À propos de Citrix Receiver pour Mac 12.0

Jun 22, 2016

Citrix Receiver pour Mac permet aux utilisateurs d'accéder en libre-service aux ressources publiées sur des serveurs XenApp ou XenDesktop. Receiver 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.

Nouveautés dans la version 12.1

Authentification par carte à puce à NetScaler

Cette fonctionnalité permet à Citrix Receiver d'accéder à des applications et bureaux via NetScaler Gateway à l'aide de l'authentification par carte à puce. Consultez la section Configuration requise pour l'authentification par carte à puce pour de plus amples informations sur cette fonctionnalité.

Prise en charge de l'écran partagé dans El Capitan

Dans la version précédente de Citrix Receiver pour Mac (12.0), nous avons introduit la prise en charge de OS X El Capitan. Dans cette version, la fonctionnalité d'écran partagé de El Capitan est entièrement prise en charge.

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

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

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

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

> ### Remarque
>
> Cette fonctionnalité fournit un paramètre de gestion des sessions supplémentaire dans XenApp et XenDesktop, **TransportReconnectRetryMaxTimeSeconds**.
>
> **TransportReconnectDelay** et **TransportReconnectRetries** ne sont plus utilisés. Pour plus d'informations, veuillez consulter la section Gestion des sessions.

Fonctionnalités introduites dans la version 12.0

Lorsqu'elle est utilisée en conjonction avec les capacités de personnalisation et de valorisation de la marque centralisées de StoreFront 3.0, cette version de Receiver pour Mac permet aux utilisateurs de bénéficier d'une expérience de sélection d'applications et de bureaux gérée de manière centralisée depuis StoreFront. Il s'agit de la même expérience utilisateur que celle offerte par les Receiver de bureau Windows et les Receiver Web HTML5 et Chrome lorsqu'ils sont associés à

StoreFront 3.0.

Prise en charge de OS X El Capitan (10.11).

Prise en charge des cookies de session : Citrix Receiver pour Mac 12.0 prend en charge les cookies de session Web afin d'utiliser la nouvelle API Web requise pour StoreFront 3.0 et pour prendre en charge l'équilibrage de charge.

Améliorations apportées au fuseau : Citrix Receiver pour Mac 12.0 détecte de façon plus précise les fuseaux horaires locaux et de villes lorsqu'il est utilisé avec la redirection du fuseau horaire de XenApp. Pour plus d'informations veuillez consulter la section : Paramètres de stratégie Contrôle des fuseaux horaires.

Problèmes résolus dans Citrix Receiver pour Mac 12

Feb 22, 2016

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 résolus dans Citrix Receiver pour Mac 12,1

- 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 12.1.100

- 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 connexions IPV6 à NetScaler Gateway échouaient. [LC4512]
- 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 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 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 connus avec Citrix Receiver pour Mac 12

Jul 07, 2016

Problèmes connus avec Citrix Receiver pour Mac 12

Les problèmes connus suivants ont été observés dans cette version :

- Sur OS X El Capitan (10.11), les applications et les bureaux virtuels ne s'affichent pas correctement en vue fractionnée. [#582397]
- La session XenDesktop ne se lance pas lors de l'utilisation d'une authentification par carte à puce. [#550781]
- Lors de l'utilisation d'une carte à puce PIV, Receiver ne peut pas se reconnecter à une session XenDesktop 5.6. [#550986]
- 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]
- 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]
- 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]
- 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]
- 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]
- 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]
- 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]
- 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]
- 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]
- 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.

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]

Configuration système requise pour Citrix Receiver pour Mac 12.0

Oct 31, 2016

Systèmes d'exploitation pris en charge pour Citrix Receiver pour Mac 12.0

- OS X El Capitan (10.11)
- OS X Yosemite (10.10)
- OS X Mavericks (10.9)
- OS X Mountain Lion (10.8)

Les versions OS X antérieures à Mountain Lion ne sont pas prises en charge.

Si vous avez besoin d'une version de Citrix Receiver pour Mac OS X Lion (10.7) ou version antérieure, consultez la section Citrix Receiver pour Mac 11.9.x.

Configuration matérielle requise

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

Serveurs pris en charge

- XenApp (l'un des produits suivants) :
  - Citrix XenApp 7.6 pour Windows Server 2012 R2
  - Citrix XenApp 7.5 pour Windows Server 2012 R2
  - Citrix XenApp 6.5 pour Windows Server 2008 R2
- XenDesktop (l'un des produits suivants) :
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7
- Citrix VDI-in-a-Box 5.4 et 5.3
- StoreFront :
  - StoreFront 3.0
  - StoreFront 2.6
  - StoreFront 2.5
  - StoreFront 2.1
- 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 Receiver plutôt que d'un navigateur Web
- Pour déployer Receiver :
  - Citrix Receiver pour Web 2.1, 2.5 et 2.6
  - Interface Web Citrix 5.4

Navigateurs pris en charge

- Safari 6.0 ou version ultérieure

- Mozilla Firefox 22.x ou version ultérieure
- Google Chrome 28.x ou version ultérieure

Connectivité

Si vos utilisateurs exécutent Citrix Receiver pour Mac 12 sur OS X El Capitan et qu'ils rencontrent des problèmes de connexion, ils devront peut-être mettre à niveau leur NetScaler Gateway Plugin. Pour de plus amples informations, consultez l'article suivant sur la page des téléchargements de Citrix : NetScaler Gateway Plug-in v3.1.4 pour Mac OS X (prise en charge de El Capitan).

Citrix Receiver prend en charge les connexions HTTP, HTTPS et ICA-over-TLS à XenApp ou XenDesktop par le biais des configurations suivantes.

Pour les connexions LAN :

- StoreFront utilisant StoreFront Services ou des sites Receiver pour Web
- Interface Web 5.4 pour Windows utilisant des sites XenApp Services

Pour les connexions sécurisées à distance ou locales :

- Citrix NetScaler Gateway 11.0 avec VPX
- Citrix NetScaler Gateway 10.5 avec VPX
- Citrix NetScaler Gateway 10.1 avec VPX
- Citrix Access Gateway édition Enterprise 10.x avec VPX
- Citrix Access Gateway édition Enterprise 9.x avec VPX
- Citrix Access Gateway VPX
- Citrix Secure Gateway 3.x (pour utilisation avec l'Interface Web uniquement)

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

Authentification

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

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

Deux facteurs (domaine avec jeton de sécurité) SMS	**Receiver pour Web à l'aide de navigateurs**	**Site StoreFront Services (natif)**	**Site StoreFront XenApp Services (natif)**	Oui* **NetScaler sur Receiver pour Web (navigateur)** Oui*	Oui* **NetScaler sur site StoreFront Services (natif)** Oui*
Cartes à puce**	Oui	Oui		Oui*	Oui*
Certificat utilisateur				Oui (NetScaler Gateway Plugin)	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 pouvoir utiliser des cartes à puce sur OS X 10.10, OS X 10.10.2 ou supérieur doit être installé.

Pour les connexions à l'Interface Web 5.4, Receiver 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	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.

**Les cartes à puce ne sont pas prises en charge par OS X 10.10 en raison d'une modification par Apple de la prise en charge des cartes à puce.

Pour de plus amples informations sur l'authentification, reportez-vous à la documentation NetScaler Gateway ou Access Gateway et à la documentation Produit de Citrix. Pour de plus amples informations sur les autres méthodes d'authentification prises en charge par l'Interface Web, reportez-vous à la rubrique Configuration de l'authentification pour l'Interface Web dans la documentation Produit de Citrix.

Configuration requise pour l'authentification par carte à puce

Nov 13, 2015

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 XenDesktop 5.6 et version supérieure ou XenApp 6.5 et version supérieure à l'aide d'un accès par navigateur.
- 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 : 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.
- Dans des sessions double-hop : si un double-hop est requis, une connexion supplémentaire est établie entre Receiver et le bureau virtuel de l'utilisateur.

  Les déploiements qui prennent en charge le double-hop sont décrits dans la documentation XenApp et XenDesktop. Pour plus d'informations, veuillez consulter la section Déploiements de carte à puce.

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 vous invite à sélectionner un certificat. Après sélection d'un certificat, Citrix Receiver 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 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

À l'aide des options de configuration avancées disponibles dans la fenêtre Préférences de Citrix Receiver, vous pouvez spécifier le module PKCS#11 à utiliser pour l'authentification :

1. Dans Citrix Receiver, sélectionnez **Préférences**.
2. Dans la fenêtre Préférences, cliquez sur **Avancé**.
3. 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.
4. Après avoir sélectionné le module approprié, cliquez sur **Ajouter**.

Lecteurs, middleware et cartes à puce pris en charge

Receiver pour Mac prend en charge la plupart des lecteurs de carte à puce et middleware cryptographiques compatibles avec Mac OS X. 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

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

Restrictions

- Les certificats doivent être stockés sur une carte à puce et non sur la machine utilisateur.
- Receiver pour Mac n'enregistre pas le certificat choisi par l'utilisateur.
- 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.
- 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 unique à StoreFront avec NetScaler Gateway Plug-in n'est pas disponible pour les utilisateurs de cartes à puce.

Informations supplémentaires

Voir :

- Configuration de Citrix XenDesktop 7.6 et NetScaler Gateway 10.5 avec l'authentification par carte à puce PIV (PDF)
- 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 suppression de Receiver pour Mac

Oct 31, 2016

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, Access Gateway et Secure Gateway.

Dans cet article :

Installation

Receiver peut être installé de l'une des manières suivantes :

- Par un utilisateur à partir de Citrix.com
  - Un utilisateur qui utilise Receiver pour la première fois et qui obtient Receiver à partir de Citrix.com ou depuis votre propre site de téléchargement peut créer un compte en entrant une adresse e-mail à la place d'une adresse URL de serveur. Receiver 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 Receiver sur sa machine.
  - La découverte de compte basée sur l'adresse e-mail pour un nouvel utilisateur ne s'applique pas si Receiver est téléchargé à partir d'un emplacement autre que Citrix.com (tel qu'un site Receiver pour Web).
  - Si votre site nécessite la configuration de Receiver, utilisez une autre méthode de déploiement.
- Automatiquement à partir de Receiver pour Web où de l'Interface Web
  - Un utilisateur qui utilise Receiver 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 Receiver pour la première fois doit entrer l'adresse URL d'un serveur pour créer un compte.

Installation manuelle de Receiver pour Mac

Les utilisateurs peuvent installer Receiver 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 Receiver pour Mac

1. Téléchargez le fichier .dmg correspondant à la version de Receiver 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 vers Receiver pour Mac 12.0

Les mises à niveau sont prises en charge à partir des versions 10.x et 11.x de Online Plug-in pour Mac. Vous pouvez également mettre à niveau à partir des versions 11.3, 11.4, 11.5, 11.6, 11.7.x, 11.8.x et 11.9.x de Receiver pour Mac.

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 Receiver pour Mac

Pour les déploiements avec StoreFront :

- Il est recommandé de configurer NetScaler Gateway et StoreFront 2.x comme décrit dans la documentation relative à ces produits dans la documentation Produit de Citrix. Joignez le fichier de provisioning créé par StoreFront à un e-mail et indiquez aux utilisateurs comment mettre à niveau et ouvrir le fichier de provisioning après l'installation de Receiver.
- Si vous ne souhaitez pas utiliser le fichier de provisioning, demandez aux utilisateurs d'entrer l'adresse URL 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 Receiver, 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 11.9 et faites savoir à vos utilisateurs comment mettre à niveau Receiver. 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 Receiver.

Déploiement de Receiver à partir de Receiver pour Web

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

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

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

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

Vous pouvez également mettre des légendes d'installation à la disposition des utilisateurs. Il s'agit de liens qui sont présentés aux utilisateurs dans l'écran Messages. Il leur suffit de cliquer sur ces liens pour démarrer le processus de détection et de déploiement de client. Vous pouvez également utiliser des légendes d'installation pour permettre aux utilisateurs

d'accéder au processus de détection et de déploiement de client afin de mettre à niveau leurs clients Citrix.

Pour utiliser le processus de détection et de déploiement de client, les fichiers d'installation de Receiver doivent être disponibles sur le serveur Interface Web. Par défaut, l'Interface Web suppose que les noms de fichiers des fichiers d'installation de Receiver sont les mêmes que ceux des fichiers fournis sur le support d'installation de XenApp ou XenDesktop. Si vous téléchargez Receiver depuis le site Web Citrix ou que vous prévoyez de déployer des versions antérieures de Receiver, vérifiez que les noms des fichiers d'installation de Receiver appropriés sont spécifiés pour le paramètre ClientIcaMac dans les fichiers de configuration de vos sites XenApp Web.

Pour plus d'informations, veuillez consulter la documentation relative à l'Interface Web.

Suppression de Receiver pour Mac

Vous pouvez désinstaller Receiver 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 Receiver pour Mac

Nov 13, 2015

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

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

Configurer la mise à disposition d'applications

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

Mode d'accès Web

Sans aucune configuration, 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 Receiver ou de configurer 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 Receiver. Cette expérience enrichie est similaire à celle que propose un magasin d'applications mobiles. En mode libre-service, vous pouvez configurer des paramètres de mots-clés pour les applications sélectionnées, auto-provisionnées et obligatoires selon vos besoins. Lorsque l'un de vos utilisateurs sélectionne une application, un raccourci de l'application est placé dans le dossier Applications sur sa machine.

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

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

Configurer le mode libre-service

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

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 saisissez lorsque vous publiez 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 Receiver, ajoutez la chaîne KEYWORDS:Featured à la description de l'application.

Pour plus d'informations, veuillez consulter la documentation de 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. Créez des magasins qui énumèrent et regroupent les bureaux et applications des sites XenDesktop et des batteries XenApp, tout en mettant ces ressources à la disposition des utilisateurs.

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

   Remarque : pour les administrateurs soucieux d'exercer un contrôle plus rigoureux, Citrix fournit un modèle que vous pouvez utiliser pour créer un site de téléchargement pour Receiver.
2. Configurez des magasins pour CloudGateway comme vous le feriez pour toute autre application XenApp ou XenDesktop. Aucune configuration spéciale n'est nécessaire pour Receiver. 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 Receiver 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

Receiver. Receiver identifie le serveur NetScaler Gateway, Access Gateway ou StoreFront associé à l'adresse e-mail en se basant sur les enregistrements SRV de DNS et invite les utilisateurs à ouvrir une session pour accéder à leurs applications 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 ou Access Gateway afin d'accepter les connexions utilisateur à l'aide d'une adresse e-mail pour découvrir l'adresse URL de NetScaler Gateway, StoreFront ou d'Access Gateway, consultez la section *— Connexion à StoreFront à l'aide de la découverte basée sur l'adresse e-mail* dans la documentation NetScaler Gateway ou Access 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 Receiver, il leur suffit d'ouvrir le fichier pour configurer Receiver. Si vous configurez des sites Receiver pour Web, les utilisateurs peuvent également obtenir les fichiers de provisioning à partir de ces sites.

Pour plus d'informations, veuillez consulter la documentation de 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 Receiver 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 l'accès à l'aide de NetScaler Gateway ou d'Access Gateway, l'adresse de NetScaler Gateway ou d'Access Gateway, l'édition du produit et la méthode d'authentification requise
  Pour de plus amples informations sur la configuration de NetScaler Gateway ou d'Access Gateway, consultez la documentation NetScaler Gateway ou Access Gateway.

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

Optimisation de votre environnement Receiver pour Mac

Nov 13, 2015

Pour tirer le meilleur de Receiver, vous pouvez optimiser votre environnement comme suit :

- Reconnexion automatique des utilisateurs
- Mise à disposition de la fiabilité de session HDX Broadcast
- Mise à disposition de la continuité pour utilisateurs itinérants
- mappant les machines clientes ;

Reconnexion des utilisateurs

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 HDX Broadcast - Reconnexion automatique des clients, Receiver 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. Receiver 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 HDX Broadcast - 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, Receiver ferme le bureau et le démarre.

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

Mise à disposition de la fiabilité de session HDX Broadcast

Grâce à la fonction de fiabilité de session HDX Broadcast, 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 HDX Broadcast à l'aide de paramètres de stratégie sur le serveur. Pour plus d'informations, veuillez consulter la documentation relative à XenDesktop et XenApp.

Les utilisateurs Receiver ne peuvent pas personnaliser ces réglages.

Important : si la fiabilité de session HDX Broadcast est activée, le port par défaut utilisé pour les communications 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 Receiver 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.

mappant les machines clientes ;

Receiver 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.

Veuillez noter que 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.

Receiver 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 Receiver.

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

1. Sur la page d'accueil de Receiver, 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 autre mappage réseau Toujours me demander.

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 Receiver, 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 Receiver et ouvrez une session sur le serveur.
6. Exécutez une invite de commande. À l'invite, tapez
   net use comx: \\client\comz:

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

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

Amélioration de l'expérience utilisateur dans Receiver pour Mac

Nov 13, 2015

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

- 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

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 Receiver.

Receiver 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

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

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

La fonctionnalité de dictée numérique est disponible avec Receiver. Pour de plus amples informations sur cette fonctionnalité, veuillez consulter la documentation relative à XenApp et XenDesktop.

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 Receiver :

- 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

Receiver 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. Suppr
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

Touche PC ou action	Options Mac

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 Receiver 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 Receiver 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)

Touche Windows ou combinaison de touches	Équivalents sur Mac
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
Échap.	Échap Choisir le clavier > Envoyer une touche > Échap
F1 à F12	F1 à F12 Choisir le clavier > Envoyer une touche de fonction > F1 à F12
Home	Home Fn–Flèche gauche
Insérer	Choisir le clavier > Envoyer une touche > Insérer
Verr. Num.	Suppr

Page suivante

Touche Windows ou combinaison de touches	Equivalents sur Mac
Page suivante	Fn–Flèche vers le bas
Page haut	Page haut Fn–Flèche vers le haut
Barre espace	Choisir le clavier > Envoyer une touche > Espace
Onglets	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

Receiver 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.

Receiver 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

Receiver 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 10.7, 10.8 et 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 Receiver

Mar 03, 2016

Dans cet article :

Pour sécuriser les communications entre votre batterie de serveurs et Receiver, vous pouvez intégrer vos connexions Citrix Receiver à la batterie de serveurs grâce à un large choix de technologies de sécurité, dont :

- Citrix NetScaler Gateway ou Citrix Access Gateway. Pour obtenir des informations sur la configuration de ces derniers avec 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 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 Receiver avec un pare-feu de réseau qui mappe l'adresse IP interne du serveur sur une adresse Internet externe (c'est-à-dire, la traduction d'adresse de réseau, ou NAT), configurez l'adresse externe.

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

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

Certificats intermédiaires avec Access Gateway ou NetScaler Gateway

Si votre chaîne de certificat contient un certificat intermédiaire, ce dernier doit être mappé au certificat du serveur Access Gateway ou NetScaler Gateway. Pour de plus amples informations sur cette tâche, reportez-vous à la documentation NetScaler Gateway. Pour obtenir des informations équivalentes sur Access Gateway, reportez-vous à l'article de la base de connaissances qui correspond à l'édition de votre produit :

CTX114146 : comment installer un certificat intermédiaire sur Access Gateway édition Enterprise

Connexion avec NetScaler Gateway ou Access Gateway édition Enterprise

Pour permettre aux utilisateurs distants de se connecter à votre déploiement CloudGateway via NetScaler Gateway ou Access Gateway, vous pouvez configurer ces derniers de manière à fonctionner avec StoreFront (un composant de CloudGateway). La méthode que vous allez choisir pour autoriser l'accès dépend de l'édition de CloudGateway dans votre déploiement.

Si vous déployez CloudGateway Express dans votre réseau, autorisez les connexions des utilisateurs internes ou distants à StoreFront via NetScaler Gateway ou Access Gateway en intégrant NetScaler Gateway ou Access 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, reportez-vous à la section Configuration des paramètres NetScaler Gateway avec l'assistant d'accès à distance. Pour de plus amples informations sur la configuration de ces connexions avec Access Gateway, reportez-vous à la section Intégration d'Access Gateway avec CloudGateway.

Pour permettre aux utilisateurs distants de se connecter via Access Gateway à votre déploiement Interface Web, configurez Access Gateway de manière à fonctionner avec l'Interface Web, comme décrit dans la section Configuration d'Access Gateway édition Enterprise pour communiquer avec l'Interface Web et ses sous-rubriques.

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

Receiver utilise 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 Receiver, 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 (Secure Gateway).

Si vous utilisez le mode Relais, le serveur Secure Gateway fonctionne comme un serveur proxy. Dans ce cas, vous devez configurer Receiver pour qu'il utilise :

- le nom de domaine complet du serveur Citrix Secure Gateway ;
- le numéro de port du serveur Citrix Secure Gateway. Veuillez noter que le mode Relais n'est pas pris en charge par Secure Gateway, version 2.0.

Le nom de domaine complet (FQDN) doit contenir, dans l'ordre, les trois composants suivants :
- Nom d'hôte
- domaine intermédiaire ;
- domaine de tête.

Par exemple : mon_ordinateur.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 Receiver et les serveurs. Receiver prend en charge les protocoles de proxy SOCKS et de proxy sécurisé.

Lorsqu'il communique avec le serveur XenApp ou XenDesktop, Receiver 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, Receiver 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, Receiver doit pouvoir communiquer via le pare-feu avec le serveur Web et le serveur Citrix. Le pare-feu doit permettre le trafic HTTP (généralement via le port http 80 ou 443 si un serveur Web sécurisé est utilisé) pour les communications entre la machine utilisateur et le serveur Web. Pour les communications entre Receiver et le serveur Citrix , le pare-feu doit autoriser le trafic ICA entrant sur les ports1494 et 2598.

Si le pare-feu est configuré pour la traduction des adresses réseau, vous pouvez vous servir de l'Interface Web pour définir les mappages depuis les adresses internes vers les adresses externes et les ports. Par exemple, si votre serveur XenApp ou XenDesktop n'est pas configuré avec une adresse secondaire, vous pouvez configurer l'Interface Web pour qu'elle fournisse une adresse secondaire à Receiver. Receiver se connecte ensuite au serveur à l'aide de l'adresse externe et du numéro de port. Pour plus d'informations, veuillez consulter la documentation relative à l'Interface Web.

Connexion avec le Relais SSL

Vous pouvez intégrer Receiver au service Relais SSL avec Receiver pour Mac 12.0, qui prend en charge TLS 1.0, 1.1 et 1.2 avec les suites de chiffrement suivantes pour les connexions TLS entre Citrix Receiver et 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

TLS (Transport Layer Security) est la dernière version normalisée du protocole SSL. Le groupe de travail Internet Engineering Taskforce (IETF) l'a rebaptisé TLS lorsqu'il est devenu responsable du développement de SSL sous la forme d'une norme ouverte.

TLS garantit la sécurité des communications de données grâce à l'authentification des serveurs, au cryptage du flux de données et aux contrôles d'intégrité des messages. Certaines organisations, telles que les organisations gouvernementales américaines requièrent l'utilisation du protocole TLS pour sécuriser les communications de données. Ces organisations peuvent également exiger l'utilisation d'une cryptographie éprouvée, telle que FIPS 140. La norme FIPS 140 est une norme de cryptographie.

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

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

- Entre un Receiver et un serveur sur lesquels TLS est activé.
- Avec un serveur exécutant l'Interface Web, entre le serveur XenApp et le serveur Web.

Pour obtenir des informations sur la configuration et l'utilisation du Relais SSL pour sécuriser votre installation ou la configuration du serveur Interface Web afin d'utiliser le cryptage TLS, consultez la documentation XenApp et Interface Web.

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

Configuration et activation de Receiver 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 Receiver sur lequel TLS est activé et la batterie de serveurs, vous avez besoin d'un certificat racine sur la machine utilisateur afin de vérifier la signature de l'autorité de certification sur le certificat de serveur.

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 SSL et par toute autre application utilisant SSL.

À propos des stratégies SSL

Cette section fournit des informations sur la configuration des stratégies de sécurité pour les sessions ICA via SSL dans Citrix Receiver pour Mac version 12.0. Vous pouvez configurer certains paramètres SSL utilisés pour les connexions ICA dans Citrix Receiver. Ces paramètres ne sont pas exposés dans l'interface utilisateur ; pour les modifier, vous devez exécuter une commande sur l'appareil exécutant Receiver.

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

Les stratégies SSL 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 :

- **None**. 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 des stratégies SSL

Pour configurer les paramètres SSL 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

Dans cette formule :

: 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

Dans cette formule :

: nom du paramètre décrit ci-dessus.

Par exemple : COPIER

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