Application Citrix Workspace pour Mac

Contents

À propos de cette version

August 24, 2022

> **Remarque :**
>
> L'application Citrix Workspace pour Mac 2208 a été annulée en raison d'un bogue. Nous travaillons activement sur un correctif et nous l'annoncerons sous peu.
>
> 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.

Prise en charge native de la puce Apple (M1) [Technical Preview]

L'application Citrix Workspace pour macOS propose désormais une prise en charge native des Mac dotés de la puce Apple (M1) via une architecture universelle. Grâce à l'architecture universelle, l'application Citrix Workspace s'exécute en mode natif sur les ordinateurs Mac dotés de la puce Apple et ceux dotés d'un processeur Intel sans émulation Rosetta. La version Technical Preview fonctionne nativement sur les Mac équipés de puce Apple et doit être installée et testée sur des Mac utilisant des puces M1.

> **Remarque :**
>
> Citrix continue de prendre en charge les Mac basés sur Intel qui utilisent le traducteur binaire dynamique Rosetta 2. Toutefois, Citrix abandonnera bientôt l'application Citrix Workspace pour Mac qui utilise l'émulation Rosetta. Une annonce sera bientôt publiée dans la section Fin de prise en charge.

Vous pouvez télécharger la version architecture universelle à partir de la section **Citrix Workspace App for macOS (Apple silicon) - Universal Architecture** des téléchargements. Si vous utilisez l'application Citrix Workspace sur un Mac exécutant la puce Apple (M1), vous devez mettre à niveau le HDX RealTime Optimization Pack (RTOP). Cela permet d'optimiser les conférences audio-vidéo et une infrastructure de téléphonie d'entreprise VoIP via Microsoft Skype Entreprise. Vous pouvez installer HDX RealTime Media Engine 2.9.500 pour Mac à partir du site Web de Citrix dans les téléchargements.

Si votre entreprise utilise des plug-ins tiers ou des canaux virtuels, vous devez vous assurer que ces plug-ins sont compatibles avec les Mac exécutant la puce Apple. Si les plug-ins sont développés en interne, vous devez les reconstruire avant d'installer la version architecture universelle.

Pour plus d'informations, telles que la désinstallation de la version architecture universelle ou l'utilisation du SDK de canal virtuel personnalisé (VCSDK), consultez la section Prise en charge de la puce Apple [Technical preview].

Nouveautés dans la version 2206.1

Désinstaller l'application en faisant glisser l'icône de l'application Citrix Workspace dans la corbeille

Vous pouvez maintenant simplement faire glisser ou déplacer l'icône de l'application Citrix Workspace dans la corbeille pour désinstaller complètement l'application.

Auparavant, le fait de faire glisser l'icône de l'application Workspace dans la corbeille supprimait l'application mais laissait certains fichiers système sur votre Mac. Dans cette version, l'application Citrix Workspace et tous les fichiers associés sont supprimés de votre appareil lorsque vous faites glisser l'icône vers la corbeille.

Pour désinstaller l'application Citrix Workspace en la faisant glisser vers la corbeille, procédez comme suit :

1. Fermez l'application Citrix Workspace, si elle est en cours d'exécution.
2. Faites glisser l'application Citrix Workspace dans la corbeille.
   Vous pouvez également cliquer avec le bouton droit de la souris sur l'application Citrix Workspace et sélectionner **Options** > **Déplacer vers la corbeille**.
3. Fournissez les informations d'identification de votre système lorsque vous y êtes invité.
4. Fermez toutes les applications en cours d'exécution (Citrix Workspace) et cliquez sur **Continuer** pour confirmer.
   L'application Citrix Workspace et tous ses fichiers système sont supprimés de votre appareil.

Prise en charge de la continuité de service dans le navigateur Safari

La fonctionnalité de continuité de service de Citrix Workspace est désormais prise en charge pour le navigateur Safari. Les utilisateurs doivent installer l'application Citrix Workspace pour Mac et l'extension Web Citrix Workspace. La fonction Continuité du service supprime (ou réduit) la dépendance à l'égard de la disponibilité des composants impliqués dans le processus de connexion. Elle vous permet de vous connecter à vos applications et bureaux virtuels quel que soit l'état de santé des services cloud. Pour plus d'informations sur la fonctionnalité de continuité de service, consultez la section Continuité de service.

Prise en charge améliorée de l'annulation de l'écho audio [Tech Preview]

L'application Citrix Workspace prend désormais en charge l'annulation de l'écho dans les codecs audio adaptatifs et audio hérités. Cette fonctionnalité est conçue pour les cas d'utilisation audio en temps réel et améliore l'expérience utilisateur.
Citrix recommande d'utiliser l'audio adaptatif.

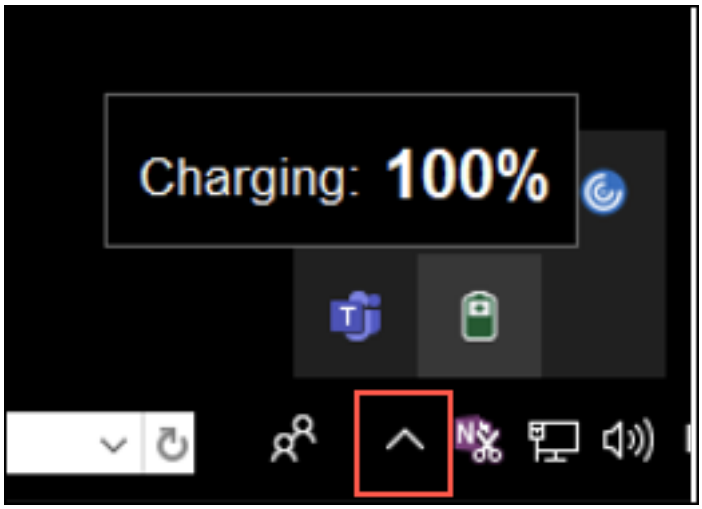
> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en Tech Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est recommandé de ne pas déployer les versions Bêta dans des environnements de production.

Améliorations apportées à Microsoft Teams optimisé

Dans Microsoft Teams optimisé, vous pouvez désormais utiliser la fonction vidéo lorsque plusieurs sessions d'application ou de bureau virtuel sont utilisées.

Indicateur d'état de la batterie [Tech Preview]

L'état de la batterie de l'appareil s'affiche désormais dans la zone de notification d'une session Citrix Desktop.



> **Remarque :**
>
> L'indicateur d'état de la batterie n'apparaît pas pour les VDA du serveur.
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en Tech Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est recommandé de ne pas déployer les versions Bêta dans des environnements de production.

Citrix Workspace Browser

Cette version inclut Citrix Workspace Browser version 101.1.1.14, basé sur Chromium version 101. Pour plus d'informations sur Citrix Workspace Browser, consultez la documentation de Citrix Workspace Browser.

Problèmes résolus dans la version 2206.1

- Le pointeur de la souris est décalé sur les Mac dotés d'un écran à encoche. [CVADHELP-19337]
- Vous n'êtes pas déconnecté de l'application Workspace lorsque la valeur du délai d'inactivité expire. Ce problème se produit par intermittence. [CVADHELP-19812]
- Un message d'erreur peut s'afficher lorsque vous essayez de désinstaller l'application Citrix Workspace. [CVADHELP-19121]
- Dans Microsoft Teams optimisé, la vidéo peut ne pas fonctionner si vous démarrez une autre session d'application ou de bureau virtuel. [HDX-40451]
- Lorsque vous partagez l'écran ou une application pendant un appel Microsoft Teams, votre interlocuteur peut voir des artefacts visuels. Ce problème se produit en raison de fréquences d'images instables, telles que la lecture vidéo incorrecte (images noires figées ou transitoires). Cette version inclut des fréquences d'images ou d'échantillonnage améliorées qui réduisent les artefacts visuels. [HDX-38032]

Problèmes connus dans la version 2206.1

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

Versions précédentes

Cette section répertorie les fonctionnalités des versions précédentes, ainsi que leurs problèmes résolus et connus. Les versions atteignent la fin du cycle de vie 18 mois après la date de publication. Pour plus d'informations sur les dates de cycle de vie des versions prises en charge, consultez Étapes clés du cycle de vie de l'application Citrix Workspace et Citrix Receiver.

2204

Paramètres de Global App Configuration Service pour `allowedWebStoreURLs`

Les administrateurs peuvent désormais utiliser Global App Configuration Service pour configurer les paramètres des magasins Web personnalisés. Les administrateurs peuvent configurer les magasins Web personnalisés à l'aide de la propriété `allowedWebStoreURLs`. Pour plus d'informations sur Global App Configuration Service, consultez la section Mise en route.

Prise en charge de l'ouverture de l'application Citrix Workspace en mode agrandi

Les administrateurs peuvent configurer la propriété `maximise workspace window` dans Global App Configuration Service pour permettre à l'application Citrix Workspace de s'ouvrir en mode agrandi par défaut. Pour plus d'informations sur Global App Configuration Service, consultez la section Mise en route.

Prise en charge des écrans haute résolution [Tech Preview]

L'application Citrix Workspace pour Mac est désormais compatible avec les écrans haute résolution d'une résolution supérieure à 4K. Lors des sessions de bureau, les applications, le texte, les images et les autres éléments graphiques apparaissent dans une taille qui peut être visualisée confortablement sur ces écrans haute résolution.

Pour activer cette fonctionnalité, exécutez la commande suivante dans le terminal macOS :

```
defaults write com.citrix.receiver.nomas EnableHighDPI -bool YES
```

Les administrateurs peuvent modifier la stratégie **Limite de mémoire d'affichage**, qui spécifie la taille maximale du tampon vidéo en kilo-octets pour une session de bureau, en fonction de la résolution d'affichage. La valeur par défaut de la stratégie Limite de mémoire d'affichage est 65536 Ko. Elle est suffisante pour un maximum de 2 moniteurs 4K (2 x 32400 Ko). Les administrateurs doivent modifier cette valeur en accédant à **Citrix Studio** > **Stratégies** > **Limite de mémoire d'affichage** et utiliser une valeur de 393216 Ko pour utiliser cette fonctionnalité.

Pour plus d'informations sur la stratégie Limite de mémoire d'affichage, consultez Limite de mémoire d'affichage.

> **Remarque :**
>
> Cette fonctionnalité fonctionne avec un maximum de deux moniteurs connectés.
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en Tech Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans des environnements de production.

Améliorations apportées aux licences d'accès client (CAL) pour les sessions Bureau à distance

Avec cette version, si vous exécutez des licences d'accès client dans votre environnement pour accéder à des postes de travail distants, lorsque l'ID client est supérieur à 15 caractères, vous pouvez lancer la session Bureau à distance avec une licence permanente.

Pour activer cette fonctionnalité, les administrateurs doivent configurer le fichier **default.**ica en procédant comme suit :

1. Sur le serveur StoreFront, accédez à *C:\inetpub\wwwroot\Citrix<StoreName>\App_Data* et ouvrez le fichier **default.**ica avec un éditeur.
2. Ajoutez la ligne suivante dans la section **[WFClient]** :

```
isRDSLicensingEnabled=On
```

Restaurer les paramètres par défaut du clavier

Si vous avez déjà modifié les préférences de clavier dans l'application Citrix Workspace, vous pouvez désormais restaurer les paramètres par défaut du clavier. Pour rétablir les valeurs par défaut des paramètres du clavier, ouvrez l'application Citrix Workspace, accédez à **Préférences** > **Clavier** et cliquez sur **Restaurer paramètres par défaut**. Cliquez sur **Oui** pour confirmer votre choix.

Compatibilité de la protection des applications avec l'optimisation HDX pour Microsoft Teams

Dans cette version, le partage complet du moniteur ou du bureau est désactivé lorsque la protection des applications est activée pour le groupe de mise à disposition. Lorsque vous cliquez sur **Partager du contenu** dans Microsoft Teams, le sélecteur d'écran supprime l'option **Bureau**. Vous ne pouvez sélectionner l'option Fenêtre pour partager une application ouverte que si la version du VDA est 2109 ou une version supérieure. Si vous êtes connecté à un VDA antérieur à 2019, aucun contenu n'est sélectionnable.

Citrix Workspace Browser

Cette version inclut Citrix Workspace Browser version 99.1.1.8, basé sur Chromium version 99. Pour plus d'informations sur Citrix Workspace Browser, consultez la documentation de Citrix Workspace Browser.

Définir Citrix Workspace Browser comme navigateur par défaut

Vous pouvez désormais définir Citrix Workspace Browser comme navigateur par défaut. Une fois que vous avez défini Citrix Workspace Browser comme navigateur par défaut, tous les liens et applications Web et SaaS s'ouvrent par défaut dans Citrix Workspace Browser.
Pour définir Citrix Workspace Browser comme navigateur par défaut sous macOS, procédez comme suit :

1. Ouvrez Citrix Workspace Browser, cliquez sur l'icône représentant des points de suspension et ouvrez le menu **Paramètres**.
2. Cliquez sur l'option **Navigateur par défaut** dans le volet gauche.

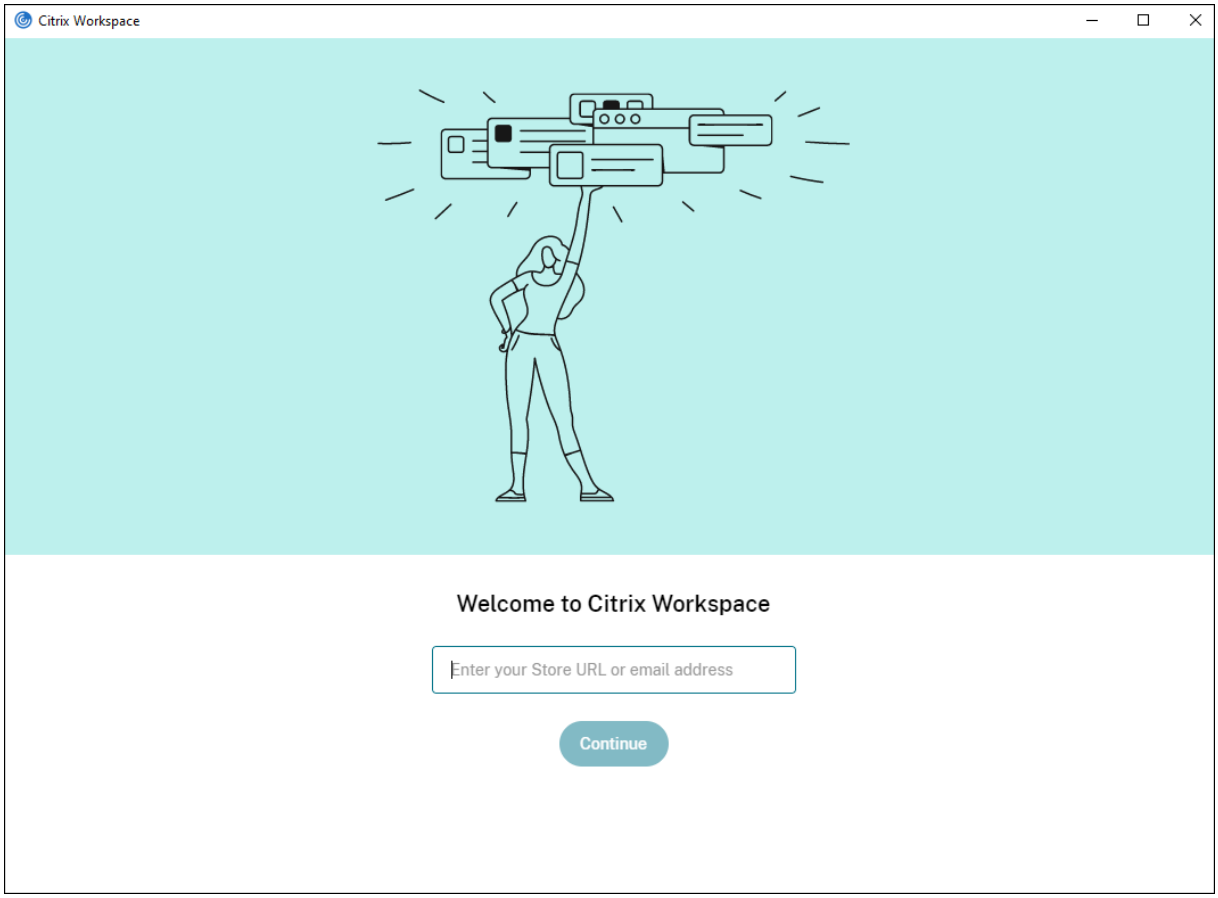
3. Dans la page Navigateur par défaut, cliquez sur **Définir par défaut**. Lorsque vous y êtes invité, cliquez sur **Utiliser Citrix Workspace Browser** pour confirmer votre choix et appliquer les modifications.

Problèmes résolus

- Le pointeur de la souris est décalé sur les Mac dotés d'un écran à encoche. [CVADHELP-19337]
- Vous n'êtes pas déconnecté de l'application Workspace lorsque la valeur du délai d'inactivité expire. Ce problème se produit par intermittence. [CVADHELP-19812]
- Un message d'erreur peut s'afficher lorsque vous essayez de désinstaller l'application Citrix Workspace. [CVADHELP-19121]
- Dans Microsoft Teams optimisé, la vidéo peut ne pas fonctionner si vous démarrez une autre session d'application ou de bureau virtuel. [HDX-40451]
- Lorsque vous partagez l'écran ou une application pendant un appel Microsoft Teams, votre interlocuteur peut voir des artefacts visuels. Ce problème se produit en raison de fréquences d'images instables, telles que la lecture vidéo incorrecte (images noires figées ou transitoires). Cette version inclut des fréquences d'images ou d'échantillonnage améliorées qui réduisent les artefacts visuels. [HDX-38032]

2203.1

Cette version inclut une expérience d'intégration simplifiée et intuitive pour les nouveaux utilisateurs.



Délai d'inactivité pour l'application Citrix Workspace

La fonctionnalité de délai d'inactivité vous déconnecte de l'application Citrix Workspace en fonction d'une valeur définie par l'administrateur. Les administrateurs peuvent spécifier la durée d'inactivité autorisée avant qu'un utilisateur ne soit automatiquement déconnecté de l'application Citrix Workspace. Vous êtes automatiquement déconnecté lorsqu'aucune activité de la souris, du clavier ou d'interaction sur l'écran ne se produit pendant l'intervalle de temps spécifié, dans la fenêtre de l'application Citrix Workspace. Le délai d'inactivité n'affecte pas les sessions Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) déjà en cours d'exécution ni les magasins Citrix StoreFront.

Pour plus d'informations, consultez Délai d'inactivité pour l'application Citrix Workspace.

Impression universelle PDF

Vous pouvez désormais utiliser la fonction d'impression universelle PDF lorsque vous imprimez à partir d'un Mac. Vous n'avez plus besoin d'installer le pilote HP Color LaserJet 2800 Series PS lors de la création automatique d'imprimantes clientes sur un Mac grâce au pilote UPD Citrix.

Pour plus d'informations sur l'utilisation de cette fonctionnalité, reportez-vous à la section Impression.

Expérience d'authentification unique (SSO) améliorée pour les applications Web et SaaS [Technical Preview]

Cette fonctionnalité simplifie la configuration du SSO pour les applications Web internes et les applications SaaS lors de l'utilisation de fournisseurs d'identité tiers (IdP). L'expérience SSO améliorée réduit l'ensemble du processus à quelques commandes. Elle élimine le besoin de configurer Citrix Secure Private Access dans la chaîne du fournisseur d'identité pour configurer SSO. Cela améliore également l'expérience utilisateur, à condition que le même IdP soit utilisé pour l'authentification à la fois auprès de l'application Citrix Workspace et de l'application Web ou SaaS qui est lancée.

Vous pouvez vous inscrire à cette Technical Preview en utilisant ce formulaire Podio.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en Tech Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans les environnements de production.

Prise en charge du protocole TLS (Transport Layer Security) version 1.3 sur les VDA Linux [Technical preview]

Si vous exécutez TLS version 1.3, vous pouvez désormais vous connecter à des applications et bureaux virtuels hébergés sur Linux.

> **Remarque :**
>
> Vous ne pouvez pas vous connecter à des applications et bureaux virtuels Windows si vous exécutez TLS version 1.3.

Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en Tech Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est recommandé de ne pas déployer les versions Bêta dans des environnements de production.

Partager des applications à l'aide de la fonctionnalité « Partager du contenu » de Microsoft Teams

Vous pouvez maintenant partager des applications, des fenêtres ou des fenêtres plein écran individuelles à l'aide de la fonctionnalité de partage d'écran de Microsoft Teams. Citrix Virtual Delivery Agent 2109 est requis pour cette fonctionnalité.
Pour afficher une application spécifique, cliquez sur **Partager du contenu** dans les commandes de votre réunion et sélectionnez l'application. Une fois qu'une bordure rouge apparaît autour de l'application sélectionnée, les participants à l'appel peuvent voir votre application. Si vous réduisez l'application, Microsoft Teams affiche la dernière image de l'application partagée. Agrandissez la fenêtre pour reprendre le partage.

Chat et réunions multi-fenêtres pour Microsoft Teams

Les utilisateurs peuvent désormais utiliser plusieurs fenêtres pour le chat et les réunions dans Microsoft Teams (1.5.00.5967 ou supérieur) grâce à l'optimisation HDX dans Citrix Virtual Apps and Desktops et Citrix DaaS. Les utilisateurs peuvent afficher leurs conversations ou leurs réunions de différentes manières. Pour plus d'informations sur la fonctionnalité pop-out ou multi-fenêtre, consultez Teams Pop-Out Windows for Chats and Meetings sur le site Microsoft Office 365.

Si vous exécutez une ancienne version de l'application Citrix Workspace ou du VDA, notez que Microsoft abandonnera le code de fenêtre unique à l'avenir. Toutefois, vous disposerez d'un minimum de neuf mois pour mettre à niveau vers une version de VDA/CWA qui prend en charge plusieurs fenêtres (2203 ou version ultérieure).

> **Remarque :**
>
> Cette fonctionnalité est disponible uniquement après le déploiement d'une future mise à jour de Microsoft Teams. Pour plus de détails, consultez la feuille de route Microsoft 365.

Donner ou prendre le contrôle dans Microsoft Teams

Vous pouvez utiliser le bouton **Donner le contrôle** pour donner le contrôle de votre écran partagé aux autres utilisateurs participant à la réunion. L'autre participant peut effectuer des sélections et modifier l'écran partagé via le clavier, la souris et le presse-papiers. Vous avez désormais tous les deux le contrôle de l'écran partagé et vous pouvez reprendre le contrôle à tout moment.

Pour prendre le contrôle lors de sessions de partage d'écran, les participants peuvent demander le contrôle via le bouton **Demander le contrôle**. L'utilisateur qui partage l'écran peut alors approuver ou refuser la demande. Lorsque vous avez le contrôle, vous pouvez contrôler les entrées effectuées à l'aide du clavier et de la souris sur l'écran partagé, et abandonner le contrôle pour arrêter le partage du contrôle.

> **Remarque :**
>
> Cette fonctionnalité est disponible uniquement après le déploiement d'une future mise à jour de Microsoft Teams.

Migration de StoreFront vers Workspace

Lorsque votre organisation passe d'une instance StoreFront locale à Workspace, les utilisateurs doivent ajouter manuellement la nouvelle URL de l'espace de travail à l'application Citrix Workspace. Cette fonctionnalité permet aux administrateurs de migrer de manière transparente les utilisateurs d'un magasin StoreFront vers un magasin Workspace avec une interaction utilisateur minimale.

Pour plus d'informations sur cette fonctionnalité, consultez la section Migration de l'URL de StoreFront vers Workspace.

Global App Config Service

Le nouveau Global App Config Service pour Citrix Workspace permet à un administrateur Citrix de fournir les URL du service Workspace et les paramètres de l'application Citrix Workspace via un service géré de manière centralisée.
Pour plus d'informations, consultez la documentation de Global App Configuration Service.

Étendre plusieurs moniteurs en mode plein écran

Vous pouvez désormais passer en mode plein écran simultanément sur deux moniteurs ou plus. Pour utiliser cette fonctionnalité, effectuez les opérations suivantes :

1. Ouvrez Citrix Viewer.
2. Pour utiliser le mode plein écran sur les autres moniteurs connectés, faites glisser la fenêtre de votre moniteur principal pour l'étendre sur les moniteurs connectés. Dans la barre de menus, sélectionnez **Afficher** > **Entrer en mode plein écran**. La fenêtre passe en mode plein écran sur ces moniteurs.

   > **Remarque :**
   >
   > Si vous avez déjà sélectionné l'option **Utiliser tous les affichages en plein écran**, veillez à la désélectionner car elle étend le mode plein écran sur tous les moniteurs connectés.

Citrix recommande d'utiliser un maximum de 3 moniteurs, y compris le moniteur principal.

Citrix Workspace Browser

Cette version inclut Citrix Workspace Browser version 98.1.2.17, basé sur Chromium version 98. Pour connaître les fonctionnalités ou les corrections de bogues dans Citrix Workspace Browser, consultez

Nouveautés dans la documentation de Citrix Workspace Browser.

Problèmes résolus

- Au cours de sessions actives, le filigrane de l'application Citrix Workspace devient transparent et affiche le contenu des fenêtres en arrière-plan. Ce problème se produit uniquement en mode transparent. [CVADHELP-19153]
- Lorsque vous lancez une session à partir d'un VDA (2112 ou supérieur) via un Citrix ADC, votre session peut être interrompue, et la fiabilité de session démarre mais ne vous reconnecte pas. [CVADHELP-19687]
- La boîte de dialogue contextuelle Large File Receive du plug-in Mimecast n'apparaît pas dans Outlook. [HDX-37137]
- Lorsque la valeur de Découverte MTU de chemin (PMTUD) n'est pas 1 500 (par défaut), les utilisateurs ne peuvent pas revenir à TCP dans un environnement cloud Azure. [HDX-37215]
- Vous pouvez rencontrer une utilisation élevée du processeur sur le point de terminaison lorsqu'une webcam est activée dans un appel vidéo Microsoft Teams optimisé. [HDX-37168]
- Dans l'application Citrix Workspace, vous pouvez rencontrer des échecs intermittents lorsque vous répondez ou passez un appel Microsoft Teams. Le message d'erreur suivant s'affiche : « L'appel n'a pas pu être établi. » [HDX-38819]
- Les sessions de l'application Citrix Workspace peuvent ne pas se lancer si Citrix AppFlow est configuré dans Citrix ADC. [HDX-39496]
- Lorsque la mise à jour automatique est désactivée et que vous accédez à **Préférences** > **Avancé**, l'application Citrix Workspace se bloque. [RFMAC-10978]

2201

Migration de StoreFront vers Workspace [Technical preview]

Lorsque votre organisation passe d'une instance StoreFront locale à Workspace, les utilisateurs doivent ajouter manuellement la nouvelle URL de l'espace de travail à l'application Citrix Workspace. Cette fonctionnalité permet aux administrateurs de migrer de manière transparente les utilisateurs d'un magasin StoreFront vers un magasin Workspace avec une interaction utilisateur minimale.

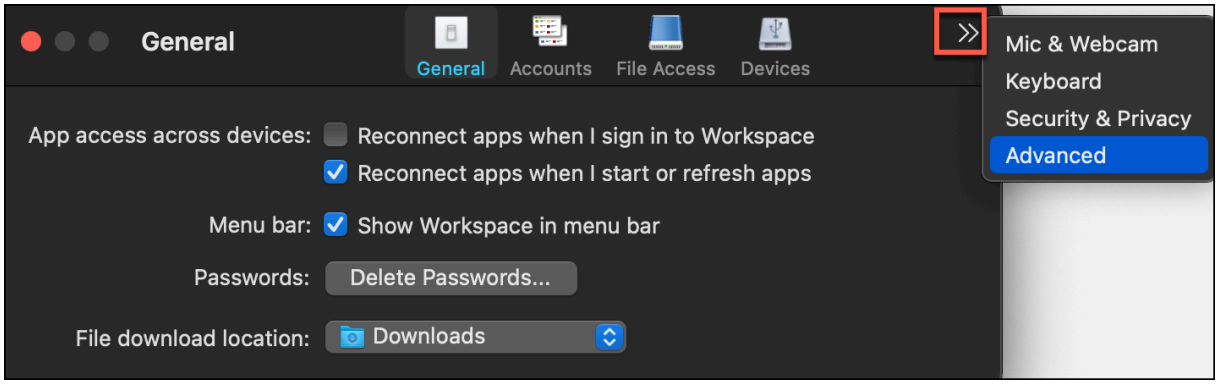
> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en Tech Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur

> gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans les environnements de production.

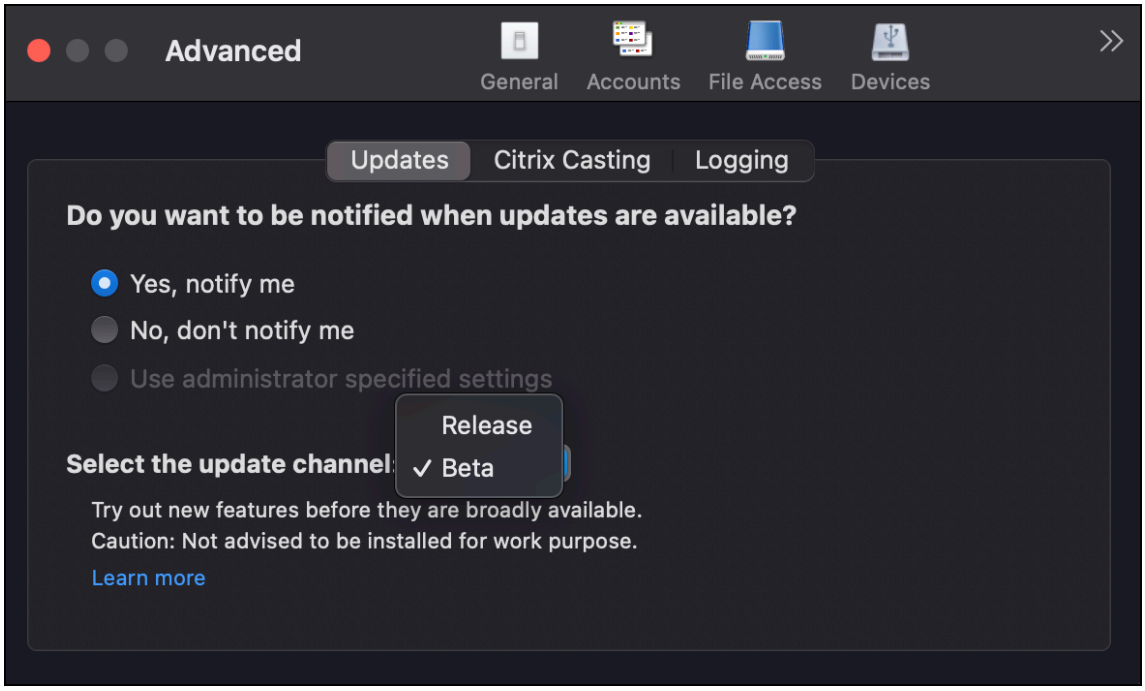
Programme Bêta de l'application Citrix Workspace

À partir de cette version, vous pouvez automatiquement mettre à jour les installations existantes de l'application Citrix Workspace vers les versions Bêta les plus récentes et les tester. Les versions Bêta sont des versions en accès anticipé publiées avant la disponibilité générale d'une mise à jour stable entièrement prise en charge. Vous recevez une notification de mise à jour lorsque l'application Citrix Workspace est configurée pour les mises à jour automatiques.

Pour accéder aux versions Bêta, ouvrez l'application Citrix Workspace, cliquez avec le bouton droit sur Citrix Workspace dans la barre d'outils, puis cliquez sur **Préférences** > **Avancé**. Pour mettre à jour vers des versions Bêta, sélectionnez le **canal Bêta** dans le menu déroulant.



- **Bêta** : version en accès anticipé pour les tests et le signalement de problèmes avant la disponibilité générale.
- **Version** : mise à jour de version stable entièrement prise en charge.



Pour plus d'informations sur l'utilisation de cette fonctionnalité, consultez Mise à jour.

Étendre plusieurs moniteurs en mode plein écran [Technical preview]

Vous pouvez désormais passer en mode plein écran simultanément sur deux moniteurs ou plus. Pour utiliser cette fonctionnalité, effectuez les opérations suivantes :

1. Ouvrez Citrix Viewer.
2. Pour utiliser le mode plein écran sur les autres moniteurs connectés, faites glisser la fenêtre de votre moniteur principal pour l'étendre sur les moniteurs connectés. Dans la barre de menus, sélectionnez **Afficher** > **Entrer en mode plein écran**. La fenêtre passe en mode plein écran sur ces moniteurs.

   > **Remarque :**
   >
   > Si vous avez déjà sélectionné l'option **Utiliser tous les affichages en plein écran**, veillez à la désélectionner car elle étend le mode plein écran sur tous les moniteurs connectés.

Citrix recommande d'utiliser un maximum de 3 moniteurs, y compris le moniteur principal.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en Tech Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur

> gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans les environnements de production.

Problèmes résolus

- Lors de la sélection du texte candidat dans la fenêtre de composition de l'éditeur de méthode d'entrée (IME) à l'aide des flèches gauche ou droite du clavier, le curseur de saisie ne se déplace pas en conséquence. Ce problème se produit lorsque vous lancez un bureau et que la case à cocher **Utiliser la disposition du clavier local, plutôt que la disposition du clavier du serveur distant** est activée dans la fenêtre **Préférences** > **Clavier** de l'application Citrix Workspace. Ce problème n'est observé qu'en chinois et en japonais. [HDX-34956]
- Le pointeur de la souris disparaît par intermittence dans les sessions d'applications Workspace et vous ne pouvez pas cliquer sur quoi que ce soit. [HDX-36820]
- La session de bureau se ferme de façon inattendue lorsque vous faites glisser une cellule dans un tableau croisé dynamique d'une feuille Excel. [HDX-37178]
- Parfois, vous rencontrez des problèmes avec les graphiques dans votre session de bureau après la mise à niveau vers la version 2112 et lorsque les stratégies de codec H.264 sans perte et plein écran sont appliquées. [HDX-37272]
- Après la mise à niveau de l'application Citrix Workspace 2010 vers la version 2112, vous ne pouvez pas vous connecter à des bureaux ou des applications. [RFMAC-10811]

2112

Nouveautés

Prise en charge des magasins Web personnalisés

Vous pouvez maintenant accéder au magasin Web personnalisé de votre organisation à partir de l'application Citrix Workspace pour Mac. Auparavant, vous accédiez à tous les magasins personnalisés uniquement via le navigateur.

L'application Citrix Workspace pour Mac charge les magasins Web personnalisés avec une expérience similaire à celle d'un navigateur et étend les fonctionnalités de protection des applications aux magasins Web personnalisés. Le fait de rendre le portail personnalisé accessible à partir de l'application Citrix Workspace native fournit des capacités et une expérience utilisateur complètes pour cette fonctionnalité. Pour plus d'informations sur Global App Configuration Service, consultez la section Mise en route.

Pour plus d'informations sur la configuration d'un magasin Web personnalisé, consultez Magasin Web personnalisé.

Demander le contrôle dans Microsoft Teams

Avec cette version, vous pouvez demander le contrôle lors d'un appel Microsoft Teams lorsqu'un participant partage l'écran. Une fois que vous avez le contrôle, vous pouvez effectuer des sélections ou des modifications sur l'écran partagé.

Pour prendre le contrôle lorsqu'un écran est partagé, cliquez sur **Demander le contrôle** en haut de l'écran Microsoft Teams. Le participant à la réunion qui partage l'écran peut accepter ou refuser votre demande. Lorsque vous avez terminé, cliquez sur **Abandonner le contrôle**.

Limitation :

L'option **Demander le contrôle** n'est pas disponible pendant les appels poste à poste entre un utilisateur optimisé et un utilisateur sur le client de bureau Microsoft Teams natif qui s'exécute sur le point de terminaison. Pour contourner le problème, les utilisateurs peuvent rejoindre une réunion pour obtenir l'option **Demander le contrôle**.

Appels d'urgence dynamiques

Avec cette version, l'application Citrix Workspace prend en charge les appels d'urgence dynamiques. Lorsque cette fonction est utilisée avec les forfaits d'appel Microsoft, Operator Connect et Direct Routing, elle vous permet d'effectuer les opérations suivantes :

- Configurer et acheminer les appels d'urgence
- Informer le personnel de sécurité

La notification est fournie en fonction de l'emplacement actuel de l'application Citrix Workspace exécutée sur le point de terminaison, au lieu du client Microsoft Teams exécuté sur le VDA. La loi Ray Baum exige que l'emplacement de la personne effectuant l'appel d'urgence soit transmis au centre de réception des appels d'urgence approprié. À partir de l'application Citrix Workspace 2112.1 pour Windows, l'optimisation Microsoft Teams avec HDX est conforme à la loi Ray Baum. Pour plus d'informations sur cette fonctionnalité, consultez la section Prise en charge des appels d'urgence dynamiques dans la section **Système téléphonique Microsoft**.

Impression universelle PDF (version Technical Preview)

La fonctionnalité d'impression universelle PDF est disponible avec la version 2112 de Citrix Virtual Apps and Desktops. Cette fonction est désactivée par défaut. Pour utiliser cette fonctionnalité, vous devez vous inscrire à l'aide de ce formulaire Web. La fonctionnalité est activée une fois que nous recevons vos informations. Vous recevez également des instructions concernant l'utilisation de la fonctionnalité et les stratégies d'impression qui doivent être activées.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en Tech Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans les environnements de production.

Continuité du service

La fonction Continuité du service supprime ou réduit la dépendance à l'égard de la disponibilité des composants impliqués dans le processus de connexion. Les utilisateurs peuvent lancer leurs applications et bureaux virtuels quel que soit l'état d'intégrité des services cloud. Les extensions Web Citrix Workspace mettent la continuité du service à la disposition des utilisateurs qui accèdent à leurs applications et bureaux via un navigateur.

Ensemble, l'application Citrix Workspace et l'extension Web Workspace utilisent des locations de connexion Workspace pour permettre aux utilisateurs du navigateur d'accéder à leurs applications et bureaux pendant les pannes. Pour plus d'informations, consultez Continuité du service.

Citrix Workspace Browser

Cette version du navigateur Workspace Browser est basée sur Chromium version 95. Pour connaître les fonctionnalités ou les corrections de bogues dans Citrix Workspace Browser, consultez Nouveautés dans la documentation de Citrix Workspace Browser.

Problèmes résolus

- L'erreur « Impossible de se connecter au serveur » s'affiche lorsque le protocole de transport passe de Enlightened Data Transport (EDT) à TCP. [CVADHELP-18310]
- Si une application PWA (Progressive Web App) protégée est ouverte sur macOS, les stratégies **Protection des applications** ne sont pas appliquées. [RFMAC-10128]

2111

Nouveautés

- Avec cette version, les utilisateurs ne peuvent pas restaurer manuellement l'application Citrix Workspace pour Mac à une version inférieure à la version installée sur leurs systèmes. Par exemple, si l'application Citrix Workspace version 2109 est installée sur un appareil Mac, vous ne pouvez pas restaurer manuellement l'application à la version 2108 ou inférieure.

- Lancez la session Bureau à distance avec une licence permanente, si vous exécutez des licences d'accès client (CAL) pour accéder à des postes de travail distants. Vous pouvez lancer la session Bureau à distance lorsque l'ID client contient plus de 15 caractères.
- Pour charger le SDK Citrix Virtual Channel sur un Mac exécutant l'application Citrix Workspace 2111, vous devez recompiler vos canaux virtuels personnalisés. Pour plus de détails, consultez Mettre à jour les canaux virtuels personnalisés sur l'application Citrix Workspace pour Mac.

Prise en charge des magasins Web personnalisés [Technical preview]

Avec cette version, vous pouvez accéder au magasin Web personnalisé de votre organisation à partir de l'application Citrix Workspace pour macOS. Pour utiliser cette fonctionnalité, les administrateurs doivent ajouter le magasin Web personnalisé à la liste des URL autorisées dans Global App Configuration Service. Une fois les URL ajoutées, vous pouvez fournir l'URL du magasin Web personnalisé dans l'option Ajouter un compte de l'application Citrix Workspace. Le magasin Web personnalisé s'ouvre dans la fenêtre de l'application Citrix Workspace pour macOS native.

> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en Tech Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans les environnements de production.

Citrix Workspace Browser : pour connaître les nouvelles fonctionnalités ou les corrections de bogues dans Citrix Workspace Browser, consultez Nouveautés dans la documentation de Citrix Workspace Browser.

Problèmes résolus

- Sur les machines exécutant macOS, le codage AAC (Advanced Audio Coding) n'est pas pris en charge. [CTXBR-1844]
- Si vous avez configuré l'application Citrix Workspace à l'aide du fichier `.cr` et que vous vous êtes connecté avec vos informations d'identification, la page d'accueil s'affiche après un délai. [RFMAC-9990]
- Ouvrez une application SaaS protégée, ouvrez un nouvel onglet et séparez le nouvel onglet dans une nouvelle fenêtre en la glissant hors de la barre d'onglets. Organisez ensuite deux fenêtres en regard de l'une de l'autre, ouvrez un nouvel onglet dans la deuxième fenêtre et effectuez une capture d'écran. Vous pouvez également effectuer une capture d'écran de l'application SaaS protégée. [RFMAC-10060]

- Le changement d'un magasin à un autre peut vous déconnecter du premier magasin. [RFMAC-10137]
- Lorsque vous saisissez des informations d'identification incorrectes lors de la connexion à l'application Citrix Workspace, le message d'erreur « Informations d'identification incorrectes » ne s'affiche pas et une invite d'authentification s'affiche à nouveau. Parfois, **Domaine\Utilisateur** apparaît dans l'invite d'authentification au lieu de **Nom d'utilisateur**. [RFMAC-10210]
- Les appels échouent lorsqu'un appel P2P Microsoft Teams optimisé est effectué depuis l'application Citrix Workspace pour Mac 2109 vers l'application Citrix Workspace pour Windows 2109. [HDX-35223]

2109.1

Nouveautés

Prise en charge de macOS Monterey

L'application Citrix Workspace pour Mac est prise en charge sur macOS Monterey (12.0.1).

Problèmes résolus

- Si vous avez ouvert une application protégée, une application SaaS non protégée et une session de bureau protégée, le navigateur se ferme de manière inattendue. Ce problème se produit lorsque vous passez de la fenêtre de session de bureau protégée à l'application SaaS non protégée. [CTXBR-2087]
- Si votre administrateur a installé des extensions externes dans Google Chrome, le navigateur Citrix Workspace Browser se bloque lorsque vous l'ouvrez. [CTXBR-2135]

2109

Nouveautés

> **Remarque :**
>
> Si la continuité du service est activée et que vous mettez à niveau vers la version 2109, les fichiers de location de connexion sont actualisés. Toutes les locations existantes sont supprimées et les nouvelles locations sont récupérées dans le cadre des améliorations apportées aux fonctionnalités.

Application Citrix Workspace pour Mac sur macOS Monterey bêta

L'application Citrix Workspace 2109 pour Mac a été testée sur macOS Monterey bêta 7. Utilisez cette configuration dans un environnement de test et faites-nous part de vos commentaires.

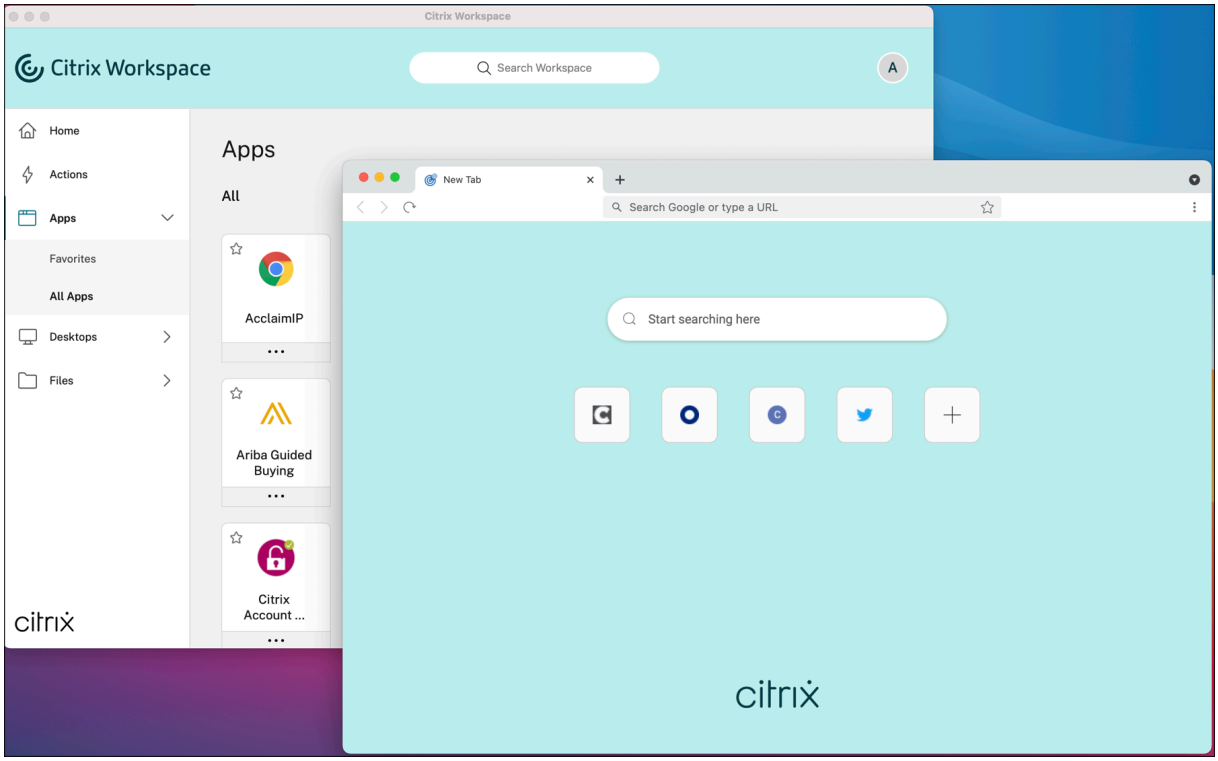
> **Attention** N'utilisez pas l'application Citrix Workspace pour Mac sur les versions macOS Monterey bêta dans des environnements de production.

Découverte automatique du magasin basée sur l'adresse e-mail

Vous pouvez maintenant fournir votre adresse e-mail dans l'application Citrix Workspace pour Mac pour détecter automatiquement le magasin associé à l'adresse e-mail. Si plusieurs magasins sont associés à un domaine, le premier magasin renvoyé par Global App Configuration Service est ajouté par défaut comme magasin de choix. Si nécessaire, les utilisateurs peuvent toujours basculer vers un autre magasin.

Citrix Workspace Browser

Citrix Workspace Browser est un navigateur natif exécuté sur la machine cliente. Il permet aux utilisateurs d'ouvrir des applications Web et SaaS depuis l'application Citrix Workspace de manière sécurisée. Il fournit une interface utilisateur cohérente lors de l'accès à différentes applications Web ou SaaS tout en améliorant votre productivité et en vous offrant des performances optimales dans la restitution de ces applications.



Nos efforts continus pour enrichir l'expérience utilisateur se traduisent par ce nouveau navigateur Workspace qui vous offre une expérience améliorée et native, ainsi que les fonctionnalités suivantes :

- Accès sans VPN aux pages Web internes
- Prise en charge du microphone et de la webcam
- Expérience de navigation à plusieurs onglets
- Affichages multi-fenêtre
- Omnibox modifiable
- Signets
- Raccourcis sur la page d'un nouvel onglet
- Paramètres personnalisables
- Analyse

Les administrateurs peuvent activer des stratégies d'accès privé sécurisé ou des stratégies de protection des applications, y compris la protection contre l'enregistrement de frappe, la prévention de capture d'écran, des restrictions liées au téléchargement, à l'impression et aux Presse-papiers, ainsi que les fonctionnalités de filigrane, selon différentes combinaisons et par URL.

Pour plus d'informations, consultez la documentation du navigateur Citrix Workspace.

Amélioration de l'analyse de point de terminaison (EPA)

À partir de cette version, l'application Citrix Workspace pour macOS prend en charge l'analyse de point de terminaison (EPA). L'analyse de point de terminaison analyse l'appareil à la recherche des exigences de sécurité de point de terminaison configurées sur Citrix Gateway. Lorsque l'analyse est terminée avec succès, l'utilisateur se voit accorder l'accès.

> **Remarque** Cette fonctionnalité ne fonctionne que si vous avez configuré l'authentification nFactor dans votre environnement.

Pour plus d'informations sur l'analyse EPA, consultez Analyses avancées des points de terminaison.

Audio adaptatif

Avec l'audio adaptatif, vous n'avez pas besoin de configurer les stratégies de qualité audio sur le VDA. L'audio adaptatif optimise les paramètres de votre environnement et remplace les anciens formats de compression audio pour offrir une excellente expérience utilisateur. Pour plus d'informations, consultez la section Audio adaptatif.

Prise en charge du codage vidéo avancé H.264 (MPEG-4 AVC) avec Microsoft Teams

Cette version prend en charge le codage/décodage vidéo H.264 avec accélération matérielle, ce qui réduit la charge sur l'utilisation de l'UC et améliore votre expérience de visioconférence. Le moteur multimédia de Citrix Microsoft Teams optimisé HDX (HdxRtcEngine.exe) utilise désormais l'infrastructure Video Toolbox d'Apple pour le codage et le décodage. Cette infrastructure compresse et décompresse la vidéo plus rapidement et en temps réel. En outre, le déchargement du codage et du décodage sur

le GPU est optimisé. Le décodage/codage vidéo avec accélération matérielle est activé par défaut si un périphérique le prend en charge. Cette amélioration réduit la charge sur l'UC lors de l'utilisation de multimédia lorsque Microsoft Teams est optimisé avec HDX.

Problèmes résolus

- Après vous être connecté à l'application Citrix Workspace pour Mac, vous êtes invité à vous authentifier après quelques heures. [RFMAC-10032]
- Lorsque vous ajoutez un magasin dans l'application Citrix Workspace, modifiez le domaine d'authentification dans la console du serveur, laissez l'application inactive pendant quelques minutes, puis ouvrez une session d'application ou de bureau, l'application Citrix Workspace peut se bloquer. [RFMAC-10133]
- Lorsqu'une application ou un bureau virtuel est déjà en cours d'exécution et que vous démarrez une autre application ou un autre bureau virtuel, Citrix Viewer s'affiche mais l'application virtuelle ne s'ouvre pas. Ce problème se produit sur les appareils exécutant macOS 11.6. [RFMAC-10134]

2108.1

Nouveautés

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

Problèmes résolus

Lorsqu'une application ou un bureau virtuel est déjà en cours d'exécution et que vous démarrez une autre application ou un autre bureau virtuel, Citrix Viewer s'affiche mais l'application virtuelle ne s'ouvre pas. Ce problème se produit sur les appareils exécutant macOS 11.6. [RFMAC-10134]

2108

Nouveautés

L'application Citrix Workspace pour Mac prend désormais en charge la découverte MTU (unité de transmission maximale) dans Enlightened Data Transport (EDT). Cela augmente la fiabilité et la compatibilité du protocole EDT et optimise l'expérience utilisateur.

> **Remarque :**
>
> La découverte MTU EDT est prise en charge sur macOS Big Sur et versions ultérieures.

Problèmes résolus

- Il y a un décalage vidéo pendant les conférences téléphoniques dans Microsoft Teams. [HDX-32603]
- Sur les clients Mac exécutant macOS Big Sur, une erreur de serveur interne HTTP 404 ou HTTP/1.1 peut se produire. Le problème se produit lors de la tentative de reconnexion à des sessions. [RFMAC-9448]

2107

Nouveautés

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

Problèmes résolus

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

2106

Nouveautés

Prise en charge des URL personnalisées grâce aux redirections 301

Vous pouvez désormais ajouter des URL qui redirigent vers Citrix Workspace à partir de StoreFront ou Citrix Gateway via des redirections HTTP 301.

Si vous effectuez une migration de StoreFront vers Citrix Workspace, vous pouvez rediriger l'URL StoreFront vers une URL Citrix Workspace via une redirection HTTP 301. Par conséquent, lors de l'ajout d'une ancienne URL StoreFront, vous êtes automatiquement redirigé vers Citrix Workspace.

Exemple de redirection :

L'URL StoreFront : `https://< Citrix Storefront url>/Citrix/Roaming/Accounts` peut être redirigée vers une URL Citrix Workspace : `https://<Citrix Workspace url>/Citrix/Roaming/Accounts`.

> **Remarque :**
>
> - L'application Citrix Workspace pour Mac ne prend pas en charge DTMF (Dual Tone Multi Frequency) avec Microsoft Teams en raison de modifications en attente de Microsoft.
> - À partir de cette version, le numéro de version de Citrix Viewer et le numéro de version de l'application Citrix Workspace peuvent ne pas correspondre. Ce changement n'affecte pas

> votre expérience.

Continuité du service

La fonction Continuité du service supprime ou réduit la dépendance à l'égard de la disponibilité des composants impliqués dans le processus de connexion. Les utilisateurs peuvent lancer leurs applications et bureaux virtuels quel que soit l'état d'intégrité des services cloud.

Pour plus d'informations, consultez la section Continuité du service dans la documentation de Citrix Workspace.

Améliorations apportées à Microsoft Teams

Lorsque **Desktop Viewer** est en mode plein écran, l'utilisateur peut sélectionner un écran à partager parmi tous les écrans couverts par **Desktop Viewer**. En mode fenêtre, l'utilisateur peut partager la fenêtre de **Desktop Viewer**. En mode transparent, l'utilisateur peut sélectionner un écran parmi les écrans connectés au terminal.
Lorsque Desktop Viewer modifie le mode de fenêtre (agrandir, restaurer ou réduire), le partage d'écran s'arrête.

Lorsque l'utilisateur souhaite partager l'écran, des aperçus de tous les écrans disponibles apparaissent dans le panneau de partage d'écran, ce qui permet de faciliter la sélection de l'écran approprié à partir des aperçus.

Problèmes résolus

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

2104

Nouveautés

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.

Problèmes résolus

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

2102

Nouveautés

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

Problèmes résolus

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

2101

Nouveautés

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 l'article du support 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 Citrix 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.

Problèmes résolus

- 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]

2012

Nouveautés

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.

Problèmes résolus

- 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 Citrix Workspace pour Mac peuvent échouer en raison de problèmes avec l'authentification unique. [RFMAC-4477]

Problèmes connus

Problème connu dans la version 2204

- Lorsque le trafic est acheminé par tunnel via NGS, l'application Citrix Workspace peut ne pas pouvoir charger ou télécharger des fichiers dont la taille est supérieure à 64 Mo. [CTXBR-3354]

Problèmes connus dans la version 2203.1

- Vous ne pouvez pas cliquer sur le bouton **Créer** dans l'application Jira tant que la fenêtre du navigateur n'est pas agrandie. [CTXBR-1976]
- Les connexions à des sockets Web ne sont pas tunnelisées via Citrix Secure Private Access. [CTXBR-2439]
- Après la mise à niveau de l'application Citrix Workspace vers la version 2203, une icône de point d'interrogation apparaît sur l'icône de Citrix Workspace Browser. Ce problème se produit si le navigateur Workspace a été épinglé sur le dock avant la mise à niveau. [CTXBR-2864]
- Lorsque vous cliquez sur l'option **Rétablir les paramètres** dans la section des paramètres **avancés** de Citrix Workspace Browser, les paramètres du journal ne sont pas rétablis par

défaut. Pour contourner le problème, cliquez sur l'option **Rétablir les paramètres de journal par défaut** disponible sur la page **Journaux**. [CTXBR-2929]

- Après la mise à niveau de Citrix Workspace Browser version 2201 vers la version 2203, les mots de passe précédemment enregistrés sont perdus et vous ne pouvez pas en enregistrer de nouveaux. [CTXBR-3063]
- Le mode plein écran n'est pas disponible sur les Mac affichant une encoche. [CVADHELP-19337]
- Lorsque vous lancez une session de bureau ou d'application à l'aide du navigateur, la fenêtre de session s'ouvre en arrière-plan, derrière la fenêtre du navigateur. [RFMAC-11362]

Problèmes connus dans la version 2201

- Le nom du client s'affiche avec des caractères aléatoires dans Citrix Broker Service et Citrix Director si vous utilisez l'application Citrix Workspace en mode hors connexion (intranet). [RFMAC-10842]

Problèmes connus dans la version 2112

- Dans l'application Citrix Workspace, vous pouvez rencontrer des échecs intermittents lorsque vous répondez ou passez un appel Microsoft Teams. Le message d'erreur suivant s'affiche : « L'appel n'a pas pu être établi. » [HDX-38819]

Problèmes connus dans la version 2111

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

Problèmes connus dans la version 2109.1

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

Problèmes connus dans la version 2109

- Si vous avez configuré l'application Citrix Workspace à l'aide du fichier `.cr` et que vous vous êtes connecté avec vos informations d'identification, la page d'accueil s'affiche après un délai. [RFMAC-9990]
- Si une application PWA (Progressive Web App) protégée est ouverte sur macOS, les stratégies *Protection des applications* ne sont pas appliquées. [RFMAC-10128]
- Lorsque vous ajoutez des magasins dans l'application Citrix Workspace, que vous modifiez **Période de réauthentification actuelle** dans **Période de réauthentification de l'application**

Workspace et que vous passez de l'application locale au magasin cloud au bout de quelques minutes, vous êtes déconnecté du magasin de cloud et une invite d'authentification s'affiche. Une fois que vous vous connectez à l'application Citrix Workspace, le compteur reste affiché et vous ne pouvez pas vous connecter. [RFMAC-10140]

Problèmes connus dans la version 2108.1

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

Problèmes connus dans la version 2108

Lorsque vous démarrez une application SaaS à laquelle vous êtes abonné après avoir modifié le domaine d'authentification dans la console du serveur, la session ne démarre pas et le message d'erreur suivant s'affiche :

« AuthDomain a été modifié. Veuillez vous reconnecter après un certain temps » [RFMAC-9616]

Problèmes connus dans la version 2107

Lorsque vous modifiez le domaine d'authentification dans la console du serveur et que vous vous connectez avec vos informations d'identification, le message d'erreur suivant s'affiche :

« Impossible de se connecter au serveur »

Vous pouvez accéder au magasin après avoir cliqué sur **OK**. [RFMAC-9494]

Problèmes connus dans la version 2106

Une fenêtre noire apparaît lorsque vous partagez votre écran. [HDX-30083]

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 Citrix 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]

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

Prise en charge native de la puce Apple [Technical preview]

August 18, 2022

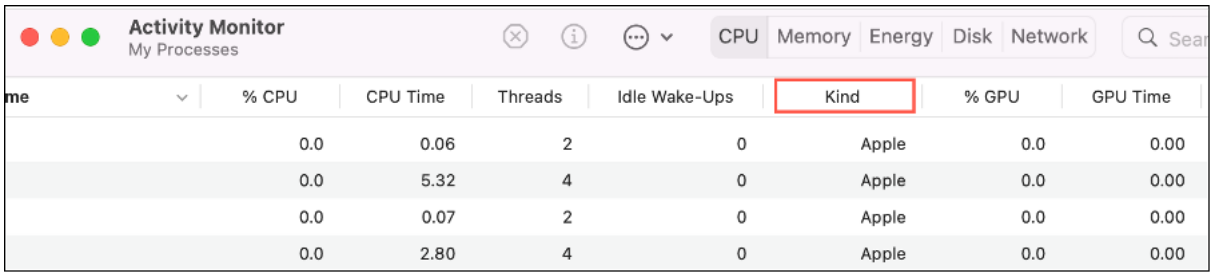
Prise en charge native de la puce Apple (M1) - Architecture universelle

L'application Citrix Workspace pour macOS propose désormais une prise en charge native des Mac dotés de la puce Apple (M1). Par défaut, la version Technical Preview fonctionne en mode natif sur les Mac équipés de puce Apple et doit être installée et testée sur des Mac utilisant des puces M1. Vous pouvez télécharger la version architecture universelle à partir de la section **Citrix Workspace App for macOS (Apple silicon) - Universal Architecture** des téléchargements.

> **Remarque :**
>
> Citrix continue de prendre en charge les Mac basés sur Intel qui utilisent le traducteur binaire dynamique Rosetta 2. Toutefois, Citrix abandonnera bientôt l'application Citrix Workspace pour Mac qui utilise l'émulation Rosetta. Une annonce sera bientôt publiée dans la section Fin de prise en charge.

Si vous utilisez l'application Citrix Workspace sur un Mac exécutant la puce Apple (M1), vous devez mettre à niveau le HDX RealTime Optimization Pack (RTOP) en installant HDX RealTime Media Engine 2.9.500 pour Mac depuis le site Web de Citrix dans Téléchargements.

Pour déterminer si l'application Citrix Workspace s'exécute en mode natif sur la puce Apple, ouvrez le **Moniteur d'activité** sur votre Mac. La colonne intitulée **Type** dans l'onglet **CPU** indique si l'application Workspace est exécutée sur puce Apple ou processeur Intel.



Désinstaller la version architecture universelle et installez l'application Citrix Workspace pour un Mac basé sur Intel

Vous pouvez basculer vers l'application Citrix Workspace pour un Mac basé sur Intel en désinstallant la version architecture universelle. Pour désinstaller l'application Citrix Workspace, consultez la section Désinstallation.

Une fois que vous avez désinstallé l'application, téléchargez la dernière version de l'application Citrix Workspace pour un Mac basé sur Intel dans les téléchargements Citrix et suivez les étapes répertoriées dans la section Installation manuelle.

SDK du canal virtuel Citrix

Le VCSDK du canal virtuel Citrix prend en charge l'écriture de pilotes du côté serveur et du côté client afin de fournir des canaux virtuels supplémentaires à l'aide du protocole ICA. Les applications de canal virtuel côté serveur se trouvent sur des serveurs Citrix Virtual Apps and Desktops. Si vous souhaitez écrire des pilotes virtuels pour d'autres plates-formes clientes, contactez le support technique Citrix.

Le SDK du canal virtuel offre ce qui suit :

- L'interface Citrix Virtual Driver Application Programming Interface (VDAPI) est utilisée avec les fonctions de canal virtuel dans le SDK de l'API Citrix Server (WFAPI SDK) pour créer de nouveaux

canaux virtuels. La prise en charge de canal virtuel fournie par VDAPI est conçue pour faciliter l'écriture de vos propres canaux virtuels.
- L'API de contrôle de Windows, qui améliore l'expérience visuelle et la prise en charge des applications tierces intégrées avec ICA.
- Un code source opérationnel pour exemples de programmes de canal virtuel qui illustrent les techniques de programmation.

Le SDK de canal virtuel requiert le SDK WFAPI pour écrire sur le côté serveur du canal virtuel.

Charger des canaux virtuels personnalisés sur un Mac doté de la puce Apple (M1)

En tant qu'utilisateur final, vous pouvez charger le SDK de canal virtuel personnalisé (VCSDK) sur un Mac doté de la puce M1. Avec une architecture universelle, vous devez charger le VCSDK sur les Mac dotés de la puce Apple en recompilant vos canaux virtuels personnalisés à l'aide du dernier VCSDK sur un appareil à puce M1. Vous pouvez télécharger la version architecture universelle à partir de la section **Virtual Channel SDK 2204 for macOS (Apple silicon) - Universal Architecture** des téléchargements.

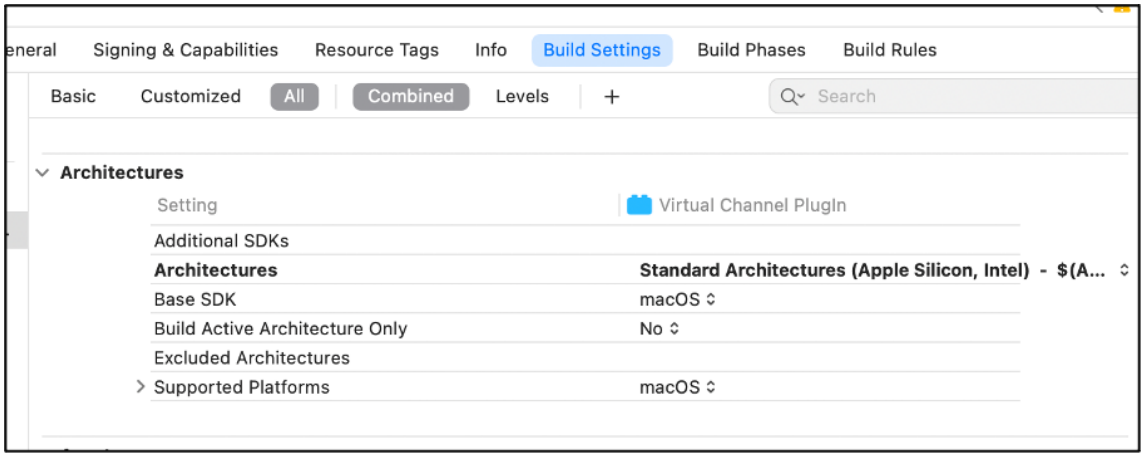
Pour charger le VCSDK, procédez comme suit :

1. Téléchargez Virtual Channel SDK 2204 for macOS depuis Téléchargements.
2. Ouvrez votre projet de canal virtuel personnalisé dans Xcode.
3. Changez votre code.
4. Compilez votre canal virtuel personnalisé pour générer le bundle de canaux virtuels.

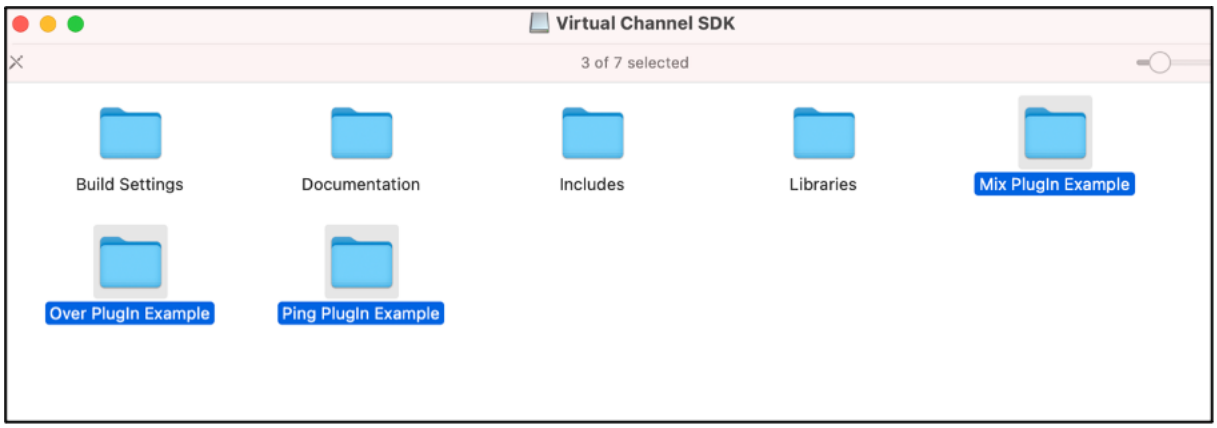
Tester votre kit de développement logiciel de canal virtuel (VCSDK)

Si vous utilisez le kit de développement logiciel de canal virtuel Citrix (VCSDK), vous devez apporter certaines modifications afin que vos canaux virtuels personnalisés s'exécutent correctement. Pour tester vos VCSDK, procédez comme suit :

1. Assurez-vous que toutes les bibliothèques liées de vos canaux virtuels personnalisés sont compilées pour Universal Binary.
2. Modifiez le fichier de projet pour prendre en charge Universal Binary :
    - Ouvrez **Project** > **Build Settings**.
    - Définissez **Architectures** sur **Standard Architectures**.



Vous trouverez des exemples de VCSDK dans *VCSDK.dmg*. Ces exemples prennent en charge le format Universal Binary macOS d'Apple qui s'exécute en mode natif sur les ordinateurs Mac dotés d'une puce Apple et ceux dotés d'un processeur Intel, car il contient du code exécutable pour les deux architectures. Vous pouvez utiliser ces exemples comme référence.



> **Remarque :**
>
> Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en Tech Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions Bêta dans les environnements de production.

Configuration système requise et compatibilité

August 24, 2022

Systèmes d'exploitation pris en charge

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

- macOS Monterey (jusqu'à 12.3.1)
- macOS Big Sur 11
- macOS Catalina (10.15)

Produits Citrix compatibles

L'application Citrix Workspace est compatible avec toutes les versions actuellement prises en charge de Citrix Virtual Apps and Desktops, Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), et de Citrix Gateway comme indiqué dans le tableau du cycle de vie des produits Citrix.

Navigateurs compatibles

L'application Citrix Workspace pour Mac est compatible avec les navigateurs suivants :

- Google Chrome
- Microsoft Edge
- Safari

Configuration matérielle requise

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

Connexions, certificats et authentification

Connexions

L'application Citrix Workspace pour Mac prend en charge les connexions suivantes à Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) :

- 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 12.x-13.x, y compris 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 :**
>
> Lorsque le certificat de la passerelle distante ne peut pas être vérifié lors de la connexion, un avertissement relatif à un certificat non approuvé s'affiche car le certificat racine n'est pas inclus dans le keystore local. Lorsqu'un utilisateur continue d'ajouter un magasin, l'ajout du magasin échoue. Toutefois, sur le navigateur Web, l'utilisateur peut être en mesure de s'authentifier auprès du magasin, mais les connexions aux sessions échouent.

Importation de certificats racine pour les appareils

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, la liaison et la mise à jour des certificats, consultez 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 **tous** les certificats fournis par le serveur (ou la passerelle). L'application Citrix Workspace pour Mac vérifie ensuite si 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.

L'application Citrix Workspace pour Mac vérifie ensuite que tous ces certificats sont valides. L'application Citrix Workspace pour Mac vérifie également qu'elle fait déjà confiance au « Certificat racine ». Si l'application Citrix Workspace pour Mac ne fait pas confiance au « Certificat racine », 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. 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. Elle recherche ensuite un certificat racine sur la machine utilisateur. Si elle trouve un certificat approuvé qui est validé correctement, 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, destiné aux situations où il existe plusieurs certificats racine. Un certificat racine antérieur est toujours utilisé en même temps qu'un certificat racine ultérieur. Dans ce cas, il y a 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 croisé et le certificat racine ont le même nom d'objet (Délivré à), mais le certificat intermédiaire croisé a un nom d'émetteur différent (Delivré 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)
Anonyme	Oui	Oui			
Domaine	Oui	Oui		Oui*	Oui*
Authentificatio pass-through au domaine					

	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)
Jeton de sécurité				Oui*	Oui*
Authentificatio à 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

July 19, 2022

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)

Par défaut, l'application Citrix Workspace est installée dans le répertoire **Applications**. Les chemins d'installation sont les suivants :

- Installation complète - `"/Applications/Citrix\ Workspace.app/"`
- Exécutable de l'application Citrix Workspace pour Mac - `"/Applications/Citrix\ Workspace.app/Contents/MacOS/Citrix\ Workspace"`

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 installer l'application en téléchargeant le fichier depuis la section Téléchargements du site Web Citrix.

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.
2. Ouvrez le fichier téléchargé.
3. Sur la page Introduction, cliquez sur **Continue**.

4. Sur la page **License**, cliquez sur **Continue**.
5. Cliquez sur **Agree** pour accepter les termes du contrat de licence.
6. Sur la page **Installation Type**, cliquez sur **Install**.
7. Sur la page **Ajouter un compte**, sélectionnez **Ajouter un compte** et cliquez sur **Continuer**.
8. Entrez le nom d'utilisateur et le mot de passe d'un administrateur sur la machine locale.

Désinstallation

Vous pouvez maintenant simplement faire glisser ou déplacer l'icône de l'application Citrix Workspace dans la corbeille pour désinstaller complètement l'application Citrix Workspace pour Mac. Pour désinstaller l'application Citrix Workspace, procédez comme suit :

1. Fermez l'application Citrix Workspace, si elle est en cours d'exécution.
2. Faites glisser l'application Citrix Workspace dans la corbeille.
   Vous pouvez également cliquer avec le bouton droit de la souris sur l'application Citrix Workspace et sélectionner **Options** > **Déplacer vers la corbeille**.
3. Fournissez les informations d'identification de votre système lorsque vous y êtes invité.
4. Fermez toutes les applications en cours d'exécution (Citrix Workspace) et cliquez sur **Continuer** pour confirmer.
   L'application Citrix Workspace et tous ses fichiers système sont supprimés de votre appareil.

Vous pouvez également 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 des Téléchargements 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. Pour plus d'informations sur les mises à jour automatiques, consultez Mise à jour automatique.

Vous pouvez mettre à niveau l'application Citrix Workspace pour Mac depuis n'importe quelle version antérieure de l'application Citrix Workspace pour Mac. Pour plus d'informations sur la mise à jour manuelle de l'application, consultez Mise à jour manuelle.

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.

Mise à jour

February 21, 2022

Mise à jour manuelle

Pour mettre à jour manuellement l'application Citrix Workspace pour Mac, téléchargez et installez la dernière version de l'application à partir de la page des téléchargements Citrix.

Mise à jour automatique

Lorsqu'une nouvelle version de l'application Citrix Workspace est publiée, Citrix envoie la mise à jour sur le système sur lequel l'application Citrix Workspace est installée. Vous êtes informé lorsque la mise à jour est disponible.

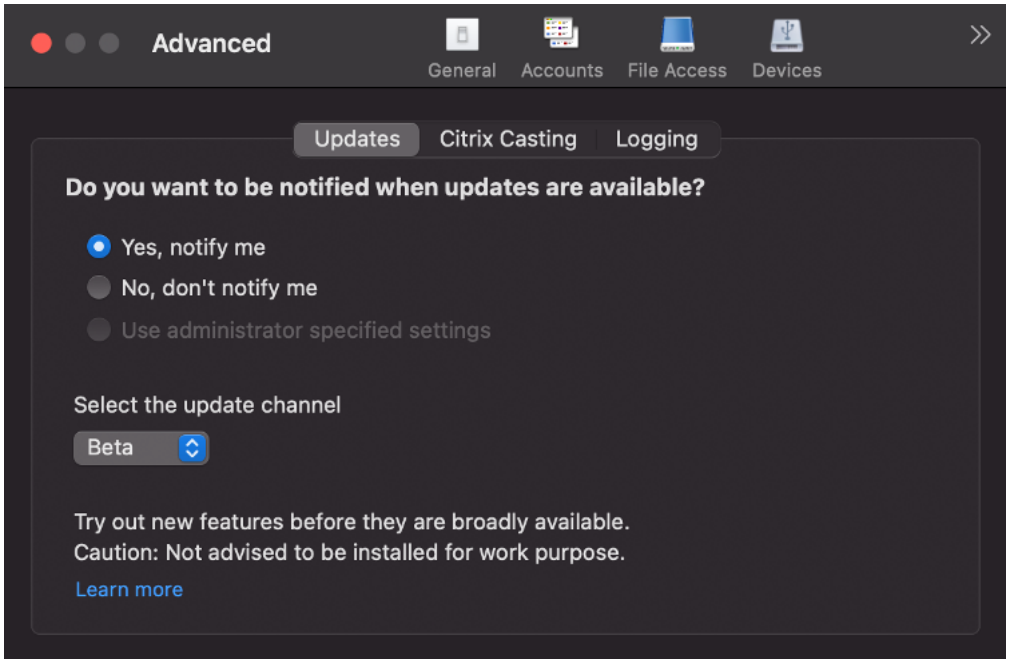
> **Remarque :**
>
> - Si vous avez configuré un proxy de sortie d'interception SSL, vous devez ajouter une exception pour le service Receiver auto-update Signature `https://citrixupdates.cloud.com/` et l'emplacement de téléchargement `https://downloadplugins.citrix.com/` afin de recevoir les mises à jour de Citrix.
> - Votre système doit disposer d'une connexion Internet pour recevoir les mises à jour.
> - Les utilisateurs de Workspace pour Web ne peuvent pas télécharger automatiquement la stratégie de StoreFront.
> - Citrix HDX RTME pour macOS est inclus dans les mises à jour de Citrix Workspace. Vous êtes informé de la mise à jour disponible de HDX RTME sur l'application Citrix Workspace.
> - À partir de la version 2111, les chemins d'accès au journal des mises à jour de Citrix Workspace ont été modifiés. Les journaux des mises à jour de Workspace se trouvent sur `/Library/Logs/Citrix Workspace Updater`. Pour plus d'informations sur la collecte des journaux, consultez la section Collecte de journaux.

Installation du programme Bêta de l'application Citrix Workspace

Vous recevez une notification de mise à jour lorsque l'application Citrix Workspace est configurée pour les mises à jour automatiques. Pour installer la version Bêta sur votre système, effectuez les étapes suivantes :

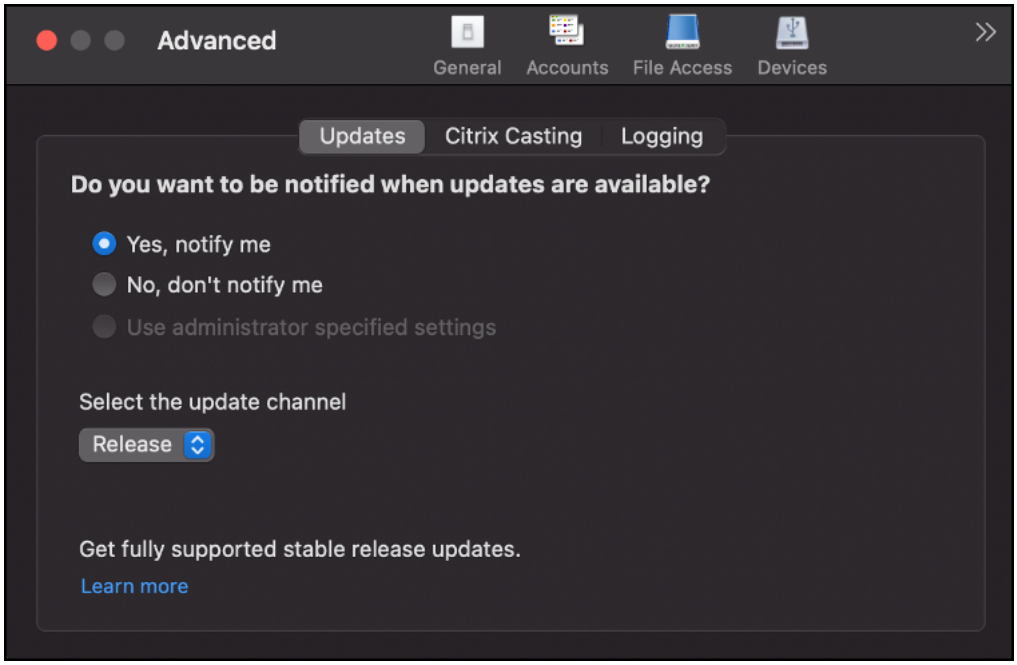
1. Ouvrez l'application Citrix Workspace.
2. Cliquez avec le bouton droit de la souris sur Citrix Workspace dans la barre d'outils et cliquez sur **Préférences** > **Avancé**.

3. Sélectionnez **Bêta** dans la liste déroulante, lorsque la version Bêta est disponible.



Pour passer d'une version Bêta à une version publiée, effectuez les étapes suivantes :

1. Ouvrez l'application Citrix Workspace.
2. Cliquez avec le bouton droit de la souris sur Citrix Workspace dans la barre d'outils et cliquez sur **Préférences** > **Avancé**.
3. Sélectionnez **Version** dans la liste déroulante **Sélectionner le canal de mise à jour**.



> **Remarque :**
>
> Les versions Bêta sont disponibles pour que les clients puissent effectuer leurs tests dans leurs environnements hors production ou de production limitée, et partager leurs commentaires. Citrix n'offre pas de support pour les versions Bêta, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est recommandé de ne pas déployer les versions Bêta dans des environnements de production.

Configuration avancée des mises à jour automatiques (mises à jour de Citrix Workspace)

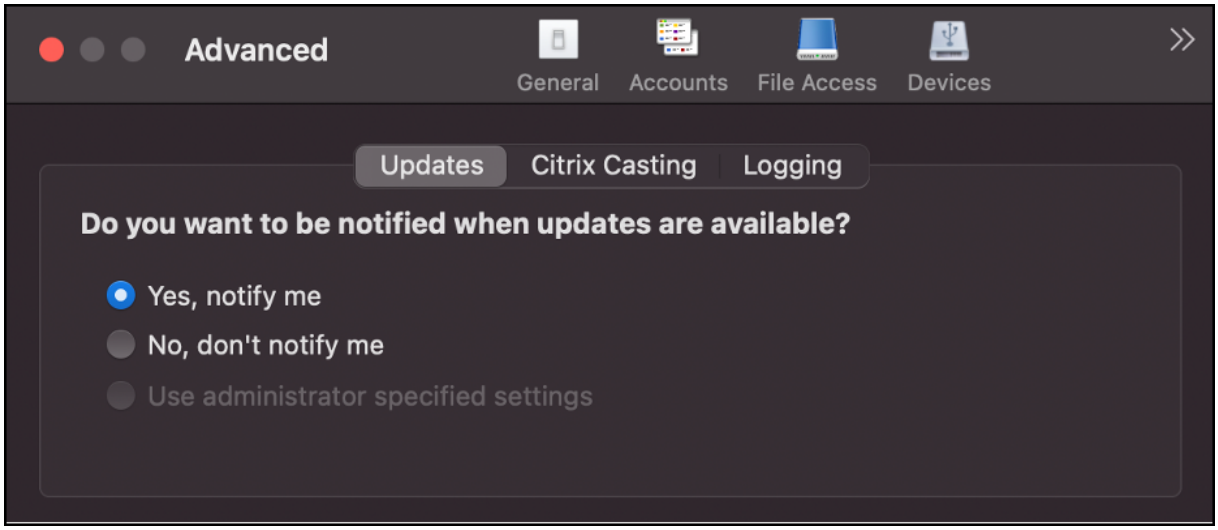
Vous pouvez configurer les mises à jour de Citrix Workspace à l'aide des méthodes suivantes :

1. GUI
2. StoreFront

Configurer les mises à jour Citrix Workspace à l'aide de l'interface utilisateur

Des utilisateurs individuels peuvent remplacer le paramètre Mises à jour de Citrix Workspace à l'aide de la boîte de dialogue **Préférences avancées**. Il s'agit d'une configuration par utilisateur, par conséquent les paramètres s'appliquent uniquement à l'utilisateur actuel. Pour configurer la mise à jour à l'aide de l'interface graphique, procédez comme suit :

1. Sélectionnez l'icône d'assistance de l'application Citrix Workspace sur votre Mac.
2. Dans la liste déroulante, sélectionnez **Préférences** > **Avancé**.
3. Sélectionnez la préférence de notification de mise à jour et fermez la fenêtre.



Configurer les mises à jour de Citrix Workspace à l'aide de StoreFront

1. Utilisez un éditeur de texte pour ouvrir le fichier `web.config`, qui se trouve généralement dans `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Recherchez l'élément de compte d'utilisateur dans le fichier (Store est le nom du compte de votre déploiement).

   Pa exemple : `<account id=... name="Store">`

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

```
<properties>
       <clear/>
 </properties>
 <!--NeedCopy-->
```

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

```
<account>

    <clear />

    <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
        F84Store"

      description="" published="true" updaterType="Citrix"
         remoteAccessType="None">

      <annotatedServices>

        <clear />

        <annotatedServiceRecord serviceRef="1__Citrix_F84Store">

          <metadata>

            <plugins>

              <clear />

            </plugins>

            <trustSettings>
```



```
24
25                <clear />
26
27              </trustSettings>
28
29              <properties>
30
31                <property name="Auto-Update-Check" value="auto" />
32
33                <property name="Auto-Update-DeferUpdate-Count" value
                     ="1" />
34
35                <property name="Auto-Update-Rollout-Priority" value=
                     "fast" />
36
37                    </properties>
38
39            </metadata>
40
41          </annotatedServiceRecord>
42
43        </annotatedServices>
44
45        <metadata>
46
47          <plugins>
48
49            <clear />
50
51          </plugins>
52
53          <trustSettings>
54
55            <clear />
56
57          </trustSettings>
58
59          <properties>
60
61            <clear />
62
63          </properties>
64
65        </metadata>
66
```



```
67      </account>
68
69  <!--NeedCopy-->
```

La signification des propriétés et leurs valeurs possibles sont détaillées comme suit :

- **Auto-update-Check :** indique que l'application Citrix Workspace détecte automatiquement une mise à jour lorsqu'elle est disponible.
- **Auto-update-Rollout-Priority:** indique la période de mise à disposition pendant laquelle vous pouvez recevoir la mise à jour.
- **Auto-update-DeferUpdate-Count:** indique le nombre de fois que vous pouvez reporter les notifications de mises à jour de la version.

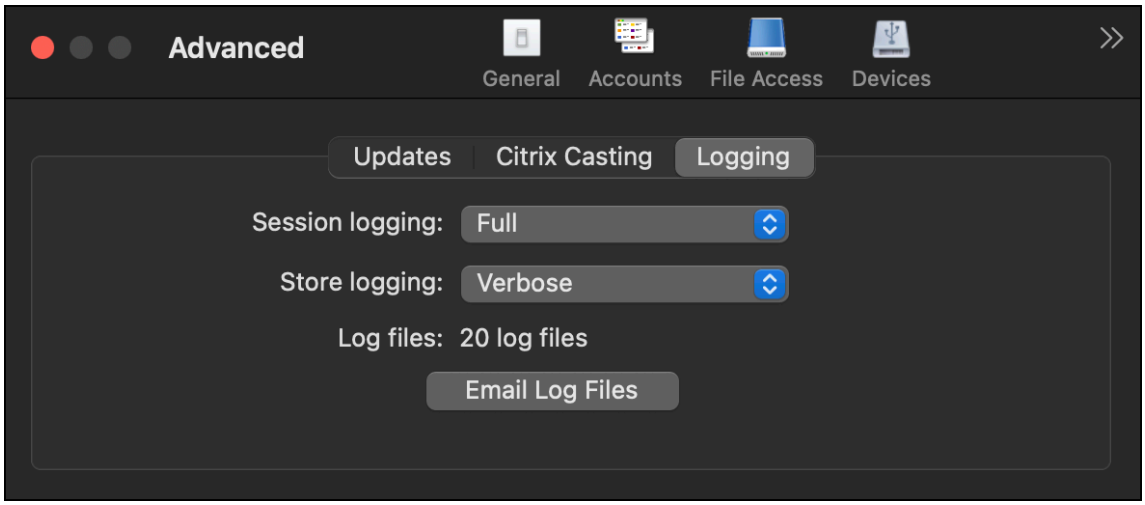
Collecte de journaux

La collecte des journaux simplifie le processus de collecte des journaux pour l'application Citrix Workspace. Les journaux aident Citrix à résoudre les problèmes et, en cas de problèmes complexes, facilitent le support.

Vous pouvez collecter des journaux à l'aide de l'interface graphique.

Collecte de journaux :

1. Ouvrez l'application Citrix Workspace.
2. Cliquez avec le bouton droit de la souris sur Citrix Workspace dans la barre d'outils et cliquez sur **Préférences** > **Avancé**.
3. Sélectionnez **Journalisation**.



4. Sélectionnez l'un des niveaux de journalisation de session suivants :
   - **Désactivé (défaut)** : des journaux minimum sont collectés pour le dépannage de base.

- **Diagnostics de connexion** : identifie les erreurs lors de la connexion. La journalisation est activée jusqu'au moment où la session est considérée comme active.
- **Complet** : capture tout, y compris les diagnostics de connexion. Une fois activée, l'application Citrix Workspace stocke jusqu'à 10 journaux de session, après quoi ils sont supprimés en commençant par le plus ancien pour conserver 10 journaux.

> **Remarque :**
>
> La sélection de l'option de journalisation **Complet** peut avoir un impact sur les performances et doit être utilisée uniquement lors du dépannage d'un problème en raison du volume de données. N'activez pas la journalisation complète pendant une utilisation normale. L'activation de ce niveau de journalisation déclenche une boîte de dialogue d'avertissement qui doit être confirmée pour pouvoir continuer.

5. Sélectionnez l'un des niveaux de journalisation de magasin suivants :
   - **Désactivé (défaut)** : des journaux minimum sont collectés pour le dépannage de base.
   - **Normal** : seuls les journaux de communication du magasin sont collectés.
   - **Détaillé** : des journaux détaillés d'authentification et de communication du magasin sont collectés.
6. Cliquez sur **Envoyer fichier journaux** pour collecter et partager les journaux en tant que fichier .zip.

Configurer

July 19, 2022

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.

> **Important :**
>
> Si vous exécutez macOS 10.15, assurez-vous que votre système est conforme aux exigences d'Apple en matière de certificats de confiance dans macOS 10.15. Effectuez cette vérification

> avant de procéder à la mise à niveau vers l'application Citrix Workspace pour Mac version 2106.

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 la 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

Sentry

Sentry est utilisé pour collecter les journaux des applications afin d'analyser les problèmes et les plantages pour améliorer la qualité des produits. Citrix ne collecte ni ne stocke aucune autre information

personnelle sur les utilisateurs et n'utilise pas Sentry pour les données d'analyse des fonctionnalités. Pour plus d'informations sur Sentry, rendez-vous sur [https://sentry.io/welcome/].

Intégration de Content Collaboration Service

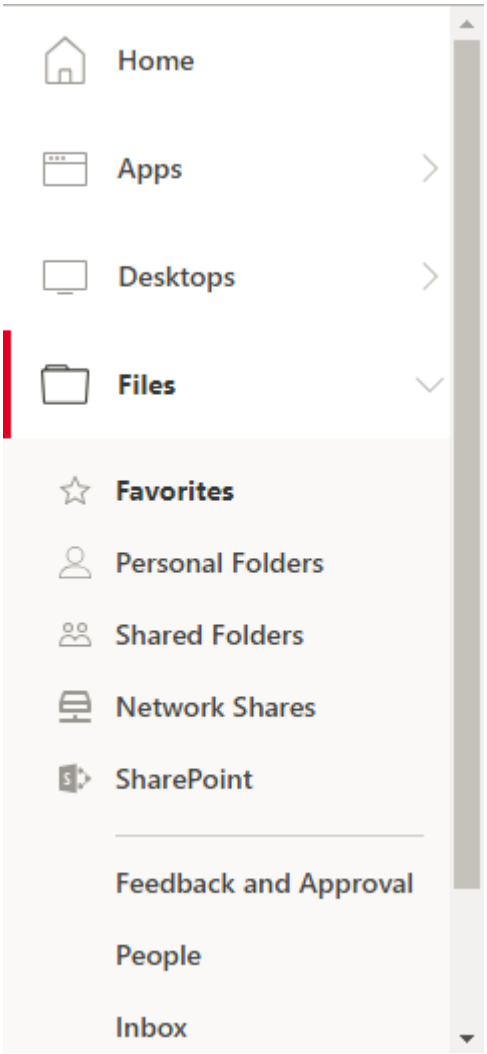
Citrix Content Collaboration vous permet d'échanger des documents facilement et en toute sécurité, d'envoyer des documents volumineux par courrier électronique, de gérer en toute sécurité les transferts de documents à des tiers et d'accéder à un espace de collaboration.

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 :**
>
> Windows Server 2012 et Windows Server 2016 ne prennent pas en charge l'intégration de Citrix Content Collaboration en raison d'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. 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. Pour limiter les types de périphériques USB disponibles pour un bureau virtuel, mettez à jour la liste des périphériques USB pris en charge pour la redirection. Vous trouverez des informations supplémentaires plus loin dans cette section.

> **Conseil**
>
> Lorsque la séparation de la sécurité entre la machine utilisateur et le serveur est requise, assurez-vous 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.

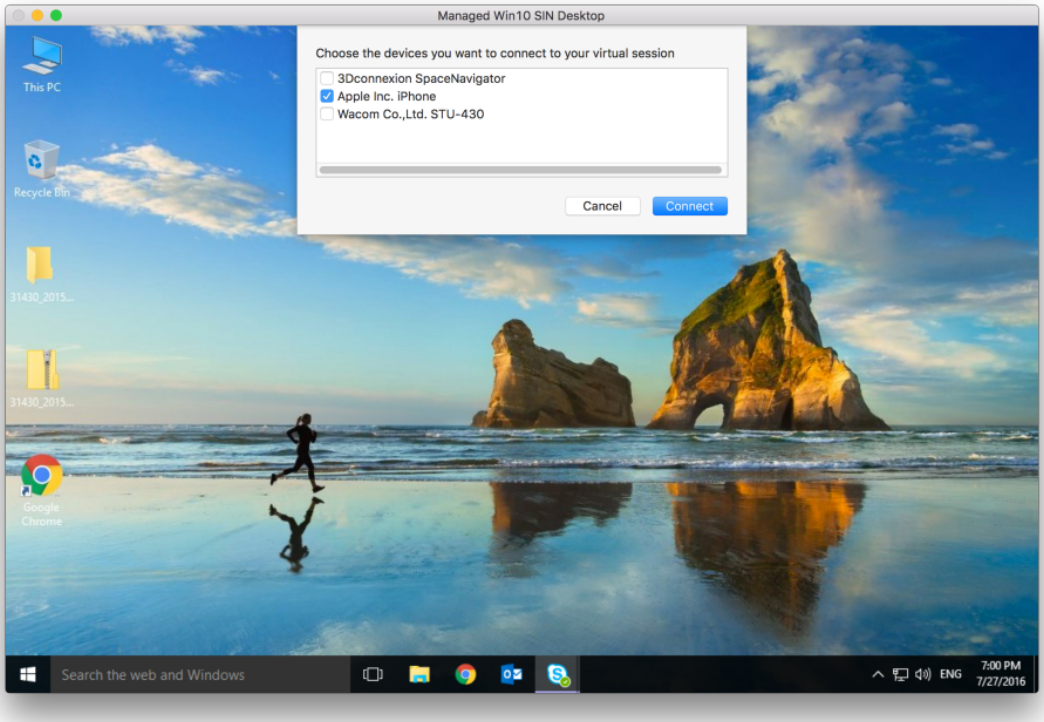
Le produit prend en charge les canaux virtuels optimisés avec des périphériques USB 3.0 et des ports USB 3.0. Par exemple, un canal virtuel CDM est utilisé pour afficher des fichiers sur une caméra ou pour fournir de l'audio à un casque. Le produit prend également en charge la redirection USB générique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

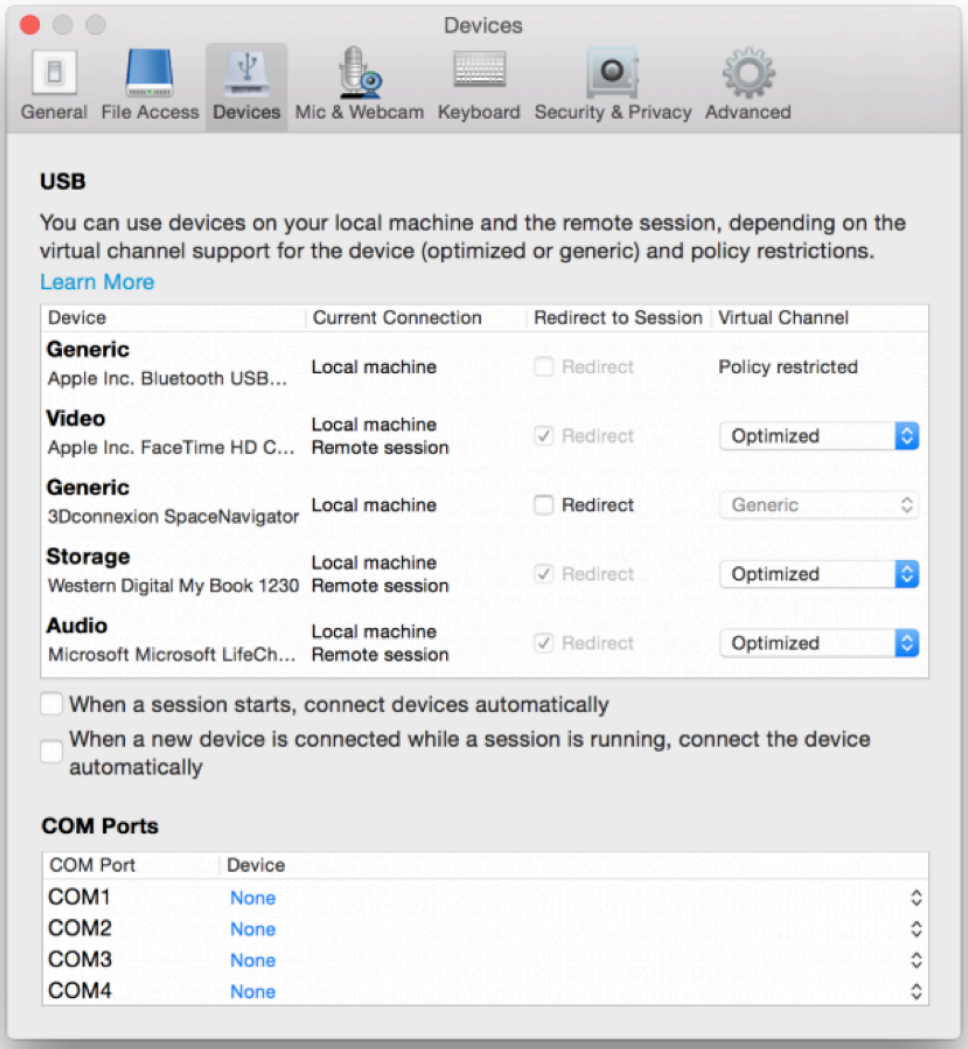
Certains périphériques ne sont pas redirigés par défaut et sont uniquement disponibles pour la session locale. Par exemple, il n'est pas approprié de rediriger une carte d'interface réseau qui est directement connectée via USB interne.

Pour utiliser la redirection USB :

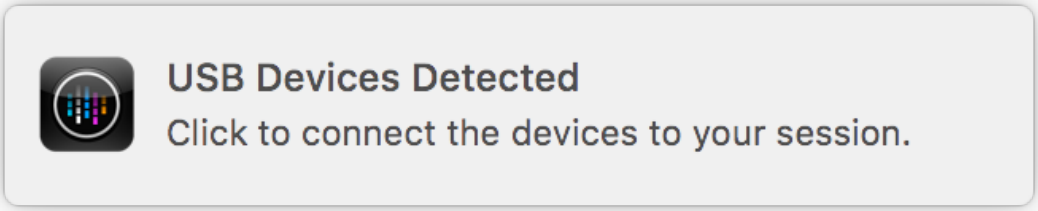
1. Connectez le périphérique USB à l'appareil sur lequel l'application Citrix Workspace pour Mac est installée.
2. Vous êtes invité à sélectionner les périphériques USB disponibles sur votre système local.



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.

Périphériques USB pris en charge

Avec Apple annonçant la dépréciation de Kernel Extensions (KEXT), l'application Citrix Workspace pour Mac a migré vers le nouveau framework USB en mode utilisateur `IOUSBHost` fourni par Apple. Cet article répertorie les périphériques USB pris en charge.

Périphériques USB compatibles avec la redirection USB

Les périphériques USB suivants fonctionnent de manière transparente avec la redirection USB :

- 3DConnexion SpaceMouse
- Périphériques de stockage de masse
- Clé USB Kingston Data Traveler
- Disque dur externe Seagate
- Clé USB Kingston/Transcend 32 Go/64 Go
- Lecteur de cartes à puce NIST PIV
- YubiKey

Périphériques USB ne prenant pas en charge la redirection USB

Le périphérique suivant n'est pas compatible avec la redirection USB :

- Disque dur externe SSD Transcend

Périphériques USB non vérifiés

Citrix ne vérifie pas la prise en charge de la redirection USB avec de nombreux périphériques par l'application Citrix Workspace pour Mac. Certains de ces périphériques incluent :

- Autres disques durs
- Touches spéciales sur le clavier et les casques utilisant le protocole HID personnalisé

Prise en charge des périphériques de stockage de masse

Nous avons constaté que les types de périphériques de stockage de masse ne peuvent pas tous être redirigés avec succès. Pour les périphériques qui ne peuvent pas être redirigés, il existe un canal virtuel optimisé appelé Mappage des lecteurs clients. À l'aide du mappage des lecteurs clients, l'accès aux périphériques de stockage de masse peut être contrôlé via des stratégies sur le Delivery Controller.

Prise en charge des périphériques isochrones

La redirection USB générique ne prend pas en charge la classe Isochrone des périphériques USB dans l'application Citrix Workspace pour Mac. Le mode isochrone de transfert de données dans une spécification USB indique les périphériques qui streament les données horodatées à un débit constant. Par exemple : webcams, casques USB, etc.

Prise en charge des périphériques composites

Un périphérique composite USB est un gadget unique qui peut exécuter plusieurs fonctions. Par exemple : imprimantes multifonctions, iPhone, etc. Actuellement, l'application Citrix Workspace pour Mac ne prend pas en charge la redirection des périphériques composites vers la session Citrix Virtual Apps and Desktops et Citrix DaaS.

Alternatives pour les périphériques USB non pris en charge

Il existe des canaux virtuels optimisés qui peuvent gérer les périphériques qui ne prennent pas en charge la redirection USB générique. Ces canaux virtuels sont optimisés pour une plus grande vitesse par rapport à la redirection USB générique. Voici quelques exemples :

- **Redirection de la webcam :** optimisée pour le trafic de webcam brut. Le pack d'optimisation de Microsoft Teams dispose de sa propre méthode de redirection de webcam. Par conséquent, le canal virtuel de redirection de webcam n'est pas concerné.
- **Redirection audio :** optimisée pour transférer des flux audio.
- **Mappage des lecteurs clients :** optimisé pour rediriger les périphériques de stockage de masse vers la session Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Par exemple : clés USB, disques durs, DVD ROM/RW, etc.

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. 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.
> - Lorsque 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 le délai d'expiration de la fiabilité de session, l'utilisateur peut se laisser distraire et s'éloigner de son appareil. Il est alors possible que des utilisateurs non autorisés accèdent à sa session.

Par défaut, 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.

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.

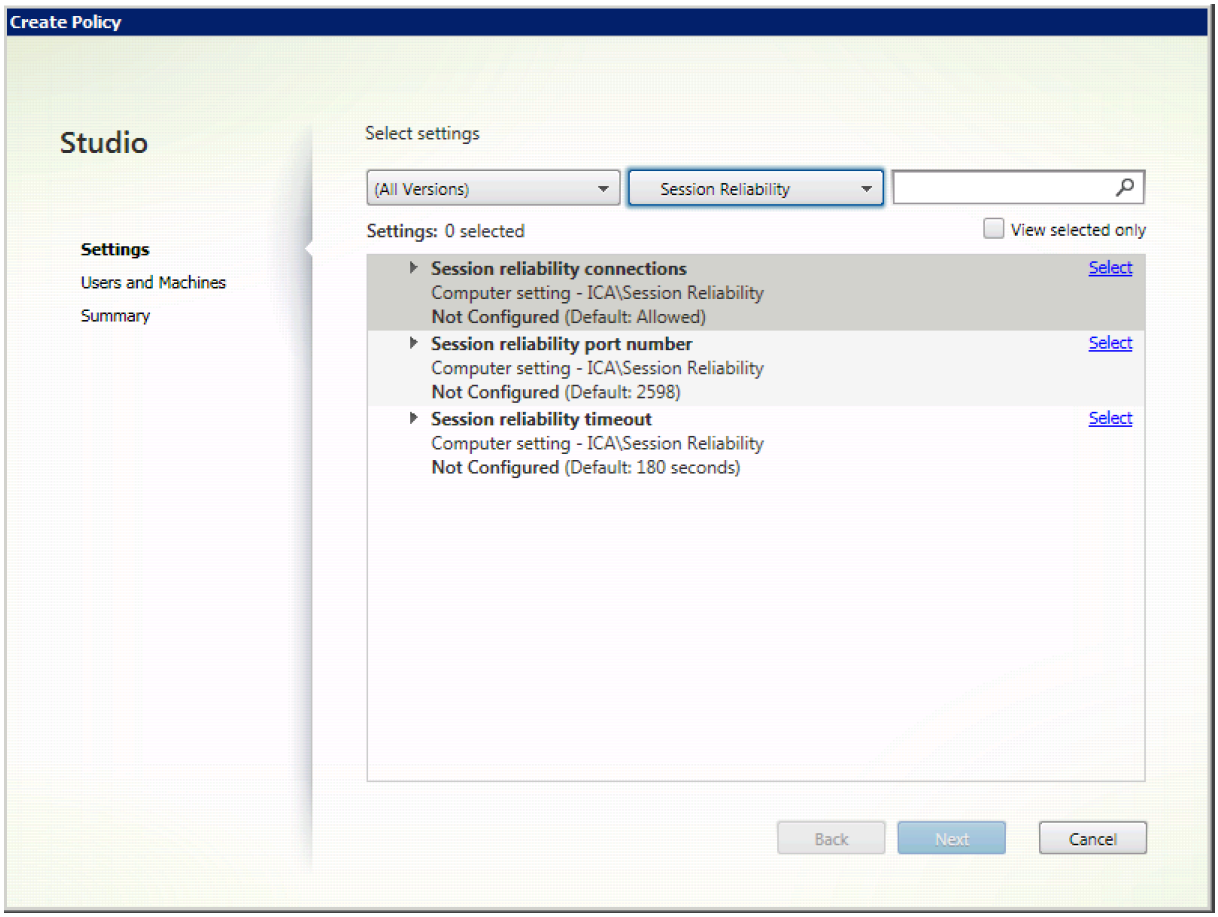
> **Remarque**
>
> La fiabilité de session est activée par défaut au niveau du serveur. Pour désactiver cette fonctionnalité, configurez la stratégie gérée par le serveur.

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 :

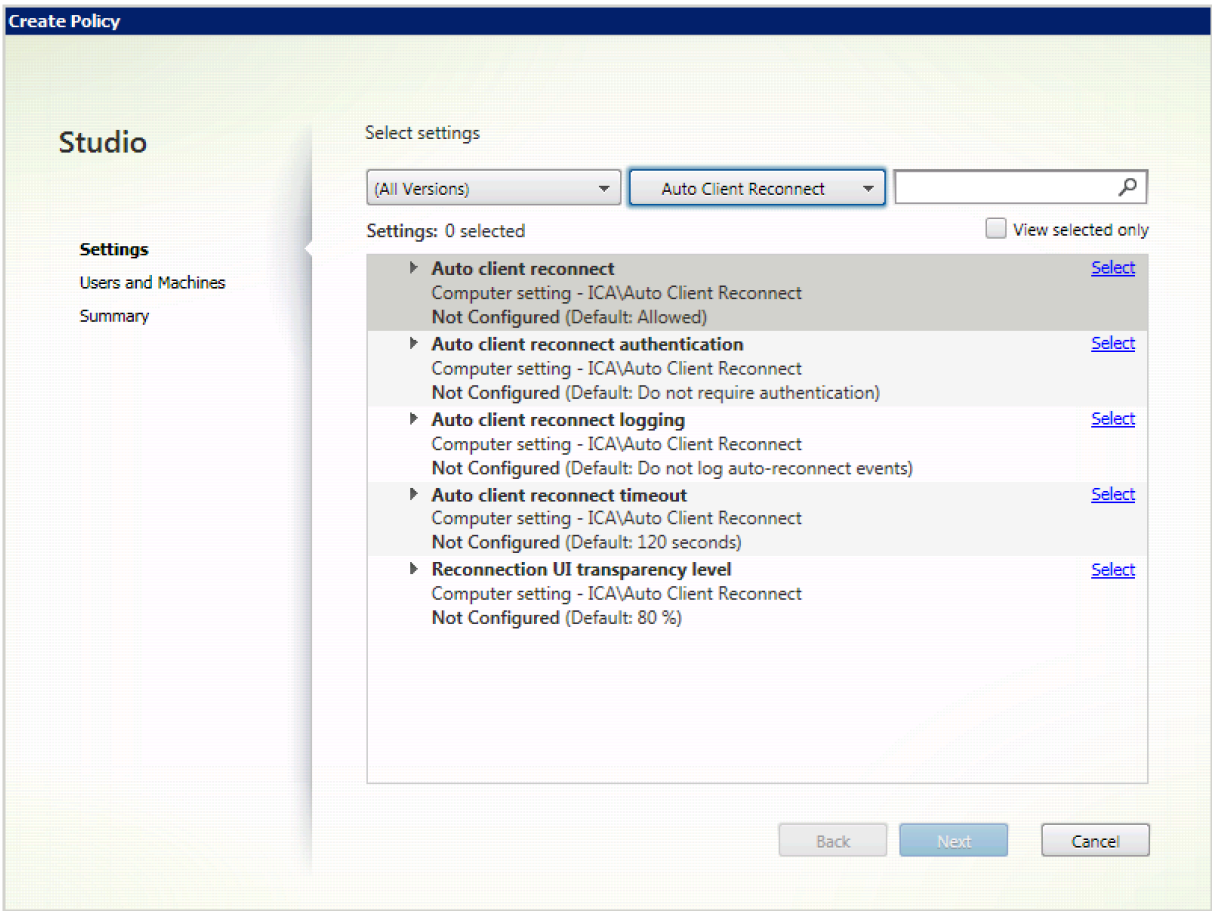
1. Lancez Citrix Studio.
2. Ouvrez la stratégie **Expiration de délai de la fiabilité de session**.
3. Modifiez la valeur du délai d'expiration.
4. Cliquez sur **OK**.

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. Citrix a amélioré les technologies de fiabilité de session et de reconnexion automatique pour résoudre ce problème.

Cette fonctionnalité permet aux utilisateurs de se reconnecter automatiquement aux sessions après une reprise suite à une interruption du réseau. Ces fonctionnalités, qui sont activées par des stratégies dans Citrix Studio, peuvent être utilisées pour améliorer 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	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.

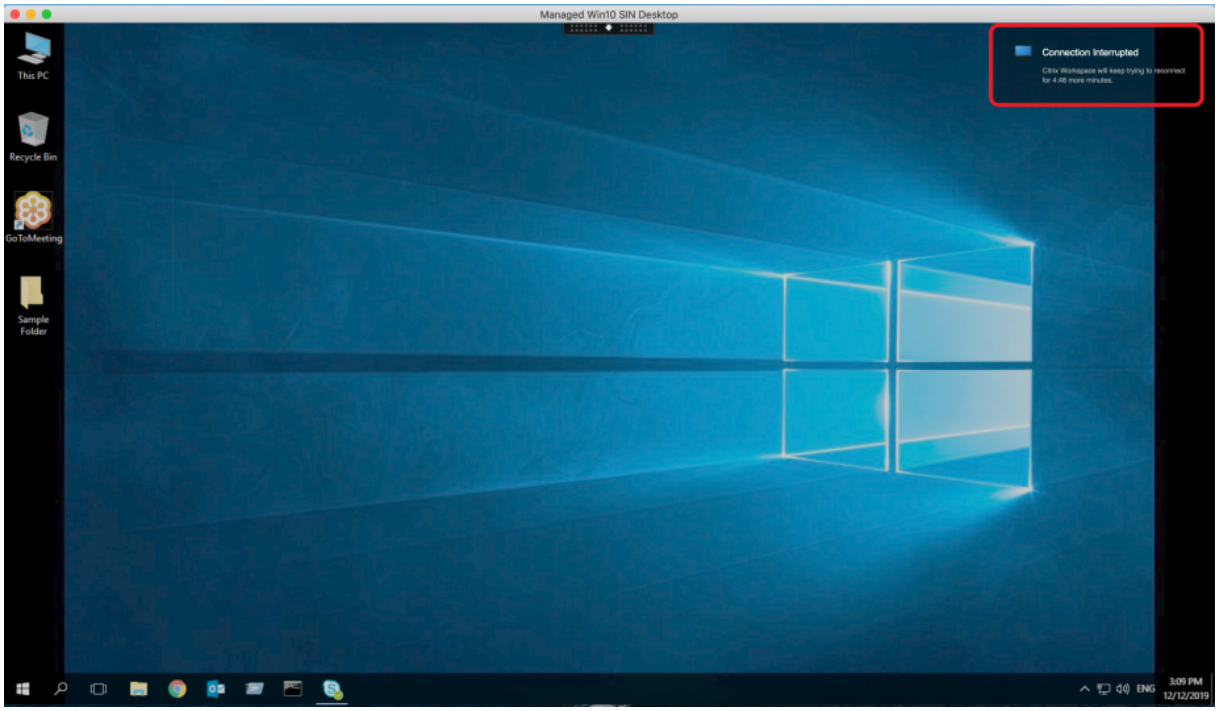
Paramètre	Exemple	Défaut
SessionReliabilityTTL	SessionReliabilityTTL=120	180

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.

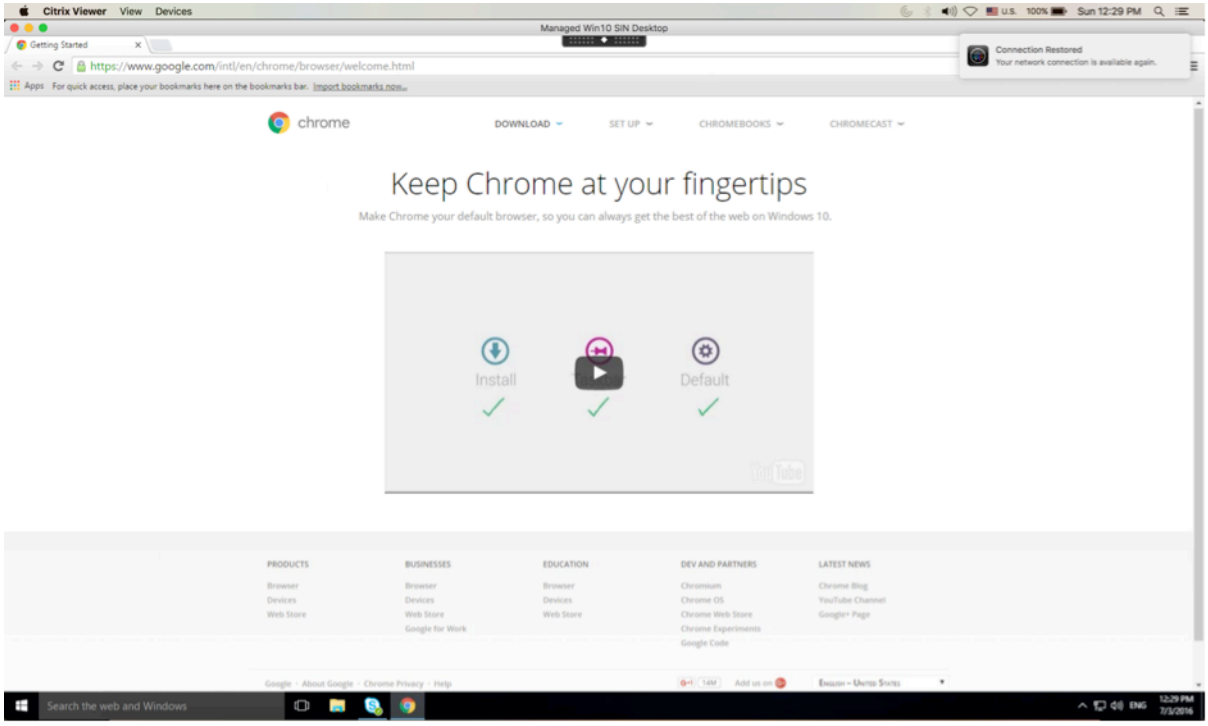
Par défaut, la notification de reconnexion commence après 5 minutes. Cette valeur représente les valeurs combinées de chacun des minuteurs (reconnexion automatique des clients et fiabilité de session), respectivement 2 et 3 minutes. L'image suivante illustre la notification qui s'affiche dans la partie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

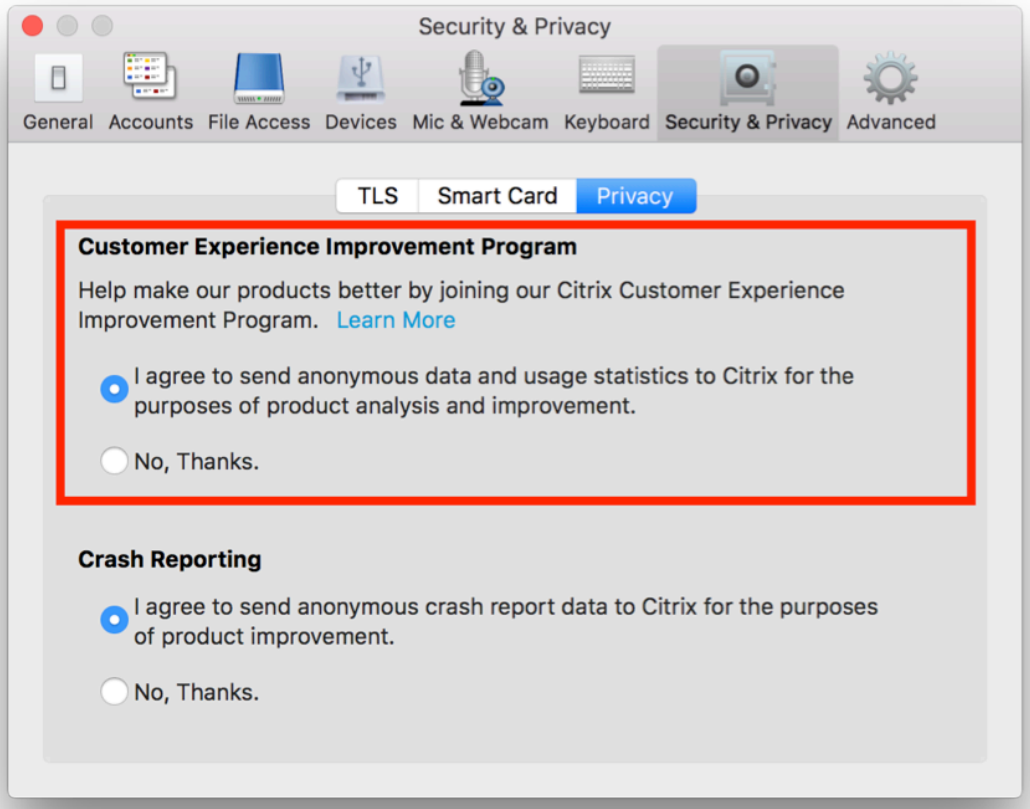
Informations supplémentaires

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 Citrix Trust Center.

Citrix utilise Google Analytics pour collecter certaines données à partir de l'application Citrix Workspace dans le cadre du programme CEIP. Informez-vous sur la manière dont Google gère les données collectées pour Google Analytics.

Pour désactiver l'envoi de données via le programme CEIP à Citrix et Google Analytics, effectuez les opérations suivantes :

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
```


> **Remarque :**
>
> Aucune donnée n'est collectée pour les utilisateurs de l'Union européenne (UE), de l'Espace économique européen (EEE), de la Suisse et du Royaume-Uni (UK).

Les données spécifiques collectées par Google Analytics sont les suivantes :

Version du système d'exploitation	Version de l'application Workspace	Utilisation de la redirection USB générique	Configuration du magasin
Utilisation de Citrix Workspace Browser	État du lancement de sessions Citrix Virtual Apps and Desktops	Préférence de mise à jour automatique	État de la mise à jour automatique
Méthode de lancement de session	Informations de désinstallation	Utilisation de la fonctionnalité de délai d'inactivité	Utilisation de la fonctionnalité de détection basée sur une adresse e-mail
Utilisation de la fonctionnalité de magasin Web personnalisé	Préférences de reconnexion	Utilisation de Global App Config Service	Utilisation de la restauration du clavier
Utilisation de la fonctionnalité de suppression du mot de passe	Canal de mise à jour automatique	Détails de la location de connexion	

Mise à disposition d'applications

Lors de la mise à disposition d'applications avec Citrix Virtual Apps and Desktops et Citrix DaaS, 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. Assurez-vous d'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 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 répertorier les applications figurant dans la liste Sélection pour Mac, ajoutez la chaîne `**KEYWORDS:Featured**` à la description de l'application.

Pour plus d'informations, veuillez consulter 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**. Ce processus correspond à 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

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

Détermine le nombre de fois que les utilisateurs sont invités à procéder à la mise à niveau avant qu'ils ne soient forcés à 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 est notifié ultérieurement lorsqu'une mise à jour est disponible.
- 0 : l'utilisateur est forcé à 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 est 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

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 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.
- Lorsqu'un utilisateur travaille au sein d'une session RDP, il n'est pas possible de modifier la disposition du clavier à l'aide des raccourcis `Alt + Shift` lorsque le protocole RDP est déployé en tant qu'application. Pour contourner ce problème, les utilisateurs peuvent utiliser la barre de langue de 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

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

> **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 plus d'informations, consultez la documentation relative à Citrix Ready Workspace Hub.

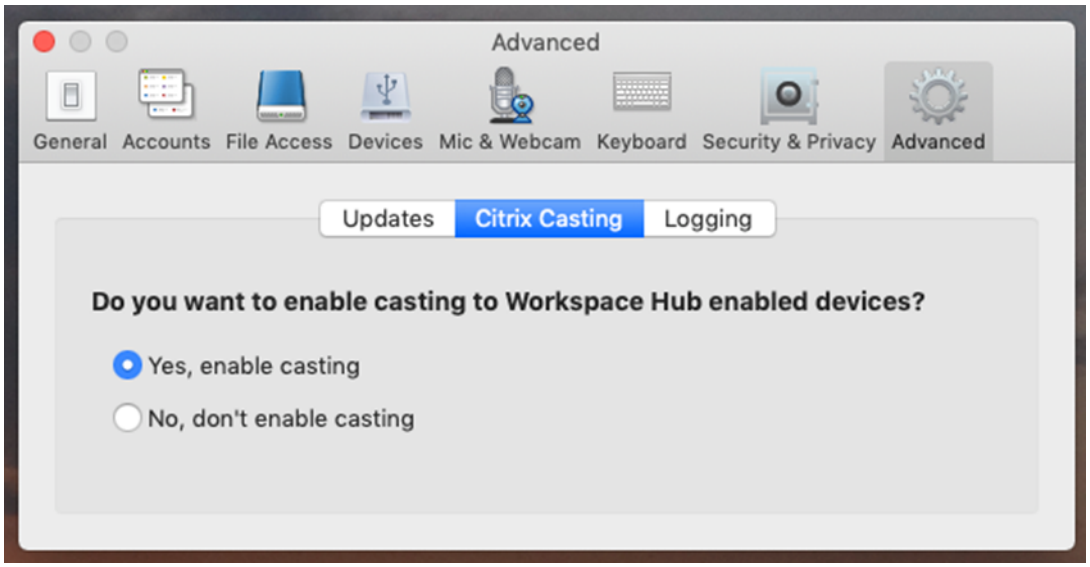
Conditions préalables

- Dernière version prise en charge de l'application Citrix Workspace.
- 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.

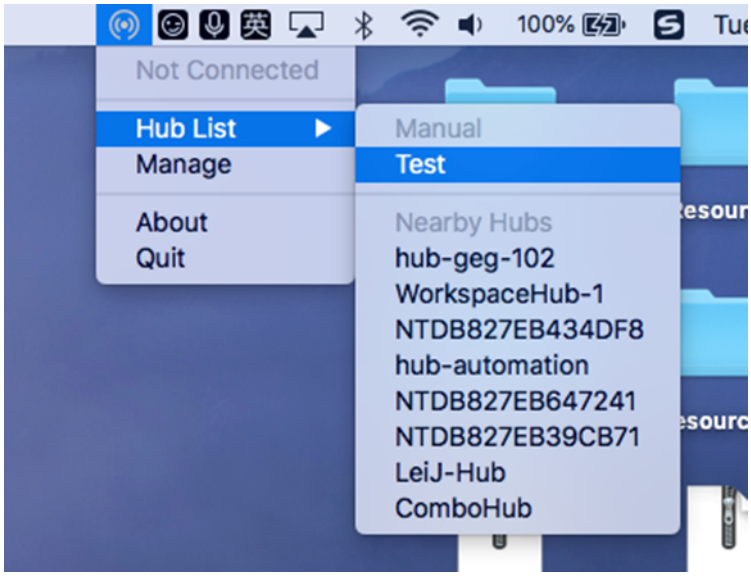
> **Remarque :**
>
> Après l'activation, Citrix Casting se lance automatiquement avec l'application Citrix Workspace

> 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 l'appareil 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**.

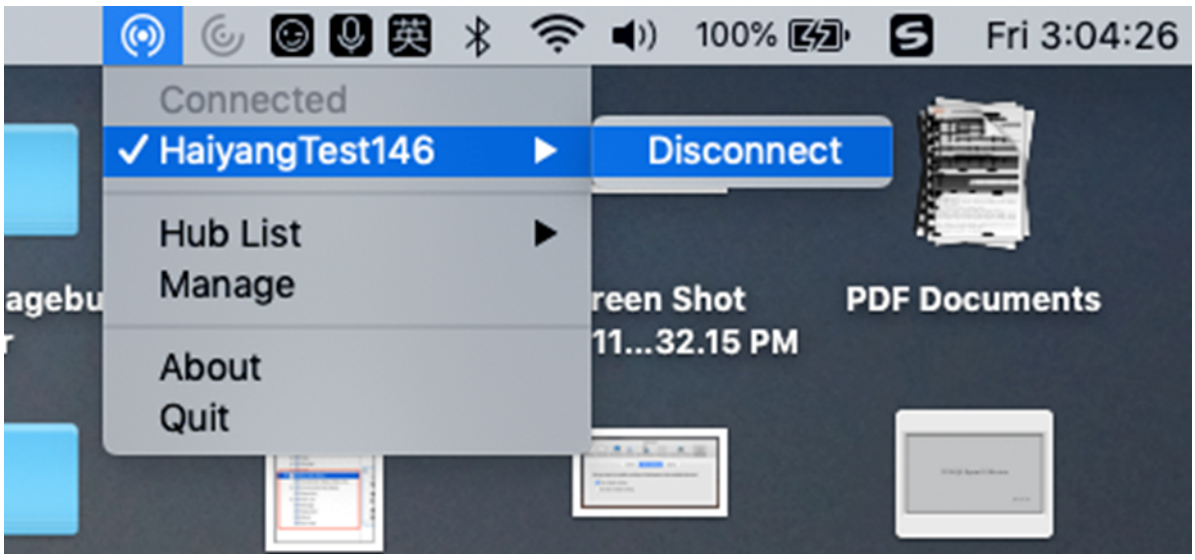
> **Remarque :**
>
> Actuellement, seul le mode **Miroir** est pris en charge. **Miroir** est le seul choix disponible dans la colonne **Mode d'affichage**.

Déconnecter l'appareil 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 utiliser les micros connectés à votre machine utilisateur dans les sessions en choisissant l'une des options suivantes dans les paramètres **Mic & Webcam** depuis **Application Citrix Workspace pour Mac** > **Préférences** :

- 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 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 permettent de saisir du texte et incluent toutes les lettres, les chiffres et les signes de ponctuation. Les touches spéciales 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
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
Début	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

Touche Windows ou combinaison de touches	Équivalents sur Mac
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. Ouvrez Citrix Viewer.
2. Dans la barre de menus, cliquez sur **Afficher** et sélectionnez l'une des options suivantes, en fonction de vos besoins :
   - **Entrer en mode plein écran** : plein écran uniquement sur le moniteur principal.
   - **Utiliser tous les affichages en plein écran** : plein écran sur tous les moniteurs connectés.
3. Faites glisser l'écran Citrix Virtual Desktops entre les moniteurs.

L'écran est maintenant étendu à tous les moniteurs.

Limitations

- 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.
- Le mode plein écran n'est pas disponible sur les Mac affichant une encoche.

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. Suivez l'une des méthodes suivantes pour passer du mode plein écran au mode fenêtré :
  - Sur OS X 10.10, cliquez sur le bouton de fenêtre vert sur la barre du menu déroulant.
  - Sur OS X 10.9, cliquez sur le bouton de menu bleu sur la barre du menu déroulant.
  - Sur toutes les versions de OS X, sélectionnez **Quitter le mode plein écran** dans le menu **Afficher** de la barre du menu déroulant.
- Le glissement entre les fenêtres en plein écran avec plusieurs moniteurs est pris en charge.

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. Par exemple, les médecins hospitaliers peuvent 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 peut se déconnecter d'un appareil dans la salle d'urgence, puis se connecter à un poste de travail du laboratoire de radiographie. Les stratégies, les mappages d'imprimante et les

mappages de lecteur client appropriés pour la session dans le laboratoire de radiographie sont alors mis en œuvre.

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'une configuration de serveur autorise le mappage des lecteurs clients, les utilisateurs peuvent accéder aux fichiers stockés localement et y travailler pendant les sessions. Ils peuvent également les enregistrer 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.

Magasin Web personnalisé

Vous pouvez accéder au magasin Web personnalisé de votre organisation à partir de l'application Citrix Workspace pour Mac. Pour utiliser cette fonctionnalité, l'administrateur doit ajouter le magasin Web personnalisé à la liste des URL autorisées dans la propriété `allowedWebStoreURLs` de Global App Configuration Service.

Pour plus d'informations sur la configuration des adresses URL des magasins Web pour les utilisateurs, consultez Global App Configuration Service.

Pour ajouter une URL de magasin Web personnalisé, procédez comme suit :

1. Ouvrez l'application Citrix Workspace et accédez à **Comptes**.
2. Dans la fenêtre **Comptes**, cliquez sur l'icône **+** et saisissez l'URL.

Pour supprimer une URL de magasin Web personnalisé, procédez comme suit :

1. Ouvrez l'application Citrix Workspace et accédez à **Comptes**.
2. Dans la fenêtre **Comptes**, sélectionnez le compte que vous souhaitez supprimer et cliquez sur l'icône **-**.

Délai d'inactivité pour l'application Citrix Workspace

La fonctionnalité de délai d'inactivité vous déconnecte de l'application Citrix Workspace en fonction d'une valeur définie par l'administrateur. Les administrateurs peuvent spécifier la durée d'inactivité autorisée avant qu'un utilisateur ne soit automatiquement déconnecté de l'application Citrix Workspace. Vous êtes automatiquement déconnecté lorsqu'aucune activité de la souris, du clavier ou d'interaction sur l'écran ne se produit pendant l'intervalle de temps spécifié, dans la fenêtre de l'application Citrix Workspace. Le délai d'inactivité n'affecte pas les sessions Citrix Virtual Apps and Desktops et Citrix DaaS déjà en cours d'exécution ni les magasins Citrix StoreFront.

La valeur de délai d'inactivité définie doit être comprise entre 1 et 1 440 minutes. Par défaut, le délai d'inactivité n'est pas configuré. Les administrateurs peuvent configurer la propriété inactivityTimeoutInMinutes à l'aide d'un module PowerShell. Cliquez ici pour télécharger les modules PowerShell pour la configuration de Citrix Workspace.

L'expérience utilisateur est la suivante :

- Une notification apparaît trois minutes avant votre déconnexion, avec la possibilité de rester connecté ou de vous déconnecter. La notification s'affiche si vous avez activé les notifications de l'application Citrix Workspace dans les préférences système de votre Mac.
- La notification n'apparaît que si la valeur de délai d'inactivité configurée est supérieure à 5 minutes. Par exemple, si la valeur configurée est de 6 minutes, une notification s'affiche après 3 minutes d'inactivité détectées. Si le délai d'inactivité configuré est inférieur ou égal à 5 minutes, l'utilisateur est déconnecté sans notification.
- Les utilisateurs peuvent cliquer sur **Rester connecté** pour ignorer la notification et continuer à utiliser l'application, auquel cas le minuteur d'inactivité est réinitialisé à sa valeur configurée. Vous pouvez également cliquer sur Déconnexion pour mettre fin à la session du magasin actuel.

Migration de StoreFront vers Workspace

La migration de l'URL StoreFront vers Workspace vous permet de migrer en toute transparence les utilisateurs d'un magasin StoreFront vers un magasin Workspace avec un minimum d'interaction utilisateur.

Considérez que tous vos utilisateurs disposent d'un magasin StoreFront `storefront.com` ajouté à leur application Workspace. En tant qu'administrateur, vous pouvez configurer un mappage de l'URL StoreFront vers l'URL Workspace {'storefront.com':'xyz.cloud.com'} dans Global App Configuration Service. Global App Config Service envoie le paramètre à toutes les instances de l'applications Citrix Workspace, sur les appareils gérés et non gérés, sur lesquels l'URL StoreFront `storefront.com` a été ajoutée.

Une fois le paramètre détecté, l'application Citrix Workspace ajoute l'URL Workspace mappée `xyz.cloud.com` en tant qu'autre magasin. Lorsque l'utilisateur lance l'application Citrix Workspace, le magasin Citrix Workspace s'ouvre. Le magasin StoreFront précédemment ajouté `storefront.com` reste ajouté à l'application Citrix Workspace. Les utilisateurs peuvent toujours revenir au magasin StoreFront `storefront.com` à l'aide de l'option **Changer de compte** dans l'application Citrix Workspace. Les administrateurs peuvent contrôler la suppression du magasin StoreFront `storefront.com` de l'application Workspace sur les points terminaux des utilisateurs. La suppression peut être effectuée via Global App Config Service.

Pour activer cette fonctionnalité, effectuez les opérations suivantes :

1. Configurez le mappage de StoreFront vers Workspace à l'aide de Global App Config Service. Pour plus d'informations, consultez Global App Configuration Service.
2. Modifiez la charge utile dans Global App Config Service :

```
1 {
2   "serviceURL": Unknown macro: {
```



```
3     ”url” }
4
5   ,
6   ”settings”:{
7
8   ”name”:”Productivity Apps”, [New Store Name]
9   ”description”:”Provides access StoreFront to Workspace Migration”,
10  ”useForAppConfig”:true,
11  ”appSettings”:
12  {
13    ”macos”:[ Unknown macro: {
14    ”category” }
15
16  ]
17   }
18
19   }
20
21   }
22
23  <!--NeedCopy-->
```

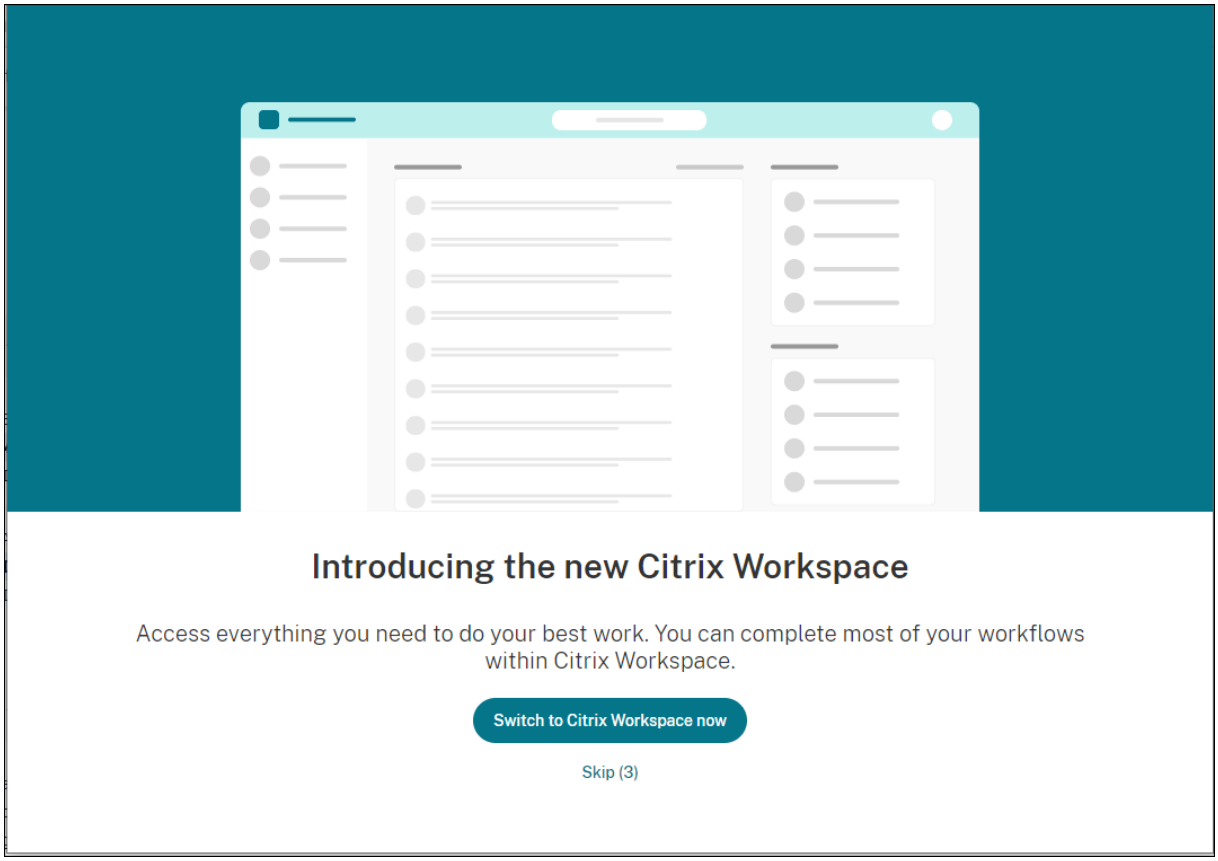
> **Remarque :**
>
> Si vous configurez la charge utile pour la première fois, utilisez `POST`.
> Si vous modifiez la configuration de la charge utile existante, utilisez `PUT` et assurez-vous que vous disposez de la charge utile comprenant tous les paramètres pris en charge.

3. Spécifiez l'URL StoreFront `storefront.com` comme valeur du champ **URL** dans la section **serviceURL**.
4. Configurez l'URL Workspace `xyz.cloud.com` dans la section **migrationUrl**.
5. Utilisez **storeFrontValidUntil** pour définir la chronologie de la suppression du magasin StoreFront de l'application Citrix Workspace. Ce champ est facultatif. Vous pouvez définir la valeur suivante en fonction de vos besoins :

   - Date de validité au format (AAAA-MM-JJ)

     > **Remarque :**
     >
     > Si vous avez indiqué une date antérieure, le magasin StoreFront est supprimé immédiatement après la migration de l'URL. Si vous avez indiqué une date ultérieure, le magasin StoreFront est supprimé à la date définie.

Une fois que les paramètres de Global App Config Service sont déployés, l'écran suivant apparaît :



Lorsque l'utilisateur clique sur **Passer à Citrix Workspace maintenant**, l'URL Workspace est ajoutée à l'application Citrix Workspace et l'invite d'authentification apparaît. Les utilisateurs ont une option limitée pour retarder la transition jusqu'à trois fois.

Microsoft Teams

Estimation des performances au niveau du codage

Le `HdxRtcEngine.exe` est le moteur multimédia WebRTC intégré à l'application Citrix Workspace qui gère la redirection Microsoft Teams. Le `HdxRtcEngine.exe` peut estimer la meilleure résolution d'encodage que le processeur du point de terminaison peut gérer sans surcharge. Les valeurs possibles sont 240p, 360p, 480p, 720p et 1080p.

Le processus d'estimation des performances utilise le code macroblock pour déterminer la meilleure résolution possible avec le point de terminaison particulier. La négociation du codec inclut la résolution la plus élevée possible. La négociation du codec peut se faire entre les homologues, ou entre l'homologue et le serveur de conférence.

Il existe quatre catégories de performances pour les points de terminaison qui ont leur propre résolution **maximale** disponible :

Performances des points de terminaison	Résolution maximale	Valeur de clé de registre
Fast (Rapide)	1080p (1920x1080 16:9 @ 30 fps)	3
Medium (Moyen)	720p (1280x720 16:9 @ 30 fps)	2
Slow (Lent)	360p (640x360 16:9 @ 30 fps ou 640x480 4:3 @ 30 fps)	1
Very slow (Très lent)	240p (320x180 16:9 @ 30 fps ou 320x240 4:3 @ 30 fps)	0

Pour définir la valeur de résolution de l'encodage vidéo, par exemple 360p, exécutez la commande suivante à partir du terminal :

```
defaults write com.citrix.HdxRtcEngine OverridePerformance -int 1
```

Pour plus d'informations, consultez Optimisation pour Microsoft Teams.

Impression

Vous pouvez désormais utiliser l'impression universelle PDF lorsque vous imprimez à partir d'un Mac. Vous n'avez plus besoin d'installer le pilote HP Color LaserJet 2800 Series PS lors de la création automatique d'imprimantes avec le pilote d'impression universelle si vous avez choisi d'utiliser l'impression universelle PDF.

Impression PostScript

Par défaut, les imprimantes clientes redirigées automatiquement sont créées avec le pilote UPD Citrix avec prise en charge PostScript.
Pour plus de détails, consultez l'article d'assistance CTX296662.

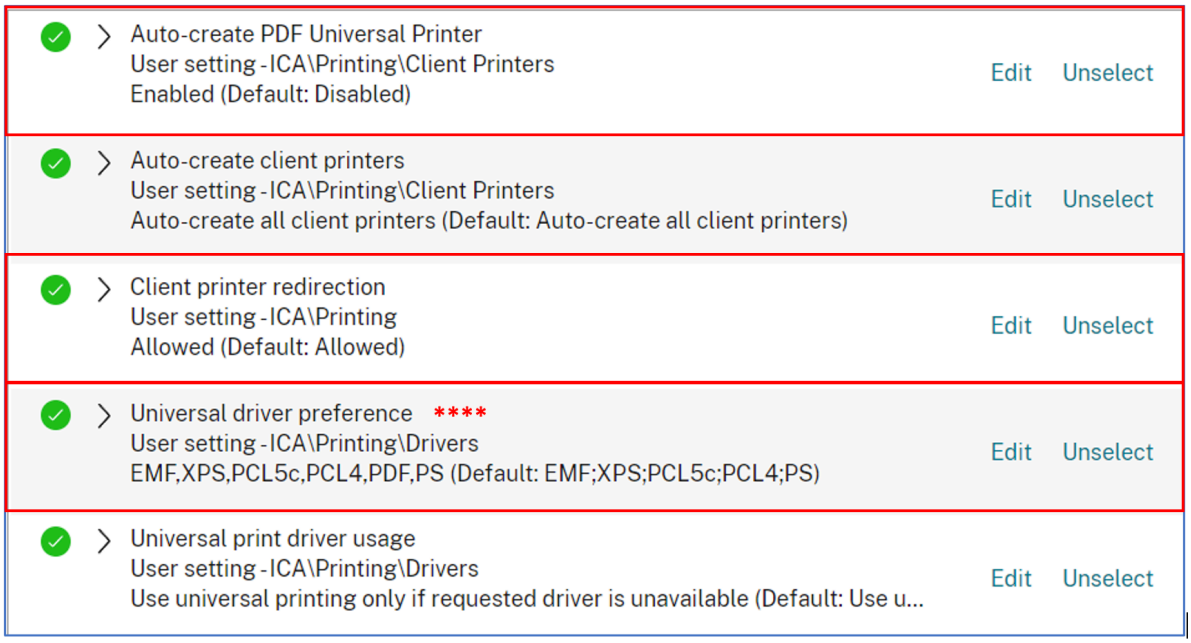
Assurez-vous que la redirection de l'imprimante cliente, l'utilisation du pilote d'impression universelle et les stratégies de priorité du pilote d'impression universelle sont définies par défaut. Vérifiez également que vous avez installé le pilote HP Color LaserJet 2800 Series PS sur le VDA.
Pour plus d'informations sur l'installation du pilote, consultez l'article d'assistance CTX140208.

Impression universelle PDF

Pré-requis :

- Application Citrix Workspace pour Mac version 2112 ou ultérieure : permet d'utiliser des flux d'impression PDF pour l'application Citrix Workspace pour Mac.

- Citrix Virtual Apps and Desktops version 2112 ou ultérieure : permet d'utiliser l'impression universelle PDF pour les imprimantes clientes créées automatiquement.
- Activez la stratégie de redirection d'imprimante cliente dans Citrix Studio ou la console Web.



**** "PDF" needs to be added manually if absent from the Universal Driver Preference policy

Vous pouvez imprimer via PDF une fois que vous avez configuré l'une des options suivantes ou les deux :

1. Fournissez une seule imprimante universelle PDF créée dans chaque session.
2. Utilisez le pilote UPD pour les imprimantes créées automatiquement de manière standard.

Fournir une seule imprimante universelle PDF créée dans chaque session

Pour activer la création de l'**imprimante universelle PDF** dans les sessions à partir d'un client Mac ou de tout autre point de terminaison client compatible PDF, accédez à Citrix Studio ou à la console Web et activez la stratégie **Créer automatiquement l'imprimante universelle PDF**.
Une fois la stratégie activée, l'imprimante universelle PDF est créée dans la session. L'imprimante s'appelle **Citrix PDF Printer**.

L'utilisation de cette imprimante dans une session génère une sortie PDF qui est livrée au client et transmise à l'application de gestion de PDF par défaut sur le point de terminaison. Pour le client macOS, il s'agit généralement de l'application **Aperçu** intégrée, mais il peut s'agir de n'importe quelle application de gestion de PDF enregistrée telle qu'Adobe Acrobat Reader.

Utiliser le pilote UPD pour les imprimantes créées automatiquement de manière standard

Pour activer l'impression universelle PDF pour toutes les imprimantes clientes redirigées dans une session à partir d'un client Mac, visitez Citrix Studio ou une console Web et configurez la stratégie de priorité du pilote d'impression universelle de manière à placer le format de métafichier PDF avant PS dans la liste des priorités.

Une fois cette modification effectuée, les imprimantes créées automatiquement qui utilisent un pilote universel avec un client Mac compatible PDF utilisent le pilote d'impression universel PDF Citrix au lieu du pilote HP Color LaserJet 2800 Series PS sur l'hôte.
Lorsque vous utilisez l'une des imprimantes créées automatiquement dans une session, le PDF est utilisé en tant que format intermédiaire de la tâche d'impression, mais la sortie d'impression est directement dirigée vers l'imprimante connectée au client sélectionnée.

Authentification

July 19, 2022

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 3.12 et versions ultérieures.
- Citrix Virtual Apps and Desktops 7 2203 et versions ultérieures.
- XenApp et XenDesktop 7.15 et versions ultérieures.
- Les applications activées pour carte à puce, telles que Microsoft Outlook et Microsoft Office, permettent aux utilisateurs de signer numériquement ou de crypter des documents disponibles dans les sessions d'application ou de bureau virtuel.
- 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.

Accès conditionnel avec Azure Active Directory

Cette méthode d'authentification n'est pas actuellement prise en charge sur l'application Citrix Workspace pour Mac.

Sécuriser les communications

August 24, 2022

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 un pare-feu 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 chiffrement 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 :

Client cipher set	VDA cipher set	Direct connections								
		TLS			DTLS v1.0			DTLS v1.2		
		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		

Client cipher set	VDA cipher set	External connections with Citrix Gateway								
		TLS			DTLS v1.0			DTLS v1.2		
		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. Donc, `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 et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), puis 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.

Installez le certificat racine sur chaque appareil, en fonction des stratégies et des procédures de votre organisation au lieu de 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. Cette action 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 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. 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 con-

> trôlés 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 :

- **None**. 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. 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. 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 de l'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 aux administrateurs de révoquer des certificats de sécurité (invalidés avant leur date d'expiration) dans le cas où les clés privées du certificat sont corrompue, ou simplement en cas de changements inattendus 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, 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.

> **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 auparavant.

<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 plusieurs valeurs doivent être spécifiées, séparez les valeurs 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

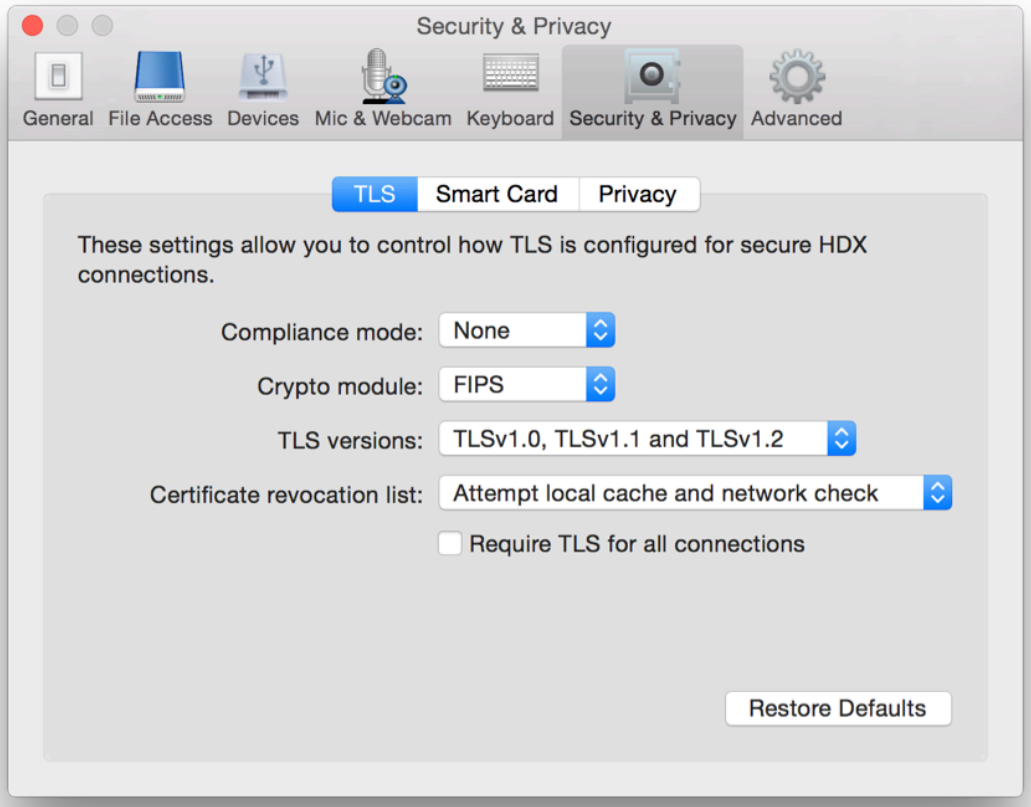
Des améliorations liées à la sécurité ont été introduites dans la version 12.3 de Citrix Receiver pour Mac, notamment :

- 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 des sessions sont désormais simplifiés et accessibles depuis l'interface utilisateur. Cette amélioration optimise l'expérience utilisateur tout en créant une méthode transparente pour l'adoption des préférences liées à la sécurité.
- Connexions TLS. Vous pouvez vérifier les connexions qui utilisent une version TLS, des algorithmes de chiffrement, 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