Application Citrix Workspace pour Mac

Contents

À propos de cette version

April 12, 2021

> **Important**
>
> À partir de macOS Catalina, Apple impose des exigences supplémentaires pour les certificats d'autorité de certification racines et les certificats intermédiaires que les administrateurs doivent configurer. Pour plus d'informations, consultez l'article HT210176 du support Apple.

Nouveautés dans la version 2104

L'application Citrix Workspace pour Mac prend en charge la connexion utilisateur manuelle aux partages réseau, sauf si l'authentification unique est activée par votre organisation. Pour accéder aux emplacements réseau partagés, ouvrez l'application Citrix Workspace, accédez à **Fichiers** > **Partages réseau** et entrez vos informations d'identification. Pour plus d'informations sur la configuration des partages réseau, consultez Créer et gérer des connecteurs StorageZone.

Nouveautés dans la version 2102

Cette version résout plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Nouveautés dans la version 2101

Prise en charge de Apple silicon (puce M1)

L'application Citrix Workspace pour Mac prend désormais en charge les appareils Apple silicon (puce M1) utilisant Rosetta 2 sur macOS Big Sur (11.0 et versions ultérieures). Par conséquent, tous les canaux virtuels tiers doivent utiliser Rosetta 2. Sinon, ces canaux virtuels pourraient ne pas fonctionner dans l'application Citrix Workspace pour Mac sur macOS Big Sur (11.0 et versions ultérieures). Pour plus d'informations sur Rosetta, consultez article de l'assistance Apple.

Prise en charge de l'optimisation de Microsoft Teams pour les sessions d'applications transparentes

L'application Citrix Workspace pour Mac prend désormais en charge l'optimisation de Microsoft Teams pour les sessions d'applications transparentes. Par conséquent, vous pouvez lancer Microsoft Teams en tant qu'application à partir de l'application Workspace. Pour plus d'informations, consultez les sections suivantes :

- Optimisation pour Microsoft Teams
- Redirection Microsoft Teams

Prise en charge de DTMF (Dual Tone Multi Frequency) avec Microsoft Teams

L'application Citrix Workspace pour Mac prend désormais en charge l'interaction de signalisation DTMF avec les systèmes de téléphonie (par exemple, RTPC) et les téléconférences dans Microsoft Teams. Par défaut, cette fonction est activée.

Nouveautés dans la version 2012

Prise en charge de Apple silicon (puce M1) en preview

L'application Citrix Workspace pour Mac prend désormais en charge les périphériques Apple silicon (puce M1) en preview.

Optimisation du partage d'écran avec Microsoft Teams

L'application Citrix Workspace pour Mac prend désormais en charge l'optimisation du partage d'écran avec Microsoft Teams. Pour plus d'informations, consultez les rubriques suivantes :

- Optimisation pour Microsoft Teams
- Redirection Microsoft Teams

Amélioration des performances

Cette version résout plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Nouveautés dans la version 2010

Amélioration de l'authentification

Pour offrir une expérience transparente, la boîte de dialogue d'authentification s'affiche désormais dans l'application Citrix Workspace. Les détails du magasin s'affichent sur l'écran d'ouverture de session. Les jetons d'authentification sont chiffrés et stockés de sorte que vous n'avez pas besoin de saisir à nouveau les informations d'identification en cas de redémarrage du système ou de redémarrage de session.

> **Remarque :**
>
> Cette amélioration de l'authentification ne s'applique qu'aux déploiements dans le cloud.

Prise en charge de macOS Big Sur

L'application Citrix Workspace pour Mac est prise en charge sur macOS Big Sur (11.0.1).

Amélioration des performances

Cette version résout plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Nouveautés dans la version 2009

Optimisation pour Microsoft Teams (Preview)

Optimisation pour Microsoft Teams à l'aide de l'application Citrix Workspace et de Citrix Virtual Apps and Desktops. L'optimisation pour Microsoft Teams est similaire à l'optimisation HDX RealTime pour Microsoft Skype Entreprise. La différence est que nous regroupons tous les composants nécessaires à l'optimisation pour Microsoft Teams dans le VDA et l'application Workspace pour Linux. L'application Citrix Workspace pour Mac prend en charge l'audio et la vidéo avec l'optimisation Microsoft Teams.

Pour plus d'informations, consultez les rubriques suivantes :

- Optimisation pour Microsoft Teams
- Redirection Microsoft Teams
- Problèmes connus

Application Citrix Workspace pour Mac sous macOS Big Sur bêta

L'application Citrix Workspace 2009 pour Mac a été testée sur macOS Big Sur bêta 8. Veuillez utiliser cette configuration dans un environnement de test et nous faire part de vos commentaires. Consultez la section Problèmes connus pour connaître les problèmes spécifiques à macOS Big Sur bêta.

> **Attention :**
>
> N'utilisez pas l'application Citrix Workspace pour Mac sur les versions macOS Big Sur bêta dans des environnements de production.

Extensions du noyau pour la redirection USB

L'application Citrix Workspace 2009 pour Mac ne dépend plus des extensions du noyau (KEXT) pour la redirection USB.

Nouveautés dans la version 2008

Amélioration des performances

Cette version résout plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Prise en charge des versions macOS

L'application Citrix Workspace 2008 pour Mac est la dernière version qui prend en charge les versions macOS High Sierra (10.13) et Mojave (10.14).

Nouveautés dans 2007

Amélioration des performances

Cette version résout plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Nouveautés de la version 2006

Mise à jour de Citrix Analytics Service

L'application Citrix Workspace est conçue pour transmettre en toute sécurité des données à Citrix Analytics Service à partir de sessions ICA que vous lancez depuis un navigateur. Pour plus d'informations sur la façon dont Citrix Analytics utilise ces informations, consultez Recherche en libre-service des performances et Recherche en libre-service pour Virtual Apps and Desktops.

Prise en charge de H.264 pour la redirection de webcam

L'application Citrix Workspace pour Mac prend désormais en charge la norme de compression vidéo H.264 (également appelée MPEG-4 AVC). Par conséquent, les applications 64 bits publiées peuvent désormais utiliser la redirection de webcam.

Améliorations apportées à la stabilité

Cette version résout un certain nombre de problèmes afin d'améliorer la stabilité générale.

Nouveautés dans la version 2005

Langues prises en charge

L'application Citrix Workspace pour Mac est désormais disponible en italien.

Amélioration des performances

- Cette version résout plusieurs problèmes afin d'améliorer la stabilité et les performances générales sur Citrix Workspace (magasins Cloud).
- Avec cette version, les utilisateurs du cloud observeront des temps d'ouverture de session et d'énumération des applications plus courts.

Nouveautés dans la version 2002

Clés de longueur 4096 bits en mode FIPS

L'application Citrix Workspace pour Mac prend désormais en charge les clés RSA d'une longueur de 4096 bits en mode de cryptographie FIPS 140.

Amélioration des performances

Cette version résout plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Nouveautés dans la version 2001

Protection des applications

L'application Citrix Workspace pour Mac prend désormais en charge la protection des applications. La protection des applications est une fonctionnalité complémentaire qui offre une sécurité renforcée lors de l'utilisation de Citrix Virtual Apps and Desktops. Elle limite le risque d'être infecté par des programmes malveillants d'enregistrement de frappe et de capture d'écran. La protection des applications empêche l'exfiltration d'informations confidentielles telles que les informations d'identification de l'utilisateur et les informations sensibles affichées à l'écran. Cette fonctionnalité empêche les utilisateurs et les attaquants de prendre des captures d'écran et d'utiliser des enregistreurs de frappe pour récupérer et exploiter des informations sensibles. Pour plus d'informations sur la configuration de la protection des applications sur Citrix Virtual Apps and Desktops, reportez-vous à la section Protection des applications.

Problèmes connus et limitations :

Pour que cette fonctionnalité fonctionne correctement, désactivez la stratégie **Redirection du Presse-papiers client** sur le VDA.

Langues prises en charge

L'application Citrix Workspace pour Mac est désormais disponible en portugais (Brésil).

Chargement des canaux virtuels tiers amélioré

L'application Citrix Workspace pour Mac offre désormais un meilleur chargement des canaux virtuels tiers. Cela améliore l'expérience utilisateur des manières suivantes :

- Les canaux virtuels tiers (par exemple, RealTime Media Engine) n'ont pas besoin d'être réinstallés lorsque vous désinstallez, puis réinstallez l'application Citrix Workspace.
- Les utilisateurs disposant de privilèges de compte standard peuvent également bénéficier d'une expérience optimisée du Pack d'optimisation HDX RealTime même lorsque leur RealTime Media Engine a été installé par un administrateur.

Nouveautés dans la version 1912

Workspace avec intelligence

Cette version de l'application Citrix Workspace pour Mac est optimisée pour profiter des futures fonctionnalités intelligentes au moment de leur publication. Pour de plus amples informations, consultez la section Fonctionnalités de Workspace Intelligence - Micro-apps.

Nouveautés dans la version 1910.2

Cette version résout les problèmes liés aux mises à jour de Citrix Workspace et macOS Catalina.

- Les clients utilisant l'application Citrix Workspace 1910 et 1910.1 pour Mac doivent effectuer une mise à niveau vers l'application Citrix Workspace pour Mac 1910.2 manuellement pour recevoir les futures mises à jour via la mise à jour automatique de Citrix Workspace.
- Les clients utilisant l'application Citrix Workspace 1906 pour Mac ou version antérieure peuvent obtenir l'application l'application Citrix Workspace 1910.2 pour Mac via les mises à jour de Citrix Workspace.

Nouveautés dans la version 1910.1

Cette version résout plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Nouveautés dans la version 1910

Prise en charge de macOS Catalina

L'application Citrix Workspace pour Mac est prise en charge sur macOS Catalina.

> **Remarque :**
>
> Lors de l'ouverture de l'application Citrix Workspace pour Mac et Citrix Viewer pour la première fois sur macOS Catalina, le système d'exploitation invite les utilisateurs à autoriser les notifications de Citrix Viewer. Cliquez sur **Autoriser** pour recevoir des notifications relatives à l'application Citrix Workspace pour Mac.

Mise à jour des suites de chiffrement

Les suites de chiffrement suivantes sont déconseillées pour une sécurité renforcée :

- Suites de chiffrement avec le préfixe « TLS_RSA_* »
- Suites de chiffrement RC4 et 3DES
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

L'application Citrix Workspace pour Mac ne prend en charge que les suites de chiffrement suivantes :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Pour les utilisateurs DTLS 1.0, l'application Citrix Workspace pour Mac 1910 ne prend en charge que la suite de chiffrement suivante :

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Citrix vous recommande de mettre à niveau votre version de NetScaler vers la version 12.1 ou ultérieure si vous souhaitez utiliser DTLS 1.0. Sinon, le protocole TLS sera utilisé conformément à la stratégie DDC. Pour plus d'informations, consultez l'article CTX250104 du centre de connaissances.

Mises à jour de Citrix Casting

Citrix Casting se déconnecte désormais automatiquement lorsque les utilisateurs ferment le capot de l'ordinateur portable.

Nouveautés dans la version 1906

Mises à jour de Citrix Casting

Contrôlez votre session sur le Citrix Ready Workspace Hub à l'aide de périphériques. Vous pouvez désormais utiliser le clavier et la souris sur le hub et le périphérique pour gérer la session. Pour de plus amples informations, consultez la section Citrix Ready Workspace Hub.

Langues prises en charge

L'application Citrix Workspace pour Mac est désormais disponible en néerlandais.

Nouveautés dans la version 1903.1

Mises à jour de Citrix Casting

Citrix Casting a été mis à jour avec de nouvelles fonctionnalités et améliorations. Pour plus d'informations sur Citrix Casting, consultez Citrix Casting.

Nouveautés dans la version 1901

Cette version résout plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Nouveautés dans la version 1812

Citrix Casting

Citrix Casting est utilisé pour diffuser votre écran Mac sur des appareils Citrix Ready Workspace Hub à proximité. Dans cette version, la mise en miroir de votre écran Mac sur des moniteurs connectés à Workspace Hub est prise en charge.

Pour plus d'informations sur Citrix Casting, consultez Configurer Citrix Casting.

Synchronisation de la disposition du clavier

À compter de cette version, l'application Citrix Workspace pour Mac fournit une synchronisation dynamique de la disposition du clavier depuis la machine cliente vers un VDA Linux dans une session. Cela vous permet de basculer entre leurs dispositions de clavier préférées sur la machine cliente, ce qui offre une expérience utilisateur cohérente, par exemple, lors du changement de la disposition du clavier de l'anglais vers l'espagnol.

Pour de plus amples informations sur la configuration de la disposition du clavier, consultez la section Configuration du clavier. Pour de plus amples informations sur la configuration de la synchronisation de la disposition du clavier sur les VDA Linux, consultez la section Synchronisation dynamique de la disposition du clavier.

Expérience de l'éditeur IME client amélioré

À partir de cette version, l'application Citrix Workspace pour Mac offre une meilleure expérience utilisateur avec les entrées IME client et les VDA Linux. Grâce à cette fonctionnalité, vous pouvez voir deux améliorations dans les entrées IME client :

- La fenêtre candidate contenant la liste des caractères de composition apparaît toujours à côté du point d'insertion plutôt que dans le coin inférieur gauche précédent.
- Les caractères composés affichés dans le VDA sont marqués de sorte que vous ne les confondez pas avec les caractères déterminés.

Cette fonctionnalité dépend de la fonction de synchronisation de la disposition du clavier.

Pour plus d'informations sur la configuration de cette amélioration de l'éditeur IME client, consultez la section Éditeur IME client amélioré. Pour plus d'informations sur la configuration de l'éditeur IME client sur un VDA Linux, consultez la section Synchronisation de l'interface utilisateur de l'éditeur IME client.

H264 sélectif

Le mode H264 sélectif permet de recevoir des parties de l'écran qui changent rapidement, par exemple lors de la lecture d'une vidéo, sous forme de flux H264. Pour activer le H264 sélectif, définissez la stratégie **Utiliser codec vidéo pour la compression** sur **Pour les zones changeant constamment**.

Nouveautés dans la version 1809

Prise en charge de macOS Mojave

L'application Citrix Workspace pour Mac prend entièrement en charge macOS Mojave, y compris le Dark Mode (thème sombre).

Prise en charge de WebApp

Secure Browser pour l'application Citrix Workspace pour Mac prend désormais en charge les cookies et les redirections lors de l'utilisation de Citrix Gateway.

Nouveautés dans la version 1808

Prise en charge 64 bits

L'application Citrix Workspace pour Mac est entièrement compatible 64 bits.

> **Remarque :**
>
> Les utilisateurs qui mettent à niveau vers l'application Citrix Workspace ne bénéficieront pas d'une expérience Skype Entreprise (Lync) optimisée en raison d'une incompatibilité de bits. L'application Citrix Workspace pour Mac est une version 64 bits, tandis que la version actuellement installée de RTME est une version 32 bits. En guise de solution de contournement, envisagez d'utiliser la version préliminaire de RTME.
>
> **Remarque :**
>
> Les canaux virtuels personnalisés 32 bits ne fonctionnent plus et doivent être mis à jour en 64 bits.

Authentification fédérée

L'application Citrix Workspace pour Mac prend désormais en charge l'authentification fédérée via Azure Active Directory.

Affichage ou masquage de la barre de langue distante

À partir de cette version, vous pouvez choisir d'afficher ou de masquer la barre de langue distante dans une session d'application à l'aide de l'interface utilisateur graphique. La barre de langue affiche la langue d'entrée préférée dans une session. Dans les versions antérieures, vous pouvez modifier ce paramètre en utilisant uniquement les clés de registre du VDA. À partir de l'application Citrix Workspace pour Mac version 1808, vous pouvez modifier les paramètres à l'aide de la boîte de dialogue **Préférences**. La barre de langue apparaît dans une session par défaut.

Pour plus d'informations, consultez la section Configuration et l'article CTX231913 du centre de connaissances.

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

Prise en charge de Citrix Analytics

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

Problèmes résolus

Problèmes résolus dans la version 2104

Cette version résout également plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus dans la version 2102

Cette version résout également plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus dans la version 2101

- Les tentatives d'ouverture d'une réunion Microsoft Teams à l'aide de OWA (Outlook Web App) peuvent échouer, entraînant la fermeture inattendue de toutes les fenêtres associées. [CTXBR-1175]
- Lorsque vous démarrez un appel vidéo, Microsoft Teams peut ne pas répondre et afficher une erreur `Citrix HDX not connected`. [RFMAC-6727]
- Sous macOS Big Sur (11.0.1), les tentatives de connexion de périphériques USB peuvent échouer, entraînant la fermeture inattendue de la session. [RFMAC-7079]

- Dans un bureau publié, les fichiers enregistrés sur votre appareil Mac local peuvent afficher une date de création de fichier du 30 novembre 1979 au lieu de la date actuelle. [CVADHELP-16309]
- Il peut arriver que l'écran d'ouverture de session dans les applications publiées ne s'affiche pas correctement, ce qui se traduit par une taille de fenêtre réduite et un arrière-plan rouge. [CVADHELP-16027]
- Les appels audio peuvent se déconnecter de votre côté lorsque vous déconnectez et connectez des périphériques audio. [RFMAC-7371]
- Les tentatives de copie de texte à partir d'applications Office 365 peuvent réussir même lorsque la stratégie de restriction du Presse-papiers est activée. [CTXBR-1166]
- Les tentatives de lancement de Microsoft Teams peuvent échouer en raison de problèmes avec le moteur HDX RealTime Connector et le message d'erreur suivant s'affiche.

  ```
  Sorry, we couldn't connect you
  ```

  [CVADHELP-16432]

Problèmes résolus dans la version 2012

- Lors de l'utilisation de l'application Citrix Workspace pour Mac 2008 ou version ultérieure, les tentatives de lancement de plusieurs instances d'une application publiée peuvent échouer. [CVADHELP-16019]
- Les tentatives de lancement de la redirection USB générique peuvent échouer lorsque vous utilisez une station d'accueil USB. [RFMAC-6687]
- Les tentatives d'ouverture d'une fenêtre à l'aide de CTRL+O dans les bureaux publiés peuvent entraîner l'ouverture de deux fenêtres. [CVADHELP-15747]
- Lors de l'utilisation de l'application Citrix Workspace pour Mac sur macOS Big Sur bêta, les appels audio peuvent se déconnecter. Le problème se produit lorsque vous déconnectez des périphériques audio et connectez d'autres périphériques audio lors d'un appel audio. [RFMAC-6112]
- Le moteur HDX RealTime Connector peut se fermer de manière inattendue lorsque vous allumez et éteignez la caméra dans Microsoft Teams. [RFMAC-6293]
- Les tentatives de lancement de Citrix Files à partir de l'application Workspace pour Mac peuvent échouer en raison de problèmes avec l'authentification unique. [RFMAC-4477]

Problèmes résolus dans la version 2010

- Les tentatives de lancement d'applications ou de bureaux publiés peuvent échouer et afficher un message d'erreur. Le problème se produit si votre nom d'ordinateur contient des caractères spéciaux. [CVADHELP-15492]

- Les tentatives de connexion aux applications publiées et aux sessions de bureau peuvent échouer. Le problème se produit lorsque vous utilisez une souris pour cliquer sur **OK** pour vous connecter. [CVADHELP-15300]

Problèmes résolus dans la version 2009

Cette version résout également plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus dans la version 2008

Si vous ajoutez le contrat de licence de l'utilisateur final aux VDA, les tentatives de lancement de bureaux publiés peuvent entraîner un écran gris ou noir. [CVADHELP-14986]

Problèmes résolus dans 2007

- Lorsqu'un utilisateur active EDT (Enlightened Data Transport) sur Citrix Gateway, des problèmes dans les paramètres audio du client peuvent entraîner la fermeture inattendue de l'application Citrix Workspace pour Mac. [CVADHELP-14686]
- Lorsque le SDK Intel est utilisé sur des VDA dont la stratégie **Utiliser codec vidéo pour la compression** est activée, les tentatives de lancement de bureaux publiés peuvent entraîner un écran vert. [CVADHELP-13647]
- Les tentatives d'obtention des données de latence WMI (Windows Management Instrumentation) peuvent échouer dans l'application Citrix Workspace pour Mac versions 2002 et 2005. [RFMAC-4325]

Problèmes résolus dans la version 2006

- Les tentatives de connexion à l'application Citrix Workspace pour Mac peuvent échouer, affichant une interface utilisateur non apparentée. Pour contourner le problème, cliquez sur **Actualiser applications** dans le menu pour charger le magasin. [RFMAC-4063]

Problèmes résolus dans la version 2005

- Les tentatives de connexion à l'application Citrix Workspace sur macOS Catalina à l'aide de cartes à puce PIV peuvent échouer, affichant le message d'erreur suivant : « Impossible de détecter le compte spécifié. » [CVADHELP-14155]
- Parfois, la fenêtre principale d'une instance publiée de Microsoft Outlook peut devenir noire lorsque sa fenêtre modale a le focus. [CVADHELP-14169]

Problèmes résolus dans la version 2002

- Les tentatives de lancement d'une session dans l'application Citrix Workspace sur macOS Catalina (10.15.2) à l'aide de cartes à puce PIV peuvent échouer, affichant le message d'erreur suivant : « Un ou plusieurs certificats racine ne sont pas valides. » [RFMAC-3365]
- Les tentatives de saisie dans des applications publiées (telles que le Bloc-notes, etc.) dont la langue est définie sur le chinois ou le japonais peuvent échouer. [RFMAC-3556]

Problèmes résolus dans la version 2001

- Lorsque la stratégie de profondeur de couleurs maximale de 16 bpp est activée sur un MacBook, les tentatives de lancement de bureaux publiés peuvent afficher un écran gris et la session peut cesser de répondre. [CVADHELP-13605]
- Les tentatives de collage de captures d'écran prises dans l'application DingTalk dans des instances publiées de Microsoft Paint et Microsoft Word peuvent échouer, affichant respectivement un écran vide ou un message d'erreur. [CVADHELP-13938]

Problèmes résolus dans la version 1912

- Lorsque vous utilisez l'application Citrix Workspace pour Mac versions 1812 ou 1901, les tentatives de déplacement d'applications publiées sur l'écran sont lentes. [RFMAC-2300]
- Les tentatives de connexion à l'application Citrix Workspace sur macOS Catalina à l'aide de cartes à puce PIV peuvent échouer. [RFMAC-2788]
- Lorsque vous utilisez l'application Citrix Workspace pour Mac version 1909, l'ouverture d'un fichier .ICA avec des noms non anglais peut entraîner la fermeture inattendue de Citrix Viewer. [RFMAC-2986]
- Les tentatives de lancement d'applications Microsoft Outlook et PowerShell publiées ne répondent pas ou sont lentes après la mise à niveau de l'application Citrix Workspace pour Mac. [LD1192]
- Les fenêtres des applications publiées ne sont pas mises à jour ou prennent beaucoup de temps à s'actualiser lorsque vous les déplacez sur l'écran. [LD1485]

Problèmes résolus dans la version 1910.2

Cette version résout également plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus dans la version 1910.1

- Lorsque vous utilisez un MacBook Pro 2018 et versions ultérieures et FaceTime, les utilisateurs peuvent voir une barre verte en bas de l'aperçu vidéo. [RFMAC-2317]
- Le lancement d'une session avec une carte à puce via Citrix Gateway peut échouer, affichant le message d'erreur « Le pair SSL distant a envoyé une alerte d'échec de négociation ». [RFMAC-2727]
- Lorsque l'authentification SAML est activée, l'écran d'authentification peut être lent ou ne pas répondre. Pour contourner le problème, redémarrez l'appareil. [RFMAC-3047]
- Le refus d'autoriser l'automatisation après le lancement d'applications auxquelles vous êtes abonné peut entraîner le blocage de l'application Citrix Workspace pour Mac. [RFMAC-3048]

Problèmes résolus dans la version 1910

- La copie de texte depuis l'application Citrix Workspace pour Mac vers une autre application peut afficher des caractères incorrects. [RFMAC-2581]
- La connexion à l'application Citrix Workspace pour Mac peut prendre plus de temps que prévu. [RFMAC-2608]
- L'utilisation d'un proxy pour se connecter peut entraîner la fermeture inattendue du proxy. [RFMAC-2612]
- Les mouvements de la souris peuvent être désynchronisés dans les applications transparentes lors de l'utilisation de plusieurs moniteurs. [RFMAC-2623]
- La reconnexion à l'application Citrix Workspace pour Mac peut entraîner la fermeture inattendue de l'application. [RFMAC-2679]
- Lorsque vous utilisez le raccourci Commande-onglet pour changer d'onglet, le bureau virtuel cesse de répondre. [RFMAC-2691]
- Le lancement de l'application ShareFile échoue lorsque la sécurité renforcée est activée. [RFMAC-2724]
- Citrix Viewer peut consommer une quantité excessive des ressources processeur. [RFMAC-2777]

Problèmes résolus dans la version 1906

- Les sessions de carte à puce peuvent se déconnecter de manière aléatoire. [RFMAC-1816, RFMAC-2313]
- Les sessions déconnectées peuvent entraîner le blocage de l'application Citrix Workspace pour Mac. [RFMAC-2137]
- La fenêtre d'affichage Web s'affiche sur toutes les applications. [RFMAC-2146]
- Après le réveil d'un MacBook, l'application Citrix Workspace pour Mac demande à plusieurs reprises à l'utilisateur de s'authentifier. [RFMAC-2161]

- Lors de la connexion, une erreur peut apparaître indiquant que le serveur est introuvable. [RFMAC-2192]
- Le lancement d'une application Web sans authentification unique configurée peut provoquer une erreur 401 au lieu de demander des informations d'identification. [RFMAC-2194]
- Les fenêtres d'application transparentes peuvent disparaître lorsqu'elles sont déplacées vers un moniteur secondaire. [RFMAC-2314]
- Une page d'erreur « Impossible de charger la page » s'affiche occasionnellement. [RFMAC-2322]
- Les utilisateurs peuvent ne pas être en mesure de sélectionner des menus lors de l'utilisation de l'application Microsoft Outlook publiée. [RFMAC-2335]
- L'utilisation d'un formulaire Web peut afficher une erreur d'authentification. [RFMAC-2349]
- Lorsque la connexion via Citrix Gateway et un serveur virtuel est configurée pour utiliser des certificats intermédiaires signés, l'application Citrix Workspace pour Mac se ferme de façon inattendue avec une erreur SSL 61. [RFMAC-2393]
- Les informations d'identification de certains sites Web peuvent être effacées, ne permettant pas aux utilisateurs de se connecter. [RFMAC-2394]
- Le lancement d'une application Web Outlook affiche une page vierge. [RFMAC-2395]
- Lors de la réduction et de l'agrandissement d'applications transparentes, il se peut que l'application ne soit pas régénérée correctement. [RFMAC-2411]
- Les utilisateurs peuvent ne pas être en mesure de charger des fichiers vers Jira lorsque l'application est lancée en tant qu'application publiée. [RFMAC-2467]

Problèmes résolus dans la version 1903.1

- L'application Citrix Workspace pour Mac peut se fermer de façon inattendue lors du lancement de sessions de bureau.
- Certaines applications personnalisées peuvent ne pas être lancées. [RFMAC-2081]
- Lors du déplacement de l'application Bloc-notes, l'application peut se déplacer en arrière-plan lorsque deux ou plusieurs applications sont actives. [RFMAC-2107]
- Lorsque vous tentez de modifier un magasin Citrix Workspace, l'interface utilisateur de Citrix Files s'affiche à la place. [RFMAC-2111]
- Lorsque vous cliquez sur l'icône du dock après le lancement d'une application transparente, mais avant que l'application transparente ne soit prête, la session n'est plus transparente. [RFMAC-2139]
- Après le réveil d'un MacBook qui était en veille, Citrix Workspace demande à plusieurs reprises à l'utilisateur de s'authentifier. [RFMAC-2161]
- Après la reconnexion à une session VDA transparente, les graphiques de la session peuvent être déformés. [RFMAC-2176]
- Lorsque vous utilisez une disposition de clavier local et un clavier japonais, la suppression de caractères saisis non validés peut ne pas fonctionner correctement. [RFMAC-2287]

Problèmes résolus dans la version 1901

- Les applications peuvent ne pas être lancées après la mise à niveau de l'application Citrix Workspace pour Mac. [CGRFM-2003]
- La redirection audio USB peut ne pas fonctionner correctement. [RFMAC-2043]
- Vous ne pouvez pas sélectionner les menus déroulants dans les versions transparentes de Microsoft Outlook. [CGRFAC-2079]
- Les sessions peuvent ne plus répondre lorsque vous utilisez des applications transparentes. [CGRFAC-2083]
- Les sessions peuvent ne plus répondre lorsque vous réduisez ou maximisez les fenêtres couvrant plusieurs moniteurs. [CGRFAC-2103]

Problèmes résolus dans la version 1812

- Après avoir vérifié une info-bulle dans une application Microsoft Office, une zone noire reste à l'endroit où l'info-bulle a été affichée. [RFMAC-1793]
- Les sessions peuvent sembler floues lors de l'utilisation d'un écran Retina. [RFMAC-1944]
- L'utilisation du geste de balayage à trois doigts sur un pavé tactile dans une session exécutée sur trois moniteurs peut ne pas fonctionner correctement. [RFMAC-1968]
- Citrix Viewer peut utiliser App Nap lors de son exécution en arrière-plan. [RFMAC-1979]
- En cas de coupure de la connexion réseau, la page d'ouverture de session peut prendre plus de temps que d'habitude pour réapparaître une fois reconnectée au réseau. [RFMAC-2001]
- En appuyant sur Supprimer, vous pouvez supprimer plusieurs caractères. [RFMAC-2011]
- Les VDA avec EDT activé risquent de ne pas répondre lors de la lecture de vidéos YouTube pendant plus de trois minutes. [RFMAC-2017]
- Si Citrix Receiver Launcher est enregistré auprès de Google Chrome, la mise à niveau vers l'application Citrix Workspace n'autorise pas les lancements de session à partir de Chrome. [RFMAC-2020]
- La stratégie Utiliser codec vidéo pour la compression peut ne pas fonctionner correctement. [RFMAC-2021]

Problèmes résolus dans la version 1809

- Les sessions qui se sont reconnectées peuvent ne pas rester connectées. [RFMAC-1823]

Problèmes résolus dans la version 1808

- Sur les Mac à GPU double, le client peut utiliser le GPU discret sur batterie au lieu du GPU intégré plus économe en énergie. [RFMAC-1439]
- Le client peut ne pas se mettre à niveau correctement lorsqu'il est installé avec JamF. [RFMAC-1523]

- Les périphériques USB peuvent ne pas apparaître dans une session lorsque vous tentez de les utiliser pour la redirection USB générique. [RFMAC-1592]
- La recherche des mises à jour du client peut échouer avec l'erreur « Problème lors de la recherche des mises à jour ». [RFMAC-1589]
- Lorsque plusieurs fenêtres d'application publiée sont ouvertes, l'activation d'une fenêtre d'application publiée peut entraîner l'apparition d'une fenêtre d'application publiée différente. [RFMAC-1696]

Problèmes connus

Problèmes connus dans la version 2104

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

Problèmes connus dans la version 2102

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

Problèmes connus dans la version 2101

- Les tentatives d'accès aux fichiers sous Partages réseau depuis l'application Workspace pour Mac peuvent échouer même lorsque l'option est activée. [RFMAC-7272]
- Sur macOS Big Sur, les tentatives de lancement de l'application d'authentification unique SAML Web sur l'application Citrix Workspace pour Mac peuvent échouer, affichant le message d'erreur suivant.

  ```
  Page could not load. Please try again later or contact your administrator
   for assistance. Incident ID:-202
  ```

  [RFMAC-7282]

Problèmes connus dans la version 2012

- Lorsque vous démarrez un appel vidéo, Microsoft Teams peut ne pas répondre et afficher une erreur `Citrix HDX not connected`. Pour contourner le problème, redémarrez Microsoft Teams ou le VDA. [RFMAC-6727]
- Les appels vidéo sur Microsoft Skype Entreprise ne sont pas pris en charge sur macOS Big Sur (11.0.1).
- Sous macOS Big Sur (11.0.1), les tentatives de connexion de périphériques USB peuvent échouer, entraînant la fermeture inattendue de la session. Pour contourner le problème, reconnectez le périphérique USB. [RFMAC-7079]

Problèmes connus dans la version 2010

- Sur Skype Entreprise, la vidéo entrante n'est pas visible sur macOS Big Sur (11.0.1).
- Lors de l'utilisation de l'application Citrix Workspace pour Mac 2008 ou version ultérieure, les tentatives de lancement de plusieurs instances d'une application publiée peuvent échouer. [CVADHELP-16019]
- Les tentatives de lancement de la redirection USB générique peuvent échouer lorsque vous utilisez une station d'accueil USB. [RFMAC-6687]
- Lorsque vous utilisez un MacBook Pro 2018 et versions ultérieures et FaceTime, les utilisateurs peuvent voir une barre rectangulaire déformée de couleur verte ou noire en bas de l'aperçu vidéo. [RFMAC-2829]

Problèmes connus dans la version 2009

macOS Big Sur bêta

- Dans un déploiement sur cloud, la couleur d'arrière-plan des postes de travail publiés peut être différente. Le problème se produit par intermittence sur certaines versions de macOS Big Sur bêta. [RFMAC-6343]
- L'icône du programme d'installation de l'application Citrix Workspace pour Mac peut être manquante lorsque vous ouvrez le fichier **CitrixWorkspaceApp.dmg**. Le problème se produit par intermittence sur certaines versions de macOS Big Sur bêta. [RFMAC-6378]

Optimisation pour Microsoft Teams (Preview)

- Seules les applications tierces (par exemple, Microsoft PowerPoint) peuvent être partagées lorsque vous utilisez le partage d'écran dans Microsoft Teams sur l'application Citrix Workspace pour Mac. Cependant, le partage d'écran entrant est entièrement pris en charge. [RFMAC-3403]
- Le moteur HDX RealTime Connector peut se fermer de manière inattendue lorsque vous allumez et éteignez la caméra dans Microsoft Teams. [RFMAC-6293]
- Le moteur HDX RealTime Connector peut se fermer de manière inattendue lorsque vous changez de caméra lors d'un appel vidéo optimisé dans Microsoft Teams. [RFMAC-6157]
- Les appels audio et vidéo peuvent se déconnecter lorsque vous changez de réseau dans Microsoft Teams. [RFMAC-6292]
- Lors de l'utilisation de l'application Citrix Workspace pour Mac sur macOS Big Sur bêta, les appels audio peuvent se déconnecter. Le problème se produit lorsque vous déconnectez des périphériques audio et connectez d'autres périphériques audio lors d'un appel audio. [RFMAC-6112]

Problèmes connus dans la version 2008

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

Problèmes connus dans 2007

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

Problèmes connus dans la version 2006

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

Problèmes connus dans la version 2005

- Les tentatives de connexion à l'application Citrix Workspace pour Mac peuvent échouer, affichant une interface utilisateur non apparentée. Pour contourner le problème, cliquez sur **Actualiser applications** dans le menu pour charger le magasin. [RFMAC-4063]

Problèmes connus dans la version 2002

- L'application Citrix Workspace pour Mac prend en charge la redirection de Webcam uniquement pour les applications 32 bits publiées. Par conséquent, la redirection de Webcam n'est pas prise en charge pour l'application Microsoft Teams 64 bits publiée. [RFMAC-2199]
- L'application Citrix Workspace pour Mac ne prend pas en charge les écrans haute résolution (Retina). Par conséquent, le texte peut apparaître flou sur ces appareils. [RFMAC-650]
- Les tentatives de connexion à l'application Citrix Workspace sur macOS Catalina à l'aide de cartes à puce PIV peuvent échouer, affichant le message d'erreur suivant : « Impossible de détecter le compte spécifié. » [CVADHELP-14155]

Problèmes connus dans la version 2001

- Les tentatives de connexion à l'application Citrix Workspace sur macOS Catalina à l'aide de cartes à puce PIV peuvent échouer, affichant le message d'erreur suivant : « Impossible de détecter le compte spécifié. » [CVADHELP-12609]
- Les tentatives de lancement d'une session dans l'application Citrix Workspace sur macOS Catalina (10.15.2) à l'aide de cartes à puce PIV peuvent échouer, affichant le message d'erreur suivant : « Un ou plusieurs certificats racine ne sont pas valides. » [RFMAC-3365]

Problèmes connus dans la version 1912

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

Problèmes connus dans la version 1910.2

- La connexion à l'application Citrix Workspace sur macOS Catalina à l'aide de cartes à puce PIV peut échouer. [RFMAC-2788]

Problèmes connus dans la version 1910.1

- La connexion à l'application Citrix Workspace sur macOS Catalina à l'aide de cartes à puce PIV peut échouer. [RFMAC-2788]

Problèmes connus dans la version 1910

- Lorsque vous utilisez un MacBook Pro 2018 et versions ultérieures et FaceTime, les utilisateurs peuvent voir une barre verte en bas de l'aperçu vidéo. [RFMAC-2317]
- Le lancement d'une session avec une carte à puce via Citrix Gateway peut échouer, affichant le message d'erreur « Le pair SSL distant a envoyé une alerte d'échec de négociation ». [RFMAC-2727]
- La connexion à l'application Citrix Workspace sur macOS Catalina à l'aide de cartes à puce PIV peut échouer. [RFMAC-2788]
- Lorsque l'authentification SAML est activée, l'écran d'authentification peut être lent ou ne pas répondre. Pour contourner le problème, redémarrez l'appareil. [RFMAC-3047]
- Le refus d'autoriser l'automatisation après le lancement d'applications auxquelles vous êtes abonné peut entraîner le blocage de l'application Citrix Workspace pour Mac. Pour contourner le problème, accédez à **Préférences Système > Sécurité et confidentialité > Confidentialité > Automatisation** et accordez les autorisations pour Citrix Viewer.app, Citrix Workspace.app et toutes les applications auxquelles vous êtes abonné. [RFMAC-3048]

Problèmes connus dans la version 1906

- Lorsque vous utilisez un MacBook Pro 2018 et versions ultérieures et FaceTime, les utilisateurs peuvent voir une barre verte en bas de l'aperçu vidéo. [RFMAC-2317]

Problèmes connus dans la version 1903.1

- Les sessions de carte à puce peuvent se déconnecter de manière aléatoire. [RFMAC-1816]
- Lors de la connexion, une erreur peut apparaître indiquant que le serveur est introuvable. [RFMAC-2192]

- Lorsque vous utilisez un MacBook Pro 2018 et versions ultérieures et FaceTime, les utilisateurs peuvent voir une barre verte en bas de l'aperçu vidéo. [RFMAC-2317]

Problèmes connus dans la version 1901

- Les sessions de carte à puce peuvent se déconnecter de manière aléatoire. [RFMAC-1816]

Problèmes connus dans la version 1812

- Les sessions de carte à puce peuvent se déconnecter de manière aléatoire. [RFMAC-1816]
- La redirection audio USB peut ne pas fonctionner correctement. [RFMAC-2043]

Problèmes connus dans la version 1809

- Les sessions d'application et de bureau risquent de ne pas démarrer lors de l'utilisation de Safari version 12. Pour contourner le problème, consultez l'article CTX238286 du centre de connaissances. Après avoir appliqué la solution de contournement, Safari demande des autorisations aux utilisateurs à chaque fois pour lancer des sessions.

Problèmes connus dans la version 1808

- Lorsqu'une erreur survient dans une application utilisant Secure SaaS, l'erreur qui apparaît dans le navigateur n'est pas traduite. [RFMAC-1836]

Avis de tiers

L'application Citrix Workspace peut inclure un logiciel tiers distribué sous une licence selon les conditions définies dans le document suivant :

Avis de tiers de l'application Citrix Workspace pour Mac

Configuration système requise et compatibilité

June 10, 2021

Systèmes d'exploitation pris en charge

L'application Citrix Workspace pour Mac prend en charge les systèmes d'exploitation suivants :

- macOS Big Sur 11 (y compris les versions mineures et correctifs)

- macOS Catalina (10.15)

Produits Citrix compatibles

L'application Citrix Workspace 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

L'application Citrix Workspace 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

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

Configuration logicielle requise

- Pour déployer l'application Citrix Workspace pour Mac :
  - Application Citrix Workspace pour Web 2.1, 2.5 et 2.6
- StoreFront :
  StoreFront 2.x ou version supérieure pour l'accès natif aux applications à partir de l'application Citrix Workspace pour Mac ou d'un navigateur Web.

Connexions, certificats et authentification

Connexions

L'application Citrix Workspace pour Mac prend en charge les connexions suivantes à Citrix Virtual Apps and Desktops :

- HTTP
- HTTPS
- ICA-over-TLS

L'application Citrix Workspace 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 un site Citrix Receiver pour Web	Citrix Gateway 10.5–12.0, y compris VPX ; Enterprise Edition 9.x-10.x, y compris VPX ; VPX

Certificats

Certificats privés (auto-signés)

Si un certificat privé est installé sur la passerelle distante, le certificat racine pour l'autorité de certification de l'organisation doit être installé sur l'appareil de l'utilisateur. Ensuite, vous pouvez accéder aux ressources Citrix à l'aide de l'application Citrix Workspace 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 démarrent pas.

Importation de certificats racine sur des machines sur lesquelles l'application Citrix Workspace pour Mac est installée

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. L'application Citrix Workspace pour Mac prend en charge les certificats génériques.

Certificats intermédiaires avec Citrix Gateway

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

Stratégie de validation des certificats de serveur

La stratégie de validation des certificats de serveur de l'application Citrix Workspace pour Mac est plus stricte.

> **Important**
>
> Avant d'installer cette version de l'application Citrix Workspace 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 inclut un certificat racine incorrect ;
> - la configuration du serveur ou de la passerelle n'inclut pas tous les certificats intermédiaires ;
> - la configuration du serveur ou de la passerelle inclut un certificat intermédiaire expiré ou non valide ;
> - la configuration du serveur ou de la passerelle inclut un certificat intermédiaire avec signature croisée.

Lors de la validation d'un certificat de serveur, l'application Citrix Workspace pour Mac utilise maintenant **tous** les certificats fournis par le serveur (ou la passerelle). Comme dans les versions précédentes de l'application Citrix Workspace 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 l'application Citrix Workspace 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 l'application Citrix Workspace pour Mac :

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

L'application Citrix Workspace pour Mac vérifie ensuite que tous ces certificats sont valides. L'application Citrix Workspace pour Mac vérifie également qu'il fait déjà confiance à « Certificat racine exemple ». Si l'application Citrix Workspace 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 à l'application Citrix Workspace 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 finissent par expirer, 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 »

L'application Citrix Workspace pour Mac utilise ces deux certificats. Il recherche ensuite un certificat racine sur la machine utilisateur. Si elle en trouve un qui est validé et également approuvé (tel que « Certificat racine exemple »), la connexion réussit. Sinon, la connexion échoue. Cette configuration fournit le certificat intermédiaire dont l'application Citrix Workspace pour Mac a besoin, mais permet également à l'application Citrix Workspace 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, l'application Citrix Workspace 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. en cas de certificats racines multiples. Un certificat racine antérieur est toujours utilisé en même temps qu'un certificat racine ultérieur. 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 entraîne la sélection du certificat racine antérieur :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »
- « Certificat intermédiaire croisé 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 l'application Citrix Workspace pour Mac ne peut pas trouver tous les certificats intermédiaires, la connexion échoue.

Authentification

Pour les connexions à StoreFront, l'application Citrix Workspace pour Mac prend en charge les méthodes d'authentification suivantes :

	Workspace pour Web utilisant des navigateurs	Site StoreFront Services (natif)	Site StoreFront XenApp Services (natif)	Citrix Gateway auprès de Workspace pour Web (navigateur)	Citrix Gateway auprès du site StoreFront Services (natif)
Anonymous	Oui	Oui			
Domaine	Oui	Oui		Oui*	Oui*
Authentificatior pass-through au domaine					
Jeton de sécurité				Oui*	Oui*
Deux facteurs (domaine avec jeton de sécurité)				Oui*	Oui*
SMS				Oui*	Oui*
Carte à puce	Oui	Oui		Oui*	Oui
Certificat utilisateur				Oui	Oui (Citrix Gateway Plug-in)

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

Installer, désinstaller et mettre à niveau

April 12, 2021

L'application Citrix Workspace pour Mac contient un seul pack d'installation et prend en charge l'accès distant via Citrix Gateway et Secure Web Gateway.

Vous pouvez installer l'application Citrix Workspace pour Mac de l'une des manières suivantes :

- À partir du site Web Citrix
- Automatiquement à partir de Workspace pour Web

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

Installation manuelle

Par un utilisateur à partir de Citrix.com

En tant que nouvel utilisateur, vous pouvez télécharger l'application Citrix Workspace pour Mac à partir de Citrix.com ou de votre propre site de téléchargement. Vous pouvez ensuite créer un compte en saisissant une adresse e-mail au lieu d'une adresse URL de serveur. L'application Citrix Workspace pour Mac identifie le serveur Citrix Gateway ou StoreFront associé à l'adresse e-mail. Ensuite, il invite l'utilisateur à ouvrir une session et à poursuivre 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 l'application Citrix Workspace pour Mac sur sa machine.

La découverte de compte basée sur l'adresse e-mail pour un nouvel utilisateur ne s'applique pas si vous avez téléchargé depuis un emplacement autre que Citrix.com (tel qu'un site Citrix Receiver pour Web).

Si votre site nécessite la configuration de l'application Citrix Workspace pour Mac, utilisez une autre méthode de déploiement.

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

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

Depuis la page Téléchargements de Citrix

Vous pouvez installer l'application Citrix Workspace pour Mac à partir d'un partage réseau ou directement sur la machine de l'utilisateur. Vous pouvez le faire en téléchargeant le fichier à partir du site Web Citrix à l'adresse Téléchargements.

Pour installer l'application Citrix Workspace pour Mac :

1. Téléchargez le fichier .dmg correspondant à la version de l'application Citrix Workspace 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. Sur la page **Ajouter un compte**, sélectionnez **Ajouter un compte** et cliquez sur **Continuer**.
7. Entrez le nom d'utilisateur et le mot de passe d'un administrateur sur la machine locale.

Désinstallation

Vous pouvez désinstaller l'application Citrix Workspace pour Mac manuellement en ouvrant le fichier .dmg. Sélectionnez **Désinstaller l'application Citrix Workspace** et suivez les instructions à l'écran. Le fichier .dmg est le fichier qui est téléchargé de Citrix lors de la première installation de l'application Citrix Workspace pour Mac. Si le fichier ne se trouve plus sur votre ordinateur, téléchargez-le à nouveau à partir de Téléchargements de Citrix pour désinstaller l'application.

Mise à niveau

L'application Citrix Workspace pour Mac vous envoie des notifications lorsqu'une mise à jour est disponible pour une version existante ou une mise à niveau vers une version plus récente. Vous pouvez également cliquer avec le bouton droit de la souris sur l'icône de l'application Citrix Workspace et cliquer sur **Rechercher les mises à jour** pour savoir si des mises à jour ou des mises à niveau sont disponibles.

Vous pouvez mettre à niveau l'application Citrix Workspace pour Mac depuis n'importe quelle version antérieure de l'application Citrix Workspace pour Mac.

Lorsque vous effectuez une mise à niveau vers une version plus récente de l'application Citrix Workspace pour Mac, la version précédente est désinstallée automatiquement. Vous n'avez pas besoin de redémarrer votre ordinateur.

Configurer

June 18, 2021

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

Les utilisateurs peuvent se connecter à partir d'Internet ou à partir d'emplacements distants. Pour ces utilisateurs, configurez l'authentification via Citrix Gateway.

Tâches et considérations de l'administrateur

Cet article discute des tâches et des considérations pertinentes pour les administrateurs de l'application Citrix Workspace pour Mac.

Gestion des feature flag

Si un problème survient avec l'application Citrix Workspace en production, nous pouvons désactiver dynamiquement une fonctionnalité affectée dans l'application Citrix Workspace même après la livraison de la fonctionnalité. Pour ce faire, nous utilisons des commutateurs de fonctionnalité et un service tiers appelé LaunchDarkly. Vous n'avez pas besoin d'effectuer des configurations pour activer le trafic vers LaunchDarkly, sauf si un pare-feu ou un proxy bloque le trafic sortant. Dans ce cas, vous activez le trafic vers LaunchDarkly via des URL ou adresses IP spécifiques, en fonction des exigences de votre stratégie.

Vous pouvez activer le trafic et la communication vers LaunchDarkly des manières suivantes :

Activer le trafic vers les URL suivantes

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `Firehose.launchdarkly.com`
- `mobile.launchdarkly.com`

Répertorier les adresses IP dans une liste verte

Si vous devez répertorier les adresses IP dans une liste verte, consultez la liste des adresses IP publiques de LaunchDarkly pour obtenir une liste de toutes les plages d'adresses IP actuelles. Vous pouvez utiliser cette liste pour vous assurer que les configurations du pare-feu sont mises à jour automatiquement en fonction des mises à jour de l'infrastructure. Pour plus d'informations sur l'état des modifications de l'infrastructure, consultez la page LaunchDarkly Statuspage.

Configuration système requise pour LaunchDarkly

Assurez-vous que les applications peuvent communiquer avec les services suivants si le split tunneling sur Citrix ADC est **désactivé** :

- Service LaunchDarkly.
- Service d'écoute APNs

Intégration de Content Collaboration Service

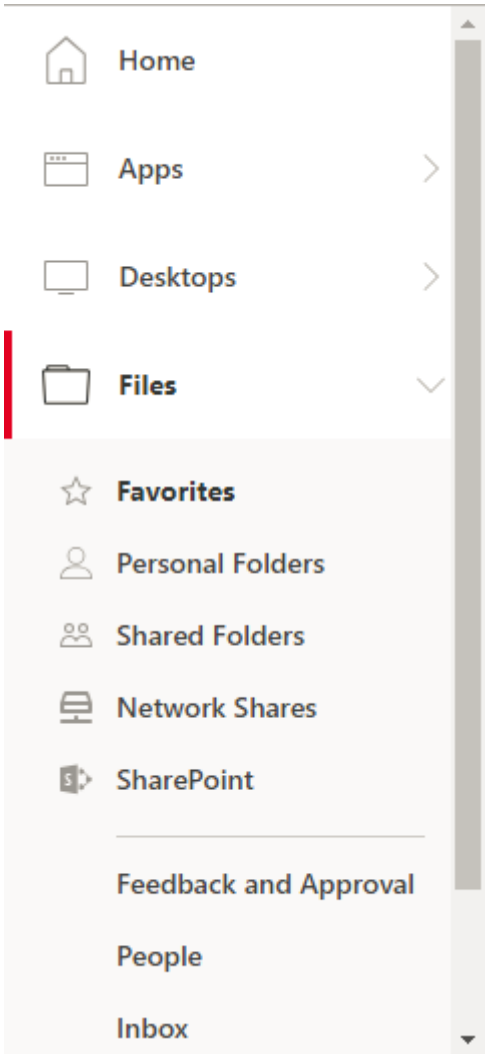
Citrix Content Collaboration vous permet d'échanger des documents facilement et en toute sécurité, d'envoyer des documents volumineux par courrier électronique, de gérer en toute sécurité les transferts de documents à des tiers et d'accéder à un espace de collaboration.

Citrix Content Collaboration met à votre disposition plusieurs façons de travailler, notamment une interface Web, des clients mobiles, des applications de bureau et une intégration avec Microsoft Outlook et Gmail.

Vous pouvez accéder aux fonctionnalités de Citrix Content Collaboration à partir de l'application Citrix Workspace à l'aide de l'onglet **Fichiers** affiché dans l'application Citrix Workspace. Vous pouvez afficher l'onglet **Fichiers** uniquement si Content Collaboration Service est activé dans la configuration de Workspace dans la console Citrix Cloud.

> **Remarque :**
>
> L'intégration de Citrix Content Collaboration dans l'application Citrix Workspace n'est pas prise en charge sur Windows Server 2012 et Windows Server 2016. Cela est dû à une option de sécurité définie dans le système d'exploitation.

L'image suivante affiche un exemple de contenu de l'onglet **Fichiers** dans la nouvelle application Citrix Workspace :



Limitations

- La réinitialisation de l'application Citrix Workspace ne provoque pas la fermeture de la session de Citrix Content Collaboration.
- Le changement de magasin dans l'application Citrix Workspace ne provoque pas la fermeture de la session de Citrix Content Collaboration.

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 ou d'une application hébergée de bureau.

Au cours d'une session, les utilisateurs peuvent brancher des périphériques Plug and Play, y compris des périphériques PTP (Picture Transfer Protocol). Par exemple :

- Appareils photo numériques, périphériques MTP (Media Transfer Protocol) tels que lecteurs audio numériques ou lecteurs multimédia portables
- Périphériques de point de vente, et autres périphériques tels que souris 3D Space, scanners, dispositifs de signature, etc.

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

La redirection de périphérique USB est disponible pour les systèmes d'exploitation suivants :

- Windows
- Linux
- Mac

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 disponibles pour un bureau virtuel en mettant à jour la liste des périphériques USB pris en charge pour la redirection. Vous trouverez des informations supplémentaires 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, l'application Citrix Workspace pour Mac utilise une carte intelligente identique à celle d'une souris.

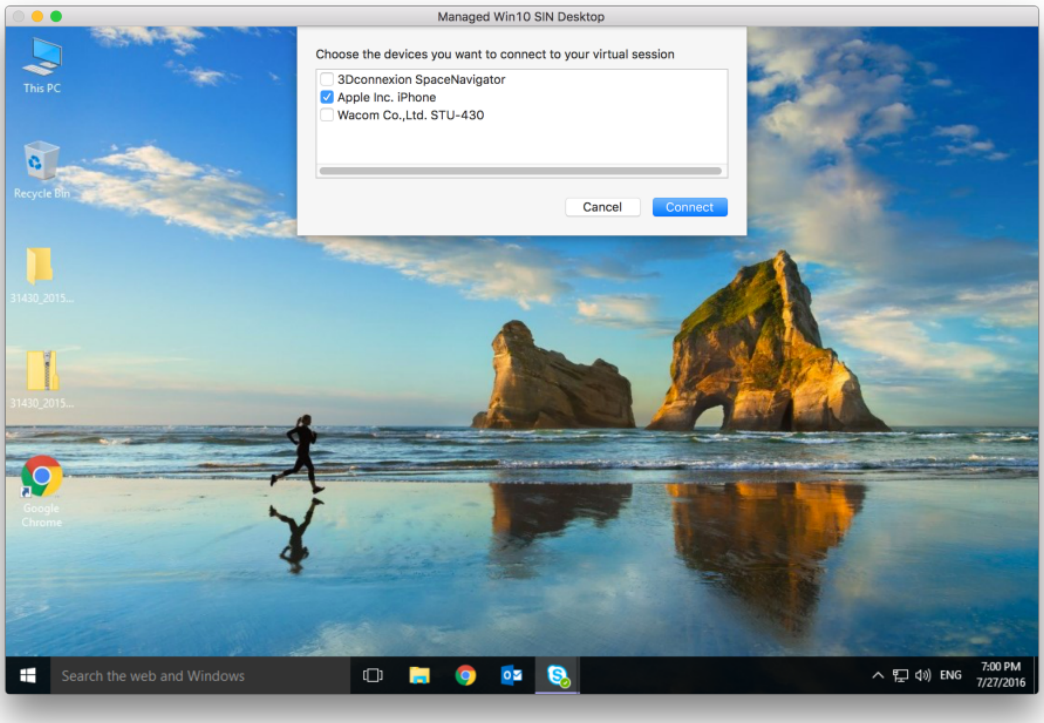
Le produit prend en charge les canaux virtuels optimisés avec des périphériques USB 3.0 et des ports USB 3.0. Par exemple, un canal virtuel CDM est utilisé pour afficher des fichiers sur une caméra ou pour fournir de l'audio à un casque. Le produit prend également en charge la redirection USB générique 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.

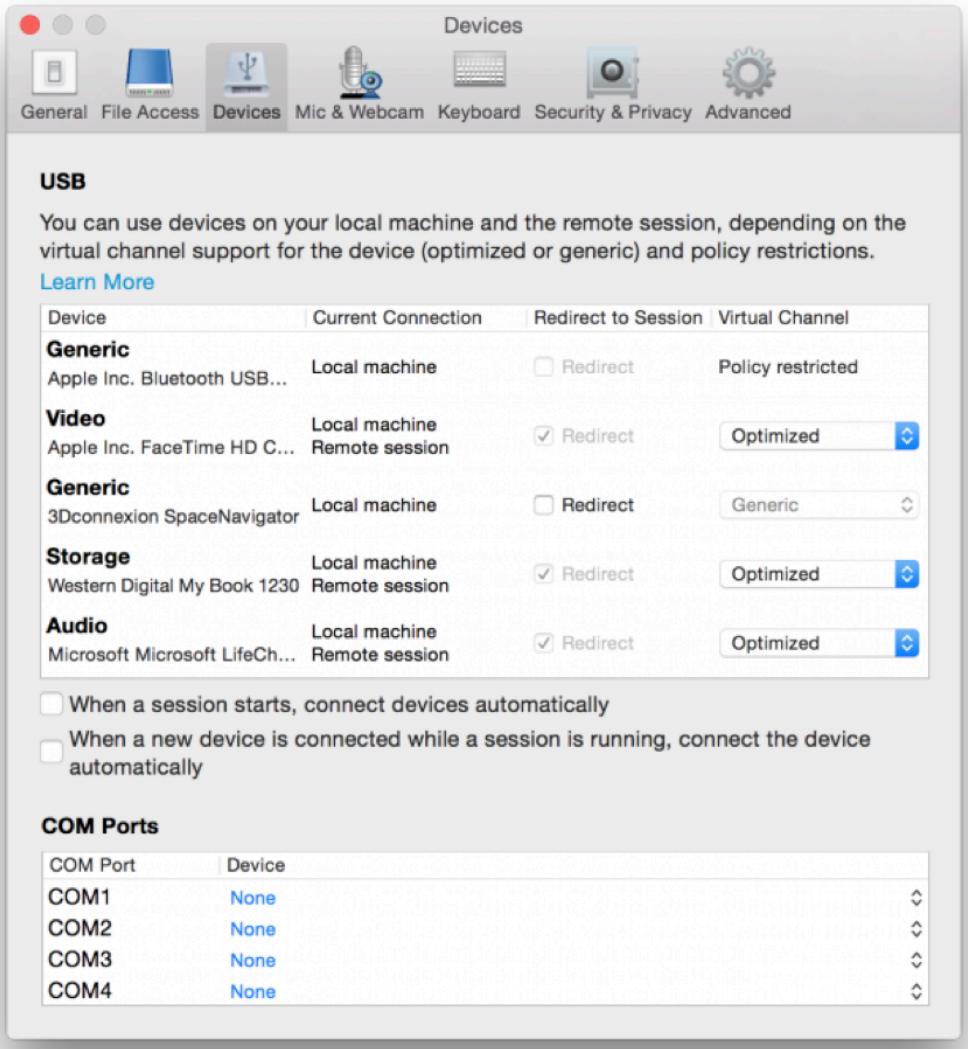
Certains périphériques ne sont pas redirigés par défaut et sont uniquement disponibles pour la session locale. Par exemple, il n'est pas approprié de rediriger une carte d'interface réseau qui est directement connectée via USB interne.

Pour utiliser la redirection USB :

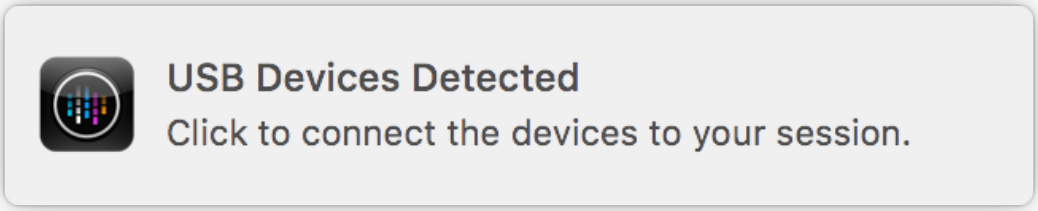
1. Connectez le périphérique USB à l'appareil sur lequel l'application Citrix Workspace pour Mac est installée.
2. Vous êtes invité à sélectionner les périphériques USB disponibles sur votre système local.



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 (Générique ou Optimisé) pour le périphérique USB.
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 l'application Citrix Workspace 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.

Enlightened Data Transport (EDT)

EDT est activé par défaut dans l'application Citrix Workspace pour Mac.

L'application Citrix Workspace 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
```

Fiabilité de session et 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 invite de s'authentifier à nouveau.

> **Important**
>
> - Les utilisateurs de l'application Citrix Workspace pour Mac ne peuvent pas changer le paramètre de serveur.
> - Si la fiabilité de session est activée, le port utilisé par défaut pour les communications de session passe de 1494 à 2598.

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 Citrix 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, un utilisateur distrait peut s'éloigner de sa machine cliente. 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.

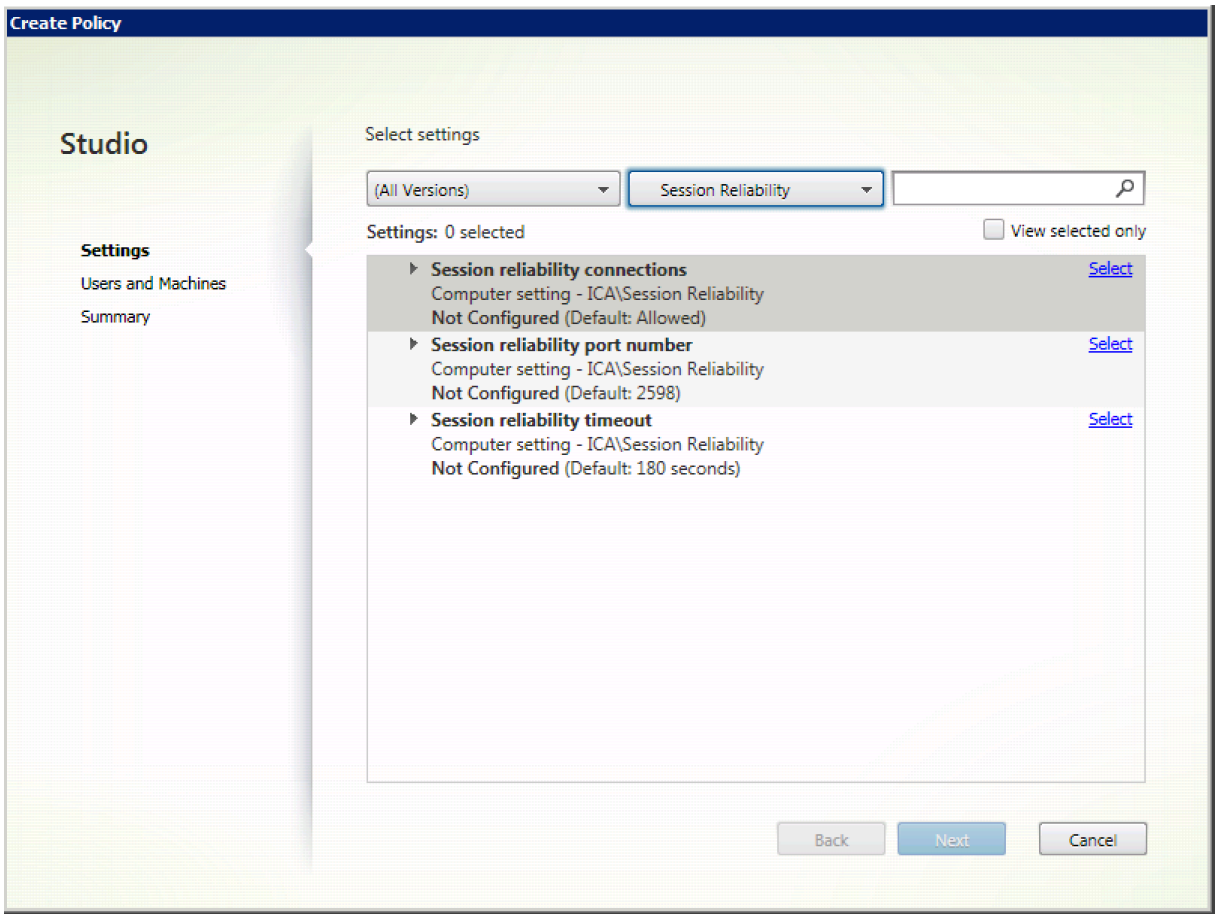
Configuration de la fiabilité de session à partir de Citrix Studio

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

Par défaut, l'expiration du délai de la fiabilité de session est réglée sur 180 secondes.

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

Pour modifier l'expiration du délai de la fiabilité de session :

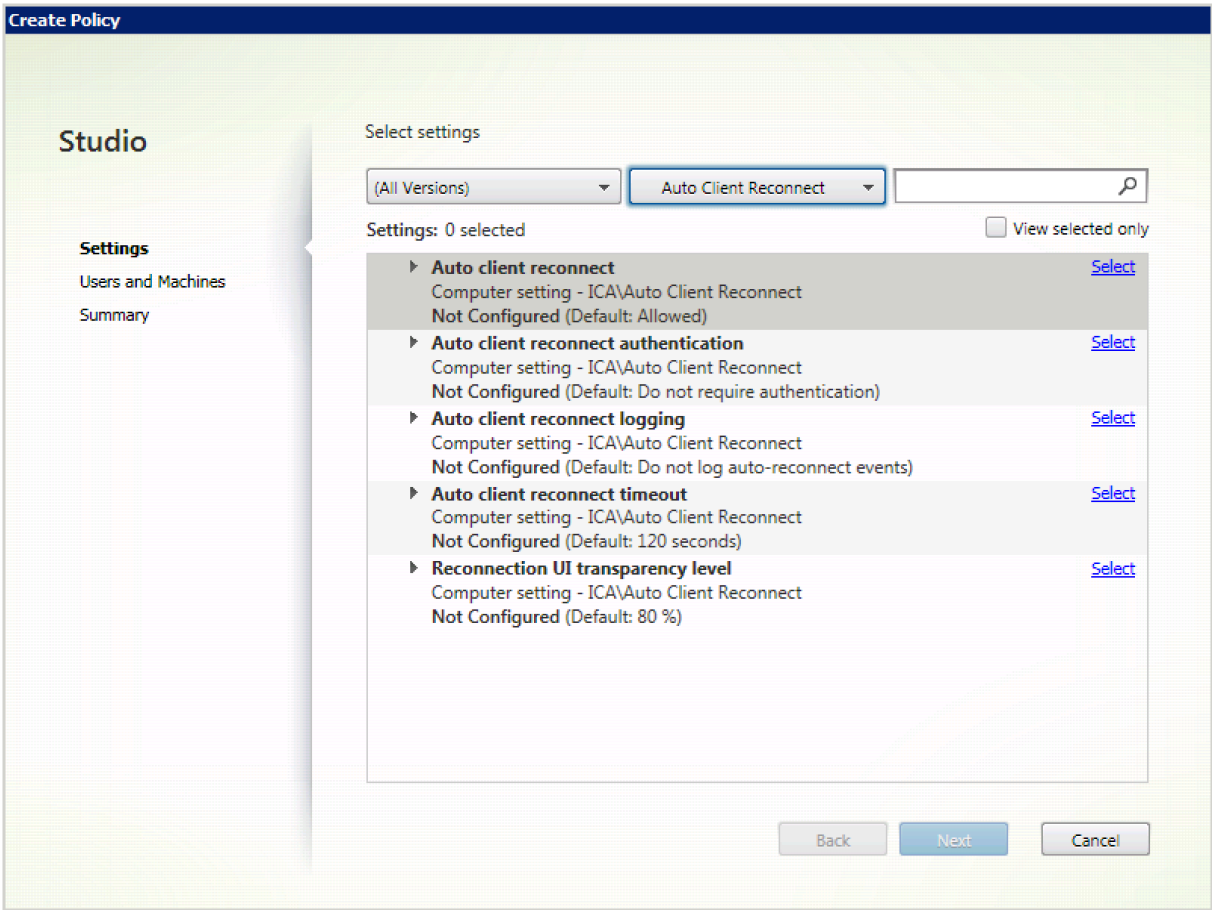
1. Lancez Citrix Studio.
2. Ouvrez la stratégie **Expiration de délai de la fiabilité de session**.
3. Modifiez la valeur du délai d'expiration.
4. Cliquez sur **OK**.

Configuration de la reconnexion automatique du client à l'aide de Citrix Studio

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 et 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, l'application Citrix Workspace 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

Il existe des 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. Ils créent des environnements complexes lorsqu'il s'agit de maintenir l'intégrité des connexions aux sessions actives de l'application Citrix Workspace pour Mac. Pour résoudre ce problème, Citrix a amélioré les technologies de fiabilité de session et de reconnexion automatique présentes dans cette version de l'application Workspace pour Mac.

La reconnexion automatique des clients, associée à la fiabilité de session permet aux utilisateurs de se reconnecter automatiquement à leurs sessions d'application Citrix Workspace pour Mac 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. Par défaut, ce délai est défini sur 120 secondes (ou deux minutes).

Paramètre	Exemple	Valeur par défaut
TransportReconnectRetryMaxT	TransportReconnectRetryMaxT	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 d'expiration de la connexion pour la fiabilité de session. Par défaut, ce délai d'expiration est défini sur 180 secondes, ou trois minutes.

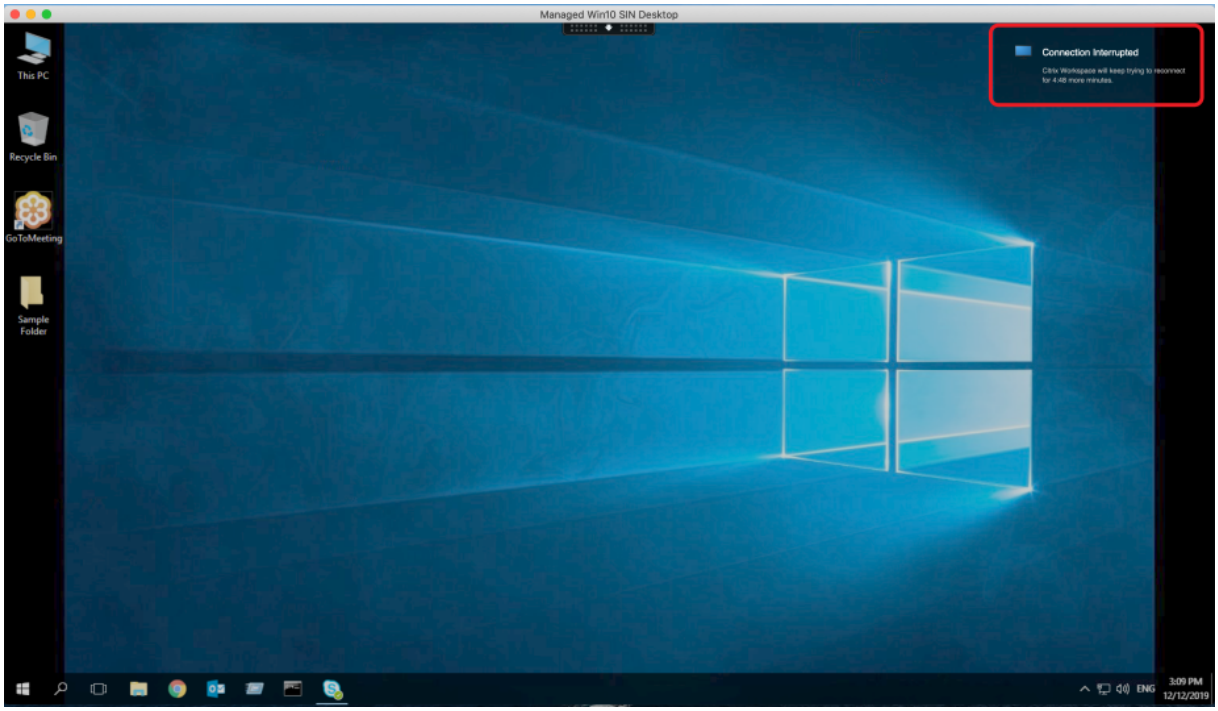
Paramètre	Exemple	Valeur par défaut
SessionReliabilityTTL	SessionReliabilityTTL=120	180

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 l'application Citrix Workspace pour Mac, tenez compte de ce qui suit :

- Une fenêtre de session est grisée lorsqu'une reconnexion est en cours. Un minuteur affiche la durée restante avant la reconnexion de la session. Une fois que la session a expiré, elle est déconnectée.

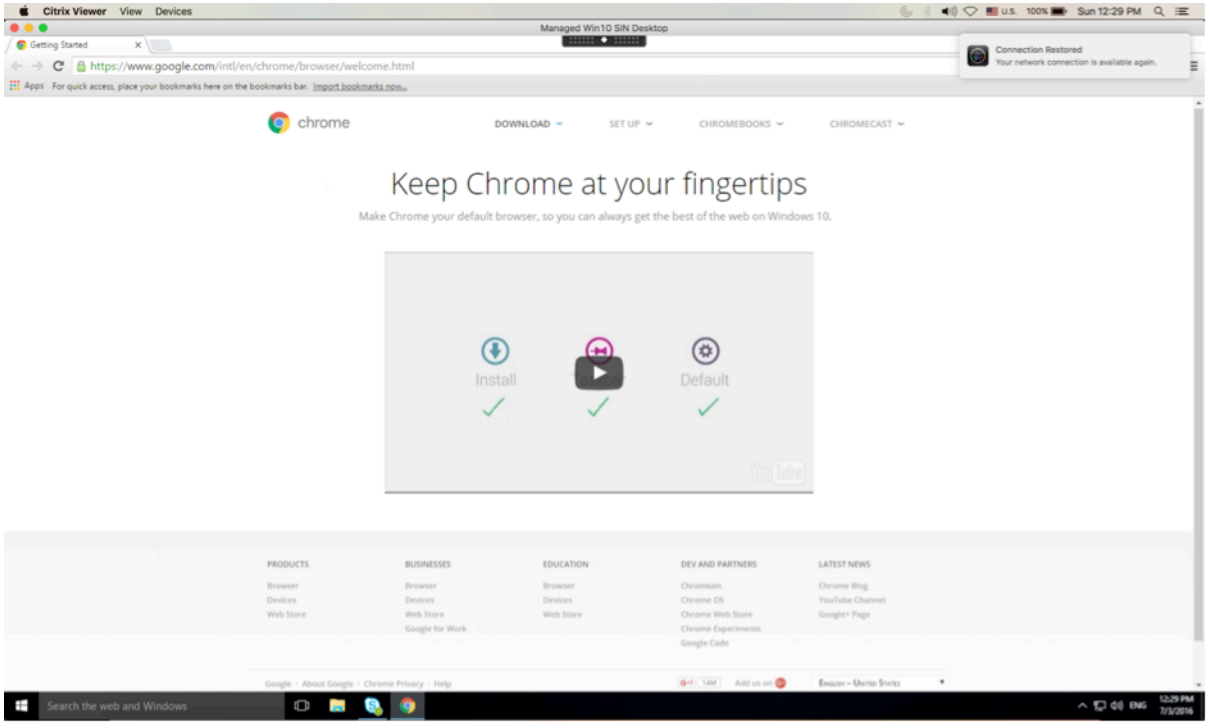
Par défaut, la notification de reconnexion commence après 5 minutes. Cette valeur représente les valeurs combinées de chacun des minuteurs (reconnexion automatique des clients et fiabilité de session), respectivement 2 et 3 minutes. L'image suivante illustre la notification qui s'affiche dans la partie 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.

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

Données collectées	Description	Quel usage faisons-nous de ces données
Données de configuration et d'utilisation	Le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) rassemble des données de configuration et d'utilisation à partir de l'application Citrix Workspace pour Mac et les envoie automatiquement à Citrix et Google Analytics.	Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de Workspace.

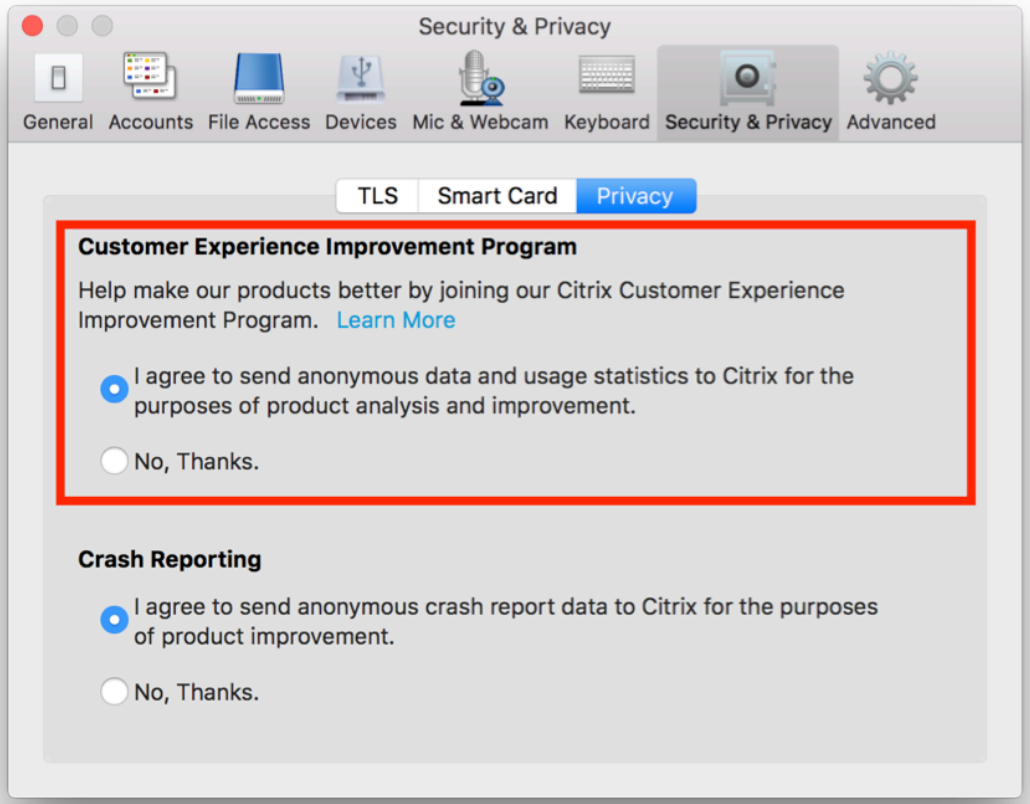
Informations supplémentaires

Citrix traite vos données conformément aux termes de votre contrat avec Citrix et les protège comme indiqué dans l'Annexe sur la sécurité des Services Citrix sur le Citrix Trust Center.

Citrix utilise Google Analytics pour collecter certaines données à partir de l'application Citrix Workspace dans le cadre du programme CEIP. Veuillez contrôler la façon dont Google gère les données collectées pour Google Analytics.

Vous pouvez désactiver l'envoi de données via le programme CEIP à Citrix et Google Analytics. Pour ce faire :

1. Dans la fenêtre **Préférences**, sélectionnez **Sécurité et confidentialité**.
2. Sélectionnez l'onglet **Confidentialité**.
3. Sélectionnez **Non merci** pour désactiver le programme CEIP ou ne pas y participer.
4. Cliquez sur **OK**.



Vous pouvez également désactiver CEIP en exécutant la commande terminal :

```
defaults write com.citrix.receiver.nomas "CEIPEnabled"-bool NO
```


Les données spécifiques collectées par Google Analytics sont les suivantes :

Version du système d'exploitation	Lancement de session	Utilisation de la redirection USB générique

Mise à disposition d'applications

Lors de la mise à disposition d'applications avec Citrix Virtual Apps and Desktops, envisagez les options suivantes pour améliorer l'expérience de vos utilisateurs lorsqu'ils accèdent à leurs applications :

Mode d'accès Web

Sans aucune configuration, l'application Citrix Workspace 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 Workspace pour 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

Ajoutez un compte StoreFront à l'application Citrix Workspace pour Mac ou configurez l'application Citrix Workspace pour Mac pour qu'elle pointe vers un site StoreFront. Ensuite, vous pouvez configurer le mode libre-service, qui permet à vos utilisateurs de s'abonner à des applications via l'application Citrix Workspace 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.

Lorsqu'ils accèdent à un site StoreFront 3.0, vos utilisateurs voient l'aperçu de l'application Citrix Workspace pour Mac.

Lors de la publication d'applications sur vos batteries Citrix Virtual Apps, vous pouvez améliorer l'expérience des utilisateurs qui accèdent à ces applications via des magasins StoreFront. Pour ce faire, pensez à inclure des descriptions claires des applications publiées. Les descriptions sont visibles par vos utilisateurs via l'application Citrix Workspace pour Mac.

Configurer le mode libre-service

Comme mentionné précédemment, vous pouvez ajouter un compte StoreFront à l'application Citrix Workspace pour Mac ou configurer l'application Citrix Workspace pour Mac pour qu'elle pointe vers un site StoreFront. Ainsi, vous pouvez configurer le mode libre-service, qui permet aux utilisateurs de s'abonner à des applications à partir de l'interface utilisateur de l'application Citrix Workspace 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.

- Abonnez automatiquement tous les utilisateurs d'un magasin à une application en ajoutant la chaîne KEYWORDS:Auto à la description que vous fournissez lors de la publication de l'application dans Citrix Virtual Apps. Lorsque les utilisateurs ouvrent une session dans le magasin, l'application est automatiquement provisionnée sans qu'ils aient à y souscrire manuellement.
- Permet d'avertir les utilisateurs de la présence d'une application ou de faciliter la recherche des applications les plus couramment utilisées en les répertoriant dans la liste Sélection de l'application Citrix Workspace pour Mac. Pour ce faire, ajoutez la chaîne KEYWORDS:Featured à la description de l'application.

Pour de plus amples informations, consultez la documentation de StoreFront.

Mises à jour de Citrix Workspace

Configuration à l'aide de l'interface utilisateur

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

1. Accédez à la boîte de dialogue **Préférences** dans l'application Citrix Workspace pour Mac.
2. Dans le panneau **Avancées**, cliquez sur **Mises à jour**. La boîte de dialogue Mise à jour de Citrix Workspace 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 Workspace à l'aide de StoreFront

Les administrateurs peuvent configurer les mises à jour de Citrix Workspace à l'aide de StoreFront. L'application Citrix Workspace pour Mac 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 : <account id=… name="Store">

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

   <properties>

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

auto-update-Check

Cela détermine si l'application Citrix Workspace pour Mac 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 Workspace.

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 l'application Citrix Workspace pour Mac. Par défaut, cette valeur est définie sur 7.

Valeurs possibles :

- -1 : l'utilisateur a toujours l'option d'être notifié ultérieurement lorsqu'une mise à jour est disponible.

- 0 : l'utilisateur est forcé de mettre à jour vers la dernière version de l'application Citrix Workspace pour Mac lorsque la mise à jour est disponible.
- Entier positif : l'utilisateur a 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 voit qu'une mise à jour est disponible.

Valeurs possibles :

- Auto : le système de mise à jour de Citrix Workspace décide lorsque les mises à jour disponibles sont déployées auprès des utilisateurs.
- Fast : les mises à jour disponibles sont déployées en priorité auprès des utilisateurs comme déterminé par l'application Citrix Workspace pour Mac.
- Medium : les mises à jour disponibles sont déployées avec une priorité moyenne auprès des utilisateurs comme déterminé par l'application Citrix Workspace pour Mac.
- Slow : les mises à jour disponibles sont déployées avec une priorité faible auprès des utilisateurs comme déterminé par l'application Citrix Workspace pour Mac.

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 lors de l'utilisation d'un VDA Windows ou Linux. 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. Les utilisateurs travaillant en japonais, chinois ou coréen peuvent utiliser le serveur IME. 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 fonctionne dans la session uniquement lorsque le basculement dans le 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.

Prise en charge de la disposition du clavier pour VDA Windows

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	

Prise en charge de la disposition du clavier pour VDA Linux

Language in MAC	Input Source in MAC
English	US.
	U.S. International - PC
	Dvorak
	Dvorak - Left
	Dvorak - Reft
	British
	British - PC
	Candian English
	Australian
	Irish
French	French
	French - Numerical
	Canadian French - CSA
	Swiss French
	French - PC
German	German
	Austrian
	Swiss German
Spanish	Spanish
	Spanish - ISO
Swedish	Swedish
Czech	Czech
Danish	Danish
Finnish	Finnish
Hungarian	Hungarian
Italian	Italian
Greek	Greek
Dutch	Belgian
	Dutch
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
Polish	Polish Pro
Icelandic	Icelandic
Norwegian	Norwegian
Japanese	Hiragana
	Katakana
	Romaji
Korean	2-Set Korean
	3-Set Korean
Chinese, Simplified	Pinyin -Simplified
Chinese, Traditional	Pinyin - Traditional

L'éditeur IME client amélioré dépend de la fonctionnalité de synchronisation de disposition du clavier. Par défaut, la fonctionnalité 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 Workspace**/, localisez le paramètre « **EnableIMEEnhancement** » et activez ou désactivez la fonctionnalité en définissant la valeur sur « true » ou « false » respectivement.

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

Barre de langue

Vous pouvez choisir d'afficher ou de masquer la barre de langue distante dans une session d'application à l'aide de l'interface utilisateur graphique. La barre de langue affiche la langue d'entrée préférée dans une session. Dans les versions antérieures, vous pouviez modifier ce paramètre en utilisant uniquement les clés de registre du VDA. À partir de Citrix Workspace pour Mac version 1808, vous pouvez modifier les paramètres à l'aide de la boîte de dialogue **Préférences**. La barre de langue apparaît dans une session par défaut.

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

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

1. Ouvrez Préférences.
2. Cliquez sur Clavier.
3. Cochez ou décochez Afficher la barre de langue distante pour les applications publiées.

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

Citrix Casting

Citrix Casting est utilisé pour diffuser votre écran Mac sur des appareils Citrix Ready Workspace Hub à proximité. L'application Citrix Workspace pour Mac prend en charge Citrix Casting pour refléter votre écran Mac sur des moniteurs connectés à Workspace Hub.

Pour de plus amples informations, consultez la documentation de Citrix Ready Workspace Hub.

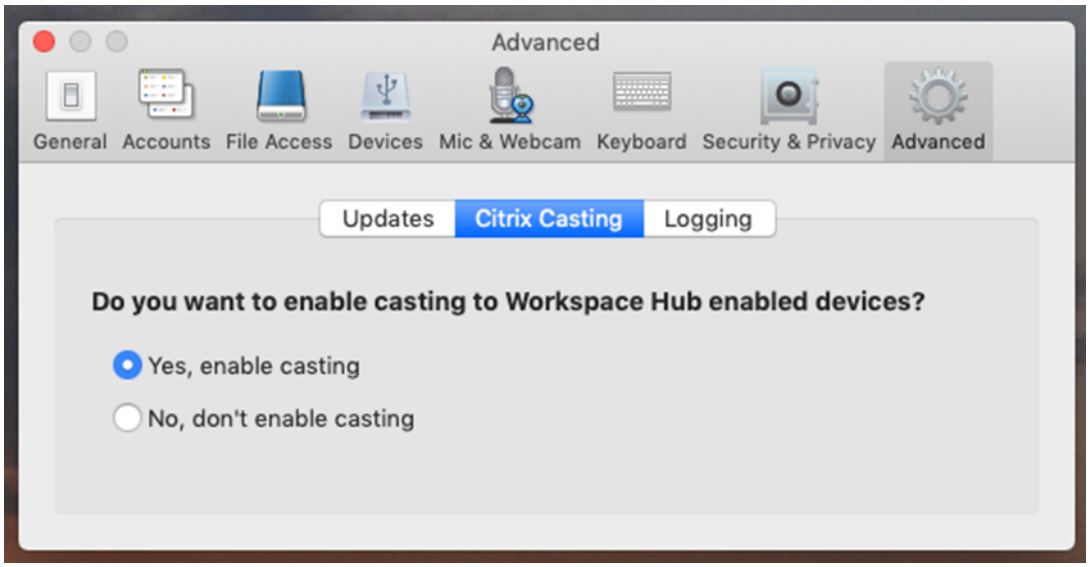
Conditions préalables

- Application Citrix Workspace 1812 pour Mac ou version ultérieure.
- Bluetooth doit être activé sur l'appareil pour la détection de Workspace Hub.
- Citrix Ready Workspace Hub et l'application Citrix Workspace doivent se trouver sur le même réseau.
- Assurez-vous que le port 55555 n'est pas bloqué entre l'appareil exécutant l'application Citrix Workspace et Citrix Ready Workspace Hub.
- Le port 55556 est le port par défaut pour les connexions SSL entre les appareils mobiles et le Citrix Ready Workspace Hub. Vous pouvez configurer un port SSL différent sur la page des paramètres de la plate-forme Raspberry Pi. Si le port SSL est bloqué, les utilisateurs ne peuvent pas établir de connexions SSL avec Workspace Hub.
- Pour Citrix Casting, assurez-vous que le port 1494 n'est pas bloqué.

Activer Citrix Casting

Citrix Casting est désactivé par défaut. Pour activer Citrix Casting à l'aide de l'application Citrix Workspace pour Mac :

1. Accédez à **Préférences**.
2. Sélectionnez **Avancé** dans le panneau, puis choisissez **Citrix Casting**.
3. Sélectionnez **Oui, activer la diffusion**.



Une notification s'affiche lorsque Citrix Casting est lancé et une icône Citrix Casting apparaît dans la barre de menus.

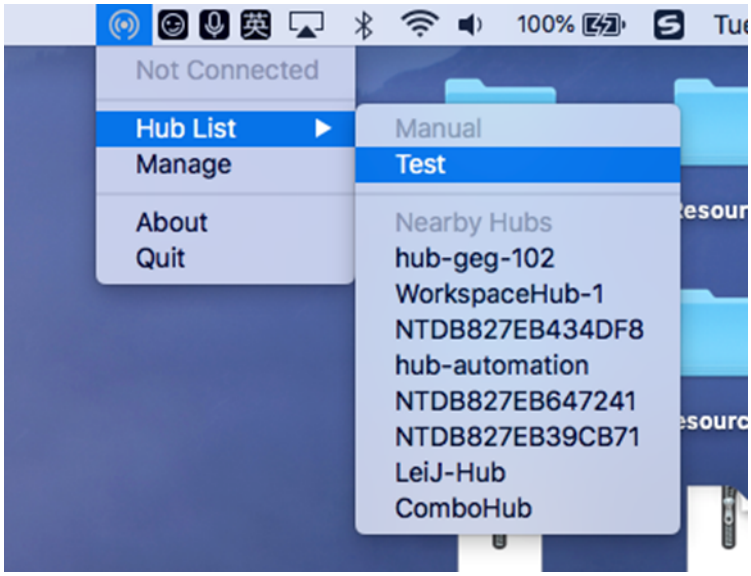
> **Remarque :**
>
> Après l'activation, Citrix Casting se lance automatiquement avec l'application Citrix Workspace

> pour Mac jusqu'à ce que vous désactiviez la diffusion en sélectionnant **Non, ne pas activer la diffusion** dans **Préférences > Avancé > Citrix Casting**.

Détecter automatiquement les appareils Workspace Hub

Pour vous connecter automatiquement aux appareils Workspace Hub :

1. Sur votre Mac, connectez-vous à l'application Citrix Workspace et assurez-vous que Bluetooth est activé. Le Bluetooth est utilisé pour découvrir les appareils Workspace Hub à proximité.
2. Sélectionnez l'icône **Citrix Casting** dans la barre de menus. Toutes les fonctions Citrix Casting sont gérées via ce menu.
3. Le sous-menu **Liste des hubs** affiche tous les appareils Workspace Hub situés à proximité sur le même réseau. Les hubs sont répertoriés dans l'ordre décroissant de leur proximité avec votre Mac et affichent leurs noms configurés pour Workspace Hub. Tous les hubs détectés automatiquement s'affichent sous **Hubs à proximité**.
4. Choisissez le hub auquel vous souhaitez vous connecter en sélectionnant son nom.



Pour annuler la sélection d'un Workspace Hub pendant la connexion, sélectionnez **Annuler**. Vous pouvez aussi utiliser **Annuler** si la connexion réseau est mauvaise et que la connexion prend plus de temps que d'habitude.

> **Remarque :**
>
> Parfois, le hub choisi peut ne pas apparaître dans le menu. Vérifiez à nouveau le menu **Liste des hubs** après quelques instants ou ajoutez votre hub manuellement. Citrix Casting reçoit la diffusion du Workspace Hub périodiquement.

Détecter manuellement les appareils Workspace Hub

Si vous ne trouvez pas le périphérique Citrix Ready Workspace Hub dans le menu **Liste des hubs**, ajoutez l'adresse IP du Workspace Hub pour y accéder manuellement. Pour ajouter un Workspace Hub :

1. Sur votre Mac, connectez-vous à l'application Citrix Workspace et assurez-vous que Bluetooth est activé. Le Bluetooth est utilisé pour découvrir les appareils Workspace Hub à proximité.
2. Sélectionnez l'icône **Citrix Casting** dans la barre de menus.
3. Sélectionnez **Gérer** dans le menu. La fenêtre **Gérer les hubs** s'affiche.
4. Cliquez sur **Ajouter** pour entrer l'adresse IP de votre hub.
5. Après avoir ajouté le périphérique, la colonne **Nom du Hub** affiche le nom convivial du hub. Utilisez ce nom pour identifier le hub dans la section **Manuel** du sous-menu **Liste des hubs**.

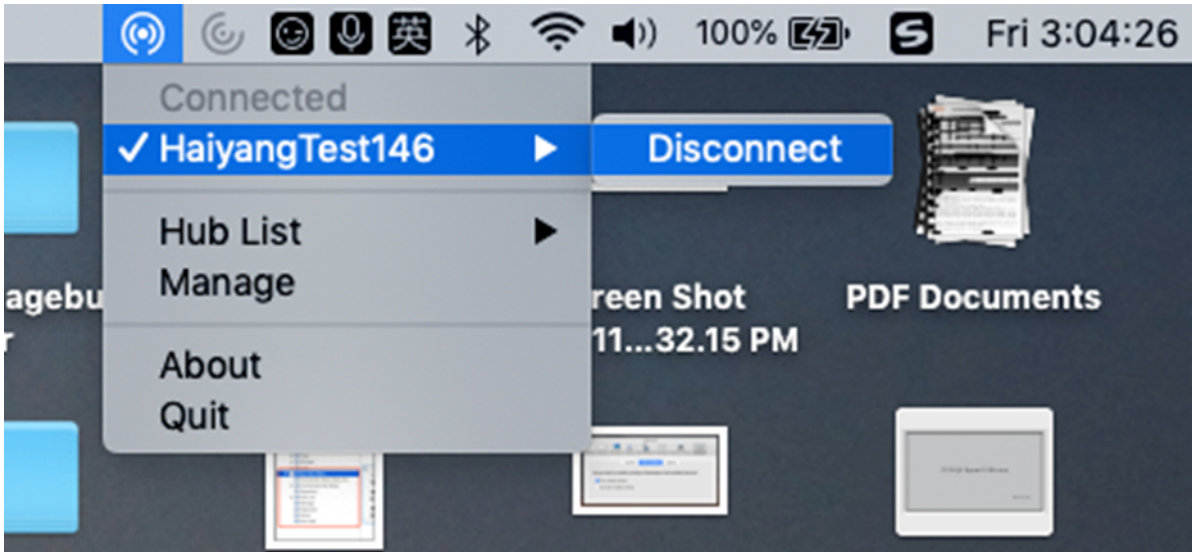
> **Remarque :**
>
> Actuellement, seul le mode **Miroir** est pris en charge. **Miroir** est le seul choix disponible dans la colonne **Mode d'affichage**.

Déconnecter le périphérique Workspace Hub

Vous pouvez déconnecter votre session actuelle et quitter Citrix Ready Workspace Hub automatiquement ou manuellement.

- Pour déconnecter automatiquement la session de casting, fermez votre ordinateur portable.
- Pour déconnecter manuellement la session de casting :

1. Sélectionnez l'icône **Citrix Casting**.
2. Dans la liste des hubs, sélectionnez le nom de votre Workspace Hub. Une option **Déconnecter** apparaît à droite.
3. Sélectionnez **Déconnecter** pour déconnecter le hub.



Problèmes connus

- Il existe de petits problèmes de latence lors de l'affichage de l'écran en miroir. Dans des conditions de réseau médiocres, la latence peut être encore plus longue.
- Lorsque SSL est activé dans un Citrix Ready Workspace Hub et que le certificat du hub n'est pas approuvé, une fenêtre d'alerte s'affiche. Pour résoudre le problème, ajoutez le certificat à votre liste de certificats approuvés à l'aide du trousseau.

Entrée microphone côté client

L'application Citrix Workspace pour Mac prend en charge de multiples entrées microphone du côté client. Les micros installés localement peuvent être utilisés pour :

- les événements en direct, tels 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 l'application Citrix Workspace pour Mac.

Vous pouvez sélectionner si vous souhaitez utiliser 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 l'**application Citrix Workspace 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 et vous invite à choisir si vous voulez utiliser votre micro dans la session.

Touches spéciales Windows

L'application Citrix Workspace pour Mac fournit plusieurs options et 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 envoyer la combinaison Commande-touche de caractère en tant que combinaison Ctrl+touche de caractère au sein d'une session. Sélectionnez « Commande ou Contrôle » dans le menu déroulant pour 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 et 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. Toutefois, 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. Pour ce faire, cochez la case « Envoyer les touches spéciales inchangées ». Cette case n'étant pas sélectionnée par défaut, l'option 1 est envoyée 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
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. Le système d'exploitation Mac les interprète. 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. Les claviers Mac ne simulent pas ces raccourcis. Toutefois, ils peuvent être envoyés au bureau distant ou à l'application 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 l'application Citrix Workspace pour Mac propose plusieurs choix de manière à garantir l'envoi des frappes clavier aux applications et bureaux hébergés. Ces frappes figurent dans le tableau. Le comportement par défaut est décrit. Si vous modifiez les paramètres par défaut (à l'aide de l'application Citrix Workspace pour Mac ou d'autres préférences), différentes combinaisons de frappes clavier peuvent être envoyées et un comportement différent peut être observé sur Remote PC Access.

> **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 permettent de saisir du texte et incluent toutes les lettres, les chiffres et les signes de ponctuation. Les touches spéciales sont celles qui ne permettent pas de saisir du texte, mais agissent comme modificateurs ou contrôleurs. 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) d'un clavier Mac. La touche de fonction fait référence à 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

Touche Windows ou combinaison de touches	Équivalents sur Mac
Ctrl+Alt+Suppr	Contrôle-Option-Fn-Commande-Supprimer ; 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
Accueil	Accueil ; 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
Tab	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

L'application Citrix Workspace 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.

L'application Citrix Workspace 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

L'application Citrix Workspace 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.

Moniteurs multiples

Les utilisateurs peuvent configurer l'application Citrix Workspace pour Mac afin de travailler en mode plein écran sur plusieurs moniteurs.

1. Sélectionnez Desktop Viewer et cliquez sur la flèche vers le bas.
2. Sélectionnez **Fenêtre**.
3. Faites glisser l'écran Citrix Virtual Desktops entre les moniteurs. Assurez-vous qu'environ la moitié de l'écran est présent dans chaque moniteur.
4. Dans la barre d'outils de Citrix Virtual Desktops, sélectionnez **Plein écran**.

L'écran est maintenant étendu sur tous les moniteurs.

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.
- Citrix recommande d'utiliser un maximum de 2 moniteurs. L'utilisation de plus de 2 moniteurs peut dégrader les performances de la session ou entraîner des problèmes d'accessibilité.

Barre d'outils de bureau

Les utilisateurs peuvent maintenant accéder à la barre d'outils du **bureau** en mode fenêtre et plein écran. Auparavant, la barre d'outils était uniquement visible en mode plein écran. Autres 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.

  - 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.

Contrôle de l'espace de travail

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, un membre du personnel se déconnecte d'un appareil utilisateur dans la salle d'urgence d'un hôpital, puis se connecte à un poste de travail du laboratoire de radiographie de l'hôpital. Les stratégies, les mappages d'imprimante et les mappages de lecteur client appropriés pour la session dans le laboratoire de radiographie sont mis en œuvre lorsque l'utilisateur ouvre une session sur l'appareil utilisateur dans le laboratoire de radiographie.

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 l'application Citrix Workspace pour Mac et choisissez **Préférences**.
2. Cliquez sur l'onglet **Général**.
3. Sélectionnez l'une des options suivantes :
   - Reconnecter les applications lorsque je démarre Citrix Workspace. Permet aux utilisateurs de se reconnecter aux applications déconnectées lorsqu'ils démarrent l'application Citrix Workspace.
   - 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 l'application Citrix Workspace pour Mac.

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.

L'application Citrix Workspace 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 l'application Citrix Workspace pour Mac.

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

1. Sur la page d'accueil de l'application Citrix Workspace pour Mac, cliquez sur l'icône de la flèche vers le bas et cliquez sur **Préférences**.
2. Cliquez sur **Accès aux fichiers**.
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.

Authentification

August 14, 2020

Carte à puce

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

- Authentification par carte à puce à Workspace pour Web ou StoreFront 2.x et version ultérieure
- Citrix Virtual Apps and Desktops 7 1808 et version ultérieure
- XenDesktop 7.1 et version ultérieure ou XenApp 6.5 et version ultérieure
- Applications compatibles avec les cartes à puce, telles que Microsoft Outlook et Microsoft Office. Elles permettent aux utilisateurs de signer ou de crypter numériquement des documents disponibles dans les sessions de bureau virtuel ou d'application.

- L'application Citrix Workspace 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 l'application Citrix Workspace pour Mac.
- Pour les sessions double-hop, une connexion supplémentaire est établie entre l'application Citrix Workspace pour Mac et le bureau virtuel de l'utilisateur.

À propos de l'authentification par carte à puce auprès de Citrix Gateway

Il existe plusieurs certificats disponibles lorsque vous utilisez une carte à puce pour authentifier une connexion. L'application Citrix Workspace pour Mac vous invite à sélectionner un certificat. Lors de la sélection d'un certificat, l'application Citrix Workspace pour Mac vous invite à saisir le mot de passe de la carte à puce. Une fois l'authentification effectuée, la session démarre.

S'il n'existe qu'un seul certificat approprié sur la carte à puce, l'application Citrix Workspace 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 Workspace à Citrix 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 l'application Citrix Workspace pour Mac, 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 souhaité n'est pas répertorié.
5. Après avoir sélectionné le module approprié, cliquez sur **Ajouter**.

Lecteurs, middleware et cartes à puce pris en charge

L'application Citrix Workspace 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 :

- Clarify
- Version du client ActivIdentity
- 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.
- L'application Citrix Workspace pour Mac n'enregistre pas le certificat choisi par l'utilisateur.
- L'application Citrix Workspace pour Mac ne stocke et n'enregistre pas le code PIN de la carte à puce de l'utilisateur. Le système d'exploitation gère l'acquisition du code PIN, qui peut disposer de son propre mécanisme de mise en cache.
- L'application Citrix Workspace 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, vous devez installer le plug-in Citrix Gateway et ouvrir une session via une page Web. Utilisez vos cartes à puce et vos codes PIN pour vous authentifier à chaque étape. L'authentification pass-through à StoreFront avec Citrix Gateway Plug-in n'est pas disponible pour les utilisateurs de cartes à puce.

Sécuriser les communications

May 24, 2021

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

> **Remarque :**
>
> Citrix recommande d'utiliser Citrix Gateway pour sécuriser les communications entre les

> serveurs StoreFront et les appareils 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 Workspace et les serveurs. L'application Citrix Workspace pour Mac prend en charge les protocoles de proxy SOCKS et de proxy sécurisé.
- Citrix Secure Web Gateway. Vous pouvez utiliser Citrix Secure Web Gateway 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 l'application Citrix Workspace 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.

> **Remarque :**
>
> À partir de macOS Catalina, Apple impose des exigences supplémentaires pour les certificats d'autorité de certification racines et les certificats intermédiaires que les administrateurs doivent configurer. Pour plus d'informations, consultez l'article HT210176 du support Apple.

Citrix Gateway

Pour permettre aux utilisateurs distants de se connecter à votre déploiement XenMobile via Citrix Gateway, vous pouvez configurer Citrix Gateway 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 Citrix Gateway en intégrant Citrix Gateway avec 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 l'application Citrix Workspace pour Mac.

Connexion avec Citrix Secure Web Gateway

Si Citrix Secure Web Gateway Proxy 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 de XenApp et Citrix Secure Web Gateway.

Si vous utilisez le mode Relais, le serveur Citrix Secure Web Gateway fonctionne comme un serveur proxy. Dans ce cas, vous devez configurer l'application Citrix Workspace pour Mac pour qu'elle utilise

:

- le nom de domaine complet du serveur Citrix Secure Web Gateway ;
- le numéro de port du serveur Citrix Secure Web Gateway. Citrix Secure Web Gateway version 2.0 ne prend pas en charge le mode Relais.

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 (`example.com`) est 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 l'application Citrix Workspace pour Mac et les serveurs. L'application Citrix Workspace pour Mac prend en charge les protocoles de proxy SOCKS et de proxy sécurisé.

Lorsque l'application Citrix Workspace pour Mac communique avec le serveur Web, elle utilise les paramètres de serveur proxy configurés pour le navigateur Web par défaut sur la machine utilisateur. Configurez 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. L'application Citrix Workspace 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 pour un serveur Web sécurisé) pour les communications entre la machine utilisateur et le serveur Web. Pour les communications entre Citrix Workspace et le serveur Citrix, le pare-feu doit autoriser le trafic ICA entrant sur les ports 1494 et 2598.

TLS

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.

L'application Citrix Workspace 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.

> **Remarque**
>
> L'application Citrix Workspace pour Mac utilise le cryptage de plate-forme (OS X) pour les connexions entre l'application Citrix Workspace pour Mac et StoreFront.

Les suites de chiffrement suivantes sont déconseillées pour une sécurité renforcée :

- Suites de chiffrement avec le préfixe « TLS_RSA_* »
- Suites de chiffrement RC4 et 3DES
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

L'application Citrix Workspace pour Mac ne prend en charge que les suites de chiffrement suivantes :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Pour les utilisateurs DTLS 1.0, l'application Citrix Workspace pour Mac 1910 et versions ultérieures ne prend en charge que la suite de chiffrement suivante :

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Mettez à niveau votre version de Citrix Gateway vers 12.1 ou une version ultérieure si vous souhaitez utiliser DTLS 1.0. Sinon, le protocole TLS sera utilisé conformément à la stratégie DDC.

Les matrices suivantes fournissent des détails sur les connexions réseau internes et externes :

		Direct connections								
		TLS			DTLS v1.0			DTLS v1.2		
Client cipher set	VDA cipher set	Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			Y		
	COM	Y	X	X	Y			Y		
	GOV	Y	Y	Y	Y			Y		
COM	ANY	Y	X	X	Y					
	COM	Y	X	X	Y					
	GOV	Y	X	X	Y					
GOV	ANY	Y	Y	Y	X			Y		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			Y		

		External connections with Citrix Gateway								
		TLS			DTLS v1.0			DTLS v1.2		
Client cipher set	VDA cipher set	Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	Y	Y	Y			X		
COM	ANY	Y	X	X	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	X	X	Y			X		
GOV	ANY	Y	Y	Y	X			X		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			X		

> **Remarque** :
>
> - Utilisez Citrix Gateway 12.1 ou version ultérieure pour que EDT fonctionne correctement. Les anciennes versions ne prennent pas en charge les suites de chiffrement ECDHE en mode DTLS.
> - Citrix Gateway ne prend pas en charge DTLS 1.2. De ce fait, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 et TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ne sont pas pris en charge. Citrix Gateway doit être configuré pour que TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA fonctionne correctement dans DTLS 1.0.

Configuration et activation de l'application Citrix Workspace pour TLS

Deux étapes principales permettent de configurer TLS :

1. Configurez le Relais SSL sur votre serveur Citrix Virtual Apps and Desktops, procurez-vous le certificat serveur approprié et installez-le.

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 une application Citrix Workspace pour Mac sur laquelle TLS est activé et la batterie de serveurs, vous avez besoin d'un certificat racine sur la machine utilisateur. Ce certificat racine vérifie la signature de l'autorité de certification sur le certificat du serveur.

macOS X est fourni avec environ 100 certificats racine commerciaux déjà installés. Vous pouvez cependant 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 macOS 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 l'application Citrix Workspace pour Mac. Vous pouvez configurer certains paramètres TLS utilisés pour les connexions ICA dans l'application Citrix Workspace pour Mac. Ces paramètres ne sont pas exposés dans l'interface utilisateur. Pour les modifier, vous devez exécuter une commande sur l'appareil exécutant l'application Citrix Workspace 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 :

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

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

SecurityAllowedTLSVersions. Ce paramètre spécifie les versions du protocole TLS qui sont 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.

```
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. 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 ou Citrix Secure Web 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 ou Citrix Secure Web 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. Si des informations de révocation sont trouvées pour un certificat, la connexion sera refusée.
- **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. Si des informations de révocation sont trouvées pour un certificat, la connexion sera refusée.

> **Remarque**
>
> Si vous ne configurez pas SSLCertificateRevocationCheckPolicy, FullAccessCheck est utilisé comme valeur par défaut.
>
> ```
> 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 de liste 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 <name> <type> <value>
```

Où :

<name> : nom du paramètre décrit ci-dessus.

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

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

```
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 <name>
```

Où :

<name> : nom du paramètre décrit auparavant.

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

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 :

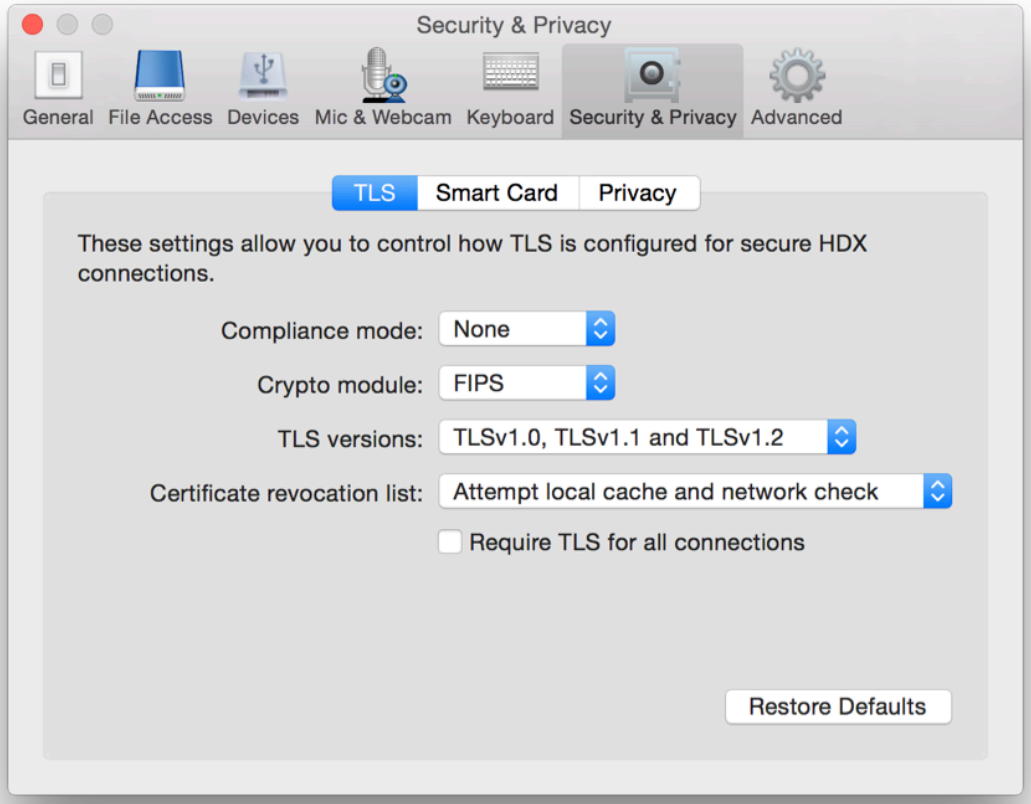
- Interface utilisateur de configuration de la sécurité améliorée. Dans les versions précédentes, la ligne de commande était la méthode préférée pour apporter des modifications liées à la sécurité. Les paramètres de configuration liés à la sécurité de la session sont maintenant simples et accessibles 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. Vous pouvez vérifier les connexions établies avec des serveurs qui utilisent une version de TLS, un algorithme de chiffrement utilisé pour la connexion, un mode, une taille de clé et un état SecureICA spécifiques. 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 suivante illustre les paramètres **Sécurité et confidentialité** accessibles depuis l'interface :



Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States