Citrix Receiver pour Windows 4.12

Contents

Nouveautés

June 27, 2019

Nouveautés dans la version 4.12

Mise à jour du kit de chiffrement

Cette version contient deux modifications importantes pour les protocoles de communications sécurisées TLS/DTLS : la prise en charge de **DTLS 1.2** et la fin de prise en charge des suites de chiffrement TLS/DTLS qui ne proposent pas la fonctionnalité Forward Secrecy.

DTLS 1.2 prend en charge le protocole de transport UDP, l'équivalent de TLS 1.2 pour le protocole de transport TCP. Des versions antérieures de Receiver pour Windows prenaient déjà en charge TLS 1.2.

Les suites de chiffrement avec le préfixe **TLS_RSA_** ne proposent pas la fonctionnalité Forward Secrecy De manière générale, ces suites de chiffrement sont maintenant obsolètes dans le secteur. Toutefois, pour prendre en charge la rétrocompatibilité avec les anciennes versions de XenApp et XenDesktop, Receiver pour Windows peut utiliser ces suites de chiffrement.

Un nouveau modèle d'administration d'objet de stratégie de groupe a été créé pour autoriser l'utilisation des suites de chiffrement obsolètes. Dans Receiver pour Windows 4.12, cette stratégie est activée par défaut, mais n'applique pas la fin de prise en charge de ces suites de chiffrement à l'aide d'algorithmes de chiffrement AES ou 3DES par défaut. Toutefois, vous pouvez modifier et utiliser cette stratégie pour appliquer la fin de prise en charge de manière plus stricte.

Voici une liste des suites de chiffrement obsolètes :

1. TLS_RSA_AES256_GCM_SHA384
2. TLS_RSA_AES128_GCM_SHA256
3. TLS_RSA_AES256_CBC_SHA256
4. TLS_RSA_AES256_CBC_SHA
5. TLS_RSA_AES128_CBC_SHA
6. TLS_RSA_3DES_CBC_EDE_SHA
7. TLS_RSA_WITH_RC4_128_MD5
8. TLS_RSA_WITH_RC4_128_SHA

> **Remarque**
>
> Les deux dernières suites de chiffrement utilisent l'algorithme RC4 qui est obsolète car ces suites de chiffrement ne sont pas sécurisées. Vous pouvez également considérer la suite de chiffrement **TLS_RSA_3DES_CBC_EDE_SHA** comme étant obsolète. Vous pouvez utiliser cette stratégie pour appliquer toutes ces suites obsolètes.

Pour plus d'informations sur la configuration DTLS v1.2, consultez la section Transport adaptatif dans la documentation XenApp et XenDesktop.

Pour plus d'informations sur la configuration des suites de chiffrement obsolètes, consultez la section Configurer les suites de chiffrement obsolètes.

Notification de l'icône de batterie

Une batterie apparaît dans la zone de notification d'hôte de la session dans laquelle les informations sur la batterie du client sont représentées.

Cette fonctionnalité s'applique uniquement au VDA fonctionnant sur les versions 7.18 et ultérieures.

Carte à puce rapide

La carte à puce rapide améliore les performances lorsque les cartes à puce sont utilisées dans des scénarios WAN à latence élevée. La carte à puce rapide est activée par défaut sur les hôtes qui exécutent Windows Server 2012, Windows Server 2016 ou Windows 10 au minimum. Pour activer la carte à puce rapide côté client, configurez le paramètre **SmartCardCryptographicRedirection** dans le fichier default.ica.

Webcam plug and play

Les applications détectent de manière dynamique une webcam connectée ou supprimée sur le client. Les utilisateurs n'ont pas besoin de redémarrer l'application pour détecter ces changements.

Prise en charge de Citrix Analytics

Citrix Receiver pour Windows est conçu pour transmettre en toute sécurité les journaux à Citrix Analytics. Lorsque la fonction est activée, les journaux sont analysés et stockés sur Citrix Analytics. Pour plus d'informations sur Citrix Analytics, consultez la documentation de Citrix Analytics.

Problèmes résolus

June 27, 2019

Citrix Receiver pour Windows 4.12

Comparaison avec : Citrix Receiver pour Windows 4.11

Redirection HDX MediaStream Flash

- Lorsque le paramètre Redirection Flash HDX MediaStream est activé, le processus Pseudo-Container2.exe peut se fermer de manière inattendue lorsque vous déconnectez la session. [#LC8802]

Clavier

- Les tentatives d'utilisation de la valeur par défaut du serveur ou des dispositions de clavier souhaitées à l'aide des fichiers APPSRV.INI ou ICA téléchargés à partir de StoreFront peuvent échouer.

  Les limitations dans ce scénario sont les suivantes :

  - Vous devez définir la disposition du clavier manuellement dans la session à l'aide du panneau de configuration lorsque vous configurez les paramètres pour la première fois, même si vous avez défini la disposition précédemment.
  - Vous devez définir la synchronisation de disposition du clavier en modifiant **Préférences avancées** et en sélectionnant **Non**. Si vous définissez la disposition sur **Oui**, l'éditeur IME local est redirigé. [#LC9593]

Session/Connexion

- Lorsque vous essayez de démarrer un bureau à l'aide de Microsoft Internet Explorer 11, ce message d'erreur peut s'afficher :

  « Échec de la connexion à avec l'état (erreur de client inconnu 0). » \[#LC8841\]

- Lors de la configuration de l'agrégation entre deux sites dans StoreFront, la session de prélancement n'est pas créée. [#LC8847]

- Certaines vidéos DVD peuvent ne pas être lues au sein d'une session via un lecteur client mappé. [#LC8912]

- Dans un scénario « double hop » avec le VDA pour OS de bureau dans le premier hop et une application dans le deuxième hop qui est lancée au sein d'un VDA, lors de la reconnexion au premier hop qui s'exécute sur le VDA pour OS de bureau, l'écran peut clignoter pendant quelques secondes. [#LC9071]

- Lorsque vous effectuez une redirection bidirectionnelle du contenu vers un VDA, une deuxième adresse URL s'ouvre sur une nouvelle fenêtre de navigateur lorsque le navigateur est déjà ouvert. [#LC9157]

- Lorsque vous démarrez une application, Citrix Receiver pour Windows peut afficher « Connexion en cours… » avant que le démarrage n'échoue. Ce message d'erreur s'affiche :

« La ressource publiée n'est pas disponible actuellement. Contactez votre administrateur système pour obtenir de l'aide. » [#LC9170]

- Lorsque vous démarrez une session en mode fenêtre et non transparente à l'aide de Citrix Receiver pour Windows, un écran gris peut s'afficher. Le problème se produit lorsque la résolution du fichier ICA est supérieure à la résolution du point de terminaison du client. [#LC9266]
- Les tentatives de démarrage d'applications à partir de Citrix Receiver pour Mac peuvent échouer. Le problème se produit lorsque la licence client (LicenseRequestClientLicense) ne peut pas être récupérée. [#LC9286]
- Les tentatives de démarrage des bureaux à l'aide de Citrix Receiver pour Windows peuvent échouer. Le problème se produit même après l'augmentation de la durée de démarrage avec le paramètre **LaunchTimeoutMs** à l'aide de StoreFront. [#LC9369]
- Si vous sélectionnez la fonction Effacer ou Supprimer le Presse-papiers dans une application publiée qui s'exécute sur un VDA pour OS de serveur, le Presse-papiers du VDA est effacé mais le texte reste dans le Presse-papiers du point de terminaison. [#LC9434]
- Lorsque vous mettez à niveau Citrix Receiver pour Windows via System Center Configuration Manager (SCCM), Receiver pour Windows peut demander un redémarrage du système. [#LC9706]
- Lors de l'installation de Citrix Receiver pour Windows via System Center Configuration Manager (SCCM) ou PSExec, une installation non assistée de Receiver pour Windows peut se produire. [#RFWIN-8188]

Cartes à puce

- Lorsque vous tentez de démarrer un bureau publié en mode plein écran à l'aide de l'authentification par carte à puce, l'invite du code PIN peut ne pas s'afficher pas sur Desktop Viewer. [#LC8579]

Exceptions système :

- Le processus wfica32 peut se terminer par intermittence lors de l'utilisation d'un appareil tactile pour se connecter à un VDA. [#LC9228]
- Le processus wfica32.exe peut se terminer par intermittence. [#LC9397]

Expérience utilisateur :

- Lorsque vous démarrez un bureau publié avec l'option **Accélération matérielle pour graphiques** activée, un aperçu gris de Desktop Viewer peut s'afficher sur la barre d'outils. [#LC8545]
- Le bureau peut disparaître peu après que vous l'ayez démarré. Le problème se produit en raison de paquets TLS dupliqués envoyés à partir de Citrix Receiver pour Windows. [#LC8724]

- Les icônes du menu Démarrer et de la barre des tâches peuvent devenir instables lorsque vous actualisez les applications dans Citrix Receiver pour Windows. [#LC8890]
- Lorsque vous démarrez un bureau publié à l'aide du codec vidéo H.265, une couleur verte s'affiche sur l'écran du bureau publié. [#LC9083]
- Les applications et les icônes peuvent être partiellement associées à des types de fichiers lors de l'utilisation de Citrix Receiver pour Windows avec le Site Citrix XenApp Services. [#LC9402]
- Si vous choisissez l'option **Non, utiliser la disposition de clavier du serveur** dans l'onglet du clavier sur la page **Clavier et barre de langue**, la synchronisation de disposition du clavier peut ne pas être prise en charge dynamiquement. Si vous choisissez l'option **Oui**, la synchronisation de disposition du clavier est prise en charge dynamiquement. Toutefois, la disposition du clavier est synchronisée lors de la connexion initiale dans les deux scénarios. [#RFWIN-7999]
- Sur une machine 64 bits, lorsque vous lancez une instance 32 bits d'une application avec une entrée de registre %ProgramFiles%, l'entrée est étendue à C:\Program Files mais pas à C:\Program Files (X86)\. Par conséquent, l'instance 32 bits du lancement de l'application revient à un lancement d'instance de serveur, provoquant l'échec de vPrefer pour cette application. [#RFWIN-8025]

Divers

- Cette correction apporte des améliorations mineures en termes de performances et de qualité pour Enlightened Data Transport (EDT). [#LC9417]

Remarque : cette version de Citrix Receiver pour Windows contient également toutes les corrections comprises dans les versions 4.11, 4.10.1, 4.10, 4.9, 4.8, 4.7, 4.6, 4.5 et 4.4.

Problèmes connus

June 27, 2019

Problèmes connus dans Citrix Receiver pour Windows 4.12

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

Citrix Receiver pour Windows 4.12 contient tous les problèmes connus présents dans les versions 4.5, 4.6, 4.7, 4.8, 4.9, 4.10 et 4.11.

Avis de tiers

November 16, 2018

Citrix Receiver pour Windows peut inclure un logiciel tiers distribué sous une licence selon les conditions définies dans le document suivant :

Avis de tiers Citrix Receiver pour Windows

Configuration système requise et compatibilité

September 12, 2019

Exigences

- Cette version de Citrix Receiver pour Windows requiert une capacité minimale de 500 Mo d'espace disque disponible et 1 Go de RAM.
- Configuration minimale requise pour .NET Framework
  - Self-Service Plug-in requiert NET 3.5 Service Pack 1. Ce plug-in vous permet de souscrire à des applications et des bureaux, et de les lancer à partir de l'interface utilisateur ou de la ligne de commande de Receiver. Pour de plus amples informations, consultez la section Configuration et utilisation de Receiver pour Windows à l'aide de paramètres de ligne de commande.
  - .NET 2.0 Service Pack 1

Matrice de compatibilité

Citrix Receiver pour Windows est compatible avec les systèmes d'exploitation Windows et les navigateurs Web suivants. Cette version est également compatible avec toutes les versions actuellement prises en charge de XenApp, XenDesktop et NetScaler Gateway comme indiqué dans le tableau du cycle de vie des produits Citrix.

> **Remarque**
>
> NetScaler Gateway End Point Analysis Plug-in (EPA) ne prend pas en charge la version native de Citrix Receiver pour Windows.

Système d'exploitation
Windows 10 éditions 32 bits et 64 bits *

Système d'exploitation
Windows 10 IoT Enterprise **
Windows 8.1, éditions 32 bits et 64 bits (y compris l'édition Embedded)
Windows 7, éditions 32 bits et 64 bits (y compris l'édition Embedded)
Windows Thin PC
Windows Server 2016
Windows Server 2012 R2, édition Standard et Datacenter
Windows Server 2008 R2, édition 64 bits
Windows Server 2019
Windows 10 Entreprise 2016 LTSB 1607

* Prend en charge Windows 10 versions 1607, 1703, 1709 et 1803.

**Prend en charge les mises à jour Windows 10 IoT Enterprise 2015 LTSB, Windows 10 IoT Enterprise 2016 LTSB, Anniversary Update, Creators Update et Falls Creators Update.

Navigateur

Navigateur
Internet Explorer
Google Chrome dernière version (requiert StoreFront)
Mozilla Firefox dernière version
Microsoft Edge

Prise en charge

Systèmes d'exploitation pris en charge sur les appareils tactiles	Systèmes d'exploitation pris en charge sur les VDA
Windows 10	Windows 10
Windows 8	Windows 8
Windows 7	Windows 7
	Windows 2012 R2

Systèmes d'exploitation pris en charge sur les appareils tactiles	Systèmes d'exploitation pris en charge sur les VDA
	Windows Server 2016
	Windows 2008 R2

Connexions, certificats et authentification

July 1, 2020

Connexions

- Magasin HTTP
- Magasin HTTPS
- NetScaler Gateway 10.5 et versions ultérieures
- Interface Web 5.4

Certificats

- Privés (auto-signés)
- Racine
- Génériques
- Intermédiaires

Certificats privés (auto-signés)

Si un certificat privé est installé sur la passerelle distante, le certificat racine de l'autorité de certification de l'organisation doit être installé sur l'appareil de l'utilisateur à partir duquel vous accédez aux ressources Citrix.

> **Remarque**
>
> Si 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, les applications ne démarrent pas.

Installation de certificats racine

Pour les ordinateurs appartenant à un domaine, vous pouvez utiliser le modèle d'administration d'objet de stratégie de groupe pour distribuer et approuver les certificats d'autorité de certification.

Pour les ordinateurs n'appartenant pas à un domaine, l'organisation peut créer un pack d'installation personnalisé pour distribuer et installer le certificat d'autorité de certification. Contactez votre administrateur système pour obtenir de l'aide.

Certificats génériques

Les certificats génériques sont utilisés sur un serveur situé dans le même domaine.

Citrix Receiver pour Windows prend en charge les certificats génériques, toutefois, ils doivent être uniquement utilisés conformément à la stratégie de sécurité de votre organisation. En pratique, des alternatives aux certificats génériques peuvent être envisagées, par exemple un certificat contenant la liste des noms de serveurs avec l'extension SAN (Autre nom de l'objet). Des autorités de certification publiques et privées émettent ces certificats.

Certificats intermédiaires

Si votre chaîne de certificat contient un certificat intermédiaire, ce dernier doit être ajouté au certificat serveur de NetScaler Gateway. Pour plus d'informations, veuillez consulter la section Configuration de certificats intermédiaires.

Authentification

Authentification auprès de StoreFront

	Receiver pour Web à l'aide de navigateurs	Site StoreFront Services (natif)	Site StoreFront XenApp et XenDesktop (natif)	NetScaler sur Receiver pour Web (navigateur)	NetScaler sur site StoreFront Services (natif)
Anonymous	Oui	Oui			
Domaine	Oui	Oui	Oui	Oui*	Oui*
Authentification pass-through au domaine	Oui	Oui	Oui		

Jeton de sécurité			Oui*	Oui*
Authentification à deux facteurs (domaine avec jeton de sécurité)			Oui*	Oui*
SMS			Oui*	Oui*
Cartes à puce	Oui	Oui	Oui	Oui
Certificat utilisateur			Oui (plug-in NetScaler)	Oui (plug-in NetScaler)

* Avec ou sans le plug-in NetScaler installé sur la machine.

> **Remarque**
>
> Citrix Receiver pour Windows prend en charge l'authentification à deux facteurs (domaine + jeton de sécurité) via NetScaler Gateway au service natif StoreFront.

Authentification auprès de l'Interface Web

Citrix Receiver pour Windows prend en charge les méthodes d'authentification suivantes (l'Interface Web utilise le terme **Explicite** pour l'authentification de domaine et par jeton de sécurité) :

	Interface Web (navigateurs)	**Site Interface Web XenApp et XenDesktop**	**NetScaler sur l'Interface Web (navigateur)**	**NetScaler sur site Interface Web XenApp et XenDesktop**
Anonymous	Oui			
Domaine	Oui	Oui	Oui*	
Authentification pass-through au domaine	Oui	Oui		

Jeton de sécurité			Oui*
Authentification à deux facteurs (domaine avec jeton de sécurité)			Oui*
SMS			Oui*
Cartes à puce	Oui	Oui	
Certificat utilisateur			Oui (plug-in NetScaler)

* Disponible uniquement dans les déploiements incluant NetScaler Gateway, avec ou sans le plug-in associé installé sur la machine.

Pour de plus amples informations sur l'authentification, consultez la section Configuration de l'authentification et de l'autorisation dans la documentation de NetScaler Gateway et les rubriques Gérer dans la documentation de StoreFront.

Pour de plus amples informations sur les méthodes d'authentification prises en charge par l'Interface Web, reportez-vous à la documentation de l'Interface Web.

Installation

June 27, 2019

Vous pouvez installer le pack d'installation CitrixReceiver.exe à l'aide de l'une des méthodes suivantes :

- Par un utilisateur depuis Citrix.com ou depuis votre propre site de téléchargement.
  - Un nouvel utilisateur qui obtient Citrix Receiver pour Windows à partir de Citrix.com ou depuis votre propre site de téléchargement peut créer un compte en entrant une adresse e-mail à la place d'une adresse URL de serveur. Citrix Receiver pour Windows identifie le serveur NetScaler Gateway ou StoreFront associé à l'adresse e-mail et invite l'utilisateur à ouvrir une session et à continuer l'installation. Cette fonctionnalité est appelée « découverte de compte basée sur une adresse e-mail ».

Remarque : un nouvel utilisateur est un utilisateur qui n'a pas encore installé Citrix Receiver pour Windows sur sa machine.
Remarque : la découverte de compte basée sur l'adresse e-mail pour un nouvel utilisateur ne s'applique pas si Citrix Receiver pour Windows est téléchargé depuis un emplacement autre que Citrix.com (tel qu'un site Receiver pour Web).

  - Si votre site nécessite la configuration de Citrix Receiver pour Windows, utilisez une autre méthode de déploiement.
- Automatiquement depuis Receiver pour Web ou Écran de connexion de l'interface Web.
  - Un nouvel utilisateur peut configurer un compte en entrant une adresse URL de serveur ou en téléchargeant un fichier de provisioning (CR).
- À l'aide d'un outil ESD (distribution électronique de logiciels)
  - Un nouvel utilisateur doit entrer l'adresse URL d'un serveur ou ouvrir un fichier de provisioning pour créer un compte.

Vous n'avez pas besoin de privilèges d'administrateur pour installer Citrix Receiver pour Windows sauf si vous utilisez l'authentification unique.

Vérification de l'intégrité de Citrix Receiver pour Windows

Citrix Receiver pour Windows est signé numériquement. La signature numérique est horodatée. Ainsi, le certificat est valide même après son expiration.

Installation avec des privilèges d'administrateur et non administrateur

Les différences suivantes existent entre les installations de Citrix Receiver pour Windows effectuées par un administrateur et celles effectuées par un utilisateur (non administrateur).

	Administrateur	Utilisateur
Dossier d'installation	C:\Program Files (x86)\Citrix\ICA Client	%USERPROFILE%\AppData\Local\Citrix\ICA Client
Type d'installation	Installation par système	Installation par utilisateur

> **Remarque**
>
> Si une instance de Citrix Receiver pour Windows installée par l'utilisateur existe sur le système et qu'un administrateur installe Citrix Receiver pour Windows sur le même système, il y aura un conflit. Citrix vous recommande de désinstaller toutes les instances de Citrix Receiver pour Windows installées par l'utilisateur avant d'installer Citrix Receiver pour Windows en tant qu'administrateur.

Mise à niveau manuelle vers Citrix Receiver pour Windows

Pour les déploiements avec StoreFront :

- Une recommandation pour vos utilisateurs BYOD (Bring Your Own Device) consiste à configurer les dernières versions de NetScaler Gateway et de StoreFront comme décrit dans la documentation relative à ces produits sur le site de documentation produit. Joignez le fichier de provisioning créé par StoreFront à un e-mail et indiquez aux utilisateurs comment mettre à niveau et ouvrir le fichier de provisioning après l'installation de Citrix Receiver pour Windows.
- Si vous ne souhaitez pas utiliser le fichier de provisioning, demandez aux utilisateurs d'entrer l'adresse URL de NetScaler Gateway. Ou, si vous avez configuré la découverte de compte basée sur une adresse e-mail comme décrit dans la documentation StoreFront, demandez aux utilisateurs d'entrer leur adresse e-mail.
- Une autre méthode consiste à configurer un site Citrix Receiver pour Web comme décrit dans la documentation de StoreFront et à procéder à la configuration décrite dans Déploiement de Citrix Receiver pour Windows à partir de Citrix Receiver pour Web. Indiquez aux utilisateurs comment mettre à niveau Citrix Receiver pour Windows, accéder au site Citrix Receiver pour Web et télécharger le fichier de provisioning à partir de Citrix Receiver pour Web (cliquez sur le nom d'utilisateur et cliquez sur Activer).

Pour les déploiements avec l'Interface Web

- Mettez à niveau votre site Interface Web avec Citrix Receiver pour Windows et procédez à la configuration comme décrit dans Déployer Citrix Receiver pour Windows à partir d'un écran d'ouverture de session de l'Interface Web. Faites savoir à vos utilisateurs comment mettre à niveau Citrix Receiver pour Windows. Vous pouvez par exemple créer un site de téléchargement auprès duquel les utilisateurs peuvent obtenir le programme d'installation renommé de Citrix Receiver.

Considérations à prendre en compte lors de la mise à niveau

Pour plus d'informations sur les considérations à prendre en compte avant la mise à niveau de Citrix Receiver pour Windows, consultez l'article CTX135933 du centre de connaissances.

HDX RealTime Media Engine (RTME)

Un seul programme d'installation combine maintenant la dernière version de Citrix Receiver pour Windows et le programme d'installation RTME HDX. Lors de l'installation de Citrix Receiver à l'aide du fichier exécutable (.exe), le RTME HDX est également installé.

Si vous avez installé HDX RealTime Media Engine, lorsque vous désinstallez et réinstallez Citrix Receiver pour Windows, assurez-vous d'utiliser le même mode que celui utilisé pour installer le RTME HDX.

> **Remarque**
>
> L'installation de la dernière version de Citrix Receiver avec RTME intégré requiert des privilèges d'administration sur la machine hôte.

Tenez compte des problèmes RTME HDX suivants lors de l'installation ou la mise à niveau de Citrix Receiver pour Windows :

- La version la plus récente de Citrix Receiver avec RTME contient RTME HDX ; aucune autre installation n'est requise pour installer RTME.
- La mise à niveau à partir d'une version antérieure de Citrix Receiver pour Windows vers la dernière version (Citrix Receiver avec RTME) est prise en charge. Les versions de RTME précédemment installées sont remplacées par la dernière version ; la mise à niveau de la même version de Citrix Receiver pour Windows vers la dernière version groupée (par exemple, Receiver 4.7 vers Receiver 4.7 avec RTME) n'est pas prise en charge.
- Si vous disposez d'une version antérieure de RTME, l'installation de la dernière version de Citrix Receiver pour Windows met automatiquement à jour RTME sur l'appareil de l'utilisateur.
- Si une version plus récente de RTME est présente, le programme d'installation conserve la dernière version.

> **Important**
>
> Pour être compatible avec le nouveau package RTME, la version minimum du HDX RealTime Connector doit être 2.0.0.417. En effet, vous ne pouvez pas utiliser RTME 2.0 avec 1.8 RTME Connector.

Configurer et installer à l'aide de paramètres de ligne de commande

September 23, 2020

Personnalisez le programme d'installation de Citrix Receiver pour Windows en spécifiant les options de ligne de commande. Le programme d'installation s'extrait automatiquement sur le répertoire temporaire de l'utilisateur avant le lancement du programme d'installation. Cet espace disponible comprend les fichiers programmes, les données utilisateur et les répertoires temporaires après le lancement de plusieurs applications.

Pour plus d'informations sur la configuration système requise, reportez-vous à la section Configuration système requise.

Pour installer Citrix Receiver pour Windows depuis une invite de commandes, utilisez la syntaxe suivante :

CitrixReceiver.exe [Options]

Mises à jour de Receiver

Option	/AutoUpdateCheck=auto/manual/disabled
Description	Indique que Citrix Receiver pour Windows détecte lorsqu'une mise à jour est disponible. **Auto** : vous êtes notifié lorsqu'une mise à jour est disponible (valeur par défaut). **Manual** : vous n'êtes pas notifié lorsque des mises à jour sont disponibles. Recherchez les mises à jour manuellement. **Disabled** : les mises à jour automatiques sont désactivées.
Exemple d'utilisation	CitrixReceiver.exe /AutoUpdateCheck = auto ; CitrixReceiver.exe /AutoUpdateCheck=manual ; CitrixReceiver.exe /AutoUpdateCheck=disabled

Option	/AutoUpdateStream=LTSR/Current
Description	Indique la version de Citrix Receiver pour Windows. **LTSR** : indique que la version est Long Term Service Release. **Current** : indique que la version est la dernière version de Citrix Receiver pour Windows.
Exemple d'utilisation	CitrixReceiver.exe /AutoUpdateStream=LTSR ; CitrixReceiver.exe /AutoUpdateStream=Current

Option	/DeferUpdateCount
Description	Indique la version de Citrix Receiver pour Windows. **-1** : indique que vous pouvez différer les notifications n'importe quel nombre de fois (par défaut la valeur = -1). **0** : indique que l'option Me rappeler plus tard ne s'affiche pas. **Tout autre nombre** : indique combien de fois l'option Me rappeler plus tard s'affiche. Par exemple, si vous définissez la valeur sur 10, l'option Me rappeler plus tard s'affiche 10 fois.
Exemple d'utilisation	CitrixReceiver.exe /DeferUpdateCount=-1 ; CitrixReceiver.exe /DeferUpdateCount=0 ; CitrixReceiver.exe /DeferUpdateCount=*any other number*

Option	/AURolloutPriority
Description	Indique la période pendant laquelle vous pouvez effectuer le déploiement. **Fast (Rapide)** : le déploiement de la mise à jour se produit au début de la période de mise à disposition. **Medium (Moyen)** : le déploiement de la mise à jour se produit au milieu de la période de mise à disposition. **Slow (Lent)** : le déploiement de la mise à jour se produit à la fin de la période de mise à disposition.
Exemple d'utilisation	CitrixReceiver.exe /AURolloutPriority=Fast ; CitrixReceiver.exe /AURolloutPriority=Medium ; CitrixReceiver.exe /AURolloutPriority=Slow

Activer la redirection bidirectionnelle du contenu

> **Remarque**
>
> Par défaut, Citrix Receiver pour Windows n'installe pas les composants de la redirection bidirectionnelle du contenu s'ils sont déjà installés sur le serveur. Si vous utilisez XenDesktop en tant que machine cliente, vous devez installer Citrix Receiver pour Windows à l'aide du commutateur

> /FORCE_LAA pour installer les composants de la redirection bidirectionnelle du contenu. La fonctionnalité, cependant, doit être configurée sur le serveur et le client.

Option	ALLOW_BIDIRCONTENTREDIRECTION=1
Description	Indique que la redirection bidirectionnelle du contenu du client vers l'hôte et de l'hôte vers le client est **activée**.
Exemple d'utilisation	CitrixReceiver.exe /ALLOW_BIDIRCONTENTREDIRECTION=1

Option Masquer Paramètres

Option	/DisableSetting
Description	Supprime l'affichage d'Option Paramètres dans la boîte de dialogue Préférences avancées.
Exemple d'utilisation	CitrixReceiver.exe /DisableSetting=3

Si vous souhaitez que Affichage des applications et Options de reconnexion soient affichés dans Option Paramètres :	Entrez CitrixReceiver.exe /DisableSetting=0
Si vous souhaitez que Option Paramètres soit masqué dans la boîte de dialogue Préférences avancées :	Entrez CitrixReceiver.exe /DisableSetting=3
Si vous souhaitez que Option Paramètres affiche uniquement Affichage des applications :	Entrez CitrixReceiver.exe /DisableSetting=2
Si vous souhaitez que Option Paramètres affiche uniquement Options de reconnexion :	Entrez CitrixReceiver.exe /DisableSetting=1

Activer Local App Access

Option	FORCE_LAA=1
Description	Par défaut, Citrix Receiver pour Windows n'installe pas les composants de Local App Access sur le client s'ils sont déjà installés sur le serveur. Pour forcer l'installation des composants de Local App Access du côté client sur Citrix Receiver, utilisez le commutateur de ligne de commande FORCE_LAA. Des privilèges d'administrateur sont requis pour effectuer ces étapes. Pour plus d'informations sur Local App Access, consultez la section Local App Access dans la documentation XenApp et XenDesktop.
Exemple d'utilisation	CitrixReceiver.exe /FORCE_LAA=1

Afficher les informations d'utilisation

Option	/? ou /help
Description	Fournit des informations sur l'utilisation
Exemple d'utilisation	CitrixReceiver.exe /? ; CitrixReceiver.exe /help

Supprimer le redémarrage lors de l'installation de l'interface utilisateur

Option	/noreboot
Description	Supprime le redémarrage lors des installations de l'interface utilisateur. Cette option n'est pas nécessaire pour les installations silencieuses. Si vous supprimez les invites de redémarrage, les périphériques USB qui sont suspendus lors de l'installation de Citrix Receiver pour Windows ne sont pas reconnus par Citrix Receiver pour Windows tant que la machine utilisateur n'est pas redémarrée.
Exemple d'utilisation	CitrixReceiver.exe /noreboot

Installation non assistée

Option	/silent
Description	Désactive les boîtes de dialogue d'erreur et de progression afin d'exécuter une installation complètement silencieuse.
Exemple d'utilisation	CitrixReceiver.exe /silent

Activer l'authentification unique (SSO)

Option	/includeSSON
Description	Indique que Citrix Receiver pour Windows sera installé avec le composant d'authentification unique. L'option associée, ENABLE_SSON, est activée lorsque /includeSSON est sur la ligne de commande. Si vous utilisez ADDLOCAL= pour spécifier des fonctionnalités et que vous voulez installer l'authentification unique, vous devez également spécifier la valeur SSON. Pour activer l'authentification pass-through sur une machine utilisateur, vous devez installer Citrix Receiver pour Windows avec des droits d'administrateur à partir d'une ligne de commande qui possède l'option /includeSSON. Pour de plus amples informations, consultez la section Comment installer et configurer manuellement Citrix Receiver pour l'authentification pass-through. **Remarque** : les stratégies Carte à puce, Kerberos et Nom de l'utilisateur et mot de passe locaux sont interdépendantes. L'ordre de configuration est important. Nous vous recommandons de désactiver tout d'abord les stratégies, puis d'activer les stratégies dont vous avez besoin. Validez le résultat attentivement.
Exemple d'utilisation	CitrixReceiver.exe /includeSSON

Activer l'authentification unique lorsque /includeSSON est spécifié

Option	ENABLE_SSON={Yes, No}
Description	Active l'authentification unique lorsque /includeSSON est spécifié. La valeur par défaut est Yes. Cette propriété est requise pour l'authentification unique par carte à puce. Les utilisateurs doivent fermer leur session et la rouvrir sur leurs machines après une installation avec l'authentification unique activée. Requiert des droits d'administrateur.
Exemple d'utilisation	CitrixReceiver.exe ENABLE_SSON=Yes

Traçage permanent

Option	/EnableTracing={true,false}
Description	Par défaut, cette fonction est définie sur true. Utilisez cette propriété pour activer ou désactiver la fonctionnalité de traçage permanent. Le traçage permanent permet de collecter des journaux critiques au moment de la connexion. Ces journaux peuvent aider à la résolution des problèmes de connectivité intermittente. La stratégie de traçage permanent remplace ce paramètre.
Exemple d'utilisation	CitrixReceiver.exe /EnableTracing=true

À propos du Programme d'amélioration de l'expérience utilisateur Citrix (CEIP)

Option	EnableCEIP={true , false }
Description	Lorsque vous choisissez de participer au Programme d'amélioration de l'expérience utilisateur (CEIP), des informations d'utilisation et des statistiques anonymes sont envoyées à Citrix pour nous aider à améliorer la qualité et les performances des produits Citrix.
Exemple d'utilisation	CitrixReceiver.exe EnableCEIP=true

Spécifier le répertoire d'installation

Option	INSTALLDIR=*Répertoire d'installation*
Description	Spécifie le chemin d'installation sur lequel la plupart des composants de Citrix Receiver sont installés. La valeur par défaut est C:\Program Files\Citrix\Receiver. Les composants Receiver suivants sont installés dans C:\Program Files\Citrix : **Authentication Manager**, **Citrix Receiver** et **Self-Service Plug-in**. Si vous utilisez cette option et que vous spécifiez un répertoire d'installation, vous devez installer le fichier RIInstaller.msi dans le répertoire \Receiver et les autres fichiers .msi dans le répertoire d'installation.
Exemple d'utilisation	CitrixReceiver.exe INSTALLDIR=c:\Citrix\Test

Identifier une machine utilisateur

Option	CLIENT_NAME=*NomClient*
Description	Spécifie le nom du client, où NomClient correspond au nom utilisé pour identifier la machine utilisateur sur le serveur. La valeur par défaut est %NOMORDINATEUR%.
Exemple d'utilisation	CitrixReceiver.exe CLIENT_NAME=%NOMORDINATEUR%

Nom de client dynamique

Option	ENABLE_CLIENT_NAME=Yes, No
Description	La fonction de nom de client dynamique permet de garder un nom de client identique au nom de machine. Lorsqu'un utilisateur change le nom de sa machine, le nom de client change en conséquence. La valeur par défaut est Yes. Pour désactiver la prise en charge du nom de client dynamique, définissez cette propriété sur No puis spécifiez une valeur pour la propriété CLIENT_NAME.
Exemple d'utilisation	CitrixReceiver.exe ENABLE_DYNAMIC_CLIENT_NAME =Yes

Installer les composants spécifiés

Option	ADDLOCAL=<fonctionnalité… ,>
Description	Installe un ou plusieurs des composants spécifiés. Lorsque vous définissez plusieurs paramètres, chaque paramètre doit être séparé par une virgule et ne contenir aucun espace. Les noms sont sensibles à la casse. Si vous ne spécifiez pas ce paramètre, tous les composants sont installés par défaut. Citrix vous recommande d'utiliser l'exemple d'utilisation ADDLOCAL ci-dessous. Si l'exemple d'utilisation n'est pas utilisé comme indiqué, cela peut éventuellement provoquer un comportement inattendu. Les composants incluent : ReceiverInside: installe l'expérience d'application Citrix Workspace (composant requis pour le fonctionnement de l'application Workspace). ICA_Client: installe l'application Citrix Workspace standard (composant requis pour le fonctionnement de l'application Workspace). WebHelper : installe le composant WebHelper. Ce composant récupère le fichier .ica à partir de StoreFront et le transmet au moteur HDX. Il vérifie également les paramètres d'environnement et les partage avec StoreFront (similaire à la détection de client ICO). [Facultatif] SSON : installe Single Sign-On. Requiert des droits d'administrateur. AM : installe Authentication Manager. SELFSERVICE : installe Self-Service Plug-in. La valeur AM doit être spécifiée sur la ligne de commande et .NET 3.5 Service Pack 1 doit être installé sur la machine de l'utilisateur. Le Self-Service Plug-in n'est pas disponible pour les Windows Thin PC, qui ne prennent pas en charge .NET 3.5. Pour de plus amples informations sur la création de scripts pour Self-Service Plug-in (SSP) et pour consulter une liste des paramètres disponibles dans Receiver pour Windows 4.2 et versions ultérieures, consultez l'article CTX200337 du centre de connaissances. Le Self-Service Plug-in permet aux utilisateurs d'accéder à des applications et bureaux virtuels à partir de la fenêtre de l'application Citrix Workspace ou d'une ligne de commande, comme décrit plus loin dans

Option	ADDLOCAL=<fonctionnalité… ,>
Exemple d'utilisation	CitrixReceiver.exe ADDLO-CAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopView

Configurer Citrix Receiver pour Windows pour ajouter des magasins manuellement

Option	ENABLE_CLIENT_NAME=Yes, No
Description	La fonction de nom de client dynamique permet de garder un nom de client identique au nom de machine. Lorsqu'un utilisateur change le nom de sa machine, le nom de client change en conséquence. La valeur par défaut est Yes. Pour désactiver la prise en charge du nom de client dynamique, définissez cette propriété sur No puis spécifiez une valeur pour la propriété CLIENT_NAME.
Exemple d'utilisation	CitrixReceiver.exe ENABLE_DYNAMIC_CLIENT_NAME =Yes

Enregistrer les informations d'identification des magasins stockés localement à l'aide du protocole PNAgent

Option	ALLOWSAVEPWD={N, S, A}
Description	La valeur par défaut est la valeur spécifiée par le serveur PNAgent lors de l'exécution. Spécifie si les utilisateurs peuvent enregistrer les informations d'identification pour des magasins localement sur leurs ordinateurs. S'applique uniquement aux magasins utilisant le protocole PNAgent. La valeur par défaut est S. **N** : ne jamais autoriser les utilisateurs à enregistrer leurs mots de passe. **S** : autoriser les utilisateurs à enregistrer des mots de passe pour les magasins sécurisés (HTTPS) et les magasins non sécurisés (HTTP). Vous pouvez également contrôler cette fonctionnalité en mettant à jour la clé de registre HKLM\Software[Wow6432Node]\Citrix\Dazzle\AllowSavePwd **Remarque**: les clés de registre suivantes doivent être ajoutées manuellement si AllowSavePwd ne fonctionne pas : **1 Clé** pour client avec OS 32 bits : HKLM\Software\Citrix\AuthManager **2 Clé** pour client avec OS 64 bits : HKLM\Software\wow6432node\Citrix\AuthManager **3 Type** : REG_SZ **4 Valeur** : never - ne jamais autoriser les utilisateurs à enregistrer leurs mots de passe. secureonly : autoriser les utilisateurs à enregistrer des mots de passe uniquement pour les magasins sécurisés (configurés avec HTTPS). always - autoriser les utilisateurs à enregistrer des mots de passe pour les magasins sécurisés (HTTPS) et les magasins non sécurisés (HTTP).
Exemple d'utilisation	CitrixReceiver.exe ALLOWADDSTORE=N

Sélectionner un certificat

Option	AM_CERTIFICATESELECTIONMODE={Prompt, SmartCardDefault, LatestExpriry }
Description	Utilisez cette option pour sélectionner un certificat. La valeur par défaut est Prompt, ce qui invite l'utilisateur à choisir un certificat dans une liste. Modifiez cette propriété afin de choisir le certificat par défaut (celui du fournisseur de carte à puce) ou le certificat doté de la date d'expiration la plus longue. S'il n'existe aucun certificat valide, l'utilisateur en est notifié et il a la possibilité d'utiliser une autre méthode d'ouverture de session, le cas échéant. Vous pouvez également contrôler cette fonctionnalité en mettant à jour la clé de registre de la ruche HKCU ou HKLM\Software[Wow6432Node]Citrix\AuthManager:Certificat Prompt | SmartCardDefault | LatestExpiry }. Les valeurs définies dans la ruche de registre HKCU ont priorité sur les valeurs définies dans la ruche de registre HKLM afin d'aider l'utilisateur à sélectionner un certificat.
Exemple d'utilisation	CitrixReceiver.exe AM_CERTIFICATESELECTIONMODE=Prompt

Utiliser les composants CSP pour gérer la saisie du code PIN de carte à puce

Option	AM_SMARTCARDPINENTRY=CSP
Description	Utilisez les composants CSP pour gérer la saisie du code PIN de carte à puce. Par défaut, les invites de saisie du code PIN sont fournies par Citrix Receiver plutôt que par le fournisseur de services cryptographiques (CSP) de la carte. Receiver invite les utilisateurs à entrer un code PIN lorsque cela est requis et transmet le code PIN au CSP de la carte à puce. Spécifiez cette propriété pour utiliser les composants CSP afin de gérer la saisie du code PIN, y compris le message invitant l'utilisateur à entrer le code PIN.
Exemple d'utilisation	CitrixReceiver.exe AM_SMARTCARDPINENTRY=CSP

Utilisation de Kerberos

Option	ENABLE_KERBEROS={Yes , No}
Description	La valeur par défaut est No. Spécifie si le moteur HDX doit utiliser l'authentification Kerberos et ne s'applique que lorsque l'authentification unique est activée. Pour de plus amples informations, consultez la section Configurer l'authentification unique au domaine avec Kerberos.
Exemple d'utilisation	CitrixReceiver.exe ENABLE_KERBEROS=No

Affichage des icônes FTA d'ancienne génération

Option	LEGACYFTAICONS={False, True}
Description	Utilisez cette option pour afficher les icônes FTA d'ancienne génération. La valeur par défaut est False. Spécifie si les icônes des applications sont affichées pour les documents qui disposent d'associations de type de fichier avec des applications faisant l'objet d'une souscription. Lorsque l'argument est défini sur False, Windows génère des icônes pour les documents pour lesquels aucune icône spécifique n'est attribuée. Les icônes générées par Windows se composent d'une icône de document générique sur laquelle est superposée une version plus petite de l'icône d'application. Citrix recommande d'activer cette option si vous prévoyez de mettre des applications Microsoft Office à la disposition des utilisateurs exécutant Windows 7.
Exemple d'utilisation	CitrixReceiver.exe LEGACYFTAICONS=False

Activation du pré-lancement

Option	ENABLEPRELAUNCH={False, True}
Description	La valeur par défaut est False. Pour plus d'informations sur le pré-lancement de session, consultez la section Réduction du temps de lancement des applications.
Exemple d'utilisation	CitrixReceiver.exe ENABLEPRELAUNCH=False

Spécification du répertoire des raccourcis du menu Démarrer

Option	STARTMENUDIR={Nom du répertoire}
Description	Par défaut, toutes les applications apparaissent sous Démarrer > Tous les programmes. Vous pouvez spécifier le chemin d'accès relatif des raccourcis dans le dossier des programmes. À titre d'exemple, pour placer les raccourcis sous Démarrer > Tous les programmes > Receiver, spécifiez STARTMENUDIR=\Receiver. Vous pouvez modifier ou déplacer le dossier à tout moment. Vous pouvez également contrôler cette fonctionnalité en utilisant la clé de registre : créez l'entrée REG_SZ pour StartMenuDir et donnez-lui la valeur « \RelativePath ». Emplacement : HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\Dazz , HKEY_CURRENT_USER\Software\Citrix\Dazzle. En ce qui concerne les applications publiées via XenApp pour lesquelles un dossier d'applications clientes (également appelé dossier Program Neighborhood) a été spécifié, vous pouvez indiquer que le dossier d'applications clientes doit être ajouté au chemin des raccourcis comme suit : créez l'entrée REG_SZ pour UseCategoryAsStartMenuPath et donnez-lui la valeur « true ». Utilisez les mêmes emplacements de registre que susmentionnés.**Remarque** : Windows 8/8.1 n'autorise pas la création de dossiers imbriqués dans le menu Démarrer. Les applications sont affichées séparément ou dans le dossier racine et pas dans les sous-dossiers de catégorie définis. Exemples : **1** Si le dossier d'applications du client est \Office, UseCategoryAsStartMenuPath est true, aucun StartMenuDir n'est spécifié et les raccourcis sont placés sous Démarrer > Tous les programmes > Office. **2** Si le dossier d'applications du client est \Office, UseCategoryAsStartMenuPath est true, StartMenuDir est \Receiver et les raccourcis sont placés sous Démarrer > Tous les programmes > Receiver > Office. Les

Option	STARTMENUDIR={Nom du répertoire}
Exemple d'utilisation	CitrixReceiver.exe STARTMENUDIR=\Office

Spécification du nom du magasin

Option	STOREx="storename;http[s]://servername.domain/IISLocatio Off] ; [storedescription] "[STOREy="–"]
Description	Utilisez cette option pour spécifier le nom du magasin. Spécifie jusqu'à 10 magasins à utiliser avec Citrix Receiver. Valeurs - **x et y** : entiers de 0 à 9 ; **storename** : nom par défaut store. Ce dernier doit correspondre au nom configuré sur le serveur StoreFront ; **servername.domain** : nom de domaine complet du serveur hébergeant le magasin ; **IISLocation** : chemin d'accès au magasin dans IIS. L'adresse URL du magasin doit correspondre à l'adresse URL des fichiers de provisioning dans StoreFront. Les adresses URL des magasins sont au format « /Citrix/store/discovery ». Pour obtenir l'adresse URL, exportez un fichier de provisioning de StoreFront, ouvrez-le dans Bloc-notes et copiez l'adresse URL à partir de l'élément *Address*. **On, Off** : le paramètre de configuration facultatif Off vous permet de délivrer des magasins désactivés, ce qui laisse aux utilisateurs le choix d'y accéder ou non. Lorsque l'état du magasin n'est pas spécifié, le paramètre par défaut est On ; **storedescription** : description facultative du magasin, telle que Magasin des applications HR.**Remarque** : dans cette version, il est important d'inclure « /discovery » dans l'URL du magasin pour garantir la réussite de l'authentification unique.
Exemple d'utilisation	CitrixReceiver.exe STORE0="Store;https://test.xx.com/Citrix/Store/Discovery"

Activation de la redirection d'URL sur les machines utilisateur

Option	ALLOW_CLIENTHOSTEDAPPSURL=1
Description	Active la fonctionnalité de redirection des adresses URL sur les machines utilisateur. Requiert des droits d'administrateur. Requiert que Citrix Receiver soit installé pour tous les utilisateurs. Pour de plus amples informations sur la redirection des adresses URL, consultez la section Local App Access et ses sous-rubriques dans la documentation XenDesktop 7.
Exemple d'utilisation	CitrixReceiver.exe ALLOW_CLIENTHOSTEDAPPSURL = 1

Activation du mode libre-service

Option	SELFSERVICEMODE={False , True}
Description	La valeur par défaut est True. Lorsque l'administrateur définit l'indicateur SelfServiceMode sur false, l'utilisateur n'a plus accès à l'interface utilisateur Citrix Receiver en libre-service. Au lieu de cela, ils peuvent accéder aux applications auxquelles ils ont souscrit dans le menu Démarrer et via des raccourcis de bureau, appelé **« mode Raccourci uniquement »**.
Exemple d'utilisation	CitrixReceiver.exe SELFSERVICEMODE=False

Spécification du répertoire des raccourcis de bureau

Option	DESKTOPDIR = *Nom du répertoire*
Description	Rassemble tous les raccourcis dans un dossier unique. Category Path est pris en charge pour les raccourcis de bureau. **Remarque** : lorsque vous utilisez l'option DESKTOPDIR, définissez la clé PutShortcutsOnDesktop sur True.
Exemple d'utilisation	CitrixReceiver.exe DESKTOPDIR=\Office

Mise à niveau d'une version non prise en charge de Citrix Receiver

> **Remarque**
>
> Lorsque vous mettez à niveau Citrix Receiver version 13.x Enterprise ou 12.x vers Citrix Receiver pour Windows Version 4.4 et versions ultérieures à l'aide de l'interface utilisateur graphique, le programme d'installation exécute l'utilitaire de nettoyage de Receiver par défaut.
>
> Toutefois, l'utilitaire n'est pas exécuté par défaut lorsque vous mettez à niveau à partir de la ligne de commande. Pour mettre à niveau à partir de la ligne de commande, exécutez la commande suivante :
>
> *CitrixReceiver.exe /rcu /silent*
>
> Lorsque vous mettez à niveau Citrix Receiver pour Windows 13.x (non Enterprise) ou 4.1 vers la version 4.2 ou versions ultérieures, le commutateur /rcu est inutile et donc ignoré.

Option	/rcu
Description	Vous permet de mettre à niveau à partir d'une version non prise en charge vers la dernière version de Citrix Receiver.
Exemple d'utilisation	CitrixReceiver.exe /rcu

Résolution des problèmes d'installation

S'il y a un problème avec l'installation, recherchez dans le répertoire %TEMP%/CTXReceiverInstallLogs de l'utilisateur les fichiers journaux comportant le préfixe CtxInstall- ou TrolleyExpress-. Par exemple :

CtxInstall-ICAWebWrapper-20141114-134516.log

TrolleyExpress-20090807-123456.log

Exemples d'installation par ligne de commande

Pour spécifier l'adresse URL du magasin NetScaler Gateway :

CitrixReceiver.exe STORE0="<StoreFriendlyName>;testserver <StoreName>;<On/Off>;<StoreDescription>"

Remarque : l'URL du magasin NetScaler Gateway doit être la première entrée dans la liste des adresses URL de magasin configurées.

Pour installer tous les composants de façon silencieuse et spécifier deux magasins applicatifs :

Pour spécifier le single sign-on (authentification pass-through) et ajouter un magasin pointant vers une adresse URL XenApp Services :

Pour lancer une application ou un bureau virtuel à partir d'une ligne de commande

Citrix Receiver pour Windows crée une application stub pour chaque bureau ou application auxquels vous avez souscrit. Vous pouvez utiliser une application stub pour lancer une application ou un bureau virtuel à partir de la ligne de commande. Les applications stub se trouvent dans %appdata%\Citrix\SelfService. Le nom de fichier d'une application stub est le nom d'affichage de l'application, dont les espaces ont été supprimés. À titre d'exemple, le nom de fichier de l'application stub pour Internet Explorer est InternetExplorer.exe.

Déployer à l'aide de System Center Configuration Manager 2012 R2

June 27, 2019

Vous pouvez utiliser Microsoft System Center Configuration Manager (SCCM) pour déployer Citrix Receiver pour Windows.

Remarque : seules la version 4.5 et les versions ultérieures de Citrix Receiver pour Windows prennent en charge le déploiement de SCCM.

Quatre tâches sont nécessaires au déploiement de Citrix Receiver pour Windows à l'aide de SCCM :

1. Ajout de Citrix Receiver pour Windows au déploiement SCCM
2. Ajout de points de distribution
3. Déploiement du logiciel Receiver sur le Centre logiciel
4. Création de regroupements de périphériques

Ajout de Citrix Receiver pour Windows au déploiement SCCM

1. Copiez le logiciel Citrix Receiver téléchargé sur un dossier sur le serveur de Configuration Manager et démarrez la console Configuration Manager.

2. Sélectionnez **Bibliothèque de logiciels** > **Gestion d'applications**. Cliquez avec le bouton droit de la souris sur **Application** et cliquez sur **Créer une application**.
   L'assistant Créer une application s'affiche.
3. Dans le panneau **Général**, sélectionnez **Spécifier manuellement les informations de l'application** et cliquez sur **Suivant**.
4. Dans le panneau **Informations générales**, spécifiez les informations relatives à l'application comme le nom, le fabricant, la version du logiciel, etc.
5. Dans l'Assistant Catalogue d'applications, spécifiez des informations supplémentaires telles que la langue, le nom de l'application, la catégorie utilisateur, etc. et cliquez sur **Suivant**.

   Remarque : les utilisateurs peuvent voir les informations que vous spécifiez ici.
6. Dans le panneau **Type de déploiement**, cliquez sur **Ajouter** pour configurer le type de déploiement pour l'installation de Citrix Receiver.

   L'Assistant Création d'un type de déploiement s'affiche.
7. Dans le panneau **Général** : définissez le type de déploiement sur Windows Installer (fichier *.msi), sélectionnez **Spécifier manuellement les informations sur le type de déploiement** et cliquez sur **Suivant**.
8. Dans le panneau **Informations générales** : spécifiez les détails du type de déploiement (par exemple, déploiement de Receiver) et cliquez sur **Suivant**.
9. Dans le panneau **Contenu** :
   a) Spécifiez le chemin dans lequel le fichier d'installation de Citrix Receiver est présent. Par exemple : Outils sur le serveur SCCM.
   b) Spécifiez **Programme d'installation** en utilisant un des éléments suivants :
      - CitrixReceiver.exe /silent pour l'installation silencieuse par défaut.
      - CitrixReceiver.exe /silent /includeSSON pour activer l'authentification pass-through au domaine.
      - -CitrixReceiver.exe /silent SELFSERVICEMODE = false pour installer Receiver en mode de non libre-service.
   c) Spécifiez **Programme de désinstallation** sur CitrixReceiver.exe /uninstall (pour permettre la désinstallation via SCCM).
10. Dans le panneau **Méthode de détection** : sélectionnez **Configurer des règles pour détecter la présence de ce type de déploiement** et cliquez sur **Ajouter une clause**.
    La boîte de dialogue Règle de détection s'affiche.
11. Définissez **Type de paramètre** sur **Système de fichiers**.
12. Sous **Spécifier le fichier ou dossier pour détecter l'application**, définissez ce qui suit :
    - **Type** : à partir du menu déroulant, sélectionnez Fichier.

- **Chemin** : %ProgramFiles (x86)%\Citrix\ICA Client\Receiver
- **Nom du fichier ou du dossier** : Receiver.exe
- **Propriété** : à partir du menu déroulant, sélectionnez **Version**.
- **Opérateur** : à partir du menu déroulant, sélectionnez **Supérieur ou égal à**.
- **Valeur** : entrez **4.3.0.65534**.

Remarque : cette combinaison de règles s'applique également aux mises à niveau de Citrix Receiver pour Windows.

13. Dans le panneau **Expérience utilisateur**, définissez :

    - **Comportement à l'installation** : Installer pour le système
    - **Condition d'ouverture de session** : Qu'un utilisateur soit connecté ou non
    - **Visibilité du programme d'installation** : Normal

    Cliquez sur **Suivant**.

    Remarque : ne spécifiez aucune exigence ni dépendance pour ce type de déploiement.

14. Dans le panneau **Résumé**, vérifiez les paramètres pour ce type de déploiement. Cliquez sur **Suivant**.

    Un message de réussite s'affiche.

15. Dans le panneau **Progression**, un nouveau type de déploiement (déploiement de Receiver) est répertorié sous les types de déploiement.

16. Cliquez sur **Suivant** et sur **Fermer**.

Ajouter des points de distribution

1. Cliquez avec le bouton droit sur Receiver pour Windows dans la console Configuration Manager et sélectionnez **Distribuer du contenu**.
   L'assistant Distribuer du contenu s'affiche.
2. Dans le panneau de Distribuer du contenu, cliquez sur **Ajouter > Points de distribution**.

   La boîte de dialogue Ajouter des points de distribution s'affiche.
3. Recherchez le serveur SCCM sur lequel le contenu est disponible et cliquez sur **OK**.

   Un message de réussite s'affiche dans le panneau Progression.
4. Cliquez sur **Fermer**.

Déployer le logiciel Receiver sur le Centre logiciel

1. Cliquez avec le bouton droit sur Receiver pour Windows dans la console Configuration Manager et sélectionnez **Déployer**.

L'Assistant Déployer le logiciel s'affiche.

2. Sélectionnez **Parcourir** dans Regroupement (il peut s'agir de Regroupement de périphériques ou Regroupement d'utilisateurs) pour sélectionner le regroupement vers lequel vous souhaitez déployer l'application et cliquez sur **Suivant**.
3. Dans le panneau **Paramètres de déploiement**, définissez **Action** sur Installer et **Objet** sur Obligatoire (active l'installation non assistée). Cliquez sur **Suivant**.
4. Dans le panneau **Planification**, spécifiez le programme de déploiement du logiciel sur les machines cibles.
5. Dans le panneau **Expérience utilisateur**, définissez le comportement **Notifications utilisateur** ; sélectionnez **Valider les modifications à l'échéance ou au cours d'une fenêtre de maintenance (requiert un redémarrage)** et cliquez sur **Suivant** pour terminer l'Assistant Déploiement logiciel.

Un message de réussite s'affiche dans le panneau Progression.

Redémarrez les machines de point de terminaison cibles (uniquement requis pour démarrer l'installation immédiatement).

Sur les machines de point de terminaison, Citrix Receiver pour Windows est visible dans le Centre logiciel sous **Logiciels disponibles**. L'installation est déclenchée automatiquement en fonction du programme que vous avez configuré. Éventuellement, vous pouvez également programmer ou installer à la demande. L'état de l'installation s'affiche dans le Centre logiciel après le démarrage de l'installation.

Création de regroupements de périphériques

1. Démarrez la console Configuration Manager, cliquez sur **Ressources et Conformité** > **Présentation** > **Périphériques**.
2. Cliquez avec le bouton droit de la souris sur **Regroupements de périphériques** et sélectionnez **Créer un regroupement de périphériques**.

   L'Assistant Création d'un regroupement de périphériques s'affiche.
3. Dans le panneau **Général**, tapez le nom du périphérique et cliquez sur **Parcourir** pour Limitation au regroupement.

   Cela détermine l'étendue des périphériques, qui peut être l'un des Regroupements de périphériques par défaut créé par SCCM.
   Cliquez sur **Suivant**.
4. Dans le panneau Règles d'adhésion, cliquez sur **Ajouter une règle** pour filtrer les périphériques.

   L'Assistant Création d'une règle d'adhésion directe s'affiche.

Dans le panneau Rechercher des ressources, sélectionnez **Nom d'attribut** en fonction des périphériques que vous souhaitez filtrer et entrez la valeur de nom d'attribut pour sélectionner les périphériques.

5. Cliquez sur **Suivant**. Dans le panneau Sélectionner les ressources, sélectionnez les périphériques qui doivent faire partie du regroupement de périphériques.

   Un message de réussite s'affiche dans le panneau Progression.

6. Cliquez sur **Fermer**.
7. Dans le panneau Règles d'adhésion, une nouvelle règle est répertoriée. Cliquez sur **Suivant**.
8. Un message de réussite s'affiche dans le panneau Progression. Cliquez sur **Fermer** pour fermer l'assistant Création d'un regroupement de périphériques.

   Le nouveau regroupement de périphériques est répertorié dans **Regroupements de périphériques**. Le nouveau regroupement de périphériques fait partie des Regroupements de périphériques lors de la navigation dans l'Assistant Déployer le logiciel.

> **Remarque**
>
> Lorsque vous définissez l'attribut **MSIRESTARTMANAGERCONTROL** sur **False**, le déploiement de Citrix Receiver pour Windows à l'aide de SCCM peut échouer.
> D'après notre analyse, Citrix Receiver pour Windows n'est PAS la cause de cet échec. En outre, une nouvelle tentative peut se solder par un déploiement réussi.

Déployer Citrix Receiver pour Windows à partir d'un écran d'ouverture de session de l'Interface Web

November 16, 2018

Cette fonctionnalité est uniquement disponible pour les versions de XenDesktop et XenApp qui prennent en charge l'Interface Web.

Vous pouvez déployer Citrix Receiver pour Windows à partir d'une page Web pour vous assurer qu'il est installé sur la machine des utilisateurs avant qu'ils n'utilisent l'Interface Web. L'Interface Web dispose d'un processus de détection et de déploiement de client dont la tâche consiste à détecter les clients Citrix susceptibles d'être déployés dans l'environnement des utilisateurs puis à les guider au travers de la procédure de déploiement.

Vous pouvez configurer l'exécution automatique du processus de détection et de déploiement de client lorsque les utilisateurs accèdent à un site XenApp Web. Si l'Interface Web détecte qu'un utilisateur ne possède pas une version compatible de Citrix Receiver pour Windows, l'utilisateur est invité à télécharger et installer Citrix Receiver pour Windows.

La découverte de compte basée sur l'adresse e-mail ne s'applique pas lorsque Citrix Receiver pour Windows est déployé à partir de l'Interface Web. Si la découverte de compte basée sur l'adresse e-mail est configurée et qu'un nouvel utilisateur installe Citrix Receiver pour Windows à partir de Citrix.com, Citrix Receiver pour Windows invite l'utilisateur à entrer une adresse e-mail ou de serveur. La saisie d'une adresse e-mail entraîne le message d'erreur suivant : **Votre e-mail ne peut pas être utilisée pour ajouter un compte**. Utilisez la configuration suivante pour inviter l'utilisateur à entrer uniquement l'adresse d'un serveur.

1. Téléchargez CitrixReceiver.exe sur votre ordinateur local.
2. Renommez CitrixReceiver.exe par CitrixReceiverWeb.exe.
3. Spécifiez le nouveau nom du fichier dans le paramètre ClientIcaWin32 dans les fichiers de configuration pour vos sites XenApp Web.

   Pour utiliser le processus de détection et de déploiement de client, les fichiers d'installation de Citrix Receiver pour Windows doivent être disponibles sur le serveur Interface Web. Par défaut, l'Interface Web suppose que les fichiers d'installation de Citrix Receiver pour Windows sont les mêmes que ceux fournis sur le support d'installation de XenApp ou XenDesktop.
4. Vous devrez ajouter à la zone Sites de confiance les sites à partir desquels sera téléchargé le fichier CitrixReceiverWeb.exe.
5. Déployez le fichier exécutable renommé à l'aide de votre méthode de déploiement habituelle.

Installation et désinstallation manuelle de Citrix Receiver pour Windows

June 27, 2019

Vous pouvez installer Citrix Receiver pour Windows à partir du support d'installation, d'un partage réseau, de l'explorateur Windows, ou d'une ligne de commande en exécutant le pack d'installation CitrixReceiver.exe. Pour obtenir les paramètres de ligne de commande d'installation et la configuration d'espace requis, consultez la section Configuration et utilisation de Receiver pour Windows à l'aide de paramètres de ligne de commande.

Validation de l'espace disque disponible

Citrix Receiver pour Windows vérifie s'il existe suffisamment d'espace disque disponible pour procéder à l'installation. La vérification est effectuée aussi bien lors d'une nouvelle installation que d'une mise à niveau.

Lors d'une nouvelle installation, l'installation se termine lorsque l'espace disque est insuffisant et que la boîte de dialogue suivante s'affiche.

Lorsque vous mettez à niveau Citrix Receiver pour Windows, l'installation se termine lorsque l'espace disque est insuffisant et que la boîte de dialogue suivante s'affiche.

Le tableau suivant fournit des informations sur l'espace disque minimal requis pour installer Citrix Receiver pour Windows.

Type d'installation	Espace disque requis
Nouvelle installation	320 Mo
Mise à niveau de Citrix Receiver	206 Mo

Remarque

- Le programme d'installation vérifie l'espace disque uniquement après l'extraction du package d'installation.
- Lorsque l'espace disque du système est insuffisant lors d'une installation silencieuse, la boîte de dialogue ne s'affiche pas, mais le message d'erreur est consigné dans **CTXInstall_TrolleyExpress-*.log**.

Désinstallation de Citrix Receiver pour Windows

Vous pouvez désinstaller Citrix Receiver pour Windows avec l'utilitaire Programmes et fonctionnalités de Windows (Ajout/Suppression de programmes).

Remarque

Vous êtes invité à désinstaller le package Citrix HDX RTME avant de poursuivre l'installation de Citrix Receiver pour Windows. Pour plus d'informations, consultez l'article CTX200340 du centre de connaissances.

Pour désinstaller Citrix Receiver pour Windows à l'aide de l'interface de ligne de commande

Vous pouvez également désinstaller Citrix Receiver pour Windows à partir d'une ligne de commande en tapant la commande appropriée :

CitrixReceiver.exe /uninstall

Les clés de registre créées par receiver.adm/receiver.adml ou receiver.admx demeurent dans le répertoire Software\Policies\Citrix\ICA Client sous HKEY_LOCAL_MACHINE et HKEY_LOCAL_USER après la désinstallation.

Lorsque vous réinstallez Citrix Receiver pour Windows, ces stratégies peuvent être appliquées, avec des risques de dysfonctionnement intempestif. Pour supprimer les personnalisations, supprimez-les manuellement.

Pour la désinstallation en mode silencieux de Receiver pour Windows, exécutez le commutateur suivant :

CitrixReceiver.exe \silent \uninstall

Déployer à l'aide d'Active Directory et d'exemples de scripts de démarrage

June 27, 2019

Vous pouvez utiliser des scripts de stratégie de groupe Active Directory pour pré-déployer Citrix Receiver pour Windows sur des systèmes en fonction de votre structure organisationnelle Active Directory. Citrix recommande d'utiliser des scripts plutôt que d'extraire les fichiers .msi car les scripts permettent depuis un point unique de procéder à des installations, mises à niveau et désinstallations. En outre, ils consolident les entrées Citrix dans Programmes et fonctionnalités et facilitent la détection de la version de Citrix Receiver déployée. Utilisez le paramètre Scripts dans la console Gestion des stratégies de groupe (GPMC) sous Configuration ordinateur ou Configuration utilisateur. Pour obtenir des informations générales sur les scripts de démarrage, reportez-vous à la documentation Microsoft.

Citrix comprend des exemples de scripts de démarrage par ordinateur destinés à installer et désinstaller CitrixReceiver.exe. Les scripts sont disponibles sur la page Téléchargements de Citrix Receiver pour Windows.

- CheckAndDeployReceiverPerMachineStartupScript.bat
- CheckAndRemoveReceiverPerMachineStartupScript.bat

Lorsque les scripts sont exécutés au démarrage ou à la fermeture d'une stratégie de groupe Active Directory, il se peut que les fichiers de configuration personnalisés soient créés dans le profil d'utilisateur par défaut d'un système. S'ils ne sont pas supprimés, ces fichiers de configuration peuvent empêcher certains utilisateurs d'accéder au répertoire de journaux de Receiver. Les scripts exemple Citrix comprennent une fonctionnalité destinée à supprimer ces fichiers de configuration.

Pour utiliser les scripts de démarrage de manière à déployer Receiver avec Active Directory

1. Créez l'unité d'organisation pour chaque script.
2. Créez un objet de stratégie de groupe (GPO) pour l'unité d'organisation que vous venez de créer.

Modifier les exemples de scripts

Modifiez les scripts en modifiant ces paramètres dans la section d'en-tête de chaque fichier :

- **Version actuelle du package** - Le numéro de version spécifié est validé et s'il n'est pas présent, le déploiement se poursuit. Par exemple, DesiredVersion= 3.3.0.XXXX doit correspondre exactement à la version spécifiée. Si vous spécifiez une version partielle, par exemple 3.3.0, elle correspond à toute version avec ce préfixe (3.3.0.1111, 3.3.0.7777 et ainsi de suite).
- **Emplacement du package/répertoire de déploiement** - Ce paramètre spécifie le partage réseau contenant les packs. Il n'est pas authentifié par le script. Le dossier partagé doit disposer d'autorisations d'accès en lecture pour Tout le monde.
- **Répertoire de journalisation du script** - Ce paramètre spécifie le partage réseau sur lequel les journaux d'installation sont copiés. Il n'est pas authentifié par le script. Le dossier partagé doit disposer d'autorisations d'accès en lecture et écriture pour Tout le monde.
- **Options de ligne de commande d'installation du package** - Ces options de ligne de commande sont transmises au programme d'installation. Pour obtenir la syntaxe de la ligne de commande, consultez la section Configuration et utilisation de Receiver pour Windows à l'aide de paramètres de ligne de commande.

Pour ajouter des scripts de démarrage par ordinateur

1. Ouvrez la Console de gestion des stratégies de groupe.
2. Sélectionnez Configuration ordinateur > Stratégies > Paramètres Windows > Scripts (ouverture/fermeture de session).
3. Dans le panneau droit de la console Gestion des stratégies de groupe, sélectionnez Démarrage.
4. Dans le menu Propriétés, cliquez sur Afficher les fichiers, copiez le script approprié sur le dossier affiché et fermez la fenêtre.
5. Dans le menu Propriétés, cliquez sur Ajouter et utilisez le bouton Parcourir pour trouver et ajouter le nouveau script que vous venez de créer.

Pour déployer Citrix Receiver pour Windows par ordinateur

1. Déplacez les machines utilisateur désignées pour recevoir ce déploiement sur l'unité d'organisation que vous avez créée.
2. Redémarrez la machine utilisateur et ouvrez une session en tant qu'utilisateur quelconque.
3. Vérifiez que Programmes et fonctionnalités (Ajout/Suppression de programmes dans les versions antérieures du système d'exploitation) contient le nouveau pack installé.

Pour supprimer Citrix Receiver pour Windows par ordinateur

1. Déplacez les machines utilisateur désignées pour suppression sur l'unité d'organisation que vous avez créée.
2. Redémarrez la machine utilisateur et ouvrez une session en tant qu'utilisateur quelconque.
3. Vérifiez que Programmes et fonctionnalités (Ajout/Suppression de programmes dans les versions antérieures du système d'exploitation) a supprimé le pack préalablement installé.

Utilisation des exemples de scripts de démarrage par utilisateur

Citrix recommande d'utiliser des scripts de démarrage par ordinateur. Dans le cadre de déploiements Windows par utilisateur, les deux scripts suivants par utilisateur Citrix Receiver pour Windows sont inclus sur le support XenDesktop et XenApp dans le dossier Citrix Receiver for Windows and Plug-ins\Windows\Receiver\Startup_Logon_Scripts.

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

Pour définir des scripts de démarrage par utilisateur

1. Ouvrez la Console de gestion des stratégies de groupe.
2. Sélectionnez Configuration utilisateur > Stratégies > Paramètres Windows > Scripts.
3. Dans le panneau droit de la console Gestion des stratégies de groupe, sélectionnez Ouverture de session .
4. Dans le menu Propriétés de : Ouverture de session, cliquez sur Afficher les fichiers, copiez le script approprié sur le dossier affiché et fermez la fenêtre.
5. Dans le menu Propriétés de : Ouverture de session, cliquez sur Ajouter et utilisez le bouton Parcourir pour trouver et ajouter le nouveau script que vous venez de créer.

Pour déployer Citrix Receiver pour Windows par utilisateur

1. Déplacez les utilisateurs désignés pour recevoir ce déploiement sur l'unité d'organisation que vous avez créée.
2. Redémarrez la machine utilisateur et ouvrez une session en tant qu'un des utilisateurs spécifiés.
3. Vérifiez que Programmes et fonctionnalités (Ajout/Suppression de programmes dans les versions antérieures du système d'exploitation) contient le nouveau pack installé.

Pour supprimer Citrix Receiver pour Windows par utilisateur

1. Déplacez les utilisateurs désignés pour suppression sur l'unité d'organisation que vous avez créée.

2. Redémarrez la machine utilisateur et ouvrez une session en tant qu'un des utilisateurs spécifiés.
3. Vérifiez que Programmes et fonctionnalités (Ajout/Suppression de programmes dans les versions antérieures du système d'exploitation) a supprimé le pack préalablement installé.

Déploiement de Citrix Receiver pour Windows à partir de Receiver pour Web

June 27, 2019

Vous pouvez déployer Citrix Receiver pour Windows à partir de Citrix Receiver pour Web pour vous assurer que Receiver est installé avant de vous connecter à une application à partir d'un navigateur. Les sites Citrix Receiver pour Web vous permettent d'accéder aux magasins StoreFront via une page Web. Si le site Citrix Receiver pour Web détecte qu'un utilisateur ne possède pas une version compatible de Citrix Receiver pour Windows, vous êtes invité à télécharger et installer Citrix Receiver pour Windows.

Pour plus d'informations, veuillez consulter la section
Sites Citrix Receiver pour Web dans la documentation de StoreFront.

La découverte de compte basée sur l'adresse e-mail n'est pas prise en charge lorsque Citrix Receiver pour Windows est déployé à partir de Citrix Receiver pour Web. Si la découverte de compte basée sur l'adresse e-mail est configurée et qu'un nouvel utilisateur installe Citrix Receiver pour Windows à partir de Citrix.com, Citrix Receiver pour Windows invite l'utilisateur à entrer une adresse e-mail ou de serveur. La saisie d'une adresse e-mail entraîne le message d'erreur suivant : « Votre e-mail ne peut pas être utilisée pour ajouter un compte. »

Utilisez la configuration suivante pour inviter l'utilisateur à entrer uniquement l'adresse d'un serveur.

1. Téléchargez CitrixReceiver.exe sur votre ordinateur local.
2. Renommez CitrixReceiver.exe par CitrixReceiverWeb.exe.
3. Déployez le fichier exécutable renommé à l'aide de votre méthode de déploiement habituelle. Si vous utilisez StoreFront, consultez la section Configuration de sites Receiver pour Web à l'aide des fichiers de configuration dans la documentation de StoreFront.

Configurer

June 27, 2019

Lors de l'utilisation de Citrix Receiver pour Windows, les étapes de configuration suivantes permettent aux utilisateurs d'accéder à leurs applications et bureaux hébergés :

- Configurer la mise à disposition d'applications et Configuration de votre environnement XenDesktop. Assurez-vous que votre environnement XenApp est configuré correctement. Comprenez les options qui vous sont offertes et fournissez des descriptions claires des applications.
- Configurer le mode libre-service en ajoutant un compte StoreFront à Citrix Receiver pour Windows. Ce mode permet aux utilisateurs de s'abonner à des applications depuis l'interface utilisateur de Citrix Receiver pour Windows.
- Configurer avec le modèle d'administration d'objet de stratégie de groupe
- Fournir des informations de compte aux utilisateurs. Fournissez aux utilisateurs les informations requises pour configurer l'accès aux comptes hébergeant leurs applications et bureaux virtuels. Dans certains environnements, les utilisateurs doivent manuellement configurer l'accès à ces comptes.

Les utilisateurs se connectant depuis l'extérieur du réseau interne doivent configurer l'authentification à l'aide de NetScaler Gateway. Pour de plus amples informations, consultez Authentification et autorisation dans la documentation de NetScaler Gateway.

Configuration de la mise à disposition d'applications

June 27, 2019

Lors de la mise à disposition d'applications avec XenDesktop ou XenApp, envisagez les options suivantes pour améliorer l'expérience des utilisateurs :

- Mode d'accès au Web : sans aucune configuration, Citrix Receiver pour Windows permet d'accéder, par le biais d'un navigateur, aux applications et aux bureaux. Vous pouvez ouvrir un site Receiver pour Web où un site Interface Web dans un navigateur pour sélectionner les applications que vous souhaitez utiliser. Dans ce mode, aucun raccourci n'est placé sur le bureau de l'utilisateur.
- Mode libre-service : il vous suffit d'ajouter un compte StoreFront à Citrix Receiver pour Windows ou de configurer Citrix Receiver pour Windows de manière à pointer vers un site StoreFront pour pouvoir configurer le *mode libre-service*, qui vous permet de vous abonner à des applications à partir de l'interface utilisateur de Citrix Receiver pour Windows. Cette expérience enrichie est similaire à celle que propose un magasin d'applications mobiles. En mode libre-service, vous pouvez configurer des paramètres de mots-clés pour les applications sélectionnées, auto-provisionnées et obligatoires selon vos besoins.

Remarque : par défaut, Citrix Receiver pour Windows vous autorise à sélectionner les applications à afficher sur le menu Démarrer.

- Mode raccourci d'application uniquement : en tant qu'administrateur Citrix Receiver, vous pouvez configurer Citrix Receiver pour Windows de manière à placer automatiquement des raccour-

cis d'applications et de bureaux directement dans le menu Démarrer ou sur le bureau, de façon similaire à Citrix Receiver pour Windows Enterprise. Le nouveau mode *raccourci uniquement* vous permet de localiser toutes les applications publiées là où vous vous attendez à les trouver à l'aide du schéma de navigation Windows habituel.

Pour plus d'informations sur la mise à disposition d'applications à l'aide de XenApp et XenDesktop 7, consultez la section Créer un groupe de mise à disposition d'application.

> **Remarque**
>
> Lorsque vous mettez à niveau ou installez Citrix Receiver pour Windows pour la première fois, vous devez ajouter les derniers fichiers de modèle à l'objet de stratégie de groupe local.

Configuration de NetScaler Gateway Store

Citrix recommande d'utiliser le modèle d'administration d'objet de stratégie de groupe pour configurer les règles du routage réseau, les serveurs proxy, la configuration de serveurs de confiance, le routage des utilisateurs, les machines utilisateur distantes et l'expérience de l'utilisateur.
Vous pouvez utiliser les fichiers de modèle receiver.admx / receiver.adml avec des stratégies de domaine et des stratégies sur l'ordinateur local. Pour les stratégies de domaine, importez le fichier de modèle à l'aide de la console de gestion des stratégies de groupe. Cela est particulièrement utile pour appliquer les paramètres de Citrix Receiver pour Windows à un certain nombre de machines utilisateur différentes réparties dans l'entreprise. Pour n'affecter qu'une seule machine utilisateur, importez le fichier de modèle à l'aide de l'éditeur de stratégie de groupe local sur la machine.

Pour ajouter ou spécifier un NetScaler Gateway à l'aide du modèle d'administration d'objet de stratégie de groupe :

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud Configuration ordinateur, accédez à **Modèles d'administration** > **Modèles d'administration classiques (ADM)** > **Composants Citrix** > **Citrix Receiver** > **StoreFront**.
3. Sélectionnez Liste de comptes StoreFront\URL de Netscaler Gateway.
4. Modifiez les paramètres.
    - Nom du magasin : indique le nom de magasin affiché
    - URL du magasin : indique l'adresse URL du magasin
    - #Store name : indique le nom du magasin derrière NetScaler Gateway
    - État activé du magasin : indique l'état du magasin, On/Off
    - Description du magasin : fournit une description du magasin
5. Ajoutez ou spécifiez l'adresse URL de NetScaler. Entrez le nom de l'URL, séparé par des points-virgules :

Exemple : HRStore #Store name;On; Store for HR staff
où #Store name est le nom du magasin derrière NetScaler Gateway ; dtls.blrwinrx.com est l'URL de NetScaler

Lorsque Citrix Receiver pour Windows est lancé après l'ajout de NetScaler Gateway via un objet de stratégie de groupe, le message ci-dessous s'affiche dans la zone de notification.

Limitations

1. L'URL de NetScaler doit être indiquée en premier, suivie de l'adresse ou des adresses URL de StoreFront.
2. Il n'est pas possible de spécifier plusieurs adresses URL de NetScaler.
3. Toute modification de l'URL de NetScaler requiert que Citrix Receiver pour Windows soit réinitialisé pour que les modifications prennent effet.
4. L'URL de NetScaler Gateway configurée à l'aide de cette méthode ne prend pas en charge le site Services PNA derrière NetScaler Gateway.

Configurer le mode libre-service

Il vous suffit d'ajouter un compte StoreFront à Citrix Receiver ou de configurer Citrix Receiver de manière à pointer vers un site StoreFront pour pouvoir configurer le *mode libre-service*. Ce dernier permet aux utilisateurs de s'abonner à des applications à partir de l'interface utilisateur de Citrix Receiver. Cette expérience enrichie est similaire à celle que propose un magasin d'applications mobiles.

> **Remarque**
>
> Par défaut, Citrix Receiver pour Windows autorise les utilisateurs à sélectionner les applications qu'ils souhaitent afficher sur leur menu Démarrer.

En mode libre-service, vous pouvez configurer des paramètres de mots-clés pour les applications sélectionnées, auto-provisionnées et obligatoires selon vos besoins.

Ajoutez des mots-clés aux descriptions que vous fournissez pour les applications de groupe de mise à disposition :

- Pour faire d'une application individuelle une application obligatoire, de sorte qu'elle ne puisse pas être supprimée de Citrix Receiver pour Windows, ajoutez la chaîne KEYWORDS:Mandatory à la description de l'application. Il n'existe aucune option Supprimer pour les utilisateurs pour annuler l'inscription aux applications obligatoires.
- Pour abonner automatiquement tous les utilisateurs d'un magasin à une application, ajoutez la chaîne KEYWORDS:Auto à la description. Lorsque les utilisateurs ouvrent une session dans le magasin, l'application est automatiquement provisionnée sans qu'ils aient à y souscrire manuellement.

- Pour publier des applications auprès des utilisateurs ou pour faciliter la recherche des applications fréquemment utilisées en les répertoriant dans la liste Sélection de Citrix Receiver, ajoutez la chaîne KEYWORDS:Featured à la description de l'application.

Personnaliser l'emplacement des raccourcis d'applications à l'aide du modèle d'objet de stratégie de groupe

> **Remarque**
>
> Nous vous recommandons d'apporter des modifications à la stratégie de groupe avant de configurer un magasin. Si à tout moment, vous souhaitez personnaliser les stratégies de groupe, réinitialisez Citrix Receiver, configurez la stratégie de groupe, puis reconfigurez le magasin.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud Configuration ordinateur, accédez à Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Receiver > Libre-service.
3. Sélectionnez la stratégie **Gérer SelfServiceMode**.
   a) Sélectionnez Activé pour afficher l'interface utilisateur en libre-service.
   b) Sélectionnez Désactivé pour vous abonner manuellement aux applications. Cette option masque l'interface utilisateur en libre-service.
4. Cliquez sur Appliquer, puis sur OK.
5. Sous le nœud Configuration ordinateur, accédez à Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Receiver > Libre-service.
6. Sélectionnez la stratégie **Gérer les raccourcis d'applications**.
7. Sélectionnez les options si nécessaire.
8. Cliquez sur Appliquer, puis sur OK.
9. Redémarrez Citrix Receiver pour Windows pour que les modifications soient prises en compte.

Utilisation des paramètres de compte StoreFront pour personnaliser l'emplacement des raccourcis d'applications

Vous pouvez configurer des raccourcis dans le menu Démarrer et sur le bureau à partir du site StoreFront. Les paramètres suivants peuvent être ajoutés dans le fichier web.config dans **C:\inetpub\wwwroot\Citrix\Roaming** dans la section **<annotatedServices>** :

- Pour placer des raccourcis sur le bureau, utilisez PutShortcutsOnDesktop. Paramètres : « true » ou « false » (false est le paramètre par défaut).
- Pour placer des raccourcis dans le menu Démarrer, utilisez PutShortcutsInStartMenu. Paramètres : « true » ou « false » (true est le paramètre par défaut).
- Pour utiliser le chemin d'accès de catégorie dans le menu Démarrer, utilisez UseCategoryAsStartMenuPath. Paramètres : « true » ou « false » (true est le paramètre par défaut).

> **Remarque**
>
> Windows 8/8.1 et Windows 10 n'autorisent pas la création de dossiers imbriqués dans le menu Démarrer. Les applications seront affichées séparément ou sous le dossier racine mais pas dans les sous-dossiers de catégorie définis avec XenApp.

- Pour définir un répertoire unique pour tous les raccourcis dans le menu Démarrer, utilisez StartMenuDir. Paramètre : valeur de chaîne, correspondant au nom du dossier dans lequel les raccourcis sont créés.
- Pour réinstaller des applications modifiées, utilisez AutoReinstallModifiedApps. Paramètres : « true » ou « false » (true est le paramètre par défaut).
- Pour afficher un répertoire unique pour tous les raccourcis sur le bureau, utilisez DesktopDir. Paramètre : valeur de chaîne, correspondant au nom du dossier dans lequel les raccourcis sont créés.
- Pour ne pas créer d'entrée sur la liste « Ajout/Suppression de programmes » des clients, utilisez DontCreateAddRemoveEntry. Paramètres : « true » ou « false » (false est le paramètre par défaut).
- Pour supprimer les raccourcis et l'icône de Receiver d'une application préalablement disponible dans le magasin mais qui n'est plus disponible, utilisez SilentlyUninstallRemovedResources. Paramètres : « true » ou « false » (false est le paramètre par défaut).

Dans le fichier web.config, les modifications doivent être ajoutées dans la section XML pour le compte. Recherchez cette section en recherchant l'onglet d'ouverture :

<account id=… name="Store"

La section se termine par la balise </account>.

Avant la fin de la section account, dans la première section properties :

<properties> <clear /> </properties>

Les propriétés peuvent être ajoutées dans cette section après la balise <clear />, un par ligne, attribuant le nom et la valeur. Par exemple :

<property name="PutShortcutsOnDesktop" value="True" />

> **Remarque**
>
> les éléments de propriété ajoutés avant la balise <clear /> peuvent les invalider. La suppression de la balise <clear /> lors de l'ajout d'un nom de propriété et d'une valeur est facultative.

Voici un exemple étendu de cette section :

<properties> <property name="PutShortcutsOnDesktop" value="True" /> <property name="DesktopDir" value="Citrix Applications" />

> **Important**
>
> Dans les déploiements faisant appel à de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, propagez vos modifications apportées à la configuration au groupe de serveurs afin que les autres serveurs du déploiement soient mis à jour.

Utilisation des paramètres par application dans XenApp et XenDesktop 7.x pour personnaliser l'emplacement des raccourcis d'applications

Citrix Receiver peut être configuré pour placer automatiquement des raccourcis d'applications et de bureaux directement dans le menu Démarrer où sur le bureau. Cette fonctionnalité est semblable à celle des versions antérieures de Citrix Receiver, cependant, la version 4.2.100 permet désormais de choisir où placer les raccourcis d'applications à l'aide des paramètres par application XenApp. Cette fonctionnalité est utile dans les environnements comportant quelques applications qui doivent être affichées dans les mêmes emplacements.

Si vous souhaitez définir l'emplacement des raccourcis de manière à ce que chaque utilisateur puisse les trouver dans le même emplacement, utilisez les paramètres par application de XenApp :

Si vous souhaitez que les paramètres par application déterminent où les applications sont placées indépendamment du mode utilisé (libre-service ou mode du menu Démarrer)…	Configurez l'application Workspace pour Windows avec **PutShortcutsInStartMenu**=**false** et activez les paramètres par application. **Remarque :** ce paramètre s'applique aux sites Interface Web uniquement.

> **Remarque**
>
> Le paramètre **PutShortcutsInStartMenu=false** s'applique à XenApp 6.5 et XenDesktop 7.x.

Configurer les paramètres par application dans XenApp 6.5

Pour configurer un raccourci par application publiée dans XenApp 6.5 :

1. Dans l'écran des **propriétés d'application** XenApp, développez les propriétés **de base**.
2. Sélectionnez l'option **Présentation du raccourci**.
3. Dans la section **Emplacement(s) du ou des raccourci(s)** de l'écran **Présentation du raccourci**,

sélectionnez la case **Ajouter un raccourci dans le menu Démarrer du client**. Après avoir sélectionné la case à cocher, entrez le nom du dossier dans lequel vous souhaitez placer le raccourci. Si vous ne spécifiez pas de nom de dossier, XenApp place le raccourci dans le menu Démarrer sans le placer dans un dossier.

4. Sélectionnez **Ajouter un raccourci sur le bureau du client** pour inclure le raccourci sur le bureau d'une machine cliente.
5. Cliquez sur **Appliquer**.
6. Cliquez sur **OK**.

Utilisation des paramètres par application dans XenApp 7.6 pour personnaliser l'emplacement des raccourcis d'applications

Pour configurer un raccourci par application publiée dans XenApp 7.6 :

1. Dans Citrix Studio, accédez à l'écran **Paramètres de l'application**.
2. Dans l'écran **Paramètres de l'application**, sélectionnez **Mise à disposition**. À l'aide de cet écran, vous pouvez spécifier la méthode à utiliser pour mettre les applications à la disposition des utilisateurs.
3. Sélectionnez l'icône appropriée pour l'application. Cliquez sur **Modifier** pour accéder à l'icône souhaitée.
4. Dans le champ **Catégorie d'application**, vous pouvez indiquer la catégorie dans Receiver dans laquelle l'application apparaît. Par exemple, si vous ajoutez des raccourcis vers des applications Microsoft Office, entrez **Microsoft Office**.
5. Cochez la case **Ajouter un raccourci sur le bureau de l'utilisateur**.
6. Cliquez sur **OK**.

Réduction des délais d'énumération ou signature numérique des stubs applicatifs

Si les utilisateurs rencontrent des délais dans l'énumération des applications à chaque ouverture de session, ou s'il est nécessaire de signer numériquement les stubs applicatifs, Receiver dispose d'une fonctionnalité qui permet de copier les stubs .EXE à partir d'un partage réseau.

Cette fonctionnalité implique un certain nombre d'étapes :

1. Créez les stubs applicatifs sur la machine cliente.
2. Copiez les stubs applicatifs sur un emplacement accessible à partir d'un partage réseau.
3. Si nécessaire, préparez une liste blanche (ou signez les stubs avec un certificat d'entreprise).
4. Ajoutez une clé de registre pour permettre à Receiver de créer les stubs en les copiant à partir du partage réseau.

Si **RemoveappsOnLogoff** et **RemoveAppsonExit** sont activés, et que les utilisateurs rencontrent des délais dans l'énumération des applications à chaque ouverture de session, utilisez les informations suivantes pour réduire les délais :

1. Utilisez regedit pour ajouter la clé HKCU\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true".
2. Utilisez regedit pour ajouter la clé HKLM\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true". HKCU a la priorité sur HKLM.

Avertissement : toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Autorisez une machine à utiliser les exécutables stub précréés qui sont stockés sur un partage réseau :

1. Sur une machine cliente, créez des exécutables stub pour toutes les applications. Pour ce faire, ajoutez toutes les applications à la machine à l'aide de Receiver ; Receiver génère les fichiers exécutables.
2. Récoltez les exécutables stub depuis %APPDATA%\Citrix\SelfService. Vous n'avez besoin que des fichiers .exe.
3. Copiez les fichiers exécutables sur un partage réseau.
4. Pour chaque machine cliente qui est verrouillée, définissez les clés de registre suivantes :
    a) Reg add HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\ReceiverStu
    b) Utilisez regedit pour ajouter la clé HKLM\logiciel Citrix Dazzle/v
    c) CopyStubsFromCommonStubDirectory /t REG_SZ /d "true". Il est également possible de configurer ces paramètres sur le registre HKCU si vous le préférez. HKCU a la priorité sur HKLM.
    d) Quittez puis redémarrez Receiver pour tester les paramètres.

Exemples de cas d'utilisation

Vous trouverez dans cette rubrique des cas d'utilisation de raccourcis d'applications.

Autoriser les utilisateurs à choisir les applications à afficher dans le menu Démarrer (libre-service)

Si vos applications se comptent par dizaines (ou même par centaines), il est conseillé d'autoriser les utilisateurs à choisir les applications qu'ils préfèrent et souhaitent ajouter au menu Démarrer :

Si vous souhaitez autoriser les utilisateurs à choisir les applications à afficher dans leur menu Démarrer…	configurez Citrix Receiver en mode libre-service. Dans ce mode, vous configurez également les paramètres de mots-clés applicatifs *auto-provisionnées* et *obligatoires*.
Si vous souhaitez que les utilisateurs puissent choisir les applications à afficher dans leur menu Démarrer, mais que vous souhaitez également placer des raccourcis d'applications spécifiques sur le bureau…	configurez Citrix Receiver sans aucune option et paramétrez individuellement chaque application que vous voulez placer sur le bureau. Utilisez des applications *auto-provisionnées* et *obligatoires* en fonction de vos besoins.

Aucun raccourci d'application dans le menu Démarrer

Si l'ordinateur d'un utilisateur est utilisé par toute la famille, vous n'aurez peut-être besoin d'aucun raccourci d'application. Dans de tels scénarios, l'approche la plus simple est l'accès par navigateur ; installez Citrix Receiver sans configuration et utilisez Citrix Receiver pour Web et l'Interface Web. Vous pouvez également configurer Citrix Receiver pour un accès en libre-service sans créer de raccourcis.

Si vous souhaitez empêcher Citrix Receiver de placer des raccourcis d'applications dans le menu Démarrer automatiquement…	définissez la clé PutShortcutsInStartMenu=False sur Citrix Receiver. Citrix Receiver ne placera aucune application dans le menu Démarrer même en mode libre-service, à moins que vous ne le fassiez individuellement pour chaque application.

Tous les raccourcis d'applications dans le menu Démarrer ou sur le bureau

Si l'utilisateur ne dispose que de quelques applications, vous pouvez toutes les placer dans le menu Démarrer ou sur le bureau, ou dans un dossier sur le bureau.

Si vous souhaitez que Citrix Receiver place tous les raccourcis d'applications dans le menu Démarrer automatiquement…	définissez la clé SelfServiceMode=False sur Citrix Receiver. Toutes les applications disponibles s'afficheront dans le menu Démarrer.
Si vous voulez placer tous les raccourcis d'applications sur le bureau…	définissez la clé PutShortcutsOnDesktop=True sur Citrix Receiver. Toutes les applications disponibles s'afficheront sur le bureau.
Si vous voulez placer tous les raccourcis dans un dossier sur le bureau…	configurez Citrix Receiver avec le DesktopDir= nom du dossier de bureau sur lequel vous souhaitez placer les applications.

Paramètres par application dans XenApp 6.5 ou 7.x

Si vous souhaitez définir l'emplacement des raccourcis de manière à ce que chaque utilisateur puisse les trouver dans le même emplacement, utilisez les paramètres par application de XenApp :

Si vous souhaitez que les paramètres par application déterminent où les applications sont placées indépendamment du mode utilisé (libre-service ou mode du menu Démarrer)…	définissez la clé PutShortcutsInStartMenu=false sur Citrix Receiver et activez les paramètres par application.

Applications dans des dossiers de catégorie ou dans des dossiers spécifiques

Si vous souhaitez que les applications s'affichent dans des dossiers spécifiques, utilisez les options suivantes :

Si vous souhaitez que les raccourcis d'applications que Citrix Receiver place dans le menu Démarrer s'affichent dans leur catégorie associée (dossier)…	définissez la clé UseCategoryAsStartMenuPath=True sur Citrix Receiver.

Si vous souhaitez que les applications que Citrix Receiver place dans le menu Démarrer s'affichent dans un dossier spécifique…	configurez Citrix Receiver avec le StartMenuDir= nom de dossier du menu Démarrer.

Supprimer les applications à la fermeture de session ou en quittant

Si vous ne souhaitez pas que les utilisateurs puissent accéder aux applications d'autres utilisateurs sur un poste de travail partagé, vous pouvez vous assurer que les applications sont supprimées lorsque l'utilisateur ferme sa session ou quitte Receiver.

Si vous souhaitez que Citrix Receiver supprime toutes les applications à la fermeture de session…	définissez la clé RemoveAppsOnLogoff=True sur Citrix Receiver.
Si vous souhaitez que Citrix Receiver supprime toutes les applications à la fin de la session…	définissez la clé RemoveAppsOnExit=True sur Citrix Receiver.

Configuration des applications Local App Access

Lors de la configuration des applications Local App Access :

- Pour spécifier l'utilisation d'une application installée localement plutôt qu'une application disponible dans Citrix Receiver, ajoutez la chaîne KEYWORDS:prefer="pattern". Cette fonctionnalité est appelée Local App Access.

  Avant d'installer une application sur l'ordinateur d'un utilisateur, Citrix Receiver recherche les modèles spécifiés pour déterminer si l'application est installée localement. Si c'est le cas, Citrix Receiver souscrit à l'application et ne crée pas de raccourci. Lorsque l'utilisateur démarre l'application à partir de la fenêtre de Citrix Receiver, Citrix Receiver démarre l'installation installée localement (préférée).

  Si un utilisateur désinstalle une application préférée en dehors de Citrix Receiver, l'abonnement à l'application est annulé lors de la prochaine actualisation de Citrix Receiver. Si un utilisateur désinstalle une application préférée à partir de Citrix Receiver, Citrix Receiver annule l'abonnement à l'application mais ne la désinstalle pas.

> **Remarque**
>
> Le mot-clé prefer est appliqué lorsque Citrix Receiver souscrit à une application. L'ajout du mot-clé après souscription à l'application n'a aucun effet.

Vous pouvez spécifier le mot-clé prefer plusieurs fois pour une application. Il suffit d'une correspondance pour appliquer le mot-clé à une application. Les modèles suivants peuvent être utilisés dans n'importe quelle combinaison :

- Pour spécifier l'utilisation d'une application installée localement plutôt qu'une application disponible dans Citrix Receiver, ajoutez la chaîne de texte KEYWORDS:prefer="pattern". Cette fonctionnalité est appelée Local App Access.

  Avant d'installer une application sur l'ordinateur d'un utilisateur, Citrix Receiver recherche les modèles spécifiés pour déterminer si l'application est installée localement. Si c'est le cas, Citrix Receiver souscrit à l'application et ne crée pas de raccourci. Lorsque l'utilisateur démarre l'application à partir de la fenêtre de Citrix Receiver, Citrix Receiver démarre l'installation installée localement (préférée).

  Si un utilisateur désinstalle une application préférée en dehors de Citrix Receiver, l'abonnement à l'application est annulé lors de la prochaine actualisation de Citrix Receiver. Si un utilisateur désinstalle une application préférée à partir de Citrix Receiver, Citrix Receiver annule l'abonnement à l'application mais ne la désinstalle pas.

  Remarque : le mot-clé prefer est appliqué lorsque Citrix Receiver souscrit à une application. L'ajout du mot-clé après souscription à l'application n'a aucun effet.

  Vous pouvez spécifier le mot-clé prefer plusieurs fois pour une application. Il suffit d'une correspondance pour appliquer le mot-clé à une application. Les modèles suivants peuvent être utilisés dans n'importe quelle combinaison :

  - prefer="Nomapplication"

    Le modèle de nom d'application correspond à toute application dont le nom du fichier de raccourci contient le nom d'application spécifié. Le nom de l'application peut être un mot ou une phrase. Les phrases doivent être entourées de guillemets. Aucune correspondance n'est établie avec les mots partiels ou les chemins d'accès à des fichiers ; en outre, la correspondance n'est pas sensible à la casse. La possibilité de faire correspondre un nom d'application à un modèle est utile pour les substitutions réalisées manuellement par un administrateur.

KEYWORDS:prefer=	Raccourci sous Programmes	Correspondances ?
Word	\Microsoft Office\Microsoft **Word** 2010	Oui

KEYWORDS:prefer=	Raccourci sous Programmes	Correspondances ?
Microsoft Word	\Microsoft Office**Microsoft Word** 2010	Oui
Console	\McAfee\VirusScan **Console**	Oui
Virus	\McAfee\VirusScan Console	Non
McAfee	\McAfee\VirusScan Console	Non

- prefer="\\Dossier1\Dossier2\…\NomApplication"

  Le modèle de chemin d'accès absolu correspond au chemin d'accès du fichier de raccourci plus le nom d'application entier sous le menu Démarrer. Le dossier Programmes est un sous-dossier du répertoire du menu Démarrer, vous devez donc l'inclure au chemin d'accès absolu pour cibler une application dans ce dossier. Des guillemets sont requis si le chemin d'accès contient des espaces. La correspondance est sensible à la casse. Le modèle de correspondance à un chemin d'accès absolu est utile pour les substitutions implémentées via un programme dans XenDesktop.

KEYWORDS:prefer=	Raccourci sous Programmes	Correspondances ?
\Programs\Microsoft Office\Microsoft Word 2010	\Programs\Microsoft Office\Microsoft Word 2010	Oui
\Microsoft Office\	\Programs\Microsoft Office\Microsoft Word 2010	Non
\Microsoft Word 2010	\Programs\Microsoft Office\Microsoft Word 2010	Non
\Programs\Microsoft Word 2010	\Programs\Microsoft Word 2010	Oui

- prefer="\\Dossier1\Dossier2\…\NomApplication"

  Le modèle de chemin d'accès relatif correspond au chemin d'accès du fichier de raccourci relatif sous le menu Démarrer. Le chemin d'accès relatif doit contenir le nom de l'application et peut éventuellement inclure les dossiers dans lesquels le raccourci réside. Une correspondance est établie sur le chemin d'accès au fichier de raccourci se termine pas le chemin d'accès relatif fourni. Des guillemets sont requis si le chemin d'accès contient des espaces. La correspondance est sensible à la casse. Le modèle de correspondance à un chemin d'accès relatif est utile pour les substitutions implémentées

via un programme.

KEYWORDS:prefer=	Raccourci sous Programmes	Correspondances ?
\Microsoft Office\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Oui
\Microsoft Office\	\Microsoft Office\Microsoft Word 2010	Non
\Microsoft Word 2010	\Microsoft Office \Microsoft Word 2010	Oui
\Microsoft Word	\Microsoft Word 2010	Non

Pour de plus amples informations sur les autres mots-clés, reportez-vous à « Recommandations supplémentaires » dans la section Optimiser l'expérience utilisateur de la documentation de StoreFront.

Configuration de StoreFront

June 27, 2019

Citrix StoreFront authentifie une connexion sur XenDesktop, XenApp et VDI-in-a-Box, en énumérant et en regroupant les applications et bureaux disponibles dans des magasins auxquels vous pouvez accéder via Citrix Receiver pour Windows.

En plus de la configuration abordée dans cette section, vous devez également configurer NetScaler Gateway afin de permettre aux utilisateurs de se connecter en dehors du réseau interne (par exemple, les utilisateurs qui se connectent à partir d'Internet ou d'emplacements distants).

> **Conseil**
>
> Lorsque vous sélectionnez l'option permettant d'afficher tous les magasins, il est possible que l'ancienne interface utilisateur de StoreFront s'affiche.

Pour configurer StoreFront

Installez et configurez StoreFront comme décrit dans la documentation de StoreFront. Citrix Receiver pour Windows requiert une connexion HTTPS. Si le serveur StoreFront est configuré pour HTTP, une clé de registre doit être définie sur la machine utilisateur comme décrit dans la section Configuration et utilisation de Receiver pour Windows à l'aide de paramètres de ligne de commande sous la description de la propriété ALLOWADDSTORE.

> **Remarque :**
>
> 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 Citrix Receiver pour Windows.

Gérer la reconnexion au contrôle de l'espace de travail

Le contrôle de l'espace de travail permet aux applications de suivre les utilisateurs lorsqu'ils naviguent d'une machine à une autre. Ceci permet, par exemple, aux médecins hospitaliers de passer d'un poste de travail à un autre sans avoir à redémarrer leurs applications sur chaque machine. Pour Citrix Receiver pour Windows, vous gérez le contrôle de l'espace de travail sur les machines clientes en modifiant le registre. Pour les machines clientes appartenant au domaine, cela peut également se faire à l'aide d'une stratégie de groupe.

> **Attention**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Créez la clé **WSCReconnectModeUser** et modifiez la clé de registre existante WSCReconnectMode dans l'image de bureau principale ou dans l'hébergement du serveur XenApp. Le bureau publié peut changer le comportement de Citrix Receiver pour Windows.

Paramètres de clé WSCReconnectMode pour Citrix Receiver pour Windows :

- 0 = non reconnecté aux sessions existantes
- 1 = reconnecté lors du lancement des applications
- 2 = reconnecté lors de l'actualisation des applications
- 3 = reconnecté lors de l'actualisation ou du lancement des applications
- 4 = reconnecté lors de l'ouverture de l'interface Receiver
- 8 = reconnecté lors de l'ouverture de session Windows
- 11 = combinaison des paramètres 3 et 8

Désactiver le contrôle de l'espace de travail pour Citrix Receiver pour Windows

Pour désactiver le contrôle de l'espace de travail pour Citrix Receiver pour Windows, créez la clé suivante :

HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 bits)

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle for (32 bits)

Nom : **WSCReconnectModeUser**

Type : REG_SZ

Données de valeur : 0

Modifiez la valeur par défaut de la clé suivante de 3 à zéro

HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 bits)

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle (32 bits)

Nom : **WSCReconnectMode**

Type : REG_SZ

Données de valeur : 0

> **Remarque**
>
> Vous pouvez également définir la valeur REG_SZ WSCReconnectAll sur false si vous ne voulez pas créer de nouvelle clé.

Modification du délai de l'indicateur d'état

Vous pouvez modifier la durée pendant laquelle l'indicateur d'état s'affiche lorsqu'un utilisateur lance une session. Pour modifier cette durée, créez une valeur REG_DWORD de SI INACTIVE MS dans HKLM\SOFTWARE\Citrix\ICA CLIENT\Engine\. La valeur REG_DWORD peut être réglée sur 4 si vous voulez que l'indicateur d'état disparaisse plus tôt.

> **Avertissement**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Personnalisation de l'emplacement du raccourci d'application depuis l'interface de ligne de commande

L'intégration du menu Démarrer et le mode de raccourci sur le bureau uniquement vous permettent d'afficher les raccourcis d'applications publiées dans le menu Démarrer de Windows et sur le bureau. Les utilisateurs n'ont pas à s'abonner à des applications à partir de l'interface utilisateur de Citrix Receiver. L'intégration du menu Démarrer et la gestion des raccourcis du bureau offrent une expérience de bureau transparente pour les groupes d'utilisateurs qui ont besoin d'accéder à un ensemble d'applications principales de manière cohérente.

En tant qu'administrateur Citrix Receiver, vous pouvez utiliser des indicateurs d'installation de ligne de commande, des objets de stratégie de groupe, des services de comptes ou des paramètres de registre pour désactiver l'interface Citrix Receiver en « libre-service » et la remplacer par un menu Démarrer préconfiguré. L'indicateur, nommé appelé SelfServiceMode, est défini sur true par défaut. Lorsque l'administrateur définit l'indicateur SelfServiceMode sur false, l'utilisateur n'a plus accès à l'interface utilisateur Citrix Receiver en libre-service. Au lieu de cela, ils peuvent accéder aux applications souscrites dans le menu Démarrer et via des raccourcis de bureau, référencés ici en tant que mode Raccourci uniquement.

Les utilisateurs et les administrateurs peuvent utiliser un certain nombre de paramètres de registre pour personnaliser la manière dont les raccourcis sont définis.

Utilisation des raccourcis

- Les utilisateurs ne peuvent pas supprimer les applications. Toutes les applications sont obligatoires lorsque vous utilisez l'indicateur SelfServiceMode défini sur false (mode Raccourci uniquement). Si l'utilisateur supprime une icône de raccourci depuis le bureau, l'icône revient lorsque l'utilisateur sélectionne Actualiser depuis l'icône Citrix Receiver pour Windows de la barre d'état système.
- Les utilisateurs ne peuvent configurer qu'un seul magasin. Les options Compte et Préférences ne sont pas disponibles. Ceci permet d'empêcher l'utilisateur de configurer d'autres magasins. L'administrateur peut accorder des privilèges spéciaux à un utilisateur pour ajouter plusieurs comptes à l'aide du modèle d'objet de stratégie de groupe, ou en ajoutant manuellement une clé de Registre (HideEditStoresDialog) sur la machine cliente. Lorsque l'administrateur accorde ce privilège à un utilisateur, l'utilisateur possède une option Préférences dans l'icône de la barre d'état système, où il peut ajouter et supprimer des comptes.
- Les utilisateurs ne peuvent pas supprimer les applications via le Panneau de configuration de Windows.
- Vous pouvez ajouter des raccourcis de bureau via un paramètre de registre personnalisable. Les raccourcis de bureau ne sont pas ajoutés par défaut. Si vous apportez des modifications aux paramètres de registre, Citrix Receiver pour Windows doit être redémarré.
- Les raccourcis sont créés dans le menu Démarrer avec un chemin d'accès de catégorie comme valeur par défaut, UseCategoryAsStartMenuPath.

> **Remarque**
>
> Windows 8/8.1 n'autorise pas la création de dossiers imbriqués dans le menu Démarrer. Les applications seront affichées séparément ou sous le dossier racine mais pas dans les sous-dossiers de catégorie définis avec XenApp.

- Vous pouvez ajouter un indicateur [/DESKTOPDIR=« Nom_Répertoire »] lors de l'installation

pour rassembler tous les raccourcis dans un dossier unique. CategoryPath est pris en charge pour les raccourcis de bureau.

- Auto Re-install Modified Apps est une fonctionnalité qui peut être activée via la clé de Registre AutoReInstallModifiedApps. Lorsque AutoReInstallModifiedApps est activée, toute modification apportée aux attributs des applications et bureaux publiés sur le serveur sont répercutées sur la machine cliente. Lorsque AutoReInstallModifiedApps est désactivée, les attributs d'applications et de bureaux ne sont pas mis à jour et les raccourcis ne sont pas stockés à nouveau lors de l'actualisation s'ils ont été supprimés sur le client. Par défaut, AutoReInstallModifiedApps est activée. Consultez la section Utilisation des clés de registre pour personnaliser l'emplacement des raccourcis d'applications.

Personnalisation de l'emplacement du raccourci d'application via le registre

> **Remarque**
>
> Les clés de registre utilisent par défaut le format de chaîne.

Nous vous recommandons d'apporter des modifications aux clés de registre avant de configurer un magasin. Si à tout moment, vous ou un utilisateur souhaitez personnaliser les clés de Registre, vous ou l'utilisateur devez réinitialiser Receiver, configurer les clés de registre, puis reconfigurer le magasin.

Clés de registre pour machines 32 bits

Clés de registre pour machines 64 bits

Configuration des options de raccourcis et de reconnexion via l'interface utilisateur graphique

> **Remarque**
>
> Les raccourcis ne peuvent être définis que pour les applications et bureaux auxquels les utilisateurs sont abonnés.
>
> Vous pouvez masquer tout ou partie de la page **Préférences avancées** disponible à partir de l'icône Citrix Receiver dans la zone de notification. Pour plus d'informations, veuillez consulter Masquer la page Préférences avancées.

1. Connectez-vous à Citrix Receiver pour Windows.
2. Cliquez avec le bouton droit sur l'icône de Citrix Receiver pour Windows dans la zone de notification et cliquez sur **Préférences avancées**.
   La fenêtre Préférences avancées s'affiche.
3. Cliquez sur **Option Paramètres**.

> **Remarque**
>
> Par défaut, l'option **Afficher applications dans le menu Démarrer** est sélectionnée.

4. Spécifiez le nom du dossier. Ceci déplace toutes les applications auxquelles vous avez souscrit dans le dossier spécifié dans le menu Démarrer. Des applications peuvent être ajoutées à un nouveau dossier ou à un dossier existant dans le menu Démarrer. Lors de l'activation de cette fonctionnalité, les applications existantes et celles nouvellement ajoutées sont ajoutées au dossier spécifié.
5. Sélectionnez la case à cocher **Afficher applications sur le bureau** sous le panneau **Options de bureau**.
6. Spécifiez le nom du dossier. Ceci déplace toutes les applications auxquelles vous avez souscrit dans le dossier spécifié de votre bureau local.
7. Sélectionnez la case à cocher **Activer chemin d'accès différent pour le Menu Démarrer et le bureau** sous **Options de catégorie**. Ceci crée le dossier des raccourcis et de catégorie pour les applications tel que défini dans le serveur des propriétés de l'application. Par ex., Applis IT, Applis Finance

   > **Remarque**
   >
   > L'option **Catégorie : chemin du menu Démarrer** est sélectionnée par défaut.

   i. Sélectionnez **Catégorie : chemin du menu Démarrer** pour afficher les applications auxquelles vous avez souscrit et leur dossier de catégorie tel que défini dans le serveur des propriétés de l'application dans le menu Démarrer de Windows.

   ii. Sélectionnez **Catégorie : chemin du bureau** pour afficher les applications auxquelles vous avez souscrit et leur dossier de catégorie tel que défini dans le serveur des propriétés de l'application sur votre bureau local.
8. Cliquez sur **OK**.

Configuration des options de reconnexion via l'interface utilisateur graphique

> **Remarque**
>
> Vous pouvez masquer tout ou partie de la page Préférences avancées disponible à partir de l'icône Citrix Receiver dans la zone de notification. Pour plus d'informations, veuillez consulter Masquer la page Préférences avancées.

Après avoir ouvert une session sur le serveur, les utilisateurs peuvent se reconnecter à tous leurs bureaux ou applications à tout moment. Par défaut, l'option Options de reconnexion ouvre les applications et bureaux qui sont déconnectés ainsi que ceux actuellement exécutés sur une autre machine

cliente. Vous pouvez configurer cette option de façon à ce qu'elle ne reconnecte que les applications ou bureaux précédemment déconnectés par l'utilisateur.

1. Connectez-vous à Citrix Receiver pour Windows.
2. Cliquez avec le bouton droit sur l'icône de Citrix Receiver pour Windows dans la barre d'état système et cliquez sur **Préférences avancées**.
   La fenêtre Préférences avancées s'affiche.
3. Cliquez sur **Option Paramètres**.
4. Cliquez sur **Options de reconnexion**.
5. Sélectionnez **Activer pour la prise en charge du contrôle de l'espace de travail** pour permettre aux utilisateurs de se reconnecter à tous leurs bureaux ou applications à tout moment.
   a) Sélectionnez **Se reconnecter à toutes les sessions actives et déconnectées** de manière à autoriser les utilisateurs à se reconnecter aux sessions déconnectées et actives.
   b) Sélectionnez **Se reconnecter uniquement aux sessions déconnectées** de manière à autoriser les utilisateurs à se reconnecter uniquement aux sessions déconnectées.

   > Remarque :
   >
   > L'option **Mode de reconnexion pris en charge** est réglée sur la valeur définie dans l'objet de stratégie de groupe. Les utilisateurs peuvent modifier cette option en accédant à **Modèles d'administration** > **Composants Citrix** > **Citrix Receiver** > **Self-Service** > **Contrôler quand Receiver tente de se reconnecter aux sessions existantes**.

   Pour modifier cette option via le registre, consultez l'article CTX136339 du centre de connaissances.
6. Cliquez sur **OK**.

Configuration des fonctionnalités

June 27, 2019

Après l'installation de Citrix Receiver pour Windows, les étapes de configuration suivantes permettent aux utilisateurs d'accéder à leurs applications et bureaux hébergés :

- Transport adaptatif : le transport adaptatif optimise le transport de données à l'aide d'un nouveau protocole Citrix nommé Enlightened Data Transport (EDT) qui remplace de TCP lorsque c'est possible. Pour plus d'informations sur la configuration du transport adaptatif, consultez la section Configuration du transport adaptatif.

- Mises à jour de Receiver : la fonctionnalité Mises à jour de Receiver fournit des mises à jour automatiques de Citrix Receiver pour Windows et du Pack d'optimisation HDX RealTime sans avoir besoin de télécharger les mises à jour manuellement. Pour plus d'informations sur la configuration de la fonctionnalité Mises à jour de Receiver, consultez la section Configuration des mises à jour de Receiver.
- Redirection bidirectionnelle du contenu : la redirection bidirectionnelle du contenu permet d'activer ou de désactiver la redirection d'adresse URL du client vers l'hôte et de l'hôte vers le client. Pour plus d'informations sur la configuration de la redirection de contenu bidirectionnelle, reportez-vous à la section Configuration de la redirection bidirectionnelle du contenu.
- Claviers Bloomberg : les périphériques USB spécialisés (par exemple, claviers Bloomberg et souris 3D) peuvent être configurés pour utiliser la prise en charge USB. Pour plus d'informations sur la configuration des claviers Bloomberg, consultez la sectionConfiguration des claviers Bloomberg.
- Périphérique USB composite : un périphérique USB composite exécute plusieurs fonctions. Chacune de ces fonctions est présentée dans une interface différente. Pour plus d'informations sur la configuration d'un périphérique USB composite, reportez-vous à la section Configuration d'un périphérique USB composite.
- Prise en charge USB : la prise en charge USB permet aux utilisateurs d'interagir avec une large gamme de périphériques USB connectés au bureau virtuel. Pour plus d'informations sur la configuration de la prise en charge USB, consultez la section Configuration de la prise en charge USB.

Configuration du transport adaptatif

June 27, 2019

Dans les versions précédentes, lorsque HDXoverUDP est défini sur **Préféré**, le transport de données via EDT est utilisé lorsque c'est possible, avec retour vers TCP.

À partir de la version 4.10 et avec la fiabilité de session activée, EDT et TCP sont tentés en parallèle lors de la connexion initiale, de la reconnexion à la fiabilité de session et de la reconnexion automatique des clients. Cette amélioration réduit le temps de connexion lorsque EDT est le protocole préféré, mais le transport UDP sous-jacent requis est indisponible et TCP doit être utilisé.

Par défaut, après le repli vers TCP, le transport adaptatif continue d'interroger EDT toutes les 5 minutes.

Exigences

- XenApp et XenDesktop 7.12 et version ultérieure (requis pour activer la fonctionnalité à l'aide de Studio).
- StoreFront 3.8.
- VDA IPv4 uniquement. Les configurations IPv6 et IPv4/IPv6 ne sont pas prises en charge.
- Ajoutez des règles de pare-feu pour autoriser le trafic entrant sur les ports UDP 1494 et 2598 du VDA.

> **Remarque**
>
> Les ports TCP 1494 et 2598 sont également requis et sont ouverts automatiquement lorsque vous installez le VDA. Toutefois, les ports UDP 1494 et 2598 ne sont pas ouverts automatiquement. Vous devez les activer.

Le transport adaptatif doit être configuré sur le VDA en appliquant la stratégie avant qu'il ne soit disponible pour les communications entre le VDA et Citrix Receiver.

Par défaut, le transport adaptatif est autorisé dans Citrix Receiver pour Windows. Toutefois, et ceci également par défaut, le client tente d'utiliser le transport adaptatif uniquement si le VDA est configuré sur **Préféré** dans la stratégie Citrix Studio et si le paramètre a été appliqué sur le VDA.

Vous pouvez activer le transport adaptatif à l'aide du paramètre de stratégie **HDX Adaptive Transport**. Définissez la nouvelle stratégie sur **Préféré** pour utiliser le transport adaptatif lorsque cela est possible, avec basculement sur TCP.

Pour désactiver le transport adaptatif sur un client spécifique, définissez les options EDT appropriées à l'aide du modèle d'administration de l'objet de stratégie de groupe Citrix Receiver.

Pour configurer l'utilisation du transport adaptatif à l'aide du modèle d'administration de l'objet de stratégie de groupe Citrix Receiver

Les étapes de configuration suivantes de personnalisation de votre environnement sont facultatives. Par exemple, vous pouvez choisir de désactiver la fonctionnalité pour un client particulier pour des raisons de sécurité.

> **Remarque**
>
> Par défaut, le transport adaptatif est défini sur Désactivé et TCP est toujours utilisé.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud Configuration ordinateur, accédez à **Modèles d'administration** > **Citrix Receiver** > **Routage réseau**.
3. Définissez la stratégie **Protocole de transport pour Receiver** sur **Activé**.

4. Sélectionnez le **protocole de communication pour Citrix Receiver** en fonction de vos besoins.
    - **Désactivé** : indique que le protocole TCP est utilisé pour le transfert de données.
    - **Préféré** : indique que Citrix Receiver tente d'abord de se connecter au serveur via UDP et bascule sur TCP si la connexion via UDP échoue.
    - **Activé** : indique que Citrix Receiver se connecte au serveur uniquement via le protocole UDP. Il n'existe pas de solution de secours vers TCP avec cette option.
5. Cliquez sur **Appliquer**, puis sur **OK**.
6. Exécutez la commande `gpupdate /force` à partir d'une ligne de commande.

Par ailleurs, pour que la configuration du transport adaptatif soit prise en compte, l'utilisateur doit ajouter les fichiers de modèle de Citrix Receiver pour Windows au dossier Définitions de stratégie. Pour plus d'informations sur l'ajout des fichiers de modèle admx/adml à l'objet de stratégie de groupe local, consultez la section Configuration de Citrix Receiver pour Windows avec le modèle d'objet de stratégie de groupe.

Pour confirmer que le paramètre de stratégie est appliqué :

Accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT et vérifiez que la clé **HDXOverUDP** est incluse.

Configuration de la prise en charge USB

March 26, 2019

La prise en charge USB vous permet d'interagir avec une large gamme de périphériques USB connectés au bureau virtuel. Vous pouvez brancher des périphériques USB à vos ordinateurs ; ils sont envoyés vers vos bureaux virtuels. Les périphériques USB suivants sont pris en charge : lecteurs flash, smartphones, ordinateurs de poche, imprimantes, scanners, lecteurs MP3, périphériques de sécurité et tablettes. Les utilisateurs Desktop Viewer peuvent spécifier si les périphériques USB sont disponibles sur le bureau virtuel à l'aide d'une préférence dans la barre d'outils.

Les fonctionnalités isochrones des périphériques USB tels que les webcams, les micros, les haut-parleurs et les micro-casques sont prises en charge dans des environnements LAN (réseaux locaux) à faible latence et à haut débit. Cela permet à ces périphériques d'interagir avec des packs tels que Microsoft Office Communicator et Skype.

Les types de périphériques suivants sont pris en charge directement dans une session XenApp et XenDesktop ; ils n'utilisent donc pas la prise en charge USB :

- Claviers
- Souris
- Cartes à puce

> **Remarque**
>
> Les périphériques USB spécialisés (par exemple, claviers et souris 3D Bloomberg) peuvent être configurés pour utiliser la prise en charge USB. Pour plus d'informations sur la configuration des claviers Bloomberg, consultez la section Configuration des claviers Bloomberg. Pour plus d'informations sur la configuration des règles de stratégie pour d'autres périphériques USB spécialisés, consultez l'article CTX122615 du Centre de connaissances.

Par défaut, certains types de périphériques USB ne sont pas pris en charge pour l'accès distant via XenDesktop et XenApp. Par exemple, une carte d'interface réseau peut être reliée à la carte système par une connexion USB interne. Il n'est pas conseillé de configurer un accès distant pour ce périphérique. Par défaut, les types de périphériques USB suivants ne sont pas pris en charge pour une utilisation dans une session XenDesktop :

- Dongles Bluetooth
- Cartes d'interface réseau intégrées
- Concentrateurs USB
- Adaptateurs graphiques USB

Les périphériques USB connectés à un concentrateur peuvent être gérés à distance, mais pas le concentrateur.

Par défaut, les types de périphériques USB suivants ne sont pas pris en charge pour une utilisation dans une session XenApp :

- Dongles Bluetooth
- Cartes d'interface réseau intégrées
- Concentrateurs USB
- Adaptateurs graphiques USB
- Périphériques audio
- Périphériques de stockage de masse

Pour obtenir des instructions sur la modification de la liste des périphériques USB disponibles pour les utilisateurs, consultez la section Mise à jour de la liste des périphériques USB disponibles pour l'accès à distance.

Pour obtenir des instructions sur la redirection automatique de périphériques USB spécifiques, consultez l'article CTX123015 du centre de connaissances.

Fonctionnement de la prise en charge USB

Lorsqu'un utilisateur branche un périphérique USB, ce dernier est comparé à la stratégie USB, et s'il est autorisé, il est envoyé sur le bureau virtuel. Si la stratégie par défaut refuse le périphérique, il n'est disponible que sur le bureau local.

Lorsqu'un utilisateur branche un périphérique USB, une notification s'affiche pour informer l'utilisateur qu'un nouveau périphérique est apparu. L'utilisateur peut choisir les périphériques USB à envoyer sur le bureau virtuel en les sélectionnant dans la liste chaque fois qu'il se connecte. L'utilisateur peut également configurer la prise en charge USB de manière à ce que tous les périphériques USB connectés avant et/ou pendant une session soient automatiquement envoyés au bureau virtuel qui a le focus.

Périphériques de stockage de masse

Pour les périphériques de stockage de masse uniquement, en plus de la prise en charge USB, l'accès à distance est disponible via le mappage des lecteurs clients, que vous configurez par le biais de la stratégie Citrix Receiver Remoting client devices > Client drive mapping. Lorsque cette stratégie est appliquée, les lecteurs de la machine utilisateur sont automatiquement mappés vers les lettres de lecteur sur le bureau virtuel lorsque les utilisateurs ouvrent une session. Les lecteurs sont affichés sous la forme de dossiers partagés associés à des lettres de lecteur mappé.

Les différences principales entre les deux types de stratégie à distance sont les suivantes :

Fonctionnalité	Mappage des lecteurs clients	Prise en charge USB
Activée par défaut	Oui	Non
Accès en lecture seule configurable	Oui	Non
Le périphérique peut être retiré en toute sécurité au cours d'une session	Non	Oui, si un utilisateur clique sur Retirer le périphérique en toute sécurité dans la zone de notification.

Si USB générique et les stratégies de mappage des lecteurs clients sont tous deux activés et qu'un périphérique de stockage de masse est inséré avant le démarrage d'une session, il sera tout d'abord redirigé à l'aide du mappage des lecteurs clients, avant d'être considéré pour la redirection via la prise en charge USB. S'il est inséré après le démarrage d'une session, il sera considéré pour la redirection à l'aide de la prise en charge USB avant le mappage des lecteurs clients.

Classes de périphériques USB autorisées par défaut

Différentes classes de périphériques USB sont autorisées par les règles de stratégie USB par défaut.

Bien qu'elles figurent sur cette liste, certaines classes ne peuvent être gérées à distance que dans les sessions XenDesktop et XenApp après une configuration supplémentaire. Elles sont indiquées ci-

dessous.

- **Audio (Classe 01)**. Comprend des périphériques d'entrée audio (micros), des périphériques de sortie audio et des contrôleurs MIDI. Les périphériques audio modernes utilisent généralement les transferts isochrones, qui sont pris en charge par XenDesktop 4 ou version ultérieure. Audio (Class01) n'est pas applicable pour XenApp car ces périphériques ne sont pas disponibles pour l'accès à distance dans XenApp à l'aide de la prise en charge USB.

> **Remarque**
>
> Certains périphériques spécialisés (par exemple les téléphones VOIP) requièrent une configuration supplémentaire. Pour plus d'informations, consultez l'article CTX123015 du centre de connaissances.

- **Périphériques d'interface physique (Classe 05)**. Ces périphériques sont similaires aux périphériques d'interface utilisateur (HID), mais ils fournissent en général des données en temps-réel et comprennent des joysticks de retour de force, des plates-formes mouvantes et des exosquelettes de retour de force.
- **Acquisition d'images fixes (Classe 06)**. Comprend scanners et appareils photo numériques. Les appareils photo numériques prennent généralement en charge la classe d'acquisition d'images fixes qui utilise le protocole PTP (Picture Transfer Protocol) ou MTP (Media Transfer Protocol) pour transférer des images sur un ordinateur ou un autre périphérique. Les appareils photo peuvent également apparaître comme périphériques de stockage de masse et il est possible de configurer un appareil photo pour utiliser les deux classes, par le biais des menus fournis par l'appareil photo.

> **Remarque**
>
> Si un appareil photo apparaît en tant que périphérique de stockage de masse, le mappage des lecteurs clients est utilisé et la prise en charge USB n'est pas requise.

- **Imprimantes (Classe 07)**. En général, la plupart des imprimantes appartiennent à cette classe, à l'exception de certaines qui utilisent des protocoles spécifiques au fabricant (classe ff). Les imprimantes multifonctions peuvent disposer d'un concentrateur interne ou être des périphériques composites. Dans les deux cas, l'élément d'impression utilise généralement la classe Imprimantes et l'élément de fax ou de numérisation utilise une autre classe ; par exemple, acquisition d'images fixes.

  Les imprimantes fonctionnent correctement sans prise en charge USB.

> **Remarque**
>
> Cette classe de périphérique (en particulier les imprimantes équipées de fonctions de numérisation) requiert une configuration supplémentaire. Pour obtenir des instructions, consultez l'article CTX123015 du centre de connaissances.

- **Stockage de masse (Classe 08)**. Les périphériques de stockage de masse les plus courants sont les lecteurs flash USB ; les disques dur USB, lecteurs CD/DVD et lecteurs de cartes SD/MMC sont également des périphériques de stockage de masse. Les périphériques avec stockage interne dotés d'une interface de stockage de masse sont également nombreux ; sont compris dans cette catégorie les lecteurs multimédias, les appareils photos numériques et les téléphones portables. Le stockage de masse (Classe 08) n'est pas applicable pour XenApp car ces périphériques ne sont pas disponibles pour l'accès à distance dans XenApp à l'aide de la prise en charge USB. Sous-classes connues :
  - 01 Périphériques flash limités
  - 02 Lecteurs de CD/DVD (ATAPI/MMC-2)
  - 03 Lecteurs de bandes (QIC-157)
  - 04 Lecteurs de disquettes (UFI)
  - 05 Lecteurs de disquettes (SFF-8070i)
  - 06 La plupart des périphériques de stockage de masse utilisent cette variante de SCSI.

  Étant donné que le mappage des lecteurs clients peut être utilisé pour accéder à la plupart des périphériques au travers du mappage de lecteur client, la prise en charge USB n'est pas requise.

> **Important**
>
> Certains virus sont connus pour se propager activement à l'aide de tous les types de stockage de masse. Posez-vous la question de savoir si les besoins de votre entreprise justifient l'utilisation de périphériques de stockage de masse, soit via le mappage de lecteurs clients, soit via la prise en charge USB.

- **Sécurité du contenu (Classe 0d)**. Les périphériques de sécurité du contenu assurent la protection du contenu, en général pour la gestion des licences ou des droits numériques. Cette classe comprend les dongles.
- **Vidéo (Classe 0e)**. La classe vidéo couvre les périphériques utilisés pour manipuler les vidéos, tels que les webcams, les caméscopes numériques, les convertisseurs vidéo analogique, certains tuner TV et certains appareils photo numériques qui prennent en charge le streaming vidéo.

> **Important**
>
> La plupart des périphériques de streaming vidéo utilisent les transferts isochrones, qui sont pris en charge par XenDesktop 4 ou version ultérieure. Certains périphériques vidéo (par exemple les webcams équipées de fonctions de détection des mouvements) requièrent une configuration supplémentaire. Pour obtenir des instructions, consultez l'article CTX123015 du centre de connaissances.

- **Santé personnelle (Classe 0f)**. Ces appareils comprennent des capteurs de pression artérielle, des moniteurs de pouls, des podomètres, des piluliers et des spiromètres.

- **Spécifique au fabricant et à l'application (Classes fe et ff)**. De nombreux périphériques utilisent des protocoles spécifiques au fabricant ou des protocoles qui n'ont pas été adoptés par le consortium USB, et ces derniers apparaissent en général en tant que spécifique au fabricant (classe ff).

Classes de périphériques USB refusées par défaut

Les différentes classes de périphériques USB suivantes sont refusées par les règles de stratégie USB par défaut.

- Communications et contrôle CDC (Classes 02 et 0a). La stratégie USB par défaut n'autorise pas ces périphériques, car l'un d'entre eux peut fournir la connexion au bureau virtuel lui-même.
- Périphériques d'interface utilisateur (Classe 03). Comprend un large éventail de périphériques d'entrée et de sortie. Les périphériques d'interface utilisateur (HID) sont composés de claviers, souris, dispositifs de pointage, tablettes graphiques, capteurs, contrôleurs de jeu, boutons et fonctions de contrôle.

  La sous-classe 01 est appelée classe « interface de démarrage » ; elle est utilisée pour les claviers et les souris.

  La stratégie USB par défaut n'autorise ni les claviers USB (classe 03, sous-classe 01, protocole 1), ni les souris USB (classe 03, sous-classe 01, protocole 2). Ceci est dû au fait que la majorité des claviers et souris sont correctement gérés sans prise en charge USB et il est normalement nécessaire d'utiliser ces périphériques localement ainsi qu'à distance lors de la connexion à un bureau virtuel.
- Concentrateurs USB (Classe 09). Les concentrateurs USB permettent de connecter des périphériques supplémentaires à l'ordinateur local. Il n'est pas nécessaire d'accéder à ces périphériques à distance.
- Carte à puce (Classe 0b). Les lecteurs de carte à puce comprennent des lecteurs de carte à puce avec ou sans contact, ainsi que des jetons USB dotés d'une puce équivalente à une carte à puce.

  L'accès distant par carte à puce est utilisé pour accéder aux lecteurs de carte à puce et la prise en charge USB n'est pas nécessaire.
- Contrôleur sans fil (Classe e0). Certains de ces appareils peuvent fournir un accès réseau critique ou connecter des périphériques critiques tels que des claviers ou des souris Bluetooth.

  La stratégie USB par défaut n'autorise pas ces appareils. Toutefois, il peut être utile pour certains appareils de fournir l'accès à l'aide de la prise en charge USB.
- **Divers périphériques réseau (classe ef, sous-classe 04)**. Certains de ces appareils peuvent fournir un accès réseau critique. La stratégie USB par défaut n'autorise pas ces appareils. Toutefois, il peut être utile pour certains appareils de fournir l'accès à l'aide de la prise en charge USB.

Mise à jour de la liste des périphériques USB disponibles pour l'accès à distance

Vous pouvez mettre à jour la liste des périphériques USB disponibles pour l'envoi vers des bureaux en modifiant le fichier de modèle Citrix Receiver pour Windows. Cela vous permet d'apporter des modifications à Citrix Receiver pour Windows via une stratégie de groupe. Le fichier se trouve dans le dossier suivant :

<lecteur racine>:\Program Files\Citrix\ICA Client\Configuration\en

Vous pouvez également modifier le registre sur chaque machine utilisateur en ajoutant la clé de registre suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Name="DeviceRules" Value=

Avertissement : toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Les règles par défaut du produit sont stockées dans :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB Type=MultiSz Name="DeviceRules" Value=

Ne modifiez pas les règles par défaut du produit.

Pour obtenir des informations sur les règles et leur syntaxe, consultez l'article CTX119722 du centre de connaissances.

Configuration de l'audio USB

> **Remarque**
>
> - Lorsque vous mettez à niveau ou installez Citrix Receiver pour Windows pour la première fois, vous devez ajouter les derniers fichiers de modèle à l'objet de stratégie de groupe local. Pour plus d'informations sur l'ajout des fichiers de modèle à l'objet de stratégie de groupe local, consultez la section Configuration du modèle d'administration d'objet de stratégie de groupe. En cas de mise à niveau, les paramètres existants sont conservés lors de l'importation des derniers fichiers.
> - Cette fonctionnalité est disponible uniquement sur un serveur XenApp.

Pour configurer des périphériques audio USB

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.

2. Sous le nœud Configuration ordinateur, accédez à **Modèles d'administration** > **Modèles d'administration classiques (ADM)** > **Composants Citrix** > **Citrix Receiver** > **Expérience utilisateur** et sélectionnez **Audio via la redirection USB générique**.
3. Modifiez les paramètres.
4. Cliquez sur **Appliquer**, puis sur **OK**.
5. Ouvrez l'invite de commande en mode administrateur.
6. Exécutez la commande suivante :
   `gpupdate /force`.

Configuration de la redirection de périphérique USB composite

November 16, 2018

Configuration de la redirection USB composite à l'aide du modèle d'administration d'objet de stratégie de groupe

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud Configuration utilisateur, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Receiver** > **Accès à distance des périphériques clients** > **Utilisation à distance de dispositifs USB génériques**.
3. Sélectionnez la stratégie **SplitDevices**.
4. Sélectionnez **Activé**.
5. Cliquez sur **Appliquer**.
6. Cliquez sur **OK** pour enregistrer la stratégie.

Pour autoriser ou interdire une interface à l'aide du modèle d'administration d'objet de stratégie de groupe

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud Configuration utilisateur, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Receiver** > **Accès à distance des périphériques clients** > **Utilisation à distance de dispositifs USB génériques**.
3. Sélectionnez la stratégie **Règles de périphériques USB**.
4. Sélectionnez **Activé**.
5. Dans la zone de texte **Règles de périphériques USB**, ajoutez le périphérique USB que vous souhaitez autoriser ou interdire.

Par exemple, *ALLOW: vid=047F pid= C039 split=01 intf=00,03 //Interfaces 00 et 03 autorisées, autres non autorisées.*

6. Cliquez sur **Appliquer**, puis sur **OK**.

Dans une session de bureau, les périphériques USB divisés sont affichés dans Desktop Viewer sous **Périphériques**. En outre, vous pouvez afficher les périphériques USB divisés dans **Préférences** > **Périphériques**.

Dans une session d'application, les périphériques USB divisés sont affichés dans le **Centre de connexion**.

Le tableau ci-dessous fournit des informations sur les scénarios de comportement lorsqu'une interface USB est autorisée ou interdite.

Pour autoriser une interface :

Divisé	Interface	Action
VRAI	Numéro valide 0 -n	Autorise l'interface spécifiée
VRAI	Numéro non valide	Autorise toutes les interfaces
FAUX	Toute valeur	Autorise USB générique du périphérique parent
Non spécifié	Toute valeur	Autorise USB générique du périphérique parent

Par exemple, SplitDevices- *true* indique que tous les périphériques sont divisés.

Pour interdire une interface :

Divisé	Interface	Action
VRAI	Numéro valide 0 -n	Interdit l'interface spécifiée
VRAI	Numéro non valide	Interdit toutes les interfaces
FAUX	Toute valeur	Interdit USB générique du périphérique parent
Non spécifié	Toute valeur	Interdit USB générique du périphérique parent

Par exemple, SplitDevices- *false* indique que les périphériques avec le numéro d'interface spécifié ne sont pas divisés.

Exemple : My_<*plantronics*> headset

Numéro d'interface

- Classe d'interface audio -0
- Classe d'interface HID -3

Exemples de règles utilisées pour My_<*plantronics*> headset :

- ALLOW: vid=047F pid= C039 split=01 intf=00,03 //Interfaces 00 et 03 autorisées, autres non autorisées
- DENY: vid=047F pid= C039 split=01 intf=00,03 // Interdire 00 et 03

Limitation :

Citrix recommande de ne pas diviser les interfaces pour une webcam. Pour contourner ce problème, redirigez le périphérique vers un périphérique unique en utilisant la redirection USB générique. Pour de meilleures performances, utilisez le canal virtuel optimisé.

Masquer la page Préférences avancées

November 16, 2018

À partir de la version 4.10, vous pouvez personnaliser la disponibilité et le contenu de la page **Préférences avancées** présente dans le menu contextuel de l'icône Citrix Receiver dans la zone de notification. Cela garantit que les utilisateurs peuvent appliquer uniquement des paramètres spécifiés par l'administrateur sur leurs systèmes. Plus spécifiquement, ils peuvent :

- Masquer entièrement la page Préférences avancées
- Masquer les paramètres spécifiques suivants sur la page :
  - Collecte des données
  - Centre de connexion
  - Outil d'analyse de la configuration
  - Clavier et barre de langue
  - DPI élevé
  - Informations de support
  - Raccourcis et reconnexion

Masquer l'option Préférences avancées dans le menu contextuel

Vous pouvez masquer la page Préférences avancées à l'aide du modèle d'administration d'objet de stratégie de groupe Citrix Receiver :

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.

2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Citrix Receiver** > **Libre-service** > **Options Préférences avancées**.
3. Sélectionnez la stratégie **Désactiver Préférences avancées**.
4. Sélectionnez **Activé** pour masquer l'option Préférences avancées dans le menu contextuel de l'icône de Citrix Receiver dans la zone de notification.

> **Remarque**
>
> L'option **Non configuré** est sélectionnée par défaut.

Masquer des paramètres spécifiques sur la page Paramètres avancés

Vous pouvez masquer des paramètres spécifiques à l'utilisateur sur la page Préférences avancées à l'aide du modèle d'administration d'objet de stratégie de groupe Citrix Receiver. Pour ce faire, procédez comme suit :

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Citrix Receiver** > **Libre-service** > **Options Préférences avancées**.
3. Sélectionnez la stratégie pour le paramètre que vous souhaitez masquer.

Masquer les paramètres spécifiques suivants sur la page :

- Outil d'analyse de la configuration
- Centre de connexion
- DPI élevé
- Collecte des données
- Supprimer les mots de passe enregistrés
- Clavier et barre de langue
- Raccourcis et reconnexion
- Informations de support

Le tableau ci-dessous répertorie les options que vous pouvez sélectionner et l'effet de chacune :

Options	Action
Non configuré	Affiche le paramètre
Activée	Masque le paramètre
Désactivée	Affiche le paramètre

Masquer l'option Réinitialiser Receiver sur la page Préférences avancées à l'aide de l'Éditeur du Registre

Vous pouvez masquer l'option **Réinitialiser Receiver** sur la page Préférences avancées uniquement à l'aide de l'Éditeur du Registre.

1. Lancer l'Éditeur du registre
2. Accédez à **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle**.
3. Créez une nouvelle clé avec la valeur de chaîne **EnableFactoryReset** et définissez-la sur une des options suivantes :
   a) True - affiche l'option Réinitialiser Receiver dans la page Préférences avancées
   b) False - masque l'option Réinitialiser Receiver dans la page Préférences avancées

Masquer l'option Mises à jour de Receiver sur la page Préférences avancées

Remarque : le chemin d'accès à la stratégie pour l'option Mises à jour de Receiver est différent de celui des autres options présentes dans la page Préférences avancées.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Receiver** > **Mises à jour de Receiver**.
3. Sélectionnez la règle **Mises à jour de Receiver**.
4. Sélectionnez **Désactivé** pour masquer les paramètres de mises à jour de Receiver de la page Préférences avancées.

Configuration des claviers Bloomberg

November 16, 2018

Citrix Receiver pour Windows prend en charge l'utilisation du clavier Bloomberg dans une session XenApp et XenDesktop. Les composants requis sont installés avec le plug-in. Vous pouvez activer la fonctionnalité de clavier Bloomberg lors de l'installation de Citrix Receiver pour Windows ou à l'aide du Registre.

Il n'est pas conseillé d'héberger plusieurs sessions avec des claviers Bloomberg. Le clavier ne fonctionne correctement que dans un environnement n'hébergeant qu'une seule session.

Pour activer ou désactiver la prise en charge du clavier Bloomberg

> **Attention**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

1. Recherchez la clé suivante dans le registre :

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

2. Procédez comme suit :

   - Pour activer cette fonctionnalité, pour l'entrée Type DWORD et Nom **EnableBloombergHID**, définissez la valeur sur 1.
   - Pour désactiver cette fonctionnalité, définissez la valeur sur 0.

Pour de plus amples informations sur la configuration du clavier Bloomberg, consultez l'article CTX122615 du centre de connaissances.

Pour empêcher l'assombrissement de la fenêtre Desktop Viewer

Si vous utilisez plusieurs fenêtres Desktop Viewer, par défaut, les bureaux qui ne sont pas actifs sont assombris. Si vous avez besoin d'afficher plusieurs bureaux simultanément, ils peuvent devenir illisibles. Vous pouvez désactiver le comportement par défaut et empêcher l'assombrissement de la fenêtre Desktop Viewer en modifiant le registre.

Avertissement : toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

1. Sur la machine utilisateur, créez une entrée REG_DWORD nommée DisableDimming dans l'une des clés suivantes, selon que vous souhaitez empêcher l'assombrissement pour l'utilisateur actuel de la machine ou pour la machine. Une entrée existe déjà si Desktop Viewer a été utilisé sur la machine :

   - HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer
   - HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop\DesktopViewer

   Vous pouvez également, plutôt que de contrôler l'assombrissement à l'aide des paramètres ci-dessus, définir une stratégie locale en créant la même entrée REG_WORD dans l'une des clés suivantes :

   - HKEY_CURRENT_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer

- HKEY_LOCAL_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer

L'utilisation de ces clés est optionnelle car les administrateurs XenDesktop, contrairement aux administrateurs ou utilisateurs de plug-ins, contrôlent généralement les paramètres de stratégie à l'aide de stratégies de groupe. Par conséquent, avant d'utiliser ces clés, demandez à votre administrateur XenDesktop s'il a déjà créé une stratégie pour cette fonctionnalité.

2. Définissez une valeur non nulle telle que 1 ou true pour l'entrée.

   Si aucune entrée n'est spécifiée ou que l'entrée est définie sur 0, la fenêtre Desktop Viewer est assombrie. Si plusieurs entrées sont spécifiées, l'ordre de priorité suivant est utilisé. La première valeur répertoriée dans cette liste, et sa valeur, déterminent si la fenêtre est assombrie :

   a) HKEY_CURRENT_USER\Software\Policies\Citrix\…
   b) HKEY_LOCAL_MACHINE\Software\Policies\Citrix\…
   c) HKEY_CURRENT_USER\Software\Citrix\…
   d) HKEY_LOCAL_MACHINE\Software\Citrix\…

Configuration de la redirection bidirectionnelle du contenu

March 26, 2019

Vous pouvez activer la redirection bidirectionnelle du contenu à l'aide de l'une des méthodes suivantes :

1. Modèle d'administration d'objet de stratégie de groupe
2. Registre

> **Remarque**
>
> - La redirection bidirectionnelle du contenu ne fonctionne pas sur les sessions sur lesquelles **Local App Access** est activé.
> - La redirection bidirectionnelle du contenu doit être activée sur le serveur et le client. Lorsqu'elle est désactivée sur le serveur ou le client, la fonctionnalité est désactivée.

Pour activer la redirection bidirectionnelle du contenu grâce au modèle d'administration d'objet de stratégie de groupe

Utilisez la configuration du modèle d'administration d'objet de stratégie de groupe pour une première installation de Citrix Receiver pour Windows.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.

2. Sous le nœud Configuration utilisateur, accédez à **Modèles d'administration** > **Modèles d'administration classiques (ADM)** > **Composants Citrix** > **Citrix Receiver** > **Expérience utilisateur**.
3. Sélectionnez la stratégie Redirection bidirectionnelle du contenu.
4. Modifiez les paramètres.

> **Remarque**
>
> Lorsque vous incluez des adresses URL, vous pouvez spécifier une seule adresse URL ou une liste d'adresses URL séparées par des points-virgules. Vous pouvez utiliser un astérisque (*) comme caractère générique.

5. Cliquez sur **Appliquer**, puis sur **OK**.
6. À partir d'une ligne de commande, exécutez la commande gpupdate /force.

Pour activer la redirection bidirectionnelle du contenu à l'aide du Registre

Pour activer la redirection bidirectionnelle du contenu, exécutez la commande **redirector.exe /RegIE** depuis le dossier d'installation de Citrix Receiver pour Windows (C:\Program Files (x86)\Citrix\ICA Client).

Limitation

- Aucun mécanisme de secours n'est présent si la redirection échoue en raison de problèmes de démarrage de session.

> **Important**
>
> - Assurez-vous que les règles de redirection n'entraînent pas une configuration en boucle. Une configuration en boucle se produit si des règles de VDA sont définies de manière à ce qu'une URL, par exemple https://www.my_company.com, soit configurée pour être redirigée sur le client, et que la même adresse URL est configurée pour être redirigée sur le VDA.
> - La redirection d'URL prend uniquement en charge les adresses URL explicites (c'est-à-dire, celles qui apparaissent dans la barre d'adresse du navigateur ou celles trouvées à l'aide de la navigation du navigateur, en fonction du navigateur).
> - Si deux applications avec le même nom d'affichage sont configurées pour utiliser des comptes StoreFront multiples, le nom d'affichage du compte StoreFront principal est utilisé pour lancer la session d'application ou de bureau.
> - Une nouvelle fenêtre de navigateur s'affiche uniquement lorsque l'adresse URL est redirigée sur le client. Lorsque l'adresse URL est redirigée sur le VDA, et que le navigateur est déjà

ouvert, l'adresse URL redirigée s'ouvre dans le nouvel onglet.
- Les liens intégrés aux fichiers tels que documents, e-mails, et fichiers PDF sont pris en charge.

Communication des informations de compte aux utilisateurs

June 27, 2019

Fournissez aux utilisateurs les informations de compte dont ils ont besoin pour accéder aux applications et bureaux virtuels. Vous pouvez leur fournir ces informations de la façon suivante :

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

Important

Citrix vous recommande de redémarrer Citrix Receiver pour Windows après l'installation. Cela garantit que les utilisateurs peuvent ajouter des comptes et que Citrix Receiver pour Windows peut détecter les périphériques USB qui étaient suspendus au moment de l'installation.

Une boîte de dialogue indiquant la réussite de l'installation s'affiche, suivie de la boîte de dialogue **Ajouter un compte**. Si vous utilisez le logiciel pour la première fois, la boîte de dialogue **Ajouter un compte** vous invite à entrer une adresse e-mail ou de serveur pour configurer un compte.

Suppression de la boîte de dialogue Ajouter un compte

La boîte de dialogue Ajouter un compte s'affiche lorsque le magasin n'est pas configuré. Les utilisateurs peuvent utiliser cette fenêtre pour créer un compte Citrix Receiver en entrant une adresse e-mail ou une adresse URL de serveur.

Citrix Receiver pour Windows identifie le serveur NetScaler Gateway ou StoreFront, ou le boîtier virtuel AppController associé à l'adresse e-mail et invite l'utilisateur à ouvrir une session pour l'énumération.

La boîte de dialogue Ajouter un compte peut être supprimée de l'une des manières suivantes :

1. **À l'ouverture de session sur le système**

   Sélectionnez **Ne pas afficher cette fenêtre automatiquement à l'ouverture de session** pour que la fenêtre Ajouter un compte ne s'affiche pas au cours des ouvertures de session suivantes. Ce paramètre est spécifique à chaque utilisateur et se réinitialise au cours d'une action de réinitialisation de Citrix Receiver pour Windows.

2. **Installation par ligne de commande**

Installez Citrix Receiver pour Windows en tant qu'administrateur avec le commutateur suivant sur l'interface de ligne de commande.
CitrixReceiver.exe /ALLOWADDSTORE=N
Ceci est un paramètre de machine ; par conséquent, le comportement s'applique à tous les utilisateurs.

Le message suivant s'affiche lorsque le magasin n'est pas configuré.

De plus, la boîte de dialogue Ajouter un compte peut être supprimée de l'une des manières suivantes.

> **Remarque**
>
> Citrix recommande aux utilisateurs de supprimer la boîte de dialogue Ajouter un compte à l'aide de la méthode Ouverture de session sur le système ou Interface de ligne de commande.

- Modifier le nom du fichier d'exécution de Citrix :
  renommez **CitrixReceiver.exe** vers **CitrixReceiverWeb.exe** pour modifier le comportement de la boîte de dialogue Ajouter un compte. Si vous renommez ce fichier, la boîte de dialogue Ajouter un compte n'est pas affichée dans le menu Démarrer.
  Consultez Déploiement de Receiver pour Windows à partir de Receiver pour Web pour plus d'informations sur Citrix Receiver pour Web
- Objet de stratégie de groupe :
  pour masquer le bouton Ajouter un compte à partir de l'assistant d'installation de Citrix Receiver pour Windows, désactivez **EnableFTUpolicy** sous le nœud Self-Service dans l'éditeur de stratégie de groupe local, comme illustré ci-dessous.
  Ceci est un paramètre de machine ; par conséquent, le comportement s'applique à tous les utilisateurs.
  Pour charger le fichier de modèle, reportez-vous à la section Configuration de Receiver avec le modèle d'objet de stratégie de groupe.

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

Lorsque vous configurez Citrix Receiver pour Windows pour la découverte de compte par e-mail, plutôt que d'entrer une adresse URL de serveur, les utilisateurs entrent leur adresse e-mail durant l'installation et la configuration initiale de Citrix Receiver pour Windows. Citrix Receiver pour Windows détermine le serveur NetScaler Gateway ou StoreFront, associé à l'adresse e-mail en se basant sur les enregistrements du service (SRV) de Domain Name System (DNS) et invite alors l'utilisateur à ouvrir une session pour accéder à ses applications et bureaux virtuels.

> **Remarque**
>
> La découverte de compte basée sur une adresse e-mail n'est pas prise en charge pour les déploiements avec l'Interface Web.

Pour configurer NetScaler Gateway, veuillez consulter la section Connexion à StoreFront à l'aide de la découverte basée sur l'adresse e-mail dans la documentation de NetScaler Gateway.

Fournir un fichier de provisioning aux utilisateurs

StoreFront fournit des fichiers de provisioning que les utilisateurs peuvent ouvrir pour se connecter aux magasins.

Vous pouvez utiliser StoreFront pour créer des fichiers de provisioning contenant les détails des comptes. Mettez ces fichiers à la disposition de vos utilisateurs pour leur permettre de configurer Citrix Receiver pour Windows automatiquement. Après l'installation de Citrix Receiver pour Windows, il leur suffit d'ouvrir le fichier pour configurer Citrix Receiver pour Windows. Si vous configurez des sites Citrix Receiver pour Web, les utilisateurs peuvent également obtenir les fichiers de provisioning Citrix Receiver pour Windows à partir de ces sites.

- Pour plus d'informations, veuillez consulter la section Pour exporter des fichiers de provisioning de magasin pour des utilisateurs dans la documentation de StoreFront.

Fournir aux utilisateurs des informations de compte à entrer manuellement

Pour permettre aux utilisateurs de créer des comptes manuellement, communiquez leur les informations dont ils ont besoin pour se connecter à leurs applications et bureaux virtuels.

- Pour les connexions à un magasin StoreFront, indiquez l'adresse URL de ce serveur. Par exemple : https://nomserveur.entreprise.com

  Pour les déploiements Interface Web, fournissez l'adresse URL du site XenApp Services.

- Pour les connexions établies via NetScaler Gateway, déterminez d'abord si l'utilisateur a accès à tous les magasins configurés ou uniquement au magasin dont l'accès distant est activé pour une passerelle NetScaler Gateway particulière.
  - Pour présenter tous les magasins configurés : fournissez aux utilisateurs le nom de domaine complet de NetScaler Gateway.
  - Pour limiter l'accès à un magasin particulier : fournissez aux utilisateurs le nom de domaine complet de NetScaler Gateway ainsi que le nom du magasin au format :

    NetScalerGatewayFQDN?NomMagasin

    Par exemple, si un magasin nommé « AppsVentes » peut accéder à distance au serveur1.com et qu'un magasin nommé « AppsRH » peut accéder à distance au serveur2.com, un utilisateur doit entrer serveur1.com?AppsVentes pour accéder à AppsVentes ou serveur2.com?AppsRH pour accéder à AppsRH. Cette fonctionnalité requiert qu'un nouvel utilisateur crée un compte en entrant une adresse URL et elle n'est pas disponible pour la découverte basée sur l'adresse e-mail.

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

Pour gérer les comptes, un utilisateur Citrix Receiver doit ouvrir la page d'accueil de Citrix Receiver pour Windows, cliquer sur et sur **Comptes**.

Partage automatique de comptes de magasins multiples

> **Avertissement**
>
> Une utilisation incorrecte de l'Éditeur du Registre peut occasionner de sérieux problèmes qui pourraient nécessiter l'installation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à effectuer une copie de sauvegarde avant de modifier le registre.

Si vous disposez de plus d'un compte, vous pouvez configurer Citrix Receiver pour Windows de manière à ce qu'il se connecte automatiquement à tous les comptes lors de l'établissement d'une session. Pour afficher automatiquement tous les comptes lors de l'ouverture de Citrix Receiver pour Windows :

Pour les systèmes 32 bits, créez la clé « CurrentAccount » :

Emplacement : HKLM\Software\Citrix\Dazzle

Nom de la clé : CurrentAccount

Valeur : AllAccount

Type : REG_SZ

Pour les systèmes 64 bits, créez la clé « CurrentAccount » :

Emplacement : HKLM\Software\Wow6432Node\Citrix\Dazzle

Nom de la clé : CurrentAccount

Valeur : AllAccount

Type : REG_SZ

Configuration des mises à jour de Citrix Receiver

June 27, 2019

Lorsque vous configurez les mises à jour de Citrix Receiver depuis Citrix Receiver pour Windows, suivez l'une des méthodes ci-dessous par ordre de priorité :

1. Modèle d'administration d'objet de stratégie de groupe
2. Interface de ligne de commande
3. Préférences avancées (par utilisateur)

> **Remarque**
>
> - Lorsque vous mettez à niveau Citrix Receiver pour Windows à l'aide des mises à jour de Citrix Receiver, la fenêtre d'ouverture de session n'apparaît pas.
> - Avec cette version, HDX RTME pour Windows est inclus dans les mises à jour de Citrix Receiver. Vous êtes informé de la mise à jour HDX RTME disponible sur la version LTSR et la version actuelle de Citrix Receiver pour Windows.

Limitations :

1. Si vous avez configuré un proxy de sortie d'interception SSL, vous devez ajouter une exception pour le service Receiver auto-update Signature `https://citrixupdates.cloud.com` et l'emplacement de téléchargement `https://downloadplugins.citrix.com`.
2. Votre système doit avoir accès à Internet.
3. Les utilisateurs de Receiver pour Web ne peuvent pas télécharger automatiquement la stratégie de StoreFront.
4. Par défaut, les mises à jour de Citrix Receiver sont désactivées sur le VDA. Cela comprend les machines de serveur multi-utilisateurs RDS, les machines VDI et les machines Remote PC.
5. Les mises à jour de Citrix Receiver sont désactivées sur les machines sur lesquelles Desktop Lock est installé.

Configuration avec le modèle d'administration d'objet de stratégie de groupe

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud Configuration ordinateur, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Receiver** > **Mises à jour de Receiver**.
3. Sélectionnez la stratégie **Définir le délai de recherche de mises à jour**. Cette stratégie vous permet d'organiser le déploiement pendant une période.
4. Sélectionnez **Activé** et, à partir du menu déroulant **Retarder groupe**, sélectionnez l'une des options suivantes :
   - **Fast (Rapide)** : le déploiement de la mise à jour se produit au début de la période de mise à disposition.
   - **Medium (Moyen)** : le déploiement de la mise à jour se produit au milieu de la période de mise à disposition.
   - **Slow (Lent)** : le déploiement de la mise à jour se produit à la fin de la période de mise à disposition.

5. Cliquez sur **Appliquer** et **OK** pour enregistrer la stratégie.
6. Dans la section Modèles de mises à jour de Receiver, sélectionnez la stratégie **Mises à jour de Receiver**.

   > **Remarque**
   >
   > Lorsque vous sélectionnez **Désactivé**, vous n'êtes pas informé des mises à jour disponibles. Cela masque également l'option **Mises à jour de Receiver** de la page **Préférences avancées**.

7. Sélectionnez **Activé** et définissez les valeurs selon vos besoins :
   - À partir du menu déroulant **Activer la stratégie de Mise à jour de Receiver**, sélectionnez l'une des options suivantes :
     - **Auto** : vous êtes informé lorsqu'une mise à jour est disponible (valeur par défaut).
     - **Manuel** : vous n'êtes pas informé lorsque des mises à jour sont disponibles. Recherchez les mises à jour manuellement.
   - Sélectionnez **LTSR UNIQUEMENT** pour obtenir les mises à jour de LTSR uniquement.
   - Dans le menu déroulant **auto-update-DeferUpdate-Count**, sélectionnez une valeur comprise entre **-1** et **30**, où
     - **-1** indique que vous pouvez différer les notifications le nombre de fois souhaité (valeur par défaut = -1).
     - **0** indique que l'option **Me rappeler plus tard** ne s'affiche pas.
     - Tout autre nombre : indique que l'option **Me rappeler plus tard** s'affiche ce nombre de fois. Par exemple, si vous définissez la valeur sur 10, l'option **Me rappeler plus tard** s'affiche 10 fois.
8. Cliquez sur **Appliquer** et **OK** pour enregistrer la stratégie.

Configuration à l'aide de l'interface de ligne de commande

Lors de l'installation de Citrix Receiver pour Windows

Pour configurer les paramètres de mise à jour de Citrix Receiver en tant qu'administrateur à l'aide de paramètres de ligne de commande lors de l'installation de Citrix Receiver :

- **/AutoUpdateCheck**= auto/manual/disabled
- **/AutoUpdateStream**= LTSR/Current. Où LTSR fait référence à la version Long Term Service et Current fait référence à la version actuelle.
- **/DeferUpdateCount**= toute valeur entre -1 et 30
- **/AURolloutPriority**= auto/fast/medium/slow

Par exemple `CitrixReceiver.exe /AutoUpdateCheck=auto /AutoUpdateStream=Current /DeferUpdateCount=-1 /AURolloutPriority=fast`

- Pour configurer les paramètres de mise à jour de Citrix Receiver en tant qu'utilisateur à l'aide de paramètres de ligne de commande lors de l'installation de Citrix Receiver :
  - **/AutoUpdateCheck=auto/manual**

Par exemple : `CitrixReceiver.exe /AutoUpdateCheck=auto`

La modification des paramètres de mise à jour de Citrix Receiver à l'aide du modèle d'administration d'objet de stratégie de groupe remplace les paramètres appliqués lors de l'installation de Citrix Receiver pour Windows pour tous les utilisateurs.

Après l'installation de Citrix Receiver pour Windows

Les mises à jour de Citrix Receiver peuvent être configurées après l'installation de Citrix Receiver pour Windows.

Pour utiliser la ligne de commande :

Ouvrez l'invite de commande Windows et changez de répertoire vers celui dans lequel se trouve **CitrixReceiverUpdater.exe**. CitrixReceiverUpdater.exe se trouve généralement dans `CitrixReceiverInstallLocation\Citrix\Ica Client\Receiver`.

Vous pouvez également définir la stratégie de ligne de commande de mise à jour de Citrix Receiver à l'aide de ce fichier binaire.

Par exemple : les administrateurs peuvent utiliser les quatre options :

- `CitrixReceiverUpdater.exe / AutoUpdateCheck=auto /AutoUpdateStream= Current/DeferUpdateCount=-1 / AURolloutPriority= fast`

Configuration à l'aide de l'interface utilisateur graphique

> **Remarque**
>
> Vous pouvez masquer tout ou partie de la page Préférences avancées disponible à partir de l'icône Citrix Receiver dans la zone de notification. Pour plus d'informations, veuillez consulter Masquer la page Préférences avancées.

Un utilisateur individuel peut remplacer le paramètre Mise à jour de Citrix Receiver à l'aide de la boîte de dialogue **Préférences avancées**. Il s'agit d'une configuration par utilisateur, par conséquent les paramètres s'appliquent uniquement à l'utilisateur actuel.

1. Faites un clic droit sur Citrix Receiver pour Windows dans la zone de notification.
2. Sélectionnez **Préférences avancées** et cliquez sur **Mise à jour de Receiver**.
3. Sélectionnez l'une des options suivantes :
   - Oui, me notifier

- Non, ne pas me notifier
- Utiliser paramètres spécifiés par l'administrateur

4. Cliquez sur **Enregistrer**.

Configuration des mises à jour de Citrix Receiver à l'aide de StoreFront

1. Utilisez un éditeur de texte pour ouvrir le fichier web.config, qui se trouve en général dans le répertoire C:\inetpub\wwwroot\Citrix\Roaming.
2. Recherchez l'élément de compte d'utilisateur dans le fichier (Store est le nom du compte de votre déploiement)

   Par exemple : <account id=… name="Store">

   Avant la balise *</account>*, accédez aux propriétés de ce compte d'utilisateur :

```
<properties>
<clear />
</properties>
```

3. Ajoutez la balise de mise à jour automatique après la balise *<clear />*.

```
<account>

    <clear />

    <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="F84Store"

      description="" published="true" updaterType="Citrix"
         remoteAccessType="None">

      <annotatedServices>

        <clear />

        <annotatedServiceRecord serviceRef="1__Citrix_F84Store">

          <metadata>

            <plugins>

              <clear />
```



```
20
21              </plugins>
22
23              <trustSettings>
24
25                <clear />
26
27              </trustSettings>
28
29              <properties>
30
31                <property name="Auto-Update-Check" value="auto" />
32
33                <property name="Auto-Update-DeferUpdate-Count" value="1"
                      />
34
35                        <property name="Auto-Update-LTSR-Only" value="
                             FALSE" />
36
37                <property name="Auto-Update-Rollout-Priority" value="fast
                      " />
38
39                     </properties>
40
41            </metadata>
42
43          </annotatedServiceRecord>
44
45        </annotatedServices>
46
47        <metadata>
48
49          <plugins>
50
51            <clear />
52
53          </plugins>
54
55          <trustSettings>
56
57            <clear />
58
59          </trustSettings>
60
61          <properties>
```



```
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
```

auto-update-Check

Cet attribut indique que Citrix Receiver pour Windows détecte lorsqu'une mise à jour est disponible.

Valeurs possibles :

- Auto : vous êtes notifié lorsqu'une mise à jour est disponible (valeur par défaut).
- Manuel : vous n'êtes pas notifié lorsque des mises à jour sont disponibles. Recherchez les mises à jour manuellement.
- Désactivé : les mises à jour de Citrix Receiver sont masquées et vous ne serez pas averti lorsqu'une mise à jour est disponible.

auto-update-LTSR-Only

Cet attribut indique que Citrix Receiver pour Windows doit accepter les mises à jour uniquement pour la version LTSR.

Valeurs possibles :

- True : les mises à jour de Citrix Receiver vérifient uniquement les mises à jour LTSR de Citrix Receiver pour Windows.
- False : les mises à jour de Citrix Receiver vérifient aussi les mises à jour non LTSR de Citrix Receiver pour Windows.

auto-update-DeferUpdate-Count

Cet attribut indique le nombre de fois que vous pouvez différer les notifications. L'option **Me rappeler plus tard** s'affiche le nombre de fois défini.

Valeurs possibles :

- -1 : indique que vous pouvez différer les notifications n'importe quel nombre de fois (valeur par défaut = -1).
- 0 : indique que l'option Me rappeler plus tard ne s'affiche pas.

- Tout autre nombre : indique combien de fois l'option Me rappeler plus tard s'affiche. Par exemple, si vous définissez la valeur sur 10, l'option Me rappeler plus tard s'affiche 10 fois.

auto-update-Rollout-Priority

Cet attribut indique la période que vous pouvez définir pour le déploiement.

Valeurs possibles :

- Fast (Rapide) : le déploiement de la mise à jour se produit au début de la période de mise à disposition.
- Medium (Moyen) : le déploiement de la mise à jour se produit au milieu de la période de mise à disposition.
- Slow (Lent) : le déploiement de la mise à jour se produit à la fin de la période de mise à disposition.

Configuration du modèle d'administration d'objet de stratégie de groupe

March 26, 2019

Citrix vous recommande d'utiliser l'Éditeur d'objet de stratégie de groupe Windows pour configurer Citrix Receiver pour Windows. Les fichiers de modèle d'administration de Citrix Receiver pour Windows se trouvent (receiver.adm ou receiver.admx\receiver.adml - en fonction du système d'exploitation) dans le répertoire d'installation.

> **Remarque**
>
> - À compter de Citrix Receiver pour Windows version 4.6, le répertoire d'installation comprend les fichiers CitrixBase.admx et CitrixBase.adml.
> - Citrix vous recommande d'utiliser les fichiers CitrixBase.admx et CitrixBase.adml pour vous assurer que les options sont correctement organisées et affichées dans l'éditeur d'objet de stratégie de groupe.
> - Le fichier .adm est uniquement destiné à être utilisé avec les plates-formes Windows XP Embedded. Les fichiers .admx/.adml sont uniquement destinés à être utilisés avec Windows Vista/Windows Server 2008 et toutes les versions ultérieures de Windows.
> - Si Citrix Receiver pour Windows a été installé avec le VDA, les fichiers admx/adml se trouvent dans le répertoire d'installation de Citrix Receiver pour Windows. Par exemple : <répertoire d'installation>\Online Plugin\Configuration.
> - Si Citrix Receiver pour Windows est installé sans VDA, les fichiers admx/adml se trouvent

> généralement dans le répertoire C:\Program Files\Citrix\ICA Client\Configuration.

Reportez-vous au tableau ci-dessous pour plus d'informations sur les fichiers de modèle Citrix Receiver pour Windows et leur emplacement.

> **Remarque**
>
> Citrix vous recommande d'utiliser les fichiers de modèle d'objet de stratégie de groupe fournis avec la dernière version de Citrix Receiver pour Windows.

Type de fichier	Emplacements du fichier
receiver.adm	<Répertoire d'installation>\ICA Client\Configuration
receiver.admx	<Répertoire d'installation>\ICA Client\Configuration
receiver.adml	<Répertoire d'installation>\ICA Client\Configuration\[MUIculture]
CitrixBase.admx	<Répertoire d'installation>\ICA Client\Configuration
CitrixBase.adml	<Répertoire d'installation>\ICA Client\Configuration\[MUIculture]

> **Remarque**
>
> - Si CitrixBase.admx\adml n'est pas ajouté à cet objet de stratégie de groupe local, la stratégie **Activer la signature de fichier ICA** peut être perdue.
> - Lors de la mise à niveau de Citrix Receiver pour Windows, vous devez ajouter les derniers fichiers de modèle à l'objet de stratégie de groupe local, comme expliqué dans la procédure ci-dessous. Lors de l'importation de la dernière version des fichiers, les paramètres précédents sont conservés.

Pour ajouter le fichier de modèle receiver.adm à l'objet de stratégie de groupe local (système d'exploitation Windows XP Embedded uniquement)

> **Remarque**
>
> Vous pouvez utiliser des fichiers de modèle .adm pour configurer des objets de stratégie de groupe locaux et/ou des objets de stratégie de groupe de domaine.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Dans le panneau gauche de l'Éditeur de stratégie de groupe, sélectionnez le dossier **Modèles d'administration**.
3. À partir du menu Action, sélectionnez **Ajout/Suppression de modèles**.
4. Sélectionnez Ajouter et accédez à l'emplacement du fichier de modèle <Répertoire d'installation>\ICA Client\Configuration\receiver.adm
5. Cliquez sur Ouvrir pour ajouter le modèle, puis cliquez sur Fermer pour retourner à l'Éditeur de stratégie de groupe.
   Le fichier de modèle de Citrix Receiver pour Windows sera disponible sur l'objet de stratégie de groupe local dans le chemin d'accès local **Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Receiver**.

Une fois que les fichiers de modèle .adm sont ajoutés au GPO local, le message suivant s'affiche :
« L'entrée suivante de la section [strings] est trop longue et a été tronquée » :
cliquez sur **OK** pour ignorer le message.

Pour ajouter les fichiers de modèle receiver.admx/adml à l'objet de stratégie de groupe local (versions ultérieures du système d'exploitation Windows)

> **Remarque**
>
> Vous pouvez utiliser des fichiers de modèle admx/adml pour configurer des objets de stratégie de groupe local et/ou des objets de stratégie de groupe basé sur un domaine. Consultez l'article Microsoft MSDN sur la gestion des fichiers ADMX.

Après l'installation de Citrix Receiver pour Windows, copiez les fichiers de modèle comme l'indique le tableau ci-dessous :

Type de fichier	Copier à partir de	Copier sur
receiver.admx	Répertoire d'installation\ICA Client\Configuration\receiver.a	%systemroot%\policyDefinitions
CitrixBase.admx	Répertoire d'installation\ICA Client\Configuration\CitrixBase.admx	%systemroot%\policyDefinitions
receiver.adml	Répertoire d'installation\ICA Client\Configuration\[MUIcultu	%systemroot%\policyDefinitions[MUIculture
CitrixBase.adml	Répertoire d'installation\ICA Client\Configuration\[MUIculture]CitrixBase.adml	%systemroot%\policyDefinitions[MUIculture

> **Remarque**
>
> Les fichiers de modèle de Citrix Receiver pour Windows sont disponibles sur l'objet de stratégie de groupe local dans le dossier Modèles d'administration > Composants Citrix > Citrix Receiver uniquement lorsque l'utilisateur ajoute le fichier CitrixBase.admx/CitrixBase.adml au dossier \policyDefinitions.

Optimiser l'environnement

November 16, 2018

Vous pouvez optimiser l'environnement en utilisant les fonctionnalités suivantes :

- Prise en charge de la configuration de l'espace de travail
- Réduction du temps de lancement des applications
- Mapper des machines clientes
- Prise en charge de la résolution de nom DNS
- Utilisation de serveurs proxy avec les connexions XenDesktop

Prise en charge de la résolution de nom DNS

November 16, 2018

Vous pouvez configurer les logiciels Citrix Receiver pour Windows qui se connectent à la batterie de serveurs en utilisant le Service XML Citrix de sorte qu'ils effectuent des requêtes de nom DNS (Domain Name System) au lieu de requêtes d'adresse IP.

Important : à moins que votre environnement DNS ne soit configuré spécialement pour l'utilisation de cette fonctionnalité, Citrix recommande de ne pas activer la résolution de nom DNS dans la batterie de serveurs.

Les logiciels Citrix Receiver pour Windows qui se connectent aux applications publiées via l'Interface Web utilisent également le Service XML Citrix. Pour Citrix Receiver pour Windows se connectant via l'Interface Web, le serveur Web résout le nom DNS pour Citrix Receiver pour Windows.

La résolution de nom DNS est désactivée par défaut dans la batterie et activée par défaut sur Citrix Receiver pour Windows. Lorsque la résolution de nom DNS est désactivée dans la batterie, tout Citrix Receiver pour Windows faisant la requête d'un nom DNS reçoit une adresse IP en réponse. Il n'est pas nécessaire de désactiver la résolution de nom DNS sur Citrix Receiver pour Windows.

Pour désactiver la résolution de nom DNS pour des machines utilisateur spécifiques

Si votre déploiement de serveurs utilise la résolution de nom DNS et que vous rencontrez des problèmes avec des machines utilisateur spécifiques, vous pouvez désactiver la résolution de nom DNS pour ces machines.

> **Attention :**
>
> Une utilisation incorrecte de l'Éditeur du Registre peut occasionner de sérieux problèmes qui pourraient nécessiter l'installation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à effectuer une copie de sauvegarde avant de modifier le registre.

1. Ajoutez une clé de registre de chaîne **xmlAddressResolutionType** à HKEY_LOCAL_MACHINE\Software\Wow6
   Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing.
2. Définissez la valeur sur **IPv4-Port**.
3. Répétez l'opération pour chaque utilisateur des machines utilisateur.

Utilisation de serveurs proxy avec XenDesktop

June 27, 2019

Si vous n'utilisez pas de serveurs proxy dans votre environnement, modifiez les paramètres proxy d'Internet Explorer sur les machines utilisateur qui exécutent Internet Explorer 7.0 sur Windows XP. Par défaut, cette configuration détecte automatiquement les paramètres proxy. Si aucun serveur proxy n'est utilisé, les utilisateurs observeront des délais durant le processus de détection.

Pour obtenir des instructions sur la modification des paramètres proxy, consultez votre documentation Internet Explorer. Vous pouvez également modifier les paramètres proxy à l'aide de l'Interface Web. Pour de plus amples renseignements, consultez la Documentation de l'interface Web.

Mappage des machines clientes

June 27, 2019

Citrix Receiver pour Windows prend en charge le mappage de machines sur les machines utilisateur de sorte que les utilisateurs puissent accéder à ces machines à partir des sessions. Les utilisateurs peuvent effectuer les opérations suivantes :

- accéder de manière transparente aux lecteurs, aux imprimantes et aux ports COM locaux ;

- couper et coller des données entre la session et le Presse-papiers local de Windows ;
- entendre des données audio (sons système et fichiers .wav) lues dans la session.

Lors de l'ouverture de session, Citrix Receiver pour Windows indique au serveur les lecteurs, ports COM et ports LPT clients disponibles. Par défaut, les lecteurs clients sont mappés sur des lettres de lecteur serveur et des files d'impression de serveur sont créées pour les imprimantes clientes de sorte que ces dernières semblent connectées directement à la session. Ces mappages sont accessibles à l'utilisateur actuel et dans la session en cours uniquement. Ils sont supprimés à la fermeture de la session et créés de nouveau à l'ouverture de session suivante.

Vous pouvez utiliser les paramètres de redirection de stratégie pour mapper les machines utilisateur qui ne sont automatiquement mappées à l'ouverture de session. Pour plus d'informations, veuillez consulter la documentation relative à XenDesktop ou XenApp.

Désactivation du mappage des machines utilisateur

Vous pouvez configurer le mappage des machines utilisateur, notamment les options de lecteurs, d'imprimantes et de ports, à l'aide du Gestionnaire de serveur Windows. Pour plus d'informations sur les options disponibles, consultez votre documentation Services Bureau à distance.

Rediriger les dossiers clients

La redirection de dossiers clients modifie la manière dont les fichiers côté client sont accessibles sur la session côté hôte. Lorsque vous activez uniquement le mappage de lecteur client sur le serveur, les volumes complets côté client sont automatiquement mappés sur les sessions en tant que liens UNC (Universal Naming Convention). Lorsque vous activez la redirection de dossiers clients sur le serveur et que l'utilisateur la configure sur la machine utilisateur, la partie du volume local spécifié par l'utilisateur est redirigée.

Seuls les dossiers spécifiés par l'utilisateur s'affichent sous forme de liens UNC dans les sessions au lieu du système de fichiers complet sur la machine utilisateur. Si vous désactivez les liens UNC via le registre, des dossiers clients apparaissent comme des lecteurs mappés au sein de la session. Pour de plus amples informations, notamment comment configurer la redirection de dossiers clients pour les machines utilisateur, consultez la documentation XenDesktop 7.

Mapper des lecteurs clients sur des lettres de lecteur du côté hôte

Le mappage des lecteurs clients permet d'affecter des lettres de lecteur du côté hôte aux lecteurs existants sur la machine utilisateur. Par exemple, dans une session utilisateur Citrix, le lecteur H peut être mappé sur le lecteur C de la machine utilisateur qui exécute Citrix Receiver pour Windows.

Le mappage des lecteurs clients fait partie intégrante des fonctions standard Citrix de redirection de périphérique de manière transparente. Pour le Gestionnaire de fichiers, l'Explorateur Windows et vos applications, ces mappages se présentent comme tout autre mappage réseau.

Le serveur hébergeant les applications et bureaux virtuels peut être configuré au cours de son installation pour mapper automatiquement les lecteurs du client sur un groupe de lettres de lecteur défini. Par défaut, l'installation mappe les lettres de lecteur affectées aux lecteurs du client en commençant par la lettre V et en remontant l'alphabet, en affectant une lettre de lecteur à chaque lecteur fixe et lecteur de CD-ROM. (Les lecteurs de disquettes sont affectés de leur lettre existante.) Cette méthode fournit les mappages de lecteur suivants dans une session :

Lettre du lecteur client	Accessible par le serveur sous :
Une	Une
B	B
C	V
D	U

Le serveur peut être configuré de façon à ce que les lettres de ses lecteurs n'entrent pas en conflit avec celles des lecteurs du client ; dans ce cas, les lettres des lecteurs du serveur sont remplacées par des lettres plus proches de la fin de l'alphabet. Par exemple, en remplaçant respectivement les lettres C et D des lecteurs du serveur par les lettres M et N, les machines clientes peuvent accéder directement à leurs disques C et D. Cette méthode produit les mappages suivants pour les lecteurs d'une session.

Lettre du lecteur client	Accessible par le serveur sous :
Une	Une
B	B
C	C
D	D

La nouvelle lettre de lecteur affectée au lecteur C du serveur est définie au moment de l'installation. Les lettres de tous les autres lecteurs de disque fixe et de CD-ROM sont remplacées par les lettres suivantes dans l'ordre alphabétique (par exemple : C > M, D > N, E > O). Elles ne doivent pas entrer en conflit avec les lettres déjà utilisées pour les mappages de lecteur réseau (effectués avec la commande Connecter un lecteur réseau). Si un mappage de lecteur réseau utilise une lettre déjà utilisée par un lecteur du serveur, le mappage de ce lecteur réseau est invalide.

Lorsqu'une machine utilisateur se connecte à un serveur, les mappages de ses lecteurs sont rétablis, sauf si le mappage automatique des machines clientes est désactivé. Le mappage des lecteurs clients est activé par défaut. Pour modifier les paramètres, utilisez l'utilitaire Configuration des services Bureau à distance (services Terminal Server). Vous pouvez aussi utiliser des stratégies vous permettant d'avoir un contrôle accru sur la manière dont le mappage des périphériques clients s'applique. Pour de plus amples informations sur les stratégies, veuillez consulter la documentation relative à XenDesktop ou XenApp dans la documentation produit Citrix.

Redirection de périphérique USB Plug and Play HDX

La redirection de périphérique USB HDX Plug and Play permet de rediriger de manière dynamique les périphériques multimédia, tels que les appareils photo, les scanners, les lecteurs multimédia et les terminaux de point de vente, vers le serveur. Vous ou l'utilisateur pouvez limiter la redirection de tous les périphériques ou de certains périphériques. Modifiez les stratégies sur le serveur ou appliquez des stratégies de groupe sur la machine utilisateur pour configurer les paramètres de redirection. Pour plus d'informations, veuillez consulter Considérations USB et lecteur client dans la documentation relative à XenApp et XenDesktop.

Important : si vous interdisez la redirection des périphériques USB Plug and Play dans une stratégie de serveur, l'utilisateur ne peut pas écraser ce paramètre de stratégie.

Un utilisateur peut définir des autorisations dans Citrix Receiver pour Windows pour autoriser ou rejeter systématiquement la redirection de périphérique chaque fois qu'un périphérique est connecté. Ce paramètre affecte uniquement les périphériques connectés après que l'utilisateur ait modifié le paramètre.

Pour mapper des ports COM clients à un port COM serveur

Le mappage des ports COM clients permet d'utiliser, au cours de sessions, les périphériques connectés aux ports COM de la machine utilisateur. Ces mappages peuvent être utilisés de la même façon que n'importe quel mappage réseau effectué au moyen de la commande Connecter un lecteur réseau.

Vous pouvez mapper les ports COM clients à partir d'une invite de commande. Vous pouvez également contrôler le mappage des ports COM clients à partir de l'utilitaire Configuration des services Bureau à distance (services Terminal Server) ou à l'aide de stratégies. Pour plus d'informations sur les stratégies, veuillez consulter la documentation relative à XenDesktop ou XenApp.

Important : le mappage des ports COM n'est pas compatible avec l'interface TAPI.

1. Pour les déploiements XenDesktop 7, activez le paramètre de stratégie Redirection de port COM client.
2. Ouvrez une session sur Citrix Receiver pour Windows.

3. À l'invite de commandes, entrez la commande suivante :

   net use comx: \\client\comz:

   où x correspond au numéro de port COM sur le serveur (les ports 1 à 9 peuvent être mappés) et z au numéro du port COM client à mapper.

4. Pour confirmer l'opération, entrez la commande suivante :

   ```
   net use
   ```

   à l'invite de commande. La liste qui apparaît affiche les lecteurs, ports LPT et ports COM mappés.

Pour utiliser ce port COM dans une application ou un bureau virtuel, installez votre machine utilisateur en utilisant le nom mappé. Par exemple, si le port COM1 du client est mappé sur le port COM5 du serveur, installez votre périphérique sur le port COM5 dans la session. Utilisez ce port COM comme vous utiliseriez n'importe quel autre port COM de la machine utilisateur.

Prise en charge de la configuration de l'espace de travail

June 27, 2019

Citrix Receiver pour Windows prend en charge la configuration d'espaces de travail pour les abonnés, qui peuvent utiliser un ou plusieurs services disponibles auprès de Citrix Cloud.

Un espace de travail fait partie d'une solution d'espace de travail numérique qui permet au service informatique de fournir de manière sécurisée l'accès aux applications à partir de n'importe quel appareil.
Cette capture d'écran est un exemple de ce que l'expérience de l'espace de travail ressemble pour vos abonnés. Cette interface évolue et peut différer de celle avec laquelle vos abonnés travaillent aujourd'hui. Par exemple, elle peut indiquer « StoreFront » en haut de la page au lieu de « Espace de travail ».

Citrix Receiver pour Windows et Receiver pour Web prennent actuellement en charge l'authentification Azure Active Directory.
Pour plus d'informations sur la configuration de l'espace de travail, consultez la section Configuration de l'espace de travail dans Citrix Cloud.

Réduction du temps de lancement des applications

January 9, 2019

Utilisez la fonctionnalité de pré-lancement de session pour réduire la durée de lancement des applications en période d'activité normale ou maximale, et ainsi offrir une meilleure expérience aux utilisateurs. La fonctionnalité de pré-lancement permet la création d'une session de pré-lancement lorsqu'un utilisateur ouvre une session Citrix Receiver pour Windows, ou à un horaire programmé si l'utilisateur a déjà ouvert une session.

Cette session de pré-lancement réduit la durée de démarrage de la première application. Lorsqu'un utilisateur ajoute une nouvelle connexion de compte à Citrix Receiver pour Windows, le pré-lancement de session prend effet lors de la session suivante. L'application par défaut ctxprelaunch.exe s'exécute dans la session, mais l'utilisateur ne la voit pas.

Le pré-lancement de session est pris en charge pour les déploiements StoreFront à compter de la version 2.0 de StoreFront. Pour les déploiements Interface Web, vous devez utiliser l'option d'enregistrement du mot de passe de l'Interface Web pour éviter les invites d'ouverture de session. Le pré-lancement de session n'est pas pris en charge avec les déploiements XenDesktop 7.

Le pré-lancement de session est désactivé par défaut. Pour activer le pré-lancement de session, spécifiez le paramètre ENABLEPRELAUNCH=true sur la ligne de commande Receiver ou définissez la clé de registre EnablePreLaunch sur true. Le paramètre par défaut, null, signifie que le pré-lancement est désactivé.

Remarque : si la machine cliente n'a pas été configurée pour prendre en charge l'authentification unique de domaine (SSON), le pré-lancement est automatiquement activé. Si vous souhaitez utiliser l'authentification unique de domaine (SSON) sans pré-lancement, définissez alors la
valeur de la clé de registre EnablePreLaunch
sur false.

Avertissement : toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Emplacements de registre :

HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle

HKEY_CURRENT_USER\Software\Citrix\Dazzle

Il existe deux types de pré-lancement :

- **Pré-lancement zéro délai**. Le pré-lancement démarre immédiatement après l'authentification des informations d'identification de l'utilisateur, et ce même en période de trafic intense. Utilisé pour les périodes de trafic normal. Un utilisateur peut déclencher le pré-lancement zéro délai en redémarrant Citrix Receiver pour Windows.

- **Pré-lancement planifié**. Le pré-lancement démarre à l'heure planifiée. Le pré-lancement planifié ne démarre que lorsque la machine utilisateur est déjà exécutée et authentifiée. Si ces deux conditions ne sont pas remplies à l'heure planifiée, aucune session n'est lancée. Pour répartir la charge réseau et serveur, la session se lance dans un intervalle de temps proche de l'heure planifiée. À titre d'exemple, si le pré-lancement planifié est programmé pour démarrer à 13:45, la session se lance en fait entre 13:15 et 13:45. Utilisé lors des périodes de trafic élevé.

La configuration du pré-lancement sur un serveur XenApp consiste à créer, modifier ou supprimer des applications de pré-lancement, et à mettre à jour les paramètres de stratégie utilisateur qui contrôlent les applications de pré-lancement. Pour obtenir des informations sur la configuration du pré-lancement de session sur le serveur XenApp, consultez la section « Pour déployer des applications de pré-lancement sur des machines utilisateur » dans la documentation XenApp.

La personnalisation de la fonctionnalité de pré-lancement à l'aide du fichier receiver.admx n'est pas prise en charge. Toutefois, vous pouvez modifier la configuration du pré-lancement en modifiant les valeurs de registre pendant ou après l'installation de Citrix Receiver pour Windows. Il existe trois valeurs HKLM et deux valeurs HKCU :

- Les valeurs HKLM sont écrites durant l'installation du client.
- Les valeurs HKCU vous permettent de fournir à différents utilisateurs sur la même machine différents paramètres. Les utilisateurs peuvent modifier les valeurs HKCU sans permissions administratives. Vous pouvez fournir à vos utilisateurs des scripts leur permettant de modifier la configuration.

Valeurs de registre HKEY_LOCAL_MACHINE

Pour Windows 7 et 8, 64 bits : HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

Pour tous les autres systèmes d'exploitation Windows 32 bits pris en charge : HKEY_LOCAL_MACHINE\SOFTWARE\C
Client\Prelaunch

Nom : UserOverride

Valeurs :

0 - Utilise les valeurs HKEY_LOCAL_MACHINE même si les valeurs de HKEY_CURRENT_USER sont également présentes.

1 - Utilise les valeurs de HKEY_CURRENT_USER si elles existent ; utilise autrement les valeurs de HKEY_LOCAL_MACHINE.

Nom : State

Valeurs :

0 - Désactive le pré-lancement.

1 - Active le pré-lancement zéro délai. (Le pré-lancement démarre après authentification des informations d'identification de l'utilisateur.)

2 - Active le pré-lancement planifié. (Le pré-lancement démarre à l'heure configurée pour Schedule.)

Nom : Schedule

Valeur :

L'heure (format 24 heures) et les jours de la semaine du pré-lancement planifié doivent être entrés au format suivant :

HH: MM	M:T:W:TH:F:S:SU où HH et MM correspondent aux heures et minutes. M:T:W:TH:F:S:SU correspondent aux jours de la semaine. Par exemple, pour activer le pré-lancement planifié le lundi, mercredi et vendredi à 13:45, définissez Schedule de la sorte : Schedule=13:45	1:0:1:0:1:0:0 . La session se lance entre 13:15 et 13:45.

Valeurs de registre HKEY_CURRENT_USER

HKEY_CURRENT_USER\Software\Citrix\ICA Client\Prelaunch

Les clés State et Schedule ont les mêmes valeurs que pour HKEY_LOCAL_MACHINE.

Amélioration de l'expérience utilisateur

May 23, 2019

Vous pouvez améliorer votre expérience avec Citrix Receiver pour Windows en utilisant les fonctionnalités suivantes :

- Lancement de vPrefer - Contrôle comment les applications publiées doivent être lancées dans des sessions de bureau publié.
- Codage vidéo H.265 - Fournit une meilleure compression des données (en utilisant moins de bande passante) sans sacrifier la qualité de l'image ou la qualité supérieure.
- Mise à l'échelle DPI - Permet au système d'exploitation de contrôler la résolution de la session.

- Éditeur IME client générique - Permet de prendre en charge les claviers logiciels et les options permettant de modifier l'éditeur IME.
- Disposition du clavier et langue - Permet d'utiliser les dispositions de clavier préférées.

En outre, vous pouvez utiliser les fonctionnalités suivantes qui permettent également de fournir une meilleure expérience utilisateur.

Mode tablette étendue dans Windows 10 avec Windows Continuum

Windows Continuum est une fonctionnalité de Windows 10 qui s'adapte à la manière dont la machine cliente est utilisée. Citrix Receiver pour Windows version 4.10 prend désormais en charge Windows Continuum, y compris le changement dynamique des modes.

Sur les appareils tactiles, le VDA Windows 10 est lancé en mode Tablette lorsqu'aucune souris ou aucun clavier n'est connecté. Il démarre en mode bureau lorsqu'un clavier ou une souris ou les deux sont connectés. Détacher ou attacher le clavier sur un périphérique client ou l'écran sur un appareil 2 en 1, comme Surface Pro, fait basculer entre les modes tablette et bureau. Pour plus d'informations, veuillez consulter Mode tablette pour appareils à écran tactile dans la documentation de XenApp et XenDesktop.

Le VDA Windows 10 détecte la présence d'un clavier ou d'une souris sur un périphérique client tactile lorsque vous vous connectez ou que vous vous reconnectez à une session. Il détecte également lorsque vous connectez ou déconnectez un clavier ou une souris pendant la session. Par défaut, cette fonction est activée sur le VDA. Pour désactiver la fonctionnalité, modifiez la stratégie **Basculer en mode tablette** à l'aide de Citrix Studio.

Le mode tablette offre une interface utilisateur qui est mieux adaptée aux écrans tactiles :

- Boutons légèrement plus grands.
- L'écran de démarrage et toutes les applications que vous démarrez s'ouvrent en mode plein écran.
- La barre des tâches contient un bouton Précédent.
- Les icônes sont retirées de la barre des tâches.

Le mode bureau offre l'interface utilisateur traditionnelle où vous interagissez de la même manière que sur un PC avec un clavier et une souris.

Remarque : les Receiver Web ne prennent pas en charge les fonctionnalités de Windows Continuum.

Pour plus d'informations, consultez la section
Notes de publication sur XenServer 7.2.

Souris relative

La prise en charge d'une souris relative fournit une option qui permet d'interpréter la position de la souris de manière relative plutôt qu'absolue. Cette capacité est requise par les applications qui exigent des entrées de souris relatives plutôt qu'absolues.

Remarque : cette fonctionnalité peut uniquement être appliquée à une session de bureau publié.

Pour activer la prise en charge de la souris relative

1. Connectez-vous à Citrix Receiver pour Windows
2. Lancez une session de bureau publié.
3. À partir de la barre d'outils de Desktop Viewer, sélectionnez **Préférences**.

   La fenêtre Citrix Receiver : Préférences s'affiche.
4. Sélectionnez Connexions.
5. Sous Paramètres de la souris relative, activez l'option **Utiliser la souris relative**.
6. Cliquez sur **Appliquer**, puis sur **OK**.

REMARQUE : cette fonctionnalité est définie par session. Elle n'est pas conservée après la reconnexion à une session déconnectée. Les utilisateurs doivent réactiver la fonctionnalité chaque fois qu'ils se connectent ou se reconnectent au bureau publié.

Décodage matériel

Lors de l'utilisation de Citrix Receiver pour Windows (avec moteur HDX 14.4), le GPU peut être utilisé pour le décodage H.264 lorsqu'il est disponible sur le client. La couche API utilisée pour le décodage GPU est DXVA (accélération vidéo DirectX).

Pour activer le décodage matériel à l'aide du modèle d'administration d'objet de stratégie de groupe Citrix Receiver :

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Citrix Receiver** > **Expérience utilisateur**.
3. Sélectionnez **Accélération matérielle pour graphiques**.
4. Sélectionnez **Activé** et cliquez sur **Appliquer**, puis sur **OK**.

Pour déterminer si la stratégie a été appliquée et si l'accélération matérielle est utilisée pour une session ICA active, recherchez les entrées de registre suivantes :

Chemin du registre : HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender

> **Conseil**
>
> La valeur de **Graphics_GfxRender_Decoder** et **Graphics_GfxRender_Renderer** doit être 2. La valeur 1 indique que le décodage basé sur le processeur est utilisé.

Lors de l'utilisation de la fonctionnalité de décodage matériel, tenez compte des limitations suivantes :

- Si le client est équipé de deux GPU et que l'un des moniteurs est actif sur le second GPU, le décodage sera effectué sur le processeur.
- Lors de la connexion à un serveur XenApp 7.x exécuté sur Windows Server 2008 R2, Citrix recommande de ne pas utiliser le décodage matériel sur la machine Windows de l'utilisateur. Si cette fonctionnalité est activée, des problèmes tels que la baisse des performances lors de la mise en surbrillance de texte et des problèmes de scintillement peuvent être observés.

Entrée microphone côté client

Citrix Receiver pour Windows prend en charge de multiples entrées microphone du côté client. Les micros installés localement peuvent être utilisés pour :

- les activités en temps réel, telles que les appels via softphone et les conférences Web ;
- les applications d'enregistrement hébergées, telles que les logiciels de dictée ;
- les enregistrements audio et vidéo.

Les utilisateurs de Citrix Receiver pour Windows peuvent sélectionner s'ils souhaitent utiliser les microphones connectés à leur appareil en modifiant un paramètre du Centre de connexion. Les utilisateurs de XenDesktop peuvent également utiliser les Préférences de XenDesktop Viewer pour désactiver leurs micros et webcams.

Prise en charge de moniteurs multiples

Citrix Receiver pour Windows vous permet d'utiliser jusqu'à huit moniteurs.

Chaque écran faisant partie d'une configuration multi-écrans dispose de sa propre résolution conçue par le fabricant. Les écrans peuvent afficher des résolutions et des orientations différentes durant les sessions.

Les sessions peuvent occuper plusieurs écrans de deux façons :

- Mode plein écran, avec écrans multiples affichés dans la session ; les applications s'alignent sur les écrans comme elles le font localement.

  XenDesktop : pour afficher la fenêtre Desktop Viewer sur n'importe quel sous-ensemble d'écrans, redimensionnez la fenêtre sur ces derniers et cliquez sur **Agrandir**.

- Mode fenêtre, avec une seule image d'écran pour la session ; les applications ne s'alignent pas sur les écrans individuels.

XenDesktop : lorsqu'un bureau appartenant au même groupe (anciennement « groupe de bureau ») est lancé ultérieurement, le paramètre de fenêtre est conservé et le bureau est affiché sur les mêmes écrans. Plusieurs bureaux virtuels peuvent être affichés sur une machine à condition que la disposition de l'écran soit rectangulaire. Si l'écran principal sur la machine est utilisé par la session XenDesktop, il devient l'écran principal dans la session. Autrement, l'écran numériquement inférieur dans la session devient l'écran principal.

Pour activer la prise en charge multi-écran, veillez à ce que les conditions suivantes soient réunies :

- La machine utilisateur est configurée pour prendre en charge de multiples écrans.
- Le système d'exploitation de la machine utilisateur doit être en mesure de détecter chaque écran. Sur les plates-formes Windows, pour vérifier que cette détection a lieu, ouvrez la boîte de dialogue Propriétés d'affichage et consultez l'onglet Paramètres pour confirmer que chaque écran y figure séparément.
- Une fois que vos écrans ont été détectés :
  - **XenDesktop** : configurez la limite de mémoire graphique à l'aide du paramètre de stratégie d'ordinateur Citrix Limite de mémoire d'affichage.
  - **XenApp** : en fonction de la version du serveur XenApp que vous avez installée :
    * Configurez la limite de mémoire graphique à l'aide du paramètre de stratégie d'ordinateur Citrix Limite de mémoire d'affichage.
    * À partir de la console de gestion Citrix du serveur XenApp, sélectionnez la batterie et dans le panneau des tâches, sélectionnez Modifier les propriétés de serveur > Modifier toutes les propriétés > Valeur par défaut du serveur > HDX Broadcast > Affichage (ou Modifier les propriétés de serveur > Modifier toutes les propriétés > Valeur par défaut du serveur > ICA > Affichage) et définissez la Mémoire maximale à utiliser pour les graphiques de chaque session.

Assurez-vous que la valeur du réglage (kilo-octets) permet de fournir une mémoire graphique suffisante. Si ce réglage est insuffisant, la ressource publiée se réduit au sous-ensemble d'écrans correspondant à la taille spécifiée.

Pour plus d'informations sur le calcul des exigences de mémoire graphique de la session pour XenApp et XenDesktop, consultez l'article CTX115637 du de centre de connaissances.

Remplacement de paramètres d'imprimante sur les machines

Si le paramètre de stratégie Valeurs par défaut de l'optimisation de l'impression universelleAutoriser les non-administrateurs à modifier ces paramètres est activé, les utilisateurs peuvent remplacer les options Compression d'image et Cache d'image et de police spécifiées dans ce paramètre de stratégie.

Pour remplacer les paramètres d'imprimante sur la machine utilisateur

1. À partir du menu Impression d'une application disponible sur la machine utilisateur, choisissez Propriétés.
2. Sur l'onglet Paramètres client, cliquez sur Optimisations avancées et apportez des modifications aux options Compression d'image et Cache d'image et de police.

Commande du clavier à l'écran

Pour activer l'accès tactile aux applications et bureaux virtuels à partir de tablettes Windows, Citrix Receiver pour Windows affiche automatiquement le clavier à l'écran lorsque vous activez un champ de saisie de texte, et lorsque l'appareil est en mode tente ou tablette.

Sur certains appareils et dans certaines circonstances, Citrix Receiver pour Windows ne parvient pas à détecter avec précision le mode de l'appareil, et le clavier à l'écran peut s'afficher lorsque vous ne souhaitez pas qu'il apparaisse.

Pour empêcher le clavier à l'écran d'apparaître lors de l'utilisation d'un appareil convertible, créez une valeur REG_DWORD DisableKeyboardPopup dans HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver et définissez-la sur 1.

Remarque : sur une machine x64, créez une valeur dans HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix Client\Engine\Configuration\Advanced\Modules\MobileReceiver.

Les 3 modes ci-après peuvent être utilisés pour définir les clés :

- **Automatique** : AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0
- **Toujours afficher** (clavier à l'écran) : AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0
- **Ne jamais afficher** (clavier à l'écran) : AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1

Raccourcis clavier

Vous pouvez configurer des combinaisons de touches auxquelles Receiver prête des fonctionnalités spéciales. Lorsque la stratégie de raccourcis clavier est activée, vous pouvez spécifier les mappages de touches de raccourci Citrix, le comportement des touches de raccourci Windows et la configuration du clavier pour les sessions.

1. En tant qu'administrateur, ouvrez la fenêtre Éditeur de stratégie de groupe en exécutant la commande gpedit.msc dans le menu Démarrer lorsque vous appliquez des stratégies sur un seul ordinateur ou en utilisant la Console de gestion des stratégies de groupe pour appliquer des stratégies de domaine.

   Remarque : si vous avez déjà importé le modèle Citrix Receiver pour Windows dans l'Éditeur de stratégies de groupe, vous pouvez ignorer les étapes 2 à 5.

2. Dans le panneau gauche de l'Éditeur de stratégie de groupe, sélectionnez le dossier Modèles d'administration.

3. À partir du menu Action, sélectionnez Ajout/Suppression de modèles.
4. Choisissez Ajouter et naviguez jusqu'au dossier Receiver Configuration (généralement, C:\Program Files\Citrix\ICA Client\Configuration) et sélectionnez le fichier de modèle Citrix Receiver pour Windows.
   Remarque : en fonction de la version du système d'exploitation Windows, sélectionnez le fichier de modèle Citrix Receiver pour Windows (receiver.adm ou receiver.admx/receiver.adml).
5. Cliquez sur Ouvrir pour ajouter le modèle, puis cliquez sur Fermer pour retourner à l'Éditeur de stratégie de groupe.
6. Dans l'Éditeur de stratégie de groupe, développez Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Receiver > Expérience utilisateur > Raccourcis clavier.
7. Dans le menu Action, choisissez Propriétés, sélectionnez Activé et choisissez les options souhaitées.

Prise en charge des icônes de couleurs 32 bits dans Citrix Receiver pour Windows

Citrix Receiver pour Windows prend en charge les icônes 65536 couleurs 32 bits et sélectionne automatiquement le nombre de couleurs des applications visibles dans la boîte de dialogue du Centre de connexion Citrix, le menu Démarrer et la barre des tâches pour fournir des applications en toute transparence.

Avertissement : toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Pour définir un nombre de couleurs, vous pouvez ajouter une clé de registre de chaîne intitulée TWIDesiredIconColor dans HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences et la régler à la valeur souhaitée. Le nombre de couleurs possible pour les icônes est de 4, 8, 16, 24 ou 32 bits par pixel. L'utilisateur peut sélectionner un nombre moindre de couleurs pour les icônes si le débit de la connexion réseau est faible.

Activation de Desktop Viewer

Différentes entreprises ont différents besoins d'entreprise. Votre configuration requise pour la manière dont les utilisateurs accèdent aux bureaux virtuels d'un utilisateur à un autre et peut varier lorsque vos besoins sont en constante évolution. L'expérience utilisateur relative à la connexion

aux bureaux virtuels et le degré d'intervention de l'utilisateur dans la configuration des connexions dépendent de la manière dont vous avez configuré Citrix Receiver pour Windows.

Utilisez **Desktop Viewer** lorsque vos utilisateurs doivent interagir avec leur bureau virtuel. Le bureau virtuel de l'utilisateur peut être un bureau virtuel publié ou un bureau dédié ou partagé. Dans ce scénario d'accès, la barre d'outils Desktop Viewer permet à l'utilisateur d'ouvrir un bureau virtuel dans une fenêtre et de faire défiler et mettre à l'échelle ce bureau au sein de son bureau local. Les utilisateurs peuvent définir des préférences et travailler avec plusieurs bureaux à l'aide de connexions XenDesktop multiples sur la même machine utilisateur.

Remarque : vos utilisateurs doivent utiliser Citrix Receiver pour Windows pour changer la résolution d'écran sur leurs bureaux virtuels. Ils ne peuvent pas changer la résolution d'écran à l'aide du Panneau de configuration de Windows.

Entrées clavier dans les sessions Desktop Viewer

Dans les sessions Desktop Viewer, la touche Windows+L est dirigée vers l'ordinateur local.

Ctrl+Alt+Suppr est dirigé vers l'ordinateur local.

Les touches qui activent les touches rémanentes, les touches filtres et les touches bascules (fonctionnalités d'accessibilité Microsoft) sont généralement dirigées vers l'ordinateur local.

En tant que fonctionnalité d'accessibilité de Desktop Viewer, la combinaison Ctrl+Alt+Attn affiche les boutons de la barre d'outils Desktop Viewer dans une fenêtre contextuelle.

Ctrl+Échap est envoyé au bureau virtuel distant.

Remarque : par défaut, si Desktop Viewer est agrandi, Alt+Tab active le focus entre les différentes fenêtres au sein de la session. Si Desktop Viewer est affiché dans une fenêtre, Alt+Tab active le focus entre les différentes fenêtres en dehors de la session.

Les séquences de raccourcis sont des combinaisons de touches conçues par Citrix. À titre d'exemple, la séquence Ctrl+F1 reproduit Ctrl+Alt+Suppr, et Maj+F2 permet de basculer les applications du mode plein écran au mode fenêtre, et vice versa. Vous ne pouvez pas utiliser de séquences de raccourcis avec des bureaux virtuels affichés dans Desktop Viewer (c'est-à-dire avec des sessions XenDesktop), mais vous pouvez les utiliser avec des applications publiées (c'est-à-dire avec des sessions XenApp).

Connexion aux bureaux virtuels

Depuis une session de bureau, les utilisateurs ne peuvent pas se connecter au même bureau virtuel. Une tentative de connexion déconnectera la session de bureau existante. C'est pourquoi Citrix recommande ce qui suit :

- Les administrateurs ne devraient pas configurer les clients sur un bureau afin de pointer vers un site qui publie le même bureau

- Les utilisateurs ne devraient pas effectuer une recherche vers un site qui héberge le même bureau, si le site est configuré pour reconnecter automatiquement les utilisateurs à des sessions existantes
- Les utilisateurs ne devraient pas effectuer une recherche vers un site qui héberge le même bureau et essayer de le démarrer

Rappelez-vous qu'un utilisateur qui ouvre une session localement sur un ordinateur agissant en tant que bureau virtuel bloque les connexions à ce bureau.

Si vos utilisateurs se connectent à des applications virtuelles (publiées avec XenApp) depuis un bureau virtuel et que votre organisation possède un administrateur XenApp distinct, Citrix recommande de travailler en collaboration avec ces derniers pour définir le mappage de machines de sorte que les machines de bureaux soient mappées de façon cohérente dans les sessions de bureau et d'application. Les lecteurs locaux étant affichés en tant que lecteurs réseau dans les sessions de bureau, l'administrateur XenApp doit changer la stratégie de mappage de lecteur afin d'inclure les lecteurs réseau.

Modification du délai de l'indicateur d'état

Vous pouvez modifier la durée pendant laquelle l'indicateur d'état s'affiche lorsqu'un utilisateur lance une session. Pour modifier cette durée, créez une valeur REG_DWORD de SI INACTIVE MS dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\. La valeur REG_DWORD peut être réglée sur 4 si vous voulez que l'indicateur d'état disparaisse plus tôt.

CEIP (programme d'amélioration de l'expérience du client)

> **Remarque**
>
> Vous pouvez masquer tout ou partie de la page Préférences avancées disponible à partir de l'icône Citrix Receiver dans la zone de notification. Pour plus d'informations, veuillez consulter Masquer la page Préférences avancées.

Le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) rassemble des données de configuration et d'utilisation anonymes à partir de Receiver pour Windows et les envoie automatiquement à Citrix. Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de Receiver.

Le programme CEIP ne collecte aucune information liée à l'environnement du client permettant d'identifier l'utilisateur.

Conseil : vous pouvez modifier votre participation au programme CEIP dans l'interface de Receiver. Vous disposez de 7 jours pour désactiver le programme CEIP après l'installation.

Pour désactiver le programme CEIP ou ne pas y participer :

1. Cliquez avec le bouton droit sur l'icône de Citrix Receiver dans la zone de notification.
2. Sélectionnez **Préférences avancées**.
   La fenêtre Préférences avancées s'affiche.
3. Sélectionnez **Collecte de données**.
4. Sélectionnez **Non merci** pour désactiver le programme CEIP ou ne pas y participer.
5. Cliquez sur **Enregistrer**.

Mise à l'échelle DPI

June 27, 2019

Citrix Receiver pour Windows permet au système d'exploitation de contrôler la résolution de la session.

Vous pouvez appliquer une résolution élevée dans une session, mais la fonctionnalité est désactivée par défaut. Cela signifie que la mise à l'échelle de la session suit la résolution du système d'exploitation.

Vous pouvez configurer la mise à l'échelle DPI en utilisant les options suivantes :

1. Modèle d'administration d'objet de stratégie de groupe (configuration par machine)
2. Préférences avancées (configuration par utilisateur)

Limitations

- Même lorsque cette fonctionnalité est activée, un léger flou est observé dans le Desktop Viewer.
- Dans une session, lorsque vous modifiez les paramètres DPI et que vous la relancez, la taille de la fenêtre de session peut ne pas être appropriée.
  Pour contourner le problème, redimensionnez la fenêtre de session.

Pour configurer la mise à l'échelle DPI à l'aide du modèle d'administration de l'objet de stratégie de groupe Citrix Receiver

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud Configuration ordinateur, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Receiver** > **DPI**.
3. Sélectionnez la stratégie **DPI élevé**.
4. Modifiez les paramètres selon vos besoins.

5. Cliquez sur Appliquer, puis sur OK.
6. Exécutez la commande `gpupdate /force` à partir d'une ligne de commande.

Pour configurer la mise à l'échelle DPI à l'aide de l'interface utilisateur graphique

> **Remarque**
>
> Vous pouvez masquer tout ou partie de la page Préférences avancées disponible à partir de l'icône Citrix Receiver dans la zone de notification. Pour plus d'informations, veuillez consulter Masquer la page Préférences avancées.

1. Faites un clic droit sur Citrix Receiver pour Windows dans la zone de notification.
2. Sélectionnez **Préférences avancées** et cliquez sur **Paramètres DPI**.
   La boîte de dialogue DPI s'ouvre.
3. Modifiez les paramètres selon vos besoins.
   L'option **Laisser le système d'exploitation régler la résolution** est sélectionnée par défaut.
4. Cliquez sur **Enregistrer**.

Redémarrez la session Citrix Receiver pour Windows pour que les modifications soient prises en compte.

Pour plus d'informations sur la résolution des problèmes liés à la mise à l'échelle DPI, consultez l'article CTX230017 du centre de connaissances.

Codage vidéo H.265

November 16, 2018

Citrix Receiver pour Windows prend en charge l'utilisation du codec vidéo H.265 pour l'accélération matérielle des graphiques et vidéos distants. Pour bénéficier de cette fonctionnalité, elle doit être prise en charge et activée à la fois sur le VDA et sur Citrix Receiver pour Windows. Si le GPU du point de terminaison ne prend pas en charge le décodage H.265 à l'aide de l'interface DXVA, le paramètre de stratégie de décodage H265 pour les graphiques est ignoré et la session utilise le codec vidéo H.264.

Conditions préalables

1. VDA 7.16 et versions ultérieures.
2. Activez la stratégie **Optimiser pour la charge des graphiques 3D** sur le VDA.
3. Activez la stratégie **Utiliser le codage matériel pour le codec vidéo** sur le VDA.

Remarque : le codage H.265 est pris en charge uniquement sur le GPU NVIDIA.

Dans Citrix Receiver pour Windows, cette fonctionnalité est définie sur **Désactivé** par défaut.

Configuration de Citrix Receiver pour Windows pour utiliser le codage vidéo H.265 à l'aide du modèle d'administration d'objet de stratégie de groupe Citrix

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Citrix Receiver** > **Expérience utilisateur**.
3. Sélectionnez la stratégie **Décodage H265 pour graphiques**.
4. Sélectionnez **Activé**.
5. Cliquez sur **Appliquer**, puis sur **OK**.

Configuration de Citrix Receiver pour Windows pour utiliser le codage vidéo H.265 à l'aide de l'Éditeur du Registre

Activation du codage vidéo H.265 sur un réseau n'appartenant pas au domaine sur un système d'exploitation 32 bits :

1. Lancez l'Éditeur du Registre en tapant regedit dans la commande Exécuter.
2. Accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Graphics Engine.
3. Créez une clé DWORD nommée EnableH265 et définissez la valeur de la clé sur 1.

Activation du codage vidéo H.265 sur un réseau n'appartenant pas au domaine sur un système d'exploitation 64 bits :

1. Lancez l'Éditeur du Registre en tapant regedit dans la commande Exécuter.
2. Accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine.
3. Créez une clé DWORD nommée EnableH265 et définissez la valeur de la clé sur 1.

Redémarrez la session pour que les modifications prennent effet.

> **Remarque**
>
> - Si la stratégie **Accélération matérielle pour graphiques** est désactivée dans le modèle d'administration de l'objet de stratégie de groupe Citrix Receiver, les paramètres de la stratégie **Décodage H265 pour graphiques** sont ignorés et la fonctionnalité ne fonctionne pas.
> - Exécutez l'outil HDX Monitor 3.x pour identifier si l'encodeur vidéo H.265 est activé dans les sessions. Pour plus d'informations sur l'outil HDX Monitor 3.x, consultez l'article CTX135817 du centre de connaissances.

Lancement de vPrefer

July 15, 2019

Configuration du lancement de vPrefer à l'aide du modèle d'administration d'objet de stratégie de groupe

Dans les versions antérieures, l'instance d'une application installée sur le VDA (appelée instance locale dans ce document) pouvait être lancée de préférence à l'application publiée en définissant l'attribut KEYWORDS:prefer = "application" dans Citrix Studio.

À partir de la version 4.11, dans un scénario double-hop (où Citrix Receiver s'exécute sur le VDA hébergeant votre session), vous pouvez désormais contrôler si Receiver lance l'instance locale d'une application installée sur le VDA (si disponible en tant qu'application locale) plutôt qu'une instance hébergée de l'application.

vPrefer est disponible sur StoreFront version 3.14 et XenApp 7.17 et versions ultérieures.

Lorsque vous lancez l'application, Citrix Receiver pour Windows lit les données de ressources présentes sur le serveur StoreFront et applique les paramètres basés sur l'indicateur **vprefer** au moment de l'énumération. Citrix Receiver pour Windows recherche le chemin d'installation de l'application dans le registre Windows sur le VDA et, s'il est présent, lance l'instance locale de l'application. Sinon, une instance hébergée de l'application est lancée.
Si vous lancez une application qui n'est pas installée sur le VDA, l'application hébergée est lancée. Pour plus d'informations sur la gestion du lancement local sur StoreFront, consultez la section Contrôle du lancement local d'applications sur des bureaux publiés dans la documentation de StoreFront.

Si vous ne voulez pas que l'instance locale de l'application soit lancée sur le VDA, définissez **LocalLaunchDisabled** sur **True** à l'aide de PowerShell sur Delivery Controller. Pour de plus amples informations, consultez la documentation de Citrix Virtual Apps and Desktops

Cette fonctionnalité permet de lancer des applications plus rapidement, offrant ainsi une meilleure expérience utilisateur. Vous pouvez configurer cette fonctionnalité avec le modèle d'administration d'objet de stratégie de groupe. Par défaut, vPrefer est activé uniquement dans un scénario double-hop.

> **Remarque**
>
> Lorsque vous mettez à niveau ou installez Citrix Receiver pour Windows pour la première fois, vous devez ajouter les derniers fichiers de modèle à l'objet de stratégie de groupe local. Pour plus d'informations sur l'ajout des fichiers de modèle à l'objet de stratégie de groupe local, consultez la section Configuration du modèle d'administration d'objet de stratégie de groupe. En cas de

> mise à niveau, les paramètres existants sont conservés lors de l'importation des derniers fichiers.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud Configuration ordinateur, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Receiver** > **Libre-service**.
3. Sélectionnez la stratégie **vPrefer**.
4. Sélectionnez **Activé** et, à partir du menu déroulant **Autoriser applications**, sélectionnez l'une des options suivantes :
    a) **Autoriser toutes les applications** : cette option lance l'instance locale de toutes les applications sur le VDA. Citrix Receiver pour Windows recherche l'application installée (y compris les applications Windows natives telles que Bloc-notes, Calculatrice, Wordpad, Invite de commandes) et lance l'application sur le VDA au lieu de l'application hébergée.
    b) **Autoriser les applications installées** : cette option lance l'instance locale de l'application installée sur le VDA. Si l'application n'est pas installée sur le VDA, elle lance l'application hébergée. Par défaut, l'option **Autoriser les applications installées** est sélectionnée lorsque la stratégie **vPrefer** est définie sur **Activé**. Cette option exclut les applications natives du système d'exploitation Windows telles que le Bloc-notes, la Calculatrice, etc.
    c) **Autoriser les applications réseau** : cette option lance l'instance d'une application publiée sur un réseau partagé.
5. Cliquez sur **Appliquer**, puis sur **OK**.
6. Redémarrez la session pour que les modifications prennent effet.

Limitation :

- Receiver pour Web ne prend pas en charge cette fonctionnalité.

Pour plus d'informations sur la fonctionnalité vPrefer, consultez l'article CTX232210 du centre de connaissances.

Éditeurs IME clients génériques

June 27, 2019

Configuration d'éditeurs IME clients génériques l'aide de l'interface de ligne de commande

Pour activer l'éditeur IME client générique, exécutez la commande **wfica32.exe /localime:on** à partir du dossier d'installation de Citrix Receiver pour Windows (C:\Program Files (x86)\Citrix\ICA Client).

> **Remarque**
>
> Vous pouvez utiliser le commutateur de ligne de commande **wfica32.exe /localime:on** pour activer l'éditeur IME client générique et la synchronisation de la disposition du clavier.

Pour déactiver l'éditeur IME client générique, exécutez la commande **wfica32.exe /localgenericime:off** à partir du dossier d'installation de Citrix Receiver pour Windows (C:\Program Files (x86)\Citrix\ICA Client). Cette commande n'affecte pas les paramètres de synchronisation de la disposition du clavier.

Si vous avez désactivé l'éditeur IME client générique à l'aide de l'interface de ligne de commande, vous pouvez activer la fonctionnalité de nouveau en exécutant la commande **wfica32.exe /localgenericime:on**.

Activer/désactiver

Citrix Receiver pour Windows permet d'activer ou de désactiver cette fonctionnalité. Vous pouvez exécuter la commande **wfica32.exe /localgenericime:on** pour activer ou désactiver la fonctionnalité. Toutefois, les paramètres de synchronisation de disposition du clavier ont priorité sur le commutateur à bascule. Si la synchronisation de la disposition du clavier est définie sur **Off**, le basculement n'active pas l'éditeur IME client générique.

Configuration d'éditeurs IME clients génériques l'aide de l'interface utilisateur graphique

L'éditeur IME client générique requiert la version 7.13 ou ultérieure du VDA.

La fonctionnalité d'éditeur IME client générique peut être activée en activant la synchronisation de la disposition du clavier. Pour plus d'informations, veuillez consulter Synchronisation de la disposition du clavier.

Citrix Receiver pour Windows vous permet de configurer différentes options d'utilisation de l'éditeur IME client générique. Vous pouvez sélectionner l'une ces options en fonction de vos exigences et de votre utilisation.

1. Dans une session d'application active, cliquez avec le bouton droit sur l'icône de Citrix Receiver dans la zone de notification et sélectionnez **Centre de connexion**.
2. Sélectionnez **Préférences** et cliquez sur **Éditeur IME local**.

Les options ci-dessous sont disponibles pour prendre en charge différents modes IME :

1. **Activer l'éditeur IME du serveur** : sélectionnez cette option pour désactiver l'éditeur IME local. Cette option signifie que seules les langues définies sur le serveur peuvent être utilisées.

2. **Définir l'éditeur IME local sur le mode Performances élevées** : sélectionnez cette option pour utiliser l'éditeur IME local avec une bande passante limitée. Cette option limite la fonctionnalité de fenêtre candidate.
3. **Définir l'éditeur IME local sur le mode Expérience optimale** : sélectionnez cette option pour utiliser l'éditeur IME local avec une expérience utilisateur optimale. Cette option consomme beaucoup de bande passante. Par défaut, cette option est sélectionnée lorsque l'éditeur IME client générique est activé.

Les modifications apportées aux paramètres sont appliquées uniquement dans la session en cours.

Activation de touches de raccourci à l'aide d'un éditeur de Registre

Lorsque l'éditeur IME client générique est activé, vous pouvez utiliser la combinaison **MAJ+F4** pour sélectionner différents mode IME. Les différentes options des modes IME s'affichent dans le coin supérieur droit de la session.

Par défaut, la touche de raccourci de l'éditeur IME client générique est désactivée.

Dans l'Éditeur du Registre, accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys.

Sélectionnez **AllowHotKey** et modifiez la valeur par défaut sur 1.

> **Remarque**
>
> Les touches de raccourci sont prises en charge dans les sessions d'application et de bureau.

Limitations

- L'éditeur IME client générique ne prend pas en charge les applications UWP (plate-forme Windows universelle) telles que l'interface utilisateur de la recherche et le navigateur Edge du système d'exploitation Windows 10. Pour contourner le problème, utilisez l'éditeur IME du serveur.
- L'éditeur IME client générique n'est pas pris en charge sur Internet Explorer version 11 en **Mode protégé**. Pour contourner le problème, vous pouvez désactiver le Mode protégé en utilisant les **Options Internet**. Pour ce faire, cliquez sur **Sécurité** et décochez **Activer le mode protégé**.

Clavier et barre de langue

June 27, 2019

Configuration du clavier

> **Remarque**
>
> Vous pouvez masquer tout ou partie de la page Préférences avancées disponible à partir de l'icône Citrix Receiver dans la zone de notification. Pour plus d'informations, veuillez consulter Masquer la page Préférences avancées.

La synchronisation de la disposition du clavier permet aux utilisateurs de basculer entre leurs dispositions de clavier préférées sur la machine cliente. Cette fonction est désactivée par défaut.

Pour activer la synchronisation de la disposition du clavier :

1. À partir de l'icône Citrix Receiver pour Windows dans la zone de notification, sélectionnez **Préférences avancées** > **Clavier et barre de langue**. La fenêtre Clavier et barre de langue apparaît.
2. Cliquez sur **Enregistrer**.

Vous pouvez désactiver la fonctionnalité en sélectionnant **Non**.

Vous pouvez également activer ou désactiver la synchronisation de la disposition du clavier via la ligne de commande en exécutant **wfica32:exe /localime:on** ou **wfica32:exe /localime:off** depuis le dossier d'installation de Citrix Receiver pour Windows (C:\program files (x86)\Citrix\ICA Client).

> **Remarque :**
>
> l'utilisation de l'option de disposition du clavier local active l'éditeur IME (Éditeur de méthode d'entrée) du client. Si les utilisateurs qui travaillent en japonais, chinois simplifié ou coréen préfèrent utiliser l'éditeur IME du serveur, ils doivent désactiver l'option de disposition du clavier local en sélectionnant **Non** ou en exécutant **wfica32:exe /localime:off**. La session va rétablir la disposition du clavier fournie par le serveur distant lorsqu'ils se connectent à la prochaine session.

Parfois, le basculement vers la disposition du clavier de la machine cliente ne prend pas effet dans une session active. Pour résoudre ce problème, fermez la session de Citrix Receiver pour Windows et reconnectez-vous.

Limitations :

- Les applications distantes exécutées avec des privilèges élevés (par exemple, clic droit sur l'icône d'une application > Exécuter 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 du côté serveur (VDA) ou désactivez le contrôle de compte d'utilisateur.
- Si l'utilisateur change la disposition du clavier sur le client au profit d'une disposition qui n'est pas prise en charge sur le serveur, la fonctionnalité de synchronisation de la disposition du clavier sera désactivée pour des raisons de sécurité - une disposition de clavier non reconnue est considérée comme une menace potentielle pour la sécurité. Pour rétablir la fonctionnalité

de synchronisation de la disposition du clavier, les utilisateurs doivent fermer leur session et la rouvrir.

- Lorsque RDP est déployé en tant qu'application et que l'utilisateur travaille au sein d'une session RDP, il n'est pas possible de modifier la disposition du clavier à l'aide du raccourci Alt + Maj. Pour contourner ce problème, l'utilisateur peut utiliser la barre de langue dans la session RDP pour changer la disposition du clavier.
- Cette fonctionnalité est désactivée dans Windows Server 2016 en raison d'un problème de tiers pouvant affecter les performances. Cette fonctionnalité peut être activée avec un paramètre de registre sur le VDA : dans HKLM\Software\Citrix\ICA\IcaIme, ajoutez une nouvelle clé appelée DisableKeyboardSync et définissez la valeur sur 0.

Barre de langue

À partir de la version 4.11, vous pouvez choisir d'afficher ou de masquer la barre de langue distante dans une session d'application à l'aide de l'interface utilisateur graphique. La barre de langue affiche la langue d'entrée préférée dans une session. Dans les versions antérieures, vous pouviez modifier ce paramètre en utilisant uniquement les clés de registre du VDA. À partir de Citrix Receiver pour Windows version 4.11, vous pouvez modifier les paramètres à l'aide de la boîte de dialogue **Préférences avancées** dans Citrix Receiver pour Windows. La barre de langue apparaît dans une session par défaut.

> **Remarque**
>
> Cette fonctionnalité est disponible dans les sessions exécutées sur VDA 7.17 et versions ultérieures.

Configurer l'affichage ou le masquage de la barre de langue distante

1. Cliquez avec le bouton droit sur l'icône Citrix Receiver pour Windows dans la zone de notification et sélectionnez **Préférences avancées**.
2. Sélectionnez **Clavier et barre de langue**.
3. Sélectionnez l'onglet **Barre de langue**.
4. Modifiez les paramètres selon vos besoins.

> **Remarque**
>
> - Les modifications de paramètres prennent effet immédiatement.
> - Vous pouvez modifier les paramètres dans une session active.
> - La barre de langue distante n'apparaît pas dans une session s'il n'y a qu'une seule langue d'entrée.

Masquer l'onglet de la barre de langue de la page Préférences avancées

Vous pouvez masquer l'onglet de la barre de langue à partir de la page **Préférences avancées** en utilisant le registre.

1. Lancez l'Éditeur du Registre.
2. Accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\L
3. Créez une nouvelle clé de valeur DWORD, **ToggleOffLanguageBarFeature**, et définissez-la sur **1** pour masquer l'option de la barre de langue dans la page Préférences avancées.

Authentification

August 1, 2018

Pour maximiser la sécurité de votre environnement, les connexions entre Citrix Receiver pour Windows et les ressources que vous publiez doivent être protégées. Vous pouvez configurer plusieurs types d'authentification pour votre logiciel Citrix Receiver pour Windows, y compris l'authentification par carte à puce, la vérification des listes de révocation de certificats et l'authentification pass-through Kerberos.

Configurer l'authentification pass-through au domaine

December 13, 2019

Single Sign-on vous permet de vous authentifier auprès d'un domaine et d'utiliser des applications et des bureaux mis à disposition par ce domaine sans avoir à vous authentifier de nouveau pour chaque application ou bureau.

Lorsque vous ouvrez une session sur Citrix Receiver, vos informations d'identification sont transmises à StoreFront, ainsi que les applications et bureaux énumérés pour vous, y compris les paramètres du menu Démarrer. Après avoir configuré Single Sign-on, vous pouvez ouvrir une session sur Citrix Receiver et lancer des sessions XenApp ou XenDesktop sans avoir à entrer vos informations d'identification à plusieurs reprises.

Lorsque vous cliquez sur une icône, Citrix Receiver transmet vos informations d'identification de domaine au Delivery Controller et l'application (ou le bureau) s'ouvre.

Vous pouvez configurer Single Sign-on lors de l'installation de Citrix Receiver à l'aide d'une des options suivantes :

- Interface de ligne de commande
- Interface utilisateur graphique

Pré-requis

1. Ajoutez le serveur StoreFront à la liste de sites de confiance à l'aide d'Internet Explorer. Pour ce faire :
   a) Démarrez Internet Explorer.
   b) Sélectionnez **Outils** > **Options Internet** > **Sécurité** > **Internet Local** et cliquez sur **Sites**. La fenêtre **Intranet Local** s'affiche.
   c) Sélectionnez **Avancé**.
   d) Ajoutez l'adresse URL de StoreFront ou le nom de domaine complet de l'Interface Web avec les protocoles HTTP ou HTTPS appropriés.
   e) Cliquez sur Appliquer, puis sur OK.
2. Modifiez les paramètres **Authentification utilisateur** dans Internet Explorer. Pour ce faire :
   a) Démarrez Internet Explorer.
   b) Dans **Options Internet** > **Sécurité**, sélectionnez **Sites de confiance**.
   c) Cliquez sur **Personnaliser le niveau**. La fenêtre **Paramètres de sécurité – Zone Sites de confiance** s'affiche.
   d) Dans le panneau **Authentification utilisateur**, sélectionnez **Ouverture de session automatique avec le nom d'utilisateur et le mot de passe actuel**.

Configuration de Single Sign-on à l'aide de l'interface de ligne de commande

Installez Citrix Receiver pour Windows à l'aide du commutateur **/includeSSON**.

Redémarrez Receiver pour Windows pour que les modifications soient prises en compte.

> **Remarque**
>
> Si Citrix Receiver est installé sans le composant Single Sign-on, la mise à niveau vers la dernière version de Citrix Receiver avec le commutateur **/includeSSON** n'est pas prise en charge.

Configuration de Single Sign-on à l'aide de l'interface utilisateur graphique

1. Recherchez le fichier d'installation de Citrix Receiver pour Windows (CitrixReceiver.exe).
2. Cliquez deux fois sur **CitrixReceiver.exe** pour lancer le programme d'installation.
3. Dans l'assistant d'installation Activer le single sign-on, sélectionnez la case Activer le single sign-on pour installer Citrix Receiver pour Windows avec la fonctionnalité SSON activée ; cela équivaut à installer Citrix Receiver pour Windows à l'aide de la ligne de commande avec l'indicateur **/includeSSON**.

L'image ci-dessous illustre comment activer l'authentification unique :

Configuration de Single Sign-on sur Receiver pour Web

Vous pouvez configurer Single Sign-on pour Receiver pour Web à l'aide du modèle d'administration d'objet de stratégie de groupe.

Remarque : lorsque vous mettez à niveau ou installez Citrix Receiver pour Windows pour la première fois, vous devez ajouter les derniers fichiers de modèle à l'objet de stratégie de groupe local. Pour plus d'informations sur l'ajout des fichiers de modèle à l'objet de stratégie de groupe local, consultez la section https://docs.citrix.com/fr-fr/receiver/windows/current-release/configure/config-gpo-template.html. Lorsque vous procédez à la mise à niveau, les paramètres existants sont conservés lors de l'importation des derniers fichiers.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Receiver** > **Authentification utilisateur**.
3. Sélectionnez la stratégie **Nom d'utilisateur et mot de passe locaux** et définissez-la sur **Activé**.
4. Cliquez sur **Activer l'authentification pass-through**. Cette option permet à Citrix Receiver d'utiliser vos informations d'identification d'ouverture de session pour l'authentification sur le serveur distant.
5. Cliquez sur **Autoriser l'authentification pass-through pour toutes les connexions ICA**. Cette option ignore toute restriction d'authentification et autorise l'authentification pass-through des informations d'identification pour toutes les connexions.
6. Cliquez sur **Appliquer**, puis sur **OK**.
7. Redémarrez Citrix Receiver pour Windows pour Web pour que les modifications soient prises en compte.

Vérifiez que Single Sign-On est activé en démarrant Citrix Receiver. Après le lancement de Receiver, démarrez le Gestionnaire des tâches et vérifiez si le processus ssonsvr.exe est exécuté.

Permettre au Delivery Controller de faire confiance à XML

Utilisez la procédure suivante pour configurer le Single Sign-on sur StoreFront et l'Interface Web :

1. Connectez-vous au Delivery Controller en tant qu'administrateur.
2. Ouvrez Windows PowerShell (avec des privilèges d'administration). À l'aide de PowerShell, vous pouvez émettre des commandes visant à permettre à Delivery Controller de faire confiance aux requêtes XML provenant de StoreFront.
3. Tapez **Add-PSSnapin Citrix*** et appuyez sur **Entrée**.
4. Tapez **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True** et appuyez sur **Entrée**.
5. Fermez PowerShell.

Configuration de Single Sign-On sur StoreFront et l'Interface Web

Configuration du StoreFront

Pour configurer SSON sur StoreFront et l'Interface Web, ouvrez Citrix Studio sur le serveur StoreFront et sélectionnez **Authentification -> Ajouter/supprimer des méthodes**. Sélectionnez **Authentification pass-through au domaine**.

Configuration de l'Interface Web

Pour configurer SSON sur l'Interface Web, sélectionnez **Gestion de l'Interface Web Citrix -> Sites XenApp Services -> Méthodes d'authentification** et activez **Authentification pass-through**.

Utilisation de l'Outil d'analyse de la configuration pour valider la configuration de Single Sign-On

L'Outil d'analyse de la configuration vous permet d'exécuter un test pour vous assurer que Single Sign-On est correctement configuré. Le test est exécuté sur les différents points de contrôle de la configuration de l'authentification unique et affiche les résultats de la configuration.

1. Cliquez avec le bouton droit sur Citrix Receiver pour Windows dans la zone de notification et sélectionnez **Préférences avancées**.
2. Cliquez sur **Outil d'analyse de la configuration**.
   La fenêtre correspondante s'affiche.
3. Sélectionnez **SSONChecker** dans le volet **Sélectionner**.
4. Cliquez sur **Exécuter**. Une barre de progression apparaît, affichant l'état du test.

La fenêtre Outil d'analyse de la configuration comporte les colonnes suivantes :

1. **État** : affiche le résultat d'un test sur un point de contrôle.
   - Une coche verte indique que le point de contrôle est correctement configuré.
   - Un I bleu indique des informations sur le point de contrôle.
   - Un X rouge indique que le point de contrôle n'est pas configuré correctement.
2. **Fournisseur :** affiche le nom du module sur lequel le test est exécuté. Dans ce cas, Single Sign-on.
3. **Suite :** indique la catégorie du test. Par exemple, Installation.
4. **Test** : indique le nom du test qui est exécuté.
5. **Détails** : fournit des informations supplémentaires sur le test, indépendamment de la réussite ou de l'échec.

L'utilisateur dispose de plus d'informations sur chaque point de contrôle et les résultats correspondants.

Les tests suivants sont effectués :

1. Installé avec Single Sign-on
2. Capture des informations d'identification d'ouverture de session
3. Enregistrement du fournisseur réseau : le résultat du test pour l'enregistrement du fournisseur de réseau affiche une coche verte uniquement si « Citrix Single Sign-On » est défini en tant que premier élément dans la liste des fournisseurs de réseau. Si Citrix Single Sign-On s'affiche ailleurs dans la liste, le résultat de test pour l'inscription du fournisseur réseau s'affiche avec un I bleu et des informations supplémentaires.
4. Processus de Single Sign-On en cours d'exécution
5. Stratégie de groupe : par défaut, cette stratégie est configurée sur le client.
6. Paramètres Internet pour les zones de sécurité : assurez-vous que vous ajoutez le magasin/l'adresse URL du service XenApp à la liste des zones de sécurité dans les Options Internet. Si les zones de sécurité sont configurées via une stratégie de groupe, toute modification de la stratégie requiert que la fenêtre Préférences avancées soit rouverte pour que les modifications soient prises en compte et afficher l'état correct du test.
7. Méthode d'authentification pour l'Interface Web ou StoreFront.

> **Remarque**
>
> - Si vous accédez à Receiver pour Web, les résultats du test ne sont pas applicables. Si Citrix Receiver pour Windows est configuré pour plusieurs magasins, les tests de méthode d'authentification sont exécutés sur tous les magasins configurés.
> - Vous pouvez enregistrer les résultats du test sous forme de rapports. Le format par défaut du rapport est .txt.
> - Si vous accédez à Receiver pour Web, les résultats du test ne sont pas applicables.
> - Si Citrix Receiver pour Windows est configuré pour plusieurs magasins, les tests de méthode d'authentification sont exécutés sur tous les magasins configurés.
> - Vous pouvez enregistrer les résultats du test sous forme de rapports. Le format par défaut du rapport est .txt.
> - Si vous accédez à Receiver pour Web, les résultats du test ne sont pas applicables.
> - Si Citrix Receiver pour Windows est configuré pour plusieurs magasins, les tests de méthode d'authentification sont exécutés sur tous les magasins configurés.
> - Vous pouvez enregistrer les résultats du test sous forme de rapports. Le format par défaut du rapport est .txt.
>   - Si vous accédez à Receiver pour Web, les résultats du test ne sont pas applicables.
>   - Si Citrix Receiver pour Windows est configuré pour plusieurs magasins, les tests de méthode d'authentification sont exécutés sur tous les magasins configurés.
>   - Vous pouvez enregistrer les résultats du test sous forme de rapports. Le format par défaut du rapport est .txt.

Pour plus d'informations sur la configuration de l'authentification pass-through du domaine, consul-

tez l'article CTX133982 du centre de connaissances.

Masquer l'outil d'analyse de la configuration dans la fenêtre Préférences avancées

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Accédez à **Composants Citrix** > **Citrix Receiver** > **Libre-service** > **DisableConfigChecker**.
3. Cliquez sur **Activé** pour masquer l'option Outil d'analyse de la configuration dans la fenêtre Préférences avancées.
4. Cliquez sur **Appliquer**, puis sur **OK**.
5. Ouvrez une invite de commandes.
6. Exécutez la commande gpupdate /force.

Limitation

L'outil d'analyse de la configuration ne comprend pas le point de contrôle pour la configuration de l'option Faire confiance aux requêtes envoyées au service XML sur les serveurs XenApp et XenDesktop.

Configuration de l'authentification par carte à puce

March 26, 2019

Citrix Receiver pour Windows prend en charge les fonctionnalités d'authentification par carte à puce suivantes. Pour de plus amples informations sur la configuration de XenDesktop et de StoreFront, reportez-vous à la documentation accompagnant ces composants. Cette rubrique décrit la configuration de Citrix Receiver pour Windows pour les cartes à puce.

- **Authentification pass-through (Single Sign-On)** : l'authentification pass-through capture les informations d'identification de la carte à puce lorsque les utilisateurs ouvrent une session sur Citrix Receiver pour Windows. Citrix Receiver pour Windows utilise les informations d'identification capturées comme suit :
  - Les utilisateurs dont les machines appartiennent au domaine qui ouvrent une session Citrix Receiver pour Windows avec des informations d'identification de carte à puce peuvent démarrer des applications et bureaux virtuels sans avoir à s'authentifier de nouveau.
  - Les utilisateurs dont les machines n'appartiennent pas au domaine qui ouvrent une session Citrix Receiver pour Windows avec des informations d'identification de carte à puce doivent de nouveau entrer leurs informations d'identification pour démarrer une application ou un bureau virtuel.

L'authentification pass-through requiert la configuration de StoreFront et Citrix Receiver pour Windows.

- **Authentification bimodale** : l'authentification bimodale offre aux utilisateurs le choix entre utiliser une carte à puce et entrer leur nom d'utilisateur et mot de passe. Cette fonctionnalité est utile si la carte à puce ne peut pas être utilisée (par exemple, si l'utilisateur l'a laissé chez lui, ou que le certificat d'ouverture de session a expiré). Les magasins dédiés doit être configurés par site pour autoriser ceci, à l'aide de la méthode DisableCtrlAltDel définie sur False pour autoriser les cartes à puce. L'authentification bimodale requiert la configuration de StoreFront. Si NetScaler Gateway est présent dans la solution, une configuration est également nécessaire.

  L'authentification bimodale offre également désormais à l'administrateur StoreFront l'opportunité d'offrir à l'utilisateur final à la fois l'authentification par nom d'utilisateur et mot de passe et par carte à puce pour le même magasin en les sélectionnant dans la console StoreFront. Consultez la documentation de StoreFront.

- **Certificats multiples** : de multiples certificats peuvent être disponibles pour une seule carte à puce et si plusieurs cartes à puce sont utilisées. Lorsqu'un utilisateur insère une carte à puce dans le lecteur de cartes, les certificats sont disponibles à toutes les applications exécutées sur la machine utilisateur, y compris Citrix Receiver pour Windows. Pour modifier la façon dont les certificats sont sélectionnés, configurez Citrix Receiver pour Windows.

- **Authentification du certificat client** : l'authentification du certificat client requiert la configuration de NetScaler Gateway et de StoreFront.

  - Pour accéder aux ressources StoreFront via NetScaler Gateway, les utilisateurs auront peut-être besoin de se ré-authentifier après le retrait d'une carte à puce.
  - Lorsque la configuration SSL de NetScaler Gateway est définie sur authentification du certificat client obligatoire, la sécurité des opérations est garantie. Toutefois, l'authentification du certificat client obligatoire n'est pas compatible avec l'authentification bimodale.

- **Sessions double-hop** : si un double-hop est requis, une connexion supplémentaire est établie entre Receiver et le bureau virtuel de l'utilisateur. Les déploiements qui prennent en charge le double-hop sont décrits dans la documentation XenDesktop.

- **Applications activées pour carte à puce** : les applications activées pour carte à puce, telles que Microsoft Outlook et Microsoft Office, permettent aux utilisateurs de signer numériquement ou de crypter des documents disponibles dans les sessions d'application ou de bureau virtuel.

Conditions préalables

Cette rubrique suppose que vous avez lu les rubriques relatives aux cartes à puce dans la documentation de XenDesktop de StoreFront.

Limitations

- Les certificats doivent être stockés sur une carte à puce et non sur la machine utilisateur.
- Citrix Receiver pour Windows ne peut pas enregistrer le choix de certificat de l'utilisateur, mais peut stocker le code PIN lors de la configuration. Le code PIN est uniquement mis en cache dans la mémoire non paginée pour la durée de la session de l'utilisateur et n'est, à aucun moment, stocké sur disque.
- Citrix Receiver pour Windows ne reconnecte pas les sessions lorsqu'une carte à puce est insérée.
- Lorsque Citrix Receiver pour Windows est configuré pour utiliser l'authentification par carte à puce, il ne prend ni en charge le Single Sign-On VPN ni le pré-lancement de session. Pour utiliser les tunnels VPN avec l'authentification par carte à puce, les utilisateurs doivent installer NetScaler Gateway Plug-in et ouvrir une session via une page Web, et utiliser leurs cartes à puce et codes PIN pour s'authentifier à chaque étape. L'authentification pass-through à StoreFront avec NetScaler Gateway Plug-in n'est pas disponible pour les utilisateurs de cartes à puce.
- Les communications de Citrix Receiver pour Windows Updater avec citrix.com et Merchandising Server ne sont pas compatibles avec l'authentification par carte à puce sur NetScaler Gateway.

> **Avertissement**
>
> certaines des configurations décrites dans cette rubrique impliquent de modifier le registre. Une utilisation incorrecte de l'Éditeur du Registre peut occasionner de sérieux problèmes qui pourraient nécessiter l'installation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à effectuer une copie de sauvegarde avant de modifier le registre.

Pour activer le Single Sign-On (SSO) pour l'authentification par carte à puce

Pour configurer Citrix Receiver pour Windows, incluez l'option de ligne de commande suivante lors de son installation :

- ENABLE_SSON=Yes

  L'authentification pass-through est également appelée Single Sign-On (SSO). L'activation de ce paramètre empêche Citrix Receiver pour Windows d'afficher une seconde invite de saisie du code PIN.

Vous pouvez également effectuer la configuration en apportant des modifications aux stratégies suivantes et au registre :

- Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Receiver > Authentification utilisateur > Nom d'utilisateur et mot de passe locaux
- Définissez SSONCheckEnabled sur false dans l'une ou l'autre des clés de registre suivantes si le composant SSO n'est pas installé. La clé empêche le gestionnaire d'authentification Citrix

Receiver pour Windows de vérifier la présence du composant SSO, ce qui permet donc à Citrix Receiver pour Windows de s'authentifier auprès de StoreFront.

HKEY_CURRENT_USER\Software\Citrix\AuthManager\protocols\integratedwindows\

HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows\

Sinon, il est possible d'activer l'authentification par carte à puce sur StoreFront à la place de Kerberos. Pour activer l'authentification par carte à puce sur StoreFront à la place de Kerberos, installez Citrix Receiver pour Windows à l'aide des options de ligne de commande ci-dessous. Cette opération nécessite des privilèges d'administrateur. La machine n'a pas besoin d'appartenir à un domaine.

- /includeSSON installe l'authentification Single Sign-On (authentification unique). Permet la mise en cache des informations d'identification et l'utilisation de l'authentification pass-through au domaine.
- Si l'utilisateur ouvre une session sur le point de terminaison avec une méthode différente de la carte à puce pour l'authentification sur Receiver (par exemple, le nom d'utilisateur et mot de passe), la ligne de commande est la suivante :

```
1  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
```

Ceci empêche la capture d'informations d'identification lors de l'ouverture de session et permet à Citrix Receiver pour Windows de mémoriser le code PIN lors de l'ouverture de session sur Citrix Receiver pour Windows.

- Rendez-vous sur Stratégie > Modèles d'administration > Modèles d'administration classiques (ADM) > Citrix Components > Citrix Receiver > User authentication > Nom d'utilisateur et mot de passe locaux

  Activer l'authentification pass-through. En fonction de la configuration et des paramètres de sécurité, vous devrez peut-être sélectionner l'option Autoriser l'authentification pass-through pour toutes les connexions ICA pour que l'authentification pass-through fonctionne.

Pour configurer StoreFront :

- Lorsque vous configurez le service d'authentification, sélectionnez la case à cocher Carte à puce.

Pour plus d'informations sur l'utilisation de cartes à puce avec StoreFront, consultez la section Configurer le service d'authentification dans la documentation de StoreFront.

Pour activer l'utilisation de cartes à puce sur les machines utilisateur

1. Importez le certificat racine d'autorité de certification dans le keystore de la machine.
2. Installez les logiciels intermédiaires de chiffrement du fournisseur de services.
3. Installez et configurez Citrix Receiver pour Windows.

Pour modifier la façon dont les certificats sont sélectionnés

Par défaut, si de multiples certificats sont valides, Citrix Receiver pour Windows invite l'utilisateur à en choisir un dans la liste. Vous pouvez également configurer Citrix Receiver pour Windows de manière à ce qu'il utilise le certificat par défaut (celui du fournisseur de carte à puce) ou le certificat doté de la date d'expiration la plus longue. S'il n'existe aucun certificat valide, l'utilisateur en est notifié et il a la possibilité d'utiliser une autre méthode d'ouverture de session, le cas échéant.

Un certificat valide doit présenter ces caractéristiques :

- L'heure actuelle de l'horloge sur l'ordinateur doit se situer dans la période de validité du certificat.
- La clé publique du sujet doit utiliser l'algorithme RSA et être d'une longueur de 1024, 2048 ou 4096 bits.
- L'utilisation de la clé doit contenir une signature numérique.
- L'autre nom du sujet doit contenir le nom d'utilisateur principal (UPN).
- L'utilisation améliorée de la clé doit contenir l'ouverture de session par carte à puce et l'authentification client, ou toute utilisation de clé.
- L'une des autorités de certification sur la chaîne de l'émetteur du certificat doit correspondre à l'un des noms uniques autorisés (DN) envoyé par le serveur dans la négociation TLS.

Modifiez la manière dont les certificats sont sélectionnés en utilisant l'une des méthodes suivantes :

- Sur la ligne de commande Citrix Receiver pour Windows, spécifiez l'option `AM\\_CERTIFICATESELECTIONM ={ Prompt | SmartCardDefault | LatestExpiry }`.

  Prompt est la valeur par défaut. Pour SmartCardDefault ou LatestExpiry, si plusieurs certificats répondent aux critères, Citrix Receiver pour Windows invite l'utilisateur à choisir un certificat.

- Ajoutez la valeur de clé suivante à la clé de registre HKCU ou HKLM\Software\[Wow6432Node\]Citrix\AuthMar `CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }`.

  Les valeurs définies dans la ruche de registre HKCU ont priorité sur les valeurs définies dans la ruche de registre HKLM afin d'aider l'utilisateur à sélectionner un certificat.

Pour utiliser des invites de code PIN CSP

Par défaut, les invites de saisie du code PIN sont fournies par Citrix Receiver pour Windows plutôt que par le fournisseur de services cryptographiques (CSP) de la carte. Citrix Receiver pour Windows invite les utilisateurs à entrer un code PIN lorsque cela est requis et transmet le code PIN au CSP de la carte à puce. Si votre site ou carte à puce impose des mesures de sécurité plus strictes, telles que désactiver la mise en cache du code PIN par processus ou par session, vous pouvez configurer Citrix Receiver pour Windows pour qu'il utilise à la place les composants du CSP pour gérer la saisie du code PIN, y compris le message invitant l'utilisateur à entrer le code PIN.

Modifiez la manière dont la saisie du code PIN est traitée en utilisant l'une des méthodes suivantes :

- Sur la ligne de commande Citrix Receiver pour Windows, spécifiez l'option AM_SMARTCARDPINENTRY=CSP.
- Ajoutez la valeur de clé suivante à la clé de registre HKLM\Software\[Wow6432Node\]Citrix\AuthManager: SmartCardPINEntry=CSP.

Configurer l'authentification pass-through au domaine avec Kerberos

June 27, 2019

Cette rubrique s'applique uniquement aux connexions entre Citrix Receiver pour Windows et StoreFront, XenDesktop ou XenApp.

Citrix Receiver pour Windows prend en charge l'authentification pass-through au domaine Kerberos pour les déploiements qui utilisent des cartes à puce. Kerberos est l'une des méthodes d'authentification incluses à l'authentification Windows intégrée (IWA).

Lorsque l'authentification Kerberos est activée, Kerberos gère l'authentification sans mots de passe à la place de Citrix Receiver pour Windows, ce qui évite les attaques de type cheval de Troie destinées à obtenir les mots de passe sur la machine utilisateur. Les utilisateurs peuvent ouvrir une session sur la machine utilisateur par le biais de n'importe quelle méthode d'authentification, notamment un identificateur biométrique (par exemple, un lecteur d'empreintes digitales), et accéder aux ressources publiées sans autre authentification.

Citrix Receiver pour Windows gère l'authentification pass-through avec Kerberos comme suit lorsque Citrix Receiver pour Windows, StoreFront, XenDesktop et XenApp sont configurés pour l'authentification par carte à puce et qu'un utilisateur ouvre une session avec une carte à puce :

1. Le service SSO de Citrix Receiver pour Windows capture le code PIN de la carte à puce.
2. Citrix Receiver pour Windows utilise IWA (Kerberos) pour authentifier l'utilisateur auprès de StoreFront. StoreFront fournit ensuite à Citrix Receiver pour Windows les informations sur les applications et bureaux virtuels disponibles.
   Remarque : vous n'avez pas besoin d'utiliser l'authentification Kerberos pour cette étape. L'activation de Kerberos sur Citrix Receiver pour Windows est uniquement requise afin d'éviter d'avoir à saisir de nouveau un code PIN. Si vous n'utilisez pas l'authentification Kerberos, Citrix Receiver pour Windows s'authentifie auprès de StoreFront à l'aide des informations d'identification de la carte à puce.
3. Le moteur HDX (anciennement appelé client ICA) transmet le code PIN de la carte à puce à XenDesktop ou XenApp afin de connecter l'utilisateur à la session Windows. XenDesktop ou XenApp met ensuite à disposition les ressources demandées.

Pour utiliser l'authentification Kerberos avec Citrix Receiver pour Windows, assurez-vous que la configuration de Kerberos est conforme à ce qui suit.

- Kerberos fonctionne uniquement entre Citrix Receiver pour Windows et des serveurs appartenant aux mêmes domaines Windows ou des domaines approuvés. Les serveurs doivent également être approuvés pour délégation, une option configurée via l'outil de gestion des utilisateurs et machines Active Directory.
- Kerberos doit être activé sur le domaine et dans XenDesktop et XenApp. Pour renforcer la sécurité et vous assurer que Kerberos est utilisé, désactivez toute option IWA non Kerberos sur le domaine.
- L'ouverture de session Kerberos n'est pas disponible pour les connexions Services Bureau à distance configurées pour utiliser l'authentification de base, pour toujours utiliser des informations d'ouverture de session spécifiées, ou pour toujours inviter les utilisateurs à entrer un mot de passe.

Le reste de cette rubrique décrit comment configurer l'authentification pass-through au domaine pour les scénarios les plus courants. Si vous migrez vers StoreFront depuis l'Interface Web et que vous avez précédemment utilisé une solution d'authentification personnalisée, contactez votre représentant de support technique Citrix pour de plus amples informations.

> **Avertissement**
>
> Certaines des configurations décrites dans cette rubrique impliquent de modifier le registre. Une utilisation incorrecte de l'Éditeur du Registre peut occasionner de sérieux problèmes qui pourraient nécessiter l'installation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à effectuer une copie de sauvegarde avant de modifier le registre.

Pour configurer l'authentification pass-through au domaine avec Kerberos en vue de l'utilisation avec des cartes à puce

Si vous n'avez jamais procédé à des déploiements avec carte à puce dans un environnement XenDesktop, nous vous recommandons de lire les informations relatives aux cartes à puce dans la section Sécuriser votre déploiementSécuriser votre déploiementSécuriser votre déploiement de la documentation XenDesktop avant de continuer.

Lorsque vous installez Citrix Receiver pour Windows, incluez l'option de ligne de commande suivante :

- /includeSSON

  Cette option installe le composant SSO sur l'ordinateur appartenant au domaine, ce qui permet à Citrix Receiver pour Windows de s'authentifier auprès de StoreFront à l'aide de IWA (Kerberos). Le composant SSO stocke le code PIN de la carte à puce, qui est ensuite utilisé par le moteur HDX lorsqu'il transmet à distance le matériel et les informations d'identification de la de carte à

puce à XenDesktop. XenDesktop sélectionne automatiquement un certificat à partir de la carte à puce et obtient le code PIN à partir du moteur HDX.

Une option connexe, ENABLE_SSON, est activée par défaut et doit rester activée.

Si une stratégie de sécurité empêche l'activation du SSO sur un appareil, configurez Citrix Receiver pour Windows via la stratégie suivante :

Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Receiver > Authentification utilisateur > Nom d'utilisateur et mot de passe locaux

> **Remarque**
>
> Dans ce scénario, vous voulez autoriser le moteur HDX à utiliser l'authentification par carte à puce et non Kerberos, c'est la raison pour laquelle vous ne devez pas utiliser l'option ENABLE_KERBEROS=Yes, ce qui forcerait le moteur HDX à utiliser Kerberos.

Pour appliquer les paramètres, redémarrez Citrix Receiver pour Windows sur la machine utilisateur.

Pour configurer StoreFront :

- Dans le fichier default.ica situé sur le serveur StoreFront, définissez DisableCtrlAltDel sur false.

> **Remarque**
>
> Cette étape n'est pas nécessaire si toutes les machines clientes exécutent Citrix Receiver pour Windows 4.2 ou version ultérieure.

- Lorsque vous configurez le service d'authentification sur le serveur StoreFront, sélectionnez la case Authentification pass-through au domaine. Ce paramètre active l'authentification Windows intégrée. Vous n'avez pas besoin de sélectionner la case Carte à puce sauf si vous disposez également de clients n'appartenant pas au domaine qui se connectent à StoreFront à l'aide de cartes à puce.

Pour plus d'informations sur l'utilisation de cartes à puce avec StoreFront, consultez la section Configurer le service d'authentification dans la documentation de StoreFront.

À propos de l'API FastConnect et de l'authentification de base HTTP

L'API FastConnect utilise la méthode d'authentification HTTP basique, qui est souvent confondue avec les méthodes d'authentification associées à l'authentification pass-through au domaine, l'authentification Kerberos et l'authentification IWA. Citrix recommande de désactiver IWA sur StoreFront et dans la stratégie de groupe ICA.

Activer la vérification de liste de révocation de certificats pour améliorer la sécurité

June 27, 2019

Lorsque vous activez la vérification de la liste de révocation de certificats (CRL), Citrix Receiver pour Windows vérifie si le certificat du serveur est révoqué. Obliger Citrix Receiver pour Windows à vérifier cette liste améliore l'authentification cryptographique du serveur et la sécurité globale de la connexion TLS entre une machine utilisateur et un serveur.

Vous pouvez activer plusieurs niveaux de vérification CRL. Par exemple, vous pouvez configurer Citrix Receiver pour Windows pour qu'il ne vérifie que sa liste de certificats locaux ou pour qu'il vérifie les listes de certificats locaux et de réseau. De plus, vous pouvez configurer la vérification des certificats pour permettre aux utilisateurs de n'ouvrir leurs sessions que si toutes les listes de révocation de certificats ont été vérifiées.

Si vous effectuez cette modification sur un ordinateur local, quittez Citrix Receiver pour Windows. Assurez-vous que tous les composants de Citrix Receiver pour Windows, y compris le **Centre de connexion**, sont fermés.

Pour plus d'informations sur la configuration de TLS, consultez la section Configurer et activer TLS.

Sécuriser les communications

August 1, 2018

Pour sécuriser les communications entre les sites XenDesktop ou les batteries de serveurs XenApp et Citrix Receiver pour Windows, vous pouvez intégrer vos connexions Citrix Receiver pour Windows à l'aide d'un large choix de technologies de sécurité, dont :

- Citrix NetScaler Gateway. Pour de plus amples informations, reportez-vous aux rubriques de cette section ainsi qu'à la documentation NetScaler Gateway et StoreFront.
  Remarque : Citrix recommande d'utiliser NetScaler Gateway pour sécuriser les communications entre les serveurs StoreFront et les machines utilisateur.
- Un pare-feu. Les pare-feu de réseau peuvent autoriser ou empêcher le passage des paquets de données en fonction de l'adresse et du port de destination. Si vous utilisez Citrix Receiver pour Windows avec un pare-feu de réseau qui mappe l'adresse IP interne du serveur sur une adresse Internet externe (c'est-à-dire, la traduction d'adresse de réseau, ou NAT), configurez l'adresse externe.
- Une configuration de serveur de confiance.

- Pour les déploiements XenApp ou Interface Web uniquement ; non applicable à XenDesktop 7 : un serveur proxy SOCKS ou serveur proxy sécurisé (également appelé serveur proxy de sécurité, serveur proxy HTTPS). Vous pouvez utiliser les serveurs proxy pour limiter l'accès à l'intérieur et à l'extérieur de votre réseau, et pour gérer les connexions entre Receiver et les serveurs. Receiver prend en charge les protocoles de proxy SOCKS et de proxy sécurisé.
- S'applique uniquement aux déploiements de XenApp ou de l'Interface Web ; ne s'applique pas aux solutions XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5, ou XenApp 7.5 : Relais SSL utilisant les protocoles TLS.
- Pour XenApp 7.6 et XenDesktop 7.6, vous pouvez activer une connexion SSL directement entre des utilisateurs et des VDA.

Citrix Receiver pour Windows est compatible avec et fonctionne dans les environnements où les modèles de sécurité de bureau Microsoft Specialized Security - Limited Functionality (SSLF) sont utilisés. Ces modèles sont pris en charge sur plusieurs plates-formes Windows.
Consultez les guides de sécurité Windows disponibles à l'adresse http://technet.microsoft.com pour plus d'informations sur les modèles et les réglages associés.

Application de la relation d'approbation

June 27, 2019

La configuration d'un serveur approuvé identifie et applique les relations d'approbation des connexions de Citrix Receiver pour Windows.

Lorsque vous activez la fonction Serveurs approuvés, Citrix Receiver pour Windows spécifie les exigences et décide si la connexion au serveur peut être approuvée ou non. Par exemple, un Citrix Receiver pour Windows se connectant à une certaine adresse (comme https://*citrix.com) avec un type de connexion donné (comme TLS) est dirigé vers une zone de confiance sur le serveur.

Lorsque vous activez cette fonctionnalité, le serveur connecté se trouve dans la zone Sites de confiance Windows. Pour obtenir des instructions étape par étape sur l'ajout des serveurs à la zone Sites de confiance Windows, veuillez consultez l'aide en ligne d'Internet Explorer.

Pour activer la configuration des serveurs approuvés avec le modèle d'administration d'objet de stratégie de groupe

Configuration requise :

Fermez les composants de Citrix Receiver pour Windows, notamment le centre de connexion.

1. En tant qu'administrateur, ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.

a) Pour appliquer la stratégie sur un seul ordinateur, lancez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver à partir du menu Démarrer.
b) Pour appliquer la stratégie sur un domaine, lancez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver à partir de la Console de gestion des stratégies de groupe.

2. Dans le nœud Configuration ordinateur, développez **Modèles d'administration** > **Modèles d'administration classiques (ADM)** > **Composants Citrix** > **Citrix Receiver** > **Routage réseau** > **Paramétrer la configuration d'un serveur approuvé**.
3. Sélectionnez **Activé** pour forcer Citrix Receiver pour Windows à effectuer l'identification de la région.
4. Sélectionnez **Appliquer configuration d'un serveur approuvé**. Cela force le client à effectuer l'identification à l'aide d'un serveur de confiance.
5. Dans la liste déroulante **Zone Internet Windows**, sélectionnez l'adresse du serveur client. Ce paramètre s'applique uniquement à la zone Sites de confiance Windows.
6. Dans le champ **Adresse**, définissez l'adresse du serveur de client pour une zone de site de confiance autre que Windows. Vous pouvez utiliser une liste séparée par des virgules.
7. Cliquez sur **OK** et sur **Appliquer**.

Configurer l'authentification par carte à puce pour l'Interface Web 5.4

November 16, 2018

Si Citrix Receiver pour Windows est installé avec un composant SSON, l'authentification pass-through est activée par défaut, même si l'authentification pass-through par code PIN pour carte à puce n'est pas activée sur le site PNAgent XenApp ; le paramètre pass-through comme méthode d'authentification ne sera plus valide. L'écran ci-dessous illustre comment activer la carte à puce comme méthode d'authentification lorsque Citrix Receiver pour Windows est configuré correctement avec le SSON.

Utilisez la stratégie de retrait de carte à puce pour contrôler le comportement de retrait de la carte à puce lorsqu'un utilisateur s'authentifie auprès du site PNAgent de l'Interface Web Citrix 5.4.

Lorsque cette stratégie est activée, l'utilisateur est déconnecté de la session XenApp si la carte à puce a été retirée de la machine cliente. Toutefois, l'utilisateur est toujours connecté à Citrix Receiver pour Windows.

Pour que cette stratégie soit appliquée, la stratégie de retrait de carte à puce doit être définie dans le site XenApp Services de l'Interface Web. Les paramètres se trouvent sur l'Interface Web 5.4, **Site XenApp Services > Authentification unique avec carte à puce > Activer l'itinérance > Fermer les sessions lors du retrait d'une carte à puce**.

Lorsque la stratégie de retrait de carte à puce est désactivée, la session XenApp de l'utilisateur est déconnectée si la carte à puce est retirée de la machine cliente ; le retrait de la carte à puce sur le site XenApp Services de l'Interface Web n'a aucun effet.
Remarque : il existe des stratégies distinctes pour les clients 32 bits et 64 bits. Pour les machines 32 bits, le nom de la stratégie est **Stratégie de retrait de carte à puce (machine 32 bits)** et pour les machines 64 bits, le nom de la stratégie est **Stratégie de retrait de carte à puce (machine 64 bits)**.

Modifications de la prise en charge et du retrait des cartes à puce

Tenez compte de ce qui suit lors de l'ouverture de session sur un site PNAgent XenApp 6.5 :

- À compter de Citrix Receiver pour Windows version 4.5, l'ouverture de session par carte à puce est prise en charge pour les connexions au site PNAgent.
- La stratégie de retrait de carte à puce a été modifiée sur le site PNAgent :
  une session XenApp est fermée lorsque la carte à puce est retirée : si le site PNAgent est configuré avec carte à puce comme méthode d'authentification, la stratégie doit être configurée sur Citrix Receiver pour Windows pour appliquer la fermeture de session de XenApp. Activez l'itinérance pour l'authentification par carte à puce sur le site PNAgent XenApp et activez la stratégie de retrait de carte à puce, qui déconnecte XenApp de la session Receiver ; l'utilisateur reste connecté à la session Receiver.

Limitation

Lorsqu'un utilisateur ouvre une session sur le site PNAgent à l'aide de l'authentification par carte à puce, le nom d'utilisateur est affiché comme **Session ouverte**.

Connexion via un serveur proxy

November 16, 2018

Les serveurs proxy permettent de limiter l'accès vers et depuis votre réseau, et de gérer les connexions entre Citrix Receiver pour Windows et les serveurs. Citrix Receiver pour Windows prend en charge les protocoles proxy SOCKS et sécurisés.

Lors de communications avec la batterie de serveurs, Receiver utilise les paramètres de serveur proxy configurés à distance sur le serveur exécutant Receiver pour Web ou l'Interface Web. Pour de plus amples informations sur la configuration du serveur proxy, reportez-vous à la documentation relative à StoreFront ou à l'Interface Web.

Pour la communication avec le serveur Web, Receiver utilise les paramètres de serveur proxy configurés au travers des paramètres Internet du navigateur Web par défaut sur la machine utilisateur. Vous

devez configurer les paramètres Internet du navigateur Web par défaut de la machine utilisateur en conséquence.

Configurez les paramètres de proxy à l'aide de l'Éditeur du Registre pour forcer Citrix Receiver pour Windows à utiliser ou à ignorer le serveur proxy lors des connexions.

> **Avertissement**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre.

1. Accédez à HKLM\Software\Citrix\AuthManager\
2. Définissez le paramètre **ProxyEnabled** (REG_SZ).
    a) True : indique que Citrix Receiver pour Windows utilise le serveur proxy lors des connexions.
    b) False : indique que Citrix Receiver pour Windows ignore le serveur proxy lors des connexions.
3. Ouvrez l'Éditeur de Registre.
4. Redémarrez la session Citrix Receiver pour Windows pour que les modifications soient prises en compte.

Connexion via un pare-feu

June 27, 2019

Les pare-feu de réseau peuvent autoriser ou empêcher le passage des paquets de données en fonction de l'adresse et du port de destination. Si vous utilisez un pare-feu dans votre déploiement, Citrix Receiver pour Windows doit pouvoir communiquer via le pare-feu avec le serveur Web et le serveur Citrix.

Ports de communication Citrix communs

Source	Type	Port	Détails
Citrix Receiver	TCP	80/443	Communication avec StoreFront
ICA/HDX	TCP	1494	Accès aux applications et bureaux virtuels

Source	Type	Port	Détails
ICA/HDX avec fiabilité de session	TCP	2598	Accès aux applications et bureaux virtuels
ICA/HDX sur SSL	TCP	443	Accès aux applications et bureaux virtuels
ICA/HDX depuis HTML5 Receiver	TCP	8008	Accès aux applications et bureaux virtuels
Audio ICA/HDX sur UDP	TCP	16500 - 16509	Plage pour les ports audio ICA/HDX
IMA	TCP	2512	Independent Management Architecture (IMA)
Console de gestion	TCP	2513	Consoles de gestion Citrix et *Services WCF Remarque : pour les plates-formes 7.5 et ultérieures basées sur FMA, le port 2513 n'est PAS utilisé.
Demande application/bureau	TCP	80/8080/443	Service XML
STA	TCP	80/8080/443	Secure Ticketing Authority (intégré au service XML)

> **Remarque**
>
> Dans XenApp 6.5, le port 2513 est utilisé par les Services XenApp Commands Reporting via WCF.

Si le pare-feu est configuré pour la traduction des adresses réseau, vous pouvez vous servir de l'Interface Web pour définir les mappages depuis les adresses internes vers les adresses externes et les ports. Par exemple, si votre serveur XenApp ou XenDesktop n'est pas configuré avec une adresse secondaire, vous pouvez configurer l'Interface Web pour qu'elle fournisse une adresse secondaire à Receiver. Citrix Receiver pour Windows se connecte ensuite au serveur à l'aide de l'adresse externe et du numéro de port. Pour de plus amples informations, consultez la documentation de Interface Web

Signature de fichier ICA pour se protéger contre le lancement d'applications ou de bureaux provenant de serveurs non approuvés

November 16, 2018

La signature de fichier ICA permet de vous protéger contre le lancement non autorisé d'applications ou de bureaux. Citrix Receiver pour Windows vérifie, à l'aide d'une stratégie administrative, qu'une source approuvée est à l'origine du lancement de l'application ou du bureau et empêche le lancement provenant de serveurs non approuvés. Vous pouvez configurer la signature de fichier ICA à l'aide du modèle d'administration des objets de stratégie de groupe, StoreFront ou Citrix Merchandising Server. Par défaut, la signature de fichier ICA n'est pas activée par défaut. Pour obtenir des informations sur l'activation de la signature de fichier ICA pour StoreFront, reportez-vous à la documentation de StoreFront.

Pour le déploiement de l'Interface Web, cette dernière active et configure le lancement d'applications ou de bureaux de manière à y inclure une signature durant le processus de lancement à l'aide du service Signature de fichier ICA. Le service peut signer le fichier ICA à l'aide d'un certificat provenant du magasin de certificats personnel de l'ordinateur.

Citrix Merchandising Server, en conjonction avec Citrix Receiver pour Windows, active et configure la vérification de la signature de lancement à l'aide de l'assistant Citrix Merchandising Server Administrator Console > Deliveries afin d'ajouter des empreintes numériques de certificats approuvés.

Configurer la signature de fichier ICA avec le modèle d'administration d'objet de stratégie de groupe

> **Remarque**
>
> Si CitrixBase.admx\adml n'est pas ajouté à l'objet de stratégie de groupe local, la stratégie **Activer la signature de fichier ICA** peut être absente.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud Configuration ordinateur, accédez à Modèles d'administration > Composants Citrix.
3. Sélectionnez la stratégie Activer la signature de fichier ICA, puis sélectionnez une option selon les besoins :
    a) Activé - Indique que vous pouvez ajouter l'empreinte numérique du certificat de signature à la liste blanche des empreintes de certificats de confiance.
    b) Certificats de confiance - Cliquez sur Afficher pour supprimer l'empreinte de certificat de signature existante de la liste blanche. Vous pouvez copier et coller les empreintes numériques de certificat de signature à partir des propriétés du certificat de signature.

c) Stratégie de sécurité - Sélectionnez l'une des options suivantes dans le menu déroulant.
   i. Autoriser uniquement les lancements signés (plus sécurisé) - Autorise uniquement le lancement d'applications ou de bureaux signés à partir d'un serveur approuvé. Un avertissement de sécurité apparaît en cas de signature invalide. Vous ne pouvez pas lancer la session en raison d'une non-autorisation.
   ii. Demander à l'utilisateur lors de lancements non signés (moins sécurisé) - Une invite de message s'affiche lorsqu'une session non signée ou non valide est lancée. Vous pouvez choisir de continuer le lancement ou d'annuler le lancement (option par défaut).

4. Cliquez sur **Appliquer** et **OK** pour enregistrer la stratégie.

Pour sélectionner et distribuer un certificat de signature numérique

Lors de la sélection d'un certificat de signature numérique, Citrix vous recommande de choisir l'une des solutions suivantes (elles apparaissent par ordre de priorité) :

1. Achetez un certificat de signature de code ou certificat de signature SSL émanant d'une autorité de certification publique (CA).
2. Si votre entreprise dispose d'une autorité de certification privée, créez un certificat de signature de code ou certificat de signature SSL à l'aide de l'autorité de certification privée.
3. Utilisez un certificat SSL existant, tel que le certificat du serveur de l'Interface Web.
4. Créez un nouveau certificat d'autorité de certification racine et distribuez-le sur les machines utilisateur à l'aide d'un objet de stratégie de groupe ou dans le cadre d'une installation manuelle.

Configurer les suites de chiffrement obsolètes

June 27, 2019

> **Remarque**
>
> Lorsque vous mettez à niveau ou installez Citrix Receiver pour Windows pour la première fois, vous devez ajouter les derniers fichiers de modèle à l'objet de stratégie de groupe local. Pour plus d'informations sur l'ajout des fichiers de modèle à l'objet de stratégie de groupe local, consultez la section Configuration du modèle d'administration d'objet de stratégie de groupe. En cas de mise à niveau, les paramètres existants sont conservés lors de l'importation des derniers fichiers.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
2. Sous le nœud Configuration ordinateur, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Receiver** > **Routage réseau**.

3. Sélectionnez la stratégie **Suites de chiffrement obsolètes**.
4. Sélectionnez **Activé** et choisissez l'une des options suivantes :
    a) **TLS_RSA_**: *By default, TLS_RSA_* is selected. Cette option doit être sélectionnée pour vous permettre d'utiliser les deux autres suites de chiffrement. Les suites de chiffrement suivantes sont incluses lorsque vous sélectionnez cette option :
        i. TLS_RSA_AES256_GCM_SHA384
        ii. TLS_RSA_AES128_GCM_SHA256
        iii. TLS_RSA_AES256_CBC_SHA256
        iv. TLS_RSA_AES256_CBC_SHA
        v. TLS_RSA_AES128_CBC_SHA
        vi. TLS_RSA_3DES_CBC_EDE_SHA
    b) **TLS_RSA_WITH_RC4_128_MD5** : sélectionnez cette option pour utiliser la suite de chiffrement RC4-MD5.
    c) **TLS_RSA_WITH_RC4_128_SHA** : sélectionnez cette option pour utiliser la suite de chiffrement RC4_128_SHA.
5. Cliquez sur **Appliquer**, puis sur **OK**.
6. Pour appliquer vos modifications, exécutez gpupdate /force.

Le tableau suivant répertorie les suites de chiffrement compris dans chaque ensemble :

Configurer et activer TLS

June 27, 2019

Cette rubrique s'applique à XenApp et XenDesktop version 7.6 et versions ultérieures.

Pour utiliser le cryptage TLS pour toutes les communications effectuées par Citrix Receiver pour Windows, configurez la machine utilisateur, Citrix Receiver pour Windows et, si vous utilisez l'Interface Web, le serveur exécutant l'Interface Web. Pour obtenir des informations sur la sécurisation de l'Interface Web, consultez la section Sécuriser dans la documentation de l'Interface Web.

Conditions préalables

Les machines utilisateur doivent présenter la configuration spécifiée dans la section [Configuration système requise].(/fr-fr/receiver/windows/current-release/system-requirements.html)

Utilisez cette stratégie pour configurer les options TLS qui permettent à Citrix Receiver pour Windows d'identifier de manière sécurisée le serveur auquel il se connecte et de crypter toutes les communications avec le serveur.

Vous pouvez utiliser les options suivantes pour :

- Imposer l'utilisation de TLS. Citrix recommande d'utiliser le protocole TLS pour toutes les connexions sur des réseaux non approuvés, y compris Internet.
- Imposer l'utilisation de la cryptographie approuvée FIPS (Federal Information Processing Standards) et vous conformer aux recommandations de la norme NIST SP 800-52. Ces options sont désactivées par défaut.
- Imposer l'utilisation d'une version spécifique du protocole TLS, et de suites de chiffrement TLS spécifiques. Citrix prend en charge les protocoles TLS 1.0, TLS 1.1 et TLS 1.2 entre Citrix Receiver pour Windows, et XenApp ou XenDesktop.
- Vous connecter uniquement à des serveurs spécifiques.
- Vérifier si le certificat de serveur est révoqué.
- Rechercher une stratégie d'émission de certificats de serveur spécifique.
- Sélectionner un certificat client particulier, si le serveur est configuré pour en demander un.

Configurer la prise en charge TLS avec le modèle d'administration d'objet de stratégie de groupe

1. En tant qu'administrateur, ouvrez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver en exécutant gpedit.msc.
    - Pour appliquer la stratégie sur un seul ordinateur, lancez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver à partir du menu Démarrer.
    - Pour appliquer la stratégie sur un domaine, lancez le modèle d'administration d'objet de stratégie de groupe Citrix Receiver à partir de la Console de gestion des stratégies de groupe.
2. Sous le nœud Configuration ordinateur, accédez à **Modèles d'administration** > **Citrix Receiver** > **Routage réseau** et sélectionnez la stratégie **Configuration de TLS et du mode de conformité**.
3. Sélectionnez **Activé** pour activer les connexions sécurisées et crypter les communications sur le serveur. Définissez les options suivantes :

    > **Remarque :** Citrix recommande d'utiliser TLS pour sécuriser les connexions.

4. Sélectionnez **Exiger TLS pour toutes les connexions** pour obliger Citrix Receiver pour Windows à utiliser TLS pour toutes les connexions aux applications et bureaux publiés.
5. Dans le menu déroulant **Mode de conformité aux normes de sécurité**, sélectionnez l'option appropriée :
    - **Aucun** : aucun mode de conformité n'est appliqué.
    - **SP800-52** : sélectionnez **SP800-52** pour la conformité avec la norme NIST SP 800-52. Sélectionnez cette option uniquement si les serveurs ou la passerelle sont conformes aux recommandations de la norme NIST SP 800-52.

Remarque :

Si vous sélectionnez SP800-52, la cryptographie approuvée FIPS est automatiquement utilisée, même si l'option **Activer FIPS** n'est pas sélectionnée. Vous devez également activer l'option de sécurité Windows **Chiffrement système : utilisez des algorithmes compatibles FIPS pour le chiffrement, le hachage et la signature**. Sinon, Citrix Receiver pour Windows peut ne pas parvenir à se connecter aux applications et bureaux publiés.

Si vous sélectionnez SP800-52, vous devez sélectionner le paramètre **Stratégie de vérification de la liste de révocation de certificats** avec **Vérifier avec accès complet** ou **Exiger vérification avec accès complet et liste de révocation de certificats**.

Si vous sélectionnez SP800-52, Citrix Receiver pour Windows vérifie que le certificat de serveur est conforme aux recommandations de la norme NIST SP 800-52. Si le certificat de serveur n'est pas conforme, Citrix Receiver pour Windows ne parviendra pas à se connecter.

6. **Activer FIPS** : sélectionnez cette option pour imposer l'utilisation de la cryptographie approuvée FIPS. Vous devez également activer l'option de sécurité Windows de la stratégie de groupe de système d'exploitation **Chiffrement système : utilisez des algorithmes compatibles FIPS pour le chiffrement, le hachage et la signature**. Sinon, Citrix Receiver pour Windows peut ne pas parvenir à se connecter aux applications et bureaux publiés.
7. Dans le menu déroulant **Serveurs TLS autorisés**, sélectionnez le numéro de port. Vous pouvez vous assurer que Citrix Receiver se connecte uniquement à un serveur spécifié dans une liste séparée par des virgules. Vous pouvez spécifier des numéros de port et des caractères génériques. Par exemple, *.citrix.com:4433 autorise les connexions à tout serveur dont le nom commun se termine par .citrix.com sur le port 4433. L'émetteur du certificat certifie l'exactitude des informations contenues dans un certificat de sécurité. Si Citrix Receiver ne reconnaît pas et n'approuve pas l'émetteur, la connexion est refusée.
8. Dans le menu déroulant **Version TLS**, sélectionnez une des options suivantes :
   - **TLS 1.0, TLS 1.1 ou TLS 1.2** : il s'agit du paramètre par défaut. Cette option est recommandée uniquement si TLS 1.0 est requis pour des raisons de compatibilité.
   - **TLS 1.1 ou TLS 1.2** : utilisez cette option pour vous assurer que les connexions ICA utilisent TLS 1.1 ou TLS 1.2
   - **TLS 1.2** : cette option est recommandée si TLS 1.2 est exigé par une entreprise.
9. **Suite de chiffrement TLS** : pour forcer l'utilisation des suites de chiffrement TLS, sélectionnez Gouvernement (GOV), Commercial (COM) ou Quelconque (ALL). Dans certaines configurations de NetScaler Gateway, vous devrez peut-être sélectionner COM. Citrix Receiver pour Windows prend en charge les clés RSA de longueur 1024, 2048 et 3072 bits. Les certificats racine avec des clés RSA de longueur de 4 096 bits sont aussi pris en charge.

> Remarque : Citrix ne recommande pas l'utilisation des clés RSA de longueur de 1 024 bits.

Consultez le tableau ci-dessous qui répertorie toutes les suites de chiffrement prises en charge.

- **Quelconque** : lorsque l'option « Quelconque » est sélectionnée, la stratégie n'est pas configurée et les suites de chiffrement suivantes sont autorisées :
  - TLS_RSA_WITH_RC4_128_MD5
  - TLS_RSA_WITH_RC4_128_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
- **Commerciale** : lorsque l'option « Commerciale » est sélectionnée, seules les suites de chiffrement suivantes sont autorisées :
  - TLS_RSA_WITH_RC4_128_MD5
  - TLS_RSA_WITH_RC4_128_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
- **Gouvernementale** : lorsque l'option « Gouvernementale » est sélectionnée, seules les suites de chiffrement suivantes sont autorisées :
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384

10. Dans le menu déroulant **Stratégie de vérification de la liste de révocation de certificats**, sélectionnez une des options suivantes :
    - **Vérifier sans accès au réseau** : la liste de révocation des certificats est vérifiée. Seuls les magasins de la liste de révocation de certificats locaux sont utilisés. Tous les points de distribution sont ignorés. L'utilisation de la liste de révocation de certificats n'est pas obligatoire à la vérification du certificat serveur présenté par le serveur Relais SSL/Secure Gateway cible.

- **Vérifier avec accès complet** : la liste de révocation de certificats est vérifiée. Les magasins locaux de la liste de révocation de certificats et tous les points de distribution sont utilisés. Si des informations de révocation sont trouvées pour un certificat, la connexion est refusée. L'utilisation d'une liste de révocation de certificats n'est pas indispensable à la vérification du certificat serveur présenté par le serveur cible.
- **Exiger vérification avec accès complet et liste de révocation de certificats** : la liste de révocation de certificats est vérifiée, à l'exception de l'autorité de certification racine. Les magasins locaux de la liste de révocation de certificats et tous les points de distribution sont utilisés. Si des informations de révocation sont trouvées pour un certificat, la connexion est refusée. Si des informations de révocation sont trouvées pour un certificat, la connexion sera refusée.
- **Exiger vérification avec accès complet et toutes les listes de révocation de certificats** : la liste de révocation de certificats est vérifiée, y compris l'autorité de certification racine. Les magasins locaux de la liste de révocation de certificats et tous les points de distribution sont utilisés. Si des informations de révocation sont trouvées pour un certificat, la connexion est refusée. Si des informations de révocation sont trouvées pour un certificat, la connexion sera refusée.
- **Aucune vérification** : la liste de révocation des certificats n'est pas vérifiée.

11. Avec **OID de l'extension de stratégie**, vous pouvez restreindre Citrix Receiver pour Windows de manière à ce qu'il puisse uniquement se connecter à des serveurs avec une stratégie d'émission de certificats spécifique. Si l'option **OID de l'extension de stratégie** est sélectionnée, Citrix Receiver pour Windows n'accepte que les certificats de serveur contenant cet OID d'extension de stratégie.
12. Dans le menu déroulant **Authentification client**, sélectionnez une des options suivantes :
    - **Désactivé** : l'authentification client est désactivée
    - **Afficher sélecteur de certificats** : toujours demander à l'utilisateur de sélectionner un certificat
    - **Sélectionner automatiquement si possible** : demander à l'utilisateur uniquement lorsque plusieurs certificats sont disponibles
    - **Non configuré** : indique que l'authentification du client n'est pas configurée.
    - **Utiliser certificat spécifié** : utiliser le certificat client défini dans l'option Certificat client.
13. Utilisez le paramètre **Certificat client** pour spécifier l'empreinte numérique du certificat d'identification et éviter une intervention inutile de l'utilisateur.
14. Cliquez sur **Appliquer** et **OK** pour enregistrer la stratégie.

Le tableau suivant répertorie les suites de chiffrement compris dans chaque ensemble :

Connexion avec Secure Gateway

August 1, 2018

Cette rubrique s'applique uniquement aux déploiements faisant appel à l'Interface Web.

Vous pouvez utiliser la passerelle Secure Gateway en mode Normal ou en mode Relais afin de fournir un canal sécurisé de communication entre Citrix Receiver pour Windows et le serveur. Il n'est pas nécessaire de configurer Citrix Receiver pour Windows si vous utilisez la passerelle Secure Gateway en mode Normal et si les utilisateurs se connectent via l'Interface Web.

Citrix Receiver pour Windows utilise des paramètres configurés à distance sur le serveur exécutant l'Interface Web pour se connecter aux serveurs exécutant Secure Gateway. Consultez les rubriques de l'Interface Web pour obtenir des informations sur la configuration des paramètres d'un serveur proxy pour Citrix Receiver pour Windows.

Pour plus d'informations sur la configuration des paramètres de serveur proxy, veuillez consulter la documentation de l'Interface Web.

Si le proxy Secure Gateway est installé sur un serveur dans le réseau sécurisé, vous pouvez l'utiliser en mode Relais.

Si vous utilisez le **mode Relais**, le serveur Secure Gateway fonctionne comme un serveur proxy. Dans ce cas, vous devez configurer Citrix Receiver pour Windows pour qu'il utilise :

- le nom de domaine complet du serveur Citrix Secure Gateway ;
- le numéro de port du serveur Citrix Secure Gateway. Veuillez noter que le mode Relais n'est pas pris en charge par Secure Gateway, version 2.0.

Le nom de domaine complet (FQDN) doit contenir, dans l'ordre, les trois composants suivants :

- Nom d'hôte
- Domaine intermédiaire
- Domaine de tête

Par exemple : mon_ordinateur.mon_entreprise.com est un nom de domaine complet car il liste dans l'ordre un nom d'hôte (mon_ordinateur), un domaine intermédiaire (mon_entreprise) et un domaine de tête (com). La combinaison du domaine intermédiaire et du domaine de tête (mon_entreprise.com) est généralement appelée nom de domaine.

Niveau d'élévation et wfcrun32.exe

August 1, 2018

Lorsque le contrôle de compte utilisateur (UAC) est activé sur des machines exécutant Windows 10, Windows 8 ou Windows 7, seuls les processus au même niveau d'élévation/d'intégrité que wfcrun32.exe peuvent lancer les applications virtuelles.

Exemple 1 :

lorsque wfcrun32.exe est exécuté en mode d'utilisateur normal (pas d'élévation), d'autres processus, tels que Receiver, doivent être exécutés en mode d'utilisateur normal pour lancer des applications via wfcrun32.exe.

Exemple 2 :

lorsque wfcrun32.exe est exécuté en mode élevé, les autres processus tels que le Centre de connexion, Receiver et les applications tierces qui utilisent l'objet de client ICA, qui sont exécutés en mode non élevé ne peuvent communiquer avec wfcrun32.exe.

Citrix Receiver pour Windows Desktop Lock

June 27, 2019

Vous pouvez utiliser Citrix Receiver pour Windows Desktop Lock lorsque vous n'avez pas besoin d'interagir avec le bureau local. Vous pouvez toujours utiliser Desktop Viewer (si cette option est activée), mais elle possède uniquement le jeu d'options requis sur la barre d'outils : Ctrl+Alt+Suppr, Préférences, Périphériques et Déconnecter.

Citrix Receiver for Windows Desktop Lock fonctionne sur des machines appartenant à un domaine, sur lesquelles SSON est activé et qui sont configurées pour le magasin ; il peut également être utilisé sur des machines n'appartenant pas à un domaine sur lesquelles le SSON n'est pas activé. Il ne prend pas en charge les sites PNA. Les versions antérieures de Desktop Lock ne sont pas prises en charge lors de la mise à niveau vers Citrix Receiver pour Windows 4.2 ou versions ultérieures.

Vous devez installer Citrix Receiver pour Windows à l'aide de la commande /includeSSON. Vous devez configurer le magasin et le Single Sign-On, au choix avec le fichier adm/admx ou l'option cmdline. Pour plus d'informations, veuillez consulter Installer et configurer Citrix Receiver à l'aide de la ligne de commande.

Puis, installez Citrix Receiver pour Windows Desktop Lock en tant qu'administrateur à l'aide du fichier CitrixReceiverDesktopLock.MSI disponible sur la page Téléchargements de Citrix.

Configuration système requise pour Citrix Receiver Desktop Lock

- Microsoft Visual C++ 2005 avec Service Pack 1 Redistributable Package Pour de plus amples informations, consultez la page de téléchargement de Microsoft.

- Pris en charge sous Windows 7 (y compris Embedded Edition), Windows 7 Thin PC, Windows 8, Windows 8.1 et Windows 10 (Anniversary Update incluse).
- Se connecte à StoreFront via des protocoles natifs uniquement.
- Postes de travail appartenant et n'appartenant pas à un domaine
- Les machines utilisateur doivent être connectées à un réseau local (LAN) ou un réseau étendu (WAN).

Local App Access

> **Important**
>
> L'activation de Local App Access peut permettre l'accès au bureau local, sauf si un verrouillage a été appliqué avec le modèle d'objet de stratégie de groupe ou une stratégie similaire. Pour plus d'informations, veuillez consulter la section Configurer Local App Access et la redirection d'adresse URL dans la documentation de XenApp et XenDesktop.

Utilisation de Citrix Receiver pour Windows Desktop Lock

- Vous pouvez utiliser Citrix Receiver pour Windows Desktop Lock avec les fonctionnalités Citrix Receiver pour Windows suivantes :
  - 3Dpro, Flash, USB, HDX Insight, plug-in Microsoft Lync 2013 et Local App Access
  - Authentification de domaine, à deux facteurs ou par carte à puce uniquement
- La fermeture de la session Citrix Receiver pour Windows Desktop Lock ferme la session sur le périphérique d'extrémité.
- La redirection Flash est désactivée sur Windows 8 et versions supérieures. La redirection Flash est activée sur Windows 7.
- Desktop Viewer est optimisé pour Citrix Receiver pour Windows Desktop Lock sans les propriétés Home, Restore, Maximize et Display.
- Ctrl+Alt+Suppr est disponible sur la barre d'outils Viewer.
- La plupart des touches de raccourci des fenêtres sont transmises à la session à distance, à l'exception de Windows+L. Pour plus de détails, consultez Transmission des touches de raccourci Windows à la session distante.
- Ctrl+F1 déclenche Ctrl+Alt+Suppr, lorsque vous désactivez la connexion ou Desktop Viewer pour les connexions de bureau.

Pour installer Citrix Receiver pour Windows Desktop Lock

Cette procédure installe Citrix Receiver pour Windows de telle sorte que les bureaux virtuels sont affichés via Citrix Receiver pour Windows Desktop Lock. Pour les déploiements utilisant des cartes à puce, reportez-vous à la section
Pour configurer des cartes à puce à utiliser avec les machines exécutant Receiver Desktop Lock.

1. Citrix vous recommande d'utiliser un compte d'administrateur local.
2. À l'invite de commandes, exécutez la commande suivante (dans Citrix Receiver et Plug-ins > Windows > dossier Citrix Receiver pour Windows sur le support d'installation).

   Par exemple :

   ```
   CitrixReceiver.exe
        /includeSSON
   STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/
      discovery;on;Desktop Store"
   ```

   Pour plus d'informations sur les commandes, consultez la documentation d'installation de Citrix Receiver pour Windows de la section Configuration et utilisation de Receiver pour Windows à l'aide de paramètres de ligne de commande.
3. Dans le même dossier sur le support d'installation, cliquez deux fois sur CitrixReceiverDesktopLock.msi. L'assistant Desktop Lock s'ouvre. Suivez les invites.
4. Une fois l'installation terminée, redémarrez la machine utilisateur. Si vous avez l'autorisation d'accéder à un bureau et que vous ouvrez une session en tant qu'utilisateur de domaine, la machine s'affiche à l'aide de Receiver Desktop Lock.

Pour vous permettre d'administrer la machine utilisateur une fois l'installation terminée, le compte utilisé pour installer CitrixReceiverDesktopLock.msi est exclus du shell de remplacement. Si ce compte est supprimé ultérieurement, vous ne pourrez pas ouvrir de session pour administrer la machine.

Pour exécuter une **installation silencieuse** de Receiver Desktop Lock, utilisez la ligne de commande suivante : msiexec /i CitrixReceiverDesktopLock.msi /qn

Pour configurer Citrix Receiver pour Windows Desktop Lock

N'accordez l'accès qu'à un seul bureau virtuel exécutant Citrix Receiver pour Windows Desktop Lock par utilisateur.

À l'aide des stratégies Active Directory, empêchez les utilisateurs de mettre les bureaux virtuels en veille prolongée.

Utilisez le même compte d'administrateur pour configurer Citrix Receiver pour Windows Desktop Lock que celui utilisé pour l'installer.

- Assurez-vous que les fichiers receiver.admx (ou receiver.adml) et receiver_usb.admx (.adml) sont chargés dans la stratégie de groupe (où les stratégies apparaissent dans Configuration ordinateur ou Configuration utilisateur > Modèles d'administration > Modèles d'administration

classiques (ADM) > Composants Citrix). Les fichiers .admx sont situés à l'adresse %Program Files%\Citrix\ICA Client\Configuration\.

- Préférences USB : lorsqu'un utilisateur connecte un périphérique USB, ce périphérique est automatiquement envoyé sur le bureau virtuel ; aucune intervention de l'utilisateur n'est requise. Le bureau virtuel est responsable du contrôle du périphérique USB et de son affichage dans l'interface utilisateur.
  - Activez la règle de stratégie USB.
  - Dans Citrix Receiver > Accès à distance des périphériques clients > Utilisation à distance de dispositifs USB génériques, activez et configurez les stratégies Périphériques USB existants et Nouveaux périphériques USB.
- Mappage de lecteur : dans Citrix Receiver > Accès à distance des périphériques clients, activez et configurez la stratégie de mappage du lecteur client.
- Microphone : dans Citrix Receiver > Accès à distance des périphériques clients, activez et configurez la stratégie du microphone client.

Pour configurer des cartes à puce à utiliser avec les machines exécutant Citrix Receiver pour Windows Desktop Lock

1. Configurer StoreFront.
   a) Configurez le service XML pour utiliser la résolution d'adresse DNS pour la prise en charge Kerberos.
   b) Configurez des sites StoreFront pour l'accès HTTPS, créez un certificat de serveur signé par votre autorité de certification de domaine et ajoutez la liaison HTTPS au site Web par défaut.
   c) Assurez-vous que l'authentification pass-through avec carte à puce est activée (activée par défaut).
   d) Activez Kerberos.
   e) Activez Kerberos et Authentification pass-through avec carte à puce.
   f) Activez Accès anonyme sur le site Web IIS par défaut et utilisez Authentification Windows intégrée.
   g) Assurez-vous que le site Web IIS par défaut ne nécessite pas SSL et ignore les certificats clients.
2. Utilisez la console de gestion des stratégies de groupe pour configurer les stratégies d'ordinateur local sur la machine utilisateur.
   a) Importez le modèle Receiver.admx depuis %Program Files%\Citrix\ICA Client\Configuration\.
   b) Développez Modèles d'administration > Modèles d'administration classiques (ADM) > Citrix Components > Citrix Receiver > User authentication.
   c) Activez Authentification par carte à puce.
   d) Activez Nom de l'utilisateur et mot de passe locaux.
3. Configurez la machine utilisateur avant d'installer Citrix Receiver pour Windows Desktop Lock.

a) Ajoutez l'adresse URL du Delivery Controller à la liste Sites de confiance de Windows Internet Explorer.
b) Ajoutez l'adresse URL pour le premier groupe de mise à disposition à la liste Sites de confiance d'Internet Explorer dans le formulaire de bureau://nom-groupe-mise-à-disposition.
c) Configurez Internet Explorer afin d'utiliser la connexion automatique aux sites de confiance.

Lorsque Citrix Receiver pour Windows Desktop Lock est installé sur la machine utilisateur, une stratégie de retrait de carte à puce cohérente est appliquée. Par exemple, si la stratégie Windows de retrait de carte à puce est définie sur Forcer la fermeture de session pour le bureau, l'utilisateur doit également fermer sa session sur la machine utilisateur, quelle que soit la stratégie Windows définie pour le retrait de la carte à puce. Cela évite de laisser la machine utilisateur dans un état incohérent. Cela s'applique uniquement aux machines utilisateur avec Citrix Receiver pour Windows Desktop Lock.

Pour supprimer Citrix Receiver pour Windows Desktop Lock

Veillez à supprimer les deux composants répertoriés ci-dessous.

1. Ouvrez une session sur le même compte d'administrateur local qui a été utilisé pour installer et configurer Citrix Receiver pour Windows Desktop Lock.
2. À partir de la fonctionnalité Windows pour la suppression ou la modification de programmes :
   - Supprimez Citrix Receiver pour Windows Desktop Lock.
   - Supprimez Citrix Receiver pour Windows.

Transmission des touches de raccourci Windows à la session distante

La plupart des touches de raccourci Windows sont transmises à la session distante. Cette section présente certains des raccourcis les plus courants.

Windows

- Win+D : réduit toutes les fenêtres sur le bureau.
- Alt+Tab : change la fenêtre active.
- Ctrl+Alt+Supprimer : via Ctrl+F1 et la barre d'outils Desktop Viewer.
- Alt+Maj+Tab
- Windows+Tab
- Windows+Maj+Tab
- Windows+toutes les touches de caractères

Windows 8

- Win+C : ouvre la barre de charme.
- Win+Q : ouvre la section Recherche de la barre de charme.
- Win+H : affiche la section Partager la barre de charme.
- Win+K : affiche la section Périphériques de la barre de charme.
- Win+I : affiche la section Paramètres de la barre de charme.
- Win+Q : permet de rechercher des applications.
- Win+W : permet de rechercher des paramètres.
- Win+F : permet de rechercher des fichiers.

Applications Windows 8

- Win+Z : affiche les options d'applications
- Win+. : ancre une application sur la gauche.
- Win + MAJ +. : ancre une application sur la droite.
- Ctrl+Tab : permet de parcourir l'historique des applications.
- Alt+F4 : ferme une application.

Bureau

- Win+D : ouvre le bureau.
- Win+, : passage furtif sur le bureau.
- Win+B : retour au bureau.

Autre

- Win+U : ouvre les options d'ergonomie.
- Ctrl+Échap : ouvre le menu Démarrer.
- Win+Entrée : ouvre le narrateur Windows.
- Win+X : permet d'accéder aux outils de menu du système.
- Win+Imprécran : permet de faire une copie d'écran et d'enregistrer les images.
- Win+Tab : permet de basculer entre les applications.
- Win+T : affiche un aperçu des fenêtres dans la barre des tâches.

SDK et API

June 27, 2019

SDK Citrix Common Connection Manager

Le SDK Common Connection Manager (CCM) fournit un ensemble d'API natives qui vous permettent d'interagir et d'effectuer des opérations de base à l'aide de scripts. Ce SDK ne nécessite pas de téléchargement distinct car il fait partie du package d'installation de Citrix Receiver pour Windows.

Remarque : certaines des API liées au lancement nécessitent le fichier ICA pour initier le processus de lancement sur les sessions XenApp ou XenDesktop.

Les capacités du SDK CCM incluent :

- Lancement de session
  - Permet de lancer des applications et des postes de travail à l'aide du fichier ICA généré.
- Déconnexion de session
  - Similaire à l'opération de déconnexion à l'aide du Centre de connexion de Receiver. La déconnexion peut s'appliquer à toutes les sessions ou à un utilisateur spécifique.
- Fermeture de session
  - Similaire à l'opération de fermeture de session à l'aide du Centre de connexion de Receiver. La fermeture peut s'appliquer à toutes les sessions ou à un utilisateur spécifique.
- Informations de session
  - Fournit différentes méthodes pour obtenir des informations liées à la connexion des sessions lancées. Cela inclut les sessions de bureau, d'application et d'application transparente inverse

Pour plus d'informations sur la documentation du SDK, reportez-vous au Guide des programmeurs pour Citrix CCM SDK.

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 Windows. Si vous souhaitez écrire des pilotes virtuels pour d'autres plates-formes clientes, contactez le support technique Citrix.

Le SDK du canal virtuel offre ce qui suit :

- L'interface Citrix Virtual Driver Application Programming Interface (VDAPI) est utilisée avec les fonctions de canal virtuel dans le SDK de l'API Citrix Server (WFAPI SDK) pour créer de nouveaux canaux virtuels. La prise en charge de canal virtuel fournie par VDAPI est conçue pour faciliter l'écriture de vos propres canaux virtuels.
- L'API de contrôle de Windows, qui améliore l'expérience visuelle et la prise en charge des applications tierces intégrées avec ICA.

- Un code source opérationnel pour 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 la documentation du SDK, reportez-vous au Citrix Virtual Channel SDK for Citrix Receiver for Chrome.

API Fast Connect 3 Credential Insertion

L'API Fast Connect 3 Credential Insertion offre une interface qui fournit des informations d'identification à la fonctionnalité Single Sign-On (SSON). Cette fonctionnalité est disponible dans Citrix Receiver pour Windows 4.2 et versions ultérieures. À l'aide de cette API, les partenaires Citrix peuvent fournir des produits d'authentification et SSO utilisant StoreFront ou l'Interface Web pour connecter les utilisateurs à des applications ou bureaux virtuels, puis les déconnecter de ces sessions.

Pour plus d'informations sur la documentation de l'API Fast Connect, reportez-vous à la sectionFast Connect 3 Credential Insertion API for Citrix Receiver for Windows.

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