

À propos de cette version

Nouveautés

-

-

-

-

-

-

-

-

-

-

-

-

-

•

•

•

•

•

•

•

•

•

•

•

•

•

-

-

-

-

-

Problèmes résolus dans cette version

Problèmes connus dans cette version

Problèmes résolus dans Citrix Receiver pour Windows 4.2

Receiver pour Windows 4.2.100

-
-
-
-
-

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

-

-

-

Receiver pour Windows 4.2

-

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

-
-
-
-
-
-
-
-
-
-
-
-
-

-

-

-

-

-

-

-

-

-

-

-

Problèmes connus dans Citrix Receiver pour Windows 4.2

Problèmes connus

-
-
-
-
-
-
-
-
-

•

•

•

•

•

•

•

•

-
-

-

Configuration système requise

Appareil

Système d'exploitation

-
-
-
-
-
-
-
-
-
-
-

Matériel

-
-
-

Périphériques tactiles

Serveurs Citrix

- -
 -
 -
 -
 -
 -
 -
- -
 -
 -
 -

-
-
-
-
-
-
-
-
-

-
-

-

-
-
-
-
-
-
-

Navigateur

-
-
-

Connectivité

-
-
-

-
-
-
-
-
-

À propos des connexions sécurisées et des certificats

Authentication

Mises à niveau

Autre

-
-
-
-
-
-

-

-

Installation de Receiver pour Windows

- -

-
-
-
-
-
-

Mise à niveau manuelle vers Receiver pour Windows

-
-
-
-

Considérations à prendre en compte lors de la mise à niveau

Considérations importantes à prendre en compte lors de la mise à niveau de la version 3.4 vers la version 4.2.100

Installation et désinstallation manuelle de Receiver pour Windows

Suppression de Receiver pour Windows

-
-
-
-
-

•

Configuration et utilisation de Receiver pour Windows à l'aide de paramètres de ligne de commande

-
-
-
-

-

-

-

-

-

-

-

-

-

-

-

-

-
-
-
-
-
-
-
-
-
-

```
CitrixReceiver.exe /silent
```

```
STORE0="MagasinApplications;https://serveurtest.net/Citrix/Monmagasin/discovery;on;Magasin des applications HR"
```

```
STORE1="MagasinSauvegardeApplications;https://serveurtest.net/Citrix/Monmagasinsauvegarde/discovery;on;Magasin  
de sauvegarde des applications HR"
```

```
CitrixReceiver.exe /INCLUDESSON /STORE0="PNAgent;https://serveurtest.net/Citrix/PNAgent/config.xml;on;Mon site  
PNAgent"
```

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

Déploiement de Receiver pour Windows à l'aide d'Active Directory et de scripts de démarrage exemples

-
-

Pour modifier les scripts

- `set DesiredVersion= 3.3.0.XXXX`
-
-
-

Pour ajouter des scripts de démarrage par ordinateur

Pour déployer Receiver par ordinateur

Pour supprimer Receiver par ordinateur

Pour définir des scripts de démarrage par utilisateur

-
-

Pour déployer Receiver par utilisateur

Pour supprimer Receiver par utilisateur

Déploiement de Receiver pour Windows à partir de Receiver pour Web

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

Configurer Receiver pour Windows

-

-

-

-

-

-

-

-

Configurer le mode libre-service

-
-

Configurer StoreFront.

Configuration de la mise à disposition d'applications

-

-

-

Configurer le mode libre-service

-

-

-

Personnalisation de l'emplacement des raccourcis d'applications

SelfServiceMode	false	SelfServiceMode	true
-----------------	-------	-----------------	------

-

SelfServiceMode	false
-----------------	-------

-

-

-

-

UseCategoryAsStartMenuPath

-

[/DESKTOPDIR="Dir_name"]
CategoryPath

-

AutoReinstallModifiedApps

Utilisation du modèle d'objet de stratégie de groupe pour personnaliser l'emplacement des raccourcis d'applications

-
-
-
-
-
-
-

Utilisation des clés de registre pour personnaliser l'emplacement des raccourcis d'applications

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

-
-
-
-
-

-
-
-

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

--	--

□

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

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

Exemples de cas d'utilisation

--	--

--	--

□

Configuration des applications Local App Access

-

- •

-

•

•

Configuration de votre environnement XenDesktop

Configurer la prise en charge USB pour les connexions XenDesktop et XenApp

-
-
-

-
-
-
-

-
-
-
-

-
-

Fonctionnement de la prise en charge USB

Périphériques de stockage de masse

Classes de périphériques USB autorisées par défaut

•

•

•

•

•

•

•

•

•

•

•

•

-

-

-

Classes de périphériques USB refusées par défaut

-

-

-

-

-

-

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

Configuration des claviers Bloomberg

-
-

Pour empêcher l'assombrissement de la fenêtre Desktop Viewer

-
-

-
-

Pour configurer les paramètres de plusieurs utilisateurs et machines

-
-
-

Configurer StoreFront.

Pour configurer StoreFront

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

-
-
-
-

SalesStore;https://sales.example.com/Citrix/Store/discovery;On;Store for Sales staff

Fournir des informations de compte aux utilisateurs

-
-
-

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

Fournir un fichier de provisioning aux utilisateurs

-

Fournir aux utilisateurs des informations de compte à entrer manuellement

-
-

-

-

NetScalerGatewayFQDN?NomMagasin

Optimisation de l'environnement de Receiver

-
-
-
-
-
-
-

Réduction du temps de lancement des applications

-

-

-
-

Valeurs de registre HKLM

Valeurs de registre HKCU

Mapper des machines clientes

-
-
-

Désactivation du mappage des machines utilisateur

Rediriger les dossiers clients

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

Redirection de périphérique USB Plug and Play HDX

Pour mapper des ports COM clients à un port COM serveur

Prise en charge de la résolution de nom DNS

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

utilisation de serveurs proxy avec les connexions XenDesktop ;

Nov 20, 2015

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 plus d'informations, veuillez consulter la [documentation Interface Web](#).

Amélioration de l'expérience utilisateur

Nov 19, 2015

Vous pouvez améliorer l'expérience de vos utilisateurs grâce aux fonctionnalités suivantes :

Receiver 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 Receiver 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.

Receiver vous permet d'utiliser jusqu'à huit moniteurs.

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 appuyez sur le bouton 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 de plus amples informations sur le calcul des exigences de mémoire graphique de la session pour XenApp et XenDesktop, consultez l'article [ctx115637](#).

Si le paramètre de stratégie Valeurs par défaut de l'optimisation de l'impression universelle Autoriser 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.

Pour activer l'accès tactile aux applications et bureaux virtuels à partir de tablettes Windows, Receiver 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, Receiver 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 (tablette avec clavier amovible), créez une valeur REG_DWORD dans DisableKeyboardPopup in HKLM\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver et définissez-la sur 1.

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

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 icaclient dans l'éditeur de stratégies de groupe, vous pouvez ignorer les étapes 2 à 5.

2. Dans le volet 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 accédez au dossier de configuration de Receiver (généralement C:\Program Files\Citrix\ICA

Client\Configuration) et sélectionnez icaclient.adm.

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) > Citrix Components > Citrix Receiver > User Experience > Keyboard shortcut.
7. Dans le menu Action, choisissez Propriétés, sélectionnez Activé et choisissez les options souhaitées.

Receiver 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 : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez 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\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.

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 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 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.

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+Attention 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).

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.

Sécurisation de vos connexions

Nov 19, 2015

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

L'authentification Stimulation/Réponse Windows NT (NTLM) est prise en charge par défaut sur les ordinateurs Windows.

Configurer l'authentification unique sur un domaine

Nov 20, 2015

Cette rubrique vous explique comment activer l'authentification unique sur un domaine pour Citrix Receiver avec XenDesktop ou XenApp.

Remarque : dans cet exemple, l'installation de Receiver, l'application d'une stratégie d'ordinateur et la configuration d'un site approuvé sur le système d'exploitation client sont effectuées manuellement. Dès qu'un modèle d'objet de stratégie de groupe (GPO) a été créé, vous pouvez l'appliquer à toute machine cliente du domaine sur laquelle Receiver a été installé.

1. Installez Citrix Receiver 4.2 à l'aide du commutateur `/includeSSON`.
 1. Installez un ou plusieurs magasins StoreFront. Vous pouvez effectuer cette étape ultérieurement. L'installation de magasins StoreFront n'est pas une condition préalable à la configuration de l'authentification unique sur un domaine. Pour de plus amples informations sur la syntaxe à utiliser pour ajouter un ou plusieurs magasins StoreFront, consultez la section [Configurer et utiliser Receiver pour Windows à l'aide de paramètres de ligne de commande](#).
 2. Vérifiez que l'authentification unique est activée en démarrant Citrix Receiver et en confirmant que le processus `ssonsvr.exe` est en cours d'exécution.
2. Ajoutez le modèle d'administration de GPO ICA Client à la stratégie Ordinateur local sur la machine locale de l'utilisateur et/ou sur l'image principale du bureau VDA :
 1. Ouvrez `gpedit.msc`.

Remarque : le composant logiciel enfichable Éditeur d'objet Stratégie de groupe, `gpedit.msc`, est disponible avec les éditions Professionnelle, Entreprise et Intégrale de Windows 7 et Windows 8.
 2. Cliquez avec le bouton droit sur Configuration ordinateur > Modèles d'administration et sélectionnez Ajout/Suppression de modèles.
 3. Ajoutez le modèle `C:\Program Files\Citrix\ICA Client\Configuration\icaclient.adm`.
3. Activez le GPO Ordinateur local sur la machine locale de l'utilisateur et/ou sur l'image principale du bureau VDA :
 1. Choisissez Local user name and password.
 2. Sélectionnez Activé.
 3. Sélectionnez Enable pass-through authentication.
 4. Sélectionnez Allow pass-through authentication for all ICA connections.
 5. Cliquez sur OK.
 6. Redémarrez l'image principale du bureau VDA.
4. Connectez-vous aux Delivery Controller, puis ouvrez Windows PowerShell et exécutez les commandes suivantes pour permettre au Delivery Controller d'approuver les requêtes XML envoyées à partir de StoreFront.
 1. Si elles ne sont pas déjà chargées, chargez les applets de commande Citrix en tapant `asnp Citrix*`. (n'oubliez pas d'ajouter le point après Citrix*).
 2. Appuyez sur Entrée.
 3. Tapez ensuite `Add-PSSnapin citrix.broker.admin.v2` et appuyez sur Entrée.
 4. Tapez ensuite `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True` et appuyez sur Entrée.
 5. Fermez PowerShell.
5. Ouvrez Internet Explorer sur la machine locale et/ou sur l'image principale du bureau VDA.
6. Dans Options Internet > Sécurité > Sites de confiance, ajoutez le nom de domaine complet du ou des serveurs StoreFront à la liste, sans le chemin d'accès au magasin. Exemple : `https://storefront.exemple.com`

Remarque : vous pouvez également ajouter le serveur StoreFront aux Sites de confiance à l'aide d'un GPO Microsoft. Le GPO est appelé Liste des attributions de sites aux zones, et vous pouvez le trouver dans Configuration ordinateur > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Onglet Sécurité.

7. Fermez la session et rouvrez une session Receiver.

Lorsque Citrix Receiver s'ouvre, si l'utilisateur actuel est connecté au domaine, ses informations d'identification sont transmises à StoreFront et énumèrent les applications et bureaux dans Citrix Receiver, ainsi que dans le menu Démarrer de l'utilisateur. Lorsque l'utilisateur clique sur une icône, Receiver transmet les informations d'identification de domaine de l'utilisateur au Delivery Controller et l'application ou le bureau s'ouvre.

Pour activer l'authentification unique lorsque des sites ne se trouvent pas dans les zones Sites de confiance ou Intranet

Nov 20, 2015

Vos utilisateurs peuvent être invités, à l'aide de leurs informations d'identification, à utiliser l'authentification unique pour se connecter au serveur, mais ils ne peuvent pas ajouter de sites aux zones Sites de confiance ou Intranet. Activez ce paramètre pour activer l'authentification unique sur tous les sites, à l'exception des sites restreints.

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 icaclient dans l'éditeur de stratégies de groupe, vous pouvez ignorer les étapes 2 à 5.
2. Dans le volet 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 Configuration de Receiver (généralement, C:\Program Files\Citrix\ICA Client\Configuration) et sélectionnez icaclient.adm.
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) > Citrix Components > Citrix Receiver > User authentication > Local user name and password.
7. À partir du menu Local user name and password Properties, sélectionnez Activé, et cochez les cases Enable pass-through authentication et Allow pass-through authentication for all ICA connections.

Configurer l'authentification unique au domaine avec Kerberos

Nov 20, 2015

Cette rubrique s'applique uniquement aux connexions entre Receiver et StoreFront, XenDesktop ou XenApp.

Receiver pour Windows prend en charge l'authentification unique de 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 Receiver, 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.

Receiver gère l'authentification unique avec Kerberos comme suit lorsque Receiver, 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 Receiver capture le code PIN de la carte à puce.
2. Receiver utilise IWA (Kerberos) pour authentifier l'utilisateur auprès de StoreFront. StoreFront fournit ensuite à Receiver 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 Receiver est uniquement requise afin d'éviter d'avoir à saisir de nouveau un code PIN. Si vous n'utilisez pas l'authentification Kerberos, Receiver 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 Receiver, assurez-vous que la configuration de Kerberos est conforme à ce qui suit.

- Kerberos fonctionne uniquement entre Receiver 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 unique 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 mauvaise

utilisation de l'Éditeur du Registre peut entraîner de sérieux problèmes et nécessiter la réinstallation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Veillez à effectuer une copie de sauvegarde avant de modifier le registre.

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 déploiement](#) de la documentation XenDesktop avant de continuer.

Lorsque vous installez Receiver, 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 Receiver 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 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 Receiver via la stratégie suivante :

Modèles d'administration > Modèles d'administration classiques (ADM) > Citrix Components > Citrix Receiver > User authentication > Local user name and password

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 Receiver 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 Receiver pour Windows 4.2 ou version ultérieure.
- Lorsque vous configurez le service d'authentification sur le serveur StoreFront, sélectionnez la case Authentification unique 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, reportez-vous à la section [Configurer le service d'authentification](#) dans la documentation de StoreFront.

Configuration de l'authentification par carte à puce

Nov 20, 2015

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 Receiver pour Windows pour les cartes à puce.

- **Authentification unique (Single Sign-On)** : l'authentification unique capture les informations d'identification de la carte à puce lorsque les utilisateurs ouvrent une session sur Receiver. Receiver utilise les informations d'identification capturées comme suit :
 - Les utilisateurs dont les machines appartiennent au domaine qui ouvrent une session Receiver 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 Receiver 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 unique requiert la configuration de StoreFront et Receiver.

- **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 laissée chez lui, ou que le certificat d'ouverture de session a expiré). Les magasins dédiés doivent être configurés par site pour autoriser cette fonctionnalité, en définissant `DisableCtrlAltDel` 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 [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 Receiver. Pour modifier la façon dont les certificats sont sélectionnés, configurez Receiver.
- **Authentification du certificat client** : l'authentification du certificat client requiert la configuration de NetScaler Gateway/Access Gateway et de StoreFront.
 - Pour accéder aux ressources StoreFront via NetScaler Gateway/Access 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/Access 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.
- 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.
- Receiver pour Windows ne reconnecte pas les sessions lorsqu'une carte à puce est insérée.
- Lorsque 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 unique à StoreFront avec NetScaler Gateway Plug-in n'est pas disponible pour les utilisateurs de cartes à puce.
- Les communications de 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 mauvaise utilisation de l'Éditeur du Registre peut entraîner de sérieux problèmes et nécessiter la réinstallation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Veillez à effectuer une copie de sauvegarde avant de modifier le registre.

Pour configurer Receiver, incluez l'option de ligne de commande suivante lors de son installation :

- `ENABLE_SSON=Yes`
L'authentification unique est également appelée Single Sign-On (SSO). L'activation de ce paramètre empêche Receiver 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) > Citrix Components > Citrix Receiver > User authentication > Local user name and password
- 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 Receiver de vérifier la présence du composant SSO, ce qui permet donc à Receiver 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 Receiver 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 unique 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 :

```
/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
```

Ceci empêche la capture d'informations d'identification lors de l'ouverture de session et permet à Receiver de stocker le code PIN lors de l'ouverture de session sur Receiver.

- 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 unique. En fonction de la configuration et des paramètres de sécurité, il se peut que vous deviez sélectionner l'option Allow pass-through authentication for all ICA pour l'authentification unique.

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, reportez-vous à la section [Configurer le service d'authentification](#) dans la documentation de StoreFront.

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 Receiver pour Windows.

Par défaut, si de multiples certificats sont valides, Receiver invite l'utilisateur à en choisir un dans la liste. Vous pouvez également configurer Receiver 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 Receiver, spécifiez l'option `AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }`.
Prompt est la valeur par défaut. Pour SmartCardDefault ou LatestExpiry, si plusieurs certificats répondent aux critères, Receiver invite l'utilisateur à choisir un certificat.
- Ajoutez la valeur de clé suivante à la ruche HKCU ou HKLM\Software\[Wow6432Node]\Citrix\AuthManager:
`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.

Par défaut, les invites de saisie du code PIN sont fournies par 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. 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 Receiver 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 Receiver, spécifiez l'option `AM_SMARTCARDPINENTRY=CSP`.
- Ajoutez la valeur de clé suivante à la clé de registre `HKLM\Software\[Wow6432Node\Citrix\AuthManager:SmartCardPINEntry=CSP`.

Pour activer la vérification des listes de révocation de certificats afin d'améliorer la sécurité de Receiver

Nov 20, 2015

Lorsque la vérification de la liste de révocation de certificats est activée, Receiver vérifie la révocation du certificat du serveur. En obligeant Receiver à vérifier ceci, vous pouvez améliorer 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 Receiver pour qu'il ne vérifie que sa liste de certificats locale ou pour qu'il vérifie les listes de certificats locale et 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 Receiver, s'il est en cours d'exécution. Assurez-vous que tous les composants de Receiver, y compris le Centre de connexion, sont fermés.

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 `icaclient` dans l'éditeur de stratégies de groupe, vous pouvez ignorer les étapes 2 à 5.
2. Dans le volet 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 Configuration de Receiver (généralement, `C:\Program Files\Citrix\ICA Client\Configuration`) et sélectionnez `icaclient.adm`.
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) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. Dans le menu Action, choisissez Propriétés et sélectionnez Activé.
8. Dans le menu déroulant CRL verification, sélectionnez l'une des options proposées.
 - Désactivée. Aucune vérification de liste de révocation n'est effectuée.
 - Only check locally stored CRLs. Les listes de révocation de certificats installées ou téléchargées préalablement sont utilisées dans la validation de certificat. La connexion échoue si le certificat est révoqué.
 - Require CRLs for connection. Les listes de révocation de certificats locales et d'émetteurs de certificats appropriés sur le serveur sont vérifiées. La connexion échoue si le certificat est révoqué ou s'il est introuvable.
 - Retrieve CRLs from network. Les listes de révocation de certificats des émetteurs de certificats appropriés sont vérifiées. La connexion échoue si le certificat est révoqué.

Si vous ne paramétrez pas le champ CRL verification, il prend par défaut la valeur Only check locally stored CRLs.

Sécurisation des communications de Receiver

Nov 19, 2015

Pour sécuriser les communications entre les sites XenDesktop ou les batteries de serveurs et Receiver, vous pouvez intégrer vos connexions Receiver à l'aide d'un large choix de technologies de sécurité, dont :

- Citrix NetScaler Gateway ou Access Gateway. Pour de plus amples informations, reportez-vous aux rubriques de cette section ainsi qu'à la documentation NetScaler Gateway, Access 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 Receiver 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. (Consultez la section [SSL](#) pour de plus amples informations sur la configuration de SSL pour XenApp 7.6 ou XenDesktop 7.6.)

Receiver 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 par les plates-formes Microsoft Windows XP, Windows Vista et Windows 7. Référez-vous aux guides de sécurité Windows XP, Windows Vista et Windows 7 disponibles à l'adresse <http://technet.microsoft.com> pour plus d'informations sur les modèles et les réglages associés.

Connexion avec NetScaler Gateway

Oct 31, 2016

Pour permettre aux utilisateurs distants de se connecter via NetScaler Gateway, configurez ce dernier pour fonctionner avec StoreFront

- Pour les déploiements StoreFront : autorisez les connexions des utilisateurs internes ou distants à StoreFront via NetScaler Gateway en intégrant NetScaler Gateway et StoreFront. Ce déploiement permet aux utilisateurs de se connecter à StoreFront pour accéder à des bureaux et applications virtuels. Les utilisateurs se connectent via Receiver.

Pour de plus amples informations sur la configuration de ces connexions, reportez-vous à la section [Intégration de NetScaler Gateway avec XenMobile App Edition](#) et aux autres rubriques sous ce nœud dans la documentation Produit de Citrix. Vous trouverez des informations sur les paramètres requis par Receiver pour Windows dans les rubriques suivantes :

- [Configuration de stratégies de session et de profils pour XenMobile App Edition](#)
- [Création du profil de session pour Receiver pour XenMobile App Edition](#)
- [Configuration de stratégies d'accès sans client personnalisées pour Receiver](#)

Pour permettre aux utilisateurs distants de se connecter via NetScaler Gateway à votre déploiement Interface Web, configurez NetScaler Gateway de manière à fonctionner avec l'Interface Web, comme décrit dans la rubrique [Fournir l'accès aux applications et bureaux virtuels via l'Interface Web](#) et ses sous-rubriques dans la documentation Produit de Citrix.

Connexion avec Access Gateway édition Enterprise

Oct 31, 2016

Pour permettre aux utilisateurs distants de se connecter via Access Gateway, configurez Access Gateway de manière à fonctionner avec StoreFront et App Controller (un composant de CloudGateway).

- Pour les déploiements StoreFront : autorisez les connexions des utilisateurs internes ou distants à StoreFront via Access Gateway en intégrant Access Gateway et StoreFront. Ce déploiement permet aux utilisateurs de se connecter à StoreFront pour accéder à des bureaux et applications virtuels. Les utilisateurs se connectent via Receiver.
- Pour les déploiements AppController : autorisez les connexions des utilisateurs distants à AppController en intégrant Access Gateway et AppController. Ce déploiement permet aux utilisateurs de se connecter à AppController afin d'accéder à leurs applications Web et SaaS et fournit les services ShareFile Enterprise aux utilisateurs de Receiver. Les utilisateurs se connectent via Receiver ou Access Gateway Plug-in.

Pour de plus amples informations sur la configuration de ces connexions, reportez-vous à la section [Intégration d'Access Gateway avec CloudGateway](#) et aux autres rubriques sous ce nœud dans la documentation Produit de Citrix. Vous trouverez des informations sur les paramètres requis par Receiver pour Windows dans les rubriques suivantes :

- [Configuration de stratégies de session et de profils pour CloudGateway](#)
- [Création du profil de session pour Receiver pour CloudGateway Enterprise](#)
- [Création du profil de session pour Receiver pour CloudGateway Express](#)
- [Configuration de stratégies d'accès sans client personnalisées pour Receiver](#)

Pour permettre aux utilisateurs distants de se connecter au travers d'Access Gateway à votre déploiement Interface Web, configurez Access Gateway de manière à fonctionner avec l'Interface Web, comme décrit dans la rubrique [Configuration d'Access Gateway édition Enterprise pour communiquer avec l'Interface Web](#) et ses sous-rubriques dans la documentation Produit de Citrix.

Connexion avec Secure Gateway

Nov 20, 2015

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 Receiver et le serveur. Il n'est pas nécessaire de configurer Receiver si vous utilisez la passerelle Secure Gateway en mode Normal et si les utilisateurs se connectent via l'Interface Web.

Receiver 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 Receiver.

Si le proxy Secure Gateway est installé sur un serveur dans le réseau sécurisé, vous pouvez l'utiliser en mode Relais. Consultez les rubriques relatives à Secure Gateway pour obtenir des informations sur le mode Relais.

Si vous utilisez le mode Relais, le serveur Secure Gateway fonctionne comme un serveur proxy. Dans ce cas, vous devez configurer Receiver 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.

Connexion via un pare-feu

Nov 20, 2015

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, Receiver doit pouvoir communiquer via le pare-feu avec le serveur Web et le serveur Citrix. Le pare-feu doit permettre le trafic HTTP (généralement via le port http 80 ou 443 si un serveur Web sécurisé est utilisé) pour les communications entre la machine utilisateur et le serveur Web. Pour les communications entre Receiver et le serveur Citrix, le pare-feu doit autoriser le trafic ICA entrant sur les ports 1494 et 2598.

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. Receiver se connecte ensuite au serveur à l'aide de l'adresse externe et du numéro de port. Pour plus d'informations, veuillez consulter la documentation relative à [l'Interface Web](#).

Application des relations d'approbation

Nov 20, 2015

La configuration d'un serveur approuvé est conçue pour identifier et appliquer des relations d'approbation ayant lieu dans les connexions de Receiver. Cette relation renforce la confiance des administrateurs et des utilisateurs de Receiver dans l'intégrité des données sur les machines utilisateur et empêche une utilisation malveillante des connexions de Receiver.

Lorsque cette fonction est activée, les logiciels Receiver peuvent spécifier les configurations requises pour l'approbation et déterminer s'ils peuvent ou non établir une connexion au serveur. Par exemple, un Receiver 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 la configuration de serveur de confiance est activée, les serveurs connectés doivent résider sur une 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 consulter l'aide en ligne d'Internet Explorer.

Pour activer une configuration de serveur de confiance

Si vous effectuez cette modification sur un ordinateur local, fermez tous les composants de Receiver, y compris le Centre de connexion.

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 `icaclient` dans l'éditeur de stratégies de groupe, vous pouvez ignorer les étapes 2 à 5.
2. Dans le volet 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 accédez au dossier de configuration de Receiver (généralement `C:\Program Files\Citrix\ICA Client\Configuration`) et sélectionnez `icaclient.adm`.
5. Cliquez sur Ouvrir pour ajouter le modèle, puis cliquez sur Fermer pour retourner à l'Éditeur de stratégie de groupe.
6. Développez le dossier Modèles d'administration sous le nœud Configuration utilisateur.
7. Dans l'éditeur de stratégie de groupe, développez Modèles d'administration > Modèles d'administration classiques (ADM) > Citrix Components > Citrix Receiver > Network routing > Configure trusted server configuration.
8. Dans le menu Action, choisissez Propriétés et sélectionnez Activé.

Niveau d'élévation et wfcrun32.exe

Nov 20, 2015

Lorsque le contrôle de compte utilisateur (UAC) est activé sur des machines exécutant Windows Vista, Windows 7 ou Windows 8, seuls les processus au même niveau d'élévation/d'intégrité que wfcrun32.exe peuvent lancer des 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.

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.

Connexion à Receiver via un serveur proxy

Nov 20, 2015

Cette rubrique s'applique uniquement aux déploiements faisant appel à l'Interface Web.

Les serveurs proxy permettent de limiter l'accès vers et depuis votre réseau, et de gérer les connexions entre les logiciels Receiver et les serveurs. Receiver prend en charge les protocoles de proxy SOCKS et de proxy sécurisé.

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.

Connexion avec le Relais SSL (Secure Sockets Layer)

Nov 20, 2015

Cette rubrique ne s'applique pas à XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 ou XenApp 7.5.

Vous pouvez intégrer Receiver avec le service Relais SSL. Receiver prend en charge les protocoles TLS. Receiver pour Windows 4.2 prend en charge le protocole TLS 1.0 uniquement.

- TLS (Transport Layer Security) est la dernière version normalisée du protocole SSL. Le groupe de travail Internet Engineering Taskforce (IETF) l'a rebaptisé TLS lorsqu'il est devenu responsable du développement de SSL sous la forme d'une norme ouverte. TLS garantit la sécurité des communications de données grâce à l'authentification des serveurs, au cryptage du flux de données et aux contrôles d'intégrité des messages. Certaines organisations, telles que les organisations gouvernementales américaines requièrent l'utilisation du protocole TLS pour sécuriser les communications de données. Ces organisations peuvent nécessiter l'utilisation d'une cryptographie validée, comme la norme FIPS 140 (Federal Information Processing Standard). La norme FIPS 140 est une norme de cryptographie.

Par défaut, le Relais SSL Citrix utilise le port TCP 443 du serveur XenApp pour les communications sécurisées TLS. Lorsque le relais SSL reçoit une connexion TLS, il déchiffre les données avant de les rediriger vers le serveur ou, si l'utilisateur a sélectionné le protocole d'exploration TLS+HTTPS, vers le Service XML Citrix.

Si vous configurez le Relais SSL Citrix pour l'écoute sur un port autre que le port 443, vous devez spécifier le numéro du port d'écoute non standard au plug-in.

Le Relais SSL Citrix vous permet de sécuriser les communications suivantes.

- Entre un client et un serveur sur lesquels TLS est activé. Les connexions utilisant le cryptage TLS sont indiquées au moyen d'une icône en forme de cadenas dans le Centre de connexion de Citrix.
- Avec un serveur exécutant l'Interface Web, entre le serveur XenApp et le serveur Web.

Pour obtenir des informations sur la configuration du Relais SSL en vue de sécuriser l'installation, veuillez consulter la documentation de XenApp.

Outre la configuration système requise, vous devez également vous assurer que :

- la machine utilisateur prenne en charge le cryptage 128 bits ;
- la machine utilisateur dispose d'un certificat racine permettant de vérifier la signature de l'autorité de certification sur le certificat de serveur ;
- Receiver « connaisse » le numéro du port d'écoute TCP utilisé par le service du Relais SSL sur la batterie de serveurs ;
- tout service pack ou mise à niveau recommandé par Microsoft soit appliqué.

Si vous utilisez Internet Explorer et si vous n'êtes pas sûr du niveau de cryptage pris en charge par votre système, consultez le site Web de Microsoft <http://www.microsoft.com> afin d'installer un service pack fournissant le cryptage 128 bits.

Important : Receiver prend en charge des longueurs de clé de certificat allant jusqu'à 4096 bits. Assurez-vous que les longueurs des certificats racine et intermédiaires de l'autorité de certification, ainsi que celles des certificats de vos serveurs, ne dépassent pas la longueur prise en charge par Receiver. Si cette condition n'est pas remplie, la connexion risque de ne pas aboutir.

Si vous effectuez cette modification sur un ordinateur local, fermez tous les composants de Receiver, y compris le Centre de connexion.

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 `icaclient` dans l'éditeur de stratégies de groupe, vous pouvez ignorer les étapes 2 à 5.
2. Dans le volet 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 accédez au dossier de configuration de plug-in (généralement `C:\Program Files\Citrix\ICA Client\Configuration`) et sélectionnez `icaclient.adm`.
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) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. Dans le menu Action, choisissez Propriétés, sélectionnez Activé et entrez un nouveau numéro de port dans la zone Allowed SSL servers au format suivant :

`serveur:NuméroPortRelaisSSL`

`NuméroPortRelaisSSL` correspond au numéro du port d'écoute. Vous pouvez utiliser un caractère générique pour spécifier plusieurs serveurs. Par exemple, `*.Test.com:NuméroPortRelaisSSL` fait correspondre toutes les connexions à `Test.com` au port spécifié.

Si vous effectuez cette modification sur un ordinateur local, fermez tous les composants de Receiver, y compris le Centre de connexion.

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 ajouté le modèle `icaclient` à l'éditeur d'objet de stratégies de groupe, vous pouvez ignorer les étapes 2 à 5.
 2. Dans le volet 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 accédez au dossier de configuration de Receiver (généralement `C:\Program Files\Citrix\ICA Client\Configuration`) et sélectionnez `icaclient.adm`.
 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) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
 7. Dans le menu Action, choisissez Propriétés, sélectionnez Activé tapez une liste de serveurs de confiance séparée par des virgules et le nouveau numéro de port dans la zone Serveurs SSL autorisés au format suivant :
- `NomServeur:NuméroPortRelaisSSL,NomServeur:NuméroPortRelaisSSL`

`NuméroPortRelaisSSL` correspond au numéro du port d'écoute. Vous pouvez spécifier une liste de serveurs SSL de confiance séparés par des virgules, similaires à l'exemple suivant :

`csgfq.Test.com:443,fred.Test.com:443,csgfq.Test.com:444`

ce qui se traduit par exemple de la manière suivante dans un fichier `appsrv.ini` :

[Word]

SSLProxyHost=csgdq.Test.com:443

[Excel]

SSLProxyHost=csgdq.Test.com:444

[Bloc-notes]

SSLProxyHost=fred.Test.com:443

Configurer et activer Receiver pour TLS

Nov 20, 2015

Cette rubrique ne s'applique pas à XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 ou XenApp 7.5.

Pour forcer Receiver à se connecter à l'aide du protocole TLS, vous devez spécifier TLS sur votre serveur Secure Gateway ou le service Relais SSL. Consultez les rubriques relatives à Secure Gateway ou votre documentation Relais SSL pour de plus amples informations.

Assurez-vous également que la machine utilisateur dispose de tous les éléments requis.

Pour utiliser le cryptage TLS pour toutes les communications effectuées par Receiver, configurez la machine utilisateur, Receiver et, si vous utilisez l'Interface Web, le serveur exécutant l'Interface Web. Pour obtenir des informations sur la sécurisation des communications StoreFront, reportez-vous aux rubriques figurant sous la section « Sécuriser » dans la documentation StoreFront.

Pour utiliser TLS afin de sécuriser les communications entre un Receiver sur lequel TLS est activé et la batterie de serveurs, vous avez besoin d'un certificat racine sur la machine utilisateur afin de vérifier la signature de l'autorité de certification sur le certificat de serveur.

Receiver prend en charge les autorités de certification prises en charge par le système d'exploitation Windows. Les certificats racine de ces autorités de certification sont installés avec Windows et gérés à l'aide d'utilitaires Windows. Il s'agit des mêmes certificats racines que ceux utilisés par Microsoft Internet Explorer.

Si vous utilisez une autorité de certification différente, vous devez obtenir un certificat racine auprès de celle-ci et installer ce certificat sur chaque machine utilisateur. Ce certificat racine est ensuite utilisé et approuvé par Microsoft Internet Explorer et par Receiver.

Vous pouvez installer le certificat racine à l'aide d'autres méthodes d'administration ou de déploiement telles que :

- l'utilisation de l'Assistant de configuration et du Gestionnaire de profil IEAK (Microsoft Internet Explorer Administration Kit) ;
- l'utilisation d'outils de déploiement tiers.

Vérifiez que les certificats installés par votre système d'exploitation Windows sont conformes aux exigences de sécurité en vigueur dans votre société, ou utilisez les certificats fournis par l'autorité de certification de votre entreprise.

1. Pour utiliser TLS afin de crypter les données d'énumération et de démarrage des applications, transmises entre Receiver et le serveur exécutant l'Interface Web, configurez les paramètres appropriés à l'aide de l'Interface Web. Vous devez inclure le nom de machine du serveur XenApp qui héberge le certificat SSL.
2. Pour utiliser le protocole HTTP sécurisé (HTTPS) pour le cryptage des informations de configuration transmises entre Receiver et le serveur exécutant l'Interface Web, entrez l'adresse URL du serveur au format `https://nomserveur`. Dans la zone de notification de Windows, cliquez avec le bouton droit de la souris sur l'icône de Receiver et choisissez Préférences.
3. Cliquez avec le bouton droit sur l'entrée Online Plug-in dans État du plug-in et choisissez Changer le serveur.

Si vous effectuez cette modification sur un ordinateur local, fermez tous les composants de Receiver, y compris le Centre de connexion.

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 avec Active Directory.
Remarque : si vous avez déjà importé le modèle `icaclient` dans l'éditeur de stratégies de groupe, vous pouvez ignorer les étapes 2 à 5.
2. Dans le volet 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 accédez au dossier de configuration de Receiver (généralement `C:\Program Files\Citrix\ICA Client\Configuration`) et sélectionnez `icaclient.adm`.
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) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. Dans le menu Action, choisissez Propriétés, sélectionnez Activé puis, dans les menus déroulants, sélectionnez les paramètres TLS.
 - Définissez le paramètre TLS sur la valeur TLS ou Detect all pour activer TLS. Si vous sélectionnez Detect all, Receiver se connecte en utilisant le cryptage TLS.
 - Définissez le paramètre SSL cipher suite sur Detect version pour que Receiver négocie un jeu d'algorithmes adapté parmi les jeux d'algorithmes « Government » et « Commercial ». Vous pouvez restreindre les jeux d'algorithme à la catégorie Government ou à la catégorie Commercial.
 - Définissez le paramètre CRL verification sur Require CRLs for connection nécessitant de Receiver qu'il tente d'extraire les listes de révocation de certificats (CRL) auprès des émetteurs de certificats pertinents.

Si vous effectuez cette modification sur un ordinateur local, fermez tous les composants de Receiver, y compris le Centre de connexion.

Pour répondre aux exigences de sécurité FIPS 140, utilisez le modèle Stratégie de groupe pour configurer les paramètres ou pour inclure les paramètres au fichier `Default.ica` sur le serveur exécutant l'Interface Web. Reportez-vous aux informations sur l'Interface Web pour obtenir davantage d'informations sur le fichier `Default.ica`.

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 `icaclient` dans l'éditeur de stratégies de groupe, vous pouvez ignorer les étapes 3 à 5.
2. Dans le volet 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 accédez au dossier de configuration de Receiver (généralement `C:\Program Files\Citrix\ICA Client\Configuration`) et sélectionnez `icaclient.adm`.
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) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.

7. Dans le menu Action, choisissez Propriétés, sélectionnez Activé puis, dans les menus déroulants, sélectionnez les paramètres corrects.
 - Définissez le paramètre TLS sur la valeur TLS ou Detect all pour activer TLS. Si vous sélectionnez Detect all, Receiver tente de se connecter en utilisant le cryptage TLS.
 - Définissez le paramètre SSL ciphersuite sur la valeur Government.
 - Paramétrez le paramètre CRL verification sur la valeur Require CRLs for connection.

Lorsque vous utilisez l'Interface Web, spécifiez le nom de l'ordinateur du serveur qui héberge le certificat SSL. Consultez les informations sur l'Interface Web pour obtenir des détails sur l'utilisation de TLS pour sécuriser les communications entre Receiver et le serveur Web.

1. Dans le menu Paramètres de configuration, sélectionnez Paramètres serveurs.
2. Sélectionnez l'option Utiliser SSL/TLS pour les communications entre les clients et le serveur Web.
3. Enregistrez vos modifications.

La sélection de cette option transforme les adresses URL afin qu'elles utilisent le protocole HTTPS.

Vous pouvez configurer le serveur exécutant XenApp pour qu'il utilise TLS afin de sécuriser les communications entre Receiver et le serveur.

1. Dans la console de gestion Citrix du serveur XenApp, ouvrez la boîte de dialogue Propriétés pour l'application que vous souhaitez sécuriser.
2. Sélectionnez Avancé > Options du client et assurez-vous de sélectionner Activer les protocoles SSL et TLS.
3. Répétez ces étapes pour chaque application que vous souhaitez sécuriser.

Lorsque vous utilisez l'Interface Web, spécifiez le nom de l'ordinateur du serveur qui héberge le certificat SSL. Consultez les informations sur l'Interface Web pour obtenir des détails sur l'utilisation de TLS pour sécuriser les communications entre Receiver et le serveur Web.

Vous pouvez configurer Receiver pour qu'il utilise TLS afin de sécuriser les communications entre Receiver et le serveur exécutant l'Interface Web.

Assurez-vous qu'un certificat racine valide est installé sur la machine utilisateur. Pour de plus amples informations, consultez la section [Installer des certificats racine sur des machines utilisateur](#).

1. Dans la zone de notification de Windows, cliquez avec le bouton droit de la souris sur l'icône de Receiver et choisissez Préférences.
2. Cliquez avec le bouton droit sur l'entrée Online Plug-in dans État du plug-in et choisissez Changer le serveur.
3. L'écran Changer le serveur affiche l'adresse URL configurée actuellement. Entrez l'adresse URL du serveur dans la zone de texte sous la forme `https://nomserveur` pour crypter les données de configuration à l'aide de TLS.
4. Cliquez sur Mettre à jour pour appliquer la modification.
5. Activez TLS dans le navigateur de la machine utilisateur. Pour plus d'informations, consultez l'aide en ligne du navigateur.

Signature de fichier ICA pour se protéger contre le lancement d'applications ou de bureaux provenant de serveurs non approuvés

Nov 20, 2015

Cette rubrique s'applique uniquement aux déploiements faisant appel à l'Interface Web utilisant des modèles administratifs d'ancienne génération.

La fonctionnalité de signature de fichier ICA permet de protéger les utilisateurs contre le lancement non autorisé d'applications ou de bureaux. Citrix Receiver 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 les lancements provenant de serveurs non approuvés. Vous pouvez configurer la stratégie de sécurité de Receiver pour vérifier la signature de lancement d'une application ou d'un bureau à l'aide d'objets de stratégie de groupe, de StoreFront ou de 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 les déploiements 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 Citrix ICA File Signing. Le service peut signer les fichiers ICA à l'aide d'un certificat provenant du magasin de certificats personnel de l'ordinateur.

Citrix Merchandising Server, en conjonction avec Receiver, 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.

Pour utiliser les objets de stratégie de groupe afin d'activer et de configurer la vérification de la signature de lancement d'une application ou d'un bureau, suivez cette procédure :

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 ica-file-signing.adm dans l'éditeur de stratégies de groupe, vous pouvez ignorer les étapes 2 à 5.
2. Dans le volet 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 accédez au dossier Configuration de Receiver (généralement C:\Program Files\Citrix\ICA Client\Configuration) et sélectionnez ica-file-signing.adm.
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) > Citrix Components > Citrix Receiver et accédez à Enable ICA File Signing.
7. Si vous choisissez Activé, vous pouvez ajouter ou supprimer des empreintes numériques de certificats de signature à la liste blanche des empreintes numériques de certificats approuvés en cliquant sur Show et en utilisant l'écran Show Contents. Vous pouvez copier et coller les empreintes numériques de certificat de signature à partir des propriétés du certificat de signature. Utilisez le menu déroulant Policy pour sélectionner Only allow signed launches (more secure) ou Prompt user on unsigned launches (less secure).

Option	Description
Only allow signed launches (more secure)	Autorise uniquement le lancement d'applications ou de bureaux correctement signés à partir d'un serveur approuvé. Un message d'avertissement s'affiche dans Receiver si une application ou un bureau dispose d'une signature non valide. L'utilisateur ne peut pas continuer et le lancement non autorisé est bloqué.
Prompt user on unsigned launches (less secure)	Invite l'utilisateur à confirmer à chaque tentative de lancement d'une application ou d'un bureau non signé ou dont la signature n'est pas valide. L'utilisateur peut soit continuer le lancement de l'application, soit abandonner le lancement (valeur par défaut).

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.

Configuration d'un navigateur Web et d'un fichier ICA pour activer l'authentification unique et gérer les connexions sécurisées aux serveurs approuvés

Nov 20, 2015

Cette rubrique s'applique uniquement aux déploiements faisant appel à l'Interface Web.

Pour utiliser l'authentification unique (SSO) et gérer les connexions sécurisées aux serveurs approuvés, ajoutez l'adresse du site du serveur Citrix aux zones Intranet local ou Sites de confiance dans Internet Explorer sous Outils > Options Internet > Sécurité sur la machine utilisateur. L'adresse peut inclure les caractères génériques (*) pris en charge par Internet Security Manager (ISM) ou être spécifique telle que protocole://URL[:port].

Le même format doit être utilisé dans le fichier ICA et les entrées du site. À titre d'exemple, si vous utilisez un nom de domaine complet (FQDN) dans le fichier ICA, vous devez également utiliser un FQDN dans l'entrée de la zone des sites. Les connexions XenDesktop utilisent uniquement un format de nom de groupe de bureau.

http[s]://10.2.3.4

http[s]://10.2.3.*

http[s]://nomhôte

http[s]://fqdn.exemple.com

http[s]://*.exemple.com

http[s]://cname.*.exemple.com

http[s]://*.exemple.co.uk

desktop://groupe-20nom

ica[s]://xaserveur1

ica[s]://xaserveur1.exemple.com

Ajoutez l'adresse exacte du site Interface Web dans la zone des sites.

Exemples d'adresses de sites Web

https://ma.société.com

http://10.20.30.40

http://serveur-nomhôte:8080

https://relais-SSL:444

Ajoutez l'adresse au format desktop://Nom du groupe de bureaux. Si le nom du groupe de bureaux contient des espaces, remplacez chaque espace par -20.

Utilisez l'un des formats suivants dans le fichier ICA pour l'adresse du site du serveur Citrix. Utilisez le même format pour l'ajouter aux zones Intranet local ou Sites de confiance dans Internet Explorer sous Outils > Options Internet > Sécurité sur la machine utilisateur.

Exemple d'entrée HttpBrowserAddress dans un fichier ICA

```
HttpBrowserAddress=XMLBroker.XenappServeur.exemple.com:8080
```

Exemples d'entrée d'adresse de serveur XenApp dans un fichier ICA

Si le fichier ICA contient uniquement le champ **Adresse** du serveur XenApp, utilisez l'un des formats suivants :

```
icas://10.20.30.40:1494
```

```
icas://ma.serveur-xenapp.société.com
```

```
ica://10.20.30.40
```

Pour définir les autorisations d'accès aux ressources clientes

Nov 20, 2015

Cette rubrique s'applique uniquement aux déploiements faisant appel à l'Interface Web.

Vous pouvez définir les autorisations d'accès aux ressources clientes à l'aide des zones Sites de confiance et Sites sensibles en :

- ajoutant le site Interface Web à la liste Sites de confiance ;
- apportant des modifications aux nouveaux paramètres de registre.

Remarque : en raison des améliorations apportées à Receiver, la procédure .ini disponible dans les versions précédentes du plug-in/Receiver est remplacée par ces procédures.

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Pour ajouter le site Interface Web à la liste des sites de confiance

1. Depuis le menu Outils d'Internet Explorer, sélectionnez Options Internet > Sécurité.
2. Sélectionnez l'icône Sites de confiance et cliquez sur le bouton Sites.
3. Dans la case Ajouter ce site Web à la zone, tapez l'adresse URL de votre site Interface Web et cliquez sur Ajouter.
4. Téléchargez les paramètres de registre depuis <http://support.citrix.com/article/CTX133565> et apportez les modifications qui s'imposent. Utilisez SsonRegUpx86.reg pour les machines utilisateur Win32 et SsonRegUpx64.reg pour les machines utilisateur Win64.
5. Fermez la session sur la machine utilisateur, puis ouvrez-en une nouvelle.

Pour modifier les autorisations d'accès aux ressources clientes dans le registre

1. Téléchargez les paramètres de registre depuis <http://support.citrix.com/article/CTX133565> et importez-les sur chaque machine utilisateur. Utilisez SsonRegUpx86.reg pour les machines utilisateur Win32 et SsonRegUpx64.reg pour les machines utilisateur Win64.
2. Dans l'éditeur de registre, accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Client Selective Trust, et dans les zones appropriées, remplacez les valeurs par défaut par les valeurs d'accès requises pour les ressources suivantes :

Clé de ressource	Description de la ressource
FileSecurityPermission	Lecteurs clients
MicrophoneAndWebcamSecurityPermission	Micros et webcams
ScannerAndDigitalCameraSecurityPermission	Périphériques USB et autres

Valeur	Description
0	Aucun accès
1	Accès en lecture seule
2	Accès complet
3	Inviter l'utilisateur à s'identifier pour accéder aux ressources

Receiver Desktop Lock

Nov 19, 2015

Vous pouvez utiliser Receiver Desktop Lock lorsque les utilisateurs n'interagissent pas avec le bureau local. Les utilisateurs peuvent 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.

Receiver Desktop Lock fonctionne sur des machines appartenant à un domaine, sur lesquelles SSON est activé et qui sont configurées pour le magasin. 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 Receiver pour Windows 4.2.x.

Vous devez installer Citrix Receiver pour Windows à l'aide de l'indicateur /includeSSON . Vous devez configurer le magasin et le Single Sign-On, au choix avec le fichier adm ou l'option cmdline.

Puis, installez Receiver Desktop Lock en tant qu'administrateur à l'aide de l'option CitrixReceiverDesktopLock.MSI disponible à l'emplacement citrix.com/downloads.

Configuration système requise pour Citrix Receiver Desktop Lock

- Pris en charge sous Windows XP (édition Embedded), Windows 7 (y compris édition Embedded), Windows 7 Thin PC, Windows 8 et Windows 8.1.
- Se connecte à StoreFront via des protocoles natifs uniquement.
- Points de terminaison appartenant à des domaines.
- Les machines utilisateur doivent être connectées à un réseau local (LAN) ou un réseau étendu (WAN).

Remarque : la prise en charge de Windows XP a pris fin le 8 avril 2014 et coïncide avec l'arrêt de la prise en charge étendue de Windows XP par Microsoft.

Accès aux applications locales

Attention : 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. Voir [Configurer Local App Access et la redirection d'adresse URL](#) dans XenApp et XenDesktop pour plus d'informations.

Utilisation de Receiver Desktop Lock

- Vous pouvez utiliser Receiver Desktop Lock avec les fonctionnalités 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 Receiver 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 Receiver 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 de plus amples informations, consultez la section [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 Receiver Desktop Lock

Cette procédure installe Receiver pour Windows de telle sorte que les bureaux virtuels sont affichés via Receiver Desktop Lock. Pour les déploiements qui utilisent des cartes à puce, consultez 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 Receiver sur le

support d'installation).

Pour Receiver pour Windows 4.2 :

```
CitrixReceiver.exe /includeSSON STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/discovery;on;Desktop Store"
```

Pour des détails de commande, consultez la documentation relative à l'installation de Receiver pour Windows dans la section [Configurer et utiliser 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 Receiver Desktop Lock

N'accordez l'accès qu'à un seul bureau virtuel exécutant Receiver 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 Receiver Desktop Lock que celui utilisé pour l'installer.

- Assurez-vous que les fichiers `icaclient.adm` et `icaclient_usb.adm` 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 `.adm` 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 > Remoting client devices > Generic USB Remoting, activez et configurez les stratégies Existing USB Devices et New USB Devices.
- Mappage de lecteur : dans Citrix Receiver > Remoting client devices, activez et configurez la stratégie de mappage du lecteur client.
- Microphone : dans Citrix Receiver > Remoting client devices, activez et configurez la stratégie du microphone client.

Pour configurer des cartes à puce à utiliser avec les machines exécutant Receiver Desktop Lock

1. Configurer StoreFront.
 1. Configurez le service XML pour utiliser la résolution d'adresse DNS pour la prise en charge Kerberos.
 2. 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.
 3. Assurez-vous que l'authentification unique avec carte à puce est activée (activée par défaut).
 4. Activez Kerberos.
 5. Activez Kerberos et Authentification unique avec carte à puce.
 6. Activez Accès anonyme sur le site Web IIS par défaut et utilisez Authentification Windows intégrée.
 7. 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.
 1. Importez le modèle `icaclient.adm` depuis `%Program Files%\Citrix\ICA Client\Configuration\`.

2. Développez Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Receiver > Authentification de l'utilisateur.
 3. Activez Authentification par carte à puce.
 4. Activez Nom de l'utilisateur et mot de passe locaux.
3. Configurez la machine utilisateur avant d'installer Receiver Desktop Lock.
 1. Ajoutez l'adresse URL du Delivery Controller à la liste Sites de confiance de Windows Internet Explorer.
 2. 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.
 3. Configurez Internet Explorer afin d'utiliser la connexion automatique aux sites de confiance.

Lorsque Receiver 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 Receiver Desktop Lock.

Pour supprimer Receiver 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 Receiver Desktop Lock.
2. À partir de la fonctionnalité Windows pour la suppression ou la modification de programmes :
 - Supprimez Citrix Receiver Desktop Lock.
 - Supprimez Citrix Receiver.

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+Shift+. : 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.