citrix

Secure Hub

Contents

Citrix Secure Hub

November 21, 2022

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.

Pour connaître les dernières informations sur les applications de productivité mobiles, consultez Annonces récentes.

Les sections suivantes répertorient les nouvelles fonctionnalités dans la version actuelle et les versions antérieures de Secure Hub.

> **Remarque :**
>
> la prise en charge des versions Android 6.x et iOS 11.x de Secure Hub, Secure Mail, Secure Web et de l'application Citrix Workspace a pris fin en juin 2020.

Nouveautés dans la version actuelle

Secure Hub 22.9.0

Secure Hub pour Android

Cette version comprend :

- Complexité du code d'accès de l'appareil (Android 12+)
- Prise en charge du SDK 31
- Corrections de bogues

Complexité du code d'accès de l'appareil (Android 12+)

La complexité du code d'accès est préférable à une exigence de mot de passe personnalisé. Le niveau de complexité du code d'accès est l'un des niveaux prédéfinis. De ce fait, l'utilisateur final n'est pas autorisé à définir un mot de passe avec un niveau de complexité inférieur.

La complexité du code d'accès pour les appareils tournant sous Android 12 ou version ultérieure est la suivante :

- **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 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

> **Remarques :**
>
> - 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.
> - Si la complexité du code d'accès du profil de travail est activée, la complexité du code d'accès côté appareil doit également être activée.

Pour plus d'informations, consultez la section Paramètres Android Enterprise de la documentation de Citrix Endpoint Management.

Nouveautés dans les versions précédentes

Secure Hub 22.7.0

Secure Hub pour Android

Cette version inclut des corrections de bogues.

Secure Hub 22.6.0

Secure Hub pour Android

Cette version inclut des corrections de bogues.

Secure Hub 22.5.0

Secure Hub pour iOS

Cette version inclut des corrections de bogues.

Secure Hub 22.4.0

Secure Hub pour Android

Cette version inclut des corrections de bogues.

Secure Hub 22.2.0

Secure Hub pour iOS

Cette version inclut des corrections de bogues.

Secure Hub pour Android

Cette version inclut des corrections de bogues.

Secure Hub 21.11.0

Secure Hub pour Android

Prise en charge des profils de travail pour les appareils appartenant à l'entreprise

Sur les appareils Android Enterprise, vous pouvez désormais inscrire Secure Hub dans le profil de travail des appareils appartenant à l'entreprise. Cette fonctionnalité est disponible sur les appareils exécutant Android 11 ou version ultérieure. Les appareils précédemment inscrits en mode COPE (propriété de l'entreprise avec accès privé) sont migrés automatiquement vers le profil de travail pour les appareils appartenant à l'entreprise, lorsque l'appareil est mis à niveau d'Android 10 vers Android 11 ou version ultérieure.

Secure Hub 21.10.0

Secure Hub pour iOS

Cette version inclut des corrections de bogues.

Secure Hub pour Android

Prise en charge de Android 12. À partir de cette version, Secure Hub est pris en charge sur les appareils exécutant Android 12.

Secure Hub 21.8.0

Secure Hub pour iOS

Cette version inclut des corrections de bogues.

Secure Hub 21.7.1

Secure Hub pour Android

Prise en charge d'Android 12 sur les appareils déjà inscrits. Si vous envisagez de mettre à niveau vers Android 12, assurez-vous d'abord de mettre à jour Secure Hub vers la version 21.7.1. Secure Hub 21.7.1 est la version minimale requise pour effectuer une mise à niveau vers Android 12. Cette version garantit une mise à niveau transparente d'Android 11 vers Android 12 pour les utilisateurs déjà inscrits.

> **Remarque :**
>
> Si Secure Hub n'est pas mis à jour vers la version 21.7.1 avant la mise à niveau vers Android 12, votre appareil peut nécessiter une réinscription ou une réinitialisation aux paramètres d'usine pour récupérer des fonctionnalités antérieures.
>
> Citrix s'engage à fournir, dès le premier jour, la prise en charge pour Android 12 et ajoutera d'autres mises à jour aux versions ultérieures de Secure Hub pour prendre en charge Android 12.

Secure Hub 21.7.0

Secure Hub pour iOS

Cette version inclut des corrections de bogues.

Secure Hub pour Android

Cette version inclut des corrections de bogues.

Secure Hub 21.6.0

Secure Hub pour iOS

Cette version inclut des corrections de bogues.

Secure Hub pour Android

Cette version inclut des corrections de bogues.

Secure Hub 21.5.1

Secure Hub pour iOS

Cette version inclut des corrections de bogues.

Secure Hub pour Android

Cette version inclut des corrections de bogues.

Secure Hub 21.5.0

Secure Hub pour iOS

Dans cette version, les applications encapsulées avec MDX Toolkit version 19.8.0 ou antérieure ne fonctionneront plus. Assurez-vous d'encapsuler vos applications avec la dernière version du MDX Toolkit pour garantir le bon fonctionnement des fonctionnalités.

Secure Hub 21.4.0

Revamping des couleurs de Secure Hub. Secure Hub est conforme aux mises à jour des couleurs de la marque Citrix.

Secure Hub 21.3.2

Secure Hub pour iOS

Cette version inclut des corrections de bogues.

Secure Hub 21.3.0

Cette version inclut des corrections de bogues.

Secure Hub 21.2.0

Secure Hub pour Android

Cette version inclut des corrections de bogues.

Secure Hub 21.1.0

Secure Hub pour iOS

Cette version inclut des corrections de bogues.

Secure Hub pour Android

Cette version inclut des corrections de bogues.

Secure Hub 20.12.0

Secure Hub pour iOS

Cette version inclut des corrections de bogues.

Secure Hub pour Android

Secure Hub pour Android prend en charge le mode Direct Boot. Pour plus d'informations sur le mode Direct Boot, consultez la documentation Android sur *Developer.android.com.*

Secure Hub 20.11.0

Secure Hub pour Android

Secure Hub prend en charge les exigences actuelles de l'API cible de Google Play pour Android 10.

Secure Hub 20.10.5

Cette version inclut des corrections de bogues.

Secure Hub 20.9.0

Secure Hub pour iOS

Secure Hub pour iOS prend en charge iOS 14.

Secure Hub pour Android

Cette version inclut des corrections de bogues.

Secure Hub 20.7.5

Secure Hub pour Android

- Secure Hub pour Android prend en charge Android 11.
- **Transition de Secure Hub 32 bits à 64 bits pour les applications**. Dans Secure Hub version 20.7.5, l'architecture 32 bits pour les applications n'est plus prise en charge et Secure Hub a été mis à jour vers 64 bits. Citrix recommande aux clients de mettre à niveau leur version 20.6.5.

vers la version 20.7.5. Si les utilisateurs ignorent la mise à niveau vers Secure Hub version 20.6.5 et qu'ils effectuent la mise à jour de 20.1.5 vers 20.7.5 directement, ils doivent se réauthentifier. La réauthentification implique la saisie d'informations d'identification et la réinitialisation du code PIN Secure Hub. Secure Hub version 20.6.5 est disponible dans Google Play Store.

- **Installez les mises à jour depuis l'App Store.** Dans Secure Hub pour Android, si des mises à jour sont disponibles pour les applications, l'application est mise en surbrillance et la fonctionnalité **Mises à jour disponibles** apparaît sur l'écran de l'App Store.

  Lorsque vous appuyez sur **Mises à jour disponibles**, vous accédez au magasin qui affiche la liste des applications avec des mises à jour en attente. Appuyez sur **Détails** en regard de l'application pour installer les mises à jour. Lorsque l'application est mise à jour, la flèche vers le bas dans **Détails** est remplacée par une coche.

Secure Hub 20.6.5

Secure Hub pour Android

Transition de 32 bits à 64 bits pour les applications. La version 20.6.5 de Secure Hub est la dernière version à prendre en charge une architecture 32 bits pour les applications mobiles Android. Dans les versions suivantes, Secure Hub prend en charge l'architecture 64 bits. Citrix recommande aux utilisateurs de mettre à niveau vers Secure Hub version 20.6.5 de façon à pouvoir mettre à niveau vers des versions ultérieures sans avoir à se réauthentifier. Si les utilisateurs ignorent la mise à niveau vers Secure Hub version 20.6.5 et qu'ils effectuent la mise à jour vers 20.7.5 directement, ils doivent se réauthentifier. La réauthentification implique la saisie d'informations d'identification et la réinitialisation du code PIN Secure Hub.

> **Remarque :**
>
> la version 20.6.5 ne bloque pas l'inscription des appareils exécutant Android 10 en mode d'administrateur d'appareil.

Secure Hub pour iOS

Activez un proxy configuré sur les appareils iOS. Secure Hub pour iOS requiert l'activation d'une nouvelle propriété client, `ALLOW_CLIENTSIDE_PROXY`, si vous souhaitez autoriser les utilisateurs à utiliser des serveurs proxy qu'ils configurent dans **Paramètres > Wi-Fi**. Pour de plus amples informations, consultez la section `ALLOW_CLIENTSIDE_PROXY` dans Référence des propriétés du client.

Secure Hub 20.3.0

> **Remarque :**
>
> la prise en charge des versions Android 6.x et iOS 11.x de Secure Hub, Secure Mail, Secure Web

> et de l'application Citrix Workspace prend fin en juin 2020.

Secure Hub pour iOS

- **Extension réseau désactivée.** En raison de modifications récentes apportées aux directives de révision de l'App Store, à partir de la version 20.3.0, Secure Hub ne prend pas en charge l'extension réseau (NE) sur les appareils exécutant iOS. NE n'a aucun impact sur les applications de productivité mobiles développées par Citrix. Toutefois, la suppression de NE a un certain impact sur les applications encapsulées MDX d'entreprise déployées. Les utilisateurs finaux peuvent rencontrer des basculements supplémentaires vers Secure Hub lors de la synchronisation de composants tels que les jetons d'autorisation, les minuteurs et les tentatives de saisie de codes PIN. Pour de plus amples informations, consultez https://support.citrix.com/article/CTX270296.

> **Remarque :**
>
> les nouveaux utilisateurs ne sont pas invités à installer le VPN.

- **Prise en charge des profils d'inscription améliorée.** Secure Hub prend en charge les fonctionnalités de profil d'inscription améliorées annoncées pour Citrix Endpoint Management dans la section Profils d'inscription.

Secure Hub 20.2.0

Secure Hub pour iOS

Cette version inclut des corrections de bogues.

Secure Hub 20.1.5

Cette version comprend :

- Mise à jour de la mise en forme et de l'affichage de la politique de confidentialité utilisateur. Cette mise à jour de fonctionnalité modifie le flux d'inscription à Secure Hub.
- Corrections de bogues.

Secure Hub 19.12.5

Cette version inclut des corrections de bogues.

Secure Hub 19.11.5

Cette version inclut des corrections de bogues.

Secure Hub 19.10.5

Secure Hub pour Android

Inscrire Secure Hub en mode COPE. Sur les appareils Android Enterprise, inscrivez Secure Hub en mode COPE (propriété de l'entreprise avec accès privé) lorsque Citrix Endpoint Management est configuré dans le profil d'inscription COPE.

Secure Hub 19.10.0

Cette version inclut des corrections de bogues.

Secure Hub 19.9.5

Secure Hub pour iOS

Cette version inclut des corrections de bogues.

Secure Hub pour Android

Prise en charge des fonctionnalités de keyguard pour le profil de travail Android Enterprise et les appareils entièrement gérés. Le keyguard Android gère l'appareil et les challenges d'écran de verrouillage des profils professionnels. Utilisez la stratégie de gestion du keyguard dans Citrix Endpoint Management pour contrôler la gestion du keyguard sur les appareils avec profil de travail et sur les appareils entièrement gérés et dédiés. La gestion du keyguard vous permet de spécifier les fonctionnalités disponibles pour les utilisateurs, 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.

Pour plus d'informations sur les paramètres de fonctionnalité et la manière de configurer la stratégie d'appareil, consultez la section Stratégie Gestion du keyguard.

Secure Hub 19.9.0

Secure Hub pour iOS

Secure Hub pour iOS prend en charge iOS 13.

Secure Hub pour Android

Cette version inclut des corrections de bogues.

Secure Hub pour Android 19.8.5

Cette version inclut des corrections de bogues.

Secure Hub 19.8.0

Secure Hub pour iOS

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

Secure Hub pour Android

Prise en charge de Android Q. Cette version prend en charge Android Q. Avant de mettre à niveau vers la plateforme Android Q : consultez Migrer de l'administration des appareils vers Android Enterprise pour plus d'informations sur la façon dont la dépréciation des API d'administration des appareils Google affecte les appareils exécutant Android Q. Consultez également le blog Citrix Endpoint Management et Android Enterprise : période de changement.

Secure Hub 19.7.5

Secure Hub pour iOS

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

Secure Hub pour Android

Prise en charge de Samsung Knox SDK 3.x. Secure Hub pour Android prend en charge Samsung Knox SDK 3.x. Pour plus d'informations sur la migration vers Samsung Knox 3.x, consultez la documentation Samsung Knox Developer. Cette version inclut également la prise en charge des nouveaux espaces de noms Samsung Knox. Pour plus d'informations sur les modifications apportées aux anciens espaces de noms Samsung Knox, reportez-vous à Modifications apportées aux anciens espaces de noms Samsung Knox.

> **Remarque :**
>
> Secure Hub pour Android ne prend pas en charge Samsung Knox 3.x sur les appareils fonctionnant sous Android 5.

Secure Hub 19.3.5 à 19.6.6

Ces versions incluent des améliorations de performance et des corrections de bogues.

Secure Hub 19.3.0

Prise en charge de Samsung Knox Platform for Enterprise. Secure Hub pour Android prend en charge Knox Platform for Enterprise (KPE) sur les appareils Android Enterprise.

Secure Hub 19.2.0

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

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 désormais en charge Android Enterprise. Pour de plus amples informations sur cette stratégie, consultez la section Stratégie d'appareil Wi-Fi.
- **Stratégie XML personnalisé.** La stratégie XML personnalisé prend en charge Android Enterprise désormais. Pour plus d'informations sur cette stratégie, consultez Stratégie XML personnalisé.
- **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.

Secure Hub 19.1.0

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

Secure Hub 18.12.0

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

Secure Hub 18.11.5

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

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

Secure Hub 18.10.0

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

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

- **Prise en charge d'Android SafetyNet :** vous pouvez configurer Endpoint Management pour utiliser la fonctionnalité **Android SafetyNet** permettant d'évaluer la compatibilité et la sécurité des appareils Android sur lesquels Secure Hub est installé. Les résultats peuvent être utilisés pour déclencher des actions automatisées sur les appareils. Pour plus d'informations, voir Android SafetyNet.

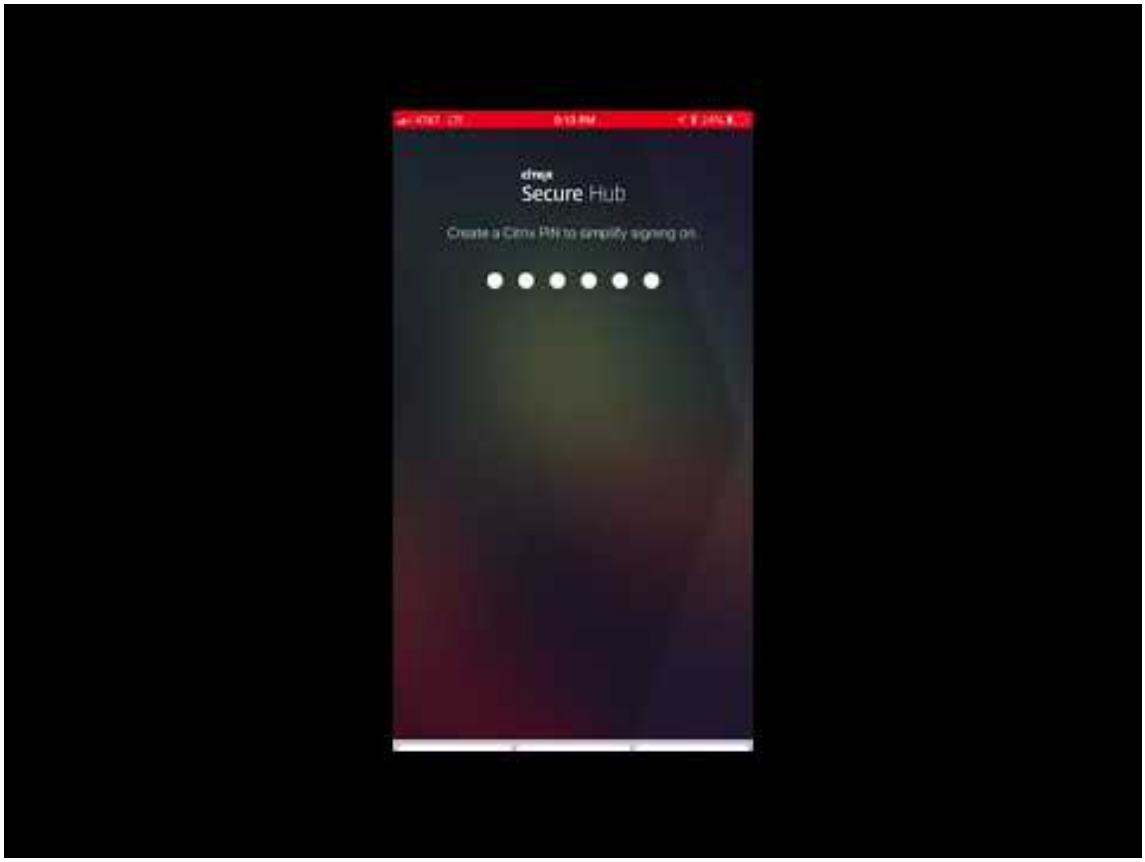
- **Empêcher l'utilisation de l'appareil photo pour les appareils Android Enterprise :** le nouveau paramètre **Autoriser l'utilisation de l'appareil photo** de la stratégie de restrictions vous permet d'empêcher les utilisateurs d'utiliser l'appareil photo sur leurs appareils Android Enterprise. Pour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

Secure Hub 10.8.60 à 18.9.0

Ces versions incluent des améliorations de performance et des corrections de bogues.

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 Configurer les espaces 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 plate-forme 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 d'informations, veuillez consulter la documentation Android Developer.

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 à ces stratégies 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 (Touch ID) 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 Gestion des appareils.
- Les autorités de certification privées/auto-signées et le service de découverte automatique (ADS) Endpoint Management 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. 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. Assurez-vous de ne pas envoyer la clé privée à 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 souhaitez ajouter au domaine, qui doivent être des certificats publics et non de la clé privée.
- 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.

Authentification par certificat + mot de passe à usage unique

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.

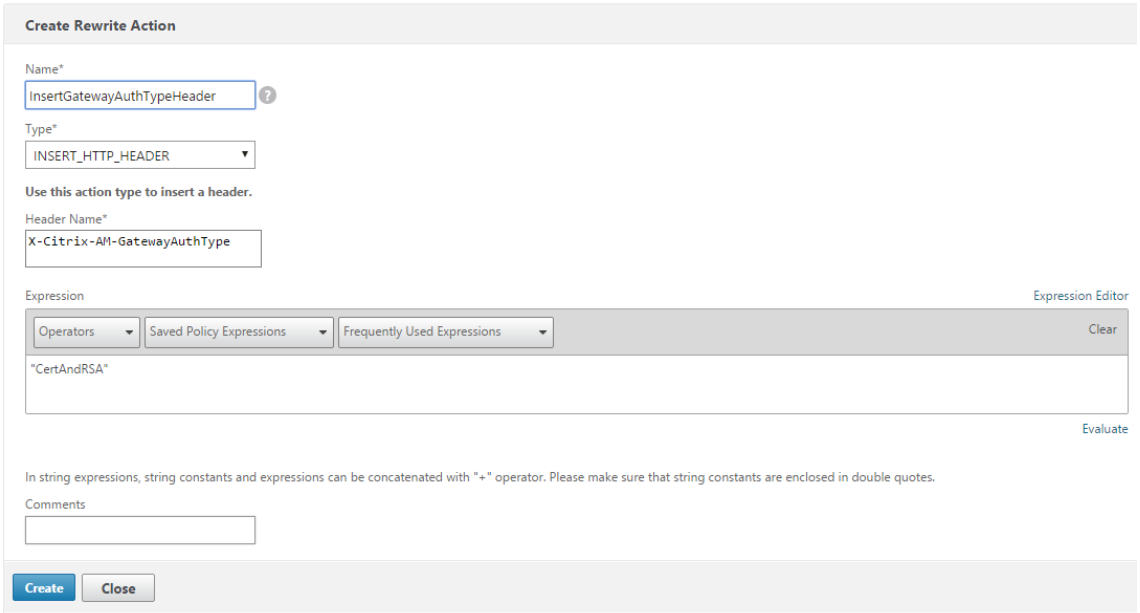
Pour permettre à Secure Hub d'utiliser le type d'authentification par certificat + mot de passe à usage unique, procédez comme suit : ajoutez une action de réécriture ainsi qu'une stratégie de réécriture dans Citrix ADC qui insère un en-tête de réponse personnalisé au format **X-Citrix-AM-GatewayAuthType: 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.

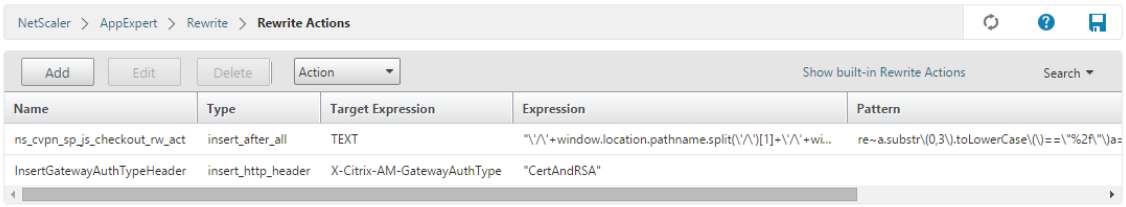
> **Remarque :**
>
> Si différents types d'ouverture de session sont définis dans Endpoint Management et Citrix ADC, la configuration de Citrix ADC a priorité. Pour de plus amples informations, consultez la section Citrix Gateway et Endpoint Management.

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

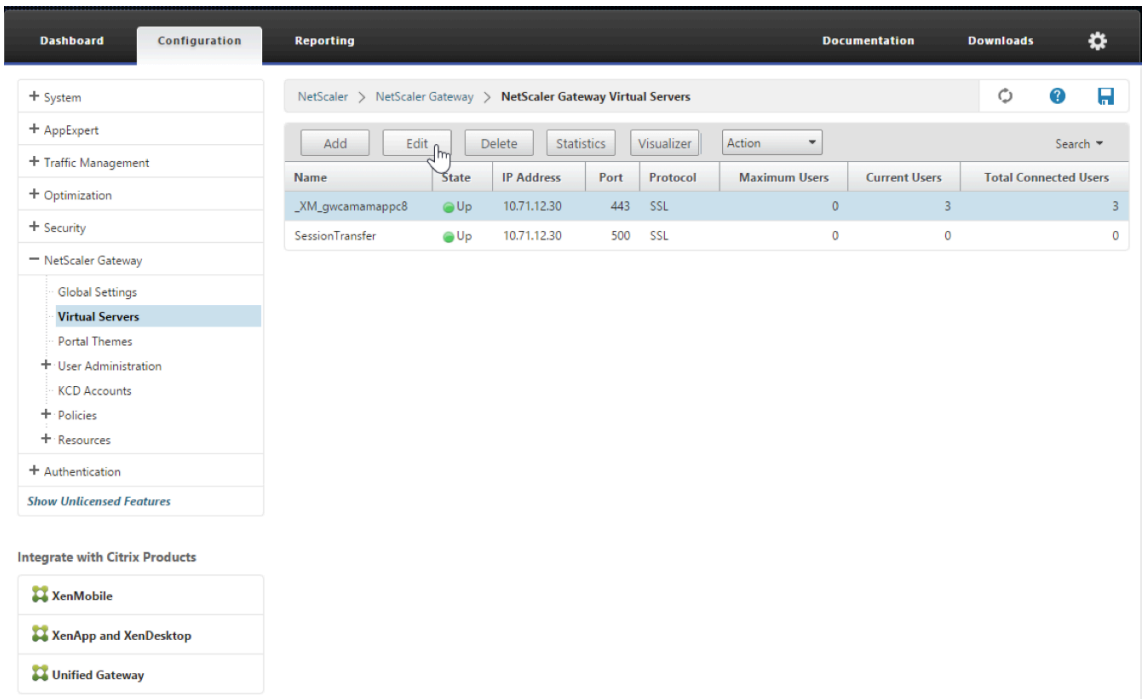
   L'écran **Create Rewrite Action** s'affiche.
3. Remplissez chaque champ, comme illustré dans la figure suivante et cliquez sur **Create**.



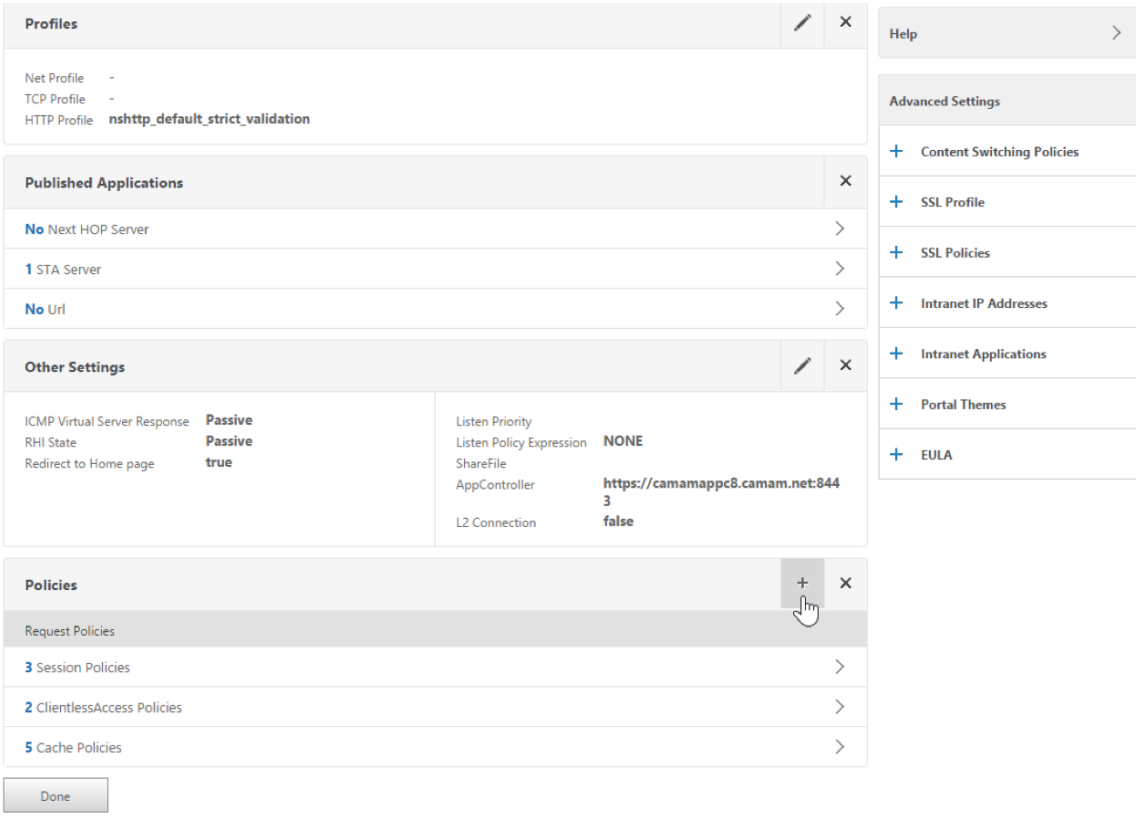
Le résultat suivant s'affiche sur l'écran principal **Rewrite Actions**.



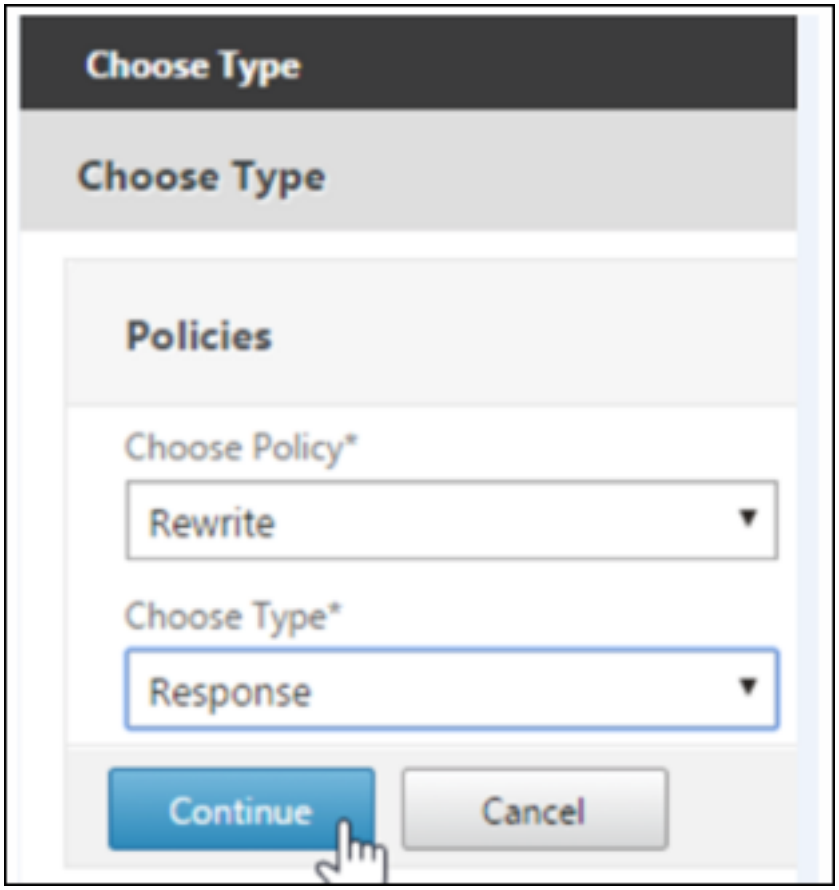
4. Liez l'action de réécriture au serveur virtuel en tant que stratégie de réécriture. Accédez à **Configuration > NetScaler Gateway > Virtual Servers** et sélectionnez votre serveur virtuel.



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

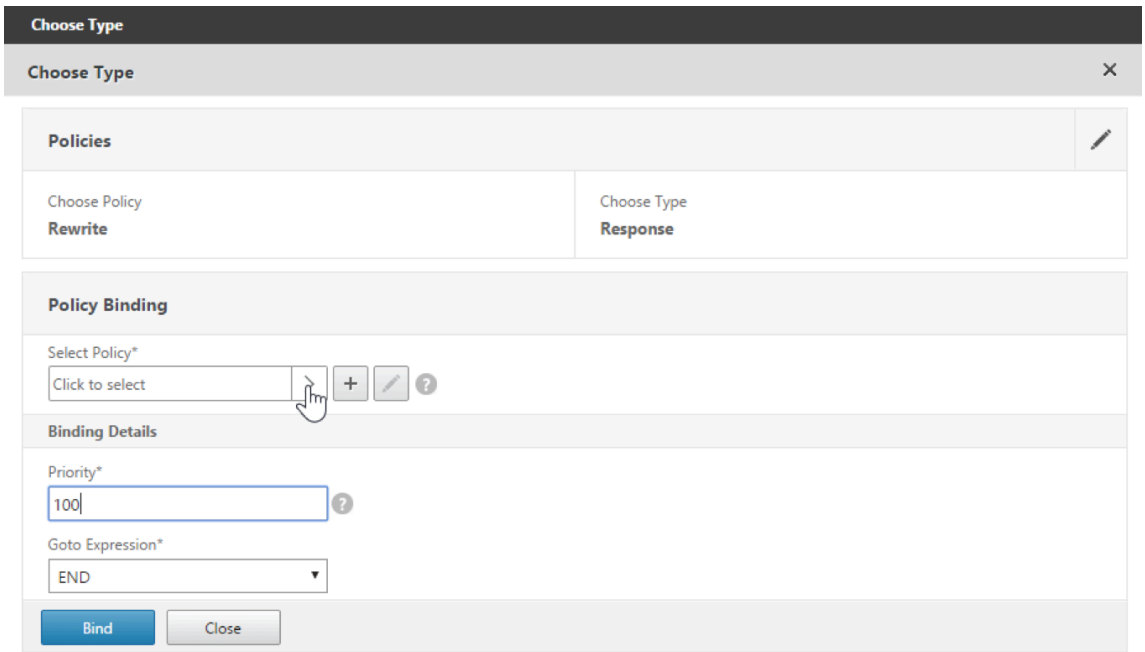


8. Dans le champ **Choose Policy**, choisissez **Rewrite**.
9. Dans le champ **Choose Type**, choisissez **Response**.



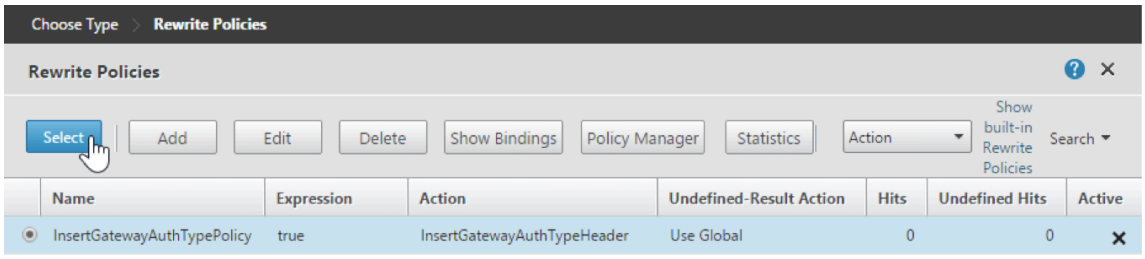
10. Cliquez sur **Continuer**.

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

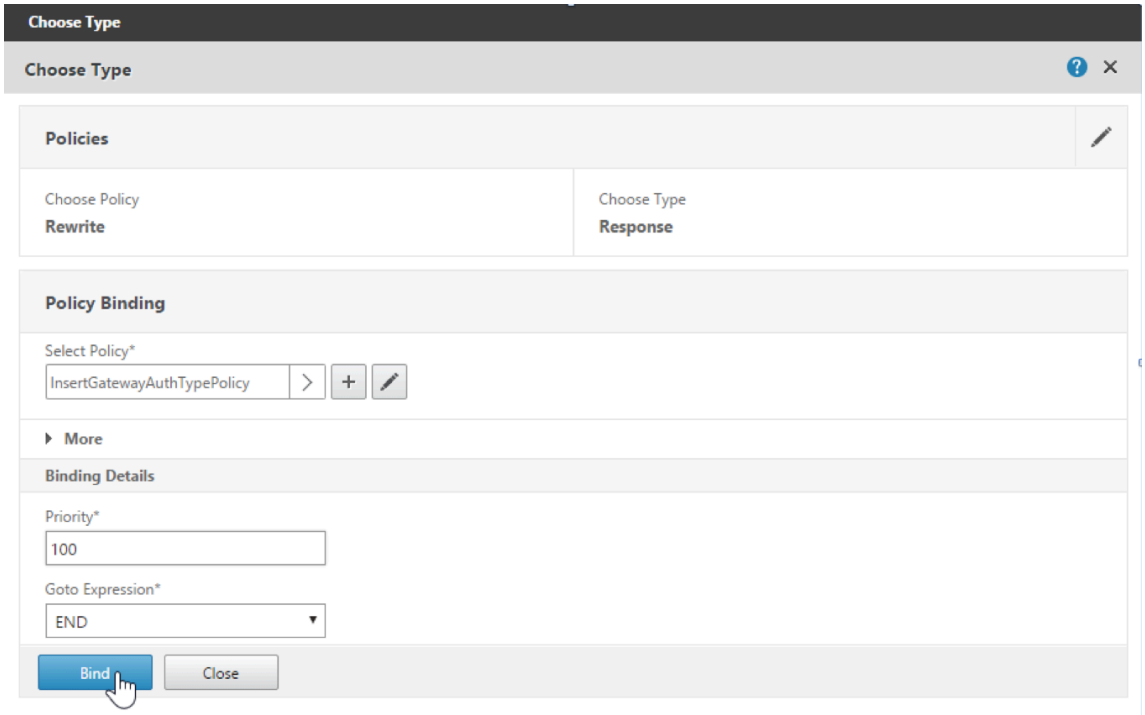


11. Cliquez sur **Select Policy**.

    Un écran répertoriant les stratégies disponibles s'affiche.

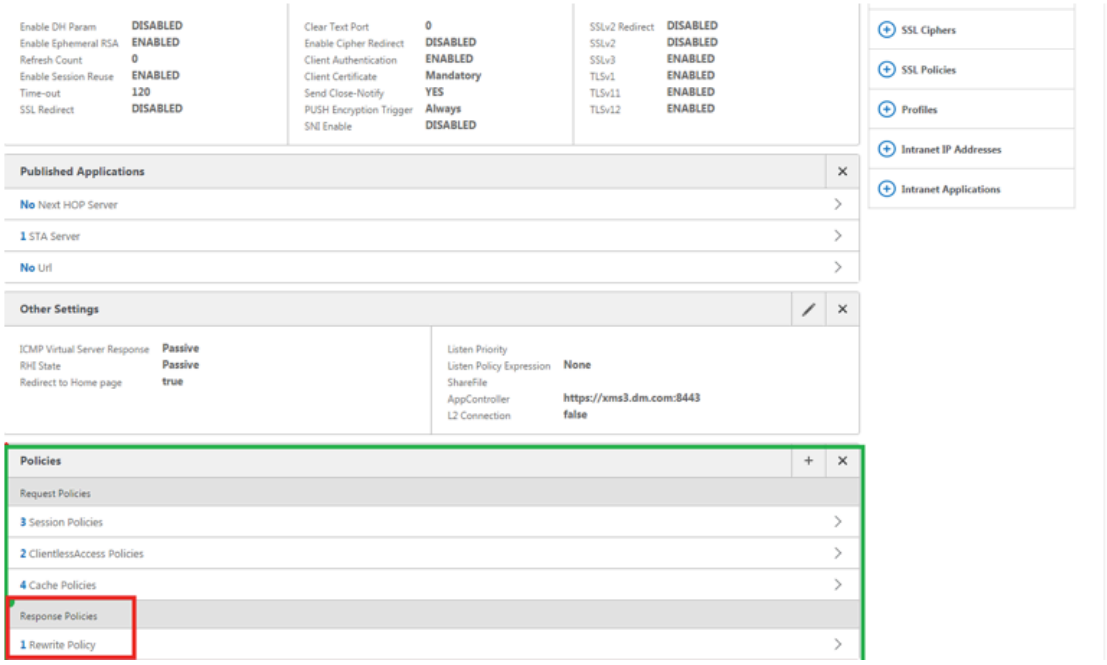


12. Cliquez sur la ligne de la stratégie que vous avez créée, puis cliquez sur **Select**. L'écran **Policy Binding** s'affiche de nouveau, avec la stratégie sélectionnée renseignée.

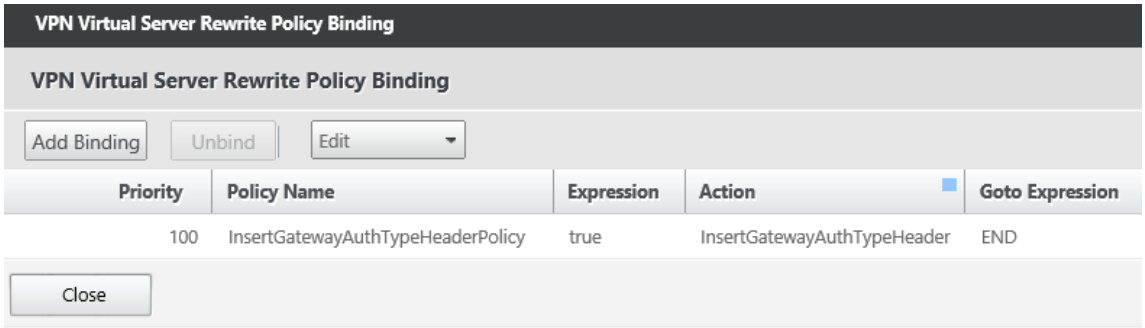


13. Cliquez sur **Bind**.

    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 envi-

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

Conditions préalables :

- 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 :

FQDN	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.

Désactiver l'option Supprimer le compte

Vous pouvez désactiver l'option **Supprimer le compte** dans Secure Hub dans les environnements où le service de détection automatique (ADS) est activé.

Effectuez les étapes suivantes pour désactiver l'option **Supprimer le compte** :

1. Configurez ADS pour votre domaine.
2. Ouvrez l'écran **Informations sur le service de détection automatique** dans Citrix Endpoint Management et définissez la valeur `displayReenrollLink` sur **False**.
   Par défaut, cette valeur est définie sur **True**.
3. Si votre appareil est inscrit en mode MDM+MAM (ENT), déconnectez-vous et connectez-vous à nouveau pour que les modifications prennent effet.
   Si votre appareil est inscrit dans d'autres modes, vous devez réinscrire l'appareil.

Utilisation de Secure Hub

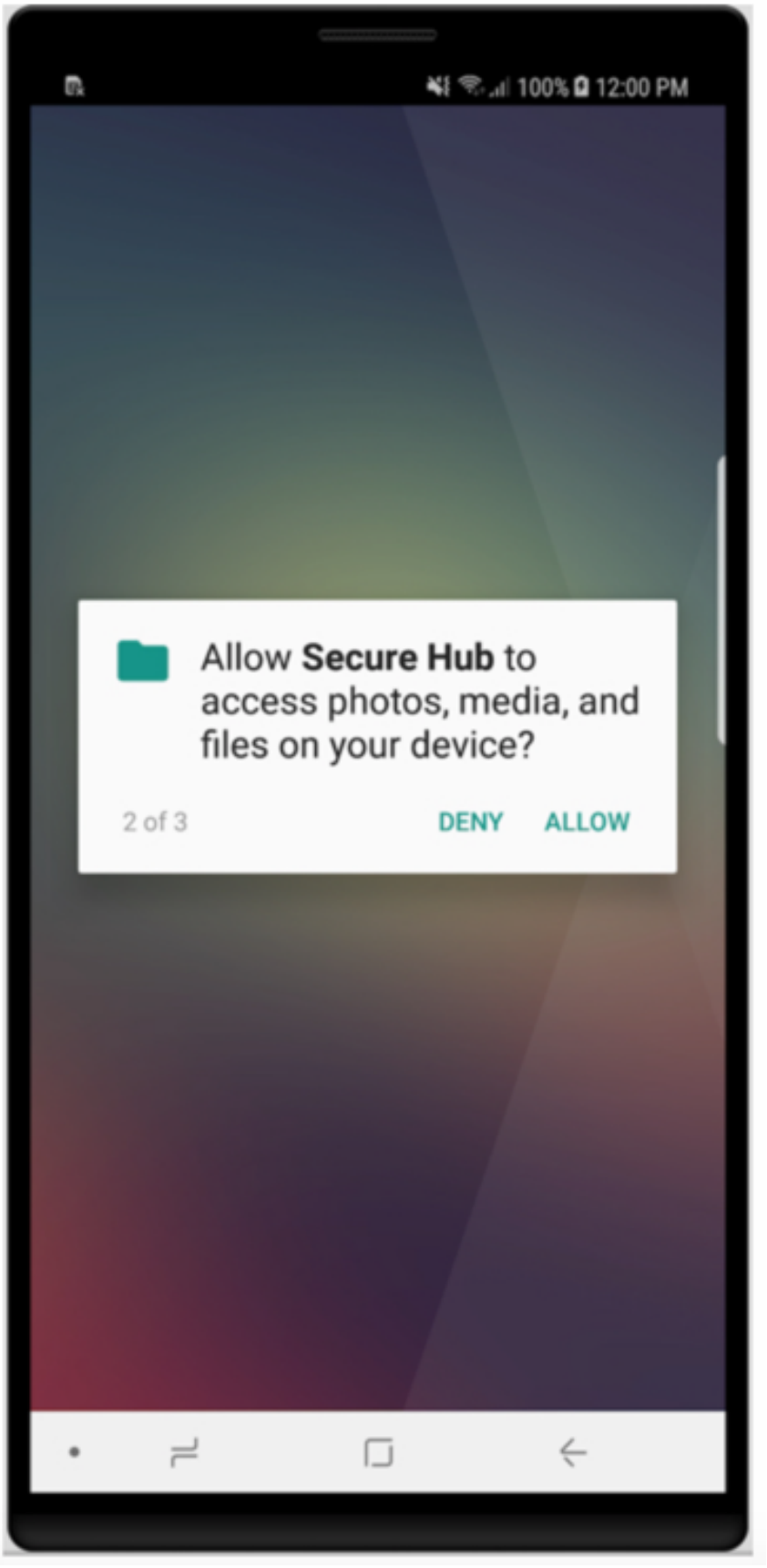
Les utilisateurs commencent par le téléchargement de Secure Hub sur leurs appareils depuis les magasins Apple ou Android.

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.

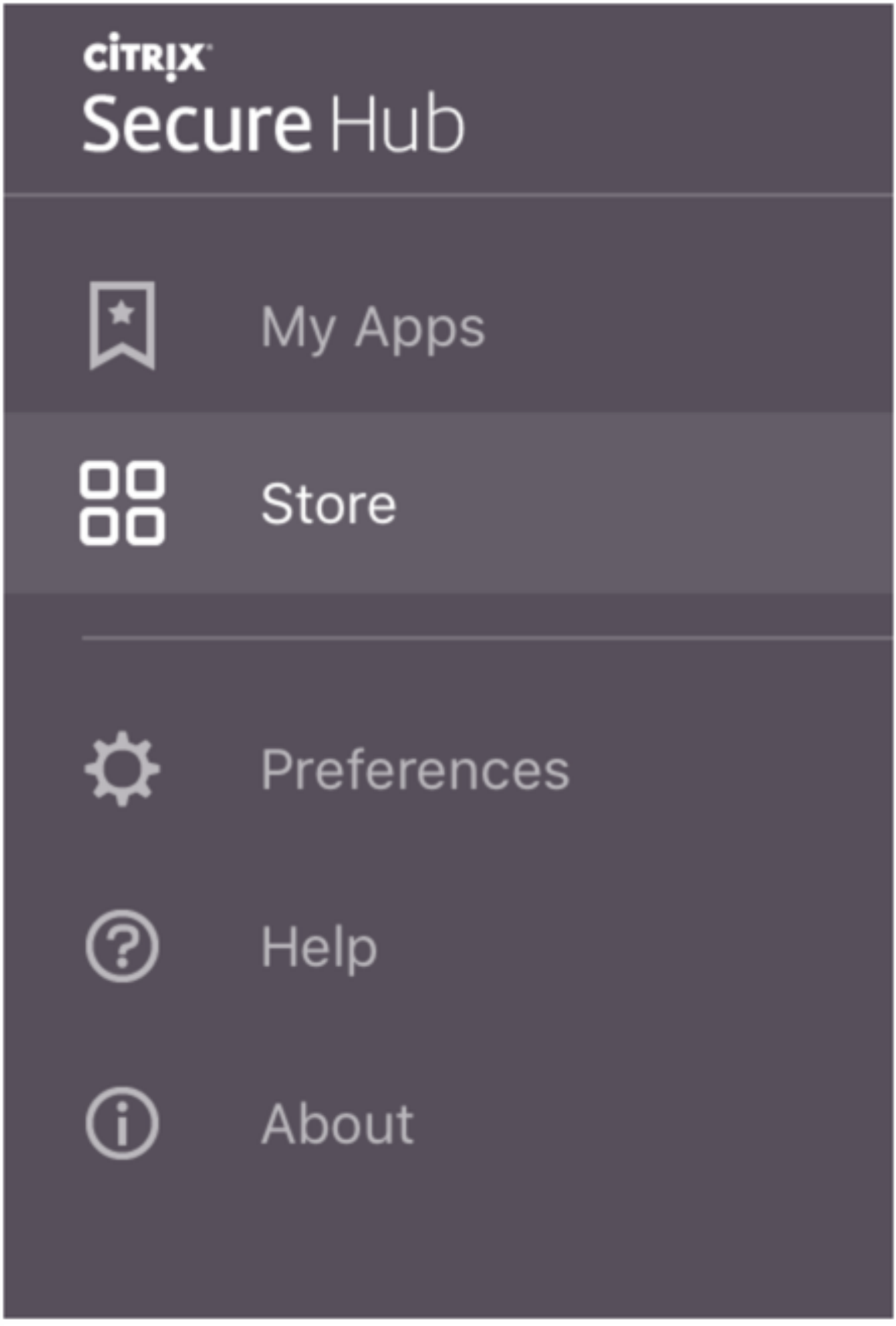
Sur Secure Hub pour Android, lors de l'installation et de l'inscription initiales, le message suivant s'affiche : Autoriser Secure Hub à accéder aux photos, médias et fichiers sur votre périphérique ?

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.

Inscription automatique dans Secure Mail

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.

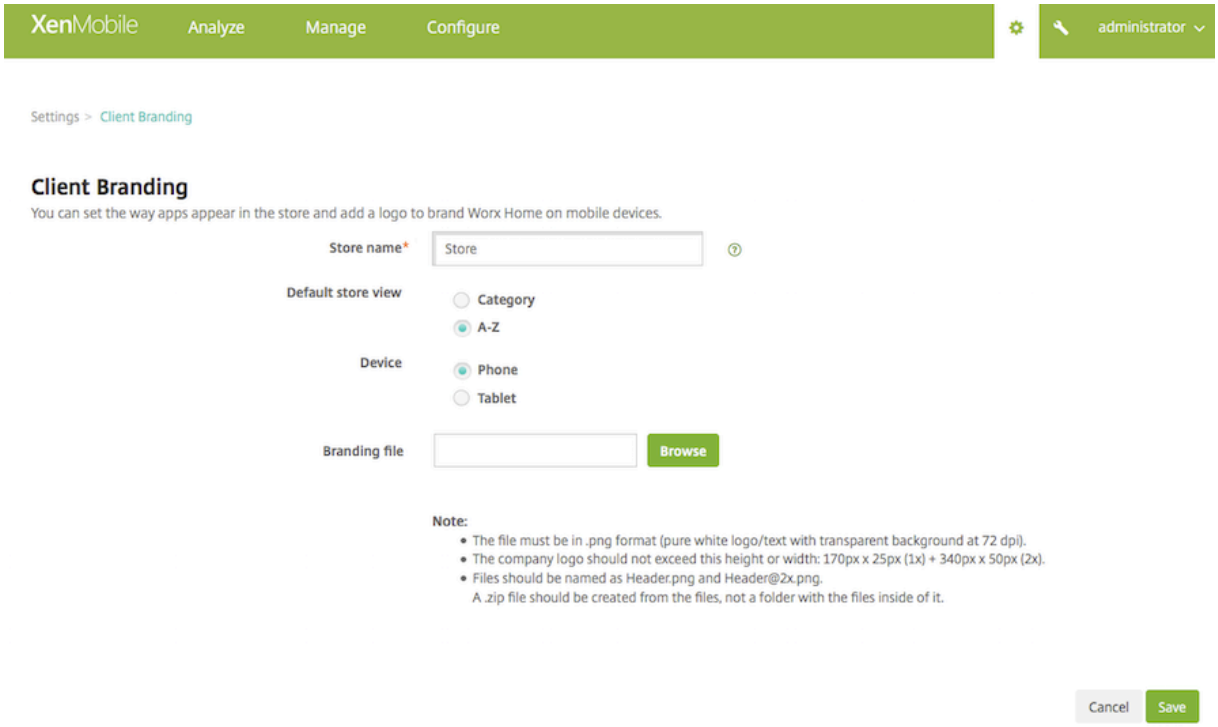
À la première utilisation de Secure Mail, Secure Mail obtient l'adresse e-mail de l'utilisateur, le domaine et l'ID utilisateur depuis Secure Hub. Secure Mail utilise l'adresse e-mail pour la détection automatique. Exchange Server est identifié par le domaine et l'ID utilisateur, ce qui permet à Secure 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 :

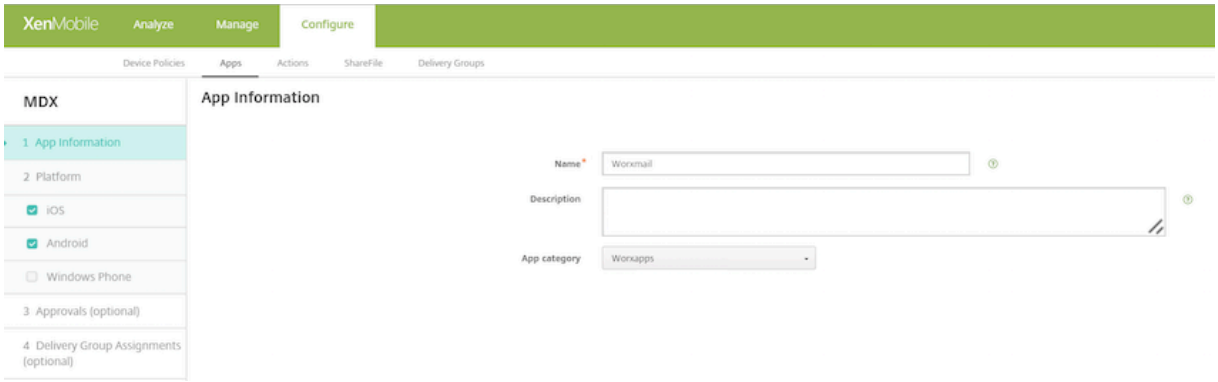
- La propriété de serveur MAM_MACRO_SUPPORT. Pour obtenir des instructions, consultez la section Propriétés de serveur.
- Les propriétés clientes ENABLE_CREDENTIAL_STORE et SEND_LDAP_ATTRIBUTES. Pour obtenir des instructions, consultez la section Propriétés de client.

Magasin personnalisé

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**.

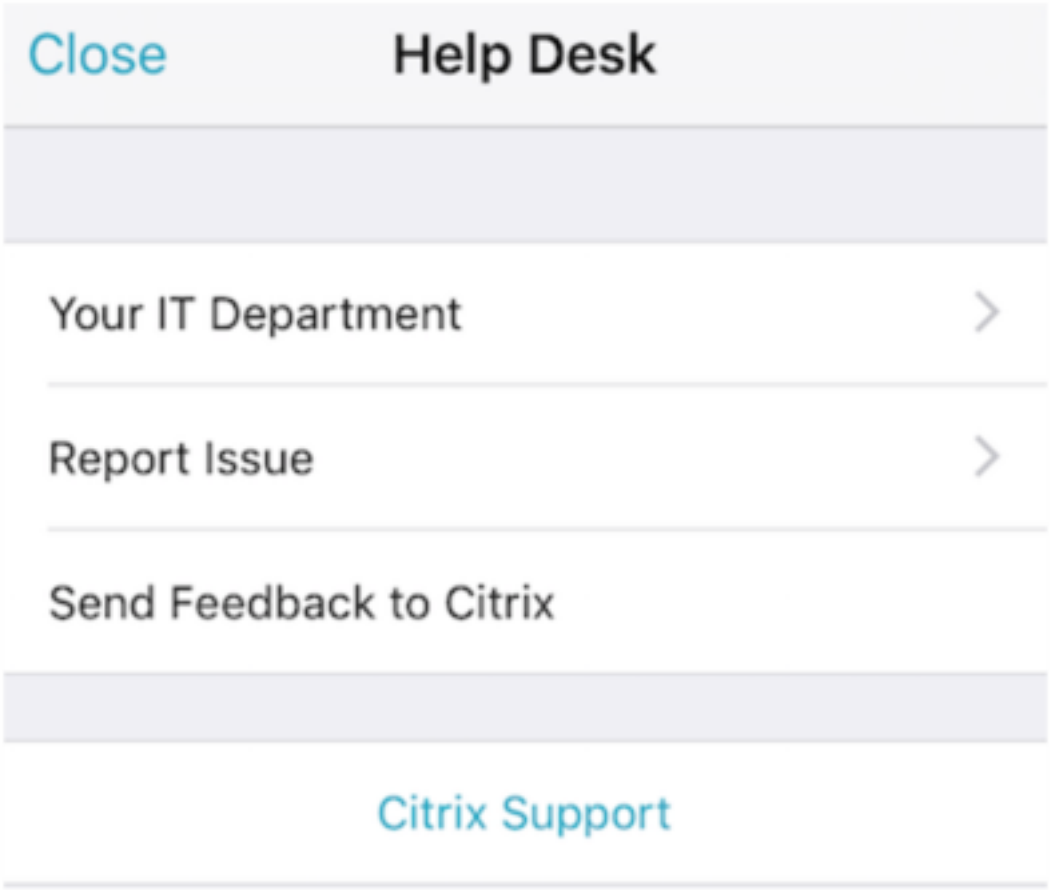


Dans le magasin, les utilisateurs peuvent rechercher uniquement les applications et bureaux que vous avez configurés et sécurisés dans Endpoint Management. Pour ajouter l'application, les utilisateurs appuient sur **Détails** et sur **Ajouter**.

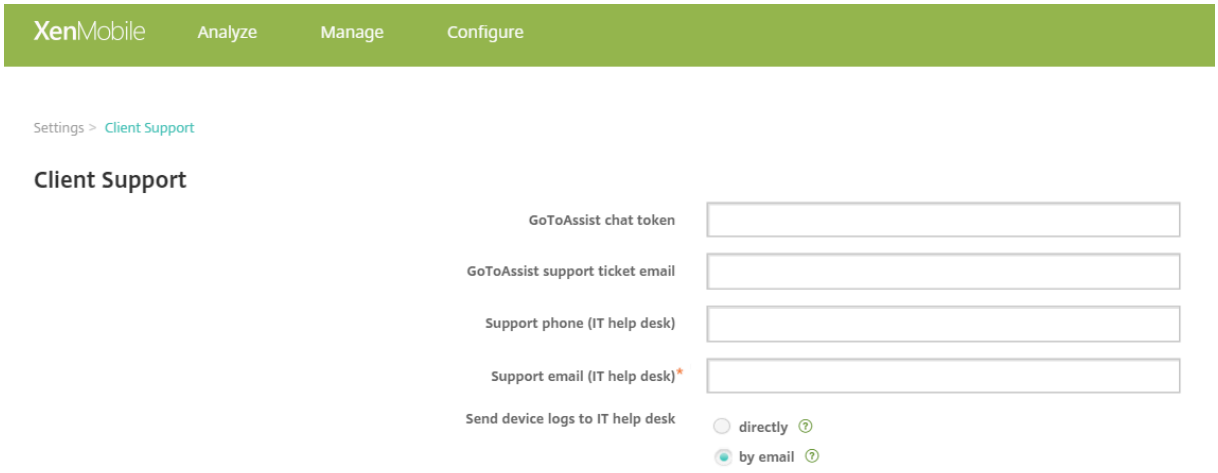
Options d'aide configurées

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.

Stratégies d'emplacement

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.

Collecte et analyse des échecs

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.

Pour connaître les fonctionnalités disponibles pour iOS et Android, consultez la matrice Fonctionnalités par plate-forme pour Citrix Secure Hub.

Problèmes connus et résolus

November 1, 2022

Citrix prend en charge les mises à niveau à partir des deux dernières versions des applications de productivité mobiles.

Secure Hub 22.9.0

Il n'y a aucun problème connu ou résolu dans cette version.

Secure Hub 22.7.0

Problèmes résolus

- Après être passé du SDK Mobile Device Experience (MDX) au SDK Citrix Mobile Application Management (MAM) et avoir mis à niveau XenMobile Server vers la version 10.13 RP4, vous ne pourrez peut-être pas accéder aux sites intranet via Secure Hub/ Secure Web.

  Le message d'erreur suivant s'affiche : « Err_Name_not_resolved ». [XMHELP-4035]
- Les paramètres de la stratégie de configuration gérée ne sont pas appliqués aux profils de travail dont la configuration d'inscription est Profil de travail sur appareils appartenant à l'entreprise (WPCOD). Le problème se produit lorsque l'authentification s'effectue via le fournisseur d'identité (IdP) et que le profil de travail n'est pas marqué comme provisionné. [XMHELP-3861]

Secure Hub 22.6.0

Il n'y a aucun problème connu ou résolu dans cette version.

Secure Hub 22.5.0

Il n'y a aucun problème connu ou résolu dans cette version.

Secure Hub 22.4.0

Il n'y a aucun problème connu ou résolu dans cette version.

Problèmes connus et résolus dans les versions antérieures

Pour connaître les problèmes connus et résolus dans les versions antérieures de Secure Hub, consultez la section Historique des problèmes connus et résolus dans Secure Hub.

Scénarios d'invite d'authentification

November 1, 2022

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.

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. Par exemple, lorsque 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 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 voient 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 :
>
> Le terme *application gérée* fait référence à une application encapsulée par l'outil MDX Toolkit, dans lequel vous avez laissé la stratégie MDX Code secret d'application activée par défaut 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.

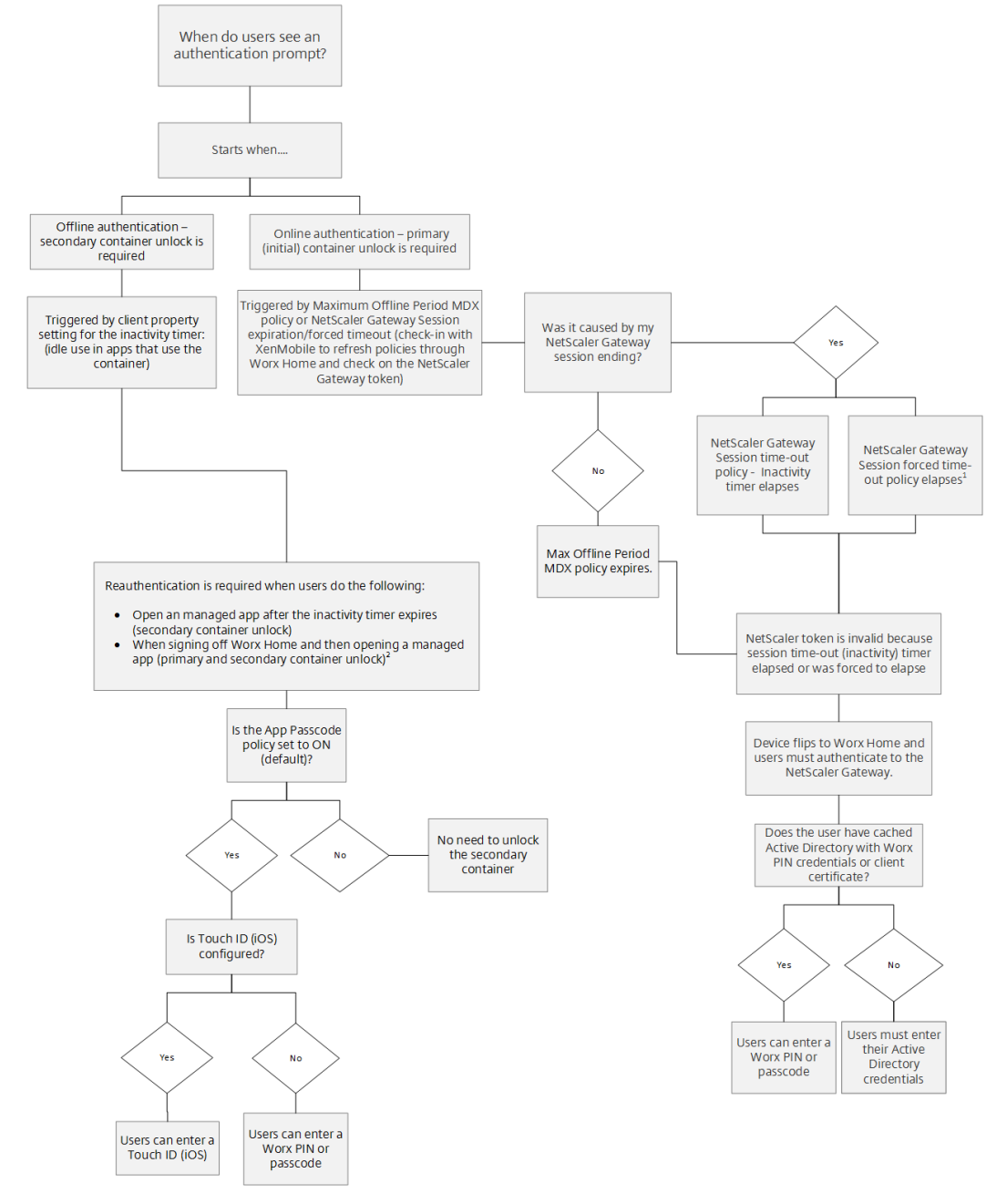
  - Sur Android, lorsque les utilisateurs redémarrent Secure Hub pour une raison quelconque, y compris le redémarrage d'un appareil.
- **Déverrouillage du conteneur secondaire :** l'authentification par empreinte digitale (si elle est configurée), un code PIN ou code secret Citrix ou des informations d'identification 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, puis ouvrent 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.



1 If you set the session forced time-out policy to a lower value than for the inactivity time-out policy, the forced time-out policy overrides the inactivity time-out policy.
2 To see how these situations differ for iOS and Android devices, see the Credential Types section in Authentication Prompt Scenarios in the Citrix documentation.

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 com-

munication avec Endpoint Management, comme indiqué par les stratégies MDX Période hors connexion 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.

Complexité du code d'accès de l'appareil (Android 12+)

La complexité du code d'accès est préférable à une exigence de mot de passe personnalisé. Le niveau de complexité du code d'accès est l'un des niveaux prédéfinis. De ce fait, l'utilisateur final n'est pas autorisé à définir un mot de passe avec un niveau de complexité inférieur.

La complexité du code d'accès pour les appareils tournant sous Android 12 ou version ultérieure est la suivante :

- **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 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

> **Remarques :**
>
> - 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.
> - Si la complexité du code d'accès du profil de travail est activée, la complexité du code d'accès côté appareil doit également être activée.

Pour plus d'informations, consultez la section Paramètres Android Enterprise de la documentation de Citrix Endpoint Management.

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).

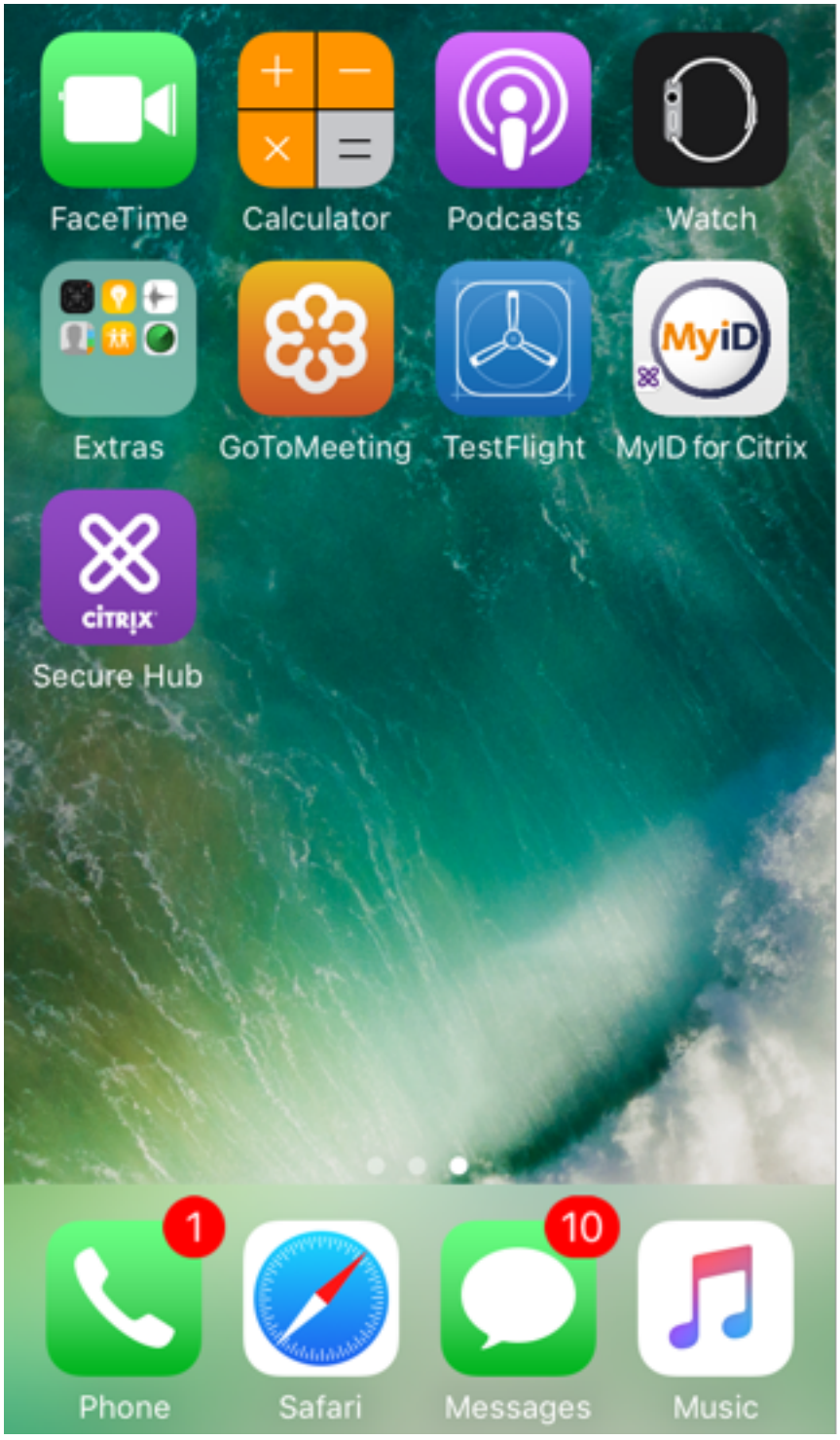
Les informations d'identification dérivées sont un certificat d'inscription qui contient l'identifiant de l'utilisateur, tel qu'un UPN (nom d'utilisateur principal). Endpoint Management stocke les informations d'identification obtenues à partir du fournisseur d'informations d'identification dans un coffre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

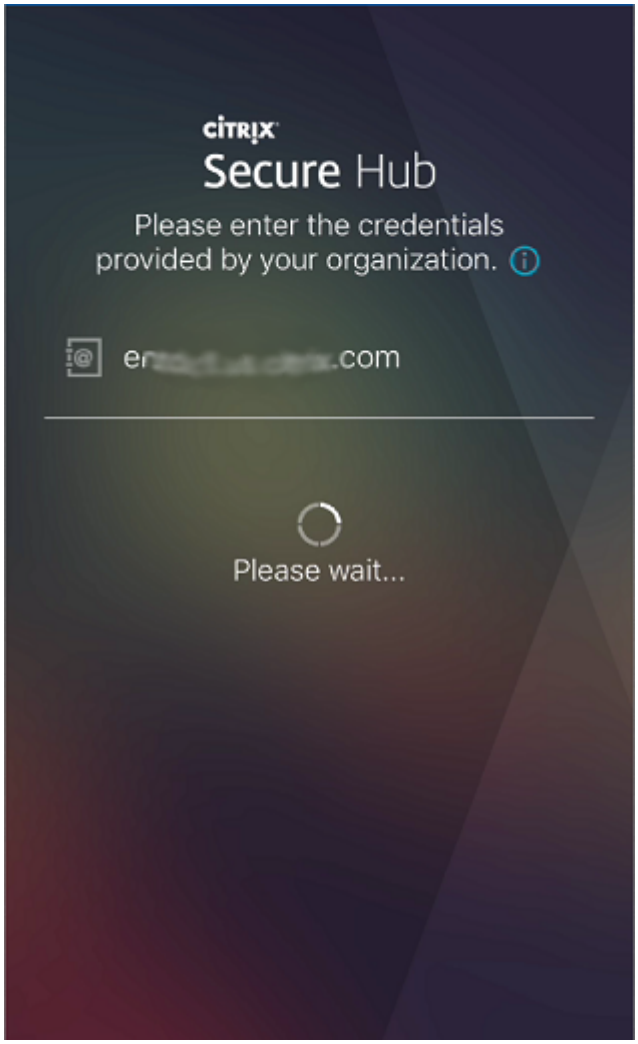
Étapes d'inscription d'un appareil lors de l'utilisation des informations d'identification dérivées

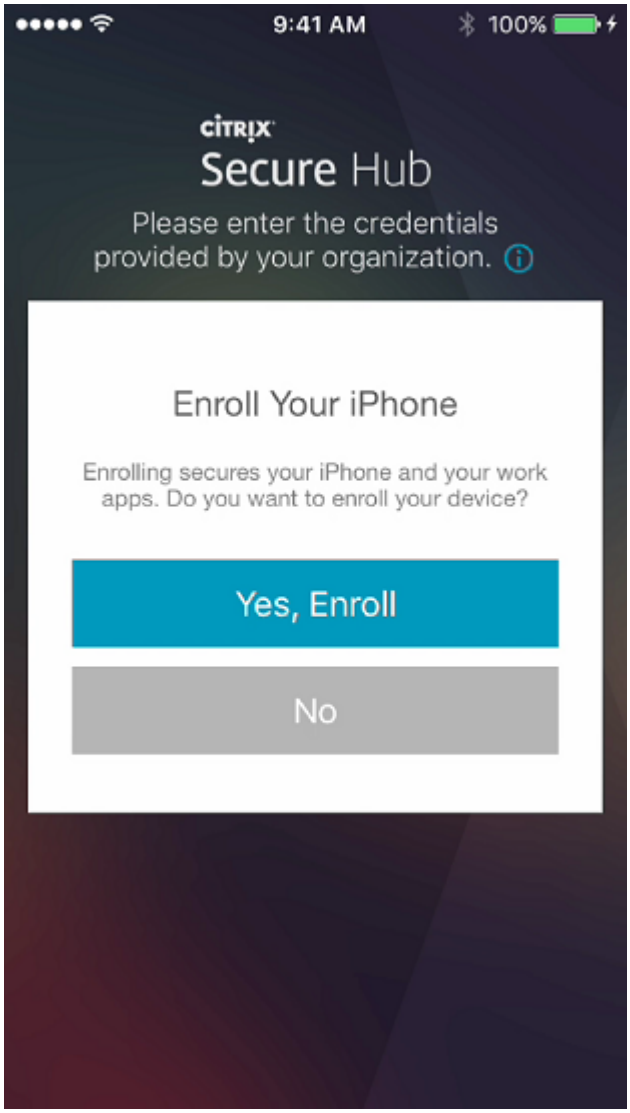
L'inscription nécessite que les utilisateurs insèrent leur carte à puce dans un lecteur connecté à leur bureau.

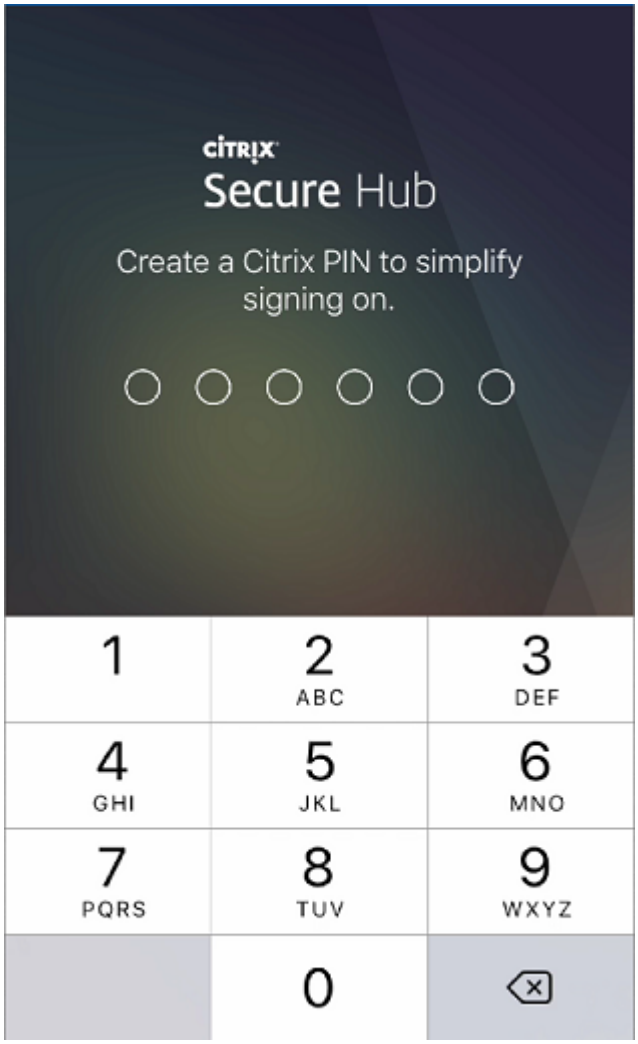
1. L'utilisateur installe Secure Hub et l'application à partir de votre fournisseur d'informations d'identification dérivées. Dans cet exemple, l'application de fournisseur d'identité est Intercede MyID Identity Agent.



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.

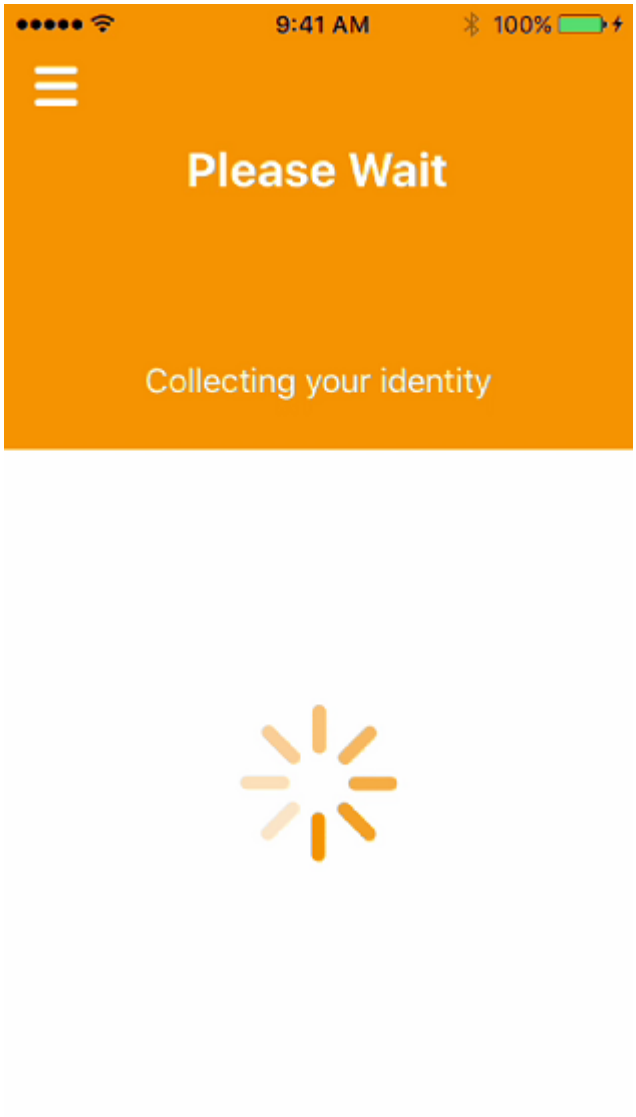




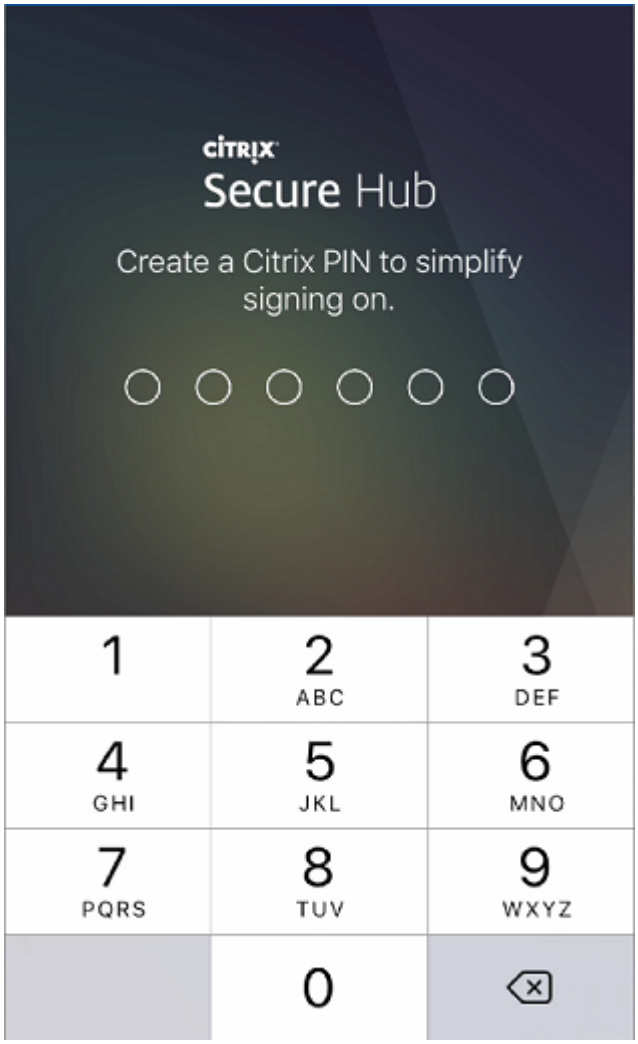


3. L’utilisateur suit les instructions permettant d’activer ses informations d’identification de carte à puce. Un écran de démarrage s’affiche, suivi d’une invite à scanner un code QR.

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**.

