Citrix Receiver pour Android 3.13

Contents

Nouveautés

October 4, 2019

Nouveautés dans la version 3.13.9

Cette version résout un certain nombre de problèmes afin d'améliorer la stabilité et les performances générales.

Nouveautés dans la version 3.13.8

Prise en charge de l'association de type de fichier pour StoreFront

Lorsque vous publiez des applications, vous les associez à certains types de fichiers présents sur le serveur. Ce faisant, vous redirigez le contenu de l'appareil utilisateur vers le serveur. Les appareils exécutant Receiver pour Android ouvrent les fichiers dont le type est associé à une application publiée spécifique. Par exemple, lorsque les utilisateurs cliquent deux fois sur une pièce jointe, la pièce jointe s'ouvre dans l'application associée.

Pour de plus amples informations, consultez la section Accéder aux fichiers à l'aide de l'association de type de fichier (FTA).

Prise en charge de l'épinglage sur Chromebook

Les raccourcis vers vos applications et bureaux favoris sont automatiquement disponibles dans Chrome App Launcher après l'ajout de votre compte à Citrix Receiver pour Android sur un Chromebook - non seulement lorsque vous vous connectez à StoreFront, mais également aux sites XenApp Services (anciennement appelés comptes PNA).

> **Remarque :**
>
> Cette fonctionnalité n'est pas prise en charge sur l'Interface Web.

Nouveautés dans la version 3.13.7

Mode de compatibilité NetScaler

L'option **Mode de compatibilité NetScaler** est disponible pour remédier à l'échec d'établissement d'une liaison TLS ou au code d'erreur 41E lors de la connexion à l'aide de versions antérieures de NetScaler. Pour obtenir davantage d'informations sur l'échec d'établissement de la liaison TLS, veuillez consulter l'article CTX221453 du centre de connaissances. Par défaut, les versions TLS sont définies sur TLS 1.0, 1.1, 1.2.

Nouveautés dans la version 3.13.6

Cette version résout un certain nombre de problèmes afin d'améliorer la stabilité et les performances générales.

Nouveautés dans la version 3.13.5

Ajouter des applications et des bureaux favoris au lanceur Chrome

Après avoir ajouté votre compte à Citrix Receiver pour Android exécuté sur un Chromebook, toutes vos applications et bureaux favoris sont automatiquement ajoutés au lanceur Chrome pour un accès rapide.

Prise en charge de HTTPS avec l'hub d'espace de travail Citrix Ready

Les connexions HTTPS sont désormais prises en charge entre Citrix Receiver pour Android et l'hub d'espace de travail Citrix Ready.

Nouveautés dans la version 3.13.4

Prise en charge de Citrix Ready Workspace Hub

Construit sur la plate-forme Raspberry Pi 3, le hub d'espace de travail Citrix Ready fournit une connexion sécurisée aux applications et données autorisées. Citrix Receiver pour Android prend en charge l'authentification des utilisateurs aux hubs d'espace de travail Citrix Ready en tant que fonctionnalité expérimentale.

Avec cette version, Citrix Receiver pour Android prend en charge Citrix Casting. Citrix Casting permet aux utilisateurs de transférer de manière sécurisée et transparente des sessions d'applications et de bureaux virtuels d'un périphérique mobile vers un hub d'espace de travail Citrix Ready en utilisant l'itinérance de session et des stations d'accueil sans fil. L'itinérance de session permet à votre téléphone de s'authentifier auprès d'un hub d'espace de travail Citrix Ready et d'utiliser en toute sécurité la session utilisateur sur le hub d'espace de travail. Les stations d'accueil sans fil permettent aux utilisateurs d'interagir avec leur téléphone et de diffuser n'importe quelle session d'application ou de bureau sur n'importe quel hub d'espace de travail.

Autorisations dynamiques

Auparavant, Citrix Receiver pour Android demandait toutes les autorisations lors de l'installation. Avec cette version, exécuté sur des appareils Android 6.x et plus récents, Citrix Receiver vous demande des autorisations dynamiquement uniquement lorsque vous en avez besoin, par exemple pour accéder à la carte SD, à l'emplacement et au téléphone.

Modifier les passerelles et les types d'authentification

Les utilisateurs peuvent maintenant modifier la passerelle préférée et le type d'authentification après l'ajout d'un compte.

> **Remarque :**
>
> Citrix Receiver renseigne tous les types d'authentification publiés par StoreFront. Les utilisateurs doivent contacter leur administrateur pour obtenir les types d'authentification pris en charge pour la passerelle sélectionnée.

Nouveautés dans la version 3.13.3

Lancement de sessions avec un certificat non approuvé

En réponse à la demande de nombreux utilisateurs, il est désormais possible de lancer des sessions avec un certificat non approuvé.

> **Remarque :**
>
> L'acceptation d'un certificat non approuvé présente un risque. Les administrateurs doivent transmettre les certificats approuvés par d'autres moyens (courrier électronique, liens de téléchargement, MDM, etc.) si possible.

Connexion simplifiée

Après s'être connecté pour la première fois, Citrix Receiver pour Android remplit automatiquement les champs de nom d'utilisateur et de domaine sur l'écran d'ouverture de session pour faciliter la connexion.

Codes QR pour hub d'espace de travail

Citrix Receiver pour Android détecte désormais le hub d'espace de travail à l'aide de codes QR.

Nouveautés dans la version 3.13.2

Synchronisation de la disposition du clavier

À compter de cette version, Citrix Receiver pour Android fournit une synchronisation dynamique de la disposition du clavier depuis la machine cliente vers le VDA dans une session. Cela permet aux utilisateurs de basculer entre leurs dispositions de clavier préférées sur la machine cliente, ce qui offre une expérience utilisateur cohérente, par exemple, lors du changement de la disposition du clavier de l'anglais vers l'espagnol. Lorsque les utilisateurs changent de disposition, ils voient un bref message

pendant que la synchronisation est en cours. Ils peuvent ensuite continuer à travailler avec la nouvelle disposition du clavier.

> **Remarque :**
>
> Cette fonctionnalité ne fonctionne que sur les claviers logiciels de l'appareil, et non sur les claviers externes. La case à cocher « Utiliser l'éditeur IME client » dans les paramètres de Citrix Receiver pour Android doit être cochée pour activer cette fonctionnalité.

Utiliser l'interface Web pour se connecter

Citrix Receiver pour Android 3.13.2 permet aux utilisateurs d'utiliser un navigateur Web pour se connecter plutôt que l'interface utilisateur native pour certaines installations antérieures.

Nouveautés dans la version 3.13.1

Nouvelle interface pour Citrix Receiver pour Android

L'interface utilisateur de Citrix Receiver pour Android a été repensée en fonction des nombreux commentaires fournis par la communauté des utilisateurs et conformément aux nouvelles directives de conception matérielle de Google pour les applications Android.

Certains avantages offerts par la nouvelle expérience utilisateur sont :

- Workflow plus rationalisé pour toutes les tâches. Il est maintenant plus facile d'exécuter les tâches dont les utilisateurs ont besoin pour être plus productifs.
- Directives de navigation pour se familiariser avec la nouvelle interface utilisateur.
- La prise en charge des commentaires est maintenant disponible dans l'application pour contacter Citrix avec la collecte automatique des journaux.
- Android Toasts et Snackbars à divers endroits pour aider à identifier le statut des opérations ainsi que les opérations d'annulation.

Prise en charge de Citrix Ready Workspace Hub

Construit sur la plate-forme Raspberry Pi 3, le hub d'espace de travail Citrix Ready fournit une connexion sécurisée aux applications et données autorisées. Dans cette version, Citrix Receiver pour Android prend en charge l'authentification des utilisateurs aux hubs d'espace de travail Citrix Ready en tant que fonctionnalité expérimentale. Cela permet aux utilisateurs authentifiés de diffuser leurs sessions sur un hub. Cette fonction est désactivée par défaut.

> **Remarque :**
>
> L'autorisation de localisation est requise pour la fonctionnalité expérimentale du hub d'espace de travail Citrix Ready. Vous pouvez refuser cette autorisation si aucun hub d'espace de travail

> n'est présent.

Prise en charge de DTLS sur le transport adaptatif

La prise en charge de DTLS a été activée pour le transport adaptatif à l'aide de NetScaler Gateway. Pour utiliser DTLS, assurez-vous que l'option EDT est activée dans le menu Paramètres de Citrix Receiver pour Android.

Scénarios de vérification recommandés pour la prise en charge de DTLS :

- Utilisez l'URL du magasin pour ajouter le magasin et lancer des sessions.
- Configurez la stratégie de transport adaptatif pour travailler dans les sessions XenApp et XenDesktop via EDT au lieu de TCP.

Pour plus d'informations sur la configuration du transport adaptatif, consultez la section Transport adaptatif.

Configuration automatique

Citrix Receiver pour Android 3.13.1 configure et détecte maintenant automatiquement les magasins pour les utilisateurs.

> **Remarque :**
>
> La configuration manuelle des magasins a été supprimée.

Problèmes résolus

October 4, 2019

Problèmes résolus dans la version 3.13.9

Cette version résout un certain nombre de problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus dans la version 3.13.8

- Après avoir ajouté un compte, le paramètre Enregistrer le mot de passe du compte de l'Interface Web peut ne pas être reflété dans une session. [RFANDROID-570]
- Sur un VDA s'exécutant sur la mise à jour cumulative 5 (CU5) de la version 7.5, vous ne pourrez peut-être pas lancer d'applications d'édition de texte telles que Bloc-notes dans une session. [RFANDROID-2164]

Problèmes résolus dans la version 3.13.7

Cette version résout un certain nombre de problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus dans la version 3.13.6

- Citrix Receiver pour Android peut ne pas lancer une session lors de l'ouverture d'un fichier ICA téléchargé à partir du navigateur. [#RFANDROID-2098]

Problèmes résolus dans la version 3.13.5

- Citrix Receiver pour Android peut ne pas lancer correctement les applications SaaS (Software-as-a-Service). [#RFANDROID-1963]

Problèmes résolus dans la version 3.13.4

- Avec ce correctif, vous pouvez redimensionner dynamiquement Citrix Receiver lorsque vous utilisez un Chromebook. [#RFANDROID-1991]

Problèmes résolus dans la version 3.13.3

- Les graphiques sur les bureaux publiés peuvent apparaître déformés lors de l'utilisation d'un compte de démo sur Android Nougat 7.1.1. [#RFANDROID-1990]
- Les magasins configurés avec des balises internes pointant vers un emplacement redirigé peuvent ne pas se connecter lorsqu'ils se trouvent sur un réseau interne. [#RFANDROID-1992]

Problèmes résolus dans la version 3.13.2

- Les sessions déconnectées ne se lancent pas lorsque vous ajoutez le compte ou que vous appuyez sur Actualiser dans le menu. [#RFANDROID-1456]
- Citrix Receiver pour Android n'énumère pas les applications lors de l'utilisation de XenApp 6.5. [#RFANDROID-1887]
- Citrix Receiver pour Android peut se fermer de manière inattendue lors du rendu d'icônes héritées. [#RFANDROID-1958]
- Citrix Receiver pour Android peut se fermer de manière inattendue lors de l'inscription à un compte de démonstration et que le prénom ou le nom de l'utilisateur contient des espaces vides. [#RFANDROID-1960]

- Citrix Receiver pour Android peut ne pas être installé sur les Chromebooks prenant en charge les applications Android. [#RFANDROID-1968]

Problèmes résolus dans la version 3.13.1

- Citrix Receiver ne reconnaît pas le nom du client dans le fichier default.ica lorsqu'il est répertorié sous une entrée d'application spécifique. [#LC7539]
- L'écran VDI clignote lors de l'utilisation de Citrix Receiver pour Android 3.11.1. [#RFANDROID - 1642, #LC7800]
- Lorsque vous utilisez uniquement des certificats pour authentifier une session, Citrix Receiver pour Android peut ne pas détecter la passerelle. [#RFANDROID-1882]
- Les mots de passe avec un espace vide au début ou à la fin ne sont pas respectés. [#RFANDROID-1890]
- Citrix Receiver pour Android peut se fermer de manière inattendue lors de la connexion à des magasins configurés sans authentification. [#RFANDROID-1929]
- Les magasins StoreFront configurés sans authentification sur NetScaler Gateway peuvent ne pas être détectés. [#RFANDROID-1936]
- Les utilisateurs peuvent ne pas être en mesure de se connecter aux sites Interface Web configurés derrière NetScaler Gateway. [#RFANDROID-1937]
- Les applications 16 bits peuvent apparaître déformées sur les périphériques exécutant Android Oreo. [#RFANDROID-1938]
- Les problèmes de connexion aux magasins PNA et XenApp sont résolus. Si vous rencontrez le code d'erreur 547, activez l'option « Autoriser l'accès aux anciens magasins » et essayez de vous reconnecter.

Problèmes connus

October 4, 2019

Problèmes connus dans la version 3.13.9

Aucun nouveau problème n'a été observé dans cette version.

Problèmes connus dans la version 3.13.8

Si vous ajoutez le compte Store configuré avec l'association de type de fichier sur Receiver pour Android version 3.13.7 et versions inférieures et que vous mettez à niveau Receiver vers la dernière version, Citrix Receiver n'est pas affiché en tant qu'option dans la boîte de dialogue « Ouvrir avec » lorsque vous sélectionnez un fichier à lancer.

Pour contourner le problème, accédez à **Paramètres** > **Actualiser**.[RFANDROID-2241]

Problèmes connus dans la version 3.13.7

Aucun nouveau problème n'a été observé dans cette version.

Problèmes connus dans la version 3.13.6

Aucun nouveau problème n'a été observé dans cette version.

Problèmes connus dans la version 3.13.5

Citrix Receiver pour Android peut ne pas lancer une session lors de l'ouverture d'un fichier ICA téléchargé à partir du navigateur. Pour contourner ce problème, téléchargez une application d'explorateur de fichiers à partir du Google Play Store, localisez le fichier sur votre appareil, puis ouvrez-le directement. [#RFANDROID-2098]

Problèmes connus dans la version 3.13.4

Aucun nouveau problème n'a été observé dans cette version.

Problèmes connus dans la version 3.13.3

Aucun nouveau problème n'a été observé dans cette version.

Problèmes connus dans la version 3.13.2

- L'option Ajouter au téléphone qui permet d'ajouter des applications et des bureaux à l'écran du téléphone ne fonctionne pas. [#RFANDROID-1896]
- Cette version de Citrix Receiver pour Android peut ne pas fonctionner correctement avec NetScaler Gateway intégré à XenApp Services et au site Web.

  Pour contourner le problème, procédez comme suit :

  1. Appuyez sur « Fermer session (toutes) » à partir des paramètres.

2. Appuyez sur « Changer de compte » pour accéder à la page « Comptes ».
3. Supprimez le magasin à partir de la page « Comptes ».
4. Ajoutez de nouveau le compte. [#RFANDROID-1900]

Problèmes connus dans la version 3.13.1

- Les sessions déconnectées ne se lancent pas lorsque vous ajoutez le compte ou que vous appuyez sur Actualiser dans le menu. [#RFANDROID-1456]
- Les applications publiées sur XenApp 6.5 ne sont pas lancées. [#RFANDROID-1887]
- L'option Ajouter au téléphone qui permet d'ajouter des applications et des bureaux à l'écran du téléphone ne fonctionne pas. [#RFANDROID-1896]
- Cette version de Citrix Receiver pour Android peut ne pas fonctionner correctement avec NetScaler Gateway intégré à XenApp Services et au site Web.

  Pour contourner le problème, procédez comme suit :

  1. Appuyez sur « Fermer session (toutes) » à partir des paramètres.
  2. Appuyez sur « Changer de compte » pour accéder à la page « Comptes ».
  3. Supprimez le magasin à partir de la page « Comptes ».
  4. Ajoutez de nouveau le compte. [#RFANDROID-1900]

Avis de tiers

August 31, 2018

Les produits Citrix contiennent souvent du code tiers octroyé sous licence à Citrix à des fins d'utilisation et de redistribution sous une licence Open Source. Afin de mieux informer ses clients, Citrix publie le code Open Source inclus dans les produits Citrix dans une liste des codes utilisés sous licence Open Source.

Vous pouvez consulter la liste Open Source ici : https://www.citrix.com/buy/licensing/open-source.html

Pour plus d'informations sur la source, consultez : https://www.citrix.com/downloads/citrix-receiver/receiver-for-android-source/htmlparser.html

Configuration système requise

October 4, 2019

Configuration requise par l'appareil

Cette version de Citrix Receiver pour Android prend en charge Android 4.4 (KitKat), 5.x (Lollipop), 6.x (Marshmallow), 7.x (Nougat), et 8.x (Oreo).

Pour garantir des résultats optimaux, mettez à jour vos appareils Android vers la dernière version du logiciel Android.

Citrix Receiver pour Android prend en charge le lancement de sessions à partir de Receiver pour Web, à condition que le navigateur Web fonctionne avec Receiver pour Web. Si le lancement échoue, configurez votre compte directement via Citrix Receiver pour Android.

Reportez-vous à la section Connectivité pour obtenir des informations sur les connexions sécurisées à votre environnement Citrix.

> **Important**
>
> Si une version Tech Preview de Citrix Receiver pour Android est installée, désinstallez-la avant d'installer la nouvelle version.

Éléments requis sur les serveurs

StoreFront :

- StoreFront 2.6 ou version ultérieure

  Permet d'accéder directement aux magasins StoreFront. Receiver prend également en charge les versions antérieures de StoreFront.

- StoreFront configuré avec un site Receiver pour Web

  Permet d'accéder aux magasins StoreFront à partir d'un navigateur Web. Pour prendre connaissance des limitations de ce déploiement, consultez la documentation StoreFront.

Interface Web (non prise en charge avec les déploiements XenDesktop 7 et ultérieurs) :

- Interface Web 5.4 avec des sites Interface Web
- Interface Web 5.4 avec des sites XenApp Services

Interface Web sur NetScaler :

Vous devez activer les stratégies de réécriture fournies par NetScaler.

XenApp et XenDesktop (l'un des produits suivants) :

- XenApp 7.5 ou version ultérieure
- XenApp 6.5 pour Windows Server 2008 R2
- XenDesktop 7.x ou version ultérieure

Connectivité

Citrix Receiver pour Android prend en charge les connexions HTTP, HTTPS et ICA-over-TLS à une batterie de serveurs XenApp par le biais des configurations suivantes.

Pour les connexions LAN :

- StoreFront 2.6 ou version ultérieure
- Interface Web 5.4
- Site XenApp Services (anciennement Program Neighborhood Agent).

Pour les connexions à distance sécurisées (l'un des produits suivants) :

- Citrix NetScaler Gateway 10 et 11 (y compris les versions VPX, MPX et SDX)
- XenMobile est uniquement pris en charge avec les versions 9 et 10.

À propos des connexions sécurisées et des certificats TLS

Pour assurer la sécurité des connexions à distance à l'aide de TLS, l'appareil mobile vérifie l'authenticité du certificat TLS de la passerelle distante par rapport à un magasin local d'autorités de certification approuvées. L'appareil reconnaît automatiquement les certificats délivrés par des sociétés de distribution (telles que VeriSign et Thawte) à condition que le certificat racine de l'autorité de certification existe dans le magasin de clés local.

Certificats privés (auto-signés)

Si un certificat privé est installé sur la passerelle distante, le certificat racine de l'autorité de certification doit être installé sur l'appareil mobile pour pouvoir accéder aux ressources Citrix à l'aide de Receiver.

> **Remarque :**
>
> Lorsque le certificat de la passerelle distante ne peut pas être vérifié lors de la connexion (car le certificat racine n'est pas inclus dans le magasin de clés), un avertissement relatif à un certificat non approuvé s'affiche. Si un utilisateur choisit d'ignorer l'avertissement, une liste des applications s'affiche ; toutefois, l'application ne se lance pas.

Certificats génériques

Les certificats génériques remplacent les certificats de serveur individuel pour n'importe quel serveur situé dans le même domaine. Citrix Receiver pour Android prend en charge les certificats génériques.

Certificats intermédiaires et NetScaler Gateway

Si votre chaîne de certificat contient un certificat intermédiaire, ce dernier doit être ajouté au certificat serveur d'Access Gateway. Consultez l'article du centre de connaissances qui correspond à votre édition d'Access Gateway :

CTX114146 : How to Install an Intermediate Certificate on NetScaler Gateway

Outre les rubriques relatives à la configuration dans cette section de la documentation Produit, consultez également :

CTX124937 : How to Configure NetScaler Gateway for Use with Citrix Receiver for Mobile Devices

Authentification

> **Remarque :**
>
> L'authentification RSA SecurID n'est pas prise en charge pour les configurations Secure Gateway. Pour utiliser l'authentification RSA SecurID, utilisez NetScaler Gateway.

Citrix Receiver pour Android prend en charge l'authentification via NetScaler Gateway à l'aide des méthodes suivantes, selon l'édition que vous possédez :

- Aucune authentification (versions Standard et Enterprise uniquement)
- Authentification de domaine
- RSA SecurID, y compris des jetons logiciels pour les appareils Wi-Fi et non Wi-Fi
- Authentification de domaine associée à RSA SecurID
- Authentification par code d'accès SMS (code PIN à usage unique)
- Authentification par carte à puce

> **Remarque :**
>
> L'authentification par carte à puce n'est pas prise en charge sur les sites Interface Web.

Citrix Receiver pour Android prend désormais en charge les configurations et produits suivants.

Lecteurs de cartes à puce pris en charge :

- Lecteur de carte à puce Bluetooth BaiMobile 3000MP

Cartes à puce prises en charge :

- Cartes PIV
- Cartes CAC

Configurations prises en charge :

- Authentification par carte à puce à NetScaler Gateway avec StoreFront 2 ou 3 et XenDesktop 7.x et versions supérieures ou XenApp 6.5 et versions supérieures.

- Authentification par carte à puce à NetScaler Gateway avec Interface Web 5.4.2 et XenDesktop 7.x et versions supérieures ou XenApp 6.5 et versions supérieures.

> **Remarque :**
>
> Les autres solutions d'authentification à base de jeton peuvent être configurées à l'aide de RADIUS. Pour plus d'informations sur l'authentification par jeton SafeWord, reportez-vous à la section Configuration de l'authentification SafeWord.

Déployer

October 4, 2019

Communiquer les informations d'accès aux utilisateurs d'appareils Android

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

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

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

Vous pouvez configurer Citrix Receiver de manière à utiliser la découverte de compte basée sur e-mail. Une fois configurée, plutôt que d'entrer une adresse URL de serveur, les utilisateurs entrent leur adresse e-mail durant l'installation et la configuration de Citrix Receiver. Citrix Receiver identifie le serveur Access Gateway ou StoreFront associé à l'adresse e-mail en se basant sur les enregistrements SRV de DNS et invite les utilisateurs à ouvrir une session pour accéder à leurs applications, données et bureaux hébergés.

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

Fournir un fichier de provisioning aux utilisateurs

Vous pouvez utiliser StoreFront pour créer des fichiers de provisioning contenant les détails des comptes. Vous pouvez mettre ces fichiers à la disposition de vos utilisateurs pour leur permettre

de configurer Citrix Receiver automatiquement. Après l'installation de Citrix Receiver, il leur suffit d'ouvrir le fichier .cr sur l'appareil pour configurer Citrix Receiver. Si vous configurez des sites Receiver pour Web, les utilisateurs peuvent également obtenir les fichiers de provisioning à partir de ces sites.

Pour de plus amples informations, consultez la documentation de StoreFront.

Fournir aux utilisateurs des informations de compte à entrer manuellement

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

- L'adresse URL de StoreFront ou du site XenApp Services hébergeant les ressources ; par exemple : nomserveur.société.com.
- Pour permettre l'accès à l'aide de Netscaler Gateway : l'adresse de NetScaler Gateway, l'édition du produit et la méthode d'authentification requise

  Pour plus d'informations sur la configuration de NetScaler Gateway, veuillez consulter la documentation relative à NetScaler Gateway.

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

Fournir l'authentification RSA SecurID aux appareils Android

Si vous configurez NetScaler Gateway pour utiliser l'authentification RSA SecurID, Citrix Receiver prend en charge le mode Jeton suivant. Lorsque cette fonctionnalité est activée et qu'un utilisateur entre un mot de passe incorrect à trois reprises (valeur par défaut), NetScaler Gateway Plug-in invite l'utilisateur à attendre que le jeton suivant soit actif avant d'ouvrir une session. Le serveur RSA peut être configuré pour désactiver un compte utilisateur si un utilisateur se connecte un certain nombre de fois à l'aide d'un mot de passe incorrect.

Pour obtenir des instructions sur la configuration de l'authentification, reportez-vous à la section Authentification et autorisation.

> **Conseil**
>
> L'authentification RSA SecurID n'est pas prise en charge pour les configurations Secure Gateway. Pour utiliser l'authentification RSA SecurID, utilisez NetScaler Gateway.

Installation de jetons logiciels RSA SecurID

Un fichier RSA SecurID Software Authenticator possède une extension de fichier .sdtid. Utilisez le convertisseur de jeton logiciel RSA SecurID pour convertir le fichier .sdtid en une chaîne numérique à 81

chiffres au format XML. Obtenez les derniers logiciels et dernières informations à partir du site Web de RSA.

Suivez ces étapes générales :

1. Sur un ordinateur (et non un appareil mobile), téléchargez l'outil de conversion ici. Suivez les instructions sur le site Web et dans le fichier Lisez-moi inclus dans l'outil de conversion.
2. Collez la chaîne numérique convertie dans un e-mail puis envoyez-le aux machines utilisateur.
3. Sur l'appareil mobile, assurez-vous que la date et l'heure sont correctes, ce qui est nécessaire pour le bon déroulement de l'authentification.
4. Sur l'appareil, ouvrez l'e-mail puis cliquez sur la chaîne pour démarrer le processus d'importation du jeton logiciel.

Après installation du jeton logiciel sur la machine, une nouvelle option permettant de gérer le jeton s'affiche dans la liste Paramètres.

> **Remarque :**
>
> pour les appareils mobiles qui n'associent pas le fichier .sdtid avec Receiver, changez l'extension de fichier sur .xml et importez-le.

Enregistrement des mots de passe

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

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

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

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

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

Pour annuler l'enregistrement des mots de passe

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

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

Configuration

October 4, 2019

Donner accès aux applications et bureaux virtuels

Citrix Receiver nécessite la configuration de l'Interface Web ou de StoreFront pour mettre à disposition des applications et des bureaux à partir de votre déploiement XenApp ou XenDesktop.

Interface Web

Il existe deux types de sites Interface Web : les sites XenApp Services (anciennement Program Neighborhood Services) et les sites XenApp Web. Les sites Interface Web permettent aux machines utilisateur de se connecter à la batterie de serveurs.

StoreFront

Vous pouvez configurer StoreFront de manière à fournir des services d'authentification et de mise à disposition de ressources pour Citrix Receiver, ce qui vous permet de créer de façon centralisée des magasins d'entreprise destinés à délivrer des bureaux et applications via XenApp et XenDesktop, ainsi que des applications mobiles Worx et des applications mobiles que vous avez préparées pour votre organisation par l'intermédiaire de XenMobile.

L'authentification entre Citrix Receiver et un site Interface Web ou un magasin StoreFront peut être gérée de plusieurs manières :

- Les utilisateurs à l'intérieur de votre pare-feu peuvent se connecter directement à l'Interface Web ou à StoreFront.
- Les utilisateurs en dehors de votre pare-feu peuvent se connecter à StoreFront ou l'Interface Web via NetScaler Gateway.
- Les utilisateurs en dehors de votre pare-feu peuvent se connecter à StoreFront via NetScaler Gateway.

Connexion via NetScaler Gateway

NetScaler Gateway 10 et 11 sont pris en charge par Citrix Receiver pour Android pour l'accès à :

- Interface Web 5.4 avec sites XenApp Services et sites XenApp Web
- Magasins StoreFront 2.6, 3.0, 3.5, 3.6, 3.7, 3.8, 3.9 et 3.11

L'authentification à source unique et l'authentification à double source sont toutes les deux prises en charge sur les sites Interface Web et StoreFront.

Vous pouvez créer de multiples stratégies de session sur le même serveur virtuel en fonction du type de connexion (telle que ICA, CVPN ou VPN) et du type de Receiver (Receiver pour Web ou des logiciels Citrix Receiver installés localement). Toutes les stratégies peuvent être appliquées à partir d'un serveur virtuel unique.

Lorsque les utilisateurs créent des comptes sur Citrix Receiver, ils doivent entrer les informations d'identification au compte, telles que leur adresse e-mail ou le nom de domaine complet du serveur NetScaler Gateway. À titre d'exemple, si la connexion échoue lors de l'utilisation du chemin d'accès par défaut, les utilisateurs doivent entrer le chemin d'accès complet au serveur NetScaler Gateway.

Pour se connecter à XenMobile

Pour permettre aux utilisateurs distants de se connecter via NetScaler Gateway à votre déploiement XenMobile, vous pouvez configurer NetScaler Gateway en vue de son utilisation avec AppController ou StoreFront (tous les deux sont des composants de XenMobile). La méthode que vous allez choisir pour autoriser l'accès dépend de l'édition de XenMobile dans votre déploiement :

Activation de l'accès à XenMobile 9 :

Authentification du certificat client

Activation de l'accès à XenMobile 10 :

NetScaler Gateway et XenMobile

Si vous déployez XenMobile dans votre réseau, autorisez les connexions des utilisateurs distants à AppController en intégrant XenMobile et AppController. Ce déploiement permet aux utilisateurs de se connecter à AppController afin d'accéder à leurs applications Web, SaaS et mobiles ainsi qu'aux documents ShareFile. Les utilisateurs se connectent via Citrix Receiver ou NetScaler Gateway Plug-in.

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

Pour déployer des applications Windows et personnalisées à vos utilisateurs, vous devez les wrapper à l'aide du MDX Toolkit. Vous trouvez plus d'informations ici :

MDX Toolkit

Connexion à StoreFront

Citrix Receiver pour Android prend en charge le lancement de sessions à partir de Receiver pour Web, à condition que le navigateur Web fonctionne avec Receiver pour Web. Si le lancement échoue, configurez votre compte directement via Citrix Receiver pour Android.

> **Conseil**
>
> Lorsque Citrix Receiver pour Web est utilisé à partir d'un navigateur, les sessions ne sont pas lancées automatiquement lors du téléchargement d'un fichier .ICA. Le fichier .ICA doit être ouvert manuellement peu après son téléchargement pour que la session puisse être lancée.

Les magasins que vous créez dans StoreFront se composent de services destinés à fournir une infrastructure d'authentification et de mise à disposition de ressources pour Citrix Receiver. Créez des magasins qui énumèrent et regroupent les bureaux et applications des sites XenDesktop et des batteries XenApp, tout en mettant ces ressources à la disposition des utilisateurs.

Pour les administrateurs soucieux d'exercer un contrôle plus rigoureux, Citrix fournit un modèle que vous pouvez utiliser pour créer un site de téléchargement pour Receiver pour Android.

Configurez des magasins pour StoreFront comme vous le feriez pour toute autre application XenApp ou XenDesktop. Aucune configuration spéciale n'est nécessaire pour les appareils mobiles. Pour les appareils mobiles, utilisez l'une de ces méthodes :

Fichier de provisioning.Vous pouvez fournir aux utilisateurs des fichiers de provisioning (.cr) contenant les informations nécessaires pour se connecter aux magasins. Après l'installation, les utilisateurs ouvrent le fichier sur leur appareil configurer automatiquement Citrix Receiver. Par défaut, les sites Receiver pour Web offrent aux utilisateurs un fichier de provisioning destiné au magasin pour lequel le site est configuré. Alternativement, vous pouvez utiliser la console de gestion Citrix StoreFront pour générer des fichiers de provisioning pour des magasins uniques ou multiples que vous distribuez manuellement à vos utilisateurs.

Configuration manuelle.Vous pouvez informer directement les utilisateurs des adresses URL de NetScaler Gateway ou de magasin nécessaires à l'accès à leurs bureaux ou applications. Pour les connexions via NetScaler Gateway, les utilisateurs doivent également connaître l'édition du produit et la méthode d'authentification requise. Après installation, les utilisateurs entrent ces détails dans Citrix Receiver, qui tente de vérifier la connexion et, si réussi, invite les utilisateurs à ouvrir une session.

Pour configurer Citrix Receiver pour accéder aux applications :

Lors de la création d'un nouveau compte, dans le champ Adresse, entrez l'adresse URL de votre magasin, telle que storefront.organisation.com.

Continuez en renseignant les champs restants et sélectionnez la méthode d'authentification à NetScaler Gateway, telle que l'activation du jeton de sécurité, le choix du type d'authentification et l'enregistrement des paramètres.

Lors de l'ajout d'un compte à l'aide la configuration automatique, vous pouvez entrer le nom de domaine complet d'un serveur StoreFront ou NetScaler, ou vous pouvez également utiliser une adresse e-mail pour créer un nouveau compte. Vous êtes ensuite invité à entrer vos informations d'identification avant de vous connecter.

Informations complémentaires :

Pour de plus amples informations sur la configuration de l'accès à StoreFront via NetScaler Gateway, consultez :

Gestion de l'accès à StoreFront via NetScaler Gateway

Intégration de StoreFront à NetScaler Gateway

Connexion à l'Interface Web

Citrix Receiver peut lancer des applications via votre site Interface Web. Configurez le site Interface Web comme vous le feriez pour tout autre application ou bureau XenApp et XenDesktop. Aucune configuration spéciale n'est nécessaire pour les appareils mobiles.

Citrix Receiver prend uniquement en charge la version 5.4 de l'Interface Web. En outre, les utilisateurs peuvent lancer des applications à partir de l'Interface Web 5.4 à l'aide du navigateur Firefox Mobile.

Pour lancer des applications sur l'appareil Android :

À partir de l'appareil, les utilisateurs ouvrent une session sur le site Interface Web à l'aide de leur nom d'ouverture de session et mot de passe habituels.

Pour plus d'informations sur la configuration de sites Interface Web, veuillez consulter :

Configuration de l'Interface Web

Synchronisation de la disposition du clavier

Pour activer la synchronisation de la disposition du clavier, accédez à Paramètres dans Citrix Receiver pour Android et cochez la case **Client IME**.

Remarques :

- Le VDA doit être la version 7.16 ou ultérieure.
- Les administrateurs doivent activer la fonctionnalité de prise en charge améliorée des langues asiatiques sur le VDA. Cette fonctionnalité est activée par défaut. Toutefois, sur un VDA Windows Server 2016, vous devez ajouter une nouvelle clé appelée DisableKeyboardSync et définir

la valeur sur 0 dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\IcaIme pour activer la fonctionnalité.
- Les administrateurs doivent activer la fonction de mappage de disposition de clavier Unicode sur le VDA. Cette fonctionnalité est désactivée par défaut. Pour l'activer, créez la clé CtxKlMap sous HKEY_LOCAL_MACHINE\SOFTWARE\Citrix et définissez la valeur DWORD EnableKlMap = 1 sous HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap.

Limitations :

- Cette fonctionnalité ne fonctionne que sur les claviers logiciels des appareils, et non sur les claviers externes.
- Certains appareils mobiles peuvent ne pas prendre en charge complètement la synchronisation de la disposition du clavier, comme le Nexus 5x
- La disposition du clavier peut uniquement être synchronisée du client au serveur. Lorsque vous modifiez la disposition du clavier côté serveur, la disposition du clavier client ne peut pas être modifiée.
- Lorsque vous modifiez la disposition du clavier client sur une disposition non compatible, la disposition peut être synchronisée du côté VDA, mais la fonctionnalité ne peut pas être confirmée.
- Les applications distantes exécutées avec des privilèges élevés (par exemple, des applications que vous exécutez en tant qu'administrateur) ne peuvent pas être synchronisées avec la disposition du clavier de la machine cliente. Pour contourner ce problème, modifiez manuellement la disposition du clavier sur le VDA ou désactivez le contrôle de compte d'utilisateur.

Activation de la prise en charge des cartes à puce

Receiver pour appareils mobiles Android prend en charge les lecteurs de carte à puce Bluetooth avec StoreFront, un site Interface Web ou un site PNA. Si la prise en charge des cartes à puce est activée, vous pouvez utiliser des cartes à puce aux fins suivantes :

- Authentification d'ouverture de session par carte à puce. Utilisez des cartes à puce pour authentifier les utilisateurs auprès de Receiver.
- Prise en charge des applications recourant à une carte à puce. Autorisez les applications recourant à une carte à puce à accéder aux lecteurs de carte à puce locaux.
- Signature de documents et d'e-mail. Les applications telles que Microsoft Word et Outlook qui sont lancées dans des sessions ICA peuvent accéder à des cartes à puce sur l'appareil mobile pour signer des documents et des e-mails.

Cartes à puce prises en charge :

- Cartes PIV
- Cartes CAC

Configuration de la prise en charge de carte à puce sur l'appareil

1. Vous devez coupler la carte à puce avec l'appareil mobile. Pour de plus amples informations sur le couplage de lecteurs de carte à puce avec l'appareil, reportez-vous aux spécifications du lecteur de carte à puce.

   Les conditions et limites suivantes s'appliquent à la prise en charge des cartes à puce sur les Android :

   - Receiver prend en charge cette fonctionnalité sur tous les appareils Android répertoriés par le middleware Biometric Associates.
   - Certains utilisateurs peuvent disposer d'un code PIN global pour les cartes à puce ; toutefois, lorsque les utilisateurs ouvrent une session à un compte de carte à puce, ils doivent entrer le code PIN de la carte PIV, et non le code PIN global. Cette limite est liée au fournisseur tiers.
   - L'authentification par carte à puce peut être plus lente que l'authentification avec mot de passe. À titre d'exemple, après la déconnexion à une session, attendez 30 secondes avant d'essayer de vous reconnecter. Receiver peut échouer si vous vous reconnectez trop rapidement à une session déconnectée.
   - L'authentification par carte à puce n'est pas prise en charge pour l'accès par navigateur où à partir d'un site XenApp.

2. Avant d'ajouter un compte prenant en charge les cartes à puce, vous devez installer le service Android PC/SC-Lite sur l'Android. Ce service est disponible sous forme de fichier .apk dans le SDK baiMobile.

   Pour Android, le fichier PC/SC-Lite .apk peut être téléchargé à partir de Google Play Store.

3. Dans Receiver, sélectionnez l'icône Paramètres, sélectionnez **Comptes** et **Ajouter un compte**, ou modifiez un compte existant.

4. Configurez la connexion et activez l'option de carte à puce.

Installation de Citrix Receiver sur une carte SD

Citrix Receiver pour Android est optimisé pour être installé localement sur des machines utilisateur. Toutefois, si l'espace de stockage est insuffisant sur ces machines, les utilisateurs peuvent installer Receiver sur une carte SD externe et monter cette dernière sur la machine de manière à pouvoir lancer des applications publiées sur leurs appareils mobiles. Ceci est pris en charge par défaut et aucune configuration supplémentaire n'est requise.

Pour lancer une application à l'aide de la carte SD, sélectionnez l'application dans la liste des applications Receiver sur la machine utilisateur, et sélectionnez ensuite Déplacer vers la carte SD.

Si les utilisateurs choisissent d'installer Receiver sur une carte SD externe pour lancer des applications, les problèmes suivants peuvent se produire :

- Si vous montez un périphérique de stockage USB alors que la carte SD est montée sur l'appareil mobile, la carte SD n'est plus disponible, et les applications en cours d'exécution cessent de fonctionner lorsque le périphérique USB est monté.
- Certains AppWidgets (tels que les widgets de l'écran d'accueil) ne sont pas disponibles lorsqu'une application est exécutée à partir de la carte SD. Après le démontage de la carte SD, les utilisateurs doivent redémarrer les AppWidgets.

Si les utilisateurs installent Receiver localement sur leur machine utilisateur, ils peuvent supprimer Receiver de la carte SD.

Accéder aux fichiers à l'aide de l'association de type de fichier (FTA)

Pour garantir le bon fonctionnement de cette fonctionnalité, accédez aux paramètres de Receiver pour Android et définissez l'option **Utiliser stockage de l'appareil** sur **Accès complet**.

Receiver pour Android lit et applique les paramètres configurés par les administrateurs dans Citrix Studio.
Pour appliquer la FTA dans une session, assurez-vous que les utilisateurs se connectent au serveur Store sur lequel la FTA est configurée.

Sur l'appareil utilisateur, sélectionnez le fichier que vous souhaitez lancer dans l'explorateur de fichiers et cliquez sur Ouvrir. Le système d'exploitation Android offre une option permettant de lancer le fichier à l'aide de Receiver pour Android (en appliquant la FTA configurée par l'administrateur) ou d'une application différente. En fonction de votre sélection antérieure, une application par défaut peut ou ne peut pas être définie. Vous pouvez changer l'application par défaut en utilisant l'option Changer défaut.

> **Remarque :**
>
> Cette fonctionnalité est disponible uniquement sur StoreFront et requiert XenApp et XenDesktop version 7 ou ultérieure.

Limitation

- Vous pouvez accéder uniquement aux formats de fichier MIME pris en charge par les applications Microsoft Office, Adobe Acrobat Reader et Bloc-notes à l'aide de la fonctionnalité d'association de type de fichier.

Activation du hub d'espace de travail Citrix Ready

November 15, 2018

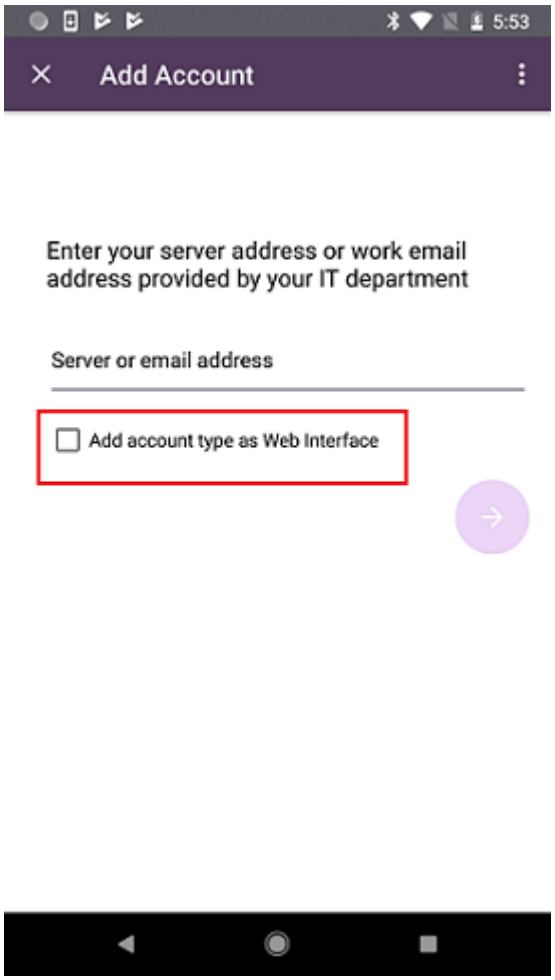
Le hub d'espace de travail Citrix Ready est désactivé par défaut dans Citrix Receiver pour Android. Pour utiliser le hub avec un appareil Android, procédez comme suit.

Conditions préalables requises sur l'appareil :

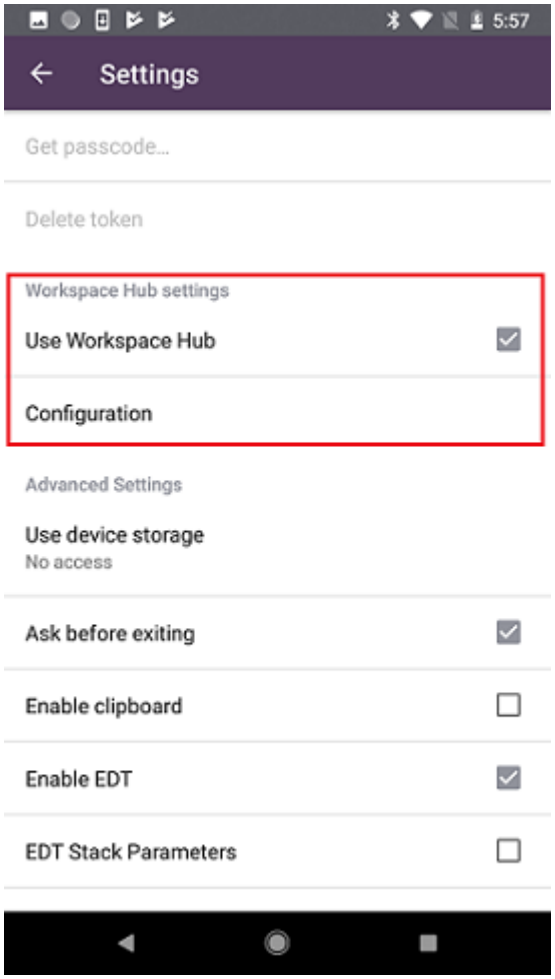
- Citrix Receiver pour Android 3.13.5 installé ou version supérieure
- Bluetooth activé (pour l'authentification de proximité)
- Appareil mobile et hub d'espace de travail utilisant le même réseau Wi-Fi

L'authentification de proximité fournit un moyen d'authentifier les utilisateurs et de lancer une session automatiquement.

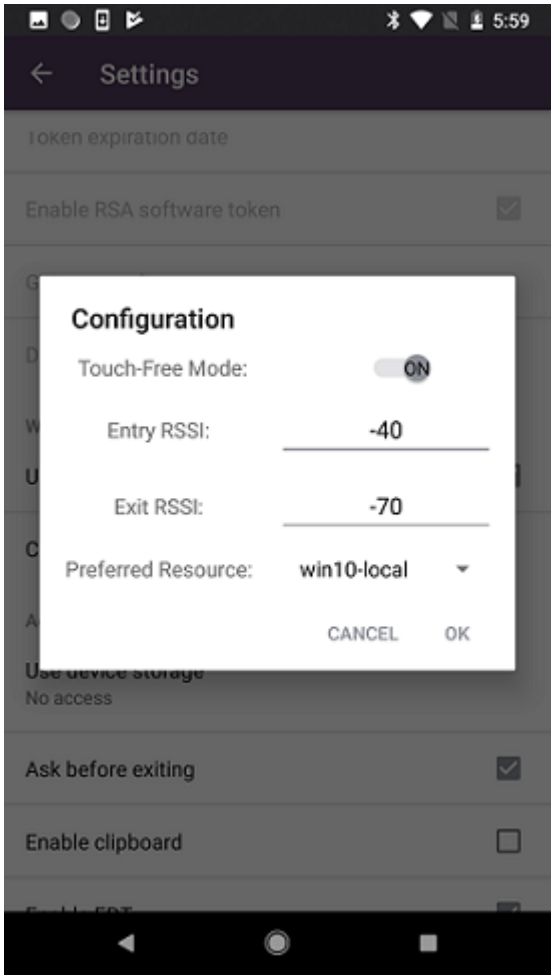
1. Pour utiliser l'authentification de proximité, activez Bluetooth sur l'appareil mobile pour vous assurer que la case à cocher « Ajouter un type de compte en tant qu'interface Web » n'est pas sélectionnée lors de la configuration du compte Citrix Receiver.



2. Dans Citrix Receiver, accédez à **Paramètres** et sélectionnez **Utiliser Workspace Hub**.



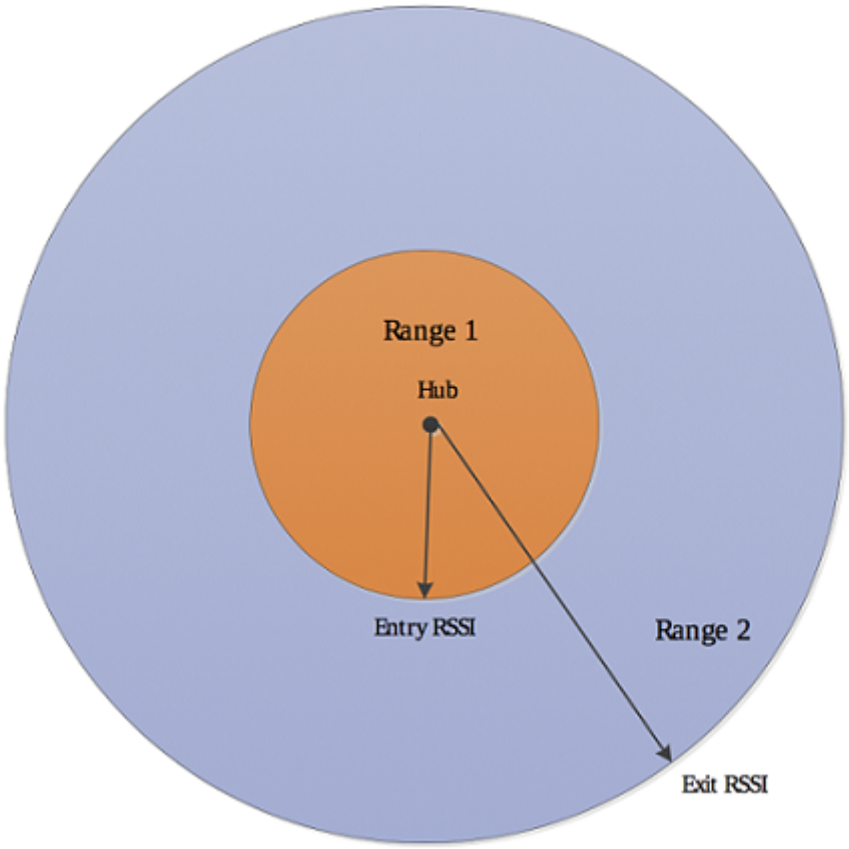
3. Cliquez sur **Configuration** pour afficher la page de configuration.



Le **Mode tactile multipoint** est un commutateur qui vous permet d'activer ou de désactiver l'authentification de proximité. Lorsque le mode tactile multipoint est désactivé, l'authentification de proximité n'est pas disponible mais les autres fonctions du hub d'espace de travail Citrix Ready le sont. Pour utiliser le mode tactile multipoint, Bluetooth doit être activé sur l'appareil.

RSSI représente la puissance du signal Bluetooth par rapport à la distance entre l'appareil mobile et le hub. RSSI d'entrée est la plage dans laquelle les balises Workspace Hub sont détectées. RSSI de sortie est le début de la plage en dehors de laquelle l'appareil mobile ne communique plus avec le Workspace Hub. Le RSSI de sortie doit être égal ou inférieur au RSSI d'entrée et les valeurs doivent être négatives. Les valeurs par défaut sont -40 (RSSI d'entrée) et -70 (RSSI de sortie), respectivement. Vous pouvez ajuster ces valeurs en fonction de votre environnement et de votre plage à partir du hub d'espace de travail.

Comme indiqué ci-dessous, lorsque vous déplacez votre appareil mobile dans la plage 1, l'authentification de proximité est déclenchée et votre bureau ou application par défaut se lance automatiquement sur le hub d'espace de travail. Tant que l'appareil mobile reste dans la plage 1 ou 2, le bureau ou l'application par défaut continue à fonctionner sur le hub d'espace de travail. Lorsque vous déplacez l'appareil hors des plages 1 et 2, le bureau ou l'application se ferme automatiquement.



Ressource préférée est le bureau ou l'application par défaut qui se lance lorsque l'appareil mobile entre dans la plage d'authentification de proximité. Ce paramètre est spécifique au compte utilisé pour se connecter à Citrix Receiver. Si vous avez plusieurs comptes, vous devez définir une ressource préférée pour chacun d'eux. Ce paramètre est persistant, ce qui signifie que vous ne devez définir votre ressource préférée qu'une seule fois par compte. Ceci fait, votre ressource préférée se lance chaque fois que vous entrez dans la plage d'authentification de proximité jusqu'à ce que vous modifiiez le paramètre.

Résolution des problèmes

August 31, 2018

Stratégie de validation des certificats de serveur

La stratégie de validation des certificats de serveur de Citrix Receiver pour Android est plus stricte.

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

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

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

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

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

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »
- « Certificat racine exemple »

Citrix Receiver pour Android vérifie ensuite que tous ces certificats sont valides.Citrix Receiver pour Android vérifie également qu'il fait déjà confiance à « Certificat racine exemple ». Si Citrix Receiver pour Android ne fait pas confiance à « Certificat racine exemple », la connexion échoue.

> **Important**
>
> Certaines autorités de certification disposent de plus d'un certificat racine. Si vous avez besoin de cette validation plus stricte, assurez-vous que votre configuration utilise le certificat racine approprié. Par exemple, il existe actuellement deux certificats (« DigiCert »/« GTE CyberTrust Global Root » et « DigiCert Baltimore Root »/« Baltimore CyberTrust Root ») qui peuvent valider les mêmes certificats de serveur. Sur certaines machines utilisateur, les deux certificats racine sont disponibles. Sur les autres machines, seul (« DigiCert Baltimore Root »/« Baltimore CyberTrust

> Root ») est disponible. Si vous configurez « GTE CyberTrust Global Root » sur la passerelle, les connexions Citrix Receiver pour Android sur ces machines utilisateur échouent.Consultez la documentation de l'autorité de certification pour déterminer quel certificat racine doit être utilisé.Notez également que les certificats racine expirent éventuellement, comme tous les certificats.
>
> **Remarque**
>
> Certains serveurs et certaines passerelles n'envoient jamais le certificat racine, même si cela est configuré. Une validation plus stricte n'est par conséquent pas possible.

Supposons maintenant qu'une passerelle soit configurée avec ces certificats valides.Cette configuration, qui ignore le certificat racine, est généralement recommandée :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »

Citrix Receiver pour Android utilise ces deux certificats. Il recherche ensuite un certificat racine sur la machine utilisateur.S'il en trouve un qui est validé et également approuvé (tel que « Certificat racine exemple »), la connexion réussit. Sinon, la connexion échoue. Cette configuration fournit le certificat intermédiaire dont Citrix Receiver pour Android a besoin, mais permet également à Citrix Receiver pour Android de choisir un quelconque certificat racine valide et approuvé.

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

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

Un navigateur Web peut ignorer le certificat racine incorrect. Toutefois, Citrix Receiver pour Android n'ignore pas le certificat racine incorrect et la connexion échoue.

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

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple 1 »
- « Certificat intermédiaire exemple 2 »

> **Important**
>
> Certaines autorités de certification utilisent un certificat intermédiaire avec signature croisée.Ce cas de figure est destiné aux situations dans lesquelles il existe plus d'un certificat racine, et qu'un certificat racine antérieur est toujours en cours d'utilisation en même temps qu'un certificat racine plus récent.Dans ce cas, il y aura au moins deux certificats intermédiaires.Par exemple, le certificat racine antérieur « Class 3 Public Primary Certification Authority » et le certificat inter-

> médiaire avec signature croisée « VeriSign Class 3 Public Primary Certification Authority - G5 » correspondant.Toutefois, un certificat racine antérieur « VeriSign Class 3 Public Primary Certification Authority - G5 » correspondant est également disponible, et il remplace « Class 3 Public Primary Certification Authority ». Le certificat racine antérieur n'utilise pas de certificat intermédiaire avec signature croisée.
>
> **Remarque**
>
> Le certificat intermédiaire avec signature croisée et le certificat racine ont le même nom de sujet (Émis pour), mais le certificat intermédiaire avec signature croisée a un nom d'émetteur différent (Émis par). Cela permet de différencier le certificat intermédiaire avec signature croisée d'un certificat intermédiaire ordinaire (tel « Certificat intermédiaire exemple 2 »).

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

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »

Évitez de configurer la passerelle de manière à utiliser le certificat intermédiaire avec signature croisée, car cela entraîne la sélection du certificat racine antérieur :

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

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

- « Certificat de serveur exemple »

Dans ce cas, si Citrix Receiver pour Android ne peut pas trouver tous les certificats intermédiaires, la connexion échoue.

SDK et API

October 4, 2019

SDK du canal virtuel Citrix

Le SDK du canal virtuel Citrix prend en charge l'écriture de pilotes du côté serveur et du côté client afin de fournir des canaux virtuels supplémentaires à l'aide du protocole ICA. Les applications de canal virtuel côté serveur se trouvent sur des serveurs XenApp ou XenDesktop. Cette version du SDK prend en charge l'écriture de nouveaux canaux virtuels pour Receiver pour Android. Si vous souhaitez écrire des pilotes virtuels pour d'autres plates-formes clientes, contactez Citrix.

Le SDK du canal virtuel offre ce qui suit :

- Les interfaces AIDL Citrix Android Virtual Driver : **IVCService.aidl** et **IVCCallback.aidl** utilisées avec les fonctions de canal virtuel dans le SDK de l'API Citrix Server (WFAPI SDK) pour créer de nouveaux canaux virtuels.
- Une classe helper **Marshall.java** conçue pour faciliter l'écriture de vos propres canaux virtuels.
- Un code source opérationnel pour trois exemples de programmes de canal virtuel qui illustrent les techniques de programmation.

Le SDK de canal virtuel requiert le SDK WFAPI pour écrire sur le côté serveur du canal virtuel. Pour plus d'informations sur le SDK, consultez Citrix Virtual Channel SDK for Citrix Receiver for Android.

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