



Application Citrix Workspace pour Mac

Contents

Application Citrix Workspace pour Mac	3
À propos de cette version	5
Fonctionnalités de la version Technical Preview	94
Prise en charge native de Mac avec la puce Apple (M1 et M2)	115
Configuration système requise et compatibilité	119
Installer, désinstaller et mettre à niveau	125
Mise à jour	129
Configurer l'application Citrix Workspace	140
Gestion des appareils mobiles	141
Configuration du magasin	148
Sécurité et authentification	153
Authentification	154
Sécurité	161
Sécuriser les communications	163
Expérience de l'application	173
Mise à disposition d'applications	173
Expérience de lancement d'applications et de bureaux virtuels améliorée pour Workspace (utilisateurs cloud uniquement)	175
Préférences de l'application	176
Collecte et surveillance des données	192
HDX et multimédia	195
Graphisme et affichage	196
Microsoft Teams optimisé	201

Transport HDX	208
Appareils	209
Audio et microphone	210
Mappage des lecteurs clients	212
Clavier	213
Impression	231
USB	233
Webcam	238
Expérience de session	240
Dépannage	248
Fin de prise en charge	252

Application Citrix Workspace pour Mac

June 26, 2024

L'application Citrix Workspace pour Mac est une application facile à installer qui vous permet d'accéder à vos applications et bureaux à l'aide de Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) à partir d'une machine cliente distante. L'application Citrix Workspace pour Mac combine facilité de déploiement et d'utilisation, et offre un accès rapide et sécurisé aux applications et bureaux hébergés.

Pour obtenir des informations détaillées sur les fonctionnalités, les problèmes résolus et les problèmes connus, consultez la page [À propos de cette version](#).

Pour plus d'informations sur les éléments obsolètes, consultez la page [Fin de prise en charge](#).

Vous pouvez utiliser l'application Citrix Workspace sur différents appareils exécutant macOS. Pour plus d'informations sur les fonctionnalités disponibles dans l'application Citrix Workspace pour Mac, consultez [Tableau des fonctionnalités de l'application Citrix Workspace](#).

Langues prises en charge

L'application Citrix Workspace pour Mac a été conçue pour être utilisée dans des langues autres que l'anglais. Pour obtenir la liste des langues prises en charge par l'application Citrix Workspace pour Mac, consultez la section [Langues prises en charge](#).

Versions antérieures

[Application Citrix Workspace 2402 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2311 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2309 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2308 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2307 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2306 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2305 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2304 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2301.1 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2301 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2211 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2210 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2209 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2208.1 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2206.1 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2204 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2203.1 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2201 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2112 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2111 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2110 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2107 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2104 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2102 pour Mac \(PDF\)](#)

[Application Citrix Workspace 2101 pour Mac \(PDF\)](#)

La documentation relative à ces versions de produit est fournie sous forme de fichiers PDF car il ne s'agit pas des versions les plus récentes. Pour obtenir le contenu le plus récent, consultez la documentation de la version actuelle de l'[application Citrix Workspace pour Mac](#). Cette documentation inclut des instructions pour la mise à niveau de versions antérieures.

REMARQUE :

Les liens vers les sites Web externes figurant dans ces fichiers PDF vous conduisent aux pages adéquates, mais les liens pointant vers d'autres sections au sein du fichier PDF ne sont plus utilisables.

Articles de référence

- [Fiche technique : Citrix Workspace](#)
- [Documentation du développeur](#)
- [Service Global App Configuration](#)
- [App Protection](#)
- [Interface utilisateur de Workspace](#)
- [Optimisation de Microsoft Teams dans les environnements Citrix Virtual Apps and Desktops](#)
- [Application Citrix Workspace pour iOS](#)
- [Calendrier de publication de l'application Citrix Workspace](#)

Nouveautés dans les produits associés

- Citrix Enterprise Browser : [À propos de cette version](#)
- Citrix Workspace : [Nouveautés](#)
- Citrix DaaS : [Nouveautés](#)
- StoreFront : [Nouveautés](#)
- Secure Private Access : [Nouveautés](#)

Ancienne documentation

Pour les versions de produits qui ont atteint leur fin de vie, consultez la section [Ancienne documentation](#).

À propos de cette version

June 27, 2024

Découvrez les nouvelles fonctionnalités, les améliorations, les problèmes résolus et les problèmes connus de l'application Citrix Workspace pour Mac.

Nous tenons à jour une liste des fonctionnalités dans la section [Fonctionnalités de la version Technical Preview](#) afin que vous puissiez y accéder en un seul endroit. Découvrez nos fonctionnalités de la version Technical Preview et partagez vos commentaires en utilisant le lien vers le formulaire Podio ci-joint.

Remarque :

Le service de mise à jour automatique est pris en charge sur la version 2304 ou ultérieure. Si vous utilisez la version 2301 ou antérieure de l'application Citrix Workspace pour Mac, vous ne pouvez pas effectuer la mise à jour vers les dernières versions via le service de mise à jour automatique. Dans ce cas, vous devrez installer manuellement la version 2304 ou ultérieure de l'application Citrix Workspace pour Mac en téléchargeant le fichier .dmg disponible sur la page [Téléchargements](#). Pour plus d'informations, consultez la section [Installation manuelle](#).

Prise en charge native de Mac avec la puce Apple (M1 et M2) - Architecture universelle

Avec la publication de la version Architecture universelle, l'application Citrix Workspace fournit désormais un support natif pour les Mac équipés de la puce Apple (séries M1 et M2). La version Architecture universelle peut s'exécuter sur n'importe quel appareil Mac, quelle que soit l'architecture de son processeur.

Si vous utilisez la version d'architecture basée sur Intel x86_64 de l'application Citrix Workspace pour Mac avec la puce Apple, vous devez utiliser l'émulation Rosetta pour exécuter l'application.

Vous pouvez télécharger la dernière version Architecture universelle et la version d'architecture basée sur Intel x86_64 à partir de [Téléchargements](#).

Remarque :

Citrix continue de prendre en charge les Mac dotés d'un processeur Intel et les Mac dotés de la puce Apple (séries M1 et M2). Cependant, Citrix abandonnera bientôt la version d'architecture basée sur Intel x86_64 pour les Mac dotés d'un processeur Intel. Citrix continue de prendre en charge la version Architecture universelle pour les Mac dotés d'un processeur Intel et les Mac dotés de la puce Apple (séries M1 et M2). 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 et M2), vous devez mettre à niveau le HDX RealTime Optimization Pack (RTOP). Cette mise à niveau 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 native de la puce Apple](#).

Nouveautés de la version 2402.10

Cette version 2402.10 résout certains problèmes afin d'améliorer la stabilité et les performances générales.

Améliorations apportées à la fonctionnalité de fermeture de l'application Citrix Workspace

À partir de la version 2402.10, la fonctionnalité de fermeture de l'application Citrix Workspace est améliorée et correspond au comportement du menu Quitter d'Apple. Lorsque vous quittez l'application Citrix Workspace à l'aide de l'une des options suivantes, l'application se ferme et ne s'exécute plus en arrière-plan.

- **Quitter Citrix Workspace** depuis la barre de menu
- **Quitter** depuis le dock

- **Quitter** depuis le menu Accès rapide, ou
- Appuyer sur les touches **Command-Q**.

Problèmes résolus dans la version 2402.10

- La vulnérabilité de sécurité qui permettait aux utilisateurs locaux authentifiés d'élever leurs privilèges au rang d'utilisateurs root a été corrigée. Pour plus d'informations, veuillez consulter l'article [CTX675851](#). [CVE-2024-5027]

Problèmes connus dans la version 2402.10

- Si le paramètre « Forcer les profils éphémères » est activé via le service Global App Configuration pour Citrix Enterprise Browser et que l'utilisateur ferme la ou les fenêtres du navigateur sans quitter le navigateur, la création de nouveaux onglets et la saisie dans l'omnibox risquent de ne pas fonctionner comme prévu. Pour résoudre ce problème, l'utilisateur doit quitter complètement le navigateur, puis le rouvrir. [CTXBR-8738]

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](#).

2402

Nouveautés

Amélioration de l'expérience de chargement des applications et des postes de travail virtuels pour les déploiements sur site L'application Citrix Workspace pour Mac a amélioré l'expérience utilisateur pour la première fois pour les déploiements sur site. Une fois l'authentification réussie, l'énumération des applications et des postes de travail virtuels est plus rapide qu'auparavant.

Support pour le décodage vidéo H.265 À partir de la version 2402, l'application Citrix Workspace pour Mac prend en charge l'utilisation du codec vidéo H.265 (HEVC) pour l'accélération matérielle des graphiques et vidéos distants. Le codec vidéo H.265 (HEVC) prend en charge l'espace colorimétrique YUV 4:2:0 par défaut. Le codec vidéo H.265 doit être pris en charge et activé à la fois sur le VDA et sur l'application Citrix Workspace. Si votre périphérique Mac ne prend pas en charge le décodage H.265

à l'aide de l'interface VideoToolbox, le paramètre de stratégie de décodage H265 pour les graphiques est ignoré et la session utilise le codec vidéo H.264. Pour plus d'informations, consultez la section [Support pour le décodage vidéo H.265](#).

Prise en charge des raccourcis système sur les sessions de bureau HDX Auparavant, les raccourcis clavier du système tels qu'**Option-Commande-Echap**, **Commande-Touche espace**, **Command-Tab**, **Contrôle-Commande-Q**, **Maj-Commande-Q**, **Contrôle flèche haut/bas/gauche/droite** ne s'appliquaient que sur macOS localement, puisqu'ils étaient utilisés uniquement par macOS.

À partir de la version 2402, l'application Citrix Workspace pour Mac prend en charge la transmission des raccourcis clavier du système macOS au VDA (session HDX) en mode fenêtre et en mode plein écran. Cette fonctionnalité vous permet de définir des préférences d'application du raccourci système sur macOS localement ou sur la session de bureau HDX en mode fenêtre ou plein écran.

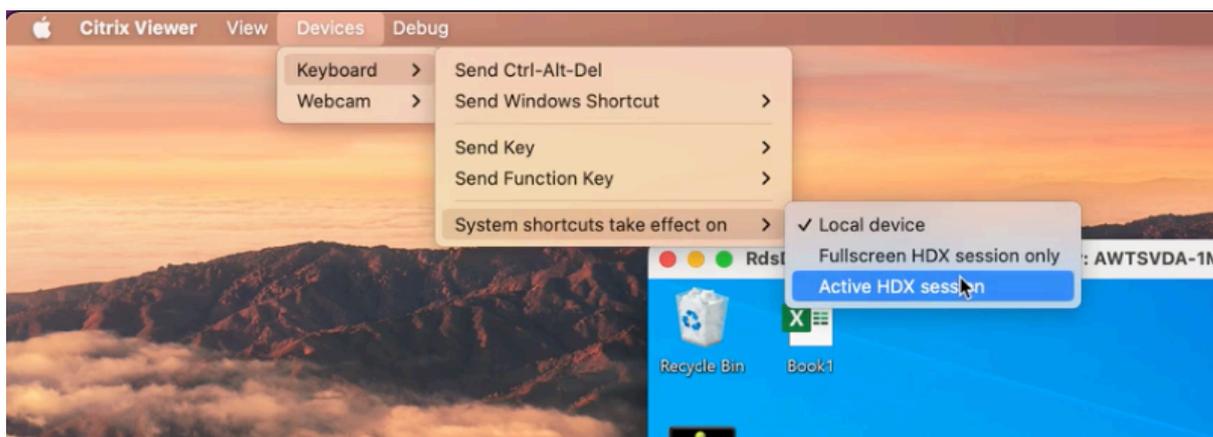
Les options suivantes des paramètres du clavier vous permettent de contrôler les raccourcis système :

- **Périphérique local** : les raccourcis système ne peuvent être appliqués que sur macOS localement. Cela n'affecte pas la session HDX. L'option **Périphérique local** est l'option par défaut.
- **Session HDX en plein écran uniquement** : les raccourcis système sont appliqués sur les sessions HDX lorsque la session est en mode plein écran. Si la session est en mode fenêtre ou s'il n'y a aucune session active, les raccourcis système ne s'appliquent pas sur les sessions HDX.
- **Session HDX active** : les raccourcis système sont appliqués sur les sessions HDX lorsque la session est en mode fenêtre et en mode plein écran. S'il n'y a pas de session HDX active ou s'il n'y a pas de fenêtre de session active sur la face avant, les raccourcis système ne peuvent être appliqués que sur macOS localement.

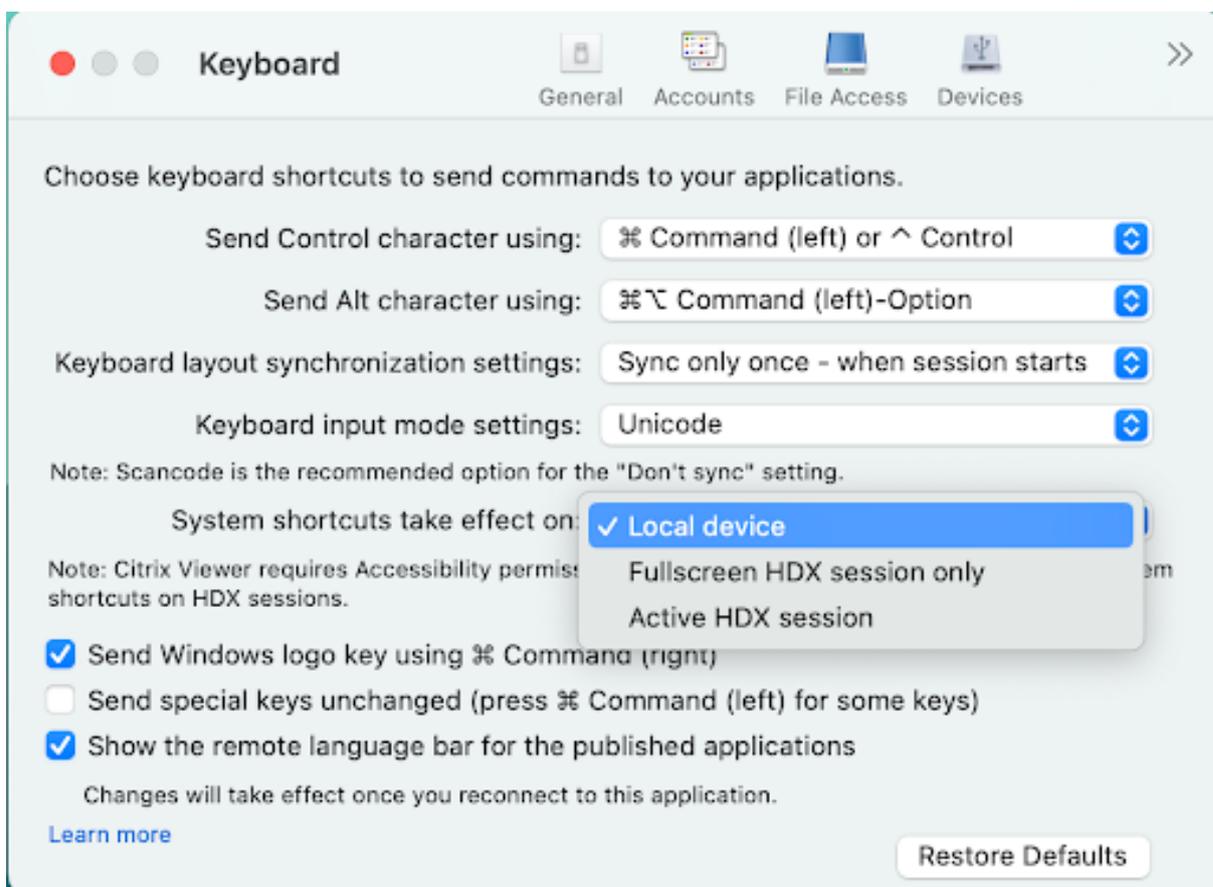
Pour que les raccourcis système soient appliqués sur la session HDX, ouvrez la session HDX. Dans la barre de menus de **Citrix Viewer**, accédez à **Périphériques > Clavier > Les raccourcis système prennent effet sur** et sélectionnez **Session HDX plein écran uniquement** ou **Session HDX active**.

Remarque :

Lorsque vous activez les raccourcis système pour les sessions HDX, vous êtes invité à fournir un accès en accessibilité à Citrix Viewer pour utiliser cette fonctionnalité. Pour fournir un accès en accessibilité à **Citrix Viewer**, cliquez sur **Ouvrir les paramètres système** dans la boîte de dialogue et activez l'accès en accessibilité à **Citrix Viewer**. Pour plus d'informations, consultez la section [Autoriser des apps d'accessibilité à accéder à votre Mac](#) dans l'article du support Apple.

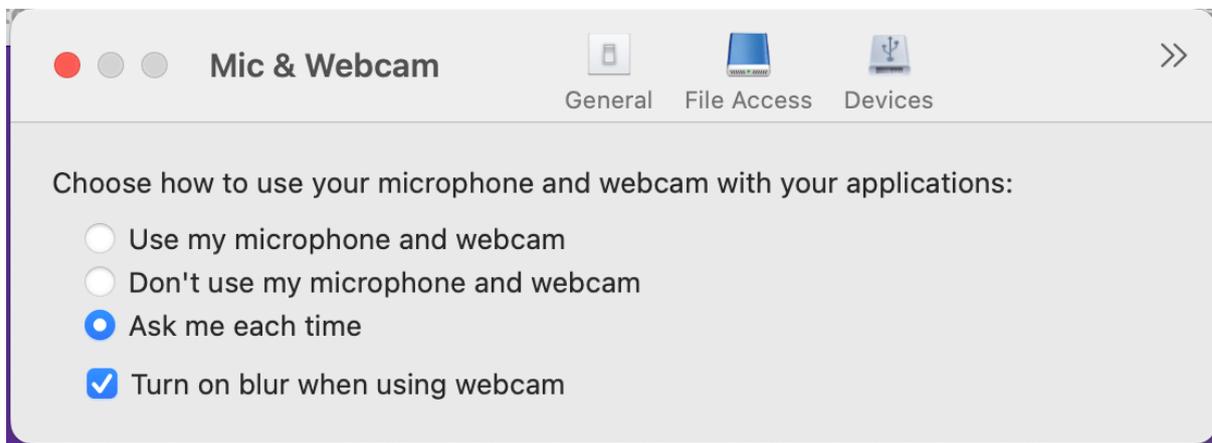


Vous pouvez également activer les raccourcis système pour qu'ils soient appliqués aux sessions HDX en mode plein écran ou en mode fenêtre en accédant à **Préférences > Clavier**. Sélectionnez l'option **Session HDX en plein écran uniquement** ou **Session HDX active** dans le menu déroulant **Les raccourcis système prennent effet sur**.



Pour plus d'informations, consultez la section [Prise en charge des raccourcis système sur les sessions de bureau HDX](#).

Prise en charge du flou d'arrière-plan pour la webcam À partir de la version 2402, l'application Citrix Workspace pour Mac prend en charge le flou d'arrière-plan lors de l'utilisation d'une webcam. Vous pouvez activer la fonctionnalité de flou d'arrière-plan en accédant à **Préférences > Micro et webcam** et en sélectionnant **Activer le flou lorsque vous utilisez la webcam**. Pour plus d'informations, consultez [Prise en charge du flou d'arrière-plan pour la webcam](#).



Prise en charge de la synchronisation du volume audio Auparavant, le contrôle du volume audio était indépendant entre le Virtual Delivery Agent (VDA) et votre appareil. Vous devez régler le volume des deux côtés pour maintenir le volume souhaité. De plus, si vous avez désactivé le volume de votre appareil, vous ne pouvez pas le réactiver sur le VDA.

À partir de la version 2402, l'application Citrix Workspace pour Mac prend en charge la synchronisation du volume audio entre le VDA et vos périphériques audio. Vous pouvez désormais régler le volume à l'aide du curseur de volume audio du VDA pour avoir le même volume que sur votre appareil et vice versa. Cette fonctionnalité est activée par défaut. Pour plus d'informations, consultez [Prise en charge de la synchronisation du volume audio](#).

Mode de tolérance de pertes pour l'audio À partir de la version 2402, l'application Citrix Workspace prend en charge le mode de tolérance de pertes (compression avec perte EDT) pour la redirection audio. Cette fonctionnalité améliore l'expérience utilisateur pour le streaming en temps réel lorsque les utilisateurs se connectent via des réseaux à latence élevée et à perte de paquets. Cette fonctionnalité est activée par défaut. Pour plus d'informations, consultez la section [Mode de tolérance de pertes pour l'audio](#).

Réducteur HDX mis à niveau vers la version 4 Auparavant, l'application Citrix Workspace pour Mac prenait en charge le réducteur HDX V3. À partir de la version 2402, l'application Citrix Workspace pour Mac prend en charge le réducteur HDX V4. Cette fonctionnalité réduit la bande passante réseau

requis pour une session type et améliore le temps de réponse. Pour plus d'informations, consultez la section [Réducteur HDX mis à niveau vers la version 4](#).

Prise en charge du partage d'écran lorsque App Protection est activée À partir de la version 2402, vous pouvez partager du contenu via Microsoft Teams avec l'optimisation HDX, même lorsque App Protection est activée. Grâce à cette fonctionnalité, vous pouvez partager un écran dans la session de bureau virtuel dans son intégralité. Pour plus d'informations, consultez la section [Compatibilité avec l'optimisation HDX pour Microsoft Teams](#).

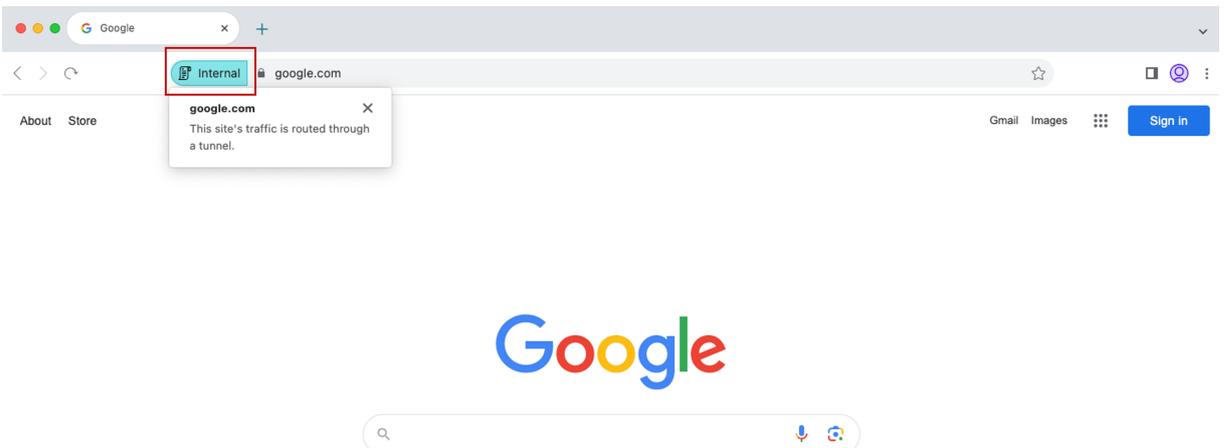
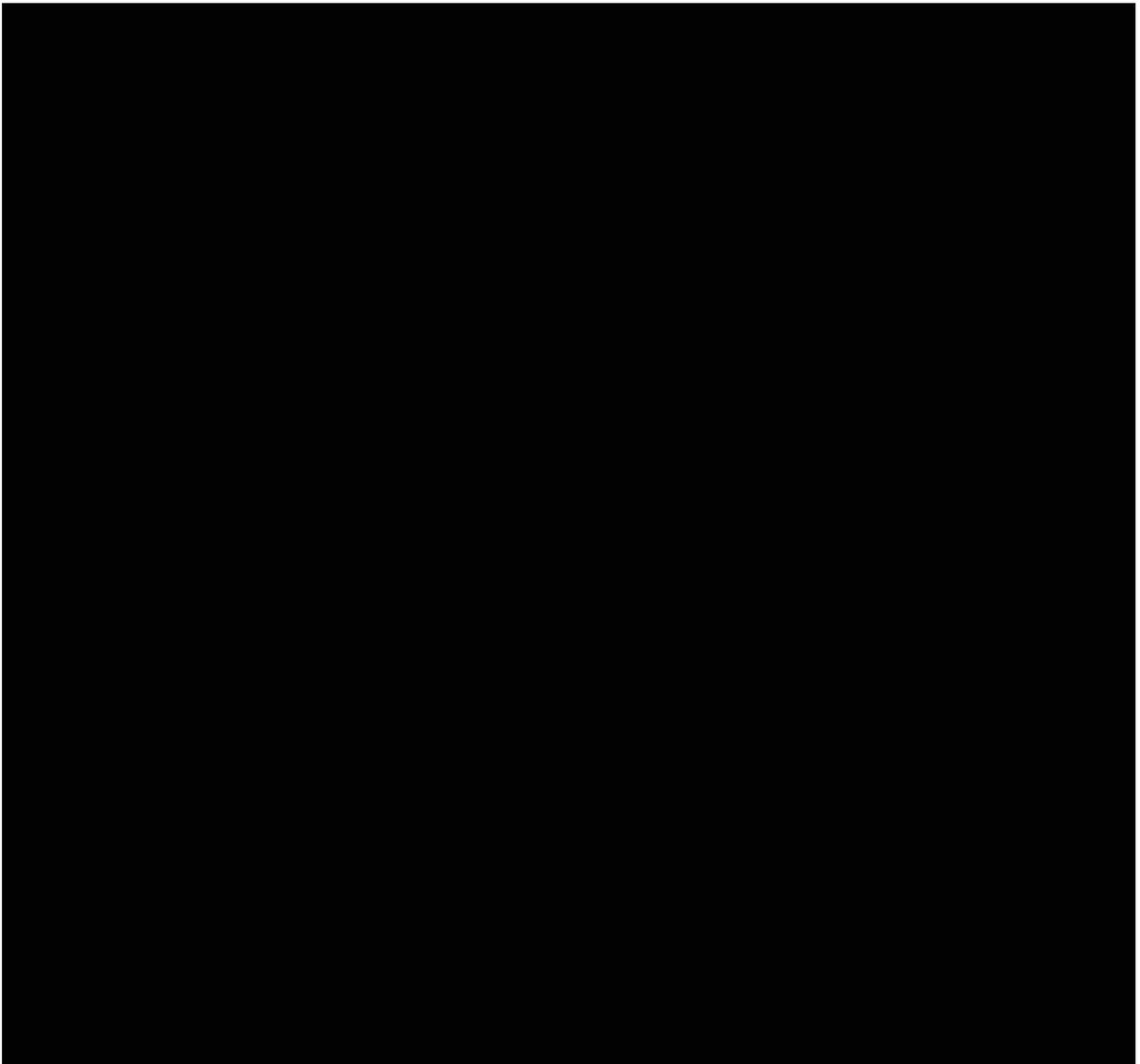
Amélioration de Global App Configuration Service À partir de la version 2402, le service GACS (Global App Configuration Service) amélioré pour Citrix Workspace prend désormais en charge les fonctionnalités suivantes :

- Paramètres sécurisés grâce à l'authentification utilisateur
- Amélioration du workflow de découverte
- Prise en charge de l'URL complète de StoreFront

Pour plus d'informations, consultez [Global App Configuration Service](#).

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 121.1.1.26, basé sur Chromium version 121. Pour plus d'informations, consultez la documentation de [Citrix Enterprise Browser](#).

Indicateur de sécurité lors de la visite de sites Web Citrix Enterprise Browser affiche désormais un indicateur de sécurité dans la barre d'adresses lorsque les utilisateurs consultent des sites Web. L'indicateur vise à informer les utilisateurs sur les aspects de sécurité des sites Web, par exemple s'il s'agit d'un site interne ou s'il existe des restrictions de sécurité potentielles. L'indicateur fournit plus d'informations lorsque vous cliquez dessus. L'indicateur apparaît par défaut sur Citrix Enterprise Browser et améliore l'expérience utilisateur.



Simplification de l'authentification unique pour accéder aux applications Web et SaaS grâce à Global App Configuration Service

REMARQUE :

Pour le système d'exploitation Mac, cette fonctionnalité n'était auparavant disponible que pour StoreFront à partir de la version 119.1.1.115. Désormais, avec la sortie de la version 121.1.1.26, elle est également disponible pour Workspace.

Auparavant, l'authentification unique (SSO) était configurée dans Citrix Enterprise Browser au moyen du module PowerShell. À partir de cette version, vous pouvez configurer la fonctionnalité SSO simplifiée dans Citrix Enterprise Browser à l'aide d'un paramètre récemment introduit dans Global App Configuration Service (GACS). Les administrateurs peuvent utiliser ce nouveau paramètre pour activer la SSO pour toutes les applications Web et SaaS dans Citrix Enterprise Browser. Cette méthode permet de se passer du module PowerShell complexe.

Pour plus d'informations sur la gestion de l'authentification unique via GACS, consultez la section Gestion de l'authentification unique pour les applications Web et SaaS via Global App Configuration Service.

Citrix Enterprise Browser introduit des paramètres supplémentaires dans Global App Configuration Service Les paramètres supplémentaires suivants ont été ajoutés à Global App Configuration Service (GACS) pour configurer Citrix Enterprise Browser :

- « Activer le remplissage automatique des adresses » - Permet aux administrateurs d'activer ou de désactiver les suggestions de remplissage automatique pour les adresses.
- « Activer le remplissage automatique des cartes de crédit » - Permet aux administrateurs d'activer ou de désactiver les suggestions de remplissage automatique pour les informations de carte de crédit.
- « Protocoles de lancement automatique à partir des origines » - Permet aux administrateurs de spécifier une liste de protocoles qui peuvent lancer une application externe à partir des origines répertoriées sans en informer l'utilisateur.
- « Activer les avertissements de sécurité des indicateurs de ligne de commande » - Permet aux administrateurs d'afficher ou de masquer les avertissements de sécurité, qui apparaissent lorsque des indicateurs de ligne de commande potentiellement dangereux tentent de lancer Enterprise Browser.
- « Paramètre de gestion des cookies par défaut » - Permet aux administrateurs de gérer les cookies d'un site Web.
- « Paramètre de gestion des fenêtres contextuelles par défaut » - Permet aux administrateurs de gérer les fenêtres contextuelles d'un site Web.
- « Sources d'installation des extensions » - Permet aux administrateurs de spécifier des sources valides pour que les utilisateurs puissent installer des extensions, des applications et des thèmes.

- « Désactiver les pages d'avertissement similaires » - Permet aux administrateurs d'indiquer des domaines préférés dans lesquels les pages d'avertissement similaires ne s'afficheront pas lorsque l'utilisateur en consulteront les pages.
- « Activer la requête de mode de paiement » - Permet aux administrateurs d'autoriser les sites Web à vérifier si les utilisateurs ont enregistré des modes de paiement.
- « Gérer l'enregistrement de l'historique du navigateur » - Permet aux administrateurs de gérer l'enregistrement de l'historique de Citrix Enterprise Browser.
- « Gérer les suggestions de recherche » - Permet aux administrateurs d'activer ou de désactiver les suggestions de recherche dans la barre d'adresses d'Enterprise Browser.
- « Activer l'exportation des signets » - Permet aux administrateurs d'activer une option permettant d'exporter les signets dans Enterprise Browser.
- « Forcer les profils éphémères » - Permet aux administrateurs d'effacer ou de conserver les données du profil utilisateur lorsque les utilisateurs ferment Enterprise Browser.

Pour plus d'informations, consultez la section [Utiliser Global App Configuration Service pour gérer Citrix Enterprise Browser](#).

Technical Preview

- Prise en charge de l'authentification unique pour accéder à Citrix Secure Access automatiquement via l'application Citrix Workspace
- Gestion des applications clientes pour le plug-in Zoom VDI
- Barre d'outils de Desktop Viewer améliorée
- Personnaliser la barre d'outils de Desktop Viewer
- Activer la dissimulation de perte de paquets pour améliorer les performances audio
- Prise en charge de l'extension automatique de la session de bureau à des moniteurs externes
- Initiative de développement durable pour l'application Citrix Workspace

Pour obtenir la liste complète des fonctionnalités préliminaires (version Technical Preview), consultez la page [Fonctionnalités de la version Technical Preview](#).

Problèmes résolus

- Lorsque vous vous connectez à l'application Citrix Workspace pour Mac version 2311, le message d'erreur suivant peut s'afficher :

Http/1.1 Erreur interne du serveur 43524

[CVADHELP-24631]

- Vous remarquerez peut-être que les stratégies de Global App Configuration Service ne sont pas appliquées sur certains appareils Mac plus anciens. [CVADHELP-24863]

Problèmes connus

- Vous remarquerez peut-être que l'écran de l'application est masqué au niveau de l'encoche lorsque vous passez en plein écran dans les sessions virtuelles sur certains Mac. Pour contourner le problème, ajustez la fenêtre de l'application pour qu'elle s'insère sous l'encoche de l'écran. [HDX-63035]

2311

Nouveautés

Prise en charge de l'authentification à l'aide de FIDO2 lors de la connexion à des magasins locaux Auparavant, l'authentification sans mot de passe basée sur FIDO2 était prise en charge pour la connexion aux magasins cloud. Pour plus d'informations, consultez [Authentification basée sur FIDO2 lors de la connexion à un magasin cloud](#).

Avec cette version, les utilisateurs peuvent également se connecter aux magasins locaux à l'aide de l'authentification FIDO2. Les clés de sécurité FIDO2 permettent aux employés de l'entreprise de s'authentifier auprès d'applications ou de bureaux prenant en charge FIDO2 sans entrer de nom d'utilisateur ou de mot de passe. Cette fonctionnalité prend actuellement en charge les authentificateurs itinérants (USB uniquement) avec code PIN et Touch ID. Cette fonctionnalité est prise en charge sur macOS 12 et versions ultérieures. Pour plus d'informations, consultez [Authentification basée sur FIDO2 lors de la connexion à un magasin local](#).

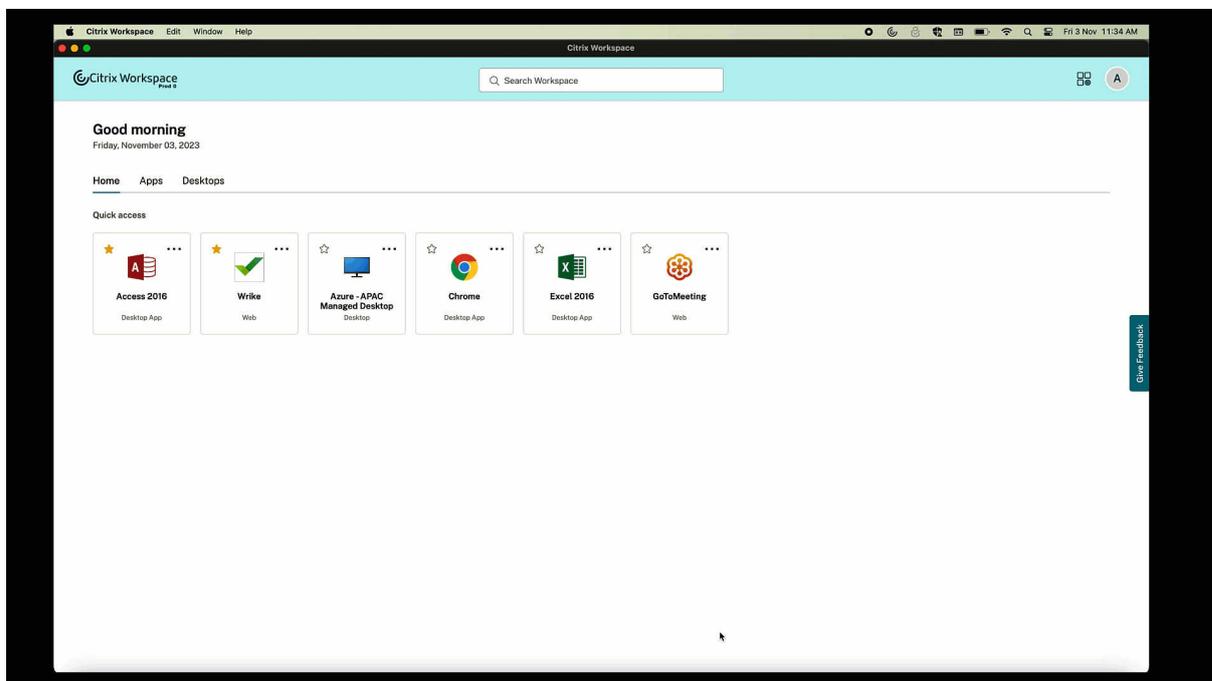
Architecture universelle améliorée conçue pour les sessions d'application et de bureau virtuels

À partir de la version 2311, la version Architecture universelle peut désormais choisir automatiquement d'exécuter les sessions virtuelles en mode Apple Silicon natif ou en mode Intel sur les Mac équipés du chipset Apple Silicon. Elle utilise l'émulation Rosetta pour lancer la session virtuelle en mode Intel. La session virtuelle est lancée en mode Apple Silicon natif, si le SDK de canal virtuel est créé sur la base de l'architecture Apple Silicon native ou s'il n'existe aucun SDK de canal virtuel. Cependant, la session virtuelle est lancée en mode Intel à l'aide de l'émulation Rosetta, si le SDK du canal virtuel est créé sur la base de l'architecture Intel x86_64.

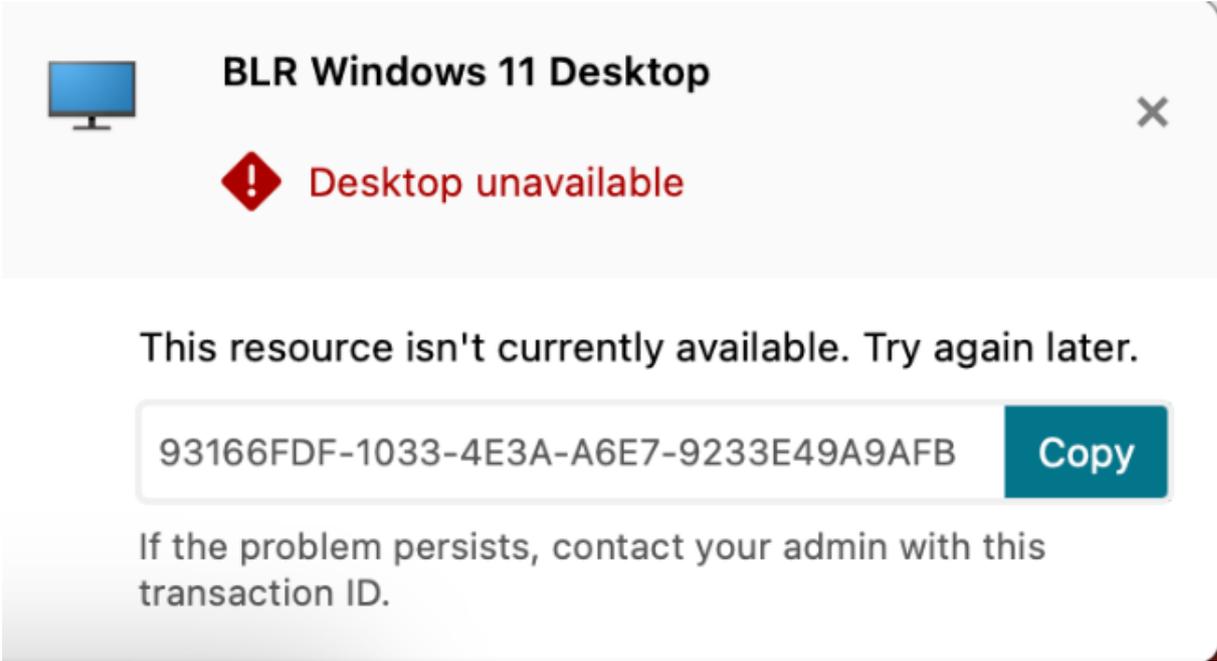
Cette amélioration de la version Architecture universelle optimise l'expérience de lancement sur les Mac équipés du chipset Apple Silicon. Pour les utilisateurs de Mac équipés d'un chipset Intel, il n'y a aucun changement, et la version Architecture universelle continue d'exécuter les sessions virtuelles de manière native.

Pour plus d'informations, consultez [Architecture universelle améliorée conçue pour les sessions d'application et de bureau virtuels](#).

Expérience de lancement d'applications et de bureaux virtuels améliorée pour Workspace (utilisateurs cloud uniquement) L'ouverture des ressources Citrix a été améliorée pour être plus intuitive, informative et conviviale. À partir de la version 2311, cette fonctionnalité est prise en charge pour les magasins en ligne personnalisés et les lancements hybrides.



La notification de progression du lancement apparaît désormais dans le coin inférieur droit de votre écran. L'état de progression des ressources en cours d'ouverture est affiché. Vous ne pouvez pas récupérer la notification une fois que vous l'avez ignorée. La notification est conservée pendant quelques secondes à compter du début de la session. Si la session ne démarre pas, la notification affiche le message d'échec. Pour plus d'informations, consultez [Expérience de lancement d'applications et de bureaux virtuels améliorée pour Workspace \(utilisateurs cloud uniquement\)](#).



The screenshot shows a window titled "BLR Windows 11 Desktop" with a close button (X) in the top right corner. Below the title bar, there is a red diamond icon with a white exclamation mark, followed by the text "Desktop unavailable". Below this, a message states: "This resource isn't currently available. Try again later." Underneath the message is a text input field containing the transaction ID "93166FDF-1033-4E3A-A6E7-9233E49A9AFB" and a teal "Copy" button. At the bottom of the message box, it says: "If the problem persists, contact your admin with this transaction ID."

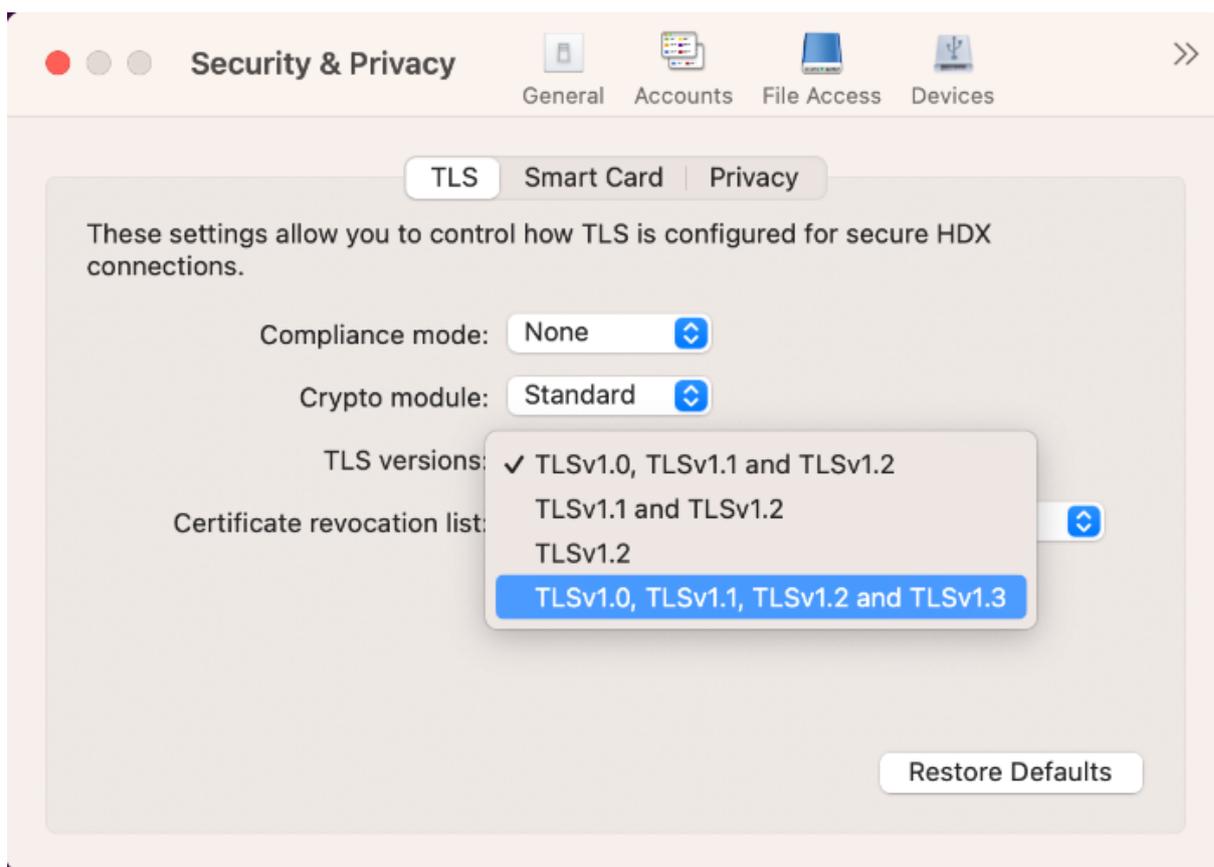
Remarque :

Cette fonctionnalité est disponible à la fois pour les sessions Workspace (cloud) et StoreFront.

SDK du canal virtuel Citrix modernisé pour l'application Citrix Workspace pour Mac À compter de la version 2311, le VCS SDK du canal virtuel Citrix prend en charge l'écriture d'applications du côté serveur et de pilotes 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. Cette version du SDK prend en charge l'écriture de nouveaux canaux virtuels et le partage d'écran pour l'application Citrix Workspace pour Mac.

Pour plus d'informations, consultez la section [SDK du canal virtuel Citrix pour l'application Citrix Workspace pour Mac](#) dans la documentation du développeur et la section [SDK du canal virtuel Citrix modernisé pour l'application Citrix Workspace pour Mac](#).

Prise en charge du protocole TLS version 1.3 À partir de la version 2311, l'application Citrix Workspace pour Mac prend en charge le dernier protocole TLS (Transport Layer Security) version 1.3. Pour activer le protocole TLS version 1.3, accédez à **Préférences > Sécurité et confidentialité > TLS** et sélectionnez l'option **TLSv1.0, TLSv1.1, TLSv1.2 et TLSv1.3** dans le menu déroulant **Versions TLS**.



Pour plus d'informations, consultez la section [TLS](#).

Prise en charge de plusieurs périphériques audio À partir de la version 2311, l'application Citrix Workspace pour Mac affiche tous les périphériques audio locaux disponibles dans une session, accompagnés de leur nom. En outre, la fonctionnalité Plug and Play est également prise en charge. Pour plus d'informations, consultez la section [Prise en charge de plusieurs périphériques audio](#).

Prise en charge de l'extension de plusieurs moniteurs en mode plein écran sur un maximum de cinq moniteurs Auparavant, Citrix prenait en charge un maximum de trois moniteurs en mode plein écran, y compris le moniteur principal.

À partir de la version 2311, vous pouvez désormais utiliser le mode plein écran sur un maximum de cinq moniteurs simultanément, y compris le moniteur principal. Pour plus d'informations, consultez la section [Prise en charge de l'extension de plusieurs moniteurs en mode plein écran sur un maximum de cinq moniteurs](#).

Fin de la prise en charge du menu International dans les paramètres du clavier Auparavant, vous pouviez activer ou désactiver les fonctionnalités **Utiliser l'éditeur IME du client**, **Utiliser mar-**

ques de composition et Utiliser disposition du clavier client dans Citrix Viewer en accédant à **Appareils > Clavier > International**.

À partir de la version 2311, le menu **International** pour les paramètres du clavier dans Citrix Viewer n'est plus pris en charge. À partir de cette version, l'éditeur IME côté client est activé par défaut. Pour plus d'informations, consultez la section [Fin de la prise en charge du menu International dans les paramètres du clavier](#).

Annnonce de fin de prise en charge du format SDP (Plan B) de WebRTC Citrix prévoit de mettre fin à la prise en charge actuelle du format SDP (Plan B) de WebRTC dans les prochaines versions. Vous devez utiliser une version de l'application Citrix Workspace compatible avec le format Unified Plan pour continuer à utiliser certaines fonctionnalités de Microsoft Teams optimisé. Pour plus d'informations, consultez [Annnonce de fin de prise en charge du format SDP \(Plan B\) de WebRTC](#).

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 119.1.1.115, basé sur Chromium version 119. Pour plus d'informations, consultez la documentation de [Citrix Enterprise Browser](#).

Amélioration de l'expérience utilisateur Auparavant, Citrix Enterprise Browser affichait une fenêtre modale de reconnexion lorsque vous tentiez d'effectuer une action après l'expiration de votre session. À partir de la version 2311 de l'application Citrix Workspace pour Mac (qui correspond à la version 119.1.1.115 de Chromium), il n'existe plus de fenêtre modale de reconnexion. À la place, une icône de chargement apparaît désormais dans l'onglet du navigateur lorsque vous tentez d'effectuer une action après l'expiration de votre session.

Amélioration du design des filigranes Citrix Enterprise Browser dispose désormais d'un nouveau design de filigranes. Moins intrusif, il offre une meilleure expérience utilisateur.

Prise en charge de l'extension de navigateur personnalisée Citrix Enterprise Browser a étendu ses fonctionnalités d'extension. Auparavant, seules les extensions du Chrome Web Store étaient autorisées. Citrix Enterprise Browser permet désormais d'ajouter des extensions personnalisées en toute sécurité. Les administrateurs peuvent configurer des extensions personnalisées dans la liste obligatoire. Les utilisateurs finaux peuvent accéder à ces extensions et les utiliser via `citrixbrowser://extensions` ou en cliquant sur l'option **Extensions** sous le bouton **Plus**, au besoin. Pour plus d'informations sur la configuration des extensions personnalisées, consultez la section [Extension de navigateur personnalisée obligatoire](#) dans la documentation de Citrix Enterprise Browser.

Simplification de la SSO aux applications Web et SaaS grâce à Global App Configuration Service

Remarque :

Cette fonctionnalité n'est disponible que pour StoreFront.

Auparavant, l'authentification unique était configurée dans Citrix Enterprise Browser au moyen du module PowerShell. À partir de cette version, cette fonctionnalité SSO simplifiée facilite la configuration de l'authentification unique dans Citrix Enterprise Browser à l'aide d'un paramètre récemment introduit dans Global App Configuration Service (GACS). Les administrateurs peuvent utiliser ce nouveau paramètre pour activer la SSO pour toutes les applications Web et SaaS dans Citrix Enterprise Browser. Cette méthode permet de se passer du module PowerShell complexe. Pour plus d'informations sur la gestion de l'authentification unique via GACS, consultez la section [Gestion de l'authentification unique pour les applications Web et SaaS via Global App Configuration Service](#).

Amélioration des fonctionnalités de surveillance des activités des utilisateurs finaux Auparavant, les administrateurs ne pouvaient pas surveiller les activités des utilisateurs finaux, telles que les applications consultées et le type de trafic. À partir de l'application Citrix Workspace pour Windows et Mac 2311 (correspondant à la version 119.1.1.115 de Chromium), il est désormais également possible de surveiller ces détails.

- **Application consultée** : Enterprise Browser fournit des informations sur toutes les applications auxquelles l'utilisateur final a accédé, à condition que l'application soit répertoriée dans le document de stratégie.
- **Type de trafic** : Enterprise Browser indique si les données sont envoyées directement ou via l'authentification Secure Private Access.

Pour surveiller les activités des utilisateurs finaux à partir d'Enterprise Browser, utilisez le service Citrix Analytics via votre compte Citrix Cloud. Une fois connecté à Citrix Cloud, accédez à **Analytics > Sécurité > Rechercher**. Recherchez ensuite **Applications et bureaux** dans la section **Recherche en libre-service**. Pour plus d'informations sur Citrix Analytics, consultez la section [Mise en route](#).

App Protection

Assistance à la configuration d'App Protection pour l'authentification et du Self-Service Plug-In pour les magasins locaux Auparavant, l'application Citrix Workspace pour Mac prenait en charge la configuration d'App Protection pour l'authentification et du Self-Service Plug-in à l'aide de l'interface utilisateur de Global App Configuration Service pour les clients des magasins cloud uniquement.

À compter de la version 2311, cette fonctionnalité est prise en charge pour les clients sur les magasins cloud et locaux. Pour plus d'informations, consultez la section [Configuration à l'aide de l'interface utilisateur de Global App Configuration Service](#) dans la documentation App Protection.

Technical Preview

- Mode de tolérance de pertes pour l'audio
- Prise en charge de la synchronisation du volume audio
- Support pour le décodage vidéo H.265
- Réducteur HDX mis à niveau vers la version 4

Pour obtenir la liste complète des fonctionnalités préliminaires (version Technical Preview), consultez la page [Fonctionnalités de la version Technical Preview](#).

Problèmes résolus

- Lorsque les utilisateurs ajoutent l'URL du magasin pour la première fois, il se peut qu'ils ne voient pas la fenêtre du navigateur d'authentification FIDO2. [RFMAC-14518]
- Lorsque vous utilisez l'application Citrix Workspace pour Mac pour accéder à des sessions virtuelles, la vitesse de défilement de la souris est peut-être trop rapide ou trop lente dans les sessions virtuelles. [CVADHELP-23514]
- Lorsque vous utilisez l'application Citrix Workspace pour Mac, il se peut que vous ne puissiez pas basculer entre les applications récentes au sein de la session d'application virtuelle en cliquant sur les touches **Options** + **tab** après la mise à niveau vers le VDA 2212 ou de version ultérieure. [CVADHELP-23464]
- Vous remarquerez peut-être que le dock macOS bloque la barre des tâches Windows de la session de l'application Remote Desktop Protocol lancée depuis l'application Citrix Workspace pour Mac. [CVADHELP-23681]
- Lorsque vous utilisez l'application Citrix Workspace pour Mac, vous pouvez rencontrer des problèmes d'authentification lorsqu'une session persistante est utilisée pour un magasin local. [CVADHELP-24062]

Problèmes connus

- La fonctionnalité de redirection vidéo HTML5 est désactivée par défaut dans l'application Citrix Workspace pour Mac à partir de la version 2311. [HDX-53015]

2309

Nouveautés

Compatibilité avec macOS 14 Sonoma L'application Citrix Workspace pour Mac est prise en charge sur macOS 14 Sonoma.

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 115.1.1.103, basé sur Chromium version 115. Pour plus d'informations, consultez la [documentation de Citrix Enterprise Browser](#).

Citrix va désormais publier des mises à niveau indépendantes pour Citrix Enterprise Browser. À partir de l'application Citrix Workspace 2309 pour Mac, vous pouvez mettre à niveau Citrix Enterprise Browser indépendamment vers des versions compatibles via la fonctionnalité de mise à jour automatique ou l'installer manuellement lorsque les mises à niveau sont disponibles dans la section [Téléchargements](#). Les mises à niveau indépendantes de Citrix Enterprise Browser ne sont prises en charge que sur la dernière version de l'application Citrix Workspace pour Mac.

Technical Preview

- Prise en charge de Citrix Secure Private Access pour les magasins locaux

Pour obtenir la liste complète des fonctionnalités préliminaires (version Technical Preview), consultez la page [Fonctionnalités de la version Technical Preview](#).

Problèmes résolus

- Dans Microsoft Teams optimisé, il est possible que vous entendiez la sonnerie de manière aléatoire si vous répondez à l'appel avant qu'il ne sonne. [HDX-55799]
- Les paramètres **USB** permettant de connecter automatiquement les périphériques, disponibles dans l'onglet **Périphériques** de la fenêtre **Préférences**, peuvent ne pas fonctionner comme prévu dans l'application Citrix Workspace 2308 pour Mac. [RFMAC-14658]
- Sur les appareils macOS Sonoma, lorsque vous copiez une image (format .jpeg/.png) depuis votre Mac vers la session virtuelle, l'image copiée dans la session virtuelle peut être corrompue. [HDX-55307]

Problèmes connus

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

2308

Nouveautés

Application Citrix Workspace pour Mac sous macOS Sonoma bêta L'application Citrix Workspace 2308 pour Mac a été testée sur macOS Sonoma Public Beta 7 version 23A5337a. Utilisez cette configuration dans un environnement de test et faites-nous part de vos [commentaires](#).

Performances graphiques améliorées À partir de la version 2308, les performances graphiques sont améliorées pour des sessions d'application transparentes. Cette fonctionnalité optimise également la charge d'utilisation du processeur. Pour plus d'informations, consultez la section [Performances graphiques améliorées](#).

Amélioration apportée au contrôle de la congestion du réseau À partir de la version 2308, le protocole de transport propriétaire de Citrix appelé Enlightened Data Transport (EDT) est amélioré pour contrôler efficacement la congestion du réseau. Cette fonctionnalité améliore le débit des données et réduit le temps de latence. Pour plus d'informations, consultez la section [Amélioration apportée au contrôle de la congestion du réseau](#).

Augmentation du nombre de canaux virtuels pris en charge Auparavant, l'application Citrix Workspace pour Mac prenait en charge jusqu'à 32 canaux virtuels. À partir de la version 2308, vous pouvez utiliser jusqu'à 64 canaux virtuels dans une session. Pour plus d'informations, consultez la section [Augmentation du nombre de canaux virtuels pris en charge](#).

App Protection

Prise en charge de la détection d'altération des stratégies La fonction de détection d'altération des stratégies empêche l'utilisateur d'accéder à la session d'application ou de bureau virtuel si les stratégies de prévention de capture d'écran et de protection contre l'enregistrement de frappe du composant App Protection sont altérées. Si une altération des stratégies est détectée, la session d'application ou de bureau virtuel est interrompue. Pour plus d'informations sur la fonctionnalité de détection d'altération des stratégies, consultez la section [Détection d'altération des stratégies](#).

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 115.1.1.103, basé sur Chromium version 115. Pour plus d'informations, consultez la [documentation de Citrix Enterprise Browser](#).

Technical Preview

- Amélioration de l'option DPI élevé
- Configuration de l'accès aux fichiers par magasin
- Prise en charge du Gestionnaire d'activités sur les magasins cloud
- Prise en charge du partage d'écran lorsque App Protection est activée
- Prise en charge de l'authentification à l'aide de FIDO2 lors de la connexion à des magasins locaux

Pour obtenir la liste complète des fonctionnalités préliminaires (version Technical Preview), consultez la page [Fonctionnalités de la version Technical Preview](#).

Problèmes résolus

- Lorsque vous utilisez l'application Citrix Workspace pour Mac pour accéder au bureau virtuel, la taille du pointeur de la souris dans le bureau virtuel peut fluctuer de manière irrégulière. [CVADHELP-23158]
- Les icônes des applications actives peuvent ne pas s'afficher dans le Gestionnaire d'activités. [WSUI-8011]
- L'application Citrix Workspace peut consommer beaucoup de mémoire après quelques minutes d'utilisation. [CVADHELP-23528]

Problèmes connus

- Après la mise à niveau de l'application Citrix Workspace pour Mac vers la version 2308, il est possible que la fenêtre des préférences ne réponde pas aux actions de l'utilisateur. Pour contourner ce problème, vous devez forcer la fermeture de l'application Citrix Workspace et la redémarrer. Pour plus d'informations sur la fermeture forcée d'une application sur Mac, consultez la section [Forcer la fermeture d'une application](#) dans l'article d'assistance Apple. [RFMAC-14596]

2307

Nouveautés

Prise en charge native pour les Mac équipés de puces M2 À compter de la version 2307, l'application Citrix Workspace pour macOS prend en charge la série M2 (ainsi que la série M1 qui était auparavant prise en charge) de la puce Apple en natif. Pour plus d'informations, consultez [Prise en charge native de la puce Apple](#).

Application Citrix Workspace pour Mac sous macOS Sonoma bêta L'application Citrix Workspace 2307 pour Mac a été testée sur macOS Sonoma Public Beta 1 version 23A5286i. 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 Sonoma bêta dans des environnements de production.

Abandon de la prise en charge de la version Catalina de macOS Comme annoncé dans la version 2304, la prise en charge de la version Catalina (10.15) de macOS est abandonnée dans la version 2307 et sera supprimée pour les prochaines versions. Pour plus d'informations, consultez [Fin de prise en charge](#).

Prise en charge de l'authentification à l'aide de FIDO2 lors de la connexion à un magasin cloud À partir de la version 2307, les utilisateurs peuvent s'authentifier à l'aide de l'authentification sans mot de passe basée sur FIDO2 lors de la connexion à un magasin cloud. Les clés de sécurité FIDO2 permettent aux employés de l'entreprise de s'authentifier auprès d'applications ou de bureaux prenant en charge FIDO2 sans entrer de nom d'utilisateur ou de mot de passe. Cette fonctionnalité prend actuellement en charge les authentificateurs itinérants (USB uniquement) avec code PIN et Touch ID. Cette fonctionnalité est prise en charge sur macOS 12 et versions ultérieures. Pour plus d'informations, consultez [Authentification basée sur FIDO2 lors de la connexion à un magasin cloud](#).

Prise en charge de l'authentification à l'aide de FIDO2 dans une session HDX À partir de la version 2307, les utilisateurs peuvent s'authentifier à l'aide de l'authentification sans mot de passe basée sur FIDO2 au sein d'une session HDX. Les clés de sécurité FIDO2 permettent aux employés de l'entreprise de s'authentifier auprès d'applications ou de sites Web prenant en charge FIDO2 sans entrer de nom d'utilisateur ou de mot de passe. Cette fonctionnalité prend actuellement en charge les authentificateurs itinérants (USB uniquement) avec code PIN. Cette fonctionnalité est prise en charge sur macOS 12 et versions ultérieures. Pour plus d'informations, consultez [Authentification basée sur FIDO2 au sein d'une session HDX](#).

Remarque :

Cette version ne prend en charge qu'une seule clé d'accès sur un appareil compatible FIDO2. Si votre appareil compatible FIDO2 possède plusieurs clés d'accès, la première clé est utilisée pour authentifier la session HDX.

Contrôle de la version à mise à jour automatique Les administrateurs peuvent désormais gérer la version de mise à jour automatique de l'application Citrix Workspace pour les appareils de l'organisation.

Les administrateurs peuvent contrôler la version en définissant la plage dans les propriétés

`maximumAllowedVersion` et `minimumAllowedVersion` dans Global App Configuration Service.

Exemple de fichier JSON dans Global App Configuration Service :

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://serviceURL:443"
6   }
7 ,
8   "settings": {
9
10    "name": "Version Control for Citrix Workspace",
11    "description": "Provides admin ability to Version Control for
12      Citrix Workspace",
13    "useForAppConfig": true,
14    "appSettings": {
15
16      "macos": [
17
18        {
19
20          "category": "AutoUpdate",
21          "userOverride": false,
22          "assignedTo": [
23            "AllUsersNoAuthentication"
24          ],
25          "settings": [
26
27            {
28
29              "name": "Auto update plugins settings",
30              "value": [
31
32                {
33
34                  "pluginName": "Citrix Workspace",
35                  "pluginId": "D99C3E77-FBF5-4B97-8EDA-4E381A1E0826",
36                  "pluginSettings": {
37
38                    "deploymentMode": "Update",
39                    "upgradeToLatest": false,
40                    "minimumAllowedVersion": "23.07.0.63",
41                    "maximumAllowedVersion": "23.07.0.63",
42                    "delayGroup": "Medium",
43                    "detectRule": ""
44                  }
45                }
46              ]
47            }
48          ]
49        }
50      ]
51    }
52  }
53 }
```

```
48     }
49
50     ]
51     }
52
53     }
54
55 }
56
57
58 <!--NeedCopy-->
```

Lorsque la plage est définie, l'application Citrix Workspace sur l'appareil de l'utilisateur est automatiquement mise à jour vers la version la plus élevée disponible se trouvant dans la plage spécifiée.

Si vous souhaitez mettre à jour automatiquement l'application Citrix Workspace vers une version spécifique, entrez la même version dans les propriétés `maximumAllowedVersion` et `minimumAllowedVersion` de Global App Configuration Service. Pour plus d'informations, consultez [Contrôle de la version à mise à jour automatique](#).

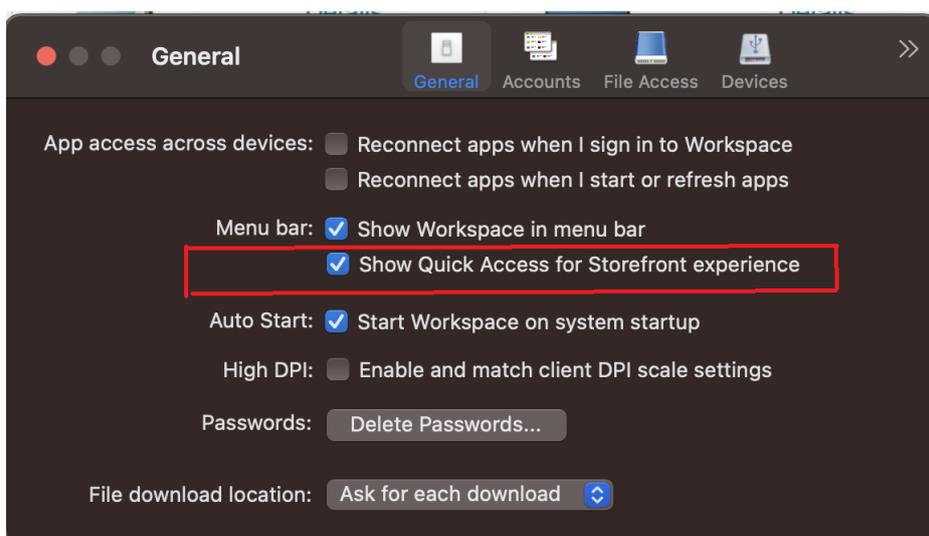
Remarque :

- Pour activer le contrôle de la version de mise à jour automatique, le paramètre `upgradeToLatest` de Global App Configuration Service doit être défini sur `false`. Si `upgradeToLatest` est défini sur `true`, les paramètres `maximumAllowedVersion` et `minimumAllowedVersion` seront ignorés.
- Ne modifiez pas la valeur de `pluginID`. L'élément `pluginId` est mappé à l'application Citrix Workspace.
- Si l'administrateur n'a pas configuré la version dans Global App Configuration Service, l'application Citrix Workspace est mise à jour vers la dernière version disponible par défaut.
- Vous ne pouvez utiliser que les plages de versions définies pour mettre à jour l'application Citrix Workspace. Toutefois, la rétrogradation n'est pas prise en charge.
- Cette fonctionnalité est prise en charge à partir de la version 2307.

Menu d'accès rapide pour StoreFront À partir de la version 2307, vous pouvez accéder rapidement et facilement à vos applications et bureaux préférés à l'aide de la fonction d'accès rapide pour les magasins locaux. Pour activer l'accès rapide, cliquez avec le bouton droit sur **Citrix Workspace** dans la barre d'outils, accédez à **Préférences > Général**, puis sélectionnez **Afficher l'accès rapide pour l'expérience Storefront**. Cette fonctionnalité vous permet de voir vos données préférées directement depuis la barre de menu Mac.



Vous pouvez activer la fonction d'accès rapide en utilisant **Préférences**.



Les administrateurs peuvent activer ou désactiver la fonctionnalité d'accès rapide en utilisant les méthodes Gestion d'appareils mobiles (MDM) ou Global App Configuration Service (GACS). Pour plus d'informations, consultez [Menu d'accès rapide de StoreFront](#).

Activation ou désactivation de l'accès rapide via MDM Pour permettre un accès rapide via MDM, les administrateurs doivent utiliser les paramètres suivants :

```
<key>ShowQuickAccessForStoreFront</key>  
<false/>
```

Activation ou désactivation de l'accès rapide via GACS Pour permettre un accès rapide via GACS, les administrateurs doivent utiliser les paramètres suivants :

```
enableQuickAccessForStoreFront
```

Configuration par magasin des niveaux d'accès au microphone et à la webcam À partir de la version 2307, l'accès au microphone et à la webcam par magasin est inclus dans le cadre de la fonction

Client Selective Trust. Cette amélioration vous permet de fournir l'accès à un microphone et à une webcam par magasin.

Pour activer l'accès au microphone et à la webcam pour un magasin, sélectionnez **Préférences > Micro et webcam**. Dans l'onglet **Micro et webcam**, sélectionnez le magasin et le type d'accès requis pour ce magasin. Pour plus d'informations, consultez la section [Configuration par magasin des niveaux d'accès au microphone et à la webcam](#).

Envoi de commentaires sur l'application Citrix Workspace L'option Envoyer des commentaires vous permet d'informer Citrix de tout problème que vous pourriez rencontrer lors de l'utilisation de l'application Citrix Workspace. Vous pouvez également envoyer des suggestions pour nous aider à améliorer votre expérience avec l'application Citrix Workspace.

Vous devez sélectionner **Aide > Envoyer des commentaires** pour afficher et renseigner les détails du problème dans le formulaire de commentaires. Vous pouvez ajouter des détails tels que les exemples fournis dans le formulaire.

Send feedback

Provide a descriptive title*

Tell us more*

Include details such as:

- What you expected to happen
- What actually happened
- Steps to recreate the issue

Logs

Basic logs are attached. We recommend you click 'Record my issue' to capture detailed logs.

For more information, see [Log collection](#)

Record my issue WorkspaceLogs_2023_07_18-14_23_43.zip

Attachments

Screenshots or screen recordings of the problem.

Choose files (Max 4 files)

Your feedback will be used to improve Citrix Workspace app. If you don't use the Mail app on your Mac, please send feedback to **cwa-mac-feedback@cloud.com** with files added manually.

Send **Cancel**

Vous pouvez joindre les fichiers journaux existants ou générer de nouveaux fichiers journaux. Pour générer des fichiers journaux, cliquez sur **Enregistrer mon problème > Démarrer l'enregistrement**, puis reproduisez le problème. Une fois le problème reproduit, cliquez sur **Arrêter l'enregistrement**. Le fichier journal est enregistré automatiquement et remplace les journaux existants par les journaux reproduits.

Remarque :

Citrix ne recueille aucune information permettant de vous identifier personnellement à partir des journaux.

Vous pouvez joindre des captures d'écran ou des enregistrements d'écran décrivant le problème pour nous aider à comprendre le problème que vous rencontrez. Cliquez sur **Choisissez des fichiers** et

ajoutez les pièces jointes, telles que des captures d'écran ou des enregistrements d'écran. Vous pouvez joindre un maximum de quatre fichiers.

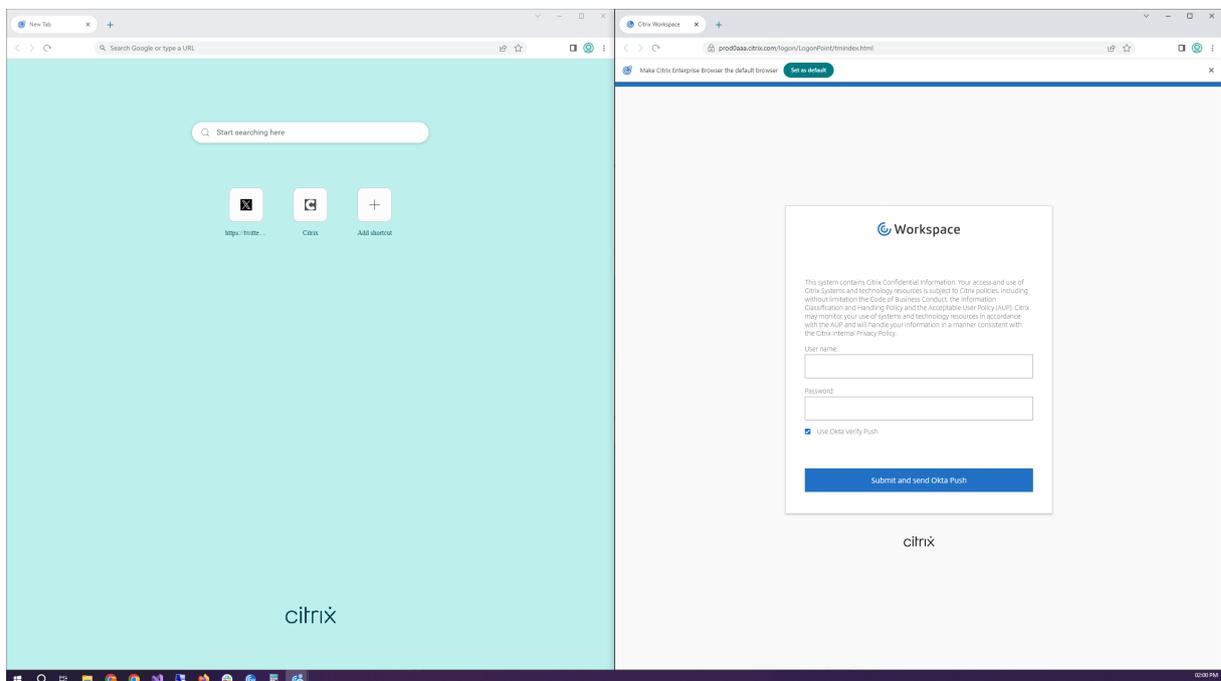
Une fois que vous avez saisi les informations nécessaires, cliquez sur **Envoyer** pour qu'un nouvel e-mail soit automatiquement créé dans votre application de messagerie avec les informations que vous avez ajoutées. À partir de là, cliquez sur le bouton **Envoyer** pour partager les commentaires à Citrix. Pour plus d'informations, consultez [Envoyer des commentaires sur l'application Citrix Workspace](#).

Remarque

Si vous n'utilisez pas l'application de messagerie par défaut, envoyez vos commentaires à cwa-mac-feedback@cloud.com depuis votre client de messagerie. Ajoutez manuellement les détails du problème, les fichiers journaux, les captures d'écran ou les enregistrements d'écran à l'e-mail.

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 113.1.1.34, basé sur Chromium version 113. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

Prise en charge de Split View Citrix Enterprise Browser sur macOS prend en charge la vue scindée, Split View, pour faciliter le multitâche. Avec la fonction Split View, vous pouvez utiliser Citrix Enterprise Browser et une autre fenêtre adjacente, sans avoir à déplacer et redimensionner manuellement les fenêtres. Pour plus d'informations, consultez l'article du [support Apple](#).



Raccourci Citrix Enterprise Browser À partir de la version 2307 de l'application Citrix Workspace pour Mac, un administrateur peut configurer et contrôler la présence du raccourci Citrix Enterprise Browser sur la rampe de lancement.

Remarque :

Par défaut, cette fonctionnalité n'est pas configurée.

Configuration

Un administrateur informatique peut configurer la présence du raccourci Citrix Enterprise Browser de l'une des manières suivantes :

- Gestion des appareils mobiles (MDM)
- Global App Configuration Service (GACS)
- Fichier web.config

Remarque :

- Toutes les méthodes de configuration ont la même priorité. L'activation de l'une d'entre elles active le raccourci.
- Si vous n'avez pas configuré le raccourci mais que vous avez un ou plusieurs magasins Workspace, le raccourci est automatiquement activé.
- Pour les utilisateurs finaux, le raccourci Citrix Enterprise Browser apparaît si l'utilisateur en fait une application favorite, quelle que soit la configuration.
- Pour désactiver cette fonctionnalité pour les magasins Workspace, les administrateurs doivent appliquer l'un des paramètres suivants :
 - Définissez l'attribut **CEBShortcutEnabled** sur **false** dans le fichier MDM ou web.config.
 - Désactivez la propriété Activer le raccourci Citrix Enterprise Browser dans GACS.

Gestion des appareils mobiles (MDM)

Les administrateurs peuvent transférer les paramètres **CEBShortcutEnabled** définis sur **true** sur l'appareil de l'utilisateur.

Pour plus d'informations sur l'utilisation de MDM, consultez la page [Gestion des appareils mobiles \(MDM\)](#).

Remarque :

Ce mode de configuration s'applique à Workspace et à StoreFront.

Global App Configuration Service (GACS)

Accédez à **Configuration de l'espace de travail > Configuration d'applications > Citrix Enterprise Browser** et activez la propriété **Activer le raccourci Citrix Enterprise Browser**.

The screenshot shows the configuration page for Citrix Enterprise Browser. It has four sections: 'List Of Allowed Extensions', 'Add Managed Bookmarks', 'Delete Browsing Data On Exit', and 'Enable Citrix Enterprise Browser Shortcut'. The 'Enable Citrix Enterprise Browser Shortcut' section is expanded, showing two rows: 'Mac' with a checked checkbox, 'Enabled' status, and a toggle switch turned on; and 'Windows' with a checked checkbox, 'Disabled' status, and a toggle switch turned off. At the bottom, there is a warning icon and text: 'You have saved drafts that are not yet published in Production. You may continue editing or publish now to apply changes to Workspace for your end users'. To the right, there are buttons for 'Review 2 unsaved setting(s)', 'Discard', and 'Publish Drafts'.

Pour plus d'informations sur l'utilisation de l'interface utilisateur GACS, consultez [Interface utilisateur](#) dans la documentation de Citrix Enterprise Browser.

Remarque :

Ce mode de configuration s'applique à Workspace et à StoreFront.

Fichier web.config

Activez l'attribut **CEBShortcutEnabled** sous les propriétés.

```
1 <properties>
2   <property name="CEBShortcutEnabled" value="
3     True" />
4 </properties>
5 <!--NeedCopy-->
```

Remarque :

Ce mode de configuration s'applique à StoreFront.

Utilisation du fichier web.config

Pour activer le raccourci Citrix Enterprise Browser, procédez comme suit :

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">`

3. Avant la balise `</account>` accédez aux propriétés de ce compte utilisateur et ajoutez ce qui suit :

```
1         <properties>
2             <property name="CEBShortcutEnabled" value=
3                 "True" />
4         </properties>
5 <!--NeedCopy-->
```

Voici un exemple du fichier web.config :

```
1 <account>
2     <clear />
3     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="F84Store"
4         description="" published="true" updatertype="Citrix"
5         remoteAccessType="None">
6         <annotatedServices>
7             <clear />
8             <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
9                 <metadata>
10                    <plugins>
11                        <clear />
12                    </plugins>
13                    <trustSettings>
14                        <clear />
15                    </trustSettings>
16                    <properties>
17                        <property name="CEBShortcutEnabled" value="True" />
18                    </properties>
19                </metadata>
20            </annotatedServiceRecord>
21        </annotatedServices>
22        <metadata>
23            <plugins>
24                <clear />
25            </plugins>
26            <trustSettings>
27                <clear />
28            </trustSettings>
29            <properties>
30                <clear />
31            </properties>
32        </metadata>
33    </account>
34 <!--NeedCopy-->
```

Comment configurer à l'aide de web.config

1. Utilisez un éditeur de texte pour ouvrir le fichier web.config, qui se trouve en général dans le répertoire C:\inetpub\wwwroot\Citrix\Roaming.
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">`

3. Avant la balise `</account>` accédez aux propriétés de ce compte utilisateur et ajoutez ce qui suit :

```
1         <properties>
2             <property name="CEBShortcutEnabled" value=
3                 "True" />
4         </properties>
5 <!--NeedCopy-->
```

Technical Preview

- Prise en charge de l'accessibilité du clavier pour la barre d'outils du bureau virtuel

Pour obtenir la liste complète des fonctionnalités préliminaires (version Technical Preview), consultez la page [Fonctionnalités de la version Technical Preview](#).

Problèmes résolus

- Lorsque vous lancez l'application publiée via le navigateur, l'application ne démarre pas directement mais télécharge un fichier ICA. L'utilisateur devra peut-être ouvrir le fichier ICA téléchargé manuellement pour lancer l'application. [CVADHELP-20835]
- Les tentatives de démarrage d'une session peuvent échouer si le mot clé StoreFront est défini sur `KEYWORDS:LogoffOnClose=true PromptMessage="Do you want to Log off?"`. [CVADHELP-23170]
- Il se peut que vous ne puissiez pas sélectionner la passerelle requise dans la liste des options proposées lors de l'utilisation de l'application Citrix Workspace pour Mac. [CVADHELP-22777]

Problèmes connus

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

2306

Nouveautés

Traçabilité des journaux et activités des utilisateurs À partir de la version 2306, lorsqu'un utilisateur signale un problème, les administrateurs peuvent utiliser les fichiers journaux pour consulter les informations de base telles que la version de macOS, la version de l'application Citrix Workspace, les détails de la mise à niveau précédente, le nombre de magasins ajoutés, etc. Les administrateurs peuvent désormais consulter les activités suivantes dans l'application Citrix Workspace pour Mac :

- Application ayant été lancée avec la version de macOS, le nombre de magasins et autres métadonnées
- Opération d'ajout et de suppression du magasin et métadonnées requises pour ajouter un compte
- Heure de début de session et état de lancement
- Activation et état de la mise à jour automatique
- Événements système tels que le déplacement de l'application en arrière-plan, le mode veille ou la fermeture de l'application

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 112.1.1.23, basé sur Chromium version 112. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

Problèmes résolus

- Après la mise à niveau de l'application Citrix Workspace pour Mac vers la version 2305, certaines applications virtuelles tierces dotées de boîtes de dialogue contextuelles permettant de saisir un nom d'utilisateur et un mot de passe peuvent ne plus répondre à l'ouverture. [CVADHELP-23032]

Problèmes connus

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

2305

Nouveautés

Défilement horizontal Auparavant, l'application Citrix Workspace pour Mac ne prenait en charge que le défilement vertical sur un trackpad. À partir de la version 2305, le défilement horizontal est

également pris en charge. Pour plus d'informations, consultez [Défilement horizontal](#).

Prise en charge améliorée de l'annulation de l'écho audio 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. Pour plus d'informations, consultez la section [Prise en charge améliorée de l'annulation de l'écho audio](#).

Amélioration des performances graphiques [version Technical Preview] À partir de la version 2305, les performances graphiques sont améliorées pour des sessions d'application transparentes. Cette fonctionnalité réduit également la charge d'utilisation du processeur.

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 version Technical 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.

Authentification basée sur des certificats À partir de la version 2305, les administrateurs Workspace peuvent configurer et appliquer les stratégies d'accès conditionnel Azure Active Directory pour les utilisateurs qui s'authentifient sur l'application Citrix Workspace.

Les méthodes suivantes peuvent être utilisées pour activer l'authentification à l'aide d'un accès conditionnel :

- Gestion des appareils mobiles (MDM)
- Global App Configuration Service (GACS)

Les valeurs des indicateurs lues par l'application Citrix Workspace sont prioritaires dans l'ordre suivant :

- Gestion des appareils mobiles (MDM)
- Global App Configuration Service (GACS)

Pour plus d'informations, consultez [Authentification basée sur des certificats](#).

Prise en charge des canaux de Global App Configuration Service Global App Configuration Service pour Citrix Workspace permet à un administrateur Citrix de fournir les URL du service Workspace et les paramètres de l'application Workspace via un service géré de manière centralisée. Global App

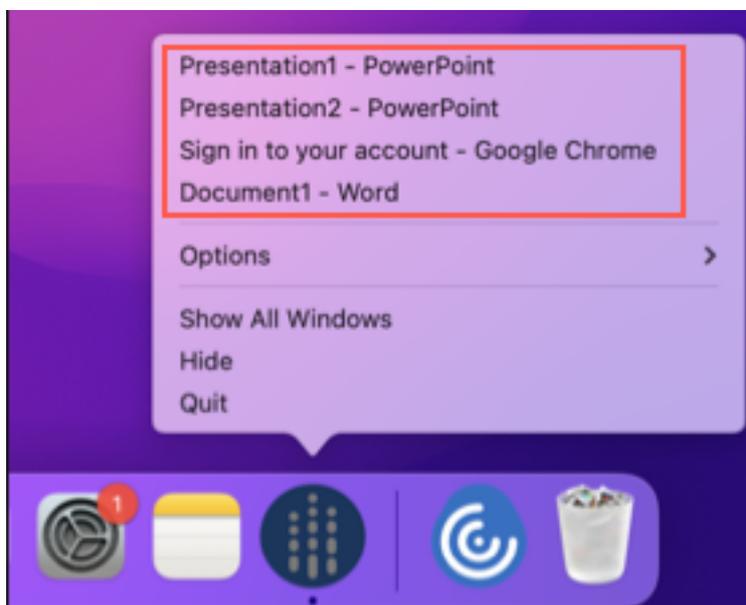
Configuration Service permet désormais aux administrateurs de tester les paramètres avant de les déployer pour tous les utilisateurs. Cette fonctionnalité permet de résoudre tous les problèmes avant d'appliquer les configurations d'application globales à l'ensemble de la base d'utilisateurs. Pour plus d'informations, consultez la section [Prise en charge des canaux de Global App Configuration Service](#).

Amélioration apportées à la mise à jour automatique La fonctionnalité de mise à jour automatique permet de mettre automatiquement à jour l'application Citrix Workspace vers la dernière version sans aucune intervention de l'utilisateur.

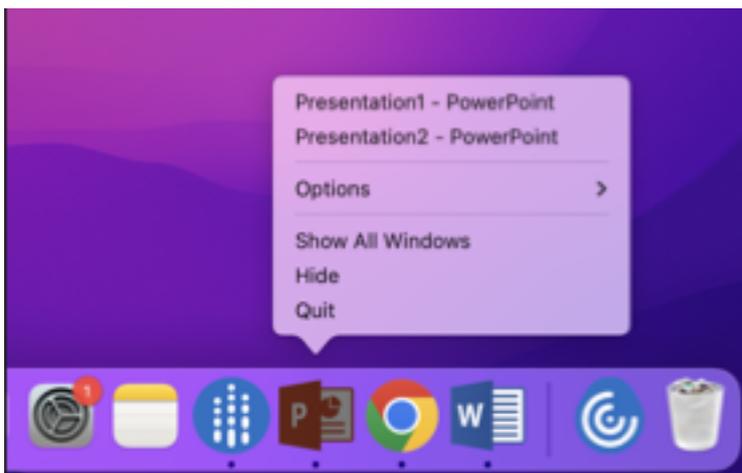
L'application Citrix Workspace vérifie et télécharge régulièrement la dernière version disponible de l'application. L'application Citrix Workspace détermine le meilleur moment pour l'installation en fonction de l'activité des utilisateurs afin de ne pas provoquer d'interruptions.

Pour plus d'informations, consultez [Améliorations apportées à la mise à jour automatique](#).

Les applications ouvertes apparaissent dans le Dock avec des icônes d'applications natives Au paravant, le fait de cliquer sur des applications virtuelles dans l'application Citrix Workspace déclenchait **Citrix Viewer** où ces applications étaient disponibles. Si vous ouvrez de nombreuses applications, les applications ou leurs instances se sont ouvertes dans **Citrix Viewer**. Vous pouvez afficher les applications ouvertes en cliquant avec le bouton droit sur l'icône **Citrix Viewer**.

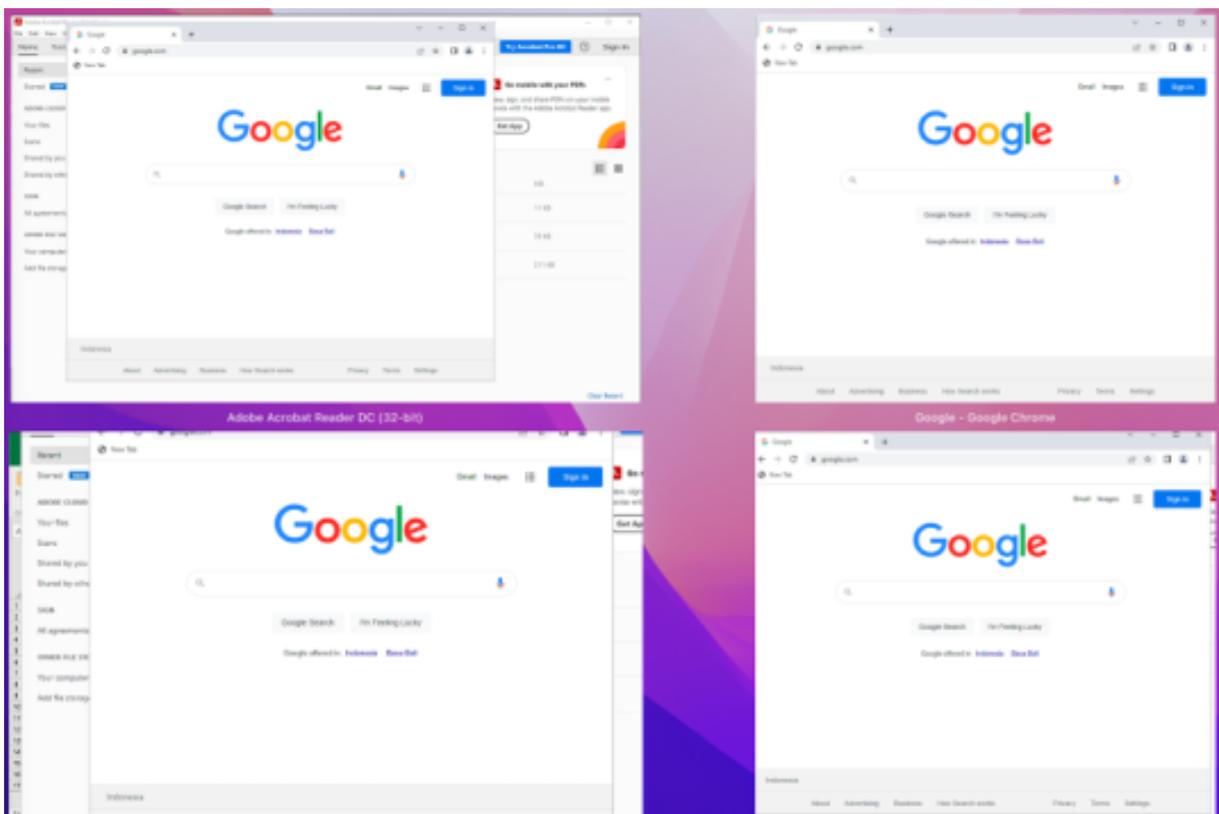


À partir de la version 2305, lorsque vous ouvrez des applications virtuelles, elles apparaissent dans le Dock (coin inférieur droit de l'écran) avec leurs icônes respectives et sont facilement identifiables. Vous pouvez ensuite accéder à l'application virtuelle depuis le dock lui-même. Si vous ouvrez plusieurs instances d'une application, ces instances ne sont pas des doublons dans le Dock mais sont regroupées au sein d'une instance du Dock.



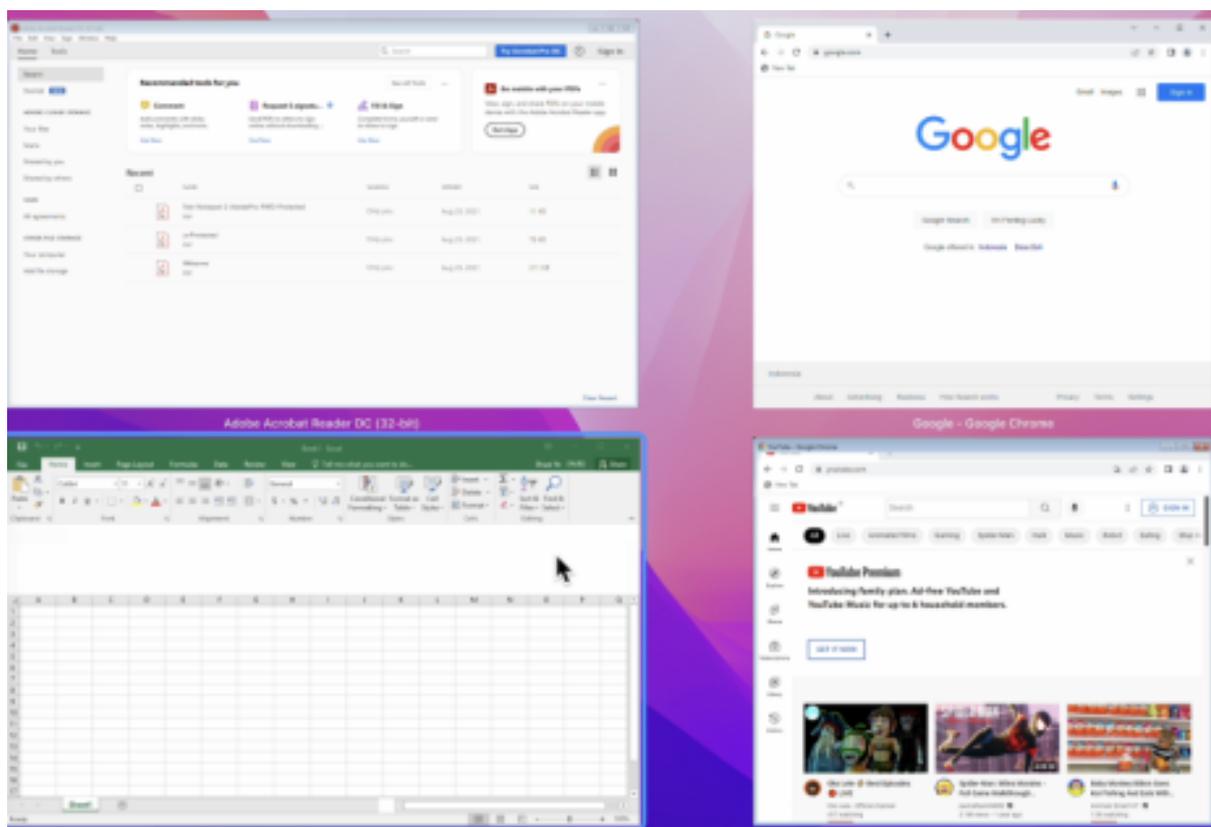
Pour plus d'informations, consultez la section [Les applications ouvertes apparaissent dans le Dock avec des icônes d'applications natives](#).

Amélioration de l'expérience Mission Control et App Expose Auparavant, l'utilisation de la fonctionnalité **Mission Control** ou **App Expose** dans une session d'application virtuelle entraînait le chevauchement de nombreuses fenêtres ouvertes.



À partir de la version 2305, lorsque vous utilisez la fonctionnalité **Mission Control** ou **App Expose** dans une session d'application virtuelle et que vous ouvrez de nombreuses fenêtres, les fenêtres ne

se chevauchent pas et vous pouvez facilement choisir l'une d'entre elles.



Pour plus d'informations, consultez [Amélioration de l'expérience Mission Control et App Expose](#).

Amélioration du mode veille pour optimiser les appels Microsoft Teams Auparavant, lorsque vous participiez à une réunion Microsoft Teams optimisée, en l'absence d'interaction avec la souris ou le clavier, l'application Citrix Workspace ou l'écran de Microsoft Teams optimisé pouvait passer en mode veille.

À partir de la version 2305, l'application Citrix Workspace ou l'écran de Microsoft Teams optimisé ne passe pas en mode veille même s'il n'y a aucune interaction avec la souris ou le clavier lors d'une réunion Microsoft Teams optimisée.

Pour plus d'informations, voir [Amélioration du mode veille pour les appels Microsoft Teams optimisés](#).

Prise en charge de l'appareil photo Continuité Avec l'appareil photo Continuité, vous pouvez désormais utiliser votre iPhone comme webcam. Pour une connexion fluide, installez votre iPhone de telle sorte que son appareil photo soit accessible à l'appareil Mac. Vous devez sélectionner **Webcam > Sélection automatique de la caméra** pour que l'iPhone apparaisse automatiquement sur l'appareil Mac en tant que caméra externe. Vous pouvez passer manuellement à n'importe quelle autre

caméra, par exemple en sélectionnant **Webcam > Caméra FaceTime HD**. L'appareil photo Continuité fonctionne avec ou sans fil et fournit une image de haute qualité. Pour plus d'informations, consultez [Prise en charge de l'appareil photo Continuité](#).

Augmentation du nombre de canaux virtuels pris en charge [version Technical Preview] Dans les versions antérieures du client, les sessions prenaient en charge jusqu'à 32 canaux virtuels. À partir de la version 2305, vous pouvez utiliser jusqu'à 64 canaux virtuels dans une session.

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 version Technical 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.

Configuration par magasin des niveaux d'accès au microphone et à la webcam [version Technical Preview] À partir de la version 2305, l'accès au microphone et à la webcam par magasin est inclus dans le cadre de la fonction Client Selective Trust. Cette amélioration vous permet de modifier les paramètres en fonction de chaque magasin. Vous pouvez cliquer sur un magasin pour activer l'accès requis au microphone ou à la caméra. Le paramètre sélectionné pour l'accès au microphone ou à la caméra est appliqué par magasin.

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 version Technical 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.

Prise en charge de l'authentification à l'aide de FIDO2 lors de la connexion à des magasins cloud [version Technical Preview] À partir de la version 2305, les utilisateurs peuvent s'authentifier à l'aide de clés de sécurité FIDO2 sans mot de passe lorsqu'ils se connectent à l'application Citrix Workspace pour Mac. Les utilisateurs peuvent se connecter aux magasins cloud à l'aide des clés de sécurité FIDO2. Les clés de sécurité prennent en charge différentes méthodes d'accès, tels que les codes PIN de sécurité, les données biométriques, la lecture de cartes, les cartes à puce et les certificats de clé publique. Cette fonctionnalité est prise en charge sur macOS 12 et versions ultérieures. Pour plus d'informations sur FIDO2, consultez [Authentification FIDO2](#).

L'application Citrix Workspace utilise le navigateur par défaut de l'utilisateur pour l'authentification FIDO2 (Webauthn). Les administrateurs peuvent configurer le type de navigateur pour l'authentification auprès de l'application Citrix Workspace. Le paramètre configuré peut être transmis à l'aide de la gestion des appareils mobiles (MDM), du Global App Configuration Service (GACS) ou des méthodes d'interface de ligne de commande. La fonctionnalité FIDO2 n'est pas prise en charge pour les magasins locaux. Pour plus d'informations sur les paramètres du navigateur Web, consultez la documentation [Global App Configuration Service](#).

Les paramètres suivants vous permettent de sélectionner le type de navigateur utilisé pour authentifier un utilisateur final dans l'application Citrix Workspace :

Embedded : permet l'authentification dans l'application Citrix Workspace. L'application Citrix Workspace enregistre les données de session ou les cookies pour l'authentification unique (par exemple, les applications SaaS) lorsque la fonctionnalité d'[authentification unique améliorée](#) est activée. Cette méthode d'authentification ne prend pas en charge les authentifications sans mot de passe telles que FIDO2.

EmbeddedWithPrivateSession : ce paramètre est similaire au paramètre **Embedded**. L'authentification unique n'est pas prise en charge car les données de session ou les cookies ne sont pas présents dans l'application Citrix Workspace.

System : vous permet d'utiliser le navigateur par défaut de l'utilisateur pour l'authentification (par exemple, Safari ou Chrome). L'authentification s'effectue en dehors de l'application Citrix Workspace. Utilisez ce paramètre pour prendre en charge l'authentification sans mot de passe. Ce paramètre essaie d'utiliser la session utilisateur existante depuis le navigateur de l'utilisateur.

SystemWithPrivateSession : ce paramètre est similaire au paramètre **System**. L'application Citrix Workspace utilise une session privée dans le navigateur pour l'authentification. Le navigateur n'enregistre pas les cookies ni les données d'authentification. L'authentification unique n'est pas prise en charge dans cette option.

Activer l'authentification à l'aide de MDM Pour activer l'authentification via MDM, les administrateurs doivent utiliser les paramètres suivants :

```
<key>WebBrowserForAuthentication</key>  
<string>System</string>
```

Activer l'authentification à l'aide de GACS Pour activer l'authentification via GACS, les administrateurs doivent utiliser les paramètres suivants :

```
1 {  
2  
3     "serviceURL": {  
4
```

```
5     "url": "https://serviceURL:443"
6   }
7   ,
8   "settings": {
9
10    "name": "Productivity Apps",
11    "description": "Provides access to MS Office and other basic apps",
12    "useForAppConfig": true,
13    "appSettings": {
14
15      "macos": [
16        {
17
18          "assignedTo": [
19            "AllUsersNoAuthentication"
20          ],
21          "category": "authentication",
22          "settings": [
23            {
24
25              "name": "web browser for authentication",
26              "value": "SystemWithPrivateSession"
27            }
28          ],
29          "userOverride": false
30        }
31      ]
32    }
33  ]
34 }
35
36 }
37
38 }
39
40
41 <!--NeedCopy-->
```

Activer l'authentification à l'aide de l'interface de ligne de commande Pour activer l'authentification à l'aide de l'interface de ligne de commande, les administrateurs doivent exécuter la commande suivante :

```
defaults write com.citrix.receiver.nomas WebBrowserForAuthentication System
```

Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le [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 version Technical 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 au mode de saisie du clavier L'application Citrix Workspace pour Mac fournit une interface utilisateur permettant de configurer le mode de saisie du clavier.

Pour configurer le mode de saisie du clavier à l'aide de l'interface graphique, procédez comme suit :

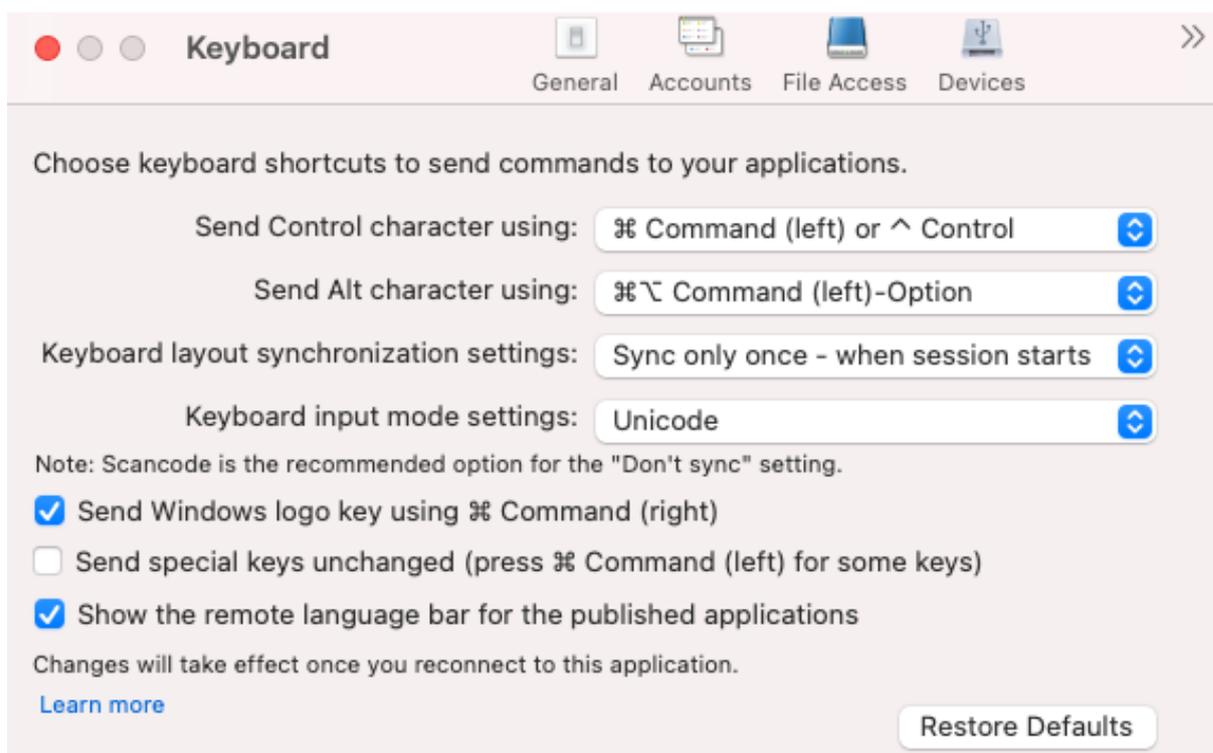
1. Depuis l'icône de l'application Citrix Workspace dans la barre de menu, cliquez sur l'icône du compte dans le coin supérieur droit et accédez à **Préférences > Clavier**.

Les paramètres du mode de saisie du clavier apparaissent.

2. Sélectionnez l'une des options suivantes :

- **Scancode** : la position des touches du clavier côté client est envoyée au VDA et le VDA génère le caractère correspondant. Applique la disposition du clavier côté serveur.
- **Unicode** : la touche du clavier côté client est envoyée au VDA et le VDA génère le même caractère dans le VDA. Applique la disposition du clavier côté client.

Cette amélioration est activée par défaut.



Par exemple, imaginez un scénario dans lequel vous utilisez une disposition de clavier international américain alors que le VDA utilise une disposition de clavier russe. Lorsque vous choisissez **Scancode** et que vous appuyez sur la touche à côté de **Verr Maj**, le code “1E” est envoyé au VDA. Le VDA utilise ensuite “1E” pour afficher le caractère “ф”. Si vous choisissez **Unicode** et que vous appuyez sur la touche à côté de **Verr Maj**, le caractère “a” est envoyé au VDA. Ainsi, même si le VDA utilise la disposition du clavier russe, le caractère “a” apparaît à l’écran.

Citrix recommande le mode de saisie au clavier suivant pour les différentes options de synchronisation de la disposition du clavier :

- Mode Scancode pour l’option **Ne pas synchroniser**.
- Mode Unicode pour **Autoriser la synchronisation dynamique** et **Synchroniser une seule fois - lorsque la session est lancée**.

Remarque :

Les modifications de configuration du clavier prennent effet une fois que vous vous reconnectez à l’application.

Vous pouvez modifier la configuration du mode de saisie du clavier dans l’interface utilisateur de l’application Citrix Workspace. Toutefois, pour bénéficier de performances optimales, utilisez les modes recommandés par Citrix pour différents scénarios, les claviers physiques et les appareils clients.

Pour plus d’informations sur les détails et les limites de configuration, consultez la section [Améliorations apportées au mode de saisie du clavier](#).

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 112.1.1.23, basé sur Chromium version 112. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

Modification de la mise en œuvre de la stratégie Authentification par mot de passe sécurisé (SPA) sur les applications Web et SaaS internes Cette fonctionnalité améliore la mise en œuvre des stratégies de sécurité sur les applications Web et SaaS. Lorsqu'une page Web et les iFrames de cette page Web disposent de stratégies différentes, une mise en œuvre plus stricte de la stratégie facilite désormais l'application cohérente de toutes les stratégies sur l'ensemble de la page Web, y compris les iFrames. Toutefois, le filigrane s'applique uniquement à la page Web.

Prise en charge des extensions de navigateur Vous pouvez ajouter des extensions fournies par votre administrateur à Citrix Enterprise Browser de manière sécurisée. Un administrateur peut déployer, gérer et contrôler les extensions. Les utilisateurs finaux peuvent afficher et utiliser l'extension sous `citrixbrowser://extensions` selon leurs besoins. Pour plus de paramètres, voir [Global App Configuration Service](#).

Pour plus d'informations sur la configuration, consultez [Prise en charge des extensions de navigateur](#).

Utiliser GACS pour gérer Citrix Enterprise Browser L'administrateur peut utiliser Global App Configuration Service pour Citrix Workspace (GACS) afin de fournir les paramètres de Citrix Enterprise Browser via un service géré de manière centralisée.

Le service GACS simplifie la configuration de Citrix Workspace et la gestion des paramètres de l'application Citrix Workspace pour les administrateurs. Cette fonctionnalité permet aux administrateurs d'utiliser le service GACS pour appliquer divers paramètres ou stratégies système à Citrix Enterprise Browser sur un magasin particulier. L'administrateur peut désormais configurer et gérer les paramètres Citrix Enterprise Browser suivants à l'aide d'API ou de l'interface administrateur GACS :

- « Enable CEB for all apps » : définit Citrix Enterprise Browser comme navigateur par défaut pour ouvrir les applications Web et SaaS à partir de l'application Citrix Workspace.
- « Enable save passwords » : autorise ou non les utilisateurs finaux à enregistrer les mots de passe.
- « Enable incognito mode » : active ou désactive le mode Navigation privée.
- « Managed Bookmarks » : autorise l'administrateur à envoyer des signets à Citrix Enterprise Browser.
- « Enable developer tools » : active ou désactive les outils de développement dans Enterprise Browser.

- « Delete browsing data on exit » : autorise l'administrateur à configurer les données que Citrix Enterprise Browser supprimera à la sortie.
- « Extension Install Force list » : autorise l'administrateur à installer des extensions dans Citrix Enterprise Browser.
- « Extension Install Allow list » : autorise l'administrateur à configurer une liste autorisée d'extensions que les utilisateurs peuvent ajouter à Citrix Enterprise Browser. Cette liste utilise le Chrome Web Store.

Pour plus d'informations, consultez la section [Utiliser Global App Configuration Service pour gérer Citrix Enterprise Browser](#).

Remarques :

- La paire nom et valeur distingue les majuscules des minuscules.
- Tous les paramètres du navigateur dans [Global App Configuration Service](#) se trouvent dans la catégorie suivante :

```
1 {
2
3     "category": "browser",
4     "userOverride": false,
5     "assignedTo": [
6         "AllUsersNoAuthentication"
7     ]
8 }
9
10
11 <!--NeedCopy-->
```

- L'administrateur peut également appliquer les paramètres à des appareils non gérés. Pour en savoir plus, consultez la documentation de [Global App Configuration Service](#).

Interface utilisateur

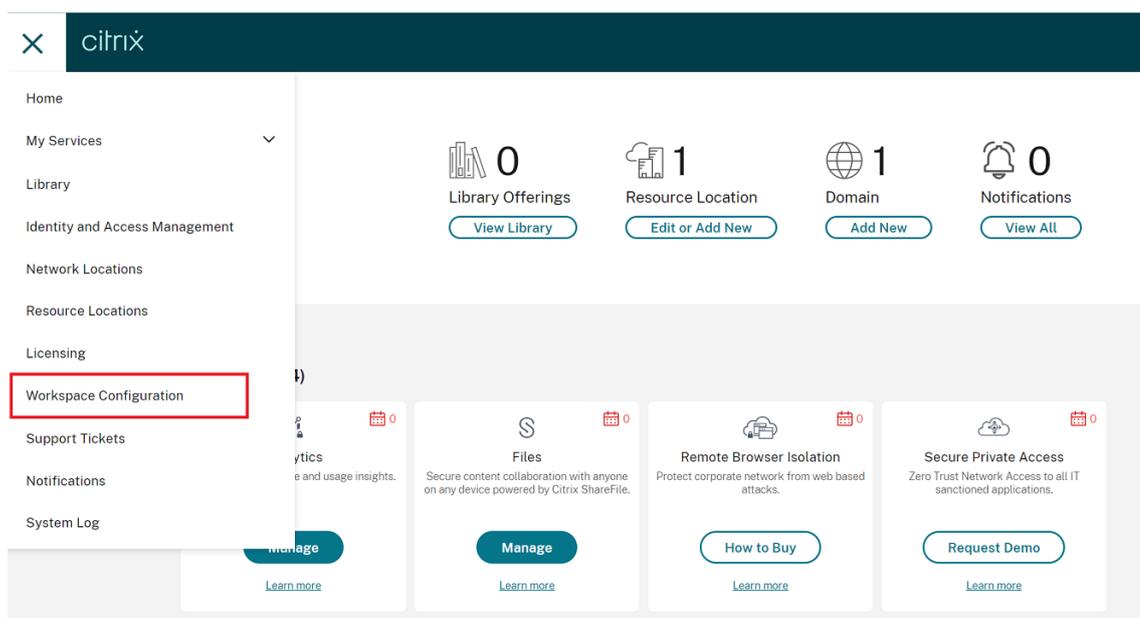
Pour configurer Citrix Enterprise Browser via l'interface utilisateur d'administration GACS, procédez comme suit :

1. Connectez-vous à citrix.cloud.com avec vos informations d'identification.

Remarque :

- Reportez-vous à l'article [Ouvrir un compte sur Citrix Cloud](#) pour obtenir des instructions détaillées sur la création d'un compte Citrix Cloud.

2. Lors de l'authentification, cliquez sur le bouton de menu situé dans le coin supérieur gauche et sélectionnez **Configuration de l'espace de travail**.



L'écran **Configuration de l'espace de travail** s'affiche.

3. Cliquez sur **Configuration d'applications > Citrix Enterprise Browser**.

Vous pouvez désormais configurer, modifier et publier les paramètres des fonctionnalités de Citrix Enterprise Browser.

Pour plus d'informations, consultez la section [Utiliser Global App Configuration Service pour gérer Citrix Enterprise Browser](#).

Technical Preview

- Gestion des applications clientes

Pour obtenir la liste complète des fonctionnalités préliminaires (version Technical Preview), consultez la page [Fonctionnalités de la version Technical Preview](#).

Problèmes résolus

- Grâce à cette amélioration, les données de localisation peuvent être collectées et envoyées à Microsoft Teams pour prendre en charge la fonctionnalité d'appel d'urgence dynamique. [CVADHELP-21117]
- Lorsque vous faites défiler l'écran d'un MacBook à l'aide d'un pavé tactile lors d'une session utilisateur ouverte via l'application Citrix Workspace pour Mac, l'expérience de défilement peut ne pas être fluide. [CVADHELP-21427]

- Lors de l'utilisation de l'application Citrix Workspace pour Mac, les utilisateurs externes peuvent être déconnectés des sessions par intermittence. [CVADHELP-22191]
- Les tentatives d'ajout d'une URL de magasin contenant un paramètre de requête peuvent échouer dans l'application Citrix Workspace pour Mac avec ce message d'erreur :

Ce magasin n'existe pas. Réessayez ou contactez l'assistance.

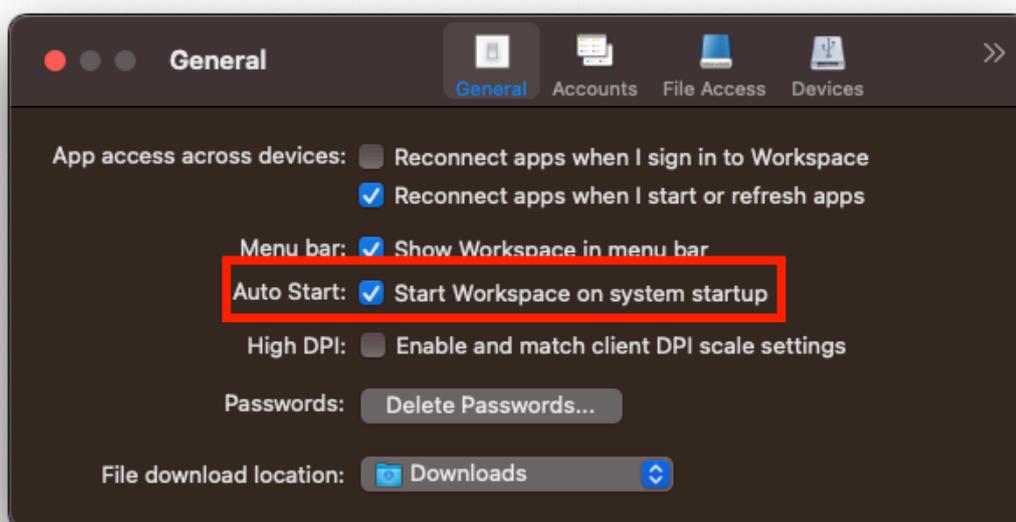
[CVADHELP-22445]

- Sur un magasin local, lorsque vous tentez d'ouvrir l'application Citrix Workspace à partir de la barre de **menus**, vous pouvez rencontrer un temps d'attente indéfini. [CVADHELP-22688]

2304

Nouveautés

Amélioration de l'expérience de démarrage automatique Auparavant, l'application Citrix Workspace pour Mac démarrait automatiquement chaque fois qu'un ordinateur était allumé. À partir de la version 2304, vous pouvez choisir de désactiver ou d'activer la fonctionnalité de démarrage automatique sur l'application Citrix Workspace pour Mac en accédant à **Préférences > Général > Démarrer Workspace** au démarrage du système. Le paramètre de démarrage automatique est activé par défaut.



Pour plus d'informations, consultez [Amélioration de l'expérience de démarrage automatique](#).

Expérience améliorée pour des visioconférences dans Microsoft Teams optimisé À compter de la version 2304, la prise en charge de la diffusion simultanée est activée par défaut pour des visioconférences dans Microsoft Teams optimisé. Avec cette version, la qualité et l'expérience des visioconférences sur différents terminaux sont améliorées. en s'adaptant à la résolution appropriée pour offrir la meilleure expérience d'appel à tous les appelants.

Grâce à cette expérience améliorée, chaque utilisateur peut diffuser plusieurs flux vidéo dans différentes résolutions (par exemple, 720p, 360p, etc.) en fonction de plusieurs facteurs, notamment la capacité du terminal, les conditions du réseau, etc. Le point de terminaison récepteur demande ensuite la résolution de qualité maximale qu'il peut gérer, offrant ainsi à tous les utilisateurs une expérience vidéo optimale.

Remarque :

Cette fonctionnalité est disponible uniquement après le déploiement d'une mise à jour de Microsoft Teams. Pour plus d'informations sur l'estimation de date de publication, accédez à <https://www.microsoft.com/> et recherchez la feuille de route de Microsoft 365. Une fois la mise à jour déployée par Microsoft, vous pourrez consulter l'article [CTX253754](#) pour obtenir la mise à jour de la documentation et l'annonce.

Pour plus d'informations, voir

[Expérience améliorée pour des visioconférences Microsoft Teams optimisées.](#)

Prise en charge de l'authentification basée sur des certificats [version Technical Preview] À partir de la version 2304, les administrateurs Workspace peuvent configurer et appliquer les stratégies d'accès conditionnel Azure Active Directory pour les utilisateurs qui s'authentifient sur l'application Citrix Workspace.

Les méthodes suivantes peuvent être utilisées pour activer l'authentification à l'aide d'un accès conditionnel :

- Gestion des appareils mobiles (MDM)
- Global App Configuration Service (GACS)

Les valeurs des indicateurs lues par l'application Citrix Workspace sont prioritaires dans l'ordre suivant :

- Gestion des appareils mobiles (MDM)
- Global App Configuration Service (GACS)

Pour plus d'informations, consultez [Authentification basée sur des certificats.](#)

Remarque :

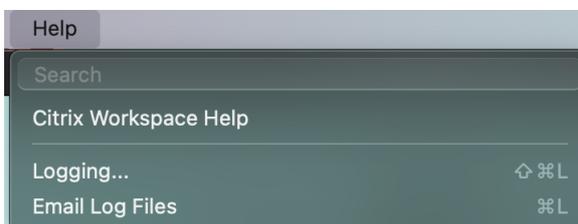
Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de [partager leurs commentaires](#). Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour 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.

Forcer l'invite de connexion pour le fournisseur d'identité fédéré L'application Citrix Workspace respecte désormais le paramètre Sessions de fournisseur d'identité fédéré. Pour plus d'informations, consultez l'article du centre de connaissances Citrix [CTX253779](#).

Vous n'avez plus besoin d'utiliser la stratégie Stocker les jetons d'authentification pour forcer l'invite de connexion. Pour plus d'informations, consultez [Forcer l'invite de connexion pour le fournisseur d'identité fédéré](#).

Dispositions de clavier des éditeurs de méthodes d'entrée (IME) dans une langue autre que l'anglais La prise en charge des dispositions de clavier IME dans une langue autre que l'anglais continue de fonctionner sans interruption après que les API Carbon sont devenues obsolètes au profit des API Cocoa. Pour plus d'informations, consultez [Dispositions de clavier des éditeurs de méthodes d'entrée \(IME\) dans une langue autre que l'anglais](#).

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. Les utilisateurs peuvent désormais collecter rapidement des journaux à l'aide de la nouvelle option fournie dans le menu **Aide** en accédant à l'**aide** et en sélectionnant l'option **Journalisation...** ou **Envoyer fichiers journaux**. Cette fonctionnalité améliore l'expérience utilisateur avec le processus de collecte des journaux.



- **Journalisation...** : cliquez sur cette option pour accéder à **Préférences > Avancé > Journalisation**
- **Envoyer fichiers journaux** : cliquez sur cette option pour collecter les derniers journaux.

Pour plus d'informations, consultez [Collecte de journaux](#).

Synchronisation pour un plus grand nombre de dispositions de clavier À compter de la version 2304, l'application Citrix Workspace pour Mac prend en charge la synchronisation de la disposition du clavier pour les modèles ou éditeurs de méthodes de saisie (IME) suivants :

- ABC anglais
- ABC anglais - Inde
- Chinois, Traditionnel : Zhuyin - Traditionnel
- Chinois, Traditionnel : Sucheng - Traditionnel
- Google Japanese IME
- Sougou Chinese IME

Pour plus d'informations, consultez la section [Synchronisation pour un plus grand nombre de dispositions de clavier](#).

Améliorations apportées à Microsoft Teams

Configurer une interface réseau préférée Vous pouvez désormais configurer une interface réseau préférée pour le trafic multimédia. Exécutez la commande suivante dans une fenêtre de terminal :

```
defaults write com.citrix.HdxRtcEngine NetworkPreference -int <value>
```

Sélectionnez l'une des valeurs suivantes selon les besoins :

- 1 : Ethernet
- 2 : Wi-Fi
- 3 : Cellulaire
- 4 : VPN
- 5 : Bouclage
- 6 : Quelconque

Par défaut, et si aucune valeur n'est définie, le moteur de média WebRTC choisit la meilleure route disponible.

Pour plus d'informations, consultez la section [Configurer une interface réseau préférée](#).

Limiter les résolutions vidéo Les administrateurs dont les utilisateurs utilisent des points de terminaison client moins performants peuvent limiter les résolutions vidéo entrantes ou sortantes afin de réduire l'impact du codage et du décodage vidéo sur ces points de terminaison. À partir de l'application Citrix Workspace 2304 pour Mac, vous pouvez limiter ces résolutions à l'aide des options de configuration du client.

Pour plus d'informations, consultez la section [Limitation des résolutions vidéo](#).

Défilement horizontal [version Technical Preview] Auparavant, l'application Citrix Workspace pour Mac ne prenait en charge que le défilement vertical sur un trackpad. À partir de la version 2304, le défilement horizontal est également pris en charge.

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 version Technical 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 au mode de saisie du clavier L'application Citrix Workspace pour Mac fournit une interface utilisateur permettant de configurer le mode de saisie du clavier.

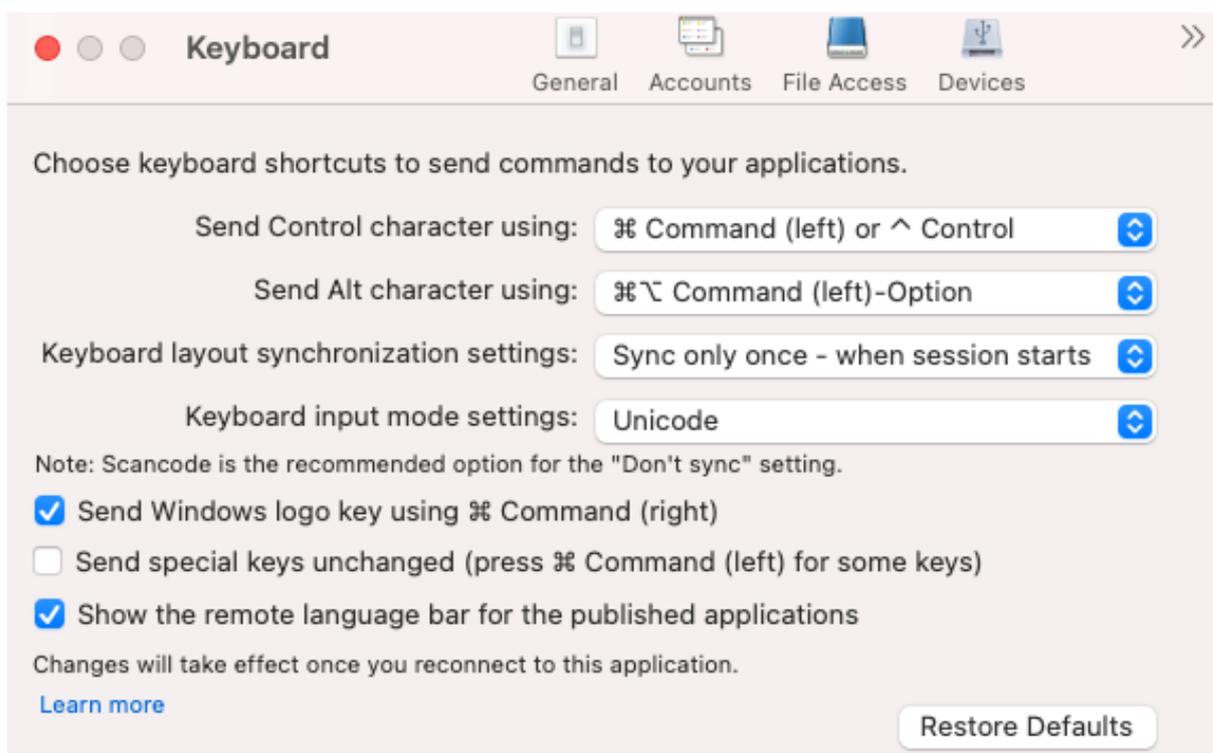
Pour configurer le mode de saisie du clavier à l'aide de l'interface graphique, procédez comme suit :

1. Depuis l'icône de l'application Citrix Workspace dans la barre de menu, cliquez sur l'icône du compte dans le coin supérieur droit et accédez à **Préférences > Clavier**.

Les paramètres du mode de saisie du clavier apparaissent.

2. Sélectionnez l'une des options suivantes :
 - **Scancode** : la position des touches du clavier côté client est envoyée au VDA et le VDA génère le caractère correspondant. Applique la disposition du clavier côté serveur.
 - **Unicode** : la touche du clavier côté client est envoyée au VDA et le VDA génère le même caractère dans le VDA. Applique la disposition du clavier côté client.

Cette amélioration est activée par défaut.



Par exemple, imaginez un scénario dans lequel vous utilisez une disposition de clavier international américain alors que le VDA utilise une disposition de clavier russe. Lorsque vous choisissez **Scancode** et que vous appuyez sur la touche à côté de **Verr Maj**, le code “1E” est envoyé au VDA. Le VDA utilise ensuite “1E” pour afficher le caractère “ф”. Si vous choisissez **Unicode** et que vous appuyez sur la touche à côté de **Verr Maj**, le caractère “a” est envoyé au VDA. Ainsi, même si le VDA utilise la disposition du clavier russe, le caractère “a” apparaît à l’écran.

Citrix recommande le mode de saisie au clavier suivant pour les différentes options de synchronisation de la disposition du clavier :

- Mode Scancode pour l’option **Ne pas synchroniser**.
- Mode Unicode pour **Autoriser la synchronisation dynamique** et **Synchroniser une seule fois - lorsque la session est lancée**.

Remarque :

Les modifications de configuration du clavier prennent effet une fois que vous vous reconnectez à l’application.

Vous pouvez modifier la configuration du mode de saisie du clavier dans l’interface utilisateur de l’application Citrix Workspace. Toutefois, pour bénéficier de performances optimales, utilisez les modes recommandés par Citrix pour différents scénarios, les claviers physiques et les appareils clients.

Pour plus d’informations sur les détails et les limites de configuration, consultez la section [Améliorations apportées au mode de saisie du clavier](#).

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 109.1.1.31, basé sur Chromium version 109. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

Technical Preview

- Numérisation rapide
- Amélioration de l'expérience de lancement de Virtual Apps and Desktops
- Prise en charge de plusieurs périphériques audio

Pour obtenir la liste complète des fonctionnalités préliminaires (version Technical Preview), consultez la page [Fonctionnalités de la version Technical Preview](#).

Problèmes résolus

- Lorsque vous créez deux fichiers XML sur un client local Mac, le VDA peut ouvrir le fichier XML incorrect. Par exemple, le VDA ouvre le fichier Snapshot.xml au lieu d'ouvrir le fichier Snapshot-Popup.xml. [HDX-45326]
- Lorsque vous modifiez les périphériques audio actifs dans les paramètres audio du terminal, il est possible que Microsoft Teams ne reçoive aucune notification concernant cette modification. Par conséquent, Microsoft Teams n'applique pas les modifications. [HDX-47080]
- Citrix Viewer peut se fermer de temps en temps lorsque vous fermez une session VDA. [HDX-45668, HDX-47138]
- La stratégie de répondeur configurée à l'aide de Citrix ADC peut ne pas fonctionner avec l'application Citrix Workspace pour Mac. Le problème se produit lorsque la stratégie configurée vérifie si le user-agent envoyé dispose de **CWAWEBVIEW**, **Citrix Receiver** ou **Citrix Workspace** comme sous-chaîne, ce qui ne correspond pas. Par conséquent, les utilisateurs peuvent être redirigés vers une autre URL Citrix Gateway. [CVADHELP-20519]
- Lorsque vous vous connectez à Citrix Gateway Store et que vous essayez de vous connecter à l'application Citrix Workspace pour Mac, la connexion peut rester bloquée ou prendre du temps. [CVADHELP-21323]
- L'application Citrix Workspace pour Mac peut ne pas démarrer une session si **Association de type de fichier** est défini pour une application dans **Paramètres de l'application** dans Citrix Studio. [CVADHELP-21371]
- Une fenêtre de connexion peut s'afficher automatiquement dans l'application Citrix Workspace pour Mac lorsque vous allumez ou redémarrez votre système. [CVADHELP-21484]

- L'application Citrix Workspace pour Mac peut se fermer de manière inattendue lorsque les applications de la plateforme Windows universelle (UWP) du VDI tentent de s'authentifier à l'aide de l'authentification FIDO2. [CVADHELP-21576]
- Les tentatives d'ouverture des ressources Web peuvent échouer avec le message d'erreur suivant :

Basculez vers un autre magasin disposant des autorisations nécessaires. Si le problème persiste, contactez votre administrateur pour lui communiquer les détails de l'erreur.

[CVADHELP-21787]

- L'application Citrix Workspace pour Mac peut utiliser un user-agent **CitrixReceiver** incorrect au lieu de **Citrix Workspace** comme sous-chaîne. Par conséquent, les stratégies d'autorisation ne sont pas respectées. [CVADHELP-21969]
- Lorsque vous utilisez la fonction d'écran à encoche, une partie du texte peut être coupée. [CVADHELP-22134]
- Lorsque vous ouvrez Citrix Enterprise Browser depuis le dock, au lieu d'ouvrir un nouvel onglet, vous voyez que la page est en cours de chargement. Pour contourner le problème, entrez l'URL dans la barre d'adresse ou ouvrez un autre onglet pour continuer à naviguer. [CTXBR-4706]
- Lorsque vous utilisez un magasin compatible avec Citrix Secure Private Access, un compteur de chargement infini peut apparaître lors du lancement du contenu publié. Le problème se produit lorsque Citrix Enterprise Browser ne s'exécute pas sur la machine utilisateur. Par conséquent, vous ne pouvez pas consulter le contenu publié. [CTXBR-4813]

2301.1

Nouveautés

La version 2301.1 résout quelques problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

- Vous pouvez rencontrer des problèmes lorsque vous ajoutez ou authentifiez un magasin, ou lorsque vous démarrez une ressource (applications ou bureaux) à l'aide de l'application Citrix Workspace native. [CVADHELP-22372]
- La vidéo entrante et le partage d'écran peuvent ne pas fonctionner pendant les appels vidéo Microsoft Teams optimisés. [HDX-50059]

Problèmes connus dans la version 2301.1

- Vous ne pouvez pas effectuer la mise à jour vers la version 2301.1 de l'application Citrix Workspace pour Mac à l'aide du service de mise à jour automatique. Pour éviter ce problème, vous devrez installer manuellement la version 2301.1 de l'application Citrix Workspace pour Mac en téléchargeant le fichier .dmg disponible sur la page [Téléchargements](#).

2301

Nouveautés

Flou et remplacement d'arrière-plan avec l'optimisation de Microsoft Teams pour Citrix L'optimisation de Microsoft Teams dans l'application Citrix Workspace pour Mac prend désormais le flou et le remplacement de l'arrière-plan. Vous pouvez utiliser cette fonctionnalité en sélectionnant **Plus > Appliquer des effets d'arrière-plan** lorsque vous participez à une réunion ou à un appel P2P.

Contrôle de la version de mise à jour automatique [version Technical Preview] Les administrateurs peuvent désormais gérer la version de mise à jour automatique de l'application Citrix Workspace pour les appareils de l'organisation.

Les administrateurs peuvent contrôler la version en définissant la plage dans les propriétés maximumAllowedVersion et minimumAllowedVersion dans Global App Configuration Service.

Exemple de fichier JSON dans Global App Configuration Service :

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://serviceURL:443"
6   }
7 ,
8   "settings": {
9
10    "name": "Version Control for Citrix Workspace",
11    "description": "Provides admin ability to Version Control for
12      Citrix Workspace",
13    "useForAppConfig": true,
14    "appSettings": {
15
16      "macos": [
17
18        "category": "AutoUpdate",
19        "userOverride": false,
20        "assignedTo": [
21          "AllUsersNoAuthentication"
```

```
22     ],
23     "settings": [
24         {
25
26             "name": "Auto update plugins settings",
27             "value": [
28                 {
29
30                     "pluginName": "Citrix Workspace",
31                     "pluginId": "D99C3E77-FBF5-4B97-8EDA-4E381A1E0826",
32                     "pluginSettings": {
33
34                         "deploymentMode": "Update",
35                         "upgradeToLatest": false,
36                         "minimumAllowedVersion": "23.04.0.36",
37                         "maximumAllowedVersion": "23.04.0.36",
38                         "delayGroup": "Medium",
39                         "detectRule": ""
40                     }
41                 }
42             ]
43         }
44     ]
45 }
46
47 ]
48 }
49
50 ]
51 }
52
53 }
54
55 }
56
57
58 <!--NeedCopy-->
```

Lorsque la plage est définie, l'application Citrix Workspace sur l'appareil de l'utilisateur est automatiquement mise à jour vers la version la plus élevée disponible se trouvant dans la plage spécifiée.

Si vous souhaitez mettre à jour automatiquement l'application Citrix Workspace vers une version spécifique, entrez la même version dans les propriétés `maximumAllowedVersion` et `minimumAllowedVersion` de Global App Configuration Service.

Remarque :

- Pour activer le contrôle de la version de mise à jour automatique, le paramètre `upgradeToLatest` de Global App Configuration Service doit être défini sur `false`. Si `upgradeToLatest` est défini sur `true`, les paramètres `maximumAllowedVersion` et

`minimumAllowedVersion` seront ignorés.

- Ne modifiez pas la valeur de `pluginID`. L'élément `pluginID` est mappé à l'application Citrix Workspace.
- Si l'administrateur n'a pas configuré la version dans Global App Configuration Service, l'application Citrix Workspace est mise à jour vers la dernière version disponible par défaut.
- Vous ne pouvez utiliser que les plages de versions définies pour mettre à jour l'application Citrix Workspace. Toutefois, la rétrogradation n'est pas prise en charge.
- Cette fonctionnalité est prise en charge à partir de la version 2301.

Vous pouvez nous faire part de vos commentaires sur cette version 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 version Technical 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.

Amélioration de la mise à jour automatique [version Technical Preview] La fonctionnalité de mise à jour automatique permet de mettre automatiquement à jour l'application Citrix Workspace vers la dernière version sans aucune intervention de l'utilisateur. L'application Citrix Workspace recherche régulièrement les dernières mises à jour et télécharge la dernière version disponible de l'application. Par défaut, les mises à jour automatiques sont activées, sauf si elles sont explicitement désactivées par votre administrateur.

L'installation démarre lorsque l'application Citrix Workspace ou les sessions sont inactives.

Remarque :

L'application Citrix Workspace n'est pas accessible pendant l'installation.

Lorsque vous démarrez l'application Citrix Workspace, une notification s'affiche pour indiquer l'état de l'installation.

Vous pouvez désactiver la fonctionnalité de mise à jour automatique en accédant à **Préférences > Avancé > Mises à jour** et en désélectionnant l'option **Maintenir l'application Workspace à jour automatiquement**.

Vous pouvez nous faire part de vos commentaires sur cette version 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 version Technical 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.

Prise en charge améliorée de l'écran à encoche À compter de la version 2301, l'application Citrix Workspace pour Mac est compatible avec les Mac dotés d'un écran à encoche. Les Mac prennent en charge un écran à encoche natif en mode plein écran pour l'affichage Retina et multi-écrans. La zone de la session sur l'écran à encoche est désormais beaucoup plus grande et offre aux clients plus d'espace sur l'écran. Cette amélioration prend également en charge une mise à l'échelle DPI haute résolution. La position de la souris apparaît également précise sur tous les moniteurs externes connectés. Pour plus d'informations, consultez la section [Prise en charge améliorée de l'écran à encoche](#).

Remarque :

Assurez-vous de ne pas sélectionner l'option **Scale to fit below built-in camera** dans Citrix Viewer. Cette option n'est pas sélectionnée par défaut et n'est disponible que sur les Mac dotés d'un écran à encoche.

Amélioration de App Protection À compter de la version 2301, App Protection est améliorée pour protéger l'application Citrix Workspace. Cette amélioration inclut la protection de l'écran d'authentification et de l'écran qui s'affiche après la connexion à l'application Workspace. Pour plus d'informations, consultez la section [App Protection](#).

Prise en charge du canal Global App Configuration Service [version Technical Preview] Global App Configuration Service pour Citrix Workspace permet à un administrateur Citrix de fournir les URL du service Workspace et les paramètres de l'application Workspace via un service géré de manière centralisée. Pour en savoir plus, consultez la documentation de [Global App Configuration Service](#).

Les administrateurs peuvent désormais utiliser le canal Global App Configuration Service pour définir des paramètres applicables à des groupes d'utilisateurs spécifiques. Cela garantit que certaines fonctions ou fonctionnalités ne peuvent être mises à la disposition que de certains utilisateurs, selon les besoins, et pas à d'autres.

Vous pouvez nous faire part de vos commentaires sur cette version Technical Preview en utilisant ce formulaire

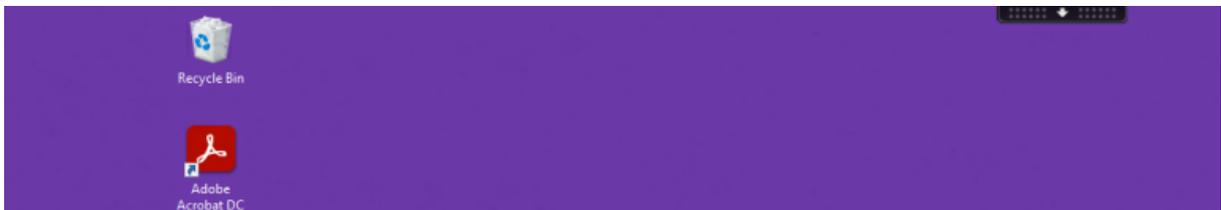
[Podio](#).

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 version Technical 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.

Prise en charge améliorée de la barre de menus À partir de la version 2301, le CWA prend entièrement en charge l'option **Masquer/afficher automatiquement la barre des menus en plein écran** dans macOS. Pour les versions antérieures à macOS 13, vous devez accéder à **Préférences système > Dock et barre de menus** et décocher l'option **Masquer/afficher automatiquement la barre des menus en plein écran**. Pour macOS 13 et les versions ultérieures, vous devez accéder à **Préférences système > Bureau et Dock** et décocher l'option **Masquer/afficher automatiquement la barre des menus en plein écran**. Vous avez la possibilité d'activer ou de désactiver cette option. Cette amélioration prend également en charge une mise à l'échelle DPI haute résolution. La position de la souris apparaît également précise sur tous les moniteurs externes connectés. Pour plus d'informations, consultez la section [Prise en charge améliorée de la barre de menu](#).

La figure ci-dessous illustre une fenêtre dans laquelle la barre de menus est masquée



La figure ci-dessous illustre une fenêtre dans laquelle la barre de menus apparaît.



Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 107.1.1.13, basé sur Chromium version 107. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

Définir Citrix Enterprise Browser comme navigateur de travail Vous pouvez désormais configurer Citrix Enterprise Browser en tant que navigateur de travail pour ouvrir tous les liens de travail. Vous pouvez sélectionner un autre navigateur pour ouvrir des liens non liés au travail.

Un lien de travail est un lien associé aux applications Web ou SaaS configurées par l'administrateur pour l'utilisateur final. Lorsqu'un utilisateur clique sur un lien dans une application native, s'il s'agit d'un lien de travail, il est ouvert via Enterprise Browser. Si ce n'est pas le cas, il est ouvert via l'autre navigateur sélectionné par l'utilisateur final.

Pour plus d'informations, voir [Définir Citrix Enterprise Browser comme navigateur de travail](#).

Problèmes résolus

- Le protocole HTTP Live Streaming (HLS) avec le flux AAC-HE (High-Efficiency Advanced Audio Coding) ne parvient pas à lire le son sur Citrix Enterprise Browser. [CTXBR-3899]
- Lorsque vous cliquez sur un lien hypertexte dans le portail personnalisé, un message d'erreur s'affiche avant d'ouvrir le lien. Le lien s'ouvre ultérieurement dans un navigateur système, par exemple Google Chrome au lieu de Citrix Enterprise Browser. [CTXBR-4051]
- Lorsque vous utilisez l'application Citrix Workspace pour Mac avec une URL de magasin Web personnalisé, les versions du système d'exploitation et de l'application Citrix Workspace peuvent ne pas apparaître dans le user-agent. [CVADHELP-21377]
- Grâce à ce correctif, certaines applications tierces telles que Epic ou Kronos n'ont pas tendance à se bloquer lorsque vous les démarrez. [HDX-46140]
- Lorsque vous essayez de démarrer une session à l'aide d'un fichier ICA provenant de la version bêta de l'application Citrix Workspace 2301 pour Mac pour la première fois, la session peut se fermer de manière inattendue. [HDX-47361]
- Lorsque vous ajoutez le site de portail personnalisé à l'application Citrix Workspace pour Mac, une page vierge peut s'afficher. [RFMAC-12857]

2211.1

Nouveautés

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

Problèmes résolus

- Vous pouvez rencontrer des problèmes lorsque vous ajoutez ou authentifiez un magasin, ou lorsque vous démarrez une ressource (applications ou bureaux) à l'aide de l'application Citrix Workspace native. [CVADHELP-22372]
- La vidéo entrante et le partage d'écran peuvent ne pas fonctionner pendant les appels vidéo Microsoft Teams optimisés. [HDX-50059]

2211

Nouveautés

Les applications Workspace apparaissent dans le Dock avec des icônes natives lorsqu'elles sont ouvertes [version Technical Preview] À partir de la version 2211, cette fonctionnalité est désactivée par défaut.

Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le [formulaire Podio](#).

Amélioration de l'expérience Mission Control et App Expose [version Technical Preview] À partir de la version 2211, cette fonctionnalité est désactivée par défaut.

Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le [formulaire Podio](#).

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 105.2.1.40, basé sur Chromium version 105. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

Problèmes résolus

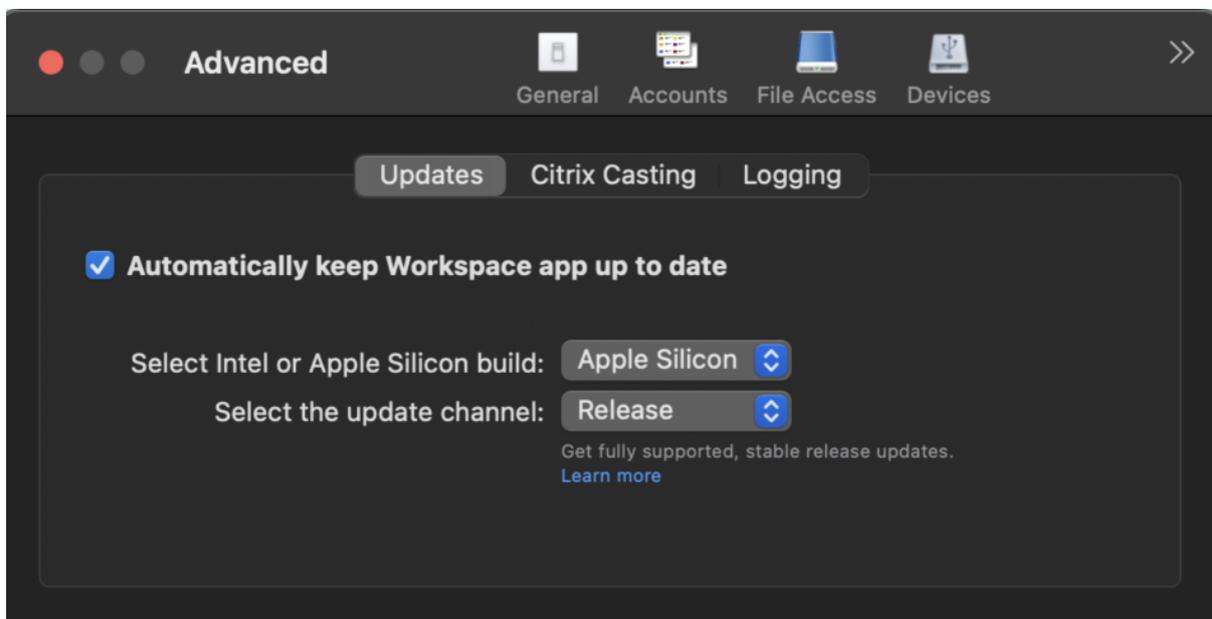
Cette version résout également plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

2210

Nouveautés

Prise en charge de macOS 13 Ventura L'application Citrix Workspace pour Mac est prise en charge sur macOS 13 Ventura (13.0).

Amélioration de la mise à jour automatique sur Mac avec puce Apple (M1) À partir de cette version, lorsque vous téléchargez la version Architecture universelle, vous pouvez choisir entre les versions puce Apple et Intel pour prendre en charge les deux, les machines Mac avec puce Apple et basées sur Intel.



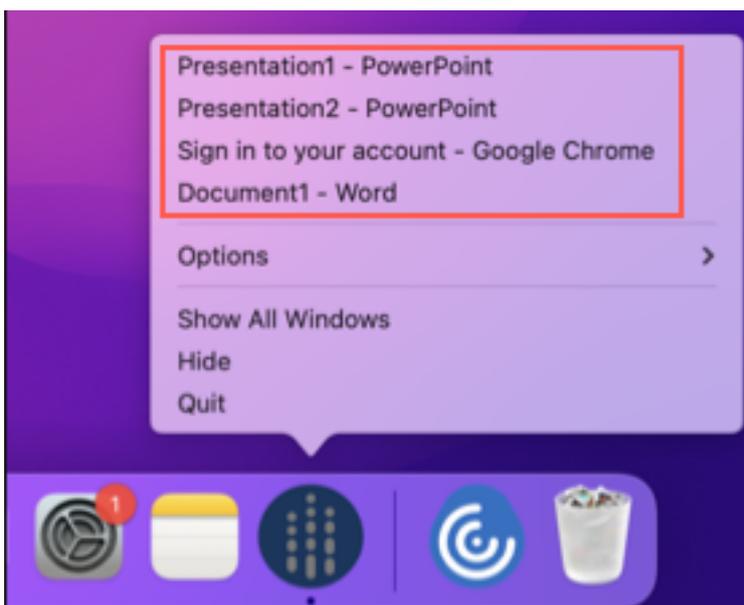
Sur les machines avec puce Apple, les utilisateurs ont la possibilité de mettre à jour automatiquement la version Intel même après avoir téléchargé la version puce Apple. L'option est fournie dans l'onglet **Préférences**.

Configuration avancée des mises à jour automatiques Vous pouvez configurer les mises à jour automatiques de Citrix Workspace sur Mac avec puce Apple (M1) à l'aide des méthodes suivantes :

- Interface utilisateur graphique
- Global App Configuration Service (GACS)
- Gestion des appareils mobiles (MDM)
- StoreFront

Pour plus d'informations, consultez [Configuration avancée des mises à jour automatiques](#).

Les applications Workspace apparaissent dans le Dock avec des icônes natives lorsqu'elles sont ouvertes [version Technical Preview] Auparavant, le fait de cliquer sur des applications virtuelles dans l'application Citrix Workspace déclenchait Citrix Viewer où ces applications étaient disponibles. Si vous ouvrez de nombreuses applications, les applications ou leurs instances se sont ouvertes dans Citrix Viewer. Vous pouvez afficher les applications ouvertes en cliquant avec le bouton droit sur l'icône Citrix Viewer.



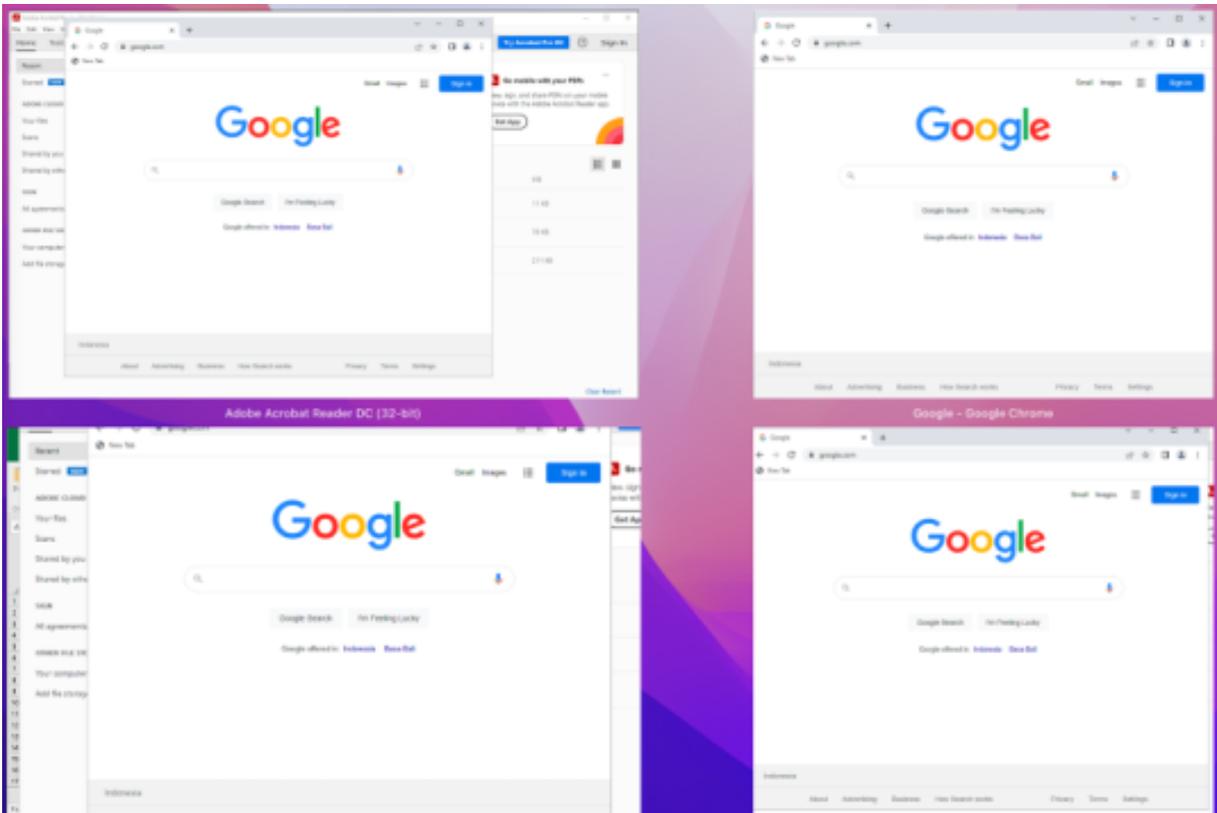
À partir de cette version, lorsque vous ouvrez des applications virtuelles, elles apparaissent dans le Dock avec leurs icônes respectives et sont facilement identifiables. Vous pouvez ensuite accéder à l'application virtuelle depuis le dock lui-même. Si vous ouvrez plusieurs instances d'une application, ces instances ne sont pas des doublons dans le Dock mais sont regroupées au sein d'une instance du Dock.



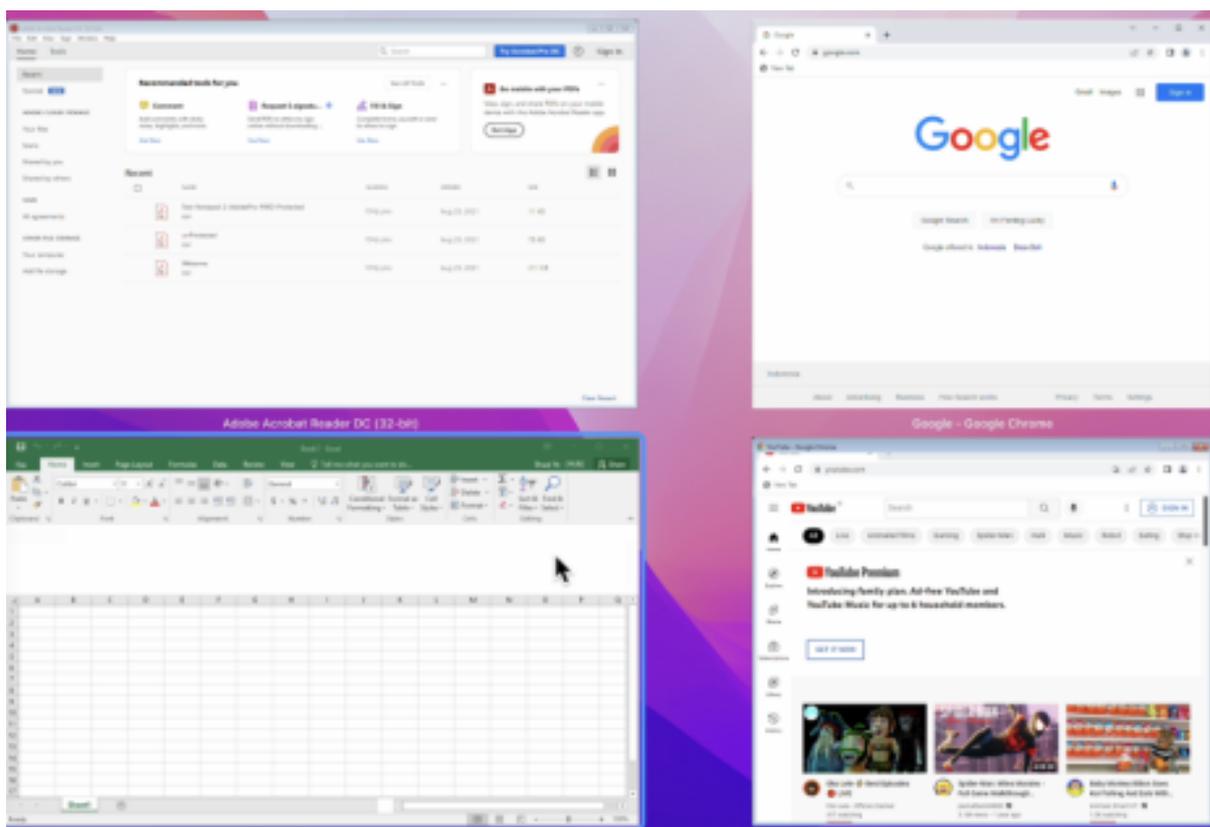
Remarque :

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 version Technical 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.

Amélioration de l'expérience Mission Control et App Expose [version Technical Preview] Au-
paravant, l'utilisation de la fonctionnalité **Mission Control** ou **App Expose** dans une session d'appli-
cation virtuelle entraînait le chevauchement de nombreuses fenêtres ouvertes.



À partir de cette version, lorsque vous utilisez la fonctionnalité **Mission Control** ou **App Expose** dans une session d'application virtuelle et que vous ouvrez de nombreuses fenêtres, les fenêtres ne se chevauchent pas et vous pouvez facilement choisir l'une d'entre elles.



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 version Technical 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.

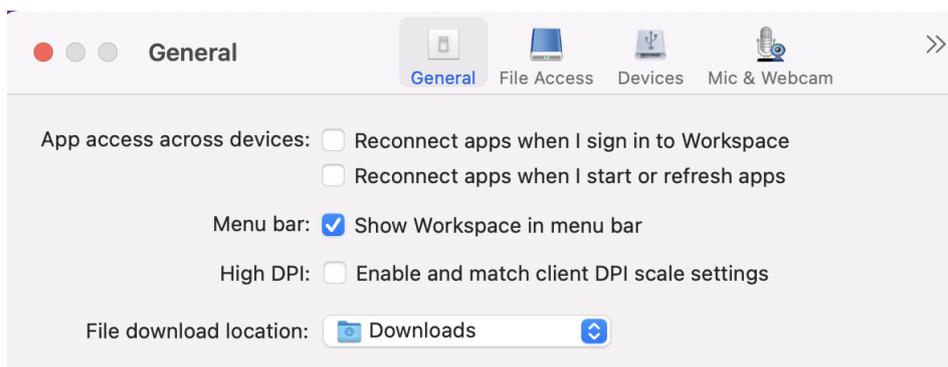
Amélioration des performances graphiques [version Technical Preview] Avec cette version, les performances graphiques sont améliorées pour les sessions de bureau.

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 version Technical 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.

Prise en charge de DPI élevé L'application Citrix Workspace pour Mac est désormais compatible avec les écrans haute résolution d'une résolution de 4K ou 5K. Avec cette fonctionnalité, le texte, les images et les autres éléments graphiques des sessions d'application ou de bureau virtuel apparaissent dans une taille qui peut être visualisée confortablement sur ces écrans haute résolution. Pour plus d'informations, consultez la section [Prise en charge de DPI élevé](#).

Pour activer cette fonctionnalité, accédez à **Préférences > Général > Haute résolution**.



Remarque :

Le nombre de moniteurs externes que vous pouvez utiliser avec votre Mac est toujours limité par le modèle Mac, ainsi que par la résolution et la fréquence d'actualisation de chaque écran. Consultez les caractéristiques techniques de votre Mac pour connaître le nombre de moniteurs externes pris en charge. Pour plus d'informations, consultez l'article [Connecter un ou plusieurs moniteurs externes avec le Mac](#) de l'assistance Apple.

Prise en charge de la configuration par les administrateurs des appareils utilisateur via l'outil MDM Les administrateurs peuvent désormais configurer les paramètres suivants lors du déploiement de l'application Citrix Workspace via n'importe quel outil de déploiement MDM tel que Citrix Endpoint Management :

- **StoreURLs** : configurez les détails du magasin afin qu'ils soient ajoutés automatiquement lorsque l'utilisateur ouvre l'application Citrix Workspace, simplifiant ainsi l'expérience de connexion.
Pour ajouter un magasin, fournissez les détails du paramètre **StoreURLs**. Par exemple, `<string>https://myorg.com/?storename</string>`.
- **BlockStoreAddition** : empêche l'utilisateur d'ajouter des magasins.
Pour empêcher l'utilisateur d'ajouter un magasin, définissez la valeur du paramètre **BlockStoreAddition** sur **True**.

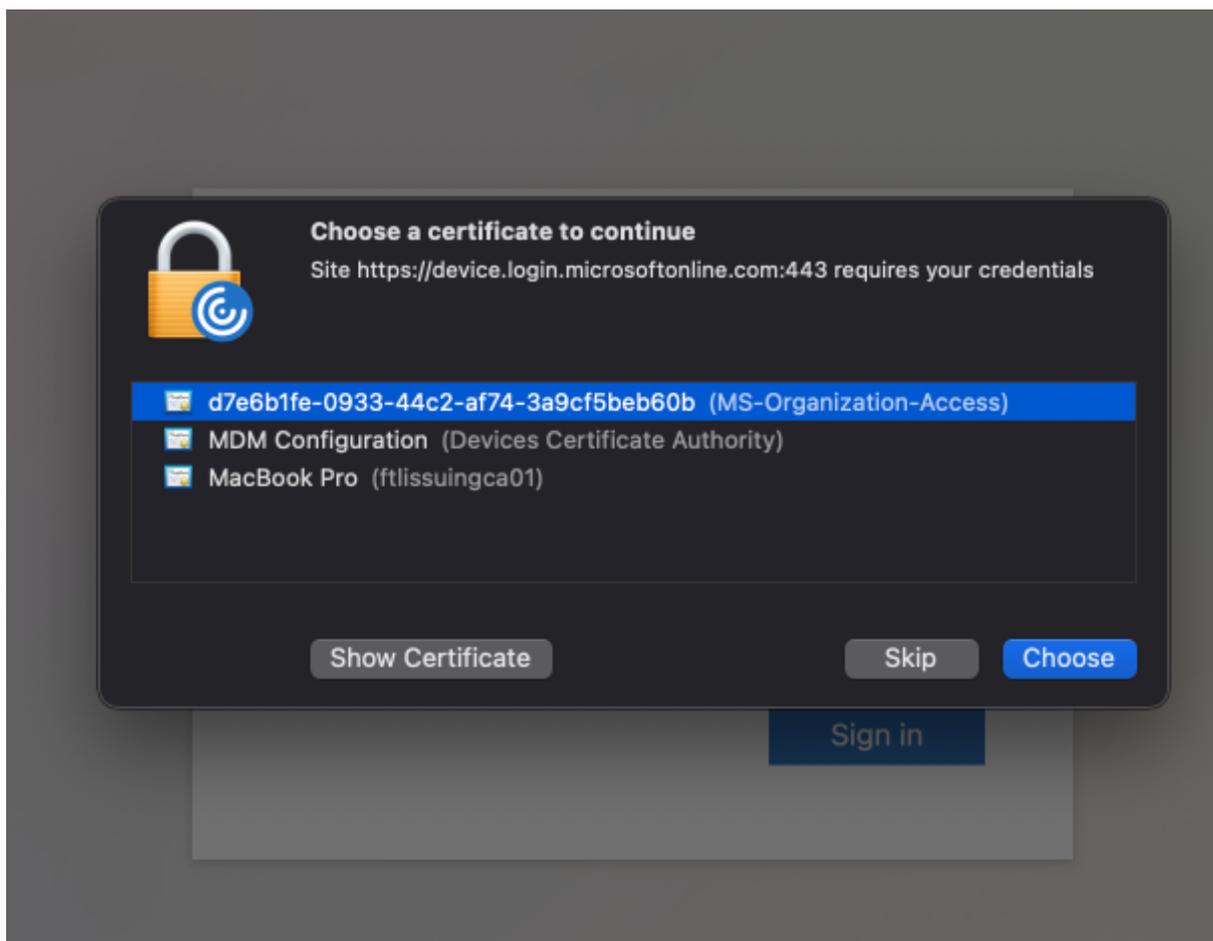
Pour plus d'informations, consultez la section [Prise en charge de la configuration de magasin des machines utilisateur via l'outil MDM](#).

Prise en charge de l'authentification basée sur des certificats [version Technical Preview] Vous pouvez désormais vous authentifier auprès de l'application Citrix Workspace (magasins cloud) à l'aide d'un certificat client.

Auparavant, l'authentification basée sur des certificats était prise en charge sur les configurations sur site et les clients utilisant des configurations cloud ne pouvaient pas se connecter à l'application Citrix Workspace. Cette fonctionnalité est désactivée par défaut et les administrateurs doivent contacter le service d'assistance Citrix pour l'activer en remplissant ce formulaire de demande.

Si votre organisation a configuré l'accès conditionnel avec Azure Active Directory, l'utilisateur est invité à sélectionner un certificat client pour l'authentification lors de la connexion. L'authentification basée sur des certificats ajoute un niveau de sécurité supplémentaire, garantissant ainsi la conformité de votre appareil.

Une fois que vous avez ajouté un magasin et que vous avez saisi des informations d'identification valides pour ce magasin, l'application Citrix Workspace affiche la liste des certificats valides disponibles dans votre trousseau pour l'authentification client. S'il n'y a qu'un seul certificat valide dans votre trousseau, il est sélectionné par défaut.



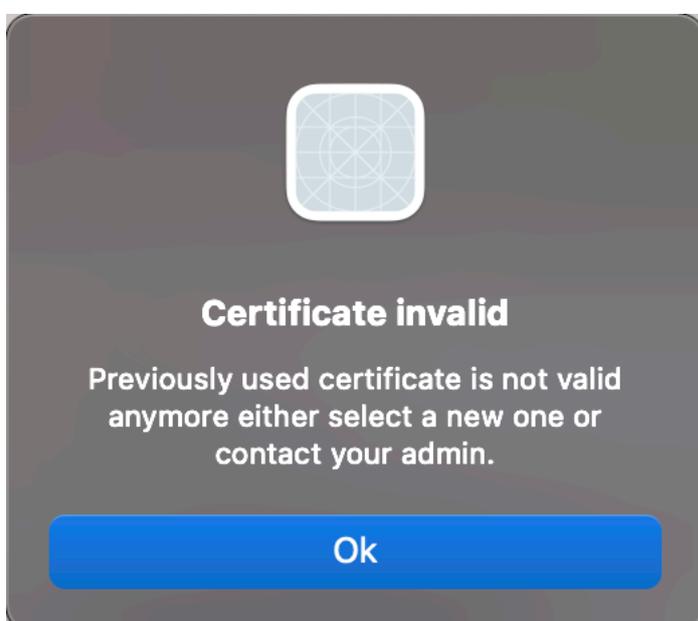
Une fois que vous avez choisi un certificat, le fournisseur d'identité le valide et le magasin d'applica-

tions Workspace apparaît en cas de validation réussie.

Remarque :

- S'il n'y a aucun certificat valide dans votre trousseau, l'application Citrix Workspace gère par défaut la demande d'authentification du certificat depuis le serveur. Cela peut empêcher l'utilisateur de se connecter.
- Si votre organisation a configuré l'accès conditionnel avec Azure Active Directory et qu'aucun certificat valide ne figure dans votre trousseau, vous ne pouvez pas vous connecter à l'application Citrix Workspace.

Si un certificat précédemment sélectionné n'est plus valide, un message d'erreur s'affiche, vous invitant à sélectionner un certificat valide ou à contacter votre administrateur en l'absence d'un tel certificat.



Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le [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 version Technical 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.

Changement de nom pour Citrix Workspace Browser Citrix Workspace Browser est désormais Citrix Enterprise Browser. Le schéma personnalisé est passé de `citrixworkspace://` à `citrixbrowser://`.

L'implémentation de cette transition dans nos produits et leur documentation est en cours. Nous vous remercions de votre patience pendant cette transition.

- L'interface utilisateur du produit, le contenu intégré au produit, ainsi que les images et les instructions de la documentation produit seront mis à jour au cours des prochaines semaines.
- Il est possible que certains éléments (tels que les commandes et les MSI) continuent à conserver leurs anciens noms pour éviter de casser les scripts clients existants.
- Documentation produit associée

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 105.1.1.19, basé sur Chromium version 105. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#). Certaines ressources (telles que des vidéos et des articles de blog) liées à cette documentation produit peuvent encore contenir d'anciens noms de produits.

Définir Citrix Enterprise Browser comme navigateur de travail [Technical Preview] Vous pouvez désormais configurer Citrix Enterprise Browser pour ouvrir tous les liens et applications de travail ou d'entreprise configurés par votre administrateur dans l'application Citrix Workspace. Cette fonctionnalité vous permet d'ouvrir uniquement des liens de travail ou des applications Web et SaaS dans Citrix Enterprise Browser.

Vous pouvez sélectionner un autre navigateur pour ouvrir d'autres liens ou applications non professionnels.

Ouvrir toutes les applications Web et SaaS via Citrix Enterprise Browser À partir de cette version, toutes les applications Web internes et les applications SaaS externes disponibles dans l'application Citrix Workspace s'ouvrent dans Citrix Enterprise Browser.

Prise en charge des extensions de navigateur [Technical Preview] Vous pouvez ajouter des extensions fournies par votre administrateur à Citrix Enterprise Browser de manière sécurisée. Un administrateur peut déployer, gérer et contrôler les extensions. Les utilisateurs finaux peuvent afficher et utiliser l'extension sous `citrixbrowser://extensions` selon leurs besoins. Pour plus de paramètres, voir [Global App Configuration Service](#).

Remarque :

Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le [formulaire Podio](#).

Pour plus d'informations sur la configuration, consultez la documentation de [Citrix Enterprise Browser](#).

Utiliser Global App Configuration Service pour gérer Citrix Enterprise Browser [version Technical Preview] L'administrateur peut utiliser Global App Configuration Service pour Citrix Workspace afin de fournir les paramètres de Citrix Enterprise Browser via un service géré de manière centralisée.

Global App Configuration Service simplifie la configuration de Citrix Workspace et la gestion des paramètres de l'application Citrix Workspace pour les administrateurs. Cette fonctionnalité permet aux administrateurs d'utiliser Global App Configuration Service pour appliquer divers paramètres ou stratégies système à Citrix Enterprise Browser sur un magasin particulier. L'administrateur peut désormais configurer et gérer les paramètres Citrix Enterprise Browser suivants à l'aide de Global App Configuration Service :

- « Enable CEB for all apps » : définit Citrix Enterprise Browser comme navigateur par défaut pour ouvrir les applications Web et SaaS à partir de l'application Citrix Workspace.
- « Enable save passwords » : autorise ou non les utilisateurs finaux à enregistrer les mots de passe.
- « Enable incognito mode » : active ou désactive le mode Navigation privée.
- « Managed Bookmarks » : autorise l'administrateur à envoyer des signets à Citrix Enterprise Browser.
- « Enable developer tools » : active ou désactive les outils de développement dans Enterprise Browser.
- « Delete browsing data on exit » : autorise l'administrateur à configurer les données que Citrix Enterprise Browser supprimera à la sortie.
- « Extension Install Force list » : autorise l'administrateur à installer des extensions dans Citrix Enterprise Browser.
- « Extension Install Allow list » : autorise l'administrateur à configurer une liste autorisée d'extensions que les utilisateurs peuvent ajouter à Citrix Enterprise Browser. Cette liste utilise le Chrome Web Store.

Remarques :

- Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le [formulaire Podio](#).
- 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 version Technical 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.

- La paire nom et valeur distingue les majuscules des minuscules.
- Tous les paramètres du navigateur dans [Global App Configuration Service](#) se trouvent dans la catégorie suivante :

```
1 {
2
3     "category": "browser",
4     "userOverride": false,
5     "assignedTo": [
6     "AllUsersNoAuthentication"
7     ]
8 }
9
10
11 <!--NeedCopy-->
```

- L'administrateur peut également appliquer les paramètres à des appareils non gérés. Pour en savoir plus, consultez la documentation de [Global App Configuration Service](#).

Technical Preview

- Version améliorée de WebRTC pour Microsoft Teams optimisé

Pour obtenir la liste complète des fonctionnalités préliminaires (version Technical Preview), consultez la page [Fonctionnalités de la version Technical Preview](#).

Problèmes résolus

- L'application Citrix Workspace peut interrompre le redémarrage ou l'arrêt de l'action d'alimentation d'un appareil Mac. [RFMAC-12530]
- La touche Maj peut ne pas fonctionner comme prévu dans l'application Citrix Workspace pour Mac version 2206. [CVADHELP-20674]

2209

Nouveautés

Déconnexion du magasin Web personnalisé lorsque vous fermez l'application Citrix Workspace

Lorsque le paramètre **signoutCustomWebstoreOnExit** est défini sur **True**, la fermeture de la fenêtre de l'application Citrix Workspace vous déconnecte du magasin Web personnalisé. Lorsque vous rouvrez l'application Citrix Workspace, l'URL du magasin Web est à nouveau chargée. Vous pouvez configurer le paramètre **signoutCustomWebstoreOnExit** dans Global App Configuration Service. Pour

plus d'informations, consultez la section [Déconnexion du magasin Web personnalisé lorsque vous fermez l'application Citrix Workspace](#)

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser (anciennement Citrix Workspace Browser) version 103.2.1.10, basé sur la version 103 de Chromium. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

Problèmes résolus

- L'application Citrix Workspace pour Mac peut démarrer automatiquement lorsque vous redémarrez l'application Citrix Workspace pour Mac ou que vous installez l'application Citrix Workspace. [RFMAC-12392]
- La fonctionnalité de partage d'écran dans Microsoft Teams optimisé pour certaines applications tierces peut échouer sur l'application Citrix Workspace pour Mac. Le problème se produit lorsque la stratégie de codec Thinwire est définie sur **Pour l'écran entier**. Par conséquent, la fonctionnalité de partage d'application est désactivée et aucune option n'est disponible dans le panneau de partage. [CVADHELP-20853]

2208.1

Nouveautés

Affichage des applications, des bureaux et de Citrix Enterprise Browser à partir de la barre de menus via un menu d'accès rapide Vous pouvez désormais afficher vos applications et bureaux les plus récemment utilisés ou préférés ou ouvrir une fenêtre Citrix Enterprise Browser en cliquant sur l'icône de Citrix Workspace dans la barre de menus. Cette fonctionnalité permet d'accéder facilement à certaines de vos ressources sans avoir à ouvrir l'application Citrix Workspace.

Remarque :

Cette fonctionnalité n'est pas disponible sur les installations locales.

Recents Favorites

Apps

-  Access 2016
-  Concur
-  Excel 2016
-  Bitbucket - code
-  Chrome

[View all applications](#)

Desktops

-  Managed Win10 SIN Desktop

[View all desktops](#)

Version: 22.06.0.0 (2206)

Si vous n'avez configuré aucun compte, une invite de connexion s'affiche.



Un maximum de 5 applications ou bureaux récemment utilisés ou favoris apparaissent respectivement dans les options sous les onglets **Récent** et **Favoris**. Pour afficher les autres applications dans l'application Citrix Workspace, cliquez sur **Afficher toutes les applications**. Pour afficher les autres bureaux dans l'application Citrix Workspace, cliquez sur **Afficher tous les bureaux**.

Recents Favorites

Apps

-  Access 2016
-  Concur
-  Excel 2016
-  Bitbucket - code
-  Chrome

[View all applications](#)

Desktops

-  Managed Win10 SIN Desktop

[View all desktops](#)

Version: 22.06.0.0 (2206)

Vous pouvez ouvrir l'interface utilisateur de Citrix Workspace en cliquant sur l'icône de l'application Citrix Workspace.

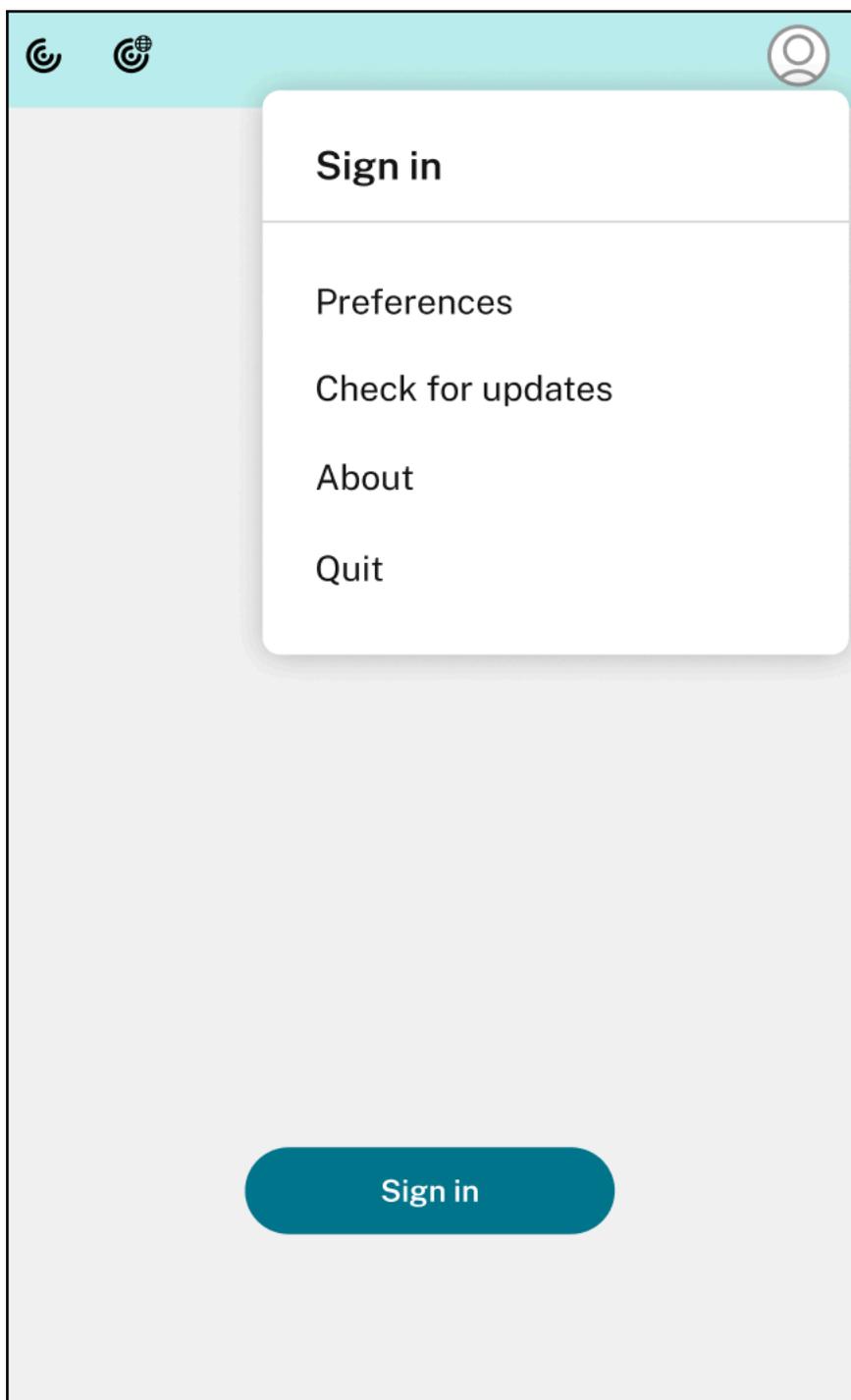


Vous pouvez ouvrir Citrix Enterprise Browser, sans ouvrir d'application Web ou SaaS en cliquant sur l'icône de Citrix Enterprise Browser.



Remarque :

Citrix Enterprise Browser n'est pas disponible si le magasin configuré ne comporte aucune application Web ou SaaS. En outre, il n'est disponible que si votre administrateur a configuré Citrix Secure Private Access.



Vous pouvez afficher les options suivantes lorsque vous cliquez sur l'icône **Compte** dans le coin supérieur droit :

- Préférences
- Rechercher les mises à jour
- À propos de

- Quitter

Pour plus d'informations, consultez la section [Affichage des applications, des bureaux et de Citrix Enterprise Browser à partir de la barre de menu via un menu d'accès rapide](#).

Prise en charge de l'authentification à l'aide de FIDO2 [version Technical Preview] Avec cette version, les utilisateurs peuvent s'authentifier au sein d'une session HDX à l'aide de clés de sécurité FIDO2 sans mot de passe. Les clés de sécurité FIDO2 permettent aux employés de l'entreprise de s'authentifier auprès d'applications ou de bureaux prenant en charge FIDO2 sans entrer de nom d'utilisateur ou de mot de passe. Pour plus d'informations sur FIDO2, consultez [Authentification FIDO2](#). Cette fonctionnalité prend actuellement en charge les authentificateurs itinérants (USB uniquement) avec code PIN et fonctionnalités tactiles. Vous pouvez configurer l'authentification basée sur les clés de sécurité FIDO2. Pour plus d'informations sur les conditions préalables et l'utilisation de cette fonctionnalité, consultez [Autorisation locale et authentification virtuelle à l'aide de FIDO2](#).

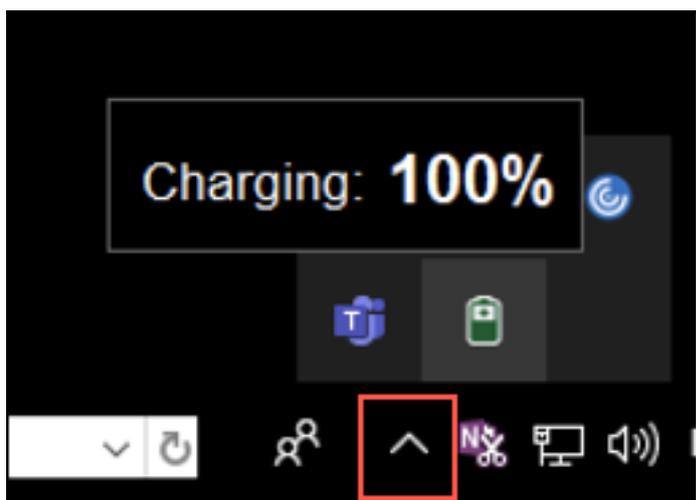
Lorsque vous accédez à une application ou à un site Web qui prend en charge FIDO2, une invite s'affiche, demandant l'accès à la clé de sécurité. Si vous avez préalablement enregistré votre clé de sécurité avec un code PIN (un minimum de 4 et un maximum de 64 caractères), vous devez saisir le code PIN lors de la connexion.

Si vous avez préalablement enregistré votre clé de sécurité sans code PIN, il vous suffit de toucher la clé de sécurité pour vous connecter.

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 version Technical 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.

Indicateur d'état de la batterie L'état de la batterie de l'appareil s'affiche désormais dans la zone de notification d'une session Citrix Desktop. Pour afficher l'état de la batterie dans la session de bureau, cliquez sur la flèche **Afficher les icônes masquées** dans la barre des tâches.



Remarque :

L'indicateur d'état de la batterie n'apparaît pas pour les VDA du serveur.

Pour plus d'informations, consultez [Indicateur d'état de la batterie](#).

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 103.1.1.14, basé sur Chromium version 103. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

Profils de Citrix Enterprise Browser Les profils vous permettent de conserver vos informations personnelles telles que l'historique, les signets, les mots de passe et d'autres paramètres séparés pour chacun de vos comptes Citrix Workspace. En fonction de votre magasin Workspace, un profil est créé, qui vous permet de bénéficier d'une expérience de navigation unique et personnalisée.

Remarque :

Après la mise à niveau vers la version 103.1.1.14 et la première connexion à l'appareil, seuls les mots de passe précédemment enregistrés sont supprimés. Lorsque vous vous connectez à l'appareil en utilisant un autre magasin pour la première fois, toutes vos données précédemment enregistrées sont perdues.

Ouvrir toutes les applications Web et SaaS via Citrix Enterprise Browser [Technical Preview]

À partir de cette version, toutes les applications Web internes et les applications SaaS externes disponibles dans l'application Citrix Workspace s'ouvrent dans Citrix Enterprise Browser. Vous pouvez vous inscrire à cette version Technical Preview en remplissant 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 version Technical 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

- Lorsque l'invite de connexion à Citrix Workspace s'affiche, le fait de cliquer sur le bouton Annuler ne ferme pas la fenêtre et elle apparaît de manière répétée. [CVADHELP-19919]
- Si vous utilisez Direct Workload Connection dans Citrix Cloud pour vous connecter directement aux VDA, un écran noir s'affiche et vous êtes déconnecté du VDA. Ce problème se produit lorsque le service de localisation de réseaux (NLS) est activé. [HDX-40588]
- Lorsque vous utilisez un geste multipoint pour passer d'une application en plein écran à une autre, la fenêtre de session de bureau Citrix Workspace devient noire pendant un moment. Ce problème se produit sur les Mac dotés d'un écran à encoche. [HDX-42314]

2206.1

Nouveautés

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.

Pour plus d'informations, consultez la section [Désinstaller](#)

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 [version Technical 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.

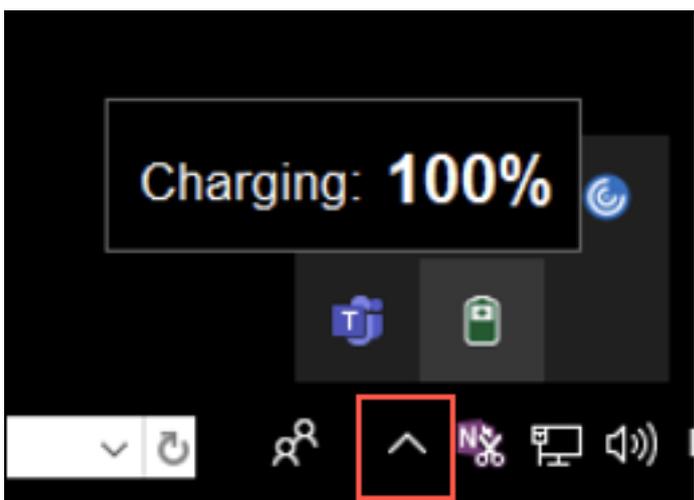
Citrix recommande d'utiliser l'audio adaptatif.

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 version Technical 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. Pour plus d'informations, consultez la section [Amélioration apportées à l'optimisation de Microsoft Teams](#)

Indicateur d'état de la batterie [version Technical 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 version Technical 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.

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 101.1.1.14, basé sur Chromium version 101. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

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, vos interlocuteurs peuvent 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]

2204

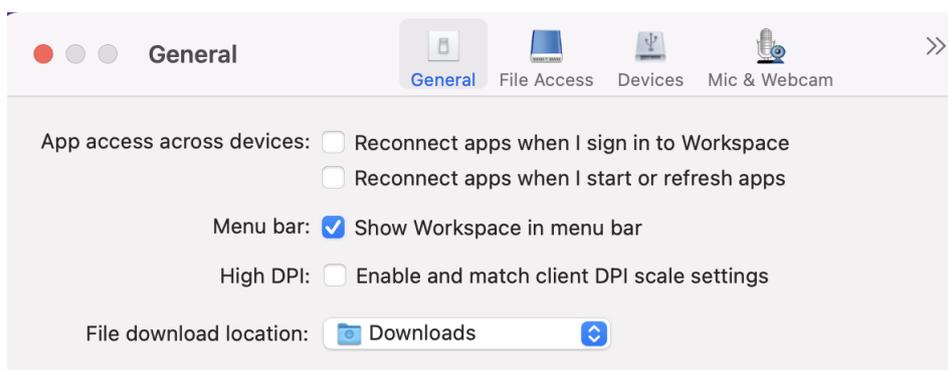
Nouveautés

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 [version Technical Preview] L'application Citrix Workspace pour Mac est désormais compatible avec les écrans haute résolution d'une résolution de 4K ou 5K. Avec cette fonctionnalité, le texte, les images et les éléments graphiques des sessions d'application ou de bureau virtuel apparaissent dans une taille qui peut être visualisée confortablement sur ces écrans haute résolution.

Pour activer cette fonctionnalité, accédez à **Préférences > Général > Haute résolution**.



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 de 65536 Ko et est suffisante pour un écran haute résolution avec une résolution 4K.

Pour les sessions d'application virtuelle, la valeur par défaut de **Limite de mémoire d'affichage** est suffisante, car la session d'application ne prend pas en charge plus d'un affichage.

Pour les sessions de bureau virtuel, les administrateurs doivent accéder à **Citrix Studio > Stratégies > Limite de mémoire d'affichage** et utiliser une valeur plus élevée, par exemple 393216 Ko pour utiliser les fonctionnalités haute résolution sur plusieurs moniteurs externes ou à résolution 5K.

Pour plus d'informations sur la stratégie Limite de mémoire d'affichage, consultez [Limite de mémoire d'affichage](#).

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 version Technical 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.

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 bureaux à distance, 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 de clavier par défaut Vous pouvez désormais restaurer les paramètres du clavier par défaut si vous les avez modifiés dans les préférences clavier de l'application Citrix Workspace. 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 App Protection avec l'optimisation HDX pour Microsoft Teams Dans cette version, le partage complet du moniteur ou du bureau est désactivé lorsque App Protection 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 Enterprise Browser Cette version inclut Citrix Enterprise Browser version 99.1.1.8, basé sur Chromium version 99. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

Définir Citrix Enterprise Browser comme navigateur par défaut Vous pouvez désormais définir Citrix Enterprise Browser comme navigateur par défaut. Une fois que vous avez défini Citrix Enterprise Browser comme navigateur par défaut, tous les liens et applications Web et SaaS s'ouvrent par défaut dans Citrix Enterprise Browser.

Pour définir Citrix Enterprise Browser comme navigateur par défaut sous macOS, procédez comme suit :

1. Ouvrez Citrix Enterprise 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 Enterprise 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, vos interlocuteurs peuvent 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

Problèmes connus dans la version 2402

- Vous remarquerez peut-être que l'écran de l'application est masqué au niveau de l'encoche lorsque vous passez en plein écran dans les sessions virtuelles sur certains Mac. Pour contourner le problème, ajustez la fenêtre de l'application pour qu'elle s'insère sous l'encoche de l'écran. [HDX-63035]

Problèmes connus dans la version 2311

La fonctionnalité de redirection vidéo HTML5 est désactivée par défaut dans l'application Citrix Workspace pour Mac à partir de la version 2311. [HDX-53015]

Problèmes connus dans la version 2308

- Après la mise à niveau de l'application Citrix Workspace pour Mac vers la version 2308, il est possible que la fenêtre des préférences ne réponde pas aux actions de l'utilisateur. Pour contourner ce problème, vous devez forcer la fermeture de l'application Citrix Workspace et la redémarrer. Pour plus d'informations sur la fermeture forcée d'une application sur Mac, consultez la section [Forcer la fermeture d'une application](#) dans l'article d'assistance Apple. [RFMAC-14596]

Problème connu dans la version 2307

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

Problème connu dans la version 2306

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

Problèmes connus dans la version 2305

- Après la mise à niveau de l'application Citrix Workspace pour Mac vers la version 2305, certaines applications virtuelles tierces dotées de boîtes de dialogue contextuelles permettant de saisir un nom d'utilisateur et un mot de passe peuvent ne plus répondre à l'ouverture. [CVADHELP-23032]

Problèmes connus dans la version 2304

- Un utilisateur possédant plusieurs comptes peut voir l'écran de chargement de l'application Citrix Workspace pendant une longue période. Pour contourner ce problème, vous devez quitter l'application Citrix Workspace et la redémarrer. [RFMAC-13432]

Problèmes connus dans la version 2301.1

- Vous ne pouvez pas effectuer la mise à jour vers la version 2301.1 de l'application Citrix Workspace pour Mac à l'aide du service de mise à jour automatique. Pour éviter ce problème, vous devrez installer manuellement la version 2301.1 de l'application Citrix Workspace pour Mac en téléchargeant le fichier .dmg disponible sur la page [Téléchargements](#).

Problèmes connus dans la version 2301

- Sur les appareils macOS Ventura, les applications PWA (Progressive Web App) ne s'ouvrent pas. Le message d'erreur suivant s'affiche :

Le nom de l'application est endommagé et ne peut pas être ouvert. Vous devriez placer cet élément dans la Corbeille.

Pour contourner le problème, cliquez avec le bouton droit sur l'application et sélectionnez Ouvrir. Si vous utilisez le clavier, appuyez sur la touche Ctrl et cliquez sur l'application. Sélectionnez Ouvrir. [CTXBR-3885]

- Une icône de chargement infini peut apparaître lorsque les utilisateurs se connectent à Citrix Workspace associé à Global App Configuration Service. Ce problème n'a aucune incidence sur StoreFront et les magasins Web personnalisés. [RFMAC-13086]

Problème connu dans la version 2211.1

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

Problèmes connus dans la version 2211

- Lorsque vous utilisez l'application Citrix Workspace pour Mac 2209 et versions ultérieures, la page de connexion utilisateur peut ne pas s'afficher lors de l'utilisation du portail Web personnalisé. Pour contourner ce problème, quittez l'application Citrix Workspace en utilisant l'option **Quitter** depuis l'icône de Citrix Workspace dans la barre de menus. [CVADHELP-21377]

Problèmes connus dans la version 2210

- Sur macOS 13 Ventura, l'interaction fluide avec les applications peut rencontrer des problèmes lorsque vous remplacez l'option par défaut **En une fois** par l'option **Une à la fois** dans la préférence **Stage Manager** sous la fonctionnalité **Stage Manager**. [HDX-44567]
- Les tentatives de démarrage d'une session de bureau en mode hors connexion peuvent échouer. Pour contourner le problème, redimensionnez la fenêtre de session. [HDX-45081]
- Lorsque vous redimensionnez une session en mode plein écran sur un MacBook, le point focal d'un curseur peut apparaître légèrement au-dessus de la position réelle du curseur. Pour contourner ce problème, accédez à **Préférences système > Dock et barre des menus** et activez l'option **Masquer/afficher automatiquement la barre des menus en plein écran**. [HDX-45585]
- Avec la version 2210, l'utilisation des fonctionnalités Mission Control ou App Expose dans une session d'application peut provoquer la fermeture inattendue de l'application Citrix Workspace. [HDX-46130]
- Lorsque vous lancez certaines applications tierces telles qu'Epic ou Kronos, la fenêtre de connexion de ces applications peut être couverte par une autre fenêtre. Par conséquent, la session se bloque. Pour contourner ce problème, effectuez l'une des actions suivantes :
 - Faites glisser la fenêtre qui bloque la fenêtre de connexion pour l'en éloigner.
 - Localisez la fenêtre de connexion à l'aide de la fonction Mission Control.
 - Utilisez le raccourci clavier **Commande+~** pour changer de fenêtre.

[HDX-46140]

Problèmes connus dans la version 2209

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

Problèmes connus dans la version 2208.1

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

Problèmes connus dans la version 2206.1

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

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 si la fenêtre du navigateur est réduite. [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 Enterprise Browser. Ce problème se produit si Citrix Enterprise Browser a été épinglé au 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 Enterprise 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 Enterprise Browser version 2201 vers la version 2203, vous ne pouvez pas enregistrer de nouveaux mots de passe et les mots de passe déjà enregistrés sont perdus. [CTXBR-3063]
- Le mode plein écran n'est pas disponible sur les Mac dotés d'un écran à 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 *App Protection* 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]

Fin de prise en charge

Pour plus d'informations sur les éléments obsolètes, consultez la page [Fin de prise en charge](#).

Ancienne documentation

Pour les versions de produits qui ont atteint leur fin de vie, consultez la section [Ancienne documentation](#).

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](#)

Fonctionnalités de la version Technical Preview

June 26, 2024

Les fonctionnalités présentées dans les versions Technical Preview sont disponibles à des fins d'utilisation 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 présentées dans les versions Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut prendre en considération les commentaires en fonction de leur gravité, criticité et importance.

Liste des fonctionnalités de la version Technical Preview

Le tableau suivant répertorie les fonctionnalités de la version Technical Preview. Ces fonctionnalités sont des fonctionnalités de prévisualisation sur demande uniquement. Pour activer l'une de ces fonctionnalités et fournir des commentaires sur celles-ci, remplissez les formulaires correspondants.

Titre	Disponible à partir de la version	Formulaire d'activation (cliquez sur l'icône)	Formulaire de commentaires (cliquez sur l'icône)
Prise en charge de l'authentification unique pour accéder à Citrix Secure Access automatiquement via l'application Citrix Workspace	2402		
Gestion des applications clientes pour le plug-in Zoom VDI	2402		
Barre d'outils de Desktop Viewer améliorée	2402		
Personnaliser la barre d'outils de Desktop Viewer	2402		
Activer la dissimulation de perte de paquets pour améliorer les performances audio	2402		

Titre	Disponible à partir de la version	Formulaire d'activation (cliquez sur l'icône)	Formulaire de commentaires (cliquez sur l'icône)
Prise en charge de l'extension automatique de la session de bureau à des moniteurs externes	2402		
Initiative de développement durable pour l'application Citrix Workspace	2402		
Prise en charge de Citrix Secure Private Access pour les déploiements locaux	2309		
Amélioration de l'option DPI élevé	2308		
Prise en charge du Gestionnaire d'activités sur les magasins cloud	2308		
Configuration de l'accès aux fichiers par magasin	2308		
Prise en charge de l'accessibilité du clavier pour la barre d'outils du bureau virtuel	2307		

Titre	Disponible à partir de la version	Formulaire d'activation (cliquez sur l'icône)	Formulaire de commentaires (cliquez sur l'icône)
Gestion des applications clientes	2305		
Numérisation rapide	2304		
Version améliorée de WebRTC pour Microsoft Teams optimisé	2210		
Prise en charge d'une expérience d'authentification unique (SSO) améliorée pour les applications Web et SaaS	2203.1		

Prise en charge de l'authentification unique pour accéder à Citrix Secure Access automatiquement via l'application Citrix Workspace

Technical Preview de la version 2402 [Formulaire d'activation](#) [Formulaire de commentaires](#)

L'application Citrix Workspace pour Mac prend désormais automatiquement en charge l'authentification unique (SSO) pour accéder à Citrix Secure Access une fois que vous vous êtes connecté à l'application Citrix Workspace. Si l'agent Citrix Secure Access et l'application Citrix Workspace sont installés sur votre périphérique, cette fonctionnalité vous permet de vous connecter automatiquement à Citrix Secure Access via SSO lorsque vous vous connectez à l'application Citrix Workspace. Pour plus d'informations, consultez la section [Authentification unique automatique \(SSO\) pour accéder à Citrix Secure Access via l'application Citrix Workspace - Technical Preview](#) dans la documentation NetScaler.

Pour activer cette fonctionnalité via MDM, l'administrateur doit utiliser les paramètres suivants :

```
<key>EnableSecureAccessAutoLogin</key><true/>
```

Remarque :

- Vous devez utiliser Citrix Secure Access version 24.03.1 ou ultérieure pour activer cette fonctionnalité.
- Cette fonctionnalité n'est prise en charge que sur les magasins dans le cloud et non sur les magasins sur site.

Gestion des applications clientes pour le plug-in Zoom VDI

Technical Preview de la
version 2402

[Formulaire d'activation](#)

[Formulaire de commentaires](#)

À partir de la version 2402, vous pouvez gérer le plug-in Zoom VDI à l'aide de la fonctionnalité Gestion des applications clientes. Grâce à cette fonctionnalité, vous pouvez télécharger, installer et mettre à jour automatiquement le plug-in Zoom VDI depuis l'application Citrix Workspace.

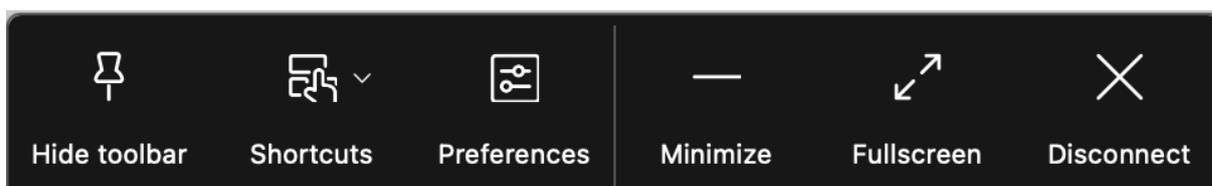
Barre d'outils de Desktop Viewer améliorée

Technical Preview de la
version 2402

[Formulaire d'activation](#)

[Formulaire de commentaires](#)

À partir de la version 2402, la barre d'outils du visualiseur de bureau virtuel a été améliorée pour être plus intuitive, moderne et conviviale.



La nouvelle barre d'outils propose les options suivantes :

- **Afficher ou masquer la barre d'outils** : cliquez sur ce bouton pour afficher ou masquer la barre d'outils de Desktop Viewer. Une encoche apparaît lorsque la barre d'outils est masquée.
- **Raccourcis** : cliquez sur ce bouton pour accéder aux raccourcis.
- **Appareils** : cliquez sur ce bouton pour accéder aux options de la section Appareils.
- **Préférences** : cliquez sur ce bouton pour accéder aux options de la section Préférences.
- **Minimiser** : cliquez sur ce bouton pour réduire la session virtuelle. Cette option est masquée en mode plein écran.

- **Plein écran** : cliquez sur ce bouton pour accéder à la session virtuelle en plein écran.
- **Restaurer** : cliquez sur ce bouton pour restaurer la session virtuelle à partir du mode plein écran.
- **Déconnecter** : cliquez sur ce bouton pour vous déconnecter d'une session virtuelle.

Vous pouvez faire glisser la barre d'outils sur tous les écrans de la session virtuelle. Lorsque vous faites glisser la barre d'outils, elle peut pivoter automatiquement en fonction de son emplacement à l'écran. Une fois que vous relâchez le curseur, celui-ci se positionne sur le bord le plus proche de l'écran.

Personnaliser la barre d'outils de Desktop Viewer

Technical Preview de la
version 2402

[Formulaire d'activation](#)

[Formulaire de commentaires](#)

Auparavant, vous pouviez désactiver complètement la barre d'outils de **Desktop Viewer**. Cependant, vous ne pouviez pas activer ou désactiver certaines options de la barre d'outils. À partir de cette version, vous pouvez personnaliser la barre d'outils de l'application Citrix Workspace en y ajoutant des options ou en les supprimant. Pour plus d'informations, consultez [Masquer ou afficher la barre d'outils du bureau dans la session de bureau virtuel](#).

Vous pouvez configurer la barre d'outils via les paramètres de gestion des appareils mobiles (MDM). Les paramètres suivants peuvent masquer les boutons Appareil, Préférences, Réduire et Plein écran :

```
1 <key>HiddenToolBarButtons</key>
2 <array>
3   <string>device</string>
4   <string>preferences</string>
5   <string>minimize</string>
6   <string>fullscreen</string>
7 </array>
8
9 <!--NeedCopy-->
```

Remarque :

Vous ne pouvez pas masquer le bouton **Épingler** de la barre d'outils.

Activer la dissimulation de perte de paquets pour améliorer les performances audio

Technical Preview de la
version 2402

[Formulaire d'activation](#)

[Formulaire de commentaires](#)

À partir de la version 2402, le mécanisme de tampon de gigue est amélioré et la dissimulation de perte de paquets (PLC, Packet Loss Concealment) est ajoutée au codec audio adaptatif. La dissimulation de perte de paquets permet de reconstruire les paquets de données perdus. Cette amélioration permet d'améliorer la tolérance à la perte de paquets et la tolérance à la gigue, et d'augmenter ainsi les performances audio et le mode de tolérance de pertes (compression avec perte EDT) pour l'audio.

Pour activer cette fonctionnalité, vous devez également activer le mode de tolérance de pertes pour la fonction audio.

Prise en charge de l'extension automatique de la session de bureau à des moniteurs externes

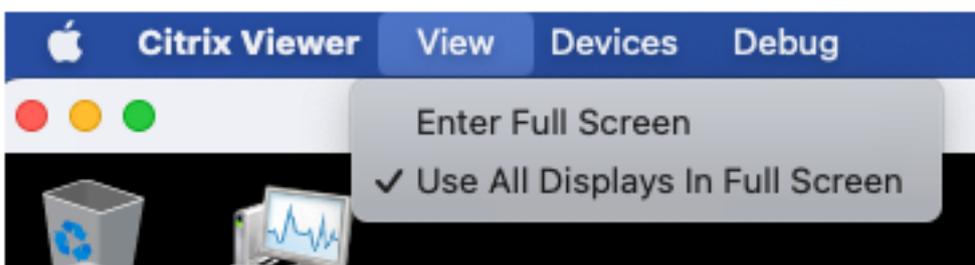
Technical Preview de la
version 2402

[Formulaire d'activation](#)

[Formulaire de commentaires](#)

À partir de la version 2402, l'application Citrix Workspace prend en charge l'extension automatique des sessions de bureau vers des moniteurs externes. Lorsque vous lancez la session de bureau sur le point de terminaison, si les écrans externes sont déjà connectés au point de terminaison, la session est automatiquement étendue aux moniteurs externes. Lorsque vous déconnectez le moniteur externe, la session peut s'ajuster automatiquement pour ne s'étendre qu'aux moniteurs connectés.

Pour activer cette fonctionnalité, accédez au menu **Afficher** de la barre de menus de **Citrix Viewer** et sélectionnez l'option **Utiliser tous les affichages en plein écran**.



Initiative de développement durable pour l'application Citrix Workspace

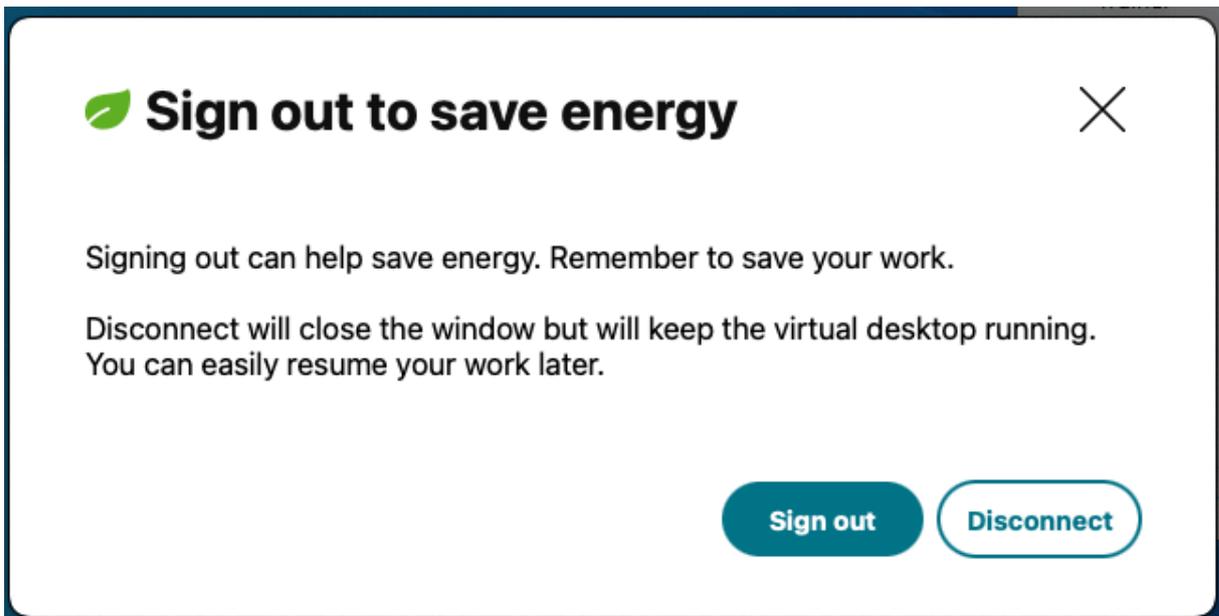
Technical Preview de la
version 2402

[Formulaire d'activation](#)

[Formulaire de commentaires](#)

À partir de la version 2402, l'application Citrix Workspace pour Mac prend en charge l'option **Déconnexion** pour la session de bureau virtuel. Cette fonctionnalité peut vous aider à économiser de l'énergie si vous vous déconnectez des machines virtuelles lorsque vous ne les utilisez pas.

Lorsque l'utilisateur clique sur **Déconnecter** ou **Déconnexion**, ou ferme un bureau virtuel, l'invite suivante s'affiche, lui recommandant d'utiliser l'option **Déconnexion** pour économiser de l'énergie.



Prise en charge de Citrix Secure Private Access pour les déploiements locaux

Technical Preview de la
version 2309

[Formulaire d'activation](#)

[Formulaire de commentaires](#)

À partir de la version 2309, l'application Citrix Workspace pour Mac prend en charge Citrix Secure Private Access pour les déploiements locaux. Pour plus d'informations, consultez [Secure Private Access pour un déploiement local \(version Technical Preview\)](#).

Amélioration de l'option DPI élevé

Technical Preview de la
version 2308

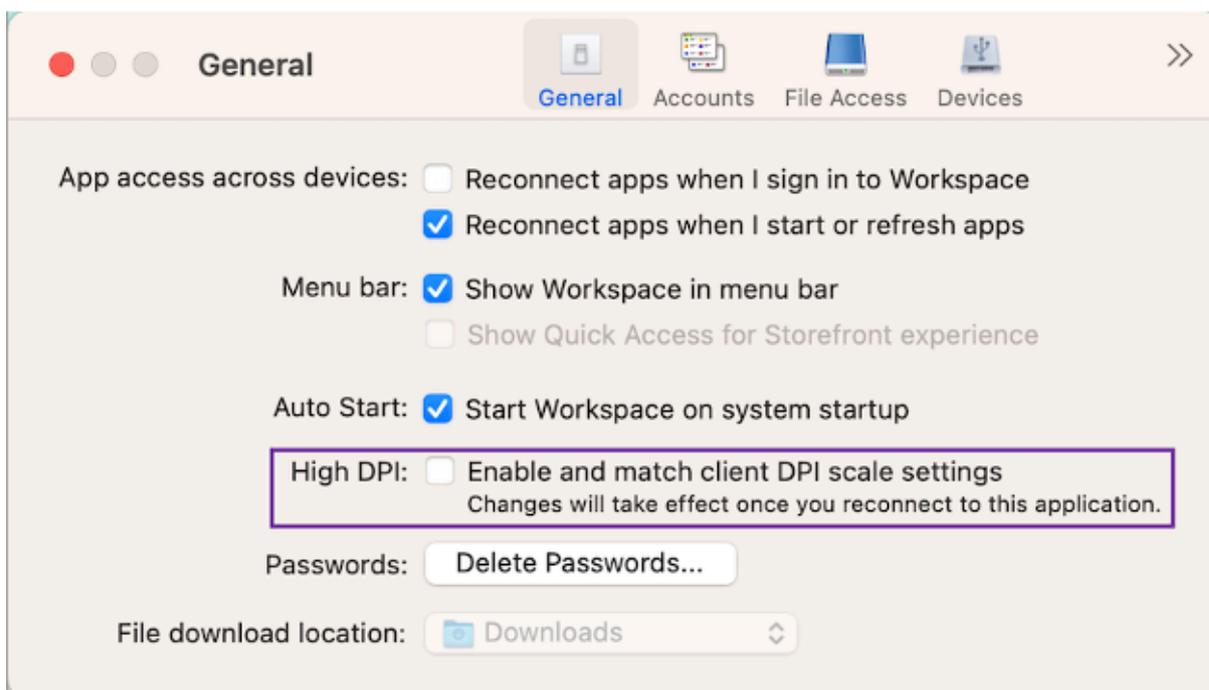
[Formulaire d'activation](#)

[Formulaire de commentaires](#)

Auparavant, l'application Citrix Workspace prenait en charge l'option **DPI élevé** uniquement pour les sessions de bureau virtuel.

À partir de la version 2308, l'activation de l'option **DPI élevé** peut également permettre des sessions d'application transparentes. De plus, vous pouvez désormais activer l'option DPI élevé sur trois moniteurs 4K. Ces fonctionnalités sont désactivées par défaut.

Pour activer l'option **DPI élevé**, vous devez sélectionner **Préférences > Général**. Dans l'onglet **Général**, sélectionnez **Activer et adapter aux paramètres de haute résolution du client**. Redémarrez l'application pour que les modifications prennent effet.



Prise en charge du Gestionnaire d'activités sur les magasins cloud

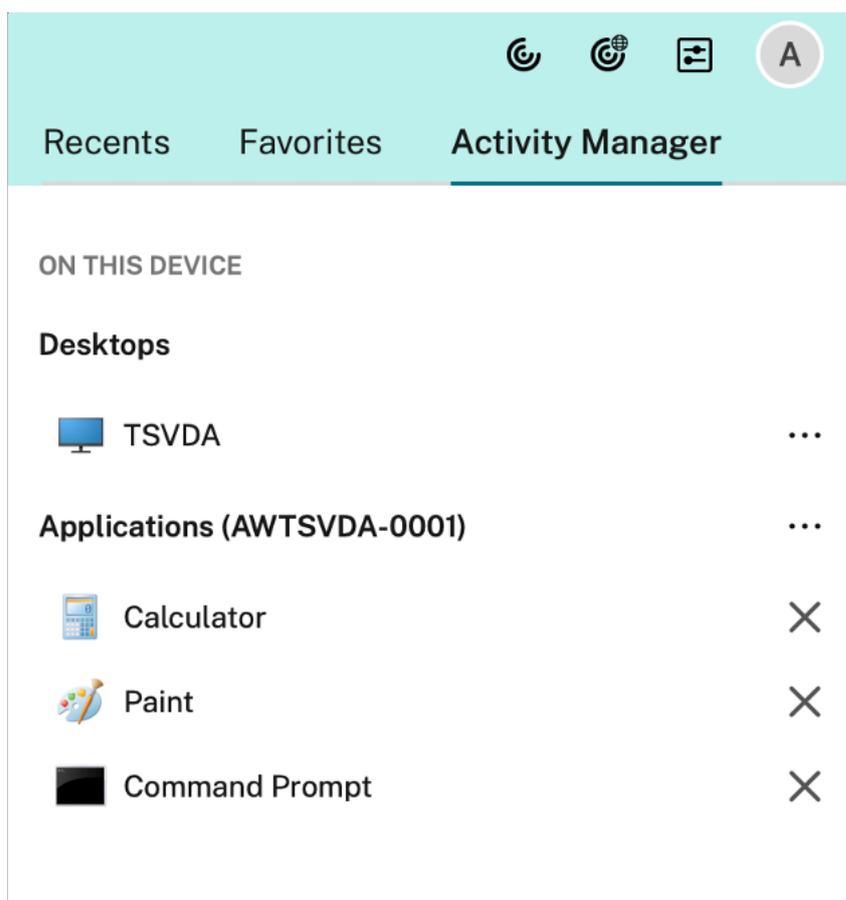
Technical Preview de la
version 2308

[Formulaire d'activation](#)

[Formulaire de commentaires](#)

L'application Citrix Workspace pour Mac prend en charge la fonctionnalité de Gestionnaire d'activités. Cette fonctionnalité permet aux utilisateurs d'afficher toutes leurs sessions d'application et de bureau actives et d'interagir avec celles-ci en un seul endroit. Vous pouvez déconnecter ou terminer les sessions actives directement depuis le Gestionnaire d'activités.

Pour afficher les sessions actives dans le **Gestionnaire d'activités**, sélectionnez l'icône de l'application Citrix Workspace dans la barre de menu, puis cliquez sur **Gestionnaire d'activités**. Pour déconnecter les sessions de bureau actives, sélectionnez le menu de points de suspension correspondant (...) et cliquez sur **Déconnecter**. Cliquez sur le bouton « X » pour mettre fin à la session d'application active. Pour plus d'informations, consultez [Gestionnaire d'activités](#).



Configuration de l'accès aux fichiers par magasin

Technical Preview de la
version 2308

[Formulaire d'activation](#)

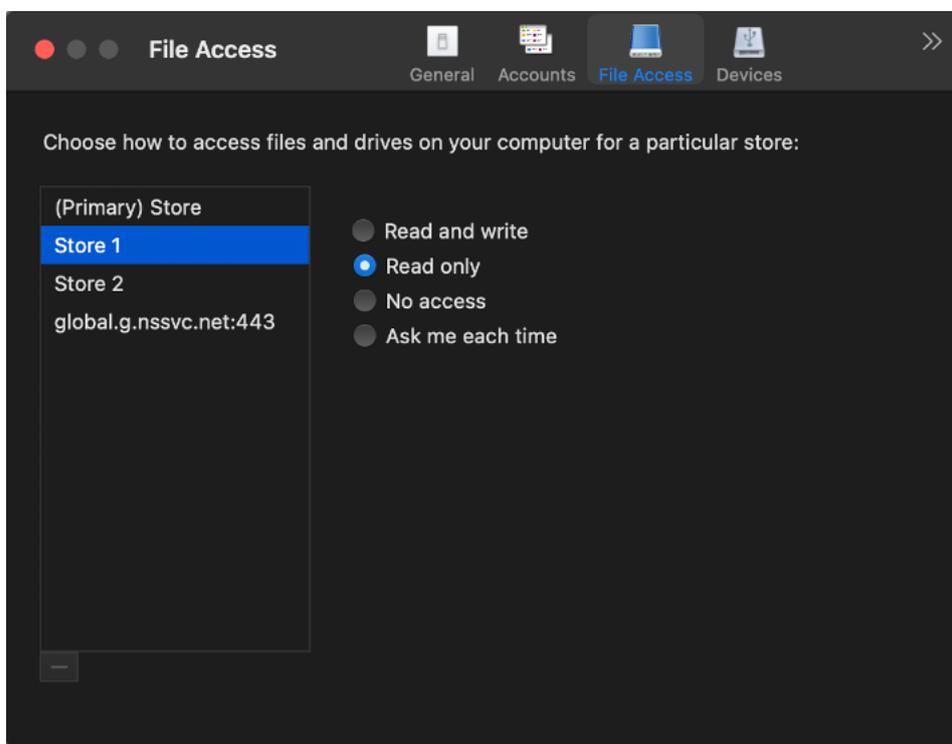
[Formulaire de commentaires](#)

À partir de la version 2308, l'accès aux fichiers par magasin est inclus dans le cadre de la fonction Client Selective Trust. Cette amélioration vous permet de fournir un accès aux fichiers par magasin.

Pour activer l'accès aux fichiers par magasin, vous devez sélectionner **Préférences > Accès aux fichiers**. Dans l'onglet **Accès aux fichiers**, sélectionnez le magasin et le type d'accès requis pour ce magasin. Vous pouvez choisir l'un des types d'accès suivants pour les fichiers et les lecteurs de votre ordinateur :

- **Lecture et écriture** : fournit un accès en lecture et en écriture aux fichiers et aux lecteurs du magasin sélectionné.
- **Lecture seule** : fournit un accès en lecture seule aux fichiers et aux lecteurs du magasin sélectionné.
- **Aucun accès** : limite l'accès aux fichiers et aux lecteurs du magasin sélectionné.

- **Toujours me demander** : demande l'autorisation d'accéder aux fichiers et aux lecteurs chaque fois qu'un accès en lecture ou en écriture est requis pour le magasin sélectionné.



Prise en charge de l'accessibilité du clavier pour la barre d'outils du bureau virtuel

Technical Preview de la
version 2307

[Formulaire d'activation](#)

[Formulaire de commentaires](#)

Dans la version 2307, vous pouvez utiliser le raccourci clavier pour accéder à la barre d'outils de l'infrastructure de bureau virtuel (VDI). Dans **Citrix Viewer**, accédez à **Affichage** dans la barre de menus et sélectionnez **Utiliser le raccourci de la barre d'outils** pour utiliser le raccourci clavier. Par défaut, l'option **Utiliser le raccourci de la barre d'outils** est activée.

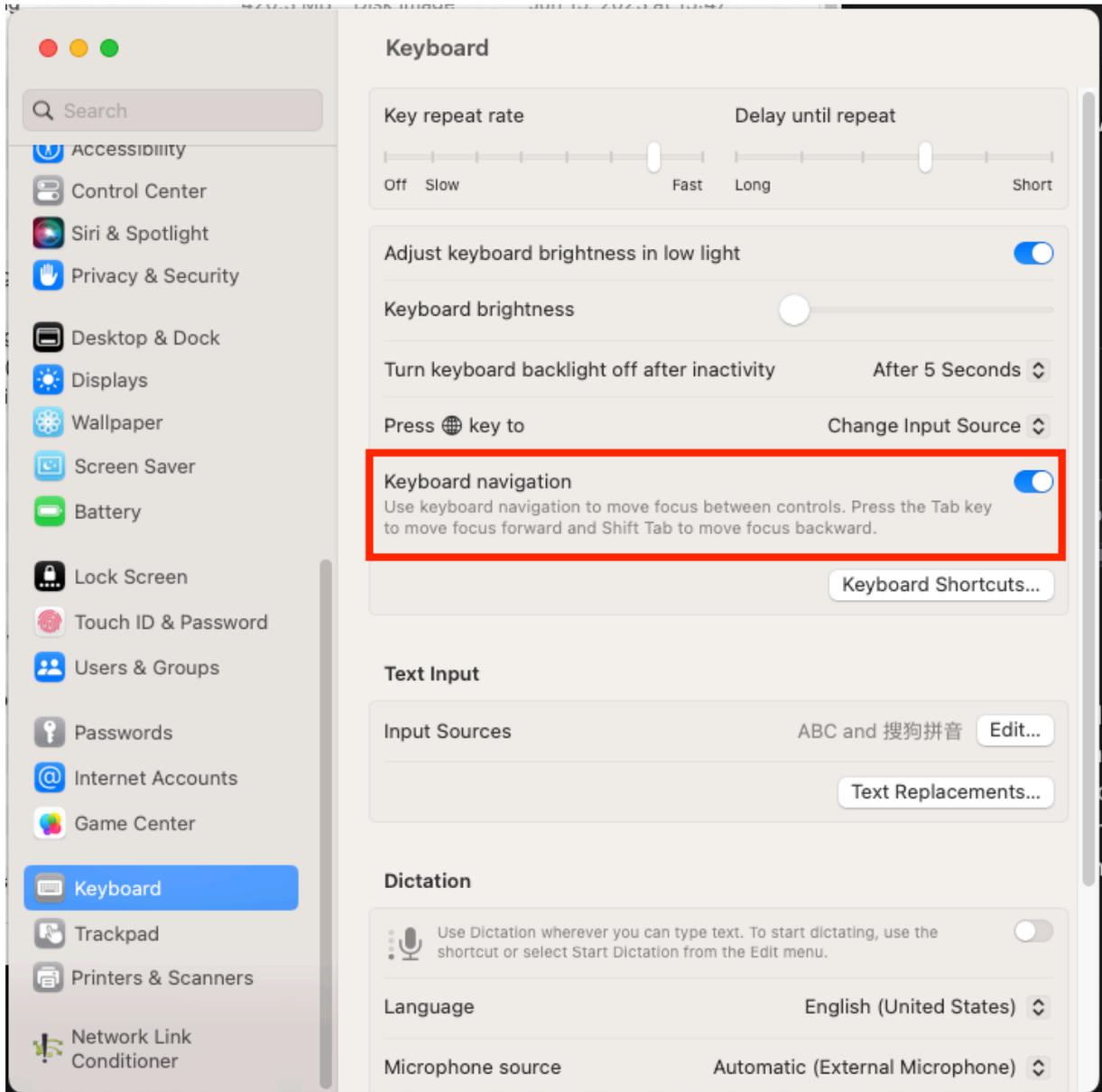


Vous pouvez utiliser les raccourcis clavier suivants pour accéder à la barre d'outils du VDI à l'aide du clavier :

- **Maj + Commande + T** : pour activer la barre d'outils du VDI.
- **Tabulation** : pour naviguer dans la barre d'outils du VDI dans le sens des aiguilles d'une montre.
- **Maj + Tabulation** : pour naviguer dans la barre d'outils du VDI dans le sens contraire des aiguilles d'une montre.

- **Espace** : pour sélectionner une option dans la barre d'outils du VDI.
- **Échap** : pour fermer le focus d'un modal.

La barre d'outils et la fenêtre de préférences CWA prennent désormais en charge la **navigation au clavier**, ce qui permet de naviguer entre les éléments de l'interface utilisateur et de mettre en évidence l'élément ciblé.



Gestion des applications clientes

L'application Citrix Workspace 2305 pour Mac offre désormais une fonctionnalité de gestion des applications clientes qui fait de l'application Citrix Workspace une application cliente unique requise sur le terminal pour installer et gérer des agents tels que le plug-in Endpoint Analysis (EPA).

Grâce à cette fonctionnalité, les administrateurs peuvent facilement déployer et gérer les agents requis à partir d'une console de gestion unique.

Remarque :

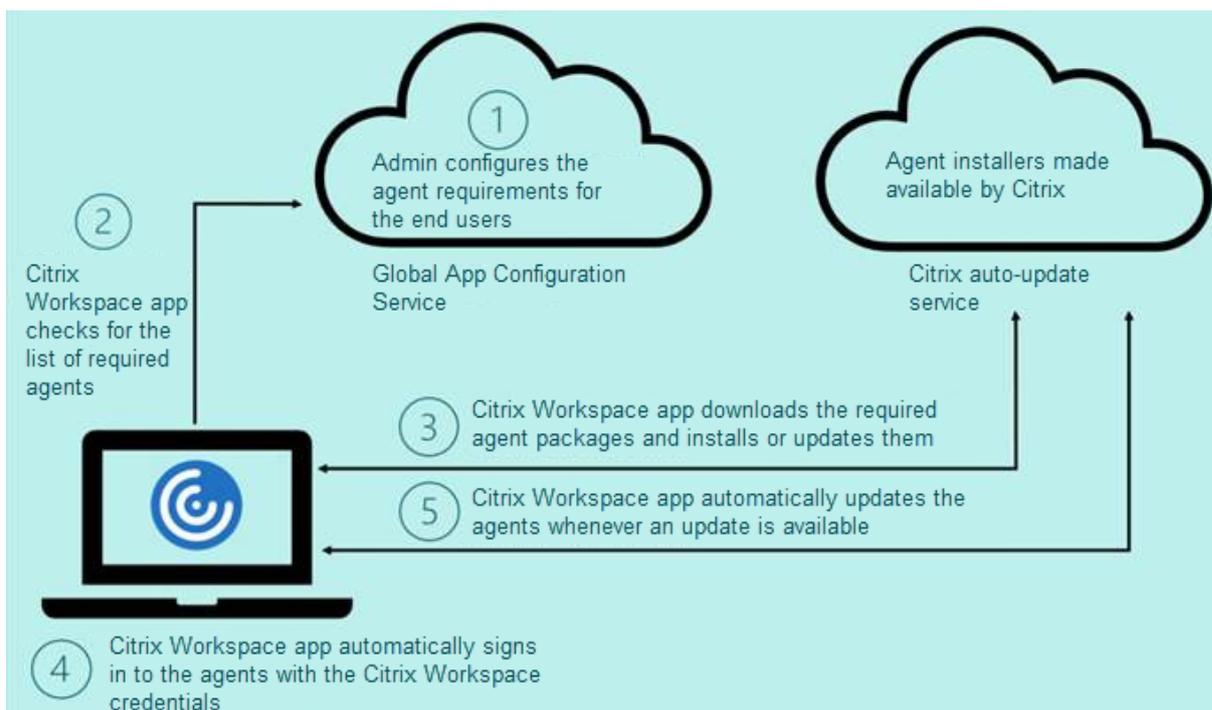
- Cette fonctionnalité s'applique uniquement aux sessions Workspace (cloud).
- Global App Configuration Service est requis pour cette fonctionnalité.

La gestion des applications clientes comprend les étapes suivantes :

- Les administrateurs doivent spécifier les agents requis sur les appareils des utilisateurs finaux dans Global App Configuration Service. Grâce à cette fonctionnalité en version Tech Preview, les administrateurs peuvent spécifier l'agent Endpoint Analysis (EPA).
- L'application Citrix Workspace extrait la liste des agents à partir de Global App Configuration Service.
- Sur la base de la liste extraite de Global App Configuration Service, l'application Citrix Workspace télécharge les packages d'agents via le service de mise à jour automatique. Si l'agent n'est pas déjà installé sur le terminal, l'application Citrix Workspace déclenche l'installation de l'agent. Si l'agent est déjà installé, l'application Citrix Workspace déclenche une mise à jour de l'agent (si la version de l'agent téléchargé est supérieure à la version installée).

L'application Citrix Workspace garantit la mise à jour automatique des agents chaque fois qu'une mise à jour est disponible à l'avenir.

Le schéma suivant illustre le workflow :



Exemple de fichier JSON dans Global App Configuration Service :

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://serviceURL:443"
6   }
7 ,
8   "settings": {
9
10    "name": "Client App management",
11    "description": "Client App management",
12    "useForAppConfig": true,
13    "appSettings": {
14
15      "macos": [
16        {
17
18          "category": "AutoUpdate",
19          "userOverride": false,
20          "assignedTo": [
21            "AllUsersNoAuthentication"
22          ],
23          "settings": [
24            {
25
26              "name": "Auto update plugins settings",
27              "value": [
28                {
```

```
29
30     "pluginName": "Citrix Endpoint
    Analysis",
31     "pluginId": "7303CB73-42EE-42BB-
    A908-9E6575912106",
32     "pluginSettings": {
33
34         "deploymentMode": "
    InstallAndUpdate",
35         "upgradeToLatest": true,
36         "minimumAllowedVersion": "1.0",
37         "maximumAllowedVersion": "24.0"
38     },
39     "delayGroup": "Medium",
40     "stream": "",
41     "isFTU": true,
42     "isBlocking": true,
43     "detectRule": ""
44     }
45 }
46 ]
47 }
48 ]
49 }
50 ]
51 }
52 ]
53 }
54 ]
55 }
56 }
57 }
58 }
59
60
61 <!--NeedCopy-->
```

Le tableau suivant répertorie le schéma, les valeurs et la description des paramètres de gestion des applications clientes.

Paramètre du schéma	Valeur	Description
isBlocking	True ou False	Lorsque le paramètre isBlocking est défini sur true, le plug-in est considéré comme obligatoire. La page de connexion apparaît uniquement lorsque le plug-in requis est installé. Citrix vous recommande de définir EPA comme plug-in obligatoire.
pluginName		Nom convivial pour le plug-in. Le nom du plug-in peut être modifié.
pluginId		Identifiant du plug-in, ne doit pas être modifié.
deploymentMode	InstallAndUpdate/Update	
maximumAllowedVersion		Version maximale autorisée du plug-in.
minimumAllowedVersion		Version minimale autorisée du plug-in.
upgradeToLatest	True ou False	

À partir de la version 2301, les administrateurs peuvent gérer la mise à jour automatique des clients EPA pour macOS via l'application Citrix Workspace et l'authentification unique à Citrix Secure Access si une connexion à l'application Citrix Workspace existe déjà.

Mise à jour automatique de Endpoint Analysis (EPA)

Vous pouvez désormais gérer la mise à jour automatique des [clients EPA pour macOS](#) via l'application Citrix Workspace. Les administrateurs doivent spécifier les agents requis sur les appareils des utilisateurs dans Global App Configuration Service. Si l'agent est déjà installé et qu'une nouvelle version de l'agent est disponible, l'application Citrix Workspace met à jour l'agent vers la version supérieure suivante. L'application Citrix Workspace garantit la mise à jour automatique des agents chaque fois qu'une nouvelle mise à jour est disponible à l'avenir.

Exemple de fichier JSON dans Global App Configuration Service :

```
1 {  
2
```

```
3   "serviceURL": {
4
5       "url": "https://serviceURL:443"
6   }
7   ,
8   "settings": {
9
10      "name": "Client App management",
11      "description": "Client App management",
12      "useForAppConfig": true,
13      "appSettings": {
14
15          "macos": [
16              {
17
18                  "category": "AutoUpdate",
19                  "userOverride": false,
20                  "assignedTo": [
21                      "AllUsersNoAuthentication"
22                  ],
23                  "settings": [
24                      {
25
26                          "name": "Auto update plugins settings",
27                          "value": [
28                              {
29
30                                  "pluginName": "Citrix Endpoint
31                                      Analysis",
32                                  "pluginId": "7303CB73-42EE-42BB-
33                                      A908-9E6575912106",
34                                  "pluginSettings": {
35
36                                      "deploymentMode": "
37                                          InstallAndUpdate",
38                                      "upgradeToLatest": true,
39                                      "minimumAllowedVersion": "1.0",
40                                      "maximumAllowedVersion": "7.0",
41                                      "delayGroup": "Medium",
42                                      "stream": "",
43                                      "isFTU": false,
44                                      "isBlocking": false,
45                                      "detectRule": ""
46                                  }
47                              }
48                          ]
49                      }
50                  ]
51              }
52          ]
53      }
54  }
```

```
53     ]
54     }
55
56     }
57
58 }
59
60
61 <!--NeedCopy-->
```

La signification des propriétés et leurs valeurs possibles pour la clé `deploymentMode` sont détaillées comme suit :

- `InstallAndUpdate` : le plug-in peut être installé et mis à jour avec la nouvelle version.
- `Update` : seule la mise à jour doit être autorisée, aucune nouvelle installation.
- `None` : aucune action n'est requise pour ce plug-in.

Authentification unique pour accéder à Citrix Secure Access à l'aide de l'application Citrix Workspace

Vous pouvez utiliser l'authentification unique pour accéder à Citrix Secure Access si vous êtes déjà connecté à l'application Citrix Workspace. Lorsque vous vous connectez à l'application Citrix Workspace et que vous ouvrez Citrix Secure Access, vous n'êtes pas invité à vous authentifier en saisissant les informations d'identification. L'authentification est automatiquement établie. Cette fonctionnalité offre aux utilisateurs une expérience fluide en autorisant l'authentification unique pour différentes applications Citrix. Cette fonctionnalité n'est disponible que pour les clients de magasins dans le cloud. Outre la dernière version de l'application Citrix Workspace, vous devez disposer d'une version compatible de Citrix Secure Access (versions 22.12.2 et ultérieures).

Numérisation rapide

Technical Preview de la
version 2304

[Formulaire d'activation](#)

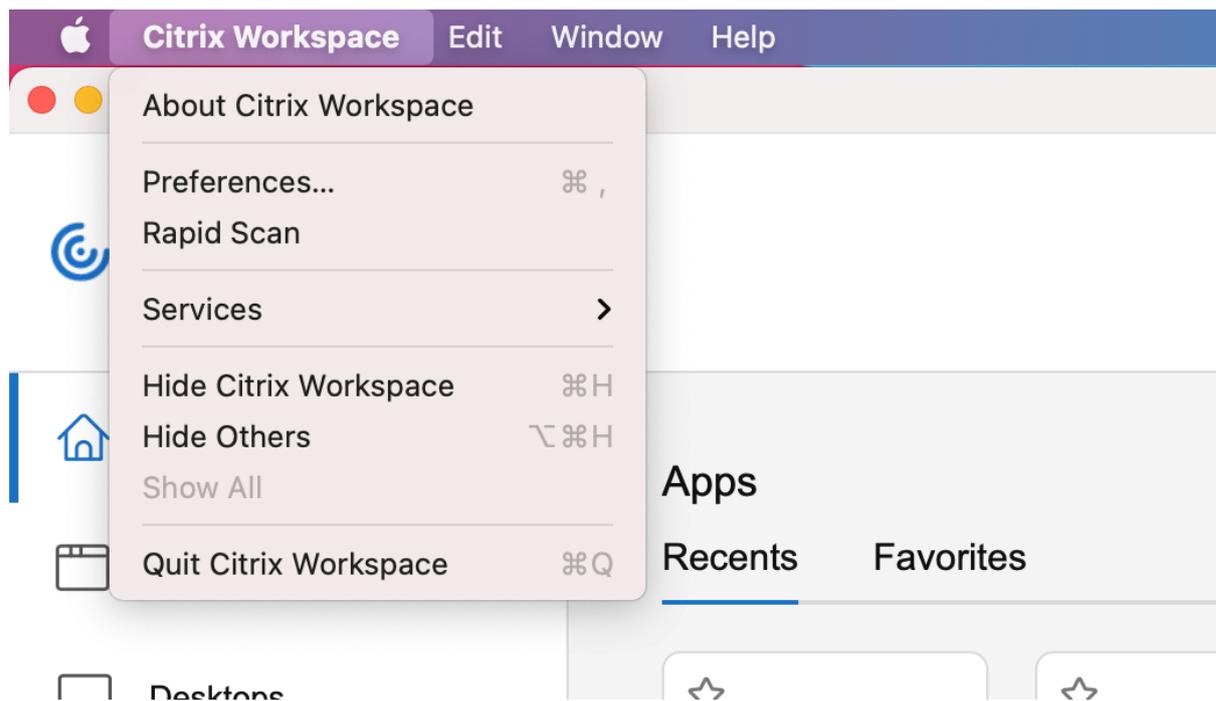
[Formulaire de commentaires](#)

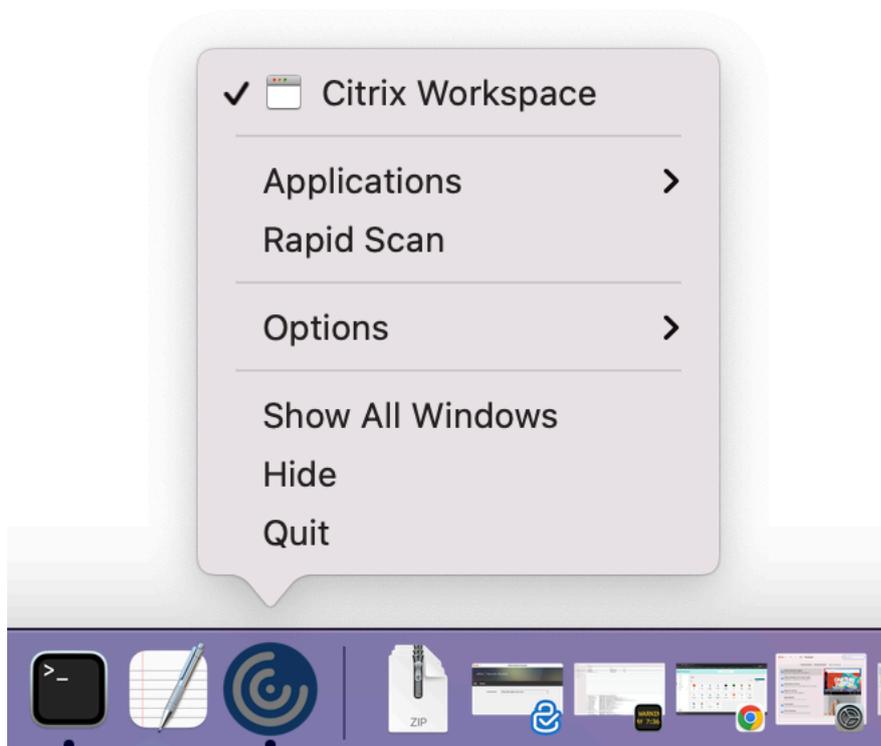
Si vous êtes connecté à l'application Citrix Workspace sur plusieurs appareils, vous pouvez utiliser la fonction de numérisation rapide pour numériser plusieurs documents avec un appareil iOS, puis transférer ces documents numérisés vers un Mac.

Pour obtenir des instructions sur l'utilisation de la fonction Numérisation rapide pour numériser des documents, procédez comme suit :

1. Sur votre Mac, cliquez avec le bouton droit sur l'icône de l'application Citrix Workspace dans votre session de bureau et cliquez sur **Numérisation rapide** pour afficher un code QR.

2. Sur votre appareil iOS, cliquez sur **Réglages > Numérisation rapide**.
3. Scannez le code QR affiché sur votre Mac pour établir la connexion entre votre Mac et les appareils iOS.
4. Numérisez n'importe quel document et envoyez-le sur votre Mac.
5. Dans votre session de bureau sur Mac, vous pouvez localiser les documents que vous avez numérisés dans le Finder.





Logiciels requis

- Le mappage des lecteurs clients (CDM) doit être activé pour le magasin.
- Vous devez être connecté au même compte dans l'application Citrix Workspace sur votre appareil iOS et votre Mac.
- Vous devez être connecté au même réseau Wi-Fi.
- La version minimale requise de l'application Citrix Workspace pour Mac est 2304.
- Cette fonctionnalité est prise en charge sur l'application Citrix Workspace pour iOS à partir de la version 23.3.5.
- La numérisation rapide nécessite un accès en lecture et en écriture sur votre appareil. Pour donner accès, procédez comme suit :
 1. Dans votre profil, cliquez sur **Paramètres de l'application > Paramètres du magasin**.
 2. Cliquez sur votre magasin actuel.
 3. Cliquez sur **Stockage de l'appareil** et sélectionnez **Accès en lecture et en écriture**.

Version améliorée de WebRTC pour Microsoft Teams optimisé

Technical Preview de la
version 2210

[Formulaire d'activation](#)

[Formulaire de commentaires](#)

À partir de la version 2210, la version de WebRTC utilisée pour Microsoft Teams optimisé a été mise à niveau vers la version M98.

Prise en charge d'une expérience d'authentification unique (SSO) améliorée pour les applications Web et SaaS

Technical Preview de la
version 2203.1

[Formulaire d'activation](#)

[Formulaire de commentaires](#)

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 authentifier l'application Citrix Workspace et l'application Web ou SaaS spécifique lancée depuis l'application Citrix Workspace.

De la version préliminaire (version Technical Preview) à la disponibilité générale (GA)

Service ou fonctionnalité	Version en disponibilité générale
Support pour le décodage vidéo H.265	2402
Réducteur HDX mis à niveau vers la version 4	2402
Mode de tolérance de pertes pour l'audio	2402
Prise en charge de la synchronisation du volume audio	2402
Prise en charge du flou d'arrière-plan pour la webcam	2402
Prise en charge du partage d'écran lorsque App Protection est activée	2402

Service ou fonctionnalité	Version en disponibilité générale
Prise en charge de l'authentification à l'aide de FIDO2 lors de la connexion à des magasins locaux	2311
Expérience de lancement d'applications et de bureaux virtuels améliorée pour Workspace (utilisateurs cloud uniquement)	2311
Performances graphiques améliorées	2308
Augmentation du nombre de canaux virtuels pris en charge	2308

Prise en charge native de Mac avec la puce Apple (M1 et M2)

February 2, 2024

Prise en charge native de Mac avec la puce Apple (M1 et M2) - Architecture universelle

Avec la publication de la version Architecture universelle, l'application Citrix Workspace fournit désormais un support natif pour les Mac équipés de la puce Apple (séries M1 et M2). La version Architecture universelle peut s'exécuter sur n'importe quel appareil Mac, quelle que soit l'architecture de son processeur.

Si vous utilisez la version d'architecture basée sur Intel x86_64 de l'application Citrix Workspace pour Mac avec la puce Apple (séries M1 et M2), vous devez utiliser l'émulation Rosetta pour exécuter l'application.

Vous pouvez télécharger la dernière version Architecture universelle et la version d'architecture basée sur Intel x86_64 à partir de [Téléchargements](#).

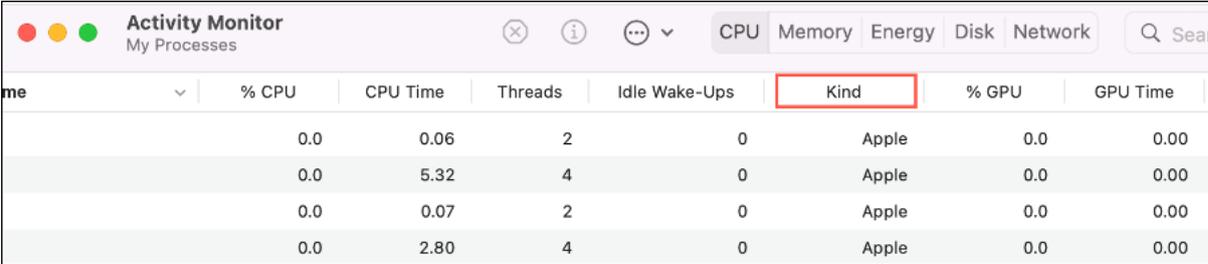
Remarque :

Citrix abandonnera bientôt la version d'architecture basée sur Intel x86_64 mais continuera de prendre en charge la version Architecture universelle pour les Mac dotés d'un processeur Intel et les Mac dotés de la puce Apple (séries M1 et M2). 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 et M2), vous devez mettre à niveau le HDX RealTime Optimization Pack (RTOP). Vous pouvez effectuer la mise à

jour en installant HDX RealTime Media Engine 2.9.500 pour Mac à partir du site Web de Citrix sous [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.



me	% CPU	CPU Time	Threads	Idle Wake-Ups	Kind	% GPU	GPU Time
	0.0	0.06	2	0	Apple	0.0	0.00
	0.0	5.32	4	0	Apple	0.0	0.00
	0.0	0.07	2	0	Apple	0.0	0.00
	0.0	2.80	4	0	Apple	0.0	0.00

Migration entre les différentes versions de l'application Citrix Workspace

Vous pouvez migrer l'application Citrix Workspace de la version d'architecture basée sur Intel x86_64 vers la version Architecture universelle et vice versa.

Pour migrer entre les versions, téléchargez la dernière version sur [Téléchargements](#) et effectuez l'installation manuelle. Pour plus d'informations, consultez la section [Installation manuelle](#).

Vous pouvez également migrer entre les versions en utilisant l'interface graphique. Cette option s'applique uniquement aux utilisateurs de Mac équipés de la technologie Apple Silicon (séries M1 et M2). Pour plus d'informations sur la migration à l'aide de l'interface utilisateur graphique, consultez la section [Configurer les mises à jour automatiques Citrix Workspace à l'aide de l'interface utilisateur graphique](#).

Remarque :

La désinstallation de l'application n'est pas requise pour migrer entre les versions.

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 (VD-API) est utilisée avec les fonctions de canal virtuel dans le SDK de l'API Citrix Server (WF-API 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 et M2)

En tant qu'utilisateur final, vous pouvez charger le SDK de canal virtuel personnalisé (VCSDK) sur un Mac doté de la puce M1 et M2. Avec une architecture universelle, vous devez charger le VCSDK en recompilant vos canaux virtuels personnalisés à l'aide du dernier VCSDK sur un appareil à puce M1 et M2. Vous pouvez télécharger la version architecture universelle à partir de la section **Virtual Channel SDK 2204 for macOS (Apple silicon) - Universal Architecture** des [téléchargements](#).

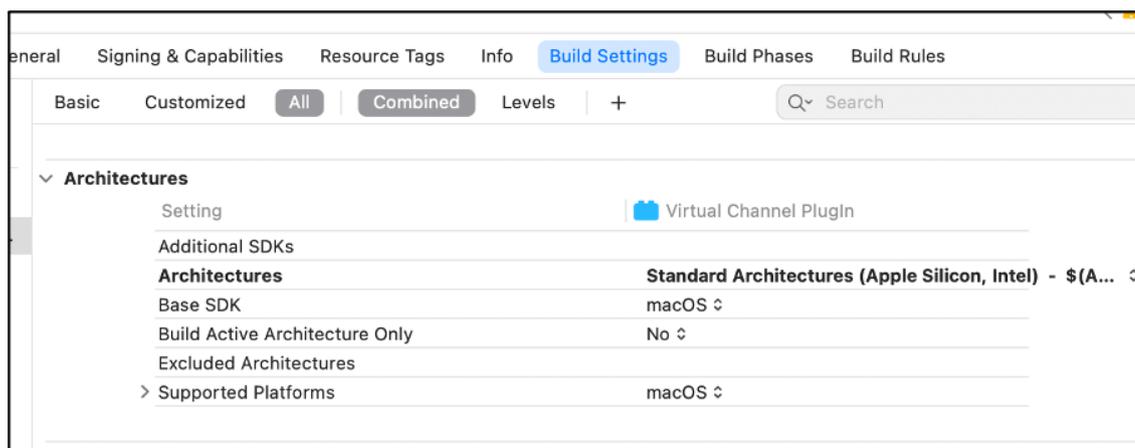
Pour charger le VCSDK, procédez comme suit :

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.

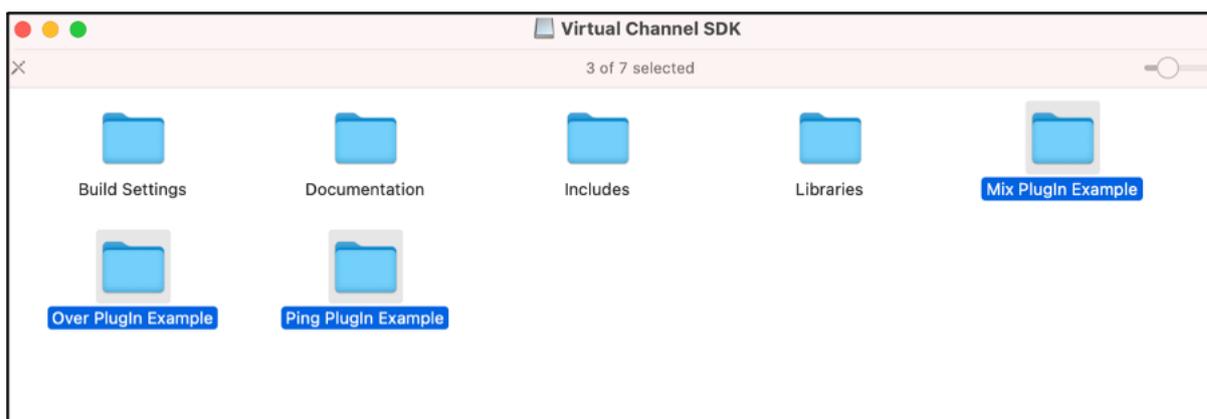
Tester votre kit de développement logiciel de canal virtuel (VCSDK)

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.



SDK du canal virtuel Citrix modernisé pour l'application Citrix Workspace pour Mac

À compter de la version 2311, le VCSDK du canal virtuel Citrix prend en charge l'écriture d'applications du côté serveur et de pilotes 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. Cette version du SDK prend en charge l'écriture de nouveaux canaux virtuels et le partage d'écran pour l'application Citrix Workspace pour Mac.

Pour plus d'informations, consultez la section [SDK du canal virtuel Citrix pour l'application Citrix Workspace pour Mac](#) dans la documentation du développeur.

Augmentation du nombre de canaux virtuels pris en charge

Auparavant, l'application Citrix Workspace pour Mac prenait en charge jusqu'à 32 canaux virtuels. À partir de la version 2308, vous pouvez utiliser jusqu'à 64 canaux virtuels dans une session.

Configuration système requise et compatibilité

May 16, 2024

Systèmes d'exploitation pris en charge

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

- macOS Sonoma 14.4.1
- macOS Ventura 13
- macOS Monterey 12
- macOS Big Sur 11

À tout moment, Citrix prend uniquement en charge les systèmes d'exploitation macOS les plus récents et les deux précédents (N, N-1 et N-2).

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
- ICA-over-DTLS

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

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.

Certificats privés (auto-signés) Si un certificat privé est installé sur la passerelle distante, vous devez installer le certificat racine pour l'autorité de certification de l'organisation 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 aucun des certificats n'est approuvé, 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 le certificat « 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 avec signature croisée et le certificat racine ont le même nom d'objet (délivré à), mais le certificat intermédiaire avec signature croisée a un nom d'émetteur différent (émis par). Cette différence au niveau du nom 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 :

Activer le trafic vers les URL suivantes

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- [Firehose.launchdarkly.com](https://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 défini sur **OFF** :

- Service LaunchDarkly.
- Service d'écoute APNs

Possibilité de désactiver le service LaunchDarkly via l'outil MDM À partir de la version 2210, vous pouvez désactiver le service LaunchDarkly sur l'application Citrix Workspace, que ses utilisateurs se trouvent à l'intérieur ou à l'extérieur du pare-feu de l'organisation. Pour désactiver le service LaunchDarkly, définissez la valeur du paramètre **DisableFeatureFlag** sur True.

Ce service est disponible pour les administrateurs qui gèrent des appareils Mac à l'aide de l'outil MDM.

Remarque :

La désactivation du FeatureFlag nécessite que l'administrateur redémarre l'appareil pour que ce paramètre prenne effet.

Pour plus d'informations sur l'utilisation de MDM, consultez la page [Gestion des appareils mobiles](#).

Installer, désinstaller et mettre à niveau

June 26, 2024

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 **Continuer**.
4. Sur la page **License**, cliquez sur **Continuer**.
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.

Utilisation de la commande du terminal

Vous pouvez installer l'application Citrix Workspace pour Mac en utilisant les commandes du terminal.

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 de la page [Téléchargements](#).
2. Ouvrez le fichier `CitrixWorkspaceApp.dmg` téléchargé.
3. Faites glisser le fichier `Install Citrix Workspace.pkg` dans le dossier.
4. Ouvrez l'application du terminal.
5. Exécutez la commande suivante dans le terminal :

```
1 sudo installer -pkg <path_to_package>/<package_name>.pkg -target /  
2 <!--NeedCopy-->
```

6. Entrez le mot de passe de l'administrateur, si vous y êtes invité.
7. Une fois la commande exécutée, l'application Citrix Workspace est correctement installée.

Désinstallation

Utilisation de la poubelle

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.
Pour fermer l'application Citrix Workspace, appliquez l'une des méthodes suivantes :
 - Dans la barre de menu, cliquez sur **Citrix Workspace**, puis sur **Quittez Citrix Workspace**,
 - Dans le dock, cliquez avec le bouton droit de la souris sur l'application Citrix Workspace et sélectionnez **Quitter** dans les options,
 - Appuyez sur les touches **Command-Q**, ou
 - Dans le menu Accès rapide, cliquez sur l'icône **Compte**, puis sur **Quitter**.

Remarque :

Si vous ne fermez pas l'application Citrix Workspace conformément aux instructions précédentes, le message d'erreur suivant peut s'afficher après avoir effectué l'étape suivante :

L'élément « Citrix Workspace » ne peut pas être déplacé dans la corbeille car il est ouvert.

2. Faites glisser l'application Citrix Workspace du dossier **Application** 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.

Utilisation du fichier .dmg

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.

Utilisation de la commande du terminal

Vous pouvez désinstaller l'application Citrix Workspace pour Mac en utilisant les commandes du terminal.

Pour désinstaller l'application Citrix Workspace pour Mac :

1. Ouvrez l'application du terminal.
2. Exécutez la commande suivante dans le terminal :

```
1 sudo /Library/Application\ Support/Citrix\ Receiver/Uninstall\  
   Citrix\ Workspace.app/Contents/MacOS/Uninstall\ Citrix\  
   Workspace --nogui  
2 <!--NeedCopy-->
```

3. Une fois la commande exécutée, l'application Citrix Workspace et tous ses fichiers système sont supprimés de votre appareil.

Mettre 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

April 17, 2024

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.

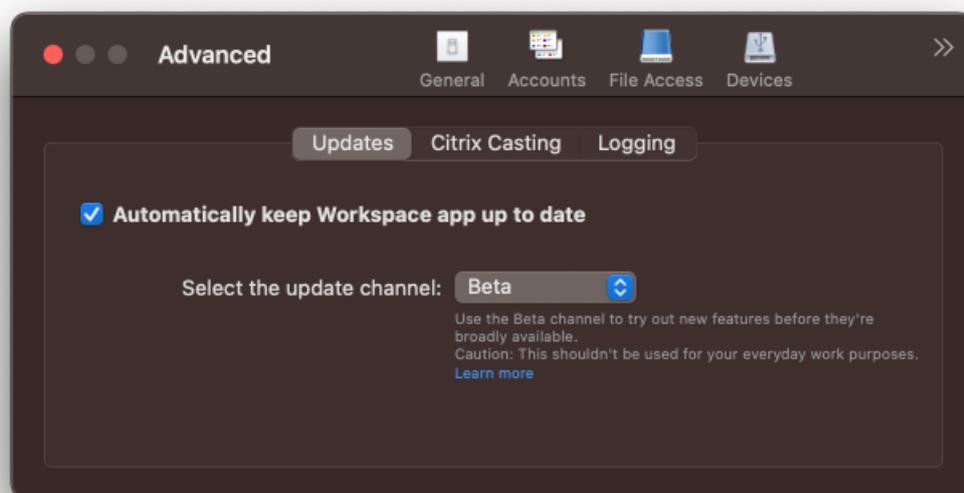
Remarque :

- Si vous avez configuré un proxy de sortie d'interception SSL, vous devez ajouter une exception pour le serveur de mise à jour automatique Workspace <https://downloadplugins.citrix.com/> afin de recevoir les mises à jour de Citrix.
- La mise à jour automatique n'est pas disponible pour les versions de l'application Citrix Workspace antérieures à 2301.1. Pour obtenir davantage d'informations, veuillez consulter l'article [CTX491310](#) du centre de connaissances.
- 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

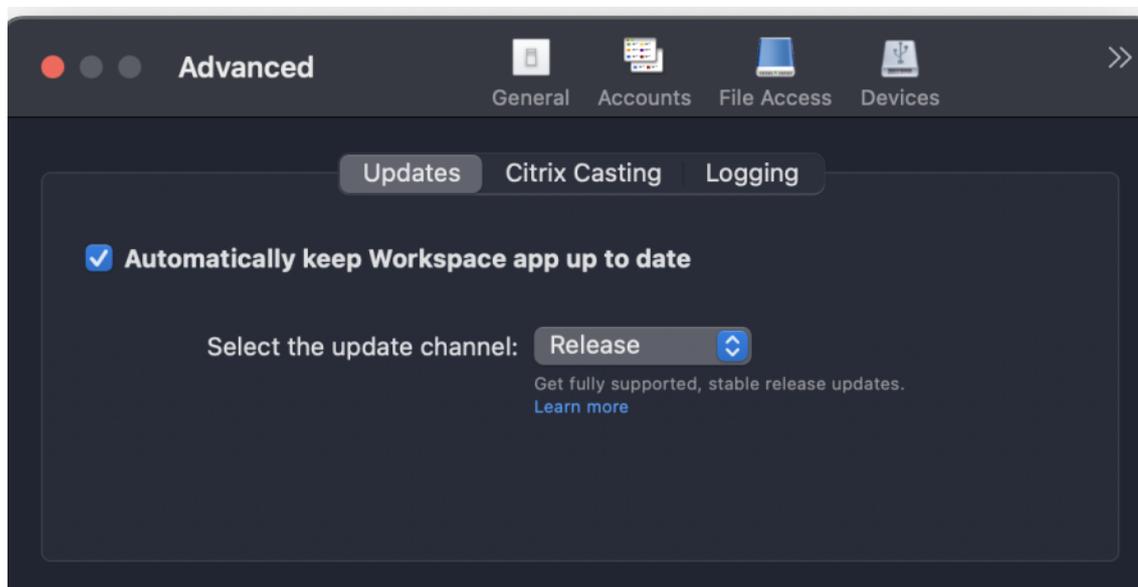
Vous recevez une notification de mise à jour lorsque l'application Citrix Workspace est configurée pour les mises à jour automatiques. Pour installer la version Bêta sur votre système, effectuez les étapes suivantes :

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.

Contrôle de la version à mise à jour automatique

Les administrateurs peuvent désormais gérer la version de mise à jour automatique de l'application Citrix Workspace pour les appareils de l'organisation.

Les administrateurs peuvent contrôler la version en définissant la plage dans les propriétés `maximumAllowedVersion` et `minimumAllowedVersion` dans Global App Configuration Service.

Exemple de fichier JSON dans Global App Configuration Service :

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://serviceURL:443"
6   }
7 ,
8   "settings": {
9
10    "name": "Version Control for Citrix Workspace",
11    "description": "Provides admin ability to Version Control for
12      Citrix Workspace",
13    "useForAppConfig": true,
14    "appSettings": {
15
16      "macos": [
17
18        {
19          "category": "AutoUpdate",
20          "userOverride": false,
21          "assignedTo": [
22            "AllUsersNoAuthentication"
23          ],
24          "settings": [
25
26            {
27              "name": "Auto update plugins settings",
28              "value": [
29
30                {
31                  "pluginName": "Citrix Workspace",
32                  "pluginId": "D99C3E77-FBF5-4B97-8EDA-4E381A1E0826",
33                  "pluginSettings": {
34
35                    "deploymentMode": "Update",
```

```
35         "upgradeToLatest": false,
36         "minimumAllowedVersion": "23.07.0.63",
37         "maximumAllowedVersion": "23.07.0.63",
38         "delayGroup": "Medium",
39         "detectRule": ""
40     }
41 }
42 }
43 ]
44 }
45 }
46 ]
47 }
48 }
49 ]
50 }
51 }
52 ]
53 }
54 ]
55 }
56 ]
57 }
58 <!--NeedCopy-->
```

Lorsque la plage est définie, l'application Citrix Workspace sur l'appareil de l'utilisateur est automatiquement mise à jour vers la version la plus élevée disponible se trouvant dans la plage spécifiée.

Si vous souhaitez mettre à jour automatiquement l'application Citrix Workspace vers une version spécifique, entrez la même version dans les propriétés `maximumAllowedVersion` et `minimumAllowedVersion` de Global App Configuration Service.

Remarque :

- Pour activer le contrôle de la version de mise à jour automatique, le paramètre **upgradeToLatest** de Global App Configuration Service doit être défini sur `false`. Si **upgradeToLatest** est défini sur `true`, les paramètres `maximumAllowedVersion` et `minimumAllowedVersion` seront ignorés.
- Ne modifiez pas la valeur de `pluginID`. L'élément `pluginID` est mappé à l'application Citrix Workspace.
- Si l'administrateur n'a pas configuré la version dans Global App Configuration Service, l'application Citrix Workspace est mise à jour vers la dernière version disponible par défaut.
- Vous ne pouvez utiliser que les plages de versions définies pour mettre à jour l'application Citrix Workspace. Toutefois, la rétrogradation n'est pas prise en charge.
- Cette fonctionnalité est prise en charge à partir de la version 2307.

Amélioration apportées à la mise à jour automatique

La fonctionnalité de mise à jour automatique permet de mettre automatiquement à jour l'application Citrix Workspace vers la dernière version sans aucune intervention de l'utilisateur.

L'application Citrix Workspace vérifie et télécharge régulièrement la dernière version disponible de l'application. L'application Citrix Workspace détermine le meilleur moment pour l'installation en fonction de l'activité des utilisateurs afin de ne pas provoquer d'interruptions.

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

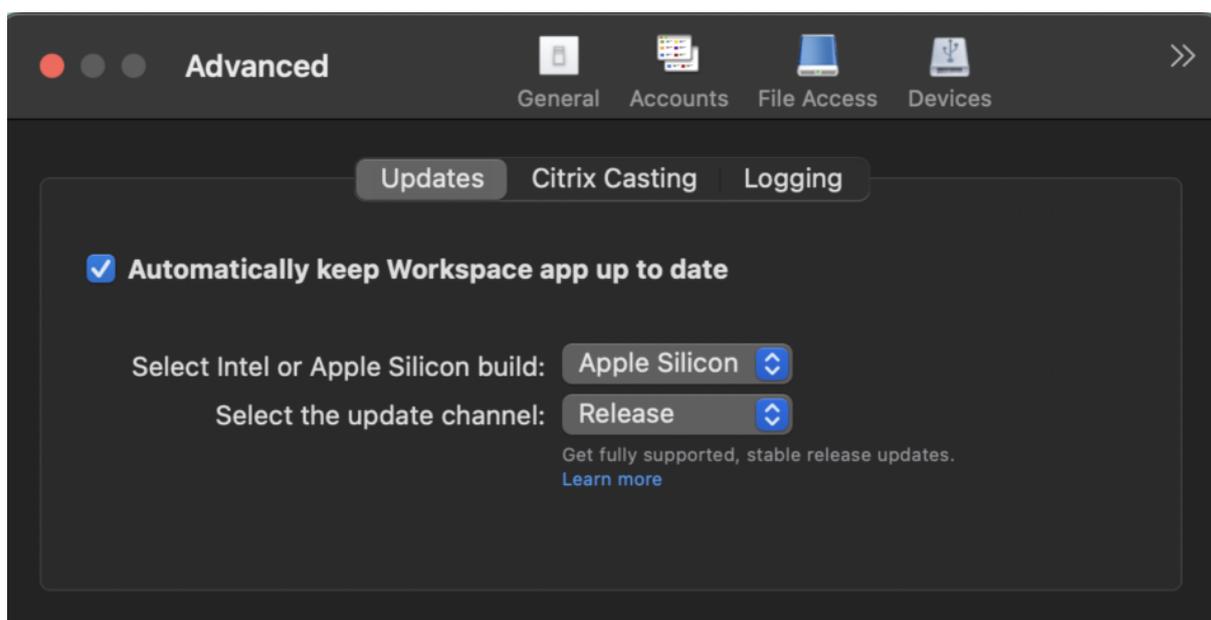
Vous pouvez configurer les mises à jour de Citrix Workspace à l'aide des méthodes suivantes :

- Interface utilisateur graphique (GUI)
- Global App Configuration Service (GACS)
- Gestion des appareils mobiles (MDM)
- StoreFront

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

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 > Mises à jour**.
3. Sélectionnez la version pour laquelle vous souhaitez installer les mises à jour automatiques. Il peut s'agir de la version puce Apple ou la version Intel (applicable uniquement aux utilisateurs de Mac équipés de processeurs avec puce Apple, série M1).



Configurer les mises à jour automatiques 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).

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

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

```

1 <properties>
2     <clear/>
3 </properties>
4 <!--NeedCopy-->

```

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

```

1 <account>
2
3     <clear />
4
5     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
6         F84Store"
7         description="" published="true" updaterType="Citrix"
8             remoteAccessType="None">
9     <annotatedServices>
10

```

```
11     <clear />
12
13     <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
14
15         <metadata>
16
17             <plugins>
18
19                 <clear />
20
21             </plugins>
22
23             <trustSettings>
24
25                 <clear />
26
27             </trustSettings>
28
29             <properties>
30
31                 <property name="Auto-Update-Check" value="Disabled"
32                     />
33
34                 <property name="Auto-Update-DeferUpdate-Count" value
35                     ="1" />
36
37                 <property name="Auto-Update-Rollout-Priority" value=
38                     "fast" />
39
40                 <property name="Auto-Update-Architecture" value="
41                     Universal" or "Intel" />
42
43             </properties>
44
45         </metadata>
46
47     </annotatedServiceRecord>
48
49 </annotatedServices>
50
51 <metadata>
52
53     <plugins>
54
55         <clear />
56
57     </plugins>
58
59     <trustSettings>
60
61         <clear />
62
63     </trustSettings>
```

```
60
61     <properties>
62
63     <clear />
64
65     </properties>
66
67 </metadata>
68
69 </account>
70
71 <!--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 (défaut) : recherche et effectue les mises à jour automatiquement.
 - Manuel : les mises à jour ne sont récupérées que lorsque l'utilisateur effectue une demande de vérification depuis le menu de la barre d'état système de l'application Citrix Workspace.
 - Désactivé : aucune recherche de mises à jour n'est effectuée.
- **Auto-Update-Rollout-Priority** : indique la période de mise à disposition pendant laquelle vous pouvez recevoir la mise à jour.
 - Rapide : les mises à jour sont déployées au début de la période de mise à disposition.
 - Moyen : les mises à jour sont déployées vers le milieu de la période de mise à disposition.
 - Lent : les mises à jour sont déployées à la fin de la période de mise à disposition.
- **Auto-Update-DeferUpdate-Count** : indique le nombre de fois que vous pouvez reporter les notifications de mises à jour de la version.

Remarque :

Cette configuration s'applique uniquement aux mises à jour interactives et non lorsque la fonction de mise à jour automatique silencieuse est activée, car l'utilisateur n'a aucune option pour différer les mises à jour.

- -1 : l'utilisateur peut différer les mises à jour autant de fois qu'il le souhaite.
- 0 : l'utilisateur ne voit pas l'option de rappel.
- Nombre : l'utilisateur voit les options de rappel accompagnées d'un nombre.

Configurer les mises à jour automatiques de Citrix Workspace à l'aide de GACS

Les administrateurs peuvent utiliser GACS pour configurer les mises à jour automatiques de la version puce Apple ou Intel en utilisant les paramètres suivants :

“name”:“**autoUpdateArchitecture**”

“value”:“**Universal**”ou “**Intel**”

Configurer les mises à jour automatiques de Citrix Workspace à l'aide de MDM

Les administrateurs peuvent utiliser la gestion MDM pour configurer les mises à jour automatiques de la version puce Apple ou Intel en utilisant les paramètres suivants :

<key>AutoUpdateArchitecture</key>

<string>Universal</string> or <string>Intel</string>

<key>AutoUpdateState</key>

<string>Auto</string> or <string>Manual</string> or <string>Disabled</string>

Pour plus d'informations sur l'utilisation de MDM, consultez la page [Gestion des appareils mobiles](#).

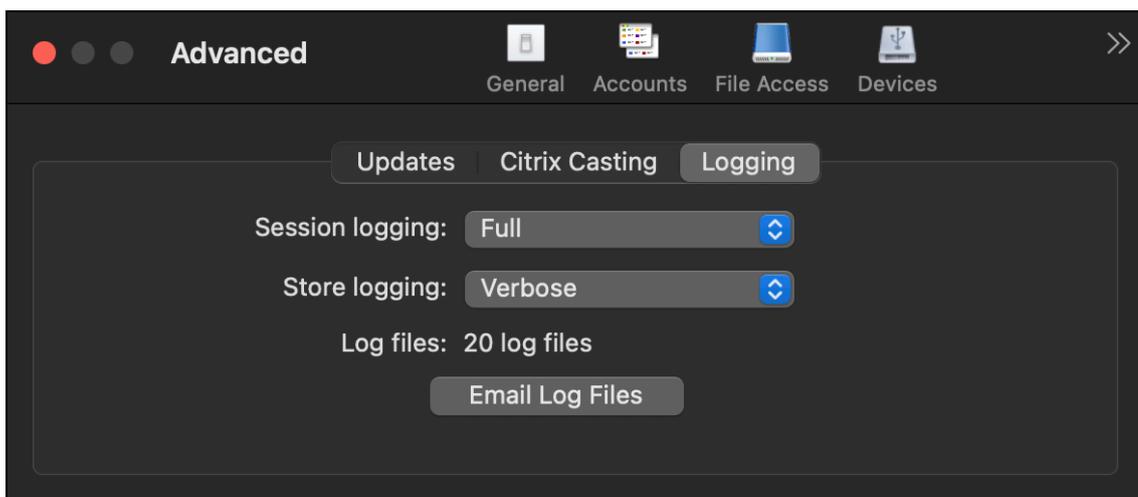
Collecte de journaux

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 minimaux 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 minimaux 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.

Architecture universelle améliorée conçue pour les sessions d'application et de bureau virtuels

À partir de la version 2311, la version Architecture universelle peut désormais choisir automatiquement d'exécuter les sessions virtuelles en mode Apple Silicon natif ou en mode Intel. Elle utilise l'émulation Rosetta pour lancer la session virtuelle en mode Intel. La session virtuelle est lancée en mode Apple Silicon natif, si le SDK de canal virtuel est créé sur la base de l'architecture Apple Silicon native ou s'il n'existe aucun SDK de canal virtuel. Cependant, la session virtuelle est lancée en mode Intel à l'aide de l'émulation Rosetta, si le SDK du canal virtuel est créé sur la base de l'architecture Intel x86_64.

Cette amélioration de la version Architecture universelle optimise l'expérience de lancement sur les Mac équipés du chipset Apple Silicon. Pour les utilisateurs de Mac équipés d'un chipset Intel, il n'y a aucun changement, et la version Architecture universelle continue d'exécuter les sessions virtuelles de manière native.

Configurer l'application Citrix Workspace

June 26, 2024

Vous pouvez configurer l'application Citrix Workspace pour Mac à l'aide de l'interface utilisateur de Global App Configuration Service et de la gestion d'appareils mobiles. Les paramètres peuvent être configurés pour les environnements cloud (Citrix Workspace) et locaux (Citrix StoreFront).

Pour plus d'informations, consultez les rubriques suivantes :

- [Service Global App Configuration](#)
 - [Configurer les paramètres des magasins cloud](#)
 - [Configurer les paramètres des magasins locaux](#)
- [Gestion des appareils mobiles](#)

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. Pour plus d'informations, consultez la section [USB](#).

Synchronisation de la disposition du clavier

La synchronisation de la disposition du clavier vous permet de basculer entre leurs dispositions de clavier préférées sur la machine cliente. Cette fonction est désactivée par défaut. Une fois que vous avez activé cette fonctionnalité, la disposition du clavier client se synchronise automatiquement avec la session d'applications et de bureaux virtuels. Pour plus d'informations, consultez la section [Synchro-nisation de la disposition du clavier](#).

Prise en charge des canaux de Global App Configuration Service

Global App Configuration Service pour Citrix Workspace permet à un administrateur Citrix de fournir les URL du service Workspace et les paramètres de l'application Workspace via un service géré de manière centralisée. Global App Configuration Service permet désormais aux administrateurs de tester les paramètres avant de les déployer pour tous les utilisateurs. Cette fonctionnalité permet de résoudre tous les problèmes avant d'appliquer les configurations d'application globales à l'ensemble de la base d'utilisateurs.

Vous pouvez bénéficier de la prise en charge des canaux en mappant les paramètres que vous souhaitez tester à un canal, puis en ajoutant le canal à la charge utile. Pour en savoir plus, consultez la [documentation du service Global App Configuration](#).

Gestion des appareils mobiles

April 17, 2024

L'application Citrix Workspace prend désormais en charge la gestion des appareils mobiles (MDM), qui permet aux administrateurs de configurer, de sécuriser et de prendre en charge l'application Citrix Workspace pour Mac en appliquant des stratégies via n'importe quel outil MDM.

Installation et désinstallation de l'application Citrix Workspace via le MDM

Vous pouvez utiliser les commandes du terminal pour installer et désinstaller l'application Citrix Workspace via le MDM. Pour plus d'informations sur l'utilisation des commandes du terminal pour l'installation et la désinstallation, consultez la section [Installation](#) et [désinstallation manuelles](#).

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 de la page [Téléchargements](#).

2. Ouvrez le fichier `CitrixWorkspaceApp.dmg` téléchargé.
3. Faites glisser le fichier `Install Citrix Workspace.pkg` dans le dossier.
4. Utilisez la commande de terminal suivante pour installer le package via le MDM :

```
1 sudo installer -pkg /Volumes/Citrix\ Workspace/Install\ Citrix\
  Workspace.pkg -target /
2 <!--NeedCopy-->
```

Pour désinstaller l'application Citrix Workspace :

Vous pouvez utiliser la commande de terminal suivante pour désinstaller l'application Citrix Workspace via le MDM :

```
1 sudo /Library/Application\ Support/Citrix\ Receiver/Uninstall\ Citrix
  \ Workspace.app/Contents/MacOS/Uninstall\ Citrix\ Workspace --
  nogui
2 <!--NeedCopy-->
```

Paramètres pris en charge sur MDM

Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut	Version prise en charge
Activer/désactiver l'authentification FIDO2 pour une session HDX	Permet aux administrateurs d'activer ou de désactiver l'authentification FIDO2 au sein d'une session HDX.	Fido2Enabled	true/false	Booléen	true	2307
Menu d'accès rapide pour StoreFront	Permet aux administrateurs d'activer ou de désactiver le menu d' accès rapide pour les magasins locaux.	ShowQuickAccessForStoreFront	true/false	Booléen	false	2307

Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut	Version prise en charge
Auto update – AutoUpdateState	Met automatiquement à jour l'application Citrix Workspace vers la dernière version sans aucune intervention de l'utilisateur.	AutoUpdateState	Auto/Manual/Disabled	Énuméré	Auto	2305
Enable Azure Active Directory	Permet aux administrateurs de configurer et d'appliquer des stratégies d'accès conditionnel Azure Active Directory pour les utilisateurs qui s'authentifient à l'application Citrix Workspace.	enableAAD	true/false	Booléen	False	2305

Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut	Version prise en charge
Démarrage automatique de l'application Citrix Workspace	Contrôle l'application Citrix Workspace pour Mac afin qu'elle démarre automatiquement chaque fois qu'un ordinateur est allumé par un utilisateur.	AutoLaunchAppOnFirstStart	True	Booléen	True	2304
Pre-configuration of Store URL	Permet aux administrateurs de préconfigurer et d'ajouter les détails du magasin à l'application Workspace afin que les utilisateurs n'aient pas à le faire.	StoreURLs	<Store URL>	Chaîne	S/O	2210

Paramètre	Description	Clé	Valeur	Type de valeur	Valeur par défaut	Version prise en charge
Block new Store addition by end-user	Empêche l'utilisateur d'ajouter un magasin dans l'application Workspace sur ses terminaux.	BlockStoreAddition	false	Booléen	False	2210
Show/Hide menu bar	Affiche ou masque le menu Citrix Workspace dans la barre de menu Mac.	ShowHelperInMenuBar	True	Booléen	True	2208.1
Auto update - AutoUpdateChannel	Permet aux administrateurs de s'assurer qu'une application Citrix Workspace reçoit des mises à jour GA ou des mises à jour Bêta lorsque la mise à jour automatique est activée.	AutoUpdateChannel	PROD/EAR	Chaîne	PROD	2201

Schéma de référence

```
1 <array>
2     <dict>
3         <key>ShowHelperInMenuBar</key>
4         <true/>
5         <key>AutoLaunchAppOnRestart</key>
6         <true/>
7         <key>StoreURLs</key>
8         <array>
9             <string>PROVIDE STORE URL HERE</string>
10        </array>
11        <key>BlockStoreAddition</key>
12        <false/>
13        <key>CEIPEnabled</key>
14        <true/>
15        <key>AutoUpdateArchitecture</key> `
16        <string>Universal</string>
17        <key>AutoUpdateState</key>
18        <string>Enable</string>
19        <key>AutoUpdateChannel</key>
20        <string>PROD</string>
21        <key>PayloadDisplayName</key>
22        <string>Citrix Workspace</string>
23        <key>PayloadIdentifier</key>
24        <string>com.citrix.receiver.nomas</string>
25        <key>PayloadType</key>
26        <string>com.citrix.receiver.nomas</string>
27        <key>PayloadUUID</key>
28        <string>3BE38AD3-7D95-423F-BD7B-8A4D1F5208EF</string>
29        <key>PayloadVersion</key>
30        <integer>1</integer>
31        <key>WebBrowserForAuthentication</key>
32        <string>System</string>
33        <key>Fido2Enabled</key>
34        <false/>
35        <key>ShowQuickAccessForStoreFront</key>
36        <true/>
37    </dict>
38 </array>
39
40 <!--NeedCopy-->
```

Configuration du magasin

May 16, 2024

Prise en charge de la configuration de magasin des machines utilisateur via l'outil MDM

Les administrateurs peuvent désormais configurer les paramètres suivants lors du déploiement de l'application Citrix Workspace via n'importe quel outil de déploiement MDM tel que Citrix Endpoint Management :

- **StoreURLs** : configurez les détails du magasin afin qu'ils soient ajoutés automatiquement lorsque l'utilisateur ouvre l'application Citrix Workspace, simplifiant ainsi l'expérience de connexion.

Pour ajouter un magasin, fournissez les détails du paramètre **StoreURLs**. Par exemple :

```
<array>  
<string>https://myorg.com/?storename</string>  
</array>
```

Vous pouvez également ajouter plusieurs magasins comme suit :

```
<array>  
<string>https://myorg.com/?storename1</string>  
<string>https://myorg.com/?storename2</string>  
</array>
```

Pour ajouter les URL des magasins à l'application Citrix Workspace, l'utilisateur doit quitter et relancer l'application Citrix Workspace.

- **BlockStoreAddition** : empêche l'utilisateur d'ajouter des magasins.

Pour empêcher l'utilisateur d'ajouter un magasin, définissez la valeur du paramètre **BlockStoreAddition** sur **True**.

Pour plus d'informations, consultez la section [Gestion des appareils mobiles](#).

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.

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 Configuration 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 Configuration Service.

Pour activer cette fonctionnalité, effectuez les opérations suivantes :

1. Configurez le mappage de StoreFront vers Workspace à l'aide de Global App Configuration Service. Pour plus d'informations, consultez [Global App Configuration Service](#).
2. Modifiez la charge utile dans Global App Configuration 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**.

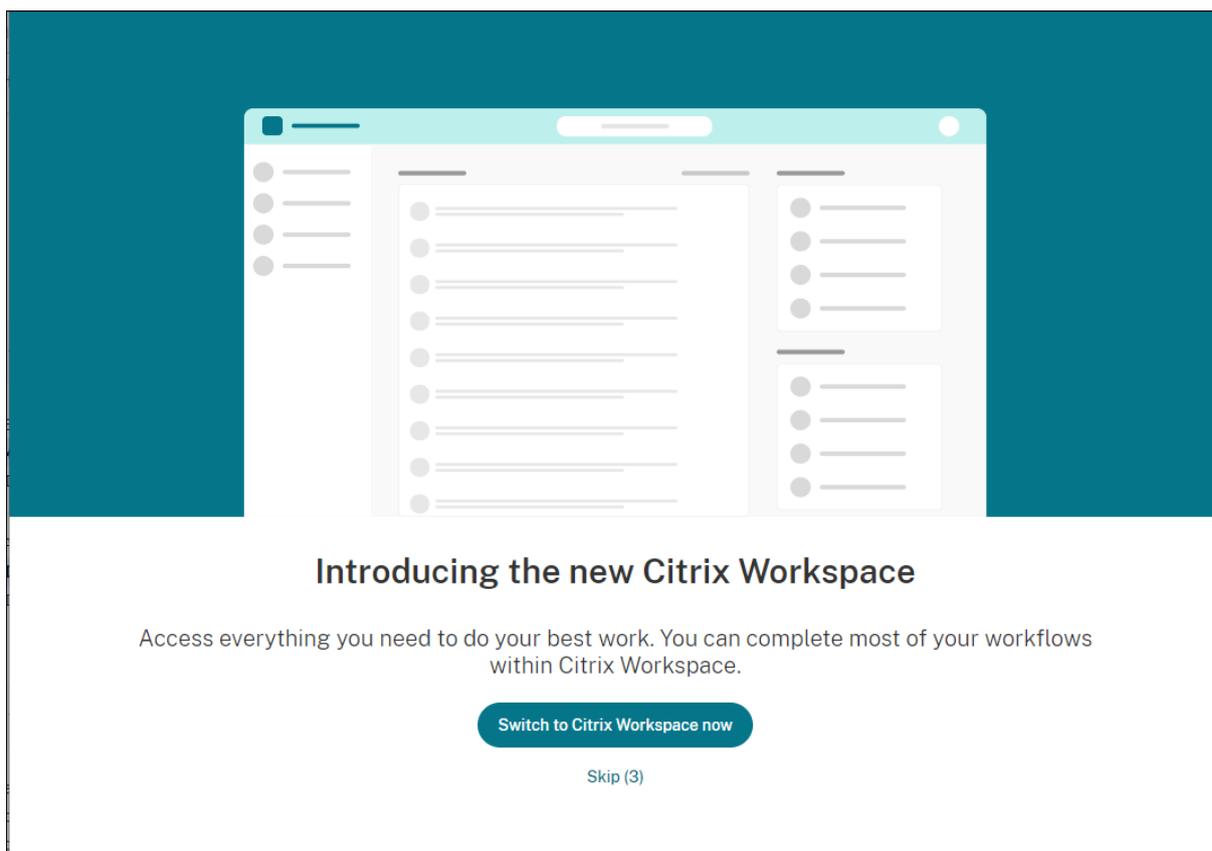
Si vous modifiez la configuration de la charge utile existante, utilisez **PUT** et assurez-vous que vous disposez de la charge utile comprenant tous les paramètres pris en charge.

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 Configuration 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.

Magasin Web personnalisé

Prise en charge des magasins Web personnalisés

À partir de la version 2112, vous pouvez 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. 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.

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 App Protection 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 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 **-**.

Prise en charge des URL personnalisées grâce aux redirections 301

À partir de la version 2106, vous pouvez ajouter des URL qui redirigent vers Citrix Workspace à partir de StoreFront ou de 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 la version 2106, 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.

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

À partir de la version 2109, vous pouvez 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.

Déconnexion du magasin Web personnalisé lorsque vous fermez l'application Citrix Workspace

Lorsque le paramètre **signoutCustomWebstoreOnExit** est défini sur **True**, la fermeture de la fenêtre de l'application Citrix Workspace vous déconnecte du magasin Web personnalisé. Lorsque vous rouvrez l'application Citrix Workspace, l'URL du magasin Web est à nouveau chargée. Vous pouvez configurer le paramètre **signoutCustomWebstoreOnExit** dans Global App Configuration Service.

Sécurité et authentification

February 2, 2024

Cette section décrit les fonctionnalités de sécurité et les détails d'authentification de l'application Citrix Workspace pour Mac.

- [Authentification](#)
- [Sécurité](#)
- [Sécuriser les communications](#)

Authentification

February 2, 2024

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 Store-Front 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 que vous souhaitez ne figure pas dans la liste.
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.

User-Agent

L'application Citrix Workspace envoie un user-agent sous forme de requêtes réseau qui peuvent être utilisées pour configurer des stratégies d'authentification, y compris la redirection de l'authentification vers d'autres fournisseurs d'identité (IDP).

Remarque :

Ne mentionnez pas les numéros de version lors de la configuration des stratégies.

Scénario	Description	user-agent
Requêtes HTTP classiques	En général, une requête réseau émise par l'application Citrix Workspace contient un élément user-agent général.	<code>CitrixReceiver /23.05.0.36 MacOSX /13.4.0 com.citrix.receiver.nomas X1Class CWACapable</code>
Magasin cloud	Par exemple, les requêtes réseau suivantes contiennent Lorsque les utilisateurs ajoutent un magasin cloud à l'application Citrix Workspace, GET/AGServices/discover les demandes réseau	<code>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15</code>
Magasin local avec Gateway Advanced Auth	Les requêtes utilisateur effectuées par l'application Citrix Workspace contiennent un élément user-agent avancé configuré sur l'application Gateway auprès de Citrix Workspace, les demandes réseau effectuées par l'application Citrix Workspace contiennent	<code>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko), AppleWebKit/23.05.0.36</code>

Scénario	Description	user-agent
Magasin Web personnalisé	Lorsqu'un utilisateur ajoute l'application Citrix Workspace d'un magasin Web personnalisé, les demandes réseau effectuées par l'application Citrix Workspace contiennent un élément user-agent spécifique.	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Safari CWA/23.05.0.18 MacOSX/13.4.0

FIDO2 pour une authentification sans mot de passe

L'application Citrix Workspace pour Mac prend en charge l'authentification sans mot de passe à l'aide de clés de sécurité FIDO2 lors de la connexion à un magasin cloud ou dans le cadre d'une session HDX. Les clés de sécurité FIDO2 permettent aux employés de l'entreprise de s'authentifier auprès d'applications ou de bureaux prenant en charge FIDO2 sans entrer de nom d'utilisateur ou de mot de passe. Cette fonctionnalité prend actuellement en charge les authentificateurs itinérants (USB uniquement) avec code PIN et Touch ID. Cette fonctionnalité est prise en charge sur macOS 12 et versions ultérieures.

Pour plus d'informations sur FIDO2, consultez [Authentification FIDO2](#).

Pour plus d'informations sur les conditions préalables et l'utilisation de cette fonctionnalité, consultez [Autorisation locale et authentification virtuelle à l'aide de FIDO2](#).

Authentification basée sur FIDO2 lors de la connexion à des magasins cloud et locaux

L'application Citrix Workspace utilise le navigateur par défaut de l'utilisateur pour l'authentification FIDO2 (authentification Web), lors de la connexion aux magasins cloud et locaux. Les administrateurs peuvent configurer le type de navigateur pour s'authentifier auprès de l'application Citrix Workspace. Pour plus d'informations sur les paramètres du navigateur Web, consultez la documentation de [Global App Configuration Service](#).

Les paramètres suivants vous permettent de sélectionner le type de navigateur utilisé pour authentifier un utilisateur final dans l'application Citrix Workspace :

Paramètres	Description
System	Vous permet d'utiliser le navigateur par défaut de l'utilisateur pour l'authentification (par exemple, Safari ou Chrome). L'authentification s'effectue en dehors de l'application Citrix Workspace. Utilisez ce paramètre pour prendre en charge l'authentification sans mot de passe. Ce paramètre essaie d'utiliser la session utilisateur existante depuis le navigateur de l'utilisateur.
SystemWithPrivateSession	Ce paramètre est similaire au paramètre System . L'application Citrix Workspace utilise une session privée dans le navigateur pour l'authentification. Le navigateur n'enregistre pas les cookies ni les données d'authentification. L'authentification unique n'est pas prise en charge dans cette option.
Embedded	Permet l'authentification dans l'application Citrix Workspace. L'application Citrix Workspace enregistre les données de session ou les cookies pour l'authentification unique (par exemple, les applications SaaS) lorsque la fonctionnalité d' authentification unique améliorée est activée. Cette méthode d'authentification ne prend pas en charge les authentifications sans mot de passe telles que FIDO2.
EmbeddedWithPrivateSession	Ce paramètre est similaire au paramètre Embedded . L'authentification unique n'est pas prise en charge car les données de session ou les cookies ne sont pas présents dans l'application Citrix Workspace.

Pour transférer le paramètre configuré, exécutez les commandes suivantes à l'aide de la gestion des appareils mobiles (MDM), du Global App Configuration Service (GACS) ou de l'interface de ligne de commande :

- **Activer FIDO2 via MDM** : Pour activer l'authentification via MDM, les administrateurs doivent utiliser le paramètre suivant :

```
<key>WebBrowserForAuthentication</key><string>System</string>
```

Pour plus d'informations sur l'utilisation de MDM, consultez la page [Gestion des appareils mobiles](#).

- **Activer FIDO2 via GACS** : Pour activer l'authentification via GACS, les administrateurs doivent utiliser le paramètre suivant :

```
1 {
2
3     "serviceURL": {
4
5         "url": "https://serviceURL:443"
6     }
7
8     ,
9     "settings": {
10
11         "name": "Web browser for Authenticating into Citrix Workspace",
12         "description": "Allows admin to select the type of browser used
13             for authenticating an end user into Citrix Workspace app",
14         "useForAppConfig": true,
15         "appSettings": {
16
17             "macos": [
18                 {
19
20                     "assignedTo": [
21                         "AllUsersNoAuthentication"
22                     ],
23                     "category": "authentication",
24                     "settings": [
25                         {
26
27                             "name": "web browser for authentication",
28                             "value": "SystemWithPrivateSession"
29                         }
30                     ]
31                 },
32                 "userOverride": false
33             ]
34         }
35     }
36 }
37
38 }
39
40
41 <!--NeedCopy-->
```

- **Activer FIDO2 à l'aide de l'interface de ligne de commande** : Pour activer l'authentification à l'aide de l'interface de ligne de commande, les administrateurs doivent exécuter la commande

suivante :

```
defaults write com.citrix.receiver.nomas WebBrowserForAuthentication  
System
```

Authentification basée sur FIDO2 au sein d'une session HDX

Vous pouvez configurer des clés de sécurité FIDO2 pour l'authentification au sein d'une session HDX. Cette fonctionnalité prend actuellement en charge les authentificateurs itinérants (USB uniquement) avec code PIN.

Lorsque vous accédez à une application ou à un site Web prenant en charge FIDO2, une invite s'affiche demandant l'accès à la clé de sécurité. Si vous avez préalablement enregistré votre clé de sécurité avec un code PIN (un minimum de 4 et un maximum de 64 caractères), vous devez saisir le code PIN lors de la connexion.

Si vous avez préalablement enregistré votre clé de sécurité sans code PIN, il vous suffit de toucher la clé de sécurité pour vous connecter.

Cette fonctionnalité est activée par défaut pour l'application Citrix Workspace pour la version 2307 et les versions ultérieures. Vous pouvez désactiver l'authentification FIDO2 à l'aide de la méthode de gestion des appareils mobiles (MDM) ou de l'interface de ligne de commande en exécutant les commandes suivantes :

- **Désactiver l'authentification basée sur FIDO2 via MDM :** Pour désactiver cette fonctionnalité via MDM, les administrateurs doivent utiliser le paramètre suivant :

```
<key>Fido2Enabled</key><false/>
```

Pour plus d'informations sur l'utilisation de MDM, consultez la page [Gestion des appareils mobiles](#).

- **Désactiver l'authentification basée sur FIDO2 à l'aide de l'interface de ligne de commande :** Pour désactiver cette fonctionnalité, exécutez la commande suivante dans les méthodes de l'interface de ligne de commande :

```
defaults write com.citrix.receiver.nomas Fido2Enabled -bool NO
```

Authentification basée sur des certificats

À partir de la version 2305, les administrateurs Workspace peuvent configurer et appliquer les stratégies d'accès conditionnel Azure Active Directory pour les utilisateurs qui s'authentifient sur l'application Citrix Workspace.

Les méthodes suivantes peuvent être utilisées pour activer l'authentification à l'aide d'un accès conditionnel :

- Gestion des appareils mobiles (MDM)
- Global App Configuration Service (GACS)

Les valeurs des indicateurs lues par l'application Citrix Workspace sont prioritaires dans l'ordre suivant :

- Gestion des appareils mobiles (MDM)
- Global App Configuration Service (GACS)

Activation de l'authentification par accès conditionnel via MDM

Pour activer l'authentification à l'aide d'un accès conditionnel avec Azure AD via MDM, les administrateurs doivent utiliser le paramètre suivant :

```
<key>enableAAD</key>  
<true/>
```

Ce paramètre prend en charge les valeurs booléennes. La valeur est définie sur false par défaut. La valeur par défaut est prise en compte si la valeur clé n'est pas disponible.

Pour plus d'informations sur l'utilisation de MDM, consultez la page [Gestion des appareils mobiles](#).

Activation de l'authentification par accès conditionnel via GACS

Pour activer l'authentification à l'aide d'un accès conditionnel avec Azure AD via GACS, les administrateurs doivent utiliser le paramètre suivant :

```
enable conditional AAD
```

Pour plus d'informations, accédez à la page [Supported settings and their values per platform](#) pour macOS dans la documentation de Global App Configuration Service (GACS).

Sécurité

May 16, 2024

App Protection

App Protection est une fonctionnalité complémentaire qui offre une sécurité renforcée lors de l'utilisation de Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops)

Service). Cette fonctionnalité limite le risque d'infection par des programmes malveillants d'enregistrement de frappe et de capture d'écran. App Protection empêche l'exfiltration d'informations confidentielles telles que les informations d'identification de l'utilisateur et les informations sensibles affichées à l'écran. Pour plus d'informations, consultez la documentation [App Protection](#).

Clause d'exclusion de responsabilité

Les stratégies App Protection filtrent l'accès aux fonctions requises du système d'exploitation sous-jacent (appels d'API spécifiques nécessaires pour capturer des écrans ou des frappes de clavier). Les stratégies App Protection fournissent une protection même contre les outils de piratage personnalisés et spécifiques. Cependant, à mesure que les systèmes d'exploitation évoluent, de nouveaux programmes d'enregistrement de frappe et de capture d'écran peuvent émerger. Bien que nous continuions à les identifier et à les traiter, nous ne pouvons pas garantir une protection complète dans des configurations et des déploiements spécifiques.

Pour configurer la protection des applications sur l'application Citrix Workspace pour Mac, consultez la section correspondante dans l'article [Configuration](#).

Remarque :

- App Protection est prise en charge uniquement à partir de l'application Citrix Workspace 2001 pour Mac ou version ultérieure.

Amélioration de App Protection

À compter de la version 2301, App Protection est améliorée pour protéger l'application Citrix Workspace. Cette amélioration inclut la protection de l'écran d'authentification et de l'écran qui s'affiche après la connexion à l'application Workspace.

Prise en charge du partage d'écran lorsque App Protection est activée

À partir de la version 2402, vous pouvez partager du contenu via Microsoft Teams avec l'optimisation HDX, même lorsque App Protection est activée. Grâce à cette fonctionnalité, vous pouvez partager un écran dans la session de bureau virtuel dans son intégralité. Pour plus d'informations, consultez la section [Compatibilité avec l'optimisation HDX pour Microsoft Teams](#).

Forcer l'invite de connexion pour le fournisseur d'identité fédéré

L'application Citrix Workspace respecte désormais le paramètre Sessions de fournisseur d'identité fédéré. Pour plus d'informations, consultez l'article du centre de connaissances Citrix [CTX253779](#).

Vous n'avez plus besoin d'utiliser la stratégie Stocker les jetons d'authentification pour forcer l'invite de connexion.

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.

Sécuriser les communications

February 2, 2024

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 (exemple.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). Obtenez ensuite le certificat de serveur nécessaire 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 contrôlés par un serveur OS X ou une autre solution de gestion des appareils mobiles.

Les stratégies TLS comprennent les paramètres suivants :

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

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

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

SecurityAllowedTLSVersions. 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.
- **TLS13.** Spécifie que le protocole TLS 1.3 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

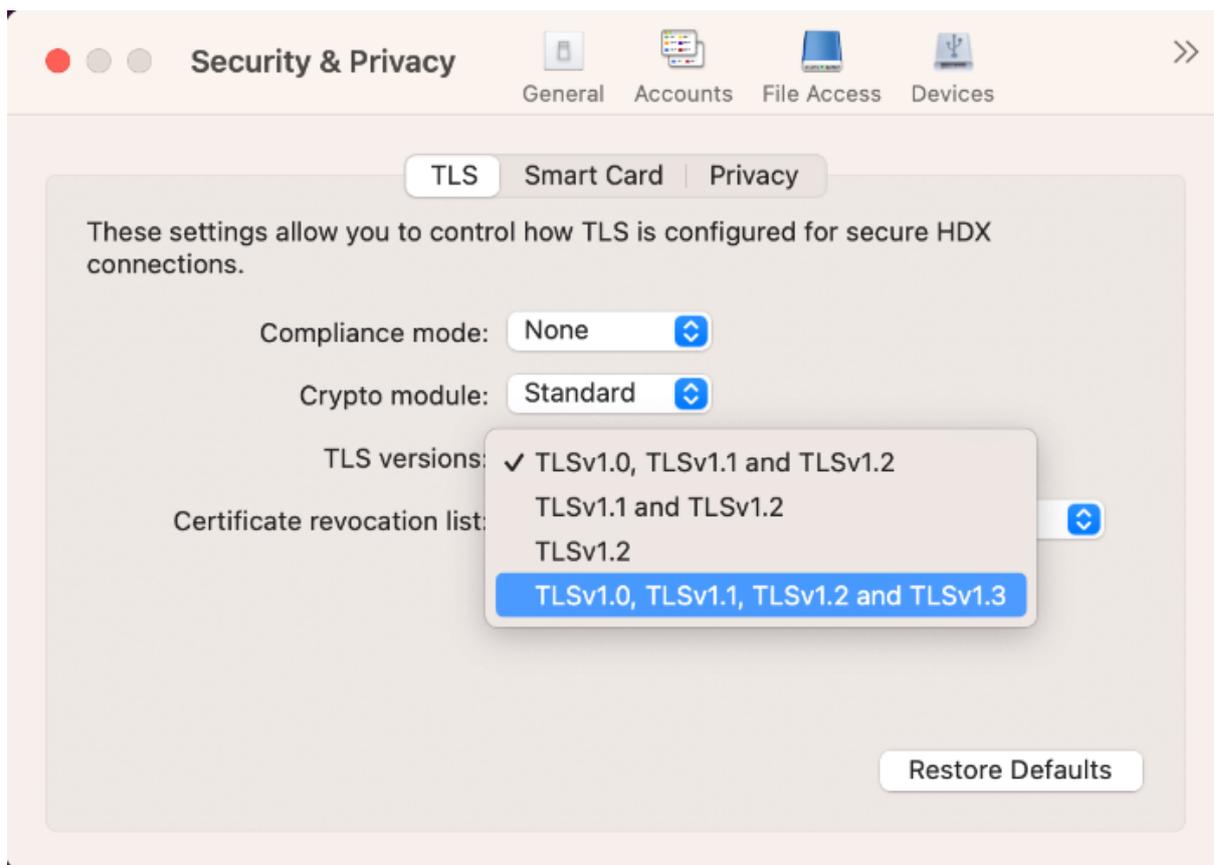
Des améliorations liées à la sécurité ont été introduites dans la version 12.3 de Citrix Receiver pour Mac, notamment :

- 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 :



Expérience de l'application

February 2, 2024

Cette section décrit les éléments suivants :

- [Mise à disposition d'applications](#)
- [Expérience de lancement d'applications et de bureaux virtuels améliorée pour Workspace \(utilisateurs cloud uniquement\)](#)
- [Préférences de l'application](#)
- [Collecte et surveillance des données](#)

Mise à disposition d'applications

April 17, 2024

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.

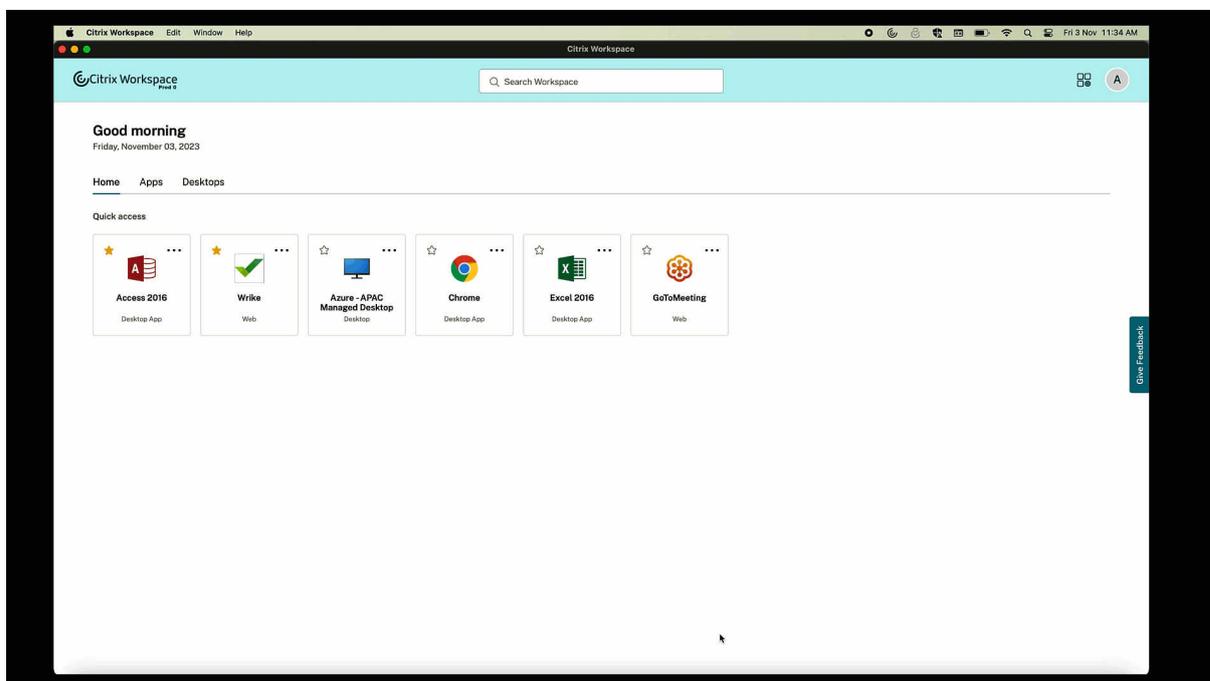
- Abonnez automatiquement tous les utilisateurs d'un magasin à une application en ajoutant la chaîne « **KEYWORDS:Auto** » à la description de l'application lors de sa publication dans Citrix Virtual Apps. Lorsque les utilisateurs se connectent au magasin, l'application est provisionnée automatiquement 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, consultez la documentation de [StoreFront](#).

Expérience de lancement d'applications et de bureaux virtuels améliorée pour Workspace (utilisateurs cloud uniquement)

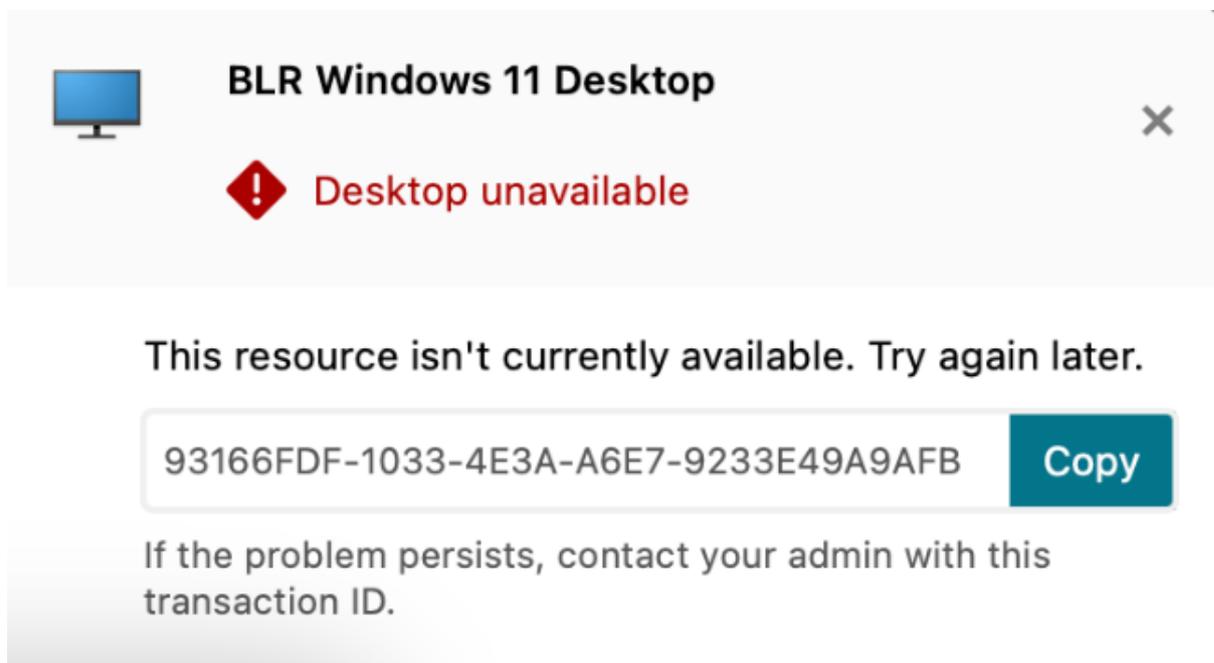
February 2, 2024

L'ouverture des ressources Citrix a été améliorée pour être plus intuitive, informative et conviviale. À partir de la version 2311, cette fonctionnalité est prise en charge pour les magasins en ligne personnalisés et les lancements hybrides.



La notification de progression du lancement apparaît désormais dans le coin inférieur droit de votre écran. L'état de progression des ressources en cours d'ouverture est affiché. Vous ne pouvez pas

recupérer la notification une fois que vous l'avez ignorée. La notification est conservée pendant quelques secondes à compter du début de la session. Si la session ne démarre pas, la notification affiche le message d'échec.



Remarque :

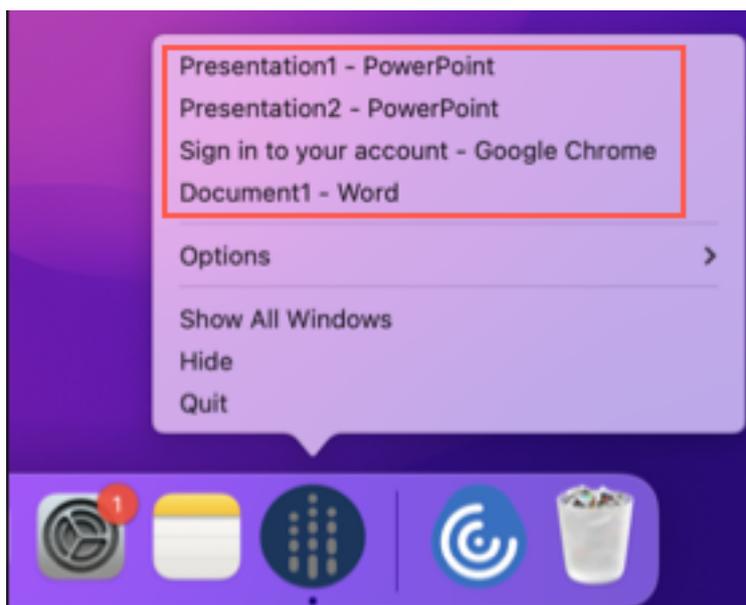
Cette fonctionnalité est disponible à la fois pour les sessions Workspace (cloud) et StoreFront.

Préférences de l'application

February 2, 2024

Les applications ouvertes apparaissent dans le Dock avec des icônes d'applications natives

Auparavant, le fait de cliquer sur des applications virtuelles dans l'application Citrix Workspace déclenchait **Citrix Viewer** où ces applications étaient disponibles. Si vous ouvrez de nombreuses applications, les applications ou leurs instances se sont ouvertes dans **Citrix Viewer**. Vous pouvez afficher les applications ouvertes en cliquant avec le bouton droit sur l'icône **Citrix Viewer**.

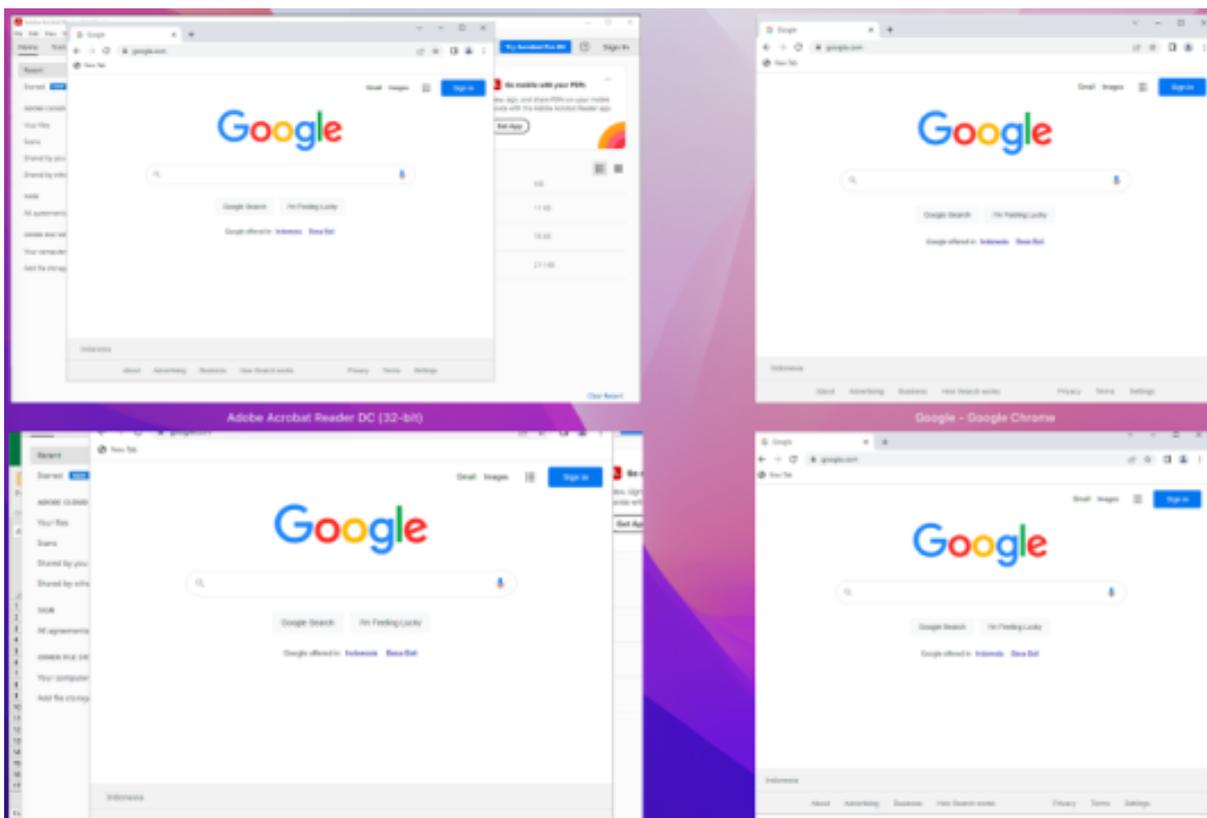


À partir de la version 2305, lorsque vous ouvrez des applications virtuelles, elles apparaissent dans le Dock (coin inférieur droit de l'écran) avec leurs icônes respectives et sont facilement identifiables. Vous pouvez ensuite accéder à l'application virtuelle depuis le dock lui-même. Si vous ouvrez plusieurs instances d'une application, ces instances ne sont pas des doublons dans le Dock mais sont regroupées au sein d'une instance du Dock.

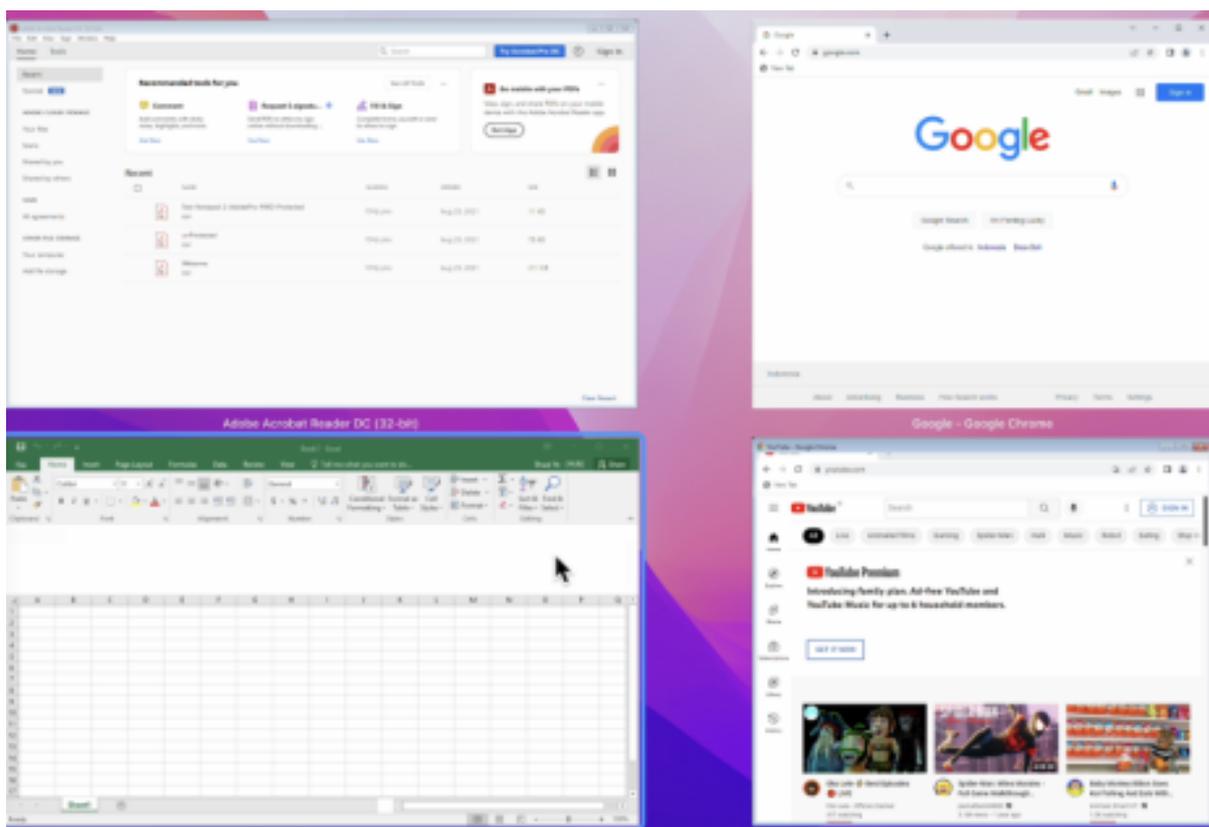


Amélioration de l'expérience Mission Control et App Expose

Auparavant, l'utilisation de la fonctionnalité **Mission Control** ou **App Expose** dans une session d'application virtuelle entraînait le chevauchement de nombreuses fenêtres ouvertes.



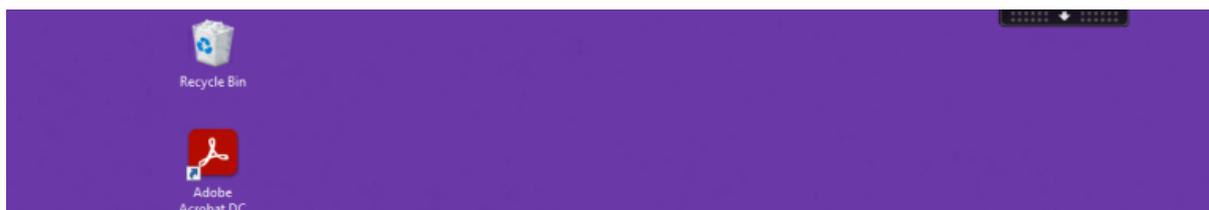
À partir de la version 2210, lorsque vous utilisez la fonctionnalité **Mission Control** ou **App Expose** dans une session d'application virtuelle et que vous ouvrez de nombreuses fenêtres, les fenêtres ne se chevauchent pas et vous pouvez facilement choisir l'une d'entre elles.



Prise en charge améliorée de la barre de menus

À partir de la version 2301, le CWA prend entièrement en charge l'option **Masquer/afficher automatiquement la barre des menus en plein écran** dans macOS. Pour les versions antérieures à macOS 13, vous devez accéder à **Préférences système > Dock et barre de menus** et décocher l'option **Masquer/afficher automatiquement la barre des menus en plein écran**. Pour macOS 13 et les versions ultérieures, vous devez accéder à **Préférences système > Bureau et Dock** et décocher l'option **Masquer/afficher automatiquement la barre des menus en plein écran**. Vous avez la possibilité d'activer ou de désactiver cette option. Cette amélioration prend également en charge une mise à l'échelle DPI haute résolution. La position de la souris apparaît également précise sur tous les moniteurs externes connectés.

La figure suivant illustre une fenêtre dans laquelle la barre de menus est masquée :



La figure suivante illustre une fenêtre dans laquelle la barre de menus apparaît :

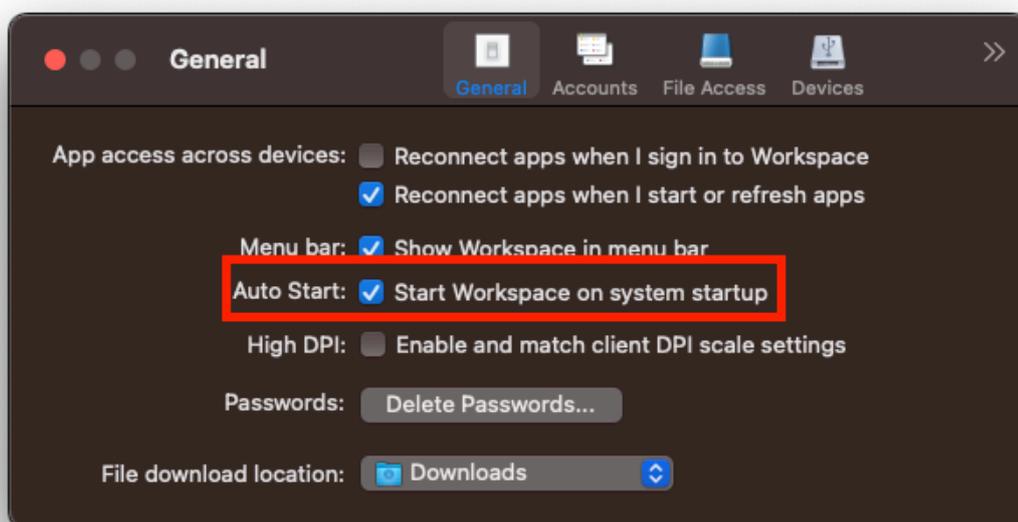


Défilement horizontal

Auparavant, l'application Citrix Workspace pour Mac ne prenait en charge que le défilement vertical sur un trackpad. À partir de la version 2305, le défilement horizontal est également pris en charge.

Amélioration de l'expérience de démarrage automatique

Auparavant, l'application Citrix Workspace pour Mac démarrait automatiquement chaque fois qu'un ordinateur était allumé. À partir de la version 2304, vous pouvez choisir de désactiver ou d'activer la fonctionnalité de démarrage automatique sur l'application Citrix Workspace pour Mac en accédant à **Préférences > Général > Démarrer Workspace** au démarrage du système. Le paramètre de démarrage automatique est activé par défaut.



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.

Affichage des applications, des bureaux et de Citrix Enterprise Browser à partir de la barre de menus via un menu d'accès rapide

Vous pouvez désormais afficher vos applications et bureaux les plus récemment utilisés ou préférés ou ouvrir une fenêtre Citrix Enterprise Browser en cliquant sur l'icône de Citrix Workspace dans la barre de menus. Cette fonctionnalité permet d'accéder facilement à certaines de vos ressources sans avoir à ouvrir l'application Citrix Workspace.

Recents Favorites

Apps

-  Access 2016
-  Concur
-  Excel 2016
-  Bitbucket - code
-  Chrome

[View all applications](#)

Desktops

-  Managed Win10 SIN Desktop

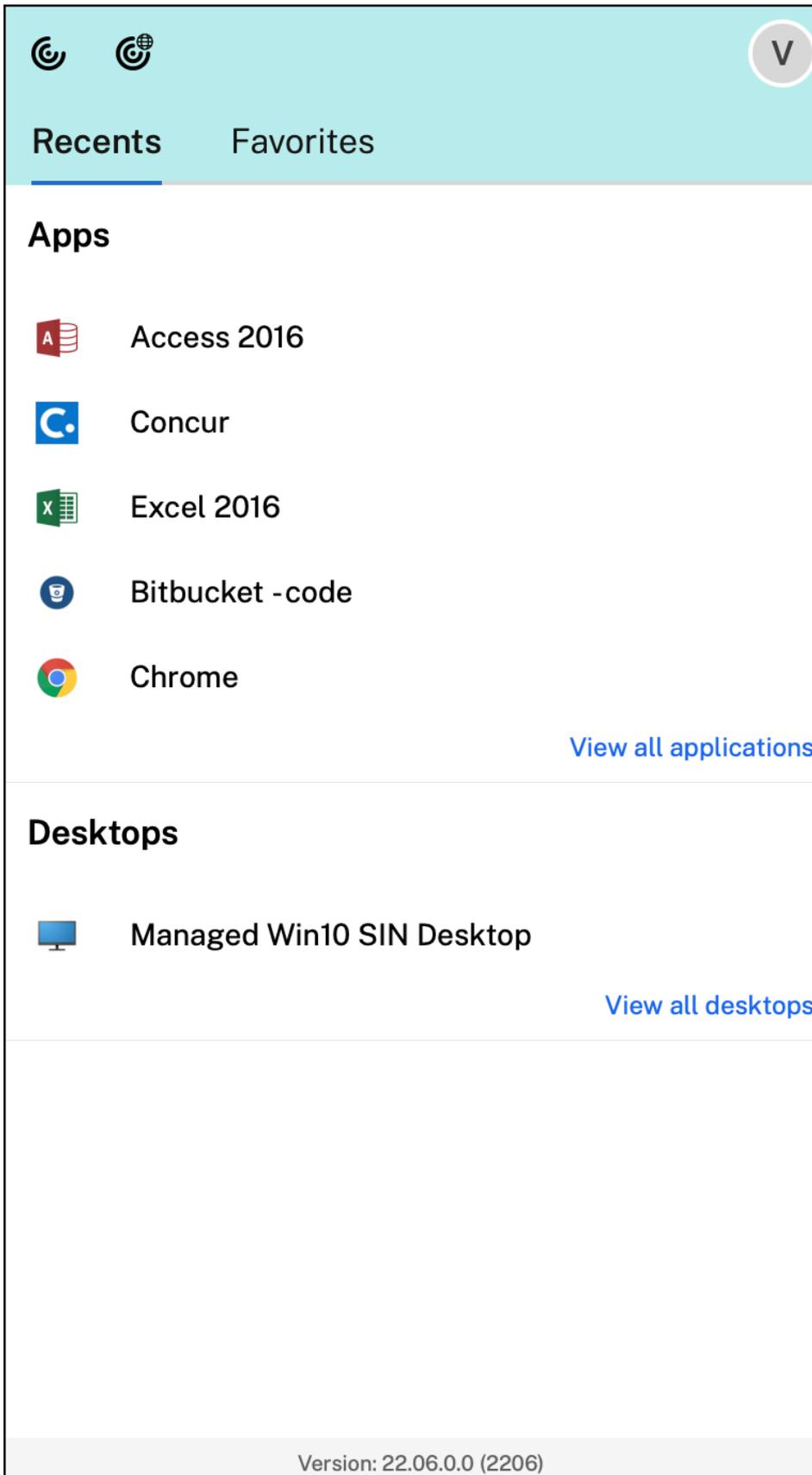
[View all desktops](#)

Version: 22.06.0.0 (2206)

Si vous n'avez configuré aucun compte, une invite de connexion s'affiche.



Un maximum de 5 applications ou bureaux récemment utilisés ou favoris apparaissent respectivement dans les options sous les onglets **Récent** et **Favoris**. Pour afficher les autres applications dans l'application Citrix Workspace, cliquez sur **Afficher toutes les applications**. Pour afficher les autres bureaux dans l'application Citrix Workspace, cliquez sur **Afficher tous les bureaux**.



Vous pouvez ouvrir l'interface utilisateur de Citrix Workspace en cliquant sur l'icône de l'application Citrix Workspace.

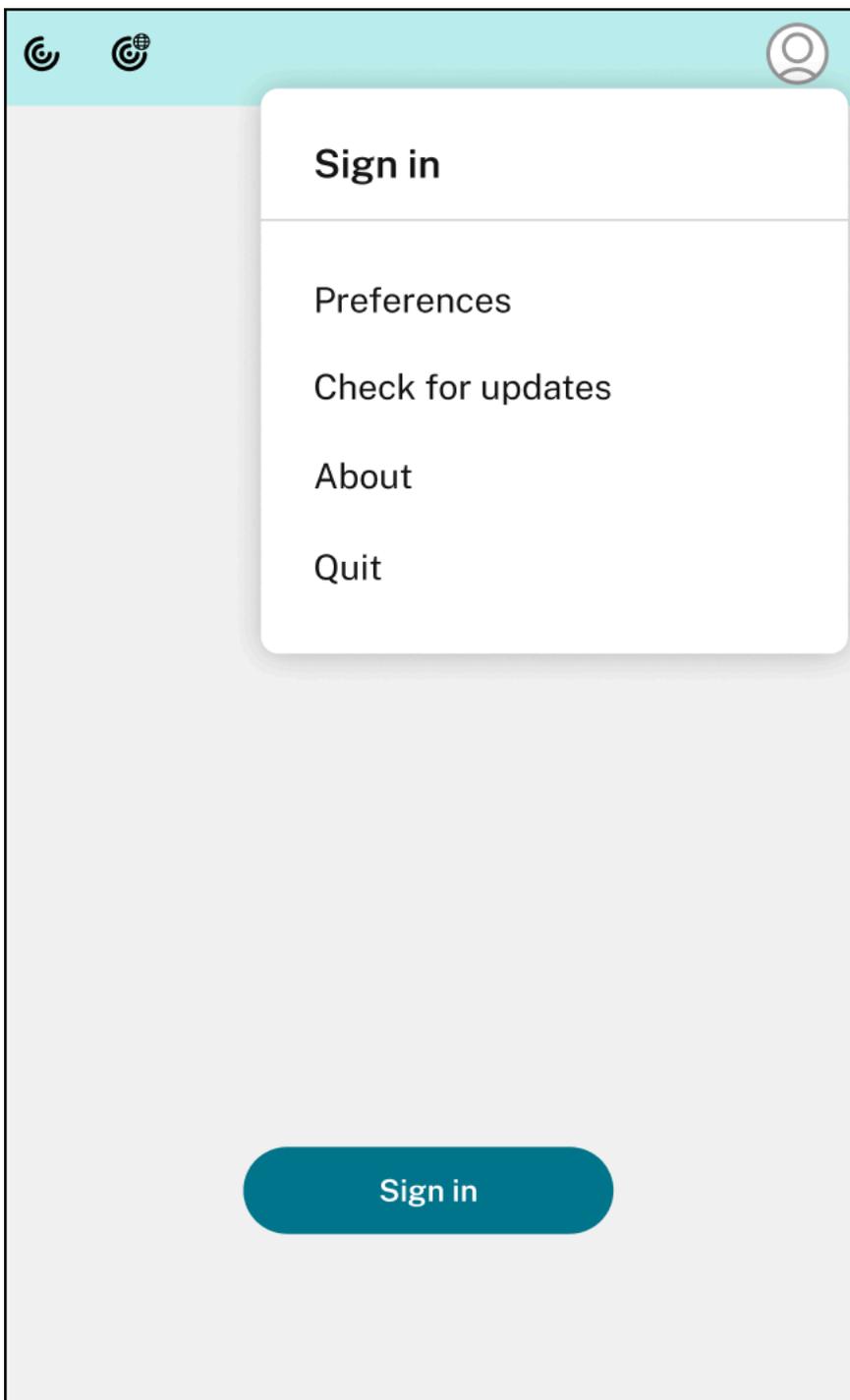


Vous pouvez ouvrir Citrix Enterprise Browser, sans ouvrir d'application Web ou SaaS en cliquant sur l'icône de Citrix Enterprise Browser.



Remarque :

Citrix Enterprise Browser n'est pas disponible si le magasin configuré ne comporte aucune application Web ou SaaS. En outre, il n'est disponible que si votre administrateur a configuré Citrix Secure Private Access.



Vous pouvez afficher les options suivantes lorsque vous cliquez sur l'icône **Compte** dans le coin supérieur droit :

- Préférences
- Rechercher les mises à jour
- À propos de

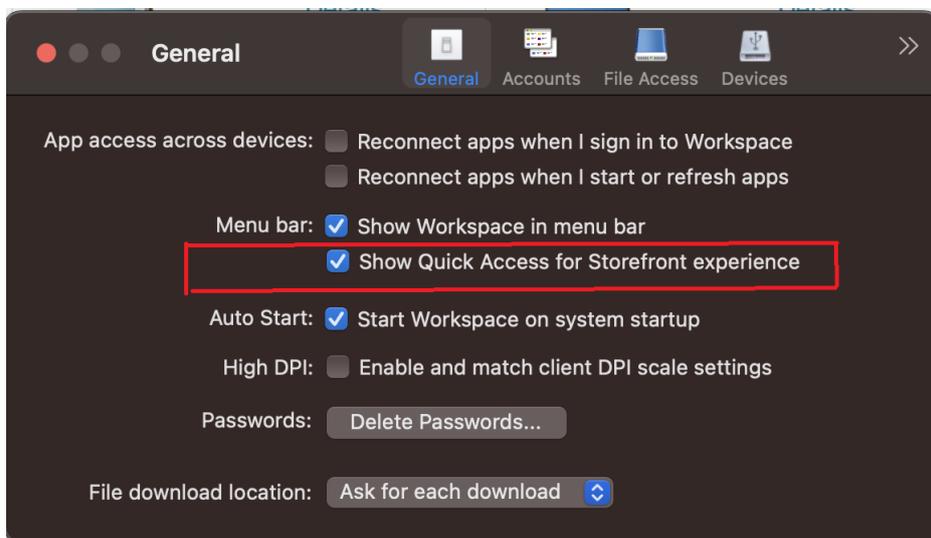
- Quitter

Menu d'accès rapide pour StoreFront

À partir de la version 2307, vous pouvez accéder rapidement et facilement à vos applications et bureaux préférés à l'aide de la fonction d'accès rapide pour les magasins locaux. Pour activer l'accès rapide, cliquez avec le bouton droit sur **Citrix Workspace** dans la barre d'outils, accédez à **Préférences > Général**, puis sélectionnez **Afficher l'accès rapide pour l'expérience Storefront**. Cette fonctionnalité vous permet de voir vos données préférées directement depuis la barre de menu Mac.



Vous pouvez activer la fonction d'accès rapide en utilisant **Préférences**.



Les administrateurs peuvent activer ou désactiver la fonctionnalité d'accès rapide en utilisant les méthodes Gestion d'appareils mobiles (MDM) ou Global App Configuration Service (GACS).

Activation ou désactivation de l'accès rapide via MDM

Pour permettre un accès rapide via MDM, les administrateurs doivent utiliser les paramètres suivants :

```
<key>ShowQuickAccessForStoreFront</key>  
<false/>
```

Pour plus d'informations sur l'utilisation de MDM, consultez la page [Gestion des appareils mobiles](#).

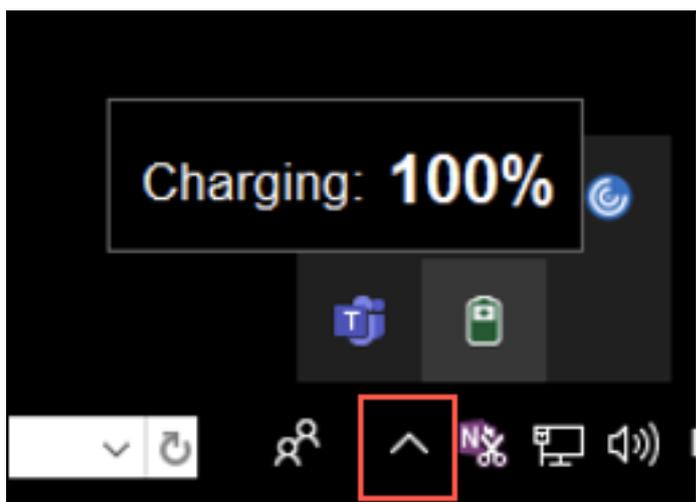
Activation ou désactivation de l'accès rapide via GACS

Pour permettre un accès rapide via GACS, les administrateurs doivent utiliser les paramètres suivants :

```
enableQuickAccessForStoreFront
```

Indicateur d'état de la batterie

L'état de la batterie de l'appareil s'affiche désormais dans la zone de notification d'une session Citrix Desktop. Pour afficher l'état de la batterie dans la session de bureau, cliquez sur la flèche **Afficher les icônes masquées** dans la barre des tâches.



Remarque :

L'indicateur d'état de la batterie n'apparaît pas pour les VDA du serveur.

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](#).

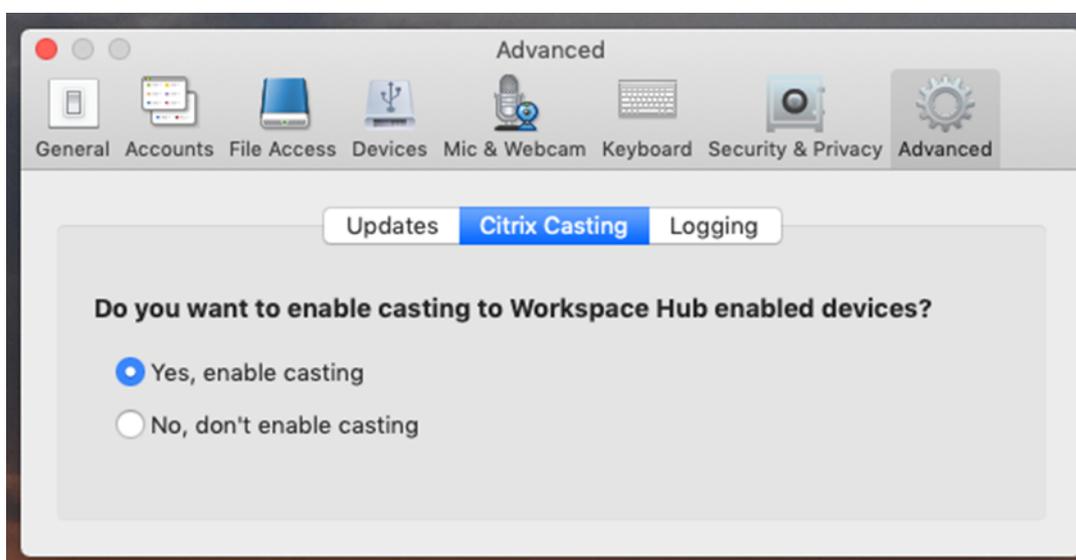
Pré-requis

- 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.

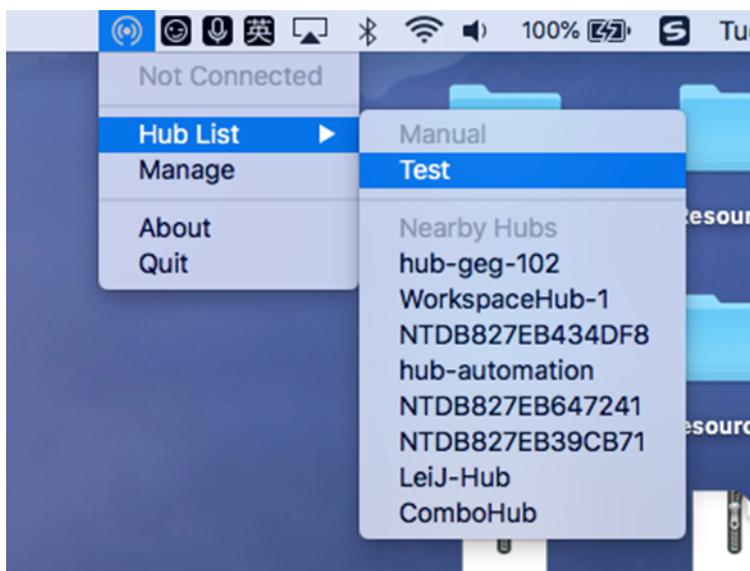
Remarque :

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**.

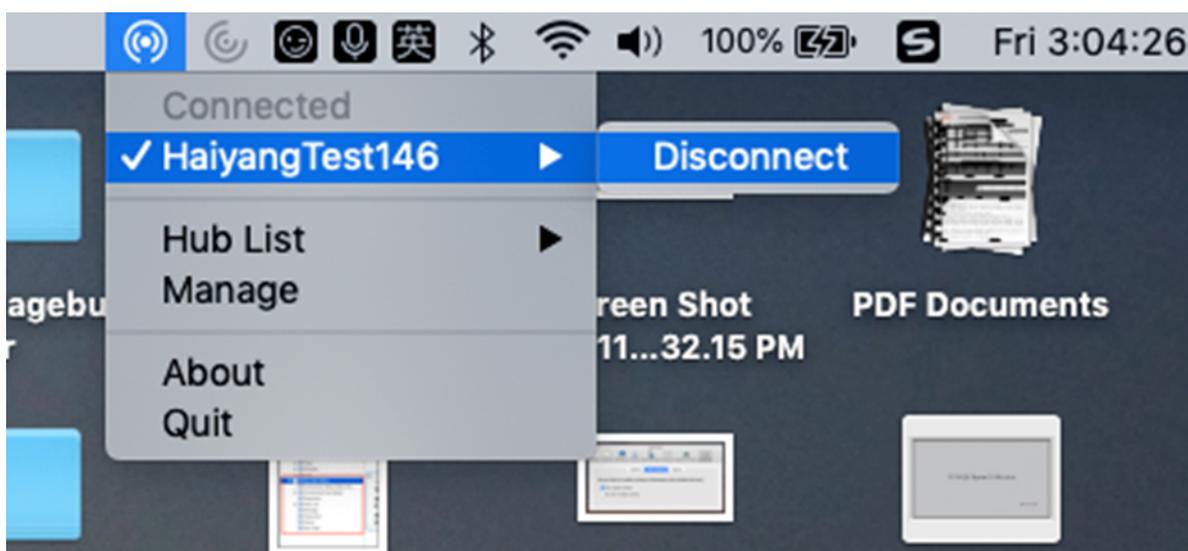
Remarque :

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.

Collecte et surveillance des données

May 16, 2024

Citrix Analytics

L’application Citrix Workspace est conçue pour transmettre en toute sécurité les journaux à Citrix Analytics. Lorsque la fonction est activée, les journaux sont analysés et stockés sur les serveurs Citrix Analytics. Pour plus d’informations sur Citrix Analytics, consultez [Citrix Analytics](#).

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.

Données collectées

Comme indiqué ci-dessus, Citrix collecte les données de configuration et d'utilisation de l'application Citrix Workspace pour améliorer la qualité, les fonctionnalités et les performances de l'application Citrix Workspace, et pour permettre à Citrix d'allouer correctement les ressources à des fins de développement de produits, ainsi que de maintenir les niveaux de service et gérer les investissements en personnel et en infrastructure. Les données sont utilisées et analysées uniquement sous forme agrégée. Aucun utilisateur ni leur machine ne sont ciblés et aucune analyse n'est effectuée sur des utilisateurs spécifiques sur la base des données CEIP.

Les données spécifiques à CEIP collectées par Google Analytics et Citrix 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 Enterprise 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

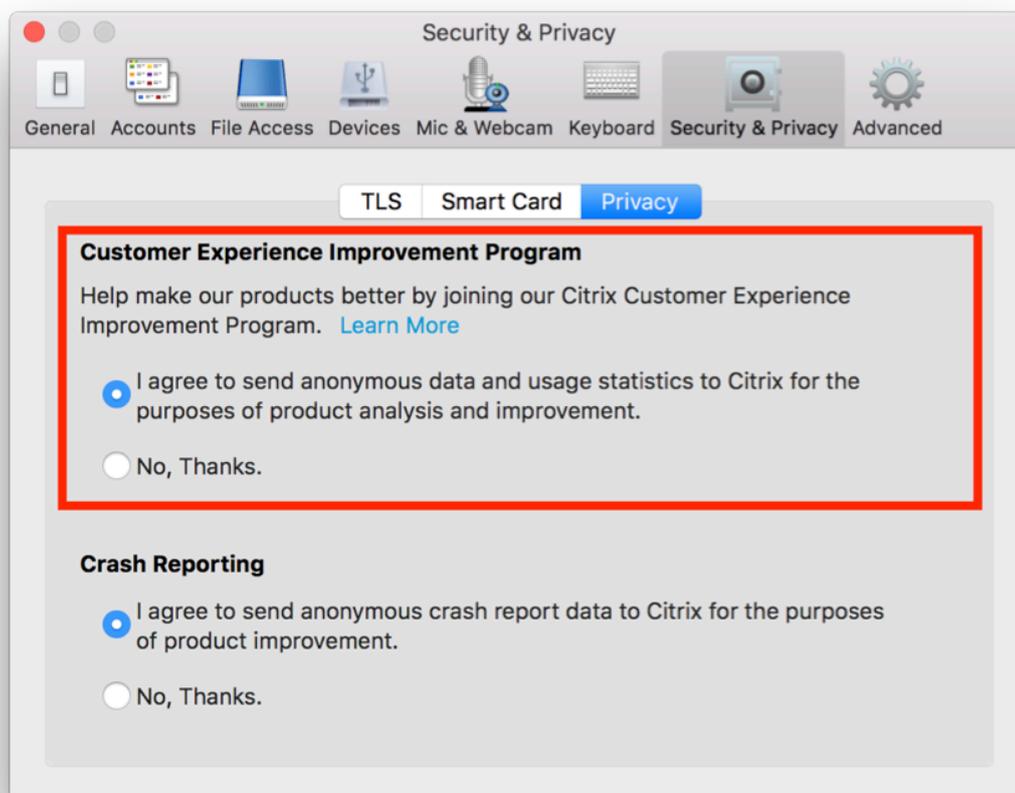
Utilisation de la fonctionnalité de magasin Web personnalisé	Préférences de reconnexion	Utilisation de Global App Configuration Service	Utilisation de la restauration du clavier
Utilisation de la fonctionnalité de suppression du mot de passe	Canal de mise à jour automatique	Détails de la location de connexion	GUID de l'utilisateur

Remarque :

- Aucune donnée n'est collectée et envoyée à Google Analytics pour les utilisateurs situés dans l'Union européenne (UE), dans l'Espace économique européen (EEE), en Suisse et au Royaume-Uni (Royaume-Uni).
- Citrix Enterprise Browser était auparavant connu sous le nom de Citrix Workspace Browser.

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. Cliquez sur 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
```

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](#).

HDX et multimédia

February 2, 2024

Cette section décrit les fonctionnalités HDX et multimédia des composants suivants :

- [Graphisme et affichage](#)
- [Microsoft Teams optimisé](#)
- [Transport HDX](#)

Graphisme et affichage

May 16, 2024

Moniteurs multiples

Vous pouvez 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

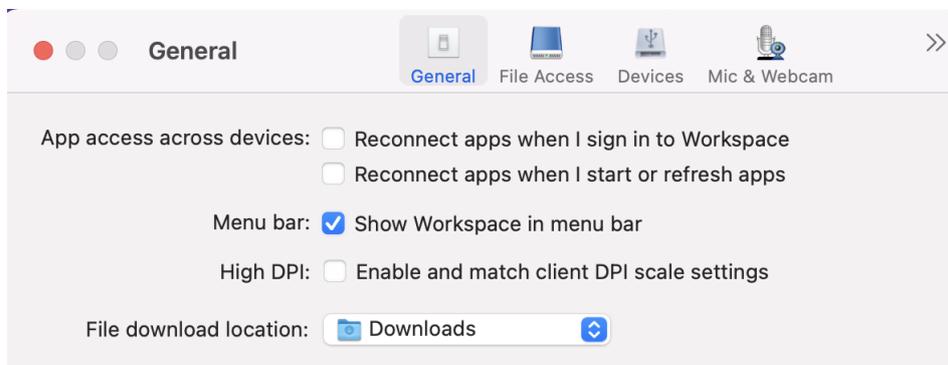
- Le mode plein écran est uniquement pris en charge sur un seul écran ou tous les écrans, ce qui est configurable via un élément de menu.
- Citrix recommande d'utiliser un maximum de 2 moniteurs. L'utilisation de plus de 2 moniteurs peut dégrader les performances de la session ou entraîner des problèmes d'accessibilité.
- Le mode plein écran n'est pas disponible sur les Mac dotés d'un écran à encoche.

Prise en charge de DPI élevé

L'application Citrix Workspace pour Mac est désormais compatible avec les écrans haute résolution d'une résolution de 4K ou 5K. Avec cette fonctionnalité, le texte, les images et les autres éléments

graphiques des sessions d'application ou de bureau virtuel apparaissent dans une taille qui peut être visualisée confortablement sur ces écrans haute résolution.

Pour activer cette fonctionnalité, accédez à **Préférences > Général > Haute résolution**.



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 de 65536 Ko et est suffisante pour un écran haute résolution avec une résolution 4K.

Pour les sessions d'application virtuelle, la valeur par défaut de **Limite de mémoire d'affichage** est suffisante, car la session d'application ne prend pas en charge plus d'un affichage.

Pour les sessions de bureau virtuel, les administrateurs doivent accéder à **Citrix Studio > Stratégies > Limite de mémoire d'affichage** et utiliser une valeur plus élevée, par exemple 393216 Ko pour utiliser les fonctionnalités haute résolution sur plusieurs moniteurs externes ou à résolution 5K.

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.

Le nombre de moniteurs externes que vous pouvez utiliser avec votre Mac est toujours limité par le modèle Mac, ainsi que par la résolution et la fréquence d'actualisation de chaque écran. Consultez les caractéristiques techniques de votre Mac pour connaître le nombre de moniteurs externes pris en charge. Pour plus d'informations, consultez l'article [Connecter un ou plusieurs moniteurs externes avec le Mac](#) de l'assistance Apple.

Prise en charge améliorée de l'écran à encoche

À compter de la version 2301, l'application Citrix Workspace pour Mac est compatible avec les Mac dotés d'un écran à encoche. Les Mac prennent en charge un écran à encoche natif en mode plein écran pour l'affichage Retina et multi-écrans. La zone de la session sur l'écran à encoche est désormais beaucoup plus grande et offre aux clients plus d'espace sur l'écran. Cette amélioration prend

également en charge une mise à l'échelle DPI haute résolution. La position de la souris apparaît également précise sur tous les moniteurs externes connectés.

Remarque :

Assurez-vous de ne pas sélectionner l'option **Scale to fit below built-in camera** dans Citrix Viewer. Cette option n'est pas sélectionnée par défaut et n'est disponible que sur les Mac dotés d'un écran à 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.

Masquer ou afficher la barre d'outils du bureau dans la session de bureau virtuel

Vous pouvez choisir de masquer ou d'afficher complètement la barre d'outils du bureau dans la session de bureau virtuel.

Pour plus d'informations sur le masquage complet de la barre d'outils du bureau, consultez l'article de support [CTX202450](#) dans le centre de connaissances.

Étendre plusieurs moniteurs en mode plein écran

À partir de la version 2203.1, vous pouvez passer en mode plein écran sur deux écrans ou plus simultanément. 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**, veuillez 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.

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

À partir de la version 2204, 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 de l'extension de plusieurs moniteurs en mode plein écran sur un maximum de cinq moniteurs

Auparavant, Citrix prenait en charge un maximum de trois moniteurs en mode plein écran, y compris le moniteur principal.

À partir de la version 2311, vous pouvez désormais utiliser le mode plein écran sur un maximum de cinq moniteurs simultanément, y compris le moniteur principal.

Remarque

Le nombre de moniteurs externes que vous pouvez utiliser avec votre Mac est toujours limité par le modèle Mac, ainsi que par la résolution et la fréquence d'actualisation de chaque écran. Consultez les caractéristiques techniques de votre Mac pour connaître le nombre de moniteurs externes pris en charge. Pour plus d'informations, consultez l'article [Connecter un ou plusieurs moniteurs externes avec le Mac](#) de l'assistance Apple.

Vous pouvez étendre plusieurs moniteurs en mode plein écran des deux manières suivantes :

- **Utilisation de la barre de menu**

1. Ouvrez **Citrix Viewer**.
2. Dans la barre de menu, cliquez sur **Afficher** et sélectionnez **Entrer en mode plein écran** pour étendre le mode plein écran.

Remarque :

Pour passer en mode plein écran sur tous les écrans connectés en même temps, activez **Utiliser tous les affichages en plein écran**, puis sélectionnez **Entrer en mode plein écran** dans le menu **Affichage**.

- **Utilisation du bouton vert dans la fenêtre d'application**

1. Ouvrez **Citrix Viewer**.
2. Faites glisser ou redimensionnez la fenêtre Citrix Viewer pour l'étendre sur les moniteurs que vous souhaitez utiliser en mode plein écran.
3. Déplacez le pointeur sur le bouton vert situé dans le coin supérieur gauche de la fenêtre, puis sélectionnez **Entrer en mode plein écran** dans le menu qui apparaît ou cliquez sur le bouton vert. L'écran est désormais étendu aux moniteurs qui ont une intersection avec la fenêtre.

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 65 536 Ko. Elle est suffisante pour un maximum de 2 moniteurs 4K (2 x 32 400 Ko). Les administrateurs doivent augmenter cette valeur pour utiliser cinq moniteurs en fonction de la résolution d'affichage. Pour modifier la **limite de mémoire d'affichage**, vous pouvez accéder à **Citrix Studio > Stratégies > Limite de mémoire d'affichage**. Pour plus d'informations sur la stratégie Limite de mémoire d'affichage, consultez la section [Limite de mémoire d'affichage](#) de la documentation XenApp et XenDesktop.

Performances graphiques améliorées

À partir de la version 2308, les performances graphiques sont améliorées pour des sessions d'application transparentes. Cette fonctionnalité optimise également la charge d'utilisation du processeur.

Support pour le décodage vidéo H.265

À partir de la version 2402, l'application Citrix Workspace pour Mac prend en charge l'utilisation du codec vidéo H.265 (HEVC) pour l'accélération matérielle des graphiques et vidéos distants. Le codec vidéo H.265 (HEVC) prend en charge l'espace colorimétrique YUV 4:2:0 par défaut. Le codec vidéo H.265 doit être pris en charge et activé à la fois sur le VDA et sur l'application Citrix Workspace. Si votre périphérique Mac ne prend pas en charge le décodage H.265 à l'aide de l'interface VideoToolbox, le

paramètre de stratégie de décodage H265 pour les graphiques est ignoré et la session utilise le codec vidéo H.264.

Logiciels requis

- VDA 7.16 ou version ultérieure utilisant les GPU suivants :
 - GPU NVIDIA de génération Maxwell ou version ultérieure
 - GPU Intel de 6e génération ou version ultérieure
 - GPU AMD de génération Raven ou version ultérieure
- Activez la stratégie **Optimiser pour la charge des graphiques 3D** sur le VDA.
- Activez la stratégie **Utiliser le codage matériel pour le codec vidéo** sur le VDA.

Sur l'application Citrix Workspace pour Mac, cette fonctionnalité est configurée pour être activée par défaut.

Pour désactiver cette fonctionnalité via la gestion des appareils mobiles (MDM), les administrateurs doivent utiliser les paramètres suivants :

```
<key>EnableXdecoderForH265</key><false/>
```

Redémarrez la session pour que les modifications prennent effet.

Remarque :

Exécutez l'outil HDX Monitor 3.x pour identifier si l'encodeur vidéo H.265 est activé dans la session. Pour plus d'informations sur l'outil HDX Monitor 3.x, consultez l'article [CTX135817](#) du centre de connaissances.

Microsoft Teams optimisé

February 2, 2024

Configurer une interface réseau préférée

À partir de la version 2304, vous pouvez configurer une interface réseau préférée pour le trafic multi-média. Exécutez la commande suivante dans le terminal :

```
defaults write com.citrix.HdxRtcEngine NetworkPreference -int <value>
```

Sélectionnez l'une des valeurs suivantes selon les besoins :

- 1 : Ethernet
- 2 : Wi-Fi
- 3 : Cellulaire
- 4 : VPN
- 5 : Bouclage
- 6 : Quelconque

Par défaut, et si aucune valeur n'est définie, le moteur de média WebRTC choisit la meilleure route disponible.

Estimation des performances au niveau du codage

Le processus `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
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 sur 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](#).

Expérience améliorée pour des visioconférences dans Microsoft Teams optimisé

À compter de la version 2304, la prise en charge de la diffusion simultanée est activée par défaut pour des visioconférences dans Microsoft Teams optimisé. Grâce à cette assistance, chaque appel est réglé à la résolution appropriée pour une expérience d'appel optimale. Cette fonctionnalité améliore la qualité et l'expérience des visioconférences sur différents points de terminaison.

Grâce à cette expérience améliorée, chaque utilisateur peut diffuser plusieurs flux vidéo dans différentes résolutions (par exemple, 720p, 360p, etc). La résolution vidéo dépend de plusieurs facteurs, notamment la capacité du point de terminaison, les conditions du réseau, etc. Le point de terminaison récepteur demande ensuite la résolution de qualité maximale qu'il peut gérer, offrant ainsi à tous les utilisateurs une expérience vidéo optimale.

Remarque :

Cette fonctionnalité est disponible uniquement après le déploiement d'une mise à jour de Microsoft Teams. Pour plus d'informations sur l'estimation de date de publication, accédez à <https://www.microsoft.com/> et recherchez la feuille de route de Microsoft 365. Une fois la mise à jour déployée par Microsoft, vous pourrez consulter l'article [CTX253754](#) pour obtenir la mise à jour de la documentation et l'annonce.

Limiter les résolutions vidéo

Les administrateurs dont les utilisateurs utilisent des points de terminaison client moins performants peuvent choisir de limiter les résolutions vidéo entrantes ou sortantes afin de réduire l'impact du codage et du décodage vidéo sur ces points de terminaison. À partir de l'application Citrix Workspace 2304 pour Mac, vous pouvez limiter ces résolutions à l'aide des options de configuration du client.

Remarque :

Les utilisateurs utilisant des résolutions restreintes affecteront la qualité vidéo globale de la conférence, car le serveur Microsoft Teams est obligé d'utiliser la résolution du plus petit dénominateur commun pour tous les participants à la conférence.

Les contraintes d'appel sont désactivées par défaut sur le client avec l'application Citrix Workspace 2304. Pour l'activer, les administrateurs doivent définir les configurations côté client suivantes à l'aide de la commande defaults :

```
defaults write com.citrix.HdxRtcEngine <Name> -<Type> <Value>
```

Nom	Type	Mandatory	Valeurs acceptées
EnableSimulcast	Entier	OUI	1-3 (Définir sur 1)

Nom	Type	Mandatory	Valeurs acceptées
MaxOutgoingResolution	Entier	OUI	180, 240, 360, 540, 720, 1080 (résolutions prises en charge par Microsoft Teams)
MaxIncomingResolution	Entier	OUI	180, 240, 360, 540, 720, 1080 (résolutions prises en charge par Microsoft Teams)
MaxIncomingStreams	Entier	OUI	1–8
MaxSimulcastLayers	Entier	OUI	1-3 (Définir sur 1)
MaxVideoFrameRate	Entier	NON	1–30
MaxScreenShareFrameRate	Entier	NON	1–15

Flou et remplacement d'arrière-plan avec l'optimisation de Microsoft Teams pour Citrix

À partir de la version 2301, l'optimisation de Microsoft Teams dans l'application Citrix Workspace pour Mac prend désormais le flou et le remplacement de l'arrière-plan. Vous pouvez utiliser cette fonctionnalité en sélectionnant **Plus > Appliquer des effets d'arrière-plan** lorsque vous participez à une réunion ou à un appel P2P.

Amélioration du mode veille pour optimiser les appels Microsoft Teams

Auparavant, lorsque vous participiez à une réunion Microsoft Teams optimisée, en l'absence d'interaction avec la souris ou le clavier, l'application Citrix Workspace ou l'écran de Microsoft Teams optimisé pouvait passer en mode veille.

À partir de la version 2305, l'application Citrix Workspace ou l'écran de Microsoft Teams optimisé ne passe pas en mode veille même s'il n'y a aucune interaction avec la souris ou le clavier lors d'une réunion Microsoft Teams optimisée.

Optimisation du partage d'écran avec Microsoft Teams

À partir de la version 2012, l'application Citrix Workspace pour Mac prend en charge l'optimisation du partage d'écran avec Microsoft Teams. Pour plus d'informations, consultez les rubriques suivantes :

- [Optimisation pour Microsoft Teams](#)
- [Redirection de Microsoft Teams](#)

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

À partir de la version 2101, l'application Citrix Workspace pour Mac prend désormais en charge l'optimisation de Microsoft Teams pour des sessions d'application 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 de Microsoft Teams](#)

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

À partir de la version 2101, l'application Citrix Workspace pour Mac prend en charge l'interaction de signalisation DTMF avec les systèmes de téléphonie (par exemple, RTPC) et les téléconférences dans Microsoft Teams. Cette fonctionnalité est activée par défaut.

Améliorations apportées à Desktop Viewer

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.

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

À partir de la version 2109, l'application Citrix Workspace pour Mac prend en charge le codage ou le décodage vidéo H.264 avec accélération matérielle. Elle 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 et le codage vidéo avec accélération matérielle sont activés par défaut si un périphérique les prend en charge. Cette amélioration réduit la charge sur l'UC lors de l'utilisation de multimédia lorsque Microsoft Teams est optimisé avec HDX.

Appels d'urgence dynamiques

À partir de la version 2112, 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. Elle n'est pas envoyée en fonction 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 **Systeme téléphonique Microsoft**.

Demander le contrôle dans Microsoft Teams

À partir de la version 2112, 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**.

Donner ou prendre le contrôle dans Microsoft Teams

À partir de la version 2203.1, vous pouvez utiliser le bouton **Donner le contrôle** pour donner le contrôle de votre écran partagé aux autres utilisateurs participant à la réunion. Les autres participants peuvent 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.

Chat et réunions multi-fenêtres pour Microsoft Teams

À partir de la version 2203.1, vous pouvez 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 de fenêtre indépendante, consultez [Microsoft 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, il est possible que Microsoft abandonne 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](#).

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

À partir de la version 2203.1, vous pouvez 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.

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.

Compatibilité de App Protection avec l'optimisation HDX pour Microsoft Teams

À partir de la version 2204, le partage complet du moniteur ou du bureau est désactivé lorsque App Protection 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.

Annonce de fin de prise en charge du format SDP (Plan B) de WebRTC

Citrix prévoit de mettre fin à la prise en charge actuelle du format SDP (Plan B) de WebRTC dans les prochaines versions. Vous devez utiliser une version de l'application Citrix Workspace compatible avec le format Unified Plan pour continuer à utiliser certaines fonctionnalités de Microsoft Teams optimisé.

Transport HDX

May 16, 2024

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.

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

```
defaults write com.citrix.receiver.nomas HDXOverUDPAAllowed -bool NO
```

Découverte de l'unité de transmission maximale (MTU) dans Enlightened Data Transport (EDT)

À partir de la version 2108, l'application Citrix Workspace pour Mac prend en charge la détection des unités de transmission maximales (MTU) 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.

Amélioration apportée au contrôle de la congestion du réseau

À partir de la version 2308, le protocole de transport propriétaire de Citrix appelé Enlightened Data Transport (EDT) est amélioré pour contrôler efficacement la congestion du réseau. Cette fonctionnalité améliore le débit des données et réduit le temps de latence.

Réducteur HDX mis à niveau vers la version 4

Auparavant, l'application Citrix Workspace pour Mac prenait en charge le réducteur HDX V3. À partir de la version 2402, l'application Citrix Workspace pour Mac prend en charge le réducteur HDX V4. Cette fonctionnalité réduit la bande passante réseau requise pour une session type et améliore le temps de réponse.

Appareils

February 2, 2024

Cette section décrit les fonctionnalités prises en charge pour les périphériques suivants :

- [Audio et microphone](#)
- [Mappage des lecteurs clients](#)
- [Clavier](#)
- [Impression](#)

- [USB](#)
- [Webcam](#)

Audio et microphone

May 16, 2024

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 améliorée de l'annulation de l'écho audio

L'application Citrix Workspace prend 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.

Entrée microphone côté client

L'application Citrix Workspace pour Mac prend en charge de multiples entrées microphone du côté client. Vous pouvez utiliser des microphones installés localement 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 choisir comment utiliser votre microphone et votre webcam avec les sessions d'applications et de bureaux virtuels. Pour appliquer le type d'accès à votre microphone et à votre webcam, sélectionnez l'un des types d'accès suivants selon vos besoins dans l'onglet **Micro et webcam** dans les paramètres **Préférences** :

- **Utiliser mon micro et ma webcam** : permet d'accéder au microphone et à la webcam lorsqu'ils sont connectés.

- **Ne pas utiliser mon micro et ma webcam** : n'accorde aucun accès au microphone et à la webcam.
- **Toujours me demander** : demande l'autorisation chaque fois qu'un accès au microphone et à la webcam est requis.

Pour appliquer un effet de flou d'arrière-plan lors de l'utilisation de la webcam, sélectionnez **Activer l'effet de flou d'arrière-plan lors de l'utilisation de la webcam**.

Prise en charge de plusieurs périphériques audio

À partir de la version 2311, l'application Citrix Workspace pour Mac affiche tous les périphériques audio locaux disponibles dans une session, accompagnés de leur nom. En outre, la fonctionnalité Plug and Play est également prise en charge.

Configuration par magasin des niveaux d'accès au microphone et à la webcam

À partir de la version 2307, l'accès au microphone et à la webcam par magasin est inclus dans le cadre de la fonction Client Selective Trust. Cette amélioration vous permet de fournir l'accès à un microphone et à une webcam par magasin.

Pour activer l'accès au microphone et à la webcam pour un magasin, sélectionnez **Préférences > Micro et webcam**. Dans l'onglet **Micro et webcam**, sélectionnez le magasin et le type d'accès requis pour ce magasin.

Prise en charge de la synchronisation du volume audio

Auparavant, le contrôle du volume audio était indépendant entre le Virtual Delivery Agent (VDA) et votre appareil. Vous devez régler le volume des deux côtés pour maintenir le volume souhaité. De plus, si vous avez désactivé le volume de votre appareil, vous ne pouvez pas le réactiver sur le VDA.

À partir de la version 2402, l'application Citrix Workspace pour Mac prend en charge la synchronisation du volume audio entre le VDA et vos périphériques audio. Vous pouvez désormais régler le volume à l'aide du curseur de volume audio du VDA pour avoir le même volume que sur votre appareil et vice versa. Cette fonctionnalité est activée par défaut.

Pour activer cette fonctionnalité, vous devez utiliser la version 2308 ou ultérieure du VDA. Pour en savoir plus, consultez la section [Synchronisation des volumes audio](#) dans la documentation Citrix Virtual Apps and Desktops.

Pour désactiver cette fonctionnalité via la gestion des appareils mobiles (MDM), les administrateurs doivent utiliser les paramètres suivants :

```
<key>EnableVolumeSync</key><false/>
```

Redémarrez la session pour que les modifications prennent effet.

Mode de tolérance de pertes pour l'audio

À partir de la version 2402, l'application Citrix Workspace prend en charge le mode de tolérance de pertes (compression avec perte EDT) pour la redirection audio. Cette fonctionnalité améliore l'expérience utilisateur pour le streaming en temps réel lorsque les utilisateurs se connectent via des réseaux à latence élevée et à perte de paquets. Cette fonctionnalité est activée par défaut.

Pour activer cette fonctionnalité, vous devez utiliser la version 2311 ou ultérieure du VDA. Pour en savoir plus, consultez la section [Prise en charge de l'audio via le mode de tolérance de pertes \(Technical Preview\)](#) dans la documentation Citrix Virtual Apps and Desktops.

Pour désactiver cette fonctionnalité via la gestion des appareils mobiles (MDM), les administrateurs doivent utiliser les paramètres suivants :

```
<key>EdtUnreliableAllowed</key><false/>
```

Redémarrez la session pour que les modifications prennent effet.

Mappage des lecteurs clients

February 2, 2024

Au cours de la session, le mappage des lecteurs clients vous permet d'accéder aux lecteurs locaux sur le périphérique matériel de l'utilisateur. Les périphériques matériels de l'utilisateur peuvent être des lecteurs de CD-ROM, des DVD et des clés USB. Lorsqu'une configuration de serveur autorise le mappage des lecteurs clients, vous pouvez accéder aux fichiers stockés localement et travailler dessus pendant les sessions. Vous pouvez également les enregistrer sur un lecteur local ou sur un lecteur du serveur.

L'application Citrix Workspace pour Mac surveille les répertoires dans lesquels les périphériques matériels utilisateur sont généralement montés sur la machine utilisateur. Elle peut automatiquement mapper tous les nouveaux répertoires apparaissant au cours d'une session à la prochaine lettre de lecteur 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.

Clavier

May 16, 2024

Synchronisation de la disposition du clavier

La synchronisation de la disposition du clavier vous permet de basculer entre leurs dispositions de clavier préférées sur la machine cliente. Cette fonction est désactivée par défaut. Une fois que vous avez activé cette fonctionnalité, la disposition du clavier client se synchronise automatiquement avec la session d'applications et de bureaux virtuels.

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 > Inter-**

national, est ajouté pour afficher l'état activé.

À compter de la version 2210, l'application Citrix Workspace pour Mac prend en charge trois modes de synchronisation de la disposition du clavier :

- **Synchroniser une seule fois –lorsque la session est lancée** : basé sur la valeur CTXIME du fichier `Config`, la disposition du clavier du client est synchronisée avec le serveur lorsque la session est lancée. Les modifications que vous apportez à la disposition du clavier du client pendant la session ne prennent pas effet immédiatement. Pour appliquer les modifications, déconnectez-vous et connectez-vous à l'application. Le mode Synchroniser une seule fois - lorsque la session est lancée est la disposition de clavier par défaut pour l'application Citrix Workspace sur Mac.
- **Autoriser la synchronisation dynamique** : cette option synchronise la disposition du clavier client sur le serveur lorsque vous modifiez la disposition du clavier client.
- **Ne pas synchroniser** - Indique que le client utilise la disposition du clavier présente sur le serveur.

Logiciels requis

- Activez la fonctionnalité de mappage de disposition du clavier Unicode sur le VDA Windows. Pour obtenir davantage d'informations, consultez l'article [CTX226335](#) du centre de connaissances.
- Activez la fonctionnalité de synchronisation dynamique de la disposition du clavier sur le VDA Linux. Pour plus d'informations, consultez la section [Synchronisation dynamique de la disposition du clavier](#).
- Lorsque vous utilisez un Windows Server 2016 ou Windows Server 2019, accédez au chemin d'accès au Registre `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\Icalme`, ajoutez une valeur **DWORD** avec le nom de clé **DisableKeyboardSync** et définissez la valeur sur **0**.

Configurer la disposition du clavier

L'application Citrix Workspace pour Mac fournit une interface utilisateur permettant de configurer les trois différents modes de synchronisation de la disposition du clavier.

Pour configurer la synchronisation de la disposition du clavier à l'aide de l'interface utilisateur :

1. Depuis l'icône de l'application Citrix Workspace dans la barre de menu, cliquez sur l'icône du compte dans le coin supérieur droit et accédez à **Préférences > Clavier**.

Les paramètres de synchronisation de la disposition du clavier s'affichent.

2. Sélectionnez l'une des options suivantes :

- **Synchroniser une seule fois** - lorsque la session est lancée : indique que la disposition du clavier n'est synchronisée avec le VDA qu'une seule fois au lancement de la session. Le mode de saisie au clavier Unicode est l'option recommandée pour le mode Synchroniser une seule fois –lorsque la session est lancée.
- **Autoriser la synchronisation dynamique** : indique que la disposition du clavier est synchronisée dynamiquement avec le VDA lorsque le clavier client est modifié dans une session. Le mode de saisie au clavier Unicode est l'option recommandée pour le mode Autoriser la synchronisation dynamique.
- **Ne pas synchroniser** : indique que le client utilise la disposition du clavier du serveur, quelle que soit la disposition du clavier sélectionnée dans le client. Le mode de saisie au clavier Scancode est l'option recommandée pour l'option **Ne pas synchroniser**. Vous devez vous assurer que la disposition du clavier du client est la même que celle du VDA si vous configurez l'option Unicode pour **Ne pas synchroniser**.

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, vous pouvez 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

Langue sur Mac	Source d'entrée sur Mac	Version de Mac OS applicable
Anglais	ABC	Tous
Anglais	ABC - Inde	Tous
Anglais	U.S.	Tous

Langue sur Mac	Source d'entrée sur Mac	Version de Mac OS applicable
Anglais	U.S. International - PC	Tous
Anglais	Dvorak	Tous
Anglais	Dvorak - Gaucher	Tous
Anglais	Dvorak - Droitier	Tous
Anglais	Anglais - R.U.	Tous
Anglais	Britannique - PC	Tous
Anglais	Anglais canadien	Tous
Anglais	Australien	Tous
Anglais	Irlandais	Tous
Français	Français	Tous
Français	Français - Numérique	Tous
Français	Français canadien - CSA	11, 12
Français	Canadien - CSA	13
Français	Français - Suisse	Tous
Français	Français - PC	Tous
Allemand	Allemand	Tous
Allemand	Autrichien	Tous
Allemand	Allemand - Suisse	Tous
Espagnol	Espagnol	Tous
Espagnol	Espagnol - ISO	10, 11
Espagnol	Espagnol - Ancien clavier	12, 13
Espagnol	Espagnol - Amérique Latine	Tous
Suédois	Suédois	Tous
Suédois	Suédois - Ancien clavier	12, 13
Suédois	Suédois - Pro	10, 11
Tchèque	Tchèque	Tous
Danois	Danois	Tous
Finnois	Finnois	Tous
Hongrois	Hongrois	Tous

Langue sur Mac	Source d'entrée sur Mac	Version de Mac OS applicable
Italien	Italien	Tous
Italien	Italien - Machine à écrire	10, 11
Italien	Italien —QZERTY	12, 13
Grec	Grec	Tous
Néerlandais	Belge	Tous
Néerlandais	Néerlandais	Tous
Russe	Russe	Tous
Russe	Russe - PC	Tous
Croate	Croate - PC	Tous
Slovaque	Slovaque	Tous
Slovaque	Slovaque - QWERTY	Tous
Turc	Turc F	Tous
Turc	Turc Q	Tous
Portugais	Brésilien	Tous
Portugais	Brésilien - ABNT2	Tous
Portugais	Brésilien - Ancien clavier	12, 13
Portugais	Brésilien - Pro	10, 11
Portugais	Portugais	Tous
Ukrainien	Ukrainien - PC	10, 11
Ukrainien	Ukrainien	12, 13
Biélorusse	Biélorusse	Tous
Slovène	Slovène	Tous
Estonien	Estonien	Tous
Letton	Letton	Tous
Polonais	Polonais - Pro	10, 11
Polonais	Polonais	12, 13
Islandais	Islandais	Tous
Norvégien	Norvégien	Tous
Japonais	Katakana	Tous

Langue sur Mac	Source d'entrée sur Mac	Version de Mac OS applicable
Japonais	Katakana demi-largeur	Tous
Japonais	Romaji	Tous
Japonais	Romaji pleine largeur	Tous
Japonais	Hiragana	Tous
Japonais	Alphanumérique (Google)	Tous
Japonais	Hiragana (Google)	Tous
Japonais	Katakana (Google)	Tous
Japonais	Katakana demi-largeur (Google)	Tous
Japonais	Alphanumérique pleine largeur (Google)	Tous
Coréen	Coréen 2-set	Tous
Chinois, Simplifié	Pinyin - Simplifié	Tous
Chinois, Simplifié	Sogou Pinyin	Tous
Chinois, Traditionnel	Pinyin - Traditionnel	Tous
Chinois, Traditionnel	Cangjie - Traditionnel	Tous
Chinois, Traditionnel	Zhuyin - Traditionnel	Tous
Chinois, Traditionnel	Sucheng - Traditionnel	Tous

Prise en charge de la disposition du clavier pour VDA Linux, Suisse romand

Langue sur Mac	Source d'entrée sur Mac	Version de Mac OS applicable
Anglais	ABC	Tous
Anglais	ABC - Inde	Tous
Anglais	U.S.	Tous
Anglais	U.S. International - PC	Tous
Anglais	Dvorak	Tous
Anglais	Dvorak - Gaucher	Tous
Anglais	Dvorak - Droitier	Tous

Langue sur Mac	Source d'entrée sur Mac	Version de Mac OS applicable
Anglais	Anglais - R.U.	Tous
Anglais	Britannique - PC	Tous
Anglais	Anglais canadien	Tous
Anglais	Australien	Tous
Anglais	Irlandais	Tous
Français	Français	Tous
Français	Français - Numérique	Tous
Français	Français canadien - CSA	11, 12
Français	Canadien - CSA	13
Français	Français - Suisse	Tous
Français	Français - PC	Tous
Allemand	Allemand	Tous
Allemand	Autrichien	Tous
Allemand	Allemand - Suisse	Tous
Espagnol	Espagnol	Tous
Espagnol	Espagnol - ISO	10, 11
Espagnol	Espagnol - Ancien clavier	12, 13
Espagnol	Espagnol - Amérique Latine	Tous
Bulgare	Bulgare	10, 11, 12
Bulgare	Bulgare —Standard	13
Suédois	Suédois	Tous
Suédois	Suédois - Ancien clavier	12, 13
Suédois	Suédois - Pro	10, 11
Tchèque	Tchèque	Tous
Danois	Danois	Tous
Finnois	Finnois	Tous
Hongrois	Hongrois	Tous
Italien	Italien	Tous
Italien	Italien - Machine à écrire	10, 11

Langue sur Mac	Source d'entrée sur Mac	Version de Mac OS applicable
Italien	Italien —QZERTY	12, 13
Grec	Grec	Tous
Belge	Belge	Tous
Néerlandais	Néerlandais	Tous
Roumain	Roumain - Standard	Tous
Russe	Russe	Tous
Russe	Russe - PC	Tous
Croate	Croate - PC	Tous
Slovaque	Slovaque	Tous
Slovaque	Slovaque - QWERTY	Tous
Turc	Turc F	Tous
Turc	Turc Q	Tous
Portugais	Brésilien	Tous
Portugais	Brésilien - ABNT2	Tous
Portugais	Brésilien - Ancien clavier	12, 13
Portugais	Brésilien - Pro	10, 11
Portugais	Portugais	Tous
Ukrainien	Ukrainien - PC	10, 11
Ukrainien	Ukrainien	12, 13
Biélorusse	Biélorusse	Tous
Slovène	Slovène	Tous
Estonien	Estonien	Tous
Polonais	Polonais - Pro	10, 11
Polonais	Polonais	12, 13
Islandais	Islandais	Tous
Norvégien	Norvégien	Tous
Japonais	Katakana	Tous
Japonais	Katakana demi-largeur	Tous
Japonais	Romaji	Tous

Langue sur Mac	Source d'entrée sur Mac	Version de Mac OS applicable
Japonais	Romaji pleine largeur	Tous
Japonais	Hiragana	Tous
Japonais	Alphanumérique (Google)	Tous
Japonais	Hiragana (Google)	Tous
Japonais	Katakana (Google)	Tous
Japonais	Katakana demi-largeur (Google)	Tous
Japonais	Alphanumérique pleine largeur (Google)	Tous
Coréen	Coréen 2-set	Tous
Chinois, Simplifié	Pinyin - Simplifié	Tous
Chinois, Simplifié	Sogou Pinyin	Tous
Chinois, Traditionnel	Pinyin - Traditionnel	Tous
Chinois, Traditionnel	Cangjie - Traditionnel	Tous
Chinois, Traditionnel	Zhuyin - Traditionnel	Tous
Chinois, Traditionnel	Sucheng - Traditionnel	Tous

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.

Améliorations apportées au mode de saisie du clavier

L'application Citrix Workspace pour Mac fournit une interface utilisateur permettant de configurer le mode de saisie du clavier.

Pour configurer le mode de saisie du clavier à l'aide de l'interface graphique, procédez comme suit :

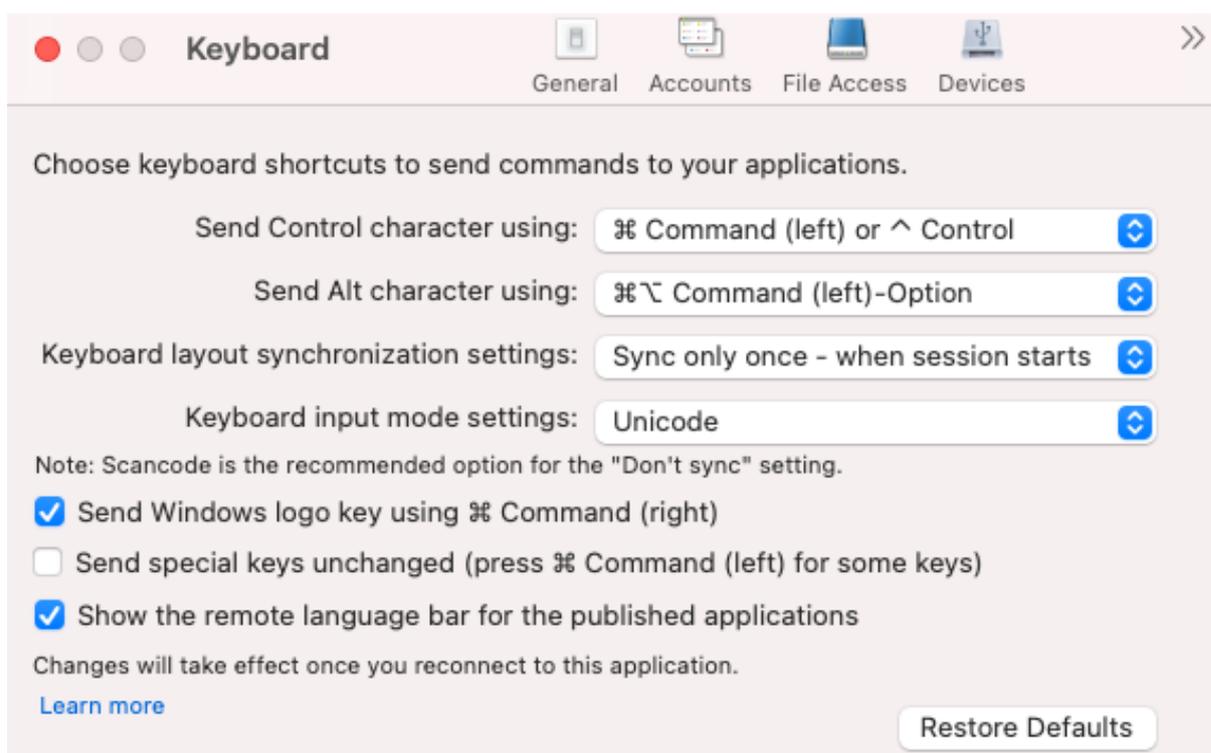
1. Depuis l'icône de l'application Citrix Workspace dans la barre de menu, cliquez sur l'icône du compte dans le coin supérieur droit et accédez à **Préférences > Clavier**.

Les paramètres du mode de saisie du clavier apparaissent.

2. Sélectionnez l'une des options suivantes :

- **Scancode** : la position des touches du clavier côté client est envoyée au VDA et le VDA génère le caractère correspondant. Applique la disposition du clavier côté serveur.
- **Unicode** : la touche du clavier côté client est envoyée au VDA et le VDA génère le même caractère dans le VDA. Applique la disposition du clavier côté client.

Cette amélioration est activée par défaut.



Par exemple, imaginez un scénario dans lequel vous utilisez une disposition de clavier international américain alors que le VDA utilise une disposition de clavier russe. Lorsque vous choisissez **Scancode** et que vous appuyez sur la touche à côté de **Verr Maj**, le code “1E” est envoyé au VDA. Le VDA utilise ensuite “1E” pour afficher le caractère “Ф”. Si vous choisissez **Unicode** et que vous appuyez sur la touche à côté de **Verr Maj**, le caractère “a” est envoyé au VDA. Ainsi, même si le VDA utilise la disposition du clavier russe, le caractère “a” apparaît à l’écran.

Citrix recommande le mode de saisie au clavier suivant pour les différentes options de synchronisation de la disposition du clavier :

- Mode Scancode pour l’option **Ne pas synchroniser**.
- Mode Unicode pour **Autoriser la synchronisation dynamique** et **Synchroniser une seule fois - lorsque la session est lancée**.

Remarque :

Les modifications de configuration du clavier prennent effet une fois que vous vous reconnectez à l'application.

Vous pouvez modifier la configuration du mode de saisie du clavier dans l'interface utilisateur de l'application Citrix Workspace. Toutefois, pour bénéficier de performances optimales, utilisez les modes recommandés par Citrix pour différents scénarios, les claviers physiques et les appareils clients.

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.

Synchronisation pour un plus grand nombre de dispositions de clavier

À compter de la version 2304, l'application Citrix Workspace pour Mac prend en charge la synchronisation de la disposition du clavier pour les modèles ou éditeurs de méthodes de saisie (IME) suivants :

- ABC anglais
- ABC anglais - Inde

- Chinois, Traditionnel : Zhuyin - Traditionnel
- Chinois, Traditionnel : Sucheng - Traditionnel
- Google Japanese IME
- Sougou Chinese IME

Dispositions de clavier des éditeurs de méthodes d'entrée (IME) dans une langue autre que l'anglais

La prise en charge des dispositions de clavier IME dans une langue autre que l'anglais continue de fonctionner sans interruption après que les API Carbon sont devenues obsolètes au profit des API Cocoa.

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
Clé <code>Alt+character</code>	Clé <code>Command-Option-character</code> (par exemple, pour envoyer <code>Alt-C</code> , utiliser <code>Command-Option-C</code>)
Clé <code>Alt+special</code>	Clé <code>Option-special</code> (par exemple, <code>Option-Tab</code>) ; clé <code>Command-Option-special</code> (par exemple, <code>Command-Option-Tab</code>)

Touche Windows ou combinaison de touches	Équivalents sur Mac
Clé Ctrl+character	Clé Command-character (par exemple, Command-C) ; clé Control-character (par exemple, Control-C)
Clé Ctrl+special	Clé Control-special (par exemple, Control-F4) ; clé Command-special (par exemple, Command-F4)
Clé Ctrl/Alt/Shift/Windows logo + fonction	Choisir le clavier > Envoyer une touche de fonction > Clé Control/Alt/Shift/Command-Fonction
Ctrl+Alt	Control-Option-Command
Ctrl+Alt+Delete	Control-Option-Fn-Command-Delete ; Choisir le clavier > Envoyer Ctrl-Alt-Suppr
Delete	Delete ; Choisir Clavier > Envoyer une touche > Supprimer ; Fn-Backspace (Fn-Delete sur certains claviers américains)
End	End ; Fn-Right Arrow
Esc	Escape ; Choisir le clavier > Envoyer une touche > Échap
F1 à F12	F1 à F12 ; Choisir le clavier > Envoyer une touche de fonction > F1 à F12
Home	Home ; Fn-Left Arrow
Insert	Choisir Clavier > Envoyer une touche > Insérer
Num Lock	Clear
Page Down	Page Down ; Fn-Down Arrow
Page Up	Page Up ; Fn-Up Arrow
Spacebar	Choisir Clavier > Envoyer une touche > Espace
Tab	Choisir Clavier > Envoyer une touche > Tab
Windows logo	Touche de Command (droite) (préférence de clavier, activée par défaut) ; Choisir Clavier > Envoyer le raccourci Windows > Démarrer
Combinaison de touches pour afficher les icônes	Choisir Clavier > Envoyer le raccourci Windows > Icônes

Touche Windows ou combinaison de touches	Équivalents sur Mac
Combinaison de touches pour afficher les commandes d'application	Choisir Clavier > Envoyer le raccourci Windows > Commandes d'application
Combinaison de touches pour ancrer les applications	Choisir Clavier > Envoyer le raccourci Windows > Ancrer
Combinaison de touches pour basculer entre les applications	Choisir 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 côté 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 côté 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 côté 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 côté client et serveur utilisent les mêmes paramètres régionaux que ceux de la langue d'entrée par défaut du côté serveur.

Restaurer les paramètres de clavier par défaut

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**. Cliquez ensuite sur **Restaurer paramètres par défaut**, puis sur **Oui** pour confirmer.

Fin de la prise en charge du menu International dans les paramètres du clavier

Auparavant, vous pouviez activer ou désactiver les fonctionnalités **Utiliser l'éditeur IME du client**, **Utiliser marques de composition** et **Utiliser disposition du clavier client** dans Citrix Viewer en accédant à **Appareils > Clavier > International**.

À partir de la version 2311, le menu **International** pour les paramètres du clavier dans Citrix Viewer n'est plus pris en charge. À partir de cette version, l'éditeur IME côté client est activé par défaut.

Prise en charge des raccourcis système sur les sessions de bureau HDX

Auparavant, les raccourcis clavier du système tels qu'**Option-Commande-Echap**, **Commande-Touche espace**, **Command-Tab**, **Contrôle-Commande-Q**, **Maj-Commande-Q**, **Contrôle flèche**

haut/bas/gauche/droite ne s'appliquaient que sur macOS localement, puisqu'ils étaient utilisés uniquement par macOS.

À partir de la version 2402, l'application Citrix Workspace pour Mac prend en charge la transmission des raccourcis clavier du système macOS au VDA (session HDX) en mode fenêtre et en mode plein écran. Cette fonctionnalité vous permet de définir des préférences d'application du raccourci système sur macOS localement ou sur la session de bureau HDX en mode fenêtre ou plein écran.

Les options suivantes des paramètres du clavier vous permettent de contrôler les raccourcis système :

- **Périphérique local** : les raccourcis système ne peuvent être appliqués que sur macOS localement. Cela n'affecte pas la session HDX. L'option **Périphérique local** est l'option par défaut.
- **Session HDX en plein écran uniquement** : les raccourcis système sont appliqués sur les sessions HDX lorsque la session est en mode plein écran. Si la session est en mode fenêtre ou s'il n'y a aucune session active, les raccourcis système ne s'appliquent pas sur les sessions HDX.
- **Session HDX active** : les raccourcis système sont appliqués sur les sessions HDX lorsque la session est en mode fenêtre et en mode plein écran. S'il n'y a pas de session HDX active ou s'il n'y a pas de fenêtre de session active sur la face avant, les raccourcis système ne peuvent être appliqués que sur macOS localement.

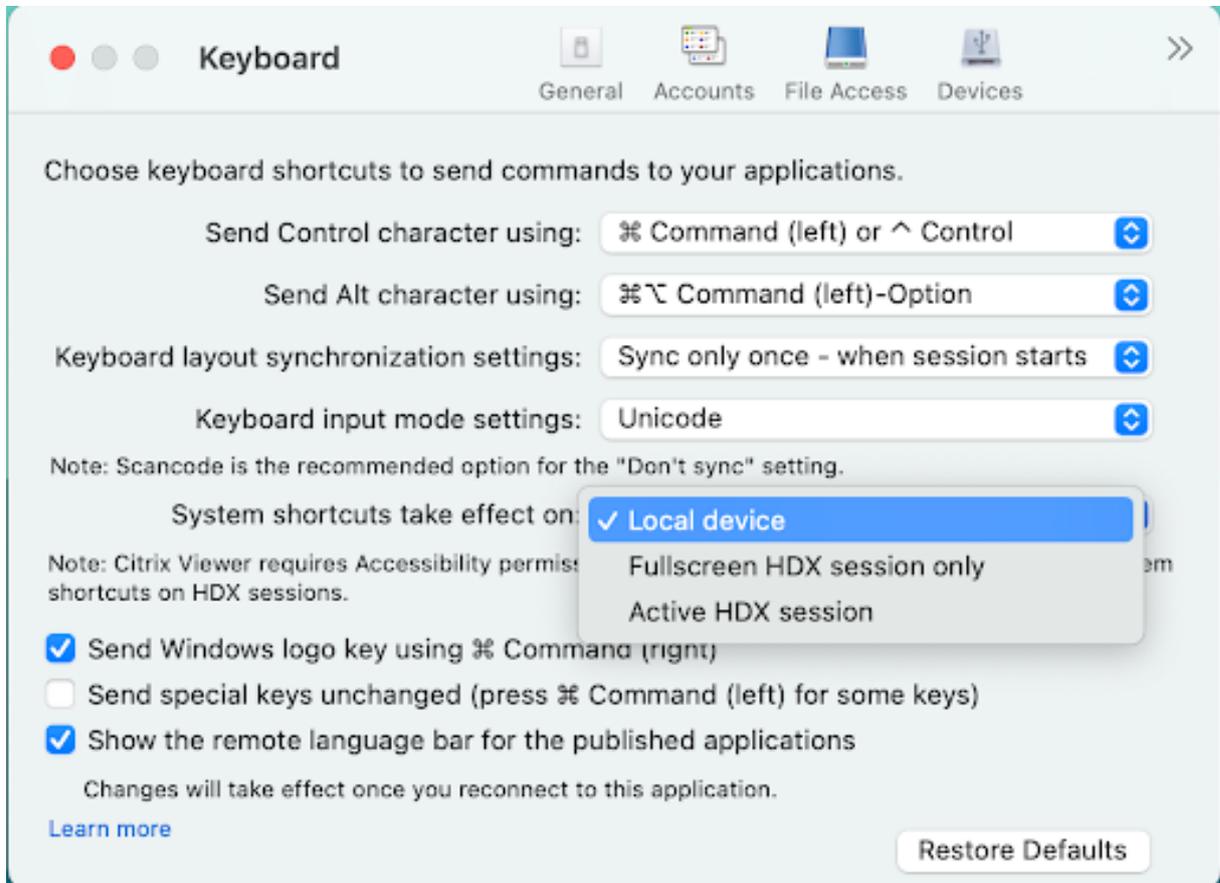
Pour que les raccourcis système soient appliqués sur la session HDX, ouvrez la session HDX. Dans la barre de menus de **Citrix Viewer**, accédez à **Périphériques > Clavier > Les raccourcis système prennent effet sur** et sélectionnez **Session HDX plein écran uniquement** ou **Session HDX active**.

Remarque :

Lorsque vous activez les raccourcis système pour les sessions HDX, vous êtes invité à fournir un accès en accessibilité à Citrix Viewer pour utiliser cette fonctionnalité. Pour fournir un accès en accessibilité à **Citrix Viewer**, cliquez sur **Ouvrir les paramètres système** dans la boîte de dialogue et activez l'accès en accessibilité à **Citrix Viewer**. Pour plus d'informations, consultez la section [Autoriser des apps d'accessibilité à accéder à votre Mac](#) dans l'article du support Apple.



Vous pouvez également activer les raccourcis système pour qu'ils soient appliqués aux sessions HDX en mode plein écran ou en mode fenêtre en accédant à **Préférences > Clavier**. Sélectionnez l'option **Session HDX en plein écran uniquement** ou **Session HDX active** dans le menu déroulant **Les raccourcis système prennent effet sur**.



Impression

February 2, 2024

À partir de la version 2203.1, vous pouvez utiliser l'impression universelle PDF lorsque vous imprimez à partir d'un périphérique Mac. Si vous avez choisi d'utiliser l'impression universelle PDF, 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'imprimante universelle.

Impression PostScript

Par défaut, les imprimantes clientes redirigées automatiquement sont créées avec le pilote UPD Citrix avec prise en charge PostScript.

Pour plus d'informations, consultez l'article d'assistance [CTX296662](#).

Vérifiez que les paramètres de priorité du pilote d'imprimante universelle, d'utilisation du pilote d'imprimante universelle et de redirection d'imprimante cliente sont tous définis 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

Logiciels 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.

	> Auto-create PDF Universal Printer User setting - ICA\Printing\Client Printers Enabled (Default: Disabled)	Edit	Unselect
	> Auto-create client printers User setting - ICA\Printing\Client Printers Auto-create all client printers (Default: Auto-create all client printers)	Edit	Unselect
	> Client printer redirection User setting - ICA\Printing Allowed (Default: Allowed)	Edit	Unselect
	> Universal driver preference **** User setting - ICA\Printing\Drivers EMF,XPS,PCL5c,PCL4,PDF,PS (Default: EMF;XPS;PCL5c;PCL4;PS)	Edit	Unselect
	> Universal print driver usage User setting - ICA\Printing\Drivers Use universal printing only if requested driver is unavailable (Default: Use u...	Edit	Unselect

**** "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**.

Utilisez cette imprimante lors d'une session afin de générer une sortie PDF à transmettre au client. Envoyez également la sortie PDF à l'application de gestion des PDF par défaut sur le point de terminaison. Pour le client macOS, il s'agit généralement de l'application **Aperçu** intégrée, mais il pourrait 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 au cours d'une session, rendez-vous sur Citrix Studio ou sur une console Web depuis un client Mac. Configurez ensuite la stratégie de priorité du pilote d'imprimante universelle pour placer le format de métafichier PDF avant PS dans la liste des priorités.

Après cette configuration, le pilote d'imprimante universelle PDF Citrix remplace le pilote HP Color LaserJet 2800 Series PS sur l'hôte pour les imprimantes créées automatiquement. Les imprimantes créées automatiquement utilisent un pilote universel avec un client Mac capable d'imprimer des PDF. 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. Cependant, la sortie d'impression est directement transmise à l'imprimante connectée au client sélectionnée.

USB

February 2, 2024

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.

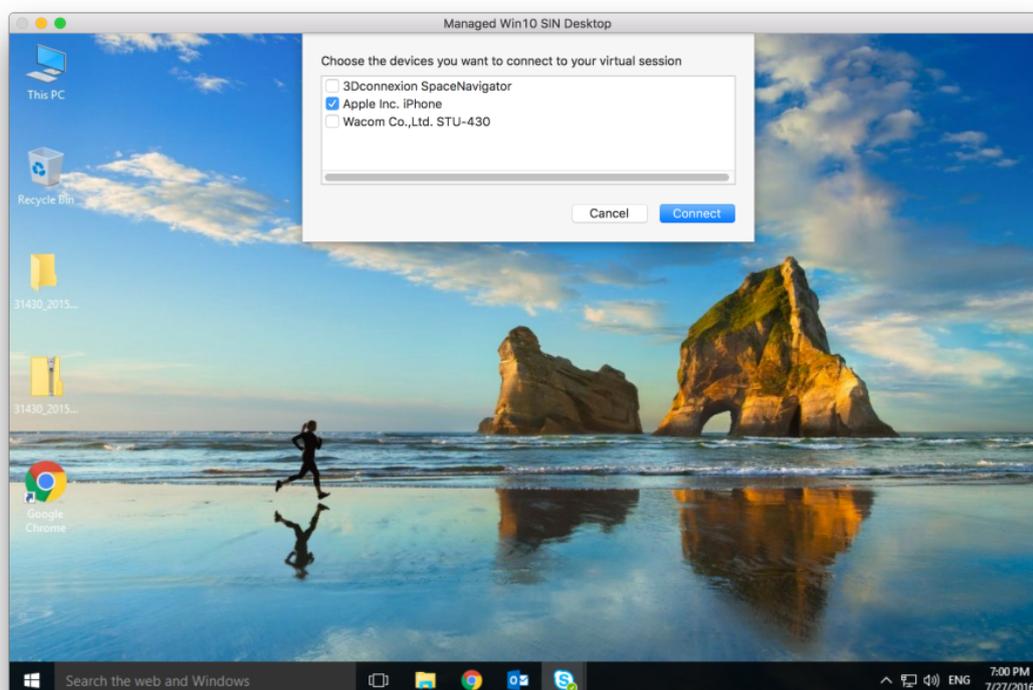
Le produit prend en charge les canaux virtuels optimisés avec des périphériques USB 3.0 et des ports USB 3.0. Par exemple, un canal virtuel CDM est utilisé pour afficher des fichiers sur une caméra ou pour fournir de l'audio à un casque. Le produit prend également en charge la redirection USB générique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

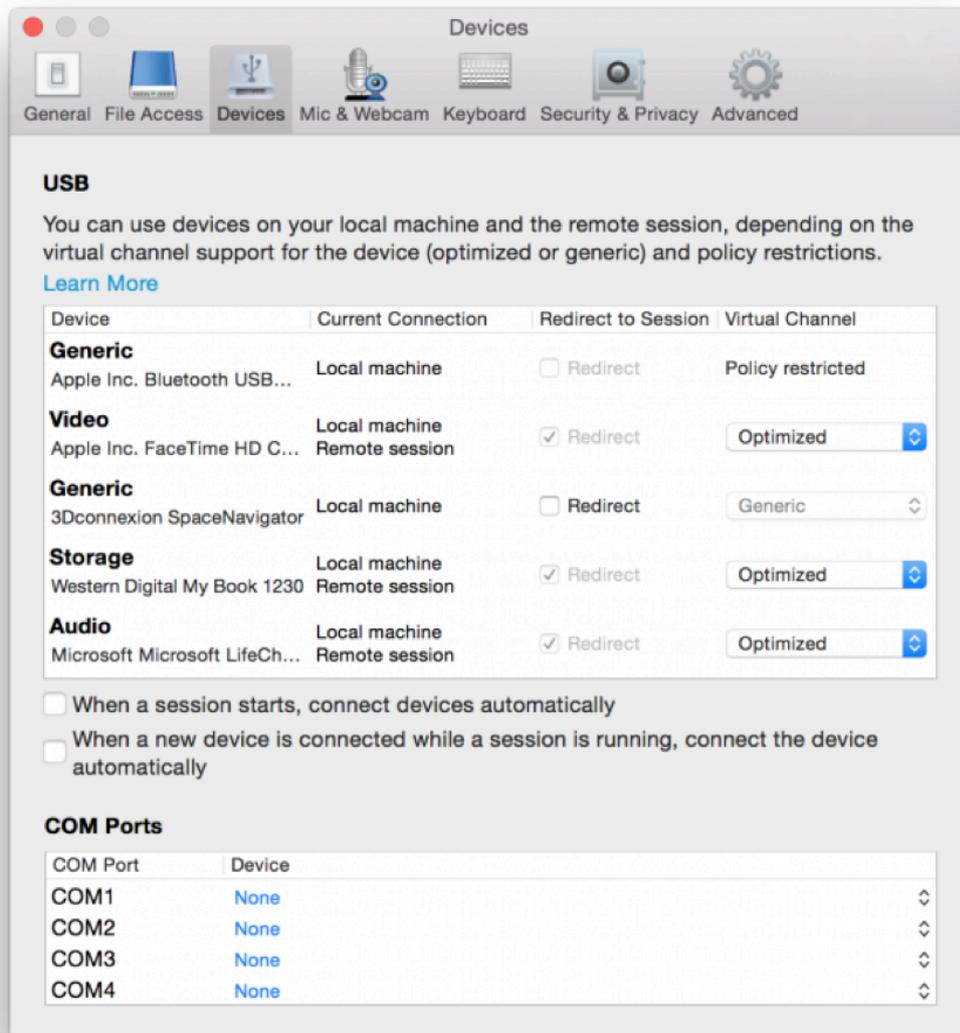
Certains périphériques ne sont pas redirigés par défaut et sont uniquement disponibles pour la session locale. Par exemple, il n'est pas approprié de rediriger une carte d'interface réseau qui est directement connectée via USB interne.

Pour utiliser la redirection USB :

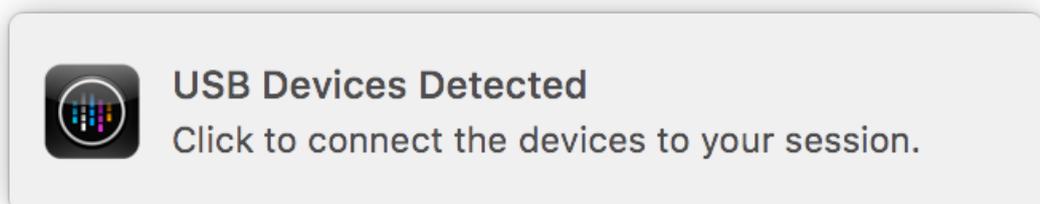
1. Connectez le périphérique USB à l'appareil sur lequel l'application Citrix Workspace pour Mac est installée.
2. Vous êtes invité à sélectionner les périphériques USB disponibles sur votre système local.



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 **Disque dur externe SSD Transcend** n'est pas compatible avec la redirection USB :

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 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.

Webcam

May 16, 2024

Prise en charge de l'appareil photo Continuité

À partir de la version 2305, vous pouvez utiliser l'iPhone comme webcam avec l'appareil photo Continuité. Pour une connexion fluide, installez votre iPhone de telle sorte que son appareil photo soit accessible à l'appareil Mac. Vous devez sélectionner **Webcam > Sélection automatique de la caméra** pour que l'iPhone apparaisse automatiquement sur l'appareil Mac en tant que caméra externe. Vous pouvez passer manuellement à n'importe quelle autre caméra, par exemple en sélectionnant **Webcam > Caméra FaceTime HD**. L'appareil photo Continuité fonctionne avec ou sans fil et fournit une image de haute qualité.

Logiciels requis

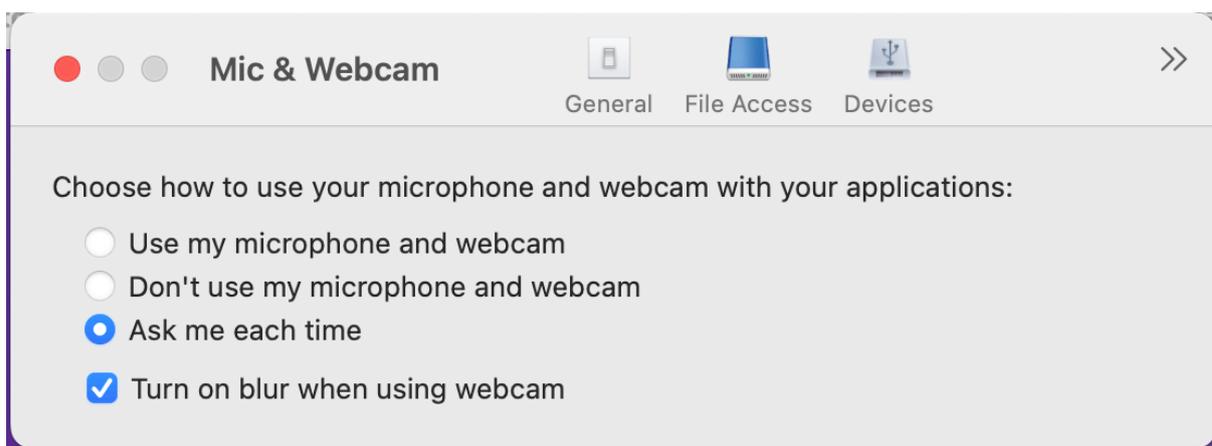
- Cette fonctionnalité est prise en charge sur les appareils Mac exécutant la version 13 de macOS.
- Cette fonctionnalité est prise en charge sur les appareils iOS exécutant la version 16 d'iOS.
- Vous devez être connecté au même compte Apple dans l'application Citrix Workspace sur votre appareil iOS et votre Mac.
- Pour une connexion filaire, l'iPhone doit être connecté à l'appareil Mac via un port USB.
- Pour une connexion sans fil, les appareils iPhone et Mac doivent se trouver à proximité et le Bluetooth et le Wi-Fi doivent être activés.

Certains des avantages sont les suivants :

- **Cadre centré** : conserve l'image dans le cadre lorsque vous vous déplacez.
- Mode **Portrait** : estompe l'arrière-plan de l'image.
- **Éclairage de studio** : produit un effet lumineux sur l'image. Il assombrit l'arrière-plan et illumine l'image.
- **Desk View** : l'iPhone divise le flux de caméra ultra grand angle en deux. Il montre le bureau et le visage en même temps.
- **Partage de fenêtres** : l'iPhone divise le flux de caméra ultra grand angle en deux. Il montre le bureau et le visage en même temps. La fonction de partage de fenêtres disponible dans les applications de visioconférence peut être utilisée pour partager le flux Desk View.

Prise en charge du flou d'arrière-plan pour la webcam

À partir de la version 2402, l'application Citrix Workspace pour Mac prend en charge le flou d'arrière-plan lors de l'utilisation d'une webcam. Vous pouvez activer la fonctionnalité de flou d'arrière-plan en accédant à **Préférences > Micro et webcam** et en sélectionnant **Activer le flou lorsque vous utilisez la webcam**.



Expérience de session

February 2, 2024

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 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 :

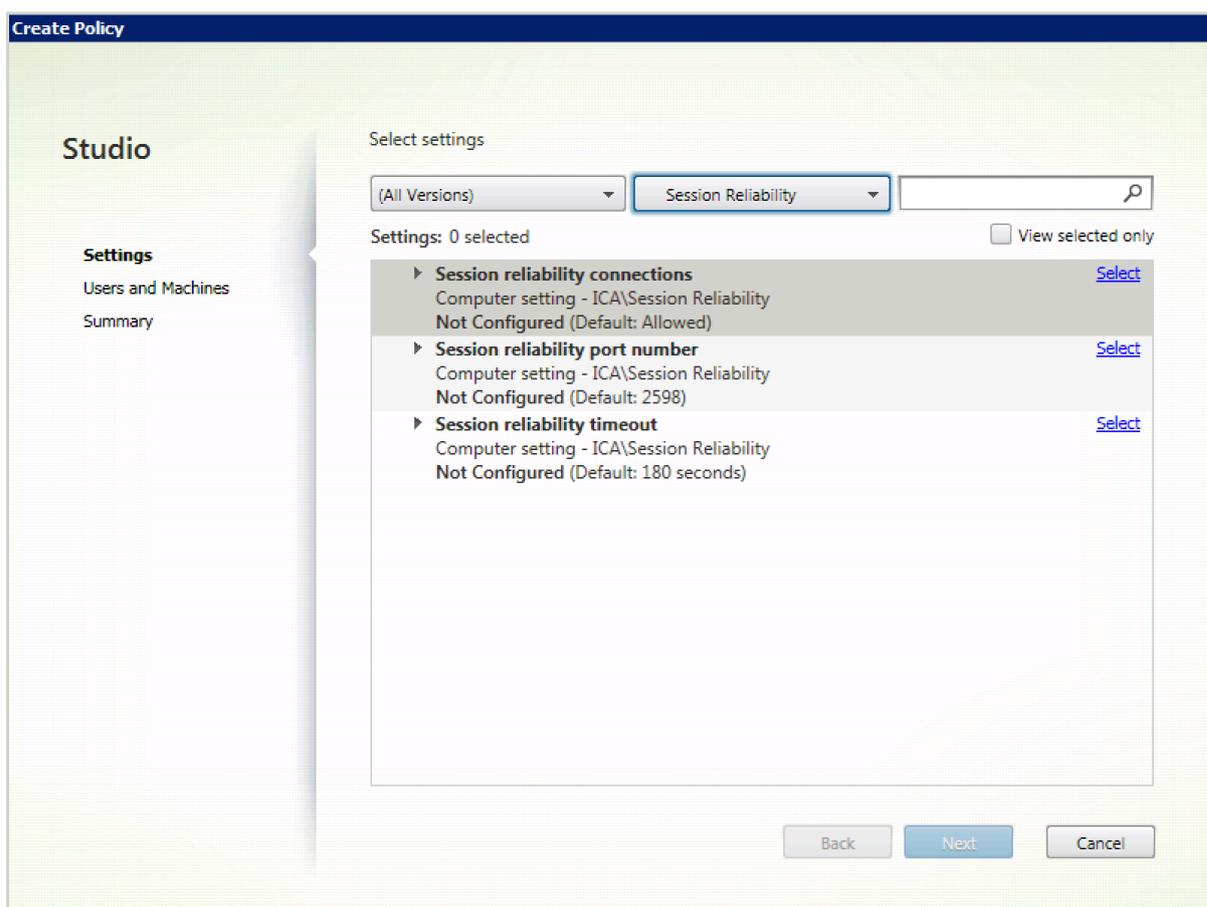
La fiabilité de session est activée par défaut au niveau du serveur. Pour désactiver cette fonctionnalité, configurez la stratégie gérée par le serveur.

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 :

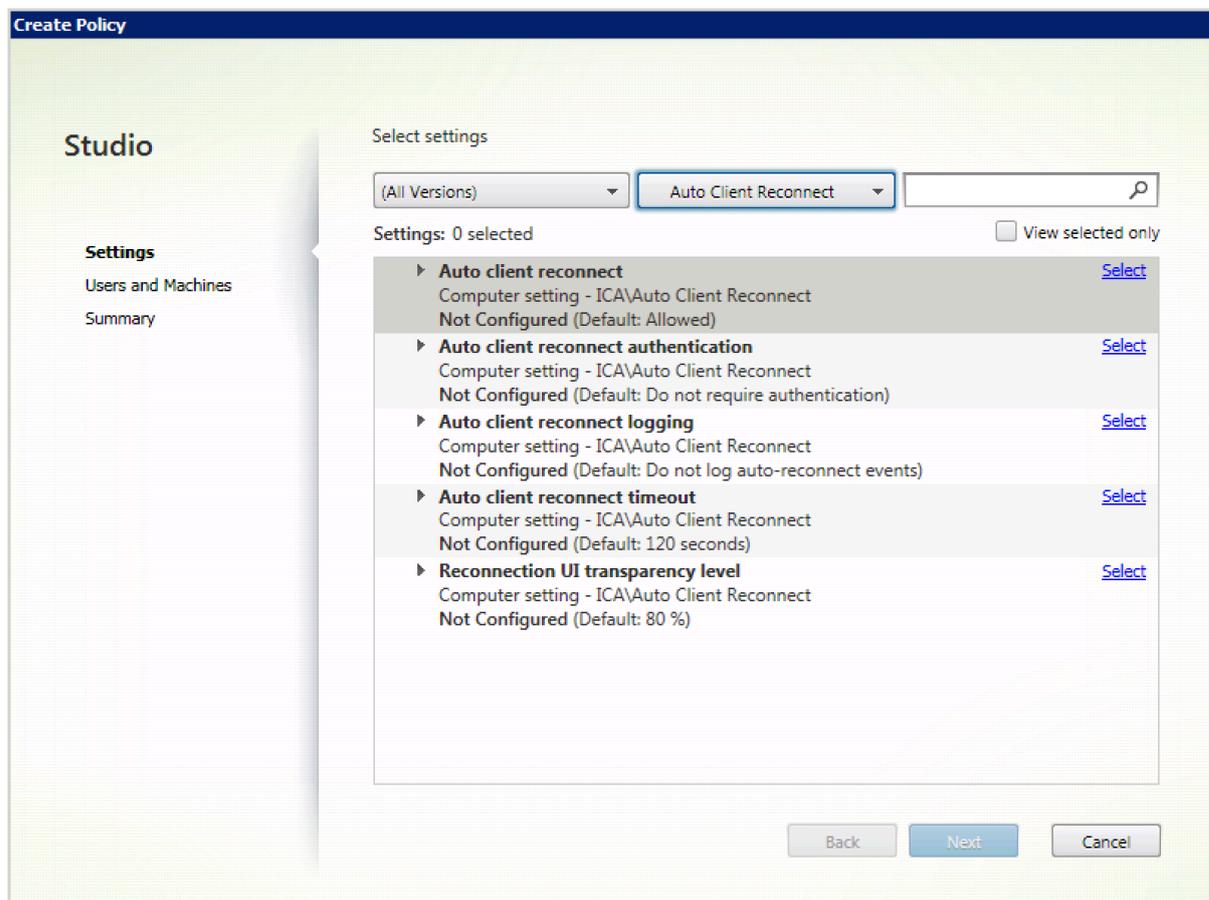
1. Lancez Citrix Studio.
2. Ouvrez la stratégie **Expiration de délai de la fiabilité de session**.
3. Modifiez la valeur du délai d'expiration.
4. Cliquez sur **OK**.

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**.

Limites :

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 modifi-

cation de cette stratégie, reportez-vous à la section Reconnexion automatique des clients plus haut dans cet article.

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

Paramètre	Exemple	Valeur par défaut
<code>TransportReconnectRetryMaxTSecs</code>	<code>TransportReconnectRetryMaxTSecs=60</code>	120

Fiabilité de session

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

Utilisez le fichier **default.ica** dans StoreFront pour modifier le délai d'expiration de la connexion pour la fiabilité de session. Par défaut, ce délai d'expiration est défini sur 180 secondes, ou trois minutes.

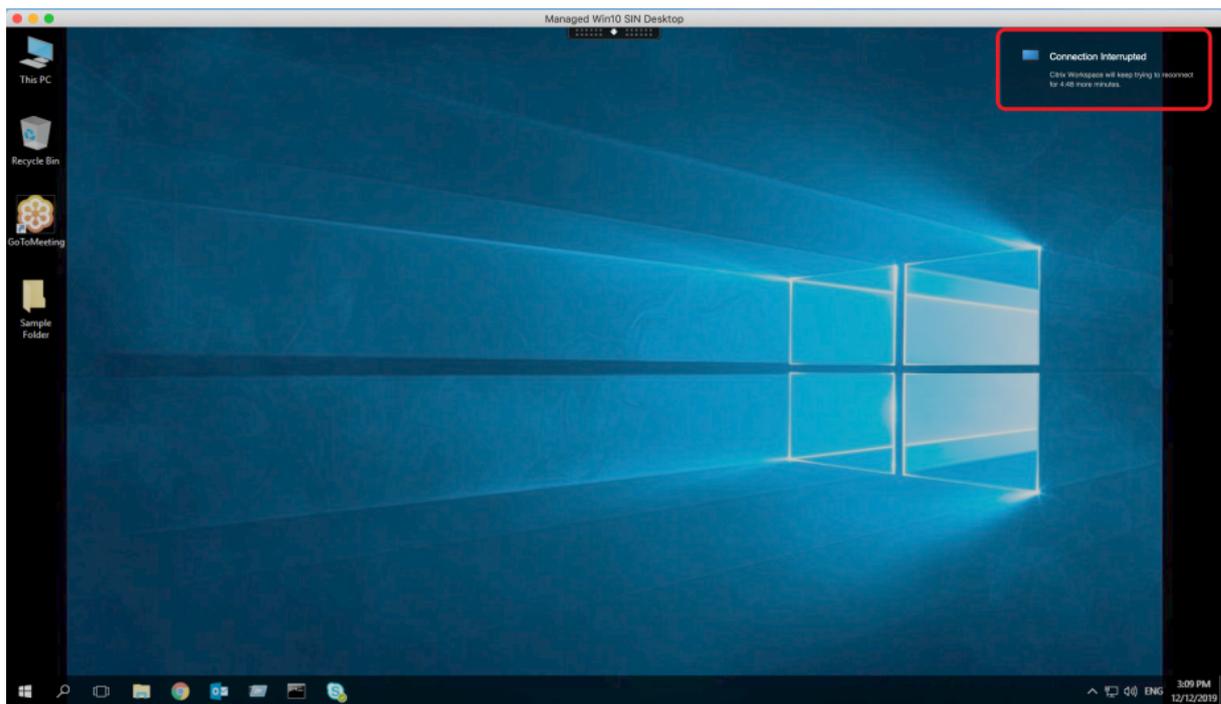
Paramètre	Exemple	Valeur par défaut
<code>SessionReliabilityTTL</code>	<code>SessionReliabilityTTL=120</code>	180

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.

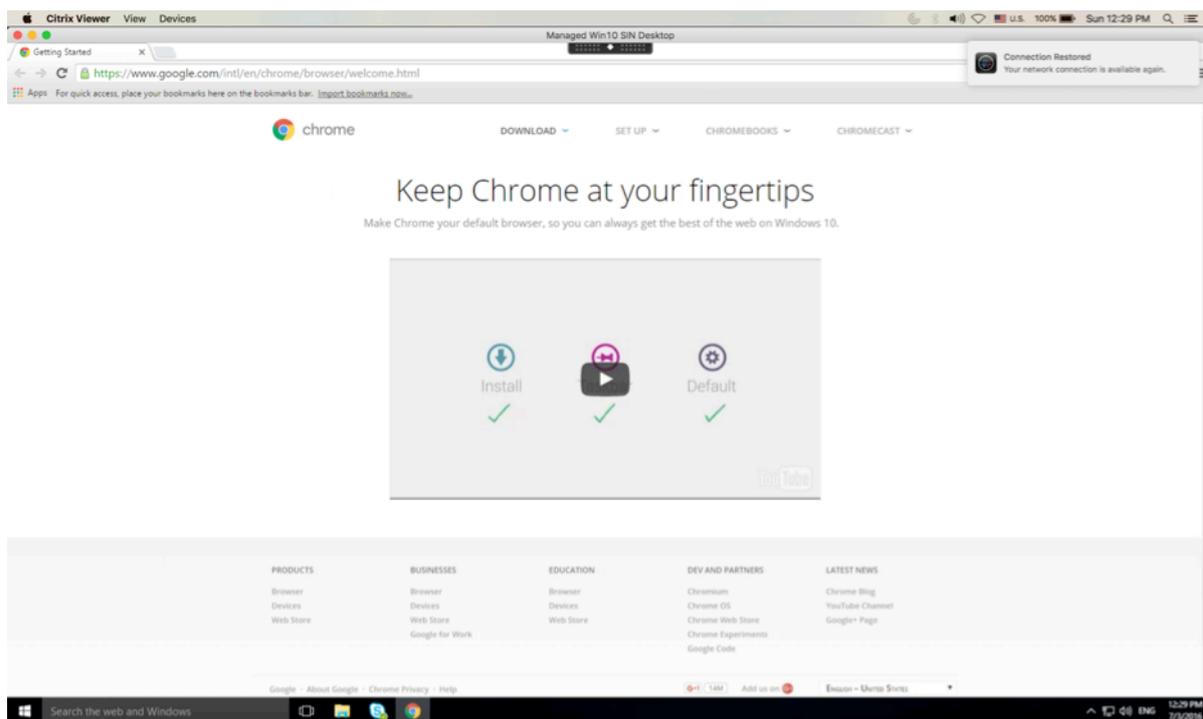
Par défaut, la notification de reconnexion commence après 5 minutes. Cette valeur représente les valeurs combinées de chacun des minuteurs (reconnexion automatique des clients et fiabilité de session), respectivement 2 et 3 minutes. L'image suivante illustre la notification qui s'affiche dans la partie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

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.

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

À partir de la version 2206.1, la fonctionnalité de continuité du service Citrix Workspace est 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](#).

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

À partir de la version 2204, si vous exécutez des licences d'accès client dans votre environnement pour accéder à des bureaux distants, lorsque l'ID client est supérieur à 15 caractères, vous pouvez lancer la session de bureau distant 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
```

Dépannage

June 26, 2024

Envoi de commentaires sur l'application Citrix Workspace

À partir de la version 2307, l'application Citrix Workspace pour Mac prend en charge la fonctionnalité **Envoyer des commentaires**. L'option Envoyer des commentaires vous permet d'informer Citrix de tout problème que vous pourriez rencontrer lors de l'utilisation de l'application Citrix Workspace. Vous pouvez également envoyer des suggestions pour nous aider à améliorer votre expérience avec l'application Citrix Workspace.

Vous devez sélectionner **Aide > Envoyer des commentaires** pour afficher et renseigner les détails du problème dans le formulaire de commentaires. Vous pouvez ajouter des détails tels que les exemples fournis dans le formulaire.

Send feedback

Provide a descriptive title*

Tell us more*

Include details such as:

- What you expected to happen
- What actually happened
- Steps to recreate the issue

Logs

Basic logs are attached. We recommend you click 'Record my issue' to capture detailed logs.

For more information, see [Log collection](#)

[Record my issue](#) WorkspaceLogs_2023_07_18-14_23_43.zip 

Attachments

Screenshots or screen recordings of the problem.

[Choose files](#) (Max 4 files)

Your feedback will be used to improve Citrix Workspace app. If you don't use the Mail app on your Mac, please send feedback to **cwa-mac-feedback@cloud.com** with files added manually.

[Send](#) [Cancel](#)

Vous pouvez joindre les fichiers journaux existants ou générer de nouveaux fichiers journaux. Pour générer des fichiers journaux, cliquez sur **Enregistrer mon problème > Démarrer l'enregistrement**, puis reproduisez le problème. Une fois le problème reproduit, cliquez sur **Arrêter l'enregistrement**. Le fichier journal est enregistré automatiquement et remplace les journaux existants par les journaux reproduits.

Remarque :

Citrix ne recueille aucune information permettant de vous identifier personnellement à partir des journaux.

Vous pouvez joindre des captures d'écran ou des enregistrements d'écran décrivant le problème pour nous aider à comprendre le problème que vous rencontrez. Cliquez sur **Choisissez des fichiers** et

ajoutez les pièces jointes décrivant vos problèmes, telles que des captures d'écran ou des enregistrements d'écran. Vous pouvez joindre un maximum de quatre fichiers.

Une fois que vous avez saisi les informations nécessaires, cliquez sur **Envoyer** pour qu'un nouvel e-mail soit automatiquement créé dans votre application de messagerie avec les informations que vous avez ajoutées. À partir de là, cliquez sur le bouton **Envoyer** pour partager les commentaires à Citrix.

Remarque :

Si vous n'utilisez pas l'application de messagerie par défaut, envoyez vos commentaires à cwa-mac-feedback@cloud.com depuis votre client de messagerie. Ajoutez manuellement les détails du problème, les fichiers journaux, les captures d'écran ou les enregistrements d'écran à l'e-mail.

Collecte de journaux

À partir de la version 2304, l'application Citrix Workspace pour Mac prend en charge la fonctionnalité **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.

À partir de la version 2402, la fonctionnalité de collecte de journaux a été améliorée et permet de collecter et envoyer par e-mail des données de journal supplémentaires. Grâce à cette fonctionnalité, vous pouvez facilement collecter toutes les informations de journal requises en une seule fois.

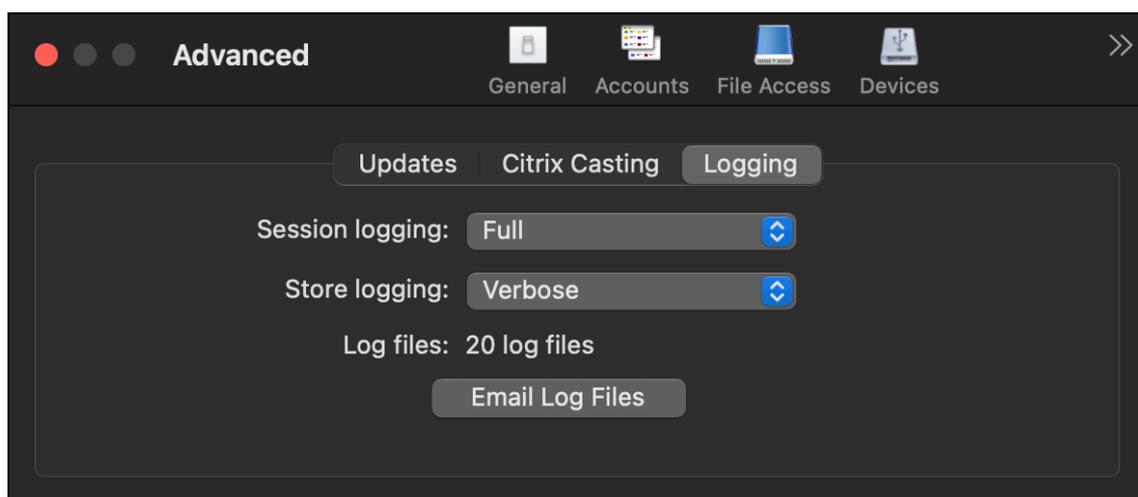
Les données de journal supplémentaires suivantes sont collectées :

- Rapport d'incident pour Citrix Process
- Fichiers associés à Citrix dans les préférences
- Fichiers associés à Citrix `launchagents` et `launchdaemons`
- Fichiers associés à Citrix dans l'application ou dans Citrix Receiver

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 minimaux 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 (par défaut)** : des journaux minimaux 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.

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/>].

Fin de prise en charge

April 17, 2024

Cet article vous informe à l'avance de l'élimination progressive de plates-formes, de produits Citrix et de fonctionnalités afin que vous puissiez prendre les décisions appropriées. Citrix surveille l'utilisation des clients et leurs commentaires pour déterminer quand les retirer. Les annonces peuvent être modifiées dans les versions ultérieures et peuvent ne pas contenir chaque fonctionnalité amenée à disparaître.

Les éléments obsolètes ne sont pas retirés immédiatement. Citrix continue de les prendre en charge dans cette version, mais ils seront retirés dans le futur.

Élément	Suppression	Abandon annoncé	Solution alternative
Prise en charge du format WebRTC SDP (Plan B)	À supprimer en février 2024	2311	Mettez à niveau l'application Citrix Workspace vers une version prise en charge.
Version macOS Big Sur (11)	Suppression prévue en mai 2024	September 2023 (2308)	Utilisez le système d'exploitation pris en charge comme indiqué dans la section Systèmes d'exploitation pris en charge .
Applications Citrix Workspace pour macOS (version Intel (x86))	Sera supprimé en avril 2024	April 2022 (2204)	Utilisez l'application Citrix Workspace pour macOS prenant en charge l'architecture universelle.

Élément	Suppression	Abandon annoncé	Solution alternative
macOS version Catalina (10.15)	Supprimé en juillet 2023 (2307)	April 2023 (2304)	Utilisez le système d'exploitation pris en charge comme indiqué dans la section Systèmes d'exploitation pris en charge .
Versions macOS High Sierra (10.13) et Mojave (10.14)	Supprimé en septembre 2020 (2009)	August 2020 (2008)	Passez à Big Sur 11 ou version ultérieure.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).