À propos de cette version

Mar 03, 2016

Citrix Receiver pour Windows permet aux utilisateurs d'accéder en libre-service et en toute sécurité aux applications et bureaux virtuels mis à disposition par XenDesktop et XenApp.

Nouveautés de cette version

Intégration de RTME (RealTime Media Engine) améliorée

Cette version apporte des améliorations à l'installation de Citrix Receiver pour Windows en incorporant RTME au sein d'un seul package d'installation et de téléchargement. Précédemment, les utilisateurs devaient installer Citrix Receiver, puis lancer un package d'installation MSI séparé pour intégrer la fonctionnalité RTME à Receiver.

Cela engendrait une expérience utilisateur moins conviviale qui freinait l'adoption à grande échelle du pack d'optimisation HDX RealTime dans certaines organisations ; les utilisateurs BYOD (et télétravailleurs) devaient d'abord installer Citrix Receiver, puis revenir sur la page des téléchargements de Citrix pour télécharger un autre programme d'installation pour le RTME HDX. Un seul programme d'installation combine maintenant la dernière version de Citrix Receiver pour Windows et le programme d'installation RTME HDX.

Reportez-vous à l'article sur l'installation pour de plus amples informations sur l'utilisation du dernier programme d'installation de Citrix Receiver (qui comprend RTME HDX dans un seul exécutable).

Définir le niveau de transparence à l'aide de la stratégie de groupe de fiabilité de session

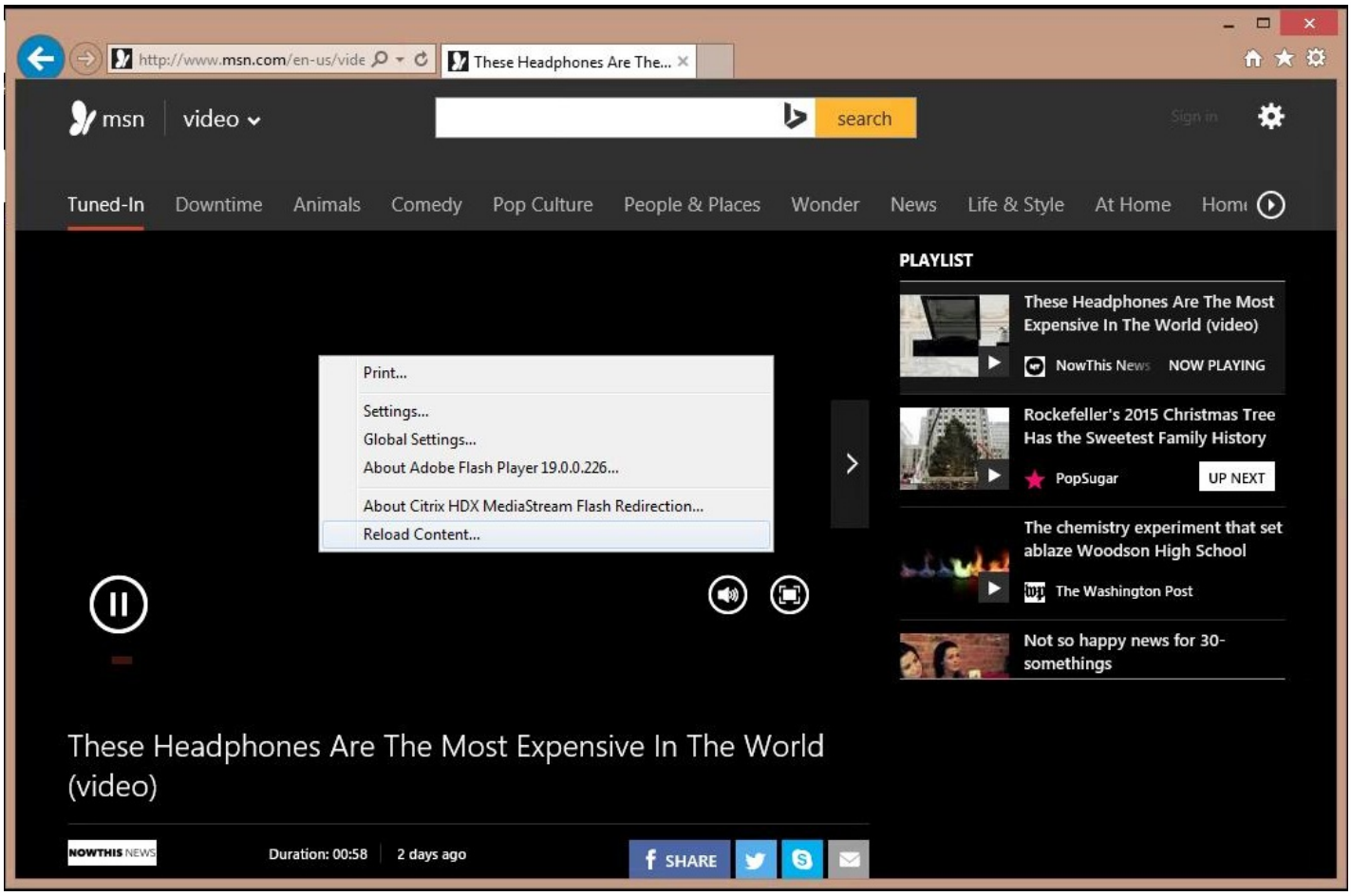
Cette version apporte des améliorations à la stratégie de groupe de fiabilité de session. Lors de la configuration de la stratégie de groupe de fiabilité de session, vous pouvez maintenant définir le niveau de transparence à appliquer à une application publiée (ou bureau) durant la période de reconnexion de la fiabilité de session. Consultez la section **Fiabilité de session et stratégie de groupe** dans la rubrique Configurer Receiver avec le modèle d'objet de stratégie de groupe pour de plus amples informations.

Retour manuel vers le rendu sur le serveur

Dans cette version, Citrix Receiver implémente un retour manuel vers le rendu sur le serveur sur le client. Dans certaines situations dans lesquelles vous visionnez du contenu Flash, un client peut constater un écran noir et ne disposer d'aucun moyen pour visionner la vidéo Flash. Dans la plupart des cas, si le contenu Flash ne peut pas être rendu sur le client, il est rendu automatiquement sur le serveur. Toutefois, dans certaines situations, le rendu échoue sur le client et n'est pas redirigé sur le serveur.

Pour remédier à de telles situations, Citrix Receiver pour Windows fournit maintenant une option qui permet aux utilisateurs d'actualiser manuellement l'écran et de forcer le rendu du contenu Flash sur le serveur. Pour utiliser le retour manuel, placez le curseur dans la fenêtre Flash noire et cliquez avec le bouton droit pour afficher un menu contextuel contenant une option permettant de « Recharger le contenu ». L'image ci-dessous illustre cette fonctionnalité.

> ### Remarque
>
> Les stratégies de prévention de retour à la vidéo définies par l'administrateur seront appliquées sur le client. Pour de plus amples informations, consultez Paramètres de stratégie multimédia et Paramètres de stratégie de la redirection Flash.



Mise à niveau des bibliothèques du SDK SSL pour prendre en charge la norme NIST SP800-52

Citrix Receiver fournit maintenant une bibliothèque SDK SSL mise à niveau pour inclure la prise de charge de la norme NIST SP800-52. Cette fonctionnalité permet à Citrix Receiver de prendre en charge la norme NIST SP800-52 pour les connexions TLS. Pour de plus amples informations, consultez la section Activer le mode de conformité avec la norme NIST SP800-52 dans la rubrique Pour définir les autorisations d'accès au client. Pour de plus amples informations sur la fiabilité de session, consultez la section **Fiabilité de session et stratégie de groupe** dans la rubrique Configurer Receiver avec le modèle d'objet de stratégie de groupe.

Processus de mise à niveau amélioré

Cette version de Citrix Receiver pour Windows dispose d'un programme d'installation mis à jour qui conserve les paramètres clients existants, ce qui améliore l'expérience utilisateur lors de la mise à jour de versions précédentes de Citrix Receiver. En outre, le programme d'installation mis à jour met à niveau les versions précédemment installées en toute transparence.

Reconnexion automatique des clients et améliorations apportées à la fiabilité de session

Ces améliorations offrent une meilleure interopérabilité avec CloudBridge et NetScaler Gateway. Une session peut se reconnecter à l'aide de la reconnexion automatique des clients et de la fiabilité de session quel que le soit le chemin de la connexion. Les améliorations spécifiques pour cette version sont les suivantes :

- Messages de connexion améliorés informant vos utilisateurs de l'état de leur connexion et leur indiquant quand ils ont perdu une connexion et comment procéder.

- Un minuteur (en minutes/secondes) affiche maintenant le temps qu'il reste avant l'expiration d'une session. Une session prend fin lorsque le minuteur expire. Par défaut, cette valeur est réglée sur 2 minutes. Vous pouvez changer la valeur par défaut dans le paramètre TransportReconnectMaxRetrySeconds du fichier ICA.

Performances HDX améliorées

Citrix Receiver a été mis à jour pour améliorer l'accélération matérielle du côté client. Cette fonctionnalité améliore les performances HDX 3D Pro sur les clients en activant l'accélération matérielle. Pour de plus amples informations sur cette fonctionnalité, reportez-vous à la section Décodage matériel dans l'article Expérience utilisateur.

Améliorations apportées à la plate-forme d'autorisation

Citrix Receiver pour Windows intègre maintenant une fonctionnalité qui améliore la façon dont vous pouvez vérifier que les clients se connectent aux serveurs à l'aide d'une version TLS spécifique. Cette fonctionnalité permet également de vérifier l'algorithme de cryptage spécifique, le mode, la taille de la clé et si SecureICA est activé ou non. Grâce à cette fonctionnalité, vous pouvez afficher le certificat d'authentification en cours utilisé par le client durant une session active. Pour plus d'informations veuillez consulter l'article XenApp - XenDesktop, qui explique comment la cryptographie est utilisée.

Boîtes de dialogue de lancement améliorées

Cette version améliore la façon dont Citrix Receiver pour Windows utilise les dialogues de lancement pour informer les utilisateurs de modifications ou mises à jour apportées au système. Elle affiche maintenant des notifications simples qui remplacent les notifications encombrantes du système lors du lancement d'une session.

Collecte d'informations de diagnostic améliorée

Cette version intègre un outil de diagnostic amélioré que vous pouvez utiliser pour collecter rapidement des informations système, et les distribuer en créant un seul package compressé qui peut être facilement transféré ou chargé sur des services tels que CIS.

Problèmes résolus dans cette version

Important : si vous utilisez XenApp ou XenDesktop 7.6, considérez l'installation du correctif VDA disponible sur CTX142037, CTX142094 et CTX142095. Ce correctif résout les problèmes lies à l'audio après la reconnexion de session, les réponses graphiques, la qualité de l'image et l'altération de l'écran dans certaines situations.

Problèmes résolus dans Citrix Receiver pour Windows 4.4

Jan 19, 2017

Receiver pour Windows 4.4 CU3 (4.4.3000)

Comparaison avec : Citrix Receiver pour Windows 4.4/CU2 (4.4.2000)

Receiver pour Windows 4.4 CU3 (4.4.3000) contient toutes les corrections qui ont été introduites dans Receiver pour Windows 4.0, 4.0.1, 4.1, 4.1.2, 4.1.100, 4.1.200, 4.2, 4.2.100, 4.3, 4.3.100, 4.4, 4.4 CU1 (4.4.1000) et 4.4 CU2 (4.4.2000) ainsi que les nouvelles corrections suivantes :

Local App Access

- Certaines applications SoftPhone ou Chrome risquent de ne pas s'afficher correctement lors de l'utilisation de Local App Access.

  [#LC4327]

- Après la déconnexion d'un bureau Local App Access (LAA) et la connexion à un bureau non-LAA en plein écran, la barre des tâches du côté client peut s'afficher au-dessus du bureau non-LAA desktop en plein écran.

  [#LC5966]

- Lors du basculement d'une fenêtre de session du mode plein écran au mode fenêtré, la boîte de dialogue suivante ne s'affiche pas :
  « La session est en mode fenêtré. Certaines fonctionnalités LAA peuvent ne pas fonctionner dans ce mode. »
  Lors du lancement d'une application en mode fenêtré, la boîte de dialogue suivante ne s'affiche pas :
  « Échec du lancement de l'application. La session est en mode fenêtré. Le lancement d'applications LAA est interdit dans ce mode. Basculez en mode plein écran pour poursuivre le lancement. »

  [#LC6291]

- Lorsque Local App Access est activé, la session de bureau est forcée de se lancer en mode plein écran.

  [#LC6294]

Mémoire, optimisation de l'UC

- Le processus SelfServicePlugin.exe peut consommer beaucoup de mémoire.

  [#LC4509]

Session/Connexion

- L'association de type de fichier peut ne pas fonctionner lors de la connexion à l'aide d'un profil utilisateur itinérant et de l'ouverture d'une application publiée.

  [#LC5184]

- Lorsque vous dictez dans SpeechMike avec une autre application de reconnaissance vocale, SpeechMike peut cesser de fonctionner.

  [#LC5632]

- L'utilisation du processus CleanUp.exe avec le commutateur /silent ne recharge pas Citrix Receiver correctement.

  [#LC6039]

- Le moteur HDX peut se fermer de manière inattendue.

  [#LC6047]

- Les tentatives de lancement d'un bureau à partir d'un client léger Wyse via NetScaler Gateway 11 peuvent entraîner le message d'erreur suivant :

  « Votre client a rencontré un problème avec l'authentification auprès du serveur. »

  [#LC6145]

- Il est possible que les sessions se bloquent si vous déplacez continuellement la fenêtre de session.

  [#LC6403]

Cartes à puce

- Lorsque Citrix Receiver pour Windows 4.4 est installé, une application publiée sur XenApp 6.5 peut envoyer une demande de clôture d'une transaction non active à une carte à puce. Citrix Receiver pour Windows peut répondre de manière incorrecte à cette demande en forçant le serveur XenApp à attendre indéfiniment une réponse ou la valeur d'expiration définie pour la transaction peut expirer.

  [#LC5772]

Expérience utilisateur

- Cette correction améliore la prise en charge des sons diffusés pendant une courte période lors de l'utilisation du mode temps réel pour l'audio client. Cette correction s'applique à l'audio de qualité moyenne.

  [#LC4941]

- L'association de type de fichier peut ne pas associer le type de fichier à l'icône et l'application correctes lors de l'utilisation de Windows 8.1 et de Windows Server 2012 R2. Grâce à cette correction, deux stratégies de groupe sont disponibles

sous « Libre-service ».
1. Activer FTA par défaut - Pour activer ou désactiver le comportement par défaut de l'association de type de fichier
2. Activer FTA - Pour activer ou désactiver la fonctionnalité d'association de type de fichier
Pour obtenir l'icône d'association de type de fichier appropriée, désactivez la stratégie de groupe « Activer FTA par défaut ».

[#LC5485]

- L'icône d'association de type de fichier (FTA) peut se comporter comme l'icône par défaut de l'association de type de fichier de Citrix Receiver pour Windows si vous vous connectez à un bureau publié ou si vous réinitialisez la configuration de Citrix Receiver pour Windows.

  [#LC5730]

- Les webcams Surface Pro 4 et HP Elite risquent de ne pas être redirigées vers une session. Remarque : la redirection webcam peut également échouer si la webcam ne prend pas en charge la résolution de l'écran.

  Pour résoudre ce problème, utilisez la clé de registre suivante :
  HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
  Nom : DefaultWidth
  Type : Dword
  Valeur : <résolution prise en charge par la webcam> Exemple (Surface Pro 4) : 1920

  HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
  Nom : DefaultHeight
  Type : Dword
  Valeur : <résolution prise en charge par la webcam> Exemple (Surface Pro 4) : 1080

  [#LC5750]

- Les bureaux attribués sur la base d'un nom de client ne sont pas énumérés correctement dans la fenêtre Libre-service. Ce problème se produit lors de l'utilisation de l'expérience unifiée StoreFront.

  [#LC5773]

Receiver pour Windows 4.4 CU2 (4.4.2000)

Comparaison avec : Citrix Receiver pour Windows 4.4/CU1 (4.4.1000)

Receiver pour Windows 4.4 CU2 (4.4.2000) contient toutes les corrections qui ont été introduites dans Receiver pour Windows 4.0, 4.0.1, 4.1, 4.1.2, 4.1.100, 4.1.200, 4.2, 4.2.100, 4.3, 4.3.100, 4.4 et 4.4 CU1 (4.4.1000) ainsi que les nouvelles corrections suivantes :

Redirection HDX MediaStream Flash	Expérience utilisateur
Clavier	Interface utilisateur
Local App Access	Interface Web

Redirection HDX MediaStream Flash

- Le contenu Flash ne s'exécute pas correctement depuis ProofHQ.com lorsque SOLFileHook est activé.

  [#LC4866]

- Lors de l'utilisation des versions 22 ou 18.0.0.360 d'Adobe Flash Player et de la navigation sur des sites Web avec contenu Flash, les URL des sites Web sont ajoutées à la liste noire dynamique et sont générées sur le serveur plutôt que sur la machine utilisateur.

  [#LC5626]

Clavier

- Lorsque la stratégie Raccourcis clavier est activée et que le processus wfica32 est exécuté sur une machine utilisateur, la fenêtre « Info : fin du mode Plein écran » peut s'afficher lors d'une connexion Bureau à distance. Cette boîte de dialogue n'accepte pas l'entrée au clavier et à la souris.

  [#LC4445]

- Le clavier local affiché à l'écran peut apparaître dans la session Citrix Receiver pour Windows chaque fois que vous entrez du texte à l'aide d'un périphérique Microsoft Surface Pro avec un clavier USB ou sans fil externe.

  [#LC5093]

Local App Access

- Lorsque Local App Access est activé, si les applications sont démarrées dans une session distante en mode plein écran ou fenêtre, les icônes des applications peuvent ne pas s'afficher dans la barre des tâches de la session VDA. Le point de terminaison peut afficher plusieurs icônes d'application dans la barre des tâches au lieu d'une seule.

  [#LC4217]

- Lorsque vous démarrez une session de bureau publié alors que Local App Access est activé, la barre des tâches Desktop Viewer peut disparaître.

  [#LC5064]

- Lorsque vous êtes connecté à un VDA sur lequel est activé Local App Access, le sélecteur de tâches du point de terminaison s'affiche par intermittence dans la session VDA lorsque vous appuyez sur ALT+TAB.

  [#LC5084]

- Un bureau sur lequel est activé Local App Access peut ne pas être généré correctement lors du basculement du mode fenêtre vers le mode plein écran.

  [#LC5091]

- Lors de la déconnexion d'un VDA sur lequel est activé Local App Access, la barre des tâches peut rester en mode

« Masquer automatiquement ».

[#LC5183]

Session/Connexion

- Les tentatives d'annulation de l'invite de certificat lorsque l'authentification de certificat client NetScaler est définie sur « Facultative » peuvent entraîner l'échec du démarrage d'une application publiée avec l'erreur client inconnu 1110.

  [#LC4169]

- Une session à plusieurs écrans avec changement rapide d'utilisateur peut afficher la session sur un seul écran après la reconnexion à la machine cliente.

  [#LC4382]

- Si vous démarrez une application transparente depuis une machine utilisateur 1 avant de vous connecter à cette machine utilisateur depuis une machine utilisateur 2 via RDP, l'application transparente démarrée peut s'afficher en mode plein écran et se superposer sur la barre des tâches de la machine utilisateur 1. Ce problème persiste après réduction et restauration de la fenêtre de l'application.

  [#LC4682]

- Les sessions connectées via NetScaler Gateway peuvent cesser de répondre tout en continuant à consommer une bande passante élevée.

  [#LC4710]

- Lorsque vous utilisez certains logiciels tiers tels que Cisco WAAS, les sessions Citrix Receiver pour Windows peuvent se déconnecter.

  [#LC4805]

- Cette correction résout un problème de mémoire dans un composant sous-jacent.

  [#LC4903]

- Après une mise à niveau vers Citrix Receiver pour Windows 4.4, les tentatives de démarrage d'applications peuvent échouer par intermittence lorsque vous vous connectez pour la première fois jusqu'à ce que Citrix Receiver pour Windows soit redémarré. Le message d'erreur suivant s'affiche :

  « Impossible de démarrer l'application. Contactez votre service d'assistance. »

  [#LC4975]

- Les tentatives d'accès à des applications via Citrix Receiver depuis StoreFront peuvent échouer depuis certaines machines utilisateur. Après avoir ajouté le magasin avec succès, le message d'erreur suivant peut d'afficher lors du processus d'énumération :

  « Connexion au serveur impossible.
  Vérifiez votre réseau et réessayez.
  Réessayez. »

[#LC5039]

- Le processus d'authentification unique (SSONSvr.exe) peut s'arrêter de manière inattendue ou les informations d'identification peuvent ne pas être transmises automatiquement à l'écran d'ouverture de session, entraînant l'affichage d'une invite à entrer les informations d'identification manuellement.

  [#LC5123]

- Citrix Receiver ignore la liste de contournement proxy dans Internet Explorer.

  [#LC5131]

- Après l'installation de Citrix Receiver pour Windows et la configuration d'un magasin via une entrée de registre ou un objet de stratégie de groupe (GPO), lorsque vous vous connectez pour la première fois après le redémarrage de la machine virtuelle, les applications peuvent ne pas être énumérées.

  [#LC5198]

- Lorsque l'option « Détecter automatiquement les paramètres de connexion » est activée dans Microsoft Internet Explorer, l'énumération des applications dans Citrix Receiver peut être lente.

  [#LC5224]

- Lorsque Framehawk est activé, le bouton de défilement d'une souris peut ne pas effectuer d'action dans une session de VDA XenDesktop 7.8. La correction côté VDA correspondante est disponible dans XenDesktop 7.9.

  [#LC5302]

- Les tentatives de démarrage d'applications en cliquant sur les icônes du menu Démarrer peuvent échouer par intermittence même si vous êtes déjà connecté.

  [#LC5306]

- Le processus wfica32.exe peut s'arrêter de manière inattendue sur la première session de saut lors de l'utilisation de Citrix Receiver pour Windows 4.4 et lorsque la machine utilisateur est un périphérique Android. Ce problème se produit lors d'une tentative de démarrage d'une application publiée dans un scénario double-hop (double saut) dans la session utilisateur.

  [#LC5391]

- Lors d'un mouvement toucher-déplacer, le bouton de la souris peut rester inactif lors de l'utilisation d'une application EPIC transparente. Lorsque vous relâchez le bouton hors de la fenêtre de l'application EPIC transparente, la session peut cesser de répondre.

  [#LC5644]

Exceptions système

- Citrix Receiver pour Windows peut s'arrêter de manière inattendue avec le message d'erreur suivant :

  « Citrix HDX Engine ne fonctionne plus. »

  [#LC4100]

- Lorsque vous exécutez un fichier .avi à plusieurs reprises dans le Lecteur Windows Media, le processus wfica32.exe peut se bloquer et s'arrêter de manière inattendue.

  [#LC4587]

- Lors du démarrage d'une application publiée via proxy, Citrix Receiver pour Windows peut s'arrêter de manière inattendue avec le message d'erreur suivant :

  « Citrix HDX Engine ne fonctionne plus. »

  [#LC5149]

- Citrix Authentication Manager (AuthMgrSvr.exe) peut s'arrêter de manière inattendue lorsque vous tentez d'ajouter un compte après avoir installé Citrix Receiver pour Windows 4.4 sur Windows Vista.

  [#LC5242]

Expérience utilisateur

- Lorsque Local App Access est activé, la fenêtre de la session peut se positionner hors de la fenêtre Desktop Viewer lorsque vous la restaurez depuis l'état agrandi.

  [#LC2930]

- Lors du mouvement toucher-déplacer, la saisie tactile depuis Citrix Receiver pour Windows peut envoyer certains événements de souris involontaires au serveur. L'application EPIC transparente peut alors cesser de répondre.

  [#LC5459]

Interface utilisateur

- Les tentatives d'ouverture de contenu sans abonnement via StoreFront avec expérience unifiée peuvent échouer avec le message d'erreur suivant :

  « Impossible de lancer votre application car les logiciels requis ne sont pas installés. »

  [#LC4308]

- Sur les systèmes d'exploitation de langue anglaise, le texte de l'erreur de protocole 1030 qui s'affiche dans Receiver pour Windows peut être illisible.

  [#LC4687]

- Lors de l'utilisation de VLC Media Player avec le mode apparence et Local App Access activés, le point de terminaison peut afficher plusieurs raccourcis de barres de tâches au lieu d'un seul.

  [#LC4744]

- L'icône GoToMeeting ne s'affiche pas dans la barre des tâches lorsqu'elle est ouverte à l'aide de l'URL de GoToMeeting dans une instance publiée de Microsoft Internet Explorer en mode transparent.

  [#LC4810]

- Lorsque vous changez d'utilisateurs d'API FastConnect, le message d'erreur suivant s'affiche :

« Vos applications ne sont pas disponibles pour l'instant. Réessayez dans quelques minutes. »

De plus, lorsque vous vous connectez à l'aide de l'API FastConnect, les raccourcis d'application de l'utilisateur précédent ne sont pas retirés du bureau.

[#LC5602]

Interface Web

- La page d'installation de Citrix Receiver pour Windows ne s'affiche pas dans l'interface Web lorsqu'une version antérieure de Citrix Receiver est installée sur la machine utilisateur.

  [#LC4242]

Divers

- Le processus wfica32.exe peut consommer jusqu'à 100 % de l'UC.

  [#LC4520]

- Lorsque vous créez un magasin à l'aide de la commande « SelfService.exe command, -init –createprovider », par exemple « C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\SelfService.exe -init -createprovider store https://<StoreFrontURL>/Citrix/store/discovery », les clés de registre liées sont créées correctement. Cependant, si vous cliquez sur l'icône Receiver dans la zone de notification pour accéder à l'interface utilisateur en libre-service, le magasin est supprimé du registre et la boîte de dialogue d'ajout de compte peut s'afficher.

  [#LC5096]

- Le processus wfica32.exe peut consommer jusqu'à 100 % de l'UC.

  [#LC5189]

- Les paramètres Client Selective Trust (CST) peuvent ne pas être conservés et l'invite d'accès au fichier HDX apparaît au cours du premier démarrage et des démarrages suivants même après avoir sélectionné l'option « Ne plus me demander pour ce bureau virtuel ». Ce problème se produit lorsque de nouveaux registres sont créés pour le même VDA sous la clé de registre « HKEY_Current_User\Software\Citrix\Ica Client\Client Selective Trust » même après avoir sélectionné l'option.

  [#LC5598]

- La configuration de NetScaler vers TLSv1.2 peut empêcher les machines utilisateur Windows 7 externes d'ajouter un compte StoreFront. Le message d'erreur suivant peut s'afficher :

  « Impossible de contacter le service d'authentification. »

  [#LC5737]

Receiver pour Windows 4.4 CU1 (4.4.1000)

Comparaison avec : Citrix Receiver pour Windows 4.4

Receiver pour Windows 4.4 CU1 (4.4.1000) contient toutes les corrections qui ont été introduites dans Receiver pour Windows 4.0, 4.0.1, 4.1, 4.1.2, 4.1.100, 4.1.200, 4.2, 4.2.100, 4.3, 4.3.100 et 4.4 ainsi que les nouvelles corrections suivantes :

Problèmes liés aux machines clientes

- Lors de l'utilisation de Citrix Receiver pour Windows 4.3, les appareils connectés via USB 3.0 (y compris les claviers et les souris) peuvent cesser de fonctionner et afficher l'erreur DRIVER_POWER_STATE_FAILURE (0x9f).

  [#LC4542]

- La redirection USB est disponible pour les appareils Surface Pro équipés de claviers Type Cover/Touch Cover. Après la redirection USB, il est possible que le curseur de la souris et le clavier ne fonctionnent plus en dehors de la session. Une règle de refus a été ajoutée à l'installation afin d'empêcher la redirection des Surface Pro équipés de claviers Type Cover/Touch Cover. Pour de plus amples informations sur la façon dont ces règles fonctionnent, reportez-vous à l'article CTX137939.

  Remarque : cette correction s'applique uniquement aux nouvelles installations de Receiver. Dans le cas d'une mise à niveau, la règle de refus suivante doit être ajoutée manuellement au registre ci-dessous.

  Pour les systèmes d'exploitation 32 bits :
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

  Pour les systèmes d'exploitation 64 bits :
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

  Modifiez la valeur DeviceRules et ajoutez des règles de refus spécifiques au périphérique USB.
  DENY:vid=045e pid=079A # Microsoft Surface Pro TouchCover
  DENY:vid=045e pid=079c # Microsoft Surface Pro Type Cover
  DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
  DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
  DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer

  Suivez la même procédure en ajoutant un identificateur VID et PID à ces périphériques, ce qui empêche la redirection.
  DENY: vid=xxxx pid=xxxx la règle dédiée à des périphériques spécifiques doit être en haut de la liste dans devicerules.

  [#LC4992]

HDX MediaStream

- Lorsque vous ouvrez Internet Explorer dans une session Local App Access et que vous naviguez vers une page Web avec du contenu Flash, et qu'une application est ouverte et agrandie, le contenu du conteneur Flash du navigateur reste sur l'écran.

  [#LC4527]

Installation, désinstallation, mise à niveau

- Les tentatives de suppression de la fenêtre « Ajouter un compte » peuvent échouer lorsque vous suivez les instructions de l'article CTX135438 du centre de connaissances. Avec cette correction, la fenêtre « Ajouter un compte » peut encore s'afficher occasionnellement, même après sa fermeture ou après la réinitialisation ou le redémarrage de Citrix Receiver.

  [#LC4593]

Clavier

- Si une application publiée utilise la combinaison Ctrl+Alt+[touche], et que Alt+[touche] ou Ctrl+[touche] est une touche d'accès rapide de Citrix, la combinaison n'est pas envoyée au serveur.

  [#LC3592]

- Lors de l'utilisation d'une session ou d'applications en mode transparent, les clics de souris ne fonctionnent pas toujours comme prévu.

  [#LC4779]

Local App Access

- Après l'installation du plug-in de redirection d'adresse URL du navigateur portable de Mozilla Firefox, il se peut qu'une grande case blanche s'affiche en bas du navigateur.

  [#LC4351]

- Lorsque vous exécutez la commande redirector.exe pour enregistrer/désenregistrer des navigateurs dans une session, une fenêtre contenant des informations inutiles s'affiche. Avec cette amélioration, cette fenêtre ne s'affiche plus sauf si vous exécutez la commande redirector.exe avec l'option /verbose.

  [#LC4480]

- Lorsqu'un bureau publié sur lequel Local App Access est activé se connecte, la fenêtre de session peut ne pas répondre ou disparaître.

  [#LC4689]

- Le processus CDViewer.exe peut cesser de répondre lorsque Local App Access et la redirection USB sont activés dans Citrix Receiver.

  [#LC5018]

Impression

- L'intégration de polices peut parfois échouer lorsque des polices avec des symboles intégrés sont utilisées avec des pilotes d'imprimante EMF.

[#LC3334]

Fenêtres transparentes

- Lorsque vous démarrez et réduisez une application transparente, vous ne pouvez pas la restaurer ni l'agrandir depuis la barre des tâches.

  [#LC3990]

Session/Connexion

- La session ne se reconnecte pas correctement via la découverte automatique de proxy Web (WPAD). Lors de la reconnexion à une session déconnectée, le message suivant s'affiche : « La connexion réseau à votre application a été interrompue. Essayez d'accéder à votre application un peu plus tard ou contactez votre service d'assistance. »

  [#LC3077]

- L'ajout d'une URL StoreFront à une région différente de celle de la configuration spécifique des sites de confiance pour cette région ne fonctionne pas.

  [#LC3281]

- Pour utiliser des associations de type de fichier locales, utilisez la clé de registre suivante. La clé de registre suivante est définie sur true par défaut. Lorsque la clé est définie sur true, l'icône de fichier local est remplacée par l'icône Citrix Receiver s'il n'existe aucun autre programme associé à ce fichier sur la machine cliente. HKEY_CURRENT_USER\Software\Citrix\Dazzle\EnabledDefaultFTAs=false (REG_SZ)

  [#LC4096]

- Après expiration du délai imparti à la fiabilité de session et à la reconnexion automatique des clients, le lancement de la session est retardé et le partage de session ne fonctionne pas.

  [#LC4143]

- La taille d'un lecteur client mappé peut s'afficher incorrectement et les fichiers ne peuvent pas être copiés sur le lecteur s'il dépasse 1 To. Avec cette correction, le lecteur affichera 0.99 To s'il dépasse 1 To. La taille d'un lecteur client mappé s'affiche uniquement lorsque l'option Mappage de lecteurs clients d'ancienne génération est activée.

  [#LC4214]

- Lorsque Local App Access (LAA) et Desktop Lock sont activés, la reconnexion à une session de bureau de serveur publiée en plein écran peut entraîner la perte de focus sur la session et cette dernière peut cesser de répondre.

  [#LC4253]

- L'option d'ouverture de session Windows « Changer d'utilisateur » change la résolution de la session du bureau virtuel.

  [#LC4452]

- Lors de l'utilisation de Citrix Receiver, le lancement d'applications peut ne pas fonctionner avec le SDK ICO.

  [Correction RcvrForWin4.4_14.4.1000][#LC4550]

- Lorsqu'un utilisateur se connecte à StoreFront via le Self Service Plug-in, le processus SelfService.exe peut, par

intermittence, pendre le focus des autres fenêtres actives toutes les heures.

[#LC4628]

- Les applications Epic peuvent parfois perdre le focus lors du basculement vers un autre réseau.

  [#LC4731]

- Le processus wfica32.exe peut se fermer de manière inattendue lorsque vous essayez de lancer une application, et le message d'erreur suivant s'affiche : « La connexion à a échoué avec le statut (Erreur de client inconnue 0) ».

  [#LC4768]

- Le paramètre de registre NotificationDelay contrôle le délai d'affichage de la barre de progression de connexion des connexions transparentes. Lorsqu'il est défini, ce paramètre de registre ne fonctionne pas toujours lors de l'utilisation du Self-Service Plug-in pour lancer l'application. Cette correction résout le problème.

  Sur Windows 32 bits :
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Nom : NotificationDelay
  Type : REG_DWORD
  Données :

  Sur Windows 64 bits :
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
  Nom : NotificationDelay
  Type : REG_DWORD
  Données :

  [#LC4969]

Exceptions système

- Lors de la mise à jour d'URL XenApp Services via un objet de stratégie de groupe, de l'application d'un nouvel objet de stratégie de groupe ou de la mise à jour du même objet de stratégie de groupe avec de nouvelles valeurs de magasin (telles que store1 et store2), Citrix Receiver pour Windows peut se fermer de manière inattendue.

  [#LC4145]

- Le processus wfica32.exe peut rencontrer une violation d'accès et se fermer de manière inattendue.

  [#LC4482]

- Le processus SelfService.exe peut consommer jusqu'à 100 % de l'UC.

  [#LC4494]

- Les sessions dans lesquelles le changement de processeur graphique est activé sur le point de terminaison peuvent cesser de répondre.

  [#LC4562]

Expérience utilisateur

- Cette correction améliore la prise en charge des sons diffusés pendant une courte période lors de l'utilisation du mode temps réel pour l'audio client. Cette correction s'applique à l'audio de faible qualité.

  [#LC2783]

- Les sons système de Windows sont parfois inaudibles dans XenApp 7.5.

  [#LC3926]

- Dans un environnement réseau instable, des messages tels que « Vos applications ne sont pas disponibles pour l'instant. Réessayez dans quelques minutes ou contactez votre service d'assistance avec les informations suivantes : Impossible de contacter [NomServeur]. » et « La connexion réseau à votre application a été interrompue. Essayez d'accéder à votre application un peu plus tard ou contactez votre service d'assistance. » peuvent s'afficher. Cette correction prend en charge la clé de registre suivante qui vous permet de désactiver ces messages.

  Sur Windows 32 bits :
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
  Nom : SuppressDisconnectMessage
  Type : REG_DWORD
  Données : 24(0x18)

  Sur Windows 64 bits :
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle
  Nom : SuppressDisconnectMessage
  Type : REG_DWORD
  Données : 24(0x18)

  [#LC4378]

Interface utilisateur

- Les raccourcis ne réapparaissent pas toujours si vous les supprimez manuellement puis que vous actualisez les applications.

  [#LC4020]

Receiver pour Windows 4.4

Comparaison avec : Citrix Receiver pour Windows 4.3.100

Receiver pour Windows 4.4 contient toutes les corrections qui ont été introduites dans Receiver pour Windows 4.0, 4.0.1, 4.1, 4.1.2, 4.1.100, 4.1.200, 4.2, 4.2.100, 4.3 et 4.3.100 ainsi que les nouvelles corrections suivantes :

Installation, désinstallation, mise à niveau	Session/Connexion
Clavier	Exceptions système
Local App Access	Expérience utilisateur
Ouverture de session/Authentification	Interface utilisateur

Installation, désinstallation, mise à niveau

- Après la désinstallation de Citrix Receiver, le Fournisseur WMI HDX Citrix peut ne pas fonctionner.

  [#LC3943]

Clavier

- Lorsque la fiabilité de session est activée, la fonctionnalité d'alignement ne fonctionne pas dans les sessions reconnectées. La fonctionnalité d'alignement est un paramètre de souris/clavier que vous configurez dans **Panneau de configuration** > **Souris** > **Options du pointeur** > **Placer automatiquement le pointeur sur le bouton par défaut dans les boîtes de dialogue**.

  [#LC1252]

- Le basculement entre fenêtres à l'aide de la combinaison Alt+Tab active les menus applicatifs dans une session de bureau publié.

  [#LC2947]

- Citrix Receiver et les sessions RDP partagent la même combinaison de raccourci clavier « Ctrl+Alt+Fin » pour invoquer la combinaison « Ctrl+Alt+Suppr » dans une session de terminal. En conséquence, le raccourci clavier pour la session RDP ne prend pas effet lorsqu'il est exécuté dans une session Citrix Receiver.

  Grâce à ce correctif, la combinaison de raccourci clavier « Ctrl+Alt+Fin » n'est pas une combinaison par défaut pour les sessions Citrix Receiver et elle peut être activée en définissant la clé de registre suivante :

  - *Sur Windows 32 bits* :

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    Nom : EnableCtrlAltEnd
    Type : DWORD
    Valeur : 1

  - *Sur Windows 64 bits* :

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
    Nom : EnableCtrlAltEnd
    Type : DWORD
    Valeur : 1 (si la valeur est 0, la combinaison Ctrl+Alt+Fin est utilisée dans la session RDP.)

  [#LC3131]

- Après la mise à niveau vers la version 4.2 de Citrix Receiver, les clics de souris dans les scénarios double hop peuvent être erratiques.

  [#LC3770]

Local App Access

- Lorsque Local App Access est activé, le fait de cliquer sur la souris pour redimensionner une session sur une machine virtuelle peut entraîner le blocage de la machine virtuelle.

  [#LC1853]

Ouverture de session/Authentification

- L'authentification unique peut ne pas fonctionner lorsque vous tentez d'ouvrir une session à l'aide d'un nom de domaine complet (FQDN) mis en cache à des fins d'identification.

  [#LC3305]

- Lorsque Receiver est configuré pour utiliser l'authentification pass-through pour un serveur Interface Web ou StoreFront dans une session de bureau publié, il est possible que Receiver ne transmette pas les informations d'identification et vous invite à les entrer.

  [#LC3388]

Session/Connexion

- Lorsque le pré-lancement de session est configuré, si vous essayez de vous reconnecter à une session dans laquelle une application publiée est exécutée, une instance supplémentaire de cette application publiée est ajoutée à la même session.

  [#LC1701]

- Une session exécutée au premier plan peut perdre le focus de manière inattendue.

  [#LC2198]

- Définissez la stratégie **ProxyEnabled = false** sous la ruche de registre **HKEY_LOCAL_MACHINE\SOFTWARE\\Citrix\AuthManager**, ce qui contournera le serveur proxy configuré sur IE. La ruche **Wow6432Node** ne s'applique pas si une architecture d'OS 32 bits est utilisée.

  [#LC3129]

- Dans une configuration Multi-Port ou Multi-Stream dans laquelle les données audio et vidéo sont configurées sur des ports distincts, l'audio peut ne pas être synchronisé avec la vidéo.

  [#LC3181]

- Les utilisateurs authentifiés auprès de Receiver 4.2 pour Windows avec une carte à puce peuvent être invités à saisir un code PIN lors du démarrage d'applications publiées XenApp.

  [#LC3187]

- La configuration « KEYWORDS:prefer » peut ne pas prendre effet pour une application publiée. Cela peut se produire lorsque l'utilisateur ferme sa session Receiver et que le processus SelfService.exe se ferme de manière inattendue.

  [#LC3190]

- Après la connexion à Citrix Receiver, les raccourcis d'application peuvent prendre beaucoup de temps à apparaître sur le menu Démarrer et le bureau de l'appareil utilisateur.

  [#LC3323]

- Les tentatives d'ouverture d'une vidéo .wmv à partir d'un e-mail dans une instance publiée de Microsoft Outlook peuvent échouer.

  [#LC3453]

- Lorsque le Desktop Viewer bascule du mode plein écran au mode fenêtre, une barre flottante peut s'afficher dans la session XenDesktop lors de l'utilisation de Receiver.

  [#LC3526]

- Les sessions de bureau peuvent se déconnecter au lieu de rester actives lorsque le système qui est installé avec Desktop Lock avec Receiver 4.3 est verrouillé.

  Pour activer cette correction, définissez la clé de registre suivante :

  - *Sur Windows 32 bits* :

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
    Nom : LiveInDesktopDisconnectonLock
    type : REG_SZ
    Valeur : False
  - *Sur Windows 64 bits* :

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle
    Nom : LiveInDesktopDisconnectonLock
    type : REG_SZ
    Valeur : False

  [#LC3579]

- Si vous avez souscrit à une application livrée en streaming sur un client pour Citrix Receiver sur lequel Citrix Offline Plug-in n'est pas installé, le message d'erreur suivant peut s'afficher lors de l'actualisation des applications dans Citrix Receiver :

  « Vos applications ne sont pas disponibles pour l'instant »

  [#LC3609]

- Lorsque vous ouvrez une session avec Citrix Receiver pour Windows, plusieurs sessions de pré-lancement sur différents serveurs de traitement peuvent s'afficher dans le même groupe de mise à disposition pour le même utilisateur.

  [#LC3676]

- Après libération de la barre d'outils Thomson Reuters Eikon dans une session comportant plusieurs moniteurs, l'espace occupé par la barre d'outils n'est pas récupéré par la session.

  [#LC3773]

- Si une version antérieure à 4.3 de Receiver pour Windows est installée sur un appareil et que l'utilisateur met à niveau le système d'exploitation de Windows 7, Windows 8 ou Windows 8.1 vers Windows 10, la désinstallation de Receiver via Ajout/Suppression de programmes peut échouer. Les tentatives de mise à niveau vers Receiver pour Windows 4.3 échouent également.

  [#LC3789]

- Le processus wfica32.exe peut se fermer de manière inattendue lors de la tentative de démarrage d'une nouvelle session.

  [#LC3795]

- Lorsque vous ouvrez des applications à partir d'un bureau publié via Citrix Receiver et que vous modifiez le dossier « %appdata% » sur un autre serveur de fichiers, le message d'erreur suivant peut s'afficher :

  Erreur 1046 : Le pilote virtuel n'est pas chargé. »

  [#LC3981]

- La fenêtre d'alarme d'une instance installée localement de Lotus Notes peut prendre le focus clavier des applications publiées.

  [#LC3889]

- Des icônes peuvent apparaître dans les dossiers de catégorie dans le menu Démarrer et sur le bureau. Il ne doit pas y avoir de dossier de catégorie pour le bureau. Le problème se produit lors de l'utilisation de la clé de registre « UseCategoryAsStartMenuPath » pour contrôler les icônes dans les dossiers de catégorie pour le menu Démarrer et le bureau.

  Pour activer cette correction, définissez les clés de registre suivantes :

  - Lorsque la clé de registre « UseDifferentPathsforStartmenuAndDesktop » est définie sur « false », la clé « UseCategoryAsStartMenuPath » contrôle la création de dossiers de catégorie aussi bien pour le menu Démarrer que le bureau.
  - Lorsque la clé de registre « UseDifferentPathsforStartmenuAndDesktop » est définie sur « true », la clé « UseCategoryAsStartMenuPath » contrôle la création d'un dossier de catégorie d'icône dans le menu Démarrer. La clé « UseCategoryAsDesktopPath » contrôle la création d'un dossier de catégorie d'icône sur le bureau.

  [#LC4052]

- Les tentatives de modification d'un mot de passe dans Citrix Receiver peuvent échouer avec le message d'erreur suivant :

  « L'ancien mot de passe saisi est incorrect. »

  [#LC4081]

Exceptions système

- Lors de l'utilisation de Microsoft AX Dynamics 2009 ou Excel 2007, Citrix Receiver 4.x peut se fermer de manière inattendue avec le message d'erreur suivant :

  « Citrix HDX Engine ne fonctionne plus. »

  [#LC3776]

Expérience utilisateur

- Lorsque vous tentez d'ajouter des icônes de raccourci au bureau dans une session Citrix Receiver, certaines icônes peuvent ne pas afficher l'icône spécifique à l'application. Au lieu de cela, l'icône de plage blanche générique s'affiche.

  [#LC4097]

- Même lorsque la clé « EnableFTU » est définie sur « false », l'assistant de connexion de Citrix Receiver ne peut pas être désactivé.

  Pour empêcher l'affichage de l'assistant de connexion, désactivez le paramètre de stratégie EnableFTU à l'aide de Receiver.adm/Receiver.admx :

  Configuration ordinateur > Modèles d'administration > Citrix Component > Citrix Receiver > SelfService > EnableFTU

  [#LC4133]

Interface utilisateur

- Après l'installation du plug-in de redirection d'adresse URL pour Mozilla Firefox, il se peut qu'une grande case blanche s'affiche en bas du navigateur.

  [#LC3409]

- Lorsque l'indicateur de registre de session transparente « ENABLE COLOR SYNC » est défini, une session peut ne pas hériter de certaines couleurs de la machine utilisateur et afficher du noir à la place.

  Pour activer cette correction, définissez la clé de registre suivante :

  HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/Citrix/wfshell/TWI
  Nom : SeamlessFlags
  Type : REG_DWORD
  Valeur : 0x10

  [#LC3768]

- Lors de la modification de l'adresse URL de StoreFront, si l'interface de Citrix Receiver Self-service Plug-in est ouverte puis fermée, il est possible que les applications définies comme désactivées s'affichent sous forme d'icônes fantômes au lieu d'être assombries.

  [#LC3863]

- L'énumération de certaines applications peut échouer par intermittence ; une icône noire s'affiche à la place de l'icône associée à ces applications.

  [#LC4065]

- Si vous modifiez l'icône d'une application publiée dans Citrix Studio, le raccourci de bureau de l'application ne s'actualise pas.

  [#LC4124]

Divers

- Lorsque vous ajoutez un compte à Citrix Receiver sur un ordinateur se trouvant derrière un proxy, Citrix Receiver n'utilise pas les paramètres du proxy lorsqu'il contacte les balises ; l'emplacement est défini sur aucun au lieu d'être défini sur extérieur ou intérieur.

  [#LC2100]

- La suppression de la valeur de registre « ConnectionCenter » de la clé suivante peut entraîner une réparation forcée de Citrix Receiver :

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

  [#LC3751]

Remarque : cette version de Citrix Receiver contient également toutes les corrections comprises dans les versions 4.3, 4.2, 4.1 et 4.0.

Problèmes connus dans Citrix Receiver pour Windows 4,4

Jan 19, 2017

Problèmes connus avec Citrix Receiver pour Windows 4.4 CU3 (4.4.3000)

Le problème connu suivant a été observé dans cette version, ainsi que les problèmes connus de Citrix Receiver pour Windows 4.4, 4.4 CU1 (4.4.1000) et 4.4 CU2 (4.4.2000) :

- Les tentatives de fermeture de Citrix Receiver après l'expiration de ACR/SR peuvent ne pas réussir. Pour résoudre ce problème, déconnectez-vous et reconnectez-vous à Citrix Receiver ou mettez fin au processus wfcrun32. [#336, #4115]

Problèmes connus avec Citrix Receiver pour Windows 4.4 CU2 (4.4.2000)

Le problème connu suivant a été observé dans cette version, ainsi que les problèmes connus de Citrix Receiver pour Windows 4.4 et 4.4 CU1 (4.4.1000) :

- « Lors du lancement d'un bureau publié dans une session Bureau à distance sans barre d'outils Desktop Viewer, la boîte de dialogue « Info : fin du mode Plein écran » peut ne pas s'afficher. Le raccourci clavier « Maj+F2 » fait apparaître ou disparaître la barre de titre de la fenêtre de session. Pour contourner le problème, appuyez sur Maj+F2 pour afficher votre bureau et réduisez la fenêtre de session. »

  [#LC4445, #639585]

Problèmes connus avec Citrix Receiver pour Windows 4.4 CU1 (4.4.1000)

Les problèmes connus suivants ont été observés dans cette version, ainsi que les problèmes connus de Citrix Receiver pour Windows 4.4 :

- Après la désinstallation de Citrix Receiver pour Windows, il est possible que la valeur de registre « Installer » sous la clé de registre HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ (sur les systèmes 32 bits) et HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ (sur les systèmes 64 bits) ne soit pas supprimée.

  [#635242]

Problèmes connus avec Citrix Receiver pour Windows 4.4

Les problèmes connus suivants ont été observés dans cette version :

- Lorsque vous changez l'orientation d'une application hébergée sur des appareils Windows 10 Surface Pro, une info-bulle indiquant « Sortie du mode plein écran » s'affiche. Pour résoudre ce problème, désactivez les info-bulles en définissant la clé de registre suivante :

  HKEY_CURRENT_USER\Software\Citrix\ica client\keyboard mappings\tips

  Utilisez 1 pour désactiver les info-bulles et 0 pour les activer ; si vous définissez cette valeur de clé de registre sur 1, toutes les info-bulles sont désactivées.

  [#608346]

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.

- Les sessions VDA sur les clients Windows 7 peuvent rencontrer des problèmes d'affichage dans lesquels un arrière-plan blanc apparaît derrière le texte de l'écran. Ce problème se produit lorsque les derniers pilotes GFX ne sont pas installés sur le client. Pour résoudre le problème sur les clients sur lesquels des anciens pilotes NVIDIA sont installés.

  Pour résoudre le problème sur les clients sur lesquels des anciens pilotes NVIDIA sont installés :

  1. Accédez au panneau de configuration NVIDIA.
  2. Accédez aux paramètres Vidéo.
  3. Dans la section « Comment régler les couleurs ? », sélectionnez « Avec les paramètres NVIDIA. »
  4. Dans les paramètres NVIDIA, sélectionnez l'onglet Avancé.
  5. Dans l'onglet Avancé, définissez la Plage dynamique sur « Complète (0-255) ».

  Vous pouvez également ignorer cette solution alternative en mettant à jour la machine cliente avec les derniers pilotes GFX.

  [#610197]

Remarque

Pour de plus amples informations sur l'utilisation du pilote NVIDIA, reportez-vous à la page Dynamic RGB Range Capability sur le site de support de NVIDIA.

- Les performances se détériorent lorsque vous êtes connecté à un VDA Windows 2008 R2 en mode graphiques H.264 lorsque le décodage matériel est activé sur le client. Citrix recommande d'utiliser le mode graphique d'ancienne génération sur le VDA pour éviter ce problème.

  [#609292, 611580]

- ACR ne parvient pas à se reconnecter à une session après de multiples cycles de déconnexion/reconnexion sur le client, ce qui oblige les utilisateurs à se reconnecter à StoreFront.

  [#567938]

- NetScaler Gateway End Point Analysis Plugin (EPA) ne fournit pas de prise en charge de Receiver pour Windows natif.

  [#534790]

- Lorsque la session d'un utilisateur anonyme est fermée, Desktop Viewer affiche un message qui n'est pas applicable pour une connexion anonyme. Dans de tels cas, les sessions anonymes sont automatiquement fermées par Receiver lorsque l'utilisateur se déconnecte. Étant donné qu'il n'existe aucune authentification pour de telles connexions, les sessions anonymes ne prennent pas en charge la reconnexion, l'itinérance entre les clients ou le contrôle de l'espace de travail.

  [#481561]

- Dans certaines instances de localisation (par exemple, l'exécution de Citrix Receiver en chinois), le démarrage d'une application et d'un bureau virtuel peut échouer si des informations d'identification localisées contiennent des paires de substitution dans un nom d'utilisateur.

[#556174]

- Si vous installez Receiver en tant qu'administrateur de domaine et sélectionnez l'option « Activer CEIP » lors de l'installation, la fenêtre de programme CEIP est grisée dans le menu À propos de.

  [#556179]

- Le contrôle du volume risque de ne pas fonctionner avec RealTimes pour Real Player au cours de la session en raison de problèmes de compatibilité avec RAVE.

  [#573549]

- Lors de l'utilisation du mode déconnecté, Receiver rencontre les problèmes suivants :
  - La perte de connectivité réseau n'entraîne pas de message d'erreur informant l'utilisateur de la condition. L'actualisation des applications, ou l'abonnement/le désabonnement, n'est pas possible lors de l'utilisation de Receiver en mode déconnecté. [#559792, #560091, #560360]
  - Les modifications apportées aux applications ou bureaux pendant que Receiver est en mode déconnecté ne sont pas synchronisées lorsque la connectivité réseau est rétablie. [#560362]

- Après la fermeture d'une session Receiver, lors de l'ouverture d'une autre session, le nom de l'utilisateur n'est pas affiché dans la partie supérieure droite de l'interface.

  [#562107]

- L'authentification par carte à puce ne fonctionne pas avec les sites XenApp Services ; cependant, cette fonctionnalité fonctionne avec les sites StoreFront. Pour résoudre ce problème, pointez l'authentification par carte à puce vers un site StoreFront.

- Les références à SSL peuvent toujours être visibles dans les étiquettes de champ dans l'interface utilisateur, par exemple **TLS and Compliance Mode Configuration**. Ces composants seront mis à jour dans une version ultérieure.

- La barre de langue ne s'affiche pas dans l'écran d'ouverture de session du client Desktop Lock. La solution consiste à utiliser la barre de langue flottante.

  [#502678]

- Les options Raccourci présentes dans Citrix Desktop Viewer ne fonctionnent pas lorsque la session est ouverte en mode fenêtre.

  [#510529]

- Le message d'alerte de Desktop Viewer lors de la déconnexion n'est pas applicable pour les sessions utilisateur anonyme. Il s'agit là d'un comportement normal.

  [#481561]

- Receiver pour Windows n'est pas installé sur une machine Windows Server 2012 R2 avec un compte utilisateur (non-admin).

  Pour résoudre ce problème :

  1. Cliquez sur **Démarrer**, tapez **regedit** et appuyez sur **Entrée**.
  2. Accédez au paramètre suivant :

  HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer

  Créer : DisableMSI Type : REG_DWORD Valeur = 0 (0 vous permet d'installer)

  [#492508]

- Les notifications de la barre d'état système peuvent parfois s'afficher en mode Desktop Lock.

  [#488620]

- Le clavier virtuel ne s'affiche pas automatiquement pour le VDA des services Terminal Server. La solution consiste à ouvrir le clavier virtuel à l'aide de l'icône de la barre d'outils de Desktop Viewer ou pour les applications, depuis l'icône de clavier virtuel sur la barre des tâches.

[#502774]

- La qualité audio est inférieure à celle attendue lors de l'accès à distance à un micro-casque USB (USB Logitech H340) via USB générique. Il s'agit là d'un comportement normal. L'optimisation audio n'est pas effectuée dans la redirection USB. Cette opération sera considérée comme une amélioration pour une version future.

  [#469670]

- Les gestes de pincement et de zoom ne fonctionnent pas sur les applications à distance au travers des versions antérieures à la version 7.0 de XenApp et XenDesktop, ou la version 7.0 ou version ultérieure de XenApp et XenDesktop sur Windows 2008 R2.

  [#517877]

Configuration système requise et compatibilité

Sep 20, 2016

Appareil

Système d'exploitation

- Windows 10
- Windows 8.1, éditions 32 bits et 64 bits (y compris l'édition Embedded)
- Windows 8, éditions 32 bits et 64 bits (y compris l'édition Embedded)
- Windows 7, éditions 32 bits et 64 bits (y compris l'édition Embedded)
- Windows Vista, éditions 32 et 64 bits
- Windows Thin PC
- Windows Server 2012 R2, édition Standard et Datacenter.
- Windows Server 2012, édition Standard et Datacenter.
- Windows Server 2008 R2, édition 64 bits
- Windows Server 2008, éditions 32 et 64 bits

Matériel

- Adaptateur vidéo VGA ou SVGA avec écran couleur
- Carte son compatible Windows pour la prise en charge du son (facultatif)
- Pour pouvoir vous connecter à la batterie de serveurs via un réseau, vous devez disposer d'une carte d'interface réseau (NIC) ainsi que d'un logiciel de transport en réseau approprié.
- Pour bénéficier de meilleures performances graphiques, les derniers pilotes GFX doivent être installés sur les machines clientes.

Périphériques tactiles

Citrix Receiver pour Windows 4.4 peut être utilisé sur des ordinateurs portables tactiles, des tablettes et moniteurs Windows 7 et 8.1, avec XenApp et XenDesktop 7 ou version ultérieure et Virtual Desktop Agents Windows 7, 8 et 2012.

Serveurs Citrix

- XenApp (l'un des produits suivants) :
  - Citrix XenApp 7.6
  - Citrix XenApp 7.5
  - Citrix XenApp 6.5, Feature Pack 2, pour Windows Server 2008 R2
  - Citrix XenApp 6.5, Feature Pack 1, pour Windows Server 2008 R2
  - Citrix XenApp 6.5 pour Windows Server 2008 R2
  - Citrix XenApp 4 avec Feature Pack 2 pour systèmes d'exploitation UNIX
- XenDesktop (l'un des produits suivants) :
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7.0
- Citrix VDI-in-a-Box
  - VDI-in-a-Box 5.3
  - VDI-in-a-Box 5.2
- Vous pouvez accéder à Citrix Receiver pour Windows 4.4 par le biais d'un navigateur en conjonction avec StoreFront

Receiver pour Web et l'Interface Web, avec ou sans le plug-in NetScaler Gateway.
StoreFront :

- StoreFront 3,0.x, 2.6, 2.5 et 2.1
  Permet d'accéder directement aux magasins StoreFront.
- StoreFront configuré avec un site Receiver pour Web
  Permet d'accéder aux magasins StoreFront à partir d'un navigateur Web. Pour connaître les limitations de ce déploiement, reportez-vous à la section « Remarques importantes » dans les sites Receiver pour Web.

Utiliser l'Interface Web en conjonction avec le client VPN NetScaler :

- Sites Web Interface Web 5.4 pour Windows
  Permet d'accéder à des applications et bureaux virtuels à partir d'un navigateur Web.
- Interface Web 5.4 pour Windows avec sites XenApp Services ou XenDesktop Services.

- Méthodes de déploiement de Citrix Receiver auprès de vos utilisateurs :
  - Autorisez les utilisateurs à effectuer un téléchargement depuis receiver.citrix.com, puis une configuration à l'aide d'une adresse e-mail ou de services en conjonction avec StoreFront.
  - Offre d'installation depuis un site Citrix Receiver pour Web (configuré avec StoreFront).
  - Offre d'installation de Receiver à partir de l'Interface Web Citrix 5.4.
  - Effectuez un déploiement à l'aide d'objets de stratégie de groupe (GPO) Active Directory (AD).
  - Effectuez un déploiement à l'aide de Microsoft System Center 2012 Configuration Manager.

Navigateur

- Internet Explorer
  Les connexions à Citrix Receiver pour Web ou à l'Interface Web prennent en charge le mode 32 bits d'Internet Explorer. Pour les versions Internet Explorer prises en charge, reportez-vous aux sections Configuration système requise pour StoreFront et Configuration requise pour l'Interface Web.

- Mozilla Firefox 18.x (version minimum prise en charge)
- Google Chrome 21 ou 20 (requiert StoreFront)

> **Remarque**
>
> Pour de plus amples informations sur les modifications apportées à la prise en charge du plug-in NPAPI de Google Chrome, consultez l'article Preparing for NPAPI being disabled by Google Chrome sur le blog de Citrix.

Connectivité

Citrix Receiver pour Windows prend en charge les connexions HTTPS et ICA-over-TLS par le biais des configurations suivantes :

- Pour les connexions LAN :
  - StoreFront utilisant StoreFront Services ou des sites Citrix Receiver pour Web
  - Interface Web 5.4 pour Windows utilisant des sites XenApp Services où XenApp Services

  Pour de plus amples informations sur les machines qui appartiennent à un domaine et celles n'appartenant pas à un domaine, reportez-vous à la documentation XenDesktop 7.

- Pour les connexions sécurisées à distance ou locales :
  - Citrix NetScaler Gateway 11.x

- Citrix NetScaler Gateway 10.5

Les machines gérées, appartenant à un domaine Windows (locales et distantes, avec ou sans VPN) et les machines n'appartenant pas à un domaine (avec ou sans VPN) sont prises en charge.

Pour de plus amples informations sur les versions de NetScaler Gateway et Access Gateway prises en charge par StoreFront, reportez-vous à la section Configuration système requise pour StoreFront.

> ### Remarque
>
> les références à NetScaler Gateway mentionnées dans cette rubrique s'appliquent également à Access Gateway, sauf indication contraire.

À propos des connexions sécurisées et des certificats

> ### Remarque
>
> Pour de plus amples informations sur les certificats de sécurité, reportez-vous aux rubriques figurant sous les sections Sécuriser les connexions et Sécuriser les communications.

Certificats privés (auto-signés)

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

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

Installation de certificats racine sur des machines utilisateur

Pour de plus amples informations sur l'installation de certificats racine sur des machines utilisateur ainsi que sur la configuration de l'Interface Web afin d'utiliser des certificats, reportez-vous à la section Sécuriser les communications de Receiver.

Certificats génériques

Les certificats génériques remplacent les certificats de serveur individuel pour n'importe quel serveur situé dans le même domaine. Citrix Receiver pour Windows prend en charge les certificats génériques, toutefois, ils doivent être uniquement utilisés conformément à la stratégie de sécurité de votre organisation. En pratique, des alternatives aux certificats génériques existent, par exemple un certificat qui contient la liste des noms de serveurs dans l'extension SAN (Subject Alternative Name) peut être pris en compte. Ce type de certificat peut être émis par des autorités de certification publiques et privées.

Certificats intermédiaires et NetScaler Gateway

Si votre chaîne de certificat contient un certificat intermédiaire, ce dernier doit être ajouté au certificat serveur de NetScaler Gateway. Pour de plus amples informations, reportez-vous à la section Configuration de certificats intermédiaires.

Authentification

Pour les connexions à StoreFront, Citrix Receiver prend en charge les méthodes d'authentification suivantes :

	Receiver pour Web à l'aide de navigateurs	**Site StoreFront Services (natif)**	**Site StoreFront XenApp Services (natif)**	**NetScaler sur Receiver pour Web (navigateur)**	**NetScaler sur site StoreFront Services (natif)**
Anonyme	Oui	Oui			
Domaine	Oui	Oui	Oui	Oui*	Oui*
Authentification pass-through au domaine	Oui	Oui	Oui		
Jeton de sécurité				Oui*	Oui*
Deux facteurs (domaine avec jeton de sécurité)				Oui*	Oui*
SMS				Oui*	Oui*
Cartes à puce	Oui	Oui	Non		
Certificat utilisateur				Oui (plug-in NetScaler)	Oui (plug-in NetScaler)

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

Remarque

Citrix Receiver pour Windows 4.4 prend en charge l'authentification à deux facteurs (domaine + jeton de sécurité) via NetScaler Gateway au service natif StoreFront.

Pour les connexions à l'Interface Web 5.4, Citrix Receiver prend en charge les méthodes d'authentification suivantes (l'Interface Web utilise le terme « Explicite » pour l'authentification de domaine et par jeton de sécurité) :

	Interface	**Site Interface**	**NetScaler sur**	**NetScaler sur un site**

	Web (navigateurs)	Web XenApp Services	l'Interface Web (navigateur)	Interface Web XenApp Services
Anonyme	Oui			
Domaine	Oui	Oui	Oui*	
Authentification pass-through au domaine	Oui	Oui		
Jeton de sécurité			Oui*	
Deux facteurs (domaine avec jeton de sécurité)			Oui*	
SMS			Oui*	
Cartes à puce	Oui	Non		
Certificat utilisateur			Oui (plug-in NetScaler)	

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

Pour de plus amples informations sur l'authentification, reportez-vous à la rubrique Configuration de l'authentification et de l'autorisation dans la documentation NetScaler Gateway et aux rubriques figurant sous la section Gérer dans la documentation StoreFront. Pour de plus amples informations sur les méthodes d'authentification prises en charge par l'Interface Web, reportez-vous à la rubrique Configuration de l'authentification pour l'Interface Web.

Mises à niveau

Citrix Receiver pour Windows 4.x peut être utilisé pour mettre Receiver pour Windows 3.x à niveau ainsi que Citrix Online Plug-in 12.x. Pour plus d'informations sur la mise à niveau, consultez la section Considérations à prendre en compte lors de la mise à niveau.

> **Remarque**
>
> Si vous effectuez une mise à niveau à partir de Citrix Receiver 3.4 vers la version 4.2.100, suivez les instructions fournies dans le Guide de mise à niveau de Receiver 3.4 vers Receiver 4.2.100. La version 4.2.100 ne prend pas en charge les mises à niveau sur place par les utilisateurs. L'administrateur informatique doit préparer l'environnement, de manière à ce que tous les utilisateurs du réseau puissent effectuer la mise à niveau. Les informations fournies dans le guide de mise à niveau proposent des instructions détaillées.

Autre

- **Configuration requise pour .NET Framework**
  - .NET 3.5 Service Pack 1 est requis par le Self-Service Plug-in, qui permet aux utilisateurs de souscrire à des applications et bureaux et de les lancer à partir de la fenêtre Receiver ou d'une ligne de commande. Pour de plus amples informations, consultez la section Configurer et utiliser Receiver pour Windows à l'aide de paramètres de ligne de commande.
  - .NET 2.0 Service Pack 1 et Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package sont requis pour garantir l'affichage de l'icône de Receiver. Le pack Microsoft Visual C++ 2005 Service Pack 1 est inclus avec .NET 2.0 Service Pack 1, .NET 3.5 et .NET 3.5 Service Pack 1 ; il est également disponible séparément.
  - Pour les connexions XenDesktop : afin d'utiliser Desktop Viewer, .NET 2.0 Service Pack 1 ou version ultérieure est requis. Cette version est requise, car en l'absence d'accès Internet, les vérifications de révocation de certificat ralentissent le lancement de la connexion. Cette version de Framework permet de désactiver les vérifications et d'améliorer les durées de démarrage mais pas avec .NET 2.0.
- Pour de plus amples informations sur l'utilisation de Receiver avec Microsoft Lync Server 2013 et le plug-in Microsoft Lync 2013 VDI pour Windows, reportez-vous à la section Prise en charge du plug-in VDI Microsoft Lync 2013 par XenDesktop, XenApp and Citrix Receiver.

- **Méthodes de connexion et transports réseau pris en charge :**
  - TCP/IP+HTTP
    Consultez l'article CTX 134341 pour obtenir les valeurs supplémentaires, qui peuvent être nécessaires.
  - TLS+HTTPS

Important

Si les magasins sont configurés dans StoreFront avec un type de transport correspondant à HTTP, vous devez également ajouter la valeur de clé suivante à la clé de registre HKLM\Software\[Wow6432Node\]Citrix\AuthManager: ConnectionSecurityMode=Any.

Avertissement

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.

Installer

Aug 25, 2016

Le pack d'installation CitrixReceiver.exe peut être installé :

- par un utilisateur depuis Citrix.com ou depuis votre propre site de téléchargement.
  - Un utilisateur qui utilise Receiver pour la première fois et qui obtient Receiver à partir de Citrix.com ou depuis votre propre site de téléchargement peut créer un compte en entrant une adresse e-mail à la place d'une adresse URL de serveur. Receiver détermine le serveur NetScaler Gateway (ou Access Gateway) ou StoreFront associé à l'adresse e-mail et invite l'utilisateur à ouvrir une session et à continuer l'installation. Cette fonctionnalité est appelée « découverte de compte basée sur une adresse e-mail ».
    Remarque : un nouvel utilisateur est un utilisateur qui n'a pas encore installé Receiver sur sa machine.
  - La découverte de compte basée sur l'adresse e-mail pour un nouvel utilisateur ne s'applique pas si Receiver est téléchargé à partir d'un emplacement autre que Citrix.com (tel qu'un site Receiver pour Web).
  - Si votre site nécessite la configuration de Receiver, utilisez une autre méthode de déploiement.
- Automatiquement à partir de Receiver pour Web où de l'écran d'ouverture de session de l'Interface Web
  - Un utilisateur qui utilise Receiver pour la première fois peut configurer un compte en entrant une adresse URL de serveur ou en téléchargeant un fichier de provisioning (CR).
- À l'aide d'un outil ESD (distribution électronique de logiciels)
  - Un utilisateur qui utilise Receiver pour la première fois doit entrer l'adresse URL d'un serveur ou ouvrir un fichier de provisioning pour créer un compte.

Aucun droit d'administrateur n'est requis pour installer Receiver à moins que l'authentification unique ne soit utilisée.

HDX RealTime Media Engine (RTME)

Un seul programme d'installation combine maintenant la dernière version de Citrix Receiver pour Windows et le programme d'installation RTME HDX. Lors de l'installation de cette version de Citrix Receiver, le RTME HDX est inclus au fichier exécutable (.exe).

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

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

- La dernière version de Citrix Receiver contient la dernière version de RTME HDX (ver 1.0.0.1) ; aucune autre installation n'est requise pour installer RTME.
- La mise à niveau à partir d'une version antérieure de Receiver vers la dernière version (Citrix Receiver avec RTME) est prise en charge. Les versions de RTME précédemment installées seront remplacées par la dernière version ; la mise à niveau à partir de la même version de Receiver vers la dernière version (par exemple, Receiver 4.4 vers Receiver 4.4 avec RTME) n'est pas prise en charge.
- Si vous disposez d'une version antérieure de RTME, l'installation de la dernière version de Receiver met automatiquement à jour RTME sur l'appareil de l'utilisateur.
- Si une version plus récente de RTME est présente, le programme d'installation conserve la dernière version.

Important

Pour être compatible avec le nouveau package RTME, la version minimum du HDX RealTime Connector installé sur vos serveurs XenApp/XenDesktop doit être 2.0.0.417 (version GA) ; en effet, RTME 2.0 ne peut pas être utilisé avec le 1.8 RTME Connector.

Mise à niveau manuelle vers Citrix Receiver pour Windows

Pour les déploiements avec StoreFront :

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

Pour les déploiements avec l'Interface Web

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

Considérations à prendre en compte lors de la mise à niveau

Conseil

Le processus de configuration de l'authentification unique (single sign-on) a été modifié pour Receiver pour Windows 4.x. Pour de plus amples informations, reportez-vous à la description de l'option /includeSSON dans la section Configurer et utiliser Receiver pour Windows à l'aide de paramètres de ligne de commande.

Citrix Receiver pour Windows 4.x peut être utilisé pour mettre Receiver pour Windows 3.x à niveau ainsi que Citrix Online Plug-in 12.x.

Si Receiver pour Windows 3.x était installé par machine, une mise à niveau par utilisateur (par un utilisateur sans privilèges administratifs) n'est pas prise en charge.

Si Receiver pour Windows 3.x était installé par utilisateur, une mise à niveau par machine n'est pas prise en charge.

Installation et désinstallation manuelle de Receiver pour Windows

Jan 29, 2016

Vous pouvez installer Receiver à partir du support d'installation, d'un partage réseau, de l'explorateur Windows, ou d'une ligne de commande en exécutant le pack d'installation CitrixReceiver.exe. Pour connaître les paramètres d'installation depuis une ligne de commande ainsi que l'espace requis, consultez la section Configurer et utiliser Receiver pour Windows à l'aide de paramètres de ligne de commande.

> ## Important
>
> Le processus de configuration de l'authentification unique (single sign-on) a été modifié pour Receiver pour Windows 4.x. Pour de plus amples informations, reportez-vous à la description de l'option /includeSSON dans la section Configurer et utiliser Receiver pour Windows à l'aide de paramètres de ligne de commande.

Si des stratégies propres à votre société vous interdisent d'utiliser un fichier .exe, reportez-vous à la section Comment extraire, installer et supprimer manuellement des fichiers .msi individuels.

Installation et configuration manuelles de Receiver pour l'authentification unique

Receiver peut être utilisé dans les scénarios d'authentification unique avec XenApp et XenDesktop. Cette section décrit également comment installer et configurer manuellement CitrixReceiver.exe de façon à utiliser l'authentification unique pour se connecter à un serveur Interface Web ou StoreFront.

Lorsque l'installation et la configuration ont été effectuées, les utilisateurs peuvent accéder à leurs ressources XenApp/XenDesktop sans avoir à entrer leurs informations d'identification. Les informations d'identification de la machine cliente sont transmises automatiquement au point de terminaison.

Tenez compte des exigences suivantes relatives à l'authentification unique :

- Le package d'installation de Citrix Receiver pour Windows est CitrixReceiver.exe.
- Chargez les fichiers de stratégie de groupe adéquats :
  - receiver.adm (situé dans le dossier %SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configuration sur une machine Windows sur laquelle Citrix Receiver est installé) ; le fichier receiver.adm doit être présent dans Windows XP, Windows 2003 et sur le client léger.
  - receiver.admx, receiver.adml (situé dans le dossier %SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configuration sur une machine Windows sur laquelle Citrix Receiver est installé) ; pour charger le fichier ADMX sur un GPO, référez-vous à la section « À propos de l'utilisation de modèles ADMX » dans la rubrique Configurer Receiver avec le modèle d'objet de stratégie de group.
- Des privilèges d'administrateur local sont requis sur la machine cliente pour permettre l'installation et la configuration de logiciels.
  Remarque : les fichiers .adm sont uniquement utilisés si vous exécutez XPe OS pour client léger.

Il existe deux scénarios de déploiement différents pour configurer l'authentification unique pour XenApp/XenDesktop lorsque des outils de déploiement logiciel d'entreprise tels que Citrix Merchandising Server ou Microsoft System Center

Configuration Manager ne sont pas utilisés :

1. Installez manuellement Citrix Receiver et effectuez la configuration à l'aide de la stratégie de groupe locale (importation de receiver.adm, receiver.admx, receiver.adml) sur différentes machines individuellement.
   Remarque : cette option est recommandée pour les environnements de petite taille.

2. Installez Citrix Receiver à l'aide de la stratégie de groupe Active Directory (par exemple, à l'aide de **CheckAndDeployCitrixReceiverEnterpriseStartupScript.bat**, qui est inclus avec XenApp). La configuration à l'aide de **receiver.adm, receiver.admx, receiver.adml** peut être appliquée à l'aide de la gestion des stratégies de groupe Active Directory à un grand nombre de machines et gérée de manière centralisée.

Cette option n'est pas traitée dans cet article en raison d'un niveau plus élevé de complexité. Référez-vous à l'article CTX134280 - Comment déployer Citrix Receiver Enterprise pour l'authentification unique à l'aide de la stratégie de groupe Active Directory pour plus d'informations.

Remarque : Citrix recommande fortement que les étapes décrites dans cet article soient testées et validées dans des environnements de test avant leur utilisation.

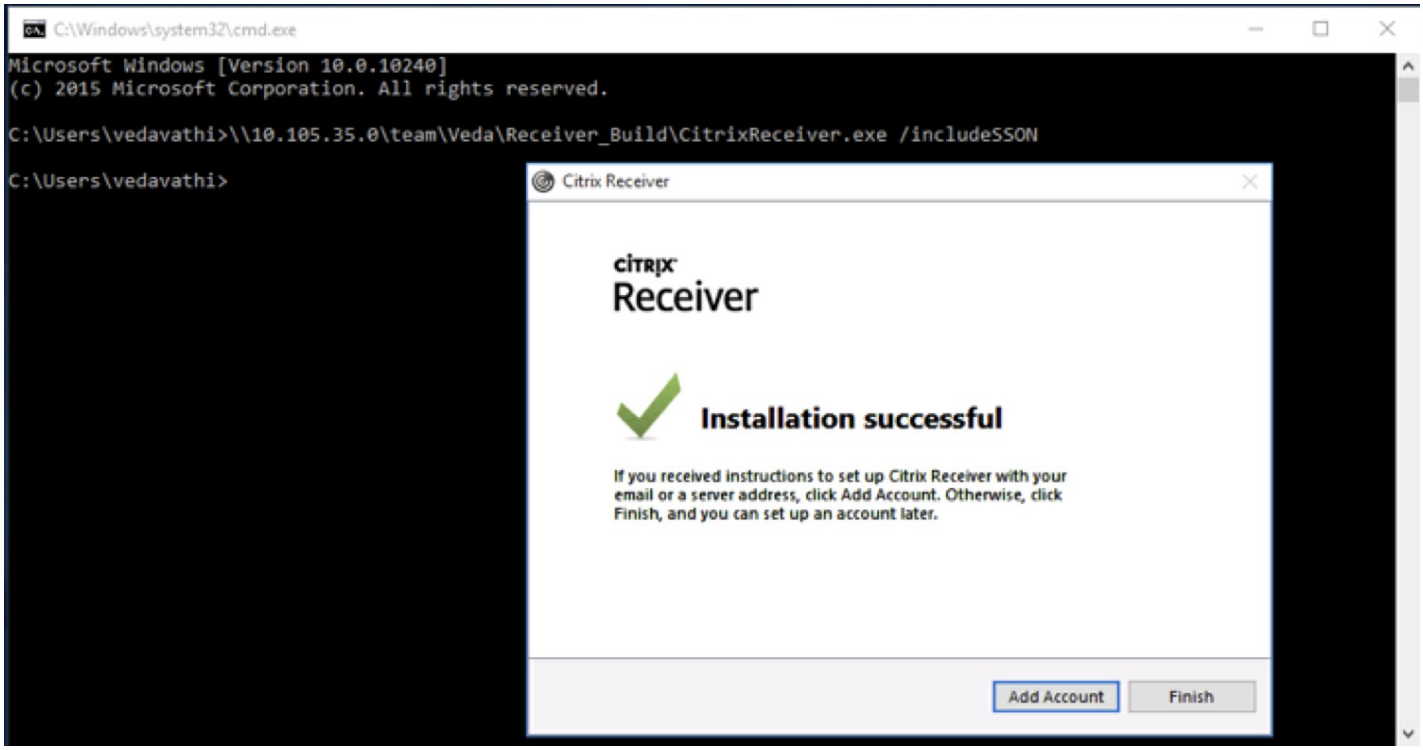
Pour installer et configurer Receiver manuellement pour l'authentification unique :

1. Exécutez la commande suivante à l'aide de PowerShell sur le Controller : **Set-BrokerSite -TrustedRequestsSentToTheXmlServicePort $True**
2. Ouvrez une session sur la machine cliente en tant qu'utilisateur disposant des droits d'administration.
3. Désinstallez les installations existantes de Online Plugin ou Citrix Receiver pour Windows de la machine cliente avant de démarrer le processus d'installation.
4. Téléchargez le pack d'installation de Citrix Receiver pour Windows (CitrixReceiver.exe) depuis le site de téléchargement de Citrix.

   Utilisez le déploiement d'installation approprié, soit à l'aide de la commande line, soit à l'aide de l'interface utilisateur.

Pour utiliser la ligne de commande :

1. Ouvrez l'**invite de commande Windows** et changez de répertoire vers celui dans lequel CitrixReceiver.exe est situé.
2. Sur **l'invite de commandes**, exécutez la commande suivante pour installer Citrix Receiver avec la fonctionnalité SSON activée : **CitrixReceiver.exe /includeSSON**. Tenez compte des informations contenues dans l'article Configuration et utilisation de Receiver pour Windows à l'aide de paramètres de ligne de commande ; le paramètre /includeSSON active l'authentification unique (SSO) pour Receiver standard (CitrixReceiver.exe). Cette option n'est pas prise en charge avec Receiver Enterprise (CitrixReceiverEnterprise.exe), qui installe Single Sign-On par défaut.
3. Une fois l'installation terminée, un message indiquant que l'installation a réussi s'affiche.



Pour utiliser l'interface utilisateur :

1. Double-cliquez sur CitrixReceiver.exe.
2. Dans l'assistant d'installation Activer l'authentification unique, sélectionnez la case Activer l'authentification unique pour installer Citrix Receiver avec la fonctionnalité SSON activée. Cela équivaut à installer Receiver à l'aide de la ligne de commande avec l'indicateur /includeSSON.

Remarque : l'assistant d'installation Activer l'authentification unique est seulement disponible pour les nouvelles installations sur une machine jointe au domaine lorsque l'installation est effectuée par un administrateur local.

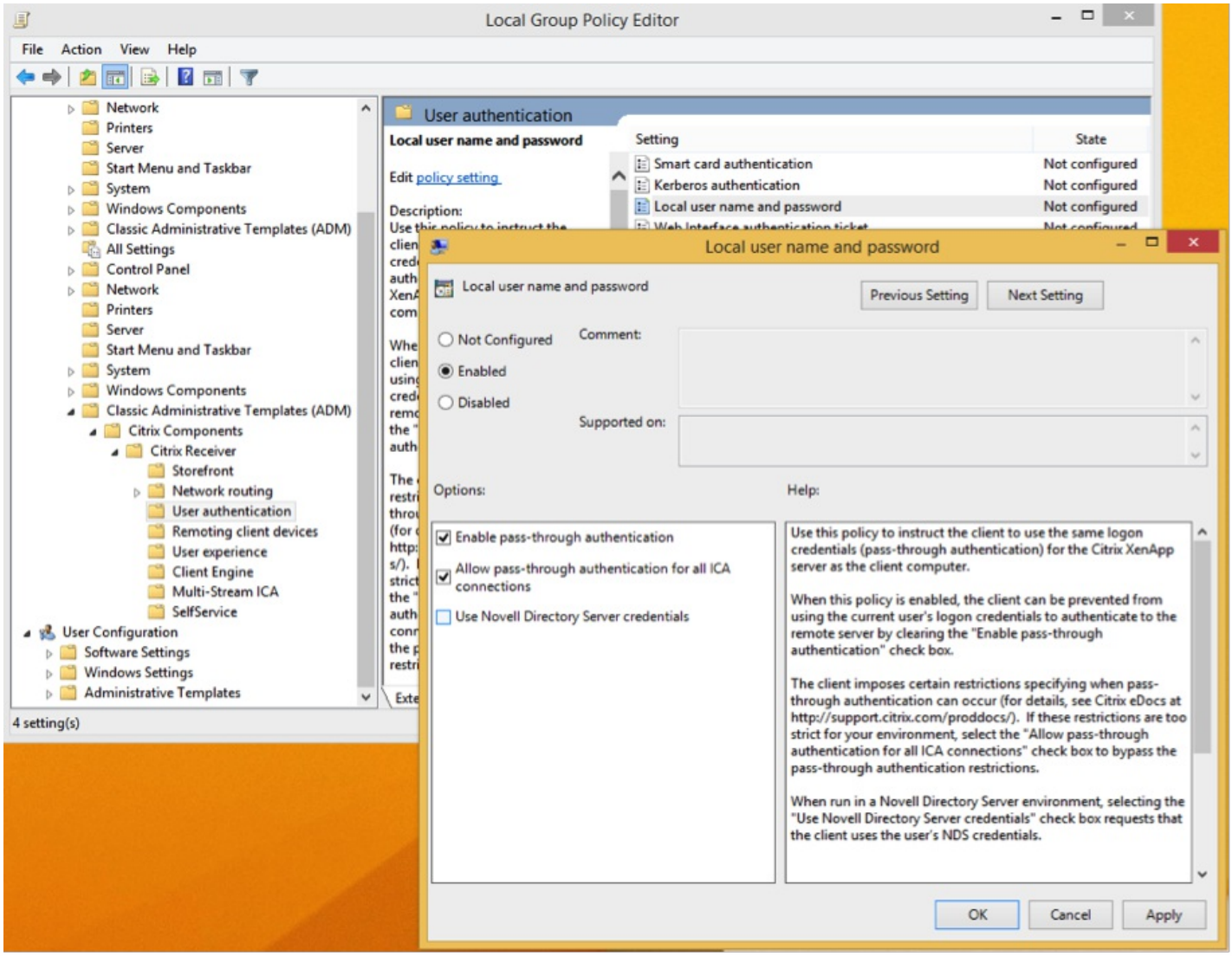
Configuration du SSON via l'éditeur de stratégie de groupe locale (GPO)

Par défaut, la stratégie de groupe du SSON (Single Sign-On) est définie sur **Enable pass-through authentication** ; cela est suffisant pour assurer le fonctionnement du SSON lorsque Desktop Viewer et Receiver pour Web ne sont pas utilisés. Lors de l'utilisation de Desktop Viewer, définissez le GPO sur **Allow pass-through authentication for all ICA connections**.

Pour utiliser le fichier ADM pour configurer l'authentification utilisateur

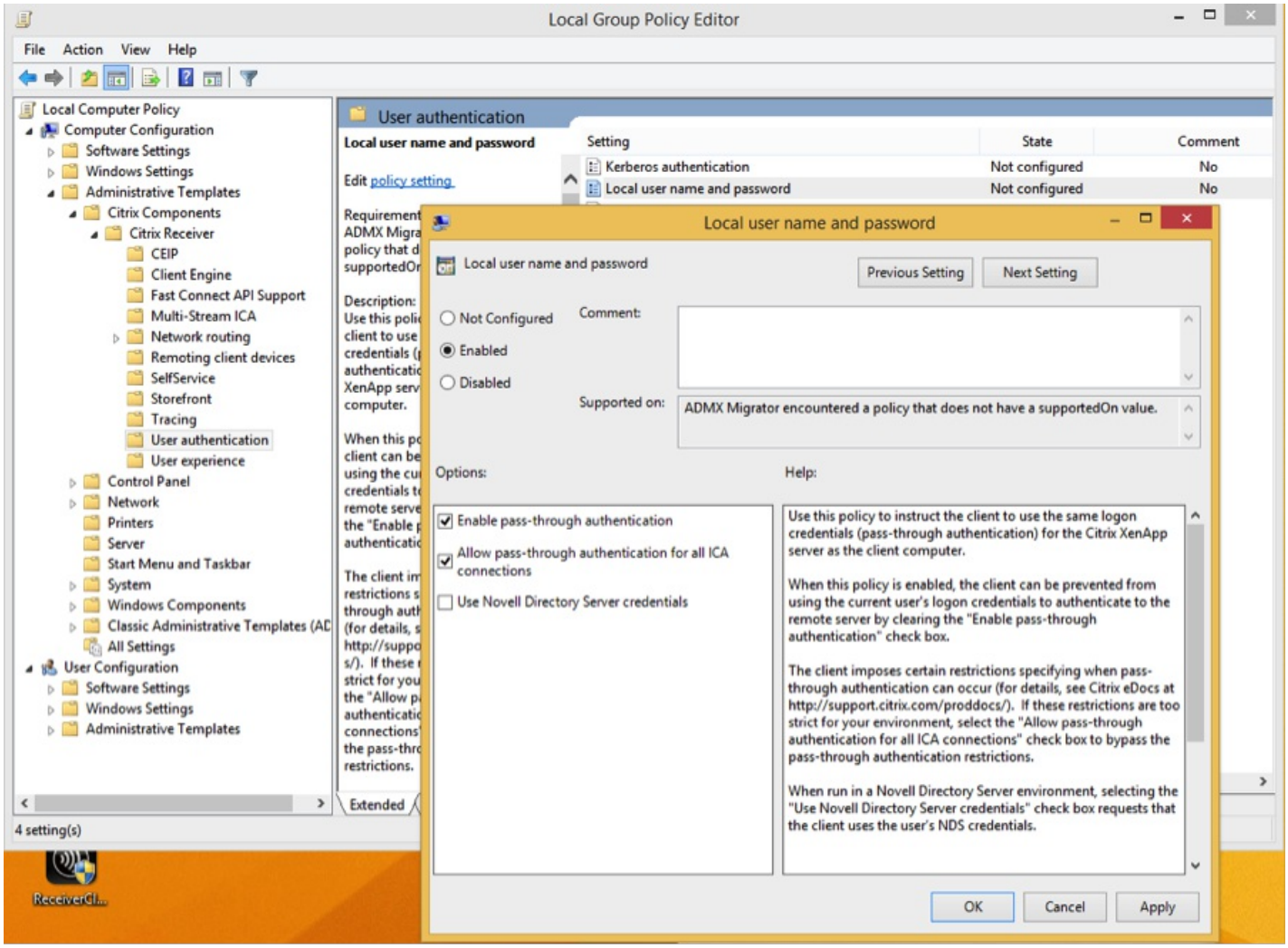
1. Ouvrez l'Éditeur de stratégie de groupe locale en exécutant la commande **gpedit.msc** ou effectuez une recherche sur « Modifier la stratégie de groupe » depuis Démarrer.
2. Ajoutez le modèle receiver.adm de l'Éditeur de stratégie de groupe locale en sélectionnant Configuration ordinateur ; cliquez avec le bouton droit sur Modèles d'administration > Ajout/Suppression de modèles > Cliquez sur **Ajouter**.
3. Une fois le modèle receiver.adm ajouté, développez Configuration ordinateur > Modèles d'administration > Modèles d'administration classiques (ADM) > Citrix Components > Citrix Receiver > User authentication.

Remarque : en fonction de la configuration et des paramètres de sécurité de StoreFront\Receiver pour Web, il peut être nécessaire de sélectionner **Allow pass-through authentication for all ICA connections** pour que l'authentification unique fonctionne.



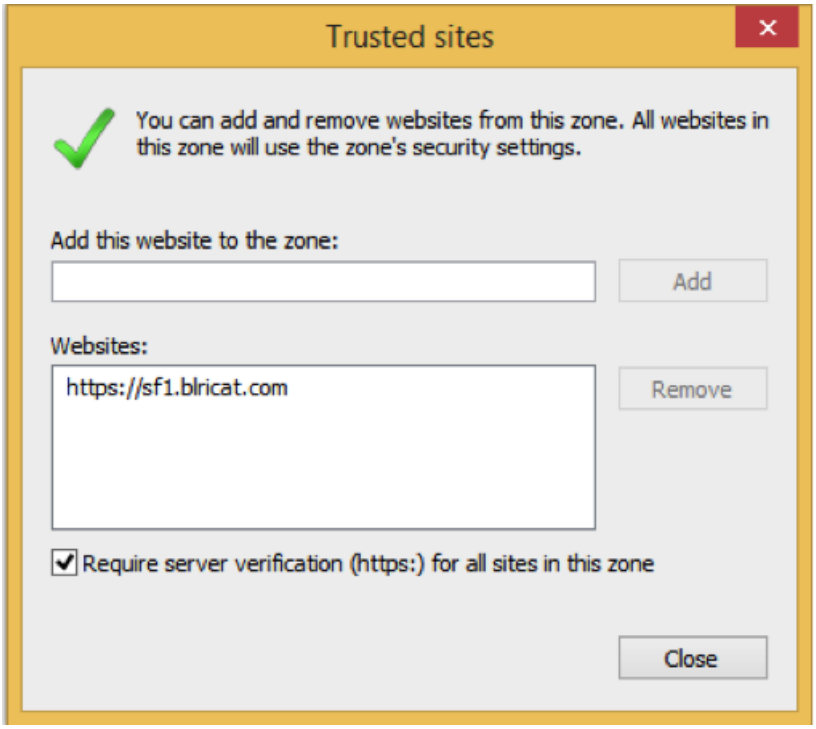
Utilisation d'un fichier ADMX pour l'authentification unique

1. Ajoutez les modèles receiver.admx et receiver.adml à l'éditeur de stratégie de groupe locale. Reportez-vous à la section « À propos de l'utilisation de modèles ADMX » de la rubrique Configuration de Receiver avec le modèle d'objet de stratégie de groupe.
2. Après avoir ajouté les modèles receiver.admx et receiver.adml, développez Configuration ordinateur > Modèles d'administration > Citrix Components > Citrix Receiver > User authentication.
3. Sélectionnez le paramètre **Local user name password**.
4. Sélectionnez les options Enable pass-through authentication et Allow pass-through authentication for all ICA connections lorsque vous activez la stratégie précédente.



Ajouter le nom de domaine complet (FQDN) à la liste des sites de confiance

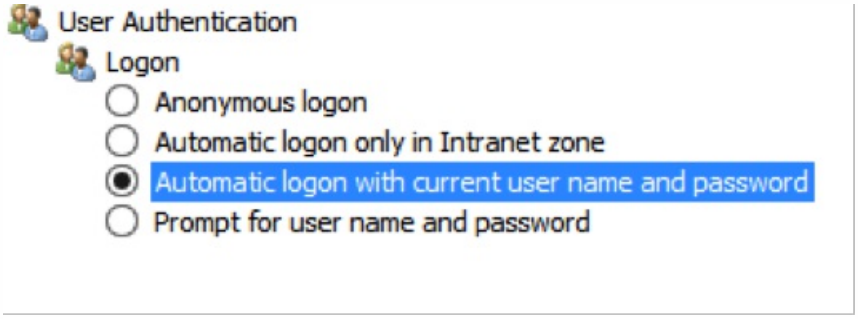
1. Sur la machine cliente, lancez Internet Explorer.
2. Dans Internet Explorer, cliquez sur Outils > Options Internet > Sites de confiance.
3. Cliquez sur **Ajouter** pour ajouter un FQDN à la liste des sites de confiance (par exemple, https://sf1.blricat.com). Une fois ajouté, le site s'affiche dans la liste des sites Web :



Après l'ajout d'un site Web à la liste des sites de confiance, sélectionnez une méthode d'authentification appropriée :

1. Dans Options Internet > onglet Sécurité, sélectionnez Sites de confiance.
2. Choisissez **Personnaliser le niveau, zone de sécurité.**
3. Faites défiler vers le bas de la liste et sélectionnez **Connexion automatique avec le nom d'utilisateur et le mot de passe actuel**.
4. Redémarrez la machine cliente pour appliquer les modifications.

Remarque : le paramètre Connexion automatique avec le nom d'utilisateur et le mot de passe actuel est un paramètre propre à chaque utilisateur ; si ces paramètres ne sont pas configurés par l'administrateur local, chaque utilisateur doit configurer cette option ; pour appliquer ce paramètre globalement, configurez un GPO en ajoutant cette valeur au niveau Personnaliser dans Internet et Sites de confiance.



Considérations de mise à niveau à prendre en compte lors de l'utilisation du Single Sign-On (SSON)

Le tableau ci-dessous contient des informations sur la mise à niveau de Receiver à l'aide de la ligne de commande avec le SSON :

SSON installé avant la mise à	Option SSON durant l'installation	Comportement

niveau	**d'un nouveau Receiver** **(Ligne de commande - /includeSSON ou option de l'interface sélectionnée)**	
Oui	Oui	Composants SSON mis à niveau Clé de registre créée La fonctionnalité SSON fonctionne ; aucune action n'est requise pour l'activer
Oui	Non	Composants SSON mis à niveau Clé de registre créée La fonctionnalité SSON fonctionne ; aucune action n'est requise pour l'activer
Non	Oui	Composants SSON mis à niveau Clé de registre créée La fonctionnalité SSON est désactivée ; l'utilisateur doit désinstaller Receiver et le réinstaller avec le SSON sélectionné via l'option de ligne de commande /includeSSON ou l'option de l'interface
Non	Non	Le composant SSON n'est pas installé

Remarque : l'assistant d'installation Activer le Single Sign-On n'est pas disponible lors de la mise à niveau d'une version existante de Citrix Receiver.

Suppression de Receiver pour Windows

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

Pour supprimer Receiver à l'aide de la ligne de commande

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

CitrixReceiver.exe /uninstall

Après avoir désinstallé Receiver d'une machine utilisateur, les clés de registre personnalisées de Receiver créées par Receiver.adm/Receiver.adml ou Receiver.admx demeurent dans le répertoire Software\Policies\Citrix\ICA Client sous HKEY_LOCAL_MACHINE et HKEY_LOCAL_USER. Si vous réinstallez Receiver, ces stratégies peuvent être appliquées, avec des risques de dysfonctionnement intempestif. Pour supprimer les personnalisations, supprimez-les manuellement.

Avertissement

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.

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

Aug 25, 2016

Personnalisez le programme d'installation de Citrix Receiver en spécifiant des options de ligne de commande. Le programme d'installation s'extrait automatiquement sur le répertoire temporaire de l'utilisateur avant le lancement du programme d'installation et requiert environ 57,8 Mo d'espace disponible dans le répertoire %temp%. Cet espace disponible comprend les fichiers programmes, les données utilisateur et les répertoires temporaires après le lancement de plusieurs applications.

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

CitrixReceiver.exe [Options]

Afficher les informations d'utilisation

Option	/? ou /help
Description	Ce commutateur affiche les informations d'utilisation.
Exemple d'utilisation	CitrixReceiver.exe /? CitrixReceiver.exe /help

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

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

Installation non assistée

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

Activer l'authentification unique (SSO)

Option	/includeSSON
Description	Installe l'authentification Single Sign-On (authentification unique). Cette option est requise pour l'authentification unique par carte à puce. L'option associée, ENABLE_SSON, est activée lorsque /includeSSON est sur la ligne de commande. Si vous utilisez ADDLOCAL= pour spécifier des fonctionnalités et que vous voulez installer l'authentification unique, vous devez également spécifier la valeur ENABLE_SSON. Pour activer l'authentification unique sur une machine utilisateur, vous devez installer Receiver avec des droits d'administrateur à partir d'une ligne de commande qui possède l'option /includeSSON. Sur la machine utilisateur, vous devez également activer ces stratégies dans Modèles d'administration > Modèles d'administration classiques (ADM) > Citrix Components > Citrix Receiver > User authentication : • Local user name and password • Enable pass-through authentication • Allow pass-through authentication for all ICA (peut être nécessaire, en fonction de la configuration et des paramètres de sécurité de l'Interface Web) Une fois les modifications effectuées, redémarrez la machine utilisateur. Pour de plus amples informations, reportez-vous à la section Comment installer et configurer manuellement Citrix Receiver pour l'authentification unique. Remarque : les stratégies Carte à puce, Kerberos et Nom de l'utilisateur et mot de passe locaux sont interdépendantes. L'ordre de configuration est important. Nous vous recommandons de désactiver tout d'abord les stratégies, puis d'activer les stratégies dont vous avez besoin. Validez le résultat attentivement.
Exemple d'utilisation	CitrixReceiver.exe /includeSSON

Activer l'authentification unique lorsque /includeSSON est spécifié

Option	ENABLE_SSON={Yes | No}
	Active l'authentification unique lorsque /includeSSON est spécifié. La valeur par défaut est Yes. Active l'authentification unique lorsque /includeSSON est également spécifié. Cette propriété est requise pour

Description	l'authentification unique par carte à puce. Les utilisateurs doivent fermer leur session et la rouvrir sur leurs machines après une installation avec l'authentification unique activée. Requiert des droits d'administrateur.
Exemple d'utilisation	CitrixReceiver.exe /ENABLE_SSON=Yes

Traçage permanent

Option	/EnableTracing={true | false}
Description	Par défaut, cette fonction est activée. Utilisez cette propriété pour activer ou désactiver explicitement la fonctionnalité de traçage permanent. Le traçage permanent permet de collecter des journaux critiques au moment de la connexion. Ces journaux peuvent aider à la résolution des problèmes de connectivité intermittente. La stratégie de traçage permanent remplace ce paramètre. Par défaut, les fichiers journaux du traçage permanent sont présents dans le répertoire *C:\Users\\AppData\Local\Temp\CTXReceiverLogs\\xxx.etl*.
Exemple d'utilisation	CitrixReceiver.exe /EnableTracing=true

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

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

Spécifier le répertoire d'installation

Option	INSTALLDIR=
Description	Spécifie le chemin d'installation, où Répertoire d'installation correspond à l'emplacement d'installation de la plupart des composants de Receiver. La valeur par défaut est C:\Program Files\Citrix\Receiver. Les composants Receiver suivants sont installés dans C:\Program Files\Citrix : Authentication Citrix Manager, Receiver et Self-Service Plug-in. Si vous utilisez cette option et que vous spécifiez un répertoire d'installation, vous devez installer RIInstaller.msi dans le répertoire d'installation \Receiver et les autres fichiers .msi dans le répertoire d'installation.

Exemple d'utilisation	CitrixReceiver.exe INSTALLDIR=c:\Citrix\Test

Identifier une machine utilisateur sur une batterie de serveurs

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

Nom de client dynamique

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

Installer les composants spécifiés

Option	ADDLOCAL=
	Installe un ou plusieurs des composants spécifiés. Lorsque vous définissez plusieurs paramètres, chaque paramètre doit être séparé par une virgule et ne contenir aucun espace. Les noms sont sensibles à la casse. Si vous ne spécifiez pas ce paramètre, tous les composants sont installés par défaut. Remarque : ReceiverInside et ICA_Client sont requis pour tous les autres composants et doivent être installés. Remarque : lorsque ADDLOCAL n'est pas spécifié, à l'exception de SSON, tous les autres composants par défaut sont installés. Composants inclus : • ReceiverInside : installe l'expérience Citrix Receiver (composant requis pour le fonctionnement de Receiver). • ICA_Client : installe le Citrix Receiver standard (composant requis pour le fonctionnement de Receiver). • WebHelper : installe le composant WebHelper. Ce composant récupère le fichier .ica à partir de StoreFront et le transmet au moteur HDX. Il vérifie également les paramètres d'environnement et les

Description	partage avec StoreFront (similaire à la détection de client ICO). • SSON : installe Single Sign-On. Requiert des droits d'administrateur. • AM : installe Authentication Manager. • SELFSERVICE : installe Self-Service Plug-in. La valeur AM doit être spécifiée sur la ligne de commande et .NET 3.5 Service Pack 1 doit être installé sur la machine de l'utilisateur. Le Self-Service Plug-in n'est pas disponible pour les Windows Thin PC, qui ne prennent pas en charge .NET 3.5. • Pour de plus amples informations sur la création de scripts pour Self-Service Plug-in (SSP), et consulter une liste des paramètres disponibles dans Receiver pour Windows 4.2 et versions ultérieures, reportez-vous à l'article http://support.citrix.com/article/CTX200337. • Le Self-Service Plug-in permet aux utilisateurs d'accéder à des applications et bureaux virtuels à partir de la fenêtre Receiver où d'une ligne de commande, comme décrit plus loin dans cette section dans Pour lancer une application ou un bureau virtuel à partir d'une ligne de commande. • USB : installe la prise en charge USB. Requiert des droits d'administrateur. • DesktopViewer : installe Desktop Viewer. • Flash : installe HDX MediaStream pour Flash. • Vd3d : active l'expérience Windows Aero (pour les systèmes d'exploitation sur lesquels Aero est pris en charge)
Exemple d'utilisation	CitrixReceiver.exe ADDLOCAL=ReceiverInside, ICA_Client, SSON

Configuration de magasins non configurés via les mises à disposition de Merchandising Server

Option	ALLOWADDSTORE={N | S | A}
Description	Spécifie si les utilisateurs peuvent ajouter et supprimer des magasins qui ne sont pas configurés via les mises à disposition de Merchandising Server ; les utilisateurs peuvent activer ou désactiver les magasins configurés via les mises à disposition de Merchandising Server, mais ils ne peuvent pas supprimer ces magasins ni changer les noms ou les adresses URL. Valeur par défaut S. Les options sont les suivantes : • N : ne jamais autoriser les utilisateurs à ajouter ou supprimer leur propre magasin. • S : autoriser les utilisateurs à ajouter ou supprimer uniquement des magasins sécurisés (configurés avec HTTPS). • A : autoriser les utilisateurs à ajouter ou supprimer des magasins sécurisés (HTTPS) et des magasins non sécurisés (HTTP). Ne s'applique pas si Receiver est installé par utilisateur. Vous pouvez également contrôler cette fonctionnalité en mettant à jour la clé de registre HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStore. Remarque : seuls les magasins sécurisés (HTTPS) sont autorisés par défaut et sont recommandés pour les environnements de production. Pour les environnements de test, vous pouvez utiliser des connexions HTTP aux magasins via la configuration suivante : 1. Définissez HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStore sur A pour permettre aux utilisateurs d'ajouter des magasins non sécurisés. 2. Définissez HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowSavePwd sur A pour permettre aux utilisateurs d'enregistrer leurs mots de passe pour des magasins non sécurisés.

	3. Pour autoriser l'ajout d'un magasin configuré dans StoreFront avec HTTP, ajoutez la valeur ConnectionSecurityMode (type REG_SZ) à HKLM\Software\[Wow6432Node\]Citrix\AuthManager et définissez-la sur Any. 4. Fermez et redémarrez Citrix Receiver.
Exemple d'utilisation	CitrixReceiver.exe ALLOWADDSTORE=N

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

Option	ALLOWSAVEPWD={N | S | A}
Description	Spécifie si les utilisateurs peuvent ajouter et supprimer des magasins qui ne sont pas configurés via les mises à disposition de Merchandising Server ; les utilisateurs peuvent activer ou désactiver les magasins configurés via les mises à disposition de Merchandising Server, mais ils ne peuvent pas supprimer ces magasins ni changer les noms ou les adresses URL. Valeur par défaut S. Les options sont les suivantes : • N : ne jamais autoriser les utilisateurs à enregistrer leurs mots de passe. • S : autoriser les utilisateurs à enregistrer des mots de passe uniquement pour les magasins sécurisés (configurés avec HTTPS). • A : autoriser les utilisateurs à enregistrer des mots de passe pour les magasins sécurisés (HTTPS) et les magasins non sécurisés (HTTP). Vous pouvez également contrôler cette fonctionnalité en mettant à jour la clé de registre HKLM\Software\[Wow6432Node]\Citrix\Dazzle\AllowSavePwd. Remarque : les clés de registre suivantes doivent être ajoutées manuellement si AllowSavePwd ne fonctionne pas : • Clé pour client avec OS 32 bits : HKLM\Software\Citrix\AuthManager • Clé pour client avec OS 64 bits : HKLM\Software\wow6432node\Citrix\AuthManager • type : REG_SZ • Valeur : jamais : ne jamais autoriser les utilisateurs à enregistrer leurs mots de passe. secureonly : autoriser les utilisateurs à enregistrer des mots de passe uniquement pour les magasins sécurisés (configurés avec HTTPS). toujours : autoriser les utilisateurs à enregistrer des mots de passe pour les magasins sécurisés (HTTPS) et les magasins non sécurisés (HTTP).
Exemple d'utilisation	CitrixReceiver.exe ALLOWSAVEPWD=N

Sélectionner un certificat

Option	AM_CERTIFICATESELECTIONMODE={Prompt | SmartCardDefault | LatestExpiry}
	Utilisez cette option pour sélectionner un certificat. La valeur par défaut est Prompt, ce qui invite l'utilisateur à choisir un certificat dans une liste. Modifiez cette propriété afin de choisir le certificat par

Description	défaut (celui du fournisseur de carte à puce) ou le certificat doté de la date d'expiration la plus longue. S'il n'existe aucun certificat valide, l'utilisateur en est notifié et il a la possibilité d'utiliser une autre méthode d'ouverture de session, le cas échéant. Vous pouvez également contrôler cette fonctionnalité en mettant à jour la clé de registre de la ruche HKCU ou HKLM\Software\[Wow6432Node\]Citrix\AuthManager : 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.
Exemple d'utilisation	CitrixReceiver.exe AM_CERTIFICATESELECTIONMODE=Prompt

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

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

Utilisation de Kerberos

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

Affichage des icônes FTA d'ancienne génération

Option	LEGACYFTAICONS={False | True}
	Utilisez cette option pour afficher les icônes FTA d'ancienne génération. La valeur par défaut est False. Spécifie si les icônes des applications sont affichées pour les documents qui disposent d'associations de type de fichier avec des applications faisant l'objet d'une souscription. Lorsque l'argument est défini sur

Description	False, Windows génère des icônes pour les documents pour lesquels aucune icône spécifique n'est attribuée. Les icônes générées par Windows se composent d'une icône de document générique sur laquelle est superposée une version plus petite de l'icône d'application. Citrix recommande d'activer cette option si vous prévoyez de mettre des applications Microsoft Office à la disposition des utilisateurs exécutant Windows 7.
Exemple d'utilisation	CitrixReceiver.exe LEGACYFTAICONS=False

Activation du pré-lancement

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

Spécification du répertoire des raccourcis du menu Démarrer

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

	• Si le dossier d'applications du client est \Office, UseCategoryAsStartMenuPath est true, aucun StartMenuDir n'est spécifié et les raccourcis sont placés sous Démarrer > Tous les programmes > Office. • Si le dossier d'applications du client est \Office, UseCategoryAsStartMenuPath est true, StartMenuDir est \Receiver et les raccourcis sont placés sous Démarrer > Tous les programmes > Receiver > Office. Les modifications apportées à ces paramètres n'ont pas d'impact sur les raccourcis déjà créés. Pour déplacer les raccourcis, vous devez désinstaller et réinstaller les applications.
Exemple d'utilisation	CitrixReceiver.exe STARTMENUDIR=\Office

Spécification du nom du magasin

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

Activation de la redirection d'URL sur les machines utilisateur

Option	ALLOW_CLIENTHOSTEDAPPSURL=1
Description	Active la fonctionnalité de redirection des adresses URL sur les machines utilisateur. Requiert des droits d'administrateur. Requiert que Citrix Receiver soit installé pour tous les utilisateurs. Pour de plus amples informations sur la redirection des adresses URL, reportez-vous à Local App Access et à ses sous-

	rubriques dans la documentation XenDesktop 7.
Exemple d'utilisation	CitrixReceiver.exe ALLOW_CLIENTHOSTEDAPPSURL=1

Activation du mode libre-service

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

Spécification du répertoire des raccourcis de bureau

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

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

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

Afficher une boîte de dialogue indiquant que l'installation est terminée durant des installations sans assistance

Lorsque l'installation se termine, une boîte de dialogue indiquant la réussite de l'installation s'affiche, suivi de l'écran **Ajouter**

un compte. Si vous utilisez le logiciel pour la première fois, la boîte de dialogue Ajouter un compte vous invite à entrer une adresse e-mail ou de serveur pour configurer un compte.

> ## Remarque
>
> Si un magasin commun n'a pas été défini par l'argument STOREx ci-dessus, ou par un objet de stratégie de groupe, les utilisateurs qui n'ont pas déjà ouvert une session sur un ordinateur sur lequel Citrix Receiver est installé peuvent apercevoir la boîte de dialogue Ajouter un compte. Pour supprimer cette boîte de dialogue, créez une valeur REG_DWORD EnableX1FTU dans la clé de registre HKLM\Software\Citrix\Receiver et définissez la valeur sur 0.

Résolution des problèmes d'installation

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

CtxInstall-ICAWebWrapper-20141114-134516.log

TrolleyExpress-20090807-123456.log

Exemples d'installation par ligne de commande

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

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"

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

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

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

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

Jan 29, 2016

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

Citrix comprend des exemples de scripts de démarrage par ordinateur destinés à installer et désinstaller CitrixReceiver.exe. Les scripts sont disponibles sur le support XenApp et XenDesktop, dans le dossier Citrix Receiver and Plug-ins\Windows\Receiver\Startup_Logon_Scripts.

- CheckAndDeployReceiverPerMachineStartupScript.bat
- CheckAndRemoveReceiverPerMachineStartupScript.bat

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

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

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

Pour modifier les scripts

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

- **Current Version of package**. Le numéro de version spécifié est validé et s'il n'est pas présent, le déploiement se poursuit. Exemple : set DesiredVersion= 3.3.0.XXXX doit correspondre exactement à la version spécifiée. Si vous spécifiez une version partielle, par exemple 3.3.0, elle correspond à toute version avec ce préfixe (3.3.0.1111, 3.3.0.7777 et ainsi de suite).
- **Package Location/Deployment directory**. Ce paramètre spécifie le partage réseau contenant les packs. Il n'est pas authentifié par le script. Le dossier partagé doit disposer d'autorisations d'accès en lecture pour Tout le monde.
- **Script Logging Directory**. Ce paramètre spécifie le partage réseau sur lequel les journaux d'installation sont copiés. Il n'est pas authentifié par le script. Le dossier partagé doit disposer d'autorisations d'accès en lecture et écriture pour Tout le monde.
- **Package Installer Command Line Options**. Ces options de ligne de commande sont transmises au programme d'installation. Pour connaître la syntaxe de la ligne de commande, consultez la section Configurer et utiliser Receiver pour Windows à l'aide de paramètres de ligne de commande.

Pour ajouter des scripts de démarrage par ordinateur

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

Pour déployer Receiver par ordinateur

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

Pour supprimer Receiver par ordinateur

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

Utilisation des exemples de scripts de démarrage par utilisateur

Citrix recommande d'utiliser des scripts de démarrage par ordinateur. Toutefois, dans les situations dans lesquelles vous avez besoin de déploiements Receiver par utilisateur, deux scripts par utilisateur Receiver sont inclus sur le support XenDesktop et XenApp dans le dossier Citrix Receiver and Plug-ins\Windows\Receiver\Startup_Logon_Scripts.

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

Pour définir des scripts de démarrage par utilisateur

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

Pour déployer Receiver par utilisateur

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

Pour supprimer Receiver par utilisateur

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

Déploiement de Receiver pour Windows à partir de Receiver pour Web

Jan 29, 2016

Vous pouvez déployer Receiver à partir de Receiver pour Web pour vous assurer qu'il est installé avant que les utilisateurs ne se connectent à une application à partir d'un navigateur. Les sites Receiver pour Web permettent aux utilisateurs d'accéder aux magasins StoreFront via une page Web. Si le site Receiver pour Web détecte qu'un utilisateur ne possède pas une version compatible de Receiver, l'utilisateur est invité à télécharger et installer Receiver. Pour de plus amples informations, reportez-vous à la section Sites Receiver pour Web dans la documentation StoreFront.

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

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

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

Jan 29, 2016

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

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

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

Pour de plus amples informations, reportez-vous à la section Configuration du déploiement des clients dans la documentation de l'Interface Web.

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

1. Téléchargez CitrixReceiver.exe sur votre ordinateur local.
2. Renommez CitrixReceiver.exe par CitrixReceiverWeb.exe.
   Important : CitrixReceiverWeb.exe est sensible à la casse.
3. Spécifiez le nouveau nom du fichier dans le paramètre ClientIcaWin32 dans les fichiers de configuration pour vos sites XenApp Web.
   Pour utiliser le processus de détection et de déploiement de client, les fichiers d'installation de Receiver doivent être disponibles sur le serveur Interface Web. Par défaut, l'Interface Web suppose que les noms de fichiers des fichiers d'installation de Receiver sont les mêmes que ceux des fichiers fournis sur le support d'installation de XenApp ou XenDesktop.
4. Vous devrez ajouter à la zone Sites de confiance les sites à partir desquels sera téléchargé le fichier CitrixReceiverWeb.exe.
5. Déployez le fichier exécutable renommé à l'aide de votre méthode de déploiement habituelle.

Configurer Citrix Receiver pour Windows

Aug 25, 2016

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

- Configurez la mise à disposition d'applications et configurez votre environnement XenDesktop. Assurez-vous que votre environnement XenApp est configuré correctement. Comprenez les options qui vous sont offertes et fournissez des descriptions claires des applications.
- Configurez le mode libre-service en ajoutant un compte StoreFront à Receiver. Ce mode permet aux utilisateurs de s'abonner à des applications depuis l'interface utilisateur de Receiver.
- Configurez le mode raccourci d'application uniquement, ce qui comprend :
  - Utilisation d'un fichier de modèle GPO pour personnaliser les raccourcis.
  - Utilisation de clés de registre pour personnaliser les raccourcis.
  - Configuration des raccourcis en fonction des paramètres de compte StoreFront.
- Fournissez des informations de compte aux utilisateurs. Fournissez aux utilisateurs les informations dont ils ont besoin pour configurer l'accès aux comptes hébergeant leurs applications et bureaux virtuels. Dans certains environnements, les utilisateurs doivent manuellement configurer l'accès à ces comptes.

- Si certains de vos utilisateurs se connectent en dehors du réseau interne (par exemple, les utilisateurs qui se connectent via Internet ou à partir d'emplacements distants), configurez l'authentification via NetScaler Gateway. Pour plus d'informations, consultez la section NetScaler Gateway.

Configurer la mise à disposition d'applications

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

Mode d'accès Web

Sans aucune configuration, Citrix Receiver pour Windows fournit un mode d'accès Web : accès aux applications et bureaux par le biais d'un navigateur. Les utilisateurs n'ont qu'à ouvrir un site Receiver pour Web où un site Interface Web dans un navigateur pour sélectionner les applications qu'ils souhaitent utiliser. En mode d'accès Web, aucun raccourci d'application n'est placé dans le dossier Applications sur l'appareil de votre utilisateur.

Mode libre-service

Il vous suffit d'ajouter un compte StoreFront ou un site Interface Web XenApp Services à Receiver pour Windows pour pouvoir configurer le mode libre-service. Ce dernier permet à vos utilisateurs de s'abonner à des applications via Receiver. Cette expérience enrichie est similaire à celle que propose un magasin d'applications mobiles. En mode libre-service, vous pouvez configurer des paramètres de mots-clés pour les applications sélectionnées, auto-provisionnées et obligatoires selon vos besoins. Lorsque l'un de vos utilisateurs sélectionne une application, un raccourci de l'application est placé dans le dossier Applications sur sa machine.

Lors de l'accès à un site StoreFront 3.0, vos utilisateurs bénéficient de l'expérience Receiver. Pour de plus amples informations sur l'expérience utilisateur Receiver, consultez la section Technology Preview de Receiver et StoreFront 3.0.

Lors de la publication d'applications sur vos batteries XenApp, pensez à inclure des descriptions claires des applications publiées afin d'améliorer l'expérience des utilisateurs qui accèdent à ces applications via des magasins StoreFront. Les descriptions sont visibles par vos utilisateurs via Citrix Receiver.

Configurer le mode libre-service

Comme indiqué précédemment, en ajoutant un compte StoreFront à Receiver ou en configurant Receiver de manière à pointer vers un site Interface Web XenApp Services, vous pouvez configurer le mode libre-service. Ce dernier permet aux utilisateurs de s'abonner à des applications à partir de l'interface utilisateur de Receiver. Cette expérience enrichie est similaire à celle que propose un magasin d'applications mobiles.

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

- Pour abonner automatiquement tous les utilisateurs d'un magasin à une application, ajoutez la chaîne KEYWORDS:Auto à la description que vous fournissez lors de la publication de l'application dans XenApp. Lorsque les utilisateurs ouvrent une session dans le magasin, l'application est automatiquement provisionnée sans qu'ils aient à y souscrire manuellement.
- Pour publier des applications auprès des utilisateurs ou pour faciliter la recherche des applications fréquemment utilisées en les répertoriant dans la liste Sélection de Receiver, ajoutez la chaîne KEYWORDS:Featured à la description de l'application.

Pour plus d'informations, veuillez consulter la documentation StoreFront.

Si l'Interface Web de votre déploiement XenApp ne dispose pas d'un site XenApp Services, créez-en un. Le nom du site et sa méthode de création dépendent de la version de l'Interface Web que vous avez installée. Pour plus d'informations, veuillez consulter la documentation relative à l'Interface Web.

> **Remarque**
>
> Lors du lancement d'une session à l'aide du mode libre-service, la connexion automatique est activée par défaut.

Configurer StoreFront.

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

1. Installez et configurez StoreFront. Pour plus d'informations, veuillez consulter la documentation StoreFront.

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

Configuration de la mise à disposition d'applications

Oct 31, 2016

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

- Mode d'accès au Web : sans aucune configuration, Receiver pour Windows 4.4 permet d'accéder, par le biais d'un navigateur, aux applications et aux bureaux. Les utilisateurs n'ont qu'à ouvrir un site Receiver pour Web où un site Interface Web dans un navigateur pour sélectionner les applications qu'ils souhaitent utiliser. Dans ce mode, aucun raccourci n'est placé sur le bureau de l'utilisateur.
- Mode libre-service : il vous suffit d'ajouter un compte StoreFront à Receiver ou de configurer Receiver de manière à pointer vers un site StoreFront pour pouvoir configurer le *mode libre-service*, qui permet aux utilisateurs de s'abonner à des applications à partir de l'interface utilisateur de Receiver. Cette expérience enrichie est similaire à celle que propose un magasin d'applications mobiles. En mode libre-service, vous pouvez configurer des paramètres de mots-clés pour les applications sélectionnées, auto-provisionnées et obligatoires selon vos besoins.

Remarque : par défaut, Receiver pour Windows 4.4 autorise les utilisateurs à sélectionner les applications qu'ils souhaitent afficher sur leur menu Démarrer.

- Mode raccourci d'application uniquement : en tant qu'administrateur Receiver, vous pouvez configurer Receiver pour Windows 4.4 de manière à placer automatiquement des raccourcis d'applications et de bureaux directement dans le menu Démarrer ou sur le bureau, de façon similaire à Receiver pour Windows 3.4 Enterprise. Le nouveau mode *raccourci uniquement* permet aux utilisateurs de localiser toutes leurs applications publiées là où ils s'attendent à les trouver à l'aide du schéma de navigation Windows habituel.

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

Remarque : incluez des descriptions significatives pour les applications dans un groupe de mise à disposition. Les descriptions sont visibles par les utilisateurs de Receiver lors de l'utilisation de l'accès Web ou du mode libre-service.
Pour plus d'informations sur la manière de configurer des raccourcis dans le menu Démarrer ou sur le bureau, consultez la section Configurer le mode raccourci uniquement dans la documentation Produit de Citrix.

Configurer le mode libre-service

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

Remarque : par défaut, Receiver pour Windows 4.4 autorise les utilisateurs à sélectionner les applications qu'ils souhaitent afficher sur leur menu Démarrer.
En mode libre-service, vous pouvez configurer des paramètres de mots-clés pour les applications sélectionnées, auto-provisionnées et obligatoires selon vos besoins.

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

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

sans qu'ils aient à y souscrire manuellement.

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

Personnalisation de l'emplacement des raccourcis d'applications

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

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

Les utilisateurs et les administrateurs peuvent utiliser un certain nombre de paramètres de registre pour personnaliser la manière dont les raccourcis sont définis. Consultez la section Utilisation des clés de registre pour personnaliser l'emplacement des raccourcis d'applications.

Utilisation des raccourcis

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

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

- Vous pouvez ajouter un indicateur [/DESKTOPDIR="Nom_Répertoire"] lors de l'installation pour rassembler tous les raccourcis dans un dossier unique. CategoryPath est pris en charge pour les raccourcis de bureau.
- Auto Re-install Modified Apps est une fonctionnalité qui peut être activée via la clé de Registre AutoReInstallModifiedApps. Lorsque AutoReInstallModifiedApps est activée, toute modification apportée aux attributs des applications et bureaux publiés sur le serveur sont répercutées sur la machine cliente. Lorsque AutoReInstallModifiedApps est désactivée, les attributs d'applications et de bureaux ne sont pas mis à jour et les raccourcis ne sont pas stockés à nouveau lors de l'actualisation s'ils ont été supprimés sur le client. Par défaut, AutoReInstallModifiedApps est activée. Consultez la section Utilisation des clés de registre pour personnaliser l'emplacement des raccourcis d'applications.

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

Remarque : nous vous recommandons d'apporter des modifications à la stratégie de groupe avant de configurer un magasin. Si à tout moment, vous ou un utilisateur souhaitez personnaliser les stratégies de groupe, vous ou l'utilisateur devez réinitialiser Receiver, configurer la stratégie de groupe, puis reconfigurer le magasin.

En tant qu'administrateur, vous pouvez configurer des raccourcis à l'aide de la stratégie de groupe.

1. Ouvrez l'éditeur de stratégie de groupe local en exécutant la commandegpedit.msc localement depuis le menu Démarrer lorsque vous appliquez des stratégies à un seul ordinateur ou en utilisant la Console de gestion des stratégies de groupe pour appliquer des stratégies de domaine.
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. Cliquez sur Ajouter, accédez au dossier de configuration de Receiver et sélectionnez receiver.admx (ou receiver.adml). Pour de plus amples informations sur le modèle ADMX, consultez À propos de l'utilisation de modèles ADMX
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, rendez-vous sur Modèles d'administration > Modèles d'administration classiques (ADM) > Citrix Components > Citrix Receiver > Self Service.
7. Sélectionnez Gérer SelfServiceMode pour activer ou désactiver l'interface utilisateur Receiver en libre-service.
8. Choisissez Gérer les raccourcis d'application pour activer ou désactiver :
   - Les raccourcis sur le bureau
   - Les raccourcis dans le menu Démarrer
   - Le répertoire de bureau
   - Le répertoire du menu Démarrer
   - Le chemin d'accès Catégorie pour les raccourcis
   - La suppression des applications lors de la fermeture de session
   - La suppression des applications lors de l'arrêt
9. Choisissez Autoriser les utilisateurs à ajouter/supprimer un compte pour accorder aux utilisateurs les privilèges permettant d'ajouter ou supprimer plus d'un compte.

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

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

Vous pouvez utiliser des paramètres de clé de registre pour personnaliser les raccourcis. Vous pouvez définir des clés de registre dans les emplacements suivants. Où ils s'appliquent, ils sont traitées dans l'ordre de préférence répertoriés.

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.
Remarque : nous vous recommandons d'apporter des modifications aux clés de registre avant de configurer un magasin. Si à tout moment, vous ou un utilisateur souhaitez personnaliser les clés de Registre, vous ou l'utilisateur devez réinitialiser Receiver, configurer les clés de registre, puis reconfigurer le magasin.
Clés de registre pour machines 32 bits

Nom de Registre	Valeur par défaut	Emplacements par ordre de préférence
RemoveAppsOnLogoff	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
RemoveAppsOnExit	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID+\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
SelfServiceMode	True	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
UseCategoryAsStartMenuPath	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties

Nom de Registre	Valeur par défaut	Emplacements par ordre de préférence
		HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
StartMenuDir	"" (vide)	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
DesktopDir	"" (vide)	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
HideEditStoresDialog	True dans SelfServiceMode, et False dans NonSelfServiceMode	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties

Nom de Registre	Valeur par défaut	Emplacements par ordre de préférence
WSCSupported	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectAll	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectMode	3	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectModeUser	Le Registre n'est pas créé lors de l'installation.	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID+\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE \Citrix\Dazzle

Clés de registre pour machines 64 bits

Nom de Registre	Valeur par défaut	Emplacements par ordre de préférence
RemoveAppsOnLogoff	False	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
RemoveAppsOnExit	False	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle

Nom de Registre	Valeur par défaut	Emplacements par ordre de préférence
		HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID+\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
SelfServiceMode	True	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
UseCategoryAsStartMenuPath	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
StartMenuDir	"" (vide)	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +

Nom de Registre	Valeur par défaut	Emplacements par ordre de préférence
		\Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
DesktopDir	"" (vide)	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
HideEditStoresDialog	True dans SelfServiceMode, et False dans NonSelfServiceMode	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
WSCSupported	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectAll	True	HKCU\Software\Citrix\Dazzle

Nom de Registre	Valeur par défaut	Emplacements par ordre de préférence
		HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectMode	3	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectModeUser	Le Registre n'est pas créé lors de l'installation.	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID+\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle

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

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

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

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

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

défaut).

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

La section se termine avec la balise .
Avant la fin de la section account, dans la première section properties :

Des propriétés peuvent être ajoutées dans cette section après la balise , une par ligne, indiquant le nom et la valeur. Par exemple :

Remarque : les éléments de propriété ajoutés avant la balise peuvent les invalider. La suppression de la balise lors de l'ajout d'un nom de propriété et d'une valeur est facultative.
Voici un exemple étendu de cette section :

Important : dans les déploiements faisant appel à de multiples serveurs, n'utilisez qu'un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n'est exécutée sur aucun des serveurs dans le déploiement. Une fois terminé, propagez les modifications que vous avez apportées à la configuration du groupe de serveurs de façon à mettre à jour les autres serveurs dans le déploiement.

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

Receiver peut être configuré pour placer automatiquement des raccourcis d'applications et de bureaux directement dans le menu Démarrer où sur le bureau. Cette fonctionnalité est semblable à celle des versions antérieures de Receiver, cependant, la version 4.4 permet désormais de choisir où placer les raccourcis d'applications à l'aide des paramètres par application XenApp. Cette fonctionnalité est utile dans les environnements comportant quelques applications qui doivent être affichées dans les mêmes emplacements.

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

Si vous souhaitez que les paramètres par application déterminent où les applications sont placées indépendamment du mode utilisé (libre-service ou mode du menu Démarrer)...	définissez la clé **PutShortcutsInStartMenu=false** sur Receiver et activez les paramètres par application. Remarque : ce paramètre s'applique aux sites Interface Web uniquement.

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

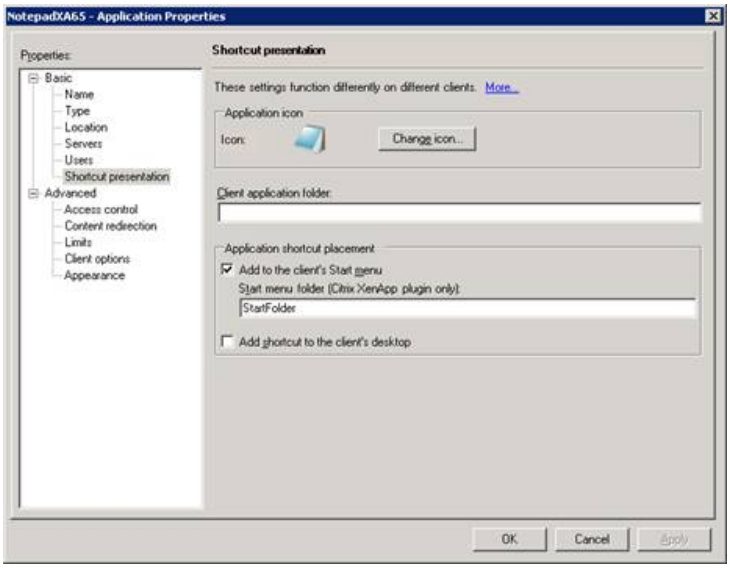
Configurer les paramètres par application dans XenApp 6.5

Pour configurer un raccourci par application publiée dans XenApp 6.5 :

1. Dans l'écran des propriétés d'application XenApp, développez les propriétés de base.
2. Sélectionnez l'option Présentation du raccourci.
3. Dans la section Emplacement(s) du ou des raccourci(s) de l'écran Présentation du raccourci, sélectionnez la case Ajouter un raccourci dans le menu Démarrer du client. Après avoir sélectionné la case à cocher, entrez le nom du dossier dans lequel vous souhaitez placer le raccourci. Si vous ne spécifiez pas de nom de dossier, XenApp place le raccourci dans le menu

Démarrer sans le placer dans un dossier.

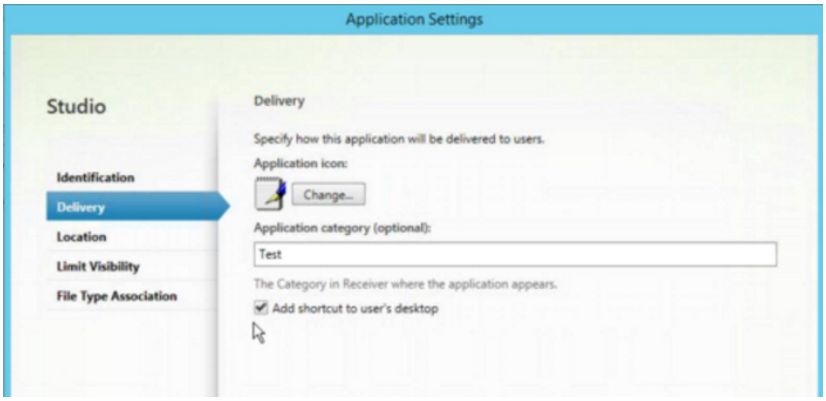
4. Sélectionnez Ajouter un raccourci sur le bureau du client pour inclure le raccourci sur le bureau d'une machine cliente.
5. Cliquez sur Appliquer.
6. Cliquez sur OK.



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

Pour configurer un raccourci par application publiée dans XenApp 7.6 :

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



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

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

Cette fonctionnalité implique un certain nombre d'étapes :

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

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

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

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

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

Exemples de cas d'utilisation

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

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

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

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

Aucun raccourci d'application dans le menu Démarrer

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

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

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

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

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

Paramètres par application dans XenApp 6.5 ou 7.x

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

Si vous souhaitez que les paramètres par application déterminent où les applications sont placées indépendamment du mode utilisé (libre-service ou mode du menu Démarrer)...	définissez la clé **PutShortcutsInStartMenu=false** sur Receiver et activez les paramètres par application. Remarque : ce paramètre s'applique aux sites Interface Web uniquement.

Applications dans des dossiers de catégorie ou dans des dossiers spécifiques

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

Si vous souhaitez que les raccourcis d'applications que Receiver place dans le menu Démarrer s'affichent dans leur catégorie associée (dossier)...	Définissez la clé UseCategoryAsStartMenuPath=True sur Receiver. Remarque : Windows 8/8.1 n'autorise pas la création de dossiers imbriqués dans le menu Démarrer. Les applications seront affichées séparément ou sous le dossier racine mais pas dans les sous-dossiers de catégorie définis avec XenApp.
Si vous souhaitez que les applications que	configurez Receiver avec le StartMenuDir= nom de dossier du menu

Receiver place dans le menu Démarrer s'affichent dans un dossier spécifique...	Démarrer.

Supprimer les applications à la fermeture de session ou en quittant

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

Si vous souhaitez que Receiver supprime toutes les applications à la fermeture de session...	Définissez la clé RemoveAppsOnLogoff=True sur Receiver.
Si vous souhaitez que Receiver supprime toutes les applications en quittant...	Définissez la clé RemoveAppsOnExit=True sur Receiver.

Configuration des applications Local App Access

Lors de la configuration des applications Local App Access :

- Pour spécifier l'utilisation d'une application installée localement plutôt qu'une application disponible dans Receiver, ajoutez la chaîne KEYWORDS:prefer="pattern". Cette fonctionnalité est appelée Local App Access.
  Avant d'installer une application sur l'ordinateur d'un utilisateur, Receiver recherche les modèles spécifiés pour déterminer si l'application est installée localement. Si c'est le cas, Receiver souscrit à l'application et ne crée pas de raccourci. Lorsque l'utilisateur démarre l'application à partir de la fenêtre de Receiver, Receiver démarre l'installation installée localement (préférée).

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

  Remarque : le mot-clé prefer est appliqué lorsque Receiver souscrit à une application. L'ajout du mot-clé après souscription à l'application n'a aucun effet.
  Vous pouvez spécifier le mot-clé prefer plusieurs fois pour une application. Il suffit d'une correspondance pour appliquer le mot-clé à une application. Les modèles suivants peuvent être utilisés dans n'importe quelle combinaison :

  - prefer="Nomapplication"

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

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

- prefer="\\Dossier1\Dossier2\...\Nomapplication"
  Le modèle de chemin d'accès absolu correspond au chemin d'accès du fichier de raccourci plus le nom d'application entier sous le menu Démarrer. Le dossier Programmes est un sous-dossier du répertoire du menu Démarrer, vous devez donc l'inclure au chemin d'accès absolu pour cibler une application dans ce dossier. Des guillemets sont requis si le chemin d'accès contient des espaces. La correspondance est sensible à la casse. Le modèle de correspondance à un chemin d'accès absolu est utile pour les substitutions implémentées via un programme dans XenDesktop.

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

- prefer="\Dossier1\Dossier2\...\Nomapplication"
  Le modèle de chemin d'accès relatif correspond au chemin d'accès du fichier de raccourci relatif sous le menu Démarrer. Le chemin d'accès relatif doit contenir le nom de l'application et peut éventuellement inclure les dossiers dans lesquels le raccourci réside. Une correspondance est établie sur le chemin d'accès au fichier de raccourci se termine pas le chemin d'accès relatif fourni. Des guillemets sont requis si le chemin d'accès contient des espaces. La correspondance est sensible à la casse. Le modèle de correspondance à un chemin d'accès relatif est utile pour les

substitutions implémentées via un programme.

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

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

Configuration de votre environnement XenDesktop

Jun 22, 2016

Les rubriques de cet article décrivent comment configurer la prise en charge USB, empêcher l'assombrissement de la fenêtre Desktop Viewer, et configurer les paramètres pour de multiples utilisateurs et périphériques.

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

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

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

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

- Claviers
- Souris
- Cartes à puce

Remarque : les périphériques USB spécialisés (par exemple, claviers et souris 3D Bloomberg) peuvent être configurés pour utiliser la prise en charge USB. Pour plus d'informations sur la configuration des claviers Bloomberg, consultez la section Configuration des claviers Bloomberg. Pour plus d'informations sur la configuration des règles de stratégie pour d'autres périphériques USB spécialisés, consultez l'article CTX 119722.
Par défaut, certains types de périphériques USB ne sont pas pris en charge pour l'accès distant via XenDesktop et XenApp. Par exemple, une carte d'interface réseau peut être reliée à la carte système par une connexion USB interne. Il n'est pas conseillé de configurer un accès distant pour ce périphérique. Par défaut, les types de périphériques USB suivants ne sont pas pris en charge pour une utilisation dans une session XenDesktop :

- dongles Bluetooth ;
- cartes d'interface réseau intégrées ;
- concentrateurs USB.
- adaptateurs graphiques USB.

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

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

- dongles Bluetooth ;
- cartes d'interface réseau intégrées ;
- concentrateurs USB.
- adaptateurs graphiques USB.
- Périphériques audio
- Périphériques de stockage de masse

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

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

Fonctionnement de la prise en charge USB

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

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

Périphériques de stockage de masse

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

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

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

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

Classes de périphériques USB autorisées par défaut

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

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

- Audio (Classe 01). Comprend des périphériques d'entrée audio (micros), des périphériques de sortie audio et des contrôleurs MIDI. Les périphériques audio modernes utilisent généralement les transferts isochrones, qui sont pris en charge par XenDesktop 4 ou version ultérieure. Audio (Class01) n'est pas applicable pour XenApp car ces périphériques ne sont pas disponibles pour l'accès à distance dans XenApp à l'aide de la prise en charge USB.
  Remarque : certains périphériques spécialisés (par exemple les téléphones VOIP) requièrent une configuration supplémentaire. Pour de plus amples informations, veuillez consulter l'article CTX123015.
- Périphériques d'interface physique (Classe 05). Ces périphériques sont similaires aux périphériques d'interface utilisateur (HID), mais ils fournissent en général des données en temps-réel et comprennent des joysticks de retour de force, des plates-formes mouvantes et des exosquelettes de retour de force.
- Acquisition d'images fixes (Classe 06). Comprend scanners et appareils photo numériques. Les appareils photo numériques prennent généralement en charge la classe d'acquisition d'images fixes qui utilise le protocole PTP (Picture Transfer Protocol) ou MTP (Media Transfer Protocol) pour transférer des images sur un ordinateur ou un autre périphérique. Les appareils photo peuvent également apparaître comme périphériques de stockage de masse et il est possible de configurer un appareil photo pour utiliser les deux classes, par le biais des menus fournis par l'appareil photo.
  Veuillez noter que si un appareil photo apparaît en tant que périphérique de stockage de masse, le mappage des lecteurs clients est utilisé et la prise en charge USB n'est pas requise.

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

  Remarque : cette classe de périphérique (en particulier les imprimantes équipées de fonctions de numérisation) requiert une configuration supplémentaire. Pour de plus amples informations, veuillez consulter l'article CTX123015.
- Stockage de masse (Classe 08). Les périphériques de stockage de masse les plus courants sont les lecteurs flash USB ; les disques dur USB, lecteurs CD/DVD et lecteurs de cartes SD/MMC sont également des périphériques de stockage de masse. Les périphériques avec stockage interne dotés d'une interface de stockage de masse sont également nombreux ; sont compris dans cette catégorie les lecteurs multimédias, les appareils photos numériques et les téléphones portables.
  Le stockage de masse (Classe 08) n'est pas applicable pour XenApp car ces périphériques ne sont pas disponibles pour l'accès à distance dans XenApp à l'aide de la prise en charge USB. Sous-classes connues :
  - 01 Périphériques flash limités
  - 02 Lecteurs de CD/DVD (ATAPI/MMC-2)
  - 03 Lecteurs de bandes (QIC-157)
  - 04 Lecteurs de disquettes (UFI)
  - 05 Lecteurs de disquettes (SFF-8070i)
  - 06 La plupart des périphériques de stockage de masse utilisent cette variante de SCSI.

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

  Important : certains virus sont connus pour se propager activement à l'aide de tous les types de stockage de masse. Posez-vous la question de savoir si les besoins de votre entreprise justifient l'utilisation de périphériques de stockage de masse, soit via le mappage de lecteurs clients, soit via la prise en charge USB.
- Sécurité du contenu (Classe 0d). Les périphériques de sécurité du contenu assurent la protection du contenu, en général pour la gestion des licences ou des droits numériques. Cette classe comprend les dongles.
- Vidéo (Classe 0e). La classe vidéo couvre les périphériques utilisés pour manipuler les vidéos, tels que les webcams, les

caméscopes numériques, les convertisseurs vidéo analogique, certains tuner TV et certains appareils photo numériques qui prennent en charge le streaming vidéo.
Remarque : la plupart des périphériques de streaming vidéo utilisent les transferts isochrones, qui sont pris en charge par XenDesktop 4 ou version ultérieure. Certains périphériques vidéo (par exemple les webcams équipées de fonctions de détection des mouvements) requièrent une configuration supplémentaire. Pour de plus amples informations, veuillez consulter l'article CTX123015.

- Santé personnelle (Classe 0f). Ces appareils comprennent des capteurs de pression artérielle, des moniteurs de pouls, des podomètres, des piluliers et des spiromètres.
- Spécifique au fabricant et à l'application (Classes fe et ff). De nombreux périphériques utilisent des protocoles spécifiques au fabricant ou des protocoles qui n'ont pas été adoptés par le consortium USB, et ces derniers apparaissent en général en tant que spécifique au fabricant (classe ff).

Classes de périphériques USB refusées par défaut

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

- Communications et contrôle CDC (Classes 02 et 0a). La stratégie USB par défaut n'autorise pas ces périphériques, car l'un d'entre eux peut fournir la connexion au bureau virtuel lui-même.
- Périphériques d'interface utilisateur (Classe 03). Comprend un large éventail de périphériques d'entrée et de sortie. Les périphériques d'interface utilisateur (HID) sont composés de claviers, souris, dispositifs de pointage, tablettes graphiques, capteurs, contrôleurs de jeu, boutons et fonctions de contrôle.
  La sous-classe 01 est appelée classe « interface de démarrage » ; elle est utilisée pour les claviers et les souris.

  La stratégie USB par défaut n'autorise ni les claviers USB (classe 03, sous-classe 01, protocole 1), ni les souris USB (classe 03, sous-classe 01, protocole 2). Ceci est dû au fait que la majorité des claviers et souris sont correctement gérés sans prise en charge USB et il est normalement nécessaire d'utiliser ces périphériques localement ainsi qu'à distance lors de la connexion à un bureau virtuel.

- Concentrateurs USB (Classe 09). Les concentrateurs USB permettent de connecter des périphériques supplémentaires à l'ordinateur local. Il n'est pas nécessaire d'accéder à ces périphériques à distance.
- Carte à puce (Classe 0b). Les lecteurs de carte à puce comprennent des lecteurs de carte à puce avec ou sans contact, ainsi que des jetons USB dotés d'une puce équivalente à une carte à puce.
  L'accès distant par carte à puce est utilisé pour accéder aux lecteurs de carte à puce et la prise en charge USB n'est pas nécessaire.

- Contrôleur sans fil (Classe e0). Certains de ces appareils peuvent fournir un accès réseau critique ou connecter des périphériques critiques tels que des claviers ou des souris Bluetooth.
  La stratégie USB par défaut n'autorise pas ces appareils. Toutefois, il peut être utile pour certains appareils de fournir l'accès à l'aide de la prise en charge USB.

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

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

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

:\Program Files\Citrix\ICA Client\Configuration\en

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

HKLM\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Nom="DeviceRules" Valeur=

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.
Les règles par défaut du produit sont stockées dans :

HKLM\SOFTWARE\Citrix\ICA Client\GenericUSB Type=MultiSz Nom="DeviceRules" Valeur=

Ne modifiez pas les règles par défaut du produit.

Pour obtenir des informations sur les règles et leur syntaxe, consultez l'article http://support.citrix.com/article/ctx119722/.

Configuration des claviers Bloomberg

Les claviers Bloomberg sont pris en charge par les sessions XenDesktop et XenApp (mais pas les autres claviers USB). Les composants requis sont installés automatiquement avec le plug-in, mais vous devez activer cette fonctionnalité durant l'installation ou ultérieurement en modifiant une clé de registre.

Il n'est pas conseillé d'héberger plusieurs sessions sur une même machine utilisateur. Le clavier ne fonctionne correctement que dans les environnements n'hébergeant qu'une seule session.

Pour activer ou désactiver la prise en charge du clavier Bloomberg

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.

1. Recherchez la clé suivante dans le registre :
   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

2. Procédez comme suit :
   - Pour activer cette fonctionnalité, pour l'entrée Type DWORD et Nom EnableBloombergHID, définissez Valeur sur 1.
   - Pour désactiver cette fonctionnalité, définissez Valeur sur 0.

Pour empêcher l'assombrissement de la fenêtre Desktop Viewer

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

Avertissement : 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.

1. Sur la machine utilisateur, créez une entrée REG_DWORD appelée DisableDimming dans l'une des clés suivantes, selon que vous souhaitiez empêcher l'assombrissement pour l'utilisateur actuel de la machine ou pour la machine. Une entrée

existe déjà si Desktop Viewer a été utilisé sur la machine :

- HKCU\Software\Citrix\XenDesktop\DesktopViewer
- HKLM\Software\Citrix\XenDesktop\DesktopViewer

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

- HKCU\Software\Policies\Citrix\XenDesktop\DesktopViewer
- HKLM\Software\Policies\Citrix\XenDesktop\DesktopViewer

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

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

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

   1. HKCU\Software\Policies\Citrix\...
   2. HKLM\Software\Policies\Citrix\...
   3. HKCU\Software\Citrix\...
   4. HKLM\Software\Citrix\...

Pour configurer les paramètres de plusieurs utilisateurs et machines

Outre les options de configuration proposées par l'interface utilisateur de Receiver, vous pouvez utiliser l'éditeur de stratégie de groupe et le fichier du modèle icaclient.adm pour configurer ces paramètres. À l'aide de l'éditeur de stratégie de groupe, vous pouvez effectuer les opérations suivantes :

- Étendre le modèle icaclient de manière à ce qu'il couvre tout paramètre de Receiver en modifiant le fichier icaclient.adm. Consultez la documentation Microsoft pour la stratégie de groupe pour obtenir davantage d'informations sur la modification des fichiers .adm et sur l'application de paramètres à un ordinateur donné.
- Effectuer des modifications qui ne s'appliquent qu'à certains utilisateurs ou à tous les utilisateurs d'une machine cliente.
- Configurer les paramètres de plusieurs machines utilisateur

Citrix recommande d'utiliser la stratégie de groupe pour configurer les machines utilisateur à distance, mais vous pouvez utiliser toute méthode, dont l'Éditeur du Registre, permettant de mettre à jour les entrées adéquates du Registre.

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. Sous le nœud Configuration utilisateur ou le nœud Configuration de l'ordinateur, modifiez les paramètres appropriés comme nécessaire.

Configurer StoreFront.

Jul 22, 2016

Citrix StoreFront authentifie les utilisateurs sur XenDesktop, XenApp et VDI-in-a-Box, en énumérant et en regroupant les applications et bureaux disponibles dans des magasins auxquels les utilisateurs accèdent via Receiver.

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

> ## Remarque
>
> Citrix Receiver pour Windows affiche toujours l'ancienne interface utilisateur StoreFront (thème avec bulles vertes) au lieu de l'interface utilisateur StoreFront mise à jour après sélection de l'option d'affichage Tous les comptes.

Pour configurer StoreFront

1. Installez et configurez StoreFront comme décrit dans la documentation StoreFront. Receiver pour Windows requiert une connexion HTTPS. Si le serveur StoreFront est configuré pour HTTP, une clé de registre doit être définie sur la machine utilisateur comme décrit dans la section Configurer et utiliser Receiver pour Windows à l'aide de paramètres de ligne de commande sous la description de la propriété ALLOWADDSTORE.
   Remarque : pour les administrateurs soucieux d'exercer un contrôle plus rigoureux, Citrix fournit un modèle que vous pouvez utiliser pour créer un site de téléchargement pour Receiver.

Gérer la reconnexion au contrôle de l'espace de travail

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

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. Vous utilisez l'Éditeur du Registre à vos propres risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

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

Paramètres de la clé WSCReconnectMode pour Receiver pour Windows :

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

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

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

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

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

Nom : **WSCReconnectModeUser**

type : REG_SZ

Données de valeur : 0

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

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

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle (32 bits)

Nom : **WSCReconnectMode**

type : REG_SZ

Données de valeur : 0

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

Modification du délai de l'indicateur d'état

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

> ## Avertissement
>
> 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.

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

Jan 19, 2017

Ajouter ou spécifier un magasin via un GPO

Citrix recommande d'utiliser l'éditeur d'objet de stratégie de groupe et fournit le fichier de modèle receiver.adm ou receiver.admx\receiver.adml (en fonction du système d'exploitation) pour configurer les paramètres liés à Citrix Receiver pour Windows.

Remarque

receiver.admx/receiver.adml est disponible sur Windows Vista/Windows Server 2008 ou version ultérieure. Les fichiers ADM sont uniquement disponibles sur les plates-formes Windows XP Embedded.

Remarque

Si Citrix Receiver pour Windows est configuré via l'installation de VDA, les fichiers admx/adml se trouvent dans le répertoire d'installation de Citrix Receiver pour Windows. Par exemple : <répertoire d'installation>\online plugin\Configuration.

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

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

Remarque

Citrix vous recommande d'utiliser les fichiers de modèle fournis avec la dernière version de Citrix Receiver pour Windows. Lors de l'importation de la dernière version des fichiers, les paramètres précédents sont conservés.

Pour ajouter des fichiers de modèle adm à l'objet de stratégie de groupe local

Remarque : vous pouvez utiliser des fichiers de modèle adm pour configurer des objets de stratégie de groupe locale et/ou des objets de stratégie de groupe basée sur un domaine.

1. En tant qu'administrateur, ouvrez la fenêtre Éditeur de stratégie de groupe en exécutant la commande gpedit.msc dans le menu Démarrer lorsque vous appliquez des stratégies sur un seul ordinateur ou en utilisant la Console de gestion des stratégies de groupe pour appliquer des stratégies de domaine.
Remarque : si vous avez déjà importé le modèle Citrix Receiver pour Windows dans l'éditeur de stratégies de groupe, vous pouvez ignorer les étapes 2 à 5.
2. Dans le 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. Sélectionnez Ajouter et accédez à l'emplacement du fichier modèle <Répertoire d'installation>\ICA Client\Configuration\receiver.adm
5. Cliquez sur Ouvrir pour ajouter le modèle, puis cliquez sur Fermer pour retourner à l'Éditeur de stratégie de groupe.
Le fichier de modèle de Citrix Receiver pour Windows sera disponible sur l'objet de stratégie de groupe local dans le chemin d'accès Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Receiver.
Une fois que les fichiers de modèle adm ont été ajoutés à l'objet de stratégie de groupe local, le message suivant s'affiche : « L'entrée suivante de la section [strings] est trop longue et a été tronquée : »
Cliquez sur OK pour ignorer le message.

Pour ajouter des fichiers de modèle admx/adml à l'objet de stratégie de groupe local

REMARQUE : vous pouvez utiliser des fichiers de modèle admx/adml pour configurer des objets de stratégie de groupe locale et/ou des objets de stratégie de groupe basée sur un domaine. Consultez l'article Microsoft MSDN sur la gestion des fichiers ADMX ici
1. Après l'installation de Citrix Receiver pour Windows, copiez les fichiers de modèle.

admx :
De : <Répertoire d'installation>\ICA Client\Configuration\receiver.admx
Vers : %systemroot%\policyDefinitions

adml :
De : <Répertoire d'installation>\ICA Client\Configuration\[MUIculture]receiver.adml
Vers : %systemroot%\policyDefinitions\[MUIculture]

Le fichier de modèle de Citrix Receiver pour Windows sera disponible sur l'objet de stratégie de groupe local dans le répertoire Modèles d'administration > Composants Citrix > Citrix Receiver.

Citrix recommande d'utiliser le fichier modèle icaclient.adm de l'Objet de stratégie de groupe pour configurer les règles du routage réseau, les serveurs proxy, la configuration de serveurs de confiance, le routage des utilisateurs, les machines utilisateur distantes et l'expérience de l'utilisateur.

Vous pouvez utiliser le fichier de modèle icaclient.adm avec des stratégies de domaine et des stratégies sur l'ordinateur local. Pour les stratégies de domaine, importez le fichier de modèle à l'aide de la console de gestion des stratégies de groupe. Cela est particulièrement utile pour appliquer les paramètres de Citrix Receiver à un certain nombre de machines utilisateur différentes réparties dans l'entreprise. Pour n'affecter qu'une seule machine utilisateur, importez le fichier de modèle à l'aide

de l'éditeur de stratégie de groupe local sur la machine.

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

> **Remarque**
>
> Citrix vous recommande d'utiliser les fichiers de modèle d'objet de stratégie de groupe fournis avec la dernière version de Citrix Receiver. Lors de l'importation de la dernière version des fichiers, les paramètres précédents sont conservés.

À propos de TLS et des stratégies de groupe

Utilisez cette stratégie pour configurer les options TLS qui permettent à Citrix Receiver d'identifier de manière sécurisée le serveur auquel il se connecte et de crypter toutes les communications avec le serveur. Pour les connexions via des réseaux non approuvés, Citrix recommande d'utiliser TLS. Citrix prend en charge les protocoles TLS 1.0, TLS 1.1 et TLS 1.2 entre Receiver et XenApp ou XenDesktop.

Lorsque cette stratégie est activée, vous pouvez obliger Receiver à utiliser TLS pour toutes les connexions aux applications et bureaux publiés en cochant la case « Require SSL for all connections » (Exiger SSL pour toutes les connexions).

Citrix Receiver identifie le serveur à l'aide du nom figurant sur le certificat de sécurité que le serveur présente. Il s'agit d'un nom DNS (par exemple, www.citrix.com). Vous pouvez restreindre Receiver de manière à ce qu'il puisse uniquement se connecter à des serveurs particuliers, qui sont spécifiés par une liste séparée par des virgules dans le paramètre « Allowed SSL servers » (Serveurs SSL autorisés). Des caractères génériques et des numéros de port peuvent être spécifiés ici ; par exemple, *.citrix.com:4433 autorise les connexions à tout serveur dont le nom commun se termine par .citrix.com sur le port 4433. La précision des informations figurant sur un certificat de sécurité est certifiée par l'émetteur du certificat. Si Receiver ne reconnaît pas et n'approuve pas l'émetteur d'un certificat, la connexion est refusée.

Lors de la connexion à l'aide de TLS, le serveur peut être configuré pour exiger que Receiver fournisse un certificat de sécurité d'identification. Utilisez le paramètre « Client Authentication » (Authentification client) pour configurer si l'identification est fournie automatiquement ou si l'utilisateur est notifié. Les options sont les suivantes :

- never supply identification (Ne jamais fournir d'identification)
- only use the certificate configured here (Utiliser uniquement le certificat configuré ici)
- to always prompt the user to select a certificate (Toujours demander à l'utilisateur de sélectionner un certificat)
- to prompt the user only if there a choice of certificate to supply (Demander à l'utilisateur uniquement lorsque plusieurs certificats sont disponibles)

> **Conseil**
>
> Utilisez le paramètre « Client Certificate » pour spécifier l'empreinte du certificat d'identification afin d'éviter l'affichage d'invites inutiles.

Lors de la vérification du certificat de sécurité du serveur, vous pouvez configurer le plug-in pour qu'il contacte l'émetteur du certificat afin d'obtenir une liste de révocation de certificats (CRL) pour vous assurer que le certificat de serveur n'a pas été révoqué. Cela permet à un certificat d'être invalidé par son émetteur au cas où le système serait compromis. Utilisez le paramètre « CRL verification setting » (Paramètre de vérification CRL) pour configurer le plug-in afin de :

- ne pas vérifier les listes de révocation de certificats
- vérifier uniquement les listes de révocation de certificats obtenues préalablement auprès de l'émetteur
- récupérer activement une liste de révocation de certificats à jour
- refuser la connexion si une liste de révocation de certificats à jour ne peut pas être obtenue

Les organisations qui configurent TLS pour une gamme de produits peuvent choisir d'identifier les serveurs conçus pour les plug-ins Citrix en spécifiant un identificateur d'objet de stratégie de certificat dans le cadre du certificat de sécurité. Si un identificateur d'objet de stratégie est configuré ici, Receiver n'accepte que les certificats qui déclarent une stratégie compatible.

Certaines des stratégies de sécurité ont des exigences liées aux algorithmes de chiffrement utilisés pour une connexion. Vous pouvez configurer le plug-in pour qu'il utilise uniquement TLS 1.0, TLS 1.1 et TLS 1.2 avec le paramètre « TLS version ». De même, vous pouvez configurer le plug-in pour qu'il utilise certains jeux d'algorithmes de chiffrement uniquement. Ces jeux d'algorithmes sont les suivants :

Jeux d'algorithmes gouvernementaux :

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384

Jeux d'algorithmes commerciaux :

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_AES_128_GCM_SHA256

Respect des normes de sécurité FIPS

Citrix Receiver pour Windows 4.4 introduit des options de configuration de TLS et du mode de conformité pour configurer FIPS (Federal Information Processing Standards). Utilisez cette fonctionnalité pour faire en sorte que seule la cryptographie approuvée par FIPS (Publication 140-2) est utilisée pour toutes les connexions ICA.

Un nouveau mode de respect des normes de sécurité assure la prise en charge de NIST SP 800-52. Par défaut, ce mode est désactivé (défini sur AUCUN).

> **Remarque**
>
> Pour de plus amples informations sur la conformité requise pour la norme NIST SP 800-52, consultez la page NIST décrivant les instructions d'implémentation de TLS.

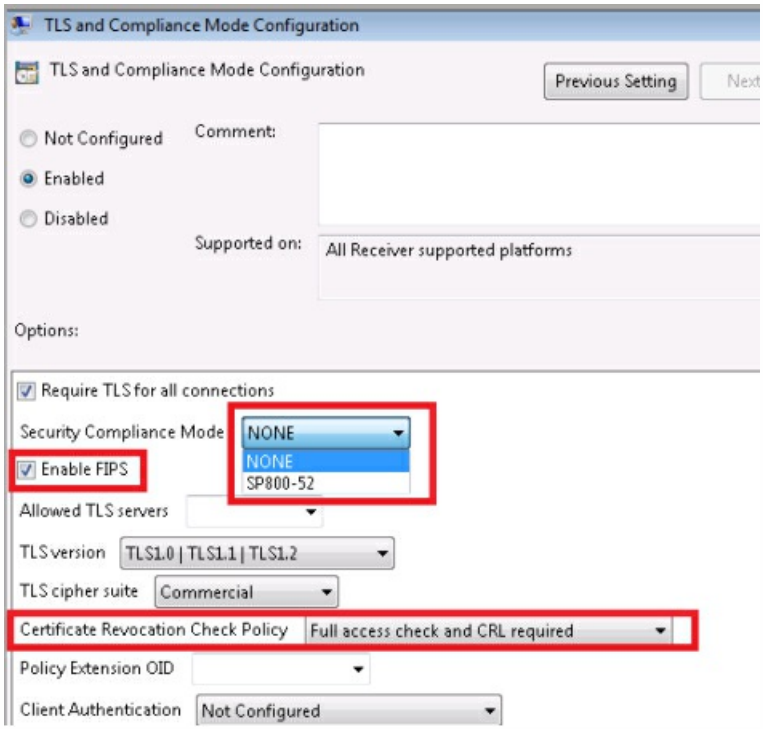
Cette version de Citrix Receiver vous permet également de définir la version TLS, qui détermine le protocole TLS pour les connexions ICA. La version disponible la plus élevée entre le client et le serveur sera sélectionnée.

Lorsque vous utilisez ces fonctionnalités, dans l'écran TLS and Compliance Mode Configuration :

- Sélectionnez la case Enable FIPS pour utiliser la cryptographie approuvée pour toutes les sessions ICA.
- Définissez l'option Security Compliance Mode sur SP 800-52.

- Sélectionnez la version de TLS.

L'image ci-dessous illustre les options FIPS.



> ## Remarque
>
> Par défaut, l'option FIPS est désactivée (non cochée).

Configuration de FIPS

Pour configurer la cryptographie FIPS entre tous les clients ICA :

1. Sélectionnez Configuration ordinateur > Modèles d'administration > Citrix Components > Network Routing > **TLS and Compliance Mode Configuration**.
2. Dans l'écran TLS and Compliance Mode Configuration, sélectionnez **Enable FIPS**.
3. Dans la section Security Compliance Mode, utilisez le menu déroulant pour sélectionner **SP 800-52**. Lors de la configuration de cette option :
   - Le mode de conformité à la norme SP 800-52 requiert le respect de la norme FIPS ; lorsque SP 800-52 est activé, le mode FIPS est également activé quel que soit le paramètre FIPS.
   - L'option Certificate Revocation Check Policy est soit définie sur *Full access check and CRL required* soit sur *Full access check and CRL required all*.
4. Sélectionnez la version appropriée du protocole TLS pour les connexions ICA ; la version disponible la plus élevée entre le client et le serveur sera sélectionnée. Les options disponibles sont les suivantes :
   - TLS 1.0 | TLS 1.1 | TLS 1.2 (option par défaut).
   - TLS 1.1 | TLS 1.2
   - TLS 1.2

À propos de l'utilisation de modèles ADMX

Avec les versions StoreFront 3.0 et Citrix Receiver 4.3, Citrix XenApp et XenDesktop prennent en charge le nouveau format Microsoft permettant d'afficher les paramètres de stratégie basés sur le registre à l'aide d'un format de fichier XML standard, appelé ADMX.

Sur Windows Vista/Windows Server 2008 ou version ultérieure, ces nouveaux fichiers remplacent les fichiers ADM, qui utilisaient leur propre langage de balisage. Les fichiers ADM sont toujours disponibles pour les plates-formes Windows XP Embedded. Les outils d'administration que vous utilisez, Éditeur d'objet de stratégie de groupe et Console de gestion des stratégies de groupe, restent pratiquement inchangés. Dans la plupart des cas, vous ne remarquerez pas la présence des fichiers ADMX lors de vos tâches d'administration de stratégie de groupe quotidiennes.

L'un des avantages principaux des nouveaux fichiers ADMX est le magasin central. Cette option est disponible lorsque vous gérez des objets de stratégie de groupe basés sur un domaine, bien que le magasin central ne soit pas utilisé par défaut. À la différence des fichiers ADM, l'Éditeur d'objets de stratégie de groupe ne copie pas chaque objet de stratégie de groupe modifié, mais offre la possibilité de les lire depuis un seul emplacement de domaine sur le contrôleur de domaine sysvol (non configurable par l'utilisateur) ou à partir du poste de travail de l'administrateur local lorsque le magasin central n'est pas disponible. Vous pouvez partager un fichier ADMX personnalisé en le copiant sur le magasin central, ce qui le met automatiquement à disposition de tous les administrateurs de stratégie de groupe dans un domaine. Cette fonctionnalité simplifie l'administration des stratégies et améliore l'optimisation du stockage pour les fichiers d'objet de stratégie de groupe.

Les fichiers ADMX sont divisés en ressources indépendantes de la langue (ADMX) et spécifiques à une langue (ADML), disponibles pour tous les administrateurs de stratégie de groupe. Ces facteurs permettent aux outils de stratégie de groupe de régler leur interface utilisateur en fonction de la langue configurée par l'administrateur.

> **Remarque**
>
> Vous trouverez des informations supplémentaires dans l'article Microsoft MSDN sur la gestion des fichiers ADMX.

Noms et emplacements des fichiers ADMX et ADML

La convention de noms de fichiers ADM (fournie dans la version précédente de Receiver) a été améliorée. Le tableau ci-dessous présente le mappage des fichiers ADM avec leurs nouveaux noms de fichier ADMX :

Version de Citrix Receiver (antérieure à 4.3)	Version de Citrix Receiver (4.3 et plus récente)
Icaclient.adm	receiver.admx \ receiver.adm
Icaclient_usb.adm	receiver_usb.admx \ receiver_usb.adm
ica-file-signing.adm	ica-file-signing.admx \ ica-file-signing.admx
HdxFlash-Client.adm	HdxFlash-Client.admx \ HdxFlash-Client.admx

Remarque

Utilisez les fichiers .admx sur Windows Vista/Windows Server 2008 et versions ultérieures ; utilisez les fichiers .adm pour les autres plates-formes.

Vous pouvez copier les fichiers ADML et ADMX personnalisés distribués avec le programme d'installation de Citrix Receiver sur le magasin central, ce qui les met automatiquement à disposition de tous les administrateurs de stratégie de groupe dans un domaine. Le tableau ci-dessous indique l'emplacement où copier les fichiers ADMX et ADML :

Type de fichier	Emplacements des fichiers
receiver.admx	\ICA Client\Configuration
ica-file-signing.admx	\ICA Client\Configuration
receiver_usb.admx	\ICA Client\Configuration\fr
HdxFlash-Client.admx	\ICA Client\Configuration
receiver.adml	\ICA Client\Configuration
ica-file-signing.adml	\ICA Client\Configuration
receiver_usb.adml	\ICA Client\Configuration\fr
HdxFlash-Client.adml	\ICA Client\Configuration\[MUIculture]

Remarque

Si Citrix Receiver est configuré via l'installation VDA, les fichiers ADMX/ADML se trouvent dans le répertoire d'installation. Par exemple : \online plugin\Configuration.

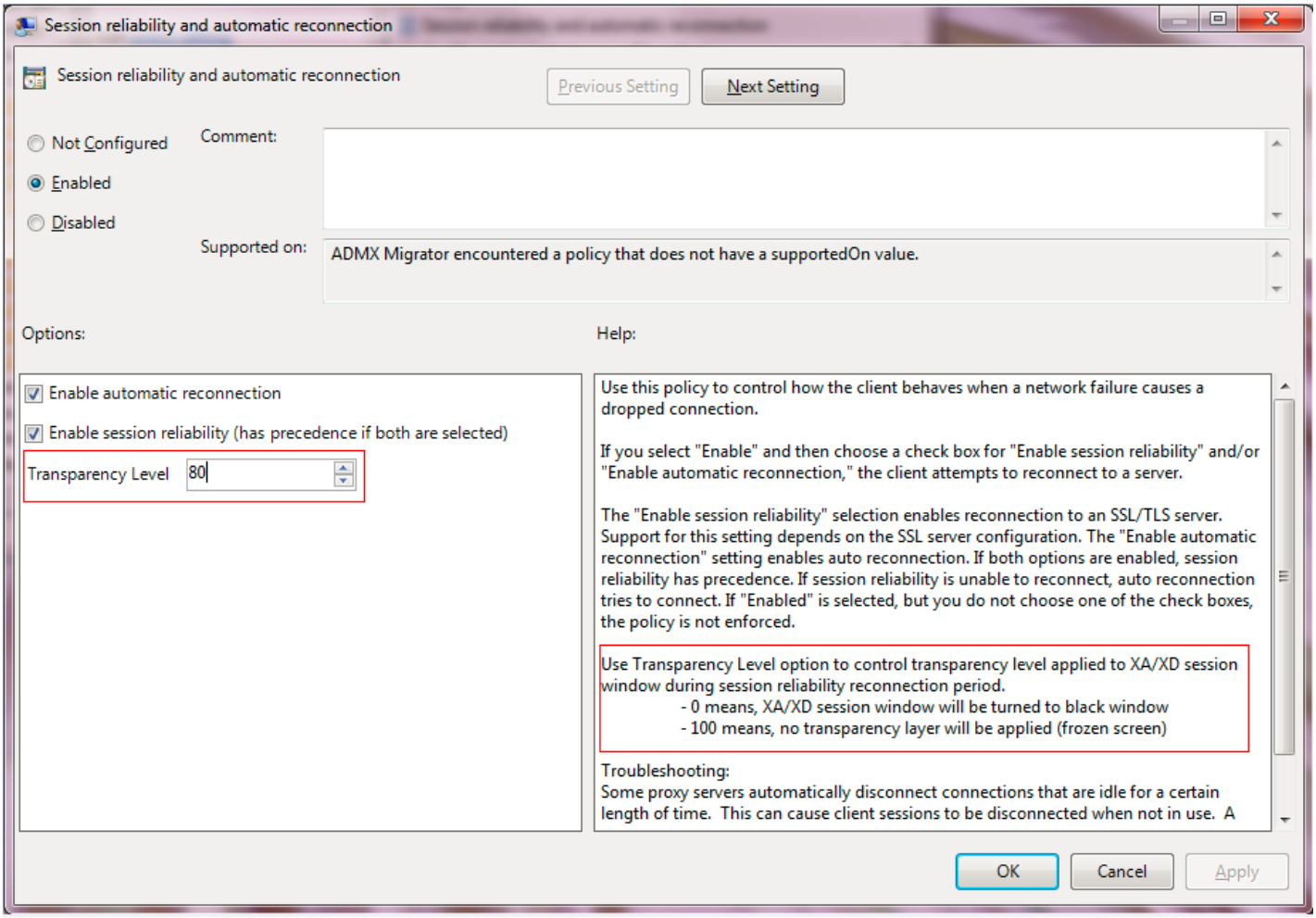
Stratégie de groupe de fiabilité de session

Lors de la configuration de la stratégie de groupe de fiabilité de session, définissez le niveau de transparence. À l'aide de cette option, vous pouvez contrôler le niveau de transparence à appliquer à une application publiée (ou bureau) durant la période de reconnexion de la fiabilité de session.

Pour configurer le niveau de transparence, sélectionnez **Configuration ordinateur - > Modèles d'administration -> Citrix Components - > Network Routing -> Session reliability and automatic reconnection - > Transparency Level**.

Remarque

Par défaut, le niveau de transparence est défini sur 80.



Fournir des informations de compte aux utilisateurs

Jan 29, 2016

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

- 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

> ## Important
>
> Demandez aux utilisateurs qui utilisent Citrix Receiver pour la première fois de redémarrer Receiver après l'avoir installé. Le redémarrage de Receiver garantit que les utilisateurs peuvent ajouter des comptes et que Receiver peut découvrir les périphériques USB qui étaient suspendus lors de l'installation de Receiver.

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

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

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

Pour configurer votre serveur DNS afin de prendre en charge la découverte basée sur l'adresse e-mail, consultez la section Configurer la découverte de compte basée sur une adresse e-mail dans la documentation StoreFront.

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

Fournir un fichier de provisioning aux utilisateurs

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

- Vous pouvez utiliser StoreFront pour créer des fichiers de provisioning contenant les détails des comptes. Mettez ces fichiers à la disposition de vos utilisateurs pour leur permettre de configurer Receiver automatiquement. Après l'installation de Receiver, il leur suffit d'ouvrir le fichier pour configurer Receiver. Si vous configurez des sites Receiver pour Web, les utilisateurs peuvent également obtenir les fichiers de provisioning à partir de ces sites.
  Pour de plus amples informations, reportez-vous à la section Pour exporter les fichiers de provisioning de magasin pour des utilisateurs dans la documentation StoreFront.

Fournir aux utilisateurs des informations de compte à entrer manuellement

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

- Pour les connexions à un magasin StoreFront, indiquez l'adresse URL de ce serveur. Par exemple : https://nomserveur.entreprise.com
  Pour les déploiements Interface Web, fournissez l'adresse URL du site XenApp Services.

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

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

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

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

Partage automatique de comptes de magasins multiples

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

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

Emplacement : HKLM\Software\Citrix\Dazzle

Nom de la clé : CurrentAccount

Valeur : AllAccount

Type : REG_SZ

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

Emplacement : HKLM\Software\Wow6432Node\Citrix\Dazzle

Nom de la clé : CurrentAccount

Valeur : AllAccount

Type : REG_SZ

Avertissement

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.

Optimiser l'environnement de Citrix Receiver

Oct 31, 2016

Vous pouvez optimiser l'environnement dans lequel Receiver fonctionne.

- Réduction du temps de lancement des applications
- Mappage des machines clientes
- Prise en charge de la résolution de nom DNS
- utilisation de serveurs proxy avec les connexions XenDesktop ;
- prise en charge des utilisateurs NDS ;
- utilisation de Receiver avec XenApp pour UNIX.
- Activer l'accès aux applications anonymes

Pour de plus amples informations sur les options d'optimisation, reportez-vous aux rubriques de la documentation XenDesktop traitant de la gestion de l'activité de la session et de l'optimisation de l'expérience HDX.

Réduction du temps de lancement des applications

Jan 29, 2016

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

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

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

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

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

HKLM\Software\[Wow6432Node]\Citrix\Dazzle

HKCU\Software\Citrix\Dazzle

Il existe deux types de pré-lancement :

- **Pré-lancement zéro délai**. Le pré-lancement démarre immédiatement après l'authentification des informations d'identification de l'utilisateur, et ce même en période de trafic intense. Utilisé pour les périodes de trafic normal. Un utilisateur peut déclencher le pré-lancement zéro en redémarrant Receiver.
- **Pré-lancement planifié**. Le pré-lancement démarre à l'heure planifiée. Le pré-lancement planifié ne démarre que lorsque la machine utilisateur est déjà exécutée et authentifiée. Si ces deux conditions ne sont pas remplies à l'heure planifiée, aucune session n'est lancée. Pour répartir la charge réseau et serveur, la session se lance dans un intervalle de temps proche de l'heure planifiée. À titre d'exemple, si le pré-lancement planifié est programmé pour démarrer à 13:45, la session se lance en fait entre 13:15 et 13:45. Utilisé pour les périodes de trafic élevé.

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

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

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

Valeurs de registre HKLM

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

Pour tous les autres systèmes d'exploitation Windows 32 bits pris en charge :HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Prelaunch

Nom : UserOverride

Valeurs :

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

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

Nom : State

Valeurs :

0 - Désactive le pré-lancement.

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

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

Nom : Schedule

Valeur :

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

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

Valeurs de registre HKCU

HKEY_CURRENT_USER\Software\Citrix\ICA Client\Prelaunch

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

mappant les machines clientes ;

Jan 29, 2016

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

- accéder de manière transparente aux lecteurs, aux imprimantes et aux ports COM locaux ;
- couper et coller des données entre la session et le Presse-papiers local de Windows ;
- entendre des données audio (sons système et fichiers .wav) lues dans la session.

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

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

Désactivation du mappage des machines utilisateur

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

Rediriger les dossiers clients

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

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

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

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

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

Le serveur hébergeant les applications et bureaux virtuels peut être configuré au cours de son installation pour mapper

automatiquement les lecteurs du client sur un groupe de lettres de lecteur défini. Par défaut, l'installation mappe les lettres de lecteur affectées aux lecteurs du client en commençant par la lettre V et en remontant l'alphabet, en affectant une lettre de lecteur à chaque lecteur fixe et lecteur de CD-ROM. (Les lecteurs de disquettes sont affectés de leur lettre existante.) Cette méthode fournit les mappages de lecteur suivants dans une session :

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

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

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

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

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

Redirection de périphérique USB Plug and Play HDX

Mis à jour : 27-01-2015

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

Important : si vous interdisez la redirection des périphériques USB Plug and Play dans une stratégie de serveur, l'utilisateur ne peut pas écraser ce paramètre de stratégie.
Un utilisateur peut définir des autorisations dans Receiver pour autoriser ou rejeter systématiquement la redirection de périphérique chaque fois qu'un périphérique est connecté. Ce paramètre affecte uniquement les périphériques connectés après que l'utilisateur ait modifié le paramètre.

Pour mapper des ports COM clients à un port COM serveur

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

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

Important : le mappage des ports COM n'est pas compatible avec l'interface TAPI. Par conséquent, les périphériques TAPI connectés aux ports COM clients ne peuvent pas être mappés.

1. Pour les déploiements XenDesktop 7, activez le paramètre de stratégie Redirection de port COM client.
2. Ouvrez une session sur Receiver.
3. À l'invite de commandes, entrez la commande suivante :

   net use comx: \\client\comz:

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

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

   net use

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

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

Prise en charge de la résolution de nom DNS

Jan 29, 2016

Vous pouvez configurer les logiciels Receiver qui se connectent à la batterie de serveurs en utilisant le Service XML Citrix de sorte qu'ils effectuent des requêtes de nom DNS (Domain Name System) au lieu de requêtes d'adresse IP.
Important : à moins que votre environnement DNS ne soit configuré spécialement pour l'utilisation de cette fonctionnalité, Citrix recommande de ne pas activer la résolution de nom DNS dans la batterie de serveurs.
Les logiciels Receiver qui se connectent aux applications publiées via l'Interface Web utilisent également le Service XML Citrix. Pour ces derniers, le serveur Web résout le nom DNS pour Receiver.

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

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

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

Attention : une 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.

1. Ajoutez une clé de registre de chaîne xmlAddressResolutionType à HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing.
2. Activez la valeur à IPv4-Port.
3. Répétez l'opération pour chaque utilisateur des machines utilisateur.

utilisation de serveurs proxy avec les connexions XenDesktop ;

Jan 29, 2016

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

Jan 29, 2016

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

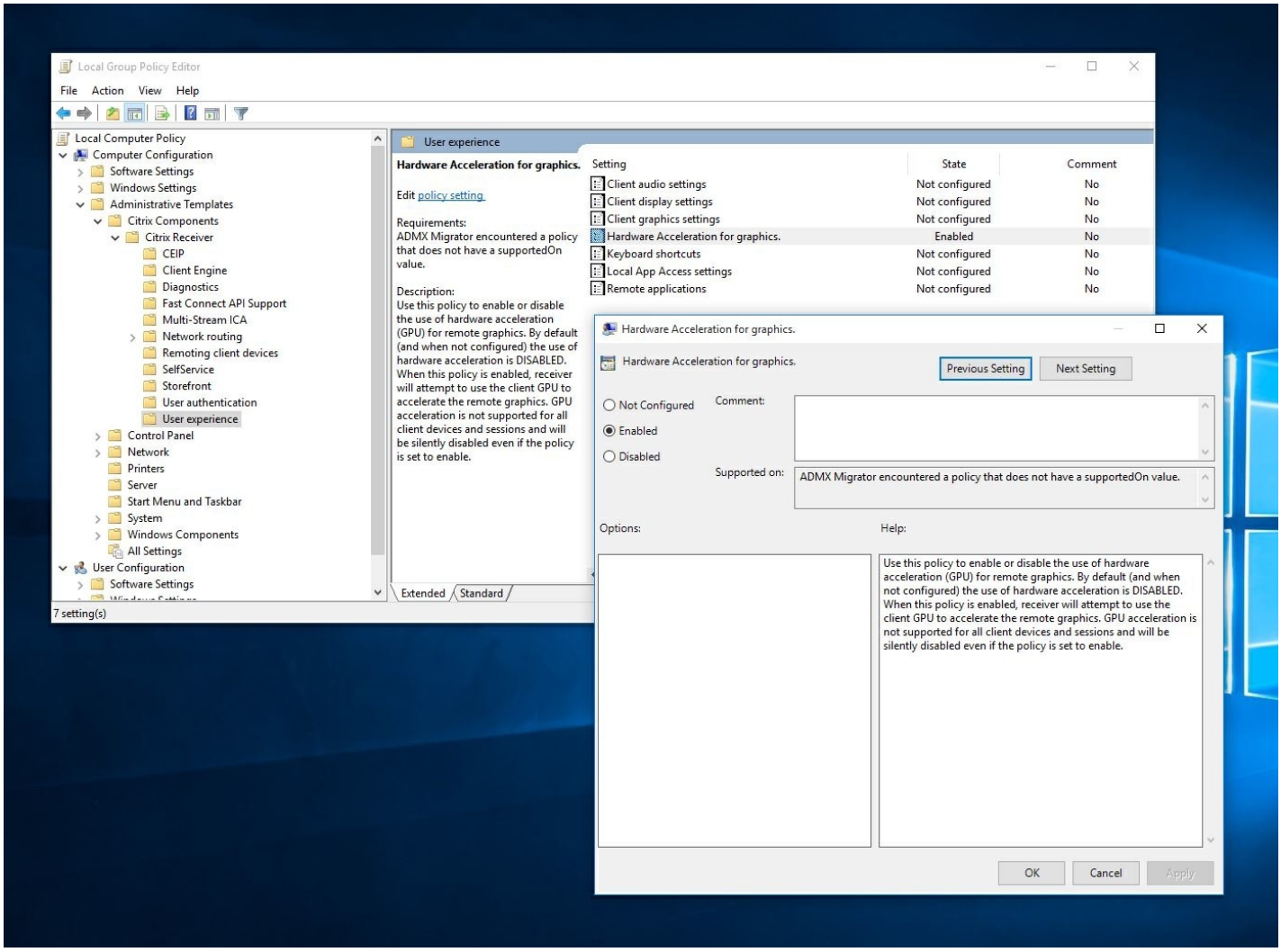
Lors de l'utilisation de la version 4.4 de Citrix Receiver pour Windows (avec moteur HDX 14.4), le GPU peut être utilisé pour le décodage H.264 lorsqu'il est disponible sur le client. La couche API utilisée pour le décodage GPU est DXVA (accélération vidéo DirectX).

Pour de plus amples informations, consultez le blog Improved User Experience: Hardware Decoding for Citrix Windows Receiver.

> ## Remarque
>
> Par défaut, le décodage matériel est désactivé ; il peut être activé dans les stratégies du côté client.

Pour activer le décodage matériel :

1. Copiez « receiver.adml » depuis « root\Citrix\ICA Client\Configuration\en » sur « C:\Windows\PolicyDefinitions\en-US ».
2. Copiez « receiver.admx » depuis « root\Citrix\ICA Client\Configuration » sur « C:\Windows\PolicyDefinitions\ ».
3. Accédez à **l'éditeur de stratégie de groupe locale**.
4. Sous Configuration ordinateur -> Modèles d'administration -> Citrix Receiver -> User Experience, ouvrez **Hardware Acceleration for graphics**.
5. Sélectionnez **Activé** et cliquez sur **OK**.



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

Chemin du registre : HKCU\Software\Citrix\ICA Client\CEIP\Data\GfxRender\

> ## Conseil
>
> La valeur de **Graphics_GfxRender_Decoder** et **Graphics_GfxRender_Renderer** doit être 2. Si la valeur est 1, cela signifie que le décodage basé sur le processeur est utilisé.

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

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

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.

Mis à jour : 28-11-2014

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

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

Les sessions peuvent occuper plusieurs écrans de deux façons :

- Mode plein écran, avec écrans multiples affichés dans la session ; les applications s'alignent sur les écrans comme elles le font localement.
  XenDesktop : pour afficher la fenêtre Desktop Viewer sur n'importe quel sous-ensemble d'écrans, redimensionnez la fenêtre sur ces derniers et 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 vise versa. Vous ne pouvez pas utiliser de séquences de raccourcis avec des bureaux virtuels affiché 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.

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

Avertissement : 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.

Sécurisation de vos connexions

Jan 29, 2016

Pour maximiser la sécurité de votre environnement, les connexions entre Citrix Receiver et les ressources que vous publiez doivent être protégées. Vous pouvez configurer plusieurs types d'authentification pour votre logiciel Citrix 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

Jan 29, 2016

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 Citrix 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 Citrix Receiver a été installé.

Il existe deux façons d'activer l'authentification unique au domaine (SSON) lors de l'installation de Citrix Receiver :

- À l'aide de l'installation par ligne de commande
- À l'aide de l'interface graphique

Activer l'authentification unique au domaine à l'aide de l'interface de ligne de commande

Pour activer l'authentification unique au domaine (SSON) à l'aide de l'interface de ligne de commande :

1. Installez Citrix Receiver 4.x à l'aide du commutateur **/includeSSON**.
   - Installez un ou plusieurs magasins StoreFront (vous pouvez effectuer cette étape plus tard) ; l'installation de magasins StoreFront n'est pas requise pour configurer l'authentification unique au domaine.
   - Vérifiez que l'authentification unique au domaine est activée en démarrant Citrix Receiver, puis confirmez que le processus ssonsvr.exe est exécuté dans le Gestionnaire des tâches après avoir redémarré la machine sur laquelle Citrix Receiver est installé.

> ## Remarque
>
> 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.

Activer l'authentification unique au domaine à l'aide de l'interface utilisateur graphique

Pour activer l'authentification unique au domaine à l'aide de l'interface utilisateur graphique :

1. Accédez au fichier d'installation de Citrix Receiver (CitrixReceiver.exe).
2. Cliquez deux fois sur **CitrixReceiver.exe** pour lancer le programme d'installation.
3. Dans l'assistant d'installation Activer l'authentification unique, sélectionnez la case Activer l'authentification unique pour

installer Citrix Receiver avec la fonctionnalité SSON activée ; cela équivaut à installer Citrix Receiver à l'aide de la ligne de commande avec l'indicateur **/includeSSON**.

L'image ci-dessous illustre comment activer l'authentification unique :

> ## Remarque
>
> L'assistant d'installation Activer l'authentification unique est seulement disponible pour les nouvelles installations sur une machine jointe au domaine.

Vérifiez que l'authentification unique au domaine est activée en démarrant Citrix Receiver, puis confirmez que le processus **ssonsvr.exe** est exécuté dans le Gestionnaire des tâches après avoir redémarré la machine sur laquelle Citrix Receiver est installé.

Utilisez les informations dans cette section pour configurer les paramètres de stratégie de groupe pour l'authentification SSON.

> ## Remarque
>
> La valeur par défaut du paramètre de stratégie GPO lié à SSON est **Enable pass-through authentication**, ce qui est suffisant pour que SSON fonctionne. Utilisez les procédures ci-dessous pour modifier ce paramètre.

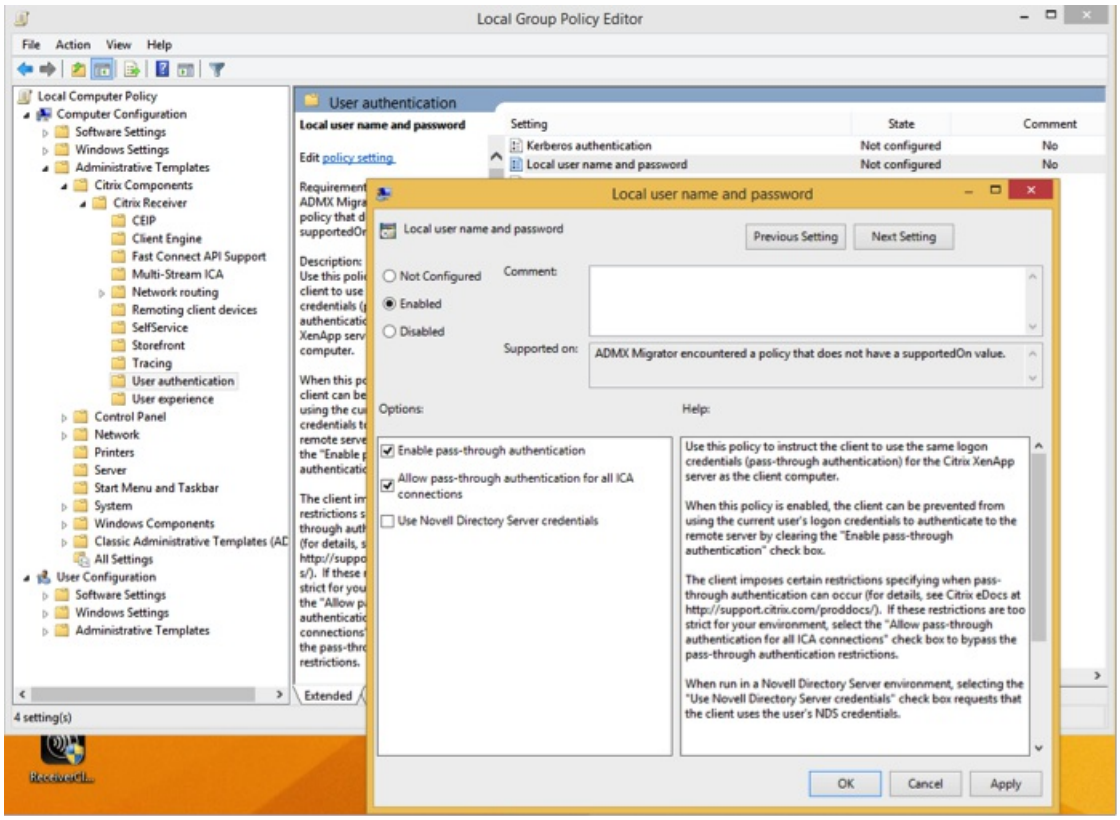
Utilisation d'un fichier ADMX pour la stratégie de groupe SSON

Utilisez la procédure suivante pour configurer des paramètres de stratégie de groupe à l'aide d'un fichier ADMX :

1. Chargez les fichiers de stratégie de groupe. Pour les installations utilisant Citrix Receiver 4.3 et versions ultérieures, utilisez **Receiver.ADMX** ou **Receiver.ADML** dans le dossier %SystemDrive%\Program Files (x86)\Citrix\ICA

Client\Configuration.

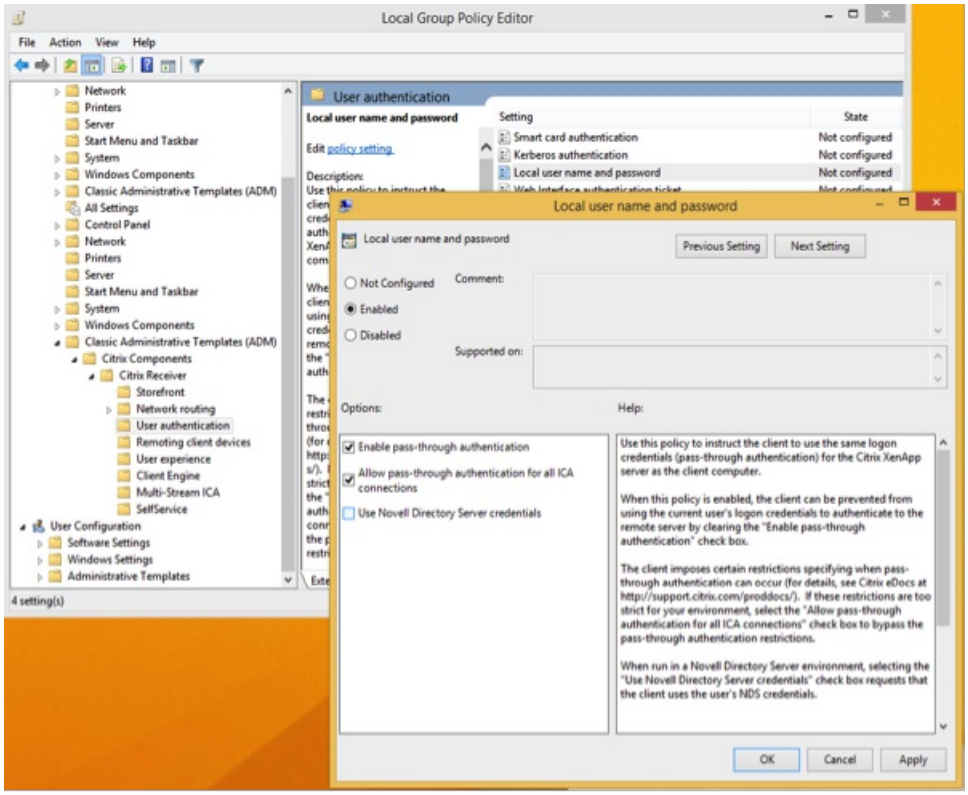
2. Ouvrez **gpedit.msc**, cliquez avec le bouton droit sur **Configuration ordinateur > Modèles d'administration - > Citrix Component-> Citrix Receiver->User Authentication**.
3. Activez les paramètres GPO Ordinateur local (sur la machine locale de l'utilisateur et/ou sur l'image principale du bureau VDA) :
   - Choisissez Local user name and password.
   - Sélectionnez **Activé**.
   - Sélectionnez **Enable pass-through authentication**.
4. Redémarrez la machine (sur laquelle Citrix Receiver est installé) ou l'image principale du bureau VDA.



Utilisation d'un fichier ADM pour la stratégie de groupe SSON

Utilisez la procédure suivante pour configurer des paramètres de stratégie de groupe à l'aide d'un fichier ADM :

1. Ouvrez l'Éditeur de stratégie de groupe locale en sélectionnant **Configuration ordinateur > Clic droit sur Modèles d'administration > Ajout/Suppression de modèles**.
2. Cliquez sur **Ajouter** pour ajouter un modèle ADM.
3. Une fois le modèle **receiver.adm** ajouté, développez **Configuration ordinateur > Modèles d'administration > Modèles d'administration classiques (ADM) > Citrix Components > Citrix Receiver > User authentication**.



4. Ouvrez Internet Explorer sur la machine locale et/où sur l'image principale du bureau VDA.

5. 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** ; vous pouvez trouver cette liste dans **Configuration ordinateur > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Onglet Sécurité**.

6. Fermez la session et rouvrez une session sur la machine Citrix Receiver.

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

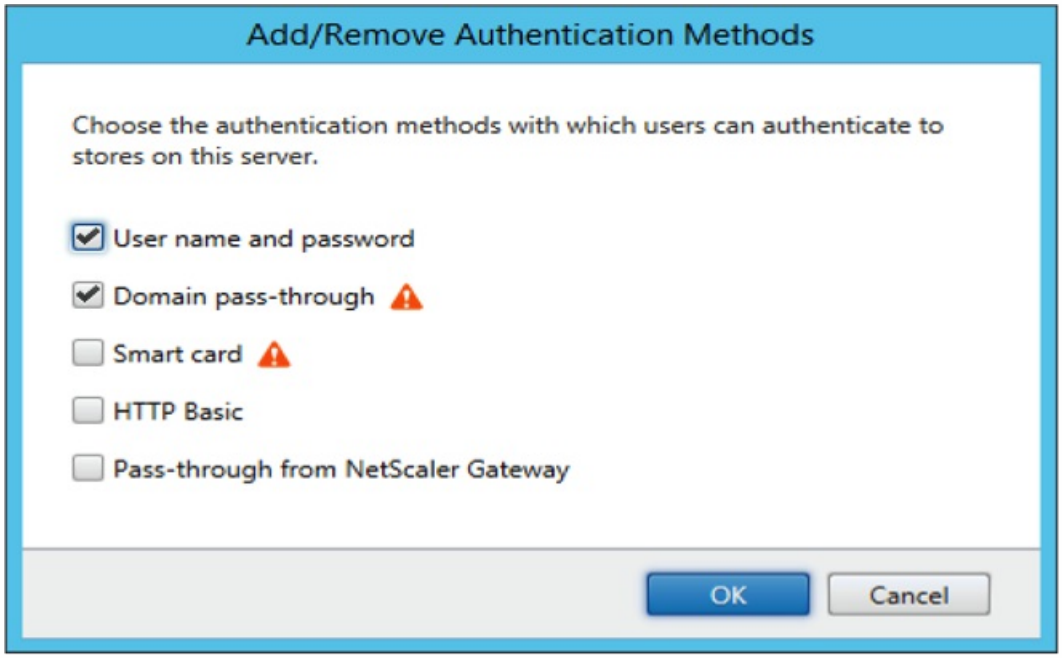
Utilisez la procédure suivante pour configurer le SSON sur StoreFront et l'Interface Web.

1. Ouvrez une session sur le Delivery Controller en tant qu'administrateur.
2. Ouvrez Windows PowerShell (avec des privilèges d'administration). À l'aide de PowerShell, vous allez émettre des commandes visant à permettre à Delivery Controller de faire confiance aux requêtes XML provenant de StoreFront.

3. Si ce n'est pas déjà fait, chargez les applets de commande Citrix en tapant **Add-PSSapin Citrix*** et appuyez sur **Entrée**.
4. Appuyez sur Entrée.
5. Tapez **Add-PSSnapin citrix.broker.admin.v2** et appuyez sur **Entrée**.
6. Tapez **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True** et appuyez sur **Entrée**.
7. Fermez PowerShell.

Configuration du StoreFront

Pour configurer SSON sur StoreFront et l'Interface Web, ouvrez Studio sur le serveur StoreFront et sélectionnez **Authentification -> Ajouter/supprimer des méthodes**. Sélectionnez **Authentification unique au domaine**.



Configuration de l'Interface Web

Pour configurer SSON sur l'Interface Web, sélectionnez **Gestion de l'Interface Web Citrix -> Sites XenApp Services -> Méthodes d'authentification** et activez **Authentification unique**.

L'API FastConnect utilise la méthode d'authentification HTTP basique, qui est souvent confondue avec les méthodes d'authentification associées à l'authentification unique au domaine, l'authentification Kerberos et l'authentification IWA. Citrix recommande de désactiver IWA sur StoreFront et dans la stratégie de groupe ICA.

Configurer l'authentification unique au domaine avec Kerberos

Jan 29, 2016

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

Citrix 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 Citrix 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.

Citrix Receiver gère l'authentification unique avec Kerberos comme suit lorsque Citrix 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 Citrix Receiver capture le code PIN de la carte à puce.
2. Citrix 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 Citrix 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 Citrix 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 de carte à puce à XenDesktop. XenDesktop sélectionne automatiquement un certificat à partir de la carte à puce et obtient le code PIN à partir du moteur HDX.

  Une option connexe, ENABLE_SSON, est activée par défaut et doit rester activée.

  Si une stratégie de sécurité empêche l'activation du SSO sur un appareil, configurez 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 à 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.

L'API FastConnect utilise la méthode d'authentification HTTP basique, qui est souvent confondue avec les méthodes d'authentification associées à l'authentification unique au domaine, l'authentification Kerberos et l'authentification IWA. Citrix recommande de désactiver IWA sur StoreFront et dans la stratégie de groupe ICA.

Configuration de l'authentification par carte à puce

Jan 29, 2016

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 laissé 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 pass-through 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 à 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.

Activation de la vérification des listes de révocation de certificats

Jan 29, 2016

Lorsque la vérification de la liste de révocation de certificats est activée, Receiver vérifie la révocation du certificat du serveur. En obligeant Citrix 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 Citrix Receiver pour qu'il ne vérifie que sa liste de certificats locale ou pour qu'il vérifie les listes de certificats locaux et de réseau. De plus, vous pouvez configurer la vérification des certificats pour permettre aux utilisateurs de n'ouvrir leurs sessions que si toutes les listes de révocation de certificats ont été vérifiées.

Si vous effectuez cette modification sur un ordinateur local, quittez Receiver, s'il est en cours d'exécution. Assurez-vous que tous les composants de Citrix 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

Jan 29, 2016

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

- Citrix NetScaler Gateway (Access Gateway). Pour de plus amples informations, reportez-vous aux rubriques de cette section ainsi qu'à la documentation NetScaler Gateway et StoreFront.
  Remarque : Citrix recommande d'utiliser NetScaler Gateway pour sécuriser les communications entre les serveurs StoreFront et les machines utilisateur.
- Un pare-feu. Les pare-feu de réseau peuvent autoriser ou empêcher le passage des paquets de données en fonction de l'adresse et du port de destination. Si vous utilisez 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.)

Citrix 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 sur plusieurs plates-formes Windows. Référez-vous aux guides de sécurité Windows disponibles à l'adresse http://technet.microsoft.com pour plus d'informations sur les modèles et les réglages associés.

Connexion avec NetScaler Gateway

Jan 29, 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.

> ## Remarque
>
> NetScaler Gateway End Point Analysis Plugin (EPA) ne fournit pas de prise en charge de Receiver pour Windows natif.

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 Citrix eDocs. 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 eDocs.

Connexion avec NetScaler Gateway édition Enterprise

Aug 25, 2016

Pour permettre aux utilisateurs distants de se connecter via NetScaler Gateway, configurez NetScaler 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 NetScaler Gateway Plug-in.

Pour de plus amples informations sur la configuration de ces connexions, reportez-vous à la section Intégration de NetScaler Gateway avec CloudGateway et aux autres rubriques sous ce nœud dans la documentation Produit 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 via 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 Citrix eDocs.

Connexion avec Secure Gateway

Jan 29, 2016

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

Jan 29, 2016

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 ports1494 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

Jan 29, 2016

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 consultez 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

Jan 29, 2016

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

Jan 29, 2016

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)

Oct 31, 2016

Cette section s'applique à XenDesktop 7.6 ou version supérieure ou XenApp 7.5 uniquement.

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.

Cette section s'applique à XenDesktop 7.6 ou version supérieure ou XenApp 7.5 uniquement.

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 décrypte 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.

Configuration requise pour la machine utilisateur

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.

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 le nouveau numéro de port dans la zone Allowed SSL servers au format suivant : serveur:NuméroPortRelaisSSL, où 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 et entrez une liste séparée par des virgules des serveurs approuvés et le nouveau numéro de port dans la zone Allowed SSL servers au format suivant : nomserveur:NuméroPortRelaisSSL, nomserveur:NuméroPortRelaisSSL où 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 :
   csghq.Test.com:443,fred.Test.com:443,csghq.Test.com:444
   ce qui se traduit par exemple de la manière suivante dans un fichier appsrv.ini : [Word]
   SSLProxyHost=csghq.Test.com:443

   [Excel]


```
SSLProxyHost=csghq.Test.com:444

[Bloc-notes]
SSLProxyHost=fred.Test.com:443
```

Configuration et activation de Receiver pour TLS

Oct 31, 2016

Cette section s'applique à XenDesktop 7.6 ou version supérieure ou XenApp 7.5 uniquement.

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 Produit de Citrix.

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

Jan 29, 2016

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

Jan 29, 2016

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

Jan 29, 2016

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 récentes améliorations apportées à Citrix 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.

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.

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

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

Lorsque Citrix Receiver énumère des applications et communique avec StoreFront, la cryptographie de la plate-forme Windows est utilisée.

Pour les connexions TCP entre Citrix Receiver et XenApp/XenDesktop, Citrix Receiver prend en charge TLS 1.0, 1.1 et 1.2 avec les suites de chiffrement suivantes :

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

Pour les connexions UDP, Citrix Receiver prend en charge DTLS 1.0 avec les suites de chiffrement suivantes :

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Activer le mode de conformité avec la norme SP 800-52

[edit this section - use previously created FIPS info and leverage new UI image in DAM]

Une nouvelle case à cocher appelée « Enable FIPS » a été introduite sous Configuration ordinateur - > Modèles d'administration -> Citrix Components - > Network Routing -> TLS and Compliance Mode Configuration. Elle a pour but de

s'assurer que seule la cryptographie approuvée par FIPS est utilisée pour toutes les connexions ICA. Par défaut, cette option est désactivée ou non cochée.

Un nouveau mode de respect des normes de sécurité appelé SP 800-52 a été introduit. Par défaut cette option est définie sur AUCUN et n'est pas activée. Veuillez consulter le lien décrivant la conformité requise pour la norme NIST SP 800-52: - http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295.

Le mode de conformité SP800-52 requiert le respect de la norme FIPS. Lorsque SP800-52 est activé, le mode FIPS est également activé quel que soit le paramètre FIPS. Les valeurs de « Certificate Revocation Check policy » autorisées sont « Full access check and CRL required » ou « Full access check and CRL required All ».

Limitation des versions TLS et des suites de chiffrement

Vous pouvez configurer Citrix Receiver afin de restreindre les versions TLS et les suites de chiffrement. À cet effet, une option vous permet de sélectionner les versions des protocoles TLS autorisés, ce qui détermine le protocole TLS pour les connexions ICA. La version TLS disponible la plus élevée entre le client et le serveur sera sélectionnée. Les options sont les suivantes :

- TLS 1.0 | TLS 1.1 | TLS 1.2 (option par défaut).
- TLS 1.1 | TLS 1.2
- TLS 1.2

Une option est disponible pour la sélection de la suite de chiffrement TLS. Citrix Receiver peut choisir entre :

- Quelconque
- Commercial
- Government

Suites de chiffrement commerciales

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

Suites de chiffrement gouvernementales

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> ### Remarque
>
> Si le paramètre **Require TLS for all connections** est activé, les demandes de connexion à StoreFront doivent également utiliser HTTPS ; l'ajout d'un magasin avec HTTP échoue et les VDA non-SSL (XenDesktop et XenApp) ne peuvent pas être lancés.

Receiver Desktop Lock

Aug 25, 2016

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.

Citrix Receiver Desktop Lock fonctionne sur des machines appartenant à un domaine, sur lesquelles SSON est activé et qui sont configurées pour le magasin ; il peut également être utilisé sur des machines n'appartenant pas à un domaine sur lesquelles le SSON n'est pas activé. Il ne prend pas en charge les sites PNA. Les versions antérieures de Desktop Lock ne sont pas prises en charge lors de la mise à niveau vers Receiver pour Windows 4.2.x.

Vous devez installer Citrix Receiver pour Windows à l'aide de la commande /includeSSON . Vous devez configurer le magasin et le Single Sign-On, au choix avec le fichier adm/admx ou l'option cmdline. Pour de plus amples informations reportez-vous à la section Installer et configurer Citrix Receiver à l'aide de la ligne de commande.

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 7 (y compris Embedded Edition), Windows 7 Thin PC, Windows 8 et Windows 8.1.
- Les machines utilisateur doivent être connectées à un réseau local (LAN) ou un réseau étendu (WAN).

Local App Access

> ## Important
>
> l'activation de Local App Access peut permettre l'accès au bureau local, sauf si un verrouillage a été appliqué avec le modèle d'objet de stratégie de groupe ou une stratégie similaire. 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).
   Par exemple :
   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 Receiver.admx (ou Receiver.adml) et Receiver_usb.admx (.adml) sont chargés dans la stratégie de groupe (où les stratégies apparaissent dans Configuration ordinateur ou Configuration utilisateur > Modèles d'administration > Modèles d'administration classiques (ADM) > Citrix Components). Les fichiers .admx sont situés à l'adresse %Program Files%\Citrix\ICA Client\Configuration\.
- Préférences USB : lorsqu'un utilisateur connecte un périphérique USB, ce périphérique est automatiquement envoyé sur le bureau virtuel ; aucune intervention de l'utilisateur n'est requise. Le bureau virtuel est responsable du contrôle du périphérique USB et de son affichage dans l'interface utilisateur.
  - Activez la règle de stratégie USB.
  - Dans Citrix Receiver > 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 Receiver.admx depuis %Program Files%\Citrix\ICA Client\Configuration\.
    2. Développez Modèles d'administration > Modèles d'administration classiques (ADM) > Citrix Components > Citrix Receiver > User authentication.
    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.

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it