Citrix Receiver pour Mac 12.9.1

May 02, 2018

Citrix Receiver pour Mac permet aux utilisateurs d'accéder en libre-service aux ressources publiées sur des serveurs XenApp ou XenDesktop. Citrix Receiver pour Mac combine facilité de déploiement et d'utilisation, et offre un accès rapide et sécurisé aux applications et bureaux hébergés.

Vous pouvez télécharger la dernière version depuis la page de téléchargement de Citrix Receiver pour Mac.

Pour de plus amples informations sur les versions antérieures de Citrix Receiver pour Mac, consultez les sections suivantes :

Citrix Receiver pour Mac 12.8

Citrix Receiver pour Mac 12.7

Citrix Receiver pour Mac 12.6

Citrix Receiver pour Mac 12.5

Citrix Receiver pour Mac 12.4

Citrix Receiver pour Mac 12.3

Citrix Receiver pour Mac 12.2

Citrix Receiver pour Mac 12

Nouveautés dans la version 12.9

May 02, 2018

Un nouveau certificat de sécurité a été publié récemment afin d'améliorer la sécurité de Citrix Receiver. Toutefois, ce certificat désactive la fonctionnalité de mise à jour automatique de Receiver. Cette version comprend l'outil de mise à jour automatique de Receiver qui permet de restaurer la fonctionnalité de mise à jour automatique de Receiver.

Nouveautés dans la version 12.9

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

> ## Remarque
>
> À compter de Citrix Receiver pour Mac 12. 9, le mode Redirection de composition du Bureau (DCR) pour l'accès distant est obsolète. Thinwire Plus est la méthode préférée pour fournir de meilleures performances pour les postes de travail virtuels.

Problèmes résolus

Mar 19, 2018

Problèmes résolus dans Citrix Receiver pour Mac 12.9

Comparaison avec : Citrix Receiver pour Mac 12.8.1

Citrix Receiver pour Mac 12.9 contient toutes les corrections qui ont été introduites dans les versions 12, 12.1, 12.1.100, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8 et 12.8.1, ainsi que les nouvelles corrections suivantes :

- Lors de la réduction de la fenêtre de certaines applications de fond d'écran tierces, l'image de fond d'écran persiste même après avoir déplacé la fenêtre. [#RFMAC-1300]
- Le raccourci Alt+Tab qui permet de sélectionner des fenêtres peut ne pas fonctionner pour les applications publiées. [#RFMAC-1390]
- Le glisser-déposer peut ne pas fonctionner lors de l'utilisation dans un bureau publié. [#RFMAC-1391]

Problèmes résolus dans Citrix Receiver pour Mac 12.8.1

Comparaison avec : Citrix Receiver pour Mac 12.8

Citrix Receiver pour Mac 12.8.1 contient toutes les corrections qui ont été introduites dans les versions 12, 12.1, 12.1.100, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7 et 12.8, ainsi que les nouvelles corrections suivantes :

- Le curseur de la souris peut disparaître lors du passage d'applications publiées à des applications Mac natives et inversement. [#RFMAC-1178]
- Lors de l'installation de Citrix Receiver pour Mac 12.8, le RealTime Media Engine peut ne pas fonctionner correctement. [#RFMAC-1287]
- Après la mise à niveau vers Citrix Receiver pour Mac 12.8, les caractères accent grave (`) et circonflexe (^) affichent un caractère Unicode étendu au lieu du caractère de base. [#RFMAC-1295]
- Le presse-papiers peut ne pas fonctionner correctement avec certains utilitaires tiers. [#RFMAC-1299]

Problèmes résolus dans Citrix Receiver pour Mac 12.8

Comparaison avec : Citrix Receiver pour Mac 12.7

Citrix Receiver pour Mac 12.7 contient toutes les corrections qui ont été introduites dans les versions 12, 12.1, 12.1.100, 12.2, 12.3, 12.4, 12.5, 12.6 et 12.7, ainsi que les nouvelles corrections suivantes :

- Le curseur de redimensionnement d'une fenêtre dans une session peut ne pas changer, même si l'utilisateur peut modifier la taille de la fenêtre. [#RFMAC-1039]
- Citrix Viewer peut se fermer de manière inattendue lors de l'utilisation de l'éditeur IME coréen local pour envoyer des caractères à une session ICA. [#RFMAC-1079]
- Sur un Mac avec un clavier Français (Canada), le caractère circonflexe (^) n'est pas mappé comme prévu dans les sessions

VDA sur Windows 7. [#RFMAC-1107]

- Copier et coller dans une version publiée de Microsoft Excel entraîne le blocage de la session pendant plus longtemps que d'habitude. [#RFMAC-1149]
- Lorsque le manifeste Citrix Receiver de StoreFront inclut un fichier avec un espace dans le nom, l'interface utilisateur Web ne parvient pas à charger. [#RFMAC-1158]
- Lorsque vous utilisez une station d'accueil, les sessions peuvent devenir inutilisables avec le temps. [#RFMAC-1232]
- Lors de l'utilisation d'un clavier en espagnol, les caractères ajoutant un accent grave à un caractère suppriment le caractère précédent. [#RFMAC-1238]
- Lors de l'ajout d'un dossier dans le Presse-papiers, Citrix Receiver pour Mac peut se fermer de façon inattendue. [#RFMAC-1241]

Problèmes résolus dans Citrix Receiver pour Mac 12.7

Comparaison avec : Citrix Receiver pour Mac 12.6

Citrix Receiver pour Mac 12.7 contient toutes les corrections qui ont été introduites dans les versions 12, 12.1, 12.1.100, 12.2, 12.3, 12.4, 12.5 et 12.6, ainsi que les nouvelles corrections suivantes :

- Le lancement d'un VDA à l'aide d'une carte à puce peut ne pas fonctionner lors de l'utilisation de NetScaler. Citrix Viewer peut cesser de répondre et doit être redémarré. [#RFMAC-445]
- Lors de la connexion à XenApp Essentials et de l'utilisation de l'authentification à deux facteurs, l'invite de saisie du code de sécurité peut ne pas s'afficher. [#RFMAC-976]
- Le fichier de configuration de la redirection USB peut ne pas être enregistré correctement lors de la mise à jour de Citrix Receiver pour Mac. [#RFMAC-981]
- Les applications publiées peuvent ne pas rediriger les adresses URL internes. [#RFMAC-982]
- Citrix Viewer peut cesser de répondre. [#RFMAC-1050]
- L'utilisation de gestes de balayage sur un Mac exécutant High Sierra peut provoquer des problèmes avec les graphiques. [#RFMAC-1073]

Problèmes résolus dans Citrix Receiver pour Mac 12.6

Comparaison avec : Citrix Receiver pour Mac 12.5

Citrix Receiver pour Mac 12.6 contient toutes les corrections qui ont été introduites dans les versions 12, 12.1, 12.1.100, 12.2, 12.3, 12.4 et 12.5, ainsi que les nouvelles corrections suivantes :

- Lors du partage d'écrans à l'aide WebEx, une fenêtre noire peut apparaître sur l'écran partagé. [#RFMAC-689, #LC6462]
- Une fois que le partage d'écran est arrêté lors de l'utilisation de WebEx, l'application peut ne plus s'afficher au premier plan du bureau. [#RFMAC-690, #LC6255]

- Sur macOS Sierra, la combinaison Maj+Inser peut ne pas fonctionner. [#RFMAC-696]
- Après la réduction de WebEx, l'application peut s'afficher incorrectement lorsque vous tentez de l'afficher à nouveau. [#RFMAC-742, #LC6840]
- Lors du lancement d'une application avec Citrix Receiver à l'aide de Google Chrome, la fenêtre « Démarrage de l'application ... » peut ne pas s'afficher. [#RFMAC-744]
- Lors de l'exécution d'une machine virtuelle, les sessions XenDesktop peuvent s'afficher en noir. [#RFMAC-808]
- Une fois qu'une application est lancée, la fenêtre de chargement s'affiche toujours. Lorsque vous cliquez sur Annuler dans la fenêtre, Citrix Receiver se ferme de manière inattendue. [#RFMAC-832, #LC7682]
- Lors de l'utilisation de la redirection des URL du serveur vers client, les adresses URL contenant un « jeton d'accès à usage unique » peuvent démarrer avec le jeton déjà expiré. [#RFMAC-856]
- Il est possible que les applications et bureaux ne se lancent pas lors de l'utilisation de Safari sur des builds macOS Sierra 10.12.6 Public Beta ou macOS High Sierra Developer Preview. [#RFMAC-869]

Problèmes résolus dans Citrix Receiver pour Mac 12.5

Comparaison avec : Citrix Receiver pour Mac 12.4

Citrix Receiver pour Mac 12.5 contient toutes les corrections qui ont été introduites dans les versions 12, 12.1, 12.1.100, 12.2, 12.3 et 12.4, ainsi que les nouvelles corrections suivantes :

- Lors de l'utilisation de cartes à puce pour se connecter à un client Bureau à distance, l'erreur « Aucun certificat n'a été trouvé sur la carte » s'affiche parfois. [#RFMAC-432, #650298]
- La détection de magasins échoue lorsque le serveur répond à l'aide d'une réponse non-UTF-8. [#RFMAC-565]
- Lorsque vous démarrez une application SAML, une erreur de type « demande non valide » peut se produire. [#RFMAC-598, #LC6558]
- ReceiverHelper peut se fermer de manière inattendue. Le problème se produit lorsque CEIPRegistry.json contient un fichier JSON non valide. [#RFMAC-639]
- Le lancement d'une application publiée à partir du Launchpad ou du Finder échoue lorsque vous êtes déconnecté de Citrix Receiver et le message d'erreur suivant s'affiche : « Impossible de se connecter. Impossible de communiquer avec le service Authentication Manager. »[#RFMAC-648]

Problèmes résolus dans Citrix Receiver pour Mac 12.4

Comparaison avec : Citrix Receiver pour Mac 12.3

Citrix Receiver pour Mac 12.4 contient toutes les corrections qui ont été introduites dans les versions 12, 12.1, 12.1.100, 12.2 et 12.3, ainsi que les nouvelles corrections suivantes :

- Citrix Viewer n'envoie pas la disposition de clavier correcte au serveur. [#581829]

- Lors de l'utilisation de Citrix Receiver pour Mac 12.1, le redimensionnement et l'échange de bureaux publiés peuvent ne pas fonctionner lors de l'utilisation de la vue fractionnée. [#604943]
- Lors de l'utilisation de plusieurs affichages dans une configuration dans laquelle l'affichage principal se trouve dans le bas, la fenêtre de l'application publiée Citrix Receiver pour Mac peut scintiller. [#652254]
- Il est possible que les utilisateurs ne puissent pas modifier ou enregistrer un fichier sur un lecteur réseau lors de l'utilisation d'applications publiées. [#660657]
- Lors de l'enregistrement d'un fichier sur un lecteur réseau, la session VDA peut se déconnecter. [#660661]
- Lors de l'utilisation d'un clavier externe dans une session VDA où une application publiée, la touche Inser ne fonctionne pas. [#660669]
- Les imprimantes dont l'affichage dans une session a été désactivé sont toujours présentes et disponibles. [#667462]

Problèmes résolus dans Citrix Receiver pour Mac 12.3

Comparaison avec : Citrix Receiver pour Mac 12.2

Citrix Receiver pour Mac 12.3 contient toutes les corrections qui ont été introduites dans les versions 12, 12.1, 12.1.100, et 12.2, ainsi que les nouvelles corrections suivantes :

- Si Citrix Receiver pour Mac est configuré pour utiliser un serveur proxy, les connexions SSL peuvent échouer. [#640652]

Problèmes résolus dans Citrix Receiver pour Mac 12.2

Comparaison avec : Citrix Receiver pour Mac 12.1.100

Citrix Receiver pour Mac 12.2 contient toutes les corrections qui ont été introduites dans les versions 12, 12.1 et 12.1.100, ainsi que les nouvelles corrections suivantes :

- Résolution d'un problème sur les claviers allemand/autrichien dans lequel la touche ALT n'était pas libérée après la saisie de Alt-l. [#LC3796]
- Résolution d'un problème dans lequel la redirection de contenu du serveur vers le client échouait si l'URL redirigée contenait des caractères non ASCII. [#LC4470]
- Cette version résout un problème dans lequel une fenêtre d'application HDX pouvait afficher des artefacts de dessin après la réduction et l'agrandissement. [#LC4668]
- Résolution d'un problème dans lequel l'authentification pass-through par carte à puce pouvait échouer. [#LC4907]
- Résolution d'un problème dans lequel l'audio diffusé à distance sur le serveur à partir d'un micro pouvait être saccadé. [#LC5157]
- Résolution d'un problème dans lequel la combinaison Ctrl-Tab n'était pas transmise aux sessions de bureau actives. [#LC5367]

- Résolution d'un problème dans lequel le mappage du clavier de la session pouvait ne pas être correct lors de la reconnexion à une session existante. [#LC5395]
- Résolution d'un problème dans lequel les cartes à puce n'étaient pas accessibles à un client Bureau à distance Microsoft exécuté au sein d'une session HDX. [#LC5454]
- Cette version résout un problème dans lequel les sessions ne se connectaient pas si l'authentification par certificat utilisateur était configurée sur NetScaler Gateway. [#LC5455]
- Résolution d'un problème dans lequel Receiver pour Mac lançait une session en mode plein écran si le paramètre ScreenPercent était spécifié dans le fichier ICA. [#605353]
- Résolution d'un problème qui entraînait le blocage de Receiver pour Mac si une session était déconnectée alors qu'une webcam était diffusée à distance sur une session active. [#612051]
- Cette version résout un problème dans lequel Receiver pour Mac n'utilisait pas la configuration du proxy système lors du téléchargement des listes de révocation de certificats. [#638176]

Problèmes résolus dans Citrix Receiver pour Mac 12.1.100

Comparaison avec : Citrix Receiver pour Mac 12.1

Citrix Receiver pour Mac 12.1.100 contient toutes les corrections qui ont été introduites dans les versions 12 et 12.1, ainsi que les nouvelles corrections suivantes :

- Résolution d'un problème dans lequel une session Receiver pour Mac échouait lors de la connexion via un VPN SSL Cisco ASA 9.32. [#LC3887]
- Résolution d'un problème dans lequel une session se bloquait lors du lancement d'une application ou d'un bureau dont le nom commençait par un caractère « @ ». [#LC4296]
- Résolution d'un problème dans lequel les sessions se déconnectaient, ce qui entraînait un message d'erreur indiquant « L'homologue SSL distant a envoyé une alerte MAC incorrecte. »[#LC4367]
- Résolution d'un problème dans lequel les connexions IPV6 à NetScaler Gateway échouaient. [#LC4512]
- Résolution d'un problème dans lequel la tentative de saisie d'un seul caractère en japonais ou chinois simplifié n'entraînait l'affichage d'aucun caractère dans la session de bureau.[#603635]

Problèmes résolus dans Citrix Receiver pour Mac 12.1

Comparaison avec : Citrix Receiver pour Mac 12

Citrix Receiver pour Mac 12.1 contient toutes les corrections qui ont été introduites dans la version 12, ainsi que les nouvelles corrections suivantes :

- Résolution d'un problème dans lequel si vous utilisiez le VPN intégré à OS X, Citrix Receiver ne parvenait pas parfois à se connecter à un compte configuré alors que le VPN était actif.

- Résolution d'un problème dans OS X El Capitan dans lequel les sessions s'affichaient de façon anormale en vue fractionnée. [#582397]
- Résolution d'un problème dans lequel la détection des balises échouait lorsque vous tentiez de vous connecter en externe via un proxy F5. [#582885]
- Résolution d'un problème dans lequel les raccourcis clavier configurés dans les préférences système n'étaient pas appliqués dans la session. [#583033]
- Résolution d'un problème dans Citrix Receiver pour Mac 11.9.15 et 12 avec l'entrée clavier '+' qui entraînait le blocage du visualisateur. [#586179, #577922]
- Résolution d'un problème dans lequel après le lancement d'une application, Citrix Receiver demandait l'authentification d'une autre application. [#592460]
- Résolution d'un problème sur les sessions de bureau dans lequel la combinaison Ctrl-Q n'était pas transmise correctement. [#600601]

Problèmes résolus dans Citrix Receiver pour Mac 12

Cette version résout un certain nombre de problèmes liés à l'intégration de cartes à puce. Certains problèmes demeurent et continuent de faire l'objet de recherches.

Autres problèmes résolus dans cette version :

- Un message incorrect était affiché dans la fenêtre de saisie des informations d'identification dans les environnements japonais (« デモアカウント にログオンしてください », ce qui signifie « Veuillez vous connecter au compte de démo »). Ce message aurait dû lire « Veuillez vous connecter à Mon bureau virtuel. » [#LC2682]
- Le montage de multiples images de disques Receiver simultanément peut entraîner le lancement du mauvais programme d'installation. [#551605]
- Les entrées de contournement proxy OS X dans la notation CIDR étaient ignorées. [#564250]
- Seuls les 256 premiers caractères de la liste de contournement OS X sont utilisés. [#567089]
- La vérification de faux positifs pour une balise interne pouvait échouer pour certains fournisseurs d'accès à Internet qui avaient installé le logiciel de redirection d'erreur DNS de Barefruit. [#572456]

Problèmes connus

Mar 19, 2018

Problèmes connus avec Citrix Receiver pour Mac 12.9

Les problèmes connus suivants ont été observés dans cette version :

- Lorsque deux applications transparentes sont en cours d'exécution, l'actualisation de l'application après le déplacement de la fenêtre peut ne pas fonctionner. [#RFMAC-1308]

Problèmes connus avec Citrix Receiver pour Mac 12.7

Les problèmes connus suivants ont été observés dans cette version :

- Lorsque la stratégie « Activer la Redirection Desktop Composition » est activée dans une session plein écran, Citrix Viewer peut rencontrer des problèmes avec les graphiques. [#RFMAC-1078]
- Citrix Viewer peut se fermer de manière inattendue lors de l'utilisation de l'éditeur IME coréen local pour envoyer des caractères à une session ICA. [#RFMAC-1079]
- Sur un Mac avec un clavier Français (Canada), le caractère circonflexe (^) n'est pas mappé comme prévu lorsque vous vous connectez à un VDA Windows 7. [#RFMAC-1107]
- Les éléments d'interface dans d'autres langues peuvent être tronqués sur le panneau de préférences Périphériques. [#RFMAC-1113]

Problèmes connus avec Citrix Receiver pour Mac 12.5

Les problèmes connus suivants ont été observés dans cette version :

- Lors de l'utilisation d'une connexion proxy, la communication via le protocole EDT échoue. [#RFMAC-1113]
- Citrix Viewer peut se fermer de manière inattendue sur macOS 10.12 lors de la déconnexion d'un bureau à partir de la barre de menus. Le problème se produit également si le mode « Utiliser tous les affichages en plein écran » est sélectionné alors que la session de bureau est fermée.[#RFMAC-618]

Problèmes connus avec Citrix Receiver pour Mac 12.4

Les problèmes connus suivants ont été observés dans cette version :

- Lors de l'utilisation d'une connexion proxy, la communication via le protocole Enlightened Data Transport (EDT) échoue. [#664725]
- Lors de l'utilisation de NetScaler Gateway configuré pour EDT avec un VDA version 7.11 ou antérieure, la connexion à TCP échoue car le mécanisme de secours vers TCP ne fonctionne pas. [#665617]

Problèmes connus avec Citrix Receiver pour Mac 12.3

Les problèmes connus suivants ont été observés dans cette version :

- Lorsqu'un serveur proxy est configuré sur une machine utilisateur, la reconnexion automatique des clients peut échouer

avec un VDA pour OS de bureau. [#659683]

- Dans un environnement IPV6, les tentatives de lancement d'une session sur laquelle SSL est activé peuvent échouer. [#659700]

Problèmes connus avec Citrix Receiver pour Mac 12.2

Les problèmes connus suivants ont été observés dans cette version :

- Receiver peut se bloquer si de multiples sessions simultanées sont exécutées simultanément lors de la redirection de cartes à puce. [#511140]
- Il est possible que les utilisateurs ne puissent pas utiliser la fonctionnalité de vue fractionnée d'OS X avec les fenêtres d'applications HDX. [#637963]
- Lors de la redirection d'un lecteur USB CD/DVD avec la redirection USB générique, il est possible que le lecteur soit éjecté. [#645484]
- Il est possible que certains périphériques USB ne fonctionnent pas dans une session si la stratégie Optimisation USB est définie sur Capturer. [#649082]
- Dans certains cas, l'écran de notification d'insertion d'un nouveau périphérique USB peut ne pas s'afficher correctement si un périphérique USB est connecté durant le processus de reconnexion automatique des clients. [#649714]
- Les utilisateurs peuvent être invités à entrer un trousseau lors de la connexion à un compte après la mise à niveau vers Receiver pour Mac 12.2. [#649885]
- Sur les systèmes exécutant Mac OS X 10.9, les cartes à puce peuvent ne pas être accessibles au client Bureau à distance Microsoft exécuté au sein d'une session HDX. [#650298]
- Les frappes clavier effectuées durant le processus de reconnexion à la fiabilité de session peuvent ne pas être transmises une fois que la session est reconnectée. [#652154]

Problèmes connus avec Citrix Receiver pour Mac 12.1

Les problèmes connus suivants ont été observés dans cette version :

- Si vous redimensionnez une fenêtre de bureau alors qu'un message d'ouverture de session Windows est affiché, cela peut rendre la session inopérante. [#525833]
- Il est possible qu'un message d'erreur s'affiche après le lancement d'un bureau virtuel depuis Chrome. [#564961]
- Le visualisateur n'envoie pas la configuration de clavier correcte au serveur, ce qui peut cause des problèmes de mappage du clavier. [#581829]
- Lorsque le Smooth Roaming est utilisé dans une session sur une machine OS X 10.11 (El Capitan), il est possible que la session ne se reconnecte pas. Utilisez la commande de menu « Actualiser applications » pour vous reconnecter à la session si la première tentative de reconnexion échoue. [#601542]

Problèmes connus avec Citrix Receiver pour Mac 12

Les problèmes connus suivants ont été observés dans cette version :

- Si une invite de commandes publiée est réduite lorsque vous vous déconnectez d'une session, il est possible qu'elle ne réapparaisse pas lorsque vous vous reconnectez. [#411702]
- Les applications HDX peuvent afficher un écran noir. Si cela se produit, déplacez les applications et fermez-les en cliquant là où le bouton de fermeture devrait se trouver. [#426991]
- Les utilisateurs équipés d'ordinateurs exécutant OS X Mountain Lion (10.8) peuvent observer un chevauchement sur la chaîne d'ouverture de session et l'icône de flèche vers le bas sur l'interface utilisateur de Receiver. Les utilisateurs peuvent cliquer sur Ouvrir une session ou sur la chaîne de nom d'utilisateur plutôt que sur l'icône de la flèche vers le bas si cela se produit. [#504302]
- Dans une configuration dotée de plusieurs moniteurs, les applications transparentes peuvent être déplacées vers l'écran principal lorsque l'un des écrans est reconfiguré. [#506532]
- Si la visionneuse est basculée en mode plein écran alors que l'application DirectX ou OpenGL est en cours d'exécution, cela peut entraîner la disparition du curseur. [#510745]
- Le SDK SSL peut signaler par erreur une chaîne de certificats comme ayant « expiré » si de multiples certificats sont installés et que certains ont expiré. Pour résoudre ce problème, supprimez les certificats ayant expiré du Trousseau d'accès. [#511574]
- Lorsque la langue d'un serveur est définie sur Chinois traditionnel, il est possible que les utilisateurs ne puissent pas saisir " [“ or “]" dans une session. [#511877]
- Le déplacement du curseur ne modifie pas l'état de Lync de Absent(e) à Disponible si la modification de l'état est due au fait que l'utilisateur est inactif. Si cela se produit, les utilisateurs doivent modifier manuellement l'état sur Disponible. [#512074]
- Les noms des applications affichées sur Receiver peuvent ne pas refléter les mises à jour effectuées sur le Broker et StoreFront si l'utilisateur a souscrit aux applications avant l'application des mises à jour. Si cela se produit, les utilisateurs peuvent supprimer l'application et y souscrire de nouveau. [#515097]
- Si vous redimensionnez une fenêtre de bureau alors qu'un message d'ouverture de session Windows est affiché, cela peut rendre la session inopérante. [#525833]
- Le lancement de sessions échoue lors de l’utilisation d’une carte à puce Gemalto .NET pour l’authentification auprès de XenDesktop 5.6. [#550781]
- Lors de l'utilisation d'une carte à puce PIV, Receiver ne peut pas se reconnecter à une session XenDesktop 5.6. [#550986]
- Lorsque vous utilisez OS X Mountain Lion (10.8) et que vous mettez à niveau Receiver 11.9 ou 11.9.15 vers Receiver 12.0, le lancement de Receiver peut entraîner le lancement d'une nouvelle version et d'une ancienne version de Receiver. [#552496]

- Lorsque vous utilisez le navigateur Google Chrome pour OS X, le fait de double-cliquer sur un fichier ICA sur la barre de téléchargement peut entraîner le lancement de plusieurs fichiers ICA et l'affichage d'un message d'erreur. [#564961]

- Il est possible que les utilisateurs ne puissent pas modifier les mots de passe expirés lorsqu'ils ouvrent une session à un compte PNA WI. [#568394]
  La partie inférieure du bouton de la barre d'outils XenDesktop peut être coupée lorsqu'un utilisateur passe en mode plein écran durant une session d'appel vidéo. [#570480]

- Sur OS X El Capitan (10.11), les applications et les bureaux virtuels ne s'affichent pas correctement en vue fractionnée. [#582397]

- Sur OS X Yosemite (10.10), la version de mise à niveau de Safari peut bloquer Receiver en tant que fenêtre contextuelle. Pour résoudre ce problème, autorisez les fenêtres contextuelles.

Configuration système requise

Mar 19, 2018

Systèmes d'exploitation pris en charge

Citrix Receiver pour Mac prend en charge les systèmes d'exploitation suivants :

- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- Mac OS X El Capitan (10.11)

> **Remarque**
>
> Les versions de Mac OS X antérieures à Mac OS X El Capitan ne sont pas prises en charge.

Produits Citrix compatibles

Citrix Receiver pour Mac est compatible avec toutes les versions actuellement prises en charge des produits Citrix suivants. Pour de plus amples informations sur le cycle de vie des produits Citrix et savoir quand Citrix arrête la prise en charge de versions spécifiques des produits, consultez le tableau du cycle de vie des produits Citrix.

Navigateurs compatibles

Citrix Receiver pour Mac est compatible avec les navigateurs suivants :

- Safari 7.0 (et versions ultérieures)
- Mozilla Firefox 22.x (et versions ultérieures)
- Google Chrome 28.x (et versions ultérieures)

Configuration matérielle requise

- 140.7 Mo d'espace disque disponible
- Un réseau ou une connexion Internet pour la connexion aux serveurs

- Interface Web :
  - Interface Web 5.4 pour Windows avec des sites XenApp Services (également appelé PNAgent Services) pour l'accès natif aux applications à partir de Citrix Receiver pour Mac plutôt que d'un navigateur Web
- Pour déployer Citrix Receiver pour Mac :
  - Citrix Receiver pour Web 2.1, 2.5 et 2.6
  - Interface Web Citrix 5.4
- StoreFront :
  StoreFront 2.x ou version supérieure pour l'accès natif aux applications à partir de Citrix Receiver pour Mac ou d'un navigateur Web.

Connectivité

Citrix Receiver pour Mac prend en charge les connexions suivantes à XenApp ou XenDesktop :

- HTTP
- HTTPS
- ICA-over-TLS

Citrix Receiver pour Mac prend en charge les configurations suivantes :

Pour les connexions LAN	**Pour les connexions sécurisées à distance ou locales**
• StoreFront utilisant StoreFront Services ou des sites Web Citrix Receiver pour Mac • Interface Web 5.4 pour Windows utilisant des sites XenApp Services	Citrix NetScaler Gateway : • 12.0 y compris VPX • 11.1 y compris VPX • 11.0 y compris VPX • 10.5 y compris VPX • Enterprise Edition 10.x y compris VPX • Enterprise Edition 9.x y compris VPX • VPX Citrix Secure Gateway 3.x (pour utilisation avec l'Interface Web uniquement)

Pour plus d'informations sur le déploiement de NetScaler Gateway avec StoreFront, consultez la documentation relative à NetScaler Gateway et à StoreFront.

Authentification

Pour les connexions à StoreFront, Citrix Receiver pour Mac 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*
Authentification pass-through au domaine					
Jeton de sécurité				Oui*	Oui*
Deux facteurs (domaine avec jeton de sécurité)				Oui*	Oui*

SMS Cartes à puce Certificat utilisateur	**Receiver pour Web à l'aide de navigateurs** Oui	**Site StoreFront Services (natif)** Oui	**Site StoreFront XenApp Services (natif)**	**NetScaler sur Receiver pour Web (navigateur)** Oui* Oui	**NetScaler sur site StoreFront Services (natif)** Oui* Oui (NetScaler Gateway Plugin)

*Uniquement disponible pour les sites Receiver pour Web et les déploiements qui contiennent NetScaler Gateway, avec ou sans installation du plug-in associé sur la machine.

Pour les connexions à l'Interface Web 5.4, Citrix Receiver pour Mac prend en charge les méthodes d'authentification suivantes :
Remarque : l'Interface Web utilise le terme Explicite pour représenter l'authentification par jeton de sécurité et domaine.

	Interface Web (navigateurs)	**Site Interface Web XenApp Services**	**NetScaler sur l'Interface Web (navigateur)**	**NetScaler sur un site Interface Web XenApp Services**
Anonyme	Oui			
Domaine	Oui	Oui	Oui	Oui
Authentification pass-through au domaine				
Jeton de sécurité			Oui*	Oui
Deux facteurs (domaine avec jeton de sécurité)			Oui*	Oui
SMS			Oui*	Oui
Cartes à puce	Oui		Oui	
Certificat utilisateur			Oui (requiert NetScaler Gateway Plugin)	Oui (requiert NetScaler Gateway Plugin)

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

Configuration requise pour l'authentification par carte à puce

Dec 12, 2017

Citrix Receiver pour Mac prend en charge l'authentification par carte à puce dans les configurations suivantes :

- Authentification par carte à puce à Receiver pour Web/StoreFront 2.x et version supérieure et XenDesktop 7.1 et version supérieure ou XenApp 6.5 et version supérieure.
- 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.
- Avec de multiples certificats : Citrix Receiver pour Mac prend en charge l'utilisation de multiples certificats avec une seule carte à puce ou avec plusieurs cartes à puce. Lorsqu'un utilisateur insère une carte à puce dans le lecteur de cartes, les certificats sont disponibles pour toutes les applications exécutées sur l'appareil, y compris Citrix Receiver pour Mac.
- Dans des sessions double-hop : si un double-hop est requis, une connexion supplémentaire est établie entre Citrix Receiver pour Mac et le bureau virtuel de l'utilisateur.

À propos de l'authentification par carte à puce à NetScaler

Lorsque vous utilisez une carte à puce pour authentifier une connexion et que cette dernière contient de multiples certificats utilisables, Citrix Receiver pour Mac vous invite à sélectionner un certificat. Après sélection d'un certificat, Citrix Receiver pour Mac vous invite à sélectionner le mot de passe de la carte à puce ; une fois authentifié, la session se lance.

S'il n'existe qu'un seul certificat approprié sur la carte à puce, Citrix Receiver pour Mac utilise ce dernier et ne vous invite pas à le sélectionner. Toutefois, vous devez toujours entrer le mot de passe associé à la carte à puce pour authentifier la connexion et démarrer la session.

Spécification d'un module PKCS#11 pour l'authentification par carte à puce

Remarque : l'installation du module PKCS#11 n'est pas obligatoire. Cette section s'applique uniquement aux sessions ICA. Elle ne s'applique pas à l'accès de Citrix Receiver à NetScaler Gateway ou StoreFront à l'aide d'une carte à puce.

Pour spécifier un module PKCS#11 pour l'authentification par carte à puce :

1. Dans Citrix Receiver, sélectionnez **Préférences**.
2. Cliquez sur **Sécurité et confidentialité**.
3. Dans la section **Sécurité et confidentialité**, cliquez sur **Carte à puce**.
4. Dans le champ **PKCS#11**, sélectionnez le module approprié ; cliquez sur **Autre** pour accéder à l'emplacement du module PKCS#11 si le module que vous recherchez n'est pas répertorié.
5. Après avoir sélectionné le module approprié, cliquez sur **Ajouter**.

Lecteurs, middleware et cartes à puce pris en charge

Citrix Receiver pour Mac prend en charge la plupart des lecteurs de carte à puce et middleware cryptographiques compatibles avec macOS. Citrix a validé le fonctionnement avec ce qui suit.

Lecteurs pris en charge :

- Lecteurs de carte à puce USB courants

Middleware pris en charge :

- Clariify
- Version du client Activeidentity
- Version du client Charismathics

Cartes à puce prises en charge :

- Cartes PIV
- Cartes CAC
- Cartes Gemalto .NET

Suivez les instructions fournies par le fournisseur des lecteurs de carte à puce et middleware cryptographiques compatibles avec macOS pour configurer les machines utilisateur.

Restrictions

- Les certificats doivent être stockés sur une carte à puce et non sur la machine utilisateur.
- Citrix Receiver pour Mac n'enregistre pas le certificat choisi par l'utilisateur.
- Citrix Receiver pour Mac ne stocke et n'enregistre pas le code PIN de la carte à puce de l'utilisateur. L'acquisition du code PIN est traitée par le système d'exploitation, qui peut disposer de son propre mécanisme de mise en cache.
- Citrix Receiver pour Mac ne reconnecte pas les sessions lorsqu'une carte à puce est insérée.
- 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.

Informations supplémentaires

Voir :

- Prise en charge des cartes à puce avec Citrix Receiver pour Mac 11.9.15 sur OS X 10.10.2

Installation, configuration, mise à niveau, déploiement ou désinstallation de Citrix Receiver pour Mac

Dec 12, 2017

Cette version de Citrix Receiver pour Mac contient un seul pack d'installation, CitrixReceiver.dmg, et prend en charge l'accès distant via NetScaler Gateway et Secure Gateway.

Dans cet article :

Installation

Citrix Receiver pour Mac peut être installé par un utilisateur depuis le site Web de Citrix, automatiquement depuis Receiver pour Web ou l'Interface Web, ou à l'aide d'un outil de distribution électronique de logiciels (ESD).

Par un utilisateur à partir de Citrix.com :

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

> ### Remarque
>
> Un nouvel utilisateur est un utilisateur qui n'a pas encore installé Citrix Receiver pour Mac sur sa machine.

- La découverte de compte basée sur l'adresse e-mail pour un nouvel utilisateur ne s'applique pas si Citrix Receiver pour Mac est téléchargé depuis 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'Interface Web

- Un utilisateur qui utilise Citrix Receiver pour Mac pour la première fois peut créer un compte en entrant une adresse URL de serveur ou en téléchargeant un fichier de provisioning.

À l'aide d'un outil ESD (distribution électronique de logiciels)

- Un utilisateur qui utilise Citrix Receiver pour Mac pour la première fois doit entrer l'adresse URL d'un serveur pour créer un compte.

Installation manuelle de Citrix Receiver pour Mac

Les utilisateurs peuvent installer Citrix Receiver pour Mac à partir de l'Interface Web, d'un partage réseau où directement sur la machine de l'utilisateur en téléchargeant le fichier CitrixReceiver.dmg depuis le site Web de Citrix à l'adresse http://www.citrix.com.

Pour installer Citrix Receiver pour Mac

1. Téléchargez le fichier .dmg correspondant à la version de Citrix Receiver pour Mac que vous souhaitez installer à partir du site Web de Citrix et ouvrez-le.
2. Sur la page Introduction, cliquez sur **Continue**.
3. Sur la page **License**, cliquez sur **Continue**.
4. Cliquez sur **Agree** pour accepter les termes du contrat de licence.
5. Sur la page **Installation Type**, cliquez sur **Install**.
6. Entrez le nom d'utilisateur et le mot de passe d'un administrateur sur la machine locale.

Mise à niveau de Citrix Receiver pour Mac

Les mises à niveau sont prises en charge à partir des versions 11.x de Online Plug-in pour Mac. Vous pouvez mettre à niveau Citrix Receiver pour Mac depuis n'importe quelle version antérieure de Citrix Receiver pour Mac.

> **Important**
>
> L'intégration à ShareFile a été supprimée de la version 11.8. Si vous avez intégré Receiver pour Mac avec ShareFile, vous serez invité, lors de la mise à niveau, à télécharger l'application ShareFile de façon à ce que puissiez continuer à accéder à vos données distantes.

À propos du déploiement et de la configuration de Citrix Receiver pour Mac

Pour les déploiements avec StoreFront :

- Il est recommandé de configurer NetScaler Gateway et StoreFront 3.x comme décrit dans la documentation relative à ces produits dans la documentation Netscaler Gateway et StoreFront. Joignez le fichier de provisioning créé par StoreFront à un e-mail et indiquez aux utilisateurs comment mettre à niveau et ouvrir le fichier de provisioning après l'installation de Citrix Receiver pour Mac.
- Si vous ne souhaitez pas utiliser le fichier de provisioning, demandez aux utilisateurs d'entrer l'adresse URL d'un serveur NetScaler Gateway. Si vous avez configuré la découverte de compte basée sur l'adresse e-mail comme décrit dans la documentation de 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. Indiquez aux utilisateurs comment mettre à niveau Citrix Receiver pour Mac, accéder au site Receiver pour Web et télécharger le fichier de provisioning à partir de l'interface 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 Mac et faites savoir à vos utilisateurs comment mettre à niveau Citrix Receiver pour Mac. Vous pouvez par exemple ajouter des légendes d'installation sur l'écran Messages pour informer les utilisateurs qu'ils doivent mettre à niveau vers la dernière version de Citrix Receiver pour Mac.

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

Vous pouvez déployer Citrix Receiver pour Mac 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 Citrix Receiver pour Mac, l'utilisateur est invité à télécharger et installer Citrix Receiver pour Mac. Pour plus d'informations, veuillez consulter la documentation de StoreFront.

Déploiement de Citrix Receiver pour Mac à partir d'un écran d'ouverture de session de l'Interface Web

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

Vous pouvez déployer Citrix Receiver pour Mac 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.

Désinstallation de Citrix Receiver pour Mac

Vous pouvez désinstaller Citrix Receiver pour Mac manuellement en ouvrant le fichier CitrixReceiver.dmg, en sélectionnant **Désinstaller Citrix Receiver** et en suivant les instructions qui s'affichent à l'écran.

Configuration de Citrix Receiver pour Mac

Dec 12, 2017

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

- Configurer la redirection USB
- Configurer la fiabilité de session
- Configurer CEIP
- Configurer la mise à disposition d'applications : assurez-vous que votre environnement XenApp est configuré correctement. Comprenez les options qui vous sont offertes et fournissez des descriptions claires des applications.
- Configurer le mode libre-service : configurez le mode libre-service, qui permet aux utilisateurs de s'abonner à des applications depuis l'interface utilisateur de Citrix Receiver pour Mac.
- Configurer StoreFront : 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.
- Fournir 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. Dans certains environnements, les utilisateurs doivent manuellement configurer l'accès aux comptes.
- Configuration de la mise à jour automatique
- Configuration de l'éditeur IME client amélioré
- Synchronisation de la disposition du clavier
- 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 redirection USB

La redirection de périphériques USB HDX autorise la redirection de périphériques USB vers et à partir d'une machine utilisateur. Par exemple, un utilisateur peut connecter un lecteur flash à un ordinateur local et y accéder à distance à partir d'un bureau virtuel où d'une application hébergée de bureau. Pendant une session, les utilisateurs peuvent ajouter des périphériques plug-and-play, y compris des périphériques Picture Transfer Protocol (PTP), tels que des appareils photo numériques, des périphériques MTP (Media Transfer Protocol), tels que des lecteurs audio numériques ou lecteurs multimédias portables, des périphériques de point de vente (POS) et d'autres périphériques tels que des souris 3D Space, des scanners, des dispositifs de signature numérique, etc.

> ### Remarque
>
> Le périphérique USB double-hop n'est pas pris en charge pour les sessions d'application hébergée de bureau.

La redirection USB est disponible pour les versions de Citrix Receiver pour Mac suivantes :

- Windows
- Linux
- Macintosh

Par défaut, la redirection USB est autorisée pour certaines classes de périphériques USB et refusée pour d'autres. Vous pouvez limiter les types de périphériques USB mis à la disposition d'un bureau virtuel en mettant à jour la liste des

périphériques USB pris en charge pour la redirection, comme décrit plus loin dans cette section.

> ## Conseil
>
> Dans les environnements dans lesquels la séparation de la sécurité entre la machine utilisateur et le serveur est nécessaire, Citrix vous recommande d'informer les utilisateurs sur les types de périphériques USB à éviter.

Des canaux virtuels optimisés sont disponibles pour rediriger les périphériques USB les plus populaires. Ils fournissent des performances supérieures et améliorent la bande passante via un réseau étendu. Les canaux virtuels optimisés sont généralement la meilleure option, notamment dans les environnements à latence élevée.

> ## Remarque
>
> À des fins de redirection USB, Citrix Receiver pour Mac utilise une carte intelligente identique à celle de la souris.

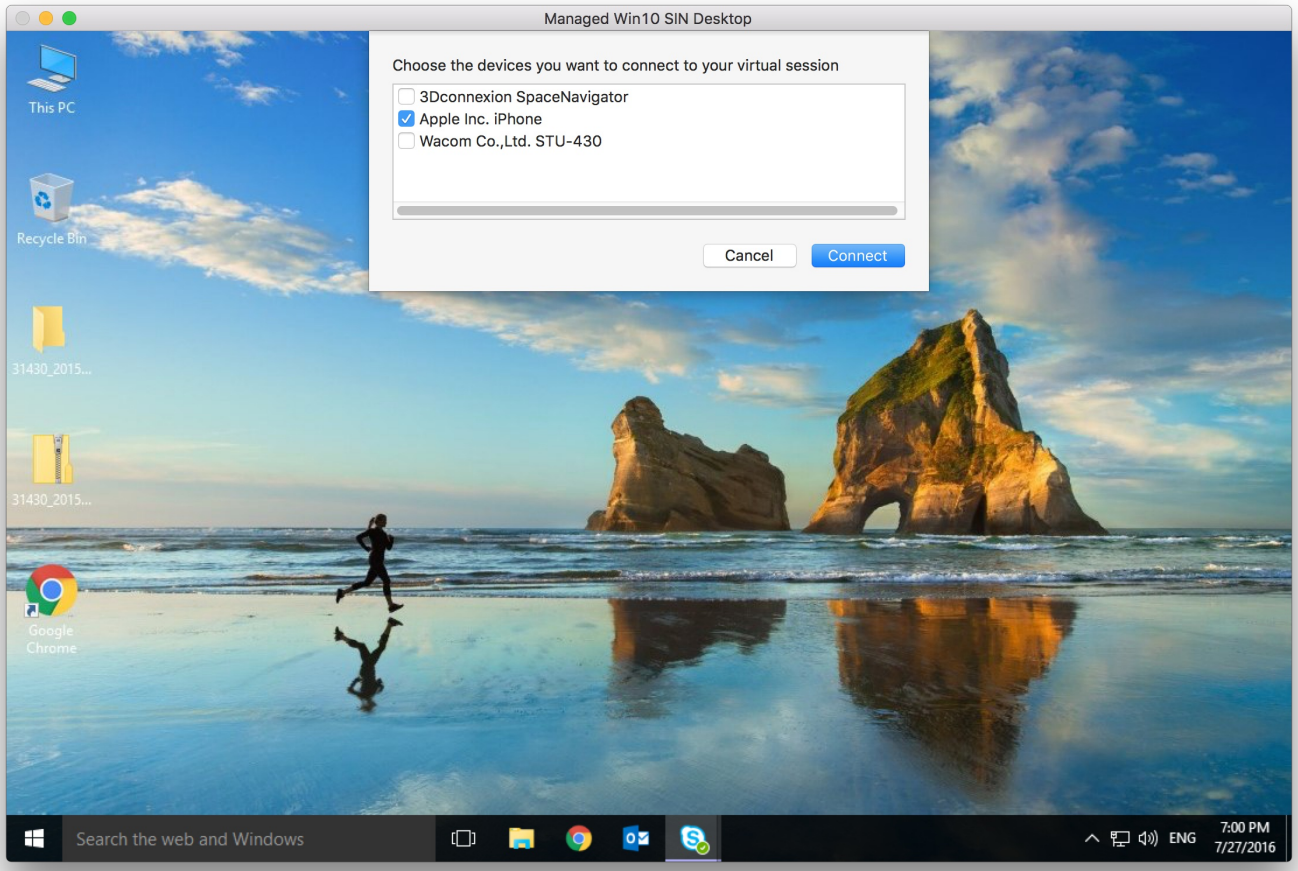
Le produit prend en charge l'utilisation de canaux virtuels optimisés avec des périphériques USB 3.0 et des ports USB 3.0, tel qu'un canal virtuel CDM (utilisé pour visualiser des fichiers sur une caméra ou pour fournir l'audio à un casque). Le produit prend également en charge la redirection USB générique de périphériques USB 3.0 connectés à un port USB 2.0.

Certaines des fonctionnalités spécifiques avancées, telles que les boutons des périphériques d'interface utilisateur (HID) sur une webcam, peuvent ne pas fonctionner correctement avec le canal virtuel optimisé ; si vous rencontrez ce problème, utilisez le canal virtuel USB générique.

Certains périphériques ne sont pas redirigés par défaut et sont uniquement disponibles pour la session locale. Par exemple, il n'est pas approprié de rediriger une carte d'interface réseau qui est directement connectée via USB interne.

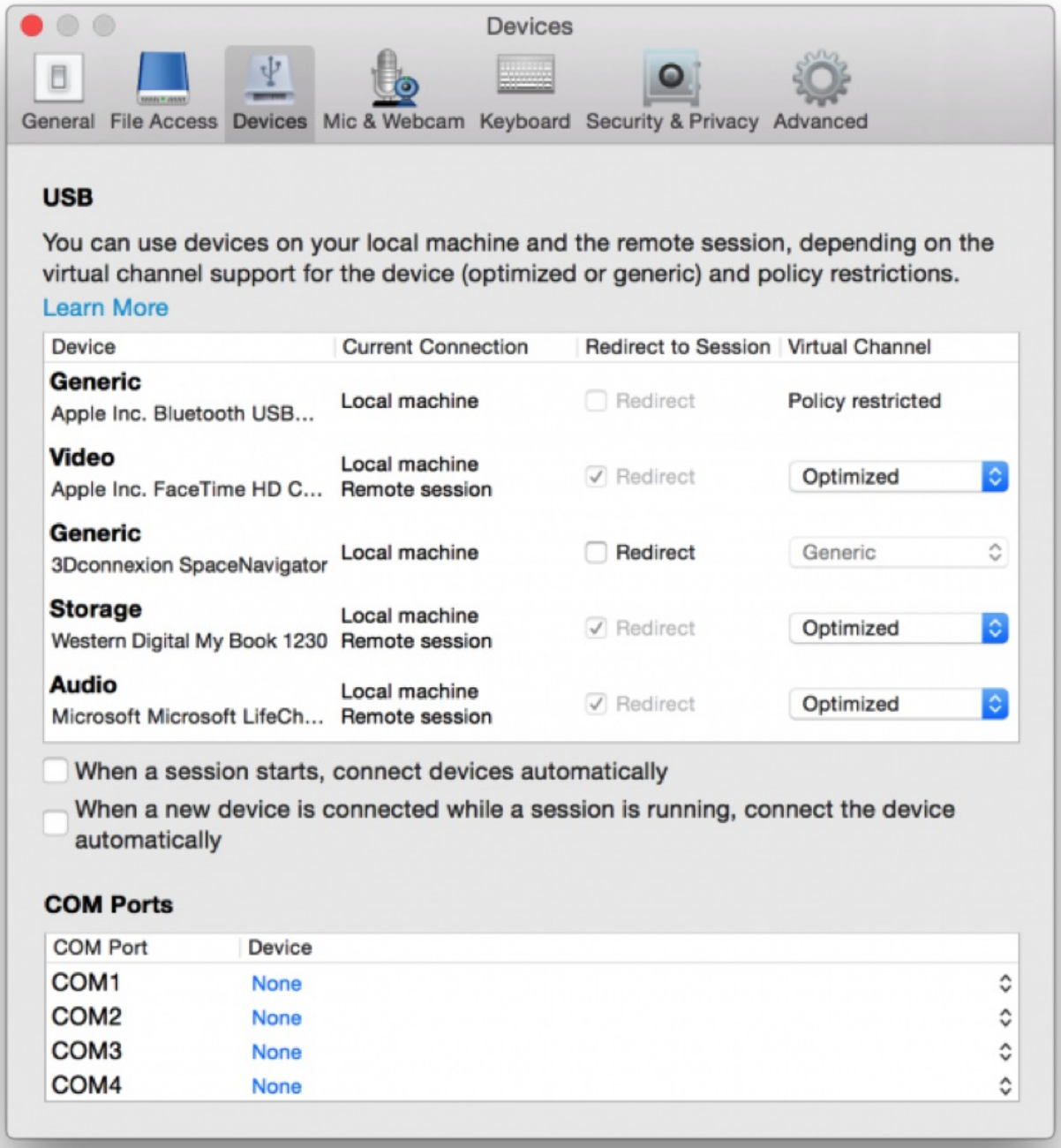
Pour utiliser la redirection USB :

1. Connectez le périphérique USB à l'appareil sur lequel Receiver est installé.
2. Vous serez invité à sélectionner les périphériques USB disponibles sur votre système local.

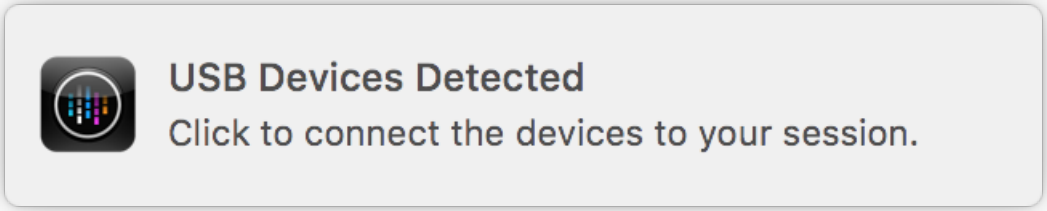


3. Sélectionnez le périphérique auquel vous voulez vous connecter et cliquez sur **Connecter**. En cas d'échec de la connexion, un message d'erreur s'affiche.

4. Dans la fenêtre **Préférences** de l'onglet **Périphériques**, le périphérique USB connecté est répertorié dans le panneau USB :



5. Sélectionnez le type de canal virtuel pour le périphérique USB, *Générique* ou *Optimisé*.
6. Un message s'affiche. Cliquez pour connecter le périphérique USB à votre session :



Utiliser et supprimer des périphériques USB

Les utilisateurs peuvent se connecter un périphérique USB avant ou après le démarrage d'une session virtuelle. Lors de l'utilisation de Citrix Receiver pour Mac, ce qui suit s'applique :

- Les périphériques connectés après démarrage d'une session apparaissent immédiatement dans le menu USB de Desktop Viewer.
- Si un périphérique USB n'est pas redirigé correctement, vous pouvez parfois résoudre le problème en attendant que la session virtuelle ait démarré avant de connecter le périphérique.
- Pour éviter la perte de données, utilisez le menu **Retrait en toute sécurité** de Windows avant de retirer le périphérique USB.

Configuration de Enlightened Data Transport (EDT)

EDT est activé par défaut dans Citrix Receiver pour Mac.

Citrix Receiver pour Mac lit les paramètres EDT tels qu'ils sont définis dans le fichier default.ica et les applique comme il se doit.

Pour désactiver EDT, exécutez la commande suivante dans une fenêtre de terminal :

defaults write com.citrix.receiver.nomas HDXOverUDPAllowed -bool NO

Configurer la fiabilité de session et la reconnexion automatique des clients

La fiabilité de session maintient les sessions actives sur l'écran de l'utilisateur lorsque la connectivité au réseau est interrompue. L'utilisateur peut donc visualiser l'application jusqu'à ce que la connexion au réseau reprenne.

Grâce à la fiabilité de session, la session reste active sur le serveur. Pour indiquer que la connectivité est interrompue, l'affichage de l'utilisateur reste figé jusqu'à ce que la connectivité soit rétablie de l'autre côté du tunnel. L'utilisateur a toujours accès à l'affichage de l'application durant l'interruption et peut reprendre l'interaction avec l'application lorsque la connexion réseau est rétablie. La fonction de fiabilité de session permet aux utilisateurs de se reconnecter sans avoir à s'authentifier de nouveau.

> ### Important
>
> Les utilisateurs de Citrix Receiver pour Mac ne peuvent pas changer le paramètre de serveur.

Vous pouvez utiliser la fonction de fiabilité de session avec le protocole TLS (Transport Layer Security).

> ## Remarque
>
> TLS crypte uniquement les données envoyées entre la machine utilisateur et NetScaler Gateway.

Utilisation des stratégies de fiabilité de session

Le paramètre de stratégie **Connexions de fiabilité de session** autorise ou interdit la fiabilité de session.

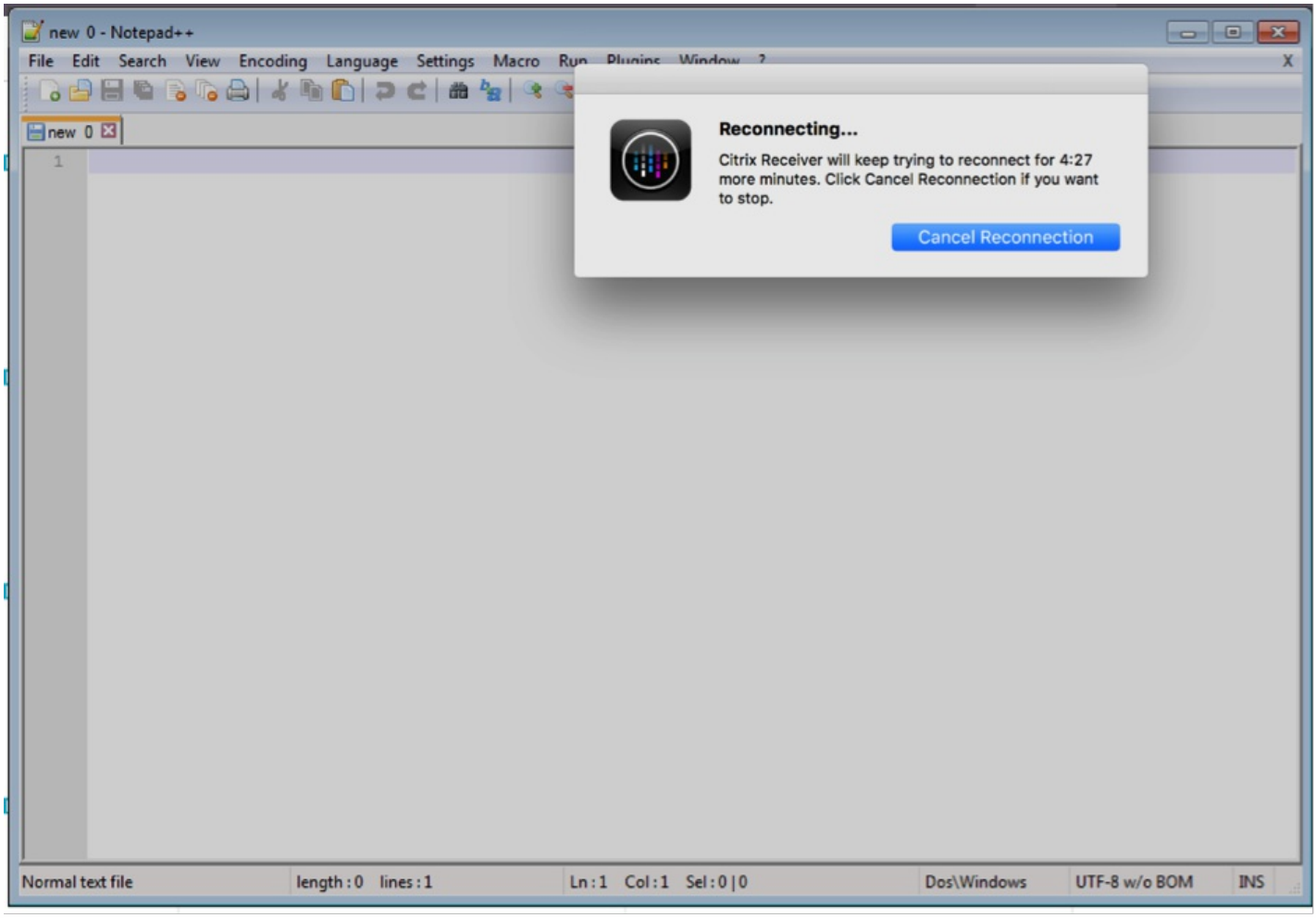
Le paramètre de stratégie **Expiration de délai de la fiabilité de session** est réglé par défaut sur 180 secondes, ou trois minutes. Bien que vous puissiez prolonger la durée pendant laquelle la fiabilité de session garde une session ouverte, le but de cette fonctionnalité est d'éviter à l'utilisateur de devoir s'authentifier à nouveau.

> ## Conseil
>
> Si vous augmentez la durée pour laquelle une session est gardée ouverte, les risques d'accès non autorisé sont accrus : un utilisateur distrait peut s'éloigner de sa machine cliente et il est alors possible que des utilisateurs non autorisés accèdent à sa session.

Les connexions entrantes de fiabilité de session utilisent le port 2598, à moins que vous ne changiez le numéro de port défini dans le paramètre de stratégie Numéro de port de la fiabilité de session.

Si vous ne souhaitez pas autoriser les utilisateurs à se reconnecter aux sessions interrompues sans authentification, utilisez la fonction de reconnexion automatique des clients. Vous pouvez configurer le paramètre de stratégie Authentification de la reconnexion automatique des clients pour inviter les utilisateurs à s'authentifier à nouveau lors de la reconnexion aux sessions interrompues.

Si vous utilisez la fonction de fiabilité de session et la fonction de reconnexion automatique des clients, ces fonctions agissent l'une après l'autre. La fonction de fiabilité de session ferme (ou déconnecte) la session utilisateur après la période spécifiée dans le paramètre de stratégie Expiration de délai de la fiabilité de session. Ensuite, les paramètres définis pour la fonction de reconnexion automatique des clients s'appliquent et la fonction tente de reconnecter l'utilisateur à la session déconnectée.



Remarque

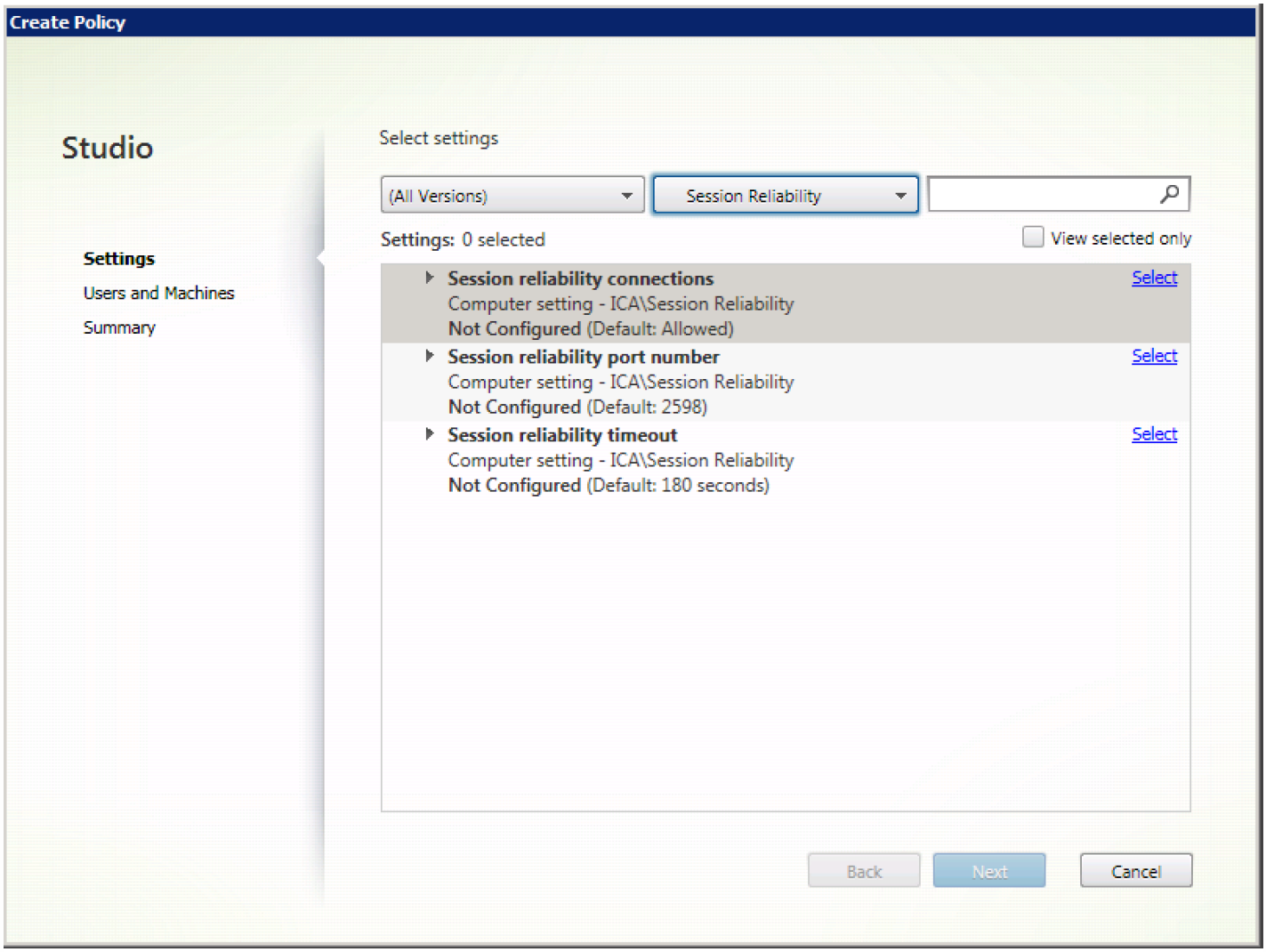
La fiabilité de session est activée par défaut au niveau du serveur. Pour désactiver cette fonctionnalité, configurez la stratégie gérée par le serveur.

Configuration de la fiabilité de session

Par défaut, la fiabilité de session est activée.

Pour désactiver la fiabilité de session :

1. Lancez Citrix Studio.
2. Ouvrez la stratégie **Connexions de fiabilité de session**.
3. Définissez la stratégie sur **Interdit**.



Configuration de l'expiration de la fiabilité de session

La fiabilité de session est définie par défaut pour expirer après 180 secondes.

Remarque : la stratégie Expiration de délai de la fiabilité de session peut uniquement être configurée avec XenApp/XenDesktop 7.11 et plus.

Pour modifier l'expiration de la fiabilité de session

1. Lancez Citrix Studio.
2. Ouvrez la stratégie **Expiration de délai de la fiabilité de session**.
3. Modifiez la valeur du délai d'expiration.
4. Cliquez sur **OK**.

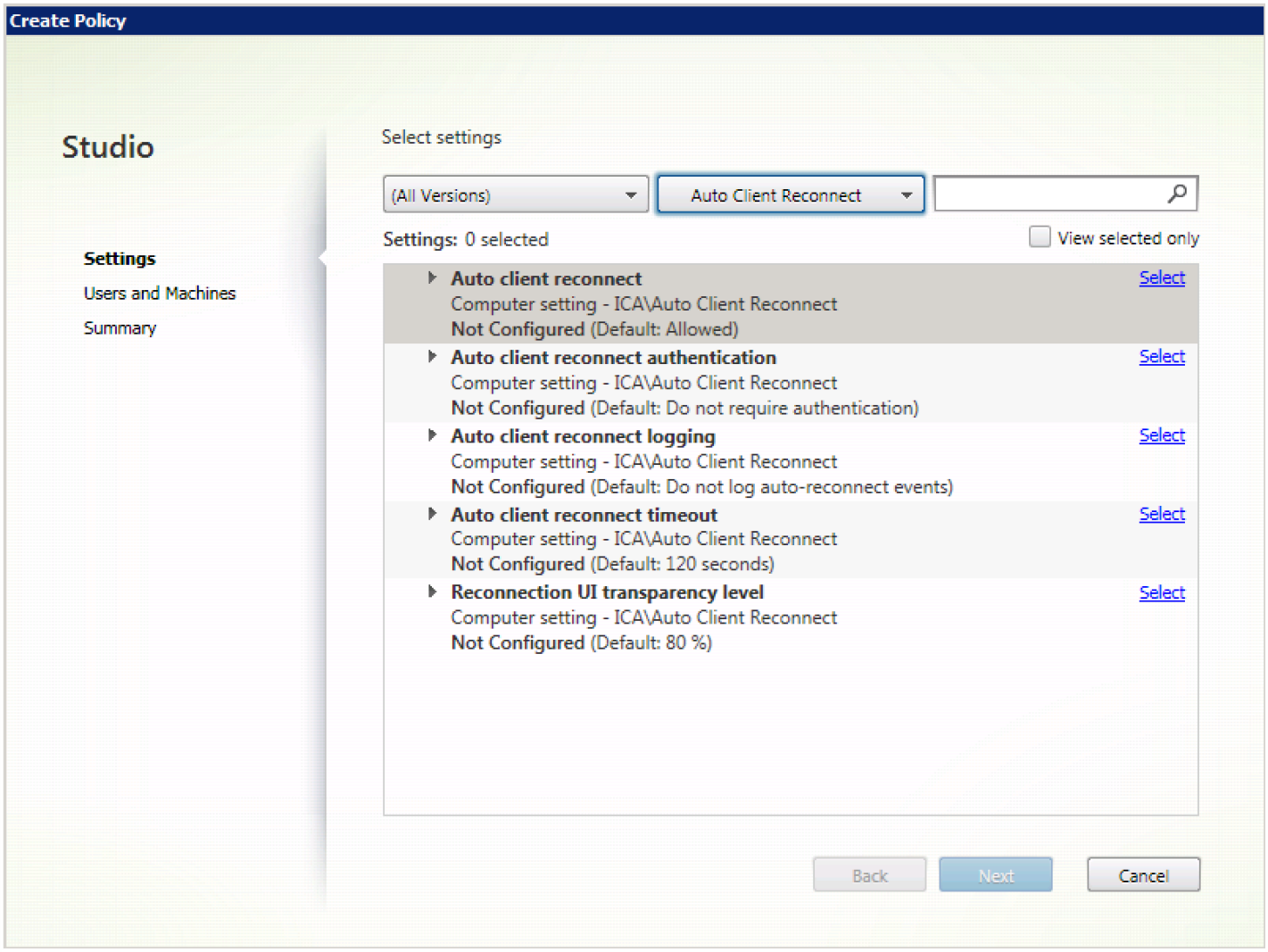
Configuration de la reconnexion automatique des clients

La reconnexion automatique des clients est activée par défaut.

Pour désactiver la reconnexion automatique des clients :

1. Lancez Citrix Studio.

2. Ouvrez la **stratégie Reconnexion automatique des clients**.
3. Définissez la stratégie sur **Interdit**.



Configuration de l'expiration de la reconnexion automatique des clients

La reconnexion automatique des clients est définie par défaut pour expirer après 120 secondes.

Remarque : la stratégie Délai de reconnexion automatique des clients peut uniquement être configurée avec XenApp/XenDesktop 7.11 et versions ultérieures.

Pour modifier l'expiration de la reconnexion automatique des clients :

1. Lancez Citrix Studio.
2. Ouvrez la stratégie **Reconnexion automatique des clients**.
3. Modifiez la valeur du délai d'expiration.
4. Cliquez sur **OK**.

Limitations :
Sur un VDA Terminal Server, Citrix Receiver pour Mac utilise 120 secondes en tant que valeur d'expiration quels que soient les paramètres utilisateur.

Configuration du niveau de transparence de l'interface durant la reconnexion

L'interface utilisateur de la session est affichée durant les tentatives de reconnexion automatique des clients et de reconnexion de la fiabilité de session. Le niveau de transparence de l'interface utilisateur peut être modifié à l'aide d'une stratégie Studio.

Par défaut, la transparence de l'interface durant la reconnexion est définie sur 80 %.

Pour modifier le niveau de transparence de l'interface durant la reconnexion :

1. Lancez Citrix Studio.
2. Ouvrez la stratégie Niveau de transparence de l'interface durant la reconnexion.
3. Modifiez la valeur.
4. Cliquez sur **OK**.

Interaction entre la reconnexion automatique des clients et la fiabilité de session

Les enjeux en matière de mobilité associés à l'utilisation de divers points d'accès, aux interruptions réseau et aux délais d'affichage liés à la latence contribuent à créer des environnements complexes lorsqu'il s'agit de maintenir l'intégrité des connexions aux sessions Citrix Receiver actives. Pour résoudre ce problème, Citrix a amélioré les technologies de fiabilité de session et de reconnexion automatique présentes dans cette version de Receiver pour Mac.

La reconnexion automatique des clients, associée à la fiabilité de session permet aux utilisateurs de se reconnecter automatiquement à leurs sessions Citrix Receiver suite au rétablissement de la connexion au réseau. Ces fonctionnalités, qui sont activées par des stratégies dans Citrix Studio, peuvent être utilisées pour améliorer considérablement l'expérience utilisateur.

> ## Remarque
>
> Les valeurs de délai de la reconnexion automatique des clients et de la fiabilité de session peuvent être modifiées à l'aide du fichier **default.ica** dans StoreFront.

Reconnexion automatique des clients

La reconnexion automatique des clients peut être activée ou désactivée à l'aide de stratégies Citrix Studio. Cette fonctionnalité est activée par défaut. Pour de plus amples informations sur la modification de cette stratégie, reportez-vous à la section Reconnexion automatique des clients plus haut dans cet article.

Utilisez le fichier default.ica dans StoreFront pour modifier le délai de connexion de la reconnexion automatique des clients ; ce délai est réglé sur 120 secondes par défaut (ou deux minutes).

Paramètre	Exemple	Mode par défaut
TransportReconnectRetryMaxTimeSeconds	TransportReconnectRetryMaxTimeSeconds=60	120

Fiabilité de session

La fiabilité de session peut être activée ou désactivée à l'aide de stratégies Citrix Studio. Cette fonctionnalité est activée

par défaut.

Utilisez le fichier **default.ica** dans StoreFront pour modifier le délai de connexion de la fiabilité de session ; ce délai est réglé sur 180 secondes par défaut (ou trois minutes).

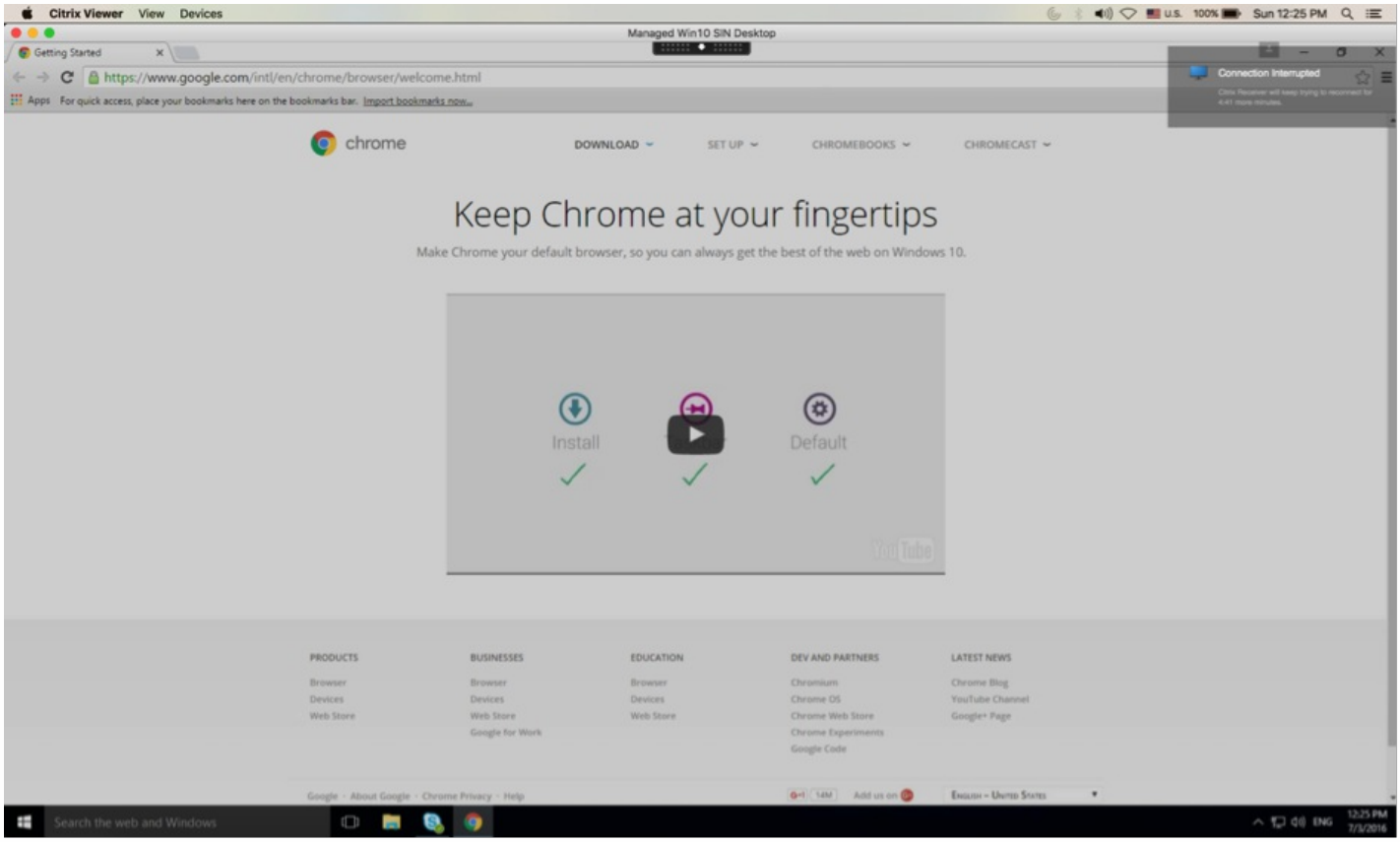
Paramètre	Exemple	Mode par défaut
SessionReliabilityTTL	SessionReliabilityTTL=120	180

Comment fonctionnent la reconnexion automatique des clients et la fiabilité de session

Lorsque la reconnexion automatique des clients et la fiabilité de session sont activées pour Citrix Receiver pour Mac, tenez compte de ce qui suit :

- Une fenêtre de session est grisée lorsqu'une reconnexion est en cours ; un minuteur affiche le temps restant avant que la session ne soit reconnectée. Une fois que la session a expiré, elle est déconnectée.

Par défaut, la notification de reconnexion démarre après 5 minutes ; cette valeur représente les valeurs combinées de chacun des minuteurs (reconnexion automatique des clients et fiabilité de session), respectivement 2 et 3 minutes. L'image ci-dessous illustre la notification qui s'affiche dans la partie supérieure droite de l'interface de la session :

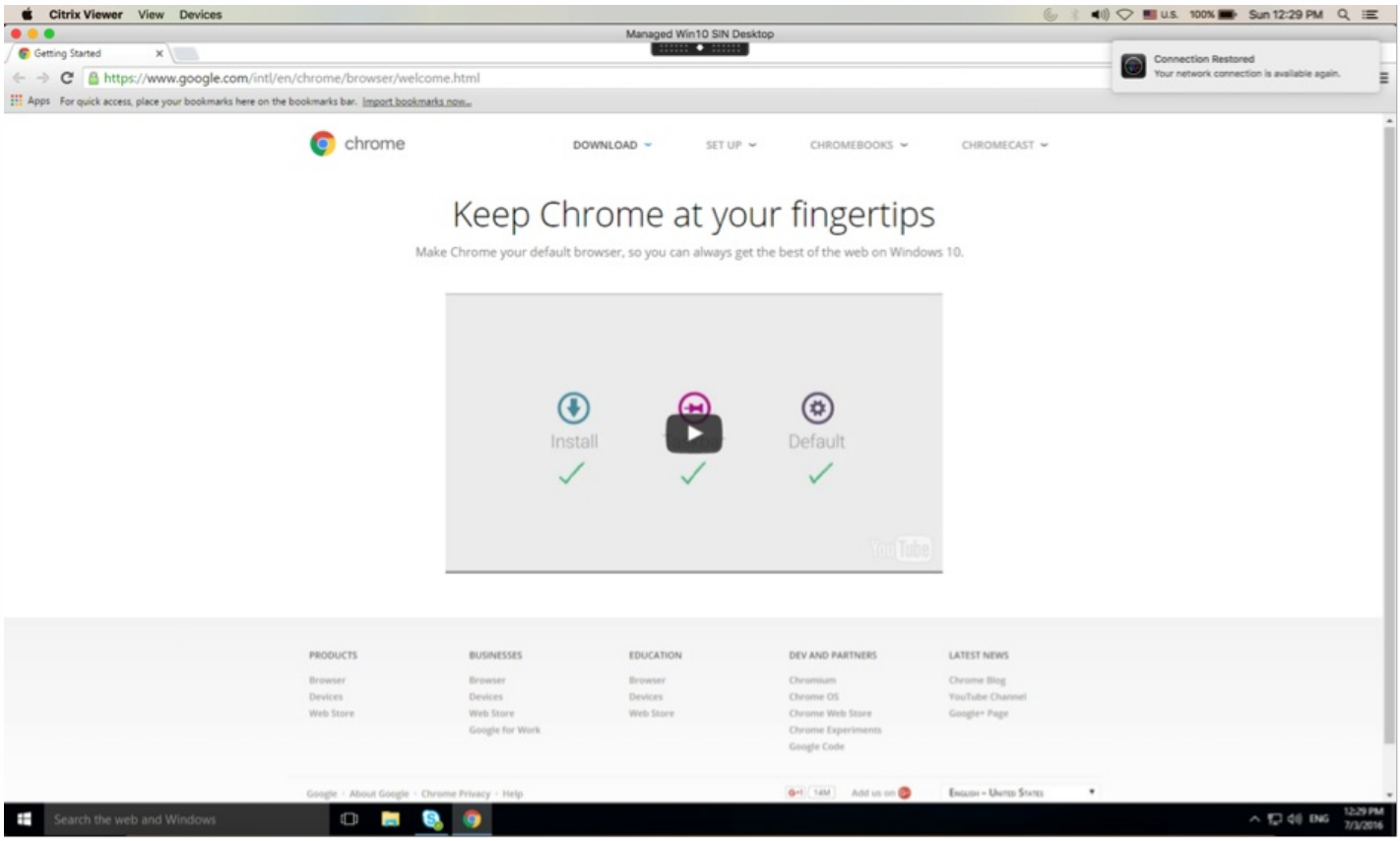


Conseil

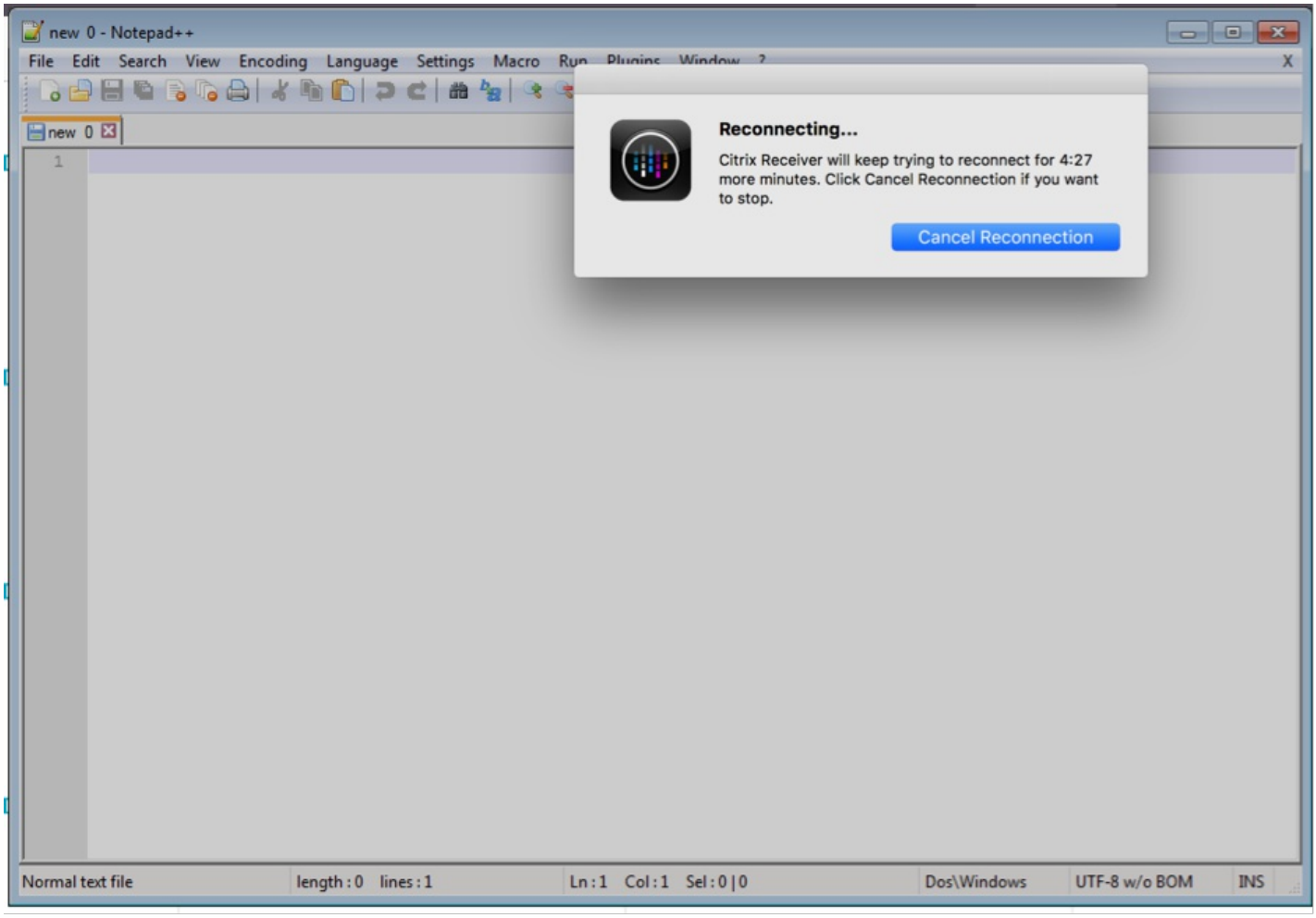
Vous pouvez modifier la luminosité des nuances de gris utilisées pour une session inactive à l'aide d'une invite de commande. Par

exemple, defaults write com.citrix.receiver.nomas NetDisruptBrightness 80. Par défaut, cette valeur est définie sur 80. La valeur maximale ne peut pas dépasser 100 (indique une fenêtre transparente) et la valeur minimale peut être réglée sur 0 (écran entièrement noir).

- Les utilisateurs sont notifiés lorsqu'une session est reconnectée (ou lorsqu'une session est déconnectée). La notification s'affiche dans la partie supérieure droite de l'interface de la session :



- Une fenêtre de session sous le contrôle de la reconnexion automatique des clients et de la fiabilité de session affiche un message d'information indiquant l'état de la connexion à la session. Cliquez sur **Annuler la reconnexion** pour revenir à une session active.



Configuration de CEIP

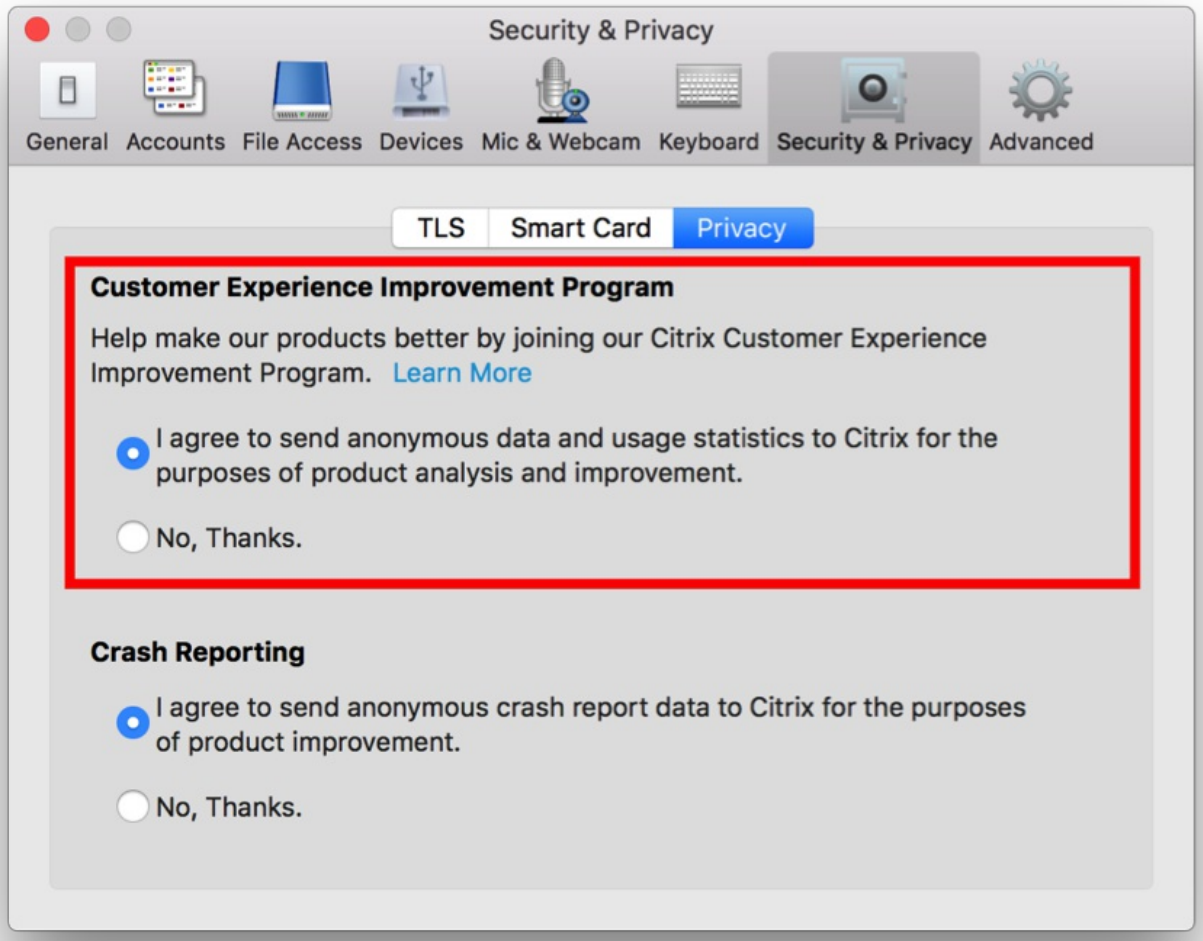
CEIP est programmé par défaut pour collecter et charger de manière sécurisée des données auprès de Citrix tous les 7 jours. Vous pouvez modifier votre participation au programme CEIP à n'importe quel moment à l'aide de l'écran **Sécurité > Préférences** de Citrix Receiver pour Mac.

Conseil

Lorsque le programme CEIP est désactivé, des informations minimales contenant uniquement la version de Citrix Receiver pour Mac installée sont chargées ; cela ne se produit qu'une seule fois. Ces informations aussi succinctes qu'elles soient sont utiles à Citrix car elles permettent de connaître la répartition des différentes versions utilisées par les clients. Cela ne se produit qu'une seule fois dès que le programme CEIP est désactivé.

Pour désactiver le programme CEIP ou ne pas y participer :

1. Dans la fenêtre **Préférences**, sélectionnez **Sécurité et confidentialité**.
2. Sélectionnez l'onglet **Confidentialité**.
3. Sélectionnez le bouton radio approprié. Par exemple, pour désactiver le programme CEIP, cliquez sur **Non merci**.
4. Cliquez sur **OK**.



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 Mac 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 à Citrix Receiver pour Mac ou de configurer Citrix Receiver de manière à pointer vers un site StoreFront pour pouvoir configurer le mode libre-service. Ce dernier permet à vos utilisateurs de s'abonner à des applications via Citrix Receiver pour Mac. 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 de la Tech Preview de Citrix Receiver pour Mac. Pour de plus amples informations sur l'expérience utilisateur de la Tech Preview de Citrix Receiver pour Mac, 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 pour Mac.

Configurer le mode libre-service

Comme indiqué précédemment, il vous suffit d'ajouter un compte StoreFront à Citrix Receiver pour Mac ou de configurer Citrix Receiver de manière à pointer vers un site StoreFront pour pouvoir configurer le mode libre-service. Ce dernier permet aux utilisateurs de s'abonner à des applications à partir de l'interface utilisateur de Citrix Receiver pour Mac. 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 avertir les utilisateurs de la présence d'une application ou faciliter la recherche des applications fréquemment utilisées en les répertoriant dans la liste Sélection de Citrix Receiver pour Mac, 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.

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 pour Mac. 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 Citrix Receiver pour Mac.
2. Configurez des magasins pour CloudGateway comme vous le feriez pour toute autre application XenApp ou XenDesktop. Aucune configuration spéciale n'est nécessaire pour Citrix Receiver pour Mac. Pour de plus amples informations, consultez la section
   — Configuration des magasins
   dans la documentation StoreFront.

Fournir des informations de compte aux utilisateurs

Après l'installation, vous devez fournir aux utilisateurs les informations de compte dont ils ont besoin pour accéder à leurs applications et bureaux hébergés. 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 une adresse URL de configuration générée automatiquement
- Fournir aux utilisateurs des informations de compte à entrer manuellement

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

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

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

Pour configurer NetScaler Gateway afin d'accepter les connexions utilisateur à l'aide d'une adresse e-mail pour découvrir l'adresse URL de StoreFront ou de 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

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

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

Fournir aux utilisateurs une adresse URL de configuration générée automatiquement

Vous pouvez utiliser l'outil Citrix Receiver for Mac Setup URL Generator pour créer une adresse URL contenant les informations de compte. Une fois Citrix Receiver pour Mac installé, les utilisateurs n'ont qu'à cliquer sur cette URL pour configurer leur compte et accéder à leurs ressources. Utilisez cet outil pour configurer les paramètres des comptes et envoyez ces informations par e-mail ou publiez-les auprès de tous vos utilisateurs simultanément.

Fournir aux utilisateurs des informations de compte à entrer manuellement

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

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

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

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

Configuration de la mise à jour automatique

Configuration à l'aide de l'interface utilisateur graphique

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

1. Accédez à la boîte de dialogue **Préférences** dans Citrix Receiver pour Mac.
2. Dans le panneau **Avancées**, cliquez sur **Mise à jour automatique**. La boîte de dialogue Mises à jour de Citrix Receiver s'affiche.
3. Sélectionnez l'une des options suivantes :
   - Oui, me notifier
   - Non, ne pas me notifier
   - Utiliser paramètres spécifiés par l'administrateur
4. Fermez la boîte de dialogue pour enregistrer les modifications.

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

Les administrateurs peuvent configurer les mises à jour de Citrix Receiver à l'aide de StoreFront. Citrix Receiver utilise uniquement cette configuration pour les utilisateurs qui ont sélectionné « Utiliser paramètres spécifiés par l'administrateur ». Pour la configurer manuellement, suivez les étapes ci-dessous.

1. Utilisez un éditeur de texte pour ouvrir le fichier web.config. L'emplacement par défaut est C:\inetpub\wwwroot\Citrix\Roaming\web.config.
2. Recherchez l'élément de compte d'utilisateur dans le fichier (Store est le nom du compte de votre déploiement)

   Par exemple :

   Avant la balise , accédez aux propriétés de ce compte d'utilisateur :

3. Ajoutez la balise de mise à jour automatique après la balise .

auto-update-Check

Cela détermine si Citrix Receiver peut détecter si des mises à jour sont disponibles.

Valeurs possibles :

- Auto : utilisez cette option pour recevoir des notifications lorsque des mises à jour sont disponibles.
- Manual : utilisez cette option pour ne pas recevoir de notifications lorsque des mises à jour sont disponibles. Les utilisateurs doivent rechercher manuellement les mises à jour en sélectionnant **Rechercher les mises à jour**.
- Disabled : utilisez cette option pour désactiver les mises à jour de Citrix Receiver.

auto-update-DeferUpdate-Count

Cela détermine le nombre de fois que les utilisateurs sont notifiés de mettre à niveau avant qu'ils ne soient obligés de mettre à jour vers la dernière version de Citrix Receiver. Par défaut, cette valeur est définie sur 7.

Valeurs possibles :

- -1 : l'utilisateur aura toujours l'option d'être notifié ultérieurement lorsqu'une mise à jour est disponible.
- 0 : l'utilisateur sera forcé de mettre à jour vers la dernière version de Citrix Receiver dès que la mise à jour est disponible.
- Entier positif : l'utilisateur sera notifié ce nombre de fois avant d'être forcé à mettre à jour. Citrix vous recommande ne pas de définir une valeur supérieure à 7.

auto-update-Rollout-Priority

Cela détermine la vitesse à laquelle un appareil verra qu'une mise à jour est disponible.

Valeurs possibles :

- Auto : le système de mise à jour de Citrix Receiver décidera lorsque les mises à jour disponibles sont déployées auprès des utilisateurs.
- Fast : les mises à jour disponibles seront déployées en priorité auprès des utilisateurs comme déterminé par Citrix Receiver.
- Medium : les mises à jour disponibles seront déployées avec une priorité moyenne auprès des utilisateurs comme déterminé par Citrix Receiver.
- Slow : les mises à jour disponibles seront déployées avec une priorité faible auprès des utilisateurs comme déterminé par Citrix Receiver.

Configuration de l'éditeur IME client amélioré à l'aide du fichier de configuration

L'éditeur IME client amélioré dépend de la fonctionnalité de synchronisation de disposition du clavier. Par défaut, la fonctionnalité IME améliorée est activée lorsque la fonctionnalité de synchronisation de la disposition du clavier est activée. Pour contrôler cette fonctionnalité uniquement, ouvrez le fichier **Config** dans le dossier **~/Library/Application Support/Citrix Receiver/**, localisez le paramètre « **EnableIMEEnhancement** » et activez ou désactivez la fonctionnalité en définissant la valeur sur « true » ou « false » respectivement.

Pour plus d'informations sur la configuration sur le VDA, reportez-vous à la section Mappage de clavier Unicode.

Remarque: la modification du paramètre prend effet après le redémarrage de la session.

Synchronisation de la disposition du clavier

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

Pour activer la synchronisation de la disposition du clavier, allez dans **Préférences > Clavier** et sélectionnez « Utiliser la

disposition du clavier local, plutôt que la disposition du clavier du serveur distant ».

Remarque :

1. l'utilisation de l'option de disposition du clavier local active l'éditeur IME (Éditeur de méthode d'entrée) du client. Si les utilisateurs qui travaillent en japonais, chinois simplifié ou coréen préfèrent utiliser l'éditeur IME du serveur, ils doivent désactiver l'option de disposition du clavier local en désélectionnant l'option dans **Préférences > Clavier**. La session va rétablir la disposition du clavier fournie par le serveur distant lorsqu'ils se connectent à la prochaine session.
2. La fonctionnalité ne fonctionne dans la session que lorsque le basculement du client est activé et que la fonctionnalité correspondante est activée sur le VDA. Un élément de menu, « **Utiliser disposition du clavier client** », dans **Périphériques** > **Clavier** > **International** est ajouté pour afficher l'état activé.

Limitations :

- Les dispositions de clavier répertoriées dans « **Configurations de clavier prises en charge sous Mac** » fonctionnent lors de l'utilisation cette fonction. Lorsque vous modifiez la disposition du clavier client sur une disposition non compatible, la disposition peut être synchronisée du côté VDA, mais la fonctionnalité ne peut pas être confirmée.
- Les applications distantes exécutées avec des privilèges élevés (par exemple, des applications exécutées en tant qu'administrateur) ne peuvent pas être synchronisées avec la disposition du clavier de la machine cliente. Pour contourner ce problème, modifiez manuellement la disposition du clavier sur le VDA ou désactivez le contrôle de compte d'utilisateur.
- Lorsque RDP est déployé en tant qu'application et que l'utilisateur travaille au sein d'une session RDP, il n'est pas possible de modifier la disposition du clavier à l'aide du raccourci Alt + Maj. Pour contourner ce problème, les utilisateurs peuvent utiliser la barre de langue dans la session RDP pour changer la disposition du clavier.

Supported keyboard layouts on Mac

Language on Mac	Input source on Mac
English	US.
	U.S. International - PC
	Dvorak
	Dvorak - Left
	Dvorak - Right
	British
	British - PC
	Canadian English
	Australian
	Irish
French	French
	French - Numerical
	Canadian French - CSA
	Swiss French
	French - PC
German	German
	Austrian
	Swiss German
Spanish	Spanish
	Spanish - ISO
Bulgarian	Bulgarian
Swedish	Swedish
Czech	Czech
Danish	Danish
Finnish	Finnish

Hungarian	Hungarian
Italian	Italian
Greek	Greek
Dutch	Belgian
	Dutch
Romanian	Romanian - Standard
Russian	Russian - PC
Croatian	Croatian - PC
Slovak	Slovak
	Slovak - QWERTY
Turkish	Turkish
	Turkish - QWERTY PC
Portuguese	Brazilian
	Brazilian - ABNT2
	Portuguese
Ukrainian	Ukrainian - PC
Belarusian	Belarusian
Slovenian	Slovenian
Estonian	Estonian
Latvian	Latvian
Polish	Polish Pro
Icelandic	Icelandic
Norwegian	Norwegian
Japanese	Hiragana
	Katakana
	Romaji
Korean	2-Set Korean
	3-Set Korean
Chinese, Simplified	
Chinese, Traditional	

Optimisation de votre environnement Citrix Receiver pour Mac

Dec 12, 2017

Vous pouvez optimiser votre environnement Citrix Receiver pour Mac comme suit :

- Reconnexion automatique des utilisateurs
- Redémarrage des bureaux
- Activation de la fiabilité de session
- Mise à disposition de la continuité pour utilisateurs itinérants
- Mappage des machines clientes
- Mappage des lecteurs clients
- Mappage des ports COM clients

Reconnexion automatique des utilisateurs

Les utilisateurs peuvent être déconnectés de leurs sessions en raison d'un manque de fiabilité réseau, de temps d'attente réseau très variables ou de limites des terminaux sans fil. Avec la fonction Reconnexion automatique des clients, Citrix Receiver pour Mac peut détecter les déconnexions de session ICA involontaires et reconnecter automatiquement les utilisateurs à leurs sessions.

Lorsque cette fonctionnalité est activée sur le serveur, les utilisateurs n'ont pas besoin de se reconnecter manuellement pour continuer à travailler. Citrix Receiver pour Mac essaie de reconnecter une session jusqu'à ce que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion. Si l'authentification utilisateur est requise, une boîte de dialogue invitant l'utilisateur à entrer ses informations d'identification s'affiche lors des reconnexions automatiques. Aucune reconnexion automatique n'a lieu lorsqu'un utilisateur quitte une application sans fermer la session.

Vous configurez la fonction Reconnexion automatique des clients à l'aide de paramètres de stratégie sur le serveur. Pour plus d'informations, veuillez consulter la documentation relative à XenApp et XenDesktop.

Redémarrage des bureaux

Les utilisateurs peuvent démarrer un bureau virtuel s'il ne démarre pas, prend trop de temps à se connecter ou devient endommagé. Vous configurez cette fonctionnalité dans XenDesktop.

L'élément **Redémarrer** du menu contextuel est disponible sur tous les bureaux auxquels les utilisateurs ont souscrit et sur la page des applications des utilisateurs. L'élément de menu est désactivé si le redémarrage du bureau n'est pas activé. Lorsque l'utilisateur choisit Redémarrer, Citrix Receiver pour Mac ferme le bureau et le démarre.

> ### Important
>
> faites savoir aux utilisateurs que le redémarrage des bureaux peut entraîner la perte de données.

Activation de la fiabilité de session

Grâce à la fonction de fiabilité de session, les fenêtres d'applications ou de bureaux hébergés sont toujours affichées même si la connexion subit des interruptions. Par exemple, les utilisateurs dotés de connexions sans fil entrant dans un tunnel

peuvent perdre leur connexion à l'entrée d'un tunnel, pour la reprendre à la sortie. Lors de telles interruptions, la fonction de fiabilité de session permet de conserver l'affichage de la fenêtre de session pendant que la restauration de la connexion est en cours.

Vous pouvez configurer votre système pour qu'il affiche une boîte de dialogue d'avertissement informant les utilisateurs lorsque la connexion n'est pas disponible.

Vous configurez la fiabilité de session à l'aide de paramètres de stratégie sur le serveur. Pour de plus amples informations sur l'interaction entre la fiabilité de session et Receiver, reportez-vous à ce document qui explique comment obtenir un service et une fiabilité de qualité supérieure.

Pour obtenir des informations supplémentaires spécifiques aux stratégies, reportez-vous à Paramètres de stratégie Reconnexion automatique des clients et Paramètres de stratégie Fiabilité de session.

Conseil

Les utilisateurs de Citrix Receiver pour Mac ne peuvent pas personnaliser les paramètres de serveur pour la fiabilité de session.

Important

Si la fiabilité de session est activée, le port utilisé par défaut pour les communications de session passe de 1494 à 2598.

Mise à disposition de la continuité pour utilisateurs itinérants

Le contrôle de l'espace de travail permet aux bureaux et 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 bureaux et applications sur chaque machine.

Les stratégies et les mappages de lecteurs clients s'adaptent à la nouvelle machine utilisateur. Ils sont appliqués en fonction de la machine utilisateur sur laquelle la session est en cours. Par exemple, si l'employé d'un centre hospitalier ferme la session qu'il a ouverte sur une machine utilisateur dans la salle des urgences et en ouvre une autre sur une machine dans le Service de radiologie, les stratégies, les mappages d'imprimante et de lecteur client correspondant à la machine utilisateur du Service de radiologie sont appliqués à l'ouverture de session sur cette machine.

Pour configurer les paramètres du contrôle de l'espace de travail

1. Cliquez sur l'icône de la flèche vers le bas dans la fenêtre de Citrix Receiver pour Mac et choisissez **Préférences**.
2. Cliquez sur l'onglet **Général**.
3. Sélectionnez l'une des options suivantes :
   - Reconnecter les applications lorsque je démarre Receiver. Permet aux utilisateurs de se reconnecter aux applications déconnectées lorsqu'ils démarrent Receiver.
   - Reconnecter les applications lorsque je démarre ou que j'actualise des applications. Permet aux utilisateurs de se reconnecter aux applications déconnectées lorsqu'ils démarrent les applications ou lorsqu'ils sélectionnent Actualiser les applications dans le menu de Citrix Receiver menu.

Mappage des machines clientes

Citrix Receiver pour Mac mappe les machines et lecteurs locaux automatiquement de façon à ce qu'ils soient disponibles au sein d'une session. Si le mappage des machines clientes est activé sur le serveur, cela permet à une application ou un bureau distant exécuté sur le serveur d'accéder à des périphériques connectés à la machine utilisateur locale. Vous pouvez :

- accéder aux lecteurs locaux, ports COM et imprimantes ;
- entendre les données audio (sons système et fichiers audio) lues dans la session.

> **Remarque**
>
> Le mappage audio du client et le mappage de l'imprimante cliente ne requièrent aucune configuration sur la machine utilisateur.

Mappage des lecteurs clients

Le mappage des lecteurs clients vous permet d'accéder aux lecteurs locaux de la machine utilisateur, par exemple, les lecteurs de CD-ROM, de DVD et les clés USB durant les sessions. Lorsqu'un serveur est configuré pour permettre le mappage des lecteurs clients, les utilisateurs peuvent accéder à leurs fichiers stockés localement, travailler sur ceux-ci lors de leurs sessions, puis les enregistrer à nouveau sur un lecteur local ou sur un lecteur du serveur.

Citrix Receiver pour Mac contrôle les répertoires dans lesquels les périphériques matériels tels que les CD-ROM, DVD et clés USB sont généralement montés sur la machine utilisateur. Tous les nouveaux répertoires apparaissant au cours d'une session sont automatiquement mappés à la prochaine lettre de lecteur disponible sur le serveur.

Vous pouvez configurer le niveau d'accès en lecture et en écriture des lecteurs mappés à l'aide des Préférences de Citrix Receiver pour Mac.

Pour configurer l'accès en lecture et en écriture des lecteurs mappés

1. Sur la page d'accueil de Citrix Receiver pour Mac, cliquez sur l'icône de la flèche vers le bas et cliquez sur **Préférences**
2. Cliquez sur **Périphériques**.
3. Sélectionnez le niveau d'accès en lecture et en écriture des lecteurs mappés à partir des options suivantes :
   - Lecture et écriture
   - Lecture seule
   - Aucun accès
   - Toujours me demander
4. Fermez toute session ouverte et reconnectez-vous pour appliquer les modifications.

Mappage des ports COM clients

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.

Les ports série Macintosh ne fournissent pas toutes les lignes de signaux utilisées par les applications Windows. Les lignes DSR (Data Set Ready), DCD (Device Carrier Detect), RI (Ring Indicator) et RTS (Request To Send) ne sont pas fournies. Les applications Windows qui dépendent de ces signaux pour la négociation matérielle et le contrôle de flux peuvent ne pas fonctionner. L'implémentation Macintosh de communication série dépend des lignes CTS (Clear To Send) et DTR (Data Terminal Ready) pour la négociation matérielle d'entrée et de sortie uniquement.

Pour mapper des ports COM clients

1. Sur la page d'accueil de Citrix Receiver pour Mac, cliquez sur l'icône de la flèche vers le bas et cliquez sur **Préférences**
2. Cliquez sur **Périphériques**.
3. Sélectionnez le port COM que vous voulez mapper à partir de la liste Ports COM mappés. Il s'agit du port COM virtuel affiché dans la session, et non du port physique de la machine locale.
4. Sélectionnez le périphérique à associer au port COM virtuel à partir du menu déroulant Périphérique.
5. Démarrez Citrix Receiver pour Mac et ouvrez une session sur le serveur.
6. Exécutez une invite de commande. À l'invite, tapez
   net use comx: \\client\comz:

   ou x correspond au numéro de port COM sur le serveur (les ports 1 à 9 peuvent être mappés) et z au numéro du port COM client à mapper (les ports 1 à 4 sont disponibles).

7. Pour confirmer le mappage, tapez net use à l'invite. Une liste des lecteurs mappés, ports LPT et ports COM mappés s'affiche.

Amélioration de l'expérience utilisateur dans Citrix Receiver pour Mac

Dec 12, 2017

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

- CEIP (programme d'amélioration de l'expérience du client)
- Lissage des polices ClearType
- Entrée microphone côté client
- Touches spéciales Windows
- Raccourcis et combinaisons de touches Windows
- Utilisation d'éditeurs (IME) et configurations de clavier international
- Utilisation de moniteurs multiples
- Utilisation de la barre d'outils de bureau

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

Le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) rassemble des données de configuration et d'utilisation anonymes à partir de Citrix Receiver pour Mac et les envoie automatiquement à Citrix. Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de Citrix Receiver pour Mac. Pour plus d'informations, veuillez consulter la section Configuration du programme CEIP.

Lissage des polices ClearType

Le lissage de polices ClearType (également appelé rendu de police subpixellaire) améliore la qualité des polices affichées au-delà de celle disponible au moyen des techniques traditionnelles de lissage de polices ou d'anticrénelage.

Si vous activez le lissage des polices ClearType sur le serveur, vous ne forcez pas les machines utilisateur à l'utiliser également. Vous activez la prise en charge par le serveur du lissage des polices ClearType sur les machines utilisateur sur lesquelles cette fonction est activée localement et qui utilisent Citrix Receiver pour Mac.

Citrix Receiver pour Mac détecte automatiquement le paramètre de lissage des polices de la machine utilisateur et l'envoie au serveur. La session se connecte en utilisant ce paramètre. Lorsque la session est déconnectée ou qu'elle s'arrête, le paramètre du serveur retourne à son réglage initial.

Entrée microphone côté client

Citrix Receiver pour Mac 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.

La fonctionnalité de dictée numérique est disponible avec Citrix Receiver pour Mac. Pour de plus amples informations sur cette fonctionnalité, consultez les informations relatives aux fonctionnalités audio sur le site de documentation sur les produits.

Vous pouvez sélectionner si vous souhaitez utiliser ou non les micros connectés à votre machine utilisateur dans les sessions en choisissant l'une des options suivantes dans l'onglet Mic & Webcam des préférences de Citrix Receiver pour Mac :

- Utiliser mon micro et ma webcam

- Ne pas utiliser mon micro et ma webcam
- Toujours me demander

Si vous sélectionnez **Toujours me demander**, une boîte de dialogue s'affiche chaque fois que vous vous connectez à une application ou un bureau hébergé et vous invite à choisir si vous voulez ou non utiliser votre micro dans la session.

Touches spéciales Windows

Citrix Receiver pour Mac fournit un certain nombre d'options supplémentaires et de méthodes simples destinées à substituer les touches spéciales, telles que les touches de fonction dans les applications Windows, avec des touches Mac. Utilisez l'onglet Clavier pour configurer les options que vous voulez utiliser comme suit :

- « Envoyer le caractère Contrôle avec » vous permet de choisir si vous voulez ou non envoyer la combinaison Commande-touche de caractère en tant que combinaison Ctrl+touche de caractère au sein d'une session. Si vous sélectionnez « Commande ou Contrôle » dans le menu déroulant, cela vous permet d'envoyer des combinaisons Commande-touche de caractère ou Ctrl-touche de caractère sur le Mac en tant que combinaisons Ctrl+touche de caractère sur le PC. Si vous sélectionnez Contrôle, vous devez utiliser les combinaisons Ctrl+touche de caractère.
- « Envoyer le caractère Alt avec » vous permet de choisir comment répliquer la touche Alt au sein d'une session. Si vous sélectionnez Commande-Option, vous pouvez envoyer des combinaisons de touches Commande-Option- telles que Alt+ combinaisons de touches dans une session. Éventuellement, si vous sélectionnez Commande, vous pouvez utiliser la touche Commande en tant que touche Alt.
- « Envoyer la touche Windows à l'aide de la touche Commande (droite) » vous permet d'envoyer la touche Windows sur vos applications et bureaux distants en appuyant sur la touche Commande située sur le côté droit du clavier. Si cette option est désactivée, la touche Commande de droite présente le même comportement que la touche Commande de gauche conformément aux deux paramètres ci-dessus du panneau des préférences, mais vous pouvez toujours envoyer la touche Windows à l'aide du menu Clavier ; choisissez Clavier > Envoyer le raccourci Windows > Démarrer.
- « Envoyer les touches spéciales inchangées » vous permet de désactiver la conversion des touches spéciales. Par exemple, la combinaison Option-1 (sur le clavier numérique) équivaut à la touche spéciale F1. Vous pouvez modifier ce comportement et configurer cette touche spéciale pour représenter 1 (le chiffre un sur le clavier) dans la session en sélectionnant la case « Envoyer les touches spéciales inchangées ». Par défaut, cette case n'est pas sélectionnée donc Option-1 est envoyé à la session en tant que F1.

Vous envoyez les touches de fonction et les touches spéciales vers une session à l'aide du menu Clavier.

Si votre clavier est équipé d'un pavé numérique, vous pouvez également utiliser les touches suivantes :

Touche PC ou action	**Options Mac**
INSÉRER	0 (le chiffre zéro) sur le pavé numérique. Le verrouillage numérique doit être désactivé ; vous pouvez l'activer ou le désactiver à l'aide de la touche Suppr. Option-Aide
SUPPRIMER	Symbole décimal sur le pavé numérique. Le verrouillage numérique doit être désactivé ; vous pouvez l'activer ou le désactiver à l'aide de la touche Suppr. Effacer

Touche PC ou action	Options Mac
F1 à F9	Option-1 à -9 (les chiffres un à neuf) sur le pavé numérique
F10	Option-0 (le chiffre zéro) sur le pavé numérique
F11	Option-signe moins sur le pavé numérique
F12	Option-signe plus sur le pavé numérique

Raccourcis et combinaisons de touches Windows

Les sessions distantes reconnaissent la plupart des combinaisons de clavier Mac utilisées pour l'entrée de texte, telles que Option-G pour saisir le symbole de copyright ©. Cependant, certaines frappes clavier effectuées lors d'une session n'apparaissent pas sur l'application distante ou le bureau distant et sont interprétées au lieu de cela par le système d'exploitation Mac. Cela peut entraîner des réponses des touches Mac.

Vous pouvez également vouloir utiliser certaines touches Windows, telles que Inser, dont beaucoup de claviers Mac ne sont pas équipés. De même, certains raccourcis clavier Windows 8 affichent des icônes et des commandes d'application, et permettent d'ancrer les applications et de basculer entre elles. Ces raccourcis ne sont pas reproduits nativement par les claviers Mac mais peuvent être envoyés à l'application ou au bureau distant à l'aide du menu Clavier.

Les claviers et la façon dont les touches sont configurées peuvent varier considérablement entre machines. C'est la raison pour laquelle Citrix Receiver pour Mac propose plusieurs choix de manière à garantir l'envoi des frappes clavier aux applications et bureaux hébergés. Ces derniers figurent dans le tableau. Le comportement par défaut est décrit. Si vous modifiez les paramètres par défaut (à l'aide de Citrix Receiver pour Mac ou d'autres préférences), différentes combinaisons de frappes clavier peuvent être envoyées et un comportement différent peut être observé sur le PC distant.

> **Important**
>
> certaines combinaisons de touches répertoriées dans le tableau ne sont pas disponibles sur les claviers Mac les plus récents. Dans la plupart des cas, la saisie au clavier peut être envoyée à la session à l'aide du menu Clavier.

Conventions utilisées dans le tableau :

- Les touches alphabétiques sont en majuscule et ne nécessitent pas que vous appuyiez simultanément sur la touche Maj.
- Les traits d'union séparant les combinaisons indiquent que vous devez appuyer simultanément sur les touches (par exemple, Ctrl-C).
- Les touches de caractères sont celles qui créent une entrée de texte. Elles comprennent toutes les lettres, nombres et signes de ponctuation ; les touches spéciales ne créent pas d'entrée mais font office de touches de modification ou de contrôle. Figurent parmi les touches spéciales Ctrl, Alt, Maj, Commande, Option, les touches de direction et les touches de fonction.
- Les instructions de menu font référence aux menus dans la session.
- En fonction de la configuration de la machine utilisateur, il est possible que certaines combinaisons de touches ne fonctionnent pas comme prévu, auquel cas d'autres combinaisons sont répertoriées.
- Fn fait référence à la touche Fn (Fonction) sur un clavier Mac ; la touche de fonction fait référence aux touches F1 à F12

sur un clavier PC ou Mac.

Touche Windows ou combinaison de touches	Équivalents sur Mac
Alt+touche de caractères	Commande–Option–touche de caractères (par exemple pour envoyer Alt-C, utilisez Commande-Option-C)
Alt+touche spéciale	Option–touche spéciale (par exemple Option-Tab) Commande–Option–touche spéciale (par exemple Commande-Option-Tab)
Ctrl+touche de caractères	Commande–touche de caractères (par exemple Commande-C) Contrôle–touche de caractères (par exemple Contrôle-C)
Ctrl+touche spéciale	Contrôle–touche spéciale (par exemple Contrôle-F4) Commande–touche de caractères (par exemple Commande-F4)
Ctrl/Alt/Maj/Windows + touche de fonction	Choisir le clavier > Envoyer une touche de fonction > Contrôle/Alt/Maj/Commande-touche de fonction
Ctrl+Alt	Contrôle-Option-Commande
Ctrl+Alt+Suppr	Contrôle–Option–Suppression avant Contrôle-Option-Fn-Suppr (sur les claviers MacBook) Choisir le clavier > Envoyer Ctrl-Alt-Suppr
Supprimer	Supprimer Choisir le clavier > Envoyer une touche > Supprimer Fn-retour arrière (Fn-Suppr sur certains claviers É-U)
Fin	Fin Fn-Flèche droite
Éch	Éch Choisir le clavier > Envoyer une touche > Échap

F1 à F12	F1 à F12 Choisir le clavier > Envoyer une touche de fonction > F1 à F12
Domicile	Domicile Fn–Flèche gauche
Inser	Choisir le clavier > Envoyer une touche > Insérer
Verr. Num.	Effacer
Pg suiv.	Pg suiv. Fn–Flèche vers le bas
Pg préc.	Pg préc. Fn–Flèche vers le haut
Barre espace	Choisir le clavier > Envoyer une touche > Espace
Onglet	Choisir le clavier > Envoyer une touche > Tab
Logo Windows	Touche de commande droite (préférence de clavier, activée par défaut) Choisir le clavier > Envoyer le raccourci Windows > Démarrer
Combinaison de touches pour afficher les icônes	Choisir le clavier > Envoyer le raccourci Windows > Icônes
Combinaison de touches pour afficher les commandes d'application	Choisir le clavier > Envoyer le raccourci Windows > Commandes d'application
Combinaison de touches pour ancrer les applications	Choisir le clavier > Envoyer le raccourci Windows > Ancrer
Combinaison de touches pour basculer entre les applications	Choisir le clavier > Envoyer le raccourci Windows > Basculer entre les applications

Utilisation d'éditeurs (IME) et configurations de clavier international

Citrix Receiver pour Mac vous permet d'utiliser un éditeur IME sur la machine utilisateur ou le serveur.

Lorsque l'éditeur IME est activé du coté client, les utilisateurs peuvent rédiger du texte au niveau du point d'insertion plutôt que dans une fenêtre distincte.

Citrix Receiver pour Mac permet également aux utilisateurs de spécifier la configuration de clavier qu'ils souhaitent utiliser.

Pour activer l'éditeur IME du coté client

1. À partir de la barre de menu Citrix Viewer, choisissez **Clavier > International > Utiliser l'éditeur IME client**.
2. Assurez-vous que l'éditeur IME côté serveur est configuré pour l'entrée directe ou le mode alphanumérique.
3. Utilisez l'éditeur IME Mac pour rédiger du texte.

Pour indiquer explicitement le point de départ lors de la rédaction de texte

- À partir de la barre de menu Citrix Viewer, choisissez **Clavier > International > Utiliser marques de composition**.

Pour utiliser un éditeur IME du côté serveur

- Assurez-vous que l'éditeur IME du coté client est configuré pour utiliser le mode alphanumérique.

Touches de mode d'entrée IME mappées du côté serveur

Citrix Receiver pour Mac fournit des configurations de clavier pour les touches de mode d'entrée IME Windows côté serveur qui ne sont pas disponibles sur les claviers Mac. Sur les claviers Mac, la touche Option est mappée sur les touches de mode d'entrée IME côté serveur suivantes, en fonction des paramètres régionaux du côté serveur :

Paramètres régionaux du système côté serveur	Touche de mode d'entrée IME côté serveur
Japonais	**Touche Kanji** (Alt + Hankaku/Zenkaku sur le clavier japonais)
Coréen	**Touche Alt droite** (bascule entre Hangul/anglais sur le clavier coréen)

Pour utiliser des configurations de clavier international

- Assurez-vous que les configurations de clavier du coté client et serveur utilisent les mêmes paramètres régionaux que ceux de la langue d'entrée par défaut du côté serveur.

Utilisation de moniteurs multiples

Les utilisateurs peuvent définir Receiver pour Mac afin de travailler en mode plein écran sur plusieurs moniteurs via l'option de menu **Utiliser tous les écrans en mode plein écran**.

Limitations connues

Le mode plein écran est uniquement pris en charge sur un seul écran ou tous les écrans, ce qui est configurable via un élément de menu.

Utilisation de la barre d'outils de bureau

Les utilisateurs peuvent maintenant accéder à la barre d'outils en mode fenêtre et plein écran. Auparavant, la barre d'outils était uniquement visible en mode plein écran. Modifications apportées à la barre d'outils :

- Le bouton **Accueil** a été supprimé de la barre d'outils. Cette fonction peut être exécutée à l'aide de l'une des commandes suivantes :
  - Cmd-Tab pour basculer vers l'application active précédente.

- Ctrl-Flèche gauche pour revenir à l'espace précédent.
- Utilisation du trackpad intégré ou des gestes Magic Mouse pour basculer vers un espace différent.
- Le déplacement du curseur sur le bord de l'écran en mode plein écran affiche un Dock à partir duquel vous pouvez choisir les applications à activer.

- Le bouton **Fenêtré** a été supprimé de la barre d'outils. Vous pouvez basculer du mode plein écran au mode fenêtré à l'aide de l'une des méthodes suivantes :
  - Sur OS X 10.10, en cliquant sur le bouton de fenêtre vert sur la barre du menu déroulant.  ou 
  - Sur OS X 10.9, en cliquant sur le bouton de menu bleu sur la barre du menu déroulant. 
  - Pour toutes les versions de OS X, en sélectionnant **Quitter le mode plein écran** dans le menu **Afficher** de la barre du menu déroulant.
- Le comportement de glissement de la barre d'outils a été mis à jour pour prendre en charge le glissement entre fenêtres en plein écran avec de multiples moniteurs.

Sécurisation des communications de Citrix Receiver pour Mac

Dec 12, 2017

Cette section explique comment sécuriser les communications dans Citrix Receiver pour Mac.

Pour sécuriser les communications entre votre batterie de serveurs et Citrix Receiver pour Mac, vous pouvez intégrer vos connexions à la batterie de serveurs grâce à un large choix de technologies de sécurité, y compris Citrix NetScaler Gateway. Pour obtenir des informations sur la configuration de la sécurité avec Citrix StoreFront, reportez-vous à la documentation de StoreFront.

> **Remarque**
>
> Citrix recommande d'utiliser NetScaler Gateway pour sécuriser les communications entre les serveurs StoreFront et les machines des utilisateurs.

- Un serveur proxy SOCKS ou serveur proxy sécurisé (également appelé serveur proxy ou 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 Citrix Receiver et les serveurs. Citrix Receiver pour Mac prend en charge les protocoles de proxy SOCKS et de proxy sécurisé.
- Secure Gateway. Vous pouvez utiliser Secure Gateway avec l'Interface Web pour fournir un point d'accès Internet unique, sécurisé et crypté aux serveurs des réseaux d'entreprise internes.
- Solutions de relais SSL avec protocoles TLS
- Un pare-feu. Les pare-feu de réseau peuvent autoriser ou empêcher le passage des paquets de données en fonction de l'adresse et du port de destination. Si vous utilisez Citrix Receiver pour Mac 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.

À propos des certificats

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 de façon à pouvoir accéder aux ressources Citrix à l'aide de Citrix Receiver pour Mac.

> **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 se lancent pas.

Importation de certificats racine sur des machines Receiver pour Mac

Obtenez le certificat racine auprès de l'émetteur du certificat et envoyez-le par e-mail à un configuré sur votre appareil. Lorsque vous cliquez sur la pièce jointe, vous êtes invité à importer le certificat racine.

Certificats génériques

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

Certificats intermédiaires avec NetScaler Gateway

Si votre chaîne de certificat contient un certificat intermédiaire, ce dernier doit être mappé vers le certificat serveur de NetScaler Gateway. Pour de plus amples informations sur cette tâche, reportez-vous à la documentation NetScaler Gateway. Pour plus d'informations sur l'installation et la liaison d'un certificat intermédiaire avec une autorité de certification principale sur un boîtier NetScaler Gateway, reportez-vous à l'article How to Install and Link Intermediate Certificate with Primary CA on NetScaler Gateway.

Stratégie de validation des certificats de serveur

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

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

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

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

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

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

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

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

Important

Certaines autorités de certification disposent de plus d'un certificat racine. Si vous avez besoin de cette validation plus stricte, assurez-vous que votre configuration utilise le certificat racine approprié. Par exemple, il existe actuellement deux certificats (« DigiCert »/« GTE CyberTrust Global Root » et « DigiCert Baltimore Root »/« Baltimore CyberTrust Root ») qui peuvent valider les mêmes certificats de serveur. Sur certaines machines utilisateur, les deux certificats racine sont disponibles. Sur les autres machines, seul (« DigiCert Baltimore Root »/« Baltimore CyberTrust Root ») est disponible. Si vous configurez « GTE CyberTrust Global Root » sur la passerelle, les connexions Citrix Receiver pour Mac sur ces machines utilisateur échouent. Consultez la documentation de l'autorité de certification pour déterminer quel certificat racine doit être utilisé. Notez également que les certificats racine expirent éventuellement, comme tous les certificats.

Remarque

Certains serveurs et certaines passerelles n'envoient jamais le certificat racine, même si cela est configuré. Une validation plus stricte n'est par conséquent pas possible.

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

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

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

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

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

Un navigateur Web peut ignorer le certificat racine incorrect. Toutefois, Citrix Receiver pour Mac n'ignore pas le certificat

racine incorrect et la connexion échoue.

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

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

Important

Certaines autorités de certification utilisent un certificat intermédiaire avec signature croisée. Ce cas de figure est destiné aux situations dans lesquelles il existe plus d'un certificat racine, et qu'un certificat racine antérieur est toujours en cours d'utilisation en même temps qu'un certificat racine plus récent. Dans ce cas, il y aura au moins deux certificats intermédiaires. Par exemple, le certificat racine antérieur « Class 3 Public Primary Certification Authority » et le certificat intermédiaire avec signature croisée « VeriSign Class 3 Public Primary Certification Authority - G5 » correspondant. Toutefois, un certificat racine antérieur « VeriSign Class 3 Public Primary Certification Authority - G5 » correspondant est également disponible, et il remplace « Class 3 Public Primary Certification Authority ». Le certificat racine antérieur n'utilise pas de certificat intermédiaire avec signature croisée.

Remarque

Le certificat intermédiaire avec signature croisée et le certificat racine ont le même nom de sujet (Émis pour), mais le certificat intermédiaire avec signature croisée a un nom d'émetteur différent (Émis par). Cela permet de différencier le certificat intermédiaire avec signature croisée d'un certificat intermédiaire ordinaire (tel « Certificat intermédiaire exemple 2 »).

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

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

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

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »
- « Certificat intermédiaire avec signature croisée exemple » [non recommandé]

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

- « Certificat de serveur exemple »

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

Connexion via NetScaler Gateway

Pour permettre aux utilisateurs distants de se connecter à votre déploiement XenMobile via NetScaler Gateway, vous

pouvez configurer ces derniers de manière à fonctionner avec StoreFront. La méthode que vous allez choisir pour autoriser l'accès dépend de l'édition de XenMobile dans votre déploiement.

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

Pour de plus amples informations sur la configuration de ces connexions avec NetScaler Gateway, consultez la documentation Intégration avec NetScaler et NetScaler Gateway.

Connexion avec la passerelle Secure Gateway

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

Vous pouvez utiliser la passerelle Secure Gateway en mode Normal ou en mode Relais afin de fournir un canal sécurisé de communication entre Citrix Receiver pour Mac et le serveur. Il n'est pas nécessaire de configurer Citrix Receiver pour Mac si vous utilisez la passerelle Secure Gateway en mode Normal et si les utilisateurs se connectent via l'Interface Web.

Citrix Receiver pour Mac utilise les paramètres configurés à distance sur le serveur Interface Web pour se connecter aux serveurs exécutant Secure Gateway. Pour plus d'informations sur la configuration des paramètres de serveur proxy pour Citrix Receiver pour Mac, veuillez consulter la documentation de l'Interface Web.

Si le proxy Secure Gateway est installé sur un serveur dans le réseau sécurisé, vous pouvez l'utiliser en mode Relais. Pour plus d'informations sur le mode Relais, veuillez consulter la documentation relative à XenApp et Secure Gateway.

Si vous utilisez le mode Relais, le serveur Secure Gateway fonctionne comme un serveur proxy. Dans ce cas, vous devez configurer Citrix Receiver pour Mac 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.exemple.com est un nom de domaine complet car il liste dans l'ordre un nom d'hôte (mon_ordinateur), un domaine intermédiaire (exemple) et un domaine de tête (com). La combinaison du domaine intermédiaire et du domaine de tête (exemple.com) est généralement appelée nom de domaine.

Connexion via un serveur proxy

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

Lorsqu'il communique avec le serveur XenApp ou XenDesktop, Citrix Receiver pour Mac utilise les paramètres de serveur proxy configurés à distance sur le serveur Interface Web. Pour plus d'informations sur la configuration des paramètres de serveur proxy pour Receiver, veuillez consulter la documentation de l'Interface Web.

Lors la communication avec le serveur Web, Citrix Receiver pour Mac utilise les paramètres de serveur proxy configurés pour le navigateur Web par défaut sur la machine utilisateur. Vous devez configurer les paramètres du serveur proxy pour le

navigateur Web par défaut sur la machine utilisateur.

Connexion via 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 un pare-feu dans votre déploiement, Citrix Receiver pour Mac 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 Citrix Receiver pour Mac. Citrix Receiver pour Mac 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.

Connexion à l’aide de TLS

Citrix Receiver pour Mac 12.3 prend en charge TLS 1.0, 1.1 et 1.2 avec les suites de chiffrement suivantes pour les connexions TLS à XenApp/XenDesktop :

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- 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

Remarque : Citrix Receiver pour Mac exécuté sur macOS Sierra ne prend pas en charge les suites de chiffrement TLS suivantes :

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

TLS (Transport Layer Security) est la dernière version normalisée du protocole TSL. Le groupe de travail Internet Engineering Taskforce (IETF) l'a rebaptisé TLS lorsqu'il est devenu responsable du développement de TLS 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, notamment des organisations gouvernementales américaines, requièrent l'utilisation du protocole TLS pour la sécurisation de leurs communications de données. Ces organisations peuvent également exiger l’utilisation d’une cryptographie éprouvée, telle que FIPS 140. La norme FIPS 140 est une norme de cryptographie.

Citrix Receiver pour Mac prend en charge les clés RSA de longueur 1024, 2048 et 3072. Les certificats racine avec des clés RSA de longueur de 4 096 bits sont aussi pris en charge.

Pour obtenir des informations sur la configuration et l'utilisation du Relais SSL en vue de sécuriser l'installation, veuillez

consulter la documentation de XenDesktop.

> **Remarque**
>
> Citrix Receiver pour Mac utilise le cryptage de plate-forme (OS X) pour les connexions entre Citrix Receiver pour Mac et StoreFront.

Configuration et activation de Citrix Receiver pour Mac pour TLS

Deux étapes principales permettent de configurer TLS :

1. Configurez le Relais SSL sur votre serveur XenApp ou XenDesktop et sur votre serveur Interface Web, procurez-vous le certificat serveur approprié et installez-le. Pour plus d'informations, veuillez consulter la documentation relative à XenApp et à l'Interface Web.
2. Installez le certificat racine équivalent sur la machine utilisateur.

Installation de certificats racine sur des machines utilisateur

Pour utiliser TLS afin de sécuriser les communications entre un Citrix Receiver pour Mac 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.

Mac OS X est fourni avec environ 100 certificats racine déjà installés, mais vous pouvez utiliser un autre certificat. Il vous suffit de vous le procurer à partir d'une autorité de certification et de l'installer sur chaque machine.

En fonction des procédures de sécurité de votre entreprise, vous pouvez soit installer le certificat racine sur chaque machine utilisateur, soit demander aux utilisateurs de l'installer eux-mêmes. Le choix le plus sûr et le plus facile consiste à ajouter des certificats racine au trousseau Mac OS X.

Pour ajouter un certificat racine au trousseau

1. Double-cliquez sur le fichier contenant le certificat. Cela démarre automatiquement l'application Trousseau d'accès.
2. Dans la boîte de dialogue Ajouter des certificats, choisissez l'une des options suivantes dans le menu déroulant Trousseau d'accès :
   - session (le certificat ne s'applique qu'à l'utilisateur actuel)
   - Système (le certificat s'applique à tous les utilisateurs d'une machine)
3. Cliquez sur OK.
4. Tapez votre mot de passe dans la boîte de dialogue S'authentifier et cliquez sur OK.

Le certificat racine est installé et peut être utilisé par des clients TLS et par toute autre application utilisant TLS.

À propos des stratégies TLS

Cette section fournit des informations sur la configuration des stratégies de sécurité pour les sessions ICA via TLS dans Citrix Receiver pour Mac. Vous pouvez configurer certains paramètres TLS utilisés pour les connexions ICA dans Citrix Receiver pour Mac. Ces paramètres ne sont pas exposés dans l'interface utilisateur ; pour les modifier, vous devez exécuter une commande sur l'appareil exécutant Citrix Receiver pour Mac.

> **Remarque**
>
> D'autres moyens permettent de gérer les stratégies TLS, tels que lorsque les appareils sont contrôlés par un serveur OS X ou une autre solution de gestion des appareils mobiles.

Les stratégies TLS comprennent les paramètres suivants :

SecurityComplianceMode. Définit le mode de conformité aux exigences de sécurité pour la stratégie. Si vous ne configurez pas SecurityComplianceMode, FIPS est utilisé en tant que valeur par défaut. Les valeurs applicables pour ce paramètre sont les suivantes :

- **Aucune**. Aucun mode de conformité n'est appliqué
- **FIPS**. Les modules cryptographiques FIPS sont utilisés
- **SP800-52**. La norme NIST SP800-52r1 est appliquée

Paramètre SecurityComplianceMode vers SP800-52 : COPIER

```
defaults write com.citrix.receiver.nomas SecurityComplianceMode SP800-52
```

SecurityAllowedTLSVersions. Ce paramètre spécifie les versions du protocole TLS qui doivent être acceptées durant la négociation du protocole. Ces informations sont représentées dans un tableau et toute combinaison des valeurs possibles est prise en charge. Lorsque ce paramètre n'est pas configuré, les valeurs TLS10, TLS11 et TLS12 sont utilisées comme les valeurs par défaut. Les valeurs applicables pour ce paramètre sont les suivantes :

- **TLS10**. Spécifie que le protocole TLS 1.0 est autorisé.
- **TLS11**. Spécifie que le protocole TLS 1.1 est autorisé.
- **TLS12**. Spécifie que le protocole TLS 1.2 est autorisé.

Paramètre SecurityAllowedTLSVersions vers TLS 1.1 et TLS 1.2 : COPIER

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array TLS11 TLS12
```

SSLCertificateRevocationCheckPolicy. Cette fonctionnalité améliore l'authentification cryptographique du serveur Citrix et la sécurité globale des connexions SSL/TLS entre un client et un serveur. Ce paramètre régit la façon dont une autorité de certification racine approuvée est traitée lors d'une tentative d'ouverture d'une session distante via SSL lors de l'utilisation du client pour OS X.

Lorsque vous activez ce paramètre, le client vérifie si le certificat du serveur est révoqué ou non. Il existe plusieurs niveaux de vérification des listes de révocation de certificats. Par exemple, le client peut être configuré pour vérifier uniquement sa liste de certificats locaux ou pour vérifier les listes de certificats locaux et de réseau. En outre, la vérification des certificats peut

être configurée pour autoriser les utilisateurs à se connecter uniquement si toutes les listes de révocation de certificats ont été vérifiées.

La vérification de la liste de révocation de certificats (CRL) est une fonctionnalité avancée prise en charge par certains émetteurs de certificats. Elle permet à un administrateur de révoquer des certificats de sécurité (invalidés avant leur date d'expiration) dans le cas où la clé privée du certificat est corrompue, ou simplement en cas de changement inattendu du nom DNS.

Les valeurs applicables pour ce paramètre sont les suivantes :

- **NoCheck**. La liste de révocation de certificats n'est pas vérifiée.
- **CheckWithNoNetworkAccess**. La liste de révocation de certificats est vérifiée. Seuls les magasins de la liste de révocation de certificats locaux sont utilisés. Tous les points de distribution sont ignorés. L'utilisation d'une liste de révocation de certificats n'est pas indispensable à la vérification du certificat serveur présenté par le serveur Relais SSL/Secure Gateway cible.
- **FullAccessCheck**. La liste de révocation de certificats est vérifiée. Les magasins locaux de la liste de révocation de certificats et tous les points de distribution sont utilisés. L'utilisation d'une liste de révocation de certificats n'est pas indispensable à la vérification du certificat serveur présenté par le serveur Relais SSL/Secure Gateway cible.
- **FullAccessCheckAndCRLRequired**. La liste de révocation de certificats est vérifiée, à l'exception de l'autorité de certification racine. Les magasins locaux de la liste de révocation de certificats et tous les points de distribution sont utilisés. L'utilisation de toutes les listes de révocation de certificats requises est essentielle à la vérification.
- **FullAccessCheckAndCRLRequiredAll**. La liste de révocation de certificats est vérifiée, y compris l'autorité de certification racine. Les magasins locaux de la liste de révocation de certificats et tous les points de distribution sont utilisés. L'utilisation de toutes les listes de révocation de certificats requises est essentielle à la vérification.

> ### Remarque
>
> Si vous ne configurez pas SSLCertificateRevocationCheckPolicy, FullAccessCheck est utilisé comme valeur par défaut.

Définition de SSLCertificateRevocationCheckPolicy sur FullAccessCheckAndCRLRequred : COPIER

```
defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy FullAccessCheckAndCRLRequired
```

Configuration de stratégies TLS

Pour configurer les paramètres TLS sur un ordinateur non géré, exécutez la commande **defaults** dans Terminal.app.

defaults est une application de ligne de commande que vous pouvez utiliser pour ajouter, modifier et supprimer des paramètres d'application dans un fichier plist de préférences OS X.

Pour modifier les paramètres :

1. Ouvrez Applications > Utilitaires > Terminal.

2. Dans Terminal, exécutez la commande :

defaults write com.citrix.receiver.nomas

Où :

: nom du paramètre décrit ci-dessus.

: commutateur identifiant le type de paramètre, -string ou -array. Si le type de paramètre est une chaîne, vous pouvez l'ignorer.

: valeur du paramètre. Si la valeur est un tableau et que vous spécifiez de multiples valeurs, les valeurs doivent être séparées par un espace.

Par exemple : COPIER

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array TLS11 TLS12
```

Rétablissement de la configuration par défaut

Pour rétablir la valeur par défaut d'un paramètre :

1. Ouvrez Applications > Utilitaires > Terminal.
2. Dans Terminal, exécutez la commande :

defaults delete com.citrix.receiver.nomas

Où :

: nom du paramètre décrit ci-dessus.

Par exemple : COPIER

```
defaults delete com.citrix.receiver.nomas SecurityAllowedTLSVersions
```

Utilisation de l'interface utilisateur pour configurer les paramètres de sécurité

De nombreuses améliorations diverses et liées à la sécurité ont été introduites dans la version 12.3 de Citrix Receiver pour Mac, notamment :

- Interface utilisateur de configuration de la sécurité améliorée. Dans les versions précédentes, la ligne de commande était la méthode préférée pour apporter des modifications à la sécurité ; les paramètres de configuration liés à la sécurité de la session sont maintenant simples et accessibles depuis l'interface, ce qui améliore l'expérience utilisateur tout en créant une méthode d'adoption des préférences homogène en matière de sécurité.

- Connexions TLS. Citrix Receiver pour Mac vous permet de vérifier les connexions établies à des serveurs qui utilisent une version de TLS spécifique, et d'obtenir des informations supplémentaires, notamment l'algorithme de cryptage utilisé pour la connexion, le mode, la taille de clé et si SecureICA est activé. Par ailleurs, vous pouvez afficher le certificat de serveur pour les connexions TLS.

L'écran **Sécurité et confidentialité** amélioré contient les nouvelles options suivantes dans l'onglet **TLS** :

- Définir le mode de conformité
- Configurer le module cryptographique
- Sélectionner la version de TLS appropriée
- Sélectionner la liste de révocation de certificats
- Activer les paramètres pour toutes les connexions TLS

L'image ci-dessous illustre les paramètres Sécurité et confidentialité accessibles depuis l'interface :