# Secure Hub

# Contents



# Citrix Secure Hub

March 1, 2019

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

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

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

## Nouveautés de cette version

### Secure Hub 19.2.0

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

## Nouveautés dans les versions précédentes

### Secure Hub 19.1.5

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

- **Stratégie Wi-Fi.** La stratégie Wi-Fi prend en charge Android Entreprise désormais. Pour de plus amples informations sur cette stratégie, consultez la section [Stratégie d'appareil Wi-Fi].(/fr-fr/citrix-endpoint-management/policies/wifi-policy.html)
- **Stratégie XML personnalisé**. La stratégie XML personnalisé prend en charge Android Entreprise désormais. Pour plus d'informations sur cette stratégie, consultez [Stratégie XML personnalisé].(/fr-fr/citrix-endpoint-management/policies/custom-xml-policy.html)
- **Stratégie de fichiers.** Vous pouvez ajouter des fichiers de script dans Citrix Endpoint Management pour exécuter des fonctions sur les appareils Android Enterprise. Pour de plus amples informations sur cette stratégie, consultez la section [Stratégie de fichiers].(/fr-fr/citrix-endpoint-management/policies/files-policy.html)

### Secure Hub 19.1.0

**Secure Hub présente de nouvelles polices et couleurs ainsi que d'autres améliorations de l'interface utilisateur.** Cette nouvelle mise en forme vous offre une expérience utilisateur enrichie

tout en s'alignant étroitement sur l'esthétique de la marque Citrix à travers notre suite complète d'applications de productivité mobile.

#### Secure Hub 18.12.0

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

#### Secure Hub 18.11.5

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

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

#### Secure Hub 18.10.0

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

  Pour configurer les fonctionnalités du mode Samsung DeX dans Citrix Endpoint Management, mettez à jour la stratégie Restrictions pour Samsung KNOX. Pour plus d'informations, voir **Paramètres Samsung KNOX** dans Stratégie de restrictions.
- **Prise en charge d'Android SafetyNet :** vous pouvez configurer Endpoint Management pour utiliser la fonctionnalité **Android SafetyNet** permettant d'évaluer la compatibilité et la sécurité des appareils Android sur lesquels Secure Hub est installé. Les résultats peuvent être utilisés pour déclencher des actions automatisées sur les appareils. Pour plus d'informations, voir Android SafetyNet.
- **Empêcher l'utilisation de l'appareil photo pour les appareils Android Enterprise :** le nouveau paramètre **Autoriser l'utilisation de l'appareil photo** de la stratégie de restrictions vous permet d'empêcher les utilisateurs d'utiliser l'appareil photo sur leurs appareils Android Entreprise. Pour plus d'informations, consultez la section Stratégies de restrictions.

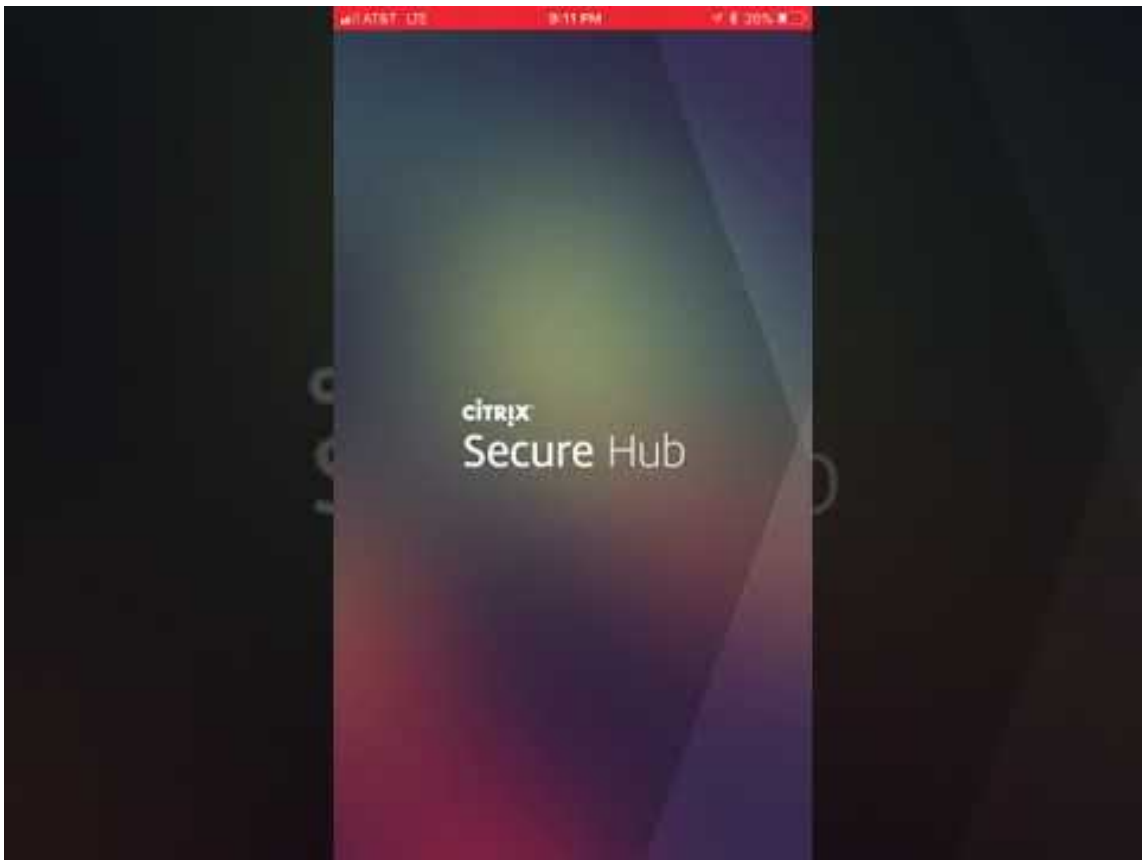
 

**Secure Hub 10.8.60 à 18.9.0**

Corrections de bugs et améliorations des performances.

**Secure Hub 10.8.60**

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




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

Pour utiliser cette fonctionnalité, configurez les éléments suivants :

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

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

**Secure Hub 10.8.55**

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

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

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

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

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

## Administration de Secure Hub

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

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

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

## Code PIN Citrix

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

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

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

Lorsque l'authentification par empreinte digitale est activée, les utilisateurs peuvent se connecter à l'aide d'une empreinte digitale lorsque l'authentification hors connexion est requise en raison de l'inactivité de l'application. Les utilisateurs doivent toujours entrer un code PIN lorsqu'ils se connectent pour la première fois à Secure Hub, qu'ils redémarrent l'appareil et après l'expiration du délai

d'inactivité. Pour plus d'informations sur l'activation de l'authentification par empreinte digitale, voir Authentification par empreinte digitale ou Touch ID.

### Certificate pinning

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

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

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

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

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

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

- Le domaine contenant les comptes avec les utilisateurs s'inscrivent.
- Le nom de domaine complet (FQDN) de Endpoint Management.
- Le nom de l'instance Endpoint Management. Par défaut, le nom de l'instance est zdm et est sensible à la casse.

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

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

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

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

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

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

> **Remarque :**
>
> Si différents types d'ouverture de session sont définis dans Endpoint Management et Citrix ADC, la configuration de Citrix ADC a priorité. Pour de plus amples informations, consultez la section Citrix Gateway et Endpoint Management.

1. Dans Citrix ADC, accédez à **Configuration > AppExpert > Rewrite > Actions**.
2. Cliquez sur **Ajouter**.

   L'écran **Create Rewrite Action** s'affiche.
3. Remplissez chaque champ, comme illustré dans la figure suivante et cliquez sur **Create**.

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

4. Liez l'action de réécriture au serveur virtuel en tant que stratégie de réécriture. Accédez à **Configuration > NetScaler Gateway > Virtual Servers** et sélectionnez votre serveur virtuel.
5. Cliquez sur **Edit**.
6. Sur l'écran **Virtual Servers configuration**, faites défiler jusqu'à **Policies**.
7. Cliquez sur **+** pour ajouter une stratégie.
8. Dans le champ **Choose Policy**, choisissez **Rewrite**.
9. Dans le champ **Choose Type**, choisissez **Response**.
10. Cliquez sur **Continuer**.

    La section **Policy Binding** va se développer.
11. Cliquez sur **Select Policy**.

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

    Si la liaison réussie, l'écran de configuration principal s'affiche avec la stratégie de réécriture.
14. Pour afficher les détails de la stratégie, cliquez sur **Rewrite Policy**.

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

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

> **Important :**
>
> Secure Hub pour Android et iOS nécessitent que vous autorisiez les appareils Android à accéder au service ADS (service de découverte automatique). Pour de plus amples informations, consultez la section Configuration requise pour les ports dans la documentation Citrix Endpoint Management. Cette communication se fait sur le port 443. Il est très probable que votre environnement soit conçu pour autoriser cet accès. Nous déconseillons aux clients qui ne peuvent pas garantir cette communication de mettre à niveau vers Secure Hub 10.2. Si vous avez des questions, contactez l'assistance Citrix.

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

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

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

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

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

Si le certificate pinning est activé :

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

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

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

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

### Fonctionnalités Secure Hub

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

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

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

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

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

Sur les tablettes, le magasin est un onglet séparé.

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

Pour les déploiements MAM exclusif, vous pouvez configurer Endpoint Management de manière à ce que les utilisateurs d'appareils Android ou iOS qui s'inscrivent dans Secure Hub avec des informations

d'identification de messagerie soient automatiquement inscrits dans Secure Mail. Les utilisateurs n'ont pas à entrer d'informations supplémentaires ou à effectuer des étapes supplémentaires pour s'inscrire dans Secure Mail.

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

Pour activer cette fonctionnalité, créez trois propriétés :

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

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

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

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

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

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

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

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

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

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

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

## Problèmes connus et résolus

March 1, 2019

### Problèmes connus dans la version 19.2.0

Il n'existe pas de problème connu dans la version 19.2.0.

### Problèmes résolus dans la version 19.2.0

#### Secure Hub pour iOS

Dans Secure Hub pour iOS, le message d'échec de handshake SSL suivant apparaît à plusieurs reprises lorsque les utilisateurs se déconnectent du magasin Secure Hub : La demande réseau de récupération d'applications a expiré sur le serveur. [CXM-61339]

#### Secure Hub pour Android

- La stratégie Fichiers pour Android Enterprise ne se déploie pas sur les appareils Android en mode profil professionnel. [CXM-61196]
- Dans Secure Hub pour Android, l'autorisation de connexion pour un nouvel utilisateur prend beaucoup de temps sur les appareils partagés. Lorsque vous vous déconnectez en tant

qu'utilisateur inscrit et essayez de vous connecter en tant que nouvel utilisateur, Secure Hub continue à charger jusqu'à ce que vous redémarriez l'appareil. [CXM-61338]
- Dans Secure Hub pour Android, les clients cloud ne peuvent pas inscrire Android Enterprise avec un fournisseur d'identité externe. [CXM-61738]
- Dans Secure Hub pour Android, lorsque vous êtes en mode COSU (appareils d'entreprise à usage unique), les icônes sont superposées dans Secure Hub. [CXM-61740]
- Dans Secure Hub pour Android, lorsque le certificate pinning est activé pour votre installation existante, l'authentification échoue et retourne à l'écran de première connexion de l'utilisateur lorsque le certificat comporte plusieurs noms de sujets alternatifs. [CXM-61933]

## Problèmes connus et résolus dans les versions précédentes

## Problèmes connus dans la version 19.1.5

- Dans Secure Hub pour Android, lorsque vous mettez à jour le mot de passe en raison d'un changement de stratégie de mot de passe, les applications en badge n'apparaissent pas sur les appareils Samsung Galaxy S8. [CXM-61177]
- Dans Secure Hub pour Android, la stratégie Fichiers Android Enterprise ne se déploie pas sur les appareils en mode profil professionnel. [CXM-61196]

### Problèmes résolus dans la version 19.1.5

- Dans Secure Hub pour Android, lorsque les utilisateurs se connectent avec le code PIN sécurisé, un tunnel VPN est établi, mais Secure Web ne charge aucun site Web. Toutefois, le site Web se charge comme prévu lorsque Secure Web est fermé et rouvert. [CXM-58576]
- Dans Secure Hub pour Android, lorsque vous vous connectez avec le code PIN sécurisé, un tunnel VPN est établi, mais Secure Web ne charge aucun site Web. Cependant, le site Internet charge comme prévu quand Web sécurisé est fermé et rouvert. [CXM-60751]
- Dans Secure Hub pour Android, lorsque vous essayez de capturer les journaux de l'application interne appelée TechXpert, Secure Hub redémarre et vous demande de vous réauthentifier. [CXM-61310]

### Problèmes connus dans la version 19.1.0

#### Secure Hub pour iOS

Dans Secure Hub pour iOS, lorsque vous déployez une application MDX et des applications Web ou SaaS, elles apparaissent dans l'écran **Mes applications**. Lorsque vous appuyez sur **Plus**, une fenêtre contextuelle apparaît avec les options **Supprimer** et **Annuler** qui ont le format de l'ancienne interface utilisateur. [CXM-60683]

### Problèmes résolus dans la version 18.12.0

- Sur les appareils Samsung Knox inscrits pour Android For Work, lorsque la stratégie de mot de passe est configurée pour expirer dans un ou deux jours, le message « Mot de passe expiré » s'affiche à plusieurs reprises. [CXM-59250]
- Vous ne pouvez pas inscrire les appareils OnePlus 5T pour Android Entreprise en utilisant la méthode d'inscription par code QR. [CXM-59288]

### Problèmes résolus dans la version 18.11.0

#### Secure Hub iOS

- Vous ne pouvez pas utiliser l'authentification unique sur les appareils Android inscrits en mode Appareil partagé. L'erreur suivante apparaît : impossible de récupérer vos informations d'identification d'entreprise pour le moment. La connexion manuelle à ShareFile est bloquée par une stratégie administrative. [CXM-58238]
- Vous ne pouvez pas modifier les niveaux de volume Android sur des appareils à usage unique (COSU) appartenant à l'entreprise. [CXM-58323]

### Problèmes résolus dans la version 18.10.5

- Si le mode FIPS est activé dans XenMobile Server, une fois que les utilisateurs ont mis à jour Secure Hub pour iOS vers la version 18.10.5, un message d'erreur lié au cryptage s'affiche lorsque les utilisateurs ouvrent des applications. Pour obtenir des mises à jour de l'état de la résolution, consultez cet article du Centre de connaissances Citrix. [CXM-56454]

### Problèmes résolus dans les versions 10.8.25 à 18.10.6

- Les versions 10.8.25 à 18.10.6 de Secure Hub (Android) ne comprennent aucun problème connu. Les problèmes suivants sont résolus dans Secure Hub. La liste comprend les problèmes liés à MDX qui affectent Secure Hub.

### Problèmes résolus dans la version 18.10.0

- Si la stratégie MVPN est désactivée dans la console EMS, Secure Hub affiche un écran vide lorsque vous essayez d'ouvrir des applications gérées par Intune. [CXM-56033, CXM-56086, CXM-54393, CXM-54823]

**Problèmes résolus dans la version 10.8.60**

- Sur les appareils Samsung Galaxy Tab Active 2 SM-T395, l'action de sécurité Effacement complet échoue pour Secure Hub pour Android lorsque les administrateurs définissent une restriction Désactiver réinitialisation des paramètres d'usine dans XenMobile. [CXM-54452]
- Secure Hub pour Android cesse de répondre lors de l'inscription d'appareils lorsque la stratégie VPN est configurée et que l'application Citrix SSO n'est pas installée sur l'appareil. Il devient réactif si vous touchez le bouton **Précédent** ou redémarrez l'application. [CXM-54627]
- Secure Hub pour Android se bloque lors de l'inscription en mode Propriétaire de l'appareil dans un environnement Android Entreprise. [CXM-55008]
- Après que les utilisateurs ont saisi un code PIN valide pour Secure Hub pour iOS, Secure Hub invite les utilisateurs à entrer leur code PIN à plusieurs reprises. [CXM-55047]
- Secure Hub pour Android se bloque lors de l'inscription en mode Propriétaire de l'appareil dans un environnement Android Entreprise. [CXM-55076]
- L'utilisation d'Android Entreprise dans Secure Hub pour Android installe Google Chrome par défaut. [CXM-55232]
- La mise à niveau de Secure Hub pour iOS vers la version 10.8.55 n'autorise pas les inscriptions d'appareils iOS existantes ou nouvelles. [CXM-55267]

**Problèmes résolus dans la version 10.8.55**

- Les utilisateurs ne peuvent pas se connecter à Secure Hub pour s'inscrire auprès de comptes Android for Work lorsque les informations d'identification de G Suite diffèrent de celles de Endpoint Management. [CXM-53956]

**Problèmes résolus liés à MDX dans la version 10.8.55**

- Les applications d'entreprise peuvent rencontrer des problèmes de connectivité avec les ressources internes lorsque le mode VPN préféré est défini sur SecureBrowse. [CXM-52309]
- Les applications qui spécifient android.support.multidex.MultiDexApplication ou android.app.Application comme classe d'application ne peuvent pas se connecter aux réseaux internes en mode de navigation sécurisée. [CXM-53126]
- Sur les appareils Android, plusieurs certificats sont générés et les certificats sont révoqués avant leur date d'expiration. [CXM-53428]

**Problème connu dans la version 10.8.50**

- Sur Secure Hub pour Android, les utilisateurs ne peuvent pas ajouter de raccourci de lien Web. [XMHELP-952]

**Problèmes résolus dans la version 10.8.35**

- Sur Android O, les raccourcis créés par les stratégies ne s'affichent pas sur l'écran d'accueil de l'appareil. Ce comportement est intentionnel dans Android O. [CXM-35460]
- Sur Android, Secure Hub ne s'ouvre pas sur les tablettes Samsung après une période d'inactivité. [CXM-50797]
- Dans Secure Hub pour Android, vous ne pouvez pas déployer la stratégie de notifications push sur les appareils Samsung Knox. [CXM-50869]
- Dans Secure Hub pour iOS, le problème suivant survient occasionnellement : une fois que les utilisateurs ont modifié leur mot de passe Active Directory, ils doivent entrer leur code PIN en boucle. [CXM-50224]

**Problèmes résolus dans la version 10.8.25**

- Pour les applications iOS Cordova tierces encapsulées avec la version 10.7.20 de MDX Toolkit, après l'activation de la stratégie **Obscurcir le contenu de l'écran**, un écran noir apparaît au lieu d'un écran de code PIN. [CXM-48471]
- Sur les appareils Zebra T51 fonctionnant sous Android 7, les utilisateurs ne peuvent pas installer l'application Citrix Launcher. [CXM-50621]

**Problèmes résolus dans la version 10.8.20**

- Une fois que les utilisateurs ont mis à jour leurs appareils Android vers la version 8 (Oreo) : ils ne peuvent pas installer les applications d'entreprise ou .apk à partir du magasin d'applications que vous déployez à partir de Endpoint Management. Même lorsqu'ils permettent l'installation d'applications tierces, le problème persiste. Le problème ne se limite pas aux appareils Samsung. [CXM-50401]

**Problèmes résolus dans la version 10.8.15**

- Secure Hub pour Android se bloque lors de la récupération des informations d'emplacement sur les appareils exécutant Android O. [CXM-47893]

**Problèmes résolus dans la version 10.8.10**

- Sur les appareils Android, lorsque plusieurs applications ne s'installent pas automatiquement ou que les utilisateurs ne cliquent pas sur **Installer** eux-mêmes, les applications continuent à se télécharger. Par conséquent, un volume important de données est utilisé. [CXM-46404]

- Sur les appareils exécutant Android 7 ou version ultérieure : lorsque vous envoyez une action de sécurisation au verrouillage avec un mot de passe à l'appareil à partir de XenMobile Server, l'appareil est verrouillé. Toutefois, le mot de passe de l'appareil n'est pas modifié si les utilisateurs possèdent un mot de passe de verrouillage de l'écran. Les utilisateurs peuvent utiliser le code secret d'origine pour déverrouiller l'appareil. [CXM-47908]

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

## Scénarios d'invite d'authentification

February 11, 2019

Plusieurs scénarios invitent les utilisateurs à s'authentifier auprès de Secure Hub en entrant leurs informations d'identification sur leurs appareils.

Les scénarios varient en fonction des facteurs suivants :

- Votre stratégie d'application MDX et la configuration de la propriété client dans les paramètres de la console Endpoint Management.
- Si l'authentification se produit hors connexion ou en ligne (l'appareil a besoin d'une connexion réseau à Endpoint Management).

En outre, le type d'informations d'identification que les utilisateurs entrent, telles qu'un mot de passe Active Directory, un code PIN ou code secret Citrix, un mot de passe unique ou une empreinte digitale (appelée Touch ID dans iOS), varie également en fonction du type d'authentification et de la fréquence d'authentification dont vous avez besoin.

Explorons les scénarios qui entrainent une invite d'authentification.

- **Redémarrage de l'appareil :** lorsque les utilisateurs redémarrent leur appareil, ils doivent se réauthentifier avec Secure Hub.
- **Inactivité hors connexion (délai d'expiration) :** lorsque la stratégie MDX Code secret d'application est activée (valeur par défaut), la propriété de client Endpoint Management appelée Délai d'inactivité entre en vigueur. Le délai d'inactivité déconnecte automatiquement les applications qui utilisent le conteneur sécurisé si aucune activité n'est détectée au-delà d'une certaine période.

Lorsque le Délai d'inactivité expire, les utilisateurs doivent se réauthentifier auprès du conteneur sécurisé sur l'appareil. Si, par exemple, les utilisateurs posent leurs appareils et s'en vont, et que le délai d'inactivité expire, aucun autre utilisateur ne peut se servir de l'appareil pour accéder à des informations confidentielles dans le conteneur. Vous définissez la propriété de client Délai d'inactivité

dans la console Endpoint Management. La valeur par défaut est 15 minutes. La combinaison de la stratégie Code secret d'application définie sur **Activé** et de la propriété client Délai d'inactivité couvre les scénarios de demande d'authentification les plus courants.

- **Déconnexion de Secure Hub :**. Lorsque les utilisateurs se déconnectent de Secure Hub, ils doivent se réauthentifier la prochaine fois qu'ils accèdent à Secure Hub ou à toute application MDX, lorsque l'application requiert un code secret comme déterminé par la stratégie MDX Code secret d'application et l'état Délai d'inactivité.
- **Période hors connexion maximale :**. Ce scénario est spécifique aux applications individuelles car il est régi par une stratégie MDX par application. La stratégie MDX Période hors connexion maximale dispose d'un paramètre par défaut de 3 jours. Si la durée pendant laquelle une application est autorisée à s'exécuter sans authentification en ligne avec Secure Hub s'écoule, une vérification auprès de Endpoint Management est requise afin de confirmer les droits d'application et d'actualiser les stratégies. Lorsque cette vérification se produit, l'application déclenche Secure Hub afin de procéder à une authentification en ligne. Les utilisateurs doivent se réauthentifier avant de pouvoir accéder à l'application MDX.

Notez la relation entre les stratégies MDX Période hors connexion maximale et Période d'interrogation active :

- La Période d'interrogation active est l'intervalle durant lequel les applications contactent Endpoint Management pour effectuer des actions de sécurité, telles que le verrouillage et l'effacement d'applications. En outre, l'application recherche également la présence de stratégies d'application mises à jour.
- Après la recherche de stratégies via la stratégie Période d'interrogation active, le minuteur de la Période hors connexion maximale est remis à zéro.

Les deux interrogations de Endpoint Management, afin de déterminer l'expiration de la Période d'interrogation active et de la Période hors connexion maximale, requièrent un jeton Citrix Gateway valide sur l'appareil. Si la machine dispose d'un jeton Citrix Gateway valide, l'application récupère les nouvelles stratégies depuis Endpoint Management sans aucune interruption pour les utilisateurs. Si l'application requiert un jeton Citrix Gateway, elle bascule vers Secure Hub et les utilisateurs voient une invite d'authentification dans Secure Hub.

Sur les appareils Android, les écrans d'activité Secure Hub s'ouvrent directement sur l'écran de l'application en cours. Sur les appareils iOS, toutefois, Secure Hub doit apparaître au premier plan, ce qui déplace temporairement l'application en cours.

Une fois que les utilisateurs ont entré leurs informations d'identification, Secure Hub bascule de nouveau vers l'application d'origine. Si, dans ce cas, vous autorisez la mise en cache des informations d'identification Active Directory ou si vous disposez d'un certificat client configuré, les utilisateurs peuvent saisir un code PIN ou un mot de passe, ou authentification par empreinte digitale. Si vous ne procédez pas de la sorte, les utilisateurs doivent entrer leurs informations d'identification Active

Directory complètes.

Le jeton Citrix ADC peut devenir non valide en raison d'absence d'activité dans la session Citrix Gateway ou de l'application d'une stratégie d'expiration de session, comme indiqué dans la liste suivante de stratégies Citrix Gateway. Lorsque les utilisateurs se connectent de nouveau à Secure Hub, ils peuvent continuer à exécuter l'application.

- **Stratégies de session Citrix Gateway :** deux stratégies Citrix Gateway affectent également quand les utilisateurs sont invités à s'authentifier. Dans ces cas, ils s'authentifient pour créer une session en ligne avec Citrix ADC pour la connexion à Endpoint Management.
  - **Expiration de la session :** la session Citrix ADC pour Endpoint Management est déconnectée si aucune activité réseau n'est détectée pendant la période de temps définie. La valeur par défaut est 30 minutes. Cependant, si vous utilisez l'assistant Citrix Gateway pour configurer la stratégie, la valeur par défaut est de 1440 minutes. Les utilisateurs verront alors un message d'authentification les invitant à se reconnecter à leur réseau d'entreprise.
  - **Expiration forcée :** si cette stratégie est **activée**, la session Citrix ADC pour Endpoint Management est déconnectée après écoulement de la période d'expiration forcée. Le délai d'expiration forcé rend la réauthentification obligatoire après une certaine période de temps. Les utilisateurs verront alors un message d'authentification les invitant à se reconnecter à leur réseau d'entreprise lors de la prochaine utilisation. La valeur par défaut est **Désactivé**. Cependant, si vous utilisez l'assistant Citrix Gateway pour configurer la stratégie, la valeur par défaut est de 1440 minutes.

### Types d'informations d'identification

La section précédente abordait les circonstances dans lesquelles les utilisateurs sont invités à s'authentifier. Cette section traite des types d'informations d'identification qu'ils doivent entrer. L'authentification est nécessaire au travers de plusieurs méthodes d'authentification pour accéder aux données chiffrées de l'appareil. Pour déverrouiller l'appareil pour la première fois, vous devez déverrouiller le *conteneur principal*. Une fois que le déverrouillage est terminé et que le conteneur est de nouveau sécurisé, pour accéder de nouveau à l'appareil, vous devez déverrouiller un *conteneur secondaire*.

> **Remarque :**
>
> Lorsque l'article fait référence à une *application gérée*, le terme fait référence à une application encapsulée par l'outil MDX Toolkit, dans lequel vous avez laissé la stratégie MDX Code secret d'application activée et pour laquelle vous utilisez la propriété de client Délai d'inactivité.

Les conditions qui déterminent les types d'informations d'identification sont les suivantes :

- **Déverrouillage du conteneur principal :** un mot de passe Active Directory, un code PIN ou code secret Citrix, un mot de passe unique, Touch ID ou une empreinte digitale est nécessaire

pour déverrouiller le conteneur principal.
  - Dans iOS, lorsque les utilisateurs ouvrent Secure Hub ou une application gérée pour la première fois après que l'application est installée sur l'appareil.
  - Dans iOS, lorsque les utilisateurs redémarrent un appareil, puis qu'ils ouvrent Secure Hub.
  - Sur Android, lorsque les utilisateurs ouvrent une application gérée si Secure Hub n'est pas en cours d'exécution.
  - Sur Android, lorsque les utilisateurs redémarrent Secure Hub pour une raison quelconque, y compris le redémarrage d'un appareil.
- **Déverrouillage du conteneur secondaire :** l'authentification par empreinte digitale (si elle est configurée), un code PIN ou code secret Citrix ou des informations d'identification Active Directory sont nécessaires pour déverrouiller le conteneur secondaire.
  - Lorsque les utilisateurs ouvrent une application gérée après expiration du délai d'inactivité.
  - Lorsque les utilisateurs se déconnectent de Secure Hub et ouvrent ensuite une application gérée.

Les informations d'identification Active Directory sont requises pour l'une ou l'autre des circonstances de déverrouillage de conteneur lorsque les conditions suivantes sont remplies :

- Lorsque les utilisateurs modifient le code secret associé à leur compte d'entreprise.
- Lorsque vous n'avez pas défini les propriétés de client dans la console Endpoint Management pour activer le code PIN Citrix : ENABLE_PASSCODE_AUTH et ENABLE_PASSWORD_CACHING.
- Lorsque la session NetScaler Gateway prend fin, ce qui se produit dans les conditions suivantes : lorsque le délai d'expiration de la session ou le délai d'expiration forcé expire, si l'appareil ne met pas en cache les informations d'identification ou qu'il ne dispose pas d'un certificat client.

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

L'organigramme suivant résume le flux décisionnel qui détermine les informations d'identification qu'un utilisateur doit entrer lorsqu'il est invité à s'authentifier.

### À propos des basculements d'écran Secure Hub

Une autre situation à considérer est lorsque le basculement d'une application vers Secure Hub et vice versa est requis. Le basculement affiche une notification que les utilisateurs doivent confirmer. L'authentification n'est pas nécessaire lorsque cela se produit. Cette situation se produit après communication avec Endpoint Management, comme indiqué par les stratégies MDX Période hors connex-

ion maximale et Période d'interrogation active, et Endpoint Management détecte les stratégies mises à jour qui ont besoin d'être déployées sur l'appareil via Secure Hub.

## Installation d'un VPN pour iOS

March 1, 2019

Sur les appareils iOS 10 et versions ultérieures, le VPN Secure Hub est utilisé pour sécuriser le partage de données locales entre Secure Hub et les applications MDX. Le VPN Secure Hub s'exécute sur iOS 10 et versions ultérieures. Le VPN Secure Hub fournit l'expérience utilisateur idéale car il permet à Secure Hub et aux applications MDX de communiquer en toute transparence via ce VPN.

Le VPN Secure Hub fonctionne pour les applications signées par des certificats du compte de développeur Apple Enterprise (« identifiant d'équipe »), des certificats Citrix, des certificats d'entreprise, ou des certificats d'éditeurs de logiciels indépendants (ISV) tiers.

Le VPN Secure Hub est utilisé par défaut sur les appareils iOS 10. Si le VPN Secure Hub n'est pas exécuté sur l'appareil iOS 10, MDX utilise le trousseau iOS partagé pour sécuriser le partage des données. Le mécanisme de trousseau iOS partagé requiert que toutes les applications soient signées avec le même certificat pour pouvoir accéder au trousseau partagé spécifique pour ce certificat « identifiant d'équipe » iOS. Si une application n'est pas signée avec le même certificat que l'application Secure Hub signée par Citrix, l'application peut basculer vers Secure Hub pour obtenir les informations requises.

Le VPN Secure Hub est uniquement disponible pour les déploiements de Citrix Endpoint Management Enterprise et MAM exclusif. Le VPN Secure Hub ne s'applique pas aux environnements Endpoint Management en mode MDM exclusif, et le VPN n'est pas installé dans les inscriptions en mode MDM exclusif.

Le VPN Secure Hub est utilisé pour les communications entre Secure Hub et les applications de productivité mobiles. Il ne filtre pas ni ne surveille le trafic réseau sur l'appareil et est indépendant du mécanisme de micro VPN MDX.

> Remarque :
>
> Citrix vous recommande de laisser le VPN Secure Hub activé dans les environnements où il est activé par défaut.
>
> Toutefois, étant donné que iOS ne permet pas l'exécution simultanée de plusieurs clients VPN sur un appareil iOS, tenez compte de la situation suivante. Le VPN Secure Hub ne peut pas être utilisé si une autre application VPN, telle que l'application Cisco AnyConnect ou Citrix VPN, doit être exécutée sur des appareils iOS de façon à établir un VPN au niveau de l'appareil. Vous pouvez définir un per app VPN iOS même si le VPN Secure Hub n'est pas désactivé. L'application qui utilise le per app VPN iOS établit une connexion per app VPN lorsque l'application est au premier

> plan.
>
> Pour désactiver le VPN Secure Hub, consultez la section suivante dans cet article. Lorsque le VPN Secure Hub est désactivé, les utilisateurs peuvent rencontrer davantage de basculements depuis une application gérée vers Secure Hub.

### Désactivation ou réactivation du VPN Secure Hub dans Endpoint Management

Le VPN Secure Hub est activé par défaut lorsque les utilisateurs commencent à utiliser Secure Hub 10.3.10 et versions ultérieures sur iOS 10.

Pour désactiver le VPN Secure Hub et définir les appareils iOS de votre déploiement pour qu'ils utilisent le mécanisme de trousseau partagé, procédez comme suit :

1. Dans la console Endpoint Management, accédez à **Paramètres > Client > Propriétés du client**.
2. Dans la page **Propriétés du client**, créez une propriété cliente personnalisée appelée **ENABLE_NETWORK_EXTENSION** et définissez sa valeur sur 0.

   Pour réactiver le VPN Secure Hub, rendez-vous sur le VPN Secure Hub et définissez la valeur de **ENABLE_NETWORK_EXTENSION** sur 1.

### Installation du VPN Secure Hub sur la machine cliente

Le VPN Secure Hub est installé dans deux cas : après l'installation de Secure Hub 10.3.10 ou version ultérieure sur un appareil iOS 10 ou lorsqu'un utilisateur met à niveau un appareil exécutant la version 10.3.10 ou une version ultérieure de Secure Hub vers la version 10 d'iOS.

Les utilisateurs voient ce message d'information.

Les utilisateurs voient ensuite un message iOS leur demandant l'autorisation d'ajouter des configurations VPN. Ce message est affiché une seule fois, lorsque le VPN est installé pour la première fois. Il n'est pas affiché lorsque les utilisateurs ouvrent Secure Hub à nouveau.

Le message sur cet écran n'est pas personnalisable. Il s'agit d'une boîte de dialogue iOS standard utilisée pour les installations de VPN.

Sur l'écran leur demandant l'autorisation d'ajouter la configuration VPN : si les utilisateurs sélectionnent **Ne pas autoriser**, ils voient un autre message indiquant qu'ils doivent installer le VPN pour pouvoir accéder à Secure Hub.

### Exécution du VPN Secure Hub sur la machine cliente

Lorsque le VPN Secure Hub fonctionne comme prévu, le texte **Connexion** s'affiche dans l'écran **Général > VPN** dans les Réglages iOS.

Ce comportement est normal et ne signifie pas que le partage MDX et les mécanismes de communication ne fonctionnent pas. Aucune action n'est requise de la part des utilisateurs s'ils voient ce message.

## Inscription à l'aide d'informations d'identification dérivées

January 25, 2019

Les informations d'identification dérivées fournissent une authentification forte pour les appareils mobiles. Les informations d'identification, dérivées d'une carte à puce, se trouvent dans un appareil mobile plutôt que sur la carte. La carte à puce est une carte Personal Identity Verification (PIV) ou une carte Common Access Card (CAC).

Les informations d'identification dérivées sont un certificat d'inscription qui contient l'identifiant de l'utilisateur, tel qu'un UPN (nom d'utilisateur principal). Endpoint Management stocke les informations d'identification obtenues à partir du fournisseur d'informations d'identification dans un coffre sécurisé sur l'appareil.

Endpoint Management peut utiliser les informations d'identification dérivées pour l'inscription d'appareils iOS. S'il est configuré pour des informations d'identification dérivées, Endpoint Management ne prend pas en charge les invitations d'inscription ou autres modes d'inscription pour les appareils iOS. Toutefois, vous pouvez utiliser le même serveur Endpoint Management pour inscrire les appareils Android via des invitations d'inscription et autres modes d'inscription.

### Étapes d'inscription d'un appareil lors de l'utilisation des informations d'identification dérivées

L'inscription nécessite que les utilisateurs insèrent leur carte à puce dans un lecteur connecté à leur bureau.

1. L'utilisateur installe Secure Hub et l'application à partir de votre fournisseur d'informations d'identification dérivées. Dans cet exemple, l'application de fournisseur d'identité est Intercede MyID Identity Agent.
2. L'utilisateur démarre Secure Hub. Lorsqu'il y est invité, l'utilisateur tape le nom de domaine complet de Endpoint Management et clique sur **Suivant**. L'inscription dans Secure Hub démarre. Si Endpoint Management prend en charge les informations d'identification dérivées, Secure Hub invite l'utilisateur à créer un code PIN Citrix.
3. L'utilisateur suit les instructions permettant d'activer ses informations d'identification de carte à puce. Un écran de démarrage s'affiche, suivi d'une invite à scanner un code QR.

4. L'utilisateur insère sa carte dans le lecteur de carte à puce qui est connecté à son bureau. Ensuite, l'application de bureau affiche un code QR et invite l'utilisateur à scanner le code à l'aide de son appareil mobile.

   L'utilisateur entre son code PIN Secure Hub lorsqu'il y est invité.

Après l'authentification du code PIN, Secure Hub télécharge les certificats. L'utilisateur suit les invites pour terminer l'inscription.

Pour afficher des informations sur l'appareil dans la console Endpoint Management, procédez comme suit :

- Accédez à **Gérer > Appareils**, puis sélectionnez un appareil pour afficher une zone de commande. Cliquez sur **Afficher plus**.
- Accédez à **Analyser > Tableau de bord**.

**Locations**
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States