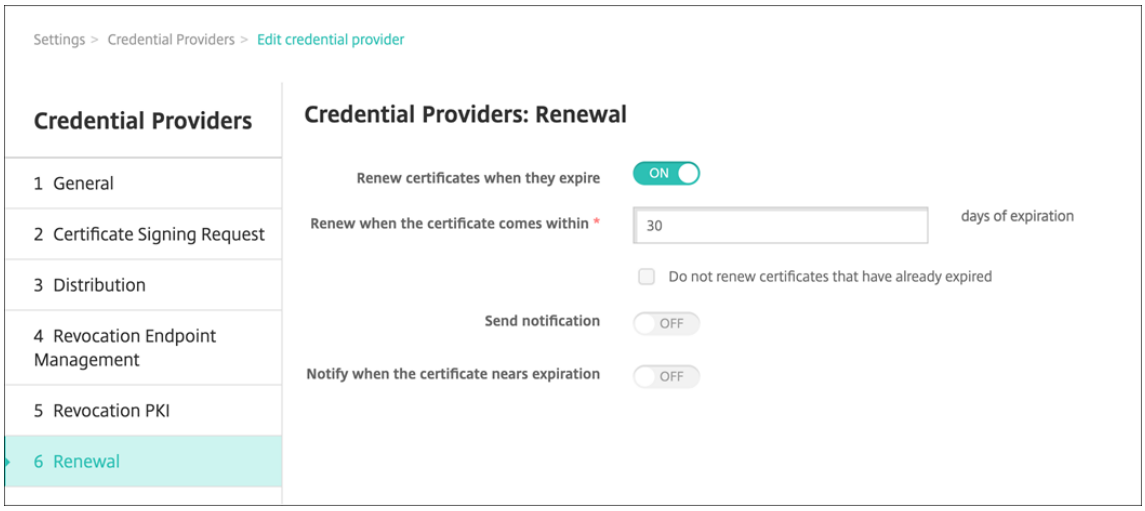
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
user.department } , O=${ user.companyname } , C=${ user.c } \
endquotation
```

- Dans la liste **Lorsque le certificat est révoqué**, cliquez sur l'une des actions suivantes à entreprendre sur l'entité PKI lorsque le certificat est révoqué :
  - Ne rien faire.
  - Renouveler le certificat.
  - Révoquer et de réinitialiser l'appareil.
- Si vous voulez que Citrix Endpoint Management envoie une notification lorsque le certificat est révoqué, définissez la valeur de **Envoyer une notification** sur **Activé**.

  Vous avez le choix entre deux options de notification :
  - Si vous sélectionnez **Sélectionner un modèle de notification**, vous pouvez sélectionner un message de notification pré-rempli que vous pouvez personnaliser. Ces modèles figurent dans la liste Modèle de notification.
  - Si vous sélectionnez **Entrer les détails de notification**, vous pouvez créer votre propre message de notification. En plus de fournir l'adresse e-mail du destinataire et le message, vous pouvez définir la fréquence à laquelle la notification est envoyée.

7. Cliquez sur **Suivant**. Sur la page **Fournisseurs d'informations d'identification : renouvellement**, effectuez la configuration suivante :



Réglez **Renouveler les certificats lorsqu'ils expirent** sur **Activé**. Des champs supplémentaires apparaissent.

- Dans le champ **Renouveler lorsque le certificat expire dans**, entrez quand le renouvellement doit être effectué, en nombre de jours avant l'expiration.
- Si vous le souhaitez, sélectionnez **Ne pas renouveler les certificats expirés**. Dans ce cas, « expiré » signifie que la date `NotAfter` (fin de validité) est dans le passé, et non pas qu'

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

il a été révoqué. Citrix Endpoint Management ne renouvelle pas les certificats après leur révocation interne.

Si vous voulez que Citrix Endpoint Management envoie une notification lorsque le certificat a été renouvelé, définissez **Envoyer une notification** sur **Activé**. Si vous voulez que Citrix Endpoint Management envoie une notification lorsque la certification arrive à échéance, définissez **Notifier quand un certificat va expirer** sur **Activé**.
Dans tous les cas, vous avez le choix entre deux options de notification :

- **Sélectionner un modèle de notification :** sélectionnez un message de notification prérempli que vous pouvez personnaliser. Ces modèles figurent dans la liste Modèle de notification.
- **Entrer les détails de notification :** créez votre propre message de notification. Indiquez l'adresse e-mail du destinataire, un message et la fréquence d'envoi de la notification.

8. Cliquez sur **Enregistrer**.

Fournisseur d'identités

March 1, 2024

Les Fournisseurs d'informations d'identification sont les configurations de certificat réelles que vous utilisez dans différentes parties du système Citrix Endpoint Management. Les fournisseurs d'informations d'identification définissent les sources, les paramètres et les cycles de vie de vos certificats. Ces opérations se produisent que les certificats fassent partie des configurations de l'appareil ou soient autonomes (c'est-à-dire, envoyés tels quels sur l'appareil).

L'inscription d'appareil limite le cycle de vie du certificat. En effet, Citrix Endpoint Management ne délivre pas de certificats avant l'inscription, bien qu'il puisse en émettre certains dans le cadre de l'inscription. En outre, les certificats émis par la PKI interne dans le cadre d'une inscription sont révoqués lorsque l'inscription est révoquée. Après la fin de la relation de gestion, aucun certificat valide n'est conservé.

Une configuration de fournisseur d'identités peut être utilisée à plusieurs endroits, par conséquent une configuration peut régir un grand nombre de certificats simultanément. L'unité existe alors sur la ressource de déploiement et le déploiement. Par exemple, si le fournisseur d'identités P est déployé sur l'appareil D dans le cadre de la configuration C : les paramètres d'émission pour P déterminent le certificat qui est déployé sur D. De même, les paramètres de renouvellement pour D s'appliquent lorsque C est mis à jour. Les paramètres de révocation pour D s'appliquent également lorsque C est supprimé ou que D est révoqué.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Selon ces règles, la configuration du fournisseur d'identités détermine ce qui suit dans Citrix Endpoint Management :

- La source des certificats.
- La méthode grâce à laquelle les certificats sont obtenus : signature d'un nouveau certificat ou récupération d'un certificat existant et d'une paire de clés.
- Les paramètres d'émission ou de récupération. Par exemple, les paramètres de demande de signature de certificat (CSR), tels que la taille de la clé, l'algorithme de clé et les extensions de certificat.
- La façon dont les certificats sont mis à disposition sur l'appareil.
- Les conditions de révocation. Bien que tous les certificats soient révoqués dans Citrix Endpoint Management lorsque la relation de gestion est rompue, la configuration peut spécifier une révocation antérieure. Par exemple, la configuration peut spécifier de révoquer un certificat lorsque la configuration d'appareil associée est supprimée. En outre, dans certaines conditions, il se peut que la révocation du certificat associé dans Citrix Endpoint Management puisse être envoyée à l'infrastructure interne à clé publique (PKI) principale. Autrement dit, la révocation de certificats dans Citrix Endpoint Management peut entraîner la révocation de certificats sur la PKI.
- Les paramètres de renouvellement. Les certificats obtenus via un fournisseur d'informations d'identification donné peuvent être automatiquement renouvelés lorsqu'ils arrivent à expiration. Ou, des notifications peuvent être émises lorsque cette expiration approche.

La disponibilité des options de configuration dépend principalement du type d'entité PKI et de la méthode d'émission que vous sélectionnez pour un fournisseur d'identités.

Méthode d'émission de certificats

Vous pouvez obtenir un certificat, connu sous le nom de méthode d'émission, par signature.

Avec cette méthode, l'émission implique la création d'une nouvelle clé privée, la création d'une demande de signature de certificat (CSR) et la soumission de la demande de signature de certificat à une autorité de certification (CA) pour signature. Citrix Endpoint Management prend en charge la méthode de signature pour les entités Services de certificats Microsoft et les entités CA discrétionnaires.

Un fournisseur d'identités utilise la méthode d'émission par signature.

Mise à disposition de certificats

Deux modes de mise à disposition de certificats sont disponibles dans Citrix Endpoint Management : centralisée et distribuée. Le mode Distribué utilise le protocole d'inscription du certificat simple (SCEP) et est uniquement disponible dans les situations dans lesquelles le client prend en charge le protocole (iOS uniquement). Le mode distribué est obligatoire dans certains cas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour qu'un fournisseur d'identités prenne en charge la mise à disposition (assisté par SCEP) distribuée, une étape de configuration spéciale est nécessaire : configuration des certificats de l'autorité d'inscription (RA). Les certificats RA sont requis, car lors de l'utilisation du protocole SCEP, Citrix Endpoint Management agit comme un délégué (registre) pour l'autorité de certification réelle. Citrix Endpoint Management doit prouver au client qu'il dispose de l'autorité d'agir en tant que tel. Cette autorité est établie par le chargement vers Citrix Endpoint Management des certificats mentionnés plus haut.

Deux rôles de certificat distincts sont requis (bien qu'un seul certificat puisse remplir les deux rôles) : la signature RA et le chiffrement RA. Les contraintes pour ces rôles sont les suivantes :

- Le certificat de signature RA doit posséder une signature numérique d'utilisation de clé X.509.
- Le certificat de chiffrement RA doit posséder un chiffrement de clé d'utilisation de clé X.509.

Pour configurer les certificats RA du fournisseur d'identités, vous chargez les certificats sur Citrix Endpoint Management, puis les associer au fournisseur d'identités.

Un fournisseur d'identités est considéré comme pouvant uniquement prendre en charge une mise à disposition distribuée s'il possède un certificat configuré pour les rôles de certificat. Vous pouvez configurer chaque fournisseur d'identités pour privilégier au choix le mode centralisé, le mode distribué ou pour requérir le mode distribué. Le résultat réel dépend du contexte : si le contexte ne prend pas en charge le mode distribué, mais que le fournisseur d'identités requiert ce mode, le déploiement échoue. De même, si le contexte requiert le mode distribué, mais que le fournisseur d'identités ne le prend pas en charge, le déploiement échoue. Dans tous les autres cas, le paramètre préféré est appliqué.

Le tableau suivant présente la distribution SCEP via Citrix Endpoint Management :

Contexte	SCEP pris en charge	SCEP requis
Service de profil iOS	Oui	Oui
Inscription à la gestion des appareils mobiles iOS	Oui	Non
Profils de configuration iOS	Oui	Non
Inscription SHTP	Non	Non
Configuration de SHTP	Non	Non
Inscription de Windows Tablet	Non	Non
Configuration de Windows Tablet	Non, à l'exception de la stratégie de réseau qui est prise en charge pour Windows 10 et Windows 11	Non

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Révocation de certificats

Il existe trois types de révocation.

- **Révocation interne :** la révocation interne du certificat affecte le statut du certificat géré par Citrix Endpoint Management. Citrix Endpoint Management vérifie ce statut lors de l'évaluation d'un certificat présenté ou lors de la fourniture d'informations de statut OCSP pour un certificat. La configuration du fournisseur d'identités détermine la manière dont le statut est affecté par plusieurs conditions. Par exemple, le fournisseur d'identités peut spécifier que les certificats soient marqués comme révoqués lorsqu'ils ont été supprimés de l'appareil.
- **Révocation propagée en externe :** également appelée révocation Citrix Endpoint Management, ce type de révocation s'applique aux certificats obtenus à partir d'une PKI externe. Le certificat est révoqué sur la PKI lorsque le certificat est révoqué en interne par Citrix Endpoint Management, sous les conditions définies par la configuration du fournisseur d'identités.
- **Révocation induite en interne :** également appelée PKI de révocation, ce type de révocation s'applique uniquement aux certificats obtenus à partir d'une PKI externe. Chaque fois que Citrix Endpoint Management évalue le statut d'un certificat donné, Citrix Endpoint Management interroge la PKI afin de déterminer ce statut. Si le certificat est révoqué, Citrix Endpoint Management révoque le certificat en interne. Ce mécanisme utilise le protocole OCSP.

Ces trois types ne sont pas exclusifs, mais s'appliquent ensemble. Une révocation externe ou une observation indépendante peut entraîner une révocation interne. Une révocation interne affecte potentiellement une révocation externe.

Renouvellement de certificat

Un renouvellement du certificat est la combinaison de révocation d'un certificat existant et de l'émission d'un autre certificat.

Citrix Endpoint Management tente tout d'abord d'obtenir le nouveau certificat avant de révoquer le certificat précédent, afin d'éviter une discontinuité du service lorsque l'émission échoue. Pour la mise à disposition distribuée (prise en charge par SCEP), la révocation ne se produit également qu'une fois le certificat installé sur l'appareil. Sinon, la révocation a lieu avant que le nouveau certificat soit envoyé à l'appareil. Cette révocation est indépendante du succès ou de l'échec de l'installation du certificat.

La configuration de la révocation nécessite que vous spécifiiez une certaine durée (en jours). Lorsque l'appareil se connecte, le serveur vérifie que la date du certificat `NotAfter` est postérieure à la date actuelle, moins la durée spécifiée. Si le certificat remplit cette condition, Citrix Endpoint Management tente de renouveler le certificat.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Créer un fournisseur d'identités

La configuration d'un fournisseur d'identités varie principalement en fonction de l'entité d'émission et de la méthode d'émission sélectionnées pour le fournisseur d'identités. Vous pouvez faire la distinction entre les fournisseurs d'identités qui utilisent une entité interne ou une entité externe :

- Une entité discrétionnaire, qui est interne à Citrix Endpoint Management, est une entité interne. La méthode d'émission pour une entité discrétionnaire est toujours la signature. La signature signifie qu'avec chaque opération d'émission, Citrix Endpoint Management signe une nouvelle paire de clés avec le certificat d'autorité de certification sélectionné pour l'entité. L'emplacement où la paire de clés est générée (l'appareil où le serveur) dépend de la méthode de distribution sélectionnée.
- Une entité externe, qui fait partie de votre infrastructure d'entreprise, inclut une autorité de certification Microsoft.

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit, puis cliquez sur **Paramètres > Fournisseurs d'informations d'identification**.
2. Sur la page **Fournisseurs d'informations d'identification**, cliquez sur **Ajouter**.

   La page **Fournisseurs d'informations d'identification : informations générales** s'affiche.
3. Sur la page **Fournisseurs d'informations d'identification : informations générales**, procédez comme suit :

   - **Nom :** entrez un nom unique pour la nouvelle configuration du fournisseur. Ce nom sera utilisé par la suite pour faire référence à la configuration dans d'autres parties de la console Citrix Endpoint Management.
   - **Description :** décrivez le fournisseur d'identités. Bien que ce champ soit facultatif, une description peut être utile pour vous fournir des détails sur ce fournisseur d'identités.
   - **Entité émettrice :** cliquez sur l'entité qui émet le certificat.
   - **Méthode d'émission :** cliquez sur **Signer** ou **Récupérer** pour choisir la méthode que le système utilise pour obtenir des certificats auprès de l'entité configurée. Pour l'authentification de certificat client, utilisez **Signer**.
   - Si la liste **Modèle** est disponible, sélectionnez le modèle que vous avez ajouté sous l'entité PKI pour le fournisseur d'identités.

     Ces modèles deviennent disponibles lorsque les entités Services de certificats Microsoft sont ajoutées sur **Paramètres > Entités PKI**.
4. Cliquez sur **Suivant**.

   La page **Fournisseur d'identités : demande de signature de certificat** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Sur la page **Fournisseurs d'identités : demande de signature de certificat**, configurez les éléments suivants en fonction de votre configuration de certificat :

   - **Algorithme de clé :** choisissez l'algorithme de clé pour la nouvelle paire de clés. Les valeurs disponibles sont **RSA**, **DSA** et **ECDSA**.
   - **Taille de la clé :** entrez la taille en octets de la paire de clés. Ce champ est obligatoire.

     Les valeurs autorisées dépendent du type de clé. Par exemple, la taille maximale des clés DSA est de 2048 bits. Pour éviter de faux résultats négatifs, qui dépendent du matériel ou du logiciel sous-jacent, Citrix Endpoint Management n'exige pas l'utilisation d'une taille de clé particulière. Vous devez toujours tester les configurations de fournisseur d'identités dans un environnement de test avant de les activer dans un environnement de production.
   - **Algorithme de signature :** cliquez sur une valeur pour le nouveau certificat. Les valeurs dépendent de l'algorithme de clé.
   - **Nom du sujet :** obligatoire. Tapez le nom unique (DN) du sujet du nouveau certificat. Par exemple :
     `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } ,C=${ user.c } \endquotation`

     For example, for client certificate authentication, use these settings:

     - **Key algorithm:** RSA
     - **Key size:** 2048
     - **Signature algorithm:** SHA256withRSA
     - **Subject name:** `cn=$user.username`
   - Pour ajouter une entrée à la table **Noms de sujet alternatifs**, cliquez sur **Ajouter**. Sélectionnez le type de nom alternatif, puis tapez une valeur dans la deuxième colonne.

     Pour l'authentification du certificat client, spécifiez :

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

       Comme avec le nom du sujet, vous pouvez utiliser les macros Citrix Endpoint Management dans le champ de valeur.

6. Cliquez sur **Suivant**.

   La page **Fournisseurs d'informations d'identification : distribution** s'affiche.

7. Sur la page **Fournisseurs d'informations d'identification : distribution**, procédez comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Dans la liste **Certificat émis par l'autorité de certification**, cliquez sur le certificat d'autorité de certification proposé. Étant donné que le fournisseur d'identités utilise une entité d'autorité de certification discrétionnaire, le certificat d'autorité de certification du fournisseur d'identités sera toujours le certificat d'autorité de certification configuré sur l'entité elle-même. Le certificat d'autorité de certification est présenté ici pour des raisons de cohérence avec les configurations utilisant des entités externes.
- Dans **Sélectionner le mode de distribution**, sélectionnez l'une des méthodes de génération et de distribution de clés :
  - **Préférer mode centralisé : génération de la clé sur le serveur :** Citrix recommande cette option centralisée. Ce mode prend en charge toutes les plates-formes prises en charge par Citrix Endpoint Management et est requis lors de l'utilisation de l'authentification NetScaler Gateway. Les clés privées sont générées et stockées sur le serveur et distribuées sur les appareils des utilisateurs.
  - **Préférer mode distribué : génération de la clé sur l'appareil.** Les clés privées sont générées et stockées sur les appareils des utilisateurs. Ce mode distribué utilise SCEP et requiert un certificat de chiffrement RA avec le keyUsage keyEncryption et un certificat de signature RA avec le KeyUsage digitalSignature. Le même certificat peut être utilisé pour le chiffrement et la signature.
  - **Distribué uniquement : génération de la clé sur l'appareil :** cette option fonctionne de la même façon que Préférer mode distribué : génération de la clé sur l'appareil, sauf qu'étant « Uniquement » au lieu de « Préférer », aucune option n'est disponible si la génération de la clé sur l'appareil échoue.

Si vous avez sélectionné **Préférer mode distribué : génération de la clé sur l'appareil** ou **Distribué uniquement : génération de la clé sur l'appareil**, cliquez sur le certificat de signature RA et le certificat de chiffrement RA. Le même certificat peut être utilisé pour les deux modes. De nouveaux champs apparaissent pour ces certificats.

8. Cliquez sur **Suivant**.

   La page **Fournisseurs d'informations d'identification : révocation Citrix Endpoint Management** s'affiche. Sur cette page, vous configurez les conditions dans lesquelles Citrix Endpoint Management marque (en interne) comme révoqué les certificats émis au travers de cette configuration de fournisseur.

9. Sur la page **Fournisseurs d'informations d'identification : révocation Citrix Endpoint Management**, procédez comme suit :

   - Dans **Révoquer les certificats émis**, sélectionnez l'une des options qui indique quand les certificats doivent être révoqués.
   - Si vous voulez que Citrix Endpoint Management envoie une notification lorsque le certificat est révoqué, définissez la valeur de **Envoyer une notification** sur **Activé** et choisissez

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

un modèle de notification.

- Si vous souhaitez révoquer le certificat sur la PKI lorsque le certificat est révoqué de Citrix Endpoint Management, définissez **Révoquer le certificat** auprès de la PKI sur **Activé** et cliquez sur un modèle dans la liste **Entité**. La liste Entité répertorie toutes les entités disponibles avec des capacités de révocation. Lorsque le certificat est révoqué de Citrix Endpoint Management, une demande de révocation est envoyée à la PKI sélectionnée à partir de la liste Entité.

10. Cliquez sur **Suivant**.

    La page **Fournisseurs d'informations d'identification : révocation PKI** s'affiche. Sur cette page, identifiez les actions à effectuer sur la PKI si le certificat est révoqué. Vous avez aussi la possibilité de créer un message de notification.

11. Sur la page **Fournisseurs d'informations d'identification : révocation PKI**, procédez comme suit si vous souhaitez révoquer les certificats de la PKI :

    - Modifiez le paramètre **Activer les vérifications de révocation externe** sur **Activé**. Des champs supplémentaires liés à la PKI de révocation apparaissent.
    - Dans la liste **Certificat CA du répondeur OCSP**, cliquez sur le nom unique (DN) du sujet du certificat.

      Vous pouvez utiliser les macros Citrix Endpoint Management pour les valeurs de champ de nom unique. Pa exemple : `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \ endquotation`

    - Dans la liste **Lorsque le certificat est révoqué**, cliquez sur l'une des actions suivantes à entreprendre sur l'entité PKI lorsque le certificat est révoqué :
      - Ne rien faire.
      - Renouveler le certificat.
      - Révoquer et de réinitialiser l'appareil.
    - Si vous voulez que Citrix Endpoint Management envoie une notification lorsque le certificat est révoqué, définissez la valeur de **Envoyer une notification** sur **Activé**.

      Vous avez le choix entre deux options de notification :

    - Si vous sélectionnez **Sélectionner un modèle de notification**, vous pouvez sélectionner un message de notification pré-rempli que vous pouvez personnaliser. Ces modèles figurent dans la liste Modèle de notification.
    - Si vous sélectionnez **Entrer les détails de notification**, vous pouvez créer votre propre message de notification. En plus de fournir l'adresse e-mail du destinataire et le message, vous pouvez définir la fréquence à laquelle la notification est envoyée.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

12. Cliquez sur **Suivant**.

    La page **Fournisseurs d'informations d'identification : renouvellement** s'affiche. Sur cette page, vous pouvez configurer Citrix Endpoint Management pour effectuer les opérations suivantes :

    - Renouveler le certificat. Vous pouvez envoyer (facultatif) une notification lors du renouvellement et exclure (facultatif) les certificats déjà expirés de l'opération.
    - Émettre une notification pour les certificats dont l'expiration approche (avant le renouvellement).

13. Sur la page **Fournisseurs d'informations d'identification : renouvellement**, procédez comme suit si vous souhaitez renouveler les certificats lorsqu'ils expirent :

    Réglez **Renouveler les certificats lorsqu'ils expirent** sur **Activé**. Des champs supplémentaires apparaissent.

    - Dans le champ **Renouveler lorsque le certificat expire dans**, entrez quand le renouvellement doit être effectué, en nombre de jours avant l'expiration.
    - Si vous le souhaitez, sélectionnez **Ne pas renouveler les certificats expirés**. Dans ce cas, « expiré » signifie que la date `NotAfter` (fin de validité) est dans le passé, et non pas qu'il a été révoqué. Citrix Endpoint Management ne renouvelle pas les certificats après leur révocation interne.

    Si vous voulez que Citrix Endpoint Management envoie une notification lorsque le certificat a été renouvelé, définissez **Envoyer une notification** sur **Activé**. Si vous voulez que Citrix Endpoint Management envoie une notification lorsque la certification arrive à échéance, définissez **Notifier quand un certificat va expirer** sur **Activé**.
    Dans tous les cas, vous avez le choix entre deux options de notification :

    - **Sélectionner un modèle de notification :** sélectionnez un message de notification prérempli que vous pouvez personnaliser. Ces modèles figurent dans la liste Modèle de notification.
    - **Entrer les détails de notification :** créez votre propre message de notification. Indiquez l'adresse e-mail du destinataire, un message et la fréquence d'envoi de la notification.

    Dans le champ **Notifier lorsque le certificat expire dans**, entrez le nombre de jours avant expiration du certificat après lequel la notification doit être envoyée.

14. Cliquez sur **Enregistrer**.

    Le fournisseur d'identités apparaît dans la table Fournisseur d'identités.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Certificats APNs

December 11, 2023

Pour inscrire et gérer des appareils Apple dans Citrix Endpoint Management, configurez un certificat Apple Push Notification Service (APNS). Le certificat permet de gérer les appareils mobiles via le réseau Apple Push Network.

Résumé du workflow :

Étape 1 : Créer une demande de signature de certificat (CSR) en utilisant l'une des méthodes suivantes :

- Créer une demande de signature de certificat à l'aide de l'application Trousseau d'accès sur macOS (recommandé par Citrix)
- Créer une demande de signature de certificat à l'aide de Microsoft IIS
- Créer une demande de signature de certificat avec OpenSSL

Étape 2 : Signer la CSR dans Citrix Endpoint Management Tools

Étape 3 : Envoyer la CSR signée à Apple pour obtenir le certificat APNs

Étape 4 : En utilisant le même ordinateur que celui utilisé pour l'étape 1, remplir la CSR et exportez un fichier PKCS #12 :

- Créer un fichier PKCS #12 à l'aide de l'application Trousseau d'accès sur macOS
- Créer un fichier PKCS #12 à l'aide de Microsoft IIS
- Création d'un fichier PKCS #12 à l'aide d'OpenSSL

Étape 5 : Importer un certificat APNs dans Citrix Endpoint Management

Étape 6 : Renouveler un certificat APNs

Créer une demande de signature de certificat

Nous vous recommandons de créer une demande de signature de certificat (CSR) à l'aide de l'application Trousseau d'accès sur macOS. Vous pouvez également créer une demande de signature de certificat à l'aide de Microsoft IIS ou OpenSSL.

> **Important :**
>
> - Pour l'identifiant Apple ID utilisé pour créer le certificat :
> - The Apple ID must be a corporate ID and not a personal ID.
> - Record the Apple ID that you use to create the certificate.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> – To renew your certificate, use the same organization name and Apple ID. Using a different Apple ID to renew the certificate require device re-enrollment.
>
> • Si vous avez délibérément ou accidentellement révoqué le certificat, vous perdrez la possibilité de gérer vos appareils.
>
> • Si vous avez utilisé iOS Developer Enterprise Program pour créer un certificat push de gestion des appareils mobiles, vous devez gérer les actions concernant les certificats migrés dans le portail Apple Push Certificates Portal.

Créer une demande de signature de certificat à l'aide de l'application Trousseau d'accès sur macOS

1. Sur un ordinateur exécutant macOS, sous **Applications > Utilitaires**, démarrez l'application Trousseau d'accès.
2. Ouvrez le menu **Trousseaux d'accès** et cliquez sur **Assistant de certification > Demander un certificat à une autorité de certification**.
3. L'Assistant de certification vous invite à entrer les informations suivantes :
   - **Adresse e-mail :** adresse de messagerie de la personne ou du compte de rôle qui gère le certificat.
   - **Nom commun :** nom commun de la personne ou compte de rôle qui gère le certificat.
   - **Adresse e-mail de l'AC :** adresse de messagerie de l'autorité de certification.
4. Sélectionnez **Enregistrée sur le disque** et **Me laisser indiquer les informations sur la bi-clé** et cliquez sur **Continuer**.
5. Entrez un nom pour le fichier CSR, enregistrez le fichier sur votre ordinateur, puis cliquez sur **Enregistrer**.
6. Spécifiez les informations de bi-clé en sélectionnant la **Dimension de clé** de 2048 bits et **Algorithme RSA**, puis cliquez sur **Continuer**. Le fichier CSR est prêt à être chargé dans le cadre du processus de certificat APNS.
7. Cliquez sur **Terminé** lorsque l'Assistant de certification termine le processus de demande de signature de certificat.
8. Pour continuer, signez la CSR.

Créer une demande de signature de certificat à l'aide de Microsoft IIS

La première étape de génération d'une demande de certificat APNS consiste à créer une demande de signature de certificat (CSR). Pour Windows, générez une CSR à l'aide de Microsoft IIS.

1. Ouvrez Microsoft IIS.
2. Double-cliquez sur l'icône Certificats de serveur pour IIS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Dans la fenêtre **Certificats de serveur**, cliquez sur **Créer une demande de certificat**.
4. Tapez les informations de nom unique (DN) appropriées. Par exemple, vous pouvez taper le nom de domaine complet (FQDN) de votre serveur Citrix Endpoint Management, par exemple `www.domain.com`. Cliquez ensuite sur **Suivant**.
5. Sélectionnez le **Fournisseur de services de chiffrement Microsoft RSA SChannel** pour le fournisseur de services de chiffrement et **2048** pour la longueur en bits, puis cliquez sur **Suivant**.
6. Entrez un nom de fichier et spécifiez un emplacement pour enregistrer la CSR, puis cliquez sur **Terminer**.
7. Pour continuer, signez la CSR.

Créer une demande de signature de certificat avec OpenSSL

Si vous ne pouvez pas utiliser un appareil macOS ou Microsoft IIS pour générer une demande de signature de certificat, utilisez OpenSSL. Vous pouvez télécharger et installer OpenSSL à partir du site Web OpenSSL.

1. Sur l'ordinateur sur lequel vous avez installé OpenSSL, exécutez la commande suivante à partir d'une invite de commandes ou de shell.

   ```
   openssl req -new -keyout Customer.key.pem –out CompanyAPNScertificate
   .csr -newkey rsa:2048
   ```

2. Le message suivant s'affiche pour les informations de nom du certificat. Entrez les informations demandées.

   ```
   You are about to be asked to enter information that will be
      incorporated into your certificate request.
   What you are about to enter is what is called a Distinguished Name
       or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
   Country Name (2 letter code) [AU]:US
   State or Province Name (full name) [Some-State]:CA
   Locality Name (eg, city) []:RWC
   Organization Name (eg, company) [Internet Widgits Pty Ltd]:
      Customer
   Organizational Unit Name (eg, section) [:Marketing
   Common Name (eg, YOUR name) []:John Doe
   Email Address []:john.doe@customer.com
   <!--NeedCopy-->
   ```

3. Dans le message suivant, entrez un mot de passe pour la clé privée de la demande de signature de certificat.

   ```
   Please enter the following 'extra' attributes
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

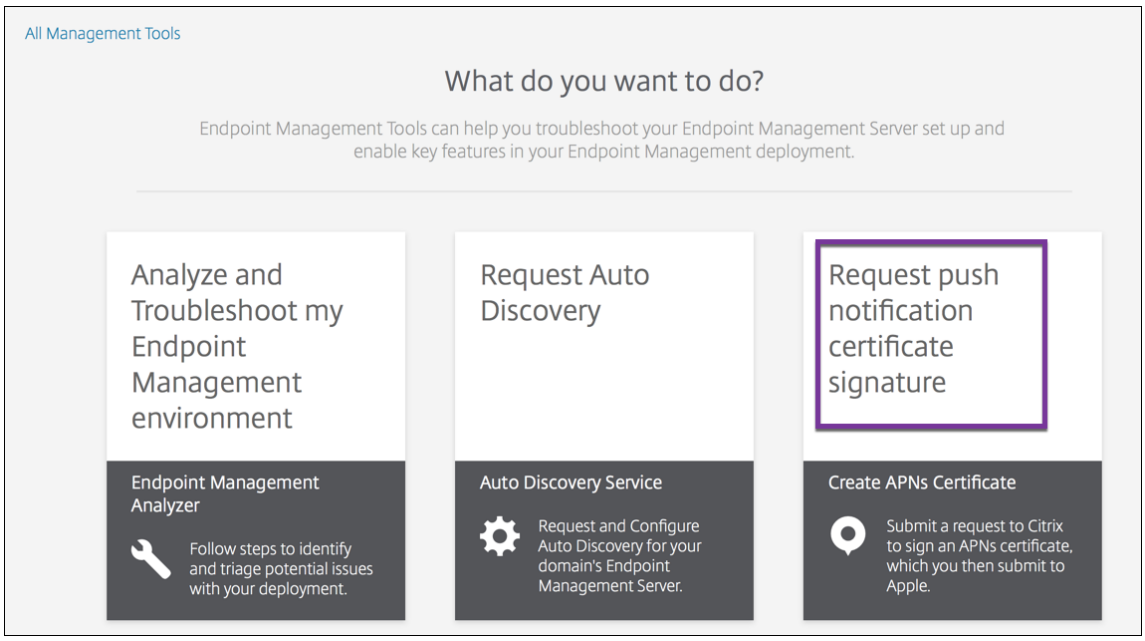
```
to be sent with your certificate request
A challenge password []:
An optional company name []:
<!--NeedCopy-->
```

4. Pour continuer, signez la demande de signature de certificat comme décrit dans la section suivante.

Signer la demande de signature de certificat

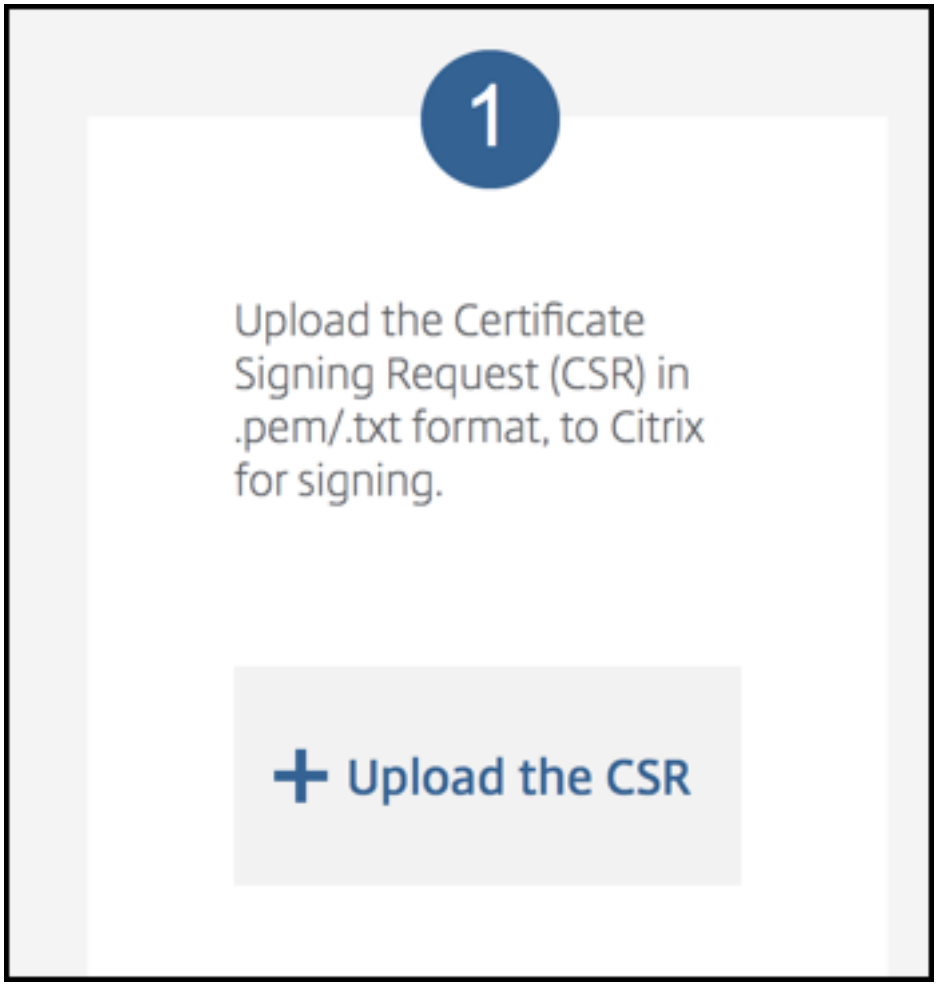
Pour utiliser un certificat avec Citrix Endpoint Management, vous devez le soumettre à Citrix à des fins de signature. Citrix signe la demande de signature de certificat (CSR) à l'aide de son certificat de signature de gestion d'appareils mobiles et renvoie le fichier signé au format `.plist`.

1. Dans votre navigateur, accédez au site Web Citrix Endpoint Management Tools, puis cliquez sur **Request push notification certificate signature**.



2. Sur la page **Creating a new certificate**, cliquez sur **Upload the CSR**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Localisez et sélectionnez le certificat.

> **Important :**
>
> le certificat doit être au format .pem/txt. Si nécessaire, remplacez l'extension de fichier du certificat par .pem ou .txt en cliquant avec le bouton droit de la souris et en renommant le fichier.

4. Sur la page **Citrix Endpoint Management APNs CSR Signing**, cliquez sur **Sign**. La demande de signature de certificat est signée et automatiquement enregistrée sur votre dossier de téléchargement configuré.
5. Pour continuer, soumettez la demande de signature de certificat signée comme décrit dans la section suivante.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Soumettre la demande de signature de certificat à Apple afin d'obtenir le certificat APNS

Après la réception de votre demande de signature de certificat (CSR) signée de Citrix, envoyez-la à Apple pour obtenir le certificat APNS nécessaire à l'importation dans Citrix Endpoint Management.

> **Remarque :**
>
> Certains utilisateurs ont signalé des problèmes lors de la connexion au portail Apple Push Portal. Vous pouvez également vous connecter au portail des développeurs Apple. Vous pouvez ensuite suivre ces étapes :

1. Dans un navigateur, accédez au portail Apple Push Certificates Portal.
2. Cliquez sur **Create a Certificate**.
3. La première fois que vous créez un certificat avec Apple, sélectionnez la case **I have read and agree to these terms and conditions** et cliquez sur **Accept**.
4. Cliquez sur **Choose File** pour charger votre demande de signature de certificat signée, accédez à la demande sur votre ordinateur, puis cliquez sur **Upload**. Un message de confirmation indique que le chargement a réussi.
5. Cliquez sur **Download** pour récupérer le certificat .pem.
6. Pour continuer, remplissez la demande de signature de certificat et exportez un fichier PKCS #12 comme décrit dans la section suivante.

Terminer la demande de signature de certificat et exporter un fichier PKCS #12

Après la réception de votre certificat APNS d'Apple, revenez à l'application Trousseau d'accès, Microsoft IIS ou OpenSSL pour exporter le certificat dans un fichier PCKS #12.

Un fichier PKCS #12 contient le fichier de certificat APNS, ainsi que votre clé privée. Les fichiers PFX ont généralement l'extension .pfx ou .p12. Vous pouvez utiliser les fichiers .pfx et .p12 de manière interchangeable.

> **Important :**
>
> Citrix vous recommande d'enregistrer ou d'exporter les clés personnelles et publiques du système local. Vous avez besoin des clés pour accéder aux certificats APNS à réutiliser. Sans ces clés, votre certificat n'est pas valide et vous devez répéter l'intégralité du processus de demande de signature de certificat et le processus APNS.

Créer un fichier PKCS #12 à l'aide de l'application Trousseau d'accès sur macOS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Important :**
>
> Utilisez le même appareil macOS pour cette tâche que vous avez utilisé pour générer la demande de signature de certificat.

1. Sur l'appareil, recherchez le certificat d'identité de produit (.pem) d'Apple.
2. Démarrez l'application Trousseaux d'accès et accédez à l'onglet **Connexion > Mes certificats**. Faites glisser et déposez le certificat d'identité de produit dans la fenêtre ouverte.
3. Cliquez sur le certificat et développez la flèche gauche pour vérifier que le certificat inclut une clé privée associée.
4. Pour commencer l'exportation du certificat dans un certificat PCKS #12 (.pfx), choisissez le certificat et la clé privée, cliquez avec le bouton droit de la souris, puis sélectionnez **Exporter 2 éléments**.
5. Donnez au fichier de certificat un nom unique à utiliser avec Citrix Endpoint Management. N'insérez pas d'espace dans le nom. Ensuite, choisissez un emplacement de dossier pour le certificat enregistré, sélectionnez le format du fichier .pfx, puis cliquez sur **Enregistrer**.
6. Entrez un mot de passe pour l'exportation du certificat. Citrix vous recommande d'utiliser un mot de passe fort et unique. Par ailleurs, conservez le certificat et le mot de passe de manière sécurisée à des fins d'utilisation ultérieure et de référence.
7. L'application Trousseau d'accès vous invite à saisir le mot de passe ou le trousseau sélectionné. Tapez le mot de passe, puis cliquez sur **OK**. Le certificat enregistré est maintenant prêt à être utilisé avec Citrix Endpoint Management Server.
8. Pour continuer, voir Importer un certificat APNS dans Citrix Endpoint Management.

Créer un fichier PKCS #12 à l'aide de Microsoft IIS

> **Important :**
>
> Utilisez le même serveur IIS pour cette tâche que vous avez utilisé pour générer la demande de signature de certificat.

1. Ouvrez Microsoft IIS.
2. Cliquez sur l'icône **Certificats de serveur**.
3. Dans la fenêtre **Certificats de serveur**, cliquez sur **Terminer la demande de certificat**.
4. Accédez au fichier Certificate.pem d'Apple. Tapez ensuite un nom convivial ou le nom du certificat, puis cliquez sur **OK**. N'insérez pas d'espace dans le nom.
5. Sélectionnez le certificat que vous avez identifié dans l'étape 4, puis cliquez sur **Exporter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Spécifiez un emplacement et un nom de fichier pour le certificat .pfx ainsi qu'un mot de passe, puis cliquez sur **OK**.

   Vous devez fournir le mot de passe du certificat pour l'importer dans Citrix Endpoint Management.

7. Copiez le certificat .pfx sur le serveur sur lequel Citrix Endpoint Management sera installé.
8. Pour continuer, voir Importer un certificat APNS dans Citrix Endpoint Management.

Création d'un fichier PKCS #12 à l'aide d'OpenSSL

Si vous utilisez OpenSSL pour créer une demande de signature de certificat, vous pouvez également utiliser OpenSSL pour créer un certificat APNS .pfx.

1. À l'invite de commandes ou shell, exécutez la commande suivante. `Customer.privatekey.pem` est la clé privée de votre demande de signature de certificat et `APNs_Certificate.pem` le certificat que vous venez de recevoir d'Apple.

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey.pem -out apns_identity.pfx
   ```

2. Entrez un mot de passe pour le fichier de certificat .pfx. Mémorisez ce mot de passe car vous l'utilisez pour charger le certificat sur Citrix Endpoint Management.
3. Notez l'emplacement du fichier de certificat .pfx. Copiez ensuite le fichier sur Citrix Endpoint Management Server, de façon à pouvoir utiliser la console pour charger le fichier.
4. Pour continuer, importez un certificat APNS dans Citrix Endpoint Management comme décrit dans la section suivante.

Importer un certificat APNS dans Citrix Endpoint Management

Une fois que vous avez reçu un nouveau certificat APNS, vous devez l'importer dans Citrix Endpoint Management pour ajouter le certificat (pour la première fois) ou remplacer un certificat.

1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Certificats**.
2. Cliquez sur **Importer > Keystore**.
3. Dans **Utiliser en tant que**, choisissez **APNS**.
4. Accédez au fichier .pfx ou .p12 sur votre ordinateur.
5. Entrez un mot de passe, puis cliquez sur **Importer**.

Pour de plus amples informations sur les certificats dans Citrix Endpoint Management, consultez la section Certificats et authentification.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Renouveler un certificat APNS

> **Important :**
>
> Si vous utilisez un identifiant Apple ID différent pour le processus de renouvellement, vous devez réinscrire les appareils utilisateur.

Pour renouveler un certificat APNs, procédez comme suit pour créer un certificat, puis accédez au portail Apple Push Certificates Portal. Utilisez ce portail pour charger le nouveau certificat. Une fois la session ouverte, votre certificat existant ou un certificat importé à partir de votre ancien compte Apple Developers apparaît.

Sur la page Certificats Portal, la seule différence lors du renouvellement du certificat est que vous cliquez sur **Renew**. Vous devez avoir un compte de développeur auprès du Certificates Portal pour accéder au site. Pour renouveler votre certificat, utilisez le même nom d'organisation et le même identifiant Apple ID.

Pour déterminer la date à laquelle votre certificat APNS expire, dans la console Citrix Endpoint Management, accédez à **Paramètres > Certificats**. Si le certificat expire, ne le révoquez pas.

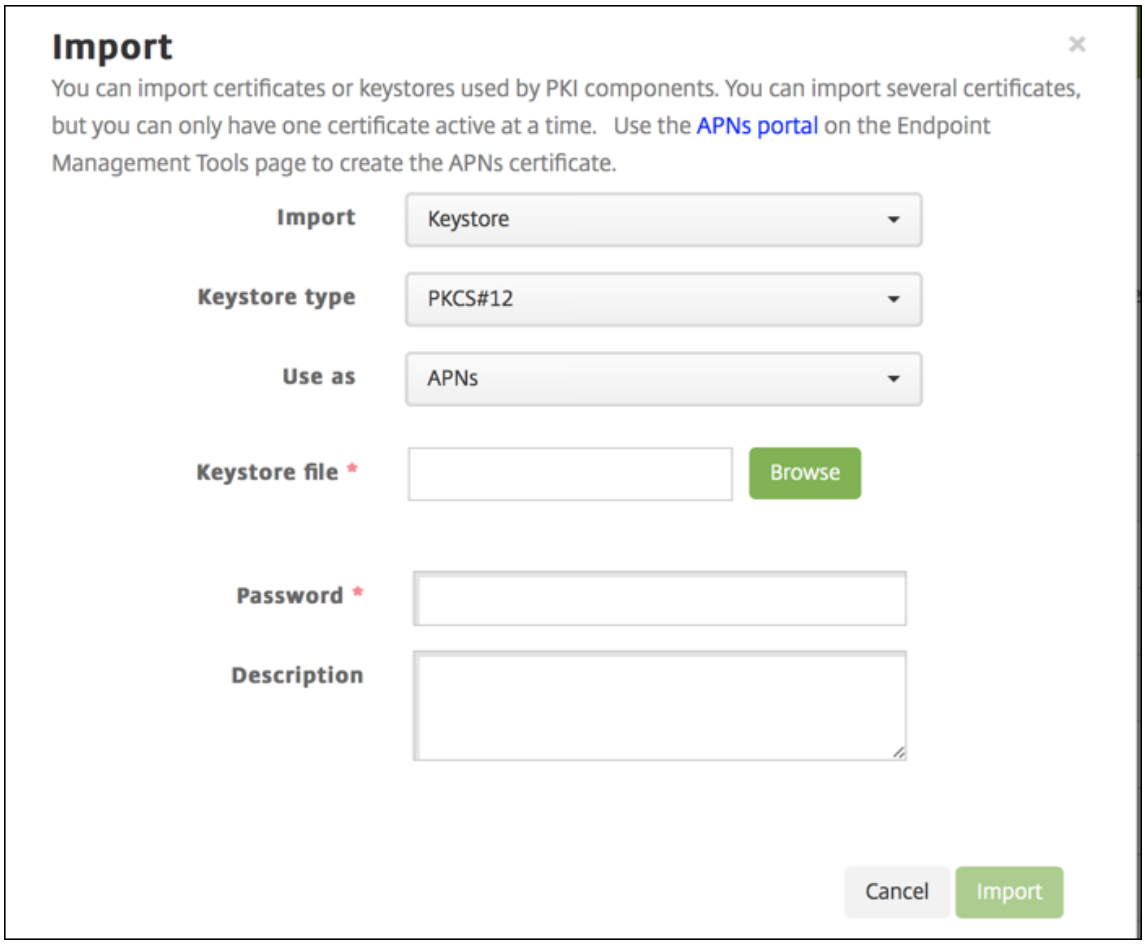
1. Générez une demande de signature de certificat à l'aide de Microsoft IIS, l'application Trousseau d'accès (macOS) ou OpenSSL. Pour plus d'informations sur la génération d'une CSR, consultez Créer une demande de signature de certificat.
2. Dans votre navigateur, accédez à Citrix Endpoint Management Tools. Cliquez ensuite sur **Request push notification certificate signature**.
3. Cliquez sur **+Upload the CSR**.
4. Dans la boîte de dialogue, accédez à la CSR, cliquez sur **Open**, puis sur **Sign**.
5. Lorsque vous recevez un fichier `.plist`, enregistrez-le.
6. Dans le titre de l'étape 3, cliquez sur **Apple Push Certificates Portal** et connectez-vous.
7. Sélectionnez le certificat que vous souhaitez renouveler et cliquez sur **Renew**.
8. Chargez le fichier `.plist`. Vous devriez recevoir un fichier .pem en sortie. Enregistrez le fichier .pem.
9. À l'aide du fichier .pem, complétez la CSR (en fonction de la méthode utilisée pour créer la CSR à l'étape 1).
10. Exportez le certificat en tant que fichier .pfx.

Dans la console Citrix Endpoint Management, importez le fichier .pfx et procédez à la configuration comme suit :

1. Accédez à **Paramètres > Certificats > Importer**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Depuis le menu **Importer**, sélectionnez **Keystore**.
3. Dans le menu **Type de magasin de clés Java**, choisissez **PKCS #12**.
4. Dans **Utiliser en tant que**, choisissez **APNS**.



5. Sous **Fichier de keystore**, cliquez sur **Parcourir** et accédez au fichier.
6. Sous **Mot de passe**, entrez le mot de passe du certificat.
7. Entrez une **Description** (facultatif).
8. Cliquez sur **Importer**.

Citrix Endpoint Management vous redirige vers la page **Certificats**. Les champs **Nom**, **État**, **Valide du** et **Valide jusqu'au** sont mis à jour.

SAML pour l'authentification unique avec Citrix Files

March 1, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Vous pouvez configurer Citrix Endpoint Management et ShareFile pour une utilisation avec SAML (Security Assertion Markup Language) afin de fournir l'accès SSO aux applications mobiles Citrix Files. Cette fonctionnalité comprend les éléments suivants :

- Applications Citrix Files pour lesquelles le SDK MAM est activé ou qui sont encapsulées à l'aide de MDX Toolkit
- Clients Citrix Files non encapsulés, tels que le site Web, Outlook Plug-in ou les clients de synchronisation
- **Pour les applications Citrix Files encapsulées :** les utilisateurs qui se connectent à Citrix Files sont redirigés vers Citrix Secure Hub pour s'authentifier et acquérir un jeton SAML. Une fois l'authentification réussie, l'application mobile Citrix Files envoie le jeton SAML à ShareFile. Après la première ouverture de session, les utilisateurs peuvent accéder à l'application mobile Citrix Files via l'authentification unique. Ils peuvent également joindre des documents à partir de ShareFile à des messages Citrix Secure Mail sans ouvrir une session à chaque fois.
- **Pour les clients Citrix Files non encapsulés :** les utilisateurs qui se connectent à Citrix Files à l'aide d'un navigateur Web ou d'un autre client Citrix Files sont redirigés vers Citrix Endpoint Management. Citrix Endpoint Management authentifie les utilisateurs, qui acquièrent alors un jeton SAML qui est envoyé à ShareFile. Après la première ouverture de session, les utilisateurs peuvent accéder aux clients Citrix Files via l'authentification unique sans se connecter à chaque fois.

Pour utiliser Citrix Endpoint Management en tant que fournisseur d'identité SAML pour ShareFile, vous devez configurer Citrix Endpoint Management de manière à l'utiliser avec des comptes Enterprise, comme décrit dans cet article. Vous pouvez également configurer Citrix Endpoint Management pour fonctionner uniquement avec des connecteurs StorageZone. Pour plus d'informations, consultez la section Utilisation de ShareFile avec Citrix Endpoint Management.

Pour un diagramme d'architecture de référence détaillé, voir Architecture.

Logiciels requis

Vous devez remplir les conditions suivantes pour pouvoir configurer l'authentification unique avec les applications Citrix Endpoint Management et Citrix Files :

- SDK MAM ou une version compatible de l'outil MDX Toolkit (pour les applications mobiles Citrix Files)

  Pour de plus amples informations, consultez la section Compatibilité Citrix Endpoint Management.
- Version compatible de Citrix Secure Hub et des applications mobiles Citrix Files.

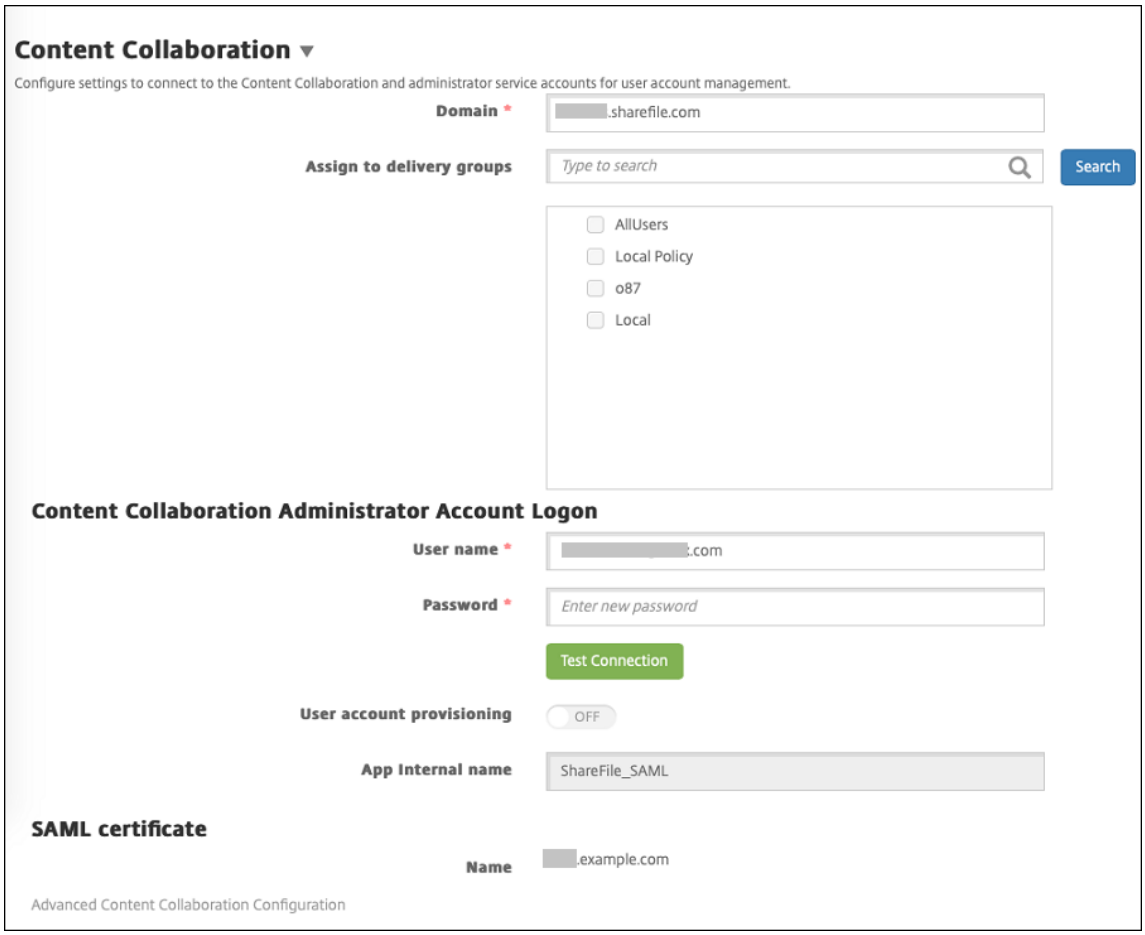
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Compte d'administrateur ShareFile.
- Connexion vérifiée entre Citrix Endpoint Management et ShareFile.

Configurer l'accès à ShareFile

Avant de configurer SAML pour ShareFile, indiquez les informations d'accès à ShareFile comme suit :

1. Dans la console Web Citrix Endpoint Management, cliquez sur **Configurer > ShareFile**. La page de configuration de **ShareFile** s'affiche.



2. Pour configurer ces paramètres :
   - **Domaine :** entrez votre nom de sous-domaine ShareFile. Par exemple : `example.sharefile.com`.
   - **Attribuer aux groupes de mise à disposition :** sélectionnez ou recherchez les groupes de mise à disposition que vous souhaitez autoriser à utiliser l'authentification unique avec ShareFile.
   - **Connexion au compte administrateur ShareFile**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Nom d'utilisateur :** tapez le nom d'utilisateur administrateur ShareFile. Cet utilisateur doit disposer des privilèges d'administrateur.
- **Mot de passe :** tapez le mot de passe d'administrateur ShareFile.
- **Provisioning du compte utilisateur :** laissez ce paramètre désactivé. Utilisez l'outil de gestion des utilisateurs ShareFile pour provisionner des utilisateurs. Voir Provisionner des comptes d'utilisateurs et des groupes de distribution.

3. Cliquez sur **Tester la connexion** pour vérifier que le nom d'utilisateur et le mot de passe du compte d'administrateur ShareFile s'authentifient sur le compte ShareFile spécifié.
4. Cliquez sur **Enregistrer**.
   - Citrix Endpoint Management se synchronise avec ShareFile et met à jour les paramètres **ID d'émetteur/d'entité ShareFile** et l'**URL de connexion** de ShareFile.
   - La page **Configurer > ShareFile** affiche le champ **Nom interne de l'application**. Vous avez besoin de ce nom pour effectuer les étapes décrites plus loin dans Modifier les paramètres d'authentification unique de Citrix Files.com.

Configurer SAML pour les applications Citrix Files MDX encapsulées

Vous n'avez pas besoin d'utiliser NetScaler Gateway pour la configuration de l'authentification unique avec des applications Citrix Files préparées avec le SDK MAM. Pour configurer l'accès aux clients Citrix Files non encapsulés, tels que le site Web, Outlook Plug-in ou les clients de synchronisation, consultez Configurer NetScaler Gateway pour d'autres clients Citrix Files.

Pour configurer SAML pour les applications MDX Citrix Files encapsulées :

1. Téléchargez les clients ShareFile pour Citrix Endpoint Management. Voir la page des téléchargements Citrix.com.
2. Préparez l'application mobile Citrix Files avec le SDK MAM. Pour de plus amples informations, consultez la section Présentation du SDK MAM.
3. Dans la console Citrix Endpoint Management, chargez l'application mobile Citrix Files préparée. Pour plus d'informations sur le chargement des applications MDX, consultez la section Pour ajouter une application MDX à Citrix Endpoint Management.
4. Vérifiez les paramètres SAML : ouvrez une session sur ShareFile avec le nom d'utilisateur et le mot de passe administrateur que vous avez configurés plus tôt.
5. Vérifiez que ShareFile et Citrix Endpoint Management sont configurés pour le même fuseau horaire. Assurez-vous que Citrix Endpoint Management indique l'heure appropriée par rapport au fuseau horaire configuré. Sinon, l'authentification unique peut échouer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Valider l'application mobile Citrix Files

1. Sur la machine utilisateur, installez et configurez Citrix Secure Hub.
2. À partir du magasin d'applications, téléchargez et installez l'application mobile Citrix Files.
3. Démarrez l'application mobile Citrix Files. Citrix Files démarre sans vous inviter à saisir un nom d'utilisateur ou un mot de passe.

Valider avec Citrix Secure Mail

1. Sur la machine utilisateur, si cela n'a pas déjà été fait, installez et configurez Citrix Secure Hub.
2. À partir du magasin d'applications, téléchargez, installez et configurez Citrix Secure Mail.
3. Ouvrez un nouveau formulaire électronique et appuyez sur **Joindre à partir de ShareFile**. Les fichiers pouvant être joints à l'e-mail sont affichés sans vous inviter à saisir un nom d'utilisateur ou un mot de passe.

Configurer NetScaler Gateway pour d'autres clients Citrix Files

Pour configurer l'accès des clients Citrix Files non encapsulés, tels que le site Web, le plug-in Outlook ou les clients de synchronisation, vous devez configurer NetScaler Gateway pour prendre en charge l'utilisation de Citrix Endpoint Management en tant que fournisseur d'identité SAML de la manière suivante.

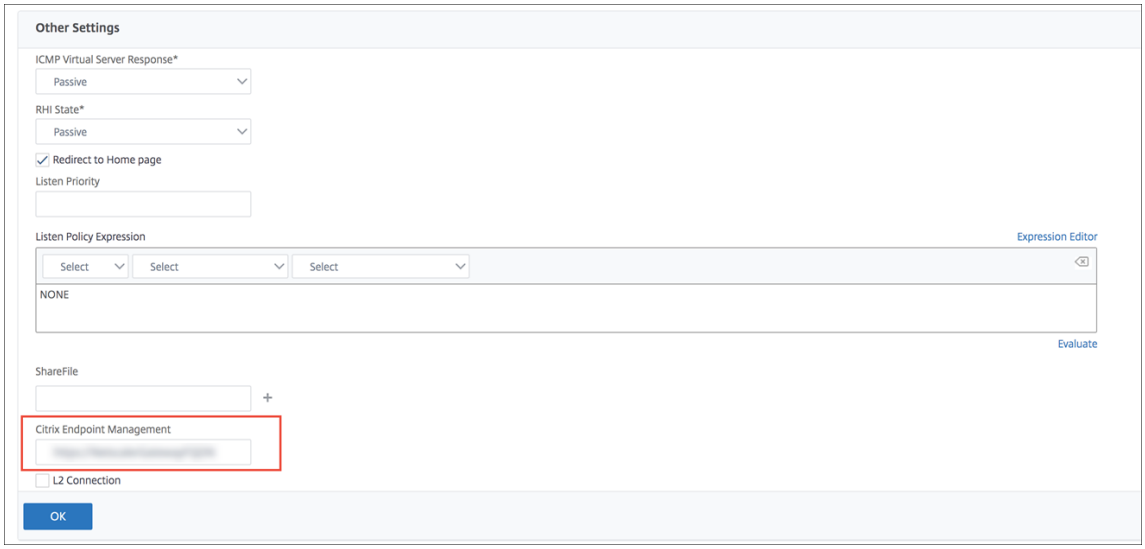
- Désactivez la redirection vers la page d'accueil.
- Créez une stratégie et un profil de session Citrix Files.
- Configurez des stratégies sur le serveur virtuel NetScaler Gateway.

Désactiver la redirection vers la page d'accueil

Désactivez le comportement par défaut pour les demandes qui passent par le chemin / cginfra. Cette action permet aux utilisateurs de voir l'URL interne demandée à la place de la page d'accueil configurée.

1. Modifiez les paramètres du serveur virtuel NetScaler Gateway qui est utilisé pour les ouvertures de session Citrix Endpoint Management. Dans NetScaler Gateway, cliquez sur **Other Settings**, puis désactivez la case à cocher intitulée **Redirect to Home Page**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Sous **ShareFile** (à présent renommé ShareFile), entrez le nom et le numéro de port de votre serveur interne Citrix Endpoint Management.
3. Sous **Citrix Endpoint Management**, tapez votre URL Citrix Endpoint Management.

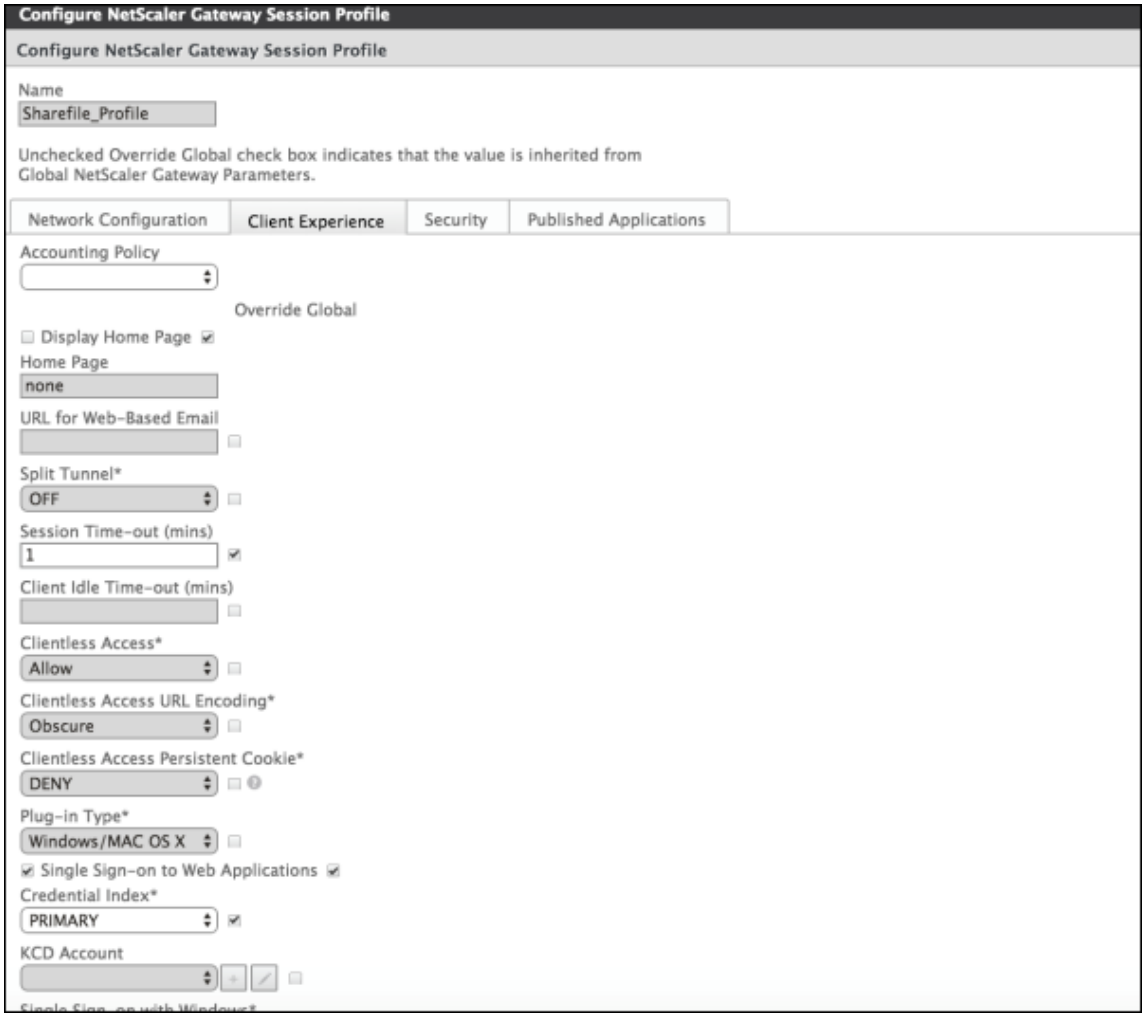
   Cette configuration autorise les demandes pour l'URL indiquée via le chemin d'accès /cginfra.

Créez une stratégie et un profil de demande de session Citrix Files

Configurez ces paramètres pour créer une stratégie et un profil de demande de session Citrix Files :

1. Dans l'utilitaire de configuration de NetScaler Gateway, dans le volet de navigation de gauche, cliquez sur **NetScaler Gateway > Policies > Session**.
2. Créez une stratégie de session. Dans l'onglet **Policies**, cliquez sur **Add**.
3. Dans le champ **Name**, tapez **ShareFile_Policy**.
4. Créez une action en cliquant sur le bouton **+**. La page **Create NetScaler Gateway Session Profile** s'affiche.

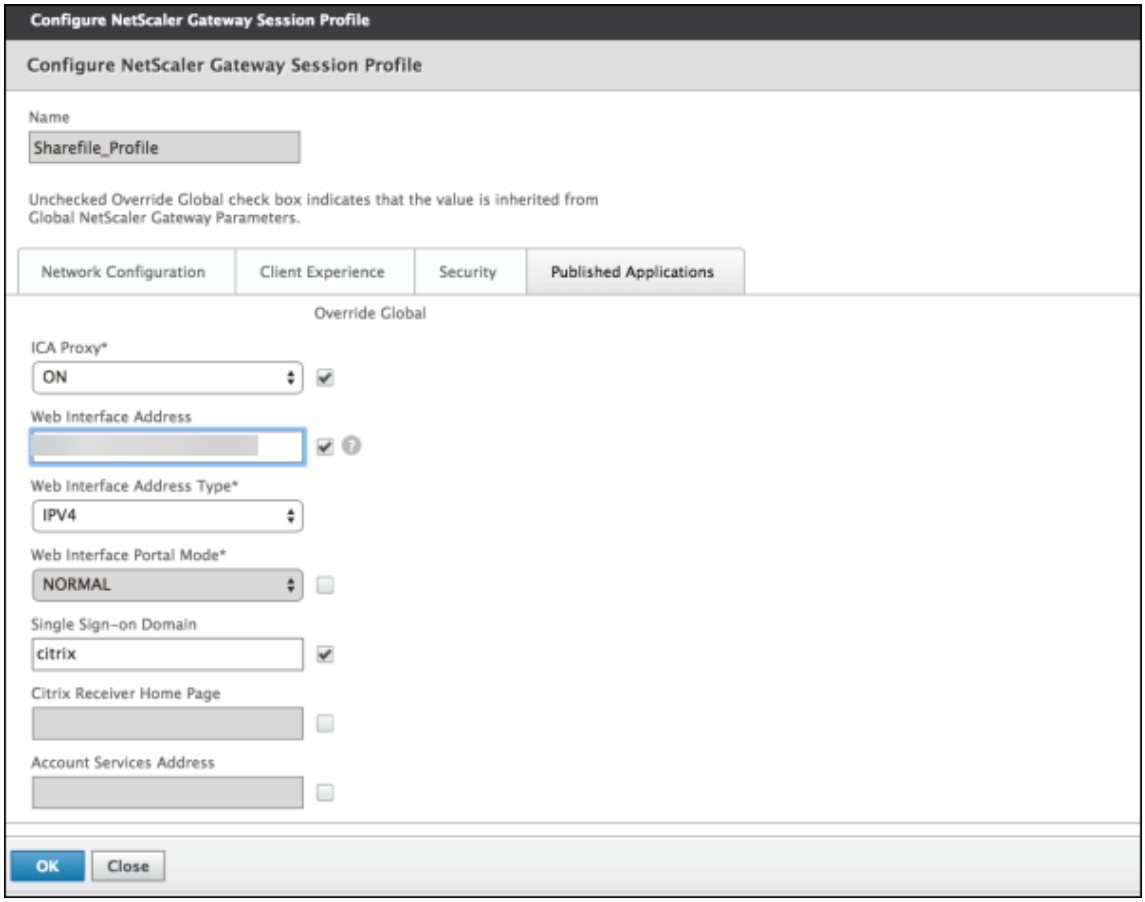
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pour configurer ces paramètres :

- **Name :** tapez **ShareFile_Profile**.
- Cliquez sur l'onglet **Client Experience**, puis configurez les paramètres suivants :
  - **Home Page :** tapez **none**.
  - **Session Time-out (mins) :** tapez **1**.
  - **Single Sign-on to Web Applications :** sélectionnez ce paramètre.
  - **Credential Index :** dans la liste, cliquez sur **PRIMARY**.
- Cliquez sur l'onglet **Published Applications**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



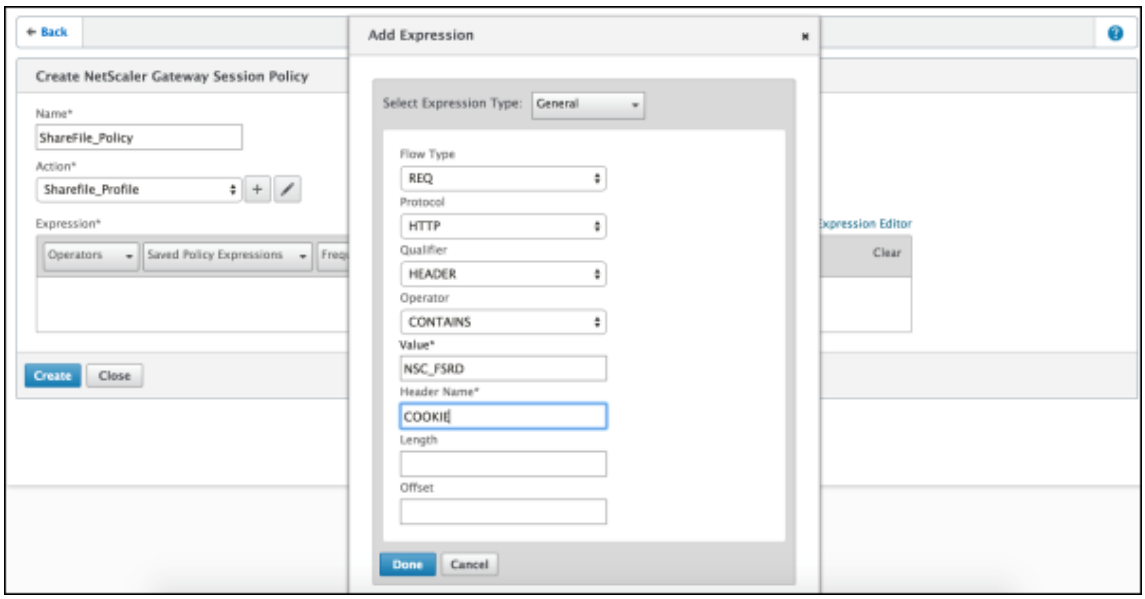
Pour configurer ces paramètres :

- **ICA Proxy :** dans la liste, cliquez sur **On**.
- **Web Interface Address :** entrez l'URL de Citrix Endpoint Management Server.
- **Single Sign-on Domain :** tapez votre nom de domaine Active Directory.

  Lors de la configuration du profil de session de NetScaler Gateway, le suffixe de domaine pour **Single Sign-on Domain** doit correspondre à l'alias de domaine Citrix Endpoint Management défini dans LDAP.

5. Cliquez sur **Create** pour définir le profil de session.
6. Cliquez sur **Expression Editor**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pour configurer ces paramètres :

- **Value :** tapez **NSC_FSRD**.
- **Header Name :** tapez **COOKIE**.

7. Cliquez sur **Create**, puis cliquez sur **Close**.

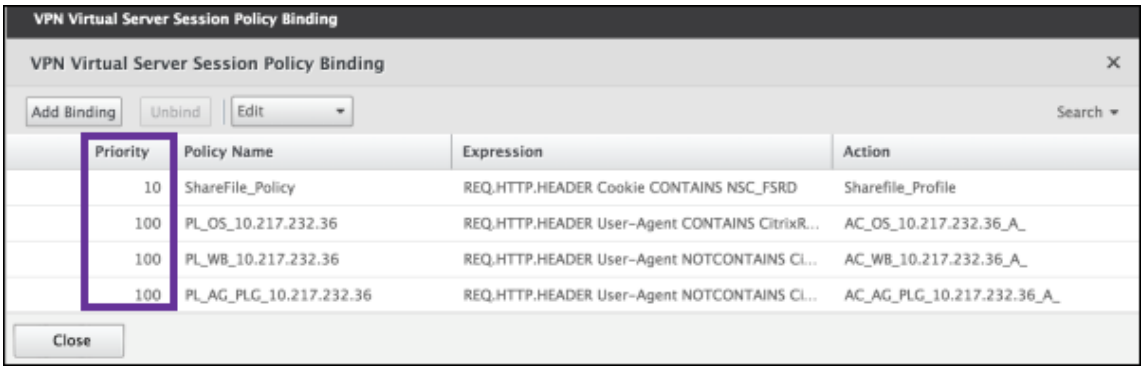
Configurer des stratégies sur le serveur virtuel NetScaler Gateway

Configurez les paramètres suivants sur le serveur virtuel NetScaler Gateway.

1. Dans l'utilitaire de configuration de NetScaler Gateway, dans le volet de navigation de gauche, cliquez sur **NetScaler Gateway > Virtual Servers**.
2. Dans le panneau **Details**, cliquez sur votre serveur virtuel NetScaler Gateway.
3. Cliquez sur **Modifier**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Cliquez sur **Configured policies > Session policies**, puis sur **Add binding**.
5. Sélectionnez **ShareFile_Policy**.
6. Modifiez le numéro de **priorité** (Priority) généré automatiquement pour la stratégie sélectionnée de manière à lui attribuer la priorité la plus élevée (le plus petit nombre) par rapport aux autres stratégies indiquées. Par exemple :



7. Cliquez sur **Done**, puis enregistrez la configuration NetScaler Gateway actuelle.

Modifier les paramètres d'authentification unique de Citrix Files.com

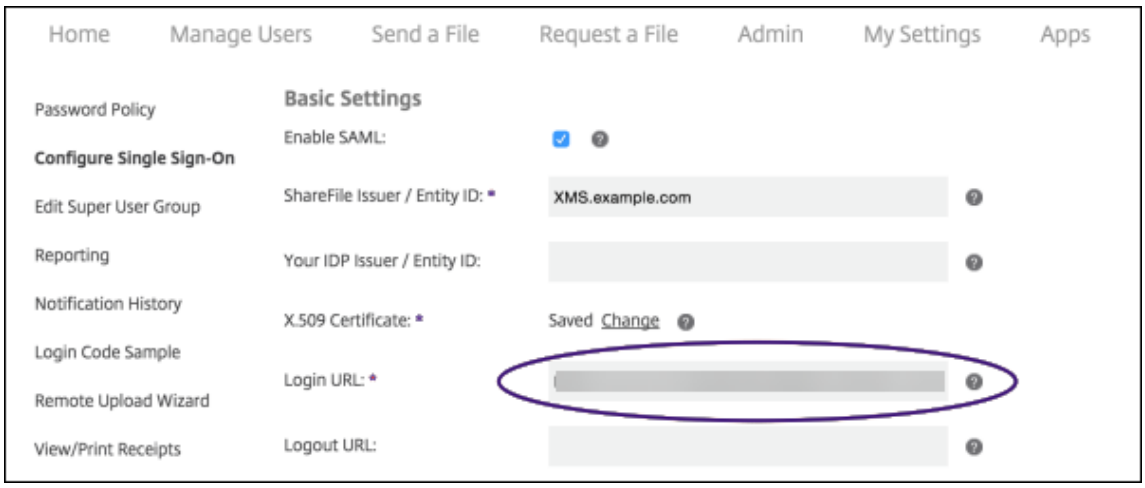
Apportez les modifications suivantes pour les applications MDX et non-MDX Citrix Files.

> **Important :**
>
> Un nouveau numéro est ajouté au nom de l'application interne :
>
> - Chaque fois que vous modifiez ou recréez l'application Citrix Files
> - Chaque fois que vous modifiez les paramètres ShareFile dans Citrix Endpoint Management
>
> Par conséquent, vous devez également mettre à jour l'URL de connexion dans le site Web Citrix Files pour refléter le nom d'application mis à jour.

1. Ouvrez une session sur votre compte ShareFile (`https://<subdomain>.sharefile.com`) en tant qu'administrateur.
2. Dans l'interface Web ShareFile, cliquez sur **Admin**, puis sélectionnez **Configurer le Single Sign-On**.
3. Modifiez l'**URL de connexion** comme suit :

   Voici un exemple d'**URL de connexion** avant les modifications : `https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Insérez le nom de domaine complet (FQDN) externe du serveur virtuel de NetScaler Gateway et **/cginfra/https/** devant le nom de domaine complet du serveur Citrix Endpoint Management, puis ajoutez **8443** après le nom de domaine complet de Citrix Endpoint Management.

  Voici un exemple d'URL modifiée: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`

- Remplacez le paramètre `&app=ShareFile_SAML_SP` par le nom de l'application Citrix Files interne. Le nom interne est `ShareFile_SAML` par défaut. Toutefois, chaque fois que vous modifiez votre configuration, un numéro est ajouté au nom interne (`ShareFile_SAML_2`, `ShareFile_SAML_3`, etc.). Vous pouvez rechercher le **nom interne de l'application** sur la page **Configurer > ShareFile**.

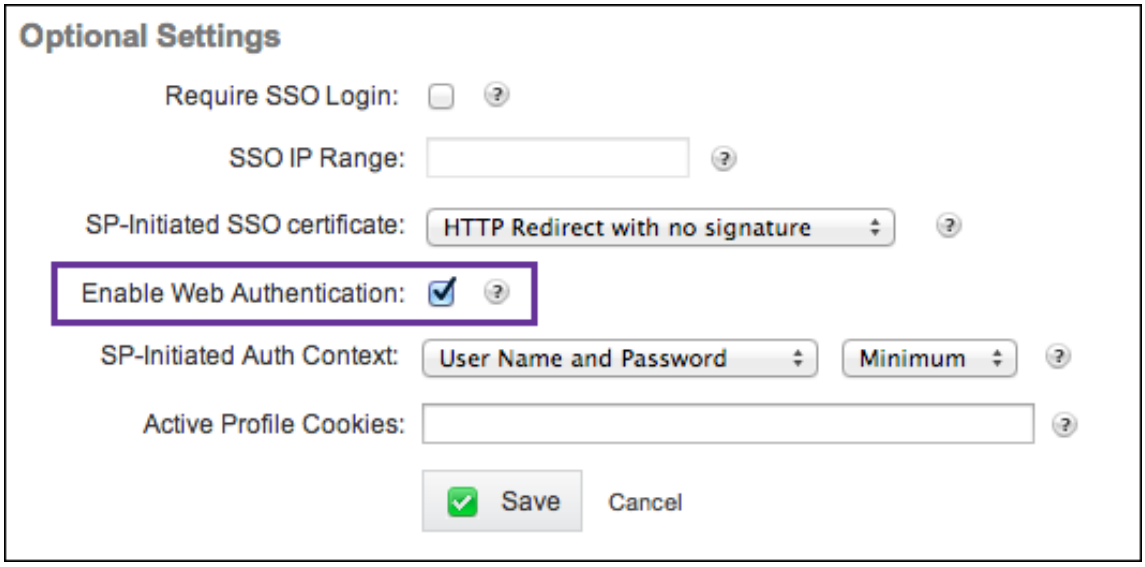
  Voici un exemple d'URL modifiée: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- Ajoutez `&nssso=true` à la fin de l'URL.

  Voici un exemple de l'URL finale : `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`.

4. Sous **Paramètres facultatifs**, sélectionnez la case à cocher **Activer l'authentification Web**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Valider la configuration

Procédez comme suit pour valider la configuration.

1. Pointez votre navigateur sur `https://<subdomain>sharefile.com/saml/login`.

   Vous êtes redirigé vers l'écran d'ouverture de session de NetScaler Gateway. Si vous n'êtes pas redirigé, vérifiez les paramètres de configuration précédents.

2. Entrez le nom d'utilisateur et le mot de passe pour l'environnement NetScaler Gateway et Citrix Endpoint Management que vous avez configuré.

   Vos dossiers Citrix Files à l'adresse `<subdomain>.sharefile.com` s'affichent. Si vos dossiers Citrix Files n'apparaissent pas, assurez-vous que les informations d'identification saisies pour l'ouverture de session sont correctes.

Authentification avec Azure Active Directory via Citrix Cloud

March 1, 2024

Citrix Endpoint Management prend en charge l'authentification avec les informations d'identification Azure Active Directory (Azure AD) via Citrix Cloud. Cette méthode d'authentification est disponible uniquement pour les utilisateurs qui s'inscrivent à MDM via l'application Citrix Secure Hub.

Pour utiliser Citrix Secure Hub avec MDM+MAM, configurez Citrix Endpoint Management pour utiliser NetScaler Gateway pour l'inscription MAM. Pour de plus amples informations, consultez NetScaler Gateway et Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Endpoint Management utilise le service Citrix Cloud appelé Identité Citrix pour se fédérer avec Azure Active Directory. Citrix recommande d'utiliser le fournisseur d'identité Citrix plutôt qu'une connexion directe à Azure Active Directory.

Citrix Endpoint Management prend en charge l'authentification avec Azure AD pour les plates-formes suivantes :

- Appareils iOS et macOS non inscrits à l'Apple Business Manager ou à l'Apple School Manager
- Appareils iOS et macOS inscrits à Apple Business Manager
- Appareils Android Enterprise (version préliminaire), pour BYOD et modes entièrement gérés

L'authentification avec Azure AD via Citrix Cloud présente les limitations suivantes :

- Non disponible pour les comptes locaux Citrix Endpoint Management.
- Ne prend pas en charge l'authentification par Azure AD pour les invitations d'inscription. Si vous envoyez une invitation d'inscription contenant une adresse URL d'inscription aux utilisateurs, les utilisateurs s'authentifient via LDAP au lieu d'Azure AD.

Logiciels requis

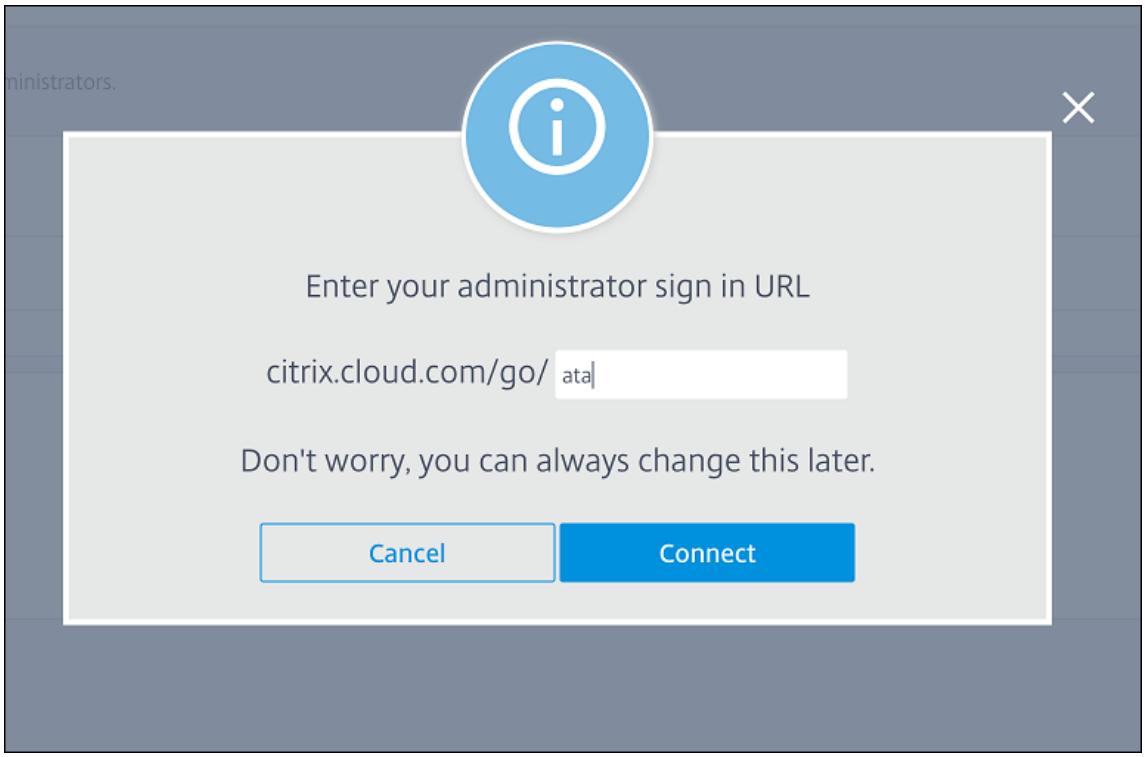
- Informations d'identification utilisateur Azure Active Directory
- Les groupes d'utilisateurs dans Active Directory doivent correspondre aux groupes d'utilisateurs dans Azure Active Directory.
- Les noms d'utilisateur et les adresses e-mail d'Active Directory doivent correspondre à ceux d'Azure Active Directory.
- Compte Citrix Cloud avec Citrix Cloud Connector installé pour la synchronisation des services d'annuaire
- NetScaler Gateway. Citrix vous recommande d'activer l'authentification basée sur des certificats ou Azure AD pour une expérience d'authentification unique complète. Si vous utilisez l'authentification LDAP sur NetScaler Gateway pour l'inscription MAM, les utilisateurs finaux bénéficient d'une double invite d'authentification lors de l'inscription. Pour de plus amples informations, consultez Authentification certificat client ou certificat + domaine.
- Dans les profils d'inscription pour Android Enterprise, définissez **Autoriser les utilisateurs à décliner la gestion des appareils** sur **Désactivé**. Si les utilisateurs déclinent la gestion des appareils, ils ne peuvent pas s'inscrire à l'aide d'un fournisseur d'identité pour s'authentifier. Pour de plus amples informations, consultez la section Sécurité de l'inscription.

Configurer Citrix Cloud pour utiliser Azure Active Directory en tant que fournisseur d'identité

Pour configurer ce service en vue d'une utilisation avec Citrix Secure Hub, configurez Azure Active Directory dans Citrix Cloud.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Accédez à https://citrix.cloud.com et connectez-vous à votre compte Citrix Cloud.
2. Dans le menu Citrix Cloud, accédez à la page **Gestion des identités et des accès** et connectez-vous à Azure Active Directory.
3. Entrez votre URL de connexion administrateur, puis cliquez sur **Connecter**.



4. Une fois que vous vous êtes connecté, votre compte Azure Active Directory se connecte à Citrix Cloud. La page **Gestion des identités et des accès > Authentification** indique les comptes à utiliser pour vous connecter à vos comptes Citrix Cloud et Azure AD.
5. Pour activer l'authentification avec Azure AD pour les utilisateurs inscrits via l'application Citrix Secure Hub, sous **Configuration de l'espace de travail > Authentification**, sélectionnez **Azure Active Directory**. Une fois la configuration terminée, vous pouvez inscrire des machines utilisateur via Citrix Secure Hub.

Configurer Identité Citrix en tant que type de fournisseur d'identité pour Citrix Endpoint Management

Cette configuration s'applique uniquement aux utilisateurs inscrits via Citrix Secure Hub. Après avoir configuré Azure Active Directory dans Citrix Cloud, configurez Citrix Endpoint Management comme suit.

1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Fournisseur d'identité (IDP)**, puis cliquez sur **Ajouter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Sur la page **Fournisseur d'identité (IDP)**, configurez les éléments suivants :

   - **Nom IdP :** entrez un nom unique pour identifier la connexion de fournisseur d'identité que vous créez.
   - **Type de fournisseur d'identité :** choisissez **Plate-forme d'identité Citrix**.
   - **Domaine d'authentification :** choisissez **Azure Active Directory**. Ce domaine correspond au domaine du fournisseur d'identité sur la page Citrix Cloud **Configuration de l'espace de travail > Authentification**.

3. Cliquez sur **Suivant**. Sur la page **Utilisation des revendications IdP**, configurez les éléments suivants :

   - **Type d'identificateur d'utilisateur :** par défaut, ce champ est défini sur **userPrincipalName**. Assurez-vous de configurer tous les utilisateurs avec le même identifiant dans votre répertoire Active Directory local et dans Azure Active Directory. Citrix Endpoint Management utilise cet identifiant pour mapper les utilisateurs du fournisseur d'identité avec les utilisateurs Active Directory locaux.
   - **Chaîne d'identificateur d'utilisateur :** ce champ est renseigné automatiquement.

4. Cliquez sur **Suivant**, vérifiez la page **Résumé**, puis cliquez sur **Enregistrer**.

   Les utilisateurs de Citrix Secure Hub, de la console Citrix Endpoint Management et du portail en libre-service peuvent maintenant se connecter avec leurs informations d'identification Azure Active Directory. Les utilisateurs Citrix Secure Hub qui sont associés à un domaine peuvent utiliser Citrix Secure Hub pour se connecter à l'aide de leurs informations d'identification Azure AD. Citrix Secure Hub utilise l'authentification de certificat client pour les appareils MAM.

Flux d'authentification Citrix Secure Hub

Citrix Endpoint Management utilise le flux suivant pour authentifier les utilisateurs avec Azure AD en tant que fournisseur d'identité sur les appareils inscrits via Citrix Secure Hub :

1. Un utilisateur démarre Citrix Secure Hub.
2. Citrix Secure Hub transmet la demande d'authentification à Identité Citrix, qui transmet la demande à Azure Active Directory.
3. L'utilisateur saisit son nom d'utilisateur et son mot de passe Azure Active Directory.
4. Azure Active Directory valide l'utilisateur et envoie un code à Identité Citrix.
5. Identité Citrix envoie le code à Citrix Secure Hub, qui envoie le code à Citrix Endpoint Management Server.
6. Citrix Endpoint Management obtient un jeton d'identification en utilisant le code et le secret, puis valide les informations utilisateur contenues dans le jeton d'identification. Citrix Endpoint Management renvoie un ID de session.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Authentification avec Azure Active Directory via NetScaler Gateway pour l'inscription MAM

March 1, 2024

Citrix Endpoint Management prend en charge l'authentification avec les informations d'identification Azure Active Directory (Azure AD) via NetScaler Gateway. Cette méthode d'authentification est disponible uniquement pour les utilisateurs qui s'inscrivent à MAM via l'application Citrix Secure Hub.

Logiciels requis

Pour configurer Citrix Endpoint Management afin d'utiliser Azure AD via NetScaler Gateway en tant que fournisseur d'identité pour les appareils inscrits à MAM, assurez-vous que les prérequis suivants sont satisfaits :

- Configurez Citrix Endpoint Management avec Azure AD via Citrix Cloud en tant que fournisseur d'identité pour les appareils inscrits à MDM. Pour plus d'informations sur la configuration d'Azure AD pour MDM, consultez la section Authentification avec Azure Active Directory via Citrix Cloud.
- Connectez Azure AD à Citrix Cloud. Pour de plus amples informations, consultez la section Connecter Azure Active Directory à Citrix Cloud.
- Activez les feature flags appropriés suivants en fonction de la plateforme, respectivement :
  - iOS :
    - iOS-V3Form-MAM
    - iOS-SAMLAuth-MAM
  - Android :
    - Android-V3Form-MAM
    - Android-SAMLAuth-MAM

> **Remarque :**
>
> pour activer le feature flag approprié dans votre environnement, remplissez le formulaire Podio.

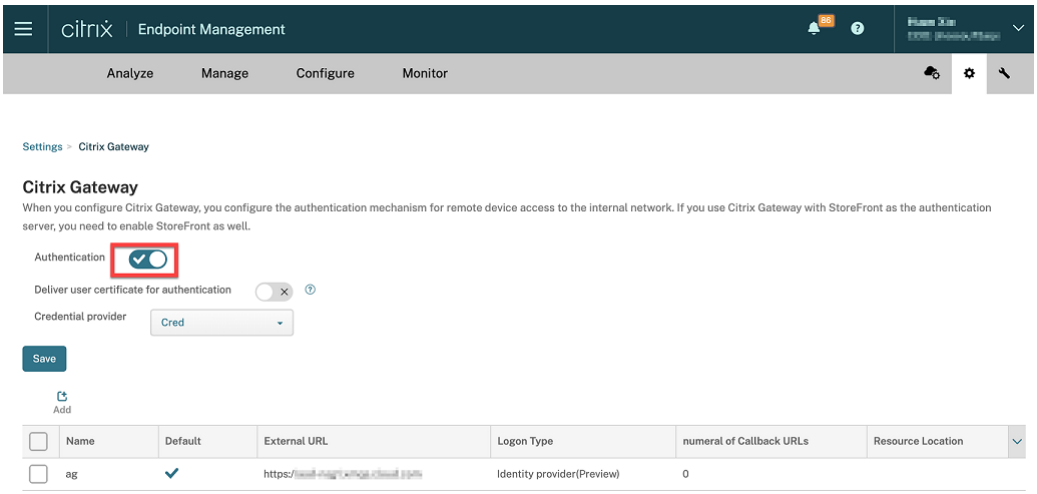
- Pour Android, activez **Android Enterprise**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Remarque :**
>
> cette fonctionnalité n'est ni testée ni vérifiée dans l'ancien mode Administrateur de machine Android. Ce mode n'est pas pris en charge.

Configurer Azure AD pour MAM en tant que fournisseur d'identité

1. Configurez NetScaler Gateway dans Endpoint Management comme suit :
   a) Connectez-vous à la console Citrix Endpoint Management, puis cliquez sur l'icône **Paramètres** .
   b) Cliquez sur **NetScaler Gateway** sous **Serveur**.
   c) Activez le bouton bascule **Authentification**.



   d) Assurez-vous que le **Type de connexion** de la passerelle est *Fournisseur d'identité*.
   e) Cliquez sur **Enregistrer**.
2. Configurez Azure AD en tant que fournisseur d'identité SAML à l'aide de Configurer Azure AD en tant que fournisseur d'identité SAML.
3. Configurez NetScaler ADC en tant que fournisseur de services SAML à l'aide de la stratégie avancée en utilisant Configurer NetScaler ADC en tant que fournisseur de services SAML.
4. Créez un serveur virtuel AAA en utilisant Pour configurer un serveur virtuel d'authentification à l'aide de l'interface graphique.
5. Configurez le serveur virtuel AAA à l'aide de Configurer le serveur virtuel d'authentification.
6. Créez et configurez le profil d'authentification à l'aide des profils d'authentification.
7. Liez le profil d'authentification au serveur virtuel Gateway et enregistrez toutes les configurations.

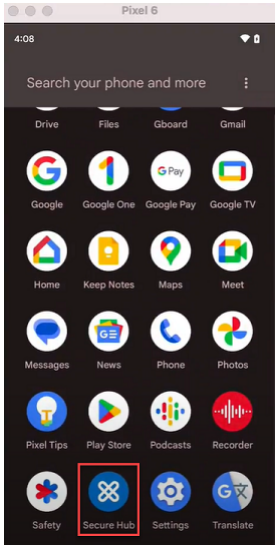
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Azure AD est désormais ajouté en tant que fournisseur d'identité pour les appareils inscrits à MAM et vous pouvez les authentifier à l'aide d'Azure AD.

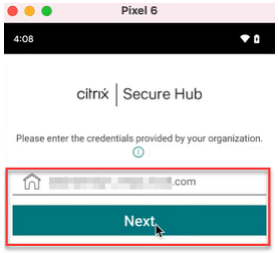
Comportement attendu

L'exemple suivant utilise un appareil Android :

1. Sur votre appareil mobile, ouvrez l'application Citrix Secure Hub.



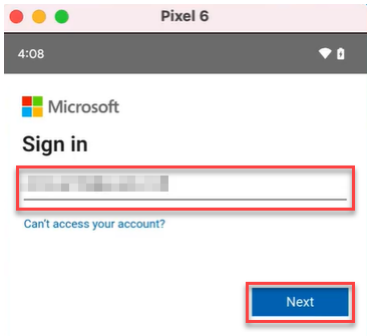
2. Fournissez les autorisations requises.
3. Sur la page de connexion, saisissez les informations d'identification fournies par votre organisation, puis appuyez sur **Suivant**.



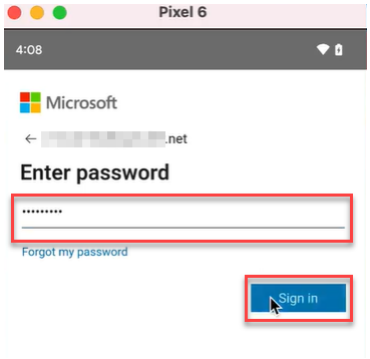
Vous êtes redirigé vers la page de connexion Microsoft.

4. Sur la page de connexion Microsoft, entrez votre adresse e-mail, puis appuyez sur **Suivant**.

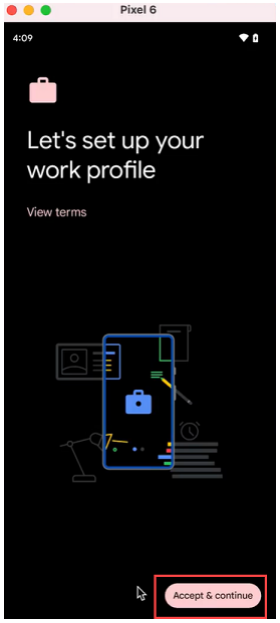
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Entrez le mot de passe, puis appuyez sur **Se connecter**.

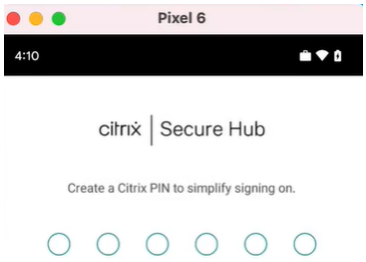


6. Sur la page **Configurons votre profil professionnel**, touchez **Accepter et continuer**.



7. Créez le code PIN pour l'application Citrix Secure Hub et confirmez-le.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Vous avez été redirigé vers la page d'accueil de Citrix Secure Hub.

Authentification avec Okta via Citrix Cloud

March 1, 2024

Citrix Endpoint Management prend en charge l'authentification avec les informations d'identification Okta via Citrix Cloud. Cette méthode d'authentification est disponible uniquement pour les utilisateurs qui s'inscrivent à MDM via l'application Citrix Secure Hub.

Les appareils qui s'inscrivent dans MAM ne peuvent pas s'authentifier à l'aide des informations d'identification Okta via Citrix Cloud. Pour utiliser Citrix Secure Hub avec MDM+MAM, configurez Citrix Endpoint Management pour utiliser NetScaler Gateway pour l'inscription MAM. Pour de plus amples informations, consultez NetScaler Gateway et Citrix Endpoint Management.

Citrix Endpoint Management utilise le service Citrix Cloud, fournisseur d'identité Citrix, pour se fédérer avec Okta. Citrix recommande d'utiliser le fournisseur d'identité Citrix plutôt qu'une connexion directe à Okta.

Citrix Endpoint Management prend en charge l'authentification avec Okta pour les plates-formes suivantes :

- Appareils iOS et macOS non inscrits à l'Apple Business Manager ou à l'Apple School Manager
- Appareils iOS et macOS inscrits à Apple Business Manager
- Appareils Android Enterprise (version préliminaire), pour BYOD et modes entièrement gérés

L'authentification avec Okta via Citrix Cloud présente les limitations suivantes :

- Non disponible pour les comptes locaux Citrix Endpoint Management.
- Ne prend pas en charge l'authentification via Okta pour les invitations d'inscription. Si vous envoyez une invitation d'inscription contenant une adresse URL d'inscription aux utilisateurs, les utilisateurs s'authentifient via LDAP au lieu d'Okta.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Logiciels requis

- Informations d'identification utilisateur Okta
- Les groupes d'utilisateurs dans Active Directory doivent correspondre aux groupes d'utilisateurs dans Okta.
- Les noms d'utilisateur et les adresses e-mail d'Active Directory doivent correspondre à ceux d'Okta.
- Compte Citrix Cloud avec Citrix Cloud Connector installé pour la synchronisation des services d'annuaire
- NetScaler Gateway. Citrix vous recommande d'activer l'authentification basée sur des certificats pour une expérience d'authentification unique complète. Si vous utilisez l'authentification LDAP sur NetScaler Gateway pour l'inscription MAM, les utilisateurs finaux bénéficient d'une double invite d'authentification lors de l'inscription. Pour de plus amples informations, consultez Authentification certificat client ou certificat + domaine.
- Dans les profils d'inscription pour Android Enterprise, définissez **Autoriser les utilisateurs à décliner la gestion des appareils** sur **Désactivé**. Si les utilisateurs déclinent la gestion des appareils, ils ne peuvent pas s'inscrire à l'aide d'un fournisseur d'identité pour s'authentifier. Pour de plus amples informations, consultez la section Sécurité de l'inscription.

Configurer Citrix Cloud pour utiliser Okta en tant que fournisseur d'identité

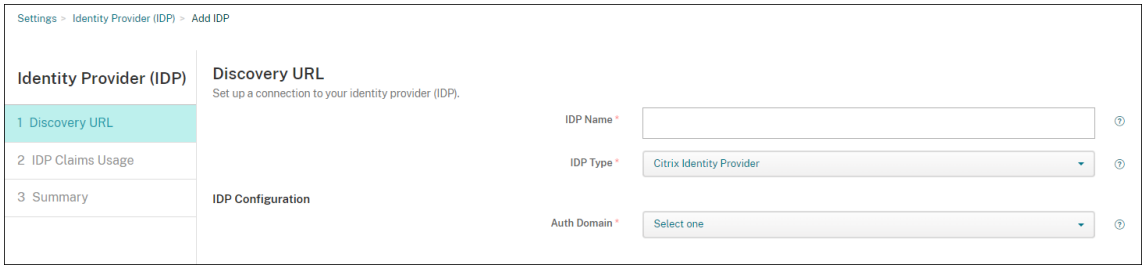
Pour configurer Okta dans Citrix Cloud, consultez la section Connecter Okta en tant que fournisseur d'identité à Citrix Cloud.

Configurer Identité Citrix en tant que type de fournisseur d'identité pour Citrix Endpoint Management

Cette configuration s'applique uniquement aux utilisateurs inscrits via Citrix Secure Hub. Après avoir configuré Azure Active Directory dans Citrix Cloud, configurez Citrix Endpoint Management comme suit :

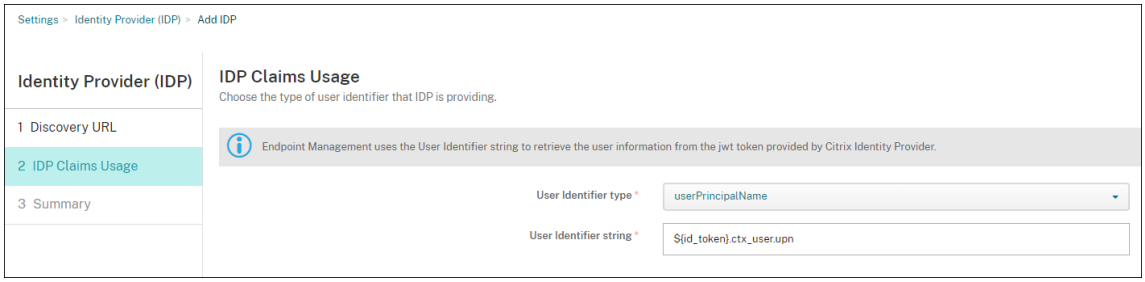
1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Fournisseur d'identité (IDP)**, puis cliquez sur **Ajouter**.
2. Sur la page **Fournisseur d'identité (IDP)**, configurez les éléments suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Nom IdP :** entrez un nom unique pour identifier la connexion de fournisseur d'identité que vous créez.
- **Type d'IdP :** choisissez **Fournisseur d'identité Citrix**.
- **Domaine d'authentification :** sélectionnez le domaine de Citrix Cloud. Si vous ne savez pas lequel choisir, votre domaine apparaît sur la page Citrix Cloud **Gestion des identités et des accès > Authentification**.

3. Cliquez sur **Suivant**. Dans la page **Utilisation des revendications IdP**, configurez les éléments suivants :



- **Type d'identificateur d'utilisateur :** ce champ est défini sur **userPrincipalName**. Assurez-vous de configurer tous les utilisateurs avec le même identifiant dans votre répertoire Active Directory local et dans Okta. Citrix Endpoint Management utilise cet identifiant pour mapper les utilisateurs du fournisseur d'identité avec les utilisateurs Active Directory locaux.
- **Chaîne d'identificateur d'utilisateur :** ce champ est renseigné automatiquement.

Une fois cette configuration effectuée, les utilisateurs Citrix Secure Hub qui sont associés à un domaine peuvent utiliser Citrix Secure Hub pour se connecter à l'aide de leurs informations d'identification Okta. Citrix Secure Hub utilise l'authentification de certificat client pour les appareils MAM.

Flux d'authentification Citrix Secure Hub

Citrix Endpoint Management utilise le flux suivant pour authentifier les utilisateurs avec Okta en tant que fournisseur d'identité sur les appareils inscrits via Citrix Secure Hub :

1. Un utilisateur démarre Citrix Secure Hub.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Citrix Secure Hub transmet la demande d'authentification à Identité Citrix, qui transmet la demande à Okta.
3. L'utilisateur tape son nom d'utilisateur et son mot de passe.
4. Okta valide l'utilisateur et envoie un code à Identité Citrix.
5. Identité Citrix envoie le code à Citrix Secure Hub, qui envoie le code à Citrix Endpoint Management Server.
6. Citrix Endpoint Management obtient un jeton d'identification en utilisant le code et le secret, puis valide les informations utilisateur contenues dans le jeton d'identification. Citrix Endpoint Management renvoie un ID de session.

Authentification avec Okta via NetScaler Gateway pour l'inscription MAM

March 1, 2024

Citrix Endpoint Management prend en charge l'authentification avec les informations d'identification Okta via NetScaler Gateway. Cette méthode d'authentification est disponible uniquement pour les utilisateurs qui s'inscrivent à MAM via l'application Citrix Secure Hub.

Logiciels requis

Pour configurer Citrix Endpoint Management afin d'utiliser Okta via NetScaler Gateway en tant que fournisseur d'identité pour les appareils inscrits à MAM, assurez-vous que les prérequis suivants sont satisfaits :

- Configurez Citrix Endpoint Management avec Okta via Citrix Cloud en tant que fournisseur d'identité pour les appareils inscrits à MDM. Pour plus d'informations sur la configuration d'Okta pour MDM, consultez la section Authentification avec Okta via Citrix Cloud.
- Activez les feature flags appropriés suivants en fonction de la plateforme, respectivement :
  - iOS :
    - iOS-V3Form-MAM
    - iOS-SAMLAuth-MAM
  - Android :
    - Android-V3Form-MAM
    - Android-SAMLAuth-MAM

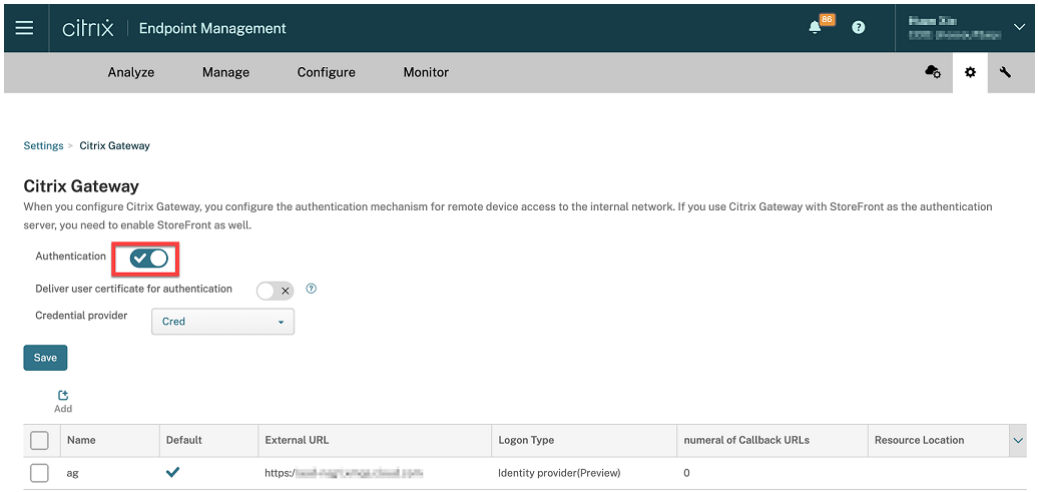
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Remarque :**
>
> pour activer le feature flag approprié dans votre environnement, remplissez le formulaire Podio.

- Téléchargez et installez la dernière version de Citrix Secure Hub.
- Assurez-vous que le service Okta est disponible pour votre organisation et que les utilisateurs et groupes concernés sont créés ou importés dans Okta.

Configurer NetScaler Gateway dans Citrix Endpoint Management

1. Connectez-vous à la console Citrix Endpoint Management, puis cliquez sur l'icône **Paramètres** .
2. Cliquez sur **NetScaler Gateway** sous **Serveur**.
3. Activez le bouton bascule **Authentification**.



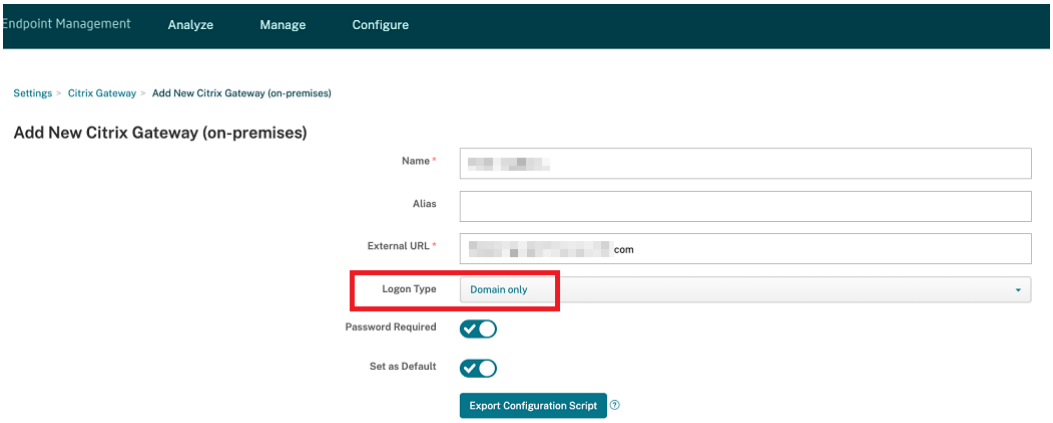
4. Assurez-vous que le **Type de connexion** de la passerelle est *Fournisseur d'identité*.
5. Cliquez sur **Enregistrer**.

Préparation de NetScaler Gateway sur site

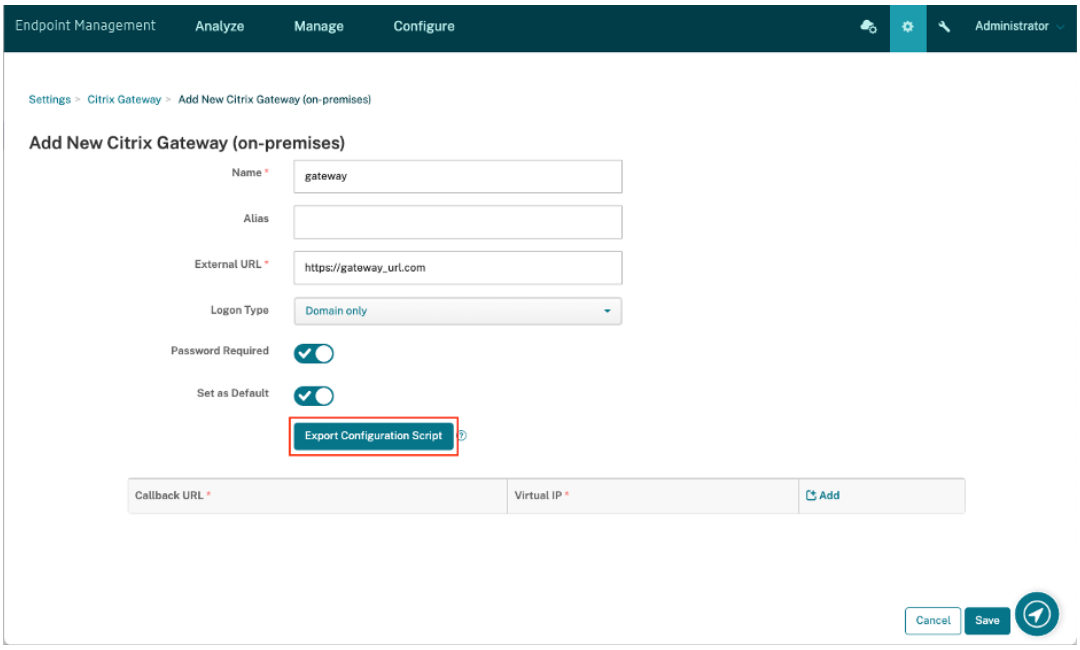
1. Si aucune instance NetScaler Gateway locale n'est configurée pour Citrix Endpoint Management, procédez comme suit :
   a) Dans la console Citrix Endpoint Management, cliquez sur l'icône **Paramètres** .
   b) Cliquez sur **NetScaler Gateway** sous **Serveur**.
   c) Cliquez sur **Modifier**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

d) Cliquez sur le menu déroulant **Type de connexion** et sélectionnez *Domaine uniquement*.

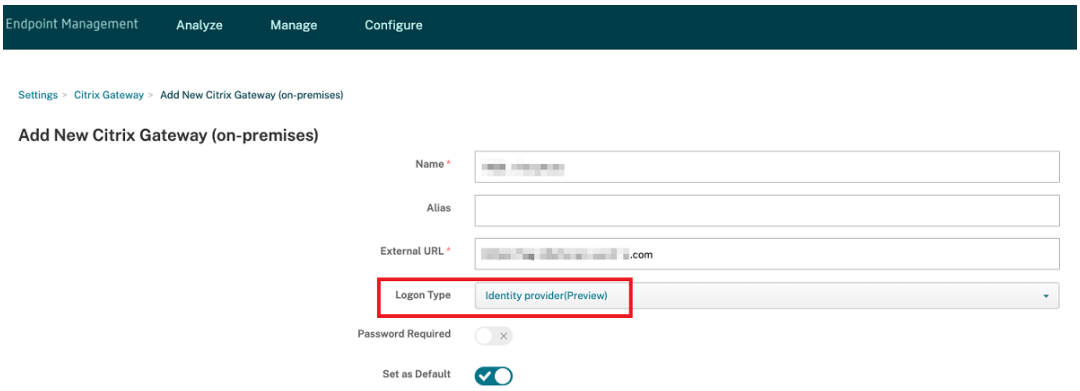


e) Cliquez sur **Exporter le script de configuration**.



Le **script de configuration d'exportation** est téléchargé.

f) Cliquez sur le menu déroulant **Type de connexion** et sélectionnez *Fournisseur d'identité*.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

g) Cliquez sur **Enregistrer**.

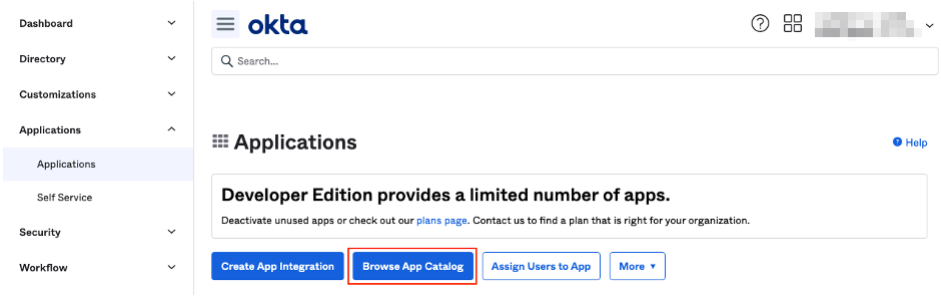
h) Ouvrez le fichier zip téléchargé et extrayez-en les fichiers.

i) Exécutez les scripts contenus dans les fichiers .txt extraits pour préparer NetScaler Gateway en local.

2. Connectez-vous à la console de gestion Citrix ADC, puis accédez à **NetScaler Gateway** > **Serveurs virtuels**.
3. Cliquez sur la passerelle correspondant à votre configuration Citrix Endpoint Management.
4. Annulez la liaison de toutes les stratégies d'authentification existantes sur NetScaler Gateway en local.

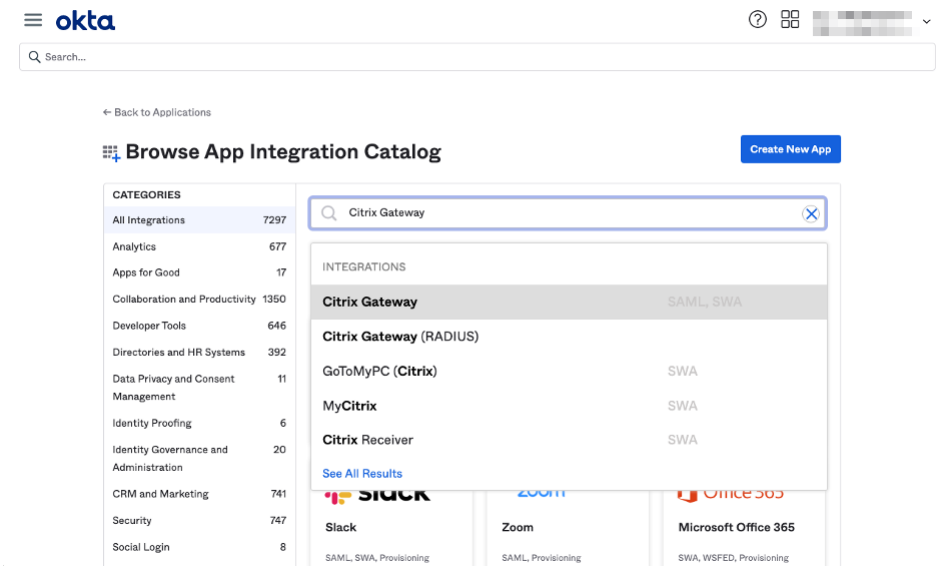
Configurer Okta

1. Connectez-vous à Okta en tant qu'administrateur.
2. Cliquez sur **Applications** > **Applications** > **Parcourir le catalogue d'applications**.

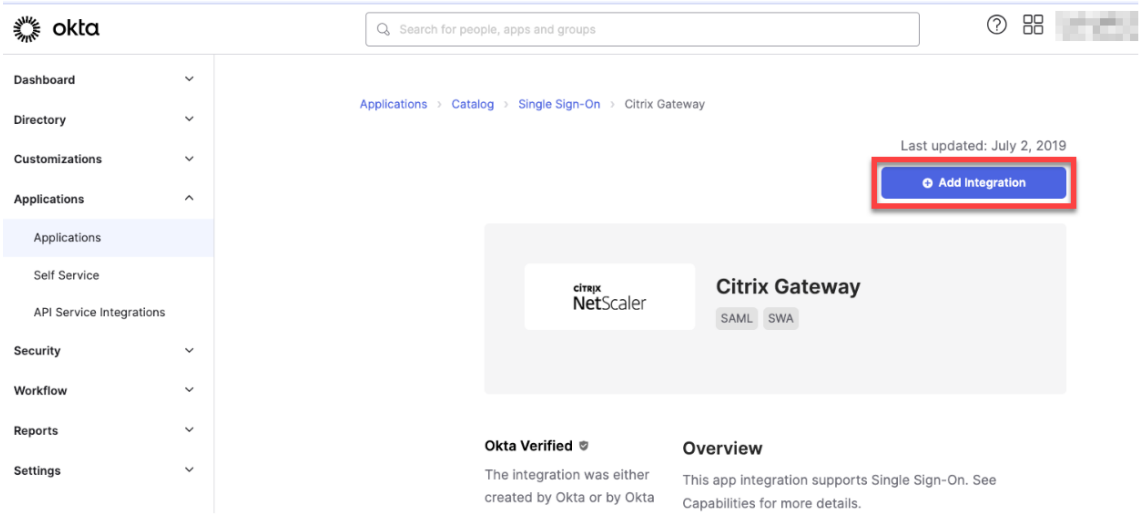


3. Tapez **NetScaler Gateway** dans la barre de recherche sous **Parcourir le catalogue d'intégration des applications**, puis sélectionnez **NetScaler Gateway (SAML, SWA)**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

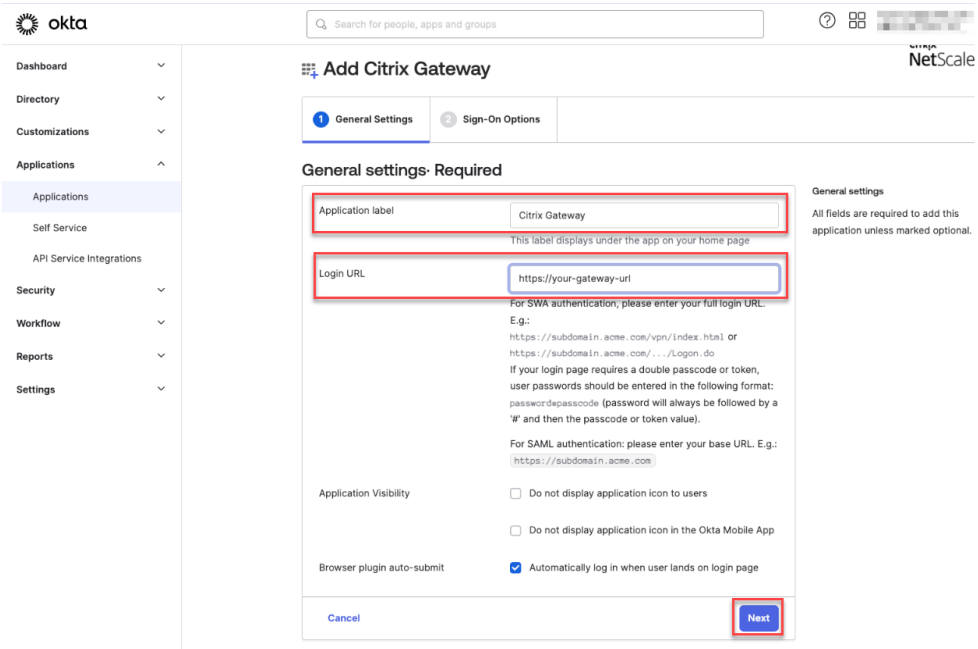


4. Cliquez sur **Ajouter une intégration**.



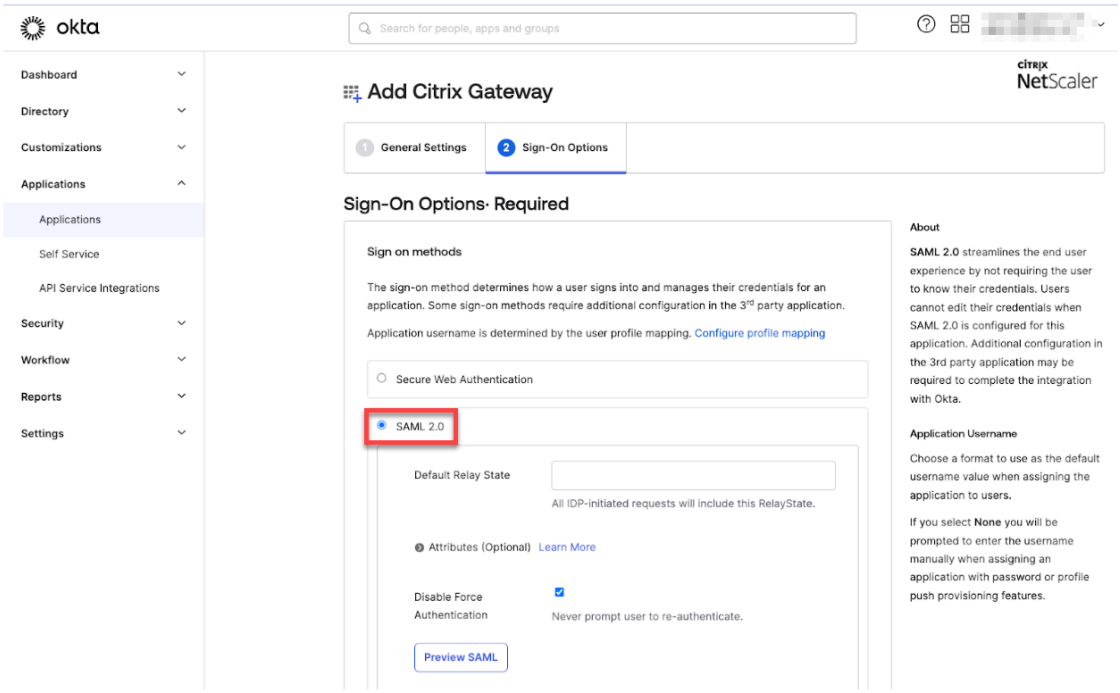
5. Entrez le nom approprié dans le champ **Libellé de l'application**.
6. Entrez l'URL du serveur virtuel de la passerelle dans le champ **URL d'ouverture de session**, puis cliquez sur **Suivant**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



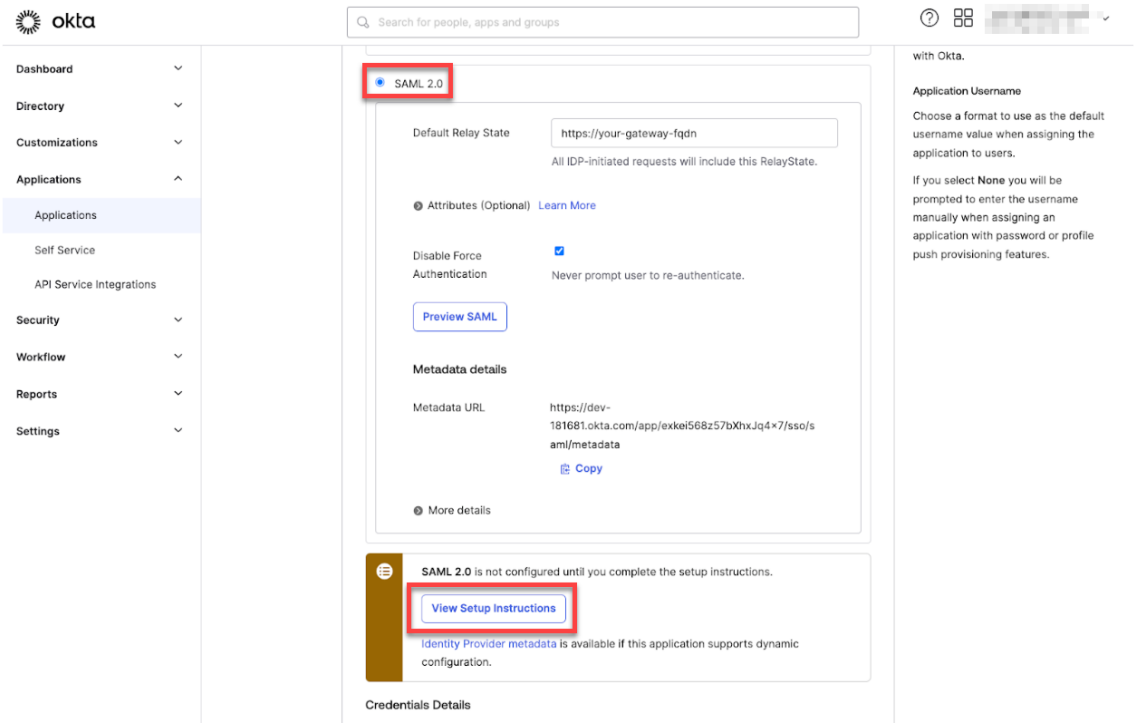
> **Remarque :**
>
> l'URL saisie dans le champ **URL d'ouverture de session** doit être identique à l'URL NetScaler Gateway pour les paramètres Citrix Endpoint Management.

7. Sous **Options de connexion requises** > **Méthodes de connexion**, sélectionnez **SAML 2.0.**



8. Cliquez sur **Afficher les instructions d'installation** et suivez les instructions fournies sur la page pour créer la stratégie SAML dans la console d'administration de la passerelle locale Citrix.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Remarque :

- Après avoir installé le certificat CA lors de la configuration de Netscaler Gateway version 11.1 ou ultérieure, créez une action SAML. Pour créer une action SAML, accédez à **Sécurité** > **AAA - Trafic des applications** > **Stratégies** > **Authentification** > **Stratégies avancées** > **Actions** > **Actions SAML**. Cliquez sur **Ajouter** et remplissez les informations comme indiqué sur la page précédente. Ne suivez pas la navigation proposée sur la page, à savoir **Netscaler Gateway** > **Stratégies** > **Authentification** > **SAML** > **Serveurs**.
- Ne suivez pas non plus les étapes fournies pour créer une stratégie SAML, car ces étapes utilisent la stratégie classique. Nous utilisons actuellement une stratégie avancée. Exécutez l'étape 9 suivante pour créer une stratégie SAML à l'aide d'une stratégie avancée.

9. Créez une stratégie SAML correspondante pour l'action SAML et liez la stratégie au serveur virtuel d'authentification comme suit :

   a) Accédez à Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées et cliquez sur Ajouter.

   b) Sur la page Créer stratégie d'authentification, fournissez les informations suivantes :

      - **Nom** : spécifiez le nom de la stratégie SAML.
      - **Type d'action** : sélectionnez *SAML* comme type d'action d'authentification.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Action** : sélectionnez le profil de serveur SAML auquel lier la stratégie SAML.
- **Expression** : affiche le nom de la règle ou de l'expression utilisée par la stratégie SAML pour déterminer si l'utilisateur doit s'authentifier auprès du serveur SAML. Dans la zone de texte, définissez la valeur **rule** = `true` pour que la stratégie SAML prenne effet et que l'action SAML correspondante soit exécutée.

c) Liez la stratégie SAML au serveur virtuel VPN et liez le serveur virtuel VPN au serveur virtuel d'authentification via un profil d'authentification. Pour plus d'informations sur la procédure de liaison, consultez la section Lier la stratégie d'authentification.

10. Créez un serveur virtuel AAA en utilisant Pour configurer un serveur virtuel d'authentification à l'aide de l'interface graphique.
11. Configurez le serveur virtuel AAA à l'aide de Configurer le serveur virtuel d'authentification.
12. Créez et configurez le profil d'authentification à l'aide des profils d'authentification.
13. Liez le profil d'authentification au serveur virtuel Gateway et enregistrez toutes les configurations.
14. Après avoir créé la stratégie SAML dans la console d'administration de la passerelle locale Citrix, cliquez sur Terminé.

    À présent, vous devez être en mesure de voir deux applications pour l'intégration de Citrix Endpoint Management, à savoir une application Web pour Citrix Cloud et une application SAML pour l'authentification MAM de Citrix Endpoint Management.
15. Attribuez les utilisateurs et groupes concernés à l'application SAML que vous venez de créer.

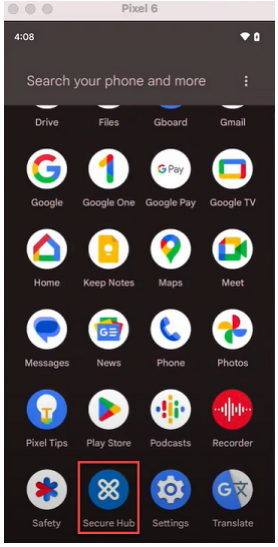
Okta est désormais ajouté en tant que fournisseur d'identité pour les appareils inscrits à MAM et vous pouvez les authentifier à l'aide d'Okta.

Comportement attendu

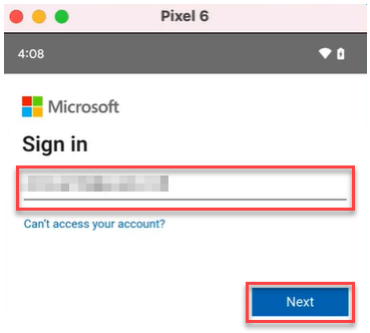
L'exemple suivant utilise un appareil Android :

1. Sur votre appareil mobile, ouvrez l'application Citrix Secure Hub.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

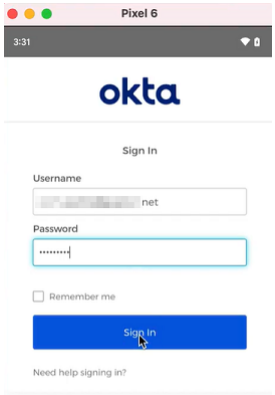


2. Fournissez les autorisations requises.
3. Sur la page de connexion, saisissez les informations d'identification fournies par votre organisation, puis appuyez sur **Suivant**.



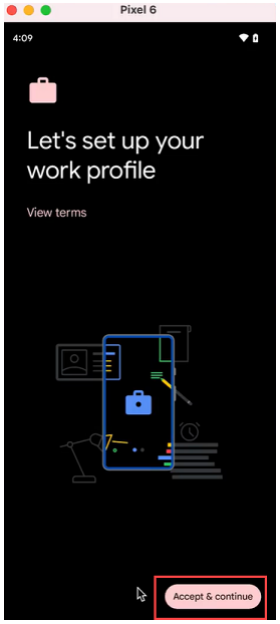
Vous êtes redirigé vers la page de connexion d'Okta.

4. Sur la page de connexion d'Okta, saisissez vos informations d'identification, puis appuyez sur **Se connecter**.

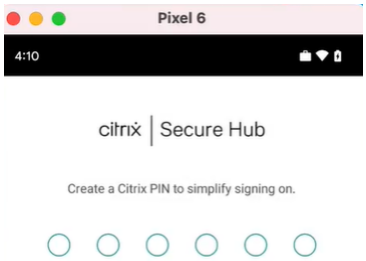


5. Sur la page **Configurons votre profil professionnel**, touchez **Accepter et continuer**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Créez le code PIN pour l'application Citrix Secure Hub et confirmez-le.



Vous avez été redirigé vers la page d'accueil de Citrix Secure Hub.

Authentification avec une passerelle NetScaler Gateway locale via Citrix Cloud

March 1, 2024

Citrix Endpoint Management prend en charge l'authentification avec une instance NetScaler Gateway locale via Citrix Cloud. Cette méthode d'authentification est disponible uniquement pour les utilisateurs qui s'inscrivent à MDM via l'application Citrix Secure Hub.

Les appareils qui s'inscrivent dans MAM ne peuvent pas s'authentifier à l'aide des informations d'identification d'une instance NetScaler Gateway locale via Citrix Cloud. Pour utiliser Citrix Secure Hub avec MDM+MAM, configurez Citrix Endpoint Management pour utiliser NetScaler Gateway pour l'

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

inscription MAM. Pour de plus amples informations, consultez NetScaler Gateway et Citrix Endpoint Management.

Citrix Endpoint Management prend en charge l'authentification avec une instance NetScaler Gateway locale via Citrix Cloud pour les plates-formes suivantes :

- Appareils iOS
- Appareils Android Enterprise, pour BYOD et modes entièrement gérés

> **Remarque :**
>
> Citrix Endpoint Management ne prend pas en charge l'authentification avec une instance NetScaler Gateway locale via Citrix Cloud pour les invitations d'inscription. Si vous envoyez une invitation d'inscription contenant une adresse URL d'inscription aux utilisateurs, les utilisateurs s'authentifient via LDAP au lieu d'une instance NetScaler Gateway locale en tant que fournisseur d'identité.

Citrix vous recommande d'activer l'authentification basée sur des certificats pour une expérience d'authentification unique complète. Si vous utilisez l'authentification LDAP sur NetScaler Gateway pour l'inscription MAM, les utilisateurs finaux bénéficient d'une double invite d'authentification lors de l'inscription. Pour de plus amples informations, consultez Authentification certificat client ou certificat + domaine.

Logiciels requis

- NetScaler Gateway. Citrix vous recommande d'activer l'authentification basée sur des certificats pour une expérience d'authentification unique complète. Si vous utilisez l'authentification LDAP sur NetScaler Gateway pour l'inscription MAM, les utilisateurs finaux bénéficient d'une double invite d'authentification lors de l'inscription. Pour de plus amples informations, consultez Authentification certificat client ou certificat + domaine.
- Compte Citrix Cloud avec Citrix Cloud Connector installé pour la synchronisation des services d'annuaire
- Citrix Secure Hub 20.5.0 et versions ultérieures.

Configurer Citrix Cloud pour utiliser NetScaler Gateway en tant que fournisseur d'identité

Pour configurer l'authentification NetScaler Gateway dans Citrix Cloud, consultez Connecter un NetScaler Gateway local en tant que fournisseur d'identité à Citrix Cloud.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer le fournisseur d'identité Citrix en tant que type de fournisseur d'identité pour Citrix Endpoint Management

Cette configuration s'applique uniquement aux utilisateurs inscrits via Citrix Secure Hub. Après avoir configuré NetScaler Gateway dans Citrix Cloud, configurez Citrix Endpoint Management comme suit.

1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Fournisseur d'identité (IDP)**, puis cliquez sur **Ajouter**.
2. Sur la page **Fournisseur d'identité (IDP)**, configurez les éléments suivants :
   - **Nom IdP :** entrez un nom unique pour identifier la connexion de fournisseur d'identité que vous créez.
   - **Type d'IdP :** choisissez **Fournisseur d'identité Citrix**.
   - **Domaine d'authentification :** choisissez **NetScaler Gateway**. Ce domaine correspond au domaine du fournisseur d'identité sur la page Citrix Cloud **Configuration de l'espace de travail > Authentification**.
3. Cliquez sur **Suivant**. Sur la page **Utilisation des revendications IdP**, configurez les éléments suivants :
   - **Type d'identificateur d'utilisateur :** par défaut, ce champ est défini sur **userPrincipalName**.
   - **Chaîne d'identificateur d'utilisateur :** ce champ est renseigné automatiquement.
4. Cliquez sur **Suivant**, vérifiez la page **Résumé**, puis cliquez sur **Enregistrer**.

   Vous pouvez désormais inscrire des machines utilisateur via Citrix Secure Hub à l'aide d'une instance NetScaler Gateway locale en tant que fournisseur d'identité.

Flux d'authentification Citrix Secure Hub

Citrix Endpoint Management utilise le flux suivant pour authentifier les utilisateurs avec une instance NetScaler Gateway locale en tant que fournisseur d'identité sur les appareils inscrits via Citrix Secure Hub :

1. Un utilisateur démarre Citrix Secure Hub.
2. Citrix Secure Hub transmet la demande d'authentification à Identité Citrix, qui transmet la demande à une instance NetScaler Gateway locale.
3. L'utilisateur tape son nom d'utilisateur et son mot de passe.
4. Une instance NetScaler Gateway locale valide l'utilisateur et envoie un code à Identité Citrix.
5. Identité Citrix envoie le code à Citrix Secure Hub, qui envoie le code à Citrix Endpoint Management Server.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Citrix Endpoint Management obtient un jeton d'identification en utilisant le code et le secret, puis valide les informations utilisateur contenues dans le jeton d'identification. Citrix Endpoint Management renvoie un ID de session.

Authentification nFactor

March 1, 2024

L'authentification nFactor vous permet d'utiliser tous les modes d'authentification actuellement possibles avec NetScaler lorsque vous utilisez Citrix Secure Hub. Elle renforce la sécurité d'une application en obligeant les utilisateurs à fournir plusieurs preuves d'identité pour y accéder. Pour plus d'informations sur l'authentification nFactor, consultez Authentification multifacteur (nFactor).

En outre, pour plus d'informations sur les différentes méthodes d'authentification et d'autorisation et sur la manière de les configurer, consultez Authentification et autorisation.

Citrix Endpoint Management prend en charge les types d'authentification suivants avec l'authentification nFactor :

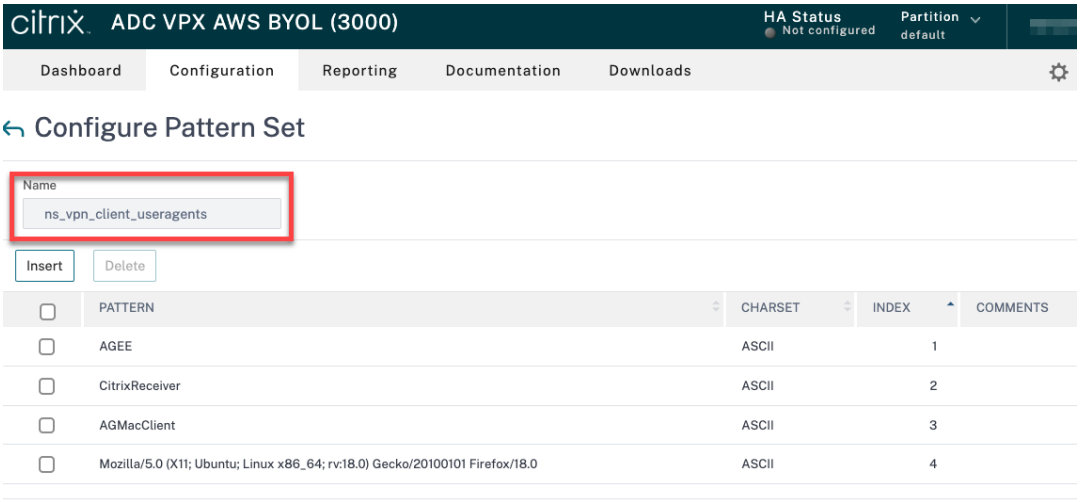
- Local
- LDAP (Lightweight Directory Access Protocol)
- RADIUS
- SAML
- Authentification du certificat client

Logiciels requis

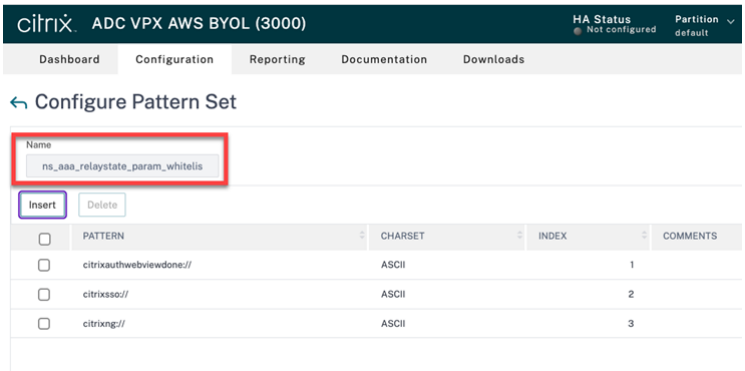
Pour configurer Citrix Endpoint Management afin qu'il utilise l'authentification nFactor, assurez-vous que les conditions préalables suivantes sont remplies :

- Assurez-vous que vous utilisez NetScaler 13.0 ou une version ultérieure.
- Assurez-vous d'avoir configuré les paramètres de jeu de modèles suivants dans NetScaler pour vos appareils Android et iOS :
  - Ns_vpn_client_useragents

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



– Ns_aaa_relaystate_param_whitelist



- Assurez-vous d'avoir installé la dernière version de Citrix Secure Hub depuis Apple ou Google Play.
- Assurez-vous d'utiliser la stratégie d'authentification avancée dans NetScaler Gateway.
- Assurez-vous de définir la propriété client **ENABLE_MAM_NFACTOR_SSO** sur **True** pour les applications locales et dans le cloud. Pour plus d'informations sur la propriété **ENABLE_MAM_NFACTOR_SSO**, consultez Référence des propriétés du client.

> **Remarque :**
>
> Si la propriété client **Enable nFactor SSO** est définie sur **False**, vous devez vous assurer que les stratégies d'authentification classiques sont liées à NetScaler Gateway.

Configurer l'authentification nFactor

Configurez l'authentification nFactor pour Citrix Endpoint Management en fonction de la configuration de votre NetScaler Gateway, comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Endpoint Management est déjà configuré avec NetScaler Gateway à l'aide de la stratégie d'authentification classique. Pour plus d'informations, consultez Mettre à jour la stratégie classique vers la stratégie d'authentification avancée dans le NetScaler Gateway existant.
- Configuration de Citrix Endpoint Management avec NetScaler Gateway à l'aide de la stratégie d'authentification avancée. Pour plus d'informations, consultez Configurer l'installation de NetScaler Gateway à l'aide de la stratégie avancée.

Mettre à jour la stratégie classique vers la stratégie d'authentification avancée dans le NetScaler Gateway existant

Si votre Citrix Endpoint Management est déjà configuré à l'aide de la stratégie d'authentification classique de NetScaler Gateway, vous devez mettre à jour la stratégie d'authentification classique vers la stratégie d'authentification avancée à l'aide de l'une des méthodes suivantes :

- Créez une nouvelle stratégie d'authentification avancée et modifiez la configuration de la passerelle pour utiliser la stratégie d'authentification avancée. Pour plus d'informations, consultez la section Stratégies d'authentification.
- Mettez à jour la stratégie d'authentification classique vers la stratégie d'authentification avancée. Pour plus d'informations, consultez Conversion d'expressions de stratégie à l'aide de l'outil NSPEPI.

Configurer l'installation de NetScaler Gateway à l'aide de la stratégie avancée

Pour configurer l'authentification nFactor pour Citrix Endpoint Management dans NetScaler Gateway à l'aide de la stratégie d'authentification avancée, consultez Configurer l'authentification nFactor.

> **Remarque :**
>
> - Vous pouvez choisir le type d'authentification approprié parmi les types d'authentification pris en charge.
> - Si vous utilisez le type d'authentification SAML, vous pouvez configurer SAML à l'aide de l'IDP MAM en utilisant l'une des méthodes suivantes :
> - Pour configurer à l'aide d'Azure Active Directory, consultez Authentification avec Azure Active Directory via NetScaler Gateway pour l'inscription MAM.
> - Pour configurer à l'aide d'Okta, consultez Authentification avec Okta via NetScaler Gateway pour l'inscription MAM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Comptes utilisateur, rôles et inscription

March 1, 2024

Vous effectuez des tâches de configuration utilisateur dans la console Citrix Endpoint Management sur l'onglet **Gérer** et la page **Paramètres**. Sauf indication contraire, les étapes des tâches suivantes sont fournies dans cet article.

- Mode et invitations d'inscription sécurisée
  - Depuis **Paramètres > Inscription**, configurez jusqu'à sept modes d'inscription sécurisée et envoyez des invitations d'inscription. Chaque mode d'inscription sécurisée dispose de son propre niveau de sécurité et d'étapes que les utilisateurs doivent suivre pour inscrire leurs appareils.
- Rôles des groupes et comptes utilisateur
  - Depuis **Paramètres > Contrôle d'accès basé sur rôle**, attribuez des rôles prédéfinis ou des ensembles d'autorisations aux utilisateurs et aux groupes. Ces autorisations contrôlent le niveau d'accès des utilisateurs aux fonctions du système. Pour plus d'informations, veuillez consulter la section Configurer des rôles avec RBAC.
  - Depuis **Paramètres > Modèles de notification**, créez ou mettez à jour des modèles de notification dans XenMobile à utiliser dans les actions automatisées, l'inscription, et les messages de notifications standard envoyés aux utilisateurs. Vous configurez les modèles de notification pour l'envoi de messages sur deux canaux différents : Citrix Secure Hub ou SMTP. Pour de plus amples informations, consultez : Création et mise à jour de modèles de notification.
- Groupes et comptes utilisateur :
  - Depuis **Gérer > Utilisateurs**, vous pouvez ajouter des comptes utilisateur locaux manuellement ou utiliser un fichier de provisioning .csv pour importer des comptes et gérer des groupes locaux. Cependant, la plupart des déploiements Citrix Endpoint Management se connectent à LDAP pour obtenir des informations sur les utilisateurs et les groupes. Vous préférerez peut-être créer des comptes utilisateur localement dans des cas d'utilisation suivants :
    - Dans des environnements, tels que la vente au détail, où les appareils sont partagés plutôt que dédiés à des utilisateurs individuels.
    - Si vous utilisez un répertoire non pris en charge, tel que Novell eDirectory.
  - Depuis **Paramètres > Workflows**, appliquez des workflows pour gérer la création et la suppression des comptes d'utilisateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

À propos des comptes utilisateur

Un compte utilisateur Citrix Endpoint Management est destiné à un utilisateur local, Active Directory ou cloud.

- **Administrateurs cloud :** Un administrateur cloud est un compte d'utilisateur spécial créé par Citrix Cloud lorsqu'un administrateur est ajouté à votre compte client Citrix Cloud. Un compte d'utilisateur cloud utilise le même nom d'utilisateur que le compte d'administrateur sur Citrix Cloud et le rôle Admin lui est attribué par défaut. Le compte d'utilisateur cloud fournit une authentification unique et exécute d'autres fonctions administratives.

  Pour ajouter des administrateurs à un compte Citrix Cloud, consultez la section Inviter de nouveaux administrateurs.

Pour les utilisateurs cloud :

- Vous pouvez modifier les rôles et les propriétés utilisateur des utilisateurs cloud via la console Citrix Cloud. Consultez la section Gérer les administrateurs Citrix Cloud.
- Pour modifier le mot de passe, consultez la section Administrateurs.
- Pour supprimer un utilisateur cloud, dans Citrix Cloud, accédez à **Gestion des identités et des accès > Administrateurs**. Cliquez sur les points de suspension à la fin de la ligne de l'utilisateur, puis sélectionnez **Supprimer un administrateur**.
- Vous ne pouvez pas ajouter d'utilisateurs cloud à un groupe local.

Configurer les modes d'inscription sécurisée

Vous configurez un mode d'inscription sécurisée d'appareil pour spécifier un niveau de sécurité et un modèle de notification pour l'inscription d'appareil dans Citrix Endpoint Management.

Citrix Endpoint Management offre six modes d'inscription sécurisée, chacun doté de son propre niveau de sécurité et de ses propres étapes que les utilisateurs doivent suivre pour inscrire leurs appareils. Vous configurez les modes d'inscription sécurisée dans la console Citrix Endpoint Management sur la page **Gérer > Invitations d'inscription**. Pour de plus amples informations, reportez-vous à la section Invitations d'inscription.

> **Remarque :**
>
> Si vous prévoyez d'utiliser des modèles de notification personnalisés, vous devez définir les modèles avant de configurer des modes d'inscription sécurisée. Pour de plus amples informations sur les modèles de notification, consultez la section Création et mise à jour de modèles de notification.

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

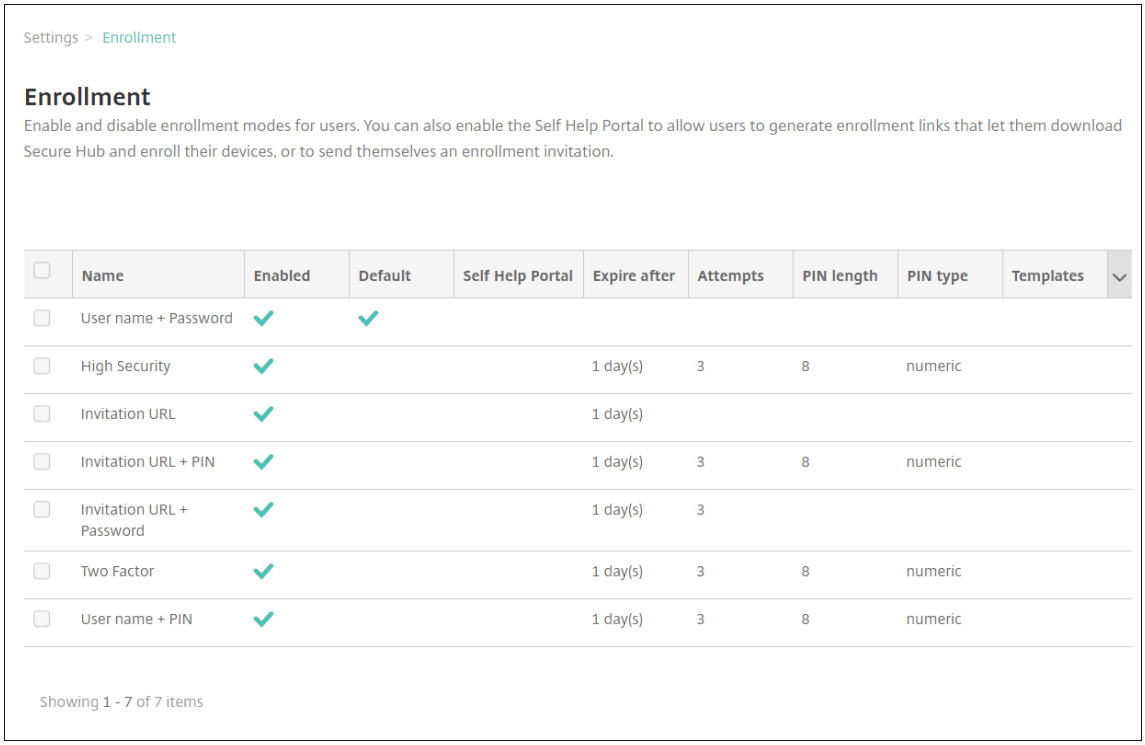
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Cliquez sur **Inscription**. La page **Inscription** s'affiche. Elle contient un tableau de tous les modes d'inscription sécurisée disponibles. Par défaut, tous les modes d'inscription sécurisée sont activés.

3. Sélectionnez un mode d'inscription sécurisée à modifier dans la liste. Ensuite, définissez le mode comme mode par défaut ou désactivez-le.

   Cochez la case en regard d'un mode d'inscription sécurisée pour afficher le menu d'options. Vous pouvez également cliquer dans la liste pour afficher le menu d'options sur le côté droit de la liste.

   > **Conseil :**
   >
   > Lorsque vous modifiez le mode d'inscription sécurisée, vous pouvez spécifier une date limite d'expiration après laquelle les utilisateurs ne peuvent pas inscrire leurs appareils. Pour de plus amples informations, consultez la section Pour modifier un mode d'inscription sécurisée dans cet article. Cette valeur s'affiche dans les pages de configuration des invitations d'inscription des utilisateurs et des groupes.



En fonction de votre plateforme, vous disposez des options suivantes pour les modes d'inscription sécurisée :

- Nom d'utilisateur + mot de passe
- URL d'invitation
- URL d'invitation + PIN

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- URL d'invitation + mot de passe
- Deux facteurs
- Nom d'utilisateur + PIN

Pour de plus amples informations sur les modes d'inscription sécurisée spécifiques à la plate-forme, consultez la section Modes d'inscription sécurisée par plate-forme.

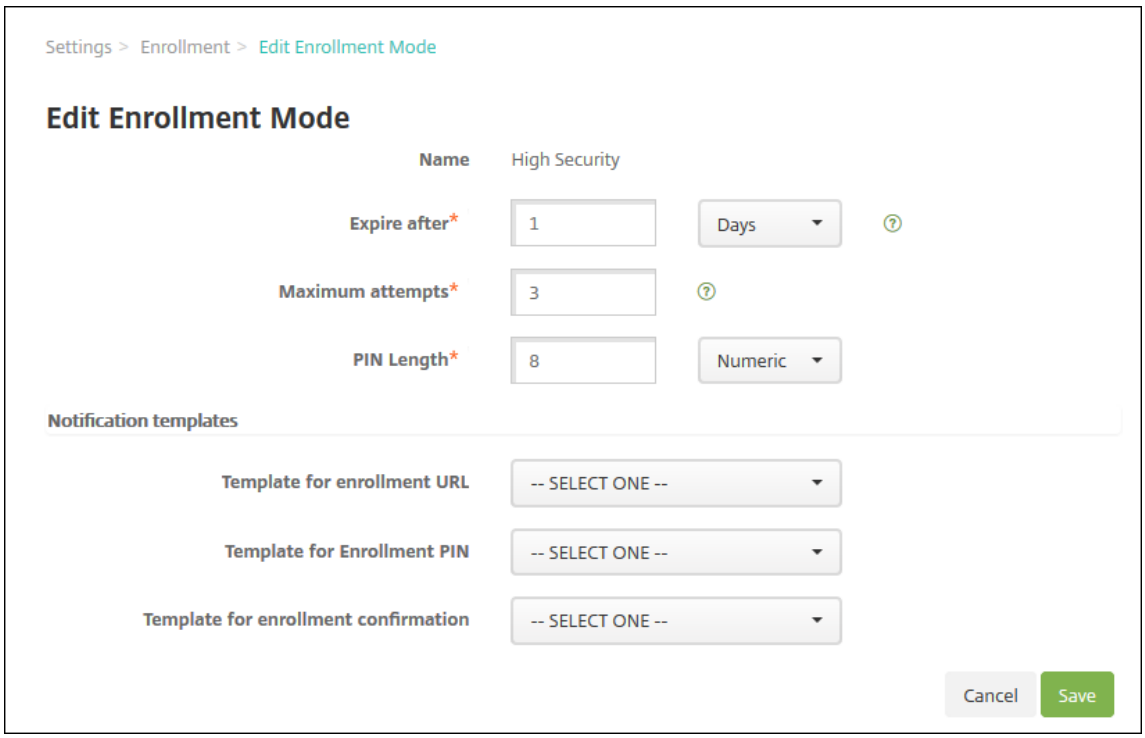
Vous pouvez utiliser les invitations d'inscription comme moyen efficace de restreindre la capacité de s'inscrire à des utilisateurs ou à des groupes spécifiques. Pour envoyer des invitations d'inscription, vous pouvez uniquement utiliser les modes d'inscription sécurisée **URL d'invitation**, **URL d'invitation + PIN** ou **URL d'invitation + mot de passe**. Pour les appareils qui sont inscrits avec **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + PIN**, les utilisateurs doivent entrer manuellement leurs informations d'identification dans Citrix Secure Hub.

Vous pouvez utiliser des invitations d'inscription avec code PIN unique (parfois appelé OTP) comme solution d'authentification à deux facteurs. Les invitations d'inscription OTP contrôlent le nombre d'appareils qu'un utilisateur peut inscrire. Les invitations OTP ne sont pas disponibles pour les appareils Windows.

Pour modifier un mode d'inscription sécurisée

1. Dans la liste **Inscription**, sélectionnez un mode d'inscription sécurisée, puis cliquez sur **Modifier**. La page **Modifier le mode d'inscription** apparaît. Selon le mode que vous sélectionnez, vous pouvez voir différentes options.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Modifiez les informations suivantes le cas échéant :

   - **Expire après :** entrez un délai d'expiration au-delà duquel les utilisateurs ne peuvent pas inscrire leurs appareils. Cette valeur s'affiche dans les pages de configuration des invitations d'inscription des utilisateurs et des groupes.

     Tapez **0** pour éviter que l'invitation n'expire.

   - **Jours :** dans la liste, cliquez sur **Jours** ou **Heures** afin qu'ils correspondent au délai d'expiration que vous avez entré dans **Expire après**.

   - **Nbre max de tentatives :** entrez le nombre de tentatives d'inscription qu'un utilisateur peut effectuer avant qu'il ne soit verrouillé du processus d'inscription. Cette valeur s'affiche dans les pages de configuration des invitations d'inscription des utilisateurs et des groupes.

     Tapez **0** pour autoriser un nombre illimité de tentatives.

   - **Longueur du code PIN :** entrez un chiffre pour définir la longueur du code PIN généré.

   - **Numérique :** dans la liste, cliquez sur **Numérique** ou **Alphanumérique** pour le type de code PIN.

   - **Modèles de notification :**

     – **Modèle pour l'URL d'inscription :** sélectionnez un modèle à utiliser pour l'adresse URL d'inscription. Par exemple, le modèle d'invitation d'inscription envoie aux util-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

isateurs un e-mail. Pour de plus amples informations sur les modèles de notification, consultez la section Création et mise à jour de modèles de notification.
  - **Modèle pour le PIN d'inscription :** dans la liste, sélectionnez un modèle à utiliser pour le PIN d'inscription.
  - **Modèle pour la confirmation d'inscription :** dans la liste, sélectionnez un modèle à utiliser pour informer un utilisateur que l'inscription a réussi.

3. Cliquez sur **Enregistrer**.

Pour définir un mode d'inscription sécurisée comme mode par défaut

Le mode d'inscription sécurisée par défaut est utilisé pour toutes les demandes d'inscription d'appareil, sauf si vous sélectionnez un autre mode d'inscription sécurisée. Si aucun mode d'inscription sécurisée n'est défini par défaut, vous devez créer une demande d'inscription pour chaque inscription d'appareil.

1. Si le mode d'inscription sécurisée que vous souhaitez utiliser par défaut n'est pas activé, sélectionnez-le et cliquez sur **Activer**. Les seuls modes d'inscription sécurisée que vous pouvez utiliser par défaut sont **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + code PIN**.
2. Sélectionnez le mode d'inscription sécurisée et cliquez sur **Par défaut**. Le mode sélectionné est maintenant le mode par défaut. Si un autre mode d'inscription sécurisée a été défini comme mode par défaut, le mode n'est plus le mode par défaut.

Pour désactiver un mode d'inscription sécurisée

La désactivation d'un mode d'inscription sécurisée rend ce dernier inutilisable, à la fois pour les invitations d'inscription de groupe et sur le portail en libre-service. Vous pouvez modifier la façon dont vous autorisez les utilisateurs à inscrire leurs appareils en désactivant un mode d'inscription sécurisée et en activant un autre.

1. Sélectionnez un mode d'inscription sécurisée.

   Vous ne pouvez pas désactiver le mode d'inscription sécurisée par défaut. Pour désactiver le mode d'inscription sécurisée par défaut, vous devez d'abord lui retirer son état de mode par défaut.
2. Cliquez sur **Désactiver**. Le mode d'inscription sécurisée n'est plus activé.

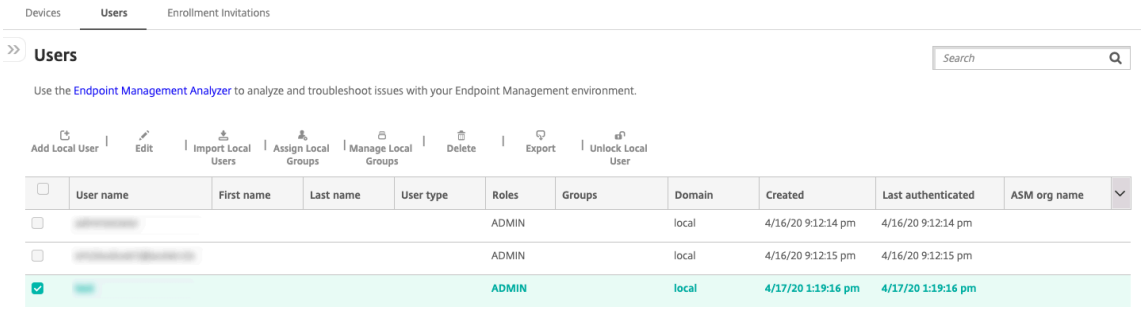
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ajouter, modifier, verrouiller ou supprimer des comptes utilisateur locaux

Vous pouvez ajouter des comptes d'utilisateur locaux à Citrix Endpoint Management manuellement ou vous pouvez utiliser un fichier de provisioning pour importer les comptes. Pour savoir comment importer des comptes utilisateur à l'aide d'un fichier de provisioning, consultez Importer comptes utilisateur.

Tous les administrateurs de Citrix Cloud sont créés en tant qu'administrateurs Citrix Endpoint Management. Si vous créez un administrateur Citrix Cloud avec un accès personnalisé, assurez-vous que cet accès inclut Citrix Endpoint Management. Pour plus d'informations sur l'ajout des administrateurs Citrix Cloud, consultez la section Ajouter des administrateurs.

1. Dans la console Citrix Endpoint Management, cliquez sur **Gérer > Utilisateurs**. La page **Utilisateurs** s'affiche.

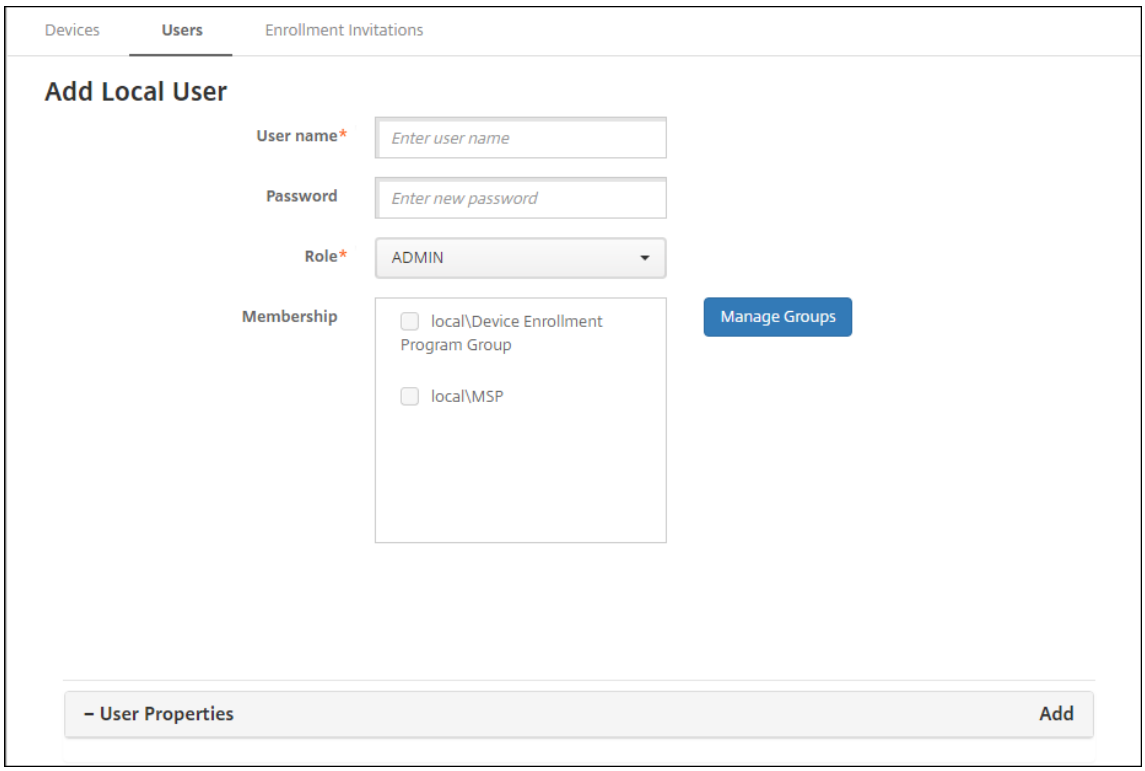


2. Cliquez sur **Afficher le filtre** pour filtrer la liste.

Pour ajouter un compte d'utilisateur local

1. Sur la page **Utilisateurs**, cliquez sur **Ajouter un utilisateur local**. La page **Ajouter un utilisateur local** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Pour configurer ces paramètres :

   - **Nom d'utilisateur :** entrez le nom (champ obligatoire). Vous pouvez inclure les éléments suivants dans les noms : espaces, lettres majuscules et lettres minuscules.
   - **Mot de passe :** entrez un mot de passe utilisateur (facultatif). Le mot de passe doit comporter au moins 14 caractères et répondre à tous les critères suivants :
     - Inclure au moins deux chiffres
     - Inclure au moins une lettre majuscule et une lettre minuscule
     - Inclure au moins un caractère spécial
     - N'incluez pas de mots du dictionnaire ou de mots restreints tels que votre nom d'utilisateur ou adresse e-mail Citrix.
     - N'incluez pas plus de trois caractères séquentiels (dans l'alphabet et sur le clavier) et répétitifs, tels que 1111, 1234 ou asdf
   - **Rôle :** cliquez sur le rôle de l'utilisateur dans la liste déroulante. Pour plus d'informations concernant les rôles, veuillez consulter la section Configurer des rôles avec RBAC. Les options possibles sont les suivantes :
     - ADMIN
     - DEVICE_PROVISIONING
     - SUPPORT
     - UTILISATEUR
   - **Adhésion :** dans la liste, cliquez sur le groupe ou les groupes auxquels ajouter l'utilisateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Propriétés utilisateur :** ajoutez des propriétés utilisateur (facultatif). Pour chaque propriété d'utilisateur que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Propriétés utilisateur :** dans la liste, cliquez sur une propriété, puis entrez l'attribut de la propriété utilisateur dans le champ en regard de la propriété.
  - Cliquez sur **Terminé** pour enregistrer la propriété utilisateur ou cliquez sur **Annuler**.

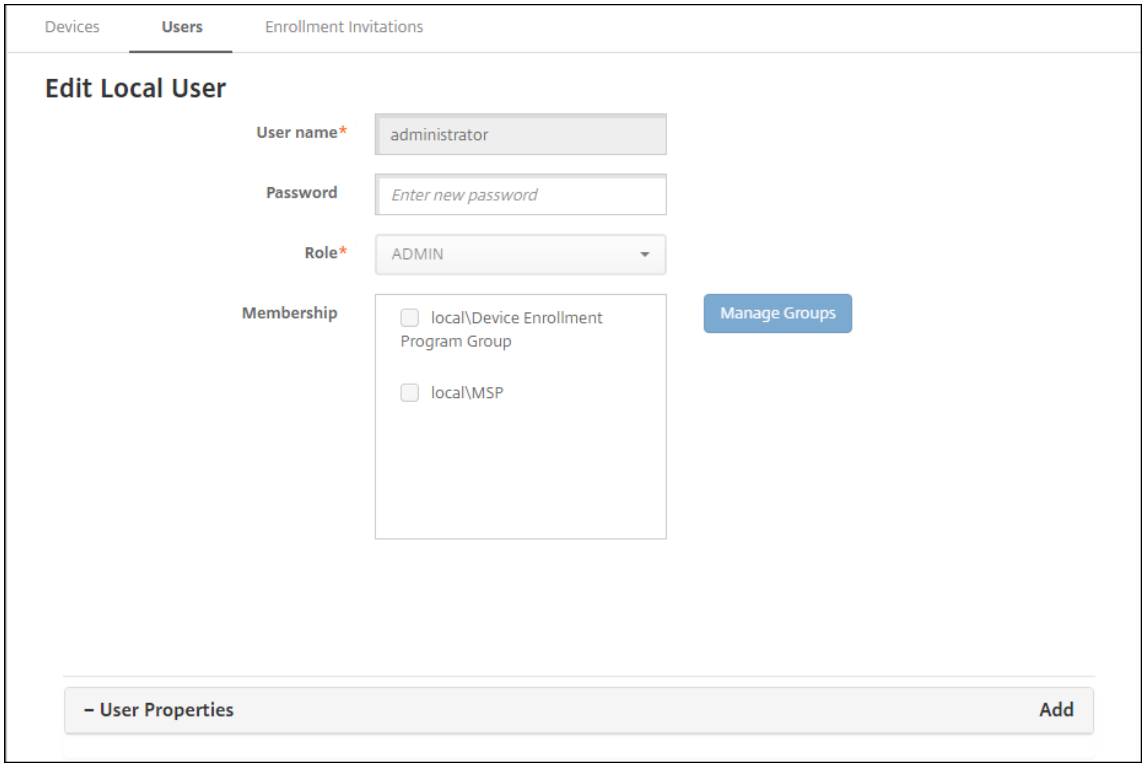
Pour supprimer une propriété utilisateur existante, placez le curseur sur la ligne contenant la propriété et cliquez sur le **X** sur le côté droit. La propriété est immédiatement supprimée.

Pour modifier une propriété utilisateur, cliquez sur la propriété et effectuez les modifications. Cliquez sur **Terminé** pour enregistrer les modifications ou sur **Annuler** pour laisser la propriété inchangée.

3. Cliquez sur **Enregistrer**. Après avoir créé un utilisateur, le champ **Type d'utilisateur** pour un compte d'utilisateur local reste vide.

Pour modifier un compte d'utilisateur local

1. Sur la page **Utilisateurs**, dans la liste des utilisateurs, cliquez pour sélectionner un utilisateur, puis cliquez sur **Modifier**. La page **Modifier un utilisateur local** apparaît.



2. Modifiez les informations suivantes le cas échéant :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Nom d'utilisateur :** vous ne pouvez pas modifier le nom d'utilisateur.
- **Mot de passe :** modifiez ou ajoutez un mot de passe utilisateur.
- **Rôle :** cliquez sur le rôle de l'utilisateur dans la liste déroulante.
- **Adhésion :** dans la liste, cliquez sur le groupe ou les groupes pour lesquels ajouter ou modifier le compte utilisateur. Pour supprimer le compte utilisateur d'un groupe, désactivez la case à cocher en regard du nom du groupe.
- **Propriétés utilisateur :** effectuez l'une des opérations suivantes :
  - Pour chaque propriété utilisateur que vous voulez modifier, cliquez sur la propriété et effectuez des modifications. Cliquez sur **Terminé** pour enregistrer les modifications ou sur **Annuler** pour laisser la propriété inchangée.
  - Pour chaque propriété d'utilisateur que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
    * **Propriétés utilisateur :** dans la liste, cliquez sur une propriété, puis entrez l'attribut de la propriété utilisateur dans le champ en regard de la propriété.
    * Cliquez sur **Terminé** pour enregistrer la propriété utilisateur ou cliquez sur **Annuler**.
  - Pour chaque propriété utilisateur que vous souhaitez supprimer, placez le curseur sur la ligne contenant la propriété, puis cliquez sur le **X** sur le côté droit. La propriété est immédiatement supprimée.

3. Cliquez sur **Enregistrer** pour enregistrer vos modifications ou sur **Annuler** pour laisser l'utilisateur inchangé.

Pour déverrouiller un compte d'utilisateur local

Un compte utilisateur local est verrouillé en fonction des propriétés du serveur suivantes :

- `local.user.account.lockout.time`
- `local.user.account.lockout.limit`

  Pour de plus amples informations, consultez la section Définitions des propriétés du serveur.

Lorsqu'un compte utilisateur local est verrouillé, vous pouvez le déverrouiller à partir de la console Citrix Endpoint Management.

1. Sur la page **Utilisateurs**, dans la liste des comptes utilisateur, cliquez pour sélectionner un compte utilisateur.
2. Cliquez sur **Déverrouiller utilisateur**. Une boîte de dialogue de confirmation s'affiche.
3. Cliquez sur **Déverrouiller** pour déverrouiller le compte utilisateur ou cliquez sur **Annuler** pour laisser l'utilisateur inchangé.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Vous ne pouvez pas déverrouiller un utilisateur Active Directory à partir de la console Citrix Endpoint Management. Un utilisateur Active Directory verrouillé doit contacter son service d'assistance Active Directory pour réinitialiser son mot de passe.

Pour supprimer un compte d'utilisateur local

1. Sur la page **Utilisateurs**, dans la liste des comptes utilisateur, cliquez pour sélectionner un compte utilisateur.

   Vous pouvez sélectionner plusieurs comptes utilisateur à supprimer en sélectionnant la case à cocher en regard de chaque compte utilisateur.

2. Cliquez sur **Delete**. Une boîte de dialogue de confirmation s'affiche.
3. Cliquez sur **Supprimer** pour supprimer le compte utilisateur ou cliquez sur **Annuler**.

Pour supprimer des utilisateurs Active Directory

Pour supprimer un ou plusieurs utilisateurs Active Directory à la fois, sélectionnez les utilisateurs et cliquez sur **Supprimer**.

Si un utilisateur que vous supprimez dispose d'appareils inscrits et que vous souhaitez ré-inscrire ces appareils, supprimez les appareils avant la réinscription. Pour supprimer un appareil, accédez à **Gérer > Appareils**, sélectionnez l'appareil et cliquez sur **Supprimer**.

Importer des comptes utilisateur

Vous pouvez importer des comptes utilisateur locaux et des propriétés à partir d'un fichier .csv appelé fichier de provisioning, que vous pouvez créer manuellement. Pour de plus amples informations sur la mise en forme des fichiers de provisioning, consultez Formats des fichiers de provisioning.

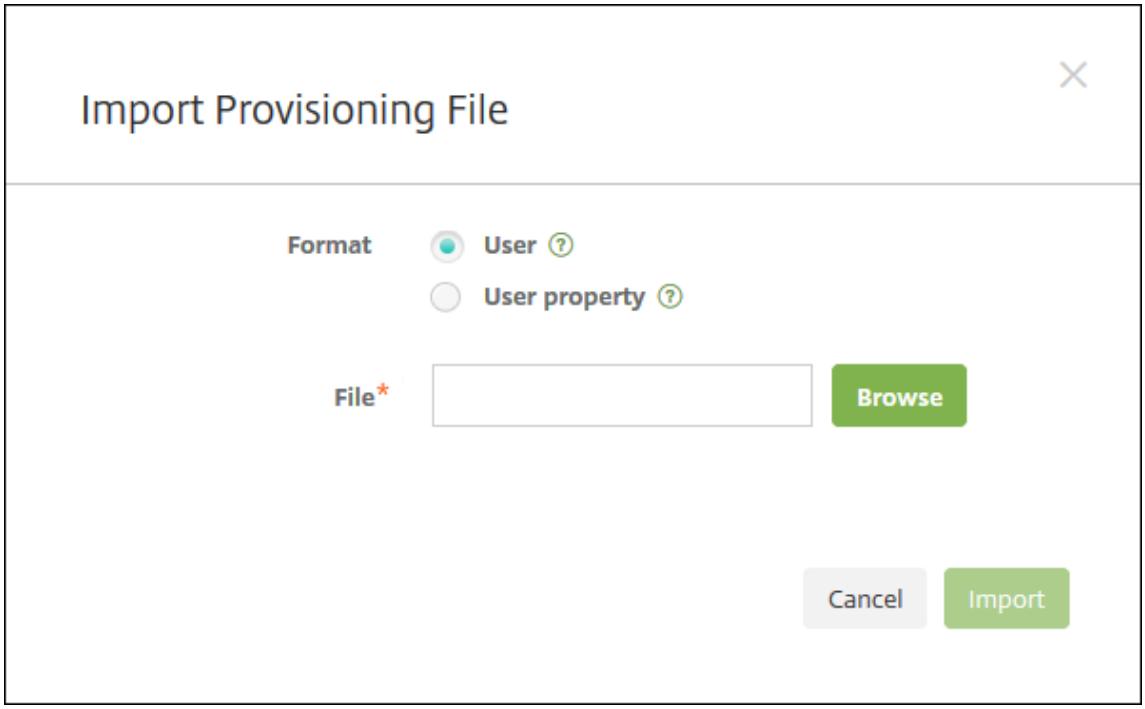
> **Remarque :**
>
> - Pour les utilisateurs locaux, utilisez le nom de domaine ainsi que le nom d'utilisateur du fichier d'importation. Par exemple, spécifiez `username@domain`. Si l'utilisateur local que vous créez ou importez est destiné à un domaine géré dans Citrix Endpoint Management, l'utilisateur ne peut pas s'inscrire en utilisant les informations d'identification LDAP correspondantes.
> - Si vous importez des comptes utilisateur sur l'annuaire utilisateur interne Citrix Endpoint Management, désactivez le domaine par défaut pour accélérer le processus d'importation. N'oubliez pas que la désactivation du domaine affecte les inscriptions. Réactivez le domaine par défaut après l'importation des utilisateurs internes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> • Les utilisateurs locaux peuvent être au format UPN (nom d'utilisateur principal). Toutefois, Citrix vous recommande de ne pas utiliser le domaine géré. Par exemple, si exemple.com est géré, ne créez pas d'utilisateur local au format UPN : utilisateur@exemple.com.

Lorsque vous préparez un fichier de provisioning, suivez ces étapes pour importer le fichier sur Citrix Endpoint Management.

1. Dans la console Citrix Endpoint Management, cliquez sur **Gérer > Utilisateurs**. La page **Utilisateurs** s'affiche.
2. Cliquez sur **Importer des utilisateurs locaux**. La boîte de dialogue **Importer le fichier de provisioning** apparaît.



3. Sélectionnez **Utilisateur** ou **Propriété** pour le format du fichier de provisioning que vous importez.
4. Sélectionnez le fichier de provisioning à utiliser en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
5. Cliquez sur **Importer**.

Formats des fichiers de provisioning

Vous pouvez créer un fichier de provisioning et l'utiliser pour importer des comptes utilisateur et des propriétés dans Citrix Endpoint Management. Utilisez l'un des formats suivants pour le fichier de provisioning :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Champs des fichiers de provisioning utilisateur :** `user;password;role;group1;group2`
- **Champs des fichiers de provisioning des attributs utilisateur :** `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

> **Remarque :**
>
> - Séparez les champs dans le fichier de provisioning par un point-virgule (;). Si une partie d'un champ contient un point-virgule, elle doit être précédée d'une barre oblique inverse (\). Par exemple, saisissez la propriété **propertyV ;test;1;2** en tant que **propertyV;test;1;2** dans le fichier de provisioning.
> - Les valeurs valides pour **Rôle** sont les rôles prédéfinis USER, ADMIN, SUPPORT et DEVICE_PROVISIONING, ainsi que tout autre rôle que vous avez défini.
> - Utilisez le point (.) comme séparateur pour créer une hiérarchie de groupe. N'utilisez pas de point dans les noms de groupe.
> - Utilisez des minuscules pour les attributs de propriété dans les fichiers de provisioning d'attribut. La base de données est sensible à la casse.

Exemple de contenu de provisioning utilisateur L'entrée `user01;pwd\\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` signifie :

- **Utilisateur :** user01
- **Mot de passe :** pwd;01
- **Rôle :** USER
- **Groupes :**
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

Dans cet autre exemple, `AUser0;1.password;USER;ActiveDirectory.test.net` signifie :

- **Utilisateur :** AUser0
- **Mot de passe :** 1.password
- **Rôle :** USER
- **Groupe :** ActiveDirectory.test.net

Exemple de contenu de provisioning d'attribut utilisateur L'entrée `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` signifie :

- **Utilisateur :** user01

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

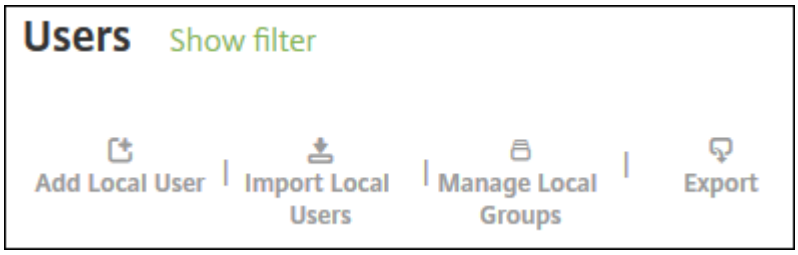
- **Propriété 1**
  - **nom :** propertyN
  - **valeur :** propertyV;test;1;2
- **Propriété 2 :**
  - **nom :** prop 2
  - **valeur :** prop2 valeur

Ajouter ou supprimer des groupes

Vous gérez les groupes dans la boîte de dialogue **Gérer les groupes** dans la console Citrix Endpoint Management sur ces pages : **Utilisateurs**, **Ajouter un utilisateur local** ou **Modifier un utilisateur local**. Aucune commande ne permet de modifier un groupe.

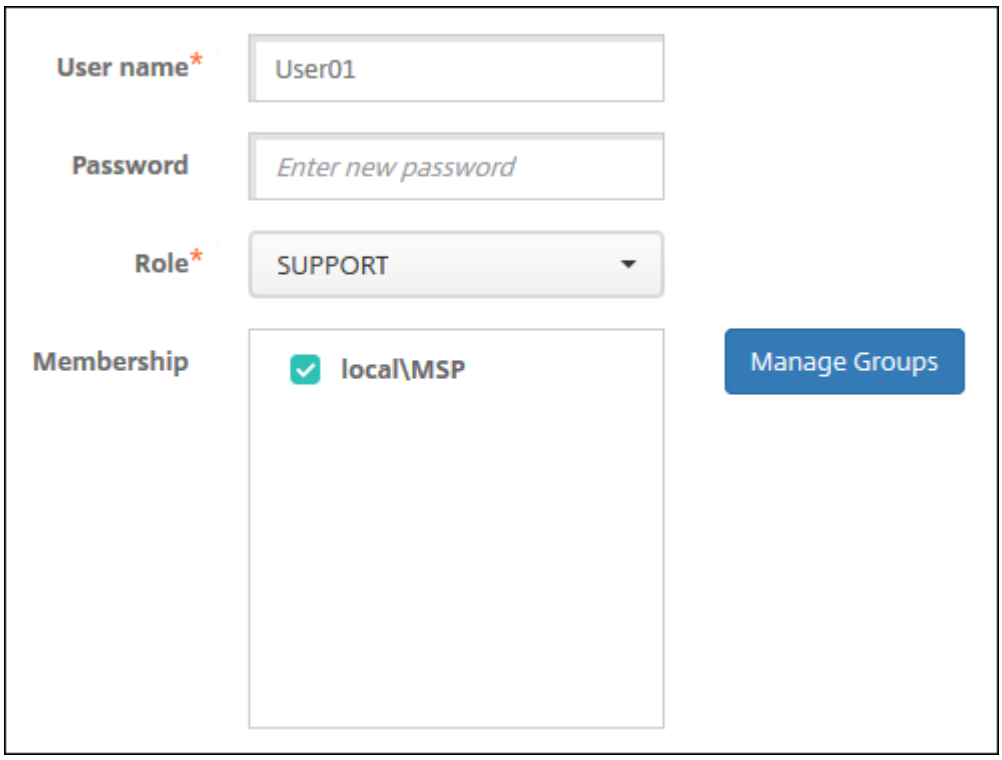
Pour ajouter un groupe local

1. Procédez comme suit :
   - Sur la page **Utilisateurs**, cliquez sur **Gérer les groupes locaux**.



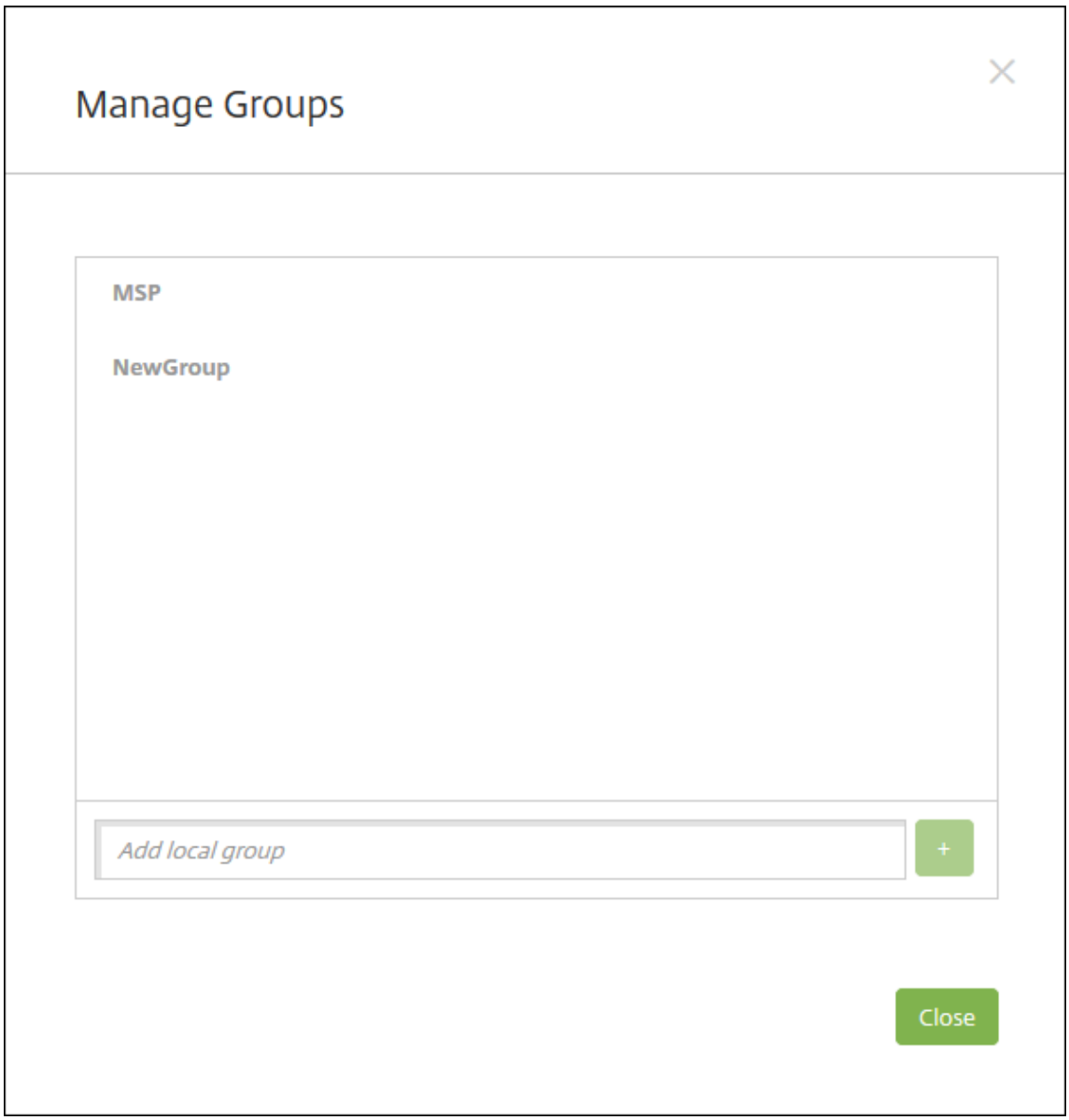
   - Sur la page **Ajouter un utilisateur local** ou la page **Modifier un utilisateur local**, cliquez sur **Gérer les groupes**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



La boîte de dialogue **Gérer les groupes** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Sous les listes de groupes, entrez un nouveau nom de groupe, puis cliquez sur le signe plus (**+**). Le groupe d'utilisateurs est ajouté à la liste.
3. Cliquez sur **Fermer**.

Pour supprimer un groupe

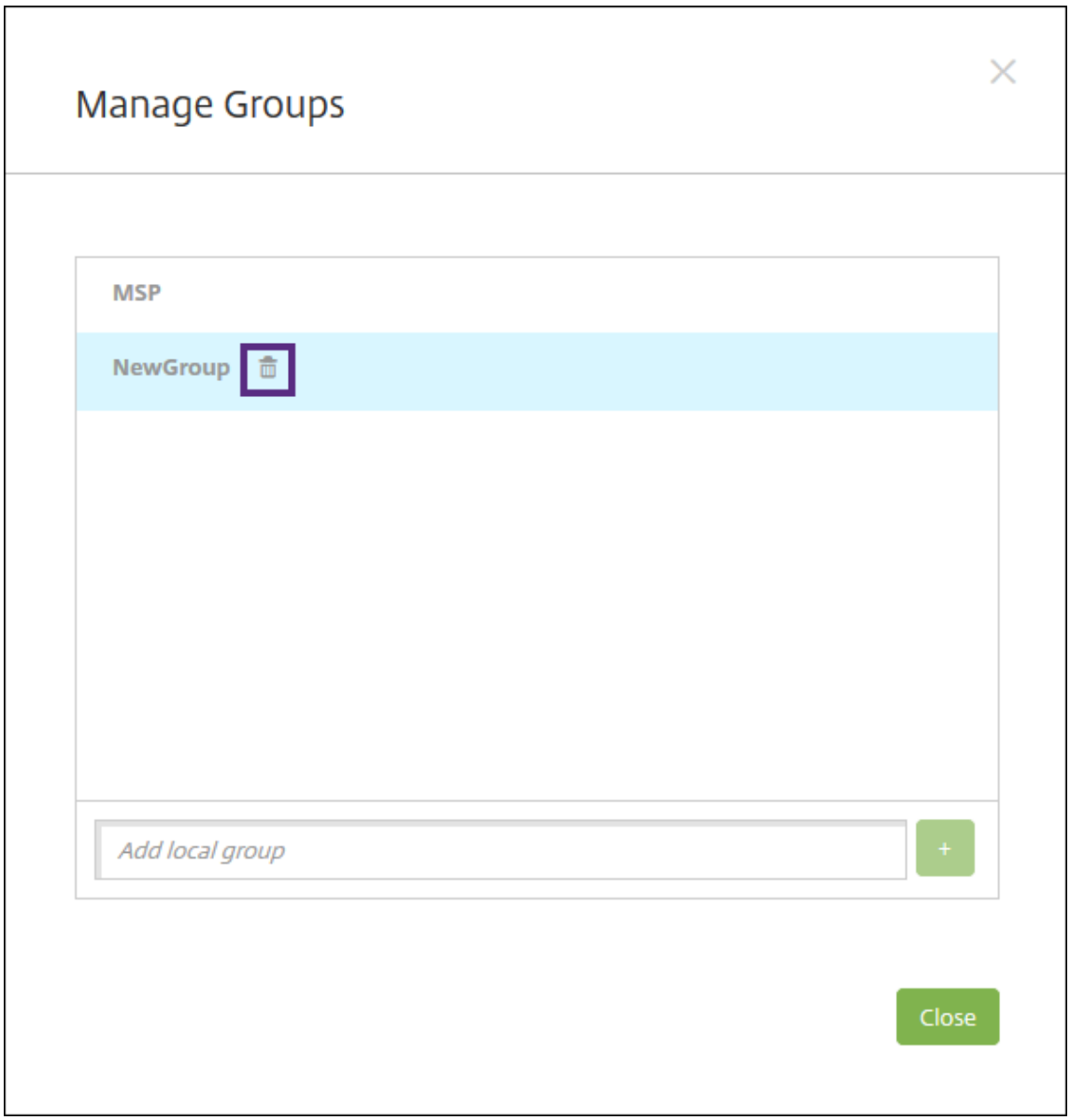
La suppression d'un groupe n'a aucun effet sur les comptes d'utilisateur. Elle supprime uniquement l'association d'utilisateurs avec ce groupe. Les utilisateurs perdent également l'accès aux applications ou profils fournis par les groupes de mise à disposition qui sont associés à ce groupe. Mais toutes les autres associations de groupes restent intactes. Si les utilisateurs ne sont associés à aucun autre groupe local, ils sont associés au niveau supérieur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Procédez comme suit :

   - Sur la page **Utilisateurs**, cliquez sur **Gérer les groupes locaux**.
   - Sur la page **Ajouter un utilisateur local** ou la page **Modifier un utilisateur local**, cliquez sur **Gérer les groupes**.

   La boîte de dialogue **Gérer les groupes** s'affiche.



2. Dans la boîte de dialogue **Gérer les groupes**, sélectionnez le groupe que vous souhaitez supprimer.
3. Cliquez sur l'icône de la corbeille à droite du nom de groupe. Une boîte de dialogue de confirmation s'affiche.
4. Cliquez sur **Supprimer** pour confirmer l'opération et supprimer le groupe.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Important :**
>
> vous ne pouvez pas annuler cette opération.

5. Dans la boîte de dialogue **Gérer les groupes**, cliquez sur **Fermer**.

Créer et gérer des workflows

Vous pouvez appliquer des workflows pour gérer la création et la suppression des comptes utilisateur. Pour pouvoir créer un workflow, vous devez identifier les personnes de votre organisation chargées d'approuver les demandes d'ouverture de comptes utilisateur. Vous pouvez ensuite utiliser le modèle de workflow pour créer et approuver les demandes.

Lorsque vous configurez Citrix Endpoint Management pour la première fois, vous configurez les paramètres d'e-mail de workflow qui doivent être définis avant que vous puissiez utiliser des workflows. Vous pouvez modifier les paramètres de messagerie de workflow à tout moment. Ces paramètres incluent le serveur de messagerie, le port, l'adresse e-mail et si la demande de création du compte utilisateur requiert une approbation.

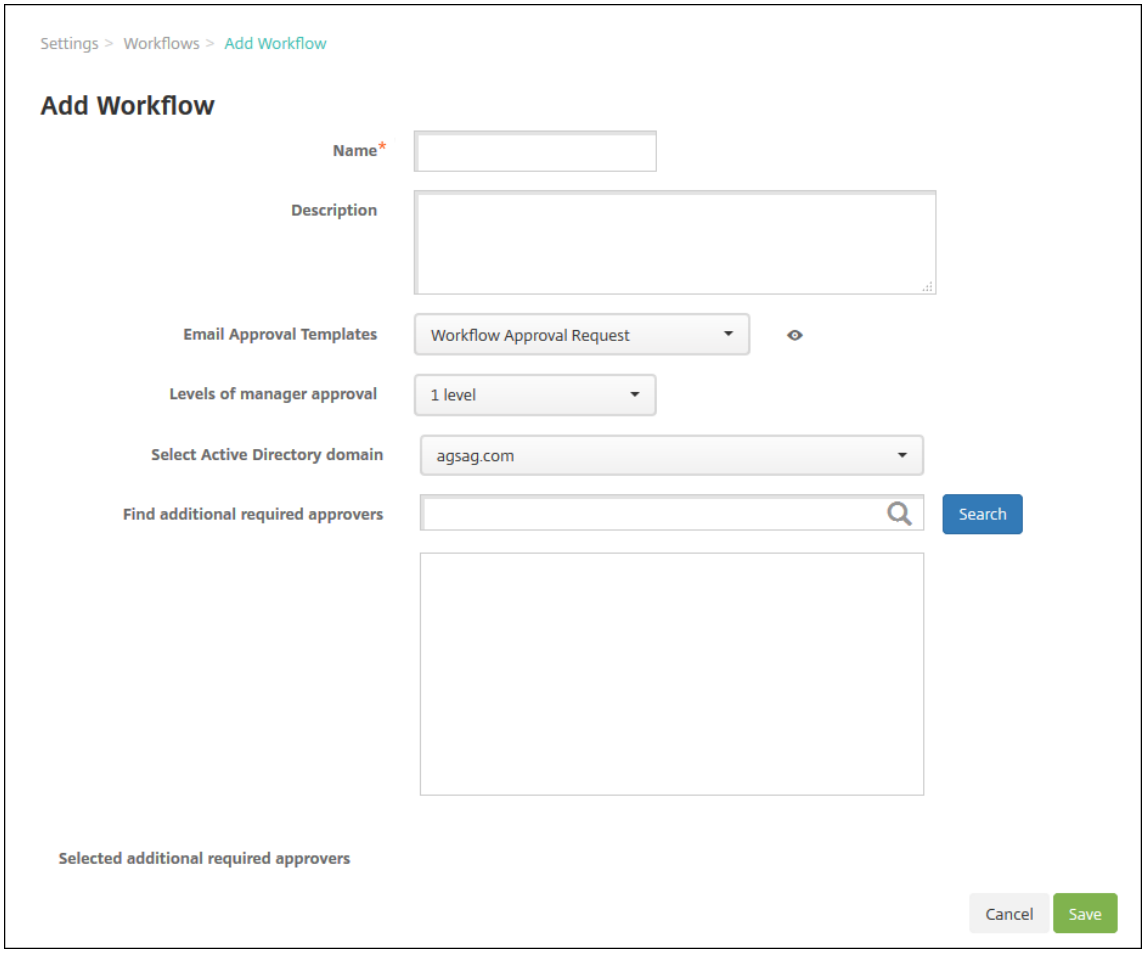
Vous pouvez configurer des workflows à deux emplacements dans Citrix Endpoint Management :

- Sur la page **Paramètres > Workflows** de la console Citrix Endpoint Management. Sur la page **Workflows**, vous pouvez configurer plusieurs workflows à utiliser pour la configuration d'applications. Lorsque vous configurez des workflows sur la page Workflows, vous pouvez sélectionner le workflow lors de la configuration de l'application.
- Lorsque vous configurez un connecteur d'applications dans l'application, vous devez fournir un nom de workflow, puis configurer les personnes qui peuvent approuver la demande d'ouverture de compte utilisateur. Voir Ajouter des applications.

Vous pouvez désigner jusqu'à trois niveaux pour l'approbation du responsable des comptes d'utilisateur. Si vous voulez faire approuver le compte utilisateur par d'autres personnes, vous pouvez les rechercher et les sélectionner en utilisant leur nom ou adresse e-mail. Lorsque Citrix Endpoint Management trouve la personne concernée, vous pouvez l'ajouter au workflow. Toutes les personnes figurant dans le workflow reçoivent un e-mail afin d'approuver ou de refuser l'ouverture du nouveau compte d'utilisateur.

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Workflows**. La page **Workflows** s'affiche.
3. Cliquez sur **Ajouter**. La page **Ajouter un workflow** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Pour configurer ces paramètres :

   - **Nom :** entrez un nom unique pour le workflow.
   - **Description :** entrez une description pour le workflow (facultatif).
   - **Modèles d'approbation d'e-mail :** dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Vous créez des modèles d'e-mail dans la section **Modèles de notification** sous **Paramètres** dans la console Citrix Endpoint Management. Lorsque vous cliquez sur l'icône d'œil à droite de ce champ, vous voyez un aperçu du modèle que vous êtes en train de configurer.
   - **Niveaux d'approbation par un responsable :** dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est **1 niveau**. Les options possibles sont les suivantes :
     - Pas nécessaire
     - 1 niveau
     - 2 niveaux
     - 3 niveaux
   - **Sélectionner un domaine Active Directory :** dans la liste, sélectionnez le domaine Active

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directory à utiliser pour le workflow.

- **Rechercher des approbateurs supplémentaires requis :** tapez un nom dans le champ de recherche et cliquez sur **Rechercher**. Les noms proviennent d'Active Directory.
- Lorsque le nom s'affiche dans le champ, sélectionnez la case à cocher en regard du nom. Le nom et l'adresse e-mail s'affichent dans la liste **Approbateurs supplémentaires requis sélectionnés**.
  - Pour supprimer un nom de la liste, effectuez l'une des opérations suivantes :
    * Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.
    * Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats de la recherche.
    * Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

5. Cliquez sur **Enregistrer**. Le workflow créé s'affiche sur la page **Workflows**.

Après avoir créé le workflow, vous pouvez afficher les détails du workflow, voir les applications associées au workflow ou supprimer le workflow. Vous ne pouvez pas modifier un workflow après sa création. Si vous avez besoin d'un workflow avec différents niveaux d'approbation ou approbateurs, créez un autre workflow.

Pour afficher les détails d'un workflow et le supprimer

1. Sur la page **Workflows**, dans la liste des workflows, sélectionnez un workflow. Pour ce faire, cliquez sur la ligne dans le tableau ou sélectionnez la case à cocher en regard du workflow.
2. Pour supprimer un workflow, cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer**.

> **Important :**
>
> vous ne pouvez pas annuler cette opération.

Profils d'inscription

March 1, 2024

Un profil d'inscription permet de spécifier les éléments suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Options d'inscription associées à la gestion d'appareils pour les appareils Android, iOS et Windows
- Options d'inscription associées à la gestion d'applications pour les appareils Android et iOS
- Autres options d'inscription :
  - Indique s'il faut limiter le nombre d'appareils qu'un utilisateur peut inscrire.

    Si le nombre maximal d'appareils est atteint, un message d'erreur informe l'utilisateur qu'il a dépassé la limite d'enregistrement d'appareils.
  - Indique s'il faut autoriser un utilisateur à refuser la gestion d'appareils.

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

- Gestion des appareils mobiles (MDM exclusif)
- MDM+Gestion des applications mobiles (MAM)
- MAM exclusif
- Inscriptions d'appareils appartenant à l'entreprise
- Inscriptions BYOD (possibilité de se désinscrire de MDM)
- Migration des inscriptions Administrateur d'appareil Android vers les inscriptions Android Enterprise (appareil entièrement géré, profil de travail, dédié)
- Inscription automatique des appareils Windows 10 et Windows 11 via l'application Citrix Workspace pour Windows (version préliminaire)

Si votre site actuel est MDM exclusif et que vous souhaitez ajouter MAM, vous devez configurer un NetScaler Gateway. Pour plus d'informations, consultez Configuration requise pour NetScaler Gateway.

Lorsque vous créez un groupe de mise à disposition, vous pouvez utiliser le profil d'inscription par défaut nommé Global ou spécifier un profil d'inscription différent.

Les caractéristiques du profil d'inscription par plateforme sont les suivantes.

- **Pour les appareils Android :** vous spécifiez le mode gestion et propriétaire de l'appareil. Par exemple : appareil appartenant à l'entreprise, entièrement géré avec profil de travail et profil de travail BYOD.

  Les nouveaux appareils s'inscrivent dans Android Enterprise par défaut. Vous pouvez choisir de gérer les appareils à l'aide du mode Administrateur des anciens appareils Android (DA). Les nouveaux appareils s'inscrivent également dans la gestion des applications par défaut.

  Pour plus d'informations sur la spécification du niveau de sécurité et les étapes d'inscription requises, voir Comptes d'utilisateurs, rôles et inscription.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Pour les appareils iOS :** vous spécifiez le type de gestion des appareils : **Inscription d'utilisateurs Apple**,**Inscription d'appareils Apple** ou **Ne pas gérer les appareils**. Ce mode **Inscription d'utilisateurs Apple** est disponible en version préliminaire publique. Pour activer cette fonctionnalité, contactez votre équipe de support technique.

  Si vous sélectionnez Inscription d'utilisateurs Apple, vous pouvez choisir d'utiliser un domaine personnalisé pour les identifiants Apple ID gérés et configurer ce domaine.

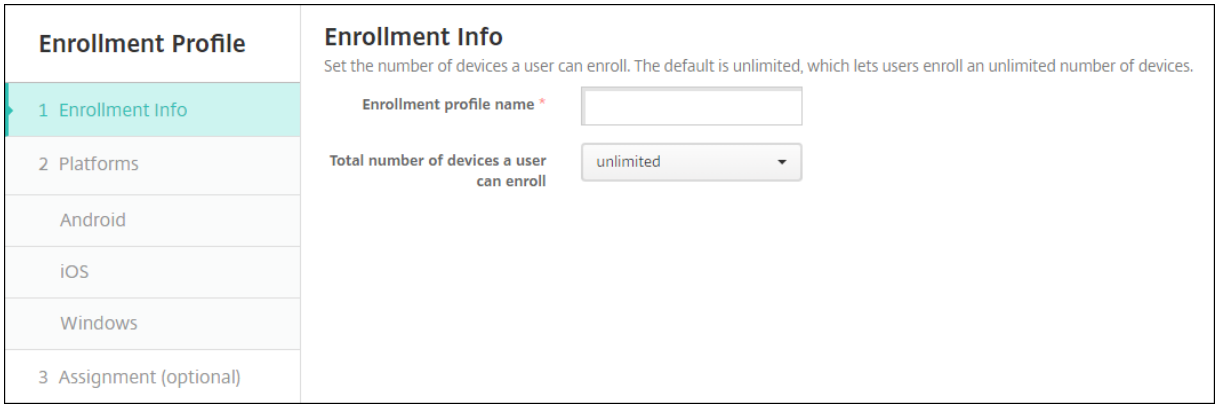
  Par défaut, les nouveaux appareils s'inscrivent dans la gestion des appareils Apple. Les nouveaux appareils s'inscrivent également dans la gestion des applications par défaut.

- **Pour les appareils Windows 10 et Windows 11 :** vous spécifiez si vous souhaitez utiliser la gestion des appareils Citrix pour Windows. Les nouveaux appareils s'inscrivent dans la gestion des appareils par défaut.

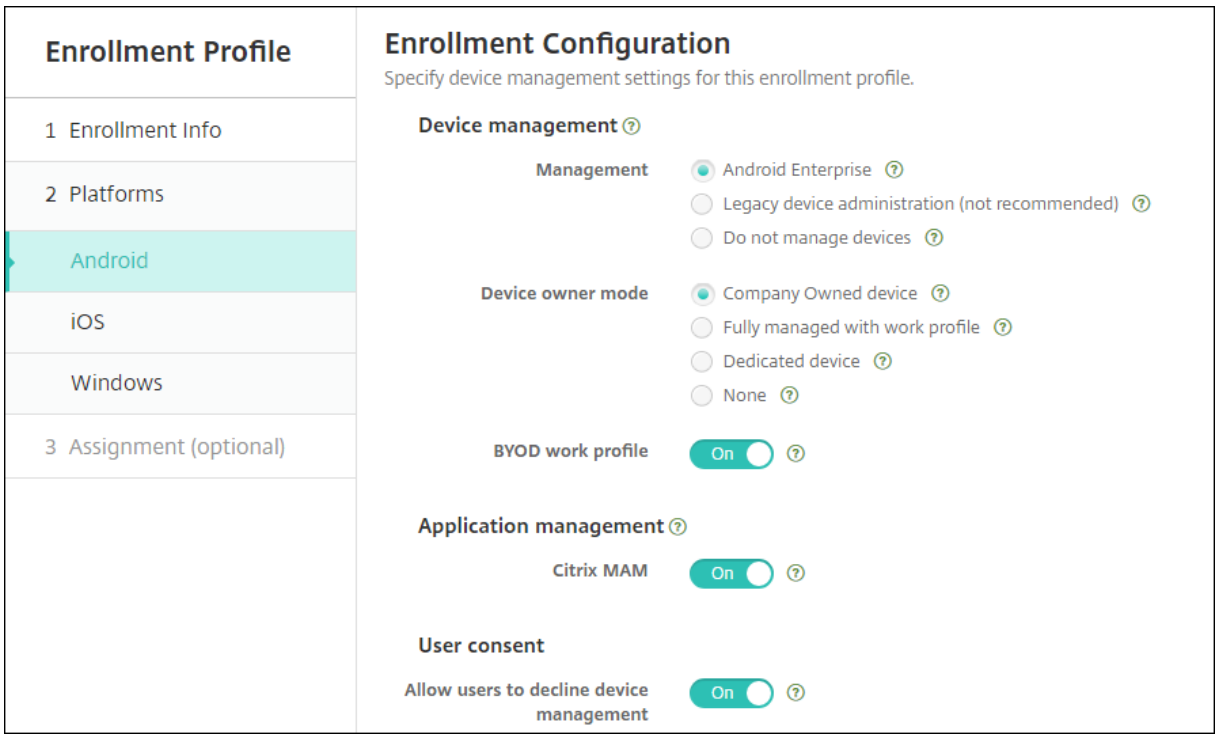
Profil d'inscription Global

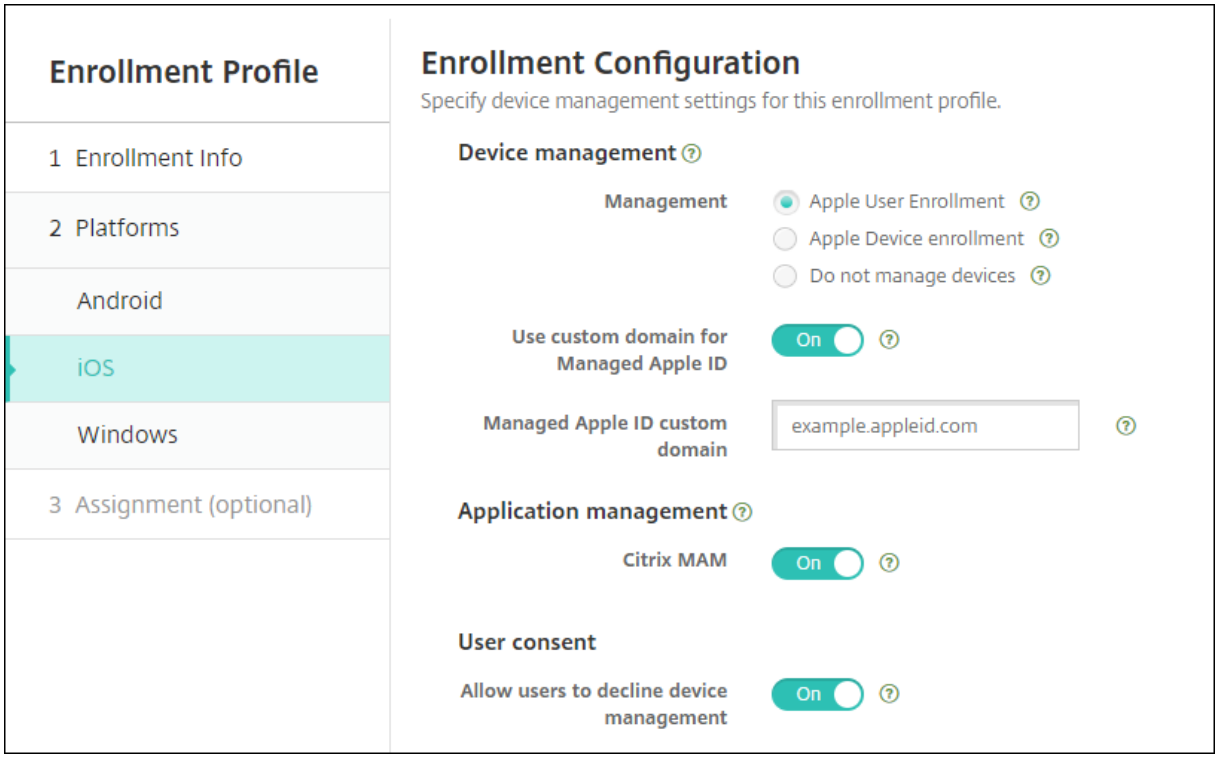
Le profil d'inscription par défaut est appelé Global. Le profil Global est utile pour effectuer des tests jusqu'à ce que vous ayez la possibilité de créer des profils d'inscription.

Si votre intégration s'effectue avec Citrix Endpoint Management 20.2.1 ou version ultérieure, le profil d'inscription Global a des paramètres prédéfinis. Les captures d'écran suivantes affichent les paramètres par défaut du profil d'inscription Global. Seuls les déploiements MAM affichent un sous-ensemble de ces options.

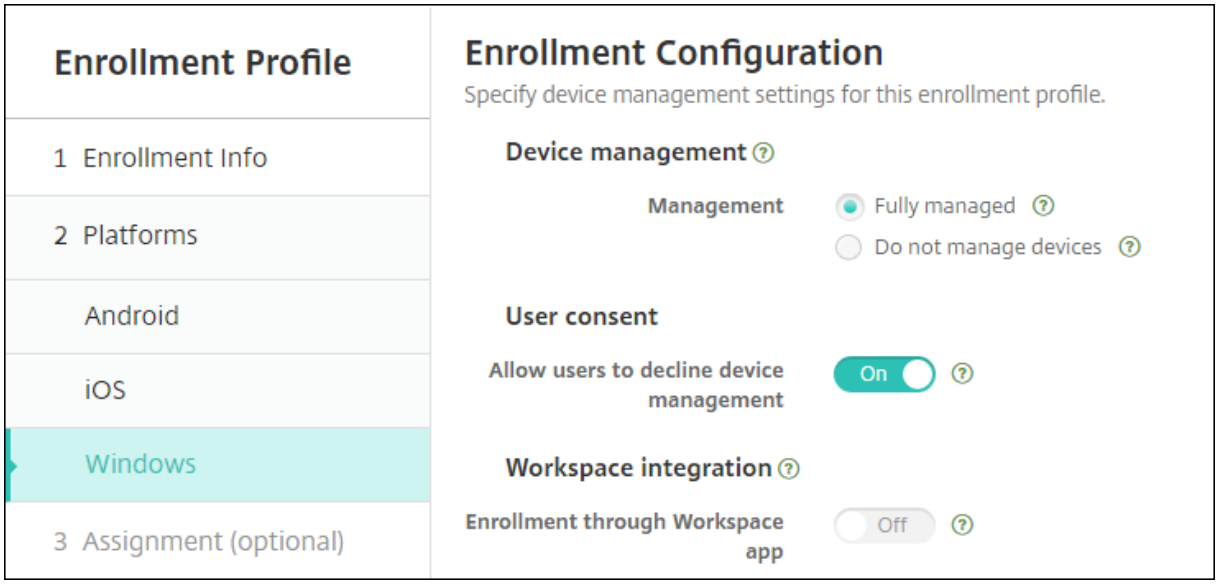


© 1999–2024 Cloud Software Group, Inc. All rights reserved.





© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Profils d'inscription, groupes de mise à disposition et inscription

Les profils d'inscription et les groupes de mise à disposition interagissent comme suit :

- Vous pouvez joindre un profil d'inscription à un ou plusieurs groupes de mise à disposition.
- Si un utilisateur appartient à plusieurs groupes de mise à disposition qui ont des profils d'inscription différents, le nom du groupe de mise à disposition détermine le profil d'inscription utilisé. Citrix Endpoint Management sélectionne le groupe de mise à disposition qui apparaît en dernier dans une liste alphabétique des groupes de mise à disposition. Par exemple, supposons que vous disposez des éléments suivants :

  - Deux profils d'inscription, nommés « EP1 » et « EP2 ».
  - Deux groupes de mise à disposition, nommés « DG1 » et « DG2 ».
  - « DG1 » est associé à « EP1 ».
  - « DG2 » est associé à « EP2 ».

  Si l'utilisateur inscrit fait partie des groupes de mise à disposition « DG1 » et « DG2 », Citrix Endpoint Management utilise le profil d'inscription « EP2 » pour déterminer le type d'inscription pour l'utilisateur.
- L'ordre de déploiement s'applique uniquement aux appareils d'un groupe de mise à disposition dont le profil d'inscription est configuré pour la gestion des appareils (MDM).
- Après l'inscription d'un appareil, certaines modifications apportées à un profil d'inscription nécessitent une réinscription :

  - Modifier la configuration pour rétrograder un appareil de l'inscription MDM+MAM à MAM

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ou MDM. Une rétrogradation peut se produire lorsque vous mettez à jour un profil d'inscription ou déplacez un appareil vers un autre groupe de mise à disposition.
  - Ajout de MAM à un profil d'inscription configuré pour MDM.
  - Ajout de MDM à un profil d'inscription configuré pour MAM.

- Le passage à un profil d'inscription différent n'affecte pas les appareils inscrits existants. Toutefois, les utilisateurs doivent désinscrire, puis réinscrire ces appareils pour que les modifications prennent effet.

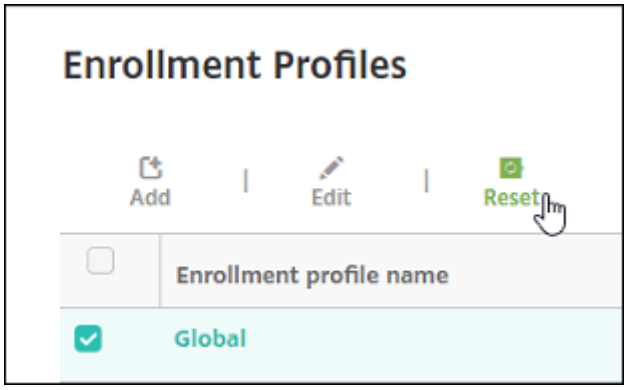
Pour créer un profil d'inscription

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Profils d'inscription**.
2. Dans la page **Infos d'inscription**, tapez un nom descriptif pour le profil. Par défaut, un utilisateur peut inscrire un nombre illimité d'appareils. Sélectionnez une valeur pour limiter le nombre d'appareils par utilisateur. La limite s'applique à la somme des appareils Android, iOS et Windows gérés par MAM ou MDM qu'un utilisateur inscrit.
3. Renseignez les pages de plates-formes. Pour plus d'informations sur les paramètres d'inscription spécifiques aux plates-formes, voir :
   - Android Enterprise : Création de profils d'inscription
   - iOS : Méthodes d'inscription prises en charge
   - Windows Desktop et Tablet : Méthodes d'inscription prises en charge
4. Sur la page **Attributions**, attachez un ou plusieurs groupes de mise à disposition au profil d'inscription.

   Un utilisateur peut appartenir à plusieurs groupes de mise à disposition ayant des profils d'inscription différents. Dans ce cas, le nom du groupe de mise à disposition détermine le profil d'inscription utilisé. Citrix Endpoint Management sélectionne le groupe de mise à disposition qui apparaît en dernier dans une liste alphabétique des groupes de mise à disposition. Pour créer des groupes de mise à disposition, accédez à **Configurer > Groupes de mise à disposition**.

La liste de vos profils d'inscription apparaît sur la page **Configurer > Profils d'inscription**. Pour modifier le profil Global ou le réinitialiser sur les valeurs par défaut d'origine, sélectionnez la ligne correspondant au profil Global et cliquez sur **Réinitialiser**. Vous ne pouvez pas supprimer le profil Global.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Notifications

November 29, 2023

Vous pouvez utiliser les notifications dans Citrix Endpoint Management aux fins suivantes :

- Pour communiquer avec des groupes d'utilisateurs sélectionnés à propos de plusieurs fonctions liées au système. Vous pouvez également cibler ces notifications pour certains utilisateurs. Par exemple, tous les utilisateurs équipés d'appareils iOS, les utilisateurs dont les appareils ne sont pas conformes, les utilisateurs équipés d'appareils leur appartenant, etc.
- Pour inscrire les utilisateurs et leurs appareils
- Pour notifier automatiquement les utilisateurs (via des actions automatisées) lorsque certaines conditions sont remplies. Par exemple :
  - Lorsqu'un appareil utilisateur est sur le point d'être bloqué du domaine d'entreprise en raison d'un problème de conformité
  - Lorsqu'un appareil a été jailbreaké ou rooté

Pour de plus amples informations sur les actions automatisées, consultez la section Actions automatisées.

Pour envoyer des notifications avec Citrix Endpoint Management, vous devez configurer une passerelle et un serveur de notification. Vous pouvez configurer un serveur de notifications dans Citrix Endpoint Management pour configurer les serveurs SMTP. Ces serveurs envoient des notifications par courriel aux utilisateurs. Vous pouvez utiliser les notifications pour envoyer des messages via SMTP.

- SMTP est un protocole texte orienté connexion avec lequel un expéditeur de messagerie communique avec un récepteur de messagerie. L'expéditeur de messagerie émet des chaînes de commande et fournit les données nécessaires, généralement via une connexion TCP. Les ses-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

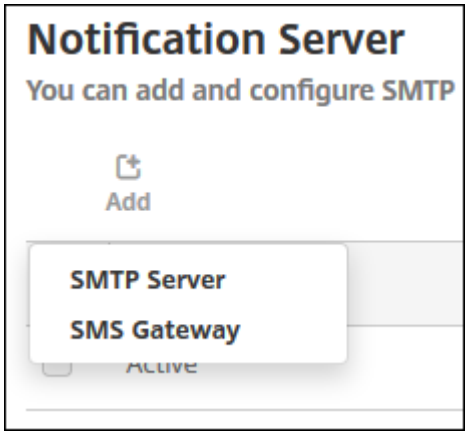
sions SMTP se composent de commandes émanant d'un client SMTP (la personne qui envoie le message) et des réponses correspondantes à partir du serveur SMTP.

Conditions préalables

- Configurez le serveur de notifications SMTP pour envoyer des messages aux utilisateurs. Si le serveur est hébergé sur un serveur interne, contactez votre administrateur système pour obtenir les informations de configuration. Si le serveur est un service de messagerie hébergé, recherchez les informations de configuration appropriées sur le site Web du fournisseur de services.
- Vous ne pouvez utiliser qu'un seul serveur SMTP actif. Ce canal de communication n'autorise qu'une seule configuration active.
- Ouvrez le port 25 depuis Citrix Endpoint Management dans la zone démilitarisée (DMZ) de votre réseau afin de pointer vers le serveur SMTP sur votre réseau interne. Cela permet à Citrix Endpoint Management d'envoyer des notifications.

Configuration d'un serveur SMTP

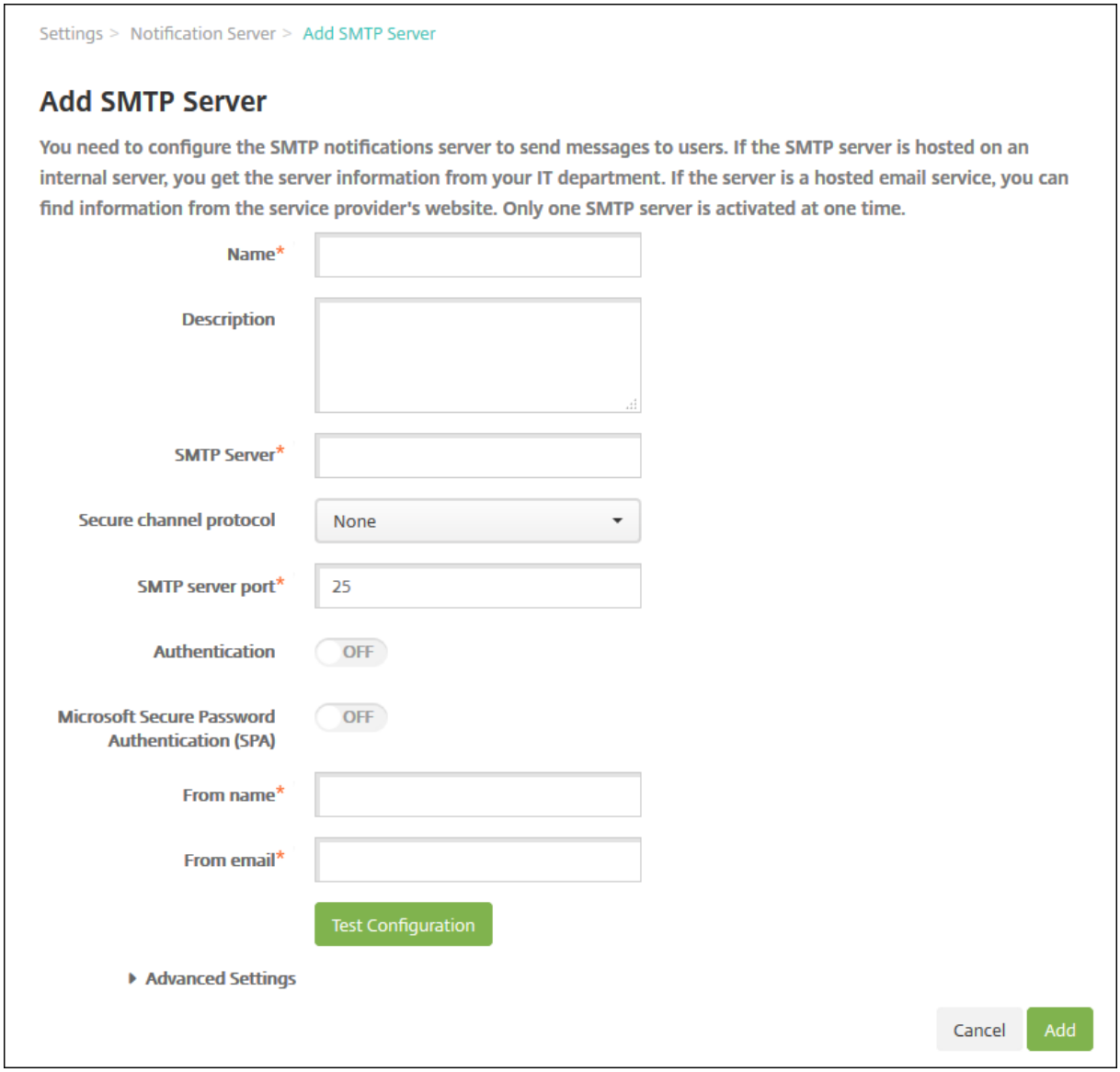
1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Notifications**, cliquez sur **Serveur de notification**. La page **Serveur de notification** s'affiche.
3. Cliquez sur **Ajouter**. Un menu s'affiche avec des options permettant de configurer un serveur SMTP.



   - Pour ajouter un serveur SMTP, cliquez sur **Serveur SMTP**, puis consultez la section Ajouter un serveur SMTP pour connaître les étapes suivantes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ajouter un serveur SMTP



1. Pour configurer ces paramètres :

   - **Nom :** entrez le nom associé à ce compte de serveur SMTP.
   - **Description :** entrez une description pour le serveur (facultatif).
   - **Serveur SMTP :** entrez le nom d'hôte du serveur. Spécifiez un nom de domaine complet (FQDN) ou une adresse IP.
   - **Secure Channel Protocol :** dans la liste, cliquez sur le protocole de canal sécurisé approprié utilisé par le serveur (si le serveur est configuré pour utiliser une authentification sécurisée) : **SSL**, **TLS** ou **Aucun**. La valeur par défaut est **Aucun**.
   - **Port du serveur SMTP :** entrez le port utilisé par le serveur SMTP. Le port est défini par défaut sur 25. Si les connexions SMTP utilisent le protocole de canal sécurisé SSL, définissez

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

le port sur 465.
- **Authentification :** sélectionnez **Activé** ou **Désactivé**. La valeur par défaut est **Off**.
- Si vous avez activé **Authentification**, configurez les paramètres suivants :
  - **Nom d'utilisateur :** entrez un nom d'utilisateur à utiliser pour l'authentification.
  - **Mot de passe :** entrez le mot de passe de l'utilisateur à utiliser pour l'authentification.
- **Authentification par mot de passe sécurisé (SPA) Microsoft :** si le serveur SMTP utilise la SPA, cliquez sur **Activé**. La valeur par défaut est **Off**.
- **Nom expéditeur :** entrez le nom affiché dans la case **De** lorsqu'un client reçoit une notification par e-mail à partir de ce serveur. Par exemple, Département Informatique.
- **E-mail expéditeur :** entrez l'adresse e-mail utilisée si le destinataire d'un e-mail répond à la notification envoyée par le serveur SMTP.

2. Cliquez sur **Tester la configuration** pour envoyer une notification par e-mail test.
3. Développez **Paramètres avancés** et configurez les paramètres suivants :
   - **Nombre d'essais SMTP :** entrez le nombre de tentatives d'envoi d'un message dont l'envoi a échoué à partir du serveur SMTP. La valeur par défaut est 5.
   - **Délai d'attente SMTP :** entrez la durée d'attente (en secondes) lors de l'envoi d'une demande SMTP. Augmentez cette valeur si l'envoi de messages échoue continuellement en raison de l'expiration des délais. Soyez prudent lorsque vous diminuez cette valeur ; évitez d'augmenter les échecs dus à l'expiration des délais ainsi que le nombre de messages non remis. La durée par défaut est de 30 secondes.
   - **Nombre max de destinataires SMTP :** entrez le nombre maximal de destinataires par message envoyés par le serveur SMTP. La valeur par défaut est 100.
4. Cliquez sur **Ajouter**.

Créer et mettre à jour des modèles de notification

Vous pouvez créer ou mettre à jour des modèles de notification dans Citrix Endpoint Management à utiliser dans les actions automatisées, l'inscription, et les messages de notifications standard envoyés aux utilisateurs. Vous configurez les modèles de notification pour l'envoi de messages sur deux canaux différents : Citrix Secure Hub ou SMTP.

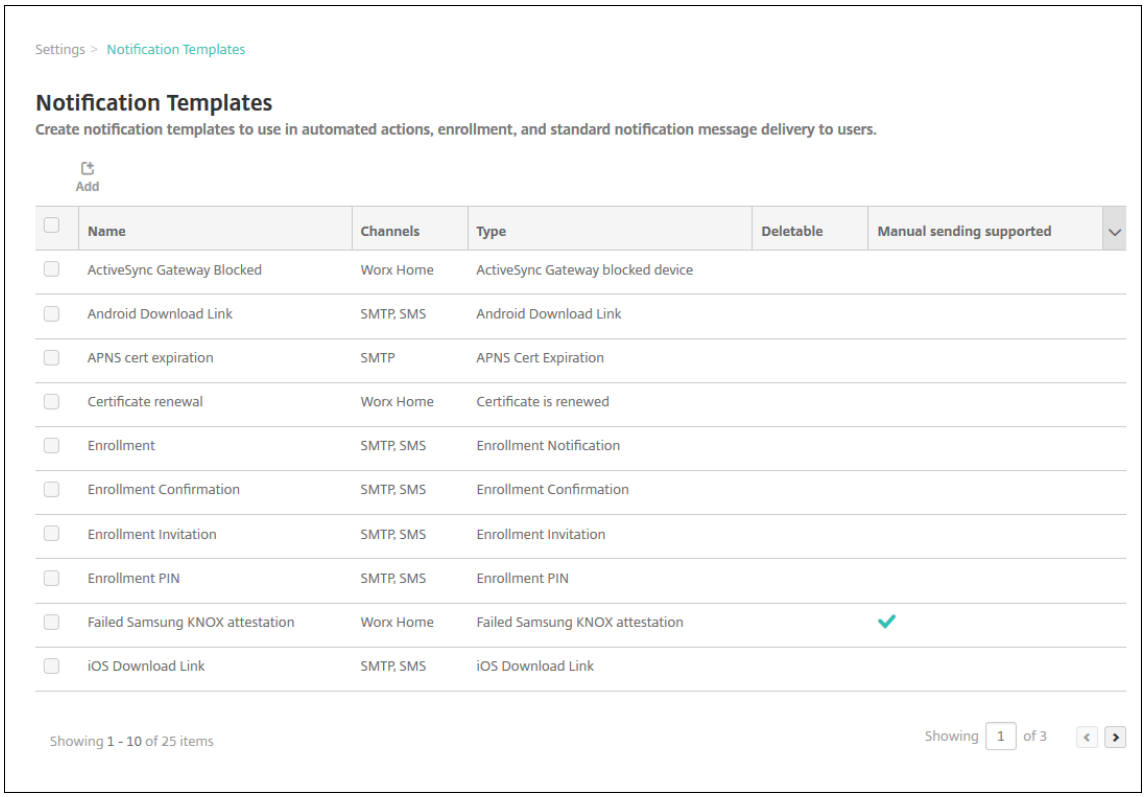
Citrix Endpoint Management inclut de nombreux modèles de notification prédéfinis. Ces modèles reflètent les différents types d'événements auxquels Citrix Endpoint Management répond automatiquement pour chaque appareil dans le système.

> **Remarque :**
>
> Si vous prévoyez d'utiliser les canaux SMTP pour envoyer des notifications aux utilisateurs, vous devez définir les canaux avant de pouvoir les activer. Citrix Endpoint Management vous invite

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> à configurer les canaux lorsque vous ajoutez des modèles de notification s'ils ne sont pas déjà configurés.

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Modèles de notification**. La page **Modèles de notification** s'affiche.



Ajouter un modèle de notification

1. Cliquez sur **Ajouter**. Si aucun serveur SMTP n'a été défini, un message s'affiche relatif à l'utilisation des notifications SMTP. Vous pouvez choisir de configurer le serveur SMTP maintenant ou les configurer les plus tard.

   Si vous choisissez de configurer les paramètres de serveur SMTP maintenant, vous serez redirigé vers la page **Serveur de notification** sur la page **Paramètres**. Après avoir configuré les canaux que vous souhaitez utiliser, vous pouvez retourner sur la page **Modèle de notification** pour continuer à ajouter ou modifier des modèles de notification.

   > **Important :**
   >
   > Si vous choisissez de configurer les paramètres du serveur SMTP ultérieurement, vous ne pouvez pas activer ces canaux lorsque vous ajoutez ou modifiez un modèle de notifica-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> tion. Par conséquent, ces canaux ne sont pas disponibles pour l'envoi de notifications utilisateur.

2. Pour configurer ces paramètres :

   - **Nom :** entrez un nom descriptif pour le modèle.
   - **Description :** entrez une description pour le modèle.
   - **Type :** dans la liste, cliquez sur le type de notification. Seuls les canaux pris en charge pour le type sélectionné s'affichent. seul un modèle de type Expiration du certificat APNS est autorisé, qui est un modèle prédéfini. Vous ne pouvez pas ajouter de modèle de ce type.

   > **Remarque :**
   >
   > Pour certains types de modèle, la phrase Envoi manuel pris en charge s'affiche en dessous du type. Ces types de modèles sont disponibles dans la liste **Notifications** du **Tableau de bord** et sur la page **Appareils**. Vous pouvez envoyer manuellement la notification aux utilisateurs à partir de ces emplacements. L'envoi manuel n'est disponible dans aucun des modèles qui utilisent les macros suivantes dans le champ Sujet ou Message d'un canal :

   - ${outofcompliance.reason(whitelist_blacklist_apps_name)}
   - ${outofcompliance.reason(smg_block)}

     > **Remarque :**
     >
     > La console Citrix Endpoint Management utilise les termes « liste noire » et « liste blanche ». Ces termes seront modifiés dans une prochaine version et les termes « liste de blocage » et « liste d'autorisation » les remplaceront.

3. Sous **Canaux**, configurez les informations pour chaque canal à utiliser avec cette notification. Vous pouvez choisir un ou tous les canaux. Le canal que vous choisissez dépend de la façon dont vous souhaitez envoyer des notifications :

   - Si vous choisissez **Citrix Secure Hub**, seuls les appareils iOS et Android reçoivent des notifications ; elles apparaissent dans la barre de notification de l'appareil.
   - Si vous choisissez **SMTP**, les utilisateurs qui se sont inscrits avec leur adresse e-mail reçoivent le message.

   Citrix Secure Hub :

   - **Activer :** cliquez pour activer le canal de notification.
   - **Message :** entrez le message à envoyer à l'utilisateur. Ce champ est obligatoire si vous utilisez Citrix Secure Hub. Pour de plus amples informations sur l'utilisation de macros dans un message, veuillez consulter la section Macros.
   - **Fichier son :** dans la liste, cliquez sur le son de notification que l'utilisateur entend lorsque la notification est reçue.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SMTP :

- **Activer :** cliquez pour activer le canal de notification.

  Vous ne pouvez activer la notification SMTP qu'après avoir configuré le serveur SMTP.

- **Expéditeur :** entrez un expéditeur (facultatif) pour la notification, qui peut être un nom, une adresse e-mail, ou les deux.

- **Destinataire :** ce champ contient une macro préconfigurée pour toutes les notifications sauf les notifications Ad-Hoc pour garantir l'envoi des notifications à l'adresse de destinataire SMTP correcte. Citrix vous recommande de ne pas modifier les macros dans les modèles. Vous pouvez ajouter d'autres destinataires (comme un administrateur d'entreprise) en ajoutant leurs adresses dans ce champ. Utilisez un point-virgule (;) pour séparer les macros et les autres adresses. Pour envoyer des notifications ad hoc, vous pouvez entrer des destinataires spécifiques, ou vous pouvez sélectionner des appareils à partir de la page **Gérer > Appareils** et envoyer des notifications à partir de cet emplacement. Pour plus de détails, voir Appareils.

- **Sujet :** entrez un sujet pour la notification. Ce champ est obligatoire.

- **Message :** entrez le message à envoyer à l'utilisateur. Pour de plus amples informations sur l'utilisation de macros dans un message, veuillez consulter la section Macros.

4. Cliquez sur **Ajouter**. Lorsque tous les canaux sont correctement configurés, ils apparaissent dans cet ordre sur la page **Modèles de notification** : SMTP et Citrix Secure Hub. Tout canal qui n'est pas correctement configuré apparaît après les canaux correctement configurés.

Modifier un modèle de notification

1. Sélectionnez un modèle de notification. La page d'édition spécifique à ce modèle apparaît. Vous pouvez modifier le modèle, à l'exception du champ **Type**, et activer ou désactiver les canaux.
2. Cliquez sur **Save**.

Supprimer un modèle de notification

Vous pouvez uniquement supprimer les modèles de notification que vous avez ajoutés. Vous ne pouvez pas supprimer les modèles de notification prédéfinis.

1. Sélectionnez un modèle de notification existant.
2. Cliquez sur **Delete**. Une boîte de dialogue de confirmation s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Cliquez sur **Supprimer** pour supprimer le modèle de notification, ou cliquez sur **Annuler** pour annuler la suppression du modèle de notification.

Configurer des rôles avec RBAC

March 1, 2024

La fonctionnalité de contrôle d'accès basé sur rôle (RBAC) de Citrix Endpoint Management vous permet d'attribuer des rôles aux utilisateurs et aux groupes. Les rôles sont des ensembles d'autorisations qui contrôlent le niveau d'accès des utilisateurs aux fonctions du système.

Citrix Endpoint Management est fourni avec les rôles utilisateur par défaut suivants. Vous pouvez utiliser les rôles par défaut en tant que modèles que vous personnalisez pour créer vos propres rôles utilisateur.

- **Administrateur :** accorde un accès complet au système.
- **Utilisateur :** autorise les utilisateurs à inscrire des appareils et à accéder au portail en libre-service.

Vous pouvez utiliser la fonctionnalité RBAC dans Citrix Endpoint Management pour :

- créer et modifier des rôles utilisateur ;
- attribuer des rôles à des groupes d'utilisateurs locaux et des groupes Active Directory ;
- attribuer des rôles aux administrateurs dans Citrix Cloud via la fonctionnalité **Gestion des identités et des accès > Administrateurs**. Voir Ajouter des rôles aux administrateurs Citrix Cloud.

Utiliser la fonctionnalité RBAC

Vous pouvez attribuer des rôles aux utilisateurs locaux, aux administrateurs cloud (dans Citrix Cloud), et aux groupes d'utilisateurs locaux et aux groupes Active Directory.

- **Utilisateurs locaux :** attribuez des rôles aux utilisateurs locaux à l'aide de **Gérer > Utilisateurs**. Vous ne pouvez attribuer qu'un seul rôle aux utilisateurs locaux. Pour modifier les rôles, vous pouvez modifier manuellement le compte utilisateur. Vous pouvez également créer un groupe pour les utilisateurs locaux et attribuer un rôle à ce groupe.
- **Administrateurs cloud :** un administrateur cloud est un compte d'utilisateur spécial créé par Citrix Cloud lorsqu'un administrateur est ajouté à votre compte client Citrix Cloud. Un compte d'administrateur cloud utilise le même nom d'utilisateur que le compte d'administrateur sur Citrix Cloud. Créez des rôles RBAC dans la console Citrix Endpoint Management et attribuez des rôles à ces utilisateurs via **Gestion des identités et des accès > Administrateurs** dans Citrix Cloud.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

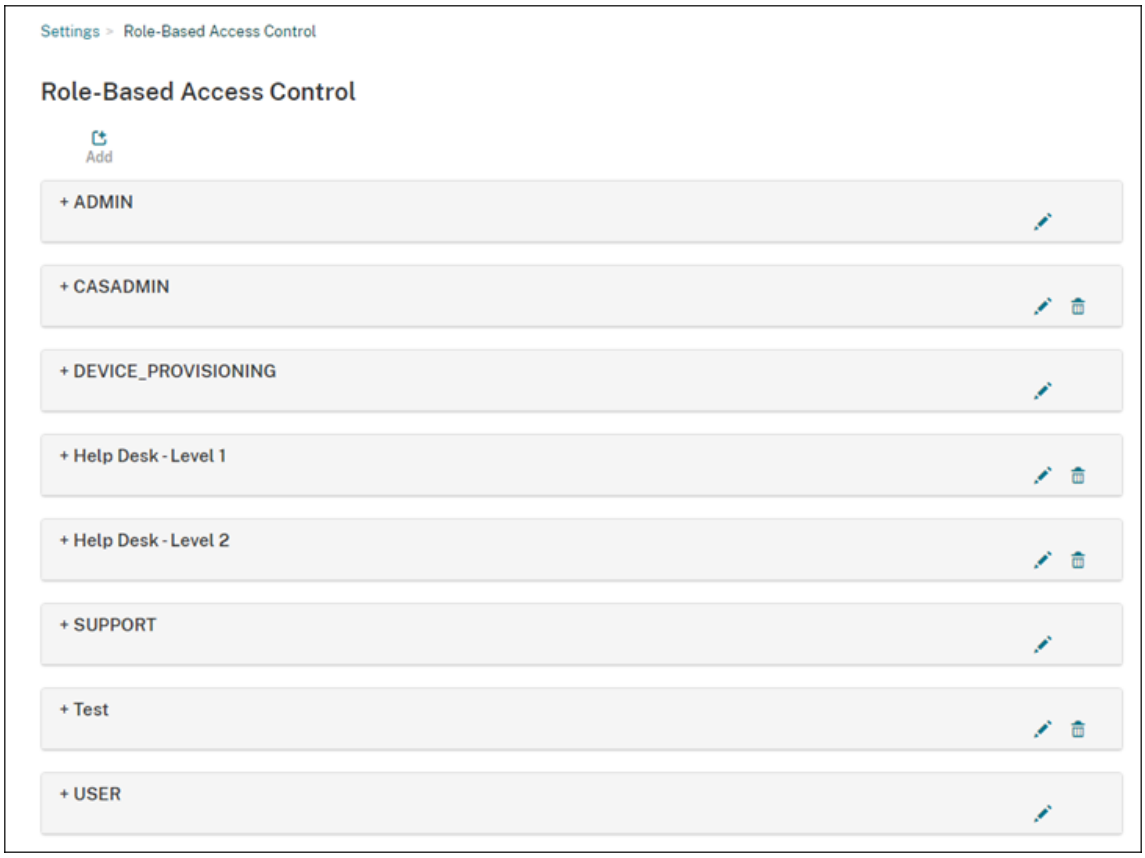
- **Groupes Active Directory :** tous les utilisateurs d'un groupe Active Directory disposent des mêmes autorisations. Si un utilisateur appartient à plusieurs groupes Active Directory, les autorisations sont fusionnées pour définir les autorisations de cet utilisateur. Par exemple, supposons que les utilisateurs d'ADGroupA puissent localiser les appareils des responsables et que les utilisateurs d'ADGroupB puissent effacer les appareils des employés. Un utilisateur appartenant aux deux groupes peut localiser et effacer les appareils des responsables et des employés. Si un utilisateur appartient à des groupes dont les autorisations sont contradictoires, les autorisations attribuées l'emportent.

Pour de plus amples informations, consultez la section À propos des comptes utilisateur.

Créer ou modifier des rôles

1. Dans la console Citrix Endpoint Management, pour accéder à la page **Paramètres**, cliquez sur l'icône d'engrenage dans le coin supérieur droit.
2. Cliquez sur **Contrôle d'accès basé sur rôle**. La page **Contrôle d'accès basé sur rôle** affiche les rôles utilisateur par défaut et les rôles que vous avez ajoutés.

   Cliquez sur le signe plus (+) à côté d'un rôle pour afficher toutes les autorisations pour ce rôle.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

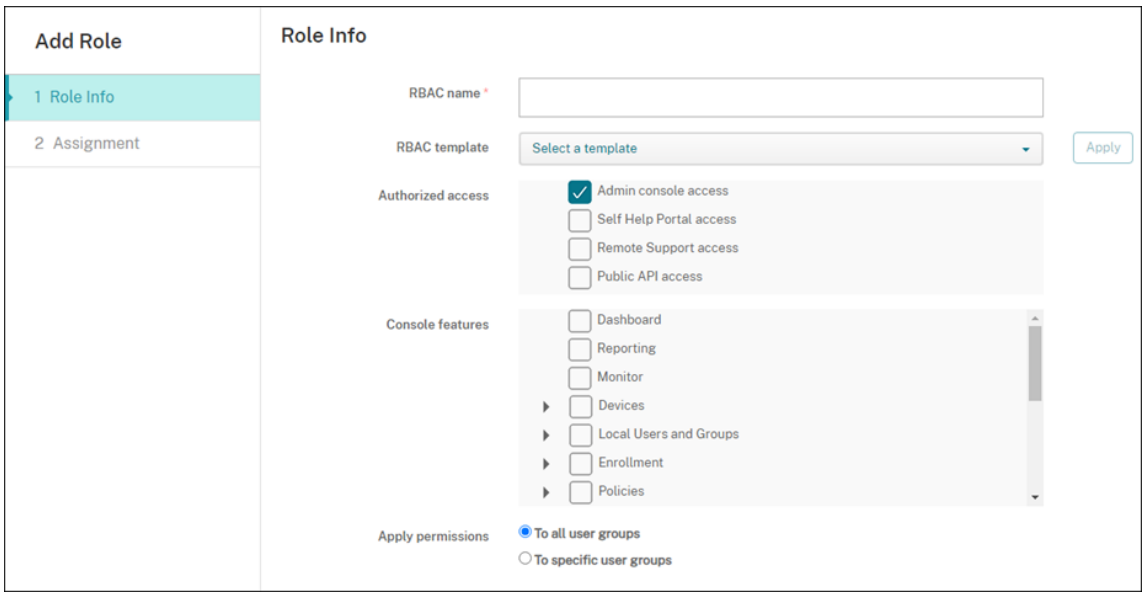
3. Pour ajouter un rôle, cliquez sur **Ajouter**. Ou cliquez sur le crayon à droite d'un rôle existant pour modifier un rôle.

   > **Remarque :**
   >
   > Vous pouvez supprimer un rôle en cliquant sur la corbeille à droite d'un rôle que vous avez défini. Vous ne pouvez pas supprimer les rôles utilisateur par défaut.

4. Sur la page **Ajouter un rôle**, entrez les informations suivantes :

   - **Nom RBAC :** entrez un nom descriptif pour le nouveau rôle utilisateur. Vous ne pouvez pas modifier le nom d'un rôle existant.
   - **Modèle RBAC :** si vous le souhaitez, sélectionnez un modèle en tant que point de départ pour le nouveau rôle. (Lors de la modification d'un rôle, vous ne pouvez pas sélectionner ou modifier les modèles.) Les modèles RBAC sont les rôles utilisateur par défaut qui définissent l'accès aux fonctions système.

   Cliquez sur le bouton **Appliquer** pour renseigner les cases **Accès autorisé** et **Fonctionnalités de la console**. Citrix Endpoint Management remplit ces champs avec les autorisations d'accès et de fonctionnalités prédéfinies pour le modèle sélectionné.



5. Sélectionnez ou décochez les cases à cocher appropriées dans **Accès autorisé** et **Fonctionnalités de la console** pour personnaliser le rôle.

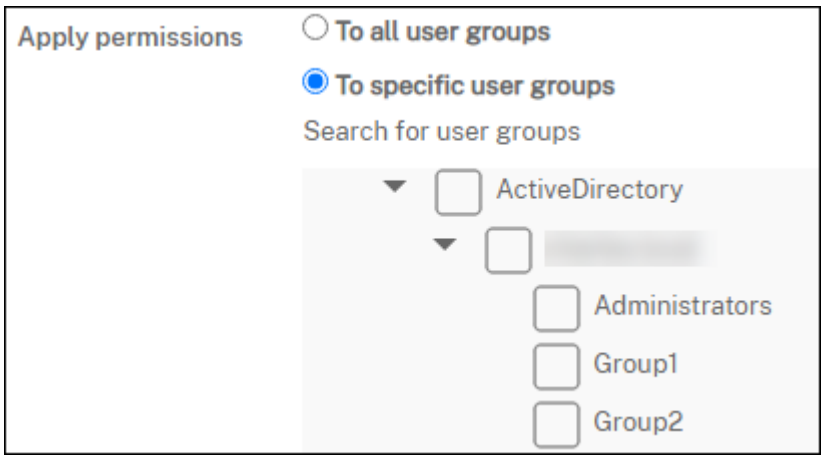
   Cliquez sur le triangle situé en regard d'une fonctionnalité de console pour afficher et sélectionner les autorisations spécifiques à cette fonctionnalité. La case à cocher de niveau supérieur ne permet pas de sélectionner les autorisations individuelles. Sélectionnez des options individuelles après avoir développé l'autorisation de niveau supérieur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. **Appliquer des autorisations :** cliquez sur **À des groupes d'utilisateurs spécifiques** pour appliquer des autorisations aux groupes que vous sélectionnez.

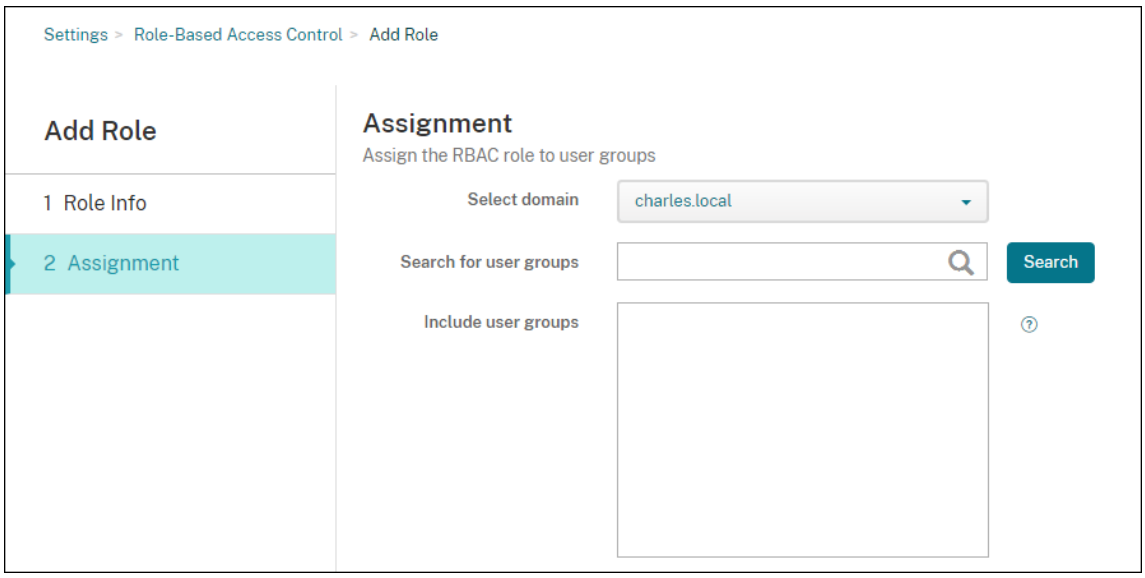
   Par exemple, si un administrateur RBAC dispose d'autorisations sur le groupe d'utilisateurs ActiveDirectory :

   - L'administrateur ne peut accéder aux informations que pour les utilisateurs qui font partie du groupe ActiveDirectory.
   - L'administrateur ne peut afficher aucun autre utilisateur local ou AD. L'administrateur peut afficher les utilisateurs qui sont membres de groupes enfants de l'un ou l'autre de ces groupes.
   - L'administrateur peut envoyer des invitations :
     - aux groupes d'autorisations et à leurs groupes enfants
     - aux utilisateurs qui sont membres des groupes d'autorisations et de leurs groupes enfants



7. Cliquez sur **Suivant** et entrez les informations suivantes pour attribuer le rôle à des groupes d'utilisateurs.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Sélectionner un domaine :** dans la liste, sélectionnez un domaine.
- **Rechercher des groupes d'utilisateurs :** cliquez sur **Rechercher** pour afficher la liste de tous les groupes disponibles. Tapez un nom de groupe complet ou partiel pour limiter la recherche.
- **Inclure des groupes d'utilisateurs :** dans la liste qui s'affiche, sélectionnez les groupes d'utilisateurs auxquels vous souhaitez attribuer le rôle.

8. Cliquez sur **Enregistrer**.

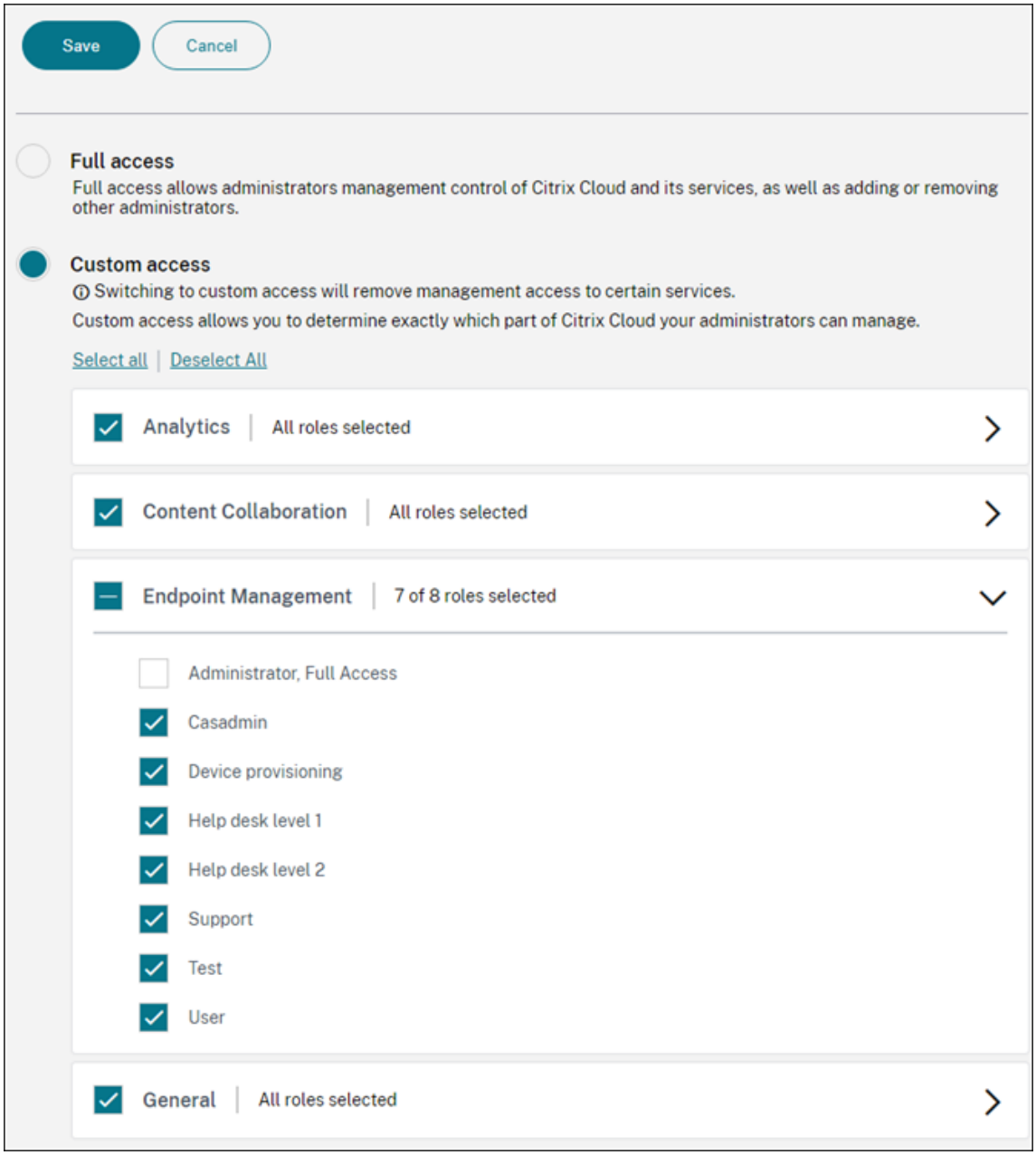
Ajouter des rôles aux administrateurs Citrix Cloud

Au lieu d'attribuer des rôles RBAC aux administrateurs Citrix Cloud via la console Citrix Endpoint Management, attribuez des rôles à partir de la console Citrix Cloud.

1. Dans la console Citrix Cloud, accédez à **Gestion des identités et des accès > Administrateurs**.
2. Sélectionnez un fournisseur d'identité, puis tapez une adresse e-mail pour ajouter un administrateur. Cliquez sur **Inviter**.

   Cliquez sur le bouton **...** à la fin d'une ligne d'administrateur existante pour modifier ces autorisations.
3. Cliquez sur **Accès personnalisé**. Lorsque vous attribuez des autorisations à l'administrateur, vous pouvez sélectionner les rôles RBAC créés dans la console Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Cliquez sur **Envoyer une invitation** pour envoyer une invitation à un nouvel administrateur ou cliquez sur **Enregistrer** pour terminer la modification d'un administrateur.

Rôles prédéfinis

Chaque rôle RBAC prédéfini dispose de certains accès et de certaines autorisations associés. Les tableaux suivants décrivent chacune des autorisations pour le rôle Administrateur et pour le rôle Utilisateur. Vous ne pouvez ni supprimer ni modifier les rôles prédéfinis.

- Pour obtenir une liste complète des autorisations par défaut pour chaque rôle intégré,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

téléchargez le PDF Role-Based Access Control Defaults.

- Pour plus d'informations sur les comptes utilisateur Citrix Endpoint Management, reportez-vous à la section À propos des comptes utilisateur.

> **Important :**
>
> Sous l'autorisation Paramètres, l'autorisation RBAC donne aux utilisateurs Admin un accès complet, y compris la possibilité d'attribuer leurs propres autorisations. Accordez cet accès uniquement aux utilisateurs auxquels vous avez l'intention de donner la possibilité de manipuler tout ce qui se trouve dans le système Citrix Endpoint Management.

Rôle d'administrateur

Le rôle Admin prédéfini fournit un accès spécifique dans Citrix Endpoint Management. Par défaut, **Accès autorisé** (sauf Portail en libre-service), **Fonctionnalités de la console** et **Appliquer des autorisations** sont activés.

Vous pouvez modifier le rôle pour les utilisateurs locaux auxquels le rôle Admin est attribué à l'aide de **Gérer > Utilisateurs**. Pour les utilisateurs du cloud qui ont le rôle Admin, utilisez la console Citrix Cloud pour modifier le rôle. Par défaut, les utilisateurs cloud et locaux dotés du rôle Admin disposent d'un accès complet.

Accès autorisé pour les administrateurs

Accès à la console d'admin	Les administrateurs ont accès à toutes les fonctions de la console Citrix Endpoint Management.
Accès au portail en libre-service	Par défaut, les administrateurs ne peuvent pas accéder au portail en libre-service. (Les utilisateurs disposant de l'accès Utilisateur peuvent uniquement accéder au portail en libre-service.)
Accès à l'assistance à distance	Les administrateurs ont accès à la fonctionnalité d'assistance à distance.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Accès à l'API publique	Les administrateurs ont accès à l'API publique pour réaliser via un programme des actions qui sont disponibles sur la console Citrix Endpoint Management. Ces actions comprennent l'administration des certificats, des applications, des appareils, des groupes de mise à disposition et des utilisateurs locaux.

Fonctionnalités de la console pour les administrateurs Les administrateurs ont un accès illimité à la console Citrix Endpoint Management.

Tableau de bord	Le **tableau de bord** est la première page que les administrateurs voient s'afficher après une ouverture de session sur la console Citrix Endpoint Management. Le **tableau de bord** contient des informations de base sur les notifications et les appareils.
Rapports	La page **Analyser > Rapports** propose des rapports prédéfinis qui vous permettent d'analyser les déploiements d'applications et d'appareils.
Appareils	La page **Gérer > Appareils** vous permet de gérer les appareils des utilisateurs. Vous pouvez ajouter des appareils un par un sur la page, ou importer un fichier de provisioning pour ajouter plusieurs appareils à la fois.
Utilisateurs et groupes locaux	La page **Gérer > Utilisateurs** vous permet d'ajouter, de modifier ou de supprimer des utilisateurs locaux et des groupes d'utilisateurs locaux.
Inscription	La page **Gérer > Invitations d'inscription** vous permet de gérer la manière dont les utilisateurs sont invités à inscrire leurs appareils dans Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégies	La page **Configurer > Stratégies d'appareil** est la page à partir de laquelle vous gérez les stratégies telles que VPN et Réseau.
Application	La page **Configurer > Applications** vous permet de gérer les applications que les utilisateurs peuvent installer sur leurs appareils.
Média	La page **Configurer > Média** vous permet de gérer le contenu multimédia que les utilisateurs peuvent installer sur leurs appareils.
Action	La page **Configurer > Actions** vous permet de gérer les réponses pour déclencher des événements.
Groupe de mise à disposition	La page **Configurer > Groupes de mise à disposition** vous permet de gérer les groupes de mise à disposition et les ressources associées.
Profil d'inscription	La page **Configurer > Profils d'inscription** indique comment les utilisateurs peuvent inscrire leurs appareils.
Alexa for Business	La page **Paramètres** vous permet de gérer vos profils Alexa for Business.
Paramètres	La page **Paramètres** vous permet de gérer les paramètres du système, tels que les propriétés client et serveur, les certificats et les fournisseurs d'identités. **Important :** ces paramètres incluent l'autorisation RBAC. L'autorisation RBAC donne aux administrateurs un accès complet, y compris la possibilité d'attribuer leurs propres autorisations. Accordez cet accès uniquement aux utilisateurs auxquels vous avez l'intention de donner la possibilité de manipuler tout ce qui se trouve dans le système Citrix Endpoint Management.
Assistance	La page **Dépannage et support** vous permet de réaliser des tâches de résolution des problèmes tels qu'effectuer des diagnostics et générer des journaux.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Restrictions d'appareil pour les administrateurs Les administrateurs accèdent aux fonctionnalités des appareils depuis la console par la définition de restrictions d'appareil, la configuration et l'envoi de notifications aux appareils, l'administration des applications sur les appareils, et ainsi de suite.

Effacer un appareil	Permet d'effacer toutes les données et applications d'un appareil, y compris des cartes mémoire si l'appareil en est doté.
Effacer la restriction	Permet de supprimer une ou plusieurs restrictions.
Effacer les données d'entreprise d'un appareil	Permet d'effacer toutes les données et applications d'entreprise d'un appareil, sans toucher aux données et applications personnelles.
Afficher la localisation	Permet d'afficher l'emplacement géographique et définir des restrictions sur un appareil. Inclut : Localiser l'appareil, Suivre l'appareil.
Verrouiller un appareil	Permet de verrouiller à distance un appareil de façon à ce que les utilisateurs ne puissent pas utiliser l'appareil.
Déverrouiller un appareil	Permet de déverrouiller à distance un appareil de façon à ce que les utilisateurs puissent utiliser l'appareil.
Verrouiller le conteneur	Permet de verrouiller à distance le conteneur d'entreprise sur un appareil.
Déverrouiller le conteneur	Permet de déverrouiller à distance le conteneur d'entreprise sur un appareil.
Réinitialiser le mot de passe du conteneur	Permet de réinitialiser le mot de passe du conteneur d'entreprise.
Activer contournement du verrouillage d'activation ASM	Stocke un code de contournement sur un appareil iOS supervisé lorsque le verrouillage d'activation est activé. Pour effacer l'appareil, utilisez ce code pour annuler automatiquement le verrouillage d'activation.
Obtenir utilisateurs résidents	Répertorie les utilisateurs qui ont des comptes actifs sur l'appareil actuel. Cette action force une synchronisation entre l'appareil et la console Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Déconnecter utilisateur résident	Force une déconnexion de l'utilisateur actuel.
Supprimer utilisateur résident	Supprime la session en cours pour un utilisateur spécifique. L'utilisateur peut se reconnecter.
Appeler l'appareil	Permet d'appeler à distance un appareil Windows à plein volume pendant 5 minutes.
Redémarrer l'appareil	Permet de redémarrer les appareils Windows à partir de la console Citrix Endpoint Management.
Déployer vers un appareil	Permet d'envoyer des applications, des notifications, des restrictions, et d'autres ressources à un appareil.
Modifier un appareil	Permet de modifier les paramètres sur l'appareil.
Notification vers un appareil	Permet d'envoyer une notification à un appareil.
Ajouter/Supprimer un appareil	Permet d'ajouter ou de supprimer des appareils dans Citrix Endpoint Management.
Importer des appareils	Permet d'importer un groupe d'appareils depuis un fichier vers Citrix Endpoint Management.
Exporter la liste des appareils	Permet de collecter des informations sur les appareils à partir de la page Appareil et de les exporter vers un fichier .csv.
Révoquer un appareil	Permet d'empêcher un appareil de se connecter à Citrix Endpoint Management.
Mode kiosque	Permet de refuser l'accès à toutes les applications sur un appareil. Sur Android, cette restriction empêche les utilisateurs de se connecter à Citrix Endpoint Management. Sur iOS, les utilisateurs peuvent se connecter, mais ils ne peuvent pas accéder aux applications.
Effacement des applications	Sur Android, cette restriction supprime le compte Citrix Endpoint Management de l'utilisateur. Sur iOS, cette restriction supprime les clés de cryptage dont les utilisateurs ont besoin pour pouvoir accéder aux fonctionnalités de Citrix Endpoint Management.
Voir l'inventaire logiciel	Permet de voir quels logiciels sont installés sur un appareil.
Demander la mise en miroir AirPlay	Permet de démarrer le streaming AirPlay.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Arrêter la mise en miroir AirPlay	Permet d'arrêter le streaming AirPlay.
Activer le mode perdu	Sur la page **Gérer > Appareils**, vous pouvez placer un appareil supervisé en mode perdu pour le bloquer sur l'écran de verrouillage. Vous pouvez ensuite localiser l'appareil en cas de perte ou de vol.
Désactiver le mode perdu	Sur la page **Gérer > Appareils**, vous pouvez désactiver le mode perdu pour un appareil.
Mise à jour de l'OS de l'appareil	Vous pouvez déployer une stratégie de mise à jour d'OS sur les appareils.
Arrêter l'appareil	Permet d'arrêter les appareils iOS à partir de la console Citrix Endpoint Management.
Redémarrer l'appareil	Permet de redémarrer les appareils iOS à partir de la console Citrix Endpoint Management.
Renouveler le certificat d'inscription d'appareil	Permet de renouveler le certificat CA de l' appareil.

Utilisateurs et groupes locaux Les administrateurs gèrent les utilisateurs locaux et les groupes d' utilisateurs locaux sur la page **Gérer > Utilisateurs** dans Citrix Endpoint Management.

Ajouter des utilisateurs locaux
Supprimer des utilisateurs locaux
Modifier un utilisateur local
Importer des utilisateurs locaux
Exporter un utilisateur local
Groupes d'utilisateurs locaux
Obtenir l'ID de verrouillage de l'utilisateur local
Supprimer verrouillage de l'utilisateur local

Inscription Les administrateurs peuvent ajouter et supprimer des invitations d'inscription, envoyer des notifications aux utilisateurs et exporter la table d'inscription vers un fichier .csv.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ajouter/supprimer inscription	Permet d'ajouter ou de supprimer une invitation d'inscription à un utilisateur ou un groupe d'utilisateurs.
Notifier un utilisateur	Permet d'envoyer une invitation d'inscription à un utilisateur ou un groupe d'utilisateurs.
Exporter la table d'invitation d'inscription	Permet de collecter des informations d'inscription à partir de la page Inscription et de les exporter vers un fichier .csv.

Stratégies

Ajouter/Supprimer une stratégie	Permet d'ajouter ou de supprimer une stratégie d'appareil ou d'application.
Modifier une stratégie	Permet de modifier une stratégie d'appareil ou d'application.
Charger la stratégie	Permet de charger une stratégie d'appareil ou d'application.
Cloner la stratégie	Permet de copier une stratégie d'appareil ou d'application.
Désactiver la stratégie	Permet de désactiver une stratégie d'application existante.
Exporter la stratégie	Permet de collecter des informations sur une stratégie à partir de la page Stratégies d'appareil et de les exporter vers un fichier .csv.
Attribuer la stratégie	Permet d'attribuer une stratégie d'appareil à un ou plusieurs groupes de mise à disposition.

Application Les administrateurs gèrent les applications sur la page **Configurer > Applications** dans Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ajouter/supprimer un magasin d'applications ou une application d'entreprise	Permet d'ajouter ou de supprimer une application de magasin d'applications public ou une application d'entreprise (non compatible avec MDX).
Modifier un magasin d'applications ou une application d'entreprise	Permet de modifier une application de magasin d'applications publiques ou une application d'entreprise (non MDX).
Ajouter/supprimer une application MDX, Web et SaaS	Permet d'ajouter ou de supprimer une application MDX, une application de votre réseau interne (application Web) ou une application d'un réseau public (SaaS) à Citrix Endpoint Management.
Modifier une application MDX, Web et SaaS	Permet de modifier une application MDX, une application de votre réseau interne (application Web) ou une application d'un réseau public (SaaS) à Citrix Endpoint Management.
Ajouter/supprimer une catégorie	Permet d'ajouter ou de supprimer une catégorie dans laquelle les applications peuvent s'afficher dans le magasin d'applications.
Attribuer une application publique/d'entreprise à un groupe de mise à disposition	Permet d'attribuer une application de magasin d'applications public ou une application MDX à un groupe de mise à disposition pour le déploiement.
Attribuer une application MDX/WebLink/SaaS à un groupe de mise à disposition	Permet d'attribuer à un groupe de mise à disposition une application MDX, ne nécessitant pas d'authentification unique (WebLink) ou provenant d'un réseau public (SaaS).
Exporter la liste des applications	Permet de collecter des informations sur les applications à partir de la page Application et de les exporter vers un fichier .csv.

Média Permet de gérer le contenu multimédia obtenu à partir d'un magasin d'applications public ou via une licence d'achat en volume.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ajouter/supprimer livres App Store ou d'entreprise
Attribuer des livres publics/d'entreprise à un groupe de mise à disposition
Modifier livres App Store ou d'entreprise

Action

Ajouter/supprimer une action	Ajouter ou supprimer une action définie par un déclencheur et une réponse associée. Un déclencheur est un événement, une propriété d'appareil ou d'utilisateur, ou un nom d'application installée.
Modifier action	Modifier une action définie par un déclencheur et une réponse associée. Un déclencheur est un événement, une propriété d'appareil ou d'utilisateur, ou un nom d'application installée.
Attribuer une action à un groupe de mise à disposition	Permet d'attribuer une action à un groupe de mise à disposition pour le déploiement vers les appareils d'utilisateurs.
Exporter action	Permet de collecter des informations sur une action à partir de la page Actions et de les exporter vers un fichier .csv.

Groupe de mise à disposition Les administrateurs gèrent les groupes de mise à disposition à partir de la page **Configurer > Groupes de mise à disposition**.

Ajouter/supprimer un groupe de mise à disposition	Permet de créer ou de supprimer un groupe de mise à disposition, ce qui ajoute les utilisateurs spécifiés et les stratégies, les applications et les actions facultatives.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Modifier un groupe de mise à disposition	Permet de modifier un groupe de mise à disposition, ce qui modifie les utilisateurs et les stratégies, les applications et les actions facultatives.
Déployer un groupe de mise à disposition	Permet de distribuer un groupe de mise à disposition.
Exporter un groupe de mise à disposition	Permet de collecter des informations sur un groupe de mise à disposition à partir de la page Groupe de mise à disposition et de les exporter vers un fichier .csv.

Profil d'inscription Permet de gérer les profils d'inscription.

Ajouter/supprimer profil d'inscription
Modifier le profil d'inscription
Attribuer profil d'inscription à un groupe de mise à disposition

Alexa for Business Permet de gérer les profils Alexa for Business.

Ajouter/Supprimer/Modifier des pièces
Ajouter/Supprimer/Modifier des profils de pièces
Ajouter/Supprimer/Modifier des groupes de Skills

Paramètres des administrateurs Les administrateurs configurent divers paramètres sur les pages **Paramètres**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

RBAC	Attribution d'un rôle RBAC. **Important :** cette autorisation donne aux administrateurs un accès complet, y compris la possibilité d'attribuer leurs propres autorisations. Accordez cet accès uniquement aux utilisateurs auxquels vous avez l'intention de donner la possibilité de manipuler tout ce qui se trouve dans le système Citrix Endpoint Management.
LDAP	Permet de gérer un ou plusieurs annuaires compatibles LDAP, tels que Active Directory, pour importer des groupes, comptes d'utilisateurs et propriétés associées.
Inscription	Permet d'activer des modes d'inscription sécurisée pour les utilisateurs ainsi que le portail en libre-service.
Gestion des versions	Permet d'afficher la version installée. Inclut : Mise à jour de la gestion des versions
Certificats	Modifier le certificat APNs
Modèles de notification	Permet de créer des modèles de notification à utiliser dans les actions automatisées, l'inscription et la remise de messages de notification standard aux utilisateurs.
Workflows	Permet de gérer la création, l'approbation et la suppression des comptes d'utilisateur à utiliser avec les configurations d'application.
Fournisseur d'identités	Permet d'ajouter un ou plusieurs fournisseurs d'informations d'identification autorisés à émettre des certificats d'appareil. Les fournisseurs d'informations d'identification contrôlent le format du certificat et les conditions de renouvellement ou de révocation du certificat.
Entités PKI	Permet de gérer les entités d'infrastructure de clé publique (générique, Services de certificats Microsoft ou autorité de certification discrétionnaire).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Tester la connexion PKI	Permet d'utiliser le bouton **Tester la connexion** sur la page **Paramètres > Entités PKI** pour vous assurer que le serveur est accessible.
Propriétés du client	Permet de gérer les différentes propriétés sur les appareils d'utilisateur, telles que le type de code secret, le niveau de sécurité et la date d'expiration.
Support client	Permet de définir la méthode utilisée par les utilisateurs pour contacter votre service d'assistance (messagerie, téléphone ou ticket d'assistance).
Personnalisation du client	Permet de personnaliser le nom du magasin et les vues de magasin par défaut dans le magasin d'applications. Permet d'ajouter un logo personnalisé qui s'affiche sur le magasin d'applications ou Citrix Secure Hub.
Passerelle SMS de l'opérateur	Permet de configurer des passerelles SMS d'opérateur pour configurer les notifications que Citrix Endpoint Management envoie via les passerelles SMS d'opérateur.
Serveur de notification	Permet de définir un serveur de passerelle SMTP pour envoyer des e-mails aux utilisateurs.
ActiveSync Gateway	Permet de gérer l'accès des utilisateurs à des utilisateurs et à des appareils à l'aide de règles et de propriétés.
Google Chrome	Permet de configurer Citrix Endpoint Management pour communiquer avec votre compte Google Workspace.
Programmes de déploiement d'Apple	Permet d'ajouter un compte de programme de déploiement d'Apple à Citrix Endpoint Management.
Inscription d'appareils dans Apple Configurator	Permet de configurer les paramètres d'Apple Configurator dans la console Citrix Endpoint Management.
Paramètres d'achat en volume/iOS	Permet d'ajouter des comptes d'achat en volume d'Apple.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NetScaler Gateway	Permet de configurer les paramètres de NetScaler Gateway (anciennement Citrix Gateway) dans Citrix Endpoint Management.
Contrôle d'accès réseau	Définissez les conditions qui déterminent si un appareil n'est pas conforme de façon à ce qu'il ne puisse pas accéder au réseau.
Propriétés du serveur	Permet d'ajouter ou de modifier des propriétés de serveur. Requiert le redémarrage de Citrix Endpoint Management sur tous les nœuds.
Virtual Apps and Desktops	Autorise les utilisateurs à ajouter Citrix Virtual Apps and Desktops via l'application Citrix Workspace.
Citrix Files	Lors de l'utilisation de Citrix Endpoint Management avec des comptes Enterprise : configurez les paramètres pour la connexion au compte ShareFile et au compte de service d'administrateur afin de gérer les comptes utilisateur. Requiert des informations d'identification d'administrateur et de domaine Citrix Files. Lors de l'utilisation de Citrix Endpoint Management avec des connecteurs StorageZone : permet de configurer Citrix Endpoint Management pour pointer vers les partages réseau et les emplacements SharePoint définis dans les connecteurs StorageZone.
Android Enterprise	Permet de configurer les paramètres de serveur Android Enterprise.
Fournisseur d'identité (IdP)	Permet de configurer un fournisseur d'identité.
Outils Citrix Endpoint Management	Permet d'accéder à la page Citrix Endpoint Management Tools.
Inscription en bloc de Windows	Permet de configurer les paramètres d'inscription en bloc de Windows.

Assistance Les administrateurs peuvent effectuer diverses tâches de support.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Test de la connectivité NetScaler Gateway	Permet de tester la connectivité de NetScaler Gateway par adresse IP. Requiert un nom d'utilisateur et un mot de passe.
Tests de la connectivité de Citrix Endpoint Management	Permet de tester la connectivité de certaines fonctionnalités Citrix Endpoint Management, telles que la base de données, DNS et Google Plan.
Documentation Produit Citrix	Permet d'accéder au site de documentation Citrix Endpoint Management public.
Centre de connaissances de Citrix	Permet d'accéder au site d'assistance de Citrix pour rechercher des articles de la base de connaissances.
Journaux	Permet d'afficher et de télécharger des fichiers journaux.
Macros	Permet de remplir les données de propriété d'appareil ou d'utilisateur dans le champ textuel d'un profil, d'une stratégie, d'une notification ou d'un modèle d'inscription. Configurez une stratégie et déployez-la auprès d'un grand nombre d'utilisateurs et de manière à ce que des valeurs spécifiques à l'utilisateur s'affichent pour chaque utilisateur ciblé.
Configuration PKI	Permet d'importer et d'exporter des informations de configuration d'infrastructure de clé publique (PKI).
Utilitaire de signature APNs	Permet d'envoyer une demande de certificats APNS ou de télécharger un certificat APNS Citrix Secure Mail pour iOS.
Citrix Insight Services	Permet de charger des journaux sur Citrix Insight Services (CIS) pour obtenir de l'aide avec divers problèmes.
État d'un appareil envoyé à NetScaler Gateway Connector pour Exchange ActiveSync	Permet d'effectuer une requête auprès de Citrix Endpoint Management pour connaître l'état d'un appareil tel qu'envoyé au connecteur pour Exchange ActiveSync. La requête est basée sur l'ID ActiveSync de l'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Restreindre l'accès aux groupes Les utilisateurs de niveau administrateur peuvent appliquer des autorisations à tous les groupes d'utilisateurs.

Fonctionnalités de la console pour le provisioning d'appareils Les utilisateurs avec le rôle Provisioning d'appareils ont l'accès limité suivant à la console Citrix Endpoint Management. Par défaut, les fonctionnalités suivantes sont activées.

Restrictions d'appareil

Modifier un appareil	Permet de modifier les paramètres sur l'appareil.
Ajouter/Supprimer un appareil	Permet d'ajouter ou de supprimer des appareils dans Citrix Endpoint Management.

Paramètres pour le provisioning d'appareils Les utilisateurs du provisioning d'appareils peuvent accéder à la page **Paramètres**, mais ils ne sont pas autorisés à configurer les fonctionnalités.

Rôle utilisateur

Les utilisateurs avec le rôle Utilisateur disposent de l'accès limité suivant à Citrix Endpoint Management.

Accès autorisé pour les utilisateurs

Portail en libre-service	Fournit un accès utilisateur uniquement au portail d'assistance (en libre-service) dans Citrix Endpoint Management.

Fonctionnalités de la console pour les utilisateurs Les utilisateurs ont l'accès limité suivant à la console Citrix Endpoint Management.

Accès restreint pour les utilisateurs

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Effacer un appareil	Permet d'effacer toutes les données et applications d'un appareil, y compris des cartes mémoire si l'appareil en est doté.
Effacer les données d'entreprise d'un appareil	Permet d'effacer toutes les données et applications d'entreprise d'un appareil, sans toucher aux données et applications personnelles.
Afficher la localisation	Permet d'afficher l'emplacement géographique et définir des restrictions sur un appareil. Inclut : Localiser un appareil, Voir l'emplacement d'un appareil, Suivre un appareil, Suivre l'emplacement d'un appareil au fil du temps.
Verrouiller un appareil	Permet de verrouiller à distance un appareil de façon à ce qu'il ne puisse pas être utilisé.
Déverrouiller un appareil	Permet de déverrouiller à distance un appareil de façon à ce qu'il puisse être utilisé.
Verrouiller le conteneur	Permet de verrouiller à distance le conteneur d'entreprise sur un appareil.
Déverrouiller le conteneur	Permet de déverrouiller à distance le conteneur d'entreprise sur un appareil.
Réinitialiser le mot de passe du conteneur	Permet de réinitialiser le mot de passe du conteneur d'entreprise.
Activer contournement du verrouillage d'activation ASM	Stocke un code de contournement sur un appareil iOS supervisé lorsque le verrouillage d'activation est activé. Pour effacer l'appareil, utilisez ce code pour annuler automatiquement le verrouillage d'activation.
Obtenir utilisateurs résidents	Répertorie les utilisateurs qui ont des comptes actifs sur l'appareil actuel. Cette action force une synchronisation entre l'appareil et la console Citrix Endpoint Management.
Déconnecter utilisateur résident	Force une déconnexion de l'utilisateur actuel.
Supprimer utilisateur résident	Supprime la session en cours pour un utilisateur spécifique. L'utilisateur peut se reconnecter.
Appeler l'appareil	Permet d'appeler à distance un appareil Windows à plein volume pendant 5 minutes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Redémarrer l'appareil	Permet de redémarrer un appareil Windows.
Mode kiosque	Permet de refuser l'accès à toutes les applications sur un appareil. Sur Android, les utilisateurs ne peuvent pas se connecter à Citrix Endpoint Management. Sur iOS, les utilisateurs peuvent se connecter, mais ils ne peuvent pas accéder aux applications.
Effacement des applications	Sur Android, cette restriction supprime le compte Citrix Endpoint Management de l'utilisateur. Sur iOS, cette restriction supprime les clés de cryptage dont les utilisateurs ont besoin pour pouvoir accéder aux fonctionnalités de Citrix Endpoint Management.
Voir l'inventaire logiciel	Permet de voir quels logiciels sont installés sur un appareil.

Restrictions d'inscription pour les utilisateurs

Ajouter/supprimer inscription	Permet d'ajouter ou de supprimer une invitation d'inscription à un utilisateur ou un groupe d'utilisateurs.
Notifier un utilisateur	Permet d'envoyer une invitation d'inscription à un utilisateur ou un groupe d'utilisateurs.

Restreindre l'accès aux groupes pour tous les rôles Pour les rôles par défaut, cette autorisation est définie par défaut et peut être appliquée à tous les groupes d'utilisateurs. Vous ne pouvez pas modifier le rôle.

Licences

November 29, 2023

Pour plus d'informations sur l'utilisation des licences Citrix, consultez :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Surveiller les licences et l'utilisation active pour les services cloud
- Surveiller les licences et l'utilisation active du service Citrix Endpoint Management

Gestion des appareils

March 1, 2024

Citrix Endpoint Management peut provisionner, gérer, sécuriser et inventorier un large éventail de types d'appareils au sein d'une seule console de gestion.

- Utilisez un ensemble commun de stratégies pour gérer les appareils pris en charge. Pour un aperçu rapide des stratégies disponibles par plate-forme :

  1. Accédez à la console Citrix Endpoint Management et cliquez sur **Configurer > Stratégies d'appareil**.
  2. Cliquez sur **Ajouter**, puis sélectionnez les plates-formes que vous souhaitez afficher.

     Pour plus d'informations, voir Filtrer la liste des stratégies d'appareil ajoutées.

- Protégez les informations de votre entreprise grâce à des mesures de sécurité strictes pour l'identité, les appareils appartenant à l'entreprise et BYO, les applications, les données et le réseau. Spécifiez l'identité utilisateur à utiliser pour s'authentifier sur les appareils. Configurez comment séparer les données d'entreprise et les données personnelles sur les appareils.
- Distribuez n'importe quelle application aux utilisateurs finaux, quel que soit l'appareil ou le système d'exploitation. Protégez vos informations au niveau des applications et fournissez la gestion des applications mobiles d'entreprise.
- Utilisez des contrôles de provisioning et de configuration pour configurer les appareils. Ces contrôles incluent l'inscription d'appareils, l'application de stratégie et les privilèges d'accès.
- Utilisez les contrôles de sécurité et de conformité pour créer une base de sécurité personnalisée avec des déclencheurs exploitables. Par exemple, vous pouvez verrouiller, effacer ou notifier un appareil ne respectant pas les normes de conformité définies.
- Utilisez les contrôles de mise à jour du système d'exploitation pour empêcher ou appliquer les mises à jour du système d'exploitation. Cette fonctionnalité est essentielle pour la prévention des pertes de données face aux vulnérabilités ciblées du système d'exploitation.

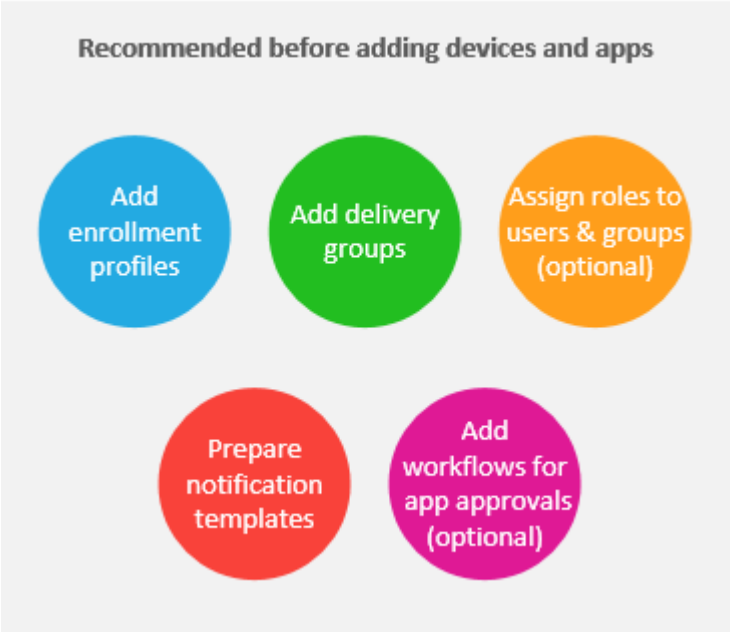
Pour accéder aux articles concernant chaque plate-forme prise en charge, développez la section « Gestion des appareils » dans la liste des contenus. Ces articles fournissent des détails spécifiques à chaque plate-forme d'appareil. Le reste de cet article décrit comment effectuer des tâches générales de gestion des appareils.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Procédure de gestion des appareils

Les diagrammes de cette section fournissent une séquence suggérée pour l'exécution des tâches de gestion des appareils.

1. **Conditions préalables recommandées pour l'ajout d'appareils et d'applications :** l'exécution de la configuration suivante à l'avance vous permet de configurer les appareils et applications sans interruption.



   Consultez :

   Déployer des ressources

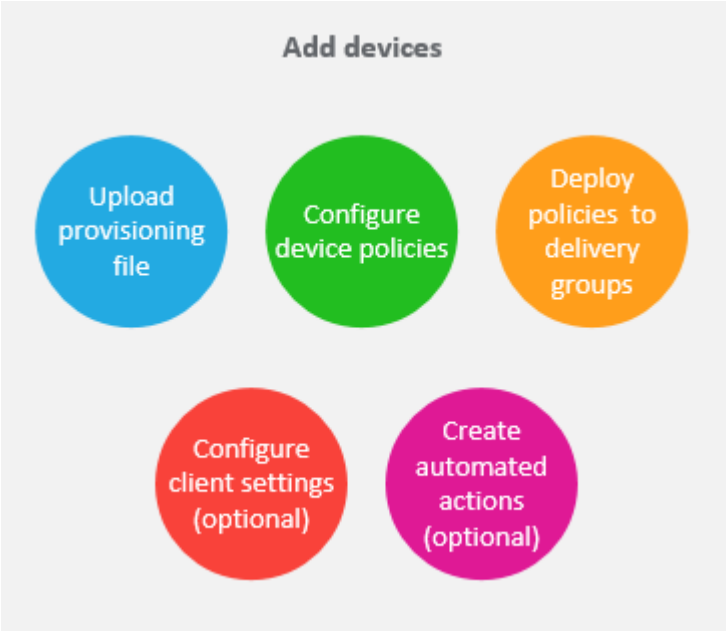
   Configurer des rôles avec RBAC

   Créer et mettre à jour des modèles de notification

   Créer et gérer des workflows

2. **Ajouter des appareils :**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Consultez :

Préparation à l'inscription d'appareils et à la mise à disposition de ressources

Stratégies d'appareil

Déployer sur des groupes de mise à disposition

Actions automatisées

3. **Préparer les invitations d'inscription :** vous pouvez envoyer des invitations d'inscription aux utilisateurs d'appareils iOS, iPadOS, macOS, Android Enterprise et d'appareils Android d'ancienne génération. Procédez comme suit si vous prévoyez d'utiliser des invitations d'inscription.

Consultez :

Configurer les modes d'inscription sécurisée

Envoyer une notification aux appareils

4. **Ajouter des applications :**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Consultez :

SDK MAM

Ajouter des applications

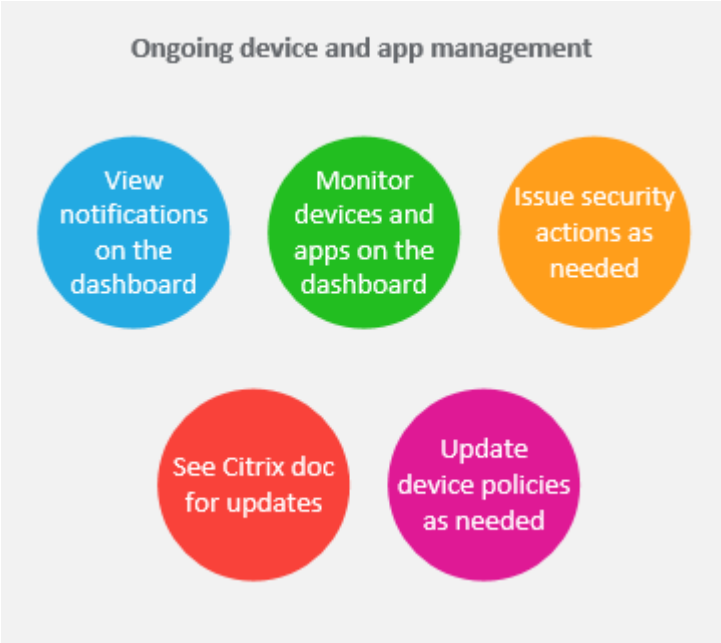
À propos des catégories d'applications

Appliquer les workflows

Déployer sur des groupes de mise à disposition

5. **Effectuer une gestion continue des appareils et des applications :** en plus d'utiliser le tableau de bord Citrix Endpoint Management, nous vous encourageons à passer en revue le contenu Nouveautés de chaque version. Les nouveautés fournissent des informations sur les actions nécessaires, telles que la configuration de nouvelles stratégies.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Consultez :

Surveillance et assistance

Rapports

Actions de sécurisation

Nouveautés

Stratégies d'appareil

Invitations d'inscription

Pour gérer les appareils utilisateur à distance et de manière sécurisée, vous devez les inscrire dans Citrix Endpoint Management. Le logiciel client Citrix Endpoint Management est installé sur l'appareil utilisateur et l'identité de l'utilisateur est authentifiée. Citrix Endpoint Management et le profil utilisateur sont installés. Pour plus d'informations sur l'inscription des plates-formes d'appareils prises en charge, consultez les articles sur les appareils de cette section.

Dans la console Citrix Endpoint Management :

- Vous pouvez envoyer une invitation d'inscription aux utilisateurs d'appareils iOS, iPadOS, macOS, Android Enterprise et d'appareils Android d'ancienne génération. Les invitations d'inscription ne sont pas disponibles pour les appareils Windows.
- Vous pouvez envoyer une URL d'invitation aux utilisateurs d'appareils iOS, iPadOS, Android Enterprise ou d'appareils Android d'ancienne génération. Les URL d'invitation ne sont pas disponibles pour les appareils Windows.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Des invitations d'inscription sont envoyées comme suit :

- Si les utilisateurs Active Directory ont une adresse e-mail dans Active Directory, ils reçoivent l'invitation. Les utilisateurs locaux reçoivent l'invitation sur l'e-mail spécifié dans les propriétés de l'utilisateur.

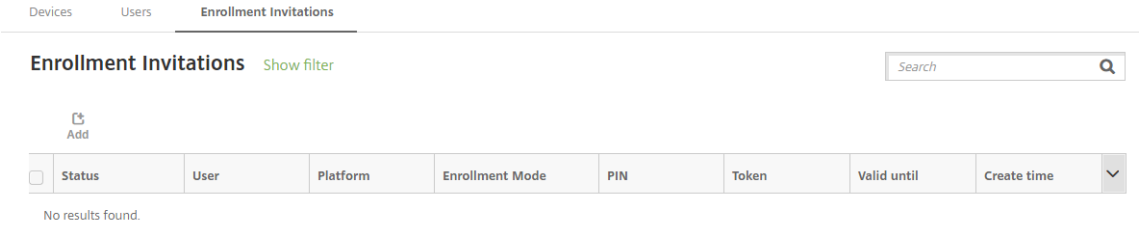
Une fois que les utilisateurs s'inscrivent, leurs appareils apparaissent en tant que gérés sous **Gérer > Appareils**. L'état de l'URL d'invitation s'affiche en tant que **Utilisée**.

Logiciels requis

- LDAP configuré
- Si vous utilisez des groupes locaux et utilisateurs locaux :
  - Un ou plusieurs groupes locaux.
  - Utilisateurs locaux attribués à des groupes locaux.
  - Des groupes de mise à disposition sont associés à des groupes locaux.
- Utilisation d'Active Directory :
  - Des groupes de mise à disposition sont associés à des groupes Active Directory.

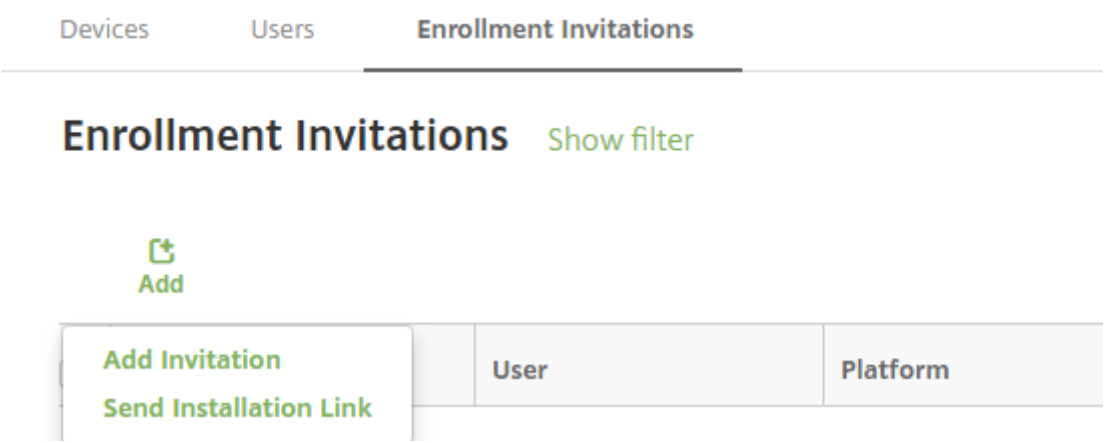
Créer une invitation d'inscription

1. Dans la console Citrix Endpoint Management, cliquez sur **Gérer > Invitations d'inscription**. La page **Invitations d'inscription** s'affiche.



2. Cliquez sur **Ajouter**. Un menu des options d'inscription s'affiche.

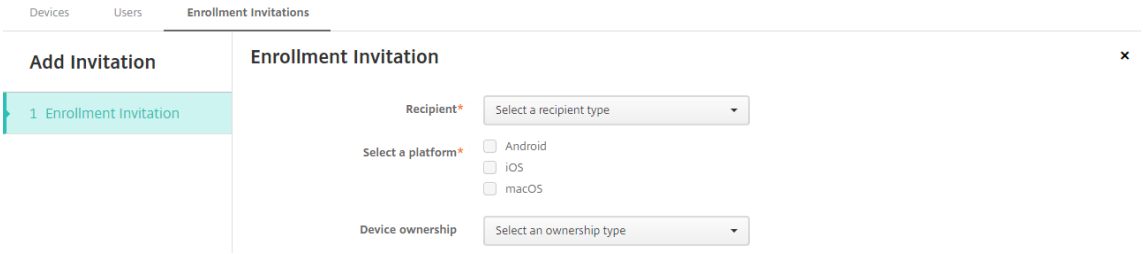
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Pour envoyer une invitation d'inscription à un utilisateur ou un groupe, cliquez sur **Ajouter une invitation**.
- Pour envoyer un lien d'installation d'inscription à une liste de destinataires via SMTP, cliquez sur **Envoyer lien d'installation**.

L'envoi d'invitations d'inscription et de liens d'installation est décrit après ces étapes.

3. Cliquez sur **Ajouter une invitation**. L'écran **Invitation d'inscription** s'affiche.



4. Pour configurer ces paramètres :

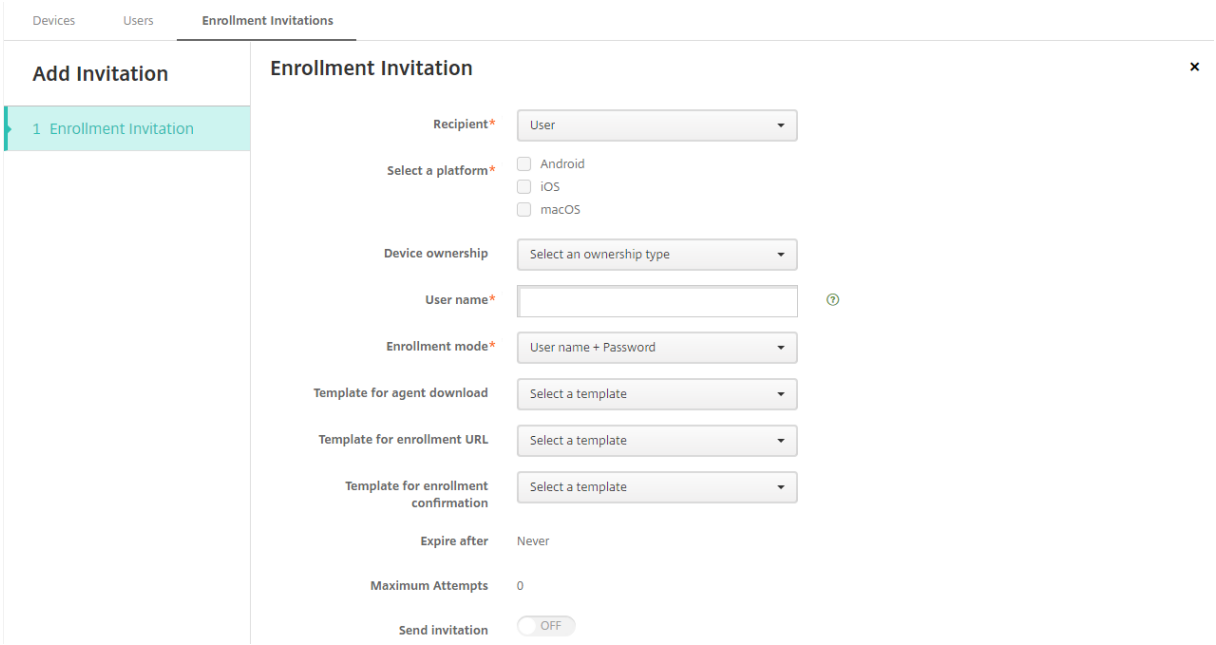
   - **Destinataire :** choisissez **Groupe** ou **Utilisateur**.
   - **Sélectionner une plate-forme :** si **Destinataire** est défini sur **Groupe**, toutes les plates-formes sont sélectionnées. Vous pouvez modifier la plate-forme sélectionnée. Si **Destinataire** est défini sur **Utilisateur**, aucune plate-forme n'est sélectionnée. Sélectionnez une plate-forme.

     Pour créer une invitation d'inscription pour les appareils Android Enterprise, sélectionnez **Android**.
   - **Propriétaire :** sélectionnez **Entreprise** ou **Employé**.

   Les paramètres pour les utilisateurs ou groupes s'affichent, comme décrit dans les sections suivantes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour envoyer une invitation d'inscription à un utilisateur



1. Configurez ces paramètres **Utilisateur** :

   - **Nom d'utilisateur :** entrez un nom d'utilisateur. L'utilisateur doit exister dans Citrix Endpoint Management en tant qu'utilisateur local ou Active Directory. Si l'utilisateur est local, configurez la propriété Email de l'utilisateur pour vous permettre de lui envoyer des notifications. S'il s'agit d'un utilisateur Active Directory, assurez-vous que LDAP est configuré.
   - **Numéro de téléphone :** ce paramètre ne s'affiche pas si vous sélectionnez plusieurs plates-formes, ou si vous sélectionnez macOS uniquement. Si vous le souhaitez, entrez le numéro de téléphone de l'utilisateur.
   - **Opérateur :** ce paramètre ne s'affiche pas si vous sélectionnez plusieurs plates-formes, ou si vous sélectionnez macOS uniquement. Choisissez un opérateur à associer au numéro de téléphone de l'utilisateur.
   - **Mode d'inscription :** choisissez le mode d'inscription sécurisée pour les utilisateurs. La valeur par défaut est **Nom d'utilisateur + mot de passe**. Certaines des options suivantes ne sont pas disponibles pour toutes les plates-formes :
     - **Nom d'utilisateur + mot de passe**
     - **URL d'invitation**
     - **URL d'invitation + PIN**
     - **URL d'invitation + mot de passe**
     - **Deux facteurs**
     - **Nom d'utilisateur + PIN**

Le mode d'inscription **Haute sécurité** n'est plus pris en charge. Pour envoyer des invitations d'

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

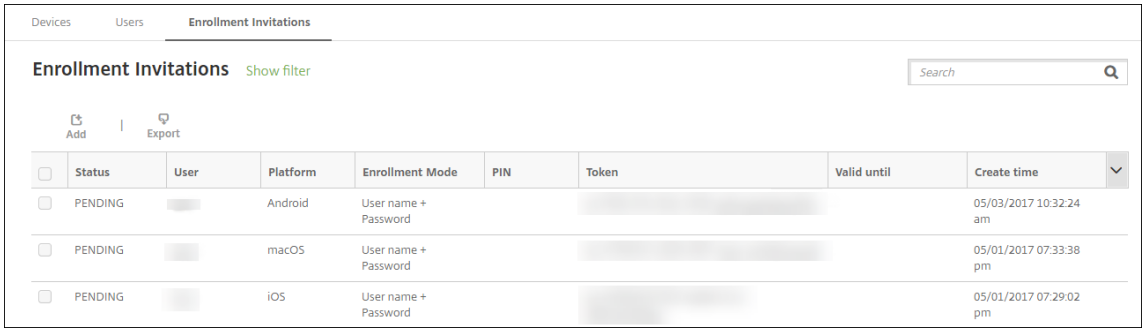
inscription, vous pouvez uniquement utiliser les modes d'inscription sécurisée **URL d'invitation**, **URL d'invitation + PIN** ou **URL d'invitation + mot de passe**. Pour les appareils qui sont inscrits avec **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + PIN**, les utilisateurs doivent télécharger Citrix Secure Hub et entrer manuellement leurs informations d'identification.

Pour de plus amples informations, consultez la section Modes d'inscription sécurisée par plateforme. Un code PIN d'inscription est également appelé un code PIN à usage unique. Ces codes PIN sont valides uniquement lorsque l'utilisateur s'inscrit.

> **Remarque :**
>
> Lorsque vous sélectionnez un mode d'inscription sécurisée qui comprend un code PIN, le champ **Modèle pour le code PIN d'inscription** s'affiche. Cliquez sur **Code PIN d'inscription**.

- **Modèle pour téléchargement de l'agent :** choisissez le modèle de lien de téléchargement appelé **Lien de téléchargement**. Ce modèle est destiné à toutes les plates-formes prises en charge.
- **Modèle pour l'URL d'inscription :** choisissez **Invitation d'inscription**.
- **Modèle pour la confirmation d'inscription :** choisissez **Confirmation d'inscription**.
- **Expire après :** ce champ est défini lorsque vous configurez le mode d'inscription sécurisée et indique quand l'inscription expire. Pour plus d'informations sur la configuration des modes d'inscription sécurisée, veuillez consulter la section Configurer les modes d'inscription sécurisée.
- **Nbre max de tentatives :** ce champ est défini lorsque vous configurez le mode d'inscription sécurisée et indique le nombre maximal de tentatives du processus d'inscription.
- **Envoyer invitation :** sélectionnez **Activé** pour envoyer l'invitation immédiatement. Sélectionnez **Désactivé** pour ajouter l'invitation au tableau sur la page **Invitations d'inscription**, mais ne pas l'envoyer.

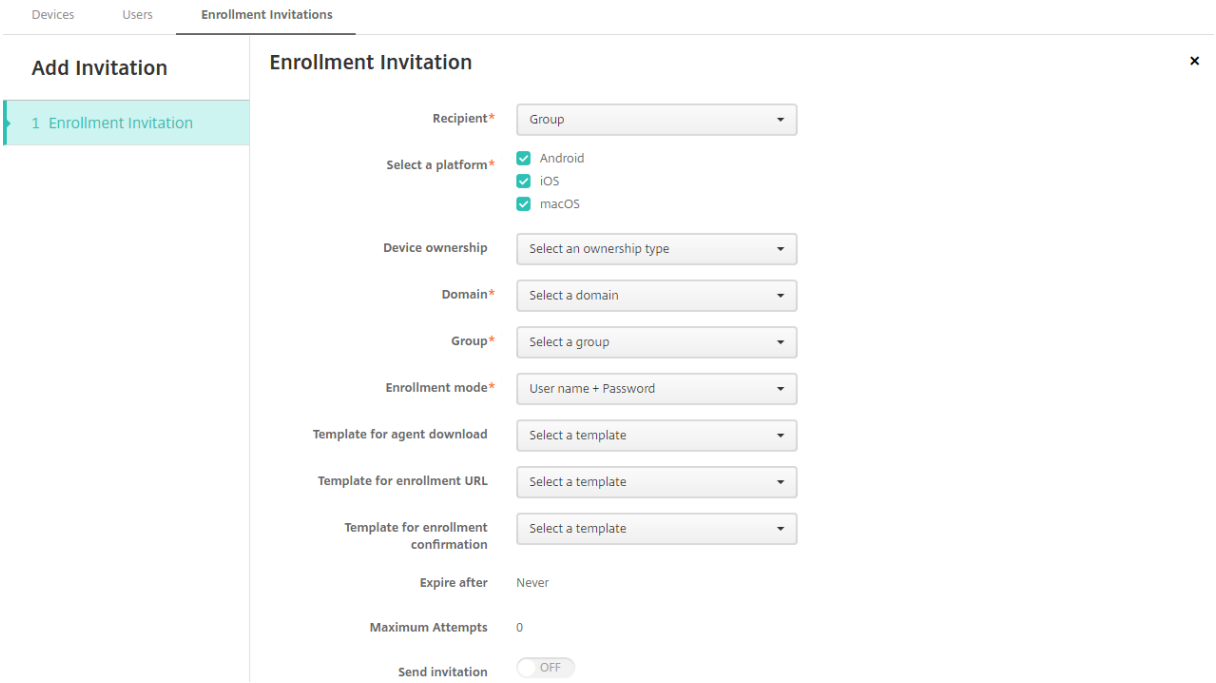
2. Cliquez sur **Enregistrer et Envoyer** si vous avez activé **Envoyer invitation**. Sinon, cliquez sur **Enregistrer**. L'invitation apparaît dans le tableau sur la page **Invitations d'inscription**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour envoyer une invitation d'inscription à un groupe

La figure suivante montre les paramètres de configuration d'une invitation d'inscription à un groupe.



1. Pour configurer ces paramètres :

   - **Domaine :** choisissez le domaine du groupe qui recevra l'invitation.
   - **Groupe :** choisissez le groupe qui recevra l'invitation. Citrix Endpoint Management obtient la liste des utilisateurs à partir d'Active Directory. Cette liste inclut les utilisateurs dont les noms contiennent des caractères spéciaux.
   - **Mode d'inscription :** choisissez la manière dont vous souhaitez que les utilisateurs du groupe s'inscrivent. La valeur par défaut est **Nom d'utilisateur + mot de passe**. Certaines des options suivantes ne sont pas disponibles pour toutes les plates-formes :
     - **Nom d'utilisateur + mot de passe**
     - **URL d'invitation**
     - **URL d'invitation + PIN**
     - **URL d'invitation + mot de passe**
     - **Deux facteurs**
     - **Nom d'utilisateur + PIN**

   Le mode d'inscription **Haute sécurité** n'est plus pris en charge. Pour envoyer des invitations d'inscription, vous pouvez uniquement utiliser les modes d'inscription sécurisée **URL d'invitation**, **URL d'invitation + PIN** ou **URL d'invitation + mot de passe**. Pour les appareils qui sont inscrits avec **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + PIN**, les

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

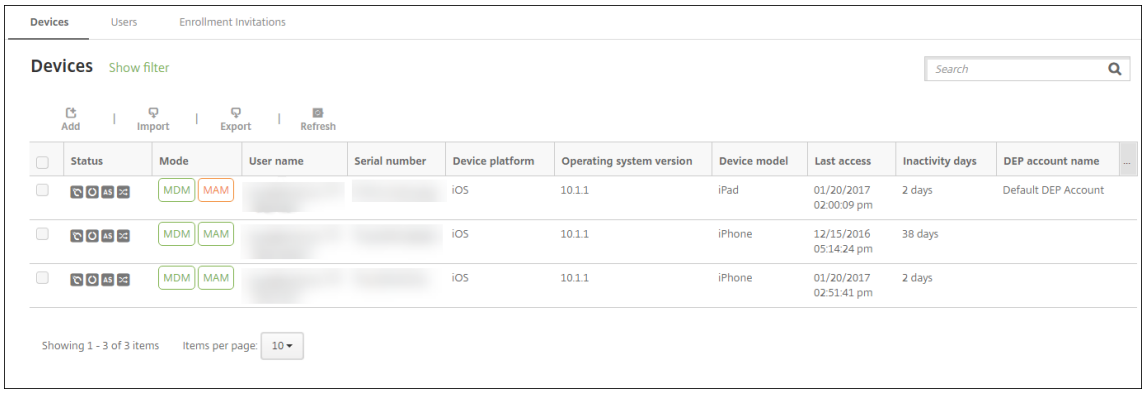
utilisateurs doivent télécharger Citrix Secure Hub et entrer manuellement leurs informations d'identification.

Seuls les mode d'inscription sécurisée qui sont valides pour chacune des plates-formes sélectionnées s'affichent. Pour de plus amples informations, consultez la section Modes d'inscription sécurisée par plate-forme.

> **Remarque :**
>
> Lorsque vous sélectionnez un mode d'inscription sécurisée qui comprend un code PIN, le champ **Modèle pour le code PIN d'inscription** s'affiche. Cliquez sur **Code PIN d'inscription**.

- **Modèle pour téléchargement de l'agent :** choisissez le modèle de lien de téléchargement appelé **Lien de téléchargement**. Ce modèle est destiné à toutes les plates-formes prises en charge.
- **Modèle pour l'URL d'inscription :** choisissez **Invitation d'inscription**.
- **Modèle pour la confirmation d'inscription :** choisissez **Confirmation d'inscription**.
- **Expire après :** ce champ est défini lorsque vous configurez le mode d'inscription sécurisée et indique quand l'inscription expire. Pour plus d'informations sur la configuration des modes d'inscription sécurisée, veuillez consulter la section Configurer les modes d'inscription sécurisée.
- **Nbre max de tentatives :** ce champ est défini lorsque vous configurez le mode d'inscription sécurisée et indique le nombre maximal de tentatives du processus d'inscription.
- **Envoyer invitation :** sélectionnez **Activé** pour envoyer l'invitation immédiatement. Sélectionnez **Désactivé** pour ajouter l'invitation au tableau sur la page **Invitations d'inscription**, mais ne pas l'envoyer.

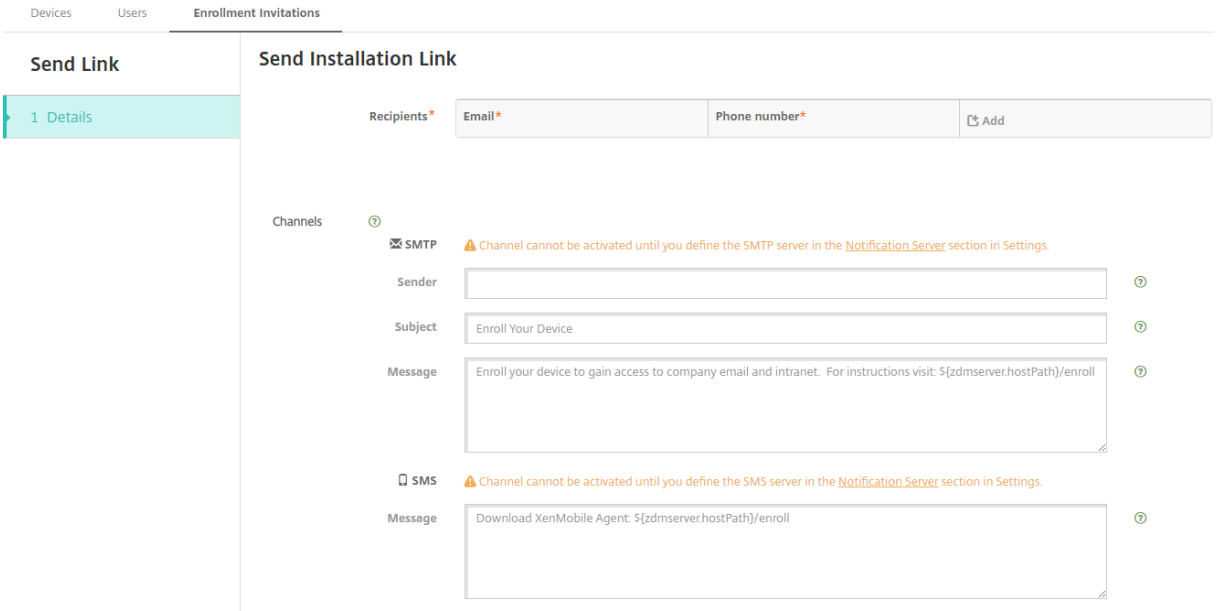
2. Cliquez sur **Enregistrer et Envoyer** si vous avez activé **Envoyer invitation**. Sinon, cliquez sur **Enregistrer**. L'invitation apparaît dans le tableau sur la page **Invitation d'inscription**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour envoyer un lien d'installation

Avant de pouvoir envoyer un lien d'installation de l'inscription, vous devez configurer les canaux (SMTP) sur le serveur de notification à partir de la page **Paramètres**. Pour plus de détails, consultez la section Notifications.



1. Configurez ces paramètres, puis cliquez sur **Enregistrer**.

   - **Destinataire :** pour chaque destinataire que vous souhaitez ajouter, cliquez sur **Ajouter** et procédez comme suit :

     - **Adresse électronique :** entrez l'adresse e-mail du destinataire. Ce champ est obligatoire.
     - **Numéro de téléphone :** entrez le numéro de téléphone de l'utilisateur. Ce champ est obligatoire.

     > **Remarque :**
     >
     > Pour supprimer un destinataire, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.
     >
     > Pour modifier un destinataire, placez le curseur sur la ligne contenant la liste. Cliquez ensuite sur l'icône de crayon sur le côté droit. Mettez la liste à jour, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

   - **Canaux :** sélectionnez un canal à utiliser pour envoyer le lien d'installation de l'inscription.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Vous pouvez envoyer des notifications via **SMTP**. Ces canaux ne peuvent pas être activés tant que vous n'avez pas configuré les paramètres du serveur sur la page **Paramètres** dans **Serveur de notification**. Pour plus de détails, consultez la section Notifications.

- **SMTP :** configurez ces paramètres facultatifs. Si vous ne renseignez pas ces champs, les valeurs par défaut spécifiées dans le modèle de notification configuré pour la plate-forme que vous avez sélectionnée sont utilisées :
  - **Expéditeur :** entrez un expéditeur (facultatif).
  - **Sujet :** entrez un sujet pour le message (facultatif). Par exemple, « inscription de votre appareil ».
  - **Message :** entrez le message à envoyer au destinataire (facultatif). Par exemple, « Inscrivez votre appareil pour accéder à la messagerie et aux applications de l'entreprise ».

2. Cliquez sur **Envoyer**.

> **Remarque :**
>
> Si votre environnement utilise l'attribut sAMAccountName : après que les utilisateurs aient reçu l'invitation et cliqué sur le lien, ils doivent modifier le nom d'utilisateur pour compléter l'authentification. Le nom d'utilisateur apparaît sous la forme de `sAMAccountName@domainname.com`. Les utilisateurs doivent supprimer la partie `@domainname.com`.

Modes d'inscription sécurisée par plateforme

Le tableau suivant affiche les modes d'inscription sécurisée que vous pouvez utiliser pour inscrire des machines utilisateur. Dans le tableau, **Oui** indique quelles plates-formes d'appareils prennent en charge des modes d'inscription et de gestion spécifiques avec différents profils d'inscription.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Mode d'inscription sécurisée MDM	Mode d'inscription sécurisée MAM sur NetScaler Gateway	Modes de gestion	Prise en charge de différents profils d'inscription	Android (ancien)	Android Enterprise	iOS (mode d'inscription des utilisateurs)	iOS	macOS	Windows
Azure AD et Okta en tant que fournisseurs d'identité via Citrix Cloud	Certificat client	MDM+MAM ou MDM	Oui	Oui	Oui	Oui	Oui	Non	Non

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Mode d'inscription sécurisée MDM	Mode d'inscription sécurisée MAM sur NetScaler Gateway	Modes de gestion	Prise en charge de différents profils d'inscription	Android (ancien)	Android Enterprise	iOS (mode d'inscription des utilisateurs)	iOS	macOS	Windows
Nom d'utilisateur + mot de passe	LDAP, LDAP + certificat client et certificat client uniquement	MDM+MAM, MDM ou MAM (le mode MAM exclusif ne prend pas en charge les certificats clients sur NetScaler Gateway)	Oui	Oui	Oui	Oui	Oui	Oui	Oui
URL d'invitation	Certificat client	MDM+MAM ou MDM	Oui	Oui	Oui	Non	Oui	Non	Non
URL d'invitation + PIN	Certificat client	MDM+MAM ou MDM	Oui	Oui	Oui	Non	Oui	Non	Non

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Mode d'inscription sécurisée MDM	Mode d'inscription sécurisée MAM sur NetScaler Gateway	Modes de gestion	Prise en charge de différents profils d'inscription	Android (ancien)	Android Enterprise	iOS (mode d'inscription des utilisateurs)	iOS	macOS	Windows
URL d'invitation + mot de passe	LDAP, LDAP + certificat client et certificat client uniquement	MDM+MAM ou MDM	Oui	Oui	Oui	Non	Oui	Non	Non
Authentification à deux facteurs (nom d'utilisateur + mot de passe + code PIN)	LDAP, LDAP + certificat client et certificat client uniquement	MDM+MAM ou MDM	Oui	Oui	Oui	Non	Oui	Oui	Non
Nom d'utilisateur + PIN	Certificat client	MDM+MAM ou MDM	Oui	Oui	Oui	Non	Oui	Oui	Non

Le comportement des modes d'inscription sécurisée sur les appareils iOS, Android et Android Enterprise est décrit ci-après :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Nom d'utilisateur + mot de passe** (défaut)
  - Envoie à un utilisateur une seule notification contenant une URL d'inscription. Lorsque l'utilisateur clique sur l'URL, Citrix Secure Hub s'ouvre. L'utilisateur tape ensuite un nom d'utilisateur et un mot de passe pour inscrire l'appareil dans Citrix Endpoint Management.
- **URL d'invitation**
  - Envoie à un utilisateur une seule notification contenant une URL d'inscription. Lorsque l'utilisateur clique sur l'URL, Citrix Secure Hub s'ouvre. Le nom du serveur Citrix Endpoint Management et le bouton **Oui, inscrire** apparaissent. L'utilisateur appuie sur **Oui, inscrire** pour inscrire l'appareil dans Citrix Endpoint Management.
- **URL d'invitation + PIN**
  - Envoie à un utilisateur les e-mails suivants :
    * Un e-mail avec une URL d'inscription, qui permet à l'utilisateur d'inscrire l'appareil dans Citrix Endpoint Management via Citrix Secure Hub.
    * Un e-mail avec un code PIN à usage unique que l'utilisateur doit entrer lors de l'inscription de l'appareil, ainsi que le mot de passe de l'utilisateur Active Directory (ou local).
  - Avec ce mode, l'utilisateur effectue l'inscription uniquement en utilisant l'URL d'inscription inclus dans la notification. Si l'utilisateur perd l'invitation de notification, il ne peut pas effectuer l'inscription. Vous pouvez, cependant, envoyer une autre invitation.
- **URL d'invitation + mot de passe**
  - Envoie à un utilisateur une seule notification contenant une URL d'inscription. Lorsque l'utilisateur clique sur l'URL, Citrix Secure Hub s'ouvre. Le nom du serveur Citrix Endpoint Management apparaît, ainsi qu'un champ permettant à l'utilisateur de taper un mot de passe.
- **Deux facteurs**
  - Envoie à un utilisateur une seule notification contenant une URL d'inscription et un code PIN unique. Lorsque l'utilisateur clique sur l'URL, Citrix Secure Hub s'ouvre. Le nom du serveur Citrix Endpoint Management apparaît, ainsi que deux champs permettant à l'utilisateur de taper un mot de passe et le PIN.
- **Nom d'utilisateur + PIN**
  - Envoie à un utilisateur les e-mails suivants :
    * Un e-mail avec une URL d'inscription, qui permet à l'utilisateur de télécharger et d'installer Citrix Secure Hub. Une fois Citrix Secure Hub ouvert, l'utilisateur est invité à taper un nom d'utilisateur et un mot de passe pour inscrire l'appareil dans Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * Un e-mail avec un code PIN à usage unique que l'utilisateur doit entrer lors de l'inscription de l'appareil, ainsi que le mot de passe de l'utilisateur Active Directory (ou local).
  - Si l'utilisateur perd l'invitation de notification, il ne peut pas effectuer l'inscription. Vous pouvez, cependant, envoyer une autre invitation.

Le comportement des modes d'inscription sécurisée sur les appareils macOS est décrit ci-après :

- **Nom d'utilisateur + mot de passe**
  - Envoie à un utilisateur une seule notification contenant une URL d'inscription. Lorsque l'utilisateur clique sur l'URL, le navigateur Safari s'ouvre. Une page de connexion apparaît, invitant l'utilisateur à taper un nom d'utilisateur et un mot de passe pour inscrire l'appareil dans Citrix Endpoint Management.
- **Deux facteurs**
  - Envoie à un utilisateur une seule notification contenant une URL d'inscription et un code PIN unique. Lorsque l'utilisateur clique sur l'URL, le navigateur Safari s'ouvre. Une page de connexion apparaît, affichant deux champs permettant à l'utilisateur de taper un mot de passe et le PIN.
- **Nom d'utilisateur + PIN**
  - Envoie à un utilisateur les e-mails suivants :
    * Un e-mail avec une URL d'inscription. Lorsque l'utilisateur clique sur l'URL, le navigateur Safari s'ouvre. Une page de connexion apparaît, invitant l'utilisateur à taper un nom d'utilisateur et un mot de passe pour inscrire l'appareil dans Citrix Endpoint Management.
    * Un e-mail avec un code PIN à usage unique que l'utilisateur doit entrer lors de l'inscription de l'appareil, ainsi que le mot de passe de l'utilisateur Active Directory (ou local).
  - Si l'utilisateur perd l'invitation de notification, il ne peut pas effectuer l'inscription. Vous pouvez, cependant, envoyer une autre invitation.

Vous ne pouvez pas envoyer d'invitations d'inscription aux appareils Windows. Les utilisateurs Windows s'inscrivent directement sur leurs appareils. Pour de plus amples informations sur l'inscription d'appareils Windows, consultez la section Appareils Windows.

Actions de sécurisation

Vous pouvez exécuter des actions de sécurité au niveau de l'application et de l'appareil à partir de la page **Gérer > Appareil**. Vous pouvez exécuter les actions suivantes sur l'appareil : révoquer, ver-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

rouiller, déverrouiller et effacer. Vous pouvez exécuter les actions de sécurité suivantes sur les applications : mode kiosque (verrouillage des applications) et effacement des applications.

- **Contourner le verrouillage d'activation :** supprime le verrouillage d'activation d'appareils iOS supervisés avant l'activation de l'appareil. Cette commande ne nécessite pas l'identifiant Apple ID ou le mot de passe personnel d'un utilisateur.
- **Mode kiosque :** refuse l'accès à toutes les applications sur un appareil. Sur Android, après un verrouillage d'application, les utilisateurs ne peuvent pas se connecter à Citrix Endpoint Management. Sur iOS, les utilisateurs peuvent se connecter, mais ils ne peuvent pas accéder aux applications.
- **Effacement des applications:** supprime le compte d'utilisateur de Citrix Secure Hub et désinscrit l'appareil. Les utilisateurs ne peuvent pas se réinscrire tant que vous n'avez pas effectué l'action **Annuler effacement des applications**.
- **Verrouillage d'activation du programme de déploiement ASM :** crée un code de contournement du verrouillage d'activation pour les appareils iOS inscrits à Apple School Manager.
- **Renouvellement de certificat :** pour les appareils iOS, macOS et Android pris en charge, l' action de sécurisation Renouvellement de certificat démarre le processus de renouvellement du certificat. Lors de la prochaine connexion d'appareils à Citrix Endpoint Management, Citrix Endpoint Management Server émet de nouveaux certificats d'appareils basés sur la nouvelle autorité de certification.
- **Effacer les restrictions :** sur les appareils iOS supervisés, cette commande permet à Citrix Endpoint Management d'effacer le mot de passe de restrictions et les paramètres de restriction configurés par l'utilisateur.
- **Activer/Désactiver le mode perdu :** place un appareil iOS supervisé en Mode perdu et envoie à l'appareil un message, un numéro de téléphone et une note de bas de page à afficher. La seconde fois que vous envoyez cette commande, l'appareil sort du mode perdu.
- **Activer le suivi :** sur les appareils Android et iOS, cette commande permet à Citrix Endpoint Management d'interroger l'emplacement d'appareils spécifiques à une fréquence que vous définissez. Pour afficher les coordonnées et l'emplacement d'un appareil sur une carte, accédez à **Gérer > Appareils**, sélectionnez un appareil, puis cliquez sur **Modifier**. Les informations sur l'appareil se trouvent dans l'onglet **Général**, sous **Sécurité**. Utilisez **Activer le suivi** pour effectuer un suivi continu de l'appareil. Citrix Secure Hub signale périodiquement l'emplacement lorsque l'appareil est en cours d'exécution.
- **Effacement complet :** efface immédiatement toutes les données et applications d'un appareil, y compris des cartes mémoire. Les appareils effacés restent dans la liste des appareils de la page **Gérer > Appareils** à des fins d'audit. Vous pouvez supprimer un appareil effacé de la liste des appareils.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Pour les appareils Android, cette demande peut également inclure l'option d'effacement de cartes mémoire.
  - Pour les appareils Android Enterprise entièrement gérés avec profil de travail (appareils COPE), vous pouvez effectuer un effacement complet après qu'un effacement des données d'entreprise aura supprimé le profil de travail.
  - Pour les appareils iOS et macOS, l'effacement se produit immédiatement, même si l'appareil est verrouillé.

    Pour les appareils iOS 11 et iPadOS 12 (version minimale) : lorsque vous confirmez l'effacement complet, vous pouvez choisir de conserver le plan de données cellulaires sur l'appareil.

    Pour les appareils iOS 11.3 (version minimale) : lorsque vous confirmez l'effacement complet, vous empêchez les appareils iOS d'effectuer une configuration de proximité. Lors de la configuration d'un nouvel appareil iOS, les utilisateurs peuvent normalement utiliser un appareil iOS déjà configuré pour configurer le leur. Vous pouvez bloquer la configuration de proximité sur les appareils qui sont gérés par Citrix Endpoint Management et qui ont été effacés.
  - Si l'utilisateur éteint l'appareil avant que le contenu de la carte mémoire soit supprimé, l'utilisateur peut toujours avoir accès aux données de l'appareil.
  - Vous pouvez annuler la demande d'effacement jusqu'à ce que la demande soit envoyée à l'appareil.

- **Localiser :** localise un appareil et signale l'emplacement de l'appareil, accompagné d'une carte, sur la page **Gérer > Appareils**, sous **Détails de l'appareil > Général**. La fonction Localiser est une action unique. Utilisez **Localiser** pour afficher l'emplacement actuel de l'appareil au moment où vous exécutez l'action. Pour effectuer un suivi continu de l'appareil sur une période donnée, utilisez **Activer le suivi**.
  - Lorsque vous appliquez cette action aux appareils Android (sauf Android Enterprise) ou aux appareils Android Enterprise (appartenant à l'entreprise ou BYOD), tenez compte du comportement suivant :
    * La fonction **Localiser** requiert que l'utilisateur donne accès à la localisation lors de l'inscription. L'utilisateur peut choisir de ne pas accorder l'autorisation de localisation. Si l'utilisateur n'accorde pas l'autorisation lors de l'inscription, Citrix Endpoint Management demande à nouveau l'autorisation de localisation lors de l'envoi de la commande **Localiser**.
  - Lorsque vous appliquez cette fonctionnalité à des appareils iOS ou Android Enterprise, tenez compte des limitations suivantes :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * Pour les appareils Android Enterprise, cette requête échoue à moins que la stratégie d'appareil Localisation n'ait défini le mode de localisation de l'appareil sur **Haute précision** ou **Économie de batterie**.
    * Pour les appareils iOS, la commande ne réussit que si les appareils sont en mode perdu MDM.

- **Verrouiller :** verrouille à distance un appareil. La fonction Verrouiller est utile si un appareil est volé et doit être verrouillé. Ensuite, Citrix Endpoint Management génère un code PIN et le configure dans l'appareil. Pour accéder à l'appareil, l'utilisateur devra entrer ce code PIN. Utilisez **Annuler le verrouillage** pour retirer le verrouillage de la console Citrix Endpoint Management.
- **Verrouiller et réinitialiser le mot de passe :** verrouille un appareil à distance et réinitialise le mot de passe.
  - Non pris en charge pour les appareils qui sont :
    * inscrits dans Android Enterprise en mode profil de travail et
    * exécutant des versions Android antérieures à Android 7.0
  - Sur les appareils inscrits dans Android Enterprise en mode Profil de travail et qui exécutent Android 7.0 ou version ultérieure :
    * Le code secret verrouille le profil de travail. L'appareil n'est pas verrouillé.
    * Si aucun code secret n'est envoyé, ou si le code envoyé ne répond pas aux exigences et que le profil de travail n'a pas de code secret, l'appareil est verrouillé.
    * Si aucun mot de passe n'est pas envoyé, ou si le mot de passe envoyé ne répond pas aux exigences, mais que le profil de travail a un mot de passe, le profil de travail est verrouillé mais l'appareil n'est pas verrouillé.
- **Notifier (sonnerie) :** émet un son sur les appareils Android.
- **Redémarrer :** redémarre les appareils Windows 10 et Windows 11. Pour les tablettes et les PC Windows, un message concernant le redémarrage en attente s'affiche. Le redémarrage s'effectue en cinq minutes.
- **Demander/Arrêter la mise en miroir AirPlay :** démarre et arrête la mise en miroir AirPlay sur les appareils iOS supervisés.
- **Redémarrer/Arrêter :** redémarre ou arrête immédiatement les appareils iOS supervisés.
- **Révoquer :** permet d'empêcher un appareil de se connecter à Citrix Endpoint Management.
- **Révoquer/Autoriser :** effectue les mêmes actions que l'effacement des données d'entreprise. Après la révocation, vous pouvez ré-autoriser l'appareil pour le réinscrire.
- **Faire sonner :** si un appareil iOS supervisé est en Mode perdu, cette option le fait sonner. L'appareil sonne jusqu'à ce qu'il soit retiré du mode perdu ou que l'utilisateur désactive le son.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Alterner clé de récupération privée :** si vous avez activé la stratégie FileVault, cette action génère une nouvelle clé de récupération privée et remplace l'ancienne clé par cette nouvelle clé. Vous pouvez annuler cette requête tant que celle-ci est toujours en attente. Pour ce faire, cliquez sur **Annuler la rotation de la clé de récupération privée**.
- **Effacer les données d'entreprise :** efface toutes les données et applications d'entreprise d'un appareil, sans toucher aux données et applications personnelles. Après une effacement sélectif, utilisez l'action **Autoriser** pour réautoriser l'appareil afin qu'un utilisateur puisse l'inscrire à nouveau. Les appareils effacés restent dans la liste des appareils de la page **Gérer > Appareils** à des fins d'audit. Vous pouvez supprimer un appareil effacé de la liste des appareils.
  - L'effacement des données d'entreprise d'un appareil Android ne déconnecte pas l'appareil de Device Manager et du réseau d'entreprise. Pour empêcher l'appareil d'accéder à Device Manager, vous devez également révoquer les certificats de l'appareil.
  - L'effacement des données d'entreprise d'un appareil Android révoque également l'appareil. Vous ne pouvez réinscrire l'appareil qu'après l'avoir réautorisé ou supprimé de la console.
  - Pour les appareils Android Enterprise entièrement gérés avec profil de travail (appareils COPE), vous pouvez effectuer un effacement complet après qu'un effacement des données d'entreprise aura supprimé le profil de travail. Vous pouvez également réinscrire l'appareil avec le même nom d'utilisateur. La réinscription de l'appareil recrée le profil de travail.
  - Pour les appareils iOS et macOS, cette commande supprime le profil installé via MDM.
  - Un effacement des données d'entreprise sur un appareil Windows supprime également le contenu du dossier de profil de tout utilisateur connecté à l'appareil à ce moment-là. Un effacement des données d'entreprise ne supprime pas les clips Web que vous mettez à la disposition des utilisateurs via une configuration. Pour supprimer les clips Web, les utilisateurs doivent désinscrire manuellement leurs appareils. Vous ne pouvez pas réinscrire un appareil dont les données d'entreprise ont été effacées.
- **Déverrouiller :** efface le code secret envoyé à l'appareil lorsqu'il a été verrouillé. Cette commande n'ouvre pas l'appareil.

Dans **Gérer > Appareils**, la page **Détails de l'appareil** dresse également la liste des propriétés de sécurité de l'appareil. Ces propriétés incluent ID fort, Verrouiller l'appareil, Contourner le verrouillage d'activation et d'autres informations relatives au type de plate-forme. Le champ **Effacement complet de l'appareil** inclut le code PIN de l'utilisateur. L'utilisateur doit entrer ce code une fois que l'appareil est effacé. Si l'utilisateur oublie le code, vous pouvez le rechercher ici.

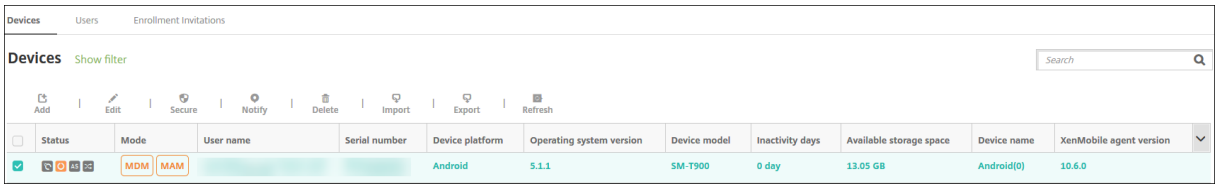
Vous pouvez automatiser certaines actions. Pour de plus amples informations, consultez la section Actions automatisées.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Supprimer un appareil de la console Citrix Endpoint Management

> **Important :**
>
> Lorsque vous supprimez un appareil de la console Citrix Endpoint Management, les applications gérées et les données restent sur l'appareil. Pour supprimer les applications gérées et les données de l'appareil, consultez la section « Supprimer un appareil » plus loin dans cet article.

Pour supprimer un appareil de la console Citrix Endpoint Management, accédez à **Gérer > Appareils**, sélectionnez un appareil géré et cliquez sur **Supprimer**.



Effacer les données d'entreprise d'un appareil

1. Accédez à **Gérer > Appareils**, sélectionnez un appareil géré et cliquez sur **Sécurisé**.
2. Dans **Actions de sécurisation**, cliquez sur **Effacer les données d'entreprise**.
3. Pour les appareils Android uniquement, déconnectez l'appareil du réseau d'entreprise : une fois que l'appareil a été effacé, dans **Actions de sécurisation**, cliquez sur **Révoquer**.

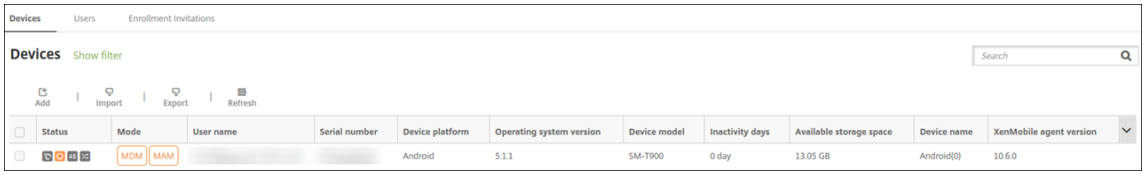
   Pour annuler une demande d'effacement des données d'entreprise avant qu'il ne soit exécuté, dans **Actions de sécurisation**, cliquez sur **Annuler l'effacement des données d'entreprise**.

Supprimer un appareil

Cette procédure supprime les applications gérées et les données de l'appareil et supprime l'appareil de la liste d'appareils dans la console Citrix Endpoint Management. Vous pouvez utiliser l'API REST publique Citrix Endpoint Management pour supprimer des appareils en bloc.

1. Accédez à **Gérer > Appareils**, sélectionnez un appareil géré et cliquez sur **Sécurisé**.
2. Cliquez sur **Effacer les données d'entreprise**. Lorsque vous y êtes invité, cliquez sur **Effacer les données d'entreprise de l'appareil**.
3. Pour vérifier que la commande d'effacement a réussi, actualisez **Gérer > Appareils**. Dans la colonne **Mode**, la couleur ambre pour MAM et MDM indique que la commande d'effacement a réussi.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Sur la page **Gérer > Appareils**, sélectionnez un appareil et cliquez sur **Supprimer**. Lorsque vous y êtes invité, cliquez de nouveau sur **Supprimer**.

Verrouiller, déverrouiller, effacer ou annuler l'effacement des applications

1. Accédez à **Gérer > Appareils**, sélectionnez un appareil géré et cliquez sur **Sécurisé**.
2. Dans **Actions de sécurisation**, cliquez sur l'action d'application.

   Vous pouvez également utiliser la boîte de dialogue **Actions de sécurisation** pour vérifier l'état de l'appareil d'un utilisateur dont le compte a été désactivé ou supprimé dans Active Directory. La présence des actions Annuler le mode kiosque ou Annuler effacement des applications indique que les applications sont verrouillées ou effacées.

Effacement et annuler effacement de l'application

1. Accédez à **Gérer > Appareils**. Sélectionnez un appareil.
2. Effacement des applications
   - Cliquez sur **Sécuriser > Effacement des applications**. Une boîte de dialogue contenant le message suivant s'affiche : **Êtes-vous sûr de vouloir effacer les applications sur cet appareil ?** Cliquez sur **Effacement des applications**.
3. Annuler effacement des applications
   - Cliquez sur **Sécuriser > Annuler effacement des applications**. Une boîte de dialogue contenant le message suivant s'affiche : **Êtes-vous sûr de vouloir annuler l'effacement des applications sur cet appareil ?** Cliquez sur **Annuler l'effacement des applications sur l'appareil**.
4. Réinscrivez l'appareil en tant que même utilisateur, dans le même mode.
5. Lancez une application MDX depuis la page **Mes applications**.
6. Lancez Citrix Secure Hub.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

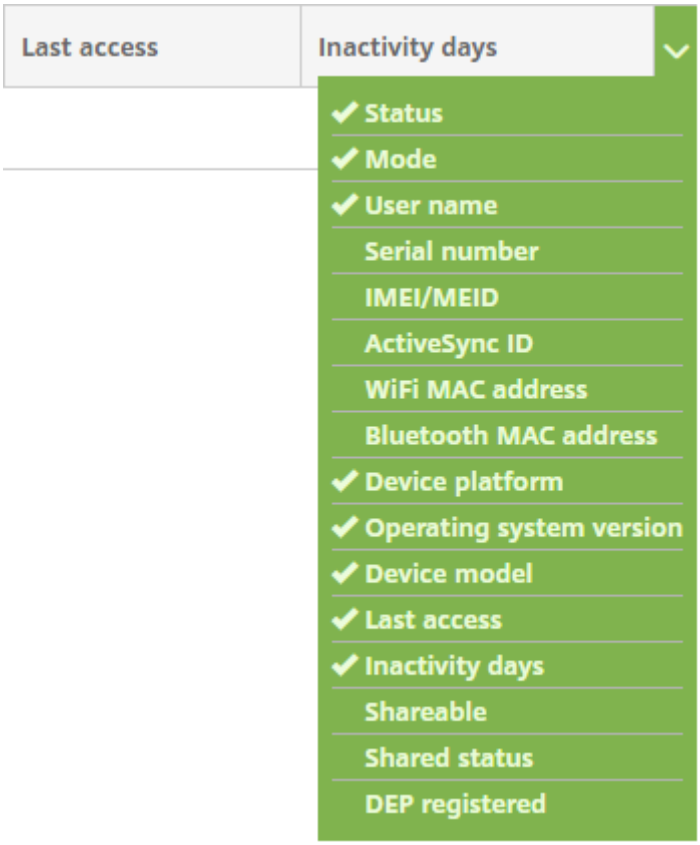
Obtenir des informations sur les appareils

La base de données d'Citrix Endpoint Management stocke une liste des appareils mobiles. Pour renseigner la console Citrix Endpoint Management avec vos appareils, vous pouvez ajouter les appareils manuellement ou importer une liste d'appareils à partir d'un fichier. Consultez la section Formats des fichiers de provisioning pour de plus amples informations sur les formats de fichier de provisioning.

La page **Gérer > Appareils** de la console Citrix Endpoint Management répertorie chaque appareil et les informations suivantes :

- **État :** les icônes indiquent si l'appareil est jailbreaké, géré, si ActiveSync Gateway est disponible et l'état du déploiement.
- **Mode :** indique le mode d'appareil, tel que MDM ou MDM+MAM.
- D'autres informations sur l'appareil : **Nom d'utilisateur**, **Plate-forme de l'appareil**, **Dernier accès** et **Jours d'inactivité**. Ces en-têtes sont les en-têtes par défaut affichés.

Pour personnaliser le tableau **Appareils**, cliquez sur la flèche vers le bas sur le dernier en-tête. Ensuite, sélectionnez les en-têtes supplémentaires que vous voulez voir dans le tableau ou désactivez les en-têtes à supprimer.



Vous pouvez ajouter des appareils manuellement, importer des appareils à partir d'un fichier de provisioning, modifier les détails de l'appareil, personnaliser les propriétés utilisateur Active Directory,

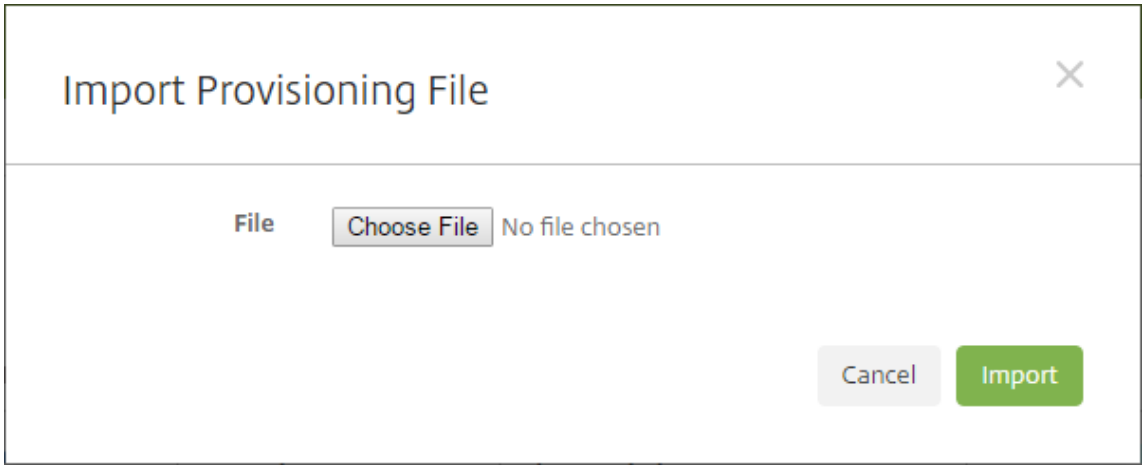
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

exécuter des actions de sécurité et envoyer des notifications aux appareils. Vous pouvez également exporter toutes les données de tableau d'un appareil dans un fichier .csv pour créer un rapport personnalisé. Le serveur exporte tous les attributs de l'appareil. Si vous appliquez des filtres, Citrix Endpoint Management les utilise lors de la création du fichier .csv.

Importer des appareils à partir d'un fichier de provisioning

Vous pouvez importer un fichier fourni par les opérateurs mobiles ou les fabricants de l'appareil, ou vous pouvez créer votre propre fichier de provisioning. Pour plus d'informations, consultez la section Formats des fichiers de provisioning dans cet article.

1. Accédez à **Gérer > Appareils** et cliquez sur **Importer**. La boîte de dialogue **Importer le fichier de provisioning** apparaît.

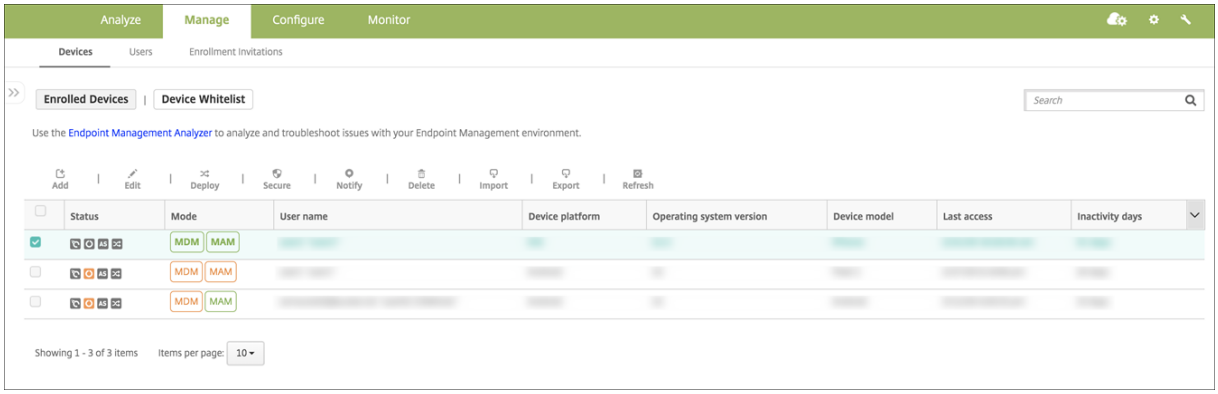


2. Cliquez sur **Choisir un fichier** et accédez au fichier que vous souhaitez importer.
3. Cliquez sur **Importer**. Le tableau **Appareils** répertorie le fichier importé.
4. Pour modifier les informations sur l'appareil, sélectionnez-le, puis cliquez sur **Modifier**. Pour plus d'informations sur les pages **Détails de l'appareil**, consultez la section Obtenir des informations sur les appareils.

Déployer vers un appareil

Vous pouvez forcer un ou plusieurs appareils à se connecter avec Citrix Endpoint Management. Les appareils sélectionnés reçoivent immédiatement des ressources sans attendre la prochaine vérification planifiée.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



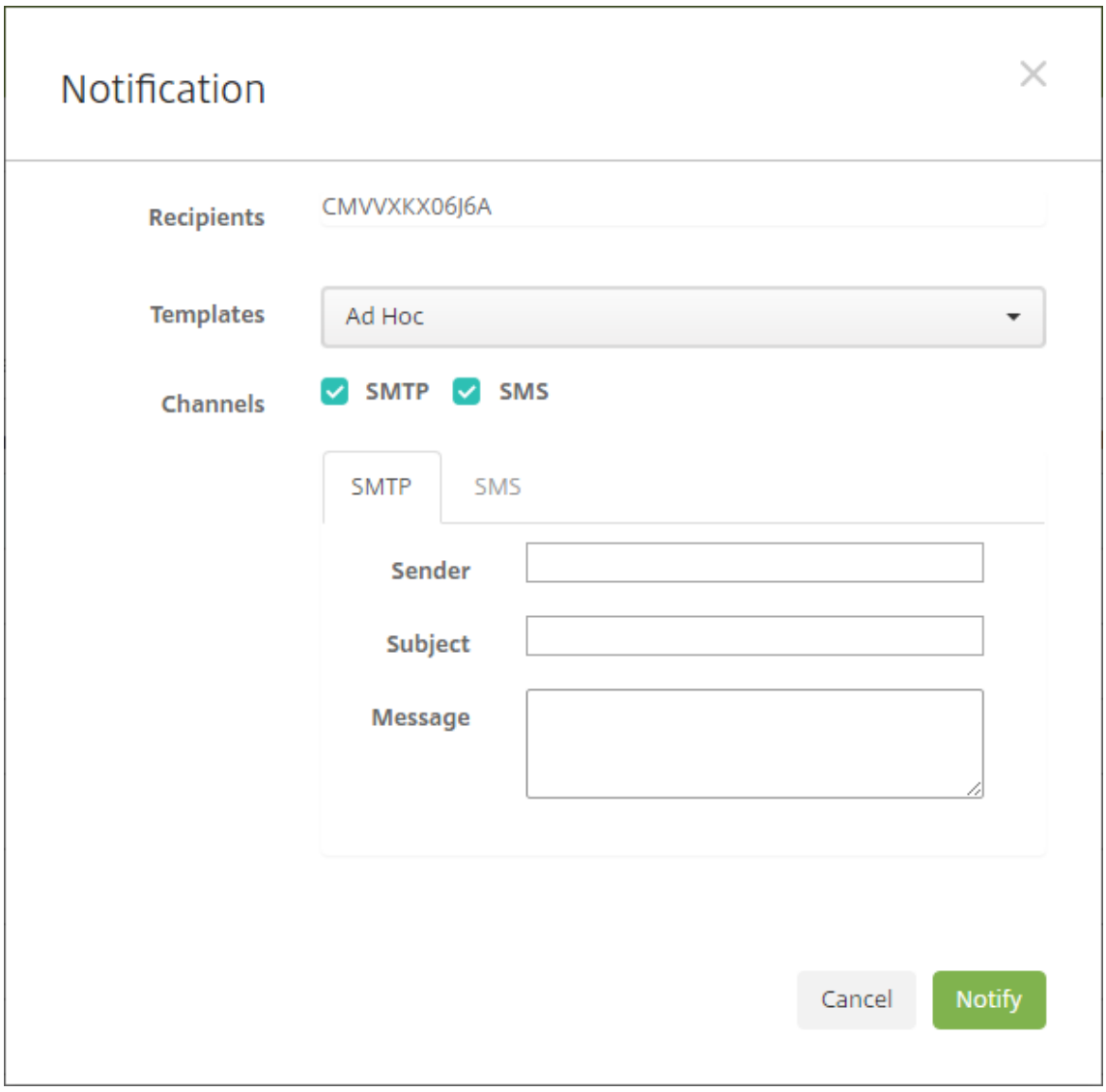
1. Accédez à **Gérer > Appareils**, sélectionnez un appareil géré MDM ou MDM+MAM, puis cliquez sur **Déployer**.
2. Dans la boîte de dialogue, cliquez sur **Déployer** pour confirmer votre action.

Envoyer une notification aux appareils

Vous pouvez envoyer des notifications aux appareils à partir de la page Appareils. Pour plus d'informations sur les notifications, veuillez consulter la section Notifications.

1. Sur la page **Gérer > Appareils** sélectionnez l'appareil ou les appareils auxquels vous souhaitez envoyer une notification.
2. Cliquez sur **Notifier**. La boîte de dialogue **Notification** s'affiche. Le champ **Destinataires** répertorie tous les appareils sélectionnés pour recevoir pour la notification.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Pour configurer ces paramètres :

   - **Modèles :** cliquez sur le type de notification que vous souhaitez envoyer dans la liste déroulante. Pour chaque modèle excepté le modèle **Ad Hoc**, les champs **Sujet** et **Message** sont renseignés avec le texte configuré pour le modèle que vous avez choisi.
   - **Canaux :** sélectionnez la méthode à utiliser pour envoyer le message. La valeur par défaut est **SMTP**. Cliquez sur les onglets pour afficher le format du message pour chaque canal.
   - **Expéditeur :** entrez un expéditeur (facultatif).
   - **Sujet :** entrez un sujet pour un message **ad hoc**.
   - **Message :** entrez le message pour un message **ad hoc**.

4. Cliquez sur **Notifier**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exporter le tableau Appareils

1. Filtrez le tableau **Appareil** en fonction de ce que vous souhaitez voir apparaître dans le fichier d'exportation.
2. Cliquez sur le bouton **Exporter** au-dessus du tableau **Appareils**. Citrix Endpoint Management extrait les informations du tableau **Appareils** filtré et les convertit en fichier .csv.
3. Ouvrez ou enregistrez le fichier .csv lorsque vous y êtes invité.

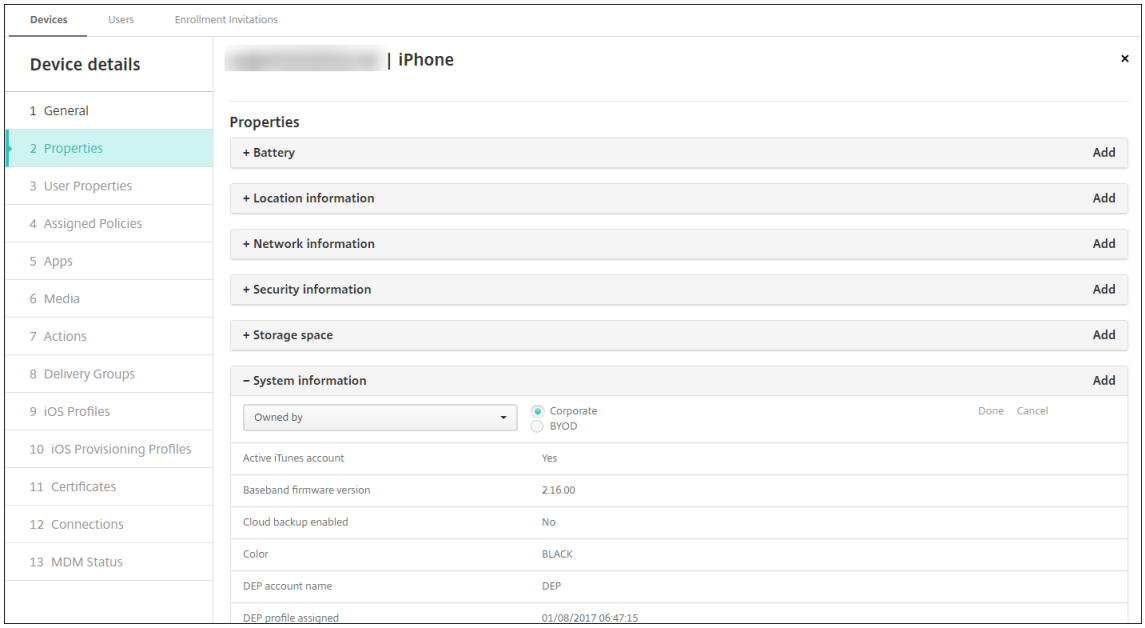
Identifier les appareils utilisateur manuellement

Vous pouvez manuellement identifier un appareil dans Citrix Endpoint Management de l'une des façons suivantes :

- Durant le processus d'inscription basé sur invitation
- Durant le processus d'inscription via le portail en libre-service
- En ajoutant le propriétaire de l'appareil en tant que propriété d'appareil

Vous avez la possibilité d'identifier l'appareil comme appartenant à la société ou à un employé. Lors de l'utilisation de l'aide du portail d'aide en libre-service pour inscrire un appareil, vous pouvez identifier l'appareil comme appartenant à la société ou à un employé. Vous pouvez également identifier un appareil manuellement, comme suit.

1. Ajoutez une propriété à l'appareil à partir de l'onglet **Appareils** dans la console Citrix Endpoint Management.
2. Ajoutez la propriété appelée **Appartient à** et choisissez **Entreprise** ou **BYOD** (appartenant à un employé).



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Personnaliser les attributs utilisateur Active Directory

Vous pouvez personnaliser certains attributs utilisateur Active Directory pour définir les attributs auxquels Citrix Endpoint Management peut accéder pour créer un compte utilisateur.

Pour afficher la liste des attributs, ajoutez la propriété serveur `optional.user.identity.attributes` en tant que clé personnalisée dans **Paramètres > Propriétés du serveur**. Dans le champ **Valeurs**, vous pouvez supprimer et restaurer ultérieurement les attributs utilisateur Active Directory facultatifs que Citrix Endpoint Management fournit par défaut. Pour plus d'informations, consultez Propriétés du serveur.

Après avoir modifié la liste des valeurs par défaut et enregistré les modifications, vous pouvez afficher les attributs utilisateur Active Directory mis à jour dans **Gérer > Appareils > Propriétés utilisateur**. Citrix Endpoint Management met à jour la console après que l'utilisateur se connecte à l'appareil ou lors de l'enregistrement planifié suivant. Si vous faites une erreur d'orthographe ou ajoutez une valeur qui n'est pas prise en charge, Citrix Endpoint Management ignore vos modifications.

La suppression des attributs utilisateur Active Directory facultatifs peut affecter les fonctionnalités suivantes :

- **Provisioning du compte utilisateur :** si vous supprimez les valeurs de prénom et de nom, Citrix Endpoint Management ne peut pas provisionner le compte utilisateur pour ShareFile et Salesforce.
- **Invitations d'inscription :** si vous supprimez les informations d'e-mail ou de téléphone mobile de l'utilisateur, l'utilisateur ne peut pas recevoir d'invitation d'inscription.
- **Actions de notification d'appareil :** si vous supprimez les détails de l'e-mail de l'utilisateur, l'utilisateur ne peut pas recevoir les notifications via SMTP.
- **Authentification unique à Citrix Secure Mail :** si vous supprimez la valeur du nom d'affichage, l'utilisateur ne peut pas se connecter à Citrix Secure Mail à l'aide de l'authentification unique (single sign-on).
- **Propriété utilisateur et règles de déploiement :** si vous supprimez l'un des attributs facultatifs que vous utilisez pour configurer la propriété utilisateur et les règles de déploiement, vous pouvez affecter les configurations existantes.
- **Actions :** si vous supprimez l'un des attributs facultatifs que vous utilisez pour définir une action automatisée dans **Configurer > Actions**, vous pouvez affecter les configurations existantes.
- **Rapports personnalisés :** si vous supprimez l'un des attributs facultatifs que vous utilisez dans les rapports personnalisés, vous pouvez affecter les configurations existantes.

Rechercher des appareils

Pour une recherche plus rapide, la portée de recherche par défaut inclut les propriétés d'appareil suivantes :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Numéro de série
- IMEI
- Adresse MAC Wi-Fi
- Adresse MAC Bluetooth
- ID Active Sync
- Nom d'utilisateur

Vous pouvez configurer la portée de recherche via une nouvelle propriété de serveur **include.device.properties.during.search**, qui est définie par défaut sur **false**. Pour inclure toutes les propriétés d'appareil dans une recherche d'appareil, accédez à **Paramètres > Propriétés du serveur** et définissez le paramètre sur **true**.

Formats des fichiers de provisioning

De nombreux opérateurs mobiles ou fournisseurs d'appareils fournissent des listes d'appareils mobiles autorisés. Vous pouvez utiliser ces listes pour éviter d'avoir à entrer manuellement une longue liste d'appareils mobiles. Citrix Endpoint Management prend en charge un format de fichier d'importation commun à ces types d'appareils pris en charge : Android, iOS et Windows.

Un fichier de provisioning que vous créez manuellement doit être au format suivant :

```
SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;
propertyName2;propertyValue2; ... propertyNameN;propertyValueN
```

Gardez à l'esprit les considérations suivantes :

- Pour connaître les valeurs valides pour chaque propriété, consultez le PDF Valeurs et noms des propriétés d'appareil.
- Utilisez le jeu de caractères UTF-8.
- Utilisez un point-virgule (;) pour séparer les champs dans le fichier de provisioning. Si une partie d'un champ contient un point-virgule, elle doit être précédée d'une barre oblique inverse (\).

  Par exemple, pour cette propriété :

  ```
  propertyV;test;1;2
  ```

  utilisez une barre oblique inverse comme caractère d'échappement :

  ```
  propertyV\;test\;1\;2
  ```
- Le numéro de série est requis pour les appareils iOS car le numéro de série est l'identifiant de l'appareil iOS.
- Pour les autres plates-formes, vous devez inclure le numéro de série ou le numéro IMEI.
- Les valeurs valides pour **OperatingSystemFamily** sont **WINDOWS**, **ANDROID** ou **iOS**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exemple de fichier de provisioning d'appareil

```
`1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;
   propertyV\;test\;1\;2;prop 2
2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;
   propertyV$*&&éééétest
3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;
4050BF3F5173010816100655105903 93;;iOS;test;
;55244201625379903;ANDROID;test.testé;value;`
```

Chaque ligne du fichier décrit un appareil. La première entrée dans cet exemple signifie :

- SerialNumber: `1050BF3F5173010816100655105903 91`
- IMEI: `15244201625379901`
- OperatingSystemFamily: `WINDOWS`
- PropertyName: `propertyN`
- PropertyValue: `propertyV\;test\;1\;2;prop 2`

Alexa for Business

November 29, 2023

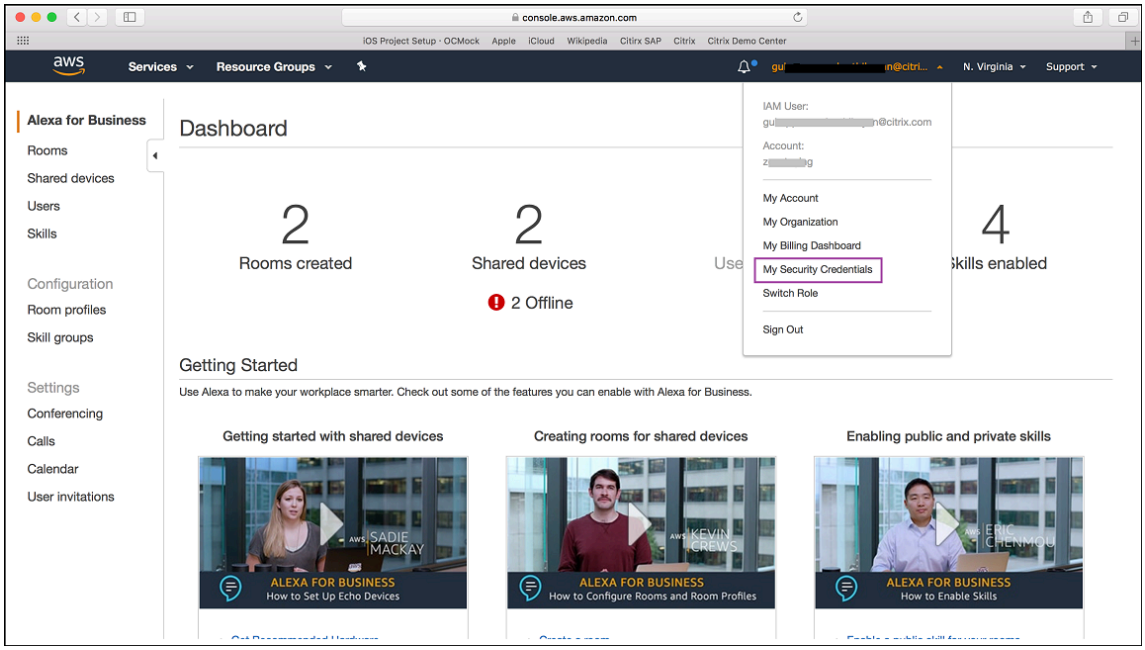
Le service Alexa for Business d'Amazon Web Services (AWS) vous permet de gérer un grand nombre d'appareils compatibles Alexa pour des utilisations professionnelles, telles que l'assistance dans les salles de conférence. Citrix Endpoint Management vous permet de configurer et de gérer ces appareils dans la console Citrix Endpoint Management. Citrix Endpoint Management ne déploie pas de stratégies directement sur les appareils Alexa. Au lieu de cela, Citrix Endpoint Management met à jour les services AWS et AWS fournit les configurations aux appareils Alexa.

Pour plus d'informations sur l'utilisation d'Alexa for Business, consultez le Guide d'administration d'Alexa for Business.

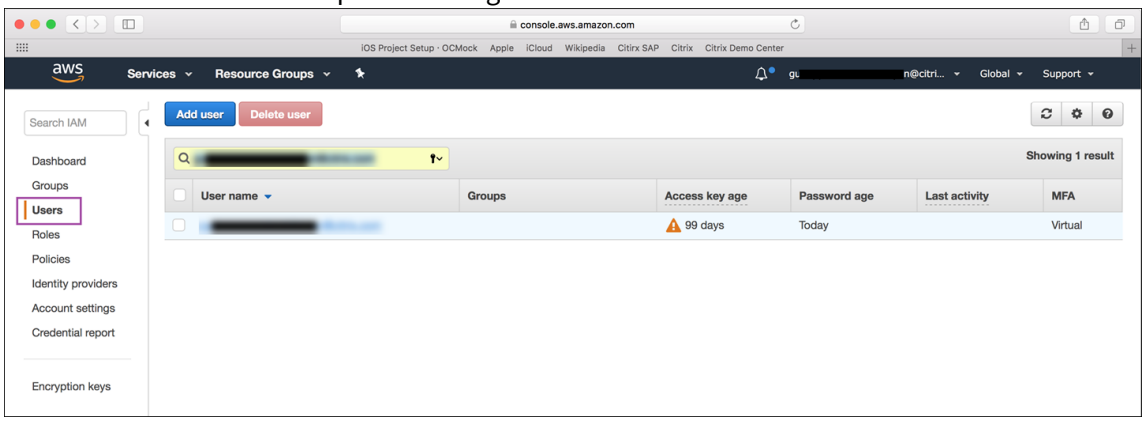
Authentifier votre compte AWS dans Citrix Endpoint Management

1. Pour obtenir vos informations d'identification de compte AWS, connectez-vous à la console AWS et sélectionnez **My Security Credentials** dans le menu utilisateur.

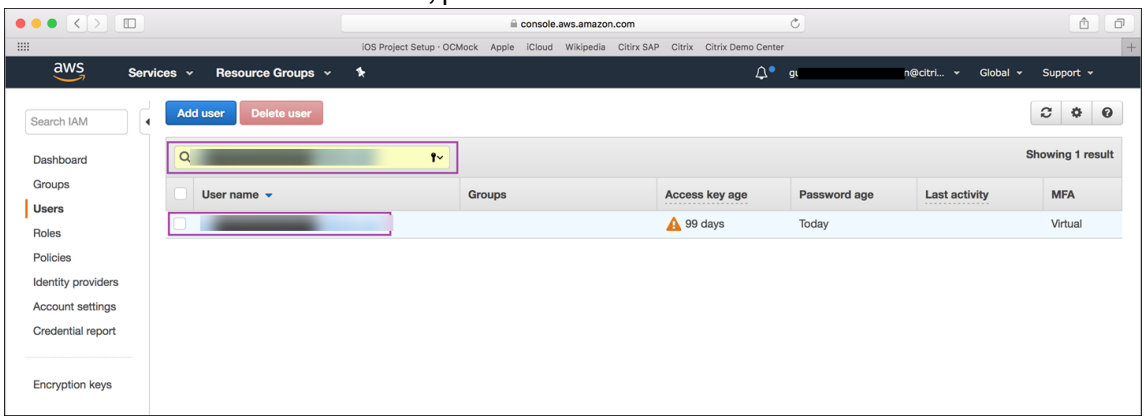
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Sélectionnez **Users** dans le panneau de gauche.

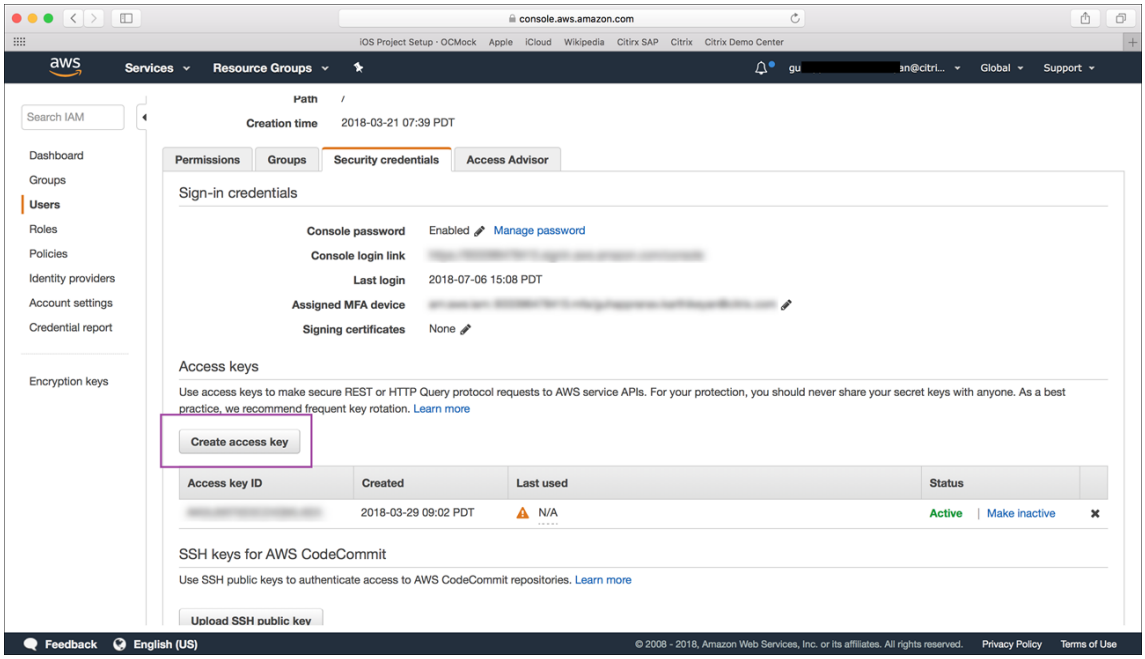


3. Recherchez votre nom d'utilisateur, puis sélectionnez-le.

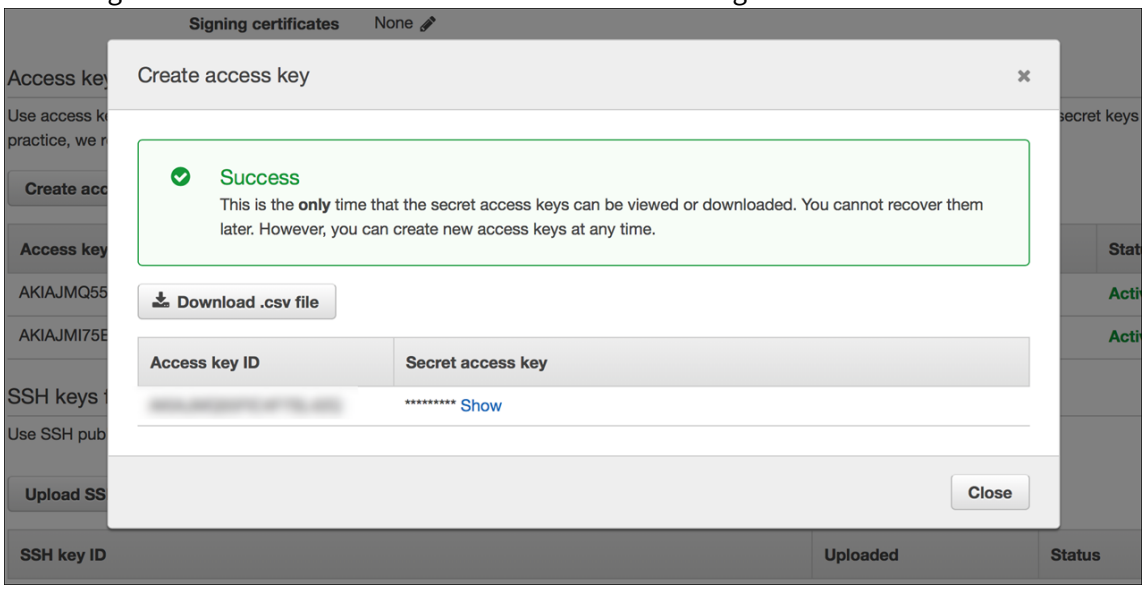


4. Dans l'onglet **Security Credentials**, cliquez sur **Create access key** pour générer votre ID de clé d'accès et votre clé d'accès secrète.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



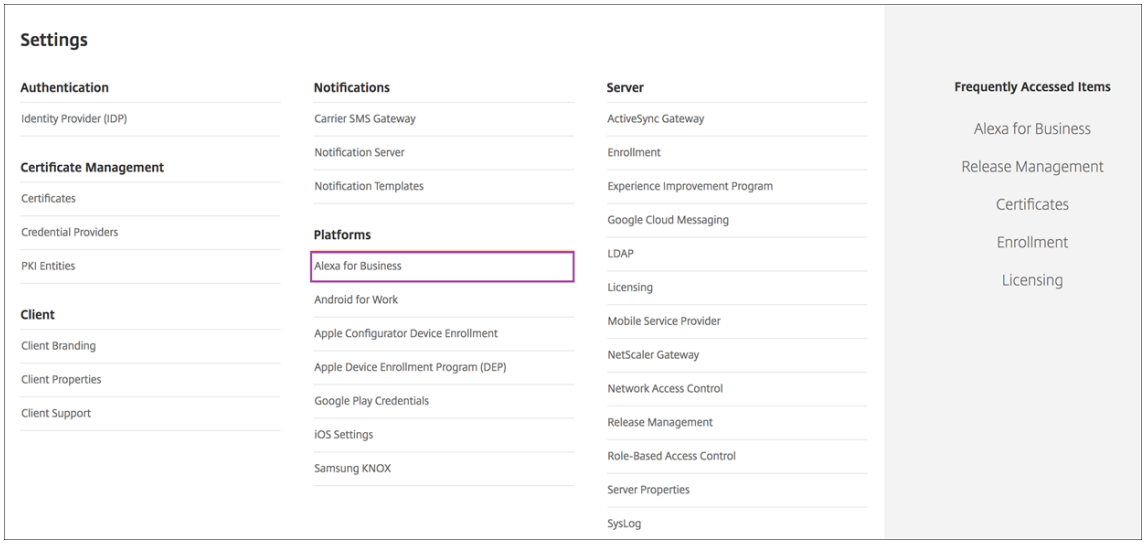
5. Téléchargez l'ID de clé d'accès et la clé d'accès secrète. Enregistrez-les ou notez-les.



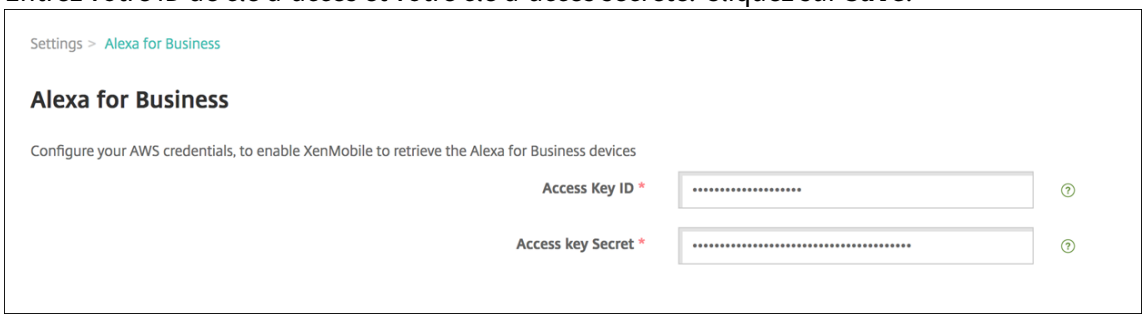
6. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage pour accéder à **Paramètres**.

7. Sous **Plates-formes**, sélectionnez **Alexa for Business**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. Entrez votre ID de clé d'accès et votre clé d'accès secrète. Cliquez sur **Save**.



Configurer Alexa for Business sur Citrix Endpoint Management

Citrix Endpoint Management vous permet de configurer ce qui suit :

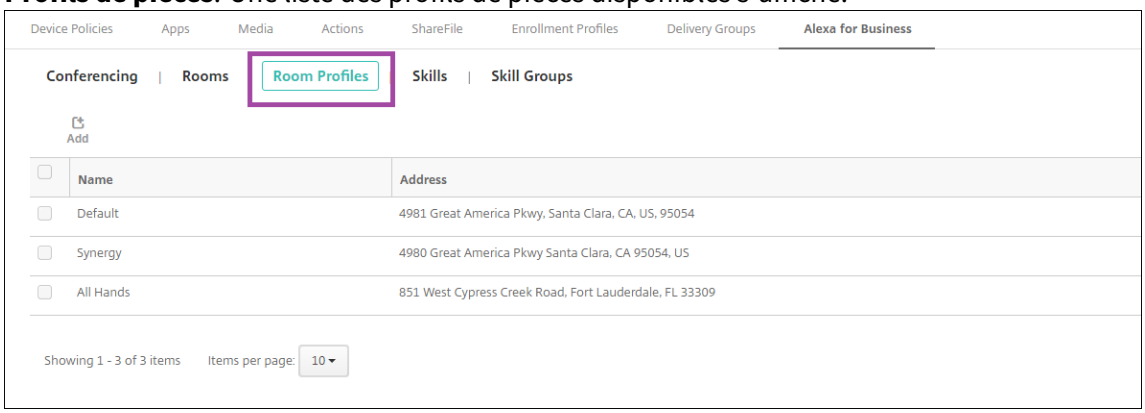
- Profils de pièces avec paramètres que vous appliquez aux pièces contenant des appareils Alexa
- Pièces représentant les pièces physiques contenant les appareils
- Groupes de Skills que vous attribuez aux pièces ou aux appareils
- Skills Alexa de la boutique Skills Alexa pouvant être ajoutées aux groupes de Skills
- Fonctionnalités de conférence qui vous permettent de choisir un fournisseur de service de téléconférence et de contrôler la façon dont les personnes planifient et rejoignent des réunions dans vos pièces

Configurer des profils de pièces

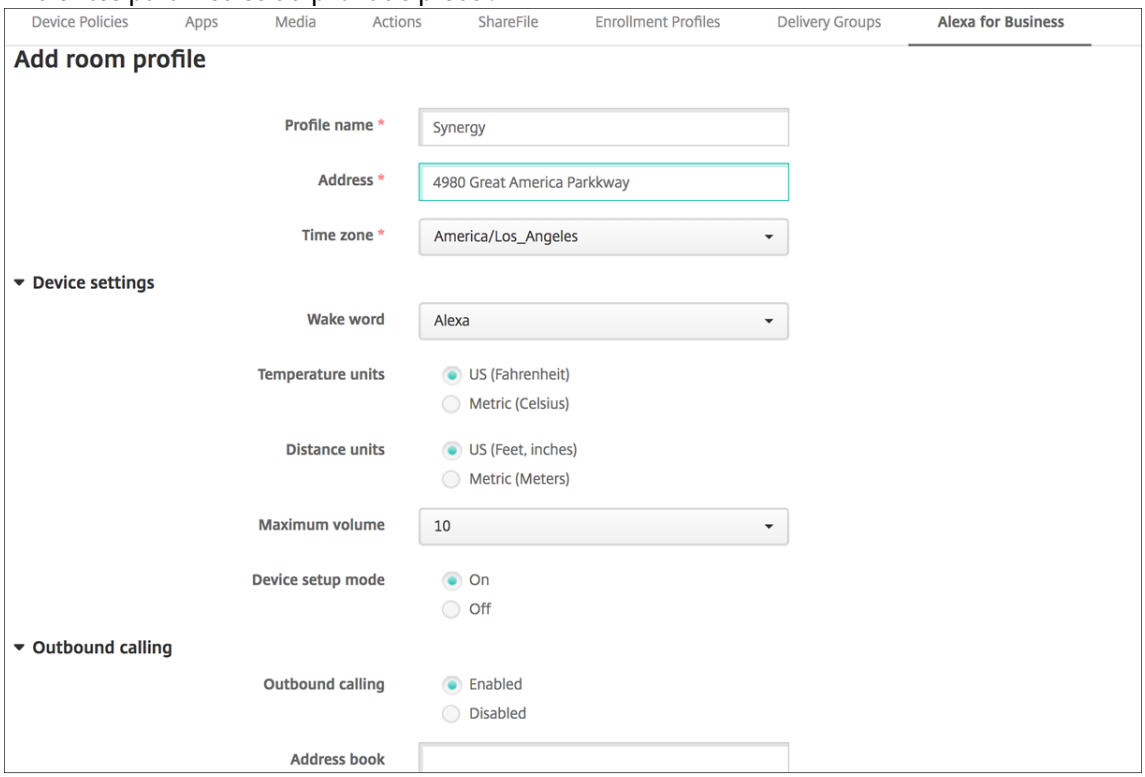
Un profil de pièce est un ensemble de configurations communes pouvant être appliquées à un ensemble de pièces contenant des appareils Alexa. Vous pouvez ajouter, modifier et supprimer des profils de pièces.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Dans la console Citrix Endpoint Management, sélectionnez **Configurer > Alexa for Business > Profils de pièces**. Une liste des profils de pièces disponibles s'affiche.



2. Pour ajouter un profil de pièce, cliquez sur **Ajouter**. Pour modifier un profil de pièce, sélectionnez le profil à modifier, puis cliquez sur **Modifier**.
3. Entrez les paramètres du profil de pièce :



- **Nom du profil :** tapez le nom du profil.
- **Address:** saisissez l'adresse physique (rue) du bâtiment où se trouvent les pièces contenant des appareils Alexa.
- **Time zone :** choisissez le fuseau horaire du lieu.
- **Mot de réveil :** choisissez le mot d'éveil auquel les appareils Alexa répondent.
- **Temperature units :** sélectionnez les unités dans lesquelles les appareils Alexa indiquent la température.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

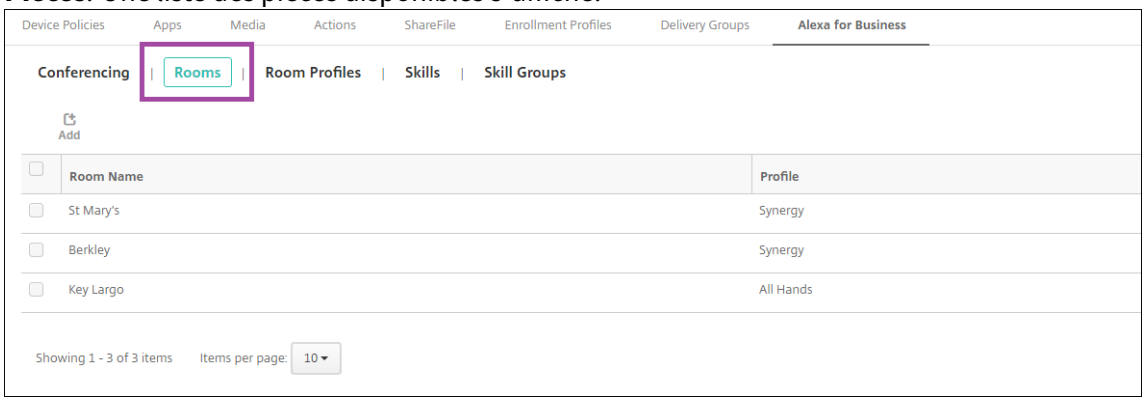
- **Unités de distance :** sélectionnez les unités dans lesquelles les appareils Alexa indiquent la distance.
- **Volume maximum :** choisissez le réglage de volume maximum pour Alexa.
- **Device setup mode :** indiquez si les appareils Alexa peuvent être reconfigurés en les forçant à accéder au mode de configuration de l'appareil.
- **Appel sortant :** activez ou désactivez la fonction d'appel sortant des appareils Alexa.
- **Address book :** définissez la configuration du carnet d'adresses pour les appareils Alexa.

4. Cliquez sur **Save**.

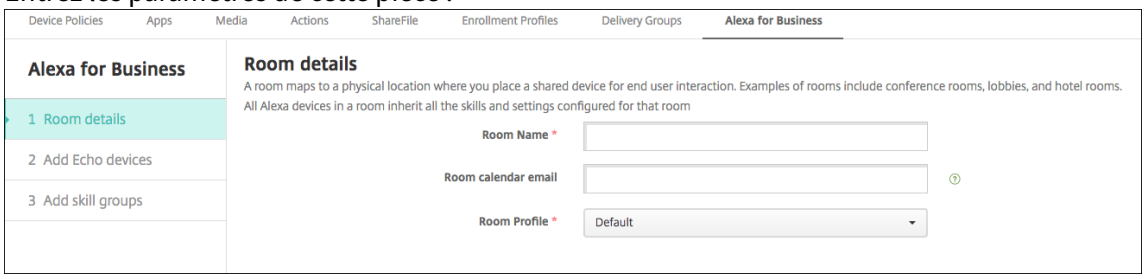
Configurer des pièces

Les pièces que vous configurez dans la console Citrix Endpoint Management représentent les salles de conférence physiques, les salles de réunion et les autres pièces du bâtiment. Lors de la configuration d'une pièce, vous associez un appareil Alexa à la pièce et ajoutez un groupe de Skills à l'appareil. Vous pouvez ajouter, modifier et supprimer des pièces.

1. Dans la console Citrix Endpoint Management, sélectionnez **Configurer > Alexa for Business > Pièces**. Une liste des pièces disponibles s'affiche.



2. Pour ajouter une pièce, cliquez sur **Ajouter**. Pour modifier une pièce, sélectionnez la pièce à modifier, puis cliquez sur **Modifier**.
3. Entrez les paramètres de cette pièce :

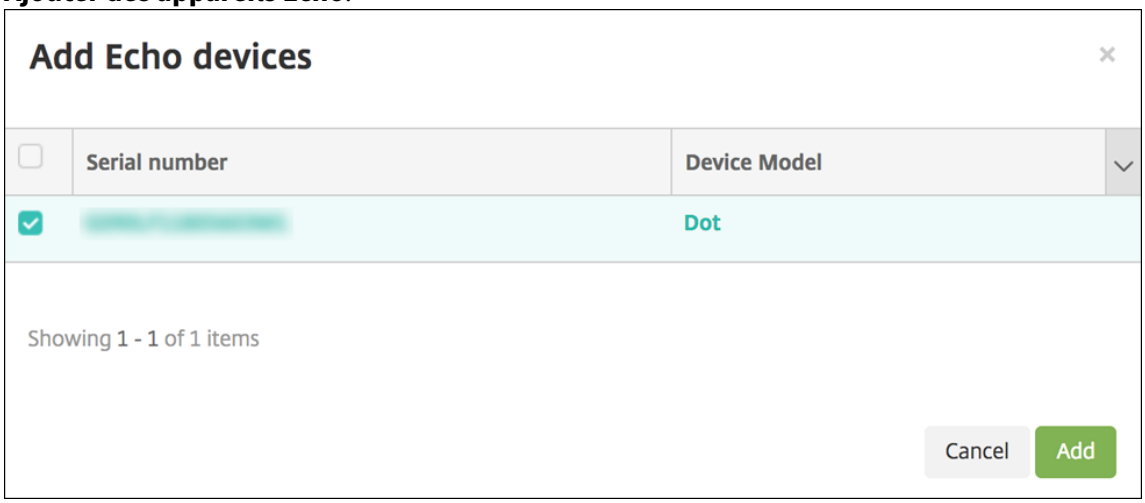


- **Nom de la pièce :** saisissez le nom de la salle de conférence, de la salle de réunion ou de toute autre pièce.

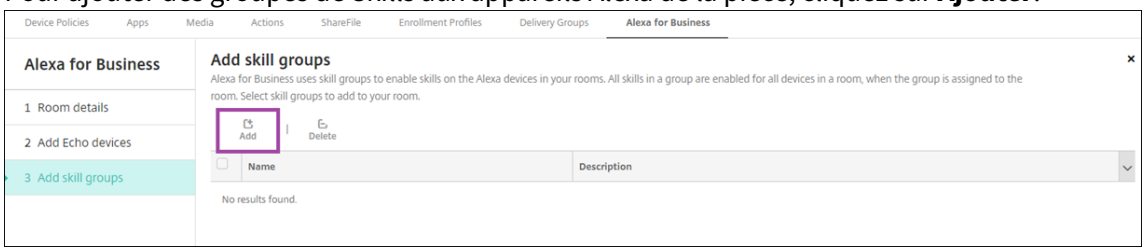
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Adresse e-mail du calendrier de la pièce :** saisissez l'adresse électronique du calendrier de la pièce.
- **Profil de pièce :** choisissez le nom de la configuration du profil de la pièce.

4. Cliquez sur **Suivant**.
5. Pour associer un appareil Alexa à la pièce, cliquez sur **Ajouter**.
6. Sélectionnez un appareil et cliquez sur **Ajouter**. L'appareil sélectionné apparaît dans la page **Ajouter des appareils Echo**.

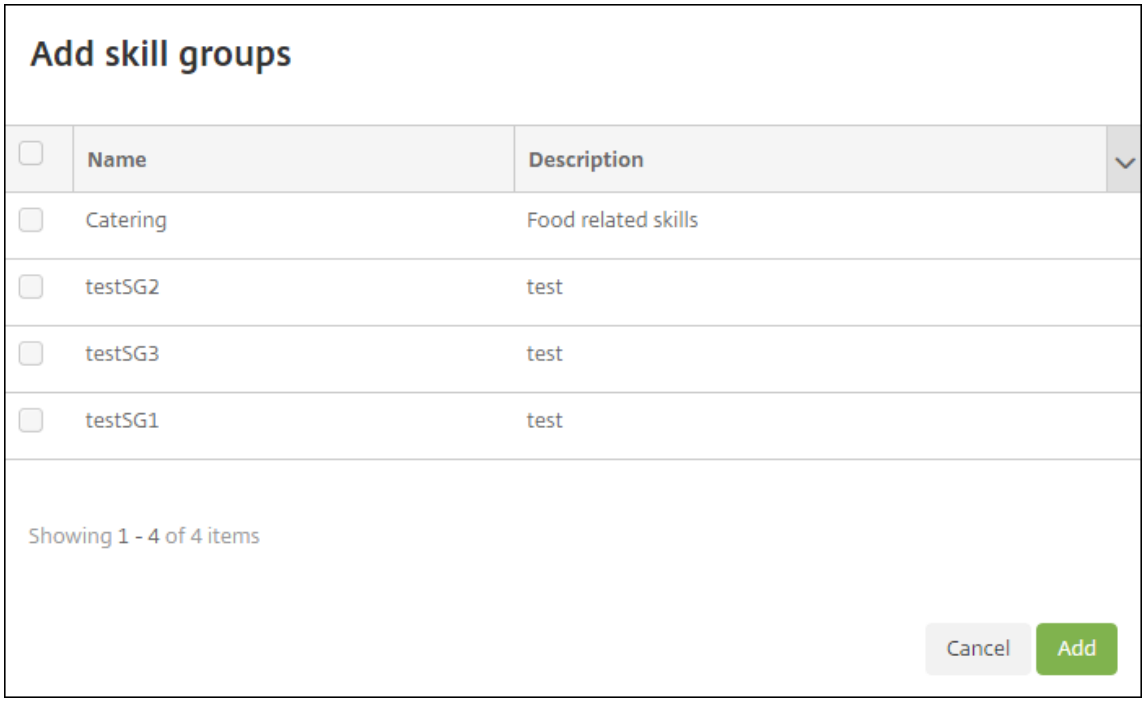


7. Cliquez sur **Suivant**.
8. Pour ajouter des groupes de Skills aux appareils Alexa de la pièce, cliquez sur **Ajouter**.



9. Sélectionnez les groupes de Skills que vous souhaitez ajouter aux appareils Alexa de la pièce. Cliquez sur **Ajouter**. Les groupes de Skills sélectionnés apparaissent dans la page **Ajouter des groupes de Skills**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

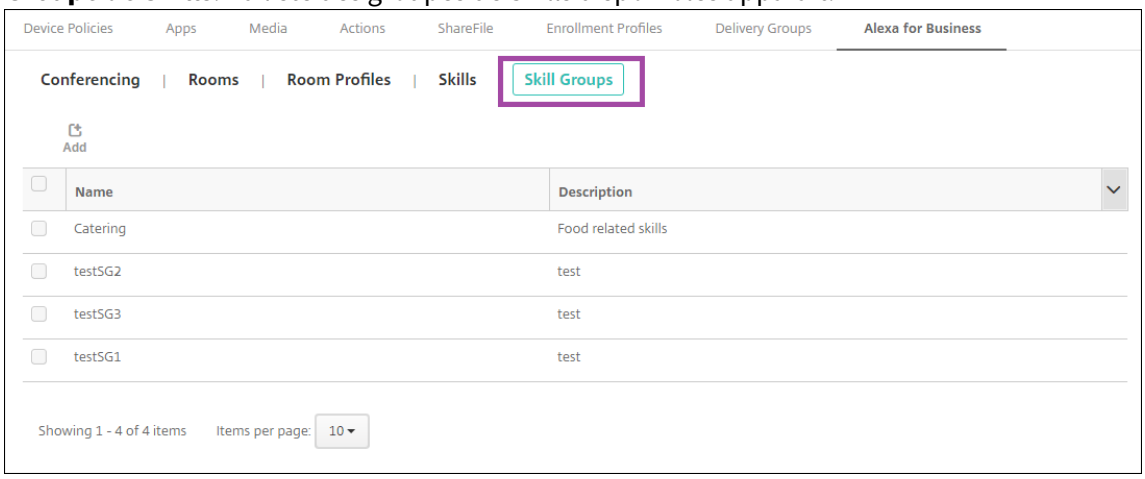


10. Cliquez sur **Save**.

Configurer des groupes de Skills

Les groupes de Skills sont des ensembles de compétences pouvant être appliqués à une pièce. Vous pouvez créer un groupe de Skills puis l'assigner à une pièce. Les compétences vous permettent d'utiliser un appareil Alexa pour certaines actions comme démarrer et terminer une réunion en ligne ou examiner l'ordre du jour. Vous pouvez ajouter, modifier et supprimer des groupes de Skills.

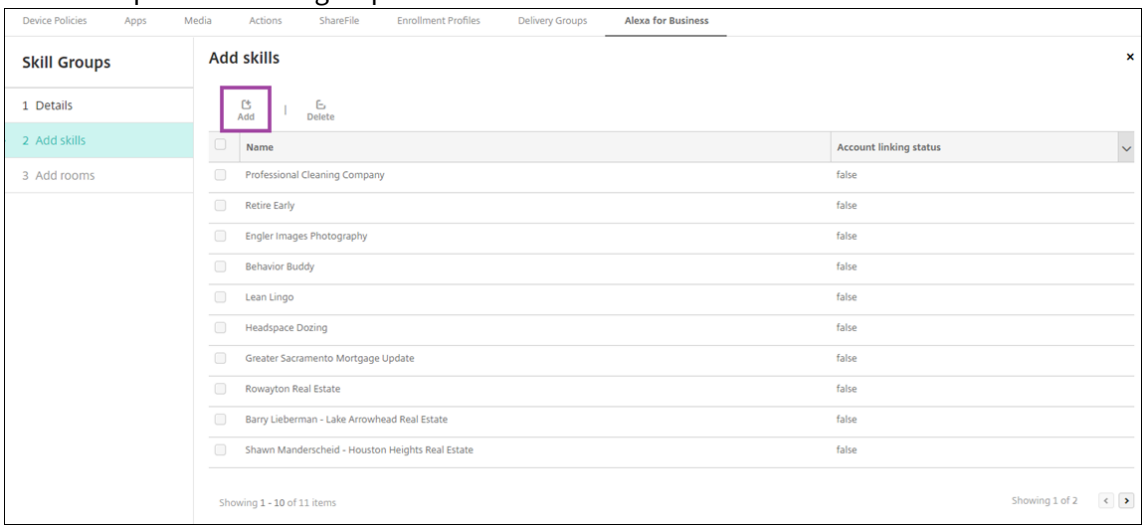
1. Dans la console Citrix Endpoint Management, sélectionnez **Configurer > Alexa for Business > Groupe de Skills**. La liste des groupes de Skills disponibles apparaît.



2. Pour ajouter un groupe de Skills, cliquez sur **Ajouter**. Pour modifier un groupe de Skills, sélectionnez le groupe à modifier et cliquez sur **Modifier**.

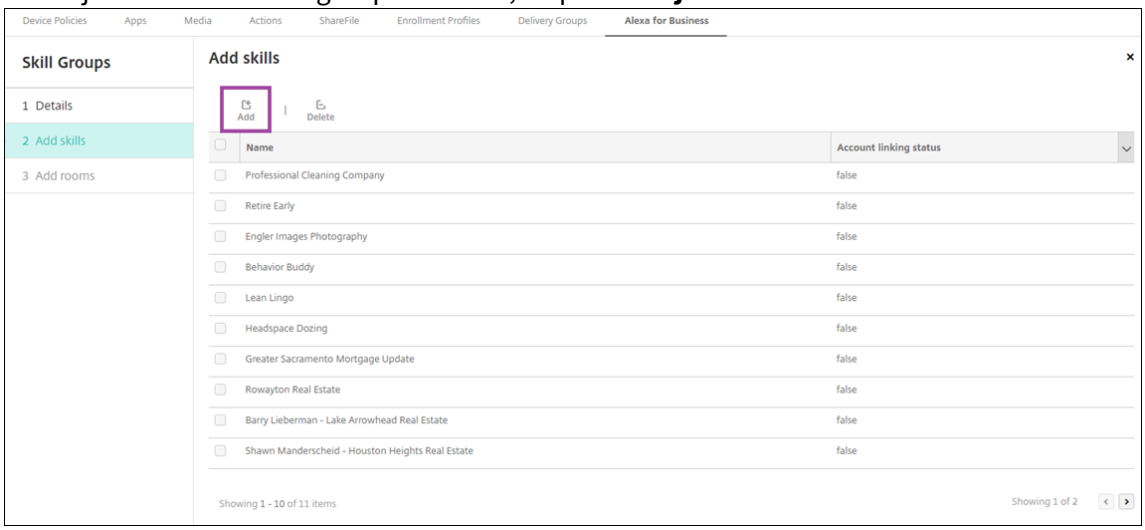
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Entrez ces paramètres de groupe de Skills :



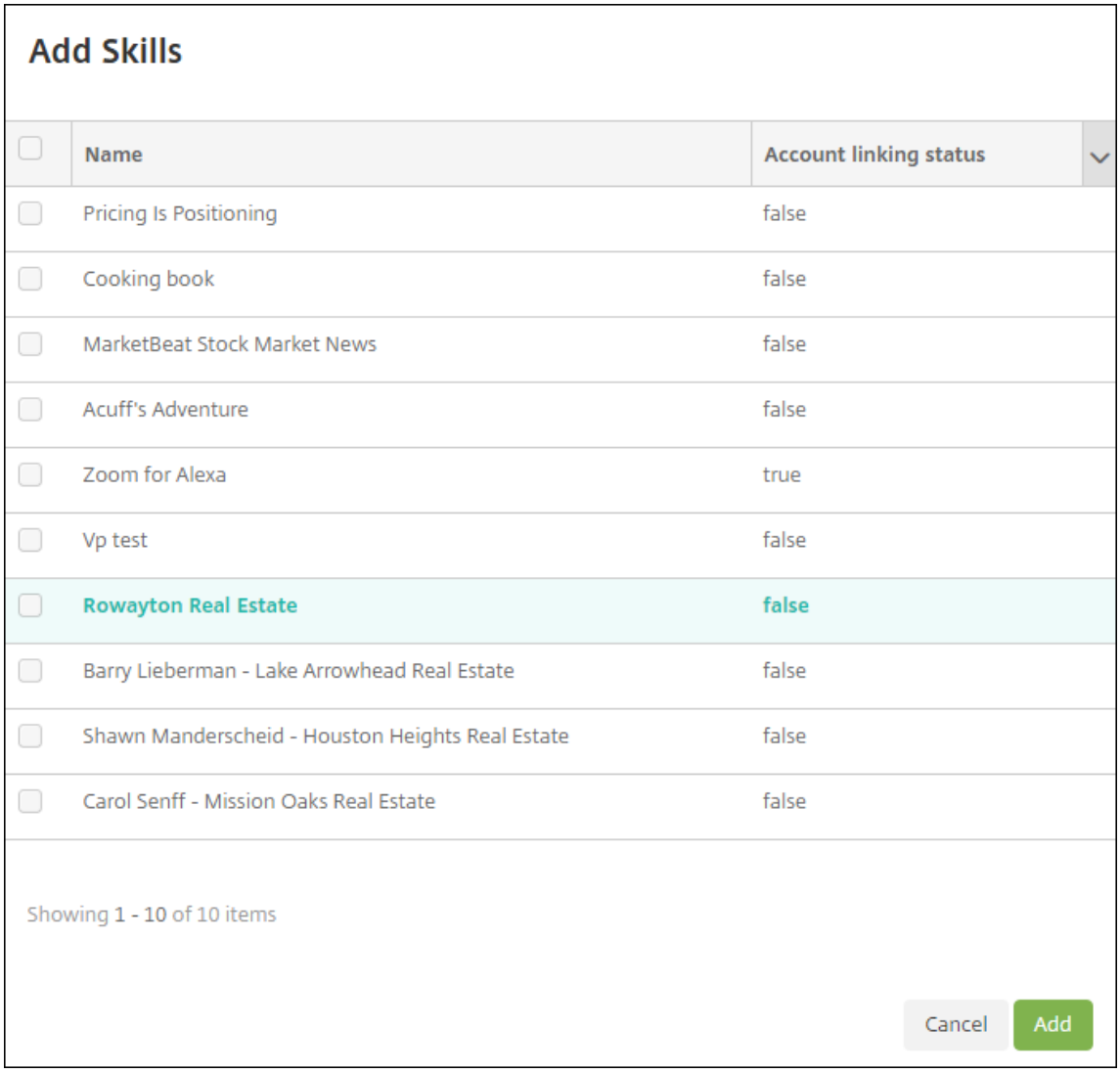
- **Nom :** tapez le nom du groupe de Skills.
- **Description :** entrez une brève description du groupe de Skills.

4. Cliquez sur **Suivant**.
5. Pour ajouter des Skills au groupe de Skills, cliquez sur **Ajouter**.

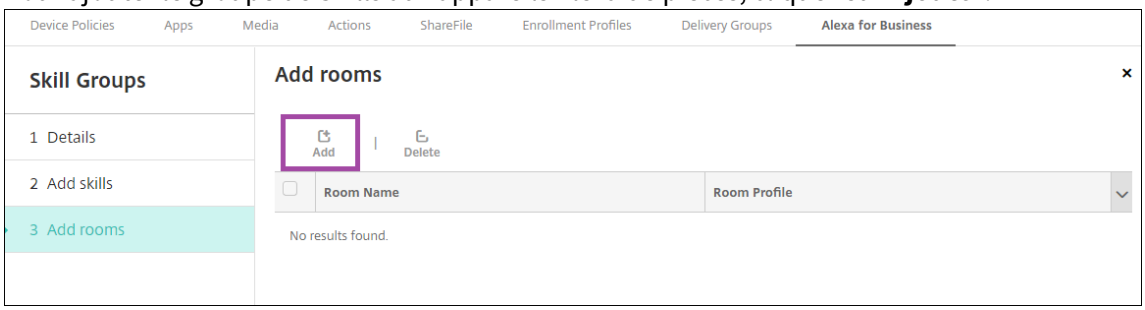


6. Sélectionnez les Skills que vous souhaitez inclure dans le groupe de Skills et cliquez sur **Ajouter**. Les Skills sélectionnés apparaissent dans la page **Ajouter des Skills**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

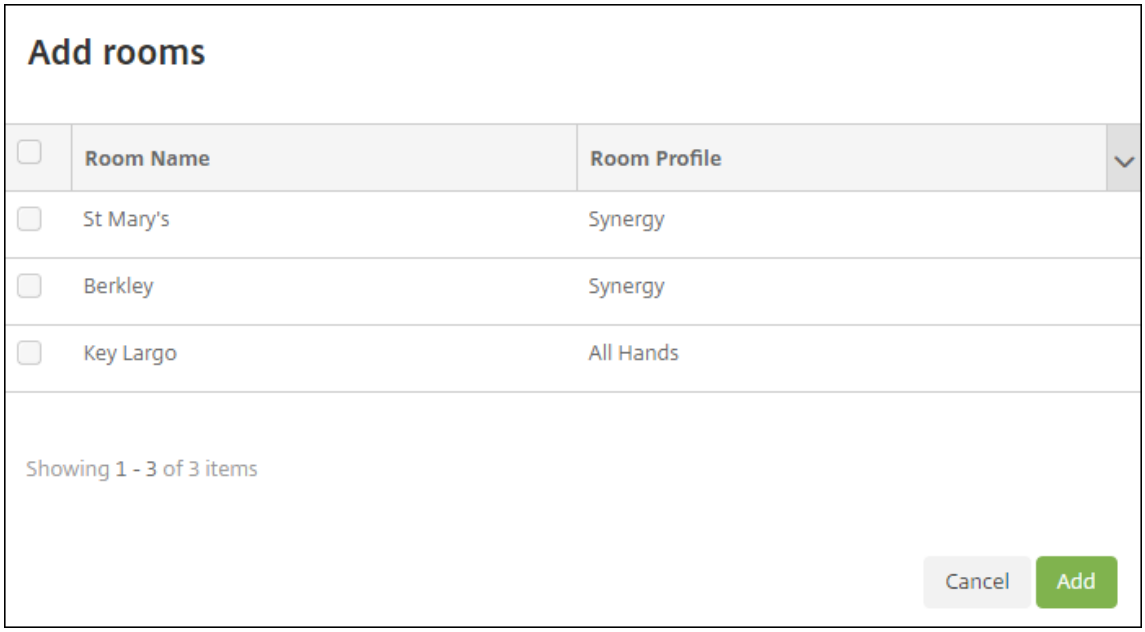


7. Pour ajouter le groupe de Skills aux appareils Alexa de pièces, cliquez sur **Ajouter**.



8. Sélectionnez les pièces.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



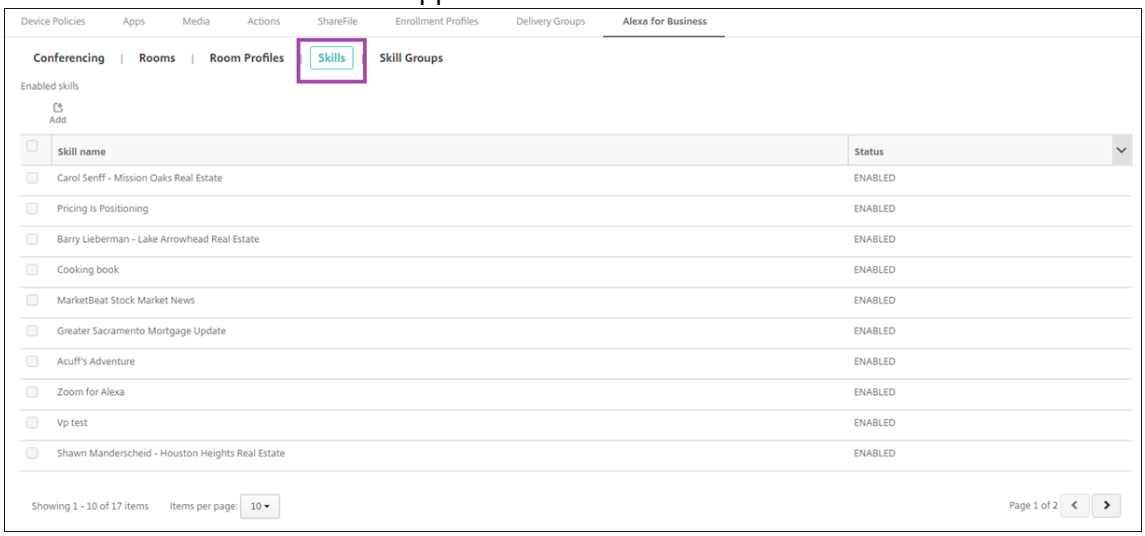
9. Cliquez sur **Save**.

Mettre les Skills à disposition des groupes de Skills

Vous devez configurer la liste des Skills Alexa à disposition des groupes de Skills de votre organisation Alexa for Business. Ces Skills proviennent de la boutique de Skills Alexa publique ou des Skills privées publiées pour votre organisation.

Ajouter des Skills à votre organisation

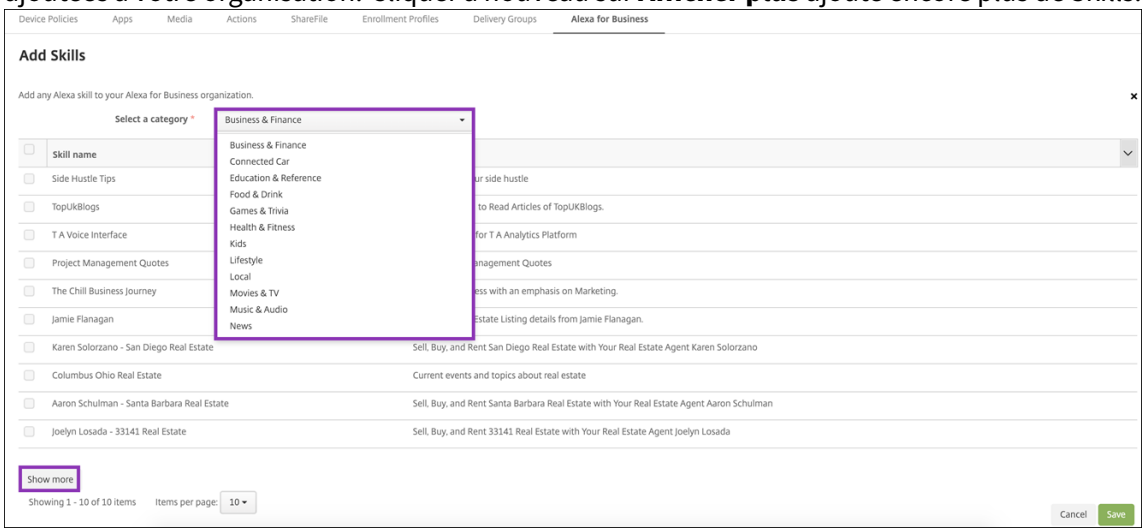
1. Dans la console Citrix Endpoint Management, sélectionnez **Configurer > Alexa for Business > Skills**. La liste des Skills activées apparaît.



2. Pour ajouter une Skill, cliquez sur **Ajouter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

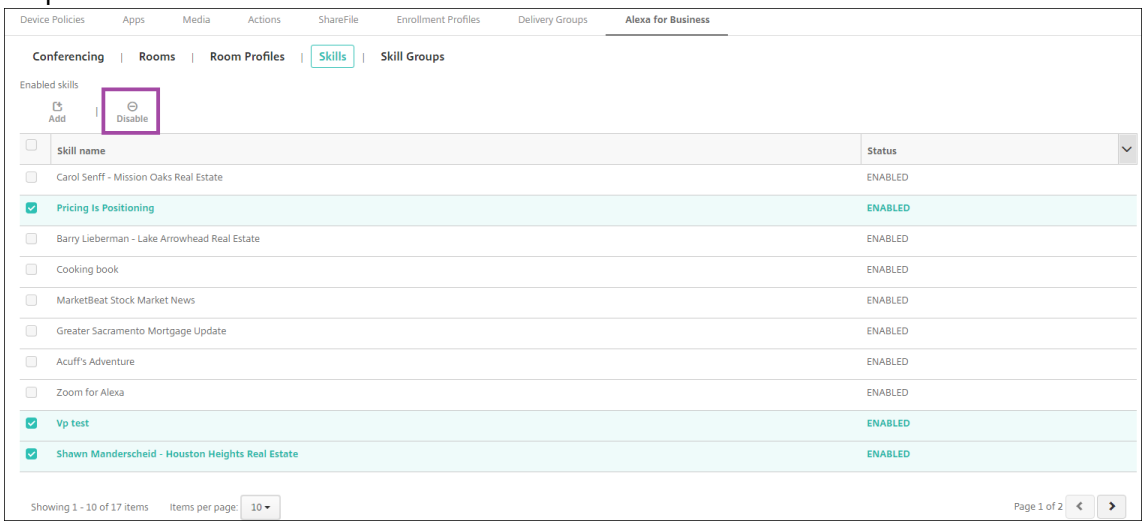
3. Pour voir plus de Skills Alexa, sélectionnez une catégorie et cliquez sur **Afficher plus**. Cliquer sur **Afficher plus** ajoute jusqu'à 10 Skills supplémentaires à la liste des Skills pouvant être ajoutées à votre organisation. Cliquer à nouveau sur **Afficher plus** ajoute encore plus de Skills.



4. Sélectionnez les Skills que vous souhaitez ajouter à votre organisation.
5. Cliquez sur **Save**.

Supprimer des Skills de votre organisation

1. Dans la console Citrix Endpoint Management, sélectionnez **Configurer > Alexa for Business > Skills**. La liste des Skills activées apparaît.
2. Sélectionnez les Skills que vous souhaitez retirer de votre organisation.
3. Cliquez sur **Désactiver**.

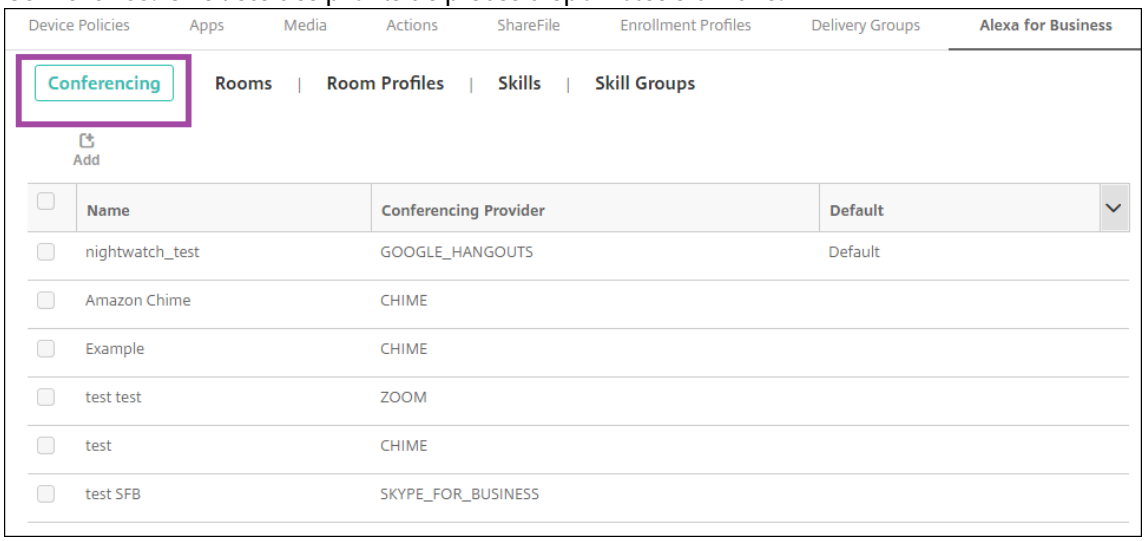


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer les conférences

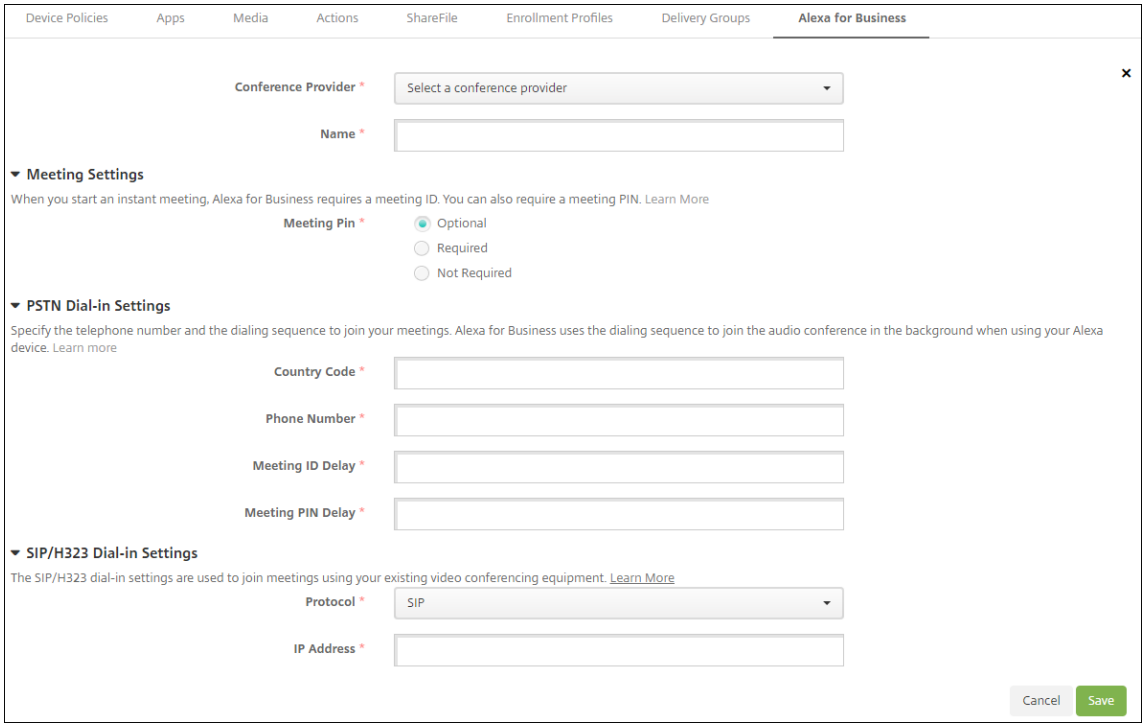
Les fonctionnalités de conférence vous permettent de configurer des fournisseurs de service de téléconférence, tels que Google Hangout ou Amazon Chime, qui contrôlent la façon dont les personnes participent à des conférences dans des pièces contenant des appareils Alexa. Vous pouvez ajouter, modifier et supprimer des fournisseurs de service de téléconférence. Vous pouvez également définir un fournisseur de service de téléconférence par défaut.

1. Dans la console Citrix Endpoint Management, sélectionnez **Configurer > Alexa for Business > Conférence**. Une liste des profils de pièces disponibles s'affiche.



2. Pour ajouter un fournisseur de service de téléconférence, cliquez sur **Ajouter**. Pour modifier un fournisseur de service de téléconférence, sélectionnez le profil de pièces à modifier et cliquez sur **Modifier**.
3. Entrez les paramètres du profil de pièce :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Fournisseur de service de téléconférence :** sélectionnez un fournisseur de service de téléconférence dans la liste.
- **Nom :** saisissez le nom que vous voulez donner au fournisseur de service de téléconférence.
- **Code PIN de réunion :** spécifiez si un code PIN est requis pour rejoindre la réunion.
- **Paramètres RTC**
  - **Indicatif du pays :** saisissez le code du pays.
  - **Numéro de téléphone :** saisissez le numéro de téléphone.
  - **Délai d'envoi de l'ID de réunion :** spécifiez le nombre de secondes avant l'envoi de l'ID de réunion.
  - **Délai du code PIN de réunion :** spécifiez le nombre de secondes avant l'envoi du code PIN.
- **Paramètres SIP/H323** Les paramètres SIP/H323 sont utilisés pour rejoindre des réunions à l'aide de votre équipement de visioconférence existant.
  - **Protocole :** sélectionnez un protocole.
  - **Adresse IP :** saisissez l'adresse IP.

4. Cliquez sur **Save**.

Si vous configurez plusieurs fournisseurs de service de téléconférence, définissez le fournisseur par défaut.

1. Dans la console Citrix Endpoint Management, sélectionnez **Configurer > Alexa for Business > Conférence**. Une liste des profils de pièces disponibles s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Sélectionnez le fournisseur de service de téléconférence que vous souhaitez définir comme fournisseur par défaut.
3. Cliquez sur **Définir par défaut**.

Migrer de l'administration des appareils vers Android Enterprise

November 29, 2023

Cet article traite des considérations et des recommandations relatives à la migration de l'administration des appareils Android d'ancienne génération vers Android Enterprise. Google est en train de mettre en place la fin de la prise en charge de l'API d'administration des appareils Android (Android Device Administration API). Cette API prend en charge les applications d'entreprise sur les appareils Android. Android Entreprise est la solution de gestion moderne recommandée par Google et Citrix.

Citrix Endpoint Management migre vers Android Entreprise comme méthode d'inscription par défaut pour les appareils Android. Une fois que Google a terminé la prise en charge des API, l'inscription échouera pour les appareils Android Q en mode d'administration de l'appareil.

Android Enterprise inclut la prise en charge des modes d'appareils entièrement gérés et d'appareils avec profil de travail. La publication Google, Android Enterprise Migration Bluebook, explique en détail comment l'administration des appareils d'ancienne génération et des appareils Android Enterprise diffèrent. Nous vous recommandons de lire les informations de migration publiées par Google.

Nous vous recommandons également de consulter l'article Citrix Tech Zone, Migration from Android Device Administrator to Android Enterprise with Citrix Endpoint Management.

Impact de la fin de prise en charge de l'administration des appareils

Google a mis fin à la prise en charge des API d'administrateur de l'appareil et ne les prendra plus en charge à partir du 2 novembre 2020. Ces API ne fonctionneront pas sur les appareils exécutant Android 10+ après la mise à niveau de Citrix Secure Hub pour cibler l'API Android niveau 29 :

- **Désactiver la caméra :** contrôle l'accès aux caméras de l'appareil.
- **Fonctionnalités Keyguard** : contrôle les fonctions liées au verrouillage des appareils, telles que la biométrie et les modèles.
- **Expiration du mot de passe :** oblige les utilisateurs à modifier leur mot de passe après une période configurable.
- **Limitation du mot de passe** : définit des exigences restrictives en matière de mot de passe

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exigences et recommandations

- Si vous pouvez mettre à niveau un appareil vers Android 10+, vous devez inscrire cet appareil dans Android Enterprise.
  - Vous devez inscrire les appareils Android 11 dans Android Enterprise.
  - À partir de septembre 2020, pour les appareils Android 10 : Citrix ne prend pas en charge les nouvelles inscriptions ou les réinscriptions d'appareils en mode administrateur d'appareil. Les appareils déjà inscrits continuent de fonctionner jusqu'au 2 novembre 2020, comme indiqué dans la section précédente.
- Pour les appareils fonctionnant sous Android 9 et versions ultérieures, nous prenons en charge le mode d'administration de l'appareil hérité. Cependant, nous vous recommandons de déplacer ces appareils vers Android Enterprise dès que possible.
- Pour les appareils nouveaux ou existants inscrits en mode Citrix MAM exclusif, aucune action n'est nécessaire. Les API Google obsolètes n'ont aucun impact sur les appareils inscrits en mode MAM exclusif. Cependant, avec le passage au cryptage de plateforme, nous vous recommandons fortement de passer du mode MAM exclusif au mode Profil de travail Android Enterprise (BYOD). Le mode Profil de travail fournit la fonctionnalité MAM, mais dans un conteneur sur l'appareil.

Analyse

La phase d'analyse de la migration comprend les étapes suivantes :

- Comprendre votre configuration Android d'ancienne génération
- Documenter votre configuration d'ancienne génération afin de pouvoir mapper les fonctionnalités d'ancienne génération aux fonctionnalités Android Enterprise

Analyse recommandée

1. Évaluez Android Entreprise sur Citrix Endpoint Management : entièrement géré, entièrement géré avec profil de travail, appareil dédié, profil de travail (BYOD).
2. Analysez les fonctionnalités actuelles d'administration de vos appareils par rapport à Android Entreprise.
3. Documentez les cas d'utilisation de l'administration de votre appareil.

Pour documenter les cas d'utilisation de l'administration de votre appareil, procédez comme suit :

1. Créez une feuille de calcul et répertoriez les groupes de stratégies actuels dans votre console Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Créez des cas d'utilisation distincts en fonction des groupes de stratégies existants.
3. Pour chaque cas d'utilisation, répertoriez les éléments suivants :
    - Nom
    - Chef d'entreprise
    - Modèle d'identité utilisateur
    - Configuration requise par l'appareil
        - Sécurité
        - Gestion
        - Utilisation
    - Inventaire des appareils
        - Marque et modèle
        - Version d'OS
    - Applications
4. Pour chaque application, répertoriez les éléments suivants :
    - Nom de l'application
    - Nom du package
    - Méthode d'hébergement
    - Si l'application est publique ou privée
    - Si l'application est obligatoire (vrai/faux)

Mappage des exigences

En vous basant sur l'analyse terminée, déterminez vos exigences en matière de fonctionnalités Android Enterprise.

Mappage des exigences recommandé

1. Déterminez le mode de gestion et la méthode d'inscription :
    - Profil de travail (BYOD) : nécessite une réinscription. Aucune réinitialisation d'usine n'est nécessaire.
    - Entièrement géré : nécessite une réinitialisation d'usine. Inscrivez les appareils à l'aide du code QR, du partage NFC, de l'identifiant du DPC ou de l'inscription sans contact.
2. Créez une stratégie de migration d'application.
3. Mappez les exigences du cas d'utilisation aux fonctionnalités Android Enterprise. Documentez la fonctionnalité pour chaque exigence de l'appareil qui correspond le mieux à l'exigence Android et sa version correspondante.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Déterminez le système d'exploitation Android minimum en fonction de la configuration requise (7.0, 8.0, 9.0).
5. Choisissez un modèle d'identité :
   - Modèle recommandé : Compte Google Play d'entreprise
   - Utilisez les comptes Google Workspace uniquement si vous êtes un client Google Cloud Identity
6. Créez une stratégie d'appareil :
   - Aucune action : si les appareils répondent au niveau minimum du système d'exploitation.
   - Mise à niveau : si les appareils peuvent être mis à jour vers le système d'exploitation pris en charge.
   - Remplacement : si les appareils ne peuvent pas être mis à jour vers le niveau du système d'exploitation pris en charge.

Stratégie de migration d'application recommandée

Une fois la correspondance des exigences effectuée, déplacez les applications de la plate-forme Android vers la plate-forme Android Enterprise. Pour plus d'informations sur la publication d'applications, consultez la section Ajouter des applications.

- Applications de magasin public
  1. Sélectionnez les applications à migrer, puis modifiez les applications en effaçant le paramètre Google Play et en sélectionnant **Android Enterprise** comme plate-forme.
  2. Sélectionnez le groupe de mise à disposition. Si une application est obligatoire, déplacez l'application vers la liste **Applications requises** dans le groupe de mise à disposition.

  Une fois l'application enregistrée, elle apparaît dans Google Play Store. Si vous avez un profil de travail, les applications apparaissent dans Google Play Store dans le profil de travail.
- Applications (d'entreprise) privées

  Les applications privées sont développées en interne ou par un développeur tiers. Nous vous recommandons de publier les applications privées à l'aide de Google Play.
  1. Sélectionnez les applications à migrer, puis modifiez les applications en sélectionnant **Android Enterprise** comme plate-forme.
  2. Chargez le fichier APK, puis configurez les paramètres de l'application.
  3. Publiez l'application dans le groupe de mise à disposition requis.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Applications MDX

  1. Sélectionnez les applications à migrer, puis modifiez les applications en sélectionnant **Android Enterprise** comme plate-forme.
  2. Chargez le fichier MDX. Procédez au processus d'approbation de l'application.
  3. Sélectionnez les stratégies MDX.

  Pour les applications MDX d'entreprise, nous vous recommandons de les remplacer par des applications encapsulées en mode SDK MDX :

  – Option 1 : hébergez l'APK dans Google Play avec un compte de développeur attribué à titre privé à votre organisation. Publiez le fichier MDX dans Citrix Endpoint Management.
  – Option 2 : publiez l'application depuis Citrix Endpoint Management en tant qu'application d'entreprise. Publiez l'APK dans Citrix Endpoint Management et sélectionnez la plate-forme **Android Enterprise** pour le fichier MDX.

Migration de stratégie d'appareil Citrix

Pour les stratégies disponibles pour les plates-formes **Android (DA hérité)** et **Android Enterprise**, modifiez la stratégie et sélectionnez la plate-forme **Android Enterprise**.

- Pour Android Enterprise, considérez la méthode d'inscription de l'appareil. Certaines options de stratégie sont disponibles uniquement pour les appareils en mode Profil de travail ou en mode entièrement géré. Consultez la section Configurer les stratégies d'appareil et d'application Android Enterprise.
- Si vous utilisez la stratégie Exchange pour les appareils en mode DA (administrateur d'appareil) hérité, créez une stratégie Configurations gérées plutôt que de configurer les paramètres de messagerie.
- Pour vous assurer que vous ciblez une stratégie sur les appareils prévus (Android Enterprise ou Android en mode DA hérité), ajoutez une règle de déploiement à la stratégie. Par exemple, pour la plate-forme Android (DA hérité), utilisez la règle de déploiement suivante :

  ```
  Limit by known device property name Android Enterprise
  Enabled Device? Isn ' t equal to true
  <!--NeedCopy-->
  ```

  Cette règle de déploiement vérifie si l'appareil n'est PAS activé pour Android Enterprise et fournit la stratégie ainsi que les applications aux appareils activés pour le mode DA hérité.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Preuve de concept

Après avoir migré des applications vers Android Entreprise, vous pouvez configurer un test de migration pour vérifier que les fonctionnalités fonctionnent comme prévu.

Configuration de l'évaluation recommandée

1. Configurez l'infrastructure de déploiement :
    - Créez un groupe de mise à disposition pour votre évaluation Android Enterprise.
    - Configurez Android Entreprise dans Citrix Endpoint Management.
2. Configurez les applications utilisateur.
3. Configurez les fonctionnalités Android Enterprise.
4. Attribuez des stratégies au groupe de mise à disposition Android Enterprise.
5. Testez et confirmez les fonctionnalités.
6. Effectuez une procédure détaillée de la configuration de l'appareil pour chaque cas d'utilisation.
7. Documentez les étapes de configuration de l'utilisateur.

Déploiement

Vous pouvez désormais déployer votre configuration Android Entreprise et préparer vos utilisateurs à la migration.

Stratégie de déploiement recommandée

La stratégie de déploiement recommandée par Citrix consiste à tester tous vos systèmes de production pour Android Enterprise, puis à terminer la migration d'appareils ultérieurement.

- Dans ce scénario, les utilisateurs continuent à utiliser des appareils d'ancienne génération avec leur configuration actuelle. Vous configurez de nouveaux appareils pour la gestion Android Entreprise.
- Migrez les appareils existants uniquement lorsqu'une mise à niveau ou un remplacement est nécessaire.
- Migrez les appareils existants vers la gestion Android Entreprise à la fin de leur cycle de vie habituel. Vous pouvez également migrer ces appareils lorsqu'ils ont besoin d'être remplacés en raison de perte ou d'endommagement.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Android Enterprise

December 11, 2023

Android Enterprise est un ensemble d'outils et de services fournis par Google en tant que solution de gestion d'entreprise pour les appareils Android. Avec Android Enterprise :

- Vous utilisez Citrix Endpoint Management pour gérer les appareils appartenant à l'entreprise et vos appareils Android BYOD (programme « Apportez votre propre appareil »).
- Vous pouvez gérer l'ensemble de l'appareil ou un profil distinct sur l'appareil. Le profil distinct permet d'isoler les comptes, applications et données d'entreprise des comptes, applications et données personnels.
- Vous pouvez également gérer des appareils dédiés à un usage unique, tels que la gestion de l'inventaire. Pour obtenir une vue d'ensemble de Google sur les fonctionnalités d'Android Enterprise, consultez Gestion Android Enterprise.

Ressources :

- Pour obtenir la liste des termes et définitions liés à Android Enterprise, consultez l'article Terminologie Android Enterprise du guide des développeurs Google Android Enterprise. Google met fréquemment à jour ces termes.
- Pour les systèmes d'exploitation Android pris en charge par Citrix Endpoint Management, consultez la section Systèmes d'exploitation d'appareils pris en charge.
- Pour plus d'informations sur les connexions sortantes à prendre en compte lors de la configuration d'environnements réseau pour Android Enterprise, consultez l'article de support Google Android Enterprise Network Requirements.
- Pour plus d'informations sur le déploiement d'Android Enterprise, consultez Déployer des ressources.

Démarrer avec Android Enterprise

> **Important :**
>
> le mode d'administration des appareils n'est plus pris en charge. Si vos utilisateurs disposent d'appareils en mode d'administration des appareils, consultez la section Migrer de l'administration des appareils vers Android Enterprise. Une fois vos appareils migrés vers Android Enterprise, procédez comme suit pour configurer les appareils Android Enterprise.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration unique

1. Créez un compte Google Play d'entreprise.

   Consultez les sections Utilisation de Google Play d'entreprise avec Citrix Endpoint Management et Configuration requise.

2. Liez votre compte Google Play à Citrix Endpoint Management.

   Consultez la section Connexion de Citrix Endpoint Management à Google Play.

3. Planifiez la façon dont vous souhaitez gérer les appareils.

   Consultez la section Scénarios et profils de déploiement d'appareils.

4. Planifiez la sécurité de l'inscription pour les machines utilisateur.

   Consultez la section Sécurité de l'inscription.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Préparez-vous à fournir des applications compatibles MDX.

   Utilisez le SDK MAM pour développer des applications. Si vous n'êtes pas prêt à passer au nouveau SDK, vous pouvez également utiliser le MDX Toolkit basé sur la ligne de commande pour encapsuler les applications.

   Consultez la section Présentation du SDK MAM.

À ce stade, vous êtes prêt à configurer vos appareils Android Enterprise avec des stratégies d'appareil et d'application, des profils d'inscription, ainsi que des applications. Consultez la section suivante pour plus d'informations.

Configurer les appareils

1. Créez des groupes de mise à disposition.

   Contrôlez quels utilisateurs reçoivent quelles ressources et à quel moment. Consultez la section Déployer des ressources.

   Nous cesserons de fournir des applications publiées pour la plate-forme en mode DA hérité aux appareils inscrits dans Android Enterprise. Pour les appareils Android Enterprise, publiez des applications pour la plate-forme Android Enterprise. Pour continuer à publier des applications en mode DA hérité sur des appareils en mode DA, créez un groupe de mise à disposition distinct pour ces applications. Voir Fin de prise en charge.

2. Ajouter des applications. Vous pouvez approuver les applications dans Google Play directement à partir de la console Citrix Endpoint Management.

   Consultez l'article de l'assistance Google, Gérer les applications dans votre organisation.

3. Créer des profils d'inscription

   Spécifiez les options d'inscription pour la gestion des appareils et des applications. Consultez les sections Scénarios et profils de déploiement d'appareils et Création de profils d'inscription.

   - Lorsque vous déployez une application du magasin d'applications public Android Enterprise sur un utilisateur d'appareil Android, cet utilisateur est automatiquement inscrit dans Android Enterprise.
   - L'inscription sans contact vous permet de configurer les appareils pour qu'ils s'inscrivent automatiquement lorsqu'ils sont mis sous tension pour la première fois. Consultez Inscription sans contact.

4. Configurez les stratégies d'appareil et d'application.

   Trouvez le juste équilibre entre sécurité de l'entreprise, confidentialité des utilisateurs et expérience utilisateur. Consultez la section Configurer les stratégies d'appareil et d'application Android Enterprise.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Distribuez les applications

   Vous utilisez Google Play d'entreprise pour ajouter, acheter et approuver des applications en vue de les déployer sur l'espace Android Enterprise d'un appareil. Les utilisateurs peuvent uniquement installer des applications à partir de Google Play d'entreprise que vous leur mettez à disposition.

   Voir :

   - Distribuer des applications Android Enterprise
   - Stratégie Configurations gérées
   - Stratégie Autorisations d'application

6. Configurez les actions de sécurité pour surveiller et garantir la conformité.

   Consultez la section Actions de sécurisation.

Utilisation de Google Play d'entreprise avec Citrix Endpoint Management

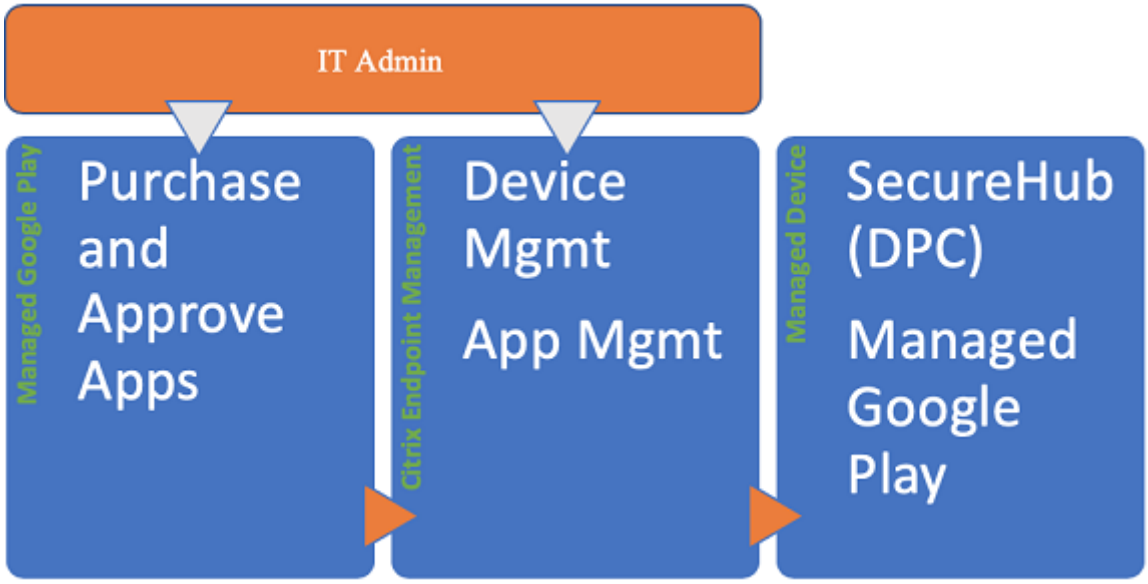
Lorsque vous intégrez Citrix Endpoint Management à Google Play d'entreprise pour utiliser Android Enterprise, vous créez une entreprise. Google définit une entreprise comme une liaison entre l'organisation et votre solution de gestion mobile d'entreprise (EMM). Tous les utilisateurs et appareils que l'organisation gère via votre solution appartiennent à son entreprise.

Une entreprise pour Android Enterprise comprend trois composants : une solution EMM, une application DPC (Device Policy Controller) et une plate-forme d'application Google Enterprise. Lorsque vous intégrez Citrix Endpoint Management à Android Entreprise, la solution complète comporte les composants suivants :

- **Citrix Endpoint Management :** solution de gestion mobile d'entreprise Citrix. Citrix Endpoint Management est la solution Citrix Endpoint Management unifiée qui sécurise l'espace de travail numérique. Citrix Endpoint Management fournit aux administrateurs informatiques le moyen de gérer les appareils et les applications de leur organisation.
- **Citrix Secure Hub :** l'application DPC Citrix. Citrix Secure Hub représente la rampe de lancement d'Citrix Endpoint Management. Citrix Secure Hub applique des stratégies sur l'appareil.
- **Google Play d'entreprise :** plate-forme d'application d'entreprise Google qui s'intègre avec Citrix Endpoint Management. L'API EMM de Google Play définit les stratégies d'application et distribue l'application.

Cette illustration montre comment les administrateurs interagissent avec ces composants et comment les composants interagissent les uns avec les autres :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Remarque :**
>
> Vous pouvez utiliser Google Play d'entreprise ou Google Workspace (anciennement G Suite) pour enregistrer Citrix en tant que fournisseur de gestion de la mobilité d'entreprise (EMM). Cet article traite de l'utilisation d'Android Enterprise avec Google Play d'entreprise. Si votre organisation utilise Google Workspace pour fournir un accès aux applications, vous pouvez l'utiliser avec Android Enterprise. Consultez la section Ancienne version d'Android Enterprise pour clients Google Workspace.

Lorsque vous utilisez Google Play d'entreprise, provisionnez des comptes Google Play d'entreprise pour les appareils et les utilisateurs. Les comptes Google Play d'entreprise permettent d'accéder à Google Play d'entreprise, ce qui permet aux utilisateurs d'installer et d'utiliser les applications que vous mettez à leur disposition. Si votre organisation utilise un service d'identité tiers, vous pouvez lier des comptes Google Play d'entreprise à vos comptes d'identité existants.

Comme ce type d'entreprise n'est pas lié à un domaine, vous pouvez créer plusieurs entreprises pour une seule organisation. Par exemple, chaque département ou région d'une organisation peut s'inscrire en tant qu'entreprise différente. L'utilisation de différentes entreprises vous permet de gérer des ensembles distincts d'appareils et d'applications.

Pour les administrateurs Citrix Endpoint Management, Google Play d'entreprise combine l'expérience utilisateur et les fonctionnalités du magasin d'applications de Google Play avec un ensemble de fonctionnalités de gestion conçues pour les entreprises. Vous utilisez Google Play d'entreprise pour ajouter, acheter et approuver des applications en vue de les déployer sur l'espace Android Enterprise d'un appareil. Vous pouvez utiliser Google Play pour déployer des applications publiques, privées, et tierces.

Pour les utilisateurs d'appareils gérés, Google Play d'entreprise correspond au magasin d'applica-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tions d'entreprise. Les utilisateurs peuvent parcourir les applications, afficher les détails des applications et les installer. Contrairement à la version publique de Google Play, les utilisateurs peuvent uniquement installer des applications à partir de Google Play d'entreprise que vous leur mettez à disposition.

Scénarios et profils de déploiement d'appareils

Les scénarios de déploiement d'appareils permettent de savoir à qui appartient les appareils que vous déployez et la façon dont vous les gérez. Les profils d'appareils font référence à la façon dont DPC gère et applique les stratégies sur les appareils.

Le profil de travail permet d'isoler les comptes, applications et données d'entreprise des comptes, applications et données personnels. Les profils de travail et les profils personnels sont séparés au niveau du système d'exploitation. Pour plus d'informations sur les profils de travail (ou profils professionnels), consultez la rubrique d'aide Qu'est-ce qu'un profil professionnel.

> **Important :**
>
> Lorsque les appareils Android Enterprise sont mis à jour vers Android 11, Google migre les appareils « entièrement gérés avec profil de travail » vers une nouvelle expérience de profil de travail optimisée pour la sécurité. Le nouveau mode d'inscription est appelé « profil de travail sur appareils appartenant à l'entreprise ». Pour plus d'informations, consultez Changes ahead for Android Enterprise's Fully Managed with Work Profile.
> Pour les appareils Android 12 , consultez Security and privacy enhancements for work profile.

Gestion des appareils	Cas d'utilisation	Profil de travail	Profil personnel	Remarques
Appareils appartenant à l'entreprise (entièrement gérés)	Appareils appartenant à l'entreprise destinés uniquement à un usage professionnel	Non	Non	Pour les appareils neufs ou réinitialisés en usine uniquement. Consultez la section Provisionner des appareils Android Enterprise entièrement gérés.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Gestion des appareils	Cas d'utilisation	Profil de travail	Profil personnel	Remarques
Entièrement géré avec un profil de travail/Profil de travail sur appareils appartenant à l'entreprise	Appareils appartenant à l'entreprise destinés à un usage professionnel et personnel	Oui	Oui. Deux copies du DPC s'exécutent sur ces appareils : l'une qui gère l'appareil en mode propriétaire de l'appareil et l'autre qui gère le profil de travail en mode propriétaire du profil. Vous pouvez appliquer des stratégies distinctes à l'appareil et au profil de travail.	Consultez la section Provisionner des appareils Android Enterprise entièrement gérés avec profil de travail ou profil de travail sur appareils appartenant à l'entreprise.
Appareils dédiés*	Appareils appartenant à l'entreprise configurés pour un seul cas d'utilisation, tels que l'affichage numérique ou l'impression de billets	Non	Non	Consultez la section Provisionner des appareils Android Enterprise dédiés.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Profil de travail BYOD**	Appareils personnels inscrits à la gestion des profils de travail (également appelée mode propriétaire du profil)	Oui	Oui. DPC gère uniquement le profil de travail, pas l'ensemble de l'appareil.	Ces appareils n'ont pas besoin d'être neufs ou réinitialisés en usine. Consultez Provisioning d'appareils Android Enterprise avec profil de travail.

* Les utilisateurs peuvent partager un appareil dédié. Lorsqu'un utilisateur se connecte à une application sur un appareil dédié, l'état de son travail est celui de l'application, et non celui de l'appareil.

** Citrix Endpoint Management ne prend pas en charge les appareils Zebra en mode profil de travail BYOD. Citrix Endpoint Management prend en charge les appareils Zebra en tant qu'appareils entièrement gérés utilisant Android Enterprise.

Sécurité de l'inscription

Les profils d'inscription déterminent si les appareils Android s'inscrivent en mode MAM, MDM ou MDM+MAM, avec la possibilité pour les utilisateurs de se désinscrire de MDM.

Pour plus d'informations sur la spécification du niveau de sécurité et les étapes d'inscription requises, voir Comptes d'utilisateurs, rôles et inscription.

Citrix Endpoint Management prend en charge les méthodes d'authentification suivantes pour les appareils Android inscrits en mode MDM ou MDM+MAM. Pour plus d'informations, consultez les articles suivants :

- Authentification domaine ou domaine + jeton de sécurité
- Authentification certificat client ou certificat + domaine
- Fournisseurs d'identité :
  - Authentification avec Azure Active Directory via Citrix Cloud (version préliminaire)
  - Authentification avec Okta via Citrix Cloud (version préliminaire)

Une autre méthode d'authentification rarement utilisée est le certificat client et le jeton de sécurité. Pour de plus amples informations, consultez https://support.citrix.com/article/CTX215200.

Exigences

Avant de commencer à utiliser Android Enterprise, vous devez disposer des éléments suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

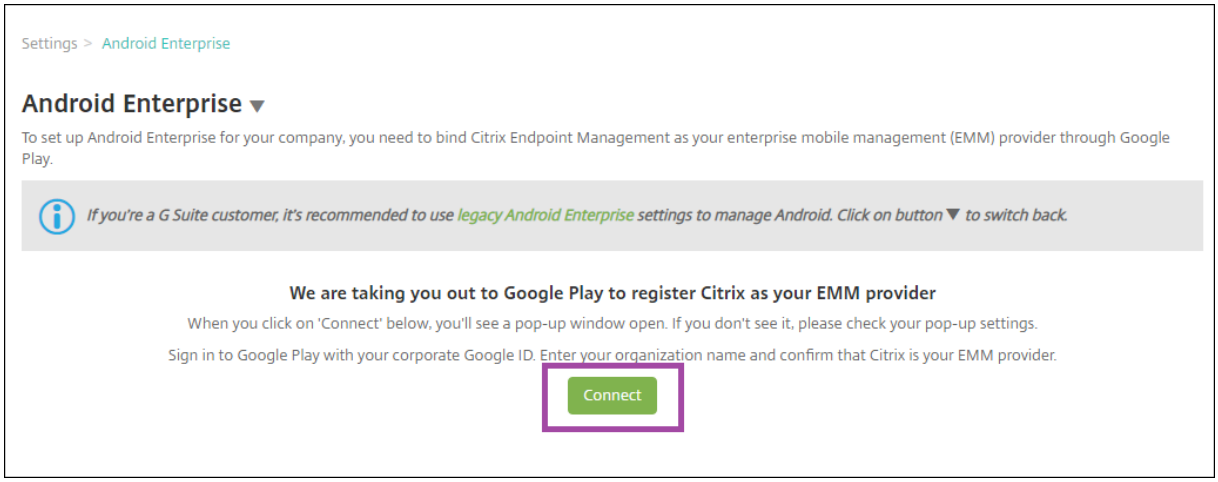
- Comptes et informations d'identification :
  - Pour configurer Android Enterprise avec Google Play d'entreprise, un compte Google d'entreprise
  - Pour télécharger les derniers fichiers MDX, un compte client Citrix
- Firebase Cloud Messaging (FCM) et une stratégie de planification de connexion configurée pour Citrix Endpoint Management. Consultez les sections Firebase Cloud Messaging et Stratégie de planification de connexion.

Connexion de Citrix Endpoint Management à Google Play

Pour configurer Android Enterprise pour votre organisation, enregistrez Citrix en tant que fournisseur de gestion de la mobilité d'entreprise (EMM) via Google Play d'entreprise. Cela permet de connecter Google Play d'entreprise à Citrix Endpoint Management et de créer une entreprise pour Android Entreprise dans Citrix Endpoint Management.

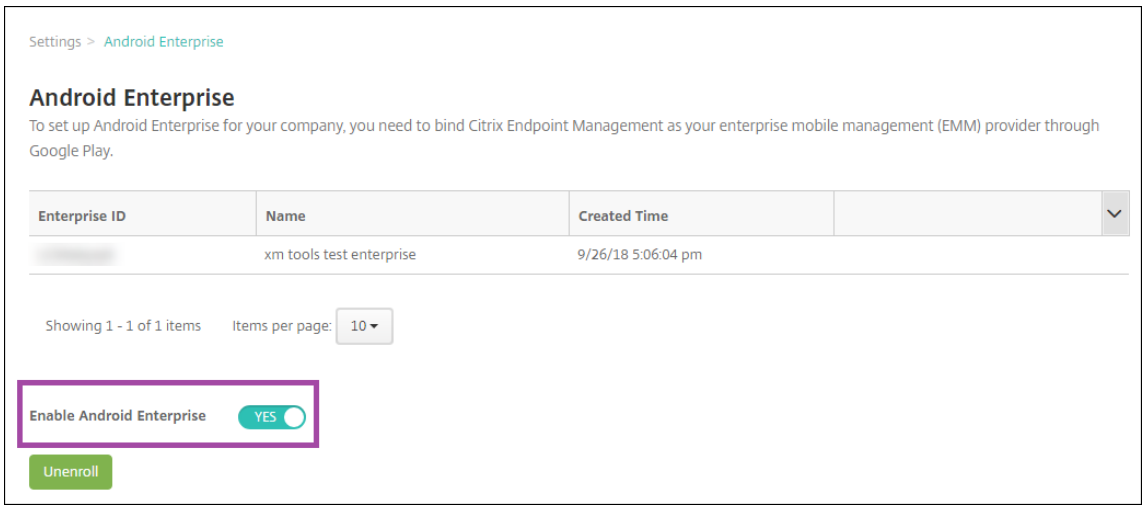
Vous avez besoin d'un compte Google d'entreprise pour vous connecter à Google Play.

1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Android Enterprise**.
2. Cliquez sur **Connect**. Google Play s'ouvre.

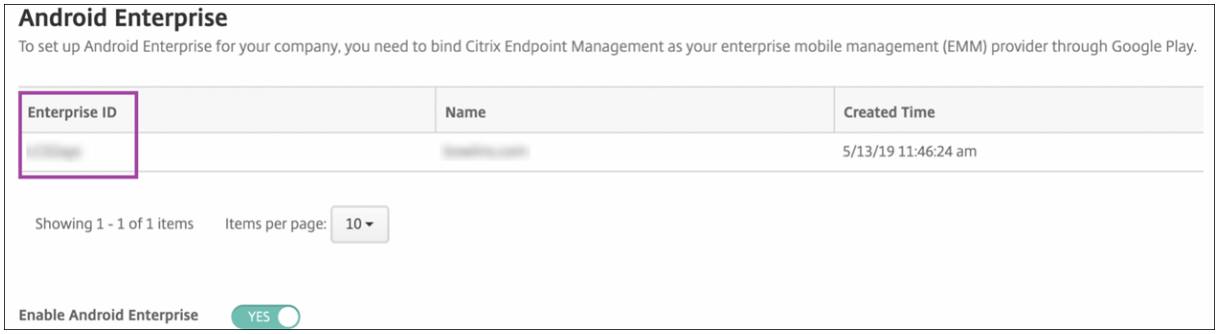


1. Connectez-vous à Google Play avec les informations d'identification de votre compte Google d'entreprise. Entrez le nom de votre organisation et confirmez que Citrix est votre fournisseur EMM.
2. Un ID d'entreprise est ajouté pour Android Enterprise. Pour activer Android Enterprise, faites glisser **Activer Android Enterprise** vers **Oui**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Votre identifiant Enterprise s'affiche dans la console Citrix Endpoint Management.



Votre environnement est connecté à Google et est prêt à gérer les appareils. Vous pouvez désormais mettre des applications à la disposition des utilisateurs.

Citrix Endpoint Management peut mettre à la disposition des utilisateurs des applications de productivité mobiles Citrix, des applications MDX, des applications de magasin d'applications public, des applications Web et SaaS, des applications d'entreprise et des liens Web. Pour de plus amples informations sur la mise à disposition de ces types d'applications pour les utilisateurs, consultez la section Distribuer des applications Android Enterprise.

La section suivante explique comment mettre à disposition des applications de productivité mobiles.

Mettre à disposition des applications de productivité mobiles Citrix aux utilisateurs d'Android Enterprise

Afin de mettre à disposition des applications de productivité mobiles Citrix aux utilisateurs d'Android Enterprise, effectuez les étapes suivantes.

1. Publiez les applications en tant qu'applications MDX. Consultez Configurer des applications en tant qu'applications MDX.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Configurez les règles pour la question de sécurité que vos utilisateurs utilisent pour accéder aux profils de travail sur leurs appareils. Consultez Configurer la stratégie de la question de sécurité.

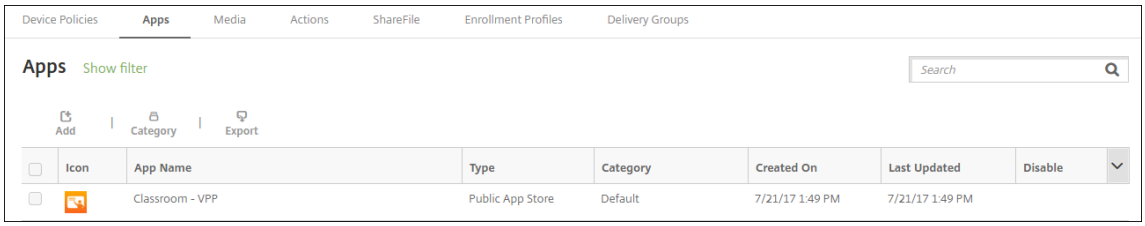
Les applications que vous publiez sont disponibles pour les appareils inscrits dans votre entreprise Android Enterprise.

> **Remarque :**
>
> Lorsque vous déployez une application du magasin d'applications public Android Enterprise sur un utilisateur Android, cet utilisateur est automatiquement inscrit dans Android Enterprise.

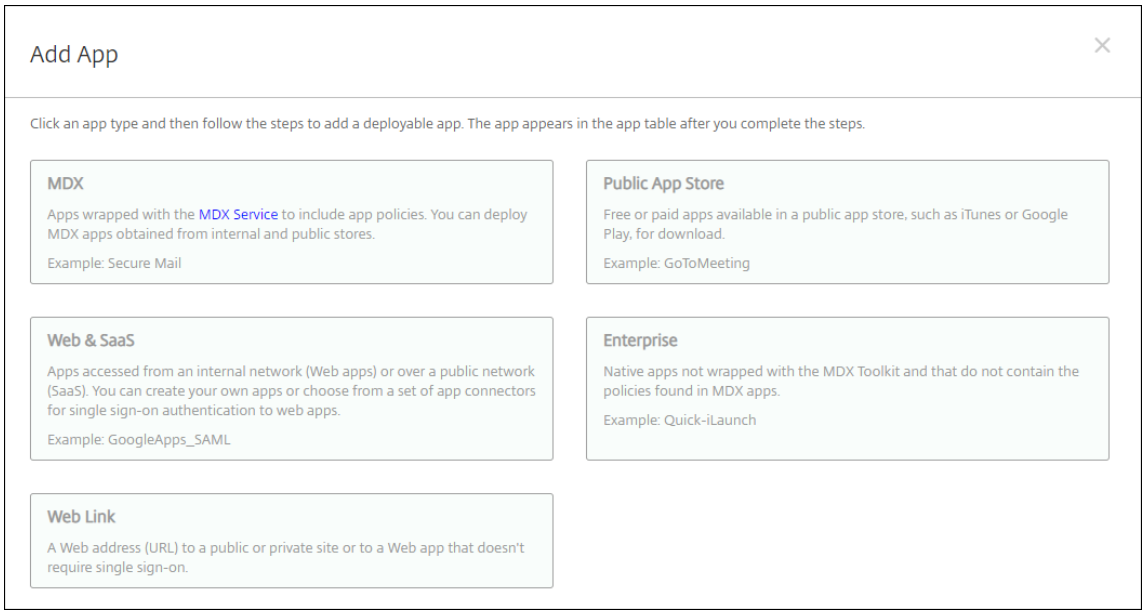
Configurer des applications en tant qu'applications MDX

Pour configurer une application de productivité Citrix en tant qu'application MDX pour Android Enterprise :

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications**. La page **Applications** s'affiche.



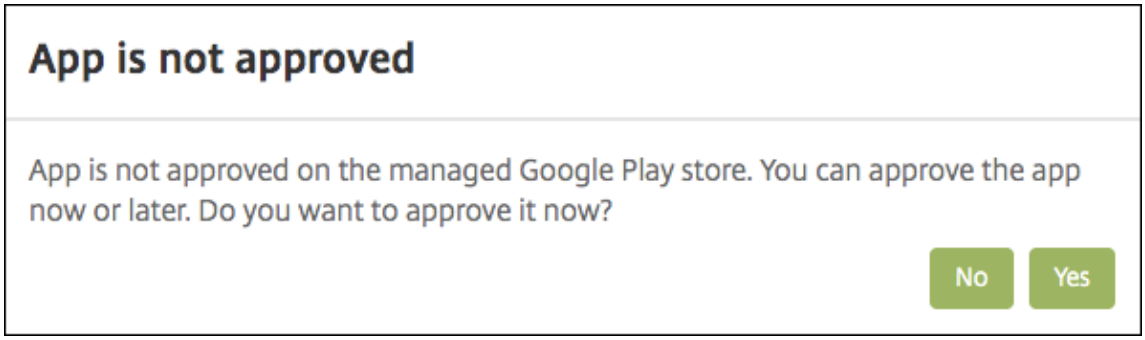
2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



3. Cliquez sur **MDX**. La page **Informations sur l'application** s'affiche.

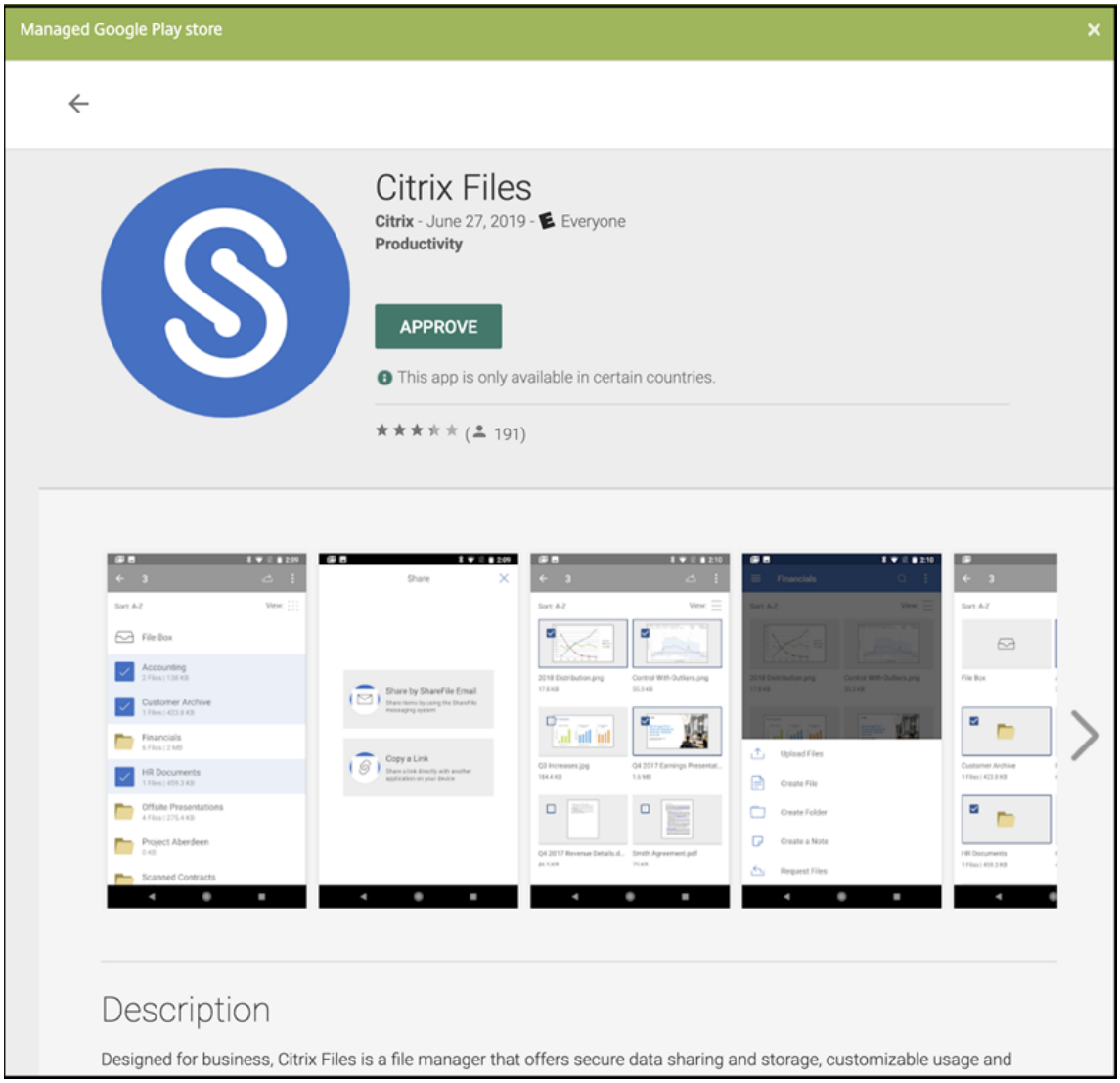
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. À gauche de la page, sélectionnez **Android Enterprise** comme plate-forme.
5. Sur la page **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous **Nom de l'application** dans le tableau **Applications**.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.
6. Cliquez sur **Suivant**. La page **Android Enterprise MDX App** s'affiche.
7. Cliquez sur **Charger** et accédez à l'emplacement des fichiers .mdx pour l'application. Sélectionnez le fichier et cliquez sur **Ouvrir**.
8. L'interface utilisateur vous avertit si l'application jointe nécessite l'approbation du Google Play Store d'entreprise. Pour approuver l'application sans quitter la console Citrix Endpoint Management, cliquez sur **Oui**.



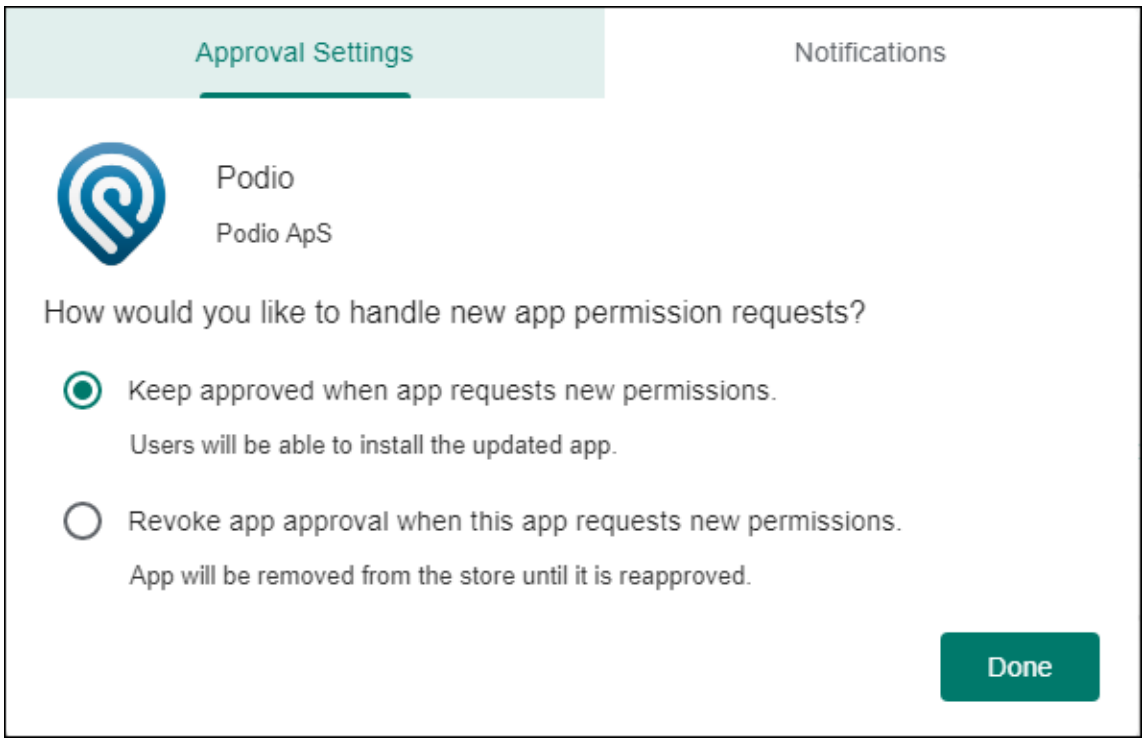
9. Lorsque la page Google Play Store d'entreprise s'ouvre, cliquez sur **Approuver**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



10. Cliquez à nouveau sur **Approuver**.
11. Sélectionnez **Maintenir l'état approuvé de cette application lorsqu'elle demande d'autres autorisations**. Cliquez sur **Save**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



12. Lorsque l'application est approuvée et enregistrée, d'autres paramètres apparaissent sur la page. Pour configurer ces paramètres :

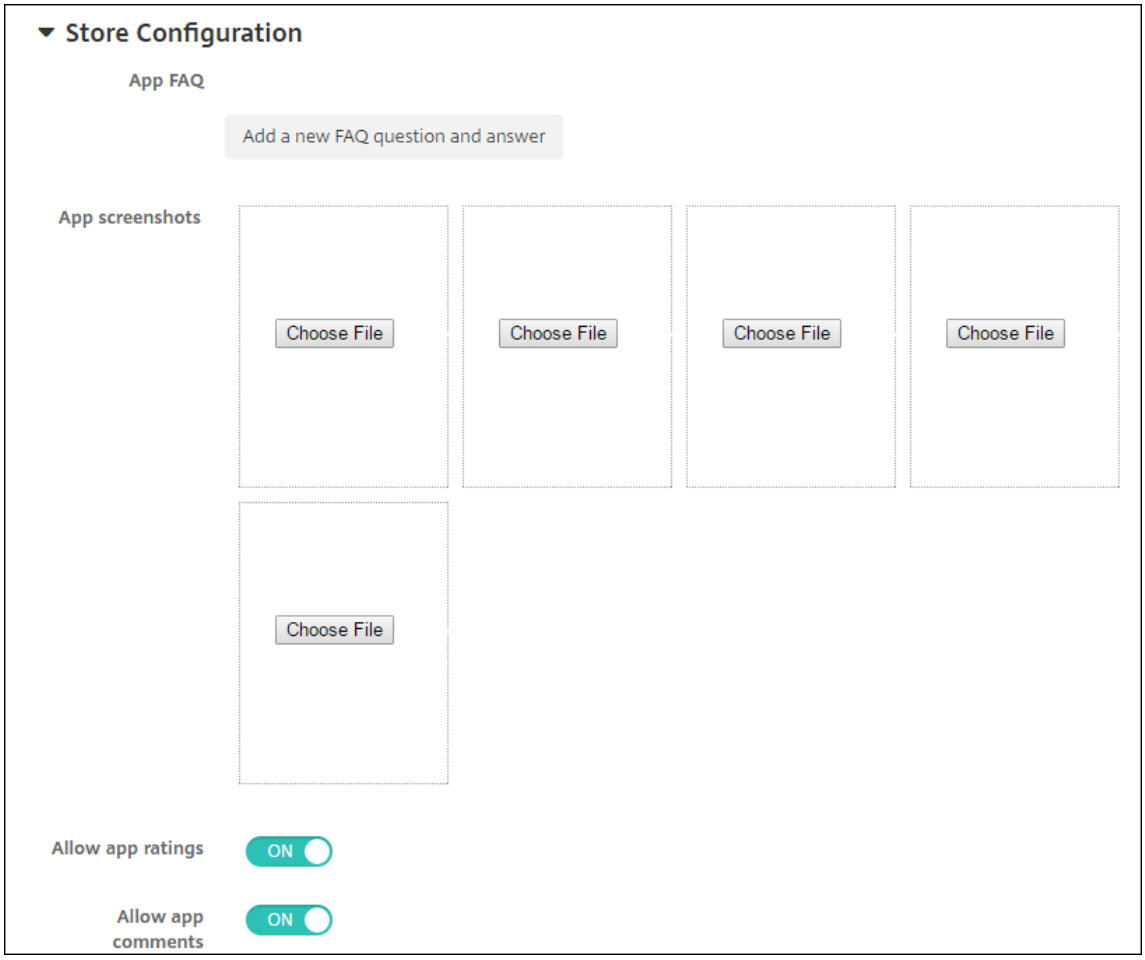
    - **Nom du fichier :** entrez le nom du fichier associé à l'application.
    - **Description de l'application :** entrez une description pour l'application.
    - **Suivi du produit :** spécifiez le suivi du produit que vous souhaitez transférer aux appareils utilisateur. Si vous avez un suivi conçu à des fins de test, vous pouvez le sélectionner et l'affecter à vos utilisateurs. La valeur par défaut est Production.
    - **Version de l'application :** si vous le souhaitez, entrez le numéro de version de l'application.
    - **ID de package :** URL de l'application dans le Google Play Store.
    - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
    - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
    - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou les modèles d'appareils qui ne peuvent pas exécuter l'application.

13. Configurez les **stratégies MDX**. Pour de plus amples informations sur les stratégies d'application pour applications MDX, veuillez consulter la section Synopsis des stratégies MDX et Présentation du SDK MAM.

14. Configurez les règles de déploiement. Pour de plus amples informations, consultez la section Déployer des ressources.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

15. Développez **Configuration du magasin**. Ce paramètre ne s'applique pas aux applications Android Enterprise, qui s'affichent uniquement dans Google Play d'entreprise.



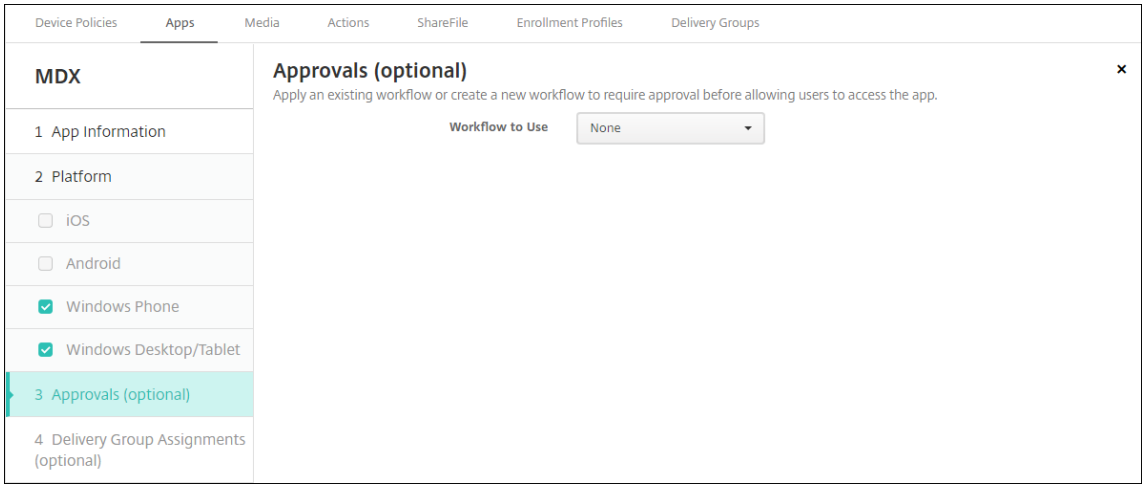
Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le magasin d'applications. Vous pouvez également indiquer si les utilisateurs peuvent évaluer ou ajouter des commentaires sur l'application.

- Pour configurer ces paramètres :
  - **FAQ sur les applications :** ajoutez des questions et réponses pour l'application.
  - **Copies d'écran des applications :** ajoutez des captures d'écran pour faciliter le classement de l'application dans le magasin d'applications. L'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.
  - **Autoriser notation des applications :** indiquez si un utilisateur peut évaluer l'application. La valeur par défaut est **Activé**.

    Autoriser commentaires sur les applications : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée. La valeur par défaut est **Activé**.

16. Cliquez sur **Suivant**. La page **Approbations** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Vous utilisez des workflows lorsque vous avez besoin d'une approbation pour créer des comptes d'utilisateur. Si vous ne souhaitez pas configurer des workflows d'approbation, vous pouvez passer à l'étape 15.

Configurez ces paramètres pour attribuer ou créer un workflow :

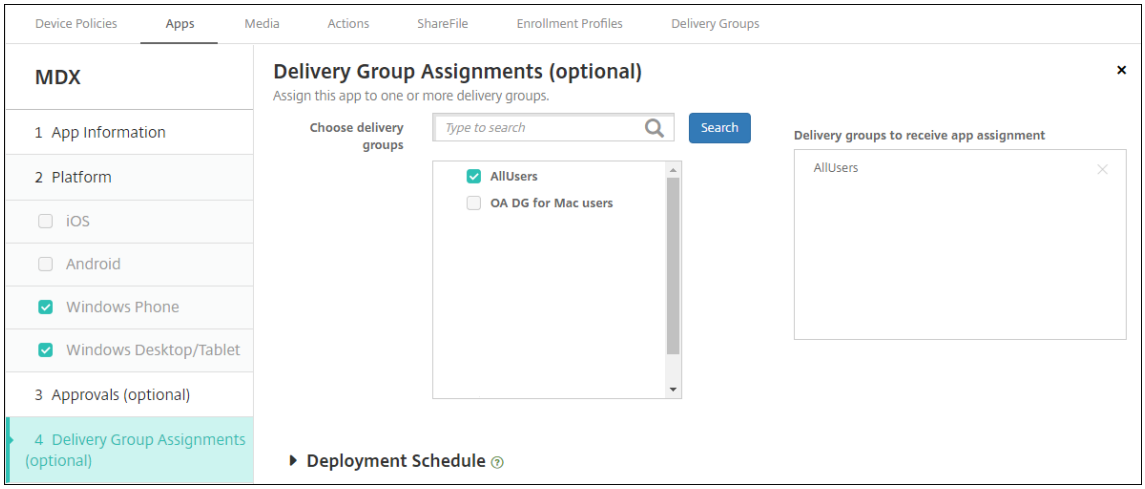
- **Workflow à utiliser :** dans la liste, cliquez sur un workflow existant ou cliquez sur **Créer un nouveau workflow**. La valeur par défaut est **Aucun**.
- Si vous sélectionnez **Créer un nouveau workflow**, configurez les paramètres suivants. Pour plus d'informations, consultez Créer et gérer des workflows.
- **Nom :** entrez un nom unique pour le workflow.
- **Description :** entrez une description pour le workflow (facultatif).
- **Modèles d'approbation d'e-mail :** dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Lorsque vous cliquez sur l'icône d'œil à droite du champ, une boîte de dialogue s'affiche dans laquelle vous pouvez afficher un aperçu du modèle.
- **Niveaux d'approbation par un responsable :** dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est 1 niveau. Les options possibles sont les suivantes :
  - Pas nécessaire
  - 1 niveau
  - 2 niveaux
  - 3 niveaux
- **Sélectionner un domaine Active Directory :** dans la liste, sélectionnez le domaine Active Directory à utiliser pour le workflow.
- **Rechercher des approbateurs supplémentaires requis :** tapez le nom de la personne dans le champ de recherche et cliquez sur **Rechercher**. Les noms proviennent d'Active Directory.
- Lorsque le nom s'affiche dans le champ, sélectionnez la case à cocher en regard du nom. Le nom et l'adresse e-mail s'affichent dans la liste **Approbateurs supplémentaires req-**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

uis sélectionnés.

- Pour supprimer une personne de la liste **Approbateurs supplémentaires requis sélectionnés**, procédez comme suit :
  * Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.
  * Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats de la recherche.
  * Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

17. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.



18. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

19. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

    - En regard de **Déployer**, cliquez sur **Activé** pour planifier le déploiement ou cliquez sur **Désactivé** pour empêcher le déploiement. L'option par défaut est **Activé**.
    - À côté du Calendrier de déploiement, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
    - Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    - En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- En regard de **Déployer pour les connexions permanentes**, assurez-vous que **Désactivé** est sélectionné. L'option par défaut est **Désactivé**. Les connexions toujours actives ne sont pas disponibles pour Android Enterprise pour les clients qui ont commencé à utiliser Citrix Endpoint Management avec la version 10.18.19 ou ultérieure. Nous ne recommandons pas ces connexions pour les clients qui ont commencé à utiliser Citrix Endpoint Management avant la version 10.18.19.

  Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

  Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

20. Cliquez sur **Save**.

Répétez les étapes pour chaque application de productivité mobile.

Configurer la stratégie de la question de sécurité

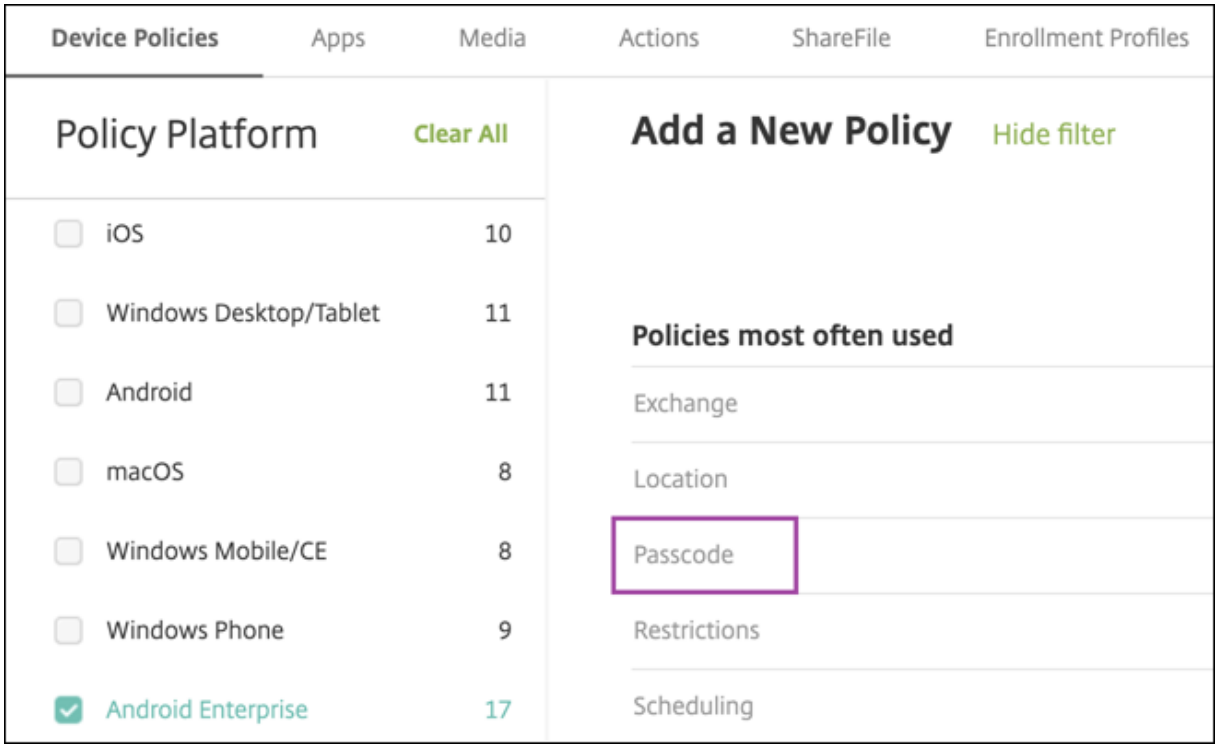
La stratégie de code secret d'appareil Citrix Endpoint Management configure des règles pour les questions de sécurité. Les questions de sécurité s'affichent lorsque les utilisateurs accèdent à leurs appareils ou aux profils professionnels Android Enterprise sur leurs appareils. Une question de sécurité peut être définie avec un mot de passe ou une reconnaissance biométrique. Pour plus d'informations sur la stratégie de code secret, consultez Stratégie de code secret.

- Si votre déploiement Android Enterprise inclut des appareils BYOD, configurez la stratégie de code secret pour le profil de travail.
- Si votre déploiement inclut des appareils entièrement gérés appartenant à l'entreprise, configurez la stratégie de code secret pour l'appareil lui-même.
- Si votre déploiement inclut les deux types d'appareils, configurez les deux types de stratégie de code secret.

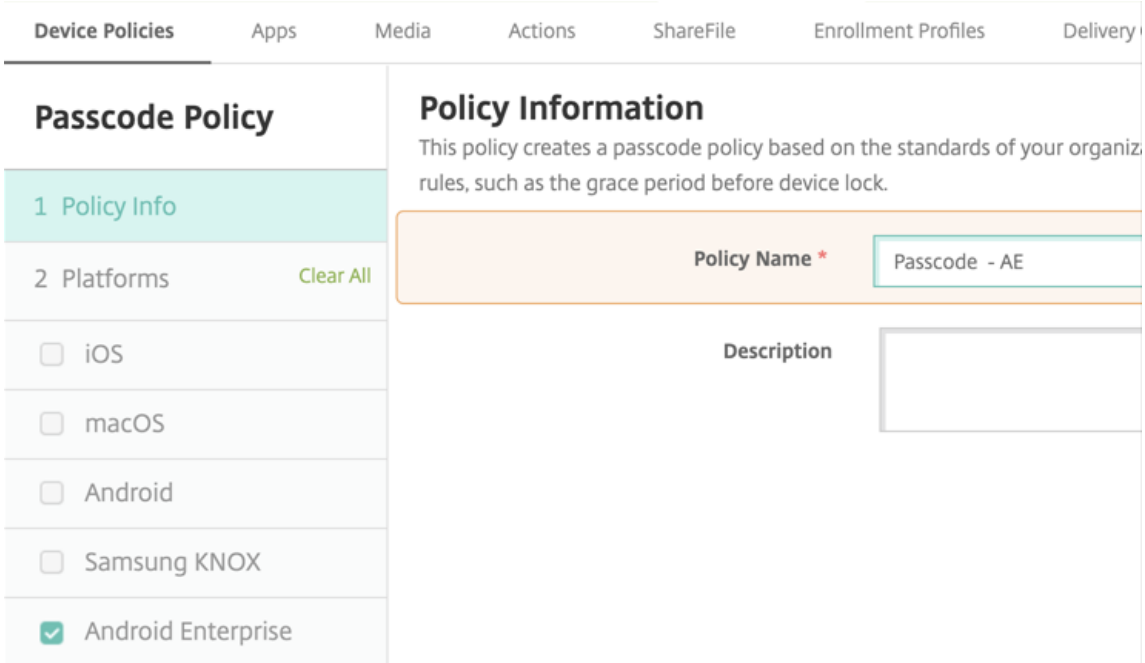
Pour configurer la stratégie de code secret, procédez comme suit :

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Stratégies d'appareil**.
2. Cliquez sur **Ajouter**.
3. Cliquez sur **Afficher le filtre** pour afficher le panneau **Stratégie par plate-forme**. Dans le panneau **Stratégie par plate-forme**, sélectionnez **Android Enterprise**.
4. Cliquez sur **Code secret** dans le panneau droit.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. Entrez un **nom de stratégie**. Cliquez sur **Suivant**.



2. Configurez les paramètres de la stratégie de code secret.

   - Définissez l'option **Code secret de l'appareil requis** sur **Activé** pour afficher les paramètres disponibles pour les questions de sécurité de l'appareil.
   - Définissez l'option **Question de sécurité du profil de travail requise** sur **Activé** pour af-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ficher les paramètres disponibles pour les questions de sécurité du profil de travail.

3. Cliquez sur **Suivant**.
4. Attribuez la stratégie à un ou plusieurs groupes de mise à disposition.
5. Cliquez sur **Save**.

Création de profils d'inscription

Les profils d'inscription contrôlent le mode d'inscription des appareils Android si Android Enterprise est activé pour votre déploiement Citrix Endpoint Management. Lorsque vous créez un profil d'inscription pour inscrire des appareils Android Enterprise, vous pouvez configurer le profil d'inscription pour inscrire de nouveaux appareils et des appareils réinitialisés en usine comme suit :

- Appareils entièrement gérés
- Appareils dédiés
- Entièrement géré avec un profil de travail/Profil de travail sur appareils appartenant à l'entreprise

Vous pouvez également configurer chacun de ces profils d'inscription Android Enterprise pour inscrire les appareils Android BYOD en tant qu'appareils avec profil de travail.

Si Android Entreprise est activé pour votre déploiement Citrix Endpoint Management, tous les appareils Android nouvellement inscrits ou réinscrits le sont en tant qu'appareils Android Entreprise. Par défaut, le profil d'inscription global inscrit les nouveaux appareils Android et les appareils soumis à une réinitialisation d'usine en tant qu'appareils entièrement gérés et les appareils Android BYOD en tant que profil de travail sur appareils appartenant à l'entreprise.

Lorsque vous créez des profils d'inscription, vous leur attribuez des groupes de mise à disposition. Si un utilisateur appartient à plusieurs groupes de mise à disposition qui ont des profils d'inscription différents, le nom du groupe de mise à disposition détermine le profil d'inscription utilisé. Citrix Endpoint Management sélectionne le groupe de mise à disposition qui apparaît en dernier dans une liste alphabétique des groupes de mise à disposition. Pour plus d'informations, voir Profils d'inscription.

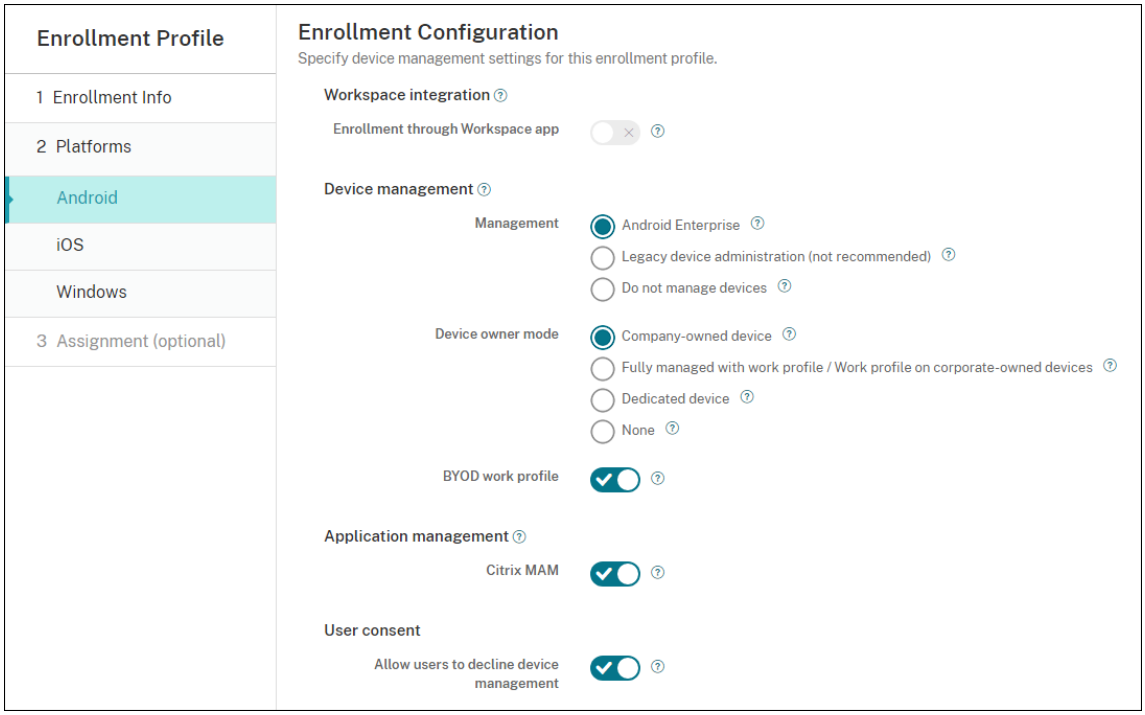
Ajouter un profil d'inscription pour les appareils entièrement gérés

Le profil d'inscription global inscrit les appareils entièrement gérés par défaut, mais vous pouvez créer d'autres profils d'inscription pour inscrire les appareils entièrement gérés.

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Profils d'inscription**.
2. Pour ajouter un profil d'inscription, cliquez sur **Ajouter**. Sur la page Infos d'inscription, entrez un nom pour le profil d'inscription.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Définissez le nombre d'appareils que les membres disposant de ce profil peuvent inscrire.
4. Sélectionnez **Android** sous **Plates-formes** ou cliquez sur **Suivant**. La page Configuration de l'inscription s'affiche.
5. Définissez **Gestion** sur **Android Enterprise**.
6. Définissez **Mode propriétaire de l'appareil** sur **Appareil appartenant à l'entreprise**.



7. Le **profil de travail BYOD** vous permet de configurer le profil d'inscription pour inscrire les appareils BYOD en tant qu'appareils avec profil de travail. Les nouveaux appareils et les appareils avec réinitialisation d'usine sont inscrits en tant qu'appareils entièrement gérés. Définissez le **profil de travail BYOD** sur **Activé** pour autoriser l'inscription d'appareils BYOD en tant qu'appareils avec profil de travail. Définissez le **profil de travail BYOD** sur **Désactivé** pour limiter l'inscription aux appareils entièrement gérés. La valeur par défaut est **Activé**.
8. Indiquez si vous souhaitez inscrire des appareils dans Citrix MAM.
9. Si vous définissez le **profil de travail BYOD** sur **Activé**, configurez le consentement de l'utilisateur. Pour autoriser les utilisateurs d'appareils avec profil de travail BYOD à refuser la gestion des appareils lorsqu'ils inscrivent leurs appareils, définissez **Autoriser les utilisateurs à décliner la gestion des appareils** sur **Activé**.

   Si le **profil de travail BYOD** est défini sur **Activé**, la valeur par défaut pour **Autoriser les utilisateurs à décliner la gestion des appareils** est **Activé**. Si le **profil de travail BYOD** est défini sur **Désactivé**, l'option **Autoriser les utilisateurs à décliner la gestion des appareils** est désactivée.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

10. Sélectionnez **Attribution (facultatif)**. L'écran Attribution de groupes de mise à disposition s'affiche.
11. Choisissez le(s) groupe(s) de mise à disposition contenant les administrateurs qui inscrivent les appareils entièrement gérés. Cliquez ensuite sur **Enregistrer**.

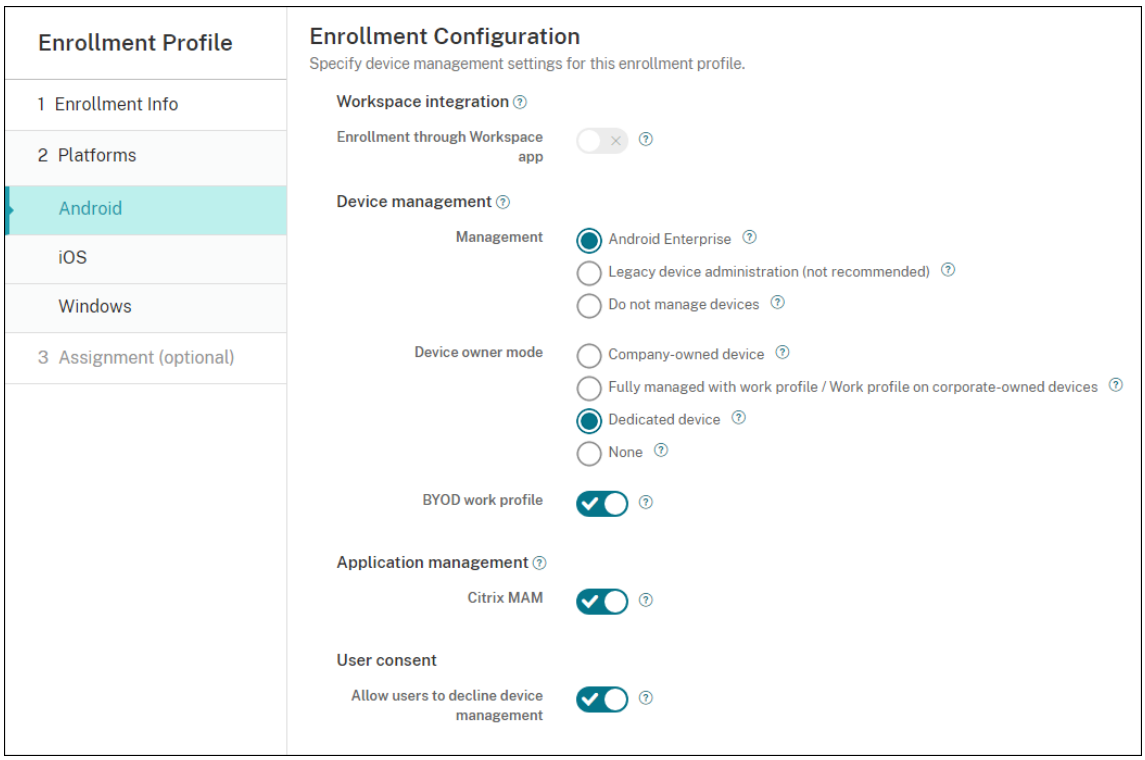
    La page Profil d'inscription apparaît avec le profil que vous avez ajouté.

Ajouter un profil d'inscription d'appareil dédié

Lorsque votre déploiement Citrix Endpoint Management inclut des appareils dédiés, un seul administrateur ou un groupe restreint d'administrateurs Citrix Endpoint Management peut inscrire de nombreux appareils dédiés. Pour vous assurer que ces administrateurs peuvent inscrire tous les appareils requis, créez un profil d'inscription pour eux avec un nombre illimité d'appareils autorisés par utilisateur.

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Profils d'inscription**.
2. Pour ajouter un profil d'inscription, cliquez sur **Ajouter**. Sur la page Infos d'inscription, entrez un nom pour le profil d'inscription. Définissez sur **Illimité** le nombre d'appareils que les membres disposant de ce profil peuvent inscrire.
3. Sélectionnez **Android** sous **Plates-formes** ou cliquez sur **Suivant**. La page Configuration de l'inscription s'affiche.
4. Définissez **Gestion** sur **Android Enterprise**.
5. Définissez **Mode propriétaire de l'appareil** sur **Appareil dédié**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Le **profil de travail BYOD** vous permet de configurer le profil d'inscription pour inscrire les appareils BYOD en tant qu'appareils avec profil de travail. Les nouveaux appareils et les appareils avec réinitialisation d'usine sont inscrits en tant qu'appareils dédiés. Définissez le **profil de travail BYOD** sur **Activé** pour autoriser l'inscription d'appareils BYOD en tant qu'appareils avec profil de travail. Définissez le **profil de travail BYOD** sur **Désactivé** pour limiter l'inscription aux appareils appartenant à l'entreprise. La valeur par défaut est **Activé**.
7. Indiquez si vous souhaitez inscrire des appareils dans Citrix MAM.
8. Si vous définissez le **profil de travail BYOD** sur **Activé**, configurez le consentement de l'utilisateur. Pour autoriser les utilisateurs d'appareils avec profil de travail BYOD à refuser la gestion des appareils lorsqu'ils inscrivent leurs appareils, définissez **Autoriser les utilisateurs à décliner la gestion des appareils** sur **Activé**.

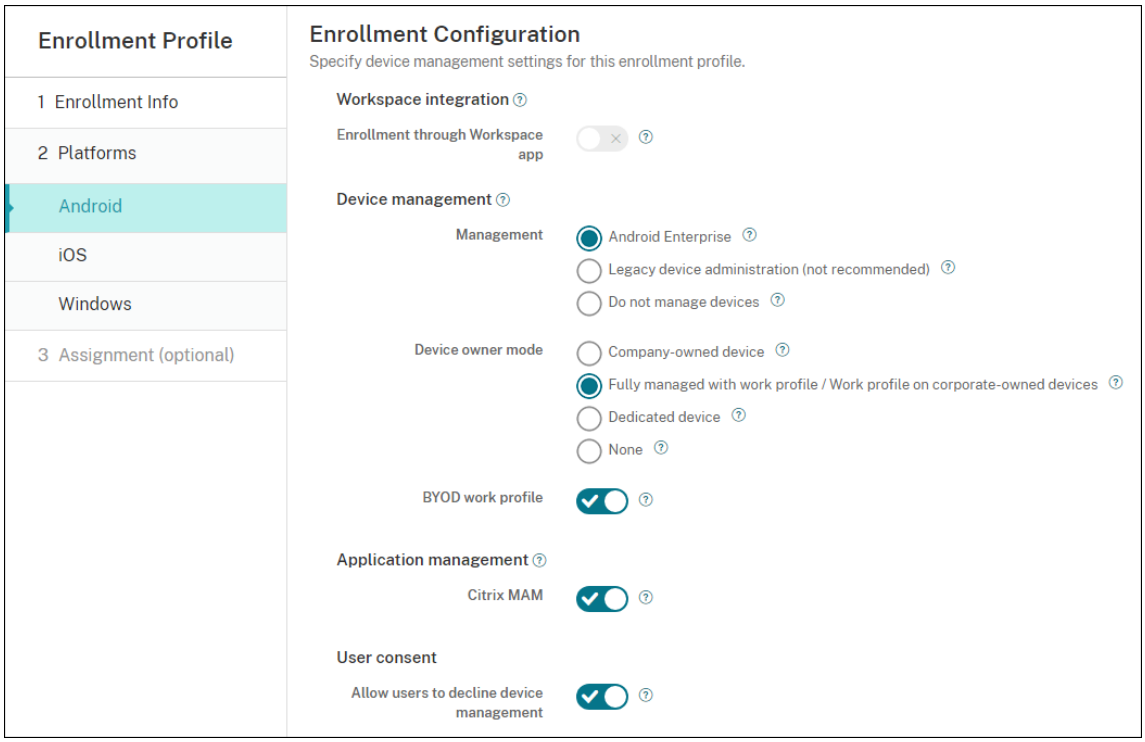
   Si le **profil de travail BYOD** est défini sur **Activé**, la valeur par défaut pour **Autoriser les utilisateurs à décliner la gestion des appareils** est **Activé**. Si le **profil de travail BYOD** est défini sur **Désactivé**, l'option **Autoriser les utilisateurs à décliner la gestion des appareils** est désactivée.
9. Sélectionnez **Attribution (facultatif)**. L'écran Attribution de groupes de mise à disposition s'affiche.
10. Choisissez le(s) groupe(s) de mise à disposition contenant les administrateurs qui inscrivent les appareils dédiés. Cliquez ensuite sur **Enregistrer**.

    La page Profil d'inscription apparaît avec le profil que vous avez ajouté.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ajouter un profil d'inscription pour les appareils entièrement gérés avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Profils d'inscription**.
2. Pour ajouter un profil d'inscription, cliquez sur **Ajouter**. Sur la page Infos d'inscription, entrez un nom pour le profil d'inscription.
3. Définissez le nombre d'appareils que les membres disposant de ce profil peuvent inscrire.
4. Sélectionnez **Android** sous **Plates-formes** ou cliquez sur **Suivant**. La page Configuration de l'inscription s'affiche.
5. Définissez **Gestion** sur **Android Enterprise**. Définissez l'option **Mode propriétaire de l'appareil** sur **Entièrement géré avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise**.



6. Le **profil de travail BYOD** vous permet de configurer le profil d'inscription pour inscrire les appareils BYOD en tant qu'appareils avec profil de travail. Les nouveaux appareils et les appareils avec réinitialisation d'usine sont inscrits en tant qu'appareils entièrement gérés avec profil de travail. Définissez le **profil de travail BYOD** sur **Activé** pour autoriser l'inscription d'appareils BYOD en tant qu'appareils avec profil de travail. Définissez le **profil de travail BYOD** sur **Désactivé** pour limiter l'inscription aux appareils dédiés. La valeur par défaut est **Off**.
7. Indiquez si vous souhaitez inscrire des appareils dans Citrix MAM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. Si vous définissez le **profil de travail BYOD** sur **Activé**, configurez le consentement de l'utilisateur. Pour autoriser les utilisateurs d'appareils avec profil de travail BYOD à refuser la gestion des appareils lorsqu'ils inscrivent leurs appareils, définissez **Autoriser les utilisateurs à décliner la gestion des appareils** sur **Activé**.

   Si le **profil de travail BYOD** est défini sur **Activé**, la valeur par défaut pour **Autoriser les utilisateurs à décliner la gestion des appareils** est **Activé**. Si le **profil de travail BYOD** est défini sur **Désactivé**, l'option **Autoriser les utilisateurs à décliner la gestion des appareils** est désactivée.

9. Sélectionnez **Attribution (facultatif)**. L'écran Attribution de groupes de mise à disposition s'affiche.

10. Choisissez le(s) groupe(s) de mise à disposition contenant les administrateurs qui inscrivent les appareils entièrement gérés avec un profil de travail. Cliquez ensuite sur **Enregistrer**.

    La page Profil d'inscription apparaît avec le profil que vous avez ajouté.

Ajout d'un profil d'inscription pour les appareils d'ancienne génération

Google ne prend plus en charge le mode administrateur de l'appareil pour la gestion des appareils. Google encourage les clients à gérer tous les appareils Android en mode propriétaire de l'appareil ou propriétaire de profil. (Consultez la section Device admin deprecation dans les guides des développeurs Google Android Enterprise.)

Pour prendre en charge ce changement :

- Citrix définit Android Enterprise comme option d'inscription par défaut pour les appareils Android.
- Si Android Entreprise est activé pour votre déploiement Citrix Endpoint Management, tous les appareils Android nouvellement inscrits ou réinscrits le sont en tant qu'appareils Android Entreprise.

Votre organisation n'est peut-être pas prête à gérer les appareils Android d'ancienne génération à l'aide d'Android Enterprise. Dans ce cas, vous pouvez continuer à les gérer en mode Administrateur de l'appareil. Si des appareils sont déjà inscrits en mode administrateur d'appareil, Citrix Endpoint Management continue de les gérer en mode administrateur d'appareil.

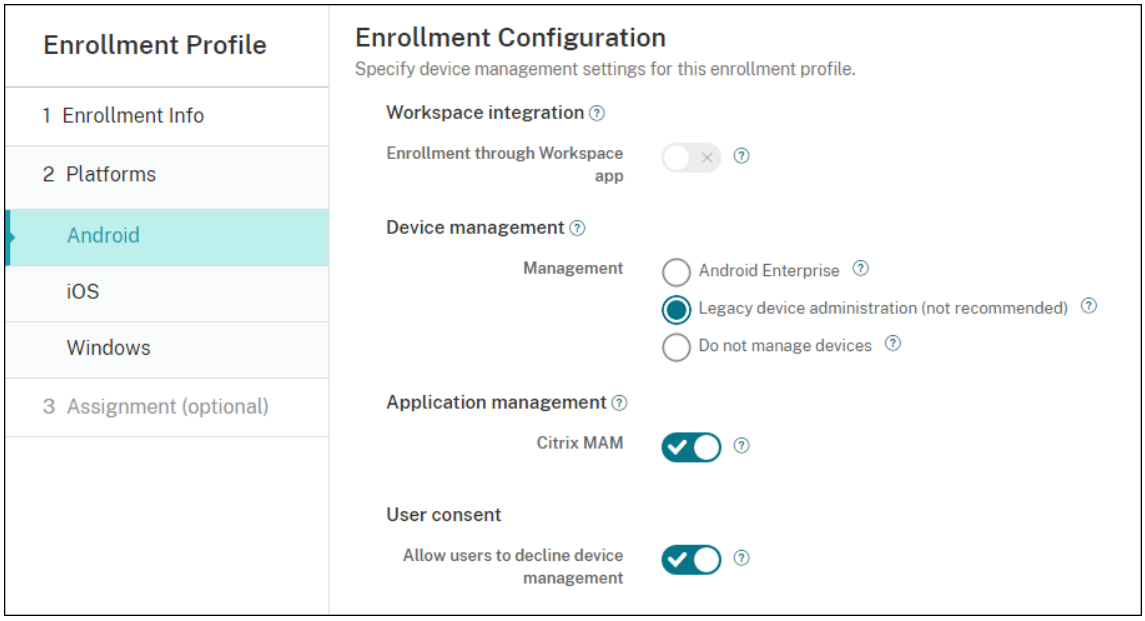
Créez un profil d'inscription pour les appareils hérités afin de permettre aux inscriptions de nouveaux appareils Android d'utiliser le mode administrateur d'appareil.

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

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Profils d'inscription**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Pour ajouter un profil d'inscription, cliquez sur **Ajouter**. Sur la page Infos d'inscription, entrez un nom pour le profil d'inscription.
3. Définissez le nombre d'appareils que les membres disposant de ce profil peuvent inscrire.
4. Sélectionnez **Android** sous **Plates-formes** ou cliquez sur **Suivant**. La page Configuration de l'inscription s'affiche.
5. Définissez **Gestion** sur **Administration des appareils d'ancienne génération (non recommandé)**. Cliquez sur **Suivant**.



6. Indiquez si vous souhaitez inscrire des appareils dans Citrix MAM.
7. Pour autoriser les utilisateurs à refuser la gestion des appareils lorsqu'ils inscrivent leurs appareils, définissez **Autoriser les utilisateurs à décliner la gestion des appareils** sur **Activé**. La valeur par défaut est **Activé**.
8. Sélectionnez **Attribution (facultatif)**. L'écran Attribution de groupes de mise à disposition s'affiche.
9. Choisissez le(s) groupe(s) de mise à disposition contenant les administrateurs qui inscrivent les appareils dédiés. Cliquez ensuite sur **Enregistrer**.

La page Profil d'inscription apparaît avec le profil que vous avez ajouté.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Provisioning d'appareils Android Enterprise avec profil de travail

Les appareils Android Enterprise avec profil de travail sont inscrits en mode Propriétaire du profil. Ces appareils n'ont pas besoin d'être neufs ou réinitialisés en usine. Les appareils BYOD sont inscrits en tant qu'appareils avec profil de travail. L'expérience d'inscription est similaire à l'inscription Android dans Citrix Endpoint Management. Les utilisateurs téléchargent Citrix Secure Hub depuis Google Play et inscrivent leurs appareils.

Par défaut, les paramètres **Débogage USB et Sources inconnues** sont désactivés sur un appareil lorsque vous inscrivez l'appareil dans Android Entreprise en tant qu'appareil avec profil de travail.

Lors de l'inscription d'appareils dans Android Enterprise en tant qu'appareils avec profil de travail, accédez toujours à Google Play. De là, activez l'affichage de Citrix Secure Hub dans le profil personnel de l'utilisateur.

Provisionner des appareils Android Enterprise entièrement gérés

Vous pouvez inscrire des appareils entièrement gérés dans le déploiement que vous avez configuré dans les sections précédentes. Les appareils entièrement gérés sont des appareils appartenant à l'entreprise et sont inscrits en mode Propriétaire de l'appareil. Seuls les appareils neufs ou qui ont fait l'objet d'une réinitialisation d'usine peuvent être inscrits en mode Propriétaire de l'appareil.

Vous pouvez inscrire des appareils en mode Propriétaire de l'appareil à l'aide de l'une des méthodes d'inscription suivantes :

- **Jeton d'identification DPC :** cette méthode d'inscription permet aux utilisateurs de saisir les caractères `afw#xenmobile` lors de la configuration de l'appareil. `afw#xenmobile` représente le jeton d'identification DPC Citrix. Ce jeton identifie l'appareil comme étant géré par Citrix Endpoint Management et télécharge Citrix Secure Hub depuis Google Play Store. Consultez Inscription d'appareils à l'aide du jeton d'identificateur DPC Citrix.
- **Partage de données à l'aide de NFC :** la méthode d'inscription à l'aide du partage NFC permet de transférer des données entre deux appareils en utilisant une communication en champ proche. Bluetooth, Wi-Fi et les autres modes de communication sont désactivés sur un nouvel appareil ou un appareil dont les paramètres d'usine ont été réinitialisés. NFC est le seul protocole de communication que l'appareil peut utiliser dans cet état. Consultez Inscription d'appareils à l'aide du partage NFC.
- **Code QR :** l'inscription à l'aide d'un code QR permet d'inscrire une flotte distribuée d'appareils qui ne prennent pas en charge la technologie NFC, tels que les tablettes. La méthode d'inscription à l'aide d'un code QR permet de configurer le mode Profil de l'appareil en scannant un code QR depuis l'assistant d'installation. Consultez Inscription d'appareils à l'aide d'un code QR.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Inscription sans contact :** l'inscription sans contact vous permet de configurer les appareils pour qu'ils s'inscrivent automatiquement lorsqu'ils sont mis sous tension pour la première fois. L'inscription sans contact est prise en charge sur certains appareils Android exécutant Android 9.0 ou version ultérieure. Consultez Inscription sans contact.
- **Comptes Google :** les utilisateurs saisissent leurs informations d'identification de compte Google pour démarrer le processus de provisioning. Cette option est destinée aux entreprises utilisant Google Workspace.

Inscription d'appareils à l'aide du jeton d'identificateur DPC Citrix

Les utilisateurs entrent `afw#xenmobile` lorsqu'ils sont invités à entrer un compte Google après avoir mis sous tension un nouvel appareil ou un appareil ayant fait l'objet d'une réinitialisation d'usine lors de la configuration initiale. Cette action télécharge et installe Citrix Secure Hub. Les utilisateurs suivent les invites de configuration de Citrix Secure Hub pour terminer l'inscription.

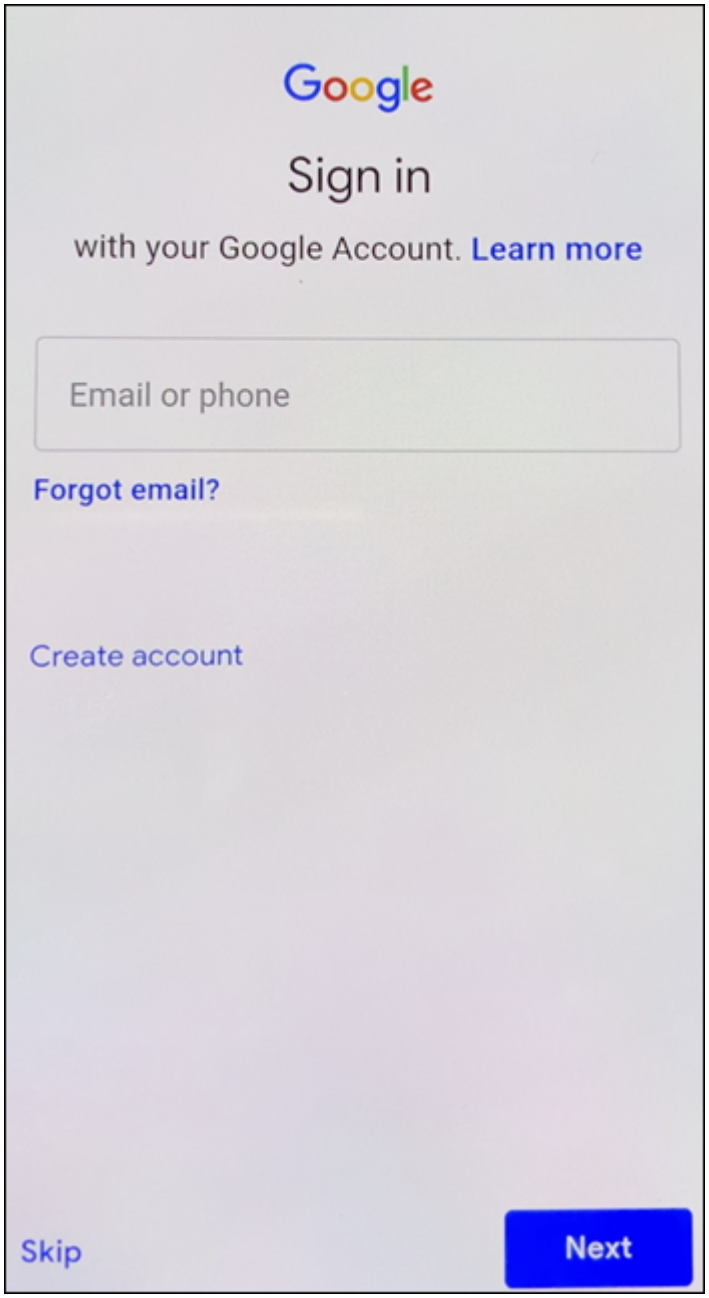
Configuration système requise

- Pris en charge sur tous les appareils Android exécutant Android OS.

Pour inscrire l'appareil

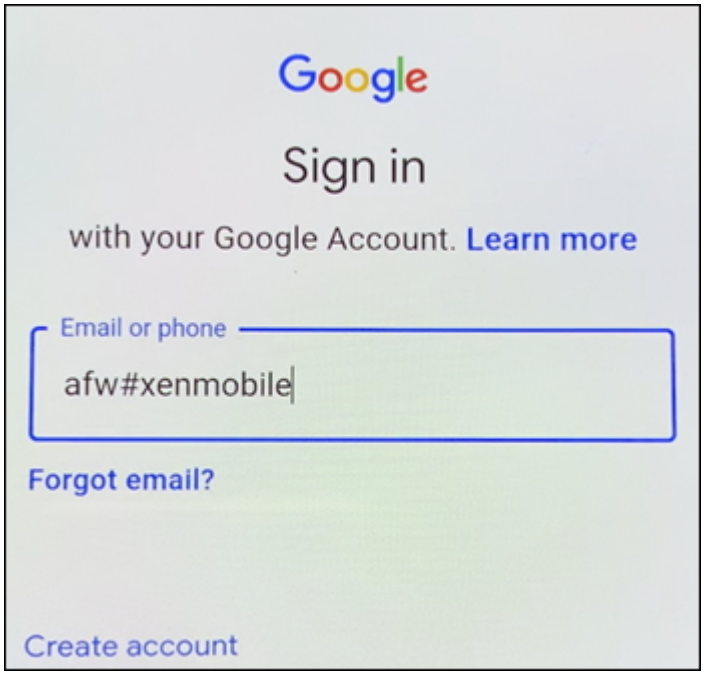
1. Mettez sous tension un nouvel appareil ou un appareil ayant fait l'objet d'une réinitialisation d'usine.
2. La configuration initiale de l'appareil s'affiche et vous invite à créer un compte Google. Si l'appareil affiche l'écran d'accueil, vérifiez dans la barre de notification une notification indiquant **Terminer la configuration**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



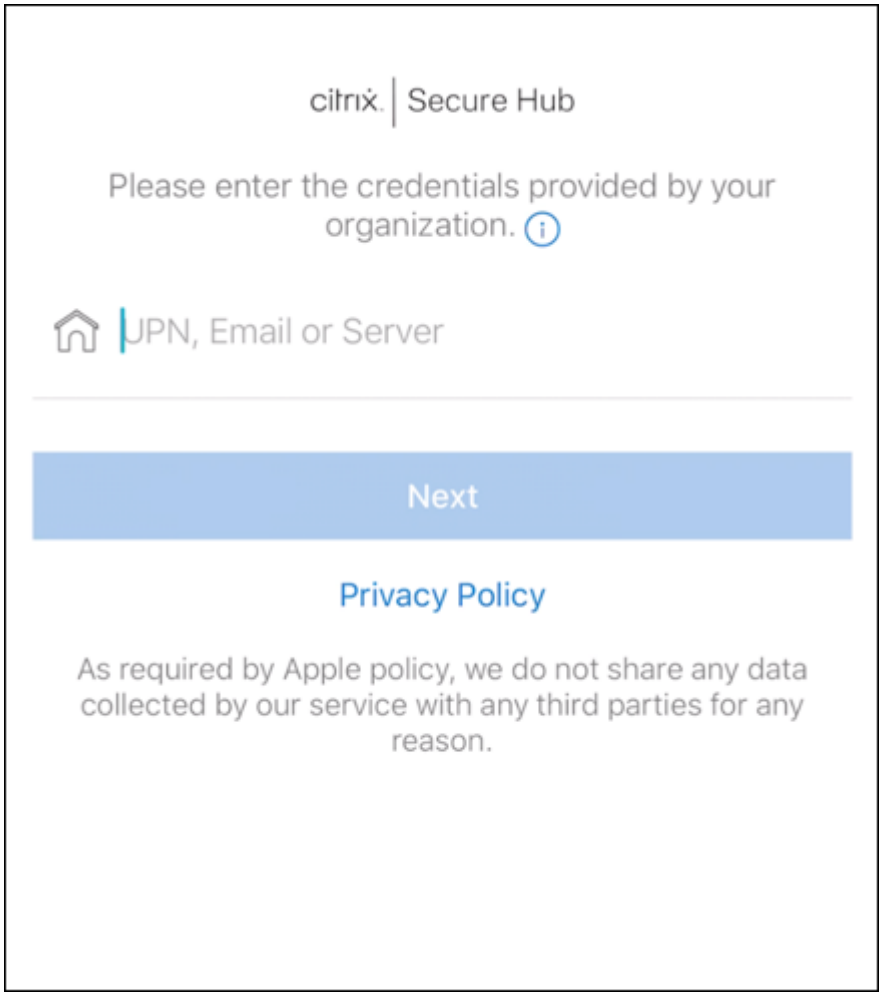
3. Entrez `afw#xenmobile` dans le champ **Adresse e-mail ou numéro de téléphone**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



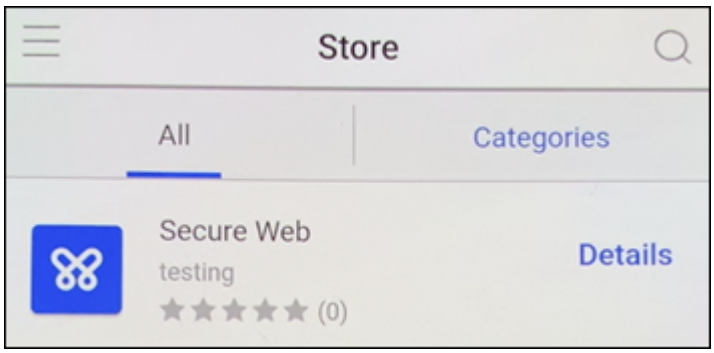
4. Touchez **Installer** sur l'écran Android Enterprise vous invitant à installer Citrix Secure Hub.
5. Touchez **Installer** sur l'écran du programme d'installation de Citrix Secure Hub.
6. Touchez **Autoriser** pour toutes les demandes d'autorisation d'application.
7. Touchez **Accepter et continuer** pour installer Citrix Secure Hub et lui permettre de gérer l'appareil.
8. Citrix Secure Hub est maintenant installé et s'affiche sur l'écran d'inscription par défaut. Dans cet exemple, la détection automatique n'est pas configurée. Si c'est le cas, lorsque l'utilisateur entre son nom d'utilisateur et son adresse e-mail, un serveur est automatiquement identifié. Entrez plutôt l'URL d'inscription de l'environnement et touchez **Suivant**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

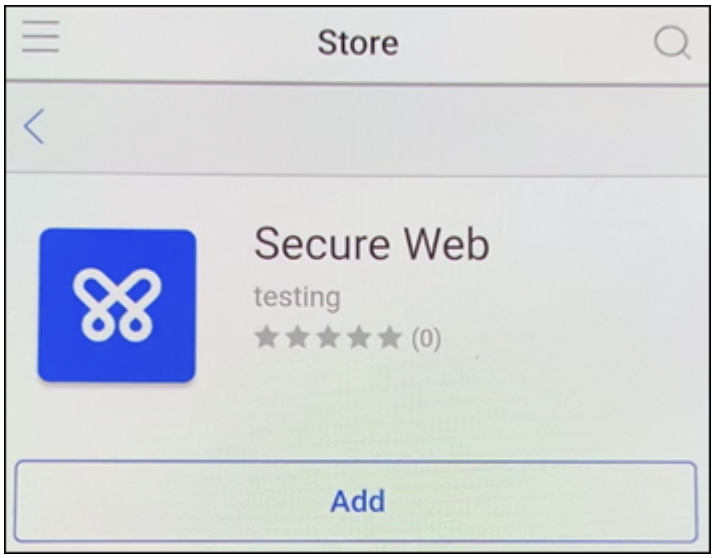


9. La configuration par défaut de Citrix Endpoint Management permet aux utilisateurs de choisir s'ils utilisent MAM ou MDM+MAM. Si vous y êtes invité, touchez **Oui, inscrire** pour choisir MDM+MAM.
10. Entrez l'adresse e-mail et le mot de passe de l'utilisateur, puis touchez **Suivant**.
11. L'utilisateur est invité à configurer un code secret pour l'appareil. Touchez **Définir** et saisissez un code secret.
12. L'utilisateur est invité à configurer une méthode de déverrouillage pour le profil de travail. Pour cet exemple, touchez **Mot de passe**, **Code PIN** et saisissez un code PIN.
13. L'appareil se trouve maintenant sur l'écran d'accueil **Mes applications** de Citrix Secure Hub. Touchez **Ajouter des applications depuis le magasin**.
14. Pour ajouter Citrix Secure Web, touchez **Citrix Secure Web**.

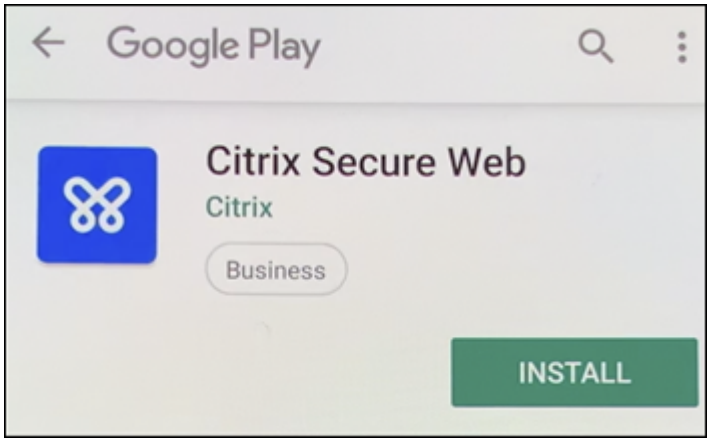
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



15. Touchez **Ajouter**.

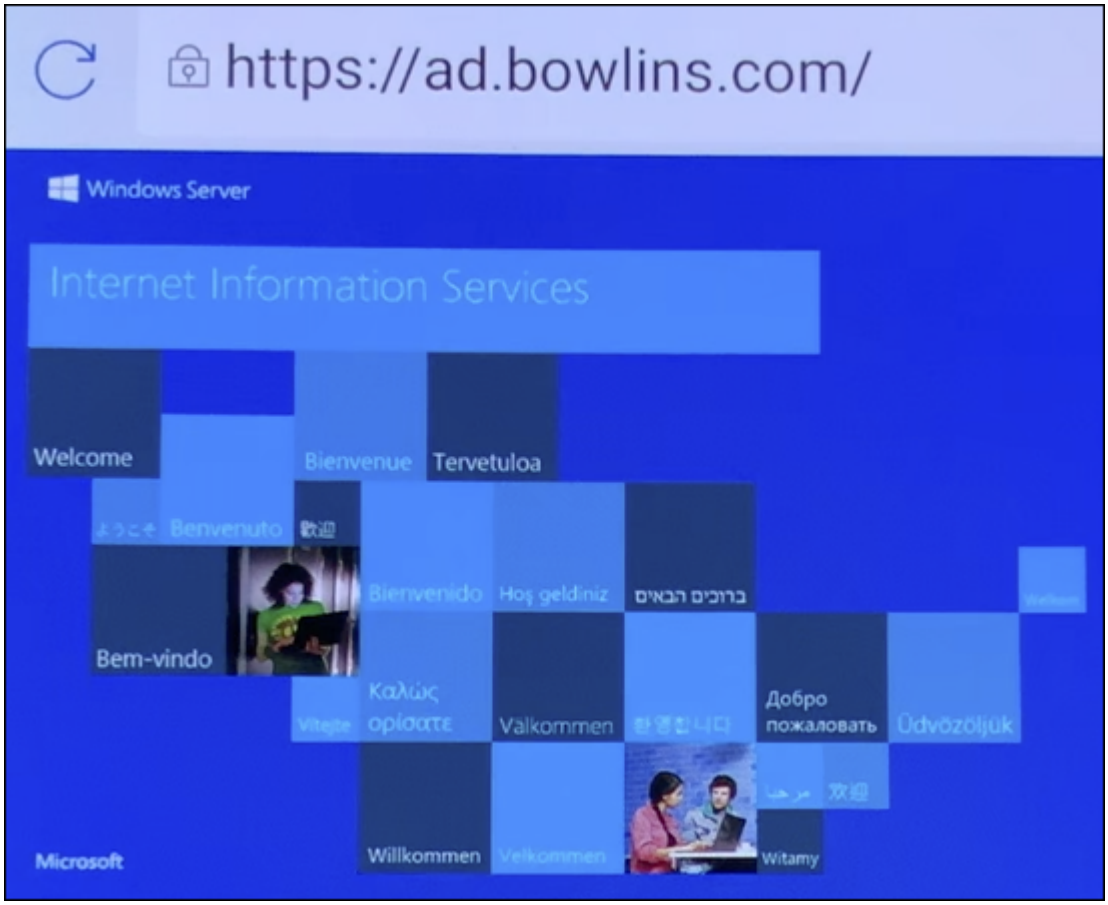


16. Citrix Secure Hub dirige l'utilisateur vers Google Play Store pour installer Citrix Secure Web. Appuyez sur **Installer**.



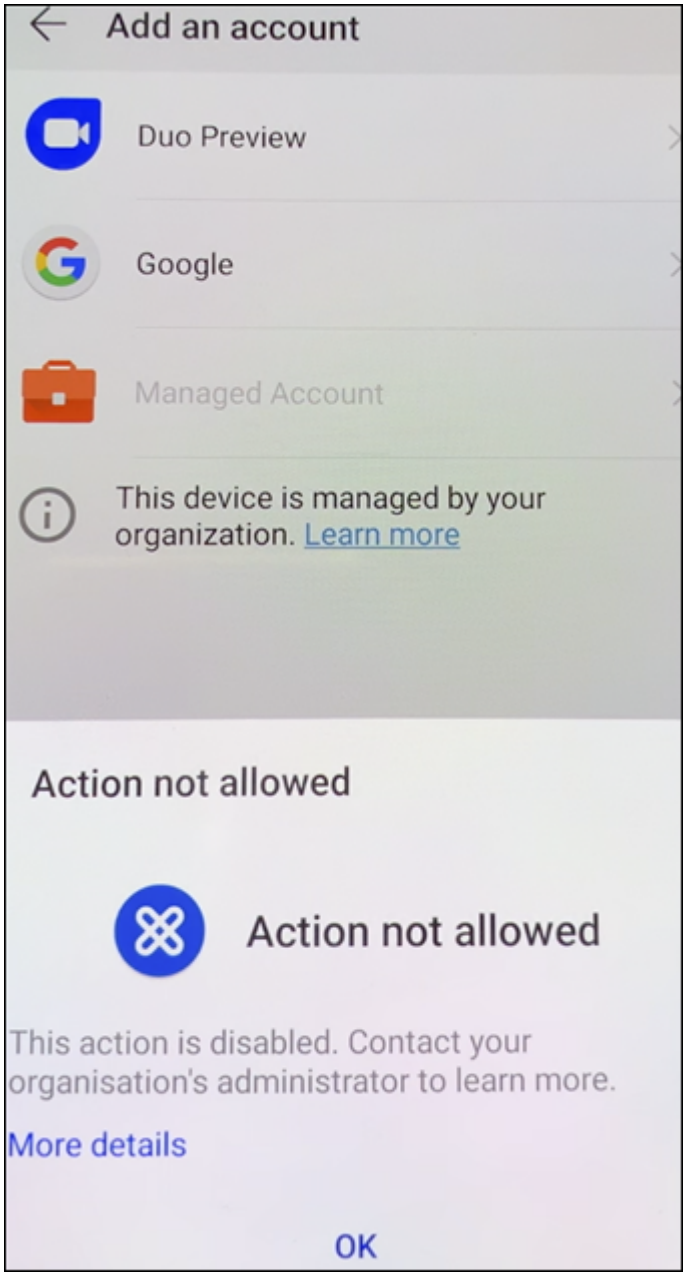
17. Après l'installation de Citrix Secure Web, touchez **Ouvrir**. Entrez une URL d'un site interne dans la barre d'adresse et vérifiez que la page se charge.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



18. Accédez à **Paramètres > Comptes** sur l'appareil. Notez que le **compte géré** ne peut pas être modifié. Les options destinées aux développeurs, telles que le partage d'écran ou le débogage à distance, sont également bloquées.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Inscription d'appareils à l'aide du partage NFC

Pour inscrire un appareil en tant qu'appareil entièrement géré à l'aide du partage NFC, deux appareils sont requis : un dont les paramètres d'usine ont été rétablis et un exécutant l'application Citrix Endpoint Management Provisioning Tool.

Configuration système requise et conditions préalables

- Appareils Android pris en charge

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Un nouvel appareil ou un appareil dont les paramètres d'usine ont été rétablis, disposant de la capacité NFC, provisionné pour Android Enterprise en tant qu'appareil entièrement géré. Consultez la section Provisionner des appareils Android Enterprise entièrement gérés.
- Un autre appareil disposant de la capacité NFC, exécutant l'application Provisioning Tool configurée. Provisioning Tool est disponible dans Citrix Secure Hub ou sur la page des téléchargements de Citrix.

Chaque appareil ne peut avoir qu'un seul profil Android Enterprise. Dans ce cas, le profil est destiné à l'instance Citrix Secure Hub gérée. La tentative d'ajout d'une deuxième application DPC supprime le Citrix Secure Hub installé.

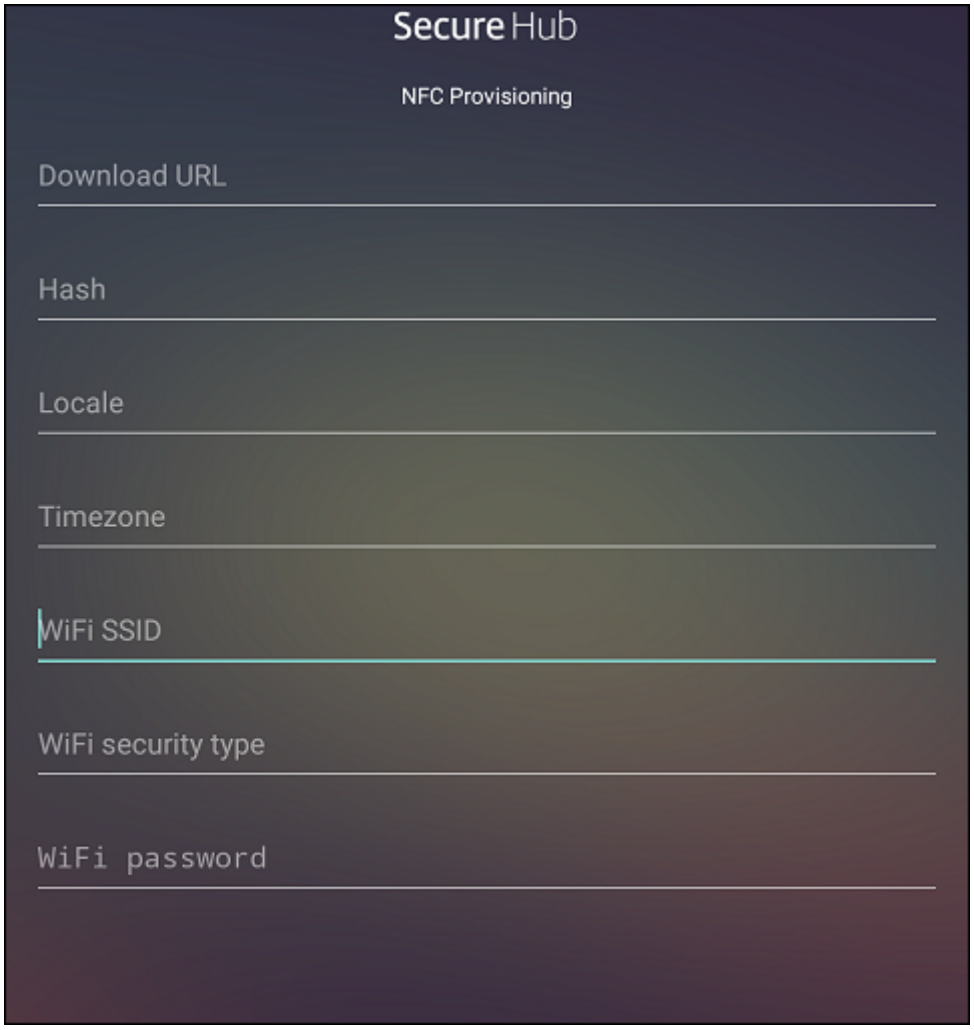
Données transférées via le partage NFC Le provisioning d'un appareil dont les paramètres d'usine ont été rétablis requiert l'envoi des données suivantes via NFC pour initialiser Android Enterprise :

- Nom du package de l'application DPC qui fait office de propriétaire de l'appareil (dans ce cas, Citrix Secure Hub).
- Emplacement intranet/Internet à partir duquel l'appareil peut télécharger l'application DPC.
- Hachage SHA256 de l'application DPC pour vérifier que le téléchargement a réussi.
- Détails de la connexion Wi-Fi de façon à ce qu'un appareil dont les paramètres d'usine ont été réinitialisés puisse se connecter et télécharger l'application DPC. Remarque : Android ne prend pas charge 802.1x Wi-Fi pour cette étape.
- Fuseau horaire de l'appareil (facultatif).
- Emplacement géographique de l'appareil (facultatif).

Lorsque les deux appareils sont « cognés », les données de Provisioning Tool sont envoyées à l'appareil dont les paramètres d'usine ont été réinitialisés. Ces données sont ensuite utilisées pour télécharger Citrix Secure Hub avec des paramètres d'administrateur. Si vous ne précisez pas le fuseau horaire ni l'emplacement, Android les configure automatiquement sur le nouvel appareil.

Configuration d'Citrix Endpoint Management Provisioning Tool Avant de partager des données avec NFC, vous devez configurer Provisioning Tool. Cette configuration est ensuite transférée à l'appareil dont les paramètres d'usine ont été réinitialisés durant le partage des données avec NFC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Vous pouvez entrer des données dans les champs requis ou les renseigner via un fichier texte. Les étapes de la procédure suivante décrivent comment configurer le fichier texte et contiennent des descriptions pour chaque champ. L'application n'enregistre pas les informations après qu'elles soient entrées, il peut donc s'avérer utile de créer un fichier texte afin de conserver les informations pour une utilisation ultérieure.

Pour configurer le Provisioning Tool à l'aide d'un fichier texte Appelez le fichier nfcprovisioning.txt et placez-le dans le dossier `/sdcard/` sur la carte SD de l'appareil. Cela permet à l'application de lire le fichier texte et renseigner les valeurs.

Le fichier texte doit contenir les données suivantes :

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=<download_location>
```

Il s'agit de l'emplacement intranet/Internet de l'application EMM du fournisseur. Après que l'appareil dont les paramètres d'usine ont été réinitialisés se soit connecté au Wi-Fi suite au partage NFC, il doit

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

avoir accès à cet emplacement pour le téléchargement. L'adresse URL est une adresse URL standard qui ne requiert aucun formatage spécial.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>`

Il s'agit de la somme de contrôle de l'application EMM du fournisseur. Elle est utilisée pour vérifier que le téléchargement a réussi. Les étapes à suivre pour obtenir la somme de contrôle sont abordées plus loin dans cet article.

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

Cette ligne est le SSID Wi-Fi connecté de l'appareil sur lequel Provisioning Tool est exécuté.

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

Les valeurs prises en charge sont WEP et WPA2. Si le Wi-Fi n'est pas protégé, ce champ doit être vide.

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

Si le Wi-Fi n'est pas protégé, ce champ doit être vide.

`android.app.extra.PROVISIONING_LOCALE=<locale>`

Entrez un code de langue et de pays. Les codes de langue sont des codes ISO de deux lettres minuscules (tels que fr) comme défini dans l'ISO 639-1. Les codes de pays sont des codes ISO de deux lettres majuscules (tels que FR) comme défini dans l'ISO 3166-1. À titre d'exemple, entrez fr_FR pour la langue française parlée en France. Si vous n'entrez aucun code, la langue et le pays sont automatiquement renseignés.

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

Fuseau horaire dans lequel l'appareil est exécuté. Tapez le nom de la base de données de la région/emplacement. Par exemple, tapez **Europe/Paris** pour l'heure de l'Europe occidentale. Si vous n'entrez rien, le fuseau horaire est automatiquement renseigné.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

Ces données ne pas requises car la valeur est codée en dur dans l'application Citrix Secure Hub. Il n'est mentionné ici que par souci de complétude.

Si un accès protégé Wi-Fi WPA2 est utilisé, un fichier nfcprovisioning.txt peut ressembler à ce qui suit :

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR
\u003d
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles

Si un accès non protégé Wi-Fi est utilisé, un fichier nfcprovisioning.txt peut ressembler à ce qui suit :

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION =https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR \u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles

Pour obtenir la somme de contrôle de Citrix Secure Hub La somme de contrôle de Citrix Secure Hub est une valeur constante : qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM. Pour télécharger un fichier APK pour Citrix Secure Hub, utilisez le lien suivant de Google Play Store : https://play.google.com/managed/downloadManagingApp?identifier=xenmobile.

Pour obtenir une somme de contrôle d'application Pré-requis :

- L'outil **apksigner** de l'Android SDK Build Tools
- Ligne de commande OpenSSL

Pour obtenir la somme de contrôle d'une application, procédez comme suit :

1. Téléchargez le fichier APK de l'application depuis le Google Play Store.
2. Dans la ligne de commande OpenSSL, accédez à l'outil **apksigner** : android-sdk/build-tools/<version>/apksigner et tapez ce qui suit :

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{
 (?<=SHA-256 digest:) .* }
 '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
<!--NeedCopy-->
```

La commande renvoie une somme de contrôle valide.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Pour générer le code QR, saisissez la somme de contrôle dans le champ `PROVISIONING_DEVICE_ADMIN_` . Par exemple :

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"
    }

 }

<!--NeedCopy-->
```

Bibliothèques utilisées Provisioning Tool utilise les bibliothèques suivantes dans son code source :

- Bibliothèque v7 `appcompat`, bibliothèque Design Support et bibliothèque v7 Palette Support par Google sous licence Apache 2.0

  Pour plus d'informations, consultez le Guide des fonctionnalités de la bibliothèque de support.

- Butter Knife par Jake Wharton sous licence Apache 2.0

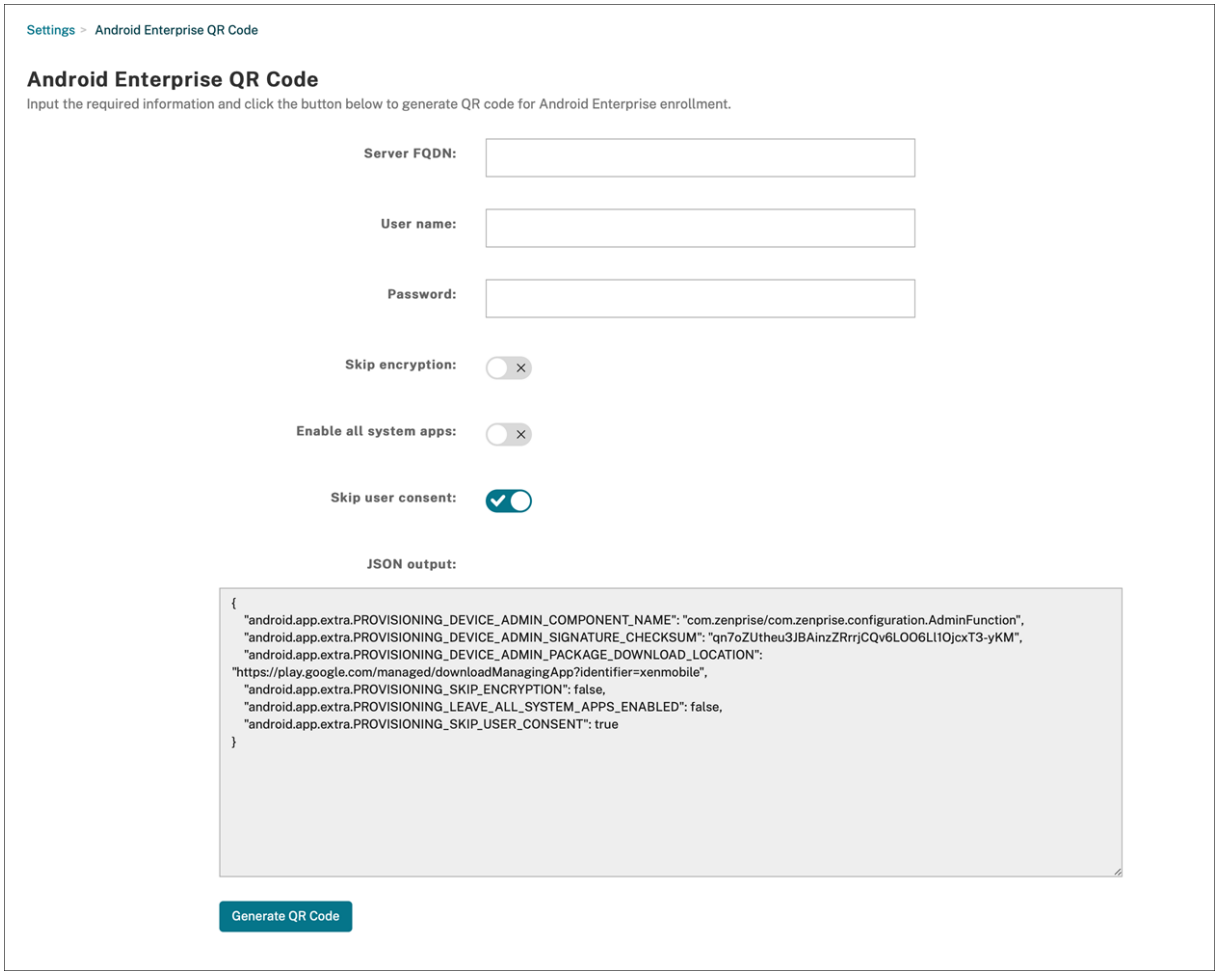
Inscription d'appareils à l'aide d'un code QR

Les utilisateurs peuvent inscrire un appareil entièrement géré à l'aide du code QR que vous leur avez généré.

Configuration système requise Appareils Android exécutant Android 7.0 ou version ultérieure.

Créer un code QR Vous générez un code QR en spécifiant les informations d'inscription, le cas échéant. Après avoir généré un code QR, enregistrez-le localement. Citrix Endpoint Management ne le stocke pas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. Accédez à **Paramètres > Code QR Android Enterprise**.
2. Si nécessaire, spécifiez les informations d'inscription suivantes :
   - **Nom de domaine complet du serveur :** saisissez le nom de domaine complet du serveur Citrix Endpoint Management (par exemple, `example.cem.cloud.com`). Ce champ est facultatif. Si vous le laissez vide, les utilisateurs doivent renseigner ces informations lorsqu'ils s'inscrivent.
   - **Nom d'utilisateur :** entrez le nom d'utilisateur utilisé pour vous inscrire. Nous vous recommandons de laisser ce champ vide si vous prévoyez de distribuer le code QR à plusieurs utilisateurs. La configuration d'un code QR avec un nom d'utilisateur et un mot de passe est utile pour inscrire des appareils kiosques. Si vous le laissez vide, les utilisateurs doivent renseigner ces informations lorsqu'ils s'inscrivent.
   - **Mot de passe :** entrez le mot de passe associé au nom d'utilisateur que vous avez saisi. Si vous le laissez vide, les utilisateurs doivent renseigner ces informations lorsqu'ils s'inscrivent.
   - **Ignorer le cryptage :** si cette option est définie sur **Activé**, l'appareil n'est pas crypté lors de l'inscription. La valeur par défaut est **Off**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Activer toutes les applications système :** si cette option est définie sur **Activé**, l'accès à toutes les applications système de l'appareil est autorisé. La valeur par défaut est **Off**.
- **Ignorer le consentement de l'utilisateur :** si cette option est définie sur **Désactivé**, les utilisateurs peuvent choisir de ne pas utiliser la gestion des appareils. La valeur par défaut est **Off**.

La zone **Sortie JSON** affiche le contenu JSON correspondant aux informations que vous avez spécifiées.

3. Pour ajouter des informations d'inscription supplémentaires, modifiez le contenu JSON dans la zone **Sortie JSON**.
4. Cliquez sur **Générer le code QR**. Le code QR apparaît à droite de la sortie JSON.
5. Cliquez avec le bouton droit de la souris sur le code QR et enregistrez-le.
6. Envoyez l'image aux utilisateurs pour l'inscription de l'appareil.

Un appareil dont les paramètres d'usine ont été réinitialisés scanne ce code QR pour s'inscrire en tant qu'appareil entièrement géré.

Pour inscrire l'appareil Après la mise sous tension d'un nouvel appareil ou d'un appareil ayant fait l'objet d'une réinitialisation d'usine, procédez comme suit :

1. Touchez l'écran 6 fois sur l'écran d'accueil pour lancer le flux d'inscription du code QR.
2. Lorsque vous y êtes invité, connectez-vous au Wi-Fi. L'emplacement de téléchargement de Citrix Secure Hub dans le code QR est accessible sur ce réseau Wi-Fi.

   Une fois que l'appareil se connecte au Wi-Fi, il télécharge un lecteur de code QR à partir de Google et lance l'appareil photo.
3. Pointez l'appareil photo sur le code QR pour scanner le code.

   Android télécharge Citrix Secure Hub à partir de l'emplacement de téléchargement dans le code QR, valide la signature du certificat de signature, installe Citrix Secure Hub et le définit comme propriétaire de l'appareil.

Pour plus d'informations, consultez ce guide Google destiné aux développeurs Android EMM : https://developers.google.com/android/work/prov-devices#qr_code_method.

Inscription sans contact

L'inscription sans contact vous permet de configurer les appareils pour qu'ils soient provisionnés en tant qu'appareils entièrement gérés lorsqu'ils sont mis sous tension pour la première fois.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Votre revendeur d'appareils vous crée un compte sur le portail d'inscription sans contact Android, un outil en ligne qui vous permet d'appliquer des configurations aux appareils. À l'aide du portail d'inscription sans contact Android, vous créez une ou plusieurs configurations d'inscription sans contact et appliquez les configurations aux appareils attribués à votre compte. Lorsque vos utilisateurs mettent ces appareils sous tension, ils sont automatiquement inscrits dans Citrix Endpoint Management. La configuration attribuée à l'appareil définit son processus d'inscription automatique.

Configuration système requise

- La prise en charge de l'inscription sans contact est disponible à partir de Android 9.0.

Appareils et informations de compte provenant de votre revendeur

- Les appareils pouvant bénéficier de l'inscription sans contact sont achetés auprès d'un revendeur d'entreprise ou d'un partenaire Google. Pour obtenir la liste des partenaires Android Enterprise prenant en charge l'inscription sans contact, consultez le site Web Android.
- Un compte provenant du portail d'inscription sans contact Android Enterprise, créé par votre revendeur.
- Des informations de connexion au compte du portail d'inscription sans contact Android Enterprise, fournies par votre revendeur.

Créer une configuration sans contact Lorsque vous créez une configuration sans contact, incluez un fichier JSON personnalisé pour spécifier les détails de la configuration.

Utilisez ce fichier JSON pour configurer l'appareil à inscrire sur le serveur Citrix Endpoint Management que vous spécifiez. Remplacez l'URL de votre serveur par « URL » dans cet exemple.

```
        {

            "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
          {

                "serverURL":"URL"
            }

         }

<!--NeedCopy-->
```

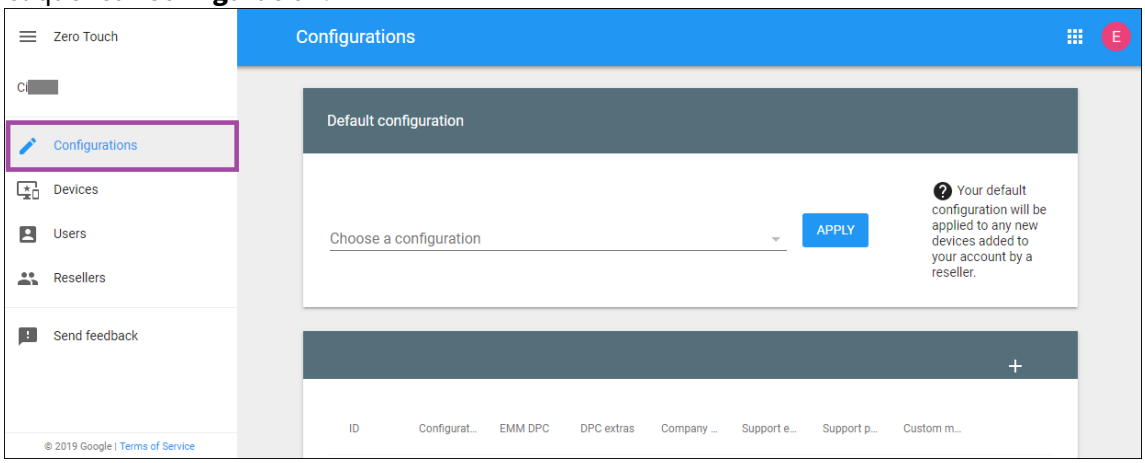
Vous pouvez utiliser un fichier JSON facultatif avec plus de paramètres pour personnaliser davantage votre configuration. Cet exemple spécifie le serveur Citrix Endpoint Management ainsi que le nom d'utilisateur et le mot de passe que les appareils configurés utilisent pour ouvrir une session sur le serveur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
1        {
2
3           "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4             {
5
6                 "serverURL":"URL",
7                 "xm_username":"username",
8                 "xm_password":"password"
9              }
10
11               }
12
13    <!--NeedCopy-->
```

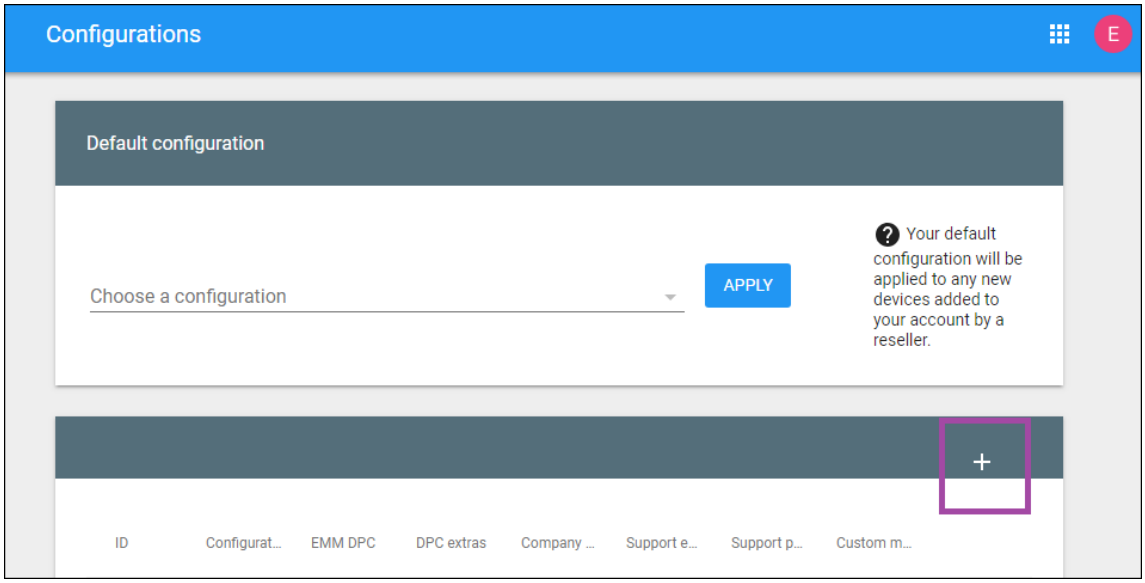
> **Important :**
>
> Pour inscrire des appareils dans le profil de travail en mode Appareils appartenant à l'entreprise, ajoutez `{ "desiredProvisioningMode": "managedProfile"}` au fichier JSON personnalisé sous `PROVISIONING_ADMIN_EXTRAS_BUNDLE`.

1. Accédez au portail d'inscription sans contact Android à l'adresse https://partner.android.com/zerotouch. Connectez-vous avec les informations de compte provenant de votre revendeur d'appareils sans contact.
2. Cliquez sur **Configuration**.



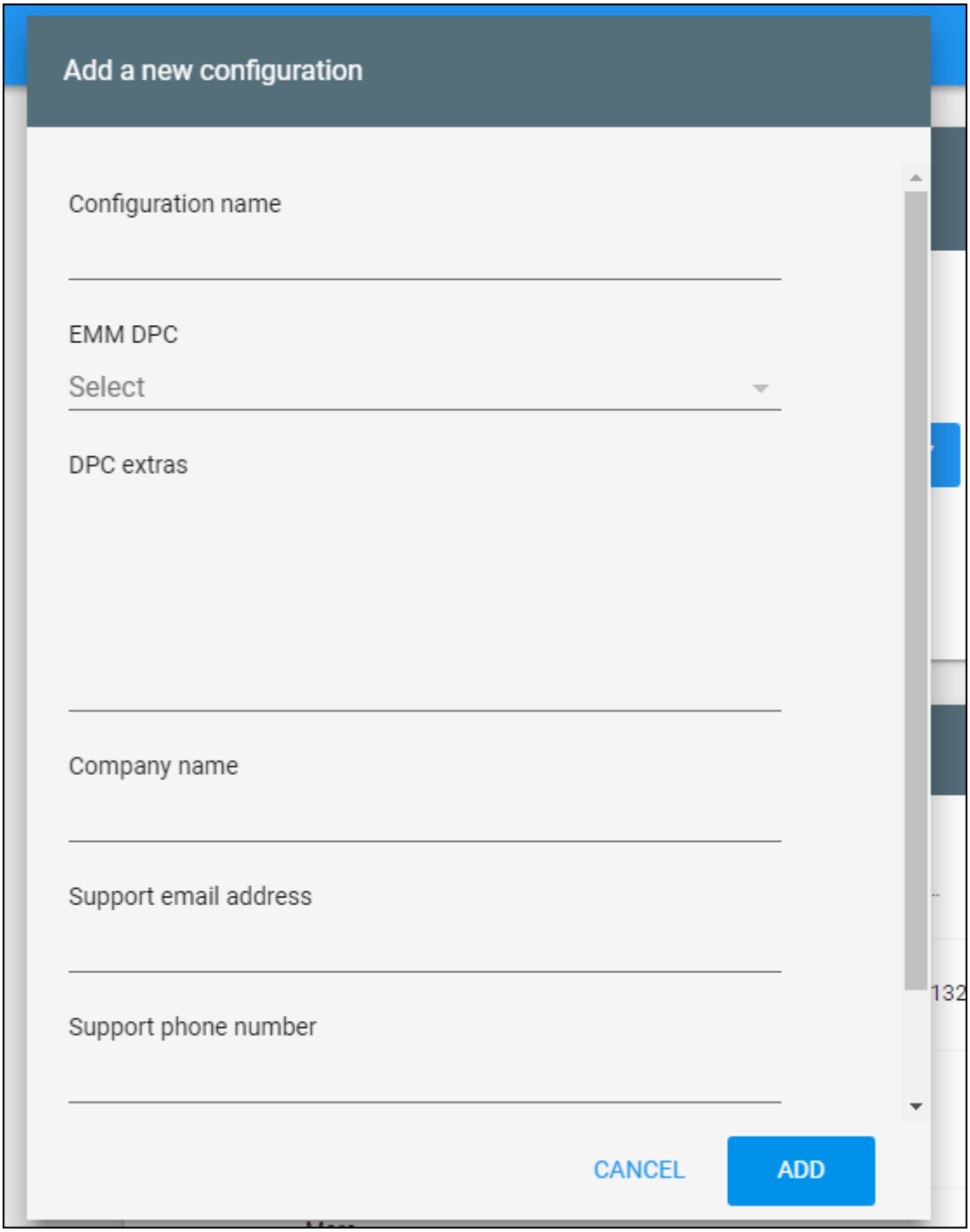
3. Cliquez sur **+** au-dessus du tableau de configuration.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Entrez vos informations de configuration dans la fenêtre de configuration qui s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



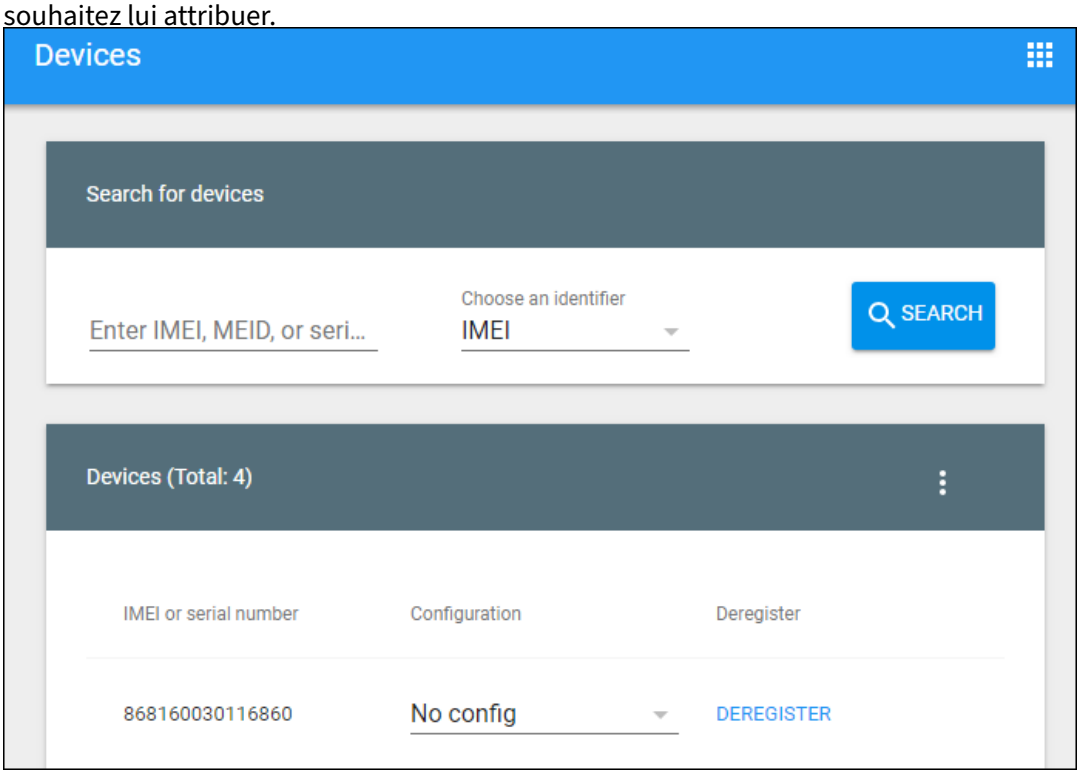
- **Configuration name :** saisissez le nom que vous avez choisi pour cette configuration.
- **EMM DPC :** choisissez **Citrix Secure Hub**.
- **DPC extras :** collez votre texte JSON personnalisé dans ce champ.
- **Company name :** saisissez le nom que vous souhaitez afficher sur vos appareils sans contact Android Enterprise pendant le provisioning de l'appareil.
- **Support email address :** saisissez une adresse e-mail que vos utilisateurs peuvent contac-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ter pour obtenir de l'aide. Cette adresse apparaît sur vos appareils sans contact Android Enterprise avant le provisioning de l'appareil.

- **Support phone number :** saisissez un numéro de téléphone que vos utilisateurs peuvent contacter pour obtenir de l'aide. Ce numéro de téléphone apparaît sur vos appareils sans contact Android Enterprise avant le provisioning de l'appareil.
- **Custom Message :** si vous le souhaitez, ajoutez une ou deux phrases pour aider vos utilisateurs à vous contacter ou leur donner plus de détails sur l'état de leur appareil. Ce message personnalisé apparaît sur vos appareils sans contact Android Enterprise avant le provisioning de l'appareil.

5. Cliquez sur **Ajouter**.
6. Pour créer des configurations supplémentaires, répétez les étapes 2 à 4.
7. Pour appliquer une configuration à un appareil, procédez comme suit :
   a) Dans le portail d'inscription sans contact Android, cliquez sur **Devices**.
   b) Recherchez l'appareil dans la liste des appareils et choisissez la configuration que vous souhaitez lui attribuer.



   c) Cliquez sur **Update**.

Vous pouvez appliquer une configuration à de nombreux appareils à l'aide d'un fichier CSV.

Pour plus d'informations sur l'application d'une configuration à de nombreux appareils, consultez Inscription sans contact pour les administrateurs informatiques. Cette rubrique d'Android Enterprise

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

contient des informations supplémentaires sur la façon de gérer les configurations et de les appliquer aux appareils.

Provisionner des appareils Android Enterprise dédiés

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

Inscrivez les appareils dédiés à l'aide de l'une des méthodes d'inscription utilisées pour d'autres appareils entièrement gérés, comme décrit dans la section Provisionner des appareils Android Enterprise entièrement gérés. Le provisioning d'appareils dédiés nécessite une configuration supplémentaire avant l'inscription.

Pour provisionner des appareils dédiés, procédez comme suit :

- Ajoutez un profil d'inscription pour les administrateurs Citrix Endpoint Management que vous autorisez à inscrire des appareils dédiés dans votre déploiement Citrix Endpoint Management. Consultez Création de profils d'inscription.
- Pour permettre à un appareil dédié d'accéder aux applications, ajoutez-les à la liste d'autorisation.
- Vous pouvez également activer le mode de verrouillage des tâches pour l'application autorisée. Lorsqu'une application est en mode de verrouillage des tâches, elle est épinglée sur l'écran de l'appareil lorsque l'utilisateur l'ouvre. Aucun bouton d'accueil n'apparaît et le bouton Retour est désactivé. L'utilisateur quitte l'application à l'aide d'une action programmée dans l'application, comme la déconnexion.
- Inscrivez chaque appareil dans le profil d'inscription que vous avez ajouté.

Configuration système requise

- L'inscription des appareils dédiés est prise en charge à partir de Android 6.0.

Autoriser les applications et définir le mode de verrouillage des tâches

La stratégie Kiosque vous permet d'autoriser les applications et de définir le mode de verrouillage des tâches. Par défaut, les services Citrix Secure Hub et Google Play sont ajoutés à la liste d'autorisation.

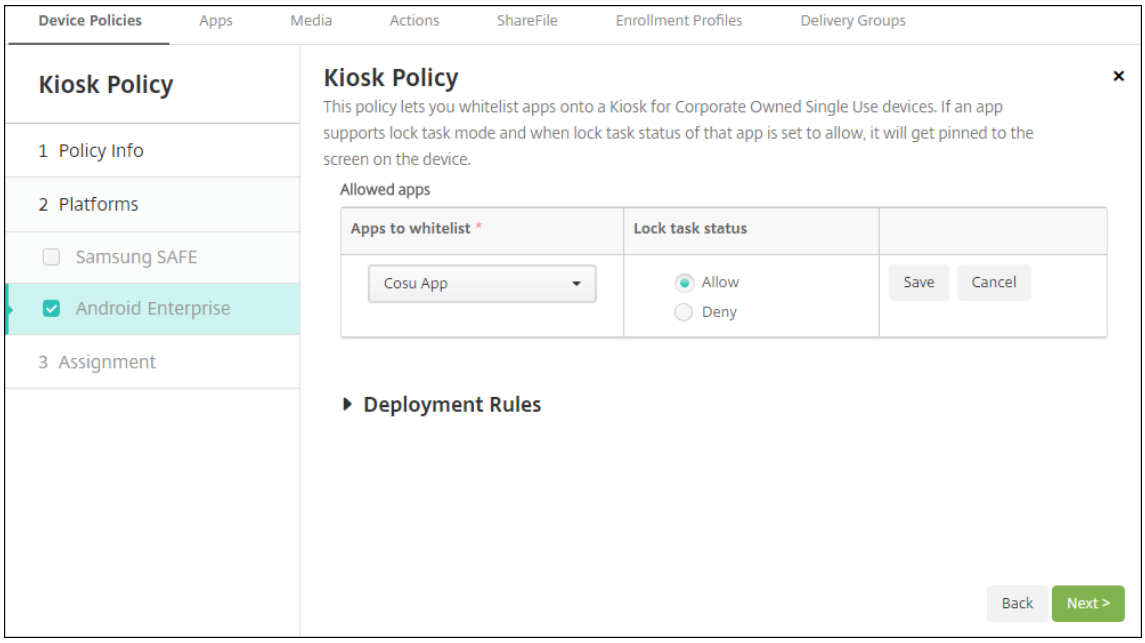
Pour ajouter la stratégie Kiosque :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.
2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.
3. Développez **Plus** puis, sous Sécurité, cliquez sur **Kiosque**. La page **Stratégie kiosque** s'affiche.
4. Sous Plates-formes, sélectionnez **Android Enterprise**. Supprimez les autres plates-formes.
5. Dans le volet Informations sur la stratégie, tapez le **nom de la stratégie** et une **description** facultative.
6. Cliquez sur **Suivant**, puis sur **Ajouter**.
7. Pour autoriser une application, et autoriser ou refuser le mode de verrouillage des tâches pour cette application, procédez comme suit :

   Sélectionnez dans la liste l'application que vous souhaitez autoriser.

   Choisissez **Autoriser** pour que l'application soit épinglée sur l'écran de l'appareil lorsque l'utilisateur démarre l'application. Choisissez **Refuser** pour que l'application ne soit pas épinglée. La valeur par défaut est **Autoriser**.



8. Cliquez sur **Save**.
9. Pour autoriser une application, et autoriser ou refuser le mode de verrouillage des tâches pour cette application, cliquez sur **Ajouter**.
10. Configurez les règles de déploiement et choisissez des groupes de mise à disposition. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Provisionner des appareils Android Enterprise entièrement gérés avec profil de travail ou profil de travail sur appareils appartenant à l'entreprise

Les appareils exécutant Android 9.0-10.x sont inscrit comme étant « entièrement gérés avec profil de travail ». À partir d'Android 11+, les appareils sont inscrits en tant que « profil de travail sur appareils appartenant à l'entreprise ». Tous ces appareils sont des appareils appartenant à l'entreprise qui sont utilisés à des fins professionnelles et personnelles. Votre organisation gère l'ensemble de l'appareil. Vous pouvez appliquer un ensemble de stratégies à l'appareil et un ensemble distinct de stratégies au profil de travail.

Dans la console Citrix Endpoint Management, les appareils entièrement gérés avec profil de travail apparaissent avec les termes suivants :

- La propriété de l'appareil est « Corporate » (Entreprise).
- Le type d'installation de l'appareil Android Enterprise est « Corporate Owner Personally Enabled » (COPE).

Configuration système requise

- La prise en charge de l'inscription d'appareils entièrement gérés avec profil de travail commence avec Android 9.0.

Pour inscrire l'appareil

Les nouveaux appareils et les appareils avec réinitialisation d'usine s'inscrivent en tant qu'appareils entièrement gérés avec profil de travail. Ces appareils utilisent l'une des méthodes d'inscription utilisées pour d'autres appareils entièrement gérés, comme décrit dans la section Provisionner des appareils Android Enterprise entièrement gérés. Les appareils exécutant Android 11 peuvent s'inscrire au mode profil de travail sur appareils appartenant à l'entreprise en utilisant le code QR ou les méthodes d'inscription sans contact décrites dans cette section.

> **Important :**
>
> Lorsque vous inscrirez des appareils au mode profil de travail sur appareils appartenant à l'entreprise à l'aide de la méthode du code QR, ajoutez les lignes suivantes à la sortie JSON, au-dessus du champ `serverURL` :
> `"desiredProvisioningMode": "managedProfile",`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

JSON output

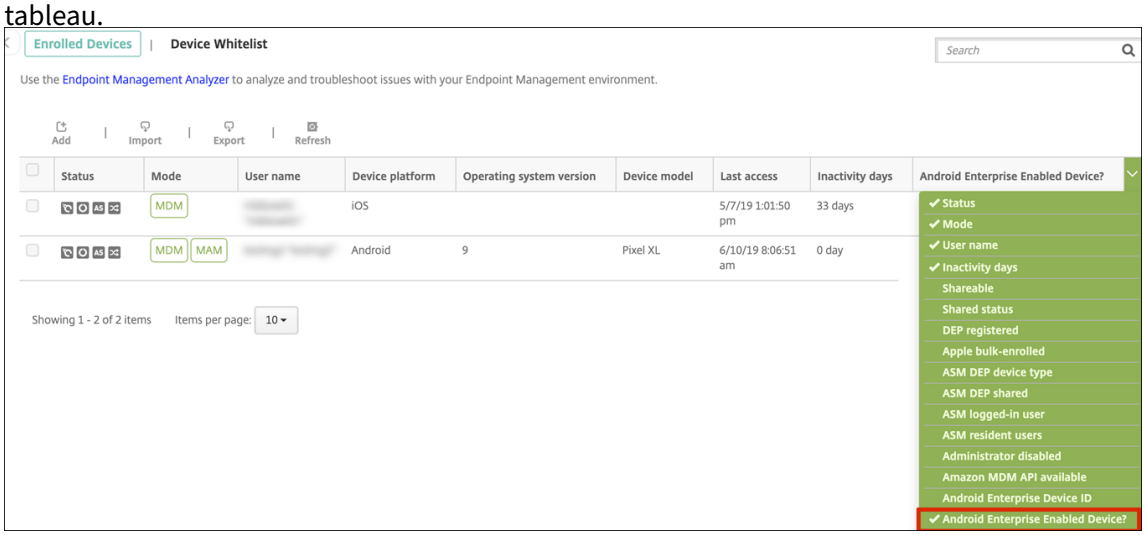

```
{
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
    "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
    "android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED": false,
    "android.app.extra.PROVISIONING_SKIP_USER_CONSENT": true,
    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
        "desiredProvisioningMode": "managedProfile",
        "serverURL": "https://testServer.xmqa.cloud.com",
        "username": "username",
        "password": "password"
    }
```


Les appareils qui ne sont pas nouveaux ou réinitialisés en usine sont inscrits en tant qu'appareils avec profil de travail, comme décrit à la section Provisioning d'appareils Android Enterprise avec profil de travail.

Affichage des appareils Android Enterprise dans la console Citrix Endpoint Management

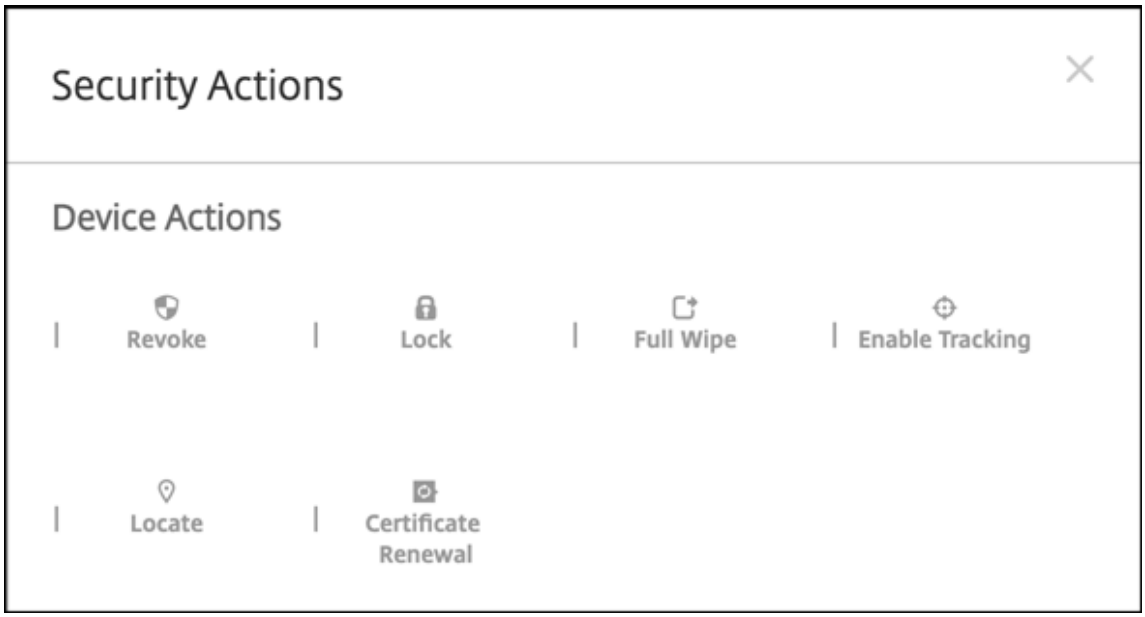
Pour afficher les appareils Android Enterprise entièrement gérés, les appareils dédiés et les appareils entièrement gérés avec profil de travail :

1. Dans la console Citrix Endpoint Management, accédez à **Gérer > Appareils**.
2. Ajouter la colonne **Appareil Android Enterprise activé ?** en cliquant sur le menu à droite du tableau.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Pour afficher les actions de sécurité disponibles, sélectionnez un appareil entièrement géré et cliquez sur **Sécurisé**. Lorsque l'appareil est entièrement géré, l'action **Effacer** est disponible, mais l'opération **Effacer les données d'entreprise** ne l'est pas. Cela est dû au fait que l'appareil n'autorise que les applications de Google Play Store d'entreprise. L'utilisateur ne peut donc pas installer des applications à partir du magasin public. Votre organisation gère tout le contenu de l'appareil.



Configurer les stratégies d'appareil et d'application Android Enterprise

Pour obtenir une vue d'ensemble des stratégies contrôlées au niveau de l'appareil et de l'application, consultez Stratégies d'appareil et stratégies MDX Android Entreprise prises en charge.

Informations clés sur les stratégies :

- **Restrictions sur l'appareil :** des dizaines de restrictions sur l'appareil vous permettent de contrôler des fonctionnalités telles que :
  - Utilisation de l'appareil photo de l'appareil
  - Utilisation du copier-coller entre les profils de travail et les profils personnels
- **Per App VPN :** utilisez la stratégie Configurations gérées pour configurer les profils VPN pour Android Enterprise.
- **Stratégie de messagerie :** nous vous recommandons d'utiliser la stratégie Configurations gérées pour configurer les applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégies d'appareil

Ce tableau répertorie toutes les stratégies d'appareils disponibles pour les appareils Android Enterprise.

> **Important :**
>
> Pour les appareils qui sont inscrits dans Android Enterprise et utilisent des applications MDX : vous pouvez contrôler certains paramètres via MDX et Android Enterprise. Utilisez les paramètres de stratégie les moins restrictifs pour MDX et contrôlez la stratégie via Android Enterprise.

	Autorisations d'application	Inventaire des applications	Désinstallation des applications
	Mettre à jour automatiquement les applications gérées	Planification de connexion	Informations d'identification
	XML personnalisé	Options Citrix Endpoint Management	Fichiers
	Gestion du keyguard	Kiosque	Configuration du Launcher
	Emplacement	Configurations gérées	Réseau
	Mise à jour d'OS	Code secret	Restrictions

Stratégies pour appareils entièrement gérés avec profil de travail (appareils COPE)

Pour les appareils entièrement gérés avec profil de travail, vous pouvez utiliser certaines stratégies pour appliquer des paramètres distincts à l'ensemble de l'appareil et au profil de travail. Vous pouvez utiliser d'autres stratégies pour appliquer des paramètres uniquement à l'ensemble de l'appareil ou uniquement au profil de travail des appareils entièrement gérés avec profil de travail. Pour les appareils inscrits au mode profil de travail sur appareils appartenant à l'entreprise, les stratégies s'appliquent uniquement au profil de travail, et non à l'appareil entier.

Stratégie	S'applique à
Autorisations d'application	Profil de travail
Inventaire des applications	Profil de travail

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie	S'applique à
Désinstallation des applications	Profil de travail
Mettre à jour automatiquement les applications gérées	Profil de travail
Planification de connexion	Profil de travail
Informations d'identification	Profil de travail
XML personnalisé	S/O
Options Citrix Endpoint Management	Profil de travail
Fichiers	Profil de travail
Gestion du keyguard	Appareil et profil professionnel
Kiosque	S/O
Configuration du Launcher	Appareil et profil professionnel
Emplacement	Appareil (mode de localisation uniquement)
Configurations gérées	Profil de travail
Réseau	Appareil
Mise à jour d'OS	S/O
Code secret	Appareil et profil professionnel
Restrictions	Appareil et profil de travail (créez des stratégies distinctes pour l'appareil et le profil de travail)
VPN	S/O

Consultez également Stratégies d'appareil et stratégies MDX Android Entreprise prises en charge et Présentation du SDK MAM.

Actions de sécurisation

Android Enterprise prend en charge les actions de sécurisation suivantes. Pour obtenir une description de chaque action, consultez la section Actions de sécurisation.

Action de sécurisation	Profil de travail	Entièrement géré
Renouvellement de certificat	Oui	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Action de sécurisation	Profil de travail	Entièrement géré
Effacer	Oui (après un effacement des données d'entreprise)	Oui
Localiser	Oui	Oui
Verrouiller	Oui	Oui
Verrouiller et réinitialiser un mot de passe	Non	Oui
Notifier (sonnerie)	Oui	Oui
Révoquer	Oui	Oui
Effacer les données d'entreprise	Oui	Oui

Notes sur les actions de sécurisation

- L'action de sécurisation Localiser échoue à moins que la stratégie d'appareil Localisation n'ait défini le mode de localisation de l'appareil sur **Haute précision** ou **Économie de batterie**. Voir Stratégie d'emplacement.
- Sur les appareils avec profil de travail qui exécutent des versions Android antérieures à Android 9.0 :
  - L'action de verrouillage et de réinitialisation du mot de passe n'est pas prise en charge.
- Sur les appareils avec profil de travail qui exécutent Android 9.0 ou supérieur :
  - Le code secret envoyé verrouille le profil de travail. L'appareil lui-même n'est pas verrouillé.
  - Si aucun code d'accès n'est défini sur le profil de travail :
    - Si aucun code secret n'est envoyé ou si le code secret envoyé ne répond pas aux exigences de code secret : l'appareil est verrouillé.
  - Si un code d'accès est défini sur le profil de travail :
    - Si aucun code secret n'est envoyé ou si le code secret envoyé ne répond pas aux exigences en matière de code secret : le profil de travail est verrouillé mais l'appareil lui-même ne l'est pas.

Désinscription d'une entreprise Android Enterprise

Si vous ne souhaitez plus utiliser votre entreprise Android Enterprise, vous pouvez annuler l'inscription de l'entreprise.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Avertissement :**
>
> une fois que vous avez désinscrit une entreprise, l'état par défaut des applications Android Enterprise sur les appareils déjà inscrits est rétabli. Google ne gère plus les appareils. Si vous inscrivez un appareil sur une nouvelle entreprise Android Enterprise, vous devez approuver les applications de la nouvelle organisation à partir de Google Play d'entreprise. Vous pouvez ensuite mettre à jour les applications à partir de la console Citrix Endpoint Management.

Une fois l'entreprise Android Enterprise désinscrite :

- Les applications Android Enterprise des appareils et des utilisateurs inscrits dans l'entreprise sont réinitialisées à leur état par défaut. Les stratégies Configurations gérées appliquées précédemment n'affectent plus les opérations.
- Citrix Endpoint Management gère les appareils inscrits dans l'entreprise. Du point de vue de Google, ces appareils ne sont pas gérés. Vous ne pouvez pas ajouter de nouvelles applications Android Enterprise. Vous ne pouvez pas appliquer les stratégies Configurations gérées. Vous pouvez appliquer d'autres stratégies, telles que Planification, Mot de passe et Restrictions, à ces appareils.
- Si vous tentez d'inscrire des appareils dans Android Enterprise, ils sont inscrits comme appareils Android et non comme appareils Android Enterprise.

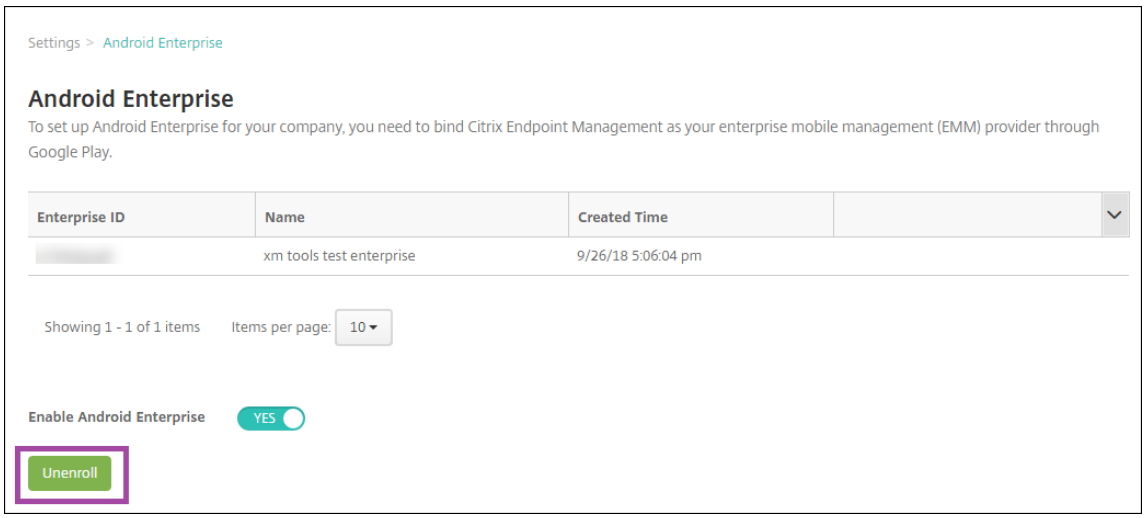
Vous pouvez désinscrire une entreprise Android Enterprise à l'aide de la console du serveur Citrix Endpoint Management et des outils Citrix Endpoint Management Tools.

Lorsque vous effectuez cette tâche, Citrix Endpoint Management ouvre une fenêtre contextuelle Outils. Avant de commencer, assurez-vous que votre navigateur a l'autorisation d'ouvrir des fenêtres contextuelles. Certains navigateurs, tels que Google Chrome, vous obligent à désactiver le blocage des fenêtres contextuelles et à ajouter l'adresse du site Citrix Endpoint Management à la liste d'autorisation des fenêtres contextuelles.

Désinscription d'une entreprise Android Enterprise :

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page Paramètres s'affiche.
2. Sur la page Paramètres, cliquez sur **Android Enterprise**.
3. Cliquez sur **Désinscrire**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Distribuer des applications Android Enterprise

November 29, 2023

Citrix Endpoint Management gère les applications déployées sur les appareils. Vous pouvez organiser et déployer les types d'applications Android Enterprise suivants.

- **Applications gérées du magasin d'applications :** ces applications incluent des applications gratuites disponibles dans le Google Play Store d'entreprise. Par exemple : GoToMeeting.
- **MDX :** applications préparées avec le SDK MAM ou encapsulées avec MDX Toolkit. Ces applications incluent des stratégies MDX. Vous obtenez des applications MDX à partir de sources internes et de magasins publics. Déployez des applications de productivité mobiles Citrix en tant qu'applications MDX.
- **Entreprise :** applications privées que vous développez ou obtenez à partir d'une autre source. Vous fournissez ces applications à vos utilisateurs via le Google Play Store d'entreprise. Le Google Play Store d'entreprise est le magasin d'applications d'entreprise Google.
- **Applications privées compatibles MDX :** applications d'entreprise préparées avec le SDK MAM ou encapsulées avec MDX Toolkit.

Vous pouvez ajouter des applications d'entreprise et des applications privées compatibles MDX de deux manières différentes.

- Ajoutez les applications à la console Citrix Endpoint Management en tant qu'applications d'entreprise, comme décrit dans les sections Applications d'entreprise et Applications privées compatibles MDX de cet article.
- Publiez les applications directement sur le Google Play Store d'entreprise à l'aide de votre compte Google Developer. Ajoutez ensuite les applications à la console Citrix Endpoint

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Management en tant qu'applications gérées du magasin d'applications. Voir Applications gérées du magasin d'applications.

Si vous publiez des applications à l'aide de votre compte Google Developer, puis passez à l'utilisation de la console Citrix Endpoint Management, l'appartenance des applications diffère. Vous devez gérer vos applications dans les deux emplacements, dans ce cas. Citrix vous recommande d'ajouter vos applications à l'aide d'une méthode ou d'une autre.

Si vous devez supprimer des applications autogérées du Google Play Store d'entreprise, ouvrez un ticket avec Google. Les développeurs peuvent désactiver, mais pas supprimer, les applications du Google Play Store géré.

Les sections suivantes fournissent des informations plus détaillées sur la configuration des applications Android Enterprise. Pour plus d'informations sur la distribution d'applications, consultez la section Ajouter des applications. Cet article contient les informations suivantes :

- Workflows généraux pour l'ajout d'applications Web et SaaS ou de liens Web
- Workflow des applications requises pour les applications d'entreprise et de magasin public
- Mise à disposition des applications d'entreprise à partir du réseau CDN Citrix pour applications d'entreprise

Applications gérées du magasin d'applications

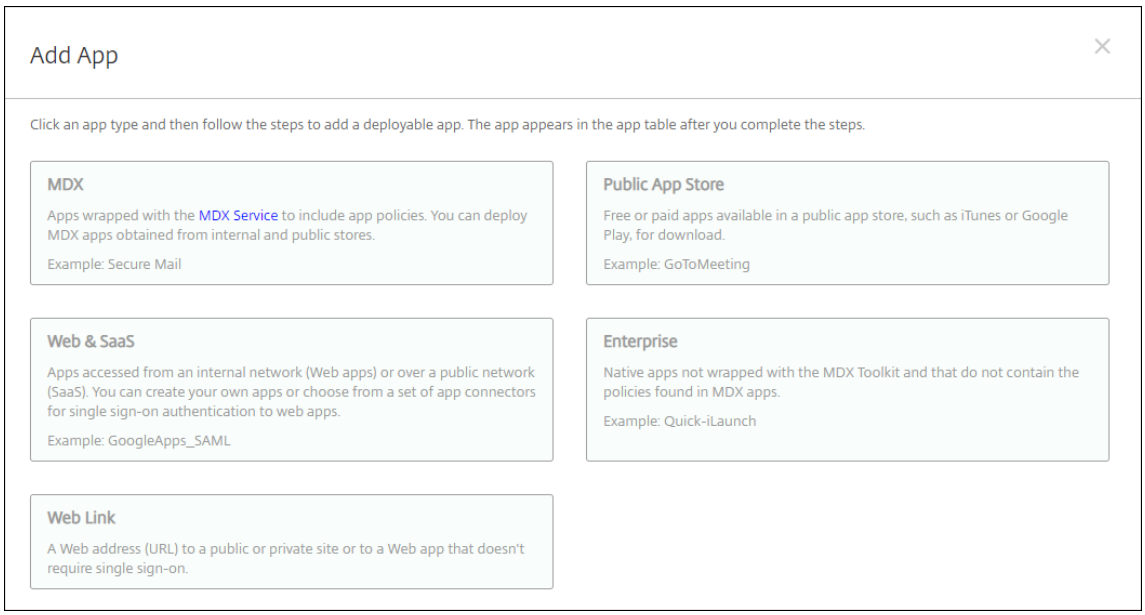
Vous pouvez ajouter des applications gratuites disponibles sur le Google Play Store d'entreprise à Citrix Endpoint Management.

> **Remarque** pour rendre toutes les applications du Google Play Store accessibles depuis le Google Play d'entreprise, utilisez la propriété de serveur **Accéder à toutes les applications du Google Play Store d'entreprise**. Consultez Propriétés du serveur. La définition de cette propriété sur **true** autorise tous les utilisateurs d'Android Enterprise d'accéder aux applications du Google Play Store public. Vous pouvez ensuite utiliser la stratégie Restrictions pour contrôler l'accès à ces applications.

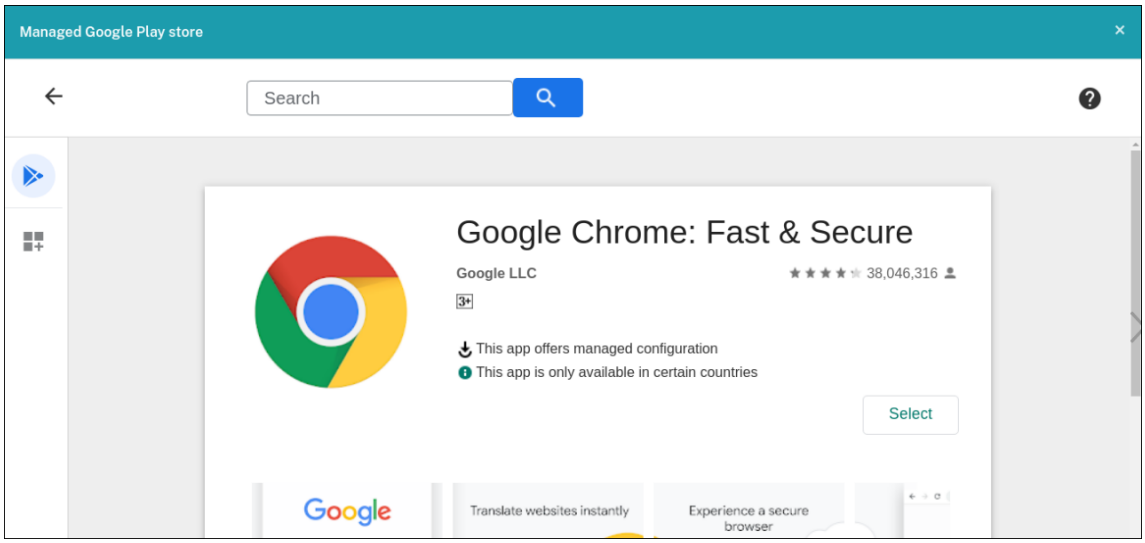
Étape 1 : Ajouter et configurer des applications

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Applications**. Cliquez sur **Ajouter**.
2. Cliquez sur **Magasin d'applications public**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

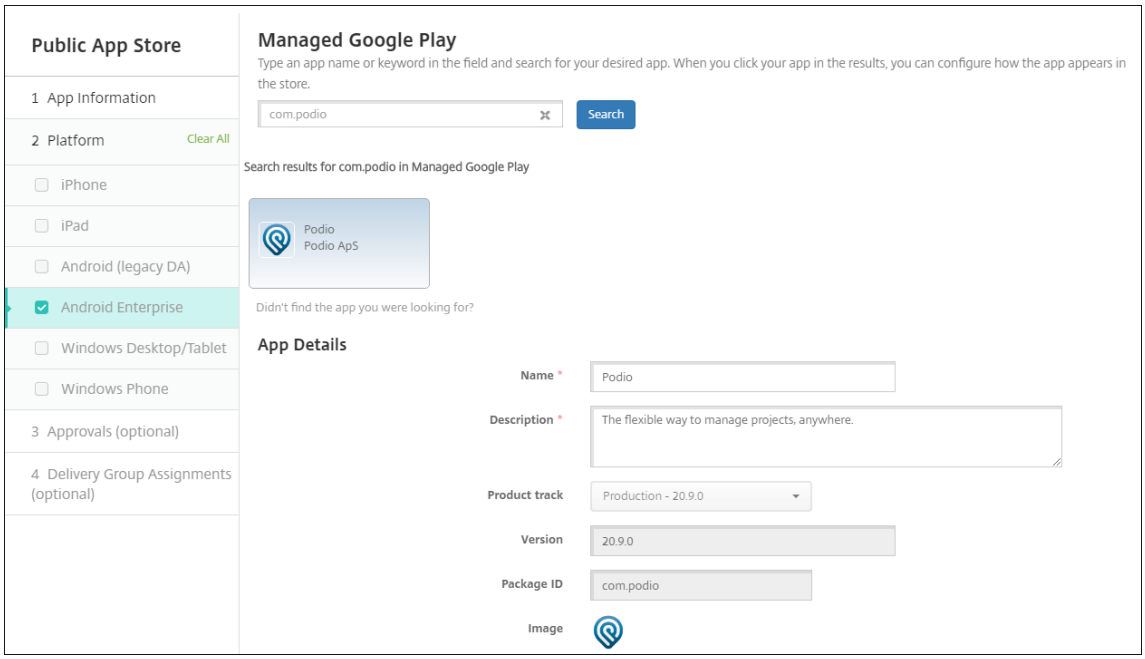


3. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous **Nom de l'application** dans le tableau **Applications**.
   - **Description :** entrez une description pour l'application (facultatif).
4. Sélectionnez **Android Enterprise** comme plate-forme.
5. Entrez le nom de l'application ou l'ID de package dans la zone de recherche et cliquez sur **Rechercher**. Vous pouvez trouver l'ID de package dans Google Play Store. L'ID se trouve dans l'URL de l'application. Par exemple, `com.Slack` est l'ID de package de `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`.
6. Les applications correspondant aux critères de recherche s'affichent. Cliquez sur l'application souhaitée, puis sur **Sélectionner**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. Cliquez à nouveau sur **Sélectionner**.
8. Cliquez sur l'icône de l'application et configurez le **nom** et la **description** de l'application.

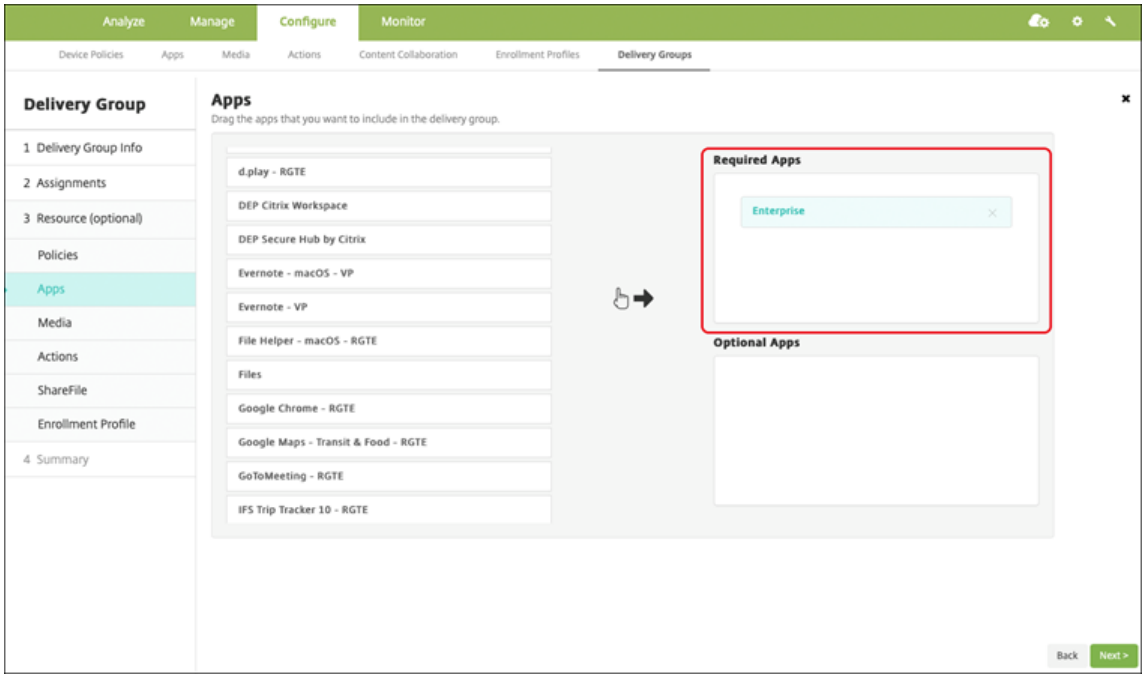


9. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**. Pour de plus amples informations, consultez la section Déployer des ressources.

Étape 2 : Configurer le déploiement de l'application

1. Accédez à **Configurer > Groupes de mise à disposition** et sélectionnez le groupe de mise à disposition que vous avez configuré. Cliquez sur **Modifier**.
2. Dans la section **Applications**, faites glisser les applications souhaitées vers la zone **Applications requises**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Sur la page **Résumé**, cliquez sur **Enregistrer**.
4. Sur la page **Groupes de mise à disposition**, sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.

Applications MDX

Ajoutez des fichiers MDX à Citrix Endpoint Management et configurez les détails de l'application et les paramètres de stratégie. Pour configurer les applications de productivité mobiles Citrix pour Android Enterprise, ajoutez-les en tant qu'applications MDX. Pour plus d'informations sur les stratégies applicatives disponibles pour chaque type de plate-forme, consultez :

- Présentation du SDK MAM
- Synopsis des stratégies MDX

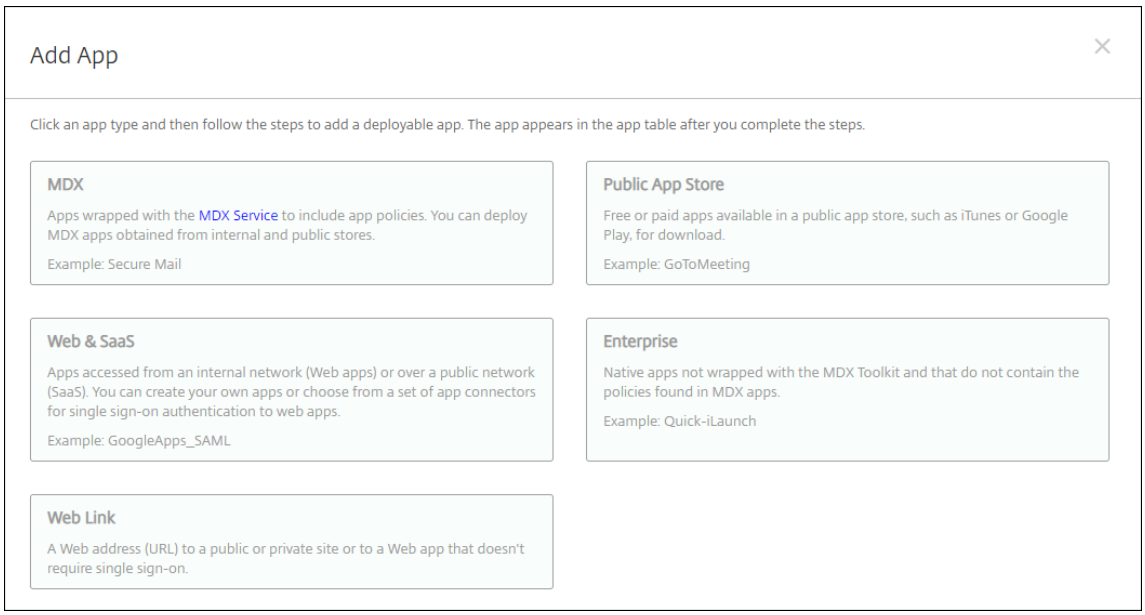
Étape 1 : Ajouter et configurer des applications

1. Pour les applications de productivité mobiles Citrix, téléchargez les fichiers MDX du magasin public : accédez à https://www.citrix.com/downloads. Accédez à **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.

   Pour les autres types d'applications MDX, obtenez le fichier MDX.

2. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications**. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



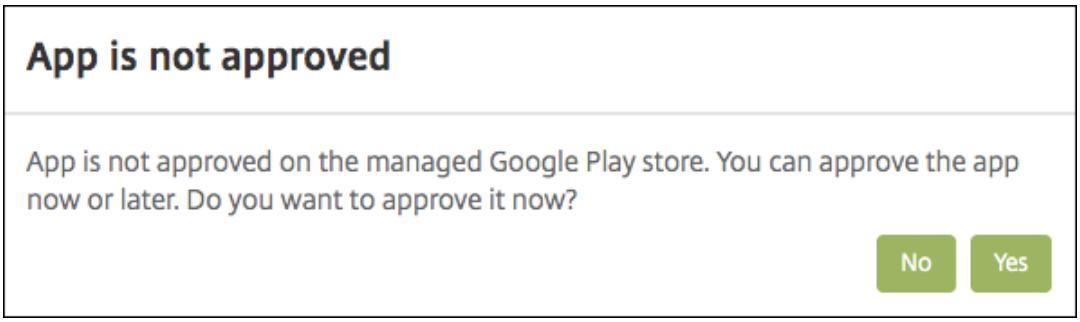
3. Cliquez sur **MDX**. La page **Informations sur l'application MDX** s'affiche. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :

   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous **Nom de l'application** dans le tableau **Applications**.
   - **Description :** entrez une description pour l'application (facultatif).

4. Sélectionnez **Android Enterprise** comme plate-forme.

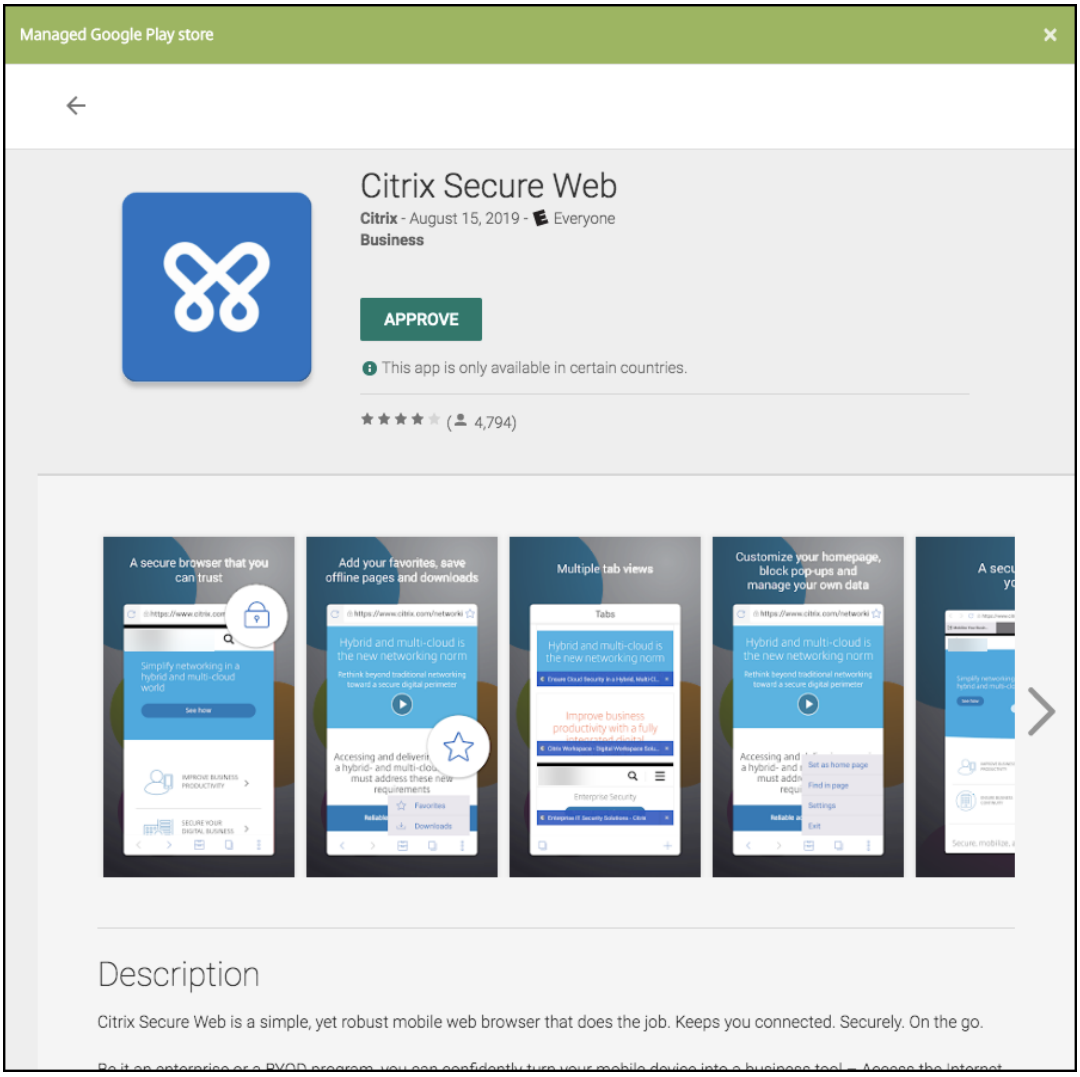
5. Cliquez sur **Charger** et accédez au fichier MDX. Android Enterprise prend uniquement en charge les applications encapsulées avec le SDK MAM ou MDX Toolkit.

   - L'interface utilisateur vous avertit si l'application jointe nécessite l'approbation du Google Play Store d'entreprise. Pour approuver l'application sans quitter la console Citrix Endpoint Management, cliquez sur **Oui**.

     Après l'ouverture du Google Play Store d'entreprise, suivez les instructions pour approuver et enregistrer l'application.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Lorsque vous ajoutez l'application, la page de **Détails sur l'application** apparaît.

6. Pour configurer ces paramètres :

   - **Nom du fichier :** entrez le nom du fichier associé à l'application.
   - **Description de l'application :** entrez une description pour l'application.
   - **Version de l'application :** si vous le souhaitez, entrez le numéro de version de l'application.
   - **ID de package :** entrez l'ID du package de l'application, obtenu à partir du Google Play Store d'entreprise.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
   - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne

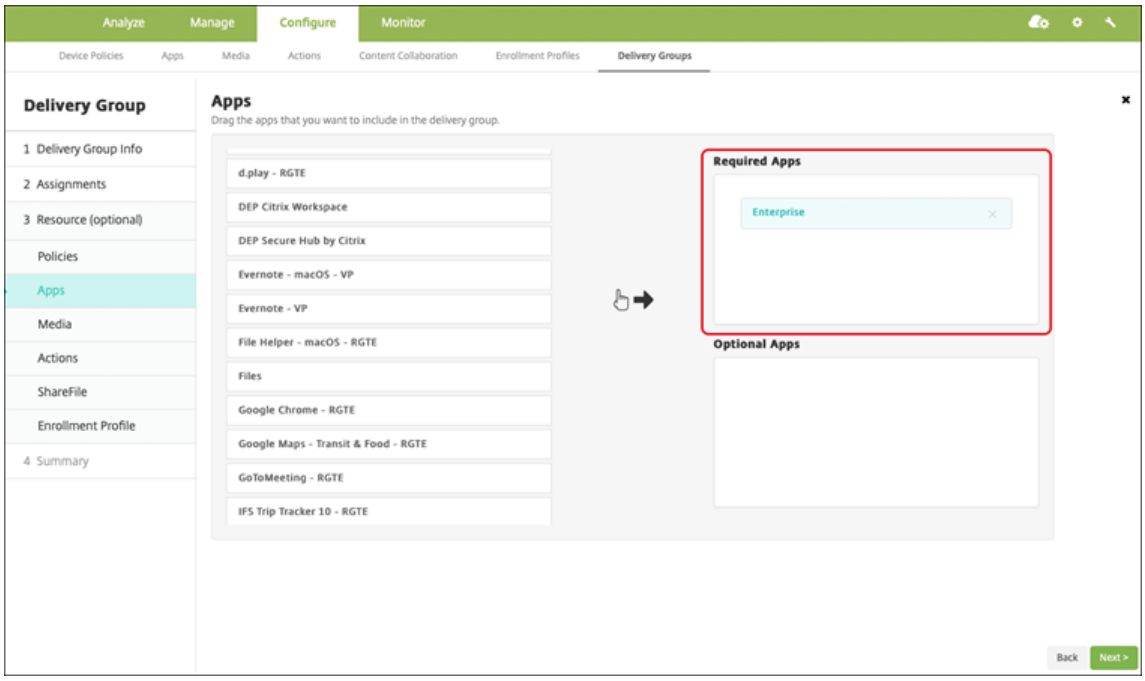
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

peuvent pas exécuter l'application.

7. Configurez les **stratégies MDX**. Les stratégies MDX varient selon la plate-forme et incluent des options dans des domaines de stratégie tels que l'authentification, la sécurité de l'appareil et les restrictions applicatives. Dans la console, les stratégies ont une info-bulle qui décrit chacune d'entre elles. Pour plus d'informations sur les stratégies applicatives disponibles pour chaque type de plate-forme, consultez :
   - Présentation du SDK MAM
   - Synopsis des stratégies MDX
8. Configurez les règles de déploiement et la configuration du magasin.
9. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**. Pour de plus amples informations, consultez la section Déployer des ressources.

Étape 2 : Configurer le déploiement de l'application

1. Accédez à **Configurer > Groupes de mise à disposition** et sélectionnez le groupe de mise à disposition que vous avez configuré. Cliquez sur **Modifier**.
2. Dans la section **Applications**, faites glisser les applications souhaitées vers la zone **Applications requises**.



3. Sur la page **Résumé**, cliquez sur **Enregistrer**.
4. Sur la page **Groupes de mise à disposition**, sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Applications d'entreprise

Les applications d'entreprise représentent des applications privées qui ne sont pas préparées avec le SDK MAM ou MDX Toolkit. Vous développez ces applications vous-même ou les obtenez directement à partir d'autres sources. Pour ajouter une application d'entreprise, vous avez besoin du fichier APK associé à l'application. Assurez-vous de suivre l'article Google Bonnes pratiques pour les applications privées.

Regardez cette vidéo pour en savoir plus :

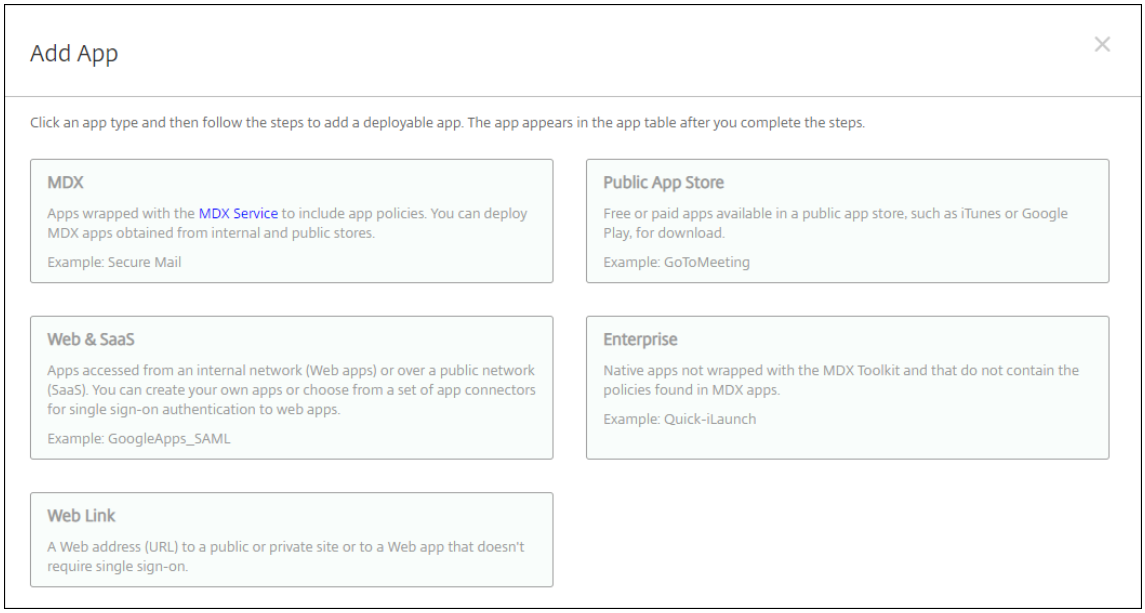
Étape 1 : Ajouter et configurer des applications

Ajoutez l'application à l'aide d'une des deux façons suivantes :

- Publiez l'application directement sur le Google Play Store d'entreprise et ajoutez-la à la console Citrix Endpoint Management en tant qu'application Play Store d'entreprise. Suivez la procédure Publier des applications privées de la documentation Google, puis suivez les étapes décrites dans la section Applications gérées du magasin d'applications.
- Ajoutez l'application à la console Citrix Endpoint Management en tant qu'application d'entreprise. Effectuez les opérations suivantes :

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications**. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



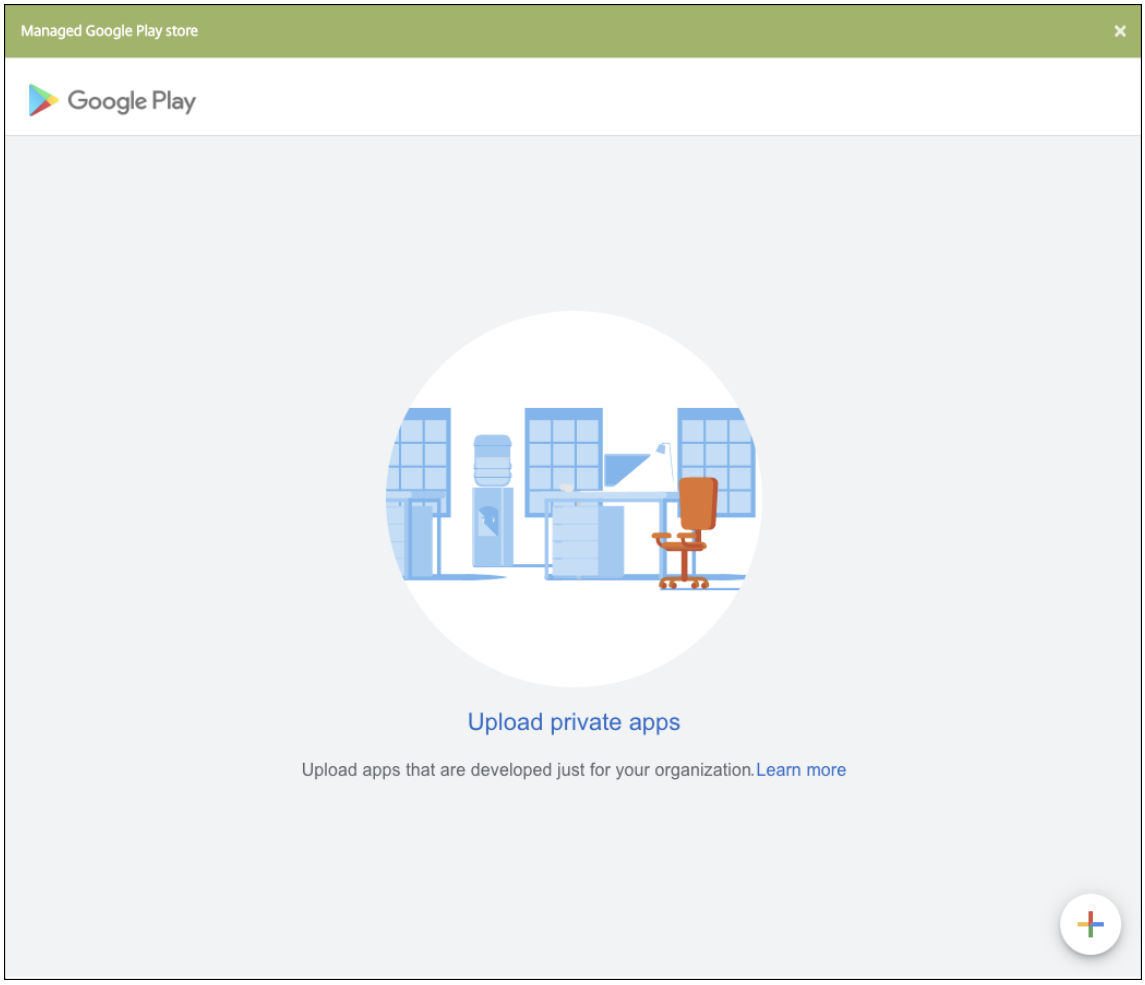
2. Cliquez sur **Entreprise**. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :

   - **Nom :** entrez un nom descriptif pour l'application. Il apparaît sous Nom de l'application dans le tableau Applications.
   - **Description :** entrez une description pour l'application (facultatif).

3. Sélectionnez **Android Enterprise** comme plate-forme.

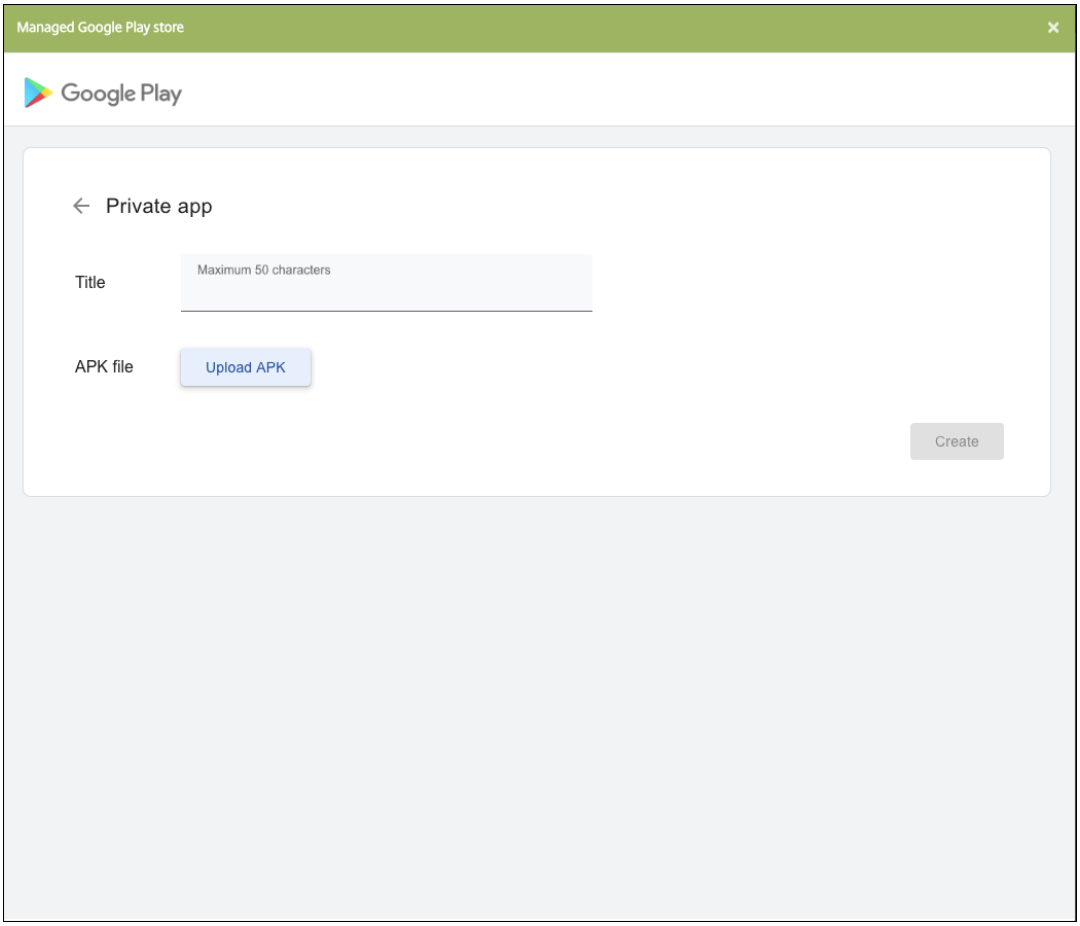
4. Le bouton **Charger** ouvre le Google Play Store d'entreprise. Vous n'avez pas besoin de vous inscrire pour créer un compte de développeur et publier une application privée. Cliquez sur l'icône **Plus** dans le coin inférieur droit pour continuer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



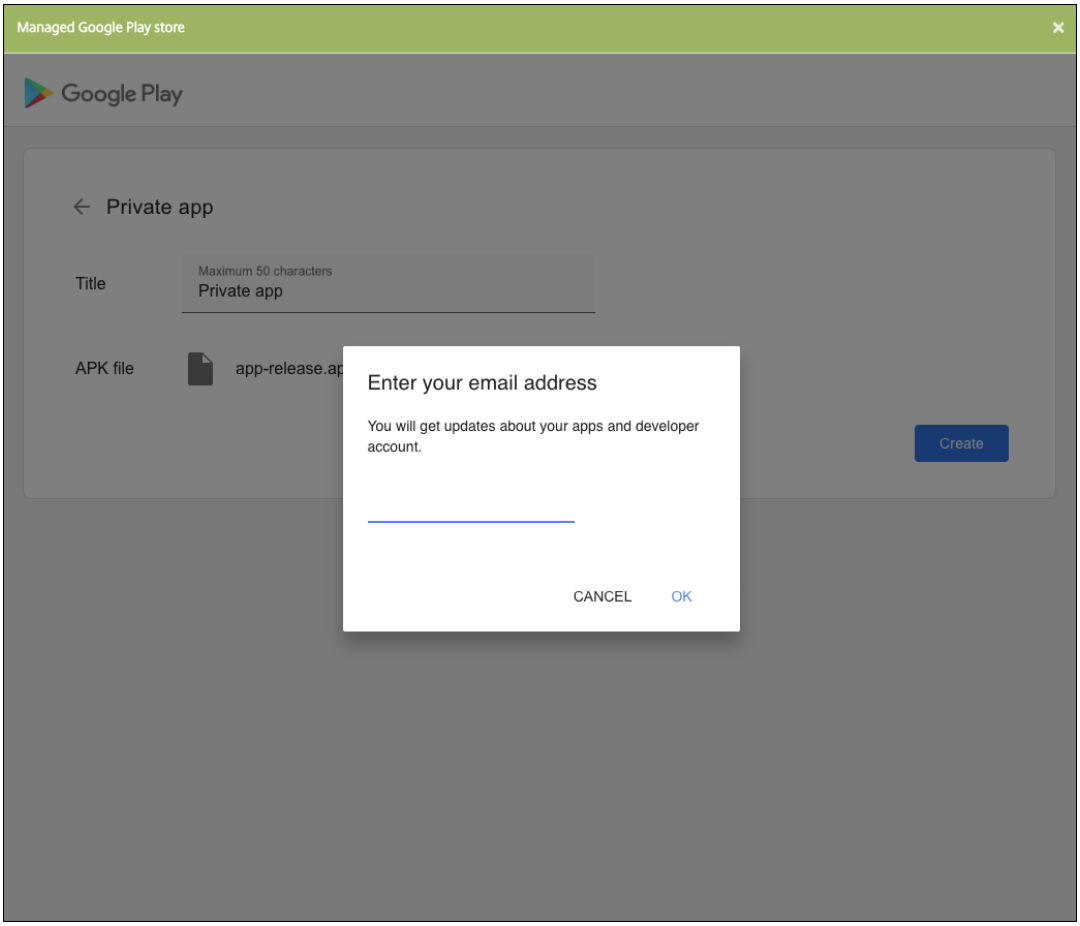
a) Tapez le nom de votre application et chargez le fichier .apk. Lorsque vous avez terminé, cliquez sur **Créer**. La publication de votre application privée peut prendre jusqu'à 10 minutes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



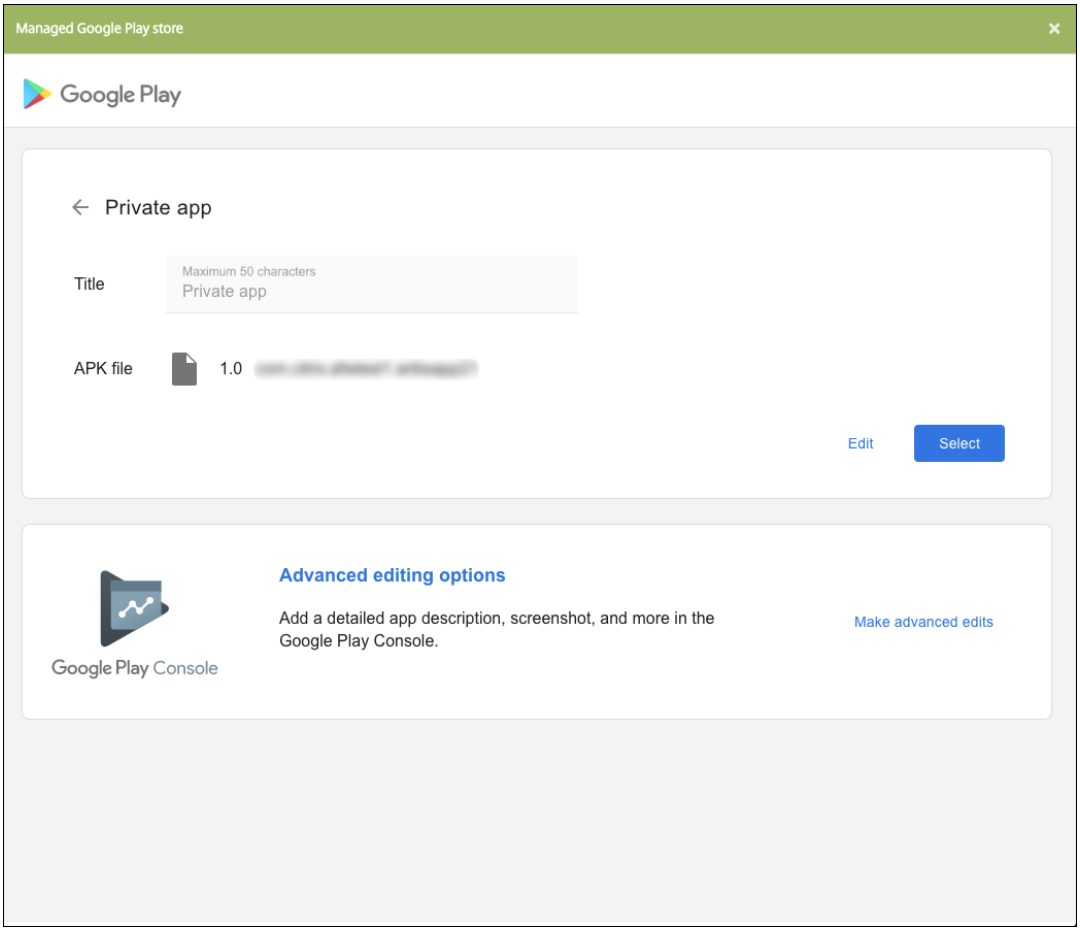
b) Entrez une adresse e-mail pour obtenir des mises à jour sur vos applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



c) Une fois votre application publiée, cliquez sur l'icône correspondant à l'application privée. Si vous souhaitez ajouter une description pour l'application, modifier l'icône de l'application et effectuer d'autres actions, cliquez sur **Apporter des modifications avancées**. Sinon, cliquez sur **Sélectionner** pour ouvrir la page d'informations sur l'application.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

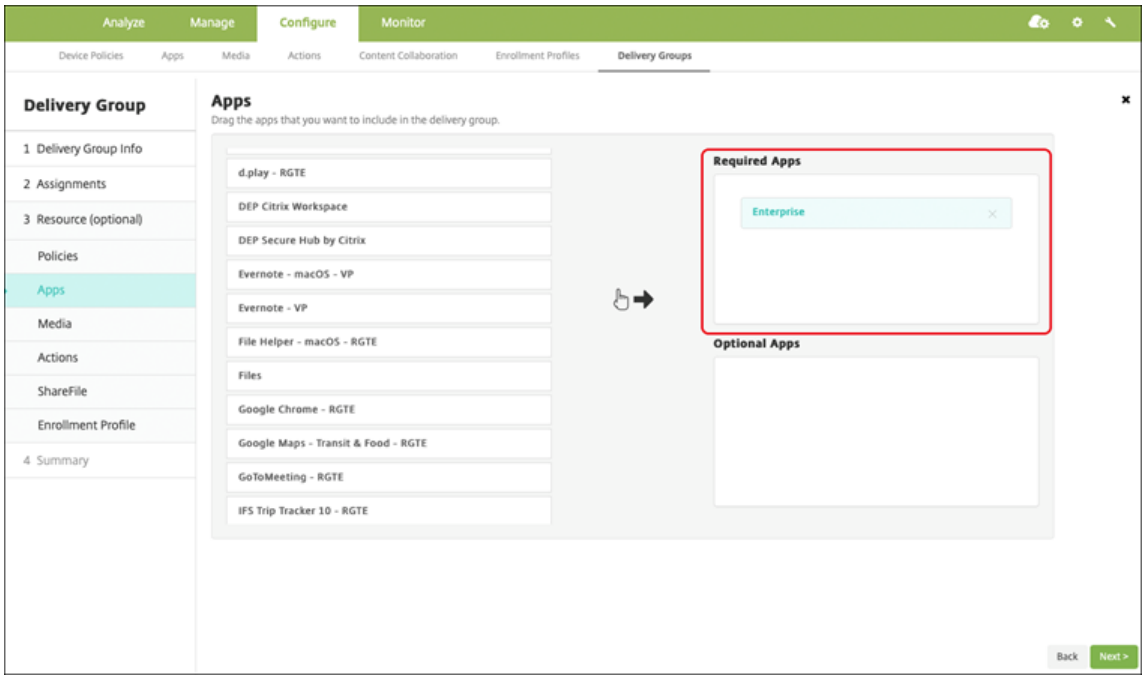


5. Cliquez sur **Suivant**. La page d'informations sur l'application pour la plate-forme s'affiche.
6. Configurez les paramètres pour le type de plate-forme, notamment :
   - **Nom du fichier :** entrez un nouveau nom pour l'application (facultatif).
   - **Description de l'application :** entrez une nouvelle description pour l'application (facultatif).
   - **Version de l'application :** vous ne pouvez pas modifier ce champ.
   - **ID de package :** identifiant unique de votre application.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
   - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.
7. Configurez les règles de déploiement et la configuration du magasin.
8. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**. Pour de plus amples informations, consultez la section Déployer des ressources.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Étape 2 : Configurer le déploiement de l'application

1. Accédez à **Configurer > Groupes de mise à disposition** et sélectionnez le groupe de mise à disposition que vous avez configuré. Cliquez sur **Modifier**.
2. Dans la section **Applications**, faites glisser les applications souhaitées vers la zone **Applications requises**.



3. Sur la page **Résumé**, cliquez sur **Enregistrer**.
4. Sur la page **Groupes de mise à disposition**, sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.

Applications privées compatibles MDX

Pour ajouter des applications Android Enterprise en tant qu'applications d'entreprise compatibles MDX :

1. Créez une application Android Enterprise privée et activez MDX sur l'application.
2. Ajoutez l'application sur la console Citrix Endpoint Management.
   - Hébergez et publiez l'application sur le Google Play Store d'entreprise.
   - Ajoutez l'application à la console Citrix Endpoint Management en tant qu'application d'entreprise.
3. Ajoutez le fichier MDX à Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si vous décidez d'héberger et de publier des applications via le Google Play Store, n'optez pas pour la signature de certificat Google. Signez l'application avec le même certificat que celui utilisé pour activer l'application avec MDX. Pour plus d'informations sur la publication d'applications, consultez la documentation Google sur Publier votre application et Signer votre application. Le SDK MAM n'encapsulant pas les applications, il ne nécessite donc pas de certificat autre que celui utilisé pour développer l'application.

Pour plus d'informations sur la publication d'applications privées via la console Google Play, consultez la documentation Google sur la procédure à suivre pour Publier des applications privées depuis la Play Console.

Pour publier une application via Citrix Endpoint Management, consultez les sections suivantes.

Préparer une application Android Enterprise

Lorsque vous créez une application Android Enterprise, assurez-vous de suivre l'article Bonnes pratiques pour les applications privées de Google.

Après avoir créé une application Android Enterprise, intégrez le SDK MAM à l'application ou encapsulez l'application à l'aide de MDX Toolkit. Ensuite, ajoutez les fichiers résultants à XenMobile.

Vous pouvez mettre à jour l'application en téléchargeant un fichier .apk mis à jour. Les étapes suivantes décrivent l'encapsulation de l'application avec MDX Toolkit.

1. Créez votre application Android Enterprise et générez un fichier .apk signé.
2. L'exemple de fichier suivant contient toutes les stratégies connues, dont certaines peuvent ne pas être applicables à votre environnement. Tous les paramètres inutilisables sont ignorés. Créez un fichier XML avec les paramètres suivants :

```
<?xml version="1.0" encoding="UTF-8"?>
<MobileAppPolicies>
    <PolicySchemaVersion>
        1.0
    </PolicySchemaVersion>
    <Policies>
        <DevicePasscode>false</DevicePasscode>
        <AppPasscode>false</AppPasscode>
        <MaxOfflinePeriod>72</MaxOfflinePeriod>
        <StepupAuthAddress/>
        <RequireUserEntropy>false</RequireUserEntropy>
        <BlockRootedDevices>true</BlockRootedDevices>
        <BlockDebuggerAccess>false</BlockDebuggerAccess>
        <RequireDeviceLock>false</RequireDeviceLock>
        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
            NonCompliantDeviceBehavior>
        <WifiOnly>false</WifiOnly>
        <RequireInternalNetwork>false</RequireInternalNetwork>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
18          <InternalWifiNetworks/>
19          <AllowedWifiNetworks/>
20          <UpgradeGracePeriod>168</UpgradeGracePeriod>
21          <WipeDataOnAppLock>false</WipeDataOnAppLock>
22          <ActivePollPeriod>60</ActivePollPeriod>
23          <PublicFileAccessLimitsList/>
24          <CutAndCopy>Unrestricted</CutAndCopy>
25          <Paste>Unrestricted</Paste>
26          <DocumentExchange>Unrestricted</DocumentExchange>
27          <OpenInExclusionList/>
28          <InboundDocumentExchange>Unrestricted</
               InboundDocumentExchange>
29          <InboundDocumentExchangeWhitelist/>
30          <connectionSecurityLevel>TLS</connectionSecurityLevel>
31          <DisableCamera>false</DisableCamera>
32          <DisableGallery>false</DisableGallery>
33          <DisableMicrophone>false</DisableMicrophone>
34          <DisableLocation>false</DisableLocation>
35          <DisableSms>false</DisableSms>
36          <DisableScreenCapture>false</DisableScreenCapture>
37          <DisableSensor>false</DisableSensor>
38          <DisableNFC>false</DisableNFC>
39          <BlockLogs>false</BlockLogs>
40          <DisablePrinting>false</DisablePrinting>
41          <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
               MvpnNetworkAccess>
42          <MvpnSessionRequired>False</MvpnSessionRequired>
43          <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>
44          <DisableLocalhostConnections>false</
               DisableLocalhostConnections>
45          <CertificateLabel/>
46          <DefaultLoggerOutput>file,console</DefaultLoggerOutput>
47          <DefaultLoggerLevel>15</DefaultLoggerLevel>
48          <MaxLogFiles>2</MaxLogFiles>
49          <MaxLogFileSize>2</MaxLogFileSize>
50          <RedirectSystemLogs>false</RedirectSystemLogs>
51          <EncryptLogs>false</EncryptLogs>
52          <GeofenceLongitude>0</GeofenceLongitude>
53          <GeofenceLatitude>0</GeofenceLatitude>
54          <GeofenceRadius>0</GeofenceRadius>
55          <EnableGoogleAnalytics>false</EnableGoogleAnalytics>
56          <Authentication>OfflineAccessOnly</Authentication>
57          <ReauthenticationPeriod>480</ReauthenticationPeriod>
58          <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
59      </Policies>
60  </MobileAppPolicies>
61  <!--NeedCopy-->
```

3. Encapsulez l'application à l'aide de l'outil MDX Toolkit. Pour de plus amples informations sur l'utilisation de l'outil MDX Toolkit, consultez la section Encapsulation d'applications mobiles Android.

   Définissez le paramètre **apptype** sur **Premium**. Utilisez le fichier XML de l'étape précédente

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

dans la commande décrite ci-dessous.

Si vous connaissez l'URL de magasin de l'application, définissez le paramètre **storeURL** sur l'URL du magasin. Les utilisateurs téléchargent l'application à partir de l'URL du magasin après la publication de l'application.

Voici un exemple de commande MDX Toolkit utilisée pour encapsuler une application appelée SampleAEapp :

```
 java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -Duser.variant
 -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
 -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
 -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
 -MinPlatform 5.0
 -keystore /MyKeystore
 -storepass mystorepwd123
 -keyalias key0
 -keypass mykeypwd123
 -storeURL "https://play.google.com/store/apps/details?id=SampleAEappPackage"
 -appType Premium
 -premiumMdxPolicies <Path to Premium policy XML>
```

L'encapsulation de l'application génère un fichier .apk encapsulé et un fichier .mdx.

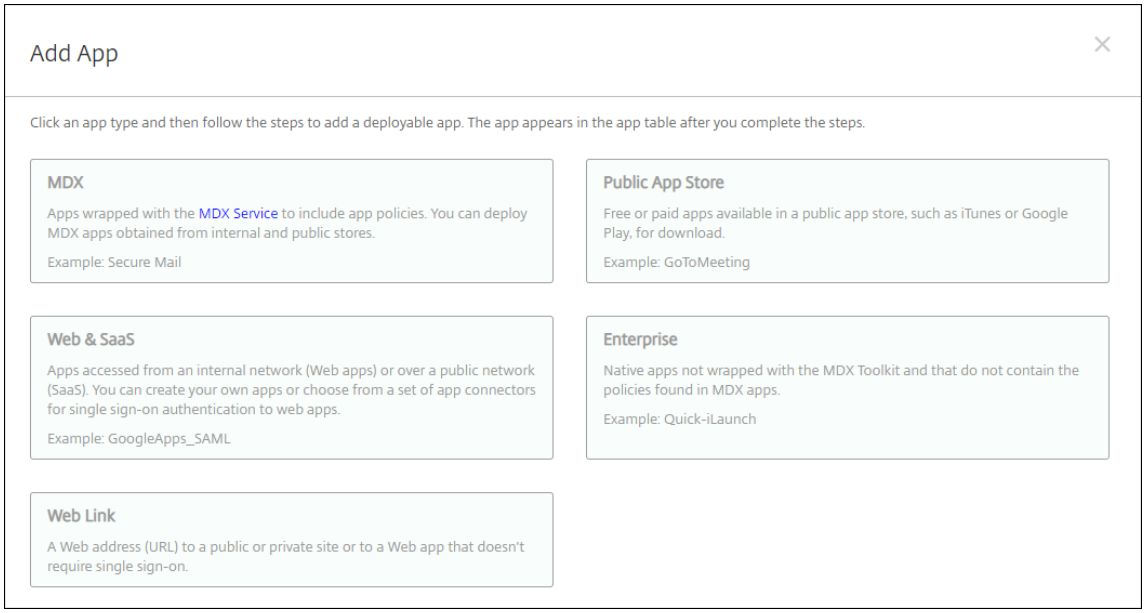
Ajouter le fichier .apk encapsulé

Ajoutez l'application à l'aide d'une des deux façons suivantes :

- Publiez l'application directement sur le Google Play Store d'entreprise et ajoutez-la à la console Citrix Endpoint Management en tant qu'application Play Store d'entreprise. Suivez la procédure Publier des applications privées de la documentation Google, puis suivez les étapes décrites dans la section Applications gérées du magasin d'applications.
- Ajoutez l'application à la console Citrix Endpoint Management en tant qu'application d'entreprise. Effectuez les opérations suivantes :

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications**. La page **Applications** s'ouvre.
2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



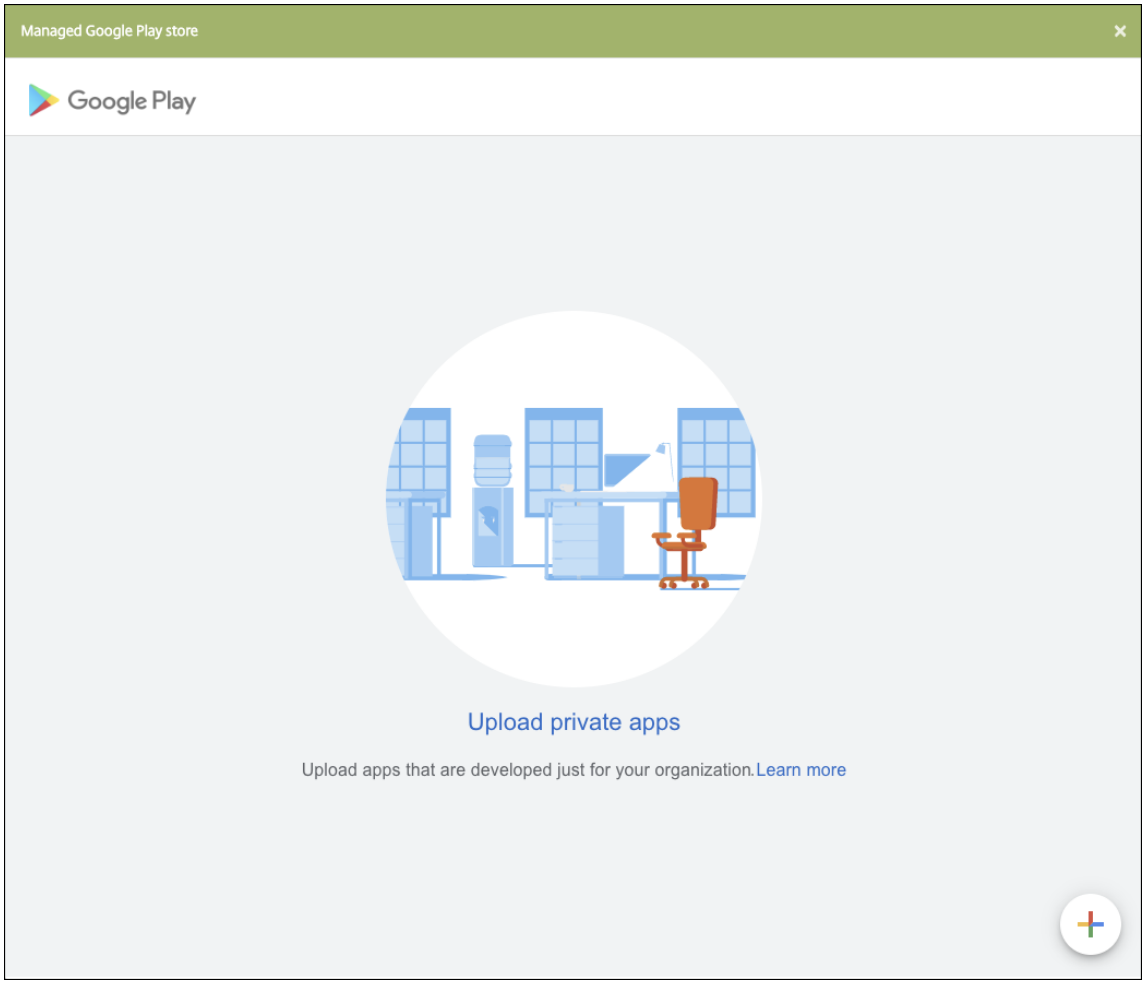
3. Cliquez sur **Entreprise**. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :

   - **Nom :** entrez un nom descriptif pour l'application. Il apparaît sous Nom de l'application dans le tableau Applications.
   - **Description :** entrez une description pour l'application (facultatif).

4. Sélectionnez **Android Enterprise** comme plate-forme.

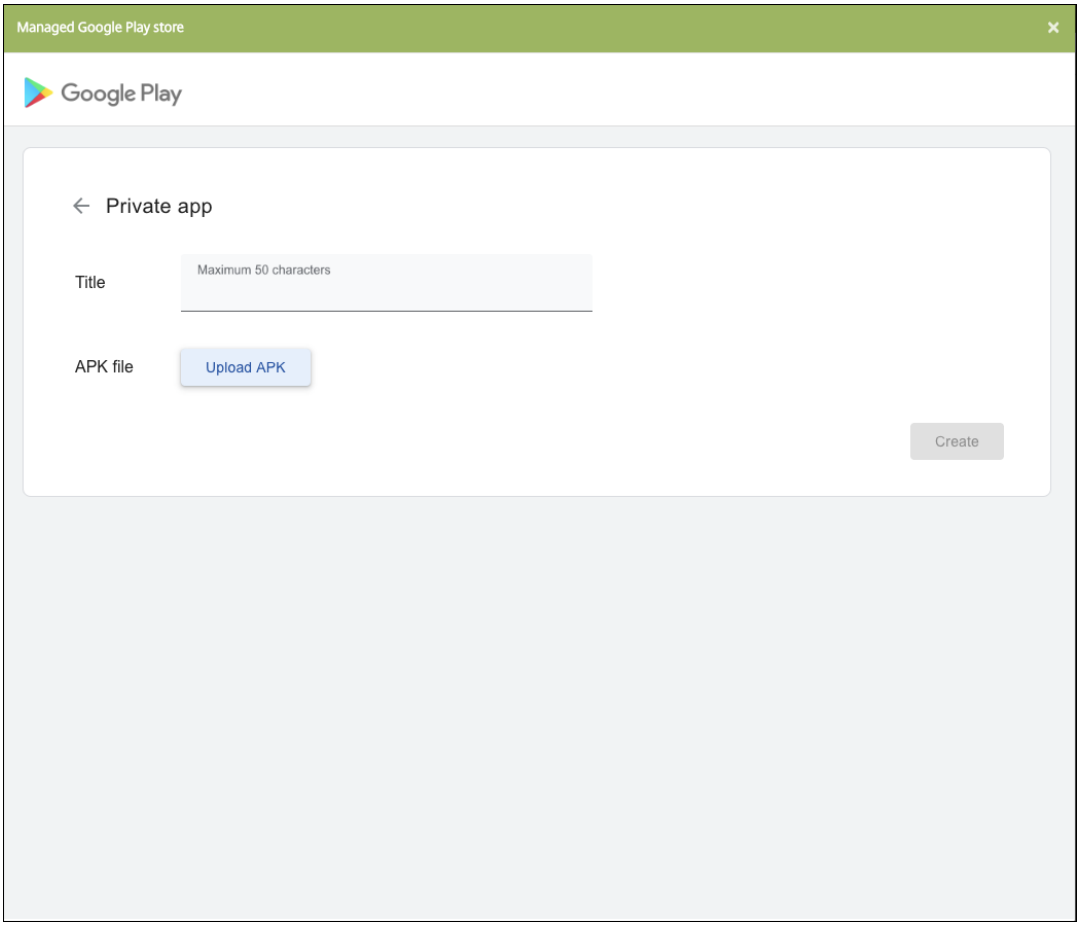
5. Le bouton **Charger** ouvre le Google Play Store d'entreprise. Vous n'avez pas besoin de vous inscrire pour créer un compte de développeur et publier une application privée. Cliquez sur l'icône **Plus** dans le coin inférieur droit pour continuer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



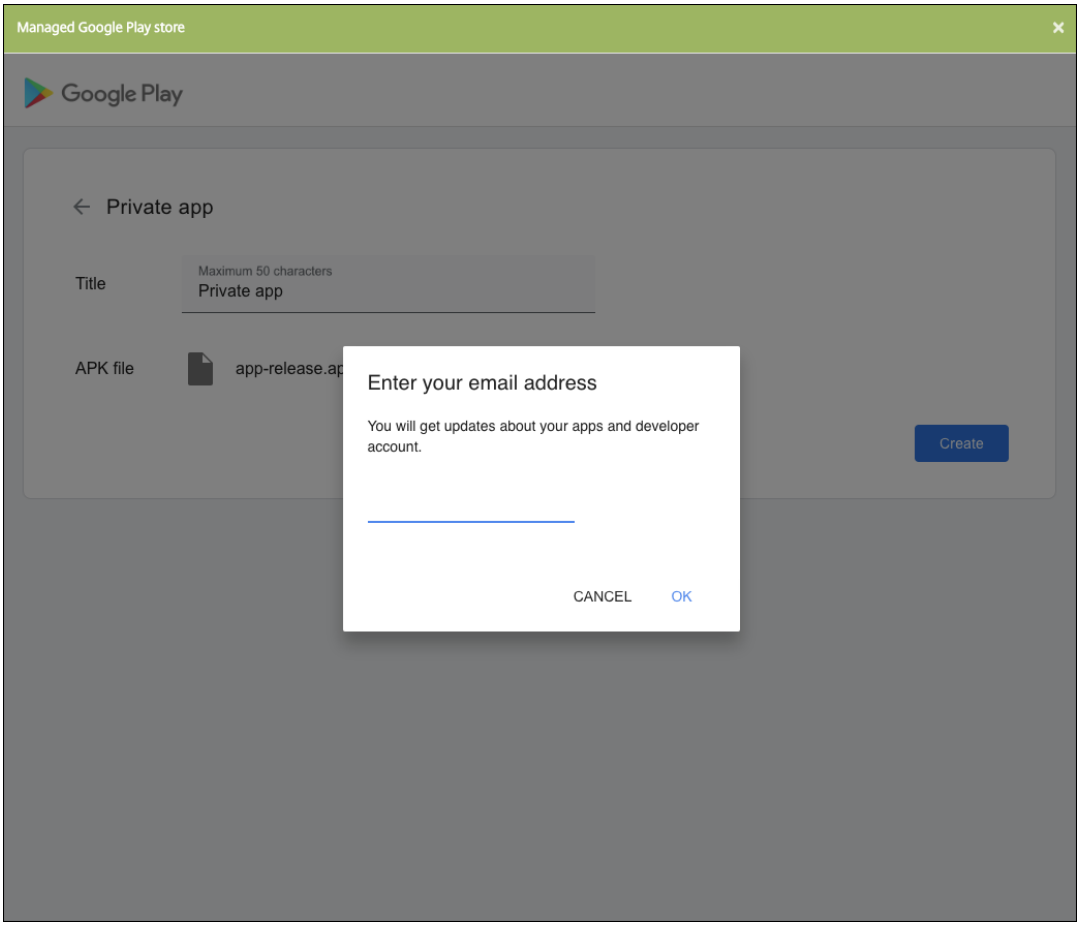
a) Tapez le nom de votre application et chargez le fichier .apk. Lorsque vous avez terminé, cliquez sur **Créer**. La publication de votre application privée peut prendre jusqu'à 10 minutes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



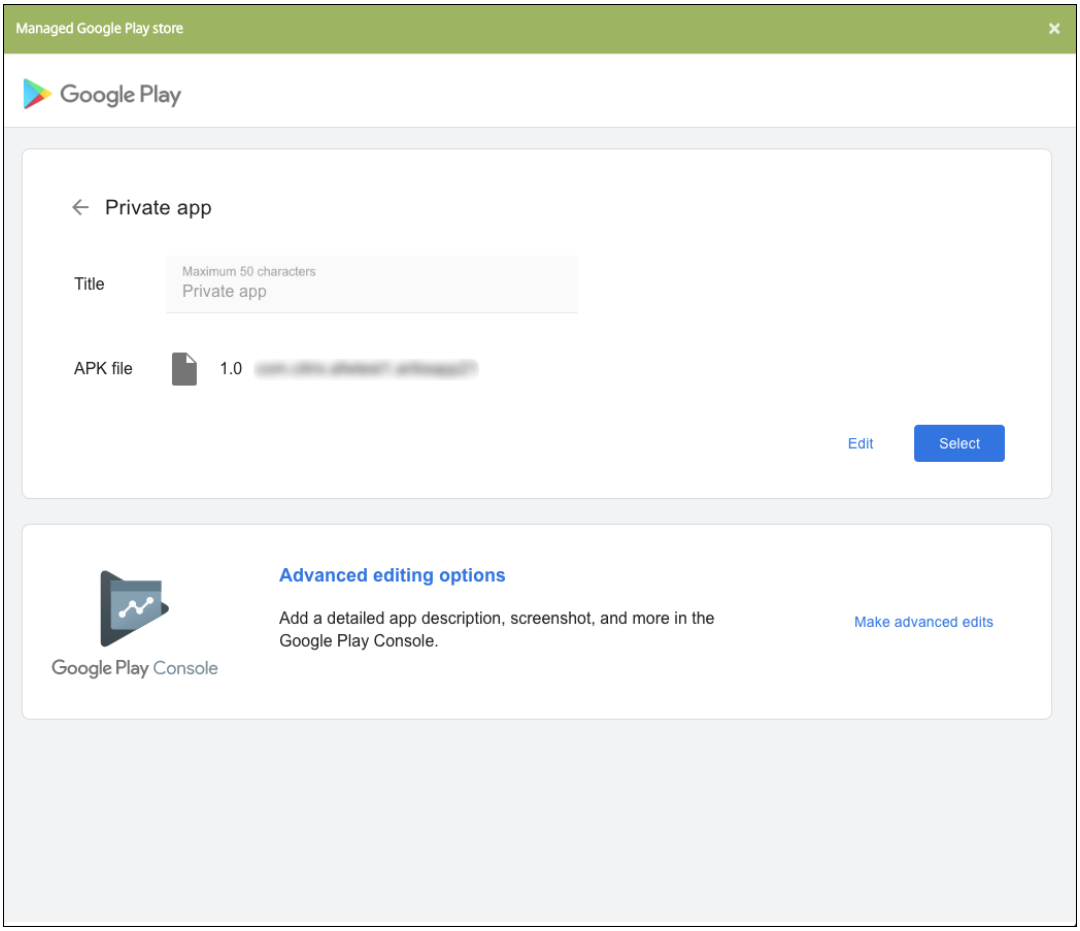
b) Entrez une adresse e-mail pour obtenir des mises à jour sur vos applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



c) Une fois votre application publiée, cliquez sur l'icône correspondant à une application privée, puis sur **Sélectionner** pour ouvrir la page d'informations de l'application.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Cliquez sur **Suivant**. La page d'informations sur l'application pour la plate-forme s'affiche.
7. Configurez les paramètres pour le type de plate-forme, notamment :
   - **Nom du fichier :** entrez un nouveau nom pour l'application (facultatif).
   - **Description de l'application :** entrez une nouvelle description pour l'application (facultatif).
   - **Version de l'application :** vous ne pouvez pas modifier ce champ.
   - **ID de package :** identifiant unique de votre application.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
   - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.
8. Configurez les règles de déploiement et la configuration du magasin.
9. Sur la page **Application d'entreprise**, cliquez sur **Suivant**. La page **Approbations** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour utiliser des workflows afin d'exiger une approbation avant d'autoriser les utilisateurs à accéder à l'application, consultez la section Appliquer les workflows. Si vous n'avez pas besoin de workflows d'approbation, vous pouvez passer à l'étape 13.

10. Cliquez sur **Suivant**.
11. La page **Attribution de groupes de mise à disposition** s'affiche. Aucune action n'est nécessaire sur cette page. Vous configurez les groupes de mise à disposition et le calendrier de déploiement pour cette application lorsque vous ajoutez le fichier .mdx. Cliquez sur **Save**.

Facultatif : ajouter ou modifier l'URL du magasin

Si vous ne connaissiez pas l'URL du magasin lorsque vous avez encapsulé l'application, ajoutez l'URL du magasin maintenant.

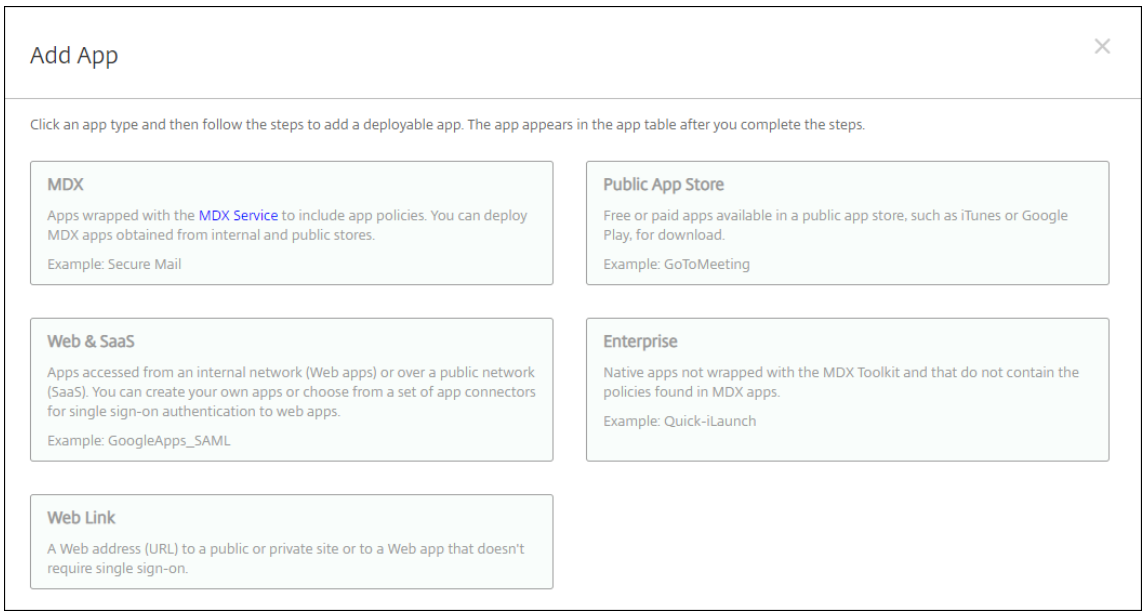
1. Affichez l'application dans le Google Play Store d'entreprise. Lorsque vous sélectionnez l'application, l'URL du magasin apparaît dans la barre d'adresse de votre navigateur. Copiez le nom du package de l'application à partir du formulaire URL. Par exemple : `https://play.google.com/store/apps/details?id=SampleAEappPackage`. L'URL que vous copiez peut commencer par `https://play.google.com/work/`. Assurez-vous de remplacer `work` par `store`.
2. Utilisez le MDX Toolkit pour ajouter l'URL du magasin au fichier .mdx :

```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \
setinfo \
-in ~/Desktop/SampleApps/Sample.mdx \
-out ~/Desktop/SampleApps/wrapped/Sample.mdx \
-storeURL "https://play.google.com/store/apps/details?id=
    SampleAEappPackage"
<!--NeedCopy-->
```

Ajouter le fichier .mdx

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications**. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



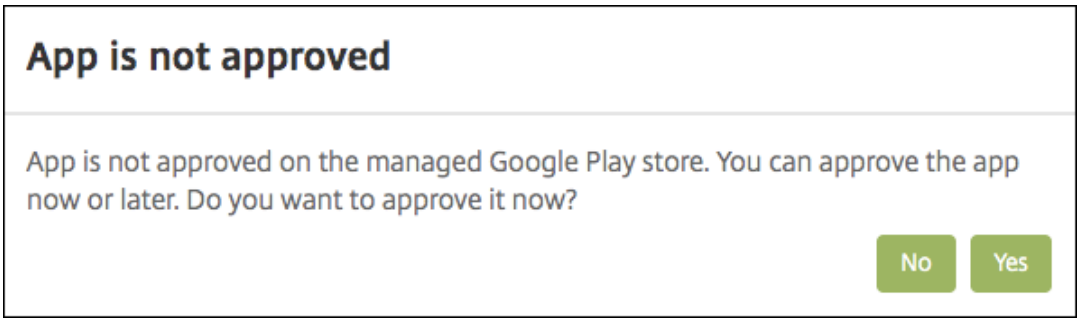
2. Cliquez sur **MDX**. La page **Informations sur l'application MDX** s'affiche. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :

   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous **Nom de l'application** dans le tableau **Applications**.
   - **Description :** entrez une description pour l'application (facultatif).

3. Sélectionnez **Android Enterprise** comme plate-forme.

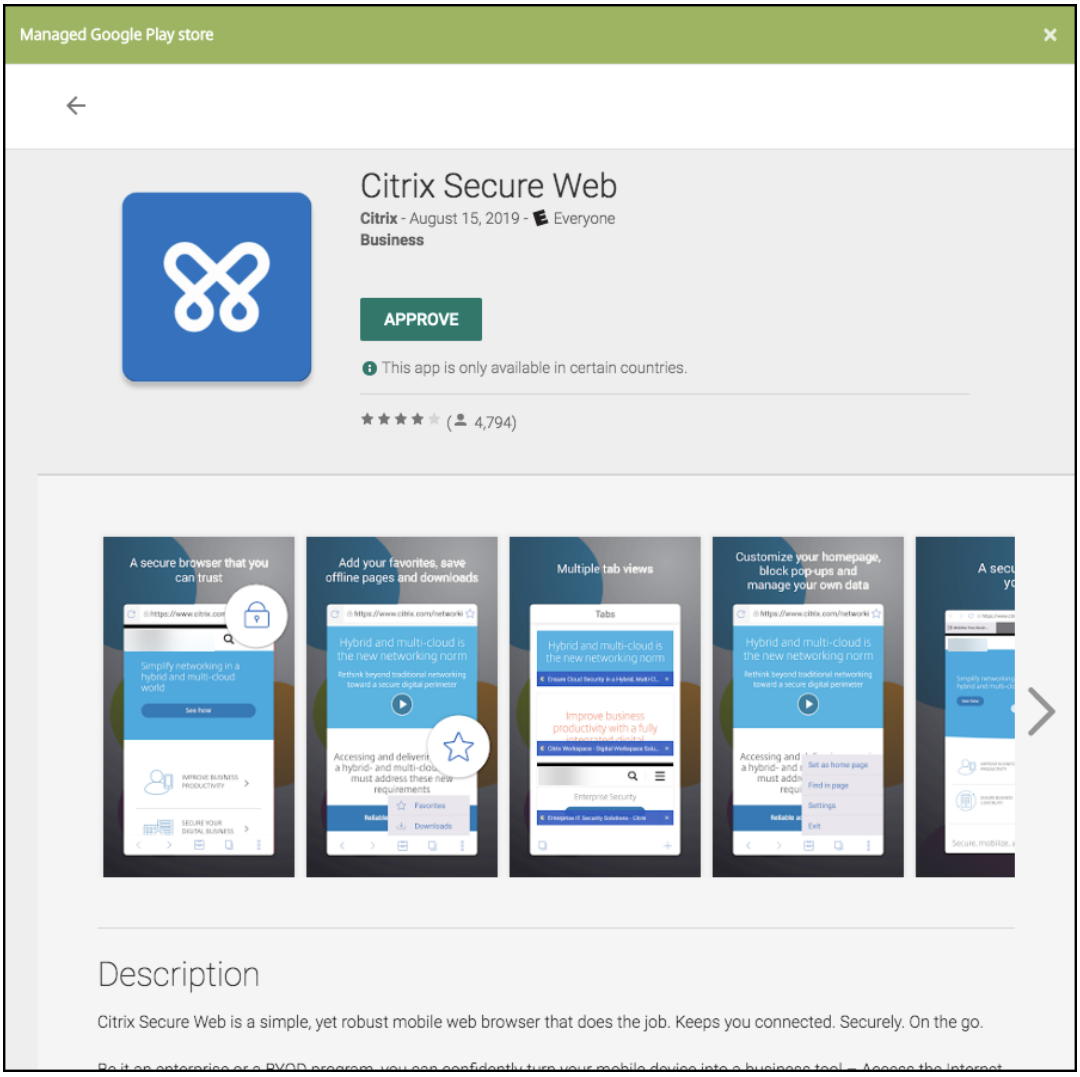
4. Cliquez sur **Charger** et accédez au fichier MDX. Android Enterprise prend uniquement en charge les applications encapsulées avec MDX Toolkit.

   - L'interface utilisateur vous avertit si l'application jointe nécessite l'approbation du Google Play Store d'entreprise. Pour approuver l'application sans quitter la console Citrix Endpoint Management, cliquez sur **Oui**.

     Après l'ouverture du Google Play Store d'entreprise, suivez les instructions pour approuver et enregistrer l'application.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Lorsque vous ajoutez l'application, la page de **Détails sur l'application** apparaît.

5. Pour configurer ces paramètres :

   - **Nom du fichier :** entrez le nom du fichier associé à l'application.
   - **Description de l'application :** entrez une description pour l'application.
   - **Version de l'application :** si vous le souhaitez, entrez le numéro de version de l'application.
   - **ID de package :** entrez l'ID du package de l'application, obtenu à partir du Google Play Store d'entreprise.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
   - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

peuvent pas exécuter l'application.

6. Configurez les **stratégies MDX**. Les stratégies MDX varient selon la plate-forme et incluent des options dans des domaines de stratégie tels que l'authentification, la sécurité de l'appareil et les restrictions applicatives. Dans la console, les stratégies ont une info-bulle qui décrit chacune d'entre elles. Pour plus d'informations sur les stratégies applicatives disponibles pour chaque type de plate-forme, consultez :

   - Présentation du SDK MAM
   - Synopsis des stratégies applicatives tierces MDX

7. Configurez les règles de déploiement et la configuration du magasin.

   L'option **Déployer pour les connexions permanentes** s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

   L'option de connexion permanente :

   - N'est pas disponible pour les appareils iOS.
   - N'est pas disponible pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec la version 10.18.19 ou ultérieure
   - N'est pas recommandée pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec une version antérieure à la version 10.18.19

   Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

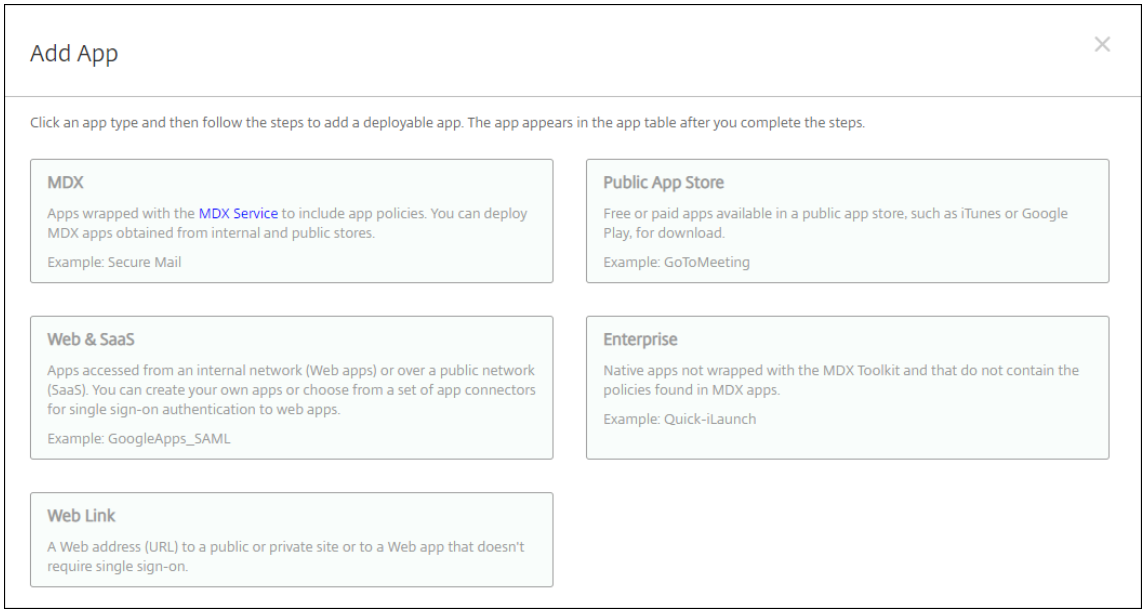
8. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**. Pour de plus amples informations, consultez la section Déployer des ressources.

Mettre à jour l'application

Pour mettre à jour l'application Android Enterprise, encapsulez et téléchargez un fichier .apk mis à jour :

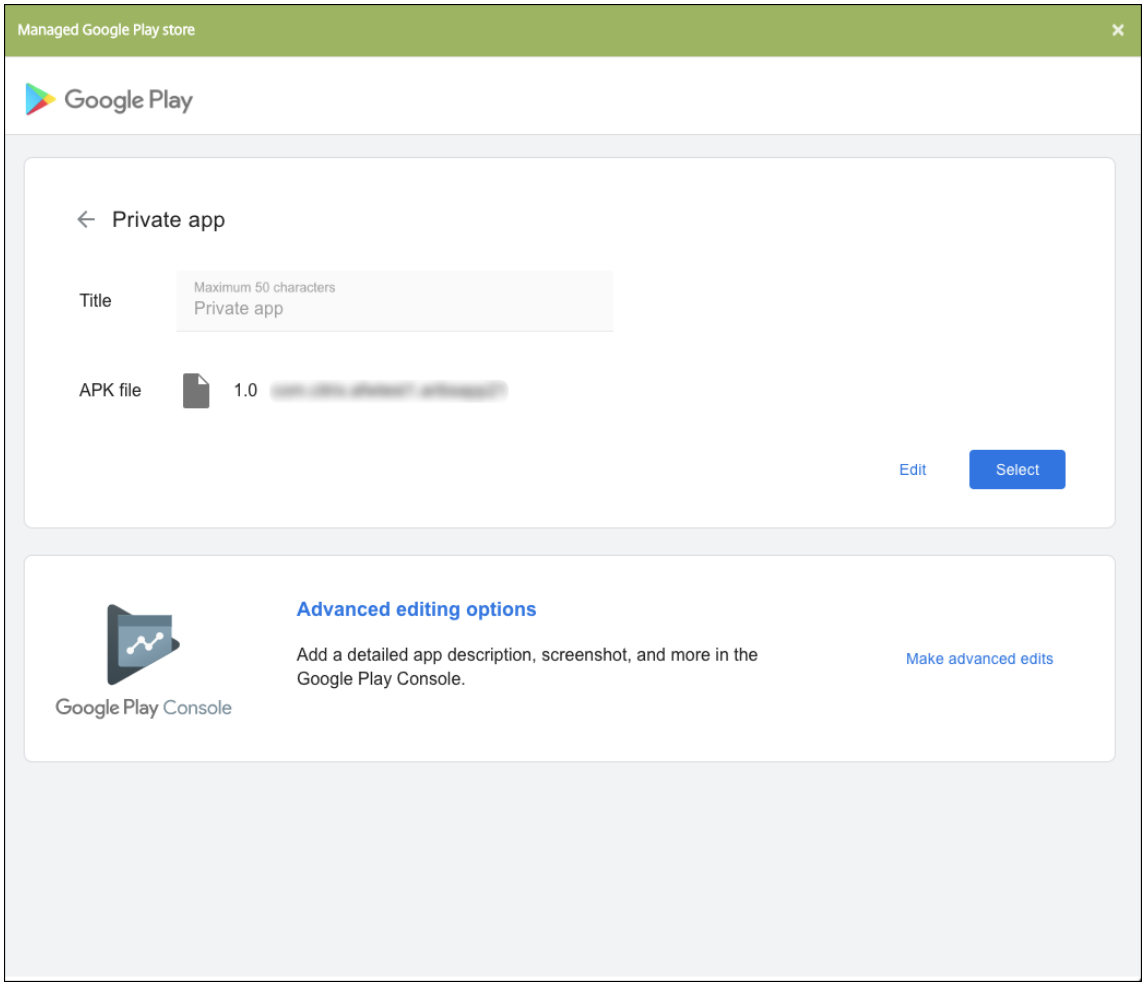
1. Encapsulez le fichier .apk de l'application mise à jour à l'aide du SDL MAM ou de MDX Toolkit.
2. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications**. La page **Applications** s'ouvre.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.
4. Cliquez sur **Entreprise**. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Il apparaît sous Nom de l'application dans le tableau Applications.
   - **Description :** entrez une description pour l'application (facultatif).
5. Sélectionnez **Android Enterprise** comme plate-forme.
6. Cliquez sur **Suivant**. La page **Application d'entreprise** s'affiche.
7. Cliquez sur **Charger**.
8. Sur la page Google Play Store d'entreprise, sélectionnez l'application que vous souhaitez mettre à jour.
9. Sur la page d'informations sur l'application, cliquez sur **Modifier** en regard du nom du fichier .apk.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



10. Accédez au nouveau fichier .apk et chargez-le.
11. Sur la page Google Play Store d'entreprise, cliquez sur **Enregistrer**.

Ancienne version d'Android Enterprise pour clients Google Workspace (anciennement G Suite)

November 29, 2023

Les clients Google Workspace doivent utiliser les paramètres de l'ancienne version d'Android Entreprise pour configurer une ancienne version d'Android Entreprise. « G Suite » a récemment été renommé « Google Workspace » par Google.

Si votre organisation utilise déjà Google Workspace pour permettre aux utilisateurs d'accéder aux applications Google, vous pouvez utiliser Google Workspace pour enregistrer Citrix comme fournisseur EMM. Si votre organisation utilise Google Workspace, elle dispose d'un identifiant d'entreprise et de

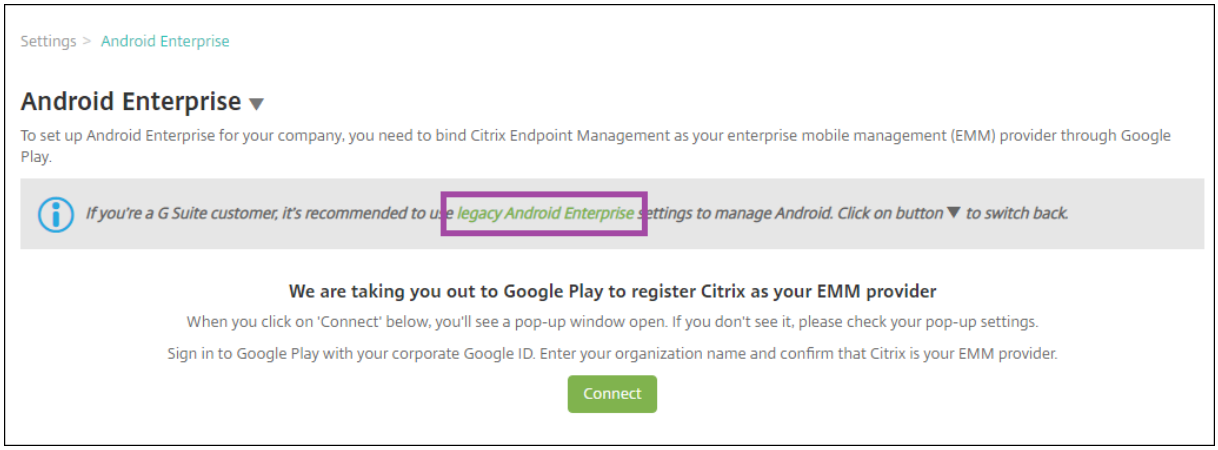
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

comptes Google existants pour les utilisateurs. Pour utiliser Citrix Endpoint Management avec Google Workspace, vous synchronisez vos données avec votre annuaire LDAP et récupérez les informations de compte Google à partir de Google à l'aide de l'API Google Directory. Étant donné que ce type d'entreprise est lié à un domaine existant, chaque domaine ne peut créer qu'une seule entreprise. Pour inscrire un appareil dans Citrix Endpoint Management, chaque utilisateur doit se connecter manuellement avec son compte Google existant. Le compte lui donne accès à Google Play d'entreprise en plus des autres services Google fournis par le forfait Google Workspace.

Configuration requise pour l'ancienne version d'Android Entreprise :

- Un domaine publiquement accessible
- Un compte d'administrateur Google
- Des appareils Android avec prise en charge des profils gérés
- Un compte Google sur lequel Google Play est installé
- Un profil de travail configuré sur l'appareil.

Pour démarrer la configuration de l'ancienne version d'Android Entreprise, cliquez sur **Ancienne version de Android Entreprise** dans la page **Android Entreprise** des paramètres Citrix Endpoint Management.



Créer un compte Android Entreprise

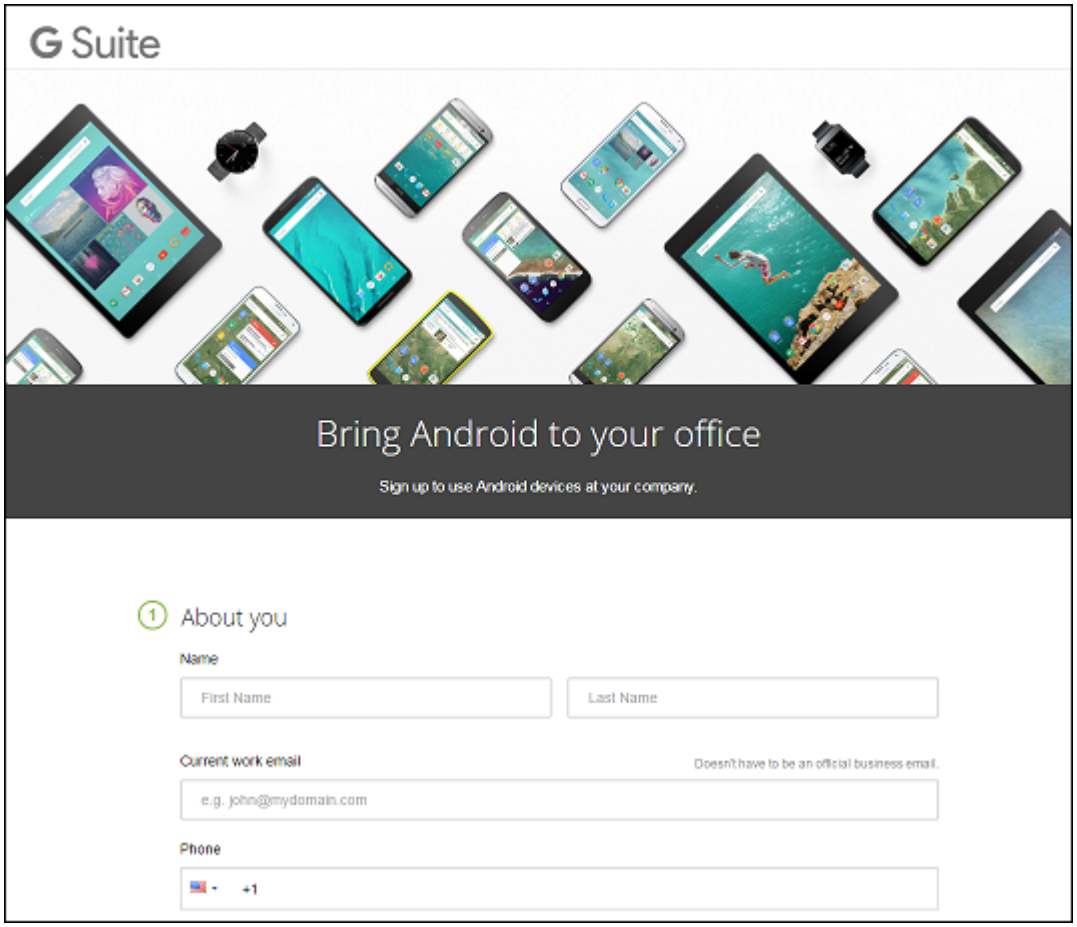
Pour pouvoir configurer un compte Android Entreprise, vous devez vérifier votre nom de domaine auprès de Google.

Si vous avez déjà vérifié votre nom de domaine auprès de Google, vous pouvez passer à cette étape : Configurer un compte de service Android Entreprise et télécharger un certificat Android Entreprise.

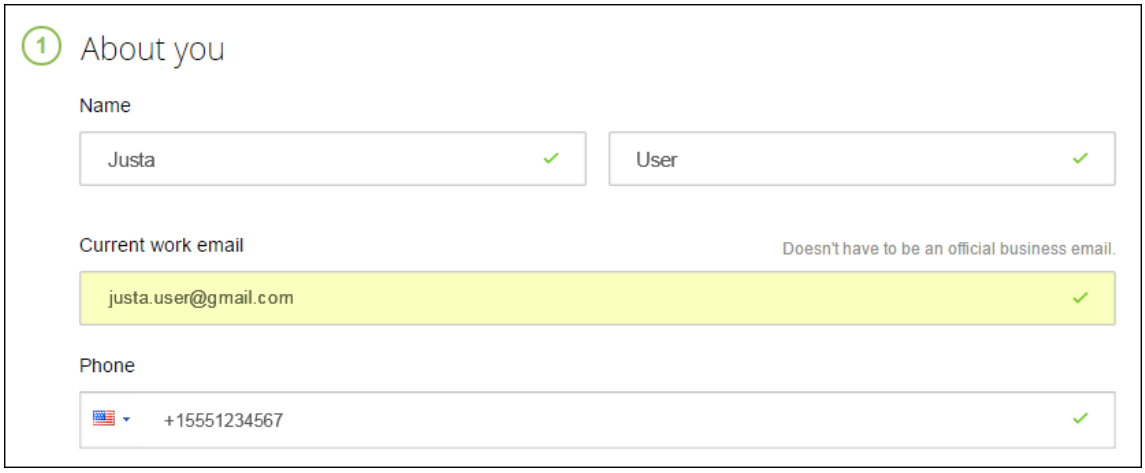
1. Accédez à https://gsuite.google.com/signup/basic/welcome.

   La page suivante s'affiche où vous entrez vos informations d'administrateur et les informations sur l'entreprise.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

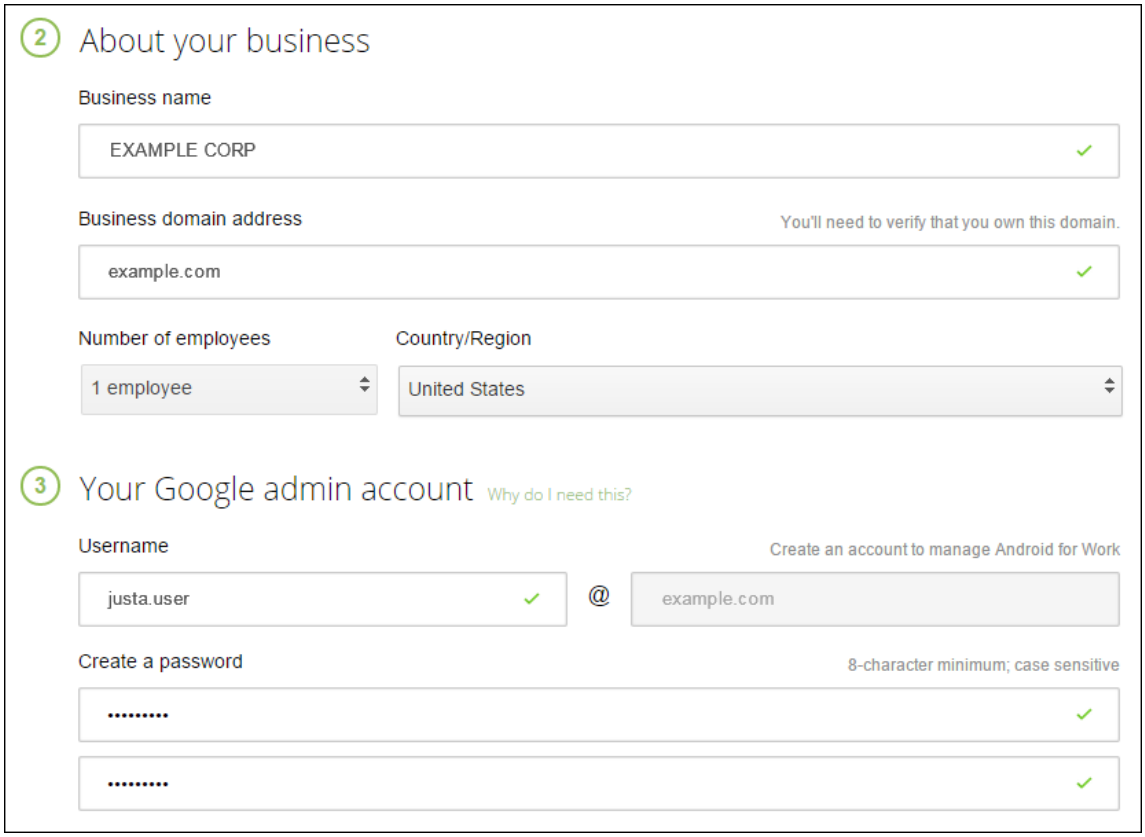


2. Entrez vos informations d'utilisateur administrateur.



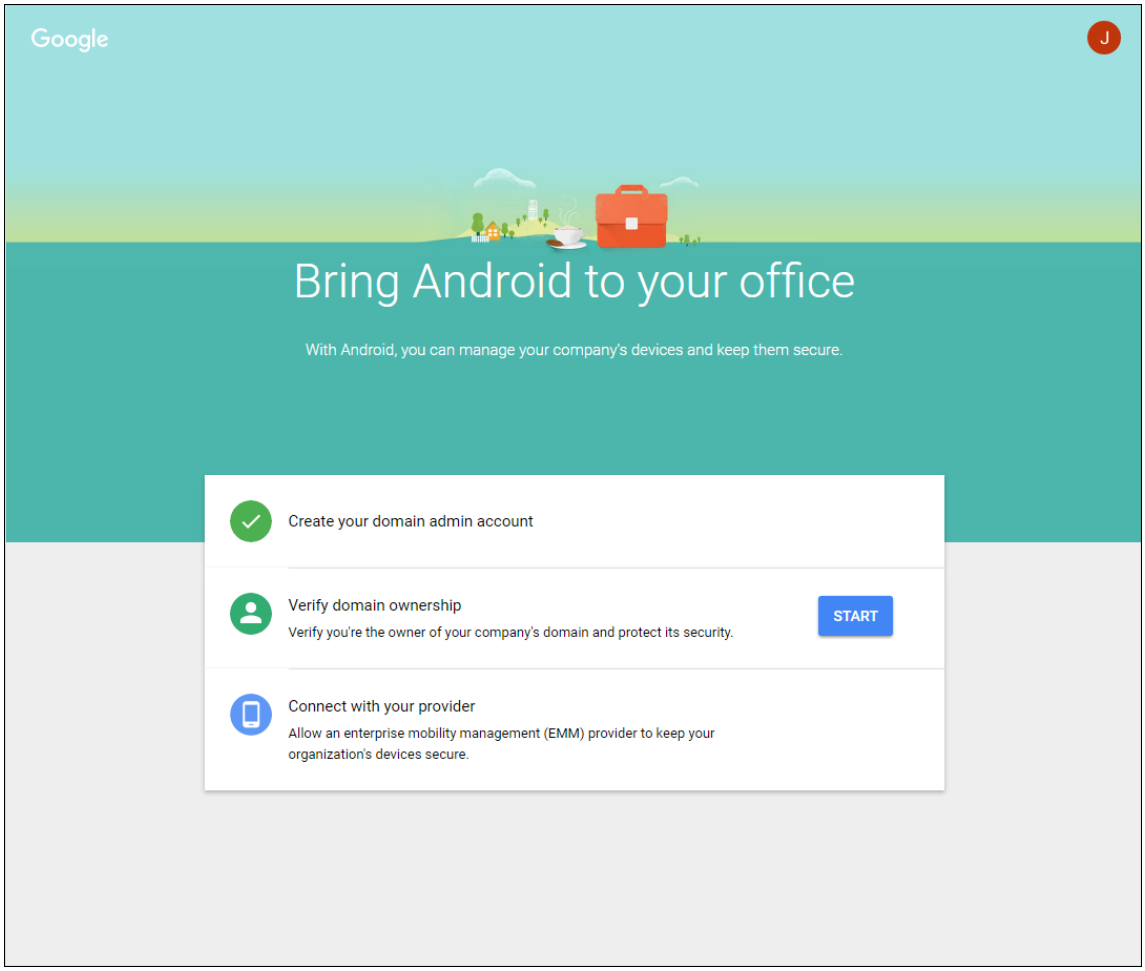
3. Entrez vos informations d'entreprise, en plus de vos informations de compte d'administrateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



La première étape de ce processus est terminée et la page suivante s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Vérifier le propriétaire du domaine

Autorisez Google à vérifier votre domaine de l'une des manières suivantes :

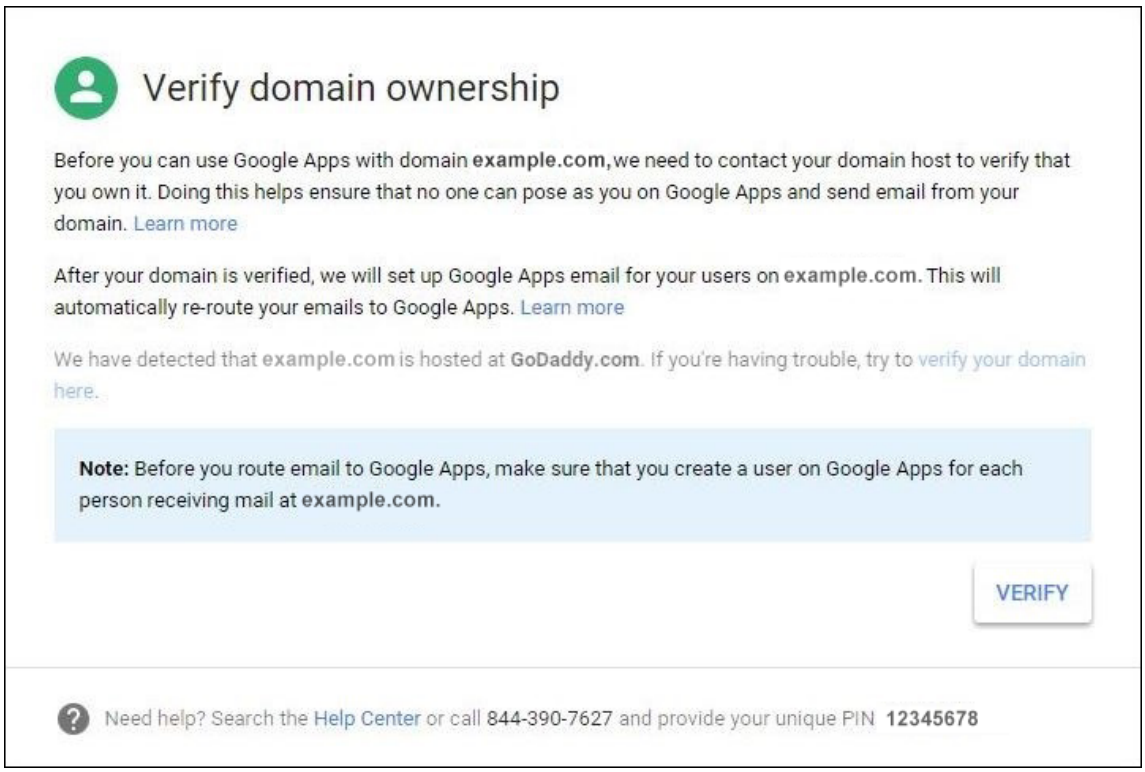
- Ajoutez un enregistrement TXT ou CNAME au site Web de votre hôte de domaine.
- Chargez un fichier HTML sur le serveur Web de votre domaine.
- Ajoutez une balise `<meta>` à votre page d'accueil. Google recommande la première méthode. Cet article ne couvre pas les étapes permettant de vérifier que votre domaine vous appartient, mais vous pouvez trouver les informations dont vous avez besoin sur : https://support.google.com/a/answer/6248925/.

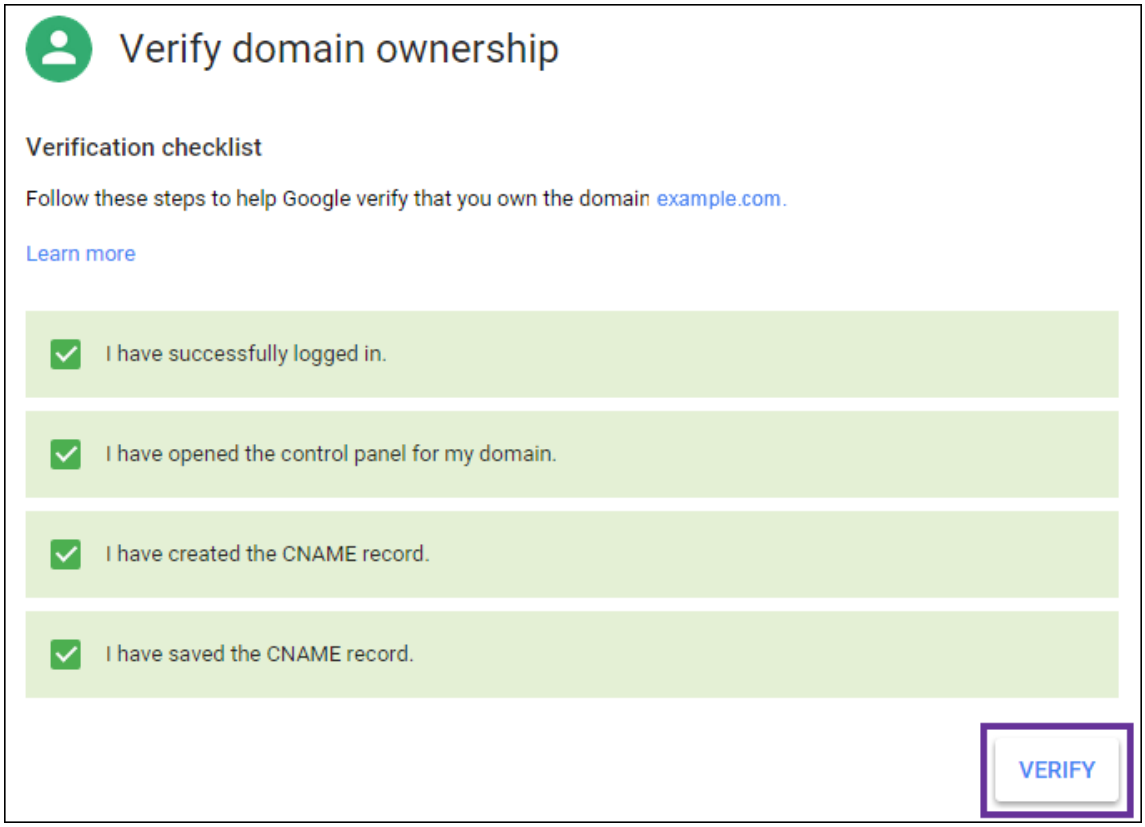
1. Cliquez sur **Démarrer** pour commencer la vérification de votre domaine.

   La page **Valider la propriété du domaine** s'affiche. Suivez les instructions sur la page pour vérifier votre domaine.

2. Cliquez sur **Vérifier**.

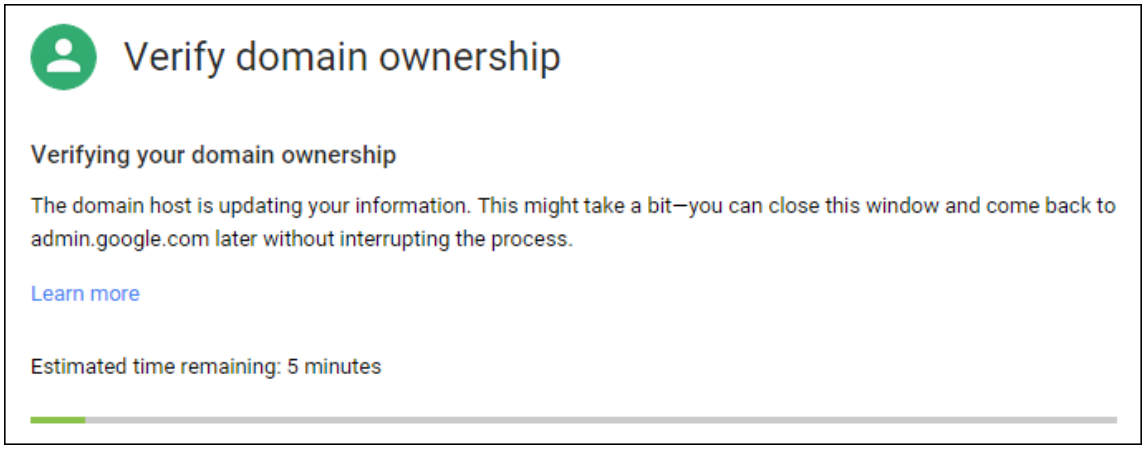
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



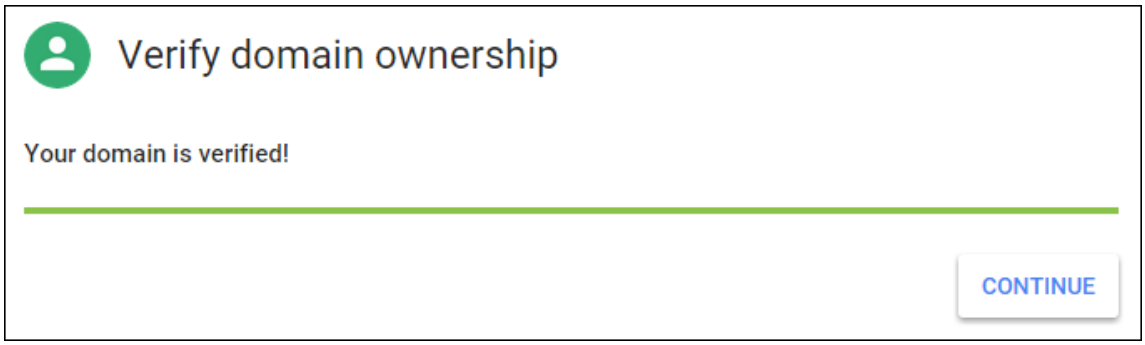


3. Google vérifie que vous êtes le propriétaire du domaine.

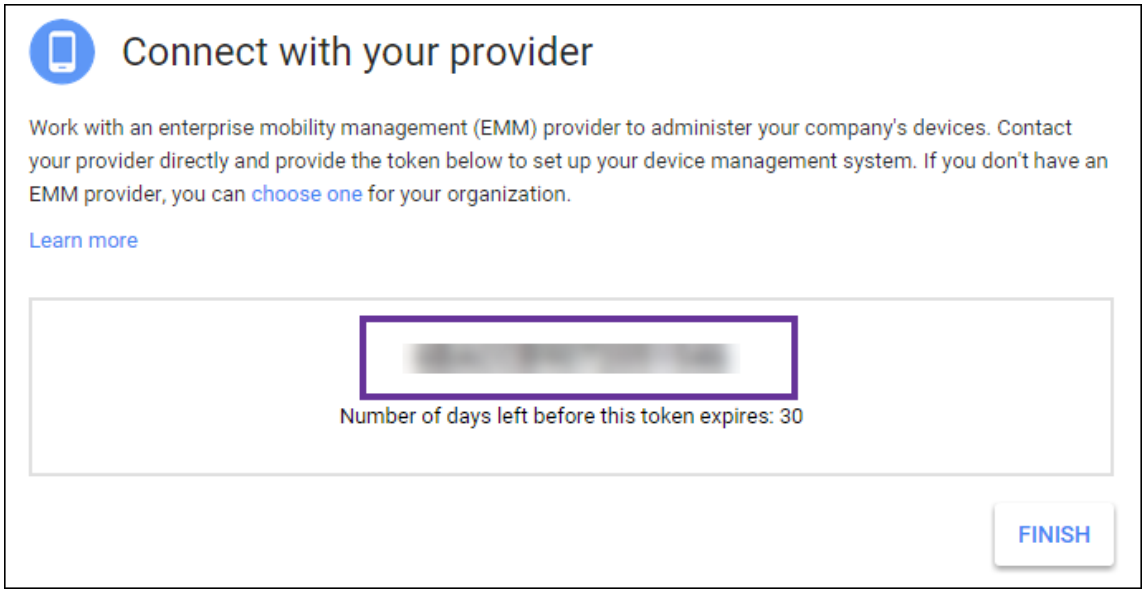
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. La page suivante s'affiche si la vérification réussit. Cliquez sur **Continuer**.



5. Google crée un jeton de liaison EMM que vous fournissez à Citrix lorsque vous configurez les paramètres d'Android Entreprise. Copiez et enregistrez le jeton ; vous en aurez besoin plus tard lors de la configuration.



6. Cliquez sur **Terminer** pour terminer la configuration d'Android Entreprise. Une page s'affiche indiquant que vous avez vérifié avec succès votre domaine.

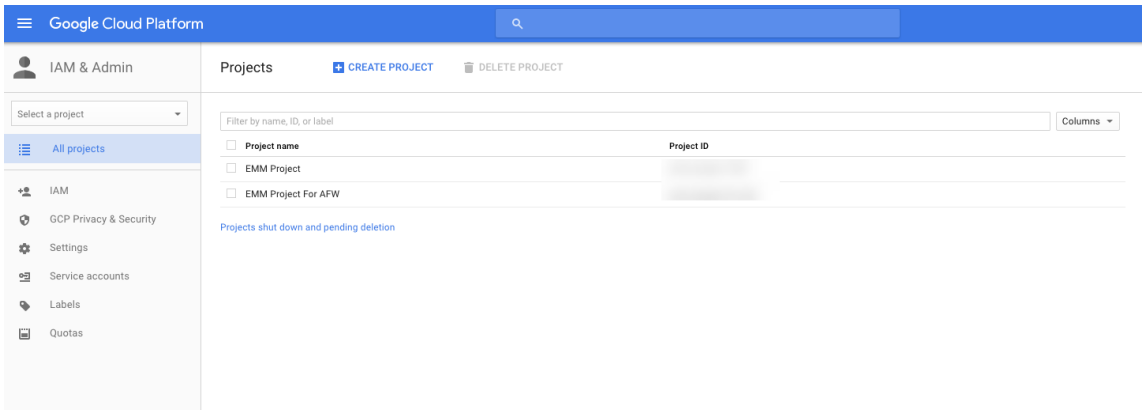
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Une fois que vous avez créé un compte de service Android Entreprise, vous pouvez ouvrir une session sur la console d'administration Google pour gérer vos paramètres de gestion de la mobilité.

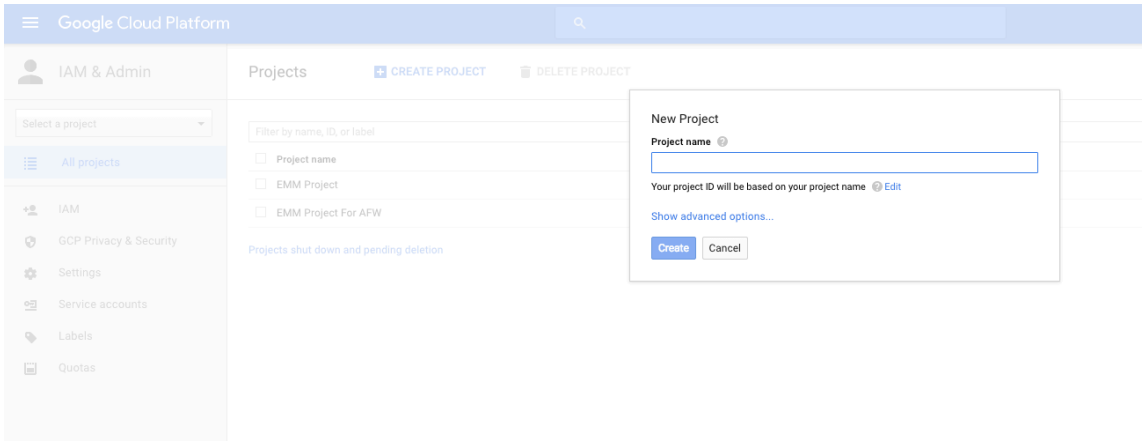
Définir un compte de service Android Entreprise et télécharger un certificat Android Entreprise

Pour autoriser Citrix Endpoint Management à contacter les services Google Play et Directory, vous devez créer un compte de service à l'aide du portail Project de Google destiné aux développeurs. Ce compte de service est utilisé pour permettre les communications entre serveurs entre Citrix Endpoint Management et les services Google pour Android. Pour plus d'informations sur le protocole d'authentification utilisé, accédez à https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

1. Dans un navigateur Web, accédez à https://console.cloud.google.com/project et ouvrez une session à l'aide de vos informations d'identification d'administrateur Google.
2. Dans la liste **Projets**, cliquez sur **Créer un projet**.

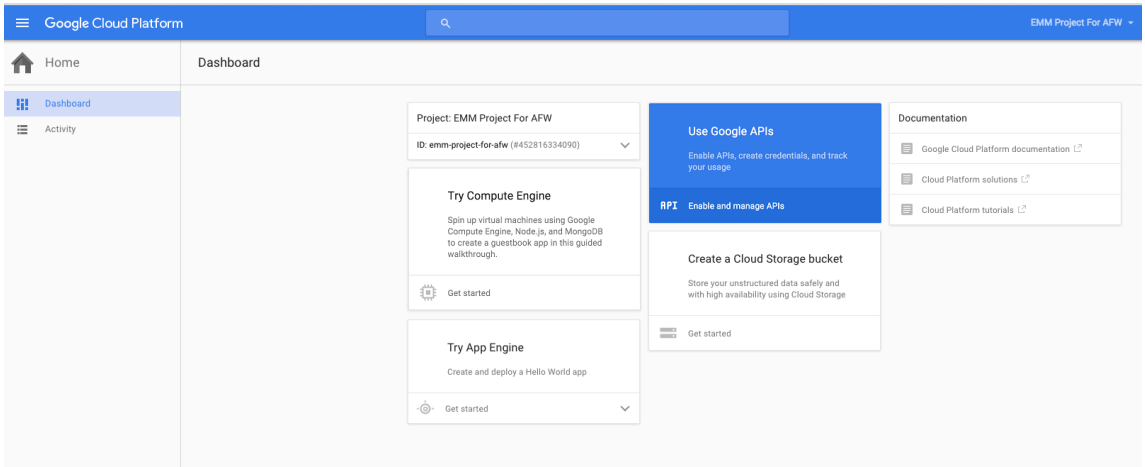


3. Dans **Nom du projet**, entrez un nom pour le projet.

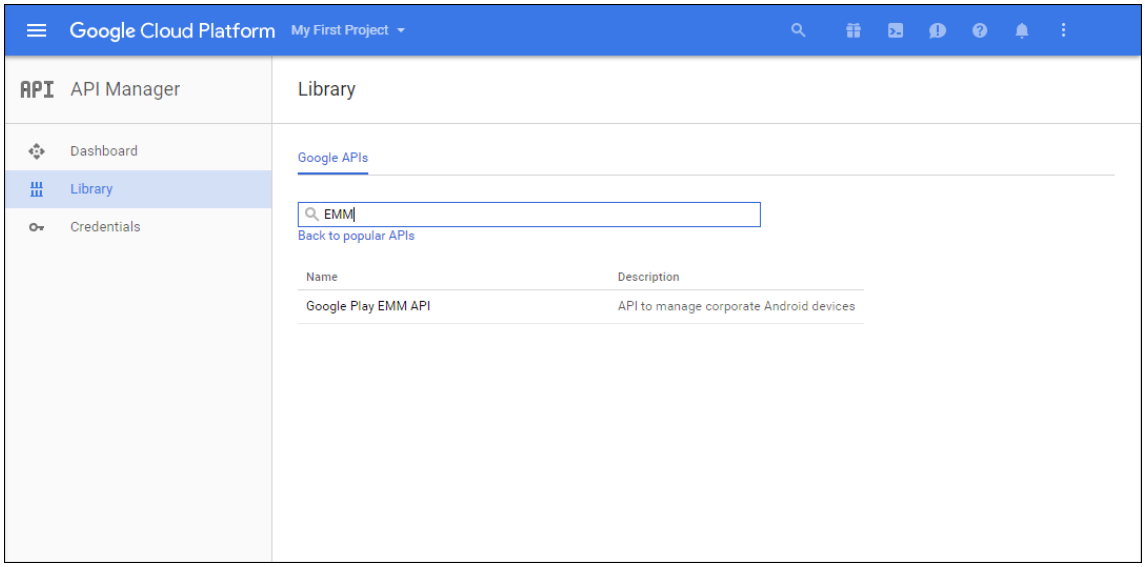


4. Sur le tableau de bord, cliquez sur **Utiliser les API de Google**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

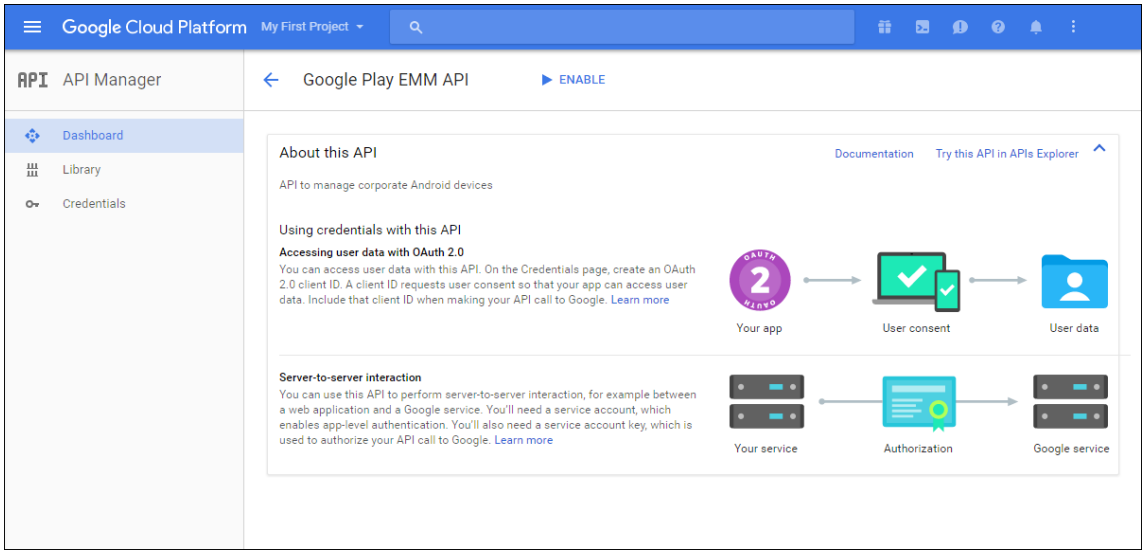


5. Cliquez sur **Bibliothèque** et dans **Rechercher**, entrez **EMM**, puis cliquez sur le résultat de la recherche.

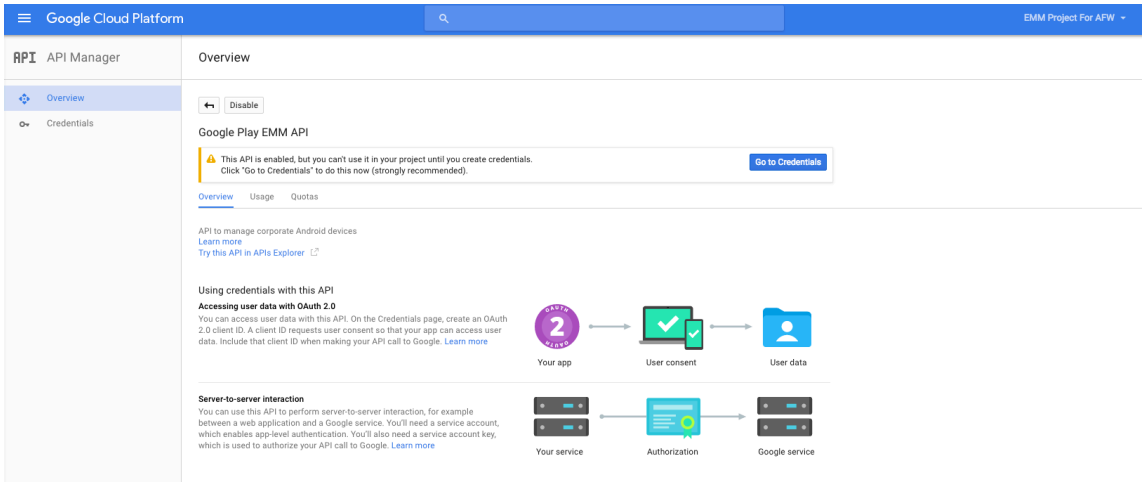


6. Sur la page de **présentation**, cliquez sur **Activer**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

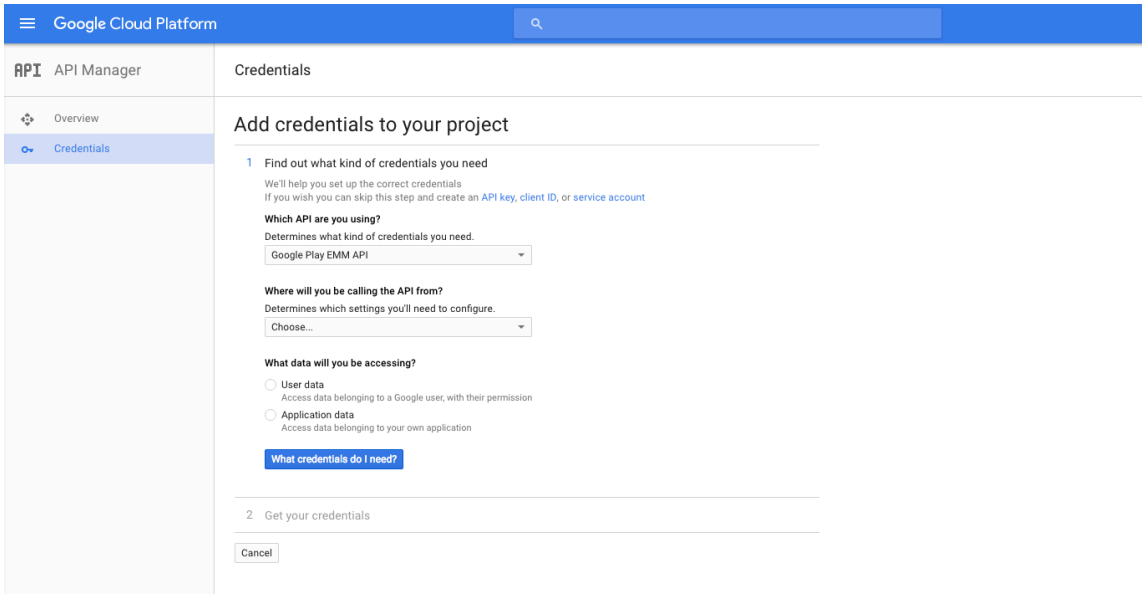


7. En regard de **Google Play EMM API**, cliquez sur **Accéder aux identifiants**.

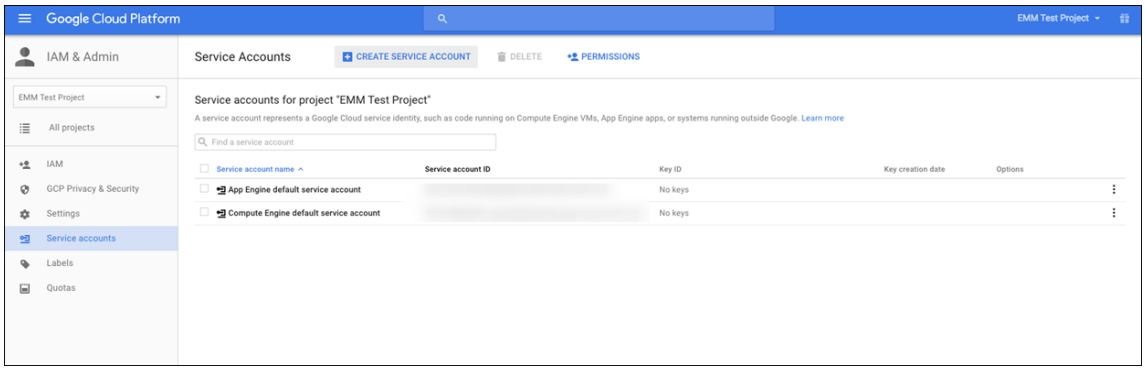


8. Dans la liste **Add credentials to our project**, dans l'étape 1, cliquez sur **service account**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

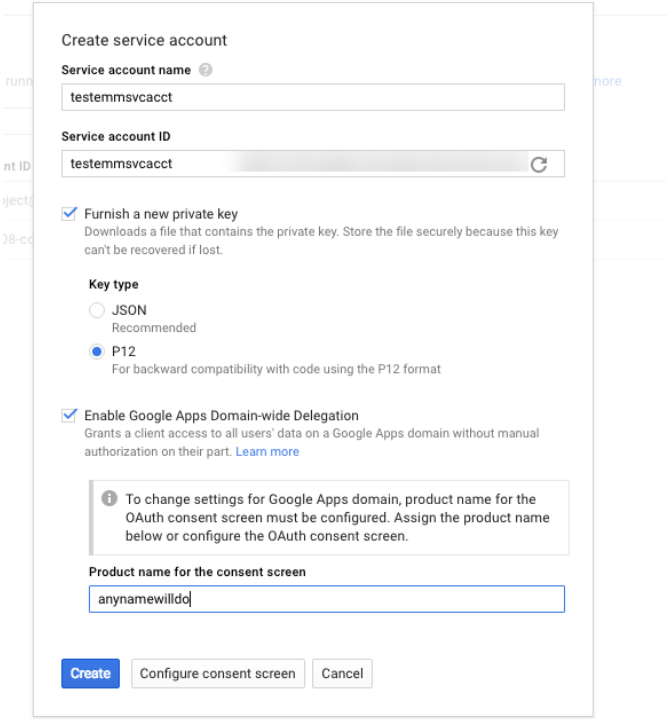


9. Sur la page **Comptes de service**, cliquez sur **Créer un compte de service**.



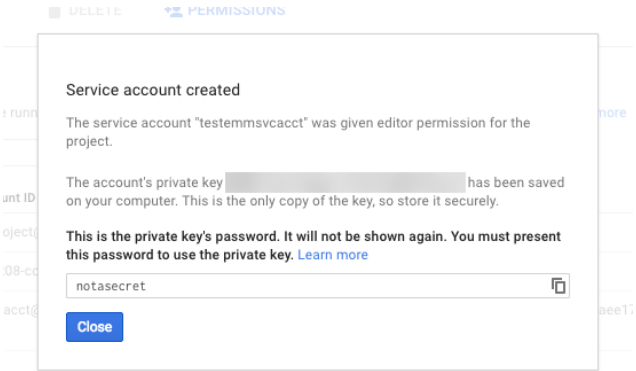
10. Dans **Créer un compte de service**, nommez le compte et sélectionnez la case **Indiquer une nouvelle clé privée**. Cliquez sur **P12**, sélectionnez la case à cocher **Activer la délégation Google Apps au niveau du domaine**, puis cliquez sur **Créer**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



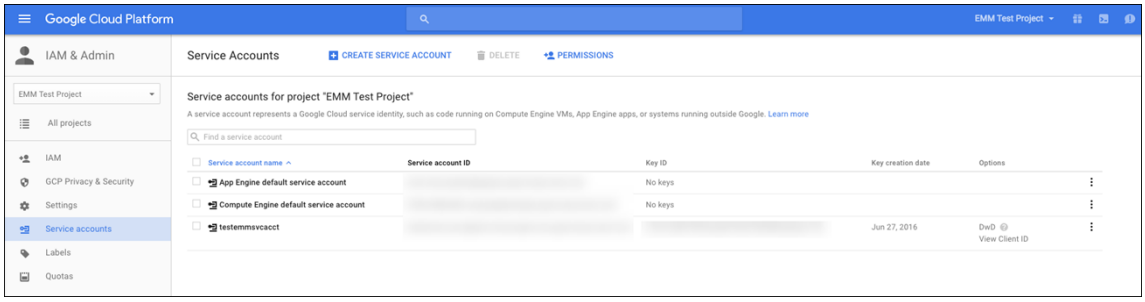
Le certificat (fichier P12) est téléchargé sur votre ordinateur. Veillez à enregistrer le certificat dans un emplacement sécurisé.

11. Sur l'écran **Compte de service créé**, cliquez sur **Fermer**.

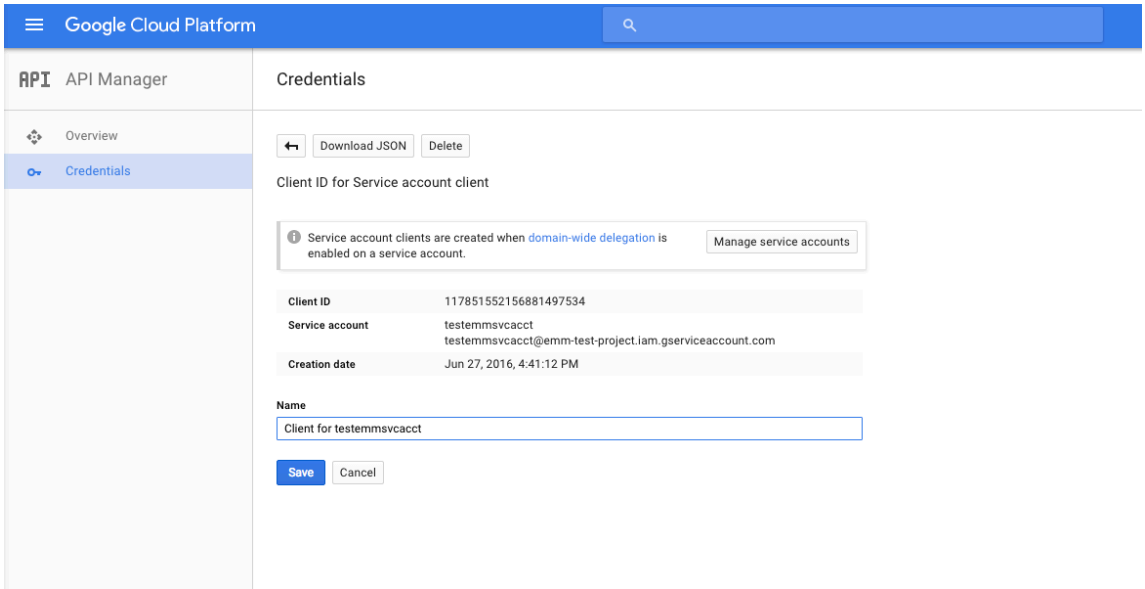


12. Dans **Autorisations**, cliquez sur **Comptes de service**, puis sous **Options** pour votre compte de service, cliquez sur **Afficher l'ID client**.

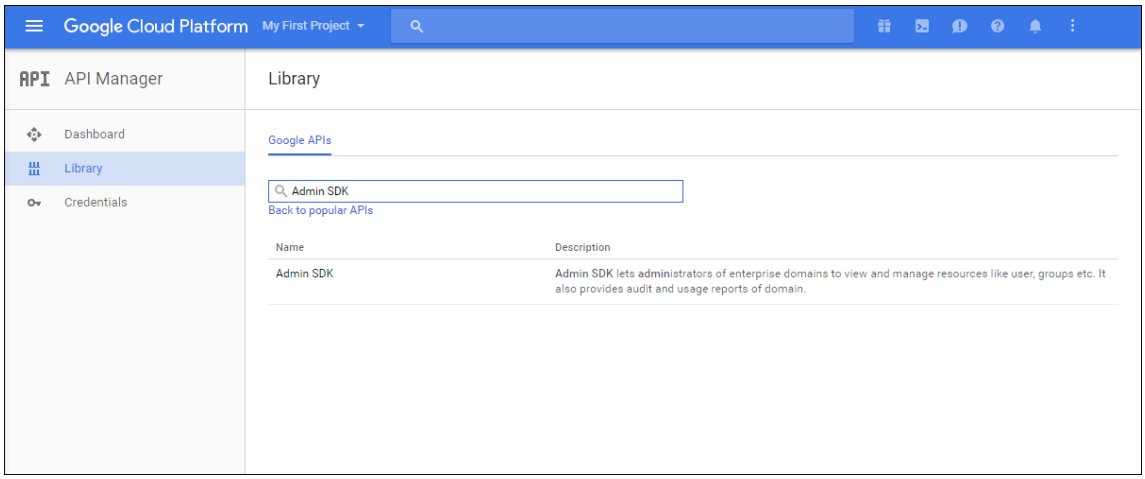
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



13. Les détails requis pour l'autorisation du compte sur la console d'administration Google s'affichent. Copiez les valeurs des champs **Client ID** et **Service account ID** sur un emplacement où vous pourrez récupérer les informations ultérieurement. Vous avez besoin de ces informations, ainsi que du nom de domaine à envoyer à l'assistance Citrix pour les ajouter à une liste d'autorisation.

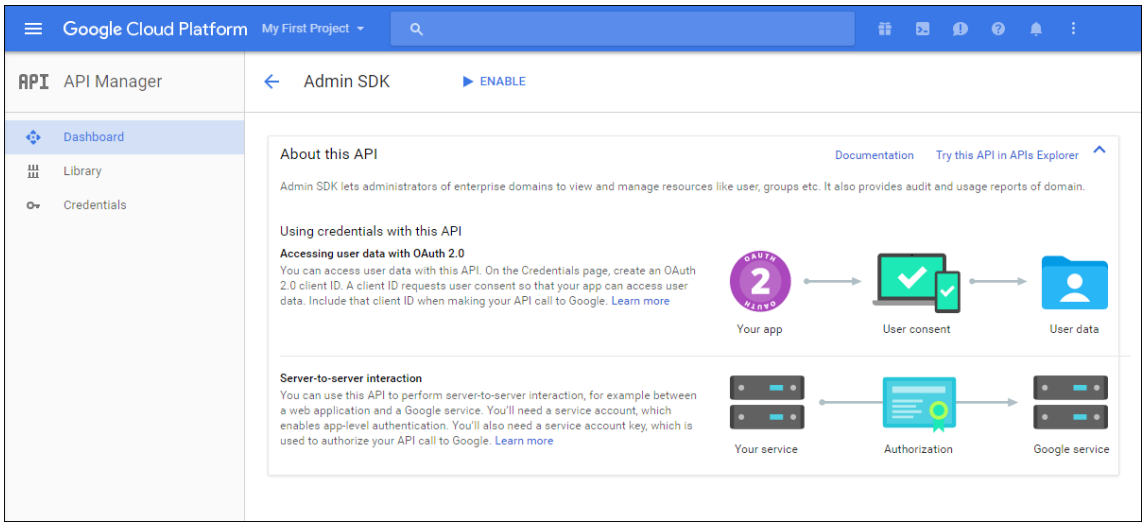


14. Sur la page **Bibliothèque**, recherchez **Admin SDK** et cliquez sur le résultat de la recherche.

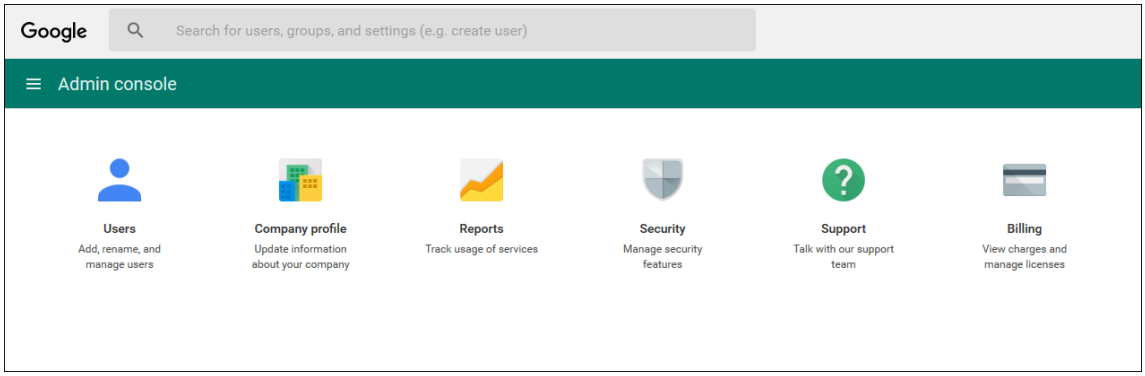


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

15. Sur la page de **présentation**, cliquez sur **Activer**.

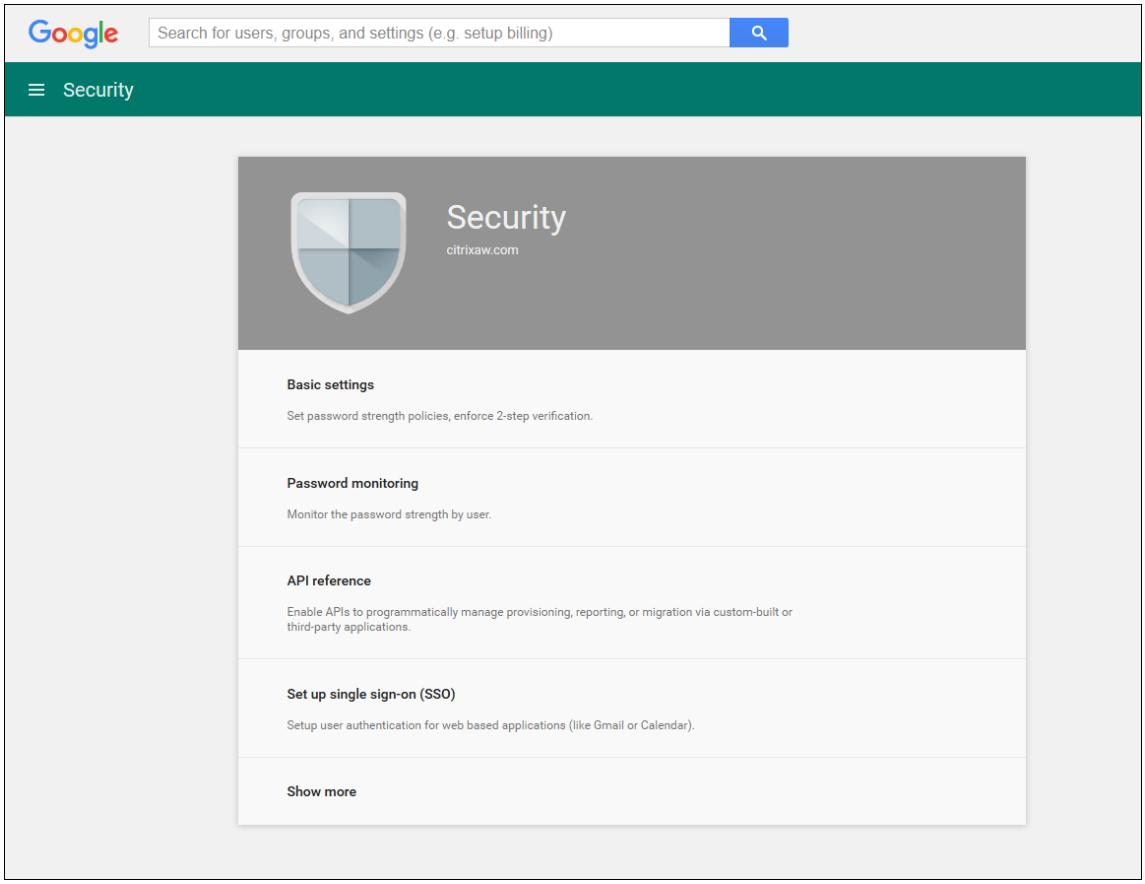


16. Ouvrez la console d'administration Google pour votre domaine et cliquez sur **Sécurité**.

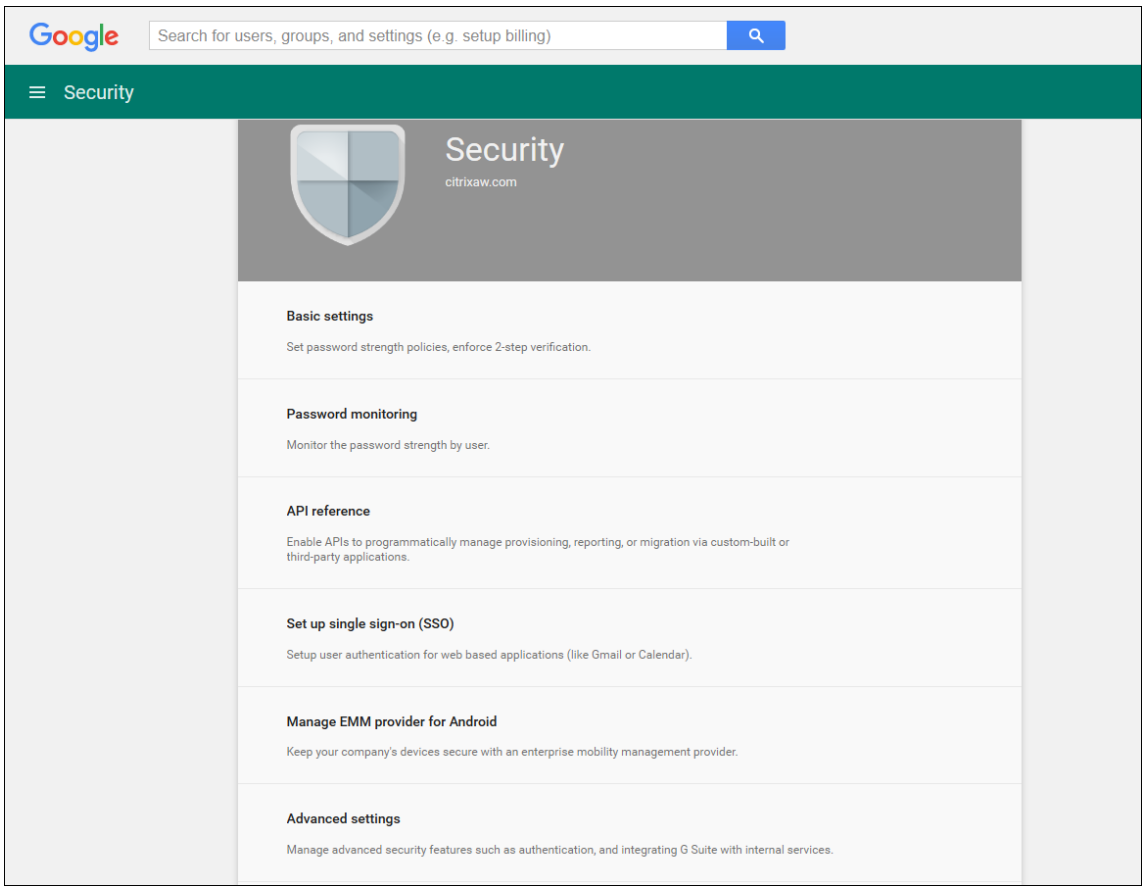


17. Sur la page **Paramètres**, cliquez sur **Afficher plus**, puis cliquez sur **Paramètres avancés**.

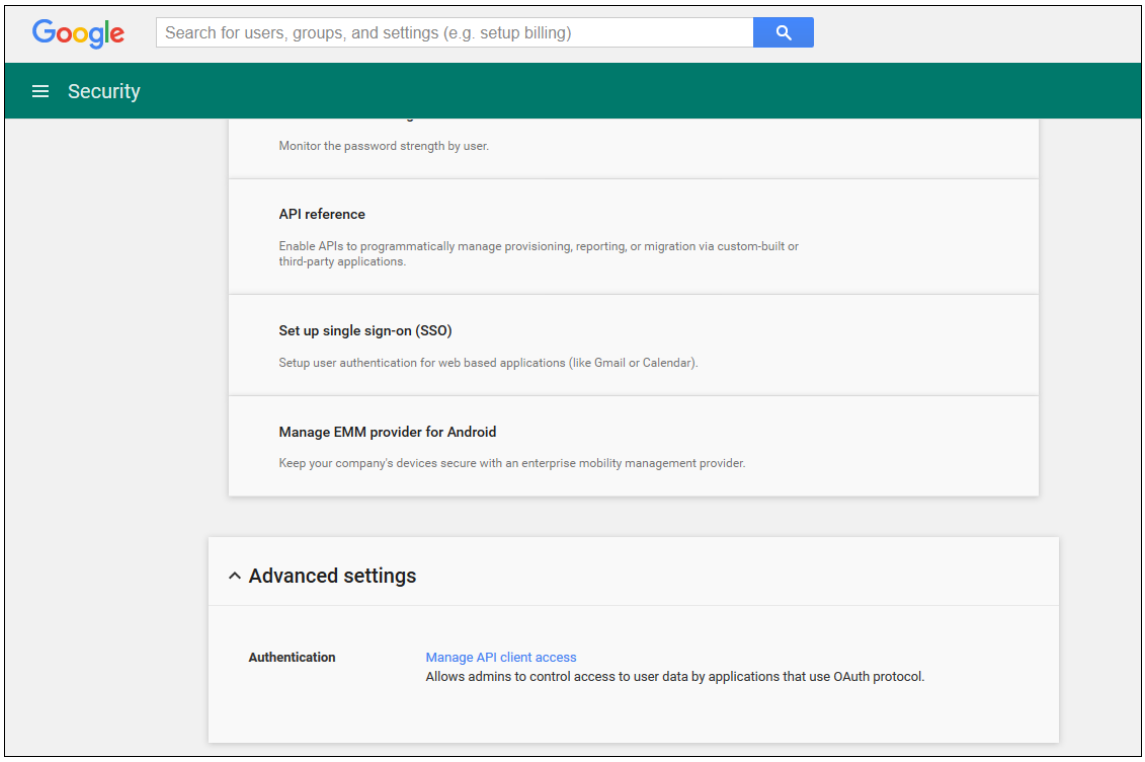
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

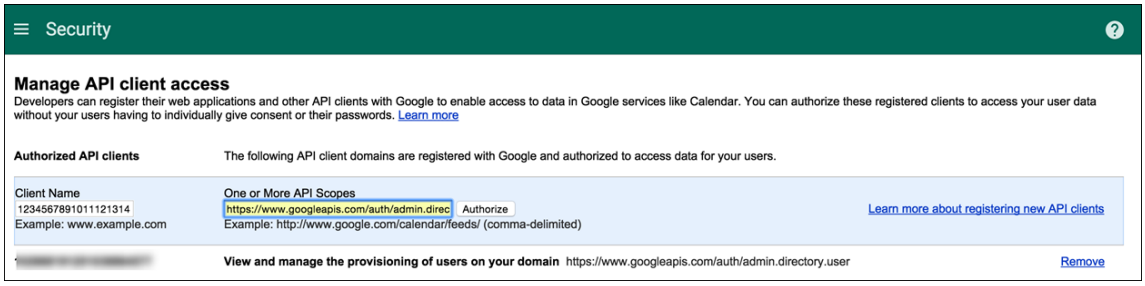


18. Cliquez sur **Gérer l'accès au client d'API**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

19. Dans **Nom du client**, entrez l'ID de client que vous avez enregistré précédemment, dans **Une ou plusieurs étendues d'API**, entrez `https://www.googleapis.com/auth/admin.directory.user` puis cliquez sur **Autoriser**.



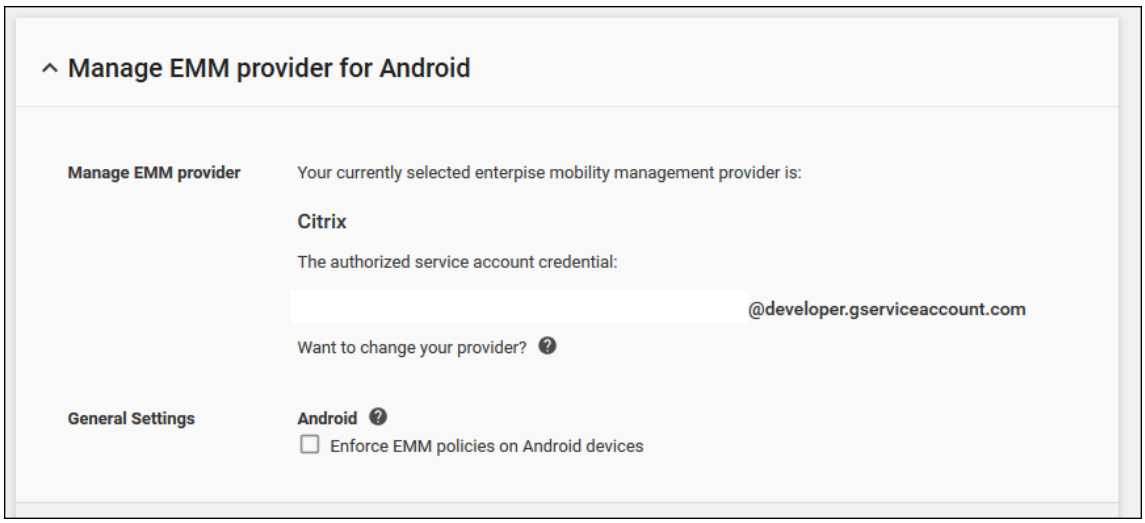
Liaison à EMM

Pour pouvoir utiliser Citrix Endpoint Management pour gérer vos appareils Android, vous devez contacter l'assistance technique de Citrix et fournir vos nom de domaine, compte de service et jeton de liaison. Citrix lie le jeton à Citrix Endpoint Management en tant que fournisseur de gestion de la mobilité d'entreprise (EMM). Pour accéder aux coordonnées du support technique Citrix, consultez la section Support technique Citrix.

1. Pour confirmer la liaison, ouvrez une session sur le portail de la console d'administration Google et cliquez sur **Sécurité**.
2. Cliquez sur **Gérer le fournisseur EMM pour Android**.

   Votre compte Google Android Entreprise est maintenant lié à Citrix en tant que fournisseur EMM.

   Après avoir confirmé la liaison du jeton, vous pouvez commencer à utiliser la console Citrix Endpoint Management pour gérer vos appareils Android. Importez le certificat P12 que vous avez généré à l'étape 14. Configurez les paramètres du serveur Android Entreprise, activez l'authentification unique SAML et définissez au moins une stratégie d'appareil Android Entreprise.

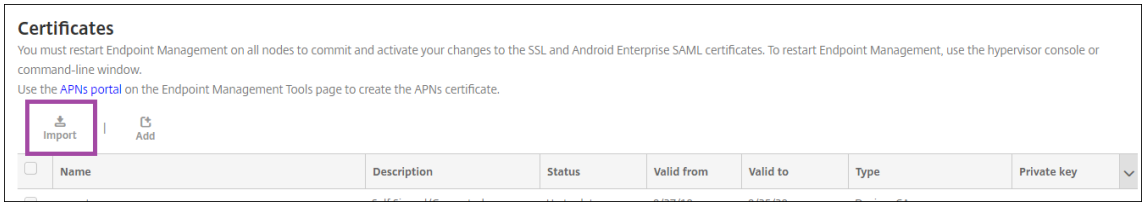


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

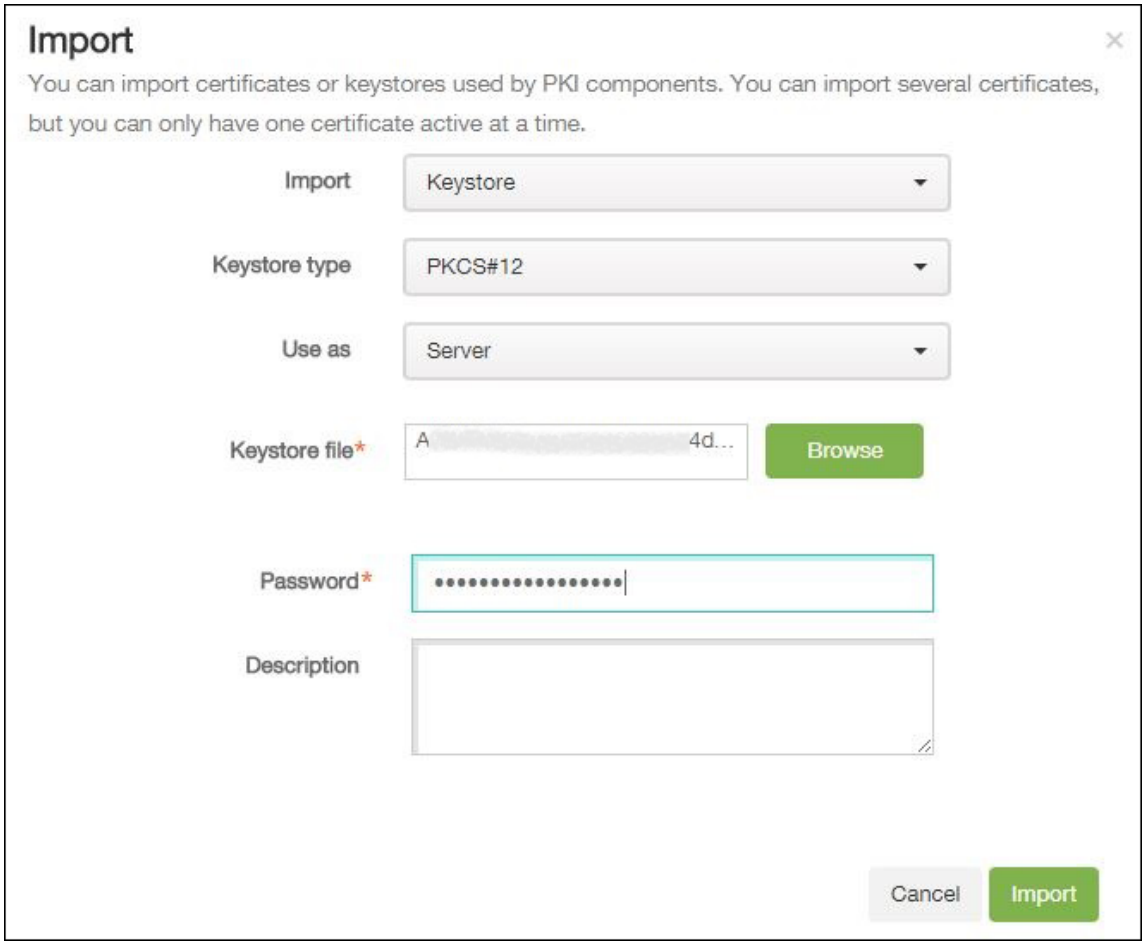
Importer le certificat P12

Suivez ces étapes pour importer votre certificat P12 Android Entreprise :

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console pour ouvrir la page **Paramètres**, puis cliquez sur **Certificats**. La page **Certificats** s'affiche.



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



Configurez les paramètres suivants :

- **Importer :** dans la liste, cliquez sur **Keystore**.
- **Type de keystore :** dans la liste, cliquez sur **PKCS#12**.
- **Utiliser en tant que :** dans la liste, cliquez sur **Serveur**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Fichier de keystore :** cliquez sur **Parcourir** et accédez au certificat P12.
- **Mot de passe :** entrez le mot de passe du certificat. Il s'agit du mot de passe de clé privée que vous avez créé lors de la configuration de votre compte Android Enterprise.
- **Description :** entrez une description pour le certificat.

3. Cliquez sur **Importer**.

Configurer les paramètres du serveur Android Entreprise

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Plates-formes**, cliquez sur **Android Entreprise**. La page **Android Entreprise** s'affiche.

Configurez ces paramètres, puis cliquez sur **Enregistrer**.

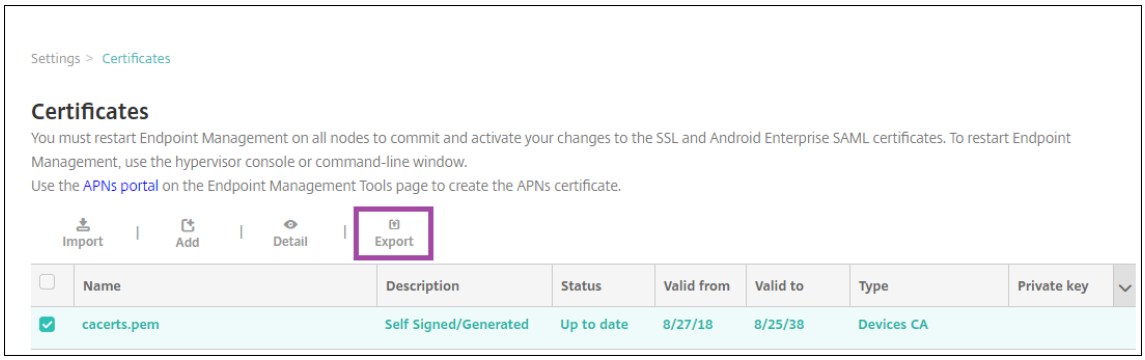
- **Nom de domaine :** entrez votre nom de domaine Android Entreprise ; par exemple, domaine.com.
- **Compte d'administrateur de domaine :** entrez le nom d'utilisateur de l'administrateur de domaine ; par exemple, le compte de messagerie utilisé pour le portail Google Developer.
- **ID du compte de service :** entrez votre ID de compte de service, par exemple, l'adresse e-mail associée au compte de service Google (`serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com`).
- **ID client :** entrez l'ID client numérique de votre compte de service Google.
- **Activer Android Entreprise :** activez ou désactivez Android Entreprise.

Activer l'authentification unique SAML

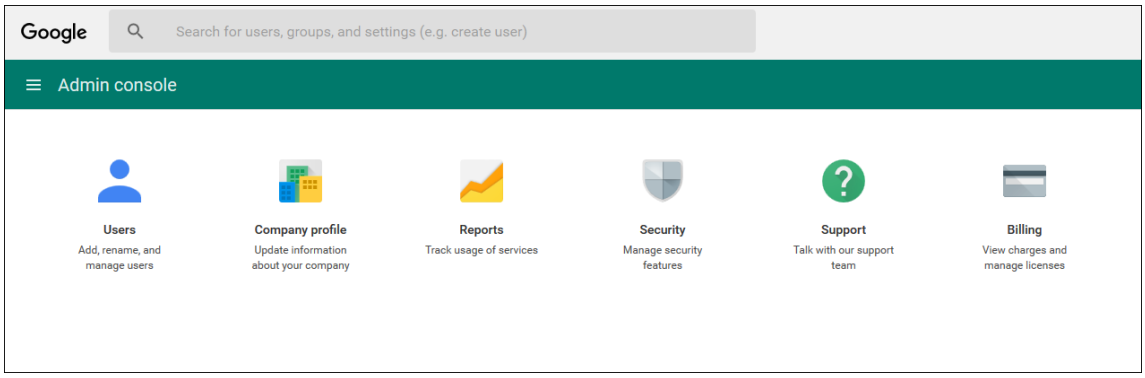
1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

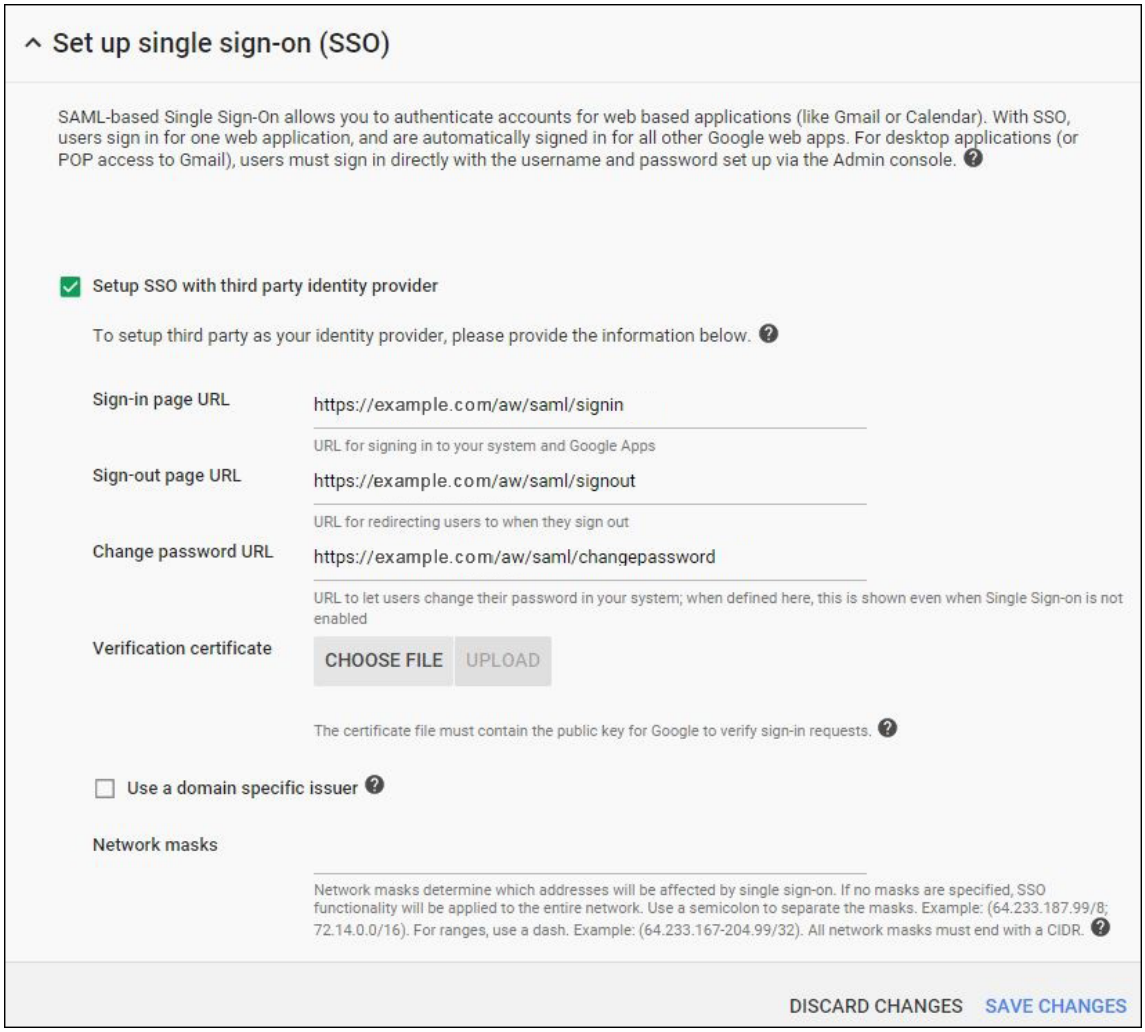


3. Dans la liste des certificats, cliquez sur le certificat SAML.
4. Cliquez sur **Exporter** et enregistrez le certificat sur votre ordinateur.
5. Connectez-vous au portail de la console d'administration Google à l'aide de vos informations d'identification d'administrateur Android Entreprise. Pour accéder au portail, veuillez consulter la section Console d'administration Google.
6. Cliquez sur **Sécurité**.



7. Dans **Sécurité**, cliquez sur **Configurer l'authentification unique (SSO)** et configurez les paramètres suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



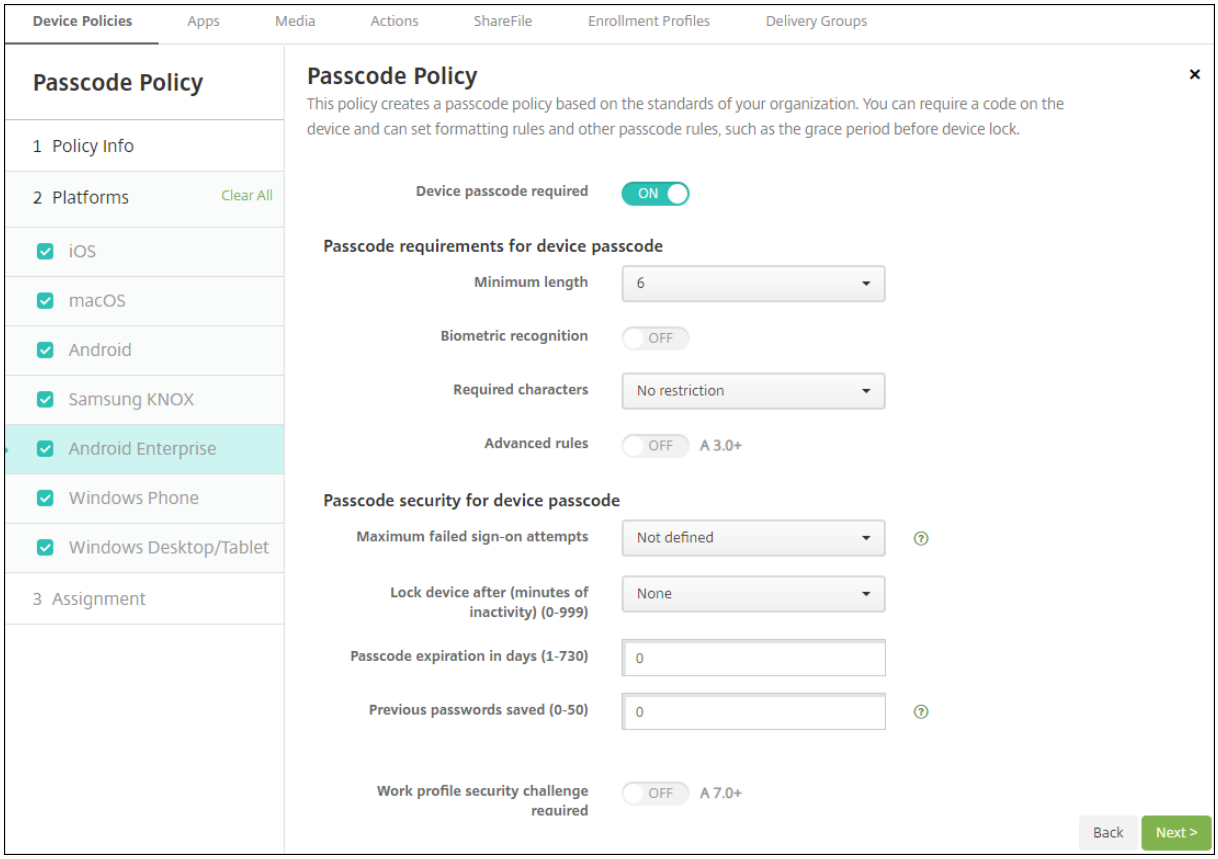
- **URL de la page de connexion :** entrez l'adresse URL pour les utilisateurs qui se connectent à votre système et Google Apps. Par exemple : `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **URL de la page de déconnexion :** entrez l'adresse URL vers laquelle les utilisateurs sont redirigés lorsqu'ils se déconnectent. Par exemple : `https://<Xenmobile-FQDN>/aw/saml/signout`.
- **URL de la page de modification du mot de passe :** entrez l'adresse URL pour permettre aux utilisateurs de modifier leur mot de passe dans votre système. Par exemple : `https://<Xenmobile-FQDN>/aw/saml/changepassword`. Si ce champ est défini, cette invite s'affiche même lorsque l'authentification unique (SSO) n'est pas disponible.
- **Certificat de vérification :** cliquez sur **CHOISIR FICHIER** et accédez à l'emplacement du certificat SAML exporté depuis Citrix Endpoint Management.

8. Cliquez sur **ENREGISTRER LES MODIFICATIONS**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer une stratégie d'appareil Android Entreprise

Configurez une stratégie de code secret afin d'obliger les utilisateurs à créer un code secret sur leurs appareils la première fois qu'ils s'inscrivent.



Les étapes de base pour configurer une stratégie sont les suivantes.

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer**, puis sur **Stratégies d'appareil**.
2. Cliquez sur **Ajouter**, puis sélectionnez la stratégie que vous souhaitez ajouter à partir de la boîte de dialogue **Ajouter une nouvelle stratégie**. Dans cet exemple, vous cliquez sur **Code secret**.
3. Remplissez la page **Informations sur la stratégie**.
4. Cliquez sur **Android Entreprise** et configurez les paramètres pour la stratégie.
5. Attribuez la stratégie à un groupe de mise à disposition.

Configurer les paramètres de compte Android Entreprise

Avant de démarrer la gestion des applications et des stratégies Android sur les appareils, vous devez définir les informations de domaine et de compte Android Entreprise dans Citrix Endpoint Manage-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ment. Commencez par effectuer les tâches de configuration Android Entreprise sur Google pour configurer un administrateur de domaine et obtenir un ID de compte de service et un jeton de liaison.

1. Dans la console web Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'ouvre.
2. Sous **Plates-formes**, cliquez sur **Android Entreprise**. La page de configuration **Android Entreprise** s'affiche.

1. Sur la page **Android Entreprise**, configurez les paramètres suivants :
   - **Nom de domaine :** entrez le nom du domaine.
   - **Compte d'administrateur de domaine :** entrez le nom d'utilisateur de l'administrateur de domaine.
   - **ID du compte de service :** entrez votre ID du compte de service Google.
   - **ID client :** entrez l'ID client de votre compte de service Google.
   - **Activer Android Entreprise :** activez ou désactivez Android Entreprise.
2. Cliquez sur **Save**.

Configurer l'accès partenaire Google Workspace pour Citrix Endpoint Management

Certaines fonctionnalités de Citrix Endpoint Management pour Chrome utilisent des API partenaires de Google pour la communication entre Citrix Endpoint Management et votre domaine Google Workspace. Par exemple, Citrix Endpoint Management requiert les API pour les stratégies qui gèrent les fonctionnalités de Chrome, telles que le mode de navigation privée et le mode Invité.

Pour activer les API partenaires, vous devez configurer votre domaine Google Workspace dans la console Citrix Endpoint Management, puis configurer votre compte Google Workspace.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

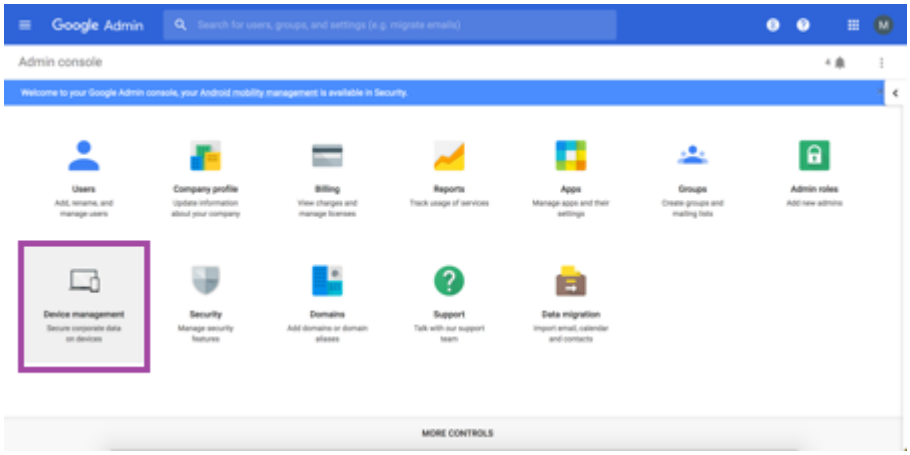
Configurer votre domaine Google Workspace dans Citrix Endpoint Management

Pour permettre à Citrix Endpoint Management de communiquer avec les API de votre domaine Google Workspace, accédez à **Paramètres > Configuration de Google Chrome** et configurez les paramètres.

- **Domaine Google Workspace :** domaine Google Workspace hébergeant les API requises par Citrix Endpoint Management.
- **Compte d'administrateur Google Workspace :** compte administrateur de votre domaine Google Workspace.
- **ID client Google Workspace :** identifiant client pour Citrix. Utilisez cette valeur pour configurer l'accès partenaire pour le domaine Google Workspace.
- **Identifiant d'entreprise Google Workspace :** identifiant d'entreprise de votre compte, renseigné à partir de votre compte d'entreprise Google.

Activer l'accès partenaire pour les appareils et les utilisateurs de votre domaine Google Workspace

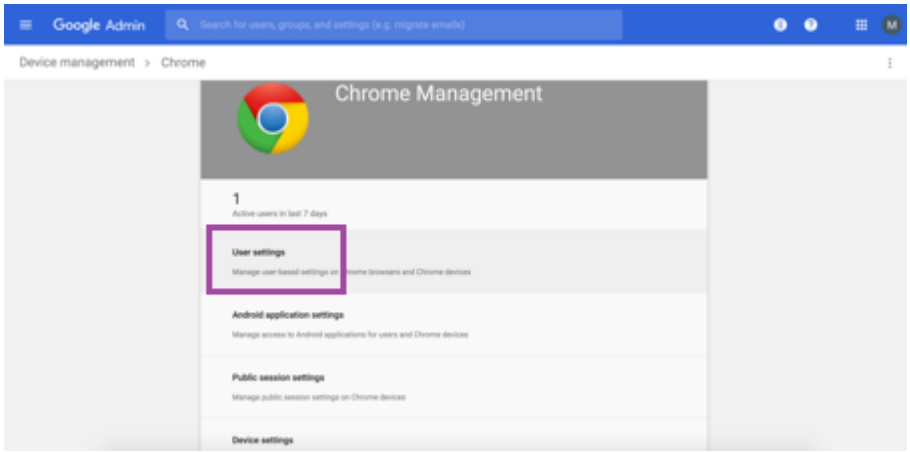
1. Connectez-vous à la console d'administration Google https://admin.google.com.
2. Cliquez sur **Gestion des appareils**.



3. Cliquez sur **Gestion de Chrome**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Cliquez sur **Paramètres utilisateur**.



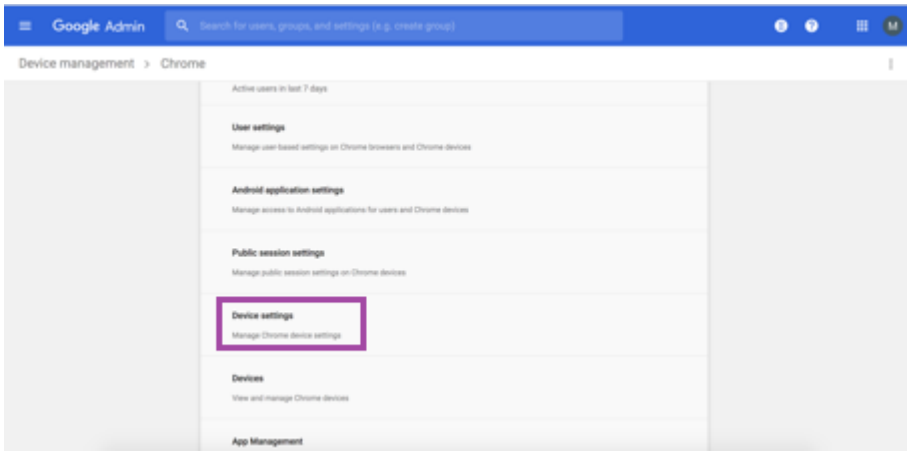
5. Recherchez **Gestion de Chrome - Accès Partenaire**.

6. Activez la case à cocher **Activer la gestion de Chrome - Accès Partenaire**.
7. Confirmez que vous comprenez et que vous souhaitez activer l'accès partenaire. Cliquez sur

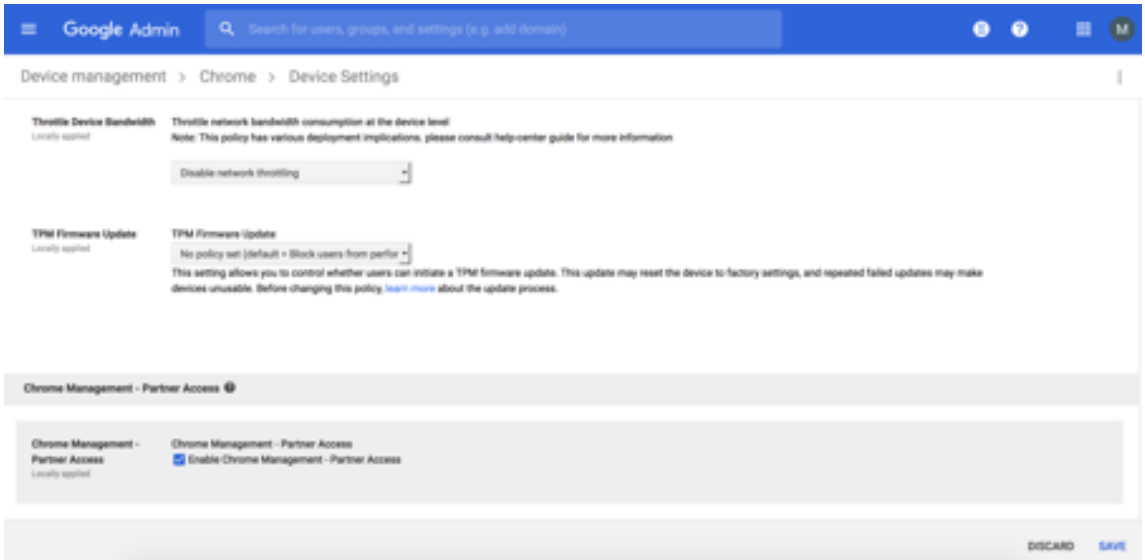
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Save.

8. Sur la page Gestion de Chrome, cliquez sur **Paramètres utilisateur**.

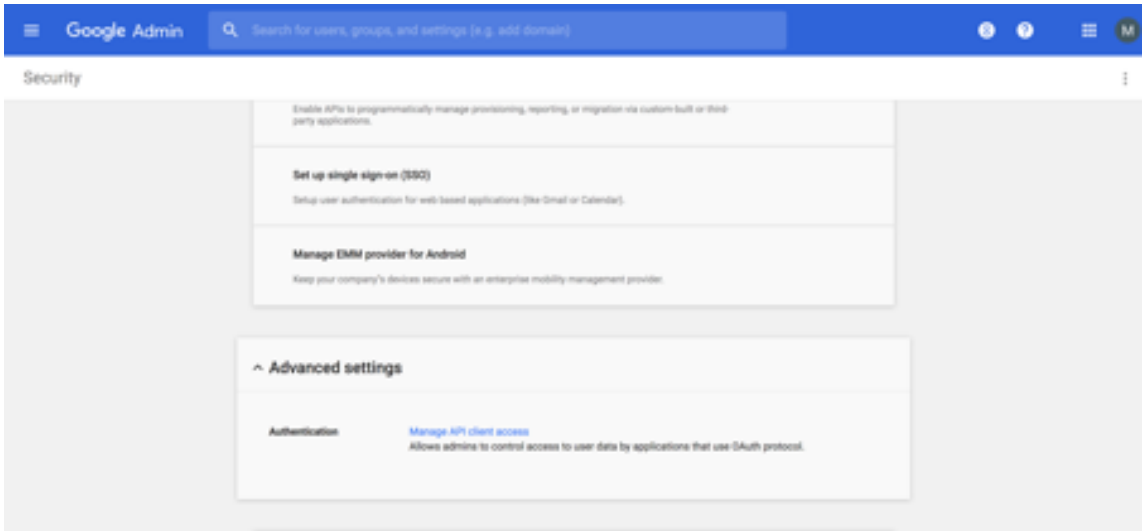


9. Recherchez **Gestion de Chrome - Accès Partenaire**.

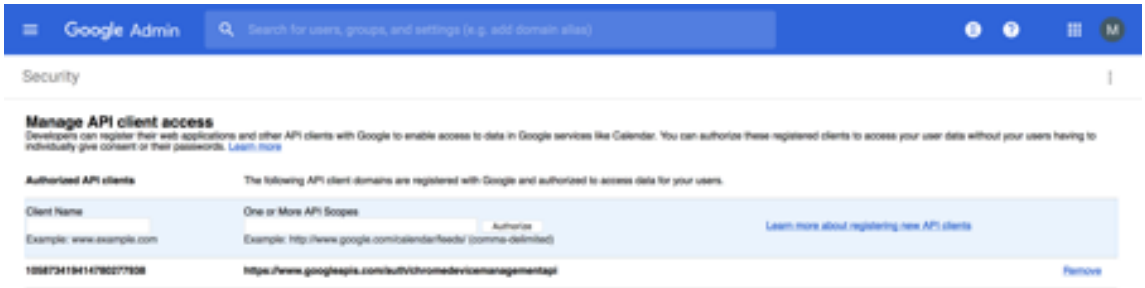


10. Activez la case à cocher **Activer la gestion de Chrome - Accès Partenaire**.
11. Confirmez que vous comprenez et que vous souhaitez activer l'accès partenaire. Cliquez sur **Save**.
12. Accédez à la page **Sécurité**, puis cliquez sur **Paramètres avancés**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



13. Cliquez sur **Gérer l'accès au client d'API**.
14. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Configuration de Google Chrome** et copiez la valeur de l'ID client G Suite. Retournez ensuite à la page **Gérer l'accès au client d'API** et collez la valeur copiée dans le champ **Nom du client**.
15. Dans **Un ou plusieurs champs d'application d'API**, ajoutez l'URL : `https://www.googleapis.com/auth/chromedevicemanagementapi`



16. Cliquez sur **Autoriser**.

    Le message « Vos paramètres ont été sauvegardés » apparaît.

Inscription d'appareils Android Entreprise

Si le processus d'inscription de votre appareil nécessite que les utilisateurs saisissent un nom d'utilisateur ou un ID utilisateur, le format accepté dépend de la configuration du serveur Citrix Endpoint Management pour la recherche des utilisateurs par nom principal d'utilisateur (UPN) ou nom de compte SAM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si le serveur Citrix Endpoint Management est configuré pour la recherche des utilisateurs par UPN, les utilisateurs doivent entrer un nom UPN au format :

- *nom d'utilisateur@domaine*

Si le serveur Citrix Endpoint Management est configuré pour la recherche des utilisateurs par SAM, les utilisateurs doivent entrer un nom SAM dans l'un des formats suivants :

- *nom d'utilisateur@domaine*
- *domaine\nom d'utilisateur*

Pour déterminer le type de nom d'utilisateur pour lequel votre serveur Citrix Endpoint Management est configuré :

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **LDAP** pour afficher la configuration de la connexion LDAP.
3. Dans la partie inférieure de la page, affichez le champ **Recherche utilisateur par** :
   - Si l'option est définie sur **userPrincipalName**, le serveur Citrix Endpoint Management est défini pour UPN.
   - Si l'option est définie sur **sAMAccountName**, le serveur Citrix Endpoint Management est défini pour SAM.

Désinscription d'une entreprise Android Enterprise

Vous pouvez désinscrire une entreprise Android Enterprise à l'aide de la console du serveur Citrix Endpoint Management et des outils Citrix Endpoint Management Tools.

Lorsque vous effectuez cette tâche, le serveur Citrix Endpoint Management ouvre une fenêtre contextuelle Citrix Endpoint Management Tools. Avant de commencer, assurez-vous que le serveur Citrix Endpoint Management est autorisé à ouvrir des fenêtres contextuelles dans le navigateur que vous utilisez. Certains navigateurs, tels que Google Chrome, vous obligent à désactiver le blocage des fenêtres contextuelles et à ajouter l'adresse du site Citrix Endpoint Management à la liste d'autorisation des fenêtres contextuelles.

> **Avertissement :**
>
> une fois l'entreprise désinscrite, l'état par défaut des applications Android Entreprise sur les appareils déjà inscrits est rétabli. Les appareils ne sont plus gérés par Google. Leur réinscription dans une entreprise Android Entreprise peut nécessiter une configuration supplémentaire pour restaurer les fonctionnalités précédentes.

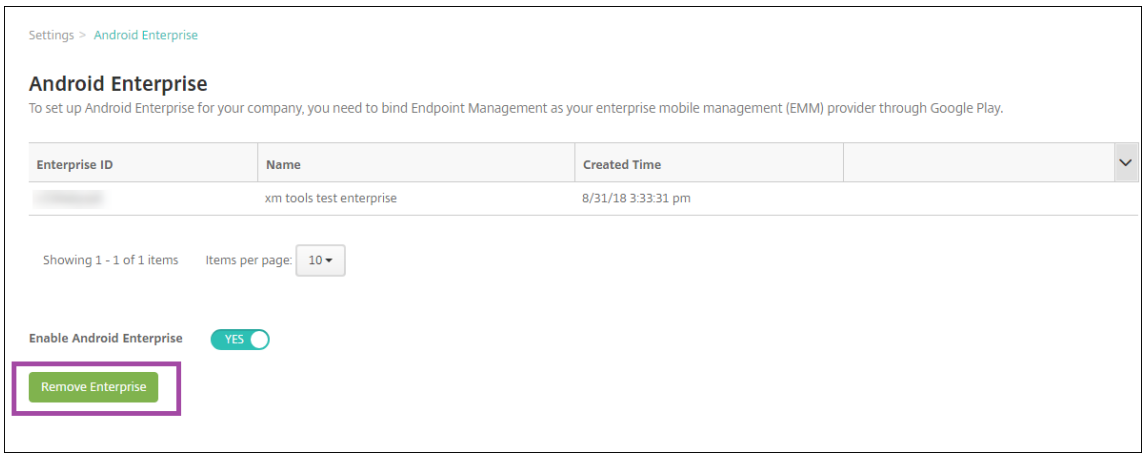
Une fois l'entreprise Android Enterprise désinscrite :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Les applications Android Enterprise des appareils et des utilisateurs inscrits dans l'entreprise sont réinitialisées à leur état par défaut. Les stratégies Autorisations de l'application et Configurations gérées appliquées précédemment n'ont plus d'effet.
- Les appareils inscrits via l'entreprise sont gérés par Citrix Endpoint Management mais ne sont pas gérés du point de vue de Google. Aucune nouvelle application Android Entreprise ne peut être ajoutée. Vous ne pouvez pas appliquer les stratégies Autorisations de l'application ou Configurations gérées. D'autres stratégies, telles que Planification, Mot de passe et Restrictions, peuvent encore être appliquées à ces appareils.
- Si vous tentez d'inscrire des appareils dans Android Enterprise, ils sont inscrits comme appareils Android et non comme appareils Android Enterprise.

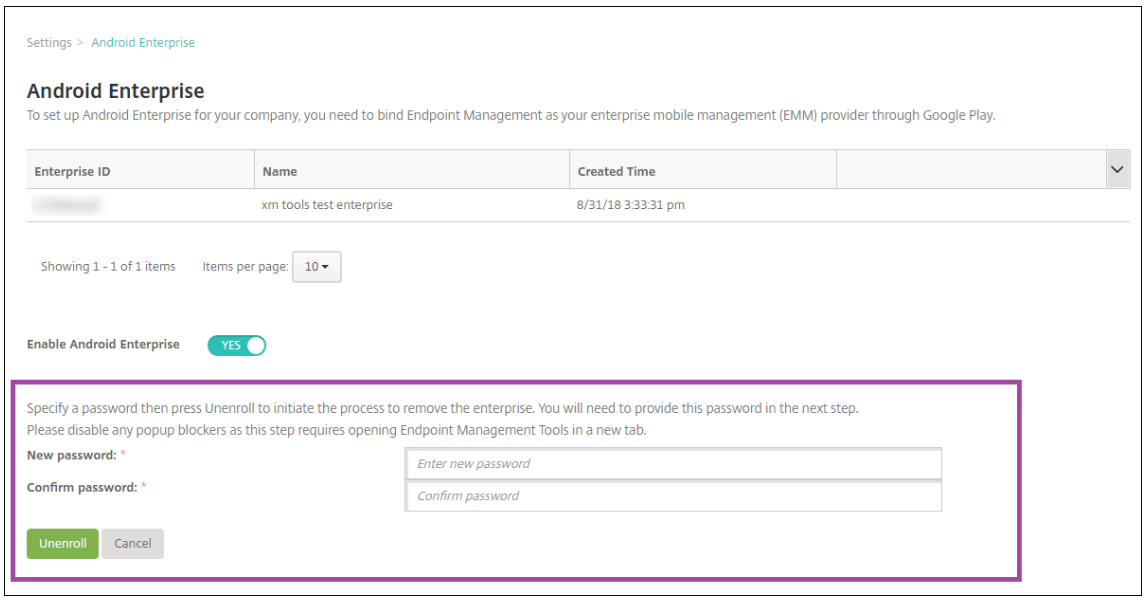
Désinscription d'une entreprise Android Enterprise :

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page Paramètres s'affiche.
2. Sur la page Paramètres, cliquez sur **Android Enterprise**.
3. Cliquez sur **Supprimer l'entreprise**.

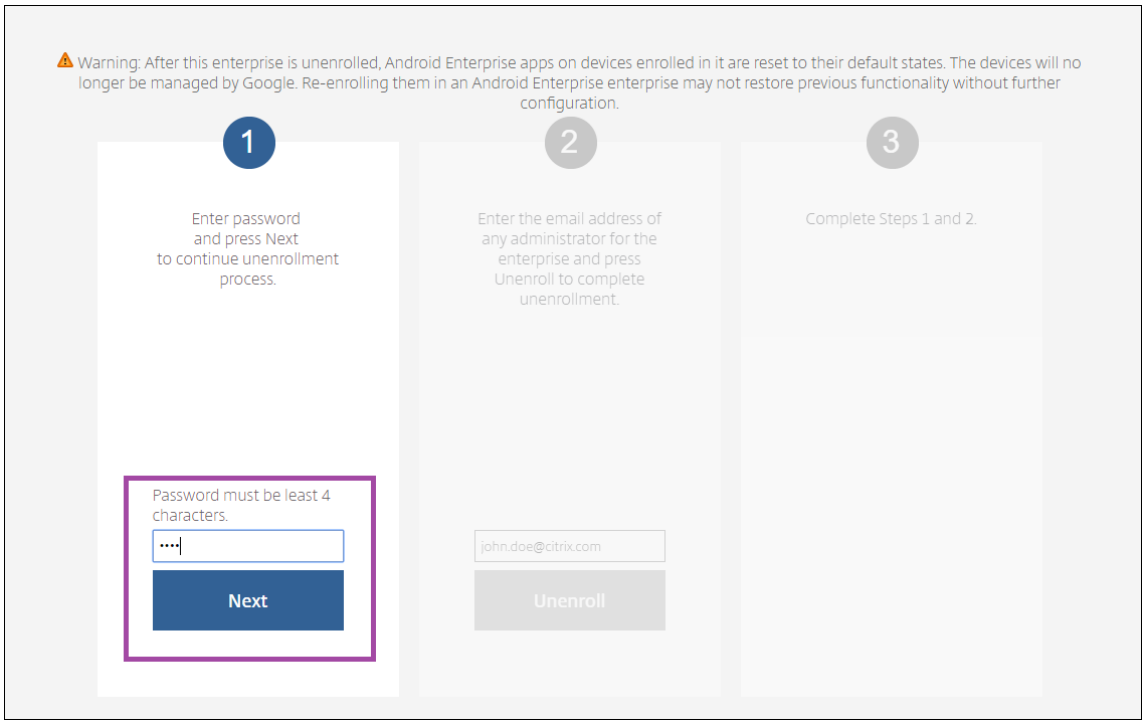


4. Spécifiez un mot de passe. Vous en aurez besoin à l'étape suivante pour terminer la désinscription. Cliquez ensuite sur **Désinscrire**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

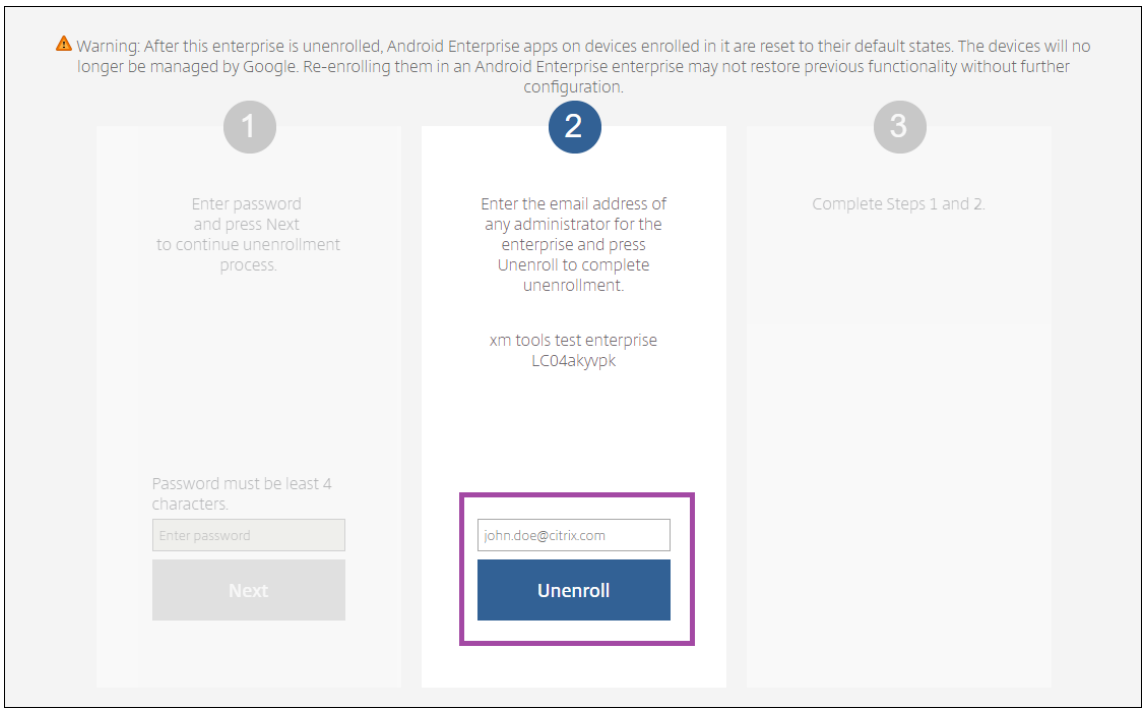


5. Lorsque la page Citrix Endpoint Management Tools s'ouvre, entrez le mot de passe que vous avez créé à l'étape précédente.



6. Cliquez sur **Désinscrire**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Provisionnement d'appareils entièrement gérés dans Android Enterprise

Seuls les appareils appartenant à l'entreprise peuvent être des appareils entièrement gérés dans Android Enterprise. Sur les appareils entièrement gérés, l'ensemble de l'appareil, et pas seulement le profil de travail, est contrôlé par l'entreprise ou l'organisation. Les appareils entièrement gérés sont également appelés appareils gérés de travail.

Citrix Endpoint Management prend en charge ces méthodes d'inscription pour les appareils entièrement gérés :

- **afw#xenmobile :** avec cette méthode d'inscription, l'utilisateur entre les caractères `afw#xenmobile` lors de la configuration de l'appareil. Ce jeton identifie l'appareil comme étant géré par Citrix Endpoint Management et télécharge Citrix Secure Hub.
- **Code QR :** le provisioning de code QR est un moyen simple de configurer une flotte distribuée d'appareils qui ne prennent pas en charge la technologie NFC, tels que les tablettes. La méthode d'inscription avec le code QR peut être utilisée sur des appareils de la flotte qui ont été réinitialisés à leurs paramètres d'usine. La méthode d'inscription avec le code QR permet de configurer les appareils entièrement gérés en scannant un code QR depuis l'assistant d'installation.
- **Partage de données à l'aide de NFC :** la méthode d'inscription avec le partage NFC peut être utilisée sur des appareils de la flotte qui ont été réinitialisés à leurs paramètres d'usine. Un partage NFC permet de transférer des données entre deux appareils en utilisant une communication en champ proche. Bluetooth, Wi-Fi et les autres modes de communication sont désactivés sur un appareil dont les paramètres d'usine ont été réinitialisés. NFC est le seul protocole

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de communication que l'appareil peut utiliser dans cet état.

`afw#xenmobile`

La méthode d'inscription est utilisée après la mise sous tension d'un nouvel appareil ou d'un appareil réinitialisé à ses paramètres d'usine lors de la configuration initiale. Les utilisateurs entrent `afw#xenmobile` lorsqu'ils sont invités à entrer un compte Google. Cette action télécharge et installe Citrix Secure Hub. Les utilisateurs suivent les invites de configuration de Citrix Secure Hub pour terminer l'inscription.

Cette méthode d'inscription est recommandée pour la plupart des clients car la dernière version de Citrix Secure Hub est téléchargée à partir de Google Play Store. Contrairement aux autres méthodes d'inscription, vous ne pouvez pas télécharger Citrix Secure Hub depuis le serveur Citrix Endpoint Management.

Prérequis :

- Pris en charge sur tous les appareils Android exécutant Android OS.

Code QR

Pour inscrire un appareil en mode Propriétaire d'appareil à l'aide d'un code QR, générez un code QR en créant un JSON et en convertissant le JSON en un code QR. Le code QR est scanné par l'appareil photo de l'appareil pour inscrire l'appareil.

Prérequis :

- Pris en charge sur tous les appareils Android exécutant Android 7.0 et supérieur.

Créer un code QR à partir d'un JSON Créez un JSON avec les champs suivants.

Ces champs sont obligatoires :

Clé : android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

Valeur : com.zenprise/com.zenprise.configuration.AdminFunction

Clé : android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

Valeur : qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Clé : android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

Valeur : `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

Ces champs sont facultatifs :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **android.app.extra.PROVISIONING_LOCALE :** entrez un code de langue et de pays.

  Les codes de langue sont des codes ISO de deux lettres minuscules (tels que fr) comme défini dans l'ISO 639-1. Les codes de pays sont des codes ISO de deux lettres majuscules (tels que FR) comme défini dans l'ISO 3166-1. À titre d'exemple, entrez fr_FR pour la langue française parlée en France.

- **android.app.extra.PROVISIONING_TIME_ZONE :** fuseau horaire dans lequel l'appareil est exécuté.

  Tapez le nom de la base de données de la région/emplacement. Par exemple, tapez **Europe/-Paris** pour l'heure de l'Europe occidentale. Si vous n'entrez rien, le fuseau horaire est automatiquement renseigné.

- **android.app.extra.PROVISIONING_LOCAL_TIME :** durée en millisecondes depuis l'heure Unix.

  L'heure Unix (également appelée heure POSIX ou Unix timestamp) est le nombre de secondes écoulées depuis le 1er janvier 1970 (minuit UTC/GMT). L'heure n'inclut pas les secondes intercalaires (dans ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION :** définissez cette option sur **true** pour ignorer le cryptage lors de la création du profil. Définissez cette option sur **false** pour forcer le cryptage lors de la création du profil.

Un fichier JSON typique ressemble à ce qui suit :

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "[illegible]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "[illegible]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": [illegible]
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

Validez le fichier JSON créé à l'aide de n'importe quel outil de validation JSON, tel que https://jsonlint.com. Convertissez cette chaîne JSON en un code QR à l'aide de n'importe quel générateur de code QR en ligne.

Ce code QR est scanné par un appareil dont les paramètres d'usine ont été réinitialisés pour inscrire l'appareil en tant qu'appareils entièrement gérés.

Pour inscrire l'appareil

Pour inscrire un appareil en tant qu'appareil entièrement géré, les paramètres d'usine de l'appareil doivent être réinitialisés.

1. Touchez l'écran 6 fois sur l'écran d'accueil pour lancer le flux d'inscription du code QR.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Lorsque vous y êtes invité, connectez-vous au Wi-Fi. L'emplacement de téléchargement de Citrix Secure Hub dans le code QR (codé dans le JSON) est accessible sur ce réseau Wi-Fi.

   Une fois que l'appareil se connecte au Wi-Fi, il télécharge un lecteur de code QR à partir de Google et lance l'appareil photo.

3. Pointez l'appareil photo sur le code QR pour scanner le code.

   Android télécharge Citrix Secure Hub à partir de l'emplacement de téléchargement dans le code QR, valide la signature du certificat de signature, installe Citrix Secure Hub et le définit comme propriétaire de l'appareil.

Pour plus d'informations sur le provisionnement des appareils à l'aide de la méthode de code QR, consultez Google API documentation for Android EMM developers.

Partage de données avec NFC

Pour inscrire un appareil en tant qu'appareil entièrement géré à l'aide du partage NFC, deux appareils sont requis : un dont les paramètres d'usine ont été rétablis et un exécutant l'application Citrix Endpoint Management Provisioning Tool.

Prérequis :

- Appareils Android pris en charge
- Citrix Endpoint Management activé pour Android Entreprise.
- Un nouvel appareil ou un appareil dont les paramètres d'usine ont été rétablis, provisionné pour Android Enterprise en tant qu'appareil entièrement géré. Les étapes à suivre pour satisfaire ces conditions préalables sont disponibles plus loin dans cet article.
- Un autre appareil avec capacité NFC, exécutant l'application Provisioning Tool configurée. Provisioning Tool est disponible dans Citrix Secure Hub ou sur la page des téléchargements de Citrix.

Chaque appareil ne peut disposer que d'un profil Android Enterprise, géré par une application de gestion de la mobilité d'entreprise (EMM). Dans Citrix Endpoint Management, Citrix Secure Hub est l'application EMM. Un seul profil est autorisé sur chaque appareil. Si vous essayez d'ajouter une deuxième application EMM, la première application EMM sera supprimée.

Données transférées via le partage NFC Le provisioning d'un appareil dont les paramètres d'usine ont été rétablis requiert l'envoi des données suivantes via NFC pour initialiser Android Enterprise :

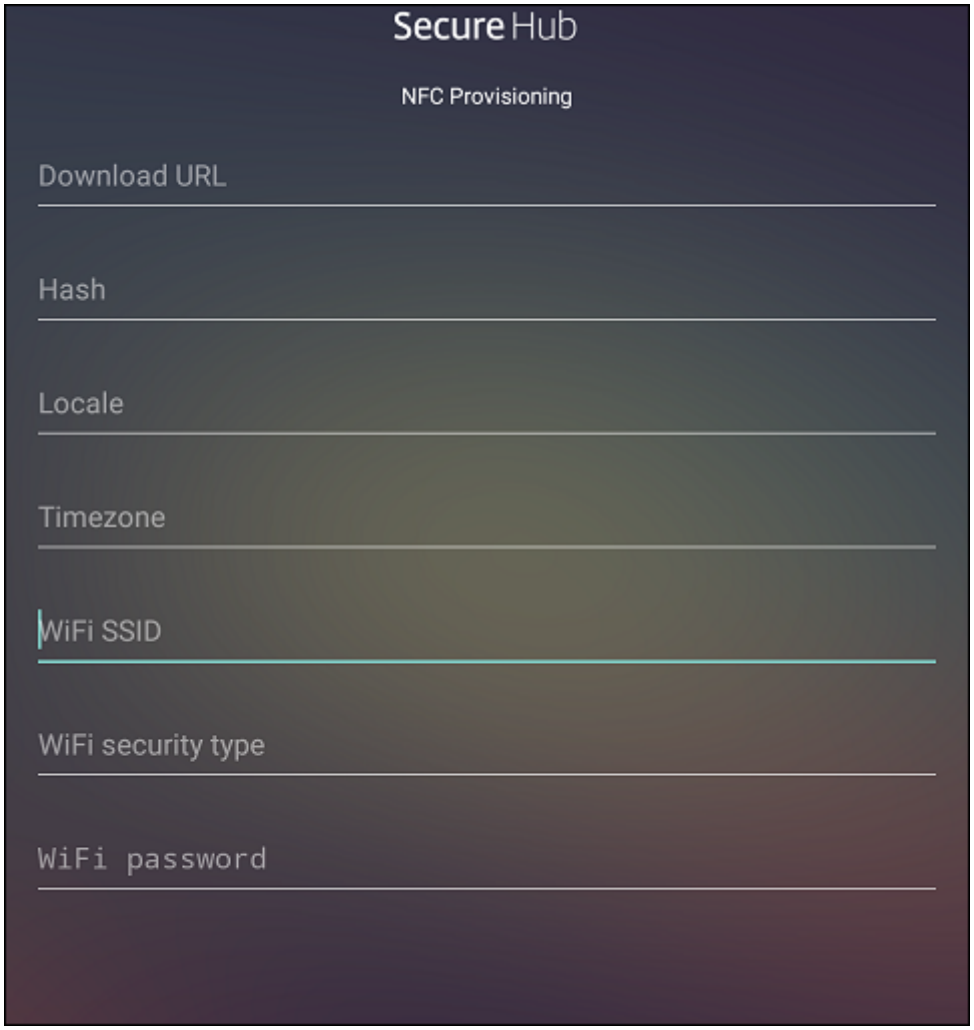
- Nom du package de l'application EMM du fournisseur qui fait office de propriétaire de l'appareil (dans ce cas, Citrix Secure Hub).
- Emplacement intranet/Internet à partir duquel l'appareil peut télécharger l'application EMM du fournisseur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Hachage SHA-256 de l'application EMM du fournisseur pour vérifier que le téléchargement a réussi.
- Détails de la connexion Wi-Fi de façon à ce qu'un appareil dont les paramètres d'usine ont été réinitialisés puisse se connecter et télécharger l'application EMM du fournisseur. Remarque : Android ne prend pas charge 802.1x Wi-Fi pour cette étape.
- Fuseau horaire de l'appareil (facultatif).
- Emplacement géographique de l'appareil (facultatif).

Lorsque les deux appareils sont « cognés », les données de Provisioning Tool sont envoyées à l'appareil dont les paramètres d'usine ont été réinitialisés. Ces données sont ensuite utilisées pour télécharger Citrix Secure Hub avec des paramètres d'administrateur. Si vous ne précisez pas le fuseau horaire ni l'emplacement, Android les configure automatiquement sur le nouvel appareil.

Configuration d'Citrix Endpoint Management Provisioning Tool Avant de partager des données avec NFC, vous devez configurer Provisioning Tool. Cette configuration est ensuite transférée à l'appareil dont les paramètres d'usine ont été réinitialisés durant le partage des données avec NFC.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Vous pouvez entrer des données dans les champs requis ou les renseigner via un fichier texte. Les étapes de la procédure suivante décrivent comment configurer le fichier texte et contiennent des descriptions pour chaque champ. L'application n'enregistre pas les informations après qu'elles soient entrées, il peut donc s'avérer utile de créer un fichier texte afin de conserver les informations pour une utilisation ultérieure.

Pour configurer le Provisioning Tool à l'aide d'un fichier texte Nommez le fichier nfcprovisioning.txt et placez-le dans le dossier **/sdcard/** sur la carte SD de l'appareil. Cela permet à l'application de lire le fichier texte et renseigner les valeurs.

Le fichier texte doit contenir les données suivantes :

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=<download_location>
```

Il s'agit de l'emplacement intranet/Internet de l'application EMM du fournisseur. Après que l'appareil dont les paramètres d'usine ont été réinitialisés se soit connecté au Wi-Fi suite au partage NFC, il doit avoir accès à cet emplacement pour le téléchargement. L'adresse URL est une adresse URL standard qui ne requiert aucun formatage spécial.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256
 hash>
```

Il s'agit de la somme de contrôle de l'application EMM du fournisseur. Elle est utilisée pour vérifier que le téléchargement a réussi. Les étapes à suivre pour obtenir la somme de contrôle sont abordées plus loin dans cet article.

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

Cette ligne est le SSID Wi-Fi connecté de l'appareil sur lequel Provisioning Tool est exécuté.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type
>
```

Les valeurs prises en charge sont WEP et WPA2. Si le Wi-Fi n'est pas protégé, ce champ doit être vide.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

Si le Wi-Fi n'est pas protégé, ce champ doit être vide.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

Entrez un code de langue et de pays. Les codes de langue sont des codes ISO de deux lettres minuscules (tels que fr) comme défini dans l'ISO 639-1. Les codes de pays sont des codes ISO de deux lettres majuscules (tels que FR) comme défini dans l'ISO 3166-1. À titre d'exemple, entrez fr_FR pour la langue française parlée en France. Si vous n'entrez aucun code, la langue et le pays sont automatiquement renseignés.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

Fuseau horaire dans lequel l'appareil est exécuté. Tapez le nom de la base de données de la région/emplacement. Par exemple, tapez **Europe/Paris** pour l'heure de l'Europe occidentale. Si vous n'entrez rien, le fuseau horaire est automatiquement renseigné.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

Ces données ne pas requises car la valeur est codée en dur dans l'application Citrix Secure Hub. Il n'est mentionné ici que par souci de complétude.

Si un accès protégé Wi-Fi WPA2 est utilisé, un fichier nfcprovisioning.txt peut ressembler à ce qui suit :

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Si un accès non protégé Wi-Fi est utilisé, un fichier nfcprovisioning.txt peut ressembler à ce qui suit :

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Pour obtenir la somme de contrôle de Citrix Secure Hub La somme de contrôle de Citrix Secure Hub est une valeur constante : `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`. Pour télécharger un fichier APK pour Citrix Secure Hub, utilisez le lien suivant de Google Play Store : `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour obtenir une somme de contrôle d'application Prérequis :

- L'outil **apksigner** de l'Android SDK Build Tools
- Ligne de commande OpenSSL

Pour obtenir la somme de contrôle d'une application, procédez comme suit :

1. Téléchargez le fichier APK de l'application depuis le Google Play Store.
2. Dans la ligne de commande OpenSSL, accédez à l'outil **apksigner** : `android-sdk/build-tools/<version>/apksigner` et tapez ce qui suit :

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{
 (?<=SHA-256 digest:) .* }
 '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
<!--NeedCopy-->
```

   La commande renvoie une somme de contrôle valide.

3. Pour générer le code QR, saisissez la somme de contrôle dans le champ `PROVISIONING_DEVICE_ADMIN_` . Par exemple :

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"
    }

 }

<!--NeedCopy-->
```

Bibliothèques utilisées Provisioning Tool utilise les bibliothèques suivantes dans son code source :

- Bibliothèque v7 `appcompat`, bibliothèque Design Support et bibliothèque v7 Palette Support

  Pour de plus amples informations, consultez le Guide des fonctionnalités de la bibliothèque de support dans la documentation pour développeurs Android.

- Butter Knife par Jake Wharton sous licence Apache 2.0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Provisionner des appareils avec profil de travail dans Android Entreprise

Sur les appareils avec profil de travail dans Android Enterprise, vous séparez en toute sécurité les espaces professionnels et personnels de l'appareil. Par exemple, les appareils BYOD peuvent être des appareils avec profil de travail. L'expérience d'inscription des appareils avec profil de travail est similaire à l'inscription Android dans Citrix Endpoint Management. Les utilisateurs téléchargent Citrix Secure Hub depuis Google Play et inscrivent leurs appareils.

Par défaut, les paramètres Débogage USB et Sources inconnues sont désactivés sur un appareil lorsqu'il est inscrit en tant qu'appareil de profil professionnel dans Android Enterprise.

> **Conseil :**
>
> Lors de l'inscription d'appareils dans Android Enterprise en tant qu'appareils avec profil de travail, accédez toujours à Google Play. De là, activez l'affichage de Citrix Secure Hub dans le profil personnel de l'utilisateur.

Système d'exploitation Android

November 29, 2023

> **Remarque :**
>
> Cet article ne s'applique pas aux appareils gérés avec Android Enterprise. Pour plus d'informations sur ces appareils, consultez d'autres articles de cette section.

Citrix Endpoint Management prend également en charge les appareils Android qui ne sont pas gérés par un programme d'entreprise Android ou Samsung. Pour contrôler quand et comment les appareils Android se connectent au service Citrix Endpoint Management, utilisez Firebase Cloud Messaging (FCM). Pour plus d'informations, voir Firebase Cloud Messaging.

Les profils d'inscription déterminent si les appareils Android s'inscrivent en mode MAM, MDM ou MDM+MAM, avec la possibilité pour les utilisateurs de se désinscrire de MDM. Citrix Endpoint Management prend en charge les types d'authentification suivants pour les appareils Android en mode MDM+MAM. Pour plus d'informations, consultez les articles suivants :

- Authentification domaine ou domaine + jeton de sécurité
- Authentification certificat client ou certificat + domaine
- Fournisseurs d'identité :
  - Authentification avec Azure Active Directory via Citrix Cloud
  - Authentification avec Okta via Citrix Cloud

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Une autre méthode d'authentification rarement utilisée est le certificat client et le jeton de sécurité. Pour de plus amples informations, consultez https://support.citrix.com/article/CTX215200.

Un workflow général pour le démarrage de la gestion des appareils Android est le suivant :

1. Effectuez le processus d'intégration. Consultez les sections Intégration et configuration des ressources et Préparation à l'inscription d'appareils et à la mise à disposition de ressources.
2. Choisissez et configurez une méthode d'inscription. Consultez la section Méthodes d'inscription prises en charge.
3. Configurez les stratégies d'appareil Android.
4. Inscrivez des appareils Android.
5. Configurez les actions de sécurité des appareils et des applications. Consultez la section Actions de sécurisation.

Pour les systèmes d'exploitation pris en charge, consultez la section Systèmes d'exploitation d'appareils pris en charge.

Méthodes d'inscription prises en charge

Le tableau suivant indique les méthodes d'inscription prises en charge par Citrix Endpoint Management pour les appareils Android :

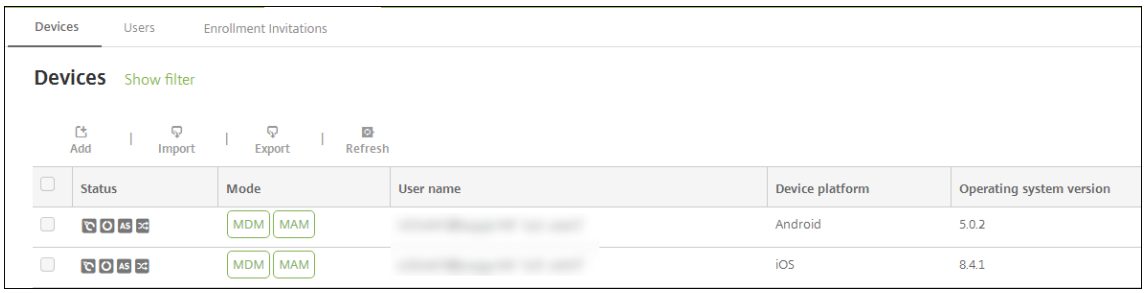
Méthode	Pris en charge
Inscription en bloc	Non
Inscription manuelle	Oui
Invitations d'inscription	Oui

Ajouter un appareil Android manuellement

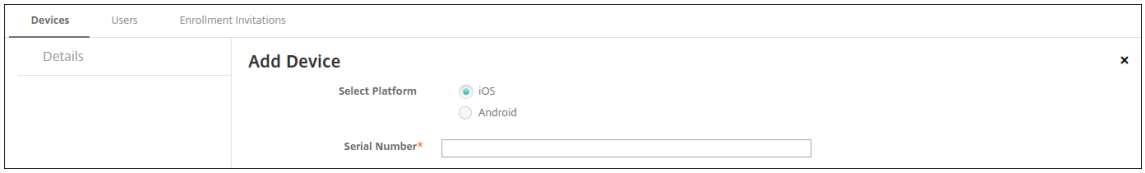
Si vous souhaitez ajouter manuellement un appareil Android ou iOS, par exemple à des fins de test, procédez comme suit.

1. Dans la console Citrix Endpoint Management, cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Cliquez sur **Ajouter**. La page **Ajouter un appareil** s'affiche.



3. Pour configurer ces paramètres :

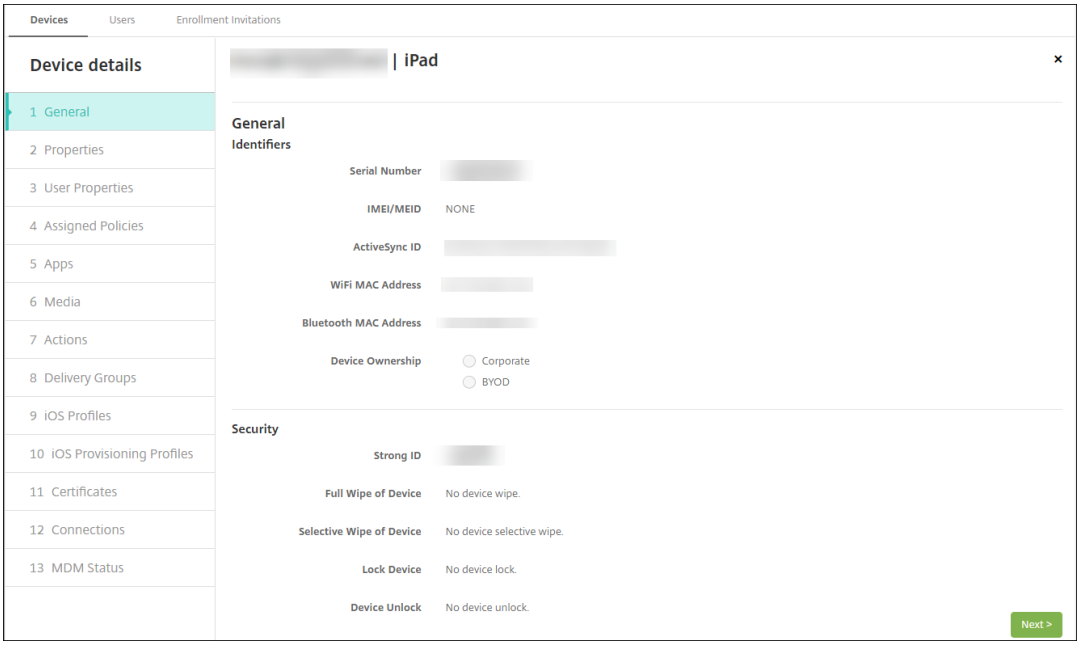
   - **Sélectionner une plate-forme :** cliquez sur **Android**.
   - **Numéro de série :** entrez le numéro de série de l'appareil.
   - **IMEI/MEID :** entrez les informations IMEi/MEID de l'appareil (facultatif).

4. Cliquez sur **Ajouter**. Le tableau **Appareils** s'affiche avec l'appareil ajouté en bas de la liste. Pour afficher et confirmer les détails de l'appareil, sélectionnez l'appareil que vous avez ajouté, puis dans le menu qui s'affiche, cliquez sur **Modifier**.

   > **Remarque :**
   >
   > Lorsque vous sélectionnez la case à cocher en regard d'un appareil, le menu d'options s'affiche au-dessus de la liste des appareils. Lorsque vous cliquez dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

   - LDAP configuré
   - Si vous utilisez des groupes locaux et utilisateurs locaux :
     - Un ou plusieurs groupes locaux.
     - Utilisateurs locaux attribués à des groupes locaux.
     - Des groupes de mise à disposition sont associés à des groupes locaux.
   - Utilisation d'Active Directory :
     - Des groupes de mise à disposition sont associés à des groupes Active Directory.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. La page **Général** dresse la liste des **identificateurs**, tels que le numéro de série et d'autres informations relatives au type de plate-forme. Pour **Propriétaire**, sélectionnez **Entreprise** ou **BYOD**.

   La page **Général** dresse également la liste des propriétés de **sécurité**, telles que ID fort, Verrouiller l'appareil, Contourner le verrouillage d'activation et d'autres informations relatives au type de plate-forme. Le champ **Effacement complet de l'appareil** inclut le code PIN de l'utilisateur. L'utilisateur doit entrer ce code une fois que l'appareil est effacé. Si l'utilisateur oublie le code, vous pouvez le rechercher ici.

6. La page **Propriétés** dresse la liste des propriétés d'appareil qu'Citrix Endpoint Management va provisionner. Cette liste affiche toutes les propriétés d'appareil incluses dans le fichier de provisioning utilisé pour ajouter l'appareil. Pour ajouter une propriété, cliquez sur **Ajouter**, puis sélectionnez une propriété dans la liste. Pour connaître les valeurs valides pour chaque propriété, consultez le PDF Valeurs et noms des propriétés d'appareil.

   Lorsque vous ajoutez une propriété, elle s'affiche initialement sous la catégorie dans laquelle vous l'avez ajoutée. Après avoir cliqué sur **Suivant** et être revenu sur la page **Propriétés**, la propriété s'affiche dans la liste appropriée.

   Pour supprimer une propriété, placez le curseur dessus et cliquez sur le **X** sur le côté droit. Citrix Endpoint Management supprime l'élément immédiatement.

7. Les sections **Détails de l'appareil** restantes contiennent des informations sommaires sur l'appareil.

   - **Propriétés utilisateur :** affiche les rôles RBAC, les appartenances aux groupes, les comptes Google Play d'entreprise et les propriétés de l'utilisateur. Vous pouvez retirer

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

un compte Google Play d'entreprise à partir de cette page.

- **Stratégies attribuées :** affiche le nombre de stratégies déployées, en attente ou ayant échoué. Fournit les informations relatives au nom, au type et à la dernière date de déploiement pour chaque stratégie. Permet de réinitialiser l'état du déploiement sur « En attente » et de redéployer les stratégies supprimées par l'utilisateur.
- **Applications :** affiche, pour le dernier inventaire, le nombre de déploiements d'applications installés, en attente et ayant échoué. Fournit le nom de l'application, l'identificateur, le type et d'autres informations. Pour une description des clés d'inventaire iOS et macOS, telles que **HasUpdateAvailable**, voir Protocole de gestion des appareils mobiles (MDM).
- **Média :** affiche, pour le dernier inventaire, le nombre de déploiements de médias installés, en attente et ayant échoué.
- **Actions :** affiche le nombre d'actions déployées, en attente et qui ont échoué. Fournit le nom de l'action et l'heure du dernier déploiement.
- **Groupes de mise à disposition :** affiche le nombre de groupes de mise à disposition ayant réussi, en attente et qui ont échoué. Pour chaque déploiement, fournit le nom du groupe mise à disposition et l'heure déploiement. Sélectionnez un groupe de mise à disposition pour afficher des informations plus détaillées, y compris l'état, l'action, le canal ou l'utilisateur.
- **Profils iOS :** affiche le dernier inventaire de profil iOS, y compris le nom, le type, l'organisation et une description.
- **Profils de provisioning iOS :** affiche les informations du profil de provisioning de distribution d'entreprise, telles que l'UUID, la date d'expiration, et si les profils sont gérés ou non gérés.
- **Certificats :** affiche pour les certificats valides, révoqués ou ayant expiré, des informations telles que le type, le fournisseur, l'émetteur, le numéro de série et le nombre de jours restants avant l'expiration.
- **Connexions :** affiche l'état de la première connexion et de la dernière connexion. Fournit pour chaque connexion, le nom d'utilisateur, l'heure de l'avant-dernière authentification et l'heure de la dernière authentification.
- **État du MDM :** affiche des informations telles que l'état du MDM, l'heure de la dernière notification push et l'heure de la dernière réponse de l'appareil.

Configurer les stratégies d'appareil Android

Utilisez ces stratégies pour configurer l'interaction entre Citrix Endpoint Management et les appareils exécutant Android. Ce tableau répertorie toutes les stratégies d'appareils disponibles pour les appareils Android.

| | | |
|—|—|—|

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

[APN](/fr-fr/citrix-endpoint-management/policies/apn-policy.html#android-settings)	[Accès aux applications](/fr-fr/citrix-endpoint-management/policies/app-access-policy.html)	[Inventaire des applications](/fr-fr/citrix-endpoint-management/policies/app-inventory-policy.html)
[Mode kiosque](/fr-fr/citrix-endpoint-management/policies/app-lock-policy.html#android-legacy-da-settings)	[Désinstallation des applications](/fr-fr/citrix-endpoint-management/policies/app-uninstall-policy.html)	[Informations d'identification](/fr-fr/citrix-endpoint-management/policies/credentials-policy.html#android-settings)
[Options Citrix Endpoint Management](/fr-fr/citrix-endpoint-management/policies/options-policy.html)	[Désinstallation de Citrix Endpoint Management](/fr-fr/citrix-endpoint-management/policies/uninsta policy.html)	[Fichiers](/fr-fr/citrix-endpoint-management/policies/files-policy.html)
[Configuration du Launcher](/fr-fr/citrix-endpoint-management/policies/launcher-configuration-policy.html)	[Emplacement](/fr-fr/citrix-endpoint-management/policies/location-policy.html#android-legacy-da-settings)	[Réseau](/fr-fr/citrix-endpoint-management/policies/network-policy.html#android-legacy-da-settings)
[Code secret](/fr-fr/citrix-endpoint-management/policies/passcode-policy.html#android-legacy-da-settings)	[Restrictions](/fr-fr/citrix-endpoint-management/policies/restrictions-policy.html#android-settings)	[Planification](/fr-fr/citrix-endpoint-management/policies/connection-scheduling-policy.html)
[Magasin](/fr-fr/citrix-endpoint-management/policies/store-policy.html)	[Termes et conditions](/fr-fr/citrix-endpoint-management/policies/terms-and-conditions-policy.html)	[Tunnel](/fr-fr/citrix-endpoint-management/policies/tunnel-policy.html)
VPN	Clip Web

Inscrire des appareils Android

1. Accédez au magasin Google Play sur votre Android et téléchargez l'application Citrix Secure Hub, puis touchez l'application.
2. Lorsque vous êtes invité à installer l'application, cliquez sur **Suivant**, puis cliquez sur **Installer**.
3. Après l'installation de Citrix Secure Hub, touchez **Ouvrir**.
4. Pour les appareils fonctionnant sous Android 6.0 ou version ultérieure, acceptez les autorisations requises :
   - Autoriser Citrix Secure Hub à passer et à gérer des appels téléphoniques ? (requis)
   - Autoriser Citrix Secure Hub à accéder aux photos, aux médias et aux fichiers de votre appareil ? (requis)
   - Autoriser Citrix Secure Hub à accéder à l'emplacement de cet appareil ? (facultatif)
5. Entrez vos informations d'identification d'entreprise, telles que le nom de votre serveur Citrix Endpoint Management, le nom d'utilisateur principal (UPN), ou votre adresse e-mail. Cliquez ensuite sur **Suivant**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Choisissez comment inscrire votre appareil :
   - Pour inscrire en mode MDM + MAM, appuyez sur **Oui, inscrire**.
   - Pour inscrire en mode MAM, appuyez sur **Non**.
7. Dans la boîte de dialogue **Activer l'administrateur de l'appareil**, touchez **Activer**.
8. Entrez votre mot de passe d'entreprise, puis touchez **Se connecter**.
9. En fonction de la configuration d'Citrix Endpoint Management, vous pouvez être invité à créer un code PIN Citrix. Vous pouvez utiliser le code PIN pour vous connecter à Citrix Secure Hub et à d'autres applications Citrix Endpoint Management, telles que Citrix Secure Mail et Citrix Files. Vous devez entrer votre code PIN Citrix deux fois. Sur l'écran **Créer un code PIN Citrix**, entrez un code PIN.
10. Entrez de nouveau le code PIN. Citrix Secure Hub s'affiche. Vous pouvez ensuite accéder à l'app store pour afficher les applications que vous pouvez installer sur votre appareil Android.
11. Si vous avez configuré Citrix Endpoint Management pour distribuer automatiquement des applications sur les appareils après l'inscription, les utilisateurs sont invités à installer les applications. En outre, les stratégies que vous configurez dans Citrix Endpoint Management sont déployées sur l'appareil. Cliquez sur **Installer** pour installer les applications.

Pour désinscrire et réinscrire un appareil Android

Les utilisateurs peuvent se désinscrire depuis Citrix Secure Hub. Lorsque les utilisateurs se désinscrivent à l'aide de la procédure suivante, l'appareil s'affiche toujours dans l'inventaire d'appareils dans la console Citrix Endpoint Management. Cependant, vous ne pouvez pas effectuer d'actions sur l'appareil. Par exemple, vous ne pouvez pas suivre l'appareil ni contrôler sa conformité.

1. Touchez pour ouvrir l'application Citrix Secure Hub.
2. Selon que vous possédez une tablette ou un téléphone, procédez comme suit :

   Sur un téléphone :

   - Balayez l'écran à partir de la gauche pour ouvrir un panneau de paramètres.
   - Touchez **Préférences**, **Comptes**, puis touchez **Supprimer le compte**.

   Sur une tablette :

   - Touchez la flèche en regard de votre adresse e-mail sur le coin supérieur droit.
   - Touchez **Préférences**, **Comptes**, puis touchez **Supprimer le compte**.
3. Dans la fenêtre **Supprimer le compte ?**, appuyez sur **Oui, supprimer**.
   Citrix Secure Hub désinscrit votre appareil. Suivez les instructions à l'écran pour réinscrire votre appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Actions de sécurisation

Android prend en charge les actions de sécurisation suivantes. Pour obtenir une description de chaque action, consultez la section Actions de sécurisation.

Mode kiosque	Effacement des applications	Renouvellement de certificat
Effacer	Localiser	Verrouiller
Verrouiller et réinitialiser un mot de passe	Notify	Révoquer
Effacer les données d'entreprise		

> **Remarque :**
>
> Pour les appareils exécutant Android 6.0 ou version ultérieure, la fonction Localiser requiert que l'utilisateur donne accès à la localisation lors de l'inscription. L'utilisateur peut choisir de ne pas accorder l'autorisation de localisation. Si l'utilisateur n'accorde pas l'autorisation lors de l'inscription, Citrix Endpoint Management demande à nouveau l'autorisation de localisation lors de l'envoi de la commande Localiser.

Firebase Cloud Messaging

November 29, 2023

> **Remarque :**
>
> Firebase Cloud Messaging (FCM) était auparavant connu sous le nom de Google Cloud Messaging (GCM). Certaines étiquettes et certains messages de la console Citrix Endpoint Management utilisent la terminologie GCM.

Citrix recommande d'utiliser Firebase Cloud Messaging (FCM) pour contrôler quand et comment les appareils Android se connectent à Citrix Endpoint Management. Citrix Endpoint Management, lorsqu'il est configuré pour FCM, envoie des notifications de connexion aux appareils Android activés pour FCM. Toute action de sécurité ou commande de déploiement déclenche une notification push afin d'inviter l'utilisateur à se reconnecter au serveur Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Une fois que vous avez terminé les étapes de configuration de cet article et qu'un appareil se connecte, l'appareil s'enregistre auprès du service FCM dans Citrix Endpoint Management. Cette connexion permet une communication quasi en temps réel de votre service Citrix Endpoint Management vers votre appareil à l'aide de FCM. L'enregistrement FCM fonctionne pour les nouveaux appareils inscrits et les appareils déjà inscrits.

Lorsque Citrix Endpoint Management doit initier une connexion avec l'appareil, il se connecte au service FCM. Ensuite, le service FCM envoie à l'appareil une notification pour qu'il se connecte. Ce type de connexion est similaire à ce qu'Apple utilise pour son service de notification Push (APNs).

Conditions préalables

- Dernier client Citrix Secure Hub
- Informations d'identification du compte Google Developer
- Services Google Play installés sur les appareils Android compatibles avec FCM

Ports du pare-feu

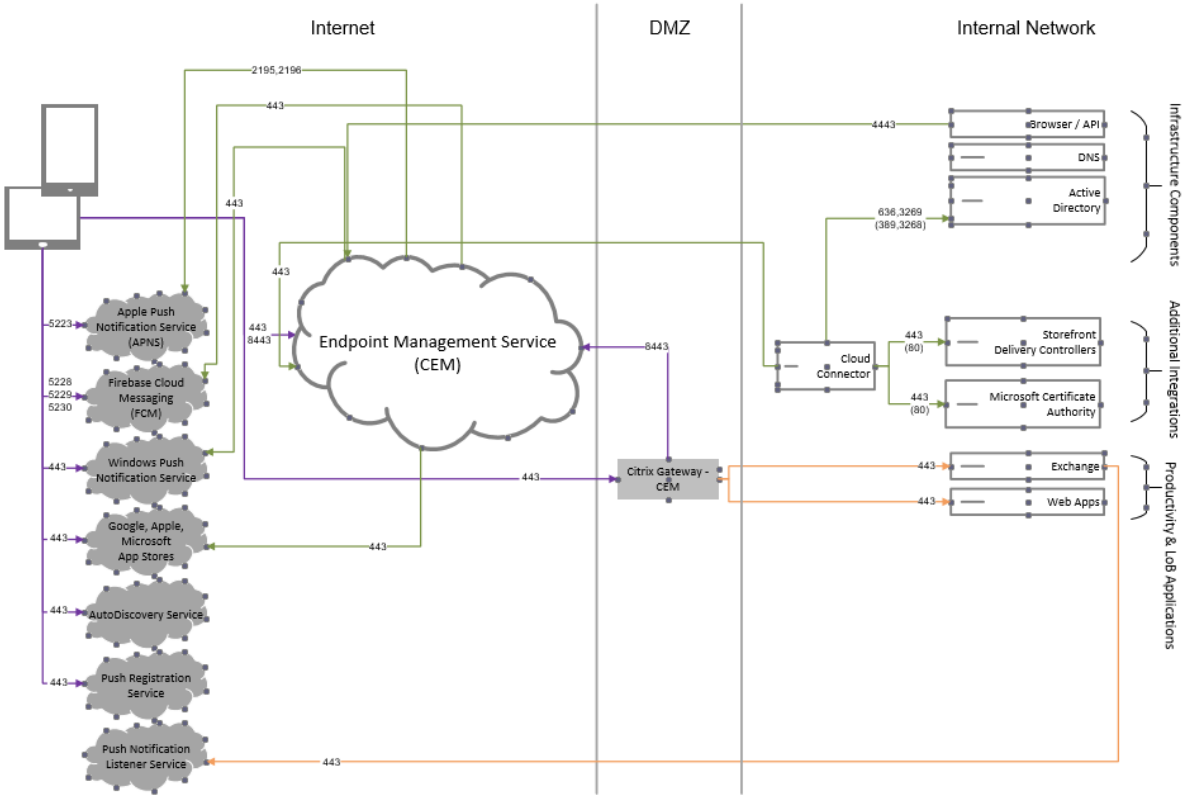
- Ouvrez le port 443 sur Citrix Endpoint Management vers `fcm.googleapis.com` et `Google.com`.
- Ouvrez la communication Internet sortante pour le réseau Wi-Fi de l'appareil sur les ports 5228, 5229 et 5230.
- Pour autoriser les connexions sortantes, FCM recommande d'ajouter les ports 5228 à 5230 à une liste d'autorisation sans restrictions IP. Toutefois, si vous avez besoin de restrictions IP, FCM recommande d'ajouter toutes les adresses IP dans les blocs IPv4 et IPv6 à une liste d'autorisation. Ces blocs sont répertoriés dans l'ASN 15169 de Google. Mettez à jour cette liste tous les mois.

Pour plus d'informations, consultez la section Configuration requise pour les ports.

Architecture

Ce diagramme illustre le flux de communication pour FCM dans le réseau interne et externe.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



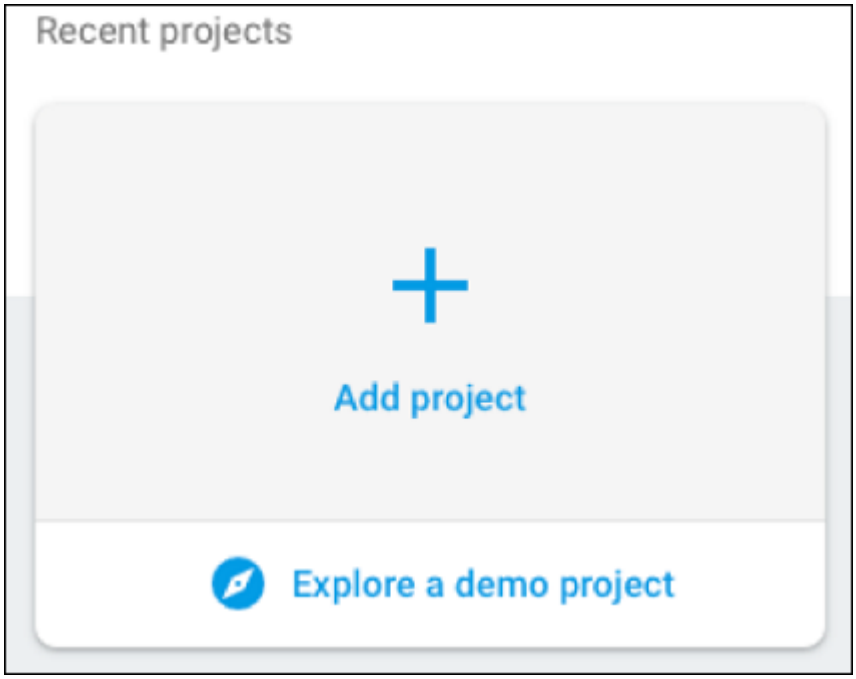
Pour configurer votre compte Google pour FCM

1. Connectez-vous à l'adresse URL suivante à l'aide des informations d'identification de votre compte Google Developer :

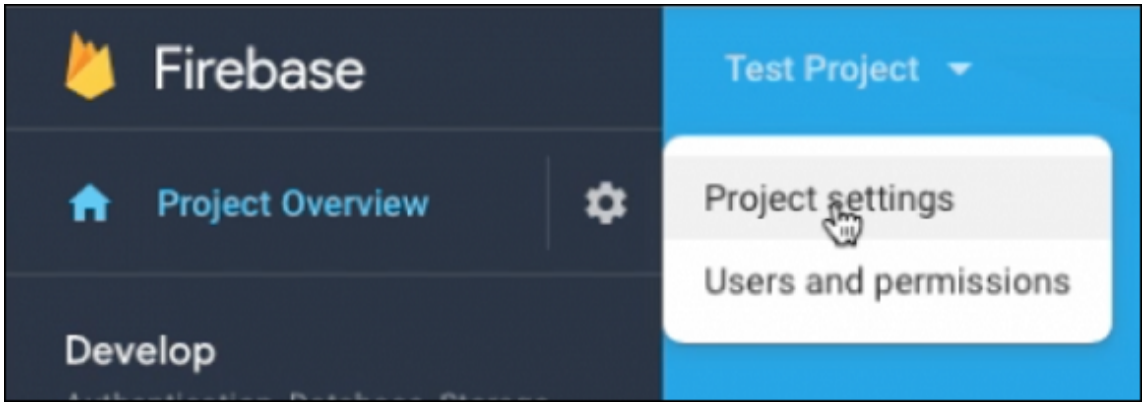
   https://console.firebase.google.com/

2. Cliquez sur **Ajouter un projet**.

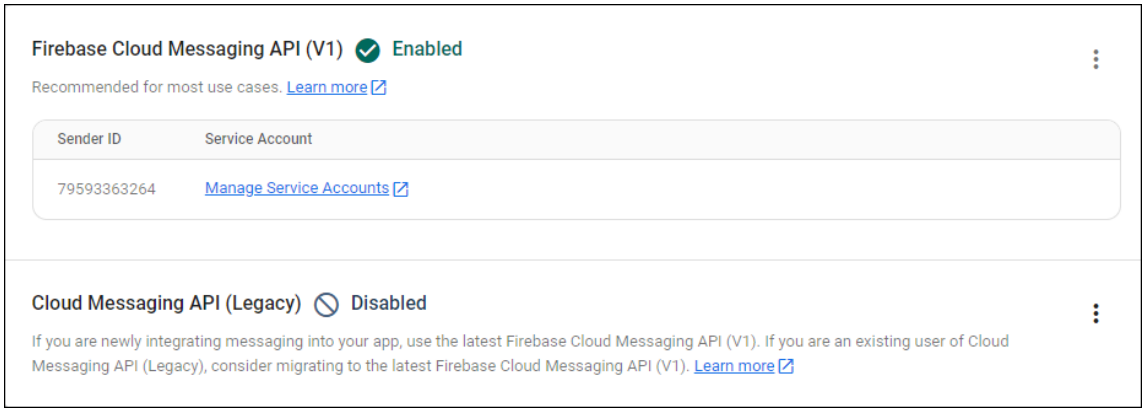
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Après avoir créé le projet, cliquez sur **Paramètres du projet**.



4. Cliquez sur l'onglet **Cloud Messaging**. Vérifiez que l'API de Firebase Cloud Messaging est activée et cliquez sur **Gérer les comptes de service**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

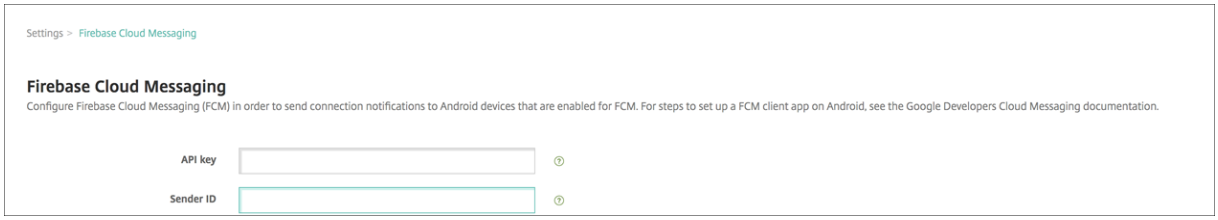
5. Copiez les valeurs des champs **Clé** et **ID client OAuth 2**. Si aucune clé n'est répertoriée, cliquez sur les points de suspension sous **Actions** pour ajouter une nouvelle clé.

Pour savoir comment configurer une application cliente FCM sur Android, consultez l'article destiné aux développeurs Google Cloud Messaging : https://firebase.google.com/docs/cloud-messaging/android/client.

Pour configurer Citrix Endpoint Management pour FCM

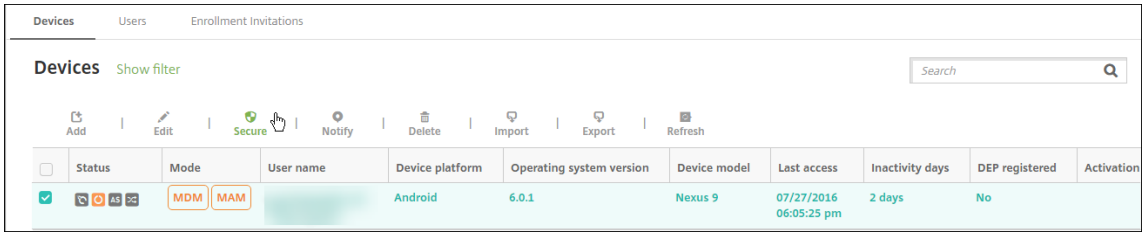
Dans la console Citrix Endpoint Management, accédez à **Paramètres > Firebase Cloud Messaging**.

- Modifiez la **clé API** et entrez la **clé** de Firebase Cloud Messaging que vous avez copiée dans la dernière étape de configuration de Firebase Cloud Messaging.
- Modifiez l'**ID de l'expéditeur** et copiez la valeur de l'**ID client OAuth 2** que vous avez copiée dans la procédure précédente.



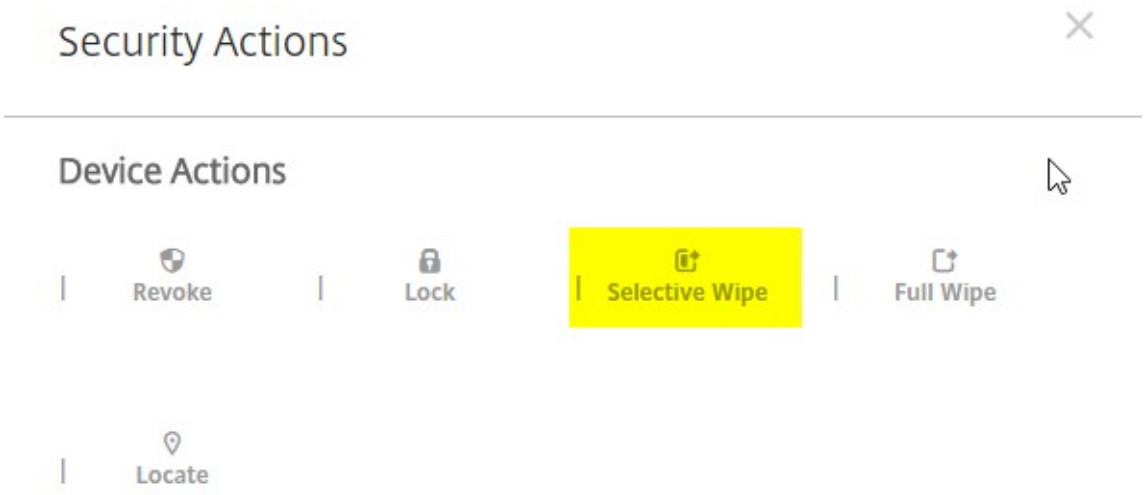
Pour tester votre configuration

1. Inscrivez un appareil Android.
2. Laissez l'appareil inactif pendant un certain temps, de façon à ce qu'il se déconnecte d'Citrix Endpoint Management.
3. À partir de la console Citrix Endpoint Management, cliquez sur **Gérer**, sélectionnez l'appareil Android, puis cliquez sur **Sécurisé**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Sous **Actions de l'appareil**, cliquez sur **Effacer les données d'entreprise**.



Dans une configuration effectuée avec succès, les données d'entreprise sont effacées sur l'appareil.

Android SafetyNet

November 29, 2023

Vous pouvez configurer la fonctionnalité Android SafetyNet pour évaluer la compatibilité et la sécurité des appareils Android sur lesquels Citrix Secure Hub est installé. Android SafetyNet n'est pas disponible pour les déploiements MAM.

Lorsque cette fonctionnalité est activée, l'API SafetyNet Attestation examine les informations logicielles et matérielles sur un appareil pour créer un profil de cet appareil. L'API recherche ensuite le même profil dans une liste de modèles d'appareils qui ont passé avec succès le test de compatibilité Android. L'API utilise également ces informations pour déterminer si Citrix Secure Hub a été modifié par une source inconnue.

Lorsque la fonctionnalité Android SafetyNet est activée, Citrix Secure Hub envoie la requête SafetyNet Attestation API aux services Google Play et le résultat est transmis à Citrix Endpoint Management. Citrix Endpoint Management met ensuite les informations sur l'appareil à jour avec les résultats de l'attestation. Vous pouvez définir des actions automatisées qui utilisent les résultats de l'attestation pour déclencher des actions sur l'appareil.

Pour plus d'informations sur le fonctionnement de l'API SafetyNet Attestation, consultez la documentation pour développeurs Android.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Estimation du nombre de requêtes de l'API SafetyNet Attestation nécessaires

Les requêtes de l'API SafetyNet Attestation sont envoyées :

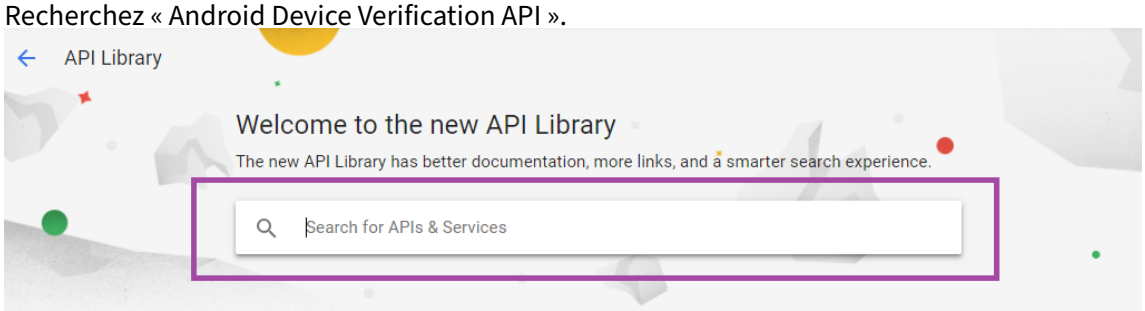
- Lorsqu'un appareil est inscrit dans Citrix Endpoint Management.
- Lors d'une authentification en ligne Citrix Secure Hub. Une authentification en ligne a lieu lorsqu'une session de serveur expire ou qu'un utilisateur se déconnecte du serveur, puis se reconnecte. Citrix Secure Hub invite l'utilisateur à envoyer des informations d'identification pour s'authentifier auprès du serveur.
- Lorsqu'un appareil est redémarré.
- À un intervalle que vous définissez, compris entre 24 et 1 000 heures.

Si votre déploiement Citrix Endpoint Management produit plus de 10 000 requêtes par jour, remplissez ce formulaire de demande de quota.

Obtention de la clé d'API SafetyNet

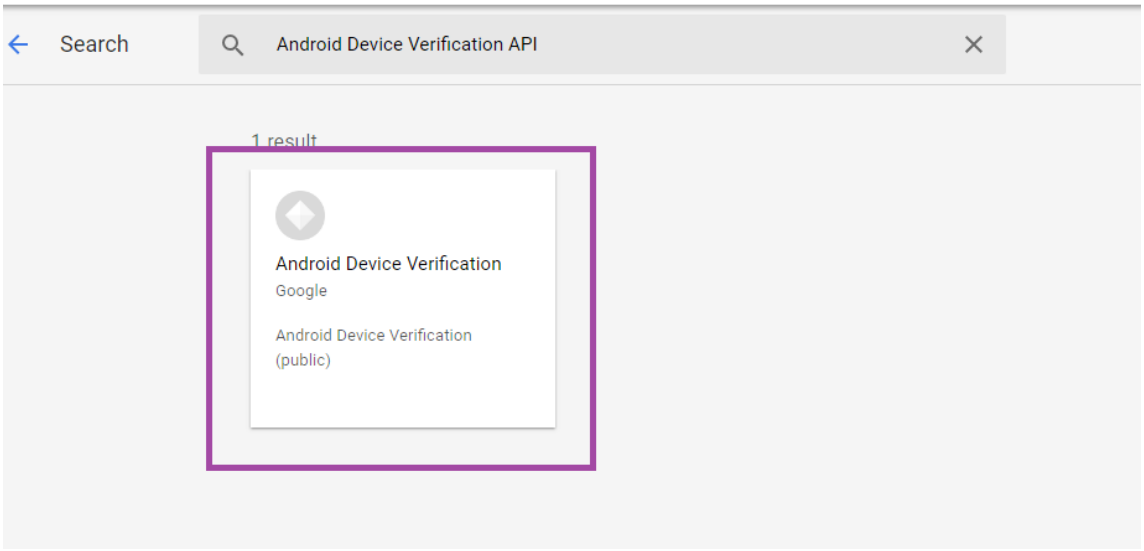
Pour activer Android SafetyNet dans Citrix Endpoint Management, vous avez besoin de la clé d'API SafetyNet.

1. Connectez-vous à la console d'API Google avec les informations d'identification de votre compte d'administrateur Google.
2. Accédez à la page Library.
3. Recherchez « Android Device Verification API ».

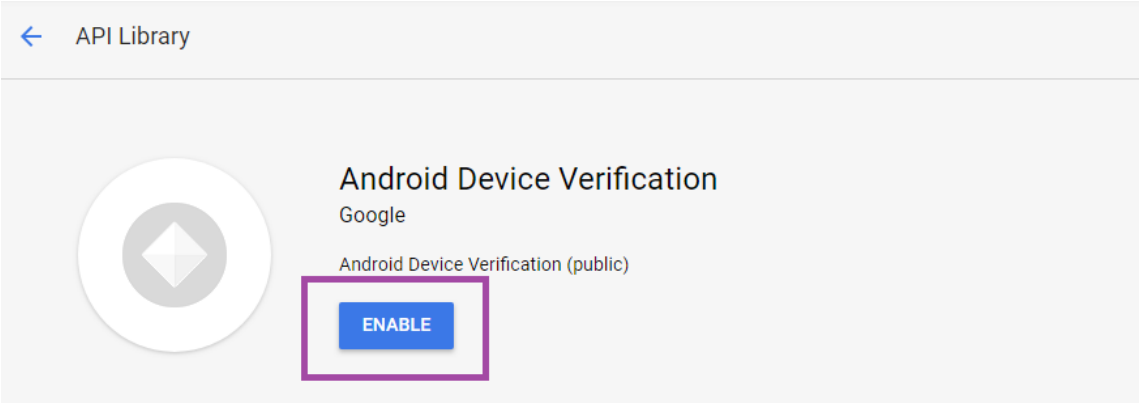


4. Cliquez sur **Android Device Verification API**.

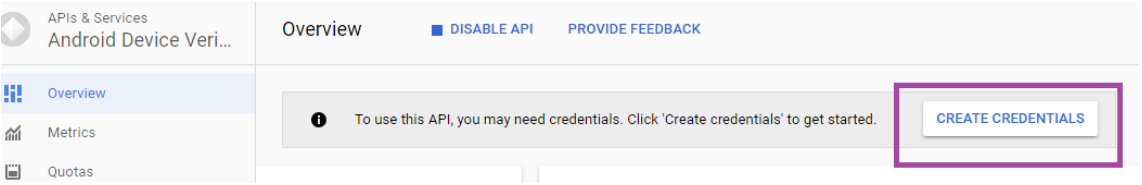
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



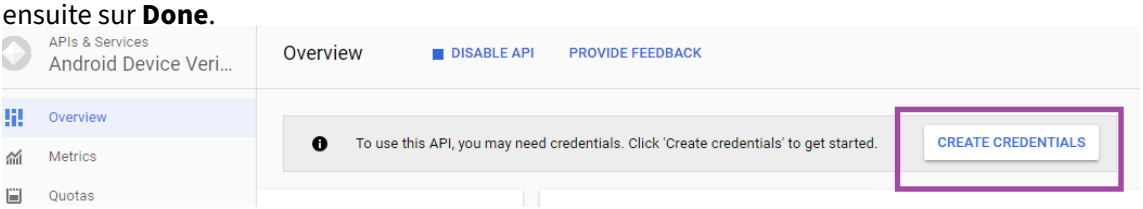
5. Si l'API n'est pas déjà activée, cliquez sur **Enable**.



6. Cliquez sur **Manage**.
7. Cliquez sur **Create Credentials** pour générer une clé d'API.

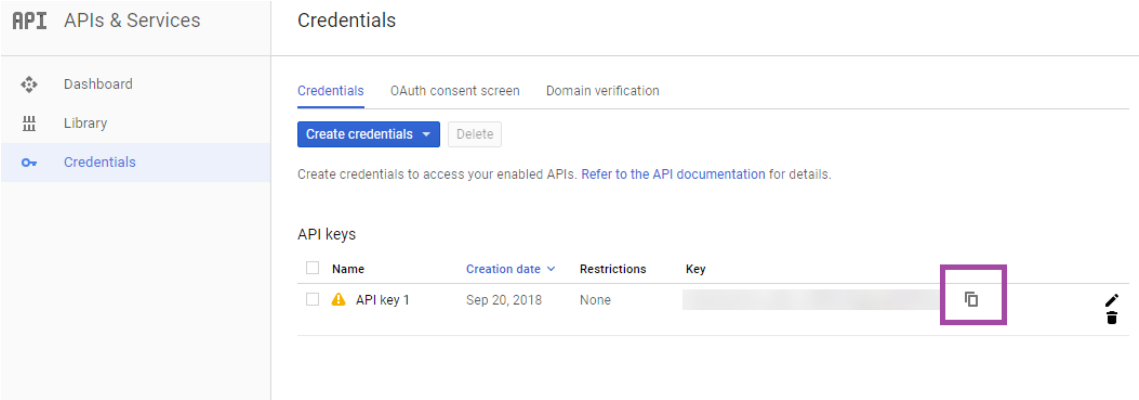


8. Sélectionnez **Android Device Verification** et cliquez sur **What credentials to I need**. Cliquez ensuite sur **Done**.



9. Dans la page **Credentials**, cliquez sur l'icône de copie en regard de la clé pour copier la clé.

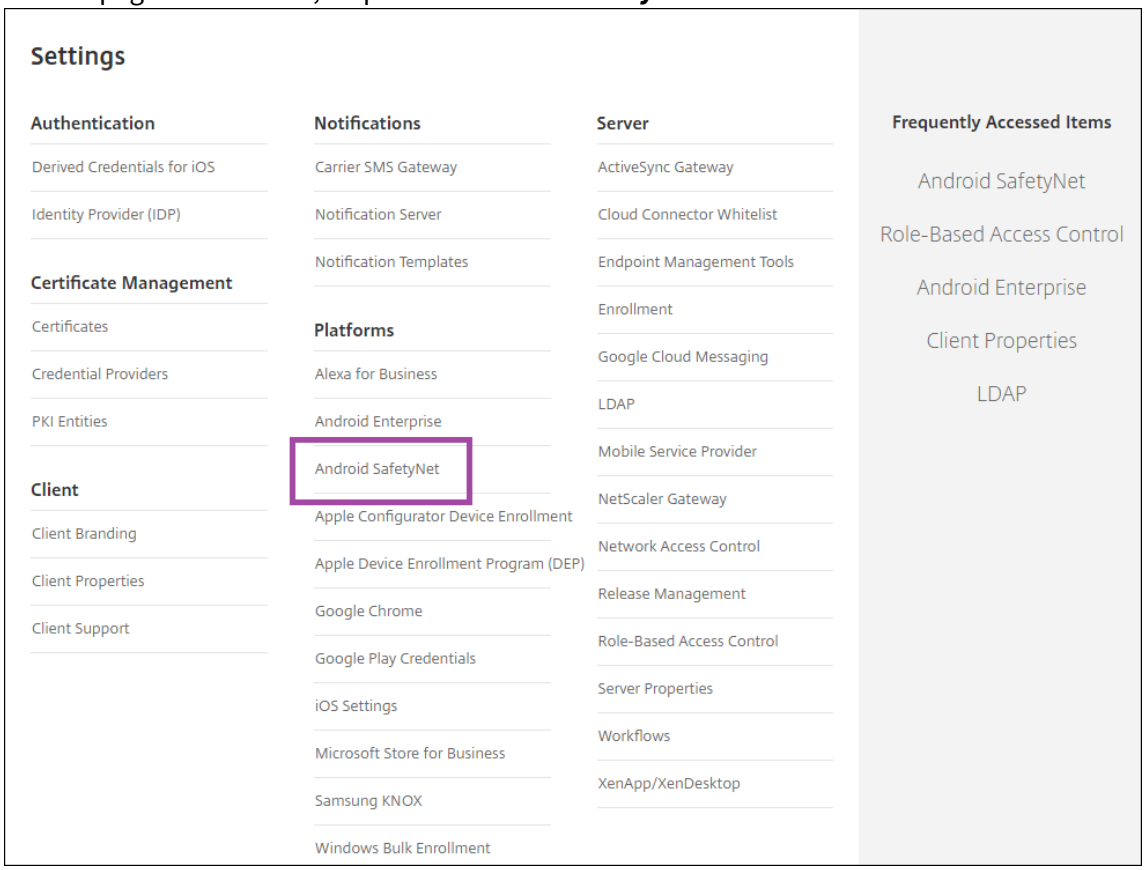
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



10. Enregistrez la clé affin de la coller dans la console Citrix Endpoint Management lorsque vous activez Android SafetyNet.

Activation d'Android SafetyNet

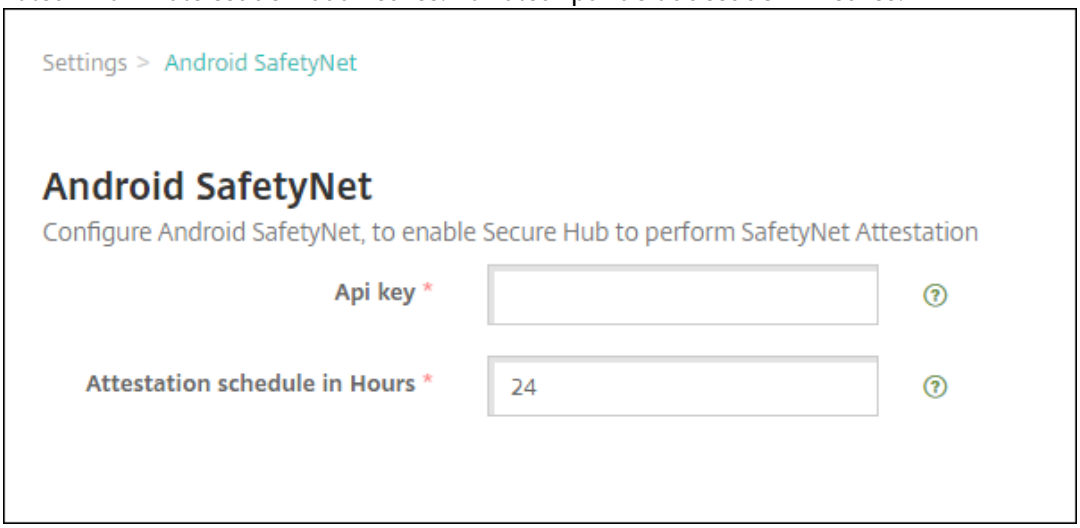
1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Dans la page **Paramètres**, cliquez sur **Android SafetyNet**.



3. Pour configurer ces paramètres :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Clé API**. Collez dans SafetyNet la clé API que vous avez obtenue depuis la console d'API Google.
- **Calendrier d'attestation en heures**. Saisissez l'intervalle en heures auquel l'API SafetyNet Attestation évalue vos appareils Android. La valeur minimale est de 24 heures. La valeur maximale est de 1 000 heures. La valeur par défaut est de 24 heures.

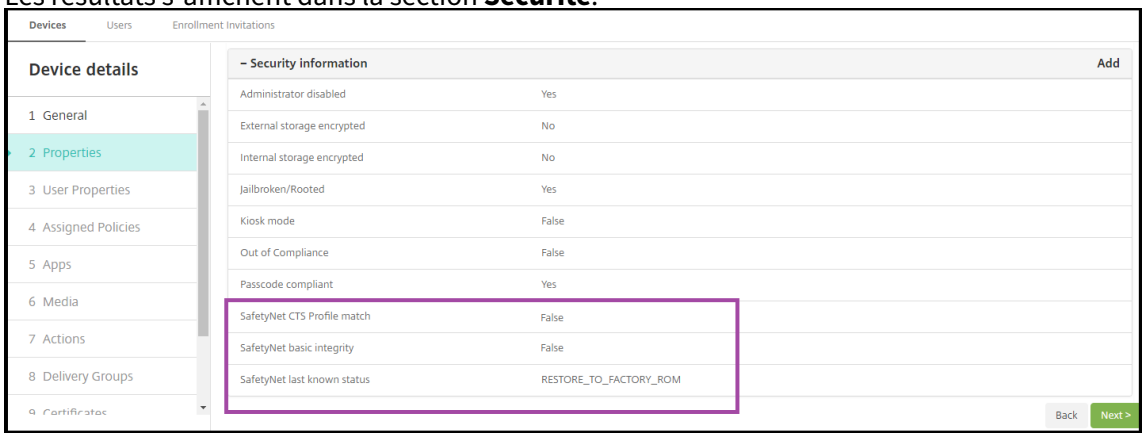


4. Cliquez sur **Save**.

Affichage des résultats d'Android SafetyNet

Pour afficher les résultats de l'évaluation de l'API SafetyNet Attestation d'un appareil :

1. Dans la console Citrix Endpoint Management, cliquez sur **Gérer > Appareils**.
2. Sélectionnez les appareils Android pour afficher les résultats de l'API SafetyNet Attestation. Cliquez sur **Afficher plus**.
3. Dans la page **Détails de l'appareil**, sélectionnez **Propriétés**.
4. Les résultats s'affichent dans la section **Sécurité**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

L'API SafetyNet Attestation renvoie ces états pour chaque appareil :

- **Correspondance de profil CTS de SafetyNet :** si cette valeur est définie sur **True**, le profil correspond à un profil qui a passé avec succès la suite de tests de compatibilité Android (CTS). Si cette valeur est définie sur **False**, le profil de l'appareil ne correspond pas à un profil qui a passé avec succès la suite de tests de compatibilité Android.
- **Intégrité de base de SafetyNet :** si cette valeur est définie sur **True**, SafetyNet Attestation API n'a trouvé aucune preuve de la modification de Citrix Secure Hub sur l'appareil par une source inconnue. Si cette valeur est définie sur **False**, Citrix Secure Hub sur l'appareil a été modifié par une source inconnue.
- **Dernier état connu de SafetyNet :** cette valeur affiche le dernier état SafetyNet connu de l'appareil :
  - **Succès :** l'API SafetyNet Attestation n'a trouvé aucune preuve de la modification de Citrix Secure Hub sur l'appareil par une source inconnue.
  - **LOCK_BOOTLOADER :** l'utilisateur doit verrouiller le bootloader de l'appareil. Citrix Secure Hub sur l'appareil a été modifié par une source inconnue.
  - **RESTORE_TO_FACTORY_ROM :** l'utilisateur doit restaurer la ROM de sortie d'usine de l'appareil. Citrix Secure Hub sur l'appareil a été modifié par une source inconnue.

API Play Integrity

November 29, 2023

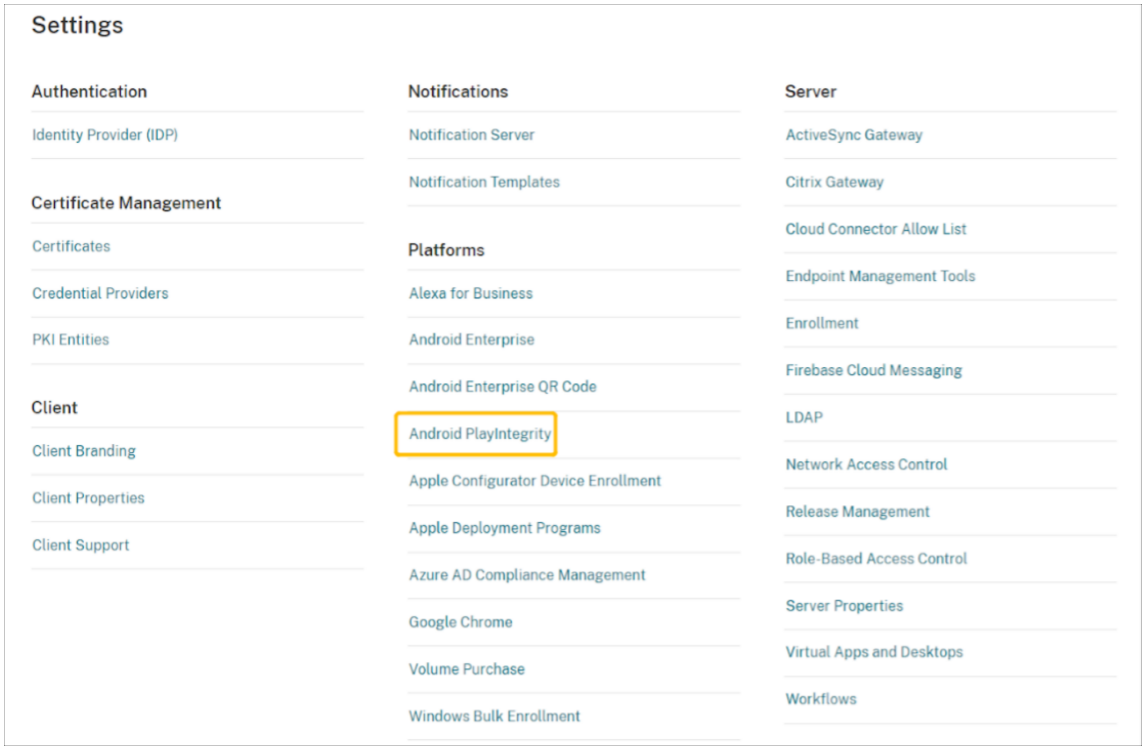
L'API Play Integrity permet de protéger vos applications et vos jeux contre les interactions potentiellement dangereuses et frauduleuses, telles que la triche et les accès non autorisés, ce qui vous permet de réagir en prenant les mesures appropriées pour prévenir les attaques et réduire les abus. Pour plus d'informations, consultez API Play Integrity.

Activer l'API Play Integrity

Suivez ces étapes pour passer à l'API Play Integrity.

1. Activez le feature flag *afw.safetynet.attestation.api.* d'obsolescence pour le serveur Citrix Endpoint Management spécifié.
2. Sur la console Citrix Endpoint Management, sélectionnez **Android PlayIntegrity** sur la page **Paramètres**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

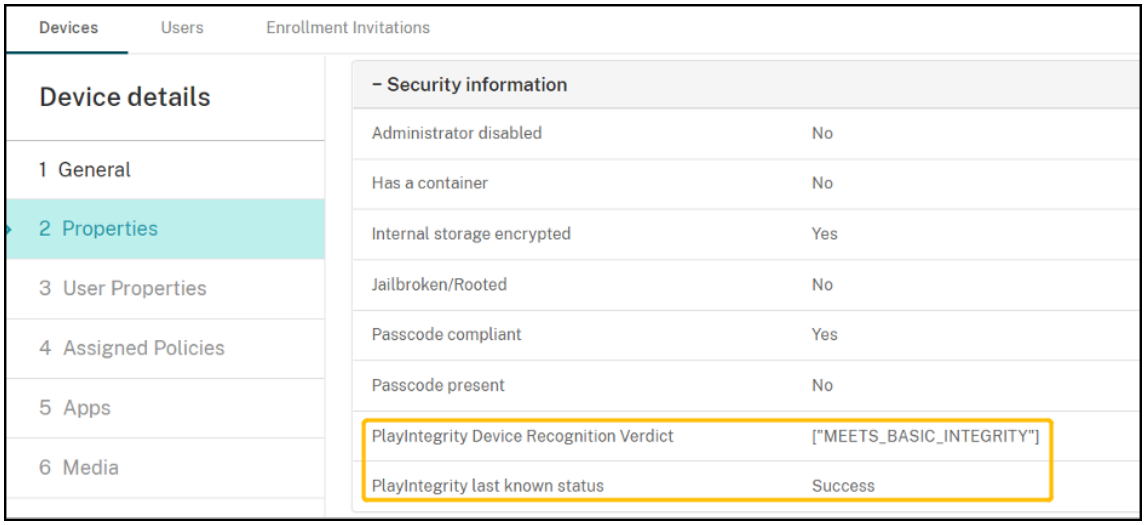


3. Entrez une valeur dans le champ Calendrier d'attestation en heures. Il s'agit de l'intervalle de temps pendant lequel l'API Play Integrity Attestation évalue votre appareil. La valeur minimale est de 24 heures et la valeur maximale de 1 000 heures. La valeur par défaut est de 24 heures. Cliquez sur **Save**.
4. Mettez à niveau vers Citrix Secure Hub Android version 23.7.0. Déconnectez-vous de votre appareil et connectez-vous à Citrix Secure Hub pour déclencher l'attestation via l'API Play Integrity.

Afficher et analyser les résultats de l'attestation de l'API Play Integrity

1. Dans la console Citrix Endpoint Management, accédez à **Gérer > Appareils**.
2. Sélectionnez l'appareil pour lequel vous souhaitez voir les résultats de l'attestation de l'API Play Integrity. Cliquez sur **Afficher plus**.
3. Dans l'onglet **Appareils**, sélectionnez **Propriétés**. Les résultats s'affichent dans la section **Informations sécurité**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. L'attestation de l'API Play Integrity renvoie les états suivants :

   - Si le champ **PlayIntegrity Device Recognition Verdict** contient **"MEETS_BASIC_INTEGRITY"** , cela signifie que Citrix Secure Hub exécuté sur l'appareil satisfait au moins aux exigences d'intégrité de base du système.
   - Si le champ **PlayIntegrity Device Recognition Verdict** ne contient pas **"MEETS_BASIC_INTEGRITY"** , cela signifie que Citrix Secure Hub sur l'appareil fonctionne peut-être sur une version non reconnue d'Android, possède peut-être un bootloader débloqué ou n'a peut-être pas été certifié par le fabricant.
   - Si le **dernier état connu de PlayIntegrity** est **Success**, cela signifie que l'attestation de l' API PlayIntegrity a été correctement exécutée.
   - Si le **dernier état connu de PlayIntegrity** est **Failure**, cela signifie que l'attestation de l' API PlayIntegrity n'a pas pu être exécutée.

> **Remarque :**
>
> L'administrateur peut désactiver le feature flag qui vous permet d'utiliser SafetyNet, avant l'arrêt définitif de SafetyNet Attestation, à la fin du mois de novembre 2023.

Limitations

1. Les appareils COSU et DO nouvellement inscrits sont marqués comme non conformes, même s'ils sont conformes.

   L'API Play Integrity renvoie une valeur vide lors de la première attestation lors de l'inscription d'un DO (device owner), ce qui donne l'impression que l'appareil n'est pas conforme. Il s'agit d'un problème connu de Google. DPC Support Lib 20230418 a été publié pour résoudre ce problème.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Le correctif est disponible à partir de la version 23.9.0. D'ici là, suivez les étapes suivantes pour contourner le problème :

- Décochez le feature flag et continuez à utiliser l'API SafetyNet pour continuer à utiliser l' API SafetyNet Attestation.
- Déconnectez-vous et reconnectez-vous pour déclencher une attestation après l'inscription. Vous pouvez également attendre la prochaine attestation périodique, qui est par défaut de 24 heures.

Ce problème se produit uniquement lors de l'inscription. L'API Play Integrity fonctionne correctement après l'inscription.

2. Les appareils WPCOD nouvellement inscrits sont marqués comme non conformes même s'ils sont conformes. Ce problème est en cours d'examen par Google.

Samsung

November 29, 2023

Samsung propose plusieurs solutions compatibles avec Citrix Endpoint Management.

Pour contrôler quand et comment les appareils Android se connectent au service Citrix Endpoint Management, utilisez Firebase Cloud Messaging (FCM). Pour plus d'informations, voir Firebase Cloud Messaging.

Les profils d'inscription déterminent si les appareils Android s'inscrivent en mode MAM, MDM ou MDM+MAM, avec la possibilité pour les utilisateurs de se désinscrire de MDM. Citrix Endpoint Management prend en charge les types d'authentification suivants pour les appareils Android inscrits en mode MDM+MAM. Pour plus d'informations, consultez les articles suivants :

- Authentification domaine ou domaine + jeton de sécurité
- Authentification certificat client ou certificat + domaine
- Fournisseurs d'identité :
  - Authentification avec Azure Active Directory via Citrix Cloud
  - Authentification avec Okta via Citrix Cloud

Une autre méthode d'authentification rarement utilisée est le certificat client et le jeton de sécurité. Pour de plus amples informations, consultez https://support.citrix.com/article/CTX215200.

Un workflow général pour le démarrage de la gestion des appareils Android est le suivant :

1. Effectuez le processus d'intégration. Consultez les sections Intégration et configuration des ressources et Préparation à l'inscription d'appareils et à la mise à disposition de ressources.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Choisissez et configurez une méthode d'inscription. Consultez la section Méthodes d'inscription prises en charge.
3. Déployez les clés de licence Samsung.
4. Configurez les stratégies d'appareil Samsung.
5. Configurez les actions de sécurité des appareils et des applications. Consultez la section Actions de sécurisation.

Pour les systèmes d'exploitation pris en charge, consultez la section Systèmes d'exploitation d'appareils pris en charge.

Méthodes d'inscription prises en charge

Le tableau suivant indique les méthodes d'inscription prises en charge par Citrix Endpoint Management pour les appareils Android :

Méthode	Pris en charge
Inscription manuelle	Oui
Invitations d'inscription	Oui

Pour de plus amples informations sur l'inscription d'appareils, consultez la section Inscription d'appareils Android.

Déployer les clés de licence Samsung

Samsung propose des clés ELM (Enterprise License Management). Les licences Samsung doivent être achetées auprès de Samsung.

Configurer les stratégies d'appareil Samsung

Stratégies d'appareil :

—	—	—
[Restrictions applicatives](/en-us/citrix-endpoint-management/policies/app-restrictions-policy.html)	[Désinstallation des applications](/fr-fr/citrix-endpoint-management/policies/app-uninstall-policy.html)	[Navigateur](/fr-fr/citrix-endpoint-management/policies/browser-policy.html)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

|[Copier les applications sur le conteneur Samsung](/fr-fr/citrix-endpoint-management/policies/copy-apps-to-samsung-container-policy.html) |[Exchange](/fr-fr/citrix-endpoint-management/policies/exchange-policy.html) |[Code secret](/fr-fr/citrix-endpoint-management/policies/passcode-policy.html)|
|Restrictions |VPN|

Actions de sécurisation

Android prend en charge les actions de sécurisation suivantes. Pour obtenir une description de chaque action, consultez la section Actions de sécurisation.

Mode kiosque	Effacement des applications	Renouvellement de certificat
Effacer	Localiser	Verrouiller
Verrouiller et réinitialiser un mot de passe	Notify	Révoquer
Effacer les données d'entreprise		

> **Remarque :**
>
> Pour les appareils exécutant Android 6.0 ou version ultérieure, la fonction Localiser requiert que l'utilisateur donne accès à la localisation lors de l'inscription. L'utilisateur peut choisir de ne pas accorder les autorisations de localisation. Si l'utilisateur n'accorde pas l'autorisation lors de l'inscription, Citrix Endpoint Management demande à nouveau les autorisations de localisation lors de l'envoi de la commande Localiser.

Contrôle d'accès réseau

March 1, 2024

Vous pouvez étendre l'évaluation de la sécurité des appareils Citrix Endpoint Management via votre solution de contrôle d'accès réseau (NAC) pour les appareils Android et Apple. Votre solution NAC utilise ensuite l'évaluation de sécurité Citrix Endpoint Management pour faciliter et gérer les décisions d'authentification. Une fois le boîtier NAC configuré, les stratégies d'appareil et les filtres NAC que vous configurez dans Citrix Endpoint Management sont appliqués.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

L'utilisation de Citrix Endpoint Management avec une solution NAC ajoute la qualité de service et un contrôle plus précis sur les appareils internes à votre réseau. Pour un résumé des avantages de l'intégration de NAC avec Citrix Endpoint Management, consultez la section Contrôle d'accès.

Citrix prend en charge ces solutions pour l'intégration à Citrix Endpoint Management :

- NetScaler Gateway
- ForeScout

Citrix ne garantit pas l'intégration avec d'autres solutions NAC.

Avec un boîtier de contrôle d'accès réseau (NAC) dans votre réseau :

- Citrix Endpoint Management prend en charge NAC en tant que fonctionnalité de sécurité de point de terminaison pour les appareils iOS, Android Enterprise et Android.
- Vous pouvez activer les filtres dans Citrix Endpoint Management pour définir les appareils comme conformes ou non conformes pour NAC, en fonction de règles ou de propriétés. Par exemple :
  - Si un appareil géré dans Citrix Endpoint Management ne répond pas aux critères spécifiés, Citrix Endpoint Management le marque comme non conforme. Le boîtier NAC bloque les appareils non conformes sur votre réseau.
  - Si un appareil géré dans Citrix Endpoint Management a installé des applications non conformes, un filtre NAC peut bloquer la connexion VPN. Par conséquent, une machine utilisateur non conforme ne peut pas accéder aux applications ou aux sites Web via le VPN.
  - Si vous utilisez NetScaler Gateway pour NAC, vous pouvez activer le split tunneling pour empêcher le plug-in NetScaler Gateway d'envoyer du trafic réseau inutile à NetScaler Gateway. Pour plus d'informations sur le split tunneling, voir Configurer le split tunneling.

Filtres de conformité NAC pris en charge

Citrix Endpoint Management prend en charge les filtres de conformité au contrôle d'accès réseau (NAC) suivants :

Appareils anonymes : vérifie si un appareil est en mode anonyme. Cette vérification est disponible si Citrix Endpoint Management ne parvient pas à authentifier à nouveau l'utilisateur lorsqu'un appareil tente de se reconnecter.

Applications sur liste noire : vérifie si un appareil dispose d'applications interdites, telles que définies dans une stratégie d'accès aux applications. Pour plus d'informations sur la stratégie, consultez la section Stratégies d'accès aux applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Appareils inactifs : vérifie si un appareil est inactif, tel que cela est défini par le paramètre **Nombre de jours maximum d'inactivité** dans la boîte de dialogue **Propriétés du serveur**. Pour de plus amples informations, consultez la section Propriétés du serveur.

Applications requises manquantes : vérifie si des applications nécessaires sont manquantes sur un appareil, tel que cela est défini dans une stratégie d'accès aux applications.

Applications non suggérées : vérifie si un appareil dispose d'applications non suggérées, telles que définies dans une stratégie d'accès aux applications.

Mot de passe non conforme : vérifie si le mot de passe utilisateur est conforme. Sur les appareils iOS et Android, Citrix Endpoint Management peut déterminer si le mot de passe actuel de l'appareil est conforme à la stratégie de code secret envoyée à l'appareil. Par exemple, sur iOS, l'utilisateur dispose de 60 minutes pour définir un mot de passe si Citrix Endpoint Management envoie une stratégie de code secret à l'appareil. Avant qu'un mot de passe ne soit défini par l'utilisateur, le code secret peut ne pas être conforme.

Appareils non conformes : vérifie si un appareil n'est pas conforme, en fonction de la propriété de l'appareil Non conforme. Cette propriété est généralement modifiée par les actions automatisées ou parce qu'un tiers utilise les API Citrix Endpoint Management.

État révoqué : vérifie si le certificat de l'appareil a été révoqué. Un appareil révoqué ne peut pas se réinscrire tant qu'il n'a pas été à nouveau autorisé.

Appareils Android rootés et iOS jailbreakés : vérifie si un appareil Android ou iOS est rooté ou jailbreaké.

Appareils non gérés : vérifie si Citrix Endpoint Management gère un appareil. Par exemple, un appareil inscrit en mode MAM ou un appareil non inscrit n'est pas géré.

> **Remarque :**
>
> Le filtre Conformité/non conformité implicite définit la valeur par défaut uniquement sur les appareils qui sont gérés par Citrix Endpoint Management. Par exemple, tous les appareils sur lesquels une application bloquée est installée ou qui ne sont pas inscrits sont marqués comme Non conformes. Le boîtier de contrôle d'accès réseau (NAC) bloque ces appareils de votre réseau.

Présentation de la configuration

Nous vous recommandons de configurer les composants NAC dans l'ordre indiqué.

1. Configurez les stratégies d'appareil pour prendre en charge NAC :

   Pour les appareils iOS : voir Configurer la stratégie VPN pour prendre en charge NAC.

   Pour les appareils Android Enterprise : voir Créer une configuration gérée par Android Enterprise pour Citrix SSO.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

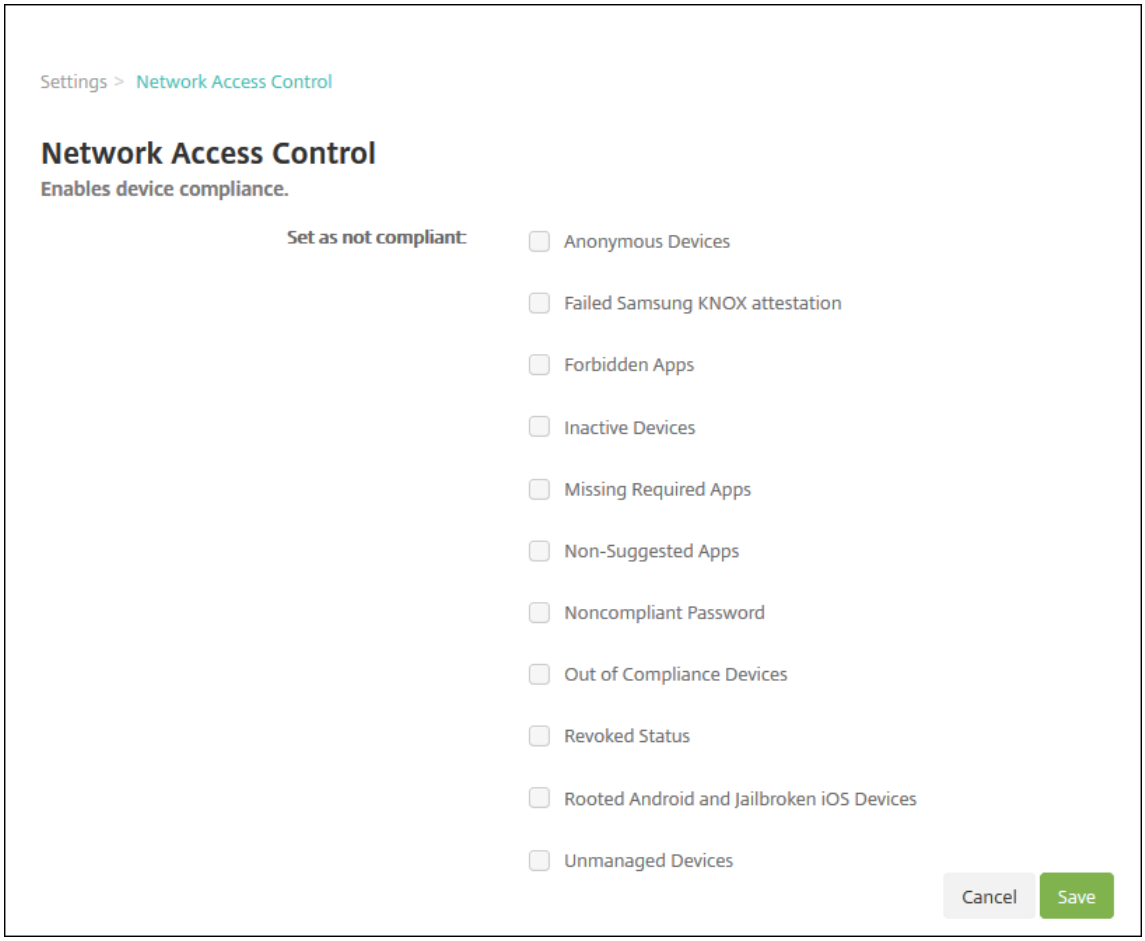
Pour les appareils Android : voir Configurer le protocole Citrix SSO pour Android.

2. Activer les filtres NAC dans Citrix Endpoint Management.
3. Configurer une solution NAC :
   - NetScaler Gateway, détaillé dans Mettre à jour les stratégies NetScaler Gateway afin de prendre en charge NAC.

     Nécessite l'installation de Citrix SSO sur les appareils. Consultez la section Clients NetScaler Gateway.
   - ForeScout : consultez la documentation ForeScout.

Activer les filtres NAC dans Citrix Endpoint Management

1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Contrôle d'accès réseau**.



2. Cochez les cases correspondant aux filtres **Définir comme non conforme** que vous souhaitez activer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Cliquez sur **Enregistrer**.

Mettre à jour les stratégies NetScaler Gateway afin de prendre en charge NAC

Vous devez configurer les stratégies d'authentification avancée (et non classique) et de sessions VPN sur votre serveur virtuel VPN.

Ces étapes mettent à jour NetScaler Gateway avec l'une des caractéristiques suivantes :

- Intégré à Citrix Endpoint Management.
- Ou, est configuré pour le VPN, ne fait pas partie de l'environnement Citrix Endpoint Management et peut atteindre Citrix Endpoint Management.

Sur votre serveur VPN virtuel, depuis une fenêtre de console, procédez comme suit. Les noms de domaine complet et les adresses IP dans les commandes et les exemples sont fictifs.

1. Supprimez et annulez la liaison de toutes les stratégies classiques si vous utilisez des stratégies classiques sur votre serveur virtuel VPN. Pour vérifier, tapez :

   ```
   show vpn vserver <VPN_VServer>
   ```

   Supprimez tout résultat contenant le terme « Classic ». Pa exemple : `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

   Pour supprimer la stratégie, tapez :

   ```
   unbind vpn vserver <VPN_VServer> -policy <policy_name>
   ```

2. Créez la stratégie de session avancée correspondante en tapant ce qui suit.

   ```
   add vpn sessionPolicy <policy_name> <rule> <session action>
   ```

   Pa exemple : `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. Liez la stratégie à votre serveur virtuel VPN en tapant ce qui suit.

   ```
   bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100
   ```

4. Créez un serveur virtuel d'authentification en tapant ce qui suit.

   ```
   add authentication vserver <authentication vserver name> <service type> <ip address>
   ```

   Par exemple : `add authentication vserver authvs SSL 0.0.0.0`
   Dans l'exemple, `0.0.0.0` signifie que le serveur virtuel d'authentification n'est pas public.

5. Liez un certificat SSL au serveur virtuel en tapant ce qui suit.

   ```
   bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pa exemple : `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. Associez un profil d'authentification au serveur virtuel d'authentification à partir du serveur virtuel VPN. Commencez par créer le profil d'authentification en tapant ce qui suit.

   `add authentication authnProfile <profile name> -authnVsName <authentication vserver name>`

   Par exemple :

   `add authentication authnProfile xm_nac_prof -authnVsName authvs`

7. Associez le profil d'authentification au serveur virtuel VPN en tapant ce qui suit.

   `set vpn vserver <vpn vserver name> -authnProfile <authn profile name>`

   Par exemple :

   `set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof`

8. Vérifiez la connexion de NetScaler Gateway à un appareil en tapant ce qui suit.

   `curl -v -k https://<Endpoint Management_server>:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"`

   Par exemple, cette requête vérifie la connectivité en obtenant l'état de conformité du premier appareil (`deviceid_1`) inscrit dans l'environnement :

   `curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"`

   Un résultat réussi est similaire à l'exemple suivant.

   ```
   HTTP/1.1 200 OK
   < Server: Apache-Coyote/1.1
   < X-Citrix-Device-State: Non Compliant
   < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   <!--NeedCopy-->
   ```

9. Lorsque l'étape précédente réussit, créez l'action d'authentification Web sur Citrix Endpoint Management. Commencez par créer une expression de stratégie pour extraire l'ID d'appareil du plug-in VPN iOS. Tapez ce qui suit.

   `add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"`

10. Envoyez la requête à Citrix Endpoint Management en tapant ce qui suit. Dans cet exemple, l'adresse IP Citrix Endpoint Management est `10.207.87.82` et le nom de domaine complet est `example.em.cloud.com:4443`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -
serverPort 4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP
/1.1\r\n"+ "Host: example.em.cloud.com:4443\r\n"+ "X-Citrix-VPN-
Device-ID: "+ xm_deviceid_expression + "\r\n\r\n"} -scheme https
 -successRule "HTTP.RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-
Citrix-Device-State\").EQ(\"Compliant\")"
```

L'état `HTTP status 200 OK` indique une réussite de NAC Citrix Endpoint Management. La valeur de l'en-tête `X-Citrix-Device-State` doit être `Compliant`.

11. Créez une stratégie d'authentification avec laquelle associer l'action en tapant ce qui suit.

    ```
    add authentication Policy <policy name> -rule <rule> -action <web
     authentication action>
    ```

    Pa exemple : `add authentication Policy xm_nac_webauth_pol -rule "HTTP .REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac`

12. Convertissez la stratégie LDAP existante en une stratégie avancée en tapant ce qui suit.

    ```
    add authentication Policy <policy_name> -rule <rule> -action <
    LDAP action name>
    ```

    Pa exemple : `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. Ajoutez un intitulé de stratégie avec lequel associer la stratégie LDAP en tapant ce qui suit.

    ```
    add authentication policylabel <policy_label_name>
    ```

    Pa exemple : `add authentication policylabel ldap_pol_label`

14. Associez la stratégie LDAP à l'intitulé de stratégie en tapant ce qui suit.

    ```
    bind authentication policylabel ldap_pol_label -policyName
    ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
    ```

15. Connectez un périphérique compatible pour effectuer un test NAC afin de vérifier si l'authentification LDAP réussit. Tapez ce qui suit.

    ```
    bind authentication vserver <authentication vserver> -policy <web
     authentication policy> -priority 100 -nextFactor <ldap policy
    label> -gotoPriorityExpression END
    ```

16. Ajoutez l'interface utilisateur à associer au serveur virtuel d'authentification. Tapez la commande suivante pour récupérer l'ID d'appareil.

    ```
    add authentication loginSchemaPolicy <schema policy>-rule <rule>
    -action lschema_single_factor_deviceid
    ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

17. Liez le serveur virtuel d'authentification en tapant ce qui suit.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -
priority 100 -gotoPriorityExpression END
```

18. Créez une stratégie d'authentification avancée LDAP pour activer la connexion Citrix Secure Hub. Tapez ce qui suit.

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER
(\"User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP
```

```
bind authentication vserver authvs -policy ldap_xm_test_pol -
priority 110 -gotoPriorityExpression NEXT
```

iOS

November 29, 2023

Pour gérer des appareils iOS dans Citrix Endpoint Management, configurez un certificat Apple Push Notification Service (APNs). Pour de plus amples informations, consultez la section Certificats APNs.

Les profils d'inscription déterminent si les appareils iOS s'inscrivent en mode MDM+MAM, avec la possibilité pour les utilisateurs de se désinscrire de la gestion d'appareils mobiles (MDM). Citrix Endpoint Management prend en charge les types d'authentification suivants pour les appareils iOS en mode MDM+MAM. Pour plus d'informations, consultez les articles suivants :

- Authentification domaine ou domaine + jeton de sécurité
- Authentification certificat client ou certificat + domaine
- Fournisseurs d'identité :
  - Authentification avec Azure Active Directory via Citrix Cloud
  - Authentification avec Okta via Citrix Cloud

> **Exigences pour les certificats de confiance dans iOS 13 :**
>
> Apple a introduit de nouvelles exigences pour les certificats de serveur TLS. Vérifiez que tous les certificats respectent les nouvelles exigences d'Apple. Consultez la publication Apple, https://support.apple.com/en-us/HT210176. Pour obtenir de l'aide sur la gestion des certificats, consultez la section Charger des certificats.

Workflow général pour le démarrage de la gestion des appareils iOS :

1. Effectuez le processus d'intégration. Consultez les sections Intégration et configuration des ressources et Préparation à l'inscription d'appareils et à la mise à disposition de ressources.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Choisissez et configurez une méthode d'inscription. Consultez la section Méthodes d'inscription prises en charge.
3. Configurez les stratégies d'appareil iOS.
4. Inscrivez les appareils iOS.
5. Configurez les actions de sécurité des appareils et des applications. Consultez la section Actions de sécurisation.

Pour les systèmes d'exploitation pris en charge, consultez la section Systèmes d'exploitation d'appareils pris en charge.

Compatibilité iOS 14

Citrix Endpoint Management et les applications mobiles Citrix sont compatibles avec iOS 14, mais ne prennent pas actuellement en charge les nouvelles fonctionnalités iOS 14.

Pour les appareils iOS supervisés, vous pouvez différer les mises à niveau logicielles jusqu'à 90 jours. Dans la stratégie Restrictions pour iOS, utilisez les paramètres suivants :

- **Retarder les mises à jour logicielles**
- **Délai imposé pour les mises à jour logicielles**

Consultez la section Paramètres iOS. Ces paramètres ne sont pas disponibles pour les appareils en mode d'inscription utilisateur ou non supervisé (MDM complet).

Noms d'hôtes Apple qui doivent rester ouverts

Certains noms d'hôtes Apple doivent rester ouverts pour assurer le bon fonctionnement d'iOS, de macOS et de l'Apple App Store. Le blocage de ces noms d'hôtes peut affecter l'installation, la mise à jour et le bon fonctionnement d'iOS, des applications iOS et de MDM et l'inscription des appareils et des applications. Pour plus d'informations, consultez https://support.apple.com/en-us/HT201999.

Méthodes d'inscription prises en charge

Vous spécifiez comment gérer les appareils iOS dans les profils d'inscription. Vous pouvez choisir entre les paramètres d'inscription suivants :

- **Inscription d'utilisateurs Apple :** Pour les appareils BYOD, offre un équilibre de confidentialité pour les données personnelles et de sécurité pour les données d'entreprise. Ce mode d'inscription est disponible en version préliminaire publique. Pour activer cette fonctionnalité, contactez votre équipe de support technique.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Inscription d'appareils Apple :** Pour les appareils iOS supervisés, avec des profils personnels et d'entreprise distincts sur l'appareil.
- **Ne pas gérer les appareils :** Excluez ces appareils de MDM si vous souhaitez uniquement gérer les applications.

Pour de plus amples informations sur la création de profils d'inscription, consultez la section Profils d'inscription.

Citrix Endpoint Management prend en charge les méthodes d'inscription suivantes pour les appareils iOS :

Méthode	Pris en charge
Apple Business Manager	Oui
Apple School Manager	Oui
Apple Configurator	Oui
Inscription manuelle	Oui
Invitations d'inscription	Oui

Les programmes de déploiement Apple incluent Apple Business Manager (ABM) pour les entreprises et Apple School Manager (ASM) pour les établissements d'enseignement. Pour de plus amples informations, consultez la section Déployer des appareils via les programmes de déploiement d'Apple.

Apple School Manager est un type de programme de déploiement Apple Éducation. Consultez la section Intégration avec les fonctionnalités Apple Éducation.

Utilisez les programmes de déploiement d'Apple pour inscrire en bloc des appareils iOS, iPadOS et macOS. Vous pouvez acheter ces appareils directement auprès d'Apple, d'un revendeur agréé Apple ou d'un opérateur. Vous pouvez aussi utiliser Apple Configurator pour inscrire des appareils iOS qu'ils aient été achetés ou non directement auprès d'Apple. Consultez la section Inscription en bloc d'appareils Apple.

Identifiants Apple gérés

L'inscription des utilisateurs intègre étroitement les identifiants Apple gérés. Vous pouvez créer un identifiant Apple géré manuellement à l'aide d'ABM/ASM ou dynamiquement avec Azure Active Directory (AAD).

Pour l'authentification non fédérée, créez des identifiants Apple gérés à l'aide d'ABM/ASM pour ajouter un compte. Pour plus d'informations sur l'ajout d'un compte dans ABM/ASM, consultez

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

la documentation Apple sur `https://support.apple.com/guide/apple-business-manager/welcome/web` et ASM sur `https://support.apple.com/guide/apple-school-manager/welcome/web`. Nous recommandons ce qui suit pour éviter des étapes supplémentaires lorsque les utilisateurs s'inscrivent :

- Utilisez un e-mail correspondant à l'adresse de messagerie d'entreprise lors de la création d'un identifiant Apple géré.
- Définissez le rôle utilisateur sur **Personnel**.
- Demandez aux utilisateurs de modifier manuellement leur mot de passe avant de s'inscrire. Faites savoir aux utilisateurs qu'ils doivent utiliser le même mot de passe que le compte d'entreprise.

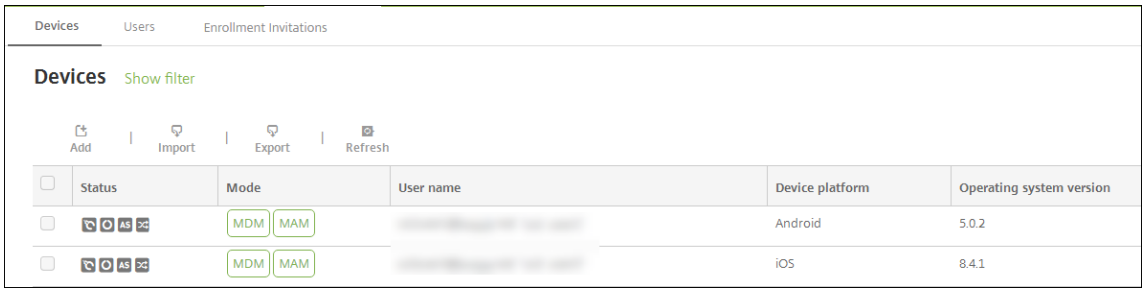
Pour créer dynamiquement des identifiants Apple gérés, configurez Citrix Cloud pour utiliser AAD en tant que fournisseur d'identité. Pour plus d'informations sur la configuration de Citrix Cloud pour utiliser AAD, consultez la section Authentification avec Azure Active Directory via Citrix Cloud. Configurez également l'authentification fédérée dans ABM/ASM. Pour en savoir plus sur la configuration de l'authentification fédérée dans ABM ou ASM, consultez le guide de l'utilisateur Apple Business Manager ou le guide de l'utilisateur Apple School Manager.

Lorsque vous créez manuellement des identifiants Apple gérés, vous pouvez configurer un domaine personnalisé à utiliser à la place du domaine par défaut. Le domaine personnalisé que vous configurez remplace le domaine existant. Par exemple, vos adresses de messagerie d'entreprise suivent le format `first.last@company.com`, mais vous souhaitez utiliser `mycompany.website.com` comme domaine pour l'identifiant Apple géré à la place. Lors de la création de l'identifiant Apple géré sur ABM/ASM, l'adresse e-mail devient `first.last@mycompany.website.com`.

Ajouter un appareil iOS manuellement

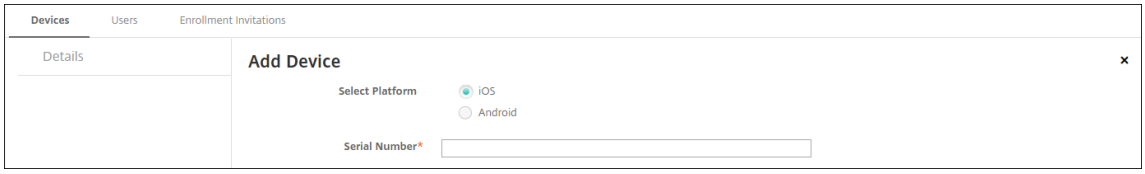
Si vous souhaitez ajouter manuellement un appareil iOS, par exemple à des fins de test, procédez comme suit.

1. Dans la console Citrix Endpoint Management, cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.



2. Cliquez sur **Ajouter**. La page **Ajouter un appareil** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Pour configurer ces paramètres :

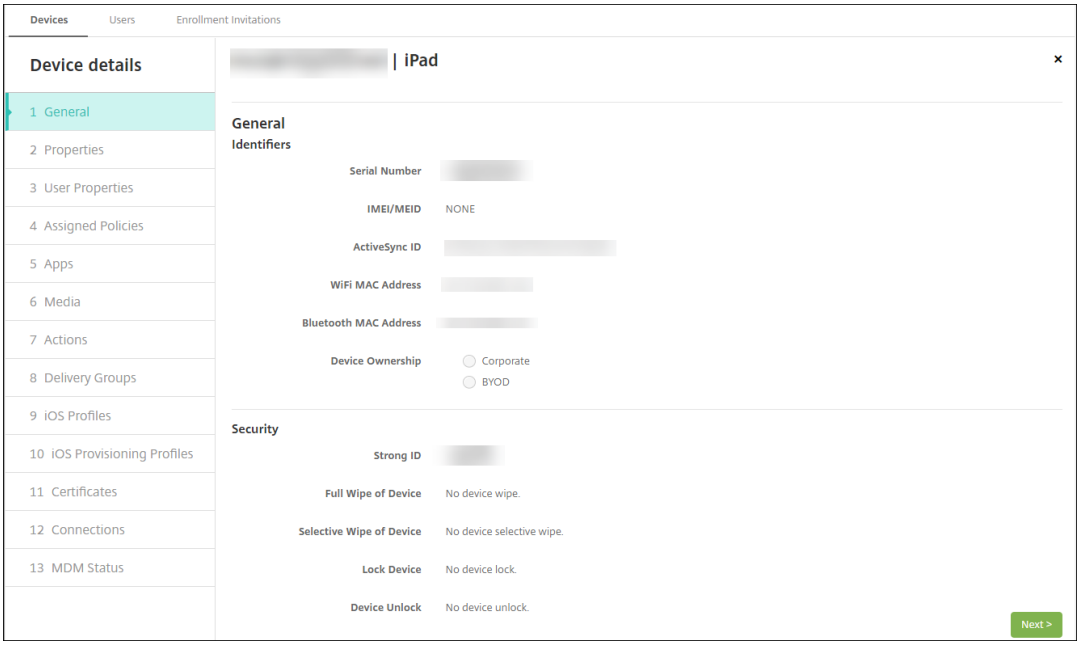
   - **Sélectionner une plate-forme :** cliquez sur **iOS**.
   - **Numéro de série :** entrez le numéro de série de l'appareil.

4. Cliquez sur **Ajouter**. Le tableau **Appareils** s'affiche avec l'appareil ajouté en bas de la liste. Pour afficher et confirmer les détails de l'appareil, sélectionnez l'appareil que vous avez ajouté, puis dans le menu qui s'affiche, cliquez sur **Modifier**.

   > **Remarque :**
   >
   > Lorsque vous sélectionnez la case à cocher en regard d'un appareil, le menu d'options s'affiche au-dessus de la liste des appareils. Lorsque vous cliquez dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

   - LDAP configuré
   - Si vous utilisez des groupes locaux et utilisateurs locaux :
     - Un ou plusieurs groupes locaux.
     - Utilisateurs locaux attribués à des groupes locaux.
     - Des groupes de mise à disposition sont associés à des groupes locaux.
   - Utilisation d'Active Directory :
     - Des groupes de mise à disposition sont associés à des groupes Active Directory.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. La page **Général** dresse la liste des **identificateurs**, tels que le numéro de série et d'autres informations relatives au type de plate-forme. Pour **Propriétaire**, sélectionnez **Entreprise** ou **BYOD**.

   La page **Général** dresse également la liste des propriétés de **sécurité**, telles que ID fort, Verrouiller l'appareil, Contourner le verrouillage d'activation et d'autres informations relatives au type de plate-forme. Le champ **Effacement complet de l'appareil** inclut le code PIN de l'utilisateur. L'utilisateur doit entrer ce code une fois que l'appareil est effacé. Si l'utilisateur oublie le code, vous pouvez le rechercher ici.

6. La page **Propriétés** dresse la liste des propriétés d'appareil qu'Citrix Endpoint Management provisionne. Cette liste affiche toutes les propriétés d'appareil incluses dans le fichier de provisioning utilisé pour ajouter l'appareil. Pour ajouter une propriété, cliquez sur **Ajouter**, puis sélectionnez une propriété dans la liste. Pour connaître les valeurs valides pour chaque propriété, consultez le PDF Valeurs et noms des propriétés d'appareil.

   Lorsque vous ajoutez une propriété, elle s'affiche initialement sous la catégorie dans laquelle vous l'avez ajoutée. Après avoir cliqué sur **Suivant** et être revenu sur la page **Propriétés**, la propriété s'affiche dans la liste appropriée.

   Pour supprimer une propriété, placez le curseur dessus et cliquez sur le **X** sur le côté droit. Citrix Endpoint Management supprime l'élément immédiatement.

7. Les sections **Détails de l'appareil** restantes contiennent des résumés sur l'appareil.

   - **Propriétés utilisateur :** affiche les rôles RBAC, les appartenances aux groupes, les comptes d'achat en volume et les propriétés de l'utilisateur. Vous pouvez retirer un compte d'achat en volume à partir de cette page.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Stratégies attribuées :** affiche le nombre de stratégies déployées, en attente ou ayant échoué. Fournit les informations relatives au nom, au type et à la dernière date de déploiement pour chaque stratégie. Permet de réinitialiser l'état du déploiement sur « En attente » et de redéployer les stratégies supprimées par l'utilisateur.
- **Applications :** affiche, pour le dernier inventaire, le nombre de déploiements d'applications installés, en attente et ayant échoué. Fournit le nom de l'application, l'identificateur, le type et d'autres informations. Pour une description des clés d'inventaire iOS et macOS, telles que **HasUpdateAvailable**, voir Protocole de gestion des appareils mobiles (MDM).
- **Média :** affiche, pour le dernier inventaire, le nombre de déploiements de médias installés, en attente et ayant échoué.
- **Actions :** affiche le nombre d'actions déployées, en attente et qui ont échoué. Fournit le nom de l'action et l'heure du dernier déploiement.
- **Groupes de mise à disposition :** affiche le nombre de groupes de mise à disposition ayant réussi, en attente et qui ont échoué. Pour chaque déploiement, fournit le nom du groupe mise à disposition et l'heure déploiement. Sélectionnez un groupe de mise à disposition pour afficher des informations plus détaillées, y compris l'état, l'action, le canal ou l'utilisateur.
- **Profils iOS :** affiche le dernier inventaire de profil iOS, y compris le nom, le type, l'organisation et une description.
- **Profils de provisioning iOS :** affiche les informations du profil de provisioning de distribution d'entreprise, telles que l'UUID, la date d'expiration, et si les profils sont gérés ou non gérés.
- **Certificats :** affiche pour les certificats valides, révoqués ou ayant expiré, des informations telles que le type, le fournisseur, l'émetteur, le numéro de série et le nombre de jours restants avant l'expiration.
- **Connexions :** affiche l'état de la première connexion et de la dernière connexion. Fournit pour chaque connexion, le nom d'utilisateur, l'heure de l'avant-dernière authentification et l'heure de la dernière authentification.
- **État du MDM :** affiche des informations telles que l'état du MDM, l'heure de la dernière notification push et l'heure de la dernière réponse de l'appareil.

Configurer les stratégies d'appareil iOS

Utilisez ces stratégies pour configurer l'interaction entre Citrix Endpoint Management et les appareils exécutant iOS ou iPadOS. Ce tableau répertorie toutes les stratégies d'appareils disponibles pour les appareils iOS et iPadOS.

| | | |
|—|—|—|
|[Mise en miroir AirPlay](/fr-fr/citrix-endpoint-management/policies/airplay-mirroring-ios-policy.html)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

[AirPrint](/fr-fr/citrix-endpoint-management/policies/airprint-ios-policy.html)	[APN](/fr-fr/citrix-endpoint-management/policies/apn-policy.html#ios-settings)
[Accès aux applications](/fr-fr/citrix-endpoint-management/policies/app-access-policy.html) |[Attributs d'application](/fr-fr/citrix-endpoint-management/policies/app-attributes-policy.html) |[Configuration d'applications](/fr-fr/citrix-endpoint-management/policies/app-configuration-policy.html#ios-settings)
[Inventaire des applications](/fr-fr/citrix-endpoint-management/policies/app-inventory-policy.html) |[Mode kiosque](/fr-fr/citrix-endpoint-management/policies/app-lock-policy.html#ios-settings) |[Désinstallation des applications](/fr-fr/citrix-endpoint-management/policies/app-uninstall-policy.html#ios-and-macos-settings)
[Notifications d'applications](/fr-fr/citrix-endpoint-management/policies/apps-notifications-policy.html) |[Bluetooth](/fr-fr/citrix-endpoint-management/policies/bluetooth-policy.html) |[Calendrier (CalDav)](/fr-fr/citrix-endpoint-management/policies/calendar-caldav-ios-policy.html) |[Cellulaire](/fr-fr/citrix-endpoint-management/policies/cellular-policy.html) |[Contacts (CardDAV)](/fr-fr/citrix-endpoint-management/policies/contacts-carddav-ios-policy.html) |[Informations d'identification](/fr-fr/citrix-endpoint-management/policies/credentials-policy.html#ios-settings) |[Nom de l'appareil](/fr-fr/citrix-endpoint-management/policies/device-name-policy.html) |[Configuration de l'éducation](/fr-fr/citrix-endpoint-management/policies/education-configuration-policy.html) |[Exchange](/fr-fr/citrix-endpoint-management/policies/exchange-policy.html#ios-settings) |[Police](/fr-fr/citrix-endpoint-management/policies/font-policy.html) |[Disposition de l'écran d'accueil](/fr-fr/citrix-endpoint-management/policies/home-screen-layout-policy.html) |[Importer le profil iOS et macOS](/fr-fr/citrix-endpoint-management/policies/import-ios-mac-os-x-profile-policy.html) |[LDAP](/fr-fr/citrix-endpoint-management/policies/ldap-policy.html) |[Emplacement](/fr-fr/citrix-endpoint-management/policies/location-policy.html) |[Message sur l'écran de verrouillage](/fr-fr/citrix-endpoint-management/policies/lock-screen-message-policy.html) |[E-mail](/fr-fr/citrix-endpoint-management/policies/mail-policy.html) |[Domaines gérés](/fr-fr/citrix-endpoint-management/policies/managed-domains-policy.html) |[Nombre maximal d'utilisateurs résidents](/fr-fr/citrix-endpoint-management/policies/maximum-resident-users-policy.html) |[Options MDM](/fr-fr/citrix-endpoint-management/policies/mdm-options-policy.html) |[Réseau](/fr-fr/citrix-endpoint-management/policies/network-policy.html#ios-settings)|[Utilisation du réseau](/fr-fr/citrix-endpoint-management/policies/network-usage-policy.html) |[Info organisation](/fr-fr/citrix-endpoint-management/policies/organization-info-policy.html) |[Mise à jour d'OS](/fr-fr/citrix-endpoint-management/policies/control-os-updates.html#ios-settings) |[Code secret](/fr-fr/citrix-endpoint-management/policies/passcode-policy.html#ios-settings) |[Période de grâce de verrouillage par code secret](/fr-fr/citrix-endpoint-management/policies/passcode-lock-grace-period.html) |[Partage de connexion](/fr-fr/citrix-endpoint-management/policies/personal-hotspot-policy.html) |[Suppression de profils](/fr-fr/citrix-endpoint-management/policies/profile-removal-policy.html)

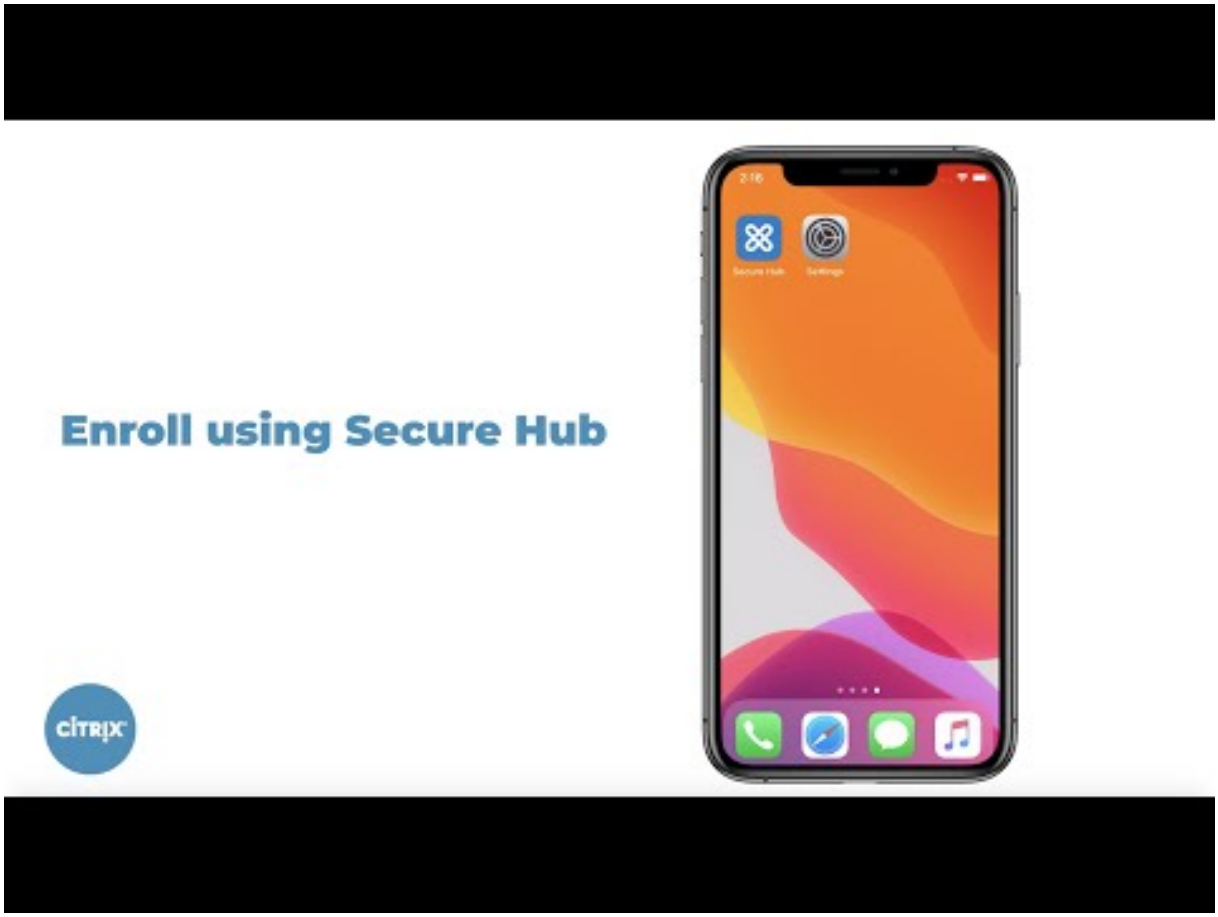
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

|[Profil de provisioning](/fr-fr/citrix-endpoint-management/policies/provisioning-profile-policy.html) |[Suppression du profil de provisioning](/fr-fr/citrix-endpoint-management/policies/provisioning-profile-removal-policy.html) |[Proxy](/fr-fr/citrix-endpoint-management/policies/proxy-policy.html) |[Restrictions](/fr-fr/citrix-endpoint-management/policies/restrictions-policy.html#ios-settings) |[Itinérance](/fr-fr/citrix-endpoint-management/policies/roaming-policy.html) |[SCEP](/fr-fr/citrix-endpoint-management/policies/scep-policy.html) |[Compte SSO](/fr-fr/citrix-endpoint-management/policies/sso-account-policy.html) |[Magasin](/fr-fr/citrix-endpoint-management/policies/store-policy.html) |[Abonnements calendriers](/fr-fr/citrix-endpoint-management/policies/subscribed-calendars-policy.html) |[Termes et conditions](/fr-fr/citrix-endpoint-management/policies/terms-and-conditions-policy.html) |[VPN](/fr-fr/citrix-endpoint-management/policies/vpn-policy.html#ios-settings) |[Fond d'écran](/fr-fr/citrix-endpoint-management/policies/wallpaper-policy.html) |Filtre de contenu Web |Clip Web | | |

Inscrire des appareils iOS

Cette section explique comment les utilisateurs inscrivent des appareils iOS (12.2 ou version ultérieure) dans Citrix Endpoint Management. Pour plus d'informations sur l'inscription iOS, regardez la vidéo suivante :

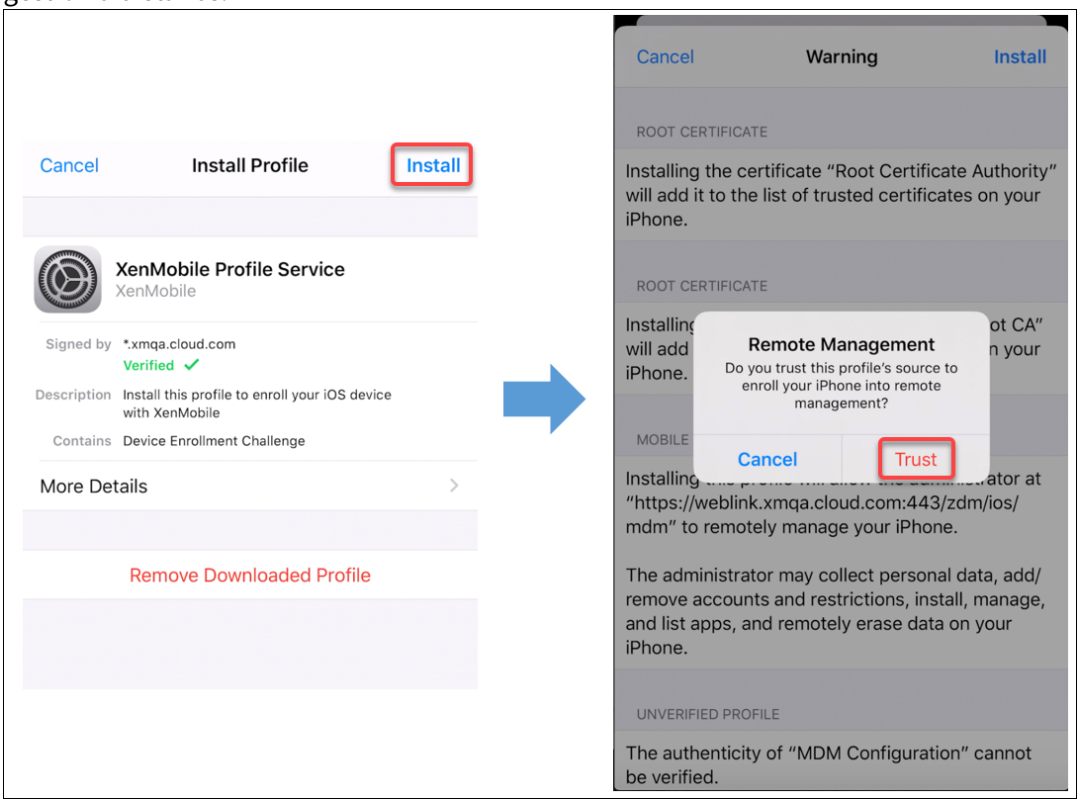
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. Accédez à l'Apple Store sur votre appareil iOS, téléchargez l'application Citrix Secure Hub, puis touchez l'application.
2. Lorsque vous êtes invité à installer l'application, touchez **Suivant**, puis **Installer**.
3. Après l'installation de Citrix Secure Hub, touchez **Ouvrir**.
4. Entrez vos informations d'identification d'entreprise, telles que le nom de votre serveur Citrix Endpoint Management, le nom d'utilisateur principal (UPN), ou votre adresse e-mail. Cliquez ensuite sur **Suivant**.
5. Touchez **Oui, inscrire** pour inscrire votre appareil iOS.
6. Une liste des données collectées par Citrix Endpoint Management s'affiche. Cliquez sur **Suivant**. Une explication de la façon dont une organisation utilise ces données apparaît. Cliquez sur **Suivant**.
7. Après avoir tapé vos informations d'identification, appuyez sur **Autoriser** lorsque vous y êtes invité, pour télécharger le profil de configuration. Après avoir téléchargé le profil de configuration, appuyez sur **Fermer**.
8. Dans les paramètres de votre appareil, installez le profil XenMobile.
   - Accédez à **Paramètres > Général > Profil > XenMobile Profile Service** et touchez **Installer** pour ajouter le profil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Dans la fenêtre de notification, touchez **Faire confiance** pour inscrire votre appareil à la gestion à distance.



9. Une fois l'inscription réussie, ouvrez Citrix Secure Hub. Si vous vous inscrivez à MDM+MAM : une fois vos informations d'identification validées, créez et confirmez votre code PIN Citrix lorsque vous y êtes invité.
10. Une fois le workflow terminé, l'appareil est inscrit. Vous pouvez ensuite accéder au magasin d'applications pour afficher les applications que vous pouvez installer sur votre appareil iOS.

Actions de sécurisation

L'inscription d'appareils pour iOS prend en charge les actions de sécurisation suivantes. Pour obtenir une description de chaque action, consultez la section Actions de sécurisation.

- Contourner le verrouillage d'activation
- Mode kiosque
- Effacement des applications
- Verrouillage d'activation ASM
- Renouvellement de certificat
- Effacer les restrictions
- Activer/Désactiver le mode perdu
- Activer/Désactiver le suivi

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Effacer
- Localiser
- Verrouiller
- Faire sonner
- Demander/Arrêter la mise en miroir AirPlay
- Redémarrer/Arrêter
- Révoquer/Autoriser
- Effacer les données d'entreprise
- Déverrouiller

L'inscription d'utilisateurs pour iOS prend en charge les actions de sécurisation suivantes :

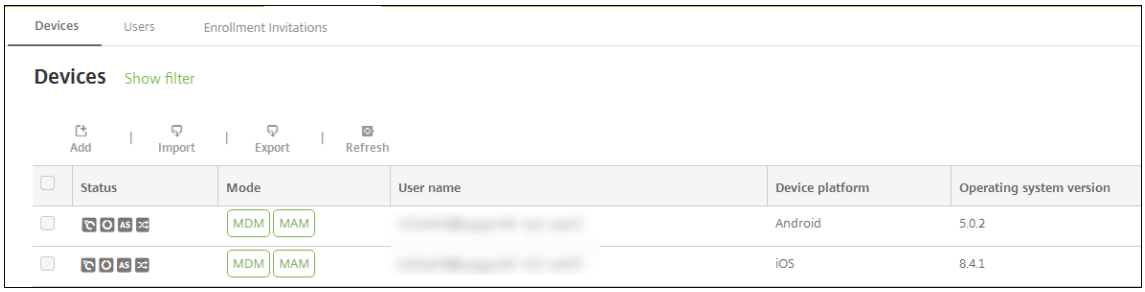
- Révoquer
- Verrouiller
- Effacer les données d'entreprise
- Renouvellement de certificat

Verrouiller les appareils iOS

Vous pouvez verrouiller un appareil iOS perdu tout en affichant un message et un numéro de téléphone sur l'écran de verrouillage.

Pour afficher un message et un numéro de téléphone sur un appareil verrouillé, définissez la stratégie Code secret sur **true** dans la console Citrix Endpoint Management. Ou bien les utilisateurs peuvent activer le code secret sur l'appareil manuellement.

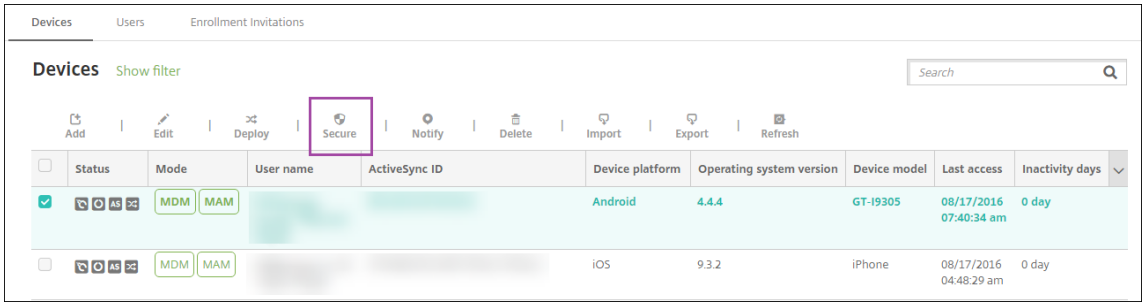
1. Cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.

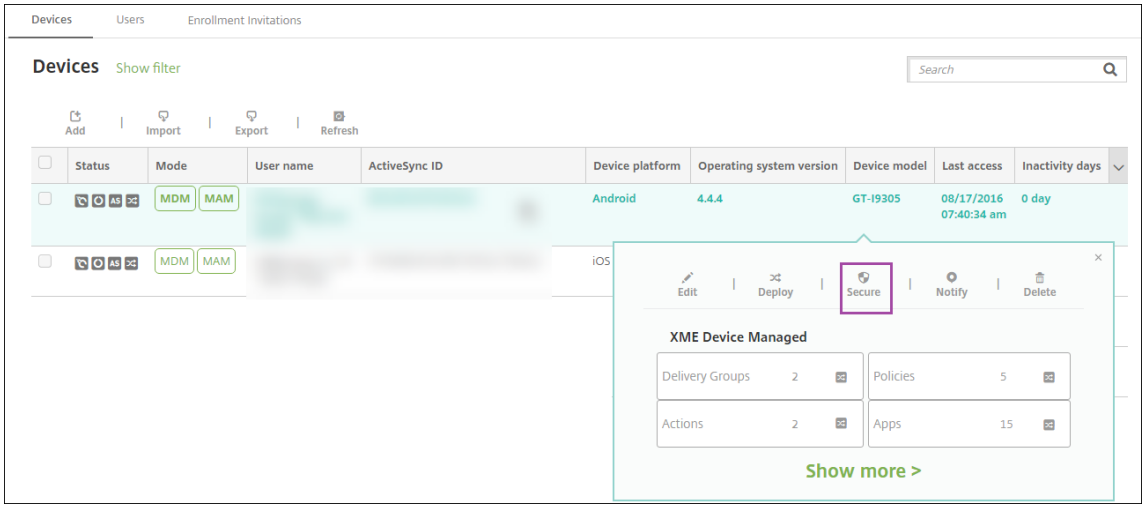


2. Sélectionnez l'appareil iOS que vous voulez verrouiller.

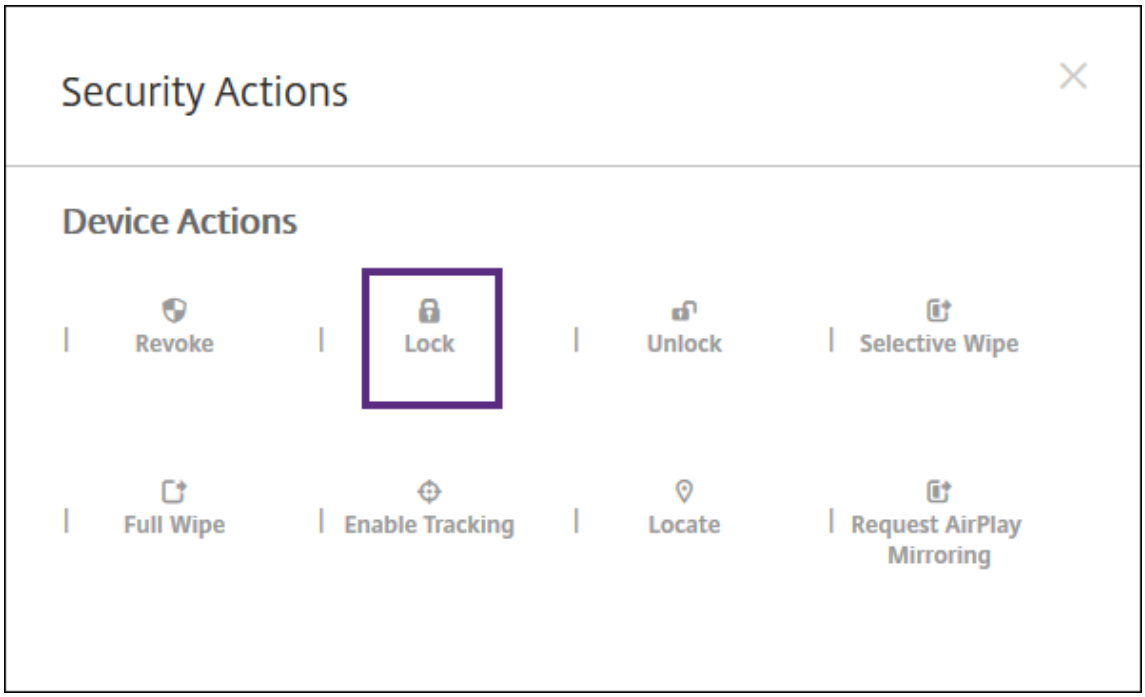
   Sélectionnez la case à cocher en regard d'un appareil pour afficher le menu d'options au-dessus de la liste des appareils. Cliquez dans la liste pour afficher le menu d'options sur le côté droit de la liste.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



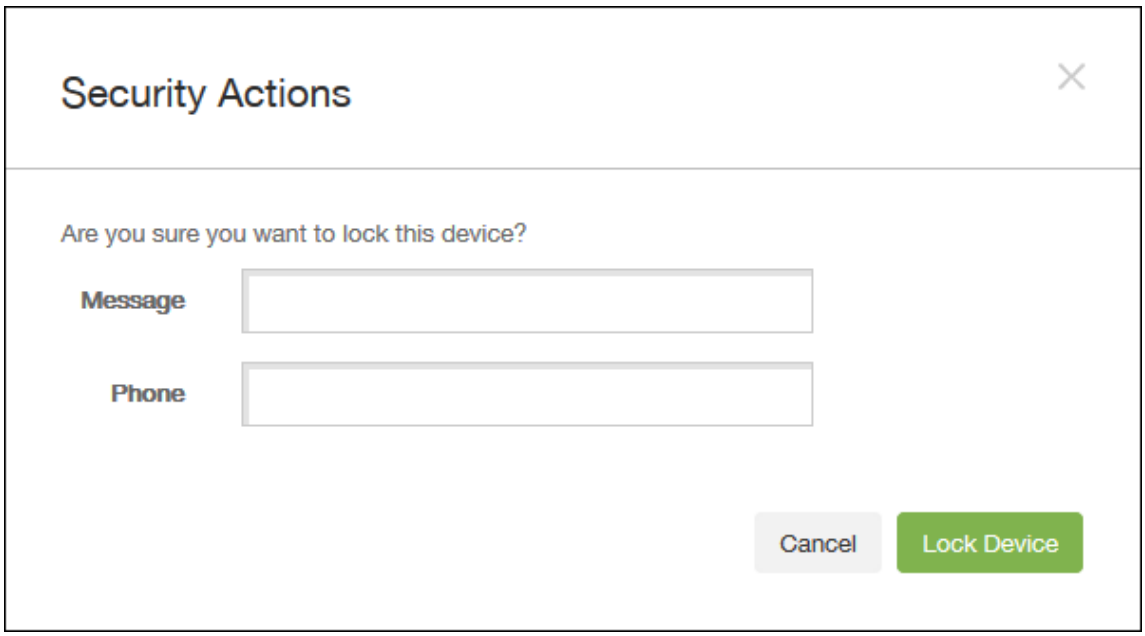


3. Dans le menu d'options, sélectionnez **Sécurité**. La boîte de dialogue **Actions de sécurisation** s'affiche.



4. Cliquez sur **Verrouiller**. La boîte de dialogue **Actions de sécurisation** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Si vous le souhaitez, entrez un message et un numéro de téléphone qui s'afficheront sur l'écran de verrouillage de l'appareil.

   iOS ajoute les mots « iPad perdu » au texte entré dans le champ **Message**.

   Si vous laissez le champ **Message** vide et que vous entrez un numéro de téléphone, Apple affiche le message « Appeler propriétaire » sur l'écran de verrouillage de l'appareil.

6. Cliquez sur **Verrouiller l'appareil**.

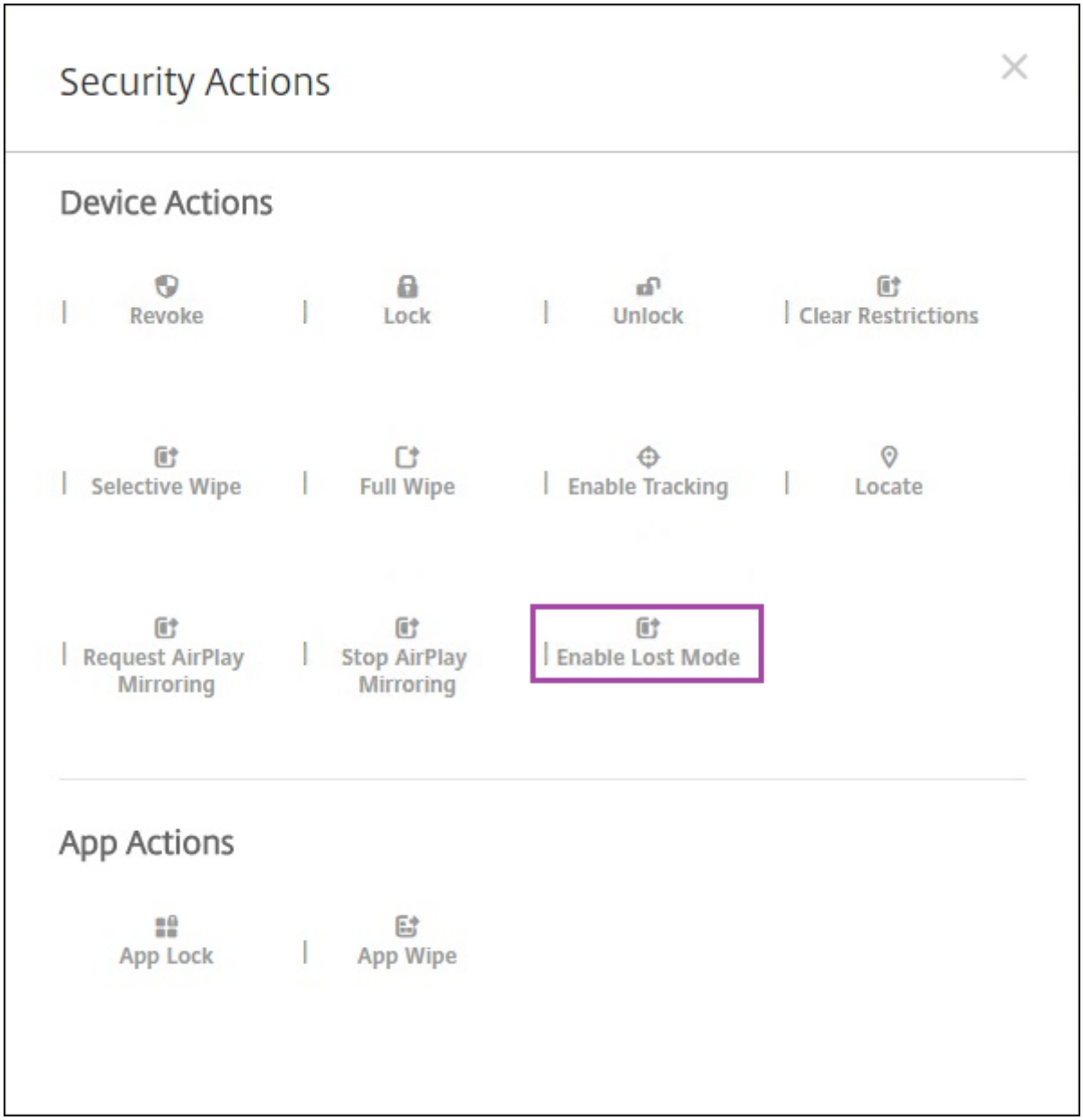
Placer les appareils iOS en Mode perdu

La propriété d'appareil Mode perdu d'Citrix Endpoint Management place un appareil iOS en Mode perdu. Contrairement au mode perdu géré d'Apple, le mode perdu de Citrix Endpoint Management ne nécessite pas qu'un utilisateur effectue une des actions suivantes pour activer la recherche de son appareil : configurer le paramètre **Localiser mon iPhone/iPad** ou activer les Services de géolocalisation pour Citrix Secure Hub.

Dans le Mode perdu d'Citrix Endpoint Management, seul Citrix Endpoint Management peut déverrouiller l'appareil. (En revanche, si vous utilisez la fonctionnalité de verrouillage d'appareil d'Citrix Endpoint Management, les utilisateurs peuvent déverrouiller l'appareil directement à l'aide d'un code PIN que vous devez fournir.

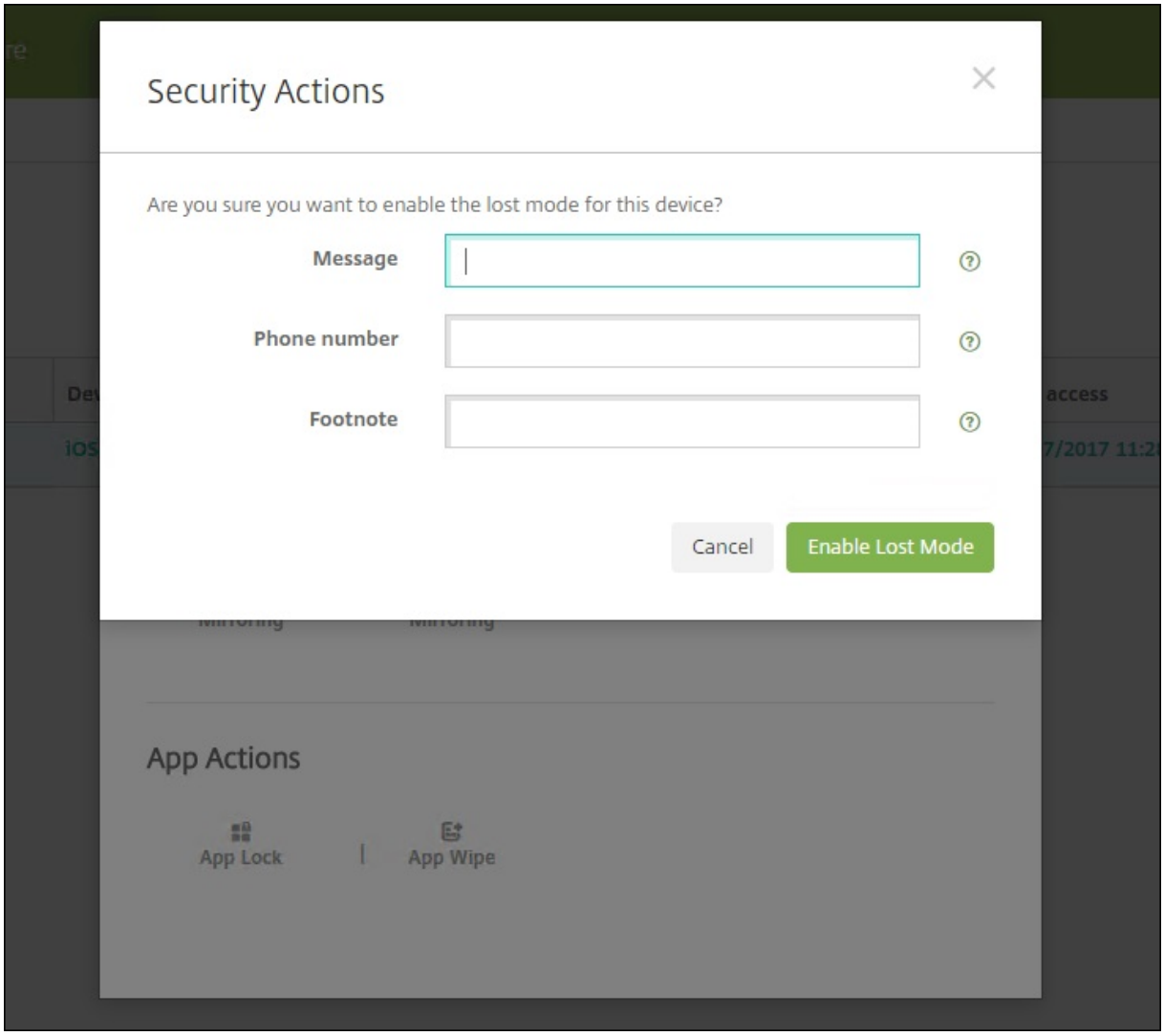
Pour activer ou désactiver le Mode perdu : accédez à **Gérer > Appareils**, choisissez un appareil iOS supervisé et cliquez sur **Sécurisé**. Ensuite, cliquez sur **Activer le mode perdu** ou **Désactiver le mode perdu**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Si vous cliquez sur **Activer le mode perdu**, entrez les informations qui sont affichées sur l'appareil lorsqu'il est en mode perdu.

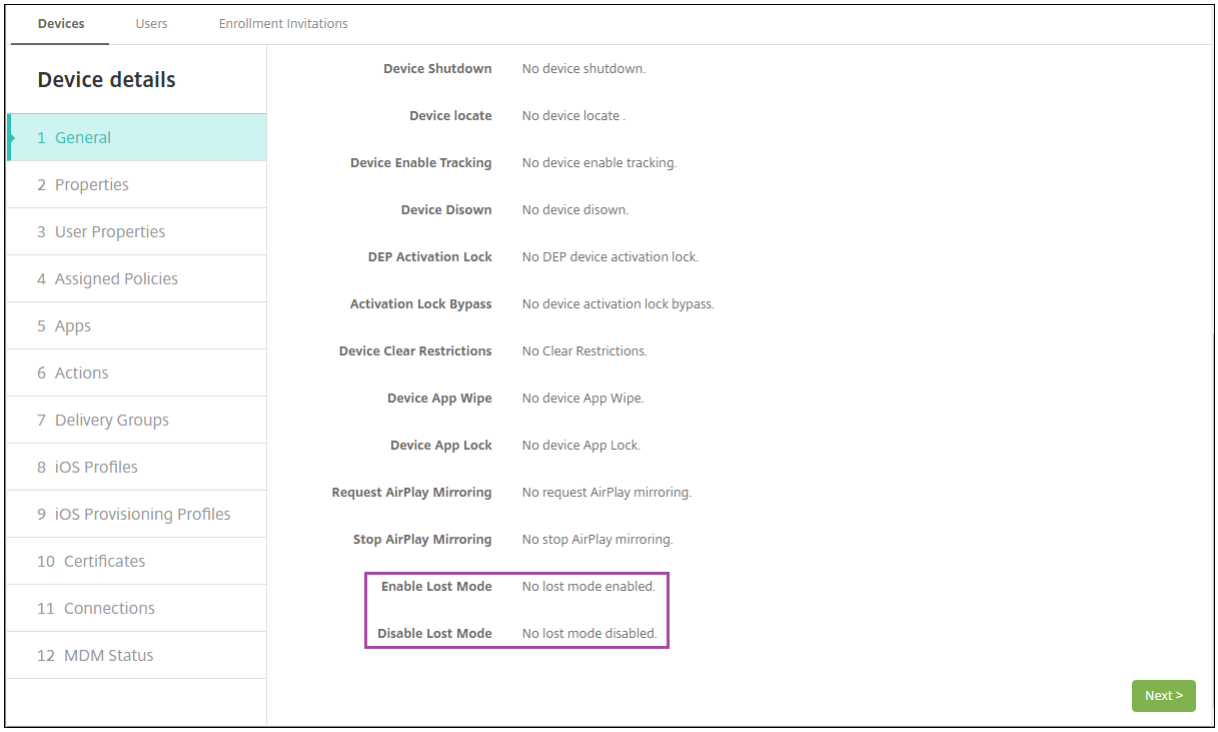
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



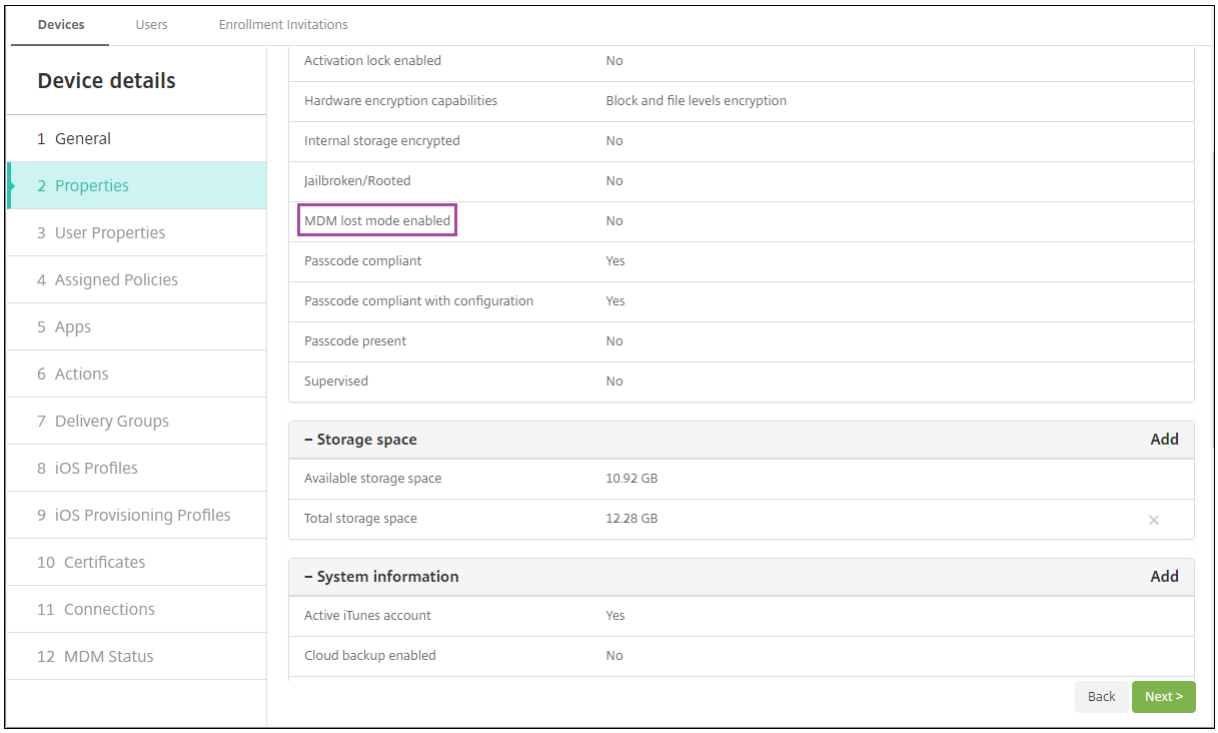
Pour vérifier l'état du mode perdu, utilisez une des méthodes suivantes :

- Dans la fenêtre **Actions de sécurisation**, vérifiez si le bouton indique **Désactiver le mode perdu**.
- Dans **Gérer > Appareils**, dans l'onglet **Général** sous **Sécurité**, consultez la dernière action Activer le mode perdu ou Désactiver le mode perdu.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Dans **Gérer > Appareils**, dans l'onglet **Propriétés**, vérifiez que la valeur du paramètre **Mode perdu MDM activé** est correcte.



Si vous activez le mode perdu de Citrix Endpoint Management sur un appareil iOS, la console Citrix Endpoint Management est également modifiée comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Dans **Configurer > Actions**, la liste **Actions** ne comprend pas ces actions automatiques : **Révoquer l'appareil**, **Effacer les données d'entreprise de l'appareil** et **Effacer toutes les données de l'appareil**.
- Dans **Gérer > Appareils**, la liste **Actions de sécurisation** n'inclut plus les actions **Révoquer** et **Effacer les données d'entreprise**. Vous pouvez toujours utiliser une action de sécurité pour effectuer une action **Effacement complet**, si nécessaire.

iOS ajoute les mots « iPad perdu » au texte entré dans **Message** dans l'écran **Actions de sécurisation**.

Si vous laissez **Message** vide et que vous entrez un numéro de téléphone, Apple affiche le message « Appeler propriétaire » sur l'écran de verrouillage de l'appareil.

Contourner un verrouillage d'activation iOS

Le verrouillage d'activation est une fonctionnalité de Localiser mon iPhone/iPad qui empêche la réactivation d'un appareil supervisé perdu ou volé. Le verrouillage d'activation requiert l'identifiant Apple et le mot de passe de l'utilisateur pour pouvoir effectuer ces actions : désactiver Localiser mon iPhone/iPad, effacer l'appareil ou réactiver l'appareil. Pour les appareils qui sont la propriété de votre organisation, il est nécessaire de contourner le verrouillage d'activation pour, par exemple, réinitialiser ou réattribuer des appareils.

Pour activer le verrouillage d'activation, configurez et déployez la stratégie Options MDM d'Citrix Endpoint Management. Vous pouvez ensuite gérer un appareil à partir de la console Citrix Endpoint Management sans les informations d'identification Apple de l'utilisateur. Pour contourner l'obligation d' entrer des informations d'identification Apple avec un verrou d'activation, émettez l'action de sécurisation Contourner le verrouillage d'activation depuis la console Citrix Endpoint Management.

Par exemple, si l'utilisateur retourne un téléphone perdu ou pour configurer l'appareil avant ou après un effacement complet : lorsque le téléphone invite à entrer les informations d'identification de compte Apple App Store, ignorez cette étape en émettant l'action de sécurité Contourner le verrouillage d'activation.

Configuration requise pour le contournement du verrouillage d'activation

- Supervisé par Apple Configurator ou le programme de déploiement Apple
- Configuré avec un compte iCloud
- Localiser mon iPhone/iPad activé
- Inscrit dans Citrix Endpoint Management
- Stratégie Options MDM, avec verrouillage d'activation activé, déployée sur les appareils

Pour contourner le verrouillage d'activation avant d'émettre un effacement complet de l'appareil :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Sécurisé**, puis cliquez sur **Contourner le verrouillage d'activation**.
2. Effacez l'appareil. L'écran de verrouillage d'activation ne s'affiche pas lors de l'installation de l'appareil.

Pour contourner le verrouillage d'activation après avoir émis un effacement complet de l'appareil :

1. Réinitialisez ou effacez l'appareil. L'écran de verrouillage d'activation s'affiche lors de l'installation de l'appareil.
2. Accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Sécurisé**, puis cliquez sur **Contourner le verrouillage d'activation**.
3. Cliquez sur le bouton Retour sur l'appareil. L'écran d'accueil s'affiche.

Gardez à l'esprit les considérations suivantes :

- Conseillez à vos utilisateurs de ne pas désactiver Localiser mon iPhone/iPad. N'effectuez pas d'effacement complet à partir de l'appareil. Dans ces deux cas, l'utilisateur est invité à entrer le mot de passe du compte iCloud. Après la validation du compte, l'utilisateur ne verra pas d'écran Activer iPhone/iPad après avoir effacé tout le contenu et les paramètres.
- Pour un appareil avec un code de contournement de verrouillage d'activation généré et avec le verrouillage d'activation activé : si vous ne pouvez pas contourner la page Activer iPhone/iPad après un effacement complet, il n'est pas nécessaire de supprimer l'appareil de Citrix Endpoint Management. Vous ou l'utilisateur pouvez contacter l'assistance Apple pour débloquer l'appareil directement.
- Lors d'un inventaire matériel, Citrix Endpoint Management interroge un appareil pour obtenir un code de contournement de verrouillage d'activation. Si un code de contournement est disponible, l'appareil l'envoie à Citrix Endpoint Management. Ensuite, pour supprimer le code de contournement de l'appareil, envoyez l'action de sécurisation Contourner le verrouillage d'activation à partir de la console Citrix Endpoint Management. À ce stade, Citrix Endpoint Management et Apple ont le code de contournement nécessaire pour débloquer l'appareil.
- L'action de sécurisation Contourner le verrouillage d'activation repose sur la disponibilité d'un service d'Apple. Si l'action ne fonctionne pas, vous pouvez débloquer un appareil de l'une des manières suivantes :
  - Sur l'appareil, entrez manuellement les informations d'identification du compte iCloud.
  - Laissez le champ de nom d'utilisateur vide et tapez le code de contournement dans le champ de mot de passe. Pour rechercher le code de contournement, accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Modifier** et cliquez sur **Propriétés**. Le **Code de contournement du verrouillage d'activation** se trouve sous **Informations de sécurité**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

macOS

November 29, 2023

Pour gérer des appareils macOS dans Citrix Endpoint Management, configurez un certificat Apple Push Notification Service (APNs). Pour de plus amples informations, consultez la section Certificats APNs.

Citrix Endpoint Management inscrit les appareils macOS en mode MDM. Citrix Endpoint Management prend en charge les types d'authentification d'inscription suivants pour les appareils macOS en mode MDM.

- Domaine
- Domaine + mot de passe unique
- URL d'invitation + mot de passe unique

> **Exigences pour les certificats de confiance dans macOS 15 :**
>
> Apple a introduit de nouvelles exigences pour les certificats de serveur TLS. Vérifiez que tous les certificats respectent les nouvelles exigences d'Apple. Consultez la publication Apple, https://support.apple.com/en-us/HT210176. Pour obtenir de l'aide sur la gestion des certificats, consultez la section Charger des certificats.

Workflow général pour le démarrage de la gestion des appareils macOS :

1. Effectuez le processus d'intégration. Consultez les sections Intégration et configuration des ressources et Préparation à l'inscription d'appareils et à la mise à disposition de ressources.
2. Choisissez et configurez une méthode d'inscription. Consultez la section Méthodes d'inscription prises en charge.
3. Configurez les stratégies macOS.
4. Inscrivez les appareils macOS.
5. Configurez les actions de sécurité des appareils et des applications. Consultez la section Actions de sécurisation.

Pour les systèmes d'exploitation pris en charge, consultez la section Systèmes d'exploitation d'appareils pris en charge.

Noms d'hôtes Apple qui doivent rester ouverts

Certains noms d'hôtes Apple doivent rester ouverts pour assurer le bon fonctionnement d'iOS, de macOS et de l'Apple App Store. Le blocage de ces noms d'hôtes peut affecter l'installation, la mise

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

à jour et le bon fonctionnement d'iOS, des applications iOS et de MDM et l'inscription des appareils et des applications. Pour plus d'informations, consultez https://support.apple.com/en-us/HT201999.

Méthodes d'inscription prises en charge

Le tableau suivant indique les méthodes d'inscription prises en charge par Citrix Endpoint Management pour les appareils macOS :

Méthode	Pris en charge
Programmes de déploiement d'Apple	Oui
Apple School Manager	Oui
Apple Configurator	Non
Inscription manuelle	Oui
Invitations d'inscription	Oui

Apple propose des programmes d'inscription d'appareil pour les comptes d'entreprise et éducation. Pour les comptes d'entreprise, vous devez vous inscrire au programme de déploiement d'Apple pour utiliser ce programme pour inscrire et gérer des appareils dans Citrix Endpoint Management. Ce programme est destiné aux appareils iOS, macOS et Apple TV. Voir Déployer des appareils via le programme de déploiement d'Apple.

Pour les comptes éducation, vous devez créer un compte Apple School Manager. Apple School Manager unifie le programme de déploiement et l'achat en volume. Apple School Manager est un type de programme de déploiement Apple Éducation. Consultez la section Intégration avec les fonctionnalités Apple Éducation.

Vous pouvez utiliser le programme de déploiement d'Apple pour inscrire en bloc des appareils iOS, macOS et Apple TV. Vous pouvez acheter ces appareils directement auprès d'Apple, d'un revendeur agréé Apple ou d'un opérateur.

Configurer les stratégies macOS

Utilisez ces stratégies pour configurer l'interaction entre Citrix Endpoint Management et les appareils exécutant macOS. Ce tableau répertorie toutes les stratégies d'appareils disponibles pour les appareils macOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Mise en miroir AirPlay	Inventaire des applications	Désinstallation des applications
Calendrier (CalDav)	Contacts (CardDAV)	Informations d'identification
Nom de l'appareil	Exchange	FileVault
Pare-feu	Police	Importer le profil iOS et macOS
LDAP	E-mail	Réseau
Mise à jour d'OS	Code secret	Suppression de profils
Restrictions	SCEP	VPN
Clips Web		

Inscrire les appareils macOS

Citrix Endpoint Management propose deux méthodes pour inscrire des appareils qui exécutent macOS. Les deux méthodes permettent aux utilisateurs macOS de s'inscrire sans fil (OTA) directement depuis leurs appareils.

- **Envoyer une invitation d'inscription aux utilisateurs :** cette méthode d'inscription vous permet de définir un des modes d'inscription sécurisée suivants pour les appareils macOS :

  - Nom d'utilisateur + mot de passe
  - Nom d'utilisateur + Code PIN
  - Authentification à deux facteurs

  Lorsque l'utilisateur suit les instructions de l'invitation d'inscription, un écran de connexion avec le nom d'utilisateur déjà renseigné s'affiche.

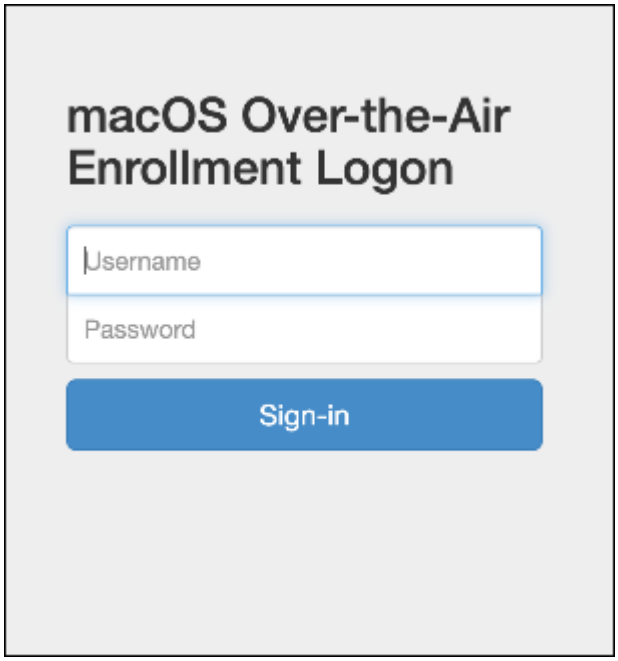
- **Envoyer un lien d'inscription aux utilisateurs :** cette méthode d'inscription pour les appareils macOS envoie aux utilisateurs un lien d'inscription qu'ils peuvent ouvrir dans les navigateurs Safari et Chrome. Ensuite, un utilisateur s'inscrit en fournissant son nom d'utilisateur et son mot de passe.

  Pour empêcher l'utilisation d'un lien d'inscription pour les appareils macOS, définissez la propriété de serveur **Activer macOS OTAE** sur **false**. Les utilisateurs macOS peuvent alors s'inscrire uniquement à l'aide d'une invitation d'inscription.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Envoyer une invitation d'inscription aux utilisateurs macOS

1. Ajoutez une invitation pour l'inscription d'utilisateurs macOS. Reportez-vous à la section Invitations d'inscription.
2. Une fois que les utilisateurs reçoivent l'invitation et cliquent sur le lien, l'écran suivant s'affiche dans le navigateur Safari. Citrix Endpoint Management remplit le nom d'utilisateur. Si vous avez choisi **Deux facteurs** pour le mode d'inscription sécurisée, un champ supplémentaire s'affiche.



3. Les utilisateurs installent les certificats, selon les besoins. Les utilisateurs sont invités à installer des certificats si vous avez configuré pour macOS un certificat SSL approuvé publiquement et un certificat de signature numérique approuvé publiquement. Pour de plus amples informations sur les certificats, consultez la section Certificats et authentification.
4. Les utilisateurs entrent les informations d'identification demandées.

   Les stratégies Mac s'installent. Vous pouvez maintenant démarrer la gestion des appareils macOS avec Citrix Endpoint Management tout comme vous gérez les appareils mobiles.

Envoyer un lien d'installation aux utilisateurs macOS

1. Envoyez le lien d'inscription `https://serverFQDN:8443/instanceName/macos/otae` que les utilisateurs peuvent ouvrir dans les navigateurs Safari ou Chrome.
   - **serverFQDN** est le nom de domaine complet du serveur exécutant Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Le port **8443** est le port sécurisé par défaut. Si vous avez configuré un port différent, utilisez-le à la place de 8443.
- Le **nom d'instance**, souvent affiché sous la forme `zdm`, est le nom spécifié lors de l'installation du serveur.

Pour de plus amples informations sur l'envoi des liens d'installation, consultez la section Pour envoyer un lien d'installation.

2. Les utilisateurs installent les certificats, selon les besoins. Si vous avez configuré un certificat SSL et un certificat de signature numérique approuvé publiquement pour iOS et macOS, les utilisateurs sont invités à installer les certificats. Pour de plus amples informations sur les certificats, consultez la section Certificats et authentification.
3. Les utilisateurs se connectent à leur Mac.

   Les stratégies Mac s'installent. Vous pouvez maintenant démarrer la gestion des appareils macOS avec Citrix Endpoint Management tout comme vous gérez les appareils mobiles.

Actions de sécurisation

macOS prend en charge les actions de sécurisation suivantes. Pour obtenir une description de chaque action, consultez la section Actions de sécurisation.

Révoquer	Verrouiller	Effacer les données d'entreprise
Effacer	Renouvellement de certificat	Alterner clé de récupération privée

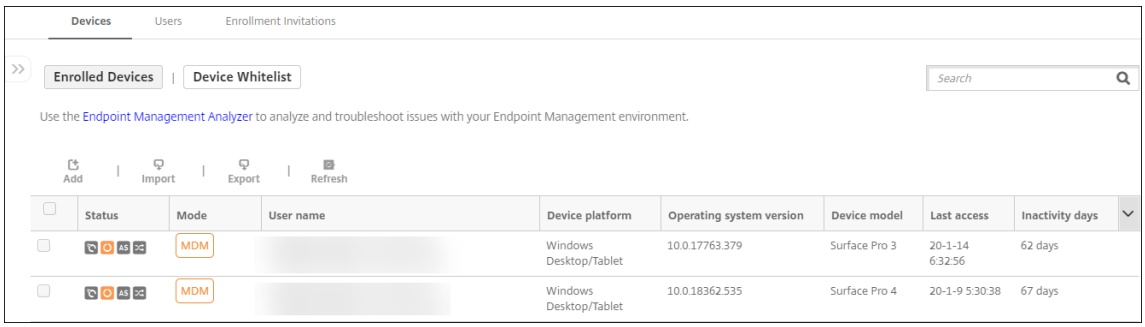
Verrouiller les appareils macOS

Vous pouvez verrouiller à distance un appareil macOS perdu. Citrix Endpoint Management verrouille l'appareil. Ensuite, il génère un code PIN et le configure dans l'appareil. Pour accéder à l'appareil, l'utilisateur devra entrer ce code PIN. Utilisez **Annuler le verrouillage** pour retirer le verrouillage de la console Citrix Endpoint Management.

Vous pouvez utiliser la stratégie Code secret pour configurer d'autres paramètres associés au code PIN. Pour plus d'informations, consultez les paramètres macOS.

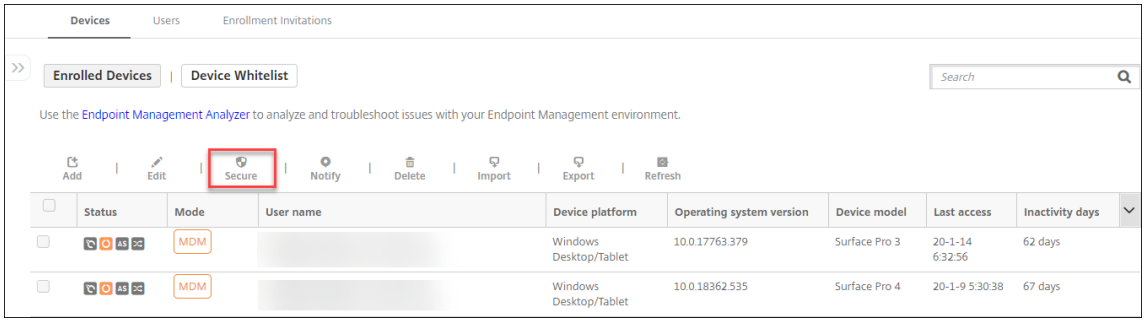
1. Cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.

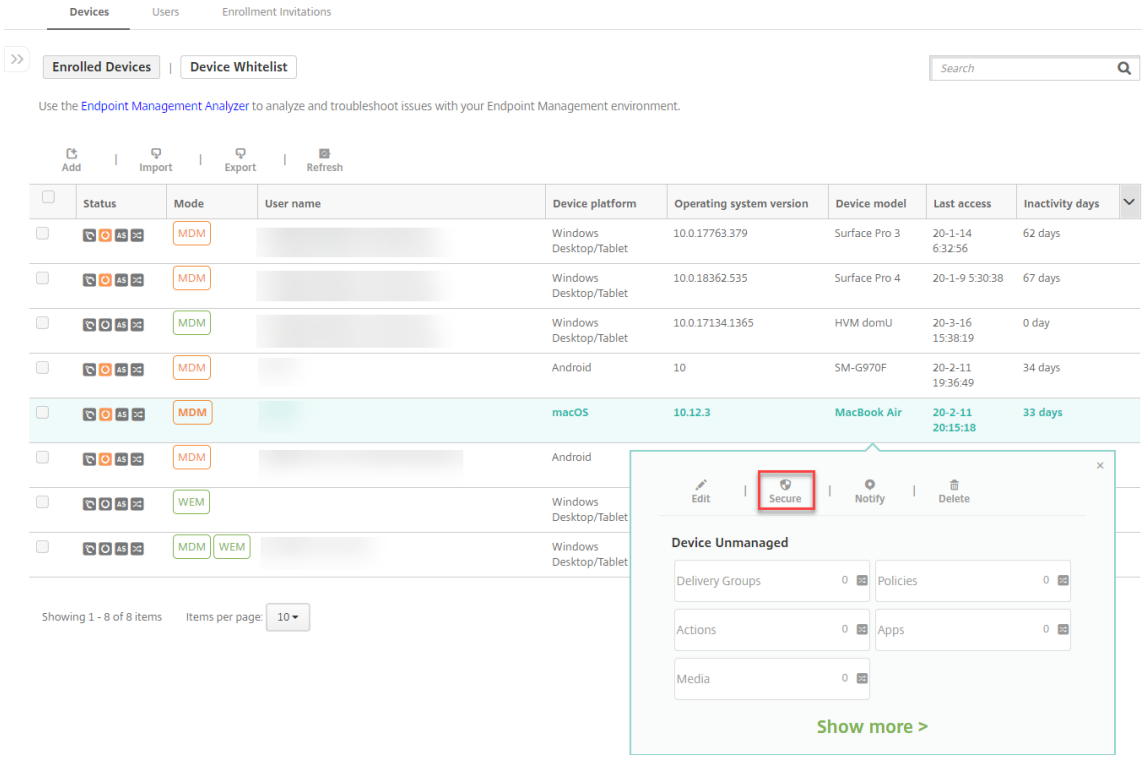
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Sélectionnez l'appareil macOS que vous voulez verrouiller.

   Sélectionnez la case à cocher en regard d'un appareil pour afficher le menu d'options au-dessus de la liste des appareils. Vous pouvez également cliquer sur un élément répertorié pour afficher le menu des options sur le côté droit de la liste.

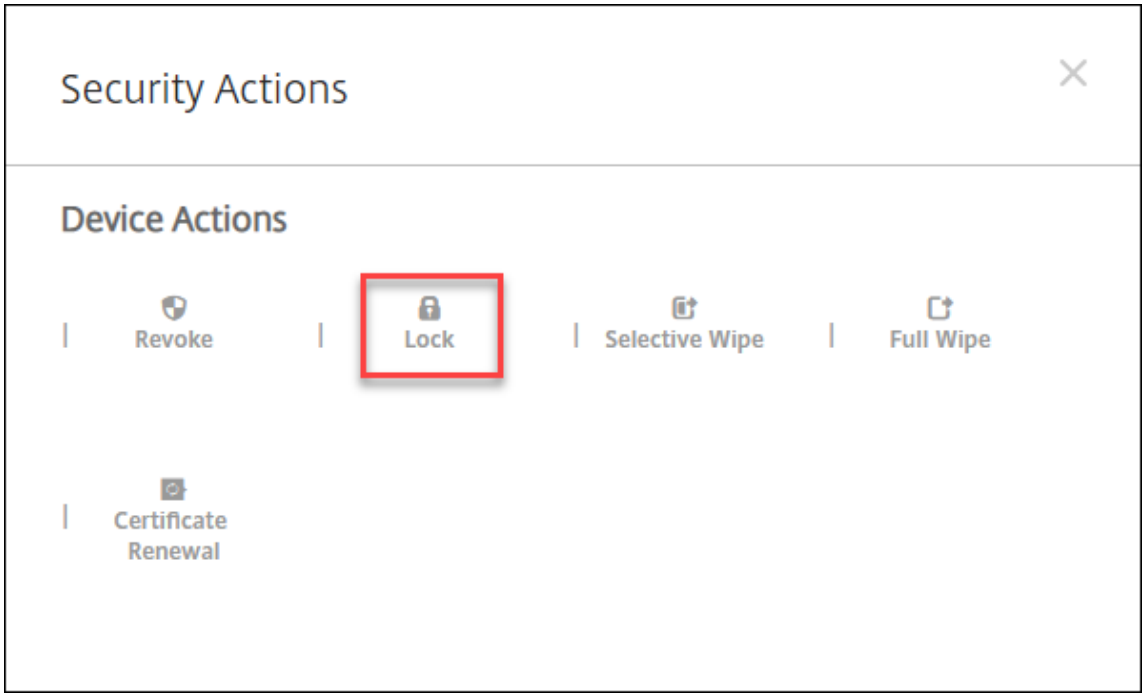




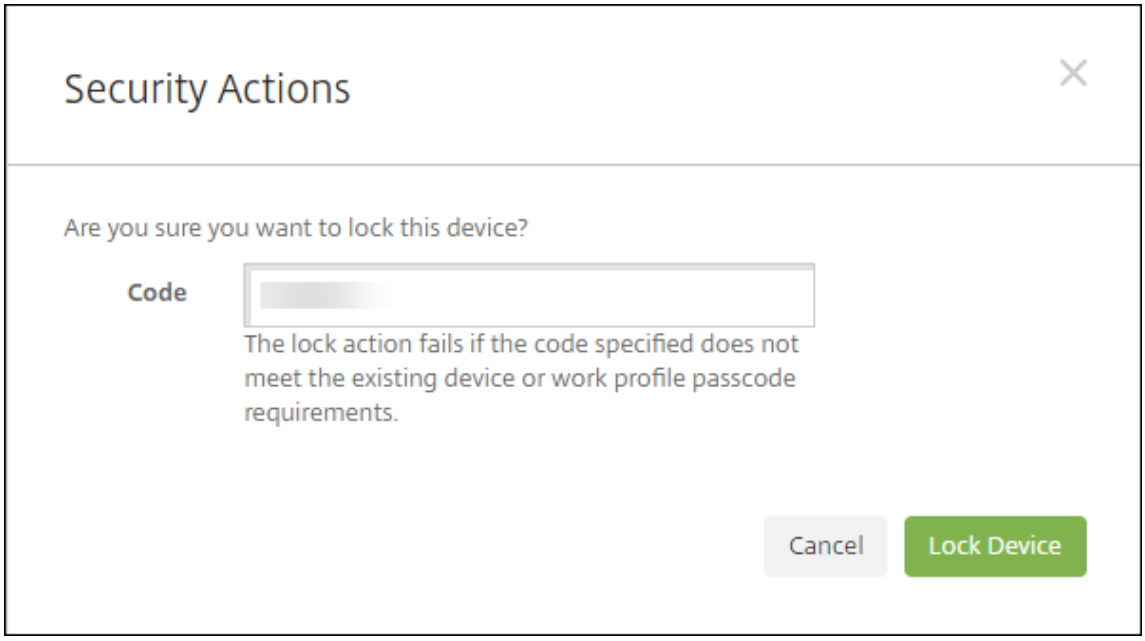
3. Dans le menu d'options, sélectionnez **Sécurité**. La boîte de dialogue **Actions de sécurisation**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

s'affiche.



4. Cliquez sur **Verrouiller**. La boîte de dialogue **Actions de sécurisation** s'affiche.



5. Cliquez sur **Verrouiller l'appareil**.

> **Important :**
>
> Vous pouvez également spécifier un mot de passe au lieu d'utiliser le code généré par Citrix Endpoint Management. L'action Verrouiller échoue si le code spécifié ne correspond pas aux exi-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> gences en matière de code de l'appareil ou du profil de travail existant.

Jeton bootstrap

Un jeton bootstrap (ou jeton d'amorçage) permet d'accorder l'attribut macOS SecureToken aux comptes lorsque vous vous connectez à un appareil macOS. SecureToken est transmis d'un compte approuvé à un autre. Les comptes compatibles SecureToken peuvent effectuer des opérations cryptographiques sur l'appareil. Sans le jeton bootstrap, vous devez suivre des workflows complexes pour créer des comptes sur cet appareil avant d'ajouter des comptes d'utilisateur individuels.

Citrix Endpoint Management prend en charge le dépôt des jetons bootstrap pour les appareils macOS inscrits via le programme de déploiement Apple. Vous utilisez le programme de déploiement d'Apple pour inscrire les appareils macOS que vous achetez directement auprès d'Apple, d'un revendeur agréé Apple ou d'un opérateur. Pour de plus amples informations sur l'inscription au programme de déploiement Apple, consultez la section Déployer des appareils via le programme de déploiement d'Apple.

Les jetons bootstrap sont générés pendant le workflow de l'assistant d'installation. Plus spécifiquement, ils sont générés lors de la création d'un compte d'utilisateur local. L'assistant d'installation s'exécute la première fois que les utilisateurs démarrent leurs appareils. Les jetons sont enregistrés dans la base de données Citrix Endpoint Management et ne sont pas visibles pour les utilisateurs. La suppression des appareils de votre site Citrix Endpoint Management supprime également les jetons. L'exécution d'une réinitialisation d'usine ne les supprime pas.

Prérequis :

- macOS 11.0 ou version ultérieure
- Appareils macOS dotés de la puce de sécurité Apple T2
- Appareils macOS inscrits via le programme de déploiement Apple

L'un des avantages du dépôt de jetons bootstrap avec Citrix Endpoint Management est que les comptes distants peuvent être activés pour FileVault et déverrouiller le volume FileVault. Pour de plus amples informations sur FileVault, consultez la section Stratégie FileVault.

Déployer des appareils via les programmes de déploiement d'Apple

March 1, 2024

Les programmes de déploiement Apple vous permettent d'inscrire automatiquement les appareils Apple à Citrix Endpoint Management sans aucune interaction nécessaire avant que les utilisateurs ne

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

les obtiennent. Une fois qu'un utilisateur déballe et active l'appareil, celui-ci est inscrit automatiquement dans Citrix Endpoint Management et tous les paramètres de gestion, les applications et les livres sont prêts à l'emploi.

Les programmes de déploiement Apple incluent Apple Business Manager (ABM) pour les entreprises et Apple School Manager (ASM) pour les établissements d'enseignement. ABM et ASM sont disponibles pour les appareils iOS, iPadOS et macOS. Pour plus d'informations sur l'éligibilité des appareils, consultez le guide de l'utilisateur Apple Business Manager ou le guide de l'utilisateur Apple School Manager.

> **Remarque :**
>
> ABM et ASM combinent l'ancien programme d'inscription d'appareils (DEP) et le programme d'achat en volume (VPP) d'Apple.

Cet article vous guide au travers des étapes de déploiement général avec ABM ou ASM :

1. S'inscrire à ABM ou ASM
2. Connecter votre compte ABM ou ASM à Citrix Endpoint Management
3. Commander des appareils
4. Attribuer des appareils à Citrix Endpoint Management
5. Acheter du contenu en volume et le synchroniser avec Citrix Endpoint Management
6. Configurer les règles de déploiement des stratégies et applications d'appareil
7. Ajouter des groupes de mise à disposition contenant des utilisateurs et des ressources qui leur sont attribués

Une fois ce processus de déploiement terminé, les appareils sont prêts à être déballés et activés pour une inscription automatique des appareils.

Logiciels requis

Ouvrez les ports requis pour la connexion entre Citrix Endpoint Management et Apple. Pour plus d'informations, consultez la section Configuration requise pour les ports.

S'inscrire à ABM ou ASM

Pour commencer à déployer des appareils dans Apple, inscrivez-vous à ABM ou ASM.

ABM et ASM sont disponibles pour les organisations et non pour les particuliers. Vous devez fournir de nombreuses informations sur l'organisation pour créer un compte. La demande et l'obtention de l'approbation peuvent ainsi prendre du temps.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

S'inscrire à ABM

Pour vous inscrire à ABM, accédez à business.apple.com. Cliquez sur **S'inscrire maintenant** pour demander un nouveau compte.

Il est recommandé d'utiliser une adresse e-mail pour votre organisation, par exemple `deployment@company.com`. Le processus d'inscription peut prendre quelques jours. Après avoir reçu vos informations d'identification d'ouverture de session, suivez les étapes fournies dans ABM pour créer un compte.

S'inscrire à ASM

Pour créer votre compte ASM, accédez à Apple School Manager et suivez les instructions d'inscription. Lors de votre première connexion à ASM, l'Assistant d'installation s'ouvre.

- Pour plus d'informations sur la configuration requise pour ASM, l'Assistant réglages et les tâches de gestion, veuillez consulter le guide de l'utilisateur d'Apple School Manager.
- Lorsque vous configurez un compte utilisateur ASM, utilisez un nom de domaine différent du nom de domaine d'Active Directory. Par exemple, ajoutez au nom de domaine ASM un préfixe tel que `appleid`.
- Lorsque vous connectez ASM à vos données de liste, ASM crée des identifiants Apple ID gérés pour les instructeurs et les étudiants. Vos données de liste comprennent les instructeurs, les étudiants et les classes. Pour plus d'informations sur l'ajout de liste à ASM, reportez-vous au Guide de l'utilisateur d'Apple School Manager, référencé précédemment.
- Vous pouvez personnaliser le format des identifiants Apple ID pour votre établissement, comme indiqué sous « Identifiants Apple gérés » dans le Guide de l'utilisateur d'Apple School Manager.

  > **Important :**
  >
  > Ne modifiez pas les identifiants Apple ID gérés après avoir importé des informations ASM dans Citrix Endpoint Management.

- Si vous avez acheté des appareils auprès de revendeurs ou d'opérateurs, liez ces appareils à ASM. Pour plus d'informations, reportez-vous au Guide de l'utilisateur d'Apple School Manager, référencé plus haut.

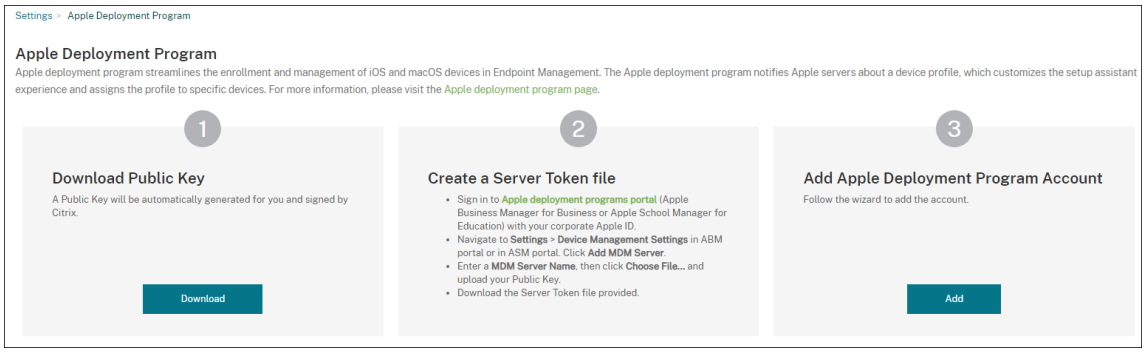
Connecter votre compte ABM ou ASM à Citrix Endpoint Management

Après avoir créé votre compte ABM ou ASM, connectez-le à votre déploiement de serveur Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Étape 1 : Télécharger une clé publique depuis votre serveur Citrix Endpoint Management

1. Dans la console Citrix Endpoint Management et accédez à **Paramètres > Programme de déploiement d'Apple**.



2. Sous **Télécharger la clé publique**, cliquez sur **Télécharger**.

Étape 2 : Créer et télécharger un fichier de jeton de serveur depuis votre compte Apple

1. Connectez-vous à Apple Business Manager ou Apple School Manager avec un compte disposant du rôle Administrateur ou Gestionnaire d'inscription des appareils.
2. En bas de la barre latérale, cliquez sur **Réglages**, puis cliquez sur **Réglages de gestion des appareils > Ajouter un serveur MDM**.
3. Dans le paramètre **Nom du serveur MDM**, tapez un nom pour le serveur Citrix Endpoint Management. Le nom du serveur que vous tapez est à titre de référence. Il ne s'agit pas de l'URL ou du nom du serveur.
4. Sous **Charger la clé publique**, cliquez sur **Choisir un fichier**. Chargez la clé publique que vous avez téléchargée depuis Citrix Endpoint Management et enregistrez les modifications.
5. Cliquez sur **Télécharger le jeton** pour télécharger le fichier de jeton de serveur sur votre ordinateur.

   Vous chargez le fichier de jeton de serveur lors de l'ajout du compte ABM ou ASM à Citrix Endpoint Management. Les informations de votre jeton s'affichent dans la console Citrix Endpoint Management après l'importation du fichier de jeton.
6. Sous **Attribution d'appareils par défaut**, cliquez sur **Modifier**. Choisissez la manière dont vous souhaitez attribuer les appareils et fournissez les informations requises. Pour de plus amples informations, consultez le Guide de l'utilisateur ABM ou le Guide de l'utilisateur Apple School Manager.

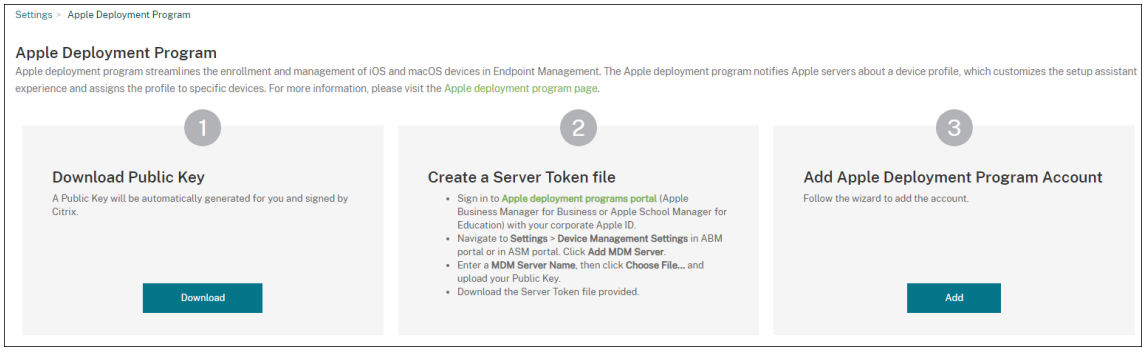
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Étape 3 : Ajouter votre compte à Citrix Endpoint Management

Vous pouvez ajouter plusieurs comptes ABM ou ASM à Citrix Endpoint Management. Cette fonctionnalité vous permet d'utiliser différents paramètres d'inscription ainsi que les options de l'Assistant d'installation par pays, département, etc. Vous pouvez associer des comptes ABM ou ASM à différentes stratégies.

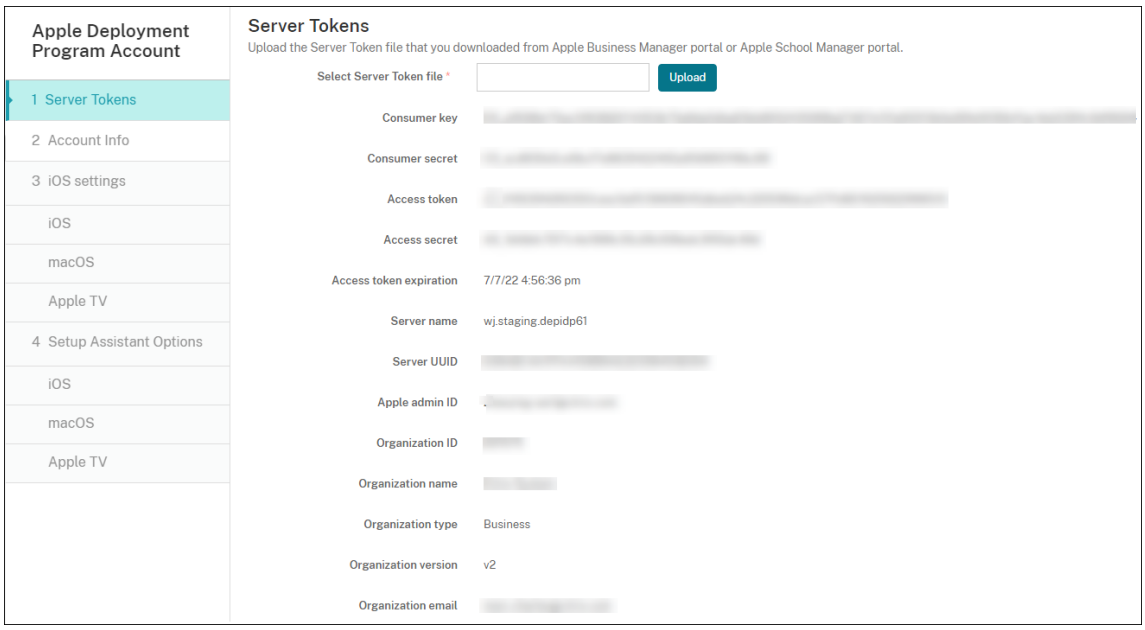
À titre d'exemple, vous pouvez centraliser tous vos comptes ABM ou ASM provenant de pays différents sur le même serveur Citrix Endpoint Management, de façon à pouvoir importer et surveiller tous les appareils ABM ou ASM. Vous devez d'abord personnaliser les paramètres d'inscription et configurer les options de l'assistant par service, hiérarchie organisationnelle ou autre structure. Vous configurez ensuite des stratégies pour fournir des fonctionnalités appropriées dans votre organisation et permettre aux utilisateurs de bénéficier de l'assistance appropriée.

1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Programme de déploiement d'Apple** et, sous **Ajouter un compte de programme de déploiement Apple**, cliquez sur **Ajouter**.



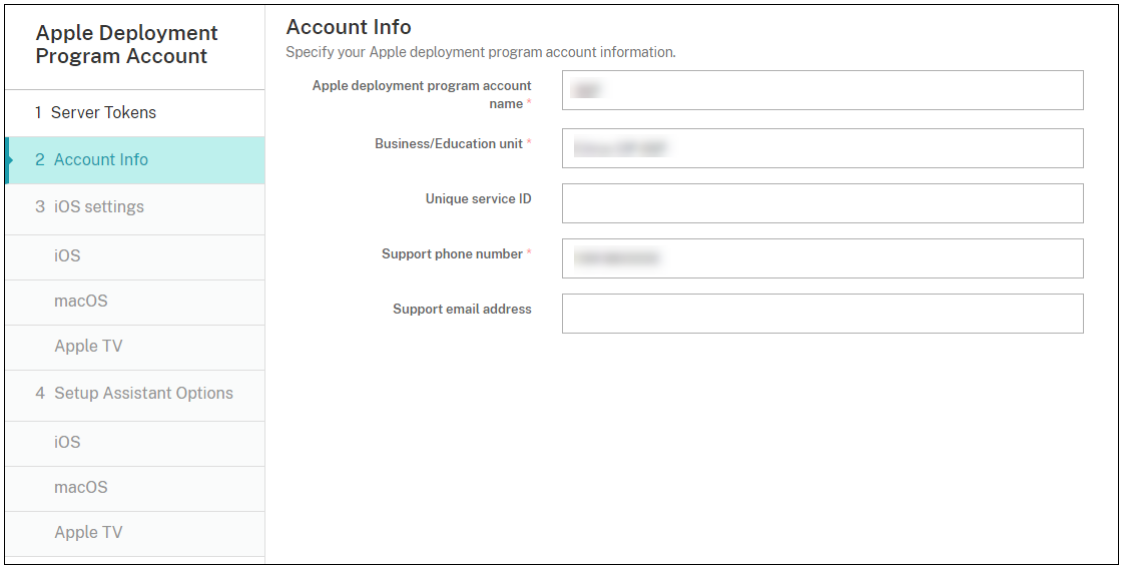
2. Sur la page **Jetons de serveur**, spécifiez votre fichier de jeton de serveur, puis cliquez sur **Charger**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Vos informations de jeton de serveur s'affichent.

3. Sur la page **Infos sur le compte**, spécifiez ces paramètres :



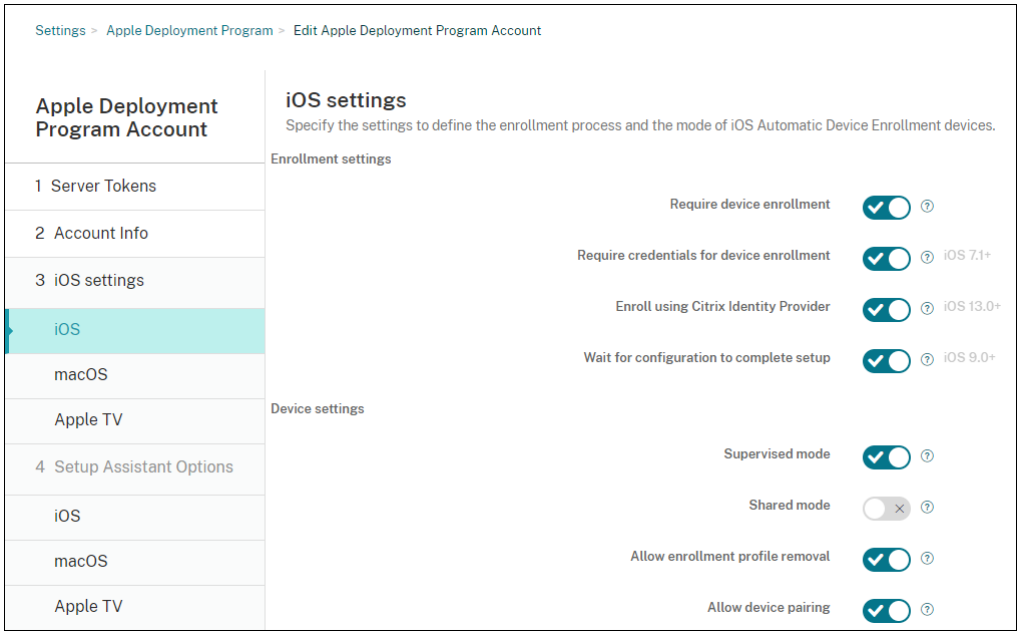
- **Nom du compte du programme de déploiement Apple :** nom descriptif unique pour ce compte ADP, identifiant la façon dont vous organisez les comptes ADP, par exemple par pays ou par hiérarchie organisationnelle.
- **Division/Département** : division ou département auquel l'appareil est attribué. Ce champ est obligatoire.
- **ID de service unique :** ID unique (facultatif) pour vous aider à identifier le compte.
- **Numéro de téléphone de l'assistance :** numéro de téléphone d'assistance que les utilisateurs peuvent appeler pour obtenir de l'aide au cours de la configuration. Ce champ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

est obligatoire.

- **Adresse e-mail de l'assistance :** adresse e-mail d'assistance (facultatif) que peuvent utiliser les utilisateurs.
- **Suffixe d'Éducation :** pour les comptes ASM. Tapez le suffixe attribué aux appareils inscrits via ce compte.

4. Dans **Paramètres iOS**, spécifiez les paramètres suivants :



Paramètres d'inscription :

- **Exiger l'inscription des appareils :** sélectionnez cette option pour obliger les utilisateurs à inscrire leurs appareils. La valeur par défaut est **Activé**.
- **Exiger des informations d'identification pour l'inscription de l'appareil :** indiquez si vous souhaitez demander aux utilisateurs d'entrer leurs informations d'identification lors de la configuration d'ABM et d'ASM. Nous recommandons de demander à tous les utilisateurs d'entrer leurs informations d'identification lors de l'inscription de l'appareil afin de limiter l'inscription des appareils aux utilisateurs autorisés. La valeur par défaut est **Activé**.

  Lorsque vous activez ABM ou ASM avant la première configuration et que vous ne sélectionnez pas cette option, Citrix Endpoint Management crée les composants ABM ou ASM. Cette création inclut des composants tels que l'utilisateur, Citrix Secure Hub, l'inventaire logiciel et le groupe de déploiement. Si vous sélectionnez cette option, Citrix Endpoint Management ne crée pas les composants. Par conséquent, si vous désactivez cette option ultérieurement, les utilisateurs qui n'ont pas entré leurs informations d'identification ne peuvent pas s'inscrire à ABM ni à ASM, car ces composants n'existent pas. Pour ajouter les composants ABM ou ASM, dans ce cas, désactivez, puis activez le compte ABM ou ASM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **S'inscrire à l'aide du fournisseur d'identité Citrix :** indique si l'inscription s'effectue à l'aide du fournisseur d'identité Citrix. Ce paramètre n'est disponible que pour les comptes ABM. Si cette option est **activée**, les appareils iOS prenant en charge ADP s'inscrivent uniquement à l'aide du fournisseur d'identité Citrix. La valeur par défaut est **Désactivé**.

  Pour activer ce paramètre, vous devez d'abord configurer Fournisseur d'identité Citrix en tant que fournisseur d'identité. Accédez à **Paramètres > Fournisseur d'identité (IdP)**, cliquez sur **Ajouter**, puis sélectionnez **Fournisseur d'identité Citrix**.

  Si ce paramètre est **activé**, prenez en compte les points suivants :

  - Vous ne pouvez pas supprimer la configuration du fournisseur d'identité Citrix correspondante sur la page **Paramètres > Fournisseur d'identité (IDP)**.
  - Lorsque vous modifiez la configuration du fournisseur d'identité Citrix correspondante, vous ne pouvez pas basculer vers un autre fournisseur d'identité.

- **Attendre la fin de l'installation :** indiquez si les appareils des utilisateurs doivent rester dans le mode Assistant d'installation jusqu'à ce que toutes les ressources MDM soient déployées sur l'appareil. Ce paramètre est disponible sur les appareils en mode supervisé. La valeur par défaut est **Désactivé**.

- La documentation Apple indique que les commandes suivantes peuvent ne pas fonctionner lorsqu'un appareil est en mode Assistant d'installation :

  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

Paramètres de l'appareil :

- **Mode supervisé :** doit être défini sur **Activé** si vous utilisez Apple Configurator pour gérer les appareils inscrits ou lorsque l'option **Attendre la fin de l'installation** est activée. La valeur par défaut est **Activé**. Pour de plus amples informations sur le placement d'un appareil iOS en mode supervisé, consultez la section Déployer des appareils à l'aide d'Apple Configurator 2.
- **Autoriser suppression du profil d'inscription :** indiquez si vous souhaitez autoriser les appareils à utiliser un profil que vous pouvez supprimer à distance. La valeur par défaut est **Désactivé**.
- **Autoriser le couplage de l'appareil :** indiquez si les appareils inscrits peuvent être gérés via Apple Music et Apple Configurator. La valeur par défaut est **Désactivé**.

Identités de supervision

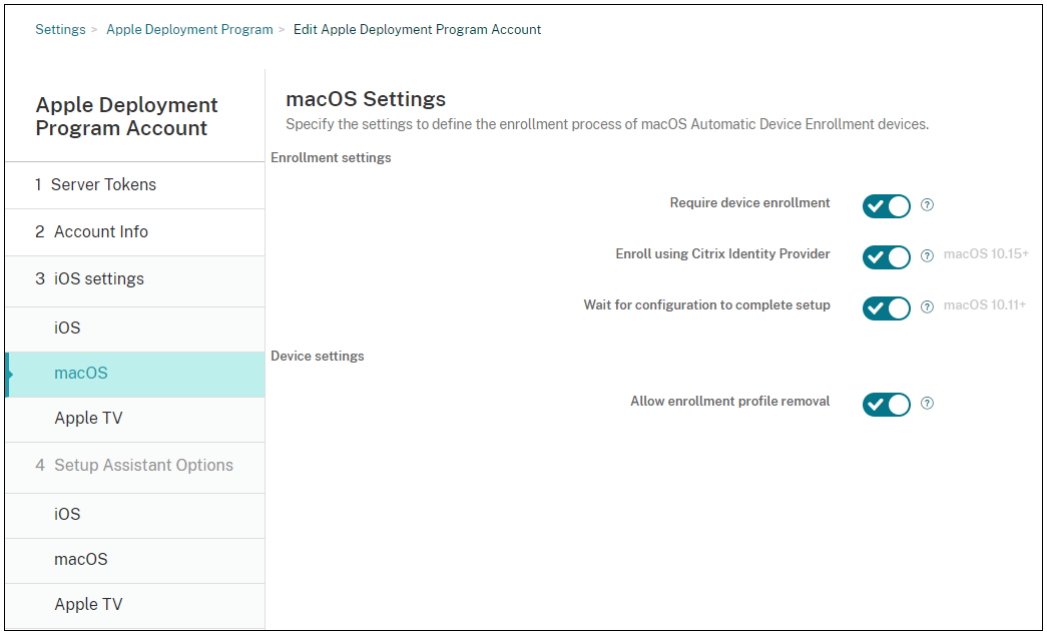
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si vous utilisez l'outil GroundControl, vous pouvez ajouter un certificat pour effectuer les opérations suivantes :

- Ignorez les restrictions liées au couplage pour éviter l'invite « Approuver cet hôte ».
- Faites passer les actions des appareils gérés via USB pour effectuer des activités telles que l'installation de profils sans interaction de l'utilisateur. Cela permet à GroundControl d'activer le mode d'application unique et le verrouillage de l'appareil pour l'extraction.
- Restaurez une sauvegarde sur les appareils ABM ou ASM.

Pour plus d'informations sur GroundControl, consultez le site Web de GroundControl.

5. Dans **Paramètres macOS**, spécifiez les paramètres suivants :



Paramètres d'inscription :

- **Exiger l'inscription des appareils :** sélectionnez cette option pour obliger les utilisateurs à inscrire leurs appareils. La valeur par défaut est **Activé**.
- **S'inscrire à l'aide du fournisseur d'identité Citrix :** indique si l'inscription s'effectue à l'aide du fournisseur d'identité Citrix. Ce paramètre n'est disponible que pour les comptes ABM. Si cette option est **activée**, les appareils macOS prenant en charge ADP s'inscrivent uniquement à l'aide du fournisseur d'identité Citrix. La valeur par défaut est **Désactivé**.

  Pour activer ce paramètre, vous devez d'abord configurer Fournisseur d'identité Citrix en tant que fournisseur d'identité. Accédez à **Paramètres > Fournisseur d'identité (IdP)**, cliquez sur **Ajouter**, puis sélectionnez **Fournisseur d'identité Citrix**.

  Si ce paramètre est **activé**, prenez en compte les points suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Vous ne pouvez pas supprimer la configuration du fournisseur d'identité Citrix correspondante sur la page **Paramètres > Fournisseur d'identité (IDP)**.
  - Lorsque vous modifiez la configuration du fournisseur d'identité Citrix correspondante, vous ne pouvez pas basculer vers un autre fournisseur d'identité.

- **Attendre la fin de l'installation :** si l'option **Activé** est sélectionnée, l'appareil macOS interrompt l'assistant d'installation jusqu'à ce que le code secret des ressources MDM soit déployé sur l'appareil. Ce déploiement se produit avant la création du compte local. Ce paramètre est disponible pour macOS 10.11 et versions ultérieures. La valeur par défaut est **Désactivé**.

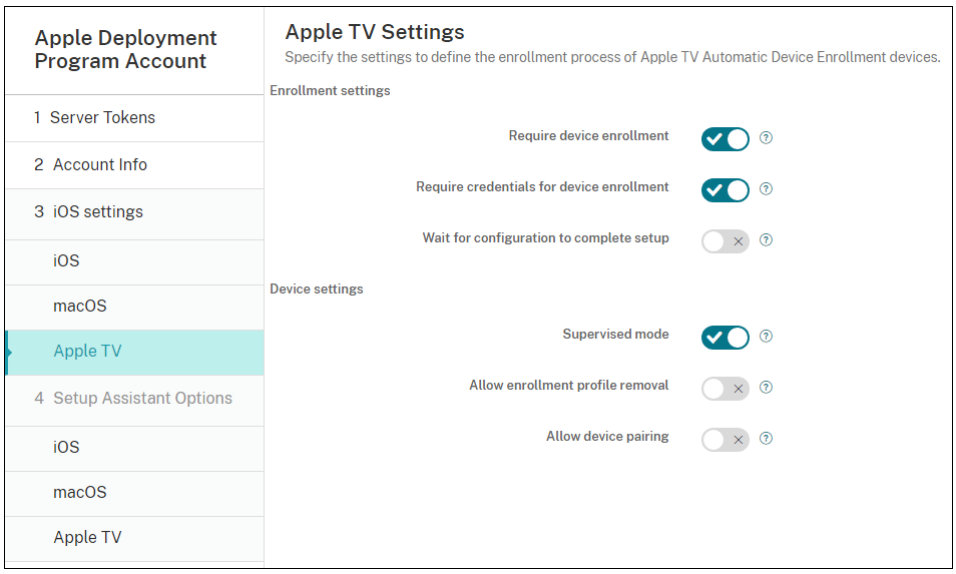
Paramètres de l'appareil :

- **Autoriser suppression du profil d'inscription :** indiquez si vous souhaitez autoriser les appareils à utiliser un profil que vous pouvez supprimer à distance. La valeur par défaut est **Désactivé**.

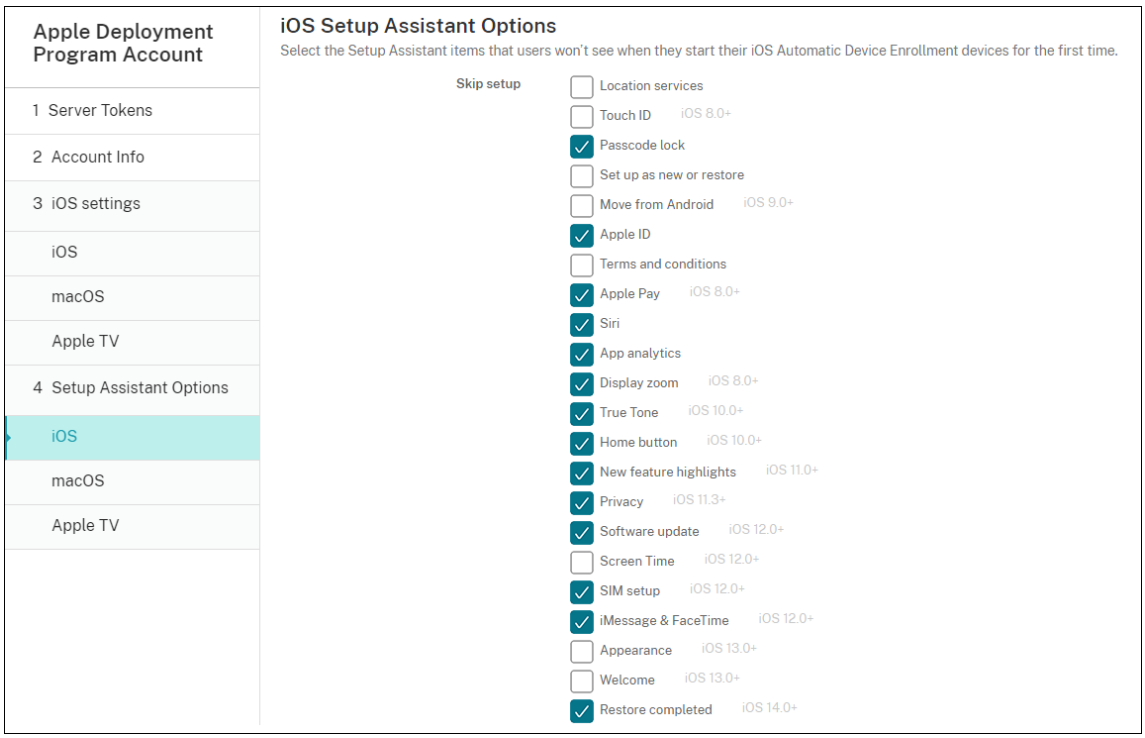
6. Dans **Paramètres Apple TV**, spécifiez les paramètres suivants :

   - **Exiger l'inscription des appareils :** empêche les utilisateurs d'ignorer l'inscription.
   - **Exiger des informations d'identification pour l'inscription de l'appareil :** demande les informations d'identification lors de l'inscription. Lorsque ce paramètre est désactivé, l' Apple TV est inscrite comme « utilisateur du programme DEP » par défaut.
   - **Attendre la fin de l'installation :** l'appareil reste sur l'écran **Assistant d'installation** jusqu'à ce que toutes les ressources soient déployées.
   - **Mode supervisé :** permet à l'administrateur de disposer de plus d'options lors de la configuration des restrictions.
   - **Autoriser la suppression du profil d'inscription :** permet aux utilisateurs de supprimer les profils d'inscription.
   - **Autoriser le couplage de l'appareil :** permet de gérer les appareils inscrits via le programme d'inscription d'appareils à l'aide d'outils Apple tels que Apple App Store et Apple Configurator.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



7. Dans **Options de l'assistant d'installation iOS**, sélectionnez les étapes que l'Assistant d'installation iOS peut ignorer lorsque les utilisateurs démarrent leurs appareils pour la première fois. Lorsqu'un écran est ignoré, la fonctionnalité associée utilise les paramètres par défaut. Les utilisateurs peuvent configurer les fonctionnalités ignorées une fois l'installation terminée, sauf si vous limitez complètement l'accès à ces fonctionnalités. Pour plus d'informations sur la restriction de l'accès aux fonctionnalités, consultez la section Stratégie de restrictions. Par défaut, tous les éléments sont désactivés. Les descriptions suivantes expliquent ce qui se produit lorsqu'un paramètre est sélectionné.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

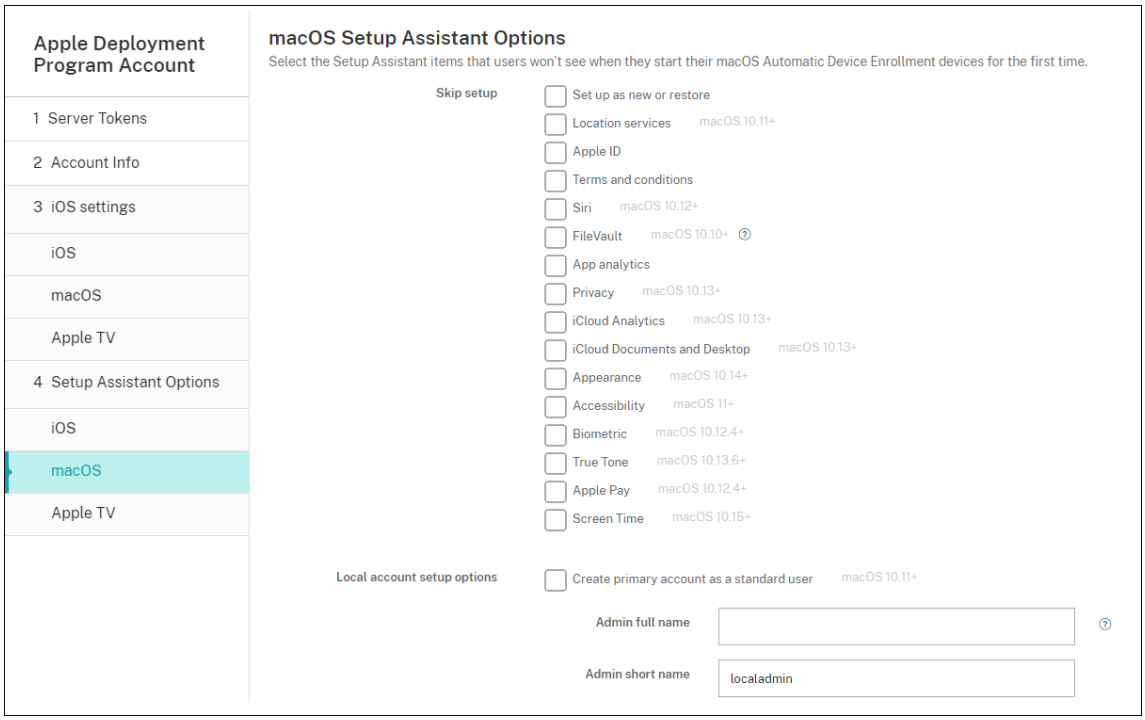
- **Services de localisation :** empêche les utilisateurs de configurer le service de localisation sur l'appareil.
- **Touch ID :** empêche les utilisateurs de configurer Touch ID ou Face ID sur les appareils iOS.
- **Verrouillage par code secret :** empêche les utilisateurs de configurer un code secret pour l'appareil. Si aucun code secret n'existe, les utilisateurs ne peuvent pas utiliser Touch ID ou Apple Pay.
- **Définir comme nouveau ou restaurer :** empêche les utilisateurs de configurer l'appareil comme nouveau ou de le restaurer à partir d'une sauvegarde de l'Apple App Store ou d'iCloud.
- **Déplacer depuis Android :** empêche les utilisateurs de transférer des données à partir d'un appareil Android vers un appareil iOS. Cette option est disponible uniquement lorsque **Définir comme nouveau ou restaurer** est sélectionné (sinon, cette étape est ignorée).
- **Apple ID :** empêche les utilisateurs de configurer un compte Apple ID géré pour l'appareil.
- **Termes et conditions :** empêche les utilisateurs de lire et d'accepter les termes et conditions d'utilisation de l'appareil.
- **Apple Pay :** empêche les utilisateurs de configurer Apple Pay. Si ce paramètre est désactivé, les utilisateurs doivent configurer Touch ID et Apple ID. Assurez-vous que ces paramètres sont effacés.
- **Siri :** empêche les utilisateurs de configurer Siri.
- **Analyse de l'application :** empêche les utilisateurs de configurer le partage des données d'incidents et des statistiques d'utilisation avec Apple.
- **Zoom d'affichage :** empêche les utilisateurs de définir la résolution d'affichage (standard ou zoom) sur les appareils iOS.
- **True Tone :** empêche les utilisateurs de configurer des capteurs à quatre canaux pour régler dynamiquement la balance des blancs de l'affichage.
- **Bouton d'accueil :** empêche les utilisateurs de configurer le style du bouton d'accueil des commentaires.
- **Présentation des nouvelles fonctionnalités :** empêche les utilisateurs d'afficher des écrans qui incluent des informations sur les nouvelles fonctionnalités du logiciel Apple.
- **Confidentialité :** empêche les utilisateurs d'afficher le panneau de données et de confidentialité. Pour iOS 11.3 et versions ultérieures.
- **Mise à jour logicielle :** empêche les utilisateurs de mettre à jour iOS vers la dernière version. Pour iOS 12.0 et versions ultérieures.
- **Screen Time :** empêche les utilisateurs d'activer la fonction Screen Time. Pour iOS 12.0 et versions ultérieures.
- **Configuration de la carte SIM :** empêche les utilisateurs de configurer un forfait de données mobiles. Pour iOS 12.0 et versions ultérieures.
- **iMessage & FaceTime :** empêche les utilisateurs d'activer iMessage et FaceTime. Pour iOS 12.0 et versions ultérieures.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Apparence :** empêche les utilisateurs de sélectionner le mode d'apparence. Pour iOS 13.0 et versions ultérieures.
- **Bienvenue :** empêche l'utilisateur d'afficher l'écran **Mise en route**. Pour iOS 13.0 et versions ultérieures.
- **Restauration terminée :** empêche les utilisateurs de voir si une restauration est terminée pendant l'installation. Pour iOS 14.0 et versions ultérieures.
- **Mise à jour terminée :** empêche les utilisateurs de voir si une mise à jour logicielle est terminée pendant l'installation. Pour iOS 14.0 et versions ultérieures.
- **Magasin d'applications :** empêche les utilisateurs de configurer le magasin d'applications. Pour iOS 11.1 et versions ultérieures.

Le compte apparaît dans **Paramètres > Programme de déploiement d'Apple**.

8. Dans **Options de l'assistant d'installation macOS**, sélectionnez les étapes que l'Assistant d'installation macOS peut ignorer lorsque les utilisateurs démarrent leurs appareils pour la première fois. Lorsqu'un écran est ignoré, la fonctionnalité associée utilise les paramètres par défaut. Les utilisateurs peuvent configurer les fonctionnalités ignorées une fois l'installation terminée, sauf si vous limitez complètement l'accès à ces fonctionnalités. Pour plus d'informations sur la restriction de l'accès aux fonctionnalités, consultez la section Stratégie de restrictions. Par défaut, tous les éléments sont désactivés. Les descriptions suivantes expliquent ce qui se produit lorsqu'un paramètre est sélectionné.



- **Définir comme nouveau ou restaurer :** empêche les utilisateurs de configurer l'appareil comme nouveau ou à partir d'une sauvegarde Time Machine ou d'effectuer une migration

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

système.

- **Services de localisation :** empêche les utilisateurs de configurer le service de localisation sur l'appareil. Pour macOS 10.11 et versions ultérieures.
- **Apple ID :** empêche les utilisateurs de configurer un compte Apple ID géré pour l'appareil.
- **Termes et conditions :** empêche les utilisateurs de lire et d'accepter les termes et conditions d'utilisation de l'appareil.
- **Siri :** empêche les utilisateurs de configurer Siri. Pour macOS 10.12 et versions ultérieures.
- **FileVault :** utilisez FileVault pour crypter le disque de démarrage. Citrix Endpoint Management applique le paramètre FileVault uniquement si le système dispose d'un seul compte utilisateur local et que ce compte est connecté à iCloud.

  Vous pouvez utiliser la fonctionnalité de cryptage de disque FileVault de macOS pour protéger le volume système en cryptant son contenu (https://support.apple.com/en-us/HT204837). Si vous exécutez l'assistant d'installation sur un Mac portable de modèle récent sur lequel FileVault n'est pas activé, vous pourrez être invité à activer cette fonctionnalité. L'invite s'affiche sur les nouveaux systèmes et les systèmes mis à niveau vers OS X 10.10 ou 10.11, mais uniquement si le système dispose d'un compte d'administrateur local unique et que ce compte est connecté à iCloud.
- **Analyse de l'application :** empêche les utilisateurs de configurer le partage des données d'incidents et des statistiques d'utilisation avec Apple.
- **Confidentialité :** empêche les utilisateurs d'afficher le panneau de données et de confidentialité. Pour macOS 10.13 et versions ultérieures.
- **Analyse d'iCloud :** empêche les utilisateurs de choisir d'envoyer des données iCloud de diagnostic à Apple. Pour macOS 10.13 et versions ultérieures.
- **Bureau et documents iCloud :** empêche les utilisateurs de configurer le bureau et les documents iCloud. Pour macOS 10.13 et versions ultérieures.
- **Apparence :** empêche les utilisateurs de sélectionner le mode d'apparence. Pour macOS 10.14 et versions ultérieures.
- **Accessibilité :** empêche les utilisateurs d'entendre la fonctionnalité VoiceOver automatiquement. Disponible uniquement si l'appareil est connecté à Ethernet. Pour macOS 11 et versions ultérieures.
- **Biométrie :** empêche l'utilisateur de configurer Touch ID et Face ID. Pour macOS 10.12.4 et versions ultérieures.
- **True Tone :** empêche les utilisateurs de configurer des capteurs à quatre canaux pour régler dynamiquement la balance des blancs de l'affichage. Pour macOS 10.13.6 et versions ultérieures.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Apple Pay :** empêche les utilisateurs de configurer Apple Pay. Si ce paramètre est désactivé, les utilisateurs doivent configurer Touch ID et Apple ID. Assurez-vous que les paramètres **Apple ID** et **Biométrie** sont effacés.
- **Screen Time :** empêche les utilisateurs d'activer la fonction Screen Time. Pour macOS 10.15 et versions ultérieures.
- **Magasin d'applications :** empêche les utilisateurs de configurer le magasin d'applications. Pour macOS 11.1 et versions ultérieures.
- **Déverrouiller avec Apple Watch :** empêche les utilisateurs de déverrouiller leur Mac à l'aide d'une Apple Watch. Pour macOS 12 et versions ultérieures.
- **Options de configuration du compte local :** spécifiez les paramètres pour créer un compte sur l'appareil. Citrix Endpoint Management crée d'abord le compte d'administrateur local à l'aide des informations que vous spécifiez ici. Lorsque les utilisateurs activent leur appareil, un compte d'utilisateur est créé en tant que compte principal. L'option **Créer un compte principal en tant qu'utilisateur standard** détermine si le compte principal dispose des privilèges d'administrateur.

> **Important :**
>
> Vous pouvez sélectionner **Créer un compte principal en tant qu'utilisateur standard** uniquement après avoir défini l'option **Attendre la fin de l'installation** sur **Activé** sur la page **Paramètres macOS**.

- **Créer un compte principal en tant qu'utilisateur standard :** lorsque cette option est sélectionnée, Citrix Endpoint Management donne à l'utilisateur des autorisations standard au lieu d'accorder à l'utilisateur des privilèges d'administrateur sur l'appareil. Ignorez cette option si vous souhaitez accorder à l'utilisateur des privilèges d'administrateur sur l'appareil. Cette option n'est pas sélectionnée par défaut.
- **Nom complet de l'administrateur :** saisissez le nom que le système affiche pour le compte administrateur.
- **Nom court de l'administrateur :** saisissez le nom que l'appareil affiche pour le dossier de base et dans le shell.
- **Mot de passe de l'administrateur :** saisissez un mot de passe sécurisé pour le compte administrateur.
- **Afficher le compte administrateur dans Utilisateurs et groupes :** si cette option n'est pas cochée, le compte administrateur n'apparaît pas dans **Utilisateurs et groupes** dans les paramètres macOS. Si vous créez le compte principal en tant qu'utilisateur standard, activez ce paramètre pour masquer le compte administrateur créé par Citrix Endpoint Management.

Pour renforcer la sécurité, Citrix Endpoint Management vérifie s'il faut alterner le mot de passe du compte administrateur quotidiennement. Par défaut, Citrix Endpoint Management alterne

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

le mot de passe tous les 7 jours. Pour modifier la valeur par défaut, mettez à jour la propriété de serveur `mac.dep.admin.passwd.rotate`. Pour plus d'informations, consultez Propriétés du serveur.

Pour renforcer le niveau de sécurité du mot de passe, Citrix Endpoint Management génère les mots de passe comme suit :

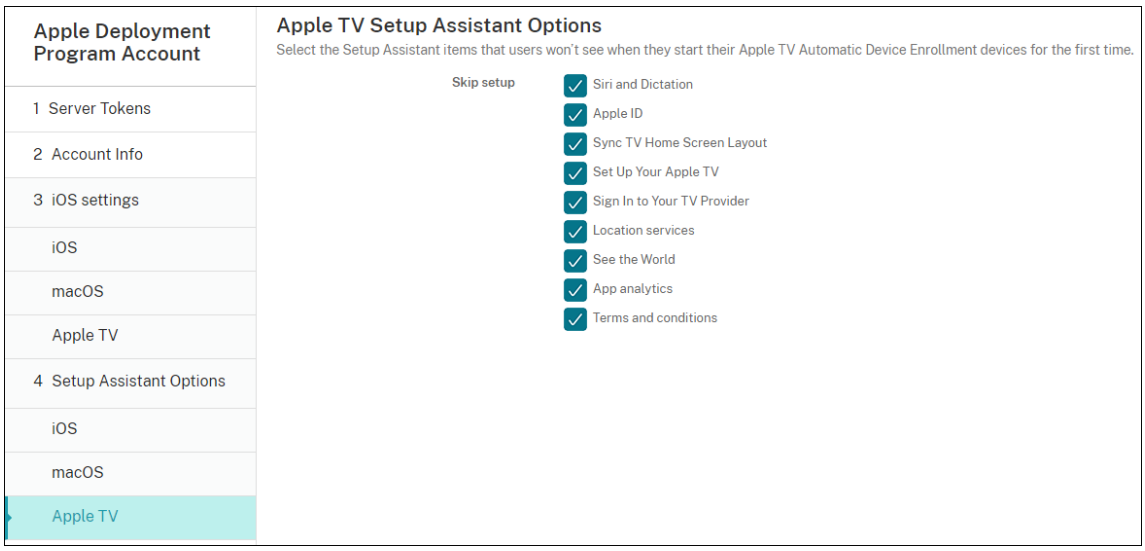
- 12 caractères
- 3 lettres majuscules
- 3 lettres minuscules
- 3 chiffres
- 3 caractères spéciaux : `! \@ \\# \$ % \\^ \* ? + = -`

Pour afficher le mot de passe précédent, le mot de passe actuel et l'état de modification du mot de passe d'un appareil, accédez à **Gestion > Appareils**. Cliquez sur l'appareil, puis sur **Afficher plus**, puis affichez la page **Détails de l'appareil > Général**. La section **Sécurité** affiche les éléments suivants :

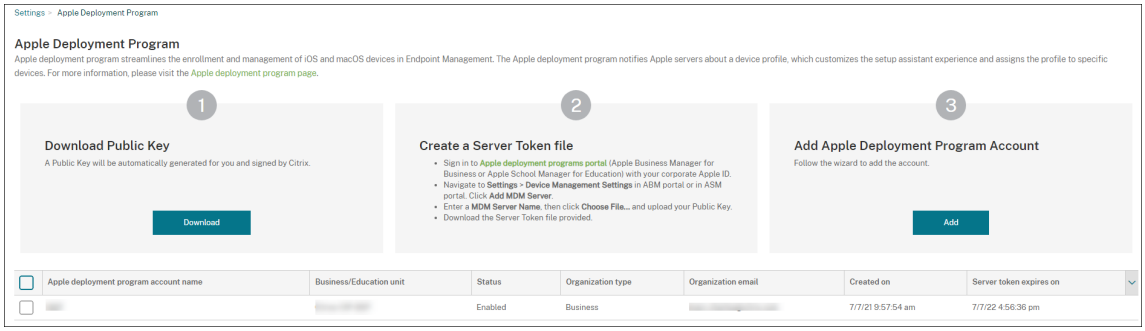
- **Mot de passe administrateur précédent :** permet d'afficher le mot de passe précédent. Citrix Endpoint Management affiche uniquement le dernier mot de passe. Cliquez sur **Afficher le mot de passe** pour afficher le mot de passe.
- **Mot de passe administrateur actuel :** permet d'afficher le mot de passe actuel.
- **Changer le mot de passe administrateur :** permet d'afficher l'état de changement du mot de passe. Les informations suivantes peuvent apparaître en fonction de l'état réel :
  - Demande de modification du mot de passe : < heure spécifique >.
  - Modification du mot de passe : < heure spécifique >.
  - Échec des tentatives de modification du mot de passe : < heure spécifique >.
  - Le mot de passe n'a pas encore été modifié.

9. Dans **Options de l'assistant d'installation Apple TV**, sélectionnez les étapes de l'Assistant d'installation Apple TV à ignorer lorsque les utilisateurs démarrent leurs appareils pour la première fois. Par défaut, tous les éléments sont désactivés. Enregistrez les modifications.

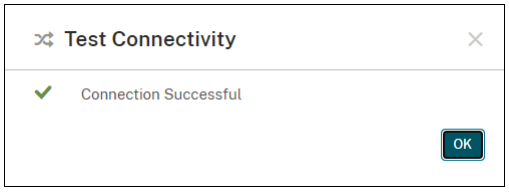
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



10. Le compte apparaît dans **Paramètres > Programme de déploiement d'Apple**. Pour tester la connexion entre Citrix Endpoint Management et Apple, sélectionnez le compte et cliquez sur **Tester la connectivité**.



Un message d'état s'affiche.



Commander des appareils

Vous pouvez commander des appareils directement depuis les canaux suivants :

- Apple. Indiquez vos numéros de client Apple au vendeur.
- Revendeur ou opérateurs agréés Apple participants. Indiquez l'ID de votre organisation au vendeur et obtenez son ID de revendeur.

Pour plus d'informations sur la gestion des fournisseurs d'appareils, consultez le guide de l'utilisateur Apple Business Manager ou le guide de l'utilisateur Apple School Manager.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Une fois votre commande expédiée, les appareils Apple que vous avez achetés sont ajoutés à votre compte ABM ou ASM.

Attribuer des appareils à Citrix Endpoint Management

Dans le portail ABM ou ASM, recherchez un numéro de commande et utilisez-le pour attribuer des appareils dans cette commande à votre instance Citrix Endpoint Management. Vous pouvez également ajouter des appareils iPhone, iPad, iPod Touch et Apple TV à ABM ou ASM à l'aide d'Apple Configurator 2, quel que soit l'endroit où les appareils ont été achetés.

Pour de plus amples informations, consultez le Guide de l'utilisateur Apple Business Manager ou le Guide de l'utilisateur Apple School Manager.

Acheter du contenu en volume et le synchroniser avec Citrix Endpoint Management

ABM et ASM vous permettent d'acheter, de distribuer et de gérer des licences d'applications et de livres en volume à partir d'un seul compte d'organisation. Pour permettre à Citrix Endpoint Management de communiquer avec ABM ou ASM afin d'obtenir les informations liées aux licences à distribuer, procédez comme suit :

1. Dans le portail ABM ou ASM, achetez des applications et des livres publics à partir du menu **Apps et Livres** ; achetez des applications personnalisées développées pour votre instance Citrix Endpoint Management à partir du menu **Applications personnalisées**.
2. Dans le portail ABM ou ASM, téléchargez le jeton de contenu attribué à votre instance Citrix Endpoint Management.

   Pour de plus amples informations sur les étapes 1 et 2, consultez le guide de l'utilisateur Apple Business Manager ou le guide de l'utilisateur Apple School Manager.
3. Dans la console Citrix Endpoint Management, créez un compte d'achat en volume basé sur le jeton de contenu que vous avez téléchargé.

   Pour de plus amples informations, consultez la section Ajouter des applications via l'achat en volume Apple.

   Une fois le compte d'achat en volume créé, les applications et les livres que vous avez achetés apparaissent dans **Gérer** > **Applications**, et les appareils que vous avez attribués au serveur Citrix Endpoint Management apparaissent dans **Gérer > Appareils**.

Configurer les règles de déploiement des stratégies et applications d'appareil

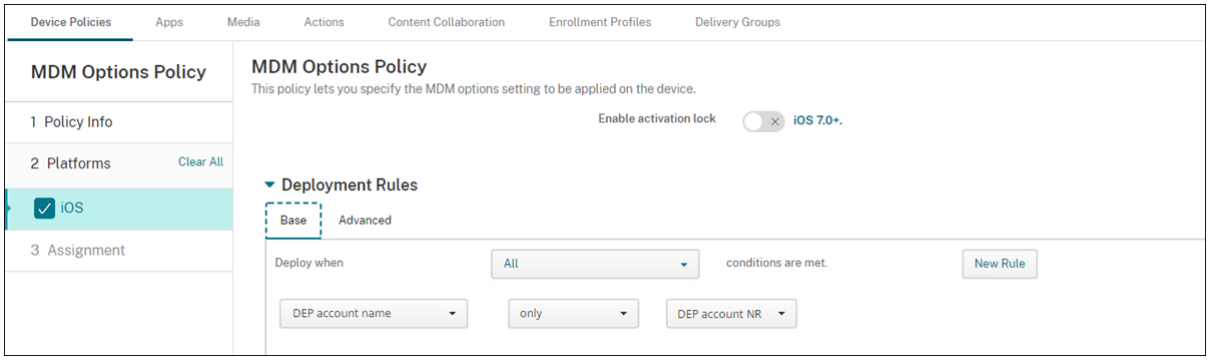
Vous pouvez associer des comptes ABM ou ASM à différentes stratégies d'appareil et applications lorsque vous configurez des stratégies d'appareil et des applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Sur les pages **Configurer > Stratégies d'appareil** et **Configurer > Applications**, développez **Règles de déploiement**.
2. Spécifiez si une stratégie ou une application est déployée pour un compte ABM particulier ou pour tous les comptes ABM à l'exception de celui sélectionné.

La liste des comptes ABM contient uniquement les comptes avec l'état activé ou désactivé. Si le compte ABM est désactivé, l'appareil ABM n'appartient pas à ce compte. Par conséquent, Citrix Endpoint Management ne déploie pas l'application ou la stratégie sur l'appareil.

Dans l'exemple suivant, une stratégie est déployée uniquement pour les appareils avec le nom de compte ABM « ABM Account NR ».



Inscription en bloc d'appareils Apple

March 1, 2024

Vous pouvez inscrire un grand nombre d'appareils iOS, iPadOS et macOS dans Citrix Endpoint Management de deux façons :

- Utilisez les programmes de déploiement Apple pour inscrire les appareils Apple que vous achetez directement auprès d'Apple ou auprès d'un revendeur agréé Apple participant ou d'un opérateur.

  Pour de plus amples informations sur le déploiement d'appareils compatibles avec les programmes de déploiement Apple, consultez la section Déployer des appareils via les programmes de déploiement d'Apple. Cet article décrit comment les utilisateurs inscrivent des appareils compatibles avec les programmes de déploiement Apple et comment les réinscrire.

- Utilisez Apple Configurator 2 pour inscrire des appareils iOS, qu'ils aient été achetés ou non directement auprès d'Apple.

Cet article explique comment déployer des appareils en bloc à l'aide d'Apple Configurator 2.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

À propos de l'inscription en bloc

Les programmes de déploiement Apple incluent Apple Business Manager (ABM) pour les entreprises et Apple School Manager (ASM) pour l'éducation. L'inscription en bloc via les fonctionnalités des programmes de déploiement Apple présente les caractéristiques suivantes :

- Vous n'avez aucune tâche de préparation à effectuer sur les appareils.
- Une fois les paramètres de déploiement configurés dans Citrix Endpoint Management, vous pouvez distribuer les appareils aux utilisateurs qui peuvent commencer à les utiliser immédiatement.
- Vous pouvez simplifier le processus de configuration pour les utilisateurs en supprimant certaines étapes de l'assistant de configuration.
- Pour plus d'informations sur la configuration d'ABM et ASM, consultez la documentation disponible pour Apple Business Manager et Apple School Manager.

L'inscription en bloc via Apple Configurator 2 présente les caractéristiques suivantes :

- Vous associez des appareils iOS à un ordinateur Mac exécutant macOS 10.7.2 ou version ultérieure et l'application Apple Configurator 2. Vous préparez les appareils iOS et configurez des stratégies à l'aide d'Apple Configurator 2.
- Les appareils sont automatiquement inscrits dans Citrix Endpoint Management pendant le processus de configuration. Une fois la configuration terminée, Citrix Endpoint Management envoie des stratégies, des applications et d'autres ressources aux appareils. Vous pouvez alors commencer à gérer les appareils.
- Pour de plus amples informations sur l'utilisation de Apple Configurator 2, consultez l'aide de Apple Configurator.

Comment les utilisateurs inscrivent des appareils compatibles avec les programmes de déploiement Apple

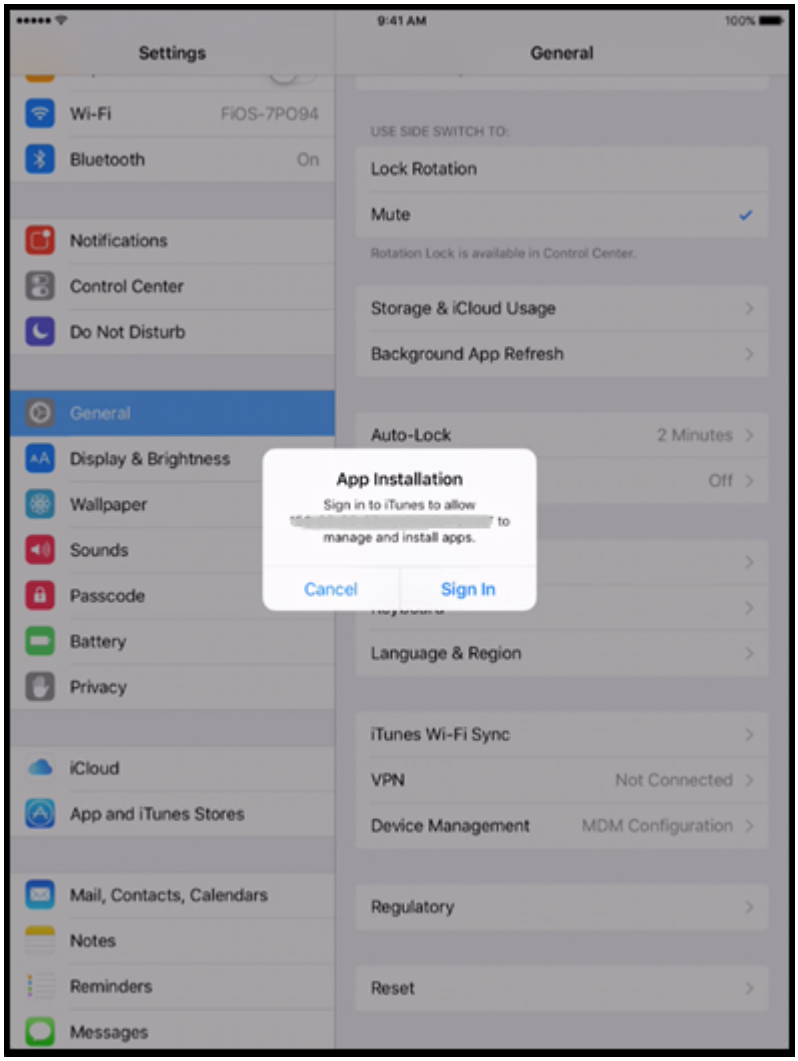
Les utilisateurs inscrivent leurs appareils dans Citrix Endpoint Management comme suit :

1. Les utilisateurs démarrent leur appareil.
2. Citrix Endpoint Management fournit à l'appareil les paramètres des programmes de déploiement Apple que vous avez configurés sur la page **Paramètres > Programmes de déploiement Apple**.
3. Les utilisateurs configurent les paramètres initiaux sur leur appareil.
4. L'appareil démarre automatiquement le processus d'inscription d'appareils d'Citrix Endpoint Management.
5. Les utilisateurs configurent les autres paramètres initiaux sur leur appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Dans l'écran d'accueil, les utilisateurs peuvent être invités à se connecter à l'Apple App Store afin de télécharger Citrix Secure Hub.

> **Remarque :**
>
> cette étape est facultative si Citrix Endpoint Management est configuré pour déployer l'application Citrix Secure Hub à l'aide de l'attribution d'applications d'achat en volume basée sur l'appareil. Dans ce cas, vous n'avez pas besoin de créer de compte Apple App Store ou d'utiliser un compte existant.



7. Les utilisateurs ouvrent Citrix Secure Hub et entrent leurs informations d'identification. Si cela est requis par la stratégie, les utilisateurs peuvent être invités à créer et vérifier un code PIN Citrix.

   Citrix Endpoint Management déploie les applications requises restantes sur l'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Réinscrire les appareils compatibles avec les programmes de déploiement Apple

Les appareils compatibles avec les programmes de déploiement Apple sont inscrits lorsqu'ils se trouvent dans une condition de réinitialisation d'usine. Pour réinscrire un appareil compatible avec les programmes de déploiement Apple, vous devez d'abord effectuer un effacement complet pour annuler l'inscription de l'appareil. Les étapes détaillées sont les suivantes :

1. Sur la page **Gérer > Appareils**, sélectionnez l'appareil.
2. Cliquez sur **Sécurité**.
3. Cliquez sur **Effacer** pour annuler l'inscription de l'appareil et le réinitialiser aux paramètres d'usine.
4. Démarrez l'appareil.

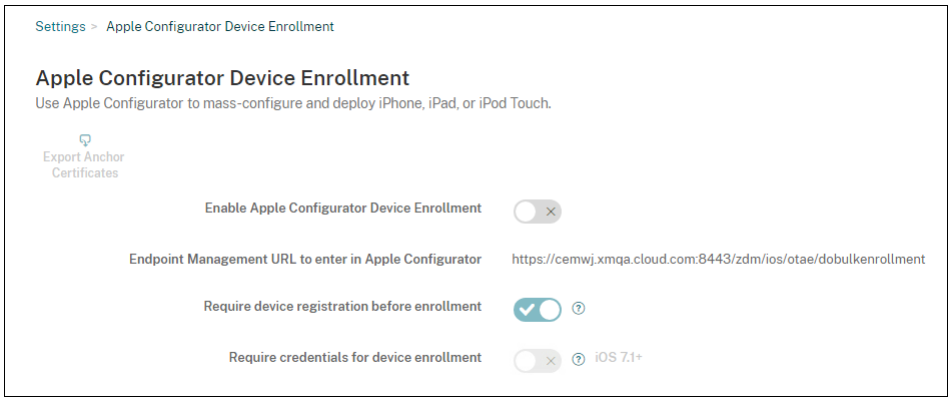
> **Important :**
>
> N'utilisez pas l'option **Effacer les données d'entreprise** pour annuler l'inscription d'un appareil compatible avec les programmes de déploiement Apple, car l'inscription nécessite que l'appareil soit réinitialisé aux paramètres d'usine.

Déployer des appareils à l'aide d'Apple Configurator 2

Vous pouvez utiliser Apple Configurator 2 pour déployer de nombreux appareils avec des paramètres, des applications et des données, et inscrire ces appareils dans Citrix Endpoint Management.

Étape 1 : Configurer les paramètres dans Citrix Endpoint Management

1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Inscription d'appareils dans Apple Configurator**.



2. Définissez **Autoriser l'inscription d'appareils dans Apple Configurator** sur **Oui**.
3. Copiez l'**URL d'inscription pour entrer dans le paramètre Apple Configurator** et collez cette URL lorsque vous configurez les paramètres dans Apple Configurator 2. Ce paramètre fournit l'

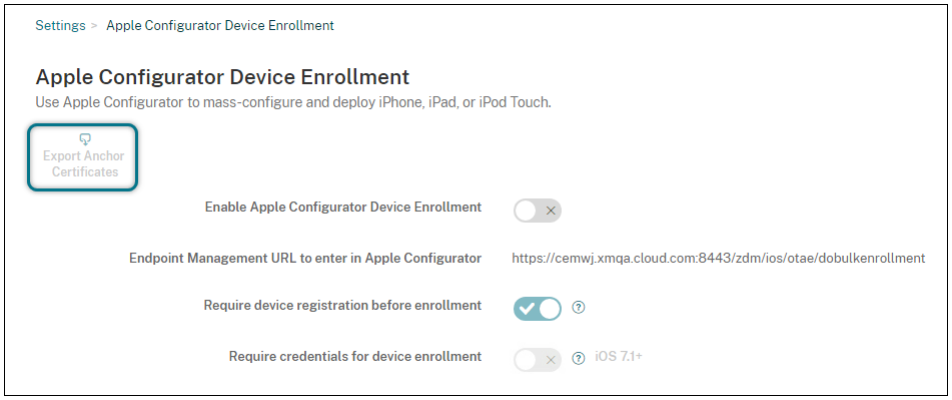
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

URL du serveur Citrix Endpoint Management qui communique avec Apple. L'URL d'inscription est le nom de domaine complet (FQDN) du serveur Citrix Endpoint Management, comme `mdm.server.url.com`, ou l'adresse IP.

4. Pour empêcher les appareils inconnus de s'inscrire, définissez **Exiger l'enregistrement des appareils avant l'inscription** sur **Oui**. Remarque : si ce paramètre est défini sur **Oui**, vous devez ajouter les appareils configurés via **Gérer > Appareils** dans Citrix Endpoint Management manuellement ou via un fichier CSV avant l'inscription.

5. Pour exiger que les utilisateurs d'appareils iOS entrent leurs informations d'identification lors de l'inscription, définissez **Exiger des informations d'identification pour l'inscription de l'appareil** sur **Oui**. La valeur par défaut est **Non**.

> **Remarque :**
>
> Si le serveur Citrix Endpoint Management utilise un certificat SSL approuvé, ignorez cette étape. Cliquez sur **Exporter les certificats d'ancrage** et enregistrez le fichier certchain.pem sur le trousseau macOS (de connexion ou système).



Étape 2 : Configurer les paramètres dans Apple Configurator 2

1. Préparez un Mac exécutant macOS 10.7.2 ou version ultérieure et sur lequel Apple Configurator 2 est installé.

2. Utilisez un câble Dock Connector vers USB pour connecter des appareils Apple au Mac. Vous pouvez configurer simultanément jusqu'à 30 appareils connectés. Si vous ne disposez pas d'un Dock Connector, utilisez un ou plusieurs hubs (alimentés) USB 2.0 haute vitesse pour connecter les appareils.

3. Démarrez Apple Configurator 2. Le configurateur affiche tous les appareils que vous pouvez préparer à des fins de supervision.

4. Pour préparer un appareil à des fins de supervision :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Sélectionnez **Superviser des appareils** si vous souhaitez conserver le contrôle de l'appareil en réappliquant régulièrement une configuration. Cliquez sur **Suivant**.

  > **Important :**
  >
  > Le fait de placer un appareil en mode supervisé installe la version sélectionnée d'iOS sur l'appareil, ce qui efface complètement toutes les données et applications précédemment stockées par l'utilisateur.

- Dans iOS, cliquez sur l'option appropriée afin d'obtenir la version **la plus récente** d'iOS que vous souhaitez installer.

5. Dans **Inscrire au serveur MDM**, choisissez un serveur MDM. Pour ajouter un serveur, cliquez sur **Suivant**.
6. Dans **Définir un serveur MDM**, indiquez un nom pour le serveur et collez l'URL du serveur MDM à partir de la console Citrix Endpoint Management.
7. Dans **Attribuer à l'organisation**, choisissez une organisation pour superviser l'appareil.

   Pour plus d'informations sur la préparation d'appareils avec Apple Configurator 2, consultez la page d'aide d'Apple Configurator Prepare devices.
8. À mesure que chaque appareil est préparé, activez-le pour démarrer l'Assistant d'installation iOS, qui prépare l'appareil pour la première utilisation.

Ajouter des appareils à ABM ou ASM à l'aide d'Apple Configurator 2

Vous pouvez ajouter des appareils iPhone, iPad et Apple TV à votre compte ABM ou ASM à l'aide d'Apple Configurator 2, quel que soit l'endroit où les appareils ont été achetés.
Lorsque vous ajoutez des appareils, ils apparaissent dans la section **Appareils**. Ces appareils n'incluent plus les paramètres d'inscription attribués via Apple Configurator 2. Pour de plus amples informations, consultez le Guide de l'utilisateur Apple Business Manager ou le Guide de l'utilisateur Apple School Manager.

Renouveler le jeton ADP

Citrix Endpoint Management affiche un avertissement d'expiration de licence lorsque votre jeton ADP expire. Remplacez le jeton depuis ASM ou ABM.

Étape 1 : Télécharger une clé publique depuis votre serveur Citrix Endpoint Management

1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Programme de déploiement d'Apple** pour télécharger une nouvelle clé publique.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Étape 2 : Créer et télécharger un fichier de jeton de serveur depuis votre compte Apple

1. Connectez-vous à ABM pour télécharger le jeton.
2. Ouvrez **Réglages** et sélectionnez le serveur auprès duquel vous devez vous procurer un jeton. Cliquez sur **Modifier**.
3. Sous **Réglages du serveur MDM**, chargez la nouvelle clé publique que vous avez téléchargée depuis Citrix Endpoint Management et enregistrez les modifications.
4. Cliquez sur **Télécharger le jeton** pour télécharger le nouveau jeton.

Étape 3 : Charger un fichier de jeton de serveur dans Citrix Endpoint Management

1. Dans Citrix Endpoint Management, accédez à **Paramètres > Programme de déploiement d' Apple**.
2. Sélectionnez le compte du programme de déploiement, cliquez sur **Modifier** et chargez votre fichier de jeton de serveur.
3. Cliquez sur **Suivant** et enregistrez les modifications.

Intégration aux fonctionnalités Apple Éducation

March 1, 2024

Vous pouvez utiliser Citrix Endpoint Management en tant que solution de gestion d'appareils mobiles (MDM) dans un environnement qui utilise Apple Éducation. La prise en charge Citrix Endpoint Management inclut Apple School Manager (ASM) et l'application En classe pour iPad. La stratégie Configuration de l'éducation d'Citrix Endpoint Management configure les appareils des instructeurs et des étudiants pour une utilisation avec Apple Éducation.

Vous devez fournir des iPad préconfigurés et supervisés aux instructeurs et aux étudiants. Cette configuration inclut l'inscription à ASM dans Citrix Endpoint Management, un compte Apple ID géré configuré avec un nouveau mot de passe et les applications et iBooks d'achat en volume requis.

Pour plus d'informations sur les fonctionnalités d'Apple Éducation, consultez le site Éducation d'Apple et le Guide de déploiement dans le secteur de l'éducation d'Apple sur ce site.

Apple School Manager

Suivez ces étapes générales pour intégrer Citrix Endpoint Management à ASM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Créez un compte pour votre établissement dans ASM afin d'inscrire votre établissement à ASM.
2. Configurez un compte d'achat en volume Éducation pour Apple School Manager.
3. Ajoutez des mots de passe pour les utilisateurs Apple School Manager.
4. Planifiez et ajoutez des ressources et des groupes de mise à disposition à Citrix Endpoint Management.
5. Testez les inscriptions d'appareil instructeur et étudiant.
6. Fournissez les appareils préconfigurés aux instructeurs et aux étudiants.
7. Gérer les données des instructeurs, des étudiants et de la classe
8. Si un appareil est perdu ou volé, vous pouvez le verrouiller et le localiser.

Pour plus d'informations sur l'inscription à ASM et la connexion de votre compte à Citrix Endpoint Management, consultez la section Déployer des appareils via le programme de déploiement d'Apple.

Logiciels requis

- NetScaler Gateway
- Profil d'inscription configuré pour MDM+MAM.
- Apple iPad 3ème génération (version minimale) ou iPad Mini, avec iOS 9.3 (version minimale)

> **Remarque :**
>
> Citrix Endpoint Management ne valide pas les comptes utilisateur ASM auprès de LDAP ou d'Active Directory. Toutefois, vous pouvez connecter Citrix Endpoint Management à LDAP ou Active Directory pour la gestion des utilisateurs et des appareils non liés à des instructeurs ou des étudiants ASM. Par exemple, vous pouvez utiliser Active Directory pour fournir Citrix Secure Mail et Citrix Secure Web à d'autres membres d'ASM, tels que les administrateurs et responsables informatiques.
>
> Étant donné que les étudiants et les instructeurs ASM sont des utilisateurs locaux, il n'est pas nécessaire de déployer Citrix Secure Hub sur leurs appareils.
>
> L'inscription MAM qui comprend l'authentification NetScaler Gateway ne prend pas en charge les utilisateurs locaux (uniquement les utilisateurs Active Directory). Par conséquent, Citrix Endpoint Management déploie uniquement les applications et iBooks d'achat en volume requis sur les appareils des instructeurs et des étudiants.

Application En classe pour iPad

L'application En classe pour iPad permet aux enseignants de se connecter aux appareils des étudiants et de les gérer. Vous pouvez afficher les écrans de l'appareil, ouvrir des applications sur les iPads,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

partager et ouvrir des liens Web et présenter un écran d'étudiant sur Apple TV.

L'application En classe est gratuite dans l'App Store. Chargez l'application sur la console Citrix Endpoint Management. Utilisez ensuite la stratégie Configuration de l'éducation pour configurer l'application En classe, que vous déployez sur les appareils des enseignants.

Pour plus d'informations sur le déploiement de l'application En classe, reportez-vous à la section Distribuer les applications Apple.

Pour plus d'informations sur la configuration requise, l'installation et les fonctionnalités de l'application En classe, consultez Guide de l'utilisateur d'En classe sur le site d'assistance d'Apple.

Ajouter des mots de passe pour les utilisateurs Apple School Manager

Après l'ajout d'un compte ASM, Citrix Endpoint Management importe les classes et les utilisateurs à partir d'ASM. Citrix Endpoint Management traite les classes en tant que groupes locaux et utilise le terme « groupe » dans la console. Si une classe a un nom de groupe dans ASM, Citrix Endpoint Management lui attribue le nom du groupe. Sinon, Citrix Endpoint Management utilise l'ID du système source pour le nom du groupe. Citrix Endpoint Management n'utilise pas le nom du cours comme nom de classe, car les noms de cours dans ASM ne sont pas uniques.

Citrix Endpoint Management utilise les identifiants Apple ID gérés pour créer des utilisateurs locaux avec le type utilisateur **ASM**. Les utilisateurs sont locaux, car ASM crée les informations d'identification indépendamment de toutes les sources de données externes. Par conséquent, Citrix Endpoint Management n'utilise pas de serveur d'annuaire pour authentifier ces nouveaux utilisateurs.

ASM n'envoie pas de mots de passe utilisateur temporaires à Citrix Endpoint Management. Vous pouvez les importer à partir d'un fichier CSV ou les ajouter manuellement. Pour importer des mots de passe utilisateur temporaires :

1. Obtenez le fichier CSV généré par ASM lorsque vous créez les mots de passe temporaires d'identifiants Apple ID gérés.
2. Modifiez le fichier CSV, en remplaçant les mots de passe temporaires par les nouveaux mots de passe que fournissent les utilisateurs pour s'inscrire à Citrix Endpoint Management. Il n'existe aucune contrainte sur le type de mot de passe dans ce cas.

   Le format d'une entrée dans le fichier CSV est le suivant : `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`

   Où :

   Utilisateur : `user@appleid.citrix.com`

   Prénom : `Firstname`

   Deuxième prénom : `Middle`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

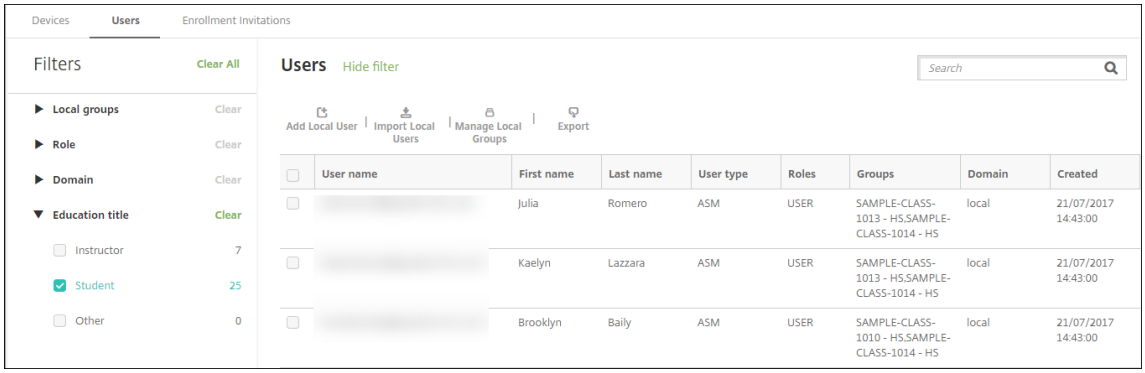
Nom : `Lastname`

Mot de passe : `Password123`!

3. Dans la console Citrix Endpoint Management, cliquez sur **Gérer > Utilisateurs**. La page **Utilisateurs** s'affiche.

   L'écran **Gérer > Utilisateurs** suivant présente un exemple de liste d'utilisateurs importée à partir d'ASM. Dans la liste **Utilisateurs** :

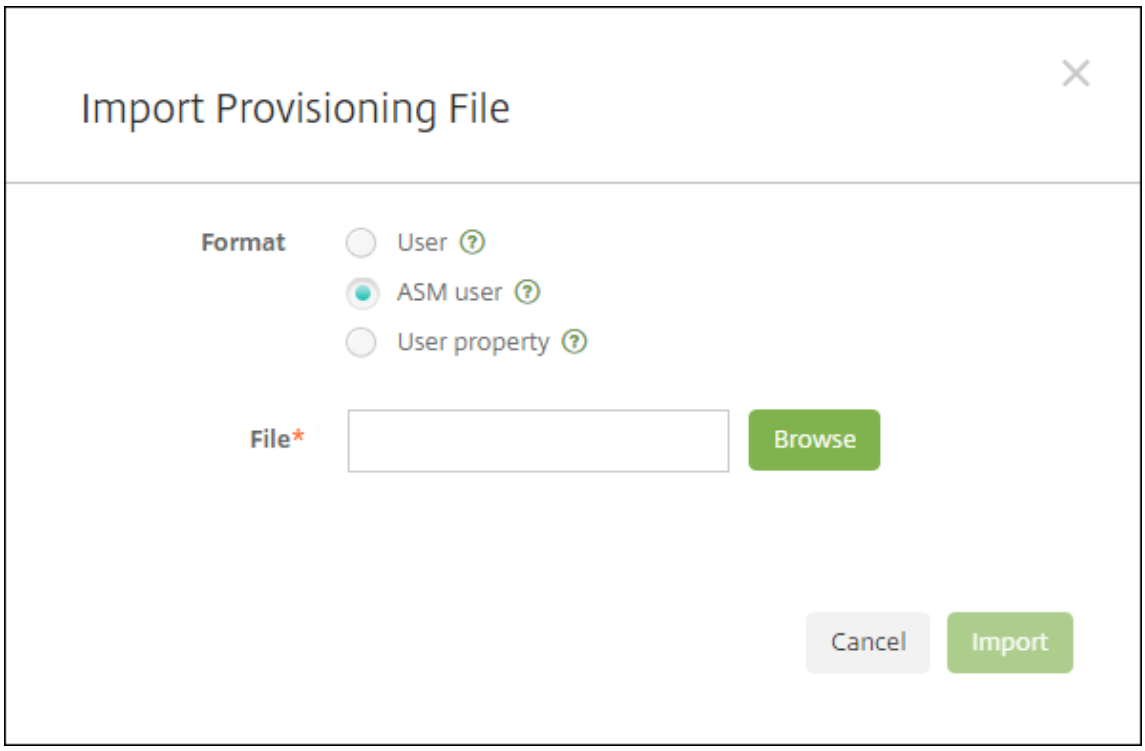
   - L'option **Nom d'utilisateur** affiche l'identifiant Apple ID géré.
   - Le type d'utilisateur est **ASM** pour indiquer que le compte provient d'ASM.
   - L'option **Groupes** indique les classes.



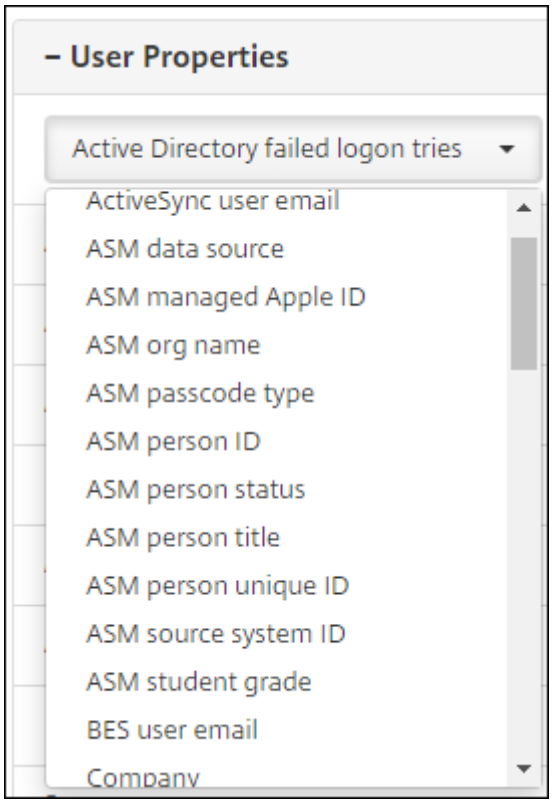
4. Cliquez sur **Importer des utilisateurs locaux**. La boîte de dialogue **Importer le fichier de provisioning** apparaît.

5. Pour le format, choisissez **Utilisateur ASM**, naviguez jusqu'au fichier CSV que vous avez préparé à l'étape 2, puis cliquez sur **Importer**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Pour afficher les propriétés d'un utilisateur local, sélectionnez l'utilisateur, puis cliquez sur **Modifier**.



Outre les propriétés de nom, ces propriétés ASM sont également disponibles :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Source de données ASM :** source de données de la classe, telle que **CSV** ou **SFTP**.
- **Identifiant Apple géré par ASM :** un identifiant Apple ID géré peut inclure le nom de votre établissement et votre `appleid`. Par exemple, l'identifiant peut ressembler à johnappleseed@appleid.myschool.edu. Citrix Endpoint Management requiert un identifiant Apple ID géré pour l'authentification.
- **Nom de l'organisation ASM :** nom que vous avez donné au compte dans Citrix Endpoint Management.
- **Type de code d'accès ASM :** stratégie de mot de passe de la personne : **complexe** (mot de passe de huit chiffres et lettres ou plus pour un non-étudiant), **quatre** (chiffres) ou **six** (chiffres).
- **Identifiant unique de l'étudiant ASM :** identifiant de l'utilisateur.
- **Statut de l'étudiant :** spécifie si l'identifiant Apple ID géré est **Actif** ou **Inactif**. Ce statut devient actif une fois que l'utilisateur fournit un nouveau mot de passe pour le compte Apple ID géré.
- **Titre de l'étudiant ASM :** Instructeur, Étudiant ou Autre.
- **Identifiant unique de l'étudiant ASM :** identifiant unique de l'utilisateur.
- **Identifiant du système source ASM :** identifiant de la source système.
- **Niveau scolaire de l'étudiant ASM :** informations sur le niveau scolaire de l'étudiant (non utilisé par les instructeurs).

Planifier et ajouter des ressources et des groupes de mise à disposition à Citrix Endpoint Management

Un groupe de mise à disposition spécifie les ressources à déployer vers des catégories d'utilisateurs. Par exemple, vous pouvez créer un groupe de mise à disposition pour instructeurs et étudiants. Éventuellement, vous pouvez créer plusieurs groupes de mise à disposition afin de pouvoir personnaliser les applications, le contenu multimédia et les stratégies envoyés vers différents instructeurs ou étudiants. Vous pouvez créer un ou plusieurs groupes de mise à disposition par classe. Vous pouvez également créer un ou plusieurs groupes de mise à disposition pour les responsables (autre personnel dans votre établissement scolaire).

Les ressources que vous déployez sur les appareils utilisateur comprennent les stratégies d'appareil, les applications d'achat en volume et les iBooks.

- Stratégies d'appareil :

  Si les instructeurs utilisent l'application En classe, la stratégie Configuration de l'éducation est requise. Veillez à consulter les autres stratégies d'appareil pour déterminer la manière dont vous souhaitez configurer et limiter les iPad des instructeurs et des étudiants.

- Applications d'achat en volume :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Endpoint Management requiert le déploiement des applications d'achat en volume en tant qu'applications requises pour les utilisateurs Éducation. Citrix Endpoint Management ne prend pas en charge le déploiement de telles applications d'achat en volume en mode facultatif.

Si vous utilisez l'application En classe d'Apple, déployez-la uniquement sur les appareils des instructeurs.

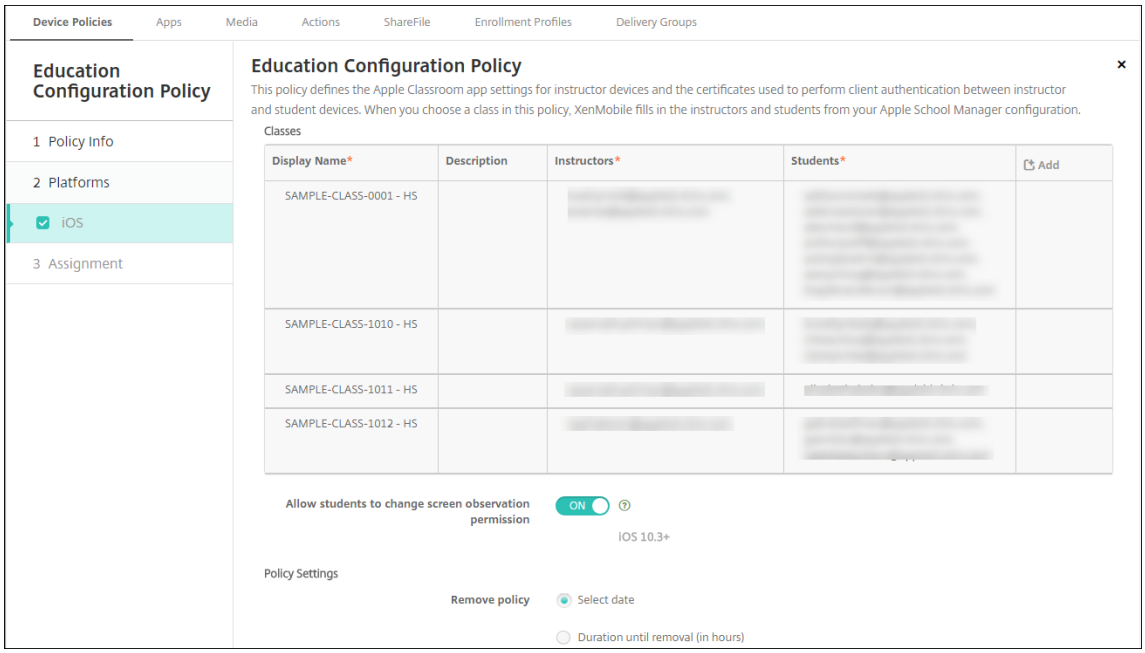
Déployez toute autre application que vous souhaitez fournir aux instructeurs ou aux étudiants. Cette solution n'utilisant pas l'application Citrix Secure Hub, il n'est pas nécessaire de la déployer vers les instructeurs ou les étudiants.

- iBooks d'achat en volume :

  Une fois qu'Citrix Endpoint Management s'est connecté à votre compte ASM, vos iBooks achetés s'affichent dans la console Citrix Endpoint Management, dans **Configurer > Média**. Les iBooks répertoriés sur cette page peuvent être ajoutés aux groupes de mise à disposition. Citrix Endpoint Management prend en charge l'ajout d'iBooks en tant que média requis uniquement.

Après avoir planifié les ressources et les groupes de mise à disposition pour les instructeurs et les étudiants, vous pouvez créer ces éléments dans la console Citrix Endpoint Management.

1. Créez les stratégies d'appareil que vous voulez déployer sur les appareils des instructeurs ou des étudiants. Pour de plus amples informations sur la stratégie Configuration de l'éducation, consultez la section Stratégie Configuration de l'éducation.



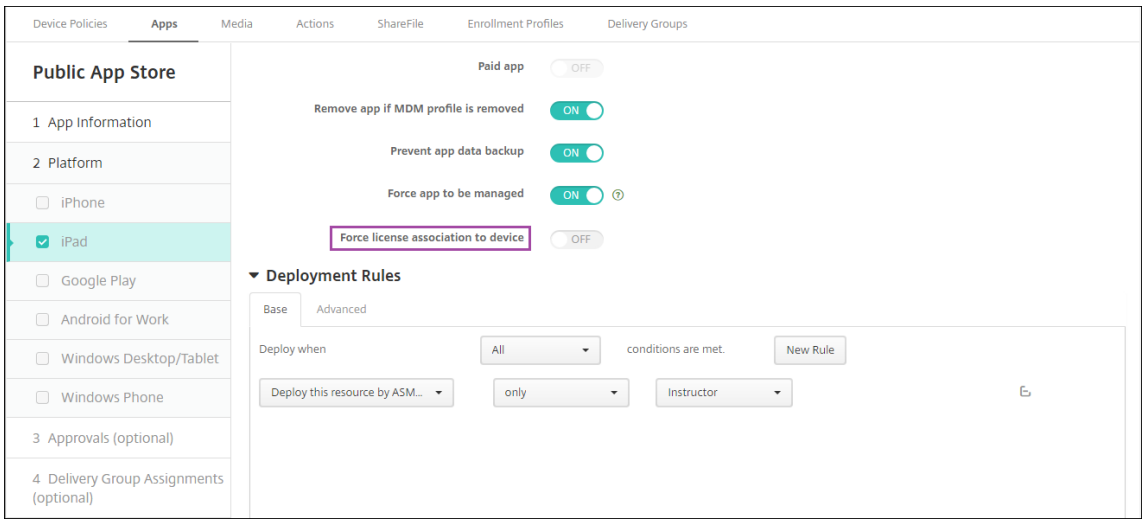
   Consultez la section Stratégies d'appareil et les articles de stratégies individuels pour de plus amples informations sur les stratégies d'appareil.

2. Configurez les applications (**Configurer > Applications**) et les iBooks (**Configurer > Média**) :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Par défaut, Citrix Endpoint Management attribue les applications et les iBooks au niveau de l'utilisateur. Lors du premier déploiement, les instructeurs et les étudiants sont invités à s'enregistrer auprès d'ASM. Après avoir accepté l'invitation, les utilisateurs reçoivent leurs applications et iBooks ASM au cours du déploiement suivant (dans les six heures). Citrix vous recommande de forcer le déploiement d'applications et d'iBooks vers les nouveaux utilisateurs ASM. Pour ce faire, sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.

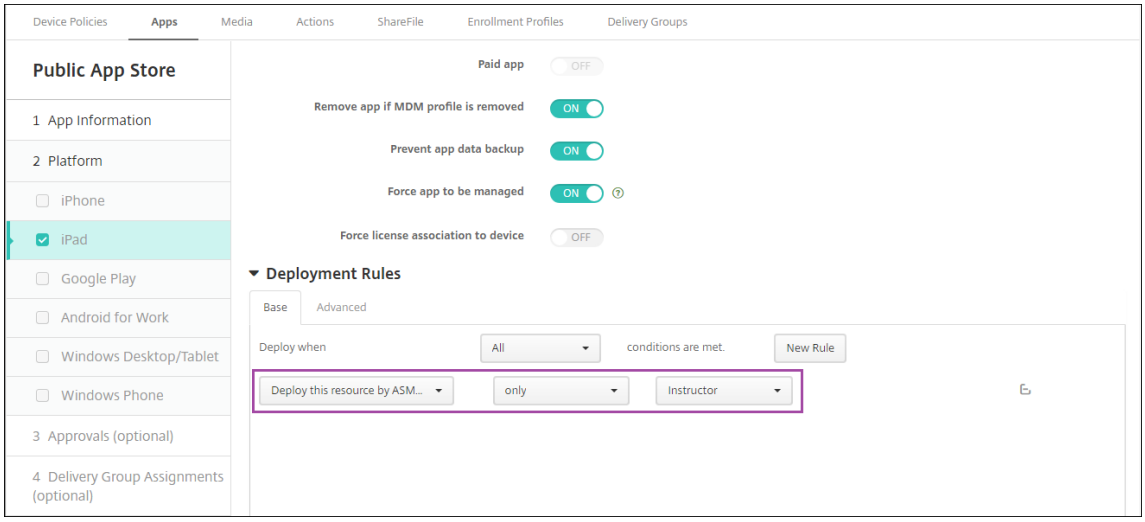
  Vous pouvez choisir d'attribuer des applications (mais pas des iBooks) au niveau de l'appareil. Pour ce faire, réglez le paramètre **Forcer l'association de licence avec l'appareil** sur **Activé**. Lorsque vous attribuez les applications au niveau de l'appareil, les utilisateurs ne reçoivent pas d'invitation à rejoindre le programme d'achat en volume.



- Pour déployer une application uniquement vers les instructeurs, sélectionnez un groupe de mise à disposition qui comprend uniquement des instructeurs ou utilisez la règle de déploiement suivante :

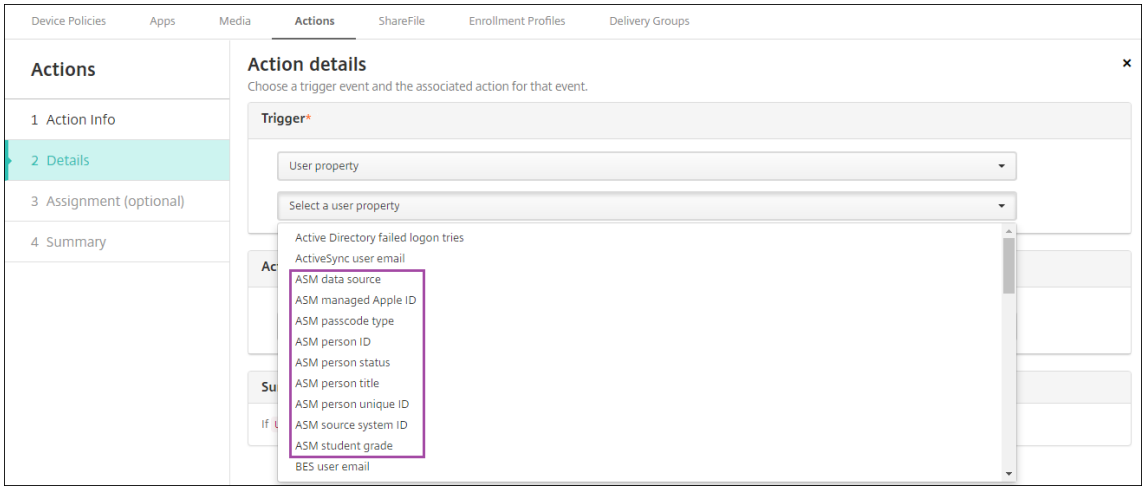
```
Deploy this resource by ASM device type
only
Instructor
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Pour obtenir de l'aide sur l'ajout d'applications d'achat en volume, consultez la section Ajouter une application d'un magasin d'applications public.

3. Facultatif. Créez des actions basées sur les propriétés utilisateur ASM. Par exemple, vous pouvez créer une action pour envoyer une notification aux appareils des étudiants lorsqu'une nouvelle application est installée. Éventuellement, vous pouvez créer une action que déclenche une propriété utilisateur, comme illustré dans l'exemple suivant.



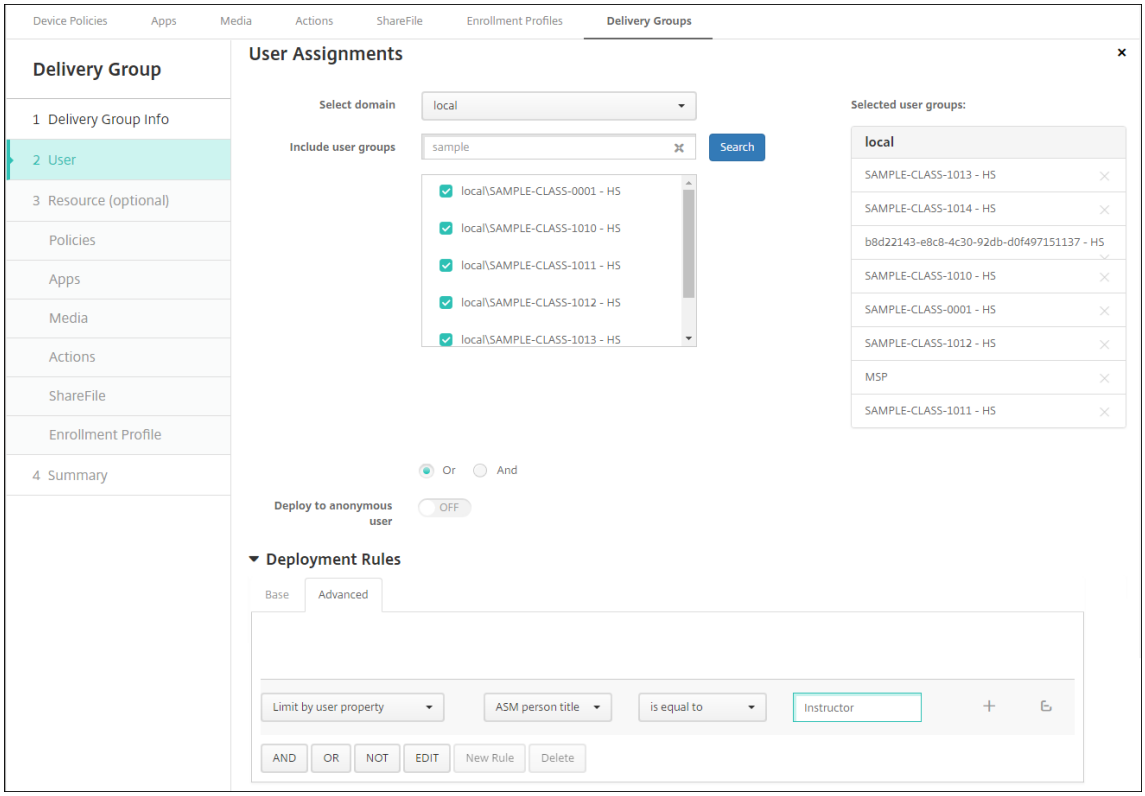
Pour créer une action, accédez à **Configurer > Actions**. Pour de plus amples informations sur la configuration des actions, consultez la section Actions automatisées.

4. Dans **Configurer > Groupes de mise à disposition**, créez des groupes de mise à disposition pour instructeurs et étudiants. Choisissez les classes importées depuis ASM. Créez aussi une règle de déploiement pour instructeurs et étudiants.

   Par exemple, les affectations utilisateur suivantes sont destinées aux instructeurs. La règle de déploiement est la suivante :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

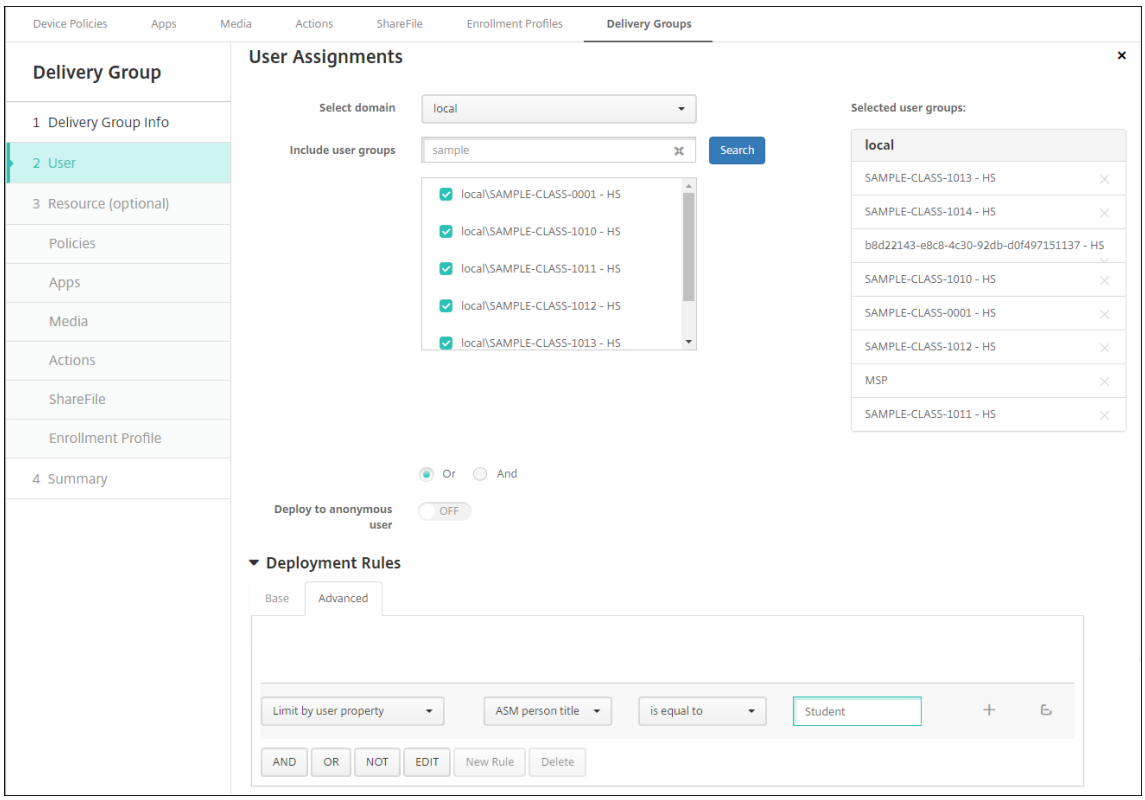
```
Limit by user property
ASM person title
is equal to
Instructor
<!--NeedCopy-->
```



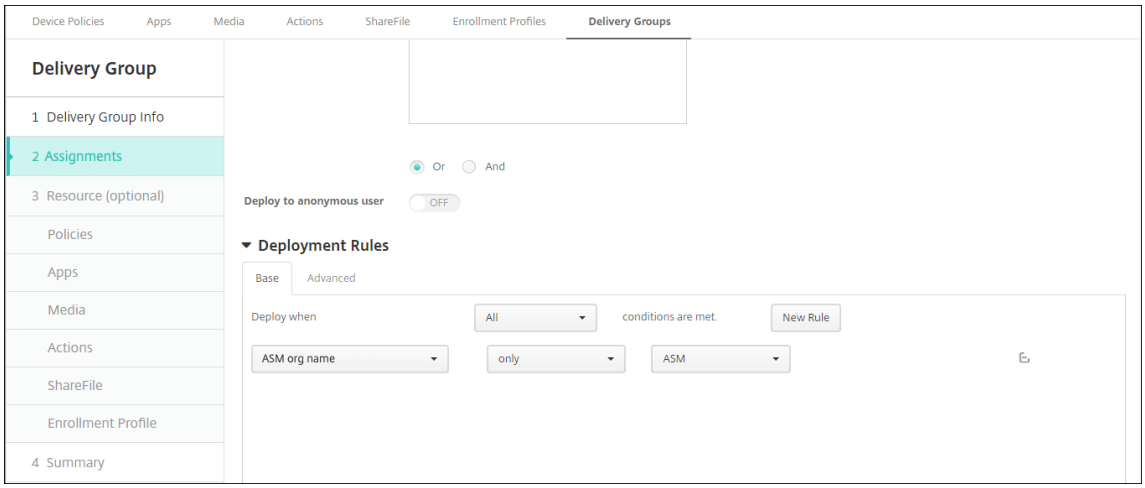
Les affectations utilisateur suivantes sont destinées aux étudiants. La règle de déploiement est la suivante :

```
Limit by user property
ASM person title
is equal to
Student
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

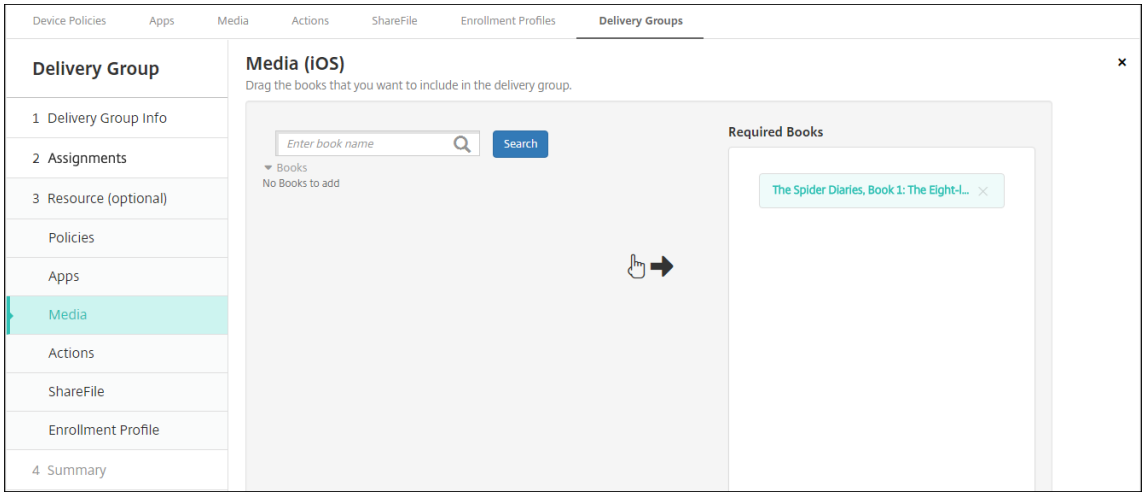


Vous pouvez également filtrer un groupe de mise à disposition à l'aide d'une règle de déploiement basée sur le nom de l'organisation ASM.

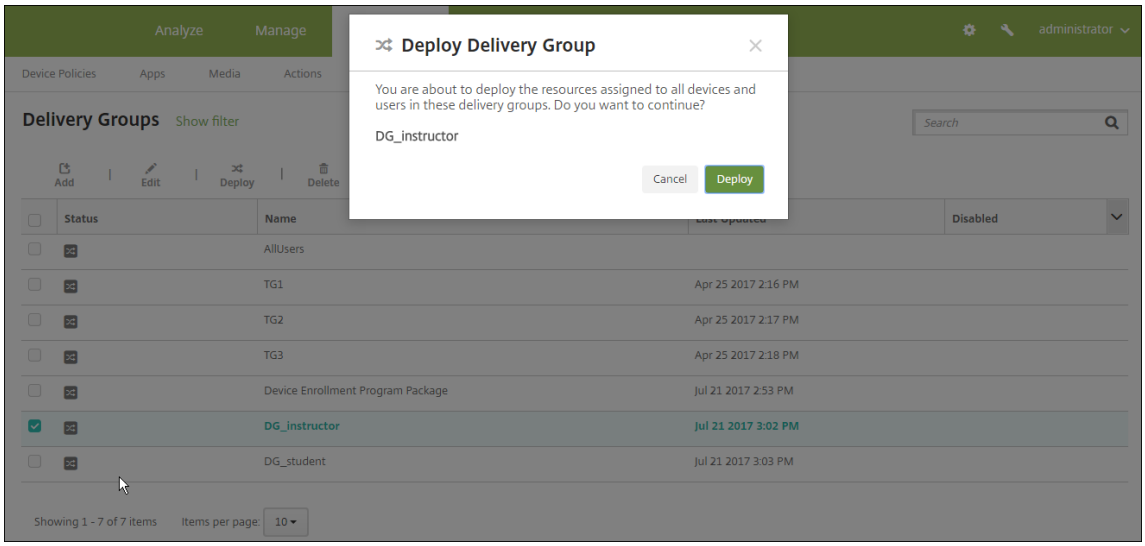


5. Attribuez les ressources à des groupes de mise à disposition. L'exemple suivant illustre un iBook contenu dans un groupe de mise à disposition.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



L'exemple suivant illustre la boîte de dialogue de confirmation qui s'affiche lorsque vous sélectionnez un groupe de mise à disposition et cliquez sur **Déployer**.



Pour plus d'informations, consultez la section « Pour modifier un groupe de mise à disposition » et « Pour déployer des groupes de mise à disposition » dans Déployer des ressources.

Tester les inscriptions d'appareil instructeur et étudiant

Vous pouvez inscrire des appareils avec une des méthodes suivantes :

- Un administrateur d'établissement scolaire peut inscrire des appareils instructeur et étudiant en utilisant le mot de passe utilisateur que vous pouvez définir dans la console Citrix Endpoint Management. Par conséquent, vous pouvez fournir aux utilisateurs des appareils qui sont déjà configurés avec les applications et les médias.
- Lorsque les utilisateurs reçoivent les appareils, ils peuvent s'inscrire à l'aide du mot de passe

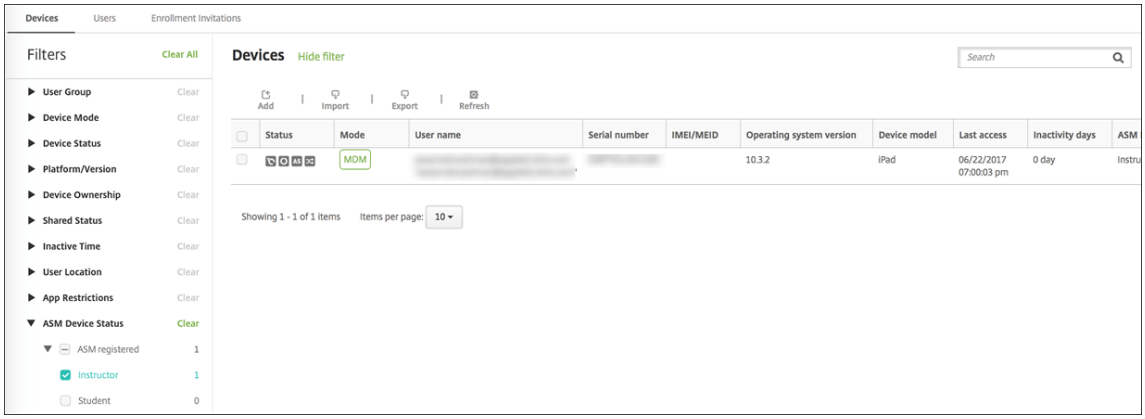
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

utilisateur que vous leur fournissez. Une fois l'inscription terminée, Citrix Endpoint Management envoie les stratégies d'appareil, les applications et le contenu multimédia aux appareils.

Pour tester l'inscription, utilisez les appareils du programme de déploiement d'Apple liés à ASM.

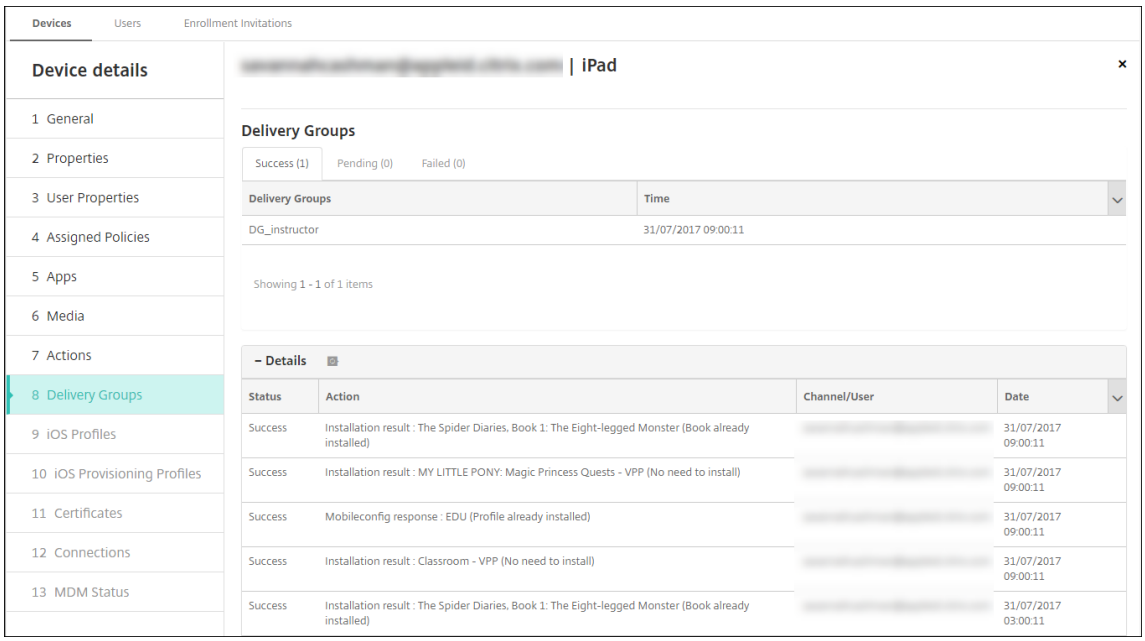
1. Si les appareils ne sont pas liés à ASM, vous devez effacer leur contenu et leurs paramètres en effectuant une réinitialisation matérielle.
2. Inscrivez un appareil ASM auprès d'un instructeur. Inscrivez ensuite un appareil ASM auprès d'un étudiant.
3. Sur la page **Gérer > Appareils**, vérifiez que les deux appareils ASM sont inscrits dans MDM uniquement.

   Vous pouvez filtrer la page **Appareils** en fonction de l'état de l'appareil ASM : **Enregistré auprès de ASM**, **Partagé avec ASM**, **Instructeur** et **Étudiant**.



4. Pour vérifier que les ressources MDM ont été déployées correctement pour chaque appareil : sélectionnez l'appareil, cliquez sur **Modifier** et vérifiez les différentes pages.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Distribuer des appareils

Apple vous recommande d'organiser un événement de façon à distribuer les appareils à des instructeurs et à des étudiants.

Si vous ne distribuez pas d'appareils pré-inscrits, vous devez également fournir les éléments suivants à ces utilisateurs :

- Mots de passe Citrix Endpoint Management pour l'inscription
- Mots de passe temporaires ASM pour les identifiants Apple ID gérés

La première expérience utilisateur se présente comme suit.

1. La première fois qu'un utilisateur démarre son appareil après une réinitialisation matérielle, Citrix Endpoint Management l'invite dans l'écran d'inscription à inscrire son appareil.
2. L'utilisateur fournit l'identifiant Apple ID géré et le mot de passe Citrix Endpoint Management qu'il a utilisés pour s'authentifier auprès d'Citrix Endpoint Management.
3. Dans l'étape de configuration de l'identifiant Apple ID, l'appareil invite l'utilisateur à entrer son identifiant Apple ID géré et son mot de passe temporaire ASM. Ces éléments authentifient l'utilisateur auprès des services d'Apple.
4. L'appareil invite l'utilisateur à créer un mot de passe pour son Apple ID géré, utilisé pour protéger ses données dans iCloud.
5. À la fin de l'Assistant d'installation, Citrix Endpoint Management démarre l'installation de stratégies, d'applications et de contenu multimédia sur l'appareil. Pour les applications et

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

iBooks attribués au niveau de l'utilisateur, l'assistant invite les instructeurs et les étudiants à s'enregistrer pour l'achat en volume. Après avoir accepté l'invitation, les utilisateurs reçoivent leurs applications et iBooks d'achat en volume au cours du déploiement suivant (dans les six heures).

Gérer les données des instructeurs, des étudiants et de la classe

Lors de la gestion des données des instructeurs, des étudiants et de la classe, notez ce qui suit :

- Ne modifiez pas les identifiants Apple ID gérés après avoir importé des informations ASM dans Citrix Endpoint Management. Citrix Endpoint Management utilise également les identifiants d'utilisateur ASM pour identifier les utilisateurs.
- Si vous ajoutez ou modifiez des données de classe dans ASM une fois que vous avez créé une ou plusieurs stratégies Configuration de l'éducation : modifiez les stratégies, puis redéployez-les.
- Si l'instructeur d'une classe change après le déploiement de la stratégie Configuration de l'éducation : vérifiez que la stratégie se met bien à jour dans la console Citrix Endpoint Management, puis redéployez-la.
- Si vous mettez à jour les propriétés utilisateur dans le portail ASM, Citrix Endpoint Management met également à jour ces propriétés dans la console. Toutefois, Citrix Endpoint Management ne reçoit pas la propriété de fonction de la personne ASM (Instructeur, Étudiant ou Autre) de la même manière que les autres propriétés. Par conséquent, si vous modifiez la fonction de la personne ASM dans ASM, procédez comme suit pour refléter cette modification dans Citrix Endpoint Management.

Pour gérer les données :

1. Dans le portail ASM, mettez à jour le niveau scolaire de l'étudiant et effacez le niveau scolaire de l'instructeur.
2. Si vous avez transformé un compte étudiant en compte instructeur, supprimez l'utilisateur de la liste des étudiants de la classe. Ensuite, ajoutez l'utilisateur à la liste des instructeurs dans la même classe ou une autre.

   Si vous avez modifié un compte instructeur vers un compte étudiant, supprimez l'utilisateur de la classe. Ensuite, ajoutez l'utilisateur à la liste des étudiants dans la même classe ou une autre. Vos mises à jour s'affichent dans la console Citrix Endpoint Management lors de la prochaine synchronisation (toutes les cinq minutes par défaut) ou récupération (par défaut, toutes les 24 heures).
3. Modifiez la stratégie Configuration de l'éducation pour appliquer la modification et redéployez-la.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si vous supprimez un utilisateur du portail ASM, Citrix Endpoint Management supprime également cet utilisateur de la console Citrix Endpoint Management après une récupération.

  Vous pouvez réduire l'intervalle de ligne de base en modifiant la valeur de cette propriété de serveur : **bulk.enrollment.fetchRosterInfoDelay** (la valeur par défaut est **1440** minutes).

- Lorsque vous déployez des ressources : si un étudiant rejoint une classe, créez un groupe de mise à disposition avec cet étudiant uniquement et déployez les ressources vers l'étudiant.

- Si un étudiant ou un instructeur perd son mot de passe temporaire, demandez-lui de contacter l'administrateur ASM. L'administrateur peut fournir le mot de passe temporaire ou en générer un nouveau.

Gérer un appareil perdu ou volé

Le service Localiser mon iPhone/iPad d'Apple comprend une fonctionnalité de verrouillage d'activation. Le verrouillage d'activation empêche les utilisateurs non autorisés d'utiliser ou de revendre un appareil perdu ou volé qui est inscrit au programme de déploiement d'Apple.

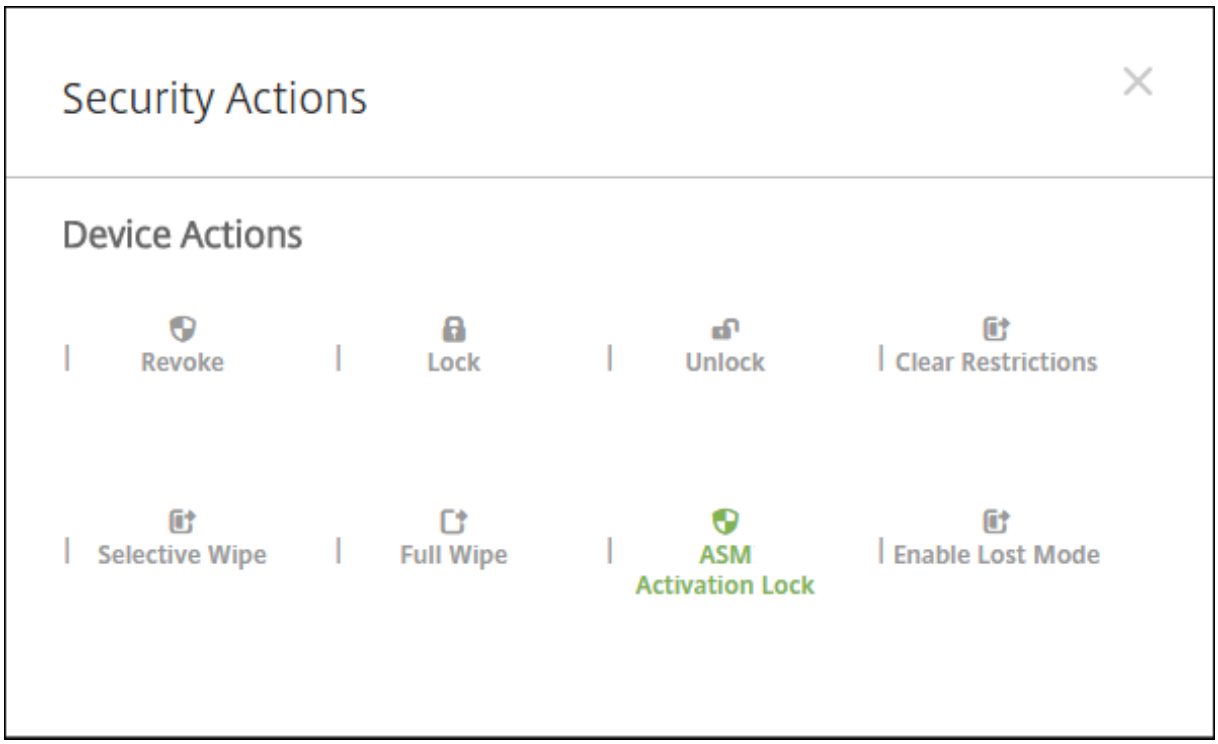
Citrix Endpoint Management comprend une action de sécurité **Verrouillage d'activation ASM** qui vous permet d'envoyer un code de verrouillage à un appareil inscrit au de déploiement Apple ASM.

Lorsque vous utilisez l'action de sécurité **Verrouillage d'activation ASM**, Citrix Endpoint Management peut localiser les appareils sans obliger les utilisateurs à activer le service Localiser mon iPhone/iPad. Lors d'une réinitialisation matérielle ou d'un effacement complet d'un appareil ASM, l'utilisateur fournit son identifiant Apple ID géré et son mot de passe pour déverrouiller l'appareil.

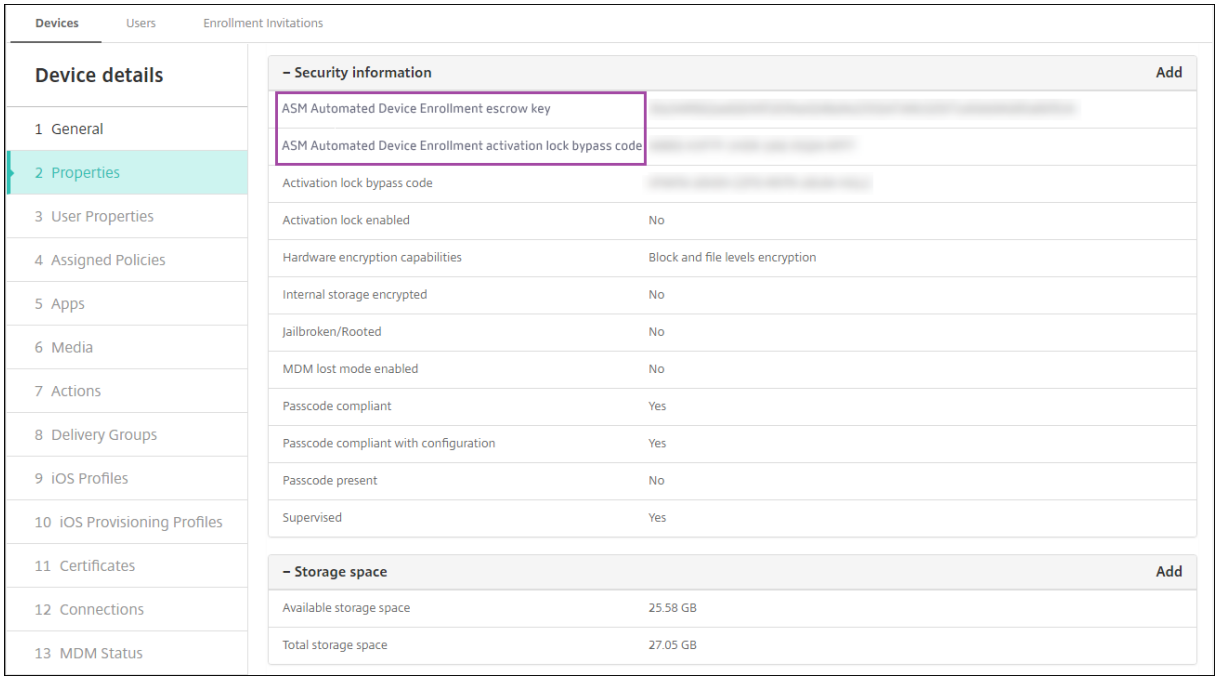
Pour libérer le verrou depuis la console, cliquez sur l'action de sécurité **Contourner le verrouillage d'activation**. Pour plus d'informations sur le contournement d'un verrouillage d'activation, consultez la section Contourner un verrouillage d'activation iOS. L'utilisateur peut également ne pas renseigner les informations de connexion et entrer le **code de contournement du verrouillage d'activation ASM** en tant que mot de passe. Ces informations sont disponibles dans **Détails de l'appareil**, sur l'onglet **Propriétés**.

Pour définir le verrouillage d'activation, accédez à **Gérer > Appareils**, sélectionnez l'appareil, cliquez sur **Sécurité**, puis cliquez sur **Verrouillage d'activation ASM**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

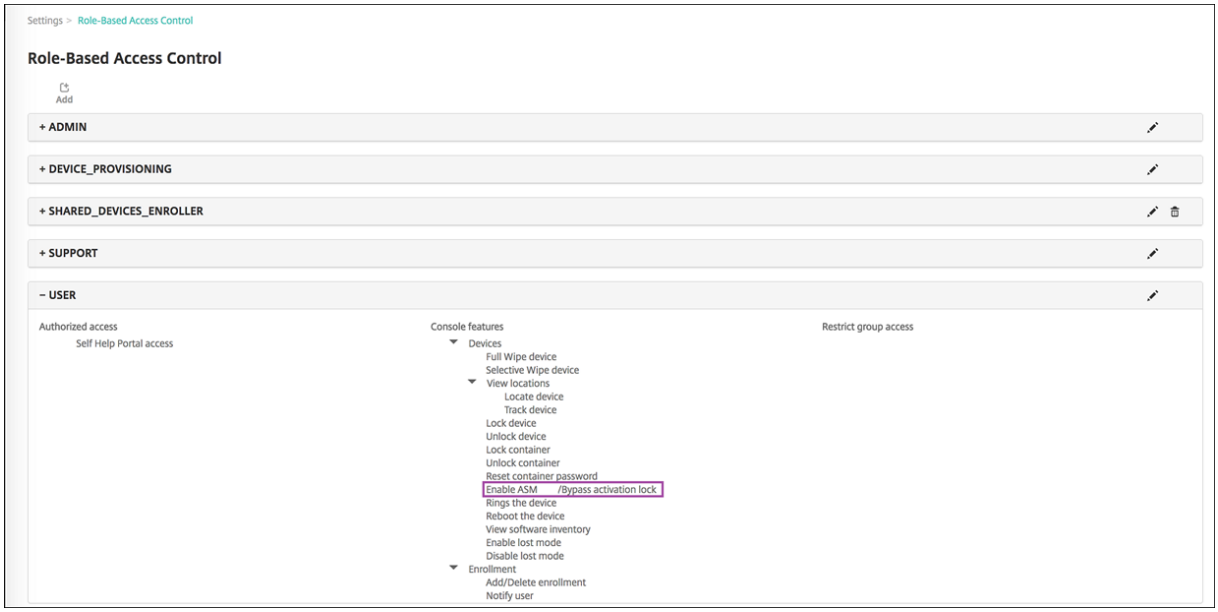


Les propriétés **Dépôt de clé ASM** et **Code de contournement du verrouillage d'activation ASM** s' affichent dans **Détails de l'appareil**.



L'autorisation RBAC pour un verrouillage d'activation ASM est **Appareils > Activer contournement du verrouillage d'activation ASM**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



iPad partagé

November 29, 2023

La fonctionnalité iPad partagé permet à plusieurs utilisateurs d'utiliser un iPad. Les expériences utilisateur peuvent être personnalisées même si les appareils sont partagés. Vous pouvez utiliser des iPad partagés à des fins éducatives ou professionnelles. Apple School Manager (ASM) prend en charge les rôles d'instructeur et d'étudiant en plus des rôles pris en charge par Apple Business Manager (ABM).

Conditions préalables pour les iPad partagés

- Apple School Manager ou Apple Business Manager
- Citrix Endpoint Management
- iPad Pro, iPad 5ème génération, iPad Air 2 ou ultérieur et iPad mini 4 ou ultérieur
- Au moins 32 Go de stockage
- Appareils supervisés

Configurer les iPad partagés

Plusieurs étudiants ou employés peuvent partager un iPad à des fins différentes.

Vous ou les propriétaires de l'appareil inscrivez les iPad partagés, puis déployez des stratégies, des applications et des médias sur ces appareils. Ensuite, les utilisateurs fournissent leurs informations

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

d'identification Apple gérées pour se connecter à un iPad partagé. Si vous avez déjà déployé une stratégie Configuration de l'éducation pour les étudiants, ils ne se connectent plus en tant que « Autre utilisateur » pour partager les appareils.

Citrix Endpoint Management utilise deux canaux de communication pour les iPad partagés : le canal système pour le propriétaire de l'appareil (instructeur ou superviseur) et le canal utilisateur pour l'utilisateur résident actuel (étudiant ou employé). Citrix Endpoint Management utilise ces canaux pour envoyer les commandes MDM appropriées aux ressources prises en charge par Apple.

Les ressources déployées sur le canal système sont les suivantes :

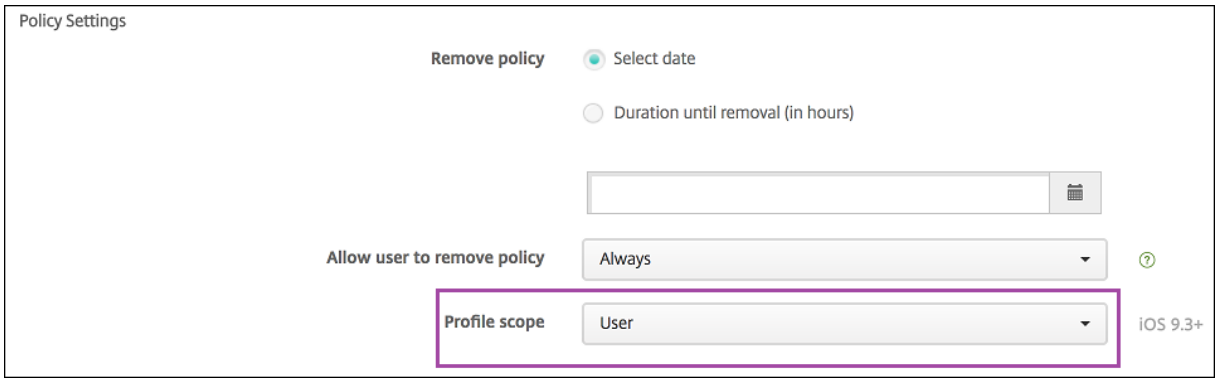
- Stratégies d'appareil, telles que Configuration de l'éducation, Message sur l'écran de verrouillage, Nombre maximal d'utilisateurs résidents et Période de grâce de verrouillage par code secret
- Applications achetées en volume basées sur les appareils
  Apple ne prend pas en charge les applications d'entreprise ni les applications d'achat en volume basées sur les utilisateurs sur les iPad partagés. Les applications installées sur un iPad partagé sont liées à l'appareil et non à l'utilisateur.
- Achat en volume basé sur l'utilisateur iBooks
  Apple prend en charge l'attribution d'iBooks achetés en volume basés sur l'utilisateur sur les iPad partagés.

Les ressources déployées sur le canal utilisateur sont les suivantes :

- Stratégies d'appareil : Notifications d'applications, Disposition de l'écran d'accueil, Restrictions et Clip Web

  Citrix Endpoint Management ne prend en charge que ces stratégies d'appareil sur le canal utilisateur.

Lors de la configuration des stratégies d'appareil, vous spécifiez le canal de déploiement dans le paramètre de stratégie **Étendue du profil**.



Pour supprimer les stratégies d'appareil que vous avez déployées sur le canal utilisateur, réglez l'**étendue de déploiement** sur **Utilisateur** pour la stratégie Suppression de profil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Workflow général

En général, vous fournissez des iPad préconfigurés et supervisés partagés aux propriétaires des appareils. Ces personnes distribuent ensuite les appareils aux étudiants ou aux employés. Si vous ne distribuez pas d'iPad partagés pré-inscrits : assurez-vous de fournir aux propriétaires des appareils leurs mots de passe du serveur Citrix Endpoint Management afin qu'ils puissent inscrire leurs appareils.

Le workflow général pour la configuration et l'inscription des iPad partagés est le suivant.

1. Utilisez la console du serveur Citrix Endpoint Management pour ajouter des comptes ASM ou ABM (**Paramètres > Programme de déploiement d'Apple**) avec le **mode partagé** activé. Pour plus d'informations, voir « Gérer les comptes pour les iPad partagés » ci-après.
2. Comme décrit dans cette section, ajoutez les stratégies d'appareil, les applications et le contenu multimédia requis à Citrix Endpoint Management. Attribuez ces ressources à des groupes de mise à disposition.
3. Demandez aux propriétaires des appareils d'effectuer une réinitialisation matérielle sur les iPad partagés. L'écran de gestion à distance pour l'inscription s'affiche.
4. Les propriétaires des appareils inscrivent les iPad partagés.
   Citrix Endpoint Management déploie les ressources configurées sur chaque iPad partagé inscrit. Après un redémarrage automatique, les propriétaires des appareils peuvent partager les appareils avec les utilisateurs. Une page de connexion apparaît sur l'iPad.
5. Un utilisateur de l'appareil saisit son identifiant Apple géré et son mot de passe ASM temporaire. L'iPad partagé s'authentifie auprès d'ASM et invite l'utilisateur à créer un mot de passe ASM. Pour sa prochaine connexion à l'iPad partagé, l'utilisateur de l'appareil fournit le nouveau mot de passe ASM.
6. Un autre utilisateur de l'appareil qui partage l'iPad peut alors se connecter en répétant l'étape précédente.

Gérer les comptes pour les iPad partagés

Si vous utilisez déjà Citrix Endpoint Management avec Apple Education ou Apple Business : un compte ASM/ABM existant est configuré dans Citrix Endpoint Management pour les appareils qui ne sont pas partagés, tels que les appareils utilisés par les propriétaires. Vous pouvez utiliser le même compte ASM/ABM et le même serveur Citrix Endpoint Management pour les appareils partagés et non partagés.

Organiser les iPad partagés en groupes d'appareils

ASM/ABM vous permet d'organiser les appareils en groupes en créant plusieurs serveurs MDM. Lorsque vous attribuez les iPad partagés à un serveur MDM, créez un groupe d'appareils pour chaque groupe d'iPad partagés :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Groupe 1 d'iPad partagés > Serveur MDM du groupe d'appareils 1
- Groupe 2 d'iPad partagés > Serveur MDM du groupe d'appareils 2
- Groupe N d'iPad partagés > Serveur MDM du groupe d'appareils N

Ajouter des comptes ASM pour chaque groupe d'appareils

Lorsque vous créez plusieurs comptes ASM/ABM à partir de la console du serveur Citrix Endpoint Management, vous importez automatiquement des groupes d'iPad partagés :

- Serveur MDM du groupe d'appareils 1 > Compte du groupe d'appareils 1
- Serveur MDM du groupe d'appareils 2 > Compte du groupe d'appareils 2
- Serveur MDM du groupe d'appareils N > Compte du groupe d'appareils N

Les exigences spécifiques aux iPad partagés sont les suivantes :

- Un compte ASM/ABM pour chaque groupe d'appareils avec ces paramètres activés :
  - **Exiger l'inscription des appareils**
  - **Mode supervisé**
  - **Mode partagé**
- Assurez-vous d'utiliser le même **suffixe d'éducation** pour tous les comptes ASM d'un établissement d'enseignement donné.

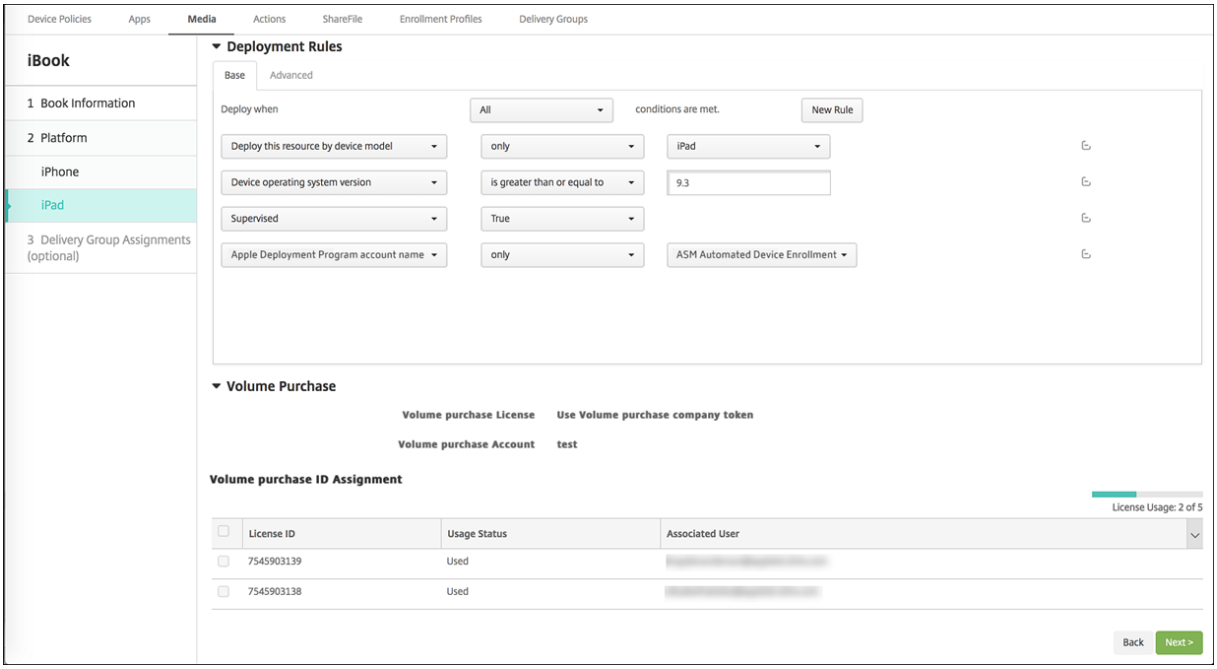
Applications pour iPad partagés

Les iPad partagés prennent en charge l'attribution d'applications d'achat en volume basées sur les appareils. Avant de déployer une application sur un iPad partagé, Citrix Endpoint Management envoie une demande au serveur d'achat en volume d'Apple pour attribuer des licences d'achat en volume aux appareils. Pour vérifier les attributions d'achat en volume, accédez à **Configurer > Applications > iPad** et développez **Achat en volume**.

Médias pour iPad partagés

Les iPad partagés prennent en charge l'attribution d'iBooks achetés en volume basés sur l'utilisateur. Avant de déployer des iBooks sur un iPad partagé, Citrix Endpoint Management envoie une demande au serveur d'achat en volume d'Apple pour attribuer des licences d'achat en volume aux utilisateurs. Pour vérifier les attributions d'achat en volume, accédez à **Configurer > Média > iPad** et développez **Achat en volume**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Règles de déploiement pour iPad partagés

Avec le déploiement d'iPad partagés, les règles au niveau du groupe de mise à disposition ne s'appliquent pas, car elles se rapportent aux propriétés utilisateur. Pour filtrer les stratégies, les applications et les médias pour chaque groupe d'appareils : ajoutez une règle de déploiement pour les ressources en fonction du nom du compte. Par exemple :

- Pour le compte du groupe d'appareils 1, définissez cette règle de déploiement :

```
Apple Deployment Program account name
Only
Device Group 1 account

<!--NeedCopy-->
```

- Pour le compte du groupe d'appareils 2, définissez cette règle de déploiement :

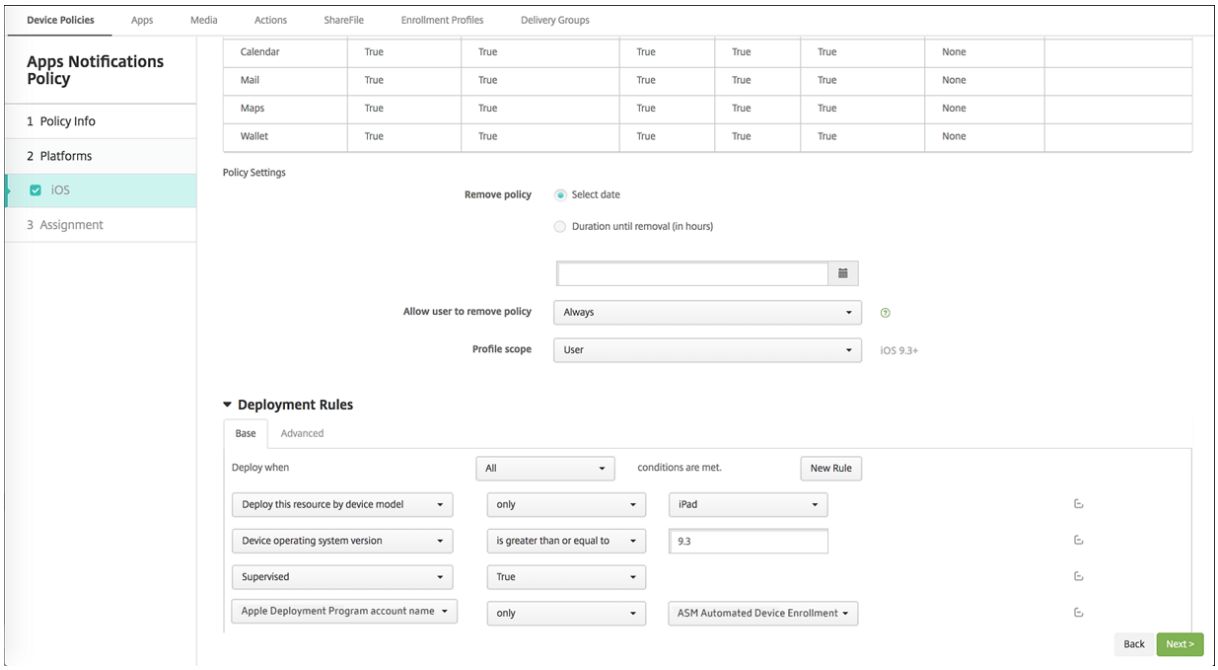
```
Apple Deployment Program account name
Only
Device Group 2 account

<!--NeedCopy-->
```

- Pour le compte du groupe d'appareils N, définissez cette règle de déploiement :

```
Apple Deployment Program account name
Only
Device Group N account
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
4
5    <!--NeedCopy-->
```



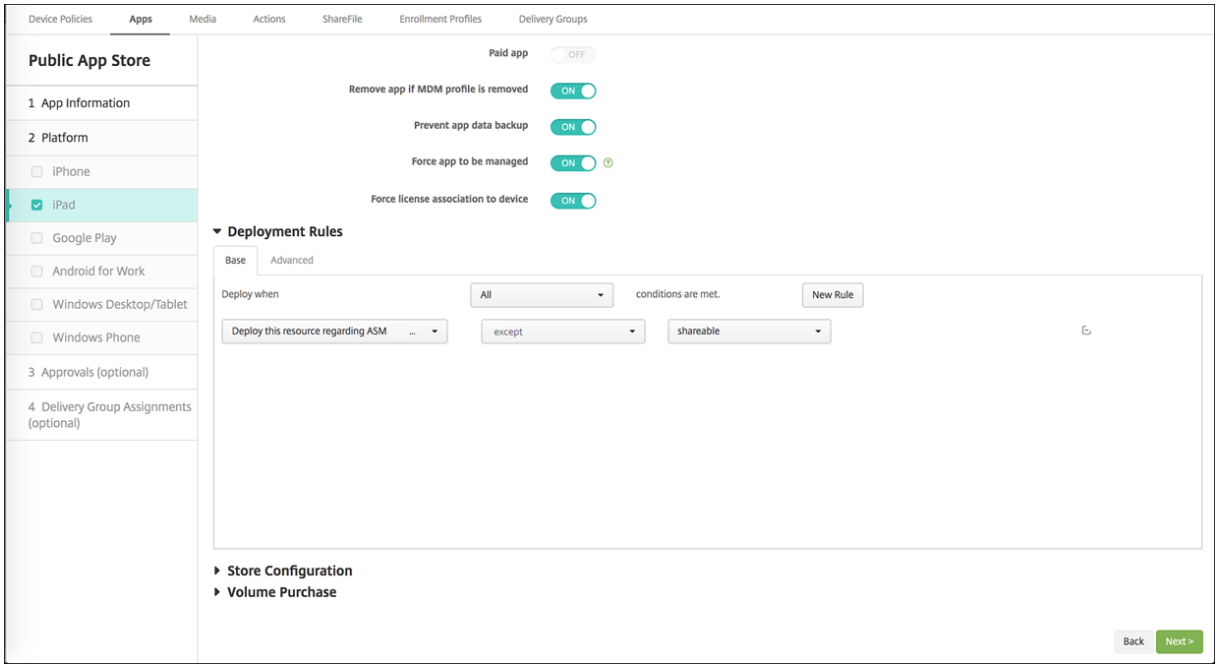
Pour déployer l'application En classe d'Apple uniquement pour les propriétaires des appareils (à l'aide d'iPad non partagés), filtrez les ressources par état partagé ASM avec ces règles de déploiement :

```
1 Deploy this resource regarding ASM/ABM shared mode
2 only
3 unshared
4
5 <!--NeedCopy-->
```

Ou :

```
1 Deploy this resource regarding ASM/ABM shared mode
2 except
3 shareable
4
5 <!--NeedCopy-->
```

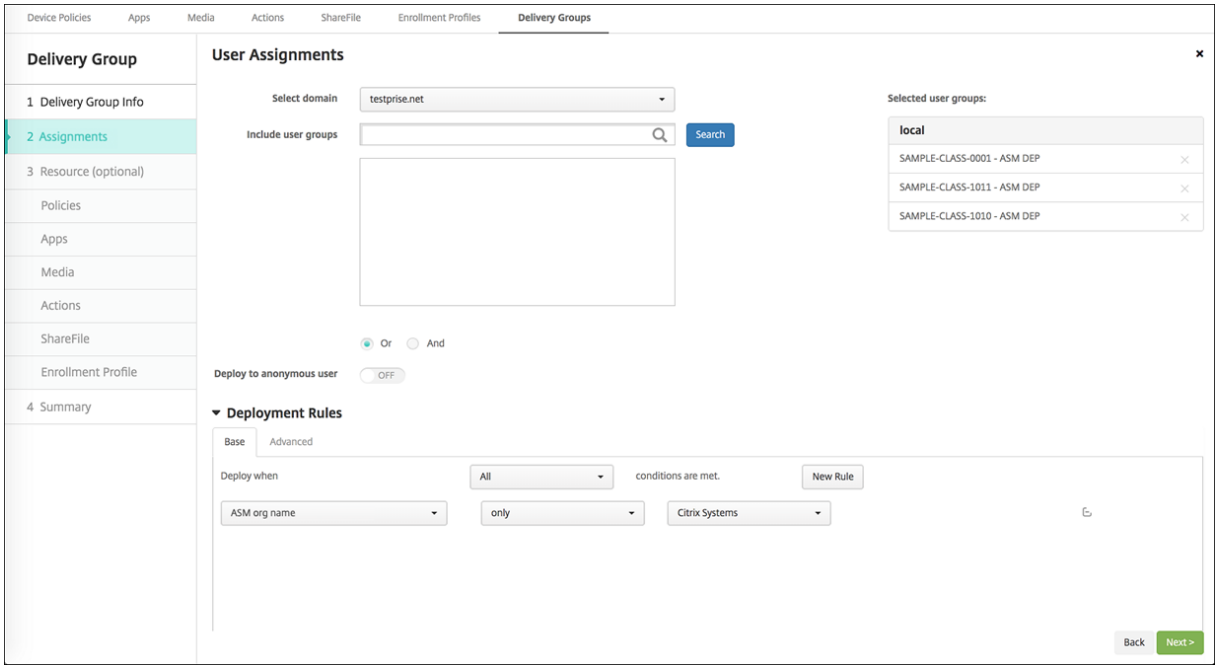
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Groupes de mise à disposition pour iPad partagés

Pour le groupe d'appareils :

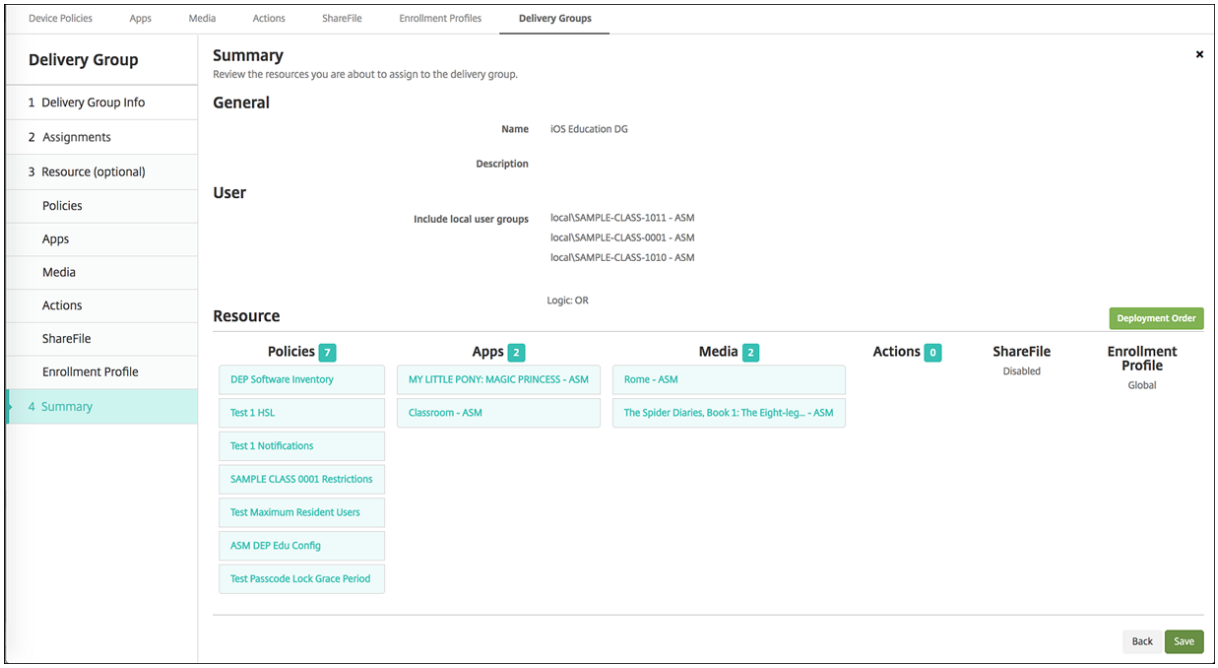
- Configurez un groupe de mise à disposition. Pour l'instructeur, attribuez toutes les classes définies par la stratégie Configuration de l'éducation.



- Ce groupe de mise à disposition doit inclure ces ressources MDM :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Stratégies d'appareil :
  * Configuration de l'éducation (pour ASM)
  * Message sur l'écran de verrouillage
  * Notifications d'applications
  * Disposition de l'écran d'accueil
  * Restrictions
  * Nombre maximal d'utilisateurs résidents
  * Période de grâce de verrouillage par code secret
- Applications achetées en volume requises
- iBooks achetés en volume requis



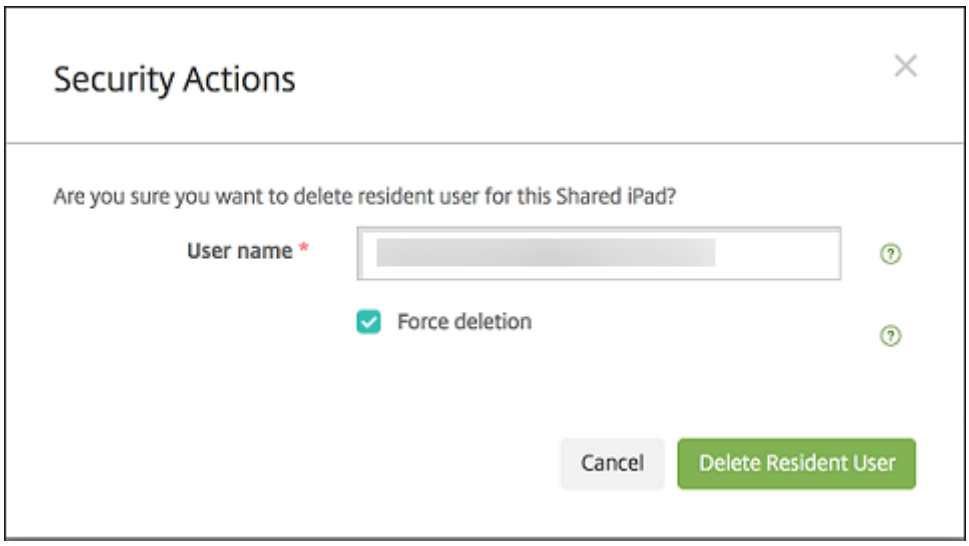
Actions de sécurisation pour iPad partagés

Outre les actions de sécurisation existantes, vous pouvez utiliser ces actions de sécurisation pour les iPad partagés :

- **Obtenir utilisateurs résidents :** répertorie les utilisateurs qui ont des comptes actifs sur l'appareil actuel. Cette action force une synchronisation entre l'appareil et la console Citrix Endpoint Management.
- **Déconnecter utilisateur résident :** force une déconnexion de l'utilisateur actuel.
- **Supprimer utilisateur résident :** supprime la session en cours pour un utilisateur spécifique. L'utilisateur peut se reconnecter.
- **Supprimer tous les utilisateurs :** supprime tous les utilisateurs de l'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Après avoir cliqué sur **Supprimer utilisateur résident**, vous pouvez spécifier le nom d'utilisateur.



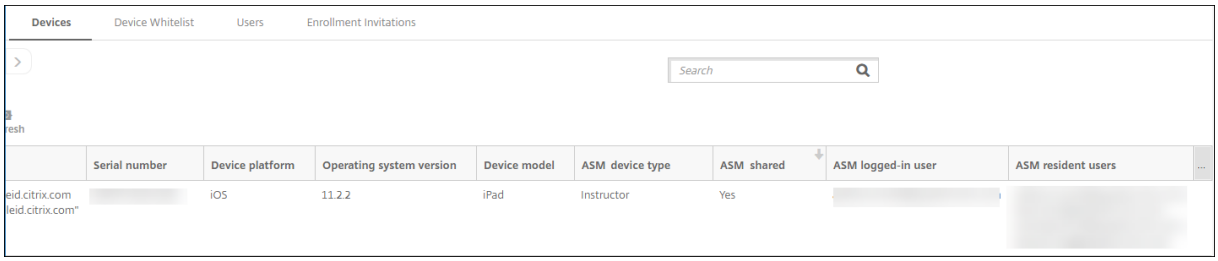
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Les résultats des actions de sécurisation apparaissent sur les pages **Gérer > Appareils > Général** et **Gérer > Appareils > Groupes de mise à disposition**.

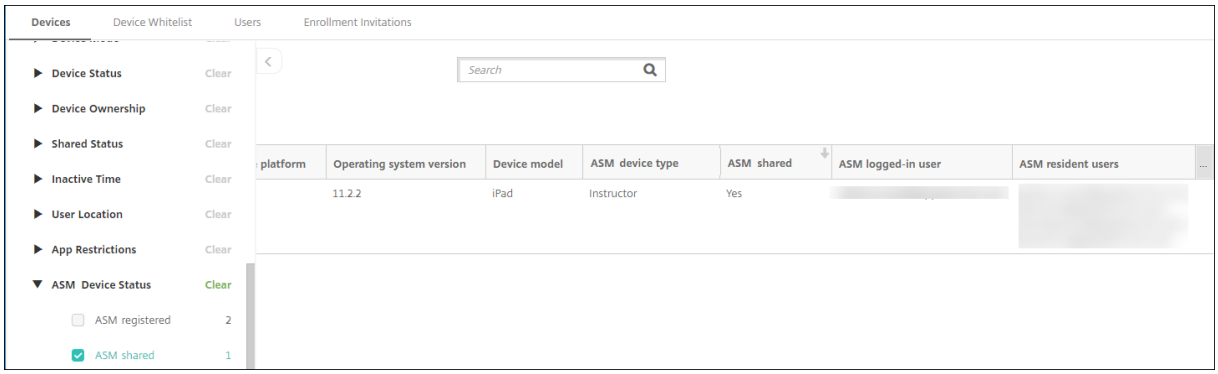
Obtenir des informations sur les iPad partagés

Vous trouverez des informations spécifiques aux iPad partagés sur la page **Gérer > Appareils** :

- Vous pouvez vérifier :
  - si un appareil est partagé (**Partagé avec ASM/ABM**) ;
  - qui est connecté à l'appareil partagé (**utilisateur ASM/ABM connecté**) ;
  - tous les utilisateurs attribués à l'appareil partagé (**utilisateurs résidents ASM/ABM**)

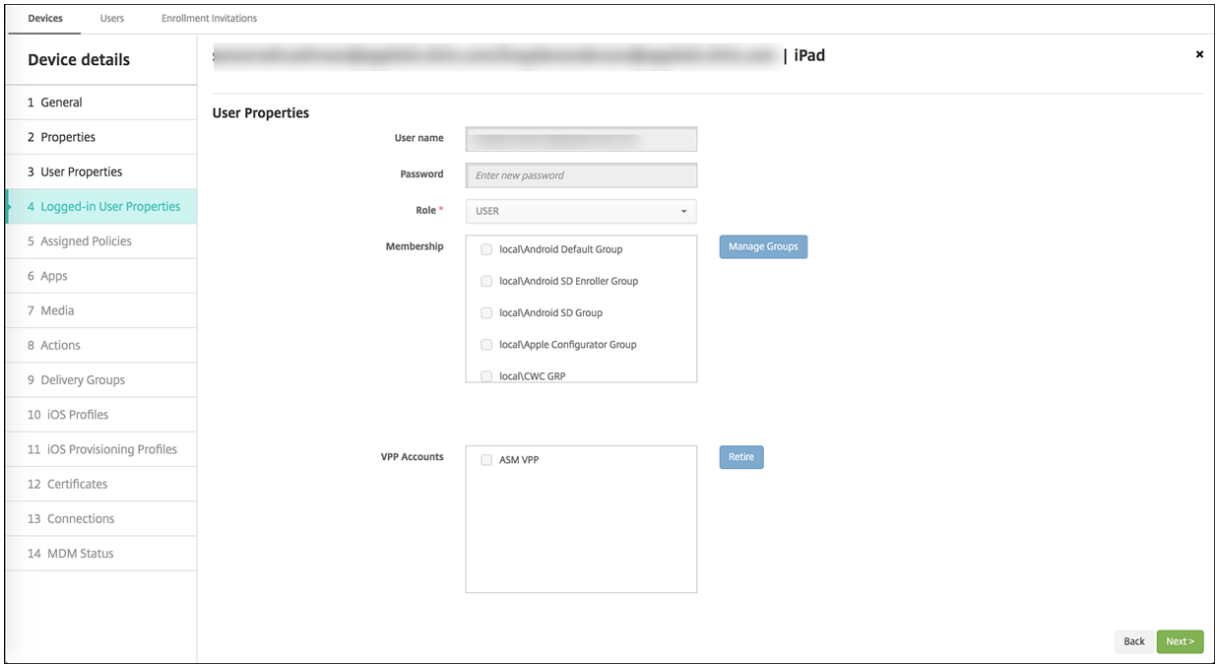


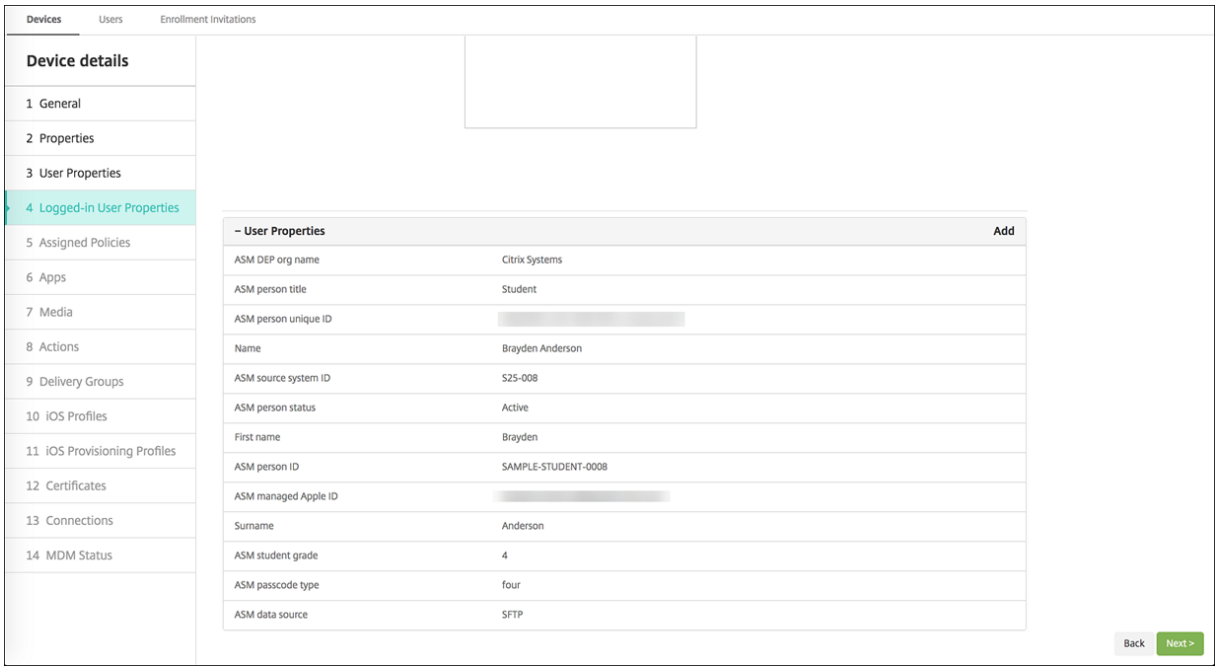
- Filtrez la liste des appareils en fonction de l'**état des appareils ASM/ABM** :



- Vous pouvez afficher les détails sur l'utilisateur connecté à un iPad partagé, depuis la page **Gérer > Appareils > Propriétés de l'utilisateur connecté**.

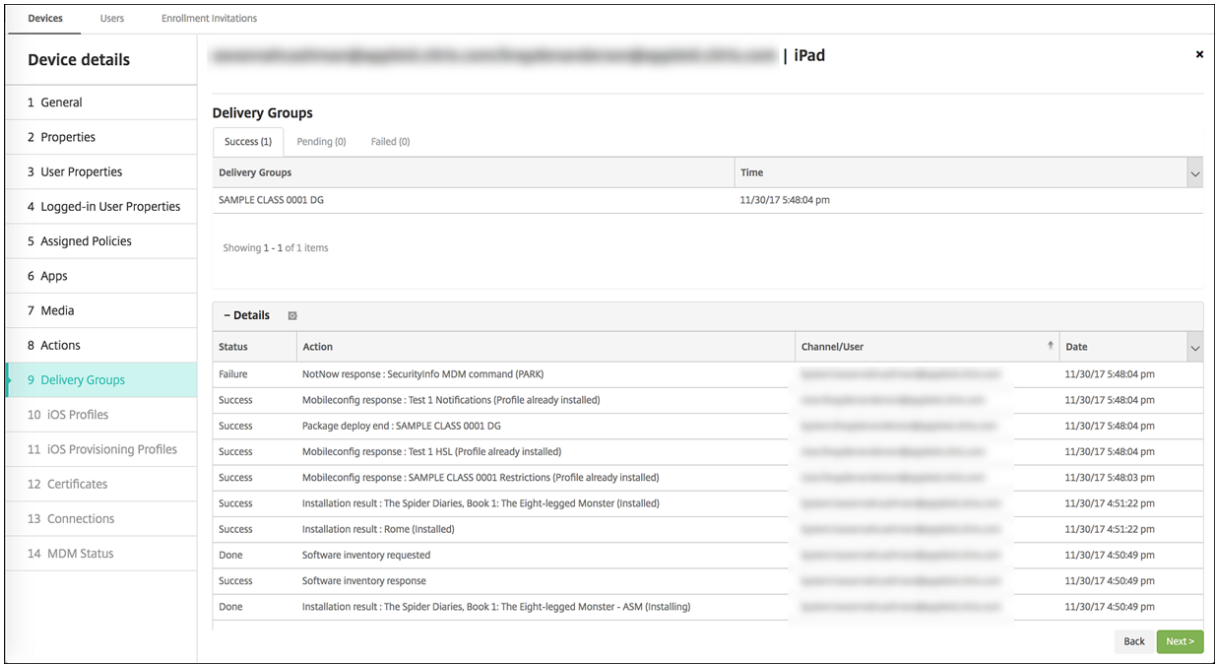
© 1999–2024 Cloud Software Group, Inc. All rights reserved.





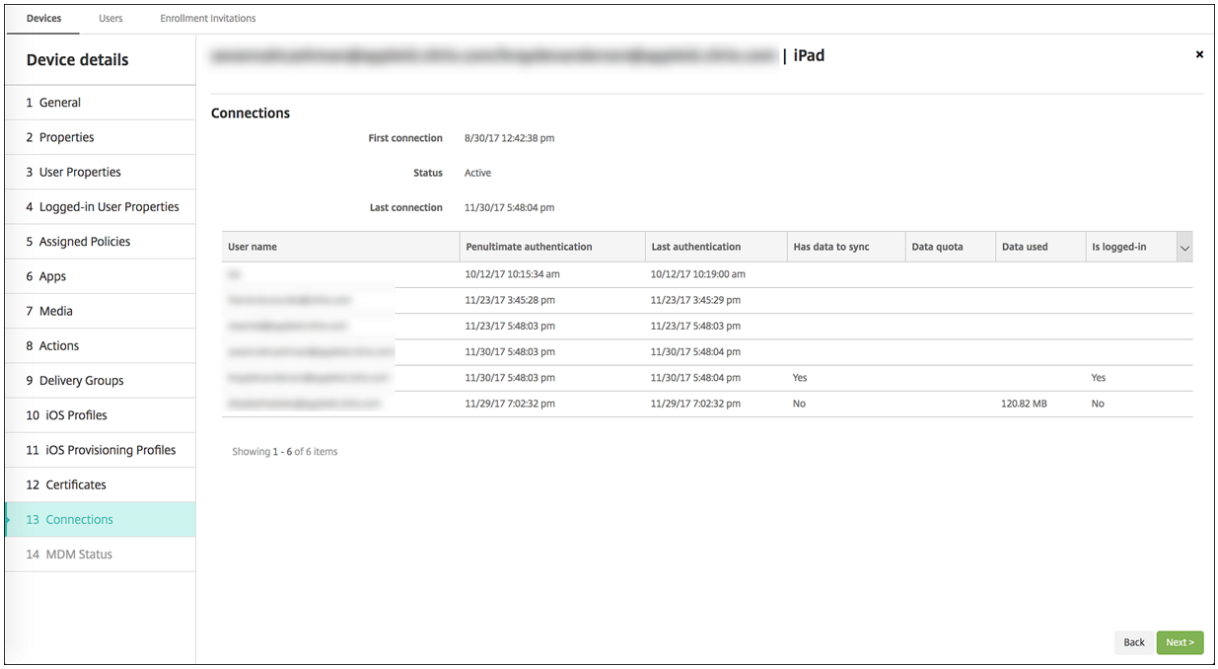
- Vous pouvez voir le canal utilisé pour déployer les ressources pour les propriétaires des appareils et les utilisateurs d'un groupe de mise à disposition sur la page **Gérer > Appareils > Groupes de mise à disposition**. La colonne **Canal/utilisateur** affiche le type (**Système** ou **Utilisateur**) et le destinataire.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

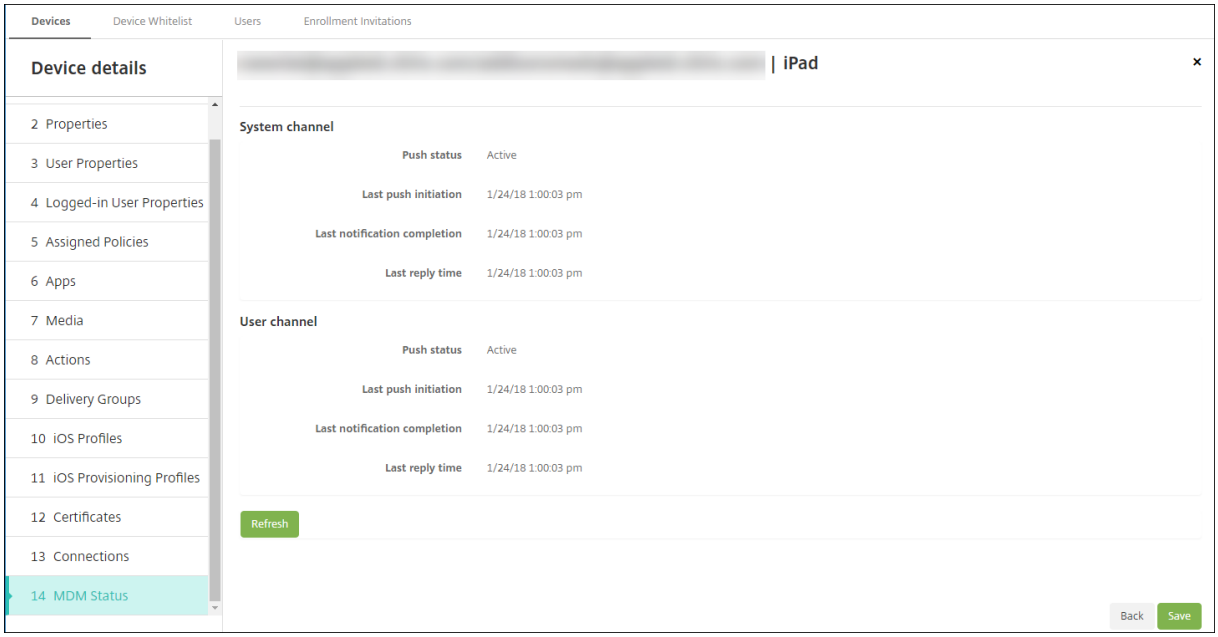


- Vous pouvez obtenir des informations sur les utilisateurs résidents :
  - **Dispose de données à synchroniser :** si l'utilisateur a des données à synchroniser avec le cloud.
  - **Quota de données :** quota de données défini pour l'utilisateur en octets. Un quota peut ne pas apparaître si les quotas utilisateur sont temporairement désactivés ou ne sont pas appliqués pour l'utilisateur.
  - **Données utilisées :** quantité de données utilisée par l'utilisateur en octets. Une valeur peut ne pas apparaître si une erreur se produit lorsque le système rassemble les informations.
  - **Est connecté :** indique si l'utilisateur est connecté à l'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Vous pouvez voir l'état de push pour les deux canaux.



Distribuer les applications Apple

November 29, 2023

Citrix Endpoint Management gère les applications déployées sur les appareils. Vous pouvez organiser

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

et déployer les types d'applications iOS/iPadOS et macOS suivants.

- **Apple App Store (iOS/iPadOS uniquement) :** ces applications peuvent être gratuites ou payantes et sont disponibles dans un magasin d'applications public, tel que l'Apple App Store ou Google Play. Par exemple : GoToMeeting.
- **Entreprise (iOS/iPadOS/macOS) :** applications natives pour lesquelles MDX n'est pas activé et qui ne contiennent pas les stratégies associées aux applications MDX.
- **MDX (iOS/iPadOS uniquement) :** applications préparées avec le SDK MAM ou encapsulées avec le MDX Toolkit. Ces applications incluent des stratégies MDX. Vous obtenez des applications MDX à partir de sources internes et de magasins publics.
- **Achat en volume (iOS/iPadOS/macOS) :** applications avec licences gérées via le programme d'achats en volume Apple.
- **Applications personnalisées iOS (iOS/iPadOS uniquement) :** applications propriétaires B2B développées en interne ou par un tiers.

Pour plus d'informations sur les différents types d'applications, reportez-vous à la section Ajouter des applications.

Certains déploiements nécessitent un compte Apple Business Manager (ABM) ou Apple School Manager (ASM). Pour plus d'informations, consultez les sections suivantes.

Pour chaque type d'application et méthode de distribution, Citrix recommande un ensemble de pratiques de configuration. Pour plus d'informations sur la distribution d'applications pour d'autres plates-formes, reportez-vous à la section Ajouter des applications. Les sections suivantes fournissent des informations plus détaillées sur la configuration des applications iOS.

Étapes générales de la distribution des applications

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Scénario	Étape 1 : Associer les comptes	Étape 2 : Ajouter et configurer des applications	Étape 3 : Configurer des groupes de mise à disposition et déployer des applications
Applications de magasin d' applications public, y compris les applications de mobilité Citrix	Non applicable	**Dans Citrix Endpoint Management : Configurer > Applications**, ajoutez des applications **Magasin d' applications public** pour iPhone ou iPad. Configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans Citrix Endpoint Management :** configurez et déployez des applications à l' aide de groupes de mise à disposition.
Applications du magasin d' applications public livrées avec l'achat en volume Apple, y compris les applications de mobilité Citrix	Inscrivez-vous au programme de déploiement d'Apple. **Dans Citrix Endpoint Management :** accédez à **Paramètres > Achat en volume** pour ajouter votre compte d'achat en volume.	**Dans ABM ou ASM :** achetez et ajoutez des applications depuis Applications et Books. **Dans Citrix Endpoint Management :** accédez à **Configurer > Applications**, configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans Citrix Endpoint Management :** configurez et déployez des applications à l' aide de groupes de mise à disposition.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Scénario	Étape 1 : Associer les comptes	Étape 2 : Ajouter et configurer des applications	Étape 3 : Configurer des groupes de mise à disposition et déployer des applications
Applications d' entreprise	Non applicable	**Dans Citrix Endpoint Management :** accédez à **Configurer > Applications**. Cliquez sur **Ajouter**, puis sur **Entreprise**. Chargez le fichier IPA. Configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans Citrix Endpoint Management :** configurez et déployez des applications à l' aide de groupes de mise à disposition.
Applications MDX	Non applicable	**Dans Citrix Endpoint Management :** accédez à **Configurer > Applications**. Cliquez sur **Ajouter**, puis sur **MDX**. Assurez-vous de sélectionner **iPad**/**iPhone** pour la plateforme. Chargez le fichier MDX. Configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans Citrix Endpoint Management :** configurez et déployez des applications à l' aide de groupes de mise à disposition.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Scénario	Étape 1 : Associer les comptes	Étape 2 : Ajouter et configurer des applications	Étape 3 : Configurer des groupes de mise à disposition et déployer des applications
Applications MDX distribuées via les achats en volume d'Apple	Inscrivez-vous au programme de déploiement d'Apple. **Dans Citrix Endpoint Management :** accédez à **Paramètres > Achat en volume** pour ajouter votre compte d'achat en volume.	**Dans ABM :** achetez et ajoutez des applications MDX depuis Applications et Books. Associez l'application à votre compte ABM. **Dans Citrix Endpoint Management :** accédez à **Configurer > Applications**, configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans Citrix Endpoint Management :** configurez et déployez des applications à l'aide de groupes de mise à disposition.
Applications personnalisées	Inscrivez-vous au programme de déploiement d'Apple. **Dans Citrix Endpoint Management :** accédez à **Paramètres > Achat en volume** pour ajouter votre compte d'achat en volume.	**Dans ABM :** ajoutez votre application à l'App Store en tant qu'application privée. Associez l'application à votre compte ABM. **Dans Citrix Endpoint Management :** accédez à **Configurer > Applications**, configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans Citrix Endpoint Management :** configurez et déployez des applications à l'aide de groupes de mise à disposition.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Scénario	Étape 1 : Associer les comptes	Étape 2 : Ajouter et configurer des applications	Étape 3 : Configurer des groupes de mise à disposition et déployer des applications
Applications personnalisées MDX	Inscrivez-vous au programme de déploiement d'Apple. **Dans Citrix Endpoint Management :** accédez à **Paramètres > Achat en volume** pour ajouter votre compte d'achat en volume.	**Dans ABM :** ajoutez votre application à l'App Store en tant qu'application privée. Associez l'application à votre compte ABM. **Dans Citrix Endpoint Management :** accédez à **Configurer > Applications** et chargez le fichier MDX. Configurez les applications et affectez-les aux groupes de mise à disposition.	**Dans Citrix Endpoint Management :** configurez et déployez des applications à l'aide de groupes de mise à disposition.

Applications de magasin d'applications public

Vous pouvez ajouter des applications gratuites et payantes disponibles sur l'App Store à Citrix Endpoint Management.

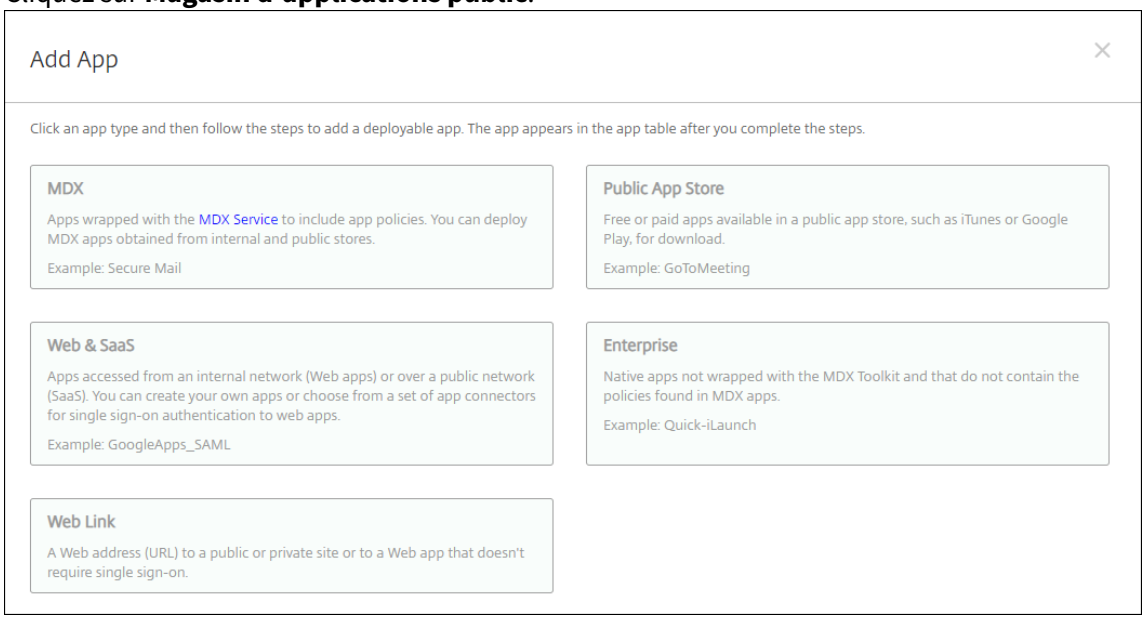
Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Non
Disponible sur	iOS/iPadOS

Étape 1 : Ajouter et configurer des applications

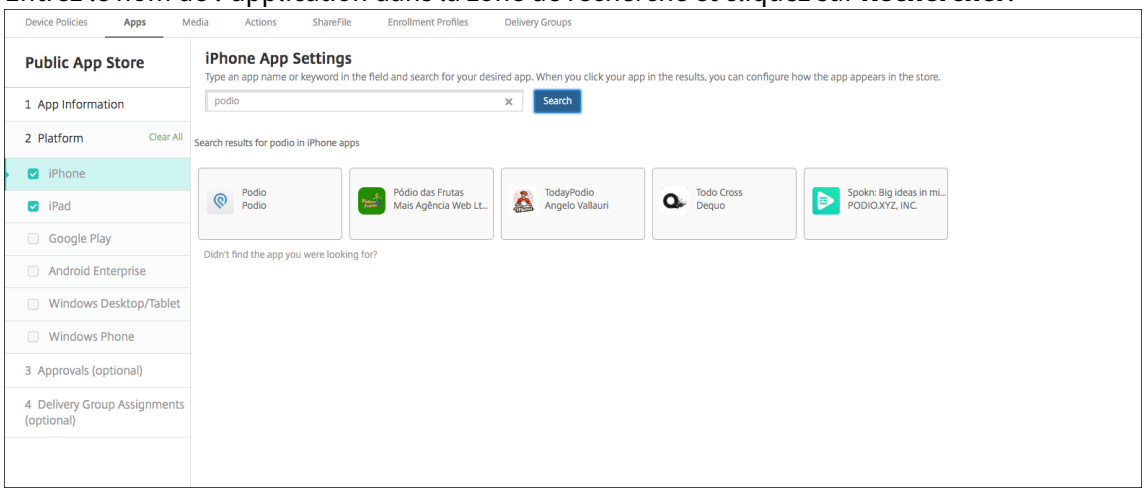
1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Applications**. Cliquez sur **Ajouter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Cliquez sur **Magasin d'applications public**.



3. Sélectionner **iPhone** ou **iPad** pour les plates-formes
4. Entrez le nom de l'application dans la zone de recherche et cliquez sur **Rechercher**.



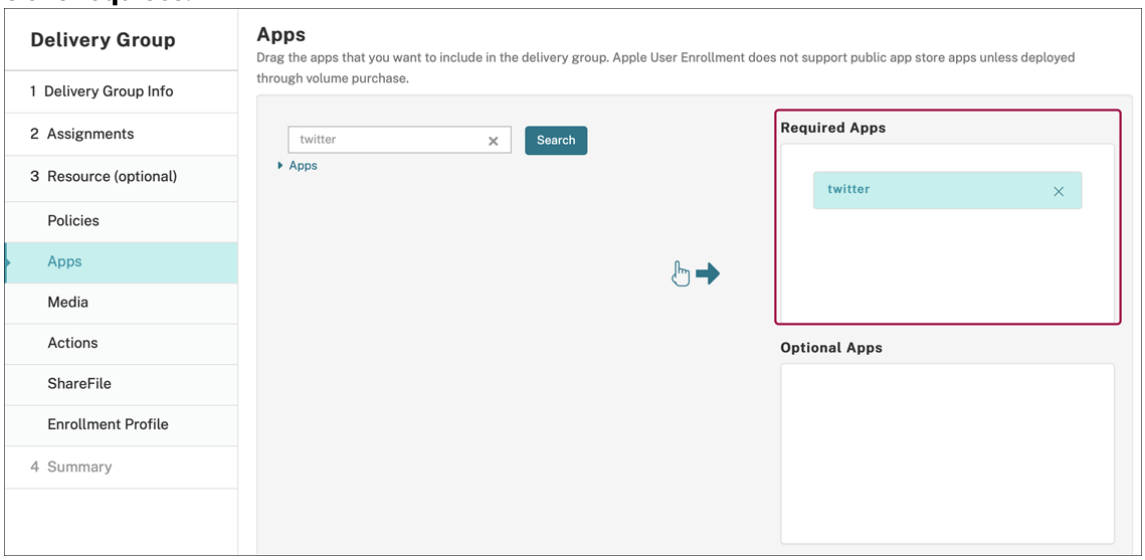
5. Les applications correspondant aux critères de recherche s'affichent. Cliquez sur l'application souhaitée.
6. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**.

Étape 2 : Configurer le déploiement de l'application

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Applications**.
2. Sélectionnez l'application que vous souhaitez configurer et cliquez sur **Modifier**.
3. Citrix recommande d'activer la fonctionnalité **Forcer l'application à être gérée**.
4. Affectez des groupes de mise à disposition et cliquez sur **Enregistrer**.
5. Accédez à **Configurer > Groupes de mise à disposition**, puis cliquez sur **Applications**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Dans la section **Applications**, faites glisser les applications souhaitées vers la zone **Applications requises**.



7. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
8. Sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.
9. Les utilisateurs reçoivent une demande d'installation de l'application et l'application s'installe en arrière-plan une fois qu'ils ont accepté.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Applications du magasin d'applications public livrées avec l'achat en volume Apple

Vous pouvez gérer les licences d'application iOS/iPadOS via le programme d'achat en volume Apple. Procédez comme suit pour ajouter des applications d'achat en volume à Citrix Endpoint Management.

Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Oui
Disponible sur	iOS/iPadOS/macOS

Étape 1 : Associer les comptes

1. Effectuez la configuration et l'inscription dans Apple Business Manager (ABM) ou Apple School Manager (ASM). Pour de plus amples informations sur ces programmes, consultez la documentation Apple.
2. Associez votre compte ABM/ASM à Citrix Endpoint Management. Pour plus d'informations sur l'association de comptes d'achat en volume, reportez-vous à la section Achats en volume Apple.
3. Lorsque vous ajoutez votre compte d'achat en volume, activez **Mise à jour automatique des applications**. Ce paramètre garantit que les applications des appareils utilisateur se mettent automatiquement à jour lorsqu'une mise à jour apparaît dans l'Apple Store. Si le paramètre **Forcer l'application à être gérée** est activé dans une application, elle est mise à jour sans intervention de l'utilisateur. La mise à jour s'effectue indépendamment du fait que l'application soit obligatoire ou facultative.

   Pour utiliser les paramètres **Forcer l'application à être gérée** et **Actualisation auto des apps**, activez la propriété de serveur `apple.app.force.managed`. Consultez Propriétés du serveur.

Étape 2 : Obtenir des applications et des licences Apple

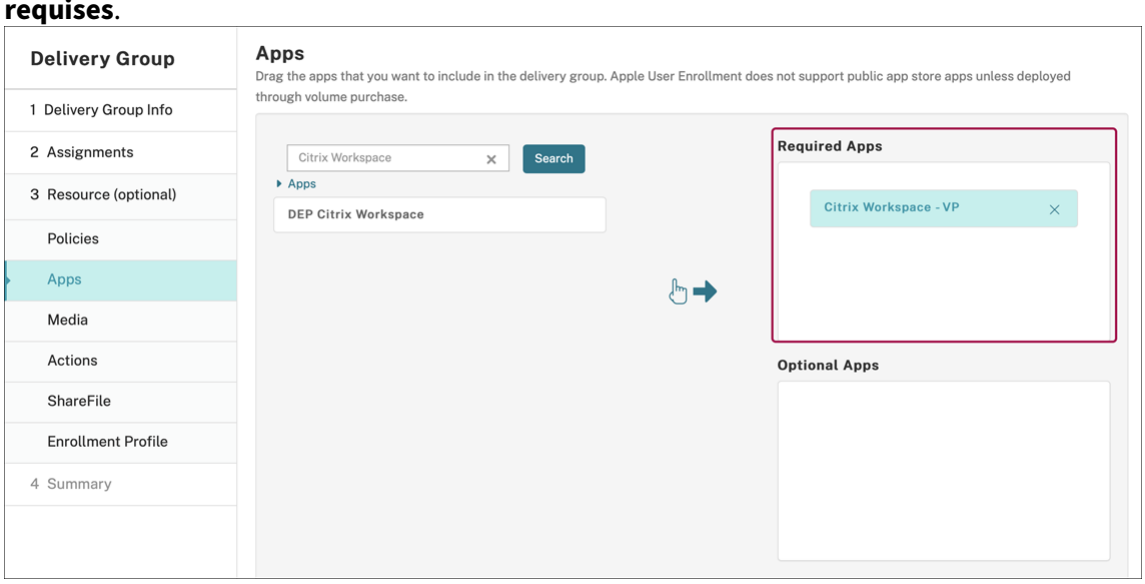
Achetez des applications sur votre compte ABM/ASM. Vous pouvez effectuer des achats dans Apple Books (pour iOS/iPadOS uniquement) et dans l'Apple App Store. N'oubliez pas que vous devez acheter toutes les applications, même si elles sont gratuites. Une fois que vous achetez des licences sur ABM/ASM, Citrix Endpoint Management affiche automatiquement l'application.

Pour plus d'informations sur la façon de rendre les applications accessibles à votre entreprise, reportez-vous à la documentation Apple.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Étape 3 : Configurer le déploiement des applications

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Applications**.
2. Sélectionnez l'application d'achat en volume que vous souhaitez configurer, puis cliquez sur **Modifier**.
3. Sélectionnez les plates-formes : **iPhone**, **iPad** ou **macOS**.
4. Citrix recommande d'activer la fonctionnalité **Forcer l'application à être gérée** (iOS/iPadOS uniquement).
5. Affectez des groupes de mise à disposition et cliquez sur **Enregistrer**.
6. Accédez à **Configurer > Groupes de mise à disposition**, puis cliquez sur **Applications**.
7. Dans la section **Applications**, faites glisser les applications souhaitées vers la zone **Applications requises**.



8. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
9. Sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.
10. Les utilisateurs reçoivent une demande d'installation de l'application et l'application s'installe en arrière-plan une fois qu'ils ont accepté.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Applications d'entreprise

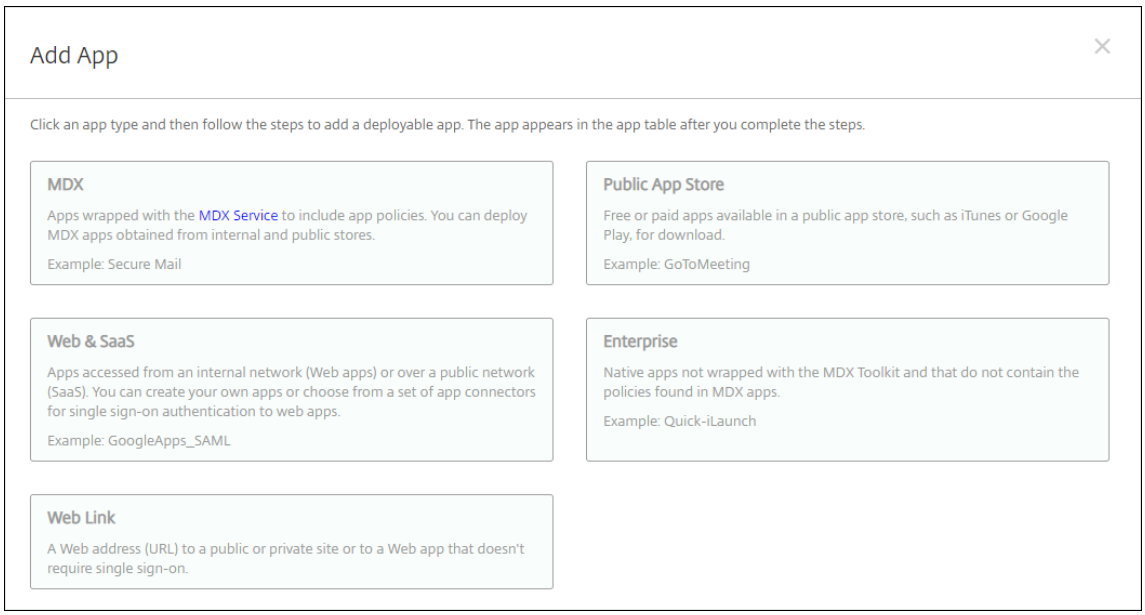
Vous pouvez également ajouter des applications natives pour lesquelles aucune stratégie MDX n'est associée. Procédez comme suit pour ajouter des applications qui n'existent pas sur l'App Store.

Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Oui
OS	iOS/iPadOS/macOS

Étape 1 : Ajouter et configurer des applications

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Applications**. Cliquez sur **Ajouter**.
2. Cliquez sur **Entreprise**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

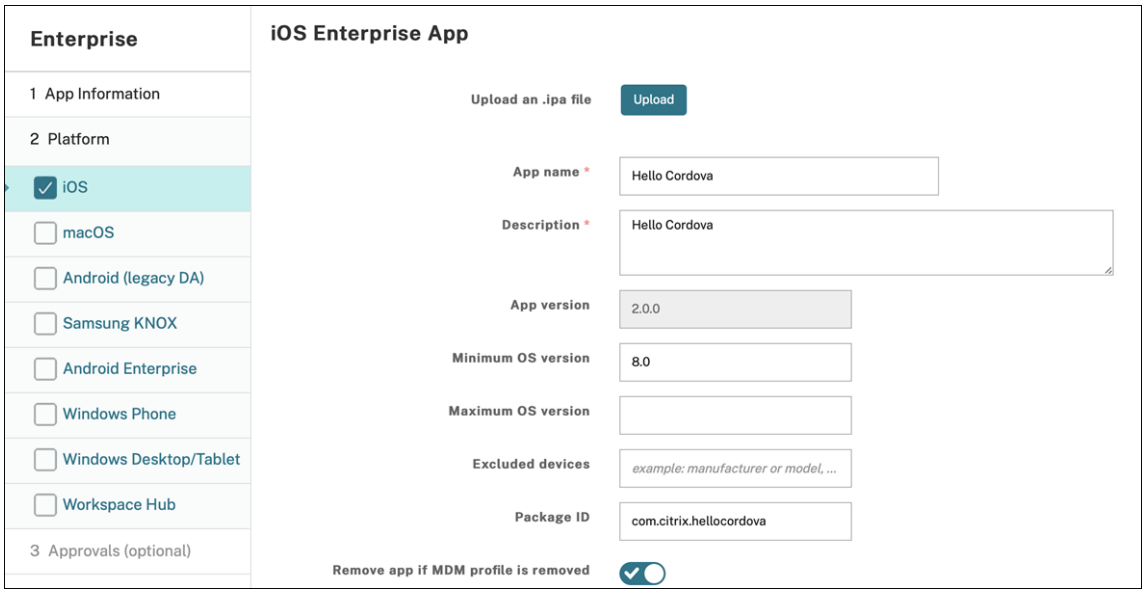


3. Sur la page **Informations sur l'application**, configurez les éléments suivants :
   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous Nom de l'application dans la table Applications.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application.
4. Cliquez sur **Suivant**. La page **Plates-formes d'applications** s'affiche.
5. Sélectionnez les plates-formes : **iPhone**, **iPad** ou **macOS**.
6. Télécharger le fichier IPA (iOS/iPadOS) ou télécharger le fichier PKG (macOS)
7. Cliquez sur **Suivant**. La page sur les **détails de l'application** s'affiche.
8. Pour configurer ces paramètres :
   - **Nom du fichier :** entrez un nouveau nom pour l'application (facultatif).
   - **Description de l'application :** entrez une nouvelle description pour l'application (facultatif).
   - **Version de l'application :** vous ne pouvez pas modifier ce champ.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
   - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Supprimer l'application si le profil MDM est supprimé :** sélectionnez cette option si vous souhaitez supprimer l'application d'un appareil lorsque le profil MDM est supprimé. La valeur par défaut est Activé (iOS/iPadOS uniquement).
- **Empêcher la sauvegarde des données d'application :** sélectionnez cette option si vous souhaitez empêcher l'application de sauvegarder les données. La valeur par défaut est Activé (iOS/iPadOS uniquement).
- **Forcer l'application à être gérée :** si vous installez une application non gérée, sélectionnez **Activé** si vous souhaitez que les utilisateurs sur des appareils non supervisés soient invités à autoriser la gestion de l'application. S'ils acceptent l'invite, l'application est gérée. Si le paramètre **Forcer l'application à être gérée** est activé dans une application, elle est mise à jour sans intervention de l'utilisateur. La mise à jour s'effectue indépendamment du fait que l'application soit obligatoire ou facultative (iOS/iPadOS uniquement).

Pour utiliser les paramètres **Forcer l'application à être gérée** et **Actualisation auto des apps**, activez la propriété de serveur `apple.app.force.managed`. Consultez Propriétés du serveur.

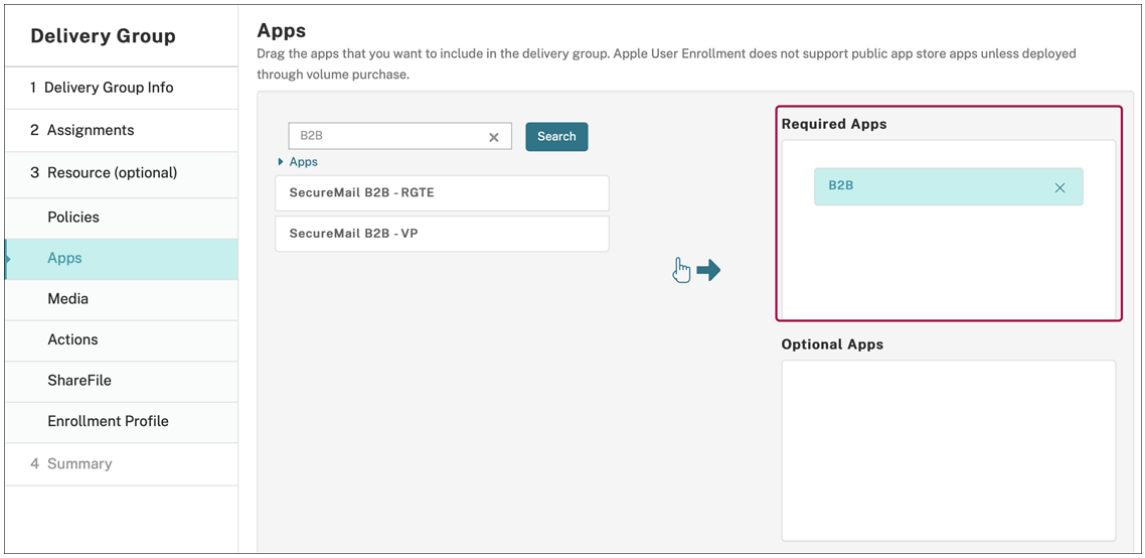


9. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**.

Étape 2 : Configurer le déploiement de l'application

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Groupes de mise à disposition**. Sélectionnez le groupe de mise à disposition à configurer et cliquez sur la page **Applications**.
2. Faites glisser les applications souhaitées vers la zone **Applications requises**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
4. Sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.
5. Les utilisateurs reçoivent une demande d'installation de l'application et l'application s'installe en arrière-plan une fois qu'ils ont accepté.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Applications MDX

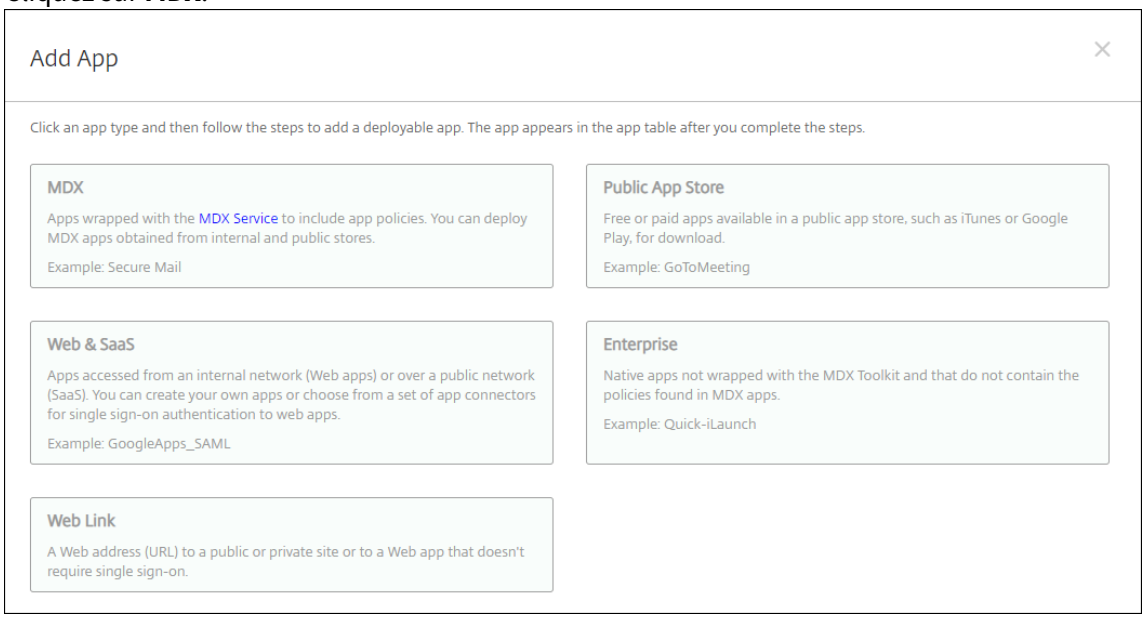
Pour utiliser les stratégies MDX et les fonctionnalités de sécurité, ajoutez des applications pour lesquelles le SDK MAM est activé ou encapsulées avec MDX. Vous pouvez déployer des applications MDX avec ou sans achat en volume.

Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Oui
Disponible sur	iOS/iPadOS

Pour ajouter la version MDX d'une application de magasin d'applications public, suivez les étapes de la section Applications de magasin d'applications public, puis suivez les étapes décrites dans cette section.

Étape 1 : Ajouter et configurer des applications

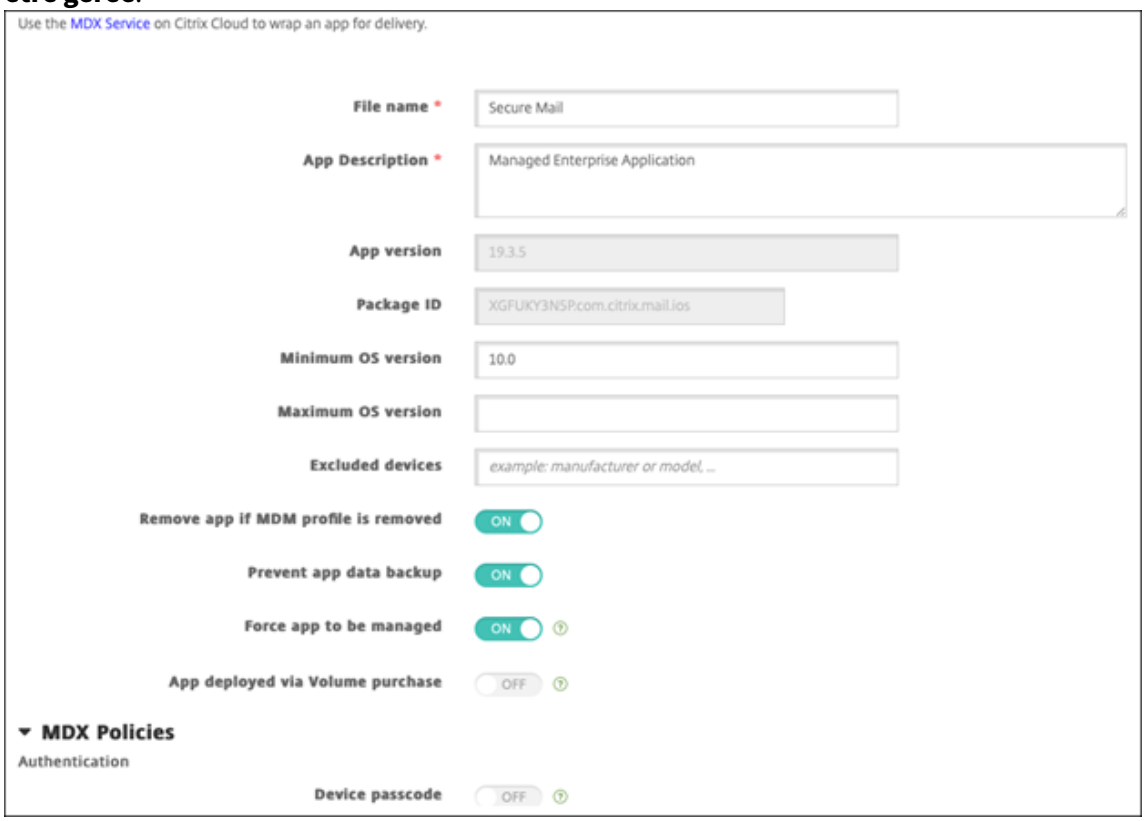
1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Applications**. Cliquez sur **Ajouter**.
2. Cliquez sur **MDX**.



3. Sélectionnez **iPhone** ou **iPad** pour les plates-formes.
4. Chargez le fichier MDX.
5. Configurez les détails de l'application. Définissez **Application déployée via l'achat en volume** sur **Désactivé**. Citrix recommande d'activer la fonctionnalité **Forcer l'application à**

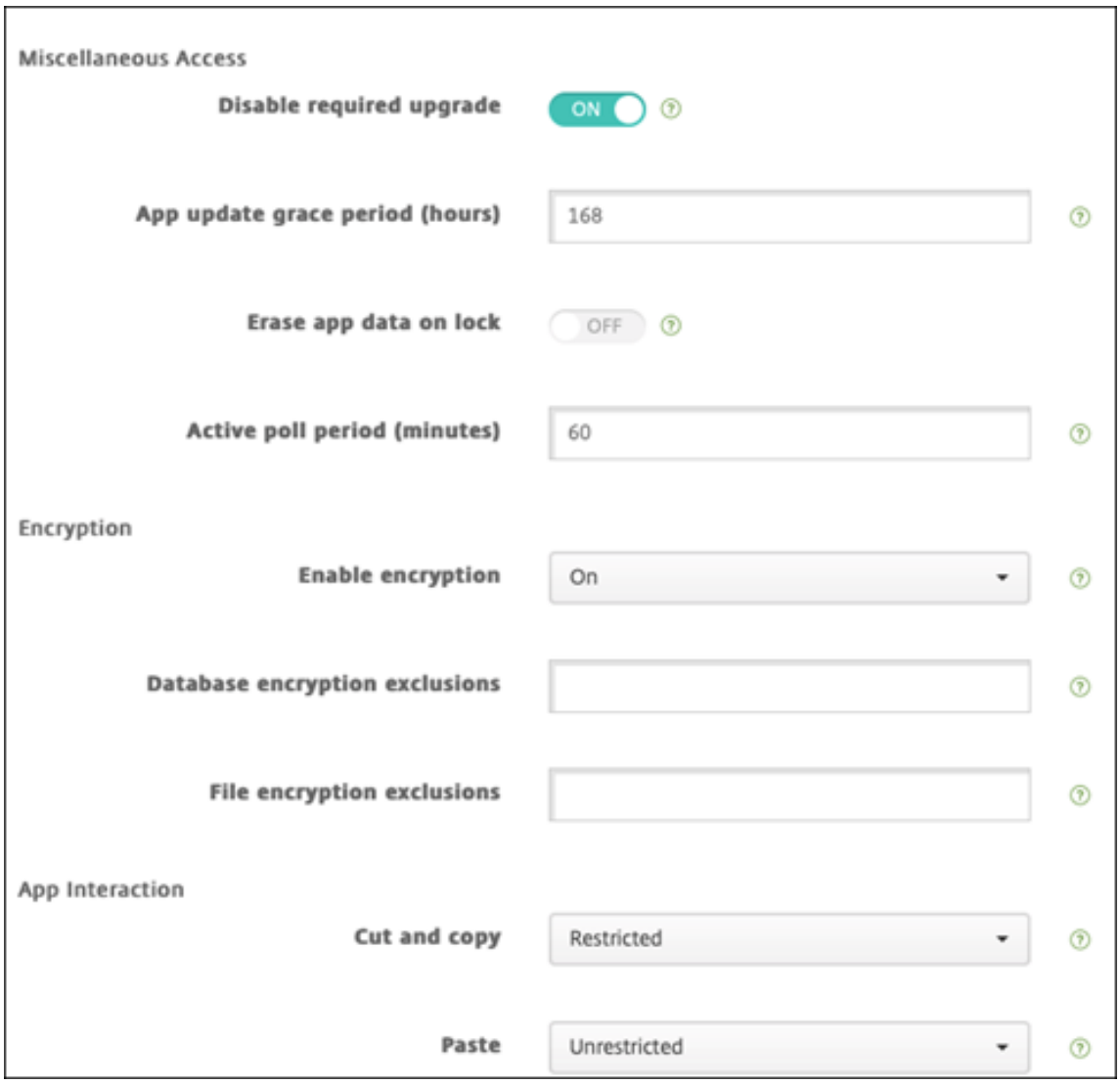
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

être gérée.



6. Configurez les stratégies MDX. Définissez **Désactiver mise à niveau requise** sur **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

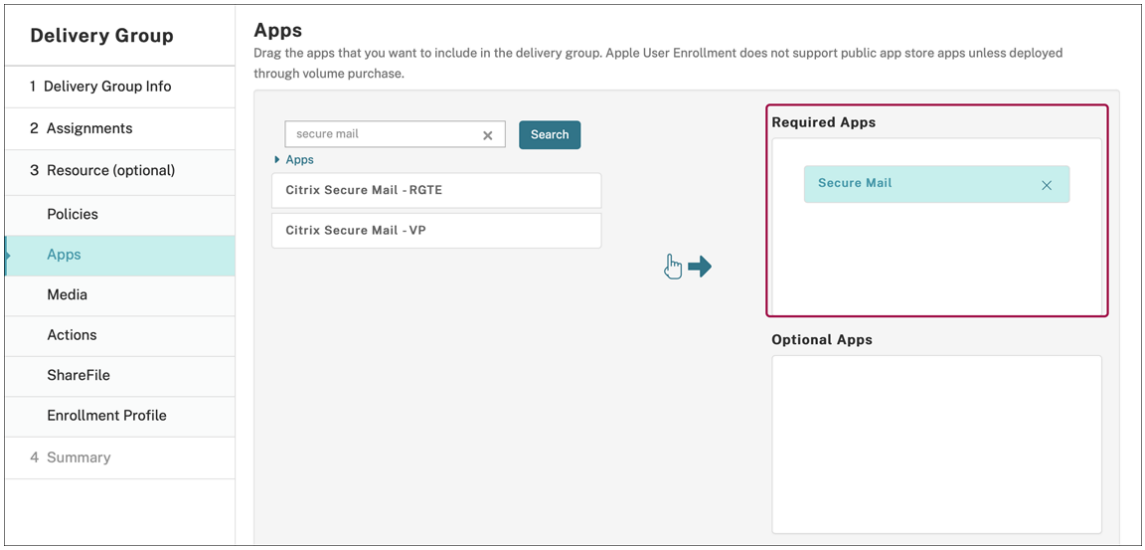


7. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**.

Étape 2 : Configurer le déploiement de l'application

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Groupes de mise à disposition**, puis cliquez sur **Ajouter**.
2. Dans la section **Applications**, faites glisser les applications souhaitées vers la zone **Applications requises**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
4. Sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.
5. Les utilisateurs reçoivent une demande d'installation de l'application et l'application s'installe en arrière-plan une fois qu'ils ont accepté.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Applications MDX distribuées via les achats en volume d'Apple

Pour utiliser les stratégies MDX et les fonctionnalités de sécurité, ajoutez des applications pour lesquelles le SDK MAM est activé ou encapsulées avec MDX. Pour déployer des applications à l'aide de l'achat en volume, les applications doivent exister sur le magasin d'applications.

Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Oui
Disponible sur	iOS/iPadOS

Étape 1 : Associer les comptes

1. Effectuez la configuration et l'inscription dans Apple Business Manager (ABM) ou Apple School Manager (ASM). Pour de plus amples informations sur ces programmes, consultez la documentation Apple.
2. Associez votre compte ABM/ASM à Citrix Endpoint Management. Pour plus d'informations sur l'association de comptes d'achat en volume, reportez-vous à la section Achats en volume Apple.
3. Lorsque vous ajoutez votre compte d'achat en volume, activez **Mise à jour automatique des applications**. Ce paramètre garantit que les applications des appareils utilisateur se mettent automatiquement à jour lorsqu'une mise à jour apparaît dans l'Apple Store. Si le paramètre **Forcer l'application à être gérée** est activé dans une application, elle est mise à jour sans intervention de l'utilisateur. La mise à jour s'effectue indépendamment du fait que l'application soit obligatoire ou facultative.

   Pour utiliser les paramètres **Forcer l'application à être gérée** et **Actualisation auto des apps**, activez la propriété de serveur `apple.app.force.managed`. Consultez Propriétés du serveur.

Étape 2 : Obtenir des applications et des licences Apple

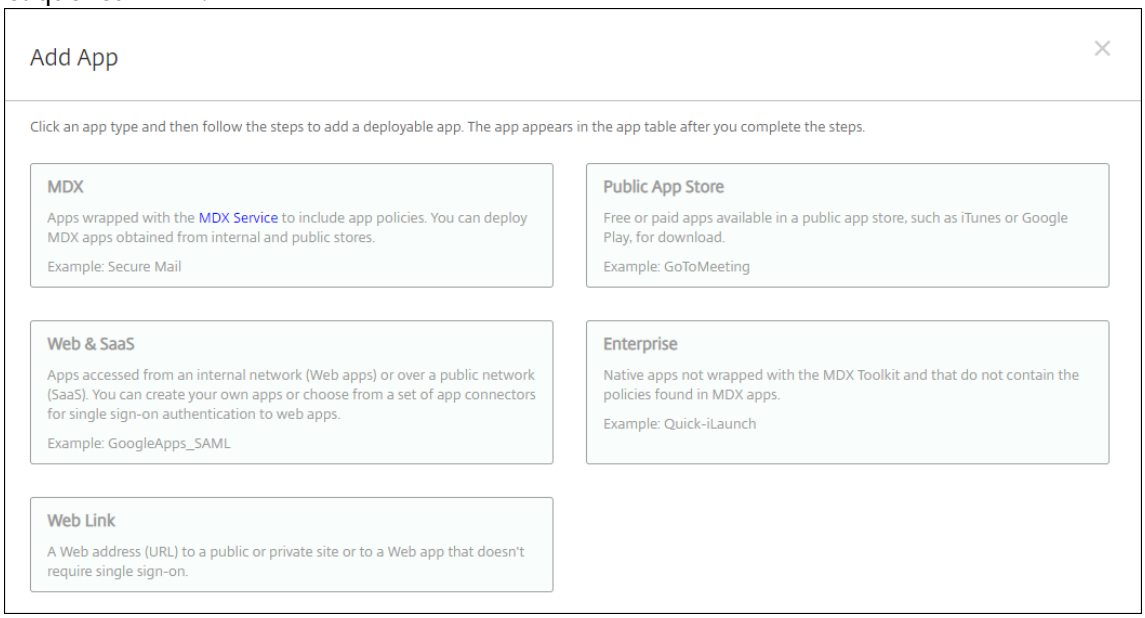
Achetez des applications sur votre compte ABM/ASM. Vous pouvez effectuer des achats dans Apple Books (pour iOS/iPadOS uniquement) et dans l'Apple App Store. N'oubliez pas que vous devez acheter toutes les applications, même si elles sont gratuites. Une fois que vous achetez des licences sur ABM/ASM, Citrix Endpoint Management affiche automatiquement l'application.

Pour plus d'informations sur la façon de rendre les applications accessibles à votre entreprise, reportez-vous à la documentation Apple.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

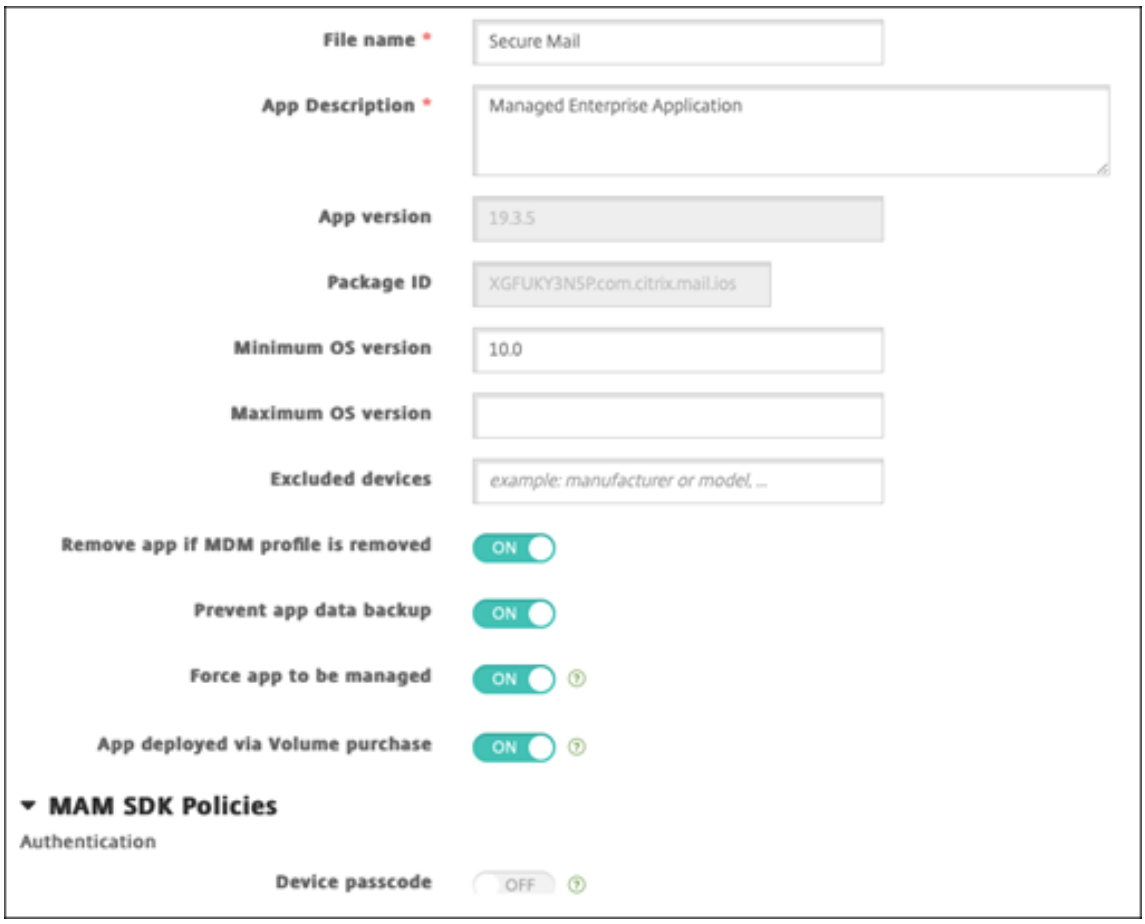
Étape 3 : Ajouter et configurer des applications

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Applications**. Cliquez sur **Ajouter**.
2. Cliquez sur **MDX**.



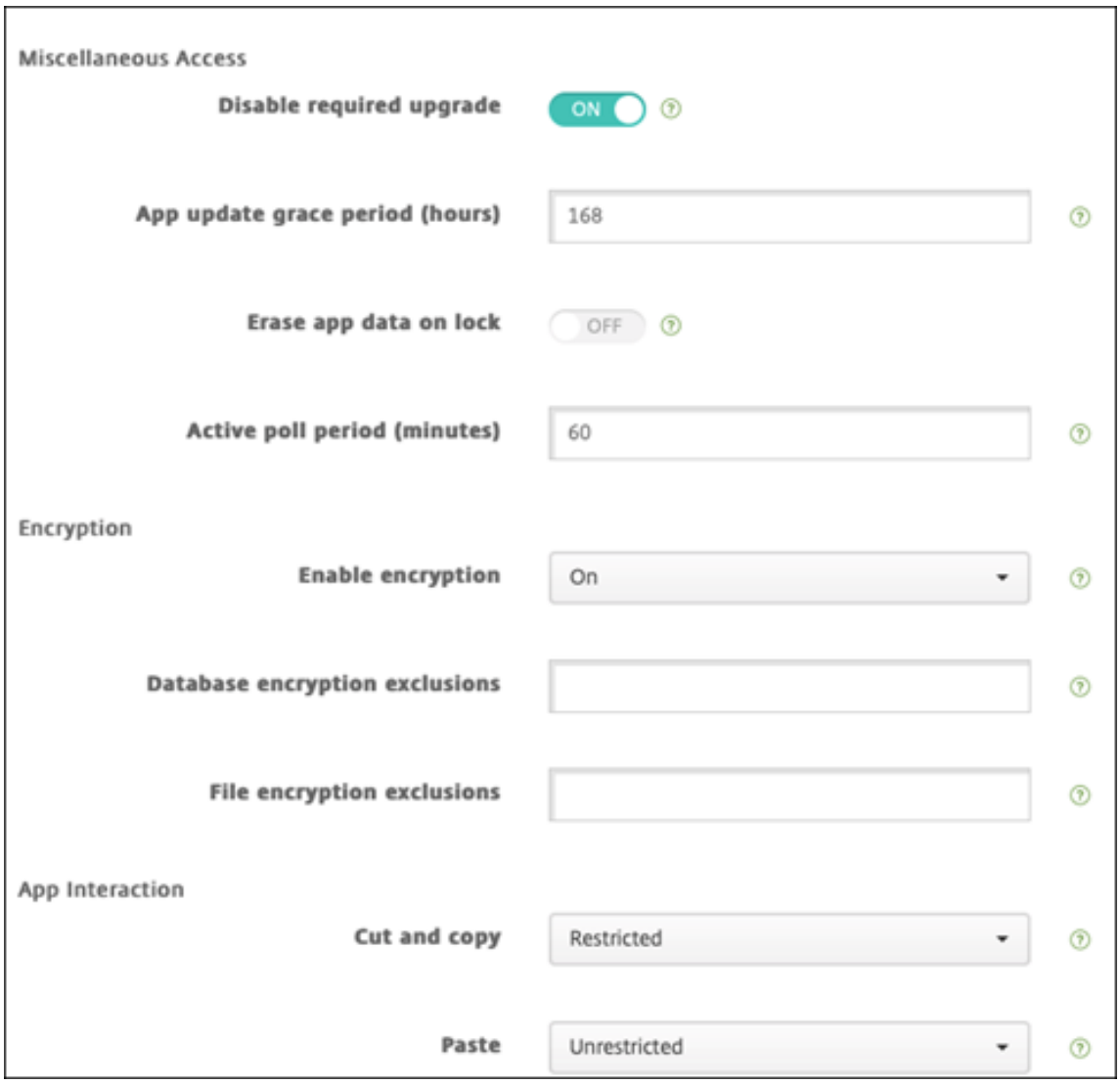
3. Sélectionnez **iPhone** ou **iPad** pour les plates-formes.
4. Chargez le fichier MDX.
5. Configurez les détails de l'application. Définissez **Application déployée via l'achat en volume** sur **Désactivée**. Citrix recommande d'activer la fonctionnalité **Forcer l'application à être gérée**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Configurez les stratégies MDX. Définissez **Désactiver mise à niveau requise** sur **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



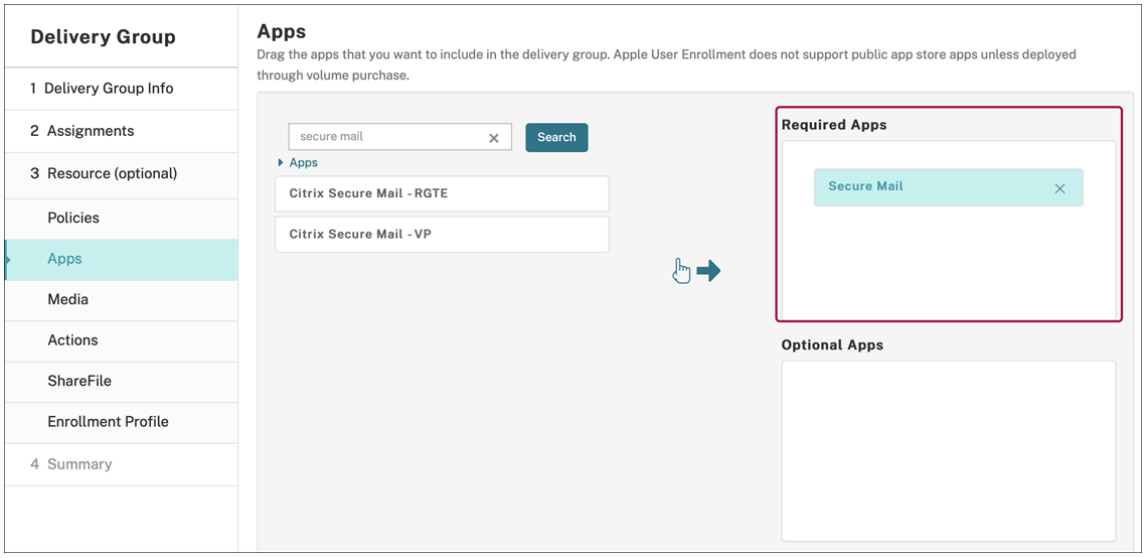
7. Affectez un groupe de mise à disposition à l'application pour chaque plate-forme et cliquez sur **Enregistrer**.

Avec cette configuration, deux entrées sont répertoriées pour cette application dans la liste des applications. Lorsque vous sélectionnez une application à configurer, sélectionnez l'application avec **Type MDX**.

Étape 4 : Configurer le déploiement des applications

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Groupes de mise à disposition**, puis cliquez sur **Ajouter**.
2. Dans la section **Applications**, faites glisser les applications MDX souhaitées vers la zone **Applications requises**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
4. Sélectionnez le groupe de mise à disposition et cliquez sur **Déployer**.
5. Les utilisateurs reçoivent une demande d'installation de l'application et l'application s'installe en arrière-plan une fois qu'ils ont accepté.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Applications personnalisées

Les applications personnalisées sont des applications propriétaires B2B. Vous pouvez utiliser Citrix Endpoint Management et l'achat en volume Apple pour distribuer des applications propriétaires de manière privée et sécurisée. Vous pouvez distribuer les applications à des partenaires, clients, franchisés et employés internes spécifiques.

Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Oui
Disponible sur	iOS/iPadOS

Conditions requises pour les applications personnalisées

- Compte Apple Business Manager ou Apple School Manager
- Compte d'achat en volume Apple (nécessite des appareils avec iOS 7 ou version ultérieure)
- Inscrire des appareils dans Citrix Endpoint Management à l'aide de l'un des modes d'inscription Apple suivants :
  - Inscription automatique des appareils
  - Inscription d'appareils
  - Inscription des utilisateurs

Étape 1 : Associer les comptes

Pour déployer des applications personnalisées à l'aide de l'achat en volume, associez votre compte d'achat en volume à Citrix Endpoint Management.

1. Effectuez la configuration et l'inscription dans Apple Business Manager (ABM). Pour de plus amples informations sur ces programmes, consultez la documentation Apple.
2. Associez votre compte ABM à Citrix Endpoint Management. Pour plus d'informations sur l'association de comptes d'achat en volume, reportez-vous à la section Achats en volume Apple.
3. Lorsque vous ajoutez votre compte d'achat en volume, activez **Mise à jour automatique des applications**. Ce paramètre garantit que les applications des appareils utilisateur se mettent automatiquement à jour lorsqu'une mise à jour apparaît dans l'Apple Store. Si le paramètre **Forcer l'application à être gérée** est activé dans une application, elle est mise à jour sans intervention de l'utilisateur. La mise à jour s'effectue indépendamment du fait que l'application soit obligatoire ou facultative.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour utiliser les paramètres **Forcer l'application à être gérée** et **Actualisation auto des apps**, activez la propriété de serveur `apple.app.force.managed`. Consultez Propriétés du serveur.

Étape 2 : Configurer les applications sur ABM

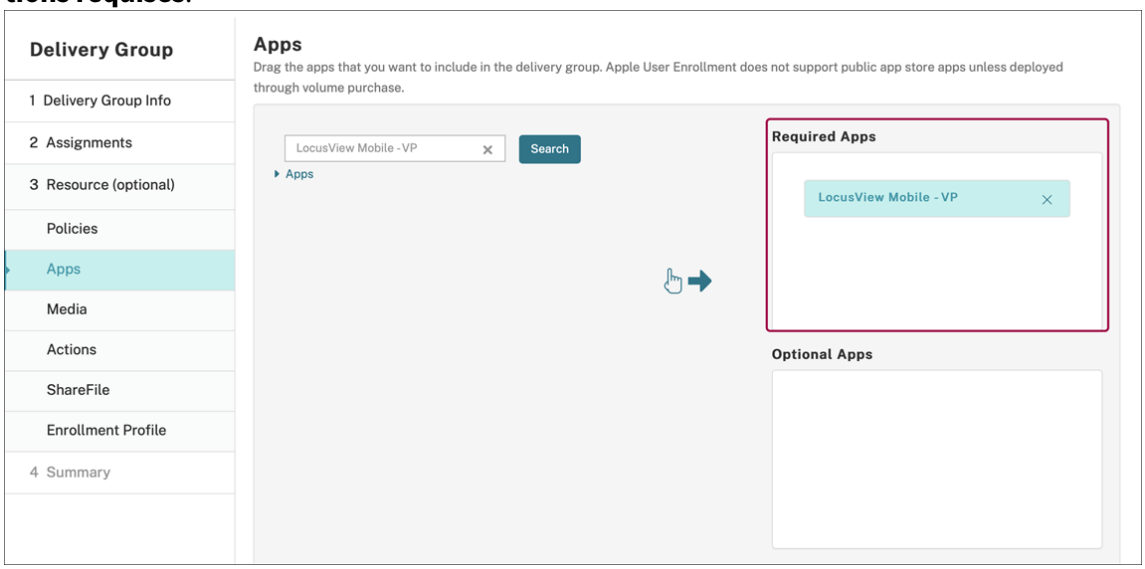
Ajoutez les applications sur votre compte ABM. Vous pouvez charger et distribuer vos propres applications personnalisées ou acheter des licences pour des applications personnalisées auprès d'autres organisations. Pour plus d'informations sur l'ajout et l'activation d'applications personnalisées sur ABM, reportez-vous à la documentation Apple.

Étape 3 : Ajouter et configurer les applications dans Citrix Endpoint Management

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Applications**. Les applications d'achat en volume apparaissent dans la liste des applications.
2. Sélectionnez l'application que vous souhaitez configurer. Cliquez sur **Modifier**.
3. Sélectionnez les plates-formes : **iPhone**, **iPad** ou **macOS**.
4. Choisissez les groupes de mise à disposition vers lesquels vous souhaitez que l'application soit distribuée. Cliquez sur **Save**.

Étape 4 : Configurer le déploiement des applications

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Groupes de mise à disposition**, puis cliquez sur **Ajouter**.
2. Dans la section **Applications**, faites glisser les applications souhaitées vers la zone **Applications requises**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
4. Sélectionnez le groupe de mise à disposition que vous souhaitez déployer, puis cliquez sur **Déployer**.
5. Les utilisateurs reçoivent une demande de déploiement d'applications. Les applications s'installent en arrière-plan après que les utilisateurs les ont acceptées.

Applications personnalisées MDX

Pour utiliser les stratégies MDX et les fonctionnalités de sécurité, ajoutez des applications personnalisées pour lesquelles le SDK MAM est activé ou encapsulées avec MDX.

Disponibilité des fonctionnalités	
Nécessite la supervision de l'appareil	Non
Disponible pour le mode d'inscription utilisateur	Oui
Disponible sur	iOS/iPadOS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Étape 1 : Associer les comptes

Pour déployer des applications personnalisées à l'aide de l'achat en volume, associez votre compte d'achat en volume à Citrix Endpoint Management.

1. Effectuez la configuration et l'inscription dans Apple Business Manager (ABM). Pour de plus amples informations sur ces programmes, consultez la documentation Apple.
2. Associez votre compte ABM à Citrix Endpoint Management. Pour plus d'informations sur l'association de comptes d'achat en volume, reportez-vous à la section Achats en volume Apple.
3. Lorsque vous ajoutez votre compte d'achat en volume, activez **Mise à jour automatique des applications**. Ce paramètre garantit que les applications des appareils utilisateur se mettent automatiquement à jour lorsqu'une mise à jour apparaît dans l'Apple Store. Si le paramètre **Forcer l'application à être gérée** est activé dans une application, elle est mise à jour sans intervention de l'utilisateur. La mise à jour s'effectue indépendamment du fait que l'application soit obligatoire ou facultative.

   Pour utiliser les paramètres **Forcer l'application à être gérée** et **Actualisation auto des apps**, activez la propriété de serveur `apple.app.force.managed`. Consultez Propriétés du serveur.

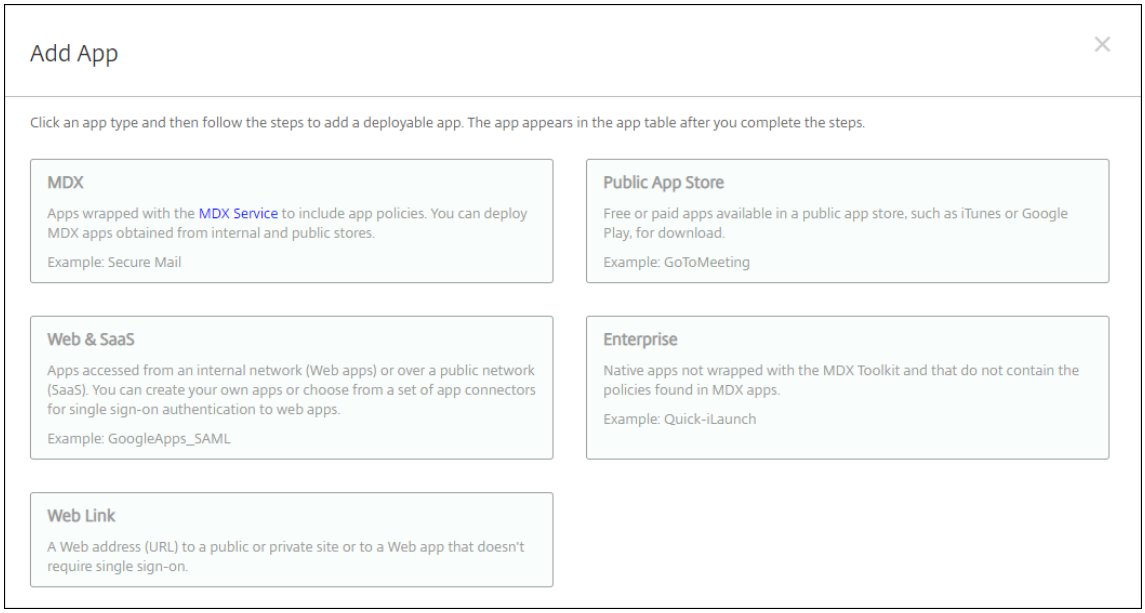
Étape 2 : Configurer les applications sur ABM

Ajoutez les applications sur votre compte ABM. Vous pouvez charger et distribuer vos propres applications personnalisées ou acheter des licences pour des applications personnalisées auprès d'autres organisations. Pour plus d'informations sur l'ajout et l'activation d'applications personnalisées sur ABM, reportez-vous à la documentation Apple.

Étape 3 : Ajouter et configurer les applications dans Citrix Endpoint Management

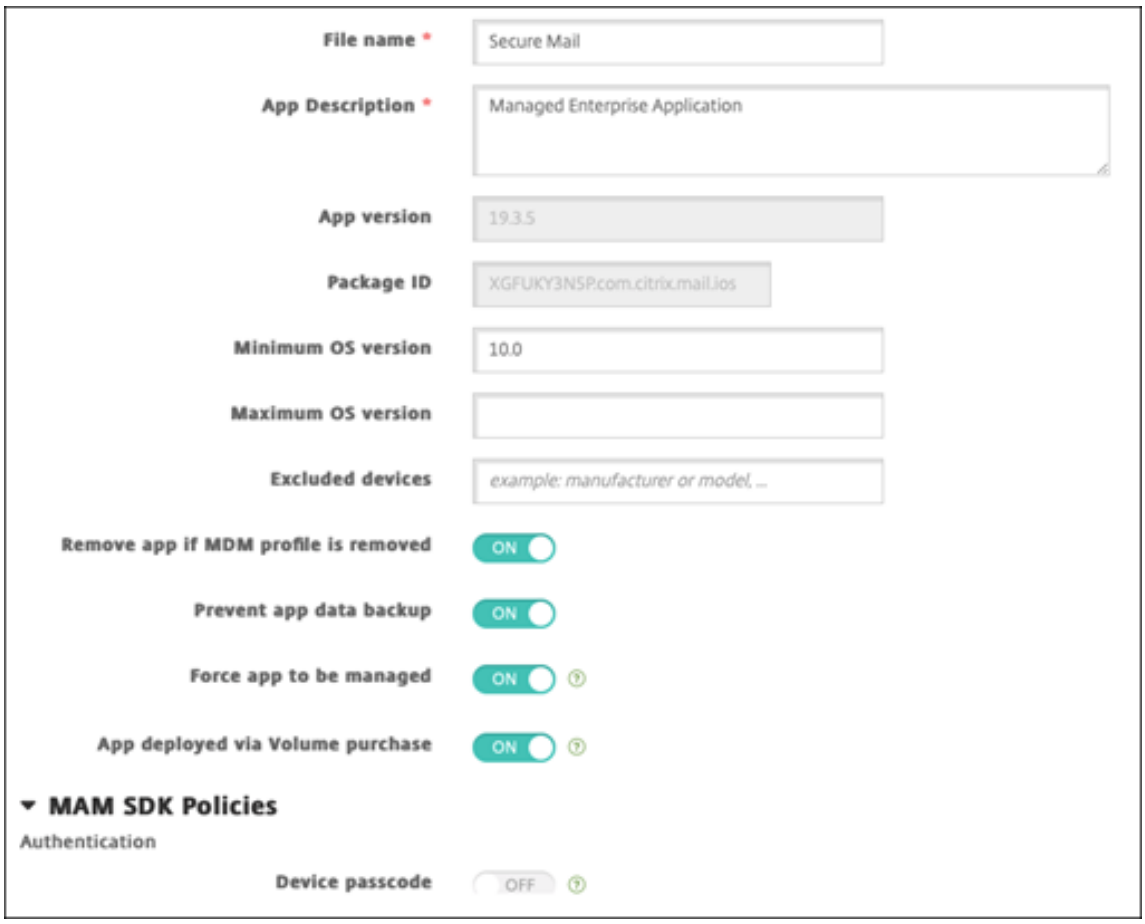
1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Applications**. Cliquez sur **Ajouter**.
2. Cliquez sur **MDX**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



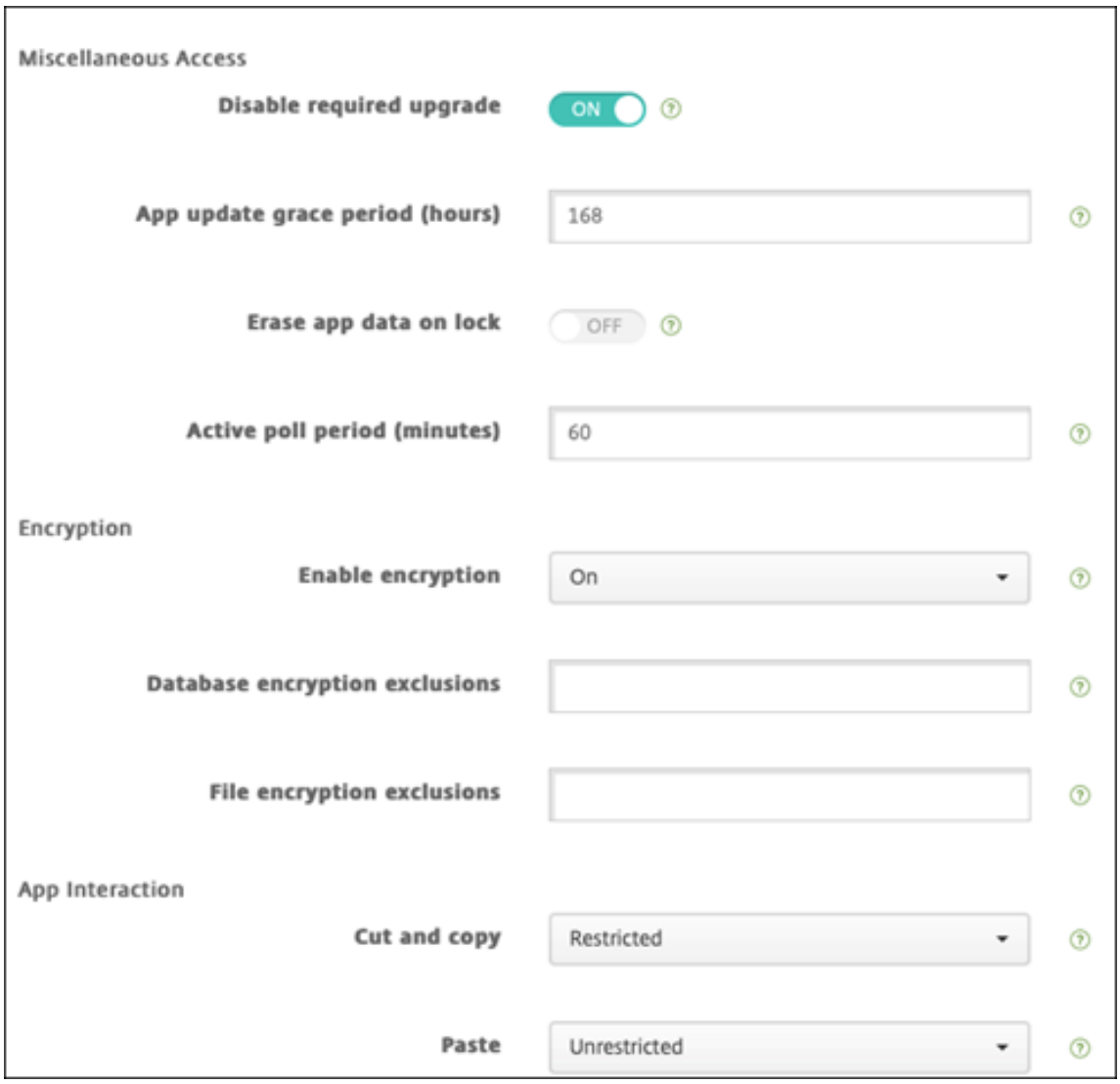
3. Sélectionnez les plateformes **iPhone** ou **iPad**.
4. Chargez le fichier MDX de l'application que vous souhaitez ajouter.
5. Configurez les détails de l'application. Définissez **Application déployée via l'achat en volume** sur **Désactivée**. Citrix recommande d'activer la fonctionnalité **Forcer l'application à être gérée**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Configurez les stratégies MDX. Définissez **Désactiver mise à niveau requise** sur **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



7. Affectez un groupe de mise à disposition à l'application et cliquez sur **Enregistrer**.

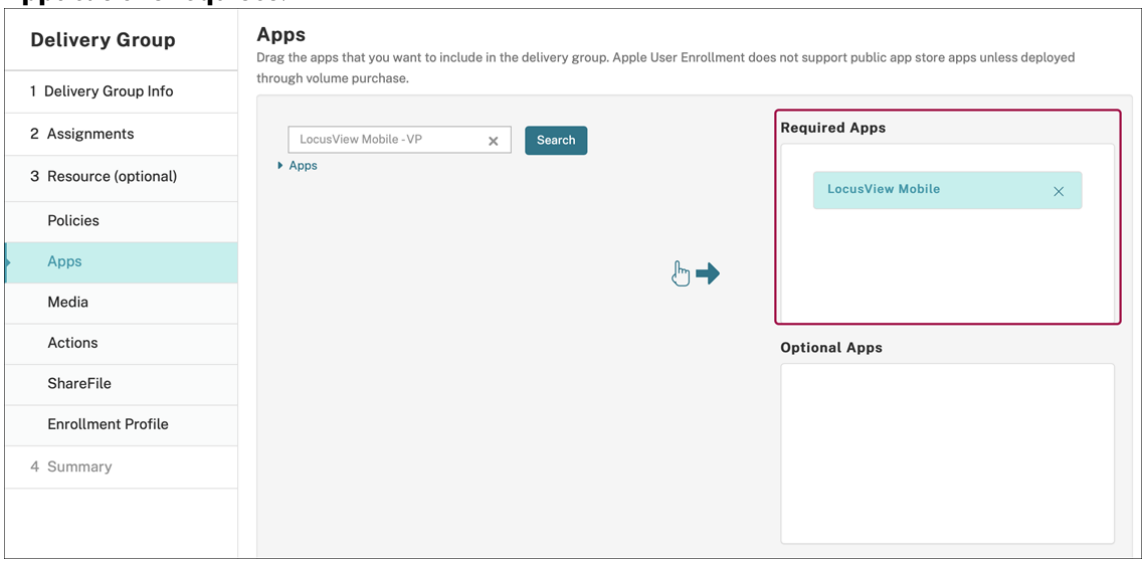
Avec cette configuration, deux entrées sont répertoriées pour cette application dans la liste des applications. Lorsque vous sélectionnez une application à configurer, sélectionnez l'application avec **Type MDX**.

Étape 4 : Configurer le déploiement des applications

1. Dans la console Citrix Endpoint Management, accédez à **Configurer > Applications**. Les applications d'achat en volume apparaissent dans la liste des applications.
2. Sélectionnez l'application que vous souhaitez configurer. Cliquez sur **Modifier**.
3. Choisissez les groupes de mise à disposition vers lesquels vous souhaitez que l'application soit distribuée sur chaque plate-forme. Cliquez sur **Save**.
4. Accédez à **Configurer > Groupes de mise à disposition**, puis cliquez sur **Applications**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Dans la section **Applications**, faites glisser les applications MDX souhaitées vers la zone **Applications requises**.



6. Naviguez jusqu'à **Configurer > Groupes de mise à disposition**.
7. Sélectionnez le groupe de mise à disposition que vous souhaitez déployer, puis cliquez sur **Déployer**.
8. Les utilisateurs reçoivent une demande de déploiement d'applications. Les applications s'installent en arrière-plan après leur acceptation.

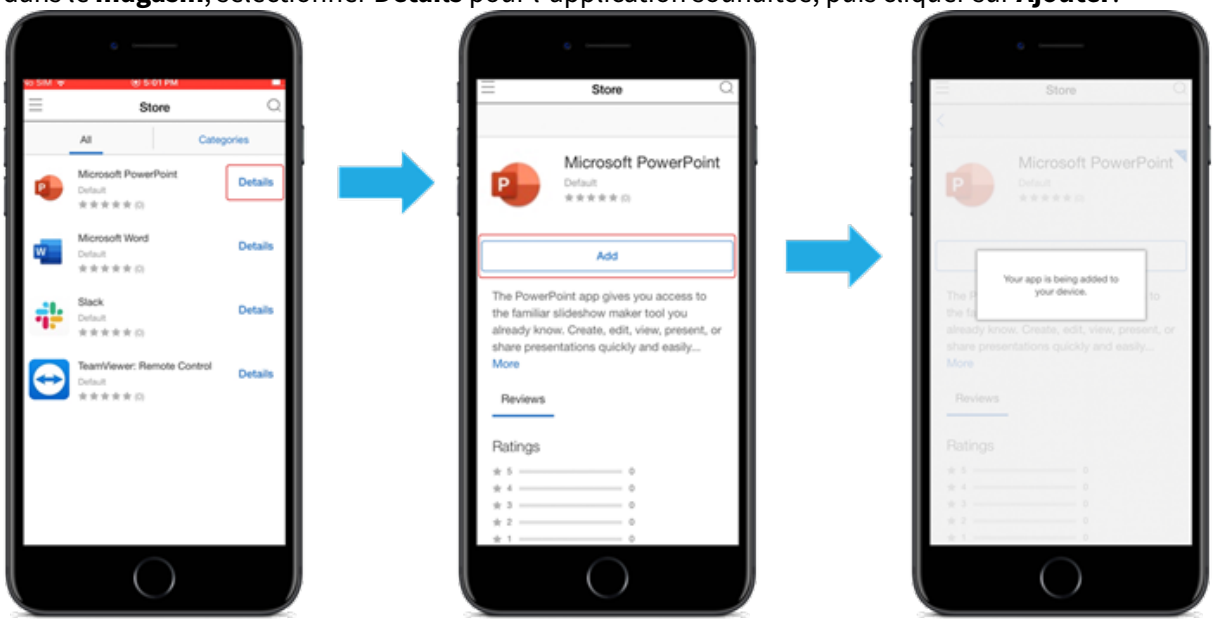
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Applications facultatives (iOS/iPadOS uniquement)

Citrix recommande le déploiement des applications comme **requises**. Les applications requises s'installent silencieusement sur les appareils utilisateur, ce qui minimise l'interaction. L'activation de cette fonctionnalité permet également aux applications de se mettre à jour automatiquement.

Les applications facultatives permettent aux utilisateurs de choisir les applications à installer, mais les utilisateurs doivent initier l'installation manuellement via Citrix Secure Hub.

Pour installer des applications facultatives, les utilisateurs doivent lancer Citrix Secure Hub, aller dans le **magasin**, sélectionner **Détails** pour l'application souhaitée, puis cliquer sur **Ajouter**.



Contrôle d'accès réseau

March 1, 2024

Vous pouvez étendre l'évaluation de la sécurité des appareils Citrix Endpoint Management via votre solution de contrôle d'accès réseau (NAC) pour les appareils Android et Apple. Votre solution NAC utilise ensuite l'évaluation de sécurité Citrix Endpoint Management pour faciliter et gérer les décisions d'authentification. Une fois le boîtier NAC configuré, les stratégies d'appareil et les filtres NAC que vous configurez dans Citrix Endpoint Management sont appliqués.

L'utilisation de Citrix Endpoint Management avec une solution NAC ajoute la qualité de service et un contrôle plus précis sur les appareils internes à votre réseau. Pour un résumé des avantages de l'intégration de NAC avec Citrix Endpoint Management, consultez la section Contrôle d'accès.

Citrix prend en charge ces solutions pour l'intégration à Citrix Endpoint Management :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- NetScaler Gateway
- ForeScout

Citrix ne garantit pas l'intégration avec d'autres solutions NAC.

Avec un boîtier de contrôle d'accès réseau (NAC) dans votre réseau :

- Citrix Endpoint Management prend en charge NAC en tant que fonctionnalité de sécurité de point de terminaison pour les appareils iOS, Android Enterprise et Android.
- Vous pouvez activer les filtres dans Citrix Endpoint Management pour définir les appareils comme conformes ou non conformes pour NAC, en fonction de règles ou de propriétés. Par exemple :
  - Si un appareil géré dans Citrix Endpoint Management ne répond pas aux critères spécifiés, Citrix Endpoint Management le marque comme non conforme. Le boîtier NAC bloque les appareils non conformes sur votre réseau.
  - Si un appareil géré dans Citrix Endpoint Management a installé des applications non conformes, un filtre NAC peut bloquer la connexion VPN. Par conséquent, une machine utilisateur non conforme ne peut pas accéder aux applications ou aux sites Web via le VPN.
  - Si vous utilisez NetScaler Gateway pour NAC, vous pouvez activer le split tunneling pour empêcher le plug-in NetScaler Gateway d'envoyer du trafic réseau inutile à NetScaler Gateway. Pour plus d'informations sur le split tunneling, voir Configurer le split tunneling.

Filtres de conformité NAC pris en charge

Citrix Endpoint Management prend en charge les filtres de conformité au contrôle d'accès réseau (NAC) suivants :

Appareils anonymes : vérifie si un appareil est en mode anonyme. Cette vérification est disponible si Citrix Endpoint Management ne parvient pas à authentifier à nouveau l'utilisateur lorsqu'un appareil tente de se reconnecter.

Applications sur liste noire : vérifie si un appareil dispose d'applications interdites, telles que définies dans une stratégie d'accès aux applications. Pour plus d'informations sur la stratégie, consultez la section Stratégies d'accès aux applications.

Appareils inactifs : vérifie si un appareil est inactif, tel que cela est défini par le paramètre **Nombre de jours maximum d'inactivité** dans la boîte de dialogue **Propriétés du serveur**. Pour de plus amples informations, consultez la section Propriétés du serveur.

Applications requises manquantes : vérifie si des applications nécessaires sont manquantes sur un appareil, tel que cela est défini dans une stratégie d'accès aux applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Applications non suggérées : vérifie si un appareil dispose d'applications non suggérées, telles que définies dans une stratégie d'accès aux applications.

Mot de passe non conforme : vérifie si le mot de passe utilisateur est conforme. Sur les appareils iOS et Android, Citrix Endpoint Management peut déterminer si le mot de passe actuel de l'appareil est conforme à la stratégie de code secret envoyée à l'appareil. Par exemple, sur iOS, l'utilisateur dispose de 60 minutes pour définir un mot de passe si Citrix Endpoint Management envoie une stratégie de code secret à l'appareil. Avant qu'un mot de passe ne soit défini par l'utilisateur, le code secret peut ne pas être conforme.

Appareils non conformes : vérifie si un appareil n'est pas conforme, en fonction de la propriété de l'appareil Non conforme. Cette propriété est généralement modifiée par les actions automatisées ou parce qu'un tiers utilise les API Citrix Endpoint Management.

État révoqué : vérifie si le certificat de l'appareil a été révoqué. Un appareil révoqué ne peut pas se réinscrire tant qu'il n'a pas été à nouveau autorisé.

Appareils Android rootés et iOS jailbreakés : vérifie si un appareil Android ou iOS est rooté ou jailbreaké.

Appareils non gérés : vérifie si Citrix Endpoint Management gère un appareil. Par exemple, un appareil inscrit en mode MAM ou un appareil non inscrit n'est pas géré.

> **Remarque :**
>
> Le filtre Conformité/non conformité implicite définit la valeur par défaut uniquement sur les appareils qui sont gérés par Citrix Endpoint Management. Par exemple, tous les appareils sur lesquels une application bloquée est installée ou qui ne sont pas inscrits sont marqués comme Non conformes. Le boîtier de contrôle d'accès réseau (NAC) bloque ces appareils de votre réseau.

Présentation de la configuration

Nous vous recommandons de configurer les composants NAC dans l'ordre indiqué.

1. Configurez les stratégies d'appareil pour prendre en charge NAC :

   Pour les appareils iOS : voir Configurer la stratégie VPN pour prendre en charge NAC.

   Pour les appareils Android Enterprise : voir Créer une configuration gérée par Android Enterprise pour Citrix SSO.

   Pour les appareils Android : voir Configurer le protocole Citrix SSO pour Android.

2. Activer les filtres NAC dans Citrix Endpoint Management.
3. Configurer une solution NAC :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

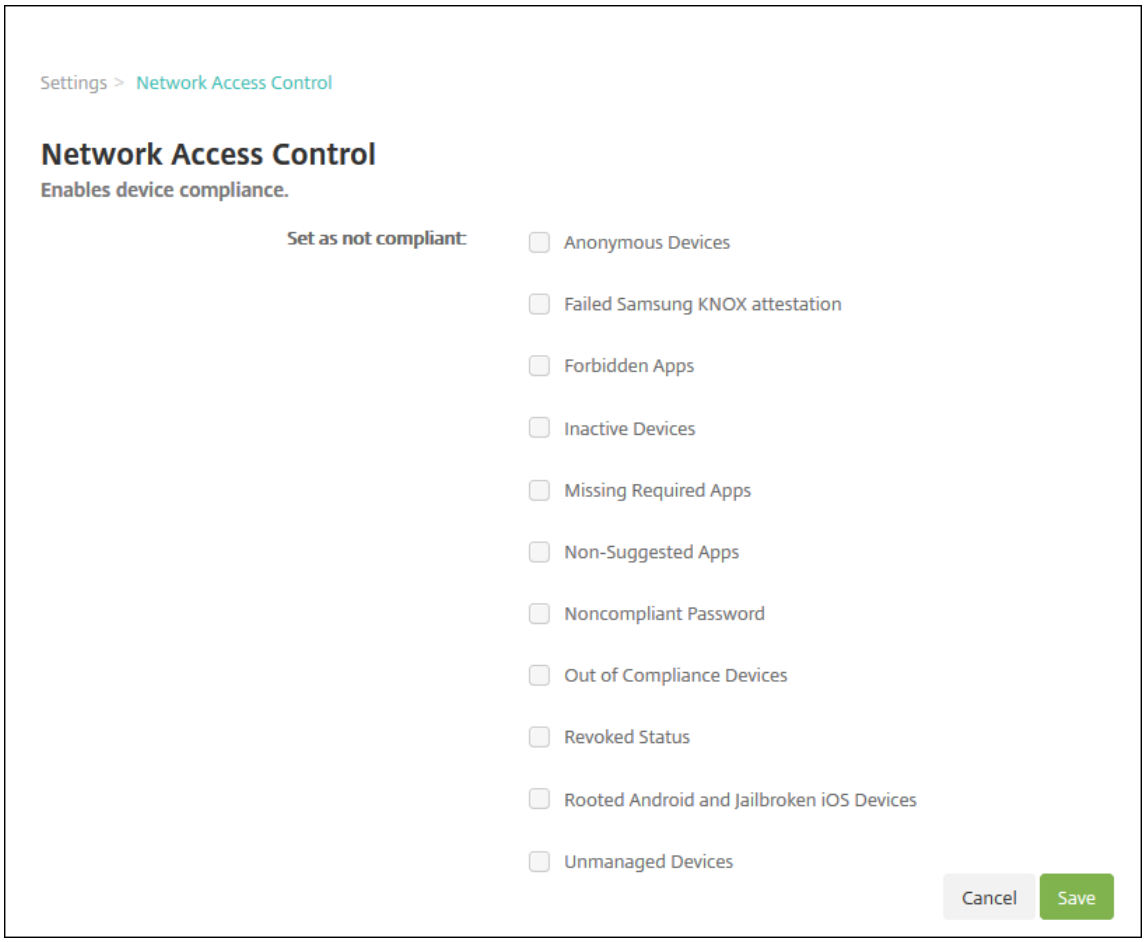
- NetScaler Gateway, détaillé dans Mettre à jour les stratégies NetScaler Gateway afin de prendre en charge NAC.

  Nécessite l'installation de Citrix SSO sur les appareils. Consultez la section Clients NetScaler Gateway.

- ForeScout : consultez la documentation ForeScout.

Activer les filtres NAC dans Citrix Endpoint Management

1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Contrôle d'accès réseau**.



2. Cochez les cases correspondant aux filtres **Définir comme non conforme** que vous souhaitez activer.
3. Cliquez sur **Enregistrer**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Mettre à jour les stratégies NetScaler Gateway afin de prendre en charge NAC

Vous devez configurer les stratégies d'authentification avancée (et non classique) et de sessions VPN sur votre serveur virtuel VPN.

Ces étapes mettent à jour NetScaler Gateway avec l'une des caractéristiques suivantes :

- Intégré à Citrix Endpoint Management.
- Ou, est configuré pour le VPN, ne fait pas partie de l'environnement Citrix Endpoint Management et peut atteindre Citrix Endpoint Management.

Sur votre serveur VPN virtuel, depuis une fenêtre de console, procédez comme suit. Les noms de domaine complet et les adresses IP dans les commandes et les exemples sont fictifs.

1. Supprimez et annulez la liaison de toutes les stratégies classiques si vous utilisez des stratégies classiques sur votre serveur virtuel VPN. Pour vérifier, tapez :

   ```
   show vpn vserver <VPN_VServer>
   ```

   Supprimez tout résultat contenant le terme « Classic ». Pa exemple : `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

   Pour supprimer la stratégie, tapez :

   ```
   unbind vpn vserver <VPN_VServer> -policy <policy_name>
   ```

2. Créez la stratégie de session avancée correspondante en tapant ce qui suit.

   ```
   add vpn sessionPolicy <policy_name> <rule> <session action>
   ```

   Pa exemple : `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. Liez la stratégie à votre serveur virtuel VPN en tapant ce qui suit.

   ```
   bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100
   ```

4. Créez un serveur virtuel d'authentification en tapant ce qui suit.

   ```
   add authentication vserver <authentication vserver name> <service type> <ip address>
   ```

   Par exemple : `add authentication vserver authvs SSL 0.0.0.0`
   Dans l'exemple, `0.0.0.0` signifie que le serveur virtuel d'authentification n'est pas public.

5. Liez un certificat SSL au serveur virtuel en tapant ce qui suit.

   ```
   bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>
   ```

   Pa exemple : `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Associez un profil d'authentification au serveur virtuel d'authentification à partir du serveur virtuel VPN. Commencez par créer le profil d'authentification en tapant ce qui suit.

   ```
   add authentication authnProfile <profile name> -authnVsName <
   authentication vserver name>
   ```

   Par exemple :

   ```
   add authentication authnProfile xm_nac_prof -authnVsName authvs
   ```

7. Associez le profil d'authentification au serveur virtuel VPN en tapant ce qui suit.

   ```
   set vpn vserver <vpn vserver name> -authnProfile <authn profile
   name>
   ```

   Par exemple :

   ```
   set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof
   ```

8. Vérifiez la connexion de NetScaler Gateway à un appareil en tapant ce qui suit.

   ```
   curl -v -k https://<Endpoint Management_server>:4443/Citrix/
   Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_<
   device_id>"
   ```

   Par exemple, cette requête vérifie la connectivité en obtenant l'état de conformité du premier appareil (`deviceid_1`) inscrit dans l'environnement :

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header
    "X-Citrix-VPN-Device-ID: deviceid_1"
   ```

   Un résultat réussi est similaire à l'exemple suivant.

   ```
   HTTP/1.1 200 OK
   < Server: Apache-Coyote/1.1
   < X-Citrix-Device-State: Non Compliant
   < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   <!--NeedCopy-->
   ```

9. Lorsque l'étape précédente réussit, créez l'action d'authentification Web sur Citrix Endpoint Management. Commencez par créer une expression de stratégie pour extraire l'ID d'appareil du plug-in VPN iOS. Tapez ce qui suit.

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY
   (10000).TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"
   ```

10. Envoyez la requête à Citrix Endpoint Management en tapant ce qui suit. Dans cet exemple, l'adresse IP Citrix Endpoint Management est `10.207.87.82` et le nom de domaine complet est `example.em.cloud.com:4443`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -
serverPort 4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP
/1.1\r\n"+ "Host: example.em.cloud.com:4443\r\n"+ "X-Citrix-VPN-
Device-ID: "+ xm_deviceid_expression + "\r\n\r\n"} -scheme https
 -successRule "HTTP.RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-
Citrix-Device-State\").EQ(\"Compliant\")"
```

L'état `HTTP status 200 OK` indique une réussite de NAC Citrix Endpoint Management. La valeur de l'en-tête `X-Citrix-Device-State` doit être `Compliant`.

11. Créez une stratégie d'authentification avec laquelle associer l'action en tapant ce qui suit.

    ```
    add authentication Policy <policy name> -rule <rule> -action <web
     authentication action>
    ```

    Pa exemple : `add authentication Policy xm_nac_webauth_pol -rule "HTTP .REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac`

12. Convertissez la stratégie LDAP existante en une stratégie avancée en tapant ce qui suit.

    ```
    add authentication Policy <policy_name> -rule <rule> -action <
    LDAP action name>
    ```

    Pa exemple : `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. Ajoutez un intitulé de stratégie avec lequel associer la stratégie LDAP en tapant ce qui suit.

    ```
    add authentication policylabel <policy_label_name>
    ```

    Pa exemple : `add authentication policylabel ldap_pol_label`

14. Associez la stratégie LDAP à l'intitulé de stratégie en tapant ce qui suit.

    ```
    bind authentication policylabel ldap_pol_label -policyName
    ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
    ```

15. Connectez un périphérique compatible pour effectuer un test NAC afin de vérifier si l'authentification LDAP réussit. Tapez ce qui suit.

    ```
    bind authentication vserver <authentication vserver> -policy <web
     authentication policy> -priority 100 -nextFactor <ldap policy
    label> -gotoPriorityExpression END
    ```

16. Ajoutez l'interface utilisateur à associer au serveur virtuel d'authentification. Tapez la commande suivante pour récupérer l'ID d'appareil.

    ```
    add authentication loginSchemaPolicy <schema policy>-rule <rule>
    -action lschema_single_factor_deviceid
    ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

17. Liez le serveur virtuel d'authentification en tapant ce qui suit.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -
priority 100 -gotoPriorityExpression END
```

18. Créez une stratégie d'authentification avancée LDAP pour activer la connexion Citrix Secure Hub. Tapez ce qui suit.

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER
(\"User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP
```

```
bind authentication vserver authvs -policy ldap_xm_test_pol -
priority 110 -gotoPriorityExpression NEXT
```

Windows Desktop et Tablet

December 11, 2023

Citrix Endpoint Management inscrit les appareils Windows 10 et Windows 11 en mode MDM. Citrix Endpoint Management prend en charge les types d'authentification suivants pour les appareils Windows 10 et Windows 11 inscrits en mode MDM :

- Authentification basée sur un domaine
  - Active Directory
  - Azure Active Directory
- Fournisseurs d'identité :
  - Azure Active Directory
  - Fournisseur d'identité Citrix

Pour de plus amples informations sur les types d'authentification pris en charge, consultez la section Certificats et authentification.

Un workflow général pour le démarrage de la gestion des appareils Windows 10 ou Windows 11 est le suivant :

1. Effectuez le processus d'intégration. Consultez les sections Intégration et configuration des ressources et Préparation à l'inscription d'appareils et à la mise à disposition de ressources.

   Si vous prévoyez d'inscrire des appareils Windows à l'aide du service de détection automatique, vous devez configurer le service de détection automatique Citrix. Contactez le support technique Citrix pour obtenir de l'aide. Pour de plus amples informations, consultez la section Demander la détection automatique pour les appareils Windows.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Choisissez et configurez une méthode d'inscription. Consultez la section Méthodes d'inscription prises en charge.
3. Configurez les stratégies d'appareil Windows Desktop et Tablet.
4. Les utilisateurs inscrivent des appareils Windows 10 et Windows 11.
5. Configurez les actions de sécurité des appareils et des applications. Consultez la section Actions de sécurisation.

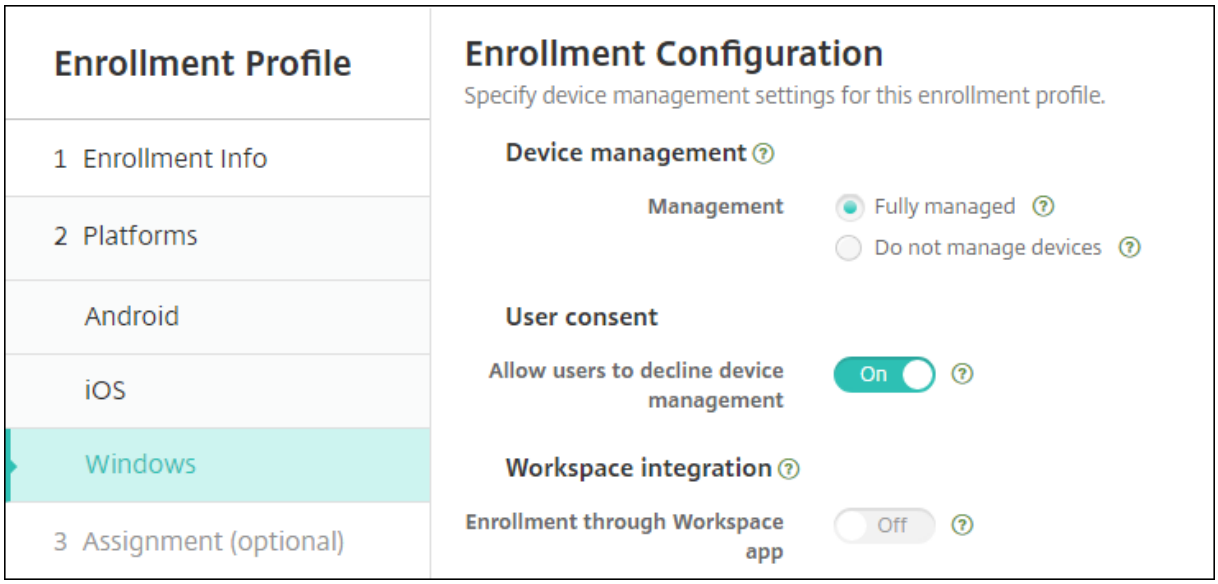
Pour les systèmes d'exploitation pris en charge, consultez la section Systèmes d'exploitation d'appareils pris en charge.

Méthodes d'inscription prises en charge

Vous spécifiez comment gérer les appareils Windows 10 et Windows 11 dans les profils d'inscription. Deux options sont disponibles :

- Entièrement géré (inscription MDM)
- Ne pas gérer les appareils (pas d'inscription MDM)

Pour configurer les paramètres d'inscription pour les appareils Windows 10 et Windows 11, accédez à **Configurer > Profils d'inscription > Windows**. Pour de plus amples informations sur les profils d'inscription, consultez la section Profils d'inscription.



Le tableau suivant indique les méthodes d'inscription prises en charge par Citrix Endpoint Management pour les appareils Windows 10 et Windows 11 :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Méthode	Pris en charge
Inscription Azure Active Directory	Oui
Inscription Service de détection automatique	Oui
Inscription en bloc de Windows	Oui
Inscription manuelle	Oui
Invitations d'inscription	Non

> **Remarque :**
>
> - L'inscription manuelle exige que les utilisateurs entrent un nom de domaine complet (FQDN) du serveur Citrix Endpoint Management. Nous ne recommandons pas d'utiliser l'inscription manuelle. Utilisez plutôt d'autres méthodes pour simplifier le processus d'inscription pour les utilisateurs.
> - Vous ne pouvez pas envoyer d'invitations d'inscription aux appareils Windows. Les utilisateurs Windows s'inscrivent directement sur leurs appareils.

Configurer les stratégies d'appareil Windows Desktop et Tablet

Utilisez ces stratégies pour configurer l'interaction entre Citrix Endpoint Management et les appareils exécutant Windows 10 ou Windows 11. Ce tableau répertorie toutes les stratégies d'appareils disponibles pour les appareils Windows Desktop et Tablet.

| | | |
|—|—|—|
|[Configuration d'applications](/fr-fr/citrix-endpoint-management/policies/app-configuration-policy.html#windows-desktoptablet-settings) |[Inventaire des applications](/fr-fr/citrix-endpoint-management/policies/app-inventory-policy.html) |[Mode kiosque](/fr-fr/citrix-endpoint-management/policies/ap
lock-policy.html#windows-desktop-and-tablet-settings) |
|[Désinstallation des applications](/fr-fr/citrix-endpoint-management/policies/app-uninstall-policy.html) |[Application Guard](/fr-fr/citrix-endpoint-management/policies/application-guard-policy.html) |[BitLocker](/fr-fr/citrix-endpoint-management/policies/bitlocker-policy.html#windows-desktop-and-tablet-settings) |
|[Informations d'identification](/fr-fr/citrix-endpoint-management/policies/credentials-policy.html#windows-desktoptablet-settings) |[XML personnalisé](/fr-fr/citrix-endpoint-management/policies/custom-xml-policy.html) |[Defender](/fr-fr/citrix-endpoint-management/policies/defender-policy.html) |
|[Device Guard](/fr-fr/citrix-endpoint-management/policies/device-guard-policy.html) |[Attestation de l'intégrité des appareils](/fr-fr/citrix-endpoint-management/policies/device-health-attestation-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

policy.html) |[Exchange](/fr-fr/citrix-endpoint-management/policies/exchange-policy.html#windows-desktoptablet-settings) |
[Pare-feu](/fr-fr/citrix-endpoint-management/policies/firewall-device-policy.html#windows-desktop-and-tablet-settings)	[Kiosque](/fr-fr/citrix-endpoint-management/policies/kiosk-policy.html#windows-desktop-and-tablet-settings)	[Réseau](/fr-fr/citrix-endpoint-management/policies/network-policy.html#windows-desktoptablet-settings)
[Bureau](/fr-fr/citrix-endpoint-management/policies/office-policy.html)	[Mise à jour d'OS](/fr-fr/citrix-endpoint-management/policies/control-os-updates.html#windows-desktop-and-tablet-settings)	[Code secret](/fr-fr/citrix-endpoint-management/policies/passcode-policy.html#windows-desktoptablet-settings)
[Restrictions](/fr-fr/citrix-endpoint-management/policies/restrictions-policy.html#windows-desktoptablet-settings)	[Magasin](/fr-fr/citrix-endpoint-management/policies/store-policy.html)	[Termes et conditions](/fr-fr/citrix-endpoint-management/policies/terms-and-conditions-policy.html#windows-tablet-settings)
[VPN](/fr-fr/citrix-endpoint-management/policies/vpn-policy.html#windows-desktoptablet-settings)	[Clips Web](/fr-fr/citrix-endpoint-management/policies/webclip-policy.html#windows-desktoptablet-settings)	[Agent Windows](/fr-fr/citrix-endpoint-management/policies/windows-agent-policy.html)
Configuration de GPO WindowsWindows	Windows Hello Entreprise

Inscrire des appareils Windows 10 et Windows 11 via Azure Active Directory

> **Important :**
>
> Avant que les utilisateurs puissent s'inscrire, vous devez configurer les paramètres Azure Active Directory (AD) dans Azure, puis configurer Citrix Endpoint Management. Pour de plus amples informations, consultez la section Connecter Citrix Endpoint Management à Azure AD.

Les appareils Windows 10 et Windows 11 peuvent s'inscrire à Azure afin de fédérer l'authentification Active Directory. Cette inscription nécessite un abonnement Azure AD Premium.

Vous pouvez joindre des appareils Windows 10 et Windows 11 à Microsoft Azure AD à l'aide de l'une des méthodes suivantes :

- Pour les appareils appartenant à l'entreprise :
  - Inscription dans MDM lorsque l'appareil est joint à Azure AD la première fois que les appareils sont allumés. Dans ce scénario, les utilisateurs effectuent l'inscription comme décrit dans cet article : https://docs.microsoft.com/en-us/azure/active-directory/devices/azuread-joined-devices-frx.

    Pour les appareils Windows que vous inscrivez avec cette méthode, vous pouvez utiliser Windows AutoPilot pour configurer et pré-configurer les appareils. Pour de plus amples

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

informations, consultez la section Utilisation de Windows AutoPilot pour installer et configurer les appareils.

  - Inscription dans MDM lorsque l'appareil est joint à Azure AD à partir de la page **Paramètres** de Windows une fois que l'appareil a été configuré. Dans ce scénario, les utilisateurs effectuent l'inscription comme décrit dans Inscription dans MDM lorsque l'appareil est joint à Azure AD après avoir configuré des appareils.

- Pour les appareils personnels (BYOD ou appareils mobiles) :
  - Inscription dans MDM lors de l'enregistrement dans Azure AD tout en ajoutant le compte professionnel Microsoft à Windows. Dans ce scénario, les utilisateurs effectuent l'inscription comme décrit dans Inscription dans MDM lors de l'enregistrement dans Azure AD.

Inscription dans MDM lorsque l'appareil est joint à Azure AD après avoir configuré des appareils

1. Sur un appareil, dans le menu Démarrer, accédez à **Paramètres > Comptes > Accès Professionnel ou Scolaire**, puis cliquez sur **Connecter**.
2. Dans la boîte de dialogue **Configurer un compte professionnel ou scolaire**, sous **Autres actions**, cliquez sur **Joindre cet appareil à Azure Active Directory**.
3. Entrez les informations d'identification Azure AD et cliquez sur **Se connecter**.
4. Acceptez les conditions générales requises par l'organisation.
   - Si les utilisateurs cliquent sur **Refuser**, l'appareil ne rejoint pas Azure AD et ne s'inscrit pas à Citrix Endpoint Management.
5. Cliquez sur **Joindre** pour poursuivre le processus d'inscription.
6. Cliquez sur **Terminé** pour terminer le processus d'inscription.

Inscription dans MDM lors de l'enregistrement dans Azure AD

1. Sur un appareil, dans le menu Démarrer, accédez à **Paramètres > Comptes > Accès Professionnel ou Scolaire**, puis cliquez sur **Connecter**.
2. Dans la boîte de dialogue **Configurer un compte professionnel ou scolaire**, entrez les informations d'identification Azure AD et cliquez sur **Se connecter**.
3. Acceptez les conditions générales requises par l'organisation. L'appareil est enregistré dans Azure AD et s'inscrit à Citrix Endpoint Management.
   - Si les utilisateurs cliquent sur **Refuser**, l'appareil est enregistré dans Azure AD mais ne s'inscrit pas à Citrix Endpoint Management. Le bouton **Info** n'est pas disponible sur le compte.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Cliquez sur **Joindre** pour poursuivre le processus d'inscription.
5. Cliquez sur **Terminé** pour terminer le processus d'inscription.

Inscrire des appareils Windows à l'aide du service de détection automatique

Pour configurer le service de détection automatique pour les appareils Windows, demandez de l'aide au support technique Citrix. Pour de plus amples informations, consultez la section Demander la détection automatique pour les appareils Windows.

> **Remarque :**
>
> Pour pouvoir inscrire des appareils Windows, le certificat d'écoute SSL doit être un certificat SSL. L'inscription échoue pour les certificats SSL auto-signés.

Les utilisateurs effectuent les étapes suivantes pour effectuer l'inscription :

1. Sur un appareil, dans le menu Démarrer, accédez à **Paramètres > Comptes > Accès Professionnel ou Scolaire**, puis cliquez sur **S'inscrire uniquement à la gestion des périphériques**.
2. Dans la boîte de dialogue **Configurer un compte professionnel ou scolaire**, entrez une adresse e-mail d'entreprise et cliquez sur **Suivant**.

   Pour vous inscrire en tant qu'utilisateur local, entrez une nouvelle adresse de messagerie avec le nom de domaine correct (par exemple, `foo\@mydomain.com`). Cette étape permet à l'utilisateur de contourner une limitation Microsoft connue avec laquelle la gestion des appareils intégrée sous Windows effectue l'inscription. Dans la boîte de dialogue **Connexion à un service**, entrez le nom d'utilisateur et le mot de passe associés à l'utilisateur local. L'appareil découvre ensuite un serveur Citrix Endpoint Management et démarre le processus d'inscription.
3. Entrez les informations d'identification et cliquez sur **Continuer**.
4. Dans la boîte de dialogue **Termes d'utilisation**, acceptez que votre appareil soit géré, puis cliquez sur **Accepter**.

L'inscription d'appareils Windows associés à un domaine via le service de détection automatique échoue si la stratégie de domaine désactive l'inscription MDM. Les utilisateurs peuvent utiliser l'une des méthodes suivantes à la place :

- Supprimez les appareils du domaine, effectuez l'inscription et joignez de nouveau les appareils.
- Entrez le nom de domaine complet du serveur Citrix Endpoint Management pour continuer.

Inscription en bloc de Windows

Avec l'inscription en bloc de Windows, vous pouvez configurer de nombreux appareils pouvant être gérés par un serveur MDM sans avoir besoin de réimager les appareils. Vous pouvez utiliser un package

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de provisioning pour l'inscription en bloc d'appareils Windows 10 et Windows 11 Desktop et Tablet. Pour de plus amples informations, consultez la section Inscription en bloc d'appareils Windows.

Actions de sécurisation

Les appareils Windows 10 et Windows 11 prennent en charge les actions de sécurité suivantes. Pour obtenir une description de chaque action, consultez la section Actions de sécurisation.

Localiser	Verrouiller	Redémarrer
Révoquer	Effacer les données d'entreprise	Effacer

Connecter Citrix Endpoint Management à Azure AD

Les appareils Windows 10 et Windows 11 peuvent s'inscrire avec Azure. Les utilisateurs créés dans Azure AD peuvent avoir accès aux appareils. Citrix Endpoint Management est déployé dans Microsoft Azure en tant que service MDM. La connexion d'Citrix Endpoint Management à Azure AD permet aux utilisateurs d'inscrire automatiquement leurs appareils à Citrix Endpoint Management lorsqu'ils les inscrivent dans Azure AD.

Pour connecter Citrix Endpoint Management à Azure AD, effectuez les opérations suivantes :

1. Dans le portail Azure, accédez à **Azure Active Directory > Mobilité (gestion des données de référence et gestion des applications mobiles) > Ajouter une application**, puis cliquez sur **Paramètres d'application GPM locale**.
2. Donnez un nom à l'application et cliquez sur **Ajouter**.
3. (Facultatif) Azure n'autorise pas l'utilisation de domaines non vérifiés, tels que cloud.com, pour la configuration de l'IDP. Si votre nom de domaine complet d'inscription à Citrix Endpoint Management inclut cloud.com, contactez le support Citrix et fournissez-leur l'enregistrement TXT provenant d'Azure. Le support Citrix vérifie le sous-domaine, ce qui vous permet de poursuivre votre configuration. Si votre nom de domaine complet se trouve sous votre propre domaine, vous pouvez le vérifier normalement dans Azure.
4. Sélectionnez l'application que vous avez créée, configurez les éléments suivants, puis cliquez sur **Enregistrer**.
   - **Portée de l'utilisateur GDR**. Sélectionnez **Tout**.
   - **URL des conditions d'utilisation de GDR**. Entrez au format `https://<Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe/tou`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **URL de détection GAM**. Entrez au format `https://<Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe`.

5. Cliquez sur **Paramètres d'application GPM locale**.

   - Dans le volet **Propriétés**, définissez **URI ID d'application** au format `https://<Citrix Endpoint Management Enrollment FQDN>:8443`. Cet URI d'ID d'application est un ID unique que vous ne pouvez pas réutiliser dans une autre application.
   - Dans le volet **Autorisations nécessaires**, sélectionnez **Microsoft Graph** et **Windows Azure Active Directory**.
   - Dans le volet **Clés**, créez la clé d'authentification. Cliquez sur **Enregistrer** pour afficher la valeur de la clé. La valeur de la clé n'apparaît qu'une seule fois. Enregistrez la clé pour une utilisation ultérieure. Vous avez besoin de la clé à l'étape 7.

6. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Fournisseur d'identité (IDP)**, puis cliquez sur **Ajouter**.

7. Sur la page **URL de détection**, configurez les éléments suivants et cliquez sur **Suivant**.

   - **Nom IdP**. Entrez un nom unique pour identifier la connexion de fournisseur d'identité que vous créez.
   - **Type d'IdP**. Sélectionnez **Azure Active Directory**.
   - **ID du locataire**. **ID de répertoire** dans Azure. Vous le voyez lorsque vous accédez à **Azure Active Directory > Propriétés** dans Azure.

8. Sur la page **Informations sur Windows MDM**, configurez ce qui suit et cliquez sur **Suivant**.

   - **URI d'ID de l'application :** URI de l'ID de l'application que vous avez saisie dans Azure.
   - **ID client**. ID d'application que vous voyez dans le volet **Propriétés** dans Azure.
   - **Clé**. Valeur de clé que vous avez créée et enregistrée à l'étape 4 ci-dessus.

9. Sur la page **Utilisation des revendications IdP**, configurez les éléments suivants et cliquez sur Suivant.

   - **Type d'identificateur d'utilisateur**. Sélectionnez **userPrincipalName**.
   - **Chaîne d'identificateur d'utilisateur**. Entrez `${ id_token } .upn`.

10. Cliquez sur **Save**.

11. Ajoutez un utilisateur Azure AD en tant qu'utilisateur local et affectez-le à un groupe d'utilisateurs local.

12. Créez une stratégie Termes et conditions et un groupe de mise à disposition qui inclut ce groupe d'utilisateurs local.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Gestion des appareils avec une intégration à Workspace Environment Management

Si vous utilisez uniquement Workspace Environment Management (WEM), les déploiements MDM ne sont pas possibles. Si vous utilisez uniquement Citrix Endpoint Management, vous êtes limité à la gestion des appareils Windows 10 et Windows 11. En intégrant les deux solutions, vous pouvez accéder aux fonctionnalités MDM via WEM et vous pouvez gérer un plus large éventail de systèmes d'exploitation Windows via Citrix Endpoint Management. Cette gestion prend la forme de la configuration d'objets de stratégie de groupe Windows. Actuellement, les administrateurs importent un fichier ADMX dans Citrix Endpoint Management et le transmettent sur les appareils Windows 10 et Windows 11 Desktop et Tablet pour configurer des applications spécifiques. À l'aide de la stratégie de configuration de GPO Windows, vous pouvez configurer des objets de stratégie de groupe et transmettre des modifications au service WEM. L'agent WEM applique ensuite les objets de stratégie de groupe aux appareils et à leurs applications.

La gestion MDM n'est pas requise pour l'intégration WEM. Vous pouvez transmettre les configurations d'objet de stratégie de groupe vers n'importe quel appareil pris en charge par WEM, même si Citrix Endpoint Management ne prend pas en charge l'appareil en mode natif.

Pour obtenir une liste des appareils pris en charge, consultez la section Configuration requise pour le système d'exploitation.

Les appareils qui reçoivent la stratégie de configuration de GPO Windows s'exécutent dans un nouveau mode Citrix Endpoint Management appelé WEM. Dans la liste **Gérer > Appareils** des appareils inscrits, la colonne **Mode** des appareils gérés par WEM répertorie **WEM**.

Pour de plus amples informations, consultez la section Stratégie de configuration de GPO Windows.

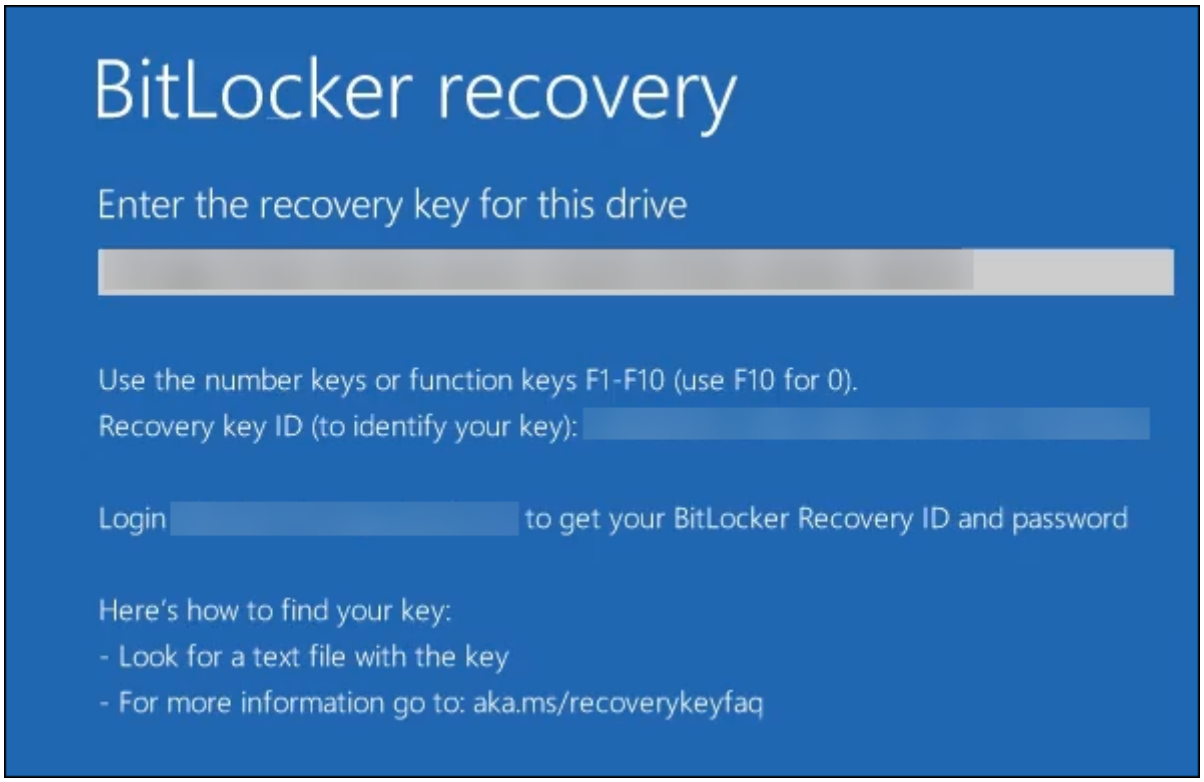
Clé de récupération BitLocker

Le cryptage des disques à l'aide de BitLocker est une fonction de sécurité utile. Cependant, le déverrouillage des appareils peut s'avérer complexe si un utilisateur perd sa clé de récupération BitLocker. Citrix Endpoint Management peut désormais enregistrer automatiquement et en toute sécurité les clés de récupération BitLocker pour les utilisateurs. Les utilisateurs peuvent trouver leur clé de récupération BitLocker sur le portail en libre-service. Pour activer et trouver la clé de récupération BitLocker, procédez comme suit :

1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Propriétés du serveur**.
2. Recherchez `shp` et activez la fonctionnalité `shp.console.enable`. Assurez-vous que `enable.new.shp` reste désactivé. Pour plus d'informations sur l'activation du portail en libre-service, consultez la section Configurer les modes d'inscription sécurisée.
3. Accédez à **Configurer > Stratégies d'appareil**. Recherchez votre stratégie BitLocker ou créez-en une et activez le paramètre **Récupération des données de BitLocker sur Citrix Endpoint Management**.

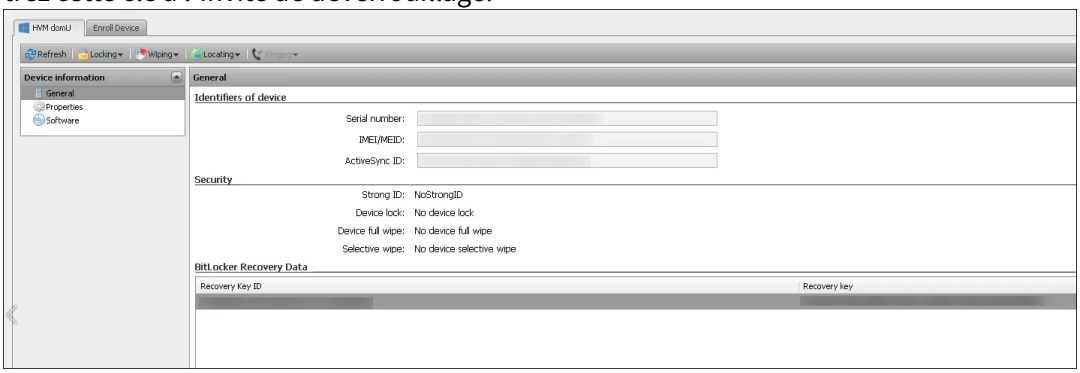
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Lors du déverrouillage de leur appareil, les utilisateurs voient un message les invitant à entrer leur clé. Le message affiche également l'ID de clé de récupération.



Pour trouver leur clé de récupération BitLocker, les utilisateurs accèdent au portail en libre-service.

1. Dans le panneau **Général**, accédez à **Données de récupération de BitLocker**.
   - **ID de la clé de récupération :** identifiant de la clé de récupération BitLocker utilisée pour crypter le disque. Cet ID doit correspondre à l'ID de clé indiqué dans le message précédent.
   - **Clé de récupération :** clé que l'utilisateur doit entrer pour déverrouiller son disque. Entrez cette clé à l'invite de déverrouillage.



Pour plus d'informations sur la stratégie BitLocker, consultez la section Stratégie BitLocker.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Inscription en bloc d'appareils Windows

November 29, 2023

Citrix Endpoint Management prend en charge l'inscription en bloc d'appareils Windows 10 et Windows 11 Desktop et Tablet. Avec l'inscription en bloc, vous pouvez configurer de nombreux appareils pouvant être gérés par Citrix Endpoint Management sans avoir besoin de créer une nouvelle image des appareils. Vous utilisez le package de provisioning pour l'inscription en bloc.

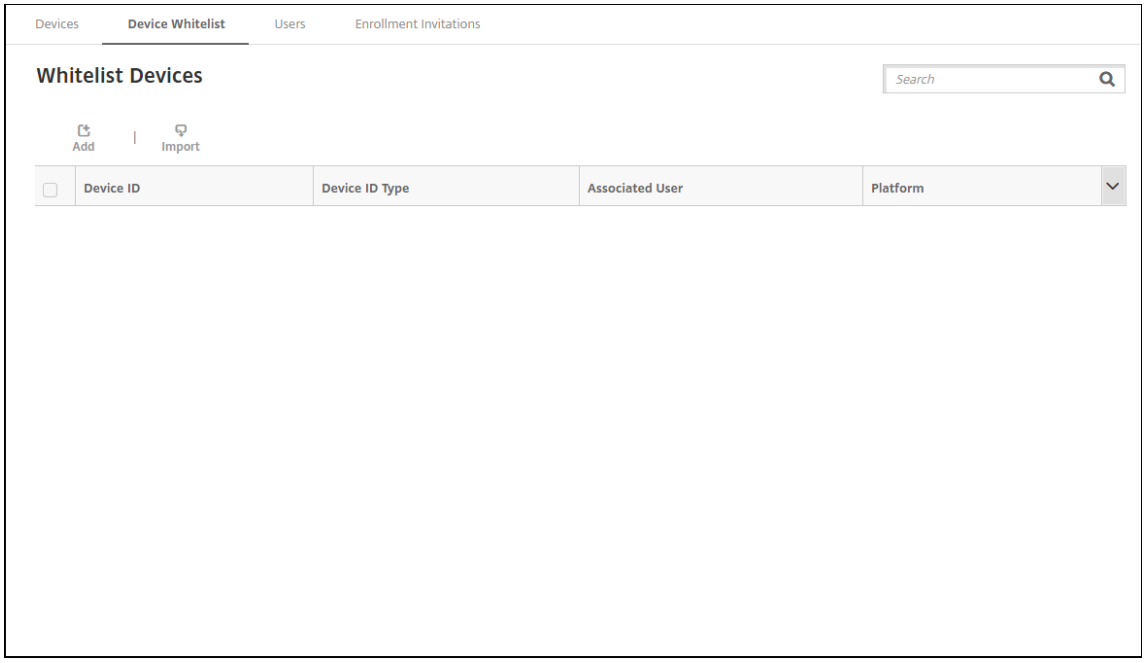
Veuillez trouver ci-dessous un workflow général pour inscrire en bloc des appareils Windows 10 et Windows 11 :

1. Attribuez des appareils. Vous pouvez effectuer les attributions par appareil ou en bloc.
2. Configurez l'inscription en bloc.
3. Créez un package de provisioning et appliquez ce package par appareil.

Avant d'exécuter l'inscription en bloc, assurez-vous d'attribuer tous les appareils aux utilisateurs appropriés. Vous pouvez effectuer ces attributions en ajoutant les appareils un à la fois ou en bloc.

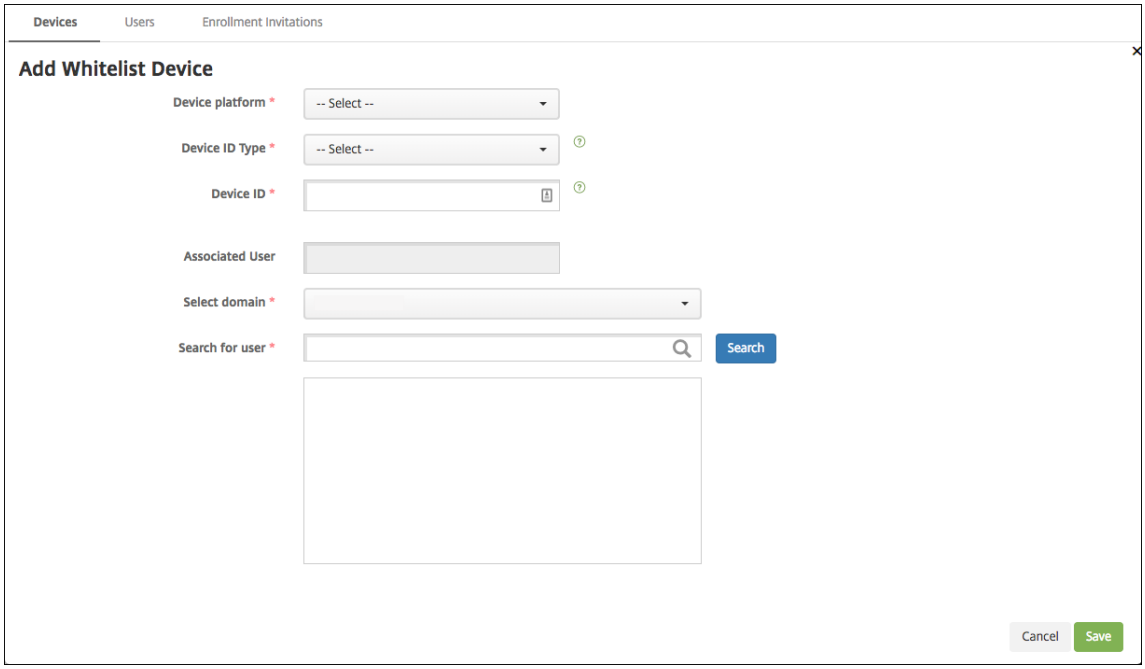
Effectuer des attributions par appareil

1. Dans la console Citrix Endpoint Management, accédez à **Gérer > Appareils > Liste d'appareils autorisés**.



2. Pour ajouter chaque appareil, cliquez sur **Ajouter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Entrez les informations suivantes :

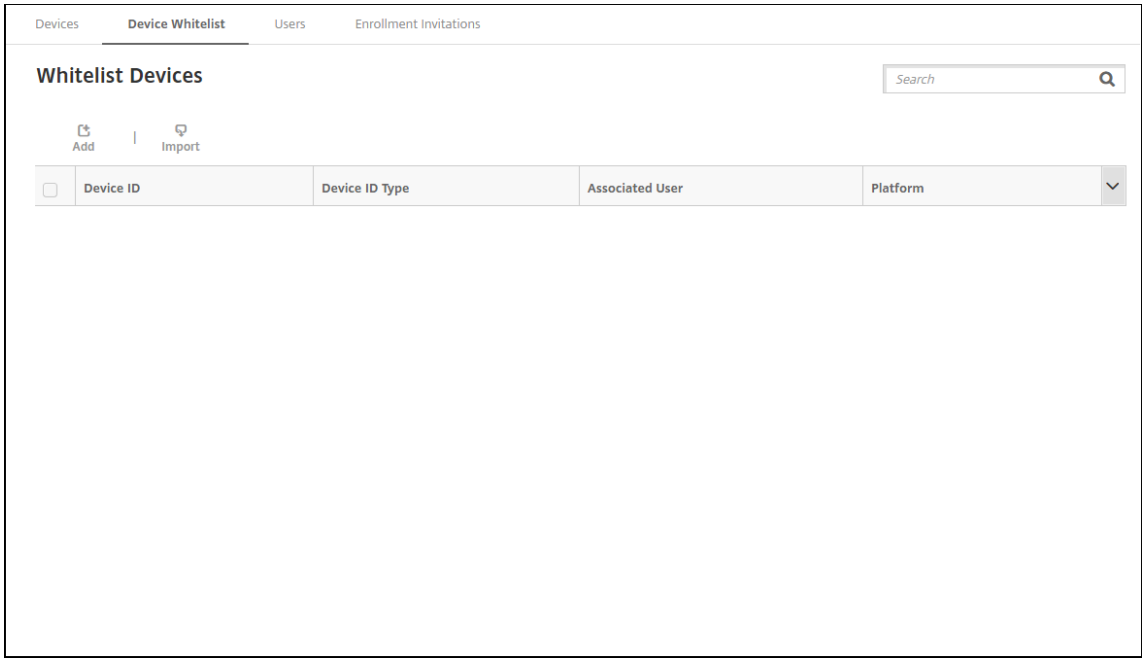
   - **Plate-forme de l'appareil :** sélectionnez **Windows**.
   - **Type d'ID d'appareil :** sélectionnez un ID à utiliser pour identifier l'appareil. Citrix Endpoint Management prend en charge l'**ID de matériel** et le **nom de l'appareil** pour les appareils Windows.
   - **ID de l'appareil :** saisissez l'ID correspondant au type que vous avez sélectionné précédemment pour l'appareil.
   - **Utilisateur associé :** affiche l'utilisateur associé pour cet appareil. Ce champ s'affiche automatiquement avec l'utilisateur que vous sélectionnez.
   - **Sélectionner domaine :** sélectionnez le domaine à partir duquel vous voulez rechercher un utilisateur associé.
   - **Rechercher un utilisateur :** saisissez le nom d'utilisateur entier ou partiel dans ce champ, puis cliquez sur **Rechercher** pour rechercher un utilisateur à associer à cet appareil.

4. Cliquez sur **Save**.

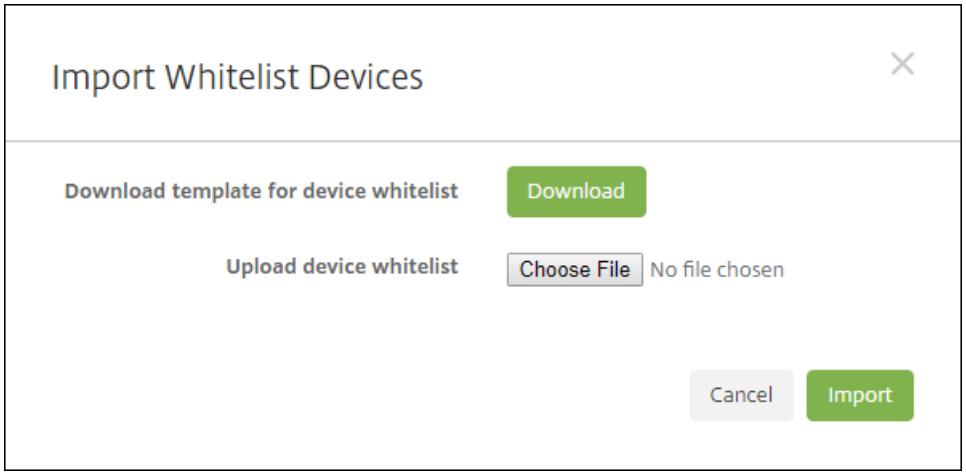
Ajouter des appareils en bloc

1. Dans la console Citrix Endpoint Management, accédez à **Gérer > Appareils > Liste d'appareils autorisés**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Cliquez sur **Importer**.



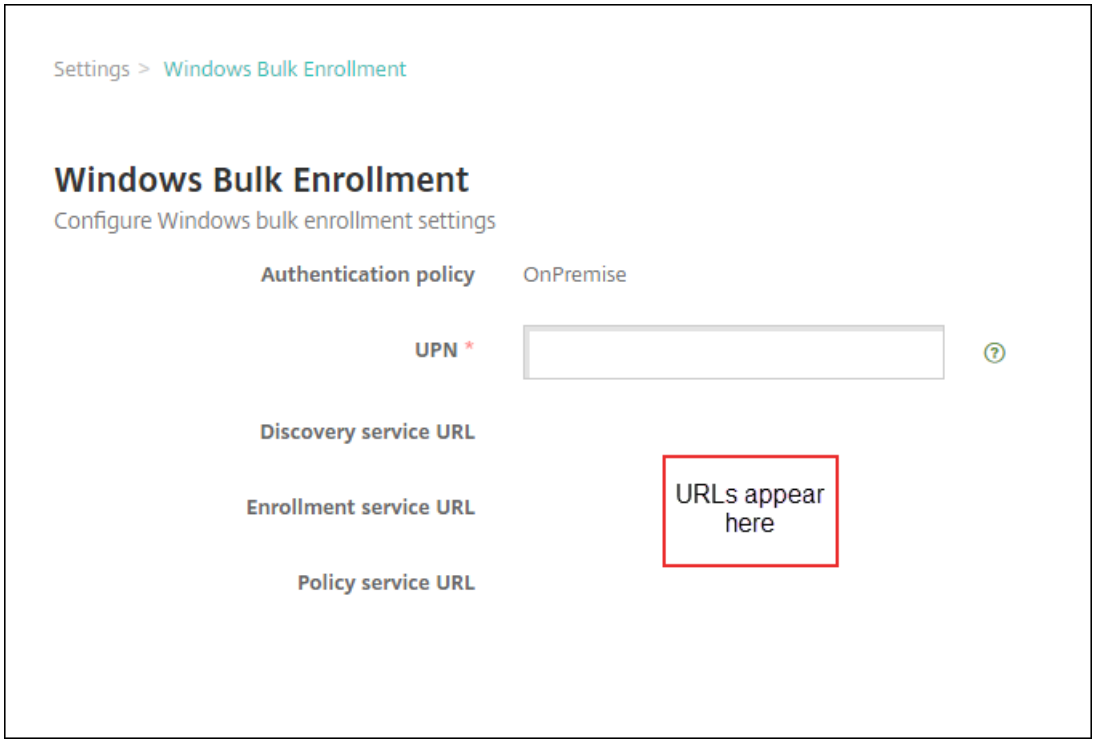
3. Cliquez sur **Télécharger** pour télécharger un modèle (feuille de calcul) pour les appareils figurant sur une liste d'autorisation. Remplissez cette feuille de calcul, puis chargez la feuille de calcul à l'aide des options **Choisir un fichier** et **Importer**.

Configurer l'inscription en bloc

1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Inscription en bloc de Windows**.
2. Dans le champ **UPN**, tapez un nom d'utilisateur à utiliser pour déployer tous les appareils. Le nom UPN doit être un utilisateur valide dans Citrix Endpoint Management disposant des autori-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sations d'inscription. Vous pouvez fournir un UPN différent de l'utilisateur associé que vous avez sélectionné précédemment.



Vous avez besoin des URL lors de la création d'un package de provisioning dans le Concepteur de configuration Windows.

3. Cliquez sur **Save**.

Créer et appliquer un package de provisioning

Pour provisionner des appareils en bloc, téléchargez le Concepteur de configuration Windows depuis le Microsoft Store. Le Concepteur de configuration Windows crée des packs de provisioning utilisés pour imager les appareils. Dans le cadre de ces packages, vous pouvez inclure les paramètres de configuration d'inscription en bloc Citrix Endpoint Management pour que les appareils provisionnés s'inscrivent automatiquement dans Citrix Endpoint Management.

Pour plus d'informations sur l'utilisation d'un package de provisioning, consultez la section https://docs.microsoft.com/en-us/windows/client-management/mdm/bulk-enrollment-using-windows-provisioning-tool. Suivez les étapes décrites dans la section *Créer et appliquer un package de provisioning pour l'authentification locale* dans ce document. Suivez ces étapes pour inclure les paramètres de configuration d'inscription en bloc Citrix Endpoint Management suivants et pour appliquer le package à chaque appareil.

- **URL du service de détection**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **URL du service d'inscription**
- **URL du service de stratégies**
- **Secret**. Mot de passe de l'UPN. Vous avez déjà tapé le nom d'utilisateur dans le champ UPN.

Inscription en bloc d'appareils prêts à l'emploi

Citrix Endpoint Management prend en charge l'inscription en bloc d'appareils Windows prêts à l'emploi. Suivez ces étapes pour configurer et effectuer l'inscription en bloc.

1. Utilisez la console Citrix Endpoint Management pour ajouter des appareils (attribution par appareil ou en boc) et configurer l'inscription en bloc. Pour de plus amples informations, consultez la section Ajouter des appareils en bloc et Configurer l'inscription en bloc.
2. Créez un package de provisioning, comme décrit dans la section Créer et appliquer un package de provisioning.

   > **Remarque :**
   >
   > Vous devez configurer le nom de l'appareil pour chaque appareil lors de la création d'un package de provisioning. Pour ce faire, dans le Concepteur de configuration Windows, accédez à **Paramètres d'exécution > Comptes > CompteOrdinateur > NomOrdinateur** et spécifiez le nom de l'appareil. Le nom de l'appareil que vous spécifiez pour chaque appareil doit correspondre au nom que vous avez utilisé lors de l'importation de la liste d'autorisation des appareils.

3. Placez ce package de provisioning sur une clé USB.
4. Insérez la clé USB dans la machine cible la première fois que l'utilisateur allume l'appareil.

   L'appareil Windows détecte automatiquement le package de provisioning (.ppkg) sur la clé USB. Pour obtenir des instructions détaillées, consultez la documentation Microsoft sur la façon d'appliquer un package d'approvisionnement lors de la configuration initiale.

L'appareil est inscrit automatiquement dans Citrix Endpoint Management.

Pour les appareils exécutant Windows 10 (version 2004 ou ultérieure) ou Windows 11, vous pouvez simplifier le processus d'inscription en créant un seul package de provisioning. Le package peut ensuite être appliqué à tous les appareils. Par conséquent, vous n'avez plus besoin de créer un package de provisioning par appareil.

Pour simplifier le processus d'inscription, effectuez les étapes suivantes lors de la création d'un package de provisioning :

1. Dans le Concepteur de configuration Windows, accédez à **Paramètres d'exécution > CompteOrdinateur > NomOrdinateur**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Dans le champ **CompteOrdinateur**, incluez la chaîne suivante dans le nom de l'appareil :% `SERIAL`%. Par exemple : `Surface-%SERIAL%`. La chaîne inclut le numéro de série BIOS de chaque appareil.

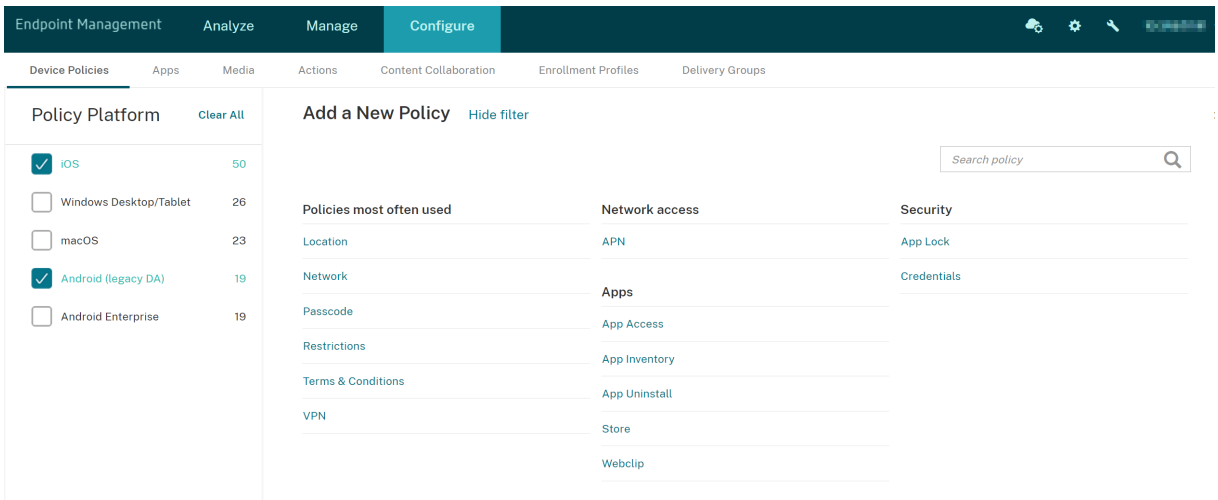
Stratégies d'appareil

March 1, 2024

Vous pouvez configurer la façon dont Citrix Endpoint Management interagit avec vos appareils en créant des stratégies. Bien que la plupart des stratégies soient communes à tous les appareils, chaque appareil dispose de stratégies spécifiques à son système d'exploitation. Par conséquent, vous pouvez constater des différences entre les plates-formes et même entre différents fournisseurs d'appareils Android.

Pour afficher les stratégies disponibles par plate-forme :

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Stratégies d'appareil**.
2. Cliquez sur **Ajouter**.
3. Chaque plate-forme apparaît dans une liste du panneau **Stratégie par plate-forme**. Si ce panneau n'est pas ouvert, cliquez sur **Afficher le filtre**.
4. Pour afficher une liste de toutes les stratégies disponibles pour une plate-forme, sélectionnez cette plate-forme. Pour afficher une liste des stratégies disponibles pour plusieurs plates-formes, sélectionnez chacune de ces plates-formes. Une stratégie apparaît dans la liste uniquement si elle s'applique à chaque plate-forme sélectionnée.



Pour obtenir un résumé de chaque stratégie, consultez la section Résumé des stratégies d'appareil dans cet article.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Remarque :**
>
> Si votre environnement est configuré avec des objets de stratégie de groupe (GPO) :
>
> Lorsque vous configurez des stratégies d'appareil Citrix Endpoint Management pour Windows 10 et Windows 11, n'oubliez pas les règles suivantes. Si une stratégie sur un ou plusieurs appareils inscrits entraîne un conflit, la stratégie correspondant au GPO est prioritaire.

Pour voir les stratégies prises en charge par le conteneur Android Enterprise, consultez la section Android Enterprise.

Logiciels requis

- Créer les groupes de mise à disposition que vous voulez utiliser.
- Installer les certificats d'autorité de certification nécessaires.

Ajouter une stratégie d'appareil

Les étapes de base pour créer une stratégie sont les suivantes :

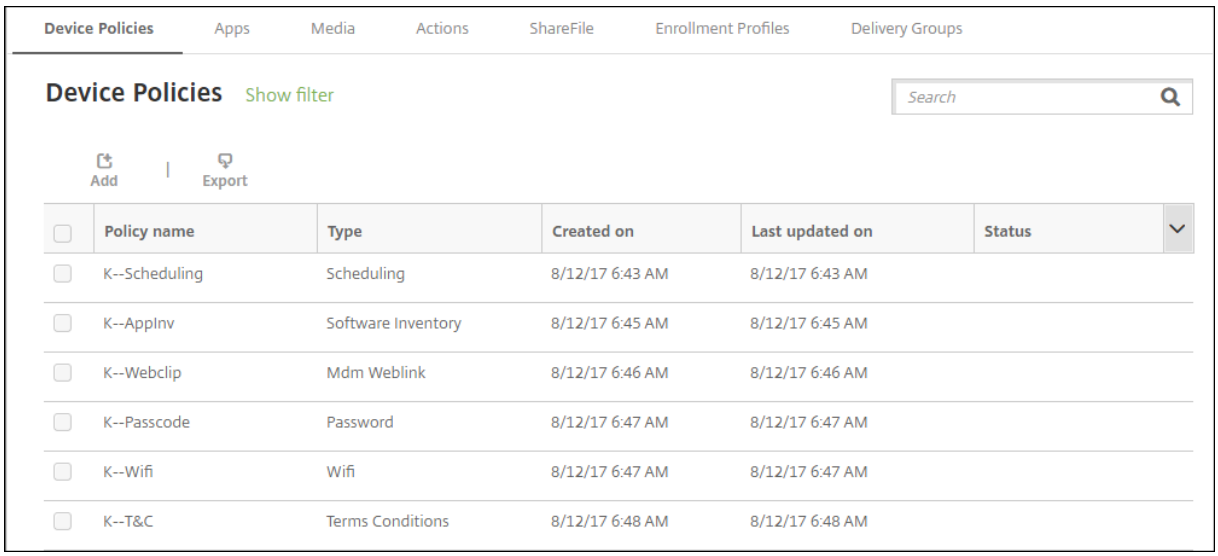
1. Fournissez un nom et une description pour la stratégie.

   > **Important :**
   >
   > N'utilisez pas de barre oblique (/) dans un nom de stratégie. Sinon, une erreur peut se produire lorsque vous modifiez la stratégie ultérieurement.

2. Configurez la stratégie pour une ou plusieurs plates-formes.
3. Créez des règles de déploiement (facultatif).
4. Attribuez la stratégie à des groupes de mise à disposition.
5. Configurez le calendrier de déploiement (facultatif).

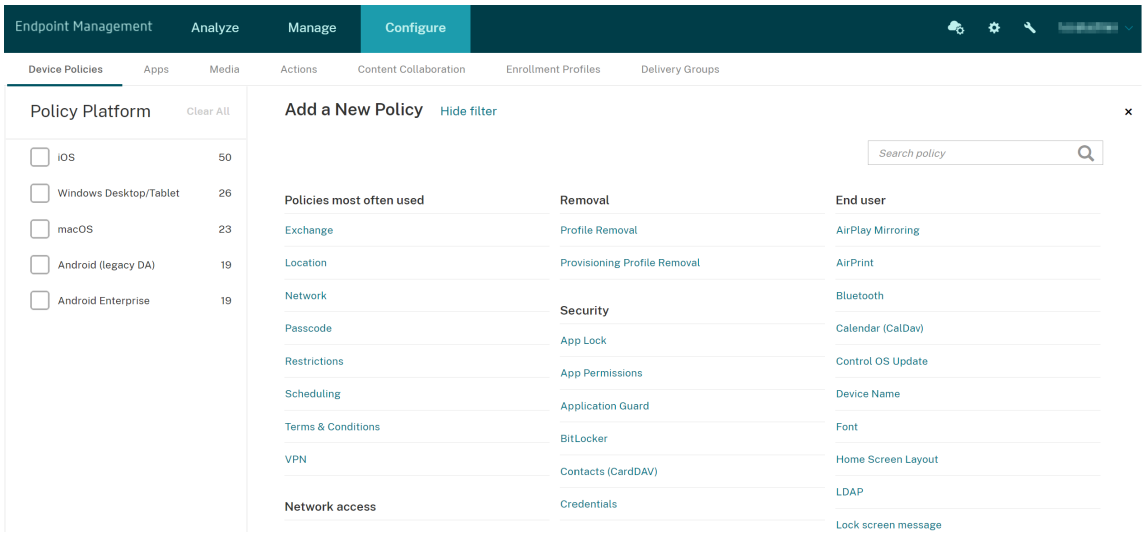
Pour créer et gérer les stratégies, accédez à **Configurer > Stratégies d'appareil**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



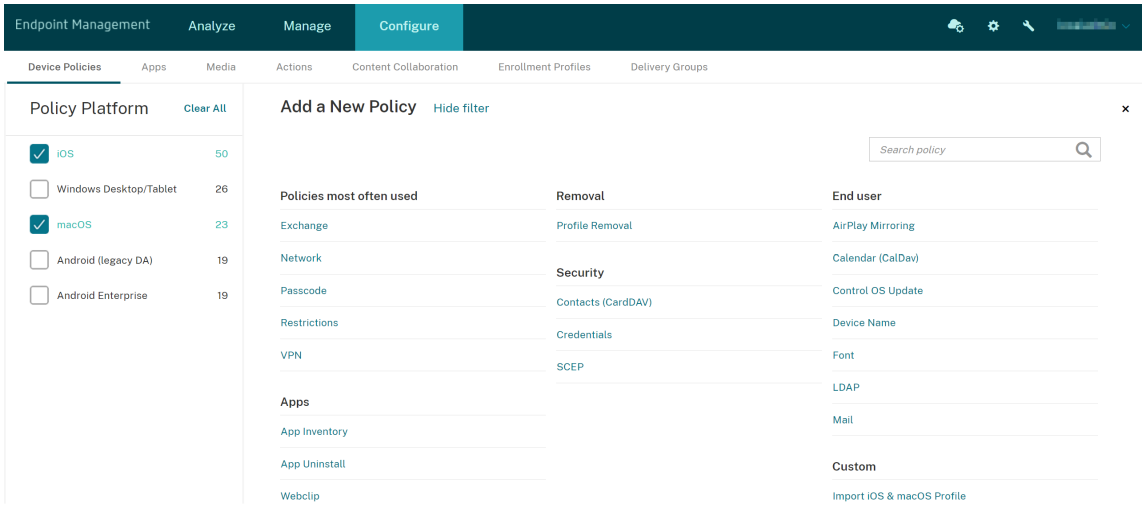
Pour ajouter une stratégie :

1. Sur la page **Stratégies d'appareil**, cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.



2. Cliquez sur une ou plusieurs plates-formes pour afficher une liste des stratégies d'appareil pour les plates-formes sélectionnées. Cliquez sur un nom de stratégie pour continuer avec l'ajout de la stratégie.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Vous pouvez aussi entrer le nom de la stratégie dans le champ de recherche. À mesure que vous tapez, des correspondances potentielles s'affichent. Si votre stratégie figure dans la liste, cliquez dessus. Seule la stratégie sélectionnée reste dans les résultats. Cliquez dessus pour ouvrir la page **Informations de stratégie** pour cette stratégie.

3. Sélectionnez les plates-formes que vous souhaitez inclure dans la stratégie. Les pages de configuration pour les plates-formes sélectionnées s'affichent dans l'étape 5.

4. Remplissez la page **Informations de stratégie** puis cliquez sur **Suivant**. La page **Informations de stratégie** collecte des informations, comme le nom de la stratégie, pour vous aider à identifier et à suivre vos stratégies. Cette page est identique pour toutes les stratégies.

5. Renseignez les pages de plates-formes. Les pages de plates-formes s'affichent pour chaque plate-forme que vous avez sélectionnée dans l'étape 3. Ces pages sont différentes pour chaque stratégie. Une stratégie peut varier d'une plate-forme à l'autre. Toutes les stratégies ne s'appliquent pas à toutes les plates-formes.

   Certaines pages incluent des tableaux d'éléments. Pour supprimer un élément existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

   Pour modifier un élément existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit.

Pour configurer les règles de déploiement, les attributions et le calendrier

Pour de plus amples informations sur la configuration des règles de déploiement, consultez la section Déployer des ressources.

1. Sur la page de la plate-forme, développez **Règles de déploiement** et configurez les paramètres suivants. L'onglet **Base** s'affiche par défaut.

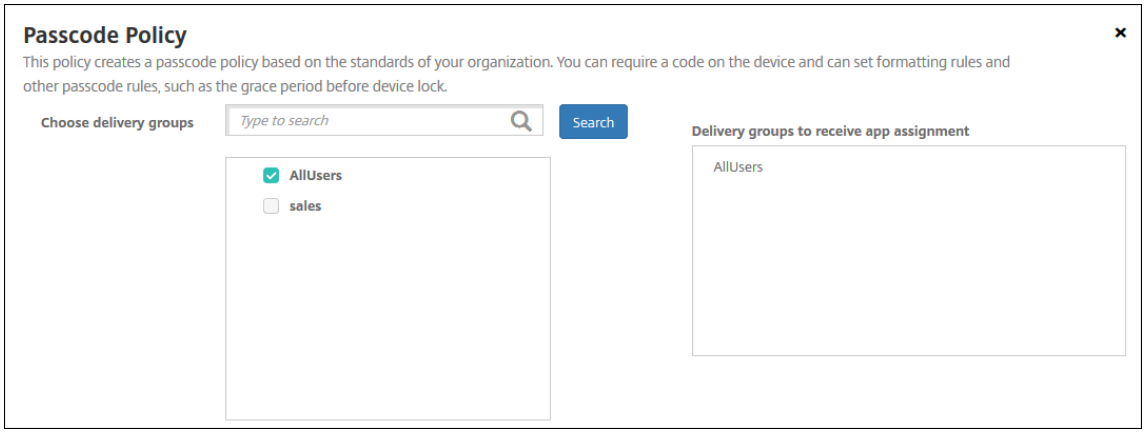
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Dans les listes, cliquez sur les options pour spécifier les conditions de déploiement. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est définie sur **Toutes**.
- Cliquez sur **Nouvelle règle** pour définir les conditions.
- Dans la liste, cliquez sur les conditions, telles que **Propriétaire** et **BYOD**.
- Cliquez sur **Nouvelle règle** de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.

2. Cliquez sur l'onglet **Avancé** pour combiner les règles avec des options booléennes. Les conditions que vous avez choisies sur l'onglet **Base** s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   - Cliquez sur **ET**, **OU** ou **SAUF**.
   - Dans les listes, sélectionnez les conditions que vous souhaitez ajouter à la règle. Cliquez ensuite sur le signe plus (**+**) sur le côté droit pour ajouter la condition à la règle.

     À tout moment, vous pouvez cliquer pour sélectionner une condition, puis cliquer sur **Modifier** ou **Supprimer**.
   - Cliquez sur **Nouvelle règle** pour ajouter une autre condition.
4. Cliquez sur **Suivant** pour passer à la page de plate-forme suivante, ou lorsque toutes les pages de plate-forme sont remplies, à la page **Attributions**.
5. Sur la page **Attribution**, sélectionnez les groupes de mise à disposition auxquels vous voulez appliquer la stratégie. Si vous cliquez sur un groupe de mise à disposition, le groupe apparaît dans la zone **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

   La zone **Groupes de mise à disposition qui vont recevoir l'attribution d'applications** n'apparaît pas tant que vous n'avez pas sélectionné un groupe de mise à disposition.



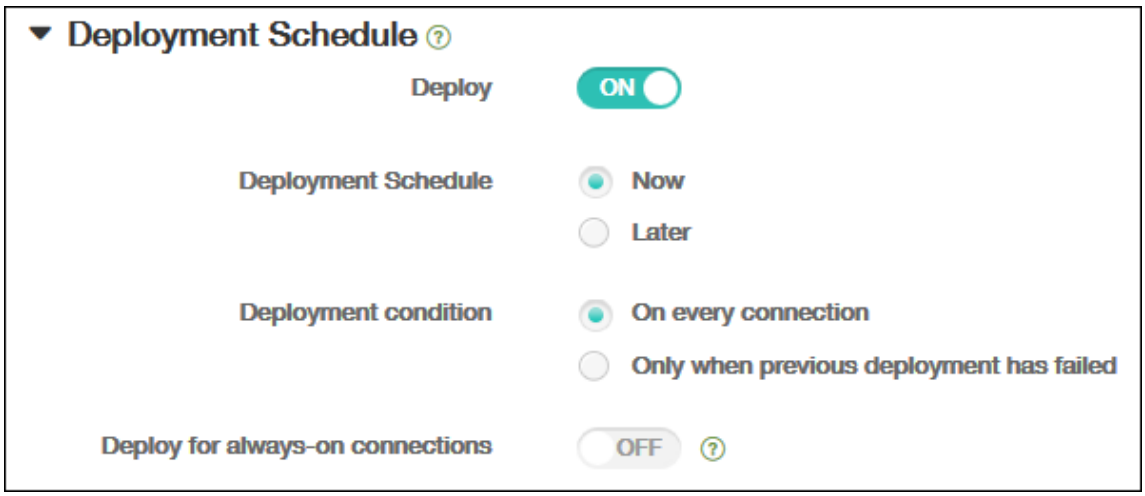
6. Sur la page **Attributions**, développez **Calendrier de déploiement** et configurez les paramètres suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- En regard de **Déployer**, cliquez sur **Activé** pour planifier le déploiement ou cliquez sur **Désactivé** pour empêcher le déploiement. L'option par défaut est définie sur **Activé**.
- À côté du **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est définie sur **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est définie sur **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **Activé** ou **Désactivé**. L'option par défaut est définie sur **Désactivé**.

> **Remarque :**
>
> Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.
>
> L'option de connexion permanente :
>
> – N'est pas disponible pour les appareils iOS.
> – N'est pas disponible pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec la version 10.18.19 ou ultérieure
> – N'est pas recommandée pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec une version antérieure à la version 10.18.19
>
> Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



7. Cliquez sur **Enregistrer**.

   La stratégie apparaît dans le tableau **Stratégies d'appareil**.

Supprimer une stratégie d'un appareil

Les étapes pour supprimer une stratégie d'un appareil dépendent de la plate-forme.

- Android

  Pour supprimer une stratégie d'un appareil Android, utilisez la stratégie de désinstallation de Citrix Endpoint Management. Pour plus d'informations, consultez la section Stratégie Désinstallation de Citrix Endpoint Management.

- iOS et macOS

  Pour supprimer une stratégie d'un appareil iOS ou macOS, utilisez la stratégie de suppression de profil. Sur les appareils iOS et macOS, toutes les stratégies font partie du profil MDM. Vous pouvez ainsi créer une stratégie de suppression de profil uniquement pour la stratégie que vous souhaitez supprimer. Le reste des stratégies et le profil restent sur l'appareil. Pour plus d'informations, consultez la section Stratégie de suppression de profil.

- Windows 10 et Windows 11

  Vous ne pouvez pas supprimer directement une stratégie d'un appareil Windows Desktop et Tablet. Toutefois, vous pouvez utiliser l'une des méthodes suivantes :

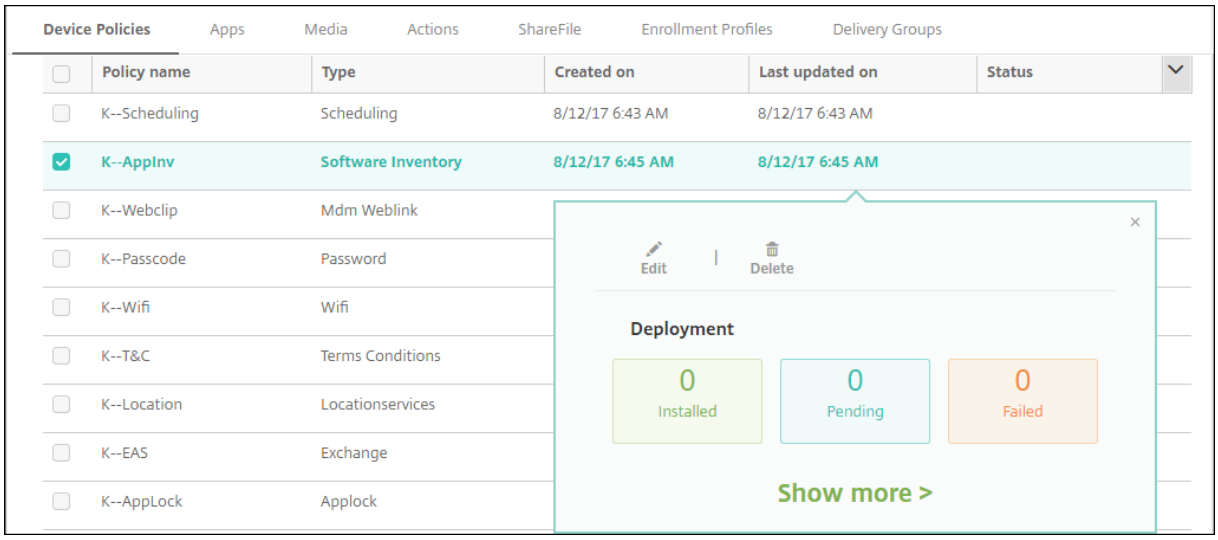
  - Désinscrivez l'appareil, puis installez un nouvel ensemble de stratégies sur l'appareil. Les utilisateurs se ré-inscrivent ensuite pour continuer.
  - Effectuez une action de sécurité pour effacer les données d'entreprise d'un appareil spécifique. Cette action supprime toutes les applications et les données d'entreprise de l'appareil. Vous supprimez ensuite la stratégie d'un groupe de mise à disposition contenant

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

uniquement cet appareil, puis vous transmettez ce groupe de mise à disposition vers l'appareil. Les utilisateurs se ré-inscrivent ensuite pour continuer.

Modifier une stratégie d'appareil

Pour modifier une stratégie, vous pouvez sélectionner la case à cocher en regard d'une stratégie. Le menu des options apparaît au-dessus de la liste de stratégies. Vous pouvez également cliquer sur une stratégie dans la liste pour afficher d'autres contrôles.



Pour afficher les détails d'une stratégie, cliquez sur **Afficher plus**.

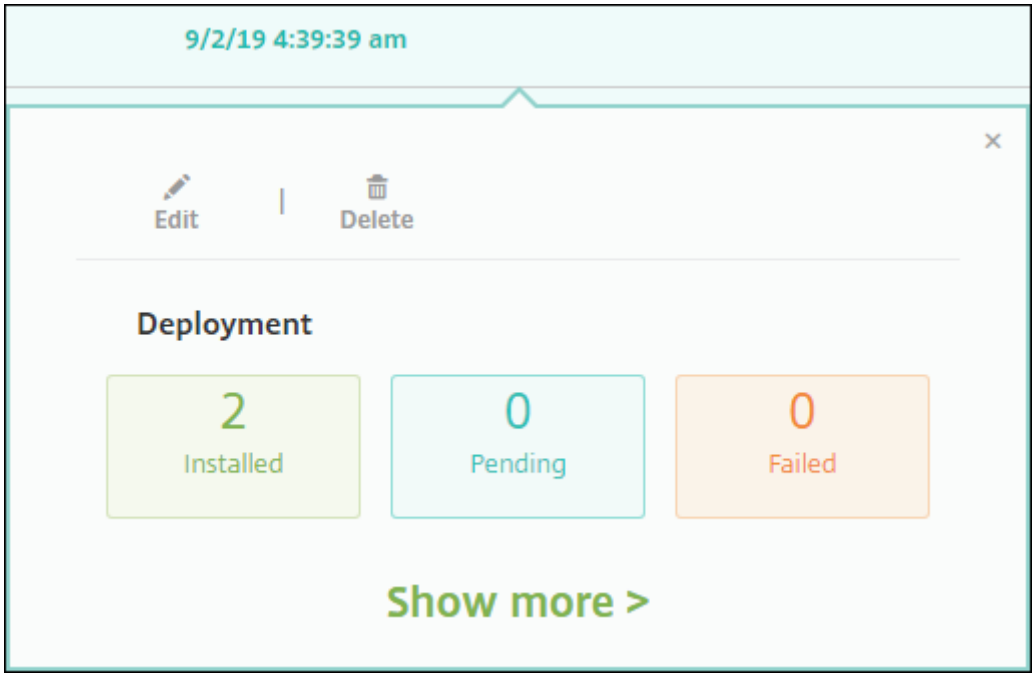
Pour modifier tous les paramètres d'une stratégie, cliquez sur **Modifier**.

Si vous cliquez sur **Supprimer**, une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer** pour supprimer la stratégie.

Vérifier l'état du déploiement de la stratégie

Cliquez sur une ligne de stratégie sur la page **Configurer > Stratégies d'appareil** pour vérifier son état de déploiement.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

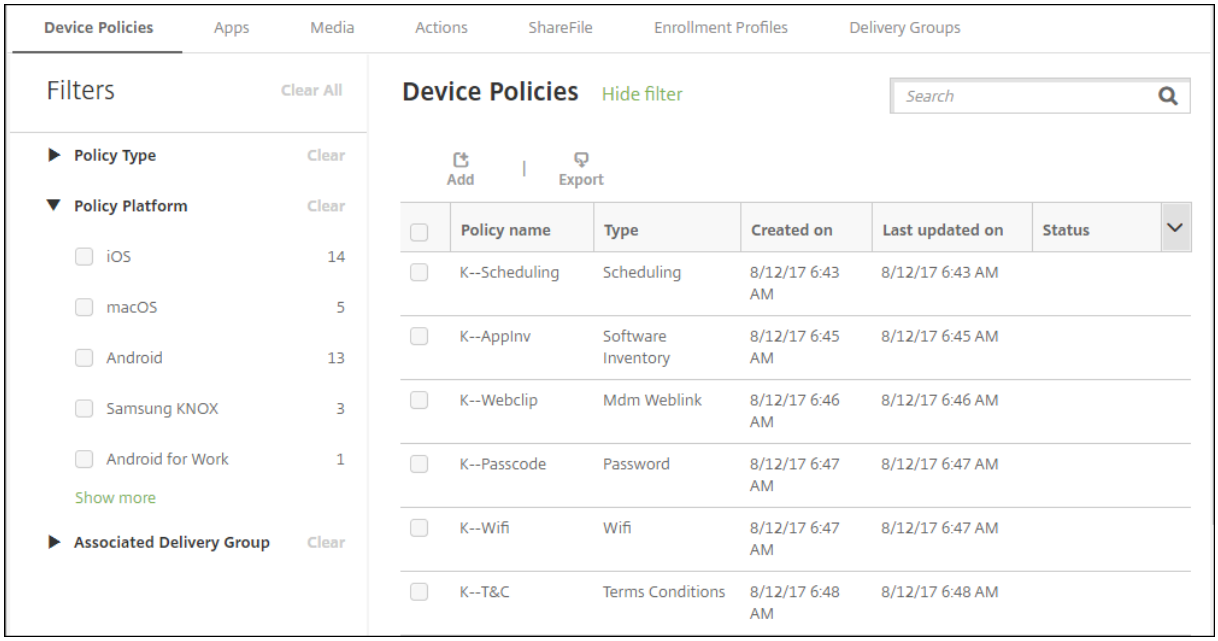


Lorsqu'un déploiement de stratégie est en attente, les utilisateurs peuvent actualiser la stratégie à partir de Citrix Secure Hub en touchant **Préférences > Informations sur l'appareil > Actualiser la stratégie**.

Filtrer la liste des stratégies d'appareil ajoutées

Vous pouvez filtrer la liste des stratégies ajoutées par types de stratégie, plates-formes et groupes de mise à disposition associés. Sur la page **Configurer > Stratégies d'appareil**, cliquez sur **Afficher le filtre**. Dans la liste, sélectionnez les cases à cocher pour les éléments que vous souhaitez voir.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Cliquez sur **ENREGISTRER CETTE VUE** pour enregistrer un filtre. Le nom du filtre s'affiche alors dans un bouton sous le bouton **ENREGISTRER CETTE VUE**.

Résumé des stratégies d'appareil

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Mise en miroir AirPlay	Ajoute des appareils AirPlay spécifiques (tels qu'un téléviseur Apple ou un autre ordinateur Mac) aux appareils iOS. Vous pouvez également ajouter des appareils à une liste d'autorisation pour les appareils supervisés. Cette option limite les utilisateurs uniquement aux appareils AirPlay de la liste d'autorisation.
AirPrint	Ajoute les imprimantes AirPrint à la liste d'imprimantes AirPrint sur les appareils iOS. Cette stratégie facilite la prise en charge d'environnements dans lesquels les imprimantes et les appareils figurent sur des sous-réseaux différents.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
APN	Détermine les paramètres utilisés pour connecter vos appareils au service GPRS d'un opérateur de téléphonie spécifique. Ce paramètre est déjà défini dans la plupart des téléphones récents. Utilisez cette stratégie si votre entreprise n'utilise pas d'APN consommateur pour se connecter à Internet à partir d'un appareil mobile.
Accès aux applications	Permet de définir une liste des applications obligatoires, facultatives ou interdites sur l'appareil. Vous pouvez ensuite créer une action automatisée dont la tâche consiste à vérifier la conformité de l'appareil par rapport à cette liste d'applications.
Attributs d'application	Spécifie des attributs, tels qu'un Bundle ID d'application gérée, ou un identifiant VPN par application pour les appareils iOS.
Configuration d'applications	Configure à distance les différents paramètres et comportements des applications qui prennent en charge la configuration gérée. Pour ce faire, vous déployez un fichier de configuration XML (appelé une liste des propriétés, ou `plist`) sur des appareils iOS. Ou vous déployez des paires clé/valeur vers des ordinateurs ou tablettes Windows 10.
Inventaire des applications	Établit un inventaire des applications sur les appareils gérés. Citrix Endpoint Management compare ensuite l'inventaire avec les stratégies d'accès aux applications déployées sur ces appareils. Vous pouvez ainsi détecter les applications figurant sur une liste d'autorisation ou de blocage et prendre les mesures qui s'imposent.
Mode kiosque	Définit une liste des applications que les utilisateurs peuvent ou ne peuvent pas exécuter sur les appareils iOS ou certains appareils Android. Peut transformer un iPad en kiosque.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Autorisations d'application	Permet de configurer la façon dont les demandes des applications Android Enterprise dans le cadre de profils de travail gèrent les autorisations qualifiées comme étant « dangereuses » par Google.
Désinstallation des applications	Supprime des applications des appareils utilisateur.
Restrictions de désinstallation d'applications	Spécifie les applications que les utilisateurs peuvent ou ne peuvent pas désinstaller.
Application Guard	Pour le navigateur Microsoft Edge uniquement, cette stratégie spécifie les paramètres de Windows Defender Application Guard. Les paramètres incluent la possibilité de bloquer le contenu externe sur les sites d'entreprise.
Notifications d'applications	Permet de contrôler la manière dont les utilisateurs iOS recevront les notifications depuis certaines applications.
Mettre à jour automatiquement les applications gérées	Contrôle la façon dont les applications gérées installées sont mises à jour sur les appareils Android Enterprise.
BitLocker	Configure les paramètres disponibles dans l'interface BitLocker sur les appareils Windows 10 et Windows 11.
Bluetooth	Active ou désactive le Bluetooth sur les appareils iOS.
Navigateur	Définit si les appareils peuvent utiliser le navigateur ou à quelles fonctions du navigateur les appareils ont accès.
Calendrier (CalDav)	Ajoute un compte de calendrier (CalDAV) aux appareils iOS ou macOS. Le compte CalDAV permet aux utilisateurs de synchroniser les données de planification avec tout serveur qui prend en charge CalDAV.
Cellulaire	Configure les paramètres du réseau cellulaire.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Planification de connexion	Requise pour que les appareils Android puissent se connecter à Citrix Endpoint Management pour pouvoir utiliser la gestion MDM, distribuer des applications et déployer des stratégies. Si vous n'envoyez pas cette stratégie à des appareils et que vous n'avez pas activé Google FCM, un appareil ne peut pas se reconnecter au serveur.
Contacts (CardDAV)	Ajoute un contact iOS (CardDAV) aux appareils iOS ou macOS. Le compte CardDAV permet aux utilisateurs de synchroniser les données de contact avec tout serveur qui prend en charge CardDAV.
Informations d'identification	Permet l'authentification intégrée avec votre configuration PKI dans Citrix Endpoint Management. Par exemple, avec une entité PKI, un keystore, un fournisseur d'identités ou un certificat de serveur.
XML personnalisé	Personnalise les fonctionnalités telles que le provisioning d'appareils, l'activation de fonctionnalités d'appareil, la configuration d'appareil et la gestion des erreurs.
Defender	Configure les paramètres de Windows Defender pour Windows 10 et Windows 11 pour bureau et tablette.
Device Guard	Active des fonctionnalités de sécurité telles que le démarrage sécurisé, le verrouillage UEFI et la virtualisation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Attestation de l'intégrité des appareils	Requiert que les appareils Windows 10 et Windows 11 signalent l'état de leur intégrité. Pour ce faire, ils envoient des informations d'exécution et des données spécifiques au service d'attestation de l'intégrité (HAS) pour analyse. Le service HAS crée et renvoie un certificat d'attestation d'intégrité que l'appareil envoie ensuite à Citrix Endpoint Management. Lorsque Citrix Endpoint Management reçoit le certificat d'attestation d'intégrité, en fonction du contenu de ce certificat, des actions automatiques que vous avez configurées peuvent être déployées.
Nom de l'appareil	Définit les noms sur des appareils iOS et macOS, ce qui vous permet d'identifier les appareils. Vous pouvez utiliser des macros et du texte, ou une combinaison des deux pour définir le nom de l'appareil.
Configuration de l'éducation	Configure les appareils des enseignants et des élèves pour une utilisation avec Apple Éducation. Si les instructeurs utilisent l'application En classe, la stratégie Configuration de l'éducation est requise. Prise en charge pour les appareils iOS (iPadOS).
Options de Citrix Endpoint Management	Configure le comportement de Citrix Secure Hub lors de la connexion à Citrix Endpoint Management à partir d'appareils Android.
Désinstallation de Citrix Endpoint Management	Désinstalle Citrix Endpoint Management des appareils Android. Lorsqu'elle est déployée, cette stratégie supprime Citrix Endpoint Management sur tous les appareils du déploiement.
Exchange	Active la messagerie ActiveSync pour le client de messagerie natif sur l'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Fichiers	Ajoute des fichiers de script à Citrix Endpoint Management qui exécutent certaines fonctions pour les utilisateurs. Ou vous pouvez ajouter des fichiers de documents auxquels vous voulez que les utilisateurs Android aient accès sur leurs appareils. Lorsque vous ajoutez le fichier, vous pouvez également spécifier le répertoire dans lequel vous souhaitez que le fichier soit stocké sur l'appareil.
FileVault	Cette stratégie vous permet d'activer le chiffrement FileVault sur les appareils macOS inscrits. Vous pouvez également contrôler combien de fois un utilisateur peut ignorer l'installation de FileVault lors de la connexion. Disponible pour macOS 10.7 ou version ultérieure.
Pare-feu	Configure les paramètres du pare-feu. Vous pouvez entrer les adresses IP, les ports et les noms d'hôte que vous souhaitez autoriser ou empêcher sur les appareils. Vous pouvez également configurer les paramètres de redirection de proxy et de proxy.
Police	Ajoute des polices aux appareils iOS et macOS. Les polices doivent être de type TrueType (.TTF) ou OpenType (.OFT). Citrix Endpoint Management ne prend pas en charge les collections de polices (.TTC, .OTC).
Disposition de l'écran d'accueil	Définit la disposition des applications et des dossiers pour l'écran d'accueil d'iOS sur les appareils iOS supervisés.
Importer le profil iOS et macOS	Importe les fichiers XML de configuration d'appareil pour iOS et macOS dans Citrix Endpoint Management. Le fichier contient des stratégies de sécurité et des restrictions que vous préparez avec Apple Configurator.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Gestion du keyguard	Contrôle les fonctionnalités disponibles pour les utilisateurs avant qu'ils déverrouillent le keyguard de l'appareil et le keyguard de challenge professionnel. Vous pouvez également contrôler les fonctions de keyguard d'appareil pour les appareils entièrement gérés et dédiés. Par exemple, vous pouvez désactiver les fonctions d'écran de verrouillage telles que le déverrouillage par empreinte digitale, les agents de confiance et les notifications.
Configuration du Launcher	Spécifie les paramètres de Citrix Launcher sur les appareils Android, tels que les applications autorisées et une image de logo personnalisée pour l'icône Launcher.
LDAP	Fournit des informations sur un serveur LDAP à utiliser pour les appareils iOS, y compris toute information nécessaire sur le compte telle que le nom d'hôte du serveur LDAP. La stratégie fournit également un ensemble de stratégies de recherche LDAP à utiliser lors de l'interrogation du serveur LDAP.
Emplacement	Permet de géo-localiser les appareils sur une carte, en supposant que le GPS est activé pour Citrix Secure Hub sur l'appareil. Après le déploiement de cette stratégie sur l'appareil, vous pouvez envoyer une commande de localisation à partir de Citrix Endpoint Management. L'appareil répond avec ses coordonnées d'emplacement. Citrix Endpoint Management prend également en charge les stratégies de géofencing et de suivi.
Message sur l'écran de verrouillage	Définit les messages à afficher sur les appareils suivants lorsqu'ils sont perdus : la fenêtre de connexion des iPad partagés et l'écran de verrouillage des appareils iOS supervisés.
E-mail	Configure un compte de messagerie sur les appareils iOS ou macOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Configurations gérées	Contrôle de nombreuses options de configuration et de restriction d'applications pour les appareils Android Entreprise.
Domaines gérés	Définit des domaines gérés qui s'appliquent à la messagerie et au navigateur Safari. Les domaines gérés vous aident à protéger les données d'entreprise en contrôlant les applications qui peuvent ouvrir des documents téléchargés depuis des domaines à l'aide de Safari. Pour les appareils supervisés iOS, vous pouvez spécifier des adresses URL ou des sous-domaines pour contrôler la manière dont les utilisateurs peuvent ouvrir des documents, des pièces jointes et des téléchargements à partir du navigateur.
Nombre maximal d'utilisateurs résidents	Spécifie le nombre maximal d'utilisateurs pour un iPad partagé. Prise en charge pour les appareils iOS et iPados.
Options MDM	Gère les fonctions Localiser mon téléphone/Verrouillage d'activation iPad sur les appareils supervisés iOS.
Réseau	Permet aux administrateurs de déployer les détails du routeur Wi-Fi vers des appareils gérés. Les détails du routeur comprennent le SSID, les données d'authentification et les données de configuration.
Utilisation du réseau	Définit des règles d'utilisation du réseau pour spécifier la manière dont les applications gérées utilisent les réseaux, tels que les réseaux de données cellulaires, sur les appareils iOS. Les règles s'appliquent uniquement aux applications gérées. Les applications gérées sont des applications que vous déployez sur les appareils des utilisateurs via Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Bureau	Déployez des applications Microsoft Office sur tous les appareils exécutant Windows 10 (version 1709 ou ultérieure) ou Windows 11.
Info organisation	Spécifie les informations d'organisation pour les messages d'alerte que Citrix Endpoint Management déploie vers les appareils iOS.
Mise à jour d'OS	Déploie les dernières mises à jour du système d'exploitation sur les appareils pris en charge et supervisés.
Code secret	Définit un code PIN ou un mot de passe sur un appareil géré. Vous pouvez définir la complexité et les délais d'expiration du code secret sur l'appareil.
Période de grâce de verrouillage par code secret	Spécifie le nombre de minutes pendant lesquelles un écran d'iPad partagé reste verrouillé avant que l'utilisateur ne doive entrer un code d'accès pour déverrouiller l'écran. Prise en charge pour les appareils iOS et iPados.
Partage de connexion	Permet aux utilisateurs de se connecter à Internet lorsqu'ils ne sont pas à portée d'un réseau Wi-Fi. Les utilisateurs se connectent via la connexion de données cellulaires de leur appareil iOS, à l'aide de la fonctionnalité de point d'accès personnel.
Suppression de profils	Supprime le profil d'application des appareils macOS.
Profil de provisioning	Spécifie un profil de provisioning de distribution d'entreprise à envoyer aux appareils. Lorsque vous développez et codez une application d'entreprise iOS, vous incluez généralement un profil de provisioning. Apple requiert que le profil de l'application s'exécute sur un appareil iOS. Si un profil de provisioning est manquant, ou s'il a expiré, l'application se bloque lorsque l'utilisateur tape pour l'ouvrir.
Suppression du profil de provisioning	Supprime les profils de provisioning iOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Proxy	Spécifie les paramètres de proxy HTTP globaux pour les appareils exécutant iOS. Vous ne pouvez déployer qu'une stratégie de proxy HTTP globale par appareil.
Restrictions	Offre des centaines d'options pour verrouiller et contrôler les fonctionnalités sur les appareils gérés. Exemples d'options de restriction : désactiver l'appareil photo ou le micro, appliquer des règles d'itinérance et imposer l'accès à des services tiers, tels que des magasins d'applications.
Itinérance	Active ou non les services de voix et de données en itinérance sur des appareils iOS. Lorsque l'itinérance de la voix est désactivée, l'itinérance des données est automatiquement désactivée.
Clé de licence MDM Samsung	Spécifie la clé Samsung Enterprise License Management (ELM) intégrée que vous devez déployer sur un appareil. Citrix Endpoint Management prend également en charge le service E-FOTA (Firmware Over-The-Air) Samsung Enterprise.
SCEP	Configure les appareils iOS et macOS afin de récupérer un certificat à partir d'un serveur SCEP externe. Vous pouvez également fournir un certificat à l'appareil à l'aide du protocole SCEP à partir d'une PKI connectée à Citrix Endpoint Management. Pour ce faire, créez une entité PKI et un fournisseur PKI en mode distribué.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Compte SSO	Crée des comptes SSO pour permettre aux utilisateurs de s'authentifier une seule fois pour accéder à Citrix Endpoint Management et à vos ressources d'entreprise internes. Les utilisateurs n'ont pas à stocker d'informations d'identification sur l'appareil. Citrix Endpoint Management utilise les informations d'identification de l'utilisateur d'entreprise du compte SSO pour toutes les applications, y compris les applications provenant de l'App Store. Cette stratégie est compatible avec l'authentification Kerberos. Disponible sur iOS.
Chiffrement du stockage	Permet de crypter le stockage interne et externe. Pour certains appareils, cette stratégie empêche les utilisateurs d'utiliser une carte de stockage sur leurs appareils.
Magasin	Indique si un clip Web du magasin d'applications s'affiche sur l'écran d'accueil des appareils utilisateur.
Abonnements calendriers	Ajoute un abonnement calendrier à la liste des calendriers sur les appareils iOS. Vous devez être abonné à un calendrier avant de pouvoir l'ajouter à la liste des abonnements calendriers sur les appareils des utilisateurs.
Termes et conditions	Requiert que les utilisateurs acceptent les stratégies spécifiques de votre entreprise relatives aux connexions au réseau d'entreprise. Lorsque les utilisateurs inscrivent leurs appareils auprès de Citrix Endpoint Management, ils doivent accepter les termes et conditions pour inscrire leurs appareils. Le refus des termes et conditions annule le processus d'inscription.
Tunnel	Définit les paramètres proxy entre le composant client de toute application d'appareil mobile et le composant de serveur d'applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
VPN	Fournit un accès aux systèmes principaux qui utilisent une technologie de passerelle VPN d'ancienne génération. Cette stratégie fournit des détails de connexion à une passerelle VPN que vous pouvez déployer sur les appareils. Citrix Endpoint Management prend en charge plusieurs fournisseurs VPN, y compris Cisco AnyConnect, Juniper et Citrix VPN. Si la passerelle VPN prend en charge cette option, vous pouvez associer cette stratégie à une autorité de certification et activer le VPN à la demande.
Fond d'écran	Ajoute un fichier .png ou .jpg en tant que fond d'écran sur l'écran d'accueil, l'écran de verrouillage ou les deux. Pour utiliser un fond d'écran différent sur iPad et iPhone, créez différentes stratégies de fond d'écran et les déployer vers les utilisateurs appropriés.
Clips Web	Place des raccourcis ou clips Web sur des sites Web de manière à ce qu'ils apparaissent à côté des applications sur les appareils des utilisateurs. Vous pouvez spécifier vos propres icônes pour représenter les clips Web sur des appareils iOS, macOS X et Android. Windows Tablet requiert uniquement un libellé et une adresse URL.
Filtre de contenu Web	Filtre le contenu web sur les appareils iOS. Citrix Endpoint Management utilise la fonction de filtrage automatique d'Apple et les sites que vous ajoutez aux listes d'autorisation et de blocage. Disponible uniquement sur les appareils iOS supervisés.
Agent Windows	Activez cette stratégie pour exécuter des scripts PowerShell chargés sur des bureaux et des tablettes Windows.
Configuration de GPO Windows	Configurez des objets de stratégie de groupe (GPO) pour tout appareil Windows pris en charge par Citrix Workspace Environment Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de la stratégie d'appareil	Description de la stratégie d'appareil
Windows Hello Entreprise	Active la fonctionnalité Windows afin que les utilisateurs puissent provisionner Windows Hello Entreprise sur leur appareil. La stratégie permet également de configurer des limitations de code d'accès et d'autres fonctionnalités de sécurité.

Stratégies applicatives par plate-forme

Stratégie	iOS	macOS	Android Enterprise	Android (ancien administrateur de l'appareil)	Windows Desktop/Tablet	Autre
Stratégie de mise en miroir AirPlay	X	X				
Stratégie AirPrint	X					
Stratégie APN	X			X		
Stratégie d'accès aux applications	X			X		
Stratégie d'attributs d'application	X					
Stratégie de configuration d'application	X				X	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie	iOS	macOS	Android Enterprise	Android (ancien administrateur de l'appareil)	Windows Desktop/Tablet	Autre
Stratégie d'inventaire des applications	X	X	X	X	X	
Stratégie de mode kiosque	X			X	X	
Stratégie Autorisations d'application			X			
Stratégie de désinstallation des applications	X	X	X	X		
Stratégie de restriction de désinstallation d'applications						X
Stratégie Application Guard					X	
Stratégie Notifications d'applications	X					

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie	iOS	macOS	Android Enterprise	Android (ancien administrateur de l' appareil)	Windows Desktop/Tablet	Autre
Mettre à jour automatiquement les applications gérées			X			
Stratégie BitLocker					X	
Stratégie Bluetooth	X					
Stratégie de navigateur						X
Stratégie de calendrier (CalDav)	X	X				
Stratégie cellulaire	X					
Stratégie de planification de connexion			X	X		
Stratégie de contacts (CardDAV)	X	X				
Stratégie Copier les applications sur le conteneur Samsung						X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie	iOS	macOS	Android Enterprise	Android (ancien administrateur de l'appareil)	Windows Desktop/Tablet	Autre
Stratégie d'informations d'identification	X	X	X	X	X	
Stratégie XML personnalisée			X		X	
Stratégies d'appareil Defender					X	
Stratégie Device Guard					X	
Stratégie d'attestation de l'intégrité des appareils					X	
Stratégie de nom d'appareil	X	X				
Stratégie Configuration de l'éducation	X					
Stratégie Options Citrix Endpoint Management			X	X		

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie	iOS	macOS	Android Enterprise	Android (ancien administrateur de l'appareil)	Windows Desktop/Tablet	Autre
Stratégie Désinstallation de Citrix Endpoint Management				X		
Stratégie Exchange	X	X	X	X	X	
Stratégie de fichiers			X	X		
Stratégie FileVault		X				
Stratégie de pare-feu		X			X	
Stratégie de police	X	X				
Stratégie Disposition de l'écran d'accueil	X					
Stratégie Importer configuration de l'appareil						X
Stratégie Importer le profil iOS et macOS	X	X				
Stratégie Gestion du keyguard			X			

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie	iOS	macOS	Android Enterprise	Android (ancien administrateur de l'appareil)	Windows Desktop/Tablet	Autre
Stratégie kiosque			X		X	
Stratégie de configuration du Launcher			X	X		
Stratégie LDAP	X	X				
Stratégie d'emplacement	X		X	X		
Stratégie de message sur l'écran de verrouillage	X					
Stratégie de messagerie	X	X				
Stratégie Configurations gérées			X			
Stratégies de domaines gérés	X					
Stratégie Nombre maximal d'utilisateurs résidents	X					
Stratégie d'options MDM	X					

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie	iOS	macOS	Android Enterprise	Android (ancien administrateur de l'appareil)	Windows Desktop/Tablet	Autre
Stratégie de réseau	X		X	X		
Stratégie Utilisation du réseau	X					
Stratégie Office					X	
Stratégie d'informations sur l'organisation	X					
Stratégie de mise à jour d'OS	X	X	X		X	
Stratégie de code secret	X	X	X	X	X	
Stratégie de période de grâce de verrouillage par code secret	X					
Stratégie Personal Hotspot	X					
Stratégie de suppression de profil	X	X				
Stratégie de profil de provisioning	X					

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie	iOS	macOS	Android Enterprise	Android (ancien administrateur de l'appareil)	Windows Desktop/Tablet	Autre
Stratégie de suppression de profil de provisioning	X					
Stratégie de proxy	X					
Stratégie de restrictions	X	X		X	X	
Stratégie d'itinérance	X					
Stratégie de clé de licence MDM Samsung			X			
Stratégie SCEP	X	X				
Stratégies de dictée et Siri	X					
Stratégie de compte SSO	X					
Stratégie de chiffrement du stockage						
Stratégie de magasin	X			X	X	
Stratégie d'abonnements calendriers	X					

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie	iOS	macOS	Android Enterprise	Android (ancien administrateur de l'appareil)	Windows Desktop/Tablet	Autre
Stratégie termes et conditions	X			X	X	
Stratégie de tunnel				X		
Stratégie VPN	X	X		X	X	
Stratégie de fond d'écran	X					
Stratégie de clip Web	X	X		X	X	
Stratégie de filtre de contenu Web	X					
Stratégie de l'agent Windows					X	
Stratégie de configuration de GPO Windows					X	
Stratégie Windows Hello Entreprise					X	

Stratégie de mise en miroir AirPlay

November 29, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

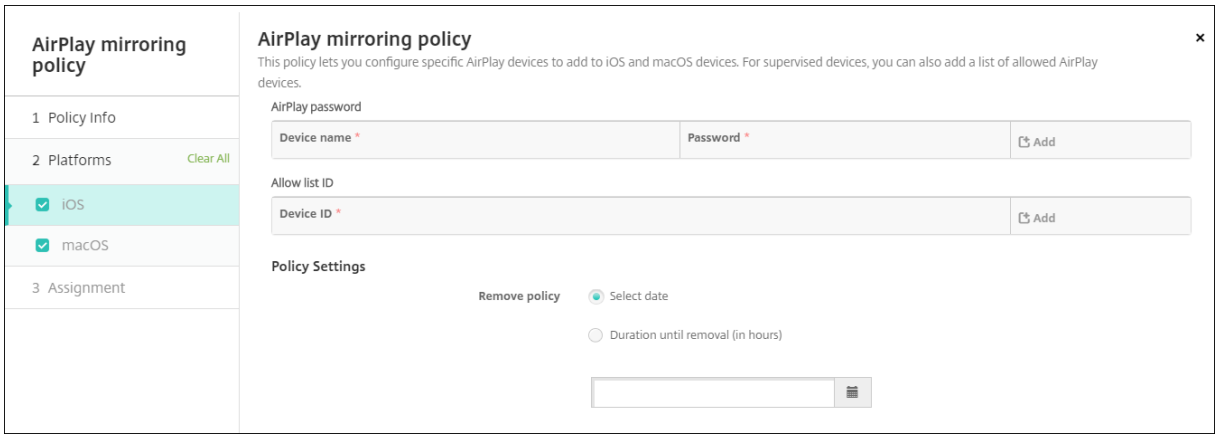
La fonctionnalité AirPlay d'Apple permet aux utilisateurs de streamer sans fil du contenu à partir d'un appareil iOS sur un écran de télé grâce à Apple TV, ou d'afficher tout ce qui figure sur l'écran d'un appareil sur un écran de télévision ou un autre ordinateur Mac.

Vous pouvez ajouter une stratégie d'appareil dans Citrix Endpoint Management afin d'ajouter des appareils AirPlay spécifiques (tels que Apple TV ou un autre ordinateur Mac) aux appareils iOS. Vous avez également la possibilité d'ajouter des appareils à une liste d'autorisation d'appareils supervisés, ce qui limite l'accès des utilisateurs uniquement à ces appareils AirPlay. Pour plus d'informations sur le placement d'un appareil en mode supervisé, voir Déployer des appareils à l'aide d'Apple Configurator 2

> **Remarque :**
>
> Avant de continuer, vérifiez que vous disposez des ID et des mots de passe de tous les appareils que vous voulez ajouter.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



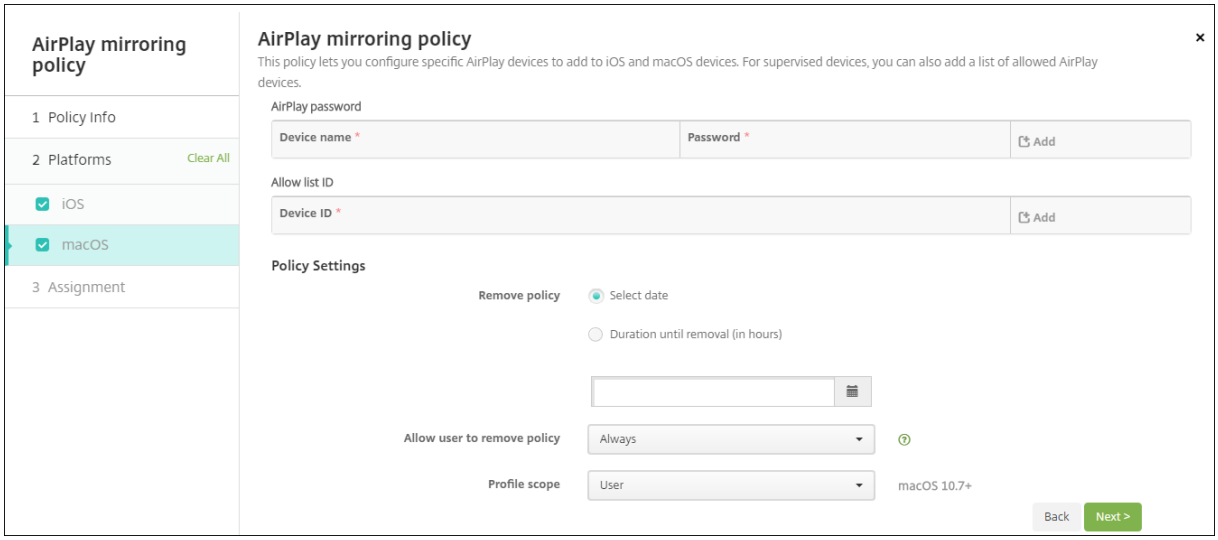
- **Mot de passe AirPlay :** pour chaque appareil que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom de l'appareil :** entrez l'adresse du matériel (adresse MAC) au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
  - **Mot de passe :** entrez un mot de passe pour l'appareil (facultatif).
  - Cliquez sur **Ajouter** pour ajouter l'appareil ou cliquez sur **Annuler** pour annuler l'ajout de l'appareil.
- **ID de liste verte :** cette liste est ignorée pour les appareils non supervisés. Les ID d'appareil de cette liste sont les seuls appareils AirPlay disponibles pour les utilisateurs. Pour chaque appareil AirPlay que vous souhaitez ajouter à la liste, cliquez sur **Ajouter**, puis procédez comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **ID de l'appareil :** entrez l'ID de l'appareil au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
  - Cliquez sur **Ajouter** pour ajouter l'appareil ou cliquez sur **Annuler** pour annuler l'ajout de l'appareil.

- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.

Paramètres macOS



- **Mot de passe AirPlay :** pour chaque appareil que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom de l'appareil :** entrez l'adresse du matériel (adresse MAC) au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
  - **Mot de passe :** entrez un mot de passe pour l'appareil (facultatif).
  - Cliquez sur **Ajouter** pour ajouter l'appareil ou cliquez sur **Annuler** pour annuler l'ajout de l'appareil.

- **ID de liste verte :** cette liste est ignorée pour les appareils non supervisés. Les ID d'appareil de cette liste sont les seuls appareils AirPlay disponibles pour les utilisateurs. Pour chaque appareil AirPlay que vous souhaitez ajouter à la liste, cliquez sur **Ajouter**, puis procédez comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **ID de l'appareil :** entrez l'ID de l'appareil au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
  - Cliquez sur **Ajouter** pour ajouter l'appareil ou cliquez sur **Annuler** pour annuler l'ajout de l'appareil.

- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Stratégie AirPrint

December 9, 2021

La stratégie AirPrint ajoute les imprimantes AirPrint à la liste d'imprimantes AirPrint sur les appareils iOS. Cette stratégie facilite la prise en charge d'environnements dans lesquels les imprimantes et les appareils figurent sur des sous-réseaux différents.

> **Remarque :**
>
> Pour configurer la stratégie AirPrint, vous avez besoin de l'adresse IP et du chemin d'accès à la ressource pour chaque imprimante.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres iOS

- **Destination AirPrint :** pour chaque destination AirPrint que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Adresse IP :** entrez l'adresse IP de l'imprimante AirPrint.
  - **Chemin d'accès à la ressource :** entrez le chemin d'accès à la ressource associé à l'imprimante. Cette valeur correspond au paramètre de l'enregistrement Bonjour `_ipps.tcp`. Par exemple, `printers/Canon_MG5300_series` ou `printers/Xerox_Phaser_7600`.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 ou version ultérieure.

Stratégie Autorisations d'application

March 1, 2024

Pour Android Enterprise dans le cadre de profils de travail : vous pouvez configurer la façon dont les demandes des applications gèrent les autorisations qualifiées comme étant « dangereuses » par Google. Vous déterminez si les utilisateurs doivent autoriser ou refuser une demande d'autorisation à partir d'applications. Cette fonctionnalité est destinée aux appareils exécutant Android 7.0 et versions ultérieures.

Google qualifie de « dangereuses » les autorisations :

- permettant à une application d'accéder aux données ou ressources impliquant des informations utilisateur privées
- ou pouvant potentiellement affecter les données stockées de l'utilisateur ou le fonctionnement d'autres applications. Par exemple, la possibilité de lire les contacts de l'utilisateur est une autorisation dangereuse.

Vous pouvez configurer un état global pour contrôler le comportement de toutes les demandes d'autorisation dangereuses. Cette configuration concerne les applications Android Enterprise incluses

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

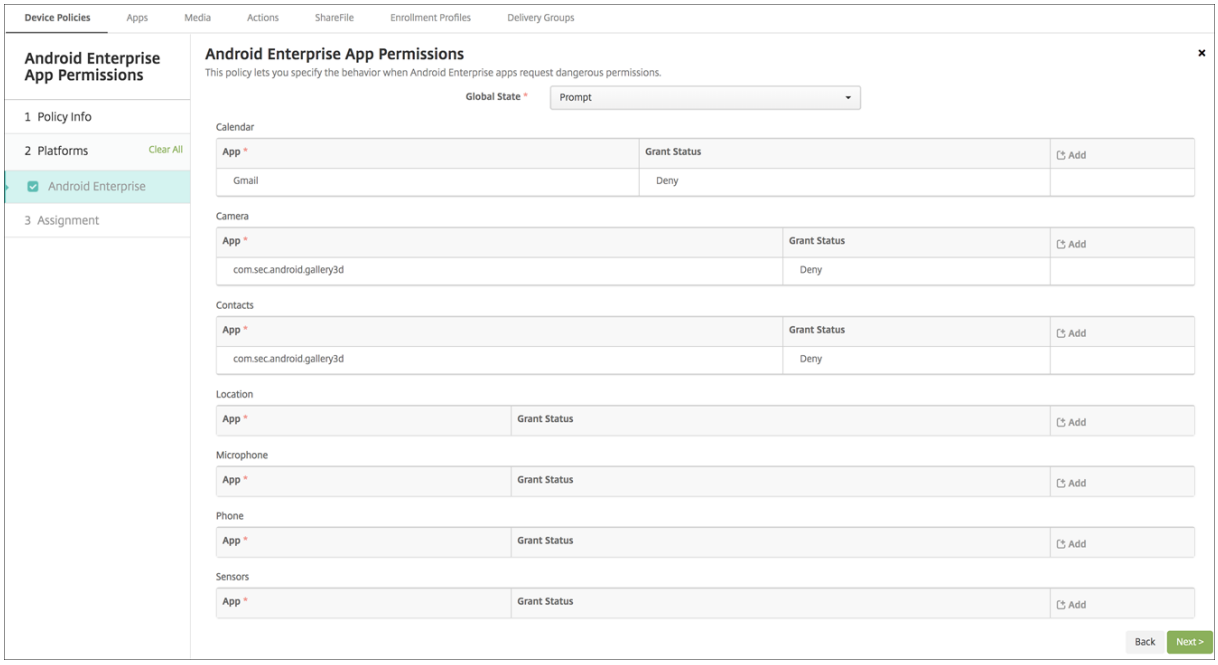
dans les profils de travail. Vous pouvez également contrôler le comportement d'une demande d'autorisation dangereuse pour des groupes d'autorisations individuels, tels que définis par Google, associée à chaque application. Ces paramètres individuels remplacent l'état global.

Pour plus d'informations sur la définition des groupes d'autorisations par Google, consultez le guide des développeurs Android.

Par défaut, les utilisateurs sont invités à autoriser ou refuser les demandes d'autorisation dangereuses.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Android Enterprise



- **État global :** contrôle le comportement de toutes les demandes d'autorisation dangereuses. Dans la liste, cliquez sur **Inviter**, **Accorder** ou **Refuser**.
  - **Inviter :** les utilisateurs sont invités à autoriser ou refuser les demandes d'autorisation dangereuses.
  - **Accorder :** toutes les demandes d'autorisations dangereuses sont accordées. La confirmation de l'utilisateur n'est pas requise.
  - **Refuser :** toutes les demandes d'autorisations dangereuses sont refusées. La confirmation de l'utilisateur n'est pas requise.

  La valeur par défaut est **Inviter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Définissez un comportement individuel pour chaque groupe d'autorisations, pour chaque application. Pour configurer le comportement d'un groupe d'autorisations, cliquez sur **Ajouter**, puis sous **Application**, choisissez une application dans la liste. Si vous configurez des applications système Android Enterprise, cliquez sur **Ajouter** et entrez le nom du package d'application que vous avez activé dans la stratégie Restrictions. Sous l'état de l'accès, choisissez **Inviter**, **Accorder**, ou **Refuser**. L'état d'accès remplace l'état global.
  - **Inviter :** les utilisateurs sont invités à autoriser ou refuser les demandes d'autorisation dangereuses provenant de ce groupe d'autorisations pour cette application.
  - **Accorder :** les demandes d'autorisation dangereuses provenant de ce groupe d'autorisations pour cette application sont accordées. La confirmation de l'utilisateur n'est pas requise.

    > **Remarque :**
    >
    > Pour les appareils inscrits en mode **Propriétaire du profil**, l'autorisation **Accorder** ne s'applique pas à la caméra, à la localisation, au microphone et au capteur si l'appareil fonctionne sous Android 12 ou version ultérieure.

  - **Refuser :** les demandes d'autorisation dangereuses provenant de ce groupe d'autorisations pour cette application sont refusées. La confirmation de l'utilisateur n'est pas requise.

  La valeur par défaut est **Inviter**.
- Cliquez sur **Enregistrer** en regard de l'application et l'état de l'accès
- Pour ajouter d'autres applications pour le groupe d'autorisations, cliquez à nouveau sur **Ajouter** et répétez ces étapes.
- Lorsque vous avez défini l'**état de l'accès** pour tous les groupes d'autorisations souhaités, cliquez sur **Suivant**.

Stratégie APN

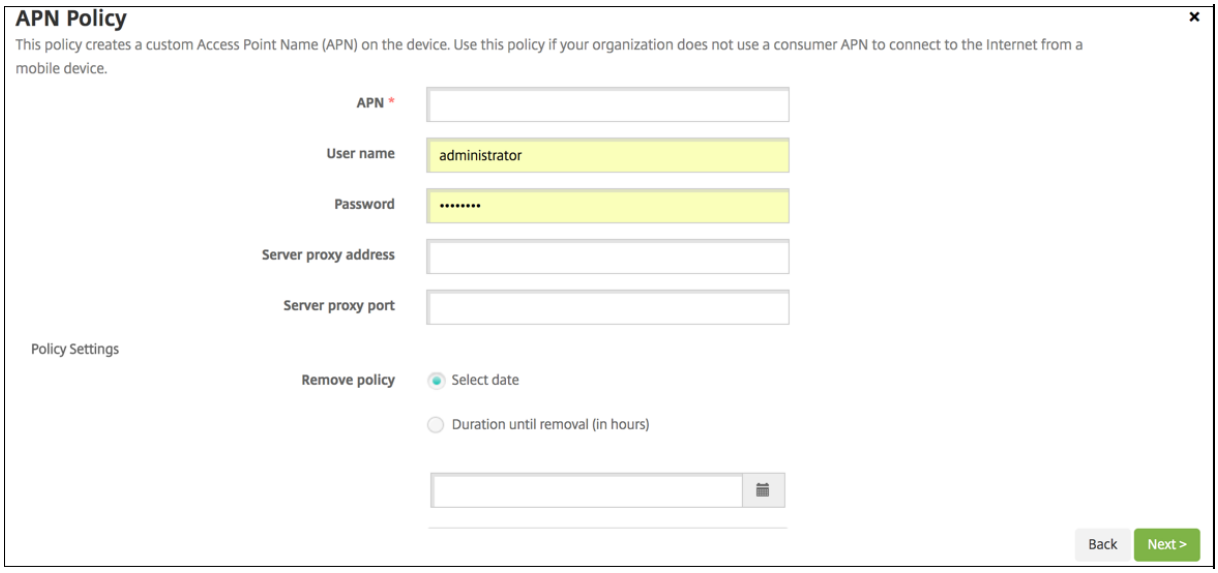
December 9, 2021

Vous pouvez ajouter une stratégie de nom de point d'accès (APN) personnalisée pour iOS et Android. Vous pouvez utiliser cette stratégie si votre entreprise n'utilise pas d'APN consommateur pour se connecter à Internet à partir d'un appareil mobile. Une stratégie APN détermine les paramètres utilisés pour connecter vos appareils au service GPRS d'un opérateur de téléphonie spécifique. Ce paramètre est déjà défini dans la plupart des téléphones les plus récents.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

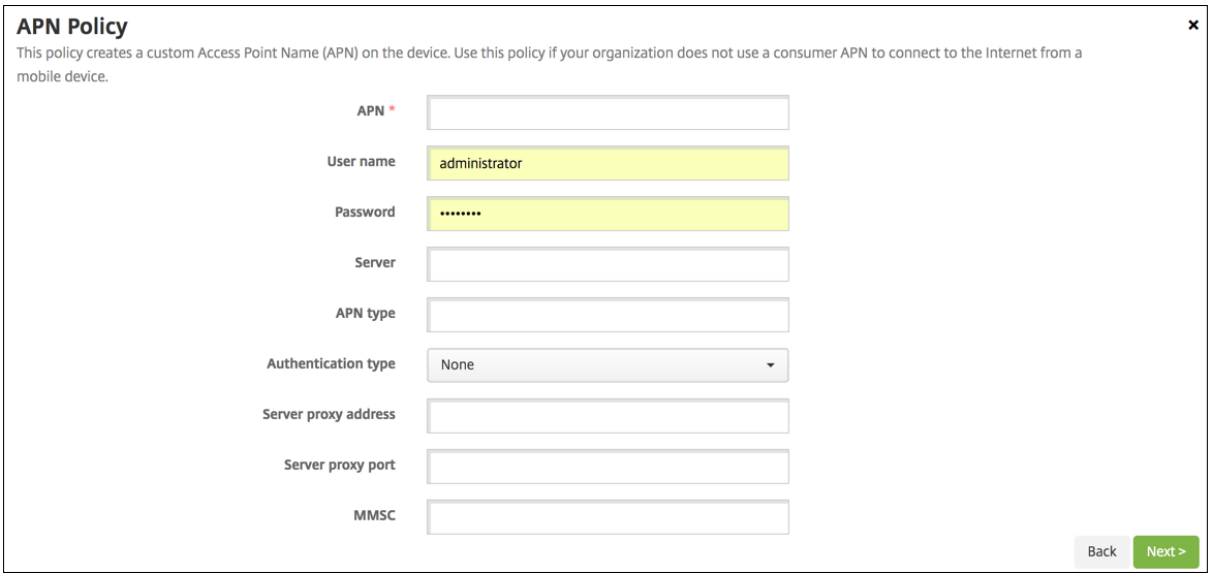


- **APN :** entrez le nom du point d'accès. Le nom doit correspondre à un APN iOS accepté, sinon la stratégie ne fonctionne pas.
- **Nom d'utilisateur :** cette chaîne spécifie le nom d'utilisateur pour ce point d'accès. S'il est manquant, l'appareil invite à saisir la chaîne lors de l'installation du profil.
- **Mot de passe :** mot de passe utilisateur pour ce point d'accès. Afin de masquer le mot de passe, ce dernier est codé. S'il est manquant dans la charge utile, l'appareil vous invite à le saisir lors de l'installation du profil.
- **Adresse du serveur proxy :** adresse IP ou adresse URL du proxy APN.
- **Port du serveur proxy :** numéro de port du proxy APN. Le numéro de port est nécessaire si vous avez entré une adresse de serveur proxy.
- Sous **Paramètres de stratégie**, à côté de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en heures)**.
  - Pour l'option **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Pour l'option **Mot de passe requis**, tapez le mot de passe.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 ou version ultérieure.

Paramètres Android



- **APN :** entrez le nom du point d'accès. Le nom doit correspondre à un APN Android accepté, sinon la stratégie ne fonctionne pas.
- **Nom d'utilisateur :** cette chaîne spécifie le nom d'utilisateur pour ce point d'accès. S'il est manquant, l'appareil invite à saisir la chaîne lors de l'installation du profil.
- **Mot de passe :** mot de passe utilisateur pour ce point d'accès. Afin de masquer le mot de passe, ce dernier est codé. S'il est manquant dans la charge utile, l'appareil vous invite à le saisir lors de l'installation du profil.
- **Serveur :** ce paramètre, antérieur à l'arrivée des smartphones, est généralement vide. Il fait référence à un serveur de passerelle WAP (Wireless Application Protocol) pour les téléphones qui ne peuvent pas accéder ou restituer des sites Web standard.
- **Type d'APN :** ce paramètre doit s'aligner avec l'utilisation prévue par l'opérateur du point d'accès. Il s'agit d'une chaîne délimitée par des virgules des spécificateurs de service APN et doit correspondre aux définitions publiées de l'opérateur sans fil. Exemples :
  - `\*` : tout le trafic transite via ce point d'accès.
  - `mms` : le trafic multimédia transite via ce point d'accès.
  - **`default`** : tout le trafic, y compris le multimédia, transite via ce point d'accès.
  - `supl` : le protocole SUPL est associé au GPS assisté.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - `dun` : l'accès réseau à distance est obsolète et rarement utilisé.
  - `hipri.` : réseau haute priorité.
  - `fota` : FOTA (Firmware over the air) est utilisé pour recevoir les mises à jour du firmware.

- **Type d'authentification :** dans la liste, cliquez sur le type d'authentification à utiliser. Valeur par défaut Aucun.
- **Adresse du serveur proxy :** adresse IP ou adresse URL du proxy HTTP APN de l'opérateur.
- **Port du serveur proxy :** numéro de port du proxy APN. Le port est nécessaire si vous avez entré une adresse de serveur proxy.
- **MMSC :** adresse du serveur MMS fournie par l'opérateur.
- **Adresse du proxy MMS :** adresse du serveur du service de messagerie pour le trafic MMS. MMS a succédé à SMS pour l'envoi de messages plus volumineux avec du contenu multimédia, tels que des images ou des vidéos. Ces serveurs nécessitent des protocoles spécifiques (tels que MM1, …MM11).
- **Port MMS :** port utilisé par le proxy MMS.

Stratégie d'accès aux applications

November 29, 2023

La stratégie d'accès aux applications vous permet de définir une liste d'applications qui doivent être installées, qui peuvent être installées ou qui ne doivent pas être installées. Si les applications d'un appareil contredisent cette stratégie, Citrix Endpoint Management marque l'appareil comme étant non conforme. Vous pouvez ensuite créer une action automatisée pour réagir à la conformité de cet appareil.

> **Important :**
>
> la stratégie d'accès aux applications n'empêche pas un utilisateur d'installer une application interdite ou de désinstaller une application requise.

Vous ne pouvez configurer qu'un type de stratégie d'accès à la fois. Chaque stratégie contient une liste d'applications obligatoires, d'applications suggérées ou d'applications interdites, mais vous ne pouvez pas combiner ces trois types de liste au sein de la même stratégie d'accès. Si vous créez une stratégie pour chaque type de liste, nommez chaque stratégie avec soin afin de pouvoir déterminer à quelle stratégie la liste des applications s'applique.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres iOS et Android (Administration anciens appareils)

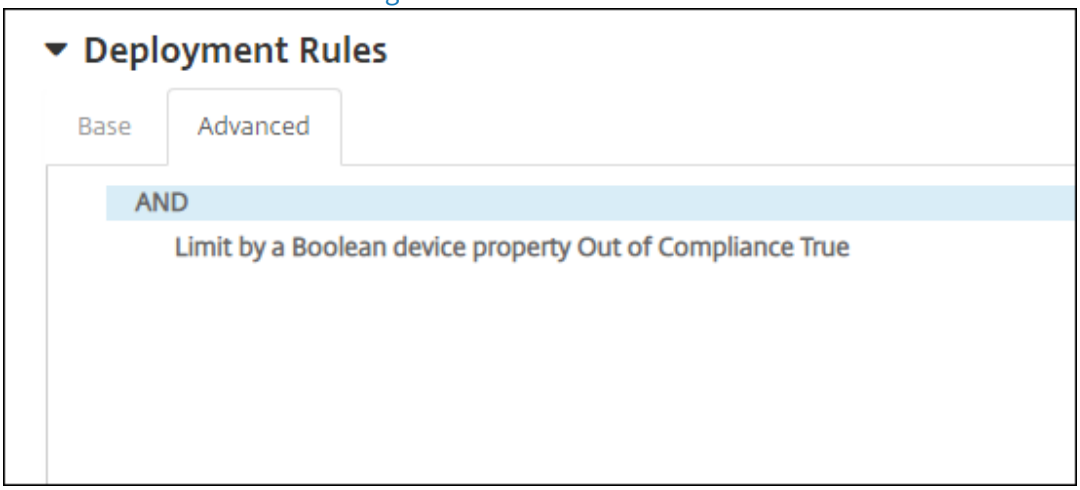
- **Stratégie d'accès** : sélectionnez le type de liste à configurer pour cette stratégie.
  - **Requis** : l'application doit exister sur l'appareil. Si l'application n'existe pas, l'appareil est marqué comme étant non conforme. **Requis** est l'option par défaut.
  - **Liste noire** : l'application ne doit pas exister sur l'appareil. Si l'application existe, l'appareil est marqué comme étant non conforme.
- Pour ajouter une ou plusieurs applications à la liste, procédez comme suit :
  1. Cliquez sur **Ajouter**, puis configurez les paramètres suivants :
     - **Nom app :** entrez un nom pour l'application.
     - **Identifiant app :** entrez un identifiant pour l'application (facultatif).
  2. Cliquez sur **Save**.
  3. Répétez ces étapes pour chaque application à ajouter.

Configurer des actions automatisées en fonction de la conformité à l'accès aux applications

1. Ajoutez une stratégie d'accès aux applications pour exiger ou interdire des applications.
2. Configurez deux actions automatisées selon que les applications en question sont requises ou interdites (sur liste noire) :
   - Obligatoire
     - Marquez un appareil comme étant non conforme si une application requise n'existe pas sur l'appareil.
     - Marquez un appareil comme étant conforme une fois que l'application requise est installée.
   - Liste noire
     - Marquez un appareil comme étant non conforme si une application interdite (sur liste noire) existe sur l'appareil.
     - Marquez un appareil comme étant conforme une fois que cette application interdite n'est plus installée.
       Pour de plus amples informations sur la configuration d'actions automatiques, consultez la section Actions automatisées.
3. Créez une stratégie de restriction avec les paramètres que vous souhaitez mettre en œuvre sur les appareils non conformes.
   a) Dans le cadre de la stratégie de restriction, ajoutez une règle de déploiement avancée en utilisant les options **Limiter par propriété booléenne de l'appareil**, **Non conforme** et

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Vrai. consultez la section Stratégie de restrictions.



4. Créez une stratégie de suppression de profil pour supprimer la stratégie de restriction une fois que l'appareil sera de nouveau conforme.
5. Ajoutez une règle de déploiement avancée en utilisant les options **Limiter par propriété booléenne de l'appareil**, **Non conforme** et **Faux**. Consultez la section Stratégie de suppression de profil.

Stratégie d'attributs d'application

November 29, 2023

La stratégie **Attributs d'application** vous permet de spécifier des attributs pour les applications sur les appareils iOS. En configurant ce type de stratégie, vous pouvez effectuer les opérations suivantes :

- Attribuer des réseaux Per App VPN aux applications.
- Empêcher les utilisateurs de désinstaller des applications stratégiques. S'applique à iOS 14 et versions ultérieures.
- Si la fonctionnalité Domaines associés est activée, spécifiez les domaines associés à ajouter aux applications. S'applique à iOS 13 et versions ultérieures.

  Pour de plus amples informations, consultez la section À propos des domaines associés.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

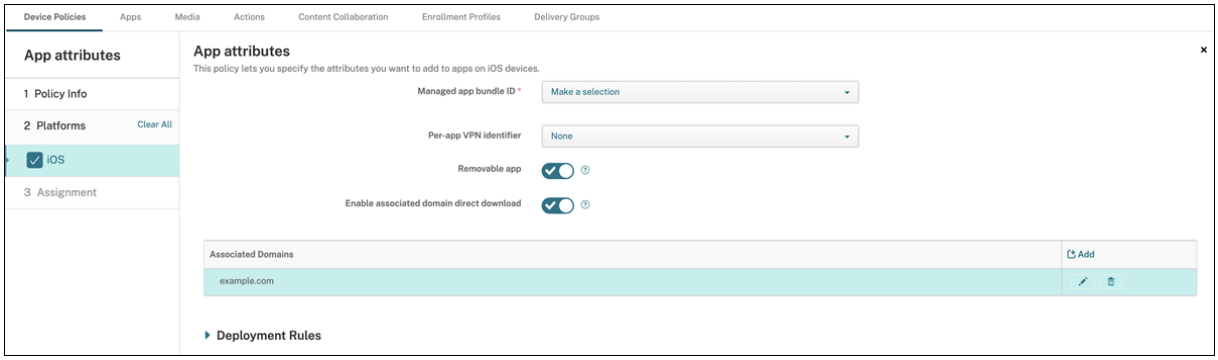
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

À propos des domaines associés

Les domaines associés vous permettent d'établir une association sécurisée entre les domaines et votre application afin que vous puissiez partager des informations d'identification ou fournir des fonctionnalités dans votre application à partir de vos sites Web. Par exemple, lorsque cette fonctionnalité est activée, vous pouvez partager des données et des informations d'identification de connexion entre les applications et les sites Web de votre organisation.

Pour plus d'informations sur la manière d'activer cette fonctionnalité, consultez Supporting Associated Domains sur le site Web d'Apple.

Paramètres iOS



- **Bundle ID d'application gérée :** spécifiez une application de l'une des manières suivantes :
  - Sélectionnez le Bundle ID d'application. Les options ne sont disponibles qu'après l'activation de la stratégie **Inventaire des applications**, qui collecte un inventaire des applications sur les appareils gérés.
  - Sélectionnez **Ajouter**, puis entrez le Bundle ID d'application.
    Pour trouver un Bundle ID d'application, consultez la section Rechercher le Bundle ID d'une application dans l'App Store.
- **Identifiant Per App VPN :** (facultatif) sélectionnez un Per App VPN pour cette application. Les options comprennent les connexions Per App VPN que vous avez configurées sur la page **Stratégies d'appareil > Stratégie VPN**.
  Pour plus d'informations, consultez la section Configurer Per App VPN.
- **Application supprimable :** (facultatif) spécifiez si cette application est supprimable par les utilisateurs lorsqu'il s'agit d'une application gérée. Pour empêcher les utilisateurs de désinstaller cette application, définissez cette option sur **Désactivé**. La valeur par défaut est **On**.
- **Activer le le téléchargement direct du domaine associé :** (facultatif) la valeur par défaut est **Activé**, ce qui indique que cette application effectue la vérification de l'association de site revendiquée directement sur le domaine plutôt que sur les serveurs d'Apple. Définissez cette option sur **Activé** uniquement pour les domaines qui ne peuvent pas accéder à Internet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Domaines associés :** (facultatif) pour ajouter un domaine associé pour cette application, cliquez sur **Ajouter**, puis entrez son nom de domaine complet (FQDN).

Rechercher le Bundle ID d'une application dans l'App Store

1. Localisez l'application dans l'App Store et copiez le numéro à la fin de l'URL. Par exemple, 363501921 est l'ID d'application pour l'application Citrix Workspace.
2. Accédez à `https://itunes.apple.com/lookup?id=` et collez le numéro après cette URL. Un fichier TXT est téléchargé automatiquement sur votre ordinateur.
3. Dans le fichier TXT, recherchez `bundleId` et obtenez le Bundle ID de l'application. Exemple : le Bundle ID pour l'application Citrix Workspace est `com.citrix.ReceiveriPad`.

Stratégie de configuration d'application

March 1, 2024

Vous pouvez configurer à distance des applications prenant en charge la configuration gérée en déployant :

- un fichier de configuration XML (`.plist`, aussi appelé une liste des propriétés) sur des appareils iOS
- des paires clé/valeur vers des téléphones, bureaux ou tablettes Windows 10 ou Windows 11

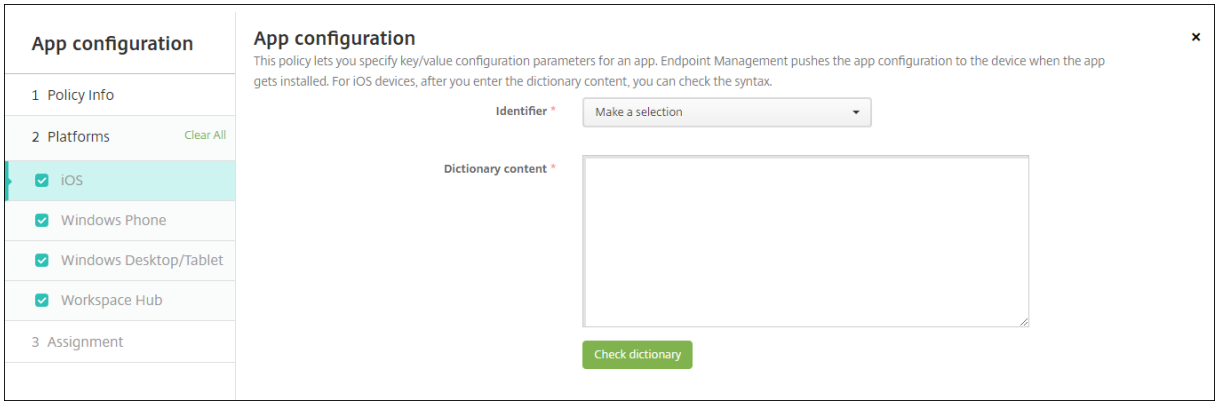
La configuration spécifie différents paramètres et comportements dans l'application. Citrix Endpoint Management transmet la configuration aux appareils lorsque l'utilisateur installe l'application. Les paramètres et les comportements que vous pouvez configurer dépendent de l'application et ne sont pas couverts dans cet article.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

> **Remarque :**
>
> Les variables de configuration de l'application sont définies par les propriétaires respectifs de l'application.
> Par exemple, les variables de configuration des applications pour Chrome sont gérées et mises à jour par Chrome. Pour en savoir plus, consultez la section Variables de configuration de l'application Chrome.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres iOS



- **Identifiant :** dans la liste, cliquez sur l'application que vous souhaitez configurer, ou cliquez sur **Ajouter** pour ajouter une application à la liste.
  - Si vous cliquez sur **Ajouter**, entrez l'identifiant de l'application dans le champ qui s'affiche.
- **Contenu du dictionnaire :** entrez, ou copiez et collez, les informations de configuration de la liste des propriétés XML (`.plist`).
- Cliquez sur **Vérifier le dictionnaire**. Citrix Endpoint Management vérifie le XML. S'il n'existe aucune erreur, veuillez consulter la section **XML valide** en dessous de la zone de contenu. Si des erreurs de syntaxe s'affichent en dessous de la zone de contenu, vous devez les corriger pour continuer.

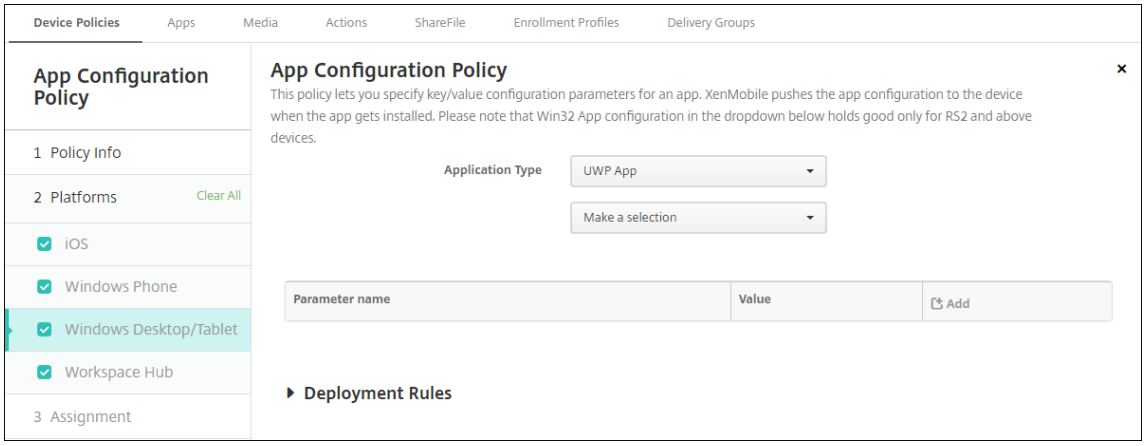
Paramètres Windows Desktop/Tablet

Vous pouvez configurer des applications Universal Windows Platform (UWP) ou des applications Win32. Pour importer les paramètres de stratégie de Microsoft Administrative Template (ADMX), configurez les applications Win32.

> **Remarque :**
>
> La stratégie de configuration d'application prend en charge les fichiers ADMX tiers pour les applications tierces telles qu'Office. Les modèles Microsoft ADMX pour Windows fournis en tant que stratégies de groupe du système d'exploitation disponibles sous `%SystemRoot%\PolicyDefinitions<!--NeedCopy-->` ne sont pas pris en charge.

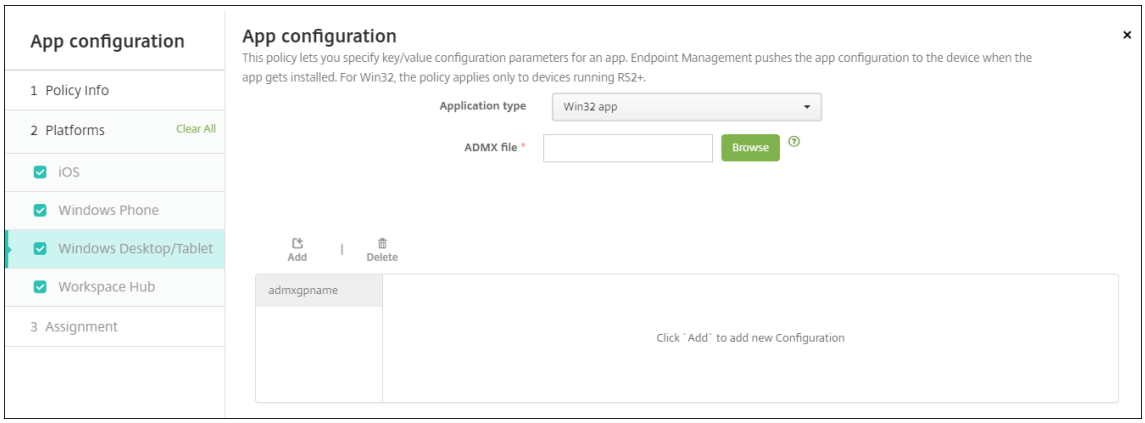
- Si vous choisissez **Application UWP** : dans la liste **Effectuer une sélection**, cliquez sur l'application que vous souhaitez configurer, ou cliquez sur **Ajouter** pour ajouter une application à la liste.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



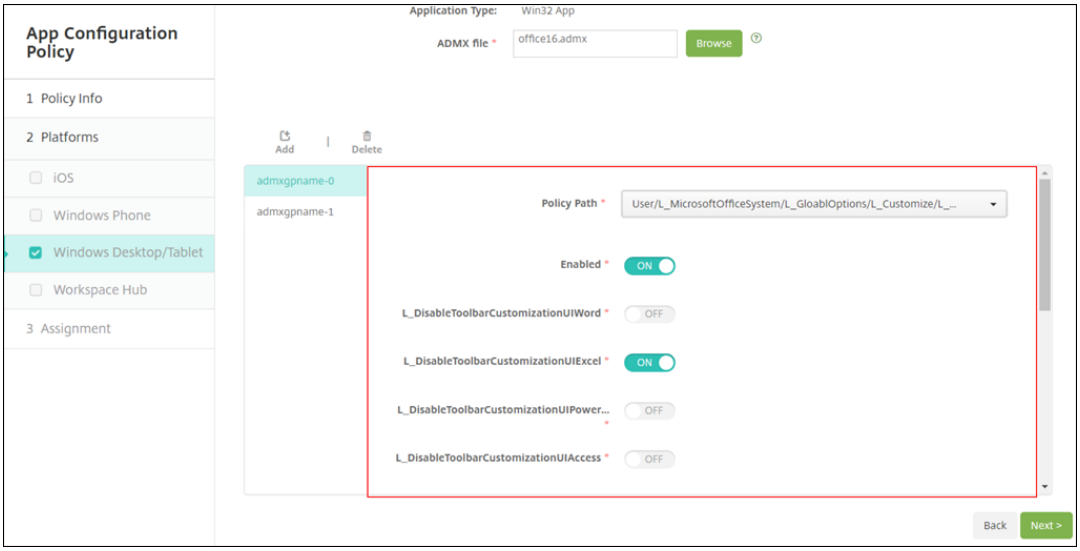
  - Si vous cliquez sur **Ajouter**, entrez le nom du package dans le champ qui s'affiche.
  - Pour chaque paramètre de configuration que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
    * **Nom du paramètre :** entrez le nom de clé d'un paramètre d'application pour le périphérique Windows. Pour de plus amples informations sur les paramètres des applications Windows, reportez-vous à la documentation Microsoft.
    * **Valeur :** entrez la valeur pour ce paramètre.
    * Cliquez sur **Ajouter** pour ajouter le paramètre, ou cliquez sur **Annuler** pour annuler l'ajout du paramètre.

- Si vous choisissez **App Win32** : cliquez sur **Parcourir** et accédez au fichier ADMX que vous souhaitez utiliser pour configurer la stratégie.



  - Cliquez sur **Ajouter**. Les options de configuration du fichier ADMX apparaissent sur le côté droit de la page.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Choisissez un chemin d'accès de la stratégie. Si vous choisissez le même chemin d'accès plusieurs fois, la configuration associée à la version la plus récente est appliquée.
- Définissez **Activer** sur **Activé**.
- Entrez les valeurs des éléments de liste requises sous forme de paires clé-valeur. Utilisez la chaîne **&#xF000** pour séparer chaque paire clé-valeur ainsi que la valeur et la clé dans la paire.
- Les valeurs qui incluent un nombre décimal peuvent nécessiter des valeurs dans une plage spécifique.

Stratégie d'inventaire des applications

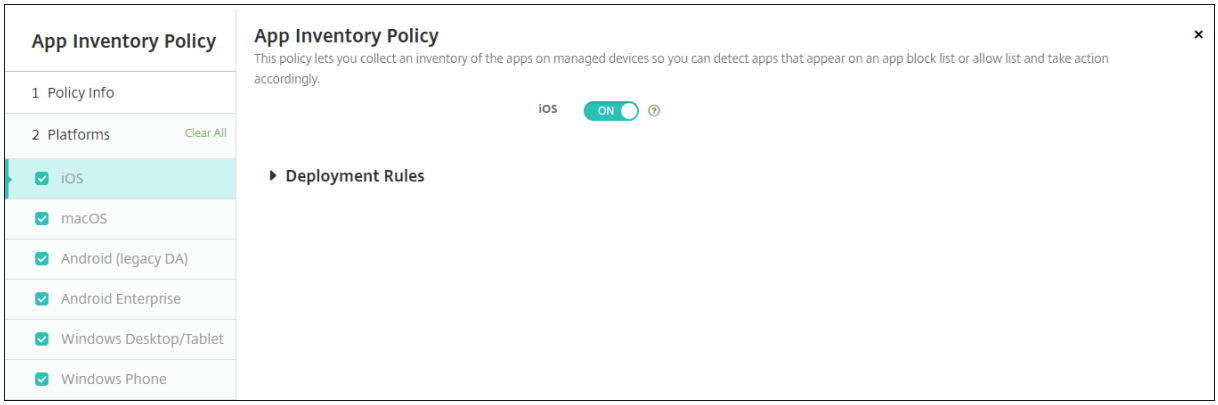
November 29, 2023

La stratégie Inventaire des applications vous permet d'établir un inventaire des applications sur les appareils gérés. Citrix Endpoint Management peut ensuite comparer l'inventaire avec les stratégies d'accès aux applications déployées sur ces appareils. Vous pouvez ainsi détecter les applications figurant sur une liste d'autorisation ou de blocage et prendre les mesures qui s'imposent. Utilisez une stratégie d'accès aux applications pour définir des listes d'autorisation ou de blocage.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

iOS, macOS, Android (ancien administrateur de l'appareil), Android Enterprise et Windows Desktop/Tablet



- Pour chaque plate-forme que vous sélectionnez, conservez le paramètre par défaut ou modifiez le paramètre (**Désactivé**). La valeur par défaut est **On**.

Inventaire et suppression d'applications Win32

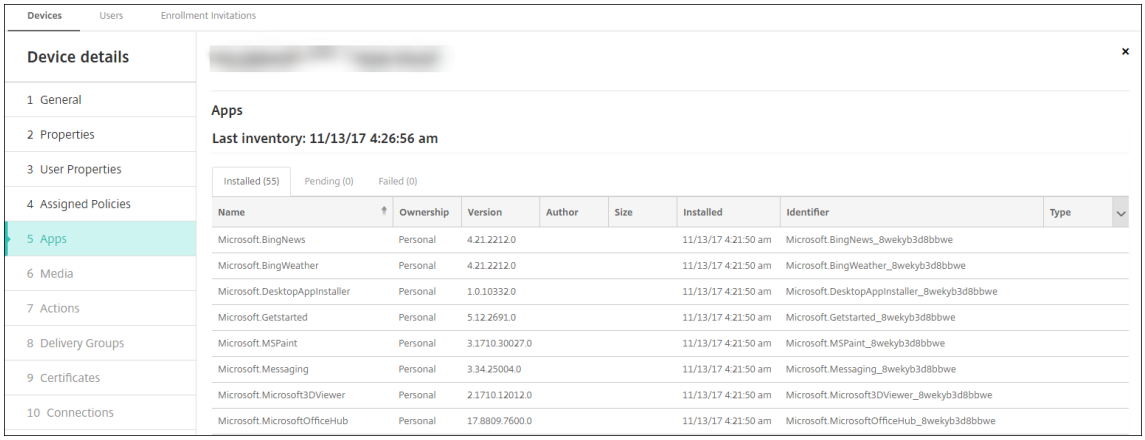
Vous pouvez déterminer si les applications Win32 sur les appareils utilisateur sont conformes à votre stratégie Accès aux applications. Pour afficher un inventaire des applications Win32 sur les appareils Windows 10 et Windows 11 Desktop et Tablet gérés :

1. Accédez à **Configurer > Stratégies d'appareil** et ajoutez une stratégie Inventaire des applications pour la plate-forme **Windows Desktop/Tablet**. Déployez la stratégie.
2. Accédez à **Gérer > Appareils**, sélectionnez l'appareil Windows 10 et Windows 11 que vous souhaitez afficher, cliquez sur **Modifier**, puis cliquez sur l'onglet **Applications**.

   Les résultats de l'inventaire s'affichent.

   > **Remarque :**
   >
   > Si vous configurez un appareil Windows 11, vous devez attendre jusqu'à 24 heures pour obtenir des résultats d'inventaire précis, un comportement conçu par Microsoft.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Comparez l'inventaire des applications avec votre stratégie Accès aux applications. Si des applications figurant sur la liste de blocage sont installées sur l'appareil, vous pouvez les supprimer des appareils.

Problèmes d'installation et de désinstallation de l'application causés par un code de produit incorrect

Si une application Win32 est configurée avec un code de produit incorrect, l'application s'installe initialement, toutefois Microsoft ne renvoie pas l'état de l'application à Citrix Endpoint Management. Résultat :

- La stratégie Désinstallation des applications ne désinstalle pas l'application.
- Citrix Endpoint Management continue à déployer l'application car aucune confirmation que l'application est installée n'a été reçue. À chaque déploiement, l'appareil génère un code d'erreur car l'application est déjà installée. L'erreur affichée dans **Gérer > Appareil > Détails du groupe de mise à disposition** est : `Msi Application received: Reporting: AppPush id:7z1701-x64.msi: Command execution failed -2147023293`

Pour corriger le code du produit :

1. Supprimez manuellement l'application de l'appareil.
2. Dans la console Citrix Endpoint Management, accédez à **Configurer > Applications** et corrigez le code de produit de l'application Win32.
3. Déployez l'application Win32.

Stratégie Application Guard

October 21, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

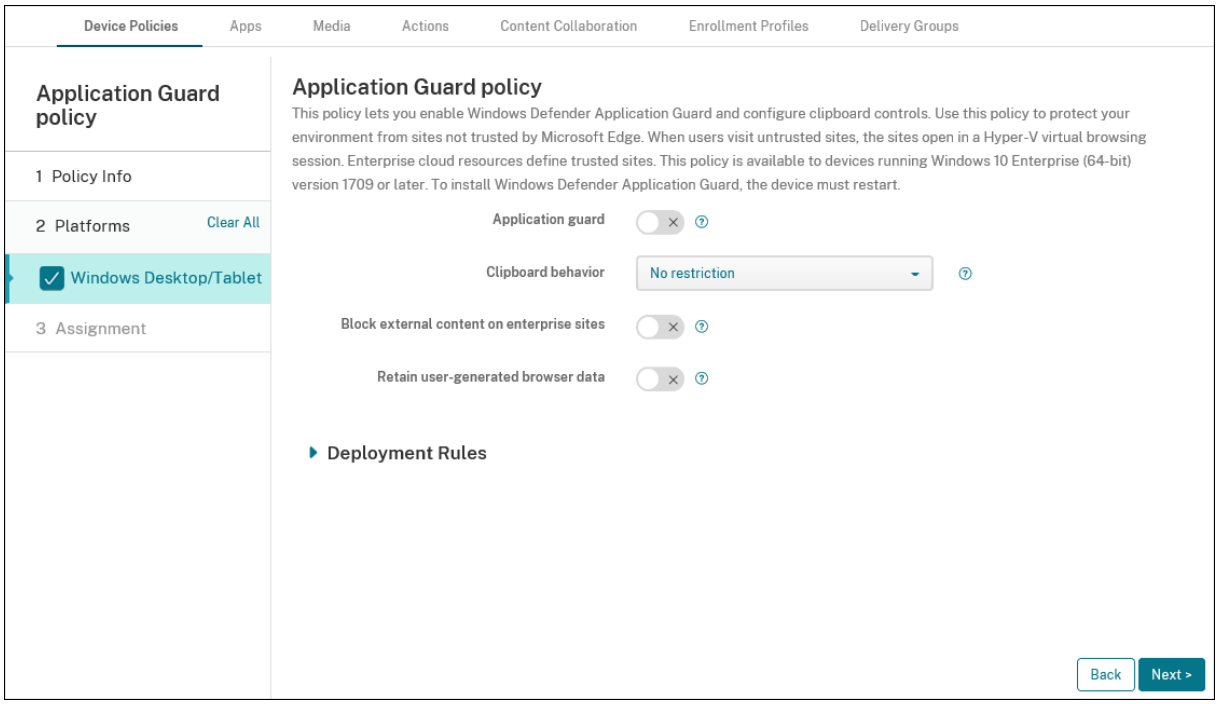
La stratégie Application Guard spécifie les paramètres de Windows Defender Application Guard. Les paramètres incluent l'activation d'Application Guard et le contrôle du comportement du Presse-papiers.

Windows Defender Application Guard protège votre environnement contre les sites qui n'ont pas été définis comme approuvés par votre organisation. Lorsque les utilisateurs visitent des sites qui ne figurent pas dans votre périmètre de réseau isolé, les sites s'ouvrent dans une session de navigation virtuelle dans Hyper-V. Les ressources de cloud d'entreprise définissent les sites de confiance.

Exigences

- Appareils exécutant Windows 10 Entreprise (64 bits) ou Windows 11 Entreprise (64 bits). Un redémarrage de l'appareil est requis pour installer Windows Defender Application Guard.
- Navigateur Microsoft Edge

Paramètres Windows Desktop et Tablet



- **Application Guard :** active Application Guard. La valeur par défaut est **Désactivé**.
  - **Ressources cloud d'entreprise :** liste séparée par des virgules des domaines de cloud d'entreprise.
- **Comportement du Presse-papiers :** contrôle le contenu pouvant être copié et collé. Les options sont les suivantes :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Non configuré**
  - **Autoriser le copier-coller uniquement du navigateur au PC :** permet aux utilisateurs de copier et de coller du contenu depuis leur navigateur vers leur ordinateur.
  - **Autoriser le copier-coller uniquement du PC au navigateur :** permet aux utilisateurs de copier et coller du contenu uniquement à partir de leur ordinateur vers leur navigateur.
  - **Autoriser le copier-coller entre le PC et le navigateur :** permet aux utilisateurs de copier et coller du contenu librement entre leur ordinateur et leur navigateur.
  - **Bloquer le copier-coller entre le PC et le navigateur :** ne permet pas aux utilisateurs de copier et coller du contenu entre leur PC et leur navigateur.

- **Contenu du Presse-papiers :** contrôle le contenu que les utilisateurs peuvent copier et coller. Les options sont les suivantes :

  - **Aucune restriction**
  - **Autoriser la copie de texte :** permet aux utilisateurs de copier du texte uniquement.
  - **Autoriser la copie d'images :** permet aux utilisateurs de copier des images uniquement.
  - **Autoriser la copie de texte et d'images :** permet aux utilisateurs de copier à la fois du texte et des images.

- **Bloquer le contenu externe sur les sites d'entreprise :** si cette option est **activée**, Windows Defender Application Guard empêche le chargement de contenu provenant de sites non approuvés sur les sites d'entreprise. La valeur par défaut est **Désactivé**.

- **Conserver les données de navigateur générées par l'utilisateur :** si cette option est **activée**, permet d'enregistrer les données utilisateur créées au cours d'une session de navigation virtuelle Application Guard. Ces données incluent les mots de passe, les favoris et les cookies. La valeur par défaut est **Désactivé**.

Stratégie de mode kiosque

November 29, 2023

La stratégie Mode kiosque définit une liste d'applications qui sont :

- Autorisées à s'exécuter sur un appareil.
- Interdites d'exécution sur un appareil.

La manière exacte dont la stratégie fonctionne diffère pour chaque plate-forme prise en charge. Par exemple, vous pouvez bloquer plusieurs applications sur un appareil iOS.

De même, pour les appareils iOS, vous pouvez sélectionner une seule application iOS par stratégie. Les utilisateurs peuvent uniquement utiliser leurs appareils pour exécuter une seule application. Ils

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ne peuvent effectuer aucune autre activité sur l'appareil, à l'exception des options que vous avez spécifiquement autorisées lorsque la stratégie de mode kiosque est appliquée.

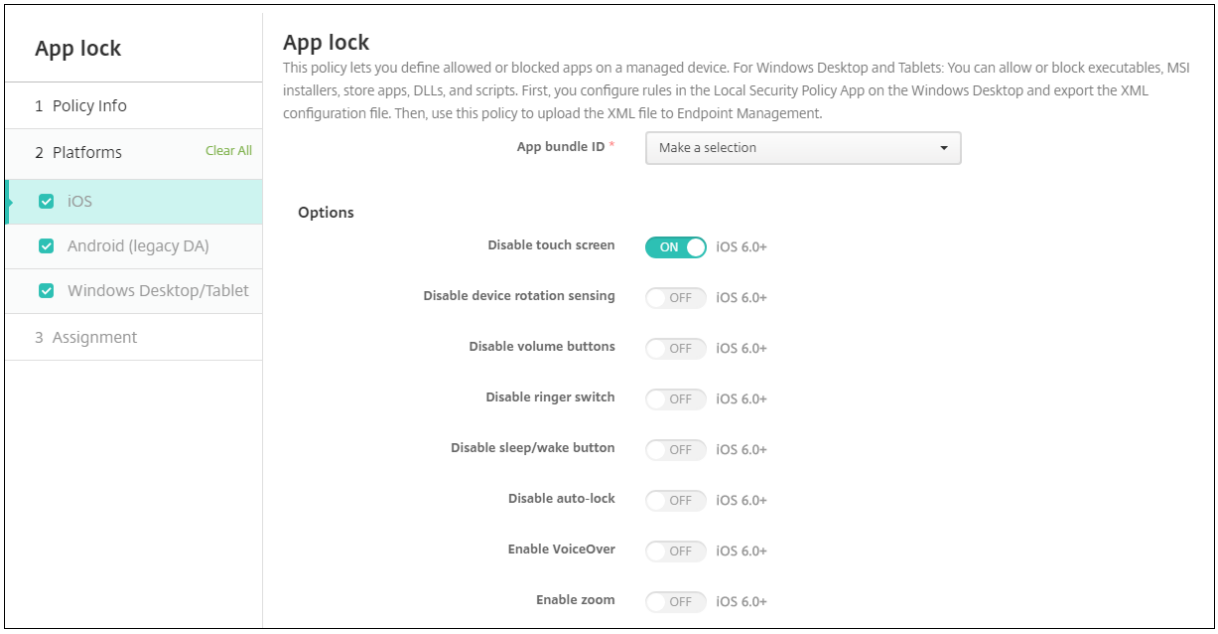
En outre, les appareils iOS doivent être supervisés pour pouvoir transmettre des stratégies de verrouillage d'applications.

Bien que la stratégie fonctionne sur la plupart des appareils Android L et M, le mode kiosque ne fonctionne pas sur les appareils Android N ou plus récents. Cela ne fonctionne pas car Google ne prend plus en charge l'API requise.

Sur les ordinateurs et les tablettes Windows gérés, vous pouvez créer une stratégie Mode kiosque définissant la liste des applications figurant sur les listes d'autorisation et de blocage. Vous pouvez autoriser ou bloquer les programmes exécutables, les programmes d'installation MSI, les applications de stockage, les DLL et les scripts.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Bundle ID d'application :** dans la liste, cliquez sur l'application à laquelle cette stratégie s'applique, ou cliquez sur **Ajouter** pour ajouter une application à la liste. Si vous sélectionnez **Ajouter**, entrez le nom de l'application dans le champ qui s'affiche.
- **Options :** pour chaque option, la valeur par défaut est **Désactivé**, sauf pour **Désactiver l'écran tactile**, qui est réglée par défaut sur **Activé**.
  - Désactiver l'écran tactile

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Désactiver détection de rotation
  - Désactiver boutons volume
  - Désactiver bouton sonnerie

    Lorsque l'option **Désactiver le commutateur de la sonnerie** est définie sur **Activé**, le comportement de la sonnerie dépend de la position dans laquelle se trouvait le commutateur lorsqu'il a été désactivé.
  - Désactiver le bouton veille
  - Désactiver verrouillage auto
  - Désactiver VoiceOver
  - Activer zoom
  - Activer l'inversion de couleurs
  - Activer AssistiveTouch
  - Activer Énoncer la sélection
  - Activer l'audio mono
  - Activer le contrôle vocal

- **Options utilisateur :** pour chaque option, la valeur par défaut est **Désactivé**.
  - Autoriser le réglage de VoiceOver
  - Autoriser le réglage du zoom
  - Autoriser le réglage d'inversion des couleurs
  - Autoriser le réglage AssistiveTouch
  - Autoriser le réglage du contrôle vocal

- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 ou version ultérieure.

Configurer un iPad en tant que kiosque

Vous pouvez utiliser la stratégie Mode kiosque pour exécuter un iPad supervisé en tant que kiosque. Apple utilise le terme « mode App individuelle » pour désigner cette fonctionnalité. Pour plus d'in-

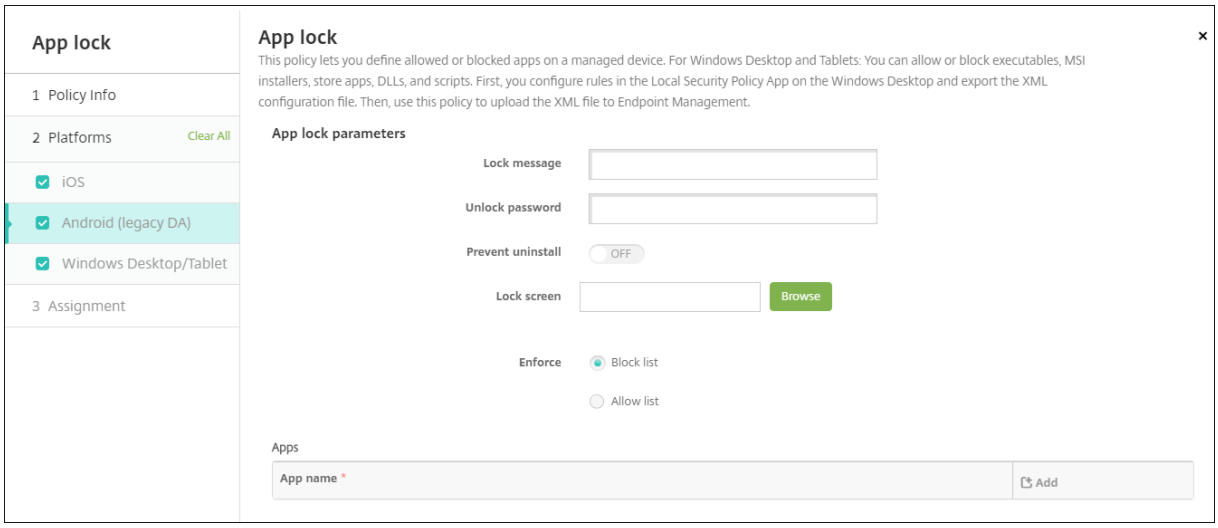
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

formations sur cette fonctionnalité, veuillez consulter la documentation Apple. Assurez-vous de déployer l'application que vous souhaitez exécuter avant de déployer cette stratégie.

1. Accédez à **Configurer > Stratégies d'appareil**, puis cliquez sur **Ajouter**.
2. Sélectionnez la stratégie **Mode kiosque**.
3. Tapez un **nom de stratégie** et, éventuellement, une **description**.
4. Sélectionnez uniquement la plate-forme **iOS**.
5. Pour **Bundle ID d'application**, sélectionnez l'application que vous souhaitez exécuter sur l'iPad.
6. Configurez toutes les options souhaitées, comme décrit précédemment, et enregistrez la stratégie.
7. Ajoutez la stratégie au même groupe de mise à disposition que votre iPad et déployez la stratégie.

Paramètres Android (DA hérité)

> **Remarque :**
>
> Vous ne pouvez pas bloquer l'application Paramètres Android à l'aide de la stratégie Mode kiosque.



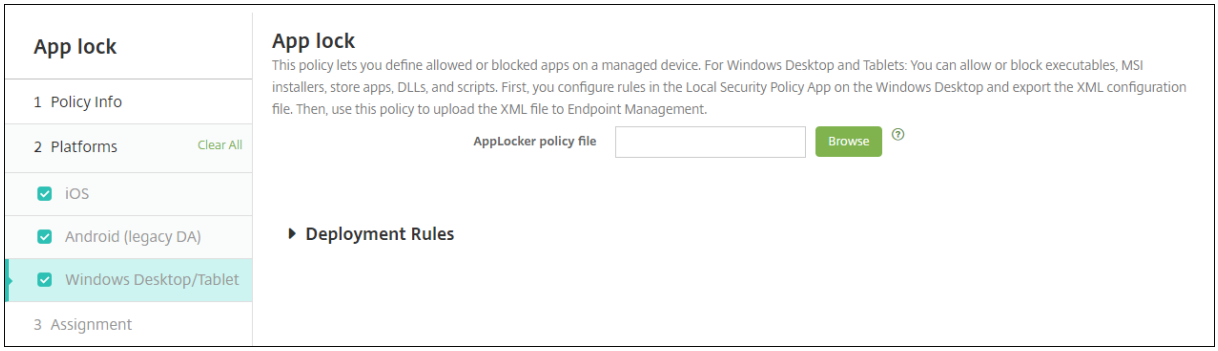
- **Paramètres du mode kiosque**
  - **Message de verrouillage :** entrez un message que les utilisateurs voient lorsqu'ils tentent d'ouvrir une application en mode kiosque.
  - **Mot de passe de déblocage :** entrez le mot de passe pour déverrouiller l'application.
  - **Empêcher la désinstallation :** indiquez si les utilisateurs sont autorisés à désinstaller les applications. La valeur par défaut est **Off**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Écran de verrouillage :** sélectionnez l'image qui s'affiche sur l'écran de verrouillage de l'appareil en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.
  - **Appliquer :** cliquez sur **Liste rouge** pour créer une liste d'applications qui ne sont pas autorisées à s'exécuter sur des appareils. Cliquez sur **Liste verte** pour créer une liste d'applications autorisées à s'exécuter sur des appareils.

- **Applications :** cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom de l'application :** dans la liste, cliquez sur le nom de l'application à ajouter à la liste d'autorisation ou de blocage. Vous pouvez également cliquer sur **Ajouter** pour ajouter une application à la liste des applications disponibles.
  - Si vous sélectionnez **Ajouter**, entrez le nom de l'application dans le champ qui s'affiche.
  - Cliquez sur **Enregistrer** ou **Annuler**.
  - Répétez ces étapes pour chaque application que vous souhaitez ajouter à la liste d'autorisation ou de blocage.

Paramètres Windows Desktop et Tablet



Prérequis pour le verrouillage d'application

- Dans Windows, configurez les règles dans l'éditeur Stratégie de sécurité locale sur un bureau Windows 10 ou Windows 11.
- Exportez le fichier XML de la stratégie. Citrix vous recommande de créer des règles par défaut dans Windows pour éviter de verrouiller la configuration par défaut ou d'entraîner des problèmes sur les appareils.
- Ensuite, téléchargez le fichier XML sur Citrix Endpoint Management à l'aide de la stratégie Mode kiosque. Pour plus d'informations sur la création de stratégies, consultez cet article Microsoft : https://docs.microsoft.com/en-us/windows/security/threat-protection/applocker/applocker-overview

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour configurer et exporter le fichier XML de la stratégie à partir de Windows

> **Important :**
>
> Lors de la configuration du fichier XML de la stratégie via l'éditeur de stratégie Windows, utilisez le mode Audit uniquement.

1. Sur l'ordinateur Windows, démarrez l'éditeur **Stratégie de sécurité locale**. Cliquez sur **Démarrer**, tapez **stratégie de sécurité locale** (ou local security policy), puis cliquez sur **Stratégie de sécurité locale**.
2. Dans l'arborescence de la console, développez **Stratégies de contrôle de l'application**.
3. Cliquez sur **AppLocker**, puis dans le volet central, cliquez sur **Configurer la mise en application des règles**.
4. Sélectionnez **Configuré**, puis **Appliquer les règles**. Lorsque vous activez une règle, **Appliquer les règles** est la valeur par défaut.
5. Cliquez avec le bouton droit sur **AppLocker**, cliquez sur **Exporter la stratégie**, puis enregistrez le fichier XML.

> **Remarque :**
>
> Vous pouvez créer **Règles de l'exécutable**, **Règles Windows Installer**, **Règles de script** et **Règles d'applications empaquetées**. Pour ce faire, cliquez avec le bouton droit sur le dossier, puis cliquez sur **Créer une règle**.

Pour importer le fichier XML de stratégie dans Citrix Endpoint Management

Créez une stratégie Mode kiosque. En regard du paramètre de **fichier de stratégie Mode kiosque**, cliquez sur **Parcourir** et naviguez jusqu'au fichier XML.

Pour arrêter d'appliquer une stratégie Mode kiosque

Après avoir déployé une stratégie Mode kiosque dans Citrix Endpoint Management : pour arrêter d'appliquer cette stratégie Mode kiosque, créez un fichier XML vide. Ensuite, créez une autre stratégie Mode kiosque, chargez le fichier et déployez la stratégie. Les appareils sur lesquels le mode kiosque est activé ne sont pas attribués. Sur les appareils qui reçoivent la stratégie pour la première fois, la stratégie Mode kiosque n'est pas appliquée.

Stratégie Notifications d'applications

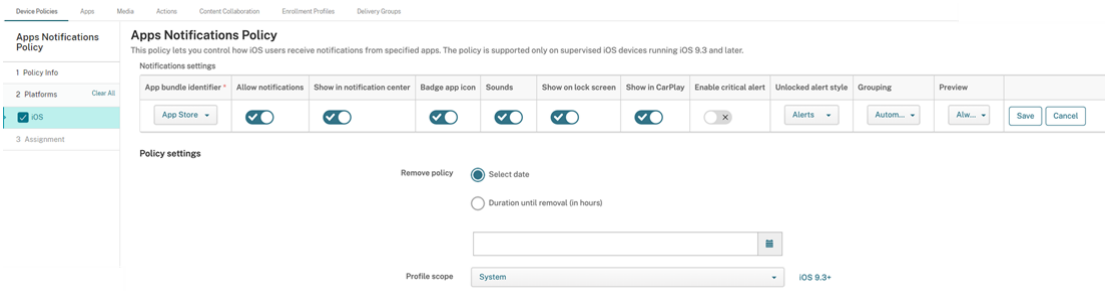
December 9, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La stratégie Notifications d'applications vous permet de contrôler la manière dont les utilisateurs iOS recevront les notifications depuis certaines applications. La stratégie est prise en charge uniquement sur les appareils iOS supervisés exécutant iOS 9.3 et versions ultérieures.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Bundle ID d'application :** spécifiez l'application dans laquelle vous souhaitez gérer les paramètres de notification :
  - Sélectionnez le Bundle ID d'application. Les options ne sont disponibles qu'après l'activation de la stratégie **Inventaire des applications**, qui collecte un inventaire des applications sur les appareils gérés.
  - Sélectionnez **Ajouter**, puis entrez le Bundle ID d'application.
    Pour trouver un Bundle ID d'application, consultez la section Rechercher le Bundle ID d'une application dans l'App Store.
- **Autoriser les notifications :** sélectionnez **Activé** pour autoriser les notifications.
- **Afficher dans le Centre de notifications :** sélectionnez **Activé** pour afficher les notifications dans le Centre de notifications des appareils utilisateur.
- **Pastille sur l'icône d'app :** sélectionnez **Activé** pour afficher une pastille sur l'icône d'application avec les notifications.
- **Sons :** sélectionnez **Activé** pour inclure des sons avec les notifications.
- **Afficher sur l'écran de verrouillage :** sélectionnez **Activé** pour afficher les notifications sur l'écran de verrouillage des appareils utilisateur.
- **Afficher dans CarPlay :** sélectionnez **Activé** pour afficher les notifications dans Apple CarPlay. S'applique à iOS 12 et versions ultérieures. La valeur par défaut est **Activé**.
- **Activer alerte critique :** sélectionnez **Activé** pour autoriser une application à marquer une notification comme critique qui ignore les paramètres Ne pas déranger et Sonnerie. S'applique à iOS 12 et versions ultérieures. La valeur par défaut est **Désactivé**.
- **Style d'alerte si déverrouillé :** sélectionnez **Aucune**, **Bannière** ou **Alertes** pour configurer l'apparence des alertes déverrouillées.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Aperçu :** sélectionnez la façon dont les appareils affichent les aperçus de notification pour l'application. S'applique à iOS 14 et versions ultérieures.
  - **Toujours :** pour afficher des aperçus de notification lorsque l'appareil est verrouillé ou déverrouillé.
  - **Une fois déverrouillé :** pour afficher des aperçus de notification uniquement lorsque l'appareil est déverrouillé.
  - **Jamais :** pour désactiver les aperçus de notification sur l'appareil.
- **Regroupement :** sélectionnez la manière dont les appareils regroupent les notifications de l'application. S'applique aux appareils iOS 12 et versions ultérieures.
  - **Automatique :** pour regrouper les notifications dans des groupes spécifiés par l'application.
  - **Par application :** pour regrouper les notifications de l'application dans un seul groupe.
  - **Désactivé :** pour désactiver le regroupement de notifications pour l'application. Les appareils affichent toutes les notifications dans l'ordre.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Ces options sont notamment :
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. S'applique à iOS 6.0 ou version ultérieure.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. S'applique à iOS 9.3 et versions ultérieures.

Stratégie de désinstallation des applications

November 29, 2023

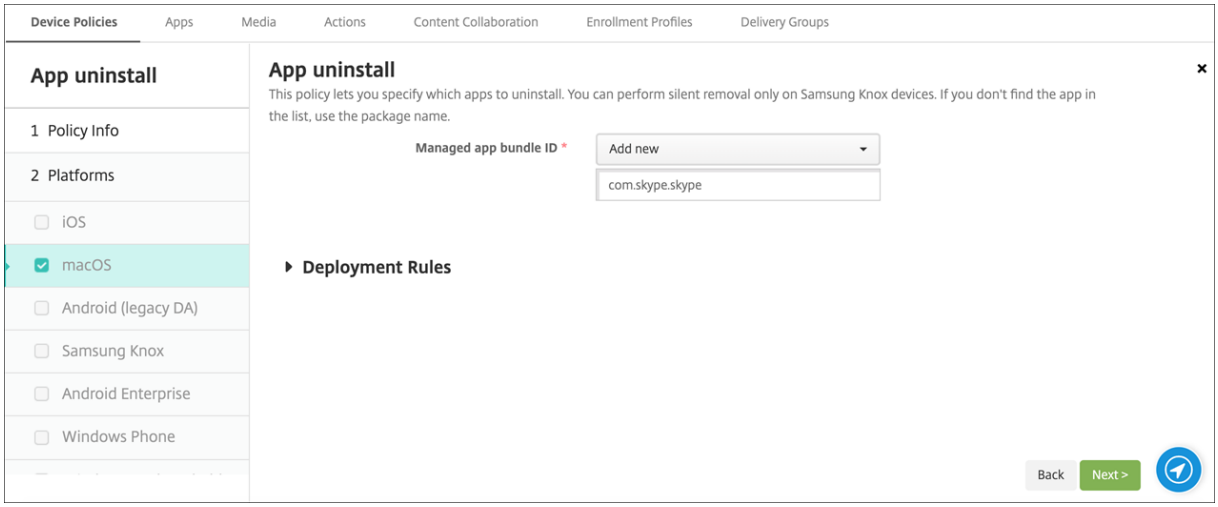
La stratégie de désinstallation d'application vous permet de supprimer des applications des appareils utilisateur. Vous pouvez supprimer une application si vous ne souhaitez plus la prendre en charge ou si vous souhaitez la remplacer par une application similaire d'un fournisseur différent.

Lorsque cette stratégie est déployée sur les appareils des utilisateurs, les utilisateurs sont invités à désinstaller l'application, puis l'application est supprimée.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres iOS et macOS



- **Bundle ID d'application gérée :** dans la liste, sélectionnez une application gérée existante ou **Ajouter**. Si aucune application n'est configurée pour cette plate-forme, la liste est vide et vous devez ajouter une nouvelle application gérée. Lorsque vous sélectionnez **Ajouter**, un champ apparaît dans lequel vous pouvez taper un nom d'application gérée. Disponible pour iOS 5.0 et versions ultérieures et macOS 11.0 et versions ultérieures.

Paramètres Android (ancien administrateur de l'appareil), Android Enterprise et Windows Desktop/Tablet

- **Applications à désinstaller :** pour chaque application que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom app :** dans la liste, cliquez sur une application existante ou sur **Ajouter** pour entrer un nouveau nom d'application. s'il n'existe pas d'applications configurées pour cette plate-forme, la liste est vide et vous devez ajouter de nouvelles applications.
  - Cliquez sur **Ajouter** pour ajouter l'application, ou cliquez sur **Annuler** pour annuler l'ajout de l'application.

Pour les applications Android Enterprise, activez également la stratégie d'inventaire des applications. Consultez la section Stratégie d'inventaire des applications.

Désinstaller automatiquement une application d'entreprise une fois que l'application de magasin public correspondante est installée

Vous pouvez configurer Citrix Endpoint Management pour supprimer la version d'entreprise des applications Citrix lors de l'installation de la version de magasin d'applications public. Cette fonctionnalité

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

empêche les appareils utilisateur d'avoir deux icônes d'application identiques après l'installation de la version de magasin d'applications public.

Une condition de déploiement pour la stratégie de désinstallation d'application déclenche la suppression par Citrix Endpoint Management des anciennes applications depuis les appareils utilisateur lors de l'installation de la nouvelle version. Cette fonctionnalité est uniquement disponible pour les appareils iOS gérés connectés à un serveur Citrix Endpoint Management en mode d'entreprise (XME).

Pour configurer une règle de déploiement avec la condition Nom de l'application installée :

- Spécifiez le **Bundle ID d'application gérée** pour l'application d'entreprise.
- Ajouter une règle : cliquez sur **Nouvelle règle**, puis, comme illustré dans l'exemple, choisissez **Nom de l'application installée** et **est égal à**. Entrez le bundle ID d'application pour l'application du magasin d'applications public.

Dans l'exemple, lors de l'installation de l'application de magasin d'applications public (com.citrix.mail.ios) sur un appareil dans les groupes de mise à disposition spécifiés, Citrix Endpoint Management supprime la version d'entreprise (com.citrix.mail).

Stratégie de restriction de désinstallation d'applications

July 7, 2022

Vous pouvez spécifier les applications que les utilisateurs peuvent ou ne peuvent pas désinstaller sur un appareil Amazon.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Amazon

- **Paramètres de restriction de désinstallation d'application :** pour chaque règle d'application que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom de l'application :** dans la liste, cliquez sur une application ou sur **Ajouter** pour ajouter une nouvelle application.
  - **Règle :** indiquez si les utilisateurs peuvent désinstaller l'application. Par défaut, la désinstallation est autorisée.
  - Cliquez sur **Enregistrer** ou **Annuler**.

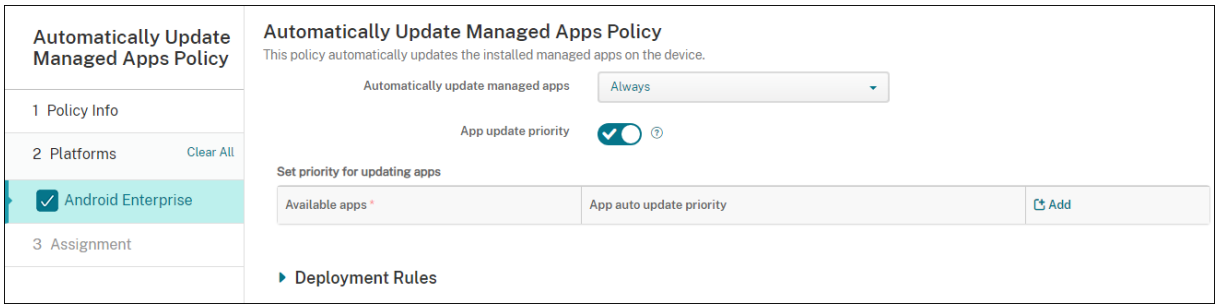
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie de mise à jour automatique des applications gérées

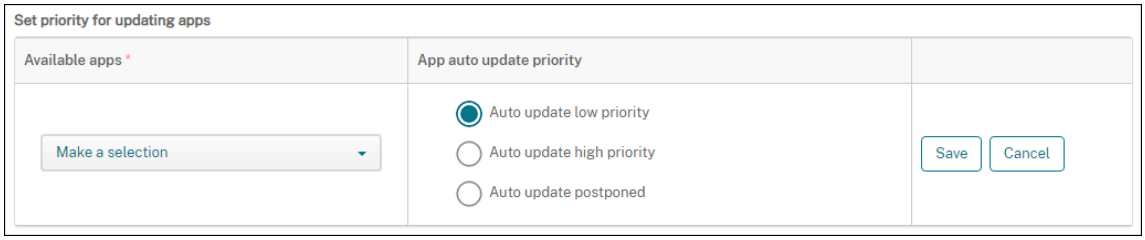
May 5, 2022

Cette stratégie contrôle la façon dont les applications gérées installées sont mises à jour sur les appareils Android Enterprise. Vous pouvez limiter la capacité des utilisateurs à autoriser les mises à jour automatiques des applications sur leurs appareils. Si vous autorisez les utilisateurs à contrôler les mises à jour automatiques des applications sur leurs appareils, ils définissent des stratégies de mise à jour automatique des applications dans le Google Play Store d'entreprise.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.



- **Mise à jour automatique des applications gérées**
  - **Toujours** : permet d'activer les mises à jour automatiques des applications. **Toujours** est la valeur par défaut.
  - **Autoriser l'utilisateur à configurer la stratégie** : permet à l'utilisateur de configurer la stratégie de mise à jour automatique des applications pour l'appareil dans le Google Play Store d'entreprise.
  - **Jamais** : permet de désactiver les mises à jour automatiques des applications.
  - **Uniquement lorsque l'appareil est connecté au Wi-Fi** : permet d'autoriser les mises à jour automatiques des applications uniquement lorsque l'appareil est connecté au Wi-Fi.
- **Priorité de mise à jour des applications :** si cette option est **activée**, vous pouvez configurer un niveau de priorité de mise à jour pour chaque application gérée.
- **Définir priorité de mise à jour des applications :** cliquez sur **Ajouter** pour configurer la priorité de mise à jour pour une application.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Applications disponibles :** sélectionnez une application dans le menu pour configurer la priorité de mise à jour.
- **Priorité de mise à jour automatique des applications :** sélectionnez une priorité de mise à jour parmi les suivantes :
  * **Priorité de mise à jour automatique basse :** l'application se met à jour lorsque l'appareil est en charge, qu'il n'est pas utilisé activement et qu'il est connecté au un réseau via un forfait.
  * **Priorité de mise à jour automatique élevée :** l'application se met à jour dès que possible, sans contraintes.
  * **Mise à jour automatique reportée :** l'application n'est pas mise à jour automatiquement pendant un maximum de 90 jours après la publication d'une nouvelle version. Après 90 jours, l'application se met automatiquement à jour avec une priorité basse. Une fois l'application mise à jour, aucune mise à jour automatique n'est effectuée pendant 90 jours. L'utilisateur peut mettre à jour l'application manuellement à tout moment.
- Cliquez sur **Save** lorsque vous avez terminé. Vous pouvez modifier une configuration en cliquant sur l'icône crayon. Supprimez la configuration en cliquant sur la corbeille.

Stratégie BitLocker

November 29, 2023

Windows 10 et Windows 11 comprennent une fonctionnalité de cryptage de disque appelée BitLocker, qui fournit une protection fichier et système supplémentaire contre tout accès non autorisé à un appareil Windows perdu ou volé. Pour une protection supplémentaire, vous pouvez utiliser BitLocker avec Trusted Platform Module (TPM), version 1.2 ou supérieure. Une puce TPM gère les opérations de chiffrement et génère, stocke et limite l'utilisation des clés cryptographiques.

À compter de Windows 10, build 1703, les stratégies MDM peuvent contrôler BitLocker. Vous pouvez utiliser la stratégie BitLocker dans Citrix Endpoint Management pour configurer les paramètres disponibles dans l'Assistant BitLocker sur les appareils Windows 10 et Windows 11. Par exemple, sur un appareil avec BitLocker activé, BitLocker invite les utilisateurs à configurer :

- la manière dont ils souhaitent déverrouiller leur lecteur au démarrage ;
- la manière de sauvegarder leur clé de récupération ;
- la manière de déverrouiller un lecteur fixe.

La configuration de la stratégie BitLocker permet également d'indiquer si :

- BitLocker doit être activé sur les appareils sans puce TPM ;

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- les options de récupération doivent être affichées sur l'interface BitLocker ;
- l'accès en écriture sur un lecteur amovible ou fixe doit être refusé si BitLocker n'est pas activé.
- Enregistrez en toute sécurité une clé de récupération BitLocker cryptée pour permettre aux utilisateurs d'y accéder au cas où ils oublieraient ou égareraient la clé. Cette clé se trouve sur le portail en libre-service.

> Remarque
>
> Une fois que le cryptage BitLocker démarre sur un appareil, vous ne pouvez pas modifier les paramètres de BitLocker sur l'appareil via le déploiement d'une stratégie BitLocker mise à jour.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

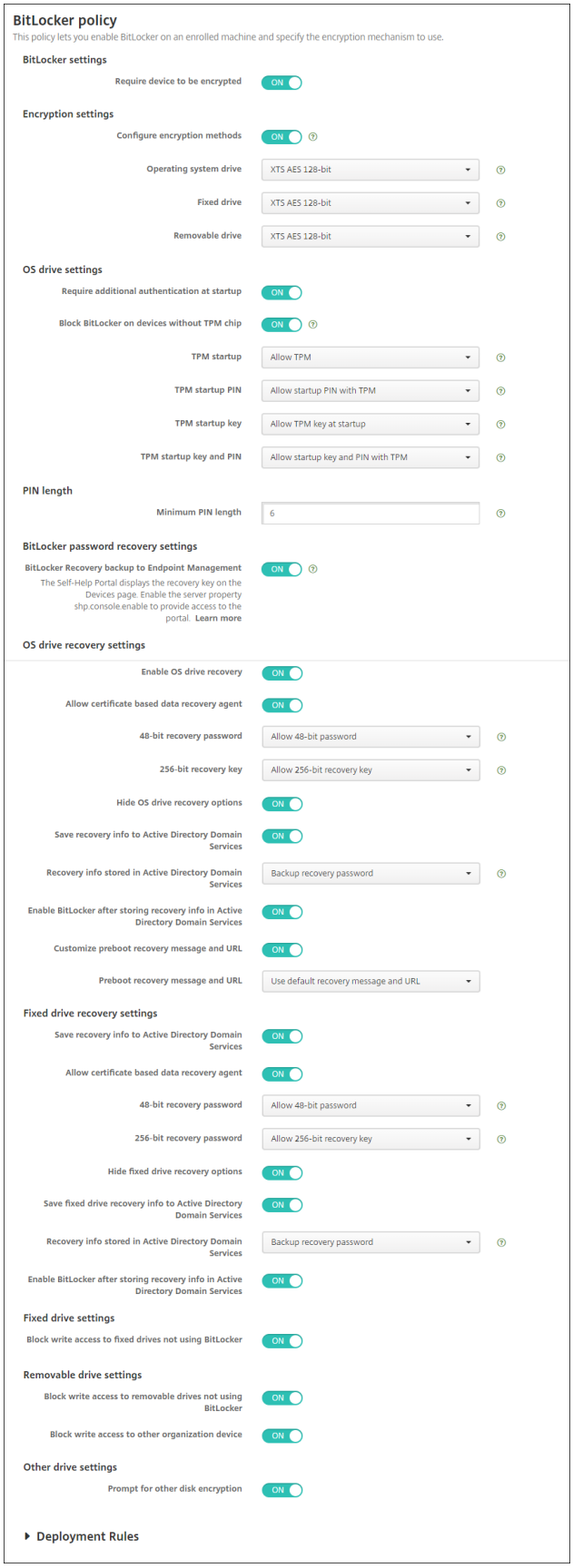
Exigences

- La stratégie BitLocker requiert Windows 10 Enterprise Edition ou Windows 11 Enterprise Edition.
- Avant de déployer la stratégie BitLocker, préparez votre environnement pour l'utilisation de BitLocker. Pour plus d'informations, y compris sur la configuration système requise pour BitLocker et son installation, consultez les articles de la page BitLocker.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Windows Desktop et Tablet



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Paramètres de BitLocker**
  - **Exiger cryptage de l'appareil :** permet d'indiquer si vous souhaitez inviter les utilisateurs à activer le cryptage BitLocker sur Windows Desktop ou Tablet. Si cette option est définie sur **Activé**, les appareils affichent un message, une fois l'inscription terminée, indiquant que l'entreprise requiert le cryptage de l'appareil. Si cette option est définie sur **Désactivé**, l'utilisateur ne reçoit pas d'invite et BitLocker utilise les paramètres de stratégie. La valeur par défaut est **Désactivé**.
- **Paramètres de cryptage**
  - **Configurer les méthodes de cryptage :** permet d'indiquer les méthodes de cryptage à utiliser pour des types de lecteurs spécifiques. Si cette option est définie sur **Désactivé**, l'assistant BitLocker invite l'utilisateur à choisir la méthode de cryptage à utiliser pour un type de lecteur. Par défaut, la méthode de cryptage pour tous les lecteurs est XTS-AES 128 bits. La méthode de cryptage pour les lecteurs amovibles est AES-CBC 128 bits par défaut. Si cette option est définie sur **Activé**, BitLocker utilise la méthode de cryptage spécifiée dans la stratégie. Si cette option est définie sur **Activé**, ces paramètres supplémentaires s'affichent : **Lecteur du système d'exploitation**, **Lecteur fixe** et **Lecteur amovible**. Choisissez la méthode de cryptage par défaut pour chaque type de lecteur. La valeur par défaut est **Désactivé**.
- **Paramètres de lecteur d'OS**
  - **Exiger authentification supplémentaire au démarrage :** indique l'authentification supplémentaire requise lors du démarrage de l'appareil. Spécifie également si vous souhaitez autoriser BitLocker sur les appareils qui ne possèdent pas de puce TPM. Si cette option est définie sur **Désactivé**, les appareils sans TPM ne peuvent pas utiliser le cryptage BitLocker. Pour plus d'informations sur la puce TPM, consultez l'article de Microsoft, Vue d'ensemble de la technologie de module de plateforme sécurisée. Si cette option est définie sur **Activé**, les paramètres supplémentaires suivants s'affichent. La valeur par défaut est **Désactivé**.
  - **Bloquer BitLocker sur les appareils sans puce TPM :** sur un appareil sans puce TPM, BitLocker exige que les utilisateurs créent un mot de passe de déverrouillage ou une clé de démarrage. La clé de démarrage est stockée sur un lecteur USB, que l'utilisateur doit connecter à l'appareil avant le démarrage. Le mot de passe de déverrouillage doit comporter un minimum de huit caractères. La valeur par défaut est **Désactivé**.
  - **Démarrage de TPM :** sur un appareil avec puce TPM, il existe quatre modes de déverrouillage : TPM uniquement, TPM + code PIN, TPM + clé et TPM + code PIN + clé. Le démarrage de TPM est pour le mode TPM uniquement, avec lequel les clés de cryptage sont stockées dans la puce TPM. Ce mode ne requiert pas qu'un utilisateur fournisse des données de déverrouillage supplémentaires. L'appareil utilisateur se déverrouille automatiquement

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

au cours du redémarrage, à l'aide de la clé de cryptage stockée dans la puce TPM. La valeur par défaut est **Autoriser TPM**.

  - **Code PIN de démarrage de TPM :** ce paramètre correspond au mode de déverrouillage TPM + code PIN. Un code PIN peut contenir jusqu'à 20 chiffres. Utilisez le paramètre **Longueur minimale du code PIN** pour spécifier la longueur minimale du code PIN. Un utilisateur configure un code PIN lors de la configuration de BitLocker et fournit le code PIN lors du démarrage de l'appareil.
  - **Clé de démarrage de TPM :** ce paramètre correspond au mode de déverrouillage TPM + clé. La clé de démarrage est stockée sur un lecteur USB ou autre lecteur amovible, que l'utilisateur doit connecter à l'appareil avant le démarrage.
  - **Clé et code PIN de démarrage de TPM :** ce paramètre correspond au mode de déverrouillage TPM + code PIN + clé.

    Si le déverrouillage réussit, le chargement du système d'exploitation démarre. Sinon, l'appareil entre en mode de récupération.

- **Longueur du code PIN**
  - **Longueur minimale du code PIN :** longueur minimale du code PIN de démarrage de la puce TPM. La valeur par défaut est de **6**.
- **Paramètres de récupération du mot de passe de BitLocker**
  - **Récupération des données de BitLocker sur Citrix Endpoint Management :** si cette option est activée, les utilisateurs qui ont besoin de déverrouiller leurs appareils peuvent trouver leur clé de récupération BitLocker sur le portail en libre-service. L'administrateur de Citrix Endpoint Management ne peut pas voir la clé de récupération BitLocker d'un utilisateur. Pour plus d'informations sur l'affichage de votre clé de récupération BitLocker, consultez la section Clé de récupération BitLocker.
- **Paramètres de récupération de lecteur d'OS :** permet de configurer les options de récupération des utilisateurs pour un lecteur d'OS crypté par BitLocker.
  - **Activer récupération de lecteur d'OS :** en cas d'échec de l'étape de déverrouillage, BitLocker invite l'utilisateur à fournir la clé de récupération configurée. Ce paramètre permet de configurer les options de récupération de lecteur du système d'exploitation à la disposition des utilisateurs lorsqu'ils ne possèdent pas de mot de passe de déverrouillage ou de clé de démarrage USB. La valeur par défaut est **Off**.
  - **Autoriser agent de récupération de données basé sur certificat :** indique si un agent de récupération des données basé sur certificat est autorisé. Ajoutez un agent de récupération de données depuis les stratégies de clé publique, qui se trouvent dans la Console de gestion des stratégie de groupe (GPMC) ou dans l'éditeur de stratégie de groupe local.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour plus d'informations sur les agents de récupération de données, consultez l'article Microsoft BitLocker Basic Deployment. La valeur par défaut est **Off**.

- **Mot de passe de récupération 48 bits :** indique si vous souhaitez autoriser les utilisateurs à utiliser un mot de passe de récupération ou les y obliger. BitLocker génère le mot de passe et l'enregistre dans un fichier ou un compte Cloud Microsoft. La valeur par défaut est **Autoriser mot de passe de 48 bits**.
- **Clé de récupération de 256 bits :** indique si vous souhaitez autoriser les utilisateurs à utiliser une clé de récupération ou les y obliger. Une clé de récupération est un fichier BEK, qui est stocké sur un lecteur USB. La valeur par défaut est **Autoriser clé de récupération de 256 bits**.
- **Masquer les options de récupération de lecteur d'OS :** indique si vous souhaitez afficher ou masquer les options de récupération sur l'interface BitLocker. Si cette option est définie sur **Activé**, aucune option de récupération ne s'affiche sur l'interface BitLocker. Dans ce cas, inscrivez les appareils sur Active Directory, enregistrez les options de récupération sur Active Directory et définissez **Enregistrer les informations de récupération sur AD DS** sur **Activé**. La valeur par défaut est **Off**.
- **Enregistrer les informations de récupération dans Active Directory Domain Services :** permet d'indiquer si vous souhaitez enregistrer les options de récupération dans les services de domaine Active Directory. La valeur par défaut est **Off**.
- **Informations de récupération stockées dans Active Directory Domain Services :** permet d'indiquer si vous souhaitez stocker le mot de passe de récupération BitLocker ou le mot de passe de récupération et le pack de clé dans les services de domaine Active Directory. Le stockage du pack de clé prend en charge la récupération des données à partir d'un lecteur qui est altéré physiquement. La valeur par défaut est **Sauvegarder le mot de passe de récupération**.
- **Activer BitLocker après avoir stocké les informations de récupération dans Active Directory Domain Services :** permet d'indiquer si vous souhaitez empêcher les utilisateurs d'activer BitLocker sauf si l'appareil est connecté à un domaine et si la sauvegarde des informations de récupération BitLocker sur Active Directory réussit. Si cette option est définie sur **Activé**, un appareil doit appartenir à un domaine avant de démarrer BitLocker. La valeur par défaut est **Off**.
- **Message et URL de récupération préalables au démarrage :** permet d'indiquer si BitLocker affiche un message et une adresse URL personnalisés sur l'écran de récupération. Si cette option est définie sur **Activé**, les paramètres supplémentaires suivants s'affichent : **Utiliser le message de récupération et l'URL par défaut**, **Utiliser un message de récupération et une URL vides**, **Utiliser un message de récupération personnalisé**, **Utiliser une URL de récupération personnalisée** et **Utiliser le message**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de récupération et l'URL de Citrix Endpoint Management. Si cette option est définie sur **Désactivé**, le message de récupération et l'URL par défaut s'affichent. La valeur par défaut est **Off**.

- **Paramètres de récupération de lecteur fixe :** permet de configurer les options de récupération des utilisateurs pour un lecteur fixe crypté par BitLocker. BitLocker n'affiche pas de message sur le cryptage de lecteur fixe. Pour déverrouiller un lecteur au cours du démarrage, un utilisateur fournit un mot de passe ou une carte à puce. Les paramètres de déverrouillage au démarrage, qui ne sont pas dans cette stratégie, s'affichent dans l'interface BitLocker lorsqu'un utilisateur active le cryptage BitLocker sur un lecteur fixe. Pour plus d'informations sur les paramètres connexes, consultez la section **Configurer la récupération de lecteur d'OS**, plus haut dans cette liste. La valeur par défaut est **Off**.
- **Paramètres de lecteur fixe**
  - **Bloquer l'accès en écriture aux lecteurs fixes n'utilisant pas BitLocker :** si cette option est définie sur **Activé**, les utilisateurs peuvent écrire sur les lecteurs fixes uniquement lorsque ces lecteurs sont cryptés avec BitLocker. La valeur par défaut est **Off**.
- **Paramètres de lecteur amovible**
- **Bloquer l'accès en écriture aux lecteurs amovibles n'utilisant pas BitLocker :** si cette option est définie sur **Activé**, les utilisateurs peuvent écrire sur les lecteurs amovibles uniquement lorsque ces lecteurs sont cryptés avec BitLocker. Configurez ce paramètre en fonction de la politique de votre organisation, selon qu'elle autorise l'accès en écriture sur les lecteurs amovibles d'une autre organisation ou non. La valeur par défaut est **Off**.
- **Bloquer l'accès en écriture aux autres appareils de l'organisation :** si cette option est définie sur **Activé**, les utilisateurs ne peuvent pas écrire sur d'autres appareils de leur organisation, tels qu'un lecteur réseau.
- **Autres paramètres de lecteur**
- **Demander autre cryptage de disque :** vous permet de désactiver l'invite d'avertissement concernant d'autre cryptage de disque sur les appareils. La valeur par défaut est **Désactivé**.

Stratégie Bluetooth

December 9, 2021

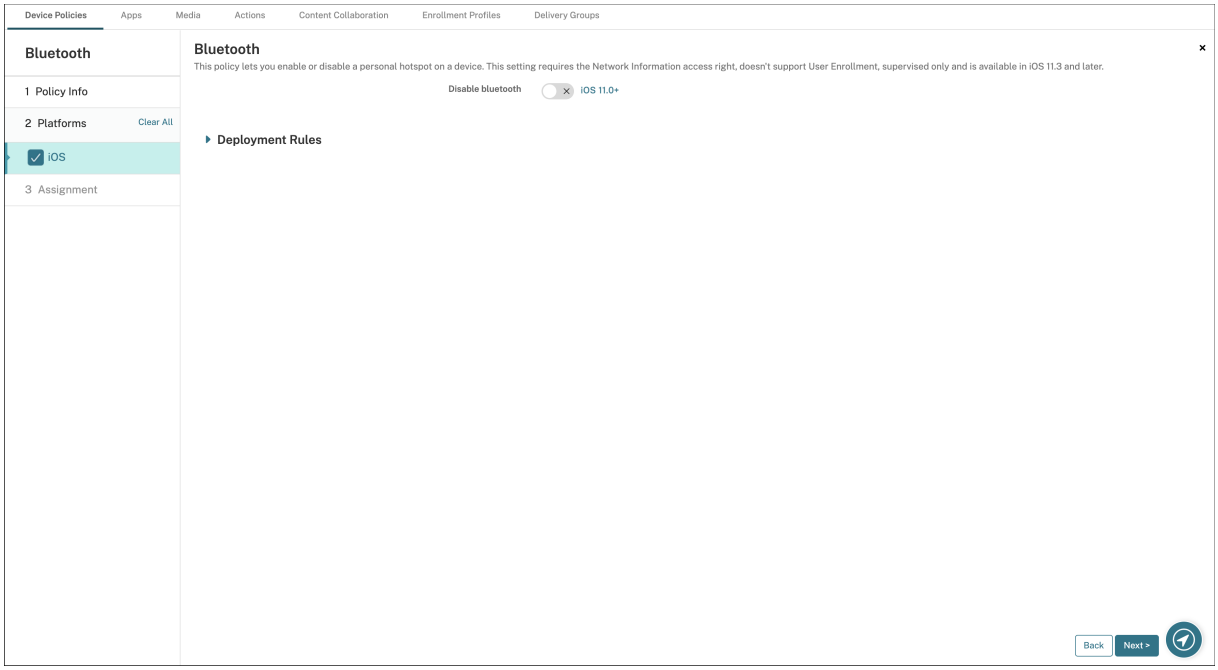
Vous pouvez configurer une stratégie Bluetooth sur les appareils iOS supervisés pour activer ou désactiver le Bluetooth.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ce paramètre nécessite le droit d'accès aux informations réseau, ne prend pas en charge l'inscription d'utilisateurs et est disponible sur iOS 11.3 et versions ultérieures.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Désactiver Bluetooth :** permet de désactiver ou d'activer le Bluetooth sur l'appareil supervisé.

Stratégie de calendrier (CalDav)

November 29, 2023

Vous pouvez ajouter une stratégie dans Citrix Endpoint Management afin d'ajouter un compte de calendrier (CalDAV) sur des appareils iOS ou macOS pour permettre à leurs utilisateurs de synchroniser les données de planification avec tout serveur qui prend en charge CalDAV.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Description du compte :** entrez une description du compte. Ce champ est obligatoire.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Nom d'hôte :** entrez l'adresse du serveur CalDAV. Ce champ est obligatoire.
- **Port :** entrez le port sur lequel se connecter au serveur CalDAV. Ce champ est obligatoire. La valeur par défaut est **8443**.
- **URL principale :** entrez l'adresse URL du calendrier de l'utilisateur.
- **Nom d'utilisateur :** entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe :** entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CalDAV. La valeur par défaut est **On**.
- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 ou version ultérieure.

Paramètres macOS

- **Description du compte :** entrez une description du compte. Ce champ est obligatoire.
- **Nom d'hôte :** entrez l'adresse du serveur CalDAV. Ce champ est obligatoire.
- **Port :** entrez le port sur lequel se connecter au serveur CalDAV. Ce champ est obligatoire. La valeur par défaut est **8443**.
- **URL principale :** entrez l'adresse URL du calendrier de l'utilisateur.
- **Nom d'utilisateur :** entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe :** entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CalDAV. La valeur par défaut est **On**.
- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Stratégie cellulaire

November 29, 2023

Cette stratégie vous permet de configurer des paramètres réseau cellulaire sur un appareil iOS.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

Vous pouvez utiliser des macros dans des champs autres que des chaînes, tels que **Port du serveur proxy**.

Par exemple, vous pouvez utiliser une macro telle que `${ device.xyz }` ou `${ setting.xyz }` qui devient un entier. Vous pouvez également utiliser les macros dans un fichier XML de configuration d'appareil que vous importez dans Citrix Endpoint Management à l'aide de la stratégie d'importation de profils iOS et macOS.

- **Attacher le nom de point d'accès**
  - **Nom :** nom de cette configuration.
  - **Type d'authentification :** dans la liste, cliquez sur **CHAP** (Challenge Handshake Authentication Protocol) ou **PAP** (Password Authentication Protocol). La valeur par défaut est **PAP**.
  - **Nom d'utilisateur** et **Mot de passe** : nom d'utilisateur et mot de passe à utiliser pour l'authentification.
- **APN**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Nom :** nom de la configuration du nom du point d'accès (APN).
  - **Type d'authentification :** dans la liste, cliquez sur **CHAP** ou **PAP**. La valeur par défaut est **PAP**.
  - **Nom d'utilisateur** et **Mot de passe** : nom d'utilisateur et mot de passe à utiliser pour l'authentification.
  - **Serveur proxy :** adresse réseau du serveur proxy.
  - **Port du serveur proxy :** port du serveur proxy.

- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.

Stratégie de planification de connexion

November 29, 2023

> **Important :**
>
> Citrix recommande d'utiliser Firebase Cloud Messaging (FCM) pour contrôler les connexions à partir des appareils Android et Android Enterprise vers Citrix Endpoint Management. Pour plus d'informations sur l'utilisation de FCM, voir Firebase Cloud Messaging.

Si vous choisissez de ne pas utiliser FCM, vous pouvez créer des stratégies de planification de connexion afin de contrôler comment et quand les appareils se connectent à Citrix Endpoint Management. Si vous choisissez d'utiliser FCM, vous devez également créer une stratégie de planification de connexion.

Vous pouvez spécifier que les utilisateurs connectent leurs appareils manuellement ou que les appareils se connectent dans un intervalle de temps défini.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Android et Android Enterprise

- **Exiger que les appareils se connectent :** cliquez sur l'option que vous souhaitez définir pour cette planification.
  - **Jamais :** connexion manuelle. Les utilisateurs doivent lancer la connexion depuis Citrix Endpoint Management sur leurs appareils. Citrix ne recommande pas cette option pour les déploiements de production, car elle empêche le déploiement des stratégies de sécurité sur les appareils, ce qui signifie que les utilisateurs ne reçoivent jamais les nouvelles applications ou stratégies. L'option **Jamais** est activée par défaut.
  - **Toutes les :** se connecte à l'intervalle défini. Lorsque cette option est activée et que vous envoyez une stratégie de sécurité telle qu'un effacement ou verrouillage, Citrix Endpoint Management traite l'action sur l'appareil la prochaine fois que l'appareil se connecte. Lorsque vous sélectionnez cette option, le champ **Se connecter toutes les N minutes** apparaît. Vous devez y entrer le nombre de minutes après lesquelles l'appareil doit se reconnecter. La valeur par défaut, et la valeur minimale, est **120**.
  - **Définir un calendrier :** Citrix Endpoint Management tente de se reconnecter à Citrix Endpoint Management Server sur l'appareil de l'utilisateur après une perte de connexion réseau. Citrix Endpoint Management surveille la connexion en transmettant des paquets de contrôle à intervalles réguliers dans le délai que vous définissez. Pour savoir comment définir un délai de connexion, consultez la section Définition d'un délai de connexion.
    - **Exiger une connexion dans chacun de ces intervalles :** les appareils des utilisateurs doivent être connectés au moins une fois dans les intervalles de temps définis.
    - **Utiliser l'heure locale de l'appareil comme référence et non l'heure UTC :** synchronise les intervalles définis avec l'appareil local plutôt que le temps universel coordonné (UTC).

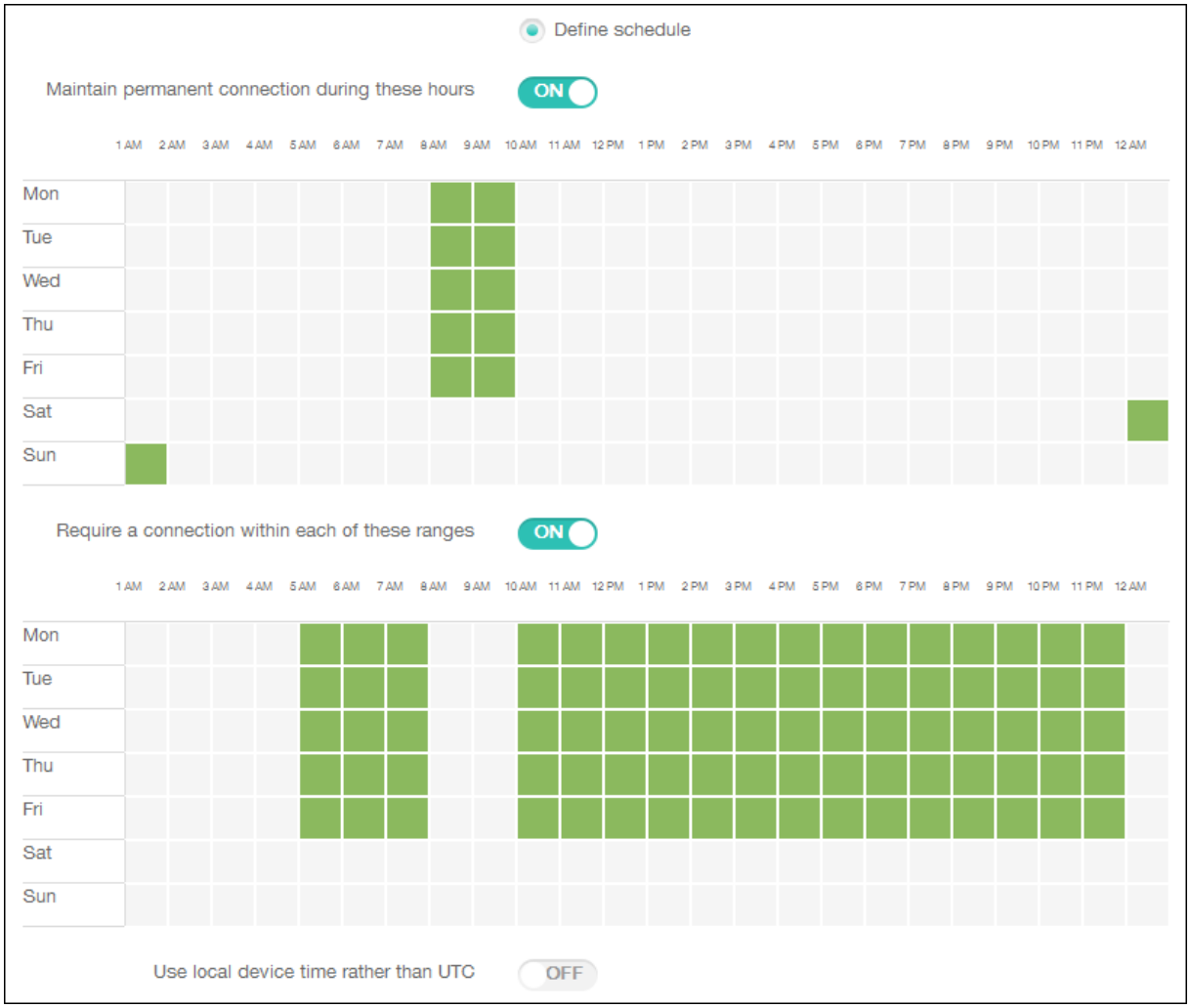
Définition d'un délai de connexion

Lorsque vous activez les options suivantes, un calendrier s'affiche dans lequel vous pouvez définir les délais souhaités. Vous pouvez activer l'une ou l'autre de ces options ou les deux options pour exiger une connexion permanente durant des heures spécifiques ou exiger une connexion dans des délais impartis. Chaque carré dans le calendrier correspond à 1 heure. Pour spécifier une connexion entre 8:00 AM et 9:00 AM chaque jour de la semaine, cliquez sur le carré sur le calendrier entre 8 AM et 9 AM chaque jour de la semaine.

Par exemple, les deux calendriers de la figure suivante nécessitent :

- Une connexion permanente entre 8h00 et 10h00 tous les jours de la semaine.
- Une connexion permanente entre 1h00 le samedi et 2h00 le dimanche.
- Au moins une connexion chaque jour de la semaine entre 5h00 et 8h00 ou entre 10h00 et 12h00.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Stratégie de contacts (CardDAV)

November 29, 2023

Vous pouvez ajouter une stratégie dans Citrix Endpoint Management afin d'ajouter un compte de contacts iOS (CalDAV) sur des appareils iOS ou macOS pour permettre à leurs utilisateurs de synchroniser les données de contact avec tout serveur qui prend en charge CalDAV.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Description du compte :** entrez une description du compte. Ce champ est obligatoire.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Nom d'hôte :** entrez l'adresse du serveur CardDAV. Ce champ est obligatoire.
- **Port :** entrez le port sur lequel se connecter au serveur CardDAV. Ce champ est obligatoire. La valeur par défaut est **8443**.
- **URL principale :** entrez l'adresse URL du calendrier de l'utilisateur.
- **Nom d'utilisateur :** entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe :** entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CardDAV. La valeur par défaut est **On**.
- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.

Paramètres macOS

- **Description du compte :** entrez une description du compte. Ce champ est obligatoire.
- **Nom d'hôte :** entrez l'adresse du serveur CardDAV. Ce champ est obligatoire.
- **Port :** entrez le port sur lequel se connecter au serveur CardDAV. Ce champ est obligatoire. La valeur par défaut est **8443**.
- **URL principale :** entrez l'adresse URL du calendrier de l'utilisateur.
- **Nom d'utilisateur :** entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe :** entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CardDAV. La valeur par défaut est **On**.
- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Stratégie XML personnalisée

November 29, 2023

Vous pouvez créer des stratégies XML personnalisées dans Citrix Endpoint Management pour personnaliser les fonctionnalités suivantes sur les appareils Windows pris en charge :

- Provisioning, qui comprend la configuration de l'appareil, et l'activation ou la désactivation de fonctionnalités.
- Configuration de l'appareil, ce qui permet aux utilisateurs de modifier les paramètres sur l'appareil.
- Mises à niveau logicielles, qui comprennent la mise à disposition de nouveaux logiciels ou de correctifs de bogues à charger sur l'appareil, y compris des applications et logiciels système.
- Gestion des pannes, ce qui comprend la réception de rapports d'erreur et d'état à partir de l'appareil.

> **Remarque :**
>
> Lorsque vous créez votre contenu XML, utilisez le caractère % avec prudence. Le caractère % est un caractère XML réservé, utilisé uniquement pour échapper les caractères spéciaux XML. Pour utiliser % dans un nom, encodez-le avec %25.

Pour les appareils Windows : vous créez votre propre configuration XML personnalisée à l'aide de l'API Open Mobile Alliance Device Management (OMA DM) dans Windows. La création de code XML personnalisé avec l'API OMA DM n'est pas couverte dans cette rubrique. Pour de plus amples informations sur l'utilisation de l'API OMA DM, veuillez consulter la section Prise en charge du protocole OMA DM sur le site de Microsoft Developer Network.

Pour les appareils Android Enterprise : vous créez la configuration XML personnalisée à l'aide du système de gestion MX (MXMS). La création de code XML personnalisé avec l'API MXMS n'est pas couverte dans cet article.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Windows Desktop/Tablet

Contenu XML : entrez, ou copiez et collez, le code XML personnalisé que vous souhaitez ajouter à la stratégie.

Une fois que vous avez cliqué sur **Suivant**, Citrix Endpoint Management vérifie la syntaxe du contenu XML. Les erreurs de syntaxe s'affichent en dessous de la zone de contenu. Vous devez résoudre les erreurs avant de continuer.

S'il n'existe pas d'erreurs de syntaxe, la page d'attribution de la **Stratégie XML personnalisée** s'affiche.

Utilisation de Windows AutoPilot pour installer et configurer les appareils

Windows AutoPilot est un ensemble de technologies utilisées pour configurer et pré-configurer de nouveaux appareils afin qu'ils soient prêts à une utilisation productive. Vous pouvez utiliser Windows AutoPilot pour réinitialiser, réutiliser et récupérer des appareils. AutoPilot permet de supprimer une partie de la complexité du déploiement de votre système d'exploitation actuel. L'utilisation d'AutoPilot réduit la tâche à un ensemble de paramètres et d'opérations simples, ce qui signifie que vos appareils peuvent être utilisés rapidement et efficacement.

Pour une brève présentation de l'utilisation de Windows AutoPilot avec Citrix Endpoint Management, regardez cette vidéo.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Conditions préalables

- Le branding de votre société est configuré dans le portail Azure Active Directory.
- La société dispose d'un abonnement Azure Active Directory Premium P1 ou P2.
- Configurer Azure Active Directory en tant que type de fournisseur d'identité pour Citrix Endpoint Management. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Fournisseur d'identité (IDP)**.
- Il existe une connectivité réseau aux services cloud utilisés par Windows AutoPilot.
- Les appareils sont préinstallés avec Windows 10 Professionnel, Entreprise ou Éducation (version 1703 ou ultérieure) ou Windows 11 Professionnel, Entreprise ou Éducation.
- Les appareils ont accès à Internet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour plus d'informations sur la configuration des prérequis, consultez la documentation Microsoft Windows sur AutoPilot : https://docs.microsoft.com.

Pour configurer le redéploiement automatique Windows dans Citrix Endpoint Management pour les appareils AutoPilot

1. Suivez les étapes pour ajouter une stratégie XML personnalisée dans la section Stratégie XML personnalisée. Ajoutez ce qui suit dans **Contenu XML :**

```
<Add>
<CmdID>\_cmdid\_</CmdID>
<Item>
<Target>
<LocURI>./Vendor/MSFT/Policy/Config/CredentialProviders/
   DisableAutomaticReDeploymentCredentials</LocURI>
</Target>
<Meta>
<Format xmlns="syncml:metinf">int</Format>
</Meta>
<Data>0</Data>
</Item>
</Add>

<!--NeedCopy-->
```

2. Sur l'écran de verrouillage Windows, entrez la combinaison de touches **CTRL + touche Windows + R**.
3. Ouvrez une session avec un compte Azure Active Directory.
4. L'appareil vérifie que l'utilisateur dispose des droits appropriés pour redéployer l'appareil. Le redéploiement de l'appareil a ensuite lieu.
5. Une fois l'appareil mis à jour avec la configuration AutoPilot, l'utilisateur peut se connecter à l'appareil récemment configuré.

Déployer un kiosque à application unique sur les appareils Windows 11

> **Remarque :**
>
> Les appareils Windows 11 ne prennent en charge que le mode kiosque à application unique.

Dans la zone de texte **Contenu XML**, copiez et collez le script XML suivant, puis remplacez les chaînes suivantes par vos paramètres :

- `your_username_here`(deux instances) : nom d'utilisateur que vous souhaitez créer sur l'appareil. Conservez les mêmes paramètres pour les deux instances.
- `your password_here` : mot de passe pour l'utilisateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `your_UWP_app_id_here` : AUMID pour l'application UMP que vous souhaitez déployer sur l'appareil.

Script XML :

```
<Add>
    <CmdID>\_cmdid\_</CmdID>
    <Item>
        <Target>
            <LocURI>./Device/Vendor/MSFT/Accounts/Users/your_username_here/Password</LocURI>
        </Target>
        <Meta>
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data>your_password_here</Data>
    </Item>
</Add>
<Replace>
    <CmdID>\_cmdid\_</CmdID>
    <Item>
        <Target>
            <LocURI>./Device/Vendor/MSFT/AssignedAccess/Configuration</LocURI>
        </Target>
        <Meta>
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data><![CDATA[<AssignedAccessConfiguration
        xmlns="http://schemas.microsoft.com/AssignedAccess/2017/config"
        xmlns:rs5="http://schemas.microsoft.com/AssignedAccess/201810/config">
            <Profiles>
                <Profile Id="{
 AFF9DA33-AE89-4039-B646-3A5706E92957 }
 ">
                    <KioskModeApp AppUserModelId="your_UWP_app_id_here" />
                </Profile>
            </Profiles>
            <Configs>
                <Config>
                    <Account>your_username_here</Account>
                    <DefaultProfile Id="{
 AFF9DA33-AE89-4039-B646-3A5706E92957 }
 "/>
                </Config>
            </Configs>
        </AssignedAccessConfiguration>]]></Data>
    </Item>
</Replace>
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

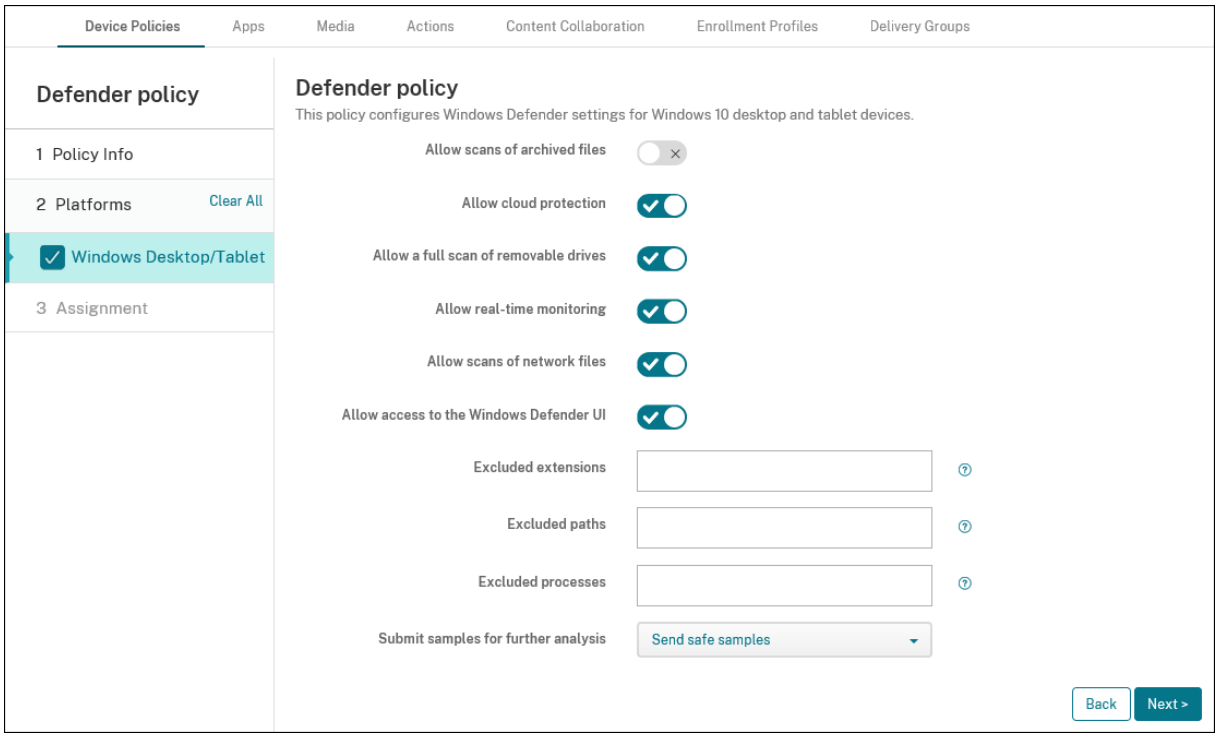
Stratégies d'appareil Defender

November 29, 2023

Windows Defender est une protection contre les logiciels malveillants intégrée à Windows 10 et Windows 11. Vous pouvez utiliser la stratégie d'appareil Citrix Endpoint Management, Defender, pour configurer la stratégie Microsoft Defender pour les appareils Windows 10 et Windows 11 Desktop et Tablet.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Windows Desktop et Tablet



- **Autoriser analyse des fichiers archivés :** autorise ou bloque Defender à analyser les fichiers archivés. La valeur par défaut est **Désactivé**.
- **Autoriser protection du cloud :** autorise ou bloque Defender à envoyer des informations relatives aux activités de logiciels malveillants à Microsoft. La valeur par défaut est **Activé**.
- **Autoriser analyse complète des lecteurs amovibles :** autorise ou bloque Defender à analyser les lecteurs amovibles tels que les clés USB. La valeur par défaut est **Activé**.
- **Autoriser surveillance en temps réel :** la valeur par défaut est **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Autoriser analyse des fichiers réseau :** autorise ou bloque Defender à analyser les fichiers réseau. La valeur par défaut est **Activé**.
- **Autoriser accès à l'interface de Windows Defender :** indique si les utilisateurs peuvent accéder à l'interface utilisateur de Windows Defender. Ce paramètre prend effet au prochain démarrage de l'appareil utilisateur. Si ce paramètre est défini sur **Désactivé**, les utilisateurs ne reçoivent aucune notification de Windows Defender. La valeur par défaut est **Activé**.
- **Extensions exclues :** les extensions à exclure des analyses en temps réel ou programmées. Pour séparer les extensions, utilisez le caractère `|`. Par exemple, `lib\|obj`.
- **Chemins d'accès exclus :** les chemins à exclure des analyses en temps réel ou programmées. Pour séparer les chemins, utilisez le caractère `|`. Par exemple, `C:\Example|C:\Example1`.
- **Processus exclus :** les processus à exclure des analyses en temps réel ou programmées. Pour séparer les processus, utilisez le caractère `|`. Par exemple, `C:\Example.exe|C:\Example1.exe`.
- **Envoyer des échantillons pour une analyse plus approfondie :** permet de spécifier si vous souhaitez envoyer à Microsoft des fichiers qui peuvent nécessiter une analyse plus approfondie pour déterminer s'ils sont malveillants. Options : **Toujours demander**, **Envoyer des échantillons sécurisés**, **Ne jamais envoyer**, **Envoyer tous les échantillons**. La valeur par défaut est **Envoyer des échantillons sécurisés**.

Stratégie Device Guard

November 29, 2023

Device Guard est une fonctionnalité de sécurité disponible avec Windows 10 et Windows 11. Cette fonctionnalité permet d'activer la sécurité basée sur la virtualisation à l'aide de l'hyperviseur Windows pour prendre en charge des services de sécurité sur l'appareil. La stratégie Device Guard vous permet d'activer des fonctionnalités de sécurité telles que le démarrage sécurisé, le verrouillage UEFI et la virtualisation.

Conditions préalables

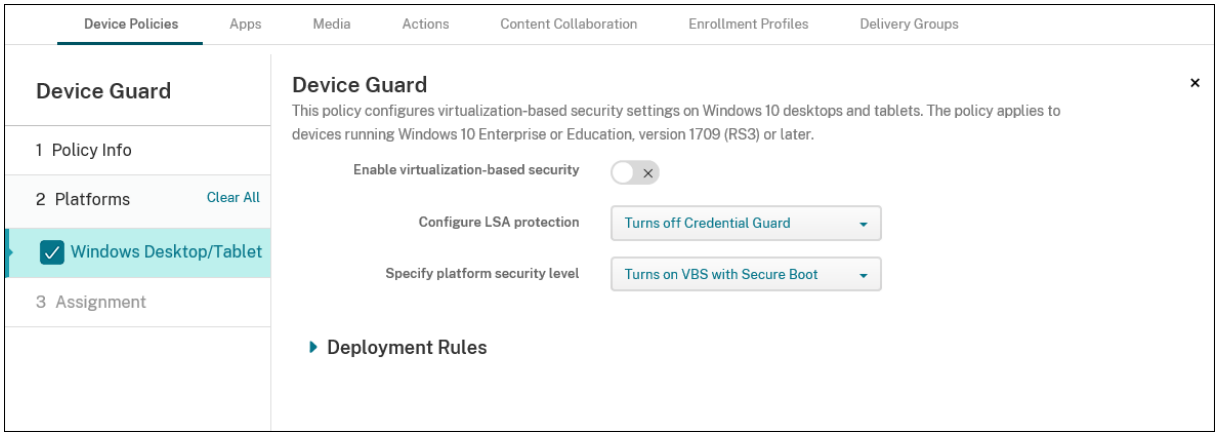
- Bureaux et tablettes Windows 10 et Windows 11 avec une licence Entreprise ou Éducation
- Device Guard activé dans Windows

  Pour plus d'informations sur Device Guard, consultez la section https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-manage.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Windows Desktop et Tablet



- **Activer la sécurité basée sur la virtualisation :** permet de désactiver ou d'activer les fonctionnalités de sécurité basées sur la virtualisation. La sécurité basée sur la virtualisation utilise l'hyperviseur Windows pour prendre en charge les services de sécurité.
- **Configurer la protection LSA :** permet de configurer Credential Guard. Ce paramètre permet aux utilisateurs d'activer Credential Guard avec une sécurité basée sur la virtualisation pour protéger les informations d'identification au prochain redémarrage. Les options sont **Désactive Credential Guard**, **Active Credential Guard avec le verrouillage UEFI** et **Active Credential Guard sans le verrouillage UEFI**. La valeur par défaut est **Désactive Credential Guard**.
- **Spécifier le niveau de sécurité de la plate-forme** : permet de spécifier le niveau de sécurité de la plate-forme lors du prochain redémarrage. Les options sont **Active VBS avec Démarrage sécurisé** et **Active VBS avec Démarrage sécurisé et accès direct à la mémoire**. La valeur par défaut est **Active VBS avec Démarrage sécurisé**.

Citrix Endpoint Management interroge un appareil pour déterminer si les paramètres de sécurité basés sur la virtualisation correspondent aux paramètres du serveur. Si les paramètres de sécurité correspondent, Citrix Endpoint Management ne déploie pas cette stratégie sur l'appareil. Si les paramètres de sécurité ne correspondent pas, Citrix Endpoint Management déploie la stratégie.

Stratégie d'attestation de l'intégrité des appareils

November 29, 2023

Dans Citrix Endpoint Management, vous pouvez exiger que les appareils Windows 10 et Windows 11 signalent l'état de leur intégrité. Pour signaler l'état de leur intégrité, les appareils envoient des informations d'exécution et des données spécifiques au service d'attestation de l'intégrité (HAS) pour analyse. Le service HAS crée et renvoie un certificat d'attestation d'intégrité que l'appareil envoie

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ensuite à Citrix Endpoint Management. Citrix Endpoint Management utilise le contenu du certificat d'attestation d'intégrité pour déployer les actions automatiques que vous avez configurées.

Les données vérifiées par le service HAS sont les suivantes :

- AIK présent ?
- État BitLocker
- Débogage du démarrage activé ?
- Version de la liste de révision du Gestionnaire de démarrage
- Intégrité du code activée ?
- Version de la liste de révision d'intégrité du code
- Stratégie du programme de déploiement d'Apple
- Pilote ELAM chargé ?
- Date d'émission
- Débogage du noyau activé ?
- PCR
- Nombre de réinitialisations
- Nombre de redémarrages
- Mode sans échec activé ?
- Hachage SBCP
- Démarrage sécurisé activé ?
- Signature du test activée ?
- VSM activé ?
- WinPE activé ?

Pour de plus amples informations, reportez-vous à la page Device HealthAttestation CSP de Microsoft.

Vous pouvez configurer DHA à l'aide de Microsoft Cloud ou d'un serveur Windows DHA sur site, comme suit :

- Pour configurer DHA à l'aide de Microsoft Cloud : ajoutez une stratégie d'attestation de l'intégrité des appareils et configurez-la comme décrit dans cet article.
- Pour configurer DHA à l'aide d'un serveur Windows DHA sur site : Configurer un serveur DHA. Ensuite, ajoutez une stratégie d'attestation de l'intégrité des appareils et configurez-la comme décrit dans cet article.

  Pour configurer un serveur DHA, installez le rôle de serveur DHA sur une machine exécutant Windows Server 2016 Technical Preview 5 ou version ultérieure. Pour obtenir des instructions, consultez la section sur la configuration d'un serveur d'attestation de l'intégrité des appareils sur site.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Windows Desktop/Tablet

Si vous configurez DHA à l'aide de Microsoft Cloud

- **Activer l'attestation de l'intégrité des appareils :** sélectionnez cette option pour exiger l'attestation de l'intégrité des appareils. La valeur par défaut est **Off**.

Si vous configurez DHA à l'aide d'un serveur Windows DHA sur site

- **Activer l'attestation de l'intégrité des appareils :** réglez sur **Activé**.
- **Configurer Health Attestation Service sur site :** réglez sur **Activé**.
- **FQDN du serveur DHA sur site :** entrez le nom de domaine complet du serveur DHA que vous avez configuré.
- **Version de l'API DHA sur site :** sélectionnez la version du service DHA installé sur le serveur DHA.

Stratégie de nom d'appareil

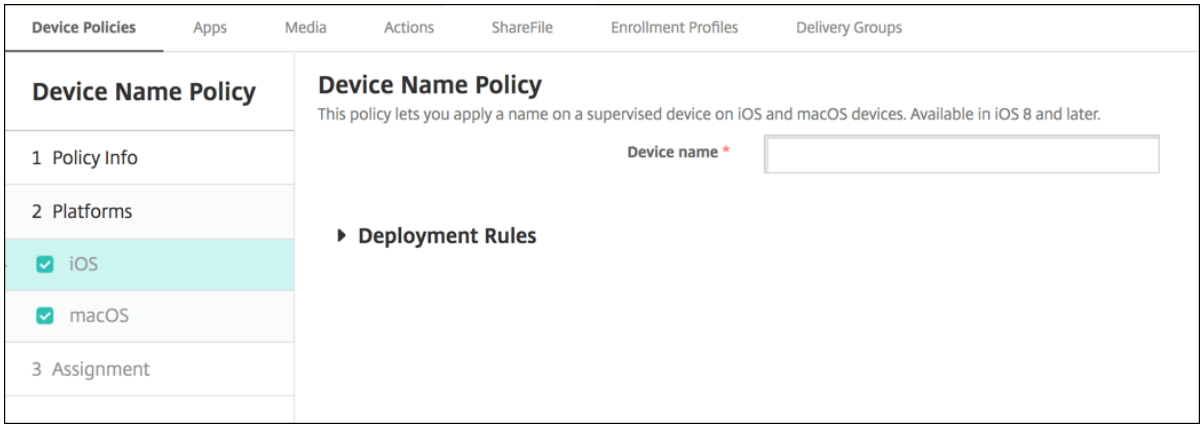
November 29, 2023

Vous pouvez définir les noms sur des appareils iOS et macOS, ce qui vous permet d'identifier facilement les appareils. Vous pouvez utiliser des macros et du texte, ou une combinaison des deux pour définir le nom de l'appareil. Par exemple, pour définir le nom de l'appareil à partir du numéro de série de l'appareil, vous devez utiliser ${device.serialnumber}. Pour définir le nom de l'appareil comme la combinaison du nom d'utilisateur et de votre domaine, vous devez utiliser ${user.username}@exemple.com. Pour de plus amples informations sur les macros, consultez la section Macros dans Citrix Endpoint Management.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres iOS et macOS



- **Nom de l'appareil :** entrez la macro, une combinaison de macros, ou une combinaison de macros et de texte pour donner un nom unique à chaque appareil. Par exemple, utilisez ${device.serialnumber} pour définir les noms d'appareil selon leur numéro de série ou utilisez ${device.serialnumber} ${user.username} pour inclure l'identifiant Apple ID de l'utilisateur dans le nom de l'appareil.

Stratégie Configuration de l'éducation

November 29, 2023

La stratégie Configuration de l'éducation définit les éléments suivants :

- Les paramètres de l'application En classe d'Apple pour les appareils des enseignants.
- Les certificats utilisés pour effectuer l'authentification du client entre les appareils des enseignants et des élèves.

La stratégie Configuration de l'éducation est prise en charge pour les appareils iOS (iPadOS).

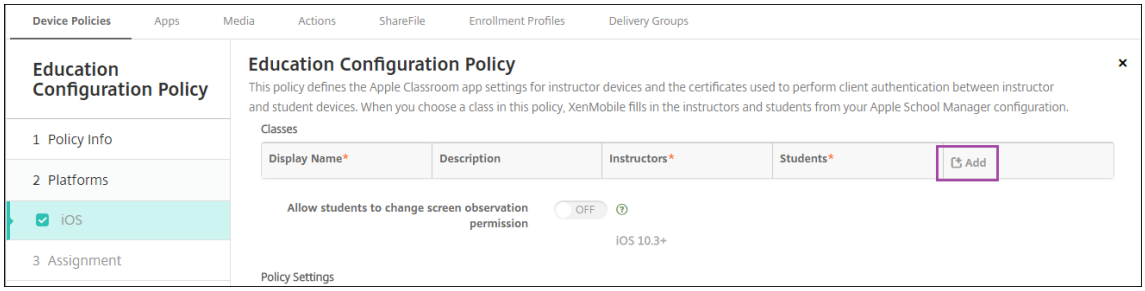
Lorsque vous choisissez une classe dans cette stratégie, la console Citrix Endpoint Management renseigne les enseignants et les élèves à partir de votre configuration Apple School Manager. Créez une seule stratégie si les paramètres de l'application En salle d'Apple dans cette stratégie sont les mêmes pour toutes les classes.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

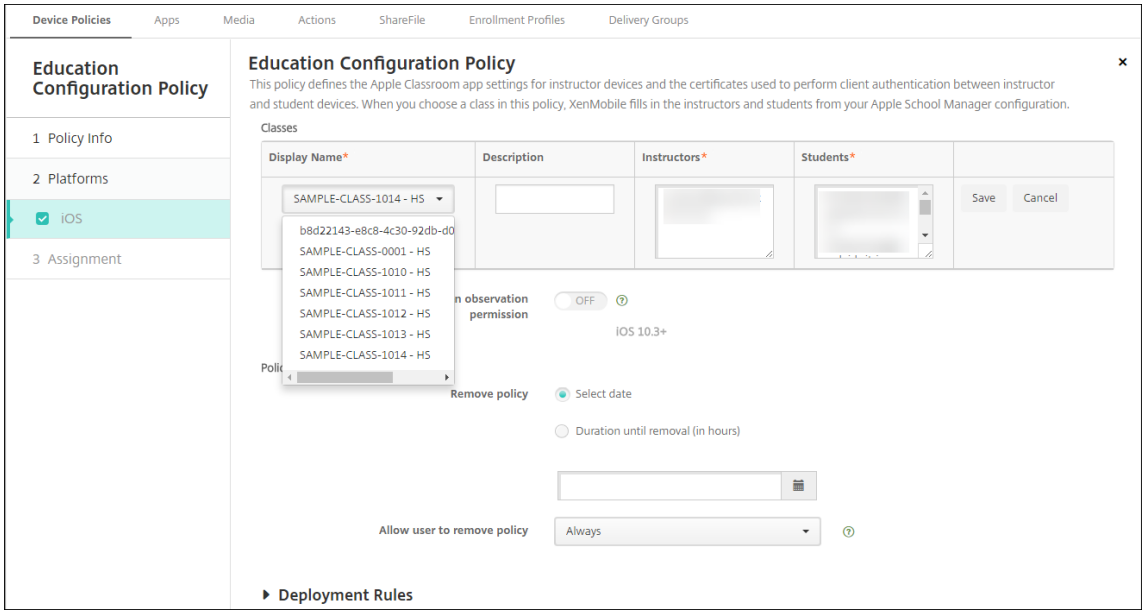
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres iOS

- **Classes :** pour ajouter une classe, cliquez sur **Ajouter**.

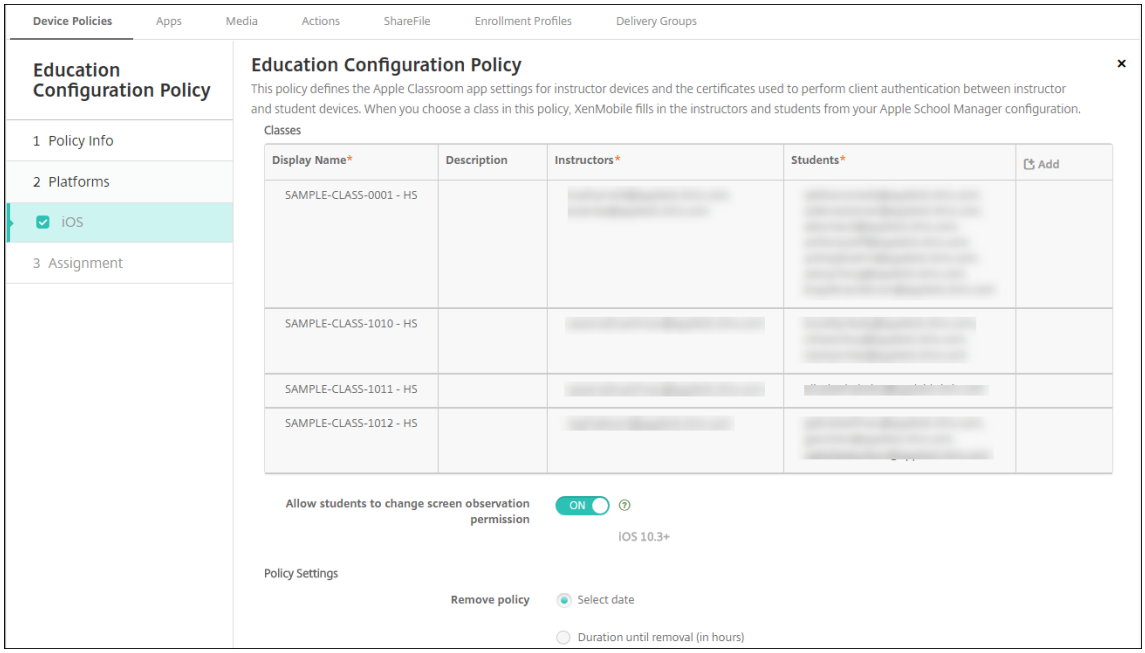


Cliquez ensuite sur la liste **Nom d'affichage**. Une liste des classes obtenue à partir de votre compte Apple School Manager connecté s'affiche.



Lorsque vous choisissez une classe dans **Nom d'affichage**, Citrix Endpoint Management renseigne les enseignants et les élèves. Continuez d'ajouter des classes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



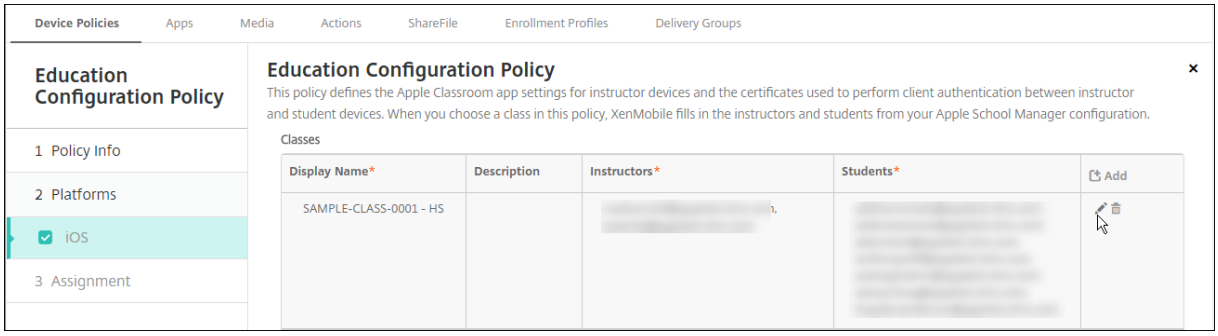
- **Autoriser les étudiants à modifier les autorisations d'observation de l'écran :** si cette option est **activée**, les étudiants inscrits dans les classes gérées peuvent choisir d'autoriser leur enseignant à observer les écrans de leurs appareils. La valeur par défaut est **Off**.
- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.

Pour modifier les informations de classe dans la stratégie

Vous pouvez ajouter une description à une classe (« Nom d'affichage » dans l'application En classe). Vous pouvez également ajouter ou supprimer des enseignants et des étudiants. Citrix Endpoint Management n'enregistre pas de telles modifications sur votre compte Apple School Manager. Pour plus d'informations, consultez la section « Gérer les données d'enseignants, d'élèves et de classe » dans Intégration avec les fonctionnalités Apple Éducation.

Placez la souris sur la colonne **Ajouter** pour la classe que vous souhaitez modifier, puis cliquez sur l'icône de crayon.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pour supprimer une classe de la stratégie, placez la souris sur la colonne **Ajouter** pour la classe que vous souhaitez supprimer, puis cliquez sur l'icône de corbeille.

Stratégie Options Endpoint Management

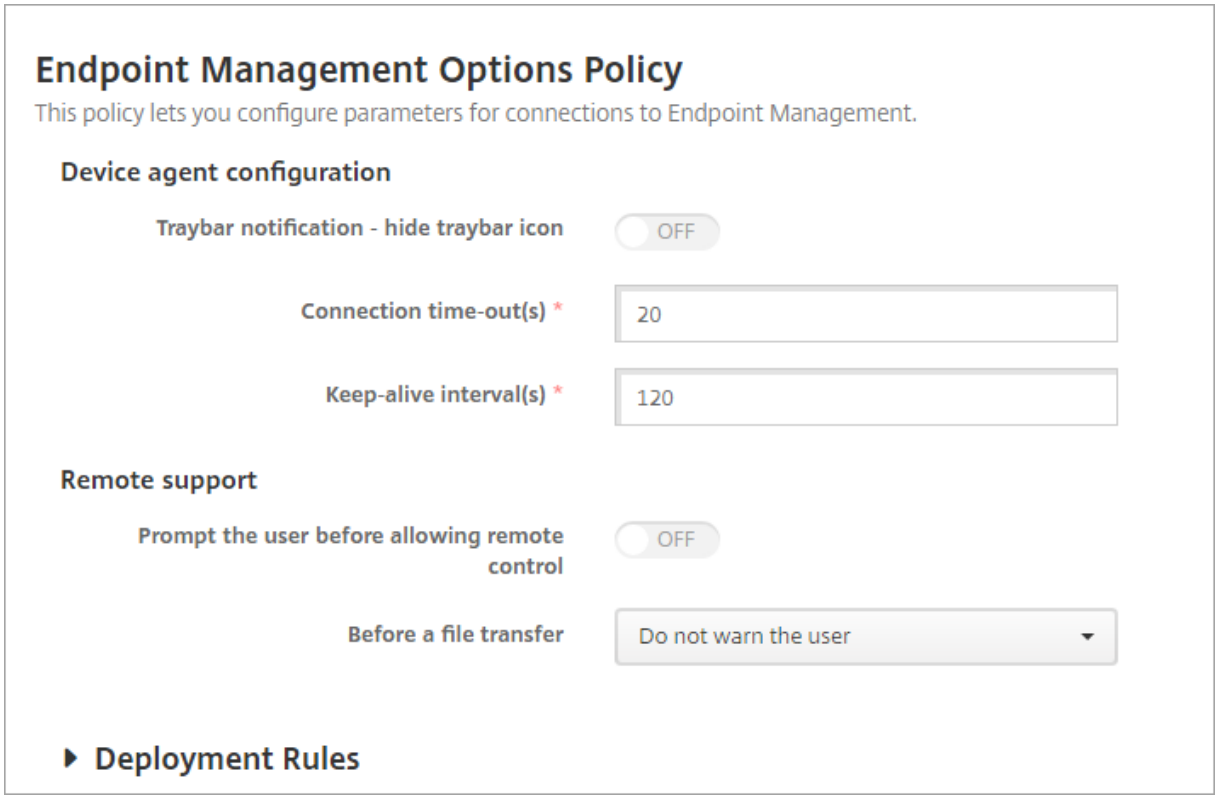
March 1, 2024

Vous ajoutez une stratégie d'options Endpoint Management pour configurer le comportement de Citrix Secure Hub lors de la connexion à Citrix Endpoint Management à partir d'appareils Android.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

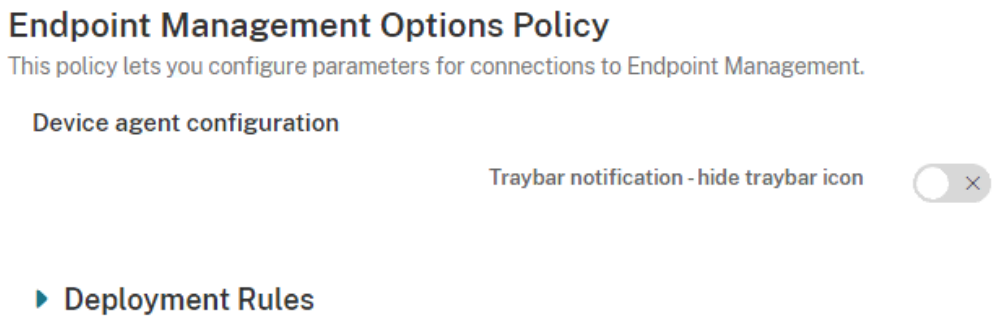
Paramètres Android



- **Zone de notification - icône masquer la zone de notification :** sélectionnez cette option pour spécifier si l'icône de la zone de notification est masquée ou visible. La valeur par défaut est **Désactivé**.
- **Délai d'expiration des connexions :** entrez la durée en secondes pendant laquelle une connexion peut rester inactive avant expiration de la connexion. La durée par défaut est de 20 secondes.
- **Intervalles de persistance des connexions :** entrez la durée en secondes pendant laquelle maintenir une connexion ouverte. La durée par défaut est de 120 secondes.
- **Demander à l'utilisateur avant d'autoriser le contrôle à distance :** indiquez si une invite s'affiche avant d'autoriser le contrôle à distance. La valeur par défaut est **Désactivé**.
- **Avant un transfert de fichiers :** dans la liste, cliquez pour informer l'utilisateur d'un transfert de fichiers ou pour lui demander l'autorisation. Valeurs disponibles : **Ne pas prévenir l'utilisateur**, **Prévenir l'utilisateur** et **Demander à l'utilisateur**. La valeur par défaut est **Ne pas prévenir l'utilisateur**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Android Enterprise



Prise en charge à partir de la version 7 d'Android.

Zone de notification - icône masquer la zone de notification : sélectionnez cette option pour spécifier si l'icône de la zone de notification est masquée ou visible. La valeur par défaut est **Désactivé**.

> **Remarque :**
>
> Si vous souhaitez activer le service VPN pour les appareils fonctionnant sur Android Enterprise, vous pouvez activer l'option **Activer VPN Always On** dans la **Stratégie VPN**. Si vous avez déjà activé l'option **Activer VPN Always On** dans la **Stratégie Options Endpoint Management** dans une version précédente, assurez-vous de l'activer à nouveau dans la **Stratégie VPN**.

Stratégie Désinstallation de Citrix Endpoint Management

November 29, 2023

Vous pouvez ajouter une stratégie dans Citrix Endpoint Management afin de désinstaller Citrix Endpoint Management des appareils Android. Lorsqu'elle est déployée, cette stratégie supprime Citrix Endpoint Management sur tous les appareils du déploiement.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Android

- **Désinstaller Citrix Endpoint Management des appareils :** sélectionnez cette option pour désinstaller Citrix Endpoint Management de chaque appareil sur lequel vous déployez cette

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

stratégie. La valeur par défaut est **Off**.

Stratégie Exchange

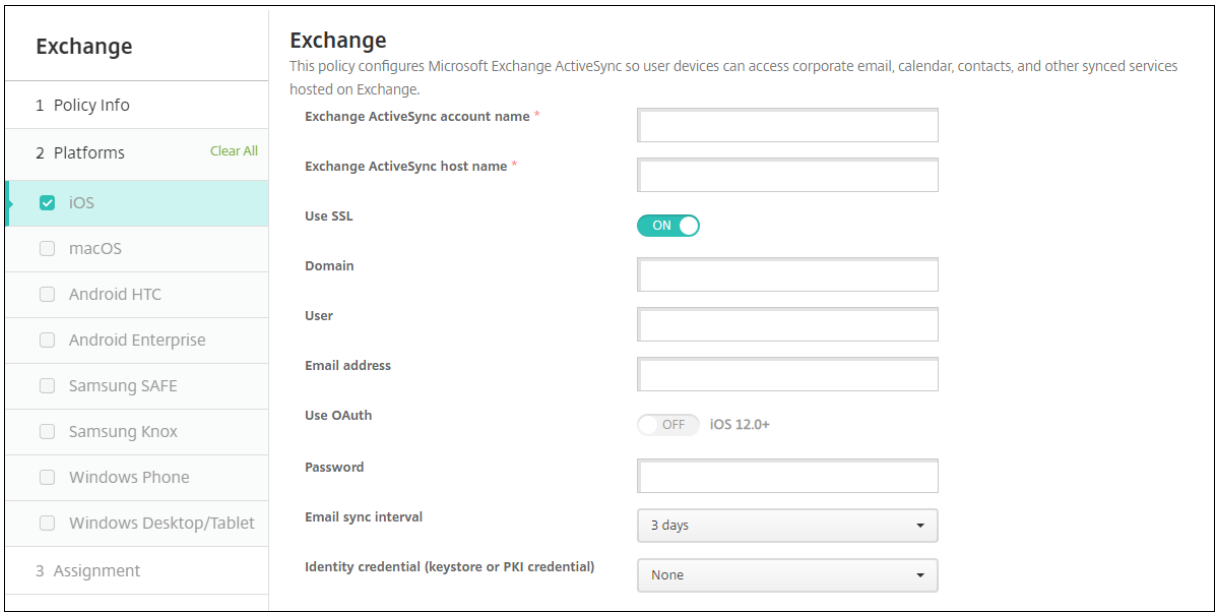
March 1, 2024

Vous pouvez utiliser la stratégie Exchange ActiveSync pour configurer un client de messagerie sur les appareils des utilisateurs pour leur permettre d'accéder à leur messagerie d'entreprise hébergée sur Exchange. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans les sections suivantes.

Pour créer cette stratégie, vous avez besoin du nom d'hôte ou de l'adresse IP du serveur Exchange. Pour plus d'informations sur les paramètres ActiveSync, consultez l'article Microsoft ActiveSync CSP.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Nom du compte Exchange ActiveSync :** entrez la description du compte de messagerie qui est affichée sur les appareils des utilisateurs.
- **Nom d'hôte Exchange ActiveSync :** entrez l'adresse du serveur de messagerie.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Utiliser SSL :** sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et le serveur Exchange. La valeur par défaut est **Activé**.
- **Domaine :** entrez le domaine dans lequel réside le serveur Exchange. vous pouvez utiliser la macro système `$user.domainname` dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
- **Utilisateur :** spécifiez le nom d'utilisateur du compte utilisateur Exchange. vous pouvez utiliser la macro système `$user.username` dans ce champ pour rechercher automatiquement les noms des utilisateurs.
- **Adresse e-mail :** spécifiez l'adresse e-mail complète. vous pouvez utiliser la macro système `$user.mail` dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Utiliser OAuth :** si cette option est définie sur **Activé**, la connexion utilise OAuth pour l'authentification. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
- **Mot de passe :** entrez un mot de passe pour le compte utilisateur Exchange. Ce paramètre n'apparaît pas lorsque **Utiliser OAuth** est **activé**.
- **Intervalle de synchronisation des e-mails :** dans la liste, choisissez la fréquence de synchronisation des e-mails avec Exchange Server. La valeur par défaut est **3 jours**.
- **Infos d'identification de l'identité (PKI ou keystore)** : dans la liste, cliquez sur des informations d'identification de l'identité si vous avez configuré un fournisseur d'identités pour Citrix Endpoint Management. Ce champ est requis uniquement lorsque Exchange requiert l'authentification du certificat client. La valeur par défaut est **Aucun**.
- **Autoriser le déplacement des e-mails entre les comptes :** sélectionnez cette option pour permettre aux utilisateurs de :
  - déplacer un e-mail de ce compte vers un autre
  - transférer un e-mail à partir d'un autre compte
  - répondre à partir d'un compte différent

  La valeur par défaut est **Désactivé**.
- **N'envoyer le courrier que depuis l'application de messagerie :** sélectionnez cette option si vous voulez que les utilisateurs soient uniquement autorisés à envoyer des e-mails avec l'application de messagerie iOS. La valeur par défaut est **Désactivé**.
- **Empêcher les utilisateurs de synchroniser les adresses récentes :** sélectionnez cette option pour empêcher les utilisateurs de synchroniser les adresses récentes. La valeur par défaut est **Désactivé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Autoriser Mail Drop :** sélectionnez cette option pour autoriser le compte à utiliser Mail Drop. La valeur par défaut est **Désactivé**.
- **Activer signature S/MIME :** indiquez si ce compte prend en charge la signature S/MIME. La valeur par défaut est **Activé**. Lorsque la valeur est définie sur **Activé**, les champs suivants apparaissent.
  - **Informations d'identification de l'identité de signature :** choisissez les informations d'identification de signature à utiliser.
  - **L'utilisateur peut remplacer la signature S/MIME :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer et désactiver la signature S/MIME dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
  - **L'utilisateur peut remplacer l'UUID du certificat de signature S/MIME :** si cette option est définie sur **Activé**, les utilisateurs peuvent sélectionner les informations d'identification de signature à utiliser dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
- **Activer chiffrement S/MIME :** sélectionnez cette option si vous souhaitez que ce compte prenne en charge le chiffrement S/MIME. La valeur par défaut est **Désactivé**. Lorsque la valeur est définie sur **Activé**, les champs suivants apparaissent.
  - **Informations d'identification de l'identité de chiffrement :** dans la liste, sélectionnez les informations d'identification de chiffrement à utiliser.
  - **Activer commutateur de chiffrement S/MIME par message :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer ou désactiver le chiffrement S/MIME pour chaque message composé. La valeur par défaut est **Désactivé**.
  - **L'utilisateur peut remplacer le chiffrement S/MIME :** si cette option est définie sur **Activé**, les utilisateurs peuvent choisir si S/MIME est activé par défaut dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
  - **L'utilisateur peut remplacer l'UUID du certificat de chiffrement S/MIME :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer et désactiver l'identité de chiffrement S/MIME dans les paramètres de leurs appareils. La valeur par défaut est **Désactivé**. Cette option s'applique à iOS 12.0 et versions ultérieures.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

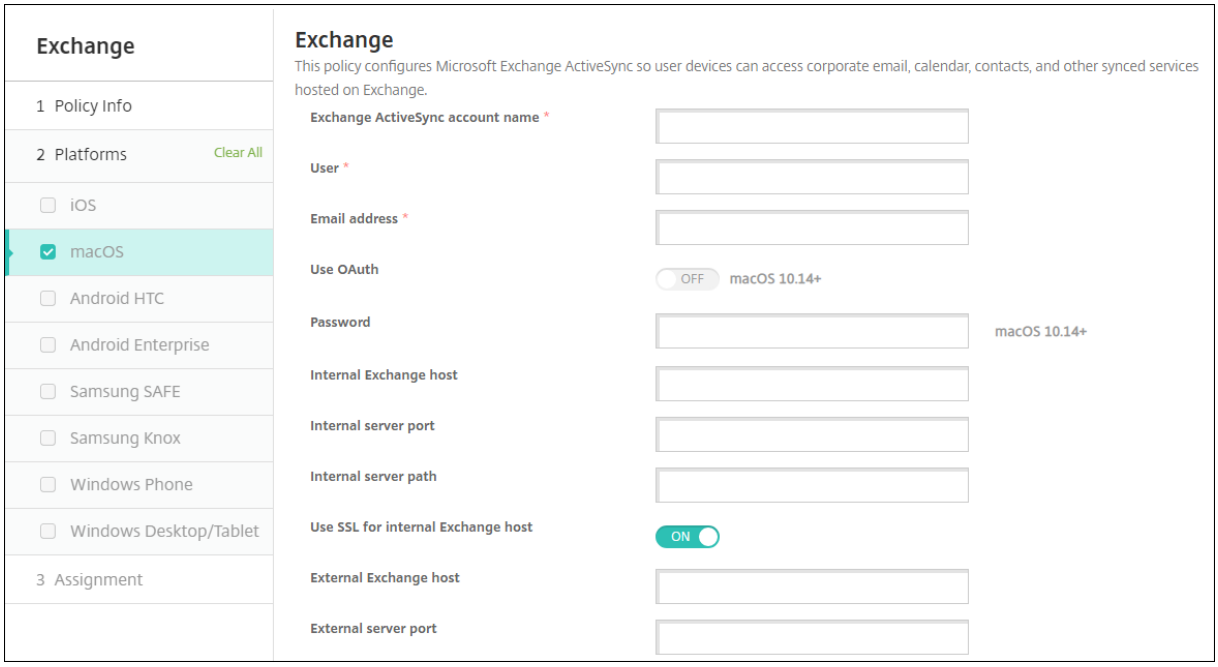
* **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.

Services Exchange synchronisés

Les paramètres des services Exchange synchronisés vous permettent de choisir de synchroniser ou non les fonctionnalités suivantes :

- Calendriers
- Contacts
- E-mail
- Remarques
- Rappels

Paramètres macOS



- **Nom du compte Exchange ActiveSync :** entrez la description du compte de messagerie qui est affichée sur les appareils des utilisateurs.
- **Utilisateur :** spécifiez le nom d'utilisateur du compte utilisateur Exchange. vous pouvez utiliser la macro système `$user.username` dans ce champ pour rechercher automatiquement les noms des utilisateurs.
- **Adresse e-mail :** spécifiez l'adresse e-mail complète. vous pouvez utiliser la macro système `$user.mail` dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.

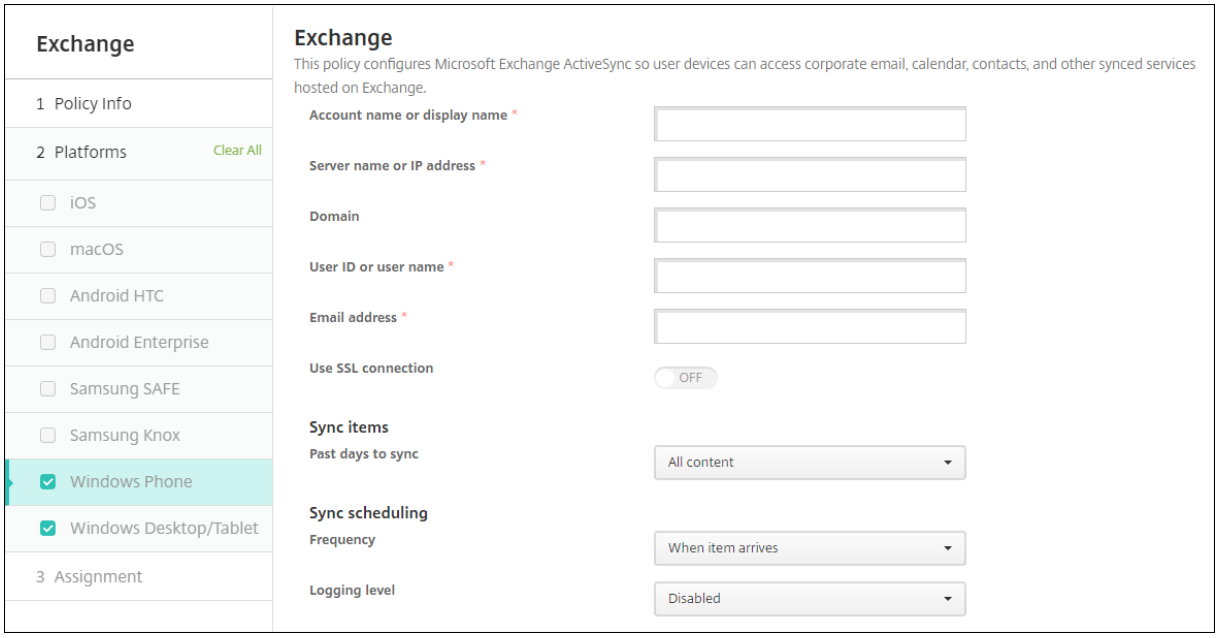
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Utiliser OAuth :** si cette option est définie sur **Activé**, la connexion utilise OAuth pour l'authentification. La valeur par défaut est **Désactivé**. Cette option s'applique à macOS 10.14 et versions ultérieures.
- **URL d'authentification OAuth :** spécifie l'URL à charger dans un affichage Web pour l'authentification via OAuth lorsque la détection automatique n'est pas utilisée. Ce champ apparaît lorsque **Utiliser OAuth** est défini sur **Activé**.
- **Mot de passe :** entrez un mot de passe pour le compte utilisateur Exchange. Ce paramètre n' apparaît pas lorsque **Utiliser OAuth** est **activé**.
- **Hôte Exchange interne :** si vous voulez que vos noms d'hôte Exchange interne et externe soient différents, tapez un nom d'hôte Exchange interne (facultatif).
- **Port du serveur interne :** si vous voulez que vos ports de serveur Exchange interne et externe soient différents, tapez un numéro de port Exchange interne (facultatif).
- **Chemin d'accès au serveur interne :** si vous voulez que vos chemins d'accès au serveur Exchange interne et externe soient différents, tapez un chemin d'accès au serveur Exchange interne (facultatif).
- **Utiliser SSL pour l'hôte Exchange interne :** sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et l'hôte Exchange interne. La valeur par défaut est **Activé**.
- **Hôte Exchange externe :** si vous voulez que vos noms d'hôte Exchange interne et externe soient différents, tapez un nom d'hôte Exchange externe (facultatif).
- **Port du serveur externe :** si vous voulez que vos ports de serveur Exchange interne et externe soient différents, tapez un numéro de port Exchange externe (facultatif).
- **Chemin d'accès au serveur externe :** si vous voulez que vos chemins d'accès au serveur Exchange interne et externe soient différents, tapez un chemin d'accès au serveur Exchange externe (facultatif).
- **Utiliser SSL pour l'hôte Exchange externe :** sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et l'hôte Exchange interne. La valeur par défaut est **Activé**.
- **Autoriser Mail Drop :** sélectionnez cette option pour permettre aux utilisateurs de partager sans fil des fichiers entre deux Mac, sans avoir à se connecter à un réseau existant. La valeur par défaut est **Désactivé**.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
- **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
- **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Paramètres Windows Desktop/Tablet



> **Remarque :**
>
> Cette stratégie ne vous permet pas de définir le mot de passe utilisateur. Les utilisateurs doivent définir ce paramètre à partir de leurs appareils après transmission de la stratégie.

- **Nom du compte ou nom d'affichage :** entrez le nom du compte Exchange ActiveSync.
- **Nom du serveur ou adresse IP :** entrez le nom d'hôte ou l'adresse IP du serveur Exchange.
- **Domaine :** entrez le domaine dans lequel réside le serveur Exchange. vous pouvez utiliser la macro système `$user.domainname` dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
- **ID utilisateur ou nom d'utilisateur :** spécifiez le nom d'utilisateur du compte utilisateur

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exchange. vous pouvez utiliser la macro système `$user.username` dans ce champ pour rechercher automatiquement les noms des utilisateurs.

- **Adresse e-mail :** spécifiez l'adresse e-mail complète. vous pouvez utiliser la macro système `$user.mail` dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Utiliser une connexion SSL :** sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et le serveur Exchange. La valeur par défaut est **Désactivé**.
- **Contenu à synchroniser :** dans la liste, cliquez sur le nombre de jours à prendre en compte pour synchroniser tout le contenu de l'appareil avec le serveur Exchange. Le paramètre par défaut est **Tout le contenu**.
- **Périodicité :** dans la liste, cliquez sur le calendrier à utiliser lors de la synchronisation des données envoyées à partir du serveur Exchange. La valeur par défaut est **À la réception d'un e-mail**.
- **Niveau d'enregistrement :** dans la liste, cliquez sur **Désactivé**, **De base** ou **Avancé** pour spécifier le niveau de détail lors de la journalisation des activités Exchange. La valeur par défaut est **Désactivé**.

Stratégie de fichiers

November 4, 2022

Vous pouvez ajouter et déployer des fichiers auxquels les utilisateurs peuvent accéder sur leurs appareils Android et Android Enterprise. Vous spécifiez le répertoire dans lequel vous souhaitez stocker le fichier sur l'appareil. Par exemple, vous souhaitez que les utilisateurs reçoivent un document ou un fichier .pdf d'entreprise. Déployez le fichier sur les appareils et informez les utilisateurs de son emplacement.

Les appareils Android ne prennent pas en charge l'exécution de scripts en mode natif. Les utilisateurs ont besoin d'un logiciel tiers pour exécuter des scripts.

Vous pouvez ajouter les types de fichiers suivants avec cette stratégie :

- Fichiers texte (.xml, .html, .py, etc.)
- Autres fichiers tels que des documents, images, feuilles de calcul ou présentations

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Android Enterprise

- **Fichier à importer :** pour sélectionner le fichier à importer, cliquez sur **Parcourir** et accédez à l'emplacement du fichier.
- **Dossier de destination :** dans la liste, sélectionnez l'emplacement où vous souhaitez stocker le fichier chargé ou sélectionnez **Ajouter** pour spécifier un emplacement de fichier. Sélectionnez la macro `%Flash Storage%\` ou `%XenMobile Storage%\` pour indiquer où stocker le fichier chargé. La macro s'étend à l'emplacement applicable sur chaque appareil.
  - `%XenMobile Storage%\` s'étend à `Android/data/com.zenprise/` dans le répertoire de stockage interne.
  - Pour Android 9.0 et versions antérieures, `%Flash Storage%\` enregistre le fichier dans le répertoire de stockage externe.
  - Pour Android 10.0 et versions ultérieures, `%Flash Storage%\` enregistre le fichier dans le dossier **Téléchargements** du répertoire de stockage interne.
  - Pour Android 11.0 et versions ultérieures, `%XenMobile Storage%\` ne s'applique plus en raison des restrictions imposées par Google sur l'accès à l'emplacement cible.
- **Nom du fichier de destination :** facultatif. Si vous devez modifier un nom de fichier avant de le déployer sur un appareil, tapez le nom du fichier.
- **Si le fichier existe :** dans la liste, indiquez si vous souhaitez copier un fichier existant. La valeur par défaut est **Copier le fichier s'ils sont différents**.

> **Important :**
>
> la stratégie Fichiers ne prend plus en charge l'ajout de scripts sur Android Enterprise. Si une stratégie existante contient un script, un message d'erreur s'affiche lors de la sélection de la stratégie, et vous pouvez ajouter à nouveau la stratégie pour résoudre le problème.

Paramètres Android

- **Fichier à importer :** pour sélectionner le fichier à importer, cliquez sur **Parcourir** et accédez à l'emplacement du fichier.
- **Type de fichier :** sélectionnez **Fichier** ou **Script**.
- **Exécuter immédiatement :** lorsque vous sélectionnez **Script**, l'option **Exécuter immédiatement** apparaît. Rien ne se produit lorsque vous activez ce paramètre. Les utilisateurs doivent exécuter le script manuellement.
- **Substituer les macros :** sélectionnez cette option si vous voulez remplacer les noms des jetons de macro dans un script avec une propriété d'appareil ou d'utilisateur. Pour connaître la syntaxe des macros, reportez-vous à la section Macros. La valeur par défaut est **Désactivé**.
- **Dossier de destination :** dans la liste, sélectionnez l'emplacement où vous souhaitez stocker le fichier chargé ou sélectionnez **Ajouter** pour spécifier un emplacement de fichier. Sélectionnez

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

la macro `%Flash Storage%\` ou `%XenMobile Storage%\` pour indiquer où stocker le fichier chargé. La macro s'étend à l'emplacement applicable sur chaque appareil.

  - `%XenMobile Storage%\` s'étend à `Android/data/com.zenprise/` dans le répertoire de stockage interne.
  - Pour Android 9.0 et versions antérieures, `%Flash Storage%\` enregistre le fichier dans le répertoire de stockage externe.
  - Pour Android 10.0 et versions ultérieures, `%Flash Storage%\` enregistre le fichier dans le dossier **Téléchargements** du répertoire de stockage interne.
  - Pour Android 11.0 et versions ultérieures, `%XenMobile Storage%\` ne s'applique plus en raison des restrictions imposées par Google sur l'accès à l'emplacement cible.

- **Nom du fichier de destination :** facultatif. Si vous devez modifier un nom de fichier avant de le déployer sur un appareil, tapez le nom du fichier.
- **Si le fichier existe :** dans la liste, indiquez si vous souhaitez copier un fichier existant. La valeur par défaut est **Copier le fichier s'ils sont différents**.

Stratégie FileVault

November 29, 2023

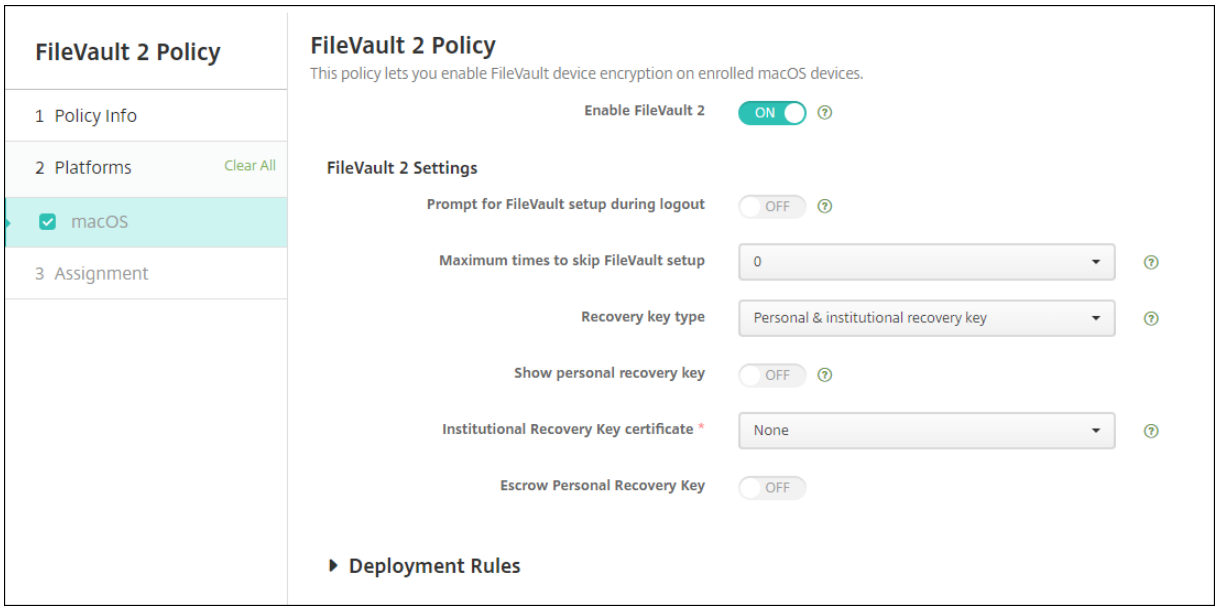
La fonctionnalité de cryptage intégral de disque FileVault de macOS (FileVault 2) protège le volume système en cryptant son contenu. Un utilisateur se connecte à un appareil macOS sur lequel FileVault est activé avec son mot de passe de compte à chaque démarrage de l'appareil. Si l'utilisateur perd son mot de passe, une clé de récupération (également appelée « clé de secours ») lui permet de déverrouiller le disque et de réinitialiser son mot de passe.

Cette stratégie active les écrans de configuration utilisateur de FileVault et configure les paramètres tels que les clés de récupération. Pour plus d'informations sur FileVault, consultez le site d'assistance Apple.

Pour ajouter la stratégie FileVault, accédez à **Configurer > Stratégies d'appareil**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres macOS



- **Activer FileVault :** si cette option est définie sur **Activé**, l'utilisateur est invité à activer FileVault au cours des N prochaines déconnexions, comme spécifié par l'option **Nbre max. de fois qu'il est possible d'ignorer l'activation de FileVault**. Si cette option est définie sur **Désactivé**, les utilisateurs ne reçoivent pas d'invite pour activer FileVault, mais ils peuvent toujours activer FileVault par eux-mêmes.
- **Exiger activation de FileVault durant la déconnexion :** si cette option est définie sur **Activé**, l'utilisateur est invité à activer FileVault lorsqu'il se déconnecte.
- **Nbre max. de fois qu'il est possible d'ignorer l'activation de FileVault :** nombre maximal de fois que l'utilisateur peut ignorer la configuration de FileVault. Lorsque l'utilisateur atteint le nombre maximal de fois défini, il doit configurer FileVault pour se connecter. Si la valeur est **0**, l'utilisateur doit activer FileVault lors de sa première tentative de connexion. La valeur par défaut est **0**.
- **Type de clé de récupération :** un utilisateur qui oublie son mot de passe peut entrer une clé de récupération pour déverrouiller le disque et réinitialiser son mot de passe. Options de clé de récupération :
  - **Clé de récupération privée :** une clé de récupération privée est propre à un utilisateur. Lors de l'installation de FileVault, un utilisateur choisit de créer une clé de récupération ou d'autoriser son compte iCloud à déverrouiller son disque. Pour afficher la clé de récupération pour l'utilisateur après la configuration de FileVault, activez **Afficher la clé de récupération privée**. L'affichage de la clé permet à l'utilisateur de noter la clé pour une utilisation ultérieure. Pour permettre aux utilisateurs de rechercher leur clé s'ils la perdent, activez **Dépôt de clé de secours privée**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

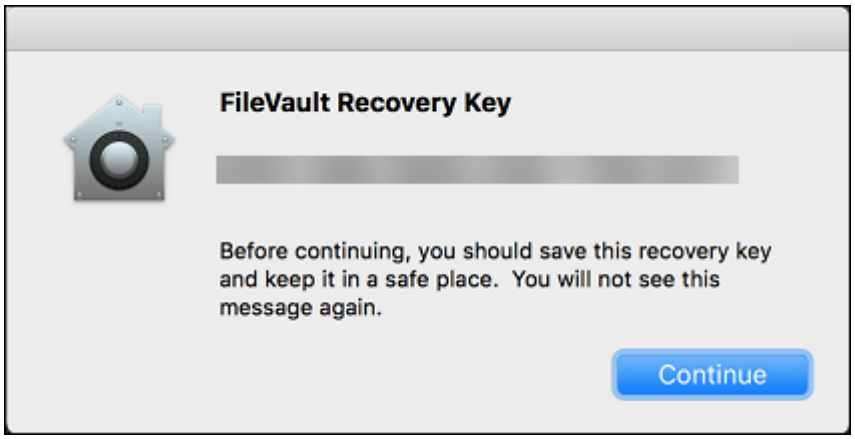
Vous pouvez alterner les clés de récupération privées via des actions de sécurité. Pour plus d'informations sur la rotation des clés de récupération privées, consultez la section Actions de sécurisation.

Pour plus d'informations sur la gestion des clés de récupération, consultez le site d'assistance Apple.

– **Clé de récupération institutionnelle :** vous pouvez créer une clé de récupération institutionnelle (ou principale) et un certificat FileVault, que vous pouvez ensuite utiliser pour déverrouiller les appareils utilisateur. Pour plus d'informations, consultez le site d'assistance Apple. Utilisez Citrix Endpoint Management pour déployer le certificat FileVault sur les appareils. Pour de plus amples informations, consultez Certificats et authentification.

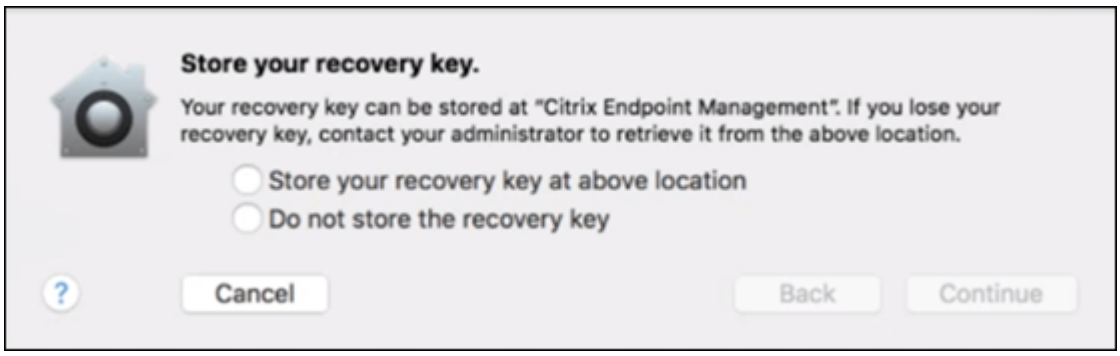
– **Clé de récupération privée et institutionnelle :** avec l'activation de ces deux types de clés de récupération, vous devez déverrouiller un appareil utilisateur uniquement si l'utilisateur perd sa clé de récupération privée.

- **Certificat de la clé de récupération institutionnelle :** si vous sélectionnez **Clé de récupération institutionnelle** ou **Clé de récupération privée et institutionnelle** comme **Type de clé de récupération**, sélectionnez le certificat de la clé de récupération associé à cette clé.
- **Afficher la clé de récupération privée :** si cette option est définie sur **Activé**, l'appareil utilisateur affiche la clé de récupération privée une fois la configuration FileVault effectuée. La valeur par défaut est **Désactivé**.



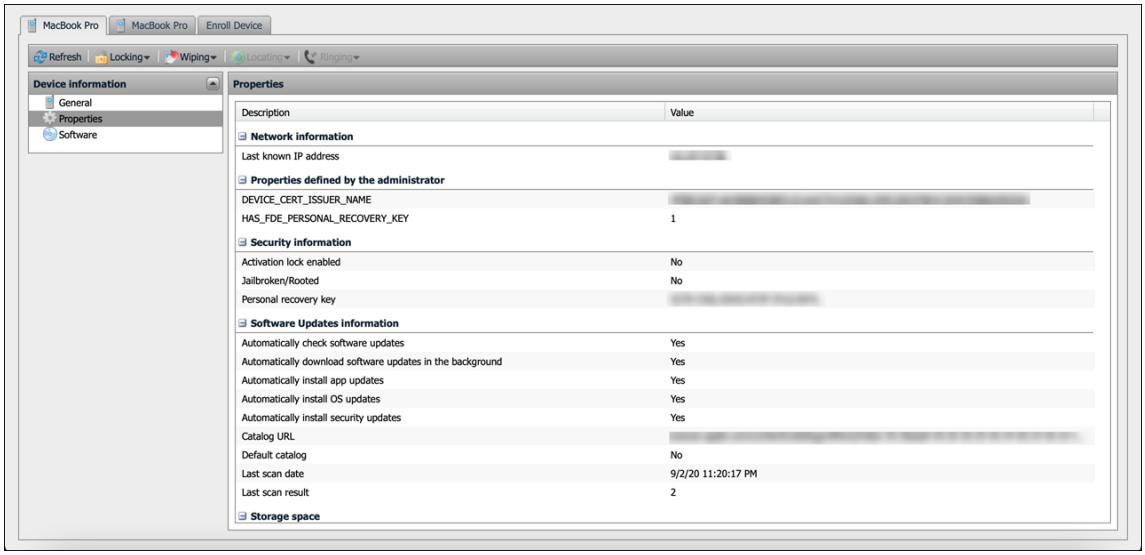
- **Dépôt de clé de secours privée :** lorsque cette option est activée, les utilisateurs peuvent stocker une copie de la clé de récupération privée pour chaque appareil avec Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pour accéder à la clé depuis Citrix Endpoint Management, accédez à **Gérer > Appareils**, sélectionnez l'appareil macOS et cliquez sur **Modifier**. Ensuite, accédez à **Détails de l'appareil > Général** et recherchez la **clé de récupération privée**.

Pour permettre aux utilisateurs d'afficher leur clé de récupération sur le portail utilisateur, activez **Dépôt de clé de secours privée** et **Afficher la clé de récupération privée**. La clé apparaît dans le portail utilisateur sur la page **Propriétés** sous **Informations de sécurité**. Pour plus d'informations sur le portail en libre-service, voir Portail en libre-service.



Vous pouvez activer le paramètre **Dépôt de clé de récupération privée** même si vous n'activez pas le paramètre **Activer FileVault**. Si vous désactivez le paramètre **Activer FileVault**, les utilisateurs peuvent toujours activer FileVault par eux-mêmes. Dans ce cas, activez l'option **Dépôt de clé de secours privée** pour permettre aux utilisateurs de stocker une copie de leur clé avec Citrix Endpoint Management.

Si un utilisateur active FileVault avant d'inscrire l'appareil à Citrix Endpoint Management, Citrix Endpoint Management ne stocke pas sa clé de récupération. L'appareil apparaît comme « FileVault activé » dans la console.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie de pare-feu

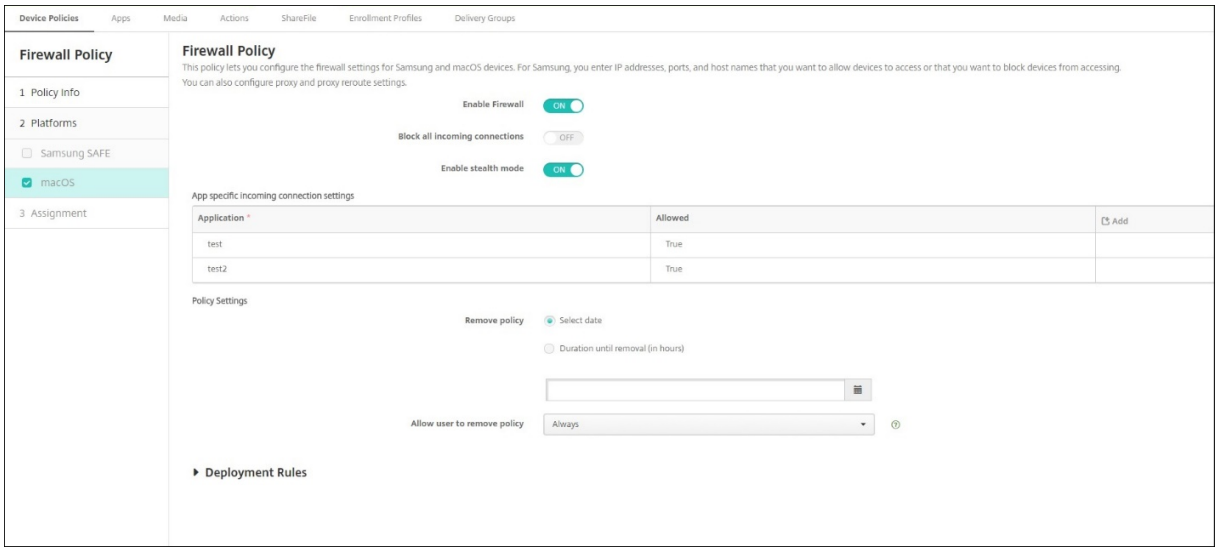
July 7, 2022

Cette stratégie vous permet de configurer les paramètres de pare-feu pour les appareils Samsung, macOS et Windows.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres macOS

Nécessite macOS 10.12 et ultérieur.

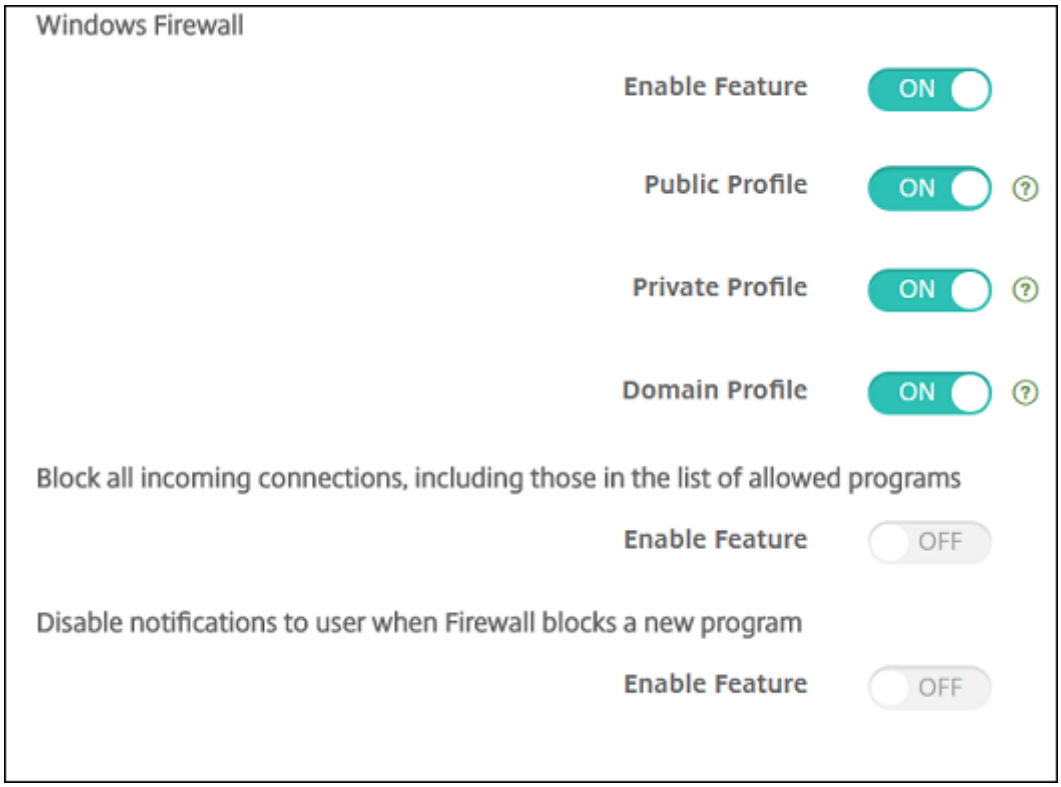


- **Activer pare-feu**. Pour activer le pare-feu, définissez cette option sur **Activé**.
- **Bloquer toutes les connexions entrantes**. Lorsque cette option est définie sur **Activé**, elle bloque toutes les connexions entrantes à l'exception des connexions requises pour les services de base.
- **Activer le mode furtif**. En mode furtif, l'appareil n'accepte pas ou ne répond pas aux tentatives d'accès à partir du réseau par des applications de test utilisant ICMP, telles que Ping. Pour activer le mode furtif, définissez cette option sur **Activé**.
- **Paramètres de connexion entrante spécifiques à l'application**. Pour permettre à des applications spécifiques de recevoir des connexions, ajoutez les applications et définissez **Autorisé** sur **True**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Windows Desktop et Tablet

Requiert des appareils Windows Desktop et Tablet exécutant Windows 10 (version 1709 ou ultérieure) ou Windows 11.



- **Activer la fonctionnalité :** cette option permet de contrôler le trafic entrant et sortant sur les ordinateurs sur lesquels cette stratégie est déployée. La valeur par défaut est **Activé**.
- **Profil public :** cette option permet de contrôler le pare-feu Windows lorsque les ordinateurs sont connectés à des réseaux non approuvés dans des lieux publics, tels que des aéroports et cafés. La valeur par défaut est **Activé**.
- **Profil privé :** cette option permet de contrôler le pare-feu Windows lorsque les ordinateurs sont connectés à des réseaux approuvés, tels qu'un réseau domestique. La valeur par défaut est **Activé**.
- **Profil de domaine :** cette option permet de contrôler le pare-feu Windows lorsque les ordinateurs sont connectés à des réseaux de domaine, tels qu'un lieu de travail. La valeur par défaut est **Activé**.
- **Bloquer toutes les connexions entrantes, y compris celles figurant dans la liste des programmes autorisés :** la valeur par défaut est **Désactivé**.
- **Désactiver les notifications utilisateur lorsque le pare-feu bloque un nouveau programme :** la valeur par défaut est **Désactivé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie de police

November 29, 2023

Vous pouvez ajouter une stratégie de police dans Citrix Endpoint Management pour ajouter des polices supplémentaires sur les appareils iOS et macOS. Les polices doivent être de type TrueType (`.ttf`) ou OpenType (`.oft`). Les collections de polices (`.ttc` ou `.otc`) ne sont pas prises en charge.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Nom visible par l'utilisateur :** entrez le nom que les utilisateurs voient dans leurs listes de polices.
- **Fichier de police :** pour sélectionner le fichier de police à ajouter aux périphériques utilisateur, cliquez sur **Parcourir**, puis accédez à l'emplacement du fichier.
- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.

Paramètres macOS

- **Nom visible par l'utilisateur :** entrez le nom que les utilisateurs voient dans leurs listes de polices.
- **Fichier de police :** pour sélectionner le fichier de police à ajouter aux périphériques utilisateur, cliquez sur **Parcourir**, puis accédez à l'emplacement du fichier.
- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Stratégie Disposition de l'écran d'accueil

November 29, 2023

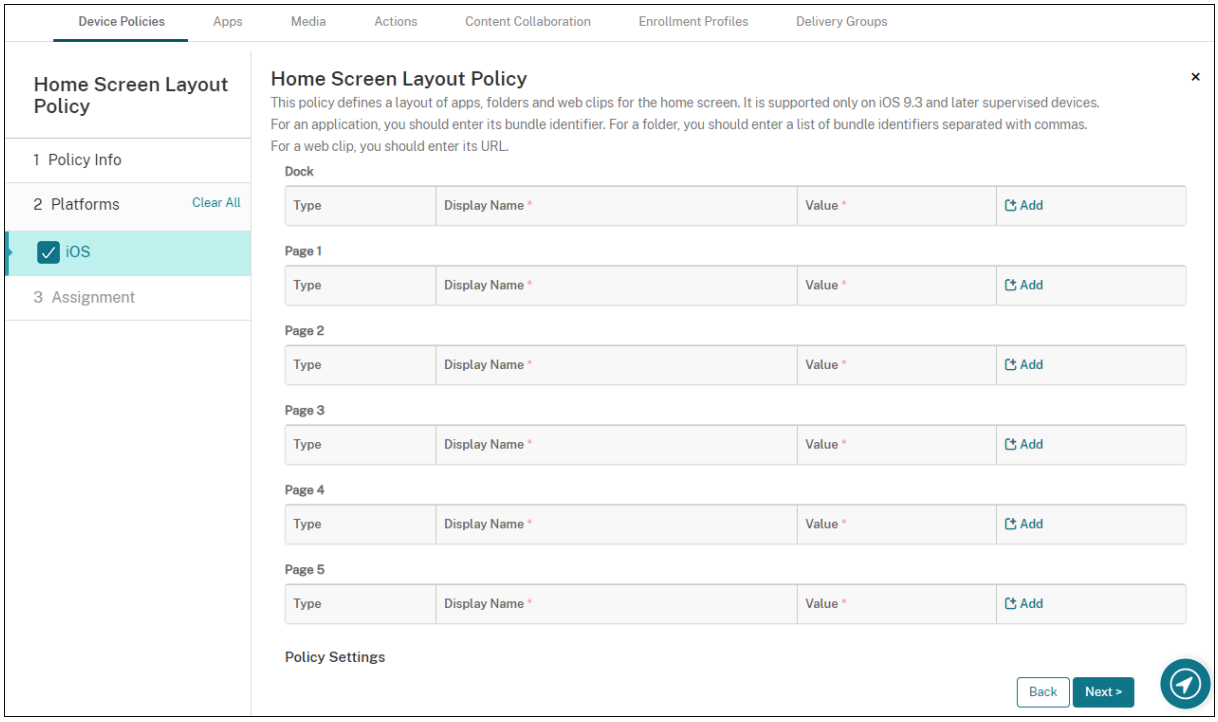
La nouvelle stratégie Disposition de l'écran d'accueil vous permet de spécifier la disposition des applications et des dossiers sur l'écran d'accueil des appareils iOS supervisés.

> **Important :**
>
> Le déploiement de plusieurs stratégies Disposition de l'écran d'accueil sur un appareil entraîne une erreur iOS sur l'appareil. Cette limitation s'applique si vous définissez l'écran d'accueil via cette stratégie Citrix Endpoint Management ou via Apple Configurator.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres iOS

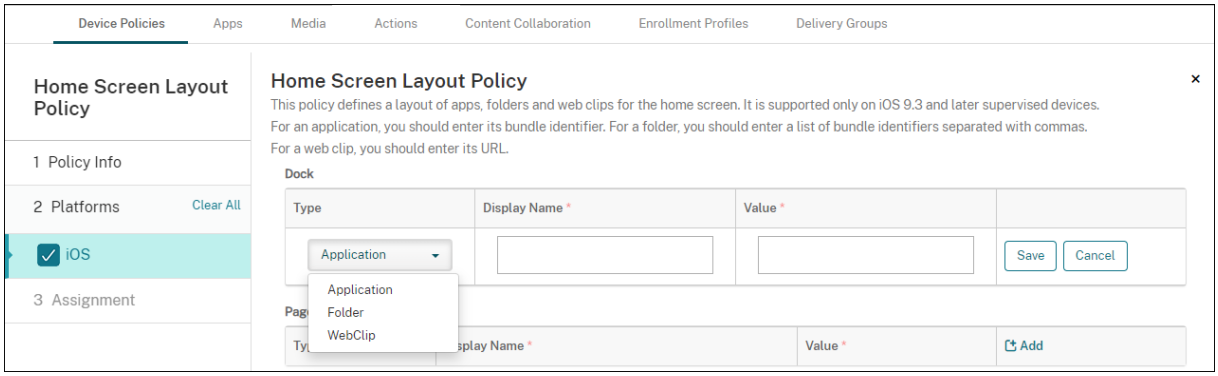


- Pour chacune des zones de l'écran que vous souhaitez configurer (telles que **Dock** ou **Page 1**), cliquez sur **Ajouter**.
- **Type :** choisissez **Application**, **Dossier** ou **Clip Web**.

  Le paramètre **Utilisation restreinte des apps > Autoriser uniquement certaines apps** dans la Stratégie Restrictions peut empêcher les clips Web d'apparaître correctement sur l'écran d'accueil. Pour que les clips Web apparaissent correctement, effectuez l'une des opérations suivantes :

  - Définissez l'option **Utilisation restreinte des apps** sur **Autoriser toutes les applications** ou **Interdire certaines apps**.
  - Si l'option **Utilisation restreinte des apps** est définie sur **Autoriser uniquement certaines apps**, ajoutez une application avec le Bundle ID `com.apple.webapp` pour autoriser les clips Web.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Nom d'affichage :** nom qui s'affichera sur l'écran d'accueil pour l'application ou le dossier.
- **Valeur :** pour les applications, entrez le bundle ID. Pour les dossiers, entrez une liste des bundle ID, séparés par des virgules. Pour les clips Web, entrez le bundle ID `com.apple.webClip.managed` et configurez l'URL du clip Web dans la stratégie de clip Web Si plusieurs valeurs de clip Web ont la même URL, le comportement n'est pas défini sur les appareils iOS 11.3 et versions ultérieures.
- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur iOS 9.3 et versions ultérieures.

Stratégie Importer le profil iOS et macOS

November 29, 2023

Vous pouvez importer les fichiers XML de configuration d'appareil pour iOS et macOS dans Citrix Endpoint Management. Le fichier contient des stratégies de sécurité et des restrictions que vous préparez avec Apple Configurator 2 ou Profile Creator. Le fichier XML de configuration peut contenir des macros. Pour de plus amples informations, veuillez consulter la section Macros.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cas d'utilisation

Importez les configurations suivantes créées en dehors de Citrix Endpoint Management pour les appareils macOS à l'aide de Profile Creator :

- **System Policy Control :** la stratégie identifie les applications signées par les développeurs Apple certifiés et permet aux utilisateurs de télécharger des applications vérifiées depuis le Mac App Store.

  Lors de la configuration de la stratégie :

  - Sélectionnez **Enable Gatekeeper** pour vous assurer que les utilisateurs exécutent uniquement des logiciels vérifiés et approuvés.
  - Sélectionnez **Allow Identified Developers** pour vous assurer que les utilisateurs installent des applications signées uniquement par des développeurs Apple certifiés.

- **Privacy Preferences Policy Control :** cette stratégie vous permet d'accorder ou de restreindre l'accès inter-applications à certains fichiers ou fonctionnalités, telles que les services de localisation, l'appareil photo et la capture d'écran.

  Configurez les paramètres que vous prévoyez déployer. Pour plus d'informations, voir Réglages des données utiles Contrôle de politique de préférences Confidentialité.

- **Kernel Extensions Policy :** cette stratégie permet aux utilisateurs d'installer des extensions d'application qui étendent les capacités natives du système d'exploitation. Les extensions du noyau s'exécutent au niveau du noyau.

  Configurez les paramètres que vous prévoyez déployer. Pour plus d'informations, consultez Réglages des données utiles Politique d'extension de noyau.

- **Ethernet Settings Policy :** cette stratégie vous permet de gérer la connexion réseau Ethernet.

  Configurez les paramètres que vous prévoyez déployer. Pour plus d'informations, consultez Réglages Ethernet.

Utilisez Apple Configurator 2 ou Profile Creator pour configurer les stratégies suivantes pour les appareils macOS et iOS :

- **Stratégie Wi-Fi :** cette stratégie vous permet de gérer la façon dont les utilisateurs connectent leurs appareils à un réseau Wi-Fi.

  Lors de la configuration de la stratégie :

  - Ajoutez le SSID cible en haut de la liste des priorités.
  - Choisissez le mode de connexion à utiliser lorsque l'utilisateur rejoint un réseau. Si vous sélectionnez **Système**, l'appareil utilise les informations d'identification système pour authentifier l'utilisateur. Si vous sélectionnez **Fenêtre de connexion**, l'appareil utilise les

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

mêmes informations d'identification entrées dans la fenêtre de connexion pour authentifier l'utilisateur.

Pour plus d'informations, consultez Réglages Wi-Fi.

- **Stratégie de restrictions :** cette stratégie autorise ou limite l'utilisation de certaines fonctionnalités sur les appareils utilisateur.

  Configurez les paramètres que vous prévoyez déployer. Pour plus d'informations, voir Passer en revue les restrictions MDM pour les appareils Apple.

- **Stratégie VPN :** cette stratégie fournit une connexion cryptée au niveau de l'appareil aux réseaux privés.

  Configurez les paramètres que vous prévoyez déployer. Pour de plus amples informations, consultez Présentation des réglages VPN.

Créer un profil de configuration à l'aide d'Apple Configurator 2

1. Installez Apple Configurator 2 à partir de l'Apple App Store.
2. Démarrez Apple Configurator 2 et accédez à **File > New Profile**. Une nouvelle fenêtre de configuration apparaît.
3. Dans le volet des paramètres **General**, tapez un nom et un identifiant pour votre profil, puis ajoutez des options de charge utile supplémentaires.
4. Dans le volet gauche, sélectionnez une charge utile, cliquez sur **Configure**, puis entrez les paramètres. Ne signez pas votre profil, car les profils signés ne sont pas pris en charge.

   Pour ajouter plusieurs charges utiles dans un même profil, sélectionnez une charge utile et cliquez sur le bouton **Add Payload** dans le coin supérieur droit.
5. Accédez à **File > Save**, choisissez un nom et un emplacement pour enregistrer le fichier XML, puis cliquez sur **Save**.

Créer un profil de configuration à l'aide de Profile Creator

1. Installez Profile Creator à partir de GitHub.
2. Démarrez Profile Creator et accédez à **File > New**. Une nouvelle fenêtre de configuration apparaît.
3. Dans le volet des paramètres **General**, tapez un nom et une description pour votre profil, puis ajoutez des options de charge utile supplémentaires.

   - Recommandation : sélectionnez **Prevent users from removing this profile**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Définissez **Payload Scope** sur **System** ou **User**.

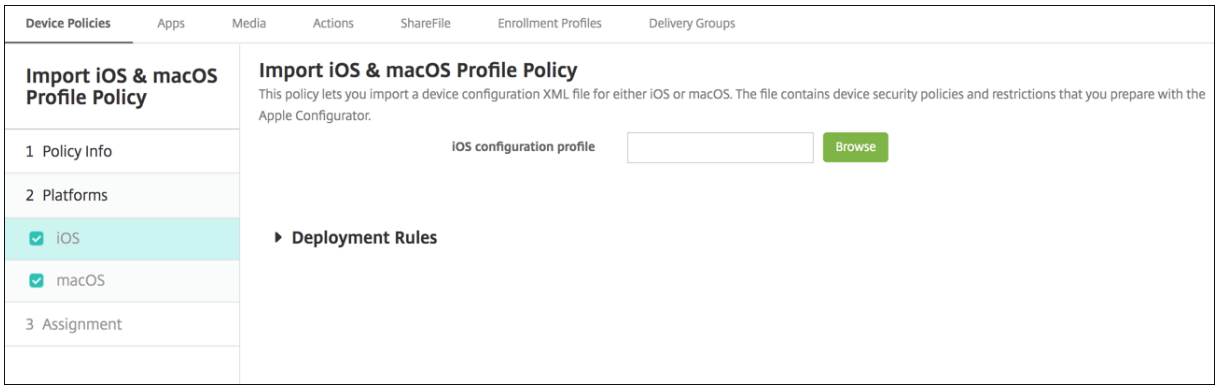
4. Dans le volet gauche, choisissez la stratégie, configurez les paramètres, puis cliquez sur **Add** dans le coin supérieur droit.

   Pour configurer plusieurs stratégies au sein d'un même profil, sélectionnez une stratégie et cliquez sur le bouton **Add**.

5. Accédez à **File > Export**, choisissez un nom et un emplacement pour enregistrer le fichier XML, puis cliquez sur **Save**.

Pour importer un fichier de configuration pour la stratégie de profil iOS et macOS dans la console Citrix Endpoint Management, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS et macOS



- **Profil de configuration iOS** ou **Profil de configuration macOS** : pour sélectionner le fichier de configuration à importer, cliquez sur **Parcourir** et accédez à l'emplacement du fichier.

Stratégie Gestion du keyguard

November 29, 2023

Le keyguard Android gère l'appareil et les challenges d'écran de verrouillage des profils professionnels. Cette stratégie vous permet de contrôler les fonctionnalités du keyguard de l'appareil avancé et du keyguard de challenge des profils professionnels Android Entreprise. Vous pouvez contrôler :

- Gestion du keyguard sur les appareils avec profil de travail. Vous pouvez spécifier les fonctionnalités disponibles pour les utilisateurs avant qu'ils déverrouillent le keyguard de l'appareil et le keyguard de challenge professionnel. Par exemple, par défaut, les utilisateurs peuvent

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

utiliser le déverrouillage par empreinte digitale et afficher les notifications non censurées sur l'écran de verrouillage.

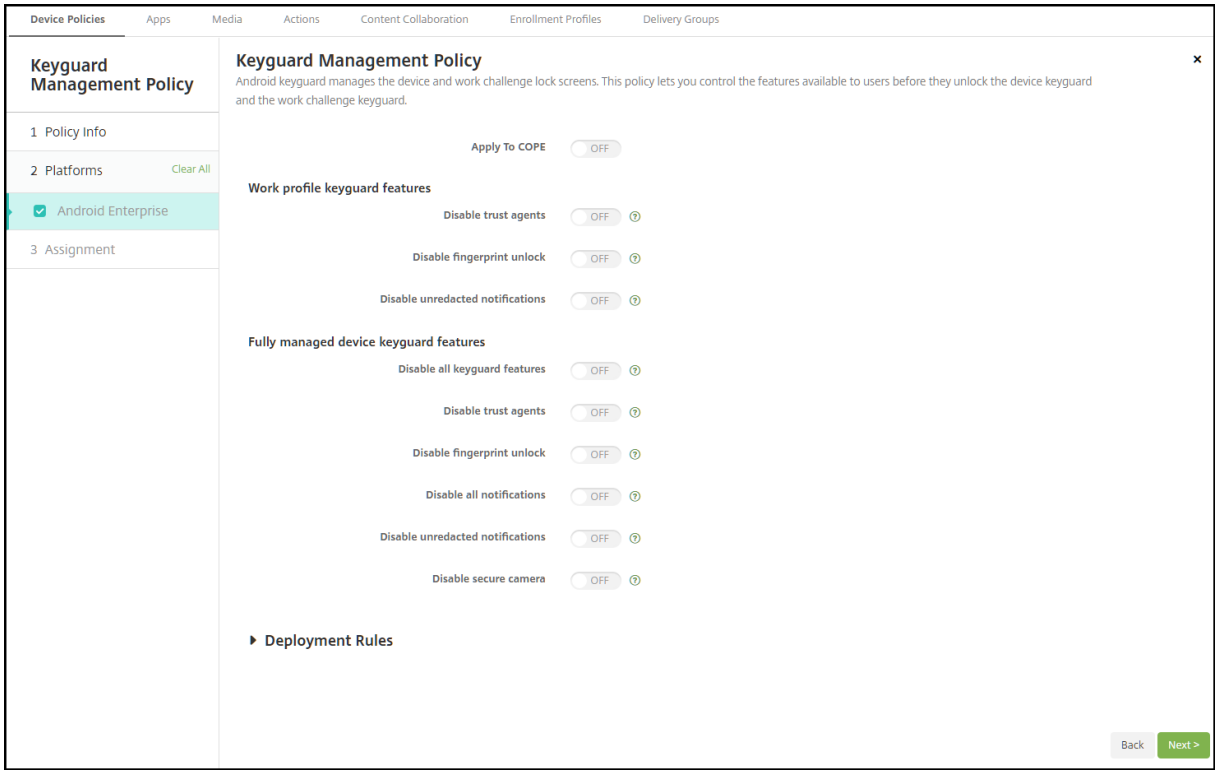
- Gestion du keyguard sur des appareils entièrement gérés et dédiés. Vous pouvez spécifier les fonctionnalités disponibles, telles que les agents de confiance et la caméra sécurisée, avant qu'ils déverrouillent l'écran du keyguard. Ou, vous pouvez choisir de désactiver toutes les fonctionnalités du keyguard.
- Gestion des Keyguard sur des appareils entièrement gérés avec profil de travail. Ces appareils étaient auparavant appelés appareils COPE. Vous pouvez utiliser une stratégie Gestion du keyguard pour appliquer des paramètres distincts à l'appareil et au profil de travail.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Regardez cette vidéo pour en savoir plus :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Android Enterprise



- **Appliquer à COPE :** permet de configurer les paramètres de stratégie Gestion du keyguard pour les appareils entièrement gérés avec profil de travail.

  Lorsque ce paramètre est **activé**, vous pouvez appliquer des paramètres distincts à l'appareil et au profil de travail sur les appareils entièrement gérés avec profil de travail.

  Lorsque ce paramètre est **Désactivé**, vous pouvez appliquer des paramètres aux appareils avec profil de travail ou aux appareils entièrement gérés. Les paramètres que vous configurez pour les profils de travail ne s'appliquent qu'aux appareils avec profil de travail. Les paramètres que vous configurez pour les appareils entièrement gérés ne s'appliquent qu'aux appareils entièrement gérés.

  La valeur par défaut est **Off**.

- **Fonctionnalités keyguard du profil de travail :** contrôle si les fonctions suivantes sont disponibles avant qu'un utilisateur déverrouille le keyguard du profil de travail (écran de verrouillage).

  – **Désactiver les agents de confiance :** si cette option est **désactivée**, les agents de confiance peuvent opérer sur des écrans de keyguard sécurisés lorsqu'un challenge est défini sur le profil de travail. Définissez l'option sur **Activé** pour désactiver tous les agents de confiance du profil de travail. La valeur par défaut est **Off**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Désactiver authentification biométrique :** si **Désactivé** est sélectionné, l'authentification biométrique est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur le profil de travail. Définissez cette option sur **Activé** pour désactiver l'authentification biométrique sur le profil de travail. Ce paramètre désactive le déverrouillage par empreinte digitale, l'authentification du visage et l'authentification de l'iris. La valeur par défaut est **Off**. Pour Android 9.0 et versions ultérieures.
  - **Désactiver le déverrouillage par empreinte digitale :** si cette option est **désactivée**, le déverrouillage par empreinte digitale est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur le profil de travail. Définissez l'option sur **Activé** pour désactiver le déverrouillage par empreinte digitale sur le profil de travail. La valeur par défaut est **Off**.
  - **Désactiver authentification du visage :** si **Désactivé** est sélectionné, l'authentification du visage est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur le profil de travail. Définissez cette option sur **Activé** pour désactiver l'authentification du visage sur le profil de travail. La valeur par défaut est **Off**. Pour Android 9.0 et versions ultérieures.
  - **Désactiver authentification de l'iris :** si **Désactivé** est sélectionné, l'authentification de l'iris est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur le profil de travail. Définissez cette option sur **Activé** pour désactiver l'authentification de l'iris sur le profil de travail. La valeur par défaut est **Off**. Pour Android 9.0 et versions ultérieures.
  - **Désactiver les notifications non censurées :** si cette option est définie sur **Désactivé**, les notifications censurées et non censurées apparaissent sur les écrans de keyguard sécurisés. Définissez cette option sur **Activé** pour désactiver les notifications non censurées et afficher uniquement les notifications censurées. La valeur par défaut est **Off**.

- **Fonctionnalités keyguard d'appareil entièrement géré :** contrôle si les fonctions suivantes sont disponibles avant qu'un utilisateur déverrouille le keyguard d'appareil (écran de verrouillage). Ces fonctionnalités s'appliquent aux appareils entièrement gérés ou dédiés.

  - **Désactiver toutes les fonctionnalités du keyguard :** si cette option est **désactivée**, toutes les personnalisations actuelles et futures de keyguard seront disponibles sur les écrans de keyguard sécurisés. Définissez sur **Activé** pour désactiver toutes les personnalisations de keyguard. La valeur par défaut est **Off**.
  - **Désactiver les agents de confiance :** si cette option est **désactivée**, les agents de confiance peuvent opérer sur des écrans de keyguard sécurisés. Définissez sur **Activé** pour désactiver les agents de confiance. La valeur par défaut est **Off**.
  - **Désactiver authentification biométrique :** si **Désactivé** est sélectionné, l'authentification biométrique est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur l'appareil. Définissez cette option sur **Activé** pour désactiver l'authentifica-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tion biométrique sur l'appareil. Les fonctions d'authentification biométrique désactivées sont le déverrouillage par empreinte digitale, l'authentification du visage et l'authentification de l'iris. La valeur par défaut est **Off**. Pour Android 9.0 et versions ultérieures.

- **Désactiver le déverrouillage par empreinte digitale :** si cette option est **désactivée**, le déverrouillage par empreinte digitale est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur l'appareil. Définissez l'option sur **Activé** pour désactiver le déverrouillage par empreinte digitale sur l'appareil. La valeur par défaut est **Off**.
- **Désactiver authentification du visage :** si **Désactivé** est sélectionné, l'authentification du visage est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur l'appareil. Définissez cette option sur **Activé** pour désactiver l'authentification du visage sur l'appareil. La valeur par défaut est **Off**. Pour Android 9.0 et versions ultérieures.
- **Désactiver authentification de l'iris :** si **Désactivé** est sélectionné, l'authentification de l'iris est disponible sur les écrans de keyguard sécurisés lorsqu'un challenge est défini sur l'appareil. Définissez cette option sur **Activé** pour désactiver l'authentification de l'iris sur l'appareil. La valeur par défaut est **Off**. Pour Android 9.0 et versions ultérieures.
- **Désactiver toutes les notifications :** si cette option est **désactivée**, toutes les notifications apparaissent sur les écrans de keyguard sécurisés. Définissez l'option sur **Activé** pour afficher toutes les notifications. La valeur par défaut est **Off**.
- **Désactiver les notifications non censurées :** si cette option est définie sur **Désactivé**, les notifications censurées et non censurées apparaissent sur les écrans de keyguard sécurisés. Définissez cette option sur **Activé** pour désactiver les notifications non censurées et afficher uniquement les notifications censurées. La valeur par défaut est **Off**.
- **Désactiver la caméra sécurisée :** si cette option est **désactivée**, la caméra sécurisée est disponible sur les écrans de keyguard sécurisés. Définissez l'option sur **Activé** pour désactiver la caméra sécurisée. La valeur par défaut est **Off**.

Stratégie kiosque

November 29, 2023

La stratégie Kiosque vous permet de restreindre les appareils au mode Kiosque en limitant les applications pouvant s'exécuter. Citrix Endpoint Management ne contrôle pas quelle partie de l'appareil se verrouille en mode Kiosque. L'appareil gère les paramètres du mode kiosque une fois la stratégie déployée.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

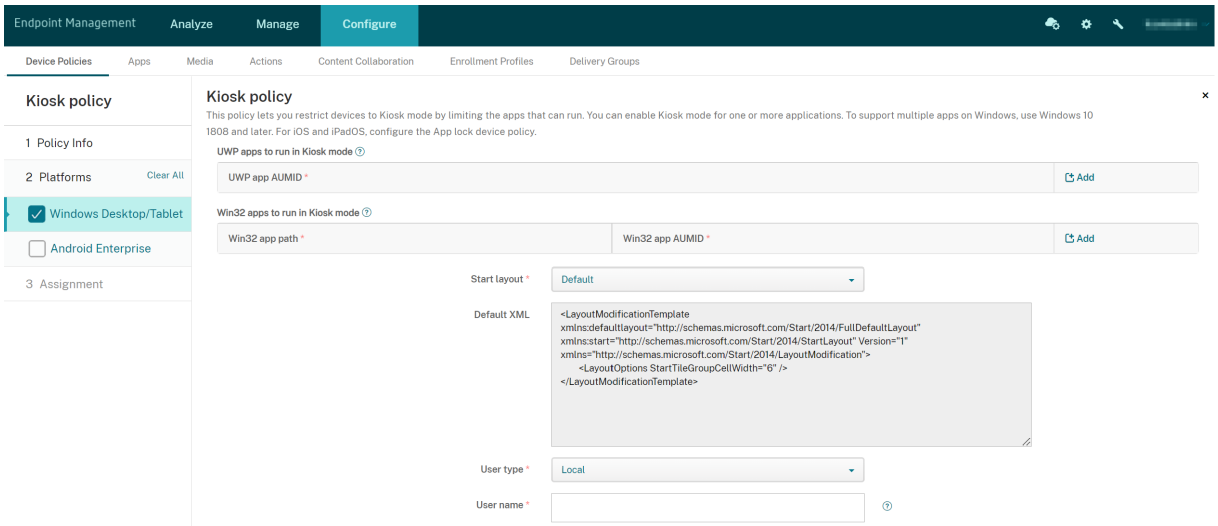
Pour configurer l'exécution des iPad en mode Kiosque, utilisez la stratégie Mode kiosque. Pour de plus amples informations sur la configuration d'iPads en tant que kiosques, consultez la section Configurer un iPad en tant que kiosque. Vous pouvez également configurer un iPad pour qu'il n'ouvre qu'un seul site Web. Pour de plus amples informations, consultez la stratégie de clip Web.

Paramètres Windows Desktop et Tablet

Pour les appareils Windows Desktop et Tablet, la stratégie Kiosque s'applique uniquement aux utilisateurs locaux et aux utilisateurs inscrits dans Azure AD.

Une ou plusieurs applications peuvent s'exécuter en mode Kiosque sur les appareils Windows Desktop et Tablet.

> **Remarque :**
>
> La stratégie Kiosque s'applique uniquement aux appareils Windows 10.
> Pour déployer un kiosque à application unique sur des appareils Windows 11, vous pouvez utiliser la stratégie XML personnalisée pour déployer le script XML que nous fournissons sur les appareils. Pour plus d'informations, consultez Déployer un kiosque à application unique sur les appareils Windows 11.



- **AUMID UWP :** cliquez sur **Ajouter**, sélectionnez l'application Universal Windows Platform (UWP) et entrez l'ID de modèle utilisateur de l'application (AUMID) pour chaque application UWP. Par exemple, entrez l'AUMID suivant :
  - `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`
- **Chemin Win32** ou **AUMID Win32** : cliquez sur **Ajouter**, sélectionnez l'application de bureau Windows (Win32) et entrez le chemin d'accès et l'AUMID pour chaque application Win32. Par exemple, entrez le chemin d'accès et l'AUMID suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - `%windir%\system32\mspaint.exe` ou `C:\Windows\System32\mspaint.exe`
  - `{ 1AC14E77-02E7-4E5D-B744-2EB1AE5198B7 } \mspaint.exe`

- **Disposition de l'écran de démarrage :** seul l'écran de démarrage pour applications par défaut est disponible.
- **XML par défaut :** seul le script XML par défaut est disponible.
- **Type d'utilisateur :** spécifie le type d'utilisateur qui recevra la stratégie Kiosque. Sélectionnez une des options suivantes :
  - **Local :** Citrix Endpoint Management crée un utilisateur pour l'appareil cible ou ajoute un utilisateur existant.
  - **Azure AD :** Citrix Endpoint Management ajoute des utilisateurs inscrits dans Azure AD.
- **Nom d'utilisateur :** entrez le nom d'utilisateur qui recevra la stratégie Kiosque.
  - Pour créer un nom d'utilisateur local sur l'appareil cible, tapez le nom. Assurez-vous que votre nom d'utilisateur local ne contient pas le domaine. Si vous entrez un nom existant, Citrix Endpoint Management ne crée pas d'utilisateur ou ne modifie pas le mot de passe actuel.
  - Pour ajouter un utilisateur Azure AD, entrez le nom au format `azuread\user`. La partie `user` peut être soit le **nom** entré lors de la création d'un utilisateur dans Azure AD, soit le **nom d'utilisateur** entré lors de la création d'un utilisateur dans Azure AD. L'utilisateur affecté ne peut pas être un administrateur Azure AD.
- **Mot de passe :** aucune configuration de mot de passe n'existe pour les utilisateurs Azure AD. Saisissez le mot de passe uniquement pour le nom d'utilisateur local.
- **Afficher la barre des tâches :** activez la barre des tâches pour fournir aux utilisateurs un moyen facile d'afficher et de gérer les applications. La valeur par défaut est **Off**.
- Cliquez sur **Suivant** et enregistrez les modifications.

Pour une application UWP que vous souhaitez autoriser en mode Kiosque, vous devez fournir l'identifiant AUMID. Pour obtenir une liste des AUMID pour toutes les applications Microsoft Store installées pour l'utilisateur actuel de l'appareil, exécutez la commande PowerShell suivante :

```
$installedapps = get-AppxPackage

$aumidList = @()
foreach ($app in $installedapps)
{

    foreach ($id in (Get-AppxPackageManifest $app).package.applications
        .application.id)
    {

        $aumidList += $app.packagefamilyname + "!"+ $id
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

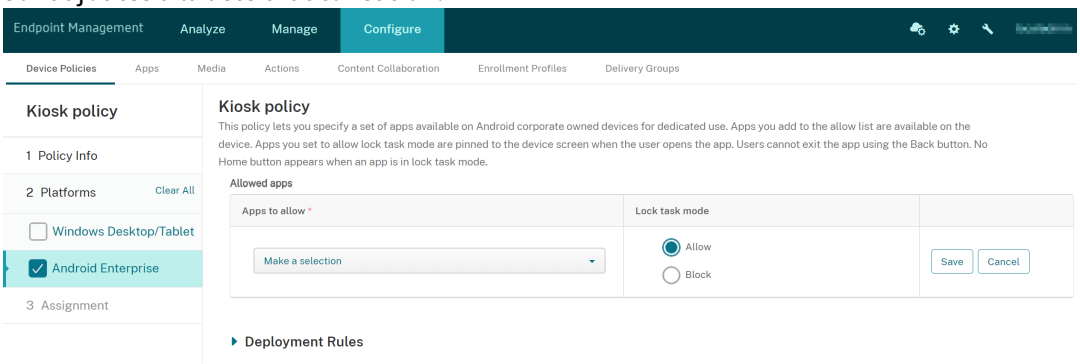
```
11        }
12
13   }
14
15
16 $aumidList
17 <!--NeedCopy-->
```

Paramètres Android Enterprise

Vous pouvez autoriser des applications et définir le mode de verrouillage des tâches pour les appareils Android Enterprise dédiés, également appelés appareils d'entreprise à usage unique (COSU).

Pour autoriser une application, cliquez sur **Ajouter**. Vous pouvez ajouter plusieurs applications à la liste d'autorisation. Pour plus d'informations, consultez la section Android Enterprise.

- **Applications à autoriser :** saisissez le nom de package de l'application que vous souhaitez autoriser ou sélectionnez son nom dans la liste.
  - Cliquez sur **Ajouter** pour entrer le nom du package de l'application autorisée dans la liste.
  - Sélectionnez l'application existante dans la liste. La liste affiche les applications chargées sur Citrix Endpoint Management. Par défaut, les services Citrix Secure Hub et Google Play sont ajoutés à la liste d'autorisation.



- **Mode de verrouillage des tâches :** choisissez **Autoriser** pour que l'application soit épinglée sur l'écran de l'appareil lorsque l'utilisateur démarre l'application. Choisissez **Bloquer** pour que l'application ne soit pas épinglée. La valeur par défaut est **Autoriser**.

Lorsqu'une application est en mode de verrouillage des tâches, elle est épinglée sur l'écran de l'appareil lorsque l'utilisateur l'ouvre. Aucun bouton d'accueil n'apparaît et le bouton **Retour** est désactivé. L'utilisateur quitte l'application à l'aide d'une action programmée dans l'application, comme la déconnexion.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie de configuration du Launcher

November 29, 2023

Citrix Launcher vous permet de personnaliser l'expérience de l'utilisateur pour les appareils Android Enterprise et les appareils Android d'ancienne génération déployés par Citrix Endpoint Management.

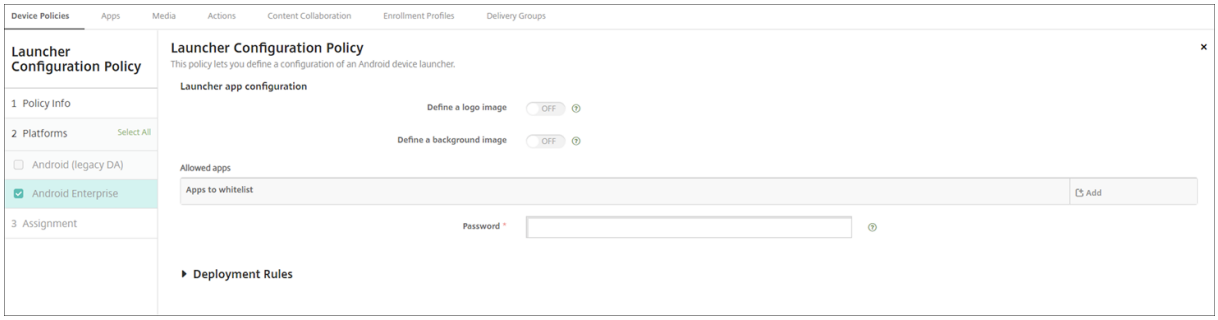
Utilisez une stratégie de configuration du Launcher pour contrôler ces fonctionnalités de Citrix Launcher :

- Gérez les appareils Android Enterprise et les appareils Android d'ancienne génération de façon à ce que les utilisateurs puissent uniquement accéder aux applications que vous spécifiez.
- Si vous le souhaitez, vous pouvez spécifier une image de logo personnalisé pour l'icône Citrix Launcher et une image d'arrière-plan personnalisée pour Citrix Launcher.
- Spécifiez un mot de passe que les utilisateurs doivent entrer pour quitter le Launcher.

Citrix Launcher n'est pas destiné à être une couche de sécurité supplémentaire venant s'ajouter à ce que la plate-forme de l'appareil offre déjà.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Android Enterprise et Android



- **Définir une image de logo :** indiquez si vous souhaitez utiliser une image de logo personnalisé pour l'icône Citrix Launcher. La valeur par défaut est **Off**.
- **Image du logo :** lorsque vous activez **Définir une image de logo**, sélectionnez le fichier d'image en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier. Les types de fichier pris en charge sont PNG, JPG, JPEG et GIF.
- **Définir une image d'arrière-plan :** indiquez si vous souhaitez utiliser une image personnalisée pour l'arrière-plan de Citrix Launcher. La valeur par défaut est **Off**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Image d'arrière-plan :** lorsque vous activez **Définir une image d'arrière-plan**, sélectionnez le fichier d'image en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier. Les types de fichier pris en charge sont PNG, JPG, JPEG et GIF.
- **Applications autorisées :** pour chaque application que vous souhaitez autoriser dans Citrix Launcher, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nouvelle application à ajouter :** entrez le nom complet de l'application à ajouter. Par exemple, com.android.calendar pour l'application calendrier d'Android.
  - Cliquez sur **Enregistrer** pour ajouter l'application, ou cliquez sur **Annuler** pour annuler l'ajout de l'application.
- **Mot de passe :** le mot de passe qu'un utilisateur doit entrer pour quitter Citrix Launcher.

Stratégie LDAP

November 29, 2023

Vous créez une stratégie LDAP pour appareils iOS dans Citrix Endpoint Management pour fournir des informations sur un serveur LDAP à utiliser, y compris toute information nécessaire sur le compte. La stratégie fournit également un ensemble de stratégies de recherche LDAP à utiliser lors de l'interrogation du serveur LDAP.

Vous devez utiliser le nom d'hôte LDAP avant de configurer cette stratégie.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Description du compte :** entrez une description du compte(facultatif).
- **Nom d'utilisateur du compte :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe du compte :** entrez un mot de passe (facultatif). Utilisez ce champ uniquement avec des profils chiffrés.
- **Nom d'hôte LDAP :** entrez le nom d'hôte du serveur LDAP. Ce champ est obligatoire.
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur LDAP. La valeur par défaut est **On**.
- **Paramètres de recherche :** ajoutez les paramètres de recherche à utiliser lors de l'interrogation du serveur LDAP. vous pouvez entrer autant de paramètres de recherche que vous voulez, mais vous devez ajouter au moins un paramètre de recherche pour faire du compte une ressource utile. Cliquez sur **Ajouter**, puis procédez comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Description :** entrez une description pour le paramètre de recherche. Ce champ est obligatoire.
  - **Portée :** choisissez **Base**, **Un niveau** ou **Sous-arborescence** pour définir la profondeur de la recherche dans l'arborescence LDAP. La valeur par défaut est **Base**.
    * **Base** recherche le nœud indiqué par la Base de recherche.
    * **Un niveau** recherche le nœud Base et un niveau en dessous.
    * **Sous-arborescence** recherche le nœud Base, ainsi que tous ses enfants, quelle que soit la profondeur.
  - **Base de recherche :** entrez le chemin d'accès au nœud à partir duquel démarrer une recherche. Par exemple, ou=people ou 0=example corp. Ce champ est obligatoire.
  - Cliquez sur **Ajouter** pour ajouter le paramètre de recherche ou cliquez sur **Annuler** pour annuler l'ajout du paramètre de recherche.
  - Répétez ces étapes pour chaque paramètre de recherche à ajouter.

- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.

Paramètres macOS

- **Description du compte :** entrez une description du compte(facultatif).
- **Nom d'utilisateur du compte :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe du compte :** entrez un mot de passe (facultatif). Utilisez ce champ uniquement avec des profils chiffrés.
- **Nom d'hôte LDAP :** entrez le nom d'hôte du serveur LDAP. Ce champ est obligatoire.
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur LDAP. La valeur par défaut est **On**.
- **Paramètres de recherche :** ajoutez les paramètres de recherche à utiliser lors de l'interrogation du serveur LDAP. vous pouvez entrer autant de paramètres de recherche que vous voulez, mais vous devez ajouter au moins un paramètre de recherche pour faire du compte une ressource utile. Cliquez sur **Ajouter**, puis procédez comme suit :
  - **Description :** entrez une description pour le paramètre de recherche. Ce champ est obligatoire.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Portée :** choisissez **Base**, **Un niveau** ou **Sous-arborescence** pour définir la profondeur de la recherche dans l'arborescence LDAP. La valeur par défaut est **Base**.
    * **Base** recherche le nœud indiqué par la Base de recherche.
    * **Un niveau** recherche le nœud Base et un niveau en dessous.
    * **Sous-arborescence** recherche le nœud Base, ainsi que tous ses enfants, quelle que soit la profondeur.
  - **Base de recherche :** entrez le chemin d'accès au nœud à partir duquel démarrer une recherche. Par exemple, ou=people ou 0=example corp. Ce champ est obligatoire.
  - Cliquez sur **Ajouter** pour ajouter le paramètre de recherche ou cliquez sur **Annuler** pour annuler l'ajout du paramètre de recherche.
  - Répétez ces étapes pour chaque paramètre de recherche à ajouter.

- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Stratégie d'emplacement

November 29, 2023

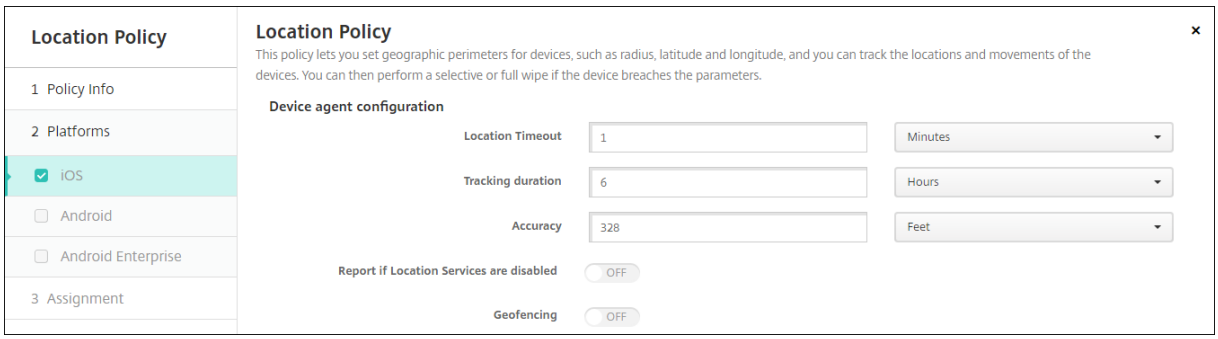
Vous pouvez créer des stratégies d'emplacement dans Citrix Endpoint Management pour imposer des limites géographiques. Lorsque les utilisateurs violent le périmètre défini, également appelé *géofencing*, Citrix Endpoint Management peut exécuter certaines actions. Par exemple, vous pouvez configurer la stratégie pour émettre un message d'avertissement aux utilisateurs lorsqu'ils violent le périmètre défini. Vous pouvez également configurer la stratégie pour effacer les données d'entreprise

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

des utilisateurs lorsqu'ils violent un périmètre, immédiatement ou après un délai. Pour plus d'informations sur les actions de sécurité, telles que le suivi et la localisation d'un appareil, reportez-vous à la section Actions de sécurisation.

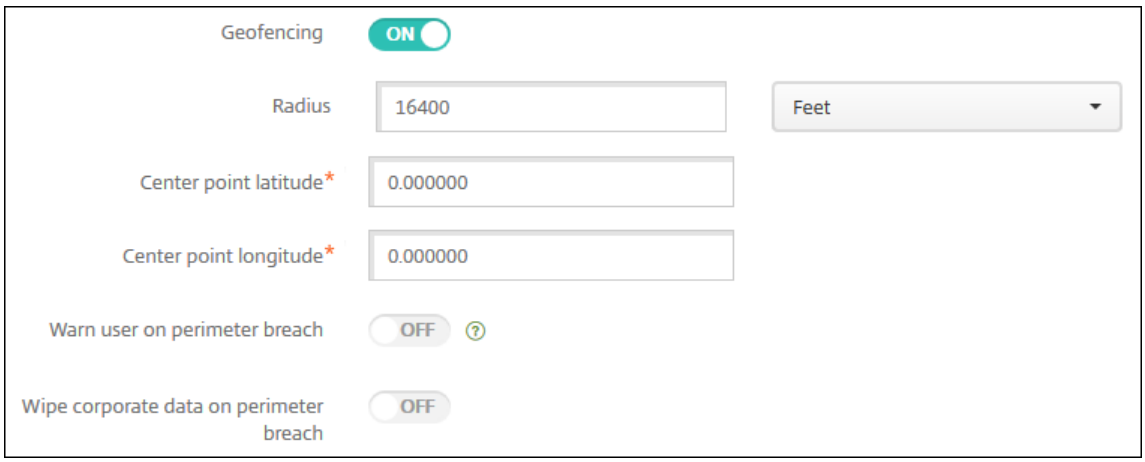
Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Délai max. de localisation :** entrez un chiffre, puis cliquez sur **Secondes** ou **Minutes** pour définir la fréquence à laquelle Citrix Endpoint Management tente de déterminer l'emplacement de l'appareil. Les valeurs valides sont 60–900 secondes ou 1–15 minutes. La valeur par défaut est **1 minute**.
- **Durée du suivi :** entrez un chiffre, puis cliquez sur **Heures** ou **Minutes** pour définir la durée pendant laquelle Citrix Endpoint Management suit l'appareil. Les valeurs valides sont 1 à 10 heures ou 10 à 600 minutes. La valeur par défaut est **6 heures**.
- **Précision :** entrez un chiffre, puis cliquez sur **Mètres**, **Feet** ou **Yards** pour définir la précision du suivi effectué par Citrix Endpoint Management. Les valeurs valides sont 10 à 5000 yards, 30 à 15000 pieds ou 10 à 5000 mètres. La valeur par défaut est **100 mètres** (**328 pieds**).
- **M'avertir si les services de localisation sont désactivés :** sélectionnez cette option si vous voulez que l'appareil envoie un rapport à Citrix Endpoint Management lorsque le GPS est désactivé. La valeur par défaut est **Off**.
- **Géofencing**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



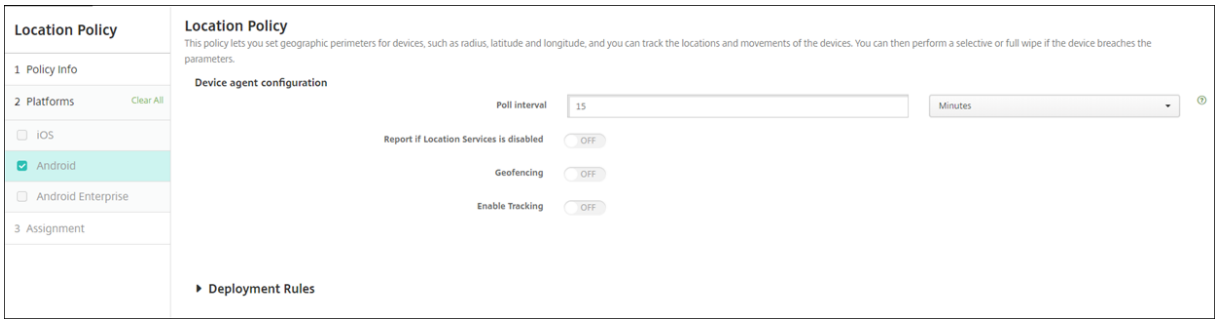
Lorsque vous activez Géofencing, configurez les paramètres suivants :

- **Rayon :** entrez un chiffre, puis cliquez sur les unités à utiliser pour mesurer le rayon. La valeur par défaut est **5000 mètres** (**16400 pieds**). Les valeurs valides pour le rayon sont :
  - 164-16400 feet (pieds)
  - 50–50000 mètres
  - 54-54680 yards
  - 1–31 miles
- **Latitude du point central :** entrez une latitude, par exemple 37.787454, pour définir la latitude du point central du géofencing.
- **Longitude du point central :** entrez une longitude, par exemple 122.402952, pour définir la longitude du point central du géofencing.
- **Avertir l'utilisateur en cas de violation du périmètre :** choisissez d'afficher un message d'avertissement lorsque les utilisateurs violent le périmètre établi. La valeur par défaut est **Off**. Aucune connexion à Citrix Endpoint Management n'est nécessaire pour afficher le message d'avertissement.
- **Effacer les données d'entreprise en cas de violation du périmètre :** indiquez si vous souhaitez effacer les appareils des utilisateurs lorsqu'ils violent le périmètre. La valeur par défaut est **Off**. Lorsque vous activez cette option, le champ **Délai avant l'effacement local** s'affiche.
  - Entrez un chiffre, puis cliquez sur **Secondes** ou **Minutes** pour définir la durée du délai avant l'effacement des données d'entreprise sur les appareils des utilisateurs. Ce délai offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que Citrix Endpoint Management n'efface leurs appareils. La valeur par défaut est **0 seconde**.

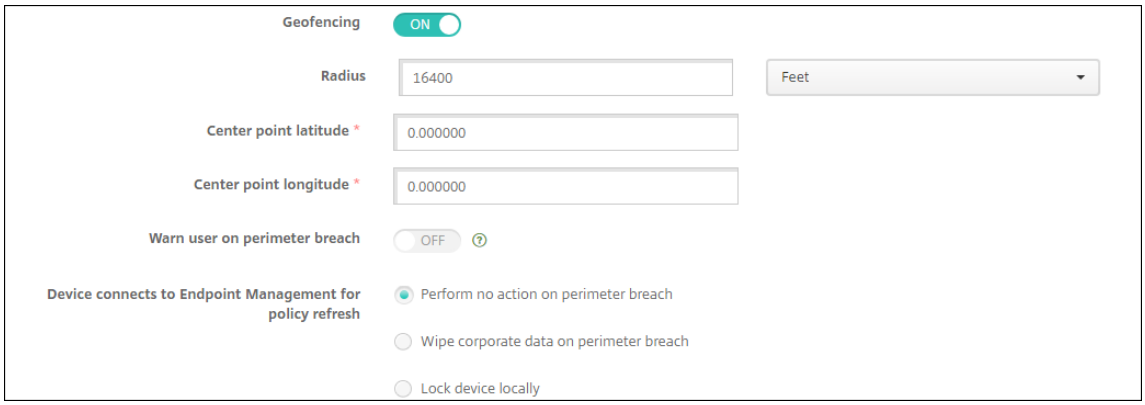
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Android (DA hérité)

La fonction de suivi de la position d'Android nécessite Android 9 et versions supérieures.



- **Echantillonnage :** entrez un chiffre, puis cliquez sur **Minutes**, **Heures** ou **Jours** pour définir la fréquence à laquelle Citrix Endpoint Management tente de déterminer l'emplacement de l'appareil. Les valeurs valides sont 15–1440 minutes, 1–24 heures ou un nombre quelconque de jours. La valeur par défaut est **15 minutes**.
- **M'avertir si les services de localisation sont désactivés :** sélectionnez cette option si vous voulez que l'appareil envoie un rapport à Citrix Endpoint Management lorsque le GPS est désactivé. La valeur par défaut est **Off**.
- **Géofencing**



Lorsque vous activez Géofencing, configurez les paramètres suivants :

- **Rayon :** entrez un chiffre, puis cliquez sur les unités à utiliser pour mesurer le rayon. La valeur par défaut est **5000 mètres** (**16400 pieds**). Les valeurs valides pour le rayon sont :
  - 164–164000 feet
  - 1–50 kilomètres
  - 50–50000 mètres
  - 54-54680 yards
  - 1–31 miles

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Latitude du point central :** entrez une latitude, par exemple 37.787454, pour définir la latitude du point central du géofencing.
- **Longitude du point central :** entrez une longitude, par exemple 122.402952, pour définir la longitude du point central du géofencing.
- **Avertir l'utilisateur en cas de violation du périmètre :** choisissez d'afficher un message d'avertissement lorsque les utilisateurs violent le périmètre établi. La valeur par défaut est **Off**. Aucune connexion à Citrix Endpoint Management n'est nécessaire pour afficher le message d'avertissement.
- **L'appareil se connecte à Citrix Endpoint Management pour actualiser la stratégie :** sélectionnez l'une des options suivantes à exécuter lorsque les utilisateurs violent le périmètre :
  - **N'effectuer aucune action en cas de violation du périmètre :** aucune action n'est prise. Il s'agit de l'option par défaut.
  - **Effacer les données d'entreprise en cas de violation du périmètre :** les données d'entreprise sont effacées après une durée spécifiée. Lorsque vous activez cette option, le champ **Délai avant l'effacement local** s'affiche.
    * Entrez un chiffre, puis cliquez sur **Secondes** ou **Minutes** pour définir la durée du délai avant l'effacement des données d'entreprise sur les appareils des utilisateurs. Ce délai offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que Citrix Endpoint Management n'efface leurs appareils. La valeur par défaut est **0 seconde**.
  - **Verrouiller l'appareil localement :** verrouille les appareils des utilisateurs après une période spécifiée. Lorsque vous activez cette option, le champ **Délai du verrouillage** s'affiche.
    * Entrez un chiffre, puis cliquez sur **Secondes** ou **Minutes** pour définir la durée du délai avant le verrouillage des appareils des utilisateurs. Ce délai offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que Citrix Endpoint Management ne verrouille leurs appareils. La valeur par défaut est **0 seconde**.
- **Activer le suivi :** indiquez si l'appareil suit l'emplacement de l'utilisateur. La valeur par défaut est **Off**.

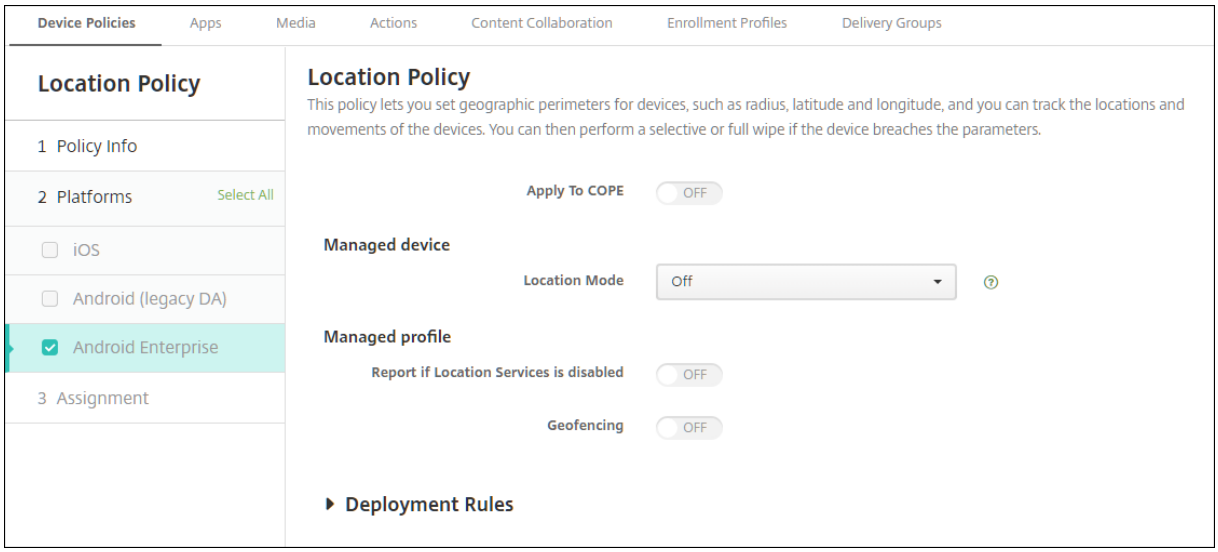
Paramètres Android Enterprise

Pour que le suivi de l'emplacement Android fonctionne, assurez-vous de remplir les conditions suivantes :

- Android 9 ou version ultérieure
- Paramètre Autoriser partage de position activé dans la stratégie Restrictions pour Android Enterprise

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Planification de connexion (Firebase Cloud Messaging recommandé)



Appliquer aux appareils entièrement gérés dotés d'un profil professionnel

Pour les appareils entièrement gérés avec profil de travail (anciennement appelés appareils COPE), seul le paramètre de mode de localisation est disponible.

- **Appliquer aux appareils entièrement gérés avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise :** permet de configurer le mode de localisation pour les appareils entièrement gérés avec profil de travail. Lorsque ce paramètre est activé, configurez les paramètres du profil de travail :
  - **M'avertir si les services de localisation sont désactivés :** sélectionnez cette option si vous voulez que l'appareil envoie un rapport à Citrix Endpoint Management lorsque le GPS est désactivé. La valeur par défaut est **Off**.
  - **Géofencing :** reportez-vous aux paramètres décrits dans cet article sous Appareil géré.

Lorsque l'option **Appliquer aux appareils entièrement gérés avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise** est désactivée, les paramètres s'appliquent à l'appareil géré et au profil de travail, comme indiqué dans les sections suivantes. La valeur par défaut est **Off**.

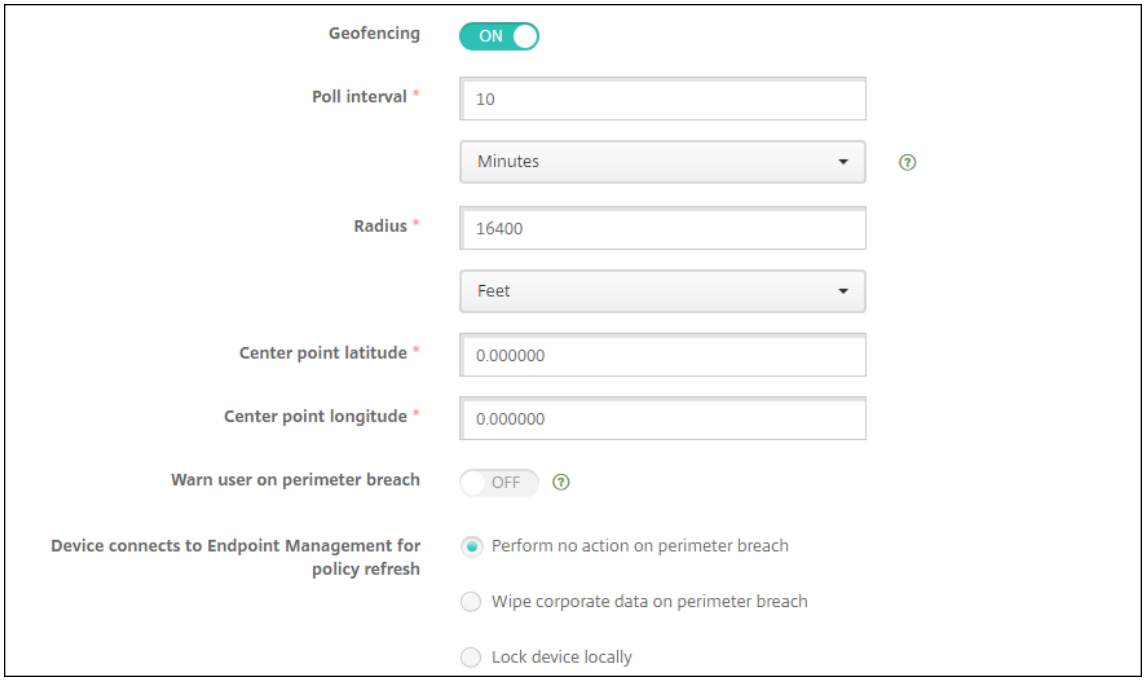
Appareil géré

- **Mode de localisation :** spécifiez le degré de détection de localisation à activer. Vous pouvez utiliser l'action de sécurisation Localiser uniquement lorsque le mode de localisation est défini sur **Haute précision** ou **Économie de batterie**. La valeur par défaut est **Haute précision**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Haute précision :** active toutes les méthodes de détection de localisation, y compris le GPS, les réseaux et autres capteurs.
  - **Capteurs seulement :** active uniquement les capteurs GPS et autres.
  - **Économie de batterie :** active uniquement le fournisseur de localisation réseau.
  - **Désactivé :** désactive la détection de la localisation.

- **Géofencing :**



Lorsque vous activez **Géofencing**, configurez les paramètres suivants :

- **Echantillonnage :** entrez un chiffre, puis cliquez sur **Minutes**, **Heures** ou **Jours** pour définir la fréquence à laquelle Citrix Endpoint Management tente de déterminer l'emplacement de l'appareil. Les valeurs valides sont 1–1440 minutes, 1–24 heures ou un nombre quelconque de jours. La valeur par défaut est **10 minutes**. Si la valeur définie est inférieure à 10 minutes, cela peut avoir un impact négatif sur l'autonomie de la batterie.
- **Rayon :** entrez un chiffre, puis cliquez sur les unités à utiliser pour mesurer le rayon. La valeur par défaut est **5000 mètres** (**16400 pieds**). Les valeurs valides pour le rayon sont :
  - 164–164000 feet
  - 1–50 kilomètres
  - 50–50000 mètres
  - 54-54680 yards
  - 1–31 miles
- **Latitude du point central :** entrez une latitude, par exemple 37.787454, pour définir la latitude du point central du géofencing. Pour vérifier la valeur, accédez à **Gérer > Appareils**, sélection-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

nez l'appareil, cliquez sur **Sécurité**, puis cliquez sur **Localiser**. Après avoir localisé l'appareil, Citrix Endpoint Management signale l'emplacement de l'appareil dans **Détails de l'appareil > Général** sous **Sécurité**.

- **Longitude du point central :** entrez une longitude, par exemple 122.402952, pour définir la longitude du point central du géofencing.
- **Avertir l'utilisateur en cas de violation du périmètre :** choisissez d'afficher un message d'avertissement lorsque les utilisateurs violent le périmètre établi. La valeur par défaut est **Off**. Aucune connexion à Citrix Endpoint Management n'est nécessaire pour afficher le message d'avertissement.
- **L'appareil se connecte à Citrix Endpoint Management pour actualiser la stratégie :** sélectionnez l'une des options suivantes à exécuter lorsque les utilisateurs violent le périmètre :
  - **N'effectuer aucune action en cas de violation du périmètre :** aucune action n'est prise. Il s'agit du réglage par défaut.
  - **Effacer les données d'entreprise en cas de violation du périmètre :** les données d'entreprise sont effacées après une durée spécifiée. Lorsque vous activez cette option, le champ **Délai avant l'effacement local** s'affiche.
    - Entrez un chiffre, puis cliquez sur **Secondes** ou **Minutes** pour définir la durée du délai avant l'effacement des données d'entreprise sur les appareils des utilisateurs. Ce délai offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que Citrix Endpoint Management n'efface leurs appareils. La valeur par défaut est **0 seconde**.
  - **Verrouiller l'appareil localement :** verrouille les appareils des utilisateurs après une période spécifiée. Lorsque vous activez cette option, le champ **Délai du verrouillage** s'affiche.
    - Entrez un chiffre, puis cliquez sur **Secondes** ou **Minutes** pour définir la durée du délai avant le verrouillage des appareils des utilisateurs. Ce délai offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que Citrix Endpoint Management ne verrouille leurs appareils. La valeur par défaut est **0 seconde**.

Profil de travail

- **M'avertir si les services de localisation sont désactivés :** sélectionnez cette option si vous voulez que l'appareil envoie un rapport à Citrix Endpoint Management lorsque le GPS est désactivé. La valeur par défaut est **Off**.
- **Géofencing :** reportez-vous aux paramètres décrits dans cet article sous Appareil géré.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie de message sur l'écran de verrouillage

December 9, 2021

La stratégie Message sur l'écran de verrouillage vous permet de définir les messages à afficher sur les appareils iOS suivants lorsqu'ils sont perdus :

- La fenêtre de connexion des iPads partagés
- L'écran de verrouillage des appareils iOS supervisés

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Informations sur l'étiquette d'inventaire de l'appareil :** le numéro d'identification de l'appareil. Les appareils Apple tronquent les chaînes longues ; veillez donc à tester une chaîne avant de déployer la stratégie en production. La longueur de la chaîne dépend du modèle de l'appareil Apple et des paramètres Apple qui peuvent changer.
- **Note de bas de page sur la fenêtre de connexion et l'écran de verrouillage :** informations, telles qu'une adresse ou d'autres coordonnés, permettant de renvoyer l'appareil. Par exemple, votre message peut être sous la forme « Si perdu, retourner à ». Les appareils Apple tronquent les chaînes longues ; veillez donc à tester une chaîne avant de déployer la stratégie en production. La longueur de la chaîne dépend du modèle de l'appareil Apple et des paramètres Apple qui peuvent changer.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

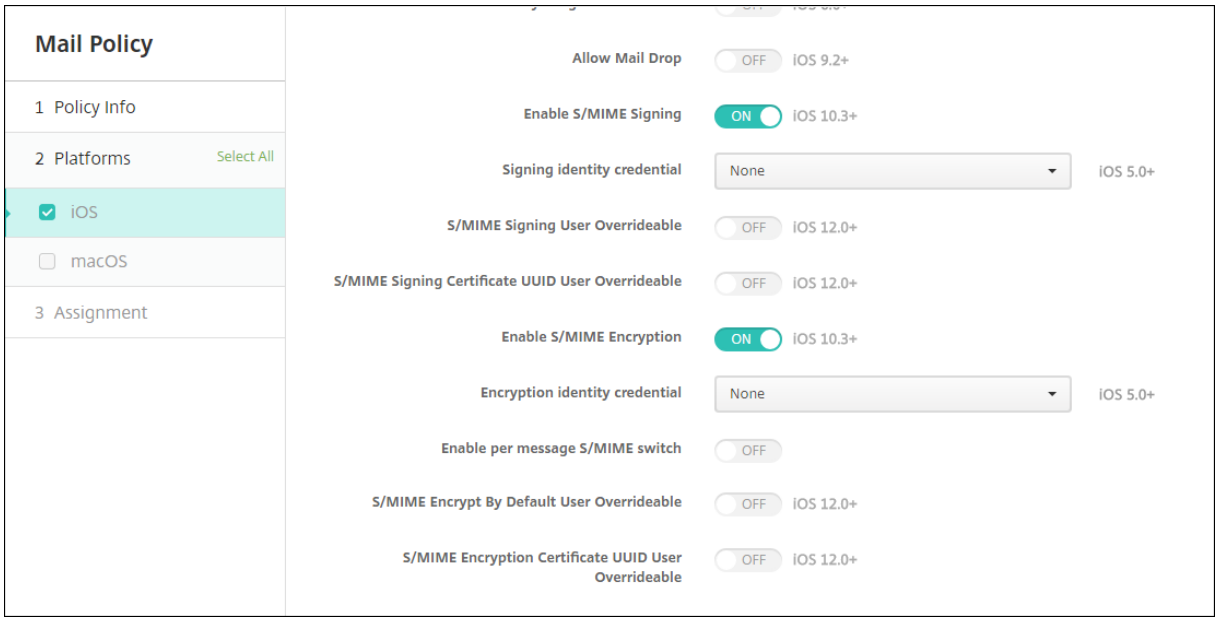
Stratégie de messagerie

November 29, 2023

Vous pouvez ajouter une stratégie de messagerie dans Citrix Endpoint Management pour configurer un compte de messagerie sur les appareils iOS ou macOS.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS et macOS



- **Description du compte :** entrez une description pour le compte ; elle apparaît dans les applications de messagerie et de paramètres. Ce champ est obligatoire.
- **Type de compte :** cliquez sur **IMAP** ou **POP** pour sélectionner le protocole à utiliser pour les comptes d'utilisateur. La valeur par défaut est **IMAP**. Lorsque vous sélectionnez le protocole **POP**, l'option **Préfixe chemin** disparaît.
- **Préfixe chemin :** entrez **INBOX** ou le chemin d'accès à votre compte de messagerie IMAP. Ce champ est obligatoire.
- **Nom d'affichage de l'utilisateur :** entrez le nom d'utilisateur à utiliser dans les messages, etc. Ce champ est obligatoire.
- **Adresse électronique :** entrez l'adresse e-mail du compte. Ce champ est obligatoire.
- **Paramètres du courrier entrant**
  - **Nom d'hôte du serveur de messagerie :** entrez le nom d'hôte ou l'adresse IP du serveur de messagerie du courrier entrant. Ce champ est obligatoire.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Port du serveur de messagerie :** entrez le numéro de port du serveur de courrier entrant. Le paramètre par défaut est **143** Ce champ est obligatoire.
  - **Nom d'utilisateur :** entrez le nom d'utilisateur du compte de messagerie. Ce nom est généralement le même que l'adresse e-mail à hauteur du caractère @. Ce champ est obligatoire.
  - **Type d'authentification :** choisissez le type d'authentification à utiliser. La valeur par défaut est **Mot de passe**. Lorsque **Aucun** est sélectionné, le champ **Mot de passe** suivant disparaît.
  - **Mot de passe :** entrez un mot de passe pour le serveur de messagerie de courrier entrant (facultatif).
  - **Utiliser SSL :** sélectionnez cette option pour que le serveur de messagerie du courrier entrant utilise l'authentification SSL. La valeur par défaut est **Off**.

- **Paramètres de messagerie du courrier sortant**
  - **Nom d'hôte du serveur de messagerie :** entrez le nom d'hôte ou l'adresse IP du serveur de messagerie du courrier sortant. Ce champ est obligatoire.
  - **Port du serveur de messagerie :** entrez le numéro de port du serveur de courrier sortant. Si vous n'entrez pas de numéro de port, le port par défaut du protocole donné est utilisé.
  - **Nom d'utilisateur :** entrez le nom d'utilisateur du compte de messagerie. Ce nom est généralement le même que l'adresse e-mail à hauteur du caractère @. Ce champ est obligatoire.
  - **Type d'authentification :** choisissez le type d'authentification à utiliser. La valeur par défaut est **Mot de passe**.
  - **Mot de passe :** entrez un mot de passe pour le serveur de messagerie de courrier sortant (facultatif).
  - **Mot de passe sortant identique au mot de passe entrant :** sélectionnez cette option pour spécifier si les mots de passe entrants et sortants sont les mêmes. La valeur par défaut est **Désactivé**, ce qui signifie que les mots de passe sont différents.
  - **Utiliser SSL :** sélectionnez cette option pour que le serveur de messagerie du courrier sortant utilise l'authentification SSL. La valeur par défaut est **Off**.

- **Stratégie**
  - **Autoriser le déplacement des e-mails entre les comptes :** sélectionnez cette option pour permettre aux utilisateurs de :
    * déplacer un e-mail de ce compte vers un autre
    * transférer un e-mail à partir d'un autre compte
    * répondre à partir d'un compte différent

    La valeur par défaut est **Off**.
  - **N'envoyer des e-mails que depuis l'application de messagerie :** sélectionnez cette option si vous voulez que les utilisateurs soient uniquement autorisés à envoyer des e-mails

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

avec l'application de messagerie iOS.

- **Désactiver la synchronisation des e-mails récents :** sélectionnez cette option pour empêcher les utilisateurs de synchroniser les adresses récentes. La valeur par défaut est **Off**. Cette option s'applique uniquement à iOS 6.0 et versions ultérieures.
- **Autoriser Mail Drop :** sélectionnez cette option pour autoriser l'utilisation d'Apple Mail Drop pour les appareils exécutant iOS 9.2 ou version ultérieure. La valeur par défaut est **Off**.
- **Activer signature S/MIME :** indiquez si ce compte prend en charge la signature S/MIME. La valeur par défaut est **On**. Lorsque la valeur est définie sur **Activé**, les champs suivants apparaissent.
  - **Informations d'identification de l'identité de signature :** choisissez les informations d'identification de signature à utiliser.
  - **Signature S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer et désactiver la signature S/MIME dans les paramètres de leurs appareils. La valeur par défaut est **Off**. Cette option s'applique à iOS 12.0 et versions ultérieures.
  - **UUID du certificat de signature S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent sélectionner les informations d'identification de signature à utiliser dans les paramètres de leurs appareils. La valeur par défaut est **Off**. Cette option s'applique à iOS 12.0 et versions ultérieures.
- **Activer chiffrement S/MIME :** sélectionnez cette option si vous souhaitez que ce compte prenne en charge le chiffrement S/MIME. La valeur par défaut est **Off**. Lorsque la valeur est définie sur **Activé**, les champs suivants apparaissent.
  - **Informations d'identification de l'identité de chiffrement :** dans la liste, sélectionnez les informations d'identification de chiffrement à utiliser.
  - **Activer commutateur de chiffrement S/MIME par message :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer ou désactiver le chiffrement S/MIME pour chaque message composé. La valeur par défaut est **Off**.
  - **Chiffrement S/MIME par défaut remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent choisir si S/MIME est activé par défaut dans les paramètres de leurs appareils. La valeur par défaut est **Off**. Cette option s'applique à iOS 12.0 et versions ultérieures.
  - **UUID du certificat de chiffrement S/MIME remplaçable par l'utilisateur :** si cette option est définie sur **Activé**, les utilisateurs peuvent activer et désactiver l'identité de chiffrement S/MIME dans les paramètres de leurs appareils. La valeur par défaut est **Off**. Cette option s'applique à iOS 12.0 et versions ultérieures.

- **Paramètre de stratégie**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Supprimer la stratégie :** pour supprimer la stratégie ultérieurement, vous pouvez configurer ce paramètre en utilisant les options **Sélectionner une date** ou **Délai avant suppression (en jours)**.
- **Autoriser l'utilisateur à supprimer la stratégie :** autorisez les utilisateurs à supprimer la stratégie de messagerie en utilisant les options **Toujours**, **Code secret requis** ou **Jamais**. Uniquement disponible pour macOS.
- **Étendue du profil :** pour macOS uniquement, choisissez si la stratégie s'applique au niveau **Utilisateur** ou à l'ensemble du **Système**.

Stratégie Configurations gérées

March 1, 2024

La stratégie Configurations gérées contrôle de nombreuses options de configuration et de restriction d'applications. Vous créez cette stratégie pour chaque application Android Enterprise que vous souhaitez contrôler.

Le développeur de l'application définit les options disponibles pour une application et les info-bulles. Si une info-bulle mentionne l'utilisation d'une « valeur basée sur un modèle », utilisez plutôt la macro Citrix Endpoint Management correspondante. Pour plus d'informations, consultez la page Remote configuration overview (sur le site développeur Android) et la section Macros.

Les paramètres de configuration de l'application peuvent inclure des éléments tels que :

- Paramètres de l'application de messagerie
- Autoriser ou bloquer les URL d'un navigateur Web
- Possibilité de contrôler la synchronisation du contenu de l'application via une connexion cellulaire ou uniquement via une connexion Wi-Fi

Pour plus d'informations sur les paramètres qui apparaissent pour vos applications, contactez le développeur de l'application.

Logiciels requis

- Terminez les tâches de configuration d'Android Entreprise sur Google et connectez Android Entreprise à Google Play d'entreprise. Pour plus d'informations, consultez la section Android Enterprise.
- Ajoutez des applications Android Enterprise à Citrix Endpoint Management. Pour plus d'informations, consultez la section Ajout d'applications à Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Configuration requise pour les réseaux Per App VPN

Pour créer une stratégie Per App VPN pour AE, vous devez effectuer des étapes supplémentaires, en plus de configurer la stratégie de configurations gérées. En outre, vous devez vérifier que les conditions préalables suivantes sont remplies :

- NetScaler Gateway sur site
- Les applications suivantes sont installées sur l'appareil :
  - Citrix SSO
  - Citrix Secure Hub

Voici un workflow général pour configurer une stratégie Per App VPN pour les appareils AE :

1. Configurez un profil VPN comme décrit dans cet article.
2. Configurez Citrix ADC pour accepter le trafic provenant du réseau Per App VPN. Pour de plus amples informations, consultez la section Full VPN setup on NetScaler Gateway.

Limitations

Les limitations suivantes s'appliquent au Per App VPN dans l'environnement Android Enterprise sur les appareils Android 11+ en raison des restrictions de visibilité des packages introduites dans Android 11 :

- Si une application figurant dans la liste des applications autorisées/refusées est déployée sur un appareil après le début de la session VPN, l'utilisateur final doit redémarrer la session VPN pour que l'application puisse acheminer son trafic via la session VPN.
- Si un Per App VPN est utilisé via une session VPN Always On, après avoir installé une nouvelle application sur l'appareil, l'utilisateur final doit redémarrer le profil professionnel ou l'appareil pour que le trafic de l'application soit acheminé via la session VPN.

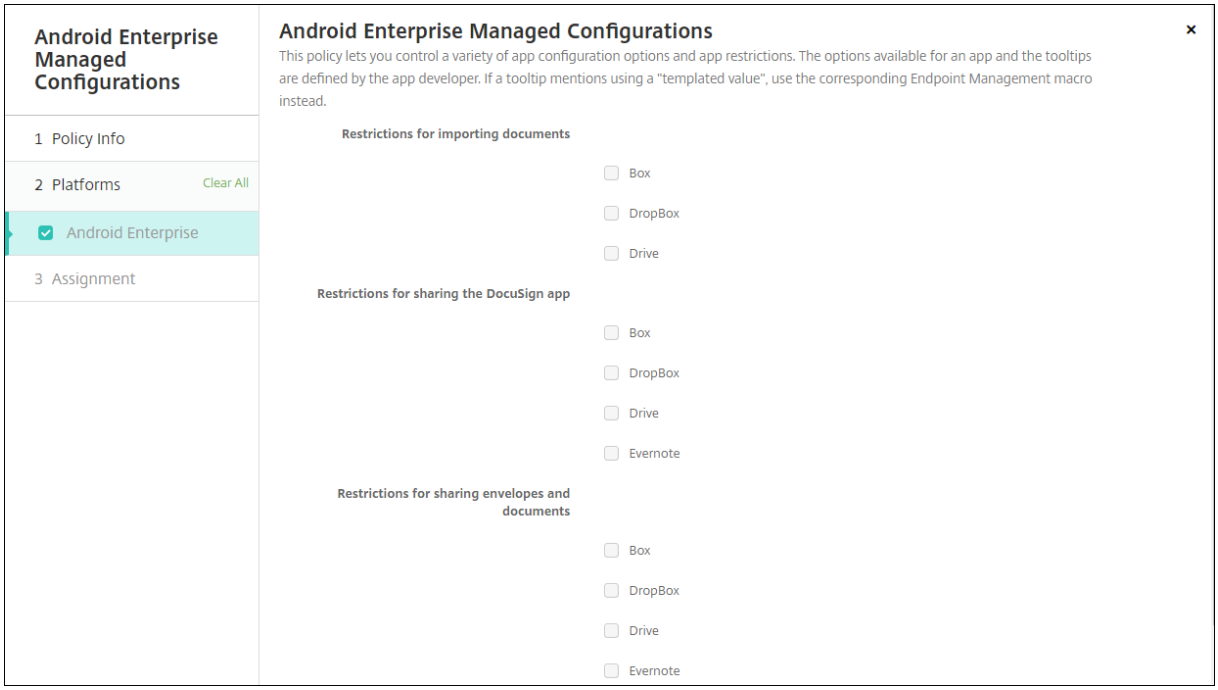
> **Remarque :**
>
> Ces limitations ne s'appliquent pas si vous utilisez Citrix SSO pour Android 23.8.1 ou des versions ultérieures. Pour plus d'informations, consultez Redémarrage automatique du VPN Always On.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Android Enterprise

Après avoir choisi d'ajouter une stratégie Configurations gérées, une invite permettant de sélectionner une application s'affiche. Si aucune application Android Enterprise n'a été ajoutée à Citrix Endpoint Management, vous ne pouvez pas continuer.

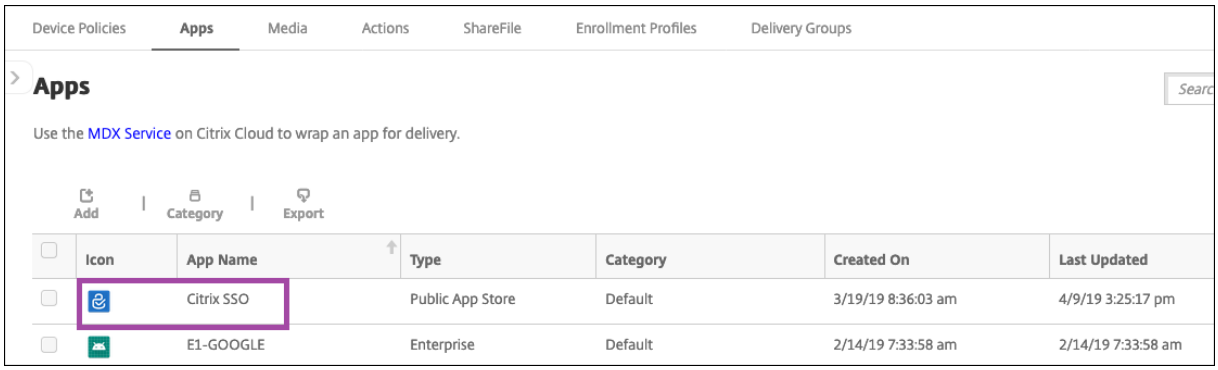
Après avoir sélectionné une application, configurez les paramètres de la stratégie. Les paramètres sont spécifiques à chaque application.



Configurer les profils VPN pour Android Enterprise

Rendez les profils VPN disponibles pour les appareils Android Enterprise à l'aide de l'application Citrix SSO avec la stratégie de configurations gérées.

Commencez par ajouter Citrix SSO à la console Citrix Endpoint Management en tant qu'application du magasin Google Play. Consultez la section Ajouter une application de magasin public.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Regardez cette vidéo pour en savoir plus :

Créer une configuration gérée par Android Enterprise pour Citrix SSO

Configurez la stratégie Configurations gérées afin de créer des profils VPN. Les appareils sur lesquels l'application Citrix SSO est installée et la stratégie déployée peuvent accéder aux profils VPN que vous créez.

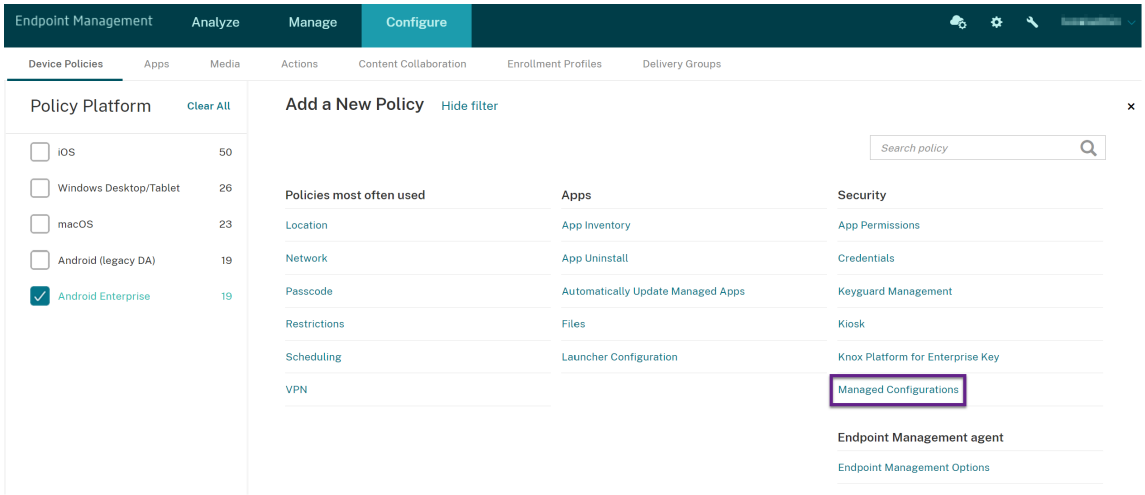
Citrix Endpoint Management utilise le certificat utilisateur dans le magasin de clés de l'appareil si :

- NetScaler Gateway est configuré pour l'authentification par certificat.
- L'option **Délivrer un certificat utilisateur pour l'authentification** est activée dans la page Citrix Endpoint Management **Paramètres > NetScaler Gateway**.

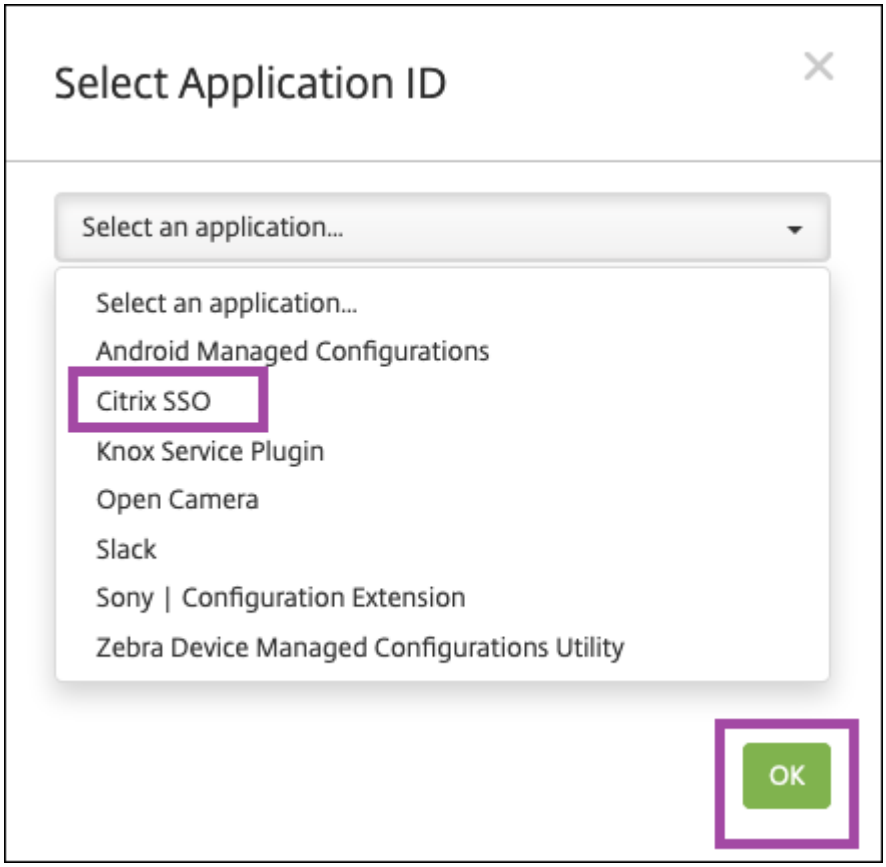
Vous avez besoin du nom de domaine complet et du port NetScaler Gateway.

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Stratégies d'appareil**. Cliquez sur **Ajouter**.
2. Sélectionnez **Android Enterprise**. Cliquez sur **Configurations gérées**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

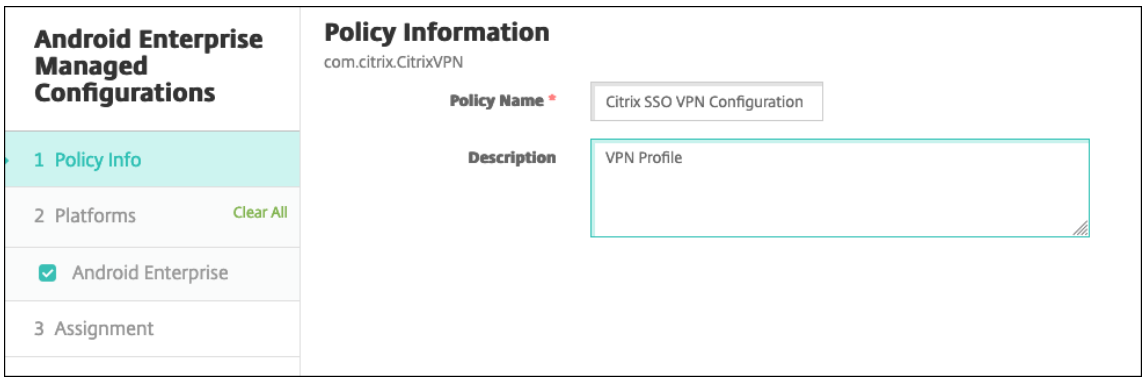


3. Lorsque la fenêtre **Sélectionner un ID d'application** s'affiche, choisissez **Citrix SSO** dans la liste et cliquez sur **OK**.



4. Saisissez un nom et une description pour votre configuration VPN Citrix SSO. Cliquez sur **Suivant**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Configurez les paramètres de profil VPN.

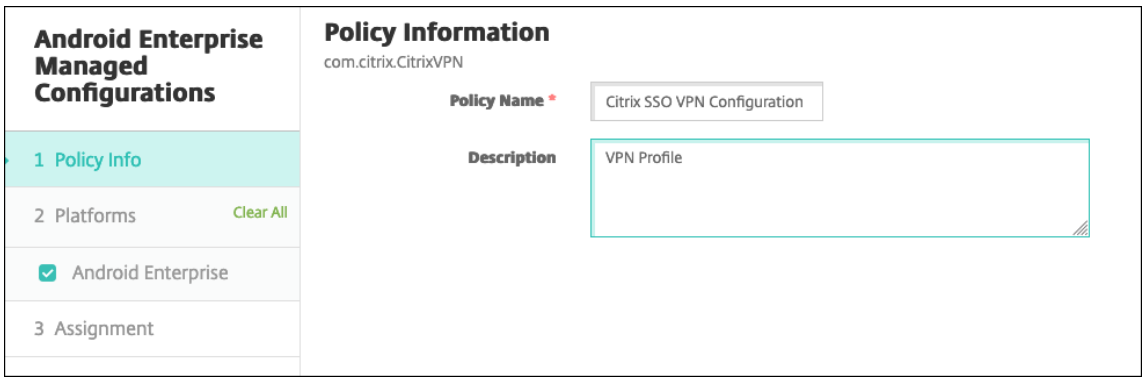
   - **Nom du profil VPN :** saisissez un nom pour le profil VPN. Si vous créez plusieurs profils VPN, utilisez un nom unique pour chaque profil. Si vous ne fournissez pas de nom, l'adresse que vous avez spécifiée dans le champ **Adresse du serveur** est utilisée comme nom de profil VPN.
   - **Adresse du serveur (*) :** saisissez votre nom de domaine complet NetScaler Gateway. Si le port NetScaler Gateway n'est pas 443, saisissez également le port. Utilisez le format URL. Par exemple, `https://gateway.mycompany.com:8443`.
   - **Nom d'utilisateur (facultatif) :** indiquez le nom d'utilisateur que les utilisateurs utilisent pour s'authentifier auprès de NetScaler Gateway. Vous pouvez utiliser la macro Citrix Endpoint Management {user.username} pour ce champ. (Consultez Macros.) Si vous ne fournissez pas de nom d'utilisateur, les utilisateurs sont invités à fournir un nom d'utilisateur lors de la connexion à NetScaler Gateway.
   - **Mot de passe (facultatif) :** indiquez le mot de passe que les utilisateurs utilisent pour s'authentifier auprès de NetScaler Gateway. Si vous ne fournissez pas de mot de passe, les utilisateurs sont invités à fournir un mot de passe lors de la connexion à NetScaler Gateway.
   - **Alias de certificat (facultatif) :** saisissez un alias de certificat. L'alias de certificat permet à l'application d'accéder plus facilement au certificat. Lorsque le même alias de certificat est utilisé avec la stratégie d'informations d'identification, l'application récupère le certificat et authentifie le VPN sans aucune action des utilisateurs.
   - **Pins de certificat Gateway (facultatif) :** objet JSON décrivant les pins de certificat utilisés pour NetScaler Gateway. Exemple de valeur : `{ "hash-alg": "sha256" , "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`. Pour plus d'informations, consultez la section Certificate pinning NetScaler Gateway avec Android Citrix SSO.
   - **Type de VPN par application (facultatif) :** si vous utilisez un VPN par application pour

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

restreindre les applications qui utilisent ce VPN, vous pouvez configurer ce paramètre. Si vous sélectionnez **Autoriser**, le trafic réseau pour les noms de packages d'applications répertoriés dans la **liste des applications Per App VPN** est acheminé via le VPN. Le trafic réseau de toutes les autres applications est acheminé en dehors du VPN. Si vous sélectionnez **Désactiver**, le trafic réseau pour les noms de packages d'applications répertoriés dans la **liste des applications Per App VPN** est acheminé en dehors du VPN. Le trafic réseau de toutes les autres applications est acheminé via le VPN. La valeur par défaut est **Autoriser**.

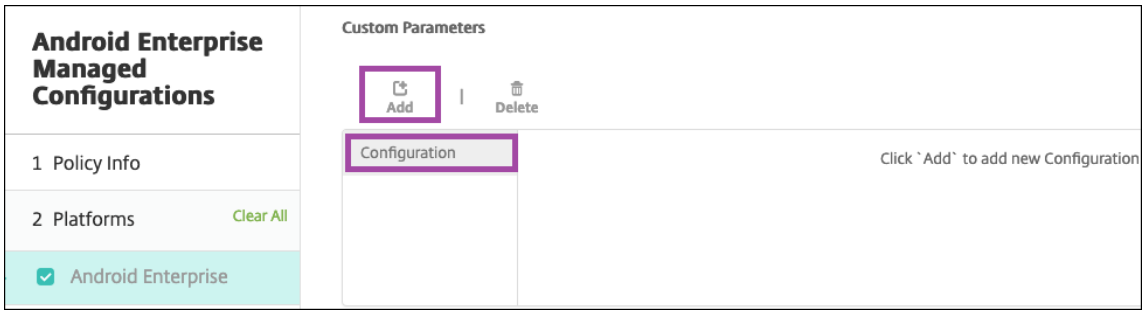
- **Liste des applications Per App VPN :** liste des applications dont le trafic est autorisé ou bloqué sur le VPN en fonction de la valeur définie pour **Type de VPN par application**. Répertoriez les noms de packages d'applications en les séparant par des virgules ou des points-virgules. Les noms de packages d'applications sont sensibles à la casse et doivent apparaître sur cette liste tels qu'ils figurent dans Google Play Store. Cette liste est facultative. Gardez cette liste vide pour le provisioning de VPN à l'échelle de l'appareil.
- **Profil VPN par défaut :** saisissez le nom du profil VPN à utiliser lorsque les utilisateurs touchent le bouton de connexion dans l'application Citrix SSO au lieu d'un profil spécifique. Si ce champ est vide, le profil principal est utilisé pour la connexion. Si un seul profil est configuré, il est marqué comme profil par défaut. Pour un VPN Always On, ce champ doit être défini sur le nom du profil VPN à utiliser pour établir un VPN Always On.
- **Désactiver les profils utilisateur :** si ce paramètre est activé, les utilisateurs ne peuvent pas créer leurs propres VPN sur leurs appareils. Si ce paramètre est désactivé, les utilisateurs peuvent créer leurs propres VPN sur leurs appareils. La valeur par défaut est Off.
- **Bloquer les serveurs non approuvés :** ce paramètre est désactivé dans l'un des scénarios suivants :
  - Lorsque vous utilisez un certificat auto-signé pour NetScaler Gateway
  - Lorsque le certificat racine de l'autorité de certification qui émet le certificat NetScaler Gateway ne figure pas dans la liste d'autorité de certification système

  Si ce paramètre est activé, le système d'exploitation Android valide le certificat NetScaler Gateway. Si la validation échoue, la connexion n'est pas autorisée. La valeur par défaut est Activé.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

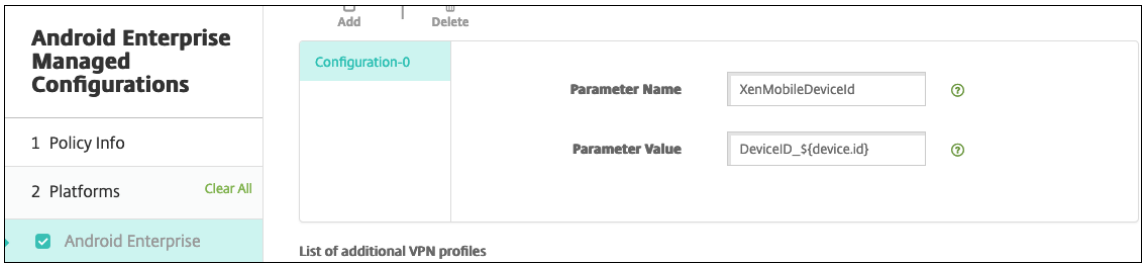
6. Vous pouvez également créer des paramètres personnalisés. Les paramètres personnalisés **XenMobileDeviceId** et **UserAgent** sont pris en charge. Sélectionnez la configuration VPN actuelle et cliquez sur **Ajouter**.



Nom du paramètre	Description	Valeur
XenMobileDeviceId	Il s'agit de l'ID d'appareil à utiliser pour la vérification d'accès au réseau en fonction de l'inscription de l'appareil dans Citrix Endpoint Management. Si Citrix Endpoint Management s'inscrit et gère l'appareil, la connexion VPN est autorisée. Sinon, l'authentification est refusée au moment de l'établissement du VPN.	Pour que Citrix Endpoint Management détermine l'état d'inscription et de gestion des appareils, la valeur de XenMobileDeviceId est définie sur `DeviceID_${ device.id }`.
UserAgent	Ce texte a été ajouté à l'en-tête HTTP de l'agent utilisateur pour effectuer une vérification supplémentaire sur NetScaler Gateway. La valeur de ce texte est ajoutée à l'en-tête HTTP de l'agent utilisateur par l'application Citrix SSO lors de la communication avec NetScaler Gateway.	saisissez le texte à ajouter à l'en-tête HTTP de l'agent utilisateur. Ce texte doit être conforme aux spécifications HTTP de l'agent utilisateur.

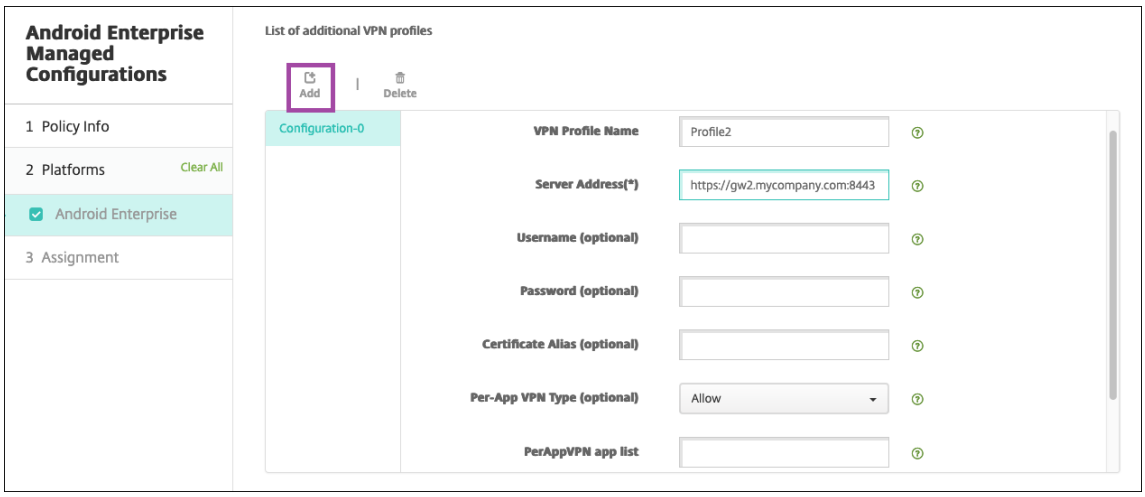
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom du paramètre	Description	Valeur
EnableDebugLogging	Activer la journalisation de débogage sur l'application Citrix SSO pour résoudre les problèmes de connectivité VPN en cas de VPN Always On. Vous pouvez l'activer dans toutes les configurations VPN gérées. La journalisation du débogage prend effet lorsque les configurations gérées sont traitées.	**True** : active la journalisation du débogage. Valeur par défaut : **False**



Pour créer un autre paramètre personnalisé, cliquez à nouveau sur **Ajouter**.

7. Vous pouvez également créer des configurations de profil VPN supplémentaires. Cliquez sur **Ajouter** dans la liste des configurations. Une nouvelle configuration apparaît dans la liste. Sélectionnez la nouvelle configuration et répétez l'étape 5 et, éventuellement, l'étape 6.



8. Lorsque vous avez créé tous les profils VPN de votre choix, cliquez sur **Suivant**.
9. Configurez les règles de déploiement associées à cette configuration gérée pour Citrix SSO.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

10. Cliquez sur **Enregistrer**.

Cette configuration gérée pour Citrix SSO apparaît désormais dans la liste des stratégies d'appareil configurées.

Pour activer Always On pour les profils VPN que vous avez configurés, définissez la stratégie Options de Citrix Endpoint Management.

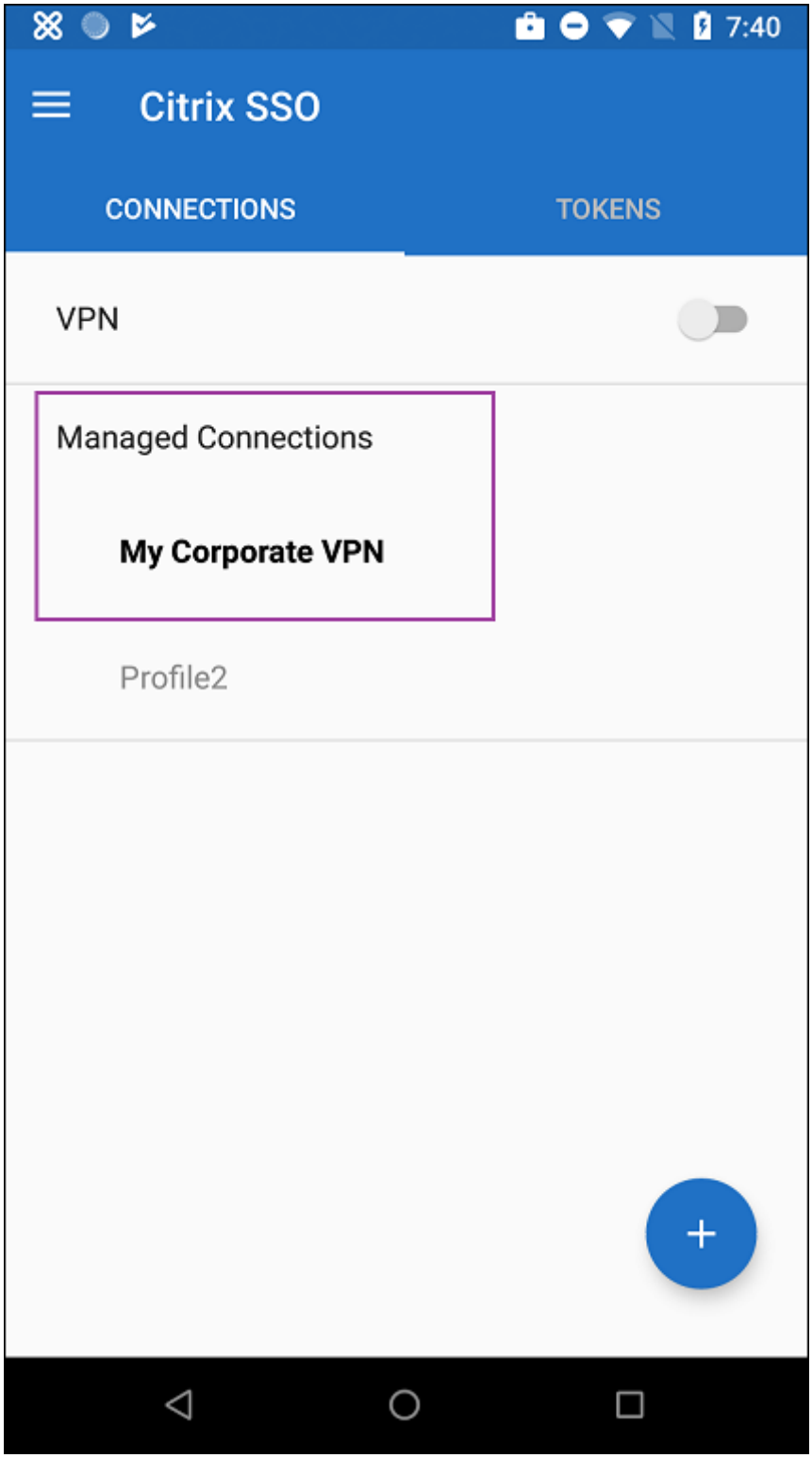
> **Remarque :**
>
> Citrix Secure Hub 19.5.5 ou supérieur est requis pour VPN Always-On pour Android Entreprise.

Accéder aux profils VPN à partir de l'appareil

Pour accéder aux profils VPN que vous avez créés, les utilisateurs Android Enterprise installent Citrix SSO à partir du Google Play Store d'entreprise.

Le ou les profils VPN que vous avez configurés apparaissent dans la zone **Connexions gérées** de l'application. Les utilisateurs touchent le profil VPN pour se connecter à l'aide de ce profil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Une fois les utilisateurs authentifiés et connectés, une coche apparaît en regard du profil VPN. L'icône de clé indique que le VPN est connecté.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Gérer les appareils Zebra Android à l'aide de Zebra OEMConfig

Gérez les appareils Zebra Android à l'aide de l'outil d'administration OEMConfig de Zebra Technologies. Pour plus d'informations sur l'application Zebra OEMConfig, consultez le site Web Zebra Technologies.

Citrix Endpoint Management prend en charge Zebra OEMConfig version 9.2 et supérieure. Pour plus d'informations sur la configuration système requise pour installer Zebra OEMConfig sur les appareils, consultez Configuration d'OEMConfig sur le site Web de Zebra Technologies.

Nous prenons actuellement en charge les appareils Zebra suivants :

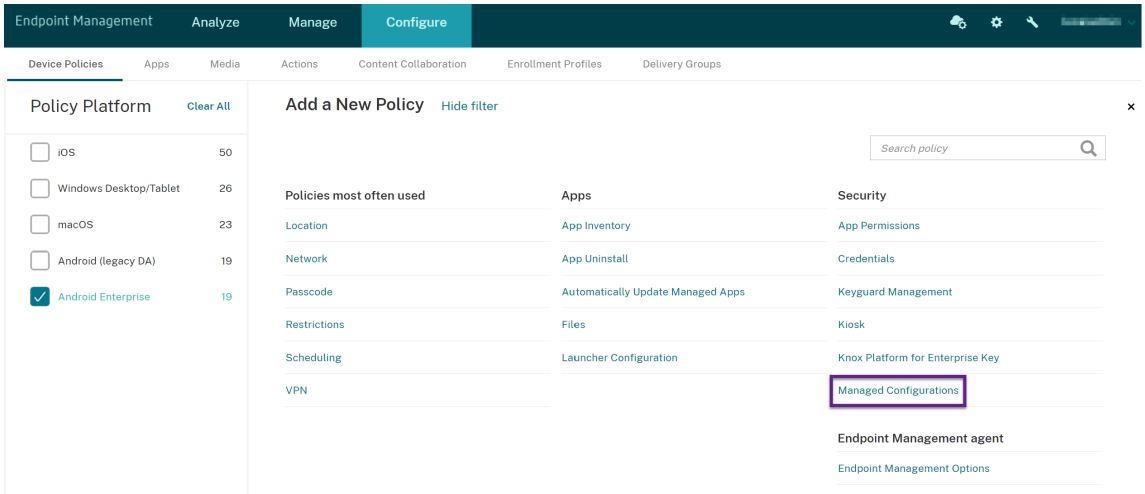
- EC50, EC55, ET56
- TC52x, TC52x-HC
- TC52ax, TC52ax-HC
- TC57x

Pour démarrer : dans la console Citrix Endpoint Management, ajoutez l'application Zebra OEMConfig en tant qu'application Google Play Store. Voir Ajouter une application de magasin public.

Créer une configuration gérée par Android Enterprise pour l'application Zebra OEMConfig

Configurez la stratégie Configurations gérées pour l'application Zebra OEMConfig. La stratégie s'applique aux appareils Zebra sur lesquels l'application Zebra OEMConfig est installée et la stratégie est déployée.

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Stratégies d'appareil**. Cliquez sur **Ajouter**.
2. Sélectionnez **Android Enterprise**. Cliquez sur **Configurations gérées**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Lorsque la fenêtre **Sélectionner l'ID d'application** apparaît, choisissez **ZebraOEMConfig powered by MX** dans la liste et cliquez sur **OK** .
4. Saisissez un nom et une description pour votre configuration Zebra OEMConfig. Cliquez sur **Suivant**.
5. Saisissez un nom pour la configuration de Zebra OEMConfig.
6. Configurez les paramètres disponibles. Par exemple :
   - Pour désactiver l'appareil photo situé à l'avant de l'appareil, sélectionnez **Camera Configuration** et définissez **Use of Front Camera** sur **Off**.
   - Pour modifier le format de l'heure des appareils, sélectionnez **Clock Configuration** et définissez **Time Format** sur **12** (12 heures) ou **24** (24 heures).

Pour obtenir une liste et une description de toutes les configurations disponibles, consultez Zebra Managed Configurations sur le site Web de Zebra Technologies.

1. Vous pouvez également créer des configurations Zebra OEMConfig supplémentaires. Cliquez sur **Ajouter** dans la liste des configurations. Une nouvelle configuration apparaît dans la liste. Sélectionnez la nouvelle configuration et configurez les paramètres.
2. Lorsque vous avez créé toutes les configurations Zebra OEMConfig souhaitées, cliquez sur **Suivant**.
3. Configurez les règles de déploiement associées à cette configuration gérée pour Zebra OEMConfig.
4. Cliquez sur **Enregistrer**.

Stratégies de domaines gérés

December 9, 2021

Vous pouvez définir des domaines gérés qui s'appliquent à la messagerie et au navigateur Safari. Les domaines gérés vous aident à protéger les données d'entreprise en contrôlant les applications qui peuvent ouvrir des documents téléchargés depuis des domaines à l'aide de Safari.

Pour les appareils iOS supervisés, vous spécifiez :

- des adresses URL ou des sous-domaines pour contrôler la manière dont les utilisateurs peuvent ouvrir des documents, des pièces jointes et des téléchargements à partir du navigateur.
- des adresses URL à partir desquelles les utilisateurs peuvent enregistrer des mots de passe dans Safari.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour plus d'informations sur la définition d'un appareil iOS en mode supervisé, consultez la section Déployer des appareils à l'aide d'Apple Configurator 2.

Lorsqu'un utilisateur envoie un e-mail à un destinataire dont le domaine n'est pas sur la liste des domaines de messagerie gérés, un message s'affiche sur l'appareil de l'utilisateur pour l'avertir qu'il envoie un message à un utilisateur en dehors de votre domaine d'entreprise.

Pour les éléments tels que document, pièce jointe ou téléchargement : lorsqu'un utilisateur tente d'ouvrir un élément à l'aide de Safari depuis un domaine Web se trouvant sur la liste de domaines gérés, l'application d'entreprise appropriée ouvre l'élément. Si l'élément ne provient pas d'un domaine Web se trouvant sur la liste des domaines Web gérés, l'utilisateur ne peut pas ouvrir l'élément avec une application d'entreprise ; il doit utiliser une application non gérée, personnelle.

Pour les appareils supervisés, même si vous ne spécifiez pas de domaines de remplissage automatique du mot de passe Safari : si l'appareil est configuré pour multi-utilisateurs éphémères, les utilisateurs ne peuvent pas enregistrer de mots de passe. Toutefois, si l'appareil n'est pas configuré pour multi-utilisateurs éphémères, les utilisateurs peuvent enregistrer tous les mots de passe.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

Pour spécifier des domaines :

Format	Description
`example.com`	Traitez n'importe quel chemin sous `example.com` comme géré, mais pas `site.example.com/`.
`foo.example.com`	Traitez n'importe quel chemin sous `foo.example.com` comme géré, mais pas `example.com/` ou `bar.example.com/`.
`\*.example.com`	Traitez n'importe quel chemin sous `foo.example.com` ou `bar.example.com` comme géré, mais pas `example.com/`.
`example.com/sub`	Traitez `example.com/sub` et n'importe quel chemin en dessous comme géré, mais pas `example.com/`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Format	Description
`foo.example.com/sub`	Traitez n'importe quel chemin sous `foo.example.com/sub` comme géré, mais pas `example.com`, `example.com/sub`, `foo.example.com/` ou `bar.example.com/sub`.
`\*.example.com/sub`	Traitez n'importe quel chemin sous `foo.example.com/sub` ou `bar.example.com/sub` comme géré, mais pas `example.com` ou `foo.example.com/`.

Règles :

- Le « www. » du début et les barres obliques de fin des adresses URL sont ignorés lorsque les domaines sont comparés.
- Si une entrée contient un numéro de port, seules les adresses spécifiant ce numéro de port sont considérées comme gérées. Dans le cas contraire, seuls les ports standard sont considérés comme gérés (port 80 pour http et port 443 pour https). Par exemple, le modèle `*.example.com:8080` correspond à `https://site.example.com:8080/page.html`, mais pas `https://site.example.com/page.html`, alors que le modèle `*.example.com` correspond à `https://site.example.com/page.html` et `https://site.example.com/page.html`, mais pas `https://site.example.com:8080/page.html`.
- Les définitions de domaines Web Safari gérés sont cumulatives. Les modèles définis par toutes les charges utiles des domaines Web Safari gérés sont utilisés pour la correspondance dans le cadre d'une demande d'adresse URL.

Paramètres :

- **Domaines gérés**
  - **Domaines de messagerie non marqués :** pour chaque domaine de messagerie à inclure dans la liste, cliquez sur **Ajouter**, puis procédez comme suit :
    - **Domaine de messagerie géré :** entrez le domaine de messagerie.
    - Cliquez sur **Enregistrer** pour enregistrer le domaine de messagerie ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **Domaines Web Safari gérés :** pour chaque domaine Web à inclure dans la liste, cliquez sur **Ajouter**, puis procédez comme suit :
    - **Domaine Web géré :** entrez le domaine Web.
    - Cliquez sur **Enregistrer** pour enregistrer le domaine Web ou cliquez sur **Annuler** pour ne pas l'enregistrer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Domaines de remplissage automatique du mot de passe Safari :** pour chaque domaine Web à inclure dans la liste, cliquez sur **Ajouter**, puis procédez comme suit :
    * **Domaine de remplissage automatique du mot de passe Safari :** entrez le domaine de remplissage automatique.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine de remplissage automatique ou cliquez sur **Annuler** pour ne pas l'enregistrer.

- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Stratégie Nombre maximal d'utilisateurs résidents

November 29, 2023

La stratégie Nombre maximal d'utilisateurs résidents est destinée aux appareils partagés exécutant iOS (iPadOS). Pour plus d'informations sur les iPads partagés, consultez la section Intégration avec les fonctionnalités Apple Éducation.

Cette stratégie doit être déployée lorsque l'iPad est en phase « en attente de configuration » dans l'Assistant d'installation. Apple n'autorise pas le déploiement de cette stratégie après l'inscription des iPad partagés.

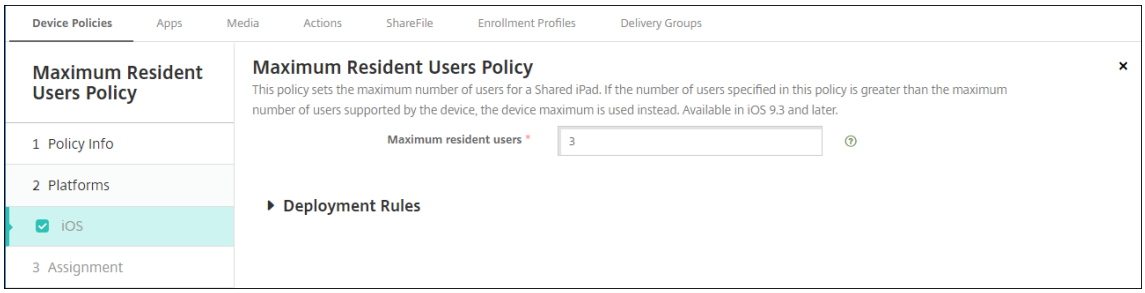
Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Nombre maximal d'utilisateurs résidents :** nombre maximal d'utilisateurs pour un iPad partagé. Si le nombre d'utilisateurs spécifié dans cette stratégie est supérieur au nombre maximal d'utilisateurs pris en charge par l'appareil, Citrix Endpoint Management utilise à la place le nombre maximal d'utilisateurs. La valeur par défaut est **5** utilisateurs.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Apple vous recommande de conserver le nombre maximal d'utilisateurs résidents aussi bas que possible. Une valeur faible maximise la quantité de stockage de l'iPad pour chaque utilisateur. De plus, une valeur faible minimise la communication avec iCloud et offre une expérience de connexion plus rapide. Pour plus d'informations sur la façon dont Apple gère le stockage partagé sur un iPad, consultez la page https://developer.apple.com/education/shared-ipad/.



Stratégie d'options MDM

November 29, 2023

La stratégie Options MDM gère les fonctions Localiser mon téléphone/Verrouillage d'activation iPad sur les appareils supervisés iOS. Pour plus d'informations sur la définition d'un appareil iOS en mode supervisé, consultez la section Déployer des appareils à l'aide d'Apple Configurator 2.

Le verrouillage d'activation est une fonctionnalité de Localiser mon iPhone/iPad qui empêche la réactivation d'un appareil supervisé perdu ou volé. Le verrouillage d'activation requiert l'identifiant Apple et le mot de passe de l'utilisateur pour pouvoir désactiver Localiser mon iPhone/iPad, effacer l'appareil ou réactiver l'appareil. Pour les appareils qui sont la propriété de votre organisation, il est nécessaire de contourner le verrouillage d'activation pour, par exemple, réinitialiser ou réattribuer des appareils.

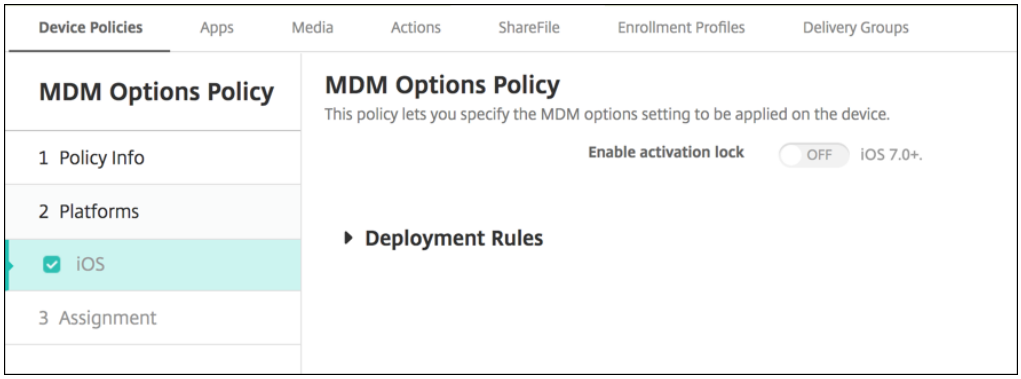
Pour activer le verrouillage d'activation, configurez et déployez la stratégie Options MDM d'Citrix Endpoint Management. Vous pouvez ensuite gérer un appareil à partir de la console Citrix Endpoint Management sans les informations d'identification Apple de l'utilisateur. Pour contourner l'obligation d'entrer des informations d'identification Apple avec un verrou d'activation, émettez l'action de sécurisation Contourner le verrouillage d'activation depuis la console Citrix Endpoint Management.

Par exemple, si l'utilisateur retourne un téléphone perdu ou pour configurer l'appareil avant ou après un effacement complet : lorsque le téléphone invite à entrer les informations d'identification de compte Apple App Store, vous pouvez ignorer cette étape en émettant l'action de sécurité Contourner le verrouillage d'activation à partir de la console Citrix Endpoint Management.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres iOS



- **Activer le verrouillage d'activation :** indiquez si vous souhaitez activer l'option Verrouillage d'activation sur les appareils sur lesquels vous déployez cette stratégie. La valeur par défaut est **Off**.

Après avoir installé le verrouillage d'activation en déployant la stratégie Options MDM : l'action de sécurisation **Contourner le verrouillage d'activation** s'affiche lorsque vous sélectionnez les appareils sur la page **Gérer > Appareils** et cliquez sur **Sécurité**. Un contournement de verrouillage d'activation vous permet de retirer le verrouillage d'activation des appareils supervisés avant l'activation de l'appareil sans connaître l'identifiant Apple et le mot de passe des utilisateurs de l'appareil. Vous pouvez envoyer un contournement de verrouillage d'activation à un appareil avant ou après un effacement complet. Pour plus d'informations, consultez la section Ne pas utiliser le verrouillage d'activation iOS.

Stratégie de réseau

March 1, 2024

La stratégie de réseau vous permet de gérer la manière dont les utilisateurs connectent leurs appareils à des réseaux Wi-Fi en définissant les éléments suivants :

- Noms et types de réseau
- Stratégies d'authentification et de sécurité
- Utilisation de serveur proxy
- Autres détails Wi-Fi associés

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Logiciels requis

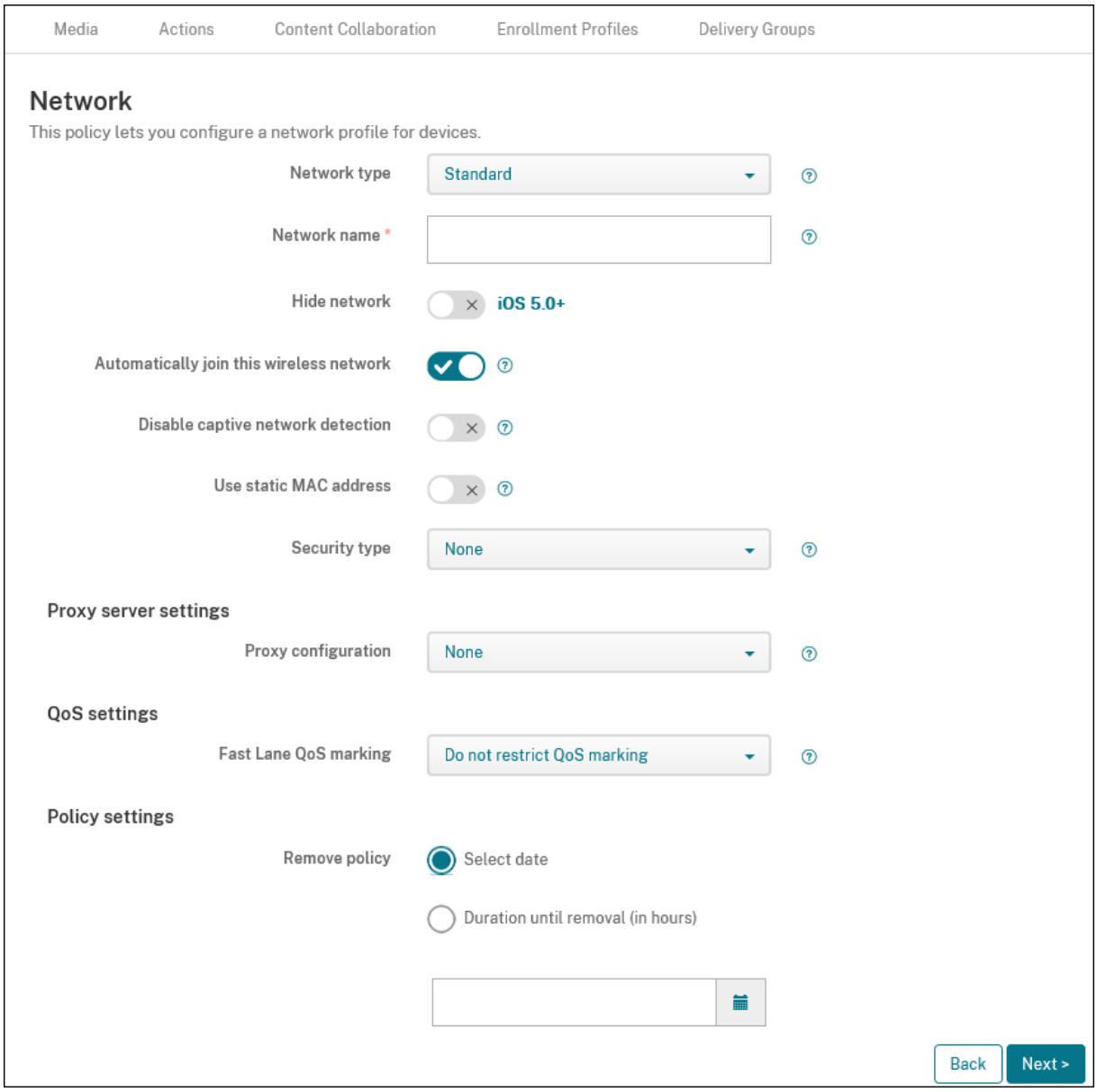
Avant de créer une stratégie, procédez comme suit :

- Créer les groupes de mise à disposition que vous voulez utiliser.
- Notez le nom et type de réseau.
- Déterminez les types d'authentification ou de sécurité que vous voulez utiliser.
- Déterminez les informations de serveur proxy dont vous avez besoin.
- Installer les certificats d'autorité de certification nécessaires.
- Vérifiez que vous disposez des clés partagées nécessaires.
- Créez l'entité PKI pour l'authentification par certificat.
- Configurez les fournisseurs d'informations d'identification.

Pour de plus amples informations, consultez la section Authentification et ses sous-articles.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres iOS



- **Type de réseau :** dans la liste, cliquez sur **Standard**, **Point d'accès d'ancienne génération** ou **Hotspot 2.0** pour définir le type de réseau que vous voulez utiliser.
- **Nom du réseau :** entrez le SSID qui est affiché dans la liste des réseaux disponibles pour l'appareil. Ne s'applique pas à **Hotspot 2.0**.
- **Masquer le réseau :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Rejoindre automatiquement ce réseau sans fil :** sélectionnez cette option pour spécifier si un appareil rejoint le réseau automatiquement. Si un appareil est connecté à un autre réseau, il ne rejoint pas ce réseau. L'utilisateur doit se déconnecter du réseau précédent avant que l'appareil ne se connecte automatiquement. La valeur par défaut est **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Désactiver détection de réseau captif :** l'assistant de réseau captif aide les utilisateurs à accéder aux réseaux d'abonnement ou de points d'accès Wi-Fi. Vous trouverez généralement ces réseaux dans les cafés, les hôtels et d'autres lieux publics. Si cette option est **activée**, les appareils peuvent toujours se connecter à des réseaux captifs, mais l'utilisateur doit ouvrir un navigateur et se connecter manuellement. La valeur par défaut est **Désactivé**.
- **Utiliser adresse MAC statique :** les adresses MAC sont des identifiants uniques qu'un appareil transmet au sein d'un réseau. Pour améliorer la confidentialité, les appareils iOS et iPadOS peuvent utiliser une adresse MAC différente chaque fois qu'ils se connectent à un réseau. Si cette option est **activée**, l'appareil utilise toujours la même adresse MAC lors de la connexion à ce réseau. Si cette option est **désactivée**, l'appareil utilise une adresse MAC différente chaque fois qu'il se connecte à ce réseau. La valeur par défaut est **Désactivé**.
- **Type de sécurité :** dans la liste, choisissez le type de sécurité que vous voulez utiliser. Ne s'applique pas à **Hotspot 2.0**.
  - Aucun : ne requiert aucune configuration supplémentaire.
  - WEP
  - WPA/WPA2/WPA3 Personnel
  - Tous (Personnel)
  - WEP Enterprise
  - WPA/WPA2/WPA3 Enterprise : dans la dernière version de Windows 10, configurez le protocole SCEP (Protocole d'inscription de certificats simple) pour utiliser WPA-2 Entreprise. Citrix Endpoint Management peut ensuite envoyer le certificat aux appareils pour l'authentification auprès du serveur Wi-Fi. Pour configurer SCEP, accédez à la page Distribution dans **Paramètres > Fournisseurs d'informations d'identification**. Pour de plus amples informations, consultez la section Fournisseurs d'identités.
  - Tous (Entreprise)

  Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.
- **Paramètres du serveur proxy**
  - **Configuration du proxy :** dans la liste, cliquez sur **Aucun**, **Manuel** ou **Automatique** pour définir la façon dont la connexion VPN transite via un serveur proxy et configurez des options supplémentaires. La valeur par défaut est **Aucun**, ce qui n'exige aucune configuration supplémentaire.
  - Si vous avez sélectionné **Manuel**, configurez les paramètres suivants :
    * **Nom d'hôte ou adresse IP :** entrez le nom ou l'adresse IP du serveur proxy.
    * **Port :** entrez le numéro de port du serveur proxy.
    * **Nom d'utilisateur :** entrez un nom d'utilisateur pour l'authentification auprès du serveur proxy (facultatif).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Mot de passe :** entrez un mot de passe pour l'authentification auprès du serveur proxy (facultatif).
  - Si vous avez sélectionné **Automatique**, configurez les paramètres suivants :
    * **URL du serveur :** entrez l'adresse URL du fichier PAC qui définit la configuration proxy.
    * **Autoriser la connexion directe si le PAC est injoignable :** indiquez si les utilisateurs sont autorisés à se connecter directement à la destination si le fichier PAC est inaccessible. La valeur par défaut est **Activé**.

- **Marquage QoS Fast Lane :** si vous ne limitez pas le marquage QoS pour un réseau Wi-Fi prenant en charge Cisco Fast Lane QoS, toutes les applications sont autorisées à utiliser le marquage L2 et L3. Si vous limitez le marquage QoS, spécifiez les applications qui peuvent utiliser le marquage L2 et L3.
  - **Activer marquage QoS :** si vous limitez le marquage QoS, utilisez ce paramètre pour le désactiver complètement ou marquer uniquement certaines applications. Si cette option est **désactivée**, vous désactivez entièrement le marquage QoS. Si cette option est **activée**, configurez une liste d'applications pouvant utiliser le marquage QoS. La valeur par défaut est **Activé**.
  - **Autoriser appels audio/vidéo Apple :** indiquez si les applications d'appel audio et vidéo peuvent utiliser le marquage QoS. Si cette option est **désactivée**, la qualité des appels vidéo et audio peut en souffrir.
  - **Autoriser des applications spécifiques :** ajoutez un ID de package d'application à cette liste pour permettre à l'application d'utiliser le marquage QoS.

- **Paramètres Hotspot 2.0**
  - **Nom d'opérateur affiché :** nom convivial diffusé par l'appareil Hotspot. Les utilisateurs voient ce nom dans leur liste de réseaux Wi-Fi disponibles.
  - **Nom de domaine :** nom de domaine utilisé pour la négociation Wi-Fi Hotspot 2.0.
  - **Autoriser la connexion aux réseaux partenaires itinérants :** si cette option est **activée**, les appareils quittant leur réseau domestique peuvent se connecter aux réseaux partenaires.
  - **Identificateurs d'organisations (OI) du consortium d'itinérance :** ajoutez une liste d'identificateurs d'organisations auxquels l'appareil peut accéder. Un OI du consortium d'itinérance appartient à une organisation avec des méthodes d'authentification partagées. Si le Hotspot que vous configurez n'est pas disponible, l'appareil se connecte à un OI du consortium d'itinérance répertorié ici.
  - **Noms de domaines d'identificateur d'accès réseau (NAI) :** configurez une liste de noms de domaine utilisés pour identifier les utilisateurs sur un réseau itinérant. Un NAI est transmis au format `user@realm`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Codes de pays mobiles (MCCs) et configurations de réseaux mobiles (MNCs) :** un code de pays mobile se compose de trois chiffres qui identifient le pays d'un réseau. Le code de réseau mobile se compose de 2 ou 3 chiffres uniques. Lorsqu'ils sont utilisés ensemble, le MCC et le MNC identifient de manière unique un opérateur ou un opérateur de réseau mobile.

- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**. Non disponible pour iOS.

Paramètres WPA, WPA Personnel, Tous (Personnel) pour iOS

Mot de passe : entrez un mot de passe (facultatif). Si vous laissez ce champ vide, les utilisateurs peuvent être invités à entrer leurs mots de passe lorsqu'ils ouvrent une session.

Paramètres WEP Entreprise, WPA Entreprise, WPA2 Entreprise, WPA3 Enterprise, Tous (Entreprise) pour iOS

Lorsque vous choisissez l'un de ces types de sécurité, les paramètres EAP apparaissent après les **paramètres QoS**.

> **Important :**
>
> si vous sélectionnez le type de sécurité **WPA2 Enterprise**, vous devez autoriser au moins un protocole EAP.

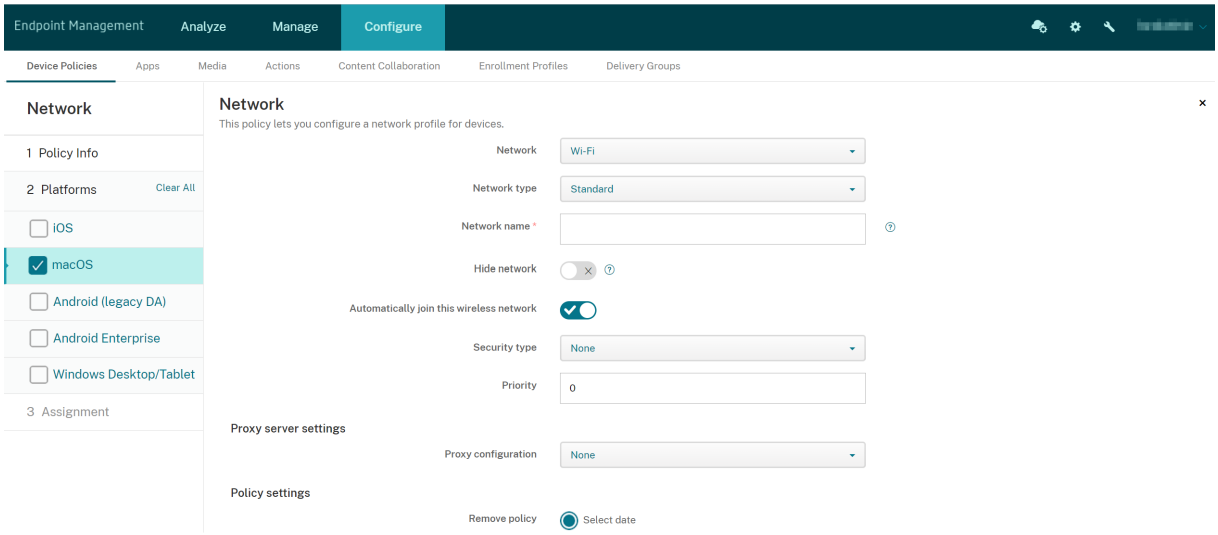
- **Protocoles EAP autorisés :** activez les types EAP que vous souhaitez prendre en charge, puis configurez les paramètres associés. La valeur par défaut est **Désactivé** pour chaque type EAP disponible.
- **Authentification interne (TTLS) :** *requis uniquement lorsque vous activez TTLS*. Dans la liste, choisissez la méthode d'authentification interne à utiliser. Les options possibles sont : **PAP**, **CHAP**, **MSCHAP** ou **MSCHAPv2**. La valeur par défaut est **MSCHAPv2**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **EAP-FAST avec PAC :** indiquez si vous souhaitez utiliser les informations d'identification d'accès protégé (PAC).
  - Si vous sélectionnez **Utiliser PAC**, indiquez si vous voulez utiliser un provisioning de PAC.
    - Si vous sélectionnez **Provisioning de PAC**, indiquez si vous souhaitez autoriser une négociation TLS anonyme entre le client et Citrix Endpoint Management.
      - **Provisioning du PAC de manière anonyme**
- **Authentification :**
  - **Nom d'utilisateur :** entrez un nom d'utilisateur.
  - **Mot de passe par connexion :** indiquez si un mot de passe sera exigé chaque fois que les utilisateurs ouvriront une session.
  - **Mot de passe :** entrez un mot de passe (facultatif). Si vous laissez ce champ vide, les utilisateurs peuvent être invités à entrer leurs mots de passe lorsqu'ils ouvrent une session.
  - **Infos d'identification de l'identité (infos d'identification magasin de clés ou PKI) :** dans la liste, cliquez sur le type d'informations d'identification de l'identité. La valeur par défaut est **Aucun**.
  - **Identité externe :** *requis uniquement lorsque vous activez* **PEAP**, **TTLS** *ou* **EAP-FAST**. Entrez le nom d'utilisateur visible en externe. Vous pouvez augmenter la sécurité en tapant un terme générique comme « anonyme » de façon à ce que le nom d'utilisateur ne soit pas être visible.
  - **Requiert un certificat TLS :** sélectionnez cette option pour exiger un certificat TLS.
- **Confiance**
  - **Certificats approuvés :** pour ajouter un certificat approuvé, cliquez sur **Ajouter** et, pour chaque certificat que vous souhaitez ajouter, procédez comme suit :
    - **Application :** dans la liste, choisissez l'application que vous souhaitez ajouter.
    - Cliquez sur **Enregistrer** pour enregistrer le certificat ou sur **Annuler**.
  - **Noms de certificats serveur de confiance :** pour ajouter des noms communs de certificat de serveur approuvés, cliquez sur **Ajouter** et, pour chaque nom que vous souhaitez ajouter, procédez comme suit :
    - **Certificat :** entrez le nom du certificat de serveur. Vous pouvez utiliser des caractères génériques pour spécifier le nom, comme wpa.*.example.com.
    - Cliquez sur **Enregistrer** pour enregistrer le nom du certificat ou sur **Annuler**.
- **Autoriser les exceptions de fiabilité :** indiquez si vous souhaitez que la boîte de dialogue d'approbation de certificat s'affiche lorsqu'un certificat n'est pas approuvé. La valeur par défaut est **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres macOS



- **Réseau :** dans la liste, choisissez l'option de réseau que vous prévoyez d'utiliser. La valeur par défaut est **Wi-Fi**.
  - Wi-Fi
  - Ethernet global
  - Premier Ethernet actif
  - Deuxième Ethernet actif
  - Troisième Ethernet actif
  - Premier Ethernet
  - Deuxième Ethernet
  - Troisième Ethernet
- **Type de réseau :** dans la liste, cliquez sur **Standard**, **Point d'accès d'ancienne génération** ou **Hotspot 2.0** pour définir le type de réseau que vous voulez utiliser.
- **Nom du réseau :** entrez le SSID qui est affiché dans la liste des réseaux disponibles pour l'appareil. Ne s'applique pas à **Hotspot 2.0**.
- **Masquer le réseau :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Rejoindre automatiquement ce réseau sans fil :** sélectionnez cette option pour spécifier si le réseau est rejoint automatiquement. Si un appareil est déjà connecté à un autre réseau, il ne rejoint pas ce réseau. L'utilisateur doit se déconnecter du réseau précédent avant que l'appareil ne se connecte automatiquement. La valeur par défaut est **Activé**.
- **Type de sécurité :** dans la liste, choisissez le type de sécurité que vous voulez utiliser. Ne s'applique pas à **Hotspot 2.0**.
  - Aucun : ne requiert aucune configuration supplémentaire.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - WEP
  - WPA/WPA2 Personnel
  - Tous (Personnel)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - Tous (Entreprise)

  Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.

- **Priorité :** si vous disposez de plusieurs réseaux, tapez un numéro pour définir la priorité de la connexion réseau. L'appareil se connecte au réseau avec d'abord le numéro de priorité le plus bas. Les nombres négatifs sont acceptables. La valeur par défaut est **0**.
- **Paramètres du serveur proxy**
  - **Configuration du proxy :** dans la liste, cliquez sur **Aucun**, **Manuel** ou **Automatique** pour définir la façon dont la connexion VPN transite via un serveur proxy et configurez des options supplémentaires. La valeur par défaut est **Aucun**, ce qui n'exige aucune configuration supplémentaire.
  - Si vous avez sélectionné **Manuel**, configurez les paramètres suivants :
    * **Nom d'hôte ou adresse IP :** entrez le nom ou l'adresse IP du serveur proxy.
    * **Port :** entrez le numéro de port du serveur proxy.
    * **Nom d'utilisateur :** entrez un nom d'utilisateur pour l'authentification auprès du serveur proxy (facultatif).
    * **Mot de passe :** entrez un mot de passe pour l'authentification auprès du serveur proxy (facultatif).
  - Si vous avez sélectionné **Automatique**, configurez les paramètres suivants :
    * **URL du serveur :** entrez l'adresse URL du fichier PAC qui définit la configuration proxy.
    * **Autoriser la connexion directe si le PAC est injoignable :** indiquez si les utilisateurs sont autorisés à se connecter directement à la destination si le fichier PAC est inaccessible. La valeur par défaut est **Activé**.
- **Paramètres Hotspot 2.0**
  - **Nom d'opérateur affiché :** nom convivial diffusé par l'appareil Hotspot. Les utilisateurs voient ce nom dans leur liste de réseaux Wi-Fi disponibles.
  - **Nom de domaine :** nom de domaine utilisé pour la négociation Wi-Fi Hotspot 2.0.
  - **Autoriser la connexion aux réseaux partenaires itinérants :** si cette option est **activée**, les appareils quittant leur réseau domestique peuvent se connecter aux réseaux partenaires.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Identificateurs d'organisations (OI) du consortium d'itinérance :** ajoutez une liste d'identificateurs d'organisations auxquels l'appareil peut accéder. Un OI du consortium d'itinérance appartient à une organisation avec des méthodes d'authentification partagées. Si le Hotspot que vous configurez n'est pas disponible, l'appareil se connecte à un OI du consortium d'itinérance répertorié ici.
  - **Noms de domaines d'identificateur d'accès réseau (NAI) :** configurez une liste de noms de domaine utilisés pour identifier les utilisateurs sur un réseau itinérant. Un NAI est transmis au format `user@realm`.
  - **Codes de pays mobiles (MCCs) et configurations de réseaux mobiles (MNCs) :** un code de pays mobile se compose de trois chiffres qui identifient le pays d'un réseau. Le code de réseau mobile se compose de 2 ou 3 chiffres uniques. Lorsqu'ils sont utilisés ensemble, le MCC et le MNC identifient de manière unique un opérateur ou un opérateur de réseau mobile.

- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Paramètres WPA, WPA Personnel, WPA 2 Personnel, Tous (Personnel) pour macOS

- **Mot de passe :** entrez un mot de passe (facultatif). Si vous laissez ce champ vide, les utilisateurs peuvent être invités à entrer leurs mots de passe lorsqu'ils ouvrent une session.

Paramètres WEP Entreprise, WPA Entreprise, WPA2 Entreprise, Tous (Entreprise) pour macOS

- **Mode de connexion :** si ce paramètre est défini sur **Activé**, choisissez le mode de connexion à utiliser lorsque l'utilisateur rejoint le réseau. La valeur par défaut est **Désactivé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Système :** si cette option est cochée, l'appareil utilise les informations d'identification système pour authentifier l'utilisateur. La valeur par défaut est Désactivé.
  - **Fenêtre de connexion :** si cette option est cochée, l'appareil utilise les mêmes informations d'identification entrées dans la fenêtre de connexion pour authentifier l'utilisateur. La valeur par défaut est Désactivé.

Lorsque vous choisissez l'un de ces types de sécurité, les paramètres EAP apparaissent après les **paramètres QoS**.

> **Important :**
>
> si vous sélectionnez le type de sécurité **WPA2 Enterprise**, vous devez autoriser au moins un protocole EAP.

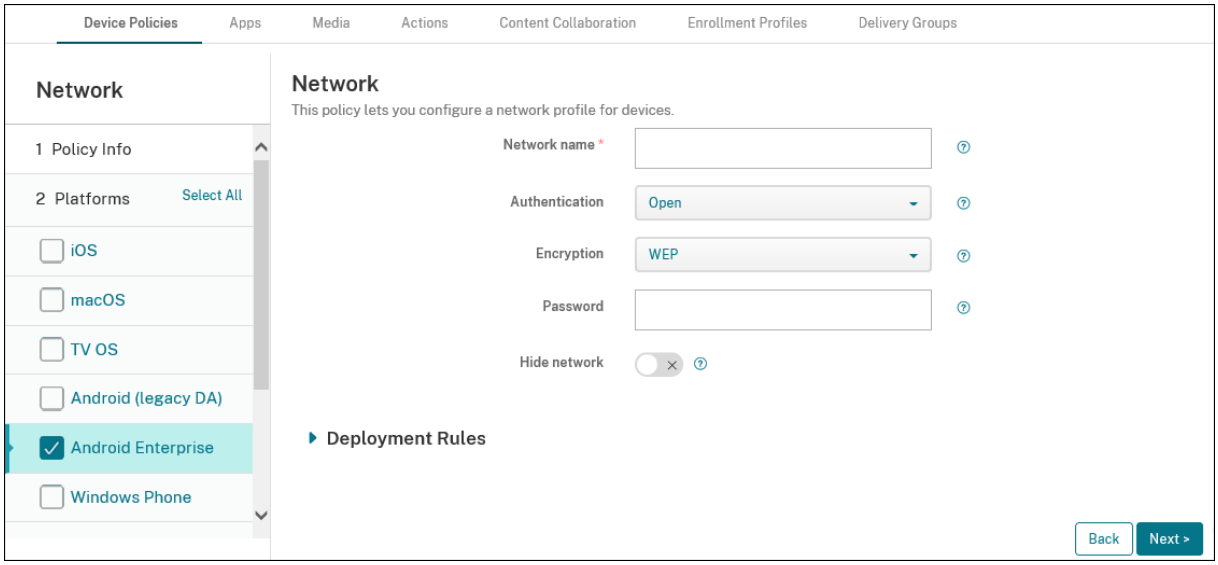
- **Protocoles EAP autorisés :** activez les types EAP que vous souhaitez prendre en charge, puis configurez les paramètres associés. La valeur par défaut est **Désactivé** pour chaque type EAP disponible.
- **Authentification interne (TTLS) :** *requis uniquement lorsque vous activez TTLS*. Dans la liste, choisissez la méthode d'authentification interne à utiliser. Les options possibles sont : **PAP**, **CHAP**, **MSCHAP** ou **MSCHAPv2**. La valeur par défaut est **MSCHAPv2**.
- **EAP-FAST avec PAC :** indiquez si vous souhaitez utiliser les informations d'identification d'accès protégé (PAC).
  - Si vous sélectionnez **Utiliser PAC**, indiquez si vous voulez utiliser un provisioning de PAC.
    - Si vous sélectionnez **Provisioning de PAC**, indiquez si vous souhaitez autoriser une négociation TLS anonyme entre le client et Citrix Endpoint Management.
      - **Provisioning du PAC de manière anonyme**
- **Authentification :**
  - **Utiliser l'authentification Active Directory :** indiquez si vous souhaitez activer l'authentification Active Directory. Disponible pour macOS 10.7 et version ultérieure. Pour rendre cette option disponible, effectuez les opérations suivantes :
    - Définissez **PEAP** comme protocole EAP.
    - Définissez l'étendue du profil sur **Système**. Vous pouvez utiliser ce paramètre uniquement lorsque vous appliquez la stratégie à l'ensemble du système.
  - **Nom d'utilisateur :** entrez un nom d'utilisateur.
  - **Mot de passe par connexion :** indiquez si un mot de passe sera exigé chaque fois que les utilisateurs ouvriront une session.
  - **Mot de passe :** entrez un mot de passe (facultatif). Si vous laissez ce champ vide, les utilisateurs peuvent être invités à entrer leurs mots de passe lorsqu'ils ouvrent une session.
  - **Infos d'identification de l'identité (infos d'identification magasin de clés ou PKI) :** dans la liste, cliquez sur le type d'informations d'identification de l'identité. La valeur par défaut est **Aucun**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Identité externe :** *requis uniquement lorsque vous activez* **PEAP**, **TTLS** *ou* **EAP-FAST**. Entrez le nom d'utilisateur visible en externe. Vous pouvez augmenter la sécurité en tapant un terme générique comme « anonyme » de façon à ce que le nom d'utilisateur ne soit pas être visible.
  - **Requiert un certificat TLS :** sélectionnez cette option pour exiger un certificat TLS.

- **Confiance**
  - **Certificats approuvés :** pour ajouter un certificat approuvé, cliquez sur **Ajouter** et, pour chaque certificat que vous souhaitez ajouter, procédez comme suit :
    * **Application :** dans la liste, choisissez l'application que vous souhaitez ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le certificat ou sur **Annuler**.
  - **Noms de certificats serveur de confiance :** pour ajouter des noms communs de certificat de serveur approuvés, cliquez sur **Ajouter** et, pour chaque nom que vous souhaitez ajouter, procédez comme suit :
    * **Certificat :** entrez le nom du certificat de serveur que vous souhaitez ajouter. Vous pouvez utiliser des caractères génériques pour spécifier le nom, comme wpa.*.example.com.
    * Cliquez sur **Enregistrer** pour enregistrer le nom du certificat ou sur **Annuler**.
- **Autoriser les exceptions de fiabilité :** indiquez si vous souhaitez que la boîte de dialogue d'approbation de certificat s'affiche lorsqu'un certificat n'est pas approuvé. La valeur par défaut est **Activé**.

Paramètres Android Enterprise



- **Nom du réseau :** entrez le SSID qui figure dans la liste des réseaux disponibles sur l'appareil de l'utilisateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Authentification :** dans la liste, choisissez le type de sécurité à utiliser avec la connexion Wi-Fi.
  - Open
  - Partagé
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante. La valeur par défaut est **Ouverte**.

Paramètres ouverts partagés pour Android Enterprise

- **Cryptage :** dans la liste, choisissez **Désactivé** ou **WEP**. La valeur par défaut est **WEP**.
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Masquer le réseau :** sélectionnez cette option pour spécifier si le réseau est masqué.

Paramètres WPA, WPA-PSK, WPA2, WPA2-PSK pour Android Enterprise

- **Cryptage :** dans la liste, choisissez **TKIP** ou **AES**. La valeur par défaut est **TKIP**.
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Masquer le réseau :** sélectionnez cette option pour spécifier si le réseau est masqué.

Paramètres 802.1x pour Android Enterprise

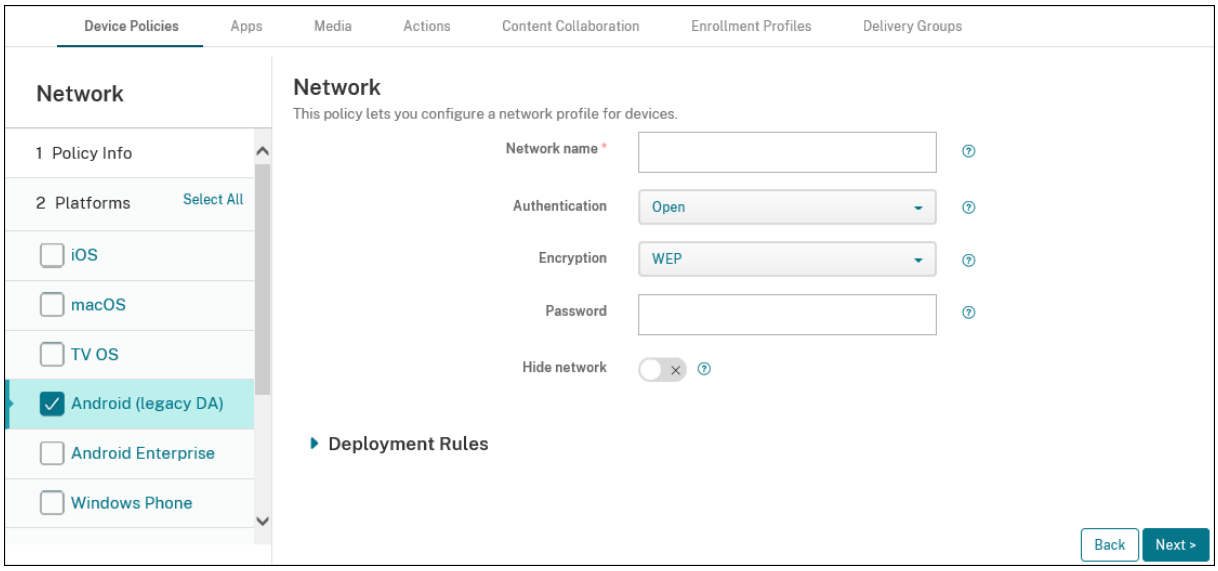
- **Type EAP :** dans la liste, choisissez **PEAP**, **TLS** ou **TTLS**. La valeur par défaut est **PEAP**.
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Authentification phase 2 :** dans la liste, choisissez **Aucun**, **PAP**, **MSCHAP**, **MSCHAPPv2** ou **GTC**. La valeur par défaut est **PAP**.
- **Identité :** entrez le nom d'utilisateur et le domaine (facultatif).
- **Anonyme :** entrez le nom d'utilisateur visible en externe (facultatif). Vous pouvez augmenter la sécurité en tapant un terme générique comme « anonyme » de façon à ce que le nom d'utilisateur ne soit pas être visible.
- **Certificat CA :** dans la liste, choisissez le certificat à utiliser.
- **Domaine :** saisissez le nom de domaine requis. Pour plus d'informations, voir [Domaine](https://developer.android.com/reference/android/net/wifi/WifiEnterpriseConfig#setDomainSuffixM

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Remarque :**
>
> Lorsque vous configurez la stratégie Wi-Fi sur les appareils fonctionnant sous Android 13 ou version ultérieure, les champs **Certificat CA** et **Domaine** doivent être obligatoirement mis à jour. S'ils ne sont pas mis à jour, la configuration échouera.

- **Infos d'identification de l'identité :** dans la liste, choisissez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
- **Masquer le réseau :** sélectionnez cette option pour spécifier si le réseau est masqué.

Paramètres Android (DA hérité)



- **Nom du réseau :** entrez le SSID qui figure dans la liste des réseaux disponibles sur l'appareil de l'utilisateur.
- **Authentification :** dans la liste, choisissez le type de sécurité à utiliser avec la connexion Wi-Fi.
  - Open
  - Partagé (Android Enterprise uniquement)
  - WPA (Android Enterprise uniquement)
  - WPA-PSK (Android Enterprise uniquement)
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres ouverts partagés pour Android

- **Cryptage :** dans la liste, choisissez **Désactivé** ou **WEP**. La valeur par défaut est **WEP**.
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Masquer le réseau :** sélectionnez cette option pour spécifier si le réseau est masqué.

Paramètres WPA, WPA-PSK, WPA2, WPA2-PSK pour Android

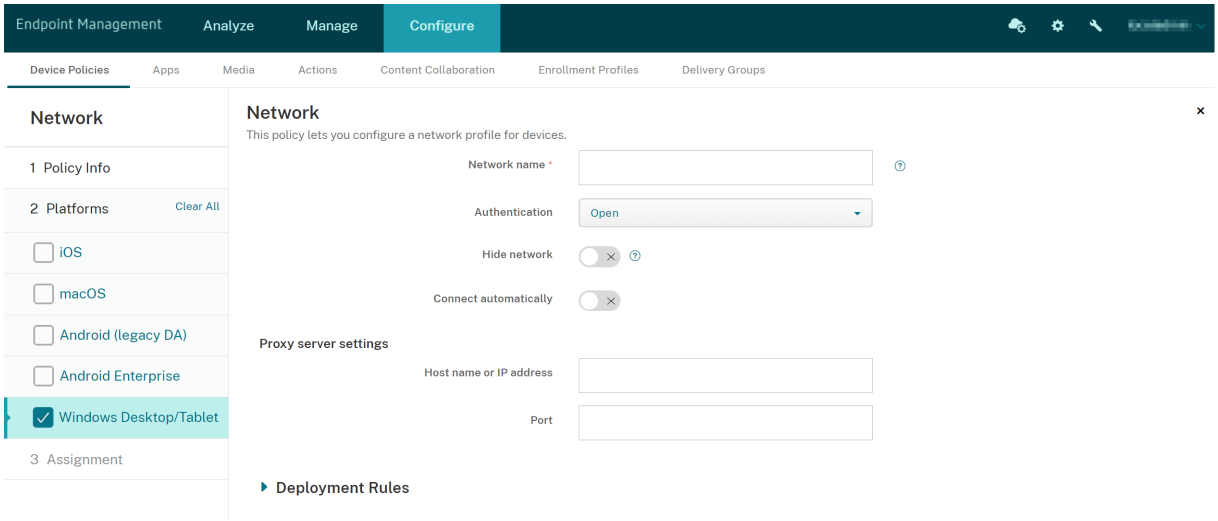
- **Cryptage :** dans la liste, choisissez **TKIP** ou **AES**. La valeur par défaut est **TKIP**.
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Masquer le réseau :** sélectionnez cette option pour spécifier si le réseau est masqué.

Paramètres 802.1x pour Android

- **Type EAP :** dans la liste, choisissez **PEAP**, **TLS** ou **TTLS**. La valeur par défaut est **PEAP**.
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Authentification phase 2 :** dans la liste, choisissez **Aucun**, **PAP**, **MSCHAP**, **MSCHAPPv2** ou **GTC**. La valeur par défaut est **PAP**.
- **Identité :** entrez le nom d'utilisateur et le domaine (facultatif).
- **Anonyme :** entrez le nom d'utilisateur visible en externe (facultatif). Vous pouvez augmenter la sécurité en tapant un terme générique comme « anonyme » de façon à ce que le nom d'utilisateur ne soit pas être visible.
- **Certificat CA :** dans la liste, choisissez le certificat à utiliser.
- **Infos d'identification de l'identité :** dans la liste, choisissez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
- **Masquer le réseau :** sélectionnez cette option pour spécifier si le réseau est masqué.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Windows Desktop/Tablet



- **Nom du réseau :** SSID affiché dans la liste des réseaux disponibles.
- **Authentification :** dans la liste, cliquez sur le type de sécurité à utiliser avec la connexion Wi-Fi.
  - Open
  - WPA Personnel
  - WPA-2 Personnel
  - WPA Entreprise
  - WPA-2 Enterprise : dans la dernière version de Windows 10, configurez SCEP pour utiliser WPA-2 Enterprise. La configuration SCEP permet à Citrix Endpoint Management d'envoyer le certificat aux appareils pour l'authentification auprès du serveur Wi-Fi. Pour configurer SCEP, accédez à la page **Distribution** dans **Paramètres > Fournisseurs d'identités**. Pour de plus amples informations, consultez la section Fournisseurs d'identités.

Les sections suivantes répertorient les options à configurer pour chaque type de connexion suivante.

Paramètres ouverts pour Windows 10 et Windows 11

- **Masquer le réseau :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Se connecter automatiquement :** sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.

Paramètres WPA Personnel, WPA-2 Personnel pour Windows 10 et Windows 11

- **Cryptage :** dans la liste, choisissez **AES** ou **TKIP** pour définir le type de cryptage. La valeur par défaut est **AES**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Clé partagée :** indiquez la clé de cryptage de la méthode que vous avez sélectionnée.
- **Masquer le réseau :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Se connecter automatiquement :** sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.

Paramètres WPA-2 Enterprise pour Windows 10 et Windows 11

- **Cryptage :** dans la liste, choisissez **AES** ou **TKIP** pour définir le type de cryptage. La valeur par défaut est **AES**.
- **Type EAP :** dans la liste, choisissez **PEAP-MSCHAPv2** ou **TLS** pour définir le type EAP. La valeur par défaut est **PEAP-MSCHAPv2**.
- **Masquer le réseau :** sélectionnez cette option pour spécifier si le réseau est masqué.
- **Se connecter automatiquement :** sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.
- **Activer SCEP ? :** indiquez si vous souhaitez distribuer le certificat aux appareils des utilisateurs via le protocole SCEP.
- **Fournisseur d'identités pour SCEP :** dans la liste, choisissez le fournisseur d'identités SCEP. La valeur par défaut est **Aucun**.

Stratégie Utilisation du réseau

November 29, 2023

Vous pouvez définir des règles d'utilisation du réseau pour spécifier la manière dont les appareils iOS utilisent les réseaux, tels que les réseaux de données cellulaires. Les règles s'appliquent aux applications gérées et aux SIM spécifiées. Les applications gérées sont des applications que vous déployez sur les appareils des utilisateurs via Citrix Endpoint Management. Elles n'incluent pas les applications que les utilisateurs ont téléchargées directement sur leurs appareils sans qu'elles soient déployées via Citrix Endpoint Management. Elles n'incluent pas non plus les applications déjà installées sur les appareils lorsqu'ils ont été inscrits dans Citrix Endpoint Management. Cette stratégie s'applique aux SIM pour appareils iOS 13. Vous pouvez configurer des règles d'application, des règles SIM ou les deux. Les règles SIM s'appliquent à toutes les applications gérées sur cet appareil.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Règles d'application**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Autoriser les données cellulaires en itinérance :** indiquez si les applications spécifiées peuvent utiliser une connexion de données cellulaires en itinérance. La valeur par défaut est **Off**.
  - **Autoriser les données cellulaires :** indiquez si les applications spécifiées peuvent utiliser une connexion de données cellulaires. La valeur par défaut est **Off**.
  - **Correspondances de l'identifiant d'application :** pour chaque application que vous souhaitez ajouter à la liste, cliquez sur **Ajouter**, puis effectuez la configuration suivante :
    * **Identifiant app :** entrez un identifiant pour l'application.
  - Cliquez sur **Enregistrer** pour enregistrer l'application dans la liste ou sur **Annuler** pour ne pas l'enregistrer dans la liste.

- **Règles SIM**
  - **Stratégie d'assistance Wi-Fi de SIM :** l'activation de **Changer la connexion si signal Wi-Fi faible** rend plus agressif le basculement de connexions Wi-Fi médiocres vers des connexions cellulaires. Ce paramètre peut augmenter l'utilisation des données cellulaires et avoir un impact sur l'autonomie de la batterie.
  - **ICCID des SIM :** pour chaque carte SIM que vous souhaitez ajouter à la liste, cliquez sur **Ajouter**, puis configurez ce qui suit :
    * **ICCID :** saisissez le numéro à 19 ou 20 chiffres de la carte SIM à ajouter.

Stratégie Office

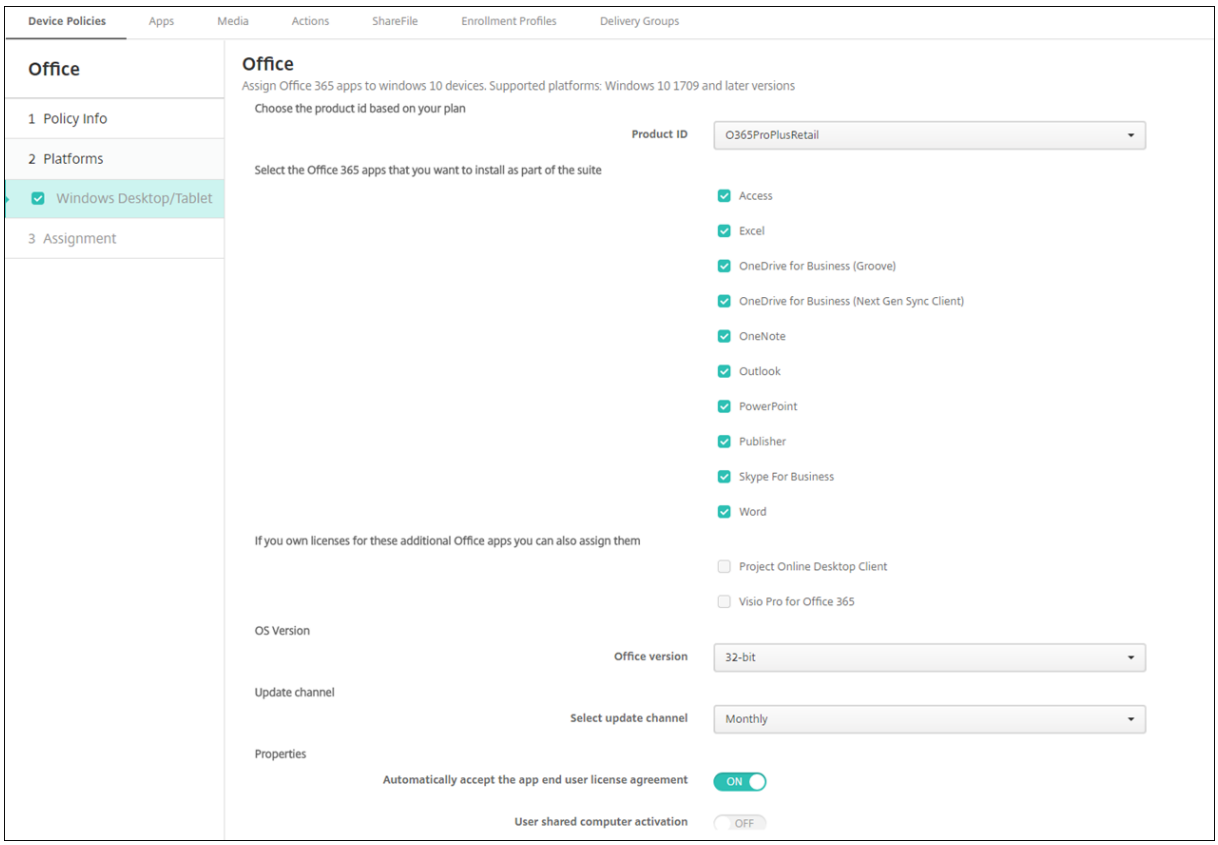
November 29, 2023

Citrix Endpoint Management permet le déploiement de produits Microsoft Office 365 à l'aide du fournisseur de services de configuration Office (CSP). En configurant la stratégie d'appareil Office, vous pouvez déployer des applications Microsoft Office sur tous les appareils exécutant Windows 10 (version 1709 ou ultérieure) ou Windows 11.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Windows Desktop/Tablet



- **ID produit :** sélectionnez un ID de produit en fonction de votre plan Office 365. Les options sont **O365ProPlusRetail, O365BusinessRetail** ou **O365SmallBusPremRetail**.
- **Applications Office 365 :** sélectionnez les applications Office 365 que vous souhaitez déployer. Toutes les applications sont sélectionnées par défaut.
- **Applications Office supplémentaires :** si vous possédez des licences pour **Project Online Desktop Client** ou **Visio Pro pour Office 365**, vous pouvez sélectionner ces applications pour les installer.
- **Version Office :** indiquez si vous souhaitez installer la version **32 bits** ou **64 bits** d'Office.
- **Canal de mise à jour :** choisissez la fréquence à laquelle vous souhaitez que les mises à jour se produisent. Les options sont **Mensuel**, **Mensuel (ciblé)**, **Semi-annuel** ou **Semi-annuel (ciblé)**.
- **Propriétés :**
  - **Accepter automatiquement le contrat de licence de l'utilisateur final de l'application :** sélectionnez **Activé** ou **Désactivé**. La valeur par défaut est **Activé**.
  - **Activation de l'ordinateur utilisateur partagé :** sélectionnez si l'ordinateur est partagé ou non. Les options sont **Activé** ou **Désactivé**. La valeur par défaut est **Désactivé**.
- **Langues Office :** Office s'installe automatiquement dans toutes les langues que Windows a déjà installées. Vous pouvez sélectionner des langues supplémentaires à installer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie d'informations sur l'organisation

November 29, 2023

La stratégie d'informations sur l'organisation dans Citrix Endpoint Management permet de spécifier les coordonnées de votre organisation à utiliser pour envoyer les messages d'alerte qui sont transmis depuis Citrix Endpoint Management vers les appareils iOS.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Nom :** entrez le nom de l'organisation exécutant Citrix Endpoint Management.
- **Adresse :** entrez l'adresse de l'organisation.
- **Téléphone :** entrez le numéro de téléphone d'assistance de l'organisation.
- **Adresse électronique :** entrez l'adresse e-mail d'assistance.
- **Magic :** entrez un mot ou une phrase décrivant les services gérés par l'organisation.

Stratégie de mise à jour d'OS

March 1, 2024

La stratégie de mise à jour d'OS vous permet de :

- Déployer les dernières mises à jour du système d'exploitation sur les appareils iOS supervisés.

  La stratégie Mise à jour d'OS ne fonctionne que pour les appareils supervisés inscrits au programme de déploiement Apple.

- Déployer le dernier système d'exploitation et les dernières mises à jour de l'application sur les appareils macOS inscrits auprès du programme de déploiement Apple exécutant macOS 10.11.5 et versions ultérieures.

> **Remarque :**
>
> Apple limite actuellement les mises à jour du système d'exploitation aux versions majeures uniquement. Les administrateurs ne sont pas autorisés à mettre à jour les versions mineures. Pour plus d'informations, consultez cet article dans la documentation Apple.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Déployer les dernières mises à jour du système d'exploitation sur les appareils Windows 10 ou Windows 11 Desktop et Tablet supervisés.

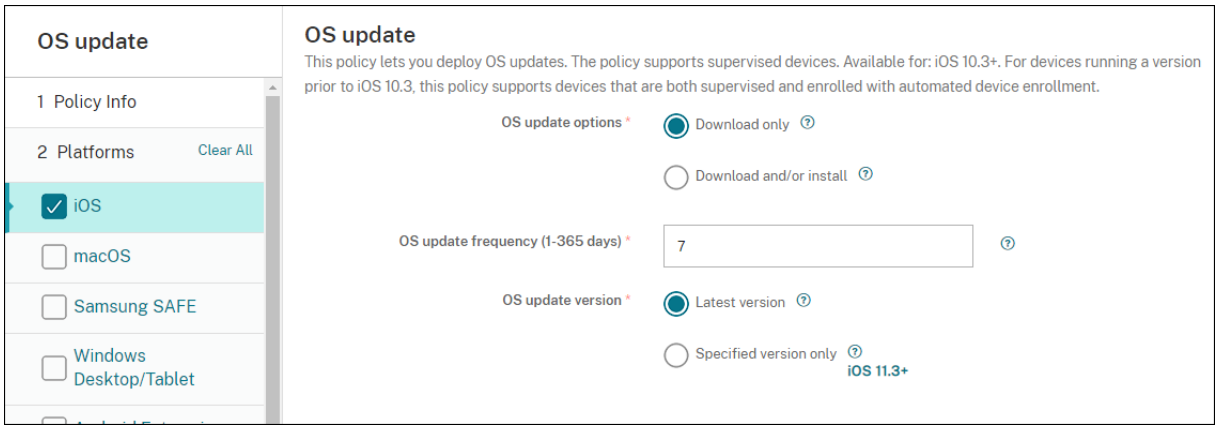
  Vous pouvez aussi utiliser la stratégie de mise à jour d'OS pour gérer les paramètres d'optimisation de la distribution pour les ordinateurs de bureau et les tablettes exécutant Windows 10 (version 1607 ou supérieure) ou Windows 11. L'optimisation de la distribution est un service de mise à jour partagée entre homologues qui est fourni par Microsoft pour les mises à jour de Windows 10 et Windows 11. L'objectif de l'optimisation de la distribution est de réduire les problèmes de bande passante lors du processus de mise à jour. Pour réduire la bande passante, la tâche de téléchargement est partagée entre plusieurs appareils. Pour plus d'informations, consultez l'article de Microsoft, Optimisation de la distribution pour les mises à jour de Windows 10.

- Déployer les dernières mises à jour d'OS sur les appareils Android Enterprise gérés (Android 7.0 et versions ultérieures).

> **Important :**
>
> la stratégie de mise à jour du système d'exploitation ne vous permet pas de désactiver entièrement les mises à jour. Pour retarder les mises à jour jusqu'à 90 jours, créez une stratégie de restriction. Consultez la section Stratégie de restrictions.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



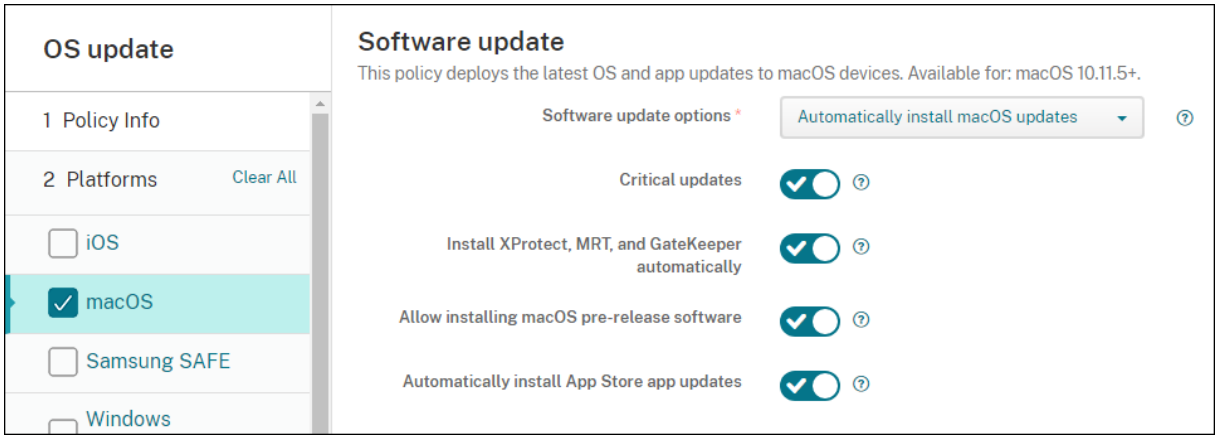
Les paramètres suivants sont destinés aux appareils iOS supervisés.

- **Options de mise à jour de l'OS :** les deux options téléchargent les dernières mises à jour du système d'exploitation sur les appareils supervisés selon la **fréquence de mise à jour de l'OS**. L'appareil invite les utilisateurs à installer les mises à jour. L'invite est visible une fois que l'utilisateur a déverrouillé l'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Fréquence de mise à jour de l'OS :** détermine la fréquence à laquelle Citrix Endpoint Management vérifie et met à jour le système d'exploitation de l'appareil. La valeur par défaut est **7** jours.
- **Version de mise à jour de l'OS :** spécifie la version à utiliser pour mettre à jour les appareils iOS supervisés. La valeur par défaut est **Dernière version**.
  - **Dernière version :** sélectionnez cette option pour mettre à jour vers la dernière version du système d'exploitation.
  - **Version spécifiée uniquement :** sélectionnez cette option pour mettre à jour vers une version de système d'exploitation spécifique, puis tapez le numéro de version.

Paramètres macOS



- **Options de mises à jour logicielles :** ce paramètre contrôle la façon dont les appareils macOS vérifient et installent les mises à jour Sélectionnez l'une des options suivantes :
  - **Installer automatiquement les mises à jour de macOS :** les mises à jour sont téléchargées et installées automatiquement.
  - **Télécharger les nouvelles mises à jour lorsqu'elles sont disponibles :** les mises à jour sont téléchargées mais nécessitent une installation manuelle.
  - **Rechercher les mises à jour :** ce paramètre vérifie si des mises à jour existent mais ne télécharge ni n'installe les mises à jour automatiquement.
  - **Ne pas vérifier la disponibilité de mises à jour :** ce paramètre ne recherche pas de nouvelles mises à jour, ni télécharge ou n'installe les mises à jour automatiquement. Les utilisateurs peuvent toujours installer les mises à jour manuellement.
- **Mises à jour critiques :** ce paramètre autorise l'installation automatique des mises à jour macOS critiques.
- **Installer automatiquement les mises à jour de xProtect, MRT et GateKeeper :** ce paramètre autorise les appareils macOS à installer automatiquement les mises à jour des logiciels de sécurité.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

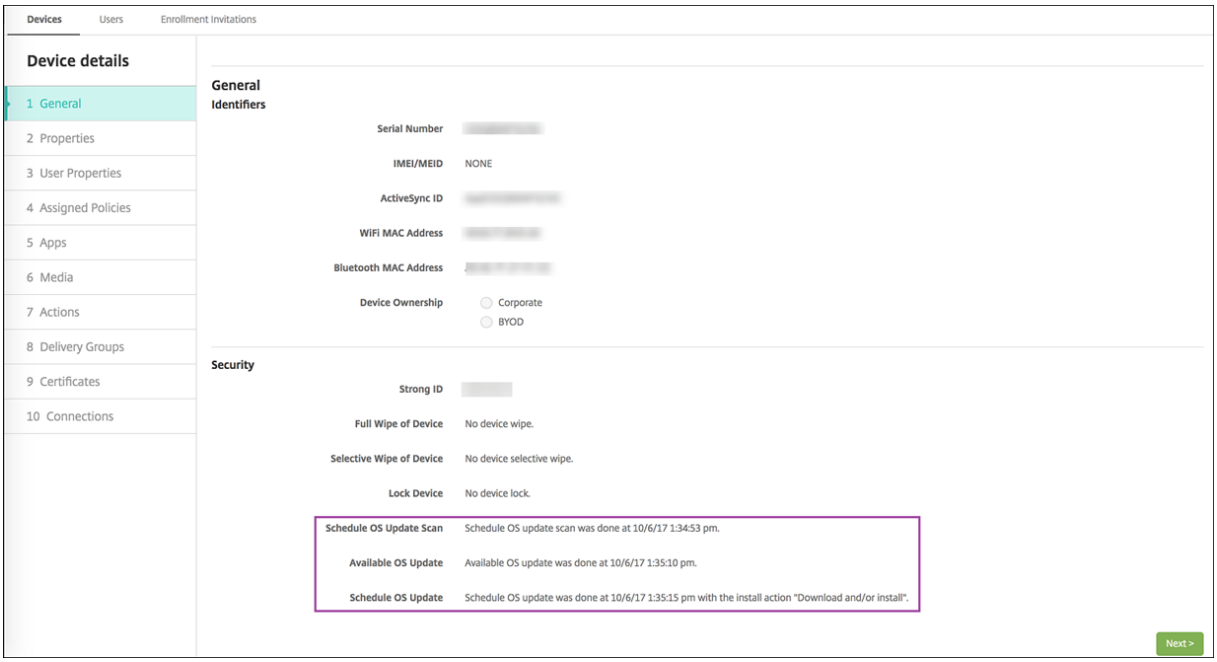
- **Autoriser l'installation de la pré-version de macOS :** ce paramètre permet aux utilisateurs d'installer les pré-versions du logiciel macOS.
- **Installer automatiquement les mises à jour des applications de l'App Store :** ce paramètre autorise la mise à jour automatique des applications de l'App Store.

Obtenir l'état des actions de mise à jour pour iOS et macOS

Pour iOS et macOS, Citrix Endpoint Management ne déploie pas la stratégie Contrôler mise à jour d'OS sur les appareils. Au lieu de cela, Citrix Endpoint Management utilise la stratégie d'envoi de ces commandes MDM aux appareils :

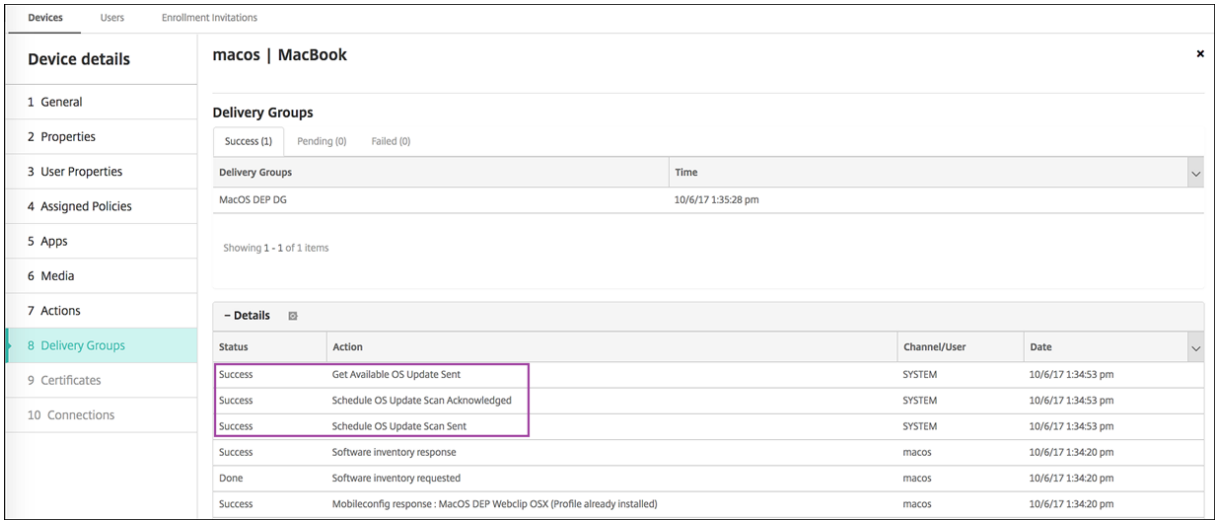
- Planification d'analyse de mise à jour d'OS : permet de demander à l'appareil d'effectuer une analyse en arrière-plan pour les mises à jour du système d'exploitation. (facultatif pour iOS)
- Mise à jour d'OS disponible : permet d'interroger l'appareil pour obtenir la liste des mises à jour du système d'exploitation disponibles.
- Planification de mise à jour d'OS : permet de demander à l'appareil d'effectuer des mises à jour macOS, des mises à jour de l'application ou les deux. Par conséquent, le système d'exploitation de l'appareil détermine lorsqu'il doit télécharger ou installer les mises à jour du système d'exploitation et de l'application.

La page **Gérer > Appareils > Détails de l'appareil (Général)** affiche l'état des analyses de mise à jour de système d'exploitation planifiées et disponibles et des mises à jour de macOS et d'applications planifiées.

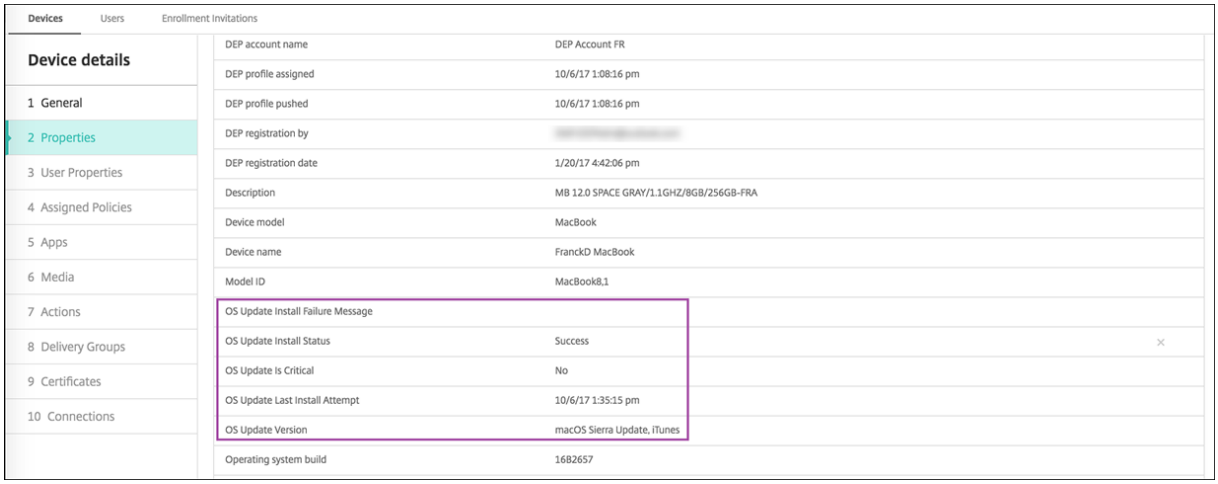


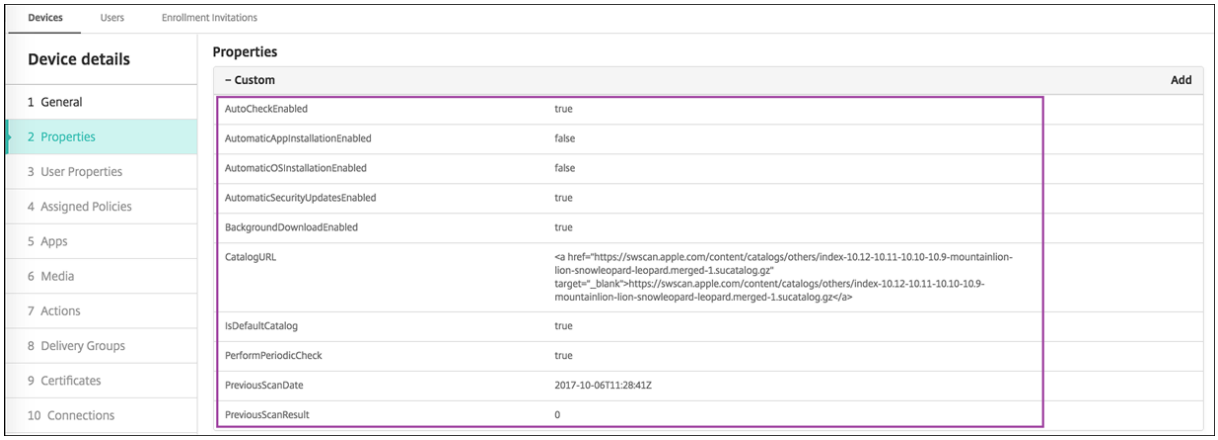
Pour de plus amples informations sur l'état des actions de mise à jour, accédez à la page **Gérer > Appareils > Détails de l'appareil (Groupes de mise à disposition)**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



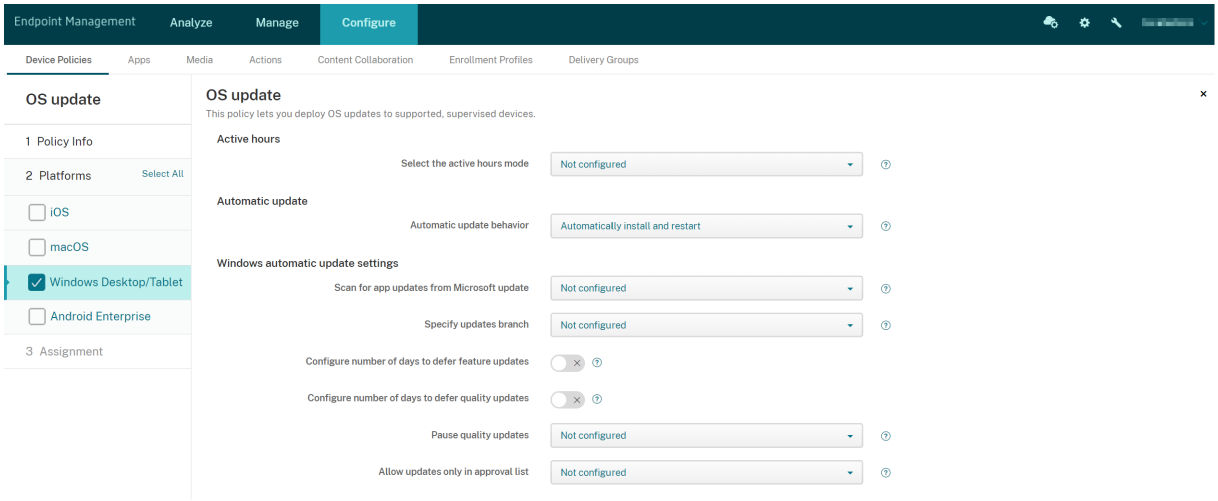
Pour de plus amples informations telles que les mises à jour du système d'exploitation disponibles et la dernière tentative d'installation, accédez à la page **Gérer > Appareils > Détails de l'appareil (Propriétés)**.





© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Windows Desktop et Tablet



- **Sélectionner le mode des heures d'activité :** sélectionnez un mode pour configurer les heures d'activité pour effectuer les mises à jour du système d'exploitation. Vous pouvez spécifier une plage d'heures ou une heure de début et de fin. Une fois que vous avez sélectionné un mode, des paramètres supplémentaires s'affichent : **Spécifier la plage maximale des heures d'activité** ou **Début des heures d'activité** et **Fin des heures d'activité**. **Non configuré** permet à Windows d'effectuer les mises à jour du système d'exploitation à tout moment. La valeur par défaut est **Non configuré**.
- **Comportement de mise à jour automatique :** configure le téléchargement, l'installation et le redémarrage du service de mise à jour Windows sur les appareils utilisateur. La valeur par défaut est **Installer automatiquement et redémarrer**.
  - **Avertir l'utilisateur avant de télécharger la mise à jour :** Windows avertit les utilisateurs lorsque des mises à jour sont disponibles. Windows ne télécharge et n'installe pas automatiquement les mises à jour. Les utilisateurs doivent lancer les actions de téléchargement et d'installation.
  - **Installer automatiquement et m'informer de planifier un redémarrage :** Windows télécharge automatiquement les mises à jour sur les réseaux non limités. Windows installe les mises à jour pendant la maintenance automatique lorsque l'appareil n'est pas utilisé et ne fonctionne pas sur batterie. Si la maintenance automatique ne peut pas installer les mises à jour pendant deux jours, Windows Update installe immédiatement les mises à jour. Si l'installation nécessite un redémarrage, Windows invite l'utilisateur à planifier l'heure de redémarrage. L'utilisateur a sept jours pour planifier le redémarrage. Après sept jours, Windows force l'appareil à redémarrer. Permettre à l'utilisateur de contrôler l'heure de démarrage réduit le risque de perte accidentelle de données causée par des applications qui ne s'arrêtent pas correctement au redémarrage.
  - **Installer automatiquement et redémarrer :** valeur par défaut. Windows télécharge au-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tomatiquement les mises à jour sur les réseaux non limités. Windows installe les mises à jour pendant la maintenance automatique lorsque l'appareil n'est pas utilisé et ne fonctionne pas sur batterie. Si la maintenance automatique ne peut pas installer les mises à jour pendant deux jours, Windows Update installe immédiatement les mises à jour. Si l'installation nécessite un redémarrage, Windows redémarre automatiquement l'appareil lorsque l'appareil est inactif.

  - **Installer automatiquement et redémarrer à une heure spécifiée :** lorsque vous choisissez cette option, d'autres paramètres apparaissent afin que vous puissiez spécifier le jour et l'heure. La valeur par défaut est 3 heures du matin tous les jours. L'installation automatique a lieu à l'heure spécifiée et le redémarrage de l'appareil se produit après un compte à rebours de 15 minutes. Lorsque Windows est prêt à redémarrer, un utilisateur connecté peut interrompre le compte à rebours de 15 minutes pour retarder le redémarrage.
  - **Installer automatiquement et redémarrer sans intervention de l'utilisateur :** Windows télécharge automatiquement les mises à jour sur des réseaux non limités. Windows installe les mises à jour pendant la maintenance automatique lorsque l'appareil n'est pas utilisé et ne fonctionne pas sur batterie. Si la maintenance automatique ne peut pas installer les mises à jour pendant deux jours, Windows Update installe immédiatement les mises à jour. Si l'installation nécessite un redémarrage, Windows redémarre automatiquement l'appareil lorsque l'appareil est inactif. Cette option place également le panneau de contrôle de l'utilisateur en lecture seule.
  - **Désactiver les mises à jour automatiques :** désactive les mises à jour automatiques sur l'appareil.

- **Rechercher des mises à jour d'applications depuis Microsoft Update :** indique si Windows accepte les mises à jour pour les autres applications Microsoft depuis le service de mise à jour Microsoft. La valeur par défaut est **Non configuré**.

  - **Non configuré :** utilisez ce paramètre si vous ne souhaitez pas configurer le comportement. Windows ne modifie pas l'interface utilisateur associée sur les appareils utilisateur. Les utilisateurs peuvent accepter ou refuser les mises à jour pour d'autres applications de Microsoft.
  - **Oui :** Windows autorise l'installation des mises à jour d'application à partir du service de mise à jour de Windows. Le paramètre associé sur l'appareil utilisateur est inactif, de sorte que l'utilisateur ne peut pas modifier le paramètre.
  - **Non :** Windows n'autorise pas l'installation des mises à jour d'application à partir du service de mise à jour de Windows. Le paramètre associé sur l'appareil utilisateur est inactif, de sorte que l'utilisateur ne peut pas modifier le paramètre.

- **Spécifier la branche des mises à jour :** indique la branche de service de mise à jour Windows à utiliser pour les mises à jour. La valeur par défaut est **Non configuré**.

  - **Non configuré :** utilisez ce paramètre si vous ne souhaitez pas configurer le comporte-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ment. Windows ne modifie pas l'interface utilisateur associée sur les appareils utilisateur. Les utilisateurs peuvent choisir une branche de service de mise à jour Windows.
  - **Current Branch :** Windows reçoit les mises à jour à partir de la branche actuelle. Le paramètre associé sur l'appareil utilisateur est inactif, de sorte que l'utilisateur ne peut pas modifier le paramètre.
  - **Current Branch for Business :** Windows reçoit les mises à jour à partir de la branche actuelle pour les entreprises. Le paramètre associé sur l'appareil utilisateur est inactif, de sorte que l'utilisateur ne peut pas modifier le paramètre.

- **Configurer le nombre de jours pendant lequel différer les mises à jour de fonctionnalité :** si cette option est **activée**, Windows diffère les mises à jour du nombre de jours spécifié et l'utilisateur ne peut pas modifier le paramètre. Si cette option est **désactivée**, l'utilisateur peut modifier le nombre de jours pour différer la mise à jour des fonctionnalités. La valeur par défaut est **Désactivé**.
- **Configurer le nombre de jours pendant lequel différer les mises à jour qualité :** si cette option est **activée**, Windows diffère les mises à jour du nombre de jours spécifié et l'utilisateur ne peut pas modifier le paramètre. Si cette option est **désactivée**, l'utilisateur peut modifier le nombre de jours pour différer la mise à jour qualité. La valeur par défaut est **Désactivé**.
- **Suspendre les mises à jour qualité :** indique s'il faut suspendre les mises à jour qualité pendant 35 jours. La valeur par défaut est **Non configuré**.
  - **Non configuré :** utilisez ce paramètre si vous ne souhaitez pas configurer le comportement. Windows ne modifie pas l'interface utilisateur associée sur les appareils utilisateur. Les utilisateurs peuvent choisir de suspendre les mises à jour qualité pendant 35 jours.
  - **Oui :** Windows interrompt l'installation des mises à jour qualité provenant du service Windows Update pendant 35 jours. Le paramètre associé sur l'appareil utilisateur est inactif, de sorte que l'utilisateur ne peut pas modifier le paramètre.
  - **Non :** Windows n'interrompt pas l'installation des mises à jour qualité provenant du service Windows Update. Le paramètre associé sur l'appareil utilisateur est inactif, de sorte que l'utilisateur ne peut pas modifier le paramètre.

- **Autoriser uniquement les mises à jour figurant dans la liste d'approbation :** indique si vous souhaitez installer uniquement les mises à jour qu'un serveur MDM approuve. Citrix Endpoint Management ne prend pas en charge la configuration d'une liste de mises à jour approuvée. La valeur par défaut est **Non configuré**.
  - **Non configuré :** utilisez ce paramètre si vous ne souhaitez pas configurer le comportement. Windows ne modifie pas l'interface utilisateur associée sur les appareils utilisateur. Les utilisateurs peuvent choisir les mises à jour à autoriser.
  - **Oui, installer uniquement les mises à jour approuvées :** permet l'installation de mises à jour approuvées uniquement.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Non, installer toutes les mises à jour applicables :** permet l'installation des mises à jour applicables sur l'appareil.

- **Utiliser le serveur de mise à jour interne :** indique si les mises à jour doivent être obtenues à partir du service de mise à jour de Windows ou d'un serveur de mise à jour interne via Windows Server Update Services (WSUS). Si cette option est **désactivée**, les appareils utilisent le service de mise à jour de Windows. Si cette option est **activée**, les appareils se connectent au serveur WSUS spécifié pour les mises à jour. La valeur par défaut est **Désactivé**.

  - **Accepter les mises à jour signées par des entités autres que Microsoft :** indique s'il faut accepter les mises à jour signées par des entités tierces autres que Microsoft. Cette fonctionnalité requiert que l'appareil approuve le certificat du fournisseur tiers. La valeur par défaut est **Désactivé**.
  - **Autoriser la connexion au service de mise à jour Microsoft :** permet au service de mise à jour Windows de l'appareil de se connecter régulièrement au service de mise à jour Microsoft, même si l'appareil est configuré pour recevoir les mises à jour depuis un serveur WSUS. La valeur par défaut est **Activé**.
  - **Serveur WSUS :** spécifiez l'URL du serveur WSUS.
  - **Serveur intranet secondaire pour héberger les mises à jour :** spécifiez une adresse URL de serveur intranet secondaire pour héberger les mises à jour et recevoir des rapports.

- **Configurer optimisation de la distribution :** indiquez si l'optimisation de la distribution doit être utilisée pour les mises à jour de Windows 10 et Windows 11. La valeur par défaut est **Off**.
- **Taille du cache :** taille maximale du cache d'optimisation de la distribution. Une valeur de **0** signifie un cache illimité. La valeur par défaut est de **10** Go.
- **Autoriser mise en cache des homologues VPN :** permet d'autoriser les appareils à participer à la mise en cache des homologues lorsqu'ils sont connectés au réseau de domaine via VPN. Lorsque cette option est **activée**, l'appareil peut être téléchargé depuis ou chargé vers d'autres appareils du réseau de domaine, que ce soit sur un VPN ou sur le réseau de domaine d'entreprise. La valeur par défaut est **Off**.
- **Méthode de téléchargement :** méthode de téléchargement que l'optimisation de la distribution peut utiliser pour les téléchargements de mises à jour Windows, d'applications et de mises à jour d'applications. La valeur par défaut est **HTTP fusionné avec une homologation derrière le même NAT**. Les options sont les suivantes :

  - **HTTP uniquement, sans homologation :** désactive la mise en cache des homologues, mais permet une optimisation de la distribution pour télécharger le contenu à partir des serveurs Windows Update ou des serveurs WSUS (Windows Server Update Services).
  - **HTTP fusionné avec une homologation derrière le même NAT :** active le partage entre homologues sur le même réseau. Le service cloud Optimisation de la distribution recherche d'autres clients qui se connectent à Internet en utilisant la même adresse IP publique que le client cible. Ces clients tentent ensuite de se connecter à d'autres

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

homologues sur le même réseau en utilisant leur adresse IP de sous-réseau privée.
  - **HTTP fusionné avec une homologation de groupe privé :** sélectionne automatiquement un groupe en fonction du site des services de domaine Active Directory (AD DS) de l'appareil ou du domaine auprès duquel l'appareil s'authentifie. L'homologation se produit sur des sous-réseaux internes, entre des appareils appartenant au même groupe, y compris des appareils dans des bureaux distants.
  - **HTTP fusionné avec une homologation Internet :** permet d'activer les sources homologues Internet pour l'optimisation de la distribution.
  - **Mode de téléchargement simple, sans homologation :** permet de désactiver l'utilisation des services cloud Optimisation de la distribution. L'optimisation de la distribution passe automatiquement à ce mode dans les conditions suivantes : lorsque les services cloud Optimisation de la distribution sont indisponibles, inaccessibles ou lorsque la taille du fichier de contenu est inférieure à 10 Mo. Dans ce mode, l'optimisation de la distribution fournit une expérience de téléchargement fiable, sans mise en cache partagé entre homologues.
  - **Ne pas utiliser l'optimisation de la distribution et utiliser BITS à la place :** permet aux clients d'utiliser BranchCache. Pour plus d'informations, veuillez consulter l'article Microsoft BranchCache.

- **Bande passante de téléchargement max. :** bande passante de téléchargement maximale en Ko/seconde. La valeur par défaut est **0**, ce qui signifie un ajustement dynamique de la bande passante.
- **Pourcentage de bande passante de téléchargement max.** : bande passante de téléchargement maximale que l'optimisation de la distribution peut utiliser pour toutes les activités de téléchargement simultanées. La valeur est un pourcentage de la bande passante de téléchargement disponible. La valeur par défaut est **0**, ce qui signifie un ajustement dynamique.
- **Bande passante de chargement max. :** bande passante de chargement maximale en Ko/seconde. La valeur par défaut est **0**. Une valeur de **0** signifie une bande passante illimitée.
- **Limite maximale mensuelle de chargement :** taille maximale en Go que l'optimisation de la distribution peut envoyer aux homologues Internet chaque mois. La valeur par défaut est de 20 Go. Une valeur de **0** signifie des chargements mensuels illimités.

Comment Citrix Endpoint Management gère les mises à jour approuvées pour les appareils Windows Desktop et Tablet

Vous pouvez spécifier si vous souhaitez installer uniquement les mises à jour approuvées. Citrix Endpoint Management gère les mises à jour comme suit :

- Pour une mise à jour de sécurité, par exemple pour les définitions Windows Defender, Citrix Endpoint Management approuve automatiquement la mise à jour et envoie une commande d'installation à l'appareil lors de la prochaine synchronisation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Pour tous les autres types de mise à jour, Citrix Endpoint Management attend votre approbation avant d'envoyer la commande d'installation à l'appareil.

Logiciels requis

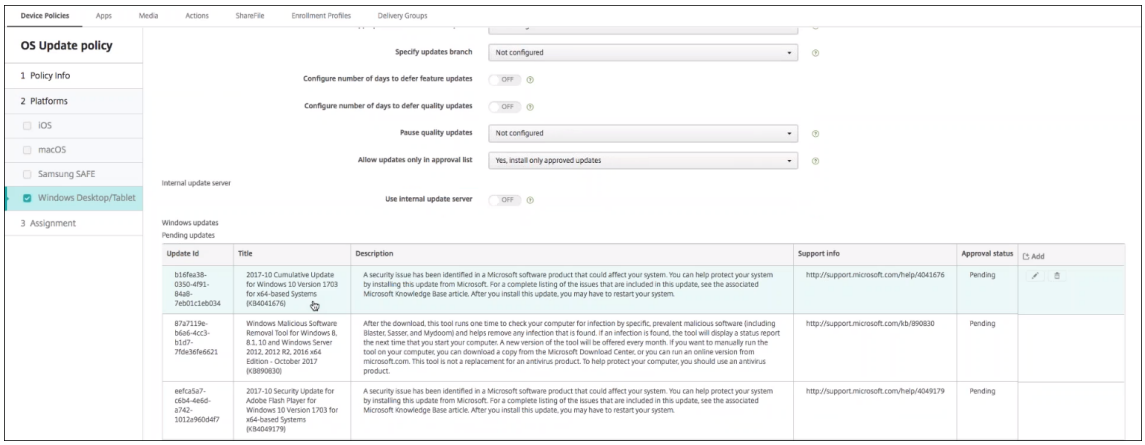
- Vous devez charger le certificat racine de Microsoft sur Citrix Endpoint Management Server en tant que certificat de serveur.
- Pour plus d'informations sur l'importation d'un certificat de serveur, consultez la section « Pour importer un certificat » dans Certificats et authentification.

Pour installer uniquement les mises à jour approuvées

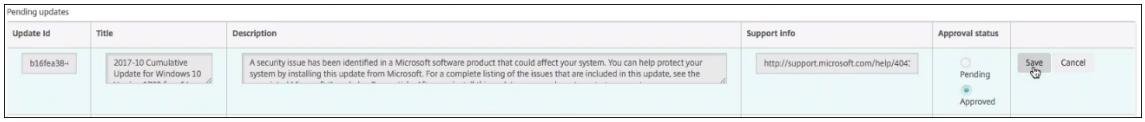
1. Accédez à **Configurer > Stratégies d'appareil** et ouvrez la stratégie de mise à jour d'OS.
2. Définissez le paramètre **Autoriser uniquement les mises à jour figurant dans la liste d'approbation** sur **Oui, installer uniquement les mises à jour approuvées**.

Pour approuver une mise à jour

1. Dans la stratégie de mise à jour d'OS, faites défiler l'écran jusqu'au tableau **Mises à jour disponible**. Citrix Endpoint Management obtient les mises à jour répertoriées dans le tableau à partir des appareils.
2. Recherchez les mises à jour avec l'**État d'approbation En attente**.
3. Cliquez sur la ligne correspondant à la mise à jour que vous souhaitez approuver, puis sur l'icône de modification de cette ligne (dans la colonne **Ajouter**).



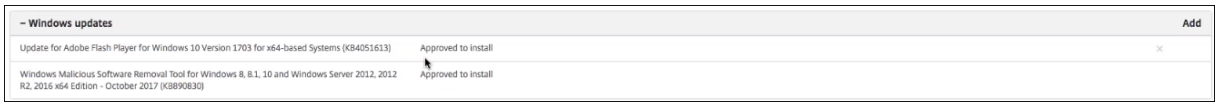
4. Pour autoriser la mise à jour, cliquez sur **Approuvé**, puis cliquez sur **Enregistrer**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Remarque :**
>
> bien que le tableau des mises à jour en attente propose des commandes d'ajout et de suppression, ces commandes n'entraînent aucune modification de la base de données Citrix Endpoint Management. La modification de l'état d'approbation est la seule action disponible pour les mises à jour en attente.

Pour afficher l'état de la mise à jour Windows pour un appareil, accédez à **Gérer > Appareils > Propriétés**.



Lorsqu'une mise à jour est publiée, l'**ID de mise à jour** apparaît dans la première colonne avec un état (Réussite ou Échec). Vous pouvez créer un rapport ou une action automatisée pour les appareils dont les mises à jour ont échoué. La date et l'heure de la publication apparaissent également.

Fonctionnement des mises à jour pour les déploiements initiaux et ultérieurs L'effet de la stratégie de mise à jour d'OS sur les appareils diffère s'il s'agit d'un déploiement initial ou d'un déploiement effectué une fois que les appareils ont obtenu des mises à jour.

- Pour que Citrix Endpoint Management interroge un appareil sur les mises à jour, vous devez configurer et attribuer à un groupe de mise à disposition au moins une stratégie de mise à jour d'OS.

  Citrix Endpoint Management envoie une requête à un appareil sur les mises à jour installables lors d'une synchronisation MDM de l'appareil.

- Après le déploiement de la première stratégie de mise à jour d'OS, la liste des mises à jour de Windows est vide car aucun appareil n'a encore été signalé.

- Lorsque les appareils dans le groupe de mise à disposition attribué signalent des mises à jour, Citrix Endpoint Management enregistre ces mises à jour dans sa base de données. Pour approuver les mises à jour signalées, modifiez à nouveau la stratégie.

  L'approbation de mise à jour s'applique uniquement à la stratégie que vous modifiez. Les mises à jour approuvées dans une stratégie ne s'affichent pas comme approuvées dans une autre stratégie. La prochaine fois qu'un appareil se synchronise, Citrix Endpoint Management envoie une commande à l'appareil pour indiquer que la mise à jour est approuvée.

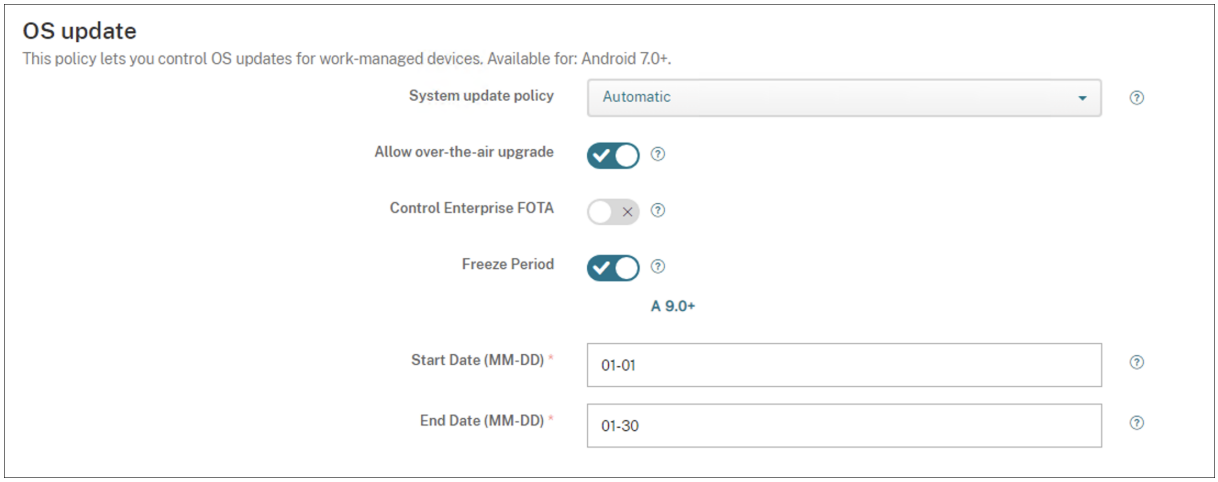
- Pour une deuxième stratégie de mise à jour d'OS, la liste de mises à jour contient les mises à jour stockées dans la base de données Citrix Endpoint Management. Approuvez les mises à jour pour chaque stratégie.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Lors de chaque synchronisation de l'appareil, Citrix Endpoint Management interroge l'appareil sur l'état de la mise à jour approuvée jusqu'à ce que l'appareil signale une mise à jour comme étant installée. Pour les mises à jour nécessitant le redémarrage après l'installation de la mise à jour, Citrix Endpoint Management interroge l'état de la mise à jour jusqu'à ce que l'appareil la signale comme étant installée.

- Citrix Endpoint Management ne limite pas les mises à jour affichées sur la page de configuration de la stratégie par groupe de mise à disposition ou appareil. Toutes les mises à jour signalées par les appareils apparaissent dans la liste.

Paramètres Android Enterprise



- **Stratégie de mise à jour du système :** permet de déterminer quand les mises à jour système se produisent. Si l'option **Contrôler Enterprise FOTA** est activée, les mises à jour se produisent automatiquement, quelle que soit la configuration de ce paramètre.
  - **Automatique :** installe une mise à jour lorsqu'elle est disponible.
  - **Créneau :** installe une mise à jour automatiquement dans la fenêtre de maintenance quotidienne spécifiée dans **Heure de début** et **Heure de fin**.
    - **Heure de début :** le début de la fenêtre de maintenance mesurée en nombre de minutes (**0** - **1440**) à partir de minuit dans l'heure locale de l'appareil. La valeur par défaut est **0**.
    - **Heure de fin :** la fin de la fenêtre de maintenance mesurée en nombre de minutes (**0** - **1440**) à partir de minuit dans l'heure locale de l'appareil. La valeur par défaut est **120**.
  - **Reporter :** permet à un utilisateur de reporter une mise à jour jusqu'à 30 jours.
  - **Valeur par défaut :** définit la stratégie de mise à jour sur la valeur par défaut du système.
- **Autoriser mise à jour par réseau cellulaire :** si cette option est désactivée, les machines utilisateur ne peuvent pas recevoir les mises à jour logicielles sans fil. La valeur par défaut est **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Freeze Period :** (Période de blocage) si cette option est **activée**, les mises à jour du système d'exploitation ne sont pas installées sur l'appareil pendant la période spécifiée pour les stratégies de mise à jour **Automatique**, **Reporter** et **Créneau**. Vous ne pouvez définir qu'une seule période de blocage à la fois pour un appareil. La durée de la période de blocage ne peut pas dépasser 90 jours.
  - **Date de début/Date de fin :** plage de dates pendant laquelle les mises à jour du système d'exploitation ne sont pas installées si la **période de blocage** est activée.

- **Freeze Period :** (Période de blocage) si cette option est **activée**, les mises à jour du système d'exploitation ne sont pas installées sur l'appareil pendant la période spécifiée pour les stratégies de mise à jour **Automatique**, **Reporter** et **Créneau**. Vous ne pouvez définir qu'une seule période de blocage à la fois pour un appareil. La durée de la période de blocage ne peut pas dépasser 90 jours.
  - **Date de début/Date de fin :** plage de dates pendant laquelle les mises à jour du système d'exploitation ne sont pas installées si la **période de blocage** est activée.

Stratégie de code secret

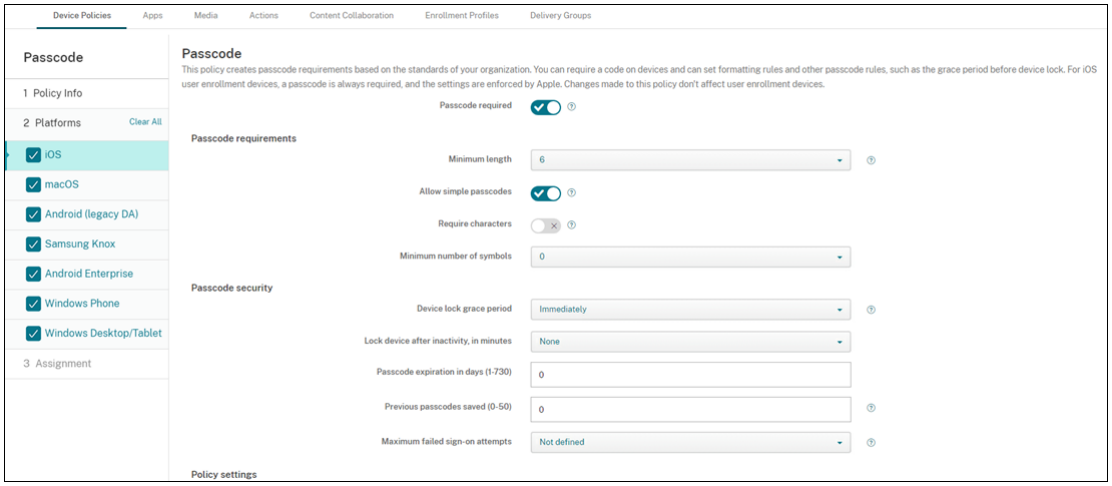
November 29, 2023

Créez une stratégie de code secret dans Citrix Endpoint Management en fonction des normes de votre organisation. Vous pouvez exiger la saisie de codes secrets sur les appareils des utilisateurs et définir diverses règles de code secret et de formatage. Créez des stratégies pour iOS, macOS, Android, Android Enterprise et Windows Desktop/Tablet. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres iOS



- **Code secret requis :** sélectionnez cette option pour exiger la saisie d'un mot de passe et afficher les options de configuration d'une stratégie de code secret pour iOS. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret, sécurité et paramètres de stratégie.
- **Exigences en matière de code secret**
  - **Longueur minimale :** dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est **6**.
  - **Autoriser les codes secrets simples :** sélectionnez cette option pour autoriser les codes secrets simples. Les codes secrets simples se caractérisent par des caractères répétés ou séquentiels. La valeur par défaut est **On**.
  - **Caractères requis :** sélectionnez cette option pour exiger que les codes secrets contiennent au moins une lettre. La valeur par défaut est **Off**.
  - **Nombre minimum de symboles :** dans la liste, cliquez sur le nombre de symboles que le code secret doit contenir. La valeur par défaut est **0**.
- **Sécurité du code secret**
  - **Période de grâce avant verrouillage de l'appareil :** dans la liste, cliquez sur la durée après laquelle les utilisateurs doivent entrer un code secret pour déverrouiller un appareil verrouillé. La valeur par défaut est **Immédiatement**.
  - **Verrouiller appareil après période d'inactivité :** dans la zone, entrez la durée pendant laquelle un appareil peut rester inactif avant d'être verrouillé. La valeur peut être comprise entre 1 et 15 minutes. Définissez la valeur sur **Aucun** pour désactiver la stratégie. La valeur par défaut est **Aucun**.
  - **Expiration du code secret en jours (1-730) :** entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.

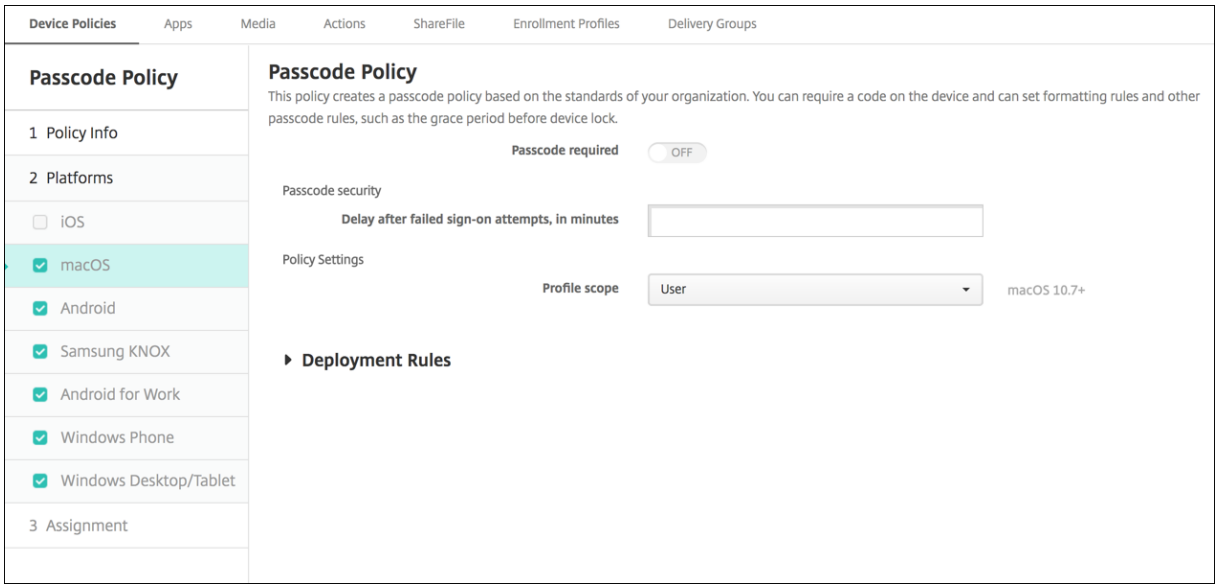
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Mots de passe précédents enregistrés (0-50) :** entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
- **Nombre maximum de tentatives de connexion infructueuses :** dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses.
  * Si vous définissez ce nombre sur une valeur supérieure à 6, après la sixième tentative, l'appareil impose un délai entre les tentatives. Le délai augmente à chaque échec. Après la dernière tentative, toutes les données et les paramètres sont effacés.
  * Si vous définissez ce nombre sur 6 ou moins, l'appareil est effacé sans délai.
  * Si vous sélectionnez **Non défini**, après 6 tentatives, les appareils imposent une limite de temps entre les tentatives mais aucun effacement n'a lieu.

  La valeur par défaut est **Aucun nombre défini**.

- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Paramètres macOS



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Code secret requis :** sélectionnez cette option pour exiger la saisie d'un mot de passe et afficher les options de configuration d'une stratégie de code secret pour iOS. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret, sécurité et paramètres de stratégie.
- Si **Code secret requis** est désactivé, en regard de **Délai après les échecs de tentatives de connexion, en minutes**, entrez le nombre de minutes après lesquelles les utilisateurs peuvent retenter de saisir leur code secret.
- Si vous activez **Code secret requis**, configurez les paramètres suivants :
- **Exigences en matière de code secret**
  - **Longueur minimale :** dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est **6**.
  - **Autoriser les codes secrets simples :** sélectionnez cette option pour autoriser les codes secrets simples. Les codes secrets simples se caractérisent par des caractères répétés ou séquentiels. La valeur par défaut est **On**.
  - **Caractères requis :** sélectionnez cette option pour exiger que les codes secrets contiennent au moins une lettre. La valeur par défaut est **Off**.
  - **Nombre minimum de symboles :** dans la liste, cliquez sur le nombre de symboles que le code secret doit contenir. La valeur par défaut est **0**.
- **Sécurité du code secret**
  - **Période de grâce avant verrouillage de l'appareil :** dans la liste, cliquez sur la durée après laquelle les utilisateurs doivent entrer un code secret pour déverrouiller un appareil verrouillé. La valeur par défaut est **Aucun**.
  - **Verrouiller appareil après période d'inactivité :** dans la liste, cliquez sur la durée pendant laquelle un appareil peut rester inactif avant d'être verrouillé. La valeur peut être comprise entre 1 et 5 minutes. Définissez la valeur sur **Aucun** pour désactiver la stratégie. La valeur par défaut est **Aucun**.
  - **Expiration du code secret en jours (1-730) :** entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
  - **Mots de passe précédents enregistrés (0-50) :** entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
  - **Nombre maximum de tentatives de connexion infructueuses :** dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses.
    - Si vous définissez ce nombre sur une valeur supérieure à 6, après la sixième tentative, l'appareil impose un délai entre les tentatives. Le délai augmente à chaque échec. Après la dernière tentative, l'appareil se verrouille.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * Si vous définissez ce nombre sur 6 ou moins, l'appareil se verrouille sans délai.
    * Si vous sélectionnez **Non défini**, après 6 tentatives, les appareils imposent une limite de temps entre les tentatives mais ne se verrouillent pas.

  La valeur par défaut est **Aucun nombre défini**.

  – **Délai après les échecs de tentatives de connexion, en minutes :** entrez le nombre de minutes avant que la fenêtre de connexion ne s'affiche après qu'un utilisateur a atteint le nombre maximal de tentatives infructueuses.

  – **Forcer la réinitialisation du code d'accès :** Si ce paramètre est **désactivé**, les utilisateurs n'ont pas besoin de réinitialiser leur code secret la prochaine fois qu'ils s'authentifient une fois que leur appareil a reçu cette stratégie La valeur par défaut est **On**.

- **Paramètre de stratégie**

  – **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.

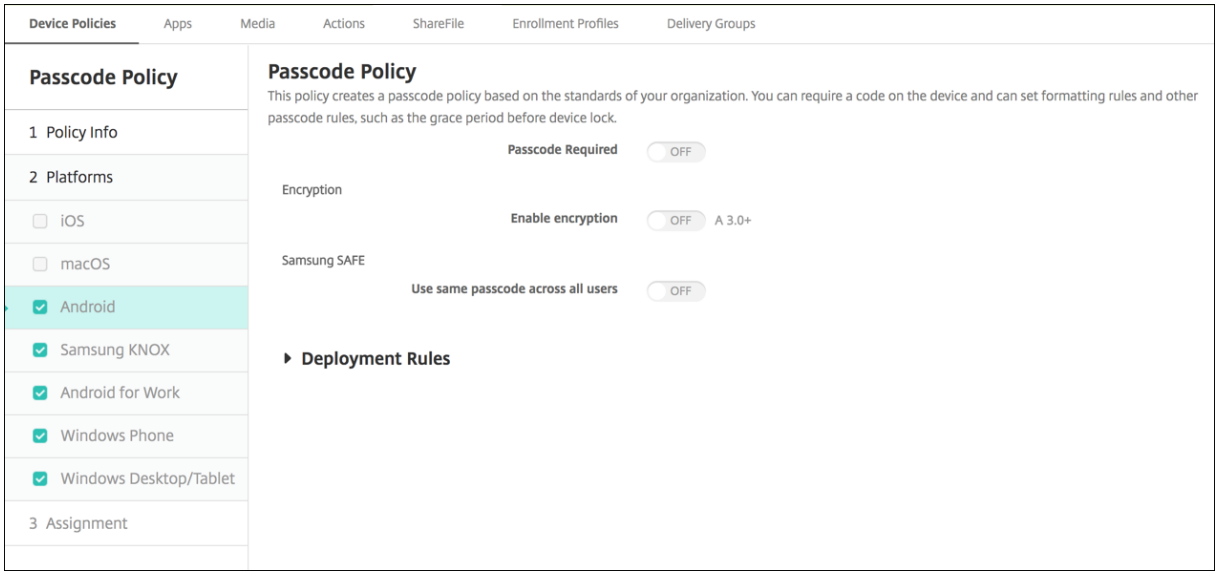
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.

  – **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.

  – **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Android (DA hérité)



> **Remarque :**
>
> Le paramètre par défaut pour Android est **Désactivé**.

- **Code secret requis :** sélectionnez cette option pour exiger la saisie d'un mot de passe et afficher les options de configuration d'une stratégie de code secret pour Android. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret, sécurité du code secret, et cryptage.
- **Exigences en matière de code secret**
  - **Longueur minimale :** dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est 6.
  - **Reconnaissance biométrique :** sélectionnez cette option pour activer la reconnaissance biométrique. Si vous activez cette option, le champ Caractères requis est masqué. La valeur par défaut est **Off**.
  - **Caractères requis :** dans la liste, cliquez sur **Aucune restriction**, **Chiffres et lettres**, **Chiffres uniquement** ou **Lettres uniquement** pour configurer la manière dont les codes secrets sont composés. La valeur par défaut est **Aucune restriction**.
  - **Règles avancées :** sélectionnez cette option si vous souhaitez appliquer des règles de code secret avancées. La valeur par défaut est **Off**.
  - Lorsque le paramètre **Règles avancées** est activé, à partir de chacune des listes suivantes et pour chaque type de caractère, cliquez sur le nombre minimal de caractère qu'un code secret doit contenir :
    - **Symboles :** nombre minimal de symboles.
    - **Lettres :** nombre minimal de lettres.
    - **Minuscules :** nombre minimum de minuscules.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Majuscules :** nombre minimum de majuscules.
    * **Chiffres ou symboles :** nombre minimal de chiffres ou de symboles.
    * **Chiffres :** nombre minimal de chiffres.

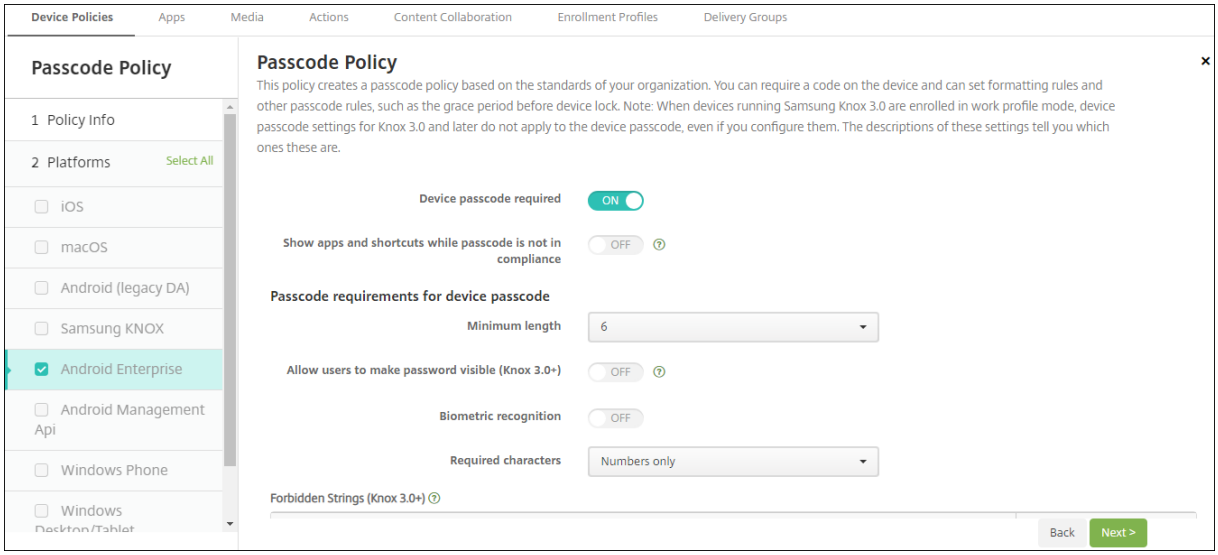
- **Sécurité du code secret**
  - **Verrouiller appareil après période d'inactivité :** dans la liste, cliquez sur la durée pendant laquelle un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est **Aucune**.
  - **Expiration du code secret en jours (1-730) :** entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
  - **Mots de passe précédents enregistrés (0-50) :** entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
  - **Nombre maximum de tentatives de connexion infructueuses :** dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil est effacé. La valeur par défaut est **Aucun nombre défini**.

- **Chiffrement**
  - **Activer le chiffrement :** sélectionnez cette option si vous souhaitez activer le chiffrement. L'option est disponible, que le paramètre **Code secret requis** soit sélectionné ou non.

    Pour crypter leurs appareils, les utilisateurs doivent commencer avec une batterie chargée et laisser l'appareil branché pendant le délai nécessaire au cryptage. Le processus peut prendre une heure ou plus. Si le processus de cryptage est interrompu, les utilisateurs risquent de perdre certaines ou toutes les données de leurs appareils. Une fois qu'un appareil est crypté, le processus ne peut pas être annulé sauf en effectuant une réinitialisation d'usine, ce qui entraîne la suppression de toutes les données de l'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Android Enterprise



Pour les appareils Android Enterprise, vous pouvez demander un code secret pour l'appareil ou une question de sécurité pour le profil de travail Android Enterprise ou les deux.

- **Code secret de l'appareil requis :** exige un code secret sur l'appareil. Lorsque ce paramètre est défini sur **Activé**, configurez les paramètres sous **Exigences de code secret de l'appareil** et **Sécurité du code secret de l'appareil**. La valeur par défaut est **Off**.
- **Afficher les applications et les raccourcis bien que le code d'accès ne soit pas conforme :**lorsque ce paramètre est **activé**, les applications et les raccourcis de l'appareil ne sont pas masqués, même lorsque le code d'accès n'est pas conforme. Lorsque ce paramètre est **désactivé**, les applications et les raccourcis sont masqués lorsque le code d'accès n'est pas conforme. Si vous activez ce paramètre, Citrix vous recommande de créer une action automatisée pour marquer l'appareil comme non conforme lorsque le code d'accès n'est pas conforme. La valeur par défaut est **Off**.
- **Exigences de code secret de l'appareil :**
  - **Longueur minimale :** spécifie la longueur minimale du code secret. La valeur par défaut est 6.
  - **Reconnaissance biométrique :** active la reconnaissance biométrique. Si ce paramètre est défini sur **Activé**, le champ **Caractères requis** est masqué. La valeur par défaut est **Off**.
  - **Caractères requis :** spécifie les types de caractères requis pour les codes secrets. Dans la liste, choisissez **Aucune restriction**, **Lettres et chiffres**, **Chiffres uniquement** ou **Lettres uniquement**. Utilisez **Aucune restriction** uniquement pour les appareils exécutant Android 7.0. Android 7.1 et versions ultérieures n'appliquent pas le paramètre **Aucune restriction**. La valeur par défaut est **Chiffres et lettres**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Règles avancées :** applique des règles avancées pour les types de caractères pouvant apparaître dans les codes secrets. Lorsque ce paramètre est défini sur **Activé**, configurez les paramètres sous **Nombre minimum de** et **Nombre maximum de**. Ce paramètre n'est pas disponible pour les appareils Android de versions antérieures à Android 5.0. La valeur par défaut est **Off**.
  - **Nombre minimum de :**
    * **Symboles :** spécifie le nombre minimal de symboles. La valeur par défaut est **0**.
    * **Lettres :** spécifie le nombre minimal de lettres. La valeur par défaut est **0**.
    * **Minuscules :** spécifie le nombre minimal de minuscules. La valeur par défaut est **0**.
    * **Majuscules :** spécifie le nombre minimal de majuscules. La valeur par défaut est **0**.
    * **Chiffres ou symboles :** spécifie le nombre minimal de chiffres ou de symboles. La valeur par défaut est **0**.
    * **Chiffres :** spécifie le nombre minimal de chiffres. La valeur par défaut est **0**.
    * **Caractères modifiés :** paramètre utilisé pour les appareils fonctionnant sous Samsung Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée. Uniquement pour les appareils entièrement gérés. Ce paramètre ne s'applique pas aux appareils inscrits en tant qu'appareils avec profil de travail. Spécifie le nombre de caractères que les utilisateurs doivent modifier par rapport à leur code secret précédent. La valeur par défaut est **0**.
  - **Nombre maximum de :** paramètre utilisé pour les appareils fonctionnant sous Samsung Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée. Uniquement pour les appareils entièrement gérés. Ce paramètre ne s'applique pas aux appareils inscrits en tant qu'appareils avec profil de travail.
    * **Nombre d'occurrences d'un caractère :** spécifie le nombre maximal d'occurrences d'un caractère dans un code secret. La valeur par défaut est **0**, ce qui signifie qu'il n'y a pas de limite maximale.
    * **Longueur des séquences alphabétiques :** spécifie la longueur maximale d'une séquence alphabétique dans un code secret. La valeur par défaut est **0**, ce qui signifie qu'il n'y a pas de limite maximale.
    * **Longueur des séquences numériques :** spécifie la longueur maximale d'une séquence numérique dans un code secret. La valeur par défaut est **0**, ce qui signifie qu'il n'y a pas de limite maximale.

- **Complexité du code d'accès de l'appareil (Android 12+) :**
  - **Appliquer complexité de code d'accès :** nécessite un mot de passe dont le niveau de complexité est défini par la plate-forme, plutôt qu'un mot de passe personnalisé. Uniquement pour les appareils disposant d'Android 12 ou version ultérieure et utilisant Citrix Secure Hub 22.9 ou version ultérieure.
  - **Niveau de complexité :** niveaux de complexité prédéfinis du mot de passe.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Aucun :** aucun mot de passe n'est requis.
    * **Faible :** les mots de passe peuvent être :
        · Un schéma
        · Un code PIN composé d'au moins quatre chiffres
    * **Moyen :** les mots de passe peuvent être :
        · Un code PIN sans séquences répétées (4444) ni séquences ordonnées (1234), et composé d'au moins quatre chiffres
        · Alphabétiques et composés d'au moins quatre caractères
        · Alphanumériques et composés d'au moins quatre caractères
    * **Élevé :** les mots de passe peuvent être :
        · Un code PIN sans séquences répétées (4444) ni séquences ordonnées (1234), et composé d'au moins huit caractères
        · Alphabétiques et composés d'au moins six caractères
        · Alphanumériques et composés d'au moins six caractères

        > **Remarque :**
        > Pour les appareils BYOD, les paramètres du code d'accès tels que Longueur minimale, Caractères requis, Reconnaissance biométrique et Règles avancées ne sont pas applicables sur Android 12+. Utilisez plutôt la fonction de complexité de code d'accès.

- **Sécurité du code secret de l'appareil :**
  - **Effacer l'appareil après (tentatives de connexion infructueuses) :** indique le nombre de tentatives de connexion infructueuses pouvant être effectuées par l'utilisateur avant que l'appareil subisse un effacement complet. La valeur par défaut est **Aucun nombre défini**.
  - **Verrouiller appareil après période d'inactivité :** indique le nombre de minutes pendant lesquelles un appareil peut rester inactif avant d'être verrouillé. Définissez la valeur sur 0 pour désactiver la stratégie.
  - **Expiration du code secret en jours (1-730) :** indique le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
  - **Mots de passe précédents enregistrés (0-50) :** indique le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
- **Question de sécurité du profil de travail :** oblige les utilisateurs à répondre à une question de sécurité pour accéder aux applications exécutées dans un profil de travail Android Enterprise. Cette fonctionnalité est destinée aux appareils exécutant Android 7.0 et versions ultérieures. Lorsque ce paramètre est défini sur **Activé**, configurez les paramètres sous **Exigences de code**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

secret de la question de sécurité du profil de travail et **Sécurité du code secret de la question de sécurité du profil de travail**. La valeur par défaut est **Off**.

- **Exigences de code secret de validation de la sécurité du profil de travail :**
  - **Longueur minimale :** spécifie la longueur minimale du code secret. La valeur par défaut est 6.
  - **Reconnaissance biométrique :** active la reconnaissance biométrique. Si ce paramètre est défini sur **Activé**, le champ **Caractères requis** est masqué. La valeur par défaut est **Off**.
  - **Caractères requis :** spécifie les types de caractères requis pour les codes secrets. Dans la liste, choisissez **Aucune restriction**, **Lettres et chiffres**, **Chiffres uniquement** ou **Lettres uniquement**. Utilisez **Aucune restriction** uniquement pour les appareils exécutant Android 7.0. Android 7.1 et versions ultérieures n'appliquent pas le paramètre **Aucune restriction**. La valeur par défaut est **Chiffres et lettres**.
  - **Règles avancées :** applique des règles avancées pour les types de caractères pouvant apparaître dans les codes secrets. Lorsque ce paramètre est défini sur **Activé**, configurez les paramètres sous **Nombre minimum de** et **Nombre maximum de**. Ce paramètre n'est pas disponible pour les appareils Android de versions antérieures à Android 5.0. La valeur par défaut est **Off**.
  - **Nombre minimum de :**
    - **Symboles :** spécifie le nombre minimal de symboles. La valeur par défaut est **0**.
    - **Lettres :** spécifie le nombre minimal de lettres. La valeur par défaut est **0**.
    - **Minuscules :** spécifie le nombre minimal de minuscules. La valeur par défaut est **0**.
    - **Majuscules :** spécifie le nombre minimal de majuscules. La valeur par défaut est **0**.
    - **Chiffres ou symboles :** spécifie le nombre minimal de chiffres ou de symboles. La valeur par défaut est **0**.
    - **Chiffres :** spécifie le nombre minimal de chiffres. La valeur par défaut est **0**.
    - **Caractères modifiés :** paramètre utilisé pour les appareils fonctionnant sous Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée. Spécifie le nombre de caractères que les utilisateurs doivent modifier par rapport à leur code secret précédent. La valeur par défaut est **0**.
  - **Nombre maximum de :** paramètre utilisé pour les appareils fonctionnant sous Knox 3.0 et versions ultérieures qui ont une clé de licence Knox valide configurée.
    - **Nombre d'occurrences d'un caractère :** spécifie le nombre maximal d'occurrences d'un caractère dans un code secret. La valeur par défaut est **0**, ce qui signifie qu'il n'y a pas de limite maximale.
    - **Longueur des séquences alphabétiques :** spécifie la longueur maximale d'une séquence alphabétique dans un code secret. La valeur par défaut est **0**, ce qui signifie qu'il n'y a pas de limite maximale.
    - **Longueur des séquences numériques :** spécifie la longueur maximale d'une

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

séquence numérique dans un code secret. La valeur par défaut est **0**, ce qui signifie qu'il n'y a pas de limite maximale.

- **Complexité du code d'accès de la question de sécurité du profil professionnel (Android 12+) :**
  - **Appliquer complexité de code d'accès :** nécessite un mot de passe dont le niveau de complexité est défini par la plate-forme, plutôt qu'un mot de passe personnalisé. Uniquement pour les appareils disposant d'Android 12 ou version ultérieure et utilisant Citrix Secure Hub 22.9 ou version ultérieure.
  - **Niveau de complexité :** niveaux de complexité prédéfinis du mot de passe.
    - **Aucun :** aucun mot de passe n'est requis.
    - **Faible :** les mots de passe peuvent être :
      - Un schéma
      - Un code PIN composé d'au moins quatre chiffres
    - **Moyen :** les mots de passe peuvent être :
      - Un code PIN sans séquences répétées (4444) ni séquences ordonnées (1234), et composé d'au moins quatre chiffres
      - Alphabétiques et composés d'au moins quatre caractères
      - Alphanumériques et composés d'au moins quatre caractères
    - **Élevé :** les mots de passe peuvent être :
      - Un code PIN sans séquences répétées (4444) ni séquences ordonnées (1234), et composé d'au moins huit caractères
      - Alphabétiques et composés d'au moins six caractères
      - Alphanumériques et composés d'au moins six caractères

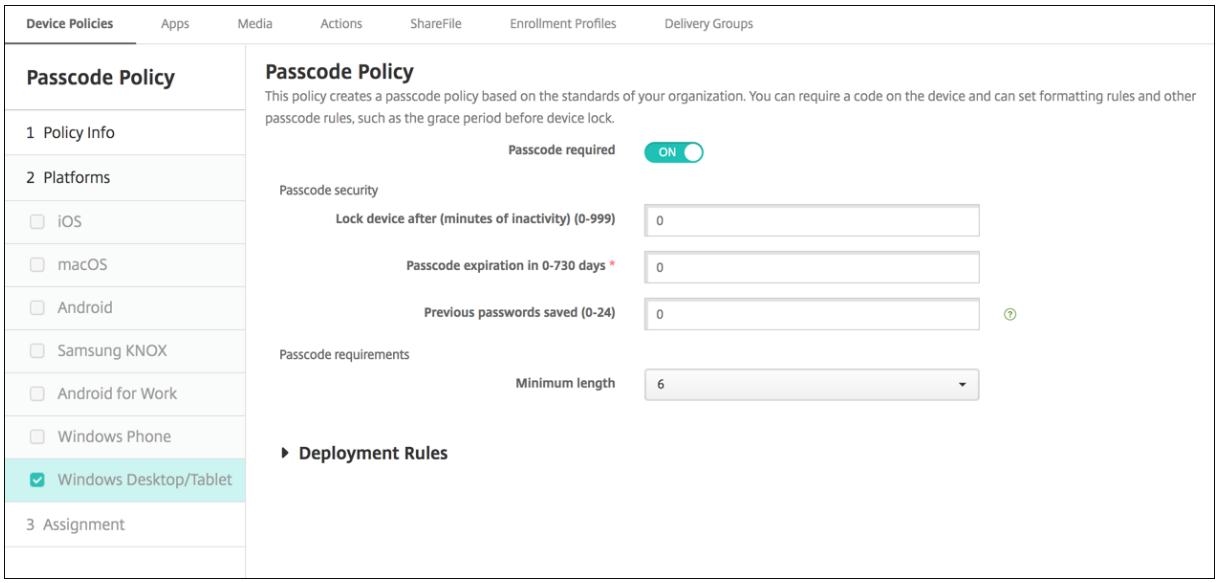
        > **Remarque :**
        > Si vous activez la complexité du code d'accès pour un profil de travail, vous devez également l'activer pour l'appareil.

- **Sécurité du code secret pour la question de sécurité du profil professionnel**
  - **Effacer le conteneur après (tentatives de connexion infructueuses) :** indique le nombre de tentatives de connexion infructueuses pouvant être effectuées par l'utilisateur avant que le profil de travail et ses données ne soient effacés de l'appareil. Les utilisateurs doivent réinitialiser le profil de travail après l'effacement. La valeur par défaut est **Aucun nombre défini**.
  - **Verrouiller conteneur après période d'inactivité :** indique le nombre de minutes pendant lesquelles un appareil peut rester inactif avant que le profil de travail ne soit verrouillé. La valeur peut être comprise entre 0 et 999 minutes. Définissez la valeur sur 0 pour désactiver la stratégie.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Expiration du code secret en jours (1-730) :** indique le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
- **Mots de passe précédents enregistrés (0-50) :** indique le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.

Paramètres Windows Desktop/Tablet



- **Code secret requis :** sélectionnez cette option pour ne pas exiger de code secret sur les appareils Windows Desktop/Tablet. Le paramètre par défaut est **Activé**, ce qui nécessite un code secret. La page se réduit et les options suivantes disparaissent lorsque vous désactivez ce paramètre.
- **Sécurité du code secret**
  - **Verrouiller appareil après période d'inactivité :** entrez le nombre de minutes pendant lesquelles un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est **0**.
  - **Expiration du code secret en jours (0 - 730) :** entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 0-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
  - **Mots de passe précédents enregistrés (0-24) :** entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des codes secrets figurant dans cette liste. Les valeurs autorisées sont 1-24. Entrez un nombre compris entre 1 et 24. La valeur par défaut est **0**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Exigences en matière de code secret**
  - **Longueur minimale :** dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est **6**.

Stratégie de période de grâce de verrouillage par code secret

December 9, 2021

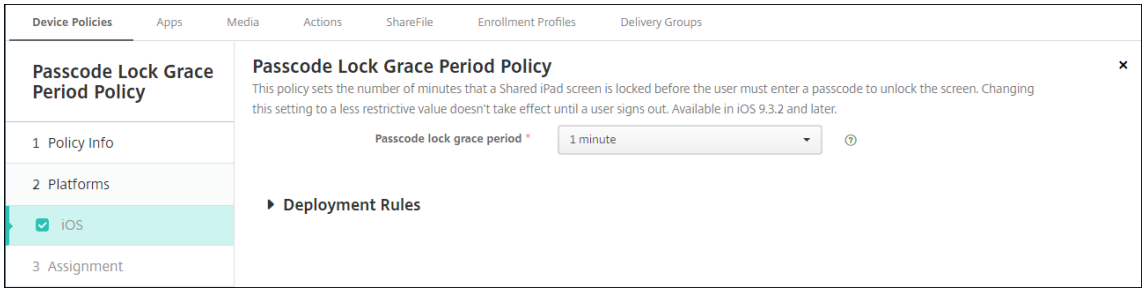
La stratégie de période de grâce de verrouillage par code secret est destinée aux appareils partagés exécutant iOS (iPadOS). Pour plus d'informations sur les iPads partagés, consultez la section Intégration avec les fonctionnalités Apple Éducation.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Période de grâce de verrouillage par code secret :** nombre de minutes pendant lesquelles un écran d'iPad partagé reste verrouillé avant que l'utilisateur ne doive entrer un code d'accès pour déverrouiller l'écran. Le réglage de ce paramètre sur une valeur moins restrictive ne prend pas effet jusqu'à ce qu'un utilisateur se déconnecte. La valeur par défaut est **Immédiatement**.

  Par défaut, l'iPad partagé se verrouille automatiquement après deux minutes d'inactivité.



Stratégie Personal Hotspot

December 9, 2021

Vous pouvez autoriser les utilisateurs à se connecter à Internet lorsqu'ils ne sont pas à portée d'un réseau Wi-Fi en utilisant la connexion des données cellulaires au travers de la fonctionnalité Partage de connexion (Personal Hotspot) de leurs appareils iOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Désactiver Personal Hotspot :** sélectionnez cette option pour désactiver la fonctionnalité Partage de connexion (Personal Hotspot) sur les appareils des utilisateurs. La valeur par défaut est **Désactivé**, ce qui désactive Partage de connexion (Personal Hotspot) sur les appareils des utilisateurs. Cette stratégie ne désactive pas la fonctionnalité. Les utilisateurs peuvent toujours utiliser Partage de connexion (Personal Hotspot) sur leurs appareils, mais lorsque la stratégie est déployée, Personal Hotspot est désactivé de manière à ne pas rester activé par défaut.

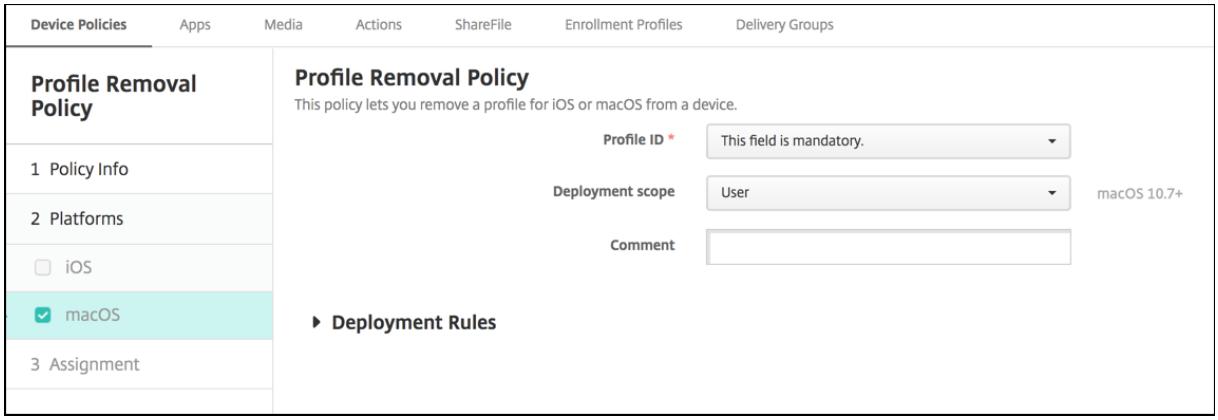
Stratégie de suppression de profil

November 29, 2023

Vous pouvez créer une stratégie de suppression de profil dans Citrix Endpoint Management. La stratégie, lorsqu'elle est déployée, supprime le profil d'application des appareils iOS ou macOS des utilisateurs.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres macOS



- **ID du profil :** dans la liste, cliquez sur l'ID du profil d'application. Ce champ est obligatoire.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Étendue du déploiement :** dans la liste, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.
- **Commentaires :** entrez un commentaire (facultatif).

Stratégie de profil de provisioning

November 29, 2023

Lorsque vous développez et codez une application d'entreprise iOS, vous incluez généralement un profil de provisioning de distribution d'entreprise, dont Apple a besoin pour que l'application s'exécute sur un appareil iOS. Si un profil de provisioning est manquant, ou s'il a expiré, l'application se bloque lorsque l'utilisateur tape pour l'ouvrir.

Le principal problème avec les profils de provisioning est qu'ils expirent un an après qu'ils sont générés sur le portail Apple Developer et vous devez conserver les dates d'expiration pour tous les profils de provisioning sur tous les appareils iOS inscrits par vos utilisateurs. Le suivi des dates d'expiration non seulement implique de surveiller les dates d'expiration, mais aussi quels utilisateurs utilisent quelle version de l'application. Les deux solutions consistent à envoyer par e-mail les profils de provisioning aux utilisateurs ou à les placer dans un portail Web pour le téléchargement et l'installation. Ces solutions fonctionnent, mais elles peuvent entraîner des erreurs car elles requièrent que les utilisateurs réagissent à des instructions dans un e-mail ou accèdent au portail Web pour télécharger le profil approprié et l'installer.

Pour effectuer cette opération de façon transparente pour les utilisateurs, vous pouvez installer et supprimer les profils de provisioning avec les stratégies d'appareil dans Citrix Endpoint Management. Les profils manquants ou arrivés à expiration sont supprimés si nécessaire et des profils à jour sont installés sur les appareils des utilisateurs, de façon à ce qu'il leur suffise de taper sur une application pour l'ouvrir.

Avant de pouvoir créer une stratégie de profil de provisioning, vous devez créer un fichier de profil de provisioning. Pour plus d'informations, consultez l'article Apple sur la création d'un profil de provisioning de développement sur le site pour développeurs Apple.

Paramètres iOS

- **Profil de provisioning iOS :** sélectionnez le fichier de profil de provisioning à importer en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie de suppression de profil de provisioning

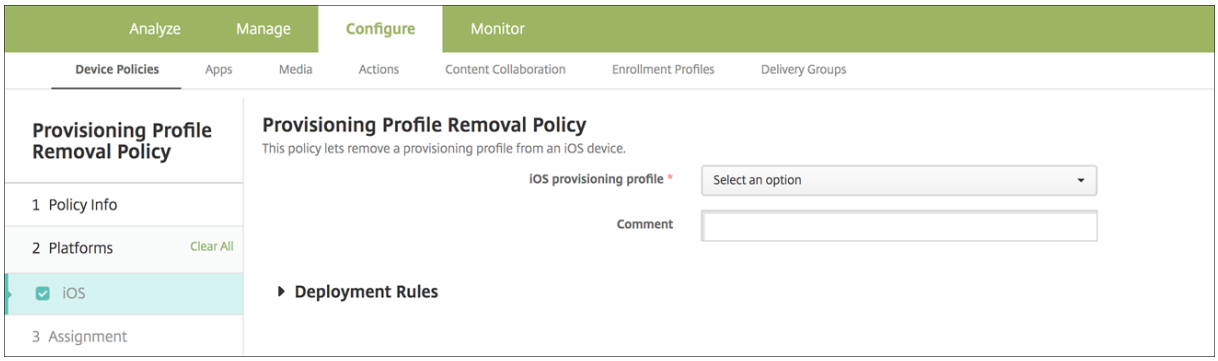
December 9, 2021

Un profil de provisioning vous permet de distribuer des applications iOS sur les appareils utilisateur. Apple exige que vous signiez une application à l'aide d'un profil de provisioning pour autoriser l'application à s'exécuter sur des appareils iOS. Pour plus d'informations, consultez la section Stratégie de profil de provisioning.

Pour supprimer ou remplacer un profil de provisioning plus ancien, utilisez la stratégie de suppression de profil de provisioning.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS



- **Profil de provisioning iOS :** dans la liste, cliquez sur le profil de provisioning que vous souhaitez supprimer.
- **Commentaire :** si vous le souhaitez, ajoutez un commentaire.

Stratégie de proxy

December 9, 2021

La stratégie Proxy spécifie les paramètres de proxy HTTP globaux pour les appareils iOS pris en charge. Vous ne pouvez déployer qu'une stratégie de proxy HTTP globale par appareil.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Conditions préalables

Avant de déployer cette stratégie, assurez-vous de définir tous les appareils iOS pour lesquels vous souhaitez définir un proxy HTTP global en mode supervisé. Pour plus de détails, voir Déployer des appareils à l'aide d'Apple Configurator 2 ou Déployer des appareils via le programme de déploiement d'Apple.

Définissez des règles de déploiement pour inscrire les appareils avant d'envoyer la stratégie Proxy aux appareils.

Paramètres iOS

- **Configuration du proxy :** cliquez sur **Manuel** ou **Automatique** pour choisir la méthode à utiliser pour configurer le proxy sur les appareils des utilisateurs.
  - Si vous avez sélectionné **Manuel**, configurez les paramètres suivants :
    - **Nom d'hôte ou adresse IP du serveur proxy :** entrez le nom d'hôte ou l'adresse IP du serveur proxy. Ce champ est obligatoire.
    - **Port du serveur proxy :** entrez le numéro de port du serveur proxy. Ce champ est obligatoire.
    - **Nom d'utilisateur :** entrez un nom d'utilisateur pour l'authentification auprès du serveur proxy (facultatif).
    - **Mot de passe :** entrez un mot de passe pour l'authentification auprès du serveur proxy (facultatif).
  - Si vous avez sélectionné **Automatique**, configurez les paramètres suivants :
    - **URL du fichier de configuration automatique de proxy :** entrez l'adresse URL du fichier PAC qui définit la configuration proxy.
    - **Autoriser la connexion directe si le PAC est injoignable :** indiquez si les utilisateurs sont autorisés à se connecter directement à la destination si le fichier PAC est inaccessible. La valeur par défaut est **Activé**.
- **Autoriser le contournement du proxy pour accéder aux réseaux captifs :** sélectionnez cette option pour autoriser le contournement du proxy afin d'accéder aux réseaux captifs. La valeur par défaut est **Désactivé**.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

* **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Stratégie de restrictions

March 1, 2024

> **Remarque :**
>
> Lorsqu'une mise à niveau inclut de nouveaux paramètres de stratégie de restrictions, vous devez modifier et enregistrer la stratégie. Citrix Endpoint Management ne déploie pas la stratégie de restrictions mise à niveau tant que vous ne l'aurez pas enregistrée.

La stratégie Restrictions autorise ou restreint certaines fonctionnalités sur les appareils des utilisateurs, telles que l'appareil photo. Vous pouvez définir des restrictions de sécurité et des restrictions sur le contenu multimédia. Vous pouvez également définir des restrictions sur les types d'applications que les utilisateurs peuvent ou ne peuvent pas installer. La plupart des paramètres de restriction sont réglés par défaut sur **Activé** ou *autorise*. Les principales exceptions sont la fonctionnalité Sécuriser - Forcer dans iOS et toutes les fonctionnalités de Windows Tablet, lesquelles prennent par défaut la valeur **Désactivé** ou appliquent des *restrictions*.

Toute option définie sur **Activé** signifie que l'utilisateur peut effectuer l'opération ou utiliser la fonctionnalité. Par exemple :

- **Appareil photo :** si l'option est réglée sur **Activé**, l'utilisateur peut utiliser l'appareil photo sur son appareil. Si l'option est réglée sur **Désactivé**, l'utilisateur ne peut pas utiliser l'appareil photo sur son appareil.
- **Capture d'écran :** si l'option est définie sur **Activé**, l'utilisateur peut prendre des captures d'écran sur son appareil. Si l'option est définie sur **Désactivé**, l'utilisateur ne peut pas prendre de captures d'écran sur son appareil.

Si la stratégie Restrictions et la stratégie Kiosque sont toutes les deux configurées, la stratégie Restrictions a priorité.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres iOS

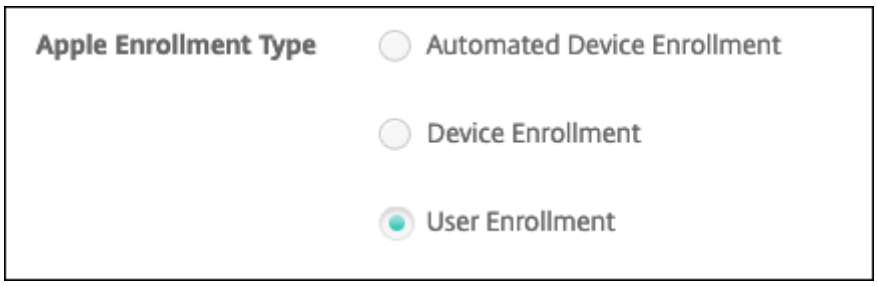
Certains paramètres de stratégie de restrictions iOS s'appliquent uniquement à des versions spécifiques d'iOS, comme indiqué ici et sur la page de stratégie Restrictions de la console Citrix Endpoint Management.

Ces paramètres s'appliquent également lorsque l'appareil est inscrit en mode d'inscription de l'utilisateur, en mode non supervisé (MDM complet) ou en mode supervisé. Le tableau suivant présente les modes d'inscription disponibles pour chaque paramètre pour iOS 13 et versions ultérieures.

- **Inscription automatisée d'appareils :** appareils supervisés. Il s'agit d'appareils inscrits via l'inscription en bloc.
- **Inscription d'appareils :** appareils non supervisés. Ces appareils sont inscrits individuellement et l'ensemble de l'appareil est entièrement géré par MDM.
- **Inscription des utilisateurs :** appareils sur lesquels seuls des utilisateurs spécifiques sont gérés. Pour plus d'informations sur l'inscription des utilisateurs, veuillez consulter la documentation Apple.

Les paramètres de stratégie de restrictions iOS peuvent s'appliquer également lorsque l'appareil est inscrit en mode d'inscription de l'utilisateur, en mode non supervisé (MDM complet) ou en mode supervisé. Le tableau suivant présente les modes d'inscription disponibles pour chaque paramètre de stratégie de restrictions pour iOS 13 et versions ultérieures.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Comme indiqué dans le tableau, certains paramètres qui étaient auparavant disponibles en mode non supervisé et supervisé ne sont disponibles qu'en mode supervisé à partir de la version iOS 13. Les règles suivantes s'appliquent :

- Si un appareil iOS 13+ supervisé est inscrit dans Citrix Endpoint Management, les paramètres s'appliquent à l'appareil.
- Si un appareil iOS 13+ non supervisé est inscrit dans Citrix Endpoint Management, les paramètres ne s'appliquent pas à l'appareil.
- Si un appareil iOS 12 (ou version inférieure) déjà inscrit dans Citrix Endpoint Management est mis à niveau vers iOS 13, il n'y a aucune modification. Les paramètres s'appliquent à l'appareil comme avant la mise à niveau.

Pour plus d'informations sur la définition d'un appareil iOS en mode supervisé, consultez la section Déployer des appareils à l'aide d'Apple Configurator 2.

Paramètre	Inscription des utilisateurs	Non supervisé	Supervisé
Autoriser le contrôle du matériel			
Caméra	Non	Oui	Oui
FaceTime	Non	Non	Oui
Captures d'écran	Oui	Non	Oui
Autoriser l'application En classe à observer à distance les écrans des étudiants	Non	Non	Oui
Autoriser l'application En classe à modifier les autorisations AirPlay et Voir l'écran sans invite	Non	Non	Oui
Flux de photos	Non	Oui	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Inscription des utilisateurs	Non supervisé	Supervisé
Flux de photos partagés	Non	Oui	Oui
Autoriser session temporaire d'iPad partagé	Non	Non	Oui
Composition vocale	Non	Oui	Oui
Siri	Oui	Oui	Oui
Autoriser lorsque l' appareil est verrouillé	Oui	Oui	Oui
Filtre d'obscénité de Siri	Non	Non	Oui
Installation d' applications	Non	Non	Oui
Autoriser récupération en arrière-plan globale en cas d'itinérance	Non	Oui	Oui
Autoriser les applications			
Apple App Store	Non	Non	Oui
Achats dans les applications	Non	Oui	Oui
Exiger le mot de passe Apple App Store pour effectuer des achats	Non	Oui	Oui
Safari	Non	Non	Oui
Remplissage automatique	Non	Non	Oui
Forcer l'avertissement de fraude	Oui	Oui	Oui
Activer JavaScript	Non	Oui	Oui
Bloquer les fenêtres contextuelles	Non	Oui	Oui
Accepter les cookies	Non	Oui	Oui
Réseau - Autoriser les actions iCloud			

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Inscription des utilisateurs	Non supervisé	Supervisé
Documents et données iCloud	Non	Non	Oui
Sauvegarde iCloud	Non	Oui	Oui
Trousseau iCloud	Non	Oui	Oui
Photothèque iCloud	Non	Oui	Oui
Sécuriser - Forcer			
Copies de sauvegarde chiffrées	Oui	Oui	Oui
Suivi limité des publicités	Non	Oui	Oui
Code secret lors du premier couplage AirPlay	Oui	Oui	Oui
Apple Watch jumelée pour utiliser la détection du poignet	Oui	Oui	Oui
Partage des documents gérés avec AirDrop	Oui	Oui	Oui
Sécurité - Autoriser			
Accepter des certificats SSL non approuvés	Non	Oui	Oui
Mise à jour automatique des paramètres d' approbation de certificat	Non	Oui	Oui
Exiger un presse-papiers géré	Oui	Oui	Oui
Documents provenant d'applications gérées dans les applications non gérées	Oui	Oui	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Inscription des utilisateurs	Non supervisé	Supervisé
Les applications non gérées lisent les contacts gérés	Non	Non	Oui
Les applications gérées écrivent sur les contacts non gérés	Non	Non	Oui
Documents provenant d'applications non gérées dans les applications gérées	Oui	Oui	Oui
Envoi d'informations de diagnostic à Apple	Oui	Oui	Oui
Touch ID pour déverrouiller un appareil	Non	Oui	Oui
Déverrouillage automatique	Non	Oui	Oui
Notifications Wallet lorsque l'appareil est verrouillé	Non	Oui	Oui
Handoff	Non	Oui	Oui
Synchronisation iCloud pour applications gérées	Oui	Oui	Oui
Sauvegarde de livres d'entreprise	Oui	Oui	Oui
Synchronisation des notes et des extraits pour les livres d'entreprise	Oui	Oui	Oui
Résultats Internet dans Spotlight	Non	Oui	Oui
Faire confiance aux applications d'entreprise	Non	Oui	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Inscription des utilisateurs	Non supervisé	Supervisé
Autoriser la publicité personnalisée Apple	Non	Oui	Oui
Paramètres supervisés uniquement - Autoriser			
Autoriser modification de la carte eSIM	Non	Non	Oui
Effacer tout le contenu et les paramètres	Non	Non	Oui
Screen Time	Non	Non	Oui
Podcasts	Non	Non	Oui
Installation des profils de configuration	Non	Non	Oui
Modification de Touch ID et Face ID	Non	Non	Oui
Installation des applications de l’appareil	Non	Non	Oui
Raccourcis clavier	Non	Non	Oui
Apple Watch couplée	Non	Non	Oui
Modification du code secret	Non	Non	Oui
Modification du nom de l’appareil	Non	Non	Oui
Modification du fond d’écran	Non	Non	Oui
Téléchargement automatique des applications	Non	Non	Oui
AirDrop	Non	Non	Oui
iMessage	Non	Non	Oui
Contenu généré par l’utilisateur dans Siri	Non	Non	Oui
iBooks	Non	Non	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Inscription des utilisateurs	Non supervisé	Supervisé
Suppression d' applications	Non	Oui	Oui
Game Center	Non	Non	Oui
Ajouter des amis	Non	Non	Oui
Jeux multijoueurs	Non	Non	Oui
Modification des paramètres de compte	Non	Non	Oui
Modification des paramètres des données cellulaires d' application	Non	Non	Oui
Modification des paramètres des données cellulaires d' application	Non	Non	Oui
Autoriser connexions de lecteurs réseau	Non	Non	Oui
Autoriser connexions de périphériques USB	Non	Non	Oui
Autoriser Localiser mon appareil	Non	Non	Oui
Autoriser les paramètres Localiser mes amis	Non	Non	Oui
Modification des paramètres Localiser mes amis	Non	Non	Oui
Couplage avec des hôtes non Configurator	Non	Non	Oui
Claviers intuitifs	Non	Non	Oui
Clavier avec correction automatique	Non	Non	Oui
Clavier avec correction d'orthographe	Non	Non	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Inscription des utilisateurs	Non supervisé	Supervisé
Autoriser le clavier QuickPath	Non	Non	Oui
Recherche des définitions	Non	Non	Oui
Bundle ID d' application unique			
Actualités	Non	Non	Oui
Service Apple Music	Non	Non	Oui
Apple Music	Non	Non	Oui
Modification des notifications	Non	Non	Oui
Utilisation restreinte des apps	Non	Non	Oui
Modification de l'envoi de diagnostics	Non	Non	Oui
Modification Bluetooth	Non	Non	Oui
Autoriser la dictée	Non	Non	Oui
Modifier si le Wi-Fi est activé ou désactivé	Non	Non	Oui
Rejoindre uniquement les réseaux Wi-Fi installés par une stratégie de réseau	Non	Non	Oui
Autoriser l'application En classe à modifier les autorisations AirPlay et Voir l'écran sans invite	Non	Non	Oui
Autoriser l'application En classe à verrouiller une application et l' appareil sans invite	Non	Non	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Inscription des utilisateurs	Non supervisé	Supervisé
Rejoindre automatiquement les cours de l'application En classe sans invite	Non	Non	Oui
Autoriser AirPrint	Non	Non	Oui
Autoriser le stockage des identifiants AirPrint dans le trousseau	Non	Non	Oui
Autoriser la détection des imprimantes AirPrint à l'aide d' iBeacons	Non	Non	Oui
Autoriser AirPrint uniquement sur les destinations avec des certificats approuvés	Non	Non	Oui
Ajout de configurations VPN	Non	Non	Oui
Modification des paramètres du forfait de données	Non	Non	Oui
Suppression des applications système	Non	Non	Oui
Configuration des nouveaux appareils à proximité	Non	Non	Oui
Autoriser le mode restreint USB	Non	Non	Oui
Retarder les mises à jour logicielles	Non	Non	Oui
Délai imposé pour les mises à jour logicielles	Non	Non	Oui
Exiger la permission de En classe pour quitter les classes	Non	Non	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Inscription des utilisateurs	Non supervisé	Supervisé
Forcer l' authentification avant le remplissage automatique	Non	Non	Oui
Forcer réglage automatique de la date et et l'heure	Non	Non	Oui
Remplissage automatique du mot de passe	Non	Non	Oui
Demander mot de passe des contacts à proximité	Non	Non	Oui
Partage de mot de passe	Non	Non	Oui
Autoriser modification du partage de connexion	Non	Non	Oui
Autoriser le démarrage en mode de récupération par un appareil non couplé	Non	Non	Oui
Installer la mise à jour de sécurité urgente	Non	Non	Oui
Retirer la mise à jour de sécurité urgente	Non	Non	Oui
Autoriser la protection de la confidentialité des e-mails	Non	Non	Oui
NFC	Non	Non	Oui
Autoriser les extraits d' app	Non	Non	Oui
Sécurité - Afficher dans l'écran de verrouillage			
Centre de contrôle	Oui	Oui	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Inscription des utilisateurs	Non supervisé	Supervisé
Notification	Oui	Oui	Oui
Vue Aujourd'hui	Oui	Oui	Oui
Contenu multimédia - Autoriser			
Musique, podcasts et cours iTunes U explicites	Non	Non	Oui
Contenu sexuel explicite dans iBooks	Non	Oui	Oui
Classements par région	Non	Oui	Oui
Films	Non	Oui	Oui
Séries TV	Non	Oui	Oui
Applications	Non	Oui	Oui

- **Autoriser le contrôle du matériel**
  - **Appareil photo :** autorise les utilisateurs à utiliser l'appareil photo sur leurs appareils.
    - **FaceTime :** autorise les utilisateurs à utiliser FaceTime sur leurs appareils. Pour les appareils iOS supervisés.
  - **Captures d'écrans :** autorise les utilisateurs à prendre des captures d'écrans sur leurs appareils.
    - **Autoriser l'application En classe à observer à distance les écrans des étudiants :** si cette restriction n'est pas sélectionnée, un instructeur ne peut pas utiliser l'application En classe pour observer les écrans des étudiants. Le paramètre par défaut est sélectionné, un instructeur peut utiliser l'application En classe pour observer les écrans des étudiants. Le paramètre **Autoriser l'application En classe à modifier les autorisations AirPlay et Voir l'écran sans invite** détermine si les élèves reçoivent une invite pour autoriser l'instructeur. Pour les appareils iOS supervisés.
    - **Autoriser l'application En classe à modifier les autorisations AirPlay et Voir l'écran sans invite :** si cette restriction est sélectionnée, l'instructeur peut modifier les autorisations AirPlay et voir l'écran de l'appareil d'un étudiant, sans demander d'autorisation. Par défaut, cette restriction n'est pas sélectionnée. Pour les appareils iOS supervisés.
  - **Flux de photos :** autorise les utilisateurs à utiliser MyPhotoStream pour partager des pho-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tos avec leurs appareils iOS via iCloud.
  - **Flux de photos partagés :** autorise les utilisateurs à utiliser le partage de photos iCloud pour partager des photos avec des collègues, amis et proches.
  - **Autoriser session temporaire d'iPad partagé :** empêche l'accès aux sessions temporaires sur les iPad partagés.
  - **Composition vocale :** active la composition sur les appareils des utilisateurs.
  - **Siri :** permet aux utilisateurs d'utiliser Siri.
    * **Autoriser lorsque l'appareil est verrouillé :** permet aux utilisateurs de se servir de Siri lorsque leur appareil est verrouillé.
    * **Filtre d'obscénité de Siri :** active le filtre d'obscénité de Siri. Par défaut, cette fonctionnalité est désactivée, ce qui signifie qu'aucun filtre d'obscénité n'est appliqué. Pour de plus amples informations sur Siri et la sécurité, consultez la section Stratégies de dictée et Siri.
  - **Installation d'applications :** autorise les utilisateurs à installer des applications. Pour les appareils iOS supervisés.
  - **Autoriser récupération en arrière-plan globale en cas d'itinérance :** autorise un appareil à synchroniser automatiquement les comptes de messagerie vers iCloud lorsqu'il est itinérant. Lorsque **Désactivé** est sélectionné, désactive l'activité de récupération en arrière-plan globale lors de l'itinérance d'un téléphone iOS. La valeur par défaut est **Activé**.

- **Autoriser les applications**
  - **Apple App Store :** autorise les utilisateurs à accéder à l'Apple App Store. Pour les appareils iOS supervisés.
  - **Achats dans les applications :** autorise les utilisateurs à effectuer des achats dans les applications.
    * **Exiger le mot de passe Apple App Store pour effectuer des achats :** exige un mot de passe pour les achats dans l'application. Par défaut, cette fonctionnalité est désactivée, ce qui signifie qu'aucun mot de passe n'est requis pour les achats intégrés dans l'application.
  - **Safari :** permet aux utilisateurs d'accéder à Safari. Pour les appareils iOS supervisés.
    * **Remplissage automatique :** autorise les utilisateurs à configurer le remplissage automatique pour les noms d'utilisateurs et mots de passe sur Safari.
    * **Forcer l'avertissement de fraude :** si ce paramètre est activé et qu'un utilisateur visite un site soupçonné d'hameçonnage, Safari alerte l'utilisateur. Par défaut, cette fonctionnalité est désactivée, ce qui signifie qu'aucun avertissement n'est émis.
    * **Activer JavaScript :** autorise JavaScript à s'exécuter sur Safari.
    * **Bloquer les fenêtres contextuelles :** bloque les fenêtres contextuelles lors de l'affichage de sites Web. Par défaut, cette fonctionnalité est désactivée, ce qui signifie

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

que les fenêtres contextuelles ne sont pas bloquées.

  - **Accepter les cookies :** définit dans quelle mesure les cookies sont acceptés. Dans la liste, choisissez sur une option pour activer ou désactiver les cookies. L'option par défaut est **Toujours**, ce qui autorise tous les sites à enregistrer des cookies dans Safari. Les autres options sont **Site Web actuel uniquement**, **Jamais** et **Des sites visités uniquement**.

- **Réseau - Autoriser les actions iCloud**

  - **Documents et données iCloud :** autorise les utilisateurs à synchroniser les documents et les données avec iCloud. Pour les appareils iOS supervisés.
  - **Sauvegarde iCloud :** autorise les utilisateurs à sauvegarder leurs appareils sur iCloud.
  - **Trousseau iCloud :** autorise les utilisateurs à stocker les mots de passe, le réseau Wi-Fi, le numéro de carte de crédit et autres informations dans le trousseau iCloud.
  - **Photothèque iCloud :** autorise les utilisateurs à accéder à leur bibliothèque de photos iCloud.

- **Sécuriser - Forcer**

  Par défaut, les fonctionnalités suivantes sont désactivées, ce qui signifie qu'aucune fonctionnalité de sécurité n'est activée.

  - **Copies de sauvegarde chiffrées :** impose le chiffrement des sauvegardes effectuées dans iCloud.
  - **Suivi limité des publicités :** bloque le suivi des publicités ciblées.
  - **Demander code secret lors du premier couplage AirPlay :** exige que les appareils compatibles avec AirPlay soient vérifiés à l'aide d'un code à usage unique s'affichant sur l'écran avant que les utilisateurs puissent utiliser AirPlay.
  - **Apple Watch jumelée pour utiliser la détection du poignet :** requiert une Apple Watch jumelée pour utiliser la **détection du poignet**.
  - **Partage des documents gérés avec AirDrop :** si vous définissez cette option sur **Activé**, AirDrop apparaît comme destination non gérée.

- **Sécurité - Autoriser**

  - **Accepter des certificats SSL non approuvés :** autorise les utilisateurs à accepter les certificats SSL non fiables de sites Web.
  - **Mise à jour automatique des paramètres d'approbation de certificat :** autorise la mise à jour automatique des certificats de confiance.
  - **Exiger un presse-papiers géré :** autorisez la fonctionnalité copier-coller à respecter les mêmes restrictions que vous appliquez à **Documents provenant d'applications gérées dans les applications non gérées** et **Documents provenant d'applications non gérées dans les applications gérées**.
    Par exemple, vous configurez ce qui suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Exiger presse-papiers géré :** Activé
    * **Documents provenant d'applications gérées dans les applications non gérées :** Désactivé
    * **Documents provenant d'applications non gérées dans les applications gérées :** Activé

      Après avoir déployé la stratégie sur les appareils iOS, les utilisateurs ne peuvent pas copier-coller des données depuis des applications gérées vers des applications non gérées, mais ils peuvent copier-coller des données d'applications non gérées vers des applications gérées.
- **Documents provenant d'applications gérées dans les applications non gérées :** autorise les utilisateurs à déplacer des données d'applications gérées (d'entreprise) vers des applications non gérées (personnelles).
- **Documents provenant d'applications non gérées dans les applications gérées :** autorise les utilisateurs à déplacer des données d'applications non gérées (personnelles) vers des applications gérées (d'entreprise).
- **Envoi d'informations de diagnostic à Apple :** autorise l'envoi à Apple de données de diagnostic anonymes relatives aux appareils des utilisateurs.
- **Touch ID ou Face ID pour déverrouiller un appareil :** autorise les utilisateurs à utiliser Touch ID ou Face ID pour déverrouiller leurs appareils.
- **Déverrouillage automatique :** si la valeur **Désactivé** est définie, l'utilisateur ne peut pas utiliser une Apple Watch pour déverrouiller un iPhone couplé. La valeur par défaut est **Activé**. Disponible pour iOS 14.5 et les versions ultérieures.
- **Notifications Wallet lorsque l'appareil est verrouillé :** autorise l'affichage de notifications Wallet sur l'écran de verrouillage.
- **Handoff :** autorise les utilisateurs à transférer des activités d'un appareil iOS vers un autre appareil iOS se trouvant à proximité.
- **Synchronisation iCloud pour applications gérées :** autorise les utilisateurs à synchroniser des applications gérées avec iCloud.
- **Sauvegarde de livres d'entreprise :** autorise la sauvegarde des livres d'entreprise dans iCloud.
- **Synchronisation des notes et des extraits pour les livres d'entreprise :** autorise la synchronisation avec iCloud des notes et extraits ajoutés aux livres d'entreprise par les utilisateurs.
- **Faire confiance aux applications d'entreprise :** permet de faire confiance aux applications d'entreprise. Les applications d'entreprise sont toutes les applications qui ont été personnalisées pour votre organisation. Elles peuvent être réalisées en interne ou elles peuvent être développées et achetées auprès d'un fournisseur externe. Pour plus d'informations, consultez Installer des applications d'entreprise personnalisées sur iOS.
- **Résultats Internet dans Spotlight :** autorise Spotlight à afficher les résultats de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

recherche sur Internet ainsi que sur l'appareil.

- **Les applications non gérées lisent des contacts gérés :** option facultative. Disponible uniquement si l'option **Documents provenant d'applications gérées dans les applications non gérées** est désactivée. Si cette stratégie est activée, des applications non gérées peuvent lire les données des contacts des comptes gérés. La valeur par défaut est **Off**. Disponible à partir d'iOS 12.
- **Les applications gérées écrivent des contacts non gérés :** option facultative. Si cette option est activée, des applications gérées peuvent écrire des contacts dans les contacts des comptes non gérés. Si l'option **Documents provenant d'applications gérées dans les applications non gérées** est activée, cette restriction n'a aucun effet. La valeur par défaut est **Off**. Disponible à partir d'iOS 12.
- **Autoriser la publicité personnalisée Apple :** si la valeur **Désactivé** est définie, les données des utilisateurs ne seront pas utilisées par la plateforme publicitaire d'Apple pour diffuser des publicités personnalisées. La valeur par défaut est **Activé**. Disponible pour iOS 14.0 et les versions ultérieures.

- **Paramètres supervisés uniquement - Autoriser**

  Ces paramètres s'appliquent uniquement aux appareils supervisés. Pour plus d'informations sur la définition d'un appareil iOS en mode supervisé, consultez la section Déployer des appareils à l'aide d'Apple Configurator 2.

  - **Autoriser modification de la carte eSIM :** autorise les utilisateurs à modifier les paramètres eSIM sur leur appareil.
  - **Effacer tout le contenu et les paramètres :** autorise les utilisateurs à effacer tout le contenu et les paramètres à partir de leurs appareils.
  - **Screen Time :** autorise les utilisateurs à activer la fonction Screen Time.
  - **Podcasts :** autorise les utilisateurs à télécharger et synchroniser des podcasts.
  - **Installation des profils de configuration :** autorise les utilisateurs à installer un autre profil de configuration que celui que vous avez déployé.
  - **Modification de Touch ID et de Face ID :** autorise les utilisateurs à modifier ou supprimer leur Touch ID ou Face ID.
  - **Installation d'applications à partir de l'appareil :** autorise les utilisateurs à installer des applications. La désactivation de ce paramètre empêche les utilisateurs finaux d'installer de nouvelles applications. L'App Store est désactivé et son icône est supprimée de l'écran d'accueil.
  - **Raccourcis clavier :** autorise les utilisateurs à créer des raccourcis clavier personnalisés pour les mots ou phrases qu'ils utilisent souvent.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Montre jumelée :** autorise les utilisateurs à jumeler une Apple Watch avec un appareil supervisé.
- **Modification du code secret :** autorise les utilisateurs à changer le code secret sur un appareil supervisé.
- **Modification du nom de l'appareil :** autorise les utilisateurs à changer le nom de leur appareil.
- **Modification du fond d'écran :** autorise les utilisateurs à changer le fond d'écran sur leurs appareils.
- **Téléchargement automatique des applications :** autorise le téléchargement des applications.
- **AirDrop :** autorise les utilisateurs à partager des photos, des vidéos, des sites Web, des emplacements et autres avec des appareils iOS se trouvant à proximité.
- **iMessage :** autorise les utilisateurs à envoyer un SMS par Wi-Fi avec iMessage.
- **Contenu généré par l'utilisateur dans Siri :** autorise Siri à interroger le contenu généré par l'utilisateur à partir du Web. Des consommateurs, plutôt que des journalistes ; contenu généré par l'utilisateur. Par exemple, les contenus disponibles sur Twitter ou Facebook sont générés par l'utilisateur.
- **iBooks :** autorise les utilisateurs à utiliser l'application iBooks.
- **Suppression d'applications :** autorise les utilisateurs à supprimer des applications à partir de leurs appareils.
- **Game Center :** autorise les utilisateurs à jouer à des jeux en ligne proposés par Game Center sur leurs appareils.
  * **Ajouter des amis :** autorise les utilisateurs à envoyer une notification à un ami pour l'inviter à rejoindre une partie.
  * **Jeux multijoueurs :** autorise les utilisateurs à lancer un jeu multijoueurs sur leur appareil.
- **Modification des paramètres de compte :** autorise les utilisateurs à modifier les paramètres du compte de leur appareil.
- **Modification des paramètres des données cellulaires d'application :** autorise les utilisateurs à modifier la façon dont les applications utilisent les données cellulaires.
- **Autoriser connexions de lecteurs réseau :** empêche la connexion aux lecteurs réseau dans l'application Fichiers.
- **Autoriser connexions de périphériques USB :** empêche la connexion à tout périphérique USB connecté dans l'application Fichiers

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Autoriser Localiser mon appareil :** désactive l'option **Localiser mon appareil** dans l'application Localiser mon appareil.
- **Autoriser Localiser mes amis :** désactive l'option **Autoriser Localiser mes amis** dans l'application Localiser mon iPhone.
- **Modification des paramètres Localiser mes amis :** autorise les utilisateurs à modifier leurs paramètres Localiser mes amis.
- **Couplage avec des hôtes non Configurator :** autorise l'administrateur à contrôler les appareils avec lesquels l'appareil d'un utilisateur peut être couplé. La désactivation de ce paramètre empêche le couplage sauf avec l'hôte superviseur exécutant Apple Configurator. Si aucun certificat d'hôte superviseur n'est configuré, tous les couplages sont désactivés.
- **Claviers intuitifs :** autorise les appareils des utilisateurs à utiliser le clavier intuitif pour leur suggérer des mots lors de la saisie. Désactivez cette option dans certaines situations spécifiques, par exemple lors de tests standardisés pendant lesquels vous ne voulez pas que les utilisateurs aient accès à des mots suggérés.
- **Clavier avec correction automatique :** autorise les appareils des utilisateurs à utiliser le clavier avec correction automatique. Désactivez cette option dans certaines situations spécifiques, par exemple lors de tests standardisés pendant lesquels vous ne voulez pas que les utilisateurs aient accès à la correction automatique.
- **Clavier avec correction d'orthographe :** autorise les appareils des utilisateurs à utiliser le correcteur orthographique lors de la saisie. Désactivez cette option dans certaines situations spécifiques, par exemple lors de tests standardisés pendant lesquels vous ne voulez pas que les utilisateurs aient accès au correcteur orthographique.
- **Recherche des définitions :** autorise les appareils des utilisateurs à utiliser la recherche de définition lors de la saisie. Désactivez cette option dans certaines situations spécifiques, par exemple lors de tests standardisés pendant lesquels vous ne voulez pas que les utilisateurs puissent rechercher des définitions pendant la saisie.
- **Bundle ID d'application unique :** crée une liste d'applications autorisées à conserver le contrôle de l'appareil et à empêcher les interactions avec d'autres applications ou fonctions.
  Pour ajouter une application, cliquez sur **Ajouter**, tapez un **nom d'application**, puis cliquez sur **Enregistrer**. Répétez cette procédure pour chaque application à ajouter.
- **News :** autorise les utilisateurs à utiliser l'application News.
- **Service Apple Music :** permet aux utilisateurs d'utiliser le service Apple Music. Si vous n'autorisez pas le service Apple Music, l'application Music s'exécute en mode classique.
- **Apple Music :** autorise les utilisateurs à utiliser Apple Music.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Modification des notifications :** permet aux utilisateurs de modifier les paramètres de notification.
- **Utilisation restreinte des apps :** autorise les utilisateurs à utiliser toutes les applications ou à utiliser ou non certaines applications en fonction des Bundle ID que vous fournissez. S'applique uniquement aux appareils supervisés. Si vous sélectionnez **Autoriser uniquement certaines applications**, ajoutez une application avec le bundle ID `com.apple.webapp` pour autoriser les clips Web.

  > **Remarque :**
  >
  > À partir de iOS 11, Apple a introduit des modifications dans les stratégies disponibles pour les restrictions d'applications. Apple ne vous permet plus de supprimer l'accès à l'application Paramètres et à l'application Téléphone en limitant l'offre d'applications iOS appropriée.

  Après avoir configuré la stratégie Restrictions pour bloquer certaines applications et déployé la stratégie : si vous souhaitez autoriser tout ou partie de ces applications ultérieurement, la modification et le déploiement de la stratégie Restrictions ne modifient pas les restrictions. Dans ce cas, iOS n'applique pas les modifications apportées au profil iOS. Utilisez la stratégie Suppression de profil pour supprimer le profil iOS et déployez la stratégie Restrictions mise à jour.

  Si vous réglez ce paramètre sur **Autoriser uniquement certaines applications** : avant de déployer cette stratégie, demandez aux utilisateurs des appareils inscrits à l'aide du programme de déploiement d'Apple de se connecter à leurs comptes Apple à partir de l'Assistant d'installation. Dans le cas contraire, les utilisateurs devront peut-être désactiver l'authentification à deux facteurs sur leurs appareils pour se connecter à leurs comptes Apple et accéder aux applications autorisées.
- **Modification de l'envoi de diagnostics :** permet aux utilisateurs de modifier les paramètres d'envoi d'informations de diagnostic ainsi que les paramètres d'analyse de l'application dans le panneau **Réglages > Diagnostics et utilisation**.
- **Modification Bluetooth :** permet aux utilisateurs de modifier les paramètres Bluetooth.
- **Autoriser la dictée :** sur appareils supervisés uniquement. Si cette restriction est définie sur **Désactivé**, la dictée n'est pas autorisée, y compris la reconnaissance vocale. Le paramètre par défaut est **Activé**.
- **Modifier si le Wi-Fi est activé ou désactivé :** empêche l'activation ou la désactivation du Wi-Fi dans les paramètres ou le Centre de contrôle. Le mode avion n'a aucun effet non plus. Cette restriction n'empêche pas de sélectionner le réseau Wi-Fi à utiliser.
- **Rejoindre uniquement les réseaux Wi-Fi installés par une stratégie de réseau :** paramètre facultatif. Supervisé uniquement Si cette restriction est définie sur **Activé**, l'

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

appareil peut rejoindre des réseaux Wi-Fi uniquement lorsqu'ils ont été configurés par le biais d'un profil de configuration. Le paramètre par défaut est **Désactivé**.

- **Autoriser l'application En classe à modifier les autorisations AirPlay et Voir l'écran sans invite :** si cette restriction est sélectionnée, l'instructeur peut modifier les autorisations AirPlay et voir l'écran de l'appareil d'un étudiant, sans demander d'autorisation. Par défaut, cette restriction n'est pas sélectionnée. Pour les appareils iOS supervisés.
- **Autoriser l'application En classe à verrouiller une application et l'appareil sans invite :** si cette restriction est définie sur **Activé**, l'application En classe verrouille automatiquement les appareils utilisateur sur une application et verrouille l'appareil, sans inviter les utilisateurs. Le paramètre par défaut est **Désactivé**. Pour les appareils supervisés exécutant iOS 11 (version minimale).
- **Rejoindre automatiquement les cours de l'application En classe sans invite :** si cette restriction est définie sur **Activé**, l'application En classe ajoute automatiquement les utilisateurs aux classes, sans inviter les utilisateurs. Le paramètre par défaut est **Désactivé**. Pour les appareils supervisés exécutant iOS 11 (version minimale).
- **Autoriser AirPrint :** si cette restriction est définie sur **Désactivé**, les utilisateurs ne peuvent pas imprimer avec AirPrint. Le paramètre par défaut est **Activé**. Lorsque cette restriction est définie sur **Activé**, les restrictions supplémentaires suivantes s'affichent. Pour les appareils supervisés exécutant iOS 11 (version minimale).
  - **Autoriser le stockage des identifiants AirPrint dans le trousseau :** si cette restriction n'est pas sélectionnée, le nom d'utilisateur et le mot de passe AirPrint ne sont pas stockés dans le trousseau. Par défaut, ce paramètre est sélectionné. Pour les appareils supervisés exécutant iOS 11 (version minimale).
  - **Autoriser la détection des imprimantes AirPrint à l'aide d'iBeacons :** si cette restriction est désactivée, la détection iBeacon des imprimantes AirPrint est désactivée. Cela empêche les balises Bluetooth AirPrint parasites de perpétrer des attaques de phishing sur le trafic réseau. Par défaut, ce paramètre est sélectionné. Pour les appareils supervisés exécutant iOS 11 (version minimale).
  - **Autoriser AirPrint uniquement aux destinations avec des certificats de confiance :** si cette restriction est sélectionnée, les utilisateurs peuvent utiliser AirPrint pour imprimer uniquement vers des destinations avec des certificats de confiance. Par défaut, cette restriction n'est pas sélectionnée. Pour les appareils supervisés exécutant iOS 11 (version minimale).
- **Ajout de configurations VPN :** si cette restriction est définie sur **Désactivé**, les utilisateurs ne peuvent pas créer de configurations VPN. Le paramètre par défaut est **Activé**. Pour les appareils supervisés exécutant iOS 11 (version minimale).
- **Modification des paramètres du forfait de données :** si cette restriction est définie sur

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Désactivé, les utilisateurs ne peuvent pas modifier les paramètres du forfait de données. Le paramètre par défaut est **Activé**. Pour les appareils supervisés exécutant iOS 11 (version minimale).

- **Suppression des applications système :** si cette restriction est définie sur **Désactivé**, les utilisateurs ne peuvent pas supprimer les applications système de leur appareil. Le paramètre par défaut est **Activé**. Pour les appareils supervisés exécutant iOS 11 (version minimale).
- **Configuration des nouveaux appareils à proximité :** si cette restriction est définie sur Désactivé, les utilisateurs ne peuvent pas configurer de nouveaux appareils à proximité. Le paramètre par défaut est Activé. Pour les appareils supervisés exécutant iOS 11 (version minimale).
- **Autoriser le mode restreint USB :** si cette option est **désactivée**, l'appareil peut toujours se connecter aux accessoires USB lorsqu'il est verrouillé. La valeur par défaut est **Activé**. Disponible uniquement sur iOS 11.3 et versions ultérieures sur les appareils supervisés.
- **Retarder les mises à jour logicielles :** si elle est définie sur **Activé**, cette option retarde la visibilité des mises à jour logicielles pour l'utilisateur. Avec cette restriction en place, l'utilisateur ne voit pas de mise à jour logicielle avant le nombre de jours spécifié après la date de publication de la mise à jour logicielle. La valeur par défaut est **Off**. Disponible uniquement sur iOS 11.3 et versions ultérieures sur les appareils supervisés. La stratégie de mise à jour d'OS contient d'autres paramètres permettant de contrôler la fréquence à laquelle les appareils reçoivent les mises à jour. Consultez la section Stratégie de mise à jour de l'OS.
- **Délai imposé pour les mises à jour logicielles (jours) :** vous permet de spécifier le nombre de jours pendant lequel retarder une mise à jour logicielle sur l'appareil. Le délai maximum est de **90** jours. La valeur par défaut est **30** jours. Disponible uniquement sur iOS 11.3 et versions ultérieures sur les appareils supervisés.
- **Exiger la permission de En classe pour quitter les classes :** si cette option est **activée**, un élève inscrit à un cours non géré avec En classe doit demander la permission à l'enseignant pour quitter le cours. La valeur par défaut est **Off**. Disponible uniquement sur iOS 11.3 et versions ultérieures sur les appareils supervisés.
- **Forcer l'authentification avant le remplissage automatique :** force l'utilisateur à s'authentifier avant de pouvoir utiliser la fonction de remplissage automatique.
- **Forcer réglage automatique de la date et de l'heure :** cette option vous permet de définir automatiquement la date et l'heure sur les appareils supervisés. Lorsque ce paramètre est défini sur **Activé**, les utilisateurs de l'appareil ne peuvent pas désactiver l'option **Définir automatiquement** sous **Général > Date et heure**. Le fuseau horaire sur l'appareil est mis à jour uniquement lorsque l'appareil peut déterminer son emplacement,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

c'est-à-dire lorsqu'un appareil dispose d'une connexion cellulaire ou d'une connexion Wi-Fi avec les services de localisation activés. La valeur par défaut est **Off**. Disponible uniquement sur iOS 12 et versions ultérieures sur les appareils supervisés.

- **Remplissage automatique du mot de passe :** option facultative. Si cette option est désactivée, les utilisateurs ne peuvent pas utiliser les fonctionnalités de remplissage automatique de mot de passe ou de mot de passe fort automatique. La valeur par défaut est **Activé**. Disponible à partir d'iOS 12.
- **Requêtes de proximité de mot de passe :** option facultative. Si cette option est désactivée, les appareils des utilisateurs ne demandent pas de mots de passe aux appareils à proximité. La valeur par défaut est **Activé**. Disponible à partir d'iOS 12.
- **Partage de mot de passe :** option facultative. Si cette option est désactivée, les utilisateurs ne peuvent pas partager leurs mots de passe à l'aide de la fonctionnalité Mots de passe AirDrop. La valeur par défaut est **Activé**. Disponible à partir d'iOS 12.
- **Autoriser modification du partage de connexion :** empêche les utilisateurs de modifier les paramètres du partage de connexion personnel.
- **Autoriser le démarrage en mode de récupération par un appareil non couplé :** si la valeur **Activé** est définie, permet aux appareils d'être démarrés en mode de récupération par un appareil non couplé. La valeur par défaut est **Désactivé**. Disponible pour iOS 14.5 et les versions ultérieures.
- **Installer mise à jour de sécurité urgente :** si la valeur **Désactivé** est définie, interdit l'installation des mises à jour de sécurité urgentes. La valeur par défaut est **Activé**.
- **Retirer la mise à jour de sécurité urgente :** si la valeur **Désactivé** est définie, interdit la suppression des mises à jour de sécurité urgentes. La valeur par défaut est **Activé**.
- **Autoriser la protection de la confidentialité des e-mails :** si la valeur **Désactivé** est définie, désactive la protection de la confidentialité des e-mails sur l'appareil. La valeur par défaut est **Activé**. Disponible pour iOS 15.2 et les versions ultérieures.
- **Communication en champ proche (NFC) :** si la valeur **Désactivé** est définie, la fonction NFC est désactivée. La valeur par défaut est **Activé**. Disponible pour iOS 14.2 et les versions ultérieures.
- **Autoriser les extraits d'app** : si la valeur **Désactivé** est définie, empêche l'utilisateur d'ajouter des extraits d'app et supprime tous les extraits d'app existants sur l'appareil. La valeur par défaut est **Activé**. Disponible pour iOS 14.0 et les versions ultérieures.

• **Sécurité - Afficher dans l'écran de verrouillage**

- **Centre de contrôle :** cette option autorise l'accès au centre de contrôle sur l'écran de verrouillage. L'option Centre de contrôle permet aux utilisateurs de modifier facilement les modes Avion, Wi-Fi, Bluetooth, Ne pas déranger et les paramètres Lock Rotation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Notification :** autorise les notifications sur l'écran de verrouillage.
  - **Vue Aujourd'hui :** autorise l'affichage de la Vue Aujourd'hui, qui effectue l'agrégation d'informations telles que la météo et les éléments du calendrier du jour actuel, sur l'écran de verrouillage.

- **Contenu multimédia - Autoriser**

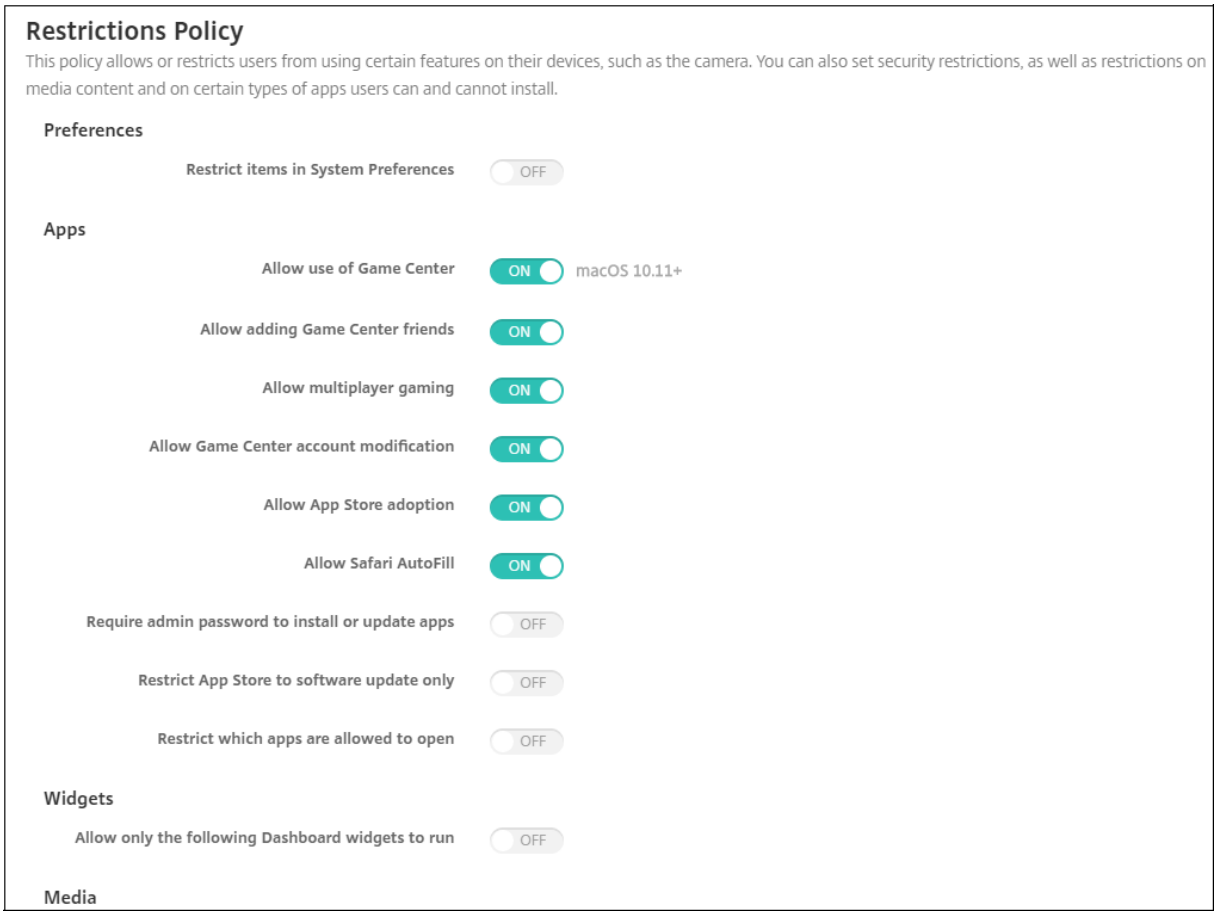
  - **Musique, podcasts et cours iTunes U explicites :** autorise l'affichage de contenus explicites sur les appareils des utilisateurs.
  - **Contenu sexuel explicite dans iBooks :** autorise le téléchargement de contenus explicites depuis iBooks.
  - **Classements par région :** définit la région à partir de laquelle les classements du contrôle parental sont obtenus. Dans la liste, cliquez sur un pays pour définir la région des classements. La valeur par défaut est **États-Unis**.
  - **Films :** détermine si les films sont autorisés sur les appareils des utilisateurs. Si les films sont autorisés, vous pouvez définir le niveau de contrôle d'accès pour les films. Dans la liste, cliquez sur une option pour autoriser ou interdire les films sur l'appareil. La valeur par défaut est Autoriser tous les films.
  - **Séries TV :** détermine si les séries télévisées sont autorisées sur les appareils des utilisateurs. Si les séries TV sont autorisées, vous pouvez définir leur niveau de contrôle d'accès. Dans la liste, cliquez sur une option pour autoriser ou interdire les séries TV sur l'appareil. La valeur par défaut est Autoriser toutes les séries TV.
  - **Applications :** détermine si les applications sont autorisées sur les appareils des utilisateurs. Si les applications sont autorisées, vous pouvez définir leur niveau de contrôle d'accès. Dans la liste, cliquez sur une option pour autoriser ou interdire les applications sur l'appareil. La valeur par défaut est Autoriser toutes les apps.

- **Paramètres de stratégie**

  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur iOS 9.3 et versions ultérieures.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres macOS



Paramètre	Non supervisé	Supervisé
Applications		
Autoriser l'utilisation de Game Center	Non	Oui
Autoriser l'ajout d'amis du Game Center	Non	Oui
Autoriser les jeux multijoueurs	Non	Oui
Autoriser la modification du compte Game Center	Oui	Oui
Autoriser l'adoption par l'App Store	Oui	Oui
Autoriser le remplissage automatique Safari	Non	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Non supervisé	Supervisé
Demander un mot de passe administrateur pour installer ou mettre à jour des applications	Oui	Oui
Autoriser uniquement l'App Store à mettre à jour les logiciels	Oui	Oui
Limiter les applications autorisées	Oui	Oui
Média		
Autoriser AirDrop	Non	Oui
Fonctionnalité		
Verrouiller l'image du bureau	Non	Oui
Autoriser l'utilisation de l' appareil photo	Non	Oui
Autoriser Apple Music	Non	Oui
Autoriser les suggestions de Spotlight	Oui	Oui
Autoriser Look Up	Oui	Oui
Autoriser l'utilisation du mot de passe iCloud pour les comptes locaux	Oui	Oui
Autoriser les documents et données iCloud	Oui	Oui
Autoriser bureau et documents iCloud	Non	Oui
Autoriser la synchronisation du trousseau iCloud	Non	Oui
Autoriser Mail iCloud	Oui	Oui
Autoriser contacts iCloud	Oui	Oui
Autoriser calendriers iCloud	Oui	Oui
Autoriser rappels iCloud	Oui	Oui
Autoriser signets iCloud	Oui	Oui
Autoriser notes iCloud	Oui	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Non supervisé	Supervisé
Autoriser photos iCloud	Oui	Oui
Autoriser déverrouillage automatique	Oui	Oui
Autoriser Touch ID pour déverrouiller votre Mac	Oui	Oui
Retarder les mises à jour logicielles	Non	Oui
Remplissage automatique du mot de passe	Non	Oui
Demander mot de passe des contacts à proximité	Non	Oui
Partage de mot de passe	Oui	Oui

- **Préférences**
  - **Limiter les éléments dans les Préférences système :** autorise ou restreint l'accès des utilisateurs aux Préférences système. La valeur par défaut est **Désactivé**, ce qui donne aux utilisateurs un accès total aux Préférences système. Si cette option est activée, vous pouvez configurer les paramètres suivants :
    - **Volets des préférences système :** indiquez si vous souhaitez que les paramètres que vous sélectionnez soient activés ou désactivés. La valeur par défaut est d'activer tous les paramètres, qui sont définis sur **Activé** par défaut.
      - Utilisateurs ou groupes
      - General
      - Accessibilité
      - Magasin d'applications
      - Mise à jour logicielle
      - Bluetooth
      - CD et DVD
      - Date et heure
      - Bureau et éco. d'écran
      - Moniteurs
      - Dock
      - Économiseur d'énergie
      - Extensions
      - Fibre Channel
      - iCloud

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Encre
  - Comptes Internet
  - Clavier
  - Langue et texte
  - Mission Control
  - Souris
  - Réseau
  - Notifications
  - Contrôle parental
  - Imprimantes et scanners
  - Profils
  - Sécurité et confidentialité
  - Partage
  - Son
  - Dictée et parole
  - Spotlight
  - Disque de démarrage
  - Time Machine
  - Trackpad
  - Xsan

- **Applications**
  - **Autoriser l'utilisation de Game Center :** autorise les utilisateurs à jouer à des jeux en ligne via Game Center. La valeur par défaut est **Activé**.
  - **Autoriser l'ajout d'amis du Game Center :** autorise les utilisateurs à envoyer une notification à un ami pour l'inviter à rejoindre une partie. La valeur par défaut est **Activé**.
  - **Autoriser les jeux multijoueurs :** autorise les utilisateurs à lancer un jeu multijoueurs. La valeur par défaut est **Activé**.
  - **Autoriser la modification du compte Game Center :** autorise les utilisateurs à modifier leurs paramètres de compte Game Center. La valeur par défaut est **Activé**.
  - **Autoriser l'adoption par l'App Store :** autorise ou restreint l'adoption des applications qui préexistent dans OS X par l'App Store. La valeur par défaut est **Activé**.
  - **Autoriser le remplissage automatique Safari :** autorise Safari à remplir automatiquement les champs des sites Web avec les mots de passe, les adresses et autres informations de base que le navigateur a stockés. La valeur par défaut est **Activé**.
  - **Demander un mot de passe administrateur pour installer ou mettre à jour des applications :** exige un mot de passe administrateur pour installer ou mettre à jour des applications. La valeur par défaut est **Désactivé**, ce qui signifie qu'aucun mot de passe administrateur n'est requis.
  - **Autoriser uniquement l'App Store à mettre à jour les logiciels :** restreint l'App Store

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

aux mises à jour, ce qui désactive tous les onglets de l'App Store, à l'exception de Mises à jour. La valeur par défaut est **Désactivé**, ce qui permet un accès complet à l'App Store.

- **Limiter les applications autorisées :** restreint ou autorise les applications que les utilisateurs peuvent utiliser. La valeur par défaut est Désactivé, ce qui permet à toutes les applications d'être utilisées. Si cette option est activée, vous pouvez configurer les paramètres suivants :
  - **Applications autorisées :** cliquez sur **Ajouter**, entrez le nom et le Bundle ID d'une application autorisée à démarrer, puis cliquez sur **Enregistrer**. Pour les applications de productivité mobiles Citrix, utilisez l'ID du champ **ID de package** lors de l'ajout de l'application. Répétez cette étape pour chaque application autorisée à démarrer.
  - **Dossiers interdits :** cliquez sur **Ajouter**, entrez le chemin d'accès d'un dossier pour lequel vous souhaitez restreindre l'accès des utilisateurs (par exemple, /Applications/Utilities), puis cliquez sur **Enregistrer**. Répétez cette étape pour tous les dossiers auxquels vous ne souhaitez pas que les utilisateurs puissent accéder.
  - **Dossiers autorisés :** cliquez sur **Ajouter**, entrez le chemin d'accès d'un dossier pour lequel vous souhaitez accorder l'accès des utilisateurs, puis cliquez sur **Enregistrer**. Répétez cette étape pour tous les dossiers auxquels vous souhaitez que les utilisateurs puissent accéder.

- **Widgets**
  - **Autoriser uniquement l'exécution des widgets du tableau de bord suivants :** Si cette option est définie sur **Activé**, les utilisateurs ne peuvent exécuter que les widgets du tableau de bord configurés dans ce paramètre. La valeur par défaut est **Désactivé**, ce qui permet aux utilisateurs d'exécuter tous les widgets. Si cette option est activée, vous pouvez configurer le paramètre suivant :
    - **Widgets autorisés :** cliquez sur **Ajouter**, entrez le nom et l'ID d'un widget qui est autorisé à être exécuté, puis cliquez sur **Enregistrer**. Répétez cette étape pour chaque widget que vous souhaitez exécuter sur le tableau de bord.

- **Média**
  - **Autoriser AirDrop :** autorise les utilisateurs à partager des photos, des vidéos, des sites Web, des emplacements et autres avec des appareils iOS se trouvant à proximité.

- **Partage**
  - **Activer automatiquement les nouveaux services de partage :** sélectionnez cette option pour activer les services de partage.
  - **Messagerie :** sélectionnez cette option pour autoriser une boîte aux lettres partagée.
  - **Facebook :** sélectionnez cette option pour autoriser un compte Facebook partagé.
  - **Services vidéo - Flickr, Vimeo, Tudou et Youku :** sélectionnez cette option pour autoriser les services vidéo partagés.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Ajouter à Aperture :** sélectionnez cette option pour autoriser la capacité partagée d'ajouter à Aperture.
  - **Sina Weibo :** sélectionnez cette option pour autoriser un compte Sina Weibo partagé.
  - **Twitter :** sélectionnez cette option pour autoriser un compte Twitter partagé.
  - **Messages :** sélectionnez cette option pour autoriser un accès partagé aux messages.
  - **Ajouter à iPhoto :** sélectionnez cette option pour autoriser la capacité partagée d'ajouter à iPhoto.
  - **Ajouter à la liste de lecture :** sélectionnez cette option pour autoriser la capacité partagée d'ajouter à la liste de lecture.
  - **AirDrop :** sélectionnez cette option pour autoriser un compte AirDrop partagé.

- **Fonctionnalité**
  - **Verrouiller l'image de bureau :** indiquez si les utilisateurs peuvent modifier l'image de bureau. La valeur par défaut est **Désactivé**, ce qui signifie que les utilisateurs peuvent modifier l'image de bureau.
  - **Autoriser l'utilisation de l'appareil photo :** indiquez si les utilisateurs peuvent utiliser l'appareil photo sur leurs appareils Mac. La valeur par défaut est **Désactivé**, ce qui signifie que les utilisateurs ne peuvent pas utiliser l'appareil-photo.
  - **Autoriser Apple Music :** permet aux utilisateurs d'utiliser le service Apple Music (macOS 10.12 et versions ultérieures). Si vous n'autorisez pas le service Apple Music, l'application Music s'exécute en mode classique. S'applique uniquement aux appareils supervisés. La valeur par défaut est **Activé**.
  - **Autoriser les suggestions de Spotlight :** indiquez si les utilisateurs peuvent utiliser les suggestions de Spotlight pour effectuer des recherches sur leur Mac et fournir des suggestions Spotlight à partir d'Internet et App Store. La valeur par défaut est **Désactivé**, ce qui empêche les utilisateurs d'utiliser les suggestions de Spotlight.
  - **Autoriser Look Up :** indiquez si les utilisateurs peuvent rechercher les définitions de termes avec le menu contextuel ou le menu de recherche Spotlight. La valeur par défaut est Désactivé, ce qui empêche les utilisateurs d'utiliser Look Up sur leurs appareils Mac.
  - **Autoriser l'utilisation du mot de passe iCloud pour les comptes locaux :** indiquez si les utilisateurs peuvent utiliser leur mot de passe Apple ID et iCloud pour se connecter à leurs appareils Mac. L'activation de cette option signifie que l'utilisateur utilise un seul identifiant et mot de passe pour *tous* les écrans d'ouverture de session sur leurs appareils Mac. La valeur par défaut est **Activé**, ce qui permet aux utilisateurs d'utiliser leur mot de passe Apple ID et iCloud pour accéder à leurs appareils Mac.
  - **Autoriser les documents et données iCloud :** indiquez si les utilisateurs peuvent accéder aux documents et aux données stockés sur iCloud sur des appareils Mac. La valeur par défaut est **Activé**, ce qui empêche les utilisateurs d'utiliser les documents et données iCloud sur des appareils Mac.
    * **Autoriser bureau et documents iCloud :** (macOS 10.12.4 et versions ultérieures)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sélectionné par défaut.

- **Autoriser la synchronisation du trousseau iCloud** : autorise la synchronisation du trousseau iCloud (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser iCloud Mail :** permet aux utilisateurs d'utiliser iCloud Mail (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser contacts iCloud :** permet aux utilisateurs d'utiliser les contacts iCloud (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser calendriers iCloud :** permet aux utilisateurs d'utiliser les calendriers iCloud (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser rappels iCloud :** permet aux utilisateurs d'utiliser les rappels iCloud (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser signets iCloud :** permet aux utilisateurs de se synchroniser avec les signets iCloud (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser notes iCloud :** permet aux utilisateurs d'utiliser les notes iCloud (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser photos iCloud :** si vous réglez ce paramètre sur **Désactivé**, les photos qui ne sont pas entièrement téléchargées à partir de la bibliothèque de photos iCloud sont supprimées du stockage local de l'appareil (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser déverrouillage automatique :** pour plus d'informations sur cette option et Apple Watch, voir https://www.imore.com/auto-unlock (macOS 10.12 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser Touch ID pour déverrouiller votre Mac :** (macOS 10.12.4 et versions ultérieures). La valeur par défaut est **Activé**.
- **Retarder les mises à jour logicielles :** si elle est définie sur **Activé**, cette option retarde la visibilité des mises à jour logicielles pour l'utilisateur. Les utilisateurs ne voient pas de mise à jour logicielle avant le nombre de jours spécifié après la date de publication de la mise à jour logicielle. La valeur par défaut est **Off**. Disponible uniquement pour les appareils supervisés exécutant macOS 10.13.4 et versions ultérieures. La stratégie de mise à jour d'OS contient d'autres paramètres permettant de contrôler la fréquence à laquelle les appareils reçoivent les mises à jour. Consultez la section Stratégie de mise à jour de l'OS.
- **Délai imposé pour les mises à jour logicielles (jours) :** spécifie le nombre de jours pendant lequel retarder une mise à jour logicielle sur l'appareil. Le délai maximum est de 90 jours. La valeur par défaut est **30**. Disponible uniquement pour les appareils supervisés exécutant macOS 10.13.4 et versions ultérieures.
- **Remplissage automatique du mot de passe :** option facultative. Si cette option est désactivée, les utilisateurs ne peuvent pas utiliser les fonctionnalités de remplissage automatique de mot de passe ou de mot de passe fort automatique. La valeur par défaut est **Activé**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

(macOS 10.14 et versions ultérieures).

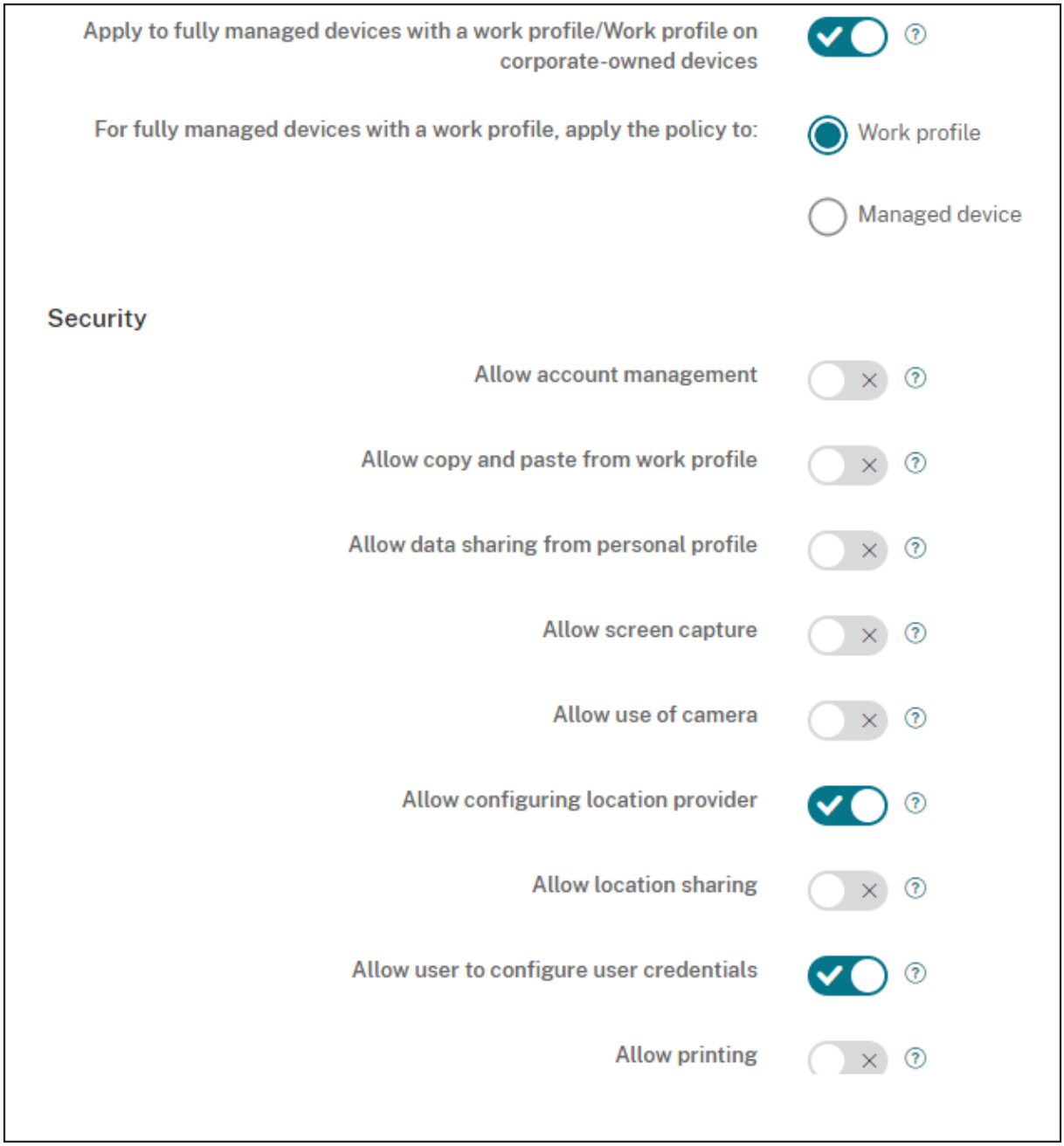
- **Requêtes de proximité de mot de passe :** option facultative. Si cette option est désactivée, les appareils des utilisateurs ne demandent pas de mots de passe aux appareils à proximité. La valeur par défaut est **Activé** (macOS 10.14 et versions ultérieures).
- **Partage de mot de passe :** option facultative. Si cette option est désactivée, les utilisateurs ne peuvent pas partager leurs mots de passe à l'aide de la fonctionnalité Mots de passe AirDrop. La valeur par défaut est **Activé** (macOS 10.14 et versions ultérieures).

Paramètres Android

- **Appareil photo :** autorise les utilisateurs à utiliser l'appareil photo sur leurs appareils. Si la valeur est définie sur **Désactivé**, l'appareil photo est désactivé. La valeur par défaut est **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Android Enterprise



Lorsqu'un nouvel appareil Android ou un appareil Android réinitialisé aux paramètres d'usine est inscrit en mode Profil de travail, les appareils exécutant Android 9.0-10.x sont inscrits en tant qu'appareils entièrement gérés avec profil de travail. Les appareils exécutant Android 11+ sont inscrits en mode Profil de travail sur appareils appartenant à l'entreprise. La stratégie de restriction peut s'appliquer au profil de travail sur l'appareil ou à l'appareil géré.

Sur les appareils inscrits en mode profil de travail sur appareils appartenant à l'entreprise, les restrictions suivantes ne fonctionnent pas :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Autoriser service de sauvegarde
- Activer les applications système
- Empêcher Keyguard de verrouiller l'appareil
- Autoriser utilisation de la barre d'état
- Laisser l'écran allumé
- Autoriser l'utilisateur à contrôler les paramètres applicatifs
- Autoriser l'utilisateur à configurer les informations d'identification
- Autoriser configuration du VPN
- Autoriser le stockage de masse USB
- Autoriser réinitialisation des paramètres d'usine
- Autoriser désinstallation d'applications
- Autoriser les applications non Google Play
- Autoriser le copier/coller entre les profils
- Activer vérification de l'application
- Autoriser la gestion des comptes
- Autoriser l'impression
- Autoriser NFC
- Autoriser l'ajout d'utilisateurs

Par défaut, les paramètres **Débogage USB et Sources inconnues** sont désactivés sur un appareil lorsqu'il est inscrit en mode Profil de travail dans Android Entreprise.

Regardez cette vidéo pour en savoir plus :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Appliquer aux appareils entièrement gérés avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise :** permet de configurer les paramètres de stratégie de restrictions pour les appareils entièrement gérés avec profil de travail. Ces appareils sont également appelés appareils COPE. Lorsque ce paramètre est **activé**, sélectionnez l'un des paramètres suivants :

  - **Profil de travail :** les paramètres de restrictions que vous configurez s'appliquent uniquement au profil de travail sur l'appareil.
  - **Appareil géré :** les paramètres de restrictions que vous configurez s'appliquent uniquement à l'appareil.

  Lorsque ce paramètre est **Désactivé**, les paramètres d'informations d'identification que vous configurez s'appliquent à l'appareil, à l'exception des paramètres qui s'appliquent explicitement au profil de travail. La valeur par défaut est **Off**.

Lorsque l'option **Appliquer aux appareils entièrement gérés avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise** est désactivée, configurez les paramètres suivants :

- **Sécurité**

  - **Autoriser la gestion des comptes :** permet au compte d'être ajouté aux appareils se trouvant dans le profil de travail et aux appareils gérés. La valeur par défaut est **Off**.
  - **Autoriser le copier-coller à partir du profil de travail :** si cette option est définie sur **Activé**, les utilisateurs peuvent copier et coller les données des applications du profil de travail vers les applications du profil personnel. La valeur par défaut est **Off**.
  - **Autoriser le partage de données à partir du profil personnel :** si cette option est définie sur **Activé**, les utilisateurs peuvent copier, coller et partager des fichiers et des données des applications du profil personnel vers les applications du profil de travail. La valeur par défaut est **Off**.
  - **Autoriser la capture d'écran :** permet aux utilisateurs d'enregistrer ou de prendre une capture d'écran de l'écran de l'appareil. La valeur par défaut est **Off**.
  - **Autoriser l'utilisation de l'appareil photo :** permet aux utilisateurs de prendre des photos et de créer des vidéos avec l'appareil photo de leurs appareils. La valeur par défaut est **Off**.
  - **Autoriser configuration du VPN :** autorise les utilisateurs à créer des configurations VPN. Pour les appareils en mode Profil de travail fonctionnant sous Android 6 et versions ultérieures et pour les appareils entièrement gérés. La valeur par défaut est **Activé**.
  - **Autoriser service de sauvegarde :** autorise les utilisateurs à sauvegarder leurs données d'application et système sur leurs appareils. La valeur par défaut est **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Autoriser NFC :** autorise les utilisateurs à envoyer des pages Web, des photos, des vidéos ou tout autre contenu de leurs appareils à un autre appareil via la communication en champ proche (NFC). Pour MDM 4.0 et versions ultérieures. La valeur par défaut est **Activé**.
- **Autoriser configuration du fournisseur de localisation :** autorise les utilisateurs à activer le GPS sur leurs appareils. Pour Android API 28 et versions ultérieures. La valeur par défaut est **Activé**.
- **Autoriser partage de position :** pour les profils gérés, le propriétaire de l'appareil peut modifier ce paramètre. La valeur par défaut est **Off**.

  > **Conseil :**
  >
  > Vous pouvez créer des stratégies d'emplacement dans Citrix Endpoint Management pour imposer des limites géographiques. Voir Stratégie d'emplacement.

- **Autoriser l'utilisateur à configurer les informations d'identification :** indiquez si les utilisateurs peuvent configurer les informations d'identification dans le keystore géré. La valeur par défaut est **Activé**.
- **Autoriser l'impression :** si ce paramètre est défini sur **Activé**, les utilisateurs peuvent imprimer sur une imprimante accessible à partir de la machine utilisateur. La valeur par défaut est **Désactivé**. Disponible pour : Android 9 et versions ultérieures.
- **Autoriser le débogage USB : Désactivé** par défaut.

• **Applications**

- **Activer les applications système :** permet aux utilisateurs d'exécuter des applications d'appareil préinstallées. La valeur par défaut est **Off**. Pour activer des applications spécifiques, cliquez sur **Ajouter** dans le tableau **Liste des applications système**.
  * **Liste des applications système :** liste des applications système que vous souhaitez activer sur l'appareil. Définissez **Activer les applications système** sur **Activé** et ajoutez le nom du package d'application. Pour rechercher le nom du package d'une application système, vous pouvez utiliser Android Debug Bridge (`adb`) pour appeler la commande de gestionnaire de packages Android (`pm`). Par exemple, `adb shell "pm list packages -f name"`, où « name » fait partie du nom du package. Pour en savoir plus, voir https://developer.android.com/studio/command-line/adb. Pour les appareils Android Enterprise, vous pouvez restreindre les autorisations des applications à l'aide de la stratégie Autorisations applicatives Android Entreprise.
- **Désactiver les applications :** bloque l'exécution d'une liste spécifique d'applications sur des appareils. La valeur par défaut est **Off**. Pour désactiver une application installée, définissez le paramètre sur **Activé**, cliquez sur **Ajouter** dans le tableau **Liste d'applications**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Liste des applications :** liste des applications que vous souhaitez bloquer. Définissez **Désactiver les applications** sur **Activé** et ajoutez l'application. Tapez le nom du package de l'application. La modification et le déploiement d'une liste d'applications écrasent la liste d'applications précédente. Par exemple : si vous désactivez com.example1 et com.example2 et modifiez ensuite la liste vers com.example1 et com.example3, Citrix Endpoint Management active com.example.2.
  - **Activer vérification de l'application :** permet au système d'exploitation d'analyser les applications pour détecter un comportement malveillant. La valeur par défaut est **Activé**.
  - **Activer Google Apps :** permet aux utilisateurs de télécharger des applications à partir de Google Mobile Services sur l'appareil. La valeur par défaut est **Activé**.
  - **Autoriser les applications non Google Play :** permet l'installation d'applications provenant de magasins autres que Google Play. La valeur par défaut est **Off**.
  - **Autoriser les applications non Google Play pour tous les profils :** si cette option est définie sur **Activé**, les utilisateurs peuvent installer des applications provenant de magasins autres que Google Play sur tous les profils de l'appareil. La valeur par défaut est **Off**.
  - **Autoriser l'utilisateur à contrôler les paramètres applicatifs :** permet aux utilisateurs de désinstaller des applications, de désactiver des applications, d'effacer le cache et les données, de forcer l'arrêt de toute application et d'effacer les paramètres par défaut. Les utilisateurs effectuent ces actions à partir de l'application Paramètres. La valeur par défaut est **Désactivé**.
  - **Autoriser désinstallation d'applications :** permet aux utilisateurs de désinstaller des applications depuis le Google Play Store d'entreprise. La valeur par défaut est **Off**.

- **Profil de travail BYOD**
  - **Activer les applications connectées :** si cette option est activée, les utilisateurs peuvent sélectionner des applications capables de communiquer entre les profils professionnels et personnels, en utilisant à la fois des données professionnelles et personnelles. Après l'activation, cliquez sur **Ajouter**, sélectionnez les applications souhaitées, puis cliquez sur **Enregistrer**. Un profil professionnel est nécessaire pour activer cette fonctionnalité. La valeur par défaut est **Off**.
  - **Autoriser les widgets d'applications de profil de travail sur l'écran d'accueil :** si ce paramètre est **Activé**, les utilisateurs peuvent placer des widgets d'application de profil de travail sur l'écran d'accueil de l'appareil. Si ce paramètre est **Désactivé**, les utilisateurs ne peuvent pas placer de widgets d'application de profil de travail sur l'écran d'accueil de l'appareil. La valeur par défaut est **Off**.
    * **Applications avec widgets autorisés :** liste des applications que vous souhaitez autoriser sur l'écran d'accueil. Définissez l'option **Autoriser les widgets d'applications de profil de travail sur l'écran d'accueil** sur **Activé** et ajoutez l'application. Cliquez sur **Ajouter** et sélectionnez dans la liste une application pour laquelle vous

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

souhaitez autoriser l'affichage des widgets sur l'écran d'accueil. Cliquez sur **Enregistrer**. Répétez ce processus pour autoriser plus de widgets d'application.

- **Autoriser les contacts de profil de travail dans les contacts de l'appareil :** affiche les contacts du profil Android Enterprise géré dans le profil parent pour les appels entrants (Android 7.0 et versions ultérieures). La valeur par défaut est **Off**.

- **Appareil entièrement géré uniquement**
  - **Autoriser l'ajout d'utilisateurs :** permet aux utilisateurs d'ajouter de nouveaux utilisateurs sur un appareil. La valeur par défaut est **Activé**.
  - **Autoriser itinérance des données :** autorise les utilisateurs à utiliser des données cellulaires en itinérance. La valeur par défaut est Désactivé, ce qui désactive l'itinérance sur les appareils des utilisateurs. La valeur par défaut est **Off**.
  - **Autoriser les SMS :** autorise les utilisateurs à envoyer et à recevoir des messages SMS. La valeur par défaut est **Off**.
  - **Autoriser utilisation de la barre d'état :** si ce paramètre est défini sur **Activé**, la barre d'état est activée sur les appareils gérés et les appareils dédiés (également appelés appareils d'entreprise à usage unique ou COSU). Cela désactive les notifications, les paramètres rapides et autres superpositions d'écran qui permettent de sortir du mode plein écran. Les utilisateurs peuvent accéder aux paramètres du système et afficher les notifications. Pour Android 6.0 et versions ultérieures. La valeur par défaut est **Off**.
  - **Autoriser le bluetooth :** autorise les utilisateurs à utiliser Bluetooth. La valeur par défaut est **Activé**.
    - **Autoriser le partage Bluetooth :** si cette option est désactivée, les utilisateurs ne peuvent pas établir de partage Bluetooth sortant sur leurs appareils. Par défaut, ce paramètre est sélectionné.
  - **Autoriser la configuration de la date et de l'heure :** permet aux utilisateurs de modifier la date et l'heure sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser réinitialisation des paramètres d'usine :** autorise les utilisateurs à effectuer une réinitialisation d'usine sur leurs appareils. La valeur par défaut est **Activé**.
  - **Laisser l'écran allumé :** si ce paramètre est **activé**, l'écran de l'appareil reste allumé lorsque l'appareil est branché. La valeur par défaut est **Off**.
  - **Autoriser le stockage de masse USB :** autorise le transfert de fichiers de données volumineux entre les appareils des utilisateurs et un ordinateur via une connexion USB. La valeur par défaut est **Activé**.
  - **Autoriser le microphone :** autorise les utilisateurs à utiliser le microphone sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser le partage de connexion :** permet aux utilisateurs de configurer des points d'accès mobiles et des données de connexion. La valeur par défaut est **Off**.
  - **Empêcher Keyguard de verrouiller l'appareil :** si ce paramètre est **activé**, il désactive

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Keyguard sur l'écran de verrouillage sur les appareils gérés et les appareils dédiés (également appelés appareils d'entreprise à usage unique). La valeur par défaut est **Off**.

- **Autoriser les modifications Wi-Fi :** si ce paramètre est **activé**, les utilisateurs peuvent activer ou désactiver le Wi-Fi et se connecter aux réseaux Wi-Fi. La valeur par défaut est **Activé**.
- **Autoriser transfert de fichiers :** permet le transfert de fichiers via USB. La valeur par défaut est **Off**.

- **Samsung**
  - **Activer le keystore TIMA :** le magasin de clé TIMA fournit un stockage de clé sécurisé basé sur TrustZone pour les clés symétriques. Les paires de clés RSA et les certificats sont routés vers le fournisseur de magasins de clés par défaut à des fins de stockage. La valeur par défaut est **Off**.
  - **Autoriser liste Partager :** autorise les utilisateurs à partager un contenu entre des applications dans la liste Partager via. La valeur par défaut est **Activé**.
  - **Activer le journal d'audit :** autorise la création de journaux d'audit d'événements pour l'analyse poussée d'un appareil. La valeur par défaut est **Off**.

- **Samsung : appareil entièrement géré uniquement**
  - **Activer la vérification du démarrage fiable ODE :** utilise la vérification du démarrage fiable ODE pour établir une chaîne d'approbation allant du bootloader vers l'image système. La valeur par défaut est **Activé**.
  - **Autoriser les appels d'urgence uniquement :** autorise les utilisateurs à activer le mode Appel d'urgence uniquement sur leurs appareils. La valeur par défaut est **Off**.
  - **Autoriser la restauration du firmware :** autorise les utilisateurs à récupérer le firmware sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser le cryptage rapide :** autorise le cryptage de l'espace de mémoire utilisé uniquement. Ce cryptage est différent du cryptage complet du disque qui crypte toutes les données. Ces données incluent les paramètres, les données d'application, les fichiers et applications téléchargés, les fichiers multimédias et autres fichiers. La valeur par défaut est **Activé**.
  - **Activer le mode Critères communs :** fait passer l'appareil en mode Critères communs. La configuration de type Critère commun applique des processus de sécurité stricts. La valeur par défaut est **Activé**.
  - **Activer la bannière de redémarrage :** affiche un message ou une bannière de notification d'utilisation du système approuvée par DoD au redémarrage des appareils. La valeur par défaut est **Off**.
  - **Autoriser la modification des paramètres :** permet aux utilisateurs de modifier les paramètres de leurs appareils entièrement gérés. La valeur par défaut est **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Activer l'utilisation des données en arrière-plan :** permet aux applications de synchroniser les données en arrière-plan. Pour les appareils entièrement gérés. La valeur par défaut est **Activé**.
- **Autoriser le presse-papiers :** autorise les utilisateurs à copier des données dans le Presse-papiers de leurs appareils.
  * **Autoriser le partage du presse-papiers :** autorise les utilisateurs à partager le contenu du Presse-papiers entre leurs appareils et un ordinateur (MDM 4.0 et versions ultérieures).
- **Autoriser la touche Origine :** autorise les utilisateurs à utiliser la touche **Début** sur leurs appareils entièrement gérés. La valeur par défaut est **Activé**.
- **Autoriser positions factices :** autorise les utilisateurs à feindre leur emplacement de géolocalisation. Pour les appareils entièrement gérés. La valeur par défaut est **Off**.
- **NFC :** autorise les utilisateurs à utiliser NFC sur leurs appareils entièrement gérés (MDM 3.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser mise hors tension :** autorise les utilisateurs à arrêter leurs appareils entièrement gérés (MDM 3.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser Wi-Fi direct :** autorise les utilisateurs à se connecter directement à un autre appareil à l'aide de leur connexion Wi-Fi. La valeur par défaut est **Activé**. Si ce paramètre est **activé**, vous devez activer le paramètre **Autoriser modifications du Wi-Fi**.
- **Autoriser carte SD :** autorise les utilisateurs à utiliser une carte SD, le cas échéant, avec leurs appareils. La valeur par défaut est **Activé**.
- **Autoriser le stockage hôte USB :** autorise les appareils des utilisateurs à agir comme hôte USB lorsqu'un périphérique USB se connecte aux appareils. Les appareils des utilisateurs fournissent ensuite l'alimentation au périphérique USB. La valeur par défaut est **Activé**.
- **Autoriser composeur vocal :** autorise les utilisateurs à utiliser le composeur vocal sur leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser S Beam :** autorise les utilisateurs à partager un contenu avec des tiers à l'aide de NFC et Wi-Fi Direct (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser S Voice :** autorise les utilisateurs à utiliser l'assistant personnel intelligent et le navigateur de connaissances sur leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser partage de connexion USB :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion USB. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, **Autoriser le partage de connexion** doit également être défini sur **Activé**.
- **Autoriser partage de connexion Bluetooth :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion Bluetooth. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, **Autoriser le partage de connexion** doit également être défini sur **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  * **Autoriser le partage Bluetooth :** si cette option est désactivée, les utilisateurs ne peuvent pas établir de partage Bluetooth sortant sur leurs appareils. Par défaut, ce paramètre est sélectionné.
- **Autoriser partage de connexion Wi-Fi :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion Wi-Fi. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, **Autoriser le partage de connexion** doit également être défini sur **Activé**.
- **Autoriser les MMS entrants :** autorise les utilisateurs à recevoir des messages MMS. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Autoriser les MMS sortants :** autorise les utilisateurs à envoyer des messages MMS. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Autoriser les SMS entrants :** autorise les utilisateurs à recevoir des messages texte. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Autoriser les SMS sortants :** autorise les utilisateurs à envoyer des messages texte. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Configurer réseaux mobiles :** permet aux utilisateurs d'utiliser leurs données cellulaires. La valeur par défaut est **Off**.
- **Limite par jour (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque jour. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Limite par semaine (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque semaine. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Limite par mois (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque mois. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Autoriser uniquement les connexions VPN sécurisées :** autorise les utilisateurs à uniquement utiliser des connexions sécurisées (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser l'enregistrement audio :** autorise les utilisateurs à effectuer des enregistrements audio avec leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser le microphone**.
- **Autoriser l'enregistrement vidéo :** autorise les utilisateurs à effectuer des enregistrements vidéo avec leurs appareils (MDM 4.0 et versions ultérieures). La valeur par

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser l'utilisation de l'appareil photo**.
  - **Autoriser messages push en itinérance :** autorise les utilisateurs à utiliser des données cellulaires pour la transmission. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser itinérance des données**.
  - **Autoriser synchronisation automatique en itinérance :** autorise les utilisateurs à utiliser les données cellulaires pour la synchronisation. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser itinérance des données**.
  - **Autoriser appels vocaux en itinérance :** autorise les utilisateurs à utiliser des données cellulaires pour les appels vocaux. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser itinérance des données**.

- **Samsung : appareil entièrement géré**
  - **Activer la vérification de révocation :** active la vérification des listes de certificats révoqués. La valeur par défaut est **Off**.

Lorsque l'option **Appliquer aux appareils entièrement gérés avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise** est activée et que l'option **Pour les appareils entièrement gérés avec un profil professionnel, appliquez la stratégie à** est définie sur **Profil de travail**, configurez ces paramètres :

- **Sécurité**
  - **Autoriser la gestion des comptes :** permet au compte d'être ajouté aux appareils se trouvant dans le profil de travail et aux appareils gérés. La valeur par défaut est **Off**.
  - **Autoriser le copier/coller entre les profils :** si cette option est définie sur **Activé**, les utilisateurs sont autorisés à copier et coller entre les applications du profil Android Enterprise et les applications dans la zone personnelle. La valeur par défaut est **Off**.
  - **Autoriser la capture d'écran :** permet aux utilisateurs d'enregistrer ou de prendre une capture d'écran de l'écran de l'appareil. La valeur par défaut est **Off**.
  - **Autoriser l'utilisation de l'appareil photo :** permet aux utilisateurs de prendre des photos et de créer des vidéos avec l'appareil photo de leurs appareils. La valeur par défaut est **Off**.
  - **Autoriser configuration du fournisseur de localisation :** autorise les utilisateurs à activer le GPS sur leurs appareils. Pour Android API 28 et versions ultérieures. La valeur par défaut est **Activé**.
  - **Autoriser partage de position :** pour les profils gérés, le propriétaire de l'appareil peut modifier ce paramètre. La valeur par défaut est **Off**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Conseil :**
>
> Vous pouvez créer des stratégies d'emplacement dans Citrix Endpoint Management pour imposer des limites géographiques. Voir Stratégie d'emplacement.

- **Autoriser l'utilisateur à configurer les informations d'identification :** indiquez si les utilisateurs peuvent configurer les informations d'identification dans le keystore géré. La valeur par défaut est **Activé**.
- **Autoriser l'impression :** si ce paramètre est défini sur **Activé**, les utilisateurs peuvent imprimer sur une imprimante accessible à partir de la machine utilisateur. La valeur par défaut est **Désactivé**. Disponible pour : Android 9 et versions ultérieures.

• **Applications**

- **Activer les applications système :** permet aux utilisateurs d'exécuter des applications d'appareil préinstallées. La valeur par défaut est **Off**. Pour activer des applications spécifiques, cliquez sur **Ajouter** dans le tableau **Liste des applications système**.
  * **Liste des applications système :** liste des applications système que vous souhaitez activer sur l'appareil. Définissez **Activer les applications système** sur **Activé** et ajoutez le nom du package d'application. Pour rechercher le nom du package d'une application système, vous pouvez utiliser Android Debug Bridge (`adb`) pour appeler la commande de gestionnaire de packages Android (`pm`). Par exemple, `adb shell "pm list packages -f name"`, où « name » fait partie du nom du package. Pour en savoir plus, voir https://developer.android.com/studio/command-line/adb. Pour les appareils Android Enterprise, vous pouvez restreindre les autorisations des applications à l'aide de la stratégie Autorisations applicatives Android Entreprise.
- **Désactiver les applications :** bloque l'exécution d'une liste spécifique d'applications sur des appareils. La valeur par défaut est **Off**. Pour désactiver une application installée, définissez le paramètre sur **Activé**, cliquez sur **Ajouter** dans le tableau **Liste d'applications**.
  * **Liste des applications :** liste des applications que vous souhaitez bloquer. Définissez **Désactiver les applications** sur **Activé** et ajoutez l'application. Tapez le nom du package de l'application. La modification et le déploiement d'une liste d'applications écrasent la liste d'applications précédente. Par exemple : si vous désactivez com.example1 et com.example2 et modifiez ensuite la liste vers com.example1 et com.example3, Citrix Endpoint Management active com.example.2.
- **Activer vérification de l'application :** permet au système d'exploitation d'analyser les applications pour détecter un comportement malveillant. La valeur par défaut est **Activé**.
- **Activer Google Apps :** permet aux utilisateurs de télécharger des applications à partir de Google Mobile Services sur l'appareil. La valeur par défaut est **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Autoriser les applications non Google Play :** permet l'installation d'applications provenant de magasins autres que Google Play. La valeur par défaut est **Off**.
  - **Autoriser l'utilisateur à contrôler les paramètres applicatifs :** permet aux utilisateurs de désinstaller des applications, de désactiver des applications, d'effacer le cache et les données, de forcer l'arrêt de toute application et d'effacer les paramètres par défaut. Les utilisateurs effectuent ces actions à partir de l'application Paramètres. La valeur par défaut est **Désactivé**.
  - **Autoriser désinstallation d'applications :** permet aux utilisateurs de désinstaller des applications depuis le Google Play Store d'entreprise. La valeur par défaut est **Off**.

- **Profil de travail BYOD**
  - **Autoriser les widgets d'applications de profil de travail sur l'écran d'accueil :** si ce paramètre est **Activé**, les utilisateurs peuvent placer des widgets d'application de profil de travail sur l'écran d'accueil de l'appareil. Si ce paramètre est **Désactivé**, les utilisateurs ne peuvent pas placer de widgets d'application de profil de travail sur l'écran d'accueil de l'appareil. La valeur par défaut est **Off**.
    * **Applications avec widgets autorisés :** liste des applications que vous souhaitez autoriser sur l'écran d'accueil. Définissez l'option **Autoriser les widgets d'applications de profil de travail sur l'écran d'accueil** sur **Activé** et ajoutez l'application. Cliquez sur **Ajouter** et sélectionnez dans la liste une application pour laquelle vous souhaitez autoriser l'affichage des widgets sur l'écran d'accueil. Cliquez sur **Enregistrer**. Répétez ce processus pour autoriser plus de widgets d'application.
  - **Autoriser les contacts de profil de travail dans les contacts de l'appareil :** affiche les contacts du profil Android Enterprise géré dans le profil parent pour les appels entrants (Android 7.0 et versions ultérieures). La valeur par défaut est **Off**.

- **Samsung**
  - **Activer le keystore TIMA :** le magasin de clé TIMA fournit un stockage de clé sécurisé basé sur TrustZone pour les clés symétriques. Les paires de clés RSA et les certificats sont routés vers le fournisseur de magasins de clés par défaut à des fins de stockage. La valeur par défaut est **Off**.
  - **Autoriser liste Partager :** autorise les utilisateurs à partager un contenu entre des applications dans la liste Partager via. La valeur par défaut est **Activé**.
  - **Activer le journal d'audit :** autorise la création de journaux d'audit d'événements pour l'analyse poussée d'un appareil. La valeur par défaut est **Off**.

- **Samsung : appareil entièrement géré**
  - **Activer la vérification de révocation :** active la vérification des listes de certificats révoqués. La valeur par défaut est **Off**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Lorsque l'option **Appliquer aux appareils entièrement gérés avec un profil de travail/profil de travail sur appareils appartenant à l'entreprise** est activée et que l'option **Pour les appareils entièrement gérés avec un profil professionnel, appliquez la stratégie à** est définie sur **Appareil géré**, configurez ces paramètres :

- **Sécurité**
  - **Autoriser la gestion des comptes :** permet au compte d'être ajouté aux appareils se trouvant dans le profil de travail et aux appareils gérés. La valeur par défaut est **Off**.
  - **Autoriser le copier/coller entre les profils :** si cette option est définie sur **Activé**, les utilisateurs sont autorisés à copier et coller entre les applications du profil Android Enterprise et les applications dans la zone personnelle. La valeur par défaut est **Off**.
  - **Autoriser la capture d'écran :** permet aux utilisateurs d'enregistrer ou de prendre une capture d'écran de l'écran de l'appareil. La valeur par défaut est **Off**.
  - **Autoriser l'utilisation de l'appareil photo :** permet aux utilisateurs de prendre des photos et de créer des vidéos avec l'appareil photo de leurs appareils. La valeur par défaut est **Off**.
  - **Autoriser configuration du VPN :** autorise les utilisateurs à créer des configurations VPN. Pour les appareils en mode Profil de travail fonctionnant sous Android 6 et versions ultérieures et pour les appareils entièrement gérés. La valeur par défaut est **Activé**.
  - **Autoriser service de sauvegarde :** autorise les utilisateurs à sauvegarder leurs données d'application et système sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser NFC :** autorise les utilisateurs à envoyer des pages Web, des photos, des vidéos ou tout autre contenu de leurs appareils à un autre appareil via la communication en champ proche (NFC). Pour MDM 4.0 et versions ultérieures. La valeur par défaut est **Activé**.
  - **Autoriser configuration du fournisseur de localisation :** autorise les utilisateurs à activer le GPS sur leurs appareils. Pour Android API 28 et versions ultérieures. La valeur par défaut est **Activé**.
  - **Autoriser partage de position :** pour les profils gérés, le propriétaire de l'appareil peut modifier ce paramètre. La valeur par défaut est **Off**.

    > **Conseil :**
    >
    > Vous pouvez créer des stratégies d'emplacement dans Citrix Endpoint Management pour imposer des limites géographiques. Voir Stratégie d'emplacement.

  - **Autoriser l'utilisateur à configurer les informations d'identification :** indiquez si les utilisateurs peuvent configurer les informations d'identification dans le keystore géré. La valeur par défaut est **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Autoriser l'impression :** si ce paramètre est défini sur **Activé**, les utilisateurs peuvent imprimer sur une imprimante accessible à partir de la machine utilisateur. La valeur par défaut est **Désactivé**. Disponible pour : Android 9 et versions ultérieures.
  - **Autoriser le débogage USB : Désactivé** par défaut.

- **Applications**
  - **Activer les applications système :** permet aux utilisateurs d'exécuter des applications d'appareil préinstallées. La valeur par défaut est **Off**. Pour activer des applications spécifiques, cliquez sur **Ajouter** dans le tableau **Liste des applications système**.
    * **Liste des applications système :** liste des applications système que vous souhaitez activer sur l'appareil. Définissez **Activer les applications système** sur **Activé** et ajoutez le nom du package d'application. Pour rechercher le nom du package d'une application système, vous pouvez utiliser Android Debug Bridge (`adb`) pour appeler la commande de gestionnaire de packages Android (`pm`). Par exemple, `adb shell "pm list packages -f name"`, où « name » fait partie du nom du package. Pour en savoir plus, voir https://developer.android.com/studio/command-line/adb. Pour les appareils Android Enterprise, vous pouvez restreindre les autorisations des applications à l'aide de la stratégie Autorisations applicatives Android Entreprise.
  - **Désactiver les applications :** bloque l'exécution d'une liste spécifique d'applications sur des appareils. La valeur par défaut est **Off**. Pour désactiver une application installée, définissez le paramètre sur **Activé**, cliquez sur **Ajouter** dans le tableau **Liste d'applications**.
    * **Liste des applications :** liste des applications que vous souhaitez bloquer. Définissez **Désactiver les applications** sur **Activé** et ajoutez l'application. Tapez le nom du package de l'application. La modification et le déploiement d'une liste d'applications écrasent la liste d'applications précédente. Par exemple : si vous désactivez com.example1 et com.example2 et modifiez ensuite la liste vers com.example1 et com.example3, Citrix Endpoint Management active com.example.2.
  - **Activer vérification de l'application :** permet au système d'exploitation d'analyser les applications pour détecter un comportement malveillant. La valeur par défaut est **Activé**.
  - **Activer Google Apps :** permet aux utilisateurs de télécharger des applications à partir de Google Mobile Services sur l'appareil. La valeur par défaut est **Activé**.
  - **Autoriser les applications non Google Play :** permet l'installation d'applications provenant de magasins autres que Google Play. La valeur par défaut est **Off**.
  - **Autoriser l'utilisateur à contrôler les paramètres applicatifs :** permet aux utilisateurs de désinstaller des applications, de désactiver des applications, d'effacer le cache et les données, de forcer l'arrêt de toute application et d'effacer les paramètres par défaut. Les utilisateurs effectuent ces actions à partir de l'application Paramètres. La valeur par défaut est **Désactivé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Autoriser désinstallation d'applications :** permet aux utilisateurs de désinstaller des applications depuis le Google Play Store d'entreprise. La valeur par défaut est **Off**.

- **Appareil entièrement géré uniquement**
  - **Autoriser l'ajout d'utilisateurs :** permet aux utilisateurs d'ajouter de nouveaux utilisateurs sur un appareil. La valeur par défaut est **Activé**.
  - **Autoriser itinérance des données :** autorise les utilisateurs à utiliser des données cellulaires en itinérance. La valeur par défaut est Désactivé, ce qui désactive l'itinérance sur les appareils des utilisateurs. La valeur par défaut est **Off**.
  - **Autoriser les SMS :** autorise les utilisateurs à envoyer et à recevoir des messages SMS. La valeur par défaut est **Off**.
  - **Autoriser utilisation de la barre d'état :** si ce paramètre est défini sur **Activé**, la barre d'état est activée sur les appareils gérés et les appareils dédiés (également appelés appareils d'entreprise à usage unique ou COSU). Cela désactive les notifications, les paramètres rapides et autres superpositions d'écran qui permettent de sortir du mode plein écran. Les utilisateurs peuvent accéder aux paramètres du système et afficher les notifications. Pour Android 6.0 et versions ultérieures. La valeur par défaut est **Off**.
  - **Autoriser le bluetooth :** autorise les utilisateurs à utiliser Bluetooth. La valeur par défaut est **Activé**.
    - **Autoriser le partage Bluetooth :** si cette option est désactivée, les utilisateurs ne peuvent pas établir de partage Bluetooth sortant sur leurs appareils. Par défaut, ce paramètre est sélectionné.
  - **Autoriser la configuration de la date et de l'heure :** permet aux utilisateurs de modifier la date et l'heure sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser réinitialisation des paramètres d'usine :** autorise les utilisateurs à effectuer une réinitialisation d'usine sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser la protection de la réinitialisation d'usine :** si cette option est définie sur **Activé**, lorsque l'appareil est réinitialisé à l'aide du mode de récupération, l'utilisateur doit fournir les informations d'identification du compte qui se trouvait sur l'appareil avant la réinitialisation. Il peut également fournir le verrouillage de l'appareil s'il a été défini avant la réinitialisation. Si cette option est définie sur **Désactivé**, l'authentification n'est pas requise après une réinitialisation. La valeur par défaut est **Activé**.
  - **Laisser l'écran allumé :** si ce paramètre est **activé**, l'écran de l'appareil reste allumé lorsque l'appareil est branché. La valeur par défaut est **Off**.
  - **Autoriser le stockage de masse USB :** autorise le transfert de fichiers de données volumineux entre les appareils des utilisateurs et un ordinateur via une connexion USB. La valeur par défaut est **Activé**.
  - **Autoriser le microphone :** autorise les utilisateurs à utiliser le microphone sur leurs appareils. La valeur par défaut est **Activé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Autoriser le partage de connexion :** permet aux utilisateurs de configurer des points d'accès mobiles et des données de connexion. La valeur par défaut est **Off**. Lorsque ce paramètre est activé, ces paramètres sont disponibles pour les appareils Samsung :
  - **Empêcher Keyguard de verrouiller l'appareil :** si ce paramètre est **activé**, il désactive Keyguard sur l'écran de verrouillage sur les appareils gérés et les appareils dédiés (également appelés appareils d'entreprise à usage unique). La valeur par défaut est **Off**.
  - **Autoriser les modifications Wi-Fi :** si ce paramètre est **activé**, les utilisateurs peuvent activer ou désactiver le Wi-Fi et se connecter aux réseaux Wi-Fi. La valeur par défaut est **Activé**.
  - **Autoriser transfert de fichiers :** permet le transfert de fichiers via USB. La valeur par défaut est **Off**.

- **Samsung**
  - **Activer le keystore TIMA :** le magasin de clé TIMA fournit un stockage de clé sécurisé basé sur TrustZone pour les clés symétriques. Les paires de clés RSA et les certificats sont routés vers le fournisseur de magasins de clés par défaut à des fins de stockage. La valeur par défaut est **Off**.
  - **Autoriser liste Partager :** autorise les utilisateurs à partager un contenu entre des applications dans la liste Partager via. La valeur par défaut est **Activé**.
  - **Activer le journal d'audit :** autorise la création de journaux d'audit d'événements pour l'analyse poussée d'un appareil. La valeur par défaut est **Off**.

- **Samsung : appareil entièrement géré uniquement**
  - **Activer la vérification du démarrage fiable ODE :** utilise la vérification du démarrage fiable ODE pour établir une chaîne d'approbation allant du bootloader vers l'image système. La valeur par défaut est **Activé**.
  - **Autoriser les appels d'urgence uniquement :** autorise les utilisateurs à activer le mode Appel d'urgence uniquement sur leurs appareils. La valeur par défaut est **Off**.
  - **Autoriser la restauration du firmware :** autorise les utilisateurs à récupérer le firmware sur leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser le cryptage rapide :** autorise le cryptage de l'espace de mémoire utilisé uniquement. Ce cryptage est différent du cryptage complet du disque qui crypte toutes les données. Ces données incluent les paramètres, les données d'application, les fichiers et applications téléchargés, les fichiers multimédias et autres fichiers. La valeur par défaut est **Activé**.
  - **Activer le mode Critères communs :** fait passer l'appareil en mode Critères communs. La configuration de type Critère commun applique des processus de sécurité stricts. La valeur par défaut est **Activé**.
  - **Activer la bannière de redémarrage :** affiche un message ou une bannière de notification d'utilisation du système approuvée par DoD au redémarrage des appareils. La valeur par

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

défaut est **Off**.

- **Autoriser la modification des paramètres :** permet aux utilisateurs de modifier les paramètres de leurs appareils entièrement gérés. La valeur par défaut est **Activé**.
- **Activer l'utilisation des données en arrière-plan :** permet aux applications de synchroniser les données en arrière-plan. Pour les appareils entièrement gérés. La valeur par défaut est **Activé**.
- **Autoriser le presse-papiers :** autorise les utilisateurs à copier des données dans le Presse-papiers de leurs appareils. La valeur par défaut est **Activé**.
  - **Autoriser le partage du presse-papiers :** autorise les utilisateurs à partager le contenu du Presse-papiers entre leurs appareils et un ordinateur (MDM 4.0 et versions ultérieures).
- **Autoriser la touche Origine :** autorise les utilisateurs à utiliser la touche **Début** sur leurs appareils entièrement gérés. La valeur par défaut est **Activé**.
- **Autoriser positions factices :** autorise les utilisateurs à feindre leur emplacement de géolocalisation. Pour les appareils entièrement gérés. La valeur par défaut est **Off**.
- **NFC :** autorise les utilisateurs à utiliser NFC sur leurs appareils entièrement gérés (MDM 3.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser mise hors tension :** autorise les utilisateurs à arrêter leurs appareils entièrement gérés (MDM 3.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser Wi-Fi direct :** autorise les utilisateurs à se connecter directement à un autre appareil à l'aide de leur connexion Wi-Fi. La valeur par défaut est **Activé**. Si ce paramètre est **activé**, vous devez activer le paramètre **Autoriser modifications du Wi-Fi**.
- **Autoriser carte SD :** autorise les utilisateurs à utiliser une carte SD, le cas échéant, avec leurs appareils. La valeur par défaut est **Activé**.
- **Autoriser le stockage hôte USB :** autorise les appareils des utilisateurs à agir comme hôte USB lorsqu'un périphérique USB se connecte aux appareils. Les appareils des utilisateurs fournissent ensuite l'alimentation au périphérique USB. La valeur par défaut est **Activé**.
- **Autoriser composeur vocal :** autorise les utilisateurs à utiliser le composeur vocal sur leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser S Beam :** autorise les utilisateurs à partager un contenu avec des tiers à l'aide de NFC et Wi-Fi Direct (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser S Voice :** autorise les utilisateurs à utiliser l'assistant personnel intelligent et le navigateur de connaissances sur leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser partage de connexion USB :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion USB. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, **Autoriser le partage de connexion** doit également être défini sur **Activé**.
- **Autoriser partage de connexion Bluetooth :** autorise les utilisateurs à partager une con-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

nexion de données mobiles avec un autre appareil à l'aide de leur connexion Bluetooth. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, **Autoriser le partage de connexion** doit également être défini sur **Activé**.

- **Autoriser partage de connexion Wi-Fi :** autorise les utilisateurs à partager une connexion de données mobiles avec un autre appareil à l'aide de leur connexion Wi-Fi. La valeur par défaut est **Désactivé**. Si le paramètre est **activé**, **Autoriser le partage de connexion** doit également être défini sur **Activé**.
- **Autoriser les MMS entrants :** autorise les utilisateurs à recevoir des messages MMS. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Autoriser les MMS sortants :** autorise les utilisateurs à envoyer des messages MMS. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Autoriser les SMS entrants :** autorise les utilisateurs à recevoir des messages texte. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Autoriser les SMS sortants :** autorise les utilisateurs à envoyer des messages texte. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser les SMS**.
- **Configurer réseaux mobiles :** permet aux utilisateurs d'utiliser leurs données cellulaires. La valeur par défaut est **Off**.
- **Limite par jour (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque jour. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Limite par semaine (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque semaine. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Limite par mois (Mo) :** entrez le volume de données mobiles, en Mo, que les utilisateurs peuvent utiliser chaque mois. La valeur par défaut est 0, ce qui désactive cette fonctionnalité (MDM 4.0 et versions ultérieures).
- **Autoriser uniquement les connexions VPN sécurisées :** autorise les utilisateurs à uniquement utiliser des connexions sécurisées (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**.
- **Autoriser l'enregistrement audio :** autorise les utilisateurs à effectuer des enregistrements audio avec leurs appareils (MDM 4.0 et versions ultérieures). La valeur par défaut est **Activé**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser le microphone**.
- **Autoriser l'enregistrement vidéo :** autorise les utilisateurs à effectuer des enregistrements vidéo avec leurs appareils (MDM 4.0 et versions ultérieures). La valeur par

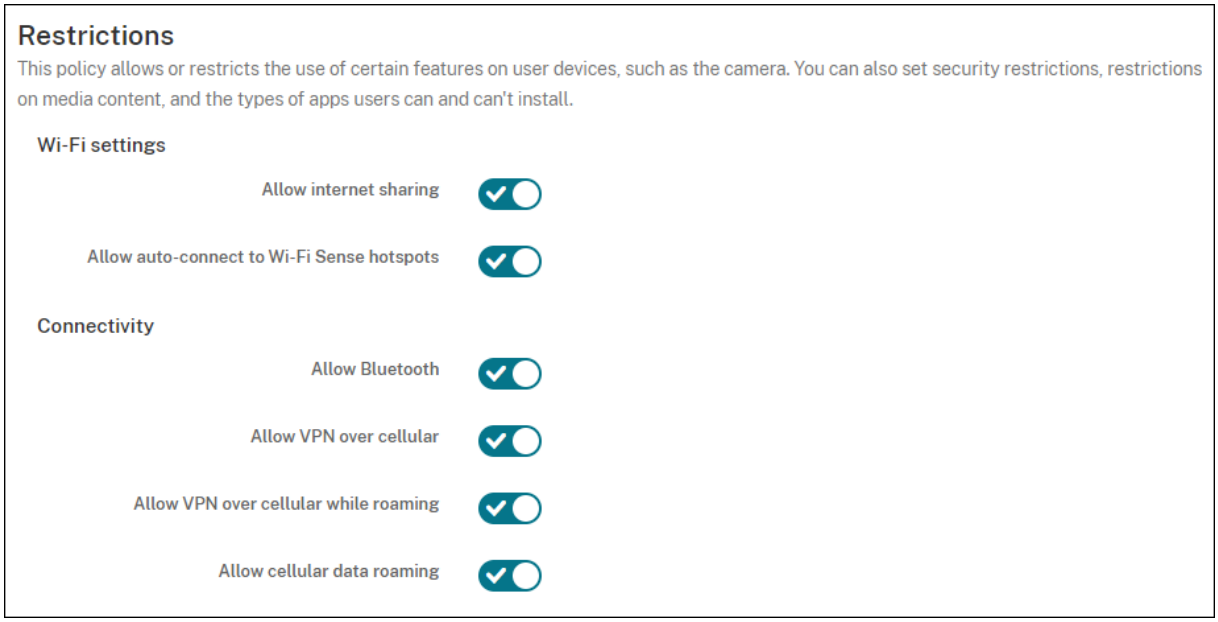
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser l'utilisation de l'appareil photo**.

- **Autoriser messages push en itinérance :** autorise les utilisateurs à utiliser des données cellulaires pour la transmission. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser itinérance des données**.
- **Autoriser synchronisation automatique en itinérance :** autorise les utilisateurs à utiliser les données cellulaires pour la synchronisation. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser itinérance des données**.
- **Autoriser appels vocaux en itinérance :** autorise les utilisateurs à utiliser des données cellulaires pour les appels vocaux. La valeur par défaut est **Off**. Si le paramètre est **activé**, vous devez activer le paramètre **Autoriser itinérance des données**.

- **Samsung : appareil entièrement géré**
  - **Activer la vérification de révocation :** active la vérification des listes de certificats révoqués. La valeur par défaut est **Off**.

Paramètres Windows Desktop/Tablet



- **Paramètres Wi-Fi**
  - **Autoriser le partage Internet :** autorise un appareil à partager sa connexion Internet avec d'autres appareils en le transformant en point d'accès Wi-Fi.

- **Connectivité**
  - **Autoriser le bluetooth :** autorise l'appareil à se connecter via Bluetooth.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Autoriser les connexions VPN via réseau cellulaire :** autorise l'appareil à se connecter à un réseau cellulaire via un VPN.
  - **Autoriser les connexions VPN via réseau cellulaire en itinérance :** autorise l'appareil à se connecter au VPN lorsque l'appareil est en itinérance sur les réseaux cellulaires.
  - **Autoriser les données cellulaires itinérantes :** autorise les utilisateurs à utiliser les données cellulaires en itinérance.

- **Comptes**
  - **Autoriser la connexion au compte Microsoft :** autorise l'appareil à utiliser un compte Microsoft pour l'authentification et les services de connexion sans relation avec la messagerie électronique.
  - **Autoriser les adresses e-mail non-Microsoft :** autoriser l'utilisateur à ajouter des comptes de messagerie autres que Microsoft.

- **System**
  - **Autoriser les cartes de stockage :** autorise l'appareil à utiliser une carte de stockage.
  - **Télémétrie :** dans la liste, cliquez sur une option pour autoriser l'appareil à envoyer des informations de télémétrie ou pour le lui interdire. La valeur par défaut est **Autorisée**. Les autres options sont **Non autorisée** et **Autorisée, à l'exception des demandes de données secondaires**.
  - **Autoriser l'accès de l'application au service de localisation :** autorise l'application à accéder aux services de localisation.
  - **Autoriser aperçu des versions internes :** autorise les utilisateurs à afficher un aperçu des versions internes de Microsoft.

- **Appareil photo :** Windows Desktop/Tablet uniquement
  - **Autoriser l'utilisation de l'appareil photo :** autorise les utilisateurs à utiliser l'appareil photo de leur appareil.

- **Bluetooth :** Windows Desktop/Tablet uniquement
  - **Autoriser le mode de découverte :** autoriser les périphériques Bluetooth à trouver le périphérique local.
  - **Nom de l'appareil local :** un nom pour le périphérique local.

- **Expérience :** Windows Desktop/Tablet uniquement
  - **Autoriser Cortana :** autorise les utilisateurs à accéder à Cortana, l'assistant personnel intelligent et navigateur de connaissances.
  - **Autoriser la détection d'appareils :** autoriser la détection réseau de l'appareil.
  - **Autoriser la désinscription MDM manuelle :** autorise les utilisateurs à désinscrire manuellement leurs appareils à partir de Citrix Endpoint Management MDM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Autoriser synchronisation des paramètres de l'appareil :** autorise les utilisateurs à synchroniser les paramètres entre des appareils Windows 10 et Windows 11 lors de l'itinérance.

- **Au dessus de l'écran de verrouillage :** Windows Desktop/Tablet uniquement
  - **Autoriser les notifications toast sur l'écran de verrouillage :** autorise les notifications toast sur l'écran de verrouillage. Windows Desktop/Tablet uniquement

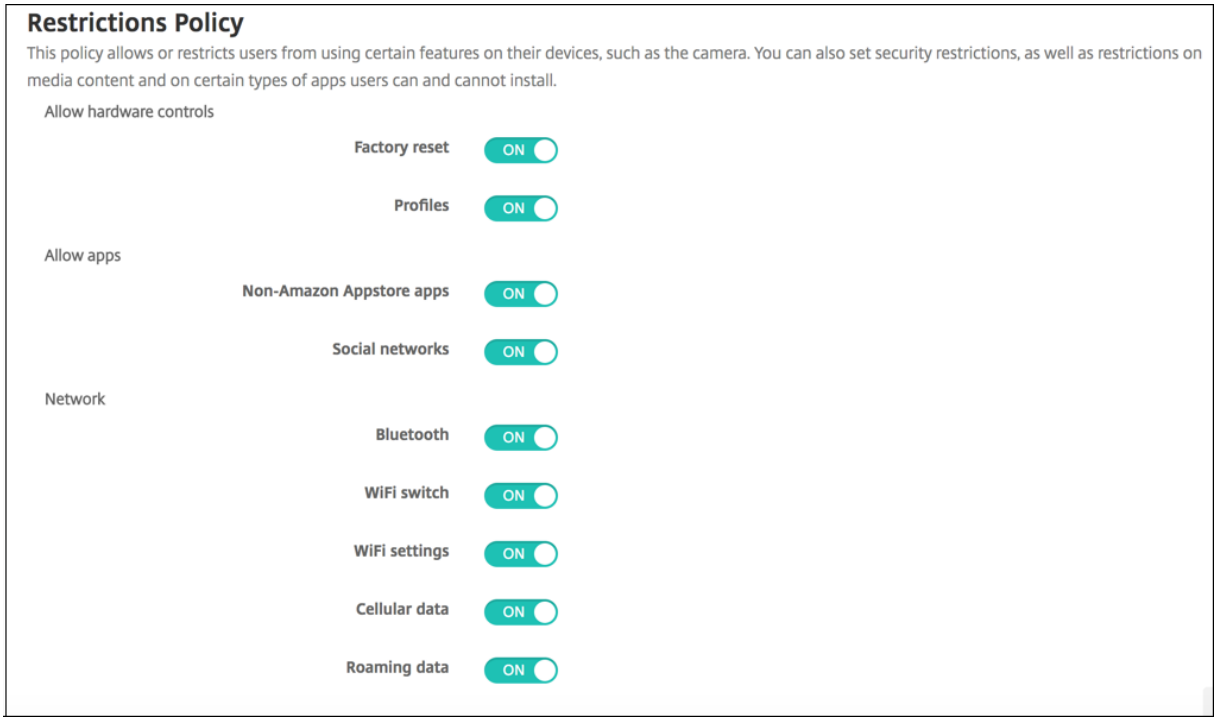
- **Applications**
  - **Autoriser les mises à jour automatiques depuis l'App Store :** autorise les applications de l'App Store à se mettre à jour automatiquement. Windows Desktop/Tablet uniquement.

- **Confidentialité :** Windows Desktop/Tablet uniquement
  - **Autoriser personnalisation de la saisie :** permet l'exécution du service de personnalisation de la saisie. Le service de personnalisation de la saisie améliore les entrées prédictives telles que le stylet et le clavier tactile en fonction de la saisie d'un utilisateur.

- **Paramètres :** Windows Desktop/Tablet uniquement.
  - **Autoriser lecture automatique :** permet aux utilisateurs de modifier les paramètres de lecture automatique.
  - **Autoriser assistant Données :** permet aux utilisateurs de modifier les paramètres de l'assistant Données.
  - **Autoriser date et heure :** permet aux utilisateurs de modifier les paramètres de date et d'heure.
  - **Autoriser langue :** permet aux utilisateurs de modifier les paramètres de langue.
  - **Autoriser mise sous tension/mise en veille :** permet aux utilisateurs de modifier les paramètres de mise sous tension et de mise en veille.
  - **Autoriser région :** permet aux utilisateurs de modifier les paramètres de région.
  - **Autoriser options de connexion :** permet aux utilisateurs de modifier les paramètres de connexion.
  - **Autoriser espace de travail :** permet aux utilisateurs de modifier les paramètres de l'espace de travail.
  - **Autoriser votre compte :** permet aux utilisateurs de modifier les paramètres de compte.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Amazon



- **Autoriser le contrôle du matériel**
  - **Réinitialisation d'usine :** autorise les utilisateurs à effectuer une réinitialisation d'usine sur leurs appareils.
  - **Profils :** autorise les utilisateurs à modifier le profil matériel sur leurs appareils.
- **Autoriser les applications**
  - **Applications non Amazon Appstore :** autorise les utilisateurs à installer des applications n'appartenant pas à l'Appstore Amazon sur leurs appareils.
  - **Réseaux sociaux :** autorise les utilisateurs à accéder à des réseaux sociaux à partir de leurs appareils.
- **Réseau**
  - **Bluetooth :** autorise les utilisateurs à utiliser Bluetooth.
  - **Commutateur Wi-Fi :** autorise les applications à modifier l'état de connectivité Wi-Fi.
  - **Paramètres Wi-Fi :** autorise les utilisateurs à modifier les paramètres Wi-Fi.
  - **Configurer réseaux mobiles :** autorise les utilisateurs à utiliser leurs données cellulaires.
  - **Données en itinérance :** autorise les utilisateurs à utiliser des données cellulaires en itinérance.
  - **Services de localisation :** autorise les utilisateurs à utiliser le GPS.
- **Actions USB :**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Débogage :** autorise les utilisateurs à se connecter à un ordinateur via USB à des fins de débogage.

Stratégie d'itinérance

November 29, 2023

Vous pouvez ajouter une stratégie d'itinérance dans Citrix Endpoint Management afin d'activer les services de voix et de données en itinérance sur des appareils iOS pris en charge. Lorsque l'itinérance de la voix est désactivée, l'itinérance des données est automatiquement désactivée.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Désactiver l'itinérance de la voix :** sélectionnez cette option pour désactiver l'itinérance vocale. Lorsque cette option est activée, l'itinérance des données est automatiquement désactivée. La valeur par défaut est **Désactivé**, ce qui active l'itinérance de la voix.
- **Désactiver l'itinérance des données :** sélectionnez cette option pour désactiver l'itinérance des données. Cette option est disponible uniquement lorsque l'itinérance de la voix est activée. La valeur par défaut est **Désactivé**, ce qui active l'itinérance des données.

Stratégie SCEP

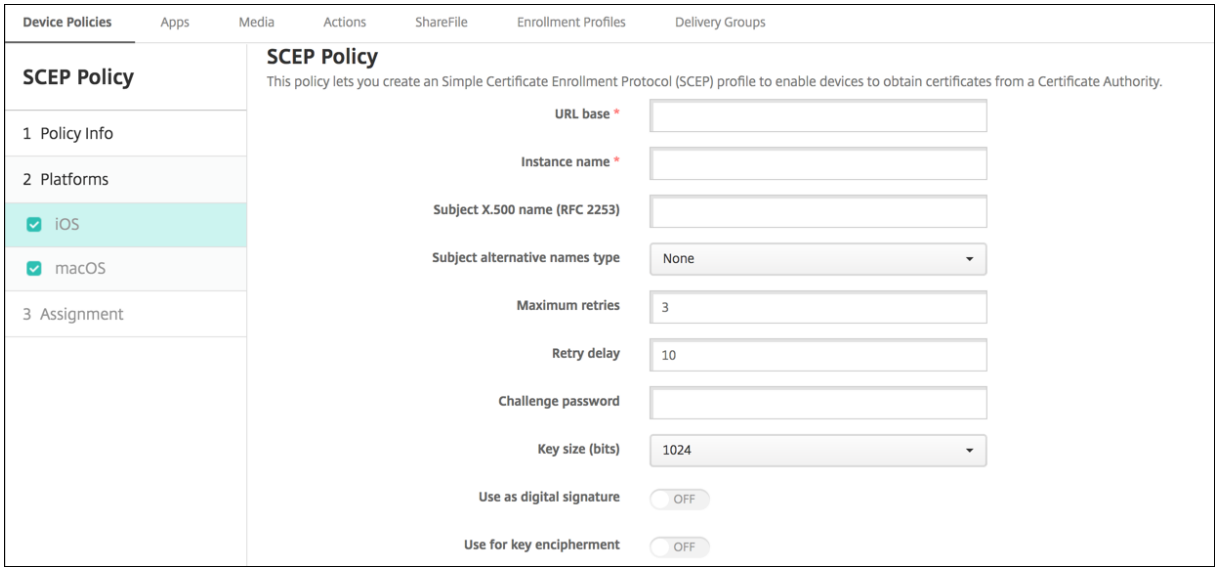
November 29, 2023

Cette stratégie vous permet de configurer des appareils iOS et macOS afin de récupérer un certificat à l'aide du protocole d'inscription du certificat simple (SCEP) à partir d'un serveur SCEP externe. Pour mettre à disposition un certificat sur l'appareil à l'aide du protocole SCEP à partir d'une PKI connectée à Citrix Endpoint Management, créez une entité PKI et un fournisseur PKI en mode distribué. Pour plus d'informations, veuillez consulter la section Entités PKI.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres iOS



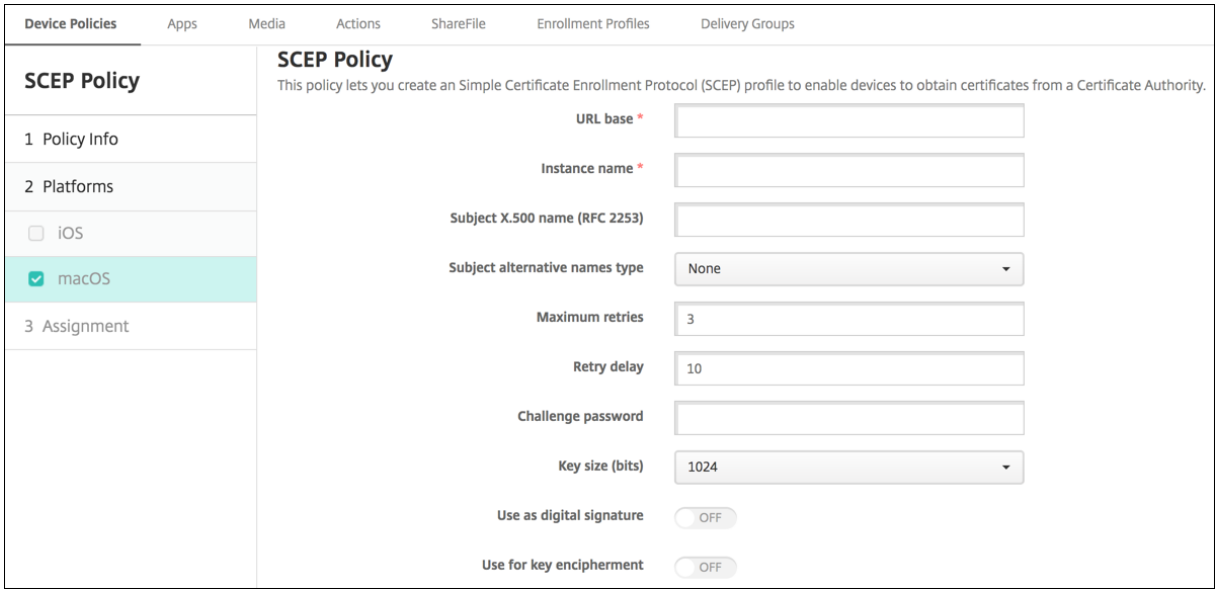
- **URL de base :** entrez l'adresse du serveur SCEP afin de définir où les demandes SCEP sont envoyées, par HTTP ou HTTPS. La clé privée n'est pas envoyée avec la demande de signature de certificat (CSR) ; il est donc possible d'envoyer la demande non chiffrée sans danger. Si le mot de passe à usage unique est configuré pour être réutilisé, utilisez HTTPS pour protéger le mot de passe. Cette étape est requise.
- **Nom d'instance :** entrez une chaîne reconnue par le serveur SCEP. Par exemple, il peut s'agir d'un nom de domaine comme exemple.org. Si une autorité de certification dispose de plusieurs certificats d'autorité de certification, vous pouvez utiliser ce champ pour différencier le domaine requis. Cette étape est requise.
- **Nom X.500 du sujet (RFC 2253) :** entrez la représentation d'un nom X.500 sous forme de tableau d'identificateurs d'objets (OID) et de valeurs. Par exemple, `/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar`, qui se traduit par `[ [ ["C", "US"] ], [ ["O", "Apple Inc."] ], …, [ ["1.2.5.3", "bar" ] ] ]`. Les OID peuvent être représentés en tant que nombres en pointillé, avec des raccourcis pour le pays (C), la ville (L), l'état (ST), l'organisation (O), l'unité d'organisation (OU) et le nom commun (CN).
- **Type de noms de sujet alternatifs :** sélectionnez un type de nom alternatif. Un type de nom alternatif facultatif fournit les valeurs requises par l'autorité de certification pour l'émission d'un certificat. Vous pouvez spécifier **Aucun**, **Nom RFC 822**, **Nom DNS** ou **URI**.
- **Nombre maximal de tentatives :** entrez le nombre de fois qu'un appareil doit réessayer lorsque le serveur SCEP envoie une réponse PENDING. La valeur par défaut est **3**.
- **Délai entre chaque tentative :** entrez le nombre de secondes entre les tentatives. La première tentative est effectuée sans délai. La valeur par défaut est **10**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Vérifier le mot de passe :** entrez un secret pré-partagé.
- **Taille de la clé (bits) :** sélectionnez **2048** ou une taille en bits plus élevée pour la clé.
- **Utiliser une signature numérique :** spécifiez si vous souhaitez utiliser le certificat en tant que signature numérique. Le serveur SCEP vérifie l'utilisation du certificat en tant que signature numérique avant d'utiliser la clé publique pour déchiffrer le hachage.
- **Utiliser pour le chiffrement des clés :** spécifiez si vous souhaitez utiliser le certificat pour le chiffrement des clés. Un serveur vérifie d'abord si le certificat fourni par un client est autorisé pour le chiffrement des clés. Le serveur utilise ensuite la clé publique dans un certificat pour vérifier qu'un élément de données a été crypté à l'aide de la clé privée. Sinon, l'opération échoue.
- **Empreinte digitale SHA-256 (chaîne hexadécimale) :** si votre autorité de certification utilise le protocole HTTP, utilisez ce champ pour fournir l'empreinte digitale du certificat CA. The device uses the fingerprint to confirm the authenticity of the CA response during enrollment. Vous pouvez fournir une empreinte digitale SHA-256, ou vous pouvez sélectionner un certificat pour importer sa signature.
- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres macOS



- **URL de base :** entrez l'adresse du serveur SCEP afin de définir où les demandes SCEP sont envoyées, par HTTP ou HTTPS. La clé privée n'est pas envoyée avec la demande de signature de certificat (CSR) ; il est donc possible d'envoyer la demande non chiffrée sans danger. Si le mot de passe à usage unique est configuré pour être réutilisé, utilisez HTTPS pour protéger le mot de passe. Cette étape est requise.
- **Nom d'instance :** entrez une chaîne reconnue par le serveur SCEP. Par exemple, il peut s'agir d'un nom de domaine comme exemple.org. Si une autorité de certification dispose de plusieurs certificats d'autorité de certification, vous pouvez utiliser ce champ pour différencier le domaine requis. Cette étape est requise.
- **Nom X.500 du sujet (RFC 2253) :** entrez la représentation d'un nom X.500 sous forme de tableau d'identificateurs d'objets (OID) et de valeurs. Par exemple, `/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar`, qui se traduit par `[ [ ["C", "US"] ], [ ["O", "Apple Inc."] ], ..., [ ["1.2.5.3", "bar" ] ] ]`. Les OID peuvent être représentés en tant que nombres en pointillé, avec des raccourcis pour le pays (C), la ville (L), l'état (ST), l'organisation (O), l'unité d'organisation (OU) et le nom commun (CN).
- **Type de noms de sujet alternatifs :** sélectionnez un type de nom alternatif. Un type de nom alternatif facultatif fournit les valeurs requises par l'autorité de certification pour l'émission d'un certificat. Vous pouvez spécifier **Aucun**, **Nom RFC 822**, **Nom DNS** ou **URI**.
- **Nombre maximal de tentatives :** entrez le nombre de fois qu'un appareil doit réessayer lorsque le serveur SCEP envoie une réponse PENDING. La valeur par défaut est **3**.
- **Délai entre chaque tentative :** entrez le nombre de secondes entre les tentatives. La première tentative est effectuée sans délai. La valeur par défaut est **10**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Vérifier le mot de passe :** entrez un secret pré-partagé.
- **Taille de la clé (bits) :** sélectionnez **2048** ou une taille en bits plus élevée pour la clé.
- **Utiliser une signature numérique :** spécifiez si vous souhaitez utiliser le certificat en tant que signature numérique. Le serveur SCEP vérifie l'utilisation du certificat en tant que signature numérique avant d'utiliser la clé publique pour déchiffrer le hachage.
- **Utiliser pour le chiffrement des clés :** spécifiez si vous souhaitez utiliser le certificat pour le chiffrement des clés. Un serveur vérifie d'abord si le certificat fourni par un client est autorisé pour le chiffrement des clés. Le serveur utilise ensuite la clé publique dans un certificat pour vérifier qu'un élément de données a été crypté à l'aide de la clé privée. Sinon, l'opération échoue.
- **Empreinte digitale SHA-256 (chaîne hexadécimale) :** si votre autorité de certification utilise le protocole HTTP, utilisez ce champ pour fournir l'empreinte digitale du certificat CA. The device uses the fingerprint to confirm the authenticity of the CA response during enrollment. Vous pouvez fournir une empreinte digitale SHA-256, ou vous pouvez sélectionner un certificat pour importer sa signature.
- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

Stratégies de dictée et Siri

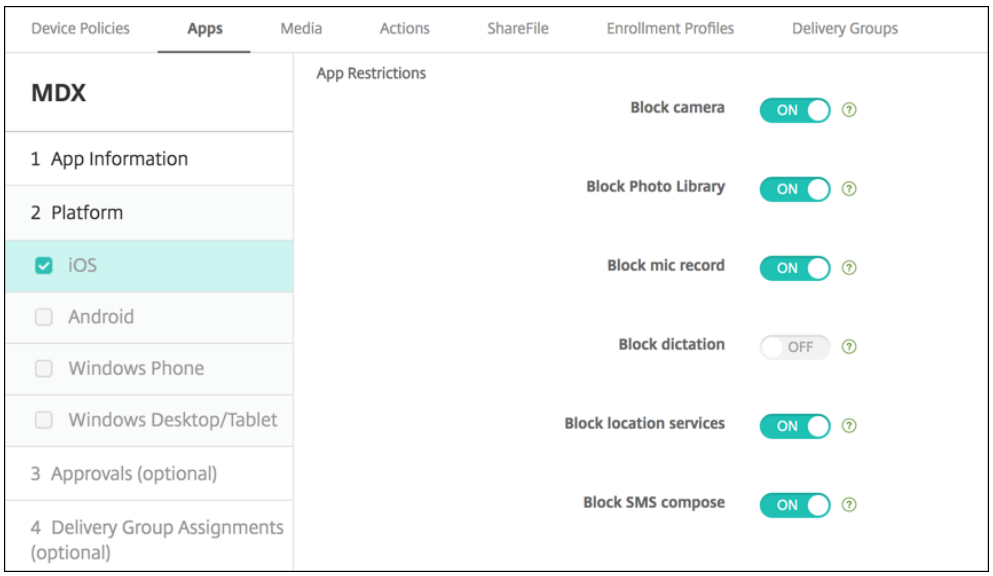
November 29, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Lorsque les utilisateurs posent une question à Siri ou qu'ils dictent du texte sur des appareils iOS gérés, Apple collecte les données vocales à des fins d'amélioration de Siri. Les données vocales transitent via les services de cloud d'Apple et par conséquent elles existent en dehors du conteneur Citrix Endpoint Management sécurisé. Le texte qui résulte de la dictée vocale reste toutefois dans le conteneur.

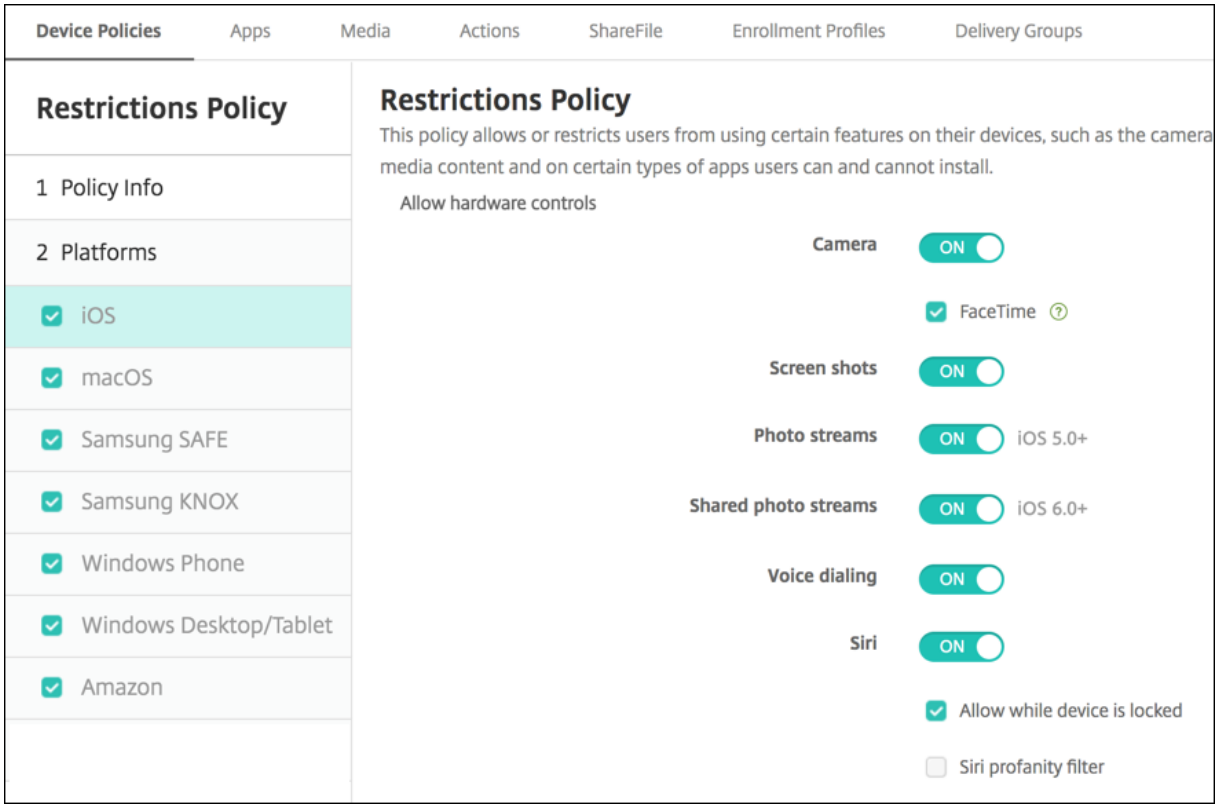
Citrix Endpoint Management vous permet de bloquer Siri et les services de dictée, selon vos besoins en matière de sécurité.

Dans les déploiements MAM, la stratégie **Bloquer la dictée** est **activée** par défaut pour chaque application, ce qui désactive le micro de l'appareil. Définissez la valeur sur **Désactivé** si vous souhaitez autoriser la dictée. Vous pouvez trouver la stratégie dans la console Citrix Endpoint Management sous **Configurer > Applications**. Sélectionnez l'application, cliquez sur **Modifier**, puis cliquez sur **iOS**.



Dans les déploiements MDM, vous pouvez également désactiver Siri avec la stratégie Siri sous **Configurer > Stratégies d'appareil**. L'utilisation de Siri est autorisée par défaut.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Quelques points à considérer lorsque vous choisissez d'autoriser Siri et la dictée :

- D'après les informations rendues publiques par Apple, Apple conserve les données des clips vocaux de la dictée et de Siri pendant un maximum de deux années. Pour représenter l'utilisateur, un nombre aléatoire est attribué aux données et les fichiers vocaux sont associés à ce nombre aléatoire.
- Vous pouvez vérifier la déclaration de confidentialité d'Apple en accédant à **Réglages > Général > Claviers** sur un appareil iOS et en touchant le lien sous **Activer dictée**.

Stratégie de compte SSO

November 29, 2023

La stratégie Compte SSO vous permet de créer des comptes Single Sign-On (authentification unique) dans Citrix Endpoint Management. Ces comptes permettent aux utilisateurs de s'authentifier une seule fois pour accéder à Citrix Endpoint Management et à vos ressources d'entreprise internes à partir de différentes applications. Les utilisateurs n'ont pas à stocker d'informations d'identification sur l'appareil. Les informations d'identification utilisateur d'entreprise du compte SSO sont utilisées pour toutes les applications, y compris les applications provenant de l'App Store. Cette stratégie est conçue pour fonctionner avec l'authentification Kerberos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Nom du compte :** entrez le nom du compte SSO Kerberos qui s'affiche sur les appareils des utilisateurs. Ce champ est obligatoire.
- **Nom principal Kerberos :** entrez le nom principal Kerberos. Ce champ est obligatoire.
- **Infos d'identification de l'identité (infos d'identification magasin de clés ou PKI) :** dans la liste, cliquez sur des infos d'identification de l'identité qui peuvent être utilisées pour renouveler les infos d'identification Kerberos sans intervention de l'utilisateur.
- **Domaine Kerberos :** entrez le domaine Kerberos pour cette stratégie. Il s'agit généralement de votre nom de domaine en lettres majuscules (par exemple, EXAMPLE.COM). Ce champ est obligatoire.
- **URL autorisées :** pour chaque adresse URL pour laquelle vous souhaitez demander l'authentification unique (SSO), cliquez sur **Ajouter**, puis procédez comme suit :
  - **URL autorisée :** entrez une adresse URL pour laquelle vous souhaitez demander l'authentification unique (SSO) lorsqu'un utilisateur visite l'URL à partir d'un appareil iOS.

    Par exemple, lorsqu'un utilisateur tente d'accéder à un site dans Safari et que le site Web lance une demande d'authentification Kerberos, si ce site ne figure pas dans la liste des URL, l'appareil iOS ne tentera pas une authentification unique en fournissant le jeton Kerberos qui a été mis en cache sur l'appareil lors d'une précédente ouverture de session Kerberos. La correspondance doit être exacte sur la partie hôte de l'URL. Par exemple, `https://shopping.apple.com` est valide, mais `https://*.apple.com` ne l'est pas.

    De même, si Kerberos n'est pas activé en fonction d'une correspondance à l'hôte, l'URL utilise un appel HTTP standard. Cela peut signifier presque tout, y compris un défi de mot de passe standard ou une erreur HTTP si l'URL est uniquement configurée pour l'authentification unique (SSO) à l'aide de Kerberos.
  - Cliquez sur **Ajouter** pour ajouter l'URL, ou cliquez sur **Annuler** pour annuler l'ajout de l'URL.
- **Identifiants application :** pour chaque application autorisée à utiliser cette connexion, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Identifiant app :** entrez un identifiant d'application pour une application qui est autorisée à utiliser cette connexion. si vous n'ajoutez aucun identifiant d'application, cette connexion correspond à **tous** les identifiants d'application.
- **Paramètre de stratégie**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
  * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Stratégie de magasin

November 29, 2023

Vous pouvez créer une stratégie dans Citrix Endpoint Management afin de spécifier si les appareils affichent un clip Web du magasin d'applications sur l'écran d'accueil.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS, Android, Windows Desktop/Tablet

Pour chaque plate-forme que vous configurez, sélectionnez si un clip Web du magasin d'applications apparaît sur les appareils des utilisateurs. La valeur par défaut est **On**.

Stratégie d'abonnements calendriers

November 29, 2023

Vous pouvez ajouter une stratégie d'appareil dans Citrix Endpoint Management afin d'ajouter un abonnement calendrier à la liste des calendriers sur les appareils iOS. La liste des calendriers publics auxquels vous pouvez vous abonner est disponible sur le site d'assistance Apple dans Téléchargements.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Conditions préalables

Vous devez être abonné à un calendrier avant de pouvoir l'ajouter à la liste des abonnements calendriers sur les appareils des utilisateurs.

Paramètres iOS

- **Description :** entrez une description pour le calendrier. Ce champ est obligatoire.
- **URL :** entrez l'URL du calendrier. Vous pouvez entrer une URL `webcal://` ou un lien `https://` vers un fichier iCalendar (.ics). Ce champ est obligatoire.
- **Nom d'utilisateur :** entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe :** entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL :** sélectionnez cette option si vous souhaitez utiliser une connexion SSL au calendrier. La valeur par défaut est **Off**.
- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Stratégie termes et conditions

November 29, 2023

Vous créez des stratégies de termes et conditions dans Citrix Endpoint Management lorsque vous souhaitez que les utilisateurs acceptent les stratégies spécifiques à votre entreprise qui régissent les connexions au réseau d'entreprise. Lorsque les utilisateurs inscrivent leurs appareils auprès de Citrix Endpoint Management, ils voient s'afficher les termes et conditions et doivent les accepter pour inscrire leurs appareils. Le refus des termes et conditions annule le processus d'inscription.

Vous pouvez créer différentes stratégies pour les termes et conditions dans différentes langues si votre société dispose d'utilisateurs internationaux pour leur permettre d'accepter les termes et conditions

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

dans leur langue maternelle. Vous devez fournir un fichier pour chaque combinaison de plate-forme et de langue que vous souhaitez déployer. Pour les appareils Android et iOS, vous devez fournir des fichiers PDF. Pour les appareils Windows, vous devez fournir des fichiers texte (.txt) et les fichiers image connexes.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS et Android

- **Fichier à importer :** sélectionnez le fichier de termes et conditions à importer en cliquant sur **Parcourir**, puis accédez à l'emplacement du fichier.
- **Termes et conditions par défaut :** sélectionnez cette option pour désigner ce fichier comme le document par défaut pour les utilisateurs qui sont membres de plusieurs groupes avec différents termes et conditions. La valeur par défaut est **Off**.

> **Remarque :**
>
> Les conditions générales ne s'affichent pas si un appareil iOS est inscrit via le programme d'inscription des appareils (DEP).

Paramètres Windows Tablet

- **Fichier à importer :** sélectionnez le fichier de termes et conditions à importer en cliquant sur **Parcourir**, puis accédez à l'emplacement du fichier.
- **Image :** sélectionnez le fichier à importer en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
- **Termes et conditions par défaut :** sélectionnez cette option pour désigner ce fichier comme le document par défaut pour les utilisateurs qui sont membres de plusieurs groupes avec différents termes et conditions. La valeur par défaut est **Off**.

Stratégie de tunnel

November 29, 2023

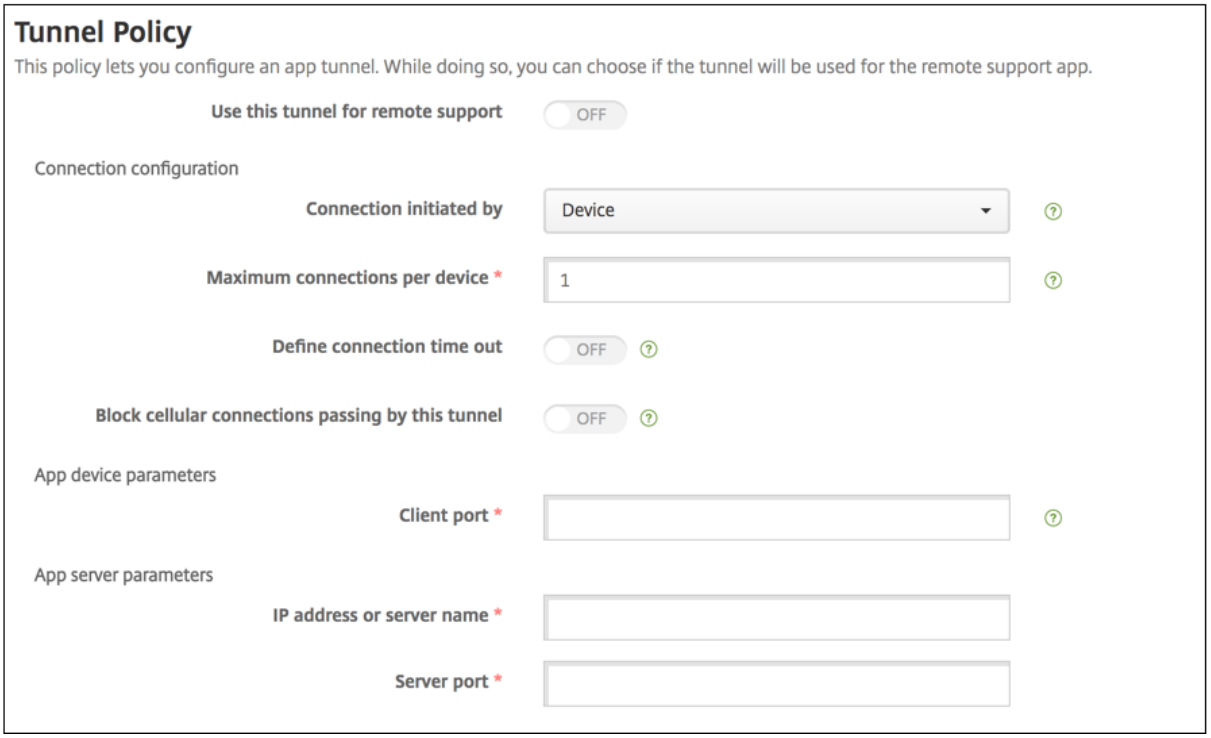
Les tunnels applicatifs sont conçus pour accroître la continuité du service et la fiabilité du transfert de données pour vos applications mobiles. Les tunnels applicatifs définissent les paramètres proxy entre le composant client de toute application d'appareil mobile et le composant de serveur d'applications. Vous pouvez configurer la stratégie de tunnel pour les appareils Android.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Tout trafic applicatif envoyé via un tunnel que vous définissez dans cette stratégie transite via Citrix Endpoint Management avant d'être redirigé vers le serveur exécutant l'application.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Android



- **Connexion initiée par :** cliquez sur **Appareil** ou **Serveur** pour spécifier la source lançant la connexion.
- **Connexions max. par appareil :** tapez un nombre pour définir le nombre de connexions TCP simultanées que l'application peut établir. Ce champ ne s'applique qu'aux connexions initiées par l'appareil.
- **Définir le délai d'expiration de la connexion :** sélectionnez cette option pour définir une durée pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
  - **Délai d'expiration de la connexion :** si vous définissez **Définir le délai d'expiration de la connexion** sur **Activé**, saisissez la durée en secondes pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
- **Bloquer les connexions cellulaires transitant par ce tunnel :** sélectionnez cette option pour spécifier si ce tunnel est bloqué en itinérance. Les connexions Wi-Fi et USB ne sont pas bloquées.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Port client :** entrez le numéro du port du client. Dans la plupart des cas, cette valeur est la même que celle du port serveur.
- **Adresse IP ou nom du serveur :** entrez l'adresse IP ou le nom du serveur applicatif. Ce champ ne s'applique qu'aux connexions initiées par l'appareil.
- **Port serveur :** entrez le numéro de port du serveur.

Stratégie VPN

March 1, 2024

La stratégie VPN configure les paramètres de réseau privé virtuel (VPN) permettant aux appareils de se connecter de manière sécurisée aux ressources d'entreprise. Vous pouvez configurer la stratégie VPN pour les plates-formes suivantes. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans cet article.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Configuration requise pour les réseaux Per App VPN

Vous configurez la fonctionnalité Per App VPN pour les plates-formes suivantes via des stratégies VPN :

- iOS
- macOS
- Android (ancien administrateur de l'appareil)

Pour Android Enterprise, utilisez la stratégie Configurations gérées pour configurer les profils VPN.

Des options Per App VPN sont disponibles pour certains types de connexion. Le tableau suivant indique quand les options Per App VPN sont disponibles.

Plateforme	Type de connexion	Remarque
iOS	Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix SSO ou SSL personnalisé	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Plateforme	Type de connexion	Remarque
macOS	Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA ou SSL personnalisé	
Android (ancien administrateur de l'appareil)	Citrix SSO	

Pour créer une stratégie Per App VPN pour les appareils iOS et Android (ancien administrateur de l'appareil) à l'aide de l'application Citrix SSO, vous devez effectuer des étapes supplémentaires, en plus de la configuration de stratégie VPN. En outre, vous devez vérifier que les conditions préalables suivantes sont remplies :

- NetScaler Gateway sur site
- Les applications suivantes sont installées sur l'appareil :
  - Citrix SSO
  - Citrix Secure Hub

Voici un workflow général pour configurer une stratégie Per App VPN pour les appareils iOS et Android à l'aide de l'application Citrix SSO :

1. Configurez la stratégie VPN selon les instructions de cet article.
   - Pour iOS, consultez la section Configurer le protocole Citrix SSO pour iOS. Après avoir configuré le protocole Citrix SSO pour iOS via une stratégie VPN, vous devez également créer une stratégie d'attributs d'application pour associer une application à la stratégie Per App VPN. Pour de plus amples informations, consultez la section Configurer une stratégie Per App VPN.
     - Pour le champ **Type d'authentification pour la connexion**, si vous sélectionnez **Certificat**, vous devez d'abord configurer l'authentification basée sur les certificats pour Citrix Endpoint Management. Consultez la section Authentification certificat client ou certificat + domaine.
   - Pour Android (administration anciens appareils), consultez la section Configurer le protocole Citrix SSO pour Android.
     - Pour le champ **Type d'authentification pour la connexion**, si vous sélectionnez **Certificat** ou **Mot de passe et certificat**, vous devez d'abord configurer l'authentification basée sur les certificats pour Citrix Endpoint Management. Consultez la section Authentification certificat client ou certificat + domaine.

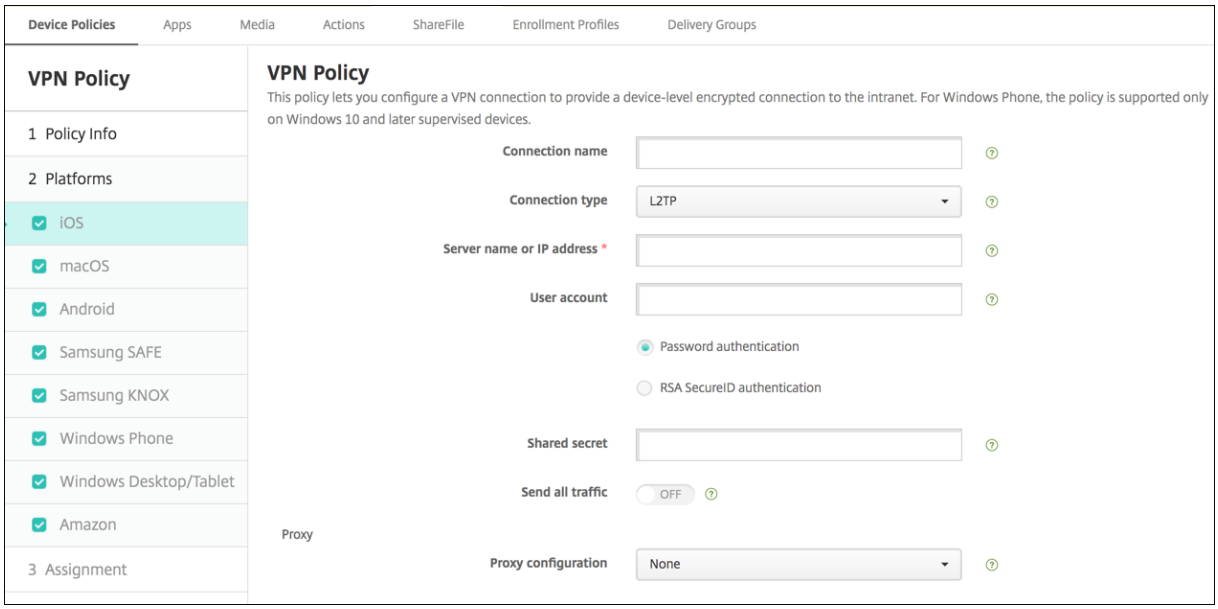
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Configurez Citrix ADC pour accepter le trafic provenant du réseau Per App VPN. Pour de plus amples informations, consultez la section Full VPN setup on NetScaler Gateway.

Paramètres iOS

Le type de connexion VPN Citrix dans la stratégie VPN pour iOS ne prend pas en charge iOS 12. Effectuez ces étapes pour supprimer votre stratégie VPN existante et créer une stratégie VPN avec le type de connexion Citrix SSO :

1. Supprimez votre stratégie VPN pour iOS.
2. Ajoutez une stratégie VPN pour iOS avec les paramètres suivants :
   - **Type de connexion : Citrix SSO**
   - **Activer Per App VPN : Activé**
   - **Type de fournisseur : Tunnel de paquet**
3. Ajoutez une stratégie d'attributs d'application pour iOS. Sous **Identifiant Per App VPN**, sélectionnez **iOS_VPN**.



- **Nom de la connexion :** entrez un nom pour la connexion.
- **Type de connexion :** dans la liste, sélectionnez le protocole à utiliser pour cette connexion. La valeur par défaut est **L2TP**.
  - **L2TP :** Layer 2 Tunneling Protocol avec authentification par clé pré-partagée.
  - **PPTP :** protocole PPTP.
  - **IPSec :** votre connexion VPN d'entreprise.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Cisco Legacy AnyConnect :** ce type de connexion requiert que le client Cisco Legacy AnyConnect VPN soit installé sur la machine utilisateur. Cisco élimine progressivement le client Cisco Legacy AnyConnect, basé sur une infrastructure VPN désormais obsolète.

  Pour utiliser le client Cisco AnyConnect actuel, utilisez un **Type de connexion** de **SSL personnalisé**. Pour plus d'informations sur les paramètres requis, consultez « Configurer le protocole SSL personnalisé » dans cette section.
- **Juniper SSL :** client Juniper Networks SSL VPN.
- **F5 SSL :** client F5 Networks SSL VPN.
- **SonicWALL Mobile Connect :** client VPN Dell unifié pour iOS.
- **Aruba VIA :** client Aruba Networks Virtual Internet Access.
- **IKEv2 (iOS uniquement) :** Internet Key Exchange version 2 pour iOS uniquement.
- **AlwaysOn IKEv2 :** accès Always On à l'aide de IKEv2.
- **Double configuration AlwaysOn IKEv2 :** accès Always On à l'aide de la double configuration iKEv2.
- **Citrix SSO:** Client Citrix SSO pour iOS 12 et versions ultérieures.
- **SSL personnalisé :** Secure Sockets Layer personnalisé. Ce type de connexion est requis pour le client Cisco AnyConnect disposant d'un bundle ID **com.cisco.anyconnect**. Réglez l'option **Nom de la connexion** sur **Cisco AnyConnect**. Vous pouvez également déployer la stratégie VPN et activer un filtre NAC (Network Access Control) pour les appareils iOS. Le filtre NAC bloque une connexion VPN pour les appareils sur lesquels des applications non conformes sont installées. La configuration nécessite des paramètres spécifiques pour la stratégie VPN d'iOS, comme décrit dans la section iOS suivante. Pour plus d'informations sur les autres paramètres requis pour activer le filtre NAC, voir Contrôle d'accès réseau.

Les sections suivantes répertorient les options de configuration pour chacun des types de connexion précédents.

Configurer le protocole L2TP pour iOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- Sélectionnez **Authentification par mot de passe** ou **Authentification RSA SecurID**.
- **Secret partagé :** entrez la clé de secret partagé IPsec.
- **Envoyer tout le trafic :** sélectionnez cette option pour envoyer tout le trafic via le VPN. La valeur par défaut est **Désactivé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer le protocole PPTP pour iOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- Sélectionnez **Authentification par mot de passe** ou **Authentification RSA SecurID**.
- **Niveau de chiffrement :** dans la liste, sélectionnez un niveau de chiffrement. La valeur par défaut est **Aucun**.
  - **Aucun :** le chiffrement n'est pas utilisé.
  - **Automatique :** utilise le niveau de chiffrement le plus élevé pris en charge par le serveur.
  - **Maximum (128 bits) :** utilise toujours le cryptage 128 bits.
- **Envoyer tout le trafic :** sélectionnez cette option pour envoyer tout le trafic via le VPN. La valeur par défaut est **Désactivé**.

Configurer le protocole IPsec pour iOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Secret partagé** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Secret partagé**.
- Si vous sélectionnez **Secret partagé**, configurez les paramètres suivants :
  - **Nom du groupe :** entrez un nom de groupe (facultatif).
  - **Secret partagé :** entrez une clé de secret partagé (facultatif).
  - **Utiliser une authentification hybride :** indiquez si vous souhaitez utiliser l'authentification hybride. Avec l'authentification hybride, le serveur s'authentifie auprès du client, puis le client s'authentifie auprès du serveur. La valeur par défaut est **Désactivé**.
  - **Demander le mot de passe :** indiquez si les utilisateurs doivent être invités à entrer leur mot de passe lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
- Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
  - **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
  - **Exiger PIN à la connexion :** sélectionnez cette option pour demander aux utilisateurs d'entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
  - **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**.
- **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
- **Domaines safari :** cliquez sur **Ajouter** pour ajouter un nom de domaine Safari.

Configurer le protocole Cisco Legacy AnyConnect pour iOS

Pour passer du client Cisco Legacy AnyConnect au nouveau client Cisco AnyConnect, utilisez le protocole SSL personnalisé.

- **Identificateur de bundle de fournisseur :** pour le client Legacy AnyConnect, le bundle ID est com.cisco.anyconnect.gui.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Groupe :** entrez un nom de groupe (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    - **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    - **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    - **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.
- **Inclure tous les réseaux :** sélectionnez si vous souhaitez autoriser tous les réseaux à utiliser cette connexion. La valeur par défaut est **Désactivé**.
- **Exclure les réseaux locaux :** sélectionnez si vous souhaitez exclure les réseaux locaux de l'utilisation de la connexion ou autoriser les réseaux. La valeur par défaut est **Désactivé**.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  - **Type de fournisseur :** indiquez si le VPN par application est fourni en tant que **Proxy d'application** ou **Tunnel de paquet**. La valeur par défaut est **Proxy d'application**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole SSL Juniper pour iOS

- **Identificateur de bundle de fournisseur :** si votre profil VPN par application contient l'identificateur de bundle d'une application avec plusieurs fournisseurs VPN du même type, spécifiez le fournisseur à utiliser ici.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Domaine :** entrez un nom de domaine (facultatif).
- **Rôle :** entrez un nom de rôle (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  - **Type de fournisseur :** indiquez si le VPN par application est fourni en tant que **Proxy d'application** ou **Tunnel de paquet**. La valeur par défaut est **Proxy d'application**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole F5 SSL pour iOS

- **Identificateur de bundle de fournisseur :** si votre profil VPN par application contient l'identificateur de bundle d'une application avec plusieurs fournisseurs VPN du même type, spécifiez le fournisseur à utiliser ici.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Type de fournisseur :** indiquez si le VPN par application est fourni en tant que **Proxy d'application** ou **Tunnel de paquet**. La valeur par défaut est **Proxy d'application**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole SonicWALL pour iOS

- **Identificateur de bundle de fournisseur :** si votre profil VPN par application contient l'identificateur de bundle d'une application avec plusieurs fournisseurs VPN du même type, spécifiez le fournisseur à utiliser ici.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Groupe ou domaine de connexion :** entrez un groupe ou domaine de connexion (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous définissez cette option sur Activé, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau.
  - **Type de fournisseur :** indiquez si le VPN par application est fourni en tant que **Proxy d'application** ou **Tunnel de paquet**. La valeur par défaut est **Proxy d'application**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole Ariba VIA pour iOS

- **Identificateur de bundle de fournisseur :** si votre profil VPN par application contient l'identificateur de bundle d'une application avec plusieurs fournisseurs VPN du même type, spécifiez le fournisseur à utiliser ici.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer les protocoles IKEv2 pour iOS

Cette section contient les paramètres utilisés pour les protocoles IKEv2, AlwaysOn IKEv2 et Double configuration AlwaysOn IKEv2. Pour le protocole Double configuration AlwaysOn IKEv2, configurez tous ces paramètres pour les réseaux cellulaires et Wi-Fi.

- **Autoriser l'utilisateur à désactiver la connexion automatique :** pour les protocoles AlwaysOn. Indiquez si vous souhaitez permettre aux utilisateurs de désactiver la connexion automatique au réseau sur leurs appareils. La valeur par défaut est **Désactivé**.
- **Nom d'hôte ou adresse IP du serveur :** entrez le nom ou l'adresse IP du serveur VPN.
- **Identifiant local :** nom de domaine complet ou adresse IP du client IKEv2. Ce champ est obligatoire.
- **Identifiant distant :** nom de domaine complet ou adresse IP du serveur VPN. Ce champ est obligatoire.
- **Authentification de l'appareil :** choisissez **Secret partagé**, **Certificat** ou **Certificat d'appareil basé sur l'identité de l'appareil** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Secret partagé**.
  - Si vous choisissez **Secret partagé**, entrez une clé de secret partagé (facultatif).
  - Si vous choisissez **Certificat**, choisissez les **Infos d'identification** de l'identité à utiliser. La valeur par défaut est **Aucun**.
  - Si vous choisissez **Certificat d'appareil basé sur l'identité de l'appareil**, choisissez le **type d'identité de l'appareil** à utiliser. La valeur par défaut est **IMEI**. Pour utiliser cette option, importez des certificats de façon groupée à l'aide de l'API REST. Consultez la section Effectuer un chargement groupé de certificats avec l'API REST. Disponible uniquement lorsque vous sélectionnez **Toujours sur IKEv2**.
- **Authentification étendue activée :** indiquez si vous souhaitez activer le protocole d'authentification étendue (EAP). Si vous choisissez **Activé**, tapez le **compte d'utilisateur** et le **mot de passe d'authentification**.
- **Intervalle DPD :** choisissez la fréquence à laquelle un appareil homologue est contacté pour vous assurer qu'il reste accessible. La valeur par défaut est **Aucun**. Les options sont les suivantes :
  - **Aucun :** désactive DPD.
  - **Faible :** contacte l'homologue toutes les 30 minutes.
  - **Moyen :** contacte l'homologue toutes les 10 minutes.
  - **Élevé :** contacte l'homologue toutes les minutes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Désactiver la mobilité et le multihoming :** sélectionnez cette option pour désactiver cette fonctionnalité.
- **Utilisez les attributs du sous-réseau interne IPv4/IPv6 :** choisissez si vous souhaitez activer cette fonctionnalité.
- **Désactiver les redirections :** choisissez si vous souhaitez désactiver les redirections.
- **Activer procédure de secours :** si cette option est activée, ce paramètre permet à un tunnel de transporter le trafic admissible à l'assistance Wi-Fi sur des données cellulaires et nécessite un VPN. La valeur par défaut est **Off**.
- **Activer Keepalive NAT lorsque l'appareil est en veille :** pour les protocoles AlwaysOn. Les paquets Keepalive maintiennent les mappages NAT pour les connexions IKEv2. La puce envoie ces paquets à intervalle régulier lorsque l'appareil est éveillé. Si ce paramètre est On, la puce envoie des paquets Keepalive même lorsque l'appareil est en veille. L'intervalle par défaut est de 20 secondes via Wi-Fi et de 110 secondes via réseau cellulaire. Vous pouvez modifier l'intervalle en utilisant le paramètre Intervalle Keepalive NAT.
- **Intervalle Keepalive NAT (secondes) :** la valeur par défaut est de 20 secondes.
- **Activer PFS (Perfect Forward Secrecy) :** choisissez si vous souhaitez activer cette fonctionnalité.
- **Adresses IP des serveurs DNS :** facultatif. Une liste des chaînes d'adresses IP du serveur DNS. Ces adresses IP peuvent inclure un mélange d'adresses IPv4 et IPv6. Cliquez sur **Ajouter** pour saisir une adresse.
- **Nom de domaine :** facultatif. Domaine principal du tunnel.
- **Domaines de recherche :** facultatif. Liste de chaînes de domaines utilisés pour donner des noms d'hôte complets uniques.
- **Ajouter des domaines de correspondance supplémentaires à la liste de résolution :** facultatif. Détermine si les domaines figurant dans la liste des domaines correspondants supplémentaires doivent être ajoutés à la liste des domaines de recherche pour la résolution. La valeur par défaut est **Activé**.
- **Domaines correspondant supplémentaires :** facultatif. Liste des chaînes de domaines utilisés pour déterminer les requêtes DNS qui devront utiliser les paramètres de résolution DNS contenus dans les adresses de serveur DNS. Cette clé crée une configuration split DNS où uniquement les hôtes de certains domaines sont résolus à l'aide de la résolution DNS du tunnel. Les hôtes ne se trouvant pas dans l'un des domaines de cette liste sont résolus à l'aide de la résolution par défaut du système.

Si ce paramètre contient une chaîne vide, cette chaîne est utilisée en tant que domaine par défaut. Cette solution permet à une configuration de split-tunnel de diriger toutes les requêtes DNS vers les

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

serveurs de VPN DNS avant les serveurs DNS principaux. Si le tunnel VPN est l'itinéraire par défaut du réseau, les serveurs DNS répertoriés deviennent la résolution par défaut. Dans ce cas, la liste des domaines correspondants supplémentaires est ignorée.

- **Paramètres IKE SA** et **Paramètres SA enfants** : configurez ces paramètres pour chaque option d'association de sécurité (SA) :
  - **Algorithme de chiffrement :** dans la liste, sélectionnez l'algorithme de chiffrement IKE à utiliser. La valeur par défaut est **3DES**.
  - **Algorithme d'intégrité :** dans la liste, sélectionnez l'algorithme d'intégrité à utiliser. La valeur par défaut est **SHA-256**.
  - **Groupe Diffie Hellman :** dans la liste, sélectionnez le numéro du groupe Diffie Hellman. La valeur par défaut est **2**.
  - **Durée de vie d'IKE en minutes :** entrez un nombre entier compris entre 10 et 1440 représentant la durée de vie SA (rekey interval). La valeur par défaut est **1440** minutes.
- **Exceptions de service :** pour les protocoles AlwaysOn. Les exceptions de service sont des services du système auxquels n'est pas appliquée l'option VPN toujours connecté. Configurez ces paramètres d'exceptions de service :
  - **Messagerie vocale :** dans la liste, sélectionnez la façon dont l'exception des messages vocaux est traitée. La valeur par défaut est **Autoriser le trafic via le tunnel**.
  - **AirPrint :** dans la liste, sélectionnez la façon dont l'exception AirPrint est traitée. La valeur par défaut est **Autoriser le trafic via le tunnel**.
  - **Autoriser le trafic en provenance de websheets captifs en dehors du tunnel VPN :** sélectionnez cette option pour autoriser les utilisateurs à se connecter à des points d'accès en dehors du tunnel VPN. La valeur par défaut est **Désactivé**.
  - **Autoriser le trafic en provenance de toutes les applications de réseaux captifs en dehors du tunnel VPN :** sélectionnez cette option pour autoriser toutes les applications de réseau de point d'accès en dehors du tunnel VPN. La valeur par défaut est **Désactivé**.
  - **Bundle ID d'applications de réseaux captifs :** pour chaque identificateur de bundle d'applications de réseau auquel les utilisateurs sont autorisés à accéder, cliquez sur **Ajouter** et entrez le **bundle ID** de réseau de point d'accès. Cliquez sur **Enregistrer** pour enregistrer le bundle ID d'application.
- **Per App VPN :** configurez ces paramètres pour les types de connexion IKEv2.
  - **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  - **Domaines safari :** cliquez sur **Ajouter** pour ajouter un nom de domaine Safari.

- **Configuration du proxy :** choisissez la façon dont la connexion VPN transite via un serveur proxy. La valeur par défaut est **Aucun**.

Configurer le protocole Citrix SSO pour iOS

Le client Citrix SSO est disponible dans le portail Apple Store.

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.

- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous définissez cette option sur Activé, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau.
  - **Type de fournisseur :** indiquez si le VPN par application est fourni en tant que **Proxy d'application** ou **Tunnel de paquet**. La valeur par défaut est **Proxy d'application**.
  - **Type de fournisseur :** définissez sur **Tunnel de paquet**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

- **XML personnalisé :** pour chaque paramètre XML personnalisé que vous souhaitez ajouter, cliquez sur **Ajouter** et spécifiez les paires clé/valeur. Les paramètres disponibles sont les suivants :
  - **disableL3 :** désactive le VPN au niveau du système. Autorise uniquement le Per App VPN. Aucune **valeur** n'est requise.
  - **user agent :** associe à cette stratégie toute stratégie NetScaler Gateway qui cible les clients de plug-in VPN. La **valeur** de cette clé est automatiquement ajoutée au plug-in VPN pour les requêtes initiées par le plug-in.

Configurer le protocole SSL personnalisé pour iOS

Pour passer du client Cisco Legacy AnyConnect au client Cisco AnyConnect :

1. Configurez la stratégie VPN avec le protocole SSL personnalisé. Déployez la stratégie sur les appareils iOS.
2. Chargez le client Cisco AnyConnect depuis https://apps.apple.com/us/app/cisco-secure-client/id1135064690, ajoutez l'application à Citrix Endpoint Management et déployez l'application sur les appareils iOS.
3. Supprimez l'ancienne stratégie VPN des appareils iOS.

Paramètres :

- **Identifiant SSL personnalisé (format DNS inverse) :** définissez sur le bundle ID. Pour le client Cisco AnyConnect, utilisez **com.cisco.anyconnect**.
- **Identificateur de bundle de fournisseur :** si l'application spécifiée dans **Identifiant SSL personnalisé** a plusieurs fournisseurs VPN du même type (Proxy d'application ou Tunnel de paquet), spécifiez cet identificateur de bundle. Pour le client Cisco AnyConnect, utilisez **com.cisco.anyconnect**.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **Activé**, consultez la section Configurer les options de l'activation VPN sur demande pour iOS.

- **Inclure tous les réseaux :** sélectionnez si vous souhaitez autoriser tous les réseaux à utiliser cette connexion. La valeur par défaut est **Désactivé**.
- **Exclure les réseaux locaux :** sélectionnez si vous souhaitez exclure les réseaux locaux de l'utilisation de la connexion ou autoriser les réseaux. La valeur par défaut est **Désactivé**.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous définissez cette option sur Activé, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau.
  - **Type de fournisseur :** un type de fournisseur indique si le fournisseur est un service VPN ou un service de proxy. Pour le service VPN, choisissez **Tunnel de paquet**. Pour le service de proxy, choisissez **Proxy d'application**. Pour le client Cisco AnyConnect, choisissez **Tunnel de paquet**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **XML personnalisé :** pour chaque paramètre XML personnalisé que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom du paramètre :** entrez le nom du paramètre à ajouter.
  - **Valeur :** entrez la valeur associée au **nom du paramètre**.
  - Cliquez sur **Enregistrer** pour enregistrer le paramètre ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer la stratégie VPN pour prendre en charge NAC

1. Le **type de connexion SSL personnalisé** est requis pour la configuration du filtre NAC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Spécifiez **VPN** comme **nom de connexion**.
3. Pour **Identifiant SSL personnalisé**, tapez **com.citrix.NetScalerGateway.ios.app**
4. Pour **Identificateur de bundle de fournisseur**, tapez **com.citrix.NetScalerGateway.ios.app.vpnplugin**

Les valeurs des étapes 3 et 4 proviennent de l'installation de Citrix SSO requise pour le filtrage NAC. Vous ne configurez pas de mot de passe d'authentification. Pour plus d'informations sur l'utilisation de la fonction NAC, voir Contrôle d'accès réseau.

Configurer les options de l'activation VPN sur demande pour iOS

- **Domaine sur demande :** pour chaque domaine et action à exécuter lorsque les utilisateurs s'y connectent, cliquez sur **Ajouter** et procédez comme suit :
- **Domaine :** entrez le domaine à ajouter.
- **Action :** dans la liste, sélectionnez l'une des actions possibles :
  - **Toujours établir :** le domaine déclenche toujours une connexion VPN.
  - **Ne jamais établir :** le domaine ne déclenche jamais de connexion VPN.
  - **Établir si nécessaire :** le domaine déclenche une tentative de connexion VPN si la résolution du nom de domaine échoue. L'échec se produit lorsque le serveur DNS ne peut pas résoudre le domaine, redirige la connexion vers un autre serveur ou expire.
  - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **Règles On Demand**
  - **Action :** dans la liste, sélectionnez l'action à exécuter. La valeur par défaut est **EvaluateConnection**. Les actions possibles sont les suivantes :
    - **Autoriser :** autoriser la connexion VPN sur demande.
    - **Connecter :** établir une connexion VPN sans condition.
    - **Déconnecter :** désactiver la connexion VPN et ne pas se reconnecter à la demande tant que la règle est active.
    - **EvaluateConnection :** évaluer la matrice ActionParameters pour chaque connexion.
    - **Ignorer :** conserver toute connexion VPN en cours mais ne pas se reconnecter à la demande tant que la règle est active.
  - **DNSDomainMatch :** pour chaque domaine avec lequel la liste de domaines de recherche d'un appareil peut correspondre, cliquez sur **Ajouter** et procédez comme suit :
    - **Domaine DNS :** entrez le nom du domaine. Vous pouvez utiliser le préfixe générique « * » pour la correspondance avec multiples domaines. Par exemple,*.exemple.com peut correspondre à mondomaine.exemple.com, tondomaine.exemple.com et sondomaine.exemple.com.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **DNSServerAddressMatch :** pour chaque adresse IP à laquelle n'importe quel des serveurs DNS spécifiés du réseau peut correspondre, cliquez sur **Ajouter** et procédez comme suit :
    * **Adresse du serveur DNS :** entrez l'adresse du serveur DNS que vous souhaitez ajouter. Vous pouvez utiliser le suffixe générique «*» pour la correspondance avec des serveurs DNS. Par exemple, 17.* correspond à n'importe quel serveur DNS u sous-réseau de classe A.
    * Cliquez sur **Enregistrer** pour enregistrer l'adresse du serveur DNS ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **InterfaceTypeMatch :** dans la liste, sélectionnez le type de matériel d'interface réseau principal utilisé. La valeur par défaut est **Non spécifié**. Valeurs possibles :
    * **Non spécifié :** correspondance avec n'importe quel matériel d'interface réseau. Cette option est la valeur par défaut.
    * **Ethernet :** correspondance uniquement avec le matériel d'interface réseau Ethernet.
    * **Wi-Fi :** correspondance uniquement avec le matériel d'interface réseau Wi-Fi.
    * **Cellulaire :** correspondance uniquement avec le matériel d'interface réseau cellulaire.
  - **SSIDMatch :** pour chaque SSID à faire correspondre avec le réseau actuel, cliquez sur **Ajouter** et procédez comme suit.
    * **SSID :** entrez le SSID à ajouter. Si le réseau n'est pas un réseau Wi-Fi, ou si le SSID ne s'affiche pas, la correspondance échoue. Laissez cette liste vide pour une correspondance avec n'importe quel SSID.
    * Cliquez sur **Enregistrer** pour enregistrer le SSID ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **URLStringProbe :** entrez une adresse URL à récupérer. Si cette adresse URL est correctement récupérée sans redirection, cette règle correspond.
  - **ActionParameters : Domains :** pour chaque domaine que EvaluateConnection doit vérifier, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **ActionParameters : DomainAction :** dans la liste, sélectionnez le **comportement du VPN** pour les domaines **ActionParameters : Domains** spécifiés. La valeur par défaut est **ConnectIfNeeded**. Les actions possibles sont les suivantes :
    * **ConnectIfNeeded :** le domaine déclenche une tentative de connexion VPN si la résolution du nom de domaine échoue. L'échec se produit lorsque le serveur DNS ne peut pas résoudre le domaine, redirige la connexion vers un autre serveur ou expire.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **NeverConnect :** le domaine ne déclenche jamais de connexion VPN.
  - **Action Parameters: RequiredDNSServers :** pour chaque serveur DNS à utiliser pour résoudre les domaines spécifiés, cliquez sur **Ajouter** et procédez comme suit :
    * **Serveur DNS :** valide uniquement si **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Saisissez l'adresse IP du serveur DNS. Ce serveur peut résider en dehors de la configuration réseau actuelle de l'appareil. Si le serveur DNS n'est pas accessible, une connexion VPN est établie en réponse. Assurez-vous que le serveur DNS est un serveur DNS interne ou un serveur DNS externe de confiance.
    * Cliquez sur **Enregistrer** pour enregistrer le serveur DNS ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **ActionParameters : RequiredURLStringProbe :** si vous le souhaitez, entrez une adresse URL HTTP ou HTTPS (recommandé) à interroger, à l'aide d'un requête GET. Si le nom d'hôte de l'adresse URL ne peut pas être résolu, si le serveur est inaccessible ou si le serveur ne répond pas, une connexion VPN est établie. Valide uniquement si **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.
  - **OnDemandRules : contenu XML :** entrez, ou copiez et collez, les règles "OnDemandRules"de la configuration XML.
    * Cliquez sur **Vérifier dict.** pour valider le code XML. Le texte **XML valide** s'affiche sous la zone de texte **Contenu XML** si le fichier XML est valide. S'il n'est pas valide, un message d'erreur s'affiche.

- **Proxy**
  - **Configuration du proxy :** dans la liste, sélectionnez la façon dont la connexion VPN transite via un serveur proxy. La valeur par défaut est **Aucun**.
    * Si vous avez sélectionné **Manuel**, configurez les paramètres suivants :
      · **Nom d'hôte ou adresse IP du serveur proxy :** entrez le nom d'hôte ou l'adresse IP du serveur proxy. Ce champ est obligatoire.
      · **Port du serveur proxy :** entrez le numéro de port du serveur proxy. Ce champ est obligatoire.
      · **Nom d'utilisateur :** entrez un nom d'utilisateur pour le serveur proxy (facultatif).
      · **Mot de passe :** entrez un mot de passe pour le serveur proxy (facultatif).
    * Si vous configurez **Automatique**, configurez ce paramètre :
      · **URL du serveur proxy :** entrez l'adresse URL du serveur proxy. Ce champ est obligatoire.

- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

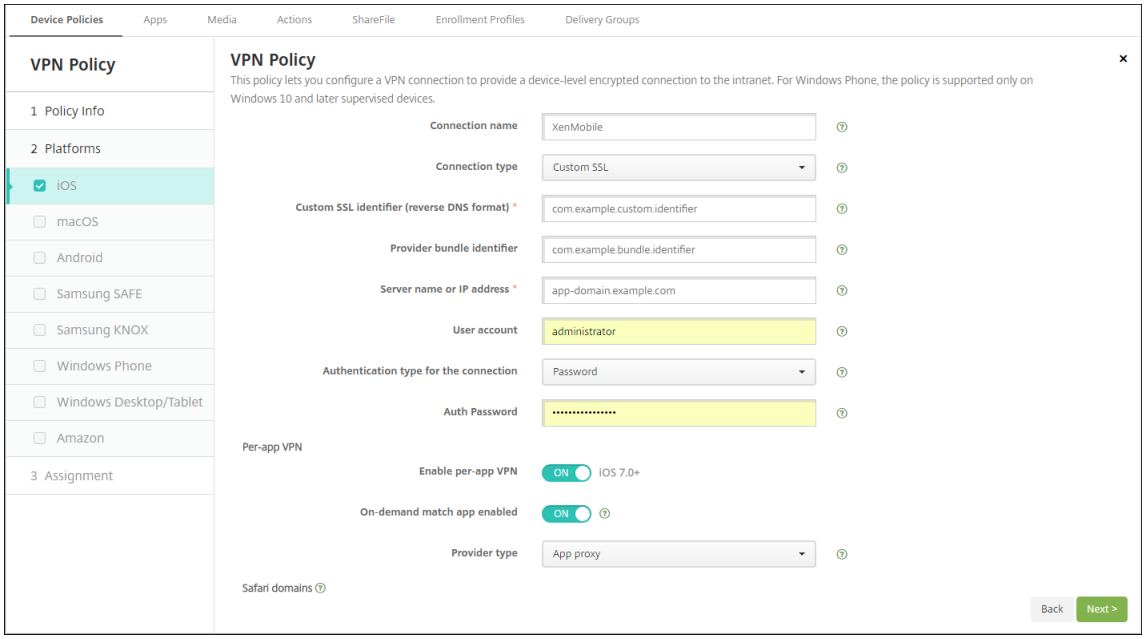
* **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
* **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Configurer une stratégie Per App VPN

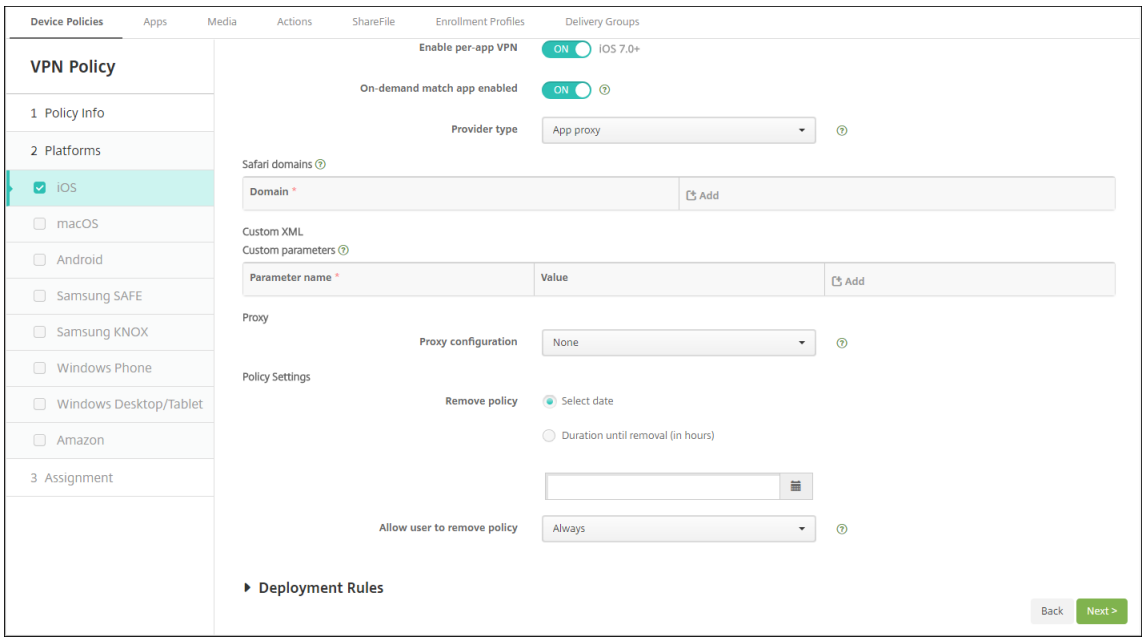
Des options Per App VPN pour iOS sont disponibles pour ces types de connexion : Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Aruba VIA, Citrix VPN, Citrix SSO et SSL personnalisé.

Pour configurer une stratégie Per App VPN :

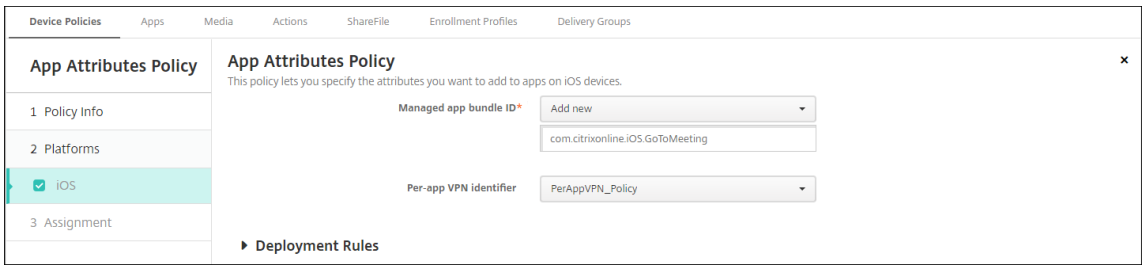
1. Dans **Configurer > Stratégies d'appareil**, créez une stratégie VPN. Par exemple :



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

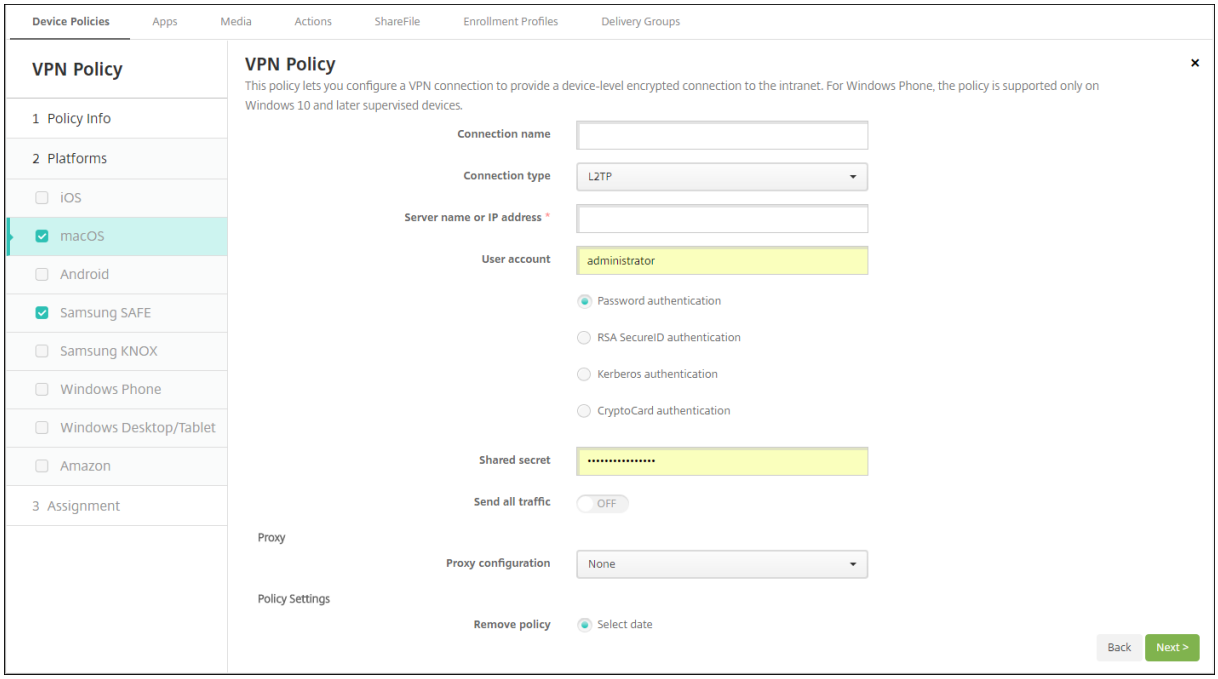


2. Dans **Configurer > Stratégies d'appareil**, créez une stratégie d'attributs d'application pour associer une application à la stratégie Per App VPN. Pour **Identifiant Per App VPN**, choisissez le nom de la stratégie VPN créée à l'étape 1. Pour **Bundle ID d'application gérée**, choisissez dans la liste d'applications ou entrez le bundle ID d'application. (Si vous déployez une stratégie d'inventaire des applications iOS, la liste des applications contient des applications).



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres macOS



- **Nom de la connexion :** entrez un nom pour la connexion.
- **Type de connexion :** dans la liste, sélectionnez le protocole à utiliser pour cette connexion. La valeur par défaut est L2TP.
  - **L2TP :** Layer 2 Tunneling Protocol avec authentification par clé pré-partagée.
  - **PPTP :** protocole PPTP.
  - **IPSec :** votre connexion VPN d'entreprise.
  - **Cisco AnyConnect :** client Cisco AnyConnect VPN.
  - **Juniper SSL :** client Juniper Networks SSL VPN.
  - **F5 SSL :** client F5 Networks SSL VPN.
  - **SonicWALL Mobile Connect :** client VPN Dell unifié pour iOS.
  - **Aruba VIA :** client Aruba Networks Virtual Internet Access.
  - **Citrix VPN :** client Citrix VPN.
  - **SSL personnalisé :** Secure Sockets Layer personnalisé.

Les sections suivantes répertorient les options de configuration pour chacun des types de connexion précédents.

Configurer le protocole L2TP pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Sélectionnez **Authentification par mot de passe**, **Authentification RSA SecurID**, **Authentification Kerberos** ou **Authentification CryptoCard**. La valeur par défaut est **Authentification par mot de passe**.
- **Secret partagé :** entrez la clé de secret partagé IPsec.
- **Envoyer tout le trafic :** sélectionnez cette option pour envoyer tout le trafic via le VPN. La valeur par défaut est **Désactivé**.

Configurer le protocole PPTP pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- Sélectionnez **Authentification par mot de passe**, **Authentification RSA SecurID**, **Authentification Kerberos** ou **Authentification CryptoCard**. La valeur par défaut est **Authentification par mot de passe**.
- **Niveau de chiffrement :** sélectionnez le niveau de chiffrement souhaité. La valeur par défaut est **Aucun**.
  - **Aucun :** le chiffrement n'est pas utilisé.
  - **Automatique :** utilise le niveau de chiffrement le plus élevé pris en charge par le serveur.
  - **Maximum (128 bits) :** utilise toujours le cryptage 128 bits.
- **Envoyer tout le trafic :** sélectionnez cette option pour envoyer tout le trafic via le VPN. La valeur par défaut est **Désactivé**.

Configurer le protocole IPsec pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Secret partagé** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Secret partagé**.
  - Si vous sélectionnez l'authentification **Secret partagé**, configurez les paramètres suivants :
    - **Nom du groupe :** entrez un nom de groupe (facultatif).
    - **Secret partagé :** entrez une clé de secret partagé (facultatif).
    - **Utiliser une authentification hybride :** indiquez si vous souhaitez utiliser l'authentification hybride. Avec l'authentification hybride, le serveur s'authentifie auprès du client, puis le client s'authentifie auprès du serveur. La valeur par défaut est **Désactivé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Demander le mot de passe :** indiquez si les utilisateurs doivent être invités à entrer leur mot de passe lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
  - Si vous avez sélectionné l'authentification **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** sélectionnez cette option pour demander aux utilisateurs d'entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.

Configurer le protocole Cisco AnyConnect pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Groupe :** entrez un nom de groupe (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.
  - **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Correspondance d'application à la demande activée :** indiquez si une connexion Per App VPN est déclenchée automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
    * **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
        · **Domaine :** entrez le domaine à ajouter.
        · Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole SSL Juniper pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Domaine :** entrez un nom de domaine (facultatif).
- **Rôle :** entrez un nom de rôle (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si une connexion Per App VPN est déclenchée automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole F5 SSL pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si une connexion Per App VPN est déclenchée automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer le protocole SonicWall Mobile Connect pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Groupe ou domaine de connexion :** entrez un groupe ou domaine de connexion (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    - **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    - **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    - **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si une connexion Per App VPN est déclenchée automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    - **Domaine :** entrez le domaine à ajouter.
    - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole Ariba VIA pour macOS

- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
- **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.
    * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
    * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.

- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
  - **Correspondance d'application à la demande activée :** indiquez si une connexion Per App VPN est déclenchée automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau. La valeur par défaut est **Désactivé**.
  - **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole SSL personnalisé pour macOS

- **Identifiant SSL personnalisé (format DNS inverse) :** entrez l'identifiant SSL au format DNS inverse. Ce champ est obligatoire.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN. Ce champ est obligatoire.
- **Compte d'utilisateur :** entrez un compte d'utilisateur (facultatif).
  - **Type d'authentification pour la connexion :** dans la liste, sélectionnez **Mot de passe** ou **Certificat** pour le type d'authentification à utiliser pour cette connexion. La valeur par défaut est **Mot de passe**.
  - Si vous activez **Mot de passe**, saisissez un mot de passe d'authentification facultatif dans le champ **Mot de passe d'authentification**.
  - Si vous avez sélectionné **Certificat**, configurez les paramètres suivants :
    * **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser. La valeur par défaut est **Aucun**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

        * **Exiger PIN à la connexion :** indiquez si les utilisateurs doivent être invités à entrer leur code PIN lorsqu'ils se connectent au réseau. La valeur par défaut est **Désactivé**.
        * **Activer VPN sur demande :** indiquez si une connexion VPN doit être déclenchée lorsque les utilisateurs se connectent au réseau. La valeur par défaut est **Désactivé**. Pour de plus amples informations sur la configuration de paramètres lorsque **Activer VPN sur demande** est réglé sur **ON**, consultez la section Configurer les options de l'activation VPN sur demande.
    - **Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. La valeur par défaut est **Désactivé**. Si vous activez cette option, configurez les paramètres suivants :
        * **Correspondance d'application à la demande activée :** indiquez si les connexions Per App VPN sont déclenchées automatiquement lorsque des applications liées au service Per App VPN initient une communication réseau.
        * **Domaines Safari :** pour chaque domaine Safari qui peut déclencher une connexion Per App VPN que vous souhaitez inclure, cliquez sur **Ajouter** et procédez comme suit :
            · **Domaine :** entrez le domaine à ajouter.
            · Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

- **XML personnalisé :** pour chaque paramètre XML personnalisé que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
    - **Nom du paramètre :** entrez le nom du paramètre à ajouter.
    - **Valeur :** entrez la valeur associée au **nom du paramètre**.
    - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer les options de l'activation VPN sur demande

- **Domaine sur demande :** pour chaque domaine et action à exécuter lorsque les utilisateurs s'y connectent, cliquez sur **Ajouter** et procédez comme suit :
    - **Domaine :** entrez le domaine à ajouter.
    - **Action :** dans la liste, sélectionnez l'une des actions possibles :
        * **Toujours établir :** le domaine déclenche toujours une connexion VPN.
        * **Ne jamais établir :** le domaine ne déclenche jamais de connexion VPN.
        * **Établir si nécessaire :** le domaine déclenche une tentative de connexion VPN si la résolution du nom de domaine échoue. L'échec se produit lorsque le serveur DNS ne peut pas résoudre le domaine, redirige la connexion vers un autre serveur ou expire.
    - Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Règles On Demand**
  - **Action :** dans la liste, sélectionnez l'action à exécuter. La valeur par défaut est **Evaluate-Connection**. Les actions possibles sont les suivantes :
    * **Autoriser :** autoriser la connexion VPN sur demande.
    * **Connecter :** établir une connexion VPN sans condition.
    * **Déconnecter :** désactiver la connexion VPN et ne pas se reconnecter à la demande tant que la règle est active.
    * **EvaluateConnection :** évaluer la matrice **ActionParameters** pour chaque connexion.
    * **Ignorer :** conserver toute connexion VPN en cours mais ne pas se reconnecter à la demande tant que la règle est active.
  - **DNSDomainMatch :** pour les domaines avec lesquels la liste de domaines de recherche d'un appareil peut correspondre, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine DNS :** entrez le nom du domaine. Vous pouvez utiliser le préfixe générique « * » pour la correspondance avec multiples domaines. Par exemple,*.exemple.com peut correspondre à mondomaine.exemple.com, tondomaine.exemple.com et son-domaine.exemple.com.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **DNSServerAddressMatch :** pour chaque adresse IP à laquelle n'importe quel des serveurs DNS spécifiés du réseau peut correspondre, cliquez sur **Ajouter** et procédez comme suit :
    * **Adresse du serveur DNS :** entrez l'adresse du serveur DNS que vous souhaitez ajouter. Vous pouvez utiliser le suffixe générique «*» pour la correspondance avec des serveurs DNS. Par exemple, 17.* correspond à n'importe quel serveur DNS u sous-réseau de classe A.
    * Cliquez sur **Enregistrer** pour enregistrer l'adresse du serveur DNS ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **InterfaceTypeMatch :** dans la liste, cliquez sur le type de matériel d'interface réseau principal utilisé. La valeur par défaut est **Non spécifié**. Valeurs possibles :
    * **Non spécifié :** correspondance avec n'importe quel matériel d'interface réseau. Cette option est la valeur par défaut.
    * **Ethernet :** correspondance uniquement avec le matériel d'interface réseau Ethernet.
    * **Wi-Fi :** correspondance uniquement avec le matériel d'interface réseau Wi-Fi.
    * **Cellulaire :** correspondance uniquement avec le matériel d'interface réseau cellulaire.
  - **SSIDMatch :** pour chaque SSID à faire correspondre avec le réseau actuel, cliquez sur **Ajouter** et procédez comme suit.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **SSID :** entrez le SSID à ajouter. Si le réseau n'est pas un réseau Wi-Fi, ou si le SSID ne s'affiche pas, la correspondance échoue. Laissez cette liste vide pour une correspondance avec n'importe quel SSID.
    * Cliquez sur **Enregistrer** pour enregistrer le SSID ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **URLStringProbe :** entrez une adresse URL à récupérer. Si cette adresse URL est correctement récupérée sans redirection, cette règle correspond.
  - **ActionParameters : Domains :** pour chaque domaine que EvaluateConnection doit vérifier, cliquez sur **Ajouter** et procédez comme suit :
    * **Domaine :** entrez le domaine à ajouter.
    * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **ActionParameters : DomainAction :** dans la liste, sélectionnez le **comportement du VPN** pour les domaines **ActionParameters : Domains** spécifiés. La valeur par défaut est **ConnectIfNeeded**. Les actions possibles sont les suivantes :
    * **ConnectIfNeeded :** le domaine déclenche une tentative de connexion VPN si la résolution du nom de domaine échoue. L'échec se produit lorsque le serveur DNS ne peut pas résoudre le domaine, redirige la connexion vers un autre serveur ou expire.
    * **NeverConnect :** le domaine ne déclenche jamais de connexion VPN.
  - **Action Parameters: RequiredDNSServers :** pour chaque serveur DNS à utiliser pour résoudre les domaines spécifiés, cliquez sur **Ajouter** et procédez comme suit :
    * **Serveur DNS :** valide uniquement si **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Tapez l'adresse IP du serveur DNS à ajouter. Ce serveur peut résider en dehors de la configuration réseau actuelle de l'appareil. Si le serveur DNS n'est pas accessible, une connexion VPN est établie en réponse. Ce serveur DNS doit être un serveur DNS interne ou un serveur DNS externe de confiance.
    * Cliquez sur **Enregistrer** pour enregistrer le serveur DNS ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **ActionParameters : RequiredURLStringProbe :** si vous le souhaitez, entrez une adresse URL HTTP ou HTTPS (recommandé) à interroger, à l'aide d'un requête GET. Si le nom d'hôte de l'adresse URL ne peut pas être résolu, si le serveur est inaccessible ou si le serveur ne répond pas, une connexion VPN est établie. Valide uniquement si **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.
  - **OnDemandRules : contenu XML :** entrez, ou copiez et collez, les règles "OnDemandRules"de la configuration XML.
    * Cliquez sur **Vérifier dict.** pour valider le code XML. Le texte **XML valide** s'affiche sous la zone de texte **Contenu XML** si le fichier XML est valide. S'il n'est pas valide, un message d'erreur s'affiche.

- **Proxy**

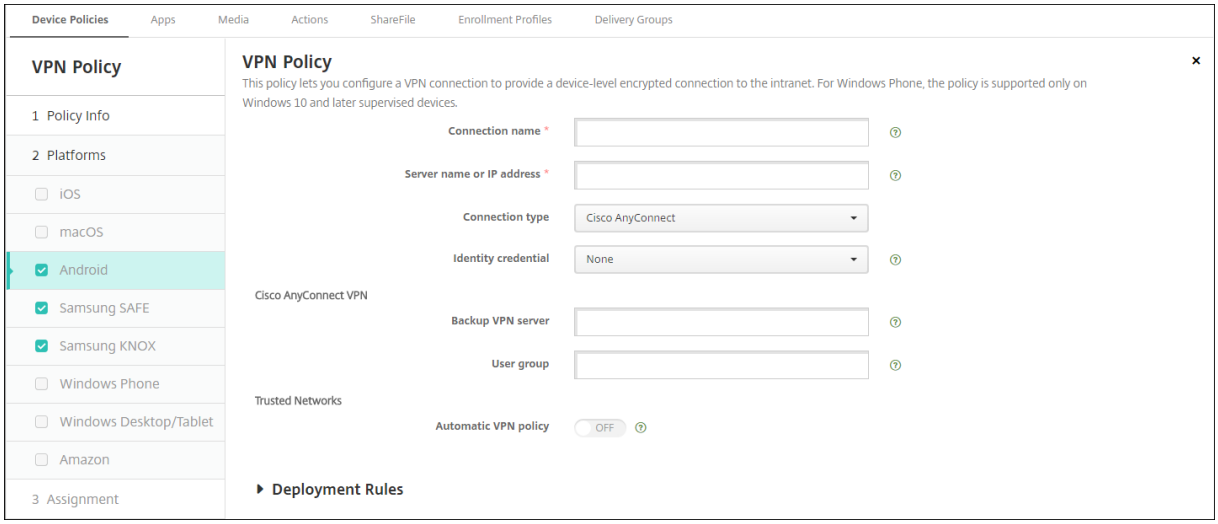
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Configuration du proxy :** dans la liste, sélectionnez la façon dont la connexion VPN transite via un serveur proxy. La valeur par défaut est **Aucun**.
    * Si vous avez sélectionné **Manuel**, configurez les paramètres suivants :
      · **Nom d'hôte ou adresse IP du serveur proxy :** entrez le nom d'hôte ou l'adresse IP du serveur proxy. Ce champ est obligatoire.
      · **Port du serveur proxy :** entrez le numéro de port du serveur proxy. Ce champ est obligatoire.
      · **Nom d'utilisateur :** entrez un nom d'utilisateur pour le serveur proxy (facultatif).
      · **Mot de passe :** entrez un mot de passe pour le serveur proxy (facultatif).
    * Si vous configurez **Automatique**, configurez ce paramètre :
      · **URL du serveur proxy :** entrez l'adresse URL du serveur proxy. Ce champ est obligatoire.

- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    * **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    * **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.
  - **Étendue du profil :** indiquez si cette stratégie s'applique à un **utilisateur** ou à un **système** entier. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur macOS 10.7 et versions ultérieures.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Android (DA hérité)



Configurer le protocole Cisco AnyConnect VPN pour Android

- **Nom de la connexion :** entrez un nom pour la connexion au VPN Cisco AnyConnect. Ce champ est obligatoire.
- **Nom du serveur ou adresse IP :** entrez le nom ou l'adresse IP du serveur VPN. Ce champ est obligatoire.
- **Infos d'identification de l'identité :** dans la liste, sélectionnez des Informations d'identification de l'identité.
- **Serveur VPN de sauvegarde :** entrez les informations du serveur VPN de sauvegarde.
- **Groupe d'utilisateurs :** entrez les informations relatives au groupe d'utilisateurs.
- **Réseaux fiables**
  - **Stratégie de VPN automatique :** activez ou désactivez cette option pour définir la façon dont le VPN réagit aux réseaux approuvés et non approuvés. Si cette option est activée, configurez les paramètres suivants :
    - **Stratégie pour réseau fiable :** dans la liste, sélectionnez la stratégie souhaitée. La valeur par défaut est **Déconnecter**. Les options possibles sont les suivantes :
      - **Déconnecter :** le client met fin à la connexion VPN dans le réseau approuvé. Il s'agit du réglage par défaut.
      - **Connecter :** le client initie une connexion VPN dans le réseau approuvé.
      - **Ne rien faire :** le client n'exécute aucune action.
      - **Mettre en pause :** met la session VPN en pause lorsqu'un utilisateur accède à un réseau configuré comme approuvé après avoir établi une session VPN à l'extérieur du réseau approuvé. Lorsque l'utilisateur quitte le réseau approuvé, la session

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

reprend. Ce paramètre élimine le besoin de créer une nouvelle session VPN après avoir quitté un réseau approuvé.

  * **Stratégie pour réseau non fiable :** dans la liste, sélectionnez la stratégie souhaitée. La valeur par défaut est **Connecter**. Les options possibles sont les suivantes :
    · **Connecter :** le client initie une connexion VPN dans le réseau non approuvé.
    · **Ne rien faire :** le client démarre une connexion VPN dans le réseau non approuvé. Cette option désactive le VPN permanent.

– **Domaines approuvés :** pour chaque suffixe de domaine que l'interface réseau possède lorsque le client est dans le réseau approuvé, cliquez sur **Ajouter** et procédez comme suit :
  * **Domaine :** entrez le domaine à ajouter.
  * Cliquez sur **Enregistrer** pour enregistrer le domaine ou cliquez sur **Annuler** pour ne pas l'enregistrer.

– **Serveurs approuvés :** pour chaque adresse de serveur que l'interface réseau possède lorsque le client est dans le réseau approuvé, cliquez sur **Ajouter** et procédez comme suit :
  * **Serveurs :** entrez le serveur à ajouter.
  * Cliquez sur **Enregistrer** pour enregistrer le serveur ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer le protocole Citrix SSO pour Android

- **Nom de la connexion :** entrez un nom pour la connexion VPN. Ce champ est obligatoire.
- **Nom du serveur ou adresse IP :** entrez le nom de domaine complet ou l'adresse IP du NetScaler Gateway.
- **Type d'authentification pour la connexion :** choisissez un type d'authentification et renseignez les champs qui s'affichent pour le type :
  – **Nom d'utilisateur** et **Mot de passe :** saisissez vos informations d'identification VPN pour les **Types d'authentification**, **Mot de passe** ou **Mot de passe et certificat**. Facultatif. Si vous ne fournissez les informations d'identification VPN, l'application Citrix VPN vous invite à entrer un nom d'utilisateur et un mot de passe.
  – **Infos d'identification de l'identité :** s'affiche pour les **Types d'authentification Certificat** ou **Mot de passe et certificat**. Dans la liste, sélectionnez des infos d'identification de l'identité.
- **Activer Per App VPN :** indiquez si vous souhaitez activer le per-app VPN. Si vous n'activez pas le per app VPN, tout le trafic transite via le tunnel VPN de Citrix. Si vous activez le per app VPN, spécifiez les paramètres suivants. La valeur par défaut est **Désactivé**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Liste verte** ou **Liste rouge** : si l'option **Liste verte** est sélectionnée, toutes les applications de la liste verte transitent via ce VPN. Si l'option **Liste rouge** est sélectionnée, toutes les applications sauf celles figurant sur la liste rouge transitent via ce VPN.
  - **Liste des applications :** les applications d'une liste d'autorisation ou d'une liste de blocage. Cliquez sur **Ajouter** et tapez une liste de noms de paquetages d'applications séparés par des virgules.

- **XML personnalisé :** cliquez sur **Ajouter**, puis entrez les paramètres personnalisés. Citrix Endpoint Management prend en charge ces paramètres pour Citrix VPN :

  - **DisableUserProfiles :** facultatif. Pour activer ce paramètre, entrez **Yes** pour **Value**. Si ce paramètre est activé, Citrix Endpoint Management n'affiche aucune connexion VPN ajoutée par l'utilisateur et l'utilisateur ne peut pas ajouter de connexion. Ce paramètre est une restriction globale et s'applique à tous les profils VPN.
  - **userAgent :** valeur de chaîne. Vous pouvez spécifier une chaîne d'agent utilisateur personnalisée à envoyer dans chaque requête HTTP. La chaîne d'agent utilisateur spécifiée est ajoutée à l'agent utilisateur Citrix VPN existant.

Configurer les VPN pour prendre en charge NAC

1. Définissez **Type de connexion** sur **SSL personnalisé** pour configurer le filtre NAC.
2. Spécifiez **VPN** comme **nom de connexion**.
3. Pour **XML personnalisé**, cliquez sur **Ajouter** et procédez comme suit :

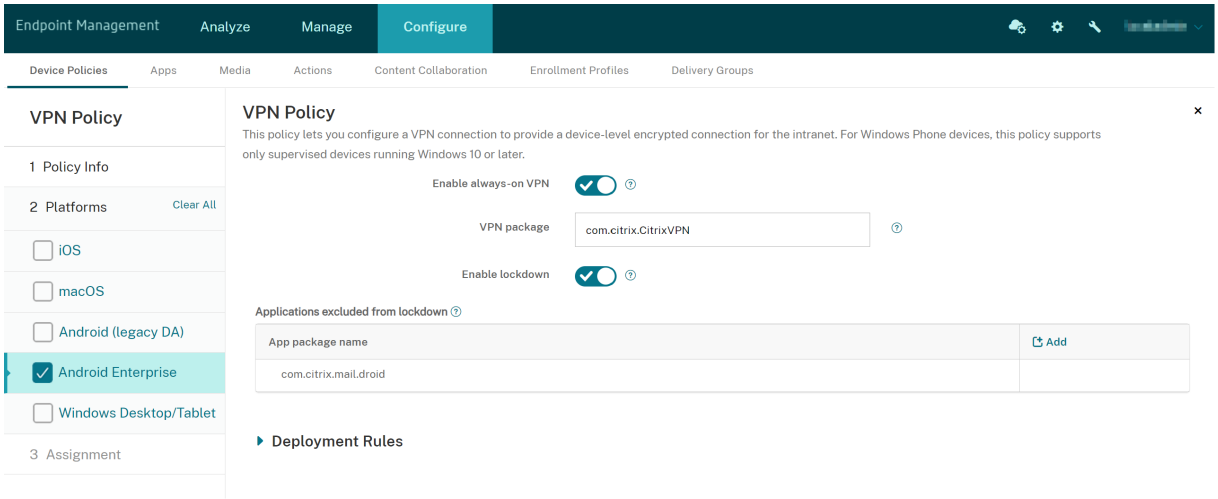
   - **Nom du paramètre :** saisissez **XenMobileDeviceId**. Il s'agit de l'ID d'appareil à utiliser pour le contrôle d'accès au réseau en fonction de l'inscription de l'appareil dans Citrix Endpoint Management. Si Citrix Endpoint Management s'inscrit et gère l'appareil, la connexion VPN est autorisée. Sinon, l'authentification est refusée au moment de l'établissement du VPN.
   - **Valeur :** tapez **DeviceID_${device.id}** qui est la valeur du paramètre **XenMobileDeviceId**.
   - Cliquez sur **Enregistrer** pour enregistrer le paramètre.

Configurer les VPN pour Android Enterprise

Pour configurer des VPN pour les appareils Android Enterprise, créez une stratégie Configurations gérées par Android Entreprise pour l'application Citrix SSO. Consultez la section Configurer les profils VPN pour Android Enterprise.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

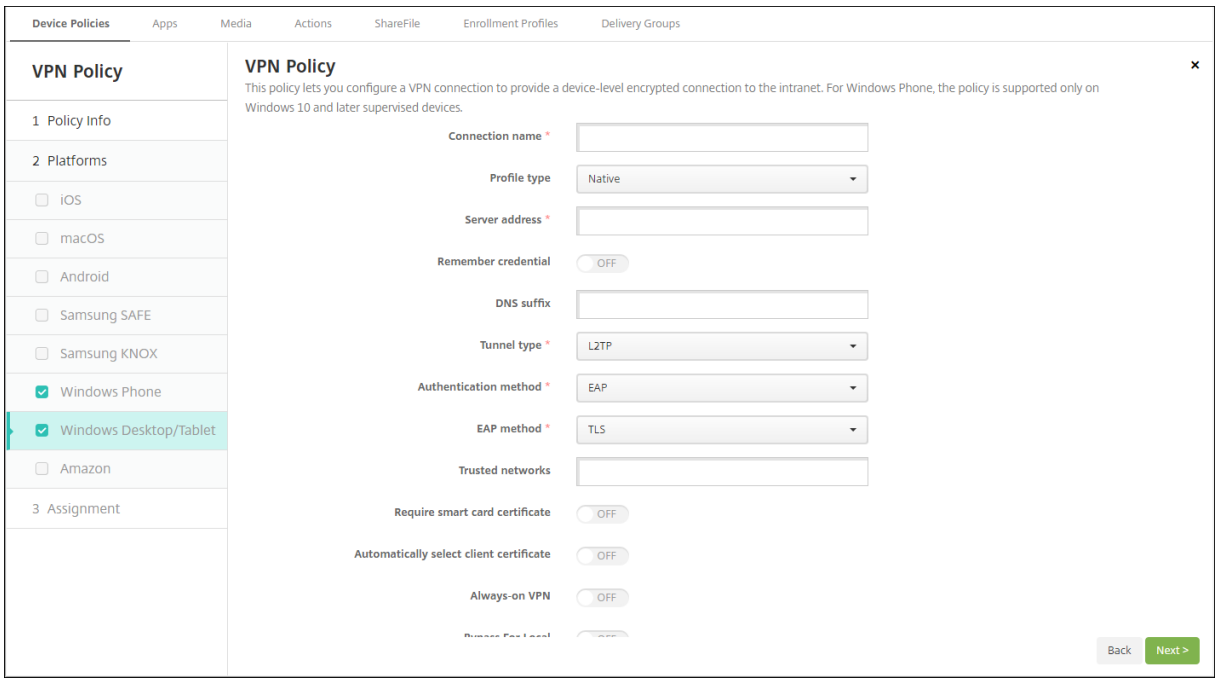
Paramètres Android Enterprise



- **Activer VPN Always On :** indiquez si le VPN Always On est activé. La valeur par défaut est **Désactivé**. Lorsque cette option est activée, la connexion VPN reste active jusqu'à ce que l'utilisateur se déconnecte manuellement.
- **Package VPN :** tapez le nom du package de l'application VPN utilisée par les appareils.
- **Activer le verrouillage :** si cette option est désactivée, aucune application ne peut accéder au réseau si aucune connexion VPN n'existe. Si cette option est activée, les applications que vous configurez dans le paramètre suivant peuvent accéder au réseau, même si aucune connexion VPN n'existe. Disponible pour les appareils Android 10 et versions ultérieures.
- **Applications exclues du verrouillage :** cliquez sur **Ajouter** pour entrer les noms des packages d'application pour lesquels vous souhaitez contourner le paramètre de verrouillage.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Windows Desktop/Tablet



- **Nom de la connexion :** entrez un nom pour la connexion Ce champ est obligatoire.
- **Type de profil :** dans la liste, sélectionnez **Natif** ou **Plug-in**. La valeur par défaut est **Natif**.
- **Configurer le type de profil natif :** ces paramètres s'appliquent au VPN intégré aux appareils Windows des utilisateurs.
  - **Adresse du serveur :** entrez le nom de domaine complet ou l'adresse IP du serveur VPN. Ce champ est obligatoire.
  - **Mémoriser les informations d'identification :** sélectionnez cette option si vous souhaitez mettre en cache les informations d'identification. La valeur par défaut est **Désactivé**. Lorsque cette option est activée, les informations d'identification sont mises en cache dès que possible.
  - **Suffixe DNS :** entrez le suffixe DNS.
  - **Type de tunnel :** dans la liste, sélectionnez le type de tunnel VPN à utiliser. La valeur par défaut est **L2TP**. Les options possibles sont les suivantes :
    - **L2TP :** Layer 2 Tunneling Protocol avec authentification par clé pré-partagée.
    - **PPTP :** protocole PPTP.
    - **IKEv2 :** Internet Key Exchange version 2.
  - **Méthode d'authentification :** dans la liste, sélectionnez la méthode d'authentification à utiliser. La valeur par défaut est **EAP**. Les options possibles sont les suivantes :
    - **EAP :** protocole d'authentification étendue.
    - **MSChapV2:** Use the Microsoft Challenge-Handshake Authentication Protocol for mutual authentication. Cette option n'est pas disponible lorsque vous sélectionnez

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

IKEv2 pour le type de tunnel.

- **Méthode EAP :** dans la liste, sélectionnez la méthode EAP à utiliser. La valeur par défaut est **TLS**. Ce champ n'est pas disponible lorsque l'authentification MSChapV2 est activée. Les options possibles sont les suivantes :
  * **TLS :** Transport Layer Security
  * **PEAP :** Protected Extensible Authentication Protocol
- **Réseaux approuvés :** entrez une liste de réseaux séparés par des virgules qui ne nécessitent pas de connexion VPN pour l'accès. Par exemple, lorsque les utilisateurs se trouvent sur le réseau sans fil de votre entreprise, ils peuvent accéder directement aux ressources protégées.
- **Exiger un certificat de carte à puce :** sélectionnez cette option pour exiger un certificat de carte à puce. La valeur par défaut est **Désactivé**.
- **Sélectionner automatiquement le certificat client :** sélectionnez cette option pour choisir automatiquement le certificat client à utiliser pour l'authentification. La valeur par défaut est **Désactivé**. Cette option n'est pas disponible lorsque vous activez **Exiger un certificat de carte à puce**.
- **VPN toujours connecté :** sélectionnez cette option pour spécifier si la connexion VPN est toujours activée. La valeur par défaut est **Désactivé**. Lorsque cette option est activée, la connexion VPN reste active jusqu'à ce que l'utilisateur se déconnecte manuellement.
- **Ne pas utiliser le VPN pour les adresses locales :** entrez l'adresse et le numéro de port pour permettre à des ressources locales pour contourner le serveur proxy.

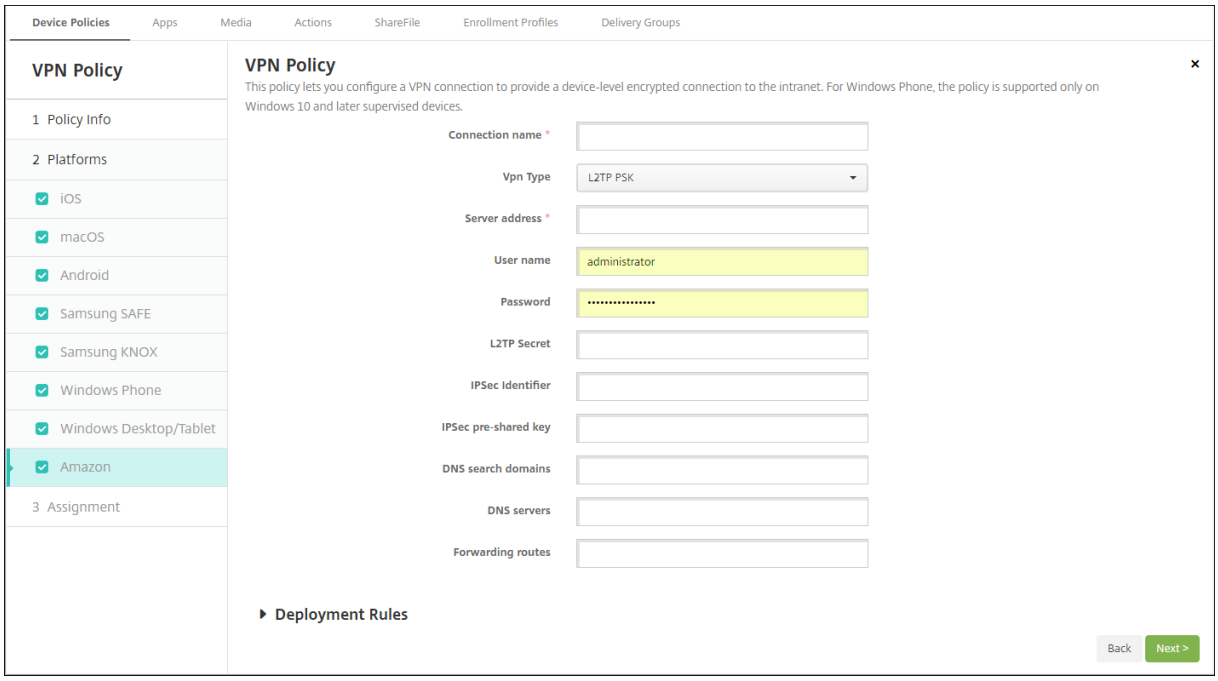
• **Configurer les paramètres du type de profil plug-in :** ces paramètres s'appliquent aux plug-ins VPN obtenus à partir du Windows Store et installés sur les appareils des utilisateurs.

- **Adresse du serveur :** entrez le nom de domaine complet ou l'adresse IP du serveur VPN. Ce champ est obligatoire.
- **Mémoriser les informations d'identification :** sélectionnez cette option si vous souhaitez mettre en cache les informations d'identification. La valeur par défaut est **Désactivé**. Lorsque cette option est activée, les informations d'identification sont mises en cache dès que possible.
- **Suffixe DNS :** entrez le suffixe DNS.
- **ID de l'application cliente :** entrez le nom de famille du package pour le plug-in VPN.
- **XML du profil du plug-in :** sélectionnez le profil de plug-in VPN personnalisé en cliquant sur **Parcourir** et accédez à l'emplacement du fichier. Contactez le fournisseur du plug-in pour des informations sur le format et plus de détails.
- **Réseaux approuvés :** entrez une liste de réseaux séparés par des virgules qui ne nécessitent pas de connexion VPN pour l'accès. Par exemple, lorsque les utilisateurs se trouvent sur le réseau sans fil de votre entreprise, ils peuvent accéder directement aux ressources protégées.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **VPN toujours connecté :** sélectionnez cette option pour spécifier si la connexion VPN est toujours activée. La valeur par défaut est **Désactivé**. Lorsque cette option est activée, la connexion VPN reste active jusqu'à ce que l'utilisateur se déconnecte manuellement.
- **Ne pas utiliser le VPN pour les adresses locales :** entrez l'adresse et le numéro de port pour permettre à des ressources locales pour contourner le serveur proxy.

Paramètres Amazon



- **Nom de la connexion :** entrez un nom pour la connexion
- **Type de VPN :** sélectionnez le type de connexion. Les options possibles sont les suivantes :
  - **L2TP PSK :** Layer 2 Tunneling Protocol (L2TP) avec authentification par clé pré-partagée. Il s'agit du réglage par défaut.
  - **L2TP RSA :** Layer 2 Tunneling Protocol avec authentification RSA.
  - **IPSEC XAUTH PSK :** Internet Protocol Security (IPSec) avec clé pré-partagée et authentification étendue
  - **IPSEC HYBRID RSA :** Internet Protocol Security (IPSec) avec authentification RSA hybride
  - **PPTP :** protocole PPTP.

Les sections suivantes répertorient les options de configuration pour chacun des types de connexion précédents.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer les paramètres L2TP PSK pour Amazon

- **Adresse du serveur :** entrez l'adresse IP du serveur VPN.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Secret L2TP :** entrez la clé du secret partagé.
- **Identificateur IPSec :** entrez le nom de la connexion VPN que les utilisateurs voient sur leurs appareils lors de la connexion.
- **Clé pré-partagée IPSec :** entrez la clé secrète.
- **Domaines de recherche DNS :** entrez les domaines avec lesquels la liste des domaines de recherche de l'appareil d'un utilisateur peut effectuer une correspondance.
- **Serveurs DNS :** entrez les adresses IP des serveurs DNS à utiliser pour résoudre les domaines spécifiés.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer les paramètres L2TP RSA pour Amazon

- **Adresse du serveur :** entrez l'adresse IP du serveur VPN.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Secret L2TP :** entrez la clé du secret partagé.
- **Domaines de recherche DNS :** entrez les domaines avec lesquels la liste des domaines de recherche de l'appareil d'un utilisateur peut effectuer une correspondance.
- **Serveurs DNS :** entrez les adresses IP des serveurs DNS à utiliser pour résoudre les domaines spécifiés.
- **Certificat serveur :** dans la liste, sélectionnez le certificat serveur à utiliser.
- **Certificat CA :** dans la liste, sélectionnez le certificat CA à utiliser.
- **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer les paramètres IPSEC XAUTH PSK pour Amazon

- **Adresse du serveur :** entrez l'adresse IP du serveur VPN.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Identificateur IPSec :** entrez le nom de la connexion VPN que les utilisateurs voient sur leurs appareils lors de la connexion.
- **Clé pré-partagée IPSec :** entrez la clé de secret partagé.
- **Domaines de recherche DNS :** entrez les domaines avec lesquels la liste des domaines de recherche de l'appareil d'un utilisateur peut effectuer une correspondance.
- **Serveurs DNS :** entrez les adresses IP des serveurs DNS à utiliser pour résoudre les domaines spécifiés.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer les paramètres IPSEC AUTH RSA pour Amazon

- **Adresse du serveur :** entrez l'adresse IP du serveur VPN.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Domaines de recherche DNS :** entrez les domaines avec lesquels la liste des domaines de recherche de l'appareil d'un utilisateur peut effectuer une correspondance.
- **Serveurs DNS :** entrez les adresses IP des serveurs DNS à utiliser pour résoudre les domaines spécifiés.
- **Certificat serveur :** dans la liste, sélectionnez le certificat serveur à utiliser.
- **Certificat CA :** dans la liste, sélectionnez le certificat CA à utiliser.
- **Infos d'identification de l'identité :** dans la liste, sélectionnez les informations d'identification de l'identité à utiliser.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer les paramètres IPSEC HYBRID RSA pour Amazon

- **Adresse du serveur :** entrez l'adresse IP du serveur VPN.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Domaines de recherche DNS :** entrez les domaines avec lesquels la liste des domaines de recherche de l'appareil d'un utilisateur peut effectuer une correspondance.
- **Serveurs DNS :** entrez les adresses IP des serveurs DNS à utiliser pour résoudre les domaines spécifiés.
- **Certificat serveur :** dans la liste, sélectionnez le certificat serveur à utiliser.
- **Certificat CA :** dans la liste, sélectionnez le certificat CA à utiliser.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Configurer les paramètres PPTP pour Amazon

- **Adresse du serveur :** entrez l'adresse IP du serveur VPN.
- **Nom d'utilisateur :** entrez un nom d'utilisateur (facultatif).
- **Mot de passe :** entrez un mot de passe (facultatif).
- **Domaines de recherche DNS :** entrez les domaines avec lesquels la liste des domaines de recherche de l'appareil d'un utilisateur peut effectuer une correspondance.
- **Serveurs DNS :** entrez les adresses IP des serveurs DNS à utiliser pour résoudre les domaines spécifiés.
- **Cryptage PPP (MPPE) :** sélectionnez cette option si vous souhaitez activer le cryptage de données avec Microsoft Point-to-Point Encryption (MPPE). La valeur par défaut est **Désactivé**.
- **Routes de transfert :** si votre serveur VPN d'entreprise prend en charge les routes de transfert, pour chaque route de transfert à utiliser, cliquez sur **Ajouter** et procédez comme suit :
  - **Route de transfert :** entrez l'adresse IP de la route de transfert.
  - Cliquez sur **Enregistrer** pour enregistrer la route ou cliquez sur **Annuler** pour ne pas l'enregistrer.

Stratégie de fond d'écran

December 9, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La stratégie Fond d'écran permet d'ajouter un fichier .png ou .jpg en tant que fond d'écran sur l'écran d'accueil, l'écran de verrouillage ou les deux. Cette stratégie n'est disponible que pour les appareils supervisés. Pour utiliser un fond d'écran différent sur iPad et iPhone, vous devez créer différentes stratégies de fond d'écran et les déployer vers les utilisateurs appropriés.

Le tableau suivant répertorie les dimensions d'image recommandées par Apple pour les appareils iOS.

iPhone

Appareil	Dimensions d'image en pixels
iPhone 12 Pro Max	2 778 x 1 284
iPhone 12 et iPhone 12 Pro	2 532 x 1 170
iPhone 12 Mini	2 340 x 1 080
iPhone 11 Max	2 688 x 1 242
iPhone 11 Pro	2 436 x 1 125
iPhone 11	1 792 x 828
iPhone XS Max	2 688 x 1 242
iPhone X, XS	2 436 x 1 125
iPhone XR	1 792 x 828
iPhone SE 2e génération	1 334 x 750
iPhone 7 Plus, 8 Plus	2 208 x 1 242
iPhone 7, 8	1 334 x 750
iPhone 8 Plus	1 334 x 750
iPhone 8	1 334 x 750

iPad

Appareil	Dimensions d'image en pixels
iPad Pro (1re, 2e et 3e génération 12,9 pouces)	2732 x 2048
iPad Pro 10,5 pouces	2224 x 1668
iPad Pro (9,7 pouces)	1 536 x 2 048

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Appareil	Dimensions d'image en pixels
iPad Air 2	2 048 x 1 536

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Appliquer à :** dans la liste, sélectionnez **Écran de verrouillage**, **Ecran d'accueil (liste d'icônes)** ou **Écrans d'accueil et de verrouillage** pour définir si le fond d'écran doit apparaître
- **Fichier de fond d'écran :** pour sélectionner le fichier de fond d'écran, cliquez sur **Parcourir** et accédez à l'emplacement du fichier.

Stratégie de filtre de contenu Web

November 29, 2023

Vous pouvez filtrer le contenu Web sur les appareils iOS à l'aide de la fonction de filtrage automatique d'Apple en conjonction avec les sites spécifiques que vous ajoutez aux listes d'autorisation et de blocage. La stratégie de filtre de contenu Web est uniquement disponible sur les appareils iOS en mode Supervisé. Pour plus d'informations sur le placement d'un appareil iOS en mode supervisé, voir Déployer des appareils à l'aide d'Apple Configurator 2

> **Remarque :**
>
> Les appareils Android ne prennent pas en charge le filtrage de contenu Web.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Type de filtre :** dans la liste, cliquez sur **Intégré** ou **Plug-in**, puis suivez les procédures ci-dessous pour l'option que vous choisissez. La valeur par défaut est **Intégré**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Type de filtre Intégré

- **Filtre de contenu Web**
  - **Filtrage automatique activé :** sélectionnez cette option pour spécifier si vous souhaitez utiliser la fonction de filtrage automatique d'Apple afin de détecter tout contenu inapproprié sur les sites Web. La valeur par défaut est **Off**.
  - **URL autorisées :** cette liste est ignorée lorsque l'option **Filtrage automatique activé** est définie sur **Désactivé**. Lorsque l'option **Filtrage automatique activé** est définie sur **Activé**, les éléments figurant dans cette liste sont toujours accessibles, que le filtrage automatique en permette l'accès ou non. Pour chaque adresse URL que vous souhaitez ajouter à la liste d'autorisation, cliquez sur **Ajouter** et procédez comme suit :
    * Entrez l'adresse URL du site Web autorisé. Vous devez ajouter `https://` ou `https://` avant l'adresse Web.
    * Cliquez sur **Enregistrer** pour enregistrer le site Web dans la liste d'autorisation ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **URL bloquée :** les éléments dans cette liste sont toujours bloqués. Pour chaque adresse URL que vous souhaitez ajouter à la liste de blocage, cliquez sur **Ajouter** et procédez comme suit :
    * Entrez l'adresse URL du site Web à bloquer. Vous devez ajouter `https://` ou `https://` avant l'adresse Web.
    * Cliquez sur **Enregistrer** pour enregistrer le site Web dans la liste de blocage ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **Ajouter la liste verte aux signets**
  - **Ajouter liste verte aux signets :** spécifie les sites auxquels les utilisateurs peuvent accéder. Pour activer l'accès aux sites web, ajoutez leur adresse URL.
    * **URL :** URL de chaque site Web auquel les utilisateurs peuvent accéder. Par exemple, pour activer l'accès au magasin Citrix Secure Hub, ajoutez l'URL du serveur Citrix Endpoint Management à la liste des **URL**. Vous devez ajouter `https://` ou `https://` avant l'adresse Web. Ce champ est obligatoire.
    * **Dossier de signets :** entrez un nom de dossier des signets (facultatif). Si ce champ est vide, le signet est ajouté au répertoire de signets par défaut.
    * **Titre :** entrez un titre descriptif pour le site Web. Par exemple, tapez « Google » pour l'adresse URL `https://google.com`.
    * Cliquez sur **Enregistrer** pour enregistrer le site Web dans la liste d'autorisation ou cliquez sur **Annuler** pour ne pas l'enregistrer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Type de filtre Plug-in

- **Nom du filtre :** entrez un nom unique pour le filtre.
- **Identifiant :** entrez le Bundle ID du plug-in qui fournit le service de filtrage.
- **Adresse du service :** entrez une adresse de serveur (facultatif). Les formats valides sont une adresse IP, un nom d'hôte ou une adresse URL.
- **Nom d'utilisateur :** entrez un nom d'utilisateur pour le service (facultatif).
- **Mot de passe :** entrez un mot de passe pour le service (facultatif).
- **Certificat :** dans la liste, cliquez sur un certificat d'identité (facultatif) à utiliser pour authentifier l'utilisateur auprès du service. La valeur par défaut est **Aucun**.
- **Filtrer le trafic WebKit :** sélectionnez cette option si vous voulez filtrer le trafic WebKit.
- **Filtrer le trafic de socket :** sélectionnez cette option si vous voulez filtrer le trafic de socket.
- **Données personnalisées :** pour chaque clé personnalisée que vous souhaitez ajouter au filtre Web, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Clé :** entrez la clé personnalisée.
  - **Valeur :** entrez une valeur pour la clé personnalisée.
  - Cliquez sur **Enregistrer** pour enregistrer la clé personnalisée ou cliquez sur **Annuler** pour ne pas l'enregistrer.
- **Paramètre de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.

Stratégie de clip Web

March 1, 2024

Vous pouvez placer des raccourcis ou clips Web sur des sites Web de manière à ce qu'ils apparaissent à côté des applications sur les appareils des utilisateurs. Vous pouvez spécifier vos propres icônes pour représenter les clips Web sur des appareils iOS, iPadOS, macOS et Android. Windows Tablet requiert uniquement un libellé et une adresse URL. Pour les appareils iOS et iPadOS, configurez la stratégie Disposition de l'écran d'accueil pour organiser les clips Web que vous créez. Si vous restreignez l'

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

accès aux applications sur iOS, assurez-vous de configurer la stratégie de restrictions pour autoriser les clips Web. Pour plus d'informations sur la configuration de ces stratégies, voir Stratégie Disposition de l'écran d'accueil et Stratégie Restrictions.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres iOS

- **Étiquette :** entrez l'étiquette qui s'affichera avec le clip Web.
- **URL :** entrez l'adresse URL associée avec le clip Web. L'adresse URL doit commencer par un protocole, par exemple, `https://server`.
- **Amovible :** indiquez si les utilisateurs peuvent supprimer le clip Web. La valeur par défaut est **Désactivé**. Cette option n'est pas prise en charge sur les iPad partagés.
- **Icône à mettre à jour :** sélectionnez l'icône à utiliser pour le clip Web en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.
- **Icône précomposée :** indiquez si des effets doivent être appliqués à cette icône (coins arrondis, ombre portée et brillant réflectif). La valeur par défaut est **Désactivé**, ce qui ajoute des effets.
- **Plein écran :** indiquez si la page Web associée s'ouvre en mode plein écran. Ce paramètre permet également à un iPad d'ouvrir un seul site Web. Pour configurer l'exécution des iPad en mode Kiosque, vous pouvez également utiliser la stratégie Mode kiosque. Pour plus d'informations, consultez Configurer un iPad en tant que kiosque. La valeur par défaut est **Désactivé**.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu. Disponible uniquement pour iOS 6.0 et versions ultérieures.
  - **Étendue du profil :** indiquez si la stratégie s'applique à un utilisateur ou à un système entier. La valeur par défaut est **Système**. Disponible uniquement pour iOS 9.3 et versions ultérieures.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres macOS

- **Étiquette :** entrez l'étiquette qui s'affichera avec le clip Web.
- **URL :** entrez l'adresse URL associée avec le clip Web. L'adresse URL doit commencer par un protocole, par exemple, `https://server`.
- **Icône à mettre à jour :** sélectionnez l'icône à utiliser pour le clip Web en cliquant sur Parcourir et en accédant à l'emplacement du fichier.
- **Paramètres de stratégie**
  - **Supprimer la stratégie :** choisissez une méthode de planification de la suppression de la stratégie. Les options disponibles sont **Sélectionner une date** et **Délai avant suppression (en heures)**.
    - **Sélectionner une date :** cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
    - **Délai avant suppression (en heures) :** saisissez un nombre, en heures, jusqu'à ce que la suppression de la stratégie ait lieu.
  - **Autoriser l'utilisateur à supprimer la stratégie :** vous pouvez sélectionner quand les utilisateurs peuvent supprimer la stratégie de leur appareil. Sélectionnez **Toujours**, **Code secret requis** ou **Jamais** dans le menu. Si vous sélectionnez **Code secret requis**, saisissez un code dans le champ **Mot de passe de suppression**.

Paramètres Android

- **Règle :** indiquez si cette stratégie ajoute ou supprime un clip Web. La valeur par défaut est **Ajouter**.
- **Étiquette :** entrez l'étiquette qui s'affichera avec le clip Web.
- **URL :** entrez l'adresse URL associée avec le clip Web.
- **Définir une icône :** indiquez si vous souhaitez utiliser un fichier d'icône. La valeur par défaut est **Désactivé**.
- **Fichier icône :** si **Définir une icône** est réglé sur **Activé**, sélectionnez le fichier d'icône à utiliser en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.

Paramètres Windows Desktop/Tablet

- **Nom :** entrez le libellé qui s'affichera avec le clip Web.
- **URL :** entrez l'adresse URL associée avec le clip Web.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégie de l'agent Windows

November 29, 2023

Utilisez la stratégie Agent Windows pour exécuter des scripts PowerShell sur les bureaux et les tablettes Windows gérés. Vous pouvez pointer vers des fichiers de script chargés sur Citrix Endpoint Management en tant qu'application d'entreprise et vers d'autres serveurs qui hébergent des scripts. Pour plus d'informations sur l'ajout d'applications d'entreprise, consultez la section Ajouter des applications.

Tous les scripts s'exécutent avec un état privilégié ; vous n'avez donc pas besoin d'exécuter les scripts en tant qu'administrateur.

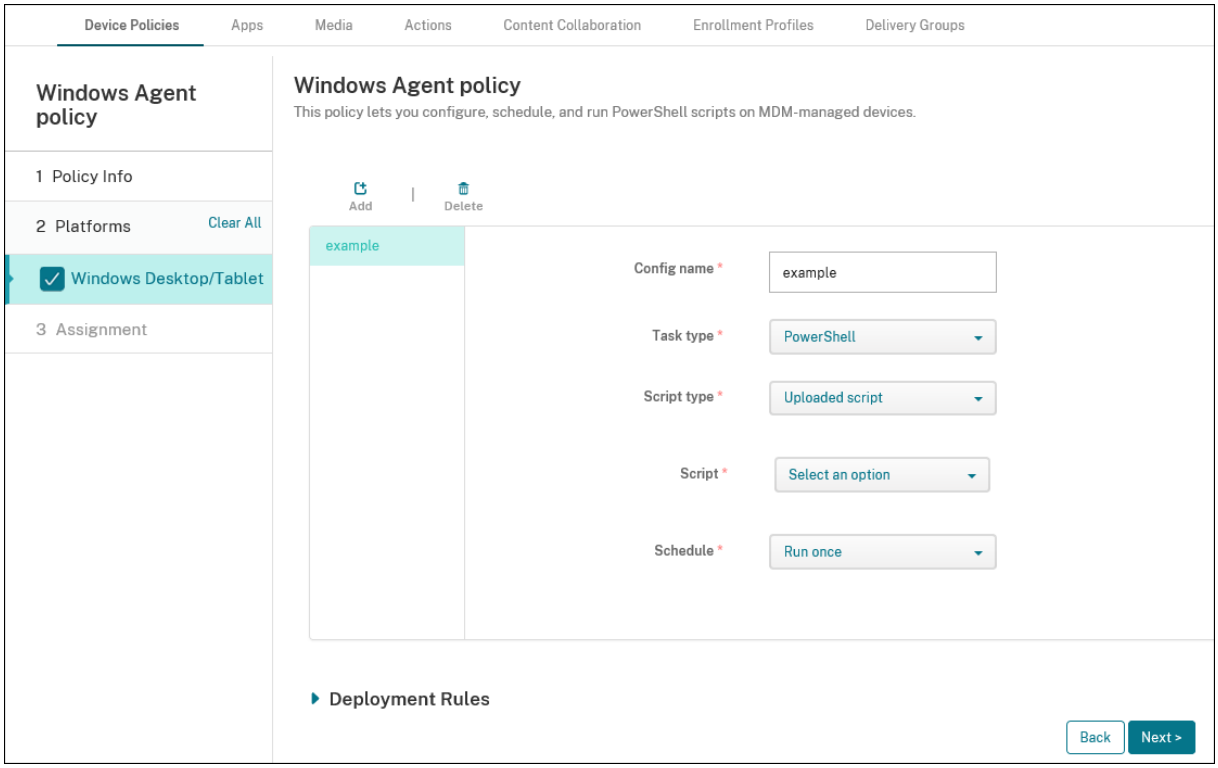
Après avoir déployé et exécuté le script, vous pouvez configurer des actions automatisées en fonction des résultats du script. Par exemple, vous exécutez un script qui surveille une clé de Registre et renvoie un résultat. Sur la base du résultat renvoyé, une action automatisée s'exécute. L'action accorde ou refuse l'accès à une application, marque l'appareil comme étant non conforme ou a d'autres effets.

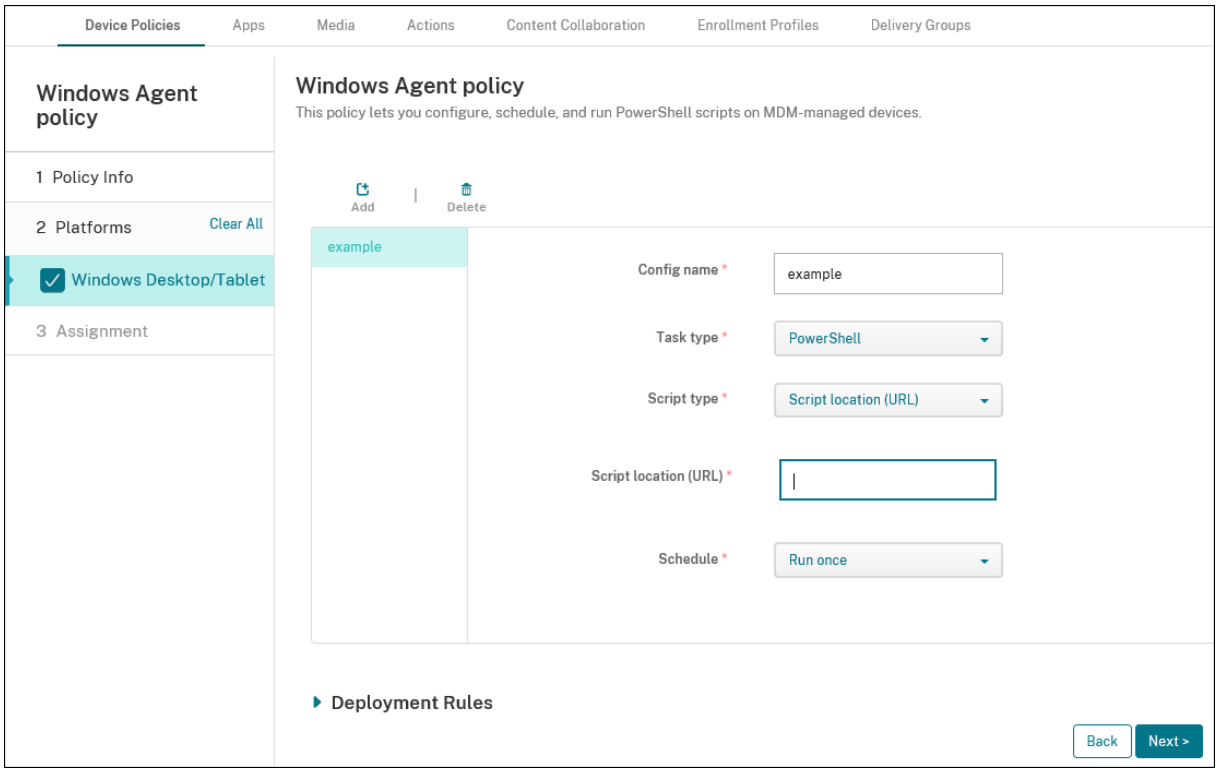
Vous pouvez également utiliser cette stratégie pour déployer des programmes d'installation MSI personnalisés en configurant un script PowerShell qui pointe vers un fichier .msi et un fichier .mst.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètres Windows Desktop et Tablet





- **Nom de la configuration :** entrez un nom descriptif pour la configuration.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Type de tâche :** sélectionnez **PowerShell**.
- **Type de script :** sélectionnez **Script chargé** pour les scripts que vous avez chargés sur Citrix Endpoint Management ou sélectionnez **URL de l'emplacement du script** pour les scripts hébergés en externe. Pour plus d'informations sur le téléchargement d'un script dans Citrix Endpoint Management, consultez la section Ajouter des applications Win32 en tant qu'applications d'entreprise.
  - **Sélectionner script :** si vous avez sélectionné **Script chargé**, sélectionnez le script à exécuter.
  - **Emplacement du script (URL) :** si vous avez choisi **Emplacement du script (URL)**, entrez l'emplacement du script à exécuter. Cette URL doit fournir le script sous forme de charge utile. Citrix Endpoint Management ne prend pas en charge les URL qui fournissent des scripts en tant que téléchargement JavaScript. Le script doit également être accessible au public.
- **Planifier :** sélectionnez **Exécuter une fois** pour exécuter le script sélectionné une fois ou sélectionnez **Exécuter régulièrement** pour exécuter le script de manière régulière.
  - **Exécuter toutes les (heures) :** entrez le nombre d'heures entre les exécutions du script.

Pour vérifier l'état d'un script, accédez à **Gérer > Appareils** dans votre console. Sélectionnez l'appareil sur lequel vous souhaitez vérifier l'état du script et cliquez sur **Modifier**. Sous **Propriétés**, vous pouvez vérifier l'état de vos scripts en cliquant sur **Télécharger** sous l'en-tête de **Agent Windows**.

Déployer un script PowerShell pour déclencher une action automatisée

1. Créez un script PowerShell pour surveiller une clé de Registre. Le script PowerShell suivant vérifie si le pare-feu est activé.

```
$body = @{
  }

$firewallEnabled = Get-ItemPropertyValue HKLM:\SYSTEM\
    CurrentControlSet\Services\SharedAccess\Parameters\
    FirewallPolicy\StandardProfile -Name EnableFirewall
if($firewallEnabled -eq 1){

$body["firewallEnabled"]="true"
 }
  else {

$body["firewallEnabled"]="false"
 }

$body | ConvertTo-Json -Depth 10
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--NeedCopy-->
```

Ce script renvoie une valeur

```
{

    "firewallEnabled":  "true"
 }

<!--NeedCopy-->
```

ou

```
{

    "firewallEnabled":  "false"
 }

<!--NeedCopy-->
```

2. Téléchargez le script sur la console Citrix Endpoint Management en tant qu'application d'entreprise ou hébergez le script sur une URL accessible.
3. Configurez la stratégie Agent Windows selon les instructions de cet article. Assurez-vous que le script est programmé pour s'exécuter immédiatement.
4. Une fois le script exécuté, déterminez l'état du script.
   a) Accédez à **Gérer > Appareils** dans votre console.
   b) Sélectionnez l'appareil pour vérifier l'état de son script, puis cliquez sur **Modifier**.
   c) Cliquez sur **Télécharger** sous l'en-tête **Agent Windows**.
5. Configurez une action automatisée en fonction de l'état reçu. Pour plus d'informations sur la configuration d'actions automatisées, voir Créer une action automatisée basée sur un résultat de la stratégie Agent Windows. Cette section présente les actions automatisées spécifiques créées pour l'exemple de script et la stratégie Agent Windows.

Stratégie de configuration de GPO Windows

November 29, 2023

La stratégie de configuration de GPO Windows vous permet de :

- Utiliser la console Citrix Endpoint Management pour importer des objets de stratégie de groupe (GPO) et les déployer sur des appareils Windows 10 et Windows 11

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

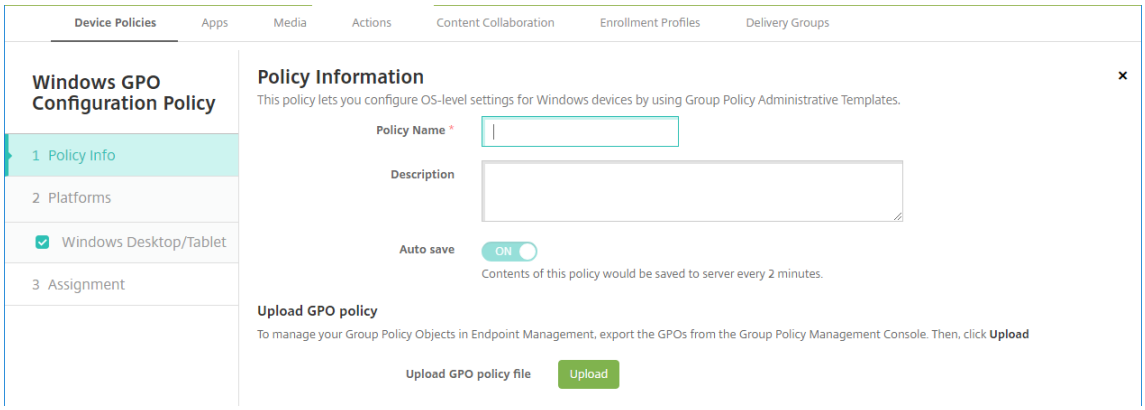
- Configurer des objets de stratégie de groupe (GPO) pour tout appareil Windows pris en charge par Citrix Workspace Environment Management
- Configurer des objets de stratégie de groupe (GPO) au niveau de l'appareil et de l'utilisateur

Importer des objets de stratégie de groupe (GPO) pour le déploiement sur des appareils Windows 10 et Windows 11

Au lieu de dépendre d'un administrateur AD pour utiliser la Console de gestion des stratégies de groupe pour gérer les objets de stratégie de groupe, vous pouvez importer et déployer des objets de stratégie de groupe via la console Citrix Endpoint Management.

Pour créer une sauvegarde de vos objets de stratégie de groupe dans Citrix Endpoint Management, procédez comme suit :

1. Demandez à votre administrateur AD d'exporter des objets de stratégie de groupe à partir de la Console de gestion des stratégies de groupe et de vous fournir les fichiers.
2. Dans la console Citrix Endpoint Management, accédez à **Configurer > Stratégies d'appareil** et créez une stratégie **Configuration de GPO Windows**.
3. Cliquez sur **Charger**, recherchez le fichier, puis cliquez sur **Ouvrir** pour importer le fichier.



   Pour plus d'informations sur la configuration des objets de stratégie de groupe, consultez cet article, Paramètres Windows Desktop et Tablet.

Configurer des objets de stratégie de groupe pour le déploiement dans Citrix Workspace Environment Management

La stratégie de configuration de GPO Windows vous permet de configurer des objets de stratégie de groupe (GPO) pour tout appareil Windows pris en charge par Citrix Workspace Environment Management (WEM). Citrix Endpoint Management transmet les stratégies vers le service Citrix WEM. Le service

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

WEM applique ensuite les objets de stratégie de groupe aux appareils et à leurs applications à l'aide de l'agent WEM installé sur les appareils.

Pour plus d'informations sur l'installation de l'agent Workspace Environment Management, consultez la section Installer et configurer.

Cette stratégie utilise tous les fichiers ADMX du système d'exploitation Windows. Si vous souhaitez télécharger un fichier ADMX tiers, utilisez la stratégie de configuration d'application. Pour plus d'informations sur le téléchargement de fichiers ADMX tiers, consultez la section Stratégie de configuration d'application.

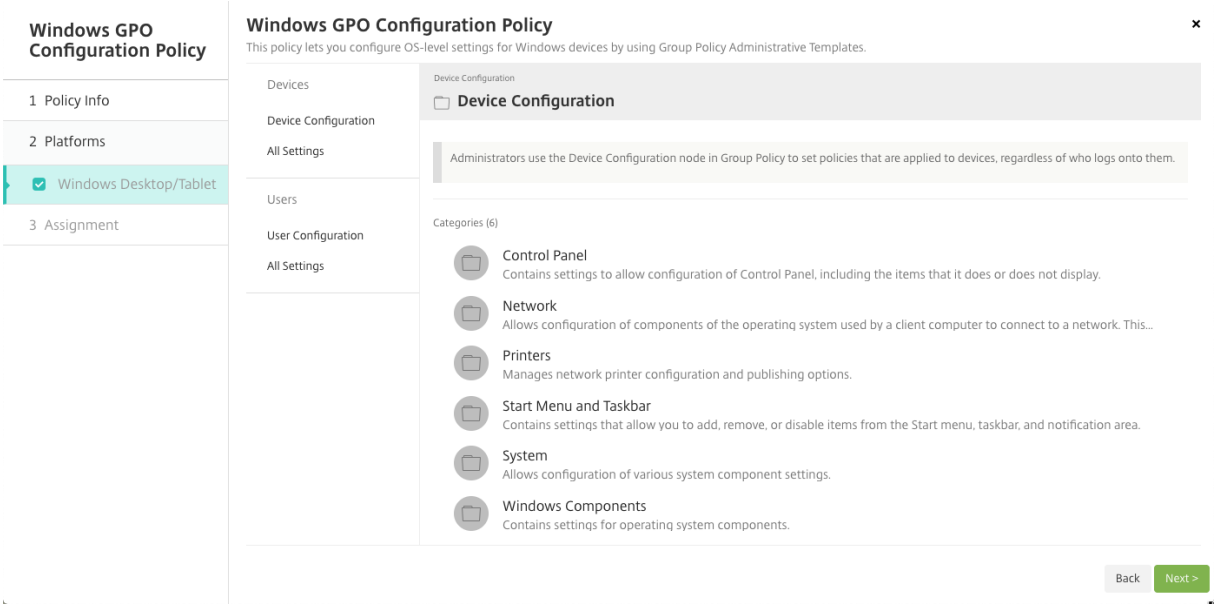
- Vous pouvez transmettre les configurations d'objet de stratégie de groupe vers n'importe quel appareil pris en charge par WEM, même si Citrix Endpoint Management ne prend pas en charge l'appareil en mode natif. Pour obtenir une liste des appareils pris en charge, consultez la section Configuration requise pour le système d'exploitation.
- Cette stratégie exige que l'agent WEM soit installé et configuré sur un appareil. Il n'est pas nécessaire d'inscrire les appareils auprès de MDM ou de MAM.
- Citrix Endpoint Management transmet les paramètres d'objet de stratégie de groupe via le canal WEM. (Microsoft ne prend pas en charge le transfert des paramètres au niveau de l'appareil via le canal MDM.) Les appareils qui reçoivent la stratégie de configuration de GPO Windows s'exécutent dans le mode Citrix Endpoint Management appelé WEM. Dans la liste **Gérer > Appareils** des appareils inscrits, la colonne **Mode** des appareils gérés par WEM répertorie **WEM**.

Pour ajouter ou configurer cette stratégie, accédez à **Configurer > Stratégies d'appareil**. Pour de plus amples informations, consultez la section Stratégies d'appareil.

Paramètres Windows Desktop et Tablet

Cette stratégie vous permet de configurer des objets de stratégie de groupe au niveau de l'appareil et de l'utilisateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Sélectionnez et configurez l'objet de stratégie de groupe Windows à déployer sur vos appareils Windows. Vous pouvez modifier la **configuration de l'appareil** et la **configuration utilisateur**. Les stratégies sont répertoriées dans une structure d'arborescence. Cliquez sur **Tous les paramètres** pour afficher chaque paramètre. Pour plus d'informations sur les paramètres, téléchargez une feuille de référence GPO à partir de Microsoft.

Pour configurer un paramètre, vous devez d'abord l'activer. Au cours de la configuration, Citrix Endpoint Management enregistre automatiquement les modifications afin que ces paramètres persistent. Si vous essayez de quitter la page avant qu'un paramètre ait été enregistré, un message contextuel indique qu'il y a des modifications non enregistrées.

Si un paramètre comporte deux options, une sélection de bouton radio s'affiche. Avec plus de deux options, un menu apparaît.

> **Remarque :**
>
> Si vous devez vérifier les paramètres que vous avez configurés, procédez comme suit.
>
> 1. Dans la console Citrix Endpoint Management, ouvrez stratégie **Configuration de GPO Windows** que vous souhaitez modifier.
> 2. Sous **Appareils** ou **Utilisateurs**, sélectionnez **Tous les paramètres**.
> 3. Triez le tableau par la colonne **État**, en ordre croissant. Toutes les stratégies non configurées affichent l'état **Non configuré**. Les stratégies que vous configurez sont répertoriées en premier.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

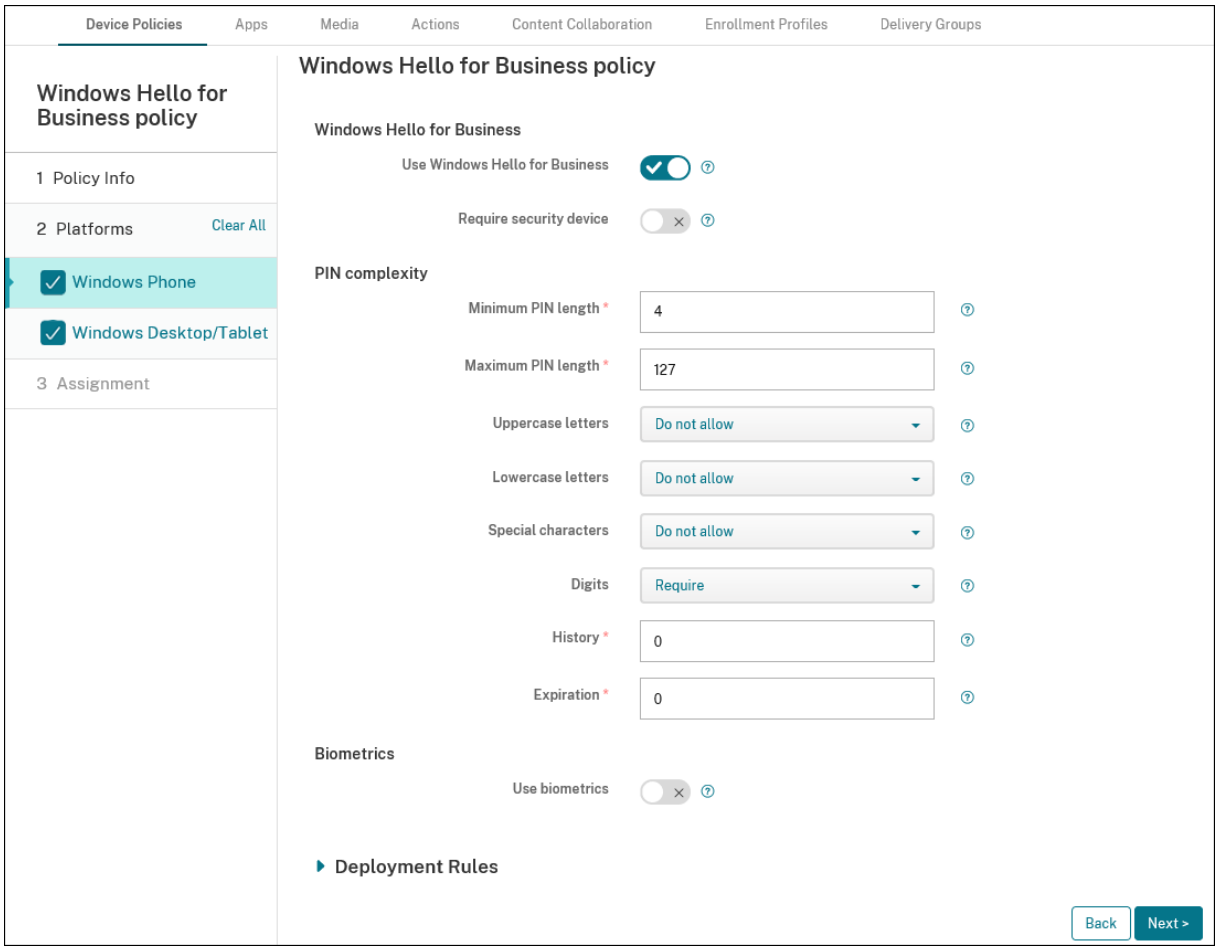
Stratégie Windows Hello Entreprise

February 21, 2022

Windows Hello Entreprise permet aux utilisateurs de se connecter aux appareils Windows à l'aide de leur compte Active Directory ou Azure Active Directory. La stratégie d'appareil Windows Hello Entreprise permet d'activer la fonctionnalité afin que les utilisateurs puissent provisionner Windows Hello Entreprise sur leur appareil. La stratégie permet également de configurer des limitations de code d'accès et d'autres fonctionnalités de sécurité.

Pour ajouter la stratégie Windows Hello Entreprise, accédez à **Configurer > Stratégies d'appareil**. Pour configurer ces paramètres :

Paramètres Windows Desktop/Tablet



- **Utiliser Windows Hello Entreprise :** cette option permet d'activer la fonctionnalité afin que les utilisateurs puissent provisionner Windows Hello Business sur leur appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Exiger dispositif de sécurité :** lorsque cette option est activée, les utilisateurs doivent disposer d'un module de plateforme sécurisée (TPM) pour se connecter.
- **Longueur minimale / maximale du code PIN :** longueur minimale et maximale des codes PIN des utilisateurs. La valeur par défaut de l'option **Longueur minimale du code PIN** est **4**. La valeur par défaut de l'option **Longueur maximale du code PIN** est **127**.
- **Majuscules**, **Minuscules**, **Caractères spéciaux :** sélectionnez l'option **Autoriser**, **Exiger** ou **Ne pas autoriser** pour chaque type de caractère. L'option par défaut est **Ne pas autoriser**.
- **Chiffres :** sélectionnez les options **Autoriser**, **Exiger** ou **Ne pas autoriser** pour les chiffres. L'option par défaut est **Exiger**.
- **Historique :** nombre de codes PIN utilisés précédemment que les utilisateurs ne peuvent pas réutiliser. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser tous les codes PIN utilisés précédemment.
- **Expiration :** nombre de jours avant qu'un utilisateur doive changer son code PIN. La valeur par défaut est **0**, ce qui signifie que les codes PIN n'expirent pas.
- **Utiliser biométrie :** cette option permet d'utiliser la biométrie à la place des codes PIN pour la connexion de l'utilisateur.

Ajouter des applications

March 1, 2024

L'ajout d'applications à Citrix Endpoint Management fournit des fonctionnalités de gestion d'application mobile (MAM). Citrix Endpoint Management vous aide à prendre en charge la mise à disposition des applications, l'attribution des licences logicielles, la configuration et la gestion du cycle de vie des applications.

Les applications compatibles MDX représentent un élément important dans la préparation de certains types d'applications pour leur distribution sur les machines utilisateur. Pour une introduction à MDX, consultez Composants Citrix Endpoint Management et Présentation du SDK MAM.

- Citrix recommande d'utiliser le SDK MAM pour les applications MDX. Vous pouvez également continuer à utiliser les applications MDX encapsulées jusqu'à ce que le MDX Toolkit ne soit plus pris en charge. Voir Fin de prise en charge.
- Vous ne pouvez pas utiliser le MDX Toolkit pour encapsuler les applications de productivité mobiles Citrix. Obtenez les fichiers MDX des applications de productivité mobile à partir des téléchargements Citrix.

Lorsque vous ajoutez des applications à la console Citrix Endpoint Management, vous effectuez les opérations suivantes :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Configurer les paramètres de l'application
- (Facultatif) Organiser les applications en catégories dans Citrix Secure Hub
- (Facultatif) Définir des workflows pour exiger une approbation avant d'autoriser les utilisateurs à accéder à une application
- Déployer des applications pour les utilisateurs

Cet article couvre les workflows généraux pour ajouter des applications. Consultez les articles suivants pour connaître les caractéristiques de la plate-forme :

- Distribuer des applications Android Enterprise
- Distribuer les applications Apple

> **Important :**
>
> Citrix Endpoint Management permet d'ajouter et de gérer jusqu'à 300 applications. Si vous dépassez cette limite, votre système devient instable.

Types et fonctionnalités d'applications

Le tableau suivant récapitule les types d'applications que vous pouvez déployer avec Citrix Endpoint Management.

Type d'application	Sources	Remarques	Voir
MDX	Applications iOS et Android que vous développez pour vos utilisateurs. Applications de productivité mobiles Citrix.	Développez des applications iOS ou Android avec le SDK MAM ou encapsulez-les avec le MDX Toolkit. Pour les applications de productivité mobiles, téléchargez les fichiers MDX du magasin public à partir des téléchargements Citrix. Ajoutez ensuite les applications à Citrix Endpoint Management.	Ajouter une application MDX

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Type d'application	Sources	Remarques	Voir
Magasin d' applications public	Applications gratuites ou payantes provenant de magasins d' applications publics tels que Google Play ou Apple App Store.	Chargez les applications, activez MDX sur les applications, puis ajoutez-les à Citrix Endpoint Management.	Ajouter une application d'un magasin d' applications public
Web et SaaS	Votre réseau interne (applications Web) ou un réseau public (SaaS).	Citrix Endpoint Management fournit une authentification unique mobile aux applications SaaS natives à partir d' appareils iOS et Android inscrits à MDM. Vous pouvez également utiliser les connecteurs d' application SAML (Security Assertion Markup Language).	Ajouter une application Web ou SaaS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Type d'application	Sources	Remarques	Voir
Entreprise	Applications privées, y compris les applications Win32, qui ne sont pas compatibles MDX. Applications Android Enterprise privées qui sont compatibles MDX. Les applications d'entreprise se trouvent dans des emplacements Content Delivery Network ou dans des serveurs Citrix Endpoint Management.	Ajoutez les applications à Citrix Endpoint Management.	Ajouter une application d'entreprise
Lien Web	Adresses Web Internet, adresses Web intranet ou applications Web qui ne nécessitent pas d'authentification unique.	Configurez les liens Web dans Citrix Endpoint Management.	Ajouter un lien Web

Lorsque vous planifiez la distribution d'applications, tenez compte des fonctionnalités suivantes :

- À propos des installations silencieuses
- À propos des applications obligatoires et facultatives
- À propos des catégories d'applications
- Fournir des applications d'entreprise à partir du CDN Citrix
- Activer les applications Microsoft 365
- Appliquer les workflows
- Personnalisation du magasin d'applications et de Citrix Secure Hub
- Citrix Virtual Apps and Desktops via le magasin d'applications

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

À propos des installations silencieuses

Citrix prend en charge l'installation silencieuse et la mise à niveau d'applications iOS, Android Enterprise et Samsung. Une installation silencieuse signifie que les utilisateurs ne sont pas invités à installer les applications que vous déployez sur l'appareil. Les applications s'installent automatiquement en arrière-plan.

Conditions préalables requises pour une installation silencieuse :

- Pour iOS, placez l'appareil iOS géré en mode supervisé. Pour plus d'informations, consultez la section Stratégie Importer le profil iOS et macOS.
- Pour Android Enterprise, les applications s'installent sur le profil de travail Android sur l'appareil. Pour de plus amples informations, consultez la section Android Enterprise.
- Pour les appareils Samsung, activez Samsung Knox sur l'appareil.

  Pour ce faire, vous devez définir la stratégie de clé de licence MDM Samsung pour générer des codes d'accès aux licences Knox et Samsung ELM. Pour de plus amples informations, consultez la section Stratégies de clé de licence MDM Samsung.

À propos des applications obligatoires et facultatives

Lorsque vous ajoutez des applications à un groupe de mise à disposition, vous devez choisir si elles sont facultatives ou requises. Citrix recommande le déploiement des applications comme **requises**.

- Les applications requises s'installent silencieusement sur les appareils utilisateur, ce qui minimise l'interaction. L'activation de cette fonctionnalité permet également aux applications de se mettre à jour automatiquement.
- Les applications facultatives permettent aux utilisateurs de choisir les applications à installer, mais les utilisateurs doivent initier l'installation manuellement via Citrix Secure Hub.

Pour les applications marquées comme requises, les utilisateurs peuvent recevoir les mises à jour plus rapidement dans certaines situations, par exemple :

- Vous chargez une nouvelle application et la marquez comme requise.
- Vous marquez une application existante comme requise.
- Un utilisateur supprime une application requise.
- Une mise à jour de Citrix Secure Hub est disponible.

Configuration requise pour le déploiement automatique des applications requises

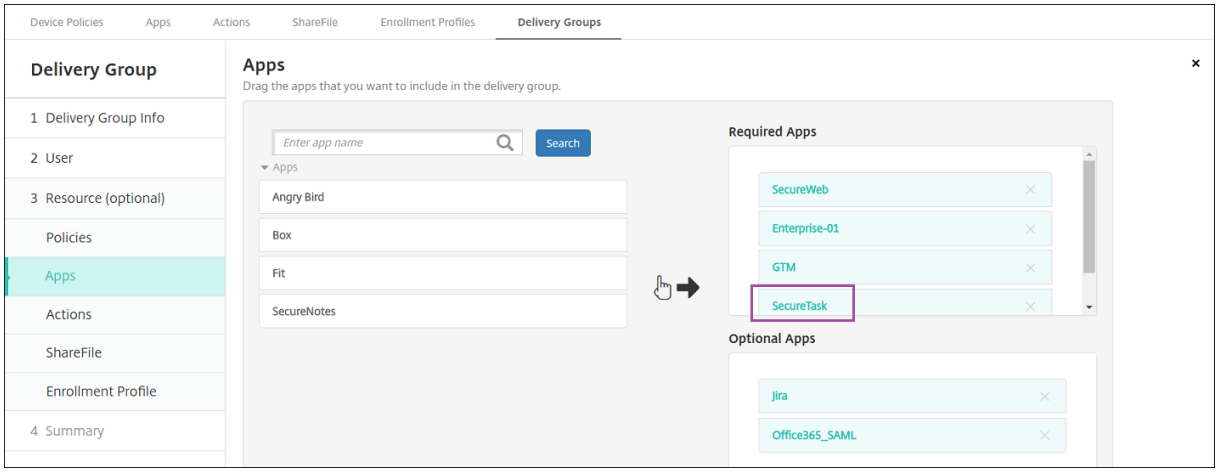
- Citrix Secure Hub 10.5.15 pour iOS et 10.5.20 pour Android (versions minimales)

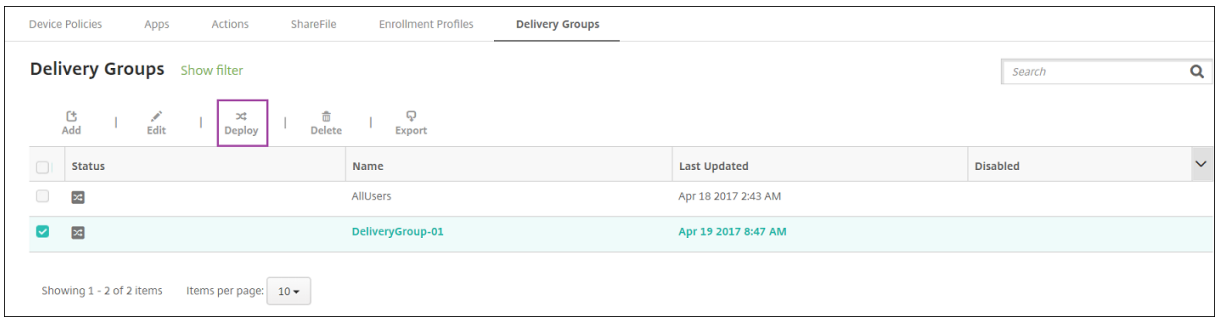
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- SDK MAM ou MDX Toolkit 10.6 (version minimale)
- Une fois que vous avez mis à niveau Citrix Endpoint Management et Citrix Secure Hub : les utilisateurs dotés d'appareils inscrits doivent se déconnecter, puis se connecter à Citrix Secure Hub pour obtenir les mises à jour du déploiement des applications requises.

Exemples

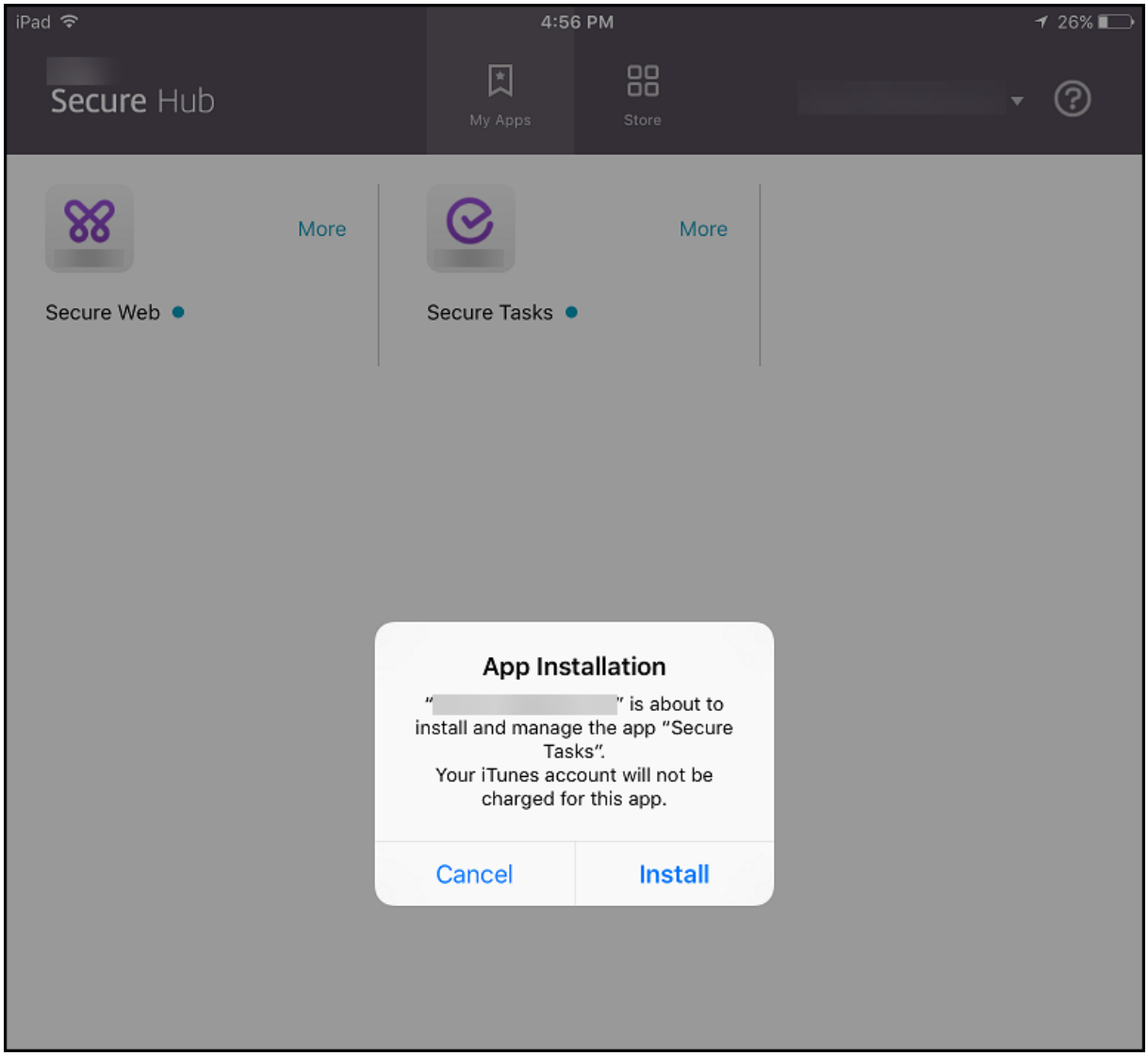
Les exemples suivants expliquent la séquence d'ajout d'une application nommée Secure Tasks à un groupe de mise à disposition et de déploiement du groupe de mise à disposition.

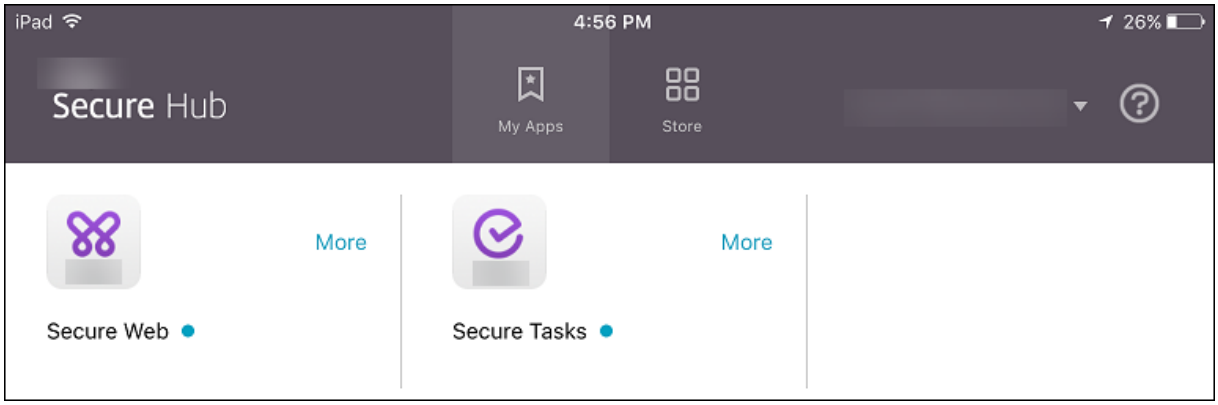




Une fois l'application Secure Tasks déployée vers l'appareil de l'utilisateur, Citrix Secure Hub invite l'utilisateur à installer l'application.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.





Important :

Les applications MDX requises, y compris les applications d'entreprise et les applications de magasin d'applications publiques, sont immédiatement mises à niveau. Cette mise à niveau se

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> produit même si vous configurez une stratégie MDX pour une période de grâce de mise à jour d' application et que l'utilisateur choisit de mettre à niveau l'application ultérieurement.

Workflow des applications iOS requises pour les applications d'entreprise et de magasin public

1. Déployer l'application de productivité mobile lors de l'inscription initiale. L'application requise est installée sur l'appareil.
2. Mettre à jour l'application dans la console Citrix Endpoint Management.
3. Utiliser la console Citrix Endpoint Management pour déployer les applications requises.
4. L'application sur l'écran d'accueil est mise à jour. Et, pour les applications de magasin public, la mise à niveau démarre automatiquement. Les utilisateurs ne sont pas invités à procéder à la mise à jour.
5. Les utilisateurs ouvrent l'application à partir de l'écran d'accueil. Les applications se mettent à niveau immédiatement, même si vous définissez une période de grâce de mise à jour des applications et que l'utilisateur choisit de mettre à niveau l'application plus tard.

Workflow des applications Android requises pour les applications d'entreprise

1. Déployer l'application de productivité mobile lors de l'inscription initiale. L'application requise est installée sur l'appareil.
2. Utiliser la console Citrix Endpoint Management pour déployer les applications requises.
3. L'application est mise à niveau. (Les appareils Nexus invitent à installer les mises à jour, mais les appareils Samsung effectuent une installation silencieuse).
4. Les utilisateurs ouvrent l'application à partir de l'écran d'accueil. Les applications se mettent à niveau immédiatement, même si vous définissez une période de grâce de mise à jour des applications et que l'utilisateur choisit de mettre à niveau l'application plus tard. (Les appareils Samsung effectuent une installation silencieuse.)

Workflow des applications Android requises pour les applications de magasin public

1. Déployer l'application de productivité mobile lors de l'inscription initiale. L'application requise est installée sur l'appareil.
2. Mettre à jour l'application dans la console Citrix Endpoint Management.
3. Utiliser la console Citrix Endpoint Management pour déployer les applications requises. Ou, ouvrir le magasin Citrix Secure Hub sur l'appareil. L'icône de mise à jour est affichée dans le magasin.
4. La mise à niveau démarre automatiquement. (Les appareils Nexus invitent les utilisateurs à installer la mise à jour.)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Ouvrez l'application à partir de l'écran d'accueil. L'application est mise à niveau. Les utilisateurs ne sont pas invités à procéder à la mise à jour après une période de grâce. (Les appareils Samsung effectuent une installation silencieuse.)

Désinstaller une application lorsque celle-ci est configurée selon les besoins

Vous pouvez permettre aux utilisateurs de désinstaller une application configurée selon les besoins. Accédez à **Configurer> Groupes de mise à disposition** et déplacez l'application de la zone **Applications requises** vers la zone **Applications facultatives**.

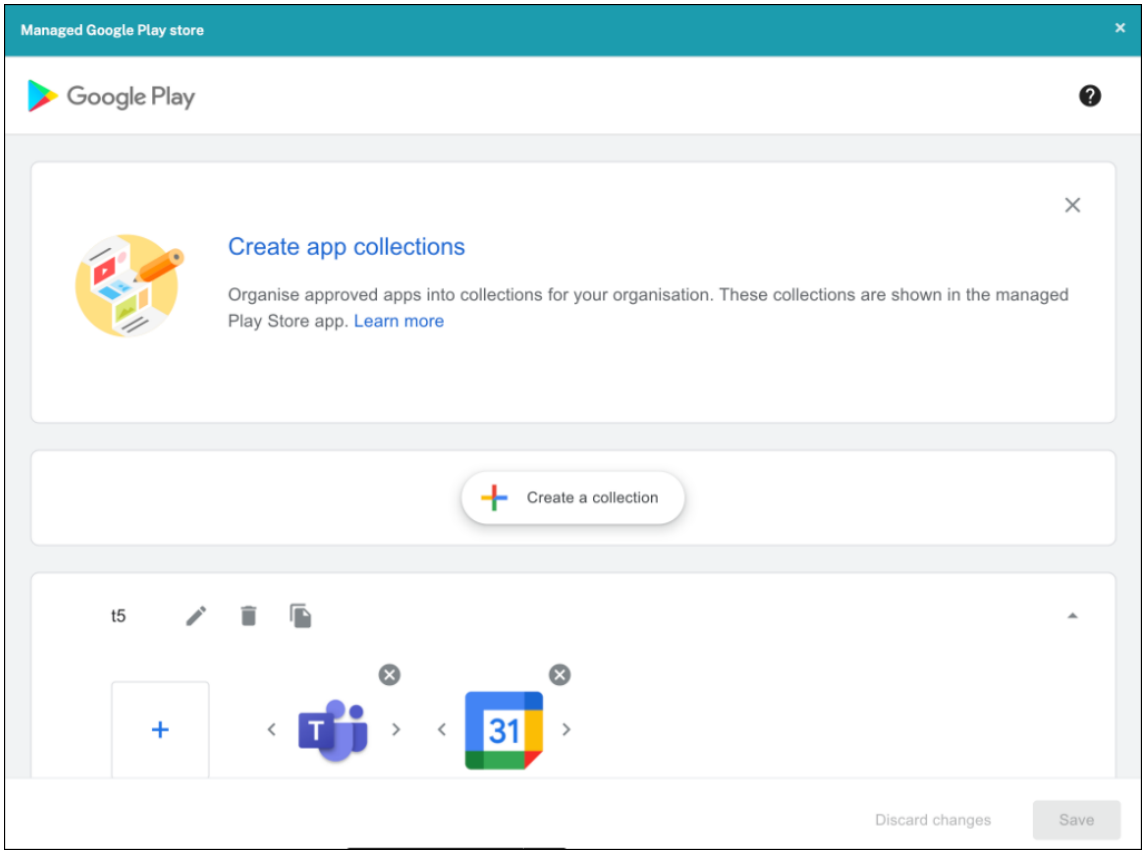
Recommandation : utilisez un groupe de mise à disposition spécial pour modifier temporairement une application et la passer en application facultative afin de permettre à des utilisateurs spécifiques de la désinstaller. Vous pouvez ensuite modifier une application requise existante et la passer en application facultative, déployer l'application sur ce groupe de mise à disposition, puis désinstaller l'application à partir de ces appareils. Si vous souhaitez ensuite que les futures inscriptions de ce groupe de mise à disposition disposent de l'application, vous pouvez redéfinir l'application et la passer en application requise.

Organiser les applications (Android Enterprise)

Lorsque les utilisateurs se connectent à Citrix Secure Hub, ils obtiennent une liste des applications, des liens Web et des magasins que vous avez configurés dans Citrix Endpoint Management. Dans Android Enterprise, vous pouvez organiser ces applications en collections afin de permettre aux utilisateurs d'accéder uniquement à certaines applications, magasins ou liens Web. Par exemple, vous créez une collection Finance, puis vous y ajoutez des applications ayant trait uniquement au secteur de la finance. Ou vous pouvez configurer une collection Ventes à laquelle vous attribuez des applications de ventes.

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications > Organiser les applications**. La fenêtre **Google Play Store d'entreprise** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Cliquez sur **Créer une collection** et sélectionnez les applications à ajouter à cette collection.
3. Lorsque vous avez terminé d'ajouter des collections, cliquez sur **Enregistrer**.

> **Remarque :**
>
> les administrateurs informatiques doivent approuver une application avant de pouvoir l'ajouter à une collection dans la fenêtre Google Play d'entreprise. Un administrateur informatique peut approuver une application en accédant à https://play.google.com/work. Dans une prochaine version, vous n'aurez pas besoin d'approuver une application avant de l'ajouter à une collection.

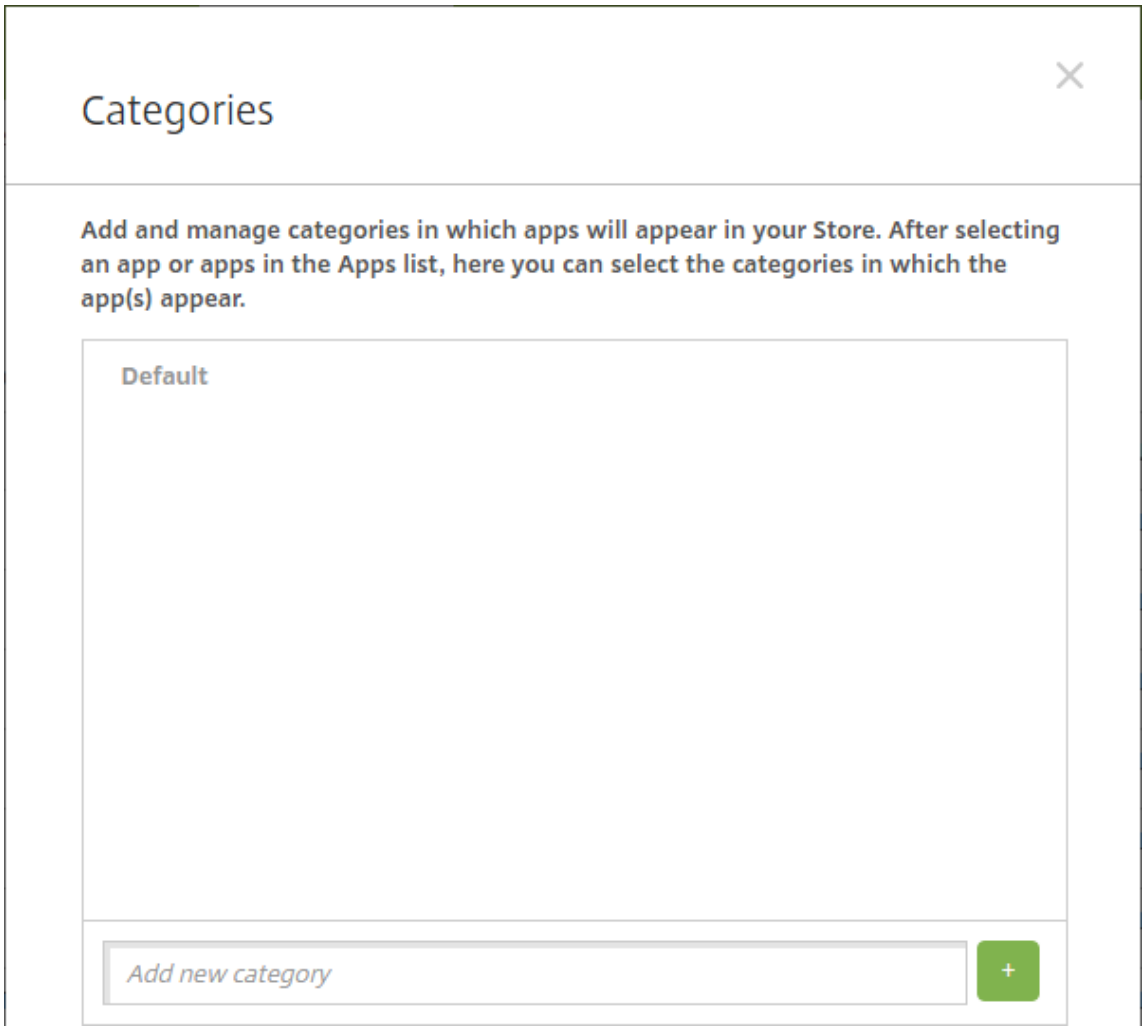
À propos des catégories d'applications (iOS et MDX)

Lorsque les utilisateurs se connectent à Citrix Secure Hub, ils obtiennent une liste des applications, des liens Web et des magasins que vous avez configurés dans Citrix Endpoint Management. Dans iOS or MDX, vous pouvez utiliser les catégories d'applications pour permettre aux utilisateurs d'accéder uniquement à certaines applications, magasins ou liens Web. Par exemple, il est possible de créer une catégorie Finance et d'y ajouter des applications ayant trait uniquement au secteur de la finance. Ou vous pouvez configurer une catégorie Ventes à laquelle vous attribuez des applications de ventes.

Lorsque vous ajoutez ou modifiez une application, un lien Web ou un magasin, vous pouvez ajouter l'application à l'une ou plusieurs des catégories configurées.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

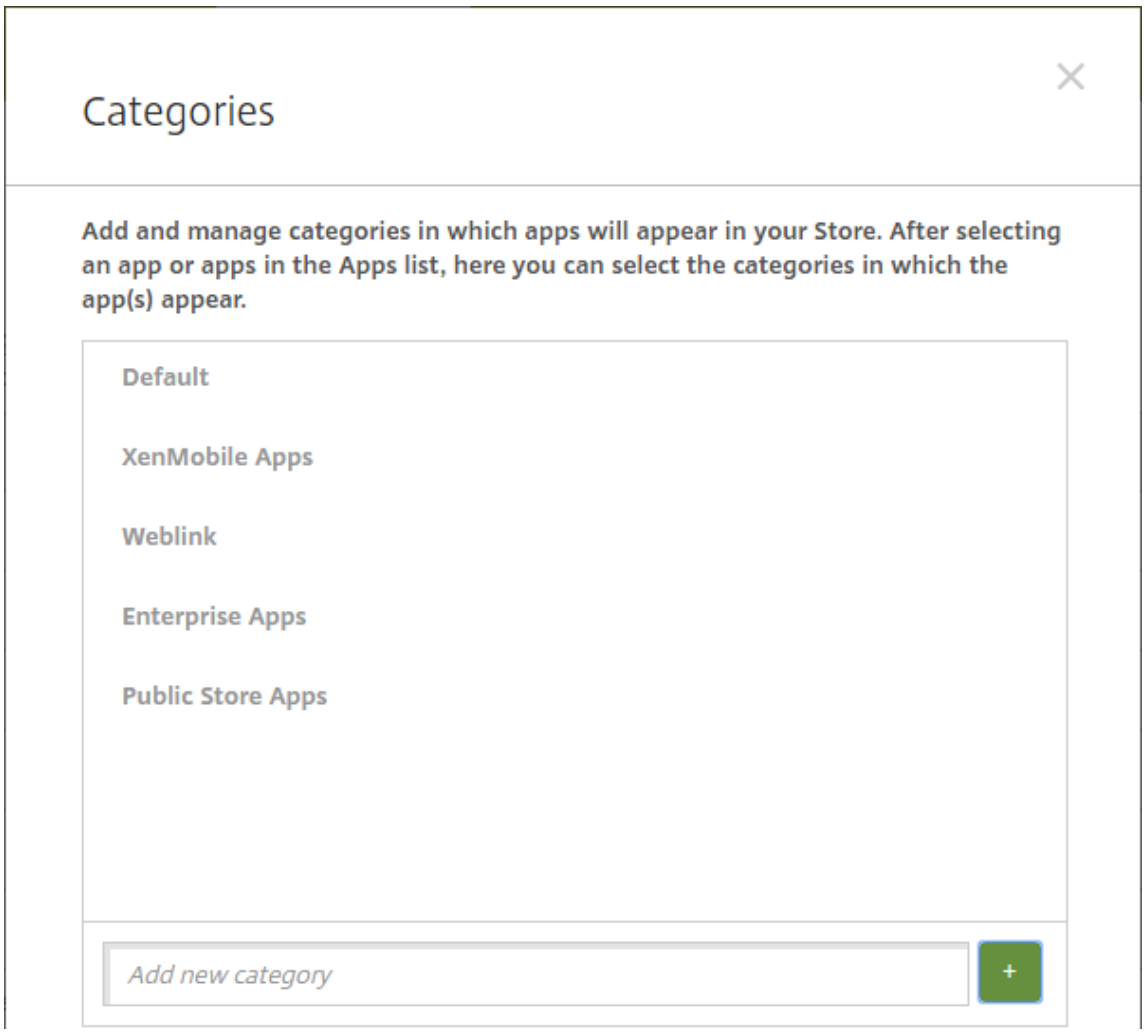
1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications > Catégorie**. La boîte de dialogue **Catégories** s'affiche.



2. Pour chaque catégorie que vous voulez ajouter, procédez comme suit :

   - Tapez le nom de la catégorie que vous souhaitez ajouter dans le champ **Ajouter une nouvelle catégorie** en bas de la boîte de dialogue. Par exemple, vous pouvez entrer Applications d'entreprise pour créer une catégorie pour les applications d'entreprise.
   - Cliquez sur le signe plus (+) pour ajouter la catégorie. La nouvelle catégorie est ajoutée et s'affiche dans la boîte de dialogue **Catégories**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Lorsque vous avez terminé d'ajouter des catégories, fermez la boîte de dialogue **Catégories**.
4. Sur la page **Applications**, vous pouvez placer une application existante dans une nouvelle catégorie.
   - Sélectionnez l'application que vous souhaitez classer.
   - Cliquez sur **Modifier**. La page **Informations sur l'application** s'affiche.
   - Dans la liste **Catégorie d'application**, appliquez la nouvelle catégorie en sélectionnant la case à cocher appropriée. Désélectionnez les cases à cocher pour les catégories que vous ne souhaitez pas appliquer à l'application.
   - Cliquez sur l'onglet **Attribution de groupes de mise à disposition** ou cliquez sur **Suivant** sur chacune des pages suivantes pour compléter les autres pages de configuration de l'application.
   - Cliquez sur **Enregistrer** sur la page **Attribution de groupes de mise à disposition** pour appliquer la catégorie. La nouvelle catégorie est appliquée à l'application et l'application s'affiche dans le tableau **Applications**.

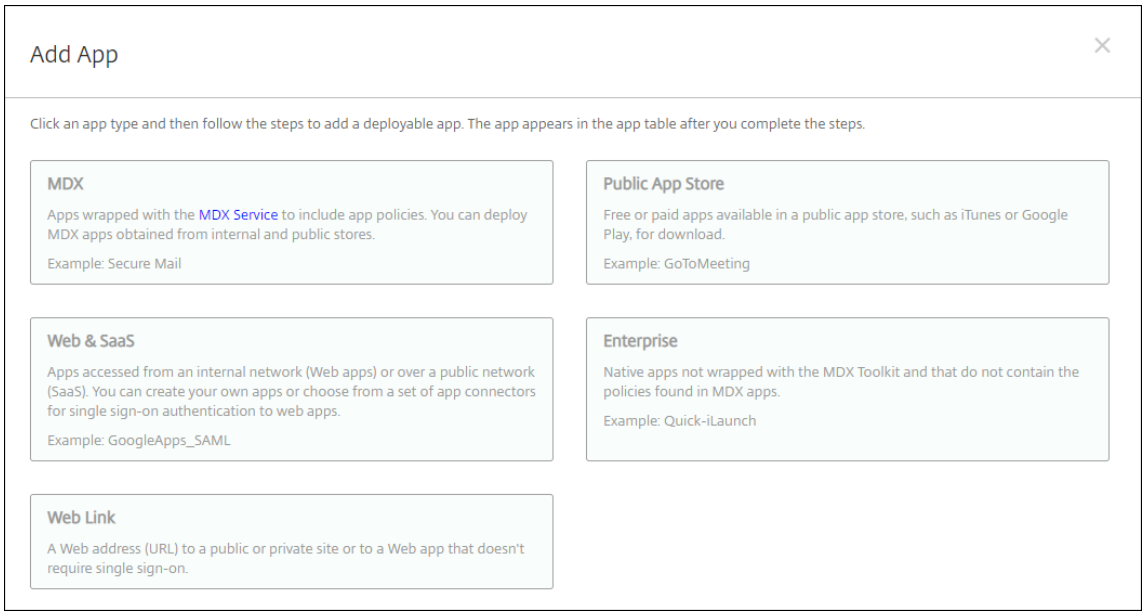
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ajouter une application MDX

Lorsque vous recevez un fichier MDX pour une application iOS ou Android, vous pouvez charger l'application dans Citrix Endpoint Management. Après le chargement de l'application, vous pouvez configurer les détails de l'application et les paramètres de stratégie. Pour plus d'informations sur les stratégies applicatives disponibles pour chaque type de plate-forme, consultez :

- Présentation du SDK MAM
- Synopsis des stratégies MDX

1. Pour les applications de productivité mobiles Citrix, téléchargez les fichiers MDX du magasin public : accédez à https://www.citrix.com/downloads. Accédez à **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.
2. Pour les autres types d'applications MDX, obtenez le fichier MDX.
3. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications > Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



4. Cliquez sur **MDX**. La page **Informations sur l'application MDX** s'affiche.
5. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom pour décrire l'application. Ce nom apparaît sous **Nom de l'application** dans le tableau **Applications**.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

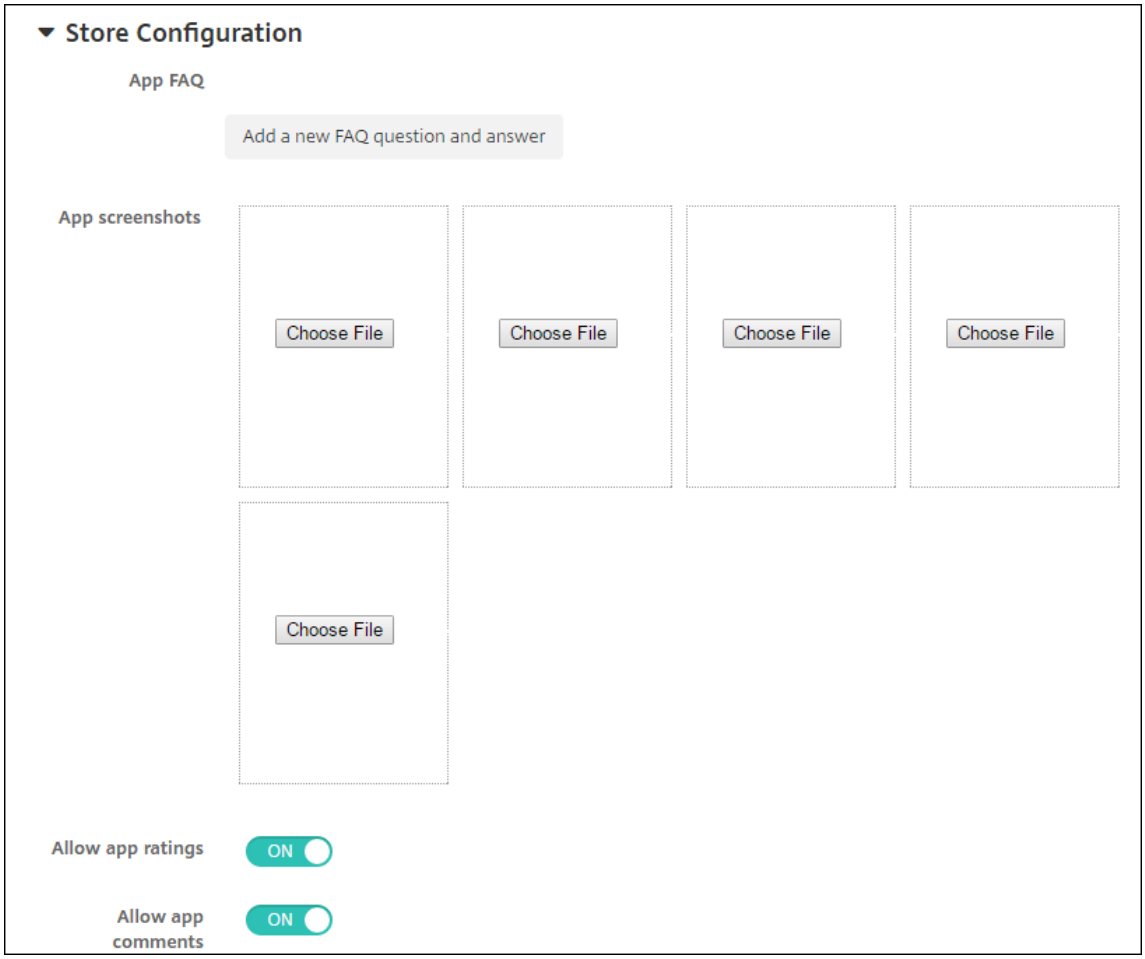
6. Cliquez sur **Suivant**. La page **Plates-formes d'applications** s'affiche.
7. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.
8. Pour sélectionner un fichier MDX à charger, cliquez sur **Charger** et accédez à l'emplacement du fichier.
9. Sur la page **Détails de l'application**, configurez les paramètres suivants :
   - **Nom du fichier :** entrez le nom du fichier associé à l'application.
   - **Description de l'application :** entrez une description pour l'application.
   - **Version de l'application :** si vous le souhaitez, entrez le numéro de version de l'application.
   - **ID de package :** entrez l'ID du package de l'application provenant du Google Play Store d'entreprise.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   - **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
   - **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou les modèles d'appareils qui ne peuvent pas exécuter l'application.
   - **Supprimer l'application si le profil MDM est supprimé :** sélectionnez cette option si vous souhaitez supprimer l'application d'un appareil lorsque le profil MDM est supprimé La valeur par défaut est **Activé**.
   - **Empêcher la sauvegarde des données d'application :** sélectionnez cette option si vous souhaitez empêcher les utilisateurs de sauvegarder les données de l'application sur les appareils iOS. La valeur par défaut est **Activé**.
   - **Suivi du produit :** spécifiez le suivi du produit que vous souhaitez transférer aux appareils iOS. Si vous avez un suivi conçu à des fins de test, vous pouvez le sélectionner et l'affecter à vos utilisateurs. La valeur par défaut est **Production**.
   - **Forcer l'application à être gérée :** lors de l'installation d'une application non gérée, sélectionnez cette option pour spécifier si vous souhaitez inviter les utilisateurs à autoriser l'application à être gérée sur les appareils non supervisés. La valeur par défaut est **Activé**.
   - **Application déployée via l'achat en volume :** indiquez si vous souhaitez déployer l'application à l'aide de l'achat en volume d'Apple. Si vous déployez une version MDX de l'application et que vous utilisez l'achat en volume pour déployer l'application lorsque cette option est définie sur **Activé**, Citrix Secure Hub affiche uniquement l'instance d'achat en volume. La valeur par défaut est **Off**.
10. Configurez les **stratégies MDX**. Les stratégies MDX varient selon la plate-forme et incluent des options dans des domaines de stratégie tels que l'authentification, la sécurité de l'appareil et

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

les restrictions applicatives. Dans la console, les stratégies ont une info-bulle qui décrit chacune d'entre elles.

11. Configurez les règles de déploiement. Pour plus d'informations, consultez la section Configurer les règles de déploiement.

12. Développez **Configuration du magasin**.

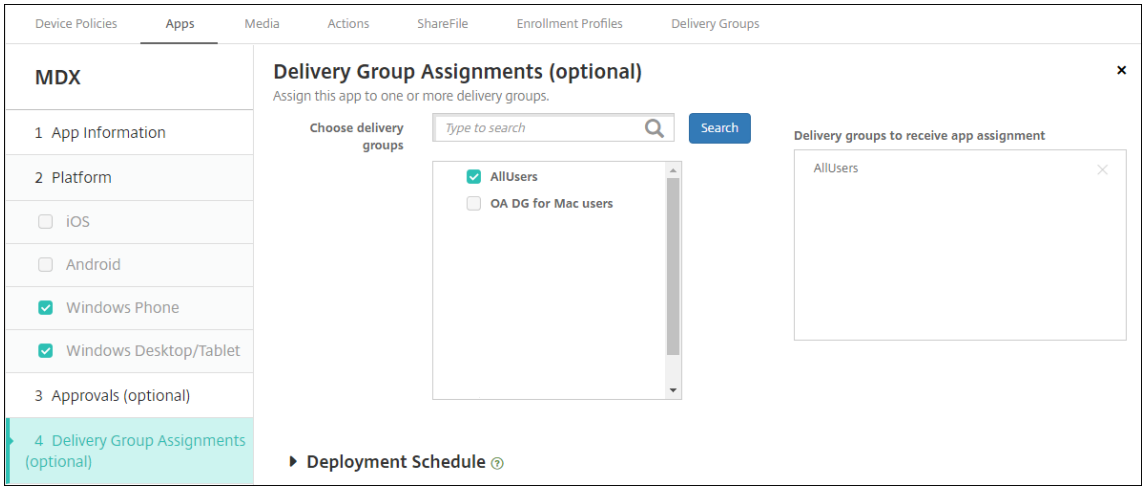


Si vous le souhaitez, vous pouvez configurer les paramètres suivants :

- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.
- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des commentaires sur l'application dans l'App Store.

13. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



14. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

15. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

    - **Déployer :** choisissez cette option si vous souhaitez déployer l'application sur les appareils. La valeur par défaut est **Activé**.
    - **Calendrier de déploiement :** choisissez l'option **Maintenant** ou **Plus tard** pour déployer l'application. Si vous sélectionnez **Plus tard**, configurez une date et une heure pour déployer l'application. La valeur par défaut est **Maintenant**.
    - **Conditions de déploiement :** choisissez **À chaque connexion** pour déployer l'application chaque fois que l'appareil se connecte. Choisissez **Uniquement lorsque le déploiement précédent a échoué** pour déployer l'application lorsque l'appareil n'a pas réussi à recevoir l'application. L'option par défaut est **À chaque connexion**.

    L'option **Déployer pour les connexions permanentes** s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

    L'option de connexion permanente :

    - N'est pas disponible pour les appareils iOS.
    - N'est pas disponible pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec la version 10.18.19 ou ultérieure
    - N'est pas recommandée pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec une version antérieure à la version 10.18.19

    Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

16. Cliquez sur **Enregistrer**.

Ajouter une application d'un magasin d'applications public

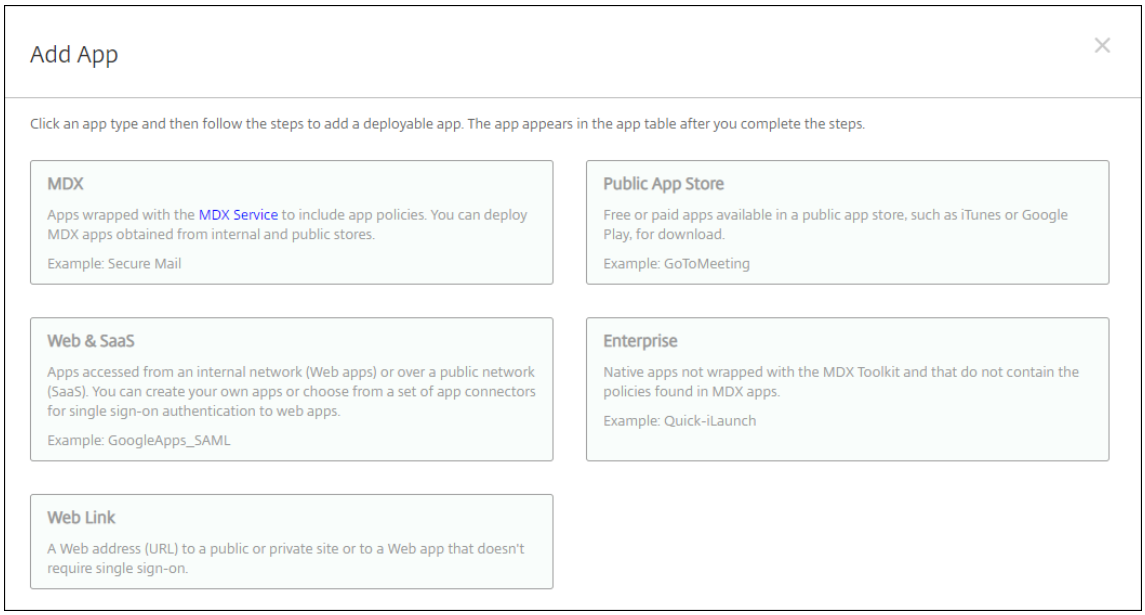
Vous pouvez ajouter des applications gratuites ou payantes à Citrix Endpoint Management qui sont disponibles dans un magasin d'applications public, tel que l'Apple App Store ou Google Play.

Vous pouvez configurer des paramètres afin de récupérer les noms et descriptions des applications dans l'App Store d'Apple. Lorsque vous récupérez les informations d'application dans le magasin, Citrix Endpoint Management remplace le nom et la description existants. Configurez manuellement les informations de l'application Google Play Store.

Lorsque vous ajoutez une application payante provenant d'un magasin d'applications public pour Android Enterprise, vous pouvez vérifier l'état de la licence d'achat groupé. Cet état représente le nombre total de licences disponibles, le nombre en cours d'utilisation et l'adresse e-mail de chaque utilisateur qui consomme des licences. Le plan Achat groupé pour Android Enterprise simplifie la recherche, l'achat et la distribution d'applications et d'autres données en bloc.

Configurez les informations de l'application et choisissez les plates-formes sur lesquelles les mettre à disposition :

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications > Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



2. Cliquez sur **Magasin d'applications public**. La page **Informations sur l'application** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Ce nom apparaît sous **Nom de l'application** dans le tableau **Applications**.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.
4. Cliquez sur **Suivant**. La page **Plates-formes d'applications** s'affiche.
5. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

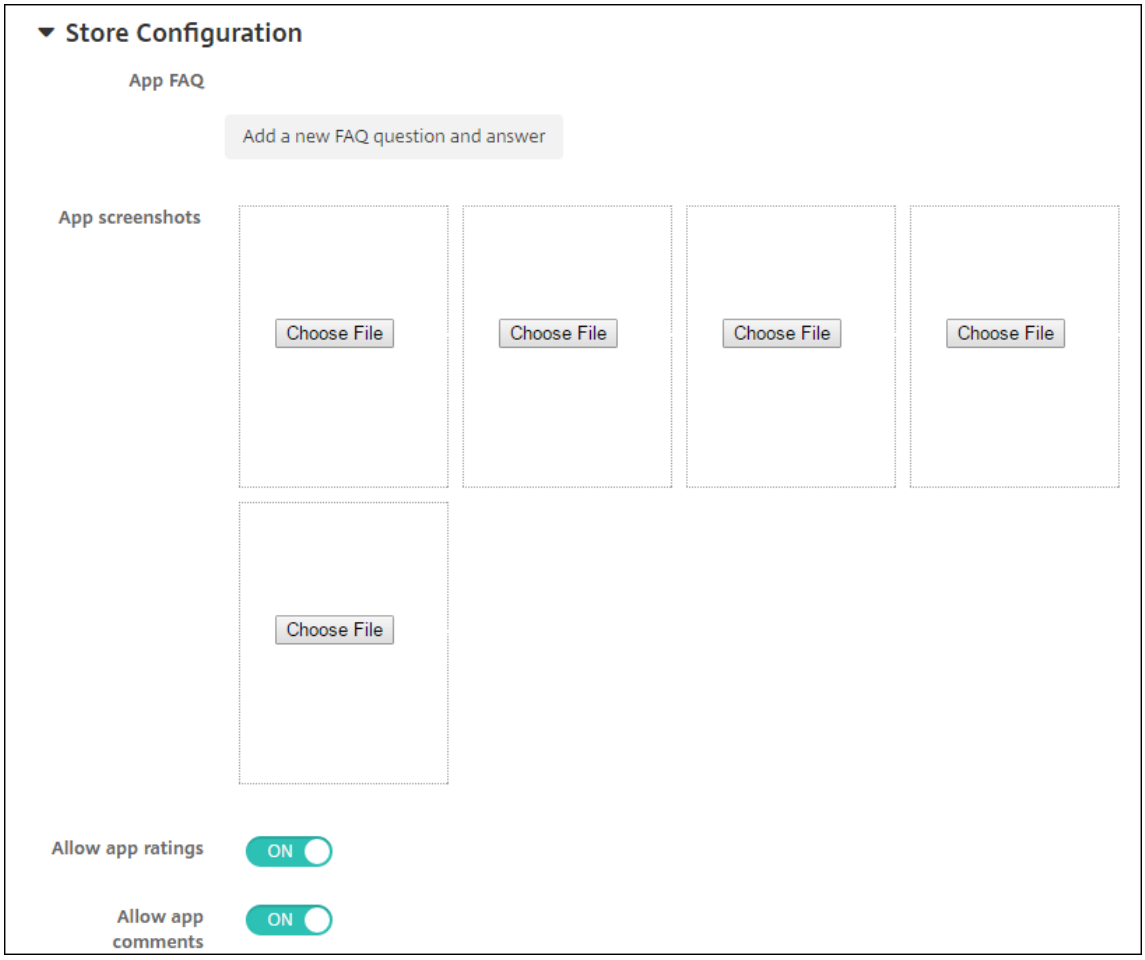
Ensuite, vous configurez les paramètres de l'application pour chaque plate-forme. Consultez :

- Configurer les paramètres d'application pour les applications Google Play
- Applications gérées du magasin d'applications
- Configurer les paramètres applicatifs pour les applications iOS

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, définissez les règles de déploiement de cette plate-forme et la configuration du magasin d'applications.

1. Configurez les règles de déploiement. Pour plus d'informations, consultez la section Configurer les règles de déploiement.
2. Développez **Configuration du magasin**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Si vous le souhaitez, vous pouvez configurer les paramètres suivants :

- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.
- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des commentaires sur l'application dans l'App Store.

Configurer les paramètres d'application pour les applications Google Play

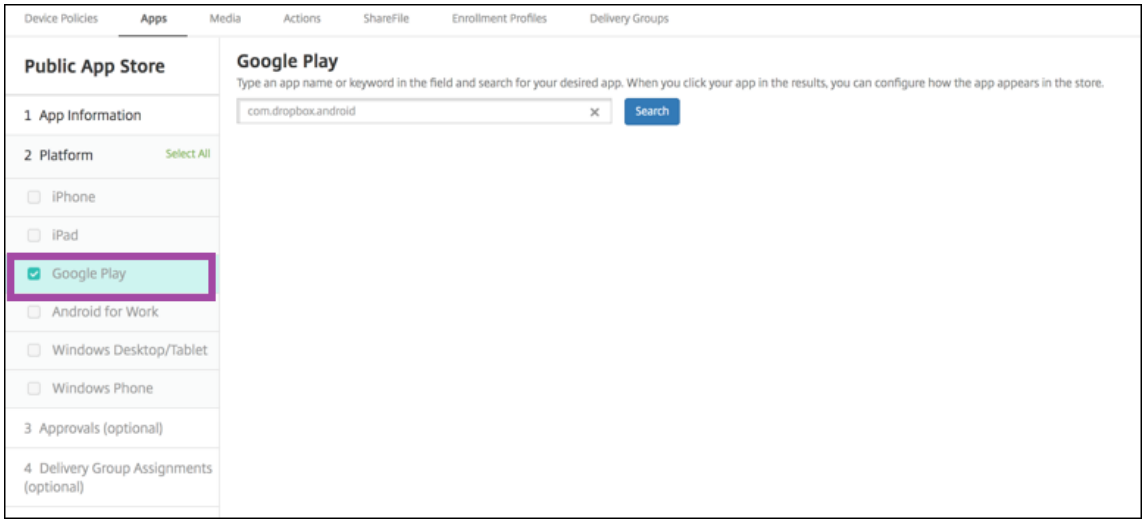
> **Remarque** pour rendre toutes les applications du Google Play Store accessibles depuis le Google Play d'entreprise, utilisez la propriété de serveur **Accéder à toutes les applications du Google Play Store d'entreprise**. (Consultez Propriétés du serveur.) La définition de cette propriété sur **true** autorise tous les utilisateurs d'Android Entreprise à accéder

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

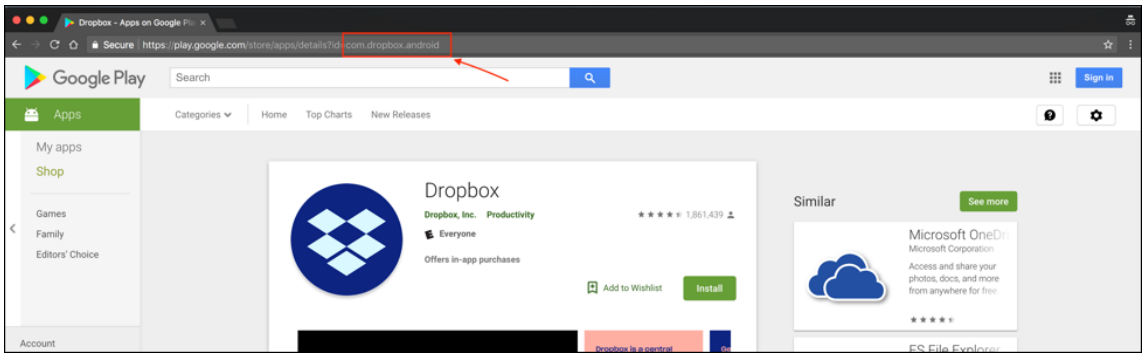
> aux applications du Google Play Store public. Vous pouvez ensuite utiliser la stratégie Restrictions pour contrôler l'accès à ces applications.

La configuration des paramètres des applications Google Play Store nécessite des étapes différentes de celles des applications d'autres plates-formes. Configurez manuellement les informations de l'application Google Play Store.

1. Assurez-vous que **Google Play** est sélectionné sous **Plates-formes**.

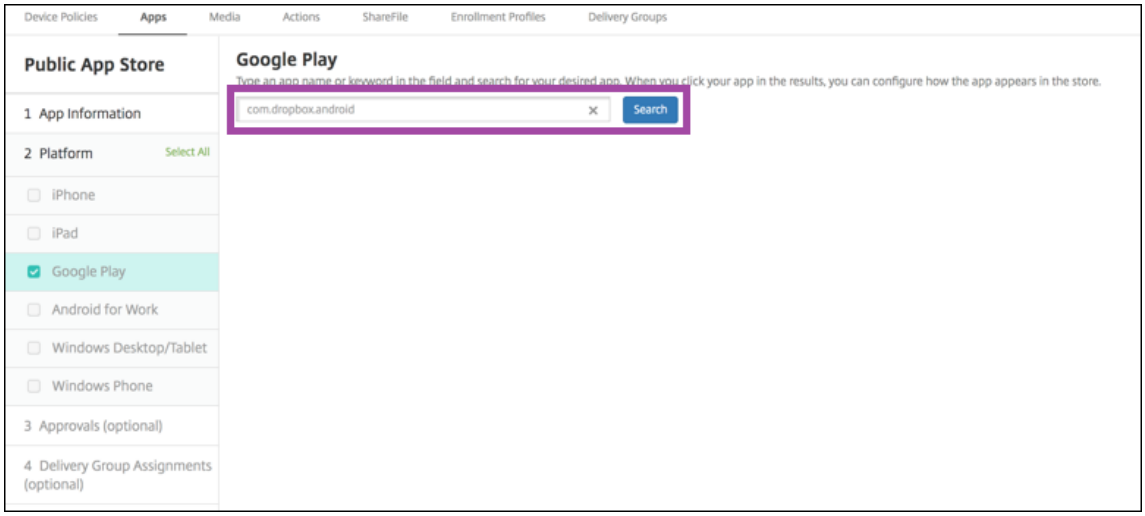


2. Accédez à Google Play. À partir de Google Play, copiez l'ID de package. L'ID se trouve dans l'URL de l'application.

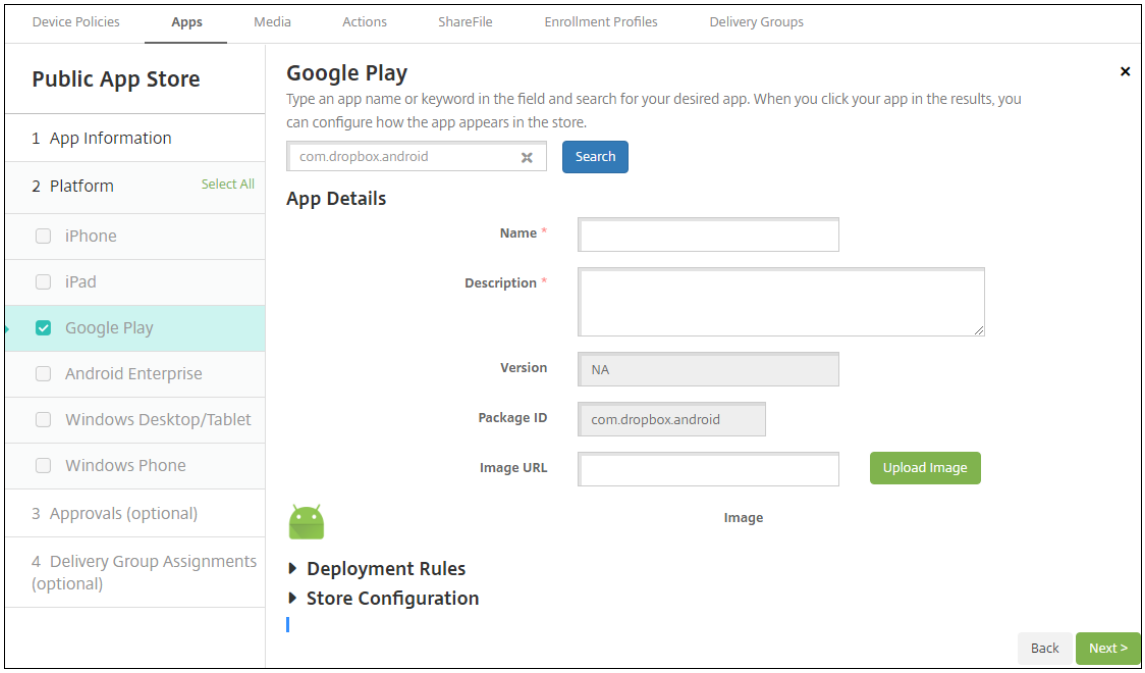


3. Lorsque vous ajoutez une application provenant d'un magasin d'applications public dans la console Citrix Endpoint Management, collez l'ID de package dans la barre de recherche. Cliquez sur **Search**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Si l'ID de package est valide, une interface utilisateur s'affiche pour vous permettre d'entrer les détails de l'application.



5. Vous pouvez configurer l'URL pour que l'image apparaisse avec l'application dans le magasin. Pour utiliser l'image de Google Play :

   a) Accédez à Google Play. Cliquez avec le bouton droit sur l'image de l'application et copiez l'adresse de l'image.

   b) Collez l'adresse de l'image dans le champ **URL d'image**.

   c) Cliquez sur **Charger image**. L'image apparaît à côté de **Image**.

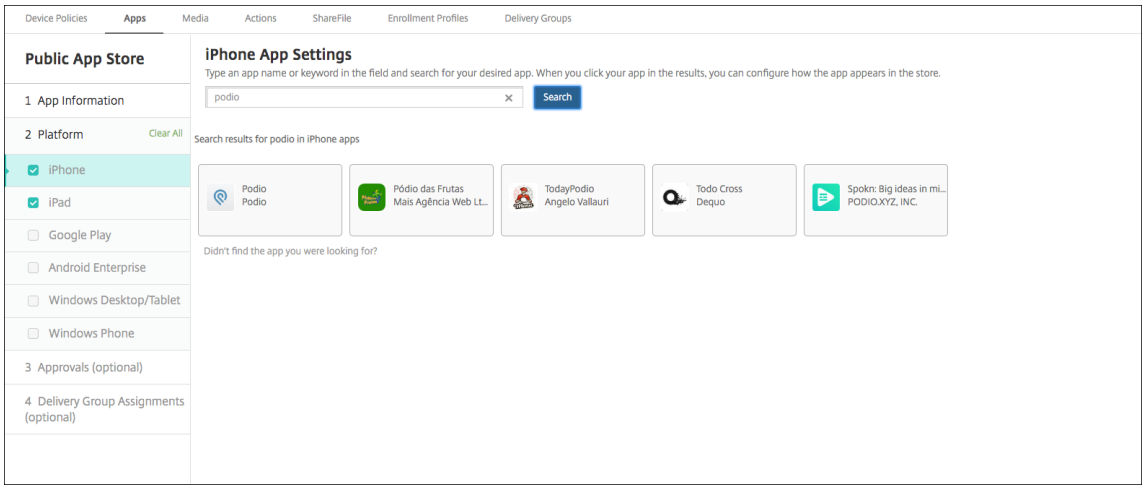
Si vous ne configurez pas d'image, l'image Android générique apparaît avec l'application.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

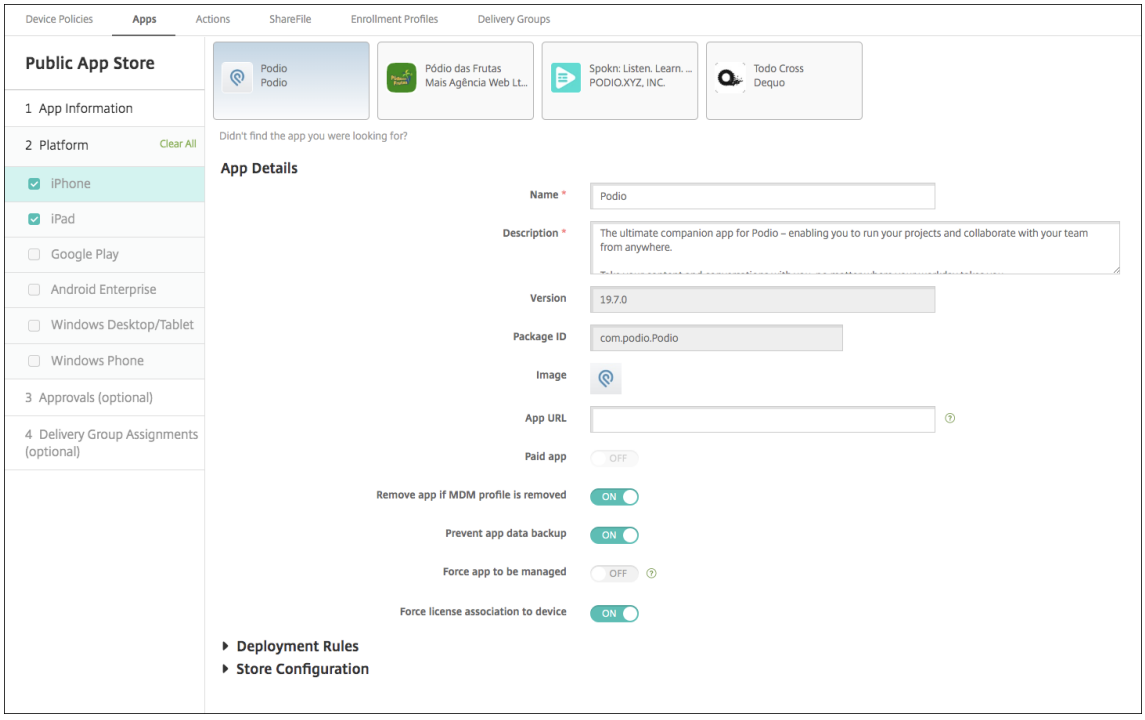
Configurer les paramètres applicatifs pour les applications iOS

1. Entrez le nom de l'application dans la zone de recherche et cliquez sur **Rechercher**. Les applications correspondant aux critères de recherche s'affichent. Les applications correspondant aux critères de recherche s'affichent.

   La figure suivante illustre le résultat de la recherche pour **podio** dans les applications de l'iPhone.



2. Cliquez sur chaque application que vous souhaitez ajouter.
3. Les champs **Détails sur l'application** sont ensuite pré-remplis avec les informations relatives à l'application choisie (y compris le nom, la description, le numéro de version et l'image).



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

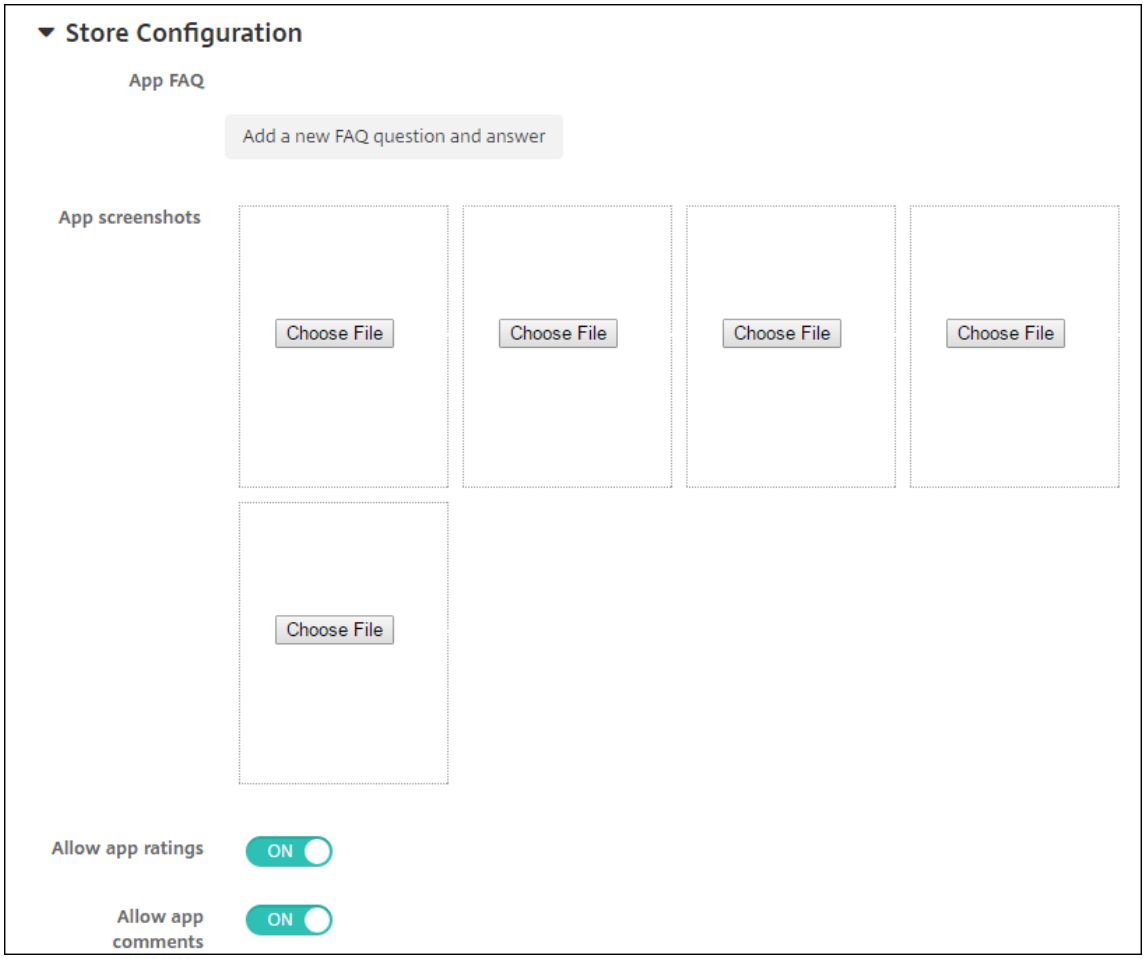
4. Pour configurer ces paramètres :

   - Si nécessaire, modifiez le nom et la description de l'application.
   - **URL de l'application :** entrez une liste d'URL séparées par des virgules pour lancer vos applications à partir de l'application Citrix Workspace. Ce champ est uniquement disponible pour les appareils iPhone et iPad.
   - **Application payante :** ce champ est préconfiguré et ne peut pas être modifié.
   - **Supprimer l'application si le profil MDM est supprimé :** sélectionnez cette option si vous souhaitez supprimer l'application lorsque le profil MDM est supprimé. La valeur par défaut est **Activé**.
   - **Empêcher la sauvegarde des données d'application :** sélectionnez cette option si vous souhaitez empêcher l'application de sauvegarder les données. La valeur par défaut est **Activé**.
   - **Suivi du produit :** spécifiez le suivi du produit que vous souhaitez transférer aux appareils utilisateur. Si vous avez un suivi conçu à des fins de test, vous pouvez le sélectionner et l'affecter à vos utilisateurs. La valeur par défaut est **Production**.
   - **Forcer l'application à être gérée :** lors de l'installation d'une application non gérée, sélectionnez cette option pour spécifier si vous souhaitez inviter les utilisateurs à autoriser l'application à être gérée sur les appareils non supervisés. La valeur par défaut est **Désactivé**. Pour les appareils iOS inscrits via l'inscription des utilisateurs, Citrix Endpoint Management n'applique pas ce paramètre et n'invite pas les utilisateurs à autoriser la gestion des applications.
   - **Forcer l'association de licence avec l'appareil :** sélectionnez cette option si vous voulez associer une application (développée en association avec un appareil) à un appareil plutôt qu'à un utilisateur. Si l'application que vous avez choisie ne prend pas en charge l'attribution à un appareil, vous ne pouvez pas modifier ce paramètre.

5. Configurez les règles de déploiement. Pour plus d'informations, consultez la section Configurer les règles de déploiement.

6. Développez **Configuration du magasin**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Si vous le souhaitez, vous pouvez configurer les paramètres suivants :

- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.
- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des commentaires sur l'application dans l'App Store.

7. Pour iPhone ou iPad, développez **Achat en volume**.

   a) Pour permettre à Citrix Endpoint Management d'appliquer une licence d'achat en volume pour l'application : dans la liste **Licence d'achat en volume**, cliquez sur **Charger un fichier de licences d'achat en volume**.

   b) Dans la boîte de dialogue qui s'affiche, importez la licence.

   Le tableau Attribution de licences affiche le nombre de licences en cours d'utilisation pour

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

l'application, par rapport au nombre total de licences disponibles.

Vous pouvez dissocier les licences d'achat en volume pour un utilisateur individuel. Cela met fin aux attributions de licence et libère des licences.

c) Lorsque vous ajoutez votre compte d'achat en volume, activez **Mise à jour automatique des applications**. Ce paramètre garantit que les applications des appareils utilisateur se mettent automatiquement à jour lorsqu'une mise à jour apparaît dans l'Apple Store. Si le paramètre **Forcer l'application à être gérée** est activé dans une application, elle est mise à jour sans intervention de l'utilisateur. La mise à jour s'effectue, que l'application soit obligatoire ou facultative.

8. Après avoir configuré les paramètres **Achat en volume**, cliquez sur **Suivant**. La page **Approbations** s'affiche.

   Pour utiliser des workflows afin d'exiger une approbation avant d'autoriser les utilisateurs à accéder à l'application, consultez la section Appliquer les workflows. Si vous n'avez pas besoin de workflow d'approbation, passez à l'étape suivante.

9. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.

10. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

    - **Déployer :** choisissez cette option si vous souhaitez déployer l'application sur les appareils. La valeur par défaut est **Activé**.
    - **Calendrier de déploiement :** choisissez l'option **Maintenant** ou **Plus tard** pour déployer l'application. Si vous sélectionnez **Plus tard**, configurez une date et une heure pour déployer l'application. La valeur par défaut est **Maintenant**.
    - **Conditions de déploiement :** choisissez **À chaque connexion** pour déployer l'application chaque fois que l'appareil se connecte. Choisissez **Uniquement lorsque le déploiement précédent a échoué** pour déployer l'application lorsque l'appareil n'a pas réussi à recevoir l'application. L'option par défaut est **À chaque connexion**.

    L'option **Déployer pour les connexions permanentes** s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

    L'option de connexion permanente :

    - N'est pas disponible pour les appareils iOS.
    - N'est pas disponible pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec la version 10.18.19 ou ultérieure

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- N'est pas recommandée pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec une version antérieure à la version 10.18.19

Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

12. Cliquez sur **Enregistrer**.

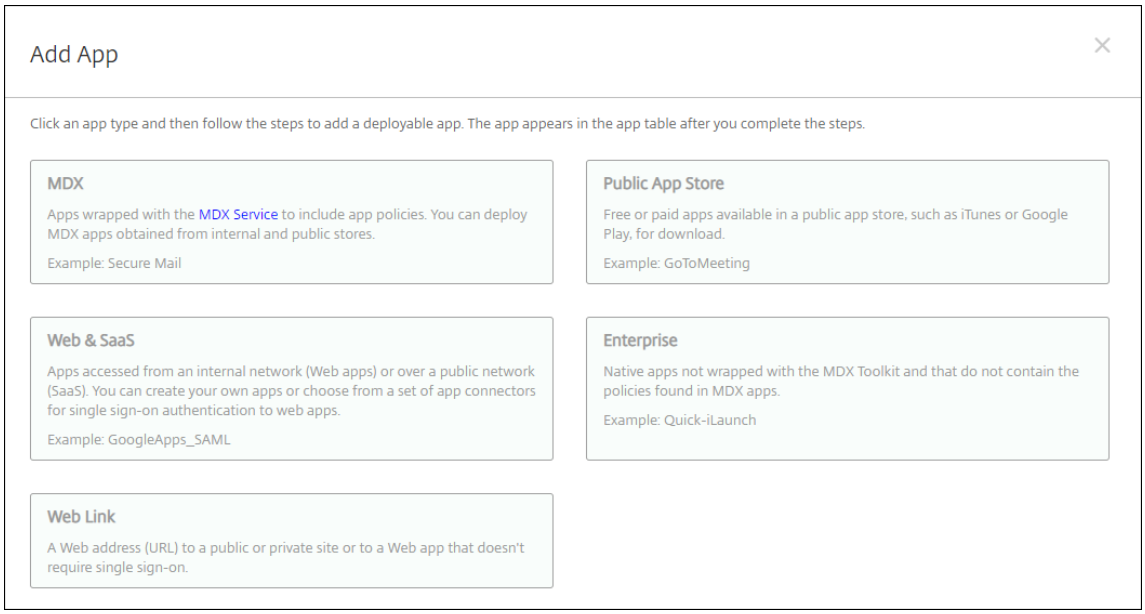
Ajouter une application Web ou SaaS

Grâce à la console Citrix Endpoint Management, vous pouvez fournir aux utilisateurs une autorisation d'authentification unique (SSO) à vos applications d'entreprise, Web et SaaS.

Vous pouvez créer votre propre connecteur dans Citrix Endpoint Management lorsque vous ajoutez une application Web ou une application SaaS. Pour obtenir la liste des types de connecteurs disponibles dans Citrix Endpoint Management, consultez Types de connecteur d'application.

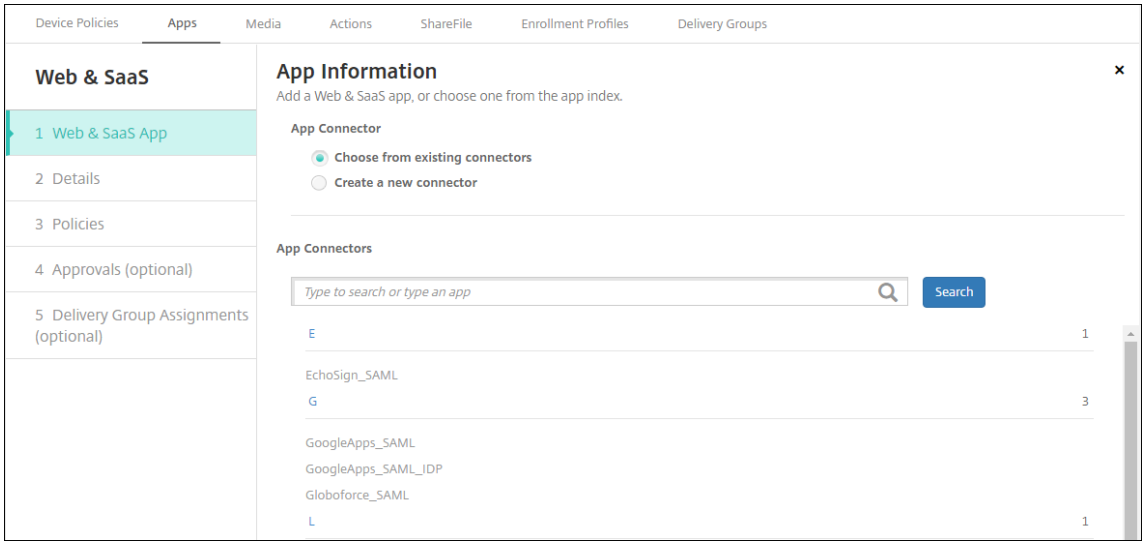
Si une application est uniquement disponible en authentification unique : une fois que vous avez enregistré les paramètres, l'application s'affiche dans l'onglet **Applications** de la console Citrix Endpoint Management.

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications > Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



2. Cliquez sur **Web et SaaS**. La page **Informations sur l'application** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Configurez un nouveau connecteur d'applications ou un connecteur existant comme suit.

Pour configurer un connecteur d'applications existant

1. Sur la page **Informations sur l'application**, l'option **Choisir parmi les connecteurs existants** est déjà sélectionnée, comme illustré précédemment. Cliquez sur le connecteur que vous souhaitez utiliser dans la liste **Connecteurs d'applications**. Les informations sur le connecteur d'applications s'affichent.
2. Pour configurer ces paramètres :
   - **Nom de l'application :** acceptez le nom attribué ou entrez un nouveau nom.
   - **Description de l'application :** acceptez la description existante ou choisissez la vôtre.
   - **URL :** acceptez l'URL attribuée ou entrez l'adresse Web de l'application. Selon le connecteur que vous choisissez, ce champ peut contenir un paramètre fictif que vous devez remplacer avant de pouvoir passer à la page suivante.
   - **Nom de domaine :** le cas échéant, entrez le nom de domaine de l'application. Ce champ est obligatoire.
   - **L'application est hébergée dans le réseau interne :** indiquez si l'application est exécutée sur un serveur de votre réseau interne. Si les utilisateurs se connectent à l'application interne à partir d'un site distant, ils doivent se connecter par l'intermédiaire de NetScaler Gateway. En réglant cette option sur **Activé**, le mot-clé VPN est ajouté à l'application et permet aux utilisateurs de se connecter via NetScaler Gateway. La valeur par défaut est **Désactivé**.
   - **Catégorie d'application :** dans la liste, cliquez sur une catégorie à appliquer à l'application (facultatif).
   - **Provisioning du compte utilisateur :** sélectionnez cette option si vous souhaitez créer des comptes utilisateur pour l'application. Si vous utilisez le connecteur Globo-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

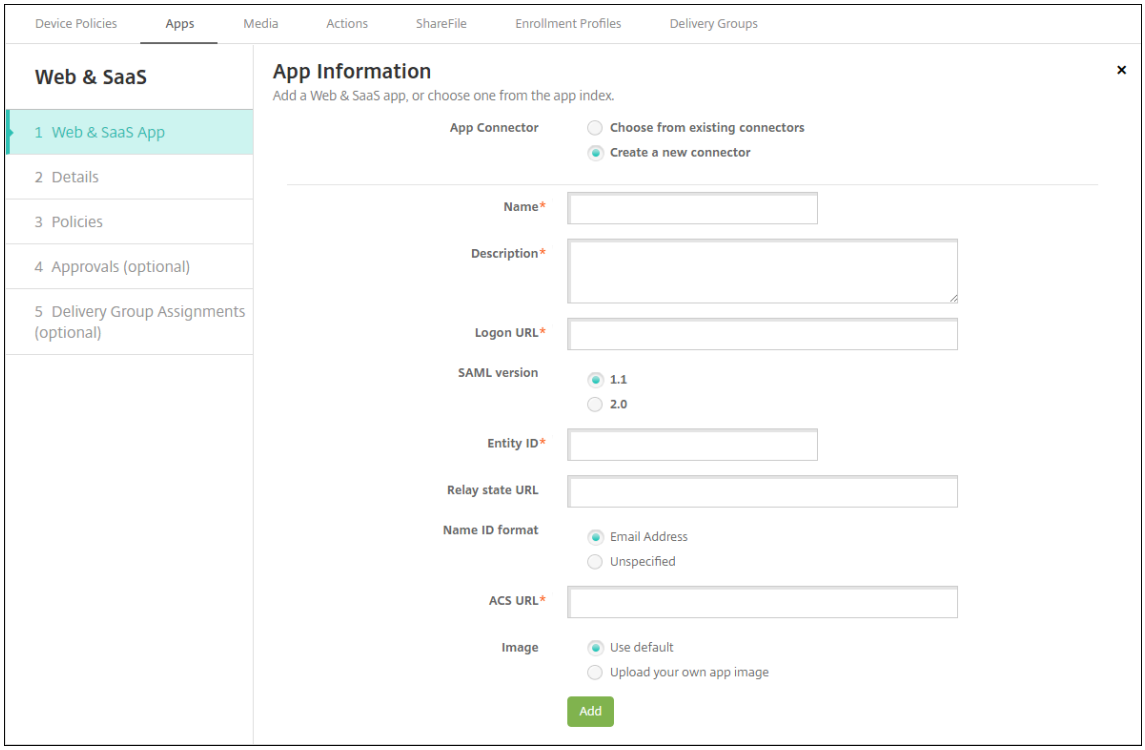
force_SAML, vous devez activer cette option pour assurer une intégration SSO transparente.

- Si vous activez **Provisioning du compte utilisateur**, configurez les paramètres suivants :
  - **Compte de service**
    - **Nom d'utilisateur :** entrez un nom pour l'administrateur de l'application. Ce champ est obligatoire.
    - **Mot de passe :** tapez le mot de passe d'administrateur de l'application. Ce champ est obligatoire.
  - **Compte utilisateur**
    - **Lorsque les droits de l'utilisateur prennent fin :** dans la liste, cliquez sur l'action à effectuer lorsque les utilisateurs ne sont plus autorisés à accéder à l'application. La valeur par défaut est **Désactiver le compte**.
  - **Règle de nom d'utilisateur**
    - Pour chaque règle de nom d'utilisateur que vous souhaitez ajouter, procédez comme suit :
      - **Attributs utilisateur :** dans la liste, cliquez sur l'attribut utilisateur à ajouter à la règle.
      - **Longueur (caractères) :** dans la liste, cliquez sur le nombre de caractères (de l'attribut utilisateur) à inclure dans la règle de nom d'utilisateur. Le paramètre par défaut est **All**
      - **Règle :** chaque attribut utilisateur que vous ajoutez est automatiquement ajouté à la règle de nom d'utilisateur.
- **Exigences de mot de passe**
  - **Longueur :** entrez la longueur minimale du mot de passe de l'utilisateur. La valeur par défaut est **8**.
- **Expiration du mot de passe**
  - **Validité (jours) :** tapez le nombre de jours pendant lequel le mot de passe est valable. Les valeurs valides sont **0 - 90**. La valeur par défaut est 90.
  - **Réinitialiser le mot de passe automatiquement après son expiration :** sélectionnez cette option si vous voulez réinitialiser le mot de passe automatiquement lors de l'expiration. La valeur par défaut est **Désactivé**. Si vous n'activez pas ce champ, les utilisateurs ne peuvent pas ouvrir l'application après que leur mot de passe expire.

Pour configurer un nouveau connecteur d'applications

1. Sur la page **Informations sur l'application**, sélectionnez **Créer un nouveau connecteur**. Les champs du connecteur d'applications s'affichent.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



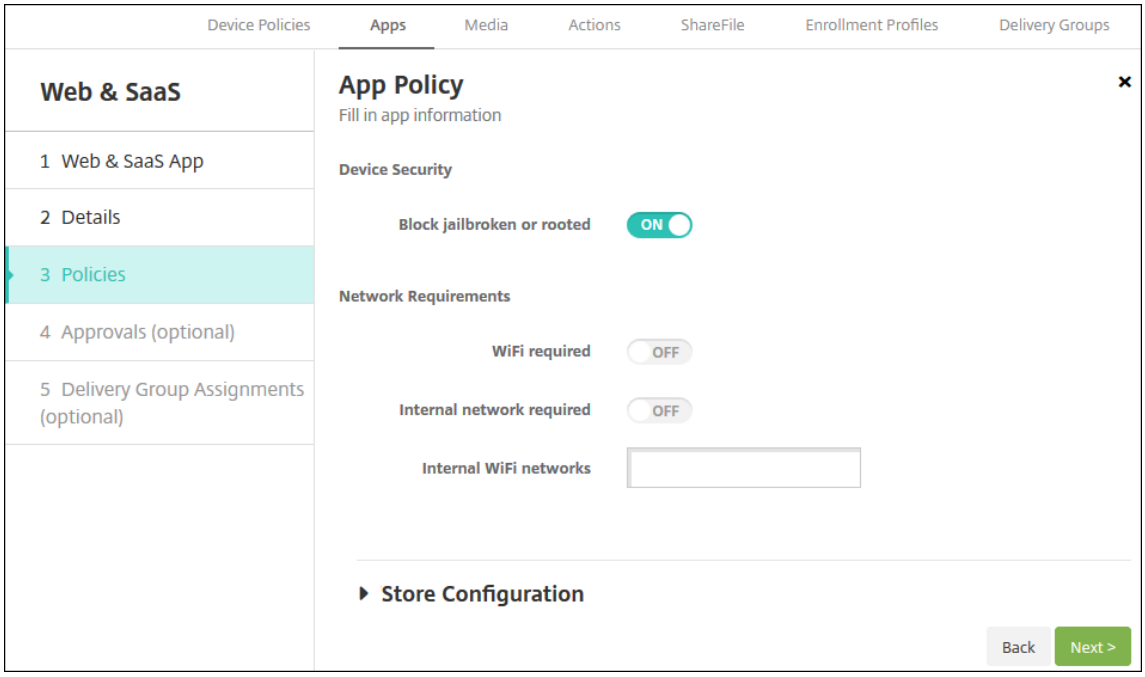
2. Pour configurer ces paramètres :

   - **Nom :** entrez un nom pour le connecteur. Ce champ est obligatoire.
   - **Description :** entrez une description pour le connecteur. Ce champ est obligatoire.
   - **URL de connexion :** entrez, ou copiez et collez, l'adresse URL de l'emplacement sur lequel les utilisateurs ouvrent une session sur le site. Par exemple, si l'application que vous souhaitez ajouter possède une page d'ouverture de session, ouvrez un navigateur Web et accédez à la page d'ouverture de session de l'application. Par exemple, `https://www.example.com/logon`. Ce champ est obligatoire.
   - **Version SAML :** sélectionnez **1.1** ou **2.0**. La valeur par défaut est **1.1**.
   - **ID de l'entité :** entrez l'identité de l'application SAML.
   - **URL d'état du relais :** entrez l'adresse Web de l'application SAML. L'URL d'état du relais représente l'URL de réponse de l'application.
   - **Format de l'ID de nom :** sélectionnez **Adresse e-mail** ou **Non spécifié**. Le paramètre par défaut est **Adresse e-mail**.
   - **URL ACS :** entrez l'URL du service ACS (consommateur d'assertion) du fournisseur de services ou d'identités. L'URL ACS offre aux utilisateurs une fonctionnalité d'authentification unique (SSO).
   - **Image :** indiquez si vous souhaitez utiliser l'image Citrix par défaut ou charger votre propre image d'application. La valeur par défaut est Utiliser valeur par défaut.
     - Pour télécharger votre propre image, cliquez sur **Parcourir** et accédez à l'emplacement du fichier. Le fichier doit être un fichier .PNG. Vous ne pouvez pas charger un

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

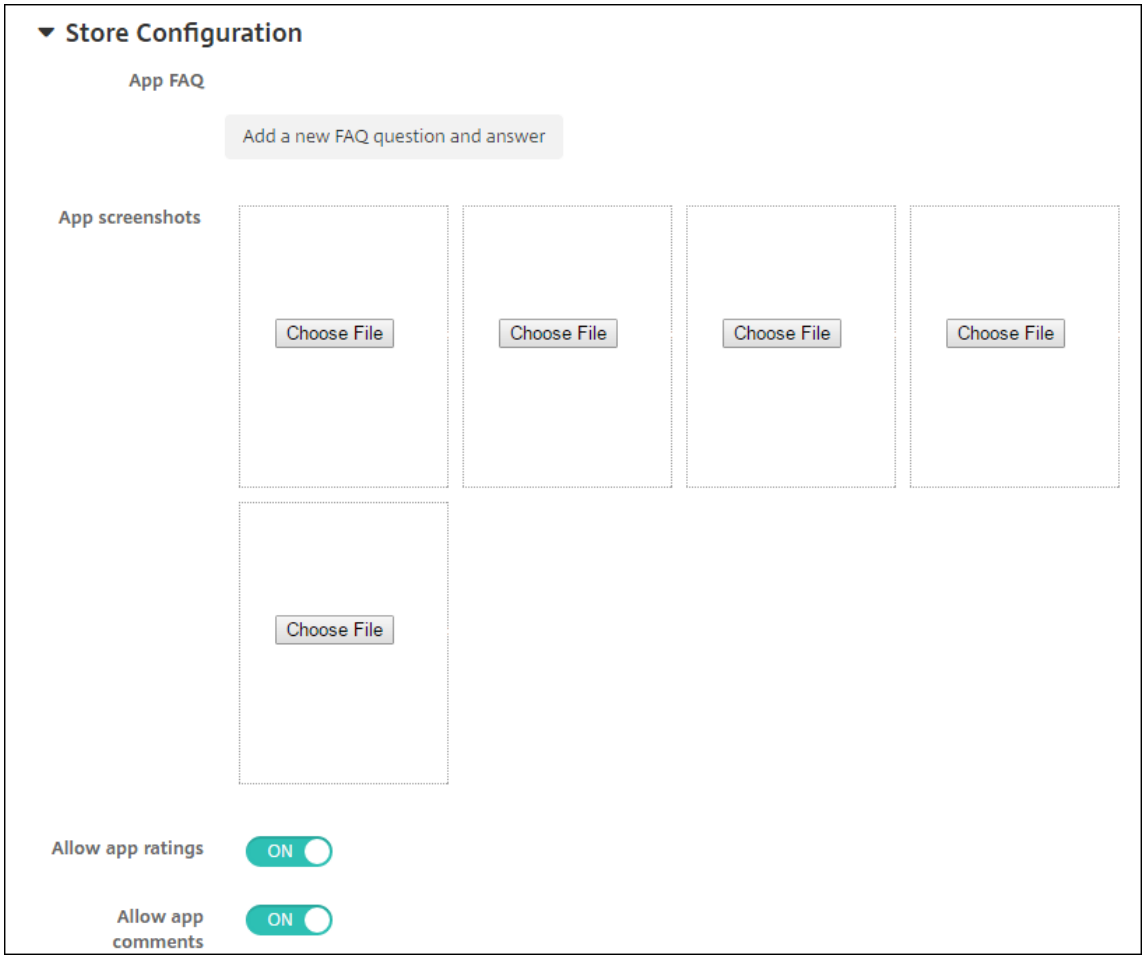
fichier GIF ou JPEG. Lorsque vous ajoutez un graphique personnalisé, vous ne pouvez pas le modifier ultérieurement.

3. Lorsque vous avez terminé, cliquez sur **Ajouter**. La page **Détails** s'affiche.
4. Cliquez sur **Suivant**. La page **Stratégie d'application** s'affiche.



5. Pour configurer ces paramètres :
   - **Sécurité de l'appareil**
   - **Bloquer les appareils jailbreakés ou rootés :** sélectionnez cette option pour empêcher les appareils jailbreakés ou rootés d'accéder à l'application. La valeur par défaut est **Activé**.
   - **Exigences du réseau**
   - **Wi-Fi requis :** sélectionnez cette option pour spécifier qu'une connexion Wi-Fi est requise pour exécuter l'application. La valeur par défaut est **Désactivé**.
   - **Réseau interne requis :** sélectionnez cette option si un réseau interne est requis pour exécuter l'application. La valeur par défaut est **Désactivé**.
   - **Réseaux Wi-Fi internes :** si vous avez activé **Wi-Fi requis**, saisissez le réseau Wi-Fi interne à utiliser.
6. Développez **Configuration du magasin**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

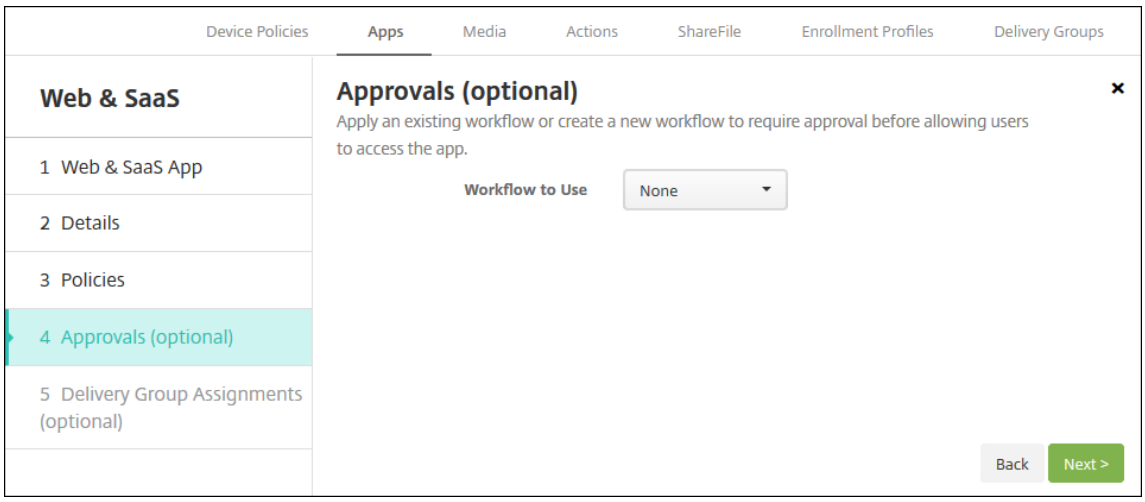


Si vous le souhaitez, vous pouvez configurer les paramètres suivants :

- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.
- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des commentaires sur l'application dans l'App Store.

7. Cliquez sur **Suivant**. La page **Approbations** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pour utiliser des workflows afin d'exiger une approbation avant d'autoriser les utilisateurs à accéder à l'application, consultez la section Appliquer les workflows. Si vous n'avez pas besoin de workflow d'approbation, passez à l'étape suivante.

8. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.
9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.
10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

    - **Déployer :** choisissez cette option si vous souhaitez déployer l'application sur les appareils. La valeur par défaut est **Activé**.
    - **Calendrier de déploiement :** choisissez l'option **Maintenant** ou **Plus tard** pour déployer l'application. Si vous sélectionnez **Plus tard**, configurez une date et une heure pour déployer l'application. La valeur par défaut est **Maintenant**.
    - **Conditions de déploiement :** choisissez **À chaque connexion** pour déployer l'application chaque fois que l'appareil se connecte. Choisissez **Uniquement lorsque le déploiement précédent a échoué** pour déployer l'application lorsque l'appareil n'a pas réussi à recevoir l'application. L'option par défaut est **À chaque connexion**.

L'option **Déployer pour les connexions permanentes** s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

L'option de connexion permanente :

- N'est pas disponible pour les appareils iOS.
- N'est pas disponible pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec la version 10.18.19 ou ultérieure

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- N'est pas recommandée pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec une version antérieure à la version 10.18.19

Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

11. Cliquez sur **Enregistrer**.

Ajouter une application d'entreprise

Les applications d'entreprise dans Citrix Endpoint Management sont des applications privées que vous développez ou obtenez à partir d'une autre source. À l'exception des applications privées Android Enterprise fournies en tant qu'applications compatibles MDX, les applications d'entreprise ne sont pas préparées avec le SDK MAM ou MDX Toolkit. Vous pouvez charger une application d'entreprise sur l'onglet **Applications** dans la console Citrix Endpoint Management. Les applications d'entreprise prennent en charge les plates-formes suivantes (et les types de fichiers correspondant) :

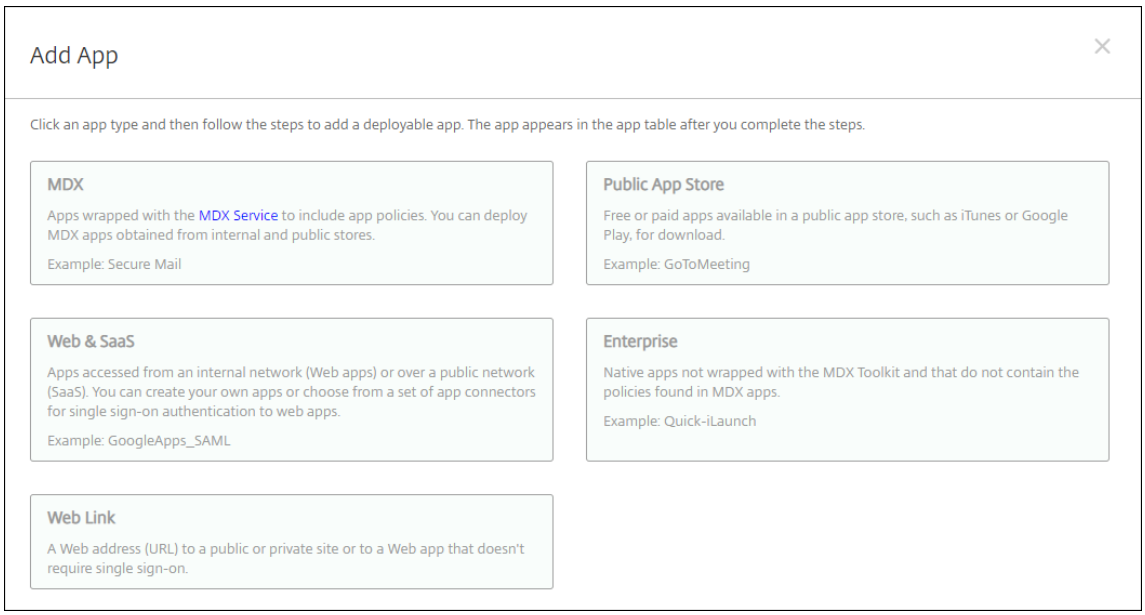
- iOS (fichier .ipa)
- macOS (fichier .pkg)

  Citrix Endpoint Management ne limite pas la taille des fichiers PKG que vous téléchargez, mais limite la durée de téléchargement des fichiers. Par défaut, vous devez terminer votre téléchargement dans un délai de 100 secondes. Pour plus d'informations, consultez Propriétés du serveur.
- Android (fichier .apk)
- Android Enterprise (fichier .apk)
- Voir aussi : Ajouter des applications Win32 en tant qu'applications d'entreprise
- Voir aussi : Applications privées compatibles MDX

L'ajout d'applications téléchargées à partir de Google Play Store en tant qu'applications d'entreprise n'est pas pris en charge. Ajoutez plutôt des applications du Google Play Store en tant qu'applications publiques. Voir Ajouter une application d'un magasin d'applications public.

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications > Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Cliquez sur **Entreprise**. La page **Informations sur l'application** s'affiche.
3. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Il apparaît sous Nom de l'application dans le tableau Applications.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.
4. Cliquez sur **Suivant**. La page **Plates-formes d'applications** s'affiche.
5. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.
6. Pour chaque plate-forme que vous avez choisie, sélectionnez le fichier à charger en cliquant sur **Charger** et accédez à l'emplacement du fichier.
7. Cliquez sur **Suivant**. La page d'informations sur l'application pour la plate-forme s'affiche.
8. Configurez les paramètres pour le type de plate-forme, notamment :
   - **Nom du fichier :** entrez un nouveau nom pour l'application (facultatif).
   - **Description de l'application :** entrez une nouvelle description pour l'application (facultatif).
   - **Version de l'application :** vous ne pouvez pas modifier ce champ.
   - **Version d'OS minimum :** si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.

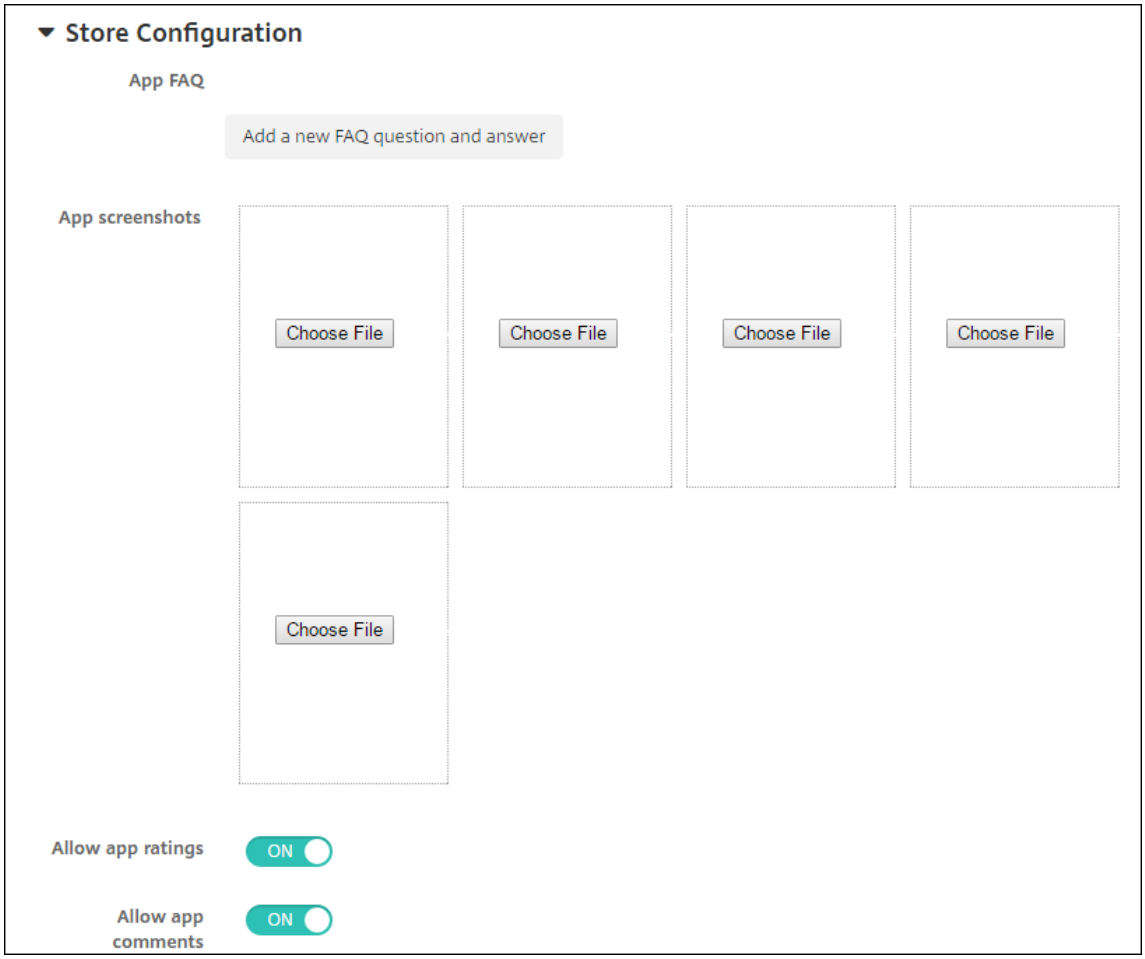
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Version d'OS maximum :** si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
- **Appareils exclus :** si vous le souhaitez, entrez le fabricant ou les modèles d'appareils qui ne peuvent pas exécuter l'application.
- **ID de package :**identifiant unique de votre application.
- **Supprimer l'application si le profil MDM est supprimé :** sélectionnez cette option si vous souhaitez supprimer l'application d'un appareil lorsque le profil MDM est supprimé. La valeur par défaut est **Activé**. Ce paramètre ne s'applique pas à macOS.
- **Empêcher la sauvegarde des données d'application :** sélectionnez cette option si vous souhaitez empêcher l'application de sauvegarder les données. La valeur par défaut est **Activé**. Ce paramètre ne s'applique pas à macOS.
- **Forcer l'application à être gérée :** sélectionnez cette option si vous souhaitez installer une application en tant qu'application gérée sur des appareils non supervisés. Le type d'appareil détermine comment Citrix Endpoint Management traite ce paramètre lorsqu'il est activé. Si vous activez ce paramètre, l'application est mise à jour sans intervention de l'utilisateur. La mise à jour s'effectue, que l'application soit obligatoire ou facultative. La valeur par défaut est **Désactivé**.
  - Pour les appareils iOS, si l'application a déjà été installée, les utilisateurs reçoivent une invite pour autoriser la gestion de l'application. Si vous déployez une application sur des appareils où l'application n'existe pas, l'application est installée en tant qu'application gérée, quel que soit l'état de ce paramètre. Disponible sur iOS 9.0 et versions ultérieures. Pour les appareils iOS inscrits via l'inscription des utilisateurs, Citrix Endpoint Management n'applique pas ce paramètre et n'invite pas les utilisateurs à autoriser la gestion des applications.
  - Pour les appareils macOS, activez le paramètre, puis déployez l'application sur les appareils. L'application est installée automatiquement en tant qu'application gérée. Les utilisateurs ne reçoivent aucune invite. Si vous déployez une application sur des appareils où l'application n'existe pas, l'application est installée en tant qu'application gérée, quel que soit l'état de ce paramètre. Disponible sur macOS 11.0 et versions ultérieures

9. Configurez les règles de déploiement. Pour plus d'informations, consultez la section Configurer les règles de déploiement.

10. Développez **Configuration du magasin**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Si vous le souhaitez, vous pouvez configurer les paramètres suivants :

- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.
- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des commentaires sur l'application dans l'App Store.

11. Cliquez sur **Suivant**. La page **Approbations** s'affiche.

    Pour utiliser des workflows afin d'exiger une approbation avant d'autoriser les utilisateurs à accéder à l'application, consultez la section Appliquer les workflows. Si vous n'avez pas besoin d'un workflow d'approbation, passez à l'étape suivante.

12. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.

13. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

à disposition ou sélectionnez un ou des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

14. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

    - **Déployer :** choisissez cette option si vous souhaitez déployer l'application sur les appareils. La valeur par défaut est **Activé**.
    - **Calendrier de déploiement :** choisissez l'option **Maintenant** ou **Plus tard** pour déployer l'application. Si vous sélectionnez **Plus tard**, configurez une date et une heure pour déployer l'application. La valeur par défaut est **Maintenant**.
    - **Conditions de déploiement :** choisissez **À chaque connexion** pour déployer l'application chaque fois que l'appareil se connecte. Choisissez **Uniquement lorsque le déploiement précédent a échoué** pour déployer l'application lorsque l'appareil n'a pas réussi à recevoir l'application. L'option par défaut est **À chaque connexion**.

    L'option **Déployer pour les connexions permanentes** s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

    L'option de connexion permanente :

    - N'est pas disponible pour les appareils iOS.
    - N'est pas disponible pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec la version 10.18.19 ou ultérieure
    - N'est pas recommandée pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec une version antérieure à la version 10.18.19

    Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

15. Cliquez sur **Enregistrer**.

Ajouter des applications Win32 en tant qu'applications d'entreprise

Vous pouvez charger des fichiers MSI, APPX, AppxBundle, PS1 ou EXE pour applications Win32 vers Citrix Endpoint Management pour le déploiement vers des appareils Windows 10 et Windows 11 Desktop et Tablet gérés. Une fois que vous avez utilisé Citrix Endpoint Management pour déployer les fichiers, l'appareil Windows installe l'application comme suit :

- Si l'application mise à niveau supprime l'ancienne version lors de l'installation, l'appareil inclut uniquement l'application mise à niveau.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si l'application mise à niveau ne peut pas supprimer l'ancienne version, mais que la nouvelle version est installée, l'appareil inclut les deux versions de l'application. Citrix Endpoint Management ne contient plus les informations de l'ancienne version.
- Si l'application mise à niveau ne peut pas s'installer lorsqu'il existe une ancienne version, la nouvelle application ne s'installe pas. Dans ce cas, déployez d'abord la stratégie de désinstallation d'application pour supprimer l'ancienne version. Déployez ensuite la nouvelle version.

Exigences

- Windows 10 (version 1607 ou ultérieure) ou Windows 11
- Windows 10 Professionnel ou Windows 11 Professionnel
- Windows 10 Entreprise ou Windows 11 Entreprise
- Applications MSI Win32 autonomes installées avec l'option /quiet. Dans ce type de déploiement, Microsoft ne prend pas en charge les MSI contenant plusieurs applications, les MSI imbriqués ou l'installation interactive.

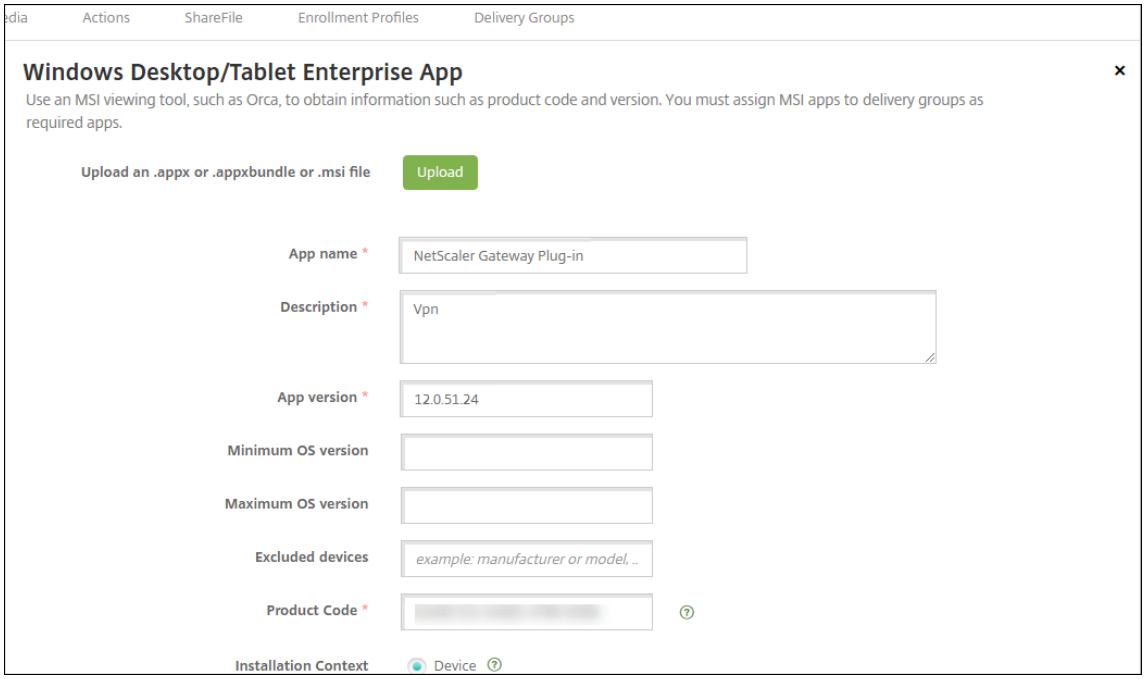
Rechercher les métadonnées Lorsque vous ajoutez une application Win32 à Citrix Endpoint Management, spécifiez les métadonnées de l'application. Pour rechercher les métadonnées, utilisez l' application Orca sur un ordinateur Windows et prenez note des informations suivantes :

- Code du produit
- Nom du produit
- Version du produit
- Type d'installation de package, soit par utilisateur, soit par machine

Ajouter une application Win32 à Citrix Endpoint Management

1. Accédez à **Configurer > Applications**, cliquez sur **Entreprise**, tapez un nom pour l'application sur la page **Informations sur l'application**.
2. Désélectionnez toutes les cases à cocher Plate-forme à l'exception de **Windows Desktop/Tablet**.
3. Sur la page **Application d'entreprise Windows Desktop/Tablet**, cliquez sur **Charger** et accédez au fichier.
4. Pour configurer ces paramètres :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

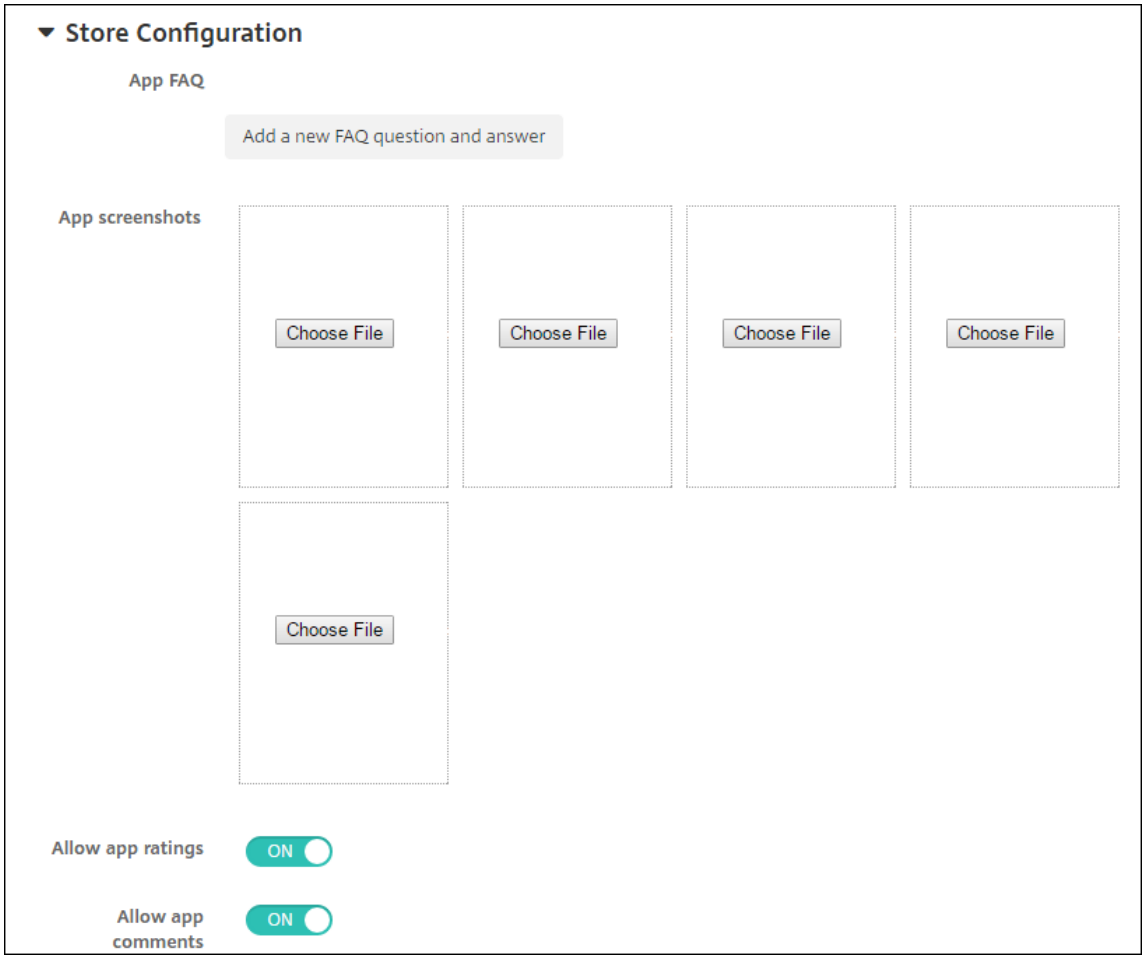


- **Nom de l'application :** nom de l'application, indiqué dans les métadonnées de l'application.
- **Description :** description de l'application.
- **Version de l'application :** numéro de version de l'application, indiqué dans les métadonnées de l'application.
- **Version d'OS minimum :** facultatif. Version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
- **Version d'OS maximum :** facultatif. Version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
- **Appareils exclus :** facultatif. Fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.
- **Code du produit :** code produit de l'application MSI, au format UUID, défini par les métadonnées de l'application.
- **Contexte d'installation :** en vous basant sur les métadonnées de l'application, sélectionnez si l'application sera installée pour l'appareil ou l'utilisateur. Ce paramètre n'est pas disponible pour les fichiers EXE.
- **Ligne de commande :** options de ligne de commande à utiliser lors de l'appel de MSIEXEC.exe
- **Ligne de commande de d'installation :** ajoutez des arguments de ligne de commande pour installer les fichiers EXE en mode silencieux.
- **Ligne de commande de désinstallation :** ajoutez des arguments de ligne de commande pour désinstaller les fichiers EXE en mode silencieux.
- **Nombre de tentatives :** nombre de fois que vous pouvez retenter une opération de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

téléchargement et d'installation avant de marquer l'installation comme ayant échoué.
- **Délai d'expiration :** nombre de minutes pendant lesquelles le processus d'installation s'exécute avant que le programme d'installation interprète l'installation comme ayant échoué et ne surveille plus le processus.
- **Intervalle entre les tentatives :** nombre de minutes entre les tentatives.

5. Configurez les règles de déploiement. Pour plus d'informations, consultez la section Configurer les règles de déploiement.
6. Développez **Configuration du magasin**.



Si vous le souhaitez, vous pouvez configurer les paramètres suivants :

- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des commentaires sur l'application dans l'App Store.

7. Cliquez sur **Suivant** jusqu'à ce que vous accédiez à la page **Résumé**, puis cliquez sur **Enregistrer**.
8. Accédez à **Configurer > Groupes de mise à disposition** et ajoutez l'application Win32 comme application requise.
9. Après avoir déployé l'application, informez vos utilisateurs que l'application est disponible.

Mettre à niveau une application Win32

1. Recherchez les métadonnées de l'application, comme indiqué précédemment dans « Rechercher les métadonnées ».
2. Accédez à **Configurer > Applications** pour télécharger la nouvelle version de l'application. Mettez à jour la **Version de l'application**. Si la nouvelle version de l'application a un **code produit** différent, mettez à jour ce paramètre.
3. Envoyez les modifications et déployez l'application.

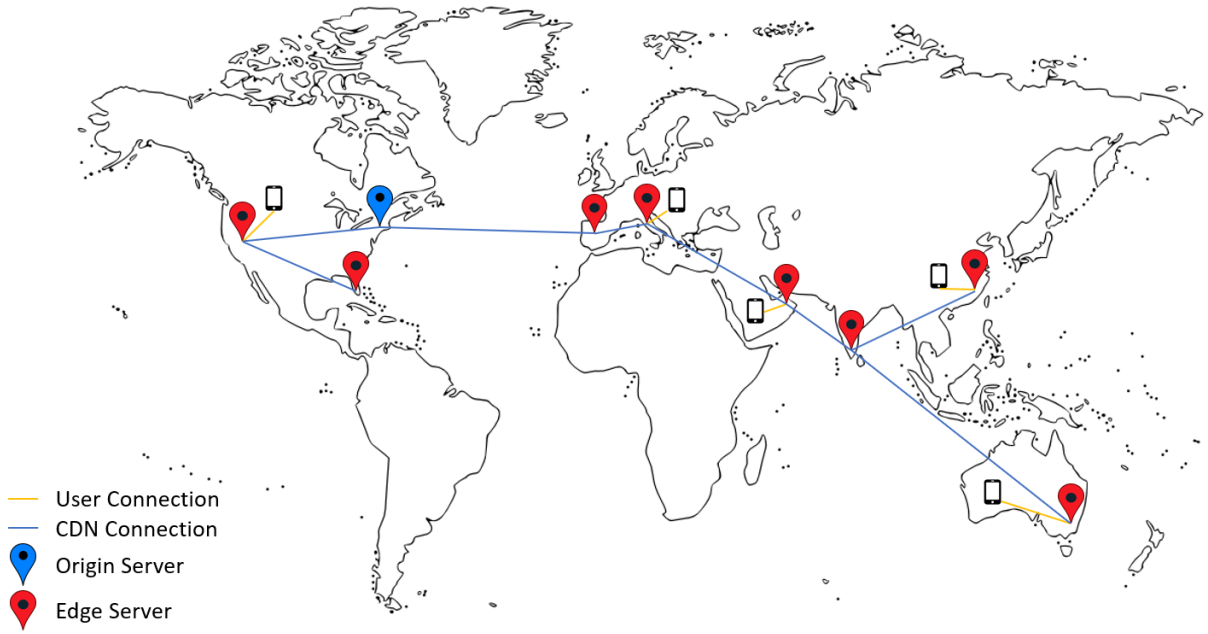
Fournir des applications d'entreprise et MDX à partir du CDN Citrix

Vous pouvez fournir des applications d'entreprise et MDX à partir du réseau de mise à disposition de contenu Citrix ou CDN (Content Delivery Network). Un CDN fait référence à un groupe de serveurs situés dans différentes zones géographiques et qui travaillent ensemble pour fournir en toute sécurité le contenu d'applications. Un serveur local fournit les applications aux appareils mobiles.

Un CDN améliore les délais de téléchargement des applications en distribuant le contenu le plus proche des appareils mobiles à l'aide d'un point de distribution CDN à proximité. Le CDN fournit les applications à partir de l'emplacement POP (Point of Presence) le plus proche d'un utilisateur.

Le diagramme suivant montre un exemple de la façon dont le CDN distribue les applications au serveur Edge Server le plus proche des utilisateurs d'appareils mobiles. Un serveur Edge Server met en cache le contenu du serveur d'origine lorsque des appareils mobiles demandent des applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Les utilisateurs peuvent se connecter aux applications à l'aide de Citrix Secure Hub. Lorsque vous ajoutez une application, Citrix Endpoint Management crée le connecteur d'application pour cette dernière.

CDN Citrix prend en charge les applications d'entreprise sur les plates-formes suivantes :

- iOS (inscription MDM ou MAM)
- Android (inscription MDM ou MAM)
- Ordinateur de bureau ou tablette Windows (inscription MDM)
- macOS (inscription MDM)

CDN Citrix prend en charge les applications MDX sur les plates-formes suivantes :

- iOS (inscription MDM ou MAM)
- Android (inscription MDM ou MAM)

Comment CDN fonctionne

Au cœur du service CDN, les serveurs sont reliés afin de distribuer les applications plus rapidement. Pour ce faire, les applications sont placées en toute sécurité sur différents points de distribution dans le monde entier. Le serveur DNS des appareils mobiles utilisé au cours de la connexion initiale au serveur Citrix Endpoint Management détermine le point de distribution.

Par exemple : supposons que l'adresse IP du serveur DNS de l'appareil mobile se trouve à Fort Lauderdale, en Floride. Le CDN utilise le point de distribution local le plus proche de cet emplacement

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

pour fournir l'application à l'appareil mobile. Cette utilisation du CDN entraîne de meilleurs délais de téléchargement d'application.

Lorsqu'un appareil mobile demande ou envoie une application d'entreprise pour la première fois, Citrix Endpoint Management copie l'application sur le point de distribution local et y conserve l'application pendant 24 heures pour les autres téléchargements d'appareil locaux.

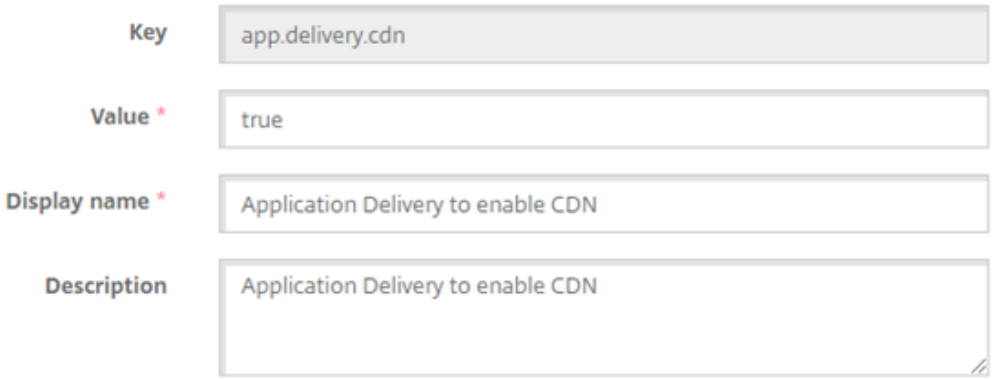
Fournir des applications d'entreprise à partir du CDN Citrix

Avec la version 19.4.1 de Citrix Endpoint Management, la mise à disposition d'applications d'entreprise est par défaut la mise à disposition CDN pour tous les nouveaux clients multi-locataires. Pour les clients existants antérieurs à cette version, suivez les instructions de cette section.

Pour les applications d'entreprise déjà disponibles sur le serveur Citrix Endpoint Management, Citrix Endpoint Management continue à distribuer ces applications depuis le serveur jusqu'à ce que ces applications soient rechargées une fois les étapes suivantes effectuées.

> **Important :**
>
> Seuls les administrateurs Citrix Cloud peuvent activer CDN pour un compte. La propriété de serveur `app.delivery.cdn` est visible dans Citrix Endpoint Management uniquement lorsque vous ouvrez une session en tant qu'administrateur Citrix Cloud. Pour plus d'informations sur l'ajout des administrateurs Citrix Cloud, consultez la section Gérer les administrateurs Citrix Cloud.

1. Activez CDN pour votre compte : dans la console Citrix Endpoint Management : Accédez à **Paramètres > Propriétés du serveur**.
2. Recherchez `app.delivery.cdn`, puis cliquez sur **Modifier**.
3. Définissez la valeur sur **true**.



4. Dans la console Citrix Endpoint Management, chargez de nouveau vos applications d'entreprise :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a) Accédez à **Configurer > Applications** et filtrez la liste d'applications par **Type** (**Entreprise**) et **Plate-forme**.
b) Sélectionnez une application, cliquez sur **Modifier**, cliquez sur **Suivant** et cliquez sur **Charger**.
c) Reprenez l'étape précédente pour chaque application d'entreprise.

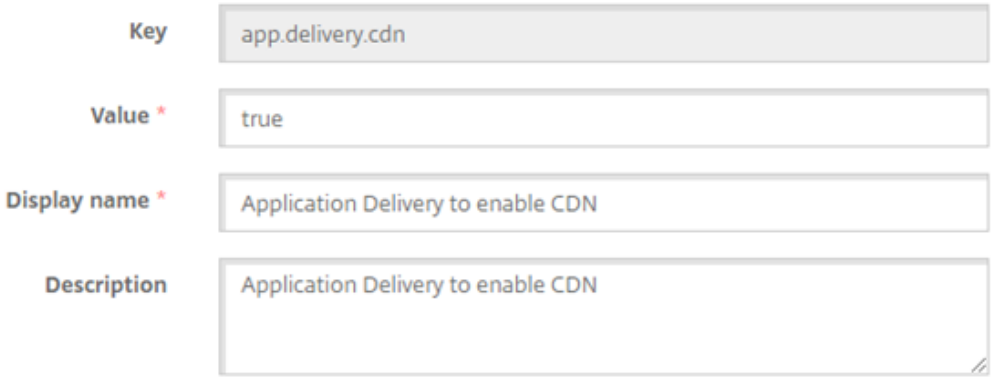
Fournir des applications MDX à partir du CDN Citrix

Avec la version 20.12.0 d'Citrix Endpoint Management, la mise à disposition d'applications MDX est par défaut la mise à disposition CDN pour tous les nouveaux clients multi-locataires. Pour les clients existants antérieurs à cette version, suivez les instructions de cette section.

Pour les applications MDX déjà disponibles sur le serveur Citrix Endpoint Management, Citrix Endpoint Management continue à distribuer ces applications depuis le serveur jusqu'à ce que ces applications soient rechargées une fois les étapes suivantes effectuées.

> **Important :**
>
> Seuls les administrateurs Citrix Cloud peuvent activer CDN pour un compte. La propriété de serveur `app.delivery.cdn` est visible dans Citrix Endpoint Management uniquement lorsque vous ouvrez une session en tant qu'administrateur Citrix Cloud. Pour plus d'informations sur l'ajout des administrateurs Citrix Cloud, consultez la section Gérer les administrateurs Citrix Cloud.

1. Activez CDN pour votre compte : dans la console Citrix Endpoint Management : Accédez à **Paramètres > Propriétés du serveur**.
2. Recherchez `app.delivery.cdn`, puis cliquez sur **Modifier**.
3. Définissez la valeur sur **true**.



4. Dans la console Citrix Endpoint Management, chargez de nouveau vos applications MDX :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a) Accédez à **Configurer > Applications** et filtrez la liste d'applications par **Type** (**MDX**) et **Plate-forme**.
b) Sélectionnez une application, cliquez sur **Modifier**, cliquez sur **Suivant** et cliquez sur **Charger**.
c) Répétez l'étape précédente pour chaque application MDX.

Ajouter un lien Web

Un lien Web est une adresse Web permettant d'accéder à un site Internet ou intranet. Un lien Web permet également d'accéder à une application Web qui ne requiert pas d'authentification unique (SSO). Une fois que vous avez terminé de configurer un lien Web, celui-ci s'affiche sous forme d'icône dans le magasin d'applications. Lorsque les utilisateurs ouvrent une session avec Citrix Secure Hub, le lien s'affiche avec la liste des applications et bureaux disponibles.

Vous pouvez configurer des liens Web dans l'onglet **Applications** de la console Citrix Endpoint Management. Une fois que vous avez terminé de configurer le lien Web, celui-ci s'affiche sous forme d'icône dans le tableau **Applications**. Lorsque les utilisateurs ouvrent une session avec Citrix Secure Hub, le lien s'affiche avec la liste des applications et bureaux disponibles.

Regardez cette vidéo pour en savoir plus :

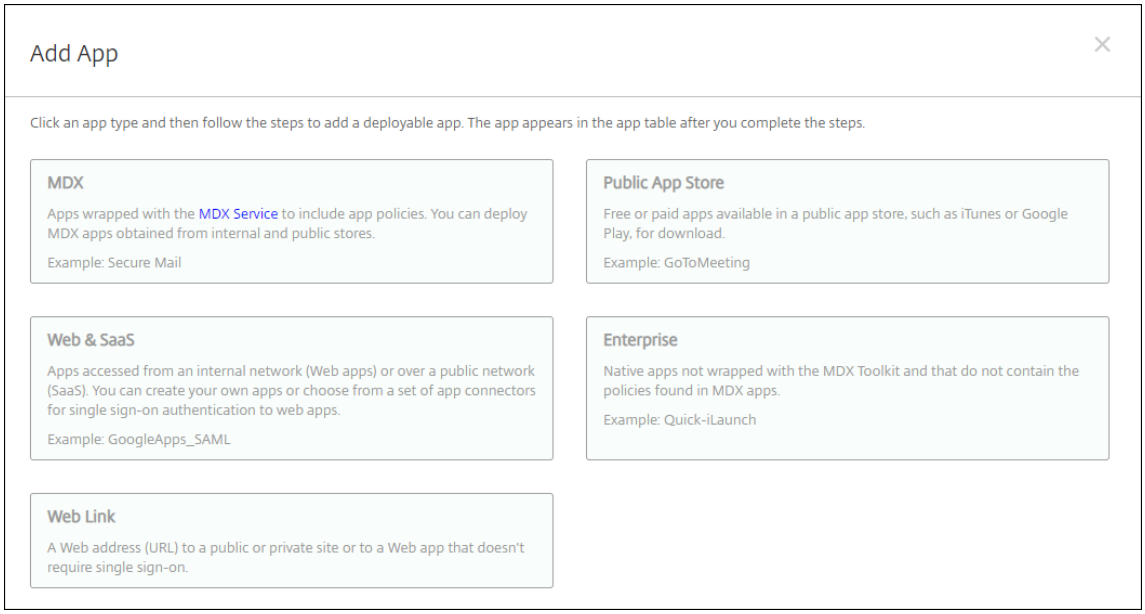
Pour ajouter le lien, vous devez fournir les informations suivantes :

- Nom du lien
- Description du lien

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Adresse Web (URL)
- Catégorie
- Rôle
- Image au format .png (facultatif)

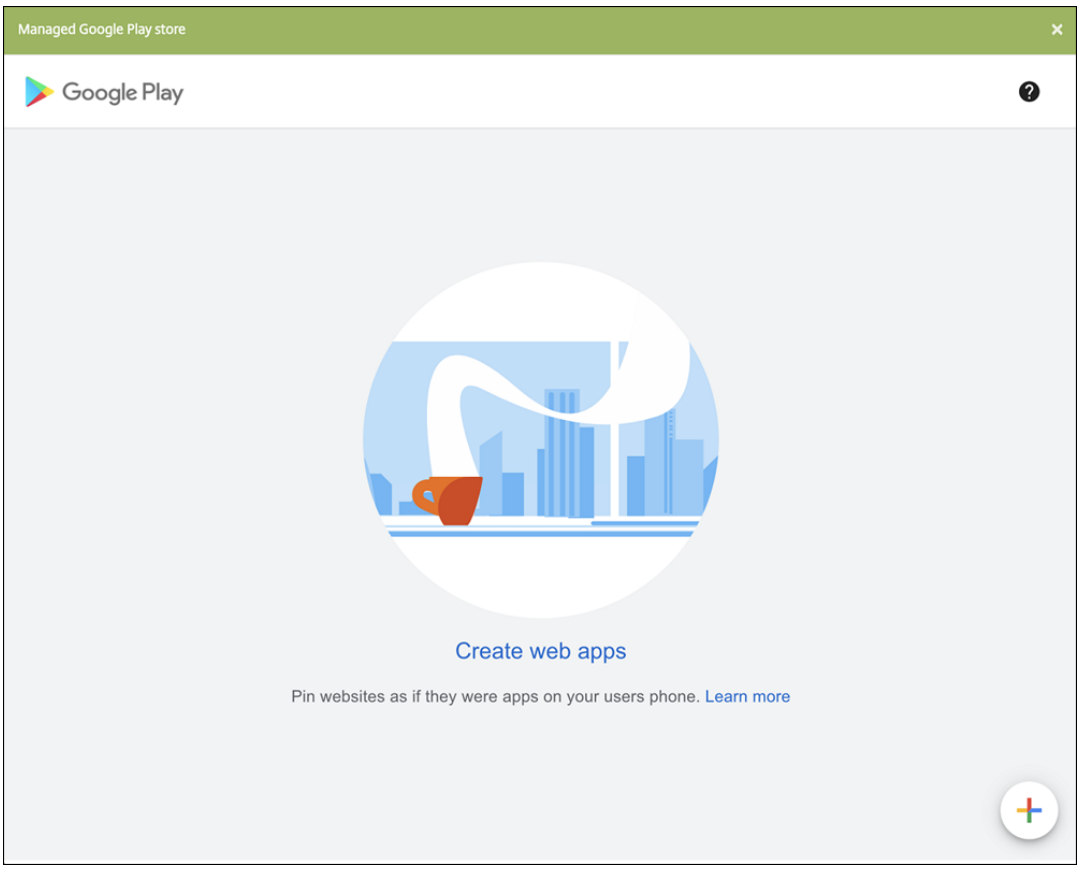
1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications > Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



2. Cliquez sur **Lien Web**. La page **Informations sur l'application** s'affiche.
3. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :
   - **Nom :** entrez un nom descriptif pour l'application. Il apparaît sous Nom de l'application dans le tableau Applications.
   - **Description :** entrez une description pour l'application (facultatif).
   - **Catégorie d'application :** si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section À propos des catégories d'applications.
4. Cliquez sur **Suivant**. La page **Plates-formes d'applications** s'affiche.
5. Sous **Plates-formes**, sélectionnez **Autres plates-formes** pour ajouter une application Web pour iOS, Android (ancien administrateur de l'appareil) et Windows 8 ou sélectionnez **Android Enterprise**. Désactivez la case à cocher pour les plates-formes que vous ne souhaitez pas inclure.
   - Si vous sélectionnez **Autres plates-formes**, passez à l'étape suivante pour configurer les paramètres.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

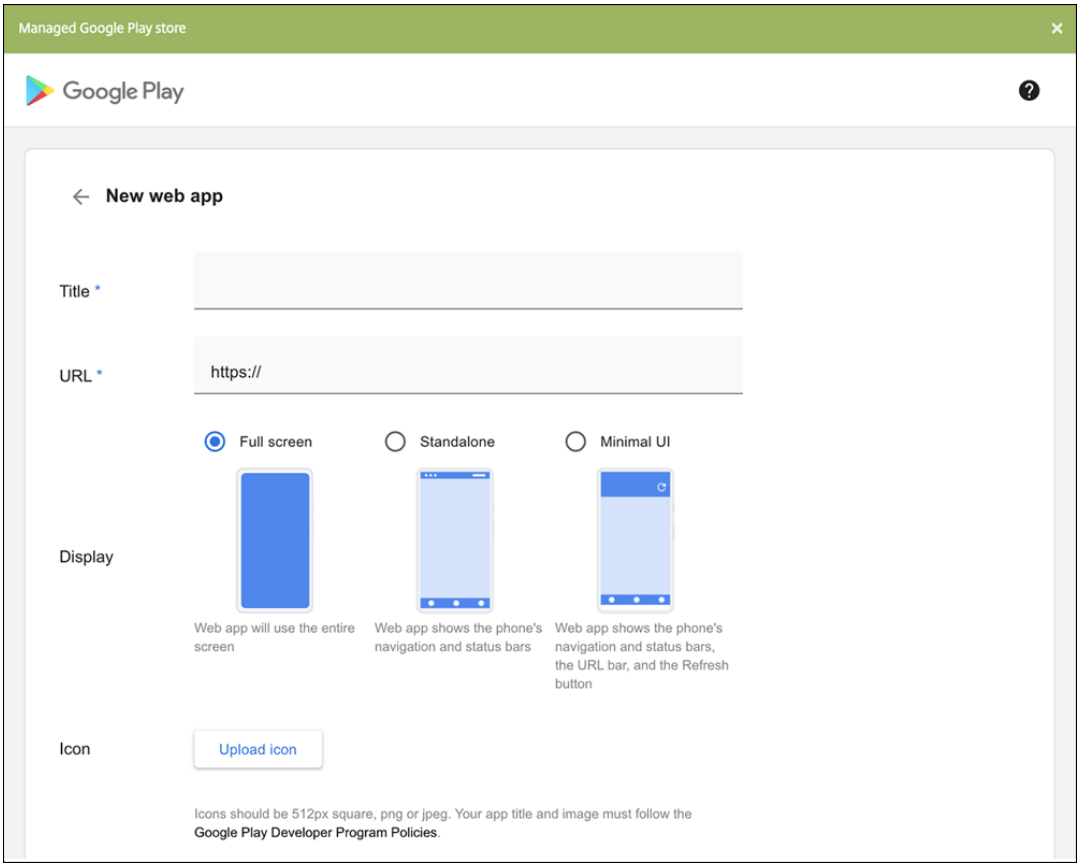
- Si vous sélectionnez **Android Enterprise**, cliquez sur le bouton **Charger** pour ouvrir le magasin Google Play Store d'entreprise. Vous n'avez pas besoin de vous inscrire pour créer un compte de développeur et publier une application Web. Cliquez sur l'icône **Plus** dans le coin inférieur droit pour continuer.



Pour configurer ces paramètres :

  - **Titre :** saisissez le nom de l'application Web.
  - **URL :** saisissez l'adresse Web de l'application.
  - **Affichage :** choisissez comment afficher l'application Web sur les machines utilisateur. Les options disponibles sont **Plein écran**, **Autonome** et **Interface minimale**.
  - **Icône :** chargez votre propre image pour l'application Web.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Lorsque vous avez terminé, cliquez sur **Créer**. La publication de votre application Web peut prendre jusqu'à 10 minutes.

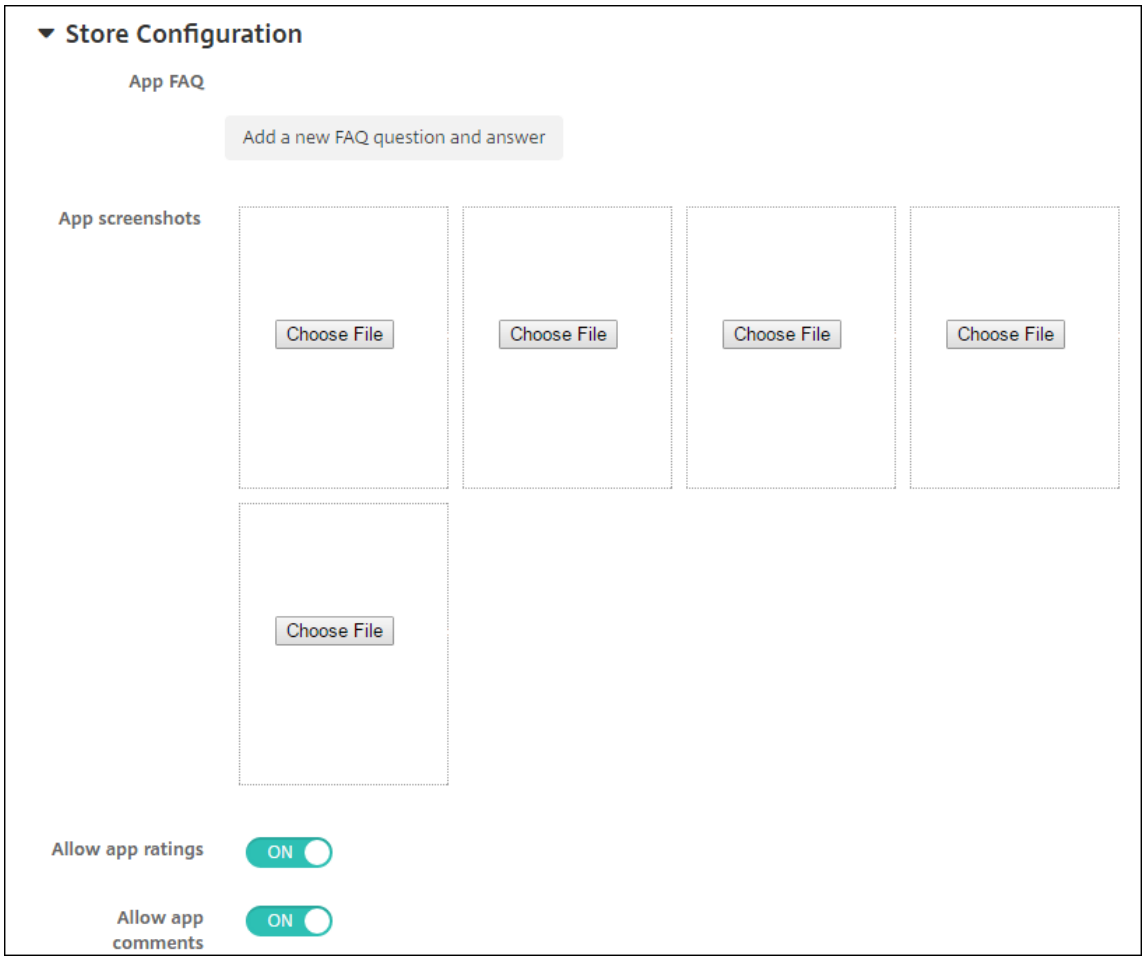
6. Pour les plates-formes autres que Android Enterprise, configurez les paramètres suivants :

   - **Nom de l'application :** acceptez le nom attribué ou entrez un nouveau nom.
   - **Description de l'application :** acceptez la description existante ou choisissez la vôtre.
   - **URL :** acceptez l'URL attribuée ou entrez l'adresse Web de l'application. Selon le connecteur que vous choisissez, ce champ peut contenir un paramètre fictif que vous devez remplacer avant de pouvoir passer à la page suivante.
   - **L'application est hébergée dans le réseau interne :** indiquez si l'application est exécutée sur un serveur de votre réseau interne. Si les utilisateurs se connectent à l'application interne à partir d'un site distant, ils doivent se connecter par l'intermédiaire de NetScaler Gateway. En réglant cette option sur **Activé**, le mot-clé VPN est ajouté à l'application et permet aux utilisateurs de se connecter via NetScaler Gateway. La valeur par défaut est **Désactivé**.
   - **Catégorie d'application :** dans la liste, cliquez sur une catégorie à appliquer à l'application (facultatif).
   - **Image :** indiquez si vous souhaitez utiliser l'image Citrix par défaut ou charger votre propre image d'application. La valeur par défaut est Utiliser valeur par défaut.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Pour télécharger votre propre image, cliquez sur **Parcourir** et accédez à l'emplacement du fichier. Le fichier doit être un fichier .PNG. Vous ne pouvez pas charger un fichier GIF ou JPEG. Lorsque vous ajoutez un graphique personnalisé, vous ne pouvez pas le modifier ultérieurement.

7. Configurez les règles de déploiement. Pour plus d'informations, consultez la section Configurer les règles de déploiement.
8. Développez **Configuration du magasin**.



Si vous le souhaitez, vous pouvez configurer les paramètres suivants :

- **FAQ sur les applications :** cliquez sur **Ajouter une nouvelle question/réponse au FAQ** pour créer une question fréquente sur l'application.
- **Ajouter des captures d'écran pour téléphones/tablettes :** ajoutez les captures d'écran qui apparaissent dans l'App Store.
- **Autoriser notation des applications :** autorisez les utilisateurs à évaluer l'application dans l'App Store.
- **Autoriser commentaires sur les applications :** autorisez les utilisateurs à laisser des commentaires sur l'application dans l'App Store.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

9. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.
10. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.
11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

    - **Déployer :** choisissez cette option si vous souhaitez déployer l'application sur les appareils. La valeur par défaut est **Activé**.
    - **Calendrier de déploiement :** choisissez l'option **Maintenant** ou **Plus tard** pour déployer l'application. Si vous sélectionnez **Plus tard**, configurez une date et une heure pour déployer l'application. La valeur par défaut est **Maintenant**.
    - **Conditions de déploiement :** choisissez **À chaque connexion** pour déployer l'application chaque fois que l'appareil se connecte. Choisissez **Uniquement lorsque le déploiement précédent a échoué** pour déployer l'application lorsque l'appareil n'a pas réussi à recevoir l'application. L'option par défaut est **À chaque connexion**.

    L'option **Déployer pour les connexions permanentes** s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

    L'option de connexion permanente :

    - N'est pas disponible pour les appareils iOS.
    - N'est pas disponible pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec la version 10.18.19 ou ultérieure
    - N'est pas recommandée pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec une version antérieure à la version 10.18.19

    Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.
12. Cliquez sur **Enregistrer**.

Activer les applications Microsoft 365

Vous pouvez ouvrir le conteneur MDX pour autoriser Citrix Secure Mail, Citrix Secure Web et Citrix Files à transférer des documents et données à des applications Microsoft Office 365. Pour de plus amples informations, consultez la section Autoriser l'interaction sécurisée avec les applications Office 365.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Appliquer les workflows

Configurez ces paramètres pour attribuer ou créer un workflow :

- **Workflow à utiliser :** dans la liste, cliquez sur un workflow existant ou cliquez sur **Créer un nouveau workflow**. La valeur par défaut est **Aucun**.

  Si vous sélectionnez **Créer un nouveau workflow**, configurez les paramètres suivants.

  - **Nom :** entrez un nom unique pour le workflow.
  - **Description :** entrez une description pour le workflow (facultatif).
  - **Modèles d'approbation d'e-mail :** dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Lorsque vous cliquez sur l'icône d'œil à droite du champ, une boîte de dialogue s'affiche dans laquelle vous pouvez afficher un aperçu du modèle.
  - **Niveaux d'approbation par un responsable :** dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est 1 niveau. Les options possibles sont les suivantes :
    * Pas nécessaire
    * 1 niveau
    * 2 niveaux
    * 3 niveaux
  - **Sélectionner un domaine Active Directory :** dans la liste, sélectionnez le domaine Active Directory à utiliser pour le workflow.
  - **Rechercher des approbateurs supplémentaires requis :** tapez le nom de la personne dans le champ de recherche et cliquez sur **Rechercher**. Les noms proviennent d'Active Directory.
  - Lorsque le nom s'affiche dans le champ, sélectionnez la case à cocher en regard du nom. Le nom et l'adresse e-mail s'affichent dans la liste **Approbateurs supplémentaires requis sélectionnés**.

    Pour supprimer une personne de la liste **Approbateurs supplémentaires requis sélectionnés**, procédez comme suit :

    * Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.
    * Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats de la recherche.
    * Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Personnalisation du magasin d'applications et de Citrix Secure Hub

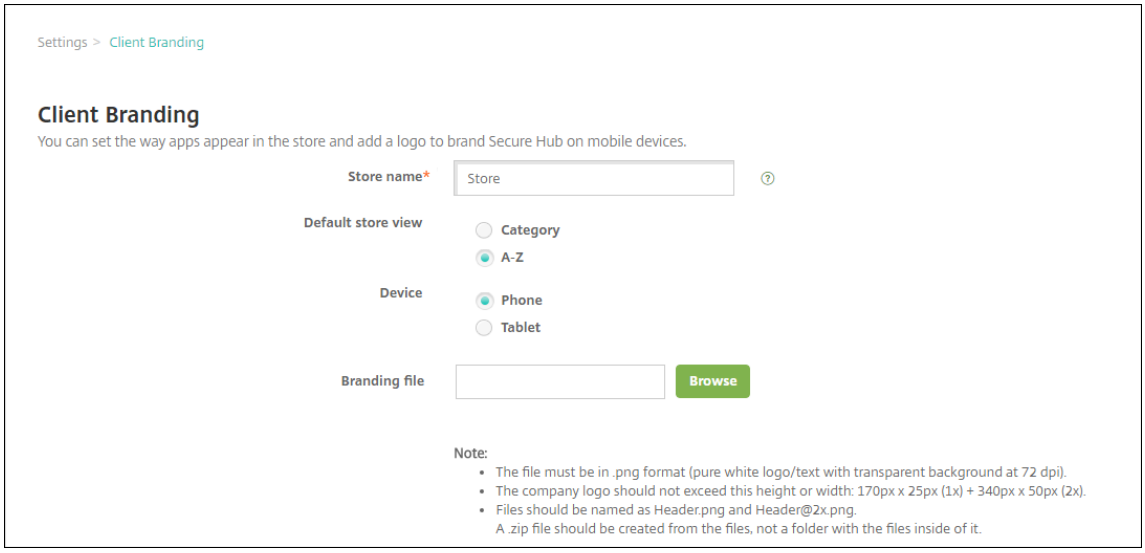
Vous pouvez définir la façon dont les applications s'affichent dans le magasin et ajouter un logo à Citrix Secure Hub et au magasin d'applications. Ces fonctionnalités de personnalisation sont disponibles pour les appareils iOS et Android.

Avant de commencer, assurez-vous que votre image personnalisée est prête et accessible.

L'image personnalisée doit répondre à ces exigences :

- Le fichier doit être au format .png.
- Utilisez un logo blanc pur ou du texte avec un arrière-plan transparent à 72 ppp.
- Le logo de la société ne peut pas dépasser cette hauteur ou largeur : 170 px x 25 px (1x) et 340 px x 50 px (2x).
- Nommez les fichiers `Header.png` et `Header@2x.png`.
- Créez un fichier .zip à partir des fichiers, et non un dossier contenant les fichiers.

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Client**, cliquez sur **Personnalisation du client**. La page **Personnalisation du client** s'affiche.



   Configurez les paramètres suivants :

   - **Nom du magasin :** le nom s'affiche dans les informations de compte de l'utilisateur. La modification du nom change également l'adresse URL utilisée pour accéder aux services du magasin. Il n'est généralement pas nécessaire de modifier le nom par défaut.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Important :**
>
> Le nom du magasin ne peut contenir que des caractères alphanumériques.

- **Vue du magasin par défaut :** sélectionnez **Catégorie** ou **A-Z**. La valeur par défaut est **A-Z**.
- **Appareil :** sélectionnez **Téléphone** ou **Tablette**. La valeur par défaut est **Téléphone**.
- **Fichier de personnalisation :** pour sélectionner une image ou un fichier .zip d'images de personnalisation, cliquez sur **Parcourir** et accédez à l'emplacement du fichier.

3. Cliquez sur **Enregistrer**.

Pour déployer ce paquetage auprès des appareils de vos utilisateurs, créez un paquetage de déploiement et déployez-le.

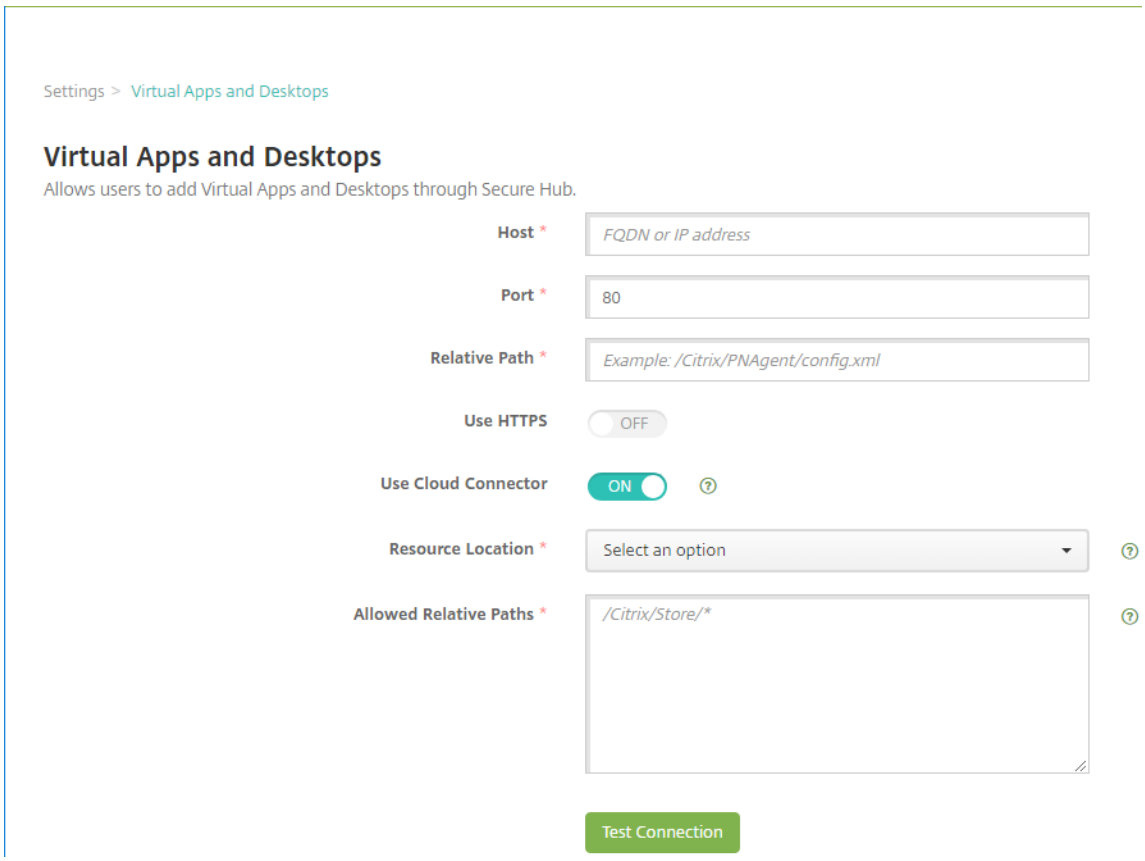
Citrix Virtual Apps and Desktops via le magasin d'applications

Citrix Endpoint Management peut collecter des applications depuis Citrix Virtual Apps and Desktops et les rendre disponibles aux utilisateurs d'appareils mobiles dans le magasin d'applications. Les utilisateurs s'abonnent directement aux applications dans le magasin d'applications et les lancent depuis Citrix Workspace. L'application Citrix Workspace doit être installée sur les machines utilisateur pour lancer les applications.

Pour configurer ce paramètre, vous devez connaître le nom de domaine complet (FQDN) ou l'adresse IP et le numéro de port du StoreFront local.

1. Dans la console web Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Virtual Apps and Desktops**. La page **Virtual Apps and Desktops** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Pour configurer ces paramètres :

   - **Hôte :** entrez le nom de domaine complet (FQDN) ou l'adresse IP pour StoreFront.
   - **Port :** entrez le numéro de port pour StoreFront. La valeur par défaut est 80.
   - **Chemin relatif :** entrez le chemin d'accès. Par exemple, /Citrix/PNAgent/config.xml
   - **Utiliser HTTPS :** sélectionnez cette option si vous souhaitez activer l'authentification sécurisée entre StoreFront et l'appareil client. La valeur par défaut est **Désactivé**.
   - **Utiliser Cloud Connector :** choisissez **Activé** pour utiliser Cloud Connector pour les connexions au serveur StoreFront. Ensuite, spécifiez un **emplacement de ressources** et des **chemins relatifs autorisés** pour la connexion.

     - **Emplacement des ressources :** choisissez parmi les emplacements de ressources définis dans Citrix Cloud Connector.
     - **Chemins relatifs autorisés :** chemins relatifs autorisés pour l'emplacement de ressources spécifié. Spécifiez un chemin d'accès par ligne. Vous pouvez utiliser le caractère générique astérisque (*).

     Si l'emplacement des ressources est `https://StoreFront.company.com`, et que vous voulez fournir un accès aux URL suivantes :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
- https://StoreFront.company.com/Citrix/PNAgent/Config.xml
- https://StoreFront.company.com/Citrix/PNAgent/enum.aspx
- https://StoreFront.company.com/Citrix/PNAgent/launch.aspx
```

Pour autoriser toutes les demandes avec l'URL `https://StoreFront.company.com/Citrix/PNAgent/*`, entrez ce chemin : `/Citrix/PNAgent/*`

Citrix Endpoint Management bloque tous les autres chemins.

4. Cliquez sur **Tester la connexion** pour vérifier que Citrix Endpoint Management peut se connecter au serveur StoreFront spécifié.
5. Cliquez sur **Enregistrer**.

Types de connecteur d'application

March 1, 2024

Le tableau suivant dresse la liste des connecteurs et des types de connecteurs disponibles dans Citrix Endpoint Management lorsque vous ajoutez une application Web ou SaaS. Vous pouvez également ajouter un connecteur à Citrix Endpoint Management lorsque vous ajoutez une application Web ou SaaS.

Il indique si le connecteur prend en charge la gestion des comptes d'utilisateur, ce qui permet de créer des comptes, de façon automatique ou à l'aide d'un workflow.

Nom du connecteur	SSO SAML	Prend en charge la gestion des comptes d'utilisateur
EchoSign_SAML	O	O
Globoforce_SAML		**Remarque :** lorsque vous utilisez ce connecteur, vous devez Activer la gestion des utilisateurs pour le provisioning pour assurer une intégration SSO transparente.
GoogleApps_SAML	O	O
GoogleApps_SAML_IDP	O	O
Lynda_SAML	O	O
Office365_SAML	O	O

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom du connecteur	SSO SAML	Prend en charge la gestion des comptes d'utilisateur
Salesforce_SAML	O	O
Salesforce_SAML_SP	O	O
SandBox_SAML	O	
SuccessFactors_SAML	O	
ShareFile_SAML	O	
ShareFile_SAML_SP	O	
WebEx_SAML_SP	O	O

Citrix Launcher

March 1, 2024

Citrix Launcher vous permet de personnaliser l'expérience de l'utilisateur pour les appareils Android Enterprise et les appareils Android d'ancienne génération déployés par Citrix Endpoint Management. Citrix Launcher vous permet d'empêcher les utilisateurs d'accéder à certains paramètres de l'appareil et de restreindre les appareils à une application ou à un petit ensemble d'applications.

La version minimale d'Android prise en charge pour la gestion Citrix Secure Hub de Citrix Launcher est Android 6.0.

Utilisez une **stratégie de configuration du Launcher** pour contrôler ces fonctionnalités de Citrix Launcher :

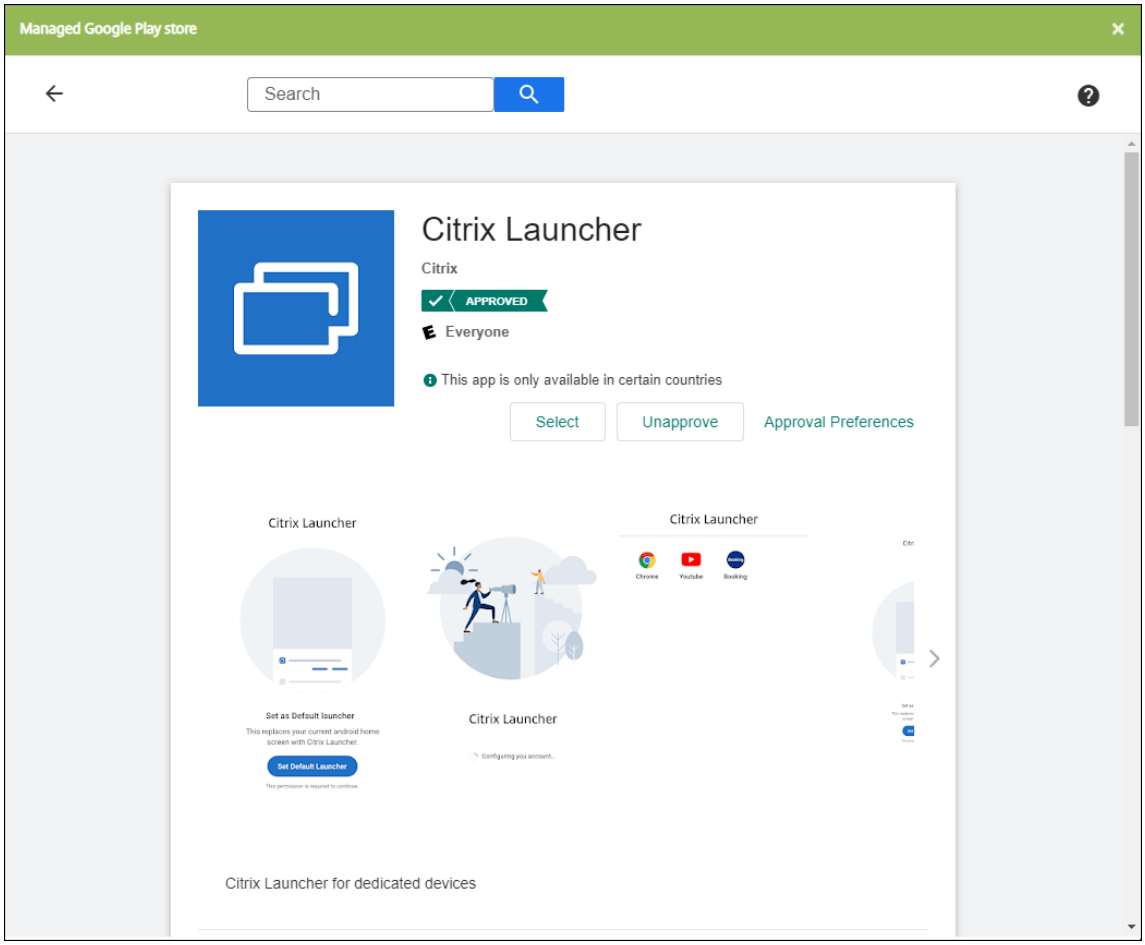
- Gérez les appareils Android Enterprise et les appareils Android d'ancienne génération de façon à ce que les utilisateurs puissent uniquement accéder aux applications que vous spécifiez.
- Si vous le souhaitez, vous pouvez spécifier une image de logo personnalisé pour l'icône Citrix Launcher et une image d'arrière-plan personnalisée pour Citrix Launcher.
- Spécifiez un mot de passe que les utilisateurs doivent entrer pour quitter le Launcher.

Citrix Launcher n'est pas destiné à être une couche de sécurité supplémentaire venant s'ajouter à ce que la plate-forme de l'appareil offre déjà.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurer Citrix Launcher pour les appareils Android Enterprise

1. Ajoutez l'application Citrix Launcher (com.citrix.launcher.droid) à Citrix Endpoint Management en tant qu'application de magasin public. Dans **Configurer > Applications**, cliquez sur **Ajouter**, puis cliquez sur **Magasin d'applications public**. Pour plus d'informations, consultez la section Ajouter une application d'un magasin d'applications public.



2. Dans la stratégie kiosque, spécifiez quelles applications doivent être disponibles sur les appareils appartenant à l'entreprise pour une utilisation dédiée (également appelés appareils d'entreprise à usage unique Android). Accédez à **Configurer > Stratégies d'appareil**, cliquez sur **Ajouter**, puis sélectionnez **Kiosque**. Sélectionnez ensuite l'application Citrix Launcher et toutes les applications supplémentaires dans la liste verte. Si vous avez déjà ajouté des applications à la liste, vous n'avez pas besoin de les télécharger à nouveau. Pour plus d'informations, consultez la section Paramètres Android Entreprise.

3. Ajoutez la stratégie de configuration du Launcher. Accédez à **Configurer > Stratégies d'appareil**, cliquez sur **Ajouter**, puis sélectionnez **Configuration du Launcher**. Dans la stratégie Configuration du Launcher, ajoutez l'une des applications que vous avez spécifiées dans la stratégie kiosque. Vous n'avez pas besoin d'ajouter toutes les applications que vous avez spé-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

cifiées dans la stratégie kiosque. Vous devez ajouter l'application Citrix Launcher uniquement dans la stratégie kiosque. Pour de plus amples informations, consultez la section Stratégie de configuration du Launcher.

4. Créez un groupe de mise à disposition et déployez des ressources. Pour plus d'informations, consultez la section Ajouter un groupe de mise à disposition et déployer des ressources de cet article.

Après avoir déployé Citrix Launcher sur des appareils Android Enterprise appartenant à l'entreprise pour une utilisation dédiée, Citrix Endpoint Management installe l'application et remplace le lanceur Citrix Secure Hub par défaut. Si vous quittez l'application Citrix Launcher, Citrix Secure Hub redevient le lanceur par défaut.

Configurer Citrix Launcher pour les appareils Android d'ancienne génération

> **Remarque :**
>
> En août 2020, Citrix a mis fin à la prise en charge de CitrixLauncher.apk pour les appareils Android d'ancienne génération. Vous pouvez continuer à utiliser l'ancienne application Citrix Launcher (com.citrix.launcher) pour les appareils Android sans recevoir les nouvelles mises à jour de fonctionnalités.

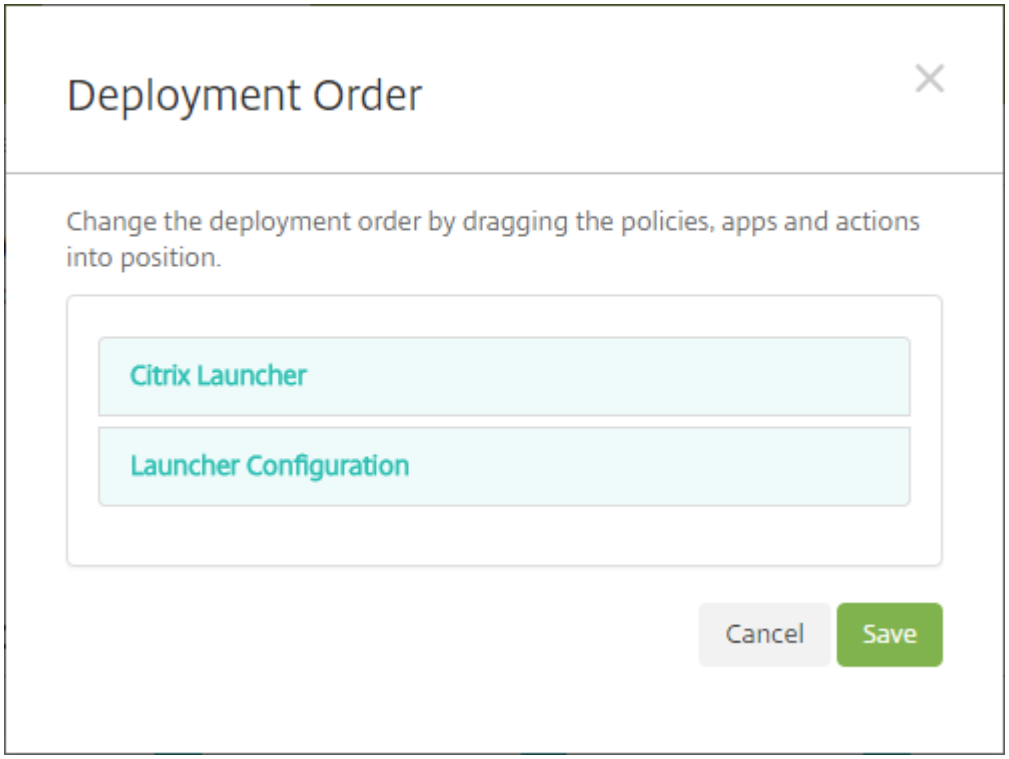
1. Pour localiser l'application Citrix Launcher, accédez à la page de téléchargement de Citrix Endpoint Management et recherchez **Citrix Launcher**. Téléchargez le dernier fichier. Le fichier est prêt à être téléchargé dans Citrix Endpoint Management et ne nécessite pas d'encapsulation.
2. Ajoutez la stratégie de configuration du Launcher. Accédez à **Configurer > Stratégies d'appareil**, cliquez sur **Ajouter**, puis sélectionnez **Configuration du Launcher**. Pour de plus amples informations, consultez la section Stratégie de configuration du Launcher.
3. Ajoutez l'application Citrix Launcher à Citrix Endpoint Management en tant qu'application d'entreprise. Dans **Configurer > Applications**, cliquez sur **Ajouter**, puis cliquez sur **Enterprise**. Pour de plus amples informations, consultez la section Ajouter une application d'entreprise.
4. Créez un groupe de mise à disposition et déployez des ressources. Pour plus d'informations, consultez la section Ajouter un groupe de mise à disposition et déployer des ressources de cet article.

Ajouter un groupe de mise à disposition et déployer des ressources

1. Créez un groupe de mise à disposition pour Citrix Launcher avec la configuration suivante dans **Configurer > Groupes de mise à disposition**.
    - Sur la page **Stratégies**, ajoutez une **Stratégie de configuration du Launcher**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Sur la page **Applications**, faites glisser **Citrix Launcher** vers **Applications requises**.
- Sur la page **Résumé**, cliquez sur **Ordre de déploiement** et assurez-vous que l'application **Citrix Launcher** précède la stratégie **Configuration du Launcher**.



2. Déployez des ressources vers un groupe de mise à disposition en envoyant une notification push à tous les utilisateurs du groupe de mise à disposition. Pour plus d'informations sur l'ajout de ressources à un groupe de mise à disposition, voir Déployer des ressources.

Gérer les appareils sans Citrix Launcher

Au lieu d'utiliser Citrix Launcher, vous pouvez utiliser des fonctionnalités déjà disponibles.

Pour provisionner des appareils dédiés, procédez comme suit :

1. Créez un profil d'inscription avec un **mode propriétaire de l'appareil** défini pour l'**appareil dédié**. Consultez la section Provisionner des appareils Android Enterprise dédiés et des profils d'inscription.
2. Créez une stratégie kiosque pour ajouter des applications à la liste verte et définir le mode de verrouillage des tâches. Si vous avez déjà ajouté des applications à la liste, vous n'avez pas besoin de les télécharger à nouveau. Pour plus d'informations, consultez la section Paramètres Android Entreprise.
3. Inscrivez chaque appareil dans le profil d'inscription que vous avez créé.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ajouter des applications via l'achat en volume Apple

March 1, 2024

Apple Business Manager (ABM) et Apple School Manager (ASM) vous permettent d'acheter des licences pour des applications et des livres en volume, et de synchroniser les informations d'achat en volume avec Citrix Endpoint Management. Vous pouvez ensuite utiliser Citrix Endpoint Management pour déployer ces applications et livres sur des appareils iOS et macOS. L'achat de contenus en volume simplifie le processus de recherche, d'achat et de distribution d'applications et de livres pour une organisation.

Pour plus d'informations sur l'achat de contenu à l'aide d'ABM ou ASM, consultez le guide de l'utilisateur Apple Business Manager ou le guide de l'utilisateur Apple School Manager. Cet article explique comment synchroniser les licences achetées en volume depuis ABM et ASM vers Citrix Endpoint Management, et comment gérer les licences.

> **Remarque :**
>
> Le programme Apple Volume Purchase Program (VPP) n'est plus disponible depuis le 14 janvier 2021. La fonction d'achat en volume a été intégrée dans ABM et ASM. Si vous utilisez actuellement le programme DEP (Device Enrollment Program) ou VPP, vous pouvez effectuer une mise à niveau vers ABM ou ASM. Pour de plus amples informations, consultez la documentation Apple Mise à niveau à partir des programmes de déploiement Apple.

À propos des achats en volume d'Apple

Lorsque vous achetez du contenu en volume à l'aide d'ABM ou d'ASM, notez les points suivants :

- Vous pouvez acheter des licences pour le contenu suivant :
  - Applications et livres publics
  - Applications personnalisées développées spécifiquement pour votre organisation
- Vous pouvez déployer des applications et des livres achetés en volume sur des appareils appartenant à l'entreprise et des appareils BYO. Les appareils appartenant à l'organisation inscrits via ABM ou ASM prennent en charge l'inscription MDM ou MDM+MAM, mais pas l'inscription MAM.
- Pour de plus amples informations sur la distribution d'applications, consultez la section Distribuer les applications Apple.
- Pour obtenir la liste des problèmes connus, consultez l'article du centre de connaissances CTX222633.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

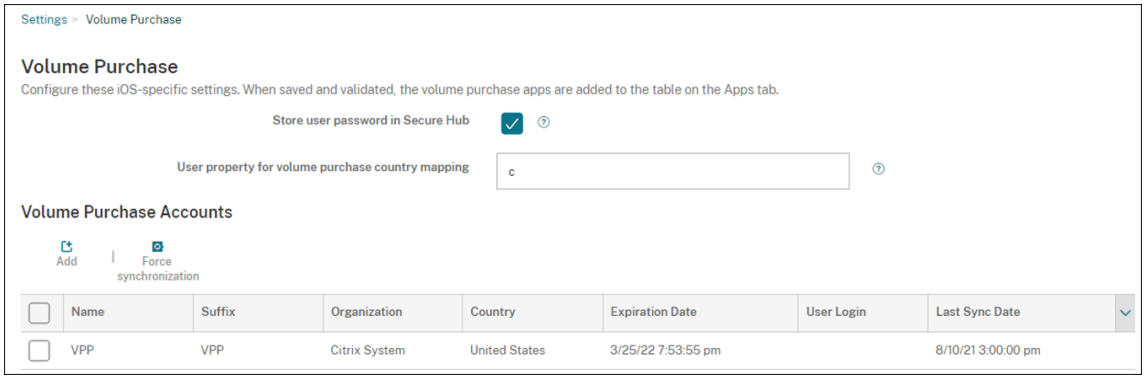
Ajouter un compte d'achat en volume

Après avoir acheté du contenu dans le portail ABM ou ASM, téléchargez le jeton de contenu associé à Citrix Endpoint Management à partir du portail. Ensuite, dans Citrix Endpoint Management, créez un compte d'achat en volume basé sur ce code de contenu. Ce code permet à Citrix Endpoint Management de synchroniser les licences de contenu depuis ABM ou ASM.

Avec l'achat en volume, vous pouvez acheter du contenu et le déployer sur des appareils à l'aide de licences gérées. Si vous utilisez actuellement des codes de téléchargement et que vous souhaitez passer à des licences gérées, consultez le document de support Apple.

Pour ajouter un compte d'achat en volume dans Citrix Endpoint Management, procédez comme suit :

1. Dans le portail ABM ou ASM, achetez le contenu selon vos besoins, puis téléchargez le fichier de code de contenu dans un emplacement sécurisé.
2. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
3. Cliquez sur **Achat en volume**. La page de configuration de **l'achat en volume** s'affiche.



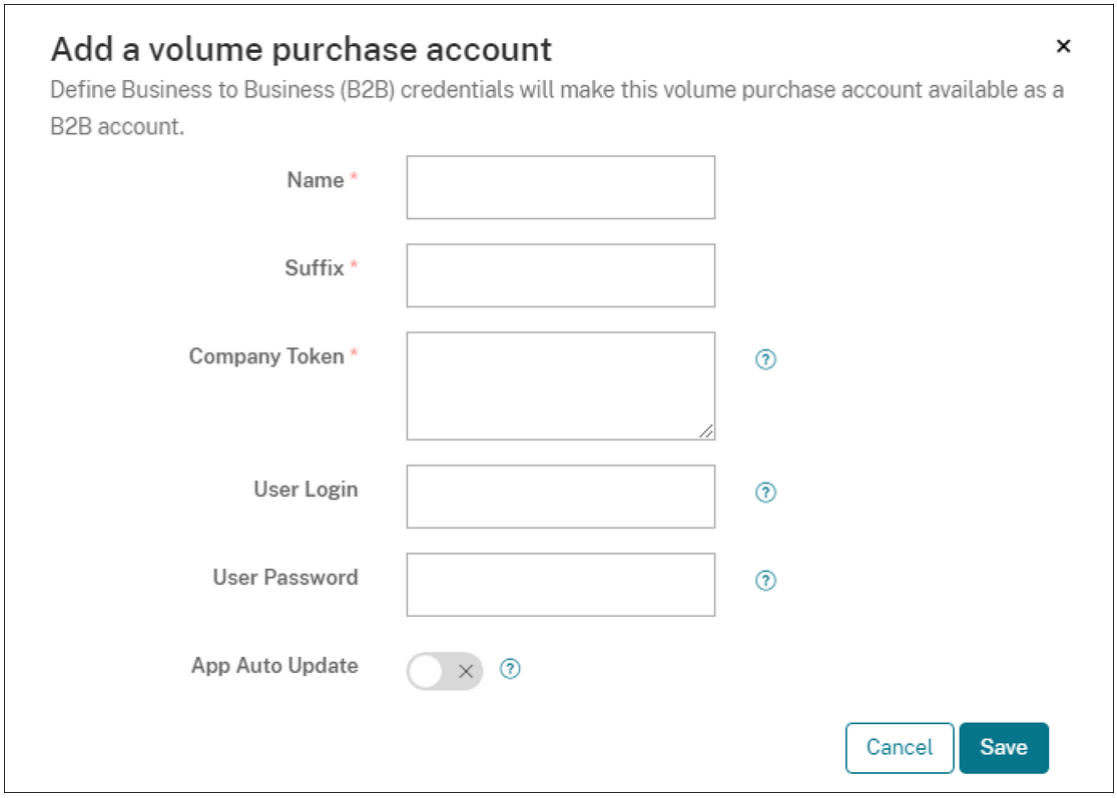
4. Configurez les paramètres suivants :

   - **Stocker le mot de passe utilisateur dans Citrix Secure Hub :** indiquez si un nom d'utilisateur et un mot de passe doivent être stockés dans Citrix Secure Hub en vue de l'authentification sur Citrix Endpoint Management. La valeur par défaut est **Activé**.
   - **Propriété utilisateur pour le choix du pays d'achat en volume :** entrez un code de pays pour autoriser les utilisateurs à télécharger des applications à partir de magasins d'applications spécifiques à un pays. Contactez votre gestionnaire de contenu pour obtenir ce code.

     Citrix Endpoint Management utilise ce code de pays pour choisir le pool de propriété de l'achat en volume. Par exemple, si la propriété utilisateur est définie sur États-Unis, l'utilisateur ne peut pas télécharger d'applications si le code de pays correspond au Royaume-Uni.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un compte d'achat en volume** s'affiche.



6. Configurez les paramètres de compte suivants :

> **Remarque :**
>
> Si vous utilisez Apple Configurator 1, chargez un fichier de licences : accédez à **Configurer > Applications**, accédez à la page de plate-forme d'une application et développez **Achat en volume**.

- **Nom :** entrez un nom descriptif pour l'application.
- **Suffixe :** entrez le suffixe qui apparaîtra avec les noms d'applications hérités des Apple Stores. Par exemple, si vous entrez **VP**, l'application **Citrix Secure Mail** s'affiche dans la liste des applications en tant que **Citrix Secure Mail - VP**.
- **Jeton d'entreprise :** copiez et collez le jeton de contenu que vous avez téléchargé à l'étape 1.
- **Connexion utilisateur :** (facultatif) entrez un nom d'utilisateur pour l'administrateur de ce compte d'achat en volume. S'ils sont configurés, le nom d'utilisateur et le mot de passe sont requis pour synchroniser les applications personnalisées achetées en volume dans Citrix Endpoint Management.
- **Mot de passe utilisateur :** (facultatif) entrez un mot de passe pour le nom d'utilisateur que vous avez saisi.
- **Actualisation auto des apps :** Si cette option est **activée**, les applications achetées en volume et les applications facultatives dans la console Citrix Endpoint Management sont

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

mises à jour automatiquement lorsqu'une nouvelle version est disponible. Vous devez toujours mettre à jour les applications d'entreprise et les applications de magasin d'applications public dans la console Citrix Endpoint Management manuellement. Si ce paramètre est défini sur **désactivé**, vous pouvez toujours mettre à jour les applications achetées en volume dans la console Citrix Endpoint Management manuellement. Une fois qu'une application est mise à jour dans la console, les appareils sur lesquels l'application est installée reçoivent également cette mise à jour. La valeur par défaut est **Désactivé**.

Une fois que le compte de volume a été ajouté, un message s'affiche pour vous informer des éléments suivants :

- Sur la page **Configurer > Applications**, les applications achetées en volume apparaissent dans la liste des applications. Les noms des applications s'affichent avec le suffixe que vous avez configuré.
- Sur la page **Configurer > Média**, les livres achetés en volume apparaissent dans la liste Média. Les noms des livres s'affichent avec le suffixe que vous avez configuré.

Configurer les applications achetées en volume

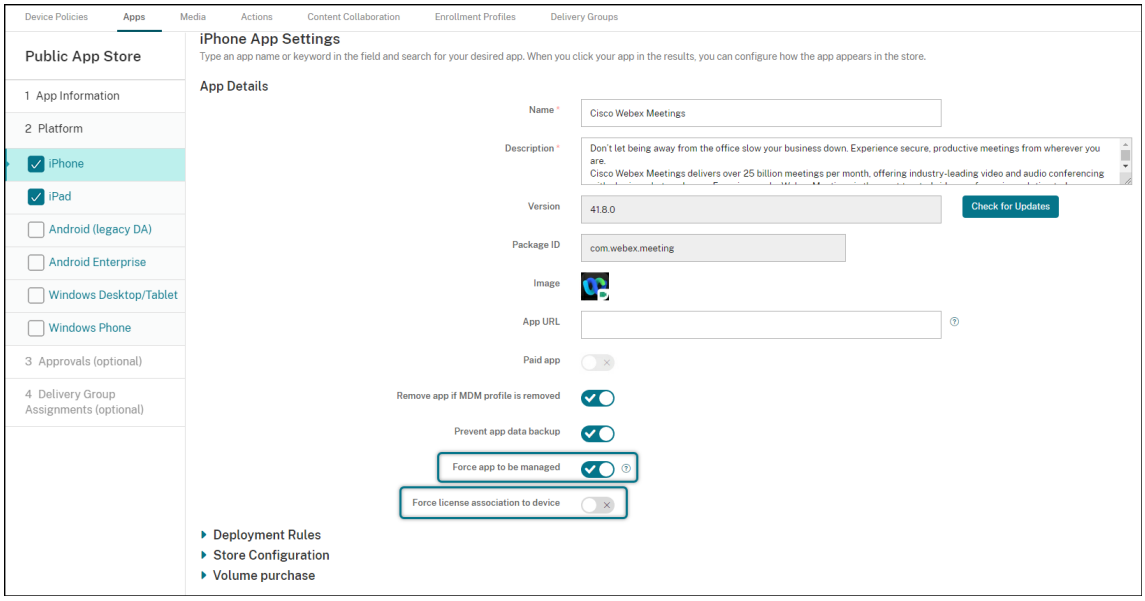
Une fois que vous avez ajouté un compte d'achat en volume, les informations de l'application sont synchronisées avec Citrix Endpoint Management et apparaissent sur la page **Configurer > Applications**. Vous pouvez à présent configurer ces applications, régler vos paramètres de groupe de mise à disposition et de stratégie pour les appareils iOS et macOS. Une fois que vous avez terminé cette configuration, les utilisateurs peuvent inscrire leurs appareils.

Lorsque vous configurez une application achetée en volume, notez les paramètres suivants :

- Sur la page **Configurer > Applications** :
  - Pour permettre à Citrix Endpoint Management de déployer une application sur un appareil plutôt que sur un utilisateur, activez **Forcer l'association de licence avec l'appareil**. Lorsque ce paramètre est activé, les utilisateurs n'ont pas besoin d'utiliser leur identifiant Apple et peuvent télécharger les applications sans se connecter à leur compte App Store.
  - Nous vous recommandons d'activer **Forcer l'application à être gérée** pour qu'une application s'installe automatiquement en tant qu'application gérée.

> **Remarque :**
>
> Pour activer le paramètre **Forcer l'application à être gérée**, vous devez configurer la propriété de serveur `apple.app.force.managed` sur **True** sur la page **Paramètres > Propriétés du serveur**. Pour plus d'informations, consultez Propriétés du serveur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Sur la page **Configurer > Groupe de mise à disposition** :

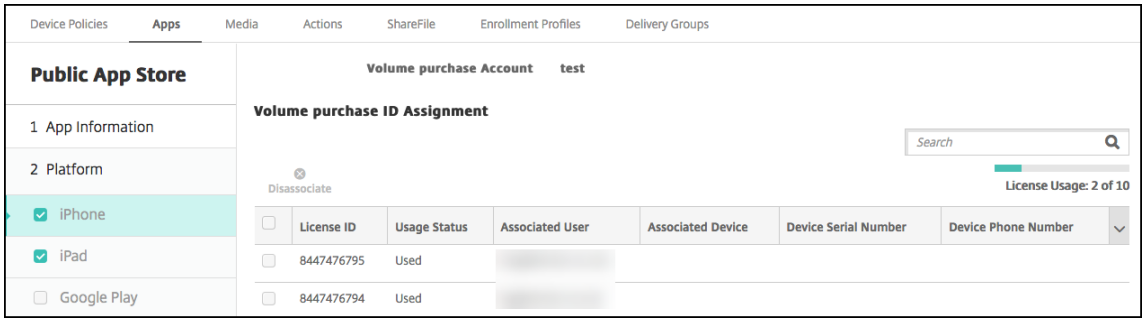
  Pour que l'application s'installe en mode silencieux sur les appareils utilisateur avec une interaction minimale de l'utilisateur, accédez à la page **Applications**, puis faites glisser l'application vers la liste **Applications requises**. Par défaut, les applications, à l'exception de Citrix Secure Hub, sont répertoriées sous **Applications facultatives**, ce qui signifie que les utilisateurs doivent démarrer l'installation de l'application manuellement via Citrix Secure Hub.

Suivre et gérer l'utilisation des licences d'application

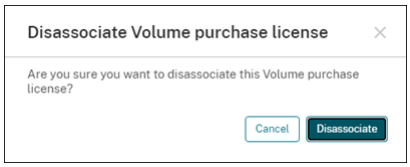
Vous pouvez suivre l'utilisation des licences associées à une application. Si nécessaire, vous pouvez reprendre une licence usagée et la mettre à la disposition d'un autre utilisateur ou d'un autre appareil.

1. Cliquez sur **Configurer > Applications**.
2. Sélectionnez une application, puis cliquez sur **Modifier**.
3. Accédez à la page **Plate-forme**, puis développez **Achat en volume**.
   Dans le tableau **Attribution de l'ID d'achat en volume**, vous pouvez suivre le nombre de licences utilisées et par quel utilisateur ou appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Pour reprendre une licence, sélectionnez-la, puis cliquez sur **Dissocier**.



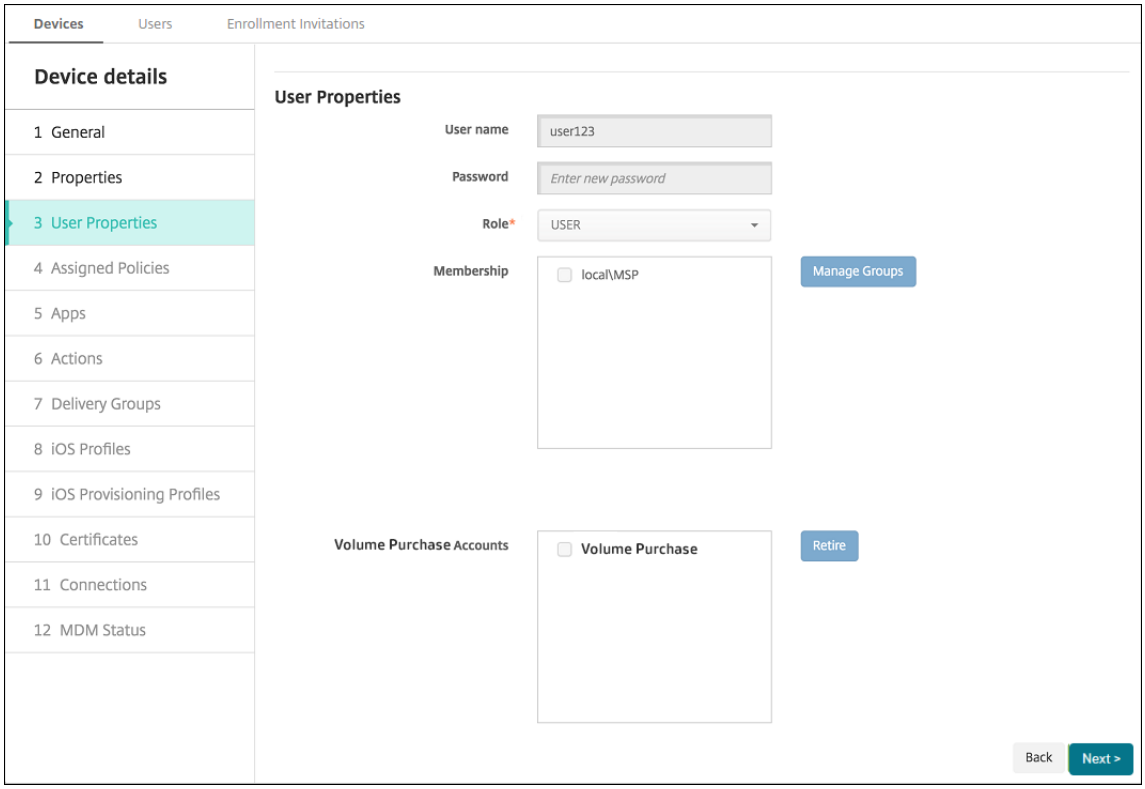
5. Cliquez sur **Dissocier** pour confirmer l'action.

Retirer un utilisateur du compte d'achat en volume

Si vous associez des licences d'application à des utilisateurs, vous pouvez retirer des utilisateurs des comptes d'achat en volume pour reprendre toutes les licences qui leur sont attribuées. Un cas d'utilisation peut être lorsqu'un utilisateur quitte votre organisation.

1. Cliquez sur **Gérer > Appareils**.
2. Sélectionnez l'appareil appartenant à l'utilisateur cible, puis cliquez sur **Modifier**.
3. Accédez à la page **Propriétés utilisateur** et sélectionnez les comptes d'achat en volume selon vos besoins.
4. Cliquez sur **Retirer**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Citrix Endpoint Management révoque les licences d'application des comptes d'achat en volume sélectionnés auprès de l'utilisateur.

Synchroniser les informations liées à l'application

Citrix Endpoint Management synchronise régulièrement les informations liées à l'application avec ABM ou ASM. Si nécessaire, vous pouvez synchroniser manuellement les informations liées à l'application. La synchronisation permet de s'assurer que les licences de l'application et les autres informations liées à l'application reflètent toutes les modifications. Ces modifications incluent la suppression manuelle d'une application importée à partir d'un compte d'achat en volume.

Modifier l'intervalle de synchronisation par défaut

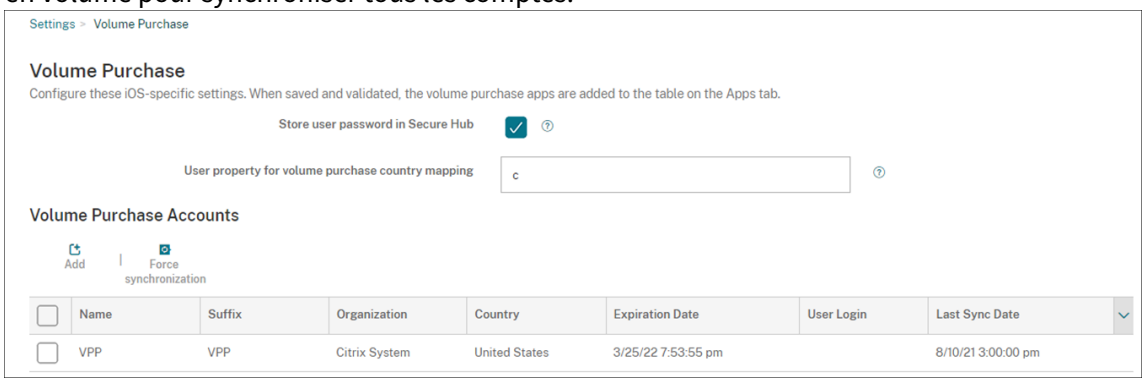
Par défaut, Citrix Endpoint Management actualise la ligne de base de licence d'achat en volume toutes les 1 440 minutes au minimum (24 heures). Un administrateur Citrix Cloud peut modifier l'intervalle par défaut via la propriété de serveur, `vpp.baseline`. Pour plus d'informations, consultez Propriétés du serveur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Synchroniser manuellement les informations liées à l'application

Vous pouvez forcer une synchronisation avec ABM ou ASM pour obtenir immédiatement les dernières informations liées à l'application.

1. Cliquez sur **Paramètres > Achat en volume**.
2. Sélectionnez un compte d'achat en volume, puis cliquez sur **Forcer la synchronisation**. Vous pouvez également cliquer sur **Forcer la synchronisation** sans sélectionner de compte d'achat en volume pour synchroniser tous les comptes.



3. Confirmez l'action de synchronisation. La synchronisation démarre.

   La synchronisation peut prendre plusieurs minutes, en fonction du nombre de licences d'achat en volume. Une fois la synchronisation terminée, Citrix Endpoint Management actualise la page **Achat en volume** et met à jour la date et l'heure de synchronisation dans la nouvelle colonne **Dernière date de synchronisation**.

Vérifier les mises à jour de l'application

Si vous activez le paramètre **Actualisation auto des apps** lorsque vous ajoutez un compte d'achat en volume, Citrix Endpoint Management vérifie régulièrement si de nouvelles versions des applications achetées en volume et facultatives sont disponibles et effectue des mises à jour. Si nécessaire, vous pouvez rechercher manuellement la nouvelle version d'une application et appliquer les mises à jour de l'application à Citrix Endpoint Management.

Une fois qu'Citrix Endpoint Management reçoit une nouvelle version d'une application requise, il envoie la nouvelle version sur l'appareil pour une installation silencieuse sans qu'une interaction de l'utilisateur ne soit nécessaire.

Pour vérifier et appliquer la nouvelle version d'une application, procédez comme suit :

1. Cliquez sur **Configurer > Applications**. La page **Applications** s'affiche.
2. Sélectionnez une application, puis cliquez sur **Modifier**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Accédez à la page **Plate-forme**, puis cliquez sur **Rechercher les mises à jour** en regard de **Version**.
4. Accédez à la page **Plate-forme**, puis cliquez sur **Rechercher les mises à jour** en regard de **Version**.
5. Dans la boîte de dialogue **Mettre à jour** qui apparaît, appliquez la mise à jour si une nouvelle version est disponible.

Renouveler le jeton de contenu de votre compte d'achat en volume

Un jeton de contenu expire chaque année. Lorsque le jeton arrive à expiration, Citrix Endpoint Management affiche un avertissement d'expiration de licence. Renouvelez le jeton de contenu à temps pour éviter toute interruption pour vos utilisateurs.

1. Depuis le portail ABM ou ASM, téléchargez un jeton mis à jour.
2. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
3. Cliquez sur **Achat en volume**. La page de configuration de l'achat en volume s'affiche.
4. Modifiez votre compte d'achat en volume avec les informations de jeton mises à jour.

Utiliser ShareFile avec Citrix Endpoint Management

March 1, 2024

Citrix Endpoint Management propose deux options d'intégration à ShareFile. Citrix Files et StorageZone Connector.

Citrix Files

Vous pouvez configurer Citrix Endpoint Management pour fournir l'accès à votre compte ShareFile. Cette configuration :

- Permet aux utilisateurs mobiles d'accéder à l'ensemble des fonctionnalités ShareFile, notamment le partage de fichiers, la synchronisation de fichiers et les connecteurs de zone de stockage.
- Permet à Citrix Files de bénéficier de l'authentification unique des utilisateurs d'applications de productivité mobiles, ainsi que des stratégies de contrôle d'accès complètes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Fournit la configuration ShareFile, le suivi de niveau de service et le contrôle de l'utilisation des licences via la console Citrix Endpoint Management.

Pour plus d'informations sur la configuration de Citrix Endpoint Management pour les comptes Enterprise, consultez la section SAML pour l'authentification unique avec Citrix Files.

Connecteurs StorageZone

Vous pouvez configurer Citrix Endpoint Management pour fournir l'accès uniquement aux connecteurs StorageZone créés via la console Citrix Endpoint Management. Cette configuration :

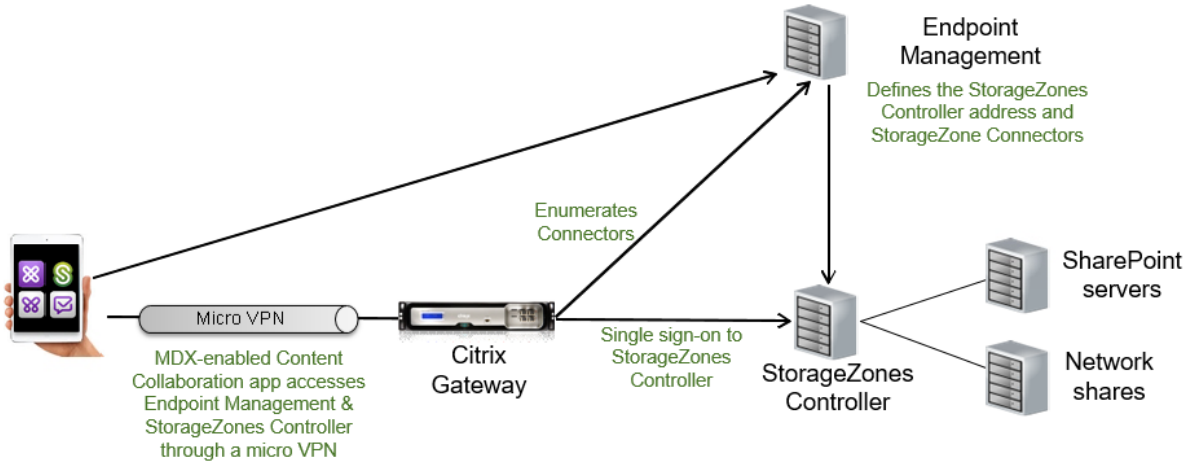
- Donne un accès mobile sécurisé aux référentiels de stockage locaux existants, tels que des sites SharePoint et des partages de fichiers réseau.
- Il n'est pas nécessaire de configurer un sous-domaine ShareFile ni d'héberger des données Citrix Files.
- Donne aux utilisateurs un accès mobiles aux données via les applications de productivité mobiles Citrix Files pour iOS et Android. Les utilisateurs peuvent modifier des documents Microsoft Office. Les utilisateurs peuvent aussi afficher un aperçu et annoter des fichiers PDF Adobe depuis des appareils mobiles
- Est conforme aux restrictions de sécurité contre la fuite d'informations utilisateur en dehors du réseau d'entreprise.
- Fournit une configuration simple des connecteurs StorageZone via la console Citrix Endpoint Management. Si vous décidez d'utiliser toutes les fonctionnalités Citrix Files avec Citrix Endpoint Management, vous pouvez modifier la configuration dans la console Citrix Endpoint Management.

Pour une intégration Citrix Endpoint Management utilisant uniquement des connecteurs StorageZone :

- ShareFile utilise votre configuration d'authentification unique à NetScaler Gateway pour s'authentifier auprès de StorageZone Controller.
- Citrix Endpoint Management ne s'authentifie par le biais de SAML, car le plan de contrôle de Citrix Files n'est pas utilisé.

Le diagramme suivant illustre l'architecture de haut niveau lors de l'utilisation de Citrix Endpoint Management avec des connecteurs StorageZone.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Exigences

- Versions minimales des composants :
  - ShareFile pour iOS (MDX) 5.3
  - ShareFile pour Android (MDX) 5.3
  - StorageZones Controller 5.11.20
    (Cet article contient des instructions pour configurer le StorageZones Controller 5.0).
- Assurez-vous que le serveur qui exécutera le StorageZones Controller répond à la configuration système requise. Pour la configuration requise, consultez la section Configuration requise.

La configuration requise pour les zones de stockage pour les données Citrix Files et pour les zones de stockage restreintes ne s'applique pas à une intégration Citrix Endpoint Management utilisant uniquement des StorageZone Connector.

Citrix Endpoint Management ne prend pas en charge les connecteurs Documentum.

- Pour exécuter des scripts PowerShell :
  - Exécutez les scripts dans la version 32 bits (x86) de PowerShell.

Tâches d'installation

Effectuez les tâches suivantes, dans l'ordre présenté, pour installer et configurer le StorageZones Controller. Ces étapes s'appliquent à une intégration Citrix Endpoint Management utilisant uniquement des connecteurs StorageZone. Certains de ces articles se trouvent dans la documentation relative au StorageZones Controller.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Configurer NetScaler pour le StorageZones Controller

   Vous pouvez utiliser NetScaler Gateway comme proxy DMZ pour StorageZones Controller.

2. Installer un certificat SSL

   Un StorageZones Controller qui héberge des zones standard nécessite un certificat SSL. Un StorageZones Controller qui héberge des zones restreintes et utilise une adresse interne ne nécessite pas de certificat SSL.

3. Préparer votre serveur

   Une configuration IIS et ASP.NET est nécessaire pour les connecteurs StorageZone.

4. Installer le StorageZones Controller

5. Préparer le StorageZones Controller pour une utilisation avec des connecteurs StorageZone uniquement

6. Spécifier un serveur proxy pour les zones de stockage

   La console du contrôleur de zones de stockage vous permet de spécifier un serveur proxy pour le contrôleur de zones de stockage. Vous pouvez également spécifier un serveur proxy à l'aide d'autres méthodes.

7. Configurer le contrôleur de domaine pour faire confiance au StorageZones Controller pour la délégation

   Configurez le contrôleur de domaine pour prendre en charge l'authentification NTLM ou Kerberos sur des partages réseau ou des sites SharePoint.

8. Associer un StorageZones Controller secondaire à une zone de stockage

   Pour configurer une zone de stockage pour une haute disponibilité, connectez au moins deux StorageZones Controller à celle-ci.

Installer le StorageZones Controller

1. Téléchargez et installez le logiciel du StorageZones Controller :

   a) Sur la page de téléchargement Citrix Files, https://www.citrix.com/downloads/sharefile.html, connectez-vous et téléchargez le dernier programme d'installation de StorageZones Controller.

   b) L'installation du contrôleur de zones de stockage modifie le site Web par défaut sur le serveur vers le chemin d'installation du contrôleur. Activez l'**authentification anonyme** sur le site Web par défaut.

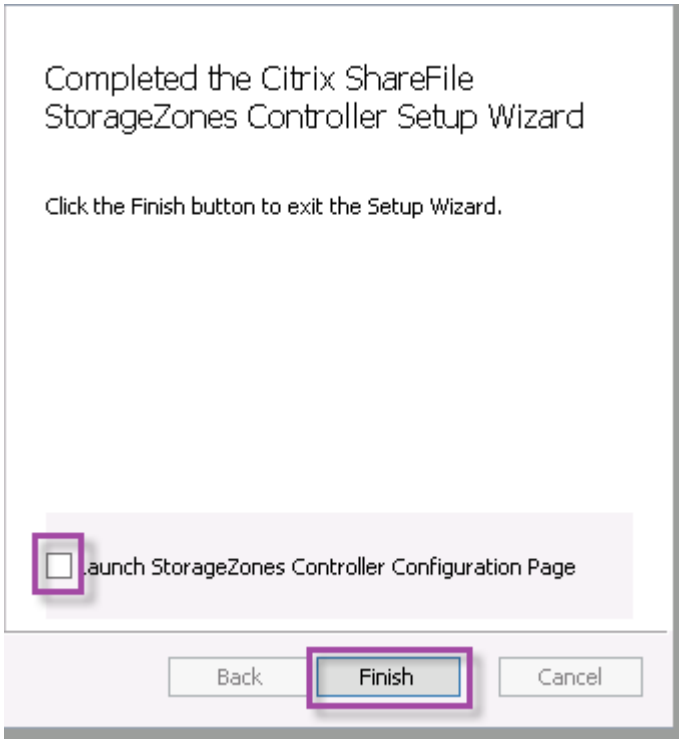
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Sur le serveur où vous souhaitez installer le StorageZones Controller, exécutez StorageCenter.msi.

   L'assistant d'installation du StorageZones Controller démarre.

3. Répondez aux invites :

   - Dans la page **Destination Folder**, si Internet Information Services (IIS) est installé dans l'emplacement par défaut, laissez les valeurs par défaut. Si ce n'est pas le cas, accédez à l'emplacement d'installation d'IIS.
   - Lorsque l'installation est terminée, désactivez la case à cocher **Launch Storage Zones Controller Configuration Page**, puis cliquez sur **Finish**.



4. Lorsque vous y êtes invité, redémarrez le StorageZones Controller.

5. Pour tester la réussite de l'installation, accédez à `https://localhost/`. (Si vous obtenez une erreur de certificat, envisagez plutôt de vous connecter avec HTTP.) Si l'installation réussit, le logo Citrix Files apparaît.

   Si le logo Citrix Files n'apparaît pas, désactivez le cache du navigateur et essayez à nouveau.

   > **Important :**
   >
   > Si vous prévoyez de cloner le contrôleur de zones de stockage, capturez l'image de disque avant de procéder à la configuration du contrôleur de zones de stockage.

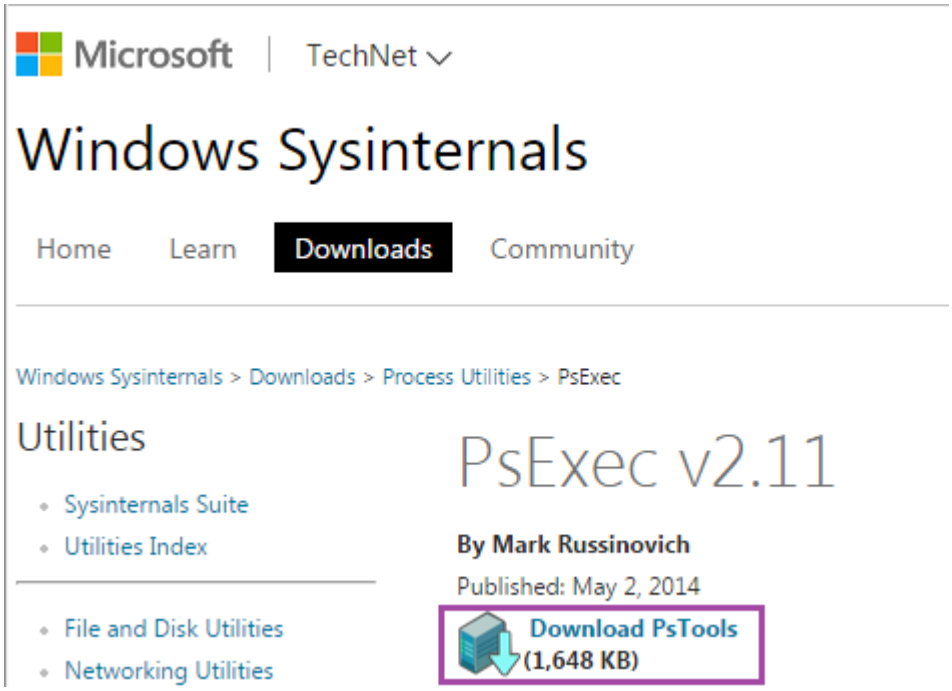
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Préparer le StorageZones Controller pour une utilisation avec des connecteurs StorageZone uniquement

Pour une intégration avec des connecteurs StorageZone uniquement, vous n'utilisez pas la console d'administration du StorageZones Controller. Cette interface nécessite un compte d'administrateur Citrix Files, qui n'est pas nécessaire pour cette solution. Par conséquent, vous exécutez un script PowerShell pour préparer le StorageZones Controller pour une utilisation sans le plan de contrôle Citrix Files. Le script effectue les actions suivantes :

- Enregistre le StorageZones Controller actuel en tant que StorageZones Controller principal. Vous pouvez joindre un contrôleur de zones de stockage secondaire au contrôleur principal plus tard.
- Crée une zone et définit la phrase secrète pour celle-ci.

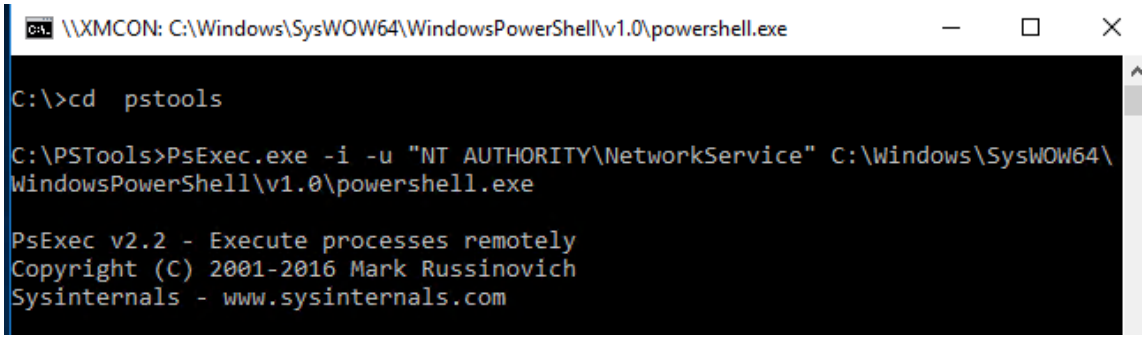
1. À partir de votre serveur StorageZone Controller principal, téléchargez l'outil PsExec : accédez à Microsoft Windows Sysinternals, puis cliquez sur **Download PsTools**. Extrayez l'outil dans la racine du lecteur C.



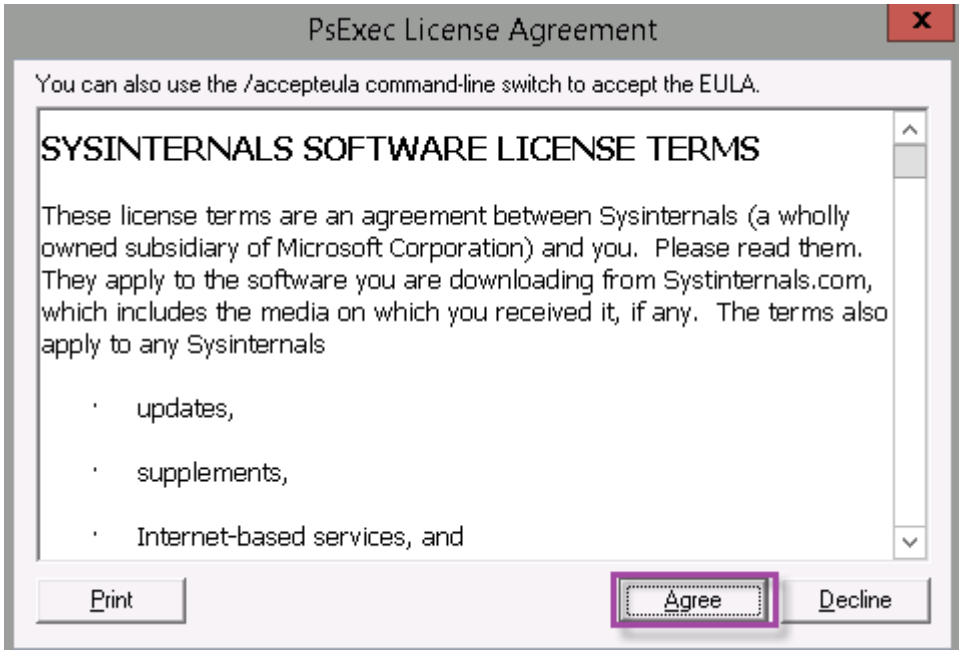
2. Exécutez l'outil PsExec : ouvrez l'invite de commande en tant qu'utilisateur administrateur et tapez ce qui suit :

```
1 ```
2 cd c:\pstools
3 PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
    \WindowsPowerShell\v1.0\powershell.exe
4 <!--NeedCopy--> ```
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Lorsque vous y êtes invité, cliquez sur **Agree** pour exécuter l'outil Sysinternals.



Une fenêtre PowerShell s'ouvre.

4. Dans la fenêtre PowerShell, tapez ce qui suit :

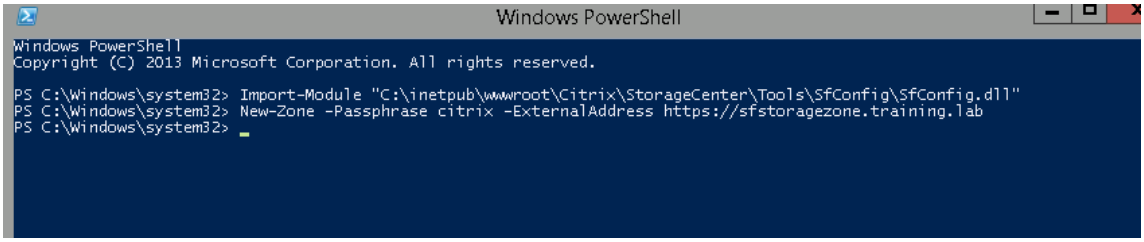
```
1 ```
2 Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\
    SfConfig\SfConfig.dll"
3 New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
    com
4 <!--NeedCopy--> ```
```

Où :

Phrase secrète : phrase secrète que vous souhaitez attribuer au site. Prenez note de cette dernière. Vous ne pouvez pas récupérer la phrase secrète à partir du contrôleur. Si vous perdez la phrase secrète, vous ne pouvez pas réinstaller les zones de stockage, joindre d'autres StorageZones Controller à la zone de stockage ou récupérer la zone de stockage si le serveur échoue.

ExternalAddress : nom de domaine complet externe du serveur du StorageZones Controller.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Votre StorageZones Controller principal est maintenant prêt.

Avant de vous connecter à Citrix Endpoint Management pour créer des connecteurs StorageZone, effectuez la configuration suivante, le cas échéant :

Spécifier un serveur proxy pour les zones de stockage

Configurer le contrôleur de domaine pour faire confiance au StorageZones Controller pour la délégation

Associer un StorageZones Controller secondaire à une zone de stockage

Pour créer des connecteurs StorageZone, voir Définir des connexions de StorageZones Controller dans Citrix Endpoint Management.

Associer un StorageZones Controller secondaire à une zone de stockage

Pour configurer une zone de stockage pour une haute disponibilité, connectez au moins deux StorageZones Controller à celle-ci. Pour joindre un contrôleur de zones de stockage secondaire à une zone, installez le contrôleur de zones de stockage sur un second serveur. Joignez ensuite ce contrôleur à la zone du contrôleur principal.

1. Ouvrez une fenêtre PowerShell sur le serveur du StorageZones Controller que vous voulez joindre au serveur principal.
2. Dans la fenêtre PowerShell, tapez ce qui suit :

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP
   >
   ```

   Par exemple :

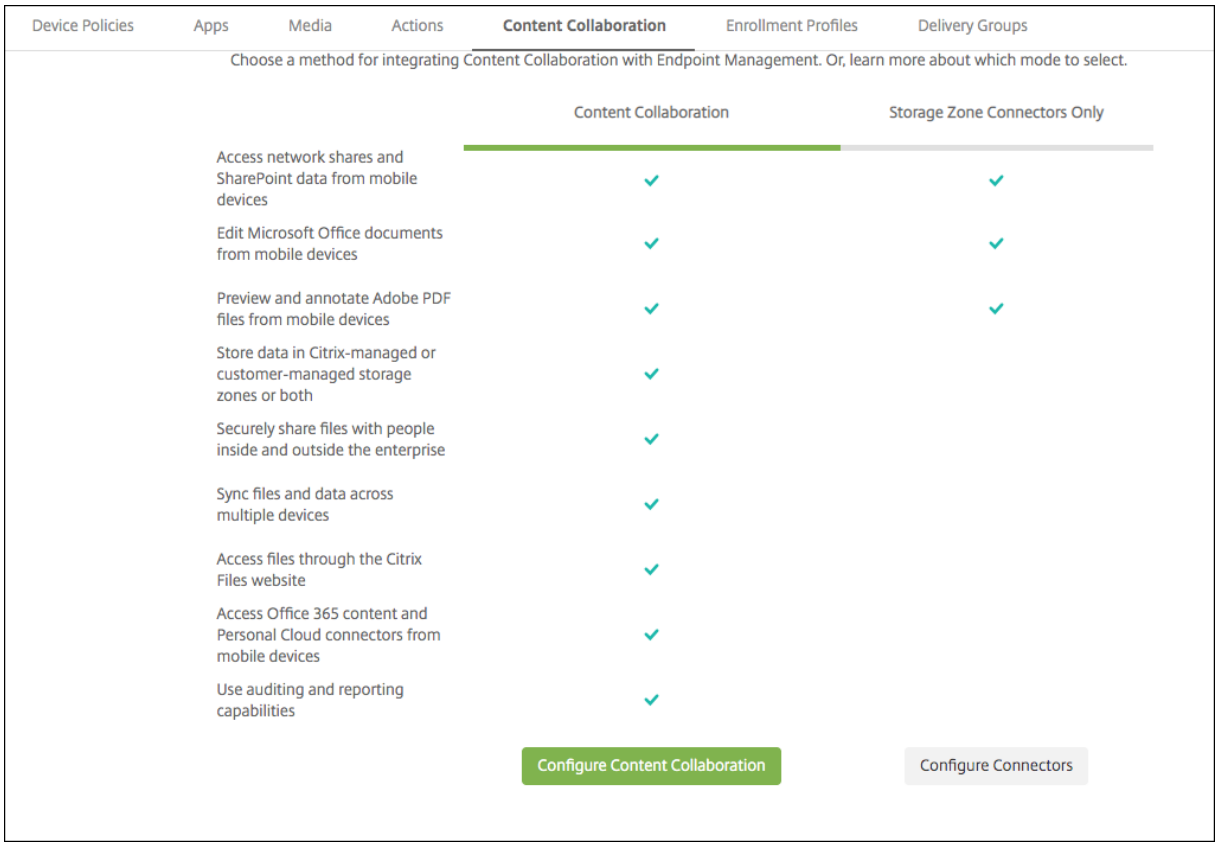
   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

Définir des connexions de StorageZones Controller dans Citrix Endpoint Management

Avant d'ajouter des connecteurs StorageZone, vous configurez les informations de connexion pour chaque StorageZones Controller activé pour les connecteurs StorageZone. Vous pouvez définir les StorageZones Controller comme décrit dans cette section, ou lorsque vous ajoutez un connecteur.

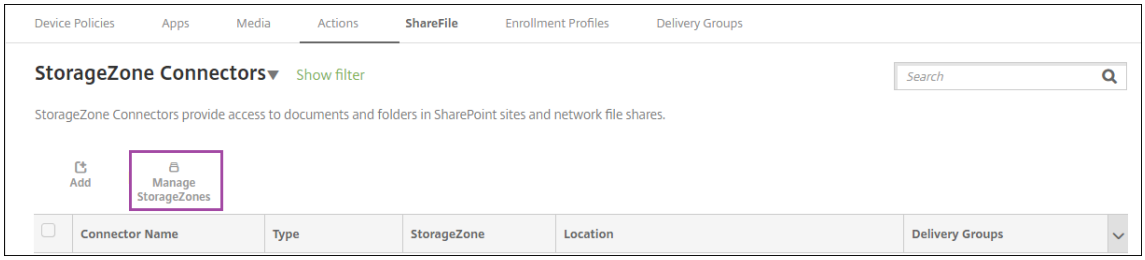
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Lors de votre premier accès à la page **Configurer > ShareFile**, la page résume les différences entre l' utilisation de Citrix Endpoint Management avec des comptes Enterprise et avec des connecteurs de zone de stockage.



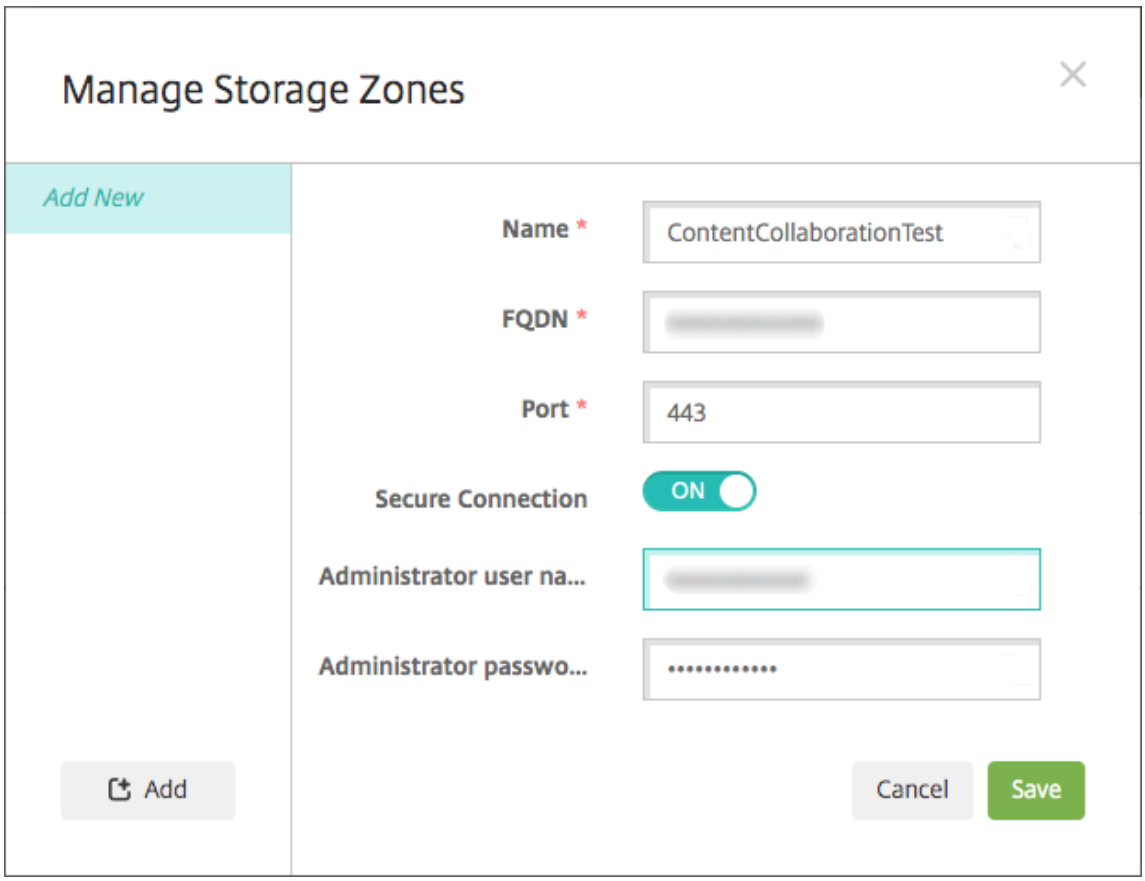
Cliquez sur **Configurer des connecteurs** pour suivre les étapes de configuration décrites dans cet article.

1. Dans **Configurer > ShareFile**, cliquez sur **Gérer les zones de stockage**.



2. Dans **Gérer les zones de stockage**, ajoutez les informations de connexion.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Nom :** nom descriptif de la zone de stockage, utilisé pour identifier la zone de stockage dans Citrix Endpoint Management. N'insérez pas d'espace ou de caractères spéciaux dans le nom.
- **Nom de domaine complet et port :** nom de domaine complet et numéro de port pour un contrôleur de zones de stockage accessible depuis le serveur Citrix Endpoint Management.
- **Connexion sécurisée :** si vous utilisez SSL pour les connexions au StorageZones Controller, utilisez le paramètre par défaut, Activé. Si vous n'utilisez pas SSL pour les connexions, définissez ce paramètre sur Désactivé.
- **Nom d'utilisateur administrateur** et **Mot de passe administrateur** : nom d'utilisateur du compte de service administrateur (au format domaine\administrateur) et mot de passe. Sinon, un compte d'utilisateur avec les autorisations Lire et Écrire sur les StorageZones Controller.

3. Cliquez sur **Enregistrer**.
4. Pour tester la connexion, vérifiez que le serveur Citrix Endpoint Management peut accéder au nom de domaine complet du StorageZones Controller sur le port 443.
5. Pour définir une autre connexion au StorageZones Controller, cliquez sur le bouton **Ajouter** dans **Gérer les zones de stockage**.

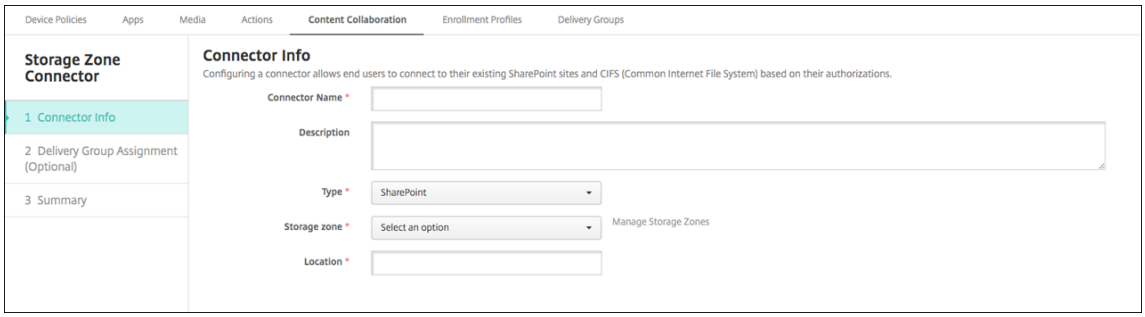
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour modifier ou supprimer les informations d'une connexion de StorageZones Controller, sélectionnez le nom de la connexion dans **Gérer les StorageZone**. Cliquez ensuite sur **Modifier** ou **Supprimer**.

Ajouter un connecteur StorageZone dans Citrix Endpoint Management

1. Accédez à **Configurer > ShareFile**, puis cliquez sur **Ajouter**.

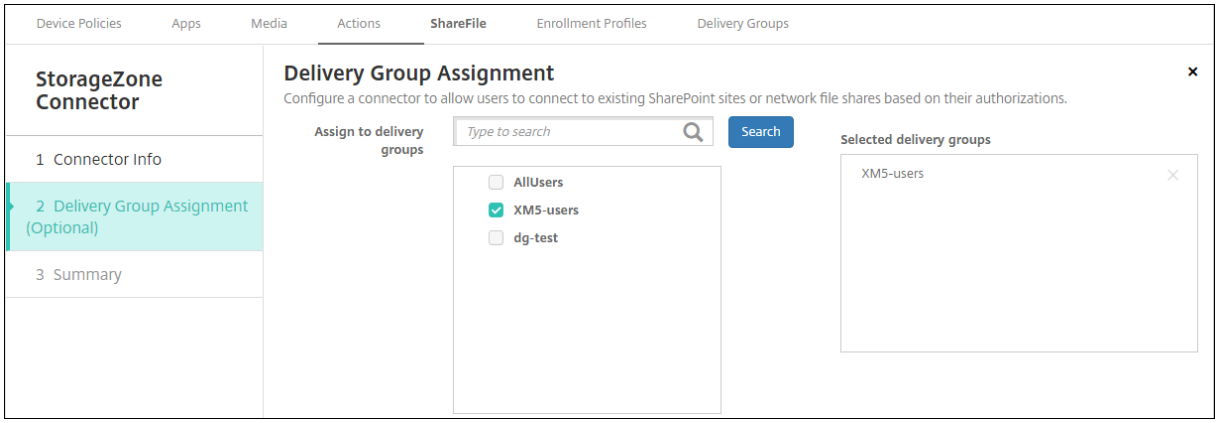
2. Sur la page **Informations sur le connecteur**, configurez les paramètres suivants :



   - **Nom du connecteur :** nom qui identifie le connecteur StorageZone dans Citrix Endpoint Management.
   - **Description :** notes facultatives sur ce connecteur.
   - **Type :** choisissez **SharePoint** ou **Réseau**.
   - **Zone de stockage :** choisissez la zone de stockage associée au connecteur. Si la zone de stockage ne figure pas dans la liste, cliquez sur **Gérer les zones de stockage** pour définir le StorageZones Controller.
   - **Emplacement :** pour SharePoint, spécifiez l'URL du site SharePoint au niveau racine, de la collection du site ou de la bibliothèque de documents, au format `https://sharepoint.company.com`. Pour un partage réseau, spécifiez le nom de domaine complet du chemin d'accès UNC (Uniform Naming Convention), au format \\serveur\partage.

3. (Facultatif) Sur la page **Attribution de groupes de mise à disposition**, attribuez le connecteur à des groupes de mise à disposition. Vous pouvez également associer des connecteurs à des groupes de mise à disposition à l'aide de **Configurer > Groupes de mise à disposition**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. Sur la page **Résumé**, vous pouvez vérifier les options que vous avez configurées. Pour régler la configuration, cliquez sur **Précédent**.
2. Cliquez sur **Enregistrer** pour enregistrer le connecteur.
3. Testez le connecteur :

   a) Lorsque vous encapsulez les clients Citrix Files, définissez la stratégie d'accès réseau sur **Tunnel - SSO Web**.

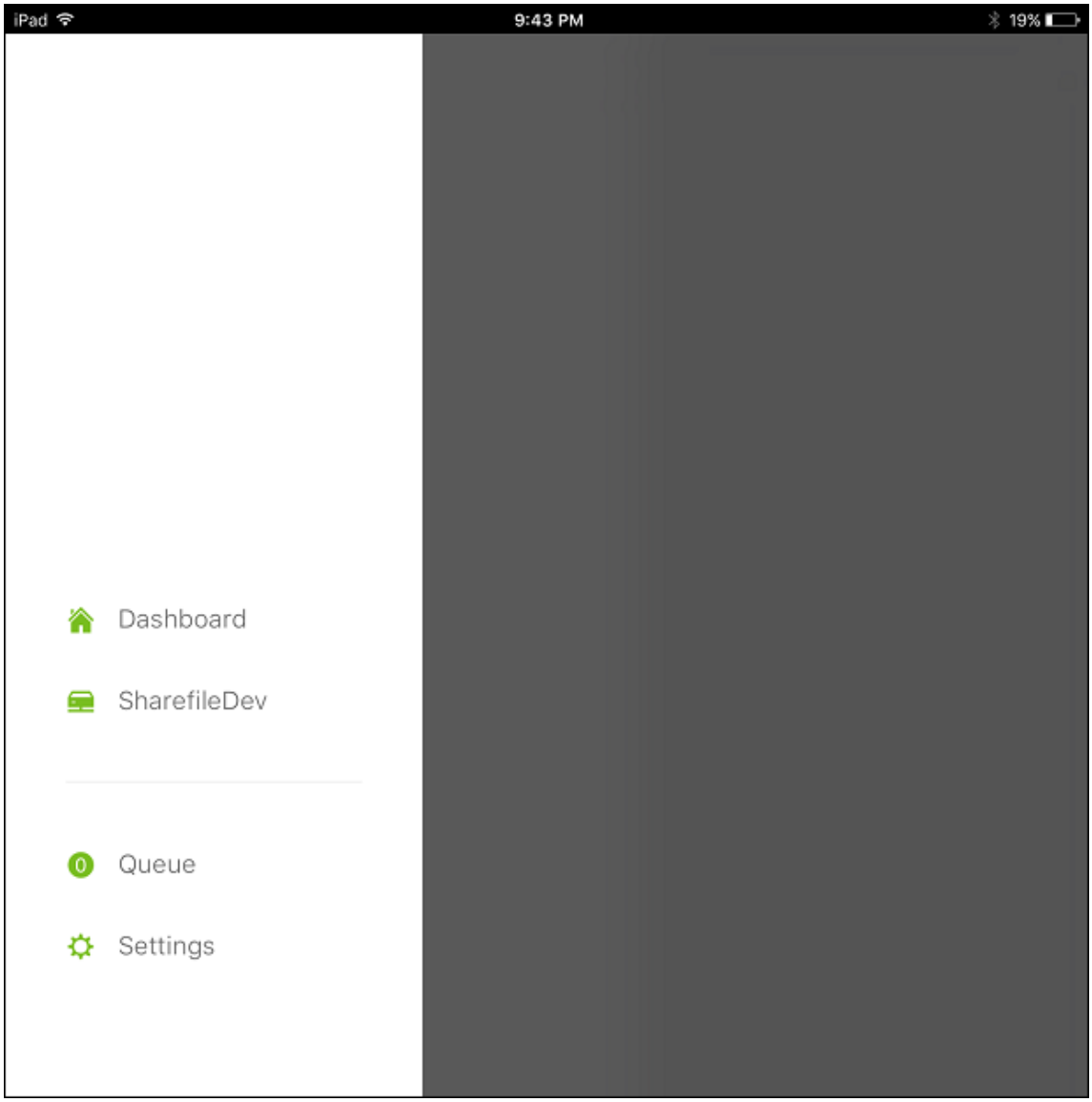
   Dans ce mode de tunneling, l'infrastructure MDX arrête le trafic SSL/HTTP en provenance d'une application MDX, puis initialise de nouvelles connexions aux connexions internes pour le compte de l'utilisateur. Ce paramètre de stratégie permet à l'infrastructure MDX de détecter et de répondre aux demandes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

   b) Ajoutez les clients Citrix Files à Citrix Endpoint Management. Pour de plus amples informations, consultez la section Pour ajouter des clients Citrix Files à Citrix Endpoint Management.

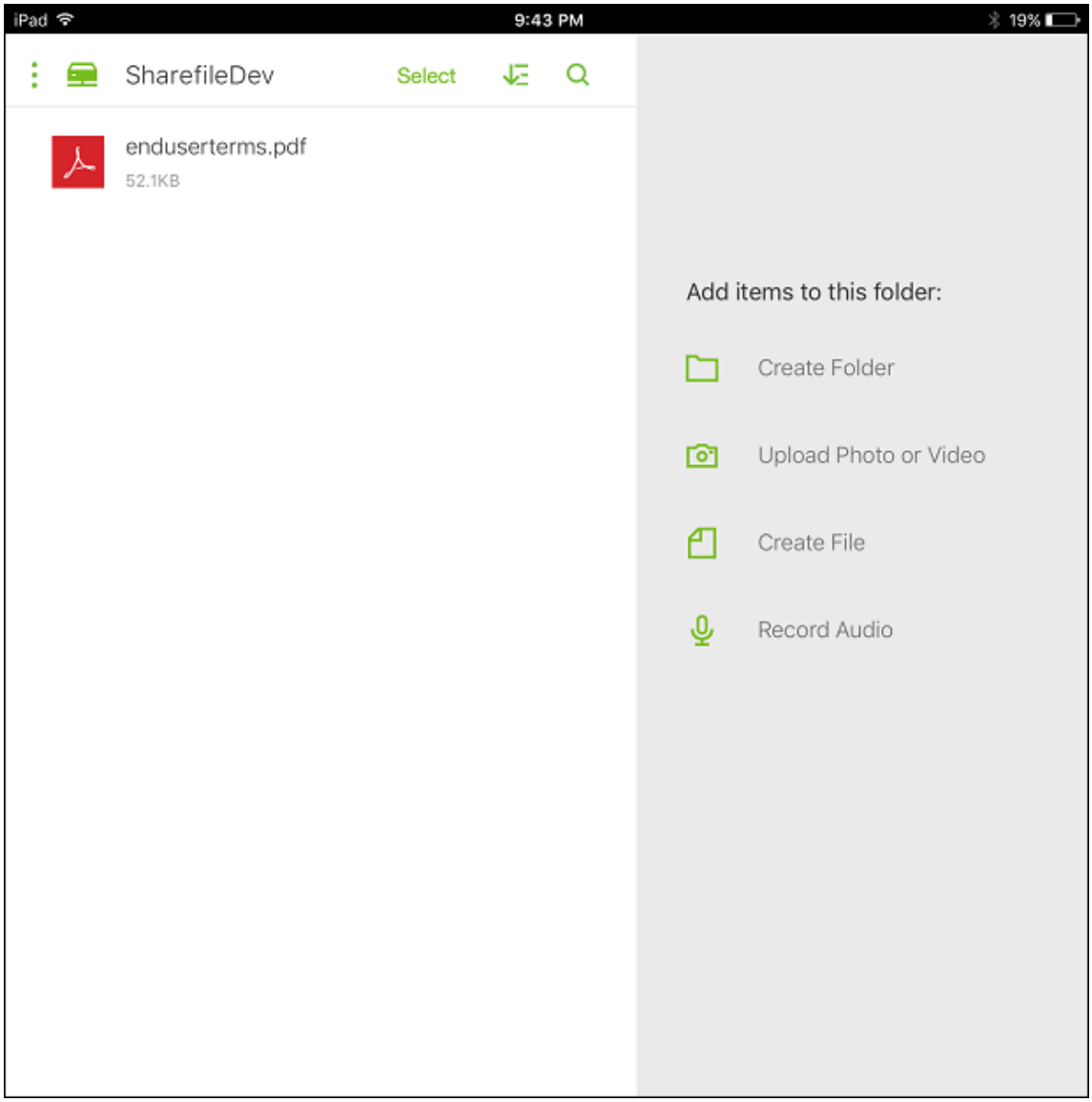
   c) À partir d'un appareil pris en charge, vérifiez l'authentification unique à Citrix Files et aux connecteurs.

Dans les exemples suivants, SharefileDev est le nom d'un connecteur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

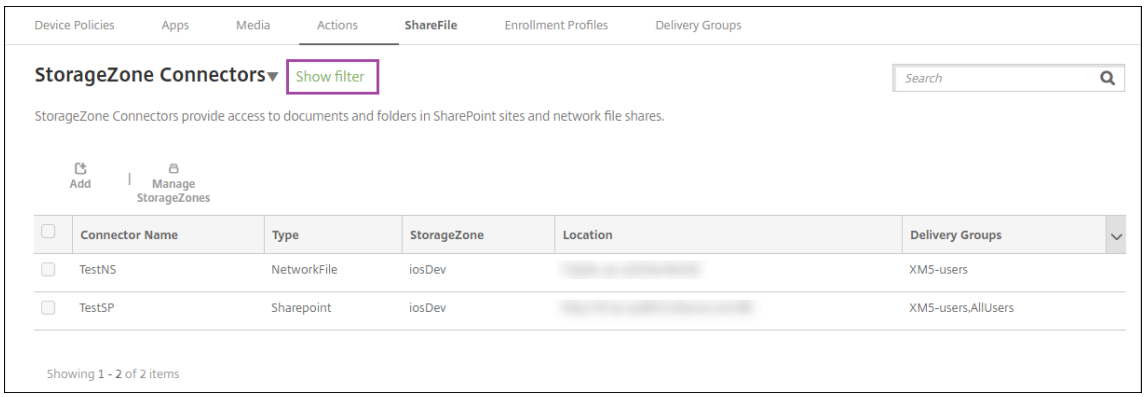


Filtrer la liste des connecteurs StorageZone

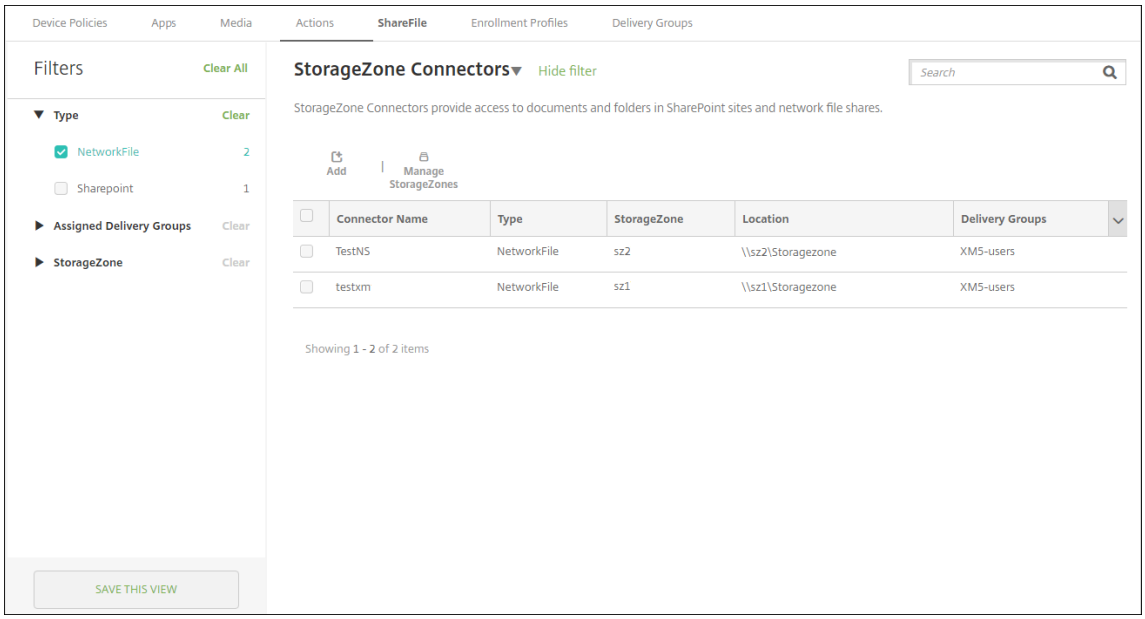
Vous pouvez filtrer la liste des connecteurs StorageZone par type de connecteur, groupe de mise à disposition attribué et zone de stockage.

1. Accédez à **Configurer > ShareFile**, puis cliquez sur **Afficher le filtre**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

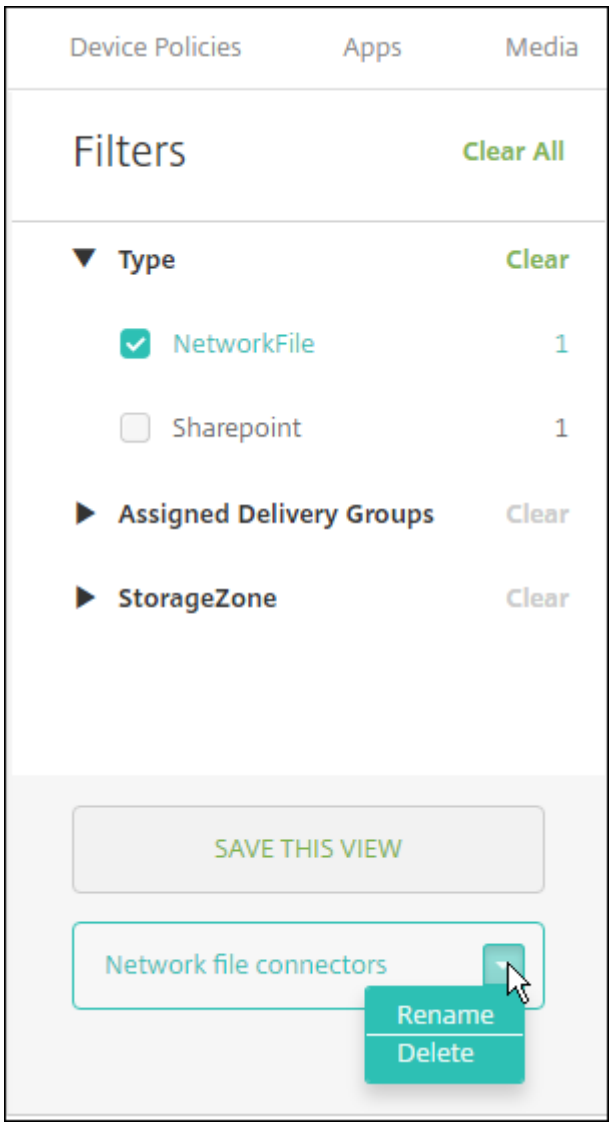


2. Développez les en-têtes de filtre pour effectuer une sélection. Pour enregistrer un filtre, cliquez sur **Enregistrer cette vue**, entrez le nom du filtre et cliquez sur **Enregistrer**.



3. Pour renommer ou supprimer un filtre, cliquez sur l'icône de flèche en regard du nom du filtre.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

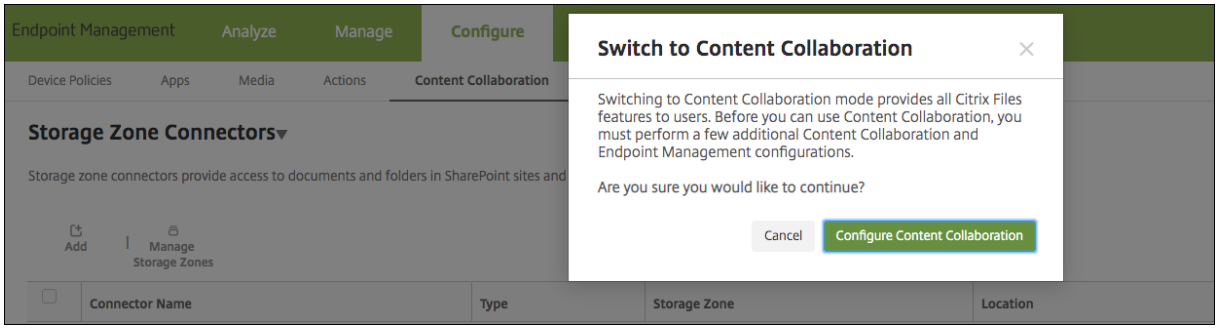


Basculer vers un compte Enterprise

Après l'intégration des connecteurs StorageZone avec Citrix Endpoint Management, vous pouvez basculer vers l'ensemble complet des fonctionnalités Enterprise. Citrix Endpoint Management conserve vos paramètres d'intégration de StorageZone Connector existants.

Accédez à **Configurer > ShareFile**, cliquez sur le menu déroulant **Connecteurs de zone de stockage**, puis cliquez sur **Configurer ShareFile**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pour plus d'informations sur la configuration des comptes Enterprise, consultez la section SAML pour l'authentification unique avec Citrix Files.

SmartAccess pour applications HDX

March 1, 2024

Cette fonctionnalité vous permet de contrôler l'accès aux applications HDX en fonction des propriétés d'un appareil, des propriétés utilisateur d'un appareil ou des applications installées sur un appareil. Pour utiliser cette fonctionnalité, vous définissez des actions automatisées pour marquer l'appareil comme non conforme pour refuser l'accès de cet appareil. Utilisées en conjonction avec cette fonctionnalité, les applications HDX sont configurées dans Citrix Virtual Apps and Desktops à l'aide d'une stratégie SmartAccess qui refuse l'accès aux appareils non conformes. Citrix Endpoint Management communique l'état de l'appareil à StoreFront à l'aide d'une balise signée et cryptée. Ensuite, StoreFront autorise ou refuse l'accès en fonction de la stratégie de contrôle d'accès de l'application.

Pour utiliser cette fonctionnalité, votre déploiement requiert :

- Citrix Virtual Apps and Desktops
- Citrix Endpoint Management
- Citrix Endpoint Management configuré avec un certificat SAML à utiliser pour la signature et le cryptage des balises. Le même certificat sans clé privée est chargé sur le serveur StoreFront.

Pour commencer à utiliser cette fonctionnalité :

- Configurer le certificat de Citrix Endpoint Management Server pour le magasin StoreFront
- Configurer au moins un groupe de mise à disposition Citrix Virtual Apps and Desktops avec la stratégie SmartAccess requise
- Définir les actions automatisées dans Citrix Endpoint Management

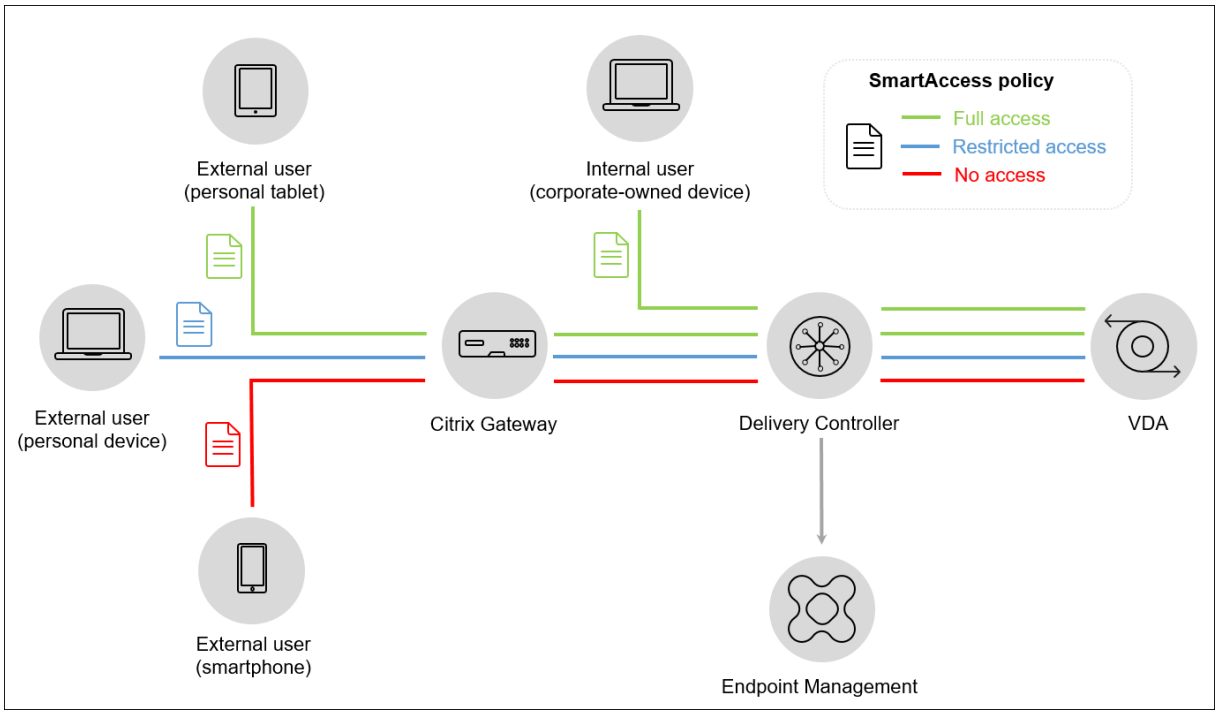
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SmartAccess aux applications HDX pour les points de terminaison

Grâce à cette fonctionnalité, vous pouvez appliquer un contrôle d'accès basé sur des stratégies pour restreindre l'accès des appareils aux applications HDX. Vous pouvez appliquer ces niveaux d'accès aux applications HDX :

- **Accès complet**. Un appareil peut accéder à toutes les applications HDX fournies par le magasin Citrix Secure Hub.
- **Accès restreint**. Un appareil peut accéder à une ou plusieurs applications HDX, mais pas à toutes.
- **Aucun accès**. Un appareil ne peut accéder à aucune application HDX.

Le graphique suivant illustre le fonctionnement du contrôle d'accès. Une tentative de lancement d'application HDX dans Citrix Secure Hub déclenche une requête auprès d'un Delivery Controller. Le Delivery Controller transmet ensuite la demande au serveur Citrix Endpoint Management pour validation. Le résultat de la validation détermine le niveau d'accès de l'appareil. Par exemple, l'accès à une application HDX est refusé si l'appareil est jailbreaké.



Exporter et configurer le certificat de Citrix Endpoint Management Server et le charger vers le magasin StoreFront

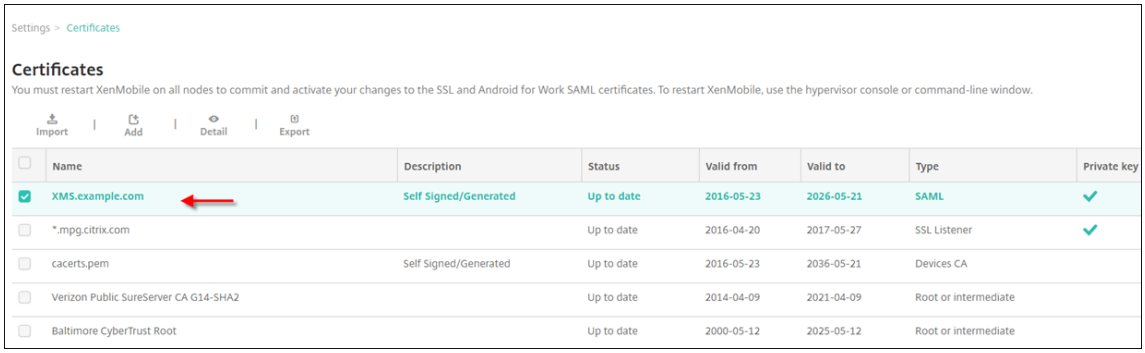
SmartAccess utilise des balises signées et cryptées pour communiquer entre le serveur StoreFront et Citrix Endpoint Management Server. Pour activer cette communication, vous ajoutez le certificat de Citrix Endpoint Management Server au magasin StoreFront.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

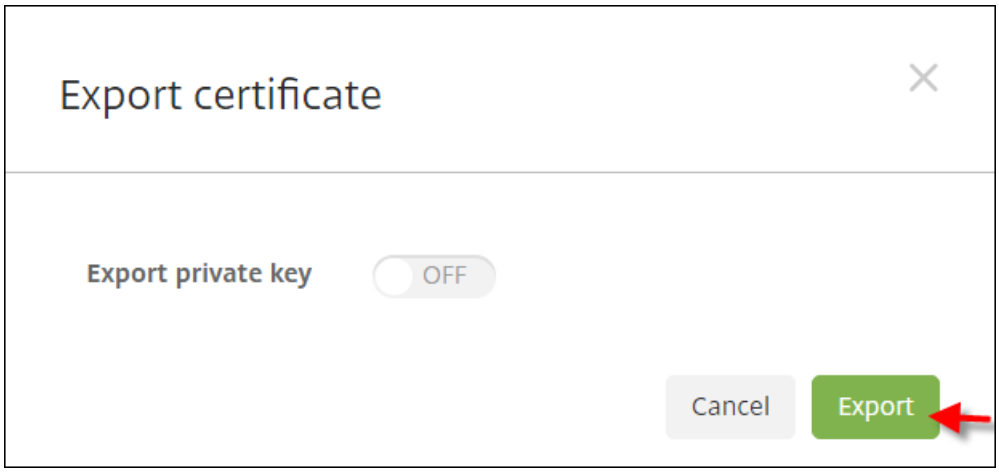
Pour plus d'informations sur l'intégration de StoreFront et Citrix Endpoint Management lorsque Citrix Endpoint Management est activé avec l'authentification basée sur domaine et sur certificats, consultez le Centre de connaissances.

Exporter le certificat SAML à partir de Citrix Endpoint Management

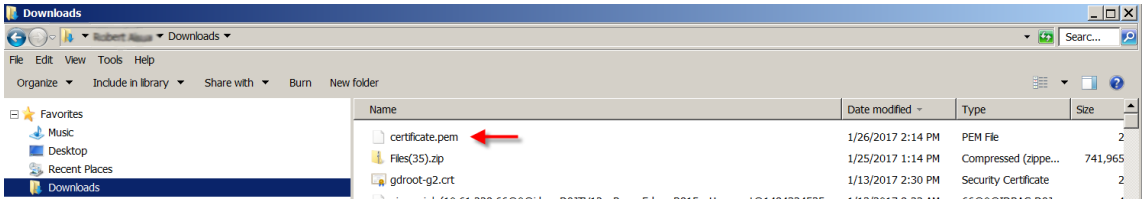
1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche. Cliquez sur **Certificats**.
2. Localisez le certificat SAML pour Citrix Endpoint Management Server.



3. Assurez-vous que **Exporter clé privée** est défini sur **Désactivé**. Cliquez sur **Exporter** pour exporter le certificat vers votre répertoire de téléchargement.



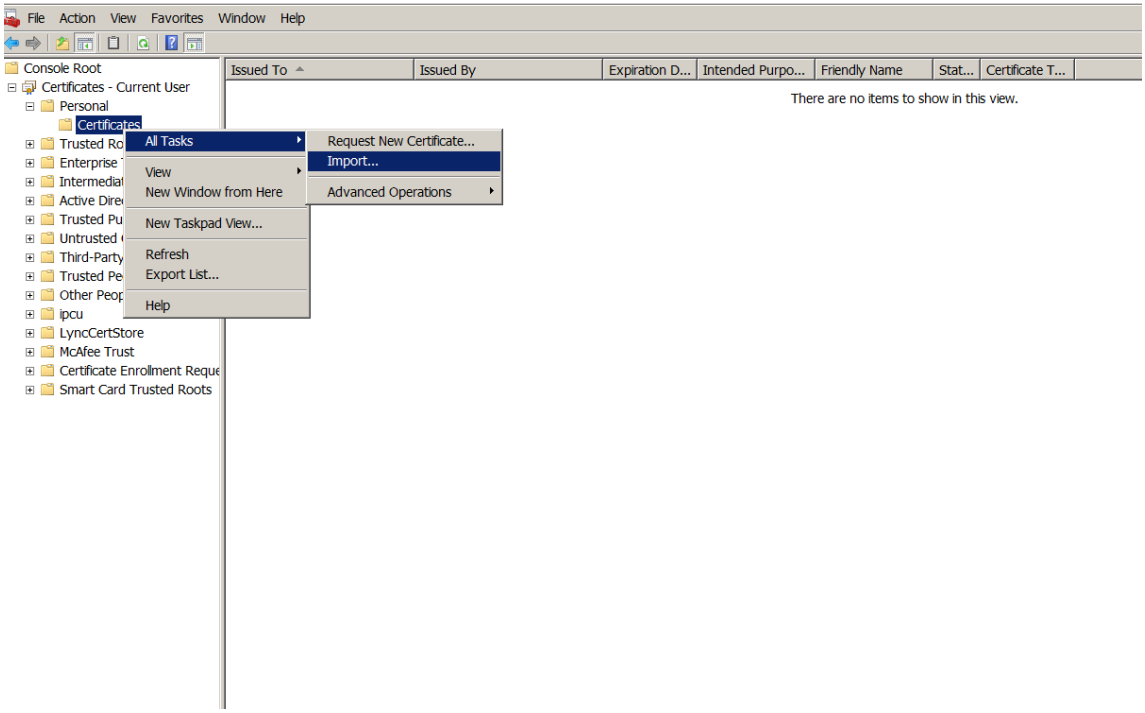
4. Localisez le certificat dans votre répertoire de téléchargement. Le certificat est au format PEM.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Convertir le certificat de PEM vers CER

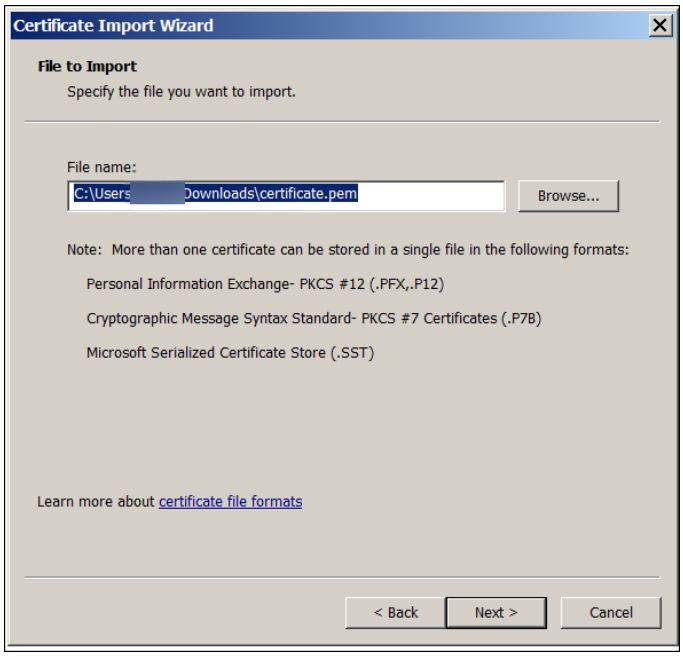
1. Ouvrez la console Microsoft Management Console (MMC) et cliquez avec le bouton droit sur **Certificats > Toutes les tâches > Importer**.



2. Lorsque l'Assistant Importation de certificat apparaît, cliquez sur **Suivant**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

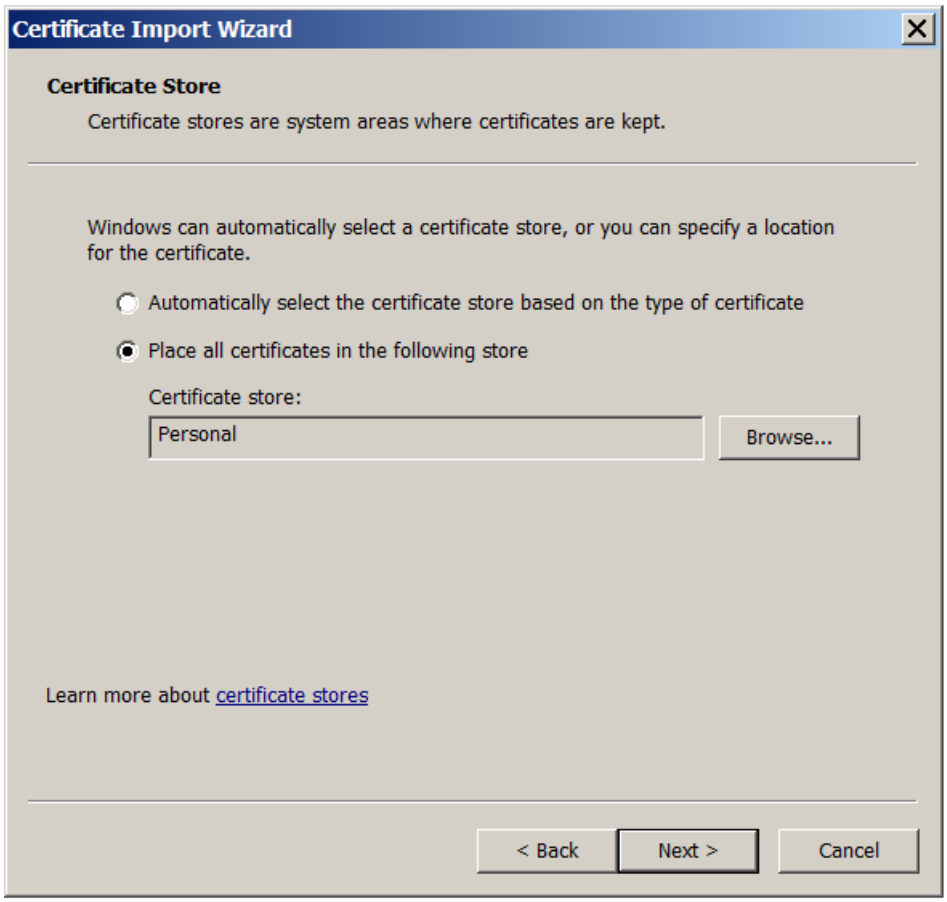
3. Accédez au certificat dans votre répertoire de téléchargement.



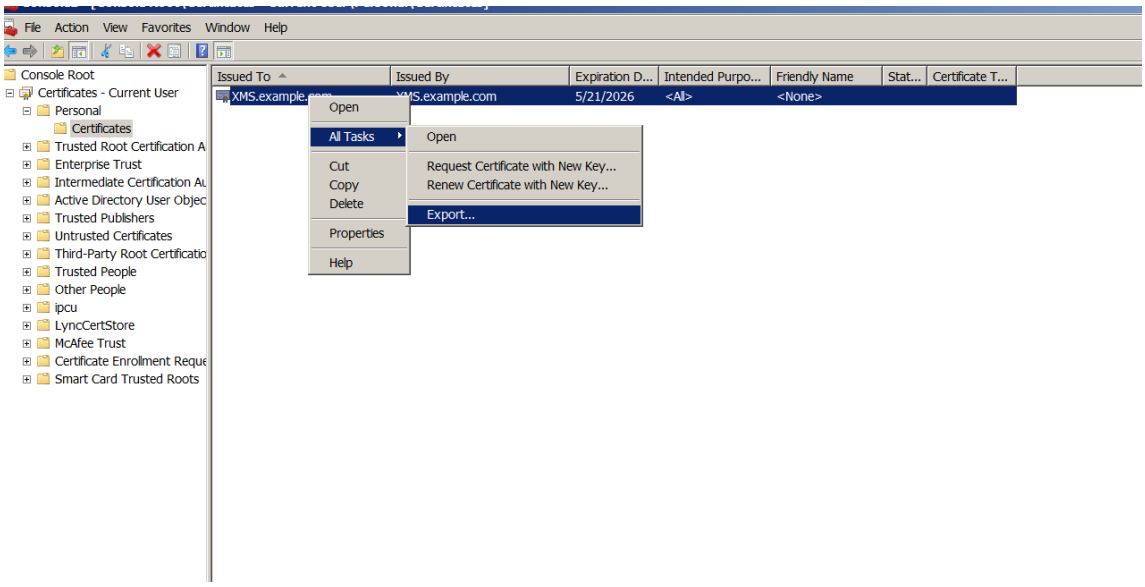
4. Sélectionnez **Placer tous les certificats dans le magasin suivant** et sélectionnez **Personnel**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

comme magasin de certificats. Cliquez sur **Suivant**.



5. Vérifiez vos sélections et cliquez sur **Terminer**. Cliquez sur **OK** dans la fenêtre de confirmation.
6. Dans la console MMC, cliquez avec le bouton droit de la souris sur le certificat et sélectionnez **Toutes les tâches > Exporter**.

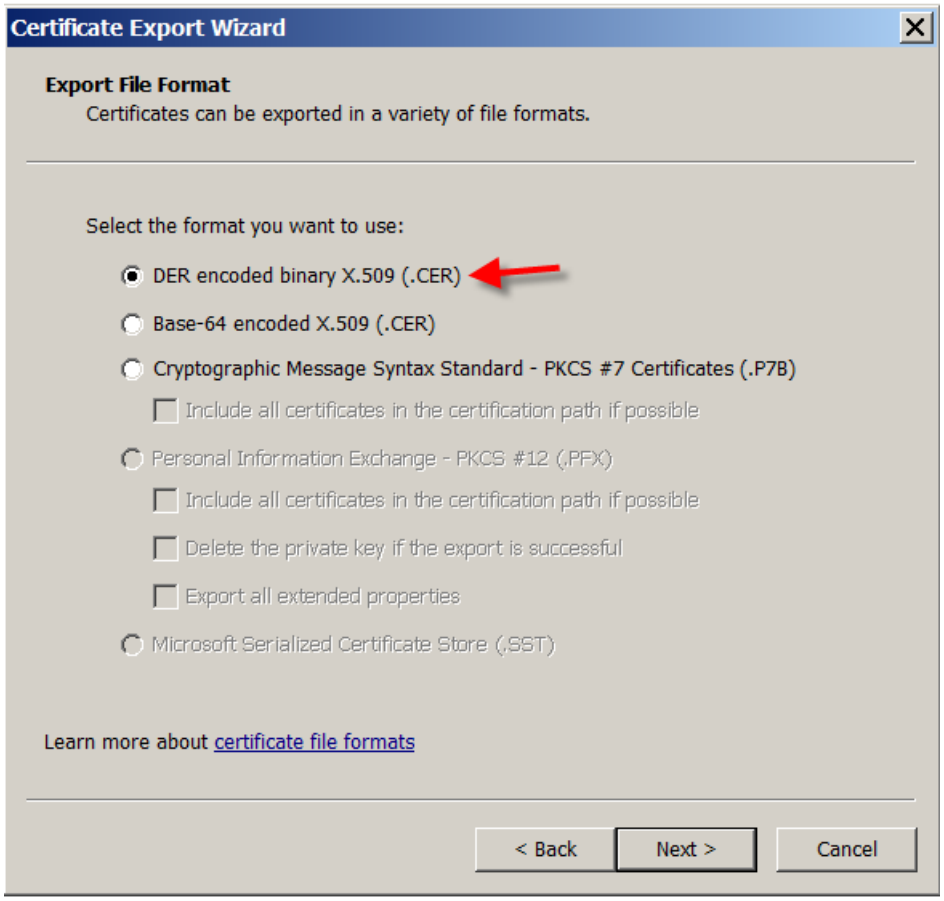


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. Lorsque l'Assistant Exportation de certificat apparaît, cliquez sur **Suivant**.

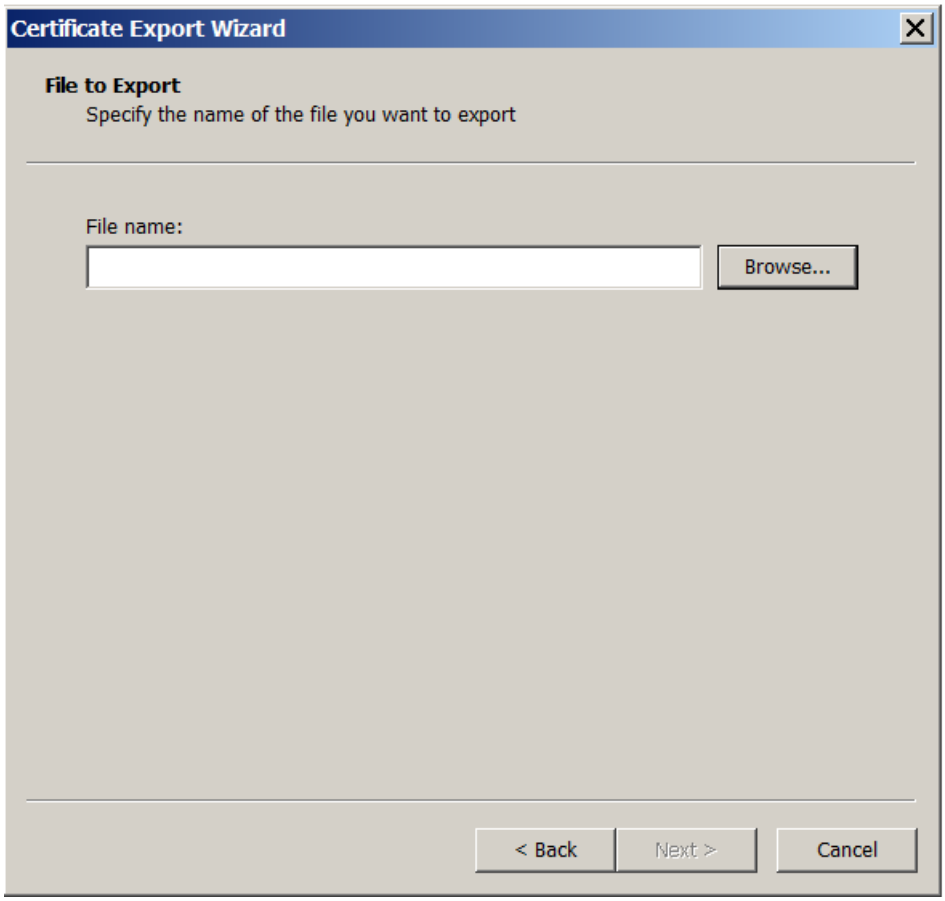
8. Choisissez le format **X.509 binaire encodé DER (*.cer)**. Cliquez sur **Suivant**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

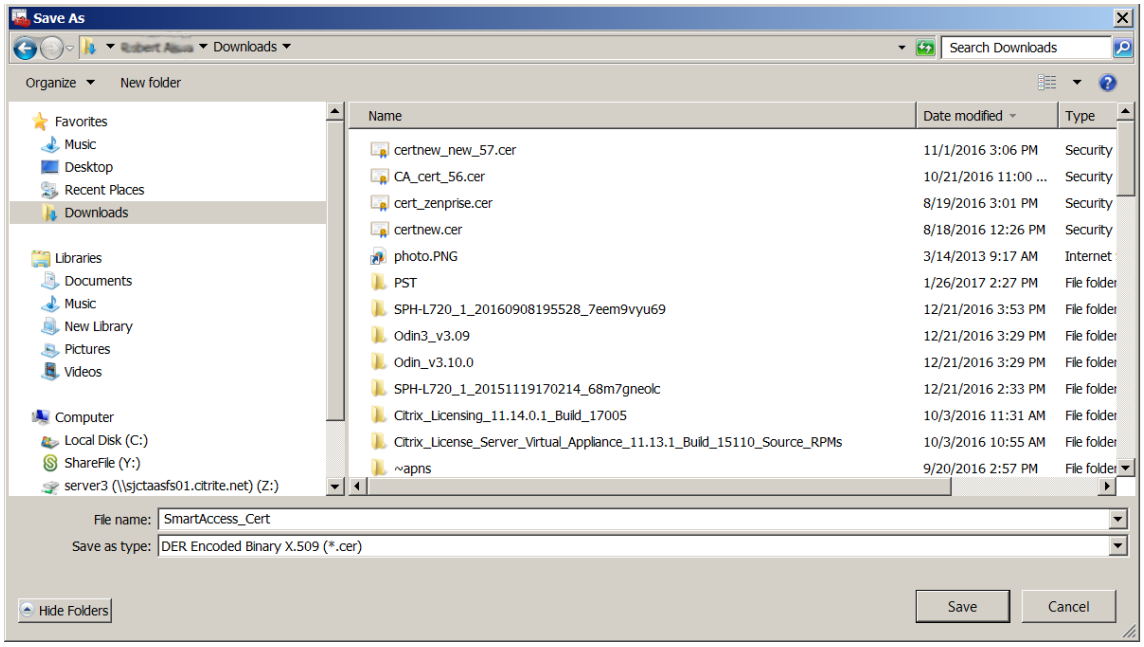


9. Localisez le certificat. Saisissez un nom pour le certificat et cliquez sur **Suivant**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

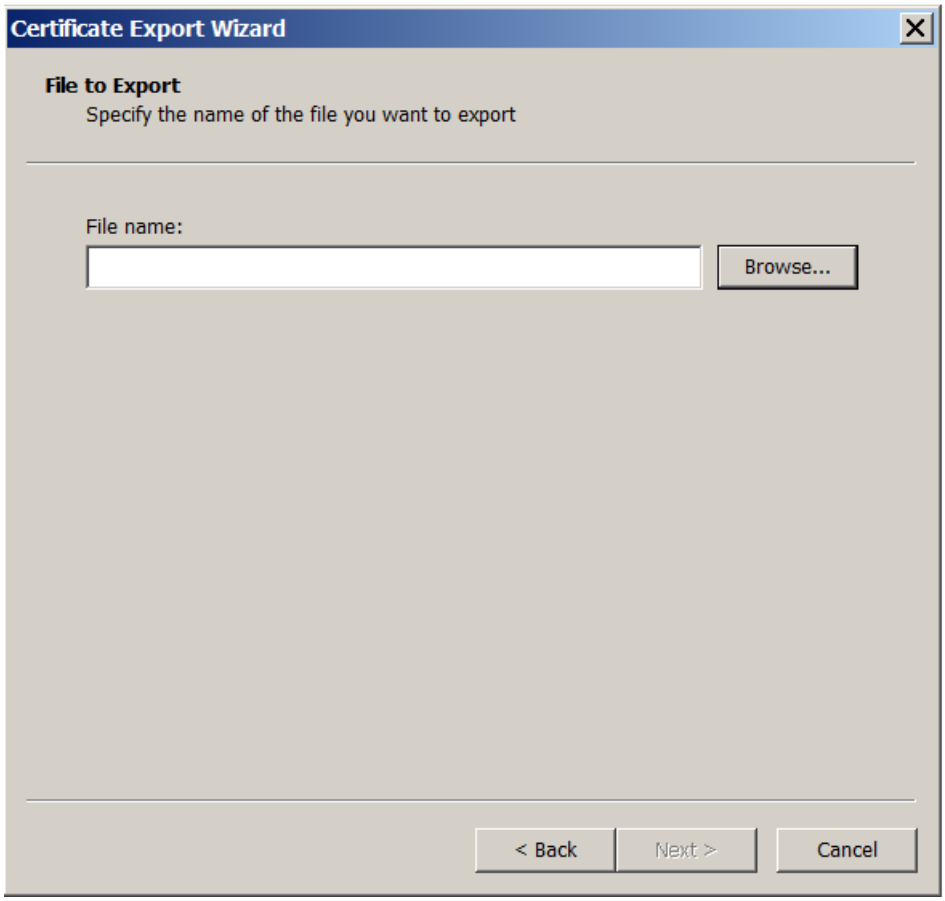


10. Enregistrez le certificat.



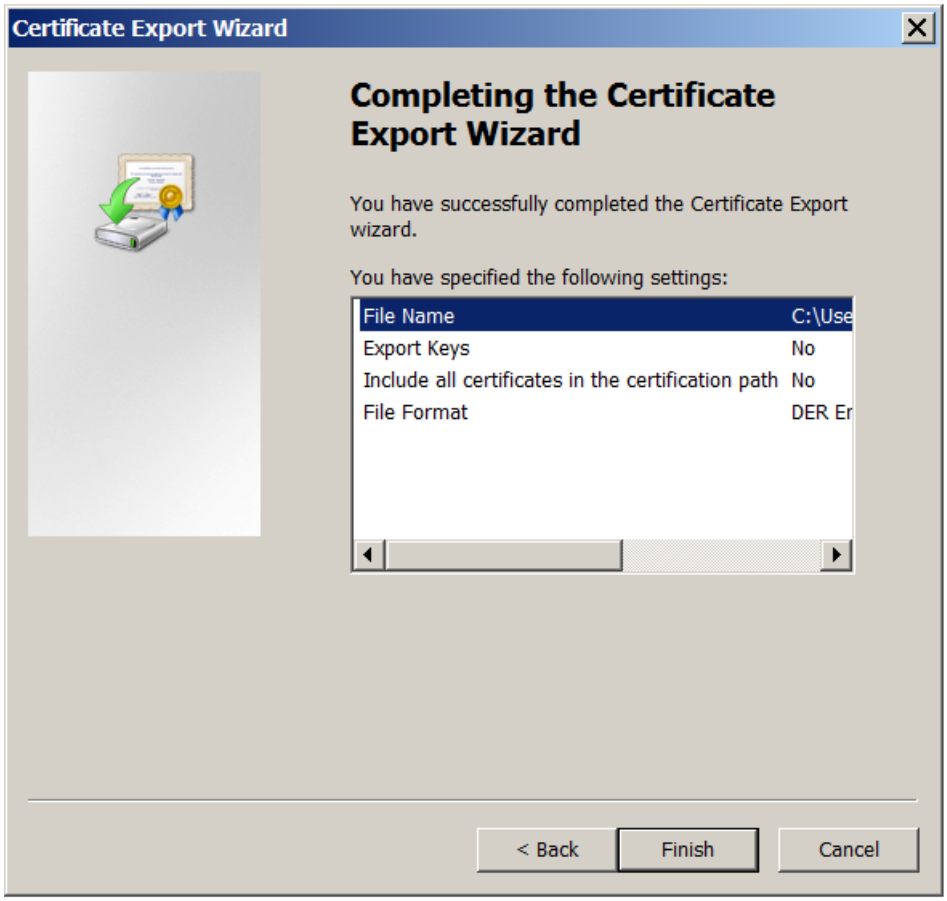
11. Localisez le certificat et cliquez sur **Suivant**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

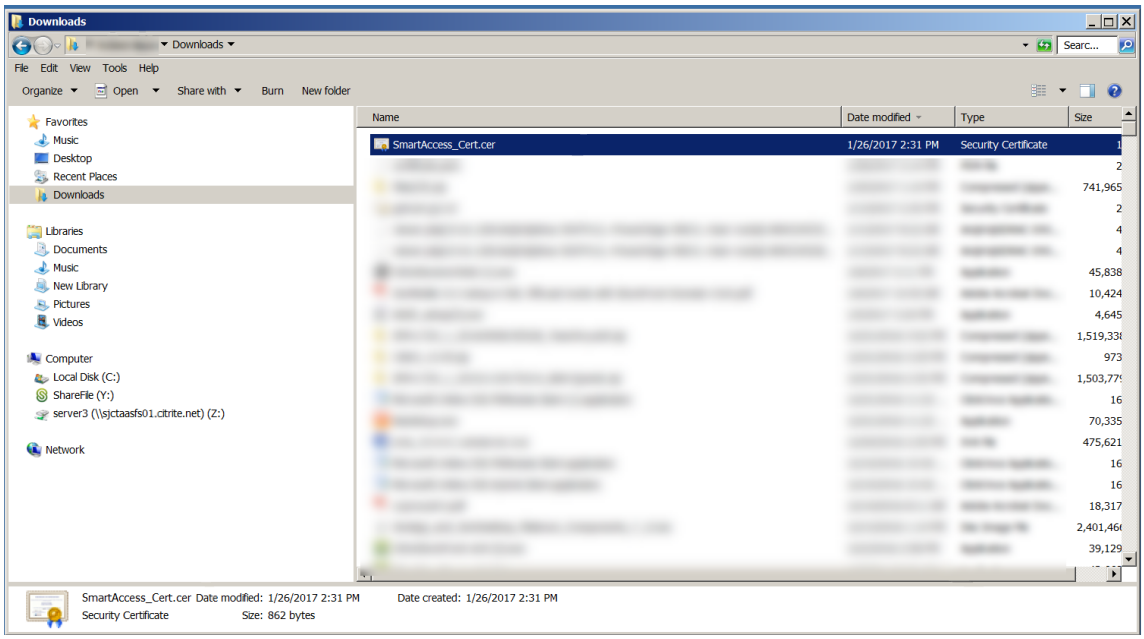


12. Vérifiez vos sélections et cliquez sur **Terminer**. Cliquez sur **OK** dans la fenêtre de confirmation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



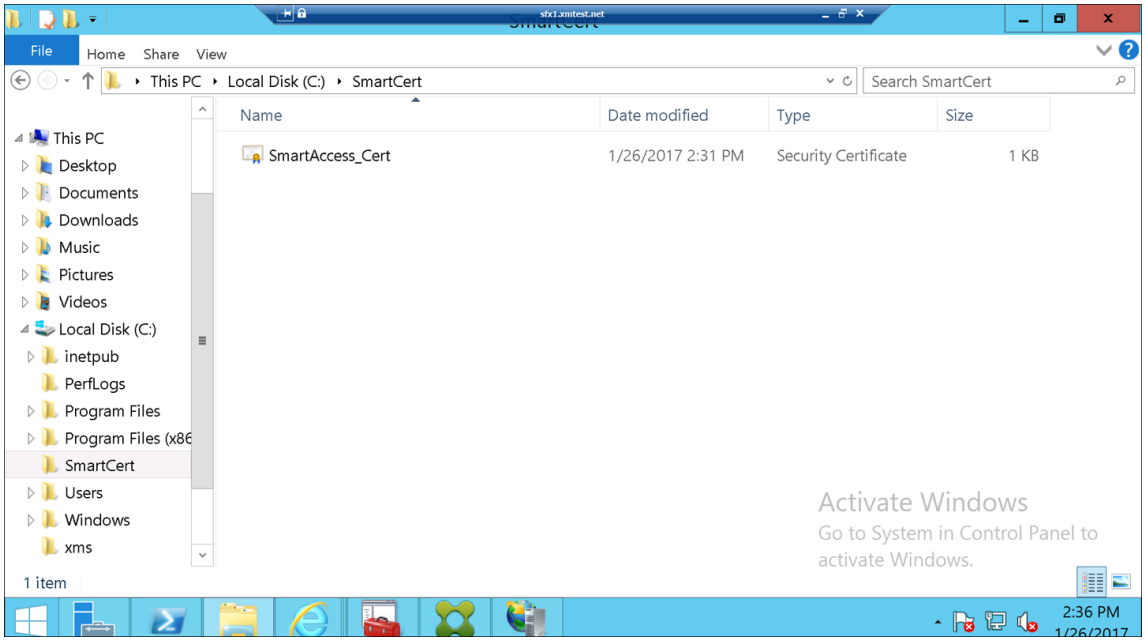
13. Localisez le certificat dans votre répertoire de téléchargement. Le certificat est au format CER.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Copiez le certificat vers le serveur StoreFront

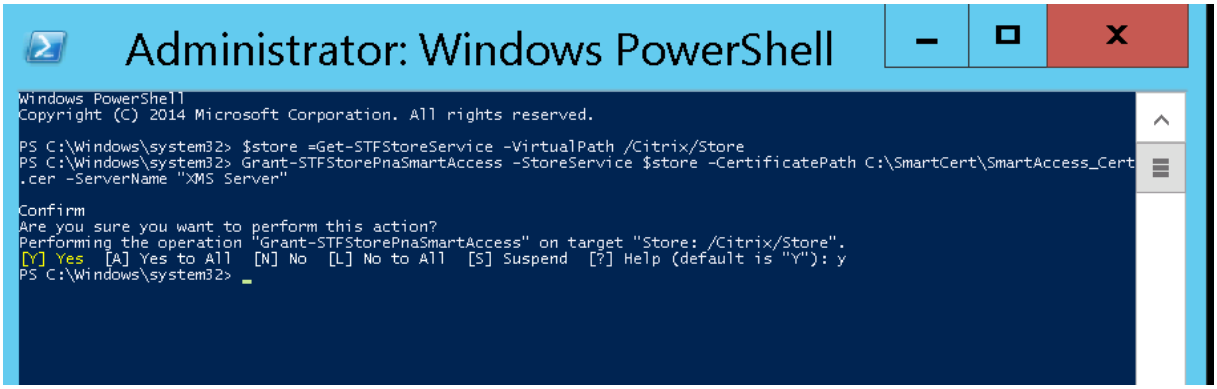
1. Sur le serveur StoreFront, créez un dossier appelé **SmartCert**.
2. Copiez le certificat dans le dossier **SmartCert**.



Configurer le certificat sur le magasin StoreFront

Sur le serveur StoreFront, exécutez cette commande PowerShell pour configurer le certificat de Citrix Endpoint Management Server converti sur le magasin :

```
1     Grant-STFStorePnaSmartAccess –StoreService $store –
        CertificatePath "C:\xms\xms.cer" –ServerName "XMS server"
2  <!--NeedCopy-->
```



S'il existe des certificats dans le magasin StoreFront, exécutez cette commande PowerShell pour les révoquer :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    Revoke-STFStorePnaSmartAccess -StoreService $store -All
<!--NeedCopy-->
```

Vous pouvez également exécuter l'une de ces commandes PowerShell sur le serveur StoreFront pour révoquer des certificats existants sur le magasin StoreFront :

- Révoquer par nom :

```
    $store = Get-STFStoreService -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess -StoreService $store -ServerName "
        My XM Server"
<!--NeedCopy-->
```

- Révoquer par empreinte numérique :

```
    $store = Get-STFStoreService -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess -StoreService $store -
        CertificateThumbprint "[Thumbprint]
<!--NeedCopy-->
```

- Révoquer par objet serveur :

```
    $store = Get-STFStoreService -VirtualPath /Citrix/Store

    $access = Get-STFStorePnaSmartAccess -StoreService $store

    Revoke-STFStorePnaSmartAccess -StoreService $store -SmartAccess
        $access.AccessConditionsTrusts[0]
<!--NeedCopy-->
```

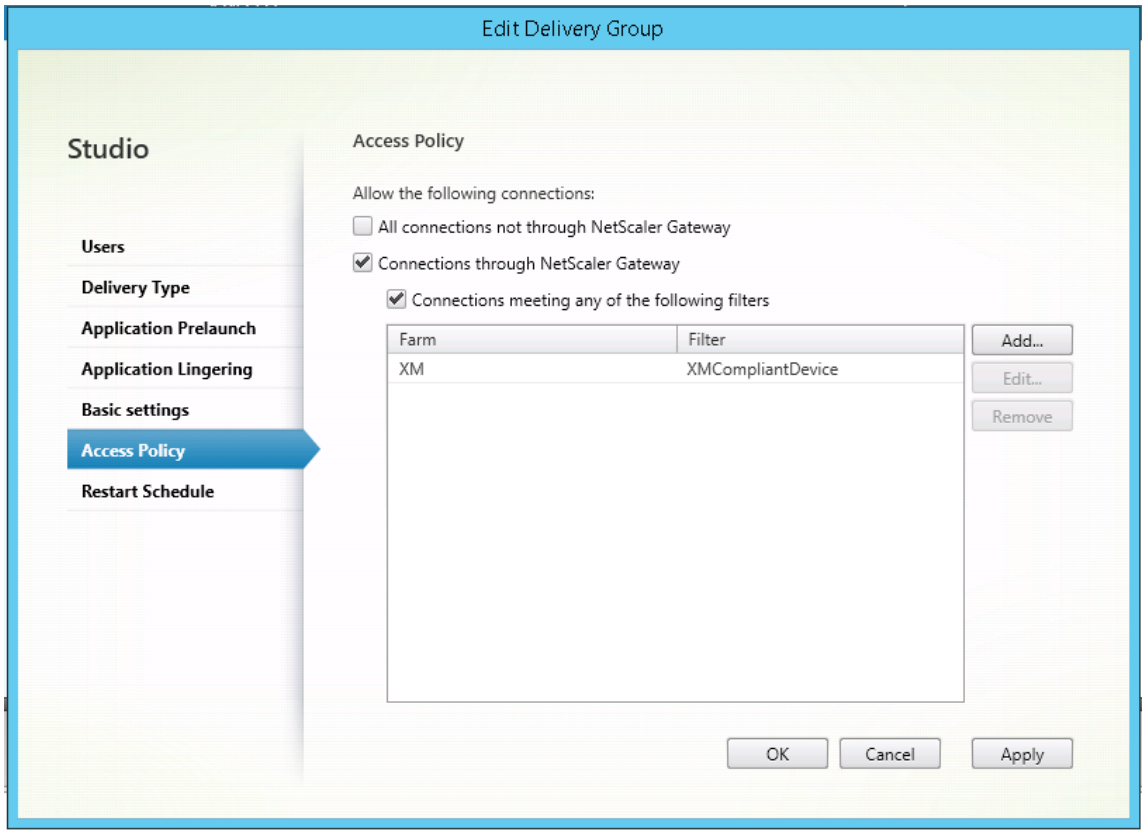
Configurer la stratégie SmartAccess pour Citrix Virtual Apps and Desktops

Pour ajouter la stratégie SmartAccess requise au groupe de mise à disposition de l'application HDX :

1. Ouvrez Citrix Studio à partir de la console Citrix Cloud.
2. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
3. Sélectionnez un groupe mettant à disposition les applications dont vous souhaitez contrôler l'accès. Sélectionnez **Modifier le groupe de mise à disposition** dans le volet **Actions**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Dans la page **Stratégie d'accès**, sélectionnez **Connexions transitant par NetScaler Gateway** et **Connexions remplissant l'un des critères de filtre suivants**.
5. Cliquez sur **Ajouter**.
6. Ajoutez une stratégie d'accès dans laquelle **Batterie** est **XM** et **Filtre** est **XMCompliantDevice**.

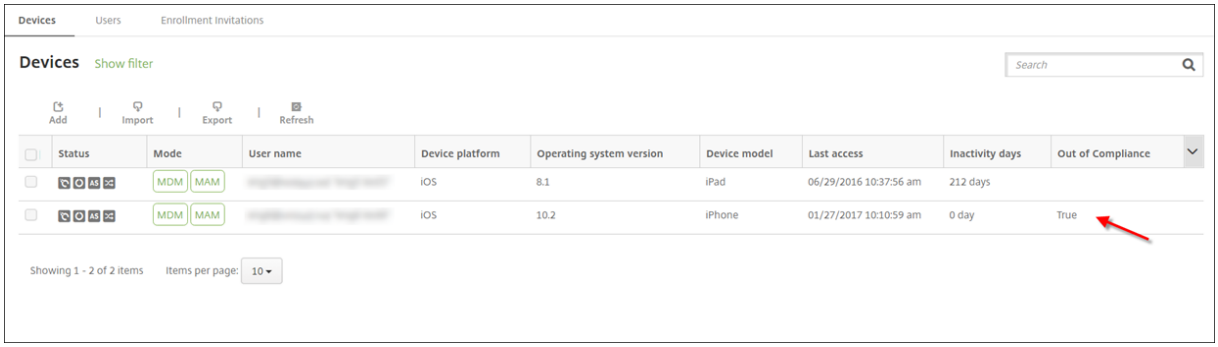


7. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

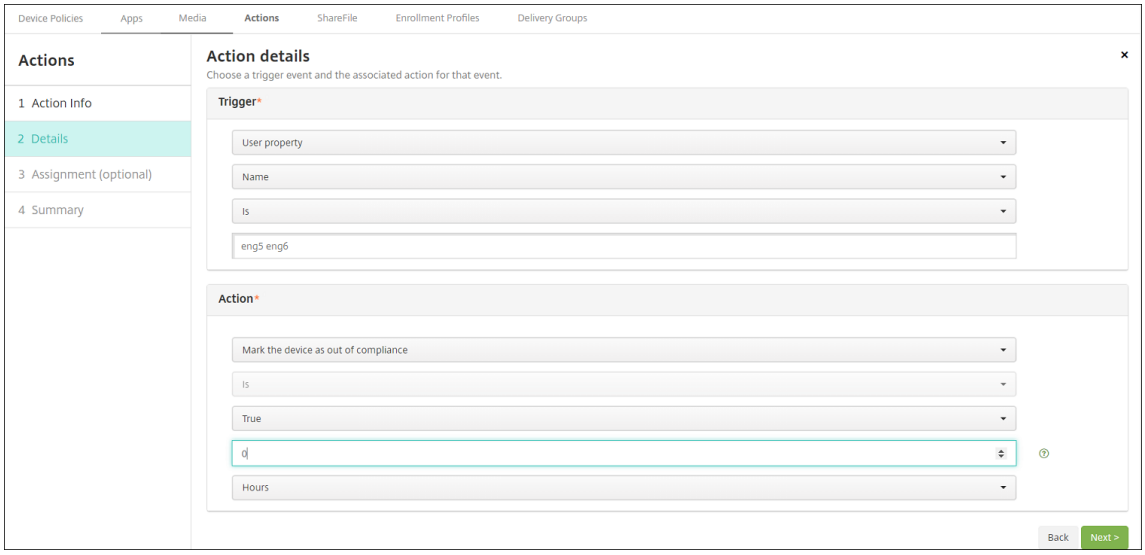
Définir les actions automatisées dans Citrix Endpoint Management

La stratégie SmartAccess que vous avez définie dans le groupe de mise à disposition pour une application HDX refuse l'accès à un appareil lorsque l'appareil n'est pas conforme. Utilisez des actions automatisées pour marquer l'appareil comme non conforme.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Actions**. La page **Actions** s'affiche.
2. Cliquez sur **Ajouter** pour ajouter une action. La page **Informations sur l'action** s'affiche.
3. Sur la page **Informations sur l'action**, entrez un nom et une description pour l'action.
4. Cliquez sur **Suivant**. La page sur les **Détails de l'action** s'affiche. Dans l'exemple suivant, un déclencheur est créé qui marque immédiatement les appareils comme non conformes s'ils ont le nom de propriété utilisateur **eng5** ou **eng6**.



5. Dans la liste **Déclencheur**, sélectionnez **Propriété de l'appareil**, **Propriété utilisateur** ou **Nom de l'application installée**. SmartAccess ne prend pas en charge les déclencheurs d'événements.
6. Dans la liste **Action** :
   - Choisissez **Marquer l'appareil comme non conforme**.
   - Choisissez **Est**.
   - Choisissez **Vrai**.
   - Pour que l'action marque l'appareil comme non conforme dès que la condition de déclencheur est remplie, définissez le délai sur **0**.

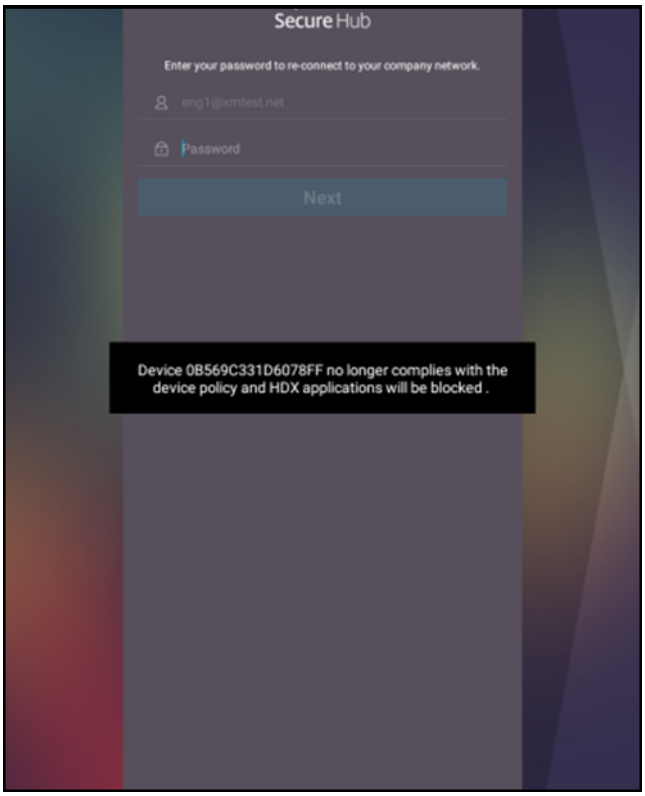
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. Choisissez les groupes de mise à disposition Citrix Endpoint Management auxquels appliquer cette action.
8. Vérifiez le récapitulatif de l'action.
9. Cliquez sur **Suivant**, puis cliquez sur **Enregistrer**.

Lorsque l'appareil est marqué comme non conforme, les applications HDX ne s'affichent plus dans le magasin Citrix Secure Hub. L'utilisateur n'est plus abonné aux applications. Aucune notification n'est envoyée à l'appareil et rien dans le magasin Citrix Secure Hub n'indique que les applications HDX ont été disponibles.

Si vous souhaitez que les utilisateurs soient avertis lorsqu'un appareil est marqué comme non conforme, créez une notification, puis créez une action automatique pour envoyer cette notification.

Cet exemple crée et envoie cette notification lorsqu'un appareil est marqué comme non conforme : « L'appareil (numéro de série ou numéro de téléphone) n'est plus conforme avec la stratégie et les applications HDX sont bloquées. »

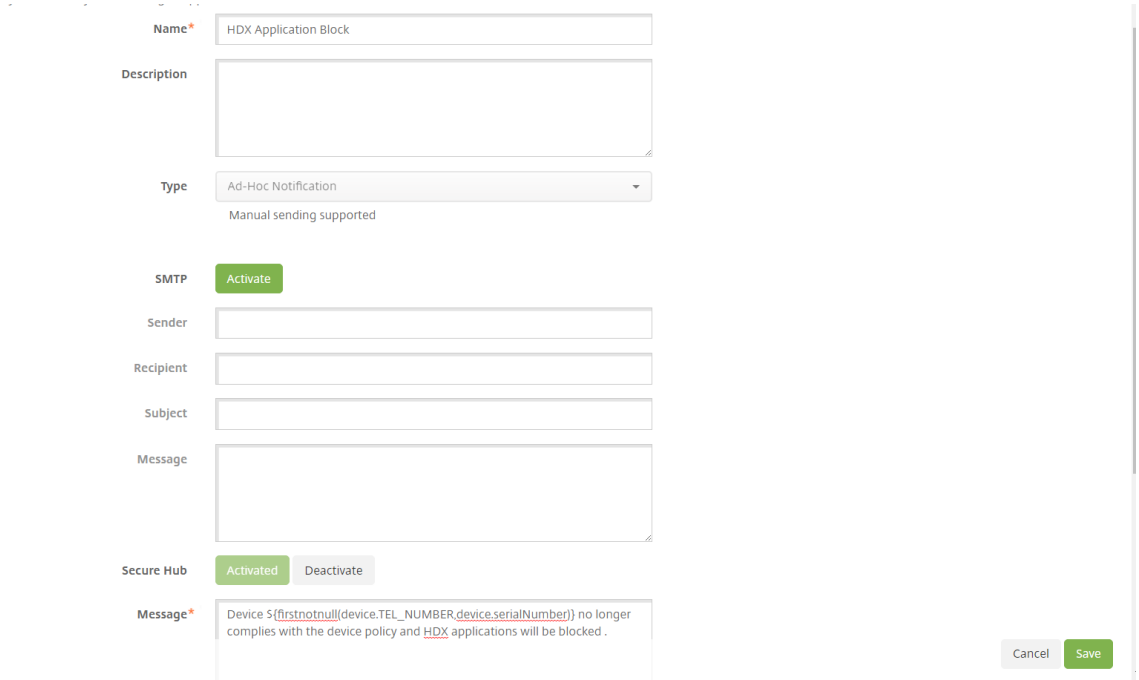


Créer la notification que les utilisateurs voient lorsqu'un appareil est marqué comme non conforme

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Cliquez sur **Modèles de notification**. La page **Modèles de notification** s'affiche.
3. Cliquez sur **Ajouter** pour ajouter un nouveau modèle de notification sur la page **Modèles de notification**.
4. Pour configurer ces paramètres :
   - **Nom :** Blocage application HDX
   - **Description :** notification de l'agent lorsqu'un appareil n'est pas conforme
   - **Type :** notification ad hoc
   - **Citrix Secure Hub :** Activé
   - **Message :** L'appareil `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` n'est plus conforme avec la stratégie et les applications HDX vont être bloquées.



5. Cliquez sur **Enregistrer**.

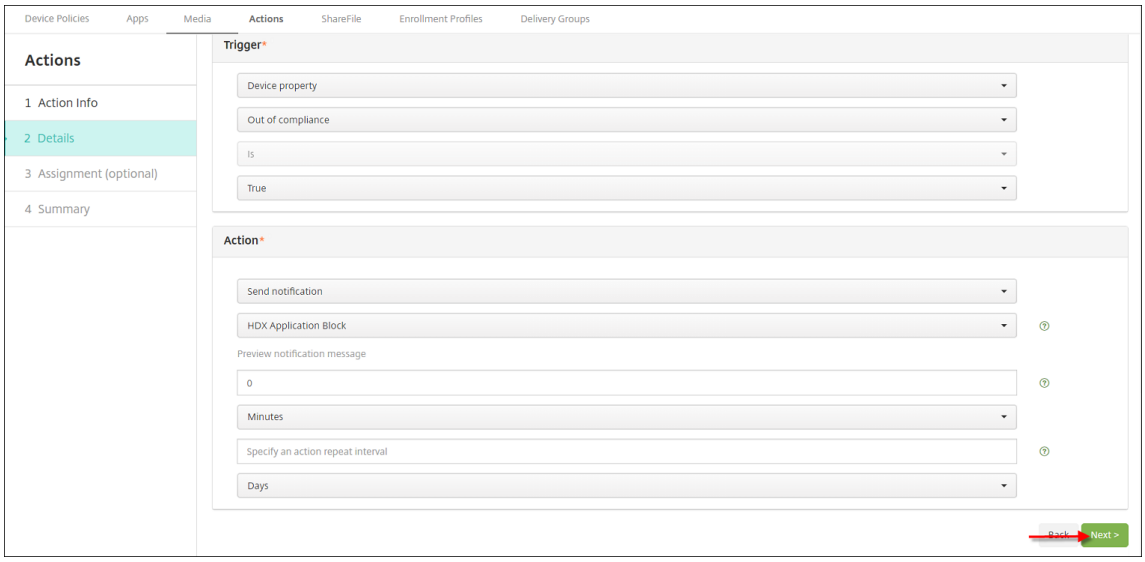
Créer l'action qui envoie la notification lorsqu'un appareil est marqué comme non conforme

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Actions**. La page **Actions** s'affiche.
2. Cliquez sur **Ajouter** pour ajouter une action. La page **Informations sur l'action** s'affiche.
3. Sur la page **Informations sur l'action**, entrez un nom et une description pour l'action.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Nom : notification HDX bloquée
- **Description :** notification HDX bloquée car l'appareil n'est pas conforme

4. Cliquez sur **Suivant**. La page sur les **Détails de l'action** s'affiche.
5. Dans la liste **Déclencheur** :
   - Choisissez **Propriété de l'appareil**.
   - Choisissez **Non conforme**.
   - Choisissez **Est**.
   - Choisissez **Vrai**.



6. Dans la liste **Action**, spécifiez les actions qui se produisent lorsque le critère du déclencheur est rencontré :
   - Choisissez **Envoyer une notification**.
   - Choisissez **L'application HDX a bloqué la notification que vous avez créée**.
   - Choisissez **0**. Lorsque cette valeur est définie sur 0, la notification est envoyée dès que la condition du déclencheur est rencontrée.
7. Choisissez les groupes de mise à disposition Citrix Endpoint Management auxquels appliquer cette action. Dans cet exemple, choisissez **AllUsers**.
8. Vérifiez le récapitulatif de l'action.
9. Cliquez sur **Suivant**, puis cliquez sur **Enregistrer**.

Pour de plus amples informations sur la configuration d'actions automatiques, consultez la section Actions automatisées.

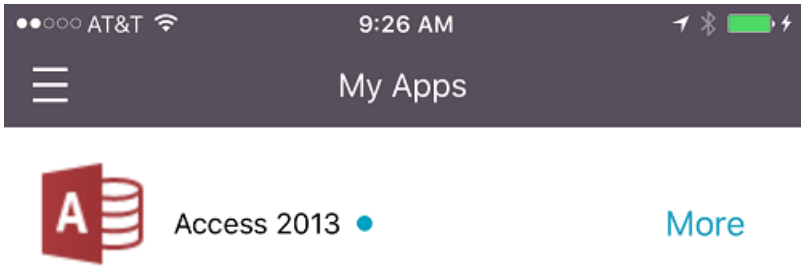
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Comment les utilisateurs peuvent rétablir l'accès aux applications HDX

Les utilisateurs peuvent de nouveau accéder aux applications HDX une fois que la conformité de l'appareil est rétablie :

1. Sur l'appareil, accédez au magasin Citrix Secure Hub pour actualiser les applications dans le magasin.
2. Accédez à l'application et touchez **Ajouter** à l'application.

Une fois que l'application est ajoutée, elle s'affiche dans Mes applications avec un point bleu, car il s'agit d'une application nouvellement installée.



Mettre à niveau les applications MDX ou Enterprise

March 1, 2024

Pour mettre à niveau une application MDX ou Enterprise dans Citrix Endpoint Management, désactivez-la dans la console Citrix Endpoint Management, puis téléchargez la nouvelle version de l'application.

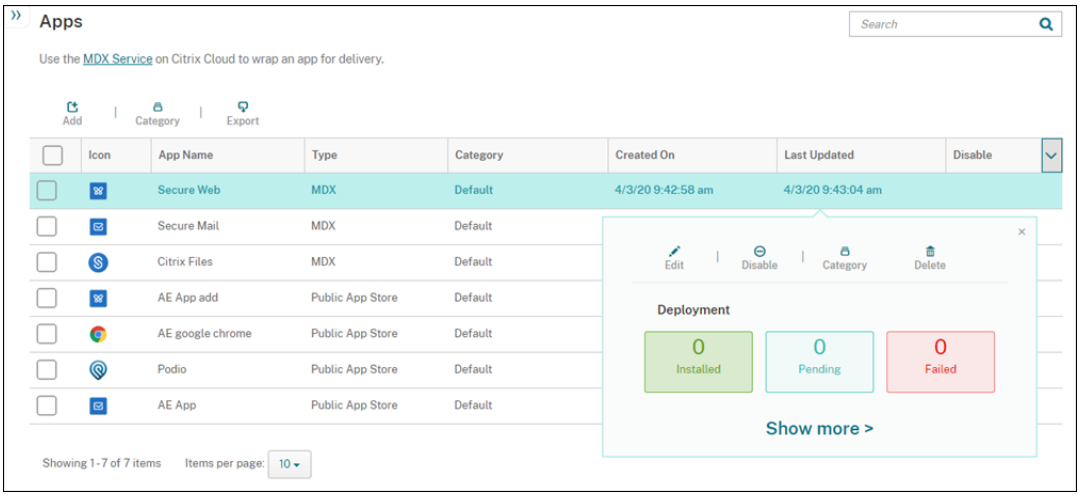
1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Applications**. La page **Applications** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Pour les appareils gérés (appareils inscrits dans Citrix Endpoint Management pour la gestion d'appareils mobiles), passez à l'étape 3. Pour les appareils non gérés (appareils inscrits dans Citrix Endpoint Management uniquement à des fins de gestion d'applications d'entreprise), procédez comme suit :

   a) Dans le tableau **Applications**, sélectionnez la case à cocher en regard de l'application, ou cliquez sur la ligne contenant l'application que vous souhaitez mettre à jour.

   b) Cliquez sur **Désactiver** dans le menu qui s'affiche.



   c) Cliquez sur **Désactiver** dans la boîte de dialogue de confirmation. *Désactivé* s'affiche dans la colonne **Désactiver** pour l'application.

> **Remarque :**
>
> Lorsque l'application est désactivée, les utilisateurs ne peuvent pas se reconnecter à l'application après avoir fermé leur session. La désactivation d'applications est un paramètre facultatif, mais nous recommandons de désactiver l'application pour éviter les problèmes avec la fonctionnalité de l'application. Par exemple, une erreur peut se produire lorsque les utilisateurs demandant de télécharger l'application en même temps que vous téléchargez la nouvelle version.

3. Dans le tableau **Applications**, cliquez sur la case à cocher en regard de l'application, ou cliquez sur la ligne contenant l'application que vous souhaitez mettre à jour.

4. Cliquez sur **Modifier** dans le menu qui s'affiche. La page **Informations sur l'application** s'affiche avec la liste des plates-formes que vous avez choisies pour l'application sélectionnée.

5. Pour configurer ces paramètres :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Nom :** si vous le souhaitez, vous pouvez modifier le nom de l'application.
- **Description :** si vous le souhaitez, vous pouvez modifier la description de l'application.
- **Catégorie d'application :** si vous le souhaitez, vous pouvez modifier la catégorie.

6. Cliquez sur **Suivant**. La première page de plate-forme sélectionnée s'affiche. Effectuez les opérations suivantes pour chaque plate-forme sélectionnée :

   a) Choisissez le fichier de remplacement que vous voulez charger en cliquant sur le bouton **Charger** et accédez à l'emplacement du fichier. L'application se charge dans Citrix Endpoint Management.

      Si vous chargez une application pour Android Enterprise, une fenêtre Google Play d'entreprise s'affiche. Chargez la nouvelle version de l'application ici. Pour plus de détails, consultez Distribuer des applications Android Enterprise.

   b) Si vous le souhaitez, vous pouvez modifier les détails de l'application et les paramètres de stratégie pour la plate-forme.

   c) Si vous le souhaitez, vous pouvez configurer des règles de déploiement et le magasin d'applications. Pour plus d'informations, consultez la section Ajouter une application MDX.

7. Cliquez sur **Enregistrer**. La page **Applications** s'affiche.

8. Si vous avez désactivé l'application à l'étape 2, effectuez les opérations suivantes :

   a) Dans le tableau des **Applications**, choisissez l'application que vous avez mis à jour puis dans le menu qui s'affiche, cliquez sur **Activer**.
   b) Dans la boîte de dialogue de confirmation qui s'affiche, cliquez sur **Activer**. Les utilisateurs peuvent désormais accéder à l'application et recevoir une notification les invitant à mettre l'application à niveau.

Ajouter un média

March 1, 2024

Vous pouvez ajouter un média à Citrix Endpoint Management afin de le déployer vers les appareils utilisateur. Vous pouvez utiliser Citrix Endpoint Management pour déployer Apple Books que vous obtenez via l'achat en volume d'Apple.

Une fois que vous avez configuré un compte d'achat en volume dans Citrix Endpoint Management, vos livres achetés et gratuits s'affichent dans **Configurer** > **Média**. À partir des pages **Média**, vous pouvez configurer les livres pour le déploiement vers les appareils iOS en choisissant des groupes de mise à disposition et en spécifiant les règles de déploiement.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

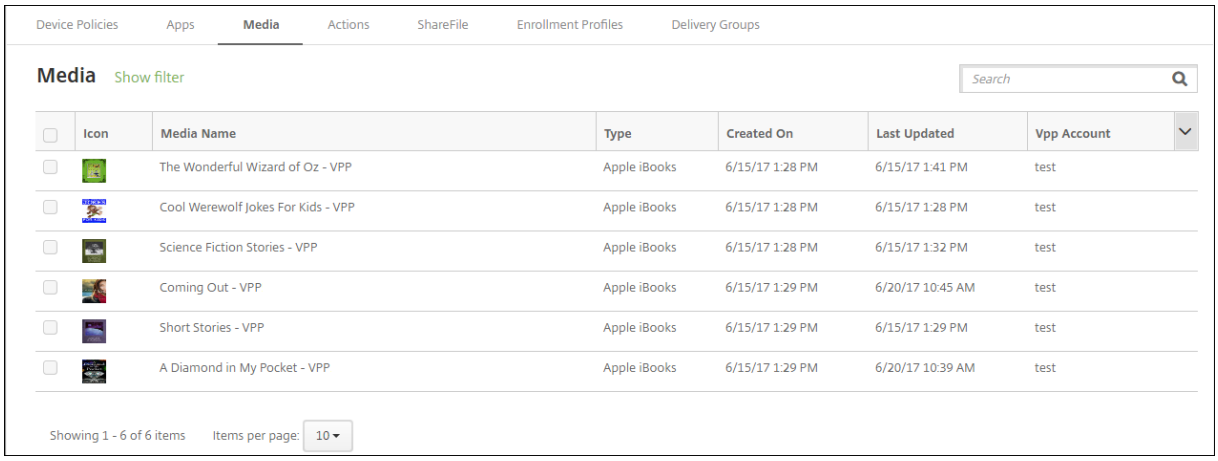
La première fois qu'un utilisateur reçoit un livre et accepte la licence d'achat en volume, les livres déployés s'installent sur l'appareil. Les livres s'affichent dans l'application Apple Books. Vous ne pouvez pas dissocier la licence du livre de l'utilisateur ou supprimer le livre de l'appareil. Citrix Endpoint Management installe les livres en tant que média obligatoire. Si un utilisateur supprime un livre installé de son appareil, le livre reste dans l'application Apple Book, prêt à être téléchargé.

Logiciels requis

- Appareils iOS
- Configurez l'achat en volume Apple dans Citrix Endpoint Management, comme décrit dans Achats en volume d'Apple.

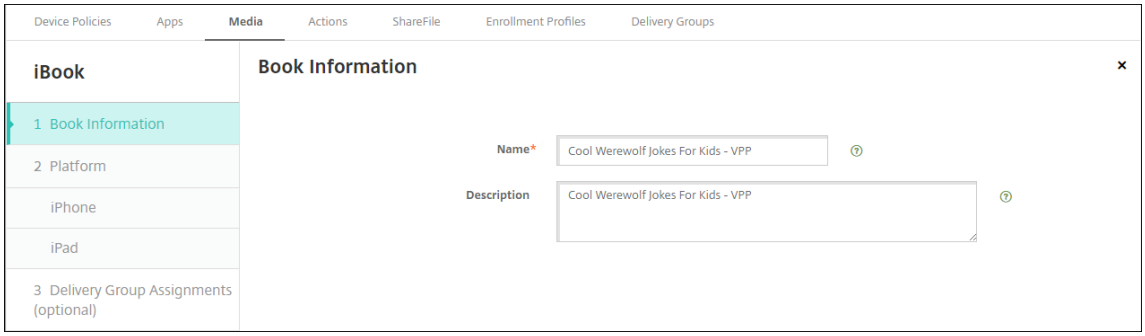
Configurer Apple Books

Les livres Apple Books obtenus via l'achat en volume s'affichent sur la page **Configurer** > **Média**.



Pour configurer un livre Apple Book en vue du déploiement

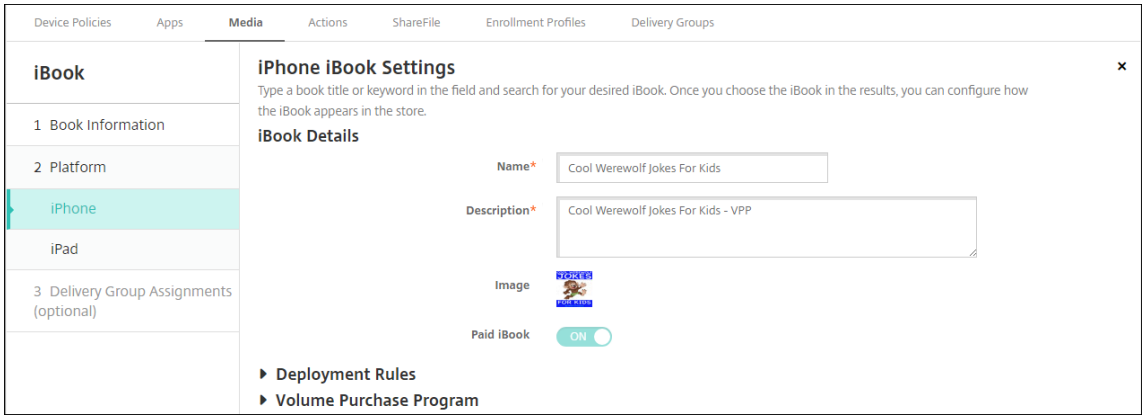
1. Dans **Configurer > Média**, sélectionnez un livre et cliquez sur **Modifier**. La page **Informations sur le livre** s'affiche.



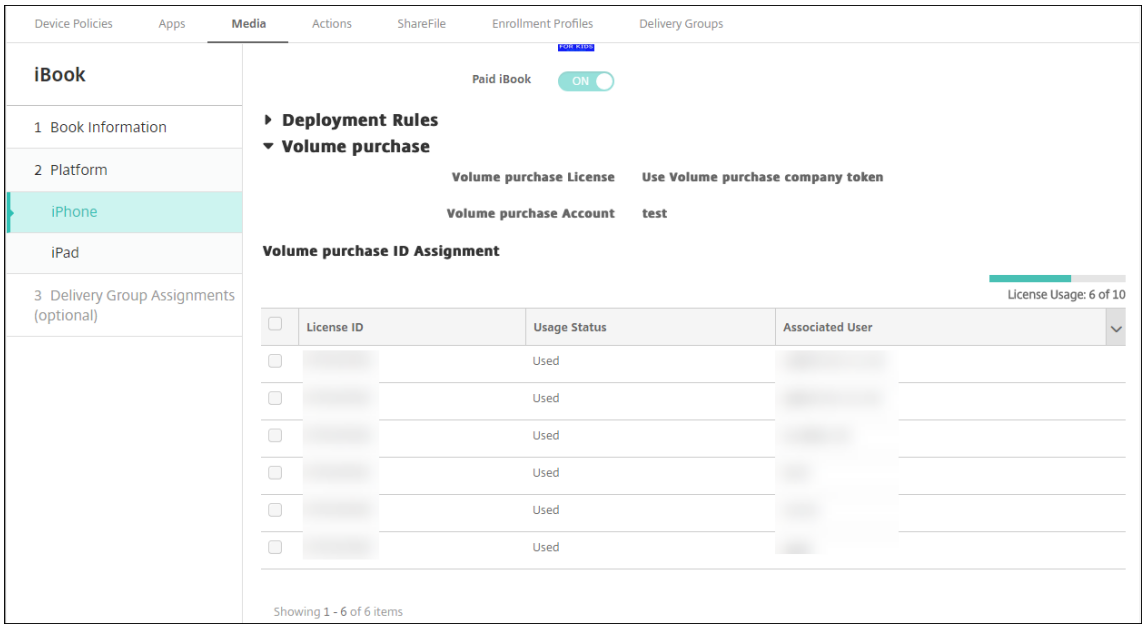
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Les champs **Nom** et **Description** n'apparaissent que dans les journaux et la console Citrix Endpoint Management.

2. Dans les pages **Paramètres iBook iPhone** et **Paramètres iBook iPad** : vous pouvez modifier le nom et la description du livre, mais Citrix vous recommande de ne pas modifier ces paramètres. L'image est fournie à titre indicatif et n'est pas modifiable. **iBook payant** indique qu'un livre a été acheté via l'achat en volume.

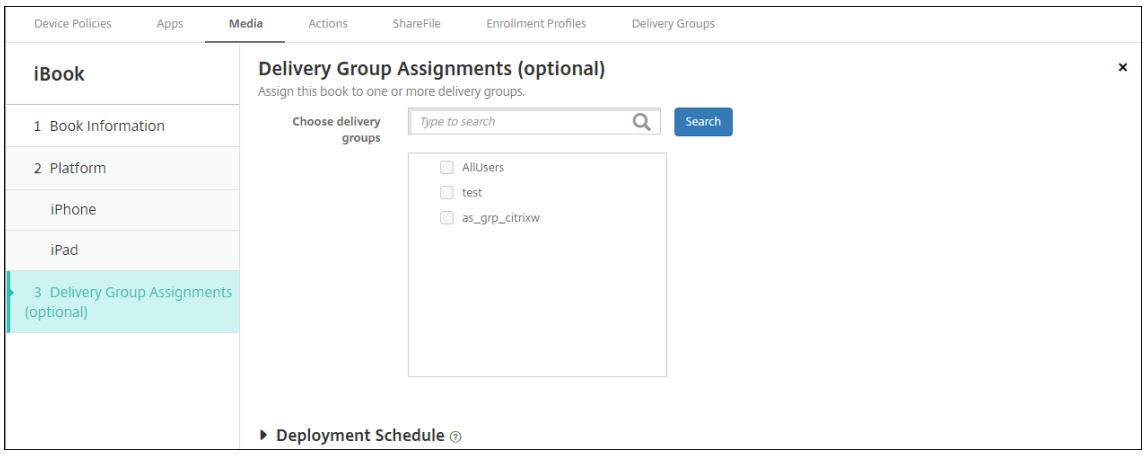


Vous pouvez également spécifier des règles de déploiement ou afficher des informations relatives à l'achat en volume.

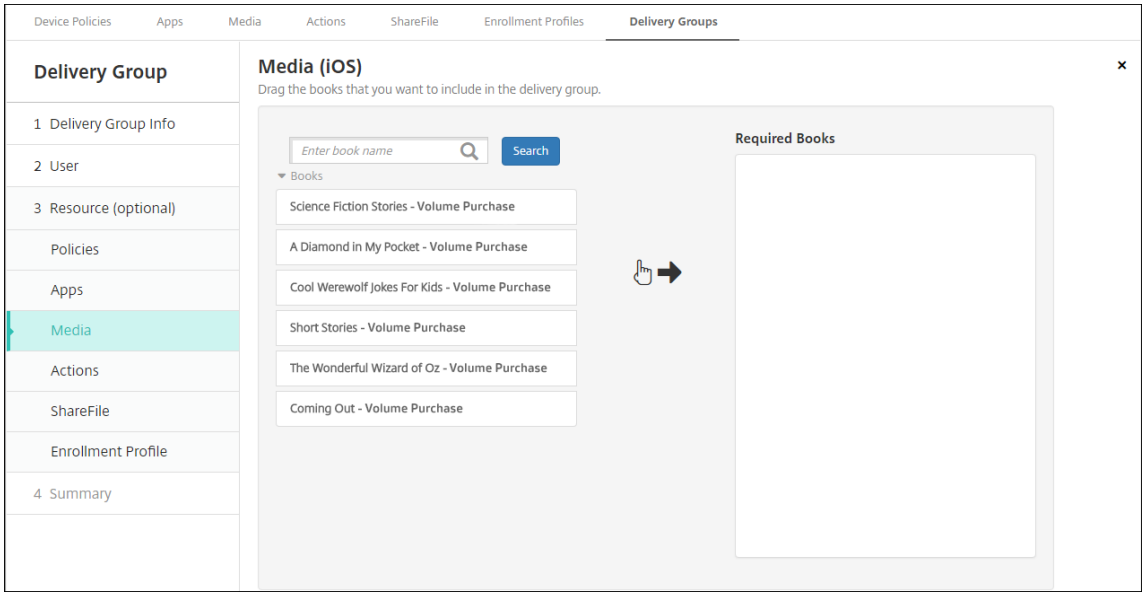


3. Si vous le souhaitez, attribuez le livre à des groupes de mise à disposition et définissez un calendrier de déploiement.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

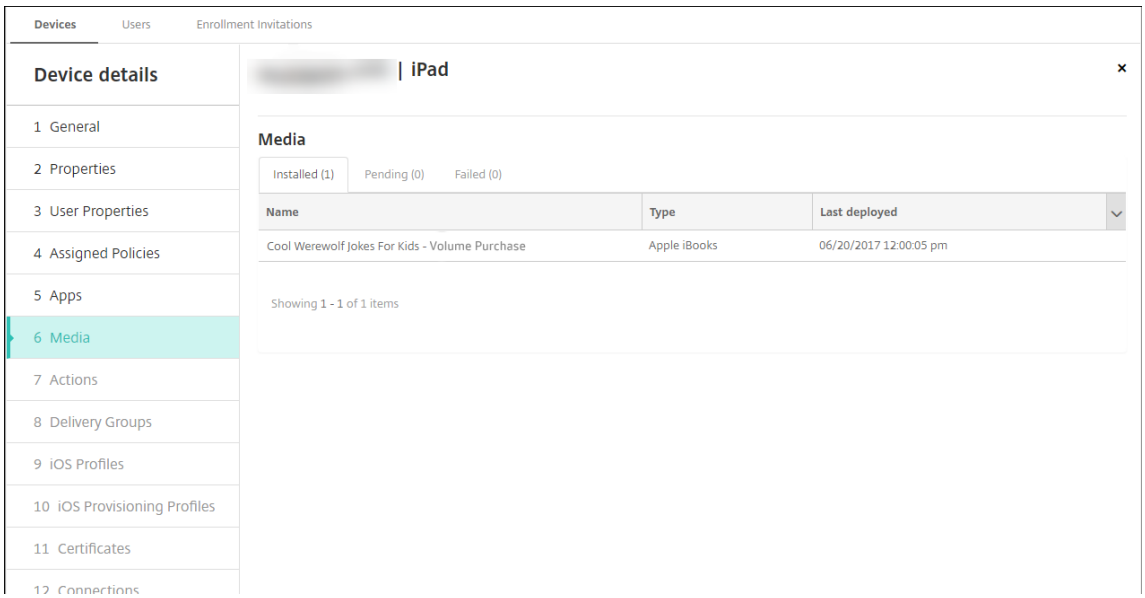


Vous pouvez également attribuer des livres à des groupes de mise à disposition à partir de l'onglet **Média** sous **Configurer > Groupes de mise à disposition**. Citrix Endpoint Management prend en charge le déploiement de livres requis uniquement.



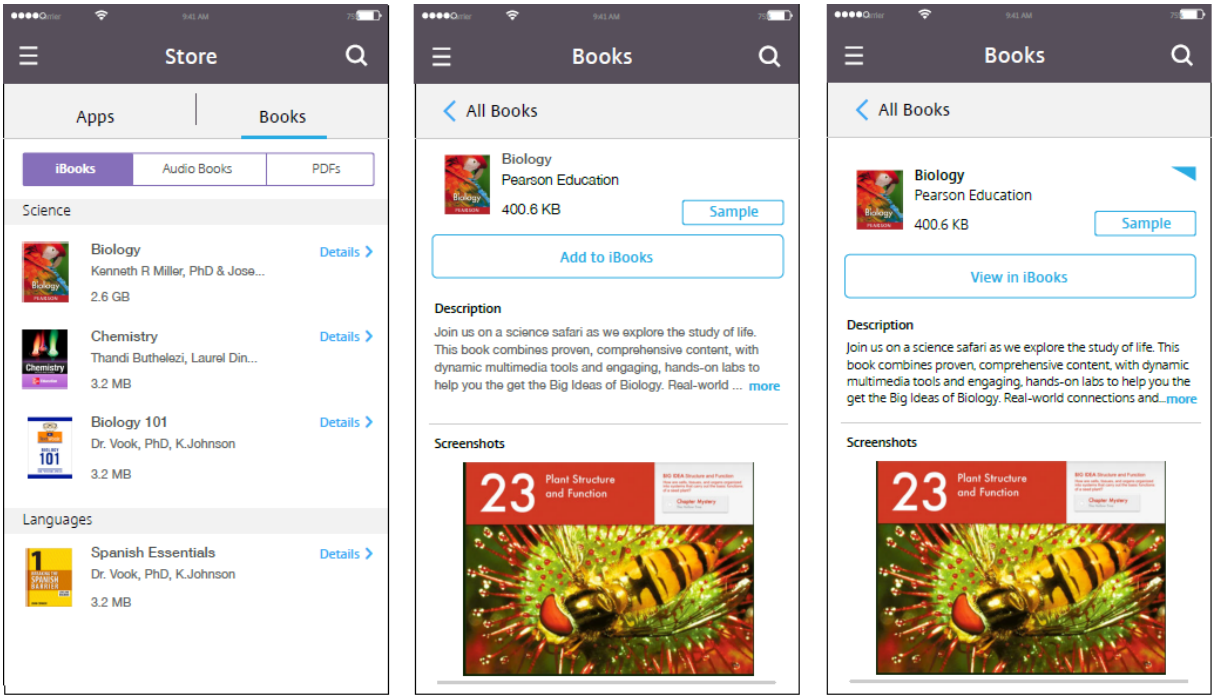
4. Utilisez l'onglet **Média** sous **Gérer > Appareils** pour afficher l'état du déploiement.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Remarque :**
>
> Sur la page **Configurer** > **Média**, si vous sélectionnez un livre et cliquez sur **Supprimer**, Citrix Endpoint Management supprime le livre de la liste. Toutefois, la prochaine fois que Citrix Endpoint Management se synchronise avec l'achat en volume Apple, le livre s'affiche de nouveau sur la liste sauf s'il a été supprimé de l'achat en volume. La suppression d'un livre de la liste ne le supprime pas de l'appareil.

Les livres s'affichent sur les appareils utilisateur comme illustré dans l'exemple suivant.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Déployer des ressources

March 1, 2024

La gestion et la configuration d'appareils impliquent généralement la création de ressources (stratégies, applications et média) et d'actions dans la console Citrix Endpoint Management, puis le packaging de ces dernières à l'aide de groupes de mise à disposition. Les groupes de mise à disposition définissent des catégories d'utilisateurs qui vous permettent de déployer des stratégies, des applications, des médias et des actions spécifiques sur leurs appareils. À l'aide de la console Citrix Endpoint Management, vous pouvez :

- Ajouter, gérer et déployer des groupes de mise à disposition ;
- Modifier l'ordre dans lequel Citrix Endpoint Management transmet les ressources et les actions d'un groupe de mise à disposition vers les appareils. Cette commande est appelée *ordre de déploiement*.

  Vous pouvez spécifier l'ordre de déploiement dans la console Citrix Endpoint Management. Cependant, Citrix Endpoint Management détermine l'ordre de déploiement lorsqu'un utilisateur figure dans plusieurs groupes de mise à disposition qui comportent des stratégies conflictuelles ou en double. Voir Étapes de calcul.

À propos des groupes de disposition

L'inclusion dans un groupe de mise à disposition est basée sur les caractéristiques des utilisateurs, telles que l'entreprise, le pays, le département, l'adresse et la fonction. Les groupes de mise à disposition vous permettent de mieux contrôler les personnes qui reçoivent les ressources et à quel moment. Vous pouvez déployer un groupe de mise à disposition vers tous les utilisateurs ou vers un groupe d'utilisateurs défini.

Le groupe de mise à disposition par défaut, AllUsers, est créé lorsque vous installez et configurez Citrix Endpoint Management. Ce groupe contient tous les utilisateurs locaux et les utilisateurs Active Directory. Vous ne pouvez pas supprimer le groupe AllUsers, mais vous pouvez le désactiver si vous ne souhaitez pas envoyer des ressources à tous les utilisateurs. Pour plus de détails, voir Activer et désactiver le groupe de mise à disposition AllUsers.

Lorsque vous déployez une ressource vers un groupe de mise à disposition, vous envoyez une notification push à tous les utilisateurs du groupe de mise à disposition. Pour les appareils Apple, utilisez le service de notification push d'Apple (APNs) pour envoyer des notifications. Pour de plus amples informations, consultez la section Certificats APNs. Pour les appareils Android, utilisez Firebase Cloud Messaging (FCM). Pour plus d'informations, voir Firebase Cloud Messaging. Pour les appareils Windows, utilisez le service de notifications push Windows (WNS).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

À propos du déploiement des ressources

Lorsque vous transmettez des ressources vers des appareils, prenez en compte les éléments suivants :

- **Ordre de déploiement :** séquence dans laquelle Citrix Endpoint Management transmet les ressources (stratégies, applications et médias) et actions à un appareil. L'ordre de déploiement s'applique uniquement aux appareils d'un groupe de mise à disposition dont le profil d'inscription est configuré pour la gestion des appareils (MDM) ou pour une combinaison de gestion des applications (MAM) et des appareils (MDM).
- **Règles de déploiement :** Citrix Endpoint Management utilise les règles de déploiement que vous spécifiez pour les propriétés d'appareil et d'utilisateur pour filtrer les stratégies, les applications, les médias, les actions et les groupes de mise à disposition. Par exemple, une règle de déploiement peut spécifier la distribution du paquetage de déploiement lorsqu'un nom de domaine correspond à une valeur particulière.

  Dans un groupe de mise à disposition, vous pouvez spécifier un sous-ensemble d'utilisateurs et d'appareils qui reçoivent les ressources en fonction de leurs propriétés d'utilisateur et d'appareil. Le filtrage des propriétés d'utilisateur et d'appareil au sein d'un groupe de mise à disposition est prioritaire sur les règles de déploiement définies sur la ressource.
- **Calendrier de déploiement :** Citrix Endpoint Management utilise le calendrier de déploiement que vous spécifiez pour les actions, les applications, les médias et les stratégies pour contrôler le déploiement de ces éléments. Vous pouvez spécifier un déploiement immédiat, à une date et heure définies, ou en fonction de conditions de déploiement. Vous spécifiez le calendrier lorsque vous créez la règle. Voir Configurez les règles de déploiement.

Avant d'ajouter des groupes de mise à disposition, déterminez comment l'ordre, les règles et le calendrier de déploiement sont liés à vos objectifs de déploiement.

Ordre de déploiement

L'ordre de déploiement est la séquence dans laquelle Citrix Endpoint Management transmet les ressources aux appareils. L'ordre de déploiement est important lorsqu'il existe des conditions préalables pour les ressources et les dépendances entre les ressources. Les ressources comprennent les stratégies, les applications, les actions et les groupes de mise à disposition.

Par exemple, si vous appliquez une stratégie Wi-Fi dotée d'une authentification basée sur les certificats, vous devez transmettre la stratégie de certification avant la stratégie Wi-Fi. Sinon, des erreurs se produisent. Inversement, pour certaines stratégies (telles que les conditions générales, l'inventaire logiciel et les actions), l'ordre de déploiement n'a pas d'importance.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Lorsque vous ajoutez un groupe de mise à disposition, vous pouvez spécifier l'ordre dans lequel les ressources sont déployées sur les appareils. Cependant, Citrix Endpoint Management identifie toujours chaque situation dans laquelle un utilisateur figure dans plusieurs groupes de mise à disposition qui comportent des stratégies conflictuelles ou en double. Dans ces cas, Citrix Endpoint Management calcule un ordre de déploiement à la fois pour les objets qu'il fournit à un appareil et pour les actions qu'il effectue.

Pour déterminer l'ordre de déploiement, Citrix Endpoint Management applique des filtres et des critères de contrôle, tels que des règles de déploiement et un calendrier de déploiement, aux ressources. Le tableau suivant indique les critères que vous pouvez appliquer à chaque type de ressource.

Ressource	Plate-forme de l'appareil	Règles de déploiement	Calendrier de déploiement	Utilisateur/groupes
Stratégie d'appareil	O	O	O	-
Application	O	O	O	-
Média	O	O	O	-
Action	-	O	O	-
Groupe de mise à disposition	-	O	-	O

Étapes de calcul

Lorsque Citrix Endpoint Management doit calculer l'ordre de déploiement, il effectue ces étapes.

> **Remarque :**
>
> La plate-forme de l'appareil n'affecte pas les étapes de calcul.

1. Détermine tous les groupes de mise à disposition d'un utilisateur spécifique, en fonction des filtres de groupes, d'utilisateurs et des règles de déploiement.
2. Crée une liste ordonnée de toutes les ressources (applications, actions, médias et stratégies) dans les groupes de mise à disposition sélectionnés. La liste est basée sur les filtres de plate-forme d'appareil, les règles de déploiement et le calendrier de déploiement. L'algorithme utilisé est le suivant :

    a) Les ressources provenant des groupes de mise à disposition qui ont un ordre de déploiement défini par l'administrateur sont placées avant les ressources provenant des groupes de mise à disposition ne disposant pas d'un ordre de déploiement. Pour plus de détails, voir Exemple de calcul avec ordre défini par l'utilisateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) Pour départager les groupes de mise à disposition, les ressources provenant de groupes de mise à disposition sont classées par nom de groupe de mise à disposition et par ordre alphabétique inverse. Par exemple, Citrix Endpoint Management place les ressources provenant du groupe de mise à disposition B avant les ressources provenant du groupe de mise à disposition A.

c) Lors du tri, si un ordre de déploiement défini par un administrateur est spécifié pour les ressources d'un groupe de mise à disposition, cet ordre est conservé. Sinon, les ressources dans ce groupe de mise à disposition sont triées par nom de ressource et par ordre alphabétique.

d) Si la même ressource apparaît plus d'une fois, la ressource dupliquée est supprimée. Seule la première de ces ressources est fournie.

Les ressources pour lesquelles un ordre a été défini par un administrateur sont déployées avant les ressources pour lesquelles aucun ordre n'a été défini par un administrateur.

Exemple de calcul avec ordre défini par l'administrateur Supposons que vous ayez deux groupes de mise à disposition :

- Groupe de mise à disposition, Gestionnaires de comptes 1 : avec un ordre *non spécifié* pour les ressources. Contient les stratégies **Réseau** et **Code secret**.
- Groupe de mise à disposition, Gestionnaires de comptes 2 : avec un ordre *spécifié* pour les ressources. Contient les stratégies **Planification de connexion**, **Restrictions**, **Code secret** et **Réseau** dans cet ordre.

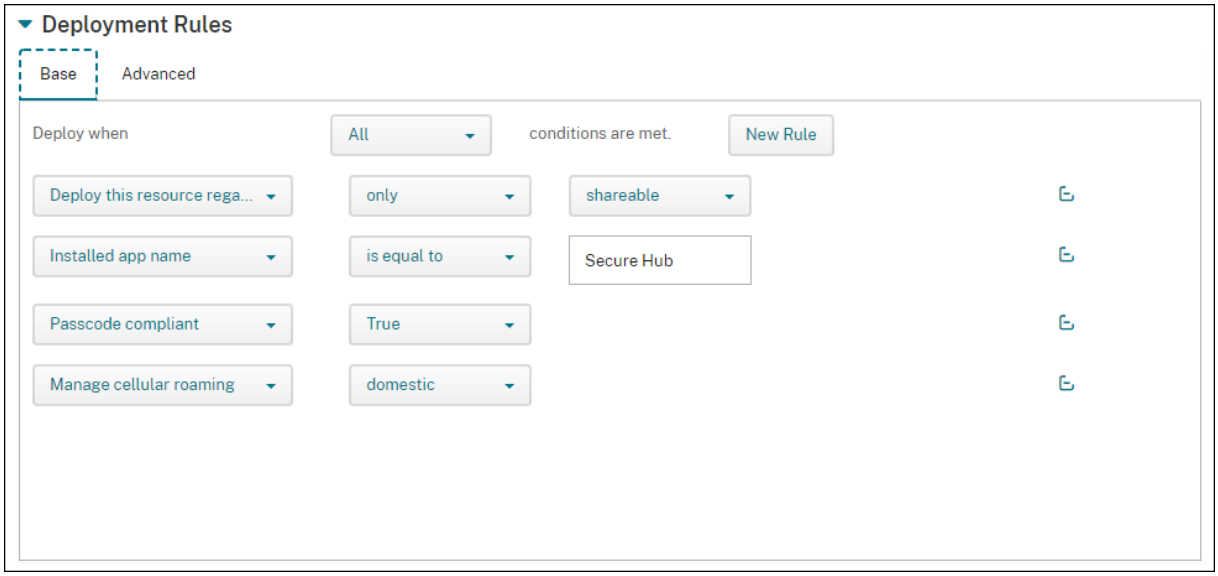
Si l'algorithme de calcul classait uniquement les groupes de déploiement par nom, Citrix Endpoint Management réaliserait le déploiement dans cet ordre, en commençant par le groupe de mise à disposition Gestionnaires de comptes 1 : **Réseau**, **Code secret**, **Planification de connexion** et **Restrictions**. Citrix Endpoint Management peut ignorer **Code secret** et **Réseau**, des doublons du groupe de mise à disposition Gestionnaires de comptes 2.

Cependant, le groupe Gestionnaires de comptes 2 a un ordre de déploiement spécifié par l'administrateur. Par conséquent, l'algorithme de calcul place les ressources provenant du groupe de mise à disposition Gestionnaires de comptes 2 dans une position plus élevée dans la liste que les ressources de l'autre groupe de mise à disposition Gestionnaires de comptes 1. Par conséquent, Citrix Endpoint Management déploie les stratégies dans cet ordre : **Planification de connexion**, **Restrictions**, **Code secret** et **Réseau**. Citrix Endpoint Management ignore les stratégies **Réseau** et **Code secret** du groupe de mise à disposition Gestionnaires de comptes 1, car elles sont dupliquées. Par conséquent, cet algorithme respecte l'ordre spécifié par l'administrateur Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurez les règles de déploiement

Configurez des règles de déploiement pour mettre des ressources à disposition lorsque des conditions spécifiques existent. Vous pouvez configurer des règles de déploiement de base ou avancées.



Lorsque vous ajoutez une règle de déploiement à l'aide de l'éditeur de règles de base, sélectionnez d'abord quand déployer la ressource.

- **Toutes :** mettez la ressource à disposition lorsque l'utilisateur ou l'appareil remplit toutes les conditions que vous configurez.
- **Une :** mettez la ressource à disposition lorsque l'utilisateur ou l'appareil remplit au moins l'une des conditions que vous configurez.

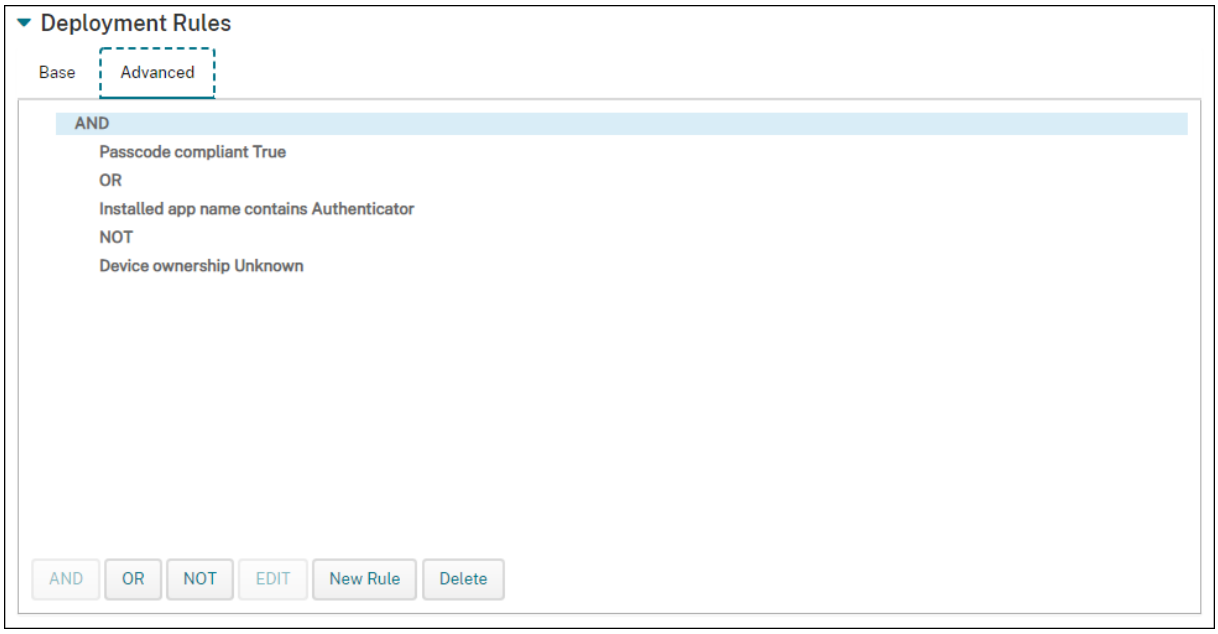
Cliquez sur **Nouvelle règle** pour choisir une règle dans la liste des règles disponibles à ajouter. Les règles disponibles varient en fonction de la ressource déployée et de la plate-forme pour laquelle vous configurez la ressource. Chaque règle contient des conditions.

Vous pouvez spécifier le déploiement de la ressource :

- uniquement lorsque la propriété sélectionnée existe ou sauf lorsque la propriété sélectionnée existe ;
- lorsque la propriété correspond exactement au texte que vous avez entré, lorsque la propriété contient le texte que vous avez entré ou lorsque la propriété ne correspond pas au texte que vous avez entré ;
- lorsque l'appareil ou l'utilisateur est conforme à la propriété sélectionnée ou n'est pas conforme à la propriété sélectionnée ;
- lorsque les propriétés de l'appareil ou de l'utilisateur correspondent à une condition que vous sélectionnez dans une liste prédéfinie.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Utilisez l'éditeur de règles avancées pour créer des règles de déploiement plus complexes. Vous pouvez sélectionner d'autres règles et vous pouvez combiner différents opérateurs logiques booléens lors de la création d'une règle avancée.



Utiliser les groupes de mise à disposition

Vous pouvez utiliser des groupes de mise à disposition de l'une des manières suivantes :

- Ajouter un groupe de mise à disposition
- Déployer sur des groupes de mise à disposition
- Supprimer un groupe de mise à disposition
- Modifier un groupe de mise à disposition
- Activer et désactiver le groupe de mise à disposition AllUsers.

Ajouter un groupe de mise à disposition

Lorsque vous créez un groupe de mise à disposition, vous spécifiez si les attributions utilisateur sont gérées dans Citrix Endpoint Management ou dans Citrix Cloud. Vous ne pouvez pas modifier cette spécification après avoir créé le groupe de mise à disposition.

Si vous prévoyez d'utiliser le groupe de mise à disposition pour mettre à disposition des services Citrix Cloud, indiquez que les attributions utilisateur sont gérées dans Citrix Cloud. Les autres services Citrix Cloud incluent Citrix Virtual Apps and Desktops, ShareFile ou Secure Browser Service. Vous pouvez ajouter des utilisateurs Active Directory uniquement aux groupes de mise à disposition gérés dans Citrix Cloud.

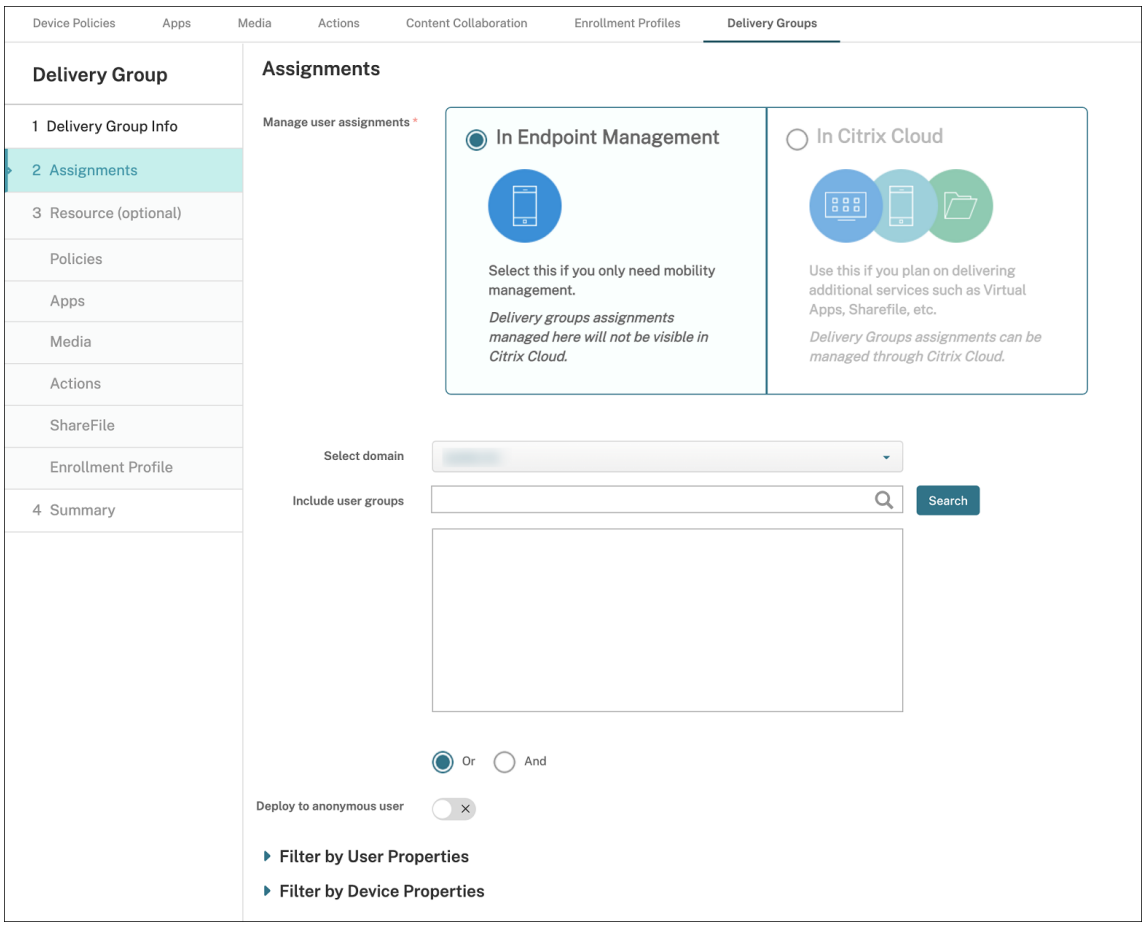
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si un groupe de mise à disposition pour les utilisateurs et les applications nécessite uniquement une gestion de la mobilité, définissez **Gérer les attributions d'utilisateurs** sur **Dans Citrix Endpoint Management**. Les groupes de mise à disposition avec des utilisateurs gérés dans Citrix Endpoint Management ne sont pas visibles dans Citrix Cloud. Par conséquent, vous ne pouvez pas utiliser les groupes de mise à disposition gérés dans Citrix Endpoint Management pour mettre à disposition d'autres services.

> **Remarque :**
>
> Nous vous recommandons d'ajouter des groupes de mise à disposition avant de créer des stratégies d'appareil et des profils d'inscription. Pour plus d'informations sur leur création, consultez Stratégies d'appareil et Profils d'inscription.

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Groupes de mise à disposition**.
2. Sur la page **Groupes de mise à disposition**, cliquez sur **Ajouter**.
3. Dans la page **Informations sur le groupe de mise à disposition**, tapez un nom et une description pour le groupe de mise à disposition, puis cliquez sur **Suivant**.
4. Sur la page **Attributions**, indiquez comment gérer les attributions du groupe de mise à disposition.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Gérer les attributions d'utilisateurs :**
  - **Dans Citrix Endpoint Management :** sélectionnez cette option si vous envisagez de créer un groupe de mise à disposition pour les utilisateurs et les applications qui n'ont besoin que de la gestion de la mobilité. Les groupes de mise à disposition dont les attributions utilisateur sont gérées dans Citrix Endpoint Management ne sont pas visibles dans Citrix Cloud et ne peuvent pas être utilisés pour mettre à disposition d'autres services.
  - **Dans Citrix Cloud :** sélectionnez cette option si vous prévoyez d'utiliser le groupe de mise à disposition pour mettre à disposition d'autres services. Ces services peuvent inclure Citrix Virtual Apps and Desktops ou ShareFile.

5. Ajoutez des utilisateurs au groupe de mise à disposition.

> **Important :**
>
> Vous ne pouvez pas modifier le paramètre **Gérer les attributions d'utilisateurs** après la création du groupe d'utilisateurs.

- **Sélectionner un domaine :** sélectionnez le domaine à partir duquel choisir les utilisateurs dans la liste.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Inclure des groupes d'utilisateurs :** effectuez l'une des opérations suivantes :
  - Dans la liste des groupes d'utilisateurs, cliquez sur les groupes que vous souhaitez ajouter. Les groupes sélectionnés s'affichent dans la liste **Groupes d'utilisateurs sélectionnés**.
  - Cliquez sur **Rechercher** pour afficher une liste de tous les groupes d'utilisateurs dans le domaine sélectionné. Vous pouvez également entrer un nom de groupe complet ou partiel dans la zone de recherche, puis cliquer sur **Rechercher** pour affiner votre recherche.

  Pour supprimer un groupe d'utilisateurs de la liste **Groupes d'utilisateurs sélectionnés**, effectuez l'une des opérations suivantes :

  - Dans la liste **Groupes d'utilisateurs sélectionnés**, cliquez sur le **X** en regard de chaque groupe que vous souhaitez supprimer.
  - Cliquez sur **Rechercher** pour afficher une liste de tous les groupes d'utilisateurs dans le domaine sélectionné. Vous pouvez également entrer un nom de groupe complet ou partiel avant de cliquer sur **Rechercher** pour affiner votre recherche. Désactivez la case à cocher en regard de chaque groupe que vous souhaitez supprimer.

- **Ou/Et :** sélectionnez cette option pour spécifier si les utilisateurs appartiennent à n'importe quel groupe (Ou) ou s'ils doivent figurer dans tous les groupes (Et) pour que la ressource puisse leur être déployée.

- **Déployer auprès d'un utilisateur anonyme :** sélectionnez cette option si vous voulez déployer auprès d'utilisateurs non authentifiés dans le groupe de mise à disposition. Les utilisateurs non authentifiés sont des utilisateurs que vous n'avez pas réussi à authentifier, mais dont les appareils sont autorisés à se connecter à Citrix Endpoint Management.

6. Développez **Filtrer par propriétés d'utilisateur** ou **Filtrer par propriétés d'appareil** pour spécifier la façon dont le groupe de mise à disposition gère les ressources.

   - Si vous choisissez **Filtrer par propriétés d'appareil**, développez la plate-forme d'appareil pour configurer les règles de déploiement :
     - **Propriétés de l'appareil - Android** (voir Créer une règle pour déployer des ressources sur des appareils Android)
     - **Propriétés de l'appareil - iOS**
     - **Propriétés de l'appareil - Tablettes ou bureaux Windows uniquement**
   - L'onglet **Base** s'affiche par défaut. Sous l'onglet **Base**, spécifiez quand la stratégie doit être déployée. Vous pouvez déployer la stratégie lorsque **toutes** les conditions sont remplies ou lorsque l'**une** des conditions est remplie. L'option par défaut est définie sur **Toutes**.
     - Cliquez sur **Nouvelle règle** pour définir les conditions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Dans les listes, choisissez les conditions. Par exemple, sélectionnez Propriétaire et BYOD.
  - Cliquez sur **Nouvelle règle** pour chaque condition que vous souhaitez ajouter.
- Cliquez sur l'onglet **Avancé** pour combiner les règles avec des options booléennes. Les conditions que vous avez choisies sur l'onglet **Base** s'affichent.
  - Cliquez sur **ET**, **OU** ou **SAUF**, puis sur **Nouvelle règle**.
  - Dans les listes, sélectionnez les conditions à ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit.
    Vous pouvez à tout moment sélectionner une condition et cliquer sur **Modifier** pour modifier la condition ou sur **Supprimer** pour la supprimer.

7. Cliquez sur **Suivant** pour accéder à la page **Stratégies**. Vous pouvez éventuellement ajouter des stratégies, des applications, des médias ou des actions pour le groupe de mise à disposition. Pour plus de détails, consultez :
   - Ajouter des stratégies à un groupe de mise à disposition
   - Ajouter des applications à un groupe de mise à disposition
   - Ajouter des médias à un groupe de mise à disposition
   - Ajouter des actions à un groupe de mise à disposition
8. Lorsque vous êtes satisfait de votre groupe de mise à disposition, cliquez sur **Résumé** pour afficher un résumé de la configuration.
9. Cliquez sur **Enregistrer**. Le nouveau groupe de mise à disposition apparaît sur la page **Groupes de mise à disposition**.

Ajouter des stratégies à un groupe de mise à disposition

1. Dans la liste **Ressources (facultatif)**, cliquez sur **Stratégies**.
2. Pour chaque stratégie que vous voulez ajouter, procédez comme suit :
   - Parcourez la liste des stratégies disponibles pour trouver la stratégie que vous souhaitez ajouter. Vous pouvez également entrer un nom de stratégie complet ou partiel dans la zone de recherche, puis cliquer sur **Rechercher**.
   - Faites glisser la stratégie que vous souhaitez ajouter dans la zone de droite.

   Pour supprimer une stratégie de la zone, cliquez sur le **X** en regard du nom de la stratégie.
3. Cliquez sur **Suivant** pour accéder à la page **Applications**.

Ajouter des applications à un groupe de mise à disposition

1. Pour chaque application que vous souhaitez ajouter, procédez comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Parcourez la liste des applications disponibles pour trouver l'application que vous souhaitez ajouter. Vous pouvez également entrer un nom d'application complet ou partiel dans la zone de recherche, puis cliquer sur **Rechercher**.
- Faites glisser l'application dans la zone **Applications requises** ou dans la zone **Applications facultatives**.

Pour les applications marquées comme requises, les utilisateurs peuvent recevoir les mises à jour plus rapidement dans certaines situations, par exemple :

- Vous chargez une nouvelle application et la marquez comme requise.
- Vous marquez une application existante comme requise.
- Un utilisateur supprime une application requise.
- Une mise à jour de Citrix Secure Hub est disponible.

Pour plus d'informations sur le déploiement forcé des applications obligatoires, notamment sur la façon d'activer la fonctionnalité, voir À propos des applications obligatoires et facultatives.

Pour supprimer une application de la zone, cliquez sur le **X** en regard du nom de l'application.

2. Cliquez sur **Suivant** pour accéder à la page **Média**.

Ajouter des médias à un groupe de mise à disposition

1. Pour chaque livre que vous souhaitez ajouter, procédez comme suit :

   - Parcourez la liste des livres disponibles pour trouver le livre que vous souhaitez ajouter. Vous pouvez également entrer un nom de livre complet ou partiel dans la zone de recherche, puis cliquer sur **Rechercher**.
   - Faites glisser le livre que vous souhaitez ajouter dans la zone **Livres obligatoires**.

   Pour les livres marquées comme obligatoires, les utilisateurs reçoivent les mises à jour plus rapidement dans certaines situations, par exemple :

   - Vous chargez un nouveau livre et le marquez comme obligatoire.
   - Vous marquez un livre existant comme obligatoire.
   - Un utilisateur supprime un livre obligatoire.
   - Une mise à jour de Citrix Secure Hub est disponible.

   Pour supprimer un livre de la zone, cliquez sur le **X** en regard du nom du livre.

2. Cliquez sur **Suivant** pour accéder à la page **Actions**.

Ajouter des actions à un groupe de mise à disposition

1. Pour chaque action que vous voulez ajouter, procédez comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Parcourez la liste des actions disponibles pour trouver l'action que vous souhaitez ajouter. Vous pouvez également entrer un nom d'action complet ou partiel dans la zone de recherche, puis cliquer sur **Rechercher**.
- Faites glisser l'action que vous souhaitez ajouter dans la zone de droite.

Pour supprimer une action de la zone, cliquez sur le **X** en regard du nom de l'action.

2. Cliquez sur **Suivant** pour accéder à la page **ShareFile**.

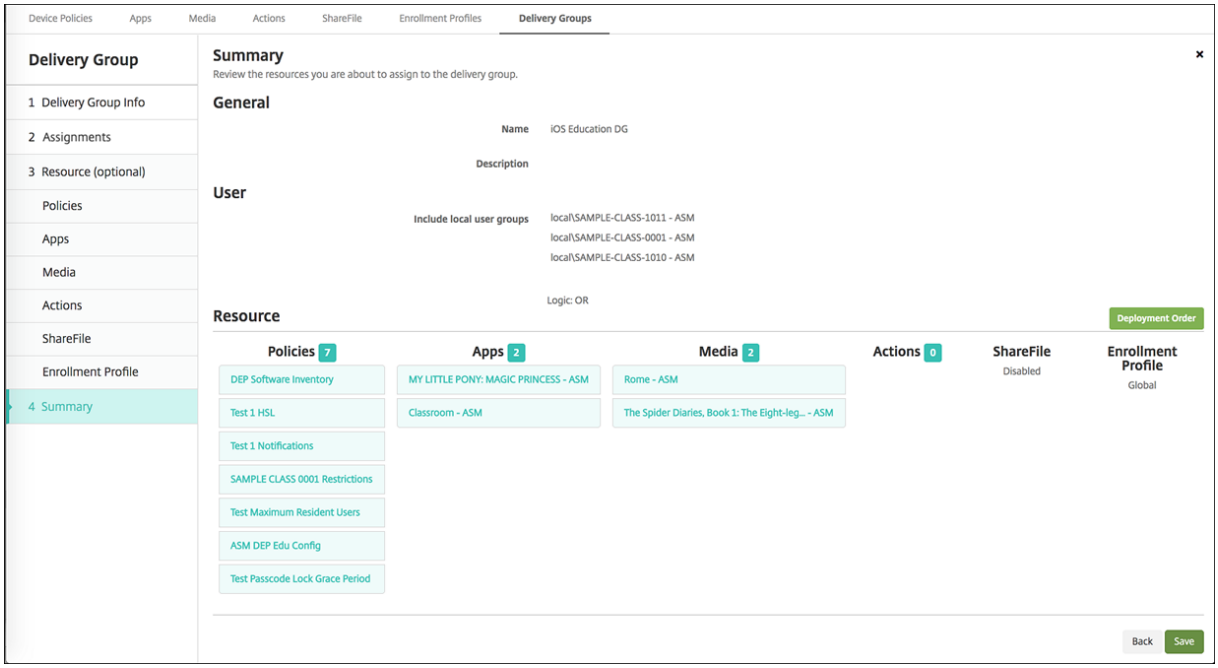
Appliquer la configuration ShareFile La page ShareFile diffère selon que vous avez configuré Citrix Endpoint Management (**Configurer > ShareFile**) pour les comptes Enterprise ou pour les connecteurs de zones de stockage.

- Si vous avez configuré des comptes Enterprise pour une utilisation avec Citrix Endpoint Management, définissez **Activer ShareFile** sur **Activé**. Ce paramètre fournit au groupe de mise à disposition un accès par authentification unique au contenu et aux données de ShareFile.
- Si vous avez configuré des connecteurs StorageZone à utiliser avec Citrix Endpoint Management, sélectionnez les connecteurs StorageZone à inclure dans le groupe de mise à disposition dans la zone de droite.

Consulter les options configurées et modifier l'ordre de déploiement Sur la page Résumé, vous pouvez vérifier les options que vous avez configurées pour le groupe de mise à disposition et modifier l'ordre de déploiement des ressources. La page Résumé affiche vos ressources par catégorie. La page Résumé n'affiche pas l'ordre de déploiement.

> **Remarque :**
>
> Cliquez sur **Retour** pour revenir aux pages précédentes pour modifier la configuration.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



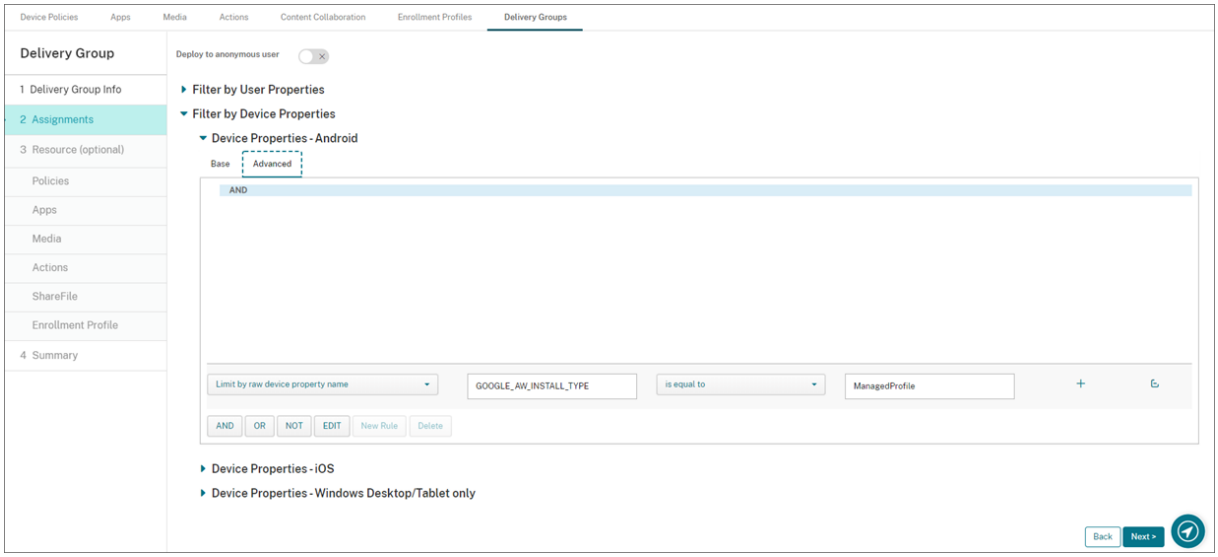
Pour afficher ou modifier l'ordre de déploiement :

1. Cliquez sur **Ordre de déploiement**.
2. Dans la boîte de dialogue Ordre de déploiement, faites glisser une ressource vers l'emplacement dans l'ordre où vous souhaitez la déployer. Le déploiement des ressources est traité de haut en bas dans l'ordre.
3. Cliquez sur **Enregistrer** pour enregistrer l'ordre de déploiement.

Lorsque vous avez terminé de configurer le groupe de mise à disposition, sur la page Résumé, cliquez sur **Enregistrer**.

Créer une règle pour déployer des ressources sur Android Enterprise Vous pouvez gérer le déploiement d'un groupe de mise à disposition sur les appareils Android Enterprise à l'aide des règles de propriété de l'appareil Android. Si vous inscrivez plusieurs appareils pour le même utilisateur, vous pouvez créer des filtres avancés pour Android Enterprise en fonction du mode d'inscription de l'appareil ou de l'ID du package d'application de l'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pour déployer un groupe de mise à disposition sur des appareils Android Enterprise à l'aide du mode d'inscription d'appareil :

1. Créez un groupe de mise à disposition.
2. Dans la page **Attributions**, développez **Filtrer par propriétés d'appareil**.
3. Dans **Propriétés de l'appareil - Android**, ouvrez l'onglet **Avancé** et cliquez sur **Nouvelle règle**.
4. Dans la liste, choisissez la condition à ajouter à la règle :
   - Pour les nouveaux appareils Android Enterprise, choisissez **Limiter par nom de propriété d'appareil brut** et entrez **GOOGLE_AW_INSTALL_TYPE** dans le premier champ de valeur. Vous devez ensuite définir la condition qui correspond à l'un des modes d'inscription.
   - Pour les appareils Android Enterprise existants, choisissez **Limiter par nom de propriété d'appareil connu** et sélectionnez **Type d'installation Android Entreprise** dans le premier champ de valeur. Vous devez ensuite définir la condition qui correspond à l'un des modes d'inscription.
5. Dans le second champ, entrez un mode d'inscription pour vos appareils Android Enterprise :
   - **DeviceAdministrator :** spécifie les appareils appartenant à l'entreprise destinés uniquement à un usage professionnel (également connus sous le nom « mode propriétaire de l'appareil »)
   - **ManagedProfile :** spécifie les appareils personnels BYOD inscrits avec la gestion des profils de travail (également connus sous le nom « mode propriétaire du profil »)
   - **CorporateOwnedSingleUse :** spécifie les appareils dédiés (anciennement connus sous le nom « appareils d'entreprise à usage unique » ou appareils COSU)
   - **CorporateOwnedPersonallyEnabled :** spécifie les appareils entièrement gérés avec un profil de travail, (anciennement connus sous le nom « appareils COPE » ou propriété de l'entreprise avec accès privé)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Terminez la configuration du groupe de mise à disposition comme décrit dans Ajouter un groupe de mise à disposition.

   Pour plus d'informations, consultez la section Scénarios et profils de déploiement d'appareils.

Pour déployer un groupe de mise à disposition sur des appareils Android Enterprise à l'aide de l'ID du package d'application de l'appareil :

1. Dans **Propriétés de l'appareil - Android**, ouvrez l'onglet **Avancé** et cliquez sur **Nouvelle règle**.
2. Dans la liste, choisissez **Nom de l'application installée** et entrez l'ID du package d'application.

Modifier un groupe de mise à disposition

Vous ne pouvez pas modifier le nom d'un groupe de mise à disposition existant. Pour mettre à jour les autres paramètres, accédez à **Configurer > Groupes de mise à disposition**, sélectionnez le groupe que vous souhaitez modifier, puis cliquez sur **Modifier**.

Activer et désactiver le groupe de mise à disposition AllUsers

AllUsers est le seul groupe de mise à disposition que vous pouvez activer ou désactiver. Vous ne pouvez pas supprimer AllUsers comme d'autres groupes de mise à disposition.

Sur la page **Groupes de mise à disposition**, sélectionnez le groupe de mise à disposition AllUsers en sélectionnant la case à cocher en regard de **AllUsers** ou en cliquant sur la ligne contenant **AllUsers**. Procédez ensuite comme suit :

- Cliquez sur **Désactiver** pour désactiver le groupe de mise à disposition AllUsers. Cette commande est uniquement disponible si AllUsers est activé (paramètre par défaut). **Désactivé** s'affiche sous le titre **Désactivé** dans le tableau des groupes de mise à disposition.
- Cliquez sur **Activer** pour activer le groupe de mise à disposition AllUsers. Cette commande est uniquement disponible si le groupe AllUsers est désactivé. **Désactivé** ne s'affiche plus sous le titre **Désactivé** dans le tableau des groupes de mise à disposition.

Déployer sur des groupes de mise à disposition

Le déploiement sur un groupe de mise à disposition implique l'envoi d'une notification de type push à tous les utilisateurs équipés d'appareils Apple, Android et Windows Tablet.

Pour les utilisateurs avec d'autres plates-formes d'appareil : si ces appareils sont déjà connectés à Citrix Endpoint Management, ils reçoivent les ressources immédiatement. Sinon, en fonction de leur stratégie de planification, ils reçoivent les ressources la prochaine fois qu'ils se connectent.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour mettre à jour les applications affichées dans la liste des applications disponibles dans le magasin d'applications sur les appareils Android des utilisateurs, vous devez d'abord déployer une stratégie d'inventaire des applications sur les appareils des utilisateurs.

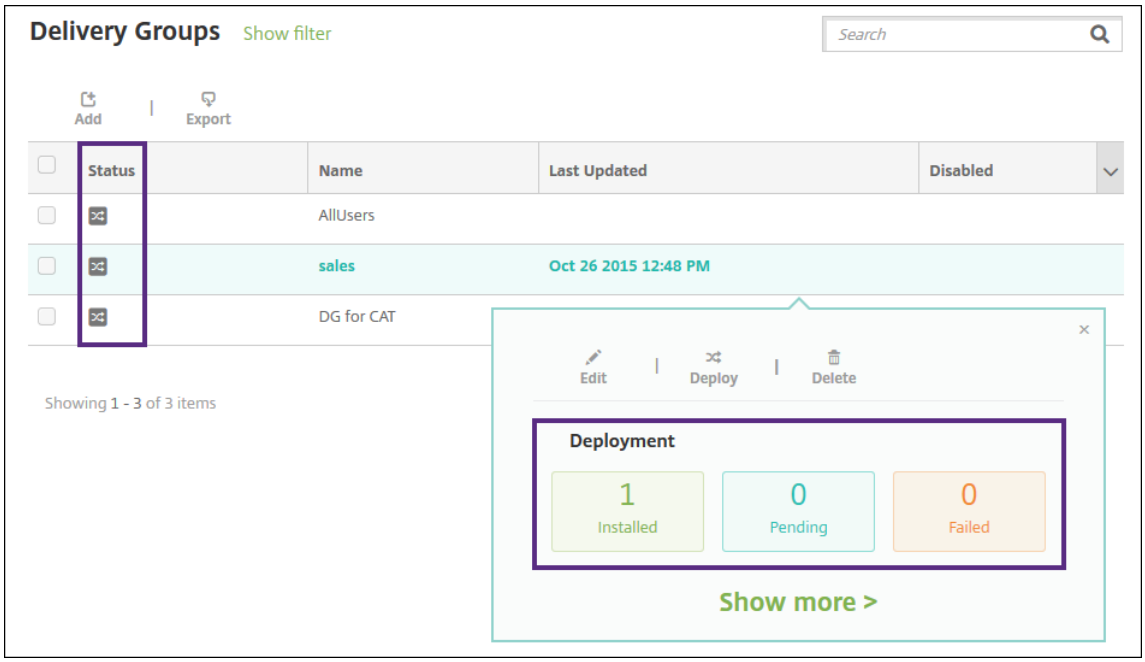
1. Sur la page **Groupes de mise à disposition**, effectuez l'une des opérations suivantes :
   - Pour déployer sur plus d'un groupe de mise à disposition à la fois, sélectionnez les cases à cocher en regard des groupes sur lesquels vous voulez déployer.
   - Pour déployer sur un seul groupe de mise à disposition, sélectionnez la case à cocher en regard de son nom ou cliquez sur la ligne contenant son nom.
2. Cliquez sur **Déployer**.

   En fonction de la manière dont vous sélectionnez un groupe de mise à disposition, la commande **Déployer** apparaît au-dessus ou à droite du groupe de mise à disposition.

   Vérifiez que les groupes auprès desquels vous souhaitez déployer des applications, des stratégies et des actions sont répertoriés. Cliquez ensuite sur **Déployer**. Les applications, stratégies et actions sont déployées auprès des groupes sélectionnés en fonction de la plate-forme d'appareil et de la stratégie de planification.

   Vous pouvez vérifier l'état du déploiement sur la page **Groupes de mise à disposition** de l'une des façons suivantes :

   - Examinez l'icône de déploiement sous l'en-tête **État** pour le groupe de mise à disposition, qui indique les échecs de déploiement.
   - Cliquez sur la ligne contenant le groupe de mise à disposition pour afficher une superposition indiquant si l'état des déploiements est défini sur **Installé**, **En attente** ou **Échec**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cloner un groupe de mise à disposition

Clonez un groupe de mise à disposition lorsque vous souhaitez créer un groupe de mise à disposition similaire à un groupe de mise à disposition existant. Utilisez le clone comme point de départ de votre nouveau groupe de mise à disposition. Apportez ensuite des modifications au clone, par exemple en ajoutant des profils d'inscription ou de nouveaux ensembles d'utilisateurs AD.

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer**, puis sélectionnez l'onglet **Groupes de mise à disposition**.
2. Dans la liste des groupes de mise à disposition, sélectionnez celui que vous souhaitez utiliser comme base pour le nouveau groupe.
3. Sélectionnez **Cloner**.
4. Dans la boîte de dialogue Cloner un groupe de mise à disposition, entrez le nom du nouveau groupe et, éventuellement, une description.
5. Sélectionnez **Cloner**.

Supprimer des groupes de mise à disposition

Vous ne pouvez pas supprimer le groupe de mise à disposition AllUsers, mais vous pouvez le désactiver si vous ne souhaitez pas envoyer des ressources à tous les utilisateurs. Voir Activer et désactiver le groupe de mise à disposition AllUsers.

> **Important :**
>
> Vous ne pouvez pas annuler une suppression.

1. Sur la page **Groupes de mise à disposition**, effectuez l'une des opérations suivantes :
   - Pour supprimer plus d'un groupe de mise à disposition à la fois, sélectionnez les cases à cocher en regard des groupes que vous voulez supprimer.
   - Pour supprimer sur un seul groupe de mise à disposition, sélectionnez la case à cocher en regard de son nom ou cliquez sur la ligne contenant son nom.
2. Cliquez sur **Delete**.

   En fonction de la manière dont vous sélectionnez un groupe de mise à disposition, la commande **Supprimer** apparaît au-dessus ou à droite du groupe de mise à disposition.
3. Dans la boîte de dialogue **Supprimer**, cliquez sur **Supprimer**.

Exporter le tableau des groupes de mise à disposition

1. Cliquez sur **Exporter** au-dessus du tableau **Groupes de mise à disposition**. Citrix Endpoint Management extrait les informations du tableau **Groupes de mise à disposition** et les convertit en fichier .csv.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Ouvrez ou enregistrez le fichier .csv en suivant les étapes habituelles de votre navigateur.

Macros

March 1, 2024

Citrix Endpoint Management fournit des macros qui permettent de renseigner les données de propriété utilisateur ou appareil dans le champ de texte des éléments suivants :

- Stratégies
- Notifications
- Modèles d'inscription
- Fichier XML de configuration d'appareil
- Actions automatisées
- Demandes de signature de certificat de fournisseurs d'identité

Citrix Endpoint Management remplace une macro avec les valeurs utilisateur ou système correspondantes. Par exemple, vous pouvez pré-remplir la valeur boîte aux lettres pour un utilisateur dans un seul profil Exchange pour des milliers d'utilisateurs.

Syntaxe des macros

Une macro peut prendre la forme suivante :

- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)] }`

Placez toute syntaxe suivie du symbole dollar ($) entre accolades ({ }).

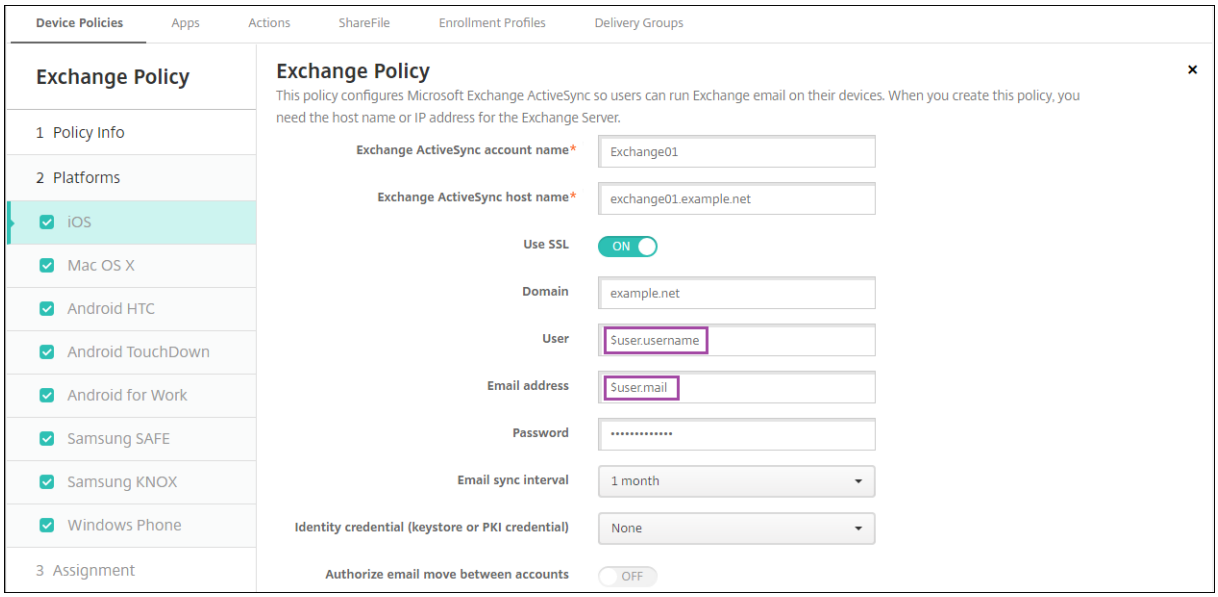
- Les noms de propriétés qualifiés font référence à une propriété utilisateur, à une propriété d'appareil ou à une propriété personnalisée.
- Les noms de propriétés qualifiés consistent en un préfixe, suivi par le nom de propriété réel.
- Les propriétés de l'utilisateur prennent la forme `${ user.[PROPERTYNAME] (prefix="user.")}`.
- Les propriétés d'appareil prennent la forme `${ device.[PROPERTYNAME] (prefix="device.")}`.
- Les noms de propriétés sont sensibles à la casse.
- Une fonction peut être une liste limitée ou un lien vers une référence tierce qui définit les fonctions. Cette macro pour un message de notification comprend la fonction `firstnotnull` :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

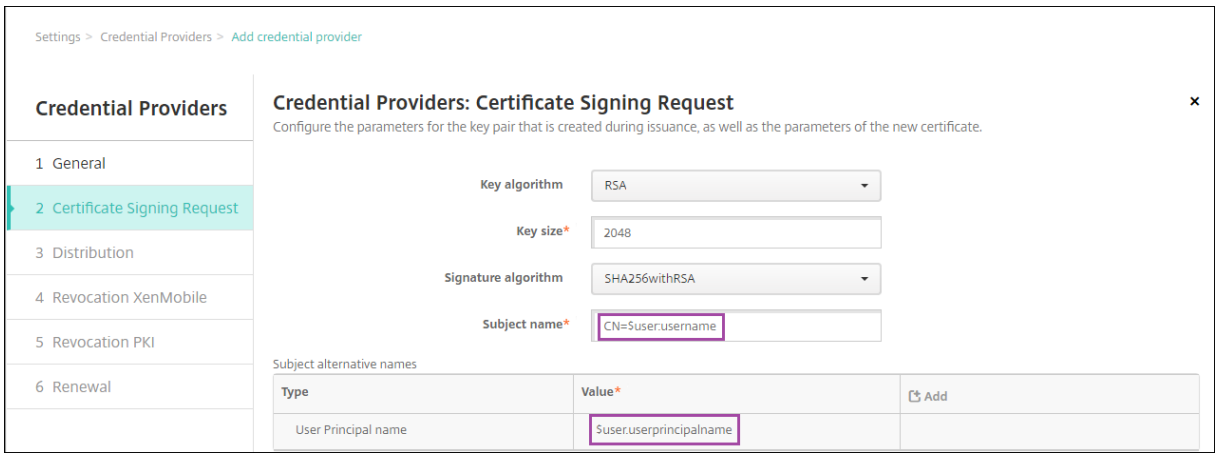
L'appareil `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` a été bloqué …

- Pour les macros personnalisées (propriétés que vous définissez), le préfixe est `${ custom }`. Vous pouvez omettre le préfixe.

Voici un exemple de macro couramment utilisée, `${ user.username }`, qui remplit la valeur de nom d'utilisateur dans le champ de texte d'une stratégie. Cette macro est utile pour la configuration des profils Exchange ActiveSync et d'autres profils utilisés par plusieurs utilisateurs. L'exemple suivant illustre comment utiliser les macros dans une stratégie Exchange. La macro pour **Utilisateur** est `${ user.username }`. La macro pour **Adresse e-mail** est `${ user.mail }`.



L'exemple suivant illustre comment utiliser les macros pour une demande de signature de certificat. La macro pour **Nom du sujet** est **CN=$user.username**. La macro pour la **Valeur** d'un **Autre nom de l'objet** est **$user.userprincipalname**.

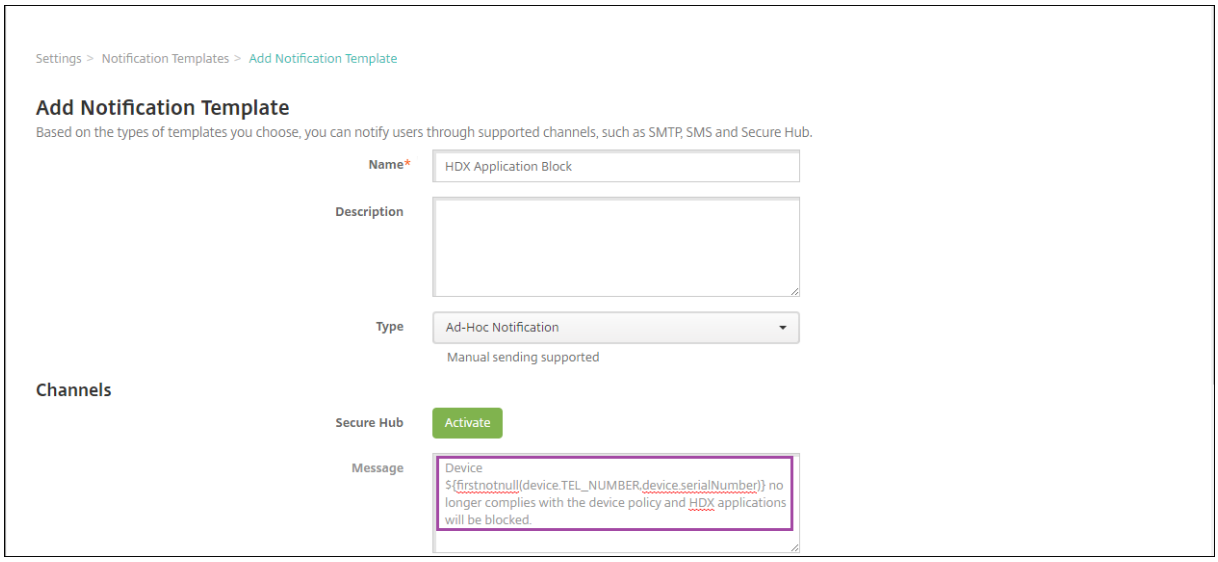


L'exemple suivant illustre comment utiliser les macros dans un modèle de notification. Le modèle

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

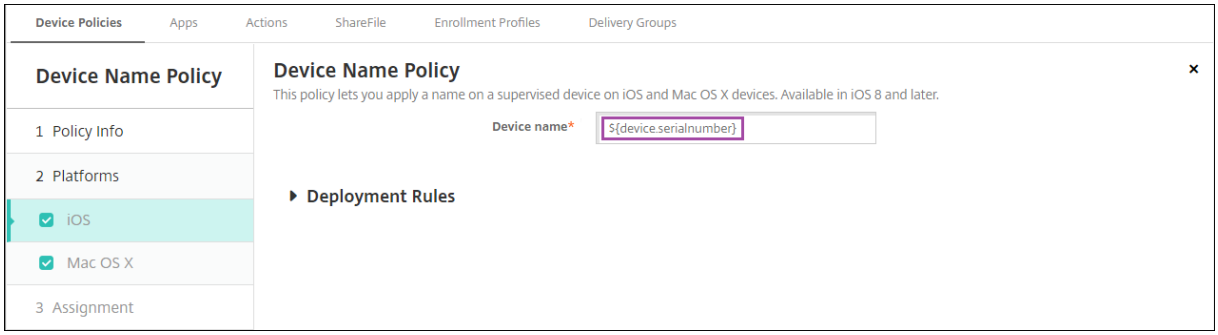
en exemple définit le message envoyé à un utilisateur lorsque les applications HDX sont bloquées en raison d'un appareil non conforme. La macro pour le **Message** est :

L'appareil `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` n'est plus conforme avec la stratégie et les applications HDX sont bloquées.



Pour plus d'exemples de macros utilisées dans les notifications, accédez à **Paramètres > Modèles de notification**, sélectionnez un modèle prédéfini et cliquez sur **Modifier**.

L'exemple suivant illustre une macro dans la stratégie de nom de l'appareil. Vous pouvez entrer une macro, une combinaison de macros, ou une combinaison de macros et de texte pour donner un nom unique à chaque appareil. Par exemple, utilisez `${ device.serialnumber }` pour définir le nom de l'appareil à partir du numéro de série de l'appareil. Utilisez `${ device.serialnumber } ${ user.username }` pour inclure le nom d'utilisateur dans le nom de l'appareil. La stratégie de nom d'appareil fonctionne sur les appareils supervisés iOS et macOS.



Macros pour les modèles de notification par défaut

Les macros suivantes sont utilisées dans les modèles de notification par défaut :

- `${ account.SUPPORT_EMAIL }`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

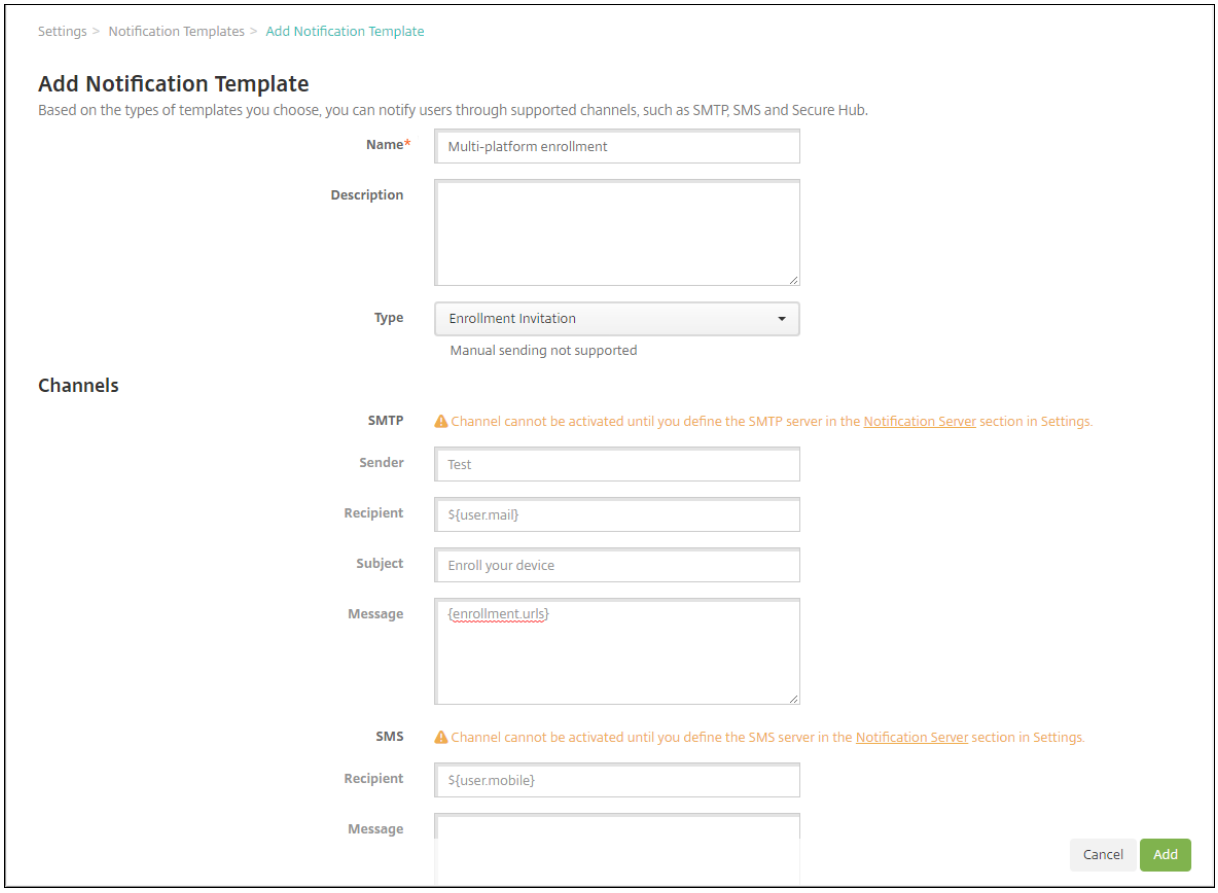
- ${ applicationName }
- ${ enrollment.andriod.agent.download.url }
- ${ enrollment.ios.agent.download.url }
- ${ enrollment.pin }
- ${ enrollment.url }
- ${ enrollment.urls }
- ${ enrollment.ios.url }
- ${ enrollment.macos.url }
- ${ enrollment.android.url }
- ${ enrollment.ios.platform }
- ${ enrollment.macos.platform }
- ${ enrollment.android.platform }
- ${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}
- ${ firstnotnull(device.TEL_NUMBER,user.mobile)}
- ${ outofcompliance.reason(smg_block)}
- ${ outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${ vpp.account }
- ${ vpp.appname }
- ${ vpp.url }
- ${ zdmserver.hostPath } /enroll

> **Remarque :**
>
> La console Citrix Endpoint Management utilise les termes « liste noire » et « liste blanche ». Ces termes seront modifiés dans une prochaine version et les termes « liste de blocage » et « liste d'autorisation » les remplaceront.

Cet exemple illustre comment créer une notification qui comprend des adresses URL d'inscription pour plusieurs plates-formes. La macro pour le **Message** est :

${enrollment.urls}

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Ces exemples montrent comment créer des messages pour les notifications qui invitent les utilisateurs à cliquer sur l'adresse URL d'inscription pour leurs plates-formes :

Exemple 1 :

```
To enroll, click the link below that applies to your device platform:

${
 enrollment.ios.platform }
  - ${
 enrollment.ios.url }


${
 enrollment.macos.platform }
  - ${
 enrollment.macos.url }


${
 enrollment.android.platform }
  - ${
 enrollment.android.url }


```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--NeedCopy-->
```

Exemple 2 :

```
To enroll an iOS device, click the link ${
 enrollment.ios.url }
 .

To enroll a macOS device, click the link ${
 enrollment.macos.url }
 .

To enroll an Android device, click the link ${
 enrollment.android.url }
 .

<!--NeedCopy-->
```

Macros pour les stratégies spécifiques

Pour la stratégie Nom de l'appareil (pour iOS et macOS), vous pouvez utiliser ces macros pour le **nom de l'appareil** :

- `${ device.serialnumber }`
- `${ user.username } @example.com`
- `${ device.serialnumber }`
- `${ device.serialnumber }`
- `${ user.username }`
- `${ enrollment.pin }`
- `${ user.dnsroot }`

Pour la stratégie Cellulaire (pour iOS), vous pouvez utiliser des macros pour les valeurs des champs qui ne sont pas des chaînes, comme le port du serveur Proxy. Par exemple, vous pouvez désormais utiliser une macro telle que `${ device.xyz }` ou `${ setting.xyz }` qui devient un entier.

Pour un fichier XML de configuration d'appareil que vous importez dans Citrix Endpoint Management à l'aide de la stratégie **d'importation de profils iOS et macOS**, vous pouvez utiliser les macros pour les valeurs des champs autres que des chaînes.

Pour la stratégie de clé de licence MDM Samsung, vous pouvez utiliser cette macro pour la **clé de licence ELM** :

- `${ elm.license.key }`

Pour la stratégie de clip Web, vous pouvez utiliser cette macro pour l'**URL** :

- `${ webeas-url }`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Macros pour obtenir des propriétés d'appareils intégrés

Nom d'affichage	Macros
ID de l'appareil	`$device.id`
GUID de l'appareil	`$device.uniqueid`
IMEI de l'appareil	`$device.imei`
OS	`$device.OSFamily`
Numéro de série	`$device.serialNumber`

Macros pour toutes les propriétés d'appareil

Nom d'affichage : Compte suspendu ?

- **Élément Web :** `GOOGLE_AW_DIRECTORY_SUSPENDED`
- **Macros :** `${ device.GOOGLE_AW_DIRECTORY_SUSPENDED }`

Nom d'affichage : Code de contournement de verrouillage d'activation

- **Élément Web :** `ACTIVATION_LOCK_BYPASS_CODE`
- **Macros :** `${ device.ACTIVATION_LOCK_BYPASS_CODE }`

Nom d'affichage : Verrouillage d'activation activé

- **Élément Web :** `ACTIVATION_LOCK_ENABLED`
- **Macros :** `${ device.ACTIVATION_LOCK_ENABLED }`

Nom d'affichage : compte Apple App Store actif

- **Élément Web :** `ACTIVE_ITUNES`
- **Macros :** `${ device.ACTIVE_ITUNES }`

Nom d'affichage : Administrateur désactivé

- **Élément Web :** `ADMIN_DISABLED`
- **Macros :** `${ device.ADMIN_DISABLED }`

Nom d'affichage : AIK présent ?

- **Élément Web :** `WINDOWS_HAS_AIK_PRESENT`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Macros :** `${ device.WINDOWS_HAS_AIK_PRESENT }`

Nom d'affichage : API Amazon MDM disponible

- **Élément Web :** `AMAZON_MDM`
- **Macros :** `${ device.AMAZON_MDM }`

Nom d'affichage : ID appareil Android Enterprise

- **Élément Web :** `GOOGLE_AW_DEVICE_ID`
- **Macros :** `${ device.GOOGLE_AW_DEVICE_ID }`

Nom d'affichage : Appareil Android Entreprise activé ?

- **Élément Web :** `GOOGLE_AW_ENABLED_DEVICE`
- **Macros :** `${ device.GOOGLE_AW_ENABLED_DEVICE }`

Nom d'affichage : Type d'installation Android Enterprise

- **Élément Web :** `GOOGLE_AW_INSTALL_TYPE`
- **Macros :** `${ device.GOOGLE_AW_INSTALL_TYPE }`

Nom d'affichage : État de la signature de l'antispyware

- **Élément Web :** `ANTI_SPYWARE_SIGNATURE_STATUS`
- **Macros :** `${ device.ANTI_SPYWARE_SIGNATURE_STATUS }`

Nom d'affichage : État de l'antispyware

- **Élément Web :** `ANTI_SPYWARE_STATUS`
- **Macros :** `${ device.ANTI_SPYWARE_STATUS }`

Nom d'affichage : État de la signature de l'antivirus

- **Élément Web :** `ANTI_VIRUS_SIGNATURE_STATUS`
- **Macros :** `${ device.ANTI_VIRUS_SIGNATURE_STATUS }`

Nom d'affichage : État de l'antivirus

- **Élément Web :** `ANTI_VIRUS_STATUS`
- **Macros :** `${ device.ANTI_VIRUS_STATUS }`

Nom d'affichage : code de contournement du verrouillage d'activation du programme de déploiement ASM

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `DEP_ACTIVATION_LOCK_BYPASS_CODE`
- **Macros :** `${ device.DEP_ACTIVATION_LOCK_BYPASS_CODE }`

Nom d'affichage : dépôt de clé du programme de déploiement ASM

- **Élément Web :** `DEP_ESCROW_KEY`
- **Macros :** `${ device.DEP_ESCROW_KEY }`

Nom d'affichage : Numéro d'identification

- **Élément Web :** `ASSET_TAG`
- **Macros :** `${ device.ASSET_TAG }`

Nom d'affichage : Rechercher automatiquement les mises à jour logicielles

- **Élément Web :** `AutoCheckEnabled`
- **Macros :** `${ device.AutoCheckEnabled }`

Nom d'affichage : Télécharger automatiquement les mises à jour logicielles en arrière-plan

- **Élément Web :** `BackgroundDownloadEnabled`
- **Macros :** `${ device.BackgroundDownloadEnabled }`

Nom d'affichage : Installer automatiquement les mises à jour applicatives

- **Élément Web :** `AutomaticAppInstallationEnabled`
- **Macros :** `${ device.AutomaticAppInstallationEnabled }`

Nom d'affichage : Installer automatiquement les mises à jour d'OS

- **Élément Web :** `AutomaticOSInstallationEnabled`
- **Macros :** `${ device.AutomaticOSInstallationEnabled }`

Nom d'affichage : Installer automatiquement les mises à jour de sécurité

- **Élément Web :** `AutomaticSecurityUpdatesEnabled`
- **Macros :** `${ device.AutomaticSecurityUpdatesEnabled }`

Nom d'affichage : État de la mise à jour automatique

- **Élément Web :** `AUTOUPDATE_STATUS`
- **Macros :** `${ device.AUTOUPDATE_STATUS }`

Nom d'affichage : RAM disponible

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `MEMORY_AVAILABLE`
- **Macros :** `${ device.MEMORY_AVAILABLE }`

Nom d'affichage : Mises à jour logicielles disponibles

- **Élément Web :** `AVAILABLE_OS_UPDATE_HUMAN_READABLE`
- **Macros :** `${ device.AVAILABLE_OS_UPDATE_HUMAN_READABLE }`

Nom d'affichage : Espace de stockage disponible

- **Élément Web :** `FREEDISK`
- **Macros :** `${ device.FREEDISK }`

Nom d'affichage : Batterie de secours

- **Élément Web :** `BACKUP_BATTERY_PERCENT`
- **Macros :** `${ device.BACKUP_BATTERY_PERCENT }`

Nom d'affichage : Version du firmware radio

- **Élément Web :** `MODEM_FIRMWARE_VERSION`
- **Macros :** '${device.MODEM_FIRMWARE_VERSION}

Nom d'affichage : Batterie en charge

- **Élément Web :** `BATTERY_CHARGING_STATUS`
- **Macros :** `${ device.BATTERY_CHARGING_STATUS }`

Nom d'affichage : Batterie en charge

- **Élément Web :** `BATTERY_CHARGING`
- **Macros :** `${ device.BATTERY_CHARGING }`

Nom d'affichage : Batterie restante

- **Élément Web :** `BATTERY_ESTIMATED_CHARGE_REMAINING`
- **Macros :** `${ device.BATTERY_ESTIMATED_CHARGE_REMAINING }`

Nom d'affichage : Autonomie de la batterie

- **Élément Web :** `BATTERY_RUNTIME`
- **Macros :** `${ device.BATTERY_RUNTIME }`

Nom d'affichage : État de la batterie

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `BATTERY_STATUS`
- **Macros :** `${ device.BATTERY_STATUS }`

Nom d'affichage : Code PIN BES

- **Élément Web :** `BES_PIN`
- **Macros :** `${ device.BES_PIN }`

Nom d'affichage : ID de l'agent du serveur BES

- **Élément Web :** `AGENT_ID`
- **Macros :** `${ device.AGENT_ID }`

Nom d'affichage : Nom du serveur BES

- **Élément Web :** `BES_SERVER`
- **Macros :** `${ device.BES_SERVER }`

Nom d'affichage : Version du serveur BES

- **Élément Web :** `BES_VERSION`
- **Macros :** `${ device.BES_VERSION }`

Nom d'affichage : Infos du BIOS

- **Élément Web :** `BIOS_INFO`
- **Macros :** `${ device.BIOS_INFO }`

Nom d'affichage : État de BitLocker

- **Élément Web :** `WINDOWS_HAS_BIT_LOCKER_STATUS`
- **Macros :** `${ device.WINDOWS_HAS_BIT_LOCKER_STATUS }`

Nom d'affichage : Adresse MAC Bluetooth

- **Élément Web :** `BLUETOOTH_MAC`
- **Macros :** `${ device.BLUETOOTH_MAC }`

Nom d'affichage : Débogage du démarrage activé ?

- **Élément Web :** `WINDOWS_HAS_BOOT_DEBUGGING_ENABLED`
- **Macros :** `${ device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED }`

Nom d'affichage : Version de la liste de révision du Gestionnaire de démarrage

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION`
- **Macros :** `${ device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION }`

Nom d'affichage : Code de l'opérateur

- **Élément Web :** `CARRIER_CODE`
- **Macros :** `${ device.CARRIER_CODE }`

Nom d'affichage : Version des paramètres opérateur

- **Élément Web :** `CARRIER_SETTINGS_VERSION`
- **Macros :** `${ device.CARRIER_SETTINGS_VERSION }`

Nom d'affichage : URL du catalogue

- **Élément Web :** `CatalogURL`
- **Macros :** `${ device.CatalogURL }`

Nom d'affichage : Altitude cellulaire

- **Élément Web :** `GPS_ALTITUDE_FROM_CELLULAR`
- **Macros :** `${ device.GPS_ALTITUDE_FROM_CELLULAR }`

nom d'affichage : Parcours cellulaire

- **Élément Web :** `GPS_COURSE_FROM_CELLULAR`
- **Macros :** `${ device.GPS_COURSE_FROM_CELLULAR }`

Nom d'affichage : Précision horizontale cellulaire

- **Élément Web :** `GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR`
- **Macros :** `${ device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR }`

Nom d'affichage : Cellulaire - Latitude

- **Élément Web :** `GPS_LATITUDE_FROM_CELLULAR`
- **Macros :** `${ device.GPS_LATITUDE_FROM_CELLULAR }`

Nom d'affichage : Cellulaire - Longitude

- **Élément Web :** `GPS_LONGITUDE_FROM_CELLULAR`
- **Macros :** `${ device.GPS_LONGITUDE_FROM_CELLULAR }`

Nom d'affichage : Vitesse cellulaire

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `GPS_SPEED_FROM_CELLULAR`
- **Macros :** `${ device.GPS_SPEED_FROM_CELLULAR }`

Nom d'affichage : Technologie cellulaire

- **Élément Web :** `CELLULAR_TECHNOLOGY`
- **Macros :** `${ device.CELLULAR_TECHNOLOGY }`

Nom d'affichage : Cellulaire - Horodatage

- **Élément Web :** `GPS_TIMESTAMP_FROM_CELLULAR`
- **Macros :** `${ device.GPS_TIMESTAMP_FROM_CELLULAR }`

Nom d'affichage : Précision verticale cellulaire

- **Élément Web :** `GPS_VERTICAL_ACCURACY_FROM_CELLULAR`
- **Macros :** `${ device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR }`

Nom d'affichage : Changer le mot de passe lors de la prochaine connexion ?

- **Élément Web :** `GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN`
- **Macros :** '${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

Nom d'affichage : ID de l'appareil client

- **Élément Web :** `CLIENT_DEVICE_ID`
- **Macros :** `${ device.CLIENT_DEVICE_ID }`

Nom d'affichage : Sauvegarde sur cloud activée

- **Élément Web :** `CLOUD_BACKUP_ENABLED`
- **Macros :** `${ device.CLOUD_BACKUP_ENABLED }`

Nom d'affichage : Intégrité du code activée ?

- **Élément Web :** `WINDOWS_HAS_CODE_INTEGRITY_ENABLED`
- **Macros :** `${ device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED }`

Nom d'affichage : Version de la liste de révision d'intégrité du code

- **Élément Web :** `WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION`
- **Macros :** `${ device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION }`

Nom d'affichage : Couleur

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `COLOR`
- **Macros :** `${ device.COLOR }`

Nom d'affichage : Fréquence du processeur

- **Élément Web :** `CPU_CLOCK_SPEED`
- **Macros :** `${ device.CPU_CLOCK_SPEED }`

Nom d'affichage : Type de processeur

- **Élément Web :** `CPU_TYPE`
- **Macros :** `${ device.CPU_TYPE }`

Nom d'affichage : Heure de création

- **Élément Web :** `GOOGLE_AW_DIRECTORY_CREATION_TIME`
- **Macros :** `${ device.GOOGLE_AW_DIRECTORY_CREATION_TIME }`

Nom d'affichage : Mises à jour logicielles critiques

- **Élément Web :** `AVAILABLE_OS_UPDATE_IS_CRITICAL`
- **Macros :** `${ device.AVAILABLE_OS_UPDATE_IS_CRITICAL }`

Nom d'affichage : Réseau opérateur courant

- **Élément Web :** `CARRIER`
- **Macros :** `${ device.CARRIER }`

Nom d'affichage : Code pays du mobile actuel

- **Élément Web :** `CURRENT_MCC`
- **Macros :** `${ device.CURRENT_MCC }`

Nom d'affichage : Code réseau du mobile actuel

- **Élément Web :** `CURRENT_MNC`
- **Macros :** `${ device.CURRENT_MNC }`

Nom d'affichage : Itinérance des données autorisée

- **Élément Web :** `DATA_ROAMING_ENABLED`
- **Macros :** `${ device.DATA_ROAMING_ENABLED }`

Nom d'affichage : date de la dernière sauvegarde iCloud

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `LAST_CLOUD_BACKUP_DATE`
- **Macros :** `${ device.LAST_CLOUD_BACKUP_DATE }`

Nom d'affichage : Catalogue par défaut

- **Élément Web :** `IsDefaultCatalog`
- **Macros :** `${ device.IsDefaultCatalog }`

Nom d'affichage : nom du compte du programme de déploiement Apple

- **Élément Web :** `BULK_ENROLLMENT_DEP_ACCOUNT_NAME`
- **Macros :** `${ device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME }`

Nom d'affichage : stratégie du programme de déploiement Apple

- **Élément Web :** `WINDOWS_HAS_DEP_POLICY`
- **Macros :** `${ device.WINDOWS_HAS_DEP_POLICY }`

Nom d'affichage : profil du programme de déploiement Apple attribué

- **Élément Web :** `PROFILE_ASSIGN_TIME`
- **Macros :** `${ device.PROFILE_ASSIGN_TIME }`

Nom d'affichage : profil du programme de déploiement Apple transmis

- **Élément Web :** `PROFILE_PUSH_TIME`
- **Macros :** `${ device.PROFILE_PUSH_TIME }`

Nom d'affichage : profil du compte du programme de déploiement Apple supprimé

- **Élément Web :** `PROFILE_REMOVE_TIME`
- **Macros :** `${ device.PROFILE_REMOVE_TIME }`

Nom d'affichage : compte qui s'est inscrit au programme de déploiement Apple

- **Élément Web :** `DEVICE_ASSIGNED_BY`
- **Macros :** `${ device.DEVICE_ASSIGNED_BY }`

Nom d'affichage : date d'inscription au programme de déploiement Apple

- **Élément Web :** `DEVICE_ASSIGNED_DATE`
- **Macros :** `${ device.DEVICE_ASSIGNED_DATE }`

Nom d'affichage : Description

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `DESCRIPTION`
- **Macros :** `${ device.DESCRIPTION }`

Nom d'affichage : Modèle d'appareil

- **Élément Web :** `SYSTEM_OEM`
- **Macros :** `${ device.SYSTEM_OEM }`

Nom d'affichage : Nom de l'appareil

- **Élément Web :** `DEVICE_NAME`
- **Macros :** `${ device.DEVICE_NAME }`

Nom d'affichage : Type d'appareil

- **Élément Web :** `DEVICE_TYPE`
- **Macros :** `${ device.DEVICE_TYPE }`

Nom d'affichage : Ne pas déranger activé

- **Élément Web :** `DO_NOT_DISTURB`
- **Macros :** `${ device.DO_NOT_DISTURB }`

Nom d'affichage : Pilote ELAM chargé ?

- **Élément Web :** `WINDOWS_HAS_ELAM_DRIVER_LOADED`
- **Macros :** `${ device.WINDOWS_HAS_ELAM_DRIVER_LOADED }`

Nom d'affichage : Conformité du chiffrement

- **Élément Web :** `ENCRYPTION_COMPLIANCE`
- **Macros :** `${ device.ENCRYPTION_COMPLIANCE }`

Nom d'affichage : ENROLLMENT_KEY_GENERATION_DATE

- **Élément Web :** `ENROLLMENT_KEY_GENERATION_DATE`
- **Macros :** `${ device.ENROLLMENT_KEY_GENERATION_DATE }`

Nom d'affichage : ID d'entreprise

- **Élément Web :** `ENTERPRISEID`
- **Macros :** `${ device.ENTERPRISEID }`

Nom d'affichage : Stockage externe 1 : espace disponible

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `EXTERNAL_STORAGE1_FREE_SPACE`
- **Macros :** `${ device.EXTERNAL_STORAGE1_FREE_SPACE }`

Nom d'affichage : Stockage externe 1 : espace disponible

- **Élément Web :** `EXTERNAL_STORAGE1_FREE_SPACE`
- **Macros :** `${ device.EXTERNAL_STORAGE1_FREE_SPACE }`

Nom d'affichage : Stockage externe 1 : nom

- **Élément Web :** `EXTERNAL_STORAGE1_NAME`
- **Macros :** `${ device.EXTERNAL_STORAGE1_NAME }`

Nom d'affichage : Stockage externe 1 : espace total

- **Élément Web :** `EXTERNAL_STORAGE1_TOTAL_SPACE`
- **Macros :** `${ device.EXTERNAL_STORAGE1_TOTAL_SPACE }`

Nom d'affichage : Stockage externe 2 : espace disponible

- **Élément Web :** `EXTERNAL_STORAGE2_FREE_SPACE`
- **Macros :** `${ device.EXTERNAL_STORAGE2_FREE_SPACE }`

Nom d'affichage : Stockage externe 2 : nom

- **Élément Web :** `EXTERNAL_STORAGE2_NAME`
- **Macros :** `${ device.EXTERNAL_STORAGE2_NAME }`

Nom d'affichage : Stockage externe 2 : espace total

- **Élément Web :** `EXTERNAL_STORAGE2_TOTAL_SPACE`
- **Macros :** `${ device.EXTERNAL_STORAGE2_TOTAL_SPACE }`

Nom d'affichage : Stockage externe chiffré

- **Élément Web :** `EXTERNAL_ENCRYPTION`
- **Macros :** `${ device.EXTERNAL_ENCRYPTION }`

Nom d'affichage : FileVault activé

- **Élément Web :** `IS_FILEVAULT_ENABLED`
- **Macros :** `${ device.IS_FILEVAULT_ENABLED }`

Nom d'affichage : État du pare-feu

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `DEVICE_FIREWALL_STATUS`
- **Macros :** `${ device.DEVICE_FIREWALL_STATUS }`

Nom d'affichage : État du pare-feu

- **Élément Web :** `DEVICE_FIREWALL_STATUS`
- **Macros :** `${ device.DEVICE_FIREWALL_STATUS }`

Nom d'affichage : État du pare-feu

- **Élément Web :** `FIREWALL_STATUS`
- **Macros :** `${ device.FIREWALL_STATUS }`

Nom d'affichage : Version du firmware

- **Élément Web :** `FIRMWARE_VERSION`
- **Macros :** `${ device.FIRMWARE_VERSION }`

Nom d'affichage : Première synchronisation

- **Élément Web :** `ZMSP_FIRST_SYNC`
- **Macros :** `${ device.ZMSP_FIRST_SYNC }`

Nom d'affichage : Alias Google Directory

- **Élément Web :** `GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS`
- **Macros :** `${ device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS }`

Nom d'affichage : Nom de famille Google Directory

- **Élément Web :** `GOOGLE_AW_DIRECTORY_FAMILY_NAME`
- **Macros :** `${ device.GOOGLE_AW_DIRECTORY_FAMILY_NAME }`

Nom d'affichage : Nom Google Directory

- **Élément Web :** `GOOGLE_AW_DIRECTORY_NAME`
- **Macros :** `${ device.GOOGLE_AW_DIRECTORY_NAME }`

Nom d'affichage : E-mail principal Google Directory

- **Élément Web :** `GOOGLE_AW_DIRECTORY_PRIMARY`
- **Macros :** `${ device.GOOGLE_AW_DIRECTORY_PRIMARY }`

Nom d'affichage : ID utilisateur Google Directory

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `GOOGLE_AW_DIRECTORY_USER_ID`
- **Macros :** `${ device.GOOGLE_AW_DIRECTORY_USER_ID }`

Nom d'affichage : GPS - Altitude

- **Élément Web :** `GPS_ALTITUDE_FROM_GPS`
- **Macros :** `${ device.GPS_ALTITUDE_FROM_GPS }`

Nom d'affichage : Parcours GPS

- **Élément Web :** `GPS_COURSE_FROM_GPS`
- **Macros :** `${ device.GPS_COURSE_FROM_GPS }`

Nom d'affichage : Précision horizontale GPS

- **Élément Web :** `GPS_HORIZONTAL_ACCURACY_FROM_GPS`
- **Macros :** `${ device.GPS_HORIZONTAL_ACCURACY_FROM_GPS }`

Nom d'affichage : GPS - Latitude

- **Élément Web :** `GPS_LATITUDE_FROM_GPS`
- **Macros :** `${ device.GPS_LATITUDE_FROM_GPS }`

Nom d'affichage : GPS - Longitude

- **Élément Web :** `GPS_LONGITUDE_FROM_GPS`
- **Macros :** `${ device.GPS_LONGITUDE_FROM_GPS }`

Nom d'affichage : Vitesse GPS

- **Élément Web :** `GPS_SPEED_FROM_GPS`
- **Macros :** `${ device.GPS_SPEED_FROM_GPS }`

Nom d'affichage : GPS - Horodatage

- **Élément Web :** `GPS_TIMESTAMP_FROM_GPS`
- **Macros :** `${ device.GPS_TIMESTAMP_FROM_GPS }`

Nom d'affichage : Précision verticale GPS

- **Élément Web :** `GPS_VERTICAL_ACCURACY_FROM_GPS`
- **Macros :** `${ device.GPS_VERTICAL_ACCURACY_FROM_GPS }`

Nom d'affichage : ID du périphérique matériel

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `HW_DEVICE_ID`
- **Macros :** `${ device.HW_DEVICE_ID }`

Nom d'affichage : Capacités de chiffrement du matériel

- **Élément Web :** `HARDWARE_ENCRYPTION_CAPS`
- **Macros :** `${ device.HARDWARE_ENCRYPTION_CAPS }`

Nom d'affichage : HAS_CONTAINER

- **Élément Web :** `HAS_CONTAINER`
- **Macros :** `${ device.HAS_CONTAINER }`

Nom d'affichage : Hash du compte Apple App Store actuellement connecté

- **Élément Web :** `ITUNES_STORE_ACCOUNT_HASH`
- **Macros :** `${ device.ITUNES_STORE_ACCOUNT_HASH }`

Nom d'affichage : Opérateur de la carte SIM

- **Élément Web :** `SIM_CARRIER_NETWORK`
- **Macros :** `${ device.SIM_CARRIER_NETWORK }`

Nom d'affichage : Code pays de la carte SIM

- **Élément Web :** `SIM_MCC`
- **Macros :** `${ device.SIM_MCC }`

Nom d'affichage : Code réseau de la carte SIM

- **Élément Web :** `SIM_MNC`
- **Macros :** `${ device.SIM_MNC }`

Nom d'affichage : ICCID

- **Élément Web :** `ICCID`
- **Macros :** `${ device.ICCID }`

Nom d'affichage : Identité

- **Élément Web :** `AS_DEVICE_IDENTITY`
- **Macros :** `${ device.AS_DEVICE_IDENTITY }`

Nom d'affichage : Numéro IMEI/MEID de l'appareil

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `IMEI`
- **Macros :** `${ device.IMEI }`

Nom d'affichage : IMSI

- **Élément Web :** `SIM_ID`
- **Macros :** `${ device.SIM_ID }`

Nom d'affichage : Stockage interne chiffré

- **Élément Web :** `LOCAL_ENCRYPTION`
- **Macros :** `${ device.LOCAL_ENCRYPTION }`

Nom d'affichage : Adresse IP

- **Élément Web :** `IP_LOCATION`
- **Macros :** `${ device.IP_LOCATION }`

Nom d'affichage : Adresse IPV4

- **Élément Web :** `IP_ADDRESSV4`
- **Macros :** `${ device.IP_ADDRESSV4 }`

Nom d'affichage : Adresse IPV6

- **Élément Web :** `IP_ADDRESSV6`
- **Macros :** `${ device.IP_ADDRESSV6 }`

Nom d'affichage : Délivré à

- **Élément Web :** `WINDOWS_HAS_ISSUED_AT`
- **Macros :** `${ device.WINDOWS_HAS_ISSUED_AT }`

Nom d'affichage : Jailbreaké/rooté

- **Élément Web :** `ROOT_ACCESS`
- **Macros :** `${ device.ROOT_ACCESS }`

Nom d'affichage : Débogage du noyau activé ?

- **Élément Web :** `WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED`
- **Macros :** `${ device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED }`

Nom d'affichage : Mode kiosque

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `IS_KIOSK`
- **Macros :** `${ device.IS_KIOSK }`

Nom d'affichage : Dernière adresse IP connue

- **Élément Web :** `LAST_IP_ADDR`
- **Macros :** `${ device.LAST_IP_ADDR }`

Nom d'affichage : Dernière date de mise à jour de la stratégie

- **Élément Web :** `LAST_POLICY_UPDATE_TIME`
- **Macros :** `${ device.LAST_POLICY_UPDATE_TIME }`

Nom d'affichage : Date dernière recherche

- **Élément Web :** `PreviousScanDate`
- **Macros :** `${ device.PreviousScanDate }`

Nom d'affichage : Résultat dernière recherche

- **Élément Web :** `PreviousScanResult`
- **Macros :** `${ device.PreviousScanResult }`

Nom d'affichage : Dernières mises à jour logicielles planifiées

- **Élément Web :** `AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME`
- **Macros :** `${ device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME }`

Nom d'affichage : Dernier message d'échec des mises à jour logicielles planifiées

- **Élément Web :** `AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG`
- **Macros :** `${ device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG }`

Nom d'affichage : Dernier état des mises à jour logicielles planifiées

- **Élément Web :** `AVAILABLE_OS_UPDATE_INSTALL_STATUS`
- **Macros :** `${ device.AVAILABLE_OS_UPDATE_INSTALL_STATUS }`

Nom d'affichage : Dernière synchronisation

- **Élément Web :** `ZMSP_LAST_SYNC`
- **Macros :** `${ device.ZMSP_LAST_SYNC }`

Nom d'affichage : Service de localisation activé

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `DEVICE_LOCATOR`
- **Macros :** `${ device.DEVICE_LOCATOR }`

Nom d'affichage : Adresse MAC

- **Élément Web :** `MAC_ADDRESS`
- **Macros :** `${ device.MAC_ADDRESS }`

Nom d'affichage : Connexion réseau de l'adresse MAC

- **Élément Web :** `MAC_NETWORK_CONNECTION`
- **Macros :** `${ device.MAC_NETWORK_CONNECTION }`

Nom d'affichage : Type d'adresse MAC

- **Élément Web :** `MAC_ADDRESS_TYPE`
- **Macros :** `${ device.MAC_ADDRESS_TYPE }`

Nom d'affichage : Configuration de la boîte aux lettres

- **Élément Web :** `GOOGLE_AW_DIRECTORY_MAILBOX_SETUP`
- **Macros :** `${ device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP }`

Nom d'affichage : Batterie principale

- **Élément Web :** `MAIN_BATTERY_PERCENT`
- **Macros :** `${ device.MAIN_BATTERY_PERCENT }`

Nom d'affichage : Mode perdu MDM activé

- **Élément Web :** `IS_MDM_LOST_MODE_ENABLED`
- **Macros :** `${ device.IS_MDM_LOST_MODE_ENABLED }`

Nom d'affichage : MDX_SHARED_ENCRYPTION_KEY

- **Élément Web :** `MDX_SHARED_ENCRYPTION_KEY`
- **Macros :** `${ device.MDX_SHARED_ENCRYPTION_KEY }`

Nom d'affichage : MEID

- **Élément Web :** `MEID`
- **Macros :** `${ device.MEID }`

Nom d'affichage : Numéro de mobile

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `TEL_NUMBER`
- **Macros :** `${ device.TEL_NUMBER }`

Nom d'affichage : ID du modèle

- **Élément Web :** `MODEL_ID`
- **Macros :** `${ device.MODEL_ID }`

Nom d'affichage : Numéro de modèle

- **Élément Web :** `MODEL_NUMBER`
- **Macros :** `${ device.MODEL_NUMBER }`

Nom d'affichage : Type de carte réseau

- **Élément Web :** `NETWORK_ADAPTER_TYPE`
- **Macros :** `${ device.NETWORK_ADAPTER_TYPE }`

Nom d'affichage : Build du système d'exploitation

- **Élément Web :** `SYSTEM_OS_BUILD`
- **Macros :** `${ device.SYSTEM_OS_BUILD }`

Nom d'affichage : Édition du système d'exploitation

- **Élément Web :** `OS_EDITION`
- **Macros :** `${ device.OS_EDITION }`

Nom d'affichage : Langue du système d'exploitation (paramètres régionaux)

- **Élément Web :** `SYSTEM_LANGUAGE`
- **Macros :** `${ device.SYSTEM_LANGUAGE }`

Nom d'affichage : Version du système d'exploitation

- **Élément Web :** `SYSTEM_OS_VERSION`
- **Macros :** `${ device.SYSTEM_OS_VERSION }`

Nom d'affichage : Adresse de l'organisation

- **Élément Web :** `ORGANIZATION_ADDRESS`
- **Macros :** `${ device.ORGANIZATION_ADDRESS }`

Nom d'affichage : E-mail de l'organisation

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `ORGANIZATION_EMAIL`
- **Macros :** `${ device.ORGANIZATION_EMAIL }`

Nom d'affichage : Organisation Magic

- **Élément Web :** `ORGANIZATION_MAGIC`
- **Macros :** `${ device.ORGANIZATION_MAGIC }`

Nom d'affichage : Nom de l'organisation

- **Élément Web :** `ORGANIZATION_NAME`
- **Macros :** `${ device.ORGANIZATION_NAME }`

Nom d'affichage : N° de tél. de l'organisation

- **Élément Web :** `ORGANIZATION_PHONE`
- **Macros :** `${ device.ORGANIZATION_PHONE }`

Nom d'affichage : Non conforme

- **Élément Web :** `OUT_OF_COMPLIANCE`
- **Macros :** `${ device.OUT_OF_COMPLIANCE }`

Nom d'affichage : Appartient à

- **Élément Web :** `CORPORATE_OWNED`
- **Macros :** `${ device.CORPORATE_OWNED }`

Nom d'affichage : Code secret conforme

- **Élément Web :** `PASSCODE_IS_COMPLIANT`
- **Macros :** `${ device.PASSCODE_IS_COMPLIANT }`

Nom d'affichage : Code secret conforme à la configuration

- **Élément Web :** `PASSCODE_IS_COMPLIANT_WITH_CFG`
- **Macros :** `${ device.PASSCODE_IS_COMPLIANT_WITH_CFG }`

Nom d'affichage : Code secret présent

- **Élément Web :** `PASSCODE_PRESENT`
- **Macros :** `${ device.PASSCODE_PRESENT }`

Nom d'affichage : PCR0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `WINDOWS_HAS_PCR0`
- **Macros :** `${ device.WINDOWS_HAS_PCR0 }`

Nom d'affichage : Violation du périmètre

- **Élément Web :** `GPS_PERIMETER_BREACH`
- **Macros :** `${ device.GPS_PERIMETER_BREACH }`

Nom d'affichage : Recherche périodique

- **Élément Web :** `PerformPeriodicCheck`
- **Macros :** `${ device.PerformPeriodicCheck }`

Nom d'affichage : Personal Hotspot activé

- **Élément Web :** `PERSONAL_HOTSPOT_ENABLED`
- **Macros :** `${ device.PERSONAL_HOTSPOT_ENABLED }`

Nom d'affichage : Code PIN du géofencing

- **Élément Web :** `PIN_CODE_FOR_GEO_FENCE`
- **Macros :** `${ device.PIN_CODE_FOR_GEO_FENCE }`

Nom d'affichage : Plate-forme

- **Élément Web :** `SYSTEM_PLATFORM`
- **Macros :** `${ device.SYSTEM_PLATFORM }`

Nom d'affichage : Niveau d'API de la plate-forme

- **Élément Web :** `API_LEVEL`
- **Macros :** `${ device.API_LEVEL }`

Nom d'affichage : Nom de stratégie

- **Élément Web :** `POLICY_NAME`
- **Macros :** `${ device.POLICY_NAME }`

Nom d'affichage : Numéro de téléphone principal

- **Élément Web :** `IDENTITY1_PHONENUMBER`
- **Macros :** `${ device.IDENTITY1_PHONENUMBER }`

Nom d'affichage : Opérateur de la carte SIM principale

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `IDENTITY1_CARRIER_NETWORK_OPERATOR`
- **Macros :** `${ device.IDENTITY1_CARRIER_NETWORK_OPERATOR }`

Nom d'affichage : ICCID de la carte SIM principale

- **Élément Web :** `IDENTITY1_ICCID`
- **Macros :** `${ device.IDENTITY1_ICCID }`

Nom d'affichage : N° IMEI de la carte SIM principale

- **Élément Web :** `IDENTITY1_IMEI`
- **Macros :** `${ device.IDENTITY1_IMEI }`

Nom d'affichage : N° IMSI de la carte SIM principale

- **Élément Web :** `IDENTITY1_IMSI`
- **Macros :** `${ device.IDENTITY1_IMSI }`

Nom d'affichage : Itinérance de la carte SIM principale

- **Élément Web :** `IDENTITY1_ROAMING`
- **Macros :** `${ device.IDENTITY1_ROAMING }`

Nom d'affichage : Itinérance de la carte SIM principale

- **Élément Web :** `IDENTITY1_ROAMING_COMPLIANCE`
- **Macros :** `${ device.IDENTITY1_ROAMING_COMPLIANCE }`

Nom d'affichage : Nom du produit

- **Élément Web :** `PRODUCT_NAME`
- **Macros :** `${ device.PRODUCT_NAME }`

Nom d'affichage : ID d'éditeur de l'appareil

- **Élément Web :** `PUBLISHER_DEVICE_ID`
- **Macros :** `${ device.PUBLISHER_DEVICE_ID }`

Nom d'affichage : Nombre de réinitialisations

- **Élément Web :** `WINDOWS_HAS_RESET_COUNT`
- **Macros :** `${ device.WINDOWS_HAS_RESET_COUNT }`

Nom d'affichage : Nombre de redémarrages

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `WINDOWS_HAS_RESTART_COUNT`
- **Macros :** `${ device.WINDOWS_HAS_RESTART_COUNT }`

Nom d'affichage : Mode sans échec activé ?

- **Élément Web :** `WINDOWS_HAS_SAFE_MODE`
- **Macros :** `${ device.WINDOWS_HAS_SAFE_MODE }`

Nom d'affichage : Hachage SBCP

- **Élément Web :** `WINDOWS_HAS_SBCP_HASH`
- **Macros :** `${ device.WINDOWS_HAS_SBCP_HASH }`

Nom d'affichage : Écran : hauteur

- **Élément Web :** `SCREEN_HEIGHT`
- **Macros :** `${ device.SCREEN_HEIGHT }`

Nom d'affichage : Écran : nombre de couleurs

- **Élément Web :** `SCREEN_NB_COLORS`
- **Macros :** `${ device.SCREEN_NB_COLORS }`

Nom d'affichage : Écran : taille

- **Élément Web :** `SCREEN_SIZE`
- **Macros :** `${ device.SCREEN_SIZE }`

Nom d'affichage : Écran : largeur

- **Élément Web :** `SCREEN_WIDTH`
- **Macros :** `${ device.SCREEN_WIDTH }`

Nom d'affichage : Écran : résolution axe X

- **Élément Web :** `SCREEN_XDPI`
- **Macros :** `${ device.SCREEN_XDPI }`

Nom d'affichage : Écran : résolution axe Y

- **Élément Web :** `SCREEN_YDPI`
- **Macros :** `${ device.SCREEN_YDPI }`

Nom d'affichage : Numéro de téléphone secondaire

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `IDENTITY2_PHONENUMBER`
- **Macros :** `${ device.IDENTITY2_PHONENUMBER }`

Nom d'affichage : Opérateur de la carte SIM secondaire

- **Élément Web :** `IDENTITY2_CARRIER_NETWORK_OPERATOR`
- **Macros :** `${ device.IDENTITY2_CARRIER_NETWORK_OPERATOR }`

Nom d'affichage : ICCID de la carte SIM secondaire

- **Élément Web :** `IDENTITY2_ICCID`
- **Macros :** `${ device.IDENTITY2_ICCID }`

Nom d'affichage : N° IMEI de la carte SIM secondaire

- **Élément Web :** `IDENTITY2_IMEI`
- **Macros :** `${ device.IDENTITY2_IMEI }`

Nom d'affichage : N° IMSI de la carte SIM secondaire

- **Élément Web :** `IDENTITY2_IMSI`
- **Macros :** `${ device.IDENTITY2_IMSI }`

Nom d'affichage : Itinérance de la carte SIM secondaire

- **Élément Web :** `IDENTITY2_ROAMING`
- **Macros :** `${ device.IDENTITY2_ROAMING }`

Nom d'affichage : Conformité de la carte SIM secondaire avec l'itinérance

- **Élément Web :** `IDENTITY2_ROAMING_COMPLIANCE`
- **Macros :** `${ device.IDENTITY2_ROAMING_COMPLIANCE }`

Nom d'affichage : Démarrage sécurisé activé ?

- **Élément Web :** `WINDOWS_HAS_SECURE_BOOT_ENABLED`
- **Macros :** `${ device.WINDOWS_HAS_SECURE_BOOT_ENABLED }`

Nom d'affichage : État du démarrage sécurisé

- **Élément Web :** `SECURE_BOOT_STATE`
- **Macros :** `${ device.SECURE_BOOT_STATE }`

Nom d'affichage : Conteneur sécurisé activé

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `DLP_ACTIVE`
- **Macros :** `${ device.DLP_ACTIVE }`

Nom d'affichage : Niveau de correctif de sécurité

- **Élément Web :** `SYSTEM_SECURITY_PATCH_LEVEL`
- **Macros :** `${ device.SYSTEM_SECURITY_PATCH_LEVEL }`

Nom d'affichage : Numéro de série

- **Élément Web :** `SERIAL_NUMBER`
- **Macros :** `${ device.SERIAL_NUMBER }`

Nom d'affichage : Prise en charge des SMS

- **Élément Web :** `IS_SMS_CAPABLE`
- **Macros :** `${ device.IS_SMS_CAPABLE }`

Nom d'affichage : Supervisé

- **Élément Web :** `SUPERVISED`
- **Macros :** `${ device.SUPERVISED }`

Nom d'affichage : Motif de la suspension

- **Élément Web :** `GOOGLE_AW_DIRECTORY_SUSPENTION_REASON`
- **Macros :** `${ device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON }`

Nom d'affichage : État altéré

- **Élément Web :** `TAMPERED_STATUS`
- **Macros :** `${ device.TAMPERED_STATUS }`

Nom d'affichage : Termes et conditions

- **Élément Web :** `TERMS_AND_CONDITIONS`
- **Macros :** `${ device.TERMS_AND_CONDITIONS }`

Nom d'affichage : Termes et conditions acceptés ?

- **Élément Web :** `GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS`
- **Macros :** `${ device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS }`

Nom d'affichage : Signature du test activée ?

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `WINDOWS_HAS_TEST_SIGNING_ENABLED`
- **Macros :** `${ device.WINDOWS_HAS_TEST_SIGNING_ENABLED }`

Nom d'affichage : RAM totale

- **Élément Web :** `MEMORY`
- **Macros :** `${ device.MEMORY }`

Nom d'affichage : Espace de stockage total

- **Élément Web :** `TOTAL_DISK_SPACE`
- **Macros :** `${ device.TOTAL_DISK_SPACE }`

Nom d'affichage : Version du TPM

- **Élément Web :** `TPM_VERSION`
- **Macros :** `${ device.TPM_VERSION }`

Nom d'affichage : UDID

- **Élément Web :** `UDID`
- **Macros :** `${ device.UDID }`

Nom d'affichage : État du contrôle de compte d'utilisateur

- **Élément Web :** `UAC_STATUS`
- **Macros :** `${ device.UAC_STATUS }`

Nom d'affichage : Agent utilisateur

- **Élément Web :** `USER_AGENT`
- **Macros :** `${ device.USER_AGENT }`

Nom d'affichage : Défini par l'utilisateur #1

- **Élément Web :** `USER_DEFINED_1`
- **Macros :** `${ device.USER_DEFINED_1 }`

Nom d'affichage : Défini par l'utilisateur #2

- **Élément Web :** `USER_DEFINED_2`
- **Macros :** `${ device.USER_DEFINED_2 }`

Nom d'affichage : Défini par l'utilisateur #3

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `USER_DEFINED_3`
- **Macros :** `${ device.USER_DEFINED_3 }`

Nom d'affichage : Langue de l'utilisateur (locale)

- **Élément Web :** `USER_LANGUAGE`
- **Macros :** `${ device.USER_LANGUAGE }`

Nom d'affichage : Fournisseur

- **Élément Web :** `VENDOR`
- **Macros :** `${ device.VENDOR }`

Nom d'affichage : Prise en charge de la voix

- **Élément Web :** `IS_VOICE_CAPABLE`
- **Macros :** `${ device.IS_VOICE_CAPABLE }`

Nom d'affichage : Itinérance voix autorisée

- **Élément Web :** `VOICE_ROAMING_ENABLED`
- **Macros :** `${ device.VOICE_ROAMING_ENABLED }`

Nom d'affichage : VSM activé ?

- **Élément Web :** `WINDOWS_HAS_VSM_ENABLED`
- **Macros :** `${ device.WINDOWS_HAS_VSM_ENABLED }`

Nom d'affichage : Adresse MAC Wi-Fi

- **Élément Web :** `WIFI_MAC`
- **Macros :** `${ device.WIFI_MAC }`

Nom d'affichage : WINDOWS_ENROLLMENT_KEY

- **Élément Web :** `WINDOWS_ENROLLMENT_KEY`
- **Macros :** `${ device.WINDOWS_ENROLLMENT_KEY }`

Nom d'affichage : WinPE activé ?

- **Élément Web :** `WINDOWS_HAS_WINPE`
- **Macros :** `${ device.WINDOWS_HAS_WINPE }`

Nom d'affichage : État de la notification WNS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Élément Web :** `PROPERTY_WNS_PUSH_STATUS`
- **Macros :** `${ device.PROPERTY_WNS_PUSH_STATUS }`

Nom d'affichage : URL de notification WNS

- **Élément Web :** `PROPERTY_WNS_PUSH_URL`
- **Macros :** `${ device.PROPERTY_WNS_PUSH_URL }`

Nom d'affichage : Date d'expiration de l'URL de notification WNS

- **Élément Web :** `PROPERTY_WNS_PUSH_URL_EXPIRY`
- **Macros :** `${ device.PROPERTY_WNS_PUSH_URL_EXPIRY }`

Nom d'affichage : ID d'agent de Citrix Endpoint Management

- **Élément Web :** `ENROLLMENT_AGENT_ID`
- **Macros :** {device.ENROLLMENT_AGENT_ID}

Nom d'affichage : Révision de l'agent de Citrix Endpoint Management

- **Élément Web :** `EW_REVISION`
- **Macros :** `${ device.EW_REVISION }`

Nom d'affichage : Version de l'agent de Citrix Endpoint Management

- **Élément Web :** `EW_VERSION`
- **Macros :** `${ device.EW_VERSION }`

Nom d'affichage : API Zebra disponible

- **Élément Web :** `ZEBRA_MDM`
- **Macros :** `${ device.ZEBRA_MDM }`

Nom d'affichage : Version du MXMF Zebra

- **Élément Web :** `ZEBRA_MDM_VERSION`
- **Macros :** `${ device.ZEBRA_MDM_VERSION }`

Nom d'affichage : Version du patch Zebra

- **Élément Web :** `ZEBRA_PATCH_VERSION`
- **Macros :** `${ device.ZEBRA_PATCH_VERSION }`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Macros pour obtenir des propriétés utilisateur intégrés

Nom d'affichage	Macros
domainname (nom de domaine, domaine par défaut)	${ user.domainname }
loginname (nom d'utilisateur + nom de domaine)	${ user.loginname }
username (nom d'ouverture de session moins le domaine, si présent)	${ user.username }

Macros pour toutes les propriétés utilisateur

Nom d'affichage	Élément Web	Macros
Échecs de connexion à Active Directory	badpwdcount	${ user.badpwdcount }
E-mail de l'utilisateur ActiveSync	asuseremail	${ user.asuseremail }
Source de données ASM	asmpersonsource	${ user.asmpersonsource }
Nom du compte du programme de déploiement ASM	asmdepaccount	${ user.asmdepaccount }
Identifiant Apple géré par ASM	asmpersonmanagedappleid	${ user.asmpersonmanagedappleid }
Type de code d'accès ASM	asmpersonpasscodetype	${ user.asmpersonpasscodetype }
Identifiant d'étudiant ASM	asmpersonid	${ user.asmpersonid }
Statut de l'étudiant ASM	asmpersonstatus	${ user.asmpersonstatus }
Titre de l'étudiant ASM	asmpersontitle	${ user.asmpersontitle }
Identifiant unique de l'étudiant ASM	asmpersonuniqueid	${ user.asmpersonuniqueid }

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom d'affichage	Élément Web	Macros
Identifiant du système source ASM	asmpersonsourcesystemid	${ user.asmpersonsourcesystemid }
Niveau scolaire de l'étudiant ASM	asmpersongrade	${ user.asmpersongrade }
E-mail de l'utilisateur BES	besuseremail	${ user.besuseremail }
Société	company	${ user.company }
Nom de la société	companyname	${ user.companyname }
Pays	c	${ user.c }
Service	department	${ user.department }
Description	description	${ user.description }
Utilisateur désactivé	disableduser	${ user.disableduser }
Nom d'affichage	displayname	${ user.displayname }
Nom unique	distinguishedname	${ user.distinguishedname }
Nom de domaine	domainname	${ user.domainname }
E-mail	mail	${ user.mail }
Prénom	givenname	${ user.givenname }
Adresse (domicile)	homestreetaddress	${ user.homestreetaddress }
Ville (domicile)	homecity	${ user.homecity }
Pays (domicile)	homecountry	${ user.homecountry }
Fax (domicile)	homefax	${ user.homefax }
Téléphone domicile	homephone	${ user.homephone }
Dép./Région (domicile)	homestate	${ user.homestate }
Code postal (domicile)	homezip	${ user.homezip }
Tél. IP	ipphone	${ user.ipphone }
Second prénom	middleinitial	${ user.middleinitial }

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom d'affichage	Élément Web	Macros
Deuxième prénom	middlename	${ user.middlename }
Téléphone portable	mobile	${ user.mobile }
Nom	cn	${ user.cn }
Adresse du bureau	physicaldeliveryofficename	${ user.physicaldeliveryofficename }
Ville (bureau)	l	${ user.l }
Fax du bureau	facsimiletelephonenumber	${ user.facsimiletelephonenumber }
Dép./Région du bureau	st	${ user.st }
Rue du bureau	officestreetaddress	${ user.officestreetaddress }
Tél. bureau	telephonenumber	${ user.telephonenumber }
Code postal du bureau	postalcode	${ user.postalcode }
Boîte postale	postofficebox	${ user.postofficebox }
Bipeur	pager	${ user.pager }
ID du groupe principal	primarygroupid	${ user.primarygroupid }
Compte SAM	samaccountname	${ user.samaccountname }
Adresse	streetaddress	${ user.streetaddress }
Surname	sn	${ user.sn }
Titre	title	${ user.title }
Nom de connexion de l'utilisateur	userprincipalname	${ user.userprincipalname }

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Actions automatisées

March 1, 2024

Vous créez des actions automatisées dans Citrix Endpoint Management pour programmer une réaction aux éléments suivants :

- Événements
- Propriétés de l'utilisateur ou de l'appareil
- Existence d'applications sur les appareils utilisateur

Lorsque vous créez une action automatisée, les déclencheurs définis pour l'action déterminent ce qui se passe sur l'appareil de l'utilisateur lorsqu'il est connecté à Citrix Endpoint Management. Lorsqu'un événement est déclenché, vous pouvez envoyer une notification à l'utilisateur pour résoudre un problème avant qu'une action plus sérieuse ne soit nécessaire.

Les effets automatiques que vous pouvez paramétrer sont :

- Effacement complet ou effacement des données d'entreprise de l'appareil.
- Rendre l'appareil non-conforme.
- Révoquer l'appareil.
- Envoyer un message à l'utilisateur pour qu'il résolve un problème avant que des actions plus sévères ne soient entreprises.

Vous pouvez configurer des actions de verrouillage et d'effacement des applications en mode MAM uniquement.

Vous pouvez utiliser des actions automatisées pour marquer des appareils Windows 10 et Windows 11 appartenant à Azure Active Directory (AD) comme non conformes dans Azure AD.

> **Remarque :**
>
> Pour avertir les utilisateurs, vous devez avoir configuré les serveurs de notification dans les paramètres Citrix Endpoint Management pour SMTP afin que Citrix Endpoint Management puisse envoyer des messages. Pour de plus amples informations, consultez la section Notifications. Configurez les modèles de notification que vous prévoyez d'utiliser avant de continuer. Pour de plus amples informations, consultez la section Notifications. Consultez la section Créer et mettre à jour des modèles de notification.

Exemples d'actions

Voici quelques exemples d'utilisation d'actions automatisées :

Exemple 1

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Vous souhaitez détecter une application que vous avez précédemment bloquée (par exemple, « Words with Friends »). Vous pouvez spécifier un déclencheur qui définit la machine utilisateur comme étant hors conformité après la détection de l'application « Words with Friends ». L'action avertit les utilisateurs qu'ils doivent supprimer l'application pour que leurs appareils soient à nouveau conformes. Vous pouvez également définir un délai pour que les utilisateurs se conforment. Après ce délai, une action définie se produit, comme l'effacement sélectif de l'appareil.

Exemple 2

- Vous souhaitez vérifier si les clients utilisent le dernier firmware et bloquer l'accès aux ressources si les utilisateurs doivent mettre à jour leurs appareils. Vous pouvez spécifier un déclencheur qui rend l'appareil utilisateur non conforme lorsqu'il ne dispose pas de la dernière version. Vous utilisez des actions automatisées pour bloquer les ressources et pour informer les clients.

Exemple 3

- Un appareil utilisateur est placé dans un état de non-conformité, puis l'utilisateur répare l'appareil de façon à ce qu'il soit conforme. Vous pouvez configurer une stratégie permettant de déployer un package qui réinitialise l'appareil dans un état de conformité.

Exemple 4

- Vous souhaitez marquer des appareils utilisateur qui ont été inactifs pendant une certaine période de temps comme étant non conformes. Vous pouvez créer une action automatisée pour les appareils inactifs comme suit :

  1. Dans la console Citrix Endpoint Management, accédez à **Paramètres > Contrôle d'accès réseau**, puis sélectionnez **Appareils inactifs**. Pour plus d'informations sur le paramètre **Appareils inactifs**, consultez la section Contrôle d'accès réseau.
  2. Suivez les étapes pour ajouter une action, comme indiqué dans Ajouter et gérer des actions. La seule différence est que vous configurez les paramètres comme suit sur la page **Détails de l'action** :
     - **Déclencheur** : sélectionnez **Propriété de l'appareil**, **Non conforme** et **Vrai**.
     - **Action**. sélectionnez **Envoyer notification** et sélectionnez un modèle que vous avez créé à l'aide du champ **Modèle de notification** dans **Paramètres**. Ensuite, définissez le délai en jours, heures ou minutes avant d'exécuter l'action. Définissez l'intervalle auquel l'action se répète jusqu'à ce que l'utilisateur corrige le problème déclencheur.

> **Conseil :**
>
> Pour supprimer des appareils inactifs en bloc, utilisez l'API REST publique Citrix Endpoint Management. Vous obtenez d'abord manuellement les ID d'appareils pour les appareils

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

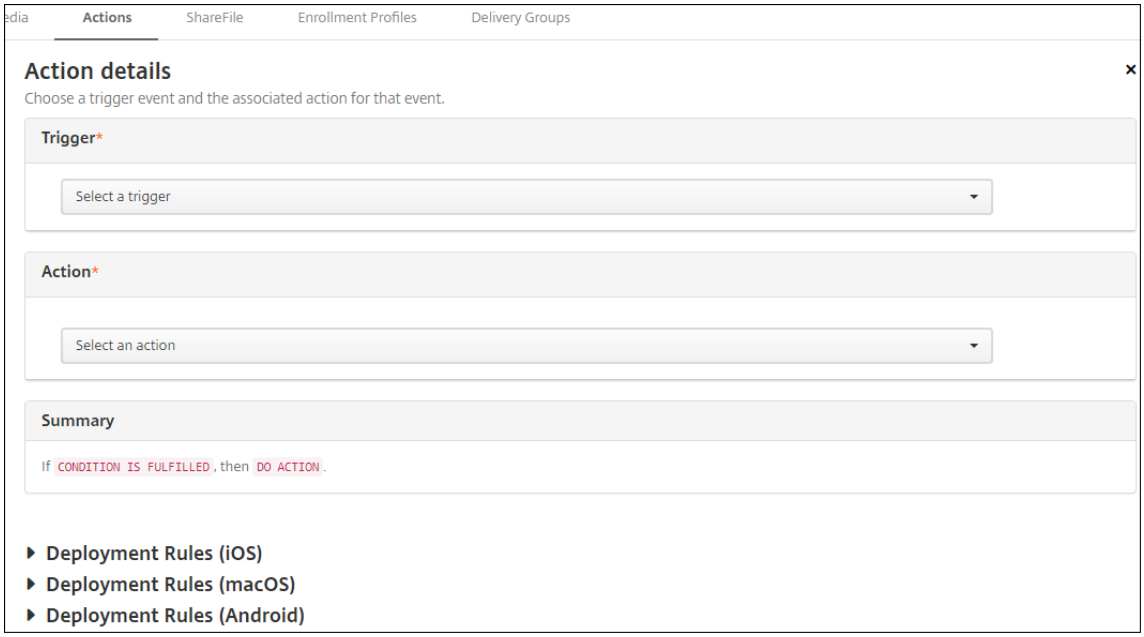
> inactifs que vous souhaitez supprimer, puis vous exécutez l'API delete pour les supprimer en bloc.

Ajouter et gérer des actions

Pour ajouter, modifier et filtrer des actions automatisées :

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Actions**. La page **Actions** s'affiche.
2. Sur la page **Actions**, effectuez l'une des actions suivantes :
   - Cliquez sur **Ajouter** pour ajouter une action.
   - Sélectionnez une action existante à modifier ou à supprimer. Cliquez sur l'option que vous voulez utiliser.
3. La page **Informations sur l'action** s'affiche.
4. Sur la page **Informations sur l'action**, entrez ou modifiez les informations suivantes :
   - **Nom :** entrez un nom permettant d'identifier l'action. Ce champ est obligatoire.
   - **Description :** décrivez ce que l'action doit faire.
5. Cliquez sur **Suivant**. La page sur les **Détails de l'action** s'affiche.

   L'exemple suivant illustre comment configurer un déclencheur **d'événement**. Si vous sélectionnez un autre déclencheur, les options sont différentes de celles affichées ici.



6. Sur la page **Détails de l'action**, entrez ou modifiez les informations suivantes :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dans la liste des **Déclencheurs**, cliquez sur le type de déclencheur d'événements pour cette action. Sélectionnez l'un des déclencheurs suivants :

- **Événement :** vérifie si l'état de l'appareil correspond à l'événement de non-conformité choisi, puis y réagit.
- **Propriété de l'appareil :** recherche une valeur spécifique associée à un attribut d'appareil sur l'appareil géré par MDM, puis y réagit. Pour de plus amples informations, consultez la section Noms et valeurs des propriétés d'appareil.
- **Propriété utilisateur :** réagit à une valeur spécifique associée à un attribut utilisateur, généralement à partir d'Active Directory.
- **Nom de l'application installée :** réagit à une application installée. Ne s'applique pas au mode MAM exclusif. Requiert que la stratégie d'inventaire des applications soit activée sur l'appareil. Par défaut, la stratégie d'inventaire des applications est activée sur toutes les plates-formes. Pour de plus amples informations, consultez la section Pour ajouter une stratégie d'inventaire des applications.
- **Valeur renvoyée par la stratégie :** vérifie si la valeur renvoyée par les scripts PowerShell répond à certains critères logiques. La stratégie Agent Windows doit être activée et configurée. Pour plus d'informations sur la stratégie Agent Windows, voir Stratégie de l'agent Windows.

7. Dans la liste suivante, cliquez sur la réponse au déclencheur.

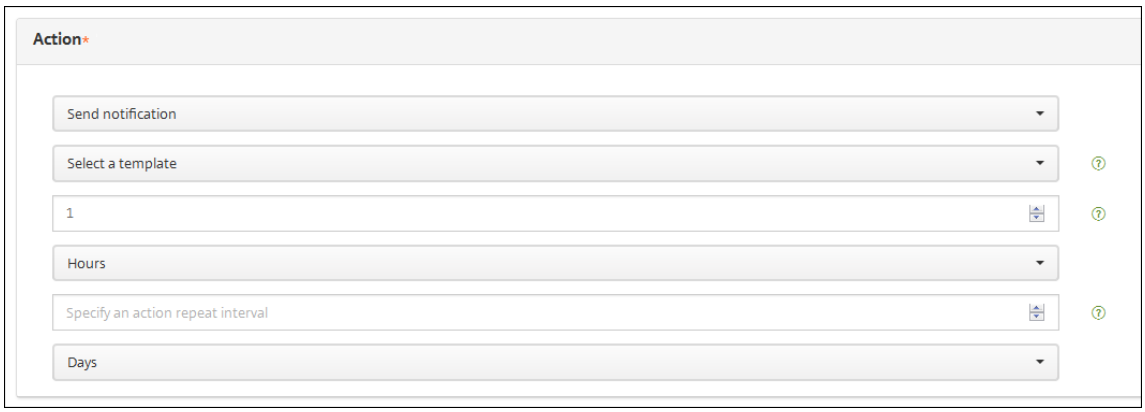
8. Dans la liste **Action**, cliquez sur l'action à effectuer lorsque le critère du déclencheur est rencontré. À l'exception de l'action **Envoyer une notification**, vous choisissez un délai au cours duquel les utilisateurs devront avoir résolu le problème qui a activé le déclencheur. Si le problème n'est pas résolu dans ce délai, l'action sélectionnée est entreprise. Pour une définition des actions, consultez la section Actions de sécurisation.

   Si vous sélectionnez **Envoyer une notification**, procédez comme suit pour envoyer une action de notification.

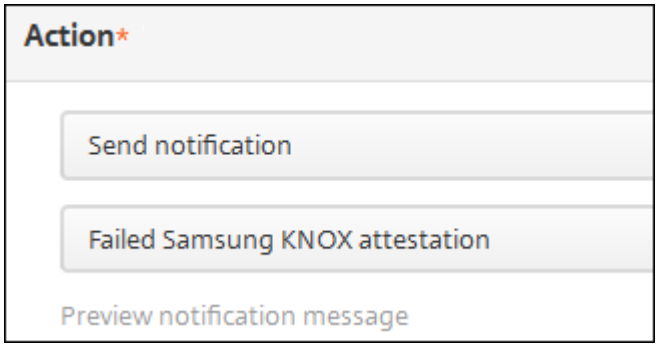
9. Dans la liste suivante, sélectionnez le modèle à utiliser pour la notification. Les modèles de notification correspondant à l'événement sélectionné apparaissent. S'il n'y a pas de modèle pour le type de notification, le message suivant vous invite à configurer un modèle : Aucun modèle de notification pour ce type d'événement. Créez un modèle à l'aide de **Modèle de notification** dans **Paramètres**.

   Pour avertir les utilisateurs, utilisez **Paramètres > Serveur de notification** pour configurer les paramètres pour SMTP afin que Citrix Endpoint Management puisse envoyer des messages. Consultez la section Notifications. En outre, avant de continuer, utilisez **Paramètres > Modèle de notification** pour configurer les modèles de notification que vous prévoyez d'utiliser. Consultez la section Créer et mettre à jour des modèles de notification.

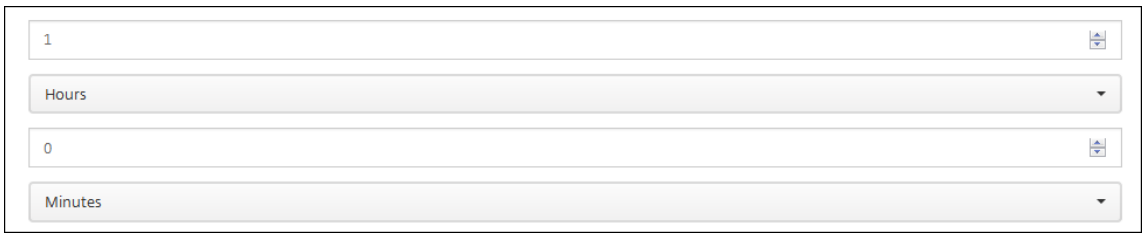
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Après avoir sélectionné le modèle, cliquez sur **Aperçu du message de notification**.



10. Dans les champs suivants, définissez le délai en jours, heures ou minutes avant d'effectuer l'action. Définissez l'intervalle auquel l'action se répète jusqu'à ce que l'utilisateur corrige le problème déclencheur.



11. Dans **Résumé**, vérifiez que vous avez créé les actions automatisées comme prévu.

12. Après avoir configuré les détails de l'action, vous pouvez configurer des règles de déploiement pour chaque plate-forme individuellement. Pour ce faire, suivez l'étape 13 pour chacune des plates-formes que vous choisissez.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

13. Configurez les règles de déploiement. Pour des informations générales sur la configuration des règles de déploiement, consultez la section Déployer des ressources.

    Pour cet exemple :

    - Le propriétaire de l'appareil doit être **BYOD**.
    - L'appareil doit avoir un code secret conforme.
    - Le code de pays mobile de l'appareil ne peut pas être uniquement Andorre.

14. Lorsque vous avez terminé de configurer les règles de déploiement par plate-forme pour l'action, cliquez sur **Suivant**. La page d'**attribution d'actions** s'affiche. Sur cette page, vous pouvez attribuer l'action à un ou plusieurs groupes de mise à disposition. Cette étape est facultative.

15. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez des groupes. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

16. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

    - En regard de **Déployer**, cliquez sur **Activé** pour planifier le déploiement ou cliquez sur **Désactivé** pour empêcher le déploiement. L'option par défaut est définie sur **Activé**. Si vous choisissez **Désactivé**, aucune autre option n'est requise.
    - À côté du **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est définie sur **Maintenant**.
    - Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    - En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est définie sur **À chaque connexion**.
    - En regard de **Déployer pour les connexions permanentes**, cliquez sur **Activé** ou **Désactivé**. L'option par défaut est définie sur **Désactivé**.

      Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.

      > **Remarque :**
      >
      > Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**.
      >
      > L'option de connexion permanente :
      >
      > – N'est pas disponible pour les appareils iOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> – N'est pas disponible pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec la version 10.18.19 ou ultérieure
> – N'est pas recommandée pour les systèmes d'exploitation Android et Android Enterprise pour les clients ayant commencé à utiliser Citrix Endpoint Management avec une version antérieure à la version 10.18.19
>
> Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**.

17. Cliquez sur **Suivant**. La page **Résumé** s'affiche, où vous pouvez vérifier la configuration de l'action.
18. Cliquez sur **Enregistrer** pour enregistrer l'action.

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

Vous pouvez effacer ou verrouiller les applications d'un appareil pour quatre catégories de déclencheurs répertoriées dans la console Citrix Endpoint Management : événement, propriété de l'appareil, propriété utilisateur et nom de l'application installée.

Pour configurer le déclenchement automatique de l'effacement des applications ou du mode kiosque

1. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Actions**.
2. Sur la page **Actions**, cliquez sur **Ajouter**.
3. Sur la page **Informations sur l'action**, entrez un nom pour l'action et une description facultative.
4. Sur la page **Détails de l'action**, sélectionnez le déclencheur de votre choix.
5. Dans **Action**, sélectionnez une action.

   Pour cette étape, tenez compte des conditions suivantes :

   Lorsque le type de déclencheur est défini sur **Événement** et que la valeur n'est pas Utilisateur **Active Directory désactivé**, les actions **Effacement des applications** et **Mode kiosque** ne s'affichent pas.

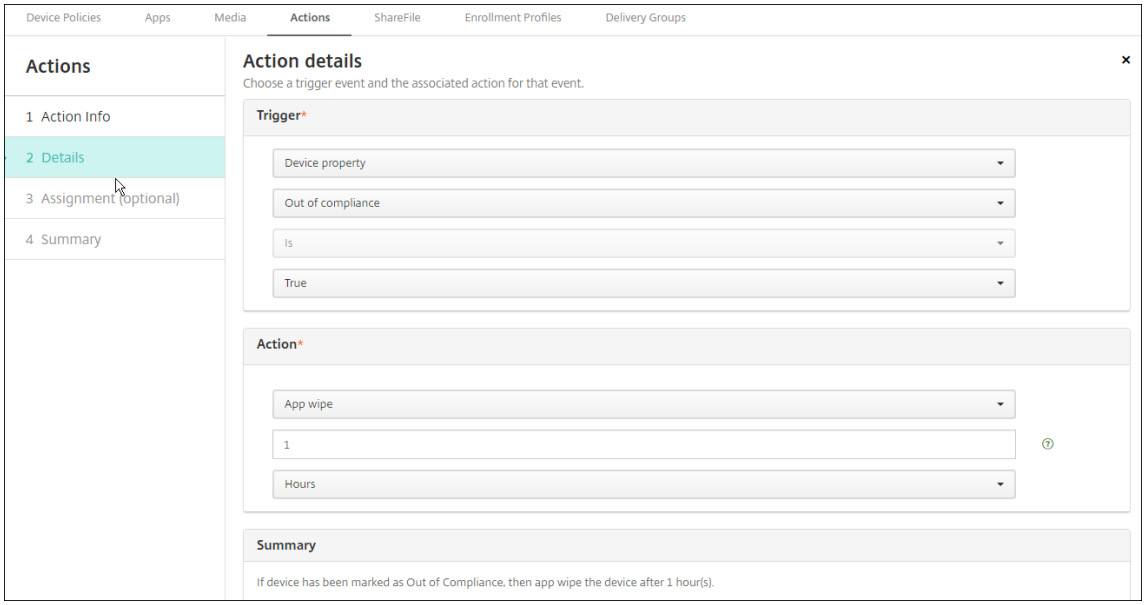
   Lorsque le type de déclencheur est défini sur **Propriété de l'appareil** et que la valeur est **Mode perdu MDM activé**, les actions suivantes ne s'affichent pas :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Effacer les données d'entreprise de l'appareil
- Effacer toutes les données de l'appareil
- Révoquer l'appareil

Pour chaque option, un délai de 1 heure est automatiquement défini, mais vous pouvez sélectionner la durée de ce délai en minutes, heures ou jours. Le but du délai est de donner aux utilisateurs le temps de résoudre un problème avant que l'action ne se produise. Pour plus d'informations sur les actions de réinitialisation de l'application et de verrouillage de l'application, voir Actions de sécurité.

> **Remarque :**
>
> Si vous définissez le déclencheur sur **Événement**, l'intervalle de répétition est réglé automatiquement sur un minimum d'1 heure. L'appareil doit actualiser les stratégies pour se synchroniser avec le serveur pour que la notification soit envoyée. En règle générale, un appareil se synchronise avec le serveur lorsque les utilisateurs se connectent ou actualisent manuellement leurs stratégies Citrix Secure Hub.
>
> Un délai supplémentaire d'environ une heure avant l'exécution de l'action est également possible, afin de permettre la synchronisation de la base de données Active Directory avec Citrix Endpoint Management.

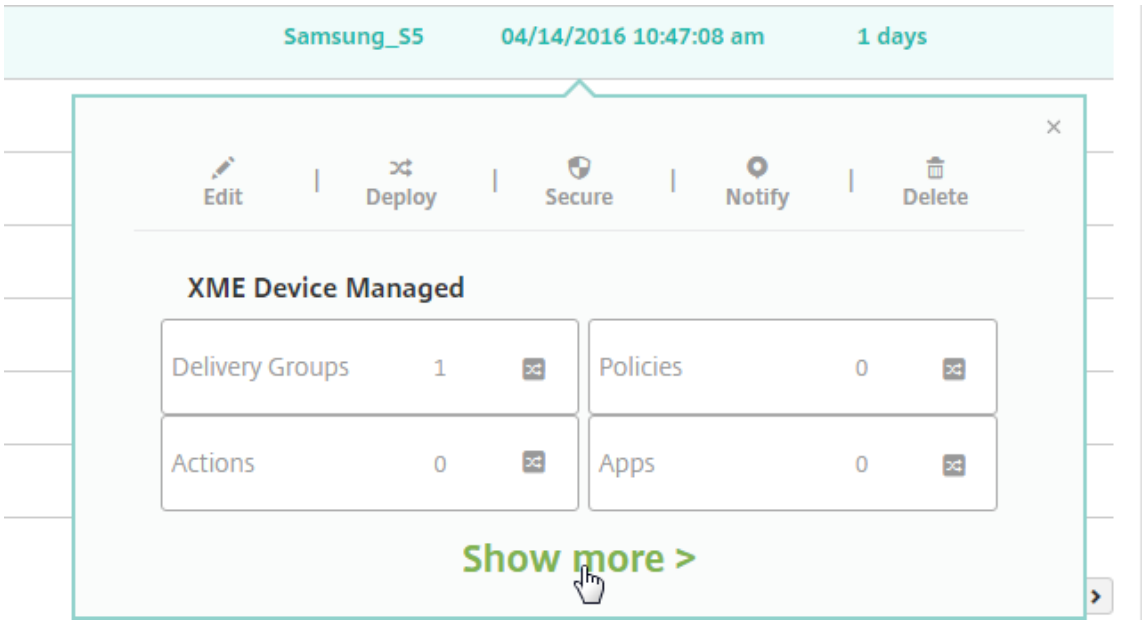


6. Configurez les règles de déploiement, puis cliquez sur **Suivant**.
7. Configurez les attributions de groupe de mise à disposition et un calendrier de déploiement, puis cliquez sur **Suivant**.
8. Cliquez sur **Enregistrer**.

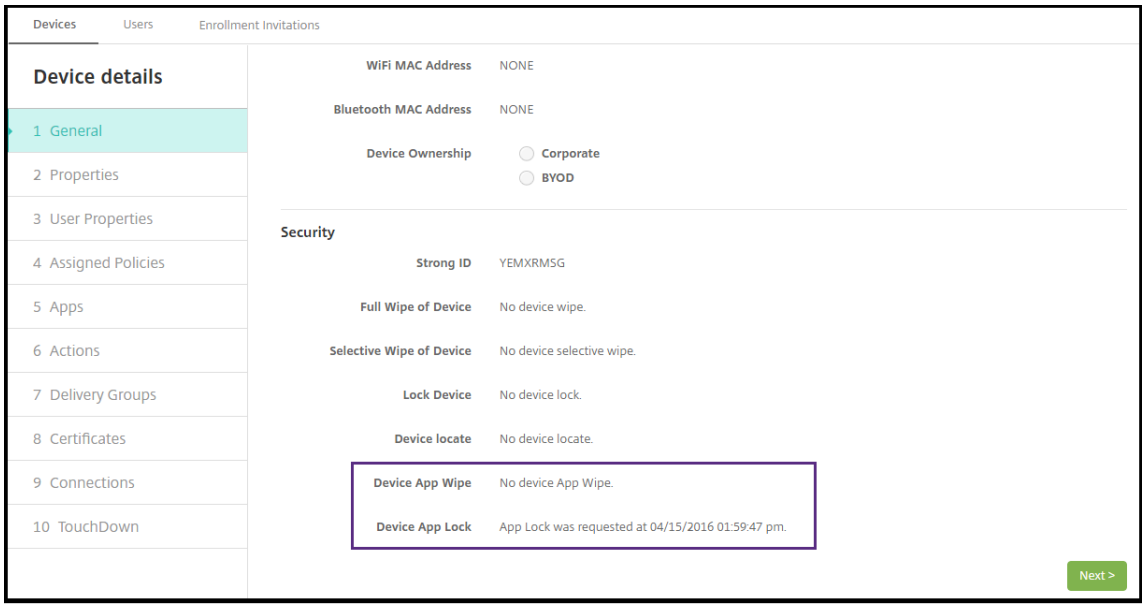
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

1. Accédez à **Gérer > Appareils**, cliquez sur un appareil et sur **Afficher plus**.

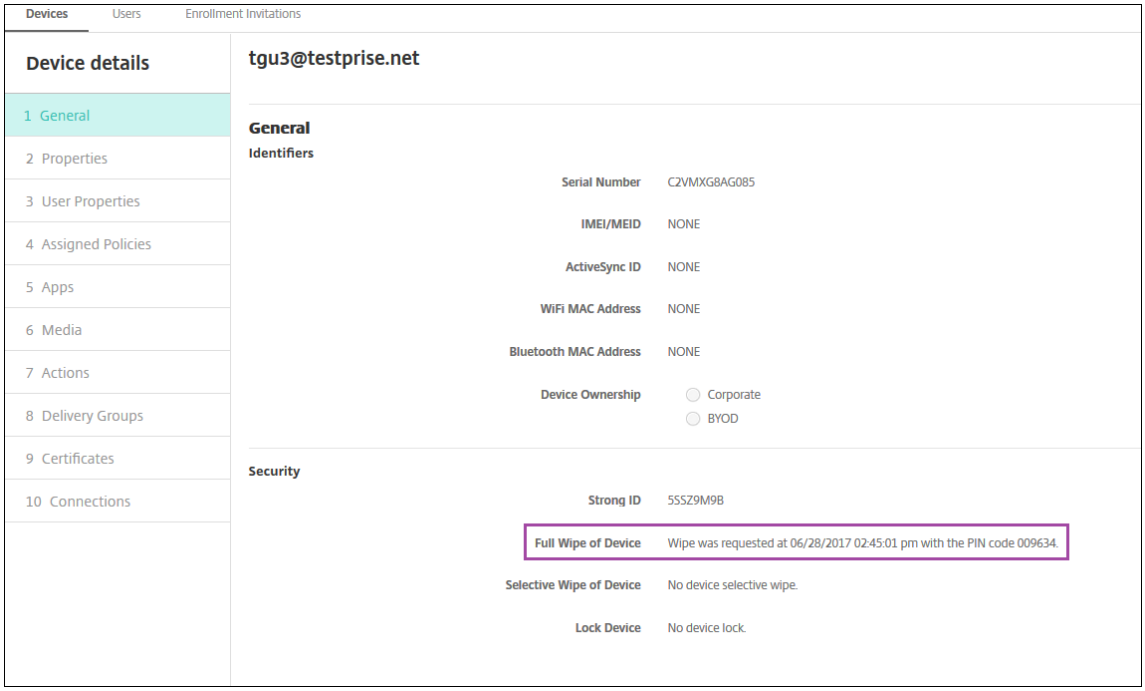


2. Faites défiler jusqu'à **Effacement des applications sur l'appareil** et **Mode kiosque sur l'appareil**.



Une fois qu'un appareil est effacé, l'utilisateur est invité à entrer un code PIN. Si l'utilisateur oublie le code, vous pouvez le rechercher dans Détails de l'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Marquer les appareils Windows 10 et Windows 11 non conformes dans Azure AD

Lorsque des appareils Windows 10 et Windows 11 appartenant à Azure AD sont marqués comme non conformes dans Citrix Endpoint Management, ils peuvent également l'être dans Azure AD. Pour activer cette fonction, ajoutez les autorisations à l'application MDM locale pour accéder à l'API Microsoft Graph dans le portail Azure AD.

1. Ouvrez une session dans le portail Azure AD avec vos informations d'identification d'administrateur Azure AD.
2. Dans le portail Azure AD, accédez à **Azure Active Directory > Mobility (MDM and MAM)**. Sélectionnez **On-premises MDM application**.
3. Cliquez sur **On-premises Application Settings > Required Permissions > Add > Select an API > Microsoft Graph**. Cliquez sur **Select** et enregistrer vos sélections.
4. Sous **Required permissions**, sélectionnez **Microsoft Graph**. Sous **Enable Access**, sélectionnez **Read and write directory data**.
5. Sous **Required permissions**, sélectionnez **Microsoft Graph**. Cliquez ensuite sur **Grant permissions**.
6. Cliquez sur **Yes** pour accorder l'autorisation.

Lorsqu'un appareil inscrit à Azure AD exécutant Windows 10 ou Windows 11 n'est pas conforme, Citrix Endpoint Management marque également l'appareil comme non conforme dans Azure AD.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Créer une action automatisée basée sur un résultat de la stratégie Agent Windows

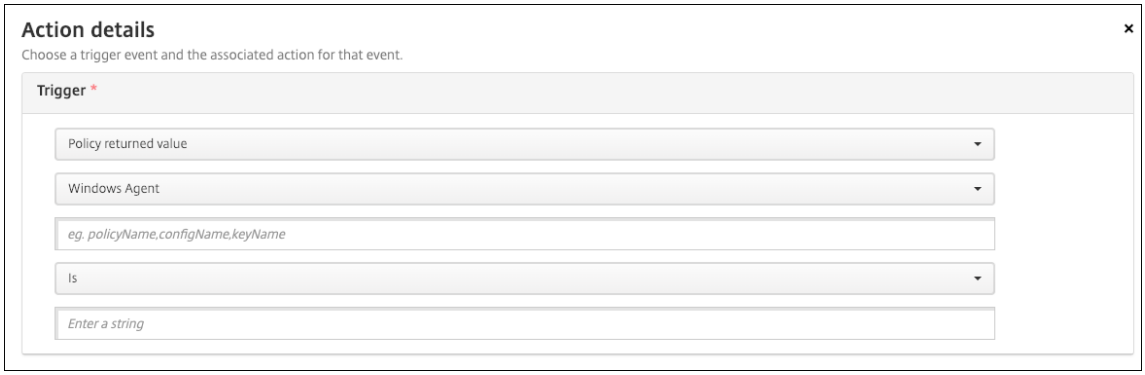
Utilisez la stratégie Agent Windows pour déployer des scripts qui surveillent les valeurs de Registre sur les bureaux et les tablettes Windows gérés. En fonction des valeurs renvoyées par un script, vous pouvez configurer une action automatisée à exécuter.

1. Configurez une stratégie Agent Windows et vérifiez les valeurs renvoyées par le script. Pour plus d'informations sur la stratégie Agent Windows, voir Stratégie de l'agent Windows.

   Cet article et cette section contiennent un exemple basé sur un script nommé `EntApp_2019_checkFirew` . La stratégie Agent Windows associée définit une configuration nommée `cName_checkFirewall` . Cette configuration exécute l'exemple de script.

   Une fois le script exécuté sur un appareil, vous obtenez les informations nécessaires pour créer une action, comme décrit dans la Stratégie de l'agent Windows.

2. Dans la console Citrix Endpoint Management, cliquez sur **Configurer > Actions**.
3. Sur la page **Actions**, cliquez sur **Ajouter**.
4. Sur la page **Informations sur l'action**, entrez un nom pour l'action et une description facultative.
5. Sur la page **Détails de l'action**, sélectionnez le déclencheur **Valeur renvoyée par la stratégie**.

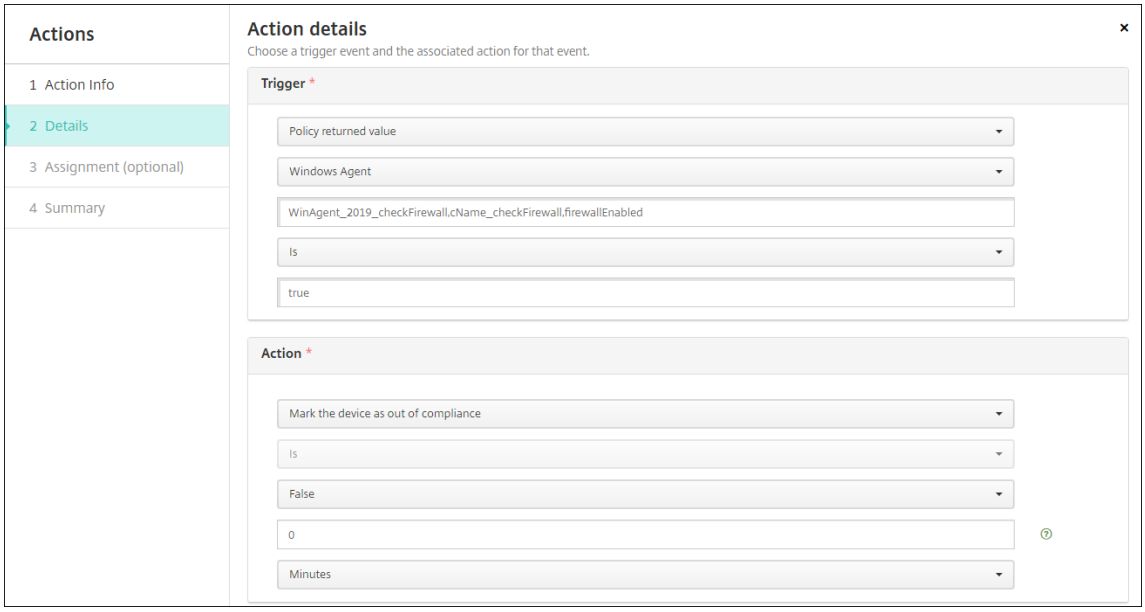


6. Dans les champs qui apparaissent, définissez le déclencheur et l'action :

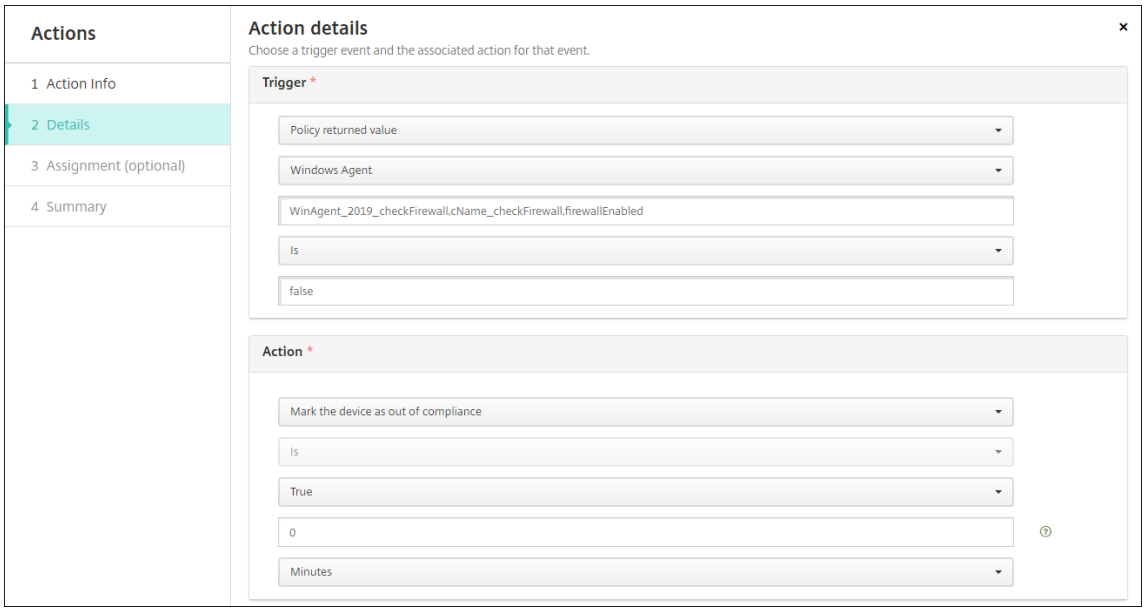
   - **Paramètres de l'Agent Windows :** tapez le nom de stratégie, le nom de configuration et le nom de clé pour la stratégie Agent Windows que vous avez créée.
   - **Menu déroulant :** sélectionnez la logique **Is**, **Is Not**, **Contains** ou **Does Not Contain**. Cette logique s'applique au champ suivant et provoque le déclenchement de l'action si la logique s'applique.
   - **Entrez une chaîne :** entrez la chaîne résultant de l'exécution du script PowerShell chargé dans votre stratégie. Pour plus d'informations sur la recherche de cette chaîne, voir Stratégie Agent Windows.
   - **Action :** sélectionnez une action, une valeur pour l'action et choisissez un délai pour la résolution de l'action.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dans notre exemple : si le nom de la clé `firewallEnabled` renvoie la valeur **`true`**, l'action suivante marque l'appareil comme conforme.



Si le nom de la clé `firewallEnabled` renvoie la valeur **`false`**, l'action suivante marque l'appareil comme conforme.



7. Si nécessaire, définissez un calendrier de déploiement et choisissez des groupes de mise à disposition.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Surveillance et assistance

March 1, 2024

Vous pouvez utiliser le tableau de bord de Citrix Endpoint Management et la page Support de Citrix Endpoint Management afin de contrôler et de résoudre les problèmes de votre serveur Citrix Endpoint Management. Utilisez la page Support de Citrix Endpoint Management pour accéder à des informations et outils de support.

Dans la console Citrix Endpoint Management, cliquez sur l'icône de la clé dans le coin supérieur droit.

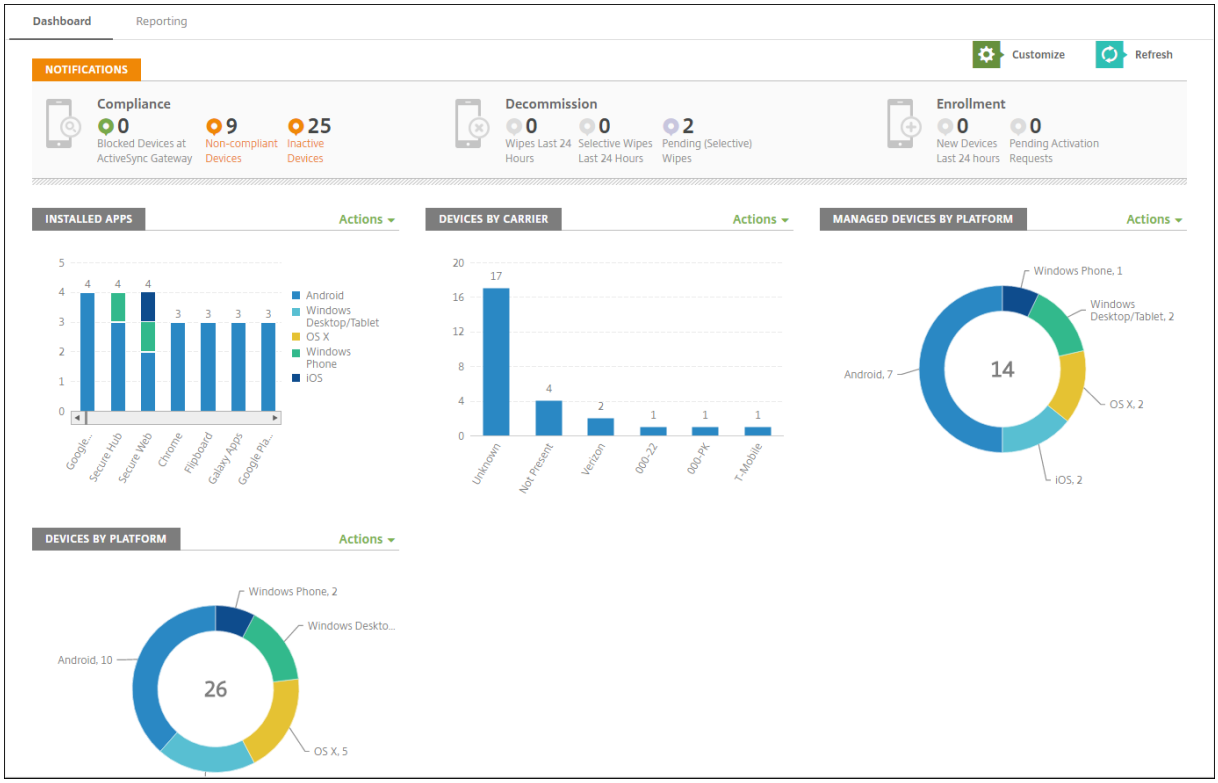
La page **Dépannage et support** s'ouvre.

Utilisez la page **Dépannage et support** de Citrix Endpoint Management pour :

- Accéder aux diagnostics.
- Accéder aux liens de la documentation produit et du centre de connaissances Citrix.
- Accéder au journal des opérations.
- Utiliser les options de configuration avancée.
- Accéder à un ensemble d'outils et d'utilitaires.

Vous pouvez afficher un synopsis des informations en accédant au tableau de bord de votre console Citrix Endpoint Management. Avec ces informations, vous pouvez voir un aperçu rapide des problèmes et des résolutions en utilisant des widgets.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Le tableau de bord est généralement la page qui s'affiche lorsque vous vous connectez à la console Citrix Endpoint Management. Pour accéder au tableau de bord ailleurs dans la console, cliquez sur **Analyser**. Cliquez sur **Personnaliser** dans le tableau de bord pour modifier la configuration de la page et pour modifier les widgets qui s'affichent.

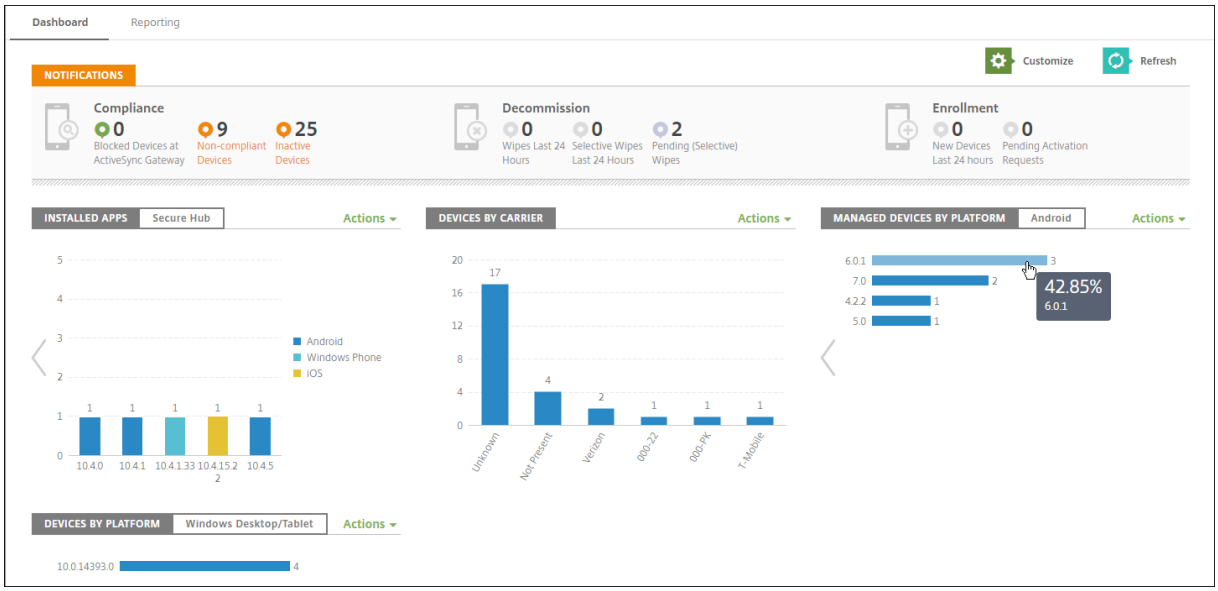
- **Mes tableaux de bord :** vous pouvez enregistrer jusqu'à quatre tableaux de bord. Vous pouvez modifier ces tableaux de bord séparément et afficher chacun d'entre eux en sélectionnant le tableau de bord enregistré.
- **Disposition :** dans cette ligne, vous pouvez sélectionner le nombre de widgets qui s'affichent sur votre tableau de bord et la manière dont les widgets sont disposés.
- **Sélection des widgets :** vous pouvez choisir les informations qui s'affichent dans votre tableau de bord.
  - **Notifications :** cochez la case au-dessus des chiffres sur la gauche pour ajouter une barre Notifications au-dessus de vos widgets. Cette barre affiche le nombre d'appareils compatibles, d'appareils inactifs et d'appareils effacés ou inscrits dans les dernières 24 heures.
  - **Appareils par plate-forme :** affiche le nombre d'appareils gérés et non gérés par plate-forme.
  - **Appareils par opérateurs :** affiche le nombre d'appareils gérés et non gérés par opérateur. Cliquez sur chaque barre pour afficher la répartition par plate-forme.
  - **Appareils gérés par plate-forme :** affiche le nombre d'appareils gérés par plate-forme.
  - **Appareils non gérés par plate-forme :** affiche le nombre d'appareils non gérés par plate-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

forme. Les appareils qui s'affichent dans ce graphique peuvent avoir un agent installé, mais leurs privilèges ont été révoqués ou ils ont été effacés.

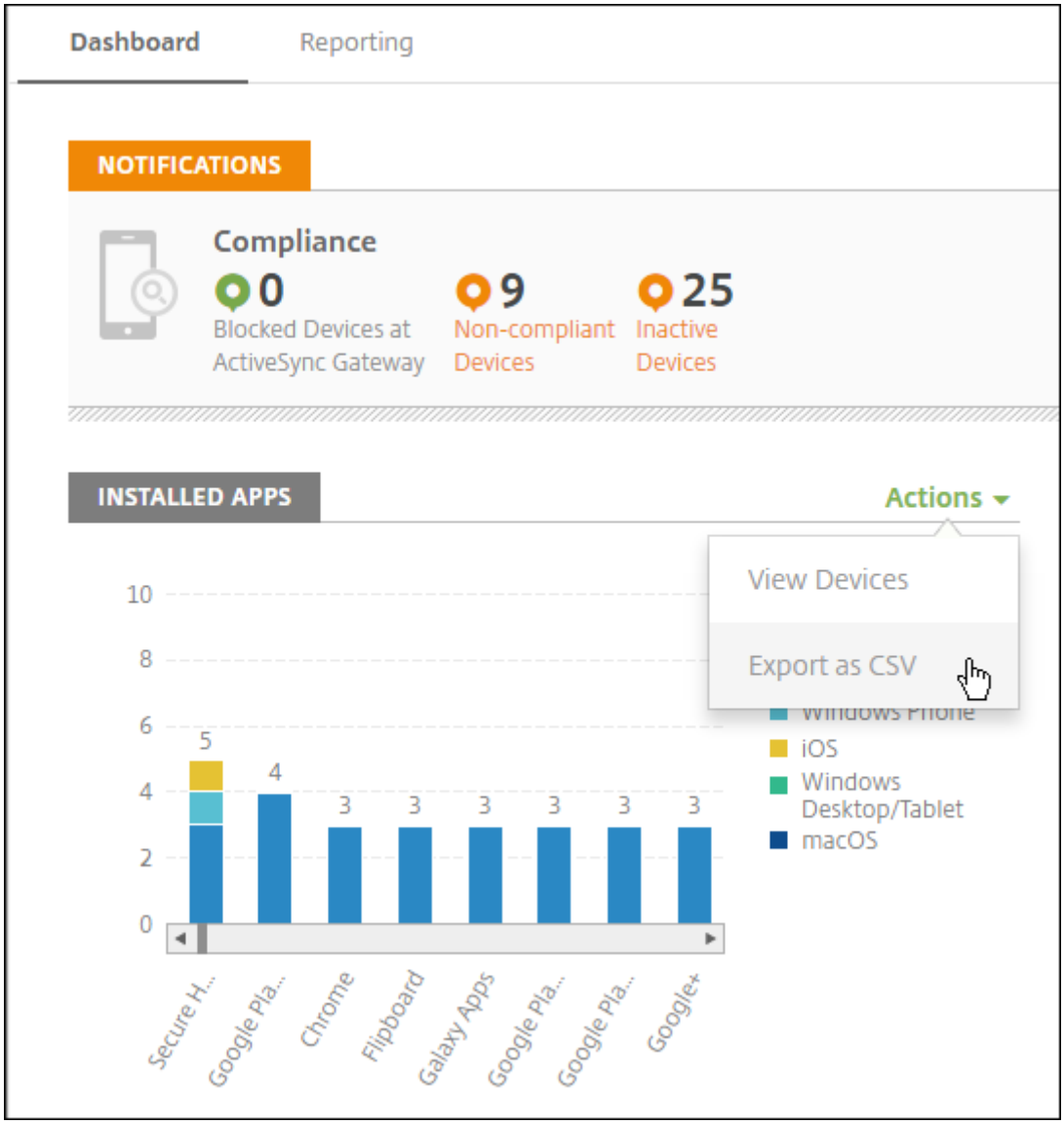
- **Appareils par état ActiveSync Gateway :** affiche le nombre d'appareils regroupés par état ActiveSync Gateway. Les informations affichent l'état Inconnu, Autorisé ou Bloqué. Vous pouvez cliquer sur chaque barre pour décomposer les données par plate-forme.
- **Appareils par appartenance :** affiche le nombre d'appareils regroupés par état d'appartenance. Les informations affichent l'état Appartenant à la société, Appartenant à l'employé ou Inconnu.
- **Déploiements de groupes de mise à disposition ayant échoué :** affiche le nombre total d'échecs de déploiements par package. Seuls les packages avec des échecs de déploiements s'affichent.
- **Appareils par motif de blocage :** affiche le nombre d'appareils bloqués par ActiveSync
- **Applications installées :** entrez un nom d'application pour un graphique des informations sur l'application.
- **Licences utilisées par les applications d'achat en volume :** affiche des statistiques d'utilisation de licences pour les applications d'achat en volume d'Apple.

Avec chaque widget, vous pouvez cliquer sur les parties individuelles pour affiner les informations.



Vous pouvez également exporter les informations sous forme de fichier .csv en cliquant sur le menu **Action**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Page Analyse pour les administrateurs du service d'assistance

Vous pouvez surveiller et résoudre les problèmes de Citrix Endpoint Management sur la page **Surveiller**. Cette interface est personnalisée pour permettre aux administrateurs du service d'assistance d'effectuer un dépannage personnalisé.

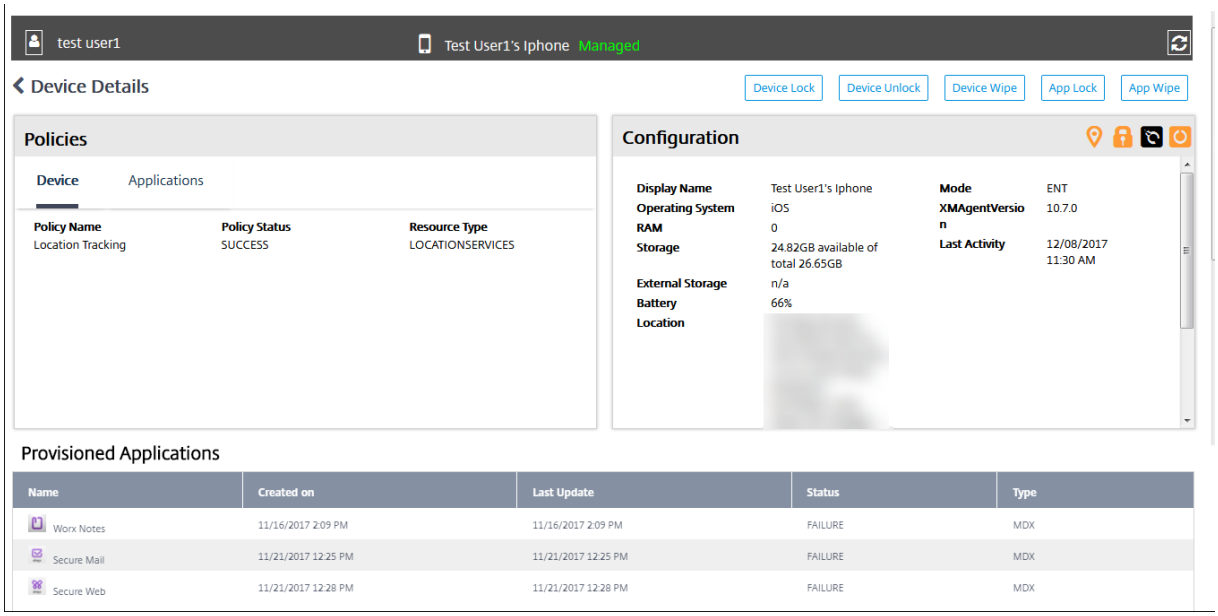
Les administrateurs du service d'assistance doivent disposer des autorisations suivantes pour accéder à la page **Surveiller** et à tous les workflows disponibles :

- Accès autorisé
  - Accès à la console d'admin
  - Accès à l'API publique

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Fonctionnalités de la console
  - Surveiller
  - Appareils
  - Effacer un appareil
  - Afficher la localisation
    - Localiser un appareil
    - Suivre un appareil
  - Verrouiller un appareil
  - Déverrouiller un appareil
  - Mode kiosque
  - Effacement des applications
  - Application

La page **Surveiller** vous donne une vue consolidée des stratégies et de la configuration de l'appareil. La vue inclut des actions de dépannage telles que le verrouillage/déverrouillage de l'application, le nettoyage de l'application, le verrouillage/déverrouillage de l'appareil et le nettoyage de l'appareil.



Utilisez la page **Surveiller** pour :

- Rechercher un utilisateur Active Directory (AD) et un appareil présentant des problèmes.
- Analyser la page **Détails de l'appareil** qui contient les informations suivantes :
  - **Stratégies :** affiche les stratégies d'appareil et d'application pour l'appareil et l'application sélectionnés. Pour plus d'informations sur la modification des stratégies, veuillez consulter les sections Stratégies d'appareil et Ajout d'applications.
  - **Configuration :** affiche la configuration de l'appareil. Ce panneau comporte des icônes indiquant si l'appareil a des services de localisation activés, s'il est jailbreaké ou géré par

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

MAM ou MDM. Le panneau affiche également l'état de chiffrement du stockage.
  - Tableau **Applications en cours d'exécution** : affiche les détails des applications en cours d'exécution sur l'appareil.

- Résoudre les problèmes de l'appareil. Les actions de sécurité disponibles sur cette page sont basées sur l'inscription de l'appareil et les autorisations accordées à l'administrateur connecté :
  - Verrouillage/déverrouillage de l'appareil
  - Réinitialisation de l'appareil
  - Mode kiosque (disponible si l'appareil est inscrit auprès de MAM)
  - Effacement des applications (disponible si l'appareil est inscrit auprès de MAM)

Pour de plus amples informations sur les actions qui peuvent être effectuées, veuillez consulter la section Actions de sécurisation.

La page Analyse peut ne pas fonctionner comme prévu 60 minutes après son dernier chargement car elle ne gère pas les actualisations du jeton de connexion. Pour résoudre ce problème, actualisez le jeton en rechargeant la page : cliquez sur le lien **Citrix Cloud** sur votre console de service, puis cliquez sur **Citrix Endpoint Management > Gérer > Surveiller**.

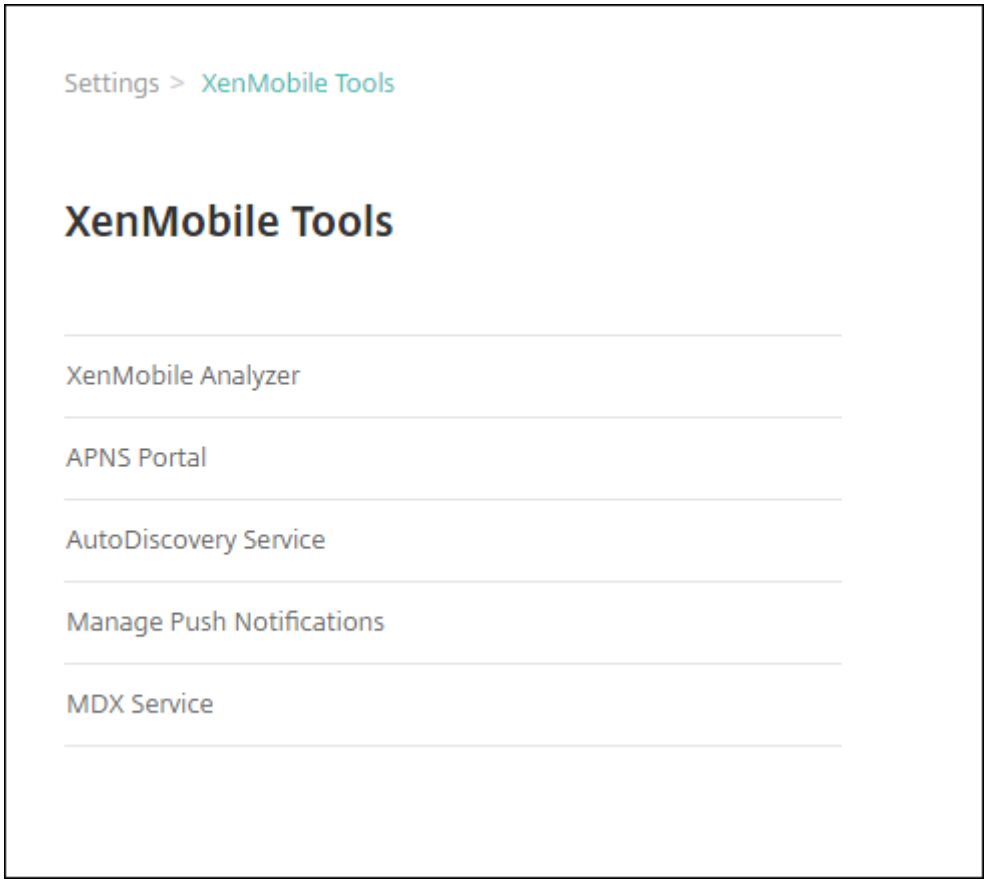
Accès à Citrix Endpoint Management Tools depuis la console

Vous pouvez accéder aux outils Citrix Endpoint Management Tools depuis la console Citrix Endpoint Management :

- **Portail APNs** –Permet d'envoyer une demande à Citrix pour signer un certificat APNs que vous soumettez ensuite à Apple.
- **AutoDiscovery Service** –Permet de demander et de configurer la détection automatique de Citrix Endpoint Management de votre domaine.
- **Gérer les notifications Push** –Permet de gérer les notifications Push pour les applications iOS et Windows mobiles.

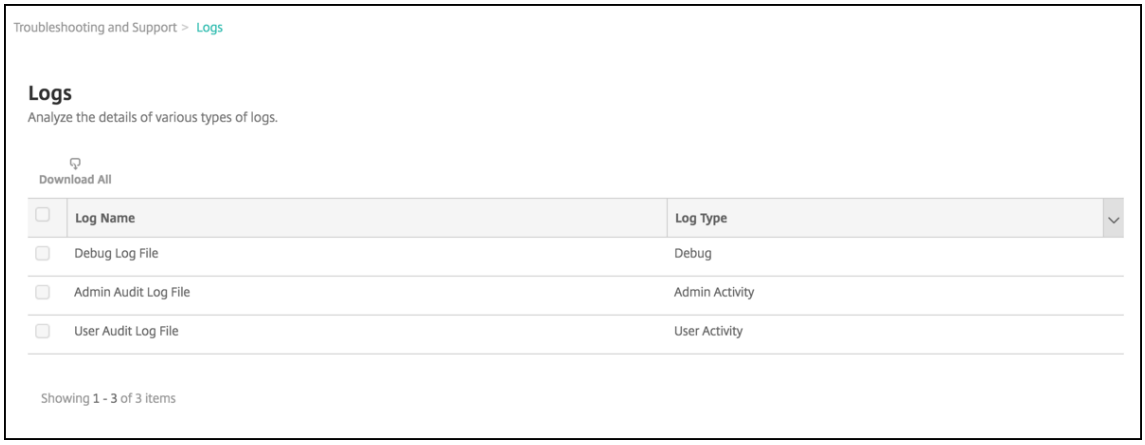
Pour accéder à ces outils, accédez à **Paramètres > Citrix Endpoint Management Tools**. Cette page est disponible auprès des utilisateurs ayant un rôle administrateur cloud ou administration client.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Visualiser et analyser les fichiers journaux dans Citrix Endpoint Management

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Dépannage et support** s'ouvre.
2. Sous **Opérations du journal**, cliquez sur **Journaux**. La page **Journaux** s'affiche. Des journaux individuels apparaissent dans un tableau.

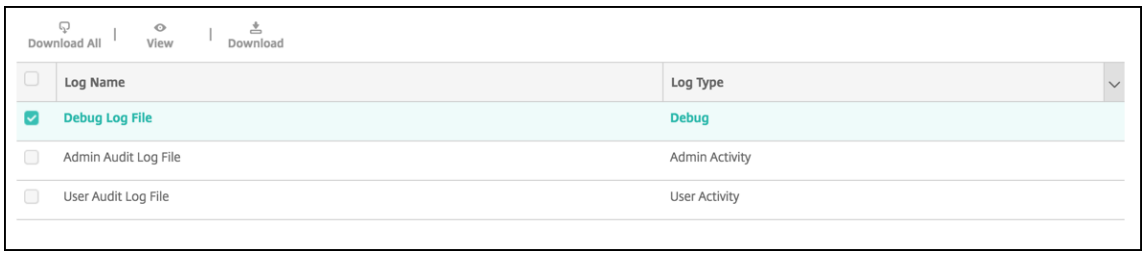


3. Sélectionnez le journal que vous souhaitez afficher :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Les fichiers journaux de débogage contiennent des informations utiles pour le support Citrix, telles que des messages d'erreur et des actions liées au serveur.
- Les fichiers journaux d'audit administrateur contiennent des informations d'audit relatives à l'activité sur la console Citrix Endpoint Management.
- Les fichiers journaux d'audit utilisateur contiennent des informations relatives aux utilisateurs configurés.

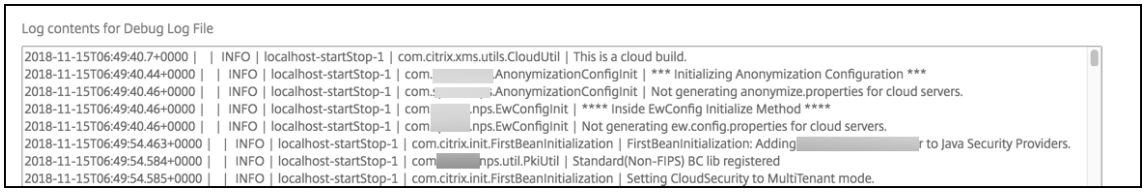
4. Utilisez les actions en haut du tableau pour télécharger tout, affiche ou télécharger un journal.



> **Remarque :**
>
> Si vous sélectionnez plusieurs fichiers journaux, seule l'option **Tout télécharger** est disponible.

5. Procédez comme suit :

   - **Tout télécharger :** la console télécharge tous les journaux présents sur le système (y compris les journaux de débogage, d'activité des utilisateurs/administrateurs, de serveur, etc.).
   - **Afficher :** affiche le contenu du journal sélectionné en dessous du tableau.
   - **Télécharger :** la console télécharge uniquement le type de fichier journal sélectionné. La console télécharge également tous les journaux archivés du même type.



Citrix Endpoint Management utilise l'appender syslog log4j pour envoyer des messages syslog formatés RFC5424. Les données du message syslog sont du texte brut sans format spécifique.

Tests de connectivité

March 1, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Depuis la page **Dépannage et support** de Citrix Endpoint Management, vous pouvez vérifier la connexion de Citrix Endpoint Management à NetScaler Gateway et à d'autres serveurs et emplacements. Pour exécuter les tests de connectivité Citrix Endpoint Management, vous avez besoin du rôle Support ou Administrateur. Définissez ce rôle à l'aide du contrôle d'accès basé sur rôle (RBAC). Pour plus d'informations concernant l'attribution des rôles, veuillez consulter la section Configurer des rôles avec RBAC.

Exécuter des tests de connectivité dans Citrix Endpoint Management

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Dépannage et support** s'ouvre.
2. Sous **Diagnostics**, cliquez sur **Tests de la connectivité de Citrix Endpoint Management**. La page **Test de la connectivité Citrix Endpoint Management** s'affiche. Si votre environnement Citrix Endpoint Management contient des nœuds en cluster, tous les nœuds sont affichés.

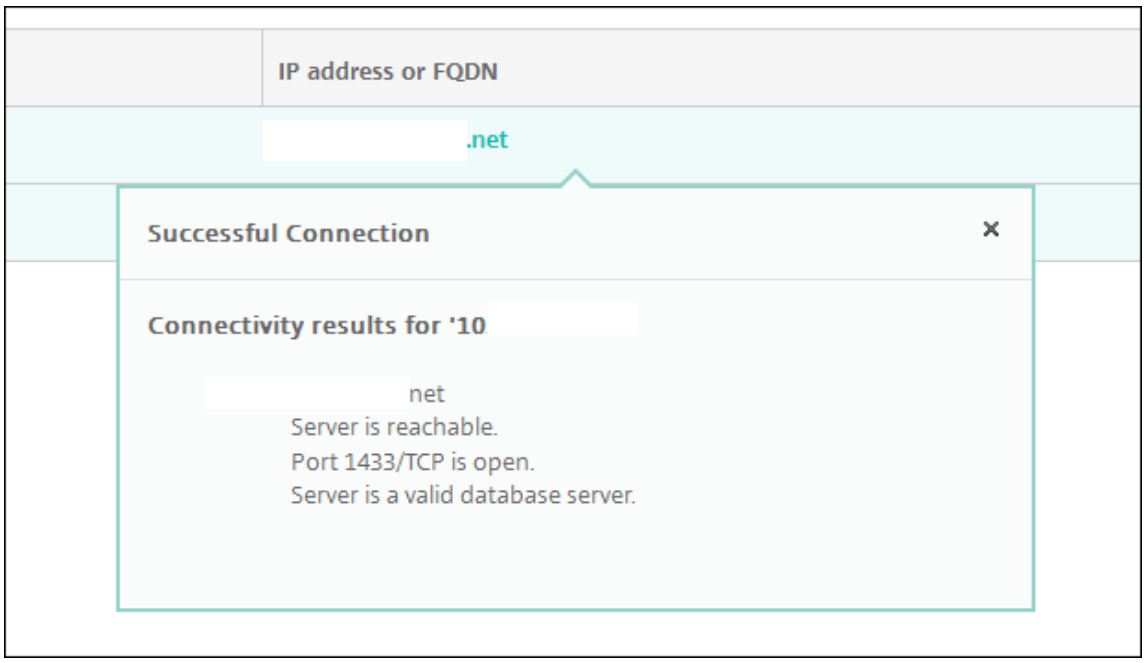
Connectivity to	IP address or FQDN
Windows Phone Store	windowsphone.com
Database	[redacted].net
Apple Feedback Push Notification Server	feedback.push.apple.com
LDAP	[redacted].net
Domain Name System (DNS)	[redacted]
Nexmo Gateway	-
Apple Push Notification Server	gateway.push.apple.com
iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
Google Play	play.google.com
Windows Security Token Service	login.live.com

3. Sélectionnez les serveurs que vous souhaitez inclure dans le test de connectivité, puis cliquez sur **Tester la connectivité**. La page des résultats du test s'affiche.

Connectivity to	IP address or FQDN	
Database	net	✓
Windows Phone Store	windowsphone.com	✓

4. Sélectionnez un serveur dans le tableau des résultats du test pour afficher les résultats détaillés pour ce serveur.

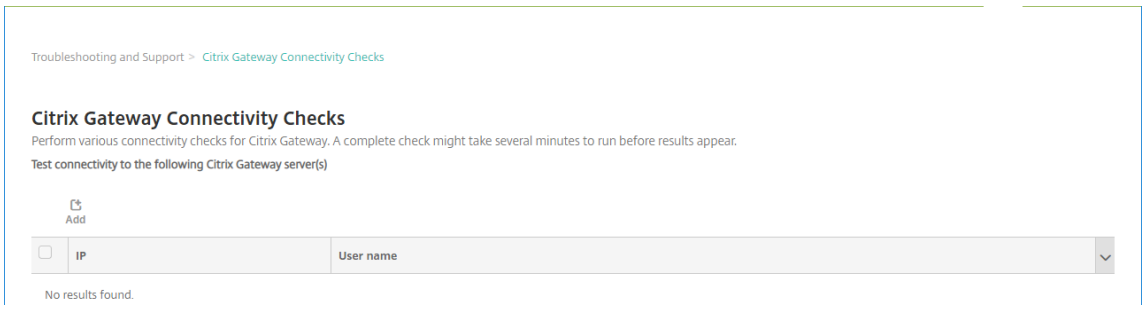
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pour plus d'informations sur les tests de connectivité que Citrix Endpoint Management peut effectuer et leurs détails, consultez la section Détails des tests de connectivité.

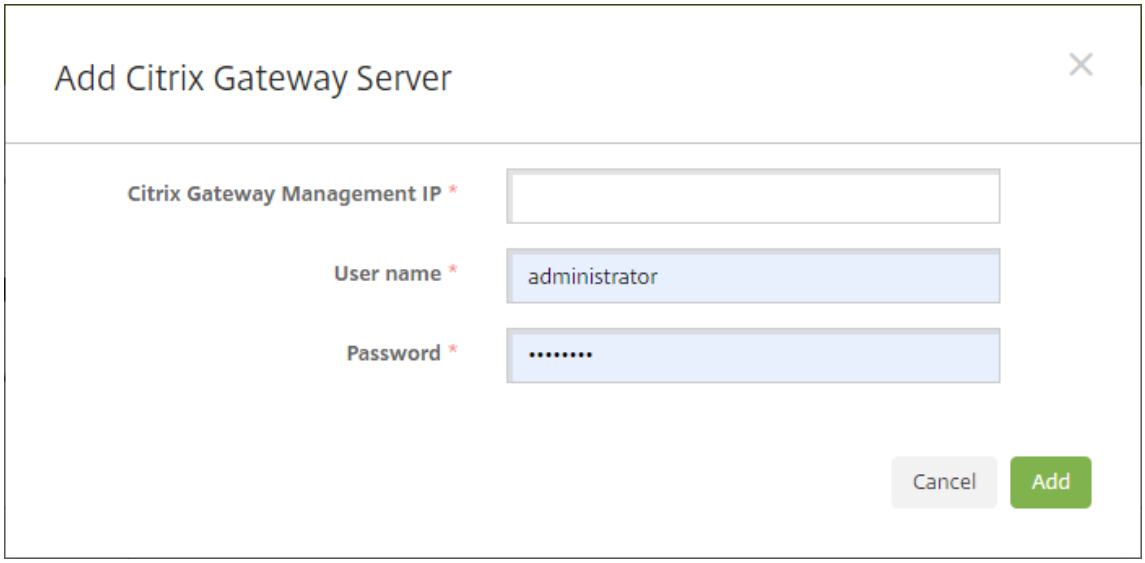
Réalisation de contrôles de connectivité pour NetScaler Gateway

1. Sur la page **Dépannage et support**, sous **Diagnostics**, cliquez sur **Test de la connectivité NetScaler Gateway**. La page **Test de la connectivité NetScaler Gateway** s'affiche. Le tableau est vide s'il n'y a pas de connexion entre Citrix Endpoint Management et NetScaler Gateway.



2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un serveur NetScaler Gateway** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Dans **Adresse IP de gestion de NetScaler Gateway**, entrez l'adresse IP de gestion du serveur exécutant NetScaler Gateway que vous voulez tester.

   Si vous effectuez un contrôle de connectivité pour un serveur NetScaler Gateway qui a déjà été ajouté, l'adresse IP est renseignée.

4. Tapez vos informations d'identification d'administrateur pour ce NetScaler Gateway.

   Si vous effectuez un contrôle de connectivité pour un serveur NetScaler Gateway qui a déjà été ajouté, le nom d'utilisateur est renseigné.

5. Cliquez sur **Ajouter**. La passerelle NetScaler Gateway est ajoutée au tableau sur la page **Test de la connectivité NetScaler Gateway**.

6. Sélectionnez le serveur NetScaler Gateway et cliquez sur **Tester la connectivité**. Les résultats du test s'affichent dans un tableau.

7. Sélectionnez un serveur dans le tableau des résultats du test pour afficher les résultats détaillés pour ce serveur.

Détails des tests de connectivité

Le tableau suivant répertorie les différents tests de connectivité que Citrix Endpoint Management peut effectuer et contient des détails sur chaque test.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Connectivité à	Adresse IP ou nom de domaine complet	Détails
Serveur de notification push Apple	api.push.apple.com	Vérifie la connectivité entre le serveur de notification push Apple et le nœud Citrix Endpoint Management. Le serveur de notification push Apple est requis pour envoyer des messages aux appareils iOS et macOS.
Serveur de notification push Apple Feedback	feedback.push.apple.com	Vérifie la connectivité entre le serveur Apple Feedback et le nœud Citrix Endpoint Management. Le serveur de notification push Apple Feedback vous fournit des informations sur les notifications à distance ayant échoué envoyées aux appareils iOS et macOS.
Serveur de licences Citrix	Adresse IP du serveur de licences	Vérifie la connectivité entre le serveur de licences Citrix et le nœud Citrix Endpoint Management. Les serveurs exécutant les produits Citrix se connectent au serveur de licences Citrix pour obtenir des licences.
NetScaler Gateway	Nom de domaine complet de NetScaler Gateway configuré dans Citrix Endpoint Management	Vérifie la connectivité entre NetScaler Gateway et le nœud Citrix Endpoint Management. NetScaler Gateway est utilisé par les applications clientes Citrix Endpoint Management (telles que Citrix Secure Mail et Citrix Secure Web) pour se connecter via un serveur VPN et accéder aux réseaux internes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Connectivité à	Adresse IP ou nom de domaine complet	Détails
Base de données	Adresse IP ou nom de domaine complet du serveur de base de données	Vérifie la connectivité entre la base de données Citrix Endpoint Management et le nœud Citrix Endpoint Management.
DNS (Système de nom de domaine)	Adresse IP configurée dans Citrix Endpoint Management	Vérifie la connectivité entre le serveur DNS et le nœud Citrix Endpoint Management.
Service Secure Ticket Authority	localhost	Vérifie la connexion du nœud Citrix Endpoint Management aux services d'authentification, aux services STA (Secure Ticket Authority) et aux services de cluster.
Serveur Firebase Cloud Messaging (FCM)		Vérifie la connectivité entre le serveur FCM et le nœud Citrix Endpoint Management. À l'aide de FCM, vous pouvez avertir une application cliente qu'un nouvel e-mail ou d'autres données sont disponibles pour la synchronisation. Vous pouvez envoyer des messages de notification pour stimuler l'engagement et la rétention des utilisateurs. FCM remplace Google Cloud Messaging (GCM).
Google Play	play.google.com	Vérifie la connectivité entre le serveur Google Store et le nœud Citrix Endpoint Management. Google Play est utilisé pour offrir des services qui incluent un magasin de mise à disposition d'applications d'entreprise gérées et privées.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Connectivité à	Adresse IP ou nom de domaine complet	Détails
iTunes Store/Achat en volume	vpp.itunes.apple.com	Vérifie la connectivité entre le serveur Apple Store et le nœud Citrix Endpoint Management. L'Apple Store est utilisé pour offrir des services qui incluent un magasin de mise à disposition d'applications d'entreprise gérées et privées.
LDAP	Adresse IP ou nom de domaine complet de LDAP configuré dans Citrix Endpoint Management	Vérifie la connectivité entre le serveur LDAP et le nœud Citrix Endpoint Management.
Serveur de notifications push Microsoft	sin.notifiy.windows.com	Vérifie la connectivité entre le serveur de notification Windows et le nœud Citrix Endpoint Management. Le serveur de notification Windows est utilisé pour envoyer des messages aux appareils Windows.
ShareFile Service	Adresse IP ou nom de domaine complet de ShareFile Service configuré dans Citrix Endpoint Management	Vérifie la connectivité entre ShareFile Service et Citrix Endpoint Management. ShareFile Service est une plateforme cloud sécurisée permettant aux entreprises de stocker et de partager des fichiers volumineux.
Windows Desktop/Tablet Store	windows.microsoft.com	Vérifie la connectivité entre Windows Desktop/Tablet Store et le nœud Citrix Endpoint Management. Windows Desktop/Tablet Store est utilisé pour offrir des services qui incluent un magasin de mise à disposition d'applications d'entreprise gérées et privées.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Connectivité à	Adresse IP ou nom de domaine complet	Détails
Service d'émission de jeton de sécurité Windows	login.live.com	Vérifie la connectivité entre le serveur d'émission de jeton de sécurité Windows et le nœud Citrix Endpoint Management. Le service d'émission de jeton de sécurité Windows prend en charge l'authentification à deux facteurs (domaine et jeton de sécurité) pour les appareils Windows.

Fournisseur de services mobiles

November 29, 2023

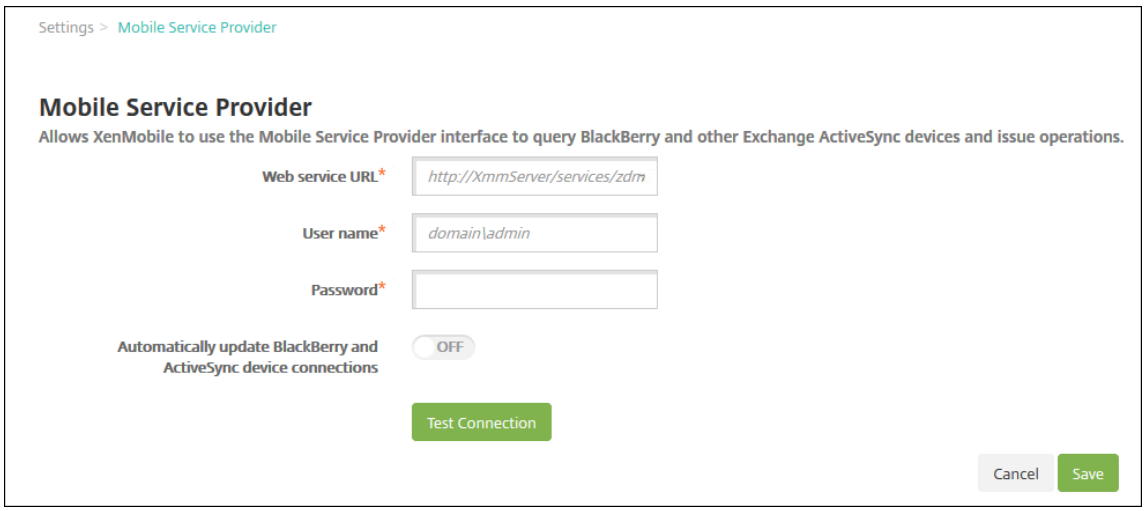
Vous pouvez configurer Citrix Endpoint Management de manière à ce qu'il utilise l'interface du fournisseur de services mobiles pour interroger les appareils BlackBerry et des appareils Exchange ActiveSync, ainsi que pour effectuer des opérations.

Supposons, par exemple, que votre organisation compte 1 000 utilisateurs et que chaque utilisateur utilise un ou plusieurs appareils. Une fois que vous avez demandé à tous les utilisateurs d'inscrire leurs appareils à Citrix Endpoint Management, la console Citrix Endpoint Management indique le nombre d'appareils que les utilisateurs inscrivent. Si vous configurez ce paramètre, vous pouvez déterminer le nombre d'appareils qui se connectent au serveur Exchange. Cela vous permet d'effectuer ce qui suit :

- Déterminer si certains utilisateurs n'ont pas encore inscrit leurs appareils.
- Émettre des commandes sur les appareils utilisateur se connectant à un serveur Exchange, telles que l'effacement de données.

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Dans **Serveur**, cliquez sur **Fournisseur de services mobiles**. La page **Fournisseur de services mobiles** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Pour configurer ces paramètres :

   - **URL du service Web :** entrez l'adresse URL du service Web, par exemple, `https://XmmServer/services/xdmservice`.
   - **Nom d'utilisateur :** entrez le nom d'utilisateur au format `domain\\admin`.
   - **Mot de passe :** entrez le mot de passe.
   - **Mettre à jour automatiquement les connexions aux appareils BlackBerry et ActiveSync :** activez cette option si vous souhaitez mettre à jour automatiquement les connexions aux appareils. La valeur par défaut est **Désactivé**.
   - Cliquez sur **Tester la connexion** pour vérifier la connexion.

4. Cliquez sur **Save**.

Rapports

March 1, 2024

Citrix Endpoint Management propose les rapports prédéfinis suivants qui vous permettent d'analyser vos déploiements d'applications et d'appareils. Chaque rapport s'affiche sous forme de tableau et de graphique. Vous pouvez trier et filtrer les tableaux par colonne. Vous pouvez sélectionner des éléments des graphiques à partir d'informations plus détaillées.

- **Nbre total de tentatives de déploiement d'application :** répertorie les applications déployées que les utilisateurs ont essayé d'installer sur leurs appareils.
- **Applications par plate-forme :** répertorie les applications et les versions des applications par plate-forme et version de l'appareil.
- **Application par type :** répertorie les applications par version, type et catégorie.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Inscription d'appareils :** répertorie tous les appareils inscrits.
- **Appareils et applications :** répertorie les appareils qui exécutent des applications gérées.
- **Appareils inactifs :** liste d'appareils sans activité pendant le nombre de jours spécifié par la propriété `device.inactivity.days.threshold` de Citrix Endpoint Management Server.
- **Appareils jailbreakés/rootés :** répertorie les appareils iOS rootés et les appareils Android jailbreakés.
- **Termes et conditions :** répertorie les utilisateurs qui ont accepté et refusé les conditions générales. Vous pouvez sélectionner des zones du graphique pour afficher plus de détails.
- **Top 10 des déploiements ayant échoué :** répertorie le top 10 des applications dont le déploiement a échoué.
- **Applications bloquées par appareil et utilisateur :** répertorie les applications figurant sur la liste rouge que les utilisateurs ont sur leur appareil.
- **Appareils non conformes :** répertorie les appareils qui ne répondent pas aux critères de conformité. Les critères déterminent si l'appareil est jailbreaké, la version du système d'exploitation en cours d'exécution et si l'appareil possède un code secret. Le rapport affiche également le nom d'utilisateur associé à l'appareil et indique si ce dernier est crypté. Pour les appareils iOS, la colonne de cryptage affiche N/A.

Vous pouvez exporter les données de chaque tableau au format .csv que vous pouvez ouvrir à l'aide de programmes tels que Microsoft Excel. Vous pouvez exporter le graphique de chaque rapport au format PDF.

L'onglet **Rapports** inclut les détails de l'appareil, tels que le numéro de série, l'IMEI/MEID, les applications et les connexions. Pour obtenir des rapports plus complets sur un appareil spécifique, accédez à **Gérer > Appareils**, cliquez sur l'appareil, cliquez sur **Afficher plus**, puis affichez la page **Détails de l'appareil**. La page **Détails de l'appareil** répertorie les propriétés de sécurité de l'appareil, les propriétés de l'appareil, les stratégies attribuées, les applications, les actions, les certificats, etc. Pour plus d'informations sur la page **Détails de l'appareil**, consultez la section Obtenir des informations sur les appareils.

Les éléments suivants déterminent la manière dont Citrix Endpoint Management collecte des informations sur les applications déployées ou installées sur des appareils gérés :

- Type d'appareil
- Méthode d'inscription
- Indique si la stratégie Inventaire des applications est déployée

Pour les appareils Android, le comportement est différent en fonction du type d'appareil et de la méthode d'inscription. Le tableau suivant indique où les applications sont répertoriées pour **Android Enterprise** (page **Détails de l'appareil**, Rapports ou Non disponible). Les listes d'applications incluent toutes les applications sauf indication contraire.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	MDM+MAM (toutes les applications)	MDM (toutes les applications)
Applications requises (stratégie d'inventaire des applications non déployée)	Page **Détails de l'appareil** et Rapports	Applications publiques ; page **Détails de l'appareil** et Rapports
Applications facultatives (stratégie d'inventaire des applications non déployée)	Non disponible	Non disponible
Applications requises (stratégie d'inventaire des applications non déployée)	Page **Détails de l'appareil** et Rapports	Page **Détails de l'appareil** et Rapports
Applications facultatives (stratégie d'inventaire des applications déployée)	Applications d'entreprise, MDX, publiques et liens Web ; Rapports	Page **Détails de l'appareil** et Rapports

Le tableau suivant indique où les applications sont répertoriées pour **Android (ancien administrateur de l'appareil)** (page **Détails de l'appareil**, Rapports ou Non disponible). Les listes d'applications incluent toutes les applications sauf indication contraire.

	MDM+MAM (toutes les applications)	MDM (applications publiques et d' entreprise)	MAM
Applications requises (stratégie d'inventaire des applications non déployée)	Page **Détails de l' appareil** et Rapports	Page **Détails de l' appareil** et Rapports	S/O
Applications facultatives (stratégie d'inventaire des applications non déployée)	Page **Détails de l' appareil** et Rapports	Page **Détails de l' appareil** et Rapports	Non disponible
Applications requises (stratégie d'inventaire des applications non déployée)	Page **Détails de l' appareil** et Rapports	Page **Détails de l' appareil** et Rapports	S/O

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	MDM+MAM (toutes les applications)	MDM (applications publiques et d' entreprise)	MAM
Applications facultatives (stratégie d'inventaire des applications déployée)	Page **Détails de l' appareil** et Rapports	Page **Détails de l' appareil** et Rapports	Non disponible

Pour les appareils iOS, le comportement est différent en fonction de la méthode d'inscription. Le tableau suivant indique où les applications sont répertoriées (page **Détails de l'appareil** ou Rapports). Les listes d'applications incluent toutes les applications sauf indication contraire.

	MDM+MAM (toutes les applications)	MDM (applications publiques et d' entreprise)	MAM (toutes les applications)
Applications requises (stratégie d'inventaire des applications non déployée)	Page **Détails de l' appareil** et Rapports	Page **Détails de l' appareil** et Rapports	Page **Détails de l' appareil** et Rapports ; ces applications sont affichées dans un état en attente (même si elles ne sont pas installées) ou restent dans un état en attente après avoir été installées manuellement.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	MDM+MAM (toutes les applications)	MDM (applications publiques et d' entreprise)	MAM (toutes les applications)
Applications facultatives (stratégie d'inventaire des applications non déployée)	Page **Détails de l' appareil** et Rapports	Page **Détails de l' appareil** et Rapports	Les applications Web, SaaS et liens Web sont répertoriées sur la page **Détails de l' appareil** en tant qu' applications installées ; elles ne sont pas répertoriées dans les rapports. Les applications d' entreprise, MDX et publiques ne sont pas répertoriées sur la page **Détails de l' appareil** après leur installation manuelle. Les applications ne sont pas répertoriées dans les rapports après avoir été installées manuellement.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	MDM+MAM (toutes les applications)	MDM (applications publiques et d' entreprise)	MAM (toutes les applications)
Applications requises (stratégie d'inventaire des applications non déployée)	Page **Détails de l' appareil** et Rapports	Page **Détails de l' appareil** et Rapports	La stratégie d' inventaire des applications ne peut pas être déployée sur les appareils. Les applications sont répertoriées sur la page **Détails de l' appareil** et dans les rapports. Ces applications sont affichées dans un état en attente (même si elles ne sont pas installées) ou restent dans un état en attente après avoir été installées manuellement.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	MDM+MAM (toutes les applications)	MDM (applications publiques et d'entreprise)	MAM (toutes les applications)
Applications facultatives (stratégie d'inventaire des applications déployée)	Page **Détails de l'appareil** et Rapports	Page **Détails de l'appareil** et Rapports	La stratégie d'inventaire des applications ne peut pas être déployée sur les appareils. Les applications Web, SaaS et liens Web sont répertoriées sur la page **Détails de l'appareil** en tant qu'applications installées ; elles ne sont pas répertoriées dans les rapports. Les applications d'entreprise, MDX et publiques ne sont pas répertoriées sur la page **Détails de l'appareil** après leur installation manuelle. Les applications ne sont pas répertoriées dans les rapports après avoir été installées manuellement.

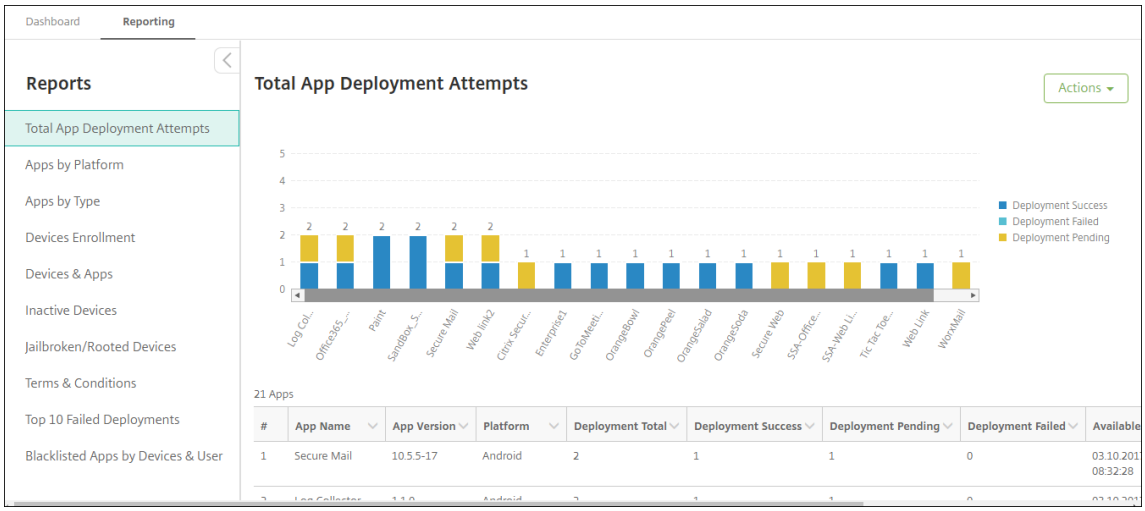
Pour les appareils macOS et Windows, Citrix Endpoint Management collecte un inventaire des applications *uniquement* lorsque la stratégie d'inventaire des applications est déployée.

Pour générer un rapport

1. Dans la console Citrix Endpoint Management, cliquez sur l'onglet **Analyser > Rapports**. La page **Rapports** s'affiche.

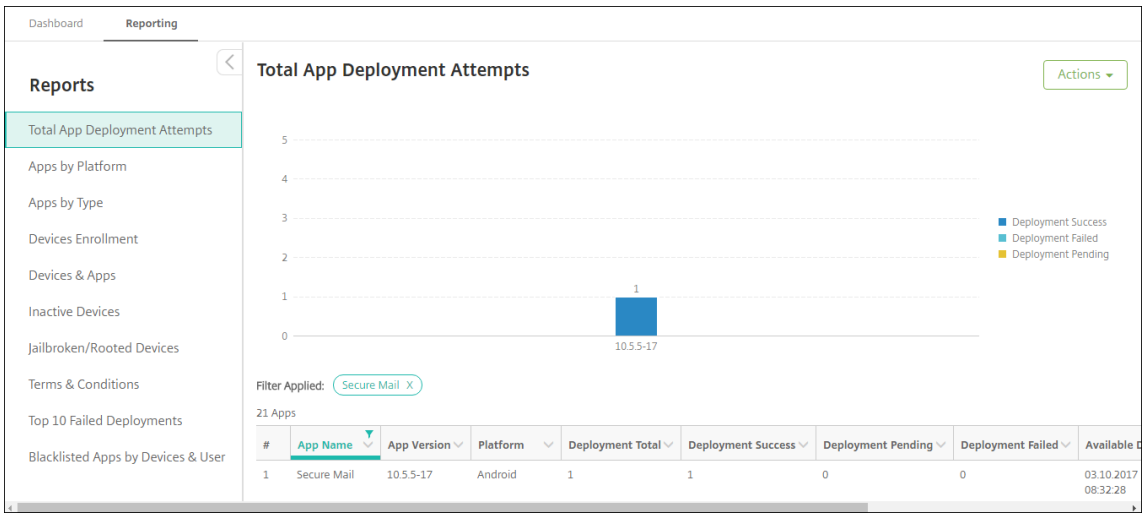
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Cliquez sur le rapport que vous souhaitez générer.



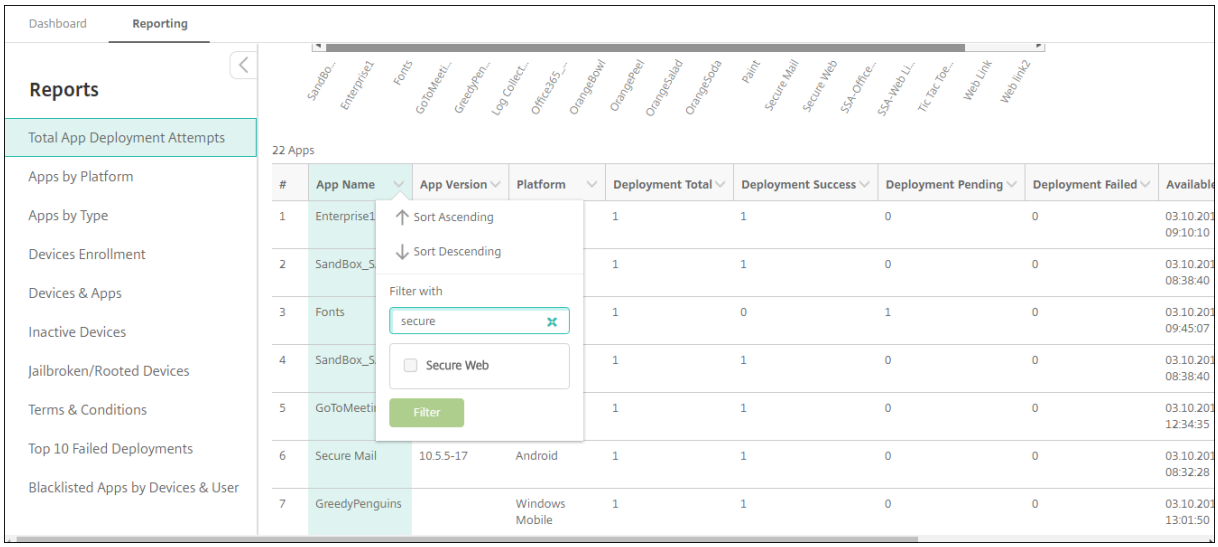
Pour afficher des détails supplémentaires dans un rapport

1. Cliquez sur les zones du graphique pour afficher des informations plus détaillées.



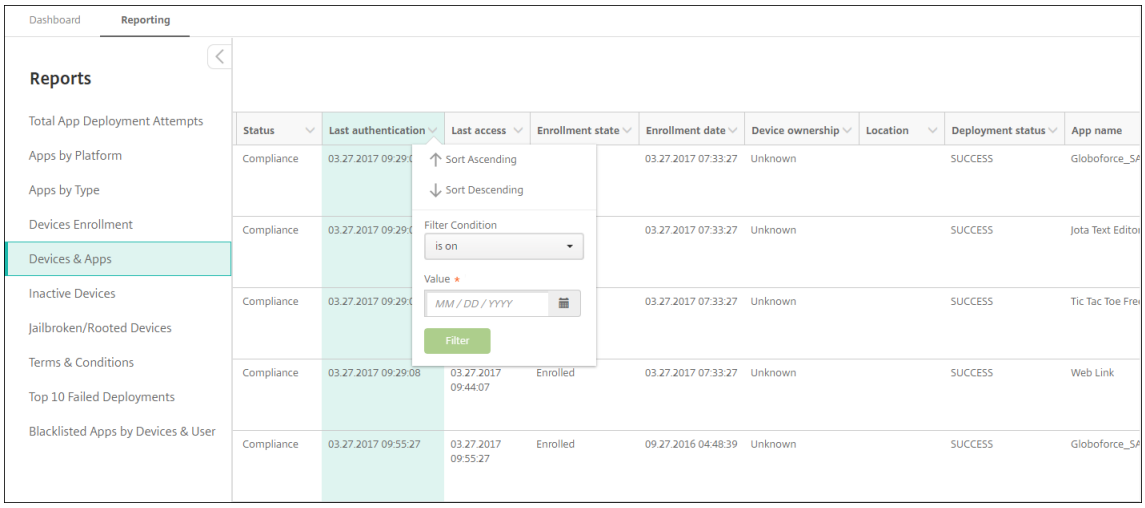
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour trier, filtrer ou rechercher une colonne d'un tableau, cliquez sur l'en-tête de la colonne



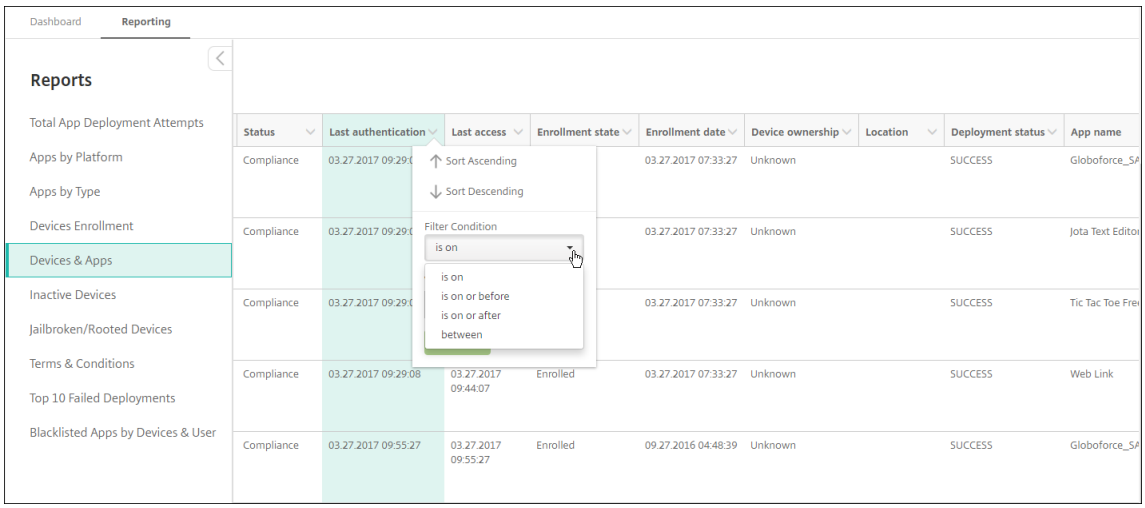
Pour filtrer le rapport par date

1. Cliquez sur un en-tête de colonne pour afficher les paramètres de filtre.

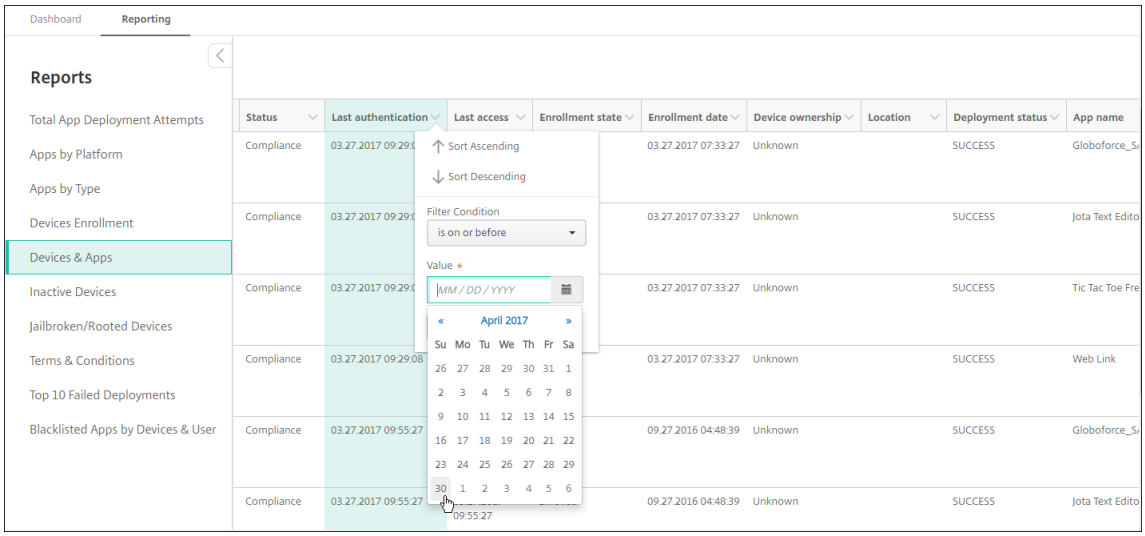


2. Dans **Condition de filtre**, choisissez la manière dont vous souhaitez restreindre les dates du rapport.

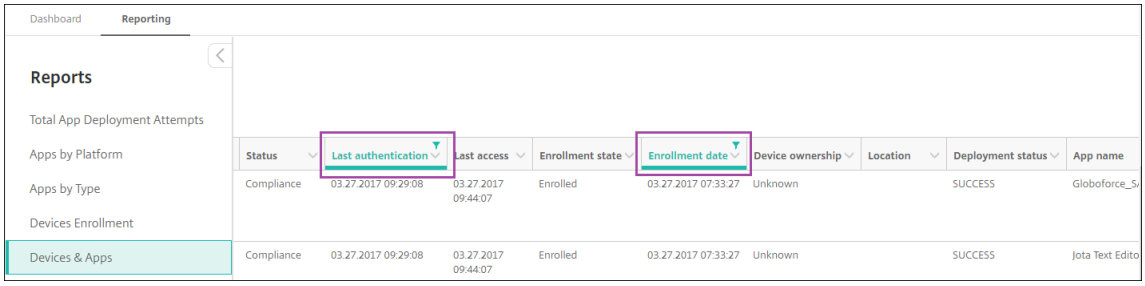
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Utilisez le sélecteur de date pour spécifier les dates.

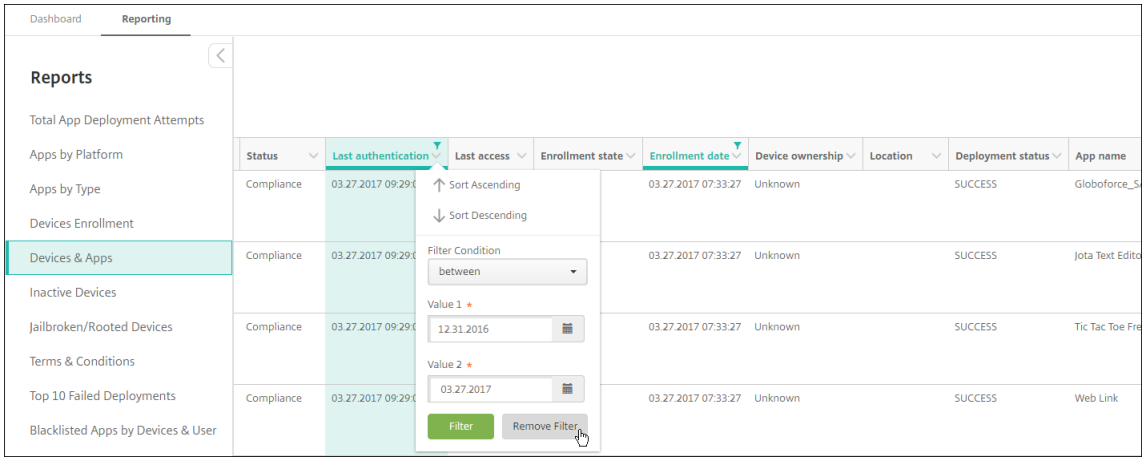


4. Une colonne avec un filtre de date s'affiche comme illustré dans l'exemple suivant.



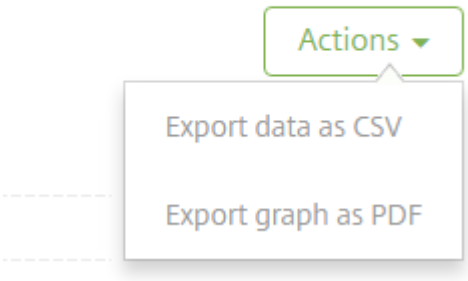
5. Pour supprimer un filtre, cliquez sur l'en-tête de colonne, puis cliquez sur **Supprimer le filtre**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pour exporter un graphique ou un tableau

- Pour exporter le graphique au format PDF, cliquez sur **Action** puis sur **Exporter graphique au format PDF**.
- Pour exporter les données du tableau au format CSV, cliquez sur **Action** puis sur **Exporter graphique au format CVS**.



API REST

March 1, 2024

Avec l'API REST d'Citrix Endpoint Management, vous pouvez :

- Appeler les services qui sont affichés dans la console Citrix Endpoint Management
- Appeler les services REST à l'aide d'un client REST quelconque

L'API n'exige pas de connexion à la console Citrix Endpoint Management pour appeler les services.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour consulter une liste complète des API actuellement disponibles, téléchargez le PDF Public API for REST Services.

Des API sont disponibles pour gérer vos terminaux mobiles et de bureau et configurer les paramètres de vos applications Workspace. Accédez à https://developer.cloud.com/citrixworkspace, puis à **Citrix Endpoint Management > Intégration d'applications mobiles**.

Autorisations requises pour accéder à l'API REST

Pour accéder à l'API REST, vous devez disposer de l'une des autorisations suivantes :

- Administrateur Citrix Cloud
- Autorisation d'accès à l'API publique définie dans le cadre de la configuration de l'accès basé sur rôle. Pour plus d'informations, veuillez consulter la section Configuration de rôles avec RBAC.
- Autorisation de super utilisateur

Pour accéder à l'API REST à l'aide de votre compte Citrix Cloud, générez les clés d'**API** :

1. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.
2. Sélectionnez **Accès aux API > Clients sécurisés**.
3. Donnez un nom à votre client sécurisé, puis cliquez sur **Créer un client**.

Citrix Cloud crée ensuite l'ID client sécurisé et la clé secrète client. Téléchargez une copie de ces informations et enregistrez-les en toute sécurité hors ligne pour votre référence. Citrix Cloud ne stocke pas les identificateurs uniques après la fermeture de la boîte de dialogue.

Pour appeler les services D'API REST

Vous pouvez appeler les services d'API REST à l'aide du client REST ou de commandes cURL. Les exemples suivants utilisent le client Advanced REST pour Chrome.

> **Remarque :**
>
> Dans les exemples suivants, modifiez le nom de l'hôte et le numéro de port afin qu'ils correspondent à votre environnement.

Connexion

L'exemple illustré ici couvre la connexion à l'aide d'un jeton récupéré via l'API Citrix Cloud.

URL : `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login/cloud`

Type de méthode : POST

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Type de contenu : application/json

Exemple de requête :

```
{

 "bearerToken": "eyJ0eOiJSUzJiibGcI1AiONiJ9.
    eyJkIjoMDExN1c2VIXiMzNDc1OTk4...qf0iQ"
 }

<!--NeedCopy-->
```

Vous devez récupérer le jeton du porteur à l'aide de l'API Citrix Cloud `https://trust.citrixworkspacesapi.net/Help/Api/POST-customer-tokens-clients`. Pour plus d'informations, consultez la documentation des développeurs.

Exemple de réponse :

```
{

 "auth_token": "q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"
 }

<!--NeedCopy-->
```

Informations connexes

- API REST Citrix Endpoint Management

ActiveSync Gateway

November 29, 2023

ActiveSync est un protocole de synchronisation des données mobiles développé par Microsoft. ActiveSync synchronise les données avec les périphériques portables et ordinateurs de bureau (ou portables).

Vous pouvez configurer des règles ActiveSync Gateway dans Citrix Endpoint Management. ActiveSync Gateway conserve une liste d'ID ActiveSync pour tous les appareils configurés dans Citrix Endpoint Management. En fonction des règles que vous configurez, vous pouvez autoriser ou refuser aux appareils l'accès aux données ActiveSync, en fonction de ces ID ActiveSync. Par exemple, si vous activez la règle **Applications requises manquantes**, Citrix Endpoint Management vérifie la stratégie d'accès aux applications requises. Si les applications requises sont manquantes, la stratégie refuse l'

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

accès aux données ActiveSync. Pour chaque règle, vous avez le choix entre **Autoriser** ou **Refuser**. Le paramètre par défaut est **Autoriser**.

Pour plus d'informations sur la stratégie d'accès aux applications, consultez la section Stratégies d'accès aux applications.

Citrix Endpoint Management prend en charge les règles suivantes :

Appareils anonymes : vérifie si un appareil est en mode anonyme. Cette vérification est disponible si Citrix Endpoint Management ne parvient pas à authentifier à nouveau l'utilisateur lorsqu'un appareil tente de se reconnecter.

Applications sur liste noire : vérifie si un appareil dispose d'applications interdites, telles que définies dans une stratégie d'accès aux applications.

Autorisation et refus implicites : cette action est la valeur par défaut pour ActiveSync Gateway. La passerelle crée une liste d'appareils de tous les appareils qui ne répondent pas à tous les critères de règle de filtre. La passerelle autorise ou refuse les connexions basées sur cette liste. Si aucune règle ne correspond, la valeur par défaut est **Autorisation implicite**.

Appareils inactifs : vérifie si un appareil est inactif, tel que cela est défini par le paramètre **Nombre de jours maximum d'inactivité** dans la boîte de dialogue **Propriétés du serveur**.

Applications requises manquantes : vérifie si des applications nécessaires sont manquantes sur un appareil, tel que cela est défini dans une stratégie d'accès aux applications.

Applications non suggérées : vérifie si un appareil dispose d'applications non suggérées, telles que définies dans une stratégie d'accès aux applications.

Mot de passe non conforme : vérifie si le mot de passe utilisateur est conforme. Sur les appareils iOS et Android, Citrix Endpoint Management peut déterminer si le mot de passe actuel de l'appareil est conforme à la stratégie de code secret envoyée à l'appareil. Par exemple, sur iOS, l'utilisateur dispose de 60 minutes pour définir un mot de passe si Citrix Endpoint Management envoie une stratégie de code secret à l'appareil. Avant qu'un mot de passe ne soit défini par l'utilisateur, le code secret peut ne pas être conforme.

Appareils non conformes : vérifie si un appareil n'est pas conforme, en fonction de la propriété de l'appareil Non conforme. Cette propriété est généralement modifiée par les actions automatisées ou parce qu'un tiers utilise les API Citrix Endpoint Management.

État révoqué : vérifie si le certificat de l'appareil a été révoqué. Un appareil révoqué ne peut pas se réinscrire tant qu'il n'a pas été à nouveau autorisé.

Appareils Android rootés et iOS jailbreakés : vérifie si un appareil Android ou iOS est rooté ou jailbreaké.

Appareils non gérés : vérifie si un appareil est toujours dans un état géré, sous le contrôle d'Citrix Endpoint Management. Par exemple, un appareil inscrit en mode MAM ou un appareil non inscrit n'

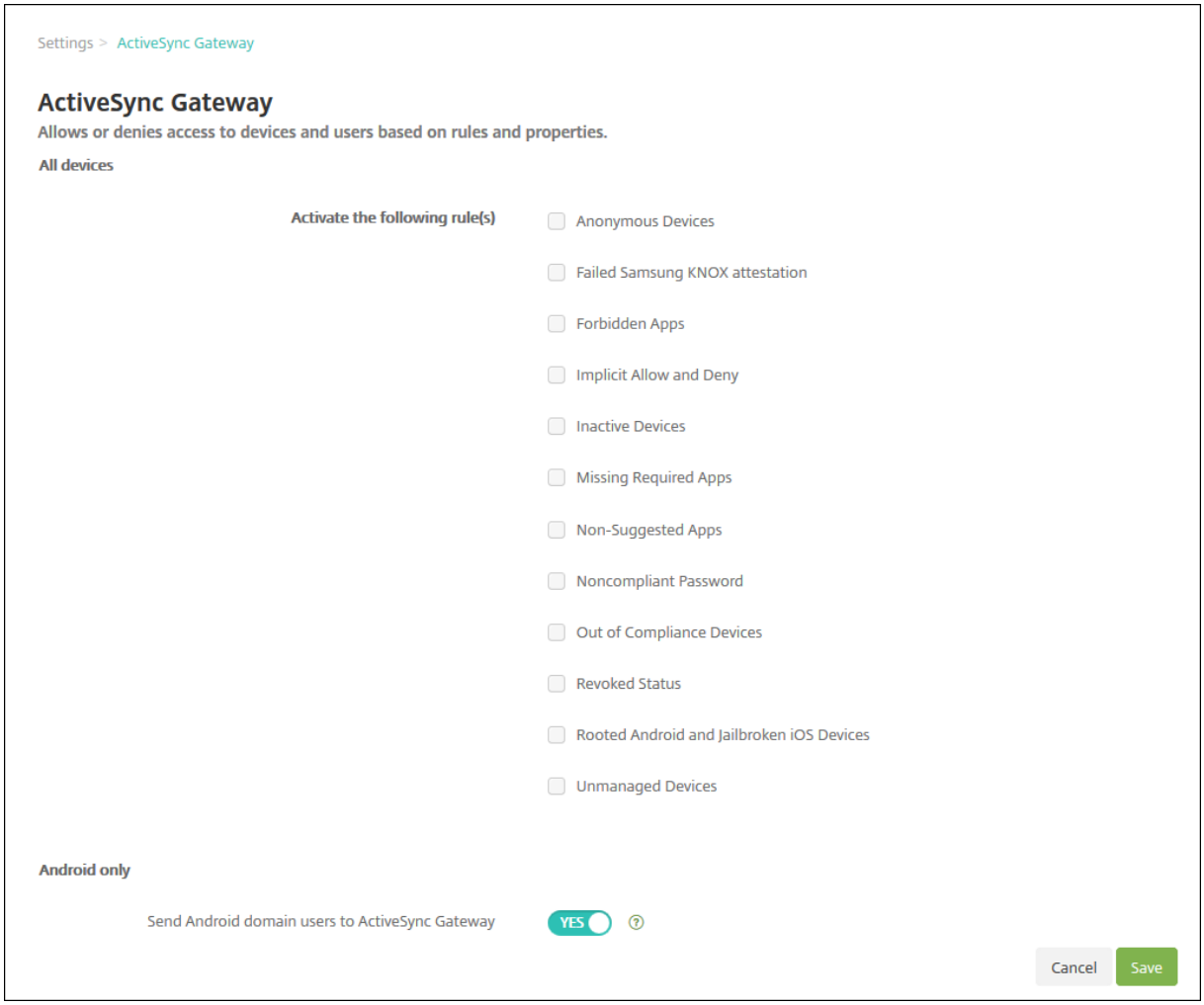
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

est pas géré.

Envoyer les utilisateurs Android à ActiveSync Gateway : cliquez sur **OUI** pour que Citrix Endpoint Management envoie le nom d'utilisateur et l'ID ActiveSync des propriétaires d'appareils Android à ActiveSync Gateway Désactivez cette fonctionnalité, sauf si vous exécutez une configuration héritée. Dans les configurations plus récentes, cette fonctionnalité permet à tout appareil d'accéder aux données ActiveSync tant que le nom d'utilisateur associé à l'appareil existe sur la passerelle.

Pour configurer les paramètres ActiveSync Gateway

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Serveur**, cliquez sur **ActiveSync Gateway**. La page **ActiveSync Gateway** s'affiche.



1. Dans **Activer la ou les règles suivantes**, sélectionnez une ou plusieurs règles à activer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Dans **Android uniquement**, sous **Envoyer les utilisateurs de domaine Android vers ActiveSync Gateway**, cliquez sur **OUI** pour vous assurer qu'Citrix Endpoint Management envoie les informations de l'appareil Android à ActiveSync Gateway.
3. Cliquez sur **Save**.

Citrix Endpoint Management Connector pour Exchange ActiveSync

March 1, 2024

XenMobile Mail Manager est maintenant nommé Citrix Endpoint Management Connector pour Exchange ActiveSync. Pour plus de détails sur le portefeuille unifié de Citrix, consultez le guide des produits Citrix.

Le connecteur étend les fonctionnalités de Citrix Endpoint Management des façons suivantes :

- Contrôle d'accès dynamique des appareils EAS (Exchange Active Sync). L'accès des appareils EAS aux services Exchange peut être automatiquement autorisé ou bloqué.
- Capacité d'Citrix Endpoint Management à accéder aux informations de partenariat d'appareil EAS fournies par Exchange.
- Capacité d'Citrix Endpoint Management à effacer un appareil mobile en fonction de l'état EAS.
- Capacité d'Citrix Endpoint Management à accéder à des informations sur des appareils Blackberry, et à réaliser des opérations de contrôle telles que l'effacement (Wipe) et la réinitialisation du mot de passe (ResetPassword).

Pour effacer un appareil en fonction de l'état EAS, configurez une action automatisée avec un déclencheur ActiveSync. Consultez la section Actions automatisées.

> **Important :**
>
> À compter d'octobre 2022, les connecteurs Citrix Endpoint Management et NetScaler Gateway pour Exchange ActiveSync ne prendront plus en charge Exchange Online en raison des modifications d'authentification annoncées par Microsoft ici. Le connecteur Citrix Endpoint Management pour Exchange continuera de fonctionner avec Microsoft Exchange Server (déploiement local).

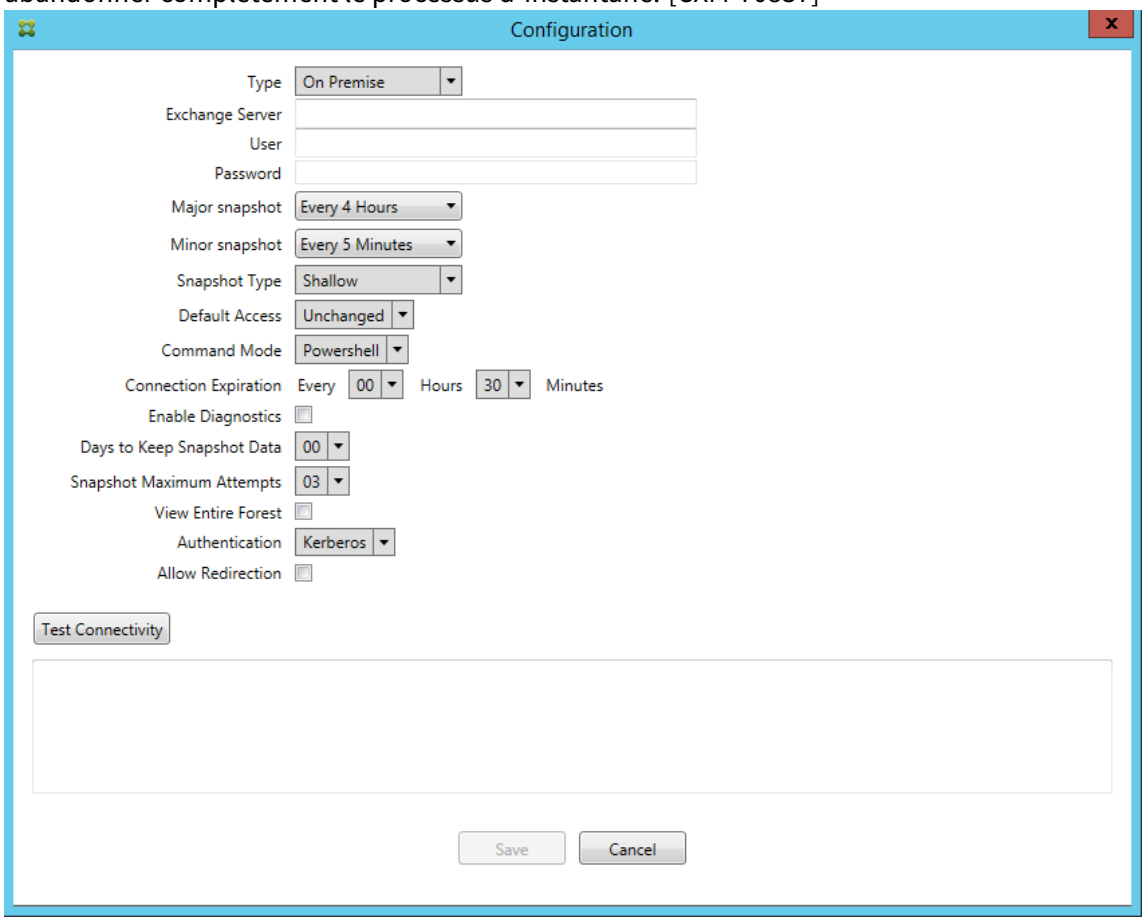
Nouveautés dans la version 10.1.10

Les problèmes suivants ont été résolus dans la version 10.1.10 :

- Les clients qui rencontrent des problèmes réseau fréquents peuvent ne pas être en mesure de réaliser un instantané au cours des trois tentatives qui étaient précédemment fournies. Avec cette version, un administrateur peut configurer le nombre maximum de tentatives (1-10).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ce correctif permet à un instantané de subir plusieurs interruptions de communication sans abandonner complètement le processus d'instantané. [CXM-70837]



- Dans les versions précédentes, le type d'instantané n'apparaissait pas dans la liste des configurations Exchange. Maintenant, le type d'instantané apparaît. [CXM-70846]
- L'exception PSRemotingTransport signalée par PowerShell indique que la session vers Exchange n'est plus viable. L'état est ajouté par défaut à la liste Erreurs critiques dans le fichier de configuration. Ce faisant, lorsque l'exception PSRemotingTransport est détectée, la connexion est marquée comme une Erreur à des fins d'élimination ultérieure. La communication suivante utilise une connexion valide ou crée une connexion. [XMHELP-2184, CXM-70836]
- Lorsqu'une modification de configuration est enregistrée, il est possible que les composants internes configurés précédemment n'aient pas tous été supprimés correctement avant de charger la nouvelle configuration. Ce problème peut conduire à un comportement imprévisible. Le comportement dépend de la modification spécifique et si la modification est en conflit avec la configuration précédente. Dans cette version, tous les composants internes sont supprimés avant de charger la nouvelle configuration. [XMHELP-2259, CXM-71388]

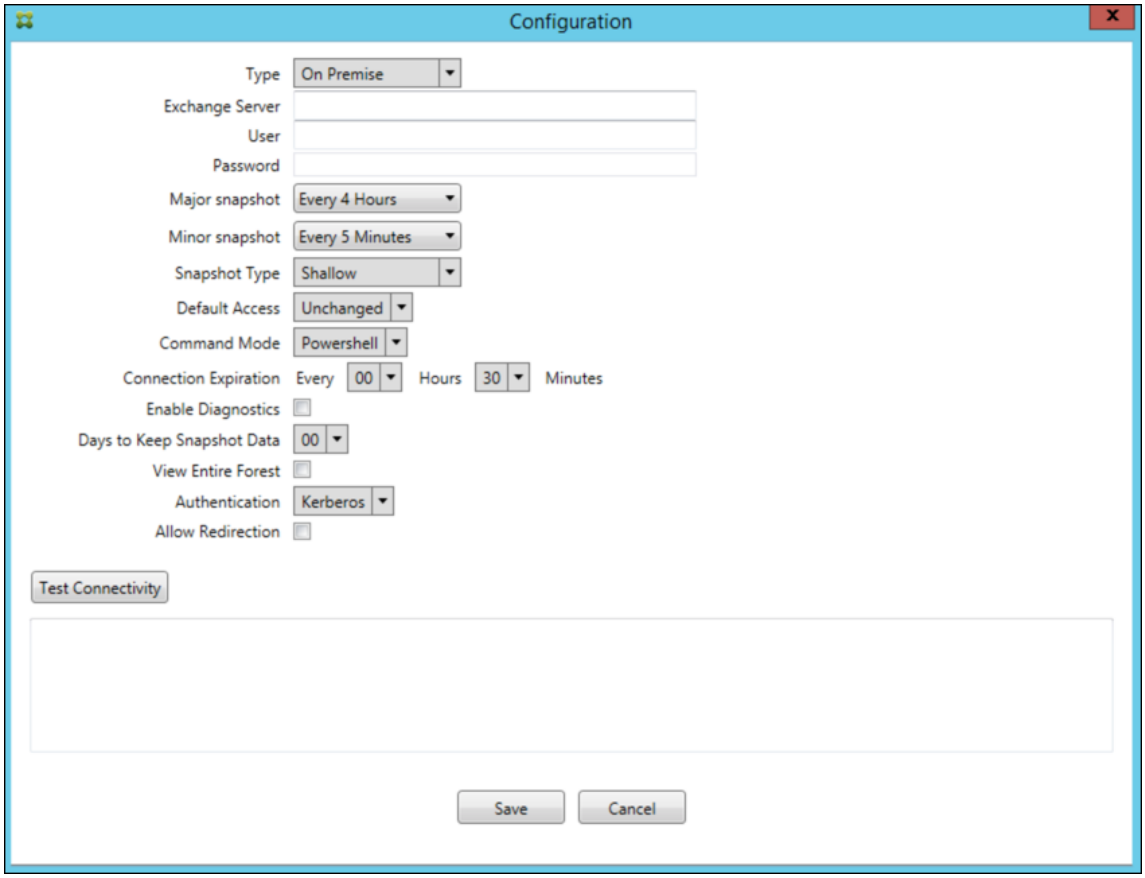
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nouveautés dans la version 10.1.9

Les problèmes suivants ont été résolus dans la version 10.1.9 :

- Les modifications de configuration sont désormais gérées de manière plus cohérente. Lorsque le service détecte un changement de configuration, chaque sous-système interne est arrêté, ce qui signifie que tout traitement actif ou planifié est interrompu. Ensuite, la nouvelle configuration est chargée et les sous-systèmes sont redémarrés, ce qui signifie que tous les programmes et autres infrastructures internes sont rétablis avec de nouveaux paramètres. Ce problème corrige un problème connu dans la version 10.1.8. [CXM-47709, CXM-61330]
- Lors d'une mise à niveau, la configuration de base de données existante n'était pas fusionnée dans le nouveau fichier de configuration. La configuration de base de données est maintenant fusionnée dans le fichier de configuration mis à niveau. [CXM-49326]
- Dans les fichiers de diagnostic liés aux instantanés, les en-têtes de colonne étaient manquants. Les en-têtes sont restaurés. [CXM-62680]
- Lors de la mise à niveau à partir d'une version précédente, la section par défaut du fichier de configuration était remplacée par la section analogue du fichier de configuration utilisé. Ce problème empêchait les ajouts ou les améliorations à la section par défaut d'être chargés par le service après la mise à niveau. À partir de cette version, la section par défaut reflète toujours la dernière configuration. [CXM-62681]
- Les administrateurs ne peuvent plus accéder à certaines options en appuyant sur Maj lors de l'exécution de l'application. Ces options étaient auparavant disponibles avec l'autorisation Citrix. Certaines options sont désormais entièrement disponibles, telles que Autoriser la redirection, tandis que d'autres, telles que Détection de blocage et Correction de comptage, sont obsolètes. [CXM-62767]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Nouveautés dans les versions précédentes

La section suivante répertorie les nouvelles fonctionnalités et les problèmes résolus dans les versions antérieures du connecteur Citrix Endpoint Management pour Exchange ActiveSync.

Nouveautés dans la version 10.1.8

- Il est possible qu'Exchange limite trop fréquemment l'envoi de commandes par le service de Citrix Endpoint Management Connector pour Exchange ActiveSync. Ce problème est un comportement courant dans les connexions à Office 365. Avec cette limitation, le service doit se mettre en pause pendant une période spécifiée avant d'envoyer la commande suivante. La console Configurer affiche désormais le temps de pause restant. [CXM-48044]
- Lorsque des modifications sont apportées aux sections « Watchdog » et/ou « SpecialistsDefaults » du fichier de configuration (config.xml), les modifications ne sont pas reflétées dans le fichier de configuration après une mise à niveau. Avec cette version, les modifications sont fusionnées correctement dans le nouveau fichier de configuration. [CXM-52523]
- Plus de détails ont été ajoutés aux analyses envoyées à Google Analytics, notamment concernant les instantanés. [CXM-56691]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- La fonctionnalité de connectivité de test Exchange tentait d'initialiser la connexion une seule fois. Étant donné que les connexions Office 365 peuvent être limitées, il était possible qu'une connectivité de test semble échouer lors de la limitation. Le connecteur Citrix Endpoint Management pour Exchange ActiveSync tente désormais d'initier une connexion jusqu'à trois fois. [CXM-58180]
- Afin d'appliquer des stratégies sur Exchange, le connecteur Citrix Endpoint Management pour Exchange ActiveSync doit compiler une commande **Set-CASMailbox** qui inclut tous les appareils concernés pour chaque boîte aux lettres, dans deux listes : autoriser et bloquer. Si un appareil n'est pas inclus dans l'une ou l'autre des listes, Exchange revient à son état d'accès par défaut. Si cet état d'accès par défaut est différent de l'état souhaité pour un appareil, cet appareil n'est plus conforme. Par conséquent, un utilisateur peut perdre l'accès à son courrier électronique si l'état d'accès par défaut d'Exchange est bloqué alors qu'il devrait être autorisé. Ou bien, un utilisateur dont l'accès au courrier électronique devrait être bloqué peut se voir accorder l'accès. Le connecteur Citrix Endpoint Management pour Exchange ActiveSync garantit désormais que tous les appareils avec un état souhaité valide sont inclus dans chaque commande **Set-CasMailbox**. [CXM-61251]

Le problème suivant est connu dans la version 10.1.8 :

Si un administrateur apporte une modification dans l'application Configurer qui modifie les données de configuration, alors que le service effectue des opérations de longue durée, telles qu'un instantané ou une évaluation des stratégies, le service peut entrer dans un état indéterminé. Un symptôme peut être que les modifications de stratégie ne sont pas traitées ou que les instantanés ne sont pas initiés. Pour rétablir l'état de fonctionnement du service, il doit être redémarré. Vous devrez peut-être utiliser le gestionnaire de services Windows pour mettre fin au processus avant de démarrer le service. [CXM-61330]

Nouveautés dans la version 10.1.7

- XenMobile Mail Manager est maintenant nommé Citrix Endpoint Management Connector pour Exchange ActiveSync.
- L'option **Disable Pipelining** dans la boîte de dialogue de configuration Exchange est désormais obsolète. Vous pouvez obtenir la même fonctionnalité en configurant plusieurs étapes pour chaque commande dans le fichier config.xml. [CXM-54593]

Les problèmes suivants ont été résolus dans la version 10.1.7 :

- Dans la fenêtre de l'historique des instantanés, les messages d'erreur peuvent être affichés avec peu de contexte. À présent, les messages d'erreur sont précédés du contexte dans lequel les erreurs se sont produites. [CXM-49157]
- Le fichier XmmGoogleAnalytics.dll ne possédait pas la version de fichier correspondante à la version commerciale. [CXM-52518]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Pour améliorer les diagnostics, nous avons récemment modifié le format de chaîne relatif à une liste d'ID d'appareils utilisés pour définir l'état Autorisé/Bloqué de la boîte aux lettres. Cependant, si un nombre trop important d'appareils est spécifié, la taille de chaîne maximale est dépassée. Nous utilisons maintenant une structure de données de tableau interne. Cette structure n'a pas de limite de taille et formate également les données de manière appropriée à des fins de diagnostic. [CXM-52610]
- Lorsque des stratégies d'appareil qui ne sont pas synchronisées avec Exchange sont détectées, leurs commandes peuvent inclure des appareils n'appartenant pas à la boîte aux lettres appropriée. Citrix Endpoint Management Connector pour Exchange ActiveSync s'assure désormais que les commandes destinées à Exchange représentent uniquement les appareils appartenant à leurs boîtes aux lettres respectives. [CXM-54842]
- Dans certains environnements, un assembly Microsoft n'est pas disponible. L'assembly requis est maintenant explicitement installé avec l'application. [CXM-55439]
- Si les noms uniques d'appareils ou de boîtes aux lettres comportent des espaces entre le nom de l'attribut et le signe égal ou des espaces après le signe égal et avant la valeur, Citrix Endpoint Management Connector pour Exchange ActiveSync peut ne pas faire correspondre un appareil à sa boîte aux lettres, et inversement. Par conséquent, certains appareils et/ou boîtes aux lettres peuvent être rejeté(e)s lors du rapprochement des instantanés. [CXM-56088]

> **Remarque :**
>
> Les sections suivantes font référence à Citrix Endpoint Management Connector pour Exchange ActiveSync sous son ancien nom XenMobile Mail Manager. Le nom a changé à partir de la version 10.1.7.

Mise à jour dans la version 10.1.6.20

Une mise à jour vers 10.1.6 contient le correctif suivant dans la version 10.1.6.20 :

- Lorsque des stratégies d'appareil qui ne sont pas synchronisées avec Exchange sont détectées, leurs commandes peuvent inclure des appareils n'appartenant pas à la boîte aux lettres appropriée. XenMobile Mail Manager s'assure désormais que les commandes destinées à Exchange représentent uniquement les appareils appartenant à leurs boîtes aux lettres respectives. [CXM-54842]

Nouveautés dans la version 10.1.6

XenMobile Mail Manager version 10.1.6 contient les améliorations et les problèmes résolus suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- La fenêtre d'historique des instantanés entre parfois dans un état où la fenêtre n'est plus mise à jour. Le mécanisme d'actualisation de Windows a été amélioré pour une mise à jour plus fiable. [CXM-47983]
- Deux modes et chemins de code distincts étaient utilisés pour les instantanés partitionnés et non partitionnés. Étant donné que les instantanés non partitionnés sont équivalents aux instantanés partitionnés avec une configuration utilisant une seule partition "*", le mode instantané non partitionné a été éliminé. Le mode instantané par défaut est désormais partitionné avec 36 partitions (0-9, A-Z). [CXM-49093]
- Dans la fenêtre de l'historique des instantanés, les messages d'erreur sont écrasés par les messages d'état. Désormais, XenMobile Mail Manager fournit deux champs distincts pour que les utilisateurs puissent voir l'état et les erreurs simultanément. [CXM-51942]
- Lors de la connexion à Exchange Online (Office 365), les requêtes liées aux images instantanées pouvaient entraîner des données tronquées. Ce problème peut se produire lorsque XenMobile Mail Manager exécute un script en pipeline à plusieurs commandes. La commande en amont ne peut pas transmettre les données assez rapidement à la commande en aval, qui termine alors le travail prématurément. En conséquence, les données sont incomplètes. XenMobile Mail Manager peut maintenant reproduire le pipeline lui-même et attendre que la commande en amont soit effectuée avant d'appeler la commande en aval. Ce changement devrait entraîner le traitement et la capture de toutes les données. [CXM-52280]
- Si une erreur non résolue se produit dans une commande de mise à jour de stratégie vers Exchange, la même commande est renvoyée à la file d'attente de travail à plusieurs reprises pendant une longue période. Cette situation entraînait l'envoi de la commande à Exchange à plusieurs reprises. Dans cette version de XenMobile Mail Manager, une commande entraînant une erreur est renvoyée à la file d'attente uniquement un nombre discret de fois. [CXM-52633]
- Si une mise à jour de stratégie pour une boîte aux lettres spécifique impliquait l'autorisation ou le blocage de tous les appareils : la commande **Set-CASMailbox** émise échouait car la liste vide était convertie en une chaîne vide au lieu de **NULL**. Désormais, les données correctes sont envoyées. [CXM-53759]
- Lors du traitement d'un nouvel appareil, Exchange peut renvoyer l'état "DeviceDiscovery"pendant un certain temps (généralement 15 minutes). XenMobile Mail Manager ne traitait pas spécifiquement cet état. XenMobile Mail Manager gère maintenant cet état. Dans l'onglet Monitor de l'interface utilisateur, les utilisateurs peuvent filtrer les appareils dans cet état. [CXM-53840]
- XenMobile Mail Manager ne vérifiait pas la possibilité d'écrire dans la base de données XenMobile Mail Manager. Par conséquent, si les autorisations étaient restreintes, le comportement était imprévisible. XenMobile Mail Manager capture et valide désormais les autorisations requises à partir de la base de données. XenMobile Mail Manager indique les autorisations restreintes lors du test de la connexion (message affiché) ou dans l'indicateur Base de données (survol du message) en bas de la fenêtre principale de configuration. [CXM-54219]
- Selon la charge de travail en cours, lorsqu'il est dirigé vers XenMobile Mail Manager, le service

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

peut ne pas s'arrêter rapidement. Par conséquent, le service semble être dans un état qui ne répond pas. Les améliorations permettent d'interrompre les tâches en cours, entraînant un arrêt plus rapide. [CXM-54282]

Nouveautés dans la version 10.1.5

XenMobile Mail Manager version 10.1.5 contient les problèmes résolus suivants :

- Lorsque Exchange applique une limitation aux activités de XenMobile Mail Manager, rien n'indique (en dehors des journaux) que la limitation est en cours. Avec cette version, un utilisateur peut survoler l'instantané actif et un état de limitation apparaît. De plus, pendant que XenMobile Mail Manager est limité, le début d'un instantané majeur est interdit jusqu'à ce que Exchange mette fin à la limitation. [CXM-49617]
- Si XenMobile Mail Manager est limité par Exchange au cours d'un instantané majeur : il est possible qu'un délai insuffisant s'écoule avant la prochaine tentative d'instantané. Ce problème entraîne une limitation supplémentaire et l'échec de l'instantané. XenMobile Mail Manager attend maintenant le délai minimum spécifié par Exchange entre les tentatives d'instantanés. [CXM-49618]
- Lorsque les diagnostics sont activés, le fichier de commandes affiche les commandes **Set-CasMailbox** qui ne contiennent pas de tirets avant chaque nom de propriété. Ce problème se produit uniquement lors du formatage du fichier de diagnostics et non de la commande elle-même vers Exchange. L'absence de tiret empêche un utilisateur de couper la commande et de la coller directement dans une invite PowerShell de test ou de validation. Les tirets ont été ajoutés. [CXM-52520]
- Si une identité de boîte aux lettres est au format `lastname, firstname`, Exchange ajoute une barre oblique inverse avant la virgule lors du renvoi de données à partir d'une requête. Cette barre oblique inverse doit être supprimée lorsque XenMobile Mail Manager utilise l'identité pour demander davantage de données. [CXM-52635]

Limitation connue

> **Remarque :**
>
> La limitation suivante est résolue dans la version 10.1.6.

XenMobile Mail Manager a une limitation connue qui peut entraîner l'échec des commandes Exchange. Pour appliquer des modifications de stratégie à Exchange, une commande **Set_CASMailbox** est émise par XenMobile Mail Manager. Cette commande peut utiliser deux listes d'appareils : une pour autoriser et une pour bloquer. La commande est appliquée aux appareils associés à une boîte aux lettres.

Ces listes sont limitées à 256 caractères chacune par l'API Microsoft. Si l'une de ces listes dépasse la limite, la commande échoue dans son intégralité, empêchant la définition des stratégies pour ces

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

appareils de la boîte aux lettres. L'erreur signalée, qui apparait dans les journaux XenMobile Mail Manager, ressemble à ceci. L'exemple représente la liste bloquée.

"Message:'Cannot bind parameter 'ActiveSyncBlockedDeviceIDs'to the target. Exception setting "ActiveSyncBlockedDeviceIDs": "The length of the property is too long. The maximum length is 256 and the length of the value provided is …"

Les longueurs d'ID d'appareil peuvent varier, mais un bon principe à suivre est qu'environ 10 appareils Autorisés ou Bloqués simultanément peuvent dépasser la limite. Bien qu'il soit rare que de nombreux appareils soient associés à une boîte aux lettres spécifique, c'est un scénario possible. Tant que XenMobile Mail Manager n'est pas amélioré pour gérer un tel scénario, nous vous recommandons de limiter le nombre d'appareils associés à un utilisateur et à une boîte aux lettres à 10 ou moins. [CXM-52633]

Nouveautés dans la version 10.1.4

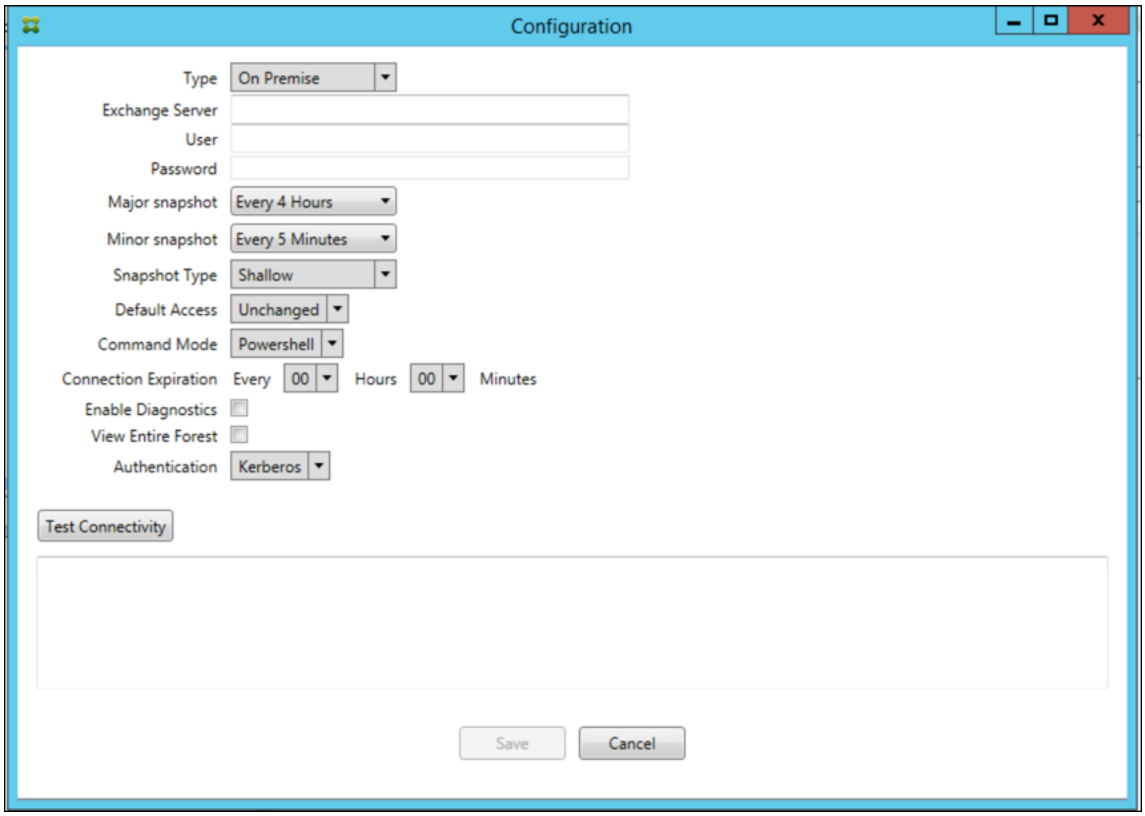
XenMobile Mail Manager version 10.1.4 contient les problèmes résolus suivants :

- En raison de leur faible niveau de sécurité, TLS 1.0 et TLS 1.1 ont été déclarés obsolètes par le PCI Council. La prise en charge de TLS 1.2 est ajoutée à XenMobile Mail Manager. [CXM-38573, CXM-32560]
- XenMobile Mail Manager inclut un nouveau fichier de diagnostic. Lorsque l'option **Enable Diagnostics** est sélectionnée dans la spécification Exchange, un nouveau fichier d'historique des instantanés est généré. À chaque tentative d'instantané, une ligne est ajoutée au fichier avec les résultats de l'instantané. [CXM-49631]
- Dans le fichier de diagnostic Commands, la liste des appareils autorisés ou bloqués n'apparaît pas pour la commande **Set-CASMailbox**. Au lieu de cela, le nom de classe interne était affiché dans le fichier pour les arguments associés. XenMobile Mail Manager affiche désormais la liste des appareils sous forme de liste délimitée par des virgules. [CXM-50693]
- Lorsqu'une tentative d'acquisition d'une connexion à Exchange échoue en raison d'une spécification incorrecte : Le message d'erreur est remplacé par un message incorrect : « All connections in use ». Des messages plus descriptifs apparaissent maintenant, tels que "All connections are inoperable", "Connection pool is empty", "All connections are throttled"et "No available connections". [CXM-50783]
- Dans certains cas, les commandes Autoriser/Bloquer/Effacer sont mises en file d'attente plusieurs fois dans le cache interne de XenMobile Mail Manager. Ce problème provoque un retard dans la commande envoyée à Exchange. XenMobile Mail Manager ne met en file d' attente qu'une seule instance de chaque commande. [CXM-51524]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nouveautés dans la version 10.1.3

- **Prise en charge de Google Analytics :** nous souhaitons savoir comment vous utilisez XenMobile Mail Manager afin de pouvoir nous concentrer sur l'amélioration du produit.
- **Paramètre d'activation des diagnostics :** une case à cocher **Enable Diagnostic** s'affiche dans la console Configure de la boîte de dialogue **Configuration**.



Problèmes résolus dans la version 10.1.3

- Dans la fenêtre **Snapshot History**, les infobulles qui montrent l'état actuel de l'instantané ne reflètent pas l'état actuel. [CXM-5570]
  Parfois, XenMobile Mail Manager ne peut pas écrire dans le fichier de diagnostic Commands. Lorsque cela se produit, l'historique des commandes n'est pas consigné dans son intégralité. [CXM-49217]
- Lorsqu'une erreur se produit avec une connexion, la connexion peut ne pas être marquée comme "erronée"(errored). Par conséquent, une commande ultérieure peut tenter d'utiliser la connexion et provoquer une autre erreur. [CXM-49495]
- Lors d'une limitation en provenance du serveur Exchange, une exception peut être envoyée dans la routine Check Health. Par conséquent, les connexions ayant rencontré une erreur ou ayant expiré risquent de ne pas être purgées. En outre, XenMobile Mail Manager peut ne pas créer de connexions jusqu'à ce que le délai de limitation expire. [CXM-49794].

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Lorsque le nombre maximal de sessions pour Exchange est dépassé, XenMobile Mail Manager signale l'erreur "Device Capture Failed", qui n'est pas un message exact. Au lieu de cela, le message doit indiquer que les deux sessions que XenMobile Mail Manager utilise normalement pour la communication Exchange sont en cours d'utilisation. [CXM-49994]

Nouveautés dans la version 10.1.2

- **Connexion améliorée à Exchange :** XenMobile Mail Manager utilise des sessions PowerShell pour communiquer avec Exchange. Une session PowerShell, en particulier avec Office 365, peut devenir instable après un certain temps, empêchant les commandes suivantes de réussir. XenMobile Mail Manager peut maintenant définir une période d'expiration pour les connexions. Lorsque la connexion atteint son heure d'expiration, XenMobile Mail Manager arrête la session PowerShell et crée une session. Ce faisant, la session PowerShell est moins susceptible de devenir instable, ce qui réduit considérablement les risques d'échec d'un instantané.
- **Flux de travail instantané amélioré :** les instantanés importants représentent une opération longue et fastidieuse. Si une erreur se produit pendant un instantané, XenMobile Mail Manager tente désormais à plusieurs reprises (jusqu'à trois) d'effectuer une capture instantanée. Les tentatives suivantes ne commencent pas depuis le début. XenMobile Mail Manager continue là où il s'est arrêté. Ce changement améliore le taux de réussite des instantanés en général en permettant aux erreurs transitoires de passer pendant qu'un instantané est encore en cours.
- **Amélioration des diagnostics :** le dépannage des opérations de capture d'instantané est maintenant plus facile avec trois nouveaux fichiers de diagnostic pouvant être générés au cours d'un instantané. Ces fichiers permettent d'identifier les problèmes de commande PowerShell, les boîtes aux lettres avec informations manquantes et les appareils qui ne peuvent pas être associés à une boîte aux lettres. Un administrateur peut utiliser ces fichiers pour identifier les données qui peuvent ne pas être correctes dans Exchange.
- **Amélioration de l'utilisation de la mémoire :** XenMobile Mail Manager utilise désormais plus efficacement la mémoire. Les administrateurs peuvent planifier le redémarrage automatique de XenMobile Mail Manager pour fournir une version nettoyée du système.
- **Microsoft .NET Framework 4.6 :** la version requise de Microsoft .NET Framework est maintenant la version 4.6.

Problèmes résolus

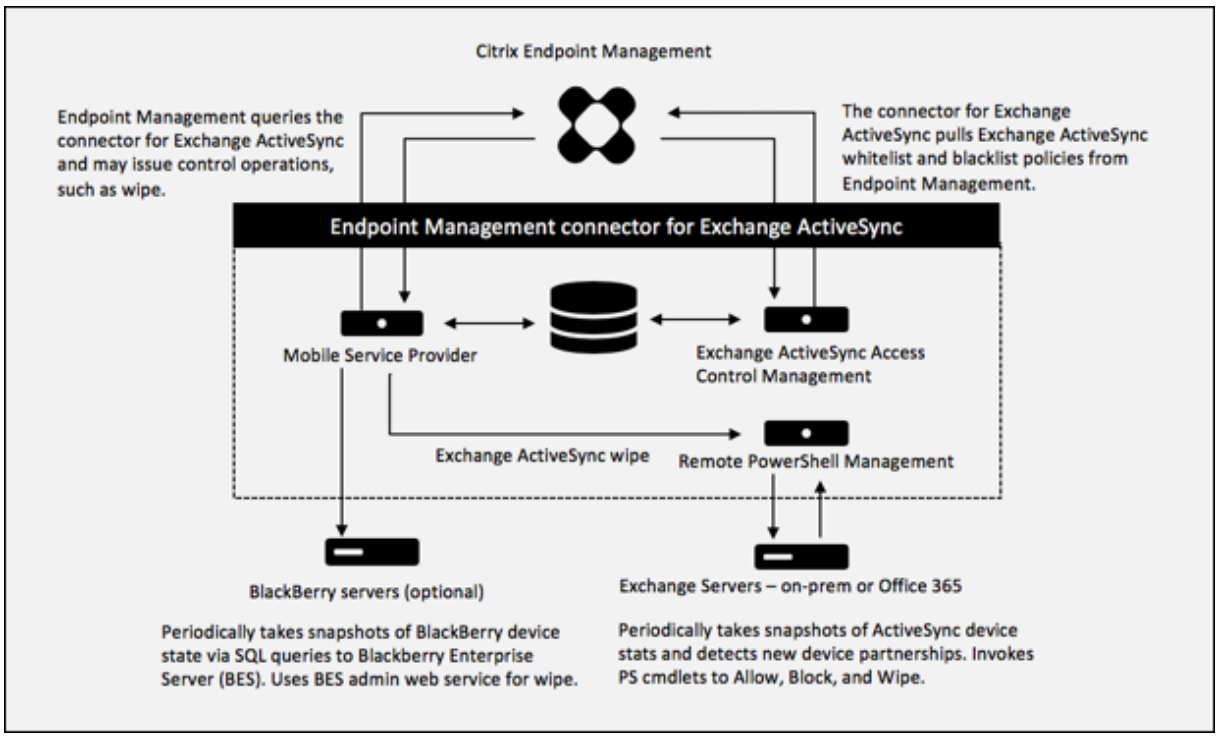
- Erreur d'invite d'informations d'identification : l'instabilité de session Office 365 a souvent causé cette erreur. L'amélioration de la connexion à Exchange résout le problème. (XMHELP-293, XMHELP-311, XMHELP-801)
- La boîte aux lettres et le nombre d'appareils sont inexacts : l'algorithme d'association de boîte aux lettres de XenMobile Mail Manager a été amélioré. La fonction d'amélioration des diagnos-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tics facilite l'identification des boîtes aux lettres et des appareils que XenMobile Mail Manager considère comme n'étant pas sous sa responsabilité. (XMHELP-623)
- Les commandes Autoriser / Bloquer / Effacer ne sont pas reconnues : correction d'un bogue avec lequel les commandes Autoriser / Bloquer / Effacer de XenMobile Mail Manager ne sont pas reconnues. (XMHELP-489)
- Gestion de la mémoire : meilleure gestion de la mémoire. (XMHELP-419)

Architecture

Le diagramme suivant présente les principaux composants du connecteur Citrix Endpoint Management pour Exchange ActiveSync. Pour un diagramme d'architecture de référence détaillé, voir Architecture.



Les deux principaux éléments sont les suivants :

- **Exchange ActiveSync Access Control Management :** communique avec Citrix Endpoint Management pour récupérer une stratégie Exchange ActiveSync depuis Citrix Endpoint Management, puis fusionne cette stratégie avec toutes les stratégies définies localement pour déterminer les appareils Exchange ActiveSync ayant le droit ou non d'accéder à Exchange. Les stratégies locales permettent d'étendre les règles de stratégie pour autoriser le contrôle d'accès par un groupe Active Directory, utilisateur, type d'appareil ou agent utilisateur de l'appareil (généralement la version de la plate-forme mobile).
- **Remote PowerShell Management :** ce composant est responsable de la planification et de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

l'appel des commandes PowerShell à distance afin d'appliquer la stratégie compilée par la gestion du contrôle d'accès à Exchange ActiveSync. Il crée régulièrement un instantané de la base de données Exchange ActiveSync pour détecter de nouveaux périphériques ou des périphériques modifiés Exchange ActiveSync.

Configuration système requise et conditions préalables

La configuration système minimale suivante est nécessaire pour utiliser Citrix Endpoint Management Connector pour Exchange ActiveSync :

- Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2008 R2 Service Pack 1. Doit être un serveur en anglais. Le support pour Windows Server 2008 R2 Service Pack 1 prend fin le 14 janvier 2020 et le support pour Windows Server 2012 R2 prend fin le 10 octobre 2023.
- Microsoft SQL Server 2016 Service Pack 2, SQL Server 2014 Service Pack 3 ou SQL Server 2012 Service Pack 4.
- Microsoft .NET Framework 4.6.
- Blackberry Enterprise Service, version 5 (facultatif).

Versions minimales prises en charge de Microsoft Exchange Server :

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013 (le support prend fin le 11 avril 2023)
- Exchange Server 2010 Service Pack 3 (la prise en charge prend fin le 14 janvier 2020)

Logiciels requis

- Windows Management Framework doit être installé.
  - PowerShell V5, V4 et V3
- La stratégie d'exécution de PowerShell doit être paramétrée sur RemoteSigned via Set-ExecutionPolicy RemoteSigned.
- Le port TCP 80 doit être ouvert entre l'ordinateur exécutant le connecteur pour Exchange ActiveSync et le serveur Exchange distant.

Clients de messagerie d'appareil : les clients de messagerie ne renvoient pas tous le même ID ActiveSync pour un appareil. Étant donné que le connecteur pour Exchange ActiveSync s'attend à un ID ActiveSync unique pour chaque appareil, seuls les clients de messagerie qui génèrent toujours le même ID ActiveSync unique pour chaque appareil sont pris en charge. Ces clients de messagerie ont été testés par Citrix et aucune erreur n'a été détectée :

- Client de messagerie natif Samsung

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Client de messagerie natif iOS

Exchange : la configuration requise pour l'ordinateur local exécutant Exchange est la suivante :

Les informations d'identification spécifiées dans l'interface utilisateur de la console Exchange Configuration doivent être en mesure de se connecter au serveur Exchange Server et bénéficier d'un accès complet pour exécuter les applets de commande PowerShell spécifiques à Exchange suivantes :

- **Pour Exchange Server 2010 SP2 :**
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-ActiveSyncDevice`
  - `Get-ActiveSyncDeviceStatistics`
  - `Clear-ActiveSyncDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`
- **Pour Exchange Server 2013 et Exchange Server 2016 :**
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`
- Si le connecteur pour Exchange ActiveSync est configuré pour afficher l'ensemble de la forêt, l'autorisation doit avoir été accordée pour exécuter : **Set-AdServerSettings -ViewEntireForest $true**
- Les informations d'identification fournies doivent avoir été autorisées à se connecter au serveur Exchange Server via le Shell distant. Par défaut, l'utilisateur qui a installé Exchange possède ce droit.
- Afin d'établir une connexion à distance et exécuter les commandes distantes, les informations d'identification doivent correspondre à un utilisateur qui est un administrateur sur l'appareil distant. Vous pouvez utiliser Set-PSSessionConfiguration pour éliminer les exigences administratives, mais cette commande n'entre pas dans le cadre de ce document. Pour plus d'informations, consultez l'article Microsoft À propos des configurations de session.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Le serveur Exchange doit être configuré pour prendre en charge les requêtes PowerShell distantes via HTTP. En règle générale, un administrateur exécutant la commande PowerShell suivante sur le serveur Exchange est la seule exigence requise : WinRM QuickConfig.
- Exchange possède de nombreuses stratégies de limitation. L'une de ces stratégies contrôle combien de connexions PowerShell simultanées sont autorisées par utilisateur. Par défaut, le nombre de connexions simultanées autorisées pour un utilisateur est de 18 sur Exchange 2010. Lorsque la limite de connexion est atteinte, le connecteur pour Exchange ActiveSync ne peut pas se connecter au serveur Exchange. Il existe plusieurs méthodes pour changer le nombre maximal de connexions simultanées autorisées via PowerShell qui ne sont pas couvertes dans cette documentation. Si vous êtes intéressé, renseignez-vous au sujet des stratégies de limitation d'Exchange relatives à la gestion à distance avec PowerShell.

Configuration requise pour Office 365 Exchange

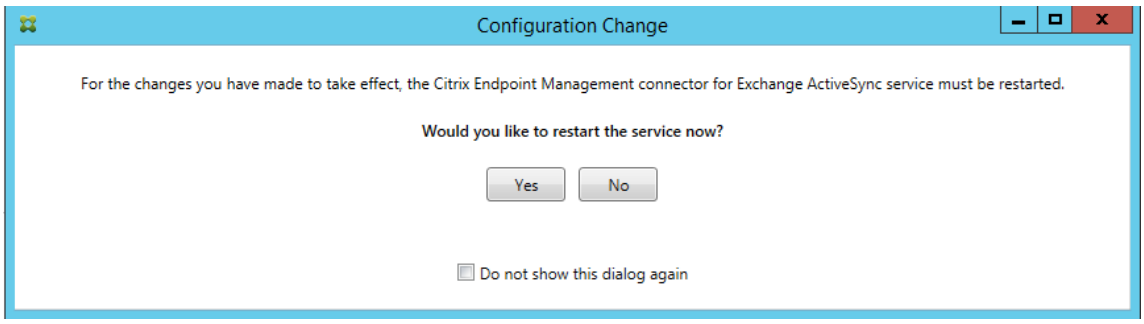
- **Autorisations :** les informations d'identification spécifiées dans l'interface utilisateur de la console Exchange Configuration doivent être en mesure de se connecter à Office 365 et bénéficier d'un accès complet pour exécuter les applets de commande PowerShell spécifiques à Exchange suivantes :
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`
- **Privilèges :** les informations d'identification fournies doit avoir été autorisées à se connecter au serveur Office 365 via le Shell distant. Par défaut, l'administrateur d'Office 365 Online possède les privilèges requis.
- **Stratégies de limitation :** Exchange possède de nombreuses stratégies de limitation. L'une de ces stratégies contrôle combien de connexions PowerShell simultanées sont autorisées par utilisateur. Par défaut, le nombre de connexions simultanées autorisées pour un utilisateur est de trois sur Office 365. Lorsque la limite de connexion est atteinte, le connecteur pour Exchange ActiveSync ne peut pas se connecter au serveur Exchange. Il existe plusieurs méthodes pour changer le nombre maximal de connexions simultanées autorisées via PowerShell qui ne sont pas couvertes dans cette documentation. Si vous êtes intéressé, renseignez-vous au sujet des stratégies de limitation d'Exchange relatives à la gestion à distance avec PowerShell.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Installer et configurer

1. Cliquez sur le fichier XmmSetup.msi puis suivez les instructions de l'assistant pour installer Citrix Endpoint Management Connector pour Exchange ActiveSync.
2. Laissez l'option **Launch the Configure utility** sélectionnée dans le dernier écran de l'assistant. Vous pouvez également ouvrir le connecteur pour Exchange ActiveSync à partir du menu **Démarrer**.
3. Configurez les propriétés de base de données suivantes :
   - Sélectionnez l'onglet **Configure > Database**.
   - Entrez le nom du serveur SQL (localhost par défaut).
   - Conservez la base de données par défaut **CitrixXmm**.
4. Sélectionnez l'un des modes d'authentification suivants utilisés pour SQL :
   - **SQL :** entrez le nom d'utilisateur et le mot de passe d'un utilisateur SQL valide.
   - **Windows Integrated :** si vous sélectionnez cette option, les informations d'identification d'ouverture de session du service XenMobile Mail Manager doivent être modifiées par un compte Windows disposant des autorisations nécessaires pour accéder au serveur SQL. Pour ce faire, ouvrez le **Panneau de configuration > Outils d'administration > Services**, cliquez avec le bouton droit de la souris sur l'entrée du service XenMobile Mail Manager, puis sélectionnez l'onglet **Log On** (Connexion).

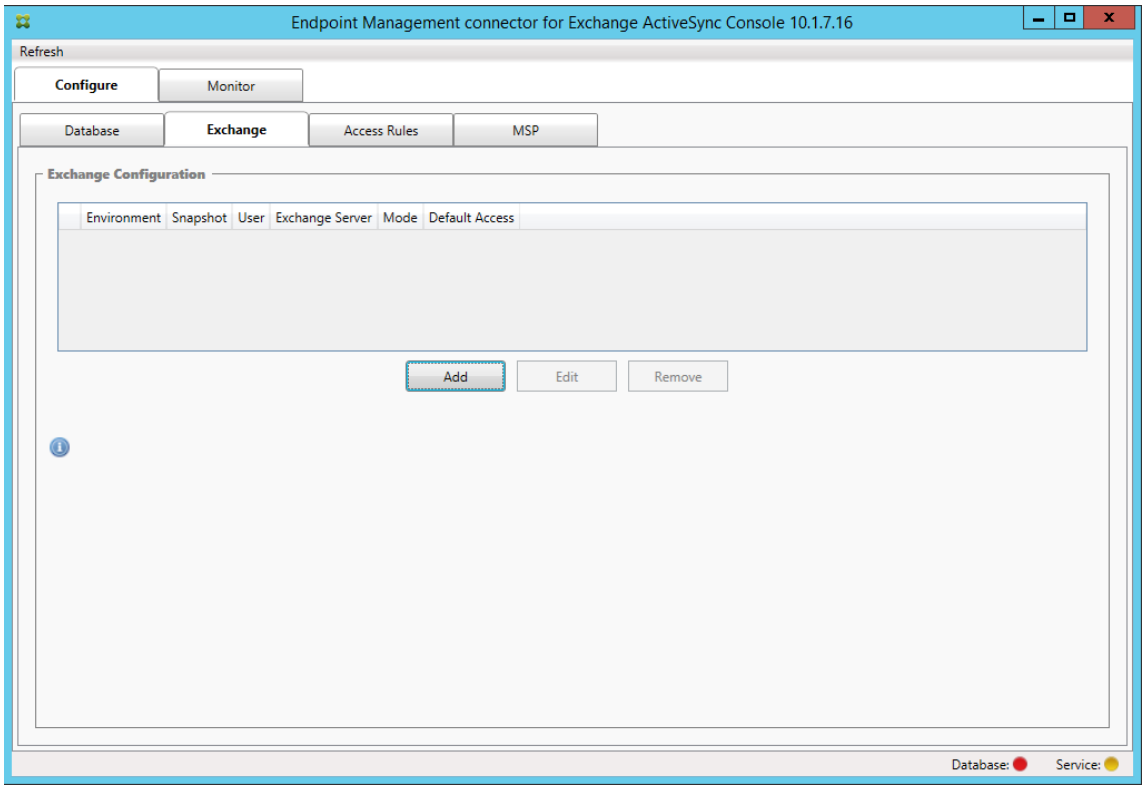
   Si Windows Integrated est également choisi pour la connexion à la base de données BlackBerry, le compte Windows spécifié ici doit également pouvoir accéder à la base de données BlackBerry.
5. Cliquez sur **Test Connectivity** pour vérifier qu'une connexion peut être établie avec le serveur SQL, puis cliquez sur **Save**.
6. Un message vous invite à redémarrer le service. Cliquez sur **Oui**.



7. Configurez un ou plusieurs serveurs Exchange :
   - Si vous ne gérez qu'un seul environnement Exchange, spécifiez un seul serveur. Si vous gérez plusieurs environnements Exchange, spécifiez un seul serveur Exchange pour chaque environnement Exchange.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Cliquez sur l'onglet **Configure > Exchange**, puis cliquez sur **Add**.



8. Sélectionnez le type d'environnement de serveur Exchange, soit **On Premise** soit **Office 365**.

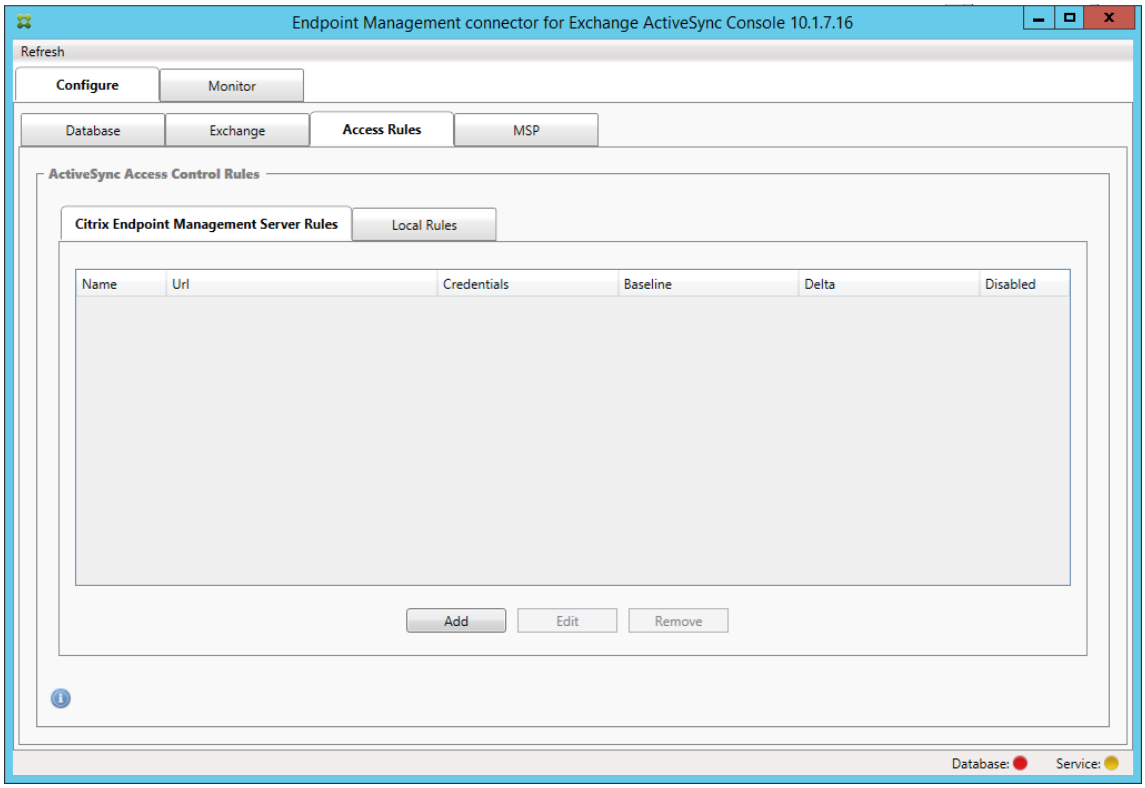
   - Si vous sélectionnez **On Premise**, entrez le nom du serveur Exchange qui sera utilisé pour les commandes PowerShell à distance.
   - Entrez le **nom d'utilisateur** d'une identité Windows disposant des droits appropriés sur le serveur Exchange comme indiqué dans la section Configuration requise et entrez le **mot de passe** de l'utilisateur.
   - Sélectionnez la planification d'exécution de captures d'instantanés principaux. Un instantané principal détecte tous les partenariats Exchange ActiveSync.
   - Sélectionnez la planification d'exécution des captures d'instantanés secondaires. Un instantané secondaire détecte les partenariats Exchange ActiveSync nouvellement créés.
   - Sélectionnez le type d'instantané : **Deep** ou **Shallow**. Les instantanés superficiels sont généralement plus rapides et suffisent pour exécuter toutes les fonctions de contrôle d'accès Exchange ActiveSync du connecteur pour Exchange ActiveSync.
   - Sélectionnez les paramètres d'accès par défaut : **Allow**, **Block** ou **Unchanged**. Ce paramètre contrôle la façon dont sont traités tous les appareils autres que ceux identifiés explicitement par des règles locales ou Citrix Endpoint Management. Si vous sélectionnez **Allow**, l'accès à ActiveSync à tous ces appareils est autorisé. Si vous sélectionnez **Block**, l'accès est refusé. Si vous sélectionnez **Unchanged**, aucune modification n'est effectuée.
   - Sélectionnez le mode de commande ActiveSync : **PowerShell** ou **Simulation**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

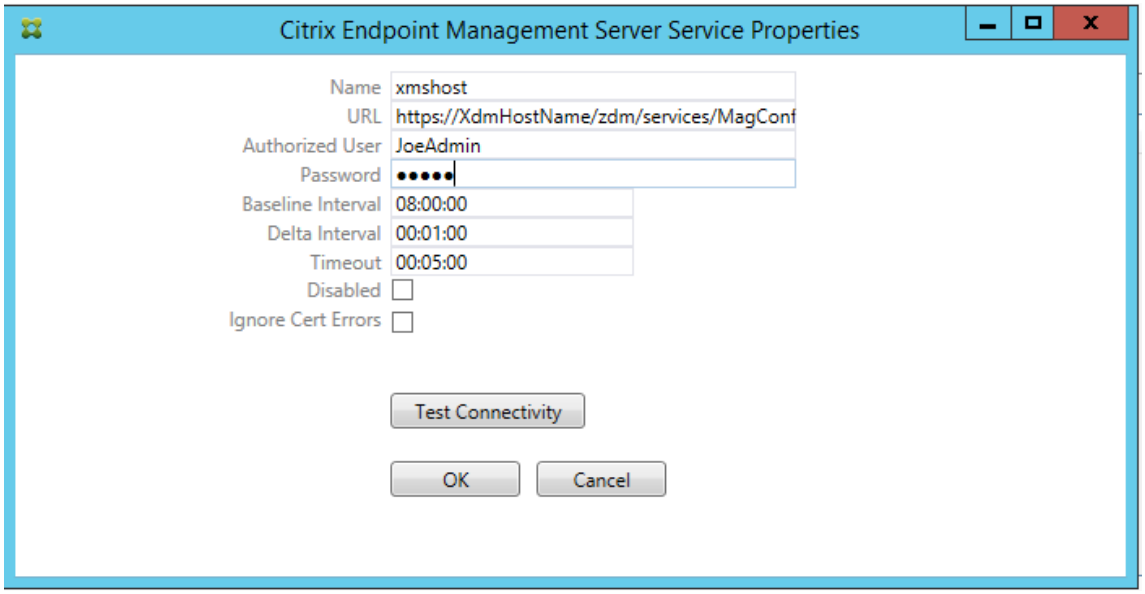
- En mode **PowerShell**,le connecteur pour Exchange ActiveSync émet des commandes PowerShell afin d'appliquer le contrôle d'accès souhaité. En mode Simulation, le connecteur pour Exchange ActiveSync n'émet pas de commandes PowerShell, mais consigne la commande prévue et les résultats escomptés dans la base de données. En mode Simulation, l'utilisateur peut alors utiliser l'onglet **Monitor** pour voir ce qui serait arrivé si le mode PowerShell était activé.
- Dans **Connection Expiration**, définissez les heures et les minutes pour la durée de vie d'une connexion. Lorsqu'une connexion atteint la durée spécifiée, elle est marquée comme expirée et n'est pas réutilisée. Lorsque la connexion expirée n'est plus utilisée, le connecteur pour Exchange ActiveSync l'arrête. Lorsqu'une connexion est de nouveau nécessaire, une nouvelle connexion est initialisée si aucune n'est disponible. Si aucune valeur n'est spécifiée, la valeur par défaut de 30 minutes est utilisée.
- Sélectionnez **View Entire Forest** pour configurer le connecteur pour Exchange ActiveSync de manière à ce qu'il affiche la forêt Active Directory entière dans l'environnement Exchange.
- Sélectionnez le protocole d'authentification : **Kerberos** ou **Basic**. Le connecteur pour Exchange ActiveSync prend en charge l'authentification de base pour les déploiements locaux. Cela permet d'utiliser le connecteur lorsque le serveur du connecteur n'est pas membre du domaine dans lequel réside le serveur Exchange.
- Cliquez sur **Test Connectivity** pour vérifier qu'une connexion peut être établie avec le serveur Exchange, puis cliquez sur **Save**.
- Un message vous invite à redémarrer le service. Cliquez sur **Oui**.

9. Configurer les règles d'accès : sélectionnez l'onglet **Configure > Access Rules** et cliquez sur l'onglet **Citrix Endpoint Management Rules**, puis sur **Add**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



10. Sur la page **Citrix Endpoint Management Server Service Properties**, modifiez la chaîne d'URL pour qu'elle pointe vers le serveur Citrix Endpoint Management. Par exemple, si le nom de l'instance est `zdm`, entrez `https://<XdmHostName>/zdm/services/MagConfigService`. Dans l'exemple, remplacez `XdmHostName` par l'adresse IP ou DNS du serveur Citrix Endpoint Management.



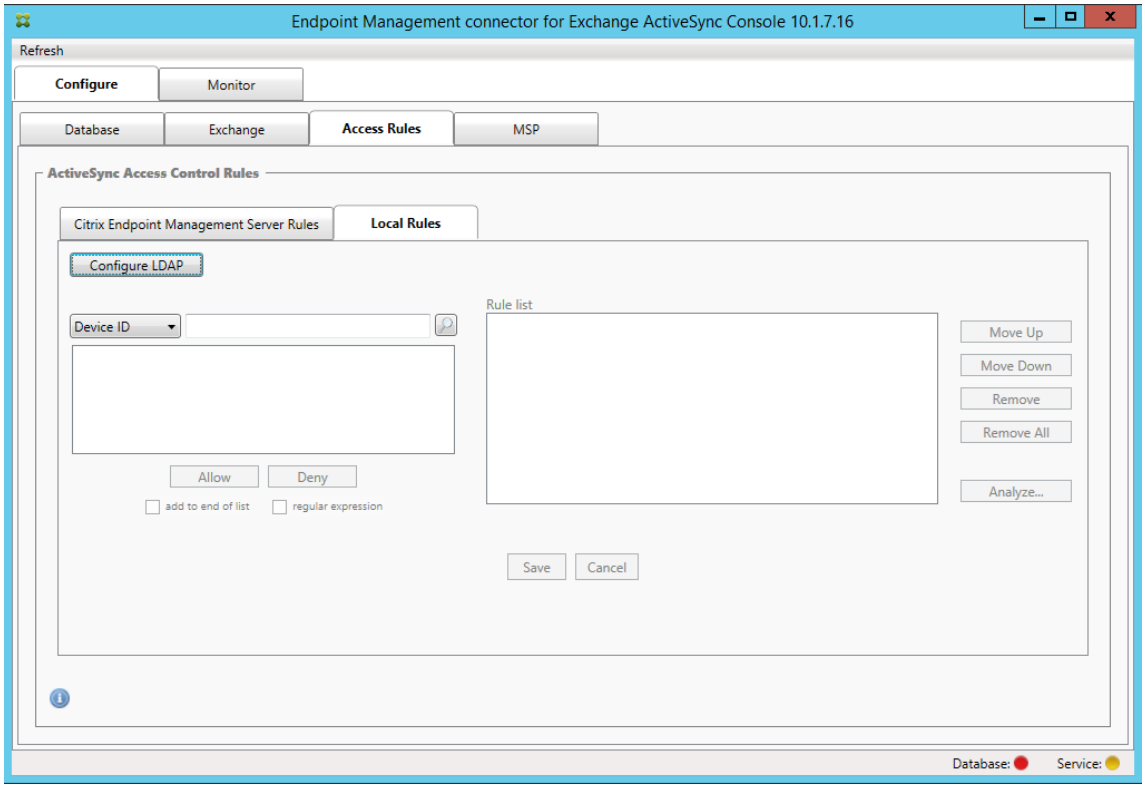
- Entrez un utilisateur autorisé sur le serveur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Entrez le mot de passe de l'utilisateur.
- Conservez les valeurs par défaut **Baseline Interval**, **Delta Interval**, et **Timeout** values.
- Cliquez sur **Test Connectivity** pour tester la connexion au serveur, puis cliquez sur **OK**.

Si la case **Disabled** est cochée, Citrix Endpoint Management Mail Service ne collecte pas de stratégie depuis Citrix Endpoint Management.

11. Cliquez sur l'onglet **Local Rules**.



- Vous pouvez ajouter des règles locales basées sur ActiveSync Device ID, Device Type, AD Group, User ou UserAgent. Sélectionnez le type approprié dans la liste.
- Tapez le texte ou les fragments de texte dans la zone de texte. Si vous le souhaitez, cliquez sur le bouton de requête pour afficher les entités qui correspondent au fragment.

Pour tous les types autres que Group, le système s'appuie sur les appareils qui ont été localisés dans un instantané. Par conséquent, si vous démarrez et que vous n'avez pas réalisé d'instantané, aucune entité n'est disponible.

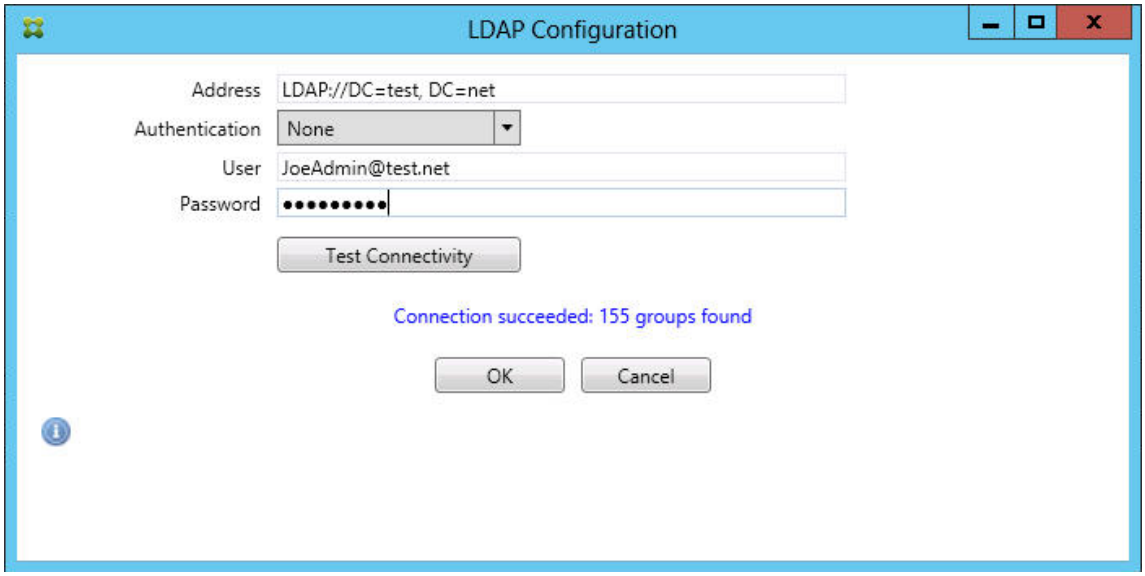
- Sélectionnez une valeur de texte, puis cliquez sur **Allow** ou **Deny** pour l'ajouter à la **Rule List** sur le côté droit. Vous pouvez modifier l'ordre des règles ou les supprimer en utilisant les boutons situés à droite du panneau de **Rule List**. L'ordre est important car pour un utilisateur et un appareil donné, les règles sont évaluées dans l'ordre indiqué. Dans le cas d'une correspondance à une règle de niveau élevé (près du haut de la liste), les règles se trouvant plus bas dans la liste n'ont pas d'effet. Par exemple, si vous possédez une règle

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

qui autorise tous les iPad, et une règle suivante bloquant l'utilisateur « Matt », l'iPad de Matt sera autorisé car la règle « iPad » possède une priorité plus élevée que la règle « Matt ».

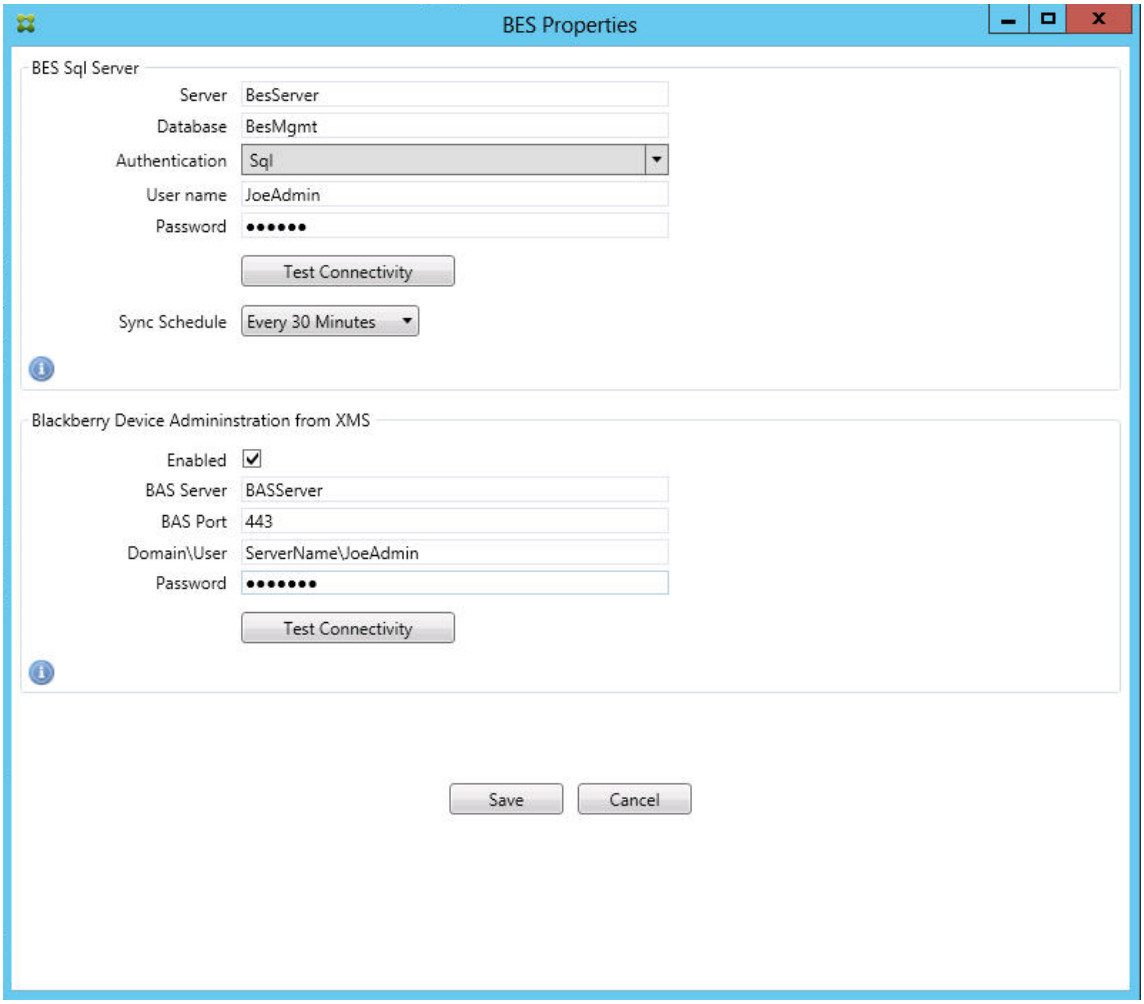
- Pour effectuer une analyse des règles dans la liste de règles afin de rechercher des remplacements, des conflits ou des constructions supplémentaires potentielles, cliquez sur **Analyze**, puis sur **Save**.

12. Si vous souhaitez créer des règles locales qui fonctionnent sur des groupes Active Directory, cliquez sur **Configure LDAP**, puis configurez les propriétés de connexion LDAP.



13. Vous pouvez également configurer une ou plusieurs instances de BlackBerry Enterprise Server (BES) : cliquez sur **Add**, puis entrez le nom du serveur BES SQL Server.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Tapez le nom de la base de données de gestion BES.
- Sélectionnez le mode **Authentication**. Si vous sélectionnez l'authentification intégrée Windows, le compte utilisateur du service du connecteur pour Exchange ActiveSync est le compte utilisé pour se connecter au serveur BES SQL. Si vous choisissez Windows Integrated pour la connexion à la base de données du connecteur, le compte Windows spécifié ici doit également pouvoir accéder à la base de données du connecteur.
- Si vous sélectionnez **SQL authentication**, entrez le nom d'utilisateur et le mot de passe.
- Définissez **Sync Schedule**. Il s'agit du calendrier utilisé pour se connecter au serveur BES SQL et rechercher toute mise à jour d'appareil.
- Cliquez sur **Test Connectivity** pour vérifier la connectivité avec le serveur SQL. Si Windows Integrated est sélectionné, ce test utilise l'utilisateur actuellement connecté et non l'utilisateur du service du connecteur et par conséquent ne teste pas correctement l'authentification SQL.
- Pour prendre en charge l'effacement à distance (Wipe) et la réinitialisation du mot de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

passe (ResetPassword) d'appareils BlackBerry depuis Citrix Endpoint Management, sélectionnez la case **Enabled**.

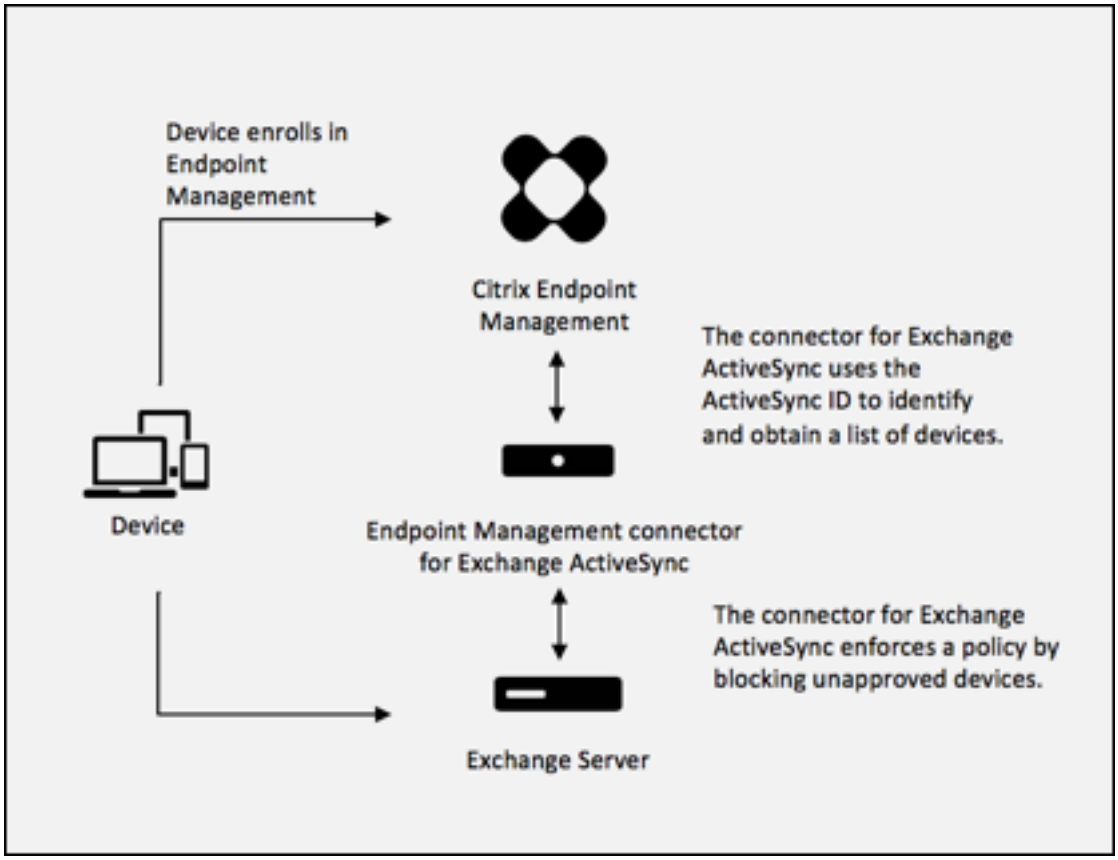
- Entrez le nom de domaine complet BES.
- Entrez le port BES utilisé pour le service Web d'administration.
- Entrez le nom d'utilisateur complet et le mot de passe requis par le service BES.
- Cliquez sur **Test Connectivity** pour tester la connexion au serveur BES, puis cliquez sur **Save**.

Appliquer les stratégies de messagerie avec des ID ActiveSync

Votre stratégie de messagerie d'entreprise peut refuser l'accès à la messagerie d'entreprise à certains appareils. Pour vous conformer à cette stratégie, vous devez vous assurer que les employés ne peuvent pas accéder à la messagerie d'entreprise à partir de tels appareils. Citrix Endpoint Management Connector pour Exchange ActiveSync et Citrix Endpoint Management fonctionnent ensemble pour appliquer une telle stratégie de messagerie. Citrix Endpoint Management configure la stratégie de l'accès à la messagerie d'entreprise. Lorsqu'un appareil non approuvé s'inscrit auprès d'Citrix Endpoint Management, le connecteur pour Exchange ActiveSync applique la stratégie.

Le client de messagerie sur un appareil se fait connaître d'Exchange Server (ou Office 365) à l'aide de l'D d'appareil, également appelé ID ActiveSync, qui est utilisé pour identifier l'appareil. Citrix Secure Hub obtient un identificateur similaire et envoie l'identificateur à Citrix Endpoint Management lorsque l'appareil est inscrit. En comparant les ID des deux appareils, Endpoint Management Connector pour Exchange ActiveSync peut déterminer si un appareil spécifique est autorisé à accéder à la messagerie d'entreprise. La figure suivante illustre ce concept :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Si Citrix Endpoint Management envoie au connecteur pour Exchange ActiveSync un ID ActiveSync différent de l'ID publié auprès d'Exchange par l'appareil, le connecteur ne peut pas indiquer à Exchange l'action à exécuter avec l'appareil.

La correspondance des ID ActiveSync fonctionne de manière fiable sur la plupart des plates-formes. Cependant, Citrix a constaté que sur certaines implémentations Android, l'ID ActiveSync de l'appareil est différent de l'ID publié par le client de messagerie auprès d'Exchange. Pour pallier ce problème, vous pouvez effectuer les tâches suivantes :

- Sur les plates-formes Android, Citrix vous recommande d'utiliser Citrix Secure Mail.

Pour garantir que votre stratégie d'accès à la messagerie d'entreprise est appliquée correctement, vous pouvez adopter une approche de sécurité défensive. Configurez Citrix Endpoint Management Connector pour Exchange ActiveSync de manière à bloquer les e-mails en définissant la stratégie statique sur **Deny** par défaut. Cela signifie que si un employé configure un autre client de messagerie sur un appareil Android et que la détection de l'ID ActiveSync ne fonctionne pas, l'employé se voit refuser l'accès à la messagerie d'entreprise.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Règles de contrôle d'accès

Citrix Endpoint Management Connector pour Exchange ActiveSync propose une approche basée sur des règles permettant de configurer dynamiquement le contrôle d'accès aux appareils Exchange ActiveSync. Une règle de contrôle d'accès au connecteur se compose de deux parties : une expression correspondante et un état d'accès souhaité (Autoriser ou Bloquer). Une règle doit être testée par rapport à un appareil ActiveSync Exchange donné pour déterminer si elle s'applique à l'appareil ou correspond à ce dernier. Il existe plusieurs types d'expressions correspondantes ; une règle peut, par exemple, correspondre à tous les appareils d'un type d'appareil donné ou à un ID d'appareil ActiveSync Exchange spécifique, ou encore à tous les appareils d'un utilisateur spécifique, etc.

À tout moment lors de l'ajout, la suppression et la réorganisation de règles dans la liste, si vous cliquez sur le bouton **Cancel**, l'état dans lequel se trouvait la liste lors de la première ouverture est rétabli. Si vous fermez l'outil de configuration sans cliquer sur **Save**, les modifications apportées sur cette fenêtre seront perdues.

Citrix Endpoint Management Connector pour Exchange ActiveSync propose trois types de règles : les règles locales, les règles du serveur Citrix Endpoint Management (aussi appelées règles XDM), et la règle d'accès par défaut.

Local rules (Règles locales) : les règles locales ont la priorité la plus élevée : si un appareil est identifié par une règle locale, l'évaluation de la règle ne s'applique pas. Ni les règles du serveur Citrix Endpoint Management ni la règle d'accès par défaut ne seront consultées. Les règles locales se configurent localement sur le connecteur pour Exchange ActiveSync via l'onglet **Configure > Access Rules > Local Rules**. La prise en charge de correspondance se base sur l'appartenance des utilisateurs à un groupe Active Directory donné. La prise en charge de correspondance se base sur des expressions régulières pour les champs suivants :

- Active Sync Device ID
- ActiveSync Device Type
- User Principal Name (UPN)
- ActiveSync User Agent (généralement la plate-forme de l'appareil ou le client de messagerie)

Si un instantané principal a été effectué et qu'il a trouvé des appareils, vous pouvez ajouter une règle d'expressions normales ou régulières. Si aucun instantané principal n'a été effectué, vous pouvez uniquement ajouter des règles d'expressions régulières.

Règles du serveur Citrix Endpoint Management : les règles du serveur Citrix Endpoint Management sont des références à un serveur Citrix Endpoint Management externe qui fournit des règles aux appareils gérés. Le serveur Citrix Endpoint Management peut être configuré avec ses propres règles de haut niveau qui identifient les appareils à autoriser ou à bloquer en fonction des propriétés connues par Citrix Endpoint Management, par exemple si l'appareil est jailbreaké ou s'il contient des applications interdites. Citrix Endpoint Management évalue les règles de haut niveau et génère un ensemble

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

d'ID d'appareils ActiveSync autorisés ou bloqués, qui sont ensuite envoyés à XenMobile Mail Manager.

Default access rule (Règle d'accès par défaut) : la règle d'accès par défaut est unique car elle peut potentiellement s'appliquer à tous les appareils et elle est toujours évaluée en dernier. C'est la règle passe-partout, ce qui signifie que si un appareil donné ne correspond pas à une règle locale ou du serveur Citrix Endpoint Management, l'état d'accès souhaité de l'appareil est déterminé par l'état d'accès souhaité de la règle d'accès par défaut.

- **Default Access –Allow (Accès par défaut - Autoriser) :** tout appareil ne correspondant pas à une règle locale ou de Citrix Endpoint Management Server sera autorisé.
- **Default Access –Block (Accès par défaut - Bloquer) :** tout appareil ne correspondant pas à une règle locale ou de Citrix Endpoint Management Server sera bloqué.
- **Default Access - Unchanged (Accès par défaut - Inchangé) :** l'état d'accès de tout appareil non associé à une règle locale ou du serveur Citrix Endpoint Management ne pourra pas être modifié par Citrix Endpoint Management Connector pour Exchange ActiveSync. Si un appareil a été placé en quarantaine par Exchange, aucune action n'est prise ; par exemple, la seule manière de retirer un appareil en quarantaine est de posséder une règle locale ou XDM qui outrepasse explicitement la quarantaine.

À propos des évaluations de règles

Pour chaque appareil pour lequel Exchange remet des rapports au connecteur pour Exchange ActiveSync, les règles sont évaluées dans l'ordre, de la priorité la plus élevée à la plus faible, comme suit :

- Règles locales
- Règles du serveur Citrix Endpoint Management
- Règle d'accès par défaut

Lorsqu'une correspondance est trouvée, l'évaluation s'arrête. Par exemple, si un appareil correspond à une règle locale, l'appareil ne sera pas évalué par rapport aux règles du serveur Citrix Endpoint Management ou à la règle d'accès par défaut. Cela reste aussi vrai pour un type de règle donné. Par exemple, s'il existe plus d'une correspondance pour un appareil donné dans la liste des règles locales, l'évaluation s'arrête dès la première correspondance.

Le connecteur pour Exchange ActiveSync réévalue l'ensemble des règles déjà définies lorsque les propriétés d'un appareil sont modifiées, lorsque des appareils sont ajoutés ou supprimés ou lorsque les règles sont modifiées. Les instantanés principaux détectent la suppression d'appareils ainsi que les modifications apportées à leurs propriétés à intervalles configurables. Les instantanés secondaires détectent les nouveaux appareils à intervalles configurables.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exchange ActiveSync possède aussi des règles régissant l'accès. Il est important de bien comprendre le fonctionnement de ces règles dans l'environnement du connecteur pour Exchange ActiveSync. Exchange peut être configuré avec trois niveaux de règles : les exemptions personnelles, les règles d'appareil et les paramètres d'organisation. Le connecteur pour Exchange ActiveSync automatise le contrôle d'accès en envoyant des requêtes PowerShell à distance via un programme pour modifier la liste des exemptions personnelles. Il s'agit de listes d'ID d'appareils Exchange ActiveSync autorisés ou bloqués associés à une boîte aux lettres donnée. Lorsqu'il est déployé, le connecteur pour Exchange ActiveSync prend en charge la gestion des listes d'exemptions dans Exchange. Consultez l'article Microsoft, Gestion des appareils avec Exchange et Configuration Manager.

L'analyse est particulièrement utile dans les situations dans lesquelles plusieurs règles ont été définies pour le même champ. Vous pouvez résoudre les relations entre les règles. Vous pouvez effectuer des analyses depuis la perspective des champs de règle ; par exemple, les règles sont analysées par groupes en fonction du champ remplissant la condition, tel que ActiveSync device ID, ActiveSync device type, User, User Agent, et ainsi de suite.

Terminologie relative aux règles

- **Règle absolue :** une substitution se produit lorsque plusieurs règles s'appliquent à un même appareil. Étant donné que les règles sont évaluées par priorité dans la liste, la ou les dernières instances de règle devant s'appliquer peuvent ne jamais être évaluées.
- **Règle conflictuelle :** un conflit survient quand plusieurs règles s'appliquent à un même appareil et que l'accès (Autoriser/Bloquer) ne correspond pas. Si les règles conflictuelles ne sont pas des expressions régulières, un conflit se traduit toujours implicitement par une substitution.
- **Règle complémentaire :** un complément a lieu lorsque plusieurs règles sont des expressions régulières et par conséquent, il peut s'avérer nécessaire de vérifier que les deux expressions régulières (ou plus) peuvent être combinées en une seule expression ou qu'il n'y ait pas duplication de fonctionnalités. Une règle complémentaire peut également causer des problèmes de conflit d'accès (Autoriser/Bloquer).
- **Règle principale :** la règle principale est la règle sur laquelle l'utilisateur a cliqué dans la boîte de dialogue. La règle est indiquée visuellement par une bordure. La règle aura également une ou deux flèches vertes pointant vers le haut ou vers le bas. Si une flèche pointe vers le haut, cela indique qu'il existe des règles secondaires qui précèdent la règle principale. Si une flèche pointe vers le bas, cela indique qu'il existe des règles secondaires qui s'appliquent après la règle principale. Seule une règle principale peut être active à tout moment.
- **Règle secondaire :** une règle secondaire est liée d'une certaine manière à la règle principale que ce soit via une relation de remplacement, de conflit ou supplémentaire. Les règles sont indiquées visuellement par une bordure en pointillés. Pour chaque règle principale, il peut y avoir une ou plusieurs règles secondaires. Lorsque vous cliquez sur une entrée soulignée, la ou les règles secondaires sélectionnées le sont toujours du point de vue de la règle principale. Par

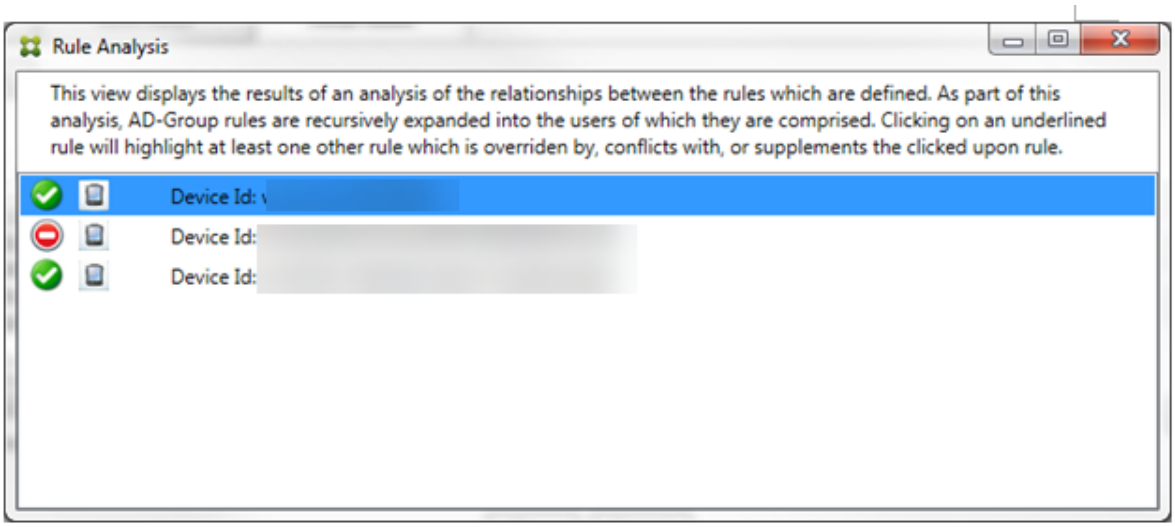
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

exemple, la règle secondaire est remplacée par la règle principale ou la règle secondaire entrera en conflit avec la règle principale ou la règle secondaire complétera la règle principale.

Apparence des types de règles dans la boîte de dialogue d'analyse des règles

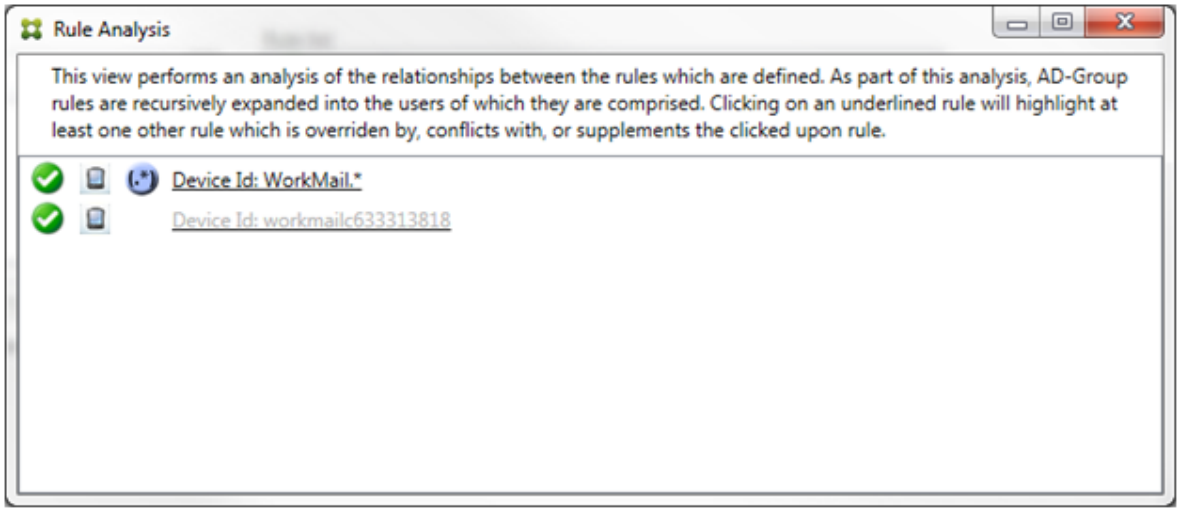
Lorsqu'il n'y a aucun conflit, remplacement, ou complément, il n'y a pas d'entrées soulignées dans la boite de dialogue Rule Analysis. Par exemple, cliquer sur des éléments n'a pas d'impact, les éléments normaux sélectionnés sont mis en évidence.

La fenêtre Rule Analysis contient une case qui, lorsqu'elle est sélectionnée, affiche uniquement les conflits, remplacements, redondances ou compléments.

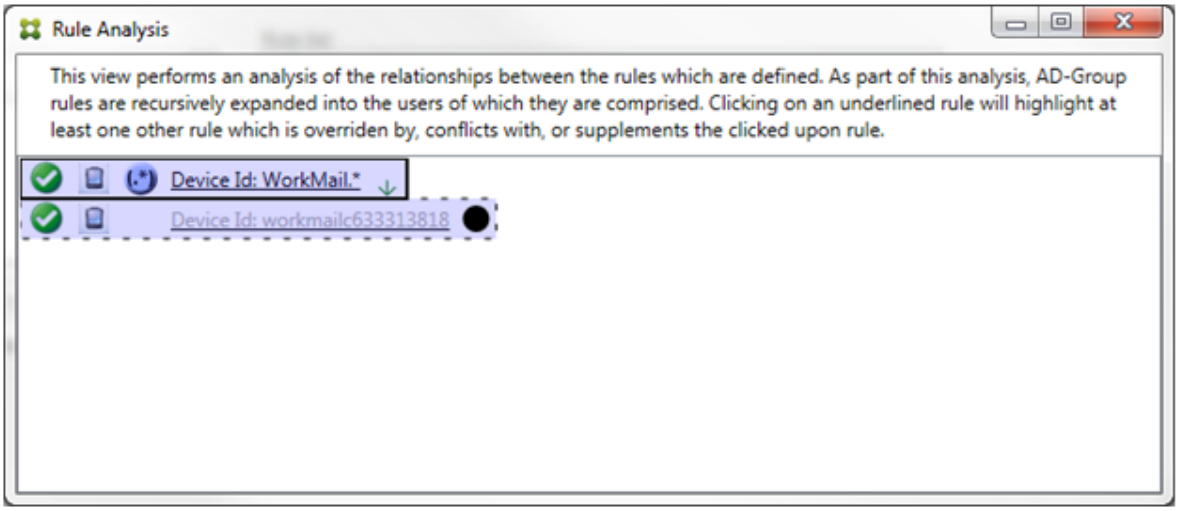


Lorsqu'une substitution se produit, au moins deux règles sont soulignées : la règle principale et la ou les règles secondaires. Au moins une règle secondaire s'affiche dans une police plus claire pour indiquer que la règle a été remplacée par une règle de priorité plus élevée. Vous pouvez cliquer sur les règles remplacées pour déterminer la ou les règles qui ont remplacé la règle. Lorsqu'une règle remplacée a été soulignée que ce soit parce que la règle est une règle principale ou secondaire, un cercle noir apparaît à côté en guise d'indication visuelle signifiant que la règle est inactive. Par exemple, avant que vous cliquiez sur la règle, la boîte de dialogue se présente comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

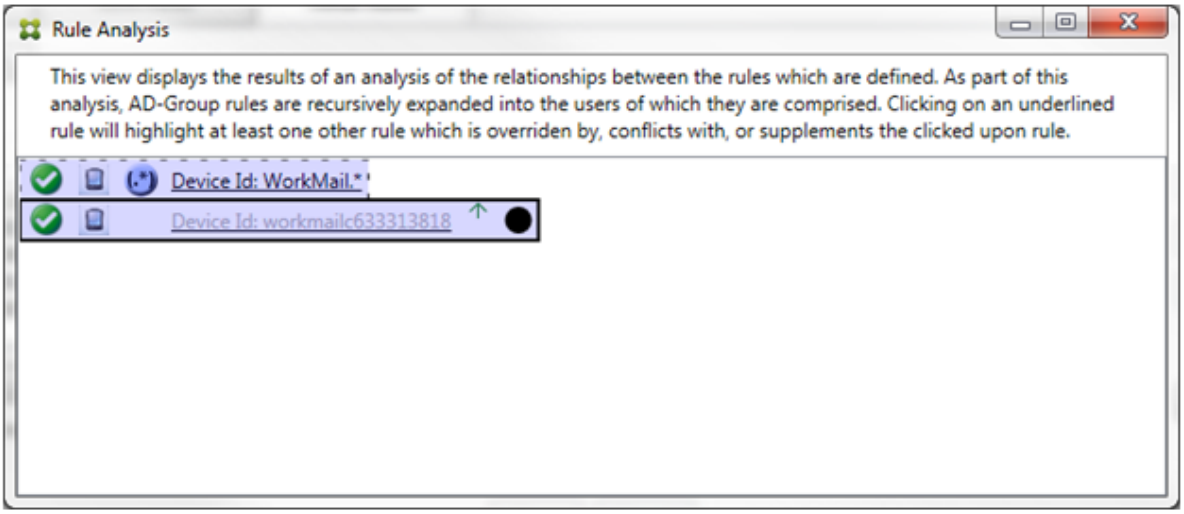


Lorsque vous cliquez sur la règle prioritaire, la boîte de dialogue se présente comme suit :



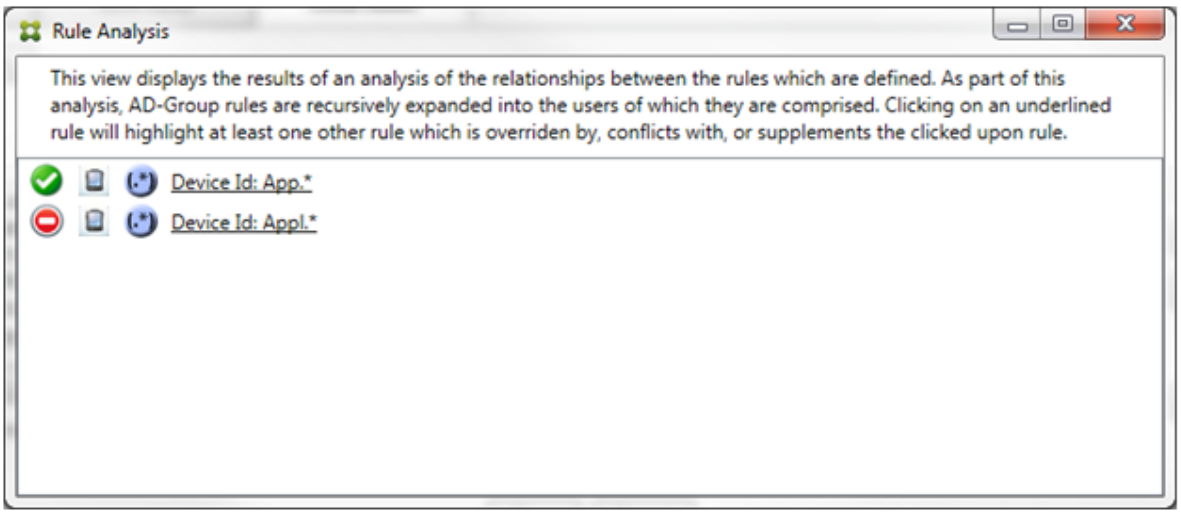
Dans cet exemple, la règle d'expression régulière `WorkMail.*` est la règle principale (indiquée par une bordure pleine) et la règle normale `workmailc633313818` est une règle secondaire (indiquée par une bordure en pointillés). Le point noir à côté de la règle secondaire est une indication visuelle qui signifie que la règle est inactive (ne sera jamais évaluée) en raison de la règle d'expression régulière prioritaire. Une fois que vous avez cliqué sur la règle remplacée, la boîte de dialogue se présente comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Dans l'exemple précédent, la règle d'expression régulière `WorkMail.*` est la règle secondaire (indiquée par une bordure en pointillés) et la règle normale `workmailc633313818` est une règle principale (indiquée par une bordure pleine). Pour cet exemple simple, il n'y a pas grande différence. Pour un exemple plus compliqué, consultez l'exemple d'expression complexe plus en avant dans cette rubrique. Dans un scénario avec de nombreuses règles définies, cliquer sur la règle remplacée permet d'identifier rapidement par quelles règles elle a été remplacée.

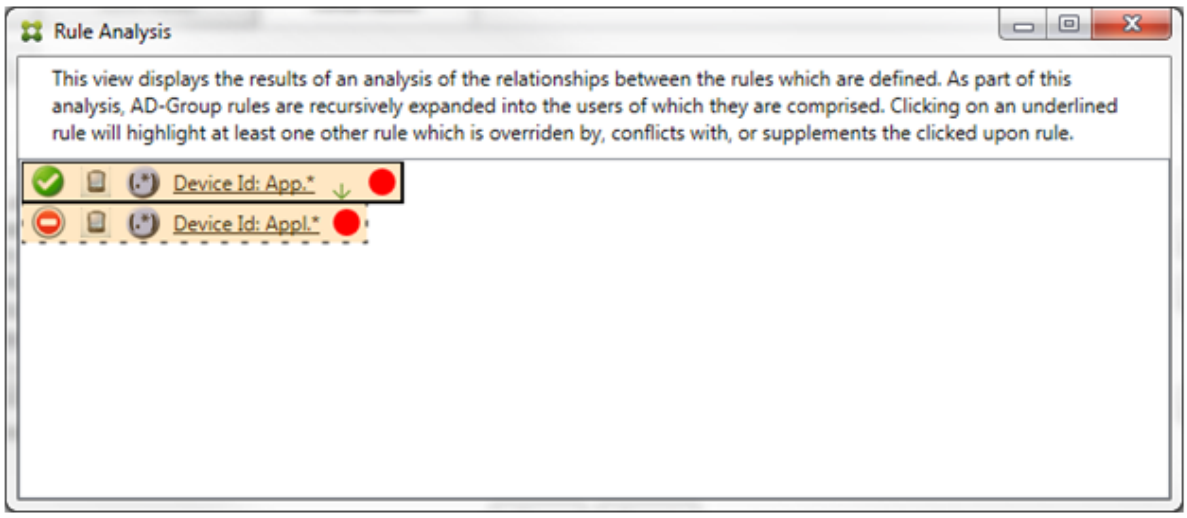
Lorsqu'un conflit se produit, au moins deux règles sont soulignées : la règle principale et la ou les règles secondaires. Les règles en conflit sont indiquées par un point rouge. Le cas de règles qui entrent seulement en conflit avec une autre règle est uniquement possible avec deux ou plusieurs règles d'expressions régulières définies. Dans tous les autres cas de conflit, il y aura non seulement un conflit, mais aussi un remplacement. Avant que vous cliquiez sur des règles dans un exemple simple, la boîte de dialogue se présente comme suit :



En inspectant les deux règles d'expressions régulières, il est évident que la première règle autorise tous les appareils avec un ID d'appareil contenant « App » et que la deuxième règle refuse tous les

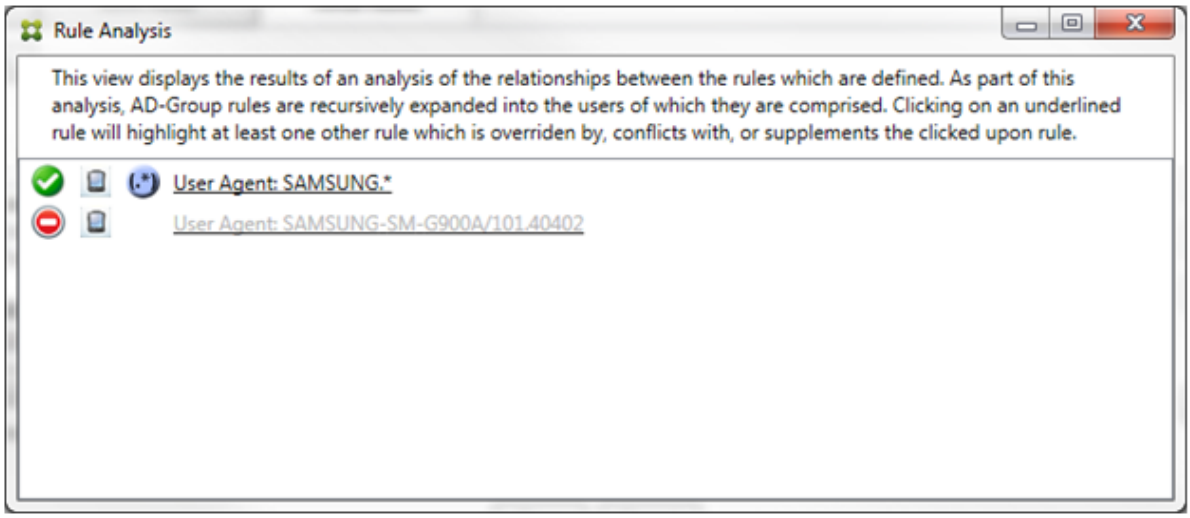
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

appareils avec un ID d'appareil contenant `Appl`. En outre, même si la deuxième règle refuse tous les appareils avec un ID d'appareil contenant `Appl`, aucun appareil correspondant à ces critères ne verra son accès refusé en raison de la priorité plus élevée de la règle l'y autorisant. Une fois que vous avez cliqué sur la première règle, la boîte de dialogue se présente comme suit :



Dans le cas précédent, la règle principale (règle d'expression régulière `App.*`) et la règle secondaire (règle d'expression régulière `Appl.*`) sont toutes deux affichées en jaune. Il s'agit simplement d'une indication visuelle vous alertant du fait que vous avez appliqué plus d'une règle d'expression régulière à un même champ de correspondance, ce qui peut entraîner un problème de redondance ou quelque chose de plus sérieux.

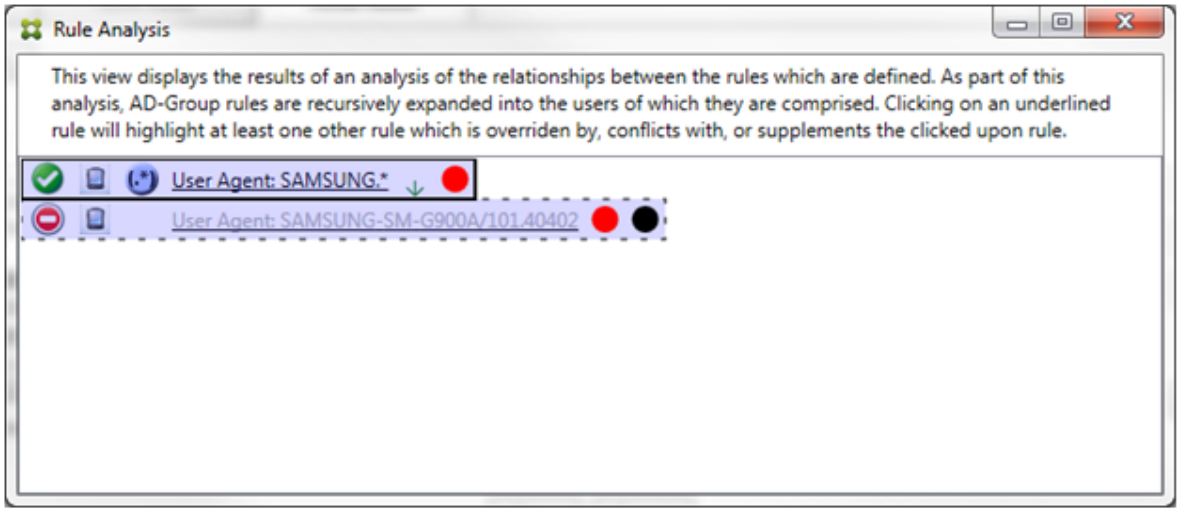
Dans un cas regroupant un conflit et un remplacement, la règle principale (règle d'expression régulière `App.*`) et la règle secondaire (règle d'expression régulière `Appl.*`) sont surlignées en jaune. Il s'agit simplement d'une indication visuelle vous alertant du fait que vous avez appliqué plus d'une règle d'expression régulière à un même champ de correspondance, ce qui peut entraîner un problème de redondance ou quelque chose de plus sérieux.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Il est facile de voir dans l'exemple précédent que la première règle (règle d'expression régulière `SAMSUNG.*`) ne remplace pas seulement la règle suivante (règle normale `SAMSUNG-SM-G900A/101.40402`), mais que l'accès des deux règles est différent (la règle principale indique Autoriser, la règle secondaire indique Bloquer). La deuxième règle (règle normale `SAMSUNG-SM-G900A/101.40402`) est affichée dans une police plus claire pour indiquer qu'elle a été remplacée et qu'elle n'est donc pas active.

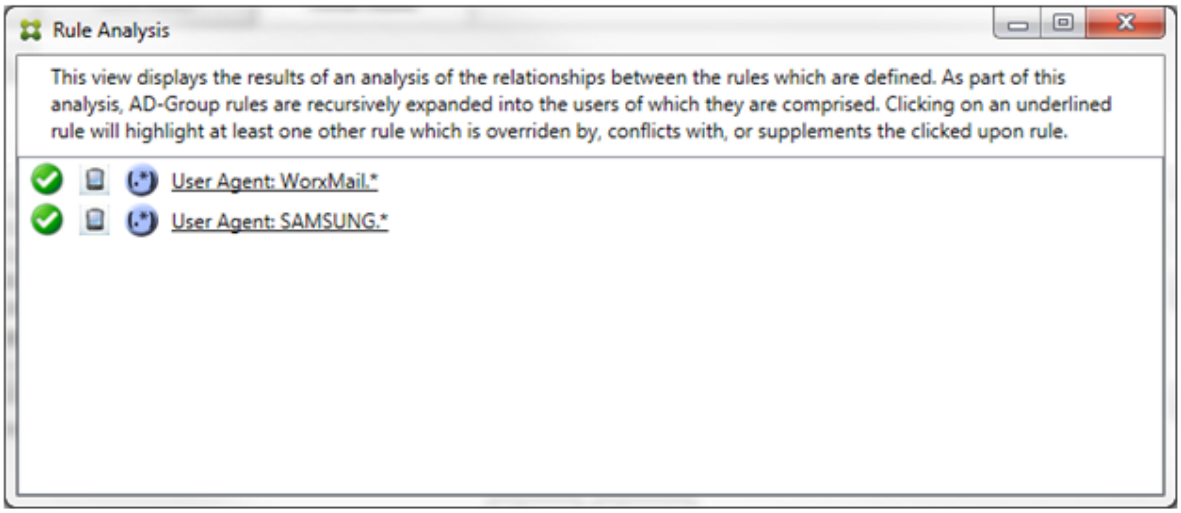
Une fois que vous avez cliqué sur la règle d'expression régulière, la boîte de dialogue se présente comme suit :



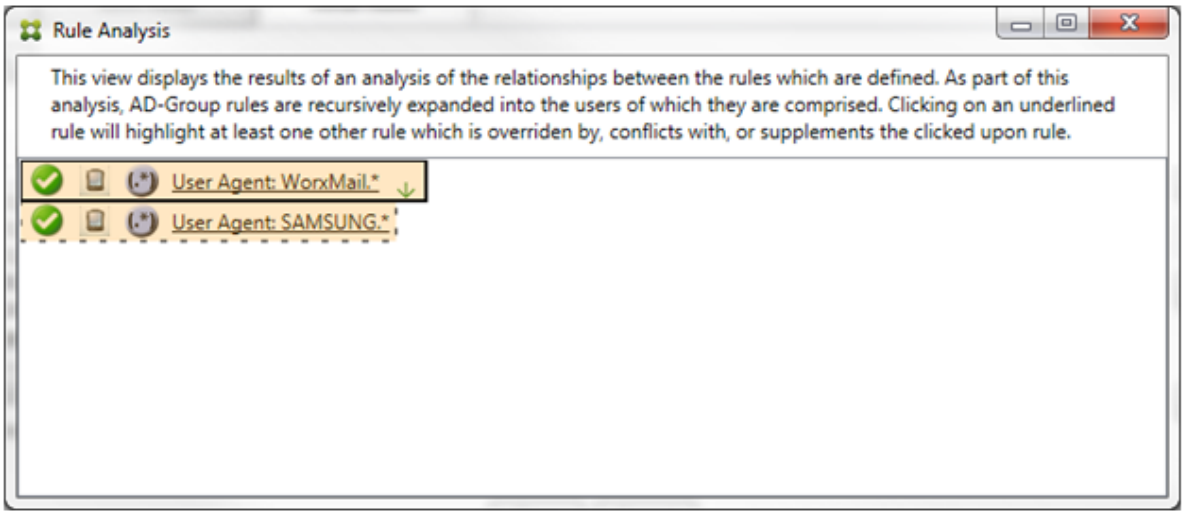
La règle principale (règle d'expression régulière `SAMSUNG.*`) est suivie d'un point rouge indiquant qu'elle entre en conflit avec une ou plusieurs règles secondaires. La règle secondaire (règle normale `SAMSUNG-SM-G900A/101.40402`) est suivie d'un point rouge pour indiquer que son état d'accès est en conflit avec la règle principale. Cette règle est également suivie d'un point noir pour indiquer qu'elle est substituée et donc inactive.

Au moins deux règles sont soulignées : la règle principale et la ou les règles secondaires. Les règles qui se complètent uniquement entre elles n'impliquent que des règles d'expressions régulières. Lorsque des règles se complètent entre elles, elles sont surlignées en jaune. Avant que vous cliquiez sur des règles dans un exemple simple, la boîte de dialogue se présente comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



L'inspection visuelle révèle facilement que les deux règles sont des règles d'expressions régulières qui s'appliquent toutes les deux au champ ActiveSync device ID dans Citrix Endpoint Management Connector pour Exchange ActiveSync. Une fois que vous avez cliqué sur la première règle, la boîte de dialogue se présente comme suit :

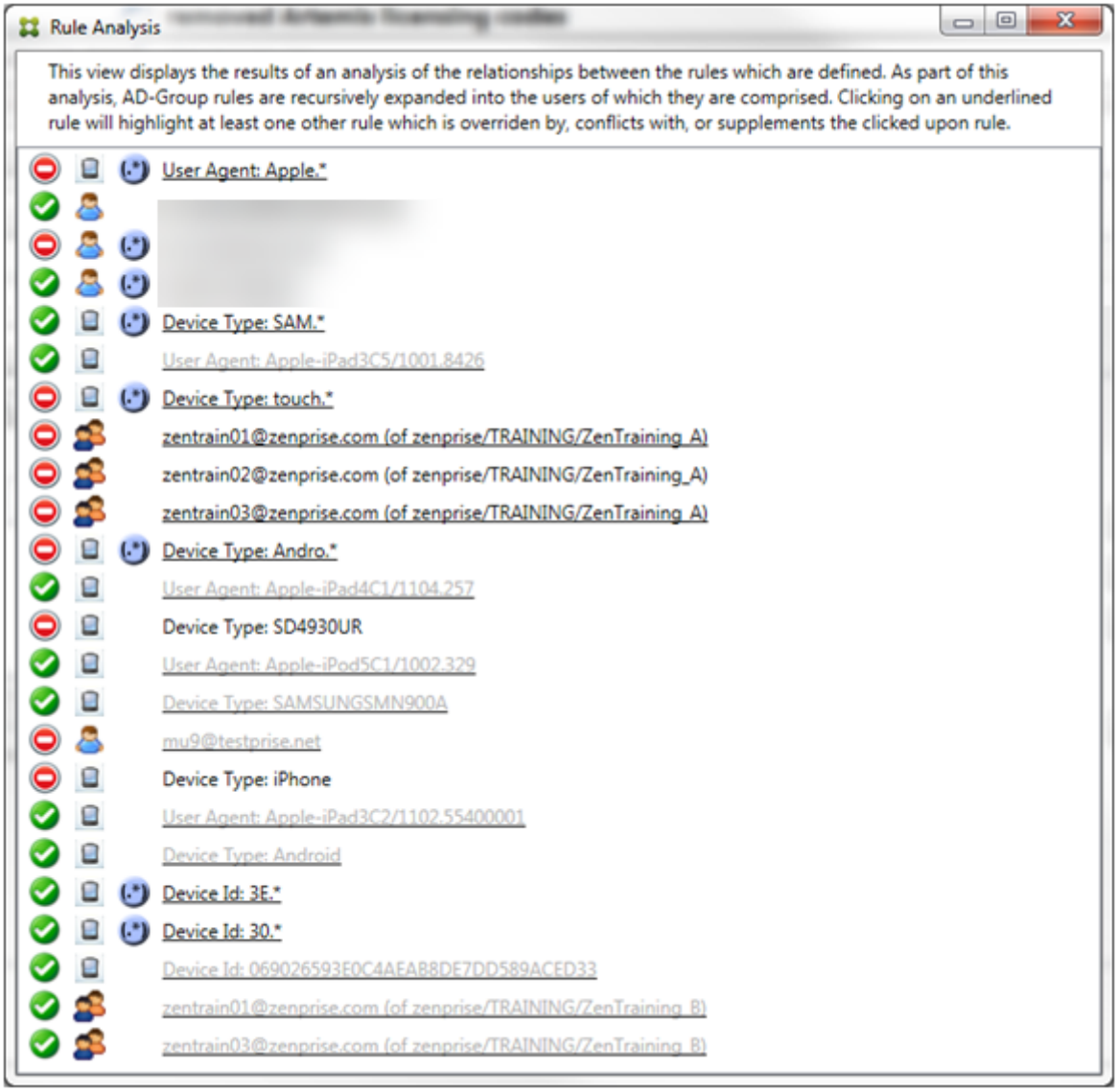


La règle principale (règle d'expression régulière `WorkMail.*`) est surlignée en jaune pour indiquer qu'il existe au moins une autre règle secondaire qui est une expression régulière. La règle secondaire (règle d'expression régulière `SAMSUNG.*`) est surlignée en jaune pour indiquer que celle-ci et la règle principale sont des règles d'expressions régulières qui s'appliquent à un même champ dans le connecteur pour Exchange ActiveSync. Dans ce cas, ce champ est ActiveSync device ID. Les expressions régulières peuvent ou non se chevaucher. C'est à vous de décider si vos expressions régulières sont correctement conçues.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exemple d'expression complexe

De nombreux remplacements, conflits ou compléments sont susceptibles de se produire, c'est pourquoi il est impossible de fournir des exemples couvrant tous les scénarios envisageables. L'exemple suivant explique ce qu'il ne faut pas faire, et sert aussi à illustrer toute la portée de la présentation visuelle de l'analyse des règles. La plupart des éléments sont soulignés dans la figure ci-après. Plusieurs des éléments s'affichent dans une police plus claire, ce qui indique que la règle en question a été remplacée par une règle dont la priorité est plus élevée. Un certain nombre de règles d'expressions régulières sont incluses dans la liste, comme l'indique l'icône .

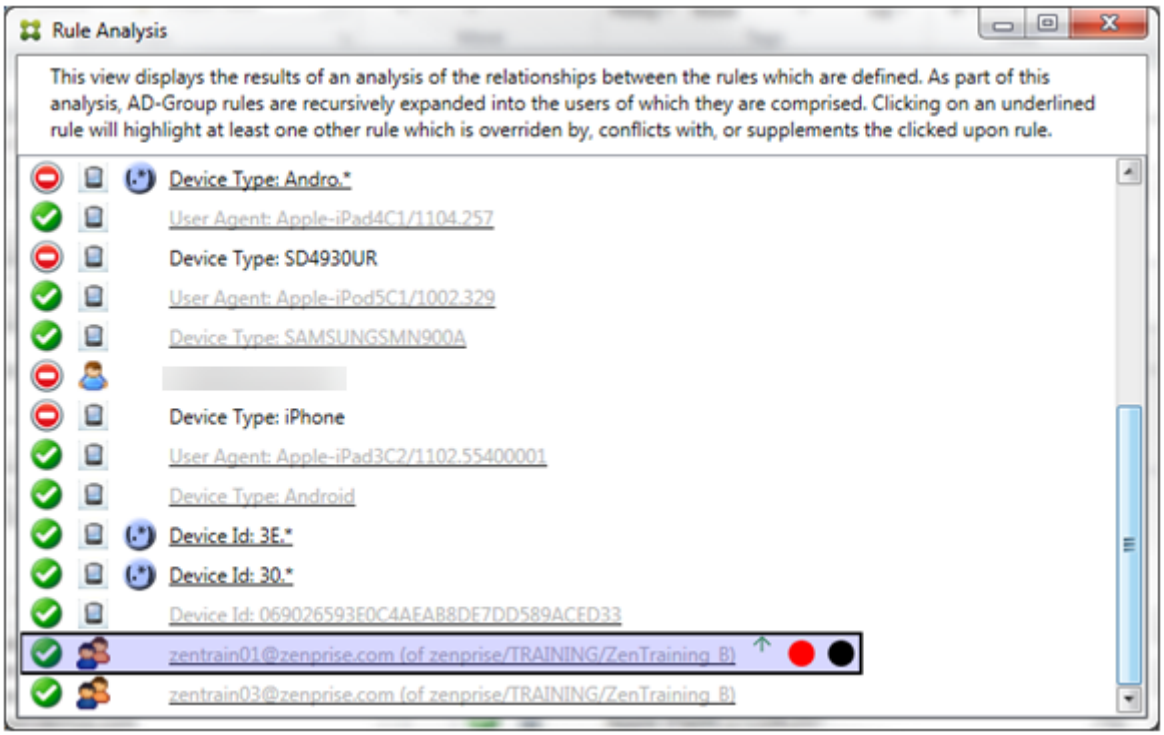


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Comment analyser un remplacement

Pour afficher la ou les règles qui ont remplacé une règle particulière, cliquez sur cette dernière.

Exemple 1 : cet exemple explique pourquoi `zentrain01@zenprise.com` a été remplacée.

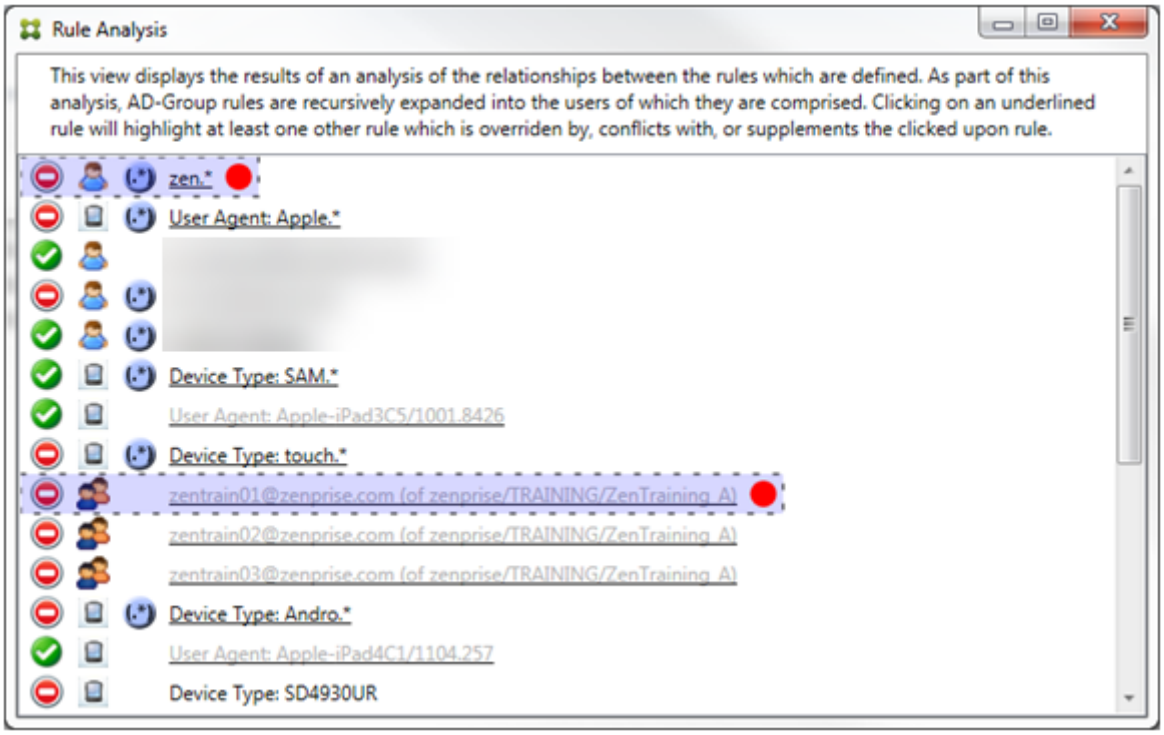


La règle principale (règle de groupe AD `zenprise/TRAINING/ZenTraining B`, dont `zentrain01@zenprise.com` est un membre) présente les caractéristiques suivantes :

- Est surlignée en bleu et encadrée par une bordure pleine.
- A une flèche verte pointant vers le haut (pour indiquer que la règle secondaire ou l'ensemble des règles se trouvent au-dessus).
- Est suivie d'un cercle rouge et d'un cercle noir pour indiquer respectivement qu'une ou plusieurs règles secondaires sont en conflit et que la règle principale a été remplacée et n'est donc pas active.

Si vous faites défiler vers le haut, vous pouvez voir ce qui suit :

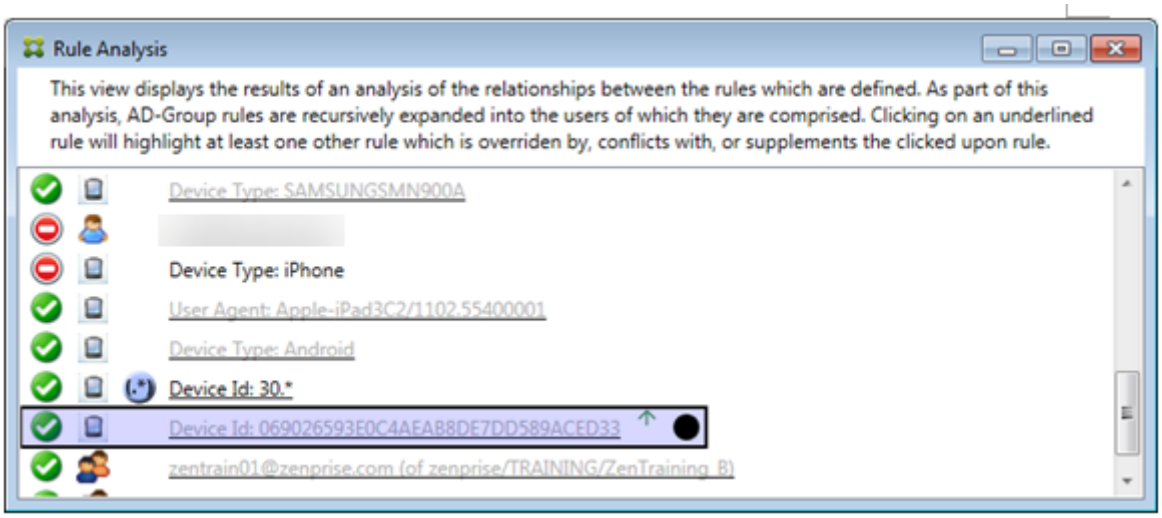
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Dans ce cas, il existe deux règles secondaires qui remplacent la règle principale : la règle d'expression régulière `zen.*` et la règle normale `zentrain01@zenprise.com` (de `zenprise/TRAINING/ZenTraining A`). Dans le cas de la dernière règle secondaire, la règle de groupe Active Directory `ZenTraining A` contient l'utilisateur `zentrain01@zenprise.com` et la règle de groupe Active Directory `ZenTraining B` contient aussi l'utilisateur `zentrain01@zenprise.com`. Toutefois, étant donné que la règle secondaire a une priorité plus élevée que la règle principale, la règle principale a été remplacée. L'accès à la règle principale est Autoriser. Et comme l'accès des deux règles secondaires est Bloquer, toutes sont suivies d'un cercle rouge indiquant un conflit d'accès.

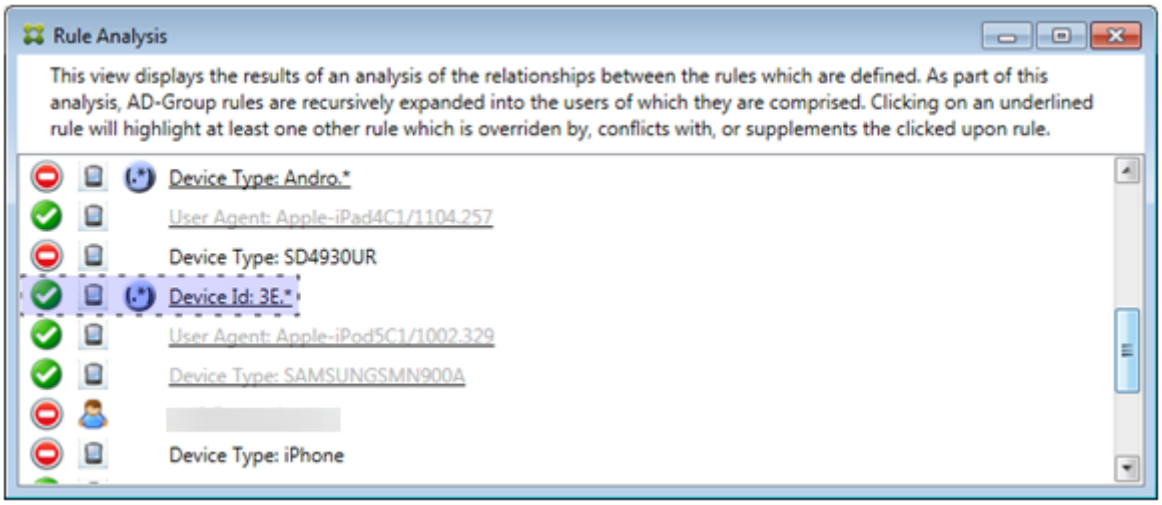
Exemple 2 : cet exemple illustre la raison pour laquelle l'appareil avec l'ID d'appareil ActiveSync `069026593E0C4AEAB8DE7DD589ACED33` a été remplacé :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



La règle principale (règle d'ID d'appareil normale `069026593E0C4AEAB8DE7DD589ACED33`) présente les caractéristiques suivantes :

- Est surlignée en bleu et encadrée par une bordure pleine.
- A une flèche verte pointant vers le haut (pour indiquer que la règle secondaire doit se trouver au-dessus).
- Est suivie par un cercle noir indiquant qu'une règle secondaire a remplacé la règle principale et que la règle est par conséquent inactive.



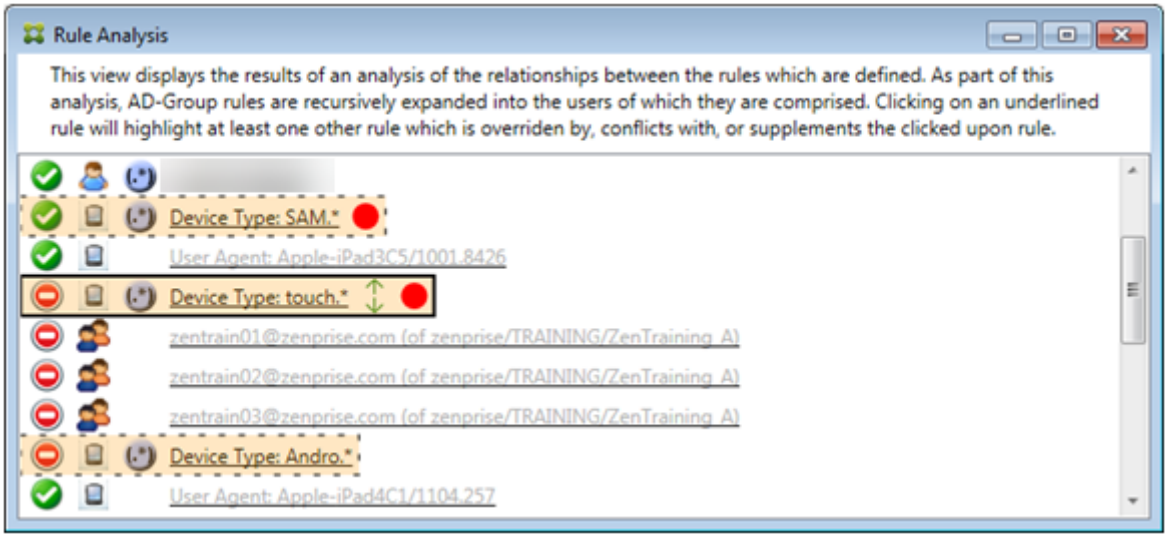
Dans ce cas, une seule règle secondaire remplace la règle principale : la règle d'expression régulière d'ID d'appareil ActiveSync est `3E.*`. Comme l'expression régulière `3E.*` correspond à `069026593E0C4AEAB8DE7DD589ACED33`, la règle ne sera jamais évaluée.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Comment analyser un supplément et un conflit

Dans ce cas, la règle principale est la règle d'expression régulière de type d'appareil ActiveSync `touch.*` Les caractéristiques sont les suivantes :

- Est signalée par une bordure pleine et surlignée en jaune indiquant qu'il y a plus d'une seule règle d'expression régulière appelant le même champ de règle, dans ce cas, ActiveSync device type.
- Deux flèches pointant vers le haut et vers le bas, ce qui indique qu'il existe au moins une règle secondaire avec une priorité plus élevée et au moins une règle secondaire avec une priorité inférieure.
- Le cercle rouge à côté indique qu'au moins une règle secondaire a son accès défini sur **Allow**, ce qui entre en conflit avec l'accès de la règle principale qui est défini sur **Block**
- Il existe deux règles secondaires : la règle d'expression régulière ActiveSync Device Type `SAM.*` et la règle d'expression régulière ActiveSync Device Type `Andro.*`.
- Les deux règles secondaires sont encadrées par des pointillés pour indiquer qu'elles sont secondaires.
- Les règles secondaires sont surlignées en jaune pour indiquer qu'elles s'appliquent aussi au champ de la règle ActiveSync Device Type.
- Vous devez vous assurer dans de tels scénarios que leurs règles d'expressions régulières ne sont pas redondantes.



Comment améliorer l'analyse des règles

Cet exemple explique pourquoi les relations entre les règles sont toujours abordées du point de vue de la règle principale. L'exemple précédent a montré comment un clic sur la règle d'expression régulière

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

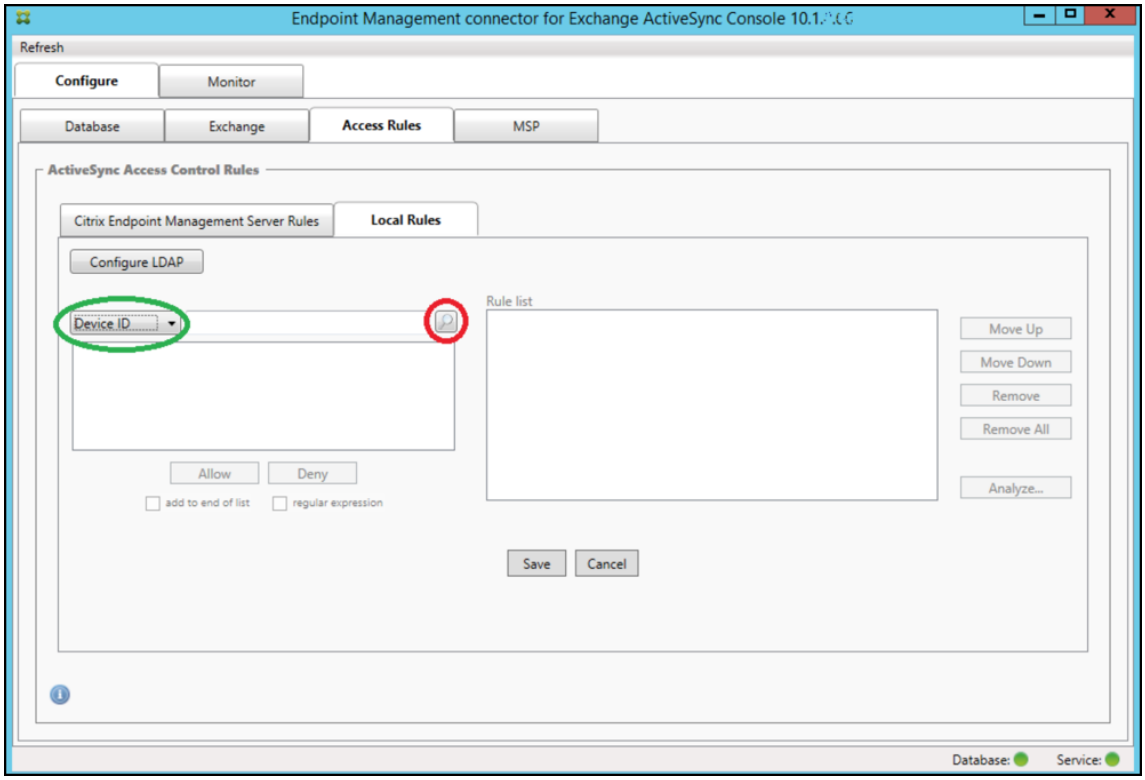
s'appliquait au champ de règle de type de périphérique avec une valeur de `touch.*`. Un clic sur la règle secondaire `Andro.*` montre un ensemble différent de règles secondaires mises en évidence.

Cet exemple présente une règle remplacée qui est inclue dans la relation de règle. Cette règle est la règle normale ActiveSync Device Type `Android`, qui est remplacée (indiquée par une police plus claire et un cercle noir à côté) et qui entre également en conflit avec la règle d'expression régulière principale ActiveSync Device Type `Andro.*`. Cette règle était auparavant une règle secondaire avant d'être sélectionnée. Dans l'exemple précédent, la règle normale ActiveSync Device Type `Android` n'était pas affichée en tant que règle secondaire, car du point de vue de la règle principale (règle d'expression régulière ActiveSync Device Type `touch.*`), elle n'était pas liée.

Pour configurer une règle locale d'expression normale

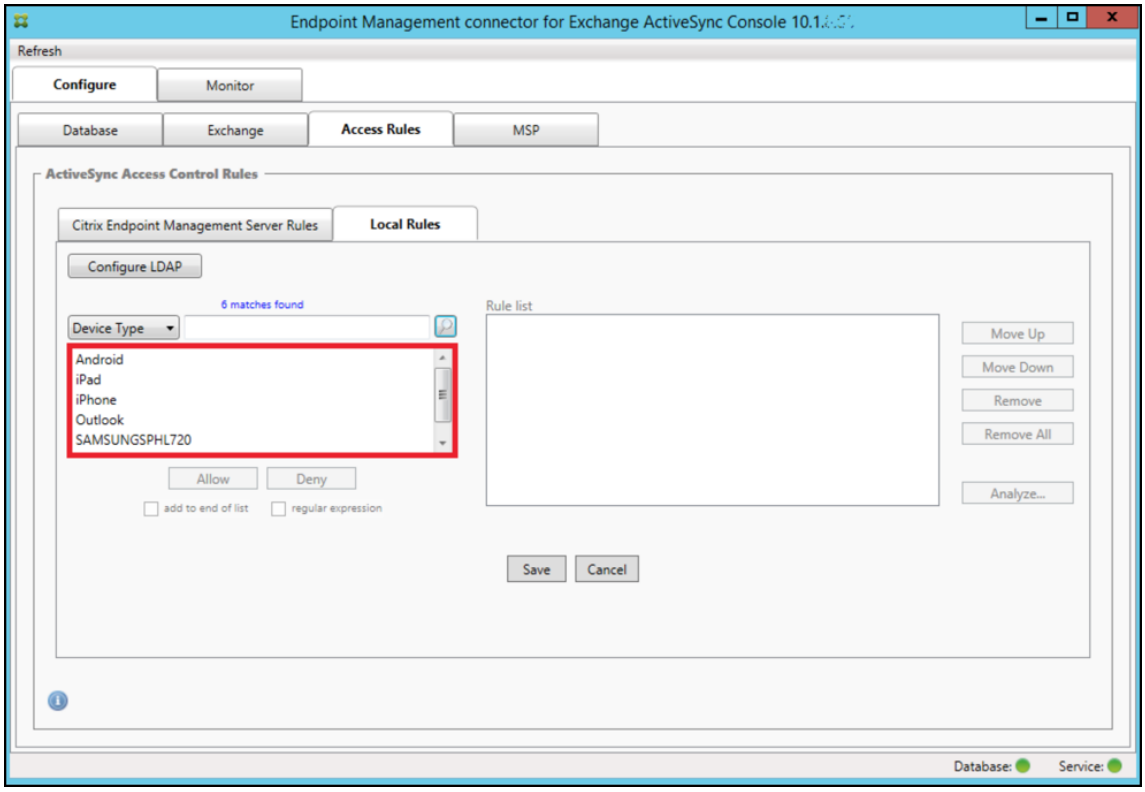
1. Cliquez sur l'onglet **Access Rules**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Dans la liste **Device ID**, sélectionnez le champ pour lequel vous souhaitez créer une règle locale.
3. Cliquez sur l'icône de la loupe pour afficher tous les résultats uniques pour le champ sélectionné. Dans cet exemple, le champ **Device Type** a été choisi et les choix sont affichés ci-dessous dans la zone de liste.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

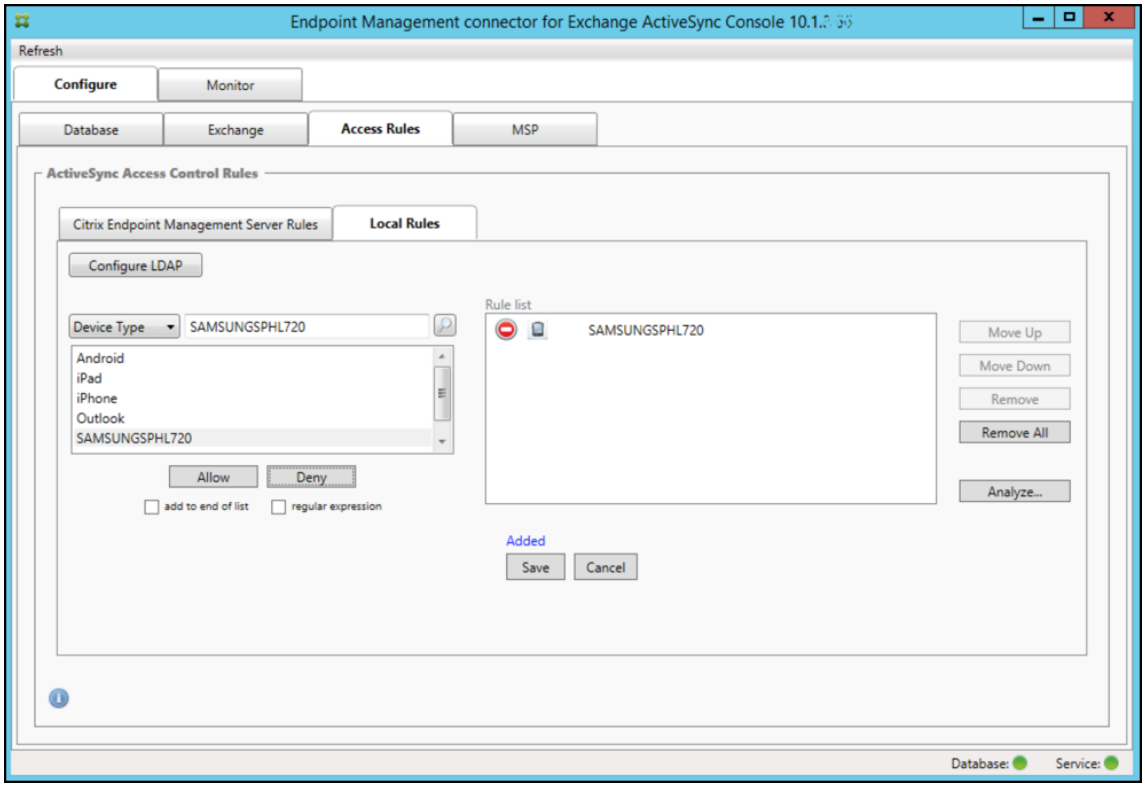


4. Cliquez sur un des éléments dans la liste des résultats et cliquez sur l'une des options suivantes :

   - **Allow** signifie qu'Exchange sera configuré pour permettre le trafic ActiveSync pour tous les appareils correspondant.
   - **Deny** signifie que Exchange sera configuré de manière à refuser le trafic ActiveSync de tous les appareils correspondant.

   Dans cet exemple, les appareils dont le type est SamsungSPhl720 se voient refuser l'accès.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



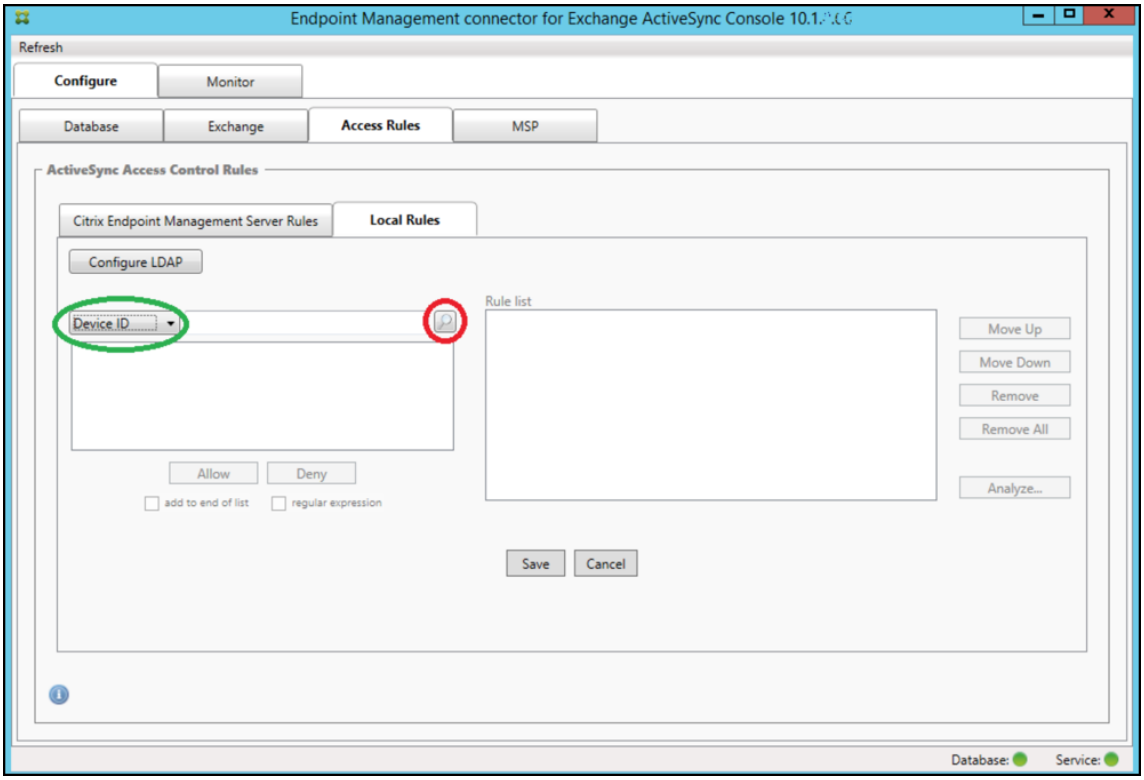
Pour ajouter une expression régulière

Les règles locales d'expressions régulières peuvent être différenciées par l'icône qui s'affiche à leur côté -  . Pour ajouter une règle d'expression régulière, vous pouvez créer une règle d'expression régulière à partir d'une valeur existante dans la liste des résultats pour un champ donné (si un instantané principal a été effectué), ou vous pouvez simplement saisir l'expression régulière que vous souhaitez.

Pour créer une expression régulière à partir d'une valeur de champ existant

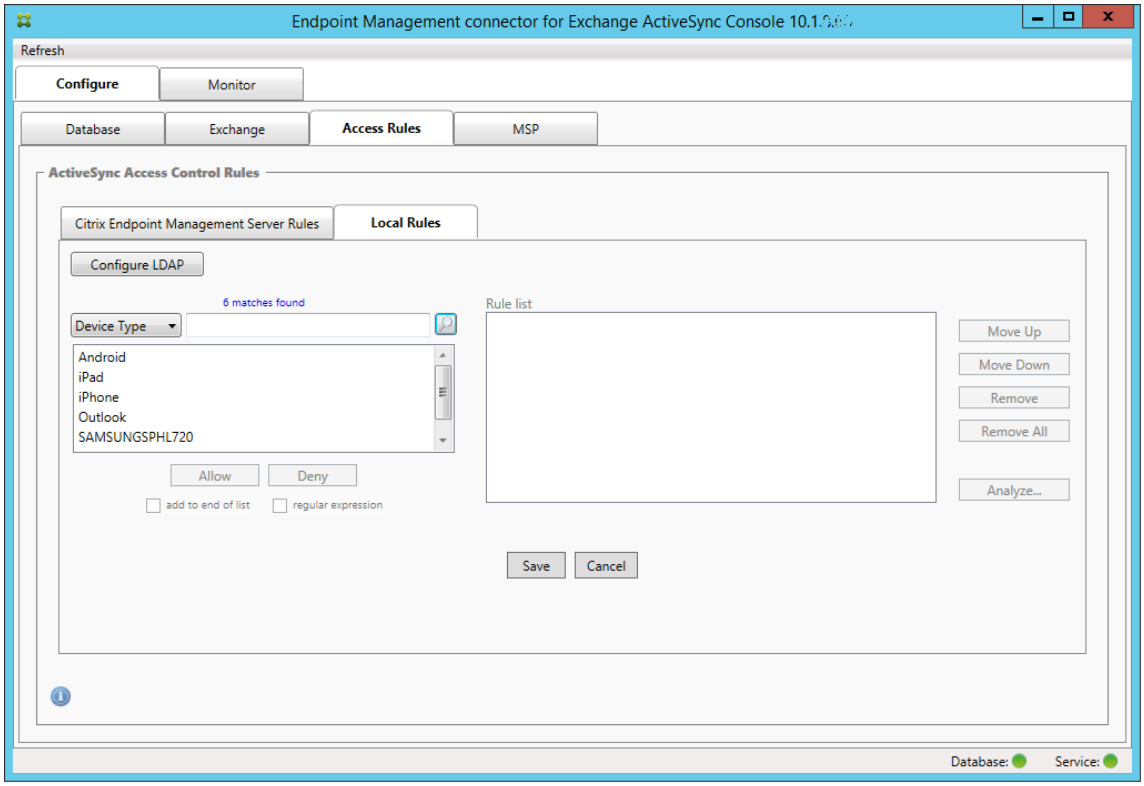
1. Cliquez sur l'onglet **Access Rules**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

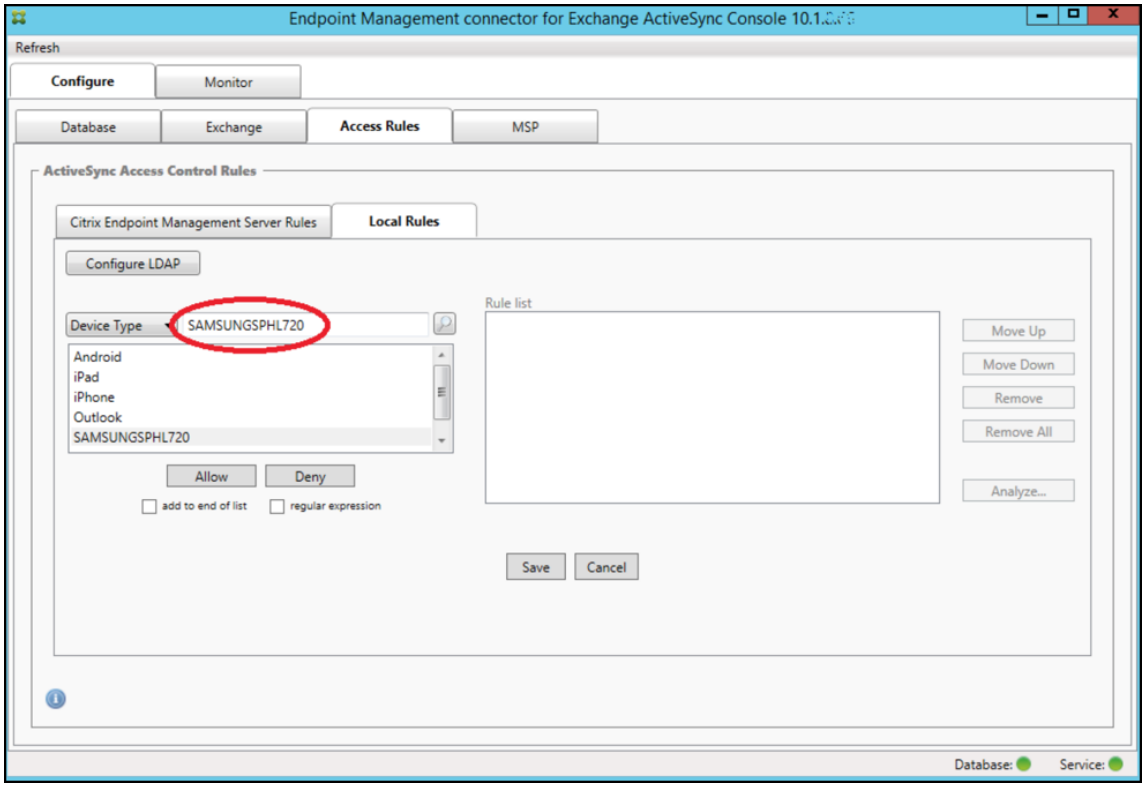


2. Dans la liste **Device ID**, sélectionnez le champ pour lequel vous souhaitez créer une règle d' expression régulière locale.
3. Cliquez sur l'icône de la loupe pour afficher tous les résultats uniques pour le champ sélectionné. Dans cet exemple, le champ **Device Type** a été choisi et les choix sont affichés ci-dessous dans la zone de liste.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Cliquez sur un des éléments dans la liste des résultats. Dans cet exemple, **SAMSUNGSPHL720** a été sélectionné et s'affiche dans la zone de texte adjacente à **Device Type**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

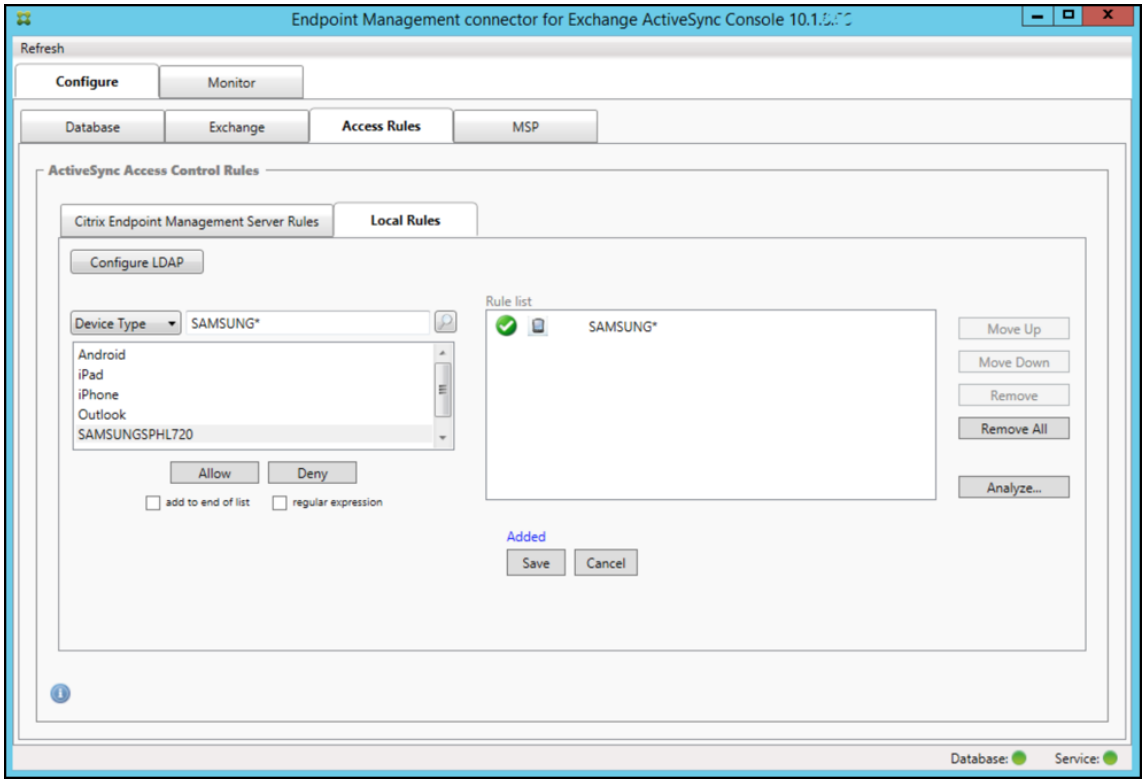
5. Pour autoriser tous les types d'appareils qui ont « Samsung » dans leur valeur Device Type, ajoutez une règle d'expression régulière en suivant les étapes suivantes :

   a. Cliquez dans la zone de texte de l'élément sélectionné.

   b. Remplacez le texte **SAMSUNGSPHL720** par **SAMSUNG.***.

   c. Vérifiez que la case regular expression est cochée.

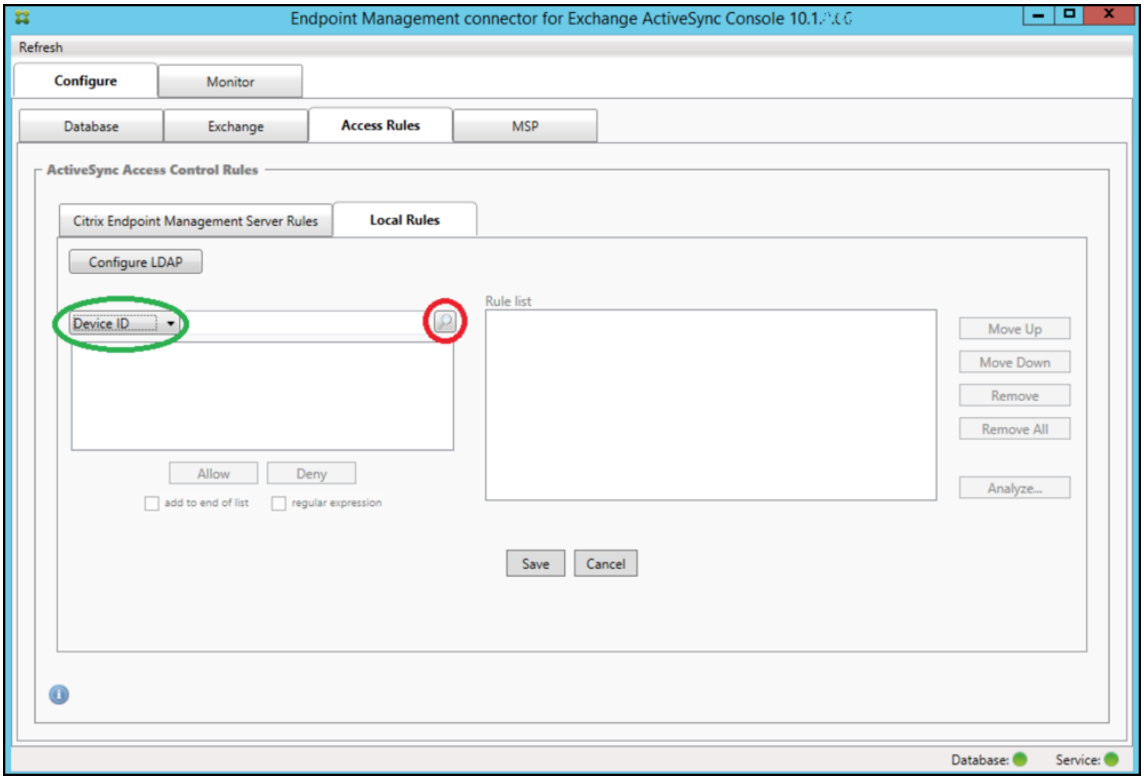
   d. Cliquez sur **Allow**.



Pour créer une règle d'accès

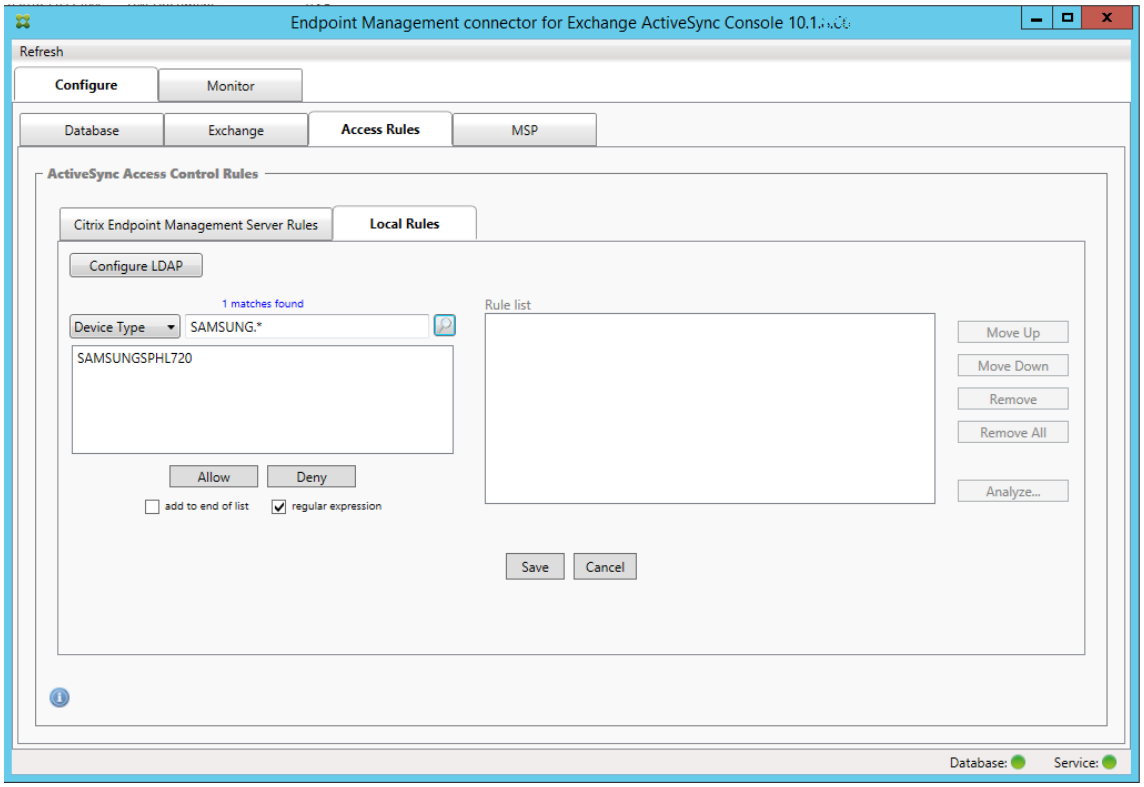
1. Cliquez sur l'onglet **Local Rules**.
2. Pour entrer l'expression régulière, vous devez utiliser la liste Device ID et la zone de texte de l'élément sélectionné.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Sélectionnez le champ que vous voulez mettre en correspondance. Cet exemple utilise **Device Type**.
4. Entrez l'expression régulière. Cet exemple utilise `samsung.*`
5. Assurez-vous que la case regular expression est cochée et cliquez sur **Allow** ou **Deny**. Dans cet exemple, le choix est **Allow**. Le résultat final est le suivant :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

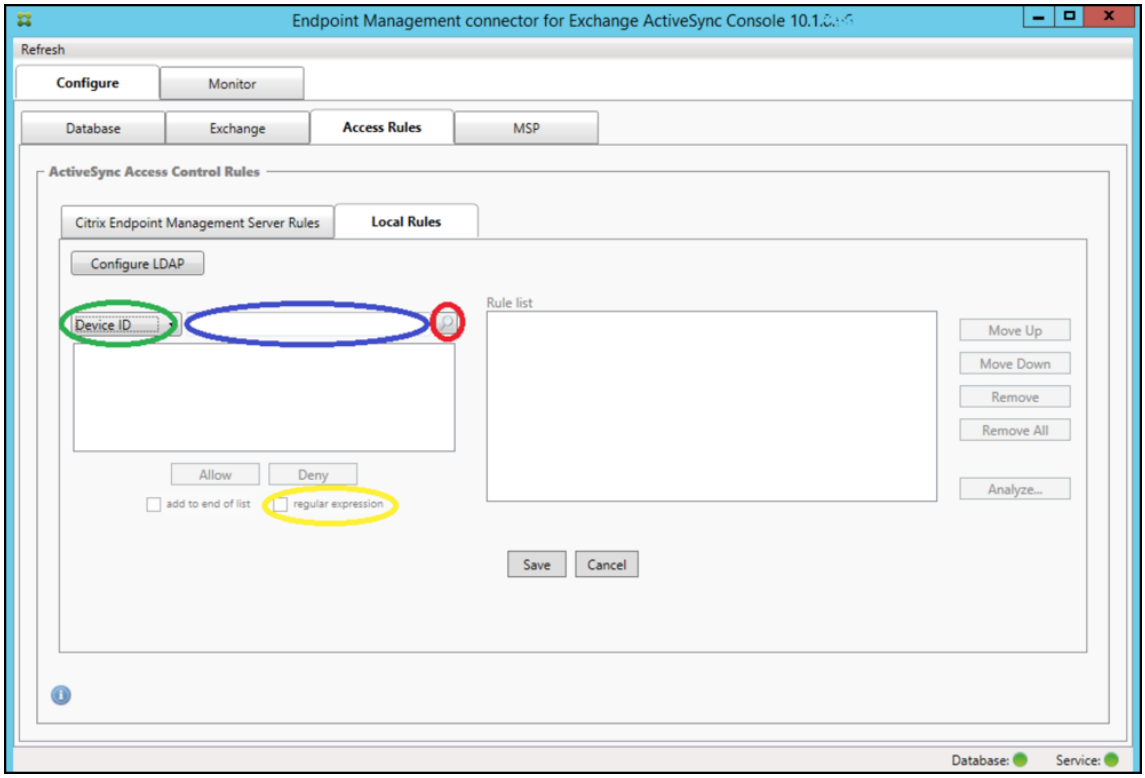


Pour rechercher des appareils

En cochant la case « regular expression », vous pouvez rechercher des appareils correspondant à l'expression donnée. Cette fonction est uniquement disponible si un instantané principal a été effectué. Vous pouvez utiliser cette fonction, même si vous ne prévoyez pas d'utiliser des règles d'expressions régulières. Imaginons que vous souhaitiez rechercher tous les appareils contenant `workmail` dans l'ID d'appareil ActiveSync. Pour ce faire, suivez cette procédure.

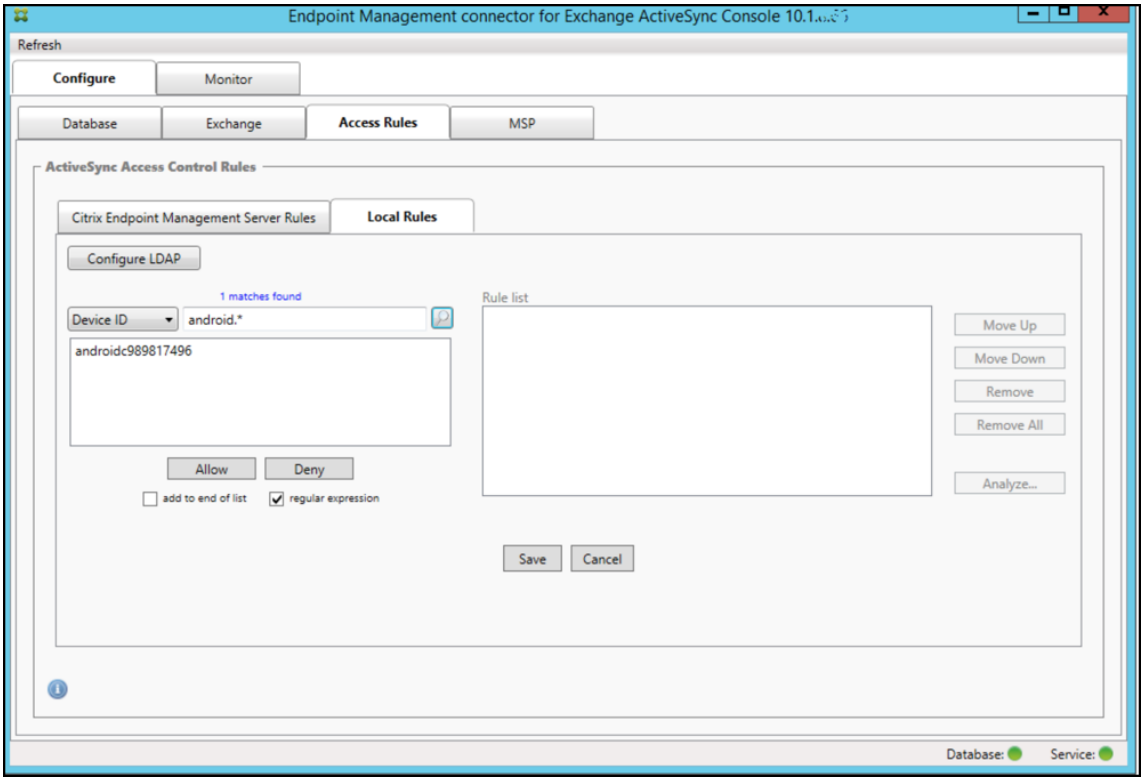
1. Cliquez sur l'onglet **Access Rules**.
2. Assurez-vous que le sélecteur de champ d'appareil est défini sur Device ID (valeur par défaut).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Cliquez sur la zone de texte de l'élément sélectionné (comme illustré en bleu dans la figure précédente) puis tapez `workmail.*`.
4. Vérifiez que la case d'expression régulière est cochée et cliquez sur l'icône de la loupe pour afficher les correspondances comme illustré dans la figure suivante.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



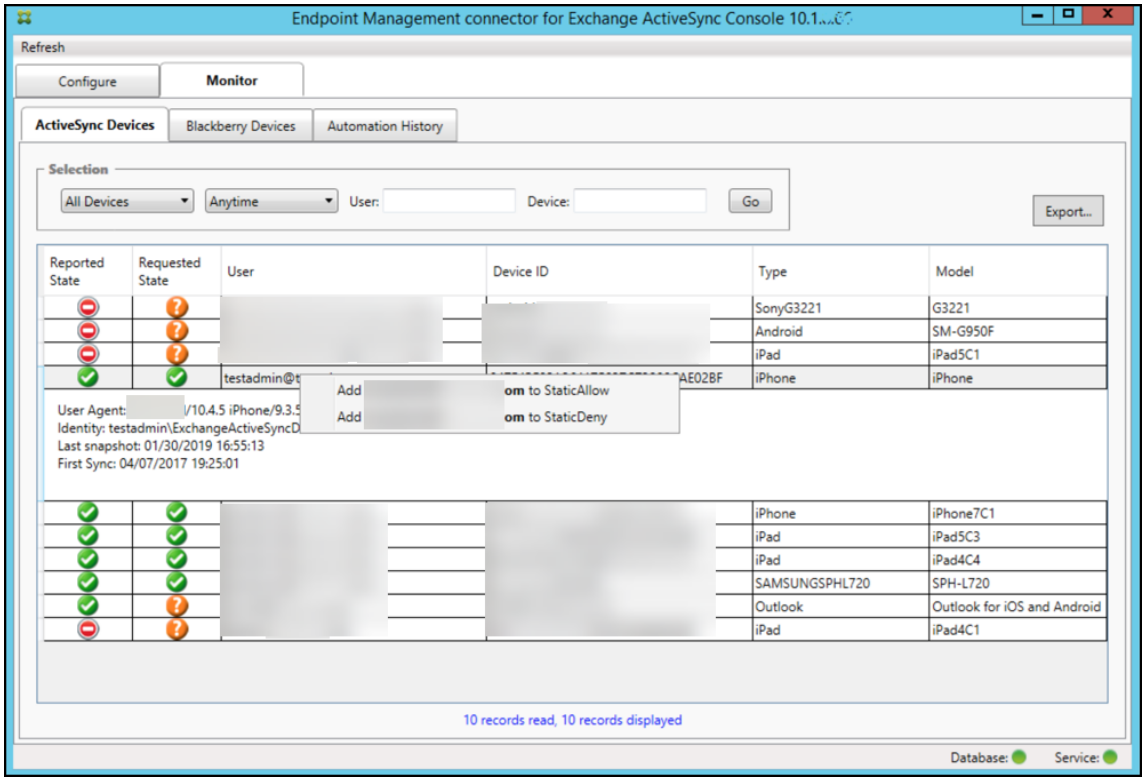
Pour ajouter un seul utilisateur, appareil ou type d'appareil à une règle statique

Vous pouvez ajouter des règles statiques basées sur l'utilisateur, l'ID d'appareil ou le type d'appareil sur l'onglet ActiveSync Devices.

1. Cliquez sur l'onglet **ActiveSync Devices**.
2. Dans la liste, cliquez avec le bouton droit sur un utilisateur, un appareil ou un type d'appareil et choisissez si vous souhaitez autoriser ou refuser votre sélection.

   L'image suivante montre l'option Allow/Deny lorsque user1 est sélectionné.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Surveillance des appareils

L'onglet **Monitor** de Citrix Endpoint Management Connector pour Exchange ActiveSync permet de visualiser les appareils Exchange ActiveSync et BlackBerry qui ont été détectés et l'historique des commandes PowerShell automatisées qui ont été émises. L'onglet **Monitor** inclut les trois onglets suivants :

- **Appareils ActiveSync :**
  - Vous pouvez exporter les partenariats d'appareils ActiveSync affichés en cliquant sur le bouton **Export**.
  - Vous pouvez ajouter des règles locales (statiques) en cliquant avec le bouton droit sur les colonnes **User**, **Device ID** où **Type** et en choisissant la règle d'autorisation ou de blocage appropriée.
  - Pour réduire une ligne développée, faites un Ctrl-clic sur la ligne développée.
- **Appareils BlackBerry**
- **Historique d'automatisation**

L'onglet **Configure** affiche l'historique de tous les instantanés. L'historique d'instantané affiche le moment où l'instantané a été capturé, la durée nécessaire à la capture, le nombre d'appareils détectés et toutes les erreurs qui se sont produites :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Sur l'onglet **Exchange**, cliquez sur l'icône d'information pour le serveur Exchange Server désiré.

Dépannage et diagnostics

Citrix Endpoint Management Connector pour Exchange ActiveSync consigne les erreurs et d'autres informations opérationnelles dans son fichier journal : *dossier d'installation*\log\XmmWindowsService.log. Le connecteur pour Exchange ActiveSync consigne également les événements importants dans le journal d'événements Windows.

Modifier le niveau de journalisation

Le connecteur Citrix Endpoint Management pour Exchange ActiveSync inclut les niveaux de journalisation suivants : Error, Info, Warn, Debug et Trace.

> **Remarque :**
>
> Chaque niveau successif génère plus de détails (plus de données). Par exemple, le niveau Error fournit le moins de détails, tandis que le niveau Trace fournit le plus de détails.

Pour modifier le niveau de journalisation, procédez comme suit :

1. Dans `C:\Program Files\Citrix\Citrix` Citrix Endpoint Management connector, ouvrez le fichier nlog.config.
2. Dans la section `<rules>`, remplacez le paramètre *minilevel* par le niveau de journalisation souhaitée. Par exemple :

```
    <rules >

    <logger name="*" writeTo="file" minlevel="Debug" />

    </rules>
<!--NeedCopy-->
```

3. Enregistrez le fichier.

   Les modifications prennent effet immédiatement. Vous n'avez pas besoin de redémarrer le connecteur pour Exchange ActiveSync.

Erreurs fréquentes

La liste suivante contient des erreurs courantes :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Le connecteur pour le service Exchange ActiveSync ne démarre pas

  En cas d'erreurs, consultez le fichier journal et le journal des événements Windows. Les raisons habituelles sont les suivantes :

  - Le connecteur pour le service Exchange ActiveSync ne peut pas accéder au serveur SQL. Cela peut être dû aux problèmes suivants :

    * Le service SQL Server n'est pas exécuté.
    * Échec de l'authentification.

    Si l'authentification Windows Integrated n'est pas configurée, le compte utilisateur du connecteur pour Exchange ActiveSync doit être une ouverture de session SQL autorisée. Le compte du connecteur pour le service Exchange ActiveSync est par défaut le compte système local, mais il peut être remplacé par un autre compte disposant des privilèges d'administrateur local. Si l'authentification SQL est configurée, l'ouverture de session SQL doit être correctement configurée dans SQL.

Outils de résolution des problèmes

Des utilitaires PowerShell destinés au dépannage sont disponibles dans le dossier Support\PowerShell.

Un outil de dépannage effectue une analyse approfondie des boîtes aux lettres et appareils des utilisateurs, détecte les conditions d'erreur et les zones de défaillance potentielles, et réalise également une analyse approfondie des RBAC (contrôle d'accès basé sur un rôle) des utilisateurs. Il peut enregistrer une sortie brute de toutes les applets de commande sur un fichier texte.

NetScaler Gateway Connector pour Exchange ActiveSync

March 1, 2024

XenMobile NetScaler Connector est maintenant nommé NetScaler Gateway Connector pour Exchange ActiveSync. Pour plus de détails sur le portefeuille unifié de Citrix, consultez le guide des produits Citrix.

Ce connecteur pour Exchange ActiveSync fournit un service d'autorisation au niveau de l'appareil des clients ActiveSync à NetScaler Gateway qui fait office de proxy inverse pour le protocole Exchange ActiveSync. Vous contrôlez l'autorisation au moyen d'une combinaison de :

- Stratégies que vous définissez dans Citrix Endpoint Management
- Règles définies localement par NetScaler Gateway Connector pour Exchange ActiveSync

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour de plus amples informations, consultez la section ActiveSync Gateway.

Pour un diagramme d'architecture de référence détaillé, voir Architecture.

La version actuelle de NetScaler Gateway Connector pour Exchange ActiveSync est la version 8.5.3.

Pour télécharger le connecteur :

1. Accédez à https://www.citrix.com/downloads.
2. Accédez à **Citrix Endpoint Management (et Citrix XenMobile Server) > XenMobile Server (local) > Logiciel produit > XenMobile Server 10 > Composants serveur**.
3. Sur la vignette **NetScaler Gateway Connector**, cliquez sur **Télécharger le fichier**.

Pour installer le connecteur, reportez-vous à la section Installation de NetScaler Gateway Connector pour Exchange ActiveSync.

> **Important :**
>
> À compter d'octobre 2022, les connecteurs Citrix Endpoint Management et NetScaler Gateway pour Exchange ActiveSync ne prendront plus en charge Exchange Online en raison des modifications d'authentification annoncées par Microsoft ici. Le connecteur Citrix Endpoint Management pour Exchange continuera de fonctionner avec Microsoft Exchange Server (déploiement local).

Nouveautés dans la version 8.5.3

- Cette version ajoute la prise en charge des protocoles ActiveSync 16.0 et 16.1.
- Plus de détails ont été ajoutés aux analyses envoyées à Google Analytics, notamment concernant les instantanés. [CXM-52261]

Nouveautés dans les versions précédentes

> **Remarque :**
>
> La section Nouveautés suivante fait référence à NetScaler Gateway Connector pour Exchange ActiveSync sous son ancien nom XenMobile NetScaler Connector. Le nom a changé à partir de la version 8.5.2.

Nouveautés dans la version 8.5.2

- XenMobile NetScaler Connector est maintenant nommé NetScaler Gateway Connector pour Exchange ActiveSync.

Les problèmes suivants ont été résolus dans cette version :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si plusieurs critères sont utilisés dans la définition d'une règle de stratégie et si un critère implique l'ID utilisateur, le problème suivant peut se produire. Si un utilisateur a plusieurs alias, les alias ne sont pas également vérifiés lors de l'application de la règle. [CXM-55355]

Nouveautés dans la version 8.5.1.11

- **Modification de la configuration système requise :** la version actuelle de NetScaler Connector requiert Microsoft .NET Framework 4.5.
- **Prise en charge de Google Analytics :** nous souhaitons savoir comment vous utilisez le connecteur afin de pouvoir nous concentrer sur l'amélioration du produit.
- **Prise en charge de TLS 1.1 et 1.2 :** en raison de leur faible niveau de sécurité, TLS 1.0 et TLS 1.1 ont été déclarés obsolètes par le PCI Council. La prise en charge de TLS 1.2 est ajoutée à XenMobile NetScaler Connector.

Surveillance de NetScaler Gateway Connector pour Exchange ActiveSync

L'utilitaire de configuration de NetScaler Gateway Connector pour Exchange ActiveSync fournit une journalisation détaillée. Utilisez les journaux pour afficher tout le trafic passant par votre serveur Exchange Server que Secure Mobile Gateway autorise ou bloque.

Utilisez l'onglet **Log** pour afficher l'historique des demandes ActiveSync transmises à Citrix Gateway Connector pour Exchange ActiveSync pour autorisation.

De plus, pour vous assurer que le connecteur pour le service Web Exchange ActiveSync est en cours d'exécution, chargez l'adresse URL suivante dans un navigateur sur le serveur du connecteur `https://<host:port>/services/ActiveSync/Version`. Si l'adresse URL retourne la version du produit en tant que chaîne, le service Web est réactif.

Simulation de trafic ActiveSync avec le connecteur pour Exchange ActiveSync

Vous pouvez utiliser NetScaler Gateway Connector pour Exchange ActiveSync pour simuler le trafic ActiveSync avec vos stratégies. Dans l'outil de configuration du connecteur, cliquez sur l'onglet **Simulator**. Les résultats vous montrent comment vos stratégies s'appliquent aux règles que vous avez configurées.

Choix des filtres pour le connecteur pour Exchange ActiveSync

Les filtres NetScaler Gateway Connector pour Exchange ActiveSync analysent un appareil à la recherche d'une violation de stratégie ou d'un paramètre de propriété donné. Si l'appareil est

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

conforme aux critères, l'appareil est placé dans une liste d'appareils. Cette liste d'appareils n'est ni une liste d'autorisation ni une liste de blocage. Il s'agit d'une liste d'appareils qui répondent aux critères définis. Les filtres suivants sont disponibles pour le connecteur pour Exchange ActiveSync dans Citrix Endpoint Management. Les deux options pour chaque filtre sont **Autoriser** ou **Refuser**.

- **Appareils anonymes :** autorise ou refuse les appareils qui sont inscrits dans Citrix Endpoint Management, mais l'identité de l'utilisateur est inconnue. Par exemple, un utilisateur inscrit possède une identité inconnue si l'utilisateur possède un mot de passe Active Directory expiré ou des informations d'identification inconnues.
- **Applications sur liste noire :** autorise ou refuse les appareils en fonction de la liste des appareils définie par les listes de blocage dans les stratégies et de la présence d'applications sur une liste de blocage.
- **Autorisations et refus implicite :** crée une liste d'appareils de tous les appareils qui ne répondent pas à tous les critères de règle de filtre et les autorise ou les refuse en se basant sur cette liste. L'option Autorisation/refus implicite garantit que l'état du connecteur pour Exchange ActiveSync dans l'onglet Appareils est activé et affiche l'état du connecteur pour vos appareils. L'option Autorisation/refus implicite contrôle également tous les autres filtres du connecteur qui ne sont pas sélectionnés. Par exemple, le connecteur refuse les applications figurant sur la liste de blocage. Toutefois, le connecteur autorise tous les autres filtres car l'option Autorisation/refus implicite est définie sur **Autoriser**.
- **Appareils inactifs :** crée une liste d'appareils des appareils qui n'ont pas communiqué avec Citrix Endpoint Management dans une période de temps spécifiée. Ces appareils sont considérés comme inactifs. Le filtre autorise ou refuse les appareils en conséquence.
- **Applications requises manquantes :** lorsqu'un utilisateur s'inscrit, l'utilisateur reçoit une liste des applications requises qui doivent être installées. Le filtre des applications requises manquantes indique qu'une ou plusieurs applications ne sont plus présentes ; par exemple, l'utilisateur a supprimé une ou plusieurs applications.
- **Applications non suggérées :** lorsqu'un utilisateur s'inscrit, l'utilisateur reçoit une liste des applications à installer. Le filtre des applications non suggérées vérifie que l'appareil ne contient pas d'applications qui ne figurent pas dans cette liste.
- **Mot de passe non conforme :** crée une liste d'appareils de tous les appareils qui ne disposent pas d'un code secret sur l'appareil.
- **Appareils non conformes :** vous permet d'interdire ou d'autoriser des appareils qui répondent à vos critères de conformité informatiques internes. La conformité est un paramètre arbitraire défini par la propriété d'appareil nommée Non conforme, qui est un indicateur booléen qui peut être soit **True** soit **False**. (Vous pouvez créer cette propriété manuellement et définir la valeur. Vous pouvez également utiliser des actions automatisées pour créer cette propriété sur un appareil, selon que celui-ci répond à des critères spécifiques.)
  - **Non conforme = True :** si un appareil ne répond pas aux normes de conformité et aux définitions de stratégie définies par votre service informatique, l'appareil n'est pas conforme.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Non conforme = False :** si un appareil répond aux normes de conformité et aux définitions de stratégie définies par votre service informatique, l'appareil est conforme.

- **État révoqué :** crée une liste d'appareils de tous les appareils révoqués et les autorise ou les refuse en fonction de l'état de révocation.
- **Android rootés/iOS jailbreakés :** crée une liste d'appareils de tous les appareils marqués comme rootés et les autorise ou les refuse en se basant sur leur état racine.
- **Appareils non gérés :** crée une liste de tous les appareils dans la base de données Citrix Endpoint Management. Déployez Mobile Application Gateway à l'aide d'un modèle restrictif (Block Mode).

Configuration d'une connexion à NetScaler Gateway Connector pour Exchange ActiveSync

NetScaler Gateway Connector pour Exchange ActiveSync communique avec Citrix Endpoint Management et d'autres fournisseurs de configuration à distance via les services Citrix Secure Web.

1. Dans l'outil de configuration du connecteur pour Exchange ActiveSync, cliquez sur l'onglet **Config Providers**, puis cliquez sur **Add**.
2. Dans la boîte de dialogue **Config Providers**, dans **Name**, entrez un nom d'utilisateur disposant des privilèges d'administration et qui est utilisé pour l'autorisation HTTP de base avec le serveur Citrix Endpoint Management.
3. Dans **Url**, entrez l'adresse Web du service Citrix Endpoint Management GCS, généralement au format `https://<FQDN>/<instanceName>/services/<MagConfigService>`. Le nom *MagConfigService* est sensible à la casse.
4. Dans **Password**, saisissez le mot de passe utilisé pour l'autorisation HTTP de base avec le serveur Citrix Endpoint Management.
5. Dans **Managing Host**, entrez le nom du serveur du connecteur pour Exchange ActiveSync.
6. Dans **Baseline Interval**, spécifiez une période de temps après laquelle un nouveau ruleset dynamique actualisé est extrait depuis Citrix Endpoint Management.
7. Dans **Delta interval**, spécifiez une période de temps après laquelle une mise à jour de règles dynamiques est extraite.
8. Dans **Request Timeout**, spécifiez l'intervalle d'expiration du délai de demande du serveur.
9. Dans **Config Provider**, sélectionnez si l'instance de serveur du fournisseur de configuration fournit la configuration de la stratégie.
10. Dans **Events Enabled**, activez cette option si vous souhaitez que le connecteur pour Exchange ActiveSync informe Citrix Endpoint Management lorsqu'un appareil est bloqué. Cette option est requise si vous utilisez les règles du connecteur dans l'une de vos actions automatisées Citrix Endpoint Management.
11. Cliquez sur **Save**, puis cliquez sur **Test Connectivity** pour tester la connectivité du fournisseur

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de configuration vers la passerelle. Si la connexion échoue, vérifiez que les paramètres du pare-feu local acceptent la connexion ou contactez votre administrateur.

12. Si la connexion réussit, désactivez la case à cocher **Disabled**, puis cliquez sur **Save**.

Lorsque vous ajoutez un fournisseur de configuration, le connecteur pour Exchange ActiveSync crée automatiquement une ou plusieurs stratégies associées au fournisseur. Une définition de modèle contenue dans `config\policyTemplates.xml` dans la section `NewPolicyTemplate` définit les stratégies. Pour chaque élément Policy est défini dans cette section, une nouvelle stratégie est créée.

L'opérateur peut ajouter, supprimer ou modifier les éléments de stratégie si les conditions suivantes sont remplies : l'élément de stratégie est conforme à la définition du schéma et les chaînes de substitution standard (entre accolades) ne sont pas modifiées. Ajoutez ensuite de nouveaux groupes pour le fournisseur et mettez à jour la stratégie pour inclure les nouveaux groupes.

Pour importer une stratégie depuis Citrix Endpoint Management

1. Dans l'outil de configuration du connecteur pour Exchange ActiveSync, cliquez sur l'onglet **Config Providers**, puis cliquez sur **Add**.
2. Dans la boîte de dialogue **Config Providers**, dans **Name**, entrez un nom d'utilisateur pour l'autorisation HTTP de base avec Citrix Endpoint Management. L'utilisateur doit disposer des privilèges d'administrateur.
3. Dans **Url**, entrez l'adresse Web du service Citrix Endpoint Management Gateway Configuration Service (GCS), généralement au format `https://<xdmHost>/xdm/services/<MagConfigService>`. Le nom MagConfigService est sensible à la casse.
4. Dans **Password**, saisissez le mot de passe qui est utilisé pour l'autorisation HTTP de base avec le serveur Citrix Endpoint Management.
5. Cliquez sur **Test Connectivity** pour tester la connectivité du fournisseur de configuration vers la passerelle. Si la connexion échoue, vérifiez que vos paramètres locaux de pare-feu autorisent la connexion ou contactez votre administrateur.
6. Lorsqu'une connexion est établie, désactivez la case à cocher **Disabled**, puis cliquez sur **Save**.
7. Dans **Managing Host**, laissez la valeur par défaut du nom DNS de l'ordinateur hôte. Ce paramètre est utilisé pour coordonner les communications avec Citrix Endpoint Management lorsque plusieurs serveurs Forefront Threat Management Gateway (TMG) sont configurés dans un tableau.

   Lorsque vous enregistrez les paramètres, ouvrez le GCS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration du mode de stratégie de NetScaler Gateway Connector pour Exchange ActiveSync

NetScaler Gateway Connector pour Exchange ActiveSync peut être exécuté dans les six modes suivants :

- **Allow All :** ce mode de stratégie accorde l'accès à tout le trafic passant via le connecteur pour Exchange ActiveSync. Aucune autre règle de filtrage n'est utilisée.
- **Deny All:** ce mode de stratégie bloque l'accès à tout le trafic passant via le connecteur pour Exchange ActiveSync. Aucune autre règle de filtrage n'est utilisée.
- **Static Rules: Block Mode :** ce mode de stratégie exécute des règles statiques avec une instruction implicite de blocage ou de refus à la fin. Le connecteur pour Exchange ActiveSync bloque les appareils qui ne sont pas autorisés par d'autres règles de filtre.
- **Static Rules: Permit Mode :** ce mode de stratégie exécute des règles statiques avec une instruction implicite d'acceptation ou d'autorisation à la fin. Les appareils qui ne sont pas bloqués ou refusés par d'autres règles de filtre sont autorisés via le connecteur pour Exchange ActiveSync.
- **Static + ZDM Rule**s: Block Mode. Ce mode de stratégie exécute tout d'abord des règles statiques, suivies par des règles dynamiques depuis Citrix Endpoint Management avec une instruction implicite de blocage ou de refus à la fin. Les appareils sont autorisés ou refusés en se basant sur des filtres définis et des règles Citrix Endpoint Management. Tous les appareils qui ne correspondent pas à des filtres et des règles définis sont bloqués.
- **Static + ZDM Rule**s: Permit Mode. Ce mode de stratégie exécute tout d'abord des règles statiques, suivies par des règles dynamiques depuis Citrix Endpoint Management avec une instruction implicite d'acceptation ou d'autorisation à la fin. Les appareils sont autorisés ou refusés en se basant sur des filtres définis et des règles Citrix Endpoint Management. Tous les appareils qui ne correspondent pas à des filtres et des règles définis sont autorisés.

Le connecteur pour Exchange ActiveSync autorise ou bloque les règles dynamiques en se basant sur des ID ActiveSync uniques pour appareils mobiles iOS et Windows reçus d'Citrix Endpoint Management. Les appareils Android changent de comportement en fonction du fabricant et certains n'exposent pas directement d'ID unique ActiveSync. Pour compenser, Citrix Endpoint Management envoie les informations d'ID de l'utilisateur pour les appareils Android pour prendre une décision d'autorisation ou de blocage. Par conséquent, si un utilisateur possède un seul appareil Android, la fonctionnalité d'autorisation et de blocage fonctionne normalement. Si l'utilisateur possède plusieurs appareils Android, tous les appareils sont autorisés, car les appareils Android ne peuvent pas être différenciés. Vous pouvez configurer la passerelle pour bloquer de façon statique ces appareils par ActiveSyncID, s'ils sont connus. Vous pouvez également configurer la passerelle pour qu'elle effectue un blocage en fonction de l'agent utilisateur ou du type d'appareil.

Pour spécifier le mode de stratégie, dans l'outil SMG Controller Configuration, procédez comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Cliquez sur l'onglet **Path Filters**, puis cliquez sur **Add**.
2. Dans la boîte de dialogue **Path Properties**, sélectionnez un mode de stratégie à partir de la liste **Policy**, puis cliquez sur **Save**.

Vous pouvez vérifier les règles sur l'onglet **Policies** de l'outil de configuration. Les règles sont traitées de haut en bas sur le connecteur pour Exchange ActiveSync. Les stratégies autorisées sont affichées avec une coche verte. Les stratégies refusées s'affichent un cercle rouge traversé d'une ligne. Pour actualiser l'écran et afficher les règles mises à jour le plus récemment, cliquez sur **Refresh**. Vous pouvez également modifier l'ordre des règles dans le fichier config.xml.

Pour tester les règles, cliquez sur l'onglet **Simulator**. Spécifiez des valeurs dans les champs. Vous pouvez obtenir les valeurs à partir des journaux. Un message de résultat spécifie Allow ou Block.

Pour configurer des règles statiques

Entrez des règles statiques avec les valeurs qui sont lues par le filtrage ISAPI des lectures de demandes HTTP de connexion ActiveSync. Les règles statiques permettent au connecteur pour Exchange ActiveSync d'autoriser ou de bloquer le trafic en fonction des critères suivants :

- **User :** le connecteur pour Exchange ActiveSync utilise la valeur de l'utilisateur autorisé et la structure de nom qui a été capturée lors de l'inscription de l'appareil. Cette structure est couramment détectée en tant que `domain\username` comme référencé par le serveur qui exécute Citrix Endpoint Management connecté à Active Directory via LDAP. L'onglet **Log** de l'outil de configuration du connecteur affiche les valeurs qui sont transmises via le connecteur. Les valeurs sont transmises si le connecteur doit déterminer la structure des valeurs ou si la structure diffère.
- **DeviceID (ActiveSyncID) :** également appelée ActiveSyncID de l'appareil connecté. Cette valeur est généralement présente sur la page de propriétés spécifiques de l'appareil dans la console Citrix Endpoint Management. Cette valeur peut également être vue depuis l'onglet **Log** de l'outil de configuration du connecteur pour Exchange ActiveSync.
- **DeviceType :** le connecteur pour Exchange ActiveSync peut déterminer si un appareil est un iPhone, un iPad ou tout autre type d'appareil et peut l'autoriser ou le bloquer en fonction de ces critères. Comme avec d'autres valeurs, l'outil de configuration du connecteur peut révéler tous les types d'appareils connectés en cours de traitement pour la connexion ActiveSync.
- **UserAgent :** contient des informations sur le client ActiveSync utilisé. Dans la plupart des cas, la valeur spécifiée correspond à une version spécifique d'un système d'exploitation et à la version de plate-forme de l'appareil mobile.

L'outil de configuration du connecteur pour Exchange ActiveSync en cours d'exécution sur le serveur gère toujours les règles statiques.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Dans l'utilitaire SMG Controller Configuration, cliquez sur l'onglet **Static Rules**, puis cliquez sur **Add**.
2. Dans la boîte de dialogue **Static Rule Properties**, spécifiez les valeurs que vous voulez utiliser en tant que critères. Par exemple, vous pouvez entrer un utilisateur pour autoriser l'accès en entrant le nom d'utilisateur (par exemple, AllowedUser), puis désactiver la case à cocher **Disabled**.
3. Cliquez sur **Enregistrer**.

   La règle statique est maintenant effective. Vous pouvez également utiliser des expressions régulières pour définir des valeurs, mais vous devez activer le mode de traitement de la règle dans le fichier config.xml.

Pour configurer les règles dynamiques Les stratégies et les propriétés d'appareils dans Citrix Endpoint Management définissent les règles dynamiques et peuvent déclencher un filtre de connecteur pour Exchange ActiveSync dynamique. Les déclencheurs sont basés sur la présence d'une violation de stratégie ou d'un paramètre de propriété. Les filtres de connecteur pour Exchange ActiveSync analysent un appareil à la recherche d'une violation de stratégie ou d'un paramètre de propriété donné. Si l'appareil est conforme aux critères, l'appareil est placé dans une liste d'appareils. Cette liste d'appareils n'est ni une liste d'autorisation ni une liste de blocage. Il s'agit d'une liste d'appareils qui satisfait au critère défini. Les options de configuration suivantes vous permettent de définir si vous souhaitez autoriser ou refuser les appareils dans la liste d'appareils en utilisant le connecteur pour Exchange ActiveSync.

> **Remarque :**
>
> Utilisez la console Citrix Endpoint Management pour configurer les règles dynamiques.

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Serveur**, cliquez sur **ActiveSync Gateway**. La page ActiveSync Gateway s'affiche.
3. Dans **Activer la ou les règles suivantes**, sélectionnez une ou plusieurs règles à activer.
4. Dans Android uniquement, dans **Envoyer les utilisateurs de domaine Android vers ActiveSync Gateway**, cliquez sur **Oui** pour vous assurer qu'Citrix Endpoint Management envoie les informations de l'appareil Android à Secure Mobile Gateway.

   Lorsque cette option est activée, Citrix Endpoint Management envoie les informations de l'appareil Android au connecteur si Citrix Endpoint Management ne dispose pas de l'identificateur ActiveSync de l'utilisateur de l'appareil.

Pour configurer des stratégies personnalisées en modifiant le fichier XML du connecteur pour Exchange ActiveSync Vous pouvez afficher les stratégies de base dans la configuration par défaut

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sur l'onglet **Policies** de l'outil de configuration du connecteur pour Exchange ActiveSync. Si vous souhaitez créer des stratégies personnalisées, vous pouvez modifier le fichier de configuration XML du connecteur NetScaler Gateway pour Exchange ActiveSync (config\config.xml).

1. Recherchez la section **PolicyList** dans le fichier, puis ajoutez un nouvel élément **Policy**.
2. Si un nouveau groupe est également requis, tel qu'un groupe statique ou un groupe pour prendre en charge un autre GCP, ajoutez le nouvel élément **Group** à la section **GroupList**.
3. Si vous le souhaitez, vous pouvez modifier l'ordre des groupes dans une stratégie existante en réorganisant les éléments **GroupRef**.

Configuration du fichier XML du connecteur pour Exchange ActiveSync Le connecteur pour Exchange ActiveSync utilise un fichier de configuration XML pour déterminer les actions du connecteur. Entre autres entrées, le fichier spécifie les fichiers du groupe et les actions associées que le filtre effectue lors de l'évaluation des requêtes HTTP. Par défaut, le fichier est appelé config.xml et est situé à l'emplacement suivant : ..\Program Files\Citrix\XenMobile NetScaler Connector\config.

Nœuds GroupRef

Les nœuds GroupRef définissent les noms des groupes logiques. Les valeurs par défaut sont AllowGroup et DenyGroup.

> **Remarque :**
>
> L'ordre des nœuds GroupRef tels qu'ils apparaissent dans le nœud GroupRefList est significatif.

La valeur de l'ID d'un nœud GroupRef identifie un conteneur logique ou une collection de membres qui sont utilisés pour la mise en correspondance des comptes d'utilisateurs ou d'appareils spécifiques. Les attributs d'action spécifient la façon dont le filtre traite un membre qui correspond à une règle dans la collection. Par exemple, un compte d'utilisateur ou un appareil qui correspond à une règle dans l'ensemble AllowGroup sera « pass. » « pass » signifie qu'il est autorisé à accéder à Exchange CAS. Un compte d'utilisateur ou un appareil qui correspond à une règle dans l'ensemble DenyGroup est « rejected. » « rejected » signifie qu'il n'est pas autorisé à accéder à Exchange CAS.

Lorsqu'un compte utilisateur/appareil particulier ou une combinaison des deux répond aux règles dans les deux groupes, une convention de priorité est utilisée pour diriger le résultat de la requête. La priorité est incorporée dans l'ordre des nœuds GroupRef dans le fichier config.xml de haut en bas. Les nœuds GroupRef sont classés par ordre de priorité. Les règles pour une condition donnée dans le groupe Allow seront toujours prioritaires sur les règles de la même condition du groupe Deny.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nœuds de groupe

Le fichier config.xml définit également les nœuds Groupe. Ces nœuds fournissent une liaison entre les conteneurs logiques AllowGroup et DenyGroup vers les fichiers XML externes. Les entrées stockées dans les fichiers externes forment la base des règles de filtre.

> **Remarque :**
>
> Dans cette version, seuls les fichiers XML externes sont pris en charge.

L'installation par défaut implémente deux fichiers XML de configuration : allow.xml et deny.xml.

Configuration de NetScaler Gateway Connector pour Exchange ActiveSync

Vous pouvez configurer NetScaler Gateway Connector pour Exchange ActiveSync pour bloquer ou autoriser les demandes ActiveSync de manière sélective en vous basant sur les propriétés suivantes : **Active Sync Service ID**, **Device type**, **User Agent** (système d'exploitation de l'appareil), **Authorized user** et **ActiveSync Command**.

La configuration par défaut prend en charge une combinaison de groupes statiques et dynamiques. Vous pouvez gérer les groupes statiques à l'aide de l'utilitaire de configuration SMG Controller. Les groupes statiques peuvent être composés de catégories d'appareils connues, telles que les appareils utilisant un agent utilisateur donné.

Une source externe appelée fournisseur de configuration de passerelle gère les groupes dynamiques. Le connecteur pour Exchange ActiveSync connecte les groupes régulièrement. Citrix Endpoint Management peut exporter des groupes d'appareils et d'utilisateurs autorisés et bloqués vers le connecteur pour Exchange ActiveSync.

Une source externe appelée fournisseur de configuration de passerelle gère les groupes dynamiques. Le connecteur pour Exchange ActiveSync collecte régulièrement les groupes dynamiques. Citrix Endpoint Management peut exporter des groupes d'appareils et d'utilisateurs autorisés et bloqués vers le connecteur.

Une stratégie est une liste ordonnée de groupes dans laquelle chaque groupe est associé à une action (autoriser ou bloquer) et une liste des membres du groupe. Une stratégie peut contenir n'importe quel nombre de groupes. L'ordre du groupe dans une stratégie est important car lorsqu'une correspondance est localisée, l'action du groupe est prise, et les autres groupes ne sont pas évalués.

Un membre définit une façon de faire correspondre les propriétés d'une demande. Il peut correspondre à une seule propriété, telle que l'ID d'appareil ou plusieurs propriétés, telles que le type d'appareil et l'agent utilisateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Choix d'un modèle de sécurité pour NetScaler Gateway Connector pour Exchange ActiveSync

L'établissement d'un modèle de sécurité est nécessaire au succès d'un déploiement d'appareils mobiles pour les organisations de toutes tailles. Il est courant d'utiliser un contrôle de réseau protégé ou en quarantaine pour autoriser l'accès à un utilisateur, un ordinateur ou un appareil par défaut. Cette pratique n'est pas toujours idéale. Chaque organisation qui gère la sécurité informatique peut avoir une approche légèrement différente ou adaptée à la sécurité pour les appareils mobiles.

La même logique s'applique à la sécurité des appareils mobiles. Un modèle permissif est un choix inadapté étant donné le grand nombre de types et d'appareils mobiles, d'appareils mobiles par utilisateur et de plates-formes de systèmes d'exploitation et d'applications disponibles. Dans la plupart des organisations, le modèle restrictif sera le choix le plus logique.

Les scénarios de configuration que Citrix autorise pour l'intégration du connecteur pour Exchange ActiveSync avec Citrix Endpoint Management sont les suivants :

Modèle permissif (Permit Mode)

Le modèle de sécurité permissif fonctionne sur le principe que l'accès est autorisé par défaut. Un blocage et une restriction seront appliqués uniquement via des règles et un filtrage. Le modèle de sécurité permissif est adapté aux organisations dans lesquelles la sécurité n'est pas une préoccupation principale pour les appareils mobiles. Le modèle applique uniquement des contrôles restrictifs pour refuser l'accès lorsque cela est approprié (lorsqu'une règle de stratégie a échoué).

Modèle restrictif (Block Mode)

Le modèle de sécurité restrictif est basé sur le principe que l'accès n'est pas autorisé par défaut. Tout le contenu transitant par le point de vérification est filtré et inspecté, et l'accès est refusé, sauf si les règles autorisant l'accès sont satisfaites. Le modèle de sécurité restrictif est adapté aux organisations qui possèdent des mesures de sécurité relativement strictes pour les appareils mobiles. Le mode accorde seulement l'accès (à des fins d'utilisation et aux fonctionnalités) aux services réseau lorsque toutes les règles autorisant l'accès sont observées.

Gestion de NetScaler Gateway Connector pour Exchange ActiveSync

Vous pouvez utiliser NetScaler Gateway Connector pour Exchange ActiveSync pour créer des règles de contrôle d'accès. Les règles autorisent ou bloquent l'accès aux demandes de connexion ActiveSync des appareils gérés. L'accès dépend de l'état de l'appareil, des listes d'autorisation ou de blocage et d'autres critères de conformité.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

À l'aide de l'outil de configuration du connecteur pour Exchange ActiveSync, vous pouvez créer des règles dynamiques et statiques qui appliquent des stratégies de messagerie d'entreprise. Ces règles et stratégies vous permettent de bloquer les utilisateurs qui enfreignent les normes de conformité. Vous pouvez également configurer le cryptage des pièces jointes aux e-mails, de sorte que toutes les pièces jointes qui sont transmises par le biais de Exchange Server vers les appareils gérés sont cryptées. Seuls les utilisateurs autorisés disposant d'appareils gérés peuvent afficher les pièces jointes cryptées.

Pour désinstaller XNC

1. Exécutez XncInstaller.exe avec un compte d'administrateur.
2. Suivez les instructions à l'écran pour procéder à la désinstallation.

Installation, mise à niveau ou désinstallation du connecteur pour Exchange ActiveSync

1. Exécutez XncInstaller.exe avec un compte administrateur pour installer le connecteur pour Exchange ActiveSync ou autoriser la mise à niveau ou la suppression d'un connecteur existant.
2. Suivez les instructions à l'écran pour procéder à l'installation, la mise à niveau ou la désinstallation.

Après avoir installé le connecteur pour Exchange ActiveSync, vous devez redémarrer manuellement le service de configuration et le service de notification d'Citrix Endpoint Management.

Installation de NetScaler Gateway Connector pour Exchange ActiveSync

Vous pouvez installer le connecteur pour Exchange ActiveSync sur son propre serveur ou sur le serveur sur lequel vous avez installé Citrix Endpoint Management.

Vous pouvez envisager d'installer le connecteur pour Exchange ActiveSync sur son propre serveur (distinct d'Citrix Endpoint Management) pour les raisons suivantes :

- Votre serveur Citrix Endpoint Management est hébergé à distance dans le cloud (emplacement physique)
- Vous ne souhaitez pas que le connecteur pour Exchange ActiveSync soit affecté par les redémarrages du serveur Citrix Endpoint Management (disponibilité)
- Vous souhaitez que les ressources système d'un serveur soient entièrement dédiées au connecteur pour Exchange ActiveSync (performances).

La charge d'UC que le connecteur pour Exchange ActiveSync place sur un serveur dépend du nombre d'appareils gérés. Une recommandation générale consiste à provisionner un noyau d'UC supplémentaire si le connecteur est déployé sur le même serveur qu'Citrix Endpoint Management. Pour un

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

grand nombre d'appareils (plus de 50 000), il se peut que vous deviez provisionner des noyaux supplémentaires si vous ne disposez pas d'un environnement en cluster. L'encombrement mémoire du connecteur n'est pas assez important pour justifier plus de mémoire.

Configuration système requise pour NetScaler Gateway Connector pour Exchange ActiveSync

NetScaler Gateway Connector pour Exchange ActiveSync communique avec NetScaler Gateway sur un pont SSL configuré sur le boîtier NetScaler Gateway. La passerelle permet au boîtier d'acheminer tout le trafic sécurisé directement vers Citrix Endpoint Management. Le connecteur pour Exchange ActiveSync requiert la configuration système minimale suivante :

Composant	Exigences
Ordinateur et processeur	733 MHz Pentium III 733 MHz ou processeur supérieur. 2.0 GHz Pentium III ou processeur supérieur (recommandé)
Citrix Gateway	Appliance Citrix Gateway avec version du logiciel 10
Memory	1 GB
Disque dur	Partition locale au format NTFS avec 150 Mo d'espace disque dur disponible
Système d'exploitation	Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2008 R2 Service Pack 1. Doit être un serveur en anglais. Le support pour Windows Server 2008 R2 Service Pack 1 prend fin le 14 janvier 2020 et le support pour Windows Server 2012 R2 prend fin le 10 octobre 2023.
Autres périphériques	Carte réseau compatible avec le système d'exploitation hôte pour les communications avec le réseau interne.
Microsoft .NET Framework	La version 8.5.1.11 requiert Microsoft .NET Framework 4.5.
Affichage	Moniteur VGA ou de plus haute résolution

L'ordinateur hôte pour le connecteur pour Exchange ActiveSync requiert l'espace disque disponible suivant :

- **Application :** 10 -15 Mo (100 Mo recommandés)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Logging.** 1 Go (20 Go recommandés)

Pour plus d'informations sur les plates-formes prises en charge pour le connecteur pour Exchange ActiveSync, consultez Systèmes d'exploitation d'appareils pris en charge.

Clients de messagerie d'appareil

Les clients de messagerie ne renvoient pas tous le même ID ActiveSync pour un appareil. Étant donné que le connecteur pour Exchange ActiveSync s'attend à un ID ActiveSync unique pour chaque appareil, seuls les clients de messagerie qui génèrent toujours le même ID ActiveSync unique pour chaque appareil sont pris en charge. Citrix a testé ces clients de messagerie et aucune erreur n'a été détectée :

- Client de messagerie natif Samsung
- Client de messagerie natif iOS

Déploiement de NetScaler Gateway Connector pour Exchange ActiveSync

NetScaler Gateway Connector pour Exchange ActiveSync vous permet d'utiliser NetScaler Gateway pour servir de proxy et équilibrer la charge des communications du serveur Citrix Endpoint Management avec les appareils gérés Citrix Endpoint Management. Le connecteur pour Exchange ActiveSync communique régulièrement avec Citrix Endpoint Management pour synchroniser les stratégies. Le connecteur pour Exchange ActiveSync et Citrix Endpoint Management peuvent être en cluster, ensemble ou indépendamment.

Composants du connecteur pour Exchange ActiveSync

- **Connecteur pour Exchange ActiveSync :** ce service offre une interface de service Web REST que NetScaler Gateway peut invoquer pour déterminer si une demande ActiveSync provenant d'un appareil est autorisée.
- **Service de configuration Citrix Endpoint Management :** ce service communique avec Citrix Endpoint Management pour synchroniser les modifications de stratégie d'Citrix Endpoint Management avec le connecteur pour Exchange ActiveSync.
- **Service de notification Citrix Endpoint Management :** ce service envoie des notifications d'accès non autorisé à Citrix Endpoint Management. De cette façon, Citrix Endpoint Management peut prendre les mesures appropriées, envoyer à l'utilisateur une notification expliquant pourquoi l'appareil a été bloqué par exemple.
- **Outil de configuration du connecteur pour Exchange ActiveSync :** cette application permet à l'administrateur de configurer et de surveiller le connecteur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration d'adresses d'écoute pour NetScaler Gateway Connector pour Exchange ActiveSync

Pour que NetScaler Gateway Connector pour Exchange ActiveSync reçoive des demandes de NetScaler Gateway pour autoriser le trafic ActiveSync, procédez comme suit. Indiquez le port sur lequel le connecteur pour Exchange ActiveSync écoute les appels de service Web NetScaler Gateway.

1. Dans le menu **Démarrer**, sélectionnez l'outil de configuration du connecteur pour Exchange ActiveSync.
2. Cliquez sur l'onglet **Web Service**, puis entrez les adresses d'écoute pour le service Web du connecteur. Vous pouvez sélectionner le protocole **HTTP** et/ou **HTTPS**. Si le connecteur pour Exchange ActiveSync est co-résident avec Citrix Endpoint Management (installé sur le même serveur), sélectionnez les valeurs de port qui ne sont pas en conflit avec Citrix Endpoint Management.
3. Une fois les valeurs configurées, cliquez sur **Save**, puis sur **Start Service** pour démarrer le service Web.

Configuration de stratégies de contrôle d'accès à l'appareil dans NetScaler Gateway Connector pour Exchange ActiveSync

Pour configurer la stratégie de contrôle d'accès que vous souhaitez appliquer à vos appareils gérés, effectuez les opérations suivantes :

1. Dans l'outil de configuration du connecteur pour Exchange ActiveSync, cliquez sur l'onglet **Path Filters**.
2. Sélectionnez la première ligne, **Microsoft-Server-ActiveSync is for ActiveSync**, puis cliquez sur **Edit**.
3. À partir de la liste **Policy**, sélectionnez la stratégie désirée. Pour une stratégie qui comprend des stratégies Citrix Endpoint Management, sélectionnez **Static + ZDM: Permit Mode ou Static + ZDM: Block Mode**. Ces stratégies combinent des règles locales (ou statiques) avec les règles d'Citrix Endpoint Management. Permit Mode signifie que tous les appareils non identifiés de manière explicite par les règles sont autorisés à accéder à ActiveSync. Block Mode signifie que de tels appareils sont bloqués.
4. Après avoir défini les stratégies, cliquez sur **Save**.

Pour configurer la communication avec Citrix Endpoint Management

Spécifiez le nom et les propriétés du serveur Citrix Endpoint Management que vous souhaitez utiliser avec NetScaler Gateway Connector pour Exchange ActiveSync et NetScaler Gateway.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Remarque :**
>
> Cette tâche suppose qu'Citrix Endpoint Management soit déjà installé ou configuré. L'outil de configuration Exchange ActiveSync utilise le terme Config Provider pour Citrix Endpoint Management.

1. Dans l'outil de configuration du connecteur pour Exchange ActiveSync, cliquez sur l'onglet **Config Providers**, puis cliquez sur **Add**.
2. Entrez le nom et l'URL du serveur Citrix Endpoint Management que vous utilisez pour ce déploiement. Si vous disposez de plusieurs serveurs Citrix Endpoint Management déployés dans un déploiement multi-locataire, ce nom doit être unique pour chaque instance de serveur.
3. Dans **Url**, entrez l'adresse Web du service Citrix Endpoint Management GCP (GlobalConfig Provider), généralement au format `https://<FQDN>/<instanceName>/services/<MagConfigService>`. Le nom *MagConfigService* est sensible à la casse.
4. Dans **Password**, saisissez le mot de passe utilisé pour l'autorisation HTTP de base avec le serveur Web Citrix Endpoint Management.
5. Dans **Managing Host**, entrez le nom du serveur sur lequel vous avez installé le connecteur pour Exchange ActiveSync.
6. Dans **Intervalle de ligne de base**, spécifiez une période de temps après laquelle un nouveau ruleset dynamique actualisé est extrait depuis Citrix Endpoint Management.
7. Dans **Request Timeout**, spécifiez l'intervalle d'expiration du délai de demande du serveur.
8. Dans **Config Provider**, sélectionnez si l'instance de serveur du fournisseur de configuration fournit la configuration de la stratégie.
9. Dans **Events Enabled**, activez cette option si vous souhaitez que Secure Mobile Gateway informe Citrix Endpoint Management lorsqu'un appareil est bloqué. Cette option est requise si vous utilisez les règles Secure Mobile Gateway dans l'une des actions automatisées d'Citrix Endpoint Management.
10. Une fois que le serveur est configuré, cliquez sur **Test Connectivity** pour tester la connexion à Citrix Endpoint Management.
11. Lorsque la connexion est établie, cliquez sur **Save**.

Déploiement de NetScaler Gateway Connector pour Exchange ActiveSync pour la redondance et la capacité à monter en charge

Pour étendre votre déploiement de NetScaler Gateway Connector pour Exchange ActiveSync et Citrix Endpoint Management, vous pouvez installer des instances du connecteur sur plusieurs serveurs Windows. Toutes les instances de connecteur pointent vers la même instance Citrix Endpoint Management. Vous pouvez ensuite utiliser NetScaler Gateway pour équilibrer la charge des serveurs.

Il existe deux modes de configuration du connecteur pour Exchange ActiveSync :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- En mode non partagé, chaque instance du connecteur pour Exchange ActiveSync communique avec un serveur Citrix Endpoint Management et conserve sa propre copie privée de la stratégie résultante. Par exemple, pour un cluster de serveurs Citrix Endpoint Management, vous pouvez exécuter une instance de connecteur sur chaque serveur Citrix Endpoint Management. Le connecteur obtient ensuite des stratégies à partir de l'instance locale Citrix Endpoint Management.
- En mode partagé, un connecteur pour le nœud Exchange ActiveSync est désigné comme le nœud principal. Le connecteur communique avec Citrix Endpoint Management. La configuration résultante est partagée entre les autres nœuds soit par un partage réseau Windows soit par une réplication Windows (ou tierce).

La totalité de la configuration du connecteur pour Exchange ActiveSync se trouve dans un dossier unique (composé de plusieurs fichiers XML). Le processus du connecteur détecte les modifications apportées à tout fichier dans ce dossier et recharge automatiquement la configuration. Il n'y a pas de basculement du nœud principal en mode partagé. Toutefois, le système peut tolérer le fait que le serveur principal soit arrêté pendant quelques minutes (par exemple, pour redémarrer). La dernière configuration correcte connue est mise en cache dans le processus du connecteur.

Concepts avancés

March 1, 2024

Les articles Concepts avancés de Citrix Endpoint Management offrent une analyse approfondie des informations produit sur Citrix Endpoint Management. L'objectif est de réduire les temps de déploiement via des techniques proposées par des experts. Ces articles citent les experts techniques qui ont rédigé le contenu.

Pour obtenir des points de décision et des conseils, accéder aux questions fréquemment posées et à des cas d'utilisation relatifs à votre environnement Citrix Endpoint Management, consultez Déploiement de Citrix Endpoint Management dans cette section.

Vous trouverez les forums de support de la communauté Citrix Endpoint Management dans Citrix Discussions.

Déploiement de Citrix Endpoint Management

March 1, 2024

Il existe un grand nombre d'éléments à prendre en compte lorsque vous planifiez un déploiement Citrix Endpoint Management. Quels appareils choisir ? Comment les gérer ? Comment s'assurer que

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

votre réseau est sécurisé tout en proposant une expérience utilisateur satisfaisante ? Quel matériel mettre en place et comment dépanner ? Les articles de cette section visent à aider à répondre à ces questions. Vous y trouverez des cas d'utilisation et des recommandations sur des sujets qui couvrent vos problèmes de déploiement.

Gardez à l'esprit qu'une directive ou une recommandation peut ne pas s'appliquer à tous les environnements ou cas d'utilisation. Assurez-vous de configurer un environnement de test avant de lancer un déploiement Citrix Endpoint Management.

Les articles de cette section couvrent les domaines suivants :

- **Évaluation :** cas d'utilisation courants et questions à prendre en compte lors de la planification de votre déploiement.
- **Conception et configuration :** recommandations pour la conception et la configuration de votre environnement.
- **Fonctionnement et surveillance :** assurer le bon fonctionnement de votre environnement d'exécution.

Évaluation

Comme pour tout déploiement, l'évaluation de vos besoins doit être votre première priorité. Pourquoi avez-vous besoin de Citrix Endpoint Management ? Est-il nécessaire de gérer tous les appareils de votre environnement ou seulement les applications, ou les deux ? Quel niveau de sécurité est nécessaire pour votre environnement Citrix Endpoint Management ? Examinons les cas d'utilisation courants et les questions à prendre en compte lors de la planification de votre déploiement.

- Modes de gestion
- Configuration requise par l'appareil
- Sécurité et expérience utilisateur
- Applications
- Communautés d'utilisateurs
- Stratégie de messagerie
- Intégration de Citrix Endpoint Management

Conception et configuration

Une fois que vous avez terminé d'évaluer vos besoins de déploiement, vous pouvez décider comment concevoir et configurer votre environnement. Éléments à planifier :

- Choisir le matériel pour votre serveur
- Configuration de stratégies pour les applications et les appareils

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Inscription des utilisateurs

Cette section contient des cas d'utilisation et des recommandations pour chacun de ces scénarios et bien plus encore.

- Intégration avec NetScaler Gateway et Citrix ADC
- Considérations SSO et proxy pour les applications MDX
- Authentification
- Propriétés du serveur
- Stratégies d'appareil et d'application
- Options d'inscription des utilisateurs

Fonctionnement et surveillance

Une fois que votre environnement Citrix Endpoint Management est opérationnel, vous devez le surveiller pour garantir son bon fonctionnement. La section Surveillance explique où vous pouvez trouver les différents journaux et messages générés par Citrix Endpoint Management et ses composants, ainsi que la manière de lire ces journaux. Cette section comprend également différentes procédures de dépannage communes que vous pouvez suivre pour réduire le temps de réponse du service client.

- Provisioning et deprovisioning d'applications
- Opérations basées sur le tableau de bord
- Contrôle d'accès basé sur les rôles et support Citrix Endpoint Management
- Surveillance et assistance
- Processus de support Citrix

Modes de gestion

March 1, 2024

Le mode de gestion est un terme qui inclut la gestion des appareils mobiles (MDM) et la gestion des applications mobiles (MAM). Vous pouvez configurer les éléments suivants :

- Profils d'inscription pour inscrire des appareils Android et iOS dans MDM, MAM ou les deux (MDM+MAM). Si vous choisissez MDM+MAM, vous pouvez donner aux utilisateurs la possibilité de se désinscrire de MDM.
- Profils d'inscription pour inscrire des appareils Windows 10 et Windows 11 dans MDM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Vous spécifiez les options d'inscription dans les profils d'inscription que vous associez aux groupes de mise à disposition. Pour de plus amples informations sur les options d'inscription, consultez la section Profils d'inscription. Les sections suivantes portent sur les considérations relatives à la gestion des appareils et des applications.

Gestion des appareils mobiles (MDM)

Grâce au mode MDM, vous pouvez configurer, sécuriser et prendre en charge les appareils mobiles. MDM vous permet de protéger les appareils et les données sur les appareils au niveau du système. Vous pouvez configurer des stratégies, des actions et des fonctions de sécurité. Par exemple, vous pouvez effacer un appareil de manière sélective si l'appareil est perdu, volé ou non conforme.

Même si vous ne choisissez pas de gérer des applications sur des appareils, vous pouvez fournir des applications mobiles, telles que des applications publiques et des applications d'entreprise.

Voici les cas d'utilisation courants pour le mode MDM :

- MDM est pris en compte pour les appareils appartenant à l'entreprise dans lesquels des stratégies ou certaines restrictions de gestion au niveau de l'appareil sont requises. Ces restrictions incluent l'effacement complet, l'effacement sélectif ou la géolocalisation.
- Lorsque les clients ont besoin de la gestion d'un appareil, mais n'ont pas besoin de stratégies MDX.
- Lorsque les utilisateurs nécessitent uniquement l'envoi d'e-mails à leurs clients de messagerie natifs sur leurs appareils, et Exchange ActiveSync ou le serveur d'accès au client est déjà accessible de l'extérieur. Dans ce cas, vous pouvez utiliser MDM pour configurer la distribution des e-mails.
- Lorsque vous déployez des applications d'entreprise natives (non-MDX), des applications de magasin d'applications publiques ou des applications MDX fournies par des magasins publics. Considérez qu'une solution MDM seule peut ne pas empêcher la fuite de données d'informations confidentielles entre les applications sur l'appareil. Des fuites de données peuvent se produire lors des opérations Copier et coller ou Enregistrer sous dans les applications Office 365.

Gestion d'applications mobiles (MAM)

Le mode MAM protège les données d'application et vous permet de contrôler le partage de données d'application. MAM facilite également la gestion des données et des ressources de l'entreprise, indépendamment des données personnelles. Lorsque Citrix Endpoint Management est configuré avec MAM, vous pouvez utiliser des applications mobiles compatibles MDX pour fournir la conteneurisation et le contrôle par application.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

En utilisant les stratégies MDX, Citrix Endpoint Management offre un contrôle au niveau de l'application sur l'accès au réseau (tel que le micro VPN), l'interaction entre l'application et l'appareil, et l'accès aux applications.

Le mode MAM est souvent adapté à l'environnement BYOD (Bring Your Own Device, Apportez votre propre appareil) car, bien que l'appareil ne soit pas géré, les données de l'entreprise restent protégées. MDX dispose de nombreuses stratégies MAM exclusif qui ne nécessitent pas de contrôle MDM.

MAM prend également en charge les applications de productivité mobiles Citrix. Cette prise en charge comprend :

- Distribution sécurisée des e-mails à Citrix Secure Mail
- Partage de données entre les applications de productivité mobiles Citrix sécurisées
- Stockage sécurisé des données dans Citrix Files.

Pour plus de détails, consultez la section Applications de productivité mobiles.

Le mode MAM convient souvent aux scénarios suivants :

- Vous mettez à disposition des applications mobiles, telles que les applications MDX, gérées au niveau de l'application.
- Vous n'êtes pas obligé de gérer les appareils au niveau du système.

MDM+MAM

Citrix Endpoint Management vous permet de spécifier si les utilisateurs peuvent refuser la gestion des appareils. Cette flexibilité est utile pour les environnements qui incluent une combinaison de cas d'utilisation. Ces environnements peuvent nécessiter la gestion d'un appareil via des stratégies MDM pour accéder à vos ressources MAM.

Le mode MDM + MAM convient aux scénarios suivants :

- Vous disposez d'un cas d'utilisation unique dans lequel le mode MDM et le mode MAM sont requis. MDM est requis pour accéder à vos ressources MAM.
- Certains cas d'utilisation nécessitent MDM alors que dans d'autres cas MDM n'est pas requis.
- Certains cas d'utilisation nécessitent MAM alors que dans d'autres cas MAM n'est pas requis.

Gestion des appareils et inscription MDM

Un environnement Citrix Endpoint Management Enterprise peut inclure une combinaison de cas d'utilisation, dont certains nécessitent une gestion des appareils via des stratégies MDM pour autoriser l'accès aux ressources MAM.

Avant de déployer des applications de productivité mobiles Citrix pour les utilisateurs, évaluez entièrement vos cas d'utilisation et décidez si vous avez besoin d'une inscription MDM. Si vous décidez

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ultérieurement de modifier la configuration requise pour l'inscription MDM, les utilisateurs devront peut-être réinscrire leurs appareils. Pour plus d'informations, voir Profils d'inscription.

Pour plus d'informations sur l'inscription et NetScaler Gateway, voir Intégration avec NetScaler Gateway et Citrix ADC.

Voici un résumé des avantages et des inconvénients (ainsi que des options d'atténuation) de la demande d'inscription MDM.

Lorsque l'inscription MDM est facultative

Avantages

- Les utilisateurs peuvent accéder aux ressources MAM sans placer leurs appareils sous la gestion MDM. Cette option peut augmenter l'adoption par les utilisateurs.
- Il est possible de sécuriser l'accès aux ressources MAM pour protéger les données de l'entreprise.
- Les stratégies MDX telles que **Code secret d'application** permettent de contrôler l'accès à l'application pour chaque application MDX.
- La configuration de NetScaler Gateway, de Citrix Endpoint Management et des délais d'attente par application, associée au code PIN Citrix, offre une couche de protection supplémentaire.
- Bien que les actions MDM ne s'appliquent pas à l'appareil, certaines stratégies MDX peuvent être utilisées pour refuser l'accès MAM. Le refus est basé sur les paramètres système, tels que les appareils jailbreakés ou rootés.
- Les utilisateurs peuvent choisir d'inscrire leur appareil avec MDM lors de la première utilisation.

Inconvénients

- Les ressources MAM sont disponibles pour les appareils non inscrits dans MDM.
- Les stratégies et les actions MDM sont disponibles uniquement pour les appareils inscrits dans MDM.

Options d'atténuation

- Demandez aux utilisateurs d'accepter les conditions générales d'une entreprise qui les tient responsables en cas de non-conformité. Demandez aux administrateurs de surveiller les appareils non gérés.
- Gérez l'accès et la sécurité des applications en utilisant des minuteurs d'application. Les valeurs de délai d'attente réduites augmentent la sécurité, mais peuvent affecter l'expérience de l'utilisateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Lorsque l'inscription MDM est requise

Avantages

- Il est possible de restreindre l'accès aux ressources MAM uniquement aux appareils gérés par MDM.
- Les stratégies et les actions MDM peuvent s'appliquer à tous les appareils de l'environnement, selon vos besoins.
- Les utilisateurs ne peuvent pas désactiver l'inscription de leur appareil.

Inconvénients

- Tous les utilisateurs doivent s'inscrire avec MDM.
- Cette option peut diminuer l'adoption par les utilisateurs qui s'opposent à la gestion d'entreprise de leurs appareils personnels.

Options d'atténuation

- Informez les utilisateurs de ce que Citrix Endpoint Management gère réellement sur leurs appareils et des informations auxquelles les administrateurs peuvent accéder.

Configuration requise par l'appareil

November 29, 2023

Un point important à prendre en compte pour tout déploiement est l'ensemble d'appareils que vous souhaitez déployer. Sur les plateformes iOS, Android et Windows, les options sont nombreuses. Pour de plus amples informations sur les appareils pris en charge dans Citrix Endpoint Management, consultez la section Plates-formes prises en charge.

Dans un environnement BYOD (Amenez votre propre appareil), un mélange de plates-formes prises en charge est possible. Toutefois, tenez compte des limitations décrites dans l'article Plates-formes prises en charge lorsque vous informez les utilisateurs des appareils qu'ils peuvent inscrire. Même si vous n'autorisez qu'un ou deux appareils dans votre environnement, Citrix Endpoint Management fonctionne légèrement différemment sur les appareils iOS, Android et Windows. Différentes fonctionnalités sont disponibles sur chaque plate-forme.

En outre, toutes les conceptions d'applications ne ciblent pas les facteurs de forme des tablettes et des téléphones. Avant de procéder à des modifications générales, testez les applications pour vous assurer qu'elles correspondent à l'écran de l'appareil que vous souhaitez déployer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Vous pouvez également prendre en compte les facteurs d'inscription. Apple et Google proposent des programmes d'inscription d'entreprise. Grâce au programme Apple Deployment (DEP) et à Google Android Entreprise, vous pouvez acheter des appareils préconfigurés et prêts à être utilisés par les employés.

Pour plus d'informations sur l'inscription, consultez la section Options d'inscription des utilisateurs.

Sécurité et expérience utilisateur

March 1, 2024

La sécurité est importante pour toute organisation, mais vous devez trouver un équilibre entre la sécurité et l'expérience utilisateur. Par exemple, vous pouvez avoir un environnement hautement sécurisé qui est difficile à utiliser pour les utilisateurs. Ou votre environnement peut être si convivial que le contrôle d'accès n'est pas aussi strict. Les autres sections de ce manuel virtuel couvrent en détail les fonctionnalités de sécurité. Le but de cet article est de donner un aperçu général des problèmes de sécurité courants et des options de sécurité disponibles dans Citrix Endpoint Management.

Voici quelques considérations clés à garder à l'esprit pour chaque cas d'utilisation :

- Voulez-vous sécuriser certaines applications, l'appareil entier ou tout ?
- Comment voulez-vous que vos utilisateurs authentifient leur identité ? Souhaitez-vous utiliser LDAP, l'authentification basée sur les certificats ou une combinaison des deux ?
- Combien de temps souhaitez-vous que la session d'un utilisateur dure avant qu'elle expire ? Gardez à l'esprit qu'il existe différentes valeurs de délai d'expiration pour les services d'arrière-plan, Citrix ADC et pour accéder aux applications en mode hors connexion.
- Souhaitez-vous que les utilisateurs configurent un code d'accès au niveau de l'appareil et un code d'accès au niveau de l'application ? Combien de tentatives de connexion souhaitez-vous autoriser ? Gardez à l'esprit les exigences d'authentification supplémentaires par application qui peuvent être implémentées avec MAM et la façon dont les utilisateurs peuvent les percevoir.
- Quelles autres restrictions voulez-vous appliquer aux utilisateurs ? Souhaitez-vous donner aux utilisateurs l'accès à des services cloud tels que Siri ? Que peuvent-ils faire avec chaque application que vous mettez à leur disposition et que ne peuvent-ils pas faire ? Souhaitez-vous déployer des stratégies de réseau (Wi-Fi) d'entreprise pour empêcher l'utilisation de forfaits de données cellulaires dans les bureaux ?

Application ou appareil

Une des premières décisions à prendre est de déterminer si vous souhaitez sécuriser :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Certaines applications uniquement (gestion d'applications mobiles ou MAM)
- L'ensemble de l'appareil (gestion d'appareils mobiles ou MDM).
- MDM+MAM

Le plus souvent, si vous n'avez pas besoin d'un contrôle au niveau de l'appareil, vous n'avez besoin que de gérer les applications mobiles, en particulier si votre organisation prend en charge Bring Your Own Device (BYOD).

Les utilisateurs équipés d'appareils qui ne sont pas gérés peuvent installer des applications via le magasin d'applications. À la place des contrôles au niveau de l'appareil, comme l'effacement partiel ou complet, vous contrôlez l'accès aux applications via des stratégies d'application. Selon les valeurs que vous avez définies, les stratégies requièrent que l'appareil vérifie régulièrement Citrix Endpoint Management pour confirmer que les applications sont toujours autorisées à s'exécuter.

MDM vous permet de sécuriser l'ensemble d'un appareil, y compris la possibilité de faire l'inventaire de tous les logiciels d'un appareil. MDM vous permet d'empêcher l'inscription si l'appareil est jailbreaké, rooté ou si un logiciel non sécurisé est installé. Toutefois, les utilisateurs se méfient d'un tel niveau de contrôle sur leurs appareils personnels et cela peut réduire les taux d'inscription.

Authentification

C'est au niveau de l'authentification qu'une grande partie de l'expérience de l'utilisateur a lieu. Si votre organisation exécute déjà Active Directory, l'utilisation d'Active Directory est le moyen le plus simple d'autoriser vos utilisateurs à accéder au système.

Les délais d'expiration représentent aussi une partie importante de l'expérience de l'utilisateur avec l'authentification. Un environnement de haute sécurité peut exiger que les utilisateurs ouvrent une session chaque fois qu'ils accèdent au système. Cette option peut ne pas être idéale pour toutes les organisations ou tous les cas d'utilisation.

Entropie utilisateur

Pour plus de sécurité, vous pouvez activer une fonctionnalité appelée *entropie utilisateur*. Citrix Secure Hub et d'autres applications partagent souvent des données communes telles que les mots de passe, les codes confidentiels et les certificats pour garantir le bon fonctionnement de tous les éléments. Ces informations sont stockées dans un coffre générique dans Citrix Secure Hub. Si vous activez l'entropie utilisateur via l'option **Crypter les secrets** (Encrypt Secrets), Citrix Endpoint Management crée un nouveau coffre appelé UserEntropy. Citrix Endpoint Management déplace les informations du coffre-fort générique vers ce nouveau coffre-fort. Pour que Citrix Secure Hub ou une autre application accède aux données, les utilisateurs doivent entrer un mot de passe ou un code PIN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

L'activation de l'entropie utilisateur ajoute une couche d'authentification supplémentaire à plusieurs emplacements. Par conséquent, chaque fois qu'une application nécessite l'accès aux données partagées dans le coffre-fort UserEntropy (y compris les mots de passe, les codes confidentiels et les certificats), les utilisateurs doivent s'authentifier.

Pour en savoir plus sur l'entropie utilisateur, consultez la section À propos de MDX Toolkit. Pour activer l'entropie utilisateur, vous pouvez trouver les paramètres associés dans les propriétés du client.

Stratégies

Les stratégies MDX et MDM offrent une grande flexibilité aux organisations, mais elles peuvent également restreindre les utilisateurs. Ces restrictions peuvent être utiles dans certaines situations, mais les stratégies peuvent également rendre un système inutilisable. Par exemple, vous pouvez souhaiter bloquer l'accès à des applications cloud telles que Siri ou iCloud qui sont susceptibles d'envoyer des données sensibles à l'extérieur. Vous pouvez configurer une stratégie pour bloquer l'accès à ces services, mais gardez à l'esprit qu'une telle stratégie peut avoir des conséquences imprévues. Par exemple, le microphone du clavier iOS repose sur l'accès au cloud.

Applications

La gestion de la mobilité d'entreprise (EMM) inclut la gestion d'appareils mobiles (MDM) et gestion d'applications mobiles (MAM). Alors que MDM permet aux entreprises de sécuriser et de contrôler les appareils mobiles, MAM facilite la livraison et la gestion des applications. Avec l'adoption croissante de la stratégie BYOD (Apportez votre propre appareil), vous pouvez généralement implémenter une solution MAM, telle que Citrix Endpoint Management, pour les opérations suivantes :

- mise à disposition des applications
- attribution de licences logicielles
- configuration
- gestion du cycle de vie des applications

Avec Citrix Endpoint Management, vous pouvez aller plus loin dans la sécurisation des applications en configurant des stratégies MAM et des paramètres VPN spécifiques pour éviter les fuites de données et autres menaces de sécurité. Citrix Endpoint Management offre aux entreprises la flexibilité nécessaire pour inclure à la fois les fonctionnalités MDM et MAM dans le même environnement.

En plus de la possibilité de mettre à disposition des applications sur des appareils mobiles, Citrix Endpoint Management propose la conteneurisation d'applications via la technologie MDX. MDX sécurise les applications grâce à un cryptage distinct du cryptage au niveau de l'appareil fourni par les plates-formes. Vous pouvez effacer ou verrouiller des applications. Les applications sont soumises à des

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

contrôles granulaires basés sur des stratégies. Les éditeurs de logiciels indépendants peuvent appliquer ces contrôles à l'aide du SDK Mobile Apps.

Dans un environnement d'entreprise, les utilisateurs utilisent diverses applications mobiles pour les aider dans leur travail. Les applications peuvent inclure des applications du magasin d'applications public, des applications développées en interne ou des applications natives. Citrix Endpoint Management classe ces applications comme suit :

Applications publiques : ces applications peuvent être gratuites ou payantes et sont disponibles dans un magasin d'applications public, tel que l'Apple App Store ou Google Play. Les fournisseurs externes à l'organisation mettent souvent à disposition leurs applications dans des magasins d'applications publics. Cette option permet aux clients de télécharger les applications directement depuis Internet. Vous pouvez utiliser de nombreuses applications publiques dans votre organisation en fonction des besoins des utilisateurs. Des exemples de telles applications incluent les applications GoToMeeting, Salesforce et EpicCare.

Citrix ne prend pas en charge le téléchargement des fichiers binaires des applications directement à partir des magasins d'applications publics ou l'encapsulation avec MDX Toolkit pour la distribution d'entreprise. Pour activer MDX pour des applications tierces, contactez le fournisseur de votre application pour obtenir les fichiers binaires de l'application. Vous pouvez encapsuler les fichiers binaires à l'aide du MDX Toolkit ou intégrer le SDK MAM aux fichiers binaires.

Applications internes : de nombreuses organisations ont des développeurs internes qui créent des applications fournissant des fonctionnalités spécifiques et étant développées et distribuées indépendamment au sein de l'organisation. Dans certains cas, certaines organisations peuvent également avoir des applications fournies par des éditeurs de logiciels indépendants. Vous pouvez déployer ces applications en tant qu'applications natives ou vous pouvez les conteneuriser en utilisant une solution MAM, telle que Citrix Endpoint Management. Par exemple, une organisation de soins de santé peut créer une application interne qui permet aux médecins de consulter les informations sur les patients à partir d'appareils mobiles. Une organisation peut alors activer le SDK MAM pour l'application ou l'encapsuler par MDM pour sécuriser les informations du patient et activer l'accès VPN au serveur de base de données du patient principal.

Applications Web et Saas : ces applications comprennent les applications accessibles à partir d'un réseau interne (applications web) ou sur un réseau public (SaaS). Citrix Endpoint Management vous permet également de créer des applications Web et SaaS personnalisées à l'aide d'une liste de connecteurs d'applications. Ces connecteurs d'application peuvent faciliter l'authentification unique (SSO) aux applications Web existantes. Pour de plus amples informations, consultez la section Types de connecteur d'application. Par exemple, vous pouvez utiliser Google Apps SAML pour l'authentification unique basée sur le langage SAML (Security Assertion Markup Language) de Google Apps.

Applications de productivité mobiles Citrix : il s'agit d'applications développées par Citrix et incluses avec la licence Citrix Endpoint Management. Pour plus de détails, consultez la section À propos des applications de productivité mobiles. Citrix propose également d'autres applications prêtes

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

à l'emploi. Les éditeurs de logiciels indépendants développent des applications prêtes à l'emploi à l'aide du SDK Mobile Apps.

Applications HDX : il s'agit d'applications hébergées par Windows que vous publiez avec StoreFront. Si vous disposez d'un environnement Citrix Virtual Apps and Desktops, vous pouvez intégrer les applications à Citrix Endpoint Management pour mettre les applications à la disposition des utilisateurs inscrits.

Selon le type d'applications mobiles que vous prévoyez de déployer et de gérer avec Citrix Endpoint Management, la configuration et l'architecture sous-jacentes diffèrent. Supposons que plusieurs groupes d'utilisateurs ayant un niveau d'autorisation différent utilisent une même application, vous pouvez créer des groupes de mise à disposition distincts pour déployer deux versions de la même application. Vous devez vous assurer que l'appartenance au groupe d'utilisateurs est mutuellement exclusive pour éviter les incohérences de stratégie sur les appareils des utilisateurs.

Vous pouvez également gérer les licences d'applications iOS à l'aide de l'achat en volume d'Apple. Cette option nécessite que vous vous inscriviez au programme d'achats en volume Apple. Vous devez également utiliser la console Citrix Endpoint Management pour configurer les paramètres d'achats en volume. Cette configuration vous permet de distribuer les applications avec les licences d'achat en volume. Avec une telle variété de cas d'utilisation, il est important d'évaluer et de planifier votre stratégie MAM avant la mise en œuvre de l'environnement Citrix Endpoint Management. Vous pouvez commencer à planifier votre stratégie MAM en définissant les éléments suivants :

Types d'applications : répertorie les différents types d'applications que vous envisagez d'utiliser. Ensuite, catégorisez les applications, telles que les applications publiques, natives, de productivité mobiles Citrix, Web, internes et ISV. En outre, catégorisez les applications selon différentes plates-formes d'appareils, telles que iOS et Android. Cette catégorisation permet d'aligner les paramètres Citrix Endpoint Management requis pour chaque type d'application. Par exemple, certaines applications peuvent ne pas être qualifiées pour l'encapsulation. Ou, quelques applications peuvent nécessiter l'utilisation du SDK Applications mobiles pour activer des API spéciales pour l'interaction avec d'autres applications.

Exigences en matière de réseau : configurez les applications avec des paramètres appropriés pour répondre aux exigences d'accès réseau spécifiques. Par exemple, certaines applications peuvent nécessiter l'accès à votre réseau interne via un VPN. Certaines applications peuvent nécessiter un accès Internet pour acheminer l'accès via la DMZ. Afin de permettre à ces applications de se connecter au réseau requis, vous devez configurer divers paramètres en conséquence. Définissez les exigences réseau par application pour vous aider à finaliser vos décisions architecturales. Ce travail rationalise le processus global de mise en œuvre.

Exigences en matière de sécurité : définissez les exigences de sécurité qui s'appliquent à des applications individuelles ou à toutes les applications. Certains paramètres, tels que les stratégies MDX, s'appliquent à des applications individuelles Les paramètres de session et d'authentification s'appliquent à toutes les applications Certaines applications peuvent avoir des exigences spécifiques en

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

matière de cryptage, de conteneurisation, d'encapsulation, d'authentification, de géofencing, de code d'accès ou de partage de données. Définissez ces exigences à l'avance afin de simplifier votre déploiement.

Exigences en matière de déploiement : vous pouvez utiliser un déploiement basé sur des stratégies pour autoriser le téléchargement des applications publiées uniquement par des utilisateurs compatibles. Par exemple, vous pouvez souhaiter que certaines applications requièrent que :

- le cryptage de l'appareil basé sur la plate-forme soit activé
- l'appareil soit géré
- l'appareil réponde à une version minimale du système d'exploitation
- certaines applications soient disponibles uniquement pour les utilisateurs d'entreprise

Définissez ces exigences à l'avance afin de pouvoir configurer les stratégies ou les actions de déploiement appropriées.

Exigences en matière de licence : enregistrez les exigences en matière de licence liées à l'application. Ces notes vous aideront à gérer efficacement l'utilisation des licences et à décider si vous devez configurer des fonctionnalités spécifiques dans Citrix Endpoint Management pour faciliter l'attribution de licences. Par exemple, si vous déployez une application iOS gratuite ou payante, Apple applique les exigences de licence sur l'application en demandant aux utilisateurs de se connecter à leur compte Apple Store. Vous pouvez vous inscrire à l'achat en volume d'Apple pour distribuer et gérer ces applications via Citrix Endpoint Management. L'achat en volume permet aux utilisateurs de télécharger les applications sans se connecter à leur compte Apple Store. En outre, des outils tels que Samsung Knox présentent des exigences de licence spéciales qui doivent être satisfaites avant le déploiement de ces fonctionnalités.

Exigences en matière de liste d'autorisation/liste de blocage : vous souhaitez probablement empêcher les utilisateurs d'installer ou d'utiliser certaines applications. Créez une liste d'autorisation d'applications qui définit la machine utilisateur comme étant hors conformité. Ensuite, configurez des stratégies pour qu'elles se déclenchent lorsqu'un appareil devient non conforme. D'un autre côté, une application peut être acceptable pour une utilisation, mais peut tomber sous la liste de blocage pour une raison quelconque. Dans ce cas, vous pouvez ajouter l'application à une liste d'autorisation et indiquer que l'utilisation de l'application est acceptable mais n'est pas requise. De plus, gardez à l'esprit que les applications préinstallées sur les nouveaux appareils peuvent inclure certaines applications couramment utilisées qui ne font pas partie du système d'exploitation. Ces applications peuvent entrer en conflit avec votre stratégie de liste de blocage.

Cas d'utilisation des applications

Une organisation de soins de santé prévoit de déployer Citrix Endpoint Management en tant que solution MAM pour leurs applications mobiles. Les applications mobiles sont mises à disposition des

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

utilisateurs professionnels et BYOD. Le département informatique décide de mettre à disposition et de gérer les applications suivantes :

- **Applications de productivité mobiles :** applications iOS et Android fournies par Citrix.
- **Citrix Files :** application permettant d'accéder aux données partagées et de partager, synchroniser et éditer des fichiers.

Magasin d'applications public

- **Citrix Secure Hub :** client utilisé par tous les appareils mobiles pour communiquer avec Citrix Endpoint Management. Le département informatique envoie les paramètres de sécurité, les configurations et les applications mobiles vers les appareils mobiles via le client Citrix Secure Hub. Les appareils Android et iOS s'inscrivent dans Citrix Endpoint Management via Citrix Secure Hub.
- **Application Citrix Workspace :** application mobile qui permet aux utilisateurs d'ouvrir des applications d'appareils mobiles hébergées par Citrix Virtual Apps.
- **GoToMeeting :** un client de réunion, de partage de bureau et de visioconférence en ligne qui permet aux utilisateurs de se rencontrer en temps réel avec d'autres utilisateurs, clients ou collègues via Internet.
- **SalesForce1 :** Salesforce1 permet aux utilisateurs d'accéder à Salesforce à partir d'appareils mobiles et rassemble toutes les applications Chatter, CRM et applications personnalisées, ainsi que les processus d'entreprise, pour une expérience unifiée pour tout utilisateur Salesforce.
- **RSA SecurID :** jeton logiciel pour l'authentification à deux facteurs.
- **Applications EpicCare :** ces applications offrent aux professionnels de la santé un accès sécurisé et portable aux dossiers des patients, aux listes de patients, aux calendriers et aux messages.
  - **Haiku :** application mobile pour les téléphones iPhone et Android.
  - **Canto :** application mobile pour l'iPad.
  - **Rover :** applications mobiles pour iPhone et l'iPad.

HDX : les applications HDX sont fournies via Citrix Virtual Apps dans Citrix Workspace.

- **Epic Hyperspace :** application Epic client pour la gestion électronique des dossiers de santé.

ISV

- **Vocera :** application VoIP et de messagerie compatible HIPAA qui étend les avantages de la technologie vocale Vocera à tout moment, n'importe où, via l'iPhone et les smartphones Android.

Applications internes

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **HCMail :** application qui permet de composer des messages cryptés, d'effectuer des recherches dans des carnets d'adresses sur des serveurs de messagerie internes et d'envoyer les messages cryptés aux contacts à l'aide d'un client de messagerie.

Applications web internes

- **PatientRounding :** application Web utilisée pour enregistrer les informations sur la santé des patients par différents départements.
- **Outlook Web Access :** permet l'accès à la messagerie via un navigateur Web.
- **SharePoint :** utilisé pour le partage de fichiers et de données à l'échelle de l'organisation.

Le tableau suivant répertorie les informations de base requises pour la configuration MAM.

Nom de l' application	Type d' application	Encapsulation MDX	iOS	Android
Citrix Secure Mail	Application de productivité mobile	Pas pour la version 10.4.1 et versions ultérieures	Oui	Oui
Citrix Secure Web	Application de productivité mobile	Pas pour la version 10.4.1 et versions ultérieures	Oui	Oui
Citrix Files	Application de productivité mobile	Pas pour la version 10.4.1 et versions ultérieures	Oui	Oui
Citrix Secure Hub	Application publique	SO	Oui	Oui
Application Citrix Workspace	Application publique	SO	Oui	Oui
GoToMeeting	Application publique	SO	Oui	Oui
SalesForce1	Application publique	SO	Oui	Oui
RSA SecurID	Application publique	SO	Oui	Oui
Epic Haiku	Application publique	SO	Oui	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de l' application	Type d' application	Encapsulation MDX	iOS	Android
Epic Canto	Application publique	SO	Oui	Non
Epic Rover	Application publique	SO	Oui	Non
Epic Hyperspace	Application HDX	SO	Oui	Oui
Vocera	Application d' éditeur de logiciels indépendant	Oui	Oui	Oui
HCMail	Application interne	Oui	Oui	Oui
PatientRounding	Application Web	SO	Oui	Oui
Outlook Web Access	Application Web	SO	Oui	Oui
SharePoint	Application Web	SO	Oui	Oui

Les tableaux suivants répertorient les exigences spécifiques que vous pouvez consulter lorsque vous configurez les stratégies MAM dans Citrix Endpoint Management.

Nom de l' application	VPN requis	Interaction (avec des applications en dehors du conteneur)	Interaction (à partir d' applications en dehors du conteneur)	Cryptage de l' appareil basé sur la plate-forme
Citrix Secure Mail	O	Autorisé de manière sélective	Autorisé	Non requis
Citrix Secure Web	O	Autorisé	Autorisé	Non requis
Citrix Files	O	Autorisé	Autorisé	Non requis
Citrix Secure Hub	O	S/O	S/O	S/O
Application Citrix Workspace	O	S/O	S/O	S/O
GoToMeeting	N	S/O	S/O	S/O
SalesForce1	N	S/O	S/O	S/O
RSA SecurID	N	S/O	S/O	S/O

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de l' application	VPN requis	Interaction (avec des applications en dehors du conteneur)	Interaction (à partir d' applications en dehors du conteneur)	Cryptage de l' appareil basé sur la plate-forme
Epic Haiku	O	S/O	S/O	S/O
Epic Canto	O	S/O	S/O	S/O
Epic Rover	O	S/O	S/O	S/O
Epic Hyperspace	O	S/O	S/O	S/O
Vocera	O	Bloqué	Bloqué	Non requis
HCMail	O	Bloqué	Bloqué	Obligatoire
PatientRounding	O	S/O	S/O	Obligatoire
Outlook Web Access	O	S/O	S/O	Non requis
SharePoint	O	S/O	S/O	Non requis

Nom de l' application	Filtrage par proxy	Gestion des licences	Géofencing	SDK Applications mobiles	Version minimale du système d' exploitation
Citrix Secure Mail	Obligatoire	S/O	Requis de manière sélective	S/O	Appliqué
Citrix Secure Web	Obligatoire	S/O	Non requis	S/O	Appliqué
Secure Notes	Obligatoire	S/O	Non requis	S/O	Appliqué
Citrix Files	Obligatoire	S/O	Non requis	S/O	Appliqué
Citrix Secure Hub	Non requis	Achat en volume	Non requis	S/O	Non appliqué
Application Citrix Workspace	Non requis	Achat en volume	Non requis	S/O	Non appliqué
GoToMeeting	Non requis	Achat en volume	Non requis	S/O	Non appliqué

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de l' application	Filtrage par proxy	Gestion des licences	Géofencing	SDK Applications mobiles	Version minimale du système d' exploitation
SalesForce1	Non requis	Achat en volume	Non requis	S/O	Non appliqué
RSA SecurID	Non requis	Achat en volume	Non requis	S/O	Non appliqué
Epic Haiku	Non requis	Achat en volume	Non requis	S/O	Non appliqué
Epic Canto	Non requis	Achat en volume	Non requis	S/O	Non appliqué
Epic Rover	Non requis	Achat en volume	Non requis	S/O	Non appliqué
Epic Hyperspace	Non requis	S/O	Non requis	S/O	Non appliqué
Vocera	Obligatoire	S/O	Obligatoire	Obligatoire	Appliqué
HCMail	Obligatoire	S/O	Obligatoire	Obligatoire	Appliqué
PatientRounding	Obligatoire	S/O	Non requis	S/O	Non appliqué
Outlook Web Access	Obligatoire	S/O	Non requis	S/O	Non appliqué
SharePoint	Obligatoire	S/O	Non requis	S/O	Non appliqué

Communautés d'utilisateurs

Chaque organisation est composée de diverses communautés d'utilisateurs qui opèrent dans différents rôles fonctionnels. Ces communautés d'utilisateurs exécutent différentes tâches et fonctions de bureau à l'aide de diverses ressources que vous fournissez via des appareils utilisateur. Les utilisateurs peuvent travailler à domicile ou dans des bureaux distants à l'aide d'appareils mobiles que vous fournissez. Les utilisateurs peuvent également posséder leurs appareils mobiles, ce qui leur permet d'accéder à des outils soumis à certaines règles de conformité de sécurité.

Avec un plus grand nombre de communautés d'utilisateurs utilisant des appareils mobiles pour leur travail, la gestion de la mobilité d'entreprise devient essentielle pour éviter la fuite de données. La gestion EMM est également essentielle pour appliquer les restrictions de sécurité d'une organisation. Pour une gestion efficace et plus sophistiquée des appareils mobiles, vous pouvez catégoriser vos communautés d'utilisateurs. Cela simplifie le mappage des utilisateurs aux ressources et applique les stratégies de sécurité appropriées pour les utilisateurs.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

L'exemple suivant illustre comment les communautés d'utilisateurs d'une organisation de soins de santé sont classées pour EMM.

Cas d'utilisation des communautés d'utilisateurs

Cet exemple d'organisation de soins de santé fournit des ressources technologiques et un accès à plusieurs utilisateurs, y compris des employés et des bénévoles du réseau et de sociétés affiliées. L'organisation a choisi de déployer la solution EMM auprès des utilisateurs non-cadres uniquement.

Vous pouvez répartir les rôles utilisateur et les fonctions de cette organisation en sous-groupes, y compris personnel médical, personnel non-médical et sous-traitants. Certains utilisateurs reçoivent des appareils mobiles d'entreprise tandis que d'autres peuvent accéder aux ressources limitées de l'entreprise à partir de leurs appareils personnels. Pour appliquer le niveau approprié de restrictions de sécurité et empêcher la fuite de données, l'organisation a décidé que l'informatique de l'entreprise gère chaque appareil inscrit. Ces appareils peuvent appartenir à une entreprise ou être de type BYOD. En outre, les utilisateurs ne peuvent inscrire qu'un seul appareil.

La section suivante donne un aperçu des rôles et des fonctions de chaque sous-groupe :

Personnel médical

- Infirmiers/Infirmières
- Médecins (docteurs, chirurgiens, etc.)
- Spécialistes (diététiciens, anesthésistes, radiologues, cardiologues, oncologues, etc.)
- Médecins externes (médecins non-employés et employés de bureau travaillant dans des bureaux éloignés)
- Services de santé à domicile (employés de bureau et travailleurs mobiles exécutant des services médicaux lors de visites à domicile auprès de patients)
- Spécialistes en recherche (travailleurs intellectuels et utilisateurs avancés dans six instituts de recherche médicale)
- Éducation et formation (infirmiers/infirmières, médecins et spécialistes en phase d'éducation et de formation)

Personnel non-médical

- Services partagés (employés de bureau effectuant diverses fonctions administratives, y compris RH, gestion des salaires, comptes fournisseurs, service de la chaîne d'approvisionnement, etc.)
- Services médicaux (employés de bureau effectuant divers services de gestion des soins de santé, services administratifs et solutions de processus commerciaux aux fournisseurs, y compris : services administratifs, analyse commerciale et intelligence économique, systèmes commerciaux,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

services aux clients, finances, gestion des soins, solutions d'accès patient, solutions de cycle des revenus, etc.)
- Services de support (employés de bureau remplissant diverses fonctions non-médicales, y compris : administration des avantages sociaux, intégration clinique, communications, rémunération et gestion du rendement, services d'équipement et de site, systèmes de technologie des RH, services d'information, vérification interne et amélioration des processus, etc.)
- Programmes philanthropiques (employés de bureau et mobiles qui exécutent diverses fonctions pour soutenir les programmes philanthropiques)

Sous-traitants

- Partenaires fabricants et fournisseurs (connectés sur site et à distance via un VPN site à site fournissant diverses fonctions de support non-médical)

Sur la base des informations précédentes, l'organisation a créé les entités suivantes. Pour plus d'informations sur les groupes de mise à disposition dans Citrix Endpoint Management, consultez la section Déployer des ressources.

Unités d'organisation et groupes Active Directory Unité d'organisation **=** Ressources Citrix Endpoint Management :

- Unité d'organisation = personnel médical ; Groupes =
  - XM - Infirmiers/Infirmières
  - XM - Médecins
  - XM - Spécialistes
  - XM - Médecins externes
  - XM - Services de santé à domicile
  - XM - Spécialistes en recherche
  - XM - Éducation et formation
- Unité d'organisation = non-médical ; Groupes =
  - XM - Services partagés
  - XM - Services médicaux
  - XM - Services de support
  - XM - Programmes philanthropiques

Utilisateurs et groupes locaux Citrix Endpoint Management Groupe = sous-traitants ; Utilisateurs =

- Vendor1

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Vendor2
- Fournisseur 3
- …Fournisseur 10

Groupes de mise à disposition Citrix Endpoint Management

- Personnel médical - Infirmiers/Infirmières
- Personnel médical - Médecins
- Personnel médical - Spécialistes
- Personnel médical - Médecins externes
- Personnel médical - Services de santé à domicile
- Personnel médical - Spécialistes en recherche
- Personnel médical - Éducation et formation
- Personnel non-médical - Services partagés
- Personnel non-médical - Services médicaux
- Personnel non-médical - Services de support
- Personnel non-médical - Programmes philanthropiques

Groupe de mise à disposition et mappage de groupe d'utilisateurs

Groupes Active Directory	Groupes de mise à disposition Citrix Endpoint Management
XM - Infirmiers/Infirmières	Personnel médical - Infirmiers/Infirmières
XM - Médecins	Personnel médical - Médecins
XM - Spécialistes	Personnel médical - Spécialistes
XM - Médecins externes	Personnel médical - Médecins externes
XM - Services de santé à domicile	Personnel médical - Services de santé à domicile
XM - Spécialistes en recherche	Personnel médical - Spécialistes en recherche
XM - Éducation et formation	Personnel médical - Éducation et formation
XM - Services partagés	Personnel non-médical - Services partagés
XM - Services médicaux	Personnel non-médical - Services médicaux
XM - Services de support	Personnel non-médical - Services de support
XM - Programmes philanthropiques	Personnel non-médical - Programmes philanthropiques

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Groupe de mise à disposition et mappage des ressources Les tableaux suivants illustrent les ressources affectées à chaque groupe de mise à disposition dans ce cas d'utilisation. Le premier tableau présente les attributions d'applications mobiles. Le deuxième tableau présente les ressources d'applications publiques, d'applications HDX et de gestion des appareils.

Groupes de mise à disposition Citrix Endpoint Management	Applications mobiles Citrix	Applications mobiles publiques	Applications mobiles HDX
Personnel médical - Infirmiers/Infirmières	X		
Personnel médical - Médecins			
Personnel médical - Spécialistes			
Personnel médical - Médecins externes	X		
Personnel médical - Services de santé à domicile	X		
Personnel médical - Spécialistes en recherche	X		
Personnel médical - Éducation et formation		X	X
Personnel non-médical - Services partagés		X	X
Personnel non-médical - Services médicaux		X	X
Personnel non-médical - Services de support	X	X	X
Personnel non-médical - Programmes philanthropiques	X	X	X
Sous-traitants	X	X	X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Groupes de mise à disposition Citrix Endpoint Management	Application publique : RSA SecurID	Application publique : EpicCare Haiku	Application HDX : Epic Hyperspace	Stratégie de code secret	Restrictions d' appareil	Actions automatisées	Stratégie de réseau
Personnel médical - Infirmiers/Infirmières							X
Personnel médical - Médecins					X		
Personnel médical - Spécialistes							
Personnel médical - Médecins externes							
Personnel médical - Services de santé à domicile							
Personnel médical - Spécialistes en recherche							
Personnel médical - Éducation et formation		X	X				

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Groupes de mise à disposition Citrix Endpoint Management	Application publique : RSA SecurID	Application publique : EpicCare Haiku	Application HDX : Epic Hyperspace	Stratégie de code secret	Restrictions d' appareil	Actions automatisées	Stratégie de réseau
Personnel non-médical - Services partagés		X	X				
Personnel non-médical - Services médicaux		X	X				
Personnel non-médical - Services de support		X	X				

Notes et considérations

- Citrix Endpoint Management crée un groupe de mise à disposition par défaut appelé Tous les utilisateurs lors de la configuration initiale. Si vous ne désactivez pas de ce groupe de mise à disposition, tous les utilisateurs Active Directory ont le droit de s'inscrire à Citrix Endpoint Management.
- Citrix Endpoint Management synchronise les utilisateurs et les groupes Active Directory à la demande en utilisant une connexion dynamique au serveur LDAP.
- Si un utilisateur fait partie d'un groupe qui n'est pas mappé dans Citrix Endpoint Management, cet utilisateur ne peut pas s'inscrire. De même, si un utilisateur est membre de plusieurs groupes, Citrix Endpoint Management catégorise uniquement l'utilisateur comme étant dans les groupes mappés à Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exigences en matière de sécurité

La portée des considérations de sécurité liées à un environnement Citrix Endpoint Management peut rapidement devenir écrasante. Il existe de nombreux composants et de paramètres imbriqués. Vous ne savez peut-être pas par où commencer ou quoi choisir pour vous assurer qu'un niveau de protection acceptable est disponible. Pour simplifier ces choix, Citrix fournit des recommandations pour une sécurité élevée, une sécurité supérieure et une sécurité maximale, comme indiqué dans le tableau suivant.

Les problèmes de sécurité seuls ne doivent pas à eux seuls dicter le mode d'inscription de vos appareils : MAM, MDM+MAM avec MDM facultatif, ou MDM+MAM avec MDM requis. Il est également important d'examiner les exigences des cas d'utilisation et de décider si vous pouvez atténuer les problèmes de sécurité avant de choisir votre mode de gestion.

Sécurité élevée : l'utilisation de ces paramètres offre une expérience utilisateur optimale tout en maintenant un niveau de sécurité de base acceptable pour la plupart des organisations.

Sécurité supérieure : ces paramètres établissent un meilleur équilibre entre sécurité et facilité d'utilisation.

Sécurité la plus élevée : suivre ces recommandations fournit un haut niveau de sécurité au détriment de la facilité d'utilisation et de l'adoption par les utilisateurs.

Considérations sur la sécurité du mode de gestion

Le tableau suivant spécifie les modes de gestion pour chaque niveau de sécurité.

Haute sécurité	Sécurité plus élevée	Sécurité la plus élevée
MAM, MDM+MAM	MDM+MAM	MDM+MAM

Remarques :

- Selon le cas d'utilisation, un déploiement MAM exclusif peut répondre aux exigences de sécurité et offrir une bonne expérience utilisateur.
- Pour les cas d'utilisation tels que le BYOD dans lequel toutes les exigences de l'entreprise et de sécurité peuvent être satisfaites uniquement avec la conteneurisation d'applications, Citrix recommande le mode MAM exclusif.
- Pour les environnements à haute sécurité (et les appareils fournis par les entreprises), Citrix recommande MDM+MAM pour tirer parti de toutes les fonctionnalités de sécurité disponibles.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Considérations relatives à la sécurité de Citrix ADC et NetScaler Gateway

Le tableau suivant spécifie les recommandations Citrix ADC et NetScaler Gateway pour chaque niveau de sécurité.

Haute sécurité	Sécurité plus élevée	Sécurité la plus élevée
Citrix ADC est recommandé. NetScaler Gateway est requis pour MAM et MDM+MAM.	Configuration standard de l'assistant NetScaler pour XenMobile avec pont SSL si Citrix Endpoint Management se trouve dans la zone démilitarisée.	Décharge SSL avec cryptage de bout en bout

Remarques :

- L'exposition du serveur Citrix Endpoint Management à Internet via NAT ou des proxies/équilibreurs de charge tiers existants peut être une option pour MDM. Toutefois, dans ce cas, le trafic SSL se termine sur un serveur Citrix Endpoint Management, ce qui pose un risque de sécurité potentiel.
- Pour les environnements hautement sécurisés, NetScaler Gateway défini avec la configuration Citrix Endpoint Management par défaut doit respecter ou dépasser les exigences de sécurité.
- Pour les inscriptions MDM ayant les besoins de sécurité les plus élevés, la terminaison SSL sur NetScaler Gateway permet d'inspecter le trafic sur le périmètre tout en assurant le cryptage SSL de bout en bout.
- Options pour définir les chiffrements SSL/TLS.
- Pour plus d'informations, voir Intégration avec NetScaler Gateway et Citrix ADC.

Considérations de sécurité d'inscription

Le tableau suivant spécifie les recommandations Citrix ADC et NetScaler Gateway pour chaque niveau de sécurité.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Haute sécurité	Sécurité plus élevée	Sécurité la plus élevée
Appartenance à un groupe Active Directory uniquement. Groupe de mise à disposition Tous les utilisateurs désactivé.	Mode d'inscription sécurisée sur invitation uniquement. Appartenance à un groupe Active Directory uniquement. Groupe de mise à disposition Tous les utilisateurs désactivé	Mode d'inscription sécurisée lié à l'ID d'appareil. Appartenance à un groupe Active Directory uniquement. Groupe de mise à disposition Tous les utilisateurs désactivé

> **Remarques :**
>
> - Citrix vous recommande généralement de limiter l'inscription aux utilisateurs appartenant à des groupes Active Directory prédéfinis uniquement. Cette restriction nécessite de désactiver le groupe de mise à disposition intégré Tous les utilisateurs.
> - Vous pouvez utiliser des invitations d'inscription pour restreindre l'inscription aux utilisateurs avec une invitation. Les invitations d'inscription ne sont pas disponibles pour les appareils Windows.
> - Vous pouvez utiliser des invitations à s'inscrire par code PIN unique (OTP) comme solution d'authentification à deux facteurs et contrôler le nombre d'appareils qu'un utilisateur peut inscrire. (Les invitations OTP ne sont pas disponibles pour les appareils Windows.)

Considérations de sécurité pour le code secret des appareils

Le tableau suivant spécifie les recommandations de code secret de l'appareil pour chaque niveau de sécurité.

Haute sécurité	Sécurité plus élevée	Sécurité la plus élevée
Recommandée. Une haute sécurité est requise pour le cryptage au niveau de l'appareil. Peut être appliqué avec MDM. Peut être défini selon les besoins pour MAM exclusif en utilisant la stratégie MDX, Comportement des appareils non conformes.	Appliqué à l'aide d'une stratégie MDM, MAM ou MDM+MAM.	Appliquée en utilisant une stratégie MDM et MDX. Stratégie de code secret complexe.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Remarques :**
>
> - Citrix recommande l'utilisation d'un code secret d'appareil.
> - Vous pouvez appliquer un code secret d'appareil via une stratégie MDM.
> - Vous pouvez utiliser une stratégie MDX pour que le code secret d'un appareil soit obligatoire pour l'utilisation des applications gérées ; par exemple, pour les cas d'utilisation BYOD.
> - Citrix recommande de combiner les options de stratégie MDM et MDX pour une sécurité accrue dans les inscriptions MDM+MAM.
> - Pour les environnements ayant les exigences de sécurité les plus élevées, vous pouvez configurer des stratégies de code d'accès complexes et les appliquer avec MDM. Vous pouvez configurer des actions automatiques pour informer les administrateurs ou émettre des effacements sélectifs/complets lorsqu'un appareil ne respecte pas une stratégie de code d'accès.

Applications

March 1, 2024

La gestion de la mobilité d'entreprise (EMM) inclut la gestion d'appareils mobiles (MDM) et gestion d'applications mobiles (MAM). Alors que MDM permet aux entreprises de sécuriser et de contrôler les appareils mobiles, MAM facilite la livraison et la gestion des applications. Avec l'adoption croissante de la stratégie BYOD (Apportez votre propre appareil), vous pouvez généralement implémenter une solution MAM, telle que Citrix Endpoint Management. Citrix Endpoint Management vous aide à prendre en charge la mise à disposition des applications, l'attribution des licences logicielles, la configuration et la gestion du cycle de vie des applications. Vous pouvez obliger ou autoriser les utilisateurs à opter pour la gestion MDM.

Avec Citrix Endpoint Management, vous pouvez sécuriser les applications en configurant des stratégies MAM et des paramètres VPN pour éviter les fuites de données et autres menaces de sécurité. Citrix Endpoint Management offre aux entreprises la flexibilité d'inscrire des appareils avec MAM exclusif ou MDM+MAM.

En plus de la possibilité de mettre à disposition des applications sur des appareils mobiles, Citrix Endpoint Management propose la conteneurisation d'applications via la technologie MDX. Les applications sont soumises à des contrôles granulaires basés sur des stratégies. Les éditeurs de logiciels indépendants peuvent appliquer ces contrôles à l'aide du SDK Mobile Apps.

Dans un environnement d'entreprise, les utilisateurs utilisent diverses applications mobiles pour les aider dans leur travail. Les applications peuvent inclure des applications du magasin d'applications

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

public, des applications développées en interne ou des applications natives. Citrix Endpoint Management classe ces applications comme suit :

- **Applications publiques :** ces applications peuvent être gratuites ou payantes et sont disponibles dans un magasin d'applications public, tel que l'Apple App Store ou Google Play. Les fournisseurs externes à l'organisation mettent souvent à disposition leurs applications dans des magasins d'applications publics. Cette option permet aux clients de télécharger les applications directement depuis Internet. Vous pouvez utiliser de nombreuses applications publiques dans votre organisation en fonction des besoins des utilisateurs. Des exemples de telles applications incluent les applications GoToMeeting, Salesforce et EpicCare.
  - **Si vous utilisez le SDK MAM :** obtenez les binaires d'application auprès du fournisseur de votre application. Ensuite, intégrez le SDK MAM dans l'application.
  - **Si vous utilisez MDX Toolkit :** Citrix ne prend pas en charge le téléchargement des fichiers binaires des applications directement à partir des magasins d'applications publics ou l'encapsulation avec MDX Toolkit pour la distribution d'entreprise. Pour encapsuler des applications tierces, collaborez avec le fournisseur de votre application pour obtenir les fichiers binaires de l'application. Vous pouvez ensuite encapsuler les fichiers binaires à l'aide de l'outil MDX Toolkit.
- **Applications internes :** de nombreuses organisations ont des développeurs internes qui créent des applications fournissant des fonctionnalités spécifiques et étant développées et distribuées indépendamment au sein de l'organisation. Dans certains cas, certaines organisations peuvent également avoir des applications fournies par des éditeurs de logiciels indépendants. Vous pouvez déployer ces applications en tant qu'applications natives ou vous pouvez les conteneuriser en utilisant une solution MAM, telle que Citrix Endpoint Management.

  Par exemple, une organisation de soins de santé peut créer une application interne qui permet aux médecins de consulter les informations sur les patients à partir d'appareils mobiles. Une organisation peut ensuite sécuriser les informations des patients et activer l'accès VPN à la base de données des patients en utilisant l'une des méthodes suivantes :
  - SDK MAM
  - MDX Toolkit
- **Applications Web et Saas :** ces applications comprennent les applications accessibles à partir d'un réseau interne (applications web) ou sur un réseau public (SaaS). Citrix Endpoint Management vous permet également de créer des applications Web et SaaS personnalisées à l'aide d'une liste de connecteurs d'applications. Ces connecteurs d'application peuvent faciliter l'authentification unique (SSO) aux applications Web existantes. Pour de plus amples informations, consultez la section Types de connecteur d'application. Par exemple, vous pouvez utiliser Google Apps SAML pour l'authentification unique basée sur le langage SAML (Security Assertion Markup Language) de Google Apps.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Applications de productivité mobiles Citrix :** il s'agit d'applications développées par Citrix et incluses avec la licence Citrix Endpoint Management. Pour plus de détails, consultez la section À propos des applications de productivité mobiles. Citrix propose également d'autres applications prêtes à l'emploi que les éditeurs de logiciels indépendants peuvent développer à l'aide du SDK Mobile Apps.
- **Applications HDX :** il s'agit d'applications hébergées par Windows que vous publiez avec StoreFront. Si vous utilisez Citrix Virtual Apps and Desktops et Citrix Workspace, les applications HDX sont disponibles pour les utilisateurs inscrits.

Selon le type d'applications mobiles que vous prévoyez de déployer et de gérer avec Citrix Endpoint Management, la configuration sous-jacente peut différer. Par exemple, si plusieurs groupes d'utilisateurs ayant des niveaux d'autorisation différents utilisent une même application, vous pouvez créer des groupes de mise à disposition distincts pour déployer deux versions distinctes de la même application. Vous devez par ailleurs vous assurer que l'appartenance au groupe d'utilisateurs est mutuellement exclusive pour éviter les incohérences de stratégie sur les appareils des utilisateurs.

Vous pouvez également gérer les licences d'applications iOS à l'aide de l'achat en volume d'Apple. Vous devrez pour cela vous inscrire au programme d'achat en volume et configurer les paramètres d'achat en volume dans la console Citrix Endpoint Management. Cette configuration vous permet de distribuer les applications avec les licences d'achat en volume. Avec une telle variété de cas d'utilisation, il est important d'évaluer et de planifier votre stratégie MAM avant la mise en œuvre de l'environnement Citrix Endpoint Management. Vous pouvez commencer à planifier votre stratégie MAM en définissant les éléments suivants :

- **Types d'applications :** répertoriez les différents types d'applications que vous souhaitez prendre en charge et catégorisez-les, tels que public, natif, Web, interne ou applications d'éditeurs de logiciels indépendants. En outre, catégorisez les applications selon différentes plates-formes d'appareils, telles que iOS et Android. Cette catégorisation permet d'aligner les différents paramètres Citrix Endpoint Management requis pour chaque type d'application. Par exemple, certaines applications peuvent nécessiter l'utilisation du SDK Mobile Apps pour activer des API spéciales pour l'interaction avec d'autres applications.
- **Exigences en matière de réseau :** configurez les paramètres d'applications avec des exigences d'accès réseau spécifiques. Par exemple, certaines applications peuvent nécessiter l'accès à votre réseau interne via un VPN. Certaines applications peuvent nécessiter un accès Internet pour acheminer l'accès via la DMZ. Pour permettre à ces applications de se connecter au réseau requis, vous devez configurer divers paramètres en conséquence. La définition des exigences réseau par application vous aide à finaliser vos décisions architecturales dès le début, ce qui simplifie le processus de mise en œuvre global.
- **Exigences en matière de sécurité :** vous pouvez définir des exigences de sécurité qui s'appliquent à des applications individuelles ou à toutes les applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Les paramètres, tels que les stratégies MDX, s'appliquent à des applications individuelles
  - Les paramètres de session et d'authentification s'appliquent à toutes les applications
  - Certaines applications peuvent avoir des exigences spécifiques en matière de conteneurisation, de MDX, d'authentification, de géofencing, de code d'accès ou de partage de données

  Définissez ces exigences à l'avance afin de simplifier votre déploiement. Pour de plus amples informations sur la sécurité dans Citrix Endpoint Management, consultez la section Sécurité et expérience utilisateur.

- **Exigences en matière de déploiement :** vous pouvez utiliser un déploiement basé sur des stratégies pour autoriser le téléchargement des applications publiées uniquement par des utilisateurs compatibles. Par exemple, certaines applications peuvent exiger que l'appareil soit géré ou que l'appareil corresponde à une version minimale du système d'exploitation. Vous pouvez également exiger que certaines applications soient uniquement disponibles pour les utilisateurs d'entreprise. Définissez ces exigences à l'avance afin de pouvoir configurer les stratégies ou les actions de déploiement appropriées.

- **Exigences en matière de licence :** enregistrez les exigences en matière de licence liées à l'application. Vos notes peuvent vous aider à gérer efficacement l'utilisation des licences et à décider si vous devez configurer des fonctionnalités spécifiques dans Citrix Endpoint Management pour faciliter l'attribution de licences. Par exemple, si vous déployez une application iOS gratuite ou payante, Apple applique les exigences de licence sur l'application. Par conséquent, les utilisateurs doivent se connecter à leur compte Apple App Store.

  Cependant, vous pouvez vous inscrire à l'achat en volume d'Apple pour distribuer et gérer ces applications via Citrix Endpoint Management. L'achat en volume permet aux utilisateurs de télécharger les applications sans se connecter à leur compte Apple App Store.

  Certaines plates-formes présentent des exigences de licence spéciales qui doivent être satisfaites avant le déploiement de ces fonctionnalités.

- **Exigences en matière de liste d'autorisation/liste de blocage :** vous pouvez identifier des applications que les utilisateurs ne doivent pas installer ou utiliser. La création d'une liste de blocage définit un événement hors conformité. Vous pouvez ensuite configurer des stratégies pour qu'elles se déclenchent lorsque l'événement se produit. D'un autre côté, une application peut être acceptable pour une utilisation, mais peut tomber sous la liste de blocage pour une raison quelconque. Dans ce cas, vous pouvez ajouter l'application à une liste d'autorisation et indiquer que l'utilisation de l'application est acceptable mais n'est pas requise. De plus, gardez à l'esprit que les applications préinstallées sur les nouveaux appareils peuvent inclure certaines applications couramment utilisées qui ne font pas partie du système d'exploitation. De telles applications peuvent entrer en conflit avec votre stratégie de liste de blocage.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cas d'utilisation

Une organisation de soins de santé prévoit de déployer Citrix Endpoint Management en tant que solution MAM pour leurs applications mobiles. Les applications mobiles sont mises à disposition des utilisateurs professionnels et BYOD. Le département informatique décide de mettre à disposition et de gérer les applications suivantes :

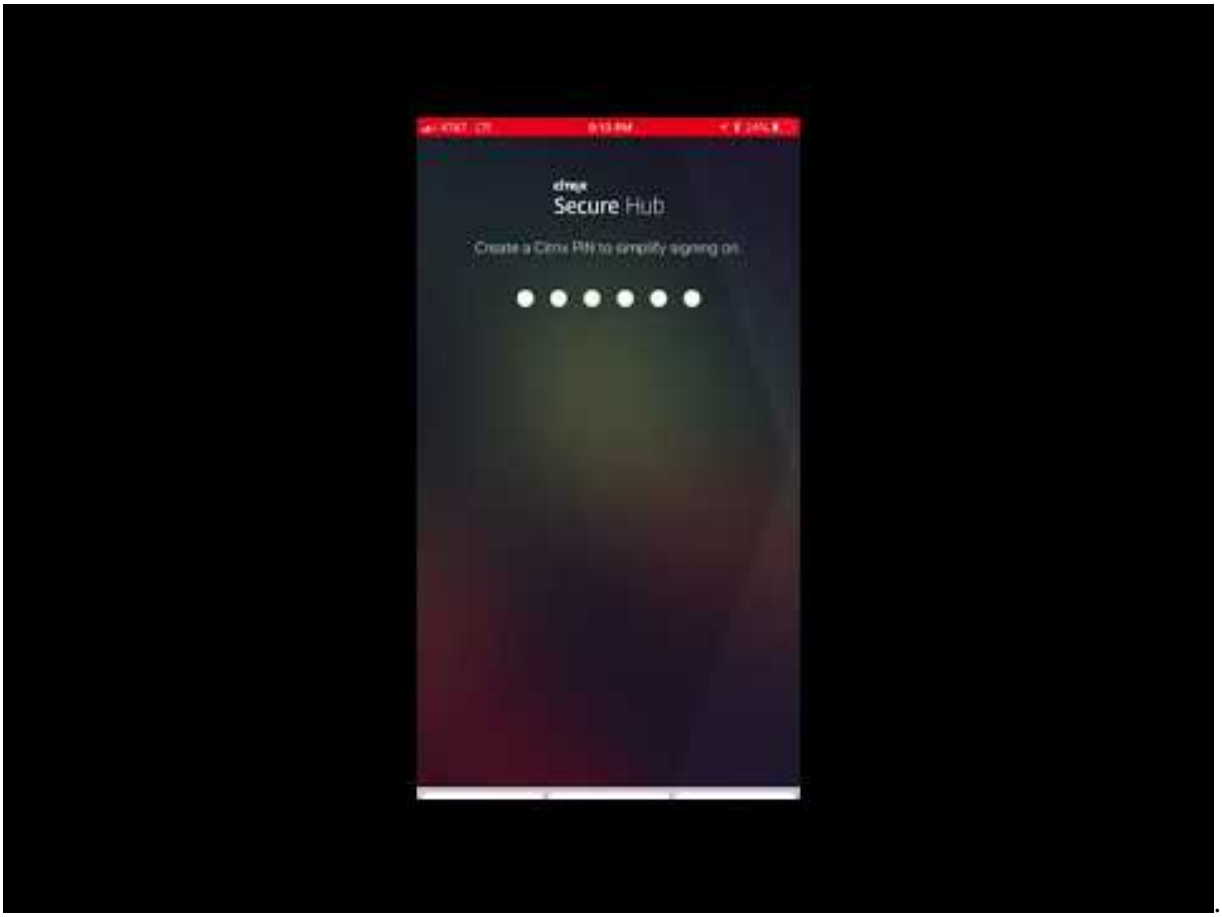
Applications de productivité mobiles : applications iOS et Android fournies par Citrix. Pour plus de détails, consultez la section Applications de productivité mobiles.

Citrix Secure Hub : pour les clients intégrés avec une version antérieure à Citrix Endpoint Management 10.18.14 : vous transmettez les paramètres de sécurité, les configurations et les applications mobiles aux appareils mobiles via Citrix Secure Hub. Les appareils Android et iOS s'inscrivent dans Citrix Endpoint Management via Citrix Secure Hub.

Pour les nouveaux clients à compter de Citrix Endpoint Management 10.18.14 : Citrix Secure Hub prend en charge l'utilisation du magasin d'applications Workspace. Lors de l'ouverture de Citrix Secure Hub, les utilisateurs ne voient plus le magasin Citrix Secure Hub. Désormais, un bouton Ajouter des applications permet aux utilisateurs d'accéder au magasin d'applications Workspace.

Voici une vidéo qui montre un appareil iOS effectuant une inscription à Citrix Endpoint Management à l'aide de l'application Citrix Workspace.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Application Citrix Workspace : l'application Citrix Workspace intègre la technologie Citrix Receiver existante, Citrix Secure Hub ainsi que les autres technologies clientes de Citrix Workspace. L'application Citrix Workspace offre aux utilisateurs finaux une expérience contextuelle unifiée.

GoToMeeting : un client de réunion, de partage de bureau et de visioconférence en ligne qui permet aux utilisateurs de se rencontrer en temps réel avec d'autres utilisateurs, clients ou collègues via Internet.

SalesForce1 : Salesforce1 permet aux utilisateurs d'accéder à Salesforce à partir d'appareils mobiles et rassemble toutes les applications Chatter, CRM et applications personnalisées, ainsi que les processus d'entreprise, pour une expérience unifiée pour tout utilisateur Salesforce.

RSA SecurID : jeton logiciel pour l'authentification à deux facteurs.

Applications EpicCare : ces applications offrent aux professionnels de la santé un accès sécurisé et portable aux dossiers des patients, aux listes de patients, aux calendriers et aux messages.

Haiku : application mobile pour les téléphones iPhone et Android.

Canto : application mobile pour l'iPad.

Rover : applications mobiles pour iPhone et l'iPad.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HDX : ces applications sont fournies via Citrix Virtual Apps dans Citrix Workspace.

- **Epic Hyperspace :** application Epic client pour la gestion électronique des dossiers de santé.

ISV :

- **Vocera :** application VoIP et de messagerie compatible HIPAA qui étend les avantages de la technologie vocale Vocera à tout moment, n'importe où, via l'iPhone et les smartphones Android.

Applications internes :

- **HCMail :** application qui permet de composer des messages cryptés, d'effectuer des recherches dans des carnets d'adresses sur des serveurs de messagerie internes et d'envoyer les messages cryptés aux contacts à l'aide d'un client de messagerie.

Applications web internes :

- **PatientRounding :** application Web utilisée pour enregistrer les informations sur la santé des patients par différents départements.
- **Outlook Web Access :** permet l'accès à la messagerie via un navigateur Web.
- **SharePoint :** utilisé pour le partage de fichiers et de données à l'échelle de l'organisation.

Le tableau suivant répertorie les informations de base requises pour la configuration MAM.

Nom de l' application	Type d' application	Compatible MDX	iOS	Android
Citrix Secure Mail	Application de productivité mobile	Non	Oui	Oui
Citrix Secure Web	Application de productivité mobile	Non	Oui	Oui
Citrix Files	Application de productivité mobile	Non	Oui	Oui
Citrix Secure Hub	Application publique	S/O	Oui	Oui
Application Citrix Workspace	Application publique	S/O	Oui	Oui
GoToMeeting	Application publique	S/O	Oui	Oui
SalesForce1	Application publique	S/O	Oui	Oui

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de l' application	Type d' application	Compatible MDX	iOS	Android
RSA SecurID	Application publique	S/O	Oui	Oui
Epic Haiku	Application publique	S/O	Oui	Oui
Epic Canto	Application publique	S/O	Oui	Non
Epic Rover	Application publique	S/O	Oui	Non
Epic Hyperspace	Application HDX	S/O	Oui	Oui
Vocera	Application d' éditeur de logiciels indépendant	Oui	Oui	Oui
HCMail	Application interne	Oui	Oui	Oui
PatientRounding	Application Web	S/O	Oui	Oui
Outlook Web Access	Application Web	S/O	Oui	Oui
SharePoint	Application Web	S/O	Oui	Oui

Le tableau suivant répertorie les exigences spécifiques que vous pouvez consulter en configurant les stratégies MAM dans Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de l'application	VPN requis	Interaction (avec des applications en dehors du conteneur)	Interaction (à partir d'applications en dehors du conteneur)	Filtrage par proxy	Gestion des licences	Géofencing	SDK Applications mobiles	Version minimale du système d'exploitation
Citrix Secure Mail	O	Autorisé de manière sélective	Autorisé	Obligatoire	S/O	Requis de manière sélective	S/O	Appliqué
Citrix Secure Web	O	Autorisé	Autorisé	Obligatoire	S/O	Non requis	S/O	Appliqué
Citrix Files	O	Autorisé	Autorisé	Obligatoire	S/O	Non requis	S/O	Appliqué
Citrix Secure Hub	O	S/O	S/O	Non requis	Achat en volume	Non requis	S/O	Non appliqué
Application Citrix Workspace	O	S/O	S/O	Non requis	Achat en volume	Non requis	S/O	Non appliqué
GoToMeeting	N	S/O	S/O	Non requis	Achat en volume	Non requis	S/O	Non appliqué
SalesForce1	N	S/O	S/O	Non requis	Achat en volume	Non requis	S/O	Non appliqué
RSA SecurID	N	S/O	S/O	Non requis	Achat en volume	Non requis	S/O	Non appliqué
Epic Haiku	O	S/O	S/O	Non requis	Achat en volume	Non requis	S/O	Non appliqué
Epic Canto	O	S/O	S/O	Non requis	Achat en volume	Non requis	S/O	Non appliqué
Epic Rover	O	S/O	S/O	Non requis	Achat en volume	Non requis	S/O	Non appliqué

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de l'application	VPN requis	Interaction (avec des applications en dehors du conteneur)	Interaction (à partir d'applications en dehors du conteneur)	Filtrage par proxy	Gestion des licences	Géofencing	SDK Applications mobiles	Version minimale du système d'exploitation
Epic Hyperspace	O	S/O	S/O	Non requis	S/O	Non requis	S/O	Non appliqué
Vocera	O	Bloqué	Bloqué	Obligatoire	S/O	Obligatoire	Obligatoire	Appliqué
HCMail	O	Bloqué	Bloqué	Obligatoire	S/O	Obligatoire	Obligatoire	Appliqué
PatientRounding	O	S/O	S/O	Obligatoire	S/O	Non requis	S/O	Non appliqué
Outlook Web Access	O	S/O	S/O	Obligatoire	S/O	Non requis	S/O	Non appliqué
SharePoint	O	S/O	S/O	Obligatoire	S/O	Non requis	S/O	Non appliqué

Communautés d'utilisateurs

November 29, 2023

Chaque organisation est composée de diverses communautés d'utilisateurs qui opèrent dans différents rôles fonctionnels. Ces communautés d'utilisateurs exécutent différentes tâches et fonctions de bureau à l'aide de diverses ressources que vous fournissez via des appareils mobiles. Les utilisateurs peuvent travailler à domicile ou dans des bureaux distants à l'aide d'appareils mobiles que vous fournissez. Les utilisateurs peuvent également utiliser des appareils mobiles personnels, ce qui leur permet d'accéder à des outils soumis à certaines règles de conformité de sécurité.

Avec un plus grand nombre de communautés d'utilisateurs utilisant des appareils mobiles, la gestion de la mobilité d'entreprise devient essentielle pour éviter la fuite de données et pour appliquer les restrictions de sécurité de l'organisation. Pour une gestion efficace et plus sophistiquée des appareils mobiles, vous pouvez catégoriser vos communautés d'utilisateurs. Cela simplifie le mappage des util-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

isateurs aux ressources et garantit que les bonnes stratégies de sécurité s'appliquent aux utilisateurs appropriés.

La catégorisation des communautés d'utilisateurs peut inclure l'utilisation des composants suivants :

- Unités d'organisation et groupes Active Directory

  Les utilisateurs ajoutés à des groupes de sécurité Active Directory spécifiques peuvent recevoir des stratégies et des ressources, telles que des applications. La suppression des utilisateurs des groupes de sécurité Active Directory supprime l'accès aux ressources Citrix Endpoint Management précédemment autorisé.

- Utilisateurs et groupes locaux Citrix Endpoint Management

  Pour les utilisateurs qui n'ont pas de compte dans Active Directory, vous pouvez créer des utilisateurs en tant qu'utilisateurs Citrix Endpoint Management locaux. Vous pouvez ajouter des utilisateurs locaux à des groupes de mise à disposition et leur affecter des ressources de la même manière que les utilisateurs Active Directory.

- Groupes de mise à disposition Citrix Endpoint Management

  Si plusieurs groupes d'utilisateurs avec différents niveaux d'autorisations doivent utiliser une seule application, vous devrez peut-être créer des groupes de mise à disposition distincts. Avec des groupes de mise à disposition distincts, vous pouvez déployer deux versions distinctes de la même application. Citrix recommande de créer des groupes de mise à disposition avant de créer des stratégies d'appareil.

- Groupe de mise à disposition et mappage de groupe d'utilisateurs

  Le groupe de mise à disposition vers les mappages de groupe Active Directory peut avoir soit une relation un-à-un (one-to-one), soit une relation un-à-plusieurs (one-to-many). Attribuez des stratégies et des applications de base à un mappage de groupe de mise à disposition un-à-plusieurs. Attribuez des stratégies et des applications spécifiques à une fonction à des mappages de groupe de disposition un-à-un.

- Groupe de mise à disposition et mappage des ressources des applications

  Attribuez des applications spécifiques à chaque groupe de mise à disposition.

- Groupe de mise à disposition et mappage des ressources MDM

  Attribuez des applications et des ressources de gestion d'appareils spécifiques à chaque groupe de mise à disposition. Par exemple, configurez un groupe de mise à disposition avec une combinaison des éléments suivants : types d'applications (public, HDX, etc.), applications spécifiques par type d'application et ressources telles que les stratégies d'appareil et les actions automatisées.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

L'exemple suivant illustre comment les communautés d'utilisateurs d'une organisation de soins de santé sont classées pour EMM.

Cas d'utilisation

Cet exemple d'organisation de soins de santé fournit des ressources technologiques et un accès à plusieurs utilisateurs, y compris des employés et des bénévoles du réseau et de sociétés affiliées. L'organisation a choisi de déployer la solution EMM auprès des utilisateurs non-cadres uniquement.

Vous pouvez répartir les rôles utilisateur et les fonctions de cette organisation en sous-groupes, y compris personnel médical, personnel non-médical et sous-traitants. Un ensemble sélectionné d'utilisateurs reçoit des appareils mobiles d'entreprise tandis que d'autres peuvent accéder aux ressources limitées de l'entreprise à partir de leurs appareils personnels (BYOD). Pour appliquer le niveau approprié de restrictions de sécurité et empêcher la fuite de données, l'organisation a décidé que l'informatique de l'entreprise gère chaque appareil inscrit. En outre, les utilisateurs ne peuvent inscrire qu'un seul appareil.

Les sections suivantes donnent un aperçu des rôles et des fonctions de chaque sous-groupe :

Personnel médical

- Infirmiers/Infirmières
- Médecins (docteurs, chirurgiens, etc.)
- Spécialistes (diététiciens, anesthésistes, radiologues, cardiologues, oncologues, etc.)
- Médecins externes (médecins non-employés et employés de bureau travaillant dans des bureaux éloignés)
- Services de santé à domicile (employés de bureau et travailleurs mobiles exécutant des services médicaux lors de visites à domicile auprès de patients)
- Spécialistes en recherche (travailleurs intellectuels et utilisateurs avancés dans six instituts de recherche médicale)
- Éducation et formation (infirmiers/infirmières, médecins et spécialistes en phase d'éducation et de formation)

Personnel non-médical

- Services partagés (employés de bureau effectuant diverses fonctions administratives, y compris RH, gestion des salaires, comptes fournisseurs, service de la chaîne d'approvisionnement, etc.)
- Services médicaux (employés de bureau effectuant divers services de gestion des soins de santé, services administratifs et solutions de processus commerciaux aux fournisseurs, y compris : services administratifs, analyse commerciale et intelligence économique, systèmes commerciaux,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

services aux clients, finances, gestion des soins, solutions d'accès patient, solutions de cycle des revenus, etc.)
- Services de support (employés de bureau remplissant diverses fonctions non-médicales, y compris : administration des avantages sociaux, intégration clinique, communications, rémunération et gestion du rendement, services d'équipement et de site, systèmes de technologie des RH, services d'information, vérification interne et amélioration des processus, etc.)
- Programmes philanthropiques (employés de bureau et mobiles qui exécutent diverses fonctions pour soutenir les programmes philanthropiques)

Sous-traitants

- Partenaires fabricants et fournisseurs (connectés sur site et à distance via un VPN site à site fournissant diverses fonctions de support non-médical)

Sur la base des informations précédentes, l'organisation a créé les entités suivantes. Pour plus d'informations sur les groupes de mise à disposition dans Citrix Endpoint Management, consultez la section Déployer des ressources dans la documentation Citrix Endpoint Management.

Unités d'organisation et groupes Active Directory

Unité d'organisation = Ressources Citrix Endpoint Management

- Unité d'organisation = personnel médical ; Groupes =
  - XM - Infirmiers/Infirmières
  - XM - Médecins
  - XM - Spécialistes
  - XM - Médecins externes
  - XM - Services de santé à domicile
  - XM - Spécialistes en recherche
  - XM - Éducation et formation
- Unité d'organisation = non-médical ; Groupes =
  - XM - Services partagés
  - XM - Services médicaux
  - XM - Services de support
  - XM - Programmes philanthropiques

Utilisateurs et groupes locaux Citrix Endpoint Management

Groupe = sous-traitants ; Utilisateurs =

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Vendor1
- Vendor2
- Fournisseur 3
- …Fournisseur 10

Groupes de mise à disposition Citrix Endpoint Management

- Personnel médical - Infirmiers/Infirmières
- Personnel médical - Médecins
- Personnel médical - Spécialistes
- Personnel médical - Médecins externes
- Personnel médical - Services de santé à domicile
- Personnel médical - Spécialistes en recherche
- Personnel médical - Éducation et formation
- Personnel non-médical - Services partagés
- Personnel non-médical - Services médicaux
- Personnel non-médical - Services de support
- Personnel non-médical - Programmes philanthropiques

Groupe de mise à disposition et mappage de groupe d'utilisateurs

Groupes Active Directory	Groupes de mise à disposition Citrix Endpoint Management
XM - Infirmiers/Infirmières	Personnel médical - Infirmiers/Infirmières
XM - Médecins	Personnel médical - Médecins
XM - Spécialistes	Personnel médical - Spécialistes
XM - Médecins externes	Personnel médical - Médecins externes
XM - Services de santé à domicile	Personnel médical - Services de santé à domicile
XM - Spécialistes en recherche	Personnel médical - Spécialistes en recherche
XM - Éducation et formation	Personnel médical - Éducation et formation
XM - Services partagés	Personnel non-médical - Services partagés
XM - Services médicaux	Personnel non-médical - Services médicaux
XM - Services de support	Personnel non-médical - Services de support
XM - Programmes philanthropiques	Personnel non-médical - Programmes philanthropiques

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Groupe de mise à disposition et mappage des ressources des applications

	Secure Mail	Secure Web	Citrix Files	Application Work-space	SalesForce1	RSA SecurID	EpicCare Haiku	Epic Hyper-space
Personnel médical - Infir-mier-s/Infir-mières	X	X	X					
Personnel médical - Médecins								
Personnel médical - Spécial-istes								
Personnel médical - Médecins externes	X		X					
Personnel médical - Services de santé à domicile	X		X					
Personnel médical - Spécial-istes en recherche	X		X					

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	Secure Mail	Secure Web	Citrix Files	Application Work-space	SalesForce1	RSA SecurID	EpicCare Haiku	Epic Hyper-space
Personnel médical - Éducation et formation							X	X
Personnel non-médical - Services partagés							X	X
Personnel non-médical - Services médicaux							X	X
Personnel non-médical - Services de support	X		X				X	X
Personnel non-médical - Programmes philanthropiques	X		X				X	X
Sous-traitants	X		X	X	X		X	X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Groupe de mise à disposition et mappage des ressources MDM

	MDM : Stratégie de code secret	MDM : Restrictions d' appareil	MDM : Actions automatisées	MDM : Stratégie de réseau
Personnel médical - Infirmiers/Infirmières				X
Personnel médical - Médecins		X		
Personnel médical - Spécialistes				
Personnel médical - Médecins externes				
Personnel médical - Services de santé à domicile				
Personnel médical - Spécialistes en recherche				
Personnel médical - Éducation et formation				
Personnel non-médical - Services partagés				
Personnel non-médical - Services médicaux				

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	MDM : Stratégie de code secret	MDM : Restrictions d'appareil	MDM : Actions automatisées	MDM : Stratégie de réseau
Personnel non-médical - Services de support				
Personnel non-médical - Programmes philanthropiques				
Sous-traitants				X

Notes et considérations

- Citrix Endpoint Management crée un groupe de mise à disposition par défaut appelé Tous les utilisateurs lors de la configuration initiale. Si vous ne désactivez pas de ce groupe de mise à disposition, tous les utilisateurs Active Directory ont le droit de s'inscrire à Citrix Endpoint Management.
- Citrix Endpoint Management synchronise les utilisateurs et les groupes Active Directory à la demande en utilisant une connexion dynamique au serveur LDAP.
- Si un utilisateur fait partie d'un groupe qui n'est pas mappé dans Citrix Endpoint Management, cet utilisateur ne peut pas s'inscrire. De même, si un utilisateur est membre de plusieurs groupes, Citrix Endpoint Management catégorise uniquement l'utilisateur comme étant dans les groupes mappés à Citrix Endpoint Management.

Stratégie de messagerie

March 1, 2024

L'accès sécurisé aux e-mails à partir d'appareils mobiles est l'un des principaux moteurs de l'initiative de gestion de la mobilité de toute organisation. Décider de la bonne stratégie de messagerie est souvent un élément clé de toute conception Citrix Endpoint Management. Citrix Endpoint Management offre plusieurs options pour prendre en charge différents cas d'utilisation, en fonction de la sécurité, de l'expérience utilisateur et de l'intégration requises. Cet article couvre le processus de décision type pour la conception et les points à prendre en compte pour choisir la bonne solution, de la sélection du client à la circulation du courrier.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Choisir vos clients de messagerie

La sélection des clients est généralement une priorité pour la conception globale de la stratégie de messagerie. Vous pouvez choisir parmi plusieurs clients : Citrix Secure Mail, la messagerie native fournie avec un système d'exploitation de plateforme mobile particulier ou d'autres clients tiers disponibles via les magasins d'applications publics. En fonction de vos besoins, vous pouvez éventuellement prendre en charge les communautés d'utilisateurs avec un seul client (standard) ou utiliser une combinaison de clients.

Le tableau suivant présente des considérations de conception pour les différentes options client disponibles :

Rubrique	Citrix Secure Mail	Natif (par exemple, iOS Mail)	Messagerie tierce
Configuration	Profils de compte Exchange configurés via une stratégie MDX.	Profils de compte Exchange configurés via une stratégie MDM. La prise en charge d' Android est limitée à : Android Enterprise. Tous les autres clients sont considérés comme des clients tiers.	Nécessite généralement une configuration manuelle par l' utilisateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sécurité	Sécurisé de par sa conception, offrant la plus haute sécurité. Utilise les stratégies MDX avec des niveaux de cryptage de données supplémentaires. Citrix Secure Mail est une application entièrement gérée via une stratégie MDX. Couche d' authentification supplémentaire avec code PIN Citrix.	Basé sur l'ensemble de fonctionnalités fournisseur/application. Fournit une sécurité plus élevée. Utilise les paramètres de cryptage de l' appareil. S'appuie sur l'authentification au niveau de l'appareil pour accéder à l' application.	Basé sur l'ensemble de fonctionnalités fournisseur/application. Fournit une sécurité élevée.
Intégration	Permet l'interaction avec les applications gérées (MDX) par défaut. Ouverture d' URL Web avec Citrix Secure Web. Enregistrement des fichiers dans Citrix Files et fichiers en pièce jointe à partir de Citrix Files. Connexion directe à GoToMeeting.	Ne peut interagir qu' avec d'autres applications non gérées (non-MDX) par défaut.	Ne peut interagir qu' avec d'autres applications non gérées (non-MDX) par défaut.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Déploiement/Licence	Vous pouvez utiliser Citrix Secure Mail via MDM, directement depuis les magasins d'applications publics. Inclus avec les licences Citrix Endpoint Management Advanced et Enterprise.	Application client incluse avec le système d'exploitation de la plateforme. Aucune licence supplémentaire requise.	Vous pouvez déployer par push via MDM, en tant qu'application d'entreprise ou directement à partir des magasins d'applications publics. Modèle/coûts de licence associés basés sur le fournisseur de l'application.
Assistance	Prise en charge d'un fournisseur unique pour le client et la solution EMM (Citrix). Informations de contact d'assistance intégrées dans les fonctionnalités de journalisation de débogage Citrix Secure Hub/application. Assistance pour un seul client.	Assistance définie par le fournisseur (Apple/Google). Une assistance pour différents clients peut être nécessaire en fonction de la plate-forme de l'appareil.	Assistance définie par le fournisseur. Assistance pour un seul client, en supposant que le client tiers est pris en charge sur toutes les plates-formes des appareils gérés.

Flux et filtrage du trafic de messagerie

Cette section présente les trois scénarios principaux et les points à prendre en compte pour la conception concernant le flux du trafic de messagerie (ActiveSync) dans le contexte de Citrix Endpoint Management.

Scénario 1 : Exchange exposé

Les environnements prenant en charge des clients externes disposent généralement de services Exchange ActiveSync exposés sur Internet. Les clients Mobile ActiveSync se connectent via ce chemin externe via un proxy inverse (NetScaler Gateway, par exemple) ou via un serveur Edge. Cette option est requise pour l'utilisation de clients de messagerie natifs ou tiers, ce qui fait de ces clients l'option

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de choix pour ce scénario. Bien que ce ne soit pas une pratique courante, vous pouvez également utiliser le client Citrix Secure Mail dans ce scénario. Ce faisant, vous bénéficiez des fonctionnalités de sécurité offertes par l'utilisation des stratégies MDX et de la gestion de l'application.

Scénario 2 : Tunneling via NetScaler Gateway (micro VPN et STA)

Ce scénario est le scénario par défaut lors de l'utilisation du client Citrix Secure Mail, en raison de ses capacités micro VPN. Dans ce cas, le client Citrix Secure Mail établit une connexion sécurisée à ActiveSync via NetScaler Gateway. En substance, vous pouvez considérer Citrix Secure Mail comme le client se connectant directement à ActiveSync à partir du réseau interne. Les clients Citrix standardisent souvent Citrix Secure Mail comme client mobile ActiveSync de leur choix. Cette décision fait partie d'une initiative visant à éviter d'exposer les services ActiveSync à Internet sur un serveur Exchange exposé, comme décrit dans le premier scénario.

Seules les applications sur lesquelles le SDK MAM est activé ou encapsulées avec le MDX peuvent utiliser la fonction micro VPN. Ce scénario ne s'applique pas aux clients natifs si vous utilisez un encapsulage MDX. Même s'il est possible d'encapsuler les clients tiers avec MDX Toolkit, cette pratique n'est pas courante. L'utilisation de clients VPN au niveau des appareils pour permettre l'accès par tunnel aux clients natifs ou tiers s'est avérée fastidieuse et n'est pas une solution viable.

Scénario 3 : Services Exchange hébergés sur le cloud

Les services Exchange hébergés sur le cloud, tels que Microsoft Office 365, gagnent en popularité. Dans le contexte de Citrix Endpoint Management, ce scénario peut être traité de la même manière que le premier scénario, car le service ActiveSync est également exposé sur Internet. Dans ce cas, les exigences des fournisseurs de services cloud dictent les choix des clients. Ces choix incluent généralement la prise en charge de la plupart des clients ActiveSync, tels que Citrix Secure Mail et d'autres clients natifs ou tiers.

La solution Citrix Endpoint Management peut être avantageuse dans trois domaines pour ce scénario :

- Clients avec stratégies MDX et gestion des applications avec Citrix Secure Mail
- Configuration du client avec l'utilisation d'une stratégie MDM sur les clients de messagerie pris en charge
- Options de filtrage ActiveSync avec Citrix Endpoint Management Connector pour Exchange ActiveSync

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Filtrage du trafic de messagerie

Comme avec la plupart des services exposés sur Internet, vous devez sécuriser le chemin et fournir un filtrage pour un accès autorisé. La solution Citrix Endpoint Management comprend deux composants conçus spécifiquement pour fournir des fonctionnalités de filtrage ActiveSync aux clients natifs et tiers : NetScaler Gateway Connector pour Exchange ActiveSync et Citrix Endpoint Management Connector pour Exchange ActiveSync.

NetScaler Gateway Connector pour Exchange ActiveSync

NetScaler Gateway Connector pour Exchange ActiveSync fournit un filtrage ActiveSync sur le périmètre en utilisant NetScaler Gateway comme proxy pour le trafic ActiveSync. Le composant de filtrage se trouve donc sur le chemin du flux de trafic de messagerie, interceptant le courrier à l'entrée ou à la sortie de l'environnement. Le connecteur pour Exchange ActiveSync agit comme un intermédiaire entre NetScaler Gateway et Citrix Endpoint Management. Lorsqu'un appareil communique avec Exchange via le serveur virtuel ActiveSync sur NetScaler Gateway, NetScaler Gateway envoie un appel HTTP au connecteur pour le service Exchange ActiveSync. Ce service vérifie ensuite l'état de l'appareil auprès de Citrix Endpoint Management. En fonction de l'état de l'appareil, le connecteur pour Exchange ActiveSync répond à NetScaler Gateway d'autoriser ou de refuser la connexion. Vous pouvez également configurer des règles statiques pour filtrer l'accès en fonction de l'utilisateur, de l'agent et du type ou de l'ID de l'appareil.

Cette configuration permet aux services Exchange ActiveSync d'être exposés sur Internet avec une couche de sécurité supplémentaire pour empêcher tout accès non autorisé. Les points à prendre en compte pour la conception sont les suivants :

- **Windows Server :** le connecteur pour Exchange ActiveSync nécessite un serveur Windows Server.
- **Ensemble de règles de filtrage :** le connecteur pour Exchange ActiveSync est conçu pour le filtrage basé sur l'état et les informations de l'appareil, plutôt que sur les informations de l'utilisateur. Bien que vous puissiez configurer des règles statiques pour filtrer par ID utilisateur, aucune option n'existe pour le filtrage basé sur l'appartenance à un groupe Active Directory, par exemple. Si le filtrage de groupe Active Directory est requis, vous pouvez utiliser Citrix Endpoint Management Connector pour Exchange ActiveSync à la place.
- **Évolutivité NetScaler Gateway :** étant donné que le trafic ActiveSync doit utiliser un proxy via NetScaler Gateway, le dimensionnement correct de l'instance NetScaler Gateway est essentiel pour prendre en charge la charge de travail supplémentaire de toutes les connexions SSL ActiveSync.
- **Mise en cache intégrée NetScaler Gateway :** la configuration du connecteur pour Exchange ActiveSync sur NetScaler Gateway utilise la fonction de mise en cache intégrée pour mettre en

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

cache les réponses du connecteur. Avec cette configuration, NetScaler Gateway n'a pas besoin d'envoyer une demande au connecteur pour chaque transaction ActiveSync dans une session donnée. Cette configuration est également essentielle pour des performances et une montée en charge adéquates. La mise en cache intégrée est disponible avec l'édition Platinum de NetScaler Gateway.

- **Stratégies de filtrage personnalisées :** vous devrez peut-être créer des stratégies NetScaler Gateway personnalisées pour restreindre certains clients ActiveSync en dehors des clients mobiles natifs standard. Cette configuration nécessite des connaissances sur les requêtes HTTP ActiveSync et la création de stratégies de répondeur NetScaler Gateway.
- **Clients Citrix Secure Mail :** Citrix Secure Mail dispose de fonctionnalités micro VPN qui éliminent le besoin de filtrage sur le périmètre. Le client Citrix Secure Mail est généralement traité comme un client ActiveSync interne (de confiance) lorsqu'il est connecté via NetScaler Gateway. Si la prise en charge de clients natifs et tiers (avec le connecteur pour Exchange ActiveSync) et Citrix Secure Mail est requise : Citrix recommande de ne pas acheminer le trafic Citrix Secure Mail via le serveur virtuel NetScaler Gateway utilisé pour le connecteur. Vous pouvez acheminer ce flux de trafic via DNS et empêcher la stratégie du connecteur d'affecter les clients Citrix Secure Mail.

Pour un diagramme de NetScaler Gateway Connector pour Exchange ActiveSync dans un déploiement Citrix Endpoint Management, voir Architecture.

Citrix Endpoint Management Connector pour Exchange ActiveSync

Citrix Endpoint Management Connector pour Exchange ActiveSync est un composant de Citrix Endpoint Management qui fournit un filtrage ActiveSync au niveau du service Exchange. Par conséquent, le filtrage ne se produit qu'une fois que le courrier parvient au service Exchange, et non lorsqu'il entre dans l'environnement Citrix Endpoint Management. Mail Manager utilise PowerShell pour interroger Exchange ActiveSync sur les informations de partenariat d'appareil et contrôler l'accès via des actions de mise en quarantaine des appareils. Ces actions mettent des appareils en quarantaine et les sortent de la quarantaine en fonction des critères de règle d'Citrix Endpoint Management Connector pour Exchange ActiveSync.

De la même manière que NetScaler Gateway Connector pour Exchange ActiveSync, le connecteur pour Exchange ActiveSync vérifie l'état de l'appareil auprès de Endpoint Management pour filtrer l'accès en fonction de la conformité des appareils. Vous pouvez également configurer des règles statiques pour filtrer l'accès en fonction du type ou de l'ID de l'appareil, de la version de l'agent et de l'appartenance à un groupe Active Directory.

Cette solution ne nécessite pas l'utilisation de NetScaler Gateway. Vous pouvez déployer le connecteur pour Exchange ActiveSync sans modifier le routage du trafic ActiveSync existant. Les points à prendre en compte pour la conception sont les suivants :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

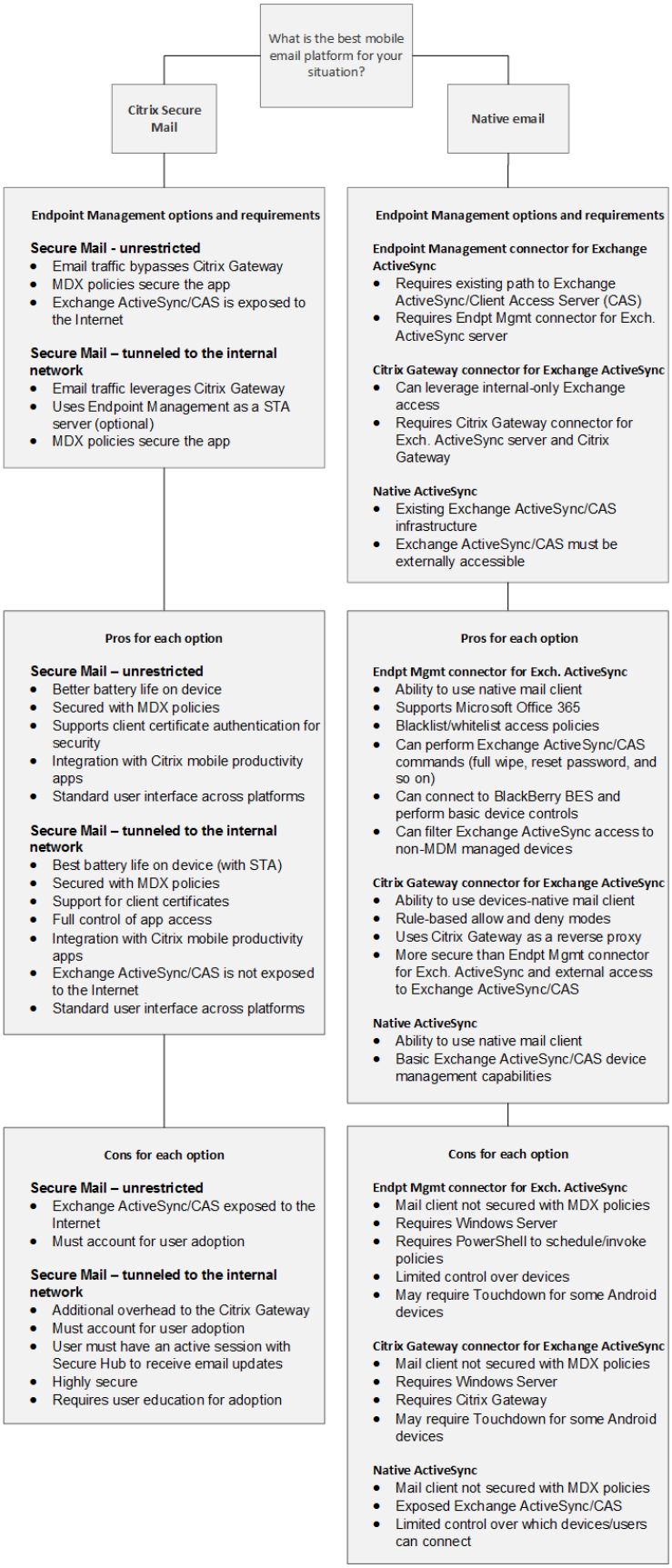
- **Windows Server :** le connecteur pour Exchange ActiveSync nécessite le déploiement de Windows Server.
- **Ensemble de règles de filtrage :** tout comme NetScaler Gateway Connector pour Exchange ActiveSync, le connecteur pour Exchange ActiveSync inclut des règles de filtrage pour évaluer l'état des appareils. En outre, le connecteur pour Exchange ActiveSync prend également en charge les règles statiques pour filtrer en fonction de l'appartenance à un groupe Active Directory.
- **Intégration Exchange :** le connecteur pour Exchange ActiveSync requiert un accès direct au serveur d'accès du client Exchange (CAS) hébergeant le rôle ActiveSync et le contrôle des actions de mise en quarantaine des appareils. Cette exigence pourrait présenter un défi selon l'architecture de l'environnement et les méthodes de sécurité. Il est essentiel d'évaluer cette exigence technique dès le départ.
- **Autres clients ActiveSync :** étant donné que le connecteur pour Exchange ActiveSync filtre au niveau du service ActiveSync, tenez compte des autres clients ActiveSync hors de l'environnement Citrix Endpoint Management. Vous pouvez configurer des règles statiques le connecteur pour Exchange ActiveSync pour éviter tout impact involontaire sur d'autres clients ActiveSync.
- **Fonctions Exchange étendues :** grâce à l'intégration directe avec Exchange ActiveSync, le connecteur pour Exchange ActiveSync permet à Citrix Endpoint Management d'effectuer un effacement Exchange ActiveSync sur un appareil mobile. Le connecteur pour Exchange ActiveSync permet également à Citrix Endpoint Management d'accéder aux informations sur les appareils Blackberry et d'effectuer d'autres opérations de contrôle.

Pour un diagramme du connecteur Citrix Endpoint Management pour Exchange ActiveSync dans un déploiement Citrix Endpoint Management, voir Architecture.

Arbre de décision pour la plateforme de messagerie

La figure suivante vous aide à distinguer les avantages et les inconvénients de l'utilisation de solutions de messagerie natives ou Citrix Secure Mail dans votre déploiement Citrix Endpoint Management. Chaque choix permet aux options et aux exigences Citrix Endpoint Management associées d'activer l'accès au serveur, au réseau et à la base de données. Les avantages et inconvénients incluent des détails sur les considérations concernant la sécurité, la stratégie et l'interface utilisateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Intégration de Citrix Endpoint Management

March 1, 2024

Cet article décrit les éléments à prendre en compte lors de la planification de l'intégration de Citrix Endpoint Management à votre réseau et à vos solutions. Par exemple, si vous utilisez déjà NetScaler Gateway pour Citrix Virtual Apps and Desktops :

- Souhaitez-vous utiliser l'instance existante de NetScaler Gateway ou une nouvelle instance dédiée ?
- Voulez-vous intégrer à Citrix Endpoint Management les applications HDX publiées avec StoreFront ?
- Avez-vous l'intention d'utiliser Citrix Files avec Citrix Endpoint Management ?
- Avez-vous une solution de contrôle d'accès réseau que vous souhaitez intégrer à Citrix Endpoint Management ?

NetScaler Gateway

NetScaler Gateway est requis pour Citrix Endpoint Management. NetScaler Gateway fournit un chemin micro VPN pour l'accès à toutes les ressources de l'entreprise et fournit une prise en charge de l'authentification forte à multi-facteurs.

Vous pouvez utiliser des instances de NetScaler Gateway existantes ou en configurer de nouvelles pour Citrix Endpoint Management. Les sections suivantes expliquent les avantages et les inconvénients de l'utilisation d'instances NetScaler Gateway dédiées existantes ou nouvelles.

NetScaler Gateway MPX partagé avec une VIP NetScaler Gateway créée pour Citrix Endpoint Management

Avantages :

- Utilise une instance NetScaler Gateway commune pour toutes les connexions distantes Citrix : Citrix Virtual Apps, VPN complet et VPN sans client.
- Utilise les configurations NetScaler Gateway existantes, telles que l'authentification par certificat et l'accès à des services tels que DNS, LDAP et NTP.
- Utilise une seule licence de plate-forme NetScaler Gateway.

Inconvénients :

- Il est plus difficile de planifier l'échelle du déploiement lorsque vous gérez deux cas d'utilisation différents sur le même NetScaler Gateway.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Parfois, vous avez besoin d'une version spécifique de NetScaler Gateway pour une utilisation spécifique de Citrix Virtual Apps. Cette même version peut présenter des problèmes connus pour Citrix Endpoint Management. Ou Citrix Endpoint Management peut présenter des problèmes connus pour la version NetScaler Gateway.
- Si une instance de NetScaler Gateway existe, vous ne pouvez pas exécuter l'assistant NetScaler for XenMobile une deuxième fois pour créer la configuration NetScaler Gateway pour Citrix Endpoint Management.
- Sauf lorsque des licences Platinum sont utilisées pour NetScaler Gateway 11.1 ou version ultérieure : les licences d'accès utilisateur installées sur NetScaler Gateway et requises pour la connectivité VPN sont regroupées. Comme ces licences sont disponibles pour tous les serveurs virtuels NetScaler Gateway, des services autres que Citrix Endpoint Management peuvent potentiellement les consommer.

Instance NetScaler Gateway VPX/MPX dédiée

Avantages :

Citrix vous recommande d'utiliser une instance dédiée de NetScaler Gateway.

- Plus facile à planifier en termes d'échelle et sépare le trafic Endpoint Management d'une instance NetScaler Gateway qui pourrait déjà être limitée en ressources.
- Évite les problèmes lorsque Citrix Endpoint Management et Citrix Virtual Apps nécessitent différentes versions du logiciel NetScaler Gateway. Il est généralement préférable d'utiliser la dernière version/build de NetScaler Gateway compatible pour Citrix Endpoint Management.
- Permet la configuration Citrix Endpoint Management de NetScaler Gateway via l'assistant NetScaler pour XenMobile intégré.
- Séparation virtuelle et physique des services.

Inconvénients :

- Nécessite l'installation de services supplémentaires sur NetScaler Gateway pour prendre en charge la configuration Citrix Endpoint Management.
- Nécessite une autre licence de plate-forme NetScaler Gateway. Licence pour chaque instance NetScaler Gateway pour NetScaler Gateway.

Pour plus d'informations sur les éléments à prendre en compte lors de l'intégration de NetScaler Gateway et Citrix ADC pour les modes de gestion Citrix Endpoint Management, consultez Intégration avec NetScaler Gateway et Citrix ADC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

StoreFront

Si vous disposez d'un environnement Citrix Virtual Apps and Desktops, vous pouvez intégrer des applications HDX avec Citrix Endpoint Management à l'aide de StoreFront. Lorsque vous intégrez des applications HDX avec Citrix Endpoint Management :

- Les applications sont disponibles pour les utilisateurs inscrits avec Citrix Endpoint Management.
- Les applications s'affichent dans le magasin d'applications avec d'autres applications mobiles.
- Citrix Endpoint Management utilise Citrix Receiver sur StoreFront.
- Lorsque l'application Citrix Workspace est installée sur un appareil, les applications HDX commencent à utiliser cette application.

StoreFront est limité à un site de services par instance. Supposons que vous ayez plusieurs magasins et que vous souhaitiez le séparer d'autres utilisations de production. Dans ce cas, Citrix vous recommande généralement d'envisager une nouvelle instance de StoreFront avec un nouveau site de services pour Citrix Endpoint Management.

Les points à prendre en compte sont les suivants :

- Existe-t-il des exigences d'authentification différentes pour StoreFront ? Le site de services StoreFront nécessite des informations d'identification Active Directory pour la connexion. Les clients utilisant uniquement l'authentification par certificat ne peuvent pas énumérer les applications via Citrix Endpoint Management en utilisant la même instance de NetScaler Gateway.
- Utiliser le même magasin ou en créer un nouveau ?
- Utiliser le même serveur StoreFront ou un serveur différent ?

Les sections suivantes indiquent les avantages et les inconvénients de l'utilisation d'instances StoreFront séparées ou combinées pour Citrix Workspace et pour les applications de productivité mobiles Citrix.

Intégrer votre instance StoreFront existante avec Citrix Endpoint Management

Avantages :

- Même magasin : aucune configuration supplémentaire de StoreFront n'est requise pour Citrix Endpoint Management, à condition que vous utilisiez le même accès par VIP NetScaler Gateway pour HDX. Supposons que vous choisissiez d'utiliser le même magasin et que vous souhaitiez diriger l'accès de Citrix Workspace vers une nouvelle VIP NetScaler Gateway. Dans ce cas, ajoutez la configuration NetScaler Gateway appropriée à StoreFront.
- Même serveur StoreFront : utilise l'installation et la configuration de StoreFront existantes.

Inconvénients :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Même magasin : toute reconfiguration de StoreFront pour gérer les charges de travail Citrix Virtual Apps and Desktops peut avoir un effet négatif sur Citrix Endpoint Management.
- Même serveur StoreFront : dans les environnements de grande taille, considérez la charge supplémentaire que représente l'utilisation de Citrix Receiver par Citrix Endpoint Management pour l'énumération et le démarrage des applications.

Utiliser une nouvelle instance StoreFront dédiée pour l'intégration à Citrix Endpoint Management

Avantages :

- Nouveau magasin : les modifications de configuration du magasin StoreFront pour Citrix Endpoint Management n'affectent pas les charges de travail Citrix Virtual Apps and Desktops existantes.
- Nouveau serveur StoreFront : les modifications de configuration du serveur n'affectent pas le flux de travail Citrix Virtual Apps and Desktops. De plus, la charge hors de l'utilisation de Citrix Receiver par Citrix Endpoint Management pour l'énumération et le lancement des applications n'affectent pas la capacité à monter en charge.

Inconvénients :

- Nouveau magasin : configuration du magasin StoreFront.
- Nouveau serveur StoreFront : requiert une nouvelle installation et une nouvelle configuration de StoreFront.

Pour plus d'informations, voir Citrix Virtual Apps and Desktops via le magasin d'applications.

ShareFile et Citrix Files

ShareFile vous permet d'échanger des documents facilement et en toute sécurité, d'envoyer des documents volumineux par courrier électronique et de gérer en toute sécurité les transferts de documents à des tiers. L'application Citrix Files permet aux utilisateurs d'accéder à toutes leurs données et de les synchroniser à partir de n'importe quel appareil. Avec Citrix Files, les utilisateurs peuvent partager des données en toute sécurité avec des personnes à l'intérieur et à l'extérieur de l'organisation.

Citrix Endpoint Management permet à Citrix Files de bénéficier des fonctionnalités suivantes :

- Authentification à connexion unique pour les utilisateurs de l'application Endpoint Management.
- Provisionnement de compte d'utilisateur basé sur Active Directory.
- Stratégies de contrôle d'accès complètes

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Les utilisateurs mobiles peuvent bénéficier de l'ensemble des fonctionnalités de compte Enterprise.

Vous pouvez également configurer Citrix Endpoint Management pour une intégration aux StorageZone Connector uniquement. Grâce aux connecteurs StorageZone, Citrix Files donne accès aux éléments suivants :

- Documents et dossiers
- Partages de fichiers réseau
- Dans les sites SharePoint : collections de sites et bibliothèques de documents.

Les partages de fichiers connectés peuvent inclure les mêmes lecteurs de base réseau que ceux utilisés dans les environnements Citrix Virtual Apps and Desktops. La console Citrix Endpoint Management permet de configurer l'intégration aux comptes Enterprise ou aux StorageZone Connector. Pour plus d'informations, consultez la section Citrix Files pour Citrix Endpoint Management.

Les sections suivantes indiquent les questions à poser lors de la prise de décision concernant la conception pour Citrix Files.

Intégration à Citrix Files ou uniquement aux connecteurs StorageZone

Questions à poser :

- Souhaitez-vous stocker des données dans des zones de stockage gérées par Citrix ?
- Voulez-vous fournir aux utilisateurs des fonctions de partage de fichiers et de synchronisation ?
- Voulez-vous permettre aux utilisateurs d'accéder aux fichiers sur le site Web Citrix Files ? Ou d'accéder à du contenu Office 365 et à des connecteurs Personal Cloud depuis des appareils mobiles ?

Décision de conception :

- Si la réponse à l'une de ces questions est « oui », intégrez un compte Enterprise.
- Une intégration aux connecteurs StorageZone uniquement offre aux utilisateurs iOS un accès mobile sécurisé aux référentiels de stockage locaux existants, tels que des sites SharePoint et des partages de fichiers réseau. Dans cette configuration, la configuration d'un sous-domaine Citrix Files, le provisioning d'utilisateurs pour Citrix Files ou l'hébergement de données Citrix Files ne sont pas nécessaires. L'utilisation de StorageZone Connector avec Citrix Endpoint Management est conforme aux restrictions de sécurité contre la fuite d'informations utilisateur en dehors du réseau d'entreprise.

Emplacement des serveurs StorageZones Controller

Questions à poser :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Avez-vous besoin d'un stockage sur site ou de fonctionnalités telles que des connecteurs StorageZone ?
- Si vous utilisez les fonctionnalités locales de Citrix Files, où se trouveront les StorageZones Controller sur le réseau ?

Décision de conception :

- Déterminez si vous souhaitez placer les serveurs StorageZones Controller dans le cloud Citrix Files, dans votre système de stockage local à locataire unique ou dans un stockage cloud tiers pris en charge.
- Les StorageZones Controller doivent disposer d'un accès à Internet pour communiquer avec le plan de contrôle Citrix Files. Vous pouvez vous connecter de plusieurs manières, y compris par accès direct ou par configurations NAT/PAT.

Connecteurs StorageZone

Questions à poser :

- Quels sont les chemins de partage CIFS ?
- Quelles sont les URL SharePoint ?

Décision de conception :

- Déterminez si les StorageZones Controller locaux doivent accéder à ces emplacements.
- En raison de la communication des StorageZone Connector avec des ressources internes telles que des référentiels de fichiers, des partages CIFS et SharePoint : Citrix recommande que les StorageZones Controller résident dans le réseau interne derrière les pare-feu DMZ et devant NetScaler Gateway.

Intégration de SAML à Citrix Endpoint Management

Questions à poser :

- L'authentification avec Active Directory est-elle requise pour Citrix Files ?
- La première utilisation de l'application Citrix Files pour Citrix Endpoint Management nécessite-t-elle une authentification unique ?
- Existe-t-il un fournisseur d'identité standard dans votre environnement actuel ?
- Combien de domaines sont requis pour utiliser SAML ?
- Existe-t-il plusieurs alias d'adresse e-mail pour les utilisateurs d'Active Directory ?
- Des migrations de domaine Active Directory sont-elles en cours ou prévues pour bientôt ?

Décision de conception :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Vous pouvez choisir d'utiliser SAML comme mécanisme d'authentification pour Citrix Files. Les options d'authentification sont les suivantes :

- Utiliser le serveur Citrix Endpoint Management en tant que fournisseur d'identité (IdP) pour SAML

  Cette option peut fournir une excellente expérience utilisateur et automatiser la création de compte Citrix Files, ainsi qu'activer les fonctionnalités SSO de l'application mobile.

  Le serveur Citrix Endpoint Management est adapté à ce processus : il ne nécessite pas la synchronisation d'Active Directory.

  Utilisez l'outil de gestion des utilisateurs Citrix Files pour provisionner des utilisateurs.

- Utiliser un fournisseur tiers pris en charge en tant que fournisseur d'identité pour SAML

  Si vous disposez déjà d'un fournisseur d'identité et pris en charge et que vous n'avez pas besoin de fonctionnalités d'authentification unique pour les applications mobiles, cette option peut vous convenir. Cette option nécessite également l'utilisation de l'outil de gestion des utilisateurs Citrix Files pour le provisionnement des comptes.

  L'utilisation de solutions d'identité tierces telles qu'ADFS peut également fournir des fonctionnalités d'authentification unique du côté client Windows. Veillez à évaluer les cas d'utilisation avant de choisir votre fournisseur d'identité SAML Citrix Files.

- Ou, pour répondre aux deux cas d'utilisation, consultez le guide de configuration de l'authentification unique ShareFile pour les fournisseurs d'identités doubles.

Applications mobiles

Questions à poser :

- Quelle application mobile Citrix Files envisagez-vous d'utiliser (public, MDM, MDX) ?

Décision de conception :

- Vous pouvez distribuer les applications de productivité mobiles Citrix à partir de l'App Store d'Apple et de Google Play Store. Avec cette distribution depuis des magasins publics, vous obtenez des applications encapsulées à partir de la page de téléchargements Citrix.
- Si vos exigences de sécurité sont faibles et que vous n'avez pas besoin de conteneurisation, l'application publique Citrix Files peut ne pas convenir.
- Pour plus d'informations, consultez les sections Applications et Citrix Files pour Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sécurité, stratégies et contrôle d'accès

Questions à poser :

- Quelles restrictions sont requises pour les utilisateurs de bureau, Web et mobiles ?
- Quels paramètres de contrôle d'accès standard souhaitez-vous pour les utilisateurs ?
- Quelle stratégie de rétention des fichiers comptez-vous utiliser ?

Décision de conception :

- Citrix Files vous permet de gérer les autorisations des employés. Pour plus d'informations, voir Autorisations des employés.
- Certains paramètres de sécurité des appareils Citrix Files et certaines stratégies MDX contrôlent les mêmes fonctionnalités. Dans ce cas, les stratégies Citrix Endpoint Management sont prioritaires, suivies des paramètres de sécurité des appareils Citrix Files. Exemples : si vous désactivez des applications externes dans Citrix Files, mais les activez dans Citrix Endpoint Management, les applications externes sont désactivées dans Citrix Files. Vous pouvez configurer les applications pour que Citrix Endpoint Management n'exige pas de code PIN/code secret, mais que l'application Citrix Files requière un code PIN/code secret.

Zones de stockage standard ou restreintes

Questions à poser :

- Avez-vous besoin de zones de stockage restreintes ?

Décision de conception :

- Une zone de stockage standard est conçue pour stocker les données non sensibles et permet aux employés de partager des données avec des personnes autres que des employés. Cette option prend en charge les workflows qui impliquent le partage de données en dehors de votre domaine.
- Une zone de stockage restreinte protège les données sensibles : seuls les utilisateurs de domaine authentifiés peuvent accéder aux données stockées dans la zone.

Contrôle d'accès

Les entreprises peuvent gérer les appareils mobiles à l'intérieur et à l'extérieur des réseaux. Les solutions de gestion de la mobilité d'entreprise telles que Citrix Endpoint Management sont excellentes pour fournir sécurité et contrôle pour les appareils mobiles, indépendamment de leur emplacement. Toutefois, en utilisant également une solution de contrôle d'accès réseau (NAC), vous pouvez ajouter

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

une qualité de service et un contrôle plus précis aux appareils internes de votre réseau. Cette combinaison vous permet d'étendre l'évaluation de la sécurité des appareils Citrix Endpoint Management via votre solution NAC. Votre solution NAC peut ensuite utiliser l'évaluation de sécurité Citrix Endpoint Management pour faciliter et gérer les décisions d'authentification.

Vous pouvez utiliser l'une de ces solutions pour appliquer les stratégies NAC :

- NetScaler Gateway
- ForeScout

Citrix ne garantit pas l'intégration à d'autres solutions NAC.

Les avantages d'une intégration de solution NAC avec Citrix Endpoint Management sont les suivants :

- Sécurité, conformité et contrôle améliorés pour tous les points de terminaison sur un réseau d'entreprise.
- Une solution NAC peut :
  - Détecter les appareils au moment où ils tentent de se connecter à votre réseau.
  - Interroger Citrix Endpoint Management sur les attributs de l'appareil.
  - Utiliser ces informations pour déterminer si ces appareils doivent être autorisés, bloqués, limités ou redirigés. Ces décisions dépendent des stratégies de sécurité que vous choisissez d'appliquer.
- Une solution NAC fournit aux administrateurs informatiques une vue des appareils non gérés et non conformes.

Vous trouverez une description des filtres de conformité NAC pris en charge par Citrix Endpoint Management et une vue d'ensemble de la configuration dans la section Contrôle d'accès réseau.

Intégration avec NetScaler Gateway et Citrix ADC

March 1, 2024

Lorsqu'il est intégré à Citrix Endpoint Management, NetScaler Gateway fournit aux appareils MAM un mécanisme d'authentification pour l'accès des appareils distants au réseau interne. Cette intégration permet aux applications de productivité mobiles Citrix de se connecter à des serveurs d'entreprise situés dans l'intranet via un micro VPN. Citrix Endpoint Management crée un micro VPN depuis les applications vers NetScaler Gateway sur l'appareil. NetScaler Gateway fournit un chemin micro VPN pour l'accès à toutes les ressources de l'entreprise et fournit une prise en charge de l'authentification forte à multi-facteurs.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Lorsqu'un utilisateur refuse l'inscription MDM, les appareils s'inscrivent à l'aide du nom de domaine complet NetScaler Gateway.

Citrix Cloud Operations gère l'équilibrage de charge Citrix ADC.

Décisions de conception

Les sections suivantes résument les nombreuses décisions de conception à prendre en compte lors de la planification d'une intégration de NetScaler Gateway avec Citrix Endpoint Management.

Certificats

Détails de la décision :

- Avez-vous besoin d'un niveau de sécurité plus élevé pour l'inscription et l'accès à l'environnement Citrix Endpoint Management ?
- Pourriez-vous considérez le protocole LDAP ?

Conseils de conception :

La configuration par défaut pour Citrix Endpoint Management est l'authentification par nom d'utilisateur et mot de passe. Pour ajouter une autre couche de sécurité pour l'inscription et l'accès à l' environnement Citrix Endpoint Management, vous pouvez utiliser l'authentification basée sur certificats. Vous pouvez utiliser des certificats avec LDAP pour l'authentification à deux facteurs, ce qui permet d'offrir un degré de sécurité supérieur sans avoir besoin d'un serveur RSA.

Si vous n'autorisez pas LDAP et utilisez des cartes à puce ou méthodes similaires, la configuration des certificats vous permet de représenter une carte à puce auprès de Citrix Endpoint Management. Les utilisateurs s'inscrivent alors à l'aide d'un code PIN unique généré par Citrix Endpoint Management. Une fois qu'un utilisateur a accès, Citrix Endpoint Management crée et déploie le certificat utilisé ultérieurement pour s'authentifier auprès de l'environnement Citrix Endpoint Management.

Citrix Endpoint Management prend en charge la liste de révocation de certificats (CRL) uniquement pour une autorité de certification tierce. Si vous disposez d'une autorité de certification Microsoft configurée, Citrix Endpoint Management utilise NetScaler Gateway pour gérer la révocation. Lorsque vous configurez l'authentification basée sur un certificat client, vous devez décider si vous avez besoin de configurer le paramètre Liste de révocation de certificats (CRL) NetScaler Gateway **Enable CRL Auto Refresh**. Cette étape garantit que l'utilisateur d'un appareil inscrit en mode MAM exclusif ne peut pas s'authentifier à l'aide d'un certificat existant sur l'appareil. Citrix Endpoint Management émet un nouveau certificat, car il n'interdit pas à un utilisateur de générer un certificat utilisateur si un certificat est révoqué. Ce paramètre renforce la sécurité des entités PKI lorsque la CRL vérifie la présence d'entités PKI expirées.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VIP NetScaler Gateway dédiés ou partagés

Détails de la décision :

- Utilisez-vous actuellement NetScaler Gateway pour Citrix Virtual Apps and Desktops ?
- Citrix Endpoint Management utilisera-t-il la même instance NetScaler Gateway que Citrix Virtual Apps and Desktops ?
- Quelles sont les exigences d'authentification pour les deux flux de trafic ?

Conseils de conception :

Lorsque votre environnement Citrix comprend Citrix Endpoint Management, Virtual Apps and Desktops, vous pouvez utiliser le même serveur virtuel NetScaler Gateway pour les deux. En raison de conflits de version et d'isolement d'environnement potentiels, une instance NetScaler Gateway dédiée est recommandée pour chaque environnement Citrix Endpoint Management.

Si vous utilisez l'authentification LDAP, Citrix Secure Hub peuvent s'authentifier auprès du même NetScaler Gateway sans problème. Si vous utilisez l'authentification par certificat, Citrix Endpoint Management envoie un certificat dans le conteneur MDX et Citrix Secure Hub utilise le certificat pour s'authentifier auprès de NetScaler Gateway.

Vous pouvez envisager cette solution, ce qui vous permet d'utiliser le même nom de domaine complet pour deux VIP NetScaler Gateway. Vous pouvez créer deux adresses IP virtuelles (VIP) NetScaler Gateway avec la même adresse IP. Cependant, celle de Citrix Secure Hub utilise le port 443 standard et celle de Citrix Virtual Apps and Desktops (qui déploie l'application Citrix Workspace) utilise le port 444. Ensuite, un nom de domaine complet résout la même adresse IP. Si vous utilisez cette solution, vous devrez peut-être configurer StoreFront pour renvoyer un fichier ICA pour le port 444, au lieu du port 443 par défaut. Avec cette solution, les utilisateurs n'ont pas besoin d'entrer un numéro de port.

Délais d'expiration NetScaler Gateway

Détails de la décision :

- Comment voulez-vous configurer les délais d'expiration NetScaler Gateway pour le trafic Citrix Endpoint Management ?

Conseils de conception :

NetScaler Gateway inclut les paramètres Délai d'expiration de session et Délai d'expiration forcé. Pour de plus amples informations, consultez la section Configurations recommandées. Gardez à l'esprit qu'il existe différentes valeurs de délai d'expiration pour les services d'arrière-plan, NetScaler Gateway et pour accéder aux applications en mode hors connexion.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Inscription du nom de domaine complet

> **Important :**
>
> Un changement de nom de domaine complet d'inscription nécessitera une nouvelle base de données SQL Server et une nouvelle build de Citrix Endpoint Management Server.

Trafic de Citrix Secure Web

Détails de la décision :

- Voulez-vous restreindre Citrix Secure Web à la navigation Web interne uniquement ?
- Voulez-vous activer Citrix Secure Web pour la navigation Web interne et externe ?

Conseils de conception :

Si vous envisagez d'utiliser Citrix Secure Web uniquement pour la navigation Web interne, la configuration de NetScaler Gateway est simple. Toutefois, si Citrix Secure Web ne parvient pas à atteindre tous les sites internes par défaut, vous devrez peut-être configurer des pare-feu et des serveurs proxy.

Si vous envisagez d'utiliser Citrix Secure Web pour la navigation interne et externe, vous devez activer l'adresse IP de sous-réseau pour avoir un accès Internet sortant. Les services informatiques considèrent généralement les appareils inscrits (à l'aide du conteneur MDX) comme une extension du réseau d'entreprise. Ainsi, ils souhaitent généralement que les connexions Citrix Secure Web reviennent à NetScaler Gateway, passent par un serveur proxy, puis sortent vers l'Internet. Par défaut, l'accès à Citrix Secure Web est tunnélisé vers le réseau interne. En effet, Citrix Secure Web utilise un tunnel VPN par application vers le réseau interne pour tous les accès réseau et NetScaler Gateway utilise les paramètres de split tunneling.

Pour une description des connexions Citrix Secure Web, consultez la section Configuration des connexions utilisateur.

Notifications push pour Citrix Secure Mail

Détails de la décision :

- Voulez-vous utiliser des notifications push ?

Conseils sur la conception pour iOS :

Si votre configuration NetScaler Gateway comprend une STA (Secure Ticket Authority) et que le split tunneling est désactivé, NetScaler Gateway doit autoriser le trafic en provenance de Citrix Secure Mail vers les URL du service d'écoute Citrix. Ces URL sont spécifiées dans les notifications push pour Citrix Secure Mail pour iOS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Conseil sur la conception pour Android :

Utilisez Firebase Cloud Messaging (FCM) pour contrôler comment et quand les appareils Android doivent se connecter à Citrix Endpoint Management. Avec la configuration de FCM, toute action de sécurité ou commande de déploiement déclenche une notification push à Citrix Secure Hub afin d'inviter l'utilisateur à se reconnecter à Citrix Endpoint Management Server.

HDX STA

Détails de la décision :

- Quelles STA utiliser si vous intégrez l'accès aux applications HDX ?

Conseils de conception :

Les STA HDX doivent correspondre aux STA dans StoreFront et doivent être valides pour le site Virtual Apps and Desktops.

Citrix Files et ShareFile

Détails de la décision :

- Utiliserez-vous un StorageZones Controller dans l'environnement ?
- Quelle URL VIP Citrix Files voulez-vous utiliser ?

Conseils de conception :

Si vous souhaitez inclure un StorageZones Controller dans votre environnement, assurez-vous de configurer correctement les éléments suivants :

- Le VIP de commutation de contenu Citrix Files (utilisé par le plan de contrôle Citrix Files pour communiquer avec les serveurs StorageZones Controller)
- Les VIP d'équilibrage de charge Citrix Files
- Toutes les stratégies et profils requis

Pour plus d'informations, veuillez consulter la documentation StorageZones Controller.

Fournisseur d'identité SAML

Détail de la décision :

- Si SAML est requis pour Citrix Files, voulez-vous utiliser Citrix Endpoint Management comme fournisseur d'identité SAML ?

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Conseils de conception :

La méthode recommandée est d'intégrer Citrix Files à Citrix Endpoint Management, une approche plus simple que la configuration de la fédération SAML. Citrix Endpoint Management permet à Citrix Files de bénéficier des fonctionnalités suivantes :

- Authentification unique (SSO) des utilisateurs d'applications de productivité mobiles Citrix
- Provisioning des comptes utilisateur basé sur Active Directory
- Stratégies de contrôle d'accès complètes

La console Citrix Endpoint Management vous permet de configurer Citrix Files et de contrôler les niveaux de service et la consommation de licences.

Il existe deux types de clients Citrix Files : clients Citrix Files pour Citrix Endpoint Management (également appelés clients Citrix Files encapsulés) et clients mobiles Citrix Files (également appelés clients Citrix Files non encapsulés). Pour comprendre les différences, consultez la section Différences entre les clients Citrix Files pour Citrix Endpoint Management et les clients mobiles Citrix Files.

Vous pouvez configurer Citrix Endpoint Management et Citrix Files pour que SAML fournisse un accès SSO aux composants suivants :

- Applications Citrix Files pour lesquelles le SDK MAM est activé ou qui sont encapsulées à l'aide de MDX Toolkit
- Clients Citrix Files non encapsulés, tels que le site Web, Outlook Plug-in ou les clients de synchronisation

Si vous souhaitez utiliser Citrix Endpoint Management comme fournisseur d'identité SAML pour Citrix Files, assurez-vous que les configurations appropriées sont en place. Pour plus d'informations, consultez la section SAML pour l'authentification unique avec Citrix Files.

Connexions directes ShareConnect

Détail de la décision :

- Les utilisateurs accèderont-ils à un ordinateur hôte à partir d'un ordinateur ou d'un appareil mobile exécutant ShareConnect à l'aide de connexions directes ?

Conseils de conception :

ShareConnect permet aux utilisateurs de se connecter à leurs ordinateurs en toute sécurité au travers d'iPads, de tablettes et de téléphones Android pour accéder à leurs fichiers et applications. Pour les connexions directes, Citrix Endpoint Management utilise NetScaler Gateway pour sécuriser l'accès aux ressources en dehors du réseau local. Pour plus d'informations sur la configuration, consultez la section ShareConnect.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nom de domaine complet d'inscription pour chaque mode de gestion

Mode de gestion	Inscription du nom de domaine complet
MDM+MAM avec inscription MDM obligatoire	Nom de domaine complet de Citrix Endpoint Management Server
MDM+MAM avec inscription MDM facultative	Nom de domaine complet de Citrix Endpoint Management Server ou nom de domaine complet NetScaler Gateway
MAM exclusif	Nom de domaine complet de Citrix Endpoint Management Server
Mode MAM uniquement (ancien mode)	Nom de domaine complet de NetScaler Gateway

Récapitulatif du déploiement

Si vous disposez de plusieurs instances Citrix Endpoint Management, telles que les environnements de test, de développement et de production, vous devez configurer manuellement NetScaler Gateway pour les environnements supplémentaires. Lorsque vous disposez d'un environnement de travail, prenez note des paramètres avant de tenter de configurer manuellement NetScaler Gateway pour Citrix Endpoint Management.

Une décision clé consiste à savoir si utiliser HTTPS ou HTTP pour la communication avec Citrix Endpoint Management Server. HTTPS fournit une communication principale sécurisée car le trafic entre NetScaler Gateway et Citrix Endpoint Management est crypté. Le recryptage impacte les performances du serveur Citrix Endpoint Management. HTTP offre de meilleures performances pour le serveur Citrix Endpoint Management. Le trafic entre NetScaler Gateway et Citrix Endpoint Management n'est pas crypté. Les tableaux suivants répertorient les exigences de port HTTP et HTTPS pour NetScaler Gateway et Citrix Endpoint Management.

HTTPS

Citrix recommande généralement le mode Pont SSL pour les configurations de serveur virtuel NetScaler Gateway MDM. Pour utiliser le mode Déchargement SSL de NetScaler Gateway avec les serveurs virtuels MDM, Citrix Endpoint Management prend en charge uniquement le port 80 en tant que service principal.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Mode de gestion	Méthode d'équilibrage de charge NetScaler Gateway	Ré-cryptage SSL	Port de Citrix Endpoint Management Server
MAM	Déchargement SSL	Activé	8443
MDM+MAM	MDM : Pont SSL	S/O	443, 8443
MDM+MAM	MAM : Déchargement SSL	Activé	8443

HTTP

Mode de gestion	Méthode d'équilibrage de charge NetScaler Gateway	Ré-cryptage SSL	Port de Citrix Endpoint Management Server
MAM	Déchargement SSL	Activé	8443
MDM+MAM	MDM : Déchargement SSL	Non pris en charge	80
MDM+MAM	MAM : Déchargement SSL	Activé	8443

Pour des diagrammes de NetScaler Gateway dans des déploiements Citrix Endpoint Management, voir Architecture.

Considérations SSO et proxy pour les applications MDX

March 1, 2024

L'intégration de Citrix Endpoint Management à NetScaler Gateway vous permet de fournir aux utilisateurs une authentification unique (SSO) à toutes les ressources HTTP / HTTPS principales. En fonction de vos exigences en matière d'authentification SSO, configurez les connexions utilisateur pour qu'une application MDX utilise Secure Browse (Tunnel - SSO Web), qui est un type de VPN sans client.

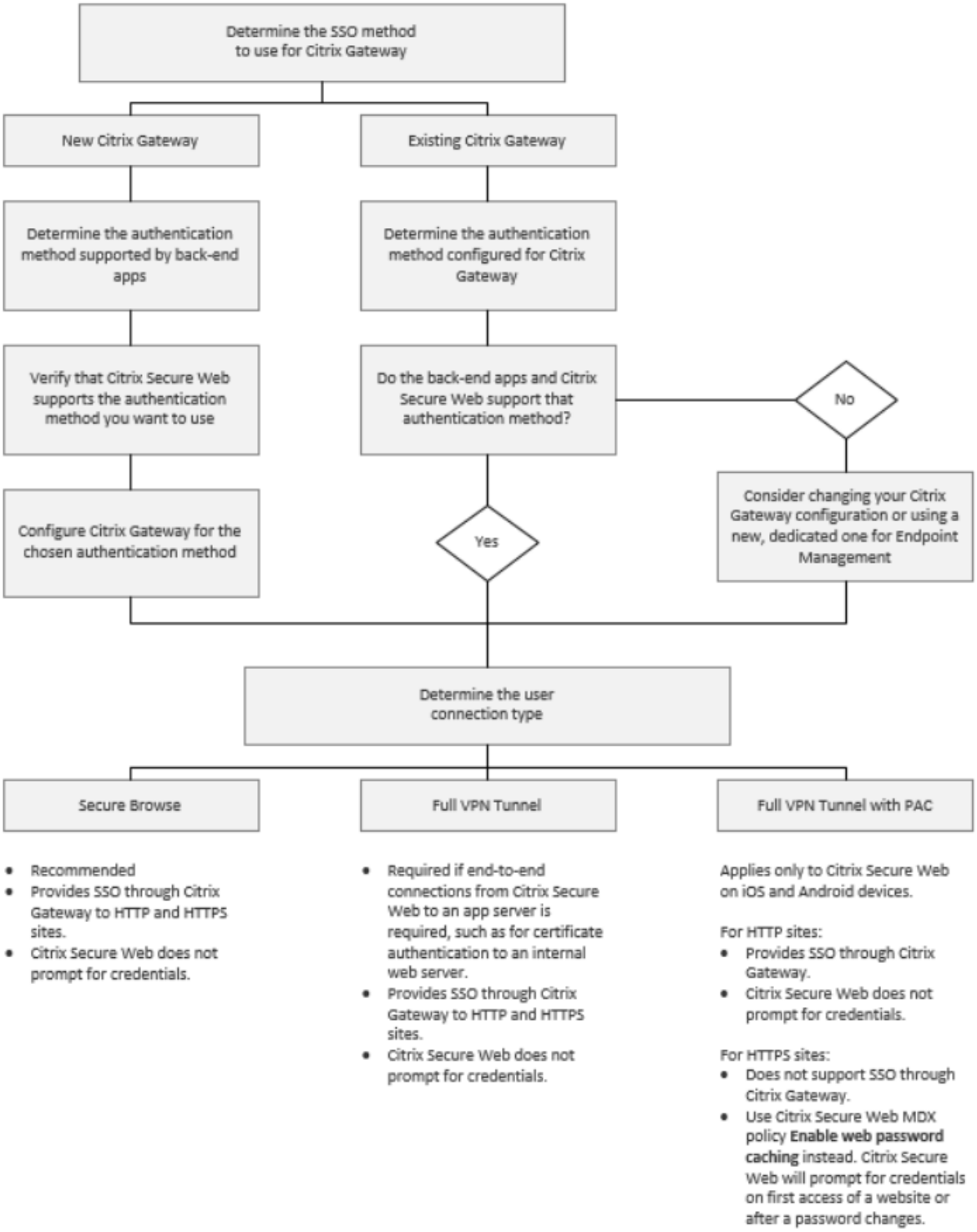
> **Important :**
>
> Citrix a mis fin à la prise en charge d'un tunnel VPN complet et d'un fichier PAC (Proxy Automatic Configuration) avec un déploiement de tunnel VPN complet pour les appareils iOS. Pour plus d'informations, consultez Fin de prise en charge.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si NetScaler Gateway n'est pas le meilleur moyen de fournir une authentification unique dans votre environnement, vous pouvez configurer une application MDX avec une mise en cache de mot de passe locale basée sur une stratégie. Cet article explore les différentes options SSO et proxy, en mettant l'accent sur Citrix Secure Web. Les concepts s'appliquent à d'autres applications MDX.

L'organigramme suivant résume le flux décisionnel pour les connexions SSO et utilisateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Méthodes d'authentification NetScaler Gateway

Cette section fournit des informations générales sur les méthodes d'authentification prises en charge par NetScaler Gateway.

Authentification SAML

Lorsque vous configurez NetScaler Gatewaypour le langage SAML (Assertion Marking Language), les utilisateurs peuvent se connecter aux applications Web prenant en charge le protocole SAML pour l'authentification unique. NetScaler Gateway prend en charge l'authentification unique de fournisseur d'identité pour les applications Web SAML.

Configuration requise :

- Configurez l'authentification unique SAML dans le profil NetScaler Gateway Traffic.
- Configurez le fournisseur d'identité SAML pour le service demandé.

Authentification NTLM

Si l'authentification unique pour les applications Web est activée dans le profil de session, NetScaler Gateway effectue automatiquement l'authentification NTLM.

Configuration requise :

- Activez l'authentification unique dans le profil de trafic ou de session NetScaler Gateway.

Emprunt d'identité Kerberos

Citrix Endpoint Management prend en charge Kerberos pour Citrix Secure Web uniquement. Lorsque vous configurez NetScaler Gateway pour Kerberos SSO, NetScaler Gaterway utilise l'emprunt d'identité lorsqu'un mot de passe utilisateur est disponible pour NetScaler Gateway. L'emprunt d'identité signifie que NetScaler Gateway utilise des informations d'identification utilisateur pour obtenir le ticket requis pour accéder aux services, tels que Citrix Secure Web.

Configuration requise :

- Configurez la stratégie de session NetScaler Gateway `Worx` pour lui permettre d'identifier le domaine Kerberos à partir de votre connexion.
- Configurez un compte Kerberos Constrained Delegation (KCD) sur NetScaler Gateway. Configurez ce compte sans mot de passe et associez-le à une stratégie de trafic sur votre passerelle Citrix Endpoint Management.
- Pour plus de détails sur la configuration, consultez le blog Citrix : WorxWeb and Kerberos Impersonation SSO.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Délégation Kerberos contrainte

Citrix Endpoint Management prend en charge Kerberos pour Citrix Secure Web uniquement. Lorsque vous configurez NetScaler Gateway pour Kerberos SSO, NetScaler utilise la délégation contrainte lorsqu'un mot de passe utilisateur n'est pas disponible pour NetScaler Gateway.

Avec une délégation contrainte, NetScaler Gateway utilise un compte d'administrateur spécifié pour obtenir des tickets au nom des utilisateurs et des services.

Configuration requise :

- Configurez un compte KCD dans Active Directory avec les autorisations requises et un compte KDC sur NetScaler Gateway.
- Activez l'authentification unique dans le profil de trafic NetScaler Gateway.
- Configurez le site Web principal pour l'authentification Kerberos.

Authentification par remplissage de formulaire

Lorsque vous configurez NetScaler Gateway pour l'authentification par remplissage de formulaire, les utilisateurs peuvent se connecter une seule fois pour accéder à toutes les applications protégées de votre réseau. Cette méthode d'authentification s'applique aux applications qui utilisent le mode Tunnel - SSO Web.

Configuration requise :

- Configurez l'authentification unique par remplissage de formulaire dans le profil de trafic NetScaler Gateway.

Authentification HTTP Digest

Si vous activez l'authentification unique pour les applications Web dans le profil de session, NetScaler Gateway effectue automatiquement l'authentification HTTP Digest. Cette méthode d'authentification s'applique aux applications qui utilisent le mode Tunnel - SSO Web.

Configuration requise :

- Activez l'authentification unique dans le profil de trafic ou de session NetScaler Gateway.

Authentification HTTP de base

Si vous activez l'authentification unique pour les applications Web dans le profil de session, NetScaler Gateway effectue automatiquement l'authentification HTTP de base. Cette méthode d'authentification s'applique aux applications qui utilisent le mode Tunnel - SSO Web.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration requise :

- Activez l'authentification unique dans le profil de trafic ou de session NetScaler Gateway.

Tunnel sécurisé–SSO Web

Cette section décrit les types de connexion utilisateur **Tunnel - SSO Web** pour Citrix Secure Web.

Les connexions qui sont tunnélisées sur le réseau interne peuvent utiliser une variante d'un VPN sans client, appelé Tunnel - SSO Web. Tunnel - SSO Web est la configuration par défaut spécifiée pour la stratégie **Mode VPN préféré** de Citrix Secure Web. Citrix recommande Tunnel - SSO Web pour les connexions qui nécessitent l'authentification unique (SSO).

En mode Tunnel - SSO Web, NetScaler Gateway divise la session HTTPS en deux parties :

- Du client à NetScaler Gateway
- De NetScaler Gateway au serveur de ressources principal

De cette manière, NetScaler Gateway a une visibilité complète sur toutes les transactions entre le client et le serveur, ce qui lui permet de fournir une authentification unique.

Vous pouvez également configurer des serveurs proxy pour Citrix Secure Web lorsque vous utilisez le mode Tunnel - SSO Web. Pour plus d'informations, consultez le blog Citrix Endpoint Management WorxWeb Traffic Through Proxy Server in Secure Browse Mode.

> **Remarque :**
>
> Citrix a annoncé la fin de la prise en charge du tunnel VPN complet avec PAC. Voir Fin de prise en charge.

Citrix Endpoint Management prend en charge l'authentification proxy fournie par NetScaler Gateway. 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. Citrix Secure Web analyse les règles du fichier PAC et envoie les informations sur le serveur proxy à NetScaler Gateway. NetScaler Gateway ignore le fichier PAC ou le serveur proxy.

Pour l'authentification aux sites Web HTTPS : la stratégie MDX de Citrix Secure Web **Activer la mise en cache du mot de passe Web** permet à Citrix Secure Web de s'authentifier et de fournir l'authentification unique (SSO) au serveur proxy via MDX.

Split tunneling de NetScaler Gateway

Lors de la planification de votre configuration SSO et proxy, vous devez également décider si vous souhaitez utiliser la fonction split tunneling de NetScaler Gateway. Citrix vous recommande d'utiliser

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

le split tunneling de NetScaler Gateway uniquement si nécessaire. Cette section fournit un aperçu général de la manière dont le split tunneling fonctionne : NetScaler Gateway détermine le chemin du trafic en fonction de sa table de routage. Lorsque le split tunneling de NetScaler Gateway est activé, Citrix Secure Hub distingue le trafic réseau interne (protégé) du trafic Internet. Citrix Secure Hub procède en fonction du suffixe DNS et des applications intranet. Citrix Secure Hub tunnellise uniquement le trafic réseau interne via le tunnel VPN. Lorsque le split tunneling de NetScaler Gateway est désactivé, tout le trafic passe par le tunnel VPN.

Si vous préférez surveiller l'ensemble du trafic pour des raisons de sécurité, désactivez le split tunneling de NetScaler Gateway. Dans ce cas, tout le trafic passe par le tunnel VPN.

NetScaler Gateway dispose également d'un mode de split tunneling inverse à micro VPN. Cette configuration prend en charge une liste d'exclusion d'adresses IP qui ne sont pas tunnellisées sur NetScaler Gateway. Ces adresses sont envoyées en utilisant la connexion Internet de l'appareil. Pour plus d'informations sur le split tunneling inverse, veuillez consulter la documentation relative à NetScaler Gateway.

Citrix Endpoint Management inclut une **liste d'exclusion de split tunneling inverse**. Pour empêcher que certains sites Web soient envoyés par un tunnel via NetScaler Gateway : ajoutez une liste séparée par des virgules des noms de domaine complet (FQDN) ou des suffixes DNS qui se connectent à l'aide du réseau LAN. Cette stratégie s'applique uniquement au mode Tunnel - SSO Web avec NetScaler Gateway configuré pour le split tunneling inverse.

Authentification

March 1, 2024

Dans un déploiement Citrix Endpoint Management, plusieurs considérations entrent en jeu lorsque vous choisissez la manière de configurer l'authentification. Cette section décrit les différents facteurs qui affectent l'authentification :

- Principales stratégies MDX, propriétés du client Citrix Endpoint Management et paramètres NetScaler Gateway impliqués dans l'authentification.
- Interaction des stratégies, des propriétés client et des paramètres
- Compromis de chaque choix

Cet article contient également trois exemples de configurations recommandées pour augmenter le niveau de sécurité.

D'une manière générale, une sécurité renforcée entraîne une expérience utilisateur moins optimale, car les utilisateurs doivent s'authentifier plus souvent. La façon dont vous conciliez ces préoccupa-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tions dépend des besoins et des priorités de votre organisation. Examinez les trois configurations recommandées pour comprendre l'interaction des différentes options d'authentification.

Modes d'authentification

Authentification en ligne : permet aux utilisateurs d'accéder au réseau Citrix Endpoint Management. Nécessite une connexion Internet.

Authentification hors connexion : se produit sur l'appareil. Les utilisateurs déverrouillent un coffre sécurisé et disposent d'un accès hors connexion à des éléments, tels que le courrier téléchargé, les sites Web mis en cache et les notes.

Méthodes d'authentification

Facteur unique **LDAP :** vous pouvez configurer une connexion dans Citrix Endpoint Management à un ou plusieurs annuaires qui sont compatibles avec le protocole LDAP (Lightweight Directory Access Protocol). Cette méthode est couramment utilisée pour fournir une authentification unique (SSO) aux environnements d'entreprise. Vous pouvez opter pour le code PIN Citrix avec la mise en cache de mot de passe Active Directory pour améliorer l'expérience utilisateur avec LDAP. En même temps, vous pouvez fournir la sécurité avec des mots de passe complexes lors de l'inscription, de l'expiration du mot de passe et du verrouillage du compte.

Pour de plus amples informations, consultez la section Domaine ou domaine + authentification par jeton de sécurité.

Certificat client : Citrix Endpoint Management peut s'intégrer aux autorités de certification standard pour utiliser les certificats comme seule méthode d'authentification en ligne. Citrix Endpoint Management fournit ce certificat après l'inscription de l'utilisateur, ce qui nécessite un mot de passe à usage unique, une URL d'invitation ou des informations d'identification LDAP. Lorsque vous utilisez un certificat client comme méthode d'authentification principale, un code PIN Citrix est requis dans les environnements de certificat client uniquement pour sécuriser le certificat sur l'appareil.

Citrix Endpoint Management prend en charge la liste de révocation de certificats (CRL) uniquement pour une autorité de certification tierce. Si vous disposez d'une autorité de certification Microsoft configurée, Citrix Endpoint Management utilise NetScaler Gateway pour gérer la révocation. Lorsque vous configurez l'authentification basée sur un certificat client, vous devez décider si vous avez besoin de configurer le paramètre Liste de révocation de certificats (CRL) NetScaler Gateway, Enable CRL Auto Refresh. Cette étape garantit qu'un appareil inscrit en mode MAM exclusif ne peut pas s'authentifier à l'aide d'un certificat existant sur l'appareil. Citrix Endpoint Management émet un nouveau certificat, car il n'interdit pas à un utilisateur de générer un certificat utilisateur si un certificat est révoqué. Ce paramètre renforce la sécurité des entités PKI lorsque la CRL vérifie la présence d'entités PKI expirées.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour afficher un diagramme indiquant le déploiement requis pour l'authentification par certificat ou pour l'utilisation de votre autorité de certification d'entreprise pour émettre des certificats d'appareil, consultez l'article Architecture.

Authentification à deux facteurs LDAP + Certificat client : cette configuration est la meilleure combinaison de sécurité et d'expérience utilisateur pour Citrix Endpoint Management. L'utilisation de l'authentification par certificat client et LDAP présente les avantages suivants :

- Offre les meilleures possibilités d'authentification unique associées à la sécurité fournie par l'authentification à deux facteurs sur NetScaler Gateway.
- Assure la sécurité à l'aide d'informations déjà connues des utilisateurs (leurs mots de passe Active Directory) et de composants dont ils disposent déjà (les certificats clients sur leurs appareils).

Citrix Secure Mail peut offrir et configurer automatiquement une première expérience d'utilisation des plus simples grâce à l'authentification du certificat client. Cette fonctionnalité nécessite un environnement de serveur d'accès client Exchange correctement configuré.

Pour une utilisabilité optimale, vous pouvez combiner l'authentification par certificat client et LDAP avec le code PIN Citrix et la mise en cache du mot de passe Active Directory.

LDAP + jeton : il s'agit de la configuration classique des informations d'identification LDAP plus un mot de passe à usage unique, via le protocole RADIUS. Pour une utilisabilité optimale, vous pouvez combiner cette option avec le code PIN Citrix et la mise en cache du mot de passe Active Directory.

Stratégies, paramètres et propriétés client clés liés à l'authentification

Les stratégies, paramètres et propriétés client suivants entrent en jeu avec les trois configurations recommandées suivantes :

Stratégies MDX

Code secret d'application : si cette option est définie sur **Activé**, un code PIN ou un code secret Citrix est requis pour déverrouiller l'application lorsqu'elle démarre ou reprend après une période d'inactivité. La valeur par défaut est **Activé**.

Pour configurer le délai d'inactivité pour toutes les applications, définissez la valeur INACTIVITY_TIMER en minutes dans **Propriétés du client** sur l'onglet **Paramètres**. La valeur par défaut est 15 minutes. Pour désactiver le délai d'inactivité, de façon à ce qu'une invite de saisie du code PIN ou du code secret invite s'affiche uniquement lorsque l'application démarre, définissez la valeur sur zéro.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Session micro VPN requise : si cette option est définie sur **Activé**, l'utilisateur doit disposer d'une connexion au réseau d'entreprise et d'une session active pour accéder à l'application sur l'appareil. Si cette option est définie sur **Désactivé**, aucune session active n'est requise pour accéder à l'application sur l'appareil. La valeur par défaut est **Off**.

Période hors connexion maximale (heures) : définit la durée maximale pendant laquelle une application peut s'exécuter sans avoir à reconfirmer les identifiants liés à l'application ni à actualiser les stratégies de Citrix Endpoint Management. Lorsque les conditions suivantes sont remplies, une application iOS récupère de nouvelles stratégies pour les applications MDX depuis Citrix Endpoint Management sans interrompre le service pour les utilisateurs :

- Vous définissez la période maximale hors connexion et
- Citrix Secure Hub pour iOS dispose d'un jeton NetScaler Gateway valide.

Si Citrix Secure Hub ne dispose pas d'un jeton NetScaler Gateway valide, les utilisateurs doivent s'authentifier via Citrix Secure Hub avant que les stratégies applicatives ne puissent être mises à jour. Le jeton NetScaler Gateway peut devenir non valide en cas d'absence d'activité dans la session NetScaler Gateway ou de l'application d'une stratégie d'expiration de session. Lorsque les utilisateurs se connectent de nouveau à Citrix Secure Hub, ils peuvent continuer à exécuter l'application.

Les utilisateurs sont invités à se connecter 30, 15 et 5 minutes avant l'expiration de ce délai. Après expiration, l'application est bloquée jusqu'à ce que les utilisateurs se connectent. La valeur par défaut est **72 heures (3 jours)**. La période minimale est 1 heure.

> **Remarque :**
>
> N'oubliez pas que dans un scénario dans lequel les utilisateurs voyagent souvent et peuvent utiliser l'itinérance internationale, la valeur par défaut de 72 heures (3 jours) peut être trop courte.

Expiration du ticket des services d'arrière-plan : durée pendant laquelle un ticket de service réseau d'arrière-plan reste valide. Lorsque Citrix Secure Mail se connecte via NetScaler Gateway à un serveur Exchange Server exécutant ActiveSync, Citrix Endpoint Management émet un jeton. Citrix Secure Mail utilise ce jeton pour se connecter au serveur Exchange Server interne. Ce paramètre de propriété détermine la durée pendant laquelle Citrix Secure Mail peut utiliser le jeton sans requérir de nouveau jeton pour l'authentification et la connexion au serveur Exchange. Lorsque la limite de temps expire, les utilisateurs doivent ouvrir une session à nouveau pour générer un nouveau jeton. La valeur par défaut est **168 heures (7 jours)**. Lorsque ce délai expire, les notifications par e-mail s'arrêtent.

Période de grâce requise pour les sessions micro VPN : détermine le nombre de minutes pendant lesquelles un utilisateur peut utiliser l'application hors ligne jusqu'à ce que la session en ligne soit validée. La valeur par défaut est **0** (pas de période de grâce).

Pour plus d'informations sur les stratégies d'authentification, consultez

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si vous utilisez le SDK MAM : Présentation du SDK MAM
- Si vous utilisez MDX Toolkit, consultez la section Stratégies MDX Citrix Endpoint Management pour iOS et Stratégies MDX Citrix Endpoint Management pour Android

Propriétés du client Citrix Endpoint Management

> **Remarque :**
>
> Les propriétés du client sont des paramètres globaux qui s'appliquent à tous les appareils qui se connectent à Citrix Endpoint Management.

Code PIN Citrix : pour une expérience de connexion simple, vous pouvez choisir d'activer le code PIN Citrix. Avec le code PIN, les utilisateurs n'ont pas besoin d'entrer d'autres informations d'identification de manière répétée, telles que leurs noms d'utilisateur et mots de passe Active Directory. Vous pouvez configurer le code PIN Citrix en tant qu'authentification hors connexion autonome uniquement, ou associer le code PIN avec la mise en cache du mot de passe Active Directory pour simplifier l'authentification pour une utilisabilité optimale. Vous pouvez configurer le code PIN Citrix dans **Paramètres > Client > Propriétés du client** dans la console Citrix Endpoint Management.

Vous trouverez ci-dessous un récapitulatif des propriétés les plus importantes. Pour de plus amples informations, consultez la section Propriétés du client.

ENABLE_PASSCODE_AUTH

Nom d'affichage : Enable Citrix PIN Authentication (Activer l'authentification du code PIN Citrix)

Cette clé permet d'activer la fonctionnalité de code PIN Citrix. Avec le code PIN ou code secret Citrix, les utilisateurs sont invités à définir un code PIN à utiliser à la place de leur mot de passe Active Directory. Activez ce paramètre si **ENABLE_PASSWORD_CACHING** est activé ou si Citrix Endpoint Management utilise l'authentification par certificat.

Valeurs possibles : true ou **false**

Valeur par défaut : false

ENABLE_PASSWORD_CACHING

Nom d'affichage : Enable User Password Caching (Activer la mise en cache du mot de passe de l'utilisateur)

Cette clé vous permet d'autoriser la mise en cache locale du mot de passe Active Directory de l'utilisateur sur l'appareil mobile. Lorsque vous définissez cette clé sur true, les utilisateurs sont invités à créer un code PIN ou code secret Citrix. La clé **ENABLE_PASSCODE_AUTH** doit être définie sur true lorsque vous définissez cette clé sur **true**.

Valeurs possibles : true ou **false**

Valeur par défaut : false

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

PASSCODE_STRENGTH

Nom d'affichage : PIN Strength Requirement (Exigences en matière de sûreté du code PIN)

Cette clé définit le niveau de sécurité du code PIN ou du code secret Citrix. Lorsque vous modifiez ce paramètre, les utilisateurs sont invités à définir un nouveau code PIN ou code secret Citrix la prochaine fois qu'ils sont invités à s'authentifier.

Valeurs possibles : Low, **Medium** ou **Strong**

Valeur par défaut : Medium

INACTIVITY_TIMER

Nom d'affichage : Inactivity Timer (Délai d'inactivité)

Cette clé définit la durée en minutes pendant laquelle les utilisateurs peuvent laisser leurs appareils inactifs et accéder à une application sans être invité à entrer un code PIN ou code secret Citrix. Pour activer ce paramètre pour une application MDX, vous devez définir le paramètre **Code secret d'application** sur **Activé**. Si le paramètre **Code secret d'application** est défini sur **Désactivé**, les utilisateurs sont redirigés vers Citrix Secure Hub pour effectuer une authentification complète. Lorsque vous modifiez ce paramètre, la valeur prend effet la prochaine fois que les utilisateurs sont invités à s' authentifier. La valeur par défaut est 15 minutes.

ENABLE_TOUCH_ID_AUTH

Nom d'affichage : Enable Touch ID Authentication (Activer l'authentification TouchID)

Permet l'utilisation du lecteur d'empreintes digitales (dans iOS uniquement) pour l'authentification hors connexion. L'authentification en ligne nécessite toujours la méthode d'authentification principale.

ENCRYPT_SECRETS_USING_PASSCODE

Nom d'affichage : Encrypt secrets using Passcode (Chiffrer les secrets à l'aide d'un code secret)

Cette clé permet de stocker les données sensibles sur l'appareil mobile dans un coffre sécurisé plutôt que dans un magasin natif basé sur la plate-forme, tel que le trousseau iOS Cette clé de configuration permet un cryptage renforcé des artefacts clés, mais ajoute également une entropie utilisateur (un code PIN généré de manière aléatoire connu uniquement de l'utilisateur).

Valeurs possibles : true ou **false**

Valeur par défaut : false

Paramètres de NetScaler Gateway

Session time-out : si vous activez ce paramètre, NetScaler Gateway déconnecte la session si NetScaler Gateway ne détecte aucune activité réseau pour l'intervalle spécifié. Ce paramètre est

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

appliqué aux utilisateurs qui se connectent avec le plug-in NetScaler Gateway, Citrix Secure Hub ou via un navigateur Web. La valeur par défaut est **1440 minutes**. Si vous passez cette valeur à 0, ce paramètre est désactivé.

Force time-out : si vous activez ce paramètre, NetScaler Gateway déconnecte la session une fois ce délai expiré, quelle que soit l'activité de l'utilisateur à ce moment. Une fois ce délai expiré, l'utilisateur ne peut rien faire pour empêcher cette déconnexion. Ce paramètre est appliqué aux utilisateurs qui se connectent avec le plug-in NetScaler Gateway, Citrix Secure Hub ou via un navigateur Web. Si Citrix Secure Mail utilise STA, un mode NetScaler Gateway spécial, ce paramètre ne s'applique pas aux sessions de Citrix Secure Mail. Par défaut, il n'y a pas de valeur, ce qui signifie que les sessions sont prolongées pour toute activité.

Pour plus d'informations sur les paramètres d'expiration pour NetScaler Gateway, veuillez consulter la documentation de NetScaler Gateway.

Pour plus d'informations sur les scénarios qui invitent les utilisateurs à s'authentifier auprès de Citrix Endpoint Management en entrant des informations d'identification sur leurs appareils, consultez Scénarios d'invite d'authentification.

Paramètres de configuration par défaut

Ces paramètres sont les paramètres par défaut fournis par :

- Assistant NetScaler pour XenMobile
- SDK MAM ou MDX Toolkit
- Console Citrix Endpoint Management

Paramètre	Où trouver le paramètre	Paramètre par défaut
Session time-out	NetScaler Gateway	1440 minutes
Délai d'expiration forcé	NetScaler Gateway	Aucune valeur (désactivé)
Période hors connexion maximale	Stratégies MDX	72 heures
Expiration du ticket des services d'arrière-plan	Stratégies MDX	168 heures (7 jours)
Session micro VPN requise	Stratégies MDX	Désactivé
Période de grâce requise pour les sessions micro VPN	Stratégies MDX	0
Code secret d'application	Stratégies MDX	On
Encrypt secrets using passcode	Propriétés du client Citrix Endpoint Management	false

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Où trouver le paramètre	Paramètre par défaut
Enable Citrix PIN Authentication	Propriétés du client Citrix Endpoint Management	false
PIN Strength Requirement	Propriétés du client Citrix Endpoint Management	Moyen
Type de code PIN	Propriétés du client Citrix Endpoint Management	Numeric
Enable User Password Caching	Propriétés du client Citrix Endpoint Management	false
Inactivity Timer	Propriétés du client Citrix Endpoint Management	15
Enable Touch ID Authentication	Propriétés du client Citrix Endpoint Management	false

Configurations recommandées

Cette section présente des exemples de trois configurations Citrix Endpoint Management allant de la sécurité la plus faible à une expérience utilisateur optimale, en passant par la sécurité la plus élevée et une expérience utilisateur plus intrusive. Ces exemples fournissent des points de référence utiles pour déterminer où sur l'échelle vous souhaitez placer votre propre configuration. La modification de ces paramètres peut vous obliger à modifier d'autres paramètres. Par exemple, la période hors connexion maximale ne doit pas dépasser le délai d'expiration de la session.

Sécurité la plus élevée

Cette configuration offre le plus haut niveau de sécurité mais comporte des compromis importants en termes d'utilisabilité.

Paramètre	Où trouver le paramètre	Réglage recommandé	Impact du comportement

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Session time-out	NetScaler Gateway	1440	Les utilisateurs entrent leurs informations d'identification Citrix Secure Hub uniquement lorsqu'une authentification en ligne est requise : toutes les 24 heures.
Délai d'expiration forcé	NetScaler Gateway	Aucune valeur	Les sessions sont prolongées pour toute activité.
Période hors connexion maximale	Stratégies MDX	23	Nécessite une actualisation de la stratégie tous les jours.
Expiration du ticket des services d'arrière-plan	Stratégies MDX	72 heures	Délai d'expiration pour STA, ce qui permet des sessions de longue durée sans jeton de session NetScaler Gateway. Pour Citrix Secure Mail, un délai d'expiration STA plus long que le délai d'expiration de la session évite que les notifications par e-mail ne s'arrêtent. Dans ce cas, Citrix Secure Mail n'invite pas l'utilisateur à ouvrir l'application avant l'expiration de la session.
Session micro VPN requise	Stratégies MDX	Désactivé	Fournit une connexion réseau valide et une session NetScaler Gateway pour utiliser les applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Période de grâce requise pour les sessions micro VPN	Stratégies MDX	0	Aucune période de grâce (si vous avez activé Session micro VPN requise).
Code secret d' application	Stratégies MDX	On	Exige un code secret pour une application.
Encrypt secrets using passcode	Propriétés du client Citrix Endpoint Management	true	Une clé dérivée de l' entropie utilisateur protège le coffre.
Enable Citrix PIN Authentication	Propriétés du client Citrix Endpoint Management	true	Active le code PIN Citrix pour une expérience d' authentification simplifiée.
PIN Strength Requirement	Propriétés du client Citrix Endpoint Management	Forte	Exigence de complexité pour le mot de passe élevée
Type de code PIN	Propriétés du client Citrix Endpoint Management	Alphanumérique	Le code PIN est une séquence alphanumérique.
Activer la mise en cache du mot de passe	Propriétés du client Citrix Endpoint Management	false	Le mot de passe Active Directory n'est pas mis en cache et le code PIN Citrix est utilisé pour les authentifications hors connexion.
Inactivity Timer	Propriétés du client Citrix Endpoint Management	15	Si l'utilisateur n'utilise pas les applications MDX ou Citrix Secure Hub pendant cette période, demandez une authentification hors connexion.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Enable Touch ID Authentication	Propriétés du client Citrix Endpoint Management	false	Désactive Touch ID pour les cas d'utilisation d'authentification hors connexion dans iOS.

Sécurité plus élevée

Cette configuration, une approche intermédiaire, nécessite que les utilisateurs s'authentifient plus souvent, tous les 3 jours au plus, au lieu de 7, augmentant ainsi le niveau de sécurité. L'augmentation du nombre d'authentifications permet de verrouiller le conteneur plus souvent, assurant la sécurité des données lorsque les appareils ne sont pas utilisés.

Paramètre	Où trouver le paramètre	Réglage recommandé	Impact du comportement
Session time-out	NetScaler Gateway	4320	Les utilisateurs entrent leurs informations d'identification Citrix Secure Hub uniquement lorsqu'une authentification en ligne est requise : tous les 3 jours.
Délai d'expiration forcé	NetScaler Gateway	Aucune valeur	Les sessions sont prolongées pour toute activité.
Période hors connexion maximale	Stratégies MDX	71	Nécessite une actualisation de la stratégie tous les 3 jours. La différence d'heure est pour permettre une actualisation avant l'expiration de la session.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Expiration du ticket des services d'arrière-plan	Stratégies MDX	168 heures	Délai d'expiration pour STA, ce qui permet des sessions de longue durée sans jeton de session NetScaler Gateway. Pour Citrix Secure Mail, un délai d'expiration STA plus long que le délai d'expiration de la session évite que les notifications par e-mail s'arrêtent sans que l'utilisateur ne soit invité à ouvrir l'application.
Session micro VPN requise	Stratégies MDX	Désactivé	Fournit une connexion réseau valide et une session NetScaler Gateway pour utiliser les applications.
Période de grâce requise pour les sessions micro VPN	Stratégies MDX	0	Aucune période de grâce (si vous avez activé Session micro VPN requise).
Code secret d'application	Stratégies MDX	On	Exige un code secret pour une application.
Encrypt secrets using passcode	Propriétés du client Citrix Endpoint Management	false	Ne nécessite pas d'entropie utilisateur pour crypter le coffre.
Enable Citrix PIN Authentication	Propriétés du client Citrix Endpoint Management	true	Active le code PIN Citrix pour une expérience d'authentification simplifiée.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

PIN Strength Requirement	Propriétés du client Citrix Endpoint Management	Moyen	Applique des règles de complexité de mot de passe moyennes.
Type de code PIN	Propriétés du client Citrix Endpoint Management	Numeric	Un code PIN est une séquence numérique.
Activer la mise en cache du mot de passe	Propriétés du client Citrix Endpoint Management	true	Le code PIN de l'utilisateur met en cache et protège le mot de passe Active Directory.
Inactivity Timer	Propriétés du client Citrix Endpoint Management	30	Si l'utilisateur n'utilise pas les applications MDX ou Citrix Secure Hub pendant cette période, demandez une authentification hors connexion.
Enable Touch ID Authentication	Propriétés du client Citrix Endpoint Management	true	Active Touch ID pour les cas d'utilisation d'authentification hors connexion dans iOS.

Haute sécurité

Cette configuration, la plus pratique pour les utilisateurs, fournit une sécurité de base.

Paramètre	Où trouver le paramètre	Réglage recommandé	Impact du comportement

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Session time-out	NetScaler Gateway	10080	Les utilisateurs entrent leurs informations d'identification Citrix Secure Hub uniquement lorsqu'une authentification en ligne est requise : tous les 7 jours.
Délai d'expiration forcé	NetScaler Gateway	Aucune valeur	Les sessions sont prolongées pour toute activité.
Période hors connexion maximale	Stratégies MDX	167	Nécessite une actualisation de la stratégie chaque semaine (tous les 7 jours). La différence d'heure est pour permettre une actualisation avant l'expiration de la session.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Expiration du ticket des services d' arrière-plan	Stratégies MDX	240	Délai d'expiration pour STA, ce qui permet des sessions de longue durée sans jeton de session NetScaler Gateway. Pour Citrix Secure Mail, un délai d' expiration STA plus long que le délai d' expiration de la session évite que les notifications par e-mail ne s'arrêtent. Dans ce cas, Citrix Secure Mail n'invite pas l'utilisateur à ouvrir l'application avant l'expiration de la session.
Session micro VPN requise	Stratégies MDX	Désactivé	Fournit une connexion réseau valide et une session NetScaler Gateway pour utiliser les applications.
Période de grâce requise pour les sessions micro VPN	Stratégies MDX	0	Aucune période de grâce (si vous avez activé Session micro VPN requise).
Code secret d' application	Stratégies MDX	On	Exige un code secret pour une application.
Encrypt secrets using passcode	Propriétés du client Citrix Endpoint Management	false	Ne nécessite pas d' entropie utilisateur pour crypter le coffre.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Enable Citrix PIN Authentication	Propriétés du client Citrix Endpoint Management	true	Active le code PIN Citrix pour une expérience d'authentification simplifiée.
PIN Strength Requirement	Propriétés du client Citrix Endpoint Management	Faible	Aucune exigence de complexité pour le mot de passe
Type de code PIN	Propriétés du client Citrix Endpoint Management	Numeric	Un code PIN est une séquence numérique.
Activer la mise en cache du mot de passe	Propriétés du client Citrix Endpoint Management	true	Le code PIN de l'utilisateur met en cache et protège le mot de passe Active Directory.
Inactivity Timer	Propriétés du client Citrix Endpoint Management	90	Si l'utilisateur n'utilise pas les applications MDX ou Citrix Secure Hub pendant cette période, demandez une authentification hors connexion.
Enable Touch ID Authentication	Propriétés du client Citrix Endpoint Management	true	Active Touch ID pour les cas d'utilisation d'authentification hors connexion dans iOS.

Utilisation de l'authentification renforcée

Certaines applications peuvent nécessiter une authentification améliorée, par exemple, un facteur d'authentification secondaire, tel qu'un jeton ou des délais d'expiration de session agressifs. Vous contrôlez cette méthode d'authentification via une stratégie MDX. La méthode nécessite également un serveur virtuel distinct pour contrôler les méthodes d'authentification (sur les mêmes appliances ou sur des appliances NetScaler Gateway distinctes).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paramètre	Où trouver le paramètre	Réglage recommandé	Impact du comportement
Passerelle NetScaler Gateway alternative	Stratégies MDX	Nécessite le nom de domaine complet et le port du boîtier NetScaler Gateway secondaire.	Permet une authentification améliorée contrôlée par les stratégies d'authentification et de session du boîtier NetScaler Gateway secondaire.

Si un utilisateur ouvre une application qui utilise l'autre instance NetScaler Gateway, toutes les autres applications utilisent cette instance NetScaler Gateway pour communiquer avec le réseau interne. La session ne reviendra à l'instance NetScaler Gateway de sécurité inférieure que lorsque la session de l'instance NetScaler Gateway avec une sécurité renforcée expire.

Utilisation de Session micro VPN requise

Pour certaines applications telles que Citrix Secure Web, vous pouvez vous assurer que les utilisateurs n'exécutent une application que lorsqu'ils ont une session authentifiée. Cette stratégie applique cette option et permet une période de grâce afin que les utilisateurs puissent terminer leur travail.

Paramètre	Où trouver le paramètre	Réglage recommandé	Impact du comportement
Session micro VPN requise	Stratégies MDX	On	S'assure qu'un appareil est en ligne et possède un jeton d'authentification valide.
Période de grâce requise pour les sessions micro VPN	Stratégies MDX	15	Autorise une période de grâce de 15 minutes avant que l'utilisateur ne puisse plus utiliser les applications

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Propriétés du serveur

March 1, 2024

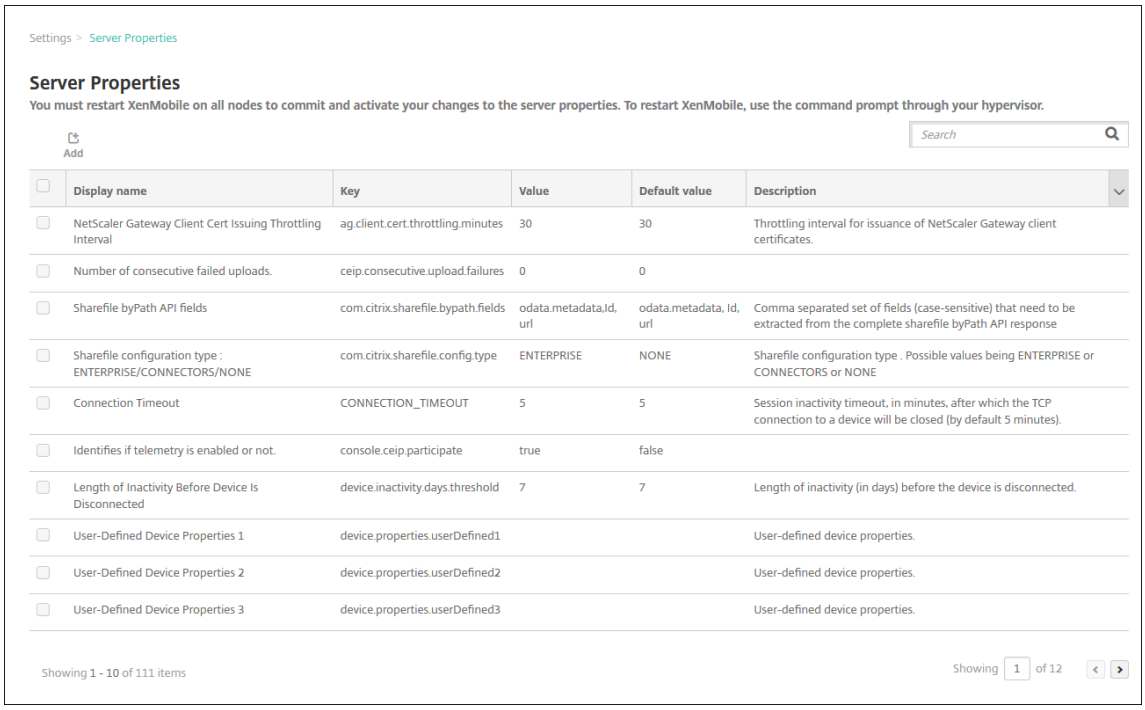
Les propriétés de serveur sont des propriétés globales qui s'appliquent aux opérations, utilisateurs et appareils sur une instance Citrix Endpoint Management entière. Citrix vous recommande d'évaluer pour votre environnement les propriétés de serveur abordées dans cet article. Assurez-vous de consulter Citrix avant de modifier d'autres propriétés du serveur.

Pour mettre à jour les propriétés du serveur, accédez à **Paramètres > Propriétés du serveur**.

Ajout, modification ou suppression de propriétés de serveur

Dans Citrix Endpoint Management, vous pouvez appliquer des propriétés au serveur.

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

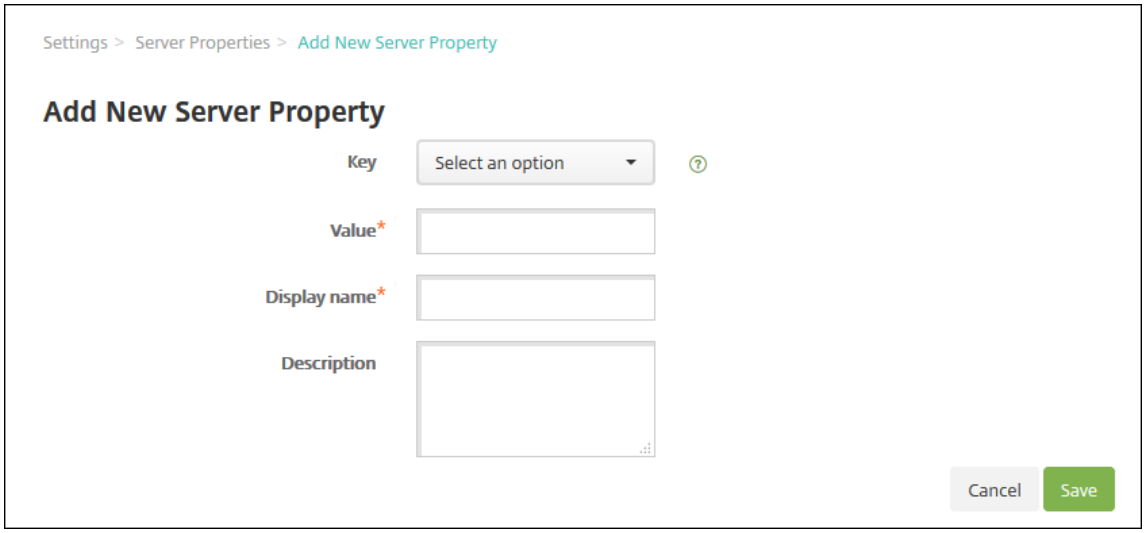


Display name	Key	Value	Default value	Description
NetScaler Gateway Client Cert Issuing Throttling Interval	ag.client.cert.throttling.minutes	30	30	Throttling interval for issuance of NetScaler Gateway client certificates.
Number of consecutive failed uploads.	ceip.consecutive.upload.failures	0	0	
Sharefile byPath API fields	com.citrix.sharefile.bypath.fields	odata.metadata,Id, url	odata.metadata, Id, url	Comma separated set of fields (case-sensitive) that need to be extracted from the complete sharefile byPath API response
Sharefile configuration type : ENTERPRISE/CONNECTORS/NONE	com.citrix.sharefile.config.type	ENTERPRISE	NONE	Sharefile configuration type . Possible values being ENTERPRISE or CONNECTORS or NONE
Connection Timeout	CONNECTION_TIMEOUT	5	5	Session inactivity timeout, in minutes, after which the TCP connection to a device will be closed (by default 5 minutes).
Identifies if telemetry is enabled or not.	console.ceip.participate	true	false	
Length of Inactivity Before Device Is Disconnected	device.inactivity.days.threshold	7	7	Length of inactivity (in days) before the device is disconnected.
User-Defined Device Properties 1	device.properties.userDefined1			User-defined device properties.
User-Defined Device Properties 2	device.properties.userDefined2			User-defined device properties.
User-Defined Device Properties 3	device.properties.userDefined3			User-defined device properties.

Pour ajouter une propriété de serveur

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Pour configurer ces paramètres :

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

3. Cliquez sur **Enregistrer**.

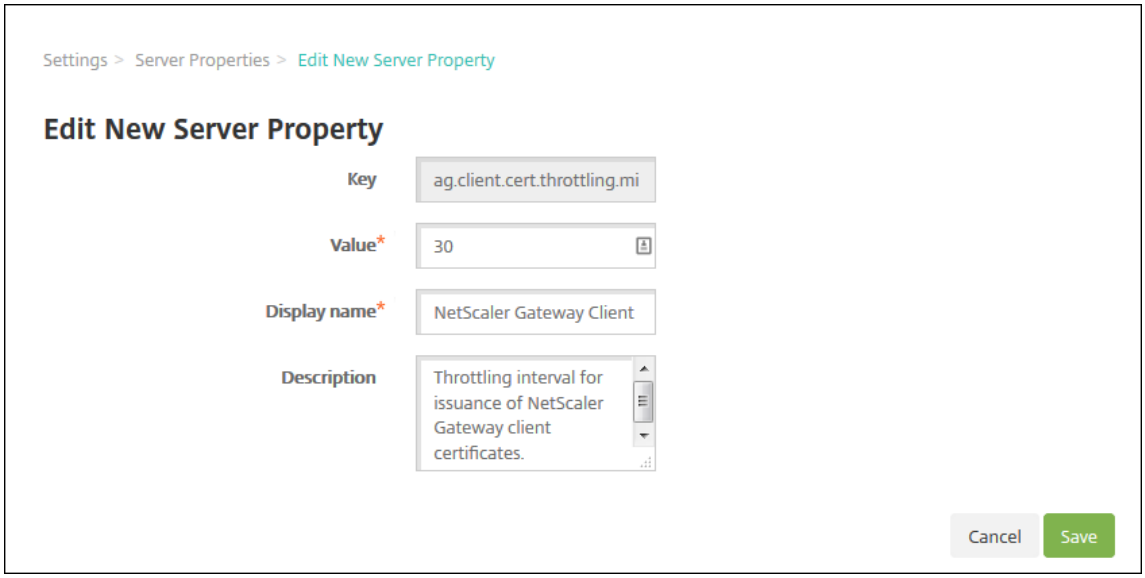
Pour modifier une propriété de serveur

1. Dans le tableau **Propriétés du serveur**, sélectionnez la propriété de serveur que vous voulez modifier.

   Lorsque vous sélectionnez la case à cocher en regard d'une propriété de serveur, le menu d'options s'affiche au-dessus de la liste des propriétés de serveur. Cliquez dans la liste pour ouvrir le menu d'options sur le côté droit de la liste.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Modifiez les informations suivantes le cas échéant :

   - Clé : vous ne pouvez pas modifier ce champ.
   - Valeur : valeur de la propriété.
   - Nom d'affichage : nom de la propriété.
   - Description : description de la propriété.

4. Cliquez sur **Enregistrer** pour enregistrer vos modifications ou sur **Annuler** pour laisser la propriété inchangée.

Pour supprimer une propriété de serveur

1. Dans le tableau **Propriétés du serveur**, sélectionnez les propriétés de serveur que vous voulez supprimer.
2. Cliquez sur **Delete**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer**.

Définitions des propriétés du serveur

Accéder à toutes les applications de la plate-forme Google Play d'entreprise

- Si la valeur est **true**, Citrix Endpoint Management rend toutes les applications du Google Play Store public accessibles depuis la plate-forme Google Play d'entreprise. Vous pouvez utiliser la stratégie Restrictions pour contrôler l'accès à ces applications. La valeur par défaut est **false**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ajouter toujours un appareil

- Si ce paramètre est défini sur **true**, Citrix Endpoint Management ajoute un appareil à la console Citrix Endpoint Management, même si son inscription échoue. Par conséquent, vous pouvez voir les appareils qui ont tenté de s'inscrire. La valeur par défaut est **false**.

AG Client Cert Issuing Throttling Interval

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

Permet la suppression des appareils qui ont été marqués comme inactifs pendant une période spécifiée

- Si la valeur est **true**, les appareils qui sont inactifs pendant une durée spécifiée (en jours) sont supprimés de Citrix Endpoint Management. La période d'activité est définie par la propriété **Durée pendant laquelle un appareil peut être inactif avant d'être automatiquement supprimé de CEM**. La valeur par défaut est **true**. Pour modifier la valeur de cette propriété, consultez votre représentant Citrix.

Enregistreur d'audit

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

Bloquer l'inscription des appareils iOS jailbreakés et des appareils Android rootés

Lorsque cette propriété est définie sur **true**, Citrix Endpoint Management bloque les inscriptions pour les appareils Android rootés et les appareils iOS jailbreakés. Le paramètre recommandé est **true** pour tous les niveaux de sécurité. La valeur par défaut est **true**.

cdn.s3.retry.interval and cdn.s3.max.retry

Les propriétés du serveur `cdn.s3.retry.interval` et `cdn.s3.max.retry` sont utilisées pour définir la durée maximale pour chaque téléchargement de fichiers PKG macOS. Par défaut, Citrix Endpoint Management limite la durée de téléchargement des fichiers à 100 secondes. Si le chargement

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

d'un fichier dépasse cette limite, il échoue. Pour modifier la valeur par défaut, configurez les clés `cdn.s3.retry.interval` et `cdn.s3.max.retry` comme suit :

- `cdn.s3.retry.interval`. Permet de définir l'intervalle, en millisecondes, après lequel Citrix Endpoint Management vérifie si le téléchargement d'un fichier se termine correctement. La valeur par défaut est `10000`.
- `cdn.s3.max.retry`. Permet de définir le nombre maximal de tentatives de vérification après lesquelles le téléchargement échoue. La valeur par défaut est `10`.

Les deux clés sont utilisées pour limiter les durées de téléchargement des fichiers. Par défaut, la durée est limitée à 100 secondes (10000*10 millisecondes).

Certificate Renewal in Seconds

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

Délai d'expiration de la connexion

- Délai d'inactivité de session, en minutes, après lequel Citrix Endpoint Management ferme la connexion TCP à un appareil. La session reste ouverte. S'applique aux appareils Android. La valeur par défaut est **5** minutes.

Canal de déploiement par défaut

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

Deprecate mobile service provider

- Désactive la prise en charge de l'interface du fournisseur de services mobiles utilisée pour interroger Blackberry et d'autres appareils Exchange ActiveSync. Lorsque cette option est activée, l'interface du **fournisseur de services mobiles** est masquée dans la console. La valeur par défaut est **True**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ajout de balises aux appareils

- Si vous définissez `enable.device.tagging` sur **true**, Citrix Endpoint Management ajoute automatiquement des balises aux appareils par type d'appareil. Vous pouvez utiliser des balises d'appareil pour déployer des stratégies et des applications ou configurer des groupes de mise à disposition. Citrix Endpoint Management ajoute des balises aux appareils dans les cas suivants :
  - Balises BYOD
    - Inscription des utilisateurs iOS
    - Profil de travail Android Enterprise
  - Balises d'entreprise
    - Appareils d'entreprise Android Enterprise entièrement gérés
    - Inscription en bloc
      - Appareils Apple Business Manager
      - Appareils Apple School Manager
      - Appareils Windows AutoPilot
      - Inscription en bloc Android Enterprise

Désactiver la vérification du nom d'hôte

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

Désactiver la vérification du serveur SSL

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

  La valeur par défaut est **True**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Enable Crash Reporting

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

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

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

Enable macOS OTAE

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

Activer le déclencheur de notifications

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

Extraction complète des utilisateurs ActiveSync autorisés et interdits

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

Identifie si la télémétrie est activée ou non

- Identifie si la télémétrie est activée ou non. La télémétrie est également appelée Programme d'amélioration de l'expérience client (CEIP). Vous pouvez choisir de participer au programme

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

CEIP lorsque vous installez ou mettez à niveau Citrix Endpoint Management. La télémétrie est désactivée si Citrix Endpoint Management a 15 tentatives de chargement infructueuses consécutives. La valeur par défaut est **false**.

Délai d'inactivité en minutes

- Nombre de minutes après lesquelles Citrix Endpoint Management ferme la session d'un utilisateur inactif. L'utilisateur doit avoir utilisé l'API publique de Citrix Endpoint Management pour accéder à la console Citrix Endpoint Management ou à toute application tierce. Un délai d'expiration de **0** signifie qu'un utilisateur inactif reste connecté. Pour les applications tierces qui accèdent à l'API, il est généralement nécessaire de rester connecté. La valeur par défaut est **5**.
- Si la propriété de serveur **WebServices timeout type** est **INACTIVITY_TIMEOUT** : cette propriété définit le nombre de minutes après lequel Citrix Endpoint Management ferme la session d'un administrateur inactif qui a fait ce qui suit :
  - Utilisé l'API publique pour les services REST pour accéder à la console Citrix Endpoint Management
  - Utilisé l'API publique pour les Services REST pour accéder à une application tierce. Un délai d'expiration de **0** signifie qu'un utilisateur inactif reste connecté.

include.device.properties.during.search

- Inclut toutes les propriétés de l'appareil dans une recherche d'appareils. La valeur par défaut **Off** limite la portée de la recherche aux propriétés de l'appareil et permet une recherche rapide :
  - Numéro de série
  - IMEI
  - Adresse MAC Wi-Fi
  - Adresse MAC Bluetooth
  - ID Active Sync
  - Nom d'utilisateur

  Lorsque cette propriété est définie sur **On**, les recherches sur les appareils peuvent prendre plus de temps.

ios.delayBeforeDeclareUnreachable; macos.delayBeforeDeclareUnreachable

- Spécifie le nombre de jours après lequel un appareil iOS ou macOS hors connexion est considéré comme inaccessible. Lorsqu'un appareil iOS ou macOS atteint la limite spécifiée, il arrête de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

communiquer avec Citrix Endpoint Management. Par défaut, les deux propriétés sont définies sur **45** jours.

Inscription à la gestion des appareils iOS : installer l'autorité de certification racine si nécessaire

- La propriété de serveur **ios.mdm.enrollment.installRootCaIfRequired** a la valeur **False** pour tous les environnements Citrix Endpoint Management. Citrix Endpoint Management utilise une chaîne de certificat de confiance publique, il n'est donc pas nécessaire d'envoyer une autorité de certification racine sur les appareils. (Cette propriété est utilisée uniquement pour les environnements locaux.)

Inscription à la gestion des appareils iOS - Dernière étape retardée

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

Gestion des appareils iOS - Mode de transmission d'identité

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

Gestion des appareils iOS - Taille de la clé d'identité

- Définit la taille des clés privées pour les identités MDM, le service de profils iOS et les identités d'agent Citrix Endpoint Management. La valeur par défaut est **2048**.

Gestion des appareils iOS - Jours de renouvellement d'identité

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Gestion des appareils iOS - Mot de passe de la clé privée

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

Durée d'inactivité avant la déconnexion de l'appareil

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

Durée pendant laquelle un appareil peut être inactif avant d'être automatiquement supprimé de CEM

- La durée (en jours) pendant laquelle un appareil peut être inactif avant d'être automatiquement supprimé de Citrix Endpoint Management. La durée minimale est de **14** jours et la valeur par défaut est de **30** jours. La propriété de serveur **Autorise la suppression des appareils marqués comme inactifs pendant une période spécifiée** doit être définie sur **true** pour que cette propriété prenne effet.

local.user.account.lockout.time

- Spécifie le nombre de minutes qu'un utilisateur doit attendre après avoir dépassé la limite de verrouillage. Les valeurs prises en charge sont 0-999. La valeur par défaut est **30** minutes.

local.user.account.lockout.limit

- Spécifie le nombre maximal de tentatives de connexion consécutives non valides par utilisateur. Les valeurs prises en charge sont 0-999. La valeur par défaut est définie sur **6**.

mac.dep.admin.passwd.rotate

Cette propriété de serveur vous permet de configurer les intervalles de rotation des mots de passe administrateur pour les appareils macOS inscrits via le programme de déploiement Apple. Citrix Endpoint Management vérifie s'il faut alterner le mot de passe du compte administrateur quotidiennement. Par défaut, Citrix Endpoint Management alterne le mot de passe toutes les 10 080 minutes (7 jours). Configurez la clé `mac.dep.admin.passwd.rotate` comme suit :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Valeur : *administrator-defined*
  Intervalle, en minutes, à partir duquel Citrix Endpoint Management alterne le mot de passe. Entrez une valeur égale ou supérieure à 360 (6 heures). Citrix Endpoint Management ignore les valeurs inférieures à 360 et alterne le mot de passe toutes les 360 minutes (6 heures) à la place.
- Nom d'affichage : *administrator-defined*
- Description : *administrator-defined*

MAM Only Device Max

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

MaxNumberOfWorker

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

Authentification unique NetScaler Gateway (NetScaler)

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

Number of consecutive failed uploads

- Affiche le nombre d'échecs consécutifs durant les chargements du programme CEIP. Citrix Endpoint Management incrémente la valeur lorsqu'un chargement échoue. Après 15 échecs de chargement, Citrix Endpoint Management désactive le programme CEIP, également appelé

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

télémétrie. Pour plus d'informations, consultez la section de la propriété de serveur **Identifies if telemetry is enabled or not**. Citrix Endpoint Management réinitialise la valeur sur **0** lorsqu'un chargement réussit.

Nombre d'utilisateurs par appareil

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

optional.user.identity.attributes

- Cette propriété de serveur vous permet de personnaliser les attributs utilisateur Active Directory facultatifs.

  Créez la clé personnalisée et, dans le champ **Valeurs**, modifiez les attributs utilisateur pour définir les attributs auxquels Citrix Endpoint Management peut accéder pour créer un compte utilisateur. Pour plus d'informations, consultez la section Personnaliser les propriétés de l'utilisateur.

  - Clé : **Clé personnalisée**
  - Clé : **optional.user.identity.attributes**
  - Valeur : **commonName, firstName, lastName, displayName, streetAddress, city, state, country, workPhone, homePhone, mobilePhone, company, department, description, employeeID, faxNumber, initials, ipPhone, manager, homePostalAddress, otherMobile, pager, physicalDeliveryOfficeName, postalCode, postOfficeBox, title, organization, preferredLanguage**
  - Nom d'affichage : **optional.user.identity.attributes**
  - Description : **Attributs utilisateur Active Directory facultatifs**

Nom de l'organisation pour les profils d'inscription macOS et iOS/iPadOS

- La valeur que vous tapez pour `apple.mdm.enrollment.profile.organization.name` correspond au nom de l'organisation qui fournit le profil d'inscription. Le nom s'affiche lorsque les utilisateurs inscrivent leur appareil à Citrix Endpoint Management. Le nom par défaut qui s'affiche est **Citrix Workspace**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Extraction des modifications incrémentielles des utilisateurs autorisés et interdits

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

Délai d'expiration de la lecture du serveur de certification Microsoft

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

REST Web Services

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

Récupère les informations sur les appareils par blocs de taille spécifiée

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

shp.console.enable

- Si cette propriété est définie sur **False**, empêche l'accès au portail en libre-service. Les utilisateurs qui accèdent au portail sur le port 4443 reçoivent un message « Accès refusé ». Si cette propriété est définie sur **True**, permet d'accéder au portail en libre-service via le port 443.

  La valeur par défaut est **False**.

enable.new.shp

- La valeur **False** empêche les utilisateurs d'activer leurs appareils à partir du portail utilisateur. La valeur **True** permet aux utilisateurs d'activer leurs appareils à partir du portail utilisateur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La fonction de clé de récupération BitLocker nécessite que vous définissiez cette propriété sur **False** et la propriété `shp.console.enable` sur **True**.

La valeur par défaut est **False**.

Nettoyage du journal de sessions (en jours)

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

ShareFile configuration type

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

Délai statique en minutes

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

  Le délai par défaut est **60**.

Déclencher la suppression du message de l'agent

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

Déclencher la suppression du son de l'agent

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Téléchargement d'applications non authentifiées pour les appareils Android

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

Téléchargement d'applications non authentifiées pour les appareils Windows

- Utilisé uniquement pour les anciennes versions de Citrix Secure Hub qui ne valident pas les tickets à usage unique. Si la valeur est définie sur **False**, vous pouvez télécharger des applications non authentifiées depuis Citrix Endpoint Management sur des appareils Windows. La valeur par défaut est **False**.

Utiliser l'ID ActiveSync pour réinitialiser un appareil ActiveSync

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

Utilisateurs d'Exchange uniquement

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

Intervalle de ligne de base pour l'achat en volume

- Intervalle minimum après lequel Citrix Endpoint Management ré-importe les licences d'achat en volume depuis Apple. L'actualisation des informations de licence permet de s'assurer que Citrix Endpoint Management reflète toutes les modifications, par exemple, lorsque vous supprimez manuellement une application importée de l'achat en volume. Par défaut, Citrix Endpoint Management actualise la ligne de base de licence d'achat en volume toutes les **1440** minutes au minimum.
  - Si de nombreuses licences d'achat en volume sont installées (plus de 50 000, par exemple), Citrix vous recommande d'augmenter l'intervalle de ligne de base pour réduire la fréquence et la charge de l'importation de licences.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Si vous prévoyez des modifications fréquentes de licence d'achat en volume depuis Apple, Citrix vous recommande de réduire la valeur pour que Citrix Endpoint Management reste à jour.
  - L'intervalle minimal entre deux lignes de base est de 60 minutes. En outre, Citrix Endpoint Management effectue une importation delta toutes les 60 minutes, pour capturer les modifications depuis la dernière importation. Par conséquent, si l'intervalle de ligne de base d'achat en volume est de 60 minutes, l'intervalle entre les lignes de base peut être retardé, jusqu'à 119 minutes.

Type de délai d'expiration des WebServices

- Indique comment faire expirer un jeton d'authentification récupéré depuis l'API publique.
  - Si **STATIC_TIMEOUT** est sélectionné, Citrix Endpoint Management considère qu'un jeton a expiré sur la base de la valeur spécifiée dans la propriété de serveur **Static Timeout in Minutes**.
  - Si **INACTIVITY_TIMEOUT** est sélectionné, Citrix Endpoint Management considère qu'un jeton a expiré sur la base de la valeur spécifiée dans la propriété de serveur **Inactivity Timeout in Minutes**. La valeur par défaut est **STATIC_TIMEOUT**.

Validité du certificat MDM de Windows Tablet prolongée (5 ans)

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

Windows WNS Channel - Number of Days Before Renewal

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

Windows WNS Heartbeat Interval

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ticket XAM à usage unique

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

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

- Ce nom de propriété reflète les anciennes versions de Citrix Endpoint Management. La propriété contrôle l'intervalle maximal d'inactivité de la console Citrix Endpoint Management. Cet intervalle est le nombre de minutes après lesquelles Citrix Endpoint Management ferme la session d'un utilisateur inactif sur la console Citrix Endpoint Management. Un délai d'expiration de **0** signifie qu'un utilisateur inactif reste connecté. La valeur par défaut est **30**.

Stratégies d'appareil et d'application

March 1, 2024

Les stratégies d'appareil et d'application Citrix Endpoint Management vous permettent d'optimiser l'équilibre entre les facteurs, tels que :

- Sécurité d'entreprise
- Protection de données et des ressources d'entreprise
- Confidentialité des utilisateurs
- Expériences utilisateur productives et positives

L'équilibre optimal entre ces facteurs peut varier. Par exemple, les organisations hautement réglementées, telles que celles du secteur financier, exigent des contrôles de sécurité plus stricts que d' autres industries, telles que l'éducation et la vente au détail, dans lesquelles la productivité des utilisateurs est une considération primordiale.

Vous pouvez contrôler et configurer de manière centralisée les stratégies en fonction de l'identité, de l'appareil, de l'emplacement et du type de connectivité des utilisateurs afin de limiter l'utilisation malveillante du contenu de l'entreprise. En cas de perte ou de vol d'un appareil, vous pouvez désactiver, verrouiller ou effacer à distance les applications et les données d'entreprise. Le résultat global est une solution qui augmente la satisfaction et la productivité des employés, tout en assurant la sécurité et le contrôle administratif.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

L'objectif principal de cet article concerne les nombreuses stratégies relatives aux appareils et aux applications liées à la sécurité.

Stratégies répondant aux risques de sécurité

Les stratégies relatives aux appareils et aux applications Citrix Endpoint Management répondent à de nombreuses situations pouvant présenter un risque de sécurité, dans les cas suivants notamment :

- Des utilisateurs tentent d'accéder à des applications et des données à partir d'appareils non approuvés et d'emplacements imprévisibles.
- Des utilisateurs transmettent des données entre les appareils.
- Un utilisateur non autorisé essaie d'accéder aux données.
- Un utilisateur qui a quitté l'entreprise a utilisé son propre appareil (BYOD).
- Un utilisateur a égaré un appareil.
- Les utilisateurs doivent toujours accéder au réseau en toute sécurité.
- Les utilisateurs ont leur propre appareil géré et que vous devez séparer les données professionnelles des données personnelles.
- Un appareil est inactif et nécessite une nouvelle vérification des informations d'identification de l'utilisateur.
- Des utilisateurs copient et collent du contenu sensible dans des systèmes de messagerie non protégés.
- Des utilisateurs reçoivent des pièces jointes à un e-mail ou des liens Web contenant des données sensibles sur un appareil qui contient des comptes personnels et d'entreprise.

Ces situations concernent deux principaux domaines de préoccupation lors de la protection des données de l'entreprise, à savoir lorsque les données sont :

- Au repos
- En transit

Protection des données au repos par Citrix Endpoint Management

Les données stockées sur les appareils mobiles sont appelées données au repos. Citrix Endpoint Management utilise le cryptage de l'appareil fourni par les plates-formes iOS et Android. Citrix Endpoint Management complète le cryptage basé sur la plate-forme avec des fonctionnalités telles que la vérification de la conformité, disponibles via le SDK Citrix MAM.

Les fonctionnalités de gestion des applications mobiles (MAM) de Citrix Endpoint Management permettent une gestion, une sécurité et un contrôle complets des applications de productivité mobiles Citrix, des applications compatibles MDX et des données associées.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Le SDK Applications mobiles permet aux applications d'être déployées pour Citrix Endpoint Management via l'utilisation de la technologie de conteneur d'applications Citrix MDX. La technologie de conteneur sépare les applications et les données d'entreprise des applications et des données personnelles sur un appareil utilisateur. Cette séparation des données vous permet de sécuriser toute application mobile personnalisée, développée par une tierce partie ou BYO avec des contrôles complets basés sur des stratégies.

Citrix Endpoint Management inclut également le cryptage au niveau de l'application. Citrix Endpoint Management crypte séparément les données stockées dans toute application compatible MDX sans nécessiter de code secret de l'appareil et sans que vous ayez besoin de gérer l'appareil pour appliquer la stratégie.

- Sur les appareils iOS, Citrix Endpoint Management utilise des services cryptographiques et des bibliothèques robustes validés par FIPS, tels que le trousseau.
- OpenSSL fournit des modules validés par FIPS pour diverses plates-formes d'appareils. OpenSSL sécurise davantage les données en mouvement et les certificats nécessaires à la gestion et à l'inscription des appareils.
- Citrix Endpoint Management utilise l'API de coffre partagé du SDK MAM pour partager le contenu géré entre les applications qui ont le même groupe de trousseaux d'accès. Par exemple, vous pouvez partager des certificats utilisateur par le biais d'une application inscrite de façon à ce que les applications puissent obtenir un certificat depuis le coffre sécurisé.
- Citrix Endpoint Management utilise le cryptage de l'appareil fourni par les plates-formes.
- Les contrôles MAM Citrix Endpoint Management au niveau de l'application effectuent une vérification de conformité pour vérifier que le cryptage de l'appareil est activé à chaque lancement d'application.

Protection des données en transit par Citrix Endpoint Management

Les données déplacées entre les appareils mobiles de votre utilisateur et votre réseau interne sont appelées données en transit. La technologie de conteneur d'applications MDX fournit un accès VPN spécifique aux applications à votre réseau interne via NetScaler Gateway.

Considérez la situation dans laquelle un employé souhaite accéder aux ressources suivantes résidant sur le réseau d'entreprise sécurisé à partir d'un appareil mobile :

- Serveur de messagerie d'entreprise
- Application Web SSL hébergée sur l'intranet d'entreprise
- Documents stockés sur un serveur de fichiers ou Microsoft SharePoint

MDX permet l'accès à toutes ces ressources d'entreprise à partir d'appareils mobiles via un micro VPN spécifique à l'application. Chaque appareil possède son propre tunnel micro VPN dédié.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La fonctionnalité Micro VPN ne nécessite pas de VPN à l'échelle de l'appareil, ce qui peut compromettre la sécurité sur les appareils mobiles non approuvés. En conséquence, le réseau interne n'est pas exposé à des logiciels malveillants ou à des attaques susceptibles d'infecter l'ensemble du système de l'entreprise. Les applications mobiles d'entreprise et les applications mobiles personnelles peuvent coexister sur un même appareil.

Pour offrir des niveaux de sécurité encore plus élevés, vous pouvez configurer des applications compatibles MDX avec une stratégie NetScaler Gateway Alternatif. La stratégie est utilisée pour l'authentification et pour les sessions micro VPN avec une application. Vous pouvez utiliser une stratégie NetScaler Gateway alternative avec la stratégie Session micro VPN requise pour forcer les applications à se réauthentifier sur la passerelle spécifique. Ces types de passerelles ont généralement des exigences d'authentification et des stratégies de gestion du trafic différentes (meilleur contrôle).

En plus des fonctionnalités de sécurité, le micro VPN offre également des techniques d'optimisation des données, y compris des algorithmes de compression. Les algorithmes de compression garantissent que :

- Seules des données minimales sont transférées.
- Le transfert se fait dans les plus brefs délais. La vitesse améliore l'expérience utilisateur, qui est un facteur clé de succès dans l'adoption d'appareils mobiles.

Réévaluez vos stratégies d'appareil périodiquement, par exemple dans les situations suivantes :

- Lorsqu'une nouvelle version de Citrix Endpoint Management inclut des stratégies nouvelles ou mises à jour en raison de la publication des mises à jour du système d'exploitation de l'appareil.
- Lorsque vous ajoutez un type d'appareil :

  Bien que la plupart des stratégies soient communes à tous les appareils, chaque appareil dispose de stratégies spécifiques à son système d'exploitation. Par conséquent, vous pouvez constater des différences entre appareils iOS, Android et Windows et même entre appareils Android de différents fournisseurs.
- Pour que l'opération Citrix Endpoint Management reste synchronisée avec les modifications de l'entreprise ou de l'industrie, telles que les nouvelles stratégies de sécurité de l'entreprise ou les réglementations de conformité.
- Lorsqu'une nouvelle version du SDK MAM inclut des stratégies nouvelles ou mises à jour
- Lorsque vous ajoutez ou mettez à jour une application.
- Pour intégrer de nouveaux workflows pour vos utilisateurs à la suite de nouvelles applications ou de nouvelles exigences.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stratégies d'application et scénarios de cas d'utilisation

Bien que vous puissiez choisir les applications disponibles via Citrix Secure Hub, vous pouvez également définir la manière dont ces applications interagissent avec Citrix Endpoint Management. Utilisez les stratégies d'application :

- Si vous souhaitez que les utilisateurs s'authentifient après une certaine période.
- Si vous souhaitez fournir aux utilisateurs un accès hors connexion à leurs informations.

Les sections suivantes incluent certaines des stratégies et des exemples d'utilisation.

- Pour obtenir la liste des stratégies tierces que vous pouvez intégrer dans votre application iOS et Android à l'aide du SDK MAM, reportez-vous à la section Présentation du SDK MAM.
- Pour un tableau des stratégies applicatives MDX par plate-forme, consultez la section Synopsis des stratégies MDX.

Authentication policies

- **Code secret de l'appareil**

  Utilisation de cette stratégie : activez la stratégie Code secret de l'appareil pour qu'un utilisateur puisse accéder à une application MDX uniquement si le code secret de l'appareil est activé sur le terminal. Cette fonctionnalité garantit l'utilisation du cryptage iOS au niveau de l'appareil.

  Exemple pour l'utilisateur : l'activation de cette stratégie signifie que l'utilisateur doit définir un code secret sur son appareil iOS avant de pouvoir accéder à l'application MDX.

- **Code secret d'application**

  Utilisation de cette stratégie : activez la stratégie Code secret d'application pour que Citrix Secure Hub invite un utilisateur à s'authentifier auprès de l'application gérée avant de pouvoir ouvrir l'application et accéder aux données. L'utilisateur peut s'authentifier avec son mot de passe Active Directory, son code PIN Citrix ou son code TouchID iOS, selon la configuration choisie sous **Paramètres > Propriétés du client** dans la console Citrix Endpoint Management. Vous pouvez définir un délai d'inactivité dans Propriétés du Client afin que Citrix Secure Hub n'invite pas l'utilisateur à se réauthentifier auprès de l'application gérée jusqu'à l'expiration du délai.

  Le code secret d'application diffère du code secret d'un appareil. Lorsqu'une stratégie de code secret d'appareil est appliquée à un appareil, Citrix Secure Hub invite l'utilisateur à configurer un code secret ou un code confidentiel. L'utilisateur doit déverrouiller son appareil lorsqu'il allume l'appareil ou lorsque le minuteur d'inactivité expire. Pour plus d'informations, consultez l'article Authentification dans Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exemple pour l'utilisateur : lors de l'ouverture de l'application Citrix Secure Web sur l'appareil, l'utilisateur doit entrer son code PIN Citrix avant de pouvoir parcourir les sites Web si la période d'inactivité a expiré.

- **Session micro VPN requise**

  Pourquoi utiliser cette stratégie : si une application nécessite l'accès à une application Web (service Web) pour s'exécuter, activez cette stratégie. Citrix Endpoint Management invite ensuite l'utilisateur à se connecter au réseau d'entreprise ou à avoir une session active avant d'utiliser l'application.

  Exemple pour l'utilisateur : lorsqu'un utilisateur tente d'ouvrir une application MDX sur laquelle la stratégie Session micro VPN requise est activée, il ne peut pas utiliser l'application tant qu'elle n'est pas connectée au réseau. La connexion doit utiliser un service cellulaire ou Wi-Fi.

- **Période hors connexion maximale**

  Pourquoi utiliser cette stratégie : utilisez cette stratégie comme option de sécurité supplémentaire. La stratégie garantit que les utilisateurs qui exécutent une application hors connexion pour une durée spécifiée doivent reconfirmer les droits d'application et actualiser les stratégies.

  Exemple pour l'utilisateur : si vous configurez une application MDX avec la stratégie Période hors connexion maximale, les utilisateurs peuvent ouvrir et utiliser l'application en mode hors connexion jusqu'à ce que la période hors connexion expire. À ce stade, l'utilisateur doit se reconnecter au réseau via un service cellulaire ou Wi-Fi et se réauthentifier, si le système le demande.

Stratégies d'accès diverses

- **Période de grâce de mise à jour des applications (heures)**

  Utilisation de cette stratégie : la stratégie Période de grâce de mise à jour des applications correspond au temps dont dispose l'utilisateur pour pouvoir mettre à jour une application dont la version plus récente est disponible dans le magasin d'applications. Au moment de l'expiration, l'utilisateur doit mettre à jour l'application avant de pouvoir accéder aux données de l'application. Lors de la définition de cette valeur, gardez à l'esprit les besoins de votre personnel mobile, en particulier les personnes qui peuvent traverser de longues périodes hors connexion lors de déplacements à l'étranger.

  Exemple pour l'utilisateur : vous chargez une nouvelle version de Citrix Secure Mail dans le magasin d'applications, puis définissez une période de grâce de mise à jour des applications de 6 heures. Les utilisateurs de Citrix Secure Hub disposent alors de 6 heures pour mettre à niveau Citrix Secure Mail avant d'être acheminés vers le magasin d'applications.

- **Période d'interrogation active (minutes)**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Utilisation de cette stratégie : la stratégie Période d'interrogation active est l'intervalle durant lequel Citrix Endpoint Management vérifie les applications pour effectuer des actions de sécurité, telles que le verrouillage et l'effacement d'applications.

Exemple pour l'utilisateur : si vous définissez la stratégie Période d'interrogation active sur 60 minutes, puis envoyez la commande Verrouillage des applications (Mode kiosque), le verrouillage se produit dans les 60 minutes suivant la dernière interrogation.

Stratégies de comportement des appareils non conformes

Lorsqu'un appareil se trouve en dessous des exigences minimales de conformité, la stratégie Appareils non conformes vous permet de sélectionner les mesures à prendre : Pour de plus amples informations, consultez la section Comportement des appareils non conformes.

Stratégies d'interaction des applications

Utilisation de ces stratégies : utilisez les stratégies d'interaction des applications pour contrôler le flux de documents et de données des applications MDX vers d'autres applications sur l'appareil. Par exemple, vous pouvez empêcher un utilisateur de :

- déplacer des données vers leurs applications personnelles en dehors du conteneur ;
- coller des données de l'extérieur du conteneur vers les applications en conteneur.

Exemple pour l'utilisateur : vous définissez une stratégie d'interaction des applications sur Restreint, ce qui signifie qu'un utilisateur peut copier du texte de Citrix Secure Mail vers Citrix Secure Web. L'utilisateur ne peut pas copier ces données vers son navigateur personnel Safari ou Chrome hors du conteneur. En outre, un utilisateur peut ouvrir un document joint à partir de Citrix Secure Mail dans Citrix Files ou QuickEdit. L'utilisateur ne peut pas ouvrir le document joint dans ses propres applications d'affichage de fichiers personnels situées à l'extérieur du conteneur.

Stratégies de restrictions applicatives

Utilisation de ces stratégies : utilisez les stratégies de restriction applicatives pour contrôler les fonctionnalités auxquelles les utilisateurs peuvent accéder à partir d'une application MDX lorsqu'elle est ouverte. Les restrictions permettent de s'assurer qu'aucune activité malveillante ne peut avoir lieu pendant que l'application est en cours d'exécution. Les stratégies de restriction applicatives varient légèrement entre iOS et Android. Par exemple, dans iOS, vous pouvez bloquer l'accès à iCloud lors de l'exécution de l'application MDX. Dans Android, vous pouvez arrêter l'utilisation de la technologie NFC pendant l'exécution de l'application MDX.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exemple pour l'utilisateur : supposez que vous activez la stratégie de restrictions applicatives pour bloquer la dictée sur iOS dans une application MDX. L'utilisateur ne peut pas utiliser la fonction de dictée sur le clavier iOS lorsque l'application MDX est en cours d'exécution. Ainsi, les données de dictée des utilisateurs ne sont pas transmises au service de dictée de cloud tiers non sécurisé. Lorsque l'utilisateur ouvre son application personnelle en dehors du conteneur, l'option de dictée reste disponible pour l'utilisateur pour ses communications personnelles.

Stratégies d'accès au réseau d'applications

Utilisation de ces stratégies : utilisez les stratégies d'accès au réseau d'entreprise pour fournir l'accès aux données stockées dans votre réseau d'entreprise à partir d'une application MDX dans le conteneur sur l'appareil. L'option Tunnel - SSO Web autorise uniquement le tunneling du trafic HTTP et HTTPS. Cette option fournit une authentification unique (SSO) pour le trafic HTTP et HTTPS et l'authentification PKINIT.

Exemple pour l'utilisateur : lorsqu'un utilisateur ouvre une application MDX sur laquelle le tunneling est activé, le navigateur ouvre un site intranet sans que l'utilisateur ait besoin de démarrer un VPN. L'application accède automatiquement au site interne à l'aide de la technologie micro VPN.

Stratégies de géolocalisation et géofencing d'application

Utilisation de ces stratégies : les stratégies qui contrôlent la géolocalisation et le géofencing des applications incluent la longitude du point central, la latitude du point central et le rayon. Ces stratégies contiennent l'accès aux données dans les applications MDX vers une zone géographique spécifique. Les stratégies définissent une zone géographique par un rayon de coordonnées de latitude et de longitude. Si un utilisateur tente d'utiliser une application en dehors du rayon défini, l'application reste verrouillée et l'utilisateur ne peut pas accéder aux données de l'application.

Exemple pour l'utilisateur : un utilisateur peut accéder aux données de fusion et d'acquisition pendant qu'elles se trouvent dans leur emplacement de bureau. Lorsqu'elles sont déplacées à l'extérieur de leur emplacement de bureau, ces données sensibles deviennent inaccessibles.

Stratégies d'application Citrix Secure Mail

- **Services réseau d'arrière-plan**

  Utilisation de cette stratégie : les services réseau en arrière-plan dans Citrix Secure Mail s'appuient sur Secure STA (Secure Ticket Authority) qui est effectivement un proxy SOCKS5 pour se connecter via NetScaler Gateway. STA prend en charge les connexions à longue durée de vie et offre une meilleure autonomie de la batterie par rapport au micro VPN. Ainsi, STA est idéal

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

pour le service de messagerie qui se connecte constamment. Citrix vous recommande de configurer ces paramètres pour Citrix Secure Mail. L'assistant NetScaler for XenMobile configure automatiquement STA pour Citrix Secure Mail.

Exemple pour l'utilisateur : lorsque STA n'est pas activé et qu'un utilisateur Android ouvre Citrix Secure Mail, il est invité à ouvrir un VPN qui reste ouvert sur l'appareil. Lorsque STA est activé et qu'un utilisateur Android ouvre Citrix Secure Mail, Citrix Secure Mail se connecte de manière transparente sans VPN requis.

- **Intervalle de synchronisation par défaut**

  Utilisation de cette stratégie : ce paramètre spécifie les jours de messagerie par défaut qui se synchronisent avec Citrix Secure Mail lorsque l'utilisateur accède à Citrix Secure Mail pour la première fois. Deux semaines d'e-mail prennent plus de temps à synchroniser que trois jours d'e-mail. Plus de données à synchroniser prolonge le processus d'installation pour l'utilisateur.

  Exemple d'utilisateur : supposons que l'intervalle de synchronisation par défaut soit défini sur trois jours lorsque l'utilisateur configure pour la première fois Citrix Secure Mail. L'utilisateur peut voir tous les e-mails qu'il a reçus dans sa boîte de réception depuis trois jours. Si un utilisateur souhaite voir les e-mails datant de plus de 3 jours, il peut effectuer une recherche. Citrix Secure Mail affiche ensuite les e-mails les plus anciens stockés sur le serveur. Après l'installation de Citrix Secure Mail, chaque utilisateur peut modifier ce paramètre pour mieux répondre à ses besoins.

Stratégies d'appareil et cas d'utilisation

Les stratégies d'appareil, parfois appelées stratégies MDM, déterminent la façon dont Citrix Endpoint Management gère les appareils. Bien que la plupart des stratégies soient communes à tous les appareils, chaque appareil dispose de stratégies spécifiques à son système d'exploitation. La liste suivante inclut certaines des stratégies d'appareil et explique leur utilisation. Pour obtenir une liste de toutes les stratégies d'appareil, consultez l'article sous Stratégies d'appareil.

- **Stratégie d'inventaire des applications**

  Utilisation de cette stratégie : déployez la stratégie d'inventaire des applications sur un appareil si vous souhaitez voir les applications installées par un utilisateur. Si vous ne déployez pas la stratégie, vous ne pouvez voir que les applications qu'un utilisateur a installées à partir du magasin d'applications et non les applications installées personnellement. Utilisez la stratégie d'inventaire des applications pour bloquer certaines applications et les empêcher de s'exécuter sur les appareils d'entreprise.

  Exemple pour l'utilisateur : un utilisateur disposant d'un appareil géré par MDM ne peut pas désactiver cette fonctionnalité. Les applications installées personnellement par l'utilisateur sont visibles par les administrateurs Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Stratégie de mode kiosque**

  Utilisation de cette stratégie : la stratégie Mode kiosque pour Android vous permet de placer des applications sur une liste d'autorisation ou une liste de blocage. Par exemple, pour les applications autorisées, vous pouvez configurer un appareil kiosque. Généralement, vous déployez la stratégie Mode kiosque uniquement sur les appareils appartenant à l'entreprise car elle permet de limiter les applications que les utilisateurs peuvent installer. Vous pouvez définir un mot de passe de remplacement pour permettre aux utilisateurs d'accéder aux applications bloquées.

  Exemple pour l'utilisateur : supposons que vous déployiez une stratégie Mode kiosque qui bloque l'application Angry Birds. L'utilisateur peut installer l'application Angry Birds à partir de Google Play, mais quand il ouvre l'application, un message l'informe que son administrateur a bloqué l'application.

- **Stratégie de planification de connexion**

  Utilisation de cette stratégie : la stratégie de planification de connexion permet aux appareils Windows Mobile de se reconnecter à Citrix Endpoint Management pour la gestion MDM, la mise à disposition d'applications et le déploiement de stratégie. Pour les appareils Android et Android Enterprise, utilisez plutôt la messagerie Google Firebase Cloud Messaging (FCM). FCM contrôle les connexions à Citrix Endpoint Management. Les options de planification sont les suivantes :

  - **Jamais :** connexion manuelle. Les utilisateurs doivent lancer la connexion depuis Citrix Endpoint Management sur leurs appareils. Citrix ne recommande pas cette option pour les déploiements de production, car elle empêche le déploiement des stratégies de sécurité sur les appareils. Par conséquent, les utilisateurs ne reçoivent aucune nouvelle application ou stratégie. L'option **Jamais** est activée par défaut.
  - **Toutes les :** se connecte à l'intervalle défini. Lorsque vous envoyez une stratégie de sécurité telle qu'un effacement ou verrouillage, Citrix Endpoint Management traite la stratégie sur l'appareil la prochaine fois que l'appareil se connecte.
  - **Définir un calendrier :** Citrix Endpoint Management tente de reconnecter l'appareil de l'utilisateur à Citrix Endpoint Management Server après une perte de connexion réseau. Citrix Endpoint Management surveille la connexion en transmettant des paquets de contrôle à intervalles réguliers dans le délai que vous définissez.

  Exemple pour l'utilisateur : vous souhaitez déployer une stratégie de code secret pour les appareils inscrits. La stratégie de planification garantit que les appareils se connectent de nouveau au serveur à intervalles réguliers pour collecter la nouvelle stratégie.

- **Stratégie d'informations d'identification**

  Utilisation de cette stratégie : souvent utilisée avec une stratégie de réseau, cette stratégie permet aux entreprises de déployer des certificats pour l'authentification auprès de ressources

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

internes qui nécessitent une authentification par certificat.

Exemple pour l'utilisateur : vous déployez une stratégie de réseau qui configure un réseau sans fil sur l'appareil. Le réseau Wi-Fi nécessite un certificat d'authentification. La stratégie d'informations d'identification déploie un certificat qui est ensuite stocké dans le keystore du système d'exploitation. L'utilisateur peut alors sélectionner le certificat lorsqu'il est connecté à la ressource interne.

- **Stratégie Exchange**

  Utilisation de cette stratégie : avec Citrix Endpoint Management, vous disposez de deux options pour envoyer des e-mails Microsoft Exchange ActiveSync.

  - **Application Citrix Secure Mail :** envoyez des e-mails à l'aide de l'application Citrix Secure Mail que vous distribuez à partir du magasin d'applications public ou du magasin d'applications.
  - **Application de messagerie native :** activez la messagerie ActiveSync pour le client de messagerie natif sur l'appareil. Vous pouvez utiliser des macros pour remplir les données utilisateur à partir de leurs attributs Active Directory, tels que `${ user.username }` pour renseigner le nom d'utilisateur et `${ user.domain }` pour renseigner le domaine utilisateur.

  Exemple pour l'utilisateur : lors de la mise à disposition de la stratégie Exchange, vous envoyez les détails du serveur Exchange à l'appareil. Citrix Secure Hub invite l'utilisateur à s'authentifier et la messagerie commence à être synchronisée.

- **Stratégie d'emplacement**

  Utilisation de cette stratégie : cette stratégie vous permet de géo-localiser les appareils sur une carte, en supposant que le GPS est activé pour Citrix Secure Hub sur l'appareil. Après avoir déployé cette stratégie, puis envoyé une commande locate depuis Citrix Endpoint Management, l'appareil répond avec les coordonnées d'emplacement.

  Exemple pour l'utilisateur : lorsque vous déployez la stratégie de localisation et que le GPS est activé sur l'appareil, si les utilisateurs déplacent leur appareil, ils peuvent se connecter au portail en libre-service Citrix Endpoint Management et choisir l'option de localisation pour afficher l'emplacement de leur appareil sur une carte. Un utilisateur choisit d'autoriser Citrix Secure Hub à utiliser les services de localisation. Vous ne pouvez pas imposer l'utilisation des services de localisation lorsque les utilisateurs inscrivent eux-mêmes un appareil. Une autre considération pour l'utilisation de cette stratégie est l'effet sur la vie de la batterie.

- **Stratégie de code secret**

  Utilisation de cette stratégie : une stratégie de code secret vous permet de définir un code PIN ou un mot de passe sur un appareil géré. Cette stratégie de code secret vous permet de définir la complexité et les délais d'expiration du code secret sur l'appareil.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Exemple pour l'utilisateur : lorsque vous déployez une stratégie de code secret d'appareil sur un appareil géré, Citrix Secure Hub invite l'utilisateur à configurer un code secret ou un code confidentiel. Le code secret ou le code PIN donne à l'utilisateur accès à son appareil pendant le démarrage ou lorsque le minuteur d'inactivité expire.

- **Stratégie de suppression de profil**

  Utilisation de cette stratégie : supposons que vous déployiez une stratégie sur un groupe d'utilisateurs et que vous deviez ensuite supprimer cette stratégie d'un sous-ensemble d'utilisateurs. Vous pouvez supprimer la stratégie pour certains utilisateurs en créant une stratégie de suppression de profil. Ensuite, utilisez les règles de déploiement pour déployer la stratégie de suppression de profil uniquement vers des utilisateurs spécifiés.

  Exemple pour l'utilisateur : lorsque vous déployez une stratégie de suppression de profil sur des appareils utilisateur, les utilisateurs peuvent ne pas remarquer la modification. Par exemple, si la stratégie de suppression de profil supprime une restriction qui a désactivé la caméra de l'appareil, l'utilisateur ne remarque pas le changement. Pensez à informer les utilisateurs lorsque des modifications affectent leur expérience utilisateur.

- **Stratégie de restrictions**

  Utilisation de cette stratégie : la stratégie de restriction vous offre plusieurs façons de verrouiller et de contrôler les fonctionnalités sur l'appareil géré. Vous pouvez activer des centaines d'options de restriction pour les appareils pris en charge. Par exemple, vous pouvez désactiver l'appareil photo ou le microphone sur un appareil, appliquer des règles d'itinérance et imposer l'accès à des services tiers tels que les magasins d'applications.

  Exemple pour l'utilisateur : si vous déployez une restriction sur un appareil iOS, il se peut que l'utilisateur ne puisse pas accéder à iCloud ou à Apple App Store.

- **Stratégie termes et conditions**

  Utilisation de cette stratégie : il peut être nécessaire d'informer les utilisateurs des implications juridiques de la gestion de leur appareil. En outre, vous pouvez vous assurer que les utilisateurs sont conscients des risques de sécurité lorsque les données d'entreprise sont transmises à l'appareil. Le document Termes et conditions vous permet de publier des règles et des avis avant l'inscription de l'utilisateur.

  Exemple pour l'utilisateur : un utilisateur voit les informations de termes et conditions durant le processus d'inscription. S'il refuse d'accepter les conditions énoncées, le processus d'inscription prend fin et il ne peut pas accéder aux données de l'entreprise. Vous pouvez générer un rapport à fournir aux équipes RH/Juridique/Conformité pour indiquer qui a accepté ou refusé les conditions.

- **Stratégie VPN**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Utilisation de cette stratégie : utilisez la stratégie VPN pour fournir un accès aux systèmes principaux en utilisant la technologie VPN Gateway plus ancienne. La stratégie prend en charge divers fournisseurs de VPN, y compris Cisco AnyConnect, Juniper et Citrix VPN. Il est également possible d'associer cette stratégie à une autorité de certification et d'activer le VPN à la demande si la passerelle VPN prend en charge cette option.

Exemple pour l'utilisateur : lorsque la stratégie VPN est activée, l'appareil d'un utilisateur ouvre une connexion VPN lorsque l'utilisateur accède à un domaine interne.

- **Stratégie de clip Web**

  Utilisation de cette stratégie : utilisez la stratégie de clip Web si vous souhaitez envoyer aux appareils une icône qui s'ouvre directement sur un site Web. Un clip Web contient un lien vers un site Web et peut inclure une icône personnalisée. Sur un appareil un clip Web ressemble à une icône d'application.

  Exemple pour l'utilisateur : un utilisateur peut cliquer sur une icône de clip Web pour ouvrir un site Internet qui fournit les services auxquels il doit accéder. L'utilisation d'un lien Web est plus pratique que de taper une adresse de lien dans un navigateur.

- **Stratégie de réseau**

  Utilisation de cette stratégie : la stratégie de réseau vous permet de déployer les détails du réseau Wi-Fi, tels que le SSID, les données d'authentification et les données de configuration, sur un appareil géré.

  Exemple pour l'utilisateur : lorsque vous déployez la stratégie de réseau, l'appareil se connecte automatiquement au réseau Wi-Fi et authentifie l'utilisateur afin qu'il puisse accéder au réseau.

- **Stratégie Endpoint Management Store**

  Utilisation de cette stratégie : le magasin d'applications est un magasin d'applications unifié où les administrateurs peuvent publier toutes les applications d'entreprise et les ressources de données dont leurs utilisateurs ont besoin. Un administrateur peut ajouter les applications suivantes :

  - Applications Web, applications SaaS et applications sur lesquelles le SDK MAM est activé ou applications encapsulées avec MDX
  - Applications de productivité mobiles Citrix
  - Applications mobiles natives telles que les fichiers .ipa ou .apk
  - Applications Apple App Store et Google Play
  - Liens Web
  - Citrix Virtual Apps publiées à l'aide de Citrix StoreFront

  Exemple pour l'utilisateur : lorsqu'un utilisateur inscrit son appareil dans Citrix Endpoint Management, il accède au magasin d'applications via l'application Citrix Secure Hub. L'utilisateur

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

peut alors voir toutes les applications et services d'entreprise mis à sa disposition. Les utilisateurs peuvent cliquer sur une application pour l'installer, accéder aux données, évaluer et vérifier l'application, et télécharger les mises à jour d'applications à partir du magasin d'applications.

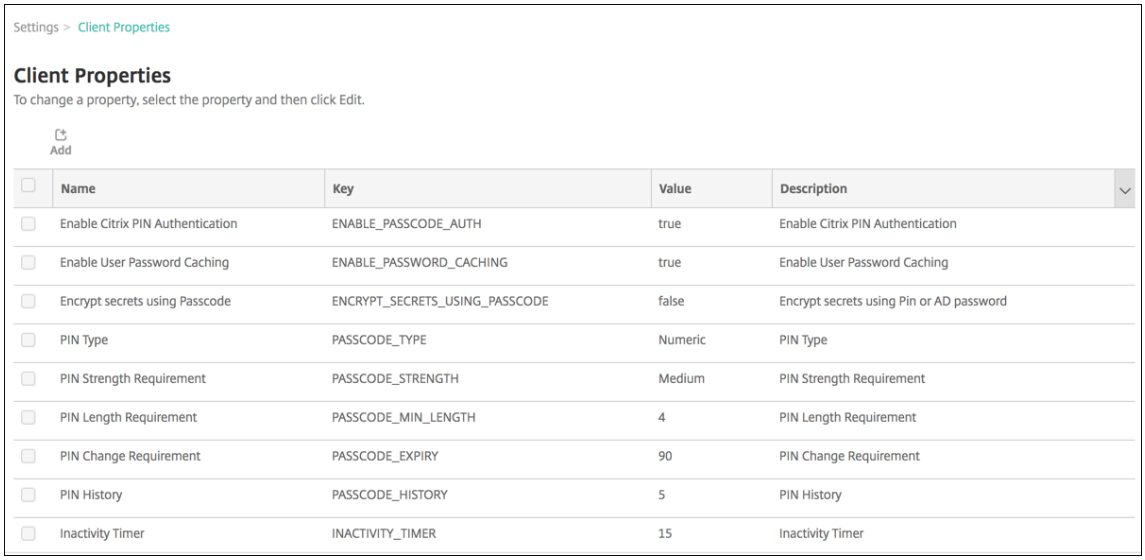
Propriétés du client

March 1, 2024

Les propriétés du client contiennent des informations qui sont fournies directement à Citrix Secure Hub sur les appareils des utilisateurs. Vous pouvez utiliser ces propriétés pour configurer des paramètres avancés tels que le code PIN Citrix. Vous obtenez les propriétés du client à partir du support de Citrix.

Les propriétés du client sont susceptibles d'être modifiées avec chaque nouvelle version de Citrix Secure Hub et occasionnellement pour les applications clientes. Pour de plus amples informations sur les propriétés du client les plus couramment configurées, consultez la section Propriété client, plus loin dans cet article.

1. Dans la console Citrix Endpoint Management, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Client**, cliquez sur **Propriétés du client**. La page **Propriétés du client** s'affiche. Vous pouvez ajouter, modifier et supprimer des propriétés de client à partir de cette page.

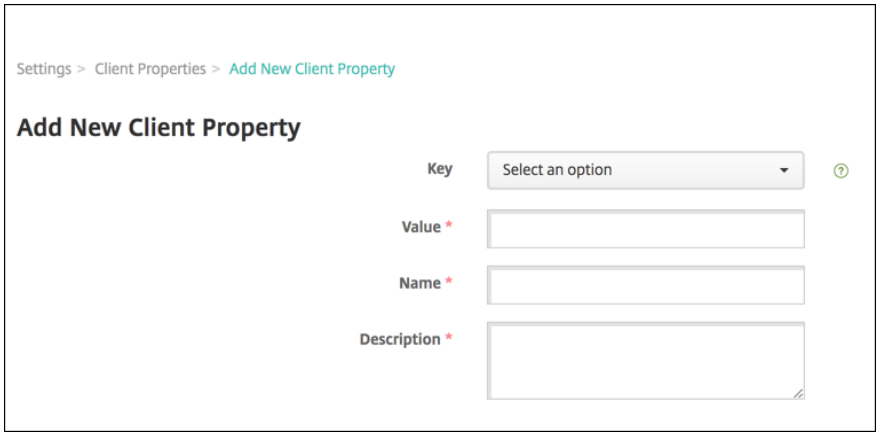


Name	Key	Value	Description
Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	true	Enable Citrix PIN Authentication
Enable User Password Caching	ENABLE_PASSWORD_CACHING	true	Enable User Password Caching
Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
PIN Type	PASSCODE_TYPE	Numeric	PIN Type
PIN Strength Requirement	PASSCODE_STRENGTH	Medium	PIN Strength Requirement
PIN Length Requirement	PASSCODE_MIN_LENGTH	4	PIN Length Requirement
PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
PIN History	PASSCODE_HISTORY	5	PIN History
Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour ajouter une propriété de client

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



2. Pour configurer ces paramètres :

   - **Clé :** cliquez sur la clé de propriété que vous souhaitez ajouter dans la liste déroulante. **Important :** contactez le support Citrix avant de mettre à jour les paramètres. Vous pouvez demander une clé spéciale.
   - **Valeur :** valeur de la propriété sélectionnée.
   - **Nom :** nom pour la propriété.
   - **Description :** description pour la propriété.

3. Cliquez sur **Enregistrer**.

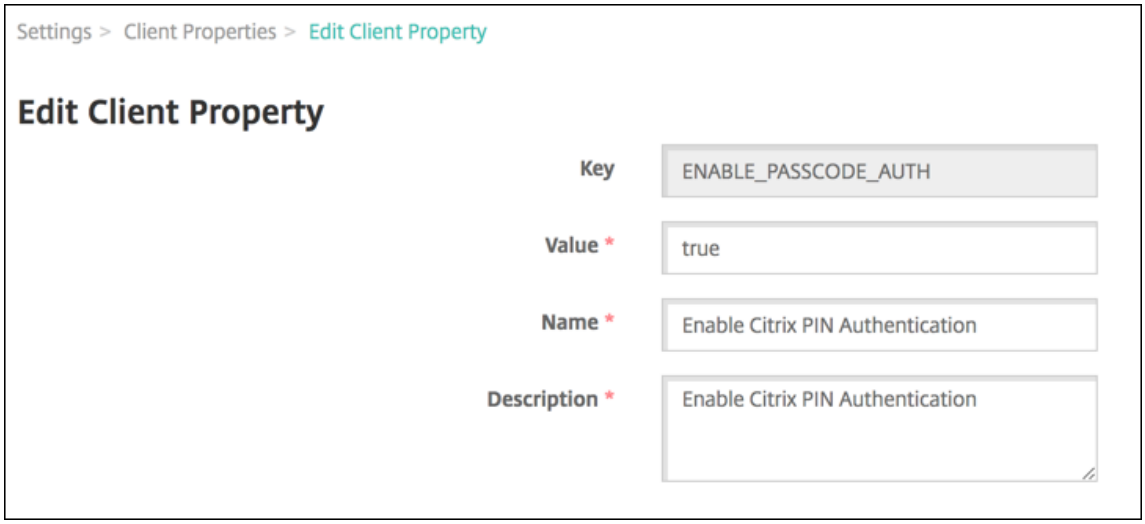
Pour modifier une propriété de client

1. Dans le tableau **Propriétés du client**, sélectionnez la propriété de client que vous voulez modifier.

   Sélectionnez la case à cocher en regard d'une propriété de client pour ouvrir le menu d'options au-dessus de la liste des propriétés de client. Cliquez dans la liste pour ouvrir le menu d'options sur le côté droit de la liste.

2. Cliquez sur **Modifier**. La page **Modifier la propriété client** s'affiche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Modifiez les informations suivantes le cas échéant :

   - **Clé :** vous ne pouvez pas modifier ce champ.
   - **Valeur :** valeur de la propriété.
   - **Nom :** nom de la propriété.
   - **Description :** description de la propriété.

4. Cliquez sur **Enregistrer** pour enregistrer vos modifications ou sur **Annuler** pour laisser la propriété inchangée.

Pour supprimer une propriété de client

1. Dans le tableau **Propriétés du client**, sélectionnez la propriété de client que vous voulez supprimer.

   Vous pouvez sélectionner plusieurs propriétés à supprimer en sélectionnant la case à cocher en regard de chaque propriété.

2. Cliquez sur **Delete**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer**.

Propriété client

Les propriétés client prédéfinies de Citrix Endpoint Management et leurs paramètres par défaut sont les suivants :

- **ALLOW_CLIENTSIDE_PROXY**
  - Nom d'affichage : ALLOW_CLIENTSIDE_PROXY

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si vos utilisateurs souhaitent utiliser un proxy qu'ils ont configuré sur leurs téléphones iOS, laissez cette stratégie personnalisée définie sur **true**, la valeur par défaut.

  Certains utilisateurs peuvent déjà avoir un proxy configuré dans **Réglages > Wi-Fi > Configurer le proxy** sur leurs appareils. Si Citrix Secure Hub ne s'ouvre pas pour ces utilisateurs, effectuez l'une des actions suivantes :

  * Supprimez la configuration du proxy de l'appareil, puis redémarrez Citrix Secure Hub.
  * Connectez l'appareil à un autre réseau Wi-Fi. Une fois que Citrix Secure Hub s'est réauthentifié, il obtient la propriété **ALLOW_CLIENTSIDE_PROXY** et s'ouvre.

- Si le paramètre **ALLOW_CLIENTSIDE_PROXY** est défini sur **false** et que les utilisateurs configurent un proxy sur leur appareil, Citrix Endpoint Management détecte le proxy. Cependant, Citrix Secure Hub n'utilise pas le proxy et affiche un message d'erreur. Si un appareil se connecte à un point d'accès ou à un routeur sur lequel un proxy est activé, Citrix Endpoint Management ne détecte pas le proxy. Pour une sécurité maximale, nous vous recommandons d'utiliser le certificate pinning. Pour plus d'informations sur l'activation du certificate pinning pour Citrix Secure Hub, consultez Certificate pinning.

- Pour configurer cette stratégie personnalisée, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **ALLOW_CLIENTSIDE_PROXY** et définissez la **valeur**.

• **CONTAINER_SELF_DESTRUCT_PERIOD**

- Nom d'affichage : MDX Container Self-Destruct Period (Période d'auto-destruction du conteneur MDX)

- La fonction d'auto-destruction empêche l'accès à Citrix Secure Hub et aux applications gérées, après un nombre spécifié de jours d'inactivité. Après la limite de temps, les applications ne sont plus utilisables. L'effacement des données inclut la suppression des données d'application pour chaque application installée, y compris le cache et les données d'utilisateur de l'application.

  Le délai d'inactivité correspond à une période de temps spécifique pendant laquelle le serveur ne reçoit pas de demande d'authentification pour valider l'utilisateur. Supposons que cette propriété soit définie sur 30 jours. Si l'utilisateur n'utilise pas l'application pendant plus de 30 jours, la stratégie s'applique.

  Cette stratégie de sécurité globale s'applique aux plates-formes iOS et Android et représente une amélioration des stratégies d'effacement et de verrouillage d'application existantes.

- Pour configurer cette stratégie globale, accédez à **Paramètres > Propriétés du client**, puis ajoutez la clé personnalisée **CONTAINER_SELF_DESTRUCT_PERIOD**.

- Valeur : nombre de jours.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **DEVICE_LOGS_TO_IT_HELP_DESK**
  - Nom d'affichage : envoyer les journaux de l'appareil au service d'assistance informatique
  - Cette propriété active ou désactive la possibilité d'envoyer des journaux au service d'assistance informatique.
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **false**
- **DISABLE_LOGGING**
  - Nom d'affichage : Disable Logging (Désactiver la journalisation)
  - Utilisez cette propriété pour empêcher les utilisateurs de collecter et de charger des journaux à partir de leurs appareils. Cette propriété désactive la journalisation pour Citrix Secure Hub et pour toutes les applications MDX installées. Les utilisateurs ne peuvent pas envoyer de journaux pour les applications à partir de la page Support. Bien que la boîte de dialogue de composition de messages s'affiche, les journaux ne sont pas joints. Un message indique que la journalisation est désactivée. Ce paramètre empêche également la mise à jour des paramètres de journal dans la console Citrix Endpoint Management pour Citrix Secure Hub et les applications MDX.

    Lorsque cette propriété est définie sur **true**, Citrix Secure Hub définit **Bloquer les journaux d'application** sur **true**. Par conséquent, les applications MDX arrêtent la journalisation lorsque la nouvelle stratégie est appliquée.
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **false** (la journalisation n'est pas désactivée)
- **ENABLE_CRASH_REPORTING**
  - Nom d'affichage : Enable Crash Reporting (Activer les rapports de plantage)
  - Si le paramètre est réglé sur **true**, Citrix collecte les rapports d'incident et les diagnostics pour aider à résoudre les problèmes avec Citrix Secure Hub pour iOS et Android. Si ce paramètre est défini sur **false**, aucune donnée n'est collectée.
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **true**
- **ENABLE_CREDENTIAL_STORE**
  - Nom d'affichage : Activer le magasin d'informations d'identification
  - L'activation du magasin d'informations d'identification signifie que les utilisateurs Android ou iOS entrent leur mot de passe une fois lorsqu'ils accèdent à des applications de productivité mobiles Citrix. Vous pouvez utiliser le magasin d'informations d'identification que vous activiez ou non le code PIN Citrix. Si vous n'activez pas le code PIN Citrix, les

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

utilisateurs entrent leur mot de passe Active Directory. Citrix Endpoint Management prend en charge l'utilisation de mots de passe Active Directory avec le magasin d'informations d'identification uniquement pour Citrix Secure Hub et les applications du magasin public. Citrix Endpoint Management ne prend pas en charge l'authentification PKI si vous utilisez des mots de passe Active Directory avec le magasin d'informations d'identification.

- L'inscription automatique dans Citrix Secure Mail exige que vous définissiez cette propriété sur **true**.
- Pour configurer cette stratégie personnalisée, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **ENABLE_CREDENTIAL_STORE** et définissez la **valeur** sur **true**.

- **ENABLE_PASSCODE_AUTH**
  - Nom d'affichage : Enable Citrix PIN Authentication (Activer l'authentification du code PIN Citrix)
  - Cette propriété permet d'activer la fonctionnalité de code PIN Citrix. Avec le code PIN ou code secret Citrix, les utilisateurs sont invités à définir un code PIN à utiliser à la place de leur mot de passe Active Directory. Ce paramètre est automatiquement activé si ENABLE_PASSWORD_CACHING est activé ou si Citrix Endpoint Management utilise l'authentification par certificat.

    Pour l'authentification en mode hors connexion, le code PIN Citrix est validé localement et les utilisateurs sont autorisés à accéder à l'application ou au contenu demandé. Pour l'authentification en ligne, le code PIN ou code secret Citrix déverrouille le mot de passe Active Directory ou le certificat qui est ensuite envoyé à des fins d'authentification auprès de Citrix Endpoint Management.

    Si ENABLE_PASSCODE_AUTH est défini sur true et ENABLE_PASSWORD_CACHING est défini sur false, l'authentification en ligne vous invite toujours à entrer le mot de passe car Citrix Secure Hub ne l'enregistre pas.
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **false**

- **ENABLE_PASSWORD_CACHING**
  - Nom d'affichage : Enable User Password Caching (Activer la mise en cache du mot de passe de l'utilisateur)
  - Cette propriété autorise la mise en cache locale des mots de passe Active Directory sur l'appareil mobile. Lorsque vous définissez cette propriété sur **true**, vous devez également définir la propriété **ENABLE_PASSCODE_AUTH** sur **true**. Lorsque la mise en cache du mot de passe de l'utilisateur est activée, les utilisateurs sont invités à créer un code PIN ou code secret Citrix.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **false**

- **ENABLE_TOUCH_ID_AUTH**

  - Nom d'affichage : Enable Touch ID Authentication (Activer l'authentification TouchID)
  - Pour les appareils qui prennent en charge l'authentification Touch ID, cette propriété active ou désactive l'authentification Touch ID sur l'appareil. Exigences :

    Le code PIN Citrix ou l'authentification LDAP doivent être activés sur les appareils utilisateur. Si l'authentification LDAP est désactivée (par exemple, lorsque seule l'authentification basée sur certificat est utilisée), les utilisateurs doivent définir un code PIN Citrix. Dans ce cas, Citrix Endpoint Management nécessite le code PIN Citrix même si la propriété de client **ENABLE_PASSCODE_AUTH** est **false**.

    Définissez **ENABLE_PASSCODE_AUTH** sur **false** de sorte que, lorsque les utilisateurs lancent une application, ils doivent répondre à une invite à utiliser la fonctionnalité Touch ID.

  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **false**

- **ENABLE_WORXHOME_CEIP**

  - Nom d'affichage : Activer CEIP Citrix Secure Hub
  - Cette propriété active le Programme d'amélioration de l'expérience utilisateur. Cette fonction va envoyer périodiquement des données de configuration et d'utilisation anonymes à Citrix. Les données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de Citrix Endpoint Management.
  - Valeur : **true** ou **false**
  - Valeur par défaut : **false**

- **ENCRYPT_SECRETS_USING_PASSCODE**

  - Nom d'affichage : Encrypt secrets using Passcode (Chiffrer les secrets à l'aide d'un code secret)
  - Cette propriété stocke les données sensibles sur l'appareil dans un coffre sécurisé plutôt que dans un magasin natif basé sur la plate-forme, tel que le trousseau iOS. Cette propriété offre un cryptage renforcé des artefacts clés et ajoute une entropie utilisateur. L'entropie utilisateur est un code PIN généré de manière aléatoire connu uniquement de l'utilisateur.

    Citrix vous recommande d'activer cette propriété de manière à fournir une sécurité plus élevée sur les appareils des utilisateurs. Par conséquent, les utilisateurs seront invités plus fréquemment à entrer le code PIN Citrix.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **false**

- **INACTIVITY_TIMER**
  - Nom d'affichage : Inactivity Timer (Délai d'inactivité)
  - Cette propriété définit la durée pendant laquelle les utilisateurs peuvent laisser leurs appareils inactifs et accéder à une application sans être invité à entrer un code PIN ou code secret Citrix. Pour activer ce paramètre pour une application MDX, vous devez définir le paramètre Code secret d'application sur Activé. Si le paramètre Code secret d'application est défini sur Désactivé, les utilisateurs sont redirigés vers Citrix Secure Hub pour effectuer une authentification complète. Lorsque vous modifiez ce paramètre, la valeur prend effet la prochaine fois que les utilisateurs sont invités à s'authentifier.

    Sur iOS, le délai d'inactivité gère également l'accès des applications MDX et non MDX à Citrix Secure Hub.
  - Valeurs possibles : tout entier positif
  - Valeur par défaut : **15** (minutes)

- **ON_FAILURE_USE_EMAIL**
  - Nom d'affichage : On failure Use Email to Send device logs to IT help desk (En cas d'échec, utiliser la messagerie pour envoyer les journaux de l'appareil au service d'assistance)
  - Cette propriété active ou désactive la possibilité d'utiliser la messagerie pour envoyer les journaux de l'appareil au service informatique.
  - Valeurs possibles : **true** ou **false**
  - Valeur par défaut : **true**

- **PASSCODE_EXPIRY**
  - Nom d'affichage : PIN Change Requirement (Exigences en matière de modification du code PIN)
  - Cette propriété définit la durée pendant laquelle le code PIN ou code secret Citrix est valide, et après laquelle l'utilisateur est obligé de modifier son code PIN ou code secret Citrix. Lorsque vous modifiez ce paramètre, la nouvelle valeur est définie uniquement lorsque le code PIN ou code secret Citrix expire.
  - Valeurs possibles : **1**-**99** recommandé. Pour éliminer les réinitialisations de code PIN, définissez la valeur sur un nombre élevé (par exemple, 100 000 000 000). Si vous avez initialement défini une période d'expiration comprise entre 1 et 99 jours et que vous la modifiez au profit d'une valeur beaucoup plus élevée, les codes PIN expirent toujours à la fin de la période initiale mais plus jamais après.
  - Valeur par défaut : **90** (jours)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **PASSCODE_HISTORY**
  - Nom d'affichage : PIN History (Historique du code PIN)
  - Cette propriété définit le nombre de codes PIN ou codes secrets Citrix précédemment utilisés que les utilisateurs ne sont pas autorisés à réutiliser lorsqu'ils changent leur code PIN ou code secret Citrix. Lorsque vous modifiez ce paramètre, la nouvelle valeur est définie la prochaine fois que les utilisateurs réinitialisent leur code PIN ou code secret Citrix.
  - Valeurs possibles : **1**-**99**
  - Valeur par défaut : **5**
- **PASSCODE_MAX_ATTEMPTS**
  - Nom d'affichage : PIN Attempts (Nombre de tentatives de saisie du code PIN)
  - Cette propriété définit le nombre de tentatives de saisie infructueuses du code PIN ou code secret Citrix que les utilisateurs peuvent effectuer avant d'être invités à fournir une authentification complète. Une fois que les utilisateurs ont effectué une authentification complète, ils sont invités à créer un code PIN ou code secret Citrix.
  - Valeurs possibles : tout entier positif
  - Valeur par défaut : **15**
- **PASSCODE_MIN_LENGTH**
  - Nom d'affichage : PIN Length Requirement (Exigences en matière de longueur du code PIN)
  - Cette propriété définit la longueur minimale des codes PIN Citrix.
  - Valeurs possibles : entre **4** et **10**
  - Valeur par défaut : **6**
- **PASSCODE_STRENGTH**
  - Nom d'affichage : PIN Strength Requirement (Exigences en matière de sûreté du code PIN)
  - Cette propriété définit le niveau de sécurité d'un code PIN ou d'un code secret Citrix. Lorsque vous modifiez ce paramètre, les utilisateurs sont invités à créer un code PIN ou code secret Citrix la prochaine fois qu'ils sont invités à s'authentifier.
  - Valeurs possibles : **Low**, **Medium**, **High** ou **Strong**
  - Valeur par défaut : **Medium**
  - Les règles de mot de passe pour chaque paramètre de sécurité en fonction du paramètre PASSCODE_TYPE sont les suivantes :

Règles pour code secret numérique :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Niveau de sécurité du code secret	Règles pour code secret numérique	Autorisé	Non autorisé
Faible	Sont autorisés tous les nombres et toute séquence	444444, 123456, 654321	
Medium (paramètre par défaut)	Ne doit contenir aucun chiffre consécutif ou répété.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
Élevé	Ne doit contenir aucun chiffre adjacent identique.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
Forte	N'utilisez pas le même chiffre plus de deux fois. N'utilisez pas trois chiffres consécutifs ou plus dans une ligne. N' utilisez pas trois chiffres consécutifs ou plus dans l'ordre inverse.	102983, 085085, 824673, 132312	132132, 131313, 902030

Règles pour code secret alphanumérique :

Niveau de sécurité du code secret	Règles pour code secret alphanumérique	Autorisé	Non autorisé
Faible	Doit contenir au moins un chiffre et une lettre.	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Niveau de sécurité du code secret	Règles pour code secret alphanumérique	Autorisé	Non autorisé
Medium (paramètre par défaut)	En plus des règles de sécurité pour un code secret de niveau moyen, les lettres et tous les chiffres ne peuvent pas être identiques. Les lettres et les nombres ne peuvent pas être consécutifs.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, ou aaa111 ; abcd12, bcd123, 123abc, xy1234, xyz345 ou cba123
Élevé	Utilisez au moins une lettre majuscule et une lettre minuscule.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
Forte	Utilisez au moins un nombre, un symbole spécial, une lettre majuscule et une lettre minuscule.	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

- **PASSCODE_TYPE**
  - Nom d'affichage : PIN Type (Type de code PIN)
  - Cette propriété définit si les utilisateurs peuvent définir un code PIN Citrix numérique ou un code secret alphanumérique. Lorsque vous sélectionnez la valeur **Numeric**, les utilisateurs peuvent uniquement utiliser des chiffres (code PIN Citrix). Lorsque vous sélectionnez la valeur **Alphanumeric**, l'utilisateur peut utiliser une combinaison de lettres et de chiffres (code secret).

    Si vous modifiez ce paramètre, les utilisateurs doivent définir un nouveau code PIN ou code secret Citrix la prochaine fois qu'ils sont invités à s'authentifier.
  - Valeurs possibles : **Numeric** ou **Alphanumeric**
  - Valeur par défaut : **Numeric**
- **REFRESHINTERVAL**
  - Nom d'affichage : REFRESHINTERVAL

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Par défaut, Citrix Endpoint Management envoie un ping au serveur de détection automatique (ADS) afin « d'épingler » les certificats tous les 3 jours. Pour modifier l'intervalle d'actualisation, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **REFRESHINTERVAL** et définissez la **valeur** sur le nombre d'heures.
  - Valeur par défaut : **72** heures (3 jours)

- **SEND_LDAP_ATTRIBUTES**
  - Pour les déploiements MAM exclusif d'appareils Android, iOS ou macOS, vous pouvez configurer Citrix Endpoint Management de manière à ce que les utilisateurs qui s'inscrivent dans Citrix Secure Hub avec des informations d'identification de messagerie soient automatiquement inscrits dans Citrix Secure Mail. Par conséquent, les utilisateurs ne fournissent pas d'informations supplémentaires et aucune étape supplémentaire n'est nécessaire pour s'inscrire dans Citrix Secure Mail.
  - Pour configurer cette stratégie globale, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **SEND_LDAP_ATTRIBUTES** et définissez la **valeur** comme suit.
  - Valeur: `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme =${ user.samaccountname } , displayName=${ user.displayName } ,mail=${ user.mail }`
  - Les valeurs d'attribut sont spécifiées en tant que macros, similaires à des stratégies MDM.
  - Voici un exemple de réponse de service de compte pour cette propriété :

    ```
    <property value="userPrincipalName=user@site.com,sAMAccountName
    =eng1,displayName=user\,test1,email=user@site.com\,user@site.
    com"name="SEND_LDAP_ATTRIBUTES"/>
    ```

  - Pour cette propriété, Citrix Endpoint Management traite les virgules en tant que terminaison de chaîne. Par conséquent, si une valeur d'attribut comprend une virgule, elle doit être précédée d'une barre oblique inverse. La barre oblique inverse empêche le client d'interpréter la virgule comme fin de la valeur d'attribut. Représentez les barres obliques inverses par `"\\"`.

- **HIDE_THREE_FINGER_TAP_MENU**
  - Lorsque cette propriété n'est pas définie ou est définie sur **false**, les utilisateurs peuvent accéder au menu des fonctionnalités masquées en effectuant un tapotement à trois doigts sur leurs appareils. Le menu des fonctions masquées permettait aux utilisateurs de réinitialiser les données de l'application. La définition de cette propriété sur **true** désactive l'accès des utilisateurs au menu des fonctionnalités masquées.
  - Pour configurer cette stratégie globale, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **HIDE_THREE_FINGER_TAP_MENU** et définissez la **valeur**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **TUNNEL_EXCLUDE_DOMAINS**
  - Nom d'affichage : Tunnel Exclude Domains
  - Par défaut, MDX exclut le tunnel micro VPN de certains points de terminaison de service que les applications et les kits de développement d'applications mobiles utilisent pour différentes fonctionnalités. Par exemple, ces points de terminaison incluent les services qui ne requièrent pas le routage via les réseaux d'entreprise, tels que Google Analytics, les services Citrix Cloud et les services Active Directory. Utilisez cette propriété de client pour remplacer la liste des domaines exclus.
  - Pour configurer cette stratégie globale, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **TUNNEL_EXCLUDE_DOMAINS** et définissez la **valeur**.
  - Valeur : pour remplacer la liste par défaut avec les domaines que vous souhaitez exclure du tunneling, tapez une liste séparée par des virgules des suffixes de domaine. Pour inclure tous les domaines dans le tunneling, entrez **none**. La valeur par défaut est :

    ```
    app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,
    cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics
    .com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.
    com, hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.
    com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.
    com,ssl.google-analytics.com,stream.launchdarkly.com
    ```

Les propriétés personnalisées du client pour Citrix Endpoint Management sont les suivantes :

ENABLE_MAM_NFACTOR_SSO:

- Cette propriété vous permet d'activer ou de désactiver l'authentification unique de la gestion d'application mobile (MAM) nFactor lors de l'inscription à la MAM ou de la connexion à Secure Hub tout en utilisant la stratégie d'authentification avancée de NetScaler Gateway. Si la valeur est définie sur **true**, l'authentification unique de la MAM nFactor est activée lors de l'inscription à la MAM ou de la connexion à Secure Hub.
- Pour configurer cette propriété, cliquez sur **Paramètres > Propriétés du client**, puis sur **Ajouter**. Sélectionnez **Clé personnalisée** dans le menu déroulant **Clé** et mettez à jour les informations suivantes le cas échéant :
  - Clé : ENABLE_MAM_NFACTOR_SSO
  - Valeur : true ou false
  - Nom : ENABLE_MAM_NFACTOR_SSO
  - Description : ajoutez la description appropriée

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Options d'inscription des utilisateurs

March 1, 2024

Vous pouvez inscrire un grand nombre d'appareils iOS dans Citrix Endpoint Management de différentes façons. Avant d'examiner les détails, décidez quels appareils vous souhaitez inscrire à MDM+MAM, MDM ou MAM. Pour plus d'informations sur ces modes de gestion, consultez la section Modes de gestion.

Au plus haut niveau, il y a quatre options d'inscription :

- **Invitation d'inscription :** envoyez une invitation d'inscription ou une URL d'invitation aux utilisateurs. Les invitations et les URL d'inscription ne sont pas disponibles pour les appareils Windows.
- **Portail en libre-service :** configurez un portail auquel les utilisateurs peuvent accéder pour télécharger Citrix Secure Hub, demander l'inscription et consulter les informations sur l'appareil.
- **Inscription manuelle :** envoyez un e-mail, un manuel ou toute autre communication permettant aux utilisateurs de savoir que le système est opérationnel et qu'ils peuvent s'inscrire. Les utilisateurs téléchargent ensuite Citrix Secure Hub et inscrivent leurs appareils manuellement.
- **Enterprise :** l'inscription des appareils peut également s'effectuer via un programme de déploiement d'Apple et Google Android Enterprise. Grâce à chacun de ces programmes, vous pouvez acheter des appareils préconfigurés, prêts à être utilisés par les employés. Pour plus d'informations, consultez les articles sur le programme de déploiement d'Apple de l'assistance Apple et la documentation sur Google Android Enterprise sur le site Web Android Enterprise.

Invitation d'inscription

Vous pouvez envoyer une invitation d'inscription aux utilisateurs d'appareils iOS, macOS, Android Enterprise et d'appareils Android d'ancienne génération. Les invitations d'inscription ne sont pas disponibles pour les appareils Windows.

Vous pouvez également envoyer un lien d'installation via SMTP aux utilisateurs d'appareils iOS, macOS, Android Enterprise, Android ou Windows. Pour de plus amples informations, consultez la section Inscription d'appareils.

Si vous choisissez d'utiliser la méthode d'invitation d'inscription, vous pouvez :

- Choisissez les modes d'inscription sécurisée **URL d'invitation**, **URL d'invitation + PIN** ou **URL d'invitation + mot de passe**.
- Utilisez n'importe quelle combinaison de modes.
- Activez ou désactivez les modes à partir de la page **Paramètres** de Citrix Endpoint Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour de plus amples informations sur chaque mode d'inscription sécurisée, consultez la section Configurer les modes d'inscription sécurisée.

Les invitations servent à plusieurs fins. L'utilisation la plus courante des invitations consiste à informer les utilisateurs que le système est disponible et qu'ils peuvent s'inscrire. Les URL d'invitation sont uniques. Une fois qu'un utilisateur a utilisé une URL d'invitation, cette URL n'est plus disponible. Vous pouvez utiliser cette propriété pour limiter les utilisateurs ou les appareils qui s'enregistrent sur votre système.

Lors de la configuration d'un profil d'inscription, vous pouvez contrôler le nombre d'appareils que des utilisateurs spécifiques peuvent inscrire, en fonction des groupes Active Directory. Par exemple, vous pouvez autoriser un seul appareil par utilisateur pour votre service financier.

Soyez conscient des coûts supplémentaires et des problèmes de certaines options d'inscription. Envoyer des invitations à l'aide de SMTP nécessite une infrastructure supplémentaire. Pour de plus amples informations, consultez la section Notifications.

En outre, pour envoyer des invitations par e-mail, assurez-vous que les utilisateurs disposent d'un moyen d'accéder à leurs e-mails en dehors de Citrix Secure Hub. Vous pouvez utiliser des modes d'inscription sécurisée à mot de passe à usage unique (OTP) comme alternative aux mots de passe Active Directory pour l'inscription MDM.

Portail en libre-service

Les utilisateurs peuvent accéder au portail en libre-service sur la même URL que celle utilisée par les administrateurs pour accéder à la console Citrix Endpoint Management. Les utilisateurs voient le portail en libre-service au lieu de la console d'administration. Les utilisateurs peuvent télécharger Citrix Secure Hub, demander l'inscription et consulter les informations sur l'appareil à partir du portail en libre-service.

Pour configurer un portail, mettez à jour ces propriétés du serveur dans **Paramètres > Propriétés du serveur** :

- `shp.console.enable` : définissez cette propriété sur **True** pour donner accès au portail utilisateur.
- `enable.new.shp` : définissez cette propriété sur **True** pour permettre aux utilisateurs d'activer leurs appareils à partir du portail utilisateur.

Inscription manuelle

Lors de l'inscription manuelle, les utilisateurs se connectent à Citrix Endpoint Management via la détection automatique ou en entrant les informations du serveur. Si la détection automatique est activée, les utilisateurs se connectent avec uniquement leur adresse e-mail ou leurs informations d'

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

identification Active Directory au format Nom d'utilisateur principal. Si la détection automatique n'est pas activée, ils doivent entrer l'adresse du serveur et leurs informations d'identification Active Directory. Pour plus d'informations sur la configuration de la découverte automatique, consultez la section Configurer la détection automatique Citrix Endpoint Management.

Vous pouvez faciliter l'inscription manuelle de plusieurs façons. Vous pouvez créer un guide, le distribuer aux utilisateurs et leur demander de s'inscrire eux-mêmes. Vous pouvez demander à votre département informatique d'inscrire manuellement des groupes d'utilisateurs dans certains créneaux horaires. Vous pouvez utiliser n'importe quelle méthode similaire où les utilisateurs doivent entrer leurs informations d'identification ou les informations sur le serveur.

Intégration de l'utilisateur

Une fois l'environnement configuré, vous devez décider comment intégrer les utilisateurs dans votre environnement. Une section précédente de cet article traite des spécificités des modes d'inscription sécurisée des utilisateurs. Cette section traite de la manière dont vous communiquez avec les utilisateurs.

Inscription ouverte ou invitation sélective

Lors de l'intégration d'utilisateurs, vous pouvez autoriser l'inscription par deux méthodes de base :

- Inscription ouverte. Par défaut, tout utilisateur disposant d'informations d'identification LDAP et d'informations d'environnement Citrix Endpoint Management peut s'inscrire.
- Inscription limitée. Vous pouvez limiter le nombre d'utilisateurs en autorisant uniquement les utilisateurs ayant des invitations d'inscription. Vous pouvez également limiter l'inscription ouverte par un groupe Active Directory.

Avec la méthode d'invitation, vous pouvez également limiter le nombre d'appareils qu'un utilisateur peut inscrire. Dans la plupart des situations, l'inscription ouverte est acceptable, mais il y a quelques points à considérer :

- Pour l'inscription MAM, vous pouvez facilement limiter l'inscription ouverte via l'appartenance à un groupe Active Directory.
- Pour l'inscription MDM, vous pouvez limiter le nombre d'appareils pouvant s'inscrire en fonction de l'appartenance à un groupe Active Directory. Si vous autorisez uniquement les appareils d'entreprise dans votre environnement, cette limitation ne pose normalement pas de problème. Toutefois, vous pouvez envisager cette méthode dans un environnement de travail BYOD dans lequel vous souhaitez limiter le nombre d'appareils.

L'invitation sélective est généralement effectuée moins souvent car elle nécessite un peu plus de travail que l'inscription ouverte. Pour que les utilisateurs puissent inscrire leurs appareils dans votre

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

environnement, vous devez envoyer une invitation unique à chaque utilisateur. Pour plus d'informations sur l'envoi d'une invitation d'inscription, reportez-vous à la section Invitations d'inscription.

Envoyez une invitation pour chaque utilisateur ou groupe que vous souhaitez inscrire dans votre environnement. Ce processus peut prendre beaucoup de temps en fonction de la taille de votre organisation. Il est possible d'utiliser des groupes Active Directory pour créer des invitations par lots, mais vous devez effectuer cette approche par vagues.

Premier contact avec les utilisateurs

Après avoir décidé d'utiliser l'inscription ouverte ou l'invitation sélective et configuré ces environnements, informez les utilisateurs de leurs options d'inscription.

Si vous utilisez la méthode d'invitation sélective, les e-mails font partie du processus. Vous pouvez également envoyer des e-mails via la console Citrix Endpoint Management pour une inscription ouverte. Pour de plus amples informations, consultez la section Invitations d'inscription.

Dans les deux cas, notez que vous avez besoin d'un serveur SMTP pour les e-mails. Cela peut occasionner des coûts supplémentaires à prendre en compte lors de votre prise de décision. Réfléchissez à la manière dont les nouveaux utilisateurs accèdent aux informations. Si vous souhaitez que tous les utilisateurs accèdent à leurs e-mails via Citrix Endpoint Management, leur envoyer un e-mail d'invitation peut être problématique.

Vous pouvez également envoyer des communications par un autre moyen en dehors de Citrix Endpoint Management pour un environnement d'inscription ouvert. Pour cette option, assurez-vous d'inclure toutes les informations pertinentes. Indiquez aux utilisateurs où ils peuvent obtenir l'application Citrix Secure Hub et quelle méthode utiliser pour s'inscrire. Si la détection est désactivée, fournissez également aux utilisateurs l'adresse du serveur Citrix Endpoint Management. Pour en savoir plus sur la découverte, voir Configurer la détection automatique Citrix Endpoint Management.

Provisioning et deprovisioning d'applications

March 1, 2024

Le provisioning des applications s'articule autour de la gestion du cycle de vie des applications mobiles : préparer, configurer, distribuer et gérer des applications mobiles dans un environnement Citrix Endpoint Management. Dans certains cas, le développement ou la modification du code d'application peut également faire partie du processus de provisioning. Citrix Endpoint Management est équipé de divers outils et processus que vous pouvez utiliser pour le provisioning d'applications.

Avant de lire cet article sur le provisioning des applications, nous vous recommandons de lire Applications et Communautés d'utilisateurs. Lorsque vous avez finalisé le type d'applications que votre

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

organisation prévoit d'offrir aux utilisateurs, vous pouvez définir le processus de gestion des applications tout au long de leur cycle de vie.

Tenez compte des points suivants lors de la définition du processus de provisioning de votre application :

- **Profilage des applications :** votre organisation peut commencer par un nombre limité d'applications. Toutefois, le nombre d'applications que vous gérez peut augmenter rapidement à mesure que les taux d'adoption par les utilisateurs augmentent et que votre environnement se développe. Définissez des profils d'application spécifiques à l'avance afin de simplifier le provisioning des applications. Le profilage des applications vous permet de catégoriser les applications en groupes logiques d'un point de vue non technique. Par exemple, vous pouvez créer des profils d'application en fonction des facteurs suivants :
  - Version : version de l'application pour le suivi
  - Instances : plusieurs instances déployées pour différents ensembles d'utilisateurs, par exemple avec différents niveaux d'accès
  - Plate-forme : iOS, Android ou Windows
  - Public cible : utilisateurs standard, départements, cadres de niveau C
  - Propriété : département propriétaire de l'application
  - Type : MDX, Public, Web et SaaS, ou liens Web
  - Cycle de mise à niveau : fréquence à laquelle l'application est mise à niveau
  - Licences : exigences en matière de licence et propriété
  - Stratégies SDK MAM ou MDX : pour appliquer des fonctionnalités MDX à vos applications mobiles
  - Accès réseau : type d'accès, tel que le tunneling du trafic HTTP et HTTPS avec une authentification unique (Tunnel - SSO Web).

Exemple :

Facteur	Citrix Secure Mail	E-mail	En interne	Epic Rover
Version	10.1	10.1	X.x	X.x
Instance	VIP	Médecins	Personnel médical	Personnel médical
Plateforme	iOS	iOS	iOS	iOS
Utilisateurs cible	Utilisateurs VIP	Médecins	Personnel médical	Personnel médical
Appartenance	Département informatique	Département informatique	Département informatique	Département informatique
Type	MDX	MDX	Natif	Public

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Facteur	Citrix Secure Mail	E-mail	En interne	Epic Rover
Cycle de mise à niveau	Trimestriel	Trimestriel	Annuel	S/O
Gestion des licences	S/O	S/O	S/O	Achat en volume
Stratégies MDX	Oui	Oui	Oui	Non
Accès réseau	VPN	VPN	VPN	Public

- **Gestion des versions des applications :** la gestion et le suivi des versions des applications constituent un élément essentiel du processus de provisioning. La gestion des versions est généralement transparente pour les utilisateurs. Ils ne reçoivent des notifications que lorsqu'une nouvelle version de l'application est disponible en téléchargement. De votre point de vue, la vérification et le test de chaque version de l'application dans une capacité de non-production est également essentiel afin d'éviter l'impact sur le site de production.

  Il est également important d'évaluer si une mise à niveau spécifique est requise. Les mises à niveau des applications sont généralement de deux types : une mise à niveau mineure, comme la correction d'un bug spécifique, ou une version majeure, qui introduit des changements significatifs. Dans les deux cas, examinez attentivement les notes de publication de l'application pour évaluer si la mise à niveau est nécessaire.

- **Développement d'applications :** lorsque vous intégrez le SDK MAM dans les applications mobiles que vous développez, vous appliquez des fonctionnalités MDX à ces applications. Consultez la section Présentation du SDK MAM.

  Le SDK MAM remplace l'outil MDX Toolkit, dont la fin de prise en charge est prévue en juillet 2023. Pour de plus amples informations sur l'encapsulation d'applications, consultez la section MDX Toolkit. Le processus de provisioning d'application pour une application encapsulée est différent du processus de provisioning pour une application standard non encapsulée.

- **Sécurité de l'application :** vous définissez les exigences en matière de sécurité des applications individuelles ou des profils d'application dans le cadre du processus de provisioning. Vous pouvez mapper des exigences de sécurité à des stratégies MDM ou MAM spécifiques avant de déployer les applications. Cette planification simplifie et accélère le déploiement des applications. Par exemple :

  - Vous pouvez déployer certaines applications différemment.
  - Il peut être utile d'apporter des modifications architecturales à votre environnement Citrix Endpoint Management. Les modifications dépendent du type de conformité de sécurité requis par les applications. Par exemple, une application particulière peut nécessiter un cryptage SSL de bout en bout ou un géofencing.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Mise à disposition de l'application :** Citrix Endpoint Management vous permet de mettre à disposition des applications en tant qu'applications MDM, ou en tant qu'applications MAM. Les applications MDM apparaissent dans l'App Store. Ce magasin vous permet de fournir facilement des applications publiques ou natives aux utilisateurs. En dehors de la mise en œuvre de restrictions au niveau de l'appareil, aucun autre contrôle d'application n'est nécessaire. En revanche, la mise à disposition des applications à l'aide de MAM permet un contrôle total sur la mise à disposition de l'application et sur l'application elle-même. La mise à disposition des applications via MAM est généralement la meilleure solution.
- **Maintenance de l'application :**
  - Effectuer un audit initial : effectuez le suivi de la version de l'application présente dans votre environnement de production, ainsi que le dernier cycle de mise à niveau. Prenez note des fonctionnalités spécifiques ou des corrections de bogues qui ont nécessité la mise à niveau.
  - Établir des références : conservez une liste des dernières versions stables de chaque application. Préparez-vous à revenir à une version antérieure de l'application en cas de problèmes inattendus après la mise à niveau. Élaborer un plan de restauration. Tester les mises à niveau d'application dans un environnement de test avant de les déployer en production. Si possible, déployer la mise à niveau vers un sous-ensemble d'utilisateurs de production d'abord, puis vers l'ensemble de la base d'utilisateurs.
  - S'abonner aux notifications de mises à jour logicielles Citrix et à toutes les notifications de fournisseurs de logiciels tiers : ceci est essentiel pour rester à jour avec les dernières versions des applications. Une version EAR (Early Access Release) peut être disponible pour les tests à l'avance.
  - Concevoir une stratégie pour informer les utilisateurs : définir une stratégie pour informer les utilisateurs lorsque des mises à niveau d'application sont disponibles. Préparer les utilisateurs avec une formation avant le déploiement. Envisagez d'envoyer plusieurs notifications avant de mettre à jour l'application. Selon l'application, la meilleure méthode de notification peut être des notifications par e-mail ou des sites Web.

La gestion du cycle de vie de l'application implique le cycle de vie complet d'une application depuis son déploiement initial jusqu'à sa mise hors service. Le cycle de vie d'une application comporte les phases suivantes :

1. Configuration requise pour les spécifications : commencez par l'analyse de rentabilisation et les exigences de l'utilisateur.
2. Développement : vérifiez que l'application répond aux besoins de l'entreprise.
3. Test : identifiez les utilisateurs de test, les problèmes et les bogues.
4. Déploiement : déployez l'application aux utilisateurs de production.
5. Maintenance : mettez à jour de la version de l'application. Déployez l'application dans un environnement de test avant de mettre à jour l'application dans un environnement de production.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opérations basées sur le tableau de bord

March 1, 2024

Vous pouvez afficher un synopsis des informations en accédant au tableau de bord de votre console Citrix Endpoint Management. Avec ces informations, vous pouvez voir un aperçu rapide des problèmes et des résolutions en utilisant des widgets.

Le tableau de bord est généralement l'écran qui s'affiche lorsque vous vous connectez à la console Citrix Endpoint Management. Pour accéder au tableau de bord ailleurs dans la console, cliquez sur **Analyser**. Cliquez sur **Personnaliser** dans le tableau de bord pour modifier la configuration de la page et pour modifier les widgets qui s'affichent.

- **Mes tableaux de bord :** vous pouvez enregistrer jusqu'à quatre tableaux de bord. Vous pouvez modifier ces tableaux de bord séparément et afficher chacun d'entre eux en sélectionnant le tableau de bord enregistré.
- **Disposition :** dans cette ligne, vous pouvez sélectionner le nombre de widgets qui s'affichent sur votre tableau de bord et la manière dont les widgets sont disposés.
- **Sélection des widgets :** vous pouvez choisir les informations qui s'affichent dans votre tableau de bord.
  - **Notifications :** cochez la case au-dessus des chiffres sur la gauche pour ajouter une barre Notifications au-dessus de vos widgets. Cette barre affiche le nombre d'appareils compatibles, d'appareils inactifs et d'appareils effacés ou inscrits dans les dernières 24 heures.
  - **Appareils par plate-forme :** affiche le nombre d'appareils gérés et non gérés par plate-forme.
  - **Appareils par opérateurs :** affiche le nombre d'appareils gérés et non gérés par opérateur. Cliquez sur chaque barre pour afficher la répartition par plate-forme.
  - **Appareils gérés par plate-forme :** affiche le nombre d'appareils gérés par plate-forme.
  - **Appareils non gérés par plate-forme :** affiche le nombre d'appareils non gérés par plate-forme. Les appareils qui s'affichent dans ce graphique peuvent avoir un agent installé, mais leurs privilèges ont été révoqués ou ils ont été effacés.
  - **Appareils par état ActiveSync Gateway :** affiche le nombre d'appareils regroupés par état ActiveSync Gateway. Les informations affichent l'état Inconnu, Autorisé ou Bloqué. Vous pouvez cliquer sur chaque barre pour décomposer les données par plate-forme.
  - **Appareils par appartenance :** affiche le nombre d'appareils regroupés par état d'appartenance. Les informations affichent l'état Appartenant à la société, Appartenant à l'employé ou Inconnu.
  - **Déploiements de groupes de mise à disposition ayant échoué :** affiche le nombre total d'échecs de déploiements par package. Seuls les packages avec des échecs de déploiements s'affichent.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Appareils par motif de blocage :** affiche le nombre d'appareils bloqués par ActiveSync
  - **Applications installées :** ce widget vous permet d'entrer le nom d'une application pour afficher un graphique contenant des informations sur cette application.
  - **Licences utilisées par les applications d'achat en volume :** affiche des statistiques d'utilisation de licences pour les applications d'achat en volume d'Apple.

Cas d'utilisation

Voici quelques exemples de nombreuses façons d'utiliser les widgets de tableau de bord pour surveiller votre environnement.

- Vous avez déployé des applications de productivité mobiles Citrix et recevez des tickets d'assistance concernant les applications de productivité mobiles dont l'installation sur les appareils a échoué. Utilisez les widgets **Appareils non conformes** et **Applications installées** pour afficher les appareils sur lesquels les applications de productivité mobiles Citrix n'ont pas été installées.
- Vous souhaitez surveiller les appareils inactifs afin de pouvoir supprimer les appareils de votre environnement et récupérer des licences. Utilisez le widget **Appareils inactifs** pour suivre cette statistique.
- Vous recevez des tickets d'assistance concernant des données qui ne sont pas synchronisées correctement. Vous pouvez utiliser les widgets **Appareils par état ActiveSync Gateway** et **Appareils par motif de blocage** pour déterminer si le problème est lié à ActiveSync.

Rapports

Une fois votre environnement configuré et les utilisateurs inscrits, vous pouvez exécuter des rapports pour en savoir plus sur votre déploiement. Citrix Endpoint Management est équipé d'un certain nombre de rapports intégrés pour vous aider à mieux comprendre les appareils fonctionnant sur votre environnement. Pour plus de détails, consultez la section Rapports.

Contrôle d'accès basé sur les rôles et support Citrix Endpoint Management

March 1, 2024

Citrix Endpoint Management utilise le contrôle d'accès basé sur les rôles (RBAC) pour restreindre l'accès des utilisateurs et des groupes aux fonctions du système Citrix Endpoint Management, telles que la console Citrix Endpoint Management, le portail en libre-service et l'API publique. Cet article

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

décrit les rôles intégrés à Citrix Endpoint Management et inclut des notions importantes à prendre en compte pour décider d'un modèle de support pour Citrix Endpoint Management qui utilise RBAC.

Rôles intégrés

Vous pouvez modifier l'accès accordé aux rôles intégrés suivants et vous pouvez ajouter des rôles. Pour obtenir l'ensemble des autorisations d'accès et de fonctionnalité associés à chaque rôle et leurs paramètres par défaut, téléchargez Paramètres par défaut du contrôle d'accès basé sur les rôles. Pour une définition de chaque fonctionnalité, consultez la section Configuration de rôles avec RBAC.

Rôle d'administrateur

Accès par défaut accordé :

- Accès complet au système, sauf au portail en libre-service.
- Par défaut, les administrateurs peuvent effectuer certaines tâches de support, telles que la vérification de la connectivité et la création de packs d'assistance.

Considérations :

- Certains ou tous vos administrateurs ont-ils besoin d'accéder au portail en libre-service ? Si c'est le cas, vous pouvez modifier le rôle Admin ou ajouter des rôles d'administrateur.
- Pour restreindre davantage l'accès à certains administrateurs ou groupes d'administrateurs, ajoutez des rôles en fonction du modèle d'administration et modifiez les autorisations.

Utilisateur

Accès par défaut accordé :

- Accès au portail en libre-service qui permet aux utilisateurs authentifiés de générer des liens d'inscription. Les liens leur permettent d'inscrire leurs appareils ou de s'envoyer une invitation d'inscription.
- Accès restreint à la console Citrix Endpoint Management : fonctionnalités d'appareil (par exemple, réinitialisation de l'appareil, verrouillage/déverrouillage de l'appareil, verrouillage/déverrouillage du conteneur ; affichage de l'emplacement et définition des restrictions géographiques, sonnerie de l'appareil, réinitialisation du mot de passe du conteneur) ; ajout, suppression et envoi des invitations d'inscription.

Considérations :

- Le rôle d'utilisateur permet aux utilisateurs de s'aider eux-mêmes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Pour prendre en charge les appareils partagés, créez un rôle d'utilisateur pour l'inscription des appareils partagés.

Notions importantes pour un modèle de support Citrix Endpoint Management

Les modèles de support que vous pouvez adopter peuvent varier considérablement et impliquer des tierces parties gérant les niveaux 1 et 2, tandis que les employés prennent en charge les niveaux 3 et 4. Quelle que soit la manière dont vous répartissez la charge de support, gardez à l'esprit les notions de cette section spécifiques à votre déploiement et à votre base d'utilisateurs Citrix Endpoint Management.

Les utilisateurs ont-ils des appareils appartenant à l'entreprise ou BYO ?
La principale question qui influence le support est de savoir à qui appartiennent les appareils utilisateur dans votre environnement Citrix Endpoint Management. Si vos utilisateurs possèdent des appareils appartenant à l'entreprise, vous pouvez proposer un niveau de support inférieur afin de verrouiller les appareils. Dans ce cas, vous pouvez fournir un service d'assistance qui aide les utilisateurs à résoudre les problèmes liés aux appareils et à l'utilisation des appareils. En fonction des types d'appareils que vous devez prendre en charge, pensez à la manière dont vous pouvez utiliser les rôles de provisioning et de prise en charge des appareils RBAC pour votre service d'assistance.

Si vos utilisateurs disposent d'appareils BYO, votre organisation peut s'attendre à ce que les utilisateurs trouvent leurs propres sources pour la prise en charge de l'appareil. Dans ce cas, le support fourni par votre organisation est davantage un rôle administratif centré sur les problèmes spécifiques à Citrix Endpoint Management.

Quel est votre modèle de support pour les ordinateurs de bureau ?
Déterminez si votre modèle de support pour les ordinateurs de bureau est approprié pour les autres appareils appartenant à l'entreprise. Pouvez-vous utiliser la même organisation de support ? De quelle formation supplémentaire aura-t-elle besoin ?

Voulez-vous autoriser les utilisateurs à accéder au portail en libre-service Citrix Endpoint Management ?
Bien que certaines organisations préfèrent ne pas autoriser les utilisateurs à accéder à Citrix Endpoint Management, offrir aux utilisateurs des fonctionnalités d'auto-assistance peut alléger la charge de votre organisation de support. Si le rôle d'utilisateur par défaut de RBAC inclut des autorisations que vous ne souhaitez pas accorder, envisagez de créer un rôle avec uniquement les autorisations que vous souhaitez inclure. Vous pouvez créer autant de rôles que nécessaire pour répondre à vos besoins.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Processus de support Citrix

March 1, 2024

Vous pouvez activer les services de support technique Citrix pour résoudre les problèmes liés aux produits Citrix. Le groupe travaille conjointement avec les équipes de développement pour propose des solutions et des résolutions aux problèmes.

Les services de conseil, Citrix Consulting Services, ou les services de formation, Citrix Education Services, proposent une assistance liée à la formation sur les produits et des conseils sur l'utilisation, la configuration et l'installation des produits, ainsi que sur la conception et l'architecture de l'environnement.

Citrix Consulting aide les projets liés aux produits Citrix, notamment ce qui suit :

- Preuve de concept
- Évaluation de l'impact économique
- Contrôles d'intégrité de l'infrastructure
- Analyse des exigences de conception
- Vérification de la conception de l'architecture
- Intégration
- Développement des processus opérationnels

Citrix Education offre une formation et une certification informatique de premier ordre sur les technologies de virtualisation, de cloud et de réseau Citrix.

Citrix vous recommande de tirer pleinement parti des ressources d'auto-assistance et des recommandations Citrix avant de créer un ticket d'assistance. Par exemple, vous pouvez accéder à plusieurs articles et bulletins écrits par des experts techniques Citrix, consulter la documentation produit relative aux solutions et aux technologies Citrix, ou lire des conseils directs des responsables, des équipes produit et des experts techniques Citrix. Consultez les pages Centre de connaissances, Documentation produit et Blogs.

Pour une assistance plus interactive, vous pouvez participer à des forums de discussion où vous pouvez poser des questions et obtenir des réponses d'autres clients, partager des idées, des opinions, des informations techniques et des meilleures pratiques au sein de groupes d'utilisateurs et de groupes d'intérêt ou interagir avec les techniciens Citrix qui contrôlent les sites de réseaux sociaux liés au support Citrix. Consultez les pages Forums de support et Communauté Citrix.

Vous avez également accès à des cours de formation et de certification pour développer vos compétences. Consultez la page Citrix Education.

Citrix Insight Services propose une plate-forme simple de dépannage en ligne et de contrôle de l'état de votre environnement Citrix. Disponible pour Citrix Endpoint Management, Citrix Virtual Apps and

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Desktops, Citrix Hypervisor et NetScaler Gateway. Consultez la page Outil d'analyse.

Pour obtenir un support technique, vous pouvez créer un ticket d'assistance par téléphone ou via le web. Vous pouvez utiliser le site Web pour les problèmes dont le niveau de gravité est faible ou moyen et utiliser l'option de téléphone pour les problèmes dont le niveau de gravité est élevé. Pour contacter le support technique et signaler des problèmes liés à Citrix Endpoint Management, consultez Citrix Support Services.

Si vous recherchez un point de contact unique hautement qualifié avec une vaste expérience dans la distribution des solutions Citrix, Citrix Services propose un gestionnaire de relations techniques. Pour plus d'informations sur les avantages et offres de services Citrix, consultez la section Citrix Worldwide Services.

Envoi d'invitations d'inscription de groupe dans Citrix Endpoint Management

March 1, 2024

Author:
John Bartel III

Vous pouvez envoyer des invitations d'inscription à des groupe ou à des groupes imbriqués dans Citrix Endpoint Management. Les invitations d'inscription ne sont pas disponibles pour les appareils Windows.

Lors de la configuration de l'invitation de groupe, vous pouvez spécifier une ou plusieurs plates-formes d'appareil. Vous pouvez également marquer les appareils pour, par exemple, distinguer les appareils appartenant à l'entreprise des appareils appartenant aux employés. Vous définissez ensuite le type d'authentification pour les machines utilisateur.

> **Remarque :**
>
> Si vous prévoyez d'utiliser des modèles de notification personnalisés, vous devez définir les modèles avant de configurer des modes de sécurité d'inscription. Pour de plus amples informations sur les modèles de notification, consultez la section Création et mise à jour de modèles de notification.

Pour plus d'informations sur les configurations de base sur les comptes utilisateur, les rôles, les modes d'inscription sécurisée et les invitations, consultez la section Comptes utilisateur, rôles et inscription.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Étapes générales

1. Dans la console Citrix Endpoint Management, cliquez sur **Gérer > Invitations d'inscription**.
2. Cliquez sur **Ajouter** dans le coin supérieur gauche de l'écran, puis cliquez sur **Ajouter une Invitation**.
3. Cliquez sur **Groupe** dans le menu **Destinataire**.

   Cette étape vous permet de choisir une ou plusieurs plates-formes. Si vous disposez de plusieurs plates-formes de système d'exploitation au sein de votre entreprise, choisissez toutes les plates-formes. Ne désactivez la sélection de plate-forme que si vous êtes sûr qu' aucun utilisateur n'utilise la plate-forme particulière.
4. Vous pouvez choisir de marquer les appareils pendant le processus d'invitation. Choisissez **Entreprise** ou **Employé**.

   Le marquage facilite la séparation des appareils appartenant à l'entreprise et des appareils appartenant aux employés.
5. Dans la liste **Domaine**, choisissez le domaine dans lequel le groupe existe.
6. Dans la liste **Groupe**, sélectionnez le groupe Active Directory auquel vous souhaitez envoyer les invitations.
7. L'option **Mode d'inscription** vous permet de définir le type d'inscription sécurisée que vous préférez pour les utilisateurs.

   - Nom d'utilisateur + mot de passe
   - Haute sécurité
   - URL d'invitation
   - URL d'invitation + PIN
   - URL d'invitation + mot de passe
   - Deux facteurs
   - Nom d'utilisateur + PIN

   > **Remarque :**
   >
   > Le mode d'inscription sécurisée **Haute sécurité** n'est plus pris en charge. Pour envoyer des invitations d'inscription, vous pouvez uniquement utiliser les modes d'inscription sécurisée **URL d'invitation**, **URL d'invitation + PIN** ou **URL d'invitation + mot de passe**. Pour les appareils qui sont inscrits avec **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + PIN**, les utilisateurs doivent télécharger Citrix Secure Hub et entrer manuellement leurs informations d'identification.
8. Pour les modèles **Téléchargement de l'agent**, **URL d'inscription**, **Code PIN d'inscription** et **Confirmation d'inscription**, choisissez le modèle de notification personnalisé que vous avez créé antérieurement. Ou choisissez la valeur par défaut qui est répertorié.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour ces modèles de notification , utilisez votre configuré SMTP serveur configuration dans Citrix Endpoint Management . Définissez d'abord vos informations SMTP avant de poursuivre.

> **Remarque :**
>
> Les options **Expire après** et **Nbre max de tentatives** varient en fonction de l'option **Mode d'inscription** que vous choisissez. Vous ne pouvez pas modifier ces options.

9. Sélectionnez Activé pour **Envoyer invitation**, puis cliquez sur **Enregistrer et envoyer** pour terminer le processus.

Prise en charge des groupes imbriqués

Vous pouvez utiliser des groupes imbriqués pour envoyer des invitations. Généralement, les groupes imbriqués sont utilisés dans des environnements à grande échelle dans lesquels des groupes ayant des autorisations similaires sont liés entre eux.

Accédez à **Paramètres > LDAP** puis à activer l'option **Prendre en charge les groupes imbriqués**.

Dépannage et limitations connues

Problème : des invitations sont envoyées aux utilisateurs même s'ils ont été supprimés d'un groupe Active Directory.

Solution : selon la taille de votre environnement Active Directory, la propagation des modifications à tous les serveurs peut prendre jusqu'à six heures. Si un utilisateur ou un groupe imbriqué est récemment supprimé, Citrix Endpoint Management peut toujours considérer ces utilisateurs comme faisant partie du groupe.

Par conséquent, il est préférable d'attendre jusqu'à six heures avant d'envoyer une autre invitation de groupe à vos utilisateurs.

Configuration de l'authentification basée sur certificat pour EWS pour les notifications push de Citrix Secure Mail

March 1, 2024

Pour que les notifications push Citrix Secure Mail fonctionnent, vous devez effectuer les opérations suivantes :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Configurez Exchange Server pour l'authentification basée sur les certificats. Cette exigence est particulièrement nécessaire lorsque Citrix Secure Hub est inscrit dans Citrix Endpoint Management avec l'authentification basée sur certificat.
- Configurez le répertoire virtuel Active Sync et Exchange Web Services (EWS) sur le serveur de messagerie Exchange avec l'authentification basée sur certificat.

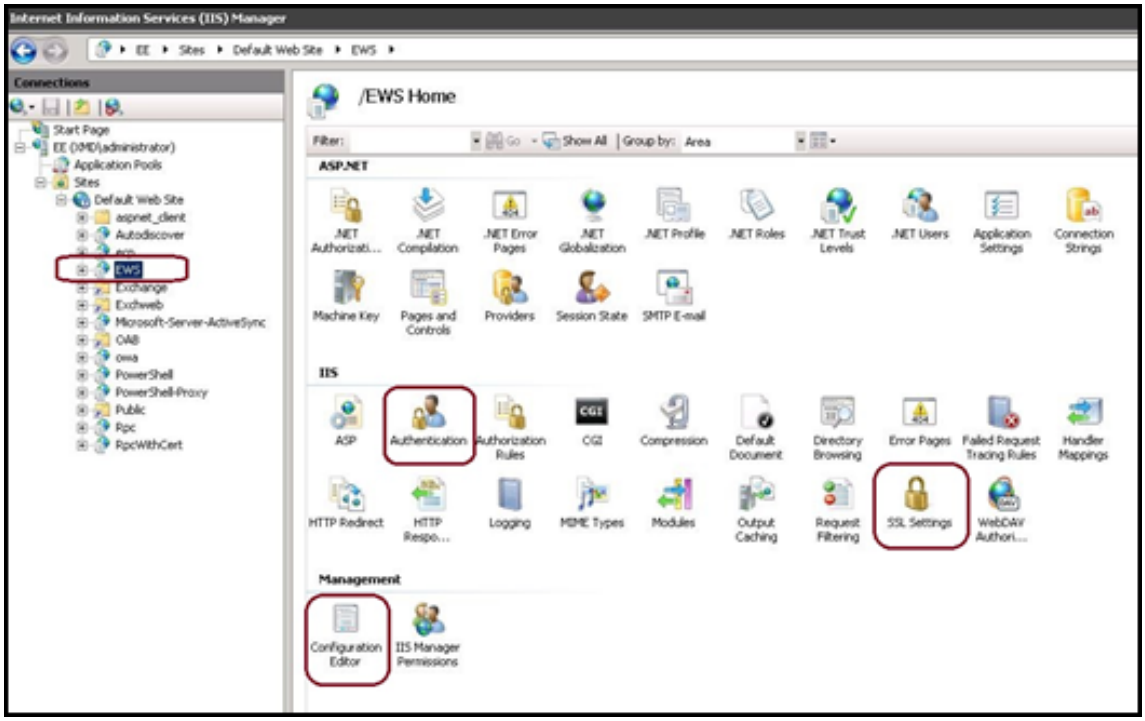
Si vous ne terminez pas ces configurations, l'abonnement aux notifications push de Citrix Secure Mail échoue et aucune mise à jour de badge ne se produit dans Citrix Secure Mail.

Cet article décrit les étapes pour configurer l'authentification basée sur certificat. Les configurations sont spécifiquement conçues pour le répertoire virtuel EWS sur Exchange Server.

Pour commencer la configuration, procédez comme suit :

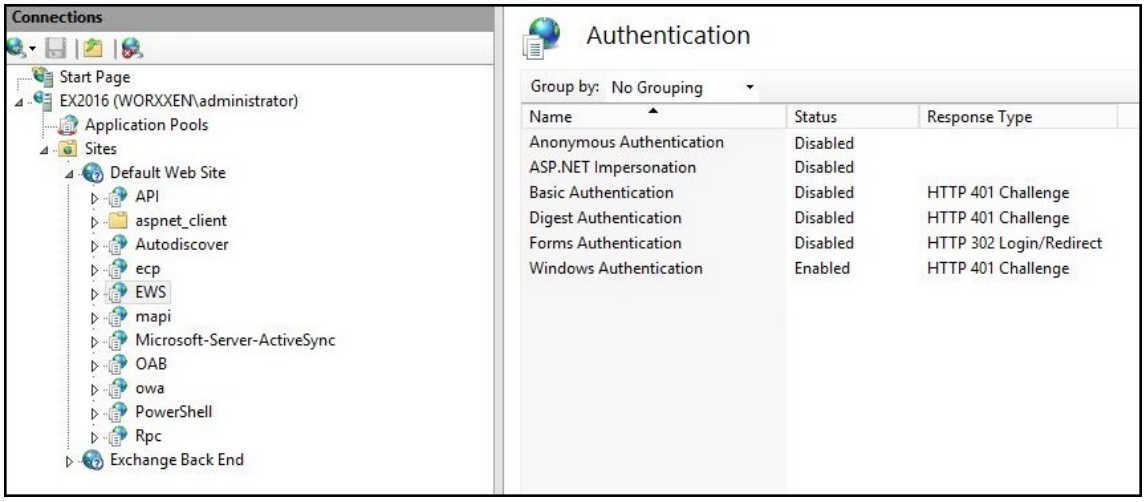
1. Connectez-vous au serveur ou aux serveurs sur lesquels le répertoire virtuel EWS est installé.
2. Ouvrez la console du gestionnaire IIS.
3. Sous **Site Web par défaut**, cliquez sur le répertoire virtuel EWS.

   Les composants logiciels enfichables Authentification, SSL et Éditeur de configuration sont situés sur le côté droit de la console du gestionnaire IIS.



4. Assurez-vous que les paramètres **Authentification** pour EWS sont configurés comme indiqué dans la figure suivante.

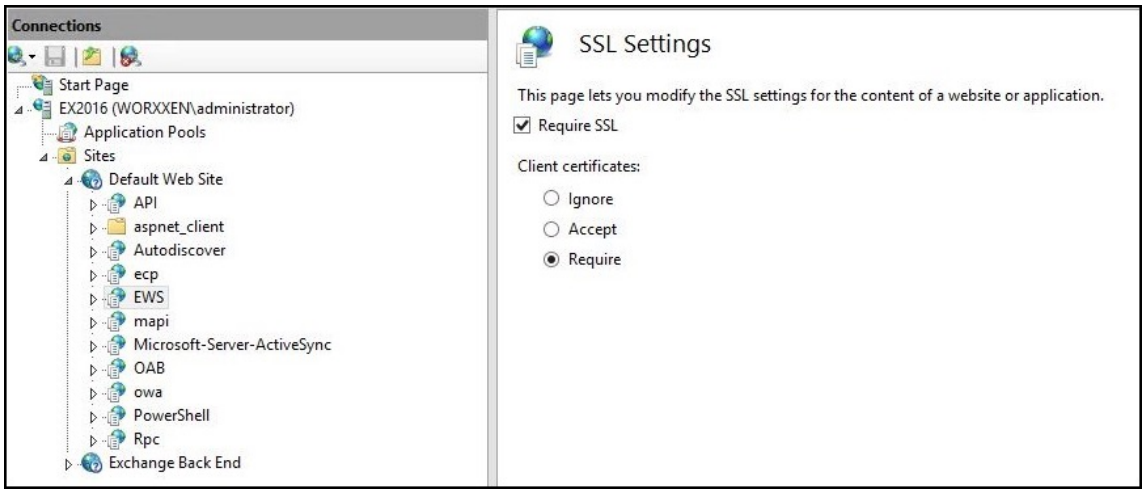
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Configurez **Paramètres SSL** pour le répertoire virtuel EWS.

   a) Sélectionnez la case à cocher **Exiger SSL**.

   b) Sous **Certificats clients**, cliquez sur **Exiger**. Ou, si d'autres clients de messagerie EWS utilisent un nom d'utilisateur et un mot de passe pour s'authentifier auprès du Exchange Server, cliquez sur **Accepter**.

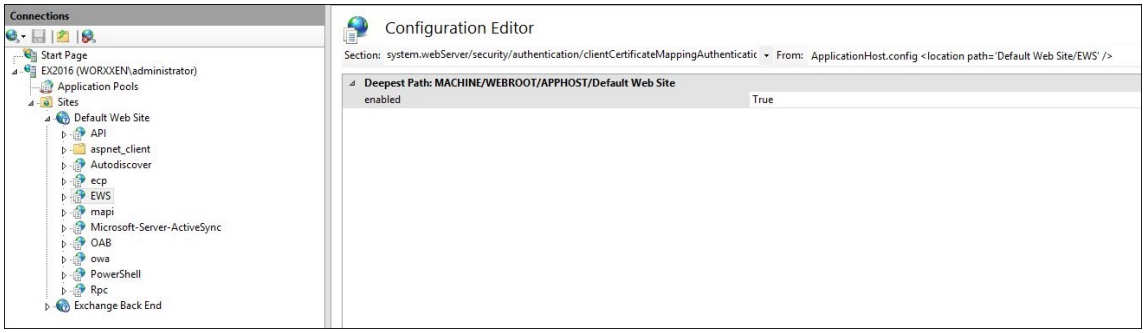


6. Cliquez sur **Éditeur de configuration**. Accédez à la section suivante dans la liste déroulante **Section** :

   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. Définissez la valeur **enabled** sur **True**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



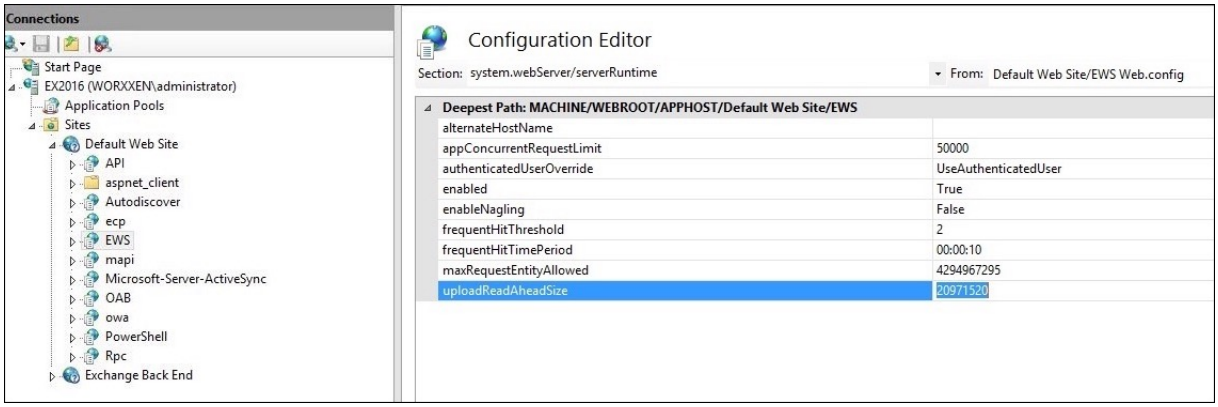
8. Cliquez sur **Éditeur de configuration**. Accédez à la section suivante dans la liste déroulante **Section** :

   - **system.webServer/serverRuntime**

9. Définissez la valeur **uploadReadAheadSize** sur **10485760** (10 Mo) ou **20971520** (20 Mo) ou sur la valeur requise par votre organisation.

   > **Important :**
   >
   > Si vous ne définissez pas cette valeur correctement, l'authentification basée sur certificat lors de l'abonnement aux notifications push EWS peut échouer avec un code d'erreur 413.
   >
   > Ne définissez pas cette valeur sur **0**.

Pour plus d'informations, consultez l'article Microsoft, Microsoft IIS Server Runtime.



Pour plus d'informations sur le dépannage des problèmes de Citrix Secure Mail avec les notifications push iOS, consultez cet article du Centre de connaissances du support Citrix.

Informations connexes

Notifications push pour Citrix Secure Mail pour iOS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration d'un serveur d'attestation de l'intégrité des appareils sur site

March 1, 2024

Vous pouvez activer l'attestation de l'intégrité des appareils (DHA) pour appareils mobiles Windows 10 et Windows 11 via un serveur Windows local. Pour activer DHA sur site, vous devez d'abord configurer un serveur DHA.

Après la configuration d'un serveur DHA, vous devez créer une stratégie Citrix Endpoint Management pour activer le service DHA sur site. Pour plus d'informations sur la création de cette stratégie, consultez la section Stratégie d'attestation de l'intégrité des appareils.

Configuration requise pour un serveur DHA

- Un serveur exécutant Windows Server Technical Preview 5 ou version ultérieure, installé à l'aide de l'option d'installation de Desktop Experience.
- Une ou plusieurs machines clientes Windows 10 et Windows 11. Ces machines doivent avoir TPM 1.2 ou 2.0 exécutant la dernière version de Windows.
- Ces certificats :
  - **Certificat SSL DHA :** un certificat SSL x.509 qui s'enchaîne à une racine de confiance d'entreprise avec une clé privée exportable. Ce certificat protège les communications de données DHA en transit, y compris :
    - communications serveur à serveur (service DHA et serveur MDM)
    - communications serveur à client (service DHA et appareil Windows 10 ou Windows 11)
  - **Certificat de signature DHA :** un certificat x.509 qui est lié à la racine de confiance d'entreprise avec une clé privée exportable. Le service DHA utilise ce certificat pour la signature numérique.
  - **Certificat de cryptage DHA :** un certificat x.509 qui est lié à la racine de confiance d'entreprise avec une clé privée exportable. Le service DHA utilise également ce certificat pour le cryptage.
- Choisissez l'un de ces modes de validation de certificat :
  - **EKCert :** le mode de validation EKCert est optimisé pour les appareils des organisations qui ne sont pas connectées à Internet. Les appareils qui se connectent à un service DHA s'exécutant en mode de validation EKCert n'ont pas d'accès direct à Internet.
  - **AIKCert :** le mode de validation AIKCert est optimisé pour les environnements opérationnels qui ont accès à Internet. Les appareils qui se connectent à un service DHA s'

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

exécutant en mode de validation AIKCert doivent avoir un accès direct à Internet et pouvoir obtenir un certificat AIK auprès de Microsoft.

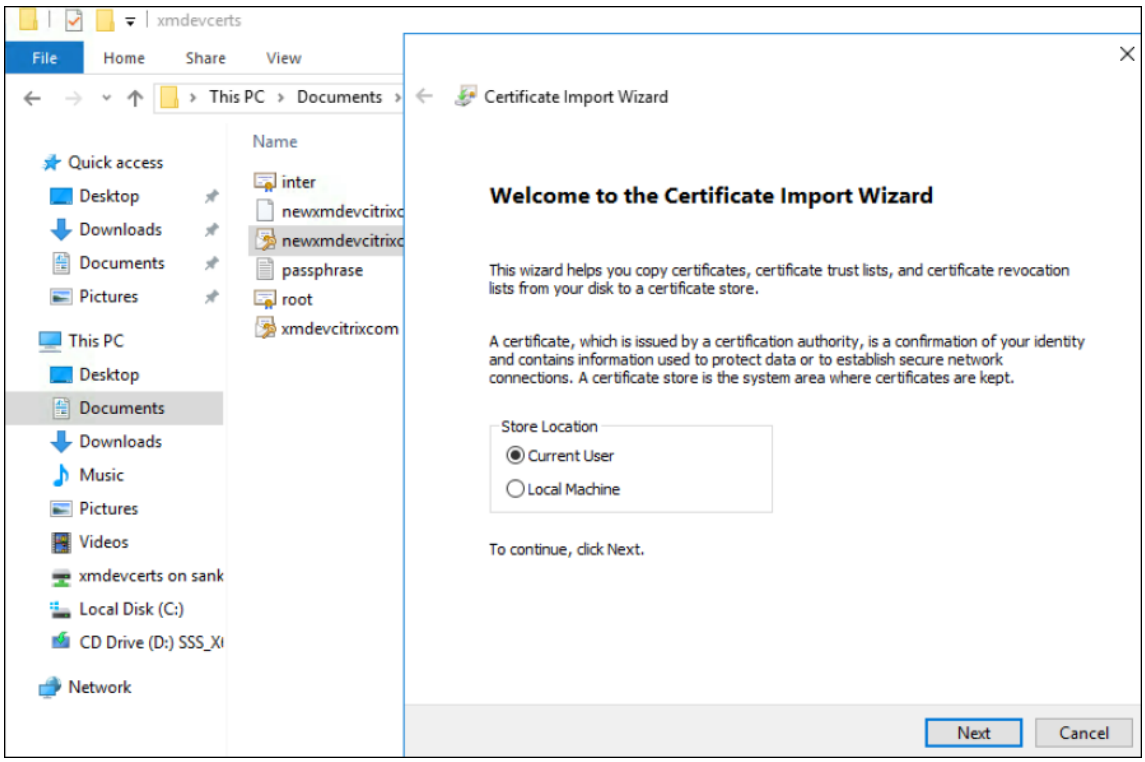
Ajouter le rôle de serveur DHA au serveur Windows

1. Sur le serveur Windows, si le Gestionnaire de serveur n'est pas déjà ouvert, cliquez sur **Démarrer**, puis sur **Gestionnaire de serveur**.
2. Cliquez sur **Ajouter des rôles et fonctionnalités**.
3. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Sélectionner un serveur du pool de serveurs**, sélectionnez le serveur, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner le rôle de serveur**, cochez la case **Attestation d'intégrité de l'appareil**.
7. Facultatif : cliquez sur **Ajouter les fonctionnalités** pour installer d'autres services et fonctionnalités de rôle requis.
8. Cliquez sur **Suivant**.
9. Sur la page **Sélectionner une fonctionnalité**, cliquez sur **Suivant**.
10. Sur la page **Rôle Serveur Web (IIS)**, cliquez sur **Suivant**.
11. Sur la page **Sélectionner les services de rôle**, cliquez sur **Suivant**.
12. Sur la page **Service d'attestation d'intégrité de l'appareil**, cliquez sur **Suivant**.
13. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
14. Une fois l'installation terminée, cliquez sur **Fermer**.

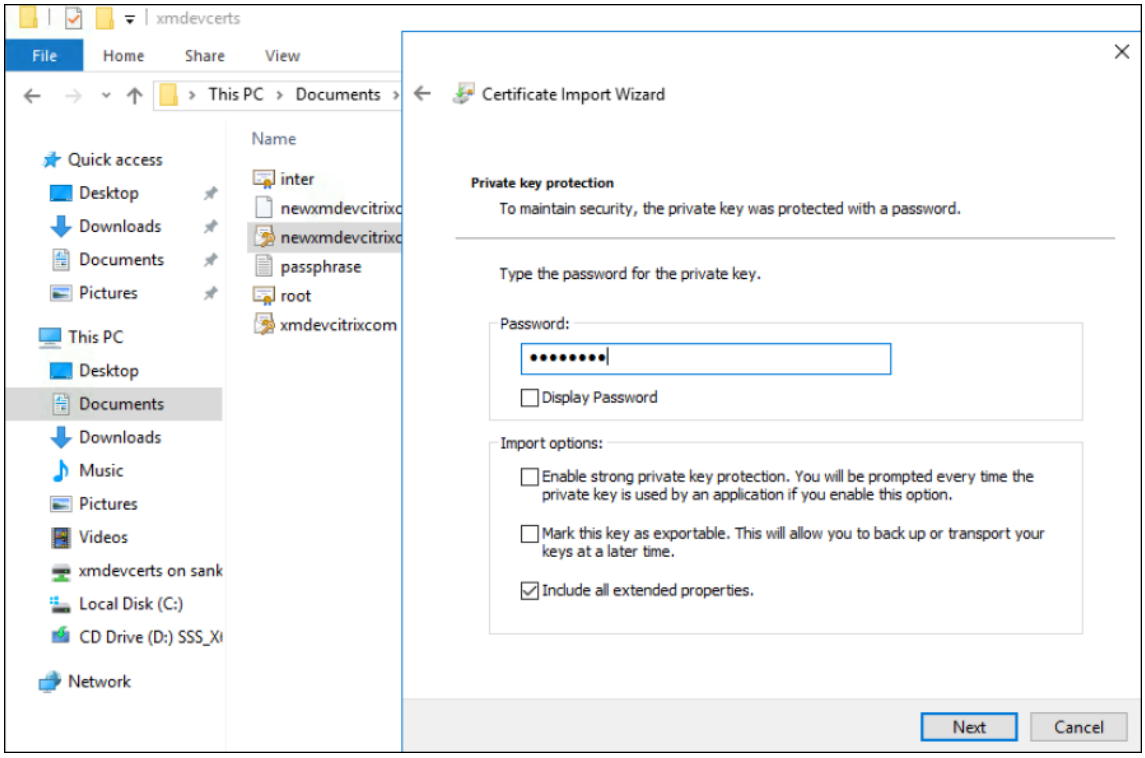
Ajouter le certificat SSL au magasin de certificats du serveur

1. Accédez au fichier de certificat SSL et sélectionnez-le.
2. Pour l'emplacement du magasin, sélectionnez **Utilisateur actuel**, puis cliquez sur **Suivant**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

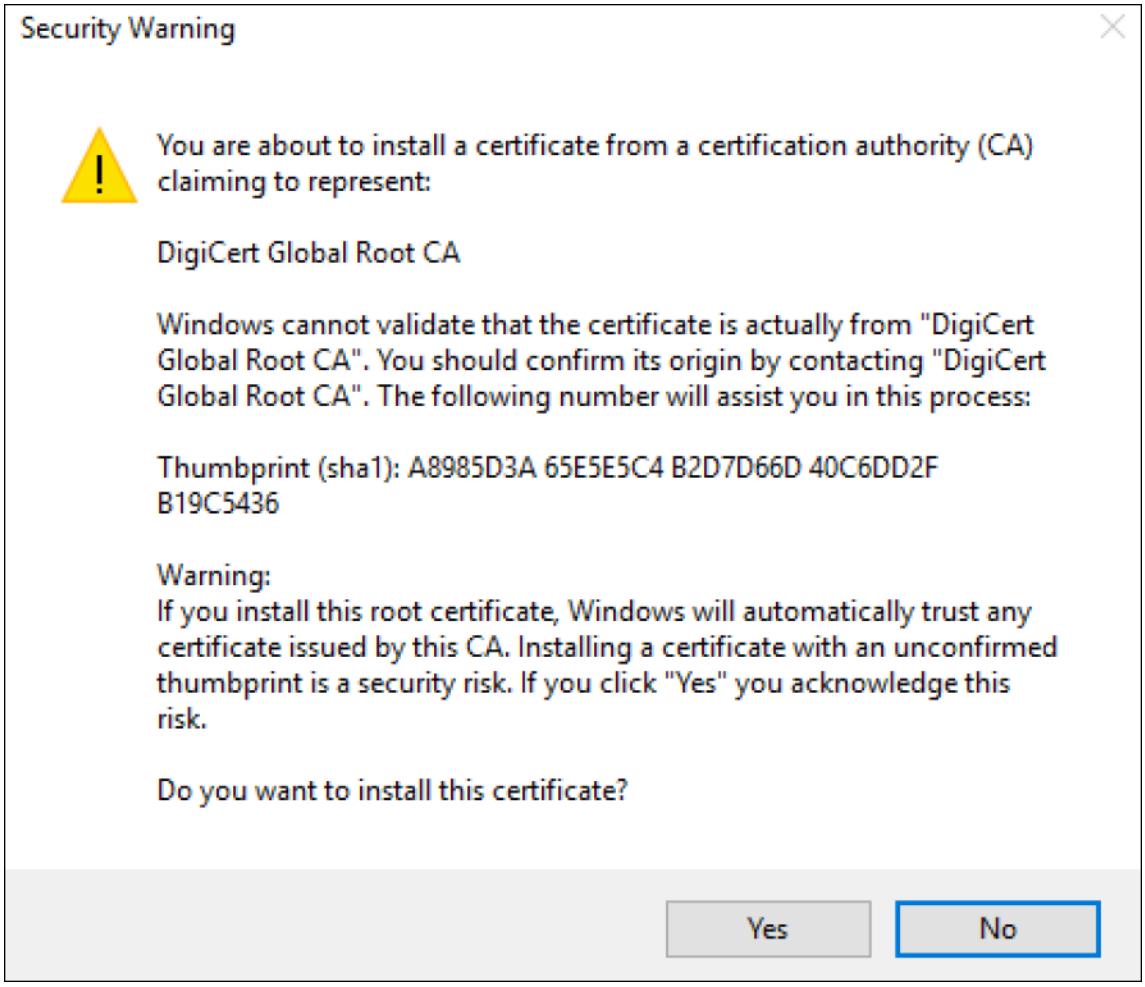


3. Tapez le mot de passe affecté à la clé privée.
4. Assurez-vous que l'option d'importation **Inclure toutes les propriétés étendues** est sélectionnée. Cliquez sur **Suivant**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Lorsque cette fenêtre s'affiche, cliquez sur **Oui**.



6. Vérifiez que le certificat est installé :

   a) Ouvrez une fenêtre d'invite de commandes.

   b) Tapez `mmc` et appuyez sur la touche **Entrée**. Pour afficher les certificats dans le magasin de machines local, vous devez être dans le rôle Administrateur.

   c) Dans le menu Fichier, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.

   d) Cliquez sur **Ajouter**.

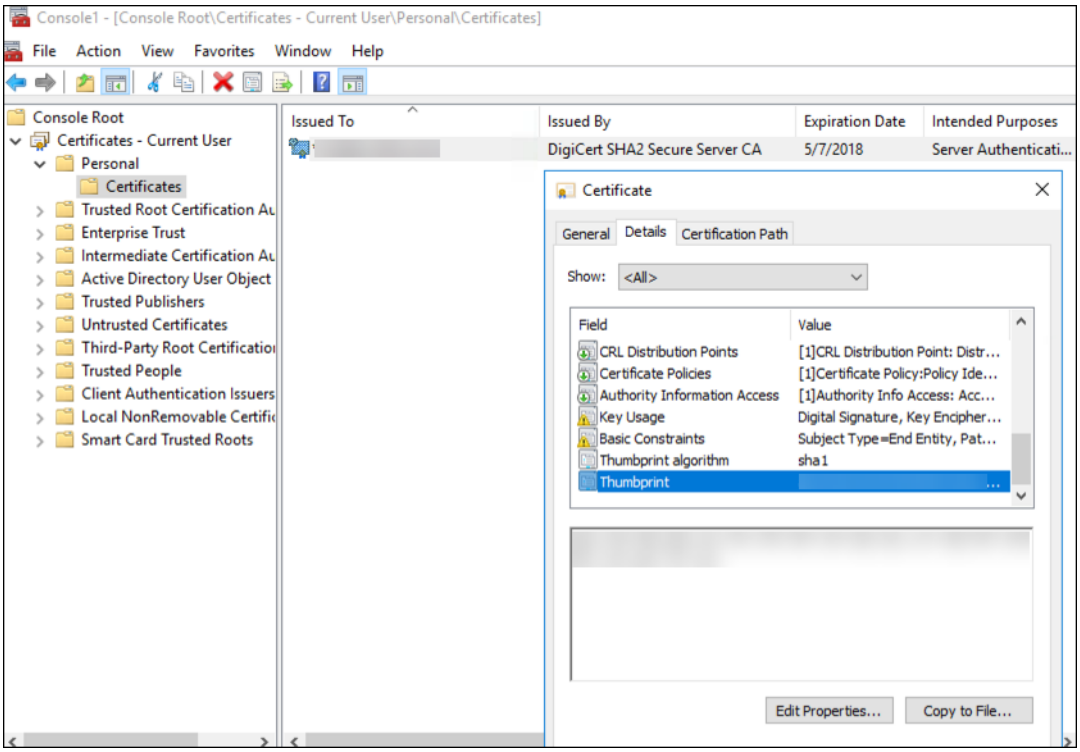
   e) Dans la boîte de dialogue Ajout d'un composant logiciel enfichable autonome, sélectionnez **Certificats**.

   f) Cliquez sur **Ajouter**.

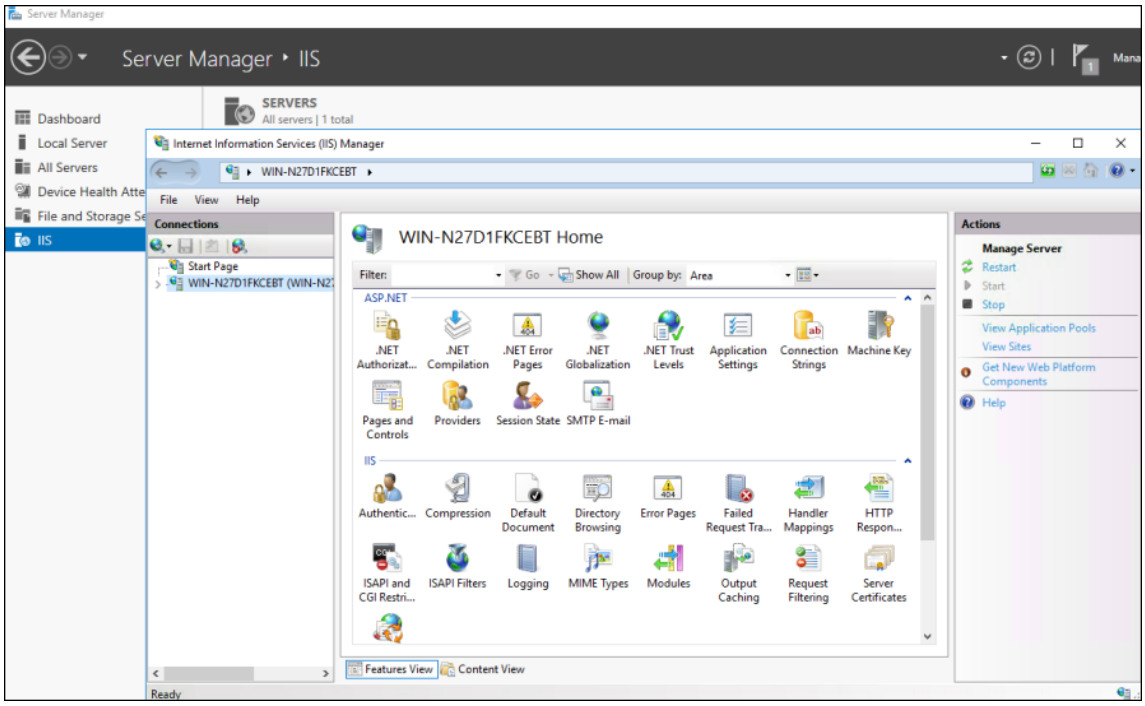
   g) Dans la boîte de dialogue Composant logiciel enfichable Certificats, sélectionnez **Mon compte d'utilisateur**. (Si vous êtes connecté en tant que titulaire d'un compte de service, sélectionnez **Compte de service**.)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

h) Dans la boîte de dialogue Sélectionner un ordinateur, cliquez sur **Terminer**.

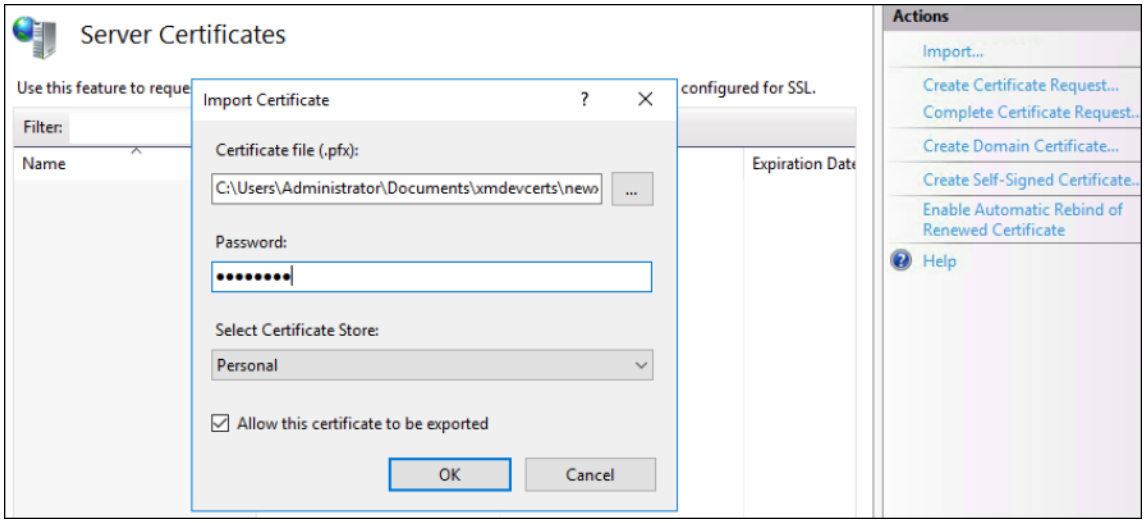


7. Accédez à **Gestionnaire de serveur > IIS** et sélectionnez **Certificats de serveur** dans la liste des icônes.



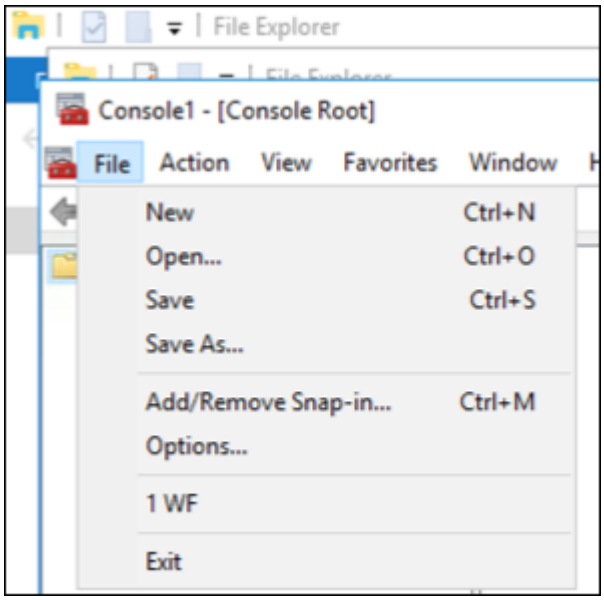
8. À partir du menu Action, sélectionnez **Importer...** pour importer le certificat SSL.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



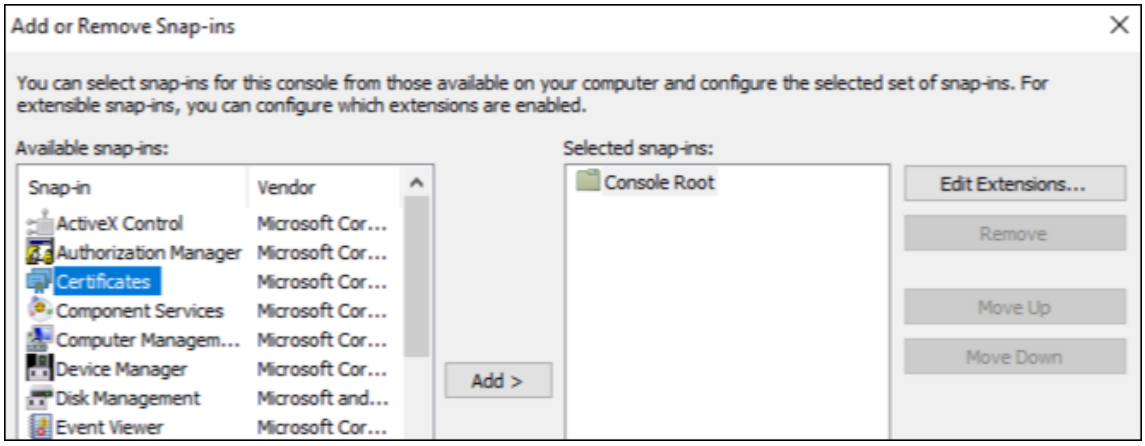
Récupérer et enregistrer l'empreinte numérique du certificat

1. Dans la barre de recherche Explorateur de fichiers, tapez `mmc`.
2. Dans la fenêtre Racine de la console, cliquez sur **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.

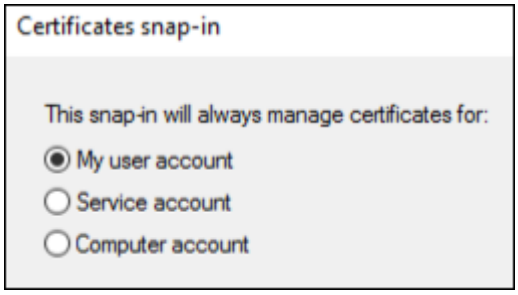


3. Sélectionnez le certificat d'un composant logiciel enfichable disponible et ajoutez-le aux composants logiciels enfichables sélectionnés.

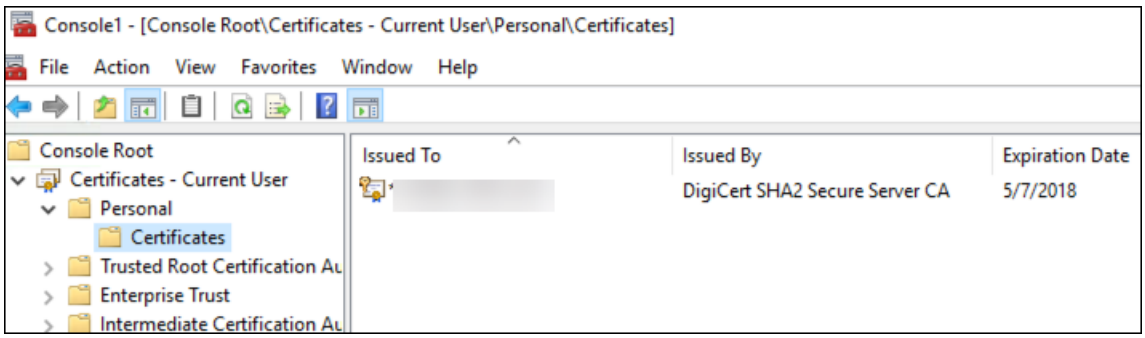
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Sélectionnez **Mon compte d'utilisateur**.

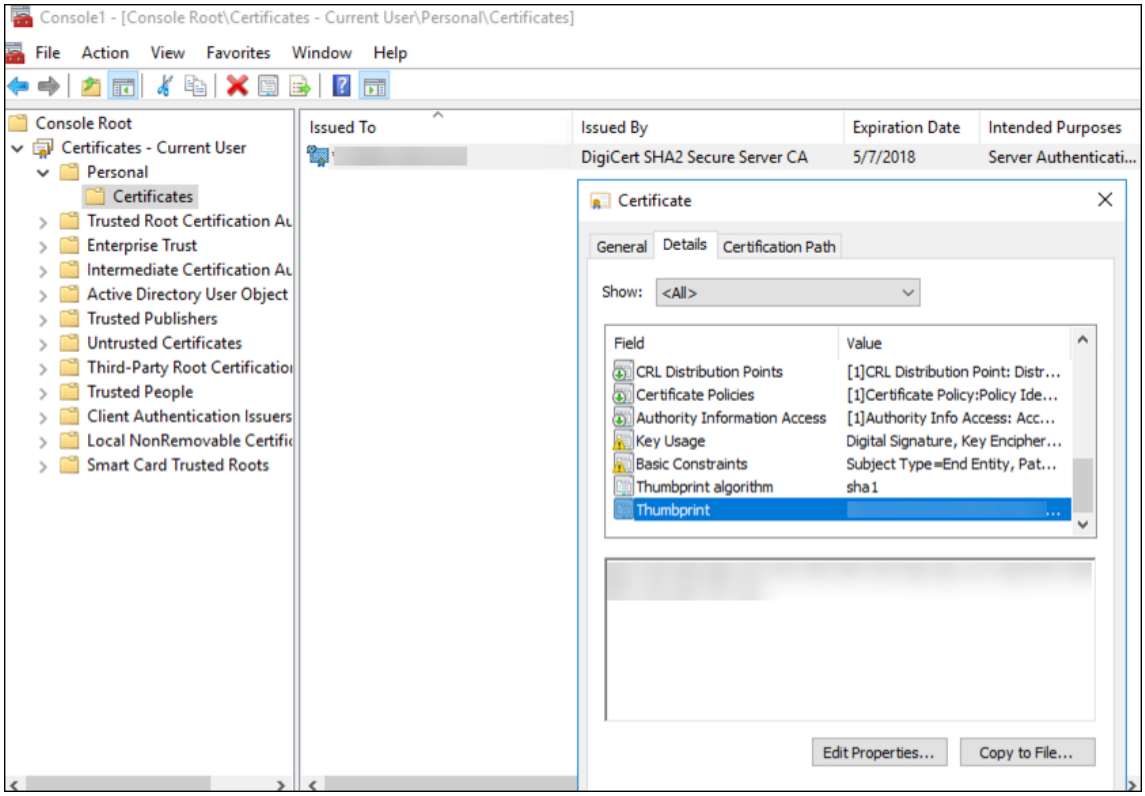


5. Sélectionnez le certificat et cliquez sur **OK**.



6. Cliquez deux fois sur le certificat, puis sélectionnez l'onglet **Détails**. Faites défiler la liste vers le bas pour afficher l'empreinte numérique du certificat.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



7. Copiez l'empreinte numérique dans un fichier. Supprimez les espaces lors de l'utilisation de l'empreinte numérique dans les commandes PowerShell.

Installer les certificats de signature et de cryptage

Exécutez ces commandes PowerShell sur le serveur Windows pour installer les certificats de signature et de cryptage.

Remplacez l'espace réservé ReplaceWithThumbprint et placez-le à l'intérieur des guillemets doubles comme indiqué.

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
 $_.Thumbprint -like "ReplaceWithThumbprint" }


$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName

$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys" +
    $keyname icacls $keypath /grant IIS_IUSRS`:R

<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Extraire le certificat racine du module de plateforme sécurisée (TPM) et installer le package de certificat de confiance

Exécutez ces commandes sur le serveur Windows :

```
mkdir .\TrustedTpm

expand -F:* .\TrustedTpm.cab .\TrustedTpm

cd .\TrustedTpm

.\setup.cmd
<!--NeedCopy-->
```

Configurer le service DHA

Exécutez cette commande sur le serveur Windows pour configurer le service DHA.

Remplacez l'espace réservé ReplaceWithThumbprint.

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
    ReplaceWithThumbprint

-SigningCertificateThumbprint ReplaceWithThumbprint

-SslCertificateStoreName My -SslCertificateThumbprint
    ReplaceWithThumbprint

-SupportedAuthenticationSchema "AikCertificate"
<!--NeedCopy-->
```

Exécutez ces commandes sur le serveur Windows pour configurer la stratégie de chaîne de certificat pour le service DHA :

```
$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
<!--NeedCopy-->
```

Répondez aux invites suivantes :

```
  Confirm

    Are you sure you want to perform this action?

    Performing the operation "Install-DeviceHealthAttestation" on
        target "[Machine Name]".

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A

    Adding SSL binding to website 'Default Web Site'.

    Add SSL binding?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.

    Add application pool?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding web application 'DeviceHealthAttestation' to website 'Default Web Site'.

    Add web application?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding firewall rule 'Device Health Attestation Service' to allow inbound connections on port(s) '443'.

    Add firewall rule?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Setting initial configuration for Device Health Attestation Service.

    Set initial configuration?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Registering User Access Logging.

    Register User Access Logging?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
<!--NeedCopy-->
```

Vérifier la configuration

Pour vérifier si le certificat DHASActiveSigningCertificate est actif, exécutez cette commande sur le serveur :

```
Get-DHASActiveSigningCertificate
```

Si le certificat est actif, le type de certificat (signature) et l'empreinte numérique sont affichés.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pour vérifier si le certificat DHASActiveSigningCertificate est actif, exécutez ces commandes sur le serveur

Remplacez l'espace réservé ReplaceWithThumbprint et placez-le à l'intérieur des guillemets doubles comme indiqué.

```
Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
    -Force

Get-DHASActiveEncryptionCertificate
<!--NeedCopy-->
```

Si le certificat est actif, l'empreinte numérique est affichée.

Pour effectuer une dernière vérification, accédez à cette URL :

```
https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate
/v1
```

Si le service DHA est en cours d'exécution, le message « Méthode non autorisée » est affiché.

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, 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).