Application Citrix Workspace pour Windows

Contents

À propos de cette version

March 26, 2019

Nouveautés dans la version 1902

Amélioration apportée à la configuration de la souris relative

La fonctionnalité de la souris relative détermine la distance de déplacement de la souris depuis la dernière image dans une fenêtre ou un écran.
La souris relative utilise l'écart des pixels entre les mouvements de la souris. Par exemple, lorsque vous modifiez la direction de la caméra à l'aide des commandes de la souris, la fonctionnalité est efficace. En outre, les applications masquent souvent le curseur de la souris car la position du curseur par rapport aux coordonnées de l'écran n'est pas pertinente lors de la manipulation d'un objet ou d'une scène 3D.

Jusqu'à présent, l'utilisateur peut activer ou désactiver la fonctionnalité à partir de Desktop Viewer ; celle-ci est disponible par session. À partir de cette version, vous pouvez configurer la fonctionnalité à la fois par utilisateur et par session. Cela vous fournit un contrôle plus précis sur la disponibilité de la fonctionnalité.

Pour plus d'informations, veuillez consulter l'article Souris relative.

Présentation du nouveau SDK

Le SDK de déclaration d'identité de certificat est introduit avec cette version. Grâce au SDK de déclaration d'identité de certificat, les développeurs peuvent créer un utilitaire qui permet à l'application Citrix Workspace de s'authentifier auprès du serveur StoreFront à l'aide du certificat installé sur la machine cliente.

Pour de plus amples informations, consultez la documentation de Certificate Identity Declaration SDK for Citrix Workspace app for Windows..

Nouveautés de l'application Citrix Workspace 1812 pour Windows

Infrastructure mise à jour

L'infrastructure incorporée Chromium sur laquelle Citrix Secure Browser est construit a été mise à jour vers la version 70. Il en résulte une meilleure expérience utilisateur lors de l'accès aux applications SaaS sécurisées.

Nouveautés de l'application Citrix Workspace 1811 pour Windows

> **Remarque :**
>
> La version 1811 de l'application Citrix Workspace est fournie avec Citrix Virtual Apps and Desktops 7 1811. Il n'est pas possible de la télécharger séparément. Toutes les fonctionnalités de la version 1811 sont également incluses dans la version 1812.

Disposition d'affichage virtuel

Cette fonctionnalité vous permet de définir une disposition de moniteur virtuel qui s'applique au bureau distant et de diviser virtuellement un seul moniteur client en un maximum de huit moniteurs sur le bureau distant. Vous pouvez configurer les moniteurs virtuels dans l'onglet **Disposition du moniteur** de Desktop Viewer. Vous pouvez y dessiner des lignes horizontales ou verticales pour séparer l'écran en moniteurs virtuels. L'écran est divisé en fonction des pourcentages spécifiés pour la résolution du moniteur client.

Vous pouvez définir un DPI pour les moniteurs virtuels qui sont utilisés pour la mise à l'échelle ou la correspondance DPI. Après avoir appliqué une disposition de moniteur virtuel, redimensionnez ou reconnectez la session.

Cette configuration s'appliquera uniquement aux sessions de bureau sur un seul moniteur plein écran, et n'affectera
aucune application publiée. Cette configuration s'appliquera à toutes les connexions suivantes à partir de ce client.

Afficher indicateur de mode graphique

La stratégie d'affichage d'indicateur de mode graphique a été mise à jour pour remplacer la stratégie Afficher indicateur sans perte.

Ce paramètre configure l'indicateur de mode graphique à exécuter dans la session utilisateur. Il vous permet d'afficher des détails sur le mode graphique utilisé, y compris le fournisseur de graphiques, l'encodeur, le codage matériel, la qualité de l'image, l'état d'affichage progressif et le texte sans perte.

Par défaut, la stratégie **Afficher indicateur de mode graphique** est désactivée. Elle remplace la stratégie **Afficher indicateur sans perte** des versions précédentes, qui était activée par défaut.

Correspondance DPI sur Windows 10

La correspondance DPI permet à la session de bureau Windows 10 de correspondre au DPI du point de terminaison lors de l'utilisation de l'application Citrix Workspace pour Windows.

> **Remarque :**
>
> Cette option est désactivée par défaut. La correspondance DPI est activée chaque fois que le paramètre de mise à l'échelle DPI est défini sur **Non**. Lorsque vous utilisez des applications hébergées sur une machine virtuelle, le DPI est défini sur 100 % par défaut.

Débit adaptatif HDX

Le débit adaptatif HDX affine intelligemment le débit maximal de la session ICA en ajustant les tampons de sortie. Le nombre de tampons de sortie est initialement défini sur une valeur élevée. Cette valeur élevée permet de transmettre les données au client plus rapidement et efficacement, en particulier dans les réseaux à latence élevée.

Grâce à une meilleure interactivité, à des transferts de fichiers plus rapides, à une lecture vidéo plus fluide, à une fréquence d'images et à une résolution plus élevées, vous bénéficiez d'une meilleure expérience utilisateur.

L'interactivité des sessions est constamment mesurée pour déterminer si des flux de données au sein de la session ICA nuisent à l'interactivité. Si c'est le cas, le débit diminue pour réduire l'impact du flux de données volumineux sur la session et permettre la récupération de l'interactivité.

Cette fonctionnalité est prise en charge uniquement sur l'application Citrix Workspace 1811 pour Windows et versions ultérieures.

> **Important :**
>
> Le débit adaptatif HDX modifie la façon dont les tampons de sortie sont définis en déplaçant ce mécanisme du client vers le VDA. Par conséquent, l'ajustement du nombre de mémoires tampons de sortie sur le client, tel que décrit dans l'article CTX125027, n'a aucun effet.

Amélioration des performances du mappage des lecteurs clients

Le mappage des lecteurs clients prend désormais en charge le transfert de données entre l'hôte et le client en tant que flux. Cette amélioration garantit que le transfert de fichier s'adapte aux conditions de débit changeantes du réseau. Il utilise également toute bande passante supplémentaire disponible pour augmenter le taux de transfert de données.

Cette fonctionnalité est activée par défaut. Ces améliorations nécessitent l'application Citrix Workspace pour Windows 1811 ou version ultérieure.

Pour désactiver cette fonctionnalité, définissez la clé de registre suivante, puis redémarrez le serveur :

Chemin :`HKEY_LOCAL_MACHINE\System\Currentcontrolset\services\picadm\Parameters`

Nom :`DisableFullStreamWrite`

Type : REG_DWORD
Valeur :
`0x01`- désactive
`0`ou supprime - active

Nouveautés de l'application Citrix Workspace 1810 pour Windows

Option permettant de choisir l'emplacement de téléchargement des fichiers Citrix

L'application Citrix Workspace vous permet maintenant de sélectionner l'emplacement de téléchargement des fichiers Citrix. Auparavant, l'emplacement de téléchargement des fichiers Citrix était défini par défaut sur le dossier Téléchargements. L'emplacement de téléchargement est désormais configurable.

Vous pouvez définir l'emplacement de téléchargement à l'aide de la boîte de dialogue **Préférences avancées** ou l'Éditeur du Registre.

Pour plus d'informations sur la configuration de l'emplacement de téléchargement de Citrix Files à l'aide de l'Éditeur du Registre, consultez Configurer l'emplacement de téléchargement de Citrix Files à l'aide de l'Éditeur du Registre.

Pour plus d'informations sur la configuration de l'emplacement de téléchargement des fichiers Citrix à l'aide de la boîte de dialogue Préférences avancés, consultez la section Configuration de l'emplacement de téléchargement à l'aide des préférences avancées dans la documentation d'aide de l'application Citrix Workspace pour Windows.

De plus, cette version fournit un certain nombre de correctifs relatifs à l'installation et au lancement de l'application Citrix Workspace pour Citrix Cloud.

Nouveautés de l'application Citrix Workspace 1809 pour Windows

Prise en charge de Citrix Ready Workspace Hub pour Citrix Casting

Citrix Ready Workspace Hub combine des environnements numériques et physiques pour fournir des applications et des données dans un espace intelligent sécurisé. Le système complet connecte des appareils (ou objets), comme des applications mobiles et des capteurs, pour créer un environnement intelligent et réactif.

Citrix Ready Workspace Hub est basé sur la plate-forme Raspberry Pi 3. L'appareil exécutant l'application Citrix Workspace se connecte au Citrix Ready Workspace Hub et diffuse les applications ou les bureaux sur un écran plus grand. Citrix Casting est pris en charge uniquement sur Microsoft Windows 10 version 1607 et versions ultérieures ou
sur Windows Server 2016.

À l'aide de la boîte de dialogue **Préférences avancées**, vous pouvez définir si vous souhaitez lancer Citrix Ready Workspace Hub lorsque l'application Citrix Workspace est lancée.

> **Remarque :**
>
> - Citrix Casting pour Windows prend en charge la version 2.40.3839 de Citrix Ready Workspace Hub et versions ultérieures. Les versions antérieures de Workspace Hub peuvent ne pas être détectées ou provoquer une erreur de diffusion.
> - La fonctionnalité Citrix Ready Workspace Hub n'est pas prise en charge sur l'application Citrix Workspace pour Windows (Store).

Pour plus d'informations sur le Citrix Ready Workspace Hub dans l'application Citrix Workspace pour Windows, consultez la section
Configurer Citrix Ready Workspace Hub.

Pour de plus amples informations sur Citrix Ready Workspace Hub, consultez la section Citrix Ready Workspace Hub dans la documentation de Citrix Virtual Apps and Desktops.

Nouveautés de l'application Citrix Workspace 1808 pour Windows

SaaS sécurisé avec navigateur Citrix Secure Browser

L'accès sécurisé aux applications SaaS assure une expérience utilisateur unifiée qui met des applications SaaS publiées à la disposition des utilisateurs. Les applications SaaS sont disponibles avec Single Sign-on. Les administrateurs peuvent à présent protéger le réseau de l'organisation et les machines des utilisateurs finaux contre les logiciels malveillants et les fuites de données en filtrant l'accès à des sites Web et des catégories de sites Web
spécifiques.

L'application Citrix Workspace pour Windows prend en charge l'utilisation d'applications SaaS avec le service de contrôle d'accès. Le service permet aux administrateurs d'offrir une expérience homogène, intégrant Single Sign-on, et l'inspection du contenu.

La mise à disposition d'applications SaaS depuis le cloud présente les avantages suivants :

- Configuration simple : simplicité d'exploitation, de mise à jour et d'utilisation.
- Single Sign-on : ouverture de session sans problème avec Single Sign-on.
- Modèle standard pour différentes applications : configuration d'applications populaires basée sur un modèle.

Pour plus d'informations sur la configuration d'applications SaaS à l'aide des services de contrôle d'accès, reportez-vous à la documentation sur le contrôle d'accès.

Pour plus d'informations sur les applications SaaS avec l'application Citrix Workspace, consultez la section Configuration de l'espace de travail.

Prise en charge de l'authentification unique (Single Sign-On) avec Citrix Gateway

Single Sign-on vous permet de vous authentifier auprès d'un domaine et d'utiliser Citrix Virtual Apps and Desktops mis à disposition par ce domaine sans procéder à une nouvelle authentification pour chaque application ou bureau. Lorsque vous ajoutez un magasin à l'aide de l'utilitaire Storebrowse, vos informations d'identification sont transmises au serveur Citrix Gateway avec les applications et les bureaux énumérés pour vous, y compris les paramètres du menu Démarrer. Après avoir configuré Single Sign-on, vous pouvez ajouter le magasin, énumérer vos applications et bureaux et lancer les ressources nécessaires sans saisir à plusieurs reprises vos informations d'identification.

Pour plus d'informations sur la configuration de Single Sign-on avec Citrix Gateway, consultez la section Configuration de Single Sign-on avec Citrix Gateway.

Test de balise

Dans cette version, l'application Citrix Workspace vous permet d'effectuer un test de balise à l'aide du contrôleur de balises disponible dans l'**outil d'analyse de la configuration**. Un test de balise permet de vérifier si la balise (ping.citrix.com) est accessible. Ce test de diagnostic permet d'écarter l'une des nombreuses causes possibles d'une énumération lente des données, à savoir l'indisponibilité de la balise.

Pour exécuter le test, cliquez avec le bouton droit de la souris sur l'application Citrix Workspace dans la zone de notification et sélectionnez **Préférences avancées** > **Outil d'analyse de la configuration**. Sélectionnez **Contrôleur de balises** dans la liste de tests et cliquez sur **Exécuter**.

Les résultats du test peuvent être les suivants :

- Accessible : la balise peut contacter l'application Citrix Workspace.
- Inaccessible : l'application Citrix Workspace ne peut pas contacter la balise.
- Partiellement accessible : l'application Citrix Workspace peut contacter la balise par intermittence.

> **Remarque :**
>
> - Les résultats du test ne s'appliquent pas à Workspace pour Web.
> - Vous pouvez enregistrer les résultats du test sous forme de rapports. Le format par défaut du rapport est .txt.

Utilitaire Storebrowse pour l'application Citrix Workspace

Storebrowse est un utilitaire de ligne de commande léger qui permet l'interaction entre le client et le serveur. Il est utilisé pour authentifier toutes les opérations dans StoreFront et avec Citrix Gateway.

Grâce à l'utilitaire Storebrowse, les administrateurs peuvent automatiser les opérations quotidiennes suivantes :

- Ajouter un magasin
- Énumérer les bureaux et les applications publiés à partir d'un magasin configuré
- Générer manuellement un fichier ICA en sélectionnant un bureau ou une application publié
- Générer un fichier ICA à l'aide de la ligne de commande Storebrowse
- Lancer l'application publiée

L'utilitaire Storebrowse fait partie du composant `Authmanager`. Après l'installation de Citrix Workspace, l'utilitaire Storebrowse se trouve dans le dossier d'installation de AuthManager. Pour plus d'informations, consultez la section Storebrowse.

Prise en charge de l'impression PDF

Avec cette version, l'application Citrix Workspace pour Windows prend en charge l'impression PDF au cours d'une session. Le pilote d'imprimante universel PDF Citrix vous permet d'imprimer les documents lancés avec des applications et des bureaux hébergés exécutant Citrix Virtual Apps and Desktops.

Lorsque vous sélectionnez l'option **Imprimante PDF Citrix** dans la boîte de dialogue **Imprimer**, le pilote d'imprimante convertit le fichier au format PDF et transfère le fichier PDF sur la machine locale. Le fichier PDF est ensuite lancé via la visionneuse de PDF par défaut à des fins d'affichage et est imprimé à partir d'une imprimante connectée localement.

Citrix recommande le navigateur Google Chrome ou Adobe Acrobat Reader pour l'affichage au format PDF.

Vous pouvez activer l'impression PDF Citrix à l'aide de Citrix Studio sur le Delivery Controller.

Pour plus d'informations sur la configuration de l'impression PDF, consultez la section Impression PDF.

Amélioration de Chrome pour la redirection du contenu du navigateur

La redirection du contenu du navigateur prend désormais en charge le navigateur Google Chrome en plus du navigateur Internet Explorer précédemment pris en charge. La redirection du contenu du navigateur permet de rediriger le contenu d'un navigateur Web vers une machine cliente et de créer un navigateur correspondant incorporé dans l'application Citrix Workspace. Cette fonctionnalité décharge l'utilisation du réseau, le traitement des pages et le rendu graphique sur le point de terminaison. Cela améliore l'expérience utilisateur lors de la navigation sur des pages Web complexes, notamment des pages Web intégrant des vidéos HTML5 ou WebRTC.

Pour plus d'informations, veuillez consulter l'article Redirection du contenu du navigateur.

Meilleur débit réseau sur les connexions à latence élevée

Nous avons augmenté le nombre par défaut de tampons de sortie ICA utilisés pour envoyer et recevoir des données de 44 (64 Ko) à 100 (~ 145 Ko). Cette modification améliore les performances de débit, même sur les connexions à latence élevée. Cette amélioration ne concerne que l'application Citrix Workspace 1808 pour Windows ou version ultérieure.

Pour plus de détails, consultez CTX125027.

Prise en charge du mappage des lecteurs clients pour les transferts de fichiers volumineux

Le mappage des lecteurs clients prend désormais en charge les transferts de fichiers supérieurs à 4 Go. La version minimale requise pour l'application Citrix Workspace pour Windows est 1808.

Prise en charge de Citrix Analytics

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

Problèmes résolus

Problèmes résolus dans la version 1902

Installation, désinstallation, mise à niveau

- Après la mise à niveau de Citrix Receiver pour Windows vers la version 4.9 CU4, la clé de registre requise pour le canal virtuel personnalisé peut ne pas être préservée. [LD0633]

Clavier

- Lorsque la fonction **Éditeur IME local** ou la fonctionnalité de synchronisation de la disposition du clavier local est activée, si vous appuyez sur la combinaison de touches qui inclut la touche **Ctrl** droite et la touche **Maj** droite, la touche **Maj** peut rester bloquée en position abaissée. [LD0585]

Session/Connexion

- Un problème d'authentification peut survenir lorsque deux magasins existent dans des états différents : un magasin dans l'état **ON** et un autre dans l'état **OFF**. [LC9511]
- Démarrez plusieurs applications dans un bureau partagé hébergé. Si vous basculez entre les clients ou effectuez une opération de déconnexion ou de reconnexion, ce message d'erreur peut s'afficher :

Citrix HDX Engine has stopped working
Exception caused the program to stop working correctly. Please close the program. [LC9772]

- Lorsque vous tentez d'accéder aux applications de bureau publiées, la session peut se déconnecter. Une fois la session déconnectée, le processus `wfica32.exe` se termine de façon inattendue. [LC9966]
- L'utilisation du processeur du processus wfica.32.exe peut être élevée dans un scénario « double-hop ». [LD0386]
- Lorsque vous exécutez une fonction qui appelle une URL Web dans l'application publiée du terminal Bloomberg, l'URL peut ne pas être redirigée vers la machine utilisateur. [LD0484]
- Lorsque la fonction d'attente d'application est configurée, les applications publiées risquent de ne pas rouvrir un fichier existant après la déconnexion de la session. [LD0742]
- Les tentatives de basculement de la caméra de face vers la caméra arrière peuvent échouer si le nom complet du bureau publié contient des caractères non ASCII. [LD0732]

Exceptions système

- Lorsque la stratégie de redirection bidirectionnelle du contenu est activée, le processus `Redirector.exe` peut se fermer de façon inattendue lorsque vous tentez d'ouvrir une page Web sur le navigateur Web local. En conséquence, la redirection bidirectionnelle du contenu ne fonctionne pas et ce message d'erreur apparaît :

  Citrix FTA, URL Redirector stopped working. [LD0420]

- Le processus `wfica32.exe` peut se fermer de manière inattendue. Le problème se produit lorsque les paramètres de proxy sont configurés et que vous essayez de démarrer une nouvelle session dans Citrix Receiver pour Web. [LD0548]

Interface utilisateur

- Lorsque vous sélectionnez l'option **Réinitialiser Receiver**, Citrix Receiver pour Windows peut vous demander d'installer .NET Framework 3.5 sur Microsoft Windows Version 10. [LD0690]

Correction de problèmes dans l'application Citrix Workspace 1812 pour Windows

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

Correction de problèmes dans l'application Citrix Workspace 1811 pour Windows

Clavier :

- Les clics de souris peuvent ne pas générer de réponses sur la session distante. Ce problème peut se produire lorsque vous ouvrez la fenêtre Préférences à partir de la barre d'outils Desktop Viewer et configurez le paramètre MouseTimer sur une valeur autre que la valeur par défaut. [LD0260]

Session/Connexion :

- Les tentatives de démarrage d'une application peuvent échouer et ce message d'erreur s'afficher :

  Impossible de lancer votre application . Contactez votre service d'assistance et fournissez les informations suivantes : Impossible d'ouvrir Citrix Receiver.

  Pour activer le correctif, l'administrateur doit définir la clé de registre suivante :

  - Clé de registre : `HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine`
  - Name:`EngineTimeout`
  - Type : DWORD
  - Valeur : plus de 20 secondes

  Pour activer le correctif, l'utilisateur doit définir la clé de registre suivante :

  - Clé de registre : `HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine`
  - Name:`EngineTimeout`
  - Type : DWORD
  - Valeur : plus de 20 secondes, par exemple, EngineTimeout = 20

[LC9771]

- Les applications démarrées à l'aide de Citrix Receiver pour Windows peuvent être mises en miroir sur le moniteur secondaire. [LC9893]
- Lors de l'utilisation d'un lecteur de codes à barres, certaines données risquent d'être perdues lors de l'envoi d'une grande quantité de données. [LD0243]

Correction de problèmes dans l'application Citrix Workspace 1810 pour Windows

Session/Connexion :

- Après la mise à niveau de Citrix Receiver pour Windows vers la version 4.9.1000, CDViewer peut afficher un écran gris lorsque vous fermez la session. [LC9290]
- Un problème de publication de l'objet GDI peut entraîner une utilisation élevée de l'UC par le processus wfica32.exe. [LC9356]

- Après avoir modifié le point balise interne dans StoreFront, vous ne pourrez peut être pas démarrer d'applications à partir de Citrix Receiver pour Windows tant que vous n'avez pas redémarré Citrix Receiver. [LC9442]
- Un problème d'authentification peut survenir lorsque deux magasins existent dans des états différents : un magasin dans l'état ON et un autre dans l'état OFF. [LC9511]
- Une erreur de syntaxe peut se produire dans le fichier receiver.admx qui est envoyé à partir d'Azure Mobile Device Management (MDM) Intune. [LC9992]
- Si vous ne choisissez pas le programme par défaut lorsque vous configurez l'association de type de fichier pour .docx pour la première fois, le message d'erreur suivant peut s'afficher :

« Windows ne parvient pas à accéder au périphérique, au chemin d'accès ou au fichier spécifié. Vous ne disposez peut-être pas des autorisations appropriées pour avoir accès à l'élément. » [LD0026]

- Avec cette correction, lorsque la fenêtre réduite d'une application transparente est placée sur un bureau plutôt que sur la barre des tâches, la fenêtre peut s'afficher correctement. [LD0034]
- Après avoir installé Citrix Receiver pour Windows 4.12 à l'aide de la ligne de commande avec l'option `EnableTracing=false`, l'assistant de configuration ne démarre pas lorsque vous cliquez avec le bouton droit de la souris sur **Receiver** > **Ouvrir**. [LD0156]
- L'instance publiée de certaines applications tierces peut s'ouvrir en tant qu'applications transparentes lors de l'utilisation des cartes graphiques NVIDIA. [LD0175]
- Les raccourcis d'application locale créés à partir de l'icône du panneau de configuration ne peuvent pas être démarrés avec `KEYWORDS:Prefer` qui est configuré à partir de Citrix Studio. [LD0288]
- Le lancement d'une application SaaS publiée dans une instance de l'application Citrix Workspace pour Windows installée par l'utilisateur risque d'échouer. [RFWIN-9329]

  Pour résoudre ce problème, procédez comme suit :

  1. Lancez l'Éditeur du Registre et accédez à HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix.
  2. Créez un dossier nommé browser et une clé de registre à valeur de chaîne extensible nommée InstallDir.
  3. Définissez la valeur de la clé sur %localAppData%\Citrix\ICAClient.

  Pour plus d'informations sur ce problème, consultez l'article CTX237199 du centre de connaissances.

Exceptions système :

- Citrix Receiver pour Windows peut se fermer de manière inattendue et ce message d'erreur s'affiche : **Citrix HDX Engine ne fonctionne plus**.

  Le problème se produit lors d'une interruption dans le module graphique. [LC9466]

- Le processus `wfica32.exe` peut se fermer de manière inattendue lorsque vous fermez la session du système. [LC9892]
- Le processus `wfica32.exe` peut se fermer de manière inattendue lors de l'utilisation de la commande permettant de basculer l'éditeur IME client générique ou l'éditeur IME local. [LD0038]

Correction de problèmes dans l'application Citrix Workspace 1809 pour Windows

Ouverture de session/Authentification :

- Lorsque vous utilisez Citrix Receiver pour Windows pour ajouter un compte, la saisie de l'URL du magasin peut entraîner le message d'erreur suivant : « Impossible de contacter le service d'authentification ». Le problème se produit lorsqu'une URL StoreFront commence par la chaîne de texte citrix.com. [LC9631]

Session/Connexion :

- Lorsque vous utilisez Citrix Receiver pour Windows 4.10.1, vous ne pourrez peut-être pas quitter certaines applications publiées. Le problème se produit lorsque le message de confirmation « Êtes-vous sûr » n'apparaît pas lorsque vous tentez de quitter les applications. [LC9353]
- Les tentatives de démarrage d'une application via une connexion sécurisée peuvent échouer. Le problème se produit lorsque la longueur du certificat, ainsi que celle du nom du sujet et du journal, sont trop élevées. [LC9853]
- Citrix Receiver pour Windows 4.11 peut se fermer par intermittence et afficher ce message d'erreur : « L'application s'est bloquée ». Le problème se produit en raison de l'application défaillante, wfica32.exe. [LC9890]

Interface utilisateur :

- Les fenêtres non transparentes peuvent être redimensionnées de manière incorrecte et afficher des barres de défilement. [LC9545]

Correction de problèmes dans l'application Citrix Workspace 1808 pour Windows

Installation, désinstallation, mise à niveau :

- Lorsque vous tentez d'installer Citrix Receiver pour Windows 4.9.2000 à l'aide de la commande d'installation silencieuse, le processus d'installation risque de ne pas s'exécuter. [LC9587]

Ouverture de session/Authentification :

- Après le redémarrage du processus AuthManSvr.exe, les tentatives de fermeture de session de l'application Citrix Workspace pour Windows échouent. [LC7981]

Session/Connexion :

- La redirection des scanners par Citrix Receiver pour Windows 4.7 risque d'échouer. Le problème se produit lorsque la prise en charge de périphériques Twain 2.0 entraîne une régression avec les périphériques non Twain 2.0 qui s'exécutent sur des VDA. [LC8215]
- Après avoir mis à niveau Citrix Receiver pour Windows de la version 13.x vers la version 14.4 à l'aide de la commande PSExec, les tentatives de connexion à un magasin peuvent échouer. En outre, Receiver pour Windows peut cesser de répondre lors de l'installation ou de la mise à niveau lorsque vous utilisez la commande `PSExec`. Une fois la correction LC9024 installée, les composants `AuthManager` s'alignent avec d'autres composants et sont installés dans le dossier du client ICA. [LC9024]
- Lorsque Local App Access est activé, les tentatives de démarrage d'un bureau hébergé peuvent échouer. Le bureau semble avoir démarré, mais un écran gris s'affiche. [LC9452]
- Lorsque vous démarrez une application Java (Javaw.exe) avec la stratégie Redirection de port LPT client activée, la session utilisateur peut se déconnecter. [LC9610]
- L'outil d'analyse de la configuration, qui valide la configuration de Single Sign-On, peut ne pas être en mesure de procéder à la validation et se bloquer lors de la vérification du processus Single Sign-On. [LC9625]
- Lorsque vous basculez entre plusieurs applications publiées à l'aide des touches Win+Tab ou Alt+Tab, les objets GDI peuvent augmenter sur le client jusqu'à ce que les applications cessent de répondre et affichent des pixels noirs. [LC9655]

Expérience utilisateur :

- Lorsque vous utilisez l'éditeur de méthode d'entrée (IME) japonais et entrez du texte dans une application en mode transparent, le texte risque de ne pas être visible. Le problème se produit lorsque la taille de police du texte est petite. [LC9882]
  Pour activer cette correction, définissez la clé de registre suivante :
  - Clé de registre : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client`
  - Name:`DisableD3DRenderWidthHeightCheck`
  - Type : REG_DWORD
  - Valeur : 1

Problèmes connus

Problèmes connus dans la version 1902

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

Problèmes connus dans la version 1812

- Une corruption d'image peut être observée dans les sessions exécutées sur des VDA avec les derniers GPU NVIDIA. Citrix travaille à résoudre ce problème.

Problèmes connus dans l'application Citrix Workspace 1810 pour Windows

- L'authentification unique échoue après la mise à niveau de Windows 10 sur un ordinateur où l'application Citrix Workspace est installée. Pour plus d'informations, consultez l'article CTX234973 du centre de connaissances. [TPV-1916]

Problèmes connus dans la version 1809

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

Problèmes connus dans la version 1808

- Si vous quittez l'installation de l'application Citrix Workspace pour Windows lorsque l'écran de démarrage s'affiche, des conflits risquent de se produire. [RFWIN-9298]
- Lorsque vous installez Citrix Receiver pour Windows version 4.11 sur un système d'exploitation Windows 10 (numéro de build 10240), la connexion au VDA peut entraîner une erreur de socket 10038.

  Pour résoudre ce problème, mettez à niveau le système d'exploitation Windows 10 du numéro de build 10240 vers le numéro de build 1803.

  Pour plus d'informations, consultez l'article CTX237203 du centre de connaissances.

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 Windows

Conditions préalables à l'installation de l'application Citrix Workspace

March 26, 2019

Configuration système requise et compatibilité

Exigences

- Cette version de l'application Citrix Workspace requiert un minimum de 1 Go de RAM.

- Configuration minimale requise pour .NET Framework
  - Self-Service Plug-in requiert NET 3.5 Service Pack 1. Ce plug-in vous permet de vous abonner à des applications et des bureaux et de les lancer à partir de l'interface utilisateur ou de la ligne de commande de Workspace pour Windows. Pour plus d'informations, veuillez consulter l'article Utilisation des paramètres de ligne de commande.
  - .NET 2.0 Service Pack 1

Matrice de compatibilité

L'application Citrix Workspace pour Windows est compatible avec les systèmes d'exploitation Windows et les navigateurs Web suivants. Cette version est également compatible avec toutes les versions actuellement prises en charge de Citrix Virtual Apps and Desktops et de Citrix Gateway comme indiqué dans le tableau du cycle de vie des produits Citrix.

> **Remarque :**
>
> Citrix Gateway End Point Analysis Plug-in (EPA) ne prend pas en charge l'application Citrix Workspace pour Windows.

Système d'exploitation
Windows 10 éditions 32 bits et 64 bits *
Windows 8.1, éditions 32 bits et 64 bits (y compris l'édition Embedded)
Windows 7, éditions 32 bits et 64 bits (y compris l'édition Embedded)
Windows Thin PC
Windows Server 2016
Windows Server 2012 R2, édition Standard et Datacenter
Windows Server 2008 R2, édition 64 bits
Windows Server 2019
Windows 10 Entreprise 2016 LTSB 1607

* Prend en charge Windows 10 versions 1607, 1703, 1709, 1803 et 1809.

Navigateur
Internet Explorer
Google Chrome dernière version (requiert StoreFront)

Navigateur
Mozilla Firefox dernière version
Microsoft Edge

Prise en charge

Système d'exploitation pris en charge sur les appareils tactiles	Système d'exploitation pris en charge sur les VDA
Windows 10	Windows 10
Windows 8	Windows 8
Windows 7	Windows 7
	Windows 2012 R2
	Windows Server 2016
	Windows 2008 R2

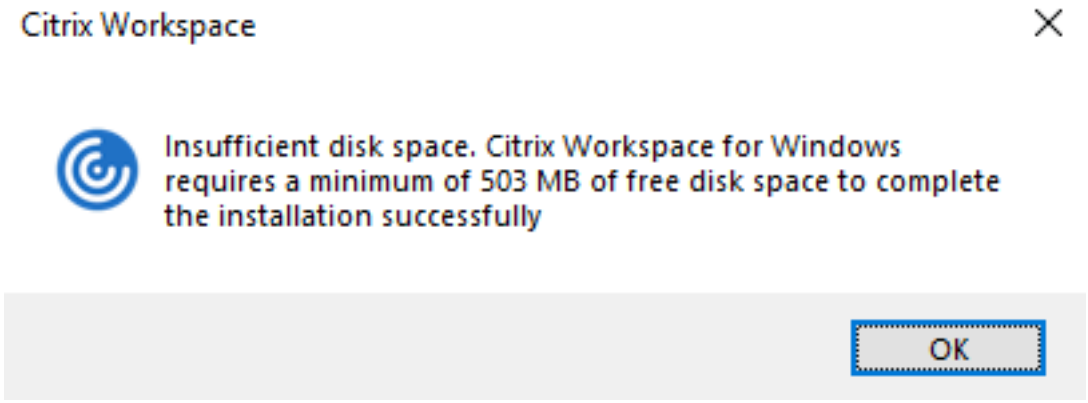
Validation de l'espace disque disponible

Le tableau suivant fournit des informations sur l'espace disque minimal requis pour installer l'application Citrix Workspace pour Windows.

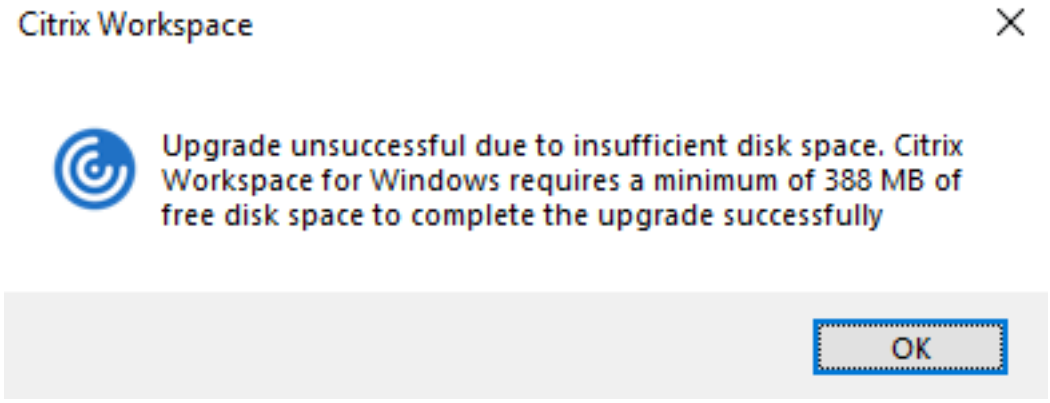
Type d'installation	Espace disque requis
Nouvelle installation	572 Mo
Mise à niveau	350 Mo

L'application Citrix Workspace vérifie si l'espace disque disponible est suffisant pour procéder à l'installation. La vérification est effectuée aussi bien lors d'une nouvelle installation que d'une mise à niveau.

Lors d'une nouvelle installation, le processus s'arrête lorsque l'espace disque est insuffisant et la boîte de dialogue suivante s'affiche.



Lors de la mise à niveau de l'application Citrix Workspace, l'installation s'arrête lorsque l'espace disque est insuffisant et la boîte de dialogue suivante s'affiche.



Remarque :

- Le programme d'installation vérifie l'espace disque uniquement après l'extraction du package d'installation.
- Lorsque l'espace disque du système est insuffisant lors d'une installation silencieuse, la boîte de dialogue ne s'affiche pas, mais le message d'erreur est consigné dans `CTXInstall\\_TrolleyExpress-\*.log`.

Connexions, certificats et authentification

Connexions

- Magasin HTTP
- Magasin HTTPS
- Citrix Gateway 10.5 et versions ultérieures
- Interface Web 5.4

Certificats

- Privés (auto-signés)
- Racine
- Génériques
- Intermédiaires

Certificats privés (auto-signés)

Si un certificat privé est installé sur la passerelle distante, le certificat racine de l'autorité de certification de l'organisation doit être installé sur l'appareil de l'utilisateur à partir duquel vous accédez aux ressources Citrix.

> **Remarque :**
>
> Si le certificat de la passerelle distante ne peut pas être vérifié lors de la connexion (car le certificat racine n'est pas inclus dans le magasin de clés), un avertissement relatif à un certificat non approuvé s'affiche. Si un utilisateur choisit d'ignorer l'avertissement, les applications s'affichent, mais ne démarrent pas.

Installation de certificats racine

Pour les ordinateurs appartenant à un domaine, vous pouvez utiliser le modèle d'administration d'objet de stratégie de groupe pour distribuer et approuver les certificats d'autorité de certification.

Pour les ordinateurs n'appartenant pas à un domaine, l'organisation peut créer un pack d'installation personnalisé pour distribuer et installer le certificat d'autorité de certification. Contactez votre administrateur système pour obtenir de l'aide.

Certificats génériques

Les certificats génériques sont utilisés sur un serveur situé dans le même domaine.

L'application Citrix Workspace prend en charge les certificats génériques. Toutefois, ils doivent être utilisés conformément à la stratégie de sécurité de votre organisation. En pratique, des alternatives aux certificats génériques peuvent être envisagées, par exemple, un certificat contenant la liste des noms de serveurs avec l'extension SAN (Autre nom de l'objet). Des autorités de certification publiques et privées émettent ces certificats.

Certificats intermédiaires

Si votre chaîne de certificat contient un certificat intermédiaire, ce dernier doit être ajouté au certificat serveur de Citrix Gateway. Pour plus d'informations, veuillez consulter la section Configuration de certificats intermédiaires.

Authentification

Authentification auprès de StoreFront

	Workspace pour Web utilisant des navigateurs	Site StoreFront Services (natif)	StoreFront, Citrix Virtual Apps and Desktops (natif)	Citrix Gateway auprès de Workspace pour Web (navigateur)	Citrix Gateway auprès du site StoreFront Services (natif)
Anonyme	Oui	Oui			
Domaine	Oui	Oui	Oui	Oui*	Oui*
Authentificatio pass-through au domaine	Oui	Oui	Oui		
Jeton de sécurité				Oui*	Oui*
Deux facteurs (domaine avec jeton de sécurité)				Oui*	Oui*
SMS				Oui*	Oui*
Carte à puce	Oui	Oui		Oui	Oui
Certificat utilisateur				Oui (Citrix Gateway plug-in)	Oui (Citrix Gateway plug-in)

* Avec ou sans Citrix Gateway Plug-in installé sur la machine

> **Remarque :**
>
> L'application Citrix Workspace prend en charge l'authentification à deux facteurs (domaine + jeton de sécurité) via Citrix Gateway au service natif StoreFront.

Authentification auprès de l'Interface Web

L'application Citrix Workspace prend en charge les méthodes d'authentification suivantes (l'Interface Web utilise le terme **Explicite** pour l'authentification de domaine avec jeton de sécurité) :

	Interface Web (navigateurs)	Site Interface Web Citrix Gateway	Citrix Gateway vers l'Interface Web (navigateur)	Citrix Gateway auprès du site Interface Web Citrix Gateway
Anonyme	Oui			
Domaine	Oui	Oui	Oui*	
Authentification pass-through au domaine	Oui	Oui		
Jeton de sécurité			Oui*	
Deux facteurs (domaine avec jeton de sécurité)			Oui*	
SMS			Oui*	
Carte à puce	Oui	Oui		
Certificat utilisateur			Oui (Citrix Gateway Plug-in)	

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

Pour de plus amples informations sur l'authentification, consultez Configuration de l'authentification et de l'autorisation dans les rubriques Documentation et gestion de Citrix Gateway de la documentation de StoreFront.

Liste de révocation de certificats

Lorsque vous activez la vérification de la liste de révocation de certificats (CRL), l'application Citrix Workspace vérifie si le certificat du serveur est révoqué. Obliger l'application Citrix Workspace à vérifier cette liste améliore l'authentification cryptographique du serveur et la sécurité globale de la connexion TLS entre la machine utilisateur et un serveur.

Vous pouvez activer la vérification CRL à plusieurs niveaux. Par exemple, vous pouvez configurer l'application Citrix Workspace pour qu'elle vérifie uniquement sa liste de certificats locaux ou pour qu'elle vérifie les listes de certificats locaux et de réseau. De plus, vous pouvez configurer la vérification des certificats pour permettre aux utilisateurs de n'ouvrir leurs sessions que si toutes les listes de révocation de certificats ont été vérifiées.

Si vous effectuez cette modification sur votre ordinateur local, quittez l'application Citrix Workspace. Vérifiez que tous les composants Citrix Workspace, y compris le **centre de connexion**, sont fermés.

Pour plus d'informations sur la configuration de TLS, consultez la section Configurer et activer TLS.

Installer, désinstaller et mettre à jour

March 26, 2019

Vous pouvez installer l'application Citrix Workspace en utilisant l'une des méthodes suivantes :

- Téléchargez le package d'installation `CitrixWorkspaceApp.exe` à partir de la page de téléchargement de l'application Citrix Workspace ou depuis la page de téléchargement de votre entreprise (si disponible). Le package peut être installé de deux façons :
  - Exécution d'un assistant d'installation Windows interactif. ou
  - Saisie du nom du fichier d'installation, des commandes d'installation et des propriétés d'installation à l'aide de l'interface de ligne de commande. Pour plus d'informations sur l'installation de l'application Citrix Workspace à l'aide de l'interface de ligne de commande, consultez la section Utilisation des paramètres de ligne de commande.
- Utilisez Active Directory et les exemples de scripts de démarrage pour déployer l'application Citrix Workspace pour Windows. Pour plus d'informations sur Active Directory, veuillez consulter la section Utilisation d'Active Directory et d'exemples de scripts de démarrage.
- Déployez l'application Citrix Workspace pour Windows à partir de Workspace pour Web pour vous assurer qu'elle est installée avant de lancer une application à partir d'un navigateur. Pour plus d'informations, veuillez consulter l'article Utilisation de Workspace pour Web.
- Utilisez un outil de distribution électronique de logiciels (ESD) comme Microsoft System Center Configuration Manager 2012 R2. Pour plus d'informations, veuillez consulter l'article Utilisation de System Center Configuration Manager 2012 R2.

Conditions préalables :

- Vérifiez que le système répond à la configuration système requise.

> **Remarque :**
>
> L'application Citrix Workspace pour Windows est signée numériquement. La signature numérique est horodatée. Ainsi, le certificat est valide même après son expiration.

Installation avec des privilèges d'administrateur et non administrateur :

Les installations de l'application Citrix Workspace pour Windows par un administrateur et par un utilisateur (non administrateur) présentent les différences suivantes.

	Dossier d'installation	Type d'installation
Administrateur	C:\Program Files (x86)\Citrix\ICA Client	Installation par système
User	%USERPROFILE%\AppData\Local\Citrix\ICA Client	Installation par utilisateur

> **Remarque :**
>
> Si un administrateur installe Citrix Workspace pour Windows sur un système alors qu'un utilisateur a déjà installé une instance de l'application sur ce système, un conflit se produira. Citrix vous recommande de désinstaller toutes les instances de l'application Citrix Workspace installées par l'utilisateur avant d'installer l'application en tant qu'administrateur.

Installer manuellement

Vous pouvez installer l'application Citrix Workspace pour Windows à partir du support d'installation, d'un partage réseau, de l'explorateur Windows ou d'une ligne de commande en exécutant manuellement le package d'installation `CitrixWorkspaceApp.exe`. Pour obtenir les paramètres d'installation de ligne de commande, consultez la section Utilisation des paramètres de ligne de commande. L'application Citrix Workspace peut être installée par un utilisateur ainsi qu'un administrateur. Vous devez disposer de privilèges d'administrateur pour utiliser l'authentification pass-through avec l'application Citrix Workspace pour Windows.

Pour installer l'application Citrix Workspace à l'aide d'un programme d'installation Windows :

1. Lancez le fichier `CitrixWorkspaceApp.exe` et cliquez sur **Démarrer**.
2. Lisez et acceptez le contrat de licence de l'utilisateur final et continuez l'installation.
3. Si vous tentez l'installation sur une machine appartenant à un domaine avec des privilèges d'administrateur, une boîte de dialogue supplémentaire s'affiche pour activer ou désactiver l'authentification unique. Consultez Authentification pass-through au domaine pour de plus amples informations.

4. Suivez le programme d'installation Windows pour terminer l'installation.

Utilisation des paramètres de ligne de commande

Vous pouvez installer l'application Citrix Workspace en tapant le nom du fichier d'installation, les commandes d'installation et les propriétés d'installation à l'aide de l'interface de ligne de commande. Vous pouvez personnaliser le programme d'installation de l'application Citrix Workspace en spécifiant des options de ligne de commande. Le programme d'installation s'extrait automatiquement sur le répertoire temporaire du système avant le lancement du programme d'installation. Cet espace disponible comprend les fichiers programmes, les données utilisateur et les répertoires temporaires après le lancement de plusieurs applications.

Pour plus d'informations sur la configuration système requise, reportez-vous à la section Configuration système requise.

Pour installer l'application Citrix Workspace à l'aide de la ligne de commande Windows, lancez l'invite de commandes, puis tapez le nom du fichier d'installation, les commandes d'installation et les propriétés d'installation sur une seule ligne. Les commandes et propriétés d'installation disponibles sont répertoriées ci-dessous :

```
CitrixWorkspaceApp.exe [commands] [properties]
```

Liste des paramètres de ligne de commande

Les paramètres sont généralement classés comme suit :

1. Paramètres courants
2. Paramètres d'installation
3. Paramètres des fonctionnalités HDX
4. Préférences et paramètres de l'interface utilisateur
5. Paramètres d'authentification

Paramètres courants

- /? Ou `/help` : répertorie toutes les commandes et propriétés d'installation.
- `/silent` : désactive les boîtes de dialogue et les invites d'installation pendant l'installation.
- `/noreboot` : supprime les invites et la boîte de dialogue de redémarrage lors de l'installation. Lorsque vous supprimez l'invite de redémarrage, les périphériques USB qui sont dans un état suspendu ne sont reconnus par l'application Workspace qu'après le redémarrage de la machine utilisateur.

- `/includeSSON` : requiert une installation en tant qu'administrateur. Indique que l'application Citrix Workspace est installée avec le composant d'authentification unique. Consultez Authentification pass-through au domaine pour de plus amples informations.
- `/rcu` : indique que l'application Citrix Workspace sera installée/mise à niveau en désinstallant la version existante du logiciel. Ce paramètre nettoie également les anciens paramètres.

Paramètres d'installation

/AutoUpdateCheck

Description :

Indique que l'application Citrix Workspace pour Windows détecte lorsqu'une mise à jour est disponible.

- Auto (valeur par défaut) : vous êtes informé lorsqu'une mise à jour est disponible. Par exemple, `CitrixWorkspaceApp.exe /AutoUpdateCheck=auto`.
- Manual (Manuel) : vous n'êtes pas informé lorsque des mises à jour sont disponibles. Recherchez les mises à jour manuellement. Par exemple, `CitrixWorkspaceApp.exe /AutoUpdateCheck=manual`.
- Disabled (Désactivé) : les mises à jour automatiques sont désactivées. Par exemple, `CitrixWorkspaceApp.exe /AutoUpdateCheck=disabled`.

/AutoUpdateStream

Description :

Indique le suivi de la publication de l'application Citrix Workspace. Consultez la section Étapes du cycle de vie pour plus d'informations.

- LTSR : indique qu'il s'agit d'une version LTSR (Long Term Service Release). Par exemple, `CitrixWorkspaceApp.exe /AutoUpdateStream=LTSR`
- Current (Actuel) : indique qu'il s'agit de la dernière version de l'application Citrix Workspace. Par exemple, `CitrixWorkspaceApp.exe /AutoUpdateStream=Current`

/DeferUpdateCount

Description :

Indique le nombre de fois où vous pouvez différer la notification de mise à jour lorsqu'une mise à jour est disponible. Consultez Mises à jour de Citrix Workspace pour de plus amples informations.

- -1 (valeur par défaut) : permet de différer la notification n'importe quel nombre de fois. Par exemple, `CitrixWorkspaceApp.exe /DeferUpdateCount=-1`.
- 0 : indique que vous recevrez une (seule) notification pour chaque mise à jour disponible. L'option **Me rappeler plus tard** est désactivée. Par exemple, `CitrixWorkspaceApp.exe /DeferUpdateCount=0`.
- Tout autre numéro « n » : permet de différer la notification de mise à jour « n » fois. L'option **Me rappeler plus tard** s'affiche le nombre « n » de fois défini. Par exemple, `CitrixWorkspaceApp.exe /DeferUpdateCount=<n>`.

/AURolloutPriority

Description :

Indique la période pendant laquelle vous pouvez effectuer le déploiement.

- Auto (valeur par défaut) : les mises à jour sont déployées pendant la période de mise à disposition telle que configurée par l'administrateur. Par exemple, `CitrixWorkspaceApp.exe /AURolloutPriority=Auto`.
- Fast (Rapide) : les mises à jour sont déployées au début de la période de mise à disposition. Par exemple, `CitrixWorkspaceApp.exe /AURolloutPriority=Fast`.
- Medium (Moyen) : les mises à jour sont déployées au milieu de la période de mise à disposition. Par exemple, `CitrixWorkspaceApp.exe /AURolloutPriority=Medium`.
- Slow (Lent) : les mises à jour sont déployées à la fin de la période de mise à disposition. Par exemple, `CitrixWorkspaceApp.exe /AURolloutPriority=Slow`.

INSTALLDIR

Description :

Spécifie le répertoire d'installation de l'application Citrix Workspace. Le chemin d'accès par défaut est `C:\Program Files\Citrix`. Par exemple, `CitrixWorkspaceApp.exe INSTALLDIR=C:\Program Files\Citrix`.

ADDLOCAL

Description :

Installe un ou plusieurs des composants spécifiés. Par exemple, `CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopViewer,Flash,Vd3d, WebHelper,BrowserEngine, WorkspaceHub`.

Paramètres des fonctionnalités HDX

ALLOW_BIDIRCONTENTREDIRECTION

Description :

Indique que la redirection bidirectionnelle du contenu du client vers l'hôte et de l'hôte vers le client est activée. Pour de plus amples informations, consultez la section Paramètres de stratégie Redirection bidirectionnelle du contenu dans la documentation de Citrix Virtual Apps and Desktops.

- 0 (valeur par défaut) : indique que la redirection bidirectionnelle du contenu est désactivée. Par exemple, `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=0`.
- 1 : indique que la redirection bidirectionnelle du contenu est activée. Par exemple, `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=1`.

FORCE_LAA

Description :

Indique que l'application Citrix Workspace est installée avec le composant Local App Access côté client. Pour de plus amples informations, consultez la section Local App Access dans la documentation de Citrix Virtual Apps and Desktops.

- 2-0 (valeur par défaut) : indique que le composant Local App Access n'est pas installé. Par exemple, `CitrixWorkspaceApp.exe FORCE_LAA =2`.
- 3-1 : indique que le composant Local App Access côté client est installé. Par exemple, `CitrixWorkspaceApp.exe FORCE_LAA =1`.

LEGACYFTAICONS

Description :

Spécifie si les icônes des applications sont affichées pour les documents ou les fichiers qui disposent d'associations de type de fichier avec des applications faisant l'objet d'une souscription.

- False (valeur par défaut) : indique que les icônes de l'application sont affichées pour les documents ou les fichiers qui disposent d'associations de type de fichier avec des applications faisant l'objet d'une souscription. Lorsque ce paramètre est défini sur false, le système d'exploitation génère une icône pour le document qui ne possède pas d'icône spécifique. L'icône générée par le système d'exploitation est une icône générique sur laquelle est superposée une version plus petite de l'icône d'application. Par exemple, `CitrixWorkspaceApp.exe LEGACYFTAICONS=False`.

- True : indique que les icônes de l'application ne sont pas affichées pour les documents ou les fichiers qui disposent d'associations de type de fichier avec des applications faisant l'objet d'une souscription. Par exemple, `CitrixWorkspaceApp.exe LEGACYFTAICONS=True`.

ALLOW_CLIENTHOSTEDAPPSURL

Description :

Active la fonctionnalité de redirection des adresses URL sur les machines utilisateur. Pour de plus amples informations, consultez la section Local App Access dans la documentation de Citrix Virtual Apps and Desktops.

- 0 (valeur par défaut) : désactive la fonctionnalité de redirection des adresses URL sur les machines utilisateur. Par exemple, `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=0`.
- 1 : active la fonctionnalité de redirection des adresses URL sur les machines utilisateur. Par exemple, `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=1`.

Préférences et paramètres de l'interface utilisateur

ALLOWSAVEPWD

Description :

Permet d'enregistrer les informations d'identification du magasin localement. Ce paramètre s'applique uniquement aux magasins utilisant le protocole PNAgent.

- S (valeur par défaut) - autorise l'enregistrement du mot de passe uniquement pour les magasins sécurisés (configurés avec HTTPS). Par exemple, `CitrixWorkspaceApp.exe ALLOWADDSTORE=S`.
- N : n'autorise pas l'enregistrement du mot de passe. Par exemple, `CitrixWorkspaceApp.exe ALLOWADDSTORE=N`.
- R : autorise l'enregistrement du mot de passe pour les magasins sécurisés (HTTPS) et les magasins non sécurisés (HTTP). Par exemple, `CitrixWorkspaceApp.exe ALLOWADDSTORE=A`.

DESKTOPDIR

Description :

Spécifie le répertoire des raccourcis sur le Bureau.

- `<Directory Name>` : par défaut, les raccourcis apparaissent dans le dossier `/Desktop`. Vous pouvez spécifier le chemin d'accès relatif des raccourcis. Par exemple, pour placer les raccourcis

sous Démarrer > Tous les programmes > Workspace, spécifiez `STARTMENUDIR=\Workspace`. Par exemple, `CitrixWorkspaceApp.exe DESKTOPDIR=\Office`.

SELFSERVICEMODE

Description :

Contrôle l'accès à l'interface utilisateur en libre-service de l'application Workspace. Consultez la section Gestion des sessions dans la documentation de l'API Fast Connect 3 Credential Insertion.

- True : indique que l'utilisateur a accès à l'interface utilisateur en libre-service. Par exemple, `CitrixWorkspaceApp.exe SELFSERVICEMODE=True`.
- False : indique que l'utilisateur n'a pas accès à l'interface utilisateur en libre-service. Par exemple, `CitrixWorkspaceApp.exe SELFSERVICEMODE=False`.

ENABLEPRELAUNCH

Description :

Contrôle le pré-lancement de session. Consultez Temps de lancement des applications pour de plus amples informations.

- True : indique que le pré-lancement de session est activé. Par exemple, `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True`.
- False : indique que le pré-lancement de session est désactivé. Par exemple, `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False`.

DisableSetting

Description :

Masque l'affichage de l'option **Raccourcis et reconnexion** sur la page **Préférences avancées**. Consultez Masquer des paramètres spécifiques sur la page Paramètres avancés pour de plus amples informations.

- 0 (valeur par défaut) : affiche les options **Raccourcis** et **Reconnexion** sur la page Préférences avancées. Par exemple, `CitrixWorkspaceApp.exe DisableSetting=0`.
- 1 : affiche uniquement l'option **Reconnexion** sur la page Préférences avancées. Par exemple, `CitrixWorkspaceApp.exe DisableSetting=1`.
- 2 : affiche uniquement l'option **Raccourcis** sur la page Préférences avancées. Par exemple, `CitrixWorkspaceApp.exe DisableSetting=2`.
- 3 : les options **Raccourcis** et **Reconnexion** sont masquées sur la page Préférences avancées. Par exemple, `CitrixWorkspaceApp.exe DisableSetting=3`.

EnableCEIP

Description :

Indique votre participation au programme d'amélioration de l'expérience utilisateur (CEIP). Consultez CEIP pour de plus amples informations.

- True (valeur par défaut) : permet de participer au programme d'amélioration de l'expérience utilisateur (CEIP). Par exemple, `CitrixWorkspaceApp.exe EnableCEIP=True`.
- False : permet de désactiver le programme d'amélioration de l'expérience utilisateur (CEIP). Par exemple, `CitrixWorkspaceApp.exe EnableCEIP=False`.

EnableTracing

Description :

Contrôle la fonction de **suivi permanent**.

- True (valeur par défaut) : active la fonction de **suivi permanent**. Par exemple, `CitrixWorkspaceApp.exe EnableTracing=true`.
- False : désactive la fonction de **suivi permanent**. Par exemple, `CitrixWorkspaceApp.exe EnableTracing=false`.

CLIENT_NAME

Description :

Spécifie le nom utilisé pour identifier la machine utilisateur sur le serveur.

- `<ClientName>` : spécifie le nom utilisé pour identifier la machine utilisateur sur le serveur. Le nom par défaut est `%COMPUTERNAME%`.

STARTMENUDIR

Description :

Spécifie le répertoire des raccourcis dans le menu Démarrer.

- `<Directory Name>` : par défaut, toutes les applications apparaissent sous **Démarrer** > **Tous les programmes**. Vous pouvez spécifier le chemin d'accès relatif des raccourcis dans le dossier `\Programs`. Par exemple, pour placer les raccourcis sous Démarrer > Tous les programmes > Workspace, spécifiez `STARTMENUDIR=\Workspace`. Par exemple, `CitrixWorkspaceApp.exe STARTMENUDIR=\Office`.

ENABLE_DYNAMIC_CLIENT_NAME

Description :

Autorise l'utilisation d'un nom de client identique au nom de machine. Lorsque vous modifiez le nom de machine, le nom de client change en conséquence.

- Yes (valeur par défaut) : autorise l'utilisation d'un nom de client identique au nom de machine. Par exemple, `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=Yes`.
- No : n'autorise pas l'utilisation d'un nom de client identique au nom de machine. Vous devez spécifier une valeur pour la propriété `CLIENT_NAME`. Par exemple, `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No`.

Paramètres d'authentification

ENABLE_SSON

Description :

Active l'authentification unique lorsque l'application Workspace est installée avec la commande `/includeSSON`. Consultez Authentification pass-through au domaine pour de plus amples informations.

- Yes (valeur par défaut) : indique que l'authentification unique est activée. Par exemple, `CitrixWorkspaceApp.exe /ENABLE_SSON=Yes`.
- No : indique que l'authentification unique est désactivée. Par exemple, `CitrixWorkspaceApp.exe /ENABLE_SSON=No`.

ENABLE_KERBEROS

Description :

Spécifie si le moteur HDX doit utiliser l'authentification Kerberos. Ce paramètre ne s'applique que lorsque l'authentification unique est activée. Pour plus d'informations, veuillez consulter l'article Authentification pass-through au domaine avec Kerberos.

- Yes : indique que le moteur HDX utilisera l'authentification Kerberos. Par exemple, `CitrixWorkspaceApp.exe ENABLE_KERBEROS=Yes`.
- No : indique que le moteur HDX n'utilisera pas l'authentification Kerberos. Par exemple, `CitrixWorkspaceApp.exe ENABLE_KERBEROS=No`.

Outre les propriétés ci-dessus, vous pouvez également spécifier l'adresse URL du magasin utilisée avec l'application Workspace. Vous pouvez ajouter jusqu'à 10 magasins. Utilisez la propriété suivante pour ce faire :


```
STOREx=" storename;http[s]://servername.domain/IISLocation/discovery;[On,
Off]; [storedescription]
```

Valeurs :

- x : entiers 0 à 9 utilisés pour identifier un magasin.
- storename : nom du magasin. Cette valeur doit correspondre au nom configuré sur le serveur StoreFront.
- servername.domain : nom de domaine complet du serveur hébergeant le magasin.
- IISLocation : chemin d'accès au magasin dans IIS. L'adresse URL du magasin doit correspondre à l'adresse URL du fichier de provisioning dans StoreFront. L'adresse URL du magasin se présente sous le format suivant `/Citrix/store/discovery`. Pour obtenir l'adresse URL, exportez un fichier de provisioning de StoreFront, ouvrez-le dans Bloc-notes et copiez l'adresse URL à partir de l'élément **Address**.
- [On, Off] : l'option **Off** vous permet de délivrer des magasins désactivés, ce qui laisse aux utilisateurs le choix d'y accéder ou non. Lorsque l'état du magasin n'est pas spécifié, le paramètre par défaut est **On**.
- storedescription : description facultative du magasin, telle que `HR App Store`.

> **Remarque :**
>
> - Il est obligatoire d'inclure `/discovery` dans l'adresse URL du magasin pour une authentification pass-through réussie.
> - L'adresse URL du magasin Citrix Gateway doit être la première entrée dans la liste des adresses URL de magasin configurées.

Mise à niveau à partir d'une version non prise en charge de l'application Citrix Workspace

> **Remarque :**
>
> Lorsque vous mettez à niveau Citrix Receiver pour Windows version 13.x Enterprise ou 12.x vers Citrix Receiver pour Windows Version 4.4 ou versions ultérieures à l'aide de l'interface utilisateur graphique, le programme d'installation exécute l'utilitaire de nettoyage de Receiver par défaut.

Toutefois, l'utilitaire n'est pas exécuté par défaut lorsque vous mettez à niveau à partir de la ligne de commande. Pour mettre à niveau à partir de la ligne de commande, exécutez la commande suivante :

```
CitrixWorkspaceApp.exe /rcu /silent
```

Lorsque vous mettez à niveau Citrix Receiver pour Windows 13.x (non Enterprise) ou 4.1 vers la version 4.2 ou versions ultérieures, le commutateur `/rcu` est inutile et donc ignoré.

Résolution des problèmes d'installation

En cas de problème avec l'installation, recherchez dans le répertoire %TEMP%/CTXWorkspaceInstallLogs de l'utilisateur les fichiers journaux comportant le préfixe CtxInstall- ou TrolleyExpress-. Exemple :

```
CtxInstall-ICAWebWrapper-20141114-134516.log
```

```
TrolleyExpress-20090807-123456.log
```

Exemples d'installation par ligne de commande

Pour spécifier l'adresse URL du magasin Citrix Gateway :

```
1 CitrixWorkspaceApp.exe HRStore;https://ag.mycompany.com#Storename;On;
     Store
```

où *Storename* indique le nom du magasin qui doit être configuré.

> **Remarque :**
>
> - L'adresse URL du magasin Citrix Gateway configurée à l'aide de cette méthode ne prend pas en charge les sites Services PNA qui utilisent Citrix Gateway.

Pour installer tous les composants de façon silencieuse et spécifier deux magasins applicatifs :

```
1 CitrixWorkspaceApp.exe /silent
2 STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;HR
     App Store"
3 STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/
     discovery;on;Backup HR App Store"
```

Pour spécifier le single sign-on (authentification pass-through) et ajouter un magasin pointant vers une adresse URL XenApp Services :

```
1 CitrixWorkspaceApp.exe / INCLUDESSON
2 /STORE0="PNAgent;https://testserver.net/Citrix/PNAgent/config.xml;on;
     MyPNAgent Site"
```

Utilisation d'Active Directory et d'exemples de scripts de démarrage

Vous pouvez utiliser des scripts de stratégie de groupe Active Directory pour déployer l'application Citrix Workspace pour Windows sur des systèmes en fonction de votre structure organisationnelle Active Directory. Citrix recommande d'utiliser les scripts plutôt que d'extraire les fichiers .msi. Pour

obtenir des informations générales sur les scripts de démarrage, reportez-vous à la documentation Microsoft.

Pour utiliser les scripts de démarrage avec Active Directory :

1. Créez l'unité d'organisation pour chaque script.
2. Créez un objet de stratégie de groupe (GPO) pour l'unité d'organisation que vous venez de créer.

Modifier les exemples de scripts

Modifiez les scripts avec les paramètres suivants dans la section d'en-tête de chaque fichier :

- **Version actuelle du package** - Le numéro de version spécifié est validé et s'il n'est pas présent, le déploiement se poursuit. Par exemple, DesiredVersion= 3.3.0.XXXX doit correspondre exactement à la version spécifiée. Si vous spécifiez une version partielle, par exemple 3.3.0, elle correspond à toute version avec ce préfixe (3.3.0.1111, 3.3.0.7777 et ainsi de suite).
- **Emplacement du package/répertoire de déploiement** - Ce paramètre spécifie le partage réseau contenant les packs. Il n'est pas authentifié par le script. Le dossier partagé doit disposer d'autorisations d'accès en lecture définies sur Tout le monde.
- **Répertoire de journalisation du script** - Ce paramètre spécifie le partage réseau sur lequel les journaux d'installation sont copiés. Il n'est pas authentifié par le script. Le dossier partagé doit disposer d'autorisations d'accès en lecture et écriture pour Tout le monde.
- **Options de ligne de commande d'installation du package** - Ces options de ligne de commande sont transmises au programme d'installation. Pour obtenir la syntaxe de la ligne de commande, consultez la section Utilisation des paramètres de ligne de commande.

Configuration par ordinateur à l'aide de scripts de démarrage

Citrix inclut des exemples de scripts de démarrage par ordinateur destinés à installer et désinstaller l'application Citrix Workspace. Les scripts se trouvent sur la page Téléchargements de l'application Citrix Workspace pour Windows.

- `CheckAndDeployWorkspacePerMachineStartupScript.bat`
- `CheckAndRemoveWorkspacePerMachineStartupScript.bat`

Pour ajouter des scripts de démarrage :

1. Ouvrez la Console de gestion des stratégies de groupe.
2. Sélectionnez **Configuration ordinateur** > **Stratégies** > **Paramètres Windows** > **Scripts (ouverture/fermeture de session)**.
3. Dans le panneau droit de la console Gestion des stratégies de groupe, sélectionnez **Démarrage**.
4. Dans le menu Propriétés, cliquez sur **Afficher les fichiers**, copiez le script approprié sur le dossier affiché et fermez la fenêtre.

5. Dans le menu Propriétés, cliquez sur **Ajouter** et utilisez le bouton **Parcourir** pour ajouter le script que vous venez de créer.

Pour déployer l'application Citrix Workspace pour Windows :

1. Déplacez les machines utilisateur désignées pour recevoir ce déploiement sur l'unité d'organisation que vous avez créée.
2. Redémarrez la machine utilisateur et ouvrez une session.
3. Vérifiez que le package que vous venez d'installer est répertorié dans Programmes et fonctionnalités.

Pour supprimer l'application Citrix Workspace pour Windows :

1. Déplacez les machines utilisateur désignées pour suppression sur l'unité d'organisation que vous avez créée.
2. Redémarrez la machine utilisateur et ouvrez une session.
3. Vérifiez que le package que vous venez d'installer n'est pas répertorié dans Programmes et fonctionnalités.

Configuration par utilisateur à l'aide de scripts de démarrage

Citrix recommande d'utiliser des scripts de démarrage par utilisateur. Dans le cadre de déploiements Windows par utilisateur, les deux scripts par utilisateur suivants de l'application Citrix Workspace pour Windows sont inclus sur le support Citrix Virtual Apps and Desktops dans le dossier Citrix Workspace for Windows et `Plug-ins\Windows\\Workspace\Startup\Logon\Scripts`.

- `CheckAndDeployWorkspacePerUserLogonScript.bat`
- `CheckAndRemoveWorkspacePerUserLogonScript.bat`

Pour ajouter des scripts de démarrage :

1. Ouvrez la Console de gestion des stratégies de groupe.
2. Sélectionnez **Configuration utilisateur** > **Stratégies** > **Paramètres Windows** > **Scripts**.
3. Dans le panneau droit de la console Gestion des stratégies de groupe, sélectionnez **Ouverture de session**.
4. Dans le menu Propriétés de : Ouverture de session, cliquez sur **Afficher les fichiers**, copiez le script approprié sur le dossier affiché et fermez la fenêtre.
5. Dans le menu Propriétés de : Ouverture de session, cliquez sur **Ajouter** et utilisez le bouton Parcourir pour trouver et ajouter le nouveau script que vous venez de créer.

Pour déployer l'application Citrix Workspace pour Windows :

1. Déplacez les utilisateurs désignés pour recevoir ce déploiement sur l'unité d'organisation que vous avez créée.
2. Redémarrez la machine utilisateur et ouvrez une session en tant qu'un des utilisateurs spécifiés.

3. Vérifiez que Programmes et fonctionnalités (Ajout/Suppression de programmes dans les versions antérieures du système d'exploitation) contient le nouveau pack installé.

Pour supprimer l'application Citrix Workspace pour Windows :

1. Déplacez les utilisateurs désignés pour suppression sur l'unité d'organisation que vous avez créée.
2. Redémarrez la machine utilisateur et ouvrez une session en tant qu'un des utilisateurs spécifiés.
3. Vérifiez que Programmes et fonctionnalités (Ajout/Suppression de programmes dans les versions antérieures du système d'exploitation) a supprimé le pack préalablement installé.

Utilisation de Workspace pour Web

Vous pouvez déployer l'application Citrix Workspace pour Windows à partir de Workspace pour Web pour vous assurer qu'elle est installée avant de vous connecter à une application à partir d'un navigateur. Les sites Workspace pour Web vous permettent d'accéder aux magasins StoreFront via une page Web. Si le site Workspace pour Web détecte qu'un utilisateur ne possède pas une version compatible de l'application Citrix Workspace pour Windows, vous êtes invité à télécharger et installer l'application Citrix Workspace pour Windows.

La découverte de compte basée sur une adresse e-mail n'est pas prise en charge lorsque l'application Citrix Workspace pour Windows est déployée à l'aide de Workspace pour Web. Si la découverte de compte basée sur une adresse e-mail est configurée et qu'un nouvel utilisateur installe l'application Citrix Workspace pour Windows à partir de Citrix.com, l'application invite l'utilisateur à entrer une adresse e-mail ou de serveur. La saisie d'une adresse e-mail entraîne le message d'erreur suivant : « Votre e-mail ne peut pas être utilisée pour ajouter un compte. »

Utilisez la configuration suivante pour inviter l'utilisateur à entrer uniquement l'adresse d'un serveur.

1. Téléchargez `CitrixWorkspaceApp.exe` sur votre ordinateur local.
2. Renommez `CitrixWorkspaceApp.exe` : `CitrixWorkspaceWeb.exe`.
3. Déployez le fichier exécutable renommé à l'aide de votre méthode de déploiement habituelle. Si vous utilisez StoreFront, consultez la section Configurer des sites Workspace pour Web à l'aide des fichiers de configuration dans la documentation de StoreFront.

Utilisation de System Center Configuration Manager 2012 R2

Vous pouvez utiliser Microsoft System Center Configuration Manager (SCCM) pour déployer l'application Citrix Workspace.

> **Remarque :**
>
> Seules la version 4.5 et les versions ultérieures de Citrix Receiver pour Windows prennent en

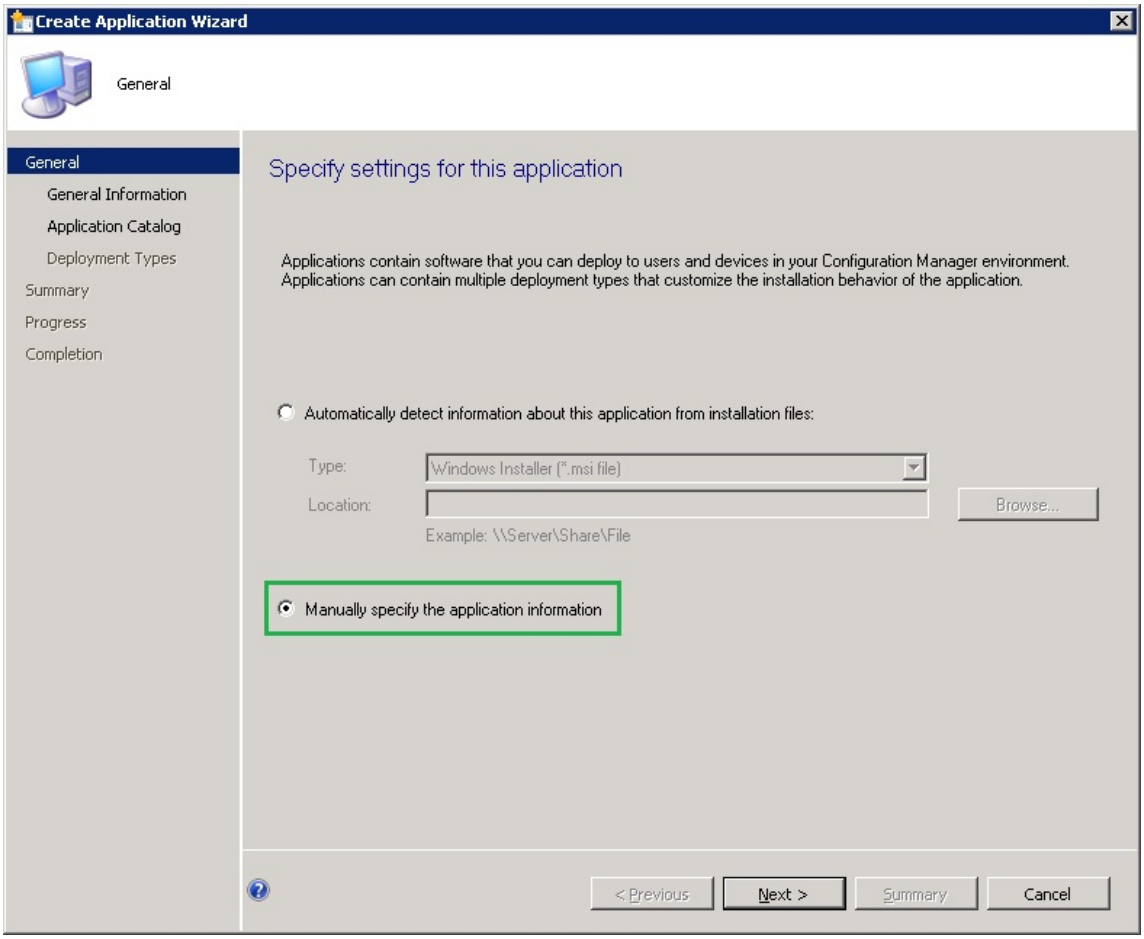
> charge le déploiement de SCCM.

Quatre tâches sont nécessaires au déploiement de l'application Citrix Workspace pour Windows à l'aide de SCCM :

1. Ajout de l'application Citrix Workspace pour Windows au déploiement SCCM
2. Ajout de points de distribution
3. Déploiement de l'application Citrix Workspace sur le Centre logiciel
4. Création de regroupements de périphériques

Ajout de l'application Citrix Workspace pour Windows au déploiement SCCM

1. Copiez le dossier d'installation de l'application Citrix Workspace téléchargé vers un dossier sur le serveur de Configuration Manager et démarrez la console Configuration Manager.
2. Sélectionnez **Bibliothèque de logiciels** > **Gestion d'applications**. Cliquez avec le bouton droit de la souris sur **Application** et cliquez sur **Créer une application**.
   L'assistant Créer une application s'affiche.

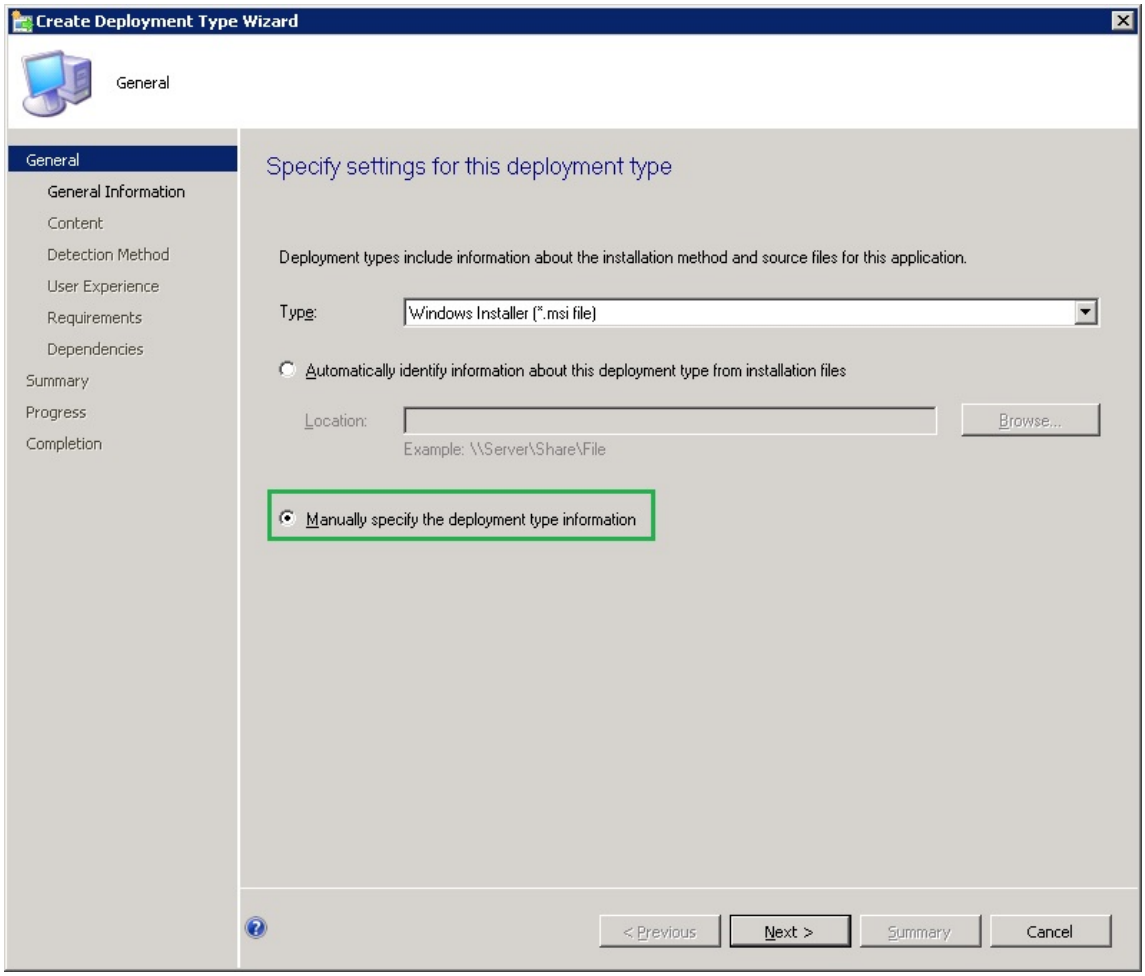


3. Dans le panneau **Général**, sélectionnez **Spécifier manuellement les informations de l'application** et cliquez sur **Suivant**.
4. Dans le panneau **Informations générales**, spécifiez les informations relatives à l'application comme le nom, le fabricant, la version du logiciel, etc.
5. Dans l'Assistant Catalogue d'applications, spécifiez des informations supplémentaires telles que la langue, le nom de l'application, la catégorie utilisateur, etc. et cliquez sur **Suivant**.

   > **Remarque :**
   >
   > Les utilisateurs peuvent voir les informations que vous spécifiez ici.

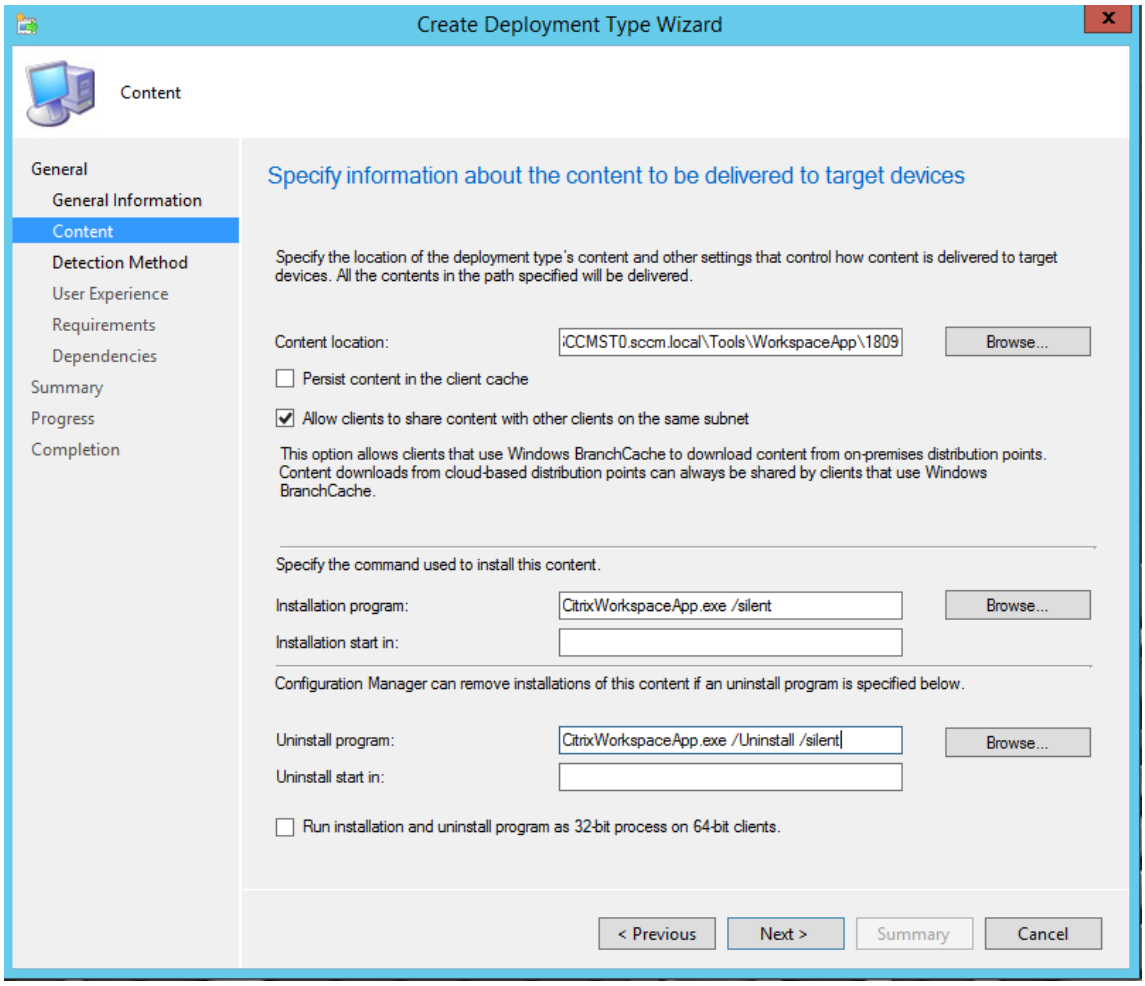
6. Dans le panneau **Type de déploiement**, cliquez sur **Ajouter** pour configurer le type de déploiement pour l'installation de l'application Citrix Workspace.

   L'Assistant Création d'un type de déploiement s'affiche.

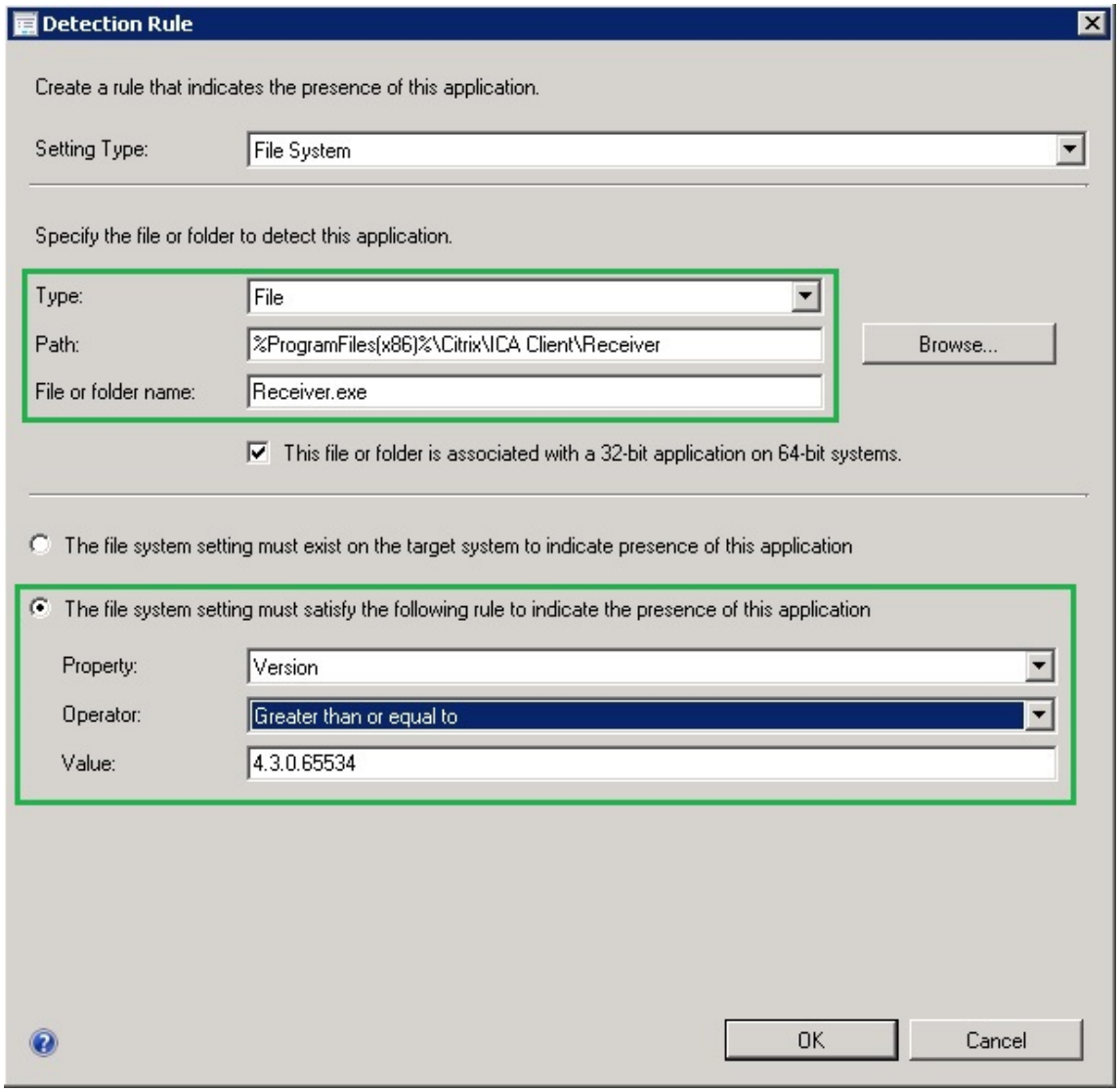


7. Dans le panneau **Général** : définissez le type de déploiement sur Windows Installer (fichier *.msi), sélectionnez **Spécifier manuellement les informations sur le type de déploiement** et cliquez sur **Suivant**.

8. Dans le panneau **Informations générales** : spécifiez les détails du type de déploiement (par exemple, déploiement de Workspace) et cliquez sur **Suivant**.
9. Dans le panneau **Contenu** :
   a) Spécifiez le chemin d'accès au fichier d'installation de l'application Citrix Workspace. Par exemple : Outils sur le serveur SCCM.
   b) Spécifiez **Programme d'installation** en utilisant un des éléments suivants :
      - `CitrixWorkspaceApp.exe /silent` pour une installation silencieuse par défaut.
      - `CitrixWorkspaceApp.exe /silent /includeSSON` pour activer l'authentification pass-through au domaine.
      - `CitrixWorkspaceApp.exe /silent SELFSERVICEMODE=false` pour installer l'application Citrix Workspace en mode de non libre-service.
   c) Spécifiez **Programme de désinstallation** sur `CitrixWorkspaceApp.exe /uninstall` (pour permettre la désinstallation via SCCM).



10. Dans le panneau **Méthode de détection** : sélectionnez **Configurer des règles pour détecter la présence de ce type de déploiement** et cliquez sur **Ajouter une clause**.
    La boîte de dialogue Règle de détection s'affiche.



- Définissez **Type de paramètre** sur Système de fichiers.
- Sous **Spécifier le fichier ou dossier pour détecter l'application**, définissez ce qui suit :
  - **Type** : à partir du menu déroulant, sélectionnez Fichier.
  - **Chemin** : %ProgramFiles (x86)%\Citrix\ICA Client\Receiver\
  - **Nom du fichier ou du dossier** : receiver.exe
  - **Propriété** : à partir du menu déroulant, sélectionnez **Version**.
  - **Opérateur** : à partir du menu déroulant, sélectionnez **Supérieur ou égal à**.
  - **Valeur** : entrez **4.3.0.65534**.

> **Remarque :**
>
> Cette combinaison de règles s'applique également aux mises à niveau de l'application Citrix Workspace pour Windows.

11. Dans le panneau **Expérience utilisateur**, définissez :

- **Comportement à l'installation** : Installer pour le système
- **Condition d'ouverture de session** : Qu'un utilisateur soit connecté ou non
- **Visibilité du programme d'installation** : Normal

  Cliquez sur Suivant.

> **Remarque :**
>
> Ne spécifiez aucune exigence ou dépendance pour ce type de déploiement.

12. Dans le panneau **Résumé**, vérifiez les paramètres pour ce type de déploiement. Cliquez sur **Next**.

    Un message de réussite s'affiche.

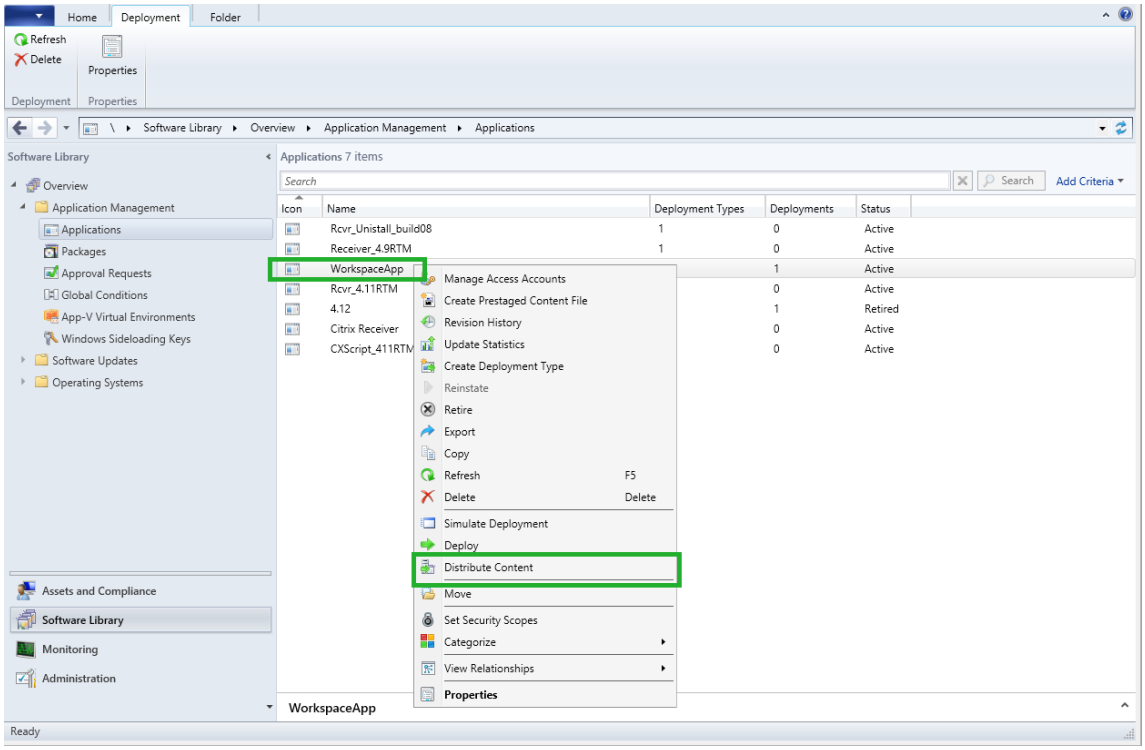
13. Dans le panneau **Progression**, un nouveau type de déploiement (déploiement de Workspace) est répertorié sous les types de déploiement.

14. Cliquez sur **Suivant** et sur **Fermer**.

Ajouter des points de distribution

1. Cliquez avec le bouton droit de la souris sur l'application Citrix Workspace dans la console Configuration Manager et sélectionnez **Distribuer du contenu**.

   L'assistant Distribuer du contenu s'affiche.



2. Dans le panneau de Distribuer du contenu, cliquez sur **Ajouter > Points de distribution**.

La boîte de dialogue Ajouter des points de distribution s'affiche.

3. Recherchez le serveur SCCM sur lequel le contenu est disponible et cliquez sur **OK**.

   Un message de réussite s'affiche dans le panneau Progression.

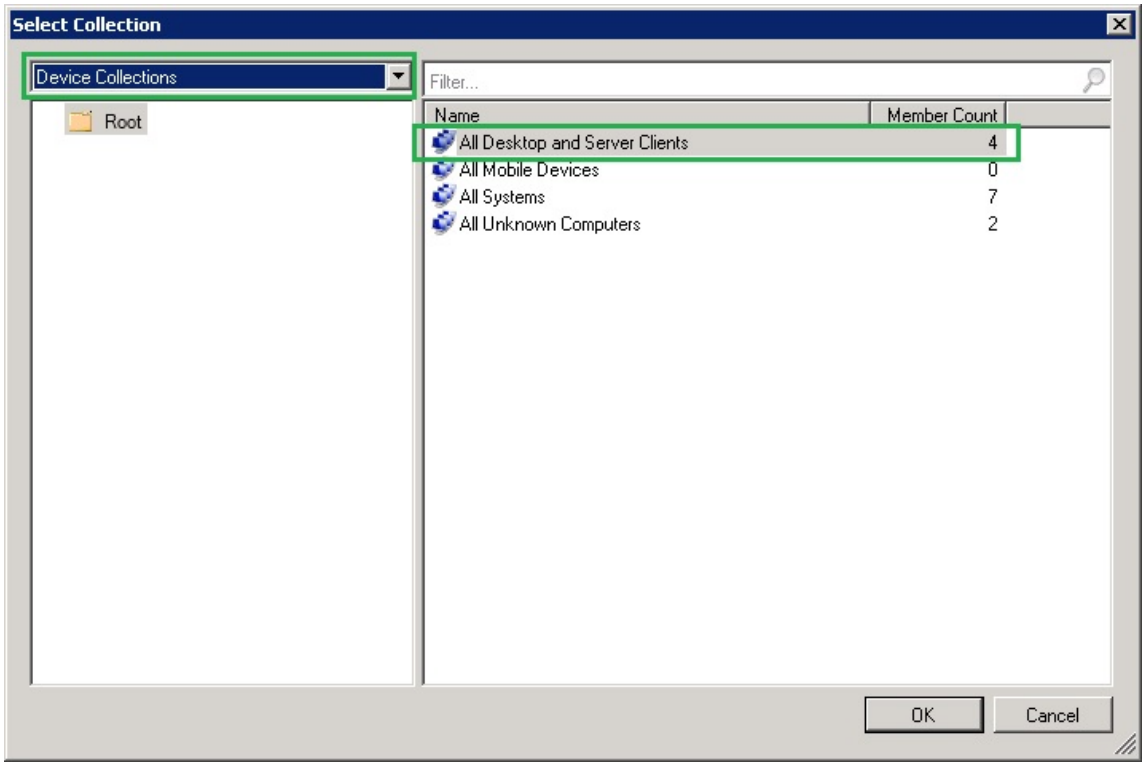
4. Cliquez sur **Fermer**.

Déployer l'application Citrix Workspace sur le Centre logiciel

1. Cliquez avec le bouton droit de la souris sur l'application Citrix Workspace dans la console Configuration Manager et sélectionnez **Déployer**.

   L'Assistant Déployer le logiciel s'affiche.

2. Sélectionnez **Parcourir** dans Regroupement (il peut s'agir de Regroupement de périphériques ou Regroupement d'utilisateurs) pour sélectionner le regroupement vers lequel vous souhaitez déployer l'application et cliquez sur **Suivant**.



3. Dans le panneau **Paramètres de déploiement**, définissez **Action** sur Installer et **Objet** sur Obligatoire (active l'installation non assistée). Cliquez sur **Next**.

4. Dans le panneau **Planification**, spécifiez le programme de déploiement du logiciel sur les machines cibles.

5. Dans le panneau **Expérience utilisateur**, définissez le comportement **Notifications utilisateur** ; sélectionnez **Valider les modifications à l'échéance ou au cours d'une fenêtre de mainte-**

nance (requiert un redémarrage) et cliquez sur **Suivant** pour terminer l'Assistant Déploiement logiciel.

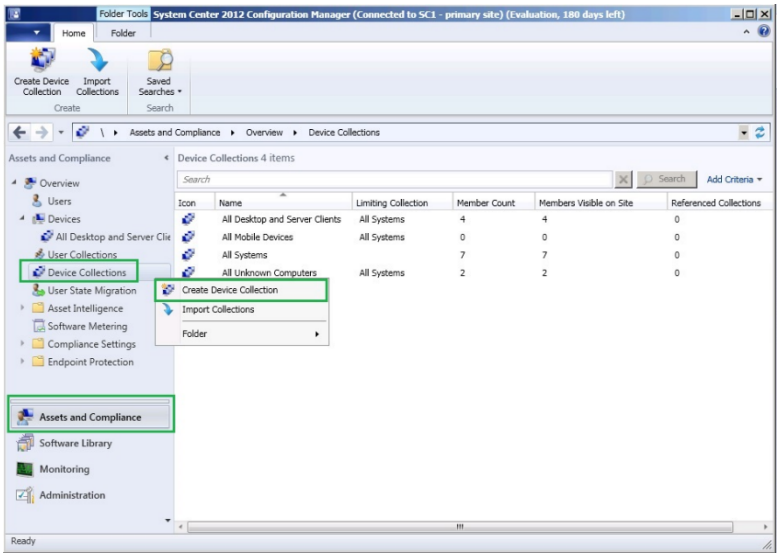
Un message de réussite s'affiche dans le panneau Progression.

Redémarrez les machines de point de terminaison cibles (uniquement requis pour démarrer l'installation immédiatement).

Sur les machines de point de terminaison, l'application Citrix Workspace pour Windows est visible dans le Centre logiciel sous **Logiciels disponibles**. L'installation est déclenchée automatiquement en fonction du programme que vous avez configuré. Éventuellement, vous pouvez également programmer ou installer à la demande. L'état de l'installation s'affiche dans le Centre logiciel après le démarrage de l'installation.

Création de regroupements de périphériques

1. Démarrez la console Configuration Manager, cliquez sur **Ressources et Conformité** > **Présentation** > **Périphériques**.



2. Cliquez avec le bouton droit de la souris sur **Regroupements de périphériques** et sélectionnez **Créer un regroupement de périphériques**.

   L'Assistant Création d'un regroupement de périphériques s'affiche.

3. Dans le panneau Général, tapez le **nom** du périphérique et cliquez sur **Parcourir** pour Limitation au regroupement.

   Cela détermine l'étendue des périphériques, qui peut être l'un des Regroupements de périphériques par défaut créé par SCCM.
   Cliquez sur **Suivant**.

4. Dans le panneau Règles d'adhésion, cliquez sur **Ajouter une règle** pour filtrer les périphériques.

   L'Assistant Création d'une règle d'adhésion directe s'affiche.

   - Dans le panneau Rechercher des ressources, sélectionnez **Nom d'attribut** en fonction des périphériques que vous souhaitez filtrer et entrez la valeur de nom d'attribut pour sélectionner les périphériques.

5. Cliquez sur **Next**. Dans le panneau Sélectionner les ressources, sélectionnez les périphériques qui doivent faire partie du regroupement de périphériques.

   Un message de réussite s'affiche dans le panneau Progression.

6. Cliquez sur **Fermer**.

7. Dans le panneau Règles d'adhésion, une nouvelle règle est répertoriée sous Cliquez sur Suivant.

8. Un message de réussite s'affiche dans le panneau Progression. Cliquez sur **Fermer** pour fermer l'assistant Création d'un regroupement de périphériques.

   Le nouveau regroupement de périphériques est répertorié dans **Regroupements de périphériques**. Le nouveau regroupement de périphériques fait partie des Regroupements de périphériques lors de la navigation dans l'Assistant Déployer le logiciel.

> **Remarque :**
>
> Lorsque vous définissez l'attribut **MSIRESTARTMANAGERCONTROL** sur **False**, le déploiement de l'application Citrix Workspace pour Windows à l'aide de SCCM peut échouer.
> D'après notre analyse, l'échec n'est pas dû à l'application Citrix Workspace pour Windows. En outre, une nouvelle tentative peut se solder par un déploiement réussi.

Désinstallation

Vous pouvez désinstaller l'application Citrix Workspace pour Windows à l'aide de l'utilitaire Programmes et fonctionnalités de Windows (Ajout/Suppression de programmes).

> **Remarque :**
>
> Vous êtes invité à désinstaller le package Citrix HDX RTME avant de poursuivre l'installation de l'application Citrix Workspace pour Windows. Cliquez sur OK pour poursuivre la désinstallation.

Désinstaller à l'aide de l'interface de ligne de commande :

Vous pouvez désinstaller l'application Citrix Workspace pour Windows à partir d'une ligne de commande en tapant la commande suivante :

```
CitrixWorkspaceApp.exe /uninstall
```


Les clés de registre créées par receiver.adm/receiver.adml ou receiver.admx demeurent dans le répertoire Software\Policies\Citrix\ICA Client sous HKEY_LOCAL_MACHINE et HKEY_LOCAL_USER après la désinstallation.

Lorsque vous réinstallez l'application Citrix Workspace pour Windows, il est possible que ces stratégies s'appliquent et entraînent un comportement inattendu. Pour supprimer les personnalisations, supprimez-les manuellement.

Pour la désinstallation en mode silencieux de l'application Citrix Workspace pour Windows, exécutez le commutateur suivant :

```
CitrixWorkspaceApp.exe /silent/uninstall
```

Mise à niveau

Mise à niveau manuelle vers l'application Citrix Workspace pour Windows

Pour les déploiements avec StoreFront :

- Une recommandation pour vos utilisateurs BYOD (Bring Your Own Device) consiste à configurer les dernières versions de Citrix Gateway et de StoreFront comme décrit dans la documentation relative à ces produits sur le site de documentation produit. Joignez le fichier de provisioning créé par StoreFront à un e-mail et indiquez aux utilisateurs comment procéder à la mise à niveau et ouvrir le fichier de provisioning après l'installation de l'application Citrix Workspace pour Windows.
- Si vous ne souhaitez pas utiliser le fichier de provisioning, demandez aux utilisateurs d'entrer l'adresse URL de Citrix Gateway. Ou, si vous avez configuré la découverte de compte basée sur une adresse e-mail comme décrit dans la documentation StoreFront, demandez aux utilisateurs d'entrer leur adresse e-mail.
- Une autre méthode consiste à configurer un site Workspace pour Web comme décrit dans la documentation StoreFront et à procéder à la configuration décrite dans Utilisation de Workspace pour Web. Indiquez aux utilisateurs comment procéder à la mise à niveau de l'application Citrix Workspace pour Windows, accéder au site Workspace pour Web et télécharger le fichier de provisioning à partir de Workspace pour Web (cliquez sur le nom d'utilisateur et sur **Activer**).

Considérations à prendre en compte lors de la mise à niveau :

Pour plus d'informations sur les considérations à prendre en compte avant la mise à niveau de l'application Citrix Workspace pour Windows, consultez l'article CTX135933 du centre de connaissances.

Mise à niveau de l'application Citrix Workspace

Pour mettre à niveau la dernière application Citrix Workspace, effectuez l'une des opérations suivantes :

- Téléchargez l'application Citrix Workspace depuis la page de téléchargement Citrix.
- Mettez à niveau votre application Citrix Workspace à l'aide de votre magasin d'applications.
- Mettez automatiquement à jour l'application Citrix Workspace à partir de Citrix Receiver à l'aide des mises à jour de Citrix Workspace.

Mises à jour de Citrix Workspace

Lorsque vous configurez les mises à jour de Citrix Workspace à partir de l'application Citrix Workspace Windows, suivez l'une des méthodes ci-dessous par ordre de priorité :

1. Modèle d'administration d'objet de stratégie de groupe
2. Interface de ligne de commande
3. Préférences avancées (par utilisateur)

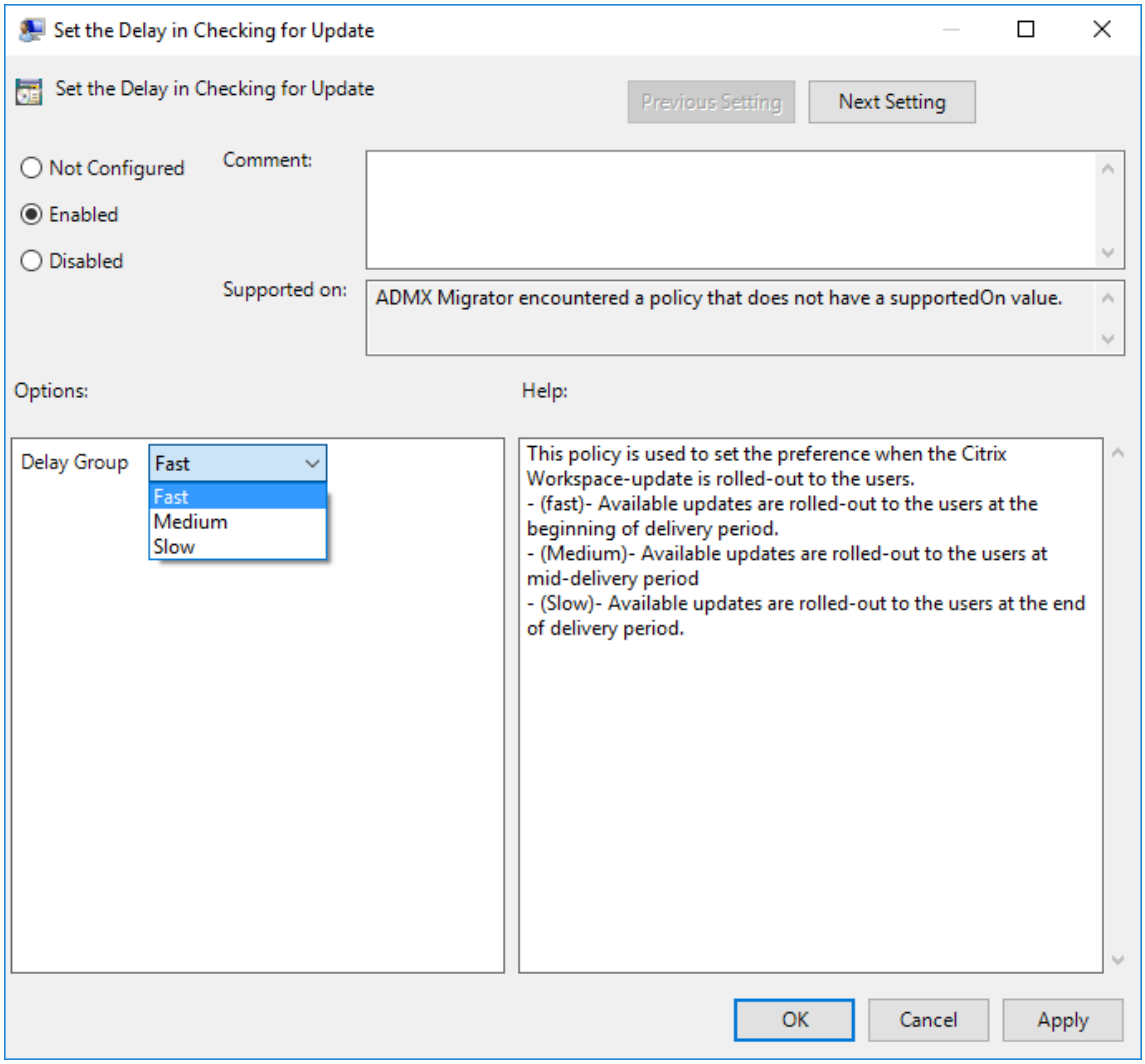
> **Remarque :**
>
> - Lorsque vous mettez à niveau l'application Citrix Workspace à l'aide des mises à jour, la fenêtre d'ouverture de session ne s'affiche pas.
> - HDX RTME pour Windows est inclus dans les mises à jour de Citrix Workspace. Vous êtes informé de la mise à jour HDX RTME disponible sur la version LTSR et la version actuelle de l'application Citrix Workspace.

Limitations :

1. Si vous avez configuré un proxy de sortie d'interception SSL, vous devez ajouter une exception pour le service Receiver auto-update Signature `https://citrixupdates.cloud.com/` et l'emplacement de téléchargement `https://downloadplugins.citrix.com/`.
2. Votre système doit avoir accès à Internet.
3. Les utilisateurs de Workspace pour Web ne peuvent pas télécharger automatiquement la stratégie de StoreFront.
4. Par défaut, les mises à jour de l'application Citrix Workspace sont désactivées sur le VDA. Cela comprend les machines de serveur multi-utilisateurs RDS, les machines VDI et les machines Remote PC.
5. Les mises à jour de l'application Citrix Workspace sont désactivées sur les machines sur lesquelles Desktop Lock est installé.

Configurer les mises à jour Citrix Workspace à l'aide du modèle d'administration d'objet de stratégie de groupe

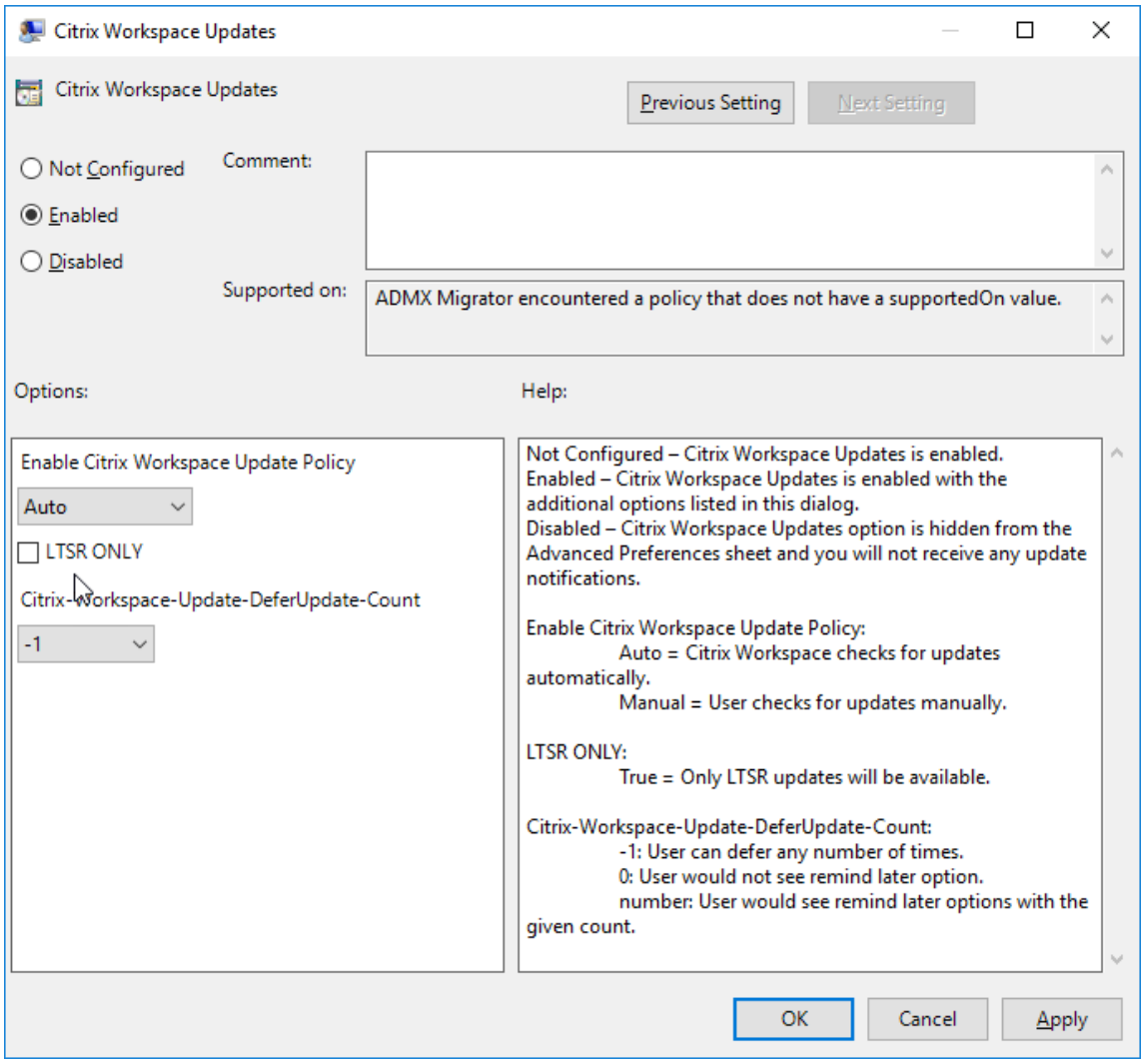
1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud Configuration ordinateur, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Mises à jour de Workspace**.
3. Sélectionnez la stratégie **Définir le délai de recherche de mises à jour**. Cette stratégie vous permet d'organiser le déploiement pendant une période.



4. Sélectionnez **Activé** et, à partir du menu déroulant **Retarder groupe**, sélectionnez l'une des options suivantes :
   - **Fast (Rapide)** : le déploiement de la mise à jour se produit au début de la période de mise à disposition.

- **Medium (Moyen)** : le déploiement de la mise à jour se produit au milieu de la période de mise à disposition.
- **Slow (Lent)** : le déploiement de la mise à jour se produit à la fin de la période de mise à disposition.

5. Cliquez sur **Appliquer** et **OK** pour enregistrer la stratégie.
6. Dans la section Modèles de mises à jour de Workspace, sélectionnez la stratégie **Mises à jour de Citrix Workspace**.



> **Remarque :**
>
> Lorsque vous sélectionnez **Désactivé**, vous n'êtes pas informé des mises à jour disponibles. Cela masque également l'option **Mises à jour de Workspace** sur la page **Préférences avancées**.

7. Sélectionnez **Activé** et définissez les valeurs selon vos besoins :
   - À partir du menu déroulant **Stratégie d'activation de la mise à jour de Citrix Workspace**,

sélectionnez l'une des options suivantes :
  - **Auto** : vous êtes informé lorsqu'une mise à jour est disponible (valeur par défaut).
  - **Manuel** : vous n'êtes pas informé lorsque des mises à jour sont disponibles. Recherchez les mises à jour manuellement.
- Sélectionnez **LTSR UNIQUEMENT** pour obtenir les mises à jour de LTSR uniquement.
- Dans le menu déroulant **auto-update-DeferUpdate-Count**, sélectionnez une valeur comprise entre **-1** et **30**, où
  - **-1** indique que vous pouvez différer les notifications le nombre de fois souhaité (valeur par défaut = -1).
  - **0** indique que l'option **Me rappeler plus tard** ne s'affiche pas.
  - Tout autre nombre indique combien de fois l'option **Me rappeler plus tard** s'affiche. Par exemple, si vous définissez la valeur sur 10, l'option **Me rappeler plus tard** s'affiche 10 fois.

8. Cliquez sur **Appliquer** et **OK** pour enregistrer la stratégie.

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

Lors de l'installation de l'application Citrix Workspace pour Windows :

Pour configurer les paramètres de mise à jour de l'application Citrix Workspace en tant qu'administrateur à l'aide de paramètres de ligne de commande lors de l'installation de l'application Citrix Workspace pour Windows :

- /AutoUpdateCheck= auto/manual/disabled
- /AutoUpdateStream= LTSR/Current. Où LTSR fait référence à la version Long Term Service et Current fait référence à la version actuelle.
- /DeferUpdateCount= toute valeur entre -1 et 30
- /AURolloutPriority= auto/fast/medium/slow

Par exemple : `CitrixWorkspaceApp.exe /AutoUpdateCheck=auto /AutoUpdateStream=Current /DeferUpdateCount=-1 /AURolloutPriority=fast*`

- Pour configurer les paramètres de mise à jour de l'application Citrix Workspace en tant qu'utilisateur à l'aide de paramètres de ligne de commande lors de l'installation de Citrix Workspace pour Windows
  `/AutoUpdateCheck=auto/manual`

Par exemple : `CitrixWorkspaceApp.exe/AutoUpdateCheck=auto*`

La modification des paramètres de mise à jour de Citrix Workspace à l'aide du modèle d'administration d'objet de stratégie de groupe remplace les paramètres appliqués lors de l'installation de l'application Citrix Workspace pour tous les utilisateurs.

Après l'installation de l'application Citrix Workspace pour Windows :

Les mises à jour de Citrix Workspace peuvent être configurées après l'installation de l'application Citrix Workspace pour Windows.

Pour utiliser la ligne de commande :

Ouvrez l'invite de commande Windows et accédez au répertoire dans lequel se trouve **CitrixWorkspaceUpdater.exe**. En règle générale, CitrixWorkspaceUpdater.exe se trouve dans *CitrixWorkspaceInstallLocation*\Citrix\Ica Client\Workspace.

Vous pouvez également définir la stratégie de ligne de commande de mise à jour de Citrix Workspace à l'aide de ce fichier binaire.

Par exemple : les administrateurs peuvent utiliser les quatre options :

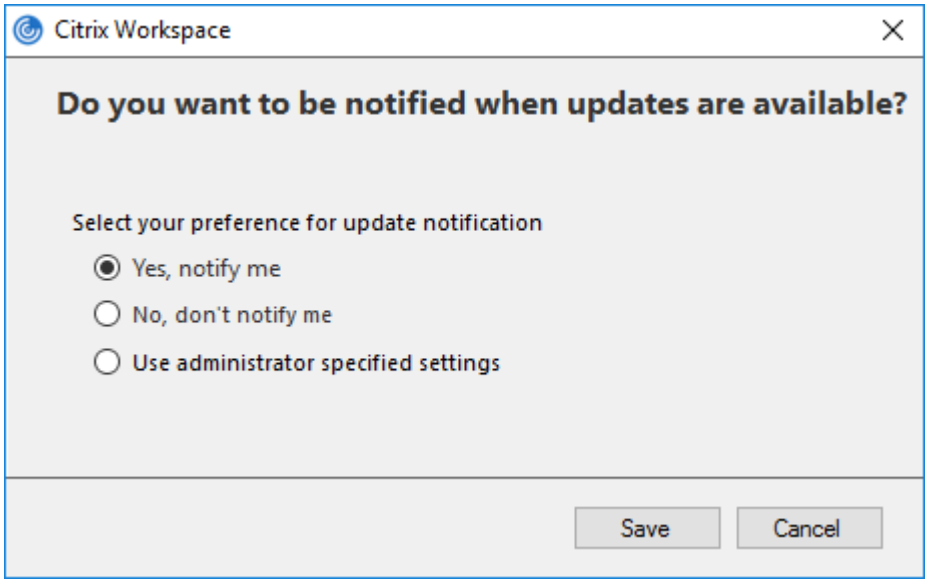
- CitrixWorkspaceUpdater.exe / AutoUpdateCheck=auto /AutoUpdateStream= Current/DeferUpdateCount=-1 / AURolloutPriority= fast

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

> **Remarque :**
>
> Vous pouvez masquer partiellement ou totalement la page Préférences avancées disponible à partir de l'icône de l'application Citrix Workspace dans la zone de notification. Pour plus d'informations, veuillez consulter l'article Masquer la page Préférences avancées.

Un utilisateur individuel peut remplacer le paramètre de mise 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.

1. Cliquez avec le bouton droit de la souris sur l'icône de l'application Citrix Workspace dans la zone de notification.
2. Sélectionnez **Préférences avancées** et cliquez sur **Mises à jour de Workspace**.



3. Sélectionnez l'une des options suivantes :
   - Oui, me notifier
   - Non, ne pas me notifier
   - Utiliser paramètres spécifiés par l'administrateur
4. Cliquez sur **Enregistrer**.

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

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

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

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

```
<properties>
       <clear/>
 </properties>
```

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

```
<account>

    <clear />

```



```
5     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
          F84Store"
6
7       description="" published="true" updaterType="Citrix"
            remoteAccessType="None">
8
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="auto" />
32
33              <property name="Auto-Update-DeferUpdate-Count" value
                    ="1" />
34
35                    <property name="Auto-Update-LTSR-Only" value
                          ="FALSE" />
36
37              <property name="Auto-Update-Rollout-Priority" value=
                    "fast" />
38
39                  </properties>
40
41          </metadata>
42
43        </annotatedServiceRecord>
44
```



```
45        </annotatedServices>
46
47        <metadata>
48
49          <plugins>
50
51            <clear />
52
53          </plugins>
54
55          <trustSettings>
56
57            <clear />
58
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
```

auto-update-Check

Cet attribut indique que l'application Citrix Workspace pour Windows détecte lorsqu'une mise à jour est disponible.

Valeurs possibles :

- Auto : vous êtes notifié lorsqu'une mise à jour est disponible (valeur par défaut).
- Manuel : vous n'êtes pas notifié lorsque des mises à jour sont disponibles. Recherchez les mises à jour manuellement.
- Désactivé : les mises à jour de Citrix Workspace sont masquées et vous ne serez pas averti lorsqu'une mise à jour est disponible.

auto-update-LTSR-Only

Cet attribut indique que l'application Citrix Workspace doit accepter les mises à jour uniquement pour la version LTSR.

Valeurs possibles :

- True : les mises à jour de Citrix Workspace recherchent uniquement les mises à jour LTSR de l'application Citrix Workspace pour Windows.
- False : les mises à jour de Citrix Workspace recherchent également les mises à jour non LTSR de l'application Citrix Workspace pour Windows.

auto-update-DeferUpdate-Count

Cet attribut indique le nombre de fois que vous pouvez différer les notifications. L'option **Me rappeler plus tard** s'affiche le nombre de fois défini.

Valeurs possibles :

- -1 : indique que vous pouvez différer les notifications n'importe quel nombre de fois (valeur par défaut = -1).
- 0 : indique que l'option Me rappeler plus tard ne s'affiche pas.
- Tout autre nombre : indique combien de fois l'option Me rappeler plus tard s'affiche. Par exemple, si vous définissez la valeur sur 10, l'option Me rappeler plus tard s'affiche 10 fois.

auto-update-Rollout-Priority

Cet attribut indique la période que vous pouvez définir pour le déploiement.

Valeurs possibles :

- Fast (Rapide) : le déploiement de la mise à jour se produit au début de la période de mise à disposition.
- Medium (Moyen) : le déploiement de la mise à jour se produit au milieu de la période de mise à disposition.
- Slow (Lent) : le déploiement de la mise à jour se produit à la fin de la période de mise à disposition.

Mise en route

March 18, 2019

Ce document de référence vous aide à configurer votre environnement après l'installation de l'application Citrix Workspace.

Conditions préalables :

Vérifiez que toutes les conditions requises pour le système sont satisfaites comme indiqué dans la section Configuration système requise.

Vous devez configurer les éléments suivants avant de commencer à utiliser l'application Citrix Workspace :

- Modèle d'administration d'objet de stratégie de groupe
- StoreFront
- Comptes utilisateur
- Mappage des lecteurs clients
- Résolution de nom DNS

Modèle d'administration d'objet de stratégie de groupe

Citrix recommande d'utiliser le modèle d'administration d'objet de stratégie de groupe pour configurer les règles du routage réseau, les serveurs proxy, la configuration de serveurs de confiance, le routage des utilisateurs, les machines utilisateur distantes et l'expérience de l'utilisateur.
Vous pouvez utiliser les fichiers de modèle receiver.admx / receiver.adml avec des stratégies de domaine et des stratégies sur l'ordinateur local. Pour les stratégies de domaine, importez le fichier de modèle à l'aide de la console de gestion des stratégies de groupe. Cela s'avère particulièrement utile pour appliquer les paramètres de l'application Citrix Workspace à différentes machines utilisateur réparties dans l'entreprise. Pour n'affecter qu'une seule machine utilisateur, importez le fichier de modèle à l'aide de l'éditeur de stratégie de groupe local sur la machine.

Citrix recommande d'utiliser le modèle d'administration d'objet de stratégie de groupe Windows pour configurer l'application Citrix Workspace.

À partir de Citrix Receiver pour Windows, version 4.6, le répertoire d'installation inclut `CitrixBase.admx` et CitrixBase.adml et les fichiers de modèle d'administration (receiver.adm ou receiver.admx\receiver.adml selon le système d'exploitation) dans le répertoire d'installation.

> **Remarque** le fichier .adm est uniquement destiné à être utilisé avec les plates-formes Windows XP Embedded. Les fichiers .admx/.adml sont uniquement destinés à être utilisés avec Windows Vista/Windows Server 2008 et toutes les versions ultérieures de Windows.

Si l'application Citrix Workspace a été installée avec le VDA, les fichiers admx/adml se trouvent dans le répertoire d'installation de l'application Citrix Workspace pour Windows. Par exemple : <répertoire d'installation>\Online Plugin\Configuration.

Si l'application Citrix Workspace a été installée sans le VDA, les fichiers admx/adml se trouvent généralement dans le répertoire C:\Program Files\Citrix\ICA Client\Configuration.

Reportez-vous au tableau ci-dessous pour plus d'informations sur les fichiers de modèle de l'application Citrix Workspace et leur emplacement.

> **Remarque :**
>
> Citrix recommande d'utiliser les fichiers de modèle d'objet de stratégie de groupe fournis avec la dernière version de l'application Citrix Workspace.

Type de fichier	Emplacements des fichiers
receiver.adm	<Répertoire d'installation>\ICA Client\Configuration
receiver.admx	<Répertoire d'installation>\ICA Client\Configuration
receiver.adml	<Répertoire d'installation>\ICA Client\Configuration\[MUIculture]
CitrixBase.admx	<Répertoire d'installation>\ICA Client\Configuration
CitrixBase.adml	<Répertoire d'installation>\ICA Client\Configuration\[MUIculture]

> **Remarque :**
>
> - Si CitrixBase.admx\adml n'est pas ajouté à cet objet de stratégie de groupe local, la stratégie **Activer la signature de fichier ICA** peut être perdue.
> - Lors de la mise à niveau de l'application Citrix Workspace, ajoutez les derniers fichiers de modèle à l'objet de stratégie de groupe local comme expliqué dans la procédure ci-dessous. Lors de l'importation de la dernière version des fichiers, les paramètres précédents sont conservés.

Pour ajouter le fichier de modèle receiver.adm à l'objet de stratégie de groupe local (système d'exploitation Windows XP Embedded uniquement) :

Citrix vous recommande d'utiliser les fichiers CitrixBase.admx et CitrixBase.adml pour vous assurer que les options sont correctement organisées et affichées dans l'éditeur d'objet de stratégie de groupe.

Vous pouvez utiliser des fichiers de modèle .adm pour configurer des objets de stratégie de groupe locaux et/ou des objets de stratégie de groupe de domaine.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Dans le panneau gauche de l'Éditeur de stratégie de groupe, sélectionnez le dossier **Modèles d'administration**.

3. À partir du menu **Action**, sélectionnez **Ajout/Suppression de modèles**.
4. Sélectionnez **Ajouter** et accédez à l'emplacement du fichier de modèle <Répertoire d'installation>\ICA Client\Configuration\receiver.adm
5. Cliquez sur **Ouvrir** pour ajouter le modèle, puis cliquez sur Fermer pour retourner à l'Éditeur de stratégie de groupe.
   Le fichier de modèle de l'application Citrix Workspace est disponible dans le répertoire de l'objet de stratégie de groupe local sous **Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Workspace**.

Une fois que les fichiers de modèle .adm sont ajoutés au GPO local, le message suivant s'affiche :
« L'entrée suivante de la section [strings] est trop longue et a été tronquée » :
cliquez sur **OK** pour ignorer le message.

Pour ajouter les fichiers de modèle receiver.admx/adml à l'objet de stratégie de groupe local (versions ultérieures du système d'exploitation Windows) :

Vous pouvez utiliser des fichiers de modèle .adm pour configurer des objets de stratégie de groupe locaux et/ou des objets de stratégie de groupe de domaine. Consultez l'article Microsoft MSDN sur la gestion des fichiers ADMX ici.

Après l'installation de l'application Citrix Workspace, copiez les fichiers de modèle comme indiqué dans le tableau ci-dessous :

Type de fichier	Copier à partir de	Copier sur
receiver.admx	Répertoire d'installation\ICA Client\Configuration\receiver.a	%systemroot%\policyDefinitions
CitrixBase.admx	Répertoire d'installation\ICA Client\Configuration\CitrixBase.admx	%systemroot%\policyDefinitions
receiver.adml	Répertoire d'installation\ICA Client\Configuration\[MUIcultu	%systemroot%\policyDefinitions[MUIculture
CitrixBase.adml	Répertoire d'installation\ICA Client\Configuration\[MUIculture]CitrixBase.adml	%systemroot%\policyDefinitions[MUIculture

> **Remarque :**
>
> Les fichiers de modèle de l'application Citrix Workspace sont disponibles sur l'objet de stratégie de groupe local dans le dossier **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** uniquement lorsque le fichier CitrixBase.admx/CitrixBase.adml est ajouté au dossier `\PolicyDefinitions`.

StoreFront

Citrix StoreFront authenticates a connection to Citrix Virtual Apps and Desktops, and VDI-in-a-Box, enumerating, and aggregating available desktops and applications into stores that you can access using Citrix Workspace app.

En plus de la configuration abordée dans cette section, vous devez également configurer Citrix Gateway afin de permettre aux utilisateurs de se connecter en dehors du réseau interne (par exemple, les utilisateurs qui se connectent à partir d'Internet ou d'emplacements distants).

> **Remarque :**
>
> Lorsque vous sélectionnez l'option permettant d'afficher tous les magasins, il est possible que l'ancienne interface utilisateur de StoreFront s'affiche.

Pour configurer StoreFront :

Installez et configurez StoreFront comme décrit dans la documentation StoreFront. L'application Citrix Workspace requiert une connexion HTTPS. Si le serveur StoreFront est configuré pour HTTP, une clé de registre doit être définie sur la machine utilisateur comme décrit dans la section Configure and install Workspace for Windows using command-line parameters sous la description de la propriété **ALLOWADDSTORE**.

> **Remarque :**
>
> Pour les administrateurs soucieux d'exercer un contrôle plus rigoureux, Citrix fournit un modèle que vous pouvez utiliser pour créer un site de téléchargement pour l'application Citrix Workspace pour Windows.

Citrix Gateway Store

Pour ajouter ou spécifier un Citrix Gateway à l'aide du modèle d'administration d'objet de stratégie de groupe :

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Modèles d'administration classiques (ADM)** > **Composants Citrix** > **Citrix Workspace** > **StoreFront**.
3. Sélectionnez **Liste de comptes StoreFront\URL de Citrix Gateway**.
4. Modifiez les paramètres.
    - Nom du magasin : indique le nom de magasin affiché
    - URL du magasin : indique l'adresse URL du magasin
    - #Store name : indique le nom du magasin derrière Citrix Gateway

- État activé du magasin : indique l'état du magasin, On/Off
- Description du magasin : fournit une description du magasin

5. Ajoutez ou spécifiez l'URL de Citrix Gateway. Entrez le nom de l'URL, séparé par des points-virgules :

Exemple : `https:` `//dtls.blrwinrx.com` #Store name.On; Store for HR staff
Où #Store name est le nom du magasin derrière Citrix Gateway ; `dtls.blrwinrx.com` est l'URL de Citrix Gateway.

Dans les versions précédentes, lorsque vous ajoutez ou supprimez un compte à l'aide de la stratégie **Liste de comptes StoreFront\URL de Citrix Gateway** dans l'objet de stratégie de groupe, vous devez réinitialiser Citrix Receiver pour que les modifications prennent effet.

À partir de la version 1808, les modifications apportées à la stratégie **Liste de comptes StoreFront\URL de Citrix Gateway** sont appliquées dans une session lorsque vous redémarrez l'application Citrix Workspace. Aucune réinitialisation n'est nécessaire.

> **Remarque :**
>
> La réinitialisation de l'application Citrix Workspace est inutile dans le cas d'une nouvelle installation de l'application Citrix Workspace version 1808 ou ultérieure. Dans le cas d'une mise à niveau vers la version 1808 ou une version ultérieure, réinitialisez l'application Citrix Workspace pour que les modifications prennent effet.

Limitations :

- L'URL de Citrix Gateway doit être indiquée en premier, suivie de l'adresse ou des adresses URL de StoreFront.
- Il n'est pas possible de spécifier plusieurs adresses URL de Citrix Gateway.
- Toute modification de l'URL de Citrix Gateway requiert la réinitialisation de l'application Citrix Workspace pour que les modifications prennent effet.
- L'URL de Citrix Gateway configurée à l'aide de cette méthode ne prend pas en charge le site Services PNA derrière Citrix Gateway.

Gérer la reconnexion au contrôle de l'espace de travail

Le contrôle de l'espace de travail permet aux applications de suivre les utilisateurs lorsqu'ils naviguent d'une machine à une autre. Ceci permet, par exemple, aux médecins hospitaliers de passer d'un poste de travail à un autre sans avoir à redémarrer leurs applications sur chaque machine. Pour l'application Citrix Workspace, vous pouvez gérer le contrôle de l'espace de travail sur les machines clientes en modifiant le registre. Pour les machines clientes appartenant au domaine, cela peut également se faire à l'aide d'une stratégie de groupe.

> **Attention**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Créez la clé **WSCReconnectModeUser** et modifiez la clé de registre existante **WSCReconnectMode** dans l'image de bureau principale ou le serveur Citrix Virtual Apps. Le bureau publié peut modifier le comportement de l'application Citrix Workspace.

Paramètres de la clé WSCReconnectMode pour l'application Citrix Workspace :

- 0 = non reconnecté aux sessions existantes
- 1 = reconnecté lors du lancement des applications
- 2 = reconnecté lors de l'actualisation des applications
- 3 = reconnecté lors de l'actualisation ou du lancement des applications
- 4 = reconnecté lors de l'ouverture de l'interface de Citrix Workspace
- 8 = reconnecté lors de l'ouverture de session Windows
- 11 = combinaison des paramètres 3 et 8

Désactiver le contrôle de l'espace de travail pour l'application Citrix Workspace

Pour désactiver le contrôle de l'espace de travail, créez la clé suivante :

`HKEY\\_CURRENT\\_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle` (64 bits)

`HKEY\\_CURRENT\\_USER\SOFTWARE\Citrix\\Dazzle` (32 bits)

Nom : **WSCReconnectModeUser**

Type : REG_SZ

Données de valeur : 0

Modifiez la valeur par défaut de la clé suivante de 3 à zéro

`HKEY\\_CURRENT\\_USER\SOFTWARE\Wow6432Node\Citrix\\Dazzle` (64 bits)

`HKEY\\_CURRENT\\_USER\SOFTWARE\Citrix\\Dazzle` (32 bits)

Nom : **WSCReconnectMode**

Type : REG_SZ

Données de valeur : 0

> **Remarque :**
>
> Vous pouvez également définir la valeur REG_SZ WSCReconnectAll sur false si vous ne voulez pas créer de clé.

Modification du délai de l'indicateur d'état

Vous pouvez modifier la durée pendant laquelle l'indicateur d'état s'affiche lorsqu'un utilisateur lance une session. Pour modifier cette durée, créez une valeur REG_DWORD de SI INACTIVE MS dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\. La valeur REG_DWORD peut être réglée sur 4 si vous voulez que l'indicateur d'état disparaisse plus tôt.

Personnalisation de l'emplacement du raccourci d'application depuis la ligne de commande

L'intégration du menu Démarrer et le mode de raccourci sur le bureau uniquement vous permettent d'afficher les raccourcis d'applications publiées dans le menu **Démarrer de Windows** et sur le bureau. Les utilisateurs n'ont pas à s'abonner à des applications à partir de l'interface utilisateur de Citrix Workspace. L'intégration du menu Démarrer et la gestion des raccourcis du bureau offrent une expérience de bureau transparente pour les groupes d'utilisateurs qui ont besoin d'accéder à un ensemble d'applications principales de manière cohérente.

En tant qu'administrateur de l'application Citrix Workspace, utilisez des indicateurs d'installation de ligne de commande, des objets de stratégie de groupe, des services de comptes ou des paramètres de registre pour désactiver l'interface en « libre-service » habituelle de l'application Citrix Workspace et la remplacer par un menu Démarrer préconfiguré. L'indicateur, nommé appelé **SelfServiceMode**, est défini sur true par défaut. Lorsque l'administrateur définit l'indicateur **SelfServiceMode** sur false, l'utilisateur n'a plus accès à l'interface utilisateur en libre-service de l'application Citrix Workspace. Au lieu de cela, ils peuvent accéder aux applications souscrites dans le menu Démarrer et via des raccourcis de bureau, référencés ici en tant que mode Raccourci uniquement.

Les utilisateurs et les administrateurs peuvent utiliser un certain nombre de paramètres de registre pour personnaliser la manière dont les raccourcis sont définis.

Utilisation des raccourcis

- Les utilisateurs ne peuvent pas supprimer les applications. Toutes les applications sont obligatoires lorsque vous utilisez l'indicateur **SelfServiceMode** défini sur false (mode Raccourci uniquement). Si l'utilisateur supprime une icône de raccourci du bureau, l'icône est rétablie lorsque l'utilisateur sélectionne Actualiser depuis l'icône application Citrix Workspace de la barre d'état système.

- Les utilisateurs ne peuvent configurer qu'un seul magasin. Les options Compte et Préférences ne sont pas disponibles. Ceci permet d'empêcher l'utilisateur de configurer d'autres magasins. L'administrateur peut accorder des privilèges spéciaux à un utilisateur pour ajouter plusieurs comptes à l'aide du modèle d'objet de stratégie de groupe, ou en ajoutant manuellement une clé de Registre (HideEditStoresDialog) sur la machine cliente. Lorsque l'administrateur accorde ce privilège à un utilisateur, l'utilisateur possède une option Préférences dans l'icône de la barre d'état système, où il peut ajouter et supprimer des comptes.
- Les utilisateurs ne peuvent pas supprimer d'applications à l'aide du **Panneau de configuration de Windows**.
- Vous pouvez ajouter des raccourcis de bureau via un paramètre de registre personnalisable. Les raccourcis de bureau ne sont pas ajoutés par défaut. Lorsque vous modifiez les paramètres de registre, redémarrez l'application Citrix Workspace.
- Les raccourcis sont créés dans le menu Démarrer avec un chemin d'accès de catégorie comme valeur par défaut, UseCategoryAsStartMenuPath.

> **Remarque :**
>
> Windows 8/8.1 et Windows 10 n'autorisent pas la création de dossiers imbriqués dans le menu Démarrer. Les applications sont affichées séparément ou sous le dossier racine mais pas dans les sous-dossiers de catégorie définis avec Citrix Virtual Apps.

- Vous pouvez ajouter un indicateur [/DESKTOPDIR=« Nom_Répertoire »] lors de l'installation pour rassembler tous les raccourcis dans un dossier unique. CategoryPath est pris en charge pour les raccourcis de bureau.
- Auto Reinstall Modified Apps est une fonctionnalité qui peut être activée via la clé de Registre AutoReInstallModifiedApps. Lorsque AutoReInstallModifiedApps est activée, toute modification apportée aux attributs des applications et bureaux publiés sur le serveur sont répercutées sur la machine cliente. Lorsque AutoReInstallModifiedApps est désactivée, les attributs d'applications et de bureaux ne sont pas mis à jour et les raccourcis ne sont pas stockés à nouveau lors de l'actualisation s'ils ont été supprimés sur le client. Par défaut, AutoReInstallModifiedApps est activée. Consultez la section Utilisation des clés de registre pour personnaliser l'emplacement des raccourcis d'applications.

Personnalisation de l'emplacement du raccourci d'application à l'aide de l'Éditeur de registre

> **Remarque :**
>
> - Les clés de registre utilisent par défaut le format de chaîne.
> - Nous vous recommandons d'apporter des modifications aux clés de registre avant de configurer un magasin. Si vous (ou un autre utilisateur) souhaitez personnaliser les clés de registre, vous devez réinitialiser l'application Citrix Workspace, configurer les clés de registre,

> puis reconfigurer le magasin.

Clés de registre pour machines 32 bits :

Registry key	Value	Key path
WSCSupported	True	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver\ SR\Store\" + primaryStoreID +\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Citrix \Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\Dazzle
WSCReconnectAll	True	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID + \Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Policies \Citrix\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\Dazzle
WSCReconnectMode	3	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID +\Properties • HKLM\SOFTWARE\Policies\Citrix \Dazzle • HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectModeUser	Registry is not created during installation	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID+\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Policies \Citrix\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE \Citrix\Dazzle

Clés de registre pour machines 64 bits :

Registry key	Value	Key path
WSCSupported	True	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Dazzle • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\D
WSCReconnectAll	True	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\Citrix\D
WSCreconnectMode	3	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver\SR\Store\"+ primaryStoreID +"\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectModeUser	Registry is not created during installation.	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver\SR\Store\"+ primaryStoreID+\Properties • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle

Comptes utilisateur

Vous pouvez fournir aux utilisateurs les informations de compte dont ils ont besoin pour accéder aux applications et bureaux virtuels à l'aide des éléments suivants :

- En configurant la découverte de compte basée sur une adresse e-mail
- Fichier de provisioning.
- En fournissant aux utilisateurs des informations de compte à entrer manuellement

> **Important**
>
> Citrix recommande de redémarrer l'application Citrix Workspace après l'installation. Cela garantit que les utilisateurs peuvent ajouter des comptes et que l'application Citrix Workspace peut détecter les périphériques USB qui étaient suspendus au moment de l'installation.

Une boîte de dialogue indiquant la réussite de l'installation s'affiche, suivie de la boîte de dialogue **Ajouter un compte**. Si vous utilisez le logiciel pour la première fois, la boîte de dialogue **Ajouter un compte** vous invite à entrer une adresse e-mail ou de serveur pour configurer un compte.

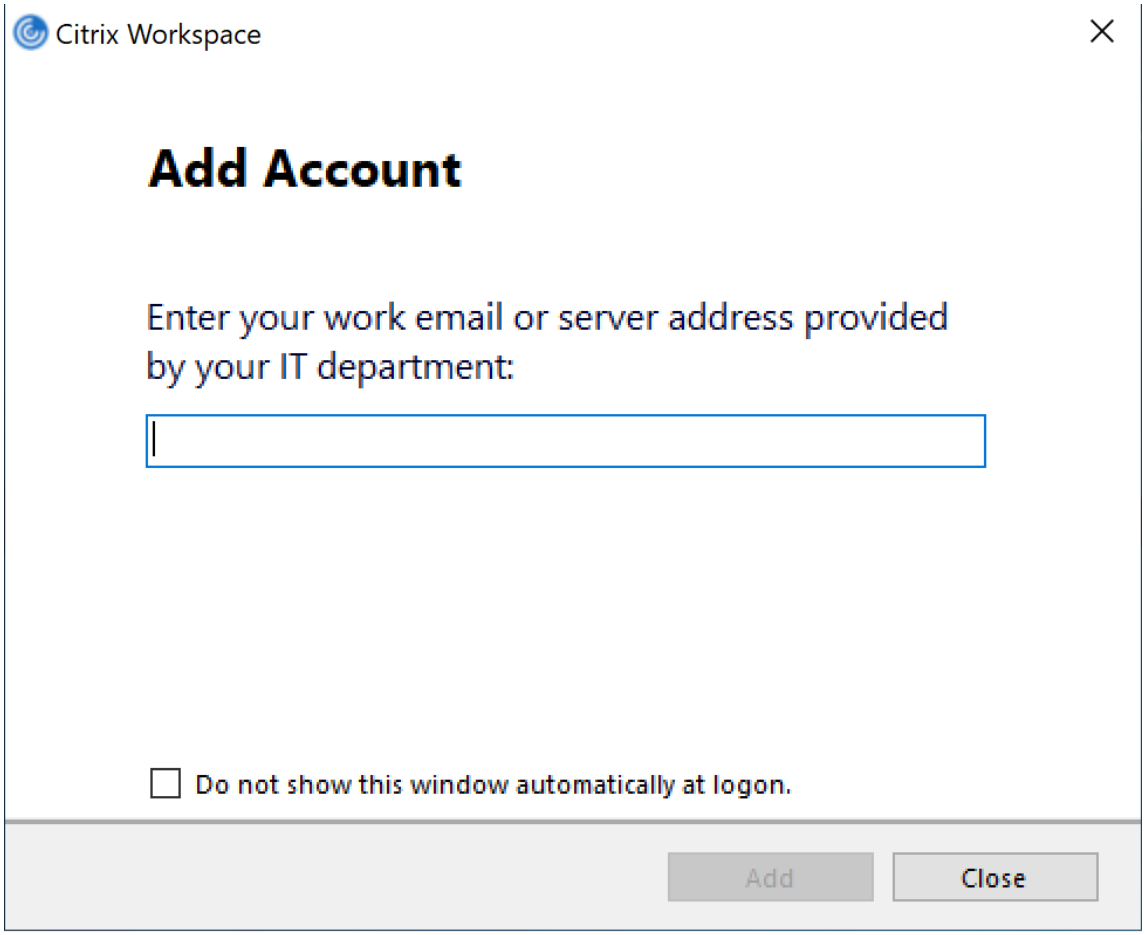
Suppression de la boîte de dialogue Ajouter un compte

La boîte de dialogue **Ajouter un compte** s'affiche lorsque le magasin n'est pas configuré. Dans la boîte de dialogue **Ajouter un compte**, vous pouvez créer un compte pour l'application Citrix Workspace en entrant une adresse e-mail ou une adresse URL de serveur.

L'application Citrix Workspace identifie le serveur Citrix Gateway ou StoreFront ou le boîtier virtuel App Controller associé à l'adresse e-mail et invite l'utilisateur à ouvrir une session pour l'énumération.

La boîte de dialogue Ajouter un compte peut être supprimée de l'une des manières suivantes :

1. **À l'ouverture de session sur le système**



Sélectionnez **Ne pas afficher cette fenêtre automatiquement à l'ouverture de session** pour que la fenêtre **Ajouter un compte** ne s'affiche pas au cours des ouvertures de session suivantes. Ce paramètre est spécifique à chaque utilisateur et se réinitialise au cours d'une action de réinitialisation de l'application Citrix Workspace pour Windows.

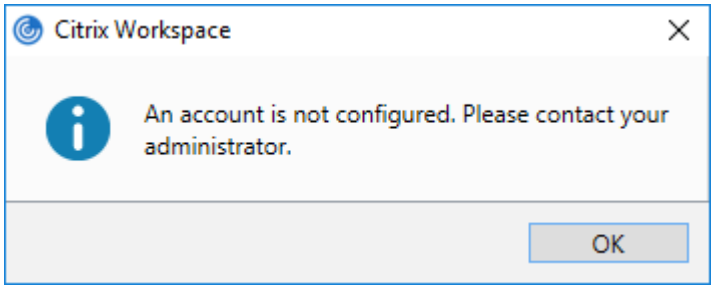
2. **Installation par ligne de commande**

   Installez l'application Citrix Workspace pour Windows en tant qu'administrateur avec le commutateur suivant sur l'interface de ligne de commande.

   ```
   CitrixWorkspaceApp.exe /ALLOWADDSTORE=N
   ```

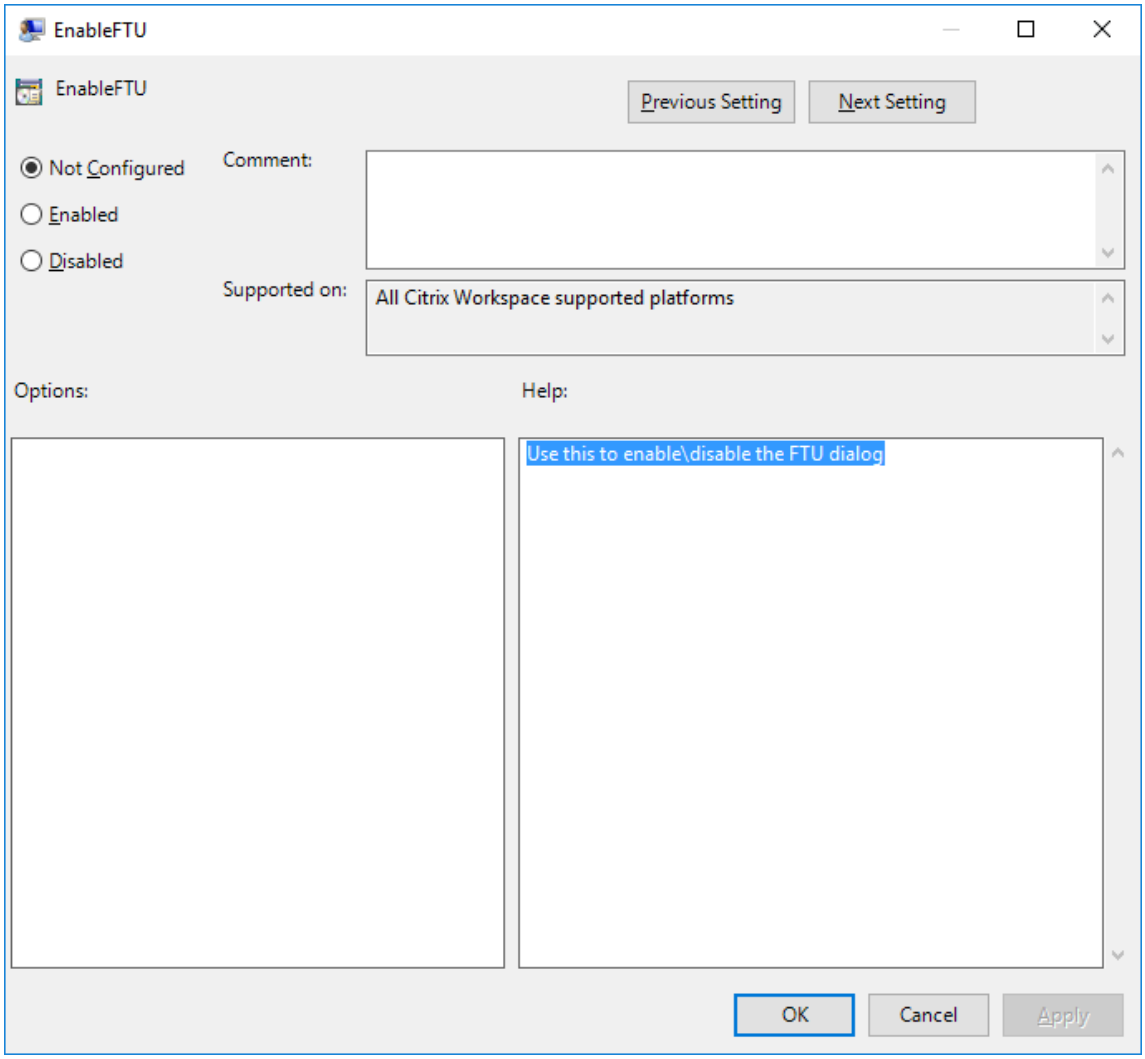
   Ce paramètre étant spécifique à la machine, il s'applique à tous les utilisateurs.

   Le message suivant s'affiche lorsque le magasin n'est pas configuré.



La boîte de dialogue **Ajouter un compte** peut être supprimée de l'une des manières suivantes.

- **Modifier le nom du fichier d'exécution de Citrix :**
  renommez **CitrixWorkspaceApp.exe CitrixWorkspaceWeb.exe** pour modifier le comportement de la boîte de dialogue **Ajouter un compte**. Si vous renommez ce fichier, la boîte de dialogue **Ajouter un compte** n'est pas affichée dans le menu Démarrer.
- **Modèle d'administration d'objet de stratégie de groupe :**
  pour masquer la boîte de dialogue **Ajouter un compte** à partir de l'assistant d'installation de l'application Citrix Workspace, désactivez **EnableFTUpolicy** sous le nœud Libre-service dans le modèle d'administration d'objet de stratégie de groupe local, comme illustré ci-dessous.
  Ce paramètre étant spécifique à la machine, il s'applique à tous les utilisateurs.



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

Lorsque vous configurez l'application Citrix Workspace pour la découverte de compte basée sur une adresse e-mail, au lieu d'entrer une adresse URL de serveur, les utilisateurs entrent leur adresse e-mail durant l'installation et la configuration initiales de l'application Citrix Workspace. L'application Citrix Workspace identifie le serveur Citrix Gateway ou StoreFront associé à l'adresse e-mail en se basant sur les enregistrements de service (SRV) de DNS, puis invite l'utilisateur à ouvrir une session pour accéder aux applications et aux bureaux virtuels.

> **Remarque :**
>
> La découverte de compte basée sur une adresse e-mail n'est pas prise en charge pour les déploiements avec l'Interface Web.

Pour plus d'informations, consultez la section Configurer la découverte de compte basée sur une adresse e-mail.

Fournir un fichier de provisioning aux utilisateurs

StoreFront fournit des fichiers de provisioning que les utilisateurs peuvent ouvrir pour se connecter aux magasins.

Vous pouvez utiliser StoreFront pour créer des fichiers de provisioning contenant les détails des comptes. Mettez ces fichiers à la disposition de vos utilisateurs pour leur permettre de configurer automatiquement l'application Citrix Workspace. Après l'installation de l'application Citrix Workspace, les utilisateurs n'ont qu'à ouvrir le fichier pour configurer l'application. Si vous configurez des sites Workspace pour Web, les utilisateurs peuvent également obtenir des fichiers de provisioning de l'application Citrix Workspace à partir de ces sites.

Pour plus d'informations, consultez la section Pour exporter les fichiers de provisioning de magasin pour des utilisateurs dans la documentation StoreFront.

Fournir aux utilisateurs des informations de compte à entrer manuellement

Pour permettre aux utilisateurs de créer des comptes manuellement, communiquez leur les informations dont ils ont besoin pour se connecter à leurs applications et bureaux virtuels.

- Pour les connexions à un magasin StoreFront, indiquez l'adresse URL de ce serveur. Par exemple : https://nomserveur.entreprise.com.

  Pour les déploiements Interface Web, fournissez l'adresse URL du site Citrix Virtual Apps and Desktops Services.

- Pour les connexions établies via Citrix Gateway, déterminez d'abord si l'utilisateur a accès à tous les magasins configurés ou uniquement au magasin dont l'accès distant est activé pour une passerelle Citrix Gateway particulière.

  - Pour présenter tous les magasins configurés : fournissez aux utilisateurs le nom de domaine complet de Citrix Gateway.
  - Pour limiter l'accès à un magasin particulier : fournissez aux utilisateurs le nom de domaine complet de Citrix Gateway ainsi que le nom du magasin au format :

CitrixGatewayFQDN?MyStoreName :

Par exemple, si un magasin nommé « AppsVentes » peut accéder à distance au serveur1.com et qu'un magasin nommé « AppsRH » peut accéder à distance au serveur2.com, un utilisateur doit entrer serveur1.com?AppsVentes pour accéder à AppsVentes ou serveur2.com?AppsRH pour accéder à AppsRH. Cette fonctionnalité requiert qu'un nouvel utilisateur crée un compte en entrant une adresse URL et elle n'est pas disponible pour la découverte basée sur l'adresse e-mail.

Lorsqu'un utilisateur entre les détails d'un nouveau compte, l'application Citrix Workspace tente de

vérifier la connexion. En cas de réussite, l'application Citrix Workspace invite l'utilisateur à se connecter au compte.

Pour gérer les comptes, ouvrez la page d'accueil de l'application Citrix Workspace, cliquez sur l'▾, puis cliquez sur **Comptes**.

Partage automatique de comptes de magasins multiples

> **Avertissement**
>
> Une utilisation incorrecte de l'Éditeur du Registre peut occasionner de sérieux problèmes qui pourraient nécessiter l'installation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à sauvegarder le registre avant de le modifier.

Si vous disposez de plusieurs comptes, vous pouvez configurer l'application Citrix Workspace pour Windows pour qu'elle se connecte automatiquement à tous les comptes lors de l'établissement d'une session. Pour afficher automatiquement tous les comptes lors de l'ouverture de l'application Citrix Workspace :

Pour les systèmes 32 bits, créez la clé « CurrentAccount » :

Emplacement : HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

Nom de la clé : CurrentAccount

Valeur : AllAccount

Type : REG_SZ

Pour les systèmes 64 bits, créez la clé « CurrentAccount » :

Emplacement : HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle

Nom de la clé : CurrentAccount

Valeur : AllAccount

Type : REG_SZ

Mappage des lecteurs clients

L'application Citrix Workspace pour Windows prend en charge le mappage de machines sur les machines utilisateur de sorte que les utilisateurs puissent accéder à ces machines à partir des sessions. Les utilisateurs peuvent effectuer les opérations suivantes :

- accéder de manière transparente aux lecteurs, aux imprimantes et aux ports COM locaux ;

- couper et coller des données entre la session et le Presse-papiers local de Windows ;
- entendre des données audio (sons système et fichiers .wav) lues dans la session.

Lors de l'ouverture de session, l'application Citrix Workspace indique au serveur les lecteurs, ports COM et ports LPT clients disponibles. Par défaut, les lecteurs clients sont mappés sur des lettres de lecteur serveur et des files d'impression de serveur sont créées pour les imprimantes clientes de sorte que ces dernières semblent connectées directement à la session. Ces mappages sont accessibles à l'utilisateur actuel et dans la session en cours uniquement. Ils sont supprimés à la fermeture de la session et créés de nouveau à l'ouverture de session suivante.

Vous pouvez utiliser les paramètres de redirection de stratégie pour mapper les machines utilisateur qui ne sont automatiquement mappées à l'ouverture de session. Pour de plus amples informations, consultez la documentation Citrix Virtual Apps and Desktops.

Désactivation du mappage des machines utilisateur

Vous pouvez configurer le mappage des machines utilisateur, notamment les options de lecteurs, d'imprimantes et de ports, à l'aide du **Gestionnaire de serveur Windows**. Pour plus d'informations sur les options disponibles, consultez votre documentation Services Bureau à distance.

Rediriger les dossiers clients

La redirection de dossiers clients modifie la manière dont les fichiers côté client sont accessibles sur la session côté hôte. Lorsque vous activez uniquement le mappage de lecteur client sur le serveur, les volumes complets côté client sont automatiquement mappés sur les sessions en tant que liens UNC (Universal Naming Convention). Lorsque vous activez la redirection de dossiers clients sur le serveur et que l'utilisateur la configure sur la machine utilisateur, la partie du volume local spécifié par l'utilisateur est redirigée.

Seuls les dossiers spécifiés par l'utilisateur s'affichent sous forme de liens UNC dans les sessions au lieu du système de fichiers complet sur la machine utilisateur. Si vous désactivez les liens UNC via le registre, des dossiers clients apparaissent comme des lecteurs mappés au sein de la session. Pour de plus amples informations, notamment comment configurer la redirection de dossiers clients pour les machines utilisateur, consultez la documentation Citrix Virtual Apps and Desktops.

Mapper des lecteurs clients sur des lettres de lecteur du côté hôte

Le mappage des lecteurs clients permet d'affecter des lettres de lecteur du côté hôte aux lecteurs existants sur la machine utilisateur. Par exemple, dans une session utilisateur Citrix, le lecteur H peut être mappé sur le lecteur C de la machine utilisateur qui exécute l'application Citrix Workspace pour Windows.

Le mappage des lecteurs clients fait partie intégrante des fonctions standard Citrix de redirection de périphérique de manière transparente. Pour le Gestionnaire de fichiers, l'Explorateur Windows et vos applications, ces mappages se présentent comme tout autre mappage réseau.

Le serveur hébergeant les applications et bureaux virtuels peut être configuré au cours de son installation pour mapper automatiquement les lecteurs du client sur un groupe de lettres de lecteur défini. Par défaut, l'installation mappe les lettres de lecteur affectées aux lecteurs du client en commençant par la lettre V et en remontant l'alphabet, en affectant une lettre de lecteur à chaque lecteur fixe et lecteur de CD-ROM. (Les lecteurs de disquettes sont affectés de leur lettre existante.) Cette méthode fournit les mappages de lecteur suivants dans une session :

Lettre du lecteur client	Accessible par le serveur sous :
Une	Une
B	B
C	V
D	U

Le serveur peut être configuré de façon à ce que les lettres de ses lecteurs n'entrent pas en conflit avec celles des lecteurs du client ; dans ce cas, les lettres des lecteurs du serveur sont remplacées par des lettres plus proches de la fin de l'alphabet. Par exemple, en remplaçant respectivement les lettres C et D des lecteurs du serveur par les lettres M et N, les machines clientes peuvent accéder directement à leurs disques C et D. Cette méthode produit les mappages suivants pour les lecteurs d'une session.

Lettre du lecteur client	Accessible par le serveur sous :
Une	Une
B	B
C	C
D	D

La nouvelle lettre de lecteur affectée au lecteur C du serveur est définie au moment de l'installation. Les lettres de tous les autres lecteurs de disque fixe et de CD-ROM sont remplacées par les lettres suivantes dans l'ordre alphabétique (par exemple : C > M, D > N, E > O). Elles ne doivent pas entrer en conflit avec les lettres déjà utilisées pour les mappages de lecteur réseau (effectués avec la commande Connecter un lecteur réseau). Si un mappage de lecteur réseau utilise une lettre déjà utilisée par un lecteur du serveur, le mappage de ce lecteur réseau est invalide.

Lorsqu'une machine utilisateur se connecte à un serveur, les mappages de ses lecteurs sont rétablis, sauf si le mappage automatique des machines clientes est désactivé. Le mappage des lecteurs clients est activé par défaut. Pour modifier les paramètres, utilisez l'utilitaire Configuration des services Bureau à distance (services Terminal Server). Vous pouvez aussi utiliser des stratégies vous permettant d'avoir un contrôle accru sur la manière dont le mappage des périphériques clients s'applique. Pour de plus amples informations sur les stratégies, consultez la documentation Citrix Virtual Apps and Desktops.

Redirection de périphérique USB Plug and Play HDX

La redirection de périphérique USB HDX Plug and Play permet de rediriger de manière dynamique les périphériques multimédia, tels que les appareils photo, les scanners, les lecteurs multimédia et les terminaux de point de vente, vers le serveur. Vous ou l'utilisateur pouvez limiter la redirection de tous les périphériques ou de certains périphériques. Modifiez les stratégies sur le serveur ou appliquez des stratégies de groupe sur la machine utilisateur pour configurer les paramètres de redirection. Pour plus d'informations, veuillez consulter la section Considérations USB et de lecteur client dans la documentation Citrix Virtual Apps and Desktops.

> **Important**
>
> Si vous interdisez la redirection des périphériques USB Plug and Play dans une stratégie de serveur, l'utilisateur ne peut pas remplacer ce paramètre de stratégie.

Un utilisateur peut définir des autorisations dans l'application Citrix Workspace pour autoriser ou rejeter systématiquement la redirection de périphérique chaque fois qu'un périphérique est connecté. Ce paramètre affecte uniquement les périphériques connectés après que l'utilisateur ait modifié le paramètre.

Pour mapper des ports COM clients à un port COM serveur :

Le mappage des ports COM clients permet d'utiliser, au cours de sessions, les périphériques connectés aux ports COM de la machine utilisateur. Ces mappages peuvent être utilisés de la même façon que n'importe quel mappage réseau effectué au moyen de la commande Connecter un lecteur réseau.

Vous pouvez mapper les ports COM clients à partir d'une invite de commande. Vous pouvez également contrôler le mappage des ports COM clients à partir de l'utilitaire Configuration des services Bureau à distance (services Terminal Server) ou à l'aide de stratégies. Pour de plus amples informations sur les stratégies, consultez la documentation Citrix Virtual Apps and Desktops.

> **Important**
>
> Le mappage des ports COM n'est pas compatible avec l'interface TAPI.

1. Pour les déploiements Citrix Virtual Apps and Desktops, activez le paramètre de stratégie Redirection de port COM client.

2. Ouvrez une session sur l'application Citrix Workspace.
3. À l'invite de commandes, entrez la commande suivante :

   ```
   net use comx: \\\\\client\\comz:
   ```

   où x correspond au numéro de port COM sur le serveur (les ports 1 à 9 peuvent être mappés) et z au numéro du port COM client à mapper.
4. Pour confirmer l'opération, entrez la commande suivante :

   ```
   net use
   ```

   à l'invite de commande. La liste qui apparaît affiche les lecteurs, ports LPT et ports COM mappés.

Pour utiliser ce port COM dans une application ou un bureau virtuel, installez votre machine utilisateur en utilisant le nom mappé. Par exemple, si le port COM1 du client est mappé sur le port COM5 du serveur, installez votre périphérique sur le port COM5 dans la session. Utilisez ce port COM comme vous utiliseriez n'importe quel autre port COM de la machine utilisateur.

Résolution de nom DNS

Vous pouvez configurer l'application Citrix Workspace pour Windows qui utilise le service XML Citrix pour qu'elle demande un nom DNS (Domain Name System) pour un serveur plutôt qu'une adresse IP.

> **Important :**
>
> À moins que votre environnement DNS ne soit configuré spécialement pour utiliser cette fonctionnalité, Citrix recommande de ne pas activer la résolution de nom DNS dans la batterie de serveurs.

L'application Citrix Workspace qui se connecte aux applications publiées via l'Interface Web utilise également le service XML Citrix. Pour l'application Citrix Workspace qui se connecte via l'Interface Web, le serveur Web résout le nom DNS pour l'application Citrix Workspace pour Windows.

La résolution de nom DNS est désactivée par défaut sur le serveur et activée par défaut sur l'application Citrix Workspace. Lorsque la résolution de nom DNS est désactivée sur le serveur, toute demande de nom DNS par l'application Citrix Workspace renvoie une adresse IP. Il n'est pas nécessaire de désactiver la résolution de nom DNS sur l'application Citrix Workspace.

Pour désactiver la résolution de nom DNS pour des machines utilisateur spécifiques :

Si votre déploiement de serveurs utilise la résolution de nom DNS et que vous rencontrez des problèmes avec des machines utilisateur spécifiques, vous pouvez désactiver la résolution de nom DNS pour ces machines.

> **Attention**
>
> Une utilisation incorrecte de l'Éditeur du Registre peut occasionner de sérieux problèmes qui pourraient nécessiter l'installation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à sauvegarder le registre avant de le modifier.

1. Ajoutez une clé de registre de chaîne **xmlAddressResolutionType** à `HKEY\\_LOCAL\\_MACHINE\Software\\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing`.
2. Définissez la valeur sur **IPv4-Port**.
3. Répétez l'opération pour chaque utilisateur des machines utilisateur.

Configurer

March 26, 2019

Lors de l'utilisation de l'application Citrix Workspace pour Windows, les configurations suivantes permettent aux utilisateurs d'accéder à leurs applications et bureaux hébergés :

Transport adaptatif

Le transport adaptatif est un mécanisme de transport de données plus rapide et évolutif qui améliore l'interactivité avec les applications et qui est plus adapté aux connexions WAN et Internet longue distance difficiles. Le transport adaptatif assure une capacité à monter en charge élevée du serveur et une utilisation efficace de la bande passante. Le transport adaptatif permet aux canaux virtuels ICA de répondre automatiquement aux conditions changeantes du réseau. Les canaux basculent intelligemment entre le protocole Citrix appelé Enlightened Data Transport (EDT) et TCP afin d'offrir des performances optimales. Cela améliore le transfert de données pour tous les canaux virtuels ICA, y compris la communication à distance d'écran Thinwire, le transfert de fichiers (mappage des lecteurs clients), l'impression et la redirection multimédia. Le même paramètre s'applique aux conditions LAN et WAN.

Dans les versions précédentes, lorsque **HDXoverUDP** est défini sur **Préféré**, le transport de données via EDT est utilisé lorsque c'est possible, avec retour vers TCP.

Lorsque la fiabilité de session est activée, EDT et TCP sont tentés en parallèle lors de la connexion initiale, de la reconnexion de la fiabilité de session et de la reconnexion automatique des clients. Cette amélioration réduit le temps de connexion lorsque EDT est le protocole préféré, mais le transport UDP sous-jacent requis est indisponible et TCP doit être utilisé.

Par défaut, après le repli vers TCP, le transport adaptatif continue d'interroger EDT toutes les 5 minutes.

Exigences :

- Citrix Virtual Apps and Desktops 7.12 ou version ultérieure requis pour activer la fonctionnalité à l'aide de Citrix Studio.
- StoreFront 3.8.
- VDA IPv4 uniquement. Les configurations IPv6 et IPv4/IPv6 ne sont pas prises en charge.
- Ajoutez des règles de pare-feu pour autoriser le trafic entrant sur les ports UDP 1494 et 2598 du VDA.

> **Remarque :**
>
> Les ports TCP 1494 et 2598 sont également requis et sont ouverts automatiquement lorsque vous installez le VDA. Toutefois, les ports UDP 1494 et 2598 ne sont pas ouverts automatiquement. Définissez-les sur **Activé**.

Le transport adaptatif doit être configuré sur le VDA via l'application de la stratégie pour être disponible pour les communications entre le VDA et l'application Citrix Workspace.

L'application Citrix Workspace facilite le transport adaptatif par défaut. Toutefois, et ceci également par défaut, le client tente d'utiliser le transport adaptatif uniquement si le VDA est configuré sur **Préféré** dans la stratégie Citrix Studio et si le paramètre a été appliqué sur le VDA.

Vous pouvez activer le transport adaptatif à l'aide du paramètre de stratégie **HDX Adaptive Transport**. Définissez la nouvelle stratégie sur **Préféré** pour utiliser le transport adaptatif lorsque cela est possible, avec basculement sur TCP.

Pour désactiver le transport adaptatif sur un client spécifique, définissez les options EDT appropriées à l'aide du modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace pour Windows.

Pour configurer le transport adaptatif à l'aide du modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace

Les étapes de configuration suivantes de personnalisation de votre environnement sont facultatives. Par exemple, vous pouvez choisir de désactiver la fonctionnalité pour un client particulier pour des raisons de sécurité.

> **Remarque :**
>
> Par défaut, le transport adaptatif est défini sur Désactivé et TCP est toujours utilisé.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.

2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Citrix Workspace** > **Routage réseau**.
3. Définissez la stratégie **Protocole de transport pour Receiver** sur **Activé**.
4. Sélectionnez le **protocole de communication pour Citrix Workspace** en fonction de vos besoins.
    - **Désactivé** : indique que le protocole TCP est utilisé pour le transfert de données.
    - **Préféré** : indique que l'application Citrix Workspace pour Windows tente d'abord de se connecter au serveur via UDP et bascule sur TCP si la connexion via UDP échoue.
    - **Activé** : indique que l'application Citrix Workspace pour Windows se connecte au serveur uniquement via le protocole UDP. Il n'existe pas de solution de secours vers TCP avec cette option.
5. Cliquez sur **Appliquer**, puis sur **OK**.
6. Exécutez la commande `gpupdate /force` à partir d'une ligne de commande.

Par ailleurs, pour que la configuration du transport adaptatif soit prise en compte, ajoutez les fichiers de modèle de l'application Citrix Workspace au dossier **Définitions de stratégie**. Pour plus d'informations sur l'ajout des fichiers de modèle à l'objet de stratégie de groupe local, consultez la section Modèle d'objet de stratégie de groupe.

Pour confirmer que le paramètre de stratégie est appliqué :

Accédez à `HKEY\\_LOCAL\\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT` et vérifiez que la clé **HDXOverUDP** est incluse.

Pour de plus amples informations, consultez Transport adaptatif dans la documentation de Citrix Virtual Apps and Desktops.

Page Préférences avancées

À partir de la version 4.10, vous pouvez personnaliser la disponibilité et le contenu de la page **Préférences avancées** présente dans le menu contextuel de l'icône de l'application Citrix Workspace dans la zone de notification. Cela garantit que les utilisateurs peuvent appliquer uniquement des paramètres spécifiés par l'administrateur sur leurs systèmes. Plus spécifiquement, ils peuvent :

- Masquer entièrement la page Préférences avancées
- Masquer les paramètres spécifiques suivants sur la page :
    - Collecte des données
    - Centre de connexion
    - Outil d'analyse de la configuration
    - Clavier et barre de langue

- DPI élevé
- Informations de support
- Raccourcis et reconnexion
- Citrix Files
- Citrix Casting

Masquer l'option Préférences avancées dans le menu contextuel

Vous pouvez masquer la page Préférences avancées à l'aide du modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace :

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Citrix Workspace** > **Libre-service** > **Options Préférences avancées**.
3. Sélectionnez la stratégie **Désactiver Préférences avancées**.
4. Sélectionnez **Activé** pour masquer l'option Préférences avancées dans le menu contextuel de l'icône de l'application Citrix Workspace dans la zone de notification.

> **Remarque :**
>
> L'option **Non configuré** est sélectionnée par défaut.

Masquer des paramètres spécifiques sur la page Paramètres avancés

Vous pouvez masquer des paramètres configurables par l'utilisateur spécifiques sur la page **Préférences avancées** à l'aide du modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace. Pour ce faire :

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Citrix Workspace** > **Libre-service** > **Options Préférences avancées**.
3. Sélectionnez la stratégie pour le paramètre que vous souhaitez masquer.

Le tableau ci-dessous répertorie les options que vous pouvez sélectionner et l'effet de chacune :

Options	Action
Non configuré	Affiche le paramètre
Activée	Masque le paramètre
Désactivée	Affiche le paramètre

Masquer les paramètres spécifiques suivants sur la page :

- Outil d'analyse de la configuration
- Centre de connexion
- DPI élevé
- Collecte des données
- Supprimer les mots de passe enregistrés
- Clavier et barre de langue
- Raccourcis et reconnexion
- Informations de support
- Citrix Files
- Citrix Casting

Masquer l'option Réinitialiser Workspace sur la page Préférences avancées à l'aide de l'Éditeur du Registre

Vous pouvez masquer l'option **Réinitialiser Workspace** sur la page Préférences avancées uniquement à l'aide de l'Éditeur du Registre.

1. Lancer l'Éditeur du registre
2. Accédez à **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle**.
3. Créez une clé avec la valeur de chaîne **EnableFactoryReset** et définissez-la sur une des options suivantes :
    a) True : affiche l'option Réinitialiser Workspace sur la page Préférences avancées.
    b) False : masque l'option Réinitialiser Workspace sur la page Préférences avancées.

Masquer de l'option Mises à jour de Citrix Workspace sur la page Préférences avancées

> **Remarque :**
>
> Le chemin de la stratégie pour l'option Mises à jour de Citrix Workspace diffère de celui des autres options de la page Préférences avancées.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Mises à jour de Workspace**.
3. Sélectionnez la stratégie **Mises à jour de Workspace**.
4. Sélectionnez **Désactivé** pour masquer les paramètres Mises à jour de Workspace sur la page **Préférences avancées**.

Mise à disposition d'applications

Lors de la mise à disposition d'applications avec Citrix Virtual Apps and Desktops, envisagez les options suivantes pour améliorer l'expérience utilisateur :

- Mode d'accès au Web : sans aucune configuration, l'application Citrix Workspace permet d'accéder aux applications et bureaux par le biais d'un navigateur. Vous pouvez ouvrir un site Workspace pour Web ou un site Interface Web dans un navigateur pour sélectionner les applications que vous souhaitez utiliser. Dans ce mode, aucun raccourci n'est placé sur le bureau de l'utilisateur.
- Mode libre-service : il vous suffit d'ajouter un compte StoreFront à l'application Citrix Workspace ou de configurer l'application Citrix Workspace pour qu'elle pointe vers un site Web StoreFront pour pouvoir configurer le *mode libre-service*, qui vous permet de vous abonner à des applications à partir de l'interface utilisateur de l'application Citrix Workspace. 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.

> **Remarque :**
>
> Par défaut, l'application Citrix Workspace vous permet de sélectionner les applications à afficher dans le menu Démarrer.

- Mode raccourci d'application uniquement : en tant qu'administrateur de l'application Citrix Workspace pour Windows, vous pouvez configurer l'application Citrix Workspace pour qu'elle place automatiquement des raccourcis d'applications et de bureaux directement dans le menu Démarrer ou sur le bureau, de la même manière que l'application Citrix Workspace Enterprise. Le nouveau mode *raccourci uniquement* vous permet de localiser toutes les applications publiées là où vous vous attendez à les trouver à l'aide du schéma de navigation Windows habituel.

Pour plus d'informations sur la mise à disposition d'applications à l'aide de Citrix Virtual Apps and Desktops 7, consultez la section Créer un groupe de mise à disposition d'application.

Configurer le mode libre-service

Il vous suffit d'ajouter un compte StoreFront à l'application Citrix Workspace ou de configurer l'application Citrix Workspace pour qu'elle pointe vers un site StoreFront pour pouvoir configurer le mode libre-service, qui permet à vos utilisateurs de s'abonner à des applications à partir de l'interface utilisateur de Citrix Workspace. Cette expérience enrichie est similaire à celle que propose un magasin d'applications mobiles.

> **Remarque :**
>
> Par défaut, l'application Citrix Workspace autorise les utilisateurs à sélectionner les applications qu'ils souhaitent afficher dans leur menu Démarrer.

En mode libre-service, vous pouvez configurer des paramètres de mots-clés pour les applications sélectionnées, auto-provisionnées et obligatoires selon vos besoins.

Ajoutez des mots-clés aux descriptions que vous fournissez pour les applications de groupe de mise à disposition :

- Pour définir une application individuelle comme obligatoire afin d'empêcher l'application Citrix Workspace de la supprimer, ajoutez la chaîne KEYWORDS: Mandatory à la description de l'application. Il n'existe aucune option Supprimer pour les utilisateurs pour annuler l'inscription aux applications obligatoires.
- Pour abonner automatiquement tous les utilisateurs d'un magasin à une application, ajoutez la chaîne KEYWORDS: Auto à la description. Lorsque les utilisateurs ouvrent une session dans le magasin, l'application est automatiquement provisionnée sans qu'ils aient à y souscrire manuellement.
- Pour publier des applications auprès des utilisateurs ou pour faciliter la recherche des applications fréquemment utilisées en les répertoriant dans la liste Sélection de Citrix Workspace, ajoutez la chaîne KEYWORDS: Featured à la description de l'application.

Personnaliser l'emplacement des raccourcis d'applications à l'aide du modèle d'objet de stratégie de groupe

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Libre-service**.
3. Sélectionnez la stratégie **Gérer SelfServiceMode**.
    a) Sélectionnez **Activé** pour afficher l'interface utilisateur en libre-service.
    b) Sélectionnez **Désactivé** pour vous abonner manuellement aux applications. Cette option masque l'interface utilisateur en libre-service.
4. Sélectionnez la stratégie **Gérer les raccourcis d'applications**.
5. Sélectionnez les options si nécessaire.
6. Cliquez sur **Appliquer, puis sur OK**.
7. Redémarrez l'application Citrix Workspace pour que les modifications prennent effet.

Utilisation des paramètres de compte StoreFront pour personnaliser l'emplacement des raccourcis d'applications

Vous pouvez configurer des raccourcis dans le menu Démarrer et sur le bureau à partir du site StoreFront. Les paramètres suivants peuvent être ajoutés dans le fichier web.config dans **C:\inetpub\wwwroot\Citrix\Roaming** dans la section **<annotatedServices>** :

- Pour placer des raccourcis sur le bureau, utilisez PutShortcutsOnDesktop. Paramètres : « true » ou « false » (false est le paramètre par défaut).
- Pour placer des raccourcis dans le menu Démarrer, utilisez PutShortcutsInStartMenu. Paramètres : « true » ou « false » (true est le paramètre par défaut).
- Pour utiliser le chemin d'accès de catégorie dans le menu Démarrer, utilisez UseCategoryAsStartMenuPath. Paramètres : « true » ou « false » (true est le paramètre par défaut).

> **Remarque :**
>
> Windows 8, 8.1 et Windows 10 n'autorisent pas la création de dossiers imbriqués dans le menu Démarrer. Les applications sont affichées séparément ou sous le dossier racine mais pas dans les sous-dossiers de catégorie définis avec Citrix Virtual Apps.

- Pour définir un répertoire unique pour tous les raccourcis dans le menu Démarrer, utilisez StartMenuDir. Paramètre : valeur de chaîne, correspondant au nom du dossier dans lequel les raccourcis sont créés.
- Pour réinstaller des applications modifiées, utilisez AutoReinstallModifiedApps. Paramètres : « true » ou « false » (true est le paramètre par défaut).
- Pour afficher un répertoire unique pour tous les raccourcis sur le bureau, utilisez DesktopDir. Paramètre : valeur de chaîne, correspondant au nom du dossier dans lequel les raccourcis sont créés.
- Pour ne pas créer d'entrée sur la liste « Ajout/Suppression de programmes » des clients, utilisez DontCreateAddRemoveEntry. Paramètres : « true » ou « false » (false est le paramètre par défaut).
- Pour supprimer des raccourcis et l'icône de Citrix Workspace d'une application préalablement disponible dans le magasin mais qui n'est plus disponible, utilisez SilentlyUninstallRemovedResources. Paramètres : « true » ou « false » (false est le paramètre par défaut).

Dans le fichier web.config, ajoutez les modifications dans la section **XML** pour le compte. Recherchez cette section en recherchant l'onglet d'ouverture :

```
<account id=... name="Store"
```

La section se termine par la balise </account>.

Avant la fin de la section account, dans la première section properties :

```
<properties> <clear> <properties>
```


Les propriétés peuvent être ajoutées dans cette section après la balise <clear />, un par ligne, attribuant le nom et la valeur. Par exemple :

```
<property name=”PutShortcutsOnDesktop”value=”True”/>
```

> **Remarque :**
>
> les éléments de propriété ajoutés avant la balise <clear /> peuvent les invalider. La suppression de la balise <clear /> lors de l’ajout d’un nom de propriété et d’une valeur est facultative.

Voici un exemple étendu de cette section :

```
<properties <property name=”PutShortcutsOnDesktop”value=”True”<property
name=”DesktopDir”value=”Citrix Applications”>
```

> **Important**
>
> Dans les déploiements faisant appel à de multiples serveurs, n’utilisez qu’un serveur à la fois pour apporter des modifications à la configuration du groupe de serveurs. Assurez-vous que la console de gestion Citrix StoreFront n’est exécutée sur aucun des serveurs dans le déploiement. Une fois les modifications terminées, propagez les modifications que vous avez apportées à la configuration du groupe de serveurs de façon à mettre à jour les autres serveurs dans le déploiement. Pour de plus amples informations, consultez la documentation de StoreFront.

Utilisation des paramètres par application dans Citrix Virtual Apps and Desktops 7.x pour personnaliser l’emplacement des raccourcis d’applications

L’application Citrix Workspace peut être configurée pour placer automatiquement des raccourcis d’applications et de bureaux directement dans le menu Démarrer ou sur le bureau. Cette fonctionnalité est similaire à celle des versions précédentes de Workspace pour Windows, mais la version 4.2.100 permet désormais de choisir où placer les raccourcis d’applications à l’aide des paramètres par application de Citrix Virtual Apps. Cette fonctionnalité est utile dans les environnements comportant quelques applications qui doivent être affichées dans les mêmes emplacements.

Si vous souhaitez définir l’emplacement des raccourcis de manière à ce que chaque utilisateur puisse les trouver dans le même emplacement, utilisez les paramètres par application de Citrix Virtual Apps :

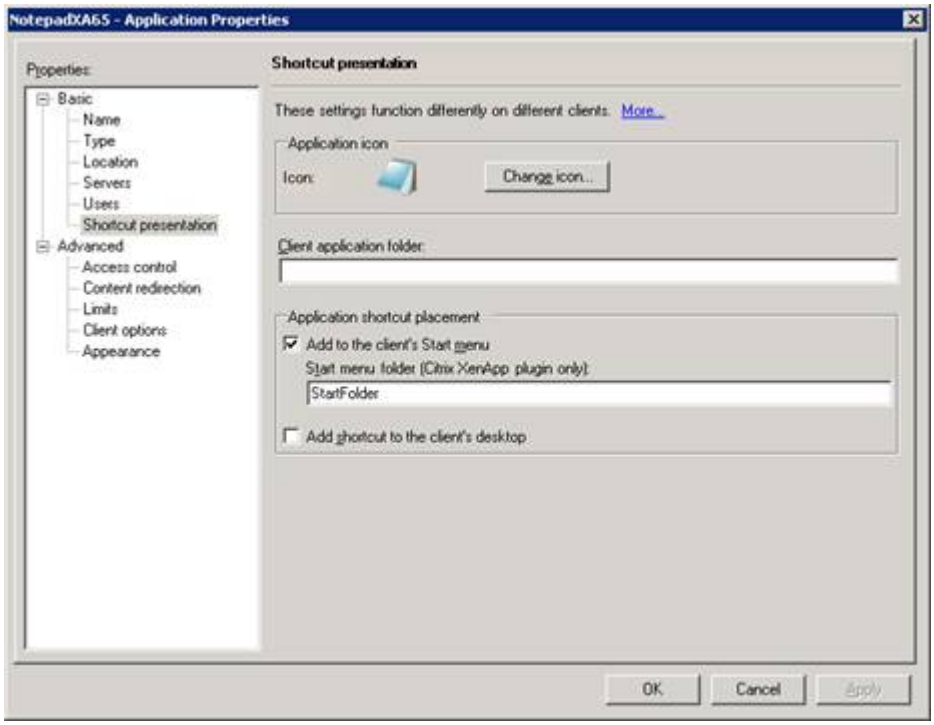
Si vous souhaitez que les paramètres par application déterminent où les applications sont placées indépendamment du mode utilisé (libre-service ou mode du menu Démarrer).	Configurez l'application Workspace pour Windows avec **PutShortcutsInStartMenu**=**false** et activez les paramètres par application. Remarque : ce paramètre s'applique aux sites Interface Web uniquement.

> **Remarque :**
>
> Le paramètre **PutShortcutsInStartMenu=false** s'applique à XenApp 6.5 et XenDesktop 7.x.

Configurer les paramètres par application dans XenApp 6.5

Pour configurer un raccourci par application publiée dans XenApp 6.5 :

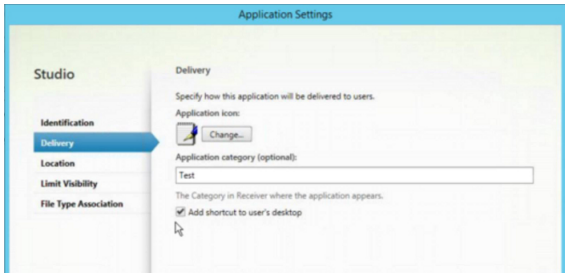
1. Dans l'écran des **propriétés d'application XenApp**, développez les propriétés **de base**.
2. Sélectionnez l'option Présentation du raccourci.
3. Dans la section Emplacement(s) du ou des raccourci(s) de l'écran **Présentation du raccourci**, sélectionnez la case **Ajouter** un raccourci dans le menu Démarrer du client. Après avoir sélectionné la case à cocher, entrez le nom du dossier dans lequel vous souhaitez placer le raccourci. Si vous ne spécifiez pas de nom de dossier, XenApp place le raccourci dans le menu Démarrer sans le placer dans un dossier.
4. Sélectionnez Ajouter un raccourci sur le bureau du client pour inclure le raccourci sur le bureau d'une machine cliente.
5. Cliquez sur **Appliquer**.
6. Cliquez sur **OK**.



Utilisation des paramètres par application dans XenApp 7.6 pour personnaliser l'emplacement des raccourcis d'applications

Pour configurer un raccourci par application publiée dans XenApp 7.6 :

1. Dans Citrix Studio, accédez à l'écran **Paramètres de l'application**.
2. Dans l'écran **Paramètres de l'application**, sélectionnez **Mise à disposition**. À l'aide de cet écran, vous pouvez spécifier la méthode à utiliser pour mettre les applications à la disposition des utilisateurs.
3. Sélectionnez l'icône appropriée pour l'application. Cliquez sur **Modifier** pour accéder à l'icône souhaitée.
4. Dans le champ **Catégorie d'application**, vous pouvez indiquer la catégorie de l'application Citrix Workspace dans laquelle l'application apparaît. Par exemple, si vous ajoutez des raccourcis vers des applications Microsoft Office, entrez Microsoft Office.
5. Cochez la case Ajouter un raccourci sur le bureau de l'utilisateur.
6. Cliquez sur OK.



Réduction des délais d'énumération ou signature numérique des stubs applicatifs

Si les utilisateurs rencontrent des délais dans l'énumération des applications à chaque ouverture de session, ou s'il est nécessaire de signer numériquement les stubs applicatifs, l'application Citrix Workspace dispose d'une fonctionnalité qui permet de copier les stubs .EXE à partir d'un partage réseau.

Cette fonctionnalité implique un certain nombre d'étapes :

1. Créez les stubs applicatifs sur la machine cliente.
2. Copiez les stubs applicatifs sur un emplacement accessible à partir d'un partage réseau.
3. Si nécessaire, préparez une liste blanche (ou signez les stubs avec un certificat d'entreprise).
4. Ajoutez une clé de registre pour permettre à Workspace pour Windows de créer les stubs en les copiant à partir du partage réseau.

Si **RemoveappsOnLogoff** et **RemoveAppsonExit** sont activés, et que les utilisateurs rencontrent des délais dans l'énumération des applications à chaque ouverture de session, utilisez les informations suivantes pour réduire les délais :

1. Utilisez regedit pour ajouter HKEY_CURRENT_USER\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true".
2. Utilisez regedit pour ajouter HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true". HKEY_CURRENT_USER est prioritaire sur HKEY_LOCAL_MACHINE.

> **Attention**
>
> La modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter de réinstaller votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Autorisez une machine à utiliser les exécutables stub précréés qui sont stockés sur un partage réseau :

1. Sur une machine cliente, créez des exécutables stub pour toutes les applications. Pour ce faire, ajoutez toutes les applications à la machine à l'aide de l'application Citrix Workspace. Cette

dernière génère les fichiers exécutables.

2. Récoltez les exécutables stub depuis %APPDATA%\Citrix\SelfService. Vous n'avez besoin que des fichiers .exe.
3. Copiez les fichiers exécutables sur un partage réseau.
4. Pour chaque machine cliente qui est verrouillée, définissez les clés de registre suivantes :
   a) Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\WorkspaceStubs"
   b) Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v
   c) CopyStubsFromCommonStubDirectory /t REG_SZ /d "true". Si vous le souhaitez, vous pouvez également configurer ces paramètres sur HKEY_CURRENT_USER. HKEY_CURRENT_USER est prioritaire sur HKEY_LOCAL_MACHINE.
   d) Quittez et redémarrez l'application Citrix Workspace pour tester les paramètres.

Exemples de cas d'utilisation :

Vous trouverez dans cette rubrique des cas d'utilisation de raccourcis d'applications.

Autoriser les utilisateurs à choisir les applications à afficher dans le menu Démarrer (libre-service)

Si vos applications se comptent par dizaines (ou même par centaines), il est conseillé d'autoriser les utilisateurs à choisir les applications qu'ils préfèrent et souhaitent ajouter au menu Démarrer :

Si vous souhaitez autoriser les utilisateurs à choisir les applications à afficher dans leur menu Démarrer…	Configurez l'application Citrix Workspace en mode libre-service. Dans ce mode, vous configurez également les paramètres de mots-clés applicatifs *auto-provisionnées* et *obligatoires*.
Si vous souhaitez que les utilisateurs puissent choisir les applications à afficher dans leur menu Démarrer, mais que vous souhaitez également placer des raccourcis d'applications spécifiques sur le bureau…	Configurez l'application Citrix Workspace sans aucune option et paramétrez individuellement chaque application que vous voulez placer sur le bureau. Utilisez des applications *auto-provisionnées* et *obligatoires* en fonction de vos besoins.

Aucun raccourci d'application dans le menu Démarrer

Si l'ordinateur d'un utilisateur est utilisé par toute la famille, vous n'aurez peut-être besoin d'aucun raccourci d'application. Dans de tels scénarios, l'approche la plus simple est l'accès par navigateur : installez l'application Citrix Workspace sans configuration et utilisez Workspace pour Web et l'Interface Web. Vous pouvez également configurer l'application Citrix Workspace pour un accès en libre-service sans placer de raccourcis.

Si vous souhaitez empêcher l'application Citrix Workspace de placer automatiquement des raccourcis d'applications dans le menu Démarrer…	Définissez la clé PutShortcutsInStartMenu=False pour l'application Citrix Workspace. L'application Citrix Workspace ne placera aucune application dans le menu Démarrer, même en mode libre-service, à moins que vous ne le fassiez individuellement pour chaque application.

Tous les raccourcis d'applications dans le menu Démarrer ou sur le bureau

Si l'utilisateur ne dispose que de quelques applications, vous pouvez toutes les placer dans le menu Démarrer ou sur le bureau, ou dans un dossier sur le bureau.

Si vous souhaitez que l'application Citrix Workspace place automatiquement tous les raccourcis d'applications dans le menu Démarrer…	Définissez la clé SelfServiceMode=False pour l'application Citrix Workspace. Toutes les applications disponibles s'affichent dans le menu Démarrer.
Si vous voulez placer tous les raccourcis d'applications sur le bureau…	Définissez la clé PutShortcutsOnDesktop=True pour l'application Citrix Workspace. Toutes les applications disponibles s'affichent sur le bureau.
Si vous voulez placer tous les raccourcis dans un dossier sur le bureau…	Configurez l'application Citrix Workspace en définissant DesktopDir sur le nom du dossier de bureau dans lequel vous souhaitez placer les applications.

Paramètres par application dans XenApp 6.5 ou 7.x

Si vous souhaitez définir l'emplacement des raccourcis de manière à ce que chaque utilisateur puisse les trouver dans le même emplacement, utilisez les paramètres par application de XenApp :

Si vous souhaitez que les paramètres par application déterminent où les applications sont placées indépendamment du mode utilisé (libre-service ou mode du menu Démarrer)…	Définissez la clé PutShortcutsInStartMenu=false pour l'application Citrix Workspace et activez les paramètres par application.

Applications dans des dossiers de catégorie ou dans des dossiers spécifiques

Si vous souhaitez que les applications s'affichent dans des dossiers spécifiques, utilisez les options suivantes :

Si vous souhaitez que les raccourcis d'applications placés par l'application Citrix Workspace dans le menu Démarrer s'affichent dans leur catégorie associée (dossier)…	Définissez la clé UseCategoryAsStartMenuPath=True pour l'application Citrix Workspace.
Si vous souhaitez que les applications placées par l'application Citrix Workspace dans le menu Démarrer s'affichent dans un dossier spécifique…	Configurez l'application Citrix Workspace en définissant StartMenuDir sur le nom de dossier du menu Démarrer.

Supprimer les applications à la fermeture de session ou en quittant

Si vous ne souhaitez pas que les utilisateurs puissent accéder aux applications d'autres utilisateurs sur un poste de travail partagé, vous pouvez vous assurer que les applications sont supprimées lorsque l'utilisateur ferme sa session ou quitte Receiver.

Si vous souhaitez que l'application Citrix Workspace supprime toutes les applications à la fermeture de session…	Définissez la clé RemoveAppsOnLogoff=True pour l'application Citrix Workspace.

Si vous souhaitez que l'application Citrix Workspace supprime toutes les applications en quittant…	Définissez la clé RemoveAppsOnExit=True pour l'application Citrix Workspace.

Configuration des applications Local App Access

Lors de la configuration des applications Local App Access :

- Pour spécifier l'utilisation d'une application installée localement plutôt qu'une application disponible dans l'application Citrix Workspace, ajoutez la chaîne de texte KEYWORDS:prefer="pattern". Cette fonctionnalité est appelée Local App Access.

  Avant d'installer une application sur l'ordinateur d'un utilisateur, l'application Citrix Workspace recherche les modèles spécifiés pour déterminer si l'application est installée localement. Si c'est le cas, l'application Citrix Workspace s'abonne à l'application et ne crée pas de raccourci. Lorsque l'utilisateur démarre l'application à partir de la fenêtre de l'application Citrix Workspace, l'application Citrix Workspace démarre l'application installée localement (préférée).

  Si un utilisateur désinstalle une application préférée en dehors de l'application Citrix Workspace, l'abonnement à l'application est annulé lors de la prochaine actualisation de l'application Citrix Workspace. Si un utilisateur désinstalle une application préférée à partir de la boîte de dialogue de l'application Citrix Workspace, l'application Citrix Workspace annule l'abonnement à l'application mais ne la désinstalle pas.

> **Remarque :**
>
> Le mot-clé prefer est appliqué lorsque l'application Citrix Workspace s'abonne à une application. L'ajout du mot-clé après souscription à l'application n'a aucun effet.

Vous pouvez spécifier le mot-clé prefer plusieurs fois pour une application. Il suffit d'une correspondance pour appliquer le mot-clé à une application. Les modèles suivants peuvent être utilisés dans n'importe quelle combinaison :

- Pour spécifier qu'une application installée localement doit être utilisée à la place d'une application disponible dans l'application Citrix Workspace, ajoutez la chaîne de texte KEYWORDS:prefer="pattern". Cette fonctionnalité est appelée Local App Access.

  Avant d'installer une application sur l'ordinateur d'un utilisateur, l'application Citrix Workspace recherche les modèles spécifiés pour déterminer si l'application est installée localement. Si c'est le cas, l'application Citrix Workspace s'abonne à l'application et ne crée pas de raccourci. Lorsque l'utilisateur démarre l'application à partir de la boîte de dialogue de l'application

Citrix Workspace, l'application Citrix Workspace démarre l'application installée localement (préférée).

Si un utilisateur désinstalle une application préférée en dehors de l'application Citrix Workspace, l'abonnement à l'application est annulé lors de la prochaine actualisation de l'application Citrix Workspace. Si un utilisateur désinstalle une application préférée à partir de l'application Citrix Workspace, l'application Citrix Workspace annule l'abonnement à l'application mais ne la désinstalle pas.

> **Remarque :**
>
> Le mot-clé prefer est appliqué lorsque l'application Citrix Workspace s'abonne à une application. L'ajout du mot-clé après souscription à l'application n'a aucun effet.

Vous pouvez spécifier le mot-clé prefer plusieurs fois pour une application. Il suffit d'une correspondance pour appliquer le mot-clé à une application. Les modèles suivants peuvent être utilisés dans n'importe quelle combinaison :

- prefer="Nomapplication"

  Le modèle de nom d'application correspond à toute application dont le nom du fichier de raccourci contient le nom d'application spécifié. Le nom de l'application peut être un mot ou une phrase. Les phrases doivent être entourées de guillemets. Aucune correspondance n'est établie avec les mots partiels ou les chemins d'accès à des fichiers ; en outre, la correspondance n'est pas sensible à la casse. La possibilité de faire correspondre un nom d'application à un modèle est utile pour les substitutions réalisées manuellement par un administrateur.

KEYWORDS:prefer=	Raccourci sous Programmes	Correspondances ?
Word	\Microsoft Office\Microsoft Word 2010	Oui
Microsoft Word	\Microsoft Office\Microsoft Word 2010	Oui
Console	McAfee\VirusScan Console	Oui
Virus	McAfee\VirusScan Console	Non
Console	McAfee\VirusScan Console	Oui

- prefer="\\Dossier1\Dossier2\…\NomApplication"

  Le modèle de chemin d'accès absolu correspond au chemin d'accès du fichier de raccourci plus le nom d'application entier sous le menu Démarrer. Le dossier Programmes est un sous-dossier du répertoire du menu Démarrer, vous devez donc l'inclure au chemin d'accès absolu pour cibler une application dans ce dossier. Des guillemets sont requis si le chemin d'accès contient

des espaces. La correspondance est sensible à la casse. Le modèle de correspondance à un chemin d'accès absolu est utile pour les substitutions implémentées via un programme dans Citrix Virtual Apps and Desktops.

KEYWORDS:prefer=	Raccourci sous Programmes	Correspondances ?
\Programs\Microsoft Office\Microsoft Word 2010	\Programs\Microsoft Office\Microsoft Word 2010	Oui
\Microsoft Office	\Programs\Microsoft Office\Microsoft Word 2010	Non
\Microsoft Word 2010	\Programs\Microsoft Office\Microsoft Word 2010	Non
\Programs\Microsoft Word 2010	\Programs\Microsoft Word 2010	Oui

- prefer="\\Dossier1\Dossier2\…\NomApplication"

  Le modèle de chemin d'accès relatif correspond au chemin d'accès du fichier de raccourci relatif sous le menu Démarrer. Le chemin d'accès relatif doit contenir le nom de l'application et peut éventuellement inclure les dossiers dans lesquels le raccourci réside. Une correspondance est établie sur le chemin d'accès au fichier de raccourci se termine pas le chemin d'accès relatif fourni. Des guillemets sont requis si le chemin d'accès contient des espaces. La correspondance est sensible à la casse. Le modèle de correspondance à un chemin d'accès relatif est utile pour les substitutions implémentées via un programme.

KEYWORDS:prefer=	Raccourci sous Programmes	Correspondances ?
\Microsoft Office\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Oui
\Microsoft Office	\Microsoft Office\Microsoft Word 2010	Non
\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Oui
\Microsoft Word	\Microsoft Word 2010	Non

Pour de plus amples informations sur les autres mots-clés, reportez-vous à « Recommandations supplémentaires » dans la section Optimiser l'expérience utilisateur de la documentation de StoreFront.

Temps de lancement des applications

Utilisez la fonctionnalité de pré-lancement de session pour réduire la durée de lancement des applications en période d'activité normale ou maximale, et ainsi offrir une meilleure expérience aux utilisateurs. La fonctionnalité de pré-lancement permet la création d'une session de pré-lancement lorsqu'un utilisateur ouvre une session sur l'application Citrix Workspace, ou à un horaire programmé si l'utilisateur a déjà ouvert une session.

Cette session de pré-lancement réduit la durée de démarrage de la première application. Lorsqu'un utilisateur ajoute une nouvelle connexion de compte à l'application Citrix Workspace pour Windows, le pré-lancement de session prend effet lors de la session suivante. L'application par défaut ctxprelaunch.exe s'exécute dans la session, mais l'utilisateur ne la voit pas.

Le pré-lancement de session est pris en charge sur les déploiements de StoreFront. Pour les déploiements Interface Web, vous devez utiliser l'option d'**enregistrement du mot de passe** de l'Interface Web pour éviter les invites d'ouverture de session. Le pré-lancement de session n'est pas pris en charge avec les déploiements Citrix Virtual Apps and Desktops.

Le pré-lancement de session est désactivé par défaut. Pour activer le pré-lancement de session, spécifiez le paramètre `ENABLEPRELAUNCH=true` sur la ligne de commande Workspace ou définissez la clé de registre `EnablePreLaunch` sur true. Le paramètre par défaut, null, signifie que le pré-lancement est désactivé.

> **Remarque :**
>
> Si la machine cliente a été configurée pour prendre en charge l'authentification pass-through au domaine (SSON), le pré-lancement est automatiquement activé. Si vous souhaitez utiliser l'authentification pass-through au domaine (SSON) sans pré-lancement, définissez la valeur de la clé de registre**EnablePreLaunch** sur
> false.

Emplacements de registre :

- HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Dazzle

Il existe deux types de pré-lancement :

- **Pré-lancement zéro délai** - Le pré-lancement démarre immédiatement après l'authentification des informations d'identification de l'utilisateur, et ce même en période de trafic intense. Utilisé pour les périodes de trafic normal. Un utilisateur peut déclencher le pré-lancement zéro délai en redémarrant l'application Citrix Workspace.
- **Pré-lancement planifié** - Le pré-lancement démarre à l'heure planifiée. Le pré-lancement planifié ne démarre que lorsque la machine utilisateur est déjà exécutée et authentifiée. Si ces deux conditions ne sont pas remplies à l'heure planifiée, aucune session n'est lancée. Pour répartir

la charge réseau et serveur, la session se lance dans un intervalle de temps proche de l'heure planifiée. À titre d'exemple, si le pré-lancement planifié est programmé pour démarrer à 13:45, la session se lance en fait entre 13:15 et 13:45. Utilisé lors des périodes de trafic élevé.

La configuration du pré-lancement sur un serveur Citrix Virtual Apps consiste à créer, modifier ou supprimer des applications de pré-lancement, et à mettre à jour les paramètres de stratégie utilisateur qui contrôlent les applications de pré-lancement.

Vous ne pouvez pas personnaliser la fonctionnalité de pré-lancement à l'aide du fichier receiver.admx. Toutefois, vous pouvez modifier la configuration du pré-lancement en modifiant les valeurs de registre pendant ou après l'installation de l'application Citrix Workspace pour Windows.

- Les valeurs HKEY_LOCAL_MACHINE sont écrites durant l'installation du client.
- Les valeurs HKEY_CURRENT_USER vous permettent de fournir différents paramètres à différents utilisateurs sur la même machine. Les utilisateurs peuvent modifier les valeurs HKEY_CURRENT_USER sans autorisations administratives. Vous pouvez fournir à vos utilisateurs des scripts leur permettant de modifier la configuration.

Valeurs de registre HKEY_LOCAL_MACHINE :

Pour les systèmes d'exploitation Windows 64 bits : HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

Pour les systèmes d'exploitation Windows 32 bits : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch

Nom : **UserOverride**

Valeurs :

0 - Utilise les valeurs HKEY_LOCAL_MACHINE même si les valeurs de HKEY_CURRENT_USER sont également présentes.

1 - Utilise les valeurs de HKEY_CURRENT_USER si elles existent ; utilise autrement les valeurs de HKEY_LOCAL_MACHINE.

Nom : **State**

Valeurs :

0 - Désactive le pré-lancement.

1 - Active le pré-lancement zéro délai. (Le pré-lancement démarre après authentification des informations d'identification de l'utilisateur.)

2 - Active le pré-lancement planifié. (Le pré-lancement démarre à l'heure configurée pour Schedule.)

Nom : **Schedule**

Valeur :

L'heure (format 24 heures) et les jours de la semaine du pré-lancement planifié doivent être entrés au format suivant :

HH: MM	M:T:W:TH:F:S:SU où HH et MM correspondent aux heures et minutes. M:T:W:TH:F:S:SU correspondent aux jours de la semaine. Par exemple, pour activer le pré-lancement planifié le lundi, mercredi et vendredi à 13:45, définissez Schedule de la sorte : Schedule=13:45	1:0:1:0:1:0:0 . La session se lance entre 13:15 et 13:45.

Valeurs de registre HKEY_CURRENT_USER :

HKEY_CURRENT_USER\Software\Citrix\ICA Client\Prelaunch

Les clés State et Schedule ont les mêmes valeurs que pour HKEY_LOCAL_MACHINE.

Redirection bidirectionnelle du contenu

La stratégie Redirection bidirectionnelle du contenu vous permet d'activer ou de désactiver la redirection client vers hôte et hôte vers URL client. Les stratégies de serveur sont définies dans Studio et les stratégies clients sont définies depuis le modèle d'administration de l'objet de stratégie de groupe de l'application Citrix Workspace.

Bien que Citrix offre également une redirection hôte vers client et Local App Access pour la redirection client vers URL, nous vous recommandons d'utiliser la redirection bidirectionnelle du contenu pour les clients Windows joints à un domaine.

Vous pouvez activer la redirection bidirectionnelle du contenu à l'aide de l'une des méthodes suivantes :

1. Modèle d'administration d'objet de stratégie de groupe
2. Éditeur du Registre

> **Remarque :**
>
> - La redirection bidirectionnelle du contenu ne fonctionne pas sur les sessions sur lesquelles **Local App Access** est activé.

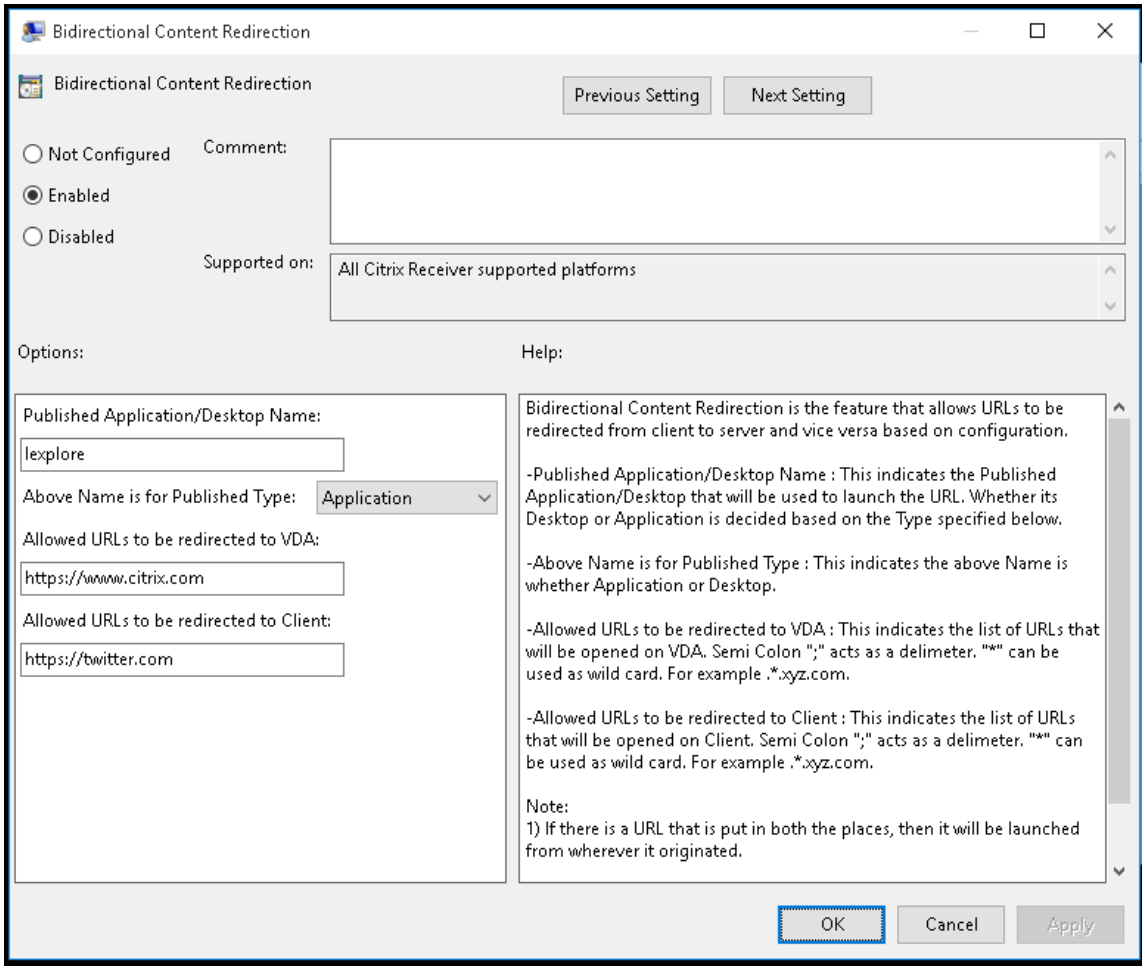
> • La redirection bidirectionnelle du contenu doit être activée sur le serveur et le client. Lorsqu'elle est désactivée sur le serveur ou le client, la fonctionnalité est désactivée.

Pour activer la redirection bidirectionnelle du contenu grâce au modèle d'administration d'objet de stratégie de groupe :

Utilisez la configuration du modèle d'administration d'objet de stratégie de groupe uniquement pour une première installation de l'application Citrix Workspace pour Windows.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration utilisateur**, accédez à **Modèles d'administration** > **Modèles d'administration classiques (ADM)** > **Composants Citrix** > **Citrix Workspace** > **Expérience utilisateur**.
3. Sélectionnez la stratégie **Redirection bidirectionnelle du contenu**.
4. Modifiez les paramètres.

> **Remarque :**
>
> Lorsque vous incluez des adresses URL, vous pouvez spécifier une seule adresse URL ou une liste d'adresses URL séparées par des points-virgules. Vous pouvez utiliser un astérisque (*) comme caractère générique.



5. Cliquez sur **Appliquer**, puis sur **OK**.
6. Exécutez la commande `gpupdate /force` à partir d'une ligne de commande.

Pour activer la redirection bidirectionnelle du contenu à l'aide du Registre :

Pour activer la redirection bidirectionnelle du contenu, exécutez la commande `redirector.exe /RegIE` à partir du dossier d'installation de l'application Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`).

> **Important :**
>
> - Assurez-vous que la règle de redirection n'entraîne pas une configuration en boucle. Une configuration en boucle se produit si des règles de VDA sont définies de manière à ce qu'une URL, par exemple `https://www.my\\_company.com`, soit configurée pour être redirigée vers le client et le VDA.
> - La redirection d'URL prend uniquement en charge les adresses URL explicites (c'est-à-dire, celles qui apparaissent dans la barre d'adresse du navigateur ou celles trouvées à l'aide de la navigation du navigateur, en fonction du navigateur).

- Si deux applications avec le même nom d'affichage sont configurées pour utiliser des comptes StoreFront multiples, le nom d'affichage du compte StoreFront principal est utilisé pour lancer la session d'application ou de bureau.
- Une nouvelle fenêtre de navigateur s'affiche uniquement lorsque l'adresse URL est redirigée sur le client. Lorsque l'adresse URL est redirigée sur le VDA, et que le navigateur est déjà ouvert, l'adresse URL redirigée s'ouvre dans le nouvel onglet.
- Les liens intégrés aux fichiers tels que les documents, e-mails et fichiers PDF sont pris en charge.

Limitation :

Aucun mécanisme de secours n'est présent si la redirection échoue en raison de problèmes de démarrage de session.

Claviers Bloomberg

L'application Citrix Workspace permet d'utiliser un clavier Bloomberg dans une session Citrix Virtual Apps and Desktops. Les composants requis sont installés avec le plug-in. Vous pouvez activer la fonctionnalité de clavier Bloomberg lors de l'installation de l'application Citrix Workspace pour Windows ou à l'aide de l'Éditeur du Registre.

Il n'est pas conseillé d'héberger plusieurs sessions avec des claviers Bloomberg. Le clavier fonctionne uniquement dans un environnement n'hébergeant qu'une session.

Configurer le clavier Bloomberg :

> **Attention**
>
> Une modification incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

1. Recherchez la clé suivante dans le registre :

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

2. Procédez comme suit :

   - Pour activer cette fonctionnalité, pour l'entrée Type DWORD et Nom **EnableBloombergHID**, définissez la valeur sur 1.
   - Pour désactiver cette fonctionnalité, définissez la valeur sur 0.

Pour de plus amples informations sur la configuration du clavier Bloomberg, consultez l'article CTX122615 du centre de connaissances.

Pour empêcher l'assombrissement de la fenêtre Desktop Viewer :

Si vous utilisez plusieurs fenêtres Desktop Viewer, par défaut, les bureaux qui ne sont pas actifs sont assombris. Si vous souhaitez afficher plusieurs bureaux simultanément, les informations peuvent devenir illisibles. Vous pouvez désactiver le comportement par défaut et empêcher l'assombrissement de la fenêtre Desktop Viewer en modifiant l'Éditeur du Registre.

> **Attention**
>
> Une modification incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à sauvegarder le registre avant de le modifier.

- Sur la machine utilisateur, créez une entrée REG_DWORD nommée **DisableDimming** dans l'une des clés suivantes, selon que vous souhaitez empêcher l'assombrissement pour l'utilisateur actuel de la machine ou pour la machine. Une entrée existe si Desktop Viewer a été utilisé sur la machine :
  - `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`
  - `HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop\DesktopViewer`

Au lieu de contrôler l'assombrissement, vous pouvez également définir une stratégie locale en créant la même entrée REG_WORD dans l'une des clés suivantes :

- `HKEY_CURRENT_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer`
- `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer`

Avant d'utiliser ces clés, demandez à votre administrateur Citrix Virtual Apps and Desktops s'il a déjà créé une stratégie pour cette fonctionnalité.

Définissez une valeur non nulle telle que 1 ou true pour l'entrée.

Si aucune entrée n'est spécifiée ou que l'entrée est définie sur 0, la fenêtre Desktop Viewer est assombrie. Si plusieurs entrées sont spécifiées, l'ordre de priorité suivant est utilisé. La première valeur répertoriée dans cette liste, et sa valeur, déterminent si la fenêtre est assombrie :

1. HKEY_CURRENT_USER\Software\Policies\Citrix\…
2. HKEY_LOCAL_MACHINE\Software\Policies\Citrix\…
3. HKEY_CURRENT_USER\Software\Citrix\…
4. HKEY_LOCAL_MACHINE\Software\Citrix\…

Citrix Casting

Citrix Ready Workspace Hub combine des environnements numériques et physiques pour fournir des applications et des données dans un espace intelligent sécurisé. Le système complet connecte des

appareils (ou objets), comme des applications mobiles et des capteurs, pour créer un environnement intelligent et réactif.

Citrix Ready Workspace Hub est basé sur la plate-forme Raspberry Pi 3. L'appareil exécutant l'application Citrix Workspace se connecte au Citrix Ready Workspace Hub et diffuse les applications ou les bureaux sur un écran plus grand. Citrix Casting est pris en charge uniquement sur Microsoft Windows 10 version 1607 et versions ultérieures ou sur Windows Server 2016.

Citrix Casting est une fonctionnalité qui vous permet d'accéder instantanément et en toute sécurité à n'importe quelle application à partir d'un appareil mobile et l'afficher sur grand écran.

> **Remarque :**
>
> - Citrix Casting pour Windows prend en charge la version 2.40.3839 de Citrix Ready Workspace Hub et versions ultérieures. Les versions antérieures de Workspace Hub peuvent ne pas être détectées ou provoquer une erreur de diffusion.
> - La fonctionnalité Citrix Casting n'est pas prise en charge sur l'application Citrix Workspace pour Windows (Store).

Conditions préalables :

- 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.
- Le port 55555 ne doit pas être bloqué entre l'appareil exécutant l'application Citrix Workspace et Citrix Ready Workspace Hub.
- Pour Citrix Casting, le port 1494 ne doit pas être bloqué.
- 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.
- Citrix Casting est pris en charge uniquement sur Microsoft Windows 10 version 1607 et versions ultérieures ou sur Windows Server 2016.

Configurer le lancement de Citrix Casting

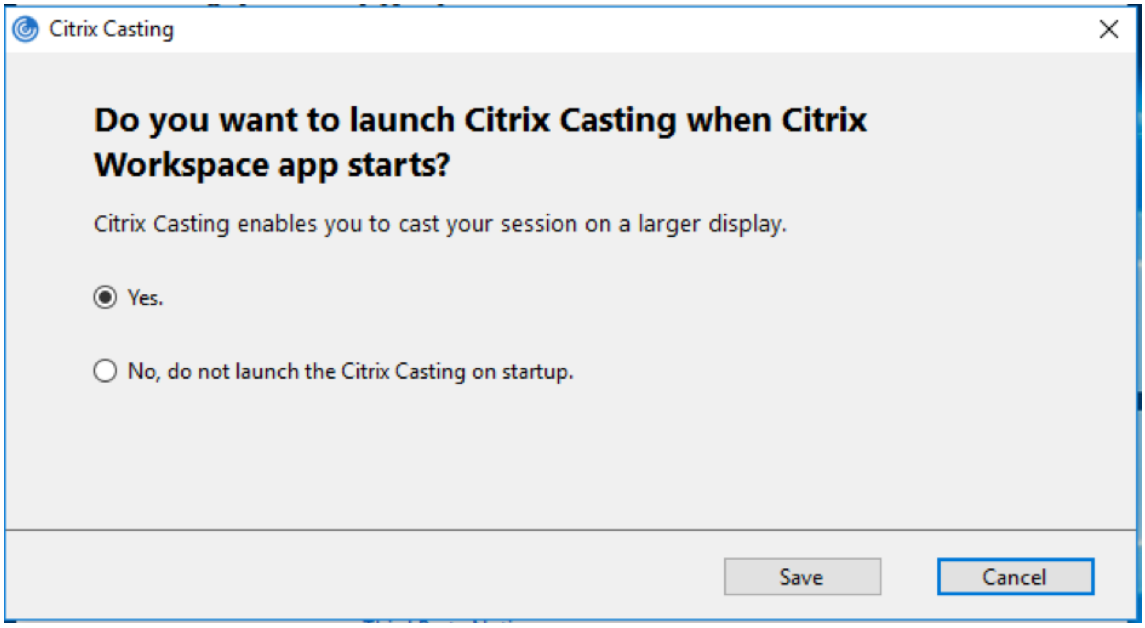
> **Remarque :**
>
> Vous pouvez masquer partiellement ou totalement la page Préférences avancées disponible à partir de l'icône de l'application Citrix Workspace dans la zone de notification. Pour plus d'informations, veuillez consulter l'article Page Préférences avancées.

1. Cliquez avec le bouton droit de la souris sur l'icône de l'application Citrix Workspace dans la zone de notification et sélectionnez **Préférences avancées**.

La boîte de dialogue **Préférences avancées** s'affiche.

2. Sélectionnez **Citrix Casting**.

   La boîte de dialogue **Citrix Casting** s'affiche.



3. Sélectionnez l'une des options suivantes :

   - Oui - Indique que Citrix Casting est lancé au démarrage de l'application Citrix Workspace.
   - Non, ne pas lancer Citrix Casting au démarrage - Indique que Citrix Casting n'est pas lancé au démarrage de l'application Citrix Workspace.

   > **Remarque :**
   >
   > La sélection de l'option **Non** ne met pas fin à la session de diffusion d'écran en cours. Le paramètre est appliqué uniquement au prochain lancement de l'application Citrix Workspace.

4. Cliquez sur **Enregistrer** pour appliquer les modifications.

Utiliser Citrix Casting avec l'application Citrix Workspace

1. Connectez-vous à l'application Citrix Workspace et activez Bluetooth sur votre appareil.

   La liste des Workspace Hub disponibles s'affiche. La liste est triée en fonction de la valeur RSSI du package de balises de Workspace Hub.

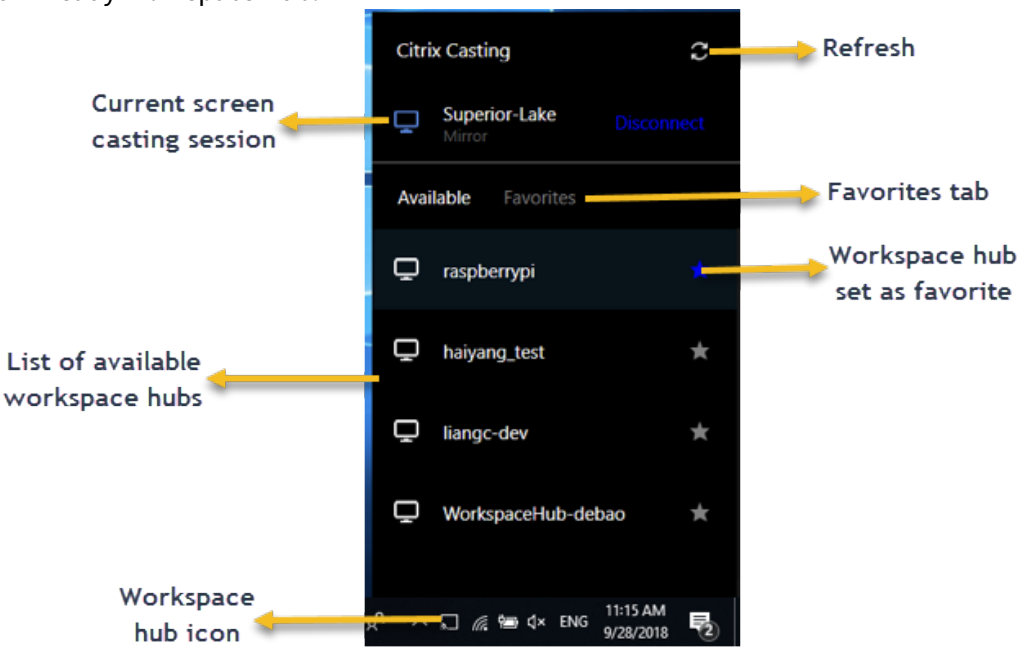
2. Sélectionnez le Workspace Hub pour la diffusion de votre écran et choisissez l'une des options suivantes :

- **Mettre en miroir** pour dupliquer l'écran principal et diffuser l'affichage sur l'appareil Workspace Hub connecté.
- **Étendre** pour utiliser l'écran de l'appareil Workspace Hub en tant qu'écran secondaire.

> **Remarque :**
>
> Lorsque vous quittez l'application Citrix Workspace, vous ne quittez pas Citrix Casting.

Dans la boîte de dialogue de **notification Citrix Casting**, les options suivantes sont disponibles :

1. La session de diffusion d'écran en cours est affichée en haut.
2. Icône **Actualiser**
3. L'option **Déconnecter** permet d'arrêter la session de diffusion d'écran en cours.
4. L'icône en forme d'étoile permet d'ajouter Workspace Hub aux **Favoris**.
5. Cliquez avec le bouton droit de la souris sur l'icône de Workspace Hub dans la zone de notification et sélectionnez **Quitter** pour déconnecter la session de diffusion d'écran et quitter Citrix Ready Workspace Hub.



Liste d'auto-vérification

Si l'application Citrix Workspace ne peut pas détecter et communiquer avec les Workspace Hubs disponibles dans la plage, veillez à effectuer les opérations suivantes dans le cadre de l'auto-vérification :

1. L'application Citrix Workspace et Citrix Ready Workspace Hub sont connectés au même réseau.
2. Bluetooth est activé et fonctionne correctement sur l'appareil sur lequel l'application Citrix Workspace est lancée.

3. L'appareil sur lequel l'application Citrix Workspace est lancée se trouve à portée (moins de 10 mètres et sans objets bloquants tels que des murs) de Citrix Ready Workspace Hub.
4. Lancez un navigateur dans l'application Citrix Workspace et tapez `http://<hub_ip>:55555/device-details.xml` pour vérifier si les détails de l'appareil du hub d'espace de travail sont affichés.
5. Cliquez sur **Actualiser** dans Citrix Ready Workspace Hub et essayez de vous reconnecter à Workspace Hub.

Problèmes connus et limitations

1. Citrix Casting ne fonctionne que si l'appareil est connecté au même réseau que Citrix Ready Workspace Hub.
2. En cas de problèmes de réseau, il peut y avoir un décalage d'affichage sur Workspace Hub Device.
3. Lorsque vous sélectionnez **Étendre**, l'écran principal sur lequel l'application Citrix Ready Workspace Hub est lancé clignote plusieurs fois.
4. Dans le mode **Étendre**, vous ne pouvez pas définir l'affichage secondaire comme affichage principal.
5. La session de diffusion d'écran se déconnecte automatiquement en cas de modification des paramètres d'affichage de l'appareil, comme par exemple, la modification de la résolution de l'écran ou la modification de l'orientation de l'écran.
6. Lors de la session de diffusion d'écran, si l'appareil exécutant l'application Citrix Workspace se verrouille, se met en veille ou en veille prolongée, une erreur apparaît lors de la connexion.
7. Plusieurs sessions de diffusion d'écran ne sont pas prises en charge.
8. La résolution d'écran maximale prise en charge par Citrix Casting est de 1920 x 1440.
9. Citrix Casting prend en charge la version 2.40.3839 de Citrix Ready Workspace Hub et versions ultérieures. Les versions antérieures de Workspace Hub peuvent ne pas être détectées ou provoquer une erreur de diffusion.
10. Cette fonctionnalité n'est pas prise en charge sur l'application Citrix Workspace pour Windows (Store).
11. Sous Windows 10, Build 1607, Citrix Casting en mode **Étendre** peut ne pas être correctement positionné.

Redirection de périphérique USB composite

Configurer la redirection de périphérique USB composite :

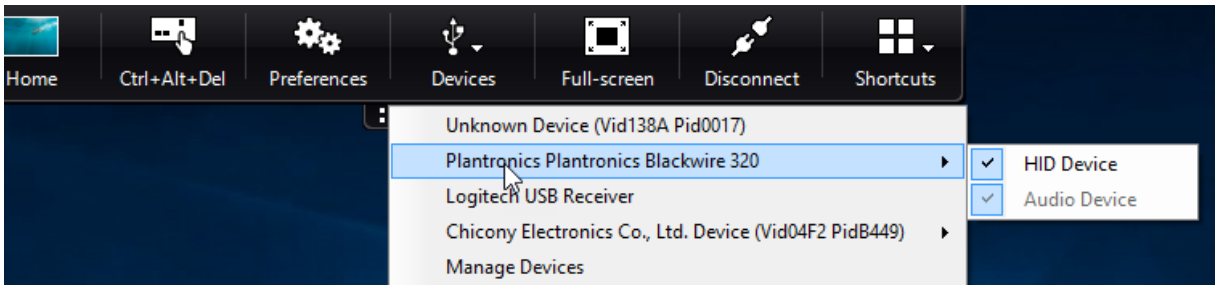
1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.

2. Sous le nœud **Configuration utilisateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Accès à distance des périphériques clients** > **Utilisation à distance de dispositifs USB génériques**.
3. Sélectionnez la stratégie **SplitDevices**.
4. Sélectionnez **Activé**.
5. Cliquez sur **Appliquer** et sur **OK** pour enregistrer la stratégie.

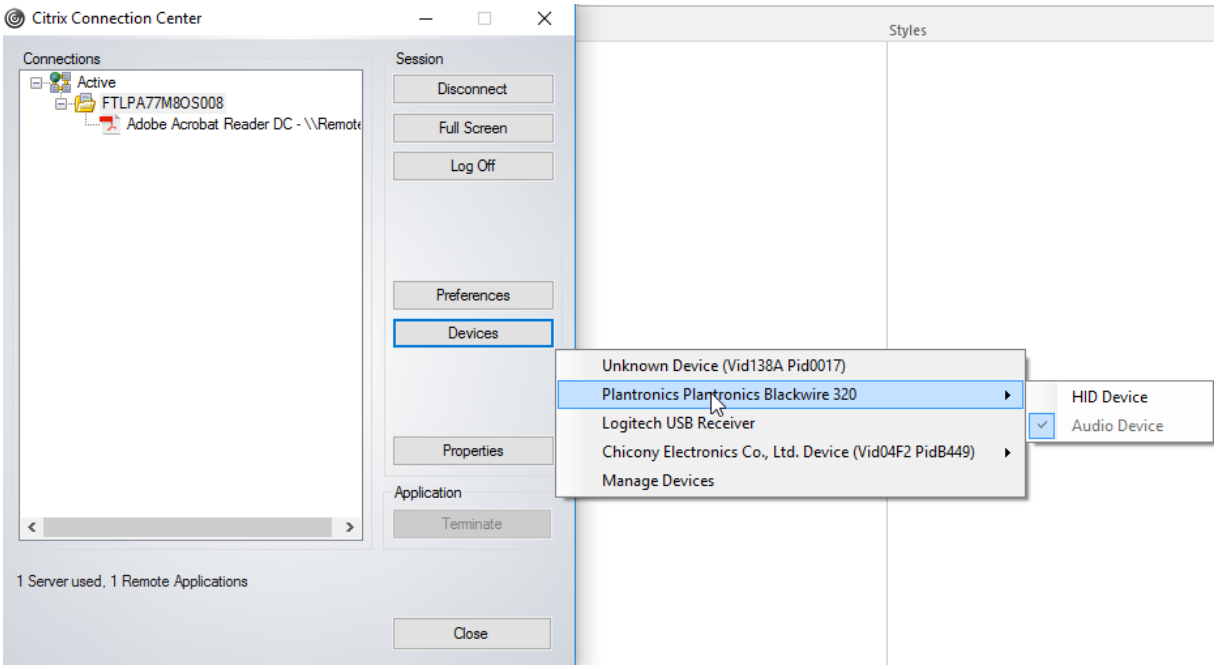
Pour autoriser ou interdire une interface :

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration utilisateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Accès à distance des périphériques clients** > **Utilisation à distance de dispositifs USB génériques**.
3. Sélectionnez la stratégie **Règles de périphériques USB**.
4. Sélectionnez **Activé**.
5. Dans la zone de texte **Règles de périphériques USB**, ajoutez le périphérique USB que vous souhaitez autoriser ou interdire.
   Par exemple, `ALLOW: vid=047F pid= C039 split=01 intf=00,03` autorise l'interface 00 et 03 et interdit les autres.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Dans une session de bureau, les périphériques USB divisés sont affichés dans Desktop Viewer sous **Périphériques**. En outre, vous pouvez afficher les périphériques USB divisés dans **Préférences** > **Périphériques**.



Dans une session d'application, les périphériques USB divisés sont affichés dans le **Centre de connexion**.



Le tableau ci-dessous fournit des informations sur les scénarios de comportement lorsqu'une interface USB est autorisée ou interdite.

Pour autoriser une interface :

Divisé	Interface	Action
VRAI	Numéro valide 0 -n	Autorise l'interface spécifiée
VRAI	Numéro non valide	Autorise toutes les interfaces
FAUX	Toute valeur	Autorise USB générique du périphérique parent
Non spécifié	Toute valeur	Autorise USB générique du périphérique parent

Par exemple, SplitDevices- *true* indique que tous les périphériques sont divisés.

Pour interdire une interface :

Divisé	Interface	Action
VRAI	Numéro valide 0 -n	Interdit l'interface spécifiée
VRAI	Numéro non valide	Interdit toutes les interfaces
FAUX	Toute valeur	Interdit USB générique du périphérique parent

Divisé	Interface	Action
Non spécifié	Toute valeur	Interdit USB générique du périphérique parent

Par exemple, SplitDevices- *false* indique que les périphériques avec le numéro d'interface spécifié ne sont pas divisés.

Exemple : *MyPlantronics* headset

Numéro d'interface :

- Classe d'interface audio -0
- Classe d'interface HID -3

Exemples de règles utilisées pour *MyPlantronics* headset :

- AUTORISER :`vid=047F pid= C039 split=01 intf=00,03 /Allowed 00 and 03 interface, restrict others`
- INTERDIRE : `vid=047F pid= C039 split=01 intf=00,03 / deny 00 and 03`

Limitation :

Citrix recommande de ne pas diviser les interfaces pour une webcam. Pour contourner ce problème, redirigez le périphérique vers un périphérique unique en utilisant la redirection USB générique. Pour de meilleures performances, utilisez le canal virtuel optimisé.

Mise à l'échelle DPI

L'application Citrix Workspace permet au système d'exploitation de contrôler la résolution de la session.

Vous pouvez appliquer une résolution élevée dans une session, mais la fonctionnalité est désactivée par défaut. Cela signifie que la mise à l'échelle de la session suit la résolution du système d'exploitation.

Vous pouvez configurer la mise à l'échelle DPI en utilisant les options suivantes :

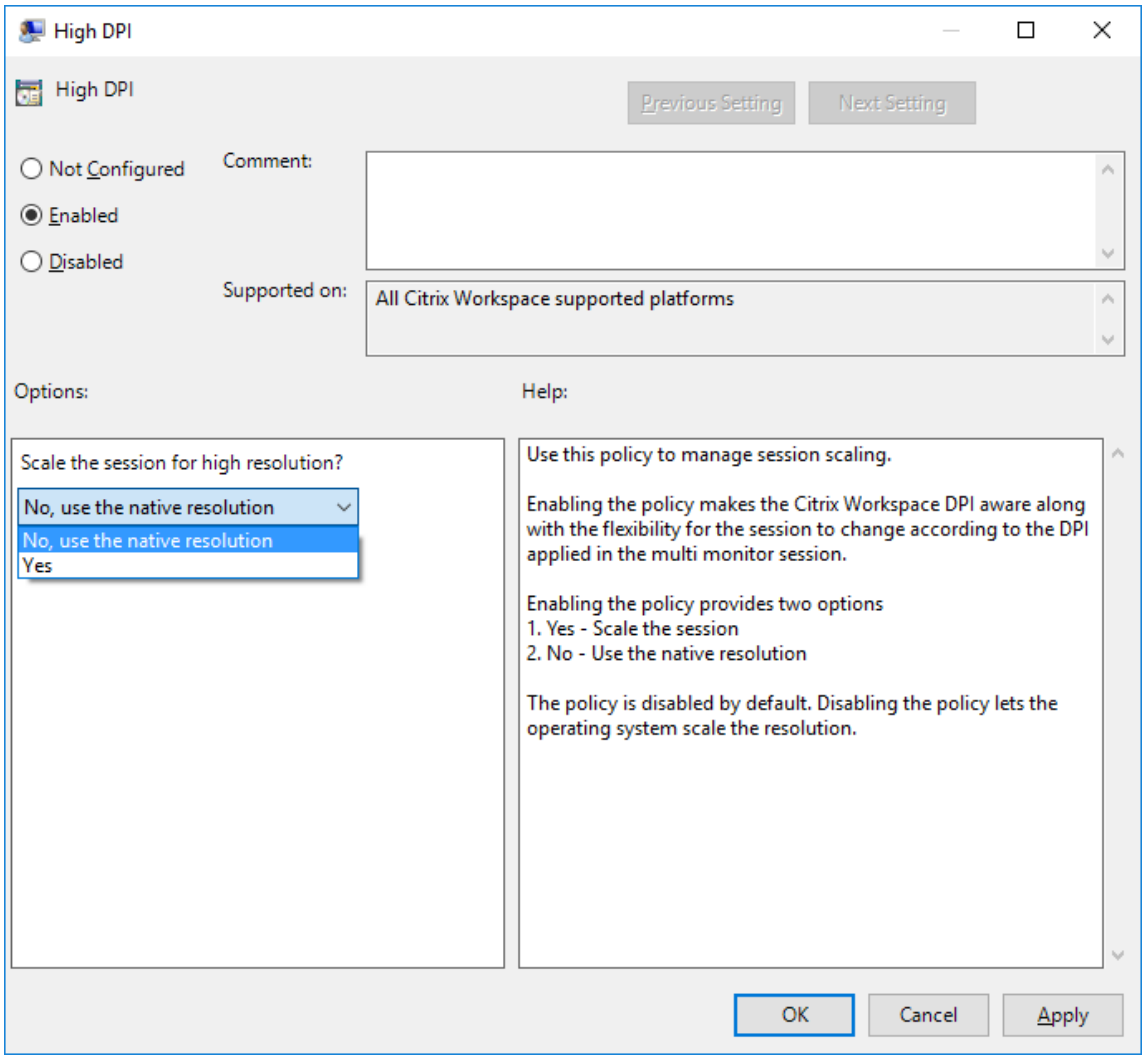
1. Modèle d'administration d'objet de stratégie de groupe (configuration par machine)
2. Préférences avancées (configuration par utilisateur)

Limitations :

- Même lorsque cette fonctionnalité est activée, un léger flou est observé dans le Desktop Viewer.
- Dans une session, lorsque vous modifiez les paramètres DPI et que vous la relancez, la taille de la fenêtre de session peut ne pas être appropriée. Pour contourner le problème, redimensionnez la fenêtre de session.

Pour configurer la mise à l'échelle DPI à l'aide du modèle d'administration d'objet de stratégie de groupe :

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **DPI**.
3. Sélectionnez la stratégie **DPI élevé**.



4. Sélectionnez l'une des options suivantes :
   a) Oui - Indique que la stratégie DPI élevé est appliquée dans une session.
   b) Non, utiliser la résolution native - Indique que la résolution est définie par le système d'exploitation.
5. Cliquez sur **Appliquer, puis sur OK**.

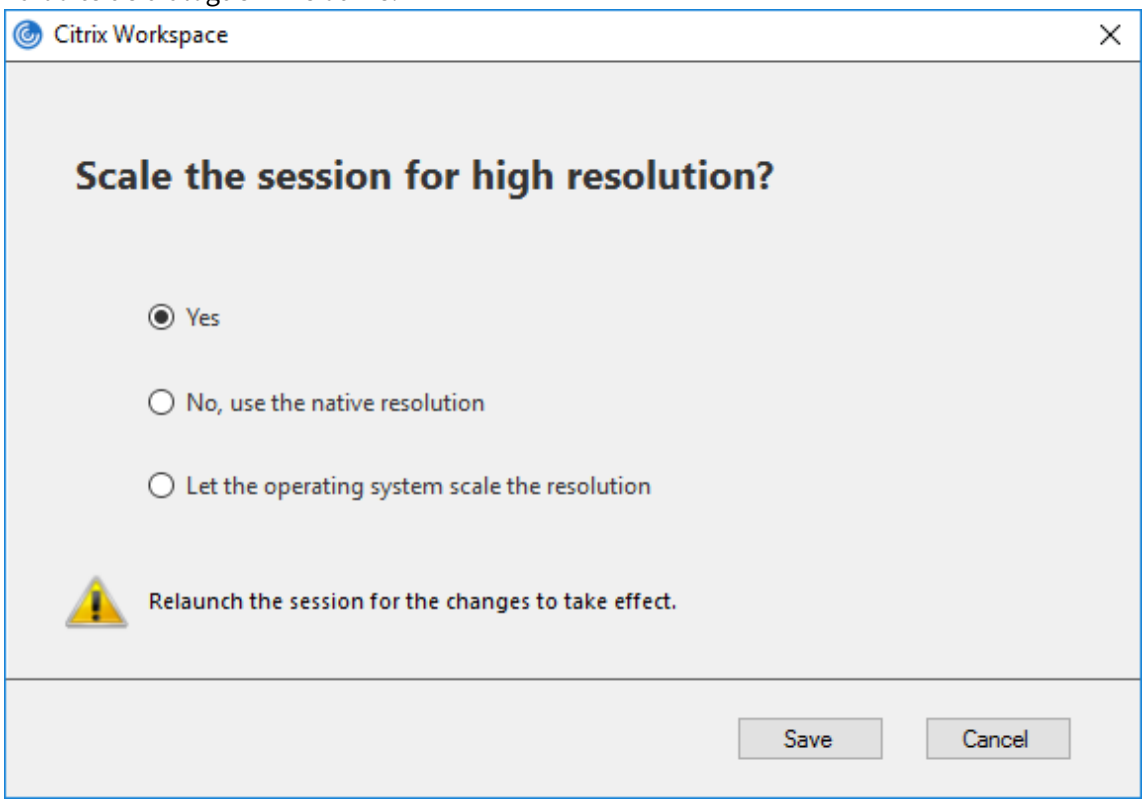
6. Exécutez la commande `gpupdate /force` à partir d'une ligne de commande pour appliquer les modifications.

Configurer la mise à l'échelle DPI à l'aide de l'interface utilisateur graphique :

> **Remarque :**
>
> Vous pouvez masquer partiellement ou totalement la page Préférences avancées disponible à partir de l'icône de l'application Citrix Workspace pour Windows dans la zone de notification. Pour plus d'informations, veuillez consulter l'article Page Préférences avancées.

1. Cliquez avec le bouton droit de la souris sur l'icône de l'application Citrix Workspace dans la zone de notification.
2. Sélectionnez **Préférences avancées** et cliquez sur **Paramètres DPI**.

   La boîte de dialogue DPI s'ouvre.



3. Sélectionnez l'une des options suivantes :

   a) Oui - Indique que la stratégie DPI élevé est appliquée dans une session.
   b) Non, utiliser la résolution native - Indique que l'application Workspace détecte le DPI sur le VDA et l'applique.
   c) Laisser le système d'exploitation régler la résolution - Cette option est sélectionnée par défaut. Elle permet à Windows de gérer la mise à l'échelle DPI. Cette option signifie également que la stratégie DPI élevé est désactivée.

4. Cliquez sur **Enregistrer**.
5. Redémarrez la session de l'application Citrix Workspace pour que les modifications prennent effet.

Options de réglage DPI

Il existe trois paramètres possibles pour la mise à l'échelle DPI dans l'application Citrix Workspace, à savoir avec une mise à l'échelle (Scaled), sans mise à l'échelle (Unscaled) et avec la mise à l'échelle du système d'exploitation. Les cas d'utilisation pour les différents paramètres sont les suivants.

Scaled :

Le paramètre Scaled met à l'échelle la résolution sur le VDA de la même manière que la mise à l'échelle du système d'exploitation. Cependant, ce paramètre prend en charge des scénarios DPI mixtes. Ce paramètre correspond au paramètre d'interface utilisateur « Oui » ou à la stratégie « DPI élevé » définie sur « Activé» dans l'objet de stratégie de groupe. Ce paramètre fonctionne bien pour les scénarios DPI mixtes lors de la connexion à des VDA modernes. Il s'agit du seul moyen d'adapter les sessions sans interruption. La mise à l'échelle peut créer un flou sur les images, en particulier dans le texte. Les performances peuvent être médiocres lors de la connexion à des VDA d'ancienne génération (6.5 ou configurés pour les anciens graphiques), Local App Access, RTOP et d'autres plug-ins utilisant les API de positionnement de l'écran ne fonctionnent pas avec la mise à l'échelle. De par leur conception, les applications transparentes basculent entre les moniteurs dans ce mode pour maintenir une mise à l'échelle correcte.
Ce paramètre est recommandé aux utilisateurs de Windows 10 qui se connectent à des VDA modernes. Il prend en charge des DPI mixtes sans impact supplémentaire sur les ressources du serveur.

Unscaled :

Le paramètre Unscaled envoie la résolution complète de tous les moniteurs de la session. Ces résolutions ne sont pas mises à l'échelle et peuvent générer du texte et des icônes de petite taille dans les applications et bureaux. Ce paramètre correspond au paramètre d'interface utilisateur « Non » ou à la stratégie « DPI élevé » définie sur « Activé» dans l'objet de stratégie de groupe. Ce paramètre n'engendre pas une apparence floue dû à la mise à l'échelle, mais peut entraîner la création de texte et d'icônes de petite taille. Lors de la connexion à une session de bureau, le DPI peut être défini dans le VDA, ce qui donne la mise à l'échelle souhaitée. Cela n'est pas possible sur les bureaux RDS ou les applications transparentes. L'activation de ce paramètre entraîne des sessions avec une résolution plus élevée, ce qui peut affecter les performances et l'évolutivité du serveur.
Ce paramètre est recommandé pour les sessions de bureau nécessitant la meilleure qualité d'image lorsque les ressources de serveur supplémentaires sont acceptables. Il peut également être utilisé dans les cas où le texte et les icônes de petite taille ne posent pas problème pour l'utilisateur.

Mise à l'échelle du système d'exploitation :

La mise à l'échelle du système d'exploitation est la valeur par défaut et correspond au paramètre de l'interface utilisateur « Laisser le système d'exploitation régler la résolution ». La stratégie « DPI élevé » est définie sur « Désactivé » dans ce scénario. Cela permet au système d'exploitation Windows de gérer la mise à l'échelle DPI pour une session. La résolution sur le VDA est mise à l'échelle en fonction du DPI, ce qui entraîne une résolution inférieure à celle de la machine cliente. Ce paramètre fonctionne bien pour les sessions à moniteur unique et est efficace lors de la connexion à des VDA 6.5 ou à des VDA configurés pour des anciens graphiques. Cette méthode ne prend pas en charge les DPI mixtes : tous les moniteurs doivent avoir le même DPI ou la session ne fonctionne pas. La mise à l'échelle peut créer un flou sur les images, en particulier dans le texte. Il peut également y avoir des problèmes de taille de curseur sur le système d'exploitation Windows 10.
Ce paramètre est recommandé aux utilisateurs de point de terminaison Windows 7 ou à ceux se connectant à des VDA d'ancienne génération. Il peut également être utilisé sur Windows 10 si aucun DPI mixte n'est présent.

Disposition d'affichage virtuel

Cette fonctionnalité vous permet de définir une disposition de moniteur virtuel qui s'applique au bureau distant et de diviser virtuellement un seul moniteur client en un maximum de huit moniteurs sur le bureau distant. Vous pouvez configurer les moniteurs virtuels dans l'onglet **Disposition du moniteur** de Desktop Viewer. Vous pouvez y dessiner des lignes horizontales ou verticales pour séparer l'écran en moniteurs virtuels. L'écran est divisé en fonction des pourcentages spécifiés pour la résolution du moniteur client.

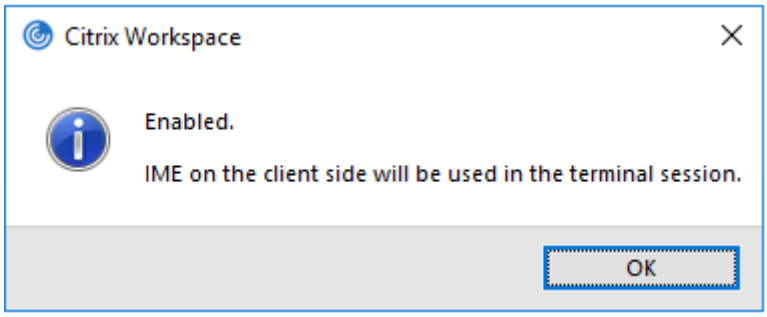
Vous pouvez définir un DPI pour les moniteurs virtuels qui sont utilisés pour la mise à l'échelle ou la correspondance DPI. Après avoir appliqué une disposition de moniteur virtuel, redimensionnez ou reconnectez la session.

Cette configuration s'appliquera uniquement aux sessions de bureau sur un seul moniteur plein écran, et n'affectera aucune application publiée. Cette configuration s'appliquera à toutes les connexions suivantes à partir de ce client.

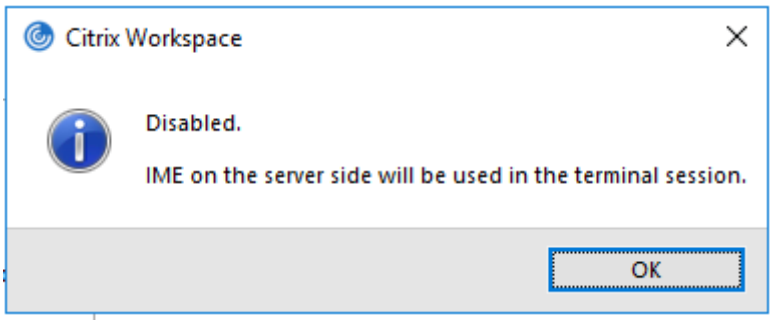
Éditeurs IME clients génériques

Configuration d'éditeurs IME clients génériques à l'aide de l'interface de ligne de commande :

- Pour activer l'éditeur IME client générique, exécutez la commande `wfica32.exe /localime:on` à partir du dossier d'installation de l'application Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`.

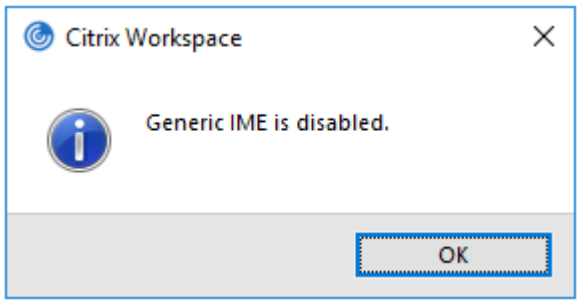


- Pour désactiver l'éditeur IME client générique, exécutez la commande `wfica32.exe /localime:off` à partir du dossier d'installation de l'application Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`.

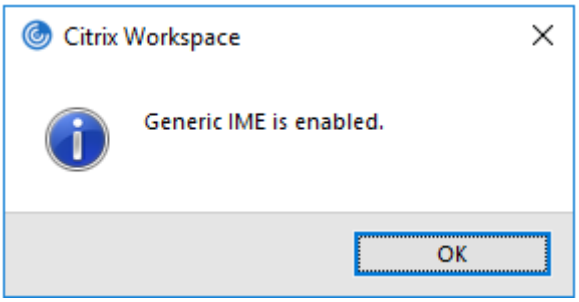


> **Remarque :**
>
> Vous pouvez utiliser le commutateur de ligne de commande `wfica32.exe /localime:on` pour activer l'éditeur IME client générique et la synchronisation de la disposition du clavier.

- Pour désactiver l'éditeur IME client générique, exécutez la commande `wfica32.exe /localgenericime:off` à partir du dossier d'installation de l'application Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`. Cette commande n'affecte pas les paramètres de synchronisation de la disposition du clavier.



Si vous avez désactivé l'éditeur IME client générique à l'aide de l'interface de ligne de commande, vous pouvez réactiver la fonctionnalité en exécutant la commande `wfica32.exe /localgenericime:on`.



Activer/désactiver :

L'application Citrix Workspace permet d'activer ou de désactiver cette fonctionnalité. Vous pouvez exécuter la commande `wfica32.exe /localgenericime:on` pour activer ou désactiver la fonctionnalité. Toutefois, les paramètres de synchronisation de disposition du clavier ont priorité sur le commutateur à bascule. Si la synchronisation de la disposition du clavier est définie sur **Off**, le basculement n'active pas l'éditeur IME client générique.

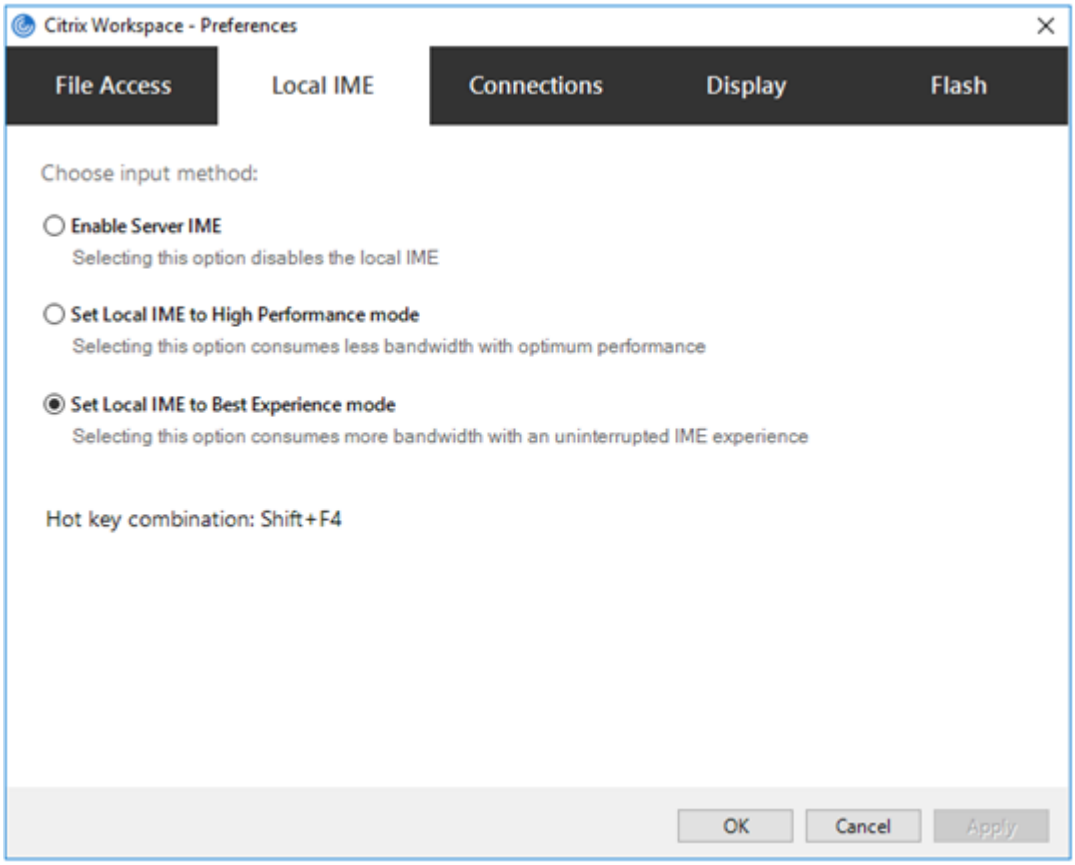
Configuration d'éditeurs IME clients génériques à l'aide de l'interface utilisateur graphique :

L'éditeur IME client générique requiert la version 7.13 ou ultérieure du VDA.

La fonctionnalité d'éditeur IME client générique peut être activée en activant la synchronisation de la disposition du clavier. Pour plus d'informations, veuillez consulter l'article Synchronisation de la disposition du clavier.

L'application Citrix Workspace vous permet de configurer différentes options d'utilisation de l'éditeur IME client générique. Vous pouvez sélectionner l'une ces options en fonction de vos exigences et de votre utilisation.

1. Dans une session d'application active, cliquez avec le bouton droit de la souris sur l'icône de l'application Citrix Workspace dans la zone de notification et sélectionnez **Centre de connexion**.
2. Sélectionnez **Préférences** et cliquez sur **Éditeur IME local**.



Les options ci-dessous sont disponibles pour prendre en charge différents modes IME :

1. **Activer l'éditeur IME du serveur :** désactive l'IME local et seules les langues définies sur le serveur peuvent être utilisées.
2. **Définir l'éditeur IME local sur le mode Performances élevées :** utilise l'éditeur IME local avec une bande passante limitée. Cette option limite la fonctionnalité de fenêtre candidate.
3. **Définir l'éditeur IME local sur le mode Expérience optimale :** utilise l'éditeur IME local avec une expérience utilisateur optimale. Cette option consomme beaucoup de bande passante. Par défaut, cette option est sélectionnée lorsque l'éditeur IME client générique est activé.

Les modifications apportées aux paramètres sont appliquées uniquement pour la session en cours.

Activation de touches de raccourci à l'aide d'un éditeur de Registre :

Lorsque l'éditeur IME client générique est activé, vous pouvez utiliser la combinaison **MAJ+F4** pour sélectionner différents mode IME. Les différentes options des modes IME s'affichent dans le coin supérieur droit de la session.

Par défaut, la touche de raccourci de l'éditeur IME client générique est désactivée.

Dans l'Éditeur du Registre, accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys.

Sélectionnez **AllowHotKey** et modifiez la valeur par défaut sur 1.

Limitations :

- L'éditeur IME client générique ne prend pas en charge les applications UWP (plate-forme Windows universelle) telles que l'interface utilisateur de la recherche et le navigateur Edge du système d'exploitation Windows 10. Pour contourner le problème, utilisez l'éditeur IME du serveur.
- L'éditeur IME client générique n'est pas pris en charge sur Internet Explorer version 11 en **Mode protégé**. Pour contourner le problème, vous pouvez désactiver le Mode protégé en utilisant les **Options Internet**. Pour ce faire, cliquez sur **Sécurité** et décochez **Activer le mode protégé**.

Codage vidéo H.265

L'application Citrix Workspace prend en charge l'utilisation du codec vidéo H.265 pour l'accélération matérielle des graphiques et vidéos distants. Vous ne pouvez bénéficier de cette fonctionnalité que si elle est prise en charge et activée à la fois sur le VDA et sur l'application Citrix Workspace. Si le GPU du point de terminaison ne prend pas en charge le décodage H.265 à l'aide de l'interface DXVA, le paramètre de stratégie de décodage H265 pour les graphiques est ignoré et la session utilise le codec vidéo H.264.

Conditions préalables :

1. VDA 7.16 et versions ultérieures.
2. Activez la stratégie **Optimiser pour la charge des graphiques 3D** sur le VDA.
3. Activez la stratégie **Utiliser le codage matériel pour le codec vidéo** sur le VDA.

> **Remarque :**
>
> Le codage H.265 est pris en charge uniquement sur le GPU NVIDIA.

Dans l'application Citrix Workspace pour Windows, cette fonctionnalité est définie sur **Désactivé** par défaut.

Configuration de l'application Citrix Workspace pour utiliser le codage vidéo H.265 à l'aide du modèle d'administration d'objet de stratégie de groupe Citrix :

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Citrix Workspace** > **Expérience utilisateur**.
3. Sélectionnez la stratégie **Décodage H265 pour graphiques**.
4. Sélectionnez **Activé**.
5. Cliquez sur **Appliquer**, puis sur **OK**.

Configuration de l'application Citrix Workspace pour utiliser le codage vidéo H.265 à l'aide de l'Éditeur du Registre :

Activation du codage vidéo H.265 sur un réseau n'appartenant pas au domaine sur un système d'exploitation 32 bits :

1. Lancez l'Éditeur du Registre en tapant regedit dans la commande Exécuter.
2. Accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Graphics Engine.
3. Créez une clé DWORD nommée **EnableH265** et définissez la valeur de la clé sur 1.

Activation du codage vidéo H.265 sur un réseau n'appartenant pas au domaine sur un système d'exploitation 64 bits :

1. Lancez l'Éditeur du Registre en tapant regedit dans la commande Exécuter.
2. Accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine.
3. Créez une clé DWORD nommée EnableH265 et définissez la valeur de la clé sur 1.

Redémarrez la session pour que les modifications prennent effet.

> **Remarque :**
>
> - Si la stratégie **Accélération matérielle pour graphiques** est désactivée dans le modèle d'administration de l'objet de stratégie de groupe de l'application Citrix Workspace pour Windows, les paramètres de la stratégie **Décodage H265 pour graphiques** sont ignorés et la fonctionnalité ne fonctionne pas.
> - Exécutez l'outil HDX Monitor 3.x pour identifier si l'encodeur vidéo H.265 est activé dans les sessions. Pour plus d'informations sur l'outil HDX Monitor 3.x, consultez l'article CTX135817 du centre de connaissances.

Clavier et barre de langue

Configuration du clavier

> **Remarque :**
>
> Vous pouvez masquer partiellement ou totalement la page Préférences avancées disponible

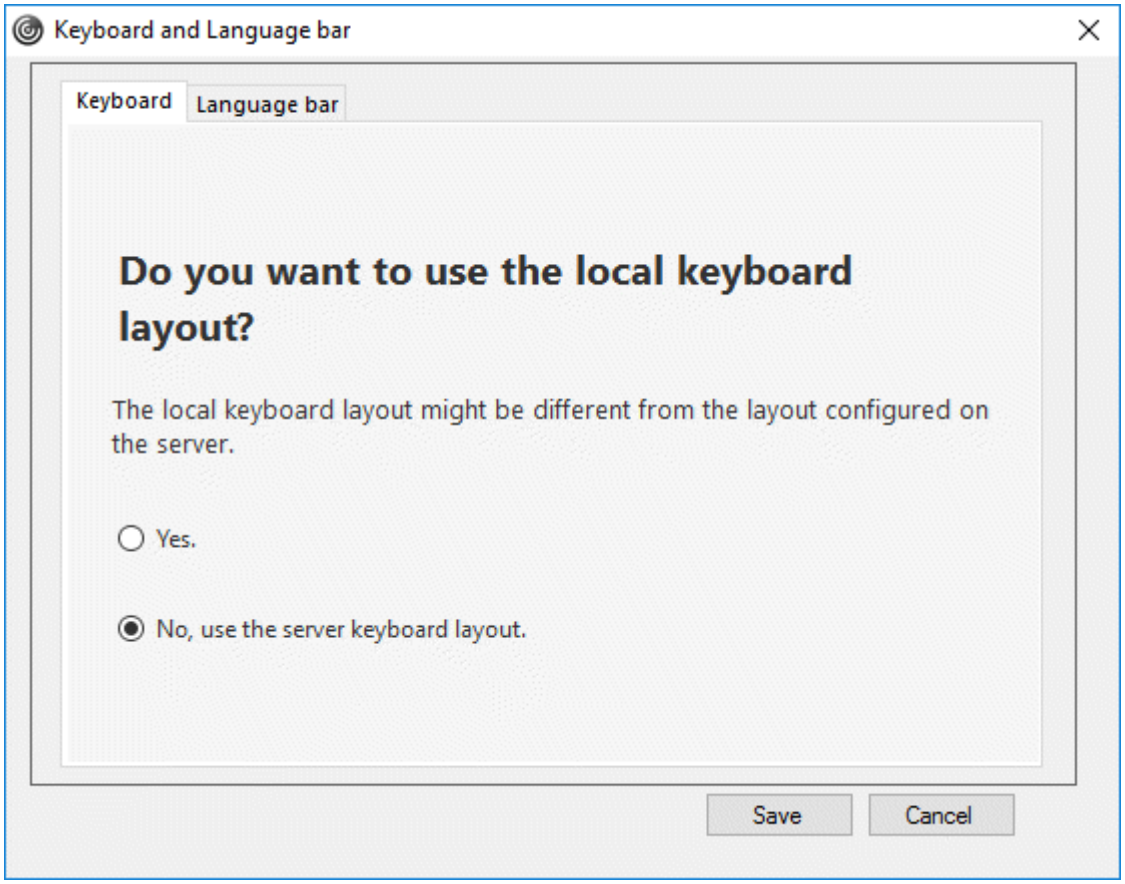
> à partir de l'icône de l'application Citrix Workspace dans la zone de notification. Pour plus d'informations, veuillez consulter l'article Page Préférences avancées.

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

Pour activer la synchronisation de la disposition du clavier :

1. À partir de l'icône de l'application Citrix Workspace dans la zone de notification, sélectionnez **Préférences avancées** > **Clavier et barre de langue**.

   La boîte de dialogue Clavier et barre de langue apparaît.



2. Sélectionnez l'une des options suivantes :

   - Oui - Indique que la disposition du clavier local est utilisée dans une session.
   - Non, utiliser la disposition de clavier du serveur - Indique que la disposition du clavier utilisée sur le VDA est appliquée dans une session. Cette option désactive la fonctionnalité de disposition du clavier local.

3. Cliquez sur **Enregistrer**.

Vous pouvez également activer et désactiver la synchronisation de la disposition du clavier à l'aide de la ligne de commande en exécutant `wfica32:exe /localime:on` ou `wfica32:exe /localime:`

`off` à partir du dossier d'installation de l'application Citrix Workspace pour Windows `C:\Program files (x86)\Citrix\ICA Client`.

l'utilisation de l'option de disposition du clavier local active l'éditeur IME (Éditeur de méthode d'entrée) du client. Si les utilisateurs qui travaillent en japonais, en chinois simplifié ou en coréen préfèrent utiliser l'éditeur IME du serveur, ils doivent désactiver l'option de disposition du clavier local en sélectionnant **Non** ou en exécutant `wfica32:exe /localime:off`. Lorsqu'ils se connecteront à la prochaine session, la disposition du clavier fournie par le serveur distant sera rétablie.

Parfois, le basculement vers la disposition du clavier de la machine cliente ne prend pas effet dans une session active. Pour résoudre ce problème, fermez la session de l'application Citrix Workspace et reconnectez-vous.

Masquer la boîte de dialogue de notification liée au changement de la disposition du clavier :

La boîte de dialogue de notification liée au changement de la disposition du clavier vous indique que la disposition du clavier de la session VDA est en train de changer. Il faut environ deux secondes pour que le changement de la disposition du clavier prenne effet. Lorsque vous masquez la boîte de dialogue de notification, attendez un certain temps avant de commencer à taper pour éviter une saisie incorrecte.

> **Avertissement**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Masquer la boîte de dialogue de notification liée au changement de la disposition de clavier à l'aide de l'Éditeur du Registre :

1. Lancez l'Éditeur du Registre et naviguez jusqu'à `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Créez une clé de valeur de chaîne nommée **HideNotificationWindow**.
3. Définissez la valeur DWORD sur **1**.
4. Cliquez sur **OK**.
5. Redémarrez la session pour que les modifications prennent effet.

Limitations :

- Les applications distantes exécutées avec des privilèges élevés (par exemple, clic droit sur l'icône d'une application > Exécuter en tant qu'administrateur) ne peuvent pas être synchronisées avec la disposition du clavier de la machine cliente. Pour résoudre ce problème, modifiez manuellement la disposition du clavier du côté serveur (VDA) ou désactivez le contrôle de compte d'utilisateur.

- Si l'utilisateur change la disposition du clavier sur le client au profit d'une disposition qui n'est pas prise en charge sur le serveur, la fonctionnalité de synchronisation de la disposition du clavier est désactivée pour des raisons de sécurité - une disposition de clavier non reconnue est considérée comme une menace potentielle pour la sécurité. Pour rétablir la fonctionnalité de synchronisation de la disposition du clavier, fermez la session et ouvrez une nouvelle session.
- Dans une session RDP, vous ne pouvez pas modifier la disposition du clavier à l'aide des raccourcis Alt + Maj. Pour résoudre ce problème, utilisez la barre de langue dans la session RDP pour changer la disposition du clavier.
- Cette fonctionnalité est désactivée dans Windows Server 2016 en raison d'un problème de tiers pouvant affecter les performances. Cette fonctionnalité peut être activée à l'aide d'un paramètre de registre sur le VDA : dans HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme, ajoutez une nouvelle clé nommée **DisableKeyboardSync** et définissez la valeur sur 0.

Barre de langue

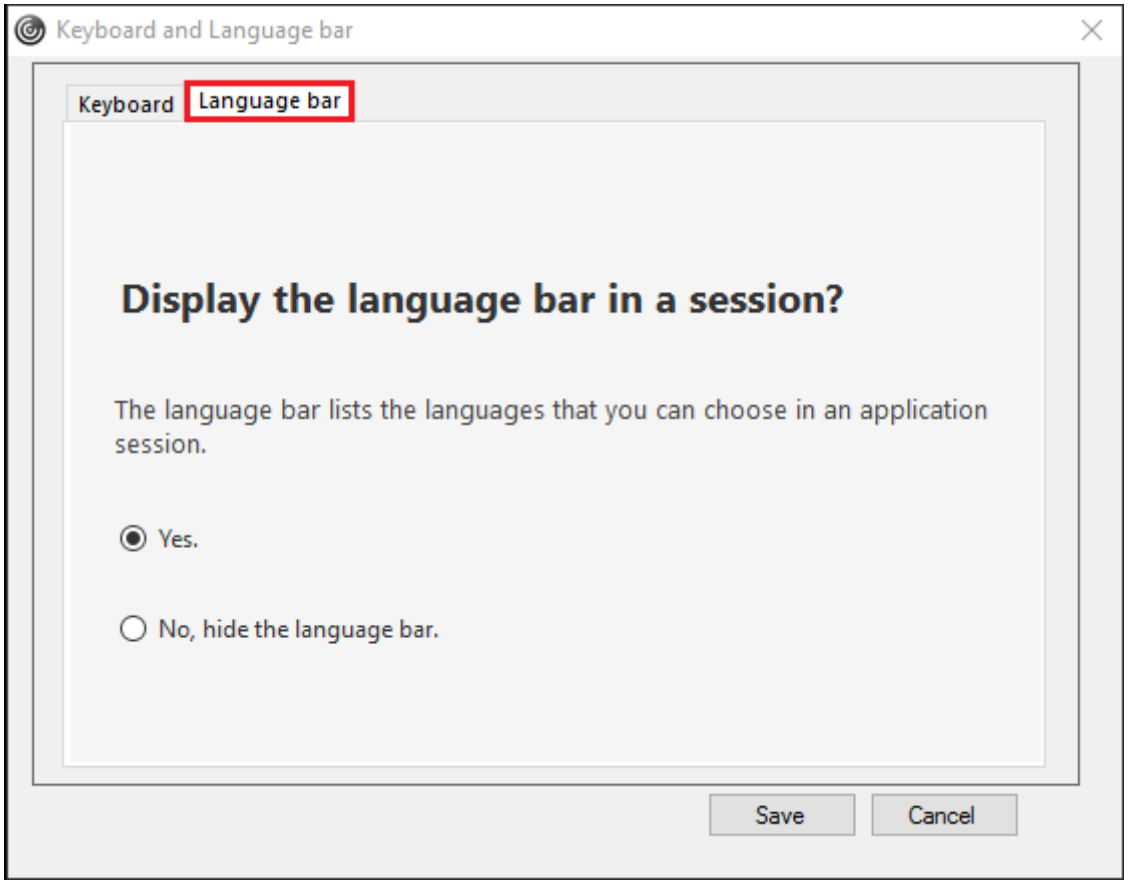
La barre de langue affiche la langue d'entrée préférée dans une session. Dans les versions antérieures, vous pouviez modifier ce paramètre en utilisant uniquement les clés de registre du VDA. À partir de Citrix Receiver pour Windows version 4.11, vous pouvez modifier les paramètres à l'aide de la boîte de dialogue **Préférences avancées**. 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. Cliquez avec le bouton droit de la souris sur l'icône de l'application Citrix Workspace dans la zone de notification et sélectionnez **Préférences avancées**.
2. Sélectionnez **Clavier et barre de langue**.
3. Sélectionnez l'onglet **Barre de langue**.
4. Sélectionnez l'une des options suivantes :
   a) Oui - Indique que la barre de langue est affichée dans une session.
   b) Non, masquer la barre de langue - Indique que la barre de langue est masquée dans une session.
5. Cliquez sur **Enregistrer**.

   Les modifications de paramètres prennent effet immédiatement.



> **Remarque :**
>
> - 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.

Masquer l'onglet de la barre de langue de la page Préférences avancées :

Vous pouvez masquer l'onglet de la barre de langue à partir de la page **Préférences avancées** en utilisant le registre.

1. Lancez l'Éditeur du Registre.
2. Accéder à `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LocalIME`.
3. Créez une clé de valeur DWORD, **ToggleOffLanguageBarFeature**, et définissez-la sur **1** pour masquer l'option de la barre de langue dans la page Préférences avancées.

Prise en charge USB

La prise en charge USB vous permet d'interagir avec une large gamme de périphériques USB connectés à Citrix Virtual Apps and Desktops. Vous pouvez brancher des périphériques USB à vos or-

dinateurs ; ils sont envoyés vers vos bureaux virtuels. Les périphériques USB suivants sont pris en charge : lecteurs flash, smartphones, ordinateurs de poche, imprimantes, scanners, lecteurs MP3, périphériques de sécurité et tablettes. Les utilisateurs Desktop Viewer peuvent spécifier si les périphériques USB sont disponibles sur Citrix Virtual Apps and Desktops à l'aide d'une préférence dans la barre d'outils.

Les fonctionnalités isochrones des périphériques USB tels que les webcams, les micros, les haut-parleurs et les micro-casques sont prises en charge dans des environnements LAN (réseaux locaux) à faible latence et à haut débit. Cela permet à ces périphériques d'interagir avec des packs tels que Microsoft Office Communicator et Skype.

Les types de périphériques suivants sont pris en charge directement dans une session Citrix Virtual Apps and Desktops ; ils n'utilisent donc pas la prise en charge USB :

- Claviers
- Souris
- Cartes à puce

Les périphériques USB spécialisés (par exemple, claviers et souris 3D Bloomberg) peuvent être configurés pour utiliser la prise en charge USB. Pour plus d'informations sur la configuration des claviers Bloomberg, consultez la section
Configuration des claviers Bloomberg.

Pour plus d'informations sur la configuration des règles de stratégie pour d'autres périphériques USB spécialisés, consultez l'article
CTX122615.

Par défaut, certains types de périphériques USB ne sont pas pris en charge pour l'accès à distance via Citrix Virtual Apps and Desktops. Par exemple, une carte d'interface réseau peut être reliée à la carte système par une connexion USB interne. Il n'est pas conseillé de configurer un accès distant pour ce périphérique. Les types de périphériques USB suivants ne sont pas pris en charge par défaut dans une session Citrix Virtual Apps and Desktops :

- Dongles Bluetooth
- Cartes d'interface réseau intégrées
- Concentrateurs USB
- Adaptateurs graphiques USB

Les périphériques USB connectés à un concentrateur peuvent être gérés à distance, mais pas le concentrateur.

Par défaut, les types de périphériques USB suivants ne sont pas pris en charge pour une utilisation dans une session Citrix Virtual Apps and Desktops :

- Dongles Bluetooth
- Cartes d'interface réseau intégrées

- Concentrateurs USB
- Adaptateurs graphiques USB
- Périphériques audio
- Périphériques de stockage de masse

Fonctionnement de la prise en charge USB :

Lorsqu'un utilisateur branche un périphérique USB, ce dernier est comparé à la stratégie USB, et s'il est autorisé, il est envoyé sur le bureau virtuel. Si la stratégie par défaut refuse le périphérique, il n'est disponible que sur le bureau local.

Lorsqu'un utilisateur branche un périphérique USB, une notification s'affiche pour informer l'utilisateur qu'un nouveau périphérique est apparu. L'utilisateur peut choisir les périphériques USB à envoyer sur le bureau virtuel en les sélectionnant dans la liste chaque fois qu'il se connecte. L'utilisateur peut également configurer la prise en charge USB de manière à ce que tous les périphériques USB connectés avant et/ou pendant une session soient automatiquement envoyés au bureau virtuel qui a le focus.

Périphériques de stockage de masse

Pour les périphériques de stockage de masse uniquement, en plus de la prise en charge USB, l'accès à distance est disponible via le mappage des lecteurs clients, que vous pouvez configurer à l'aide de la stratégie de l'application Citrix Workspace pour Windows **Accès à distance des périphériques clients** > **Mappage des lecteurs clients**. Lorsque cette stratégie est appliquée, les lecteurs de la machine utilisateur sont automatiquement mappés vers les lettres de lecteur sur le bureau virtuel lorsque les utilisateurs ouvrent une session. Les lecteurs sont affichés sous la forme de dossiers partagés associés à des lettres de lecteur mappé.

Les différences principales entre les deux types de stratégie à distance sont les suivantes :

Fonctionnalité	Mappage des lecteurs clients	Prise en charge USB
Activée par défaut	Oui	Non
Accès en lecture seule configurable	Oui	Non
Le périphérique peut être retiré en toute sécurité au cours d'une session	Non	Oui, si un utilisateur clique sur Retirer le périphérique en toute sécurité dans la zone de notification.

Si USB générique et les stratégies de mappage des lecteurs clients sont tous deux activés et qu'un

périphérique de stockage de masse est inséré avant le démarrage d'une session, il est tout d'abord redirigé à l'aide du mappage des lecteurs clients, avant d'être considéré pour la redirection via la prise en charge USB. S'il est inséré après le démarrage d'une session, il sera considéré pour la redirection à l'aide de la prise en charge USB avant le mappage des lecteurs clients.

Classes de périphériques USB autorisées par défaut :

Différentes classes de périphériques USB sont autorisées par les règles de stratégie USB par défaut.

Bien qu'elles figurent sur cette liste, certaines classes ne peuvent être gérées à distance que dans les sessions Citrix Virtual Apps and Desktops après une configuration supplémentaire. Elles sont indiquées ci-dessous.

- **Audio (Class 01)** - Comprend des périphériques d'entrée audio (micros), des périphériques de sortie audio et des contrôleurs MIDI. Les périphériques audio modernes utilisent généralement les transferts isochrones, qui sont pris en charge par XenDesktop 4 ou version ultérieure. Audio (Class01) n'est pas applicable pour Citrix Virtual Apps car ces périphériques ne sont pas disponibles pour l'accès à distance dans Citrix Virtual Apps à l'aide de la prise en charge USB.

> **Remarque :**
>
> Certains périphériques spécialisés (par exemple les téléphones VOIP) requièrent une configuration supplémentaire. Pour plus d'informations, consultez l'article CTX123015 du centre de connaissances.

- **Périphériques d'interface physique (Classe 05)** - Ces périphériques sont similaires aux périphériques d'interface utilisateur (HID), mais ils fournissent en général des données en temps-réel et comprennent des joysticks de retour de force, des plates-formes mouvantes et des exosquelettes de retour de force.
- **Acquisition d'images fixes (Classe 06)** - Comprend scanners et appareils photo numériques. Les appareils photo numériques prennent généralement en charge la classe d'acquisition d'images fixes qui utilise le protocole PTP (Picture Transfer Protocol) ou MTP (Media Transfer Protocol) pour transférer des images sur un ordinateur ou un autre périphérique. Les appareils photo peuvent également apparaître comme périphériques de stockage de masse et il est possible de configurer un appareil photo pour utiliser les deux classes, par le biais des menus fournis par l'appareil photo.

> **Remarque :**
>
> Si un appareil photo apparaît en tant que périphérique de stockage de masse, le mappage des lecteurs clients est utilisé et la prise en charge USB n'est pas requise.

- **Imprimantes (Classe 07)** - En général, la plupart des imprimantes appartiennent à cette classe, à l'exception de certaines qui utilisent des protocoles spécifiques au fabricant (classe ff). Les imprimantes multifonctions peuvent disposer d'un concentrateur interne ou être des périphériques composites. Dans les deux cas, l'élément d'impression utilise généralement

la classe Imprimantes et l'élément de fax ou de numérisation utilise une autre classe ; par exemple, acquisition d'images fixes.

Les imprimantes fonctionnent correctement sans prise en charge USB.

> **Remarque**
>
> Cette classe de périphérique (en particulier les imprimantes équipées de fonctions de numérisation) requiert une configuration supplémentaire. Pour obtenir des instructions, consultez l'article CTX123015 du centre de connaissances.

- **Stockage de masse (Classe 08)** - Les périphériques de stockage de masse les plus courants sont les lecteurs flash USB ; les disques dur USB, lecteurs CD/DVD et lecteurs de cartes SD/MMC sont également des périphériques de stockage de masse. Les périphériques avec stockage interne dotés d'une interface de stockage de masse sont également nombreux ; sont compris dans cette catégorie les lecteurs multimédias, les appareils photos numériques et les téléphones portables. Le stockage de masse (Classe 08) n'est pas applicable pour Citrix Virtual Apps car ces périphériques ne sont pas disponibles pour l'accès à distance dans Citrix Virtual Apps à l'aide de la prise en charge USB. Sous-classes connues :
  - 01 Périphériques flash limités
  - 02 Lecteurs de CD/DVD (ATAPI/MMC-2)
  - 03 Lecteurs de bandes (QIC-157)
  - 04 Lecteurs de disquettes (UFI)
  - 05 Lecteurs de disquettes (SFF-8070i)
  - 06 La plupart des périphériques de stockage de masse utilisent cette variante de SCSI.

  Étant donné que le mappage des lecteurs clients peut être utilisé pour accéder à la plupart des périphériques au travers du mappage de lecteur client, la prise en charge USB n'est pas requise.
- **Sécurité du contenu (Classe 0d)** - Les périphériques de sécurité du contenu assurent la protection du contenu, en général pour la gestion des licences ou des droits numériques. Cette classe comprend les dongles.
- **Vidéo (Classe 0e)** - La classe vidéo couvre les périphériques utilisés pour manipuler les vidéos, tels que les webcams, les caméscopes numériques, les convertisseurs vidéo analogique, certains tuner TV et certains appareils photo numériques qui prennent en charge le streaming vidéo.

> **Important**
>
> La plupart des périphériques de streaming vidéo utilisent les transferts isochrones, qui sont pris en charge par XenDesktop 4 ou version ultérieure. Certains périphériques vidéo (par exemple les webcams équipées de fonctions de détection des mouvements) requièrent une configura-

> tion supplémentaire. Pour obtenir des instructions, consultez l'article CTX123015 du centre de connaissances.

- **Santé personnelle (Classe 0f)** - Ces appareils comprennent des capteurs de pression artérielle, des moniteurs de pouls, des podomètres, des piluliers et des spiromètres.
- **Spécifique au fabricant et à l'application (Classes fe et ff)** - De nombreux périphériques utilisent des protocoles spécifiques au fabricant ou des protocoles qui n'ont pas été adoptés par le consortium USB, et ces derniers apparaissent en général en tant que spécifique au fabricant (classe ff).

Classes de périphériques USB refusées par défaut

Les différentes classes de périphériques USB suivantes sont refusées par les règles de stratégie USB par défaut.

- Communications et contrôle CDC (Classes 02 et 0a). La stratégie USB par défaut n'autorise pas ces périphériques, car l'un d'entre eux peut fournir la connexion au bureau virtuel lui-même.
- Périphériques d'interface utilisateur (Classe 03). Comprend un large éventail de périphériques d'entrée et de sortie. Les périphériques d'interface utilisateur (HID) sont composés de claviers, souris, dispositifs de pointage, tablettes graphiques, capteurs, contrôleurs de jeu, boutons et fonctions de contrôle.

  La sous-classe 01 est appelée classe « interface de démarrage » ; elle est utilisée pour les claviers et les souris.

  La stratégie USB par défaut n'autorise ni les claviers USB (classe 03, sous-classe 01, protocole 1), ni les souris USB (classe 03, sous-classe 01, protocole 2). Ceci est dû au fait que la majorité des claviers et souris sont correctement gérés sans prise en charge USB et il est normalement nécessaire d'utiliser ces périphériques localement ainsi qu'à distance lors de la connexion à un bureau virtuel.
- Concentrateurs USB (Classe 09). Les concentrateurs USB permettent de connecter des périphériques supplémentaires à l'ordinateur local. Il n'est pas nécessaire d'accéder à ces périphériques à distance.
- Carte à puce (Classe 0b). Les lecteurs de carte à puce comprennent des lecteurs de carte à puce avec ou sans contact, ainsi que des jetons USB dotés d'une puce équivalente à une carte à puce.

  L'accès distant par carte à puce est utilisé pour accéder aux lecteurs de carte à puce et la prise en charge USB n'est pas nécessaire.
- Contrôleur sans fil (Classe e0). Certains de ces appareils peuvent fournir un accès réseau critique ou connecter des périphériques critiques tels que des claviers ou des souris Bluetooth.

La stratégie USB par défaut n'autorise pas ces appareils. Toutefois, il peut être utile pour certains appareils de fournir l'accès à l'aide de la prise en charge USB.

- **Divers périphériques réseau (classe ef, sous-classe 04)** - Certains de ces appareils peuvent fournir un accès réseau critique. La stratégie USB par défaut n'autorise pas ces appareils. Toutefois, il peut être utile pour certains appareils de fournir l'accès à l'aide de la prise en charge USB.

Mise à jour de la liste des périphériques USB disponibles pour l'accès à distance

Vous pouvez mettre à jour la liste des périphériques USB disponibles pour l'envoi vers des bureaux en modifiant le fichier de modèle Citrix Workspace pour Windows. Cela vous permet d'apporter des modifications à Citrix Workspace pour Windows via une stratégie de groupe. Le fichier se trouve dans le dossier suivant :

```
\C:\Program Files\Citrix\ICA Client\Configuration\en
```

Vous pouvez également modifier le registre sur chaque machine utilisateur en ajoutant la clé de registre suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Name="DeviceRules" Value=

> **Important**
>
> La modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter de réinstaller votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Les règles par défaut du produit sont stockées dans :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB Type=MultiSz Name="DeviceRules" Value=

Ne modifiez pas les règles par défaut du produit.

Pour plus d'informations sur les paramètres de stratégie Périphériques USB, consultez Paramètres de stratégie Périphériques USB dans la documentation de Citrix Virtual Apps and Desktops.

Configuration de l'audio USB

> **Remarque :**
>
> - Lorsque vous mettez à niveau ou installez l'application Citrix Workspace pour Windows pour la première fois, ajoutez les derniers fichiers de modèle à l'objet de stratégie de groupe

> local. Pour plus d'informations sur l'ajout des fichiers de modèle à l'objet de stratégie de groupe local, consultez la section Modèle d'administration d'objet de stratégie de groupe. En cas de mise à niveau, les paramètres existants sont conservés lors de l'importation des derniers fichiers.
> - Cette fonctionnalité est disponible uniquement sur le serveur Citrix Virtual Apps.

Pour configurer des périphériques audio USB :

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Workspace> Expérience utilisateur** et sélectionnez **Audio via la redirection USB générique**.
3. Modifiez les paramètres.
4. Cliquez sur **Appliquer**, puis sur **OK**.
5. Ouvrez l'invite de commande en mode administrateur.
6. Exécutez la commande suivante
   `gpupdate /force`.

Lancement de vPrefer

Dans les versions antérieures, l'instance d'une application installée sur le VDA (appelée instance locale dans ce document) pouvait être lancée de préférence à l'application publiée en définissant l'attribut KEYWORDS:prefer = "application" dans **Citrix Studio**.

À partir de la version 4.11, dans un scénario double-hop (où l'application Citrix Workspace s'exécute sur le VDA hébergeant votre session), vous pouvez désormais contrôler si l'application Citrix Workspace lance l'instance locale d'une application installée sur le VDA (si disponible en tant qu'application locale) plutôt qu'une instance hébergée de l'application.

vPrefer est disponible sur StoreFront version 3.14 et Citrix Virtual Desktops 7.17 et versions ultérieures.

Lorsque vous lancez l'application, l'application Citrix Workspace lit les données de ressources présentes sur le serveur StoreFront et applique les paramètres en fonction de l'indicateur **vprefer** au moment de l'énumération. L'application Citrix Workspace recherche le chemin d'installation de l'application dans le registre Windows sur le VDA et, s'il est présent, lance l'instance locale de l'application. Sinon, une instance hébergée de l'application est lancée.
Si vous lancez une application qui n'est pas installée sur le VDA, l'application hébergée est lancée. Pour plus d'informations sur la gestion du lancement local sur StoreFront, consultez la section Contrôle du lancement local d'applications sur des bureaux publiés dans la documentation de StoreFront.

Si vous ne voulez pas que l'instance locale de l'application soit lancée sur le VDA, définissez **LocalLaunchDisabled** sur **True** à l'aide de PowerShell sur Delivery Controller.

Cette fonctionnalité permet de lancer des applications plus rapidement, offrant ainsi une meilleure expérience utilisateur. Vous pouvez configurer cette fonctionnalité avec le modèle d'administration d'objet de stratégie de groupe. Par défaut, vPrefer est activé uniquement dans un scénario double-hop.

> **Remarque :**
>
> Lorsque vous mettez à niveau ou installez l'application Citrix Workspace pour la première fois, ajoutez les derniers fichiers de modèle à l'objet de stratégie de groupe local. Pour plus d'informations sur l'ajout des fichiers de modèle à l'objet de stratégie de groupe local, consultez la section Modèle d'administration d'objet de stratégie de groupe. En cas de mise à niveau, les paramètres existants sont conservés lors de l'importation des derniers fichiers.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Libre-service**.
3. Sélectionnez la stratégie **vPrefer**.
4. Sélectionnez **Activé** et, à partir du menu déroulant **Autoriser applications**, sélectionnez l'une des options suivantes :
   - **Autoriser toutes les applications** : cette option lance l'instance locale de toutes les applications sur le VDA. L'application Citrix Workspace recherche l'application installée (y compris les applications Windows natives telles que le Bloc-notes, la calculatrice, WordPad ou l'invite de commandes) et lance l'application sur le VDA au lieu de l'application hébergée.
   - **Autoriser les applications installées** : cette option lance l'instance locale de l'application installée sur le VDA. Si l'application n'est pas installée sur le VDA, elle lance l'application hébergée. Par défaut, l'option **Autoriser les applications installées** est sélectionnée lorsque la stratégie **vPrefer** est définie sur **Activé**. Cette option exclut les applications natives du système d'exploitation Windows telles que le Bloc-notes, la Calculatrice, etc.
   - **Autoriser les applications réseau** : cette option lance l'instance d'une application publiée sur un réseau partagé.
5. Cliquez sur **Appliquer**, puis sur **OK**.
6. Redémarrez la session pour que les modifications prennent effet.

Limitation :

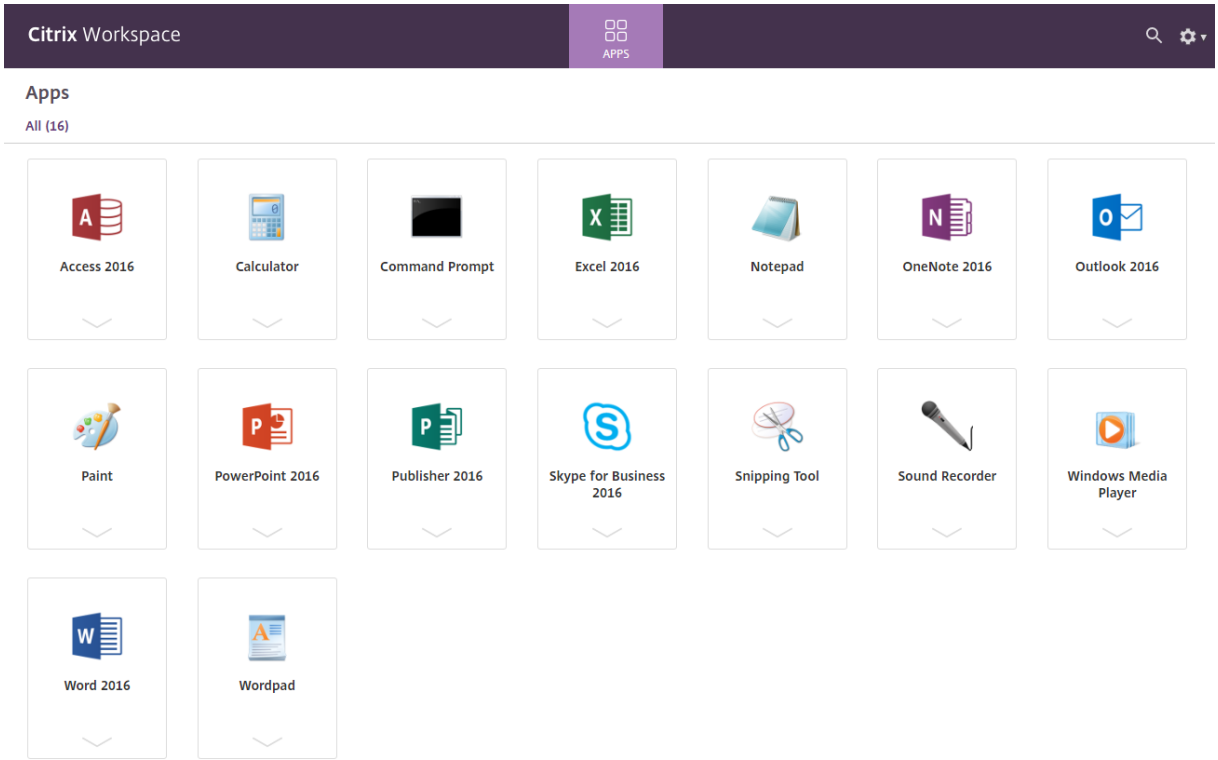
- Workspace pour Web ne prend pas en charge cette fonctionnalité.

Configuration de l'espace de travail

L'application Citrix Workspace pour Windows prend en charge la configuration d'espaces de travail pour les abonnés, qui peuvent utiliser un ou plusieurs services disponibles depuis Citrix Cloud.

L'application Citrix Workspace affiche uniquement les ressources d'espace de travail spécifiques auxquelles les utilisateurs sont autorisés à accéder. Toutes les ressources de votre espace de travail numérique disponibles dans l'application Citrix Workspace sont fournies par le service d'expérience de Citrix Cloud Workspace.

Un espace de travail fait partie d'une solution d'espace de travail numérique qui permet au service informatique de fournir de manière sécurisée l'accès aux applications à partir de n'importe quel appareil.
Cette capture d'écran est un exemple de ce que l'expérience de l'espace de travail ressemble pour vos abonnés. Cette interface évolue et peut différer de celle avec laquelle vos abonnés travaillent aujourd'hui. Par exemple, elle peut indiquer « StoreFront » en haut de la page au lieu de « Espace de travail ».



Intégration de Content Collaboration Service dans l'application Citrix Workspace

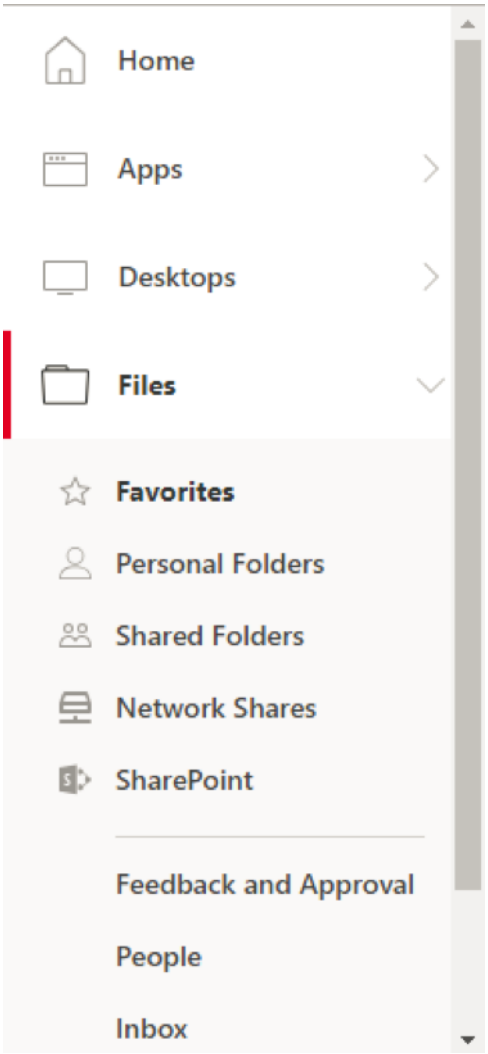
Cette version intègre Citrix Content Collaboration Service à l'application Citrix Workspace. Citrix Content Collaboration vous permet d'échanger des documents facilement et en toute sécurité, d'envoyer

des documents volumineux par courrier électronique, de gérer en toute sécurité les transferts de documents à des tiers et d'accéder à un espace de collaboration. Citrix Content Collaboration met à votre disposition plusieurs façons de travailler, notamment une interface Web, des clients mobiles, des applications de bureau et une intégration avec Microsoft Outlook et Gmail.

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

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

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



Limitations :

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

Configurer l'emplacement de téléchargement des fichiers Citrix à l'aide de l'Éditeur du Registre :

1. Lancez l'Éditeur du Registre et naviguez jusqu'à `HKEY_CURRENT_USER\Software\Citrix\Dazzle\`.
2. Créez une clé de valeur de chaîne nommée **DownloadPreference**.
3. Copiez et collez le chemin de téléchargement préféré pour les fichiers Citrix dans la colonne de valeur.
4. Si vous souhaitez afficher une invite pour chaque téléchargement, définissez la colonne de

valeur sur *.

Pour plus d'informations sur la configuration de l'emplacement de téléchargement des fichiers Citrix à l'aide de la boîte de dialogue **Préférences avancés**, consultez la section Configuration de l'emplacement de téléchargement à l'aide des préférences avancées dans la documentation d'aide de l'application Citrix Workspace pour Windows.

Applications SaaS dans l'application Citrix Workspace

L'accès sécurisé aux applications SaaS assure une expérience utilisateur unifiée qui met des applications SaaS publiées à la disposition des utilisateurs. Les applications SaaS sont disponibles avec Single Sign-on. Les administrateurs peuvent à présent protéger le réseau de l'organisation et les machines des utilisateurs finaux contre les logiciels malveillants et les fuites de données en filtrant l'accès à des sites Web et des catégories de sites Web spécifiques.

L'application Citrix Workspace pour Windows prend en charge l'utilisation d'applications SaaS avec le service de contrôle d'accès. Le service permet aux administrateurs d'offrir une expérience homogène, intégrant Single Sign-on, et l'inspection du contenu.

La mise à disposition d'applications SaaS depuis le cloud présente les avantages suivants :

- Configuration simple : simplicité d'exploitation, de mise à jour et d'utilisation.
- Single Sign-on : ouverture de session sans problème avec Single Sign-on.
- Modèle standard pour différentes applications : configuration d'applications populaires basée sur un modèle.

Conditions préalables :

- L'application SaaS doit prendre en charge l'authentification SAML 2.0 pour pouvoir appliquer la fonctionnalité Single Sign-on.
- L'option **Activer la sécurité renforcée** doit être activée dans le service de contrôle d'accès pour que le navigateur Citrix Workspace soit utilisé lors de la restitution d'une application SaaS. Si cette option n'est pas activée, les applications SaaS sont lancées à l'aide du navigateur par défaut défini sur le client.

> **Remarque :**
>
> L'application Citrix Workspace regroupe les applications, bureaux et fichiers publiés depuis des environnements locaux et de cloud pour une expérience utilisateur unifiée.

L'application Citrix Workspace inclut un navigateur Citrix Secure Browser intégré pour le lancement des applications SaaS. L'infrastructure incorporée Chromium sur laquelle Citrix Secure Browser est construit est à la version 70. Il en résulte une meilleure expérience utilisateur lors de l'accès aux applications SaaS sécurisées.

> **Remarque :**
>
> - Si vous utilisez Workspace pour Web, les applications SaaS sont lancées uniquement dans le navigateur par défaut défini sur le client et non dans le navigateur Citrix Secure Browser.
> - L'expérience utilisateur peut varier entre une application de session ICA et une application SaaS sécurisée.

Le navigateur Citrix Secure Browser prend en charge les opérations telles que celles relatives à la barre d'outils, au Presse-papiers, à l'impression, au téléchargement et aux filigranes. Ces opérations sont exécutées dans les applications Citrix Workspace comme défini dans la configuration de stratégie dans le service de contrôle d'accès.

Opérations disponibles depuis le navigateur Citrix Secure Browser :

Barre d'outils : lorsque l'option de barre d'outils est activée pour une application, vous pouvez accéder aux options Précédent, Suivant et Actualiser dans l'application lancée. La barre d'outils affiche également des points de suspension qui permettent d'accéder aux opérations relatives au Presse-papiers.

Presse-papiers : lorsque l'accès au Presse-papiers est activé pour une application, vous pouvez utiliser les options Couper, Copier et Coller disponibles dans la barre d'outils de l'application lancée. Lorsque l'accès est désactivé, ces options sont grisées.

Impression : vous pouvez exécuter une commande d'impression dans l'application lancée si l'option d'impression est activée. Lorsqu'elle est désactivée, l'option d'impression ne s'affiche pas dans l'application lancée.

Navigation : les icônes Suivant et Précédent sont disponibles dans la barre d'outils de l'application lancée lorsque l'option de navigation est activée.

Téléchargement : vous pouvez télécharger des fichiers depuis l'application lancée lorsque l'option de téléchargement est activée. Cliquez avec le bouton droit de la souris sur l'application lancée et sélectionnez **Enregistrer sous**. Accédez à l'emplacement souhaité et cliquez sur **Télécharger**.

> **Remarque :**
>
> Lorsque vous téléchargez un fichier, aucune barre de progression ne s'affiche pour indiquer le statut du téléchargement. Le téléchargement se déroule cependant correctement.

Filigranes : lorsque l'option de filigrane est activée, un filigrane contenant le nom d'utilisateur et l'adresse IP de la machine cliente s'affiche dans l'application lancée. Le filigrane est semi-transparent et ne peut pas être modifié pour afficher d'autres informations.

Limitations :

1. Lorsque vous lancez une application publiée avec l'option d'impression activée et l'option de téléchargement désactivée et que vous lancez une commande d'impression sur une application lancée, il est possible que l'enregistrement du PDF soit accessible même si la fonctionnalité de

téléchargement est restreinte. Pour remédier à ce problème, vous pouvez désactiver l'option d'impression afin de désactiver la fonctionnalité de téléchargement.
2. Il est possible que les vidéos intégrées à une application ne fonctionnent pas.

Pour plus d'informations sur la configuration de l'espace de travail, consultez la section Configuration de l'espace de travail dans Citrix Cloud.

Pour plus d'informations sur la configuration d'applications SaaS à l'aide des services de contrôle d'accès, reportez-vous à la documentation sur le contrôle d'accès.

Impression PDF

Conditions préalables :

- Application Citrix Workspace version 1808 ou ultérieure
- Citrix Virtual Apps and Desktops version 7 1808 ou ultérieure
- Au moins une visionneuse de PDF installée sur votre ordinateur

Pour activer l'impression PDF :

1. Sur le Delivery Controller, utilisez Citrix Studio pour sélectionner le nœud **Stratégie** dans le volet gauche. Vous pouvez créer une stratégie ou modifier une stratégie existante.
2. Définissez le paramètre de stratégie **Créer automatiquement l'imprimante universelle PDF** sur Activé.

Redémarrez la session de l'application Citrix Workspace pour que les modifications prennent effet.

Limitation :

- L'affichage et l'impression PDF ne sont pas pris en charge sur le navigateur Microsoft Edge.

Mode tablette étendue dans Windows 10 avec Windows Continuum

Windows Continuum est une fonctionnalité de Windows 10 qui s'adapte à la manière dont la machine cliente est utilisée. L'application Citrix Workspace pour Windows version 4.10 prend en charge Windows Continuum, y compris le changement dynamique des modes.

Sur les appareils tactiles, le VDA Windows 10 est lancé en mode Tablette lorsqu'aucune souris ou aucun clavier n'est connecté. Il démarre en mode bureau lorsqu'un clavier ou une souris ou les deux sont connectés. Détacher ou attacher le clavier sur un périphérique client ou l'écran sur un appareil 2 en 1, comme Surface Pro, fait basculer entre les modes tablette et bureau. Pour de plus amples informations, consultez Mode tablette pour appareils à écran tactile dans la documentation de Citrix Virtual Apps and Desktops.

Le VDA Windows 10 détecte la présence d'un clavier ou d'une souris sur un périphérique client tactile lorsque vous vous connectez ou que vous vous reconnectez à une session. Il détecte également

lorsque vous connectez ou déconnectez un clavier ou une souris pendant la session. Par défaut, cette fonction est activée sur le VDA. Pour désactiver la fonctionnalité, modifiez la stratégie **Basculer en mode tablette** à l'aide de Citrix Studio.

Le mode tablette offre une interface utilisateur qui est mieux adaptée aux écrans tactiles :

- Boutons légèrement plus grands.
- L'écran de **démarrage** et toutes les applications que vous démarrez s'ouvrent en mode plein écran.
- La barre des tâches contient un bouton Précédent.
- Les icônes sont retirées de la barre des tâches.

Le mode bureau offre l'interface utilisateur traditionnelle où vous interagissez de la même manière que sur un PC avec un clavier et une souris.

> **Remarque :**
>
> Workspace pour Web ne prend pas en charge la fonctionnalité Windows Continuum.

Pour plus d'informations, veuillez consulter
Notes de publication sur XenServer 7.2

Souris relative

La prise en charge d'une souris relative fournit une option qui permet d'interpréter la position de la souris de manière relative plutôt qu'absolue. Cette capacité est requise par les applications qui exigent des entrées de souris relatives plutôt qu'absolues.

> **Remarque**
>
> Cette fonctionnalité peut uniquement être appliquée à une session de bureau publié.

La configuration de la fonctionnalité à l'aide de l'Éditeur du Registre ou du fichier default.ica permet au paramètre d'être persistant même après la fin de la session.

Vous pouvez contrôler la disponibilité de la fonctionnalité par utilisateur et par machine à l'aide du Registre comme suit :

Configurer la souris relative à l'aide de l'Éditeur du Registre

Pour configurer la fonctionnalité, définissez les clés de registre suivantes le cas échéant, puis redémarrez la session pour que les modifications prennent effet :

Pour que la fonctionnalité soit disponible par session :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse
```


Pour que la fonctionnalité soit disponible par utilisateur :

`HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse`

```
- Nom : RelativeMouse
- Type : REG_SZ
- Valeur : True
```

> **Remarque :**
>
> - Les valeurs définies dans l'Éditeur du Registre ont priorité sur les paramètres du fichier ICA.
> - Les valeurs définies dans HKEY_LOCAL_MACHINE et HKEY_CURRENT_USER doivent être les mêmes. Différentes valeurs peuvent provoquer des conflits.

Configurer la souris relative à l'aide du fichier default.ica

1. Ouvrez le fichier default.ica qui se trouve généralement sur `C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica` où « site name » est le nom spécifié pour le site lors de sa création. Pour les clients StoreFront, le fichier default.ica figure généralement dans `C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica` où « Storename » est le nom spécifié pour le magasin lors de sa création.
2. Ajoutez une nouvelle clé appelée RelativeMouse dans la section WFClient, dont la valeur est définie sur la même configuration que l'objet JSON.
3. Définissez la valeur selon les besoins :
   - true : pour activer la souris relative
   - false : pour désactiver la souris relative
4. Redémarrez la session pour que les modifications prennent effet.

> **Remarque :**
>
> Les valeurs définies dans l'Éditeur du Registre ont priorité sur les paramètres du fichier ICA.

Activer la souris relative à partir de Desktop Viewer

1. Ouvrez une session sur l'application Citrix Workspace.
2. Lancez une session de bureau publié.
3. À partir de la barre d'outils de Desktop Viewer, sélectionnez **Préférences**.

   La fenêtre Citrix Workspace - Préférences s'affiche.
4. Sélectionnez **Connexions**.
5. Sous **Paramètres de la souris relative**, activez l'option **Utiliser la souris relative**.

6. Cliquez sur **Appliquer**, puis sur **OK**.

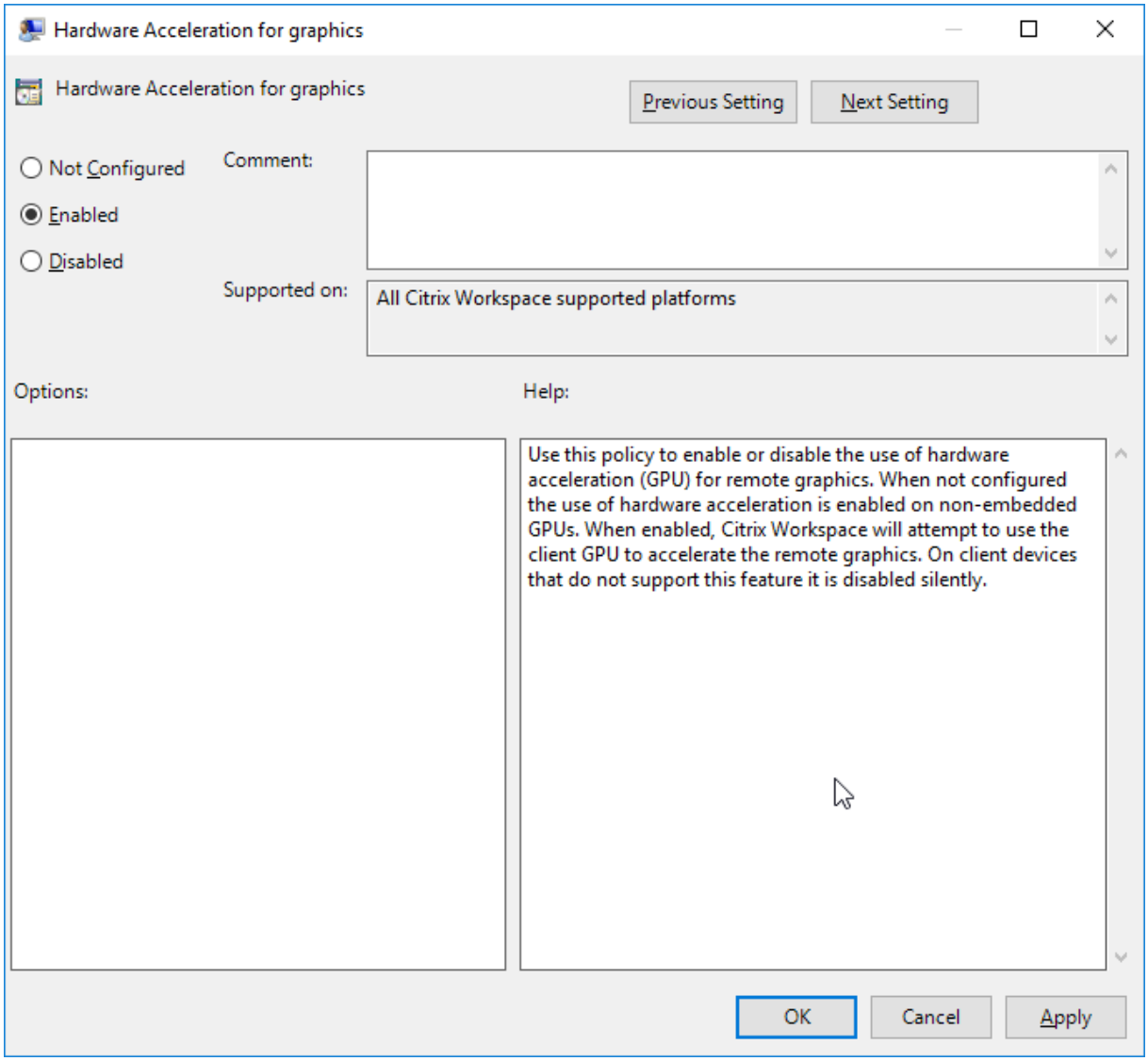
> **Remarque :**
>
> La configuration de la souris relative à partir de Desktop Viewer applique la fonctionnalité à chaque session uniquement.

Décodage matériel

Lors de l'utilisation de l'application Citrix Workspace (avec moteur HDX 14.4), le GPU peut être utilisé pour le décodage H.264 lorsqu'il est disponible sur le client. La couche API d'accélération vidéo DirectX est utilisée pour le décodage GPU.

Pour activer le décodage matériel à l'aide du modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace :

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Citrix Workspace** > **Expérience utilisateur**.
3. Sélectionnez **Accélération matérielle pour graphiques**.
4. Sélectionnez **Activé** et cliquez sur **Appliquer**, puis sur **OK**.



Pour déterminer si la stratégie a été appliquée et si l'accélération matérielle est utilisée pour une session ICA active, recherchez les entrées de registre suivantes :

Chemin du registre : HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender

> **Conseil**
>
> La valeur de **Graphics_GfxRender_Decoder** et **Graphics_GfxRender_Renderer** doit être 2. La valeur 1 indique que le décodage basé sur le processeur est utilisé.

Lors de l'utilisation de la fonctionnalité de décodage matériel, tenez compte des limitations suivantes :

- Si le client est équipé de deux GPU et que l'un des moniteurs est actif sur le second GPU, le décodage sera effectué sur le processeur.
- Lors de la connexion à un serveur Citrix Virtual Apps exécuté sur Windows Server 2008 R2, Citrix

recommande de ne pas utiliser le décodage matériel sur la machine Windows de l'utilisateur. Si cette fonctionnalité est activée, des problèmes tels que la baisse des performances lors de la mise en surbrillance de texte et des problèmes de scintillement peuvent être observés.

Entrée microphone

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

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

Les utilisateurs de l'application Citrix Workspace peuvent indiquer s'ils souhaitent utiliser les microphones connectés à leur appareil à l'aide du Centre de connexion. Les utilisateurs de Citrix Virtual Apps and Desktops peuvent également utiliser les Préférences de Citrix Virtual Apps and Desktops Viewer pour désactiver leurs micros et webcams.

Prise en charge de moniteurs multiples

L'application Citrix Workspace pour Windows permet d'utiliser jusqu'à huit moniteurs.

Chaque écran faisant partie d'une configuration multi-écrans dispose de sa propre résolution conçue par le fabricant. Les écrans peuvent afficher des résolutions et des orientations différentes durant les sessions.

Les sessions peuvent occuper plusieurs écrans de deux façons :

- Mode plein écran, avec écrans multiples affichés dans la session ; les applications s'alignent sur les écrans comme elles le font localement.

  Citrix Virtual Apps and Desktops : pour afficher la fenêtre Desktop Viewer sur n'importe quel sous-ensemble d'écrans, redimensionnez la fenêtre sur ces derniers et cliquez sur **Agrandir**.

- Mode fenêtre, avec une seule image d'écran pour la session ; les applications ne s'alignent pas sur les écrans individuels.

Citrix Virtual Apps and Desktops : lorsqu'un bureau appartenant au même groupe (anciennement « groupe de bureau ») est lancé ultérieurement, le paramètre de fenêtre est conservé et le bureau est affiché sur les mêmes écrans. Plusieurs bureaux virtuels peuvent être affichés sur une machine à condition que la disposition de l'écran soit rectangulaire. Si l'écran principal sur la machine est utilisé par la session Citrix Virtual Apps and Desktops, il devient l'écran principal dans la session. Autrement, l'écran numériquement inférieur dans la session devient l'écran principal.

Pour activer la prise en charge multi-écran, veillez à ce que les conditions suivantes soient réunies :

- La machine utilisateur est configurée pour prendre en charge de multiples écrans.
- Le système d'exploitation de la machine utilisateur doit être en mesure de détecter chaque écran. Sur les plates-formes Windows, pour vérifier que cette détection a lieu, ouvrez la boîte de dialogue **Propriétés d'affichage** et consultez l'onglet **Paramètres** pour confirmer que chaque écran y figure séparément.
- Une fois que vos écrans ont été détectés :
  - **Citrix Virtual Desktops :** configurez la limite de mémoire graphique à l'aide du paramètre de **stratégie d'ordinateur Citrix** Limite de mémoire d'affichage.
  - **Citrix Virtual Apps :** selon la version du serveur Citrix Virtual Apps que vous avez installée :
    * Configurez la limite de mémoire graphique à l'aide du paramètre de **stratégie d'ordinateur Citrix** Limite de mémoire d'affichage.
    * À partir de la console de gestion Citrix du serveur Citrix Virtual Apps, sélectionnez la batterie et dans le panneau des tâches, sélectionnez **Modifier les propriétés de serveur** > Modifier toutes les propriétés > Valeur par défaut du serveur > HDX Broadcast > Affichage (ou Modifier les propriétés de serveur > Modifier toutes les propriétés > Valeur par défaut du serveur > ICA > Affichage) et définissez la Mémoire maximale à utiliser pour les graphiques de chaque session.

Assurez-vous que la valeur du réglage (kilo-octets) permet de fournir une mémoire graphique suffisante. Si ce réglage est insuffisant, la ressource publiée se réduit au sous-ensemble d'écrans correspondant à la taille spécifiée.

Utiliser Citrix Virtual Desktops sur deux moniteurs :

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

   L'écran est maintenant étendu aux deux moniteurs.

Pour plus d'informations sur le calcul des exigences de mémoire graphique de la session pour Citrix Virtual Apps and Desktops, consultez l'article CTX115637 du centre de connaissances.

Imprimante

Pour remplacer les paramètres d'imprimante sur la machine utilisateur

1. À partir du menu **Impression** d'une application disponible sur la machine utilisateur, choisissez **Propriétés**.

2. Sur l'onglet **Paramètres client**, cliquez sur Optimisations avancées et apportez des modifications aux options Compression d'image et Cache d'image et de police.

Commande du clavier à l'écran

Pour activer l'accès tactile aux applications et bureaux virtuels à partir de tablettes Windows, l'application Citrix Workspace affiche automatiquement le clavier à l'écran lorsque vous activez un champ de saisie de texte et lorsque l'appareil est en mode tente ou tablette.

Sur certains appareils et dans certaines circonstances, l'application Citrix Workspace ne parvient pas à détecter avec précision le mode de l'appareil, et le clavier à l'écran peut s'afficher alors que vous ne souhaitez pas qu'il apparaisse.

Pour empêcher le clavier à l'écran d'apparaître lors de l'utilisation d'un appareil convertible, créez une valeur REG_DWORD DisableKeyboardPopup dans HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver et définissez-la sur 1.

> **Remarque :**
>
> Sur une machine x64, créez la valeur dans HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver.

Les 3 modes ci-après peuvent être utilisés pour définir les clés :

- **Automatique** : AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0
- **Toujours afficher** (clavier à l'écran) : AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0
- **Ne jamais afficher** (clavier à l'écran) : AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1

Raccourcis clavier

Vous pouvez configurer des combinaisons de touches auxquelles l'application Citrix Workspace prête des fonctionnalités spéciales. Lorsque la stratégie de raccourcis clavier est activée, vous pouvez spécifier les mappages de touches de raccourci Citrix, le comportement des touches de raccourci Windows et la configuration du clavier pour les sessions.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Expérience utilisateur**.
3. Sélectionnez la stratégie Raccourcis clavier.
4. Sélectionnez **Activé**, puis choisissez les options souhaitées.

5. Redémarrez la session de l'application Citrix Workspace pour que les modifications prennent effet.

Prise en charge des icônes de couleurs 32 bits dans l'application Citrix Workspace :

L'application Citrix Workspace prend en charge les icônes de couleurs 32bits et sélectionne automatiquement le nombre de couleurs des applications visibles dans la boîte de dialogue du **Centre de connexion Citrix**, le menu Démarrer et la barre des tâches pour fournir des applications en toute transparence.

> **Attention**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Pour définir un nombre de couleurs, vous pouvez ajouter une clé de registre de chaîne intitulée TWIDesiredIconColor dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences et la régler à la valeur souhaitée. Le nombre de couleurs possible pour les icônes est de 4, 8, 16, 24 ou 32 bits par pixel. L'utilisateur peut sélectionner un nombre moindre de couleurs pour les icônes si le débit de la connexion réseau est faible.

Desktop Viewer

Différentes entreprises ont différents besoins d'entreprise. Votre configuration requise pour la manière dont les utilisateurs accèdent aux bureaux virtuels d'un utilisateur à un autre et peut varier lorsque vos besoins sont en constante évolution. L'expérience utilisateur relative à la connexion aux bureaux virtuels et le degré d'intervention de l'utilisateur dans la configuration des connexions dépendent de la manière dont vous avez configuré l'application Citrix Workspace pour Windows.

Utilisez **Desktop Viewer** lorsque vos utilisateurs doivent interagir avec leur bureau virtuel. Le bureau virtuel de l'utilisateur peut être un bureau virtuel publié ou un bureau dédié ou partagé. Dans ce scénario d'accès, la barre d'outils Desktop Viewer permet à l'utilisateur d'ouvrir un bureau virtuel dans une fenêtre et de faire défiler et mettre à l'échelle ce bureau au sein de son bureau local. Les utilisateurs peuvent définir des préférences et travailler avec plusieurs bureaux à l'aide de connexions Citrix Virtual Apps and Desktops multiples sur la même machine utilisateur.

> **Remarque :**
>
> utilisez l'application Citrix Workspace pour changer la résolution d'écran sur les bureaux virtuels. Vous ne pouvez pas changer la résolution d'écran à l'aide du Panneau de configuration de Windows.

Entrées clavier dans Desktop Viewer

Dans les sessions Desktop Viewer, la touche **Windows**+L est dirigée vers l'ordinateur local.

Ctrl+Alt+Suppr est dirigé vers l'ordinateur local.

Les touches qui activent les touches rémanentes, les touches filtres et les touches bascules (fonctionnalités d'accessibilité Microsoft) sont généralement dirigées vers l'ordinateur local.

En tant que fonctionnalité d'accessibilité de Desktop Viewer, la combinaison Ctrl+Alt+Attn affiche les boutons de la barre d'outils Desktop Viewer dans une fenêtre contextuelle.

Ctrl+Échap est envoyé au bureau virtuel distant.

> **Remarque :**
>
> Par défaut, si Desktop Viewer est agrandi, Alt+Tab bascule le focus entre les différentes fenêtres au sein de la session. Si Desktop Viewer est affiché dans une fenêtre, Alt+Tab active le focus entre les différentes fenêtres en dehors de la session.

Les séquences de raccourcis sont des combinaisons de touches conçues par Citrix. À titre d'exemple, la séquence Ctrl+F1 reproduit Ctrl+Alt+Suppr, et Maj+F2 permet de basculer les applications du mode plein écran au mode fenêtre, et vice versa. Vous ne pouvez pas utiliser de séquences de raccourcis avec des bureaux virtuels affichés dans Desktop Viewer (c'est-à-dire avec des sessions Citrix Virtual Apps and Desktops), mais vous pouvez les utiliser avec des applications publiées (c'est-à-dire avec des sessions Citrix Virtual Apps).

Bureaux virtuels

Depuis une session de bureau, les utilisateurs ne peuvent pas se connecter au même bureau virtuel. Une tentative de connexion déconnectera la session de bureau existante. C'est pourquoi Citrix recommande ce qui suit :

- Les administrateurs ne devraient pas configurer les clients sur un bureau afin de pointer vers un site qui publie le même bureau
- Les utilisateurs ne devraient pas effectuer une recherche vers un site qui héberge le même bureau, si le site est configuré pour reconnecter automatiquement les utilisateurs à des sessions existantes
- Les utilisateurs ne devraient pas effectuer une recherche vers un site qui héberge le même bureau et essayer de le démarrer

Rappelez-vous qu'un utilisateur qui ouvre une session localement sur un ordinateur agissant en tant que bureau virtuel bloque les connexions à ce bureau.

Si vos utilisateurs se connectent à des applications virtuelles (publiées avec Citrix Virtual Apps) depuis un bureau virtuel et que votre organisation possède un administrateur Citrix Virtual Apps distinct, Cit-

rix recommande de travailler en collaboration avec ces derniers pour définir le mappage de machines de sorte que les machines de bureaux soient mappées de façon cohérente dans les sessions de bureau et d'application. Les lecteurs locaux étant affichés en tant que lecteurs réseau dans les sessions de bureau, l'administrateur Citrix Virtual Apps doit changer la stratégie de mappage de lecteur afin d'inclure les lecteurs réseau.

Délai de l'indicateur d'état

Vous pouvez modifier la durée pendant laquelle l'indicateur d'état s'affiche lorsqu'un utilisateur lance une session. Pour modifier cette durée, créez une valeur REG_DWORD de SI INACTIVE MS dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\. La valeur REG_DWORD peut être réglée sur 4 si vous voulez que l'indicateur d'état disparaisse plus tôt.

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

Le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) rassemble des données de configuration et d'utilisation anonymes à partir de l'application Citrix Workspace et les envoie automatiquement à Citrix. Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de Citrix Workspace.

Le programme CEIP ne collecte aucune information liée à l'environnement du client permettant d'identifier l'utilisateur.

> **Conseil**
>
> Vous pouvez choisir de participer ou non au programme CEIP dans l'application Citrix Workspace. Vous avez sept jours pour désactiver le programme après l'installation.

Pour désactiver le programme CEIP ou ne pas y participer :

> **Remarque :**
>
> Vous pouvez masquer partiellement ou totalement la page Préférences avancées disponible à partir de l'icône de l'application Citrix Workspace dans la zone de notification. Pour plus d'informations, veuillez consulter l'article Page Préférences avancées.

1. Cliquez avec le bouton droit de la souris sur l'icône de l'application Citrix Workspace dans la zone de notification.
2. Sélectionnez **Préférences avancées**.
   La fenêtre **Préférences avancées** s'affiche.
3. Sélectionnez **Collecte de données**.
4. Sélectionnez **Non merci** pour désactiver le programme CEIP ou ne pas y participer.
5. Cliquez sur **Enregistrer**.

Authentification

March 18, 2019

Pour maximiser la sécurité de votre environnement, les connexions entre l'application Citrix Workspace et les ressources que vous publiez doivent être protégées. Vous pouvez configurer plusieurs types d'authentification pour votre application Citrix Workspace, y compris l'authentification pass-through au domaine, par carte à puce et pass-through Kerberos.

Authentification pass-through au domaine

Single Sign-on vous permet de vous authentifier auprès d'un domaine et d'utiliser Citrix Virtual Apps and Desktops sans procéder à une nouvelle authentification.

Lorsque vous ouvrez une session sur l'application Citrix Workspace, vos informations d'identification sont transmises à StoreFront avec les applications et bureaux énumérés et les paramètres du menu Démarrer. Après avoir configuré Single Sign-on, vous pouvez ouvrir une session sur l'application Citrix Workspace et lancer des sessions Citrix Virtual Apps and Desktops sans ressaisir vos informations d'identification.

> **Remarque :**
>
> Single Sign-On n'est pas pris en charge si l'application Citrix Workspace est connectée à Citrix Virtual Apps and Desktops à l'aide de Citrix Gateway.

Vous pouvez configurer l'authentification Single Sign-On lors d'une nouvelle installation ou d'une mise à niveau, à l'aide de l'une des options suivantes :

- Interface de ligne de commande
- Interface utilisateur graphique

Configurer l'authentification Single Sign-On lors d'une nouvelle installation

Procédez comme suit pour configurer l'authentification Single Sign-On lors d'une nouvelle installation de l'application Citrix Workspace :

1. Configuration sur StoreFront ou l'interface Web.
2. Configurez les services d'approbation XML sur le Delivery Controller.
3. Modifiez les paramètres d'Internet Explorer.
4. Installez l'application Citrix Workspace avec Single Sign-On.

Configurer Single Sign-On sur StoreFront ou l'interface Web

Selon le déploiement Citrix Virtual Apps and Desktops, l'authentification Single Sign-On peut être configurée sur StoreFront ou l'interface Web à l'aide de la console de gestion.

Utilisez le tableau ci-dessous pour différents cas d'utilisation et la configuration associée :

Cas d'utilisation	Détails de la configuration	Informations supplémentaires
SSON configuré sur StoreFront ou l'interface Web	Lancez Citrix Studio, accédez à **Magasin** > **Gérer les méthodes d'authentification** > activez **Authentification pass-through au domaine**.	Lorsque l'application Citrix Workspace n'est pas configurée avec Single Sign-On, elle change automatiquement la méthode d'authentification de **Authentification pass-through au domaine** vers **Nom d'utilisateur et mot de passe**, le cas échéant.
Lorsque Workspace pour Web est requis	Lancez **Magasin** > **Workspace pour Web** > **Gérer les méthodes d'authentification** > activez **Authentification pass-through au domaine**.	Lorsque l'application Citrix Workspace n'est pas configurée avec Single Sign-On, elle change automatiquement la méthode d'authentification de l'authentification pass-through au domaine vers Nom d'utilisateur et mot de passe, le cas échéant.
Lorsque StoreFront n'est pas configuré	Si l'interface Web est configurée sur un serveur Citrix Virtual Apps and Desktops, lancez le site XenApp Services > **Méthodes d'authentification** > activez **Pass-through**.	Lorsque l'application Citrix Workspace n'est pas configurée avec Single Sign-On, elle change automatiquement la méthode d'authentification de **Pass-through** vers **Explicite**, le cas échéant.

Configurer Single Sign-on avec Citrix Gateway

Vous pouvez activer Single Sign-On avec Citrix Gateway via le modèle d'administration d'objet de stratégie de groupe.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Authentification utilisateur**.
3. Sélectionnez la stratégie **Single Sign-on pour Citrix Gateway**.
4. Sélectionnez **Activé**.
5. Cliquez sur **Appliquer**, puis sur **OK**.
6. Redémarrez l'application Citrix Workspace pour que les modifications prennent effet.

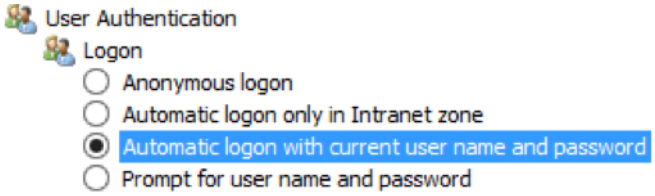
Configurer les services d'approbation XML sur le Delivery Controller

Sur Citrix Virtual Apps and Desktops, exécutez la commande PowerShell suivante en tant qu'administrateur sur le Delivery Controller :

```
asnp Citrix* Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True
```

Modifier les paramètres d'Internet Explorer

1. Ajoutez le serveur StoreFront à la liste de sites de confiance à l'aide d'Internet Explorer. Pour ce faire :
    a) Démarrez Internet Explorer.
    b) Sélectionnez **Outils** > **Options Internet** > **Sécurité** > **Internet Local** et cliquez sur **Sites**. La fenêtre **Intranet Local** s'affiche.
    c) Sélectionnez **Avancé**.
    d) Ajoutez l'adresse URL de StoreFront ou le nom de domaine complet de l'Interface Web avec les protocoles HTTP ou HTTPS appropriés.
    e) Cliquez sur **Appliquer, puis sur OK**.
2. Modifiez les paramètres **Authentification utilisateur** dans **Internet Explorer**. Pour ce faire :
    a) Démarrez Internet Explorer.
    b) Dans **Options Internet** > **Sécurité**, sélectionnez **Sites de confiance**.
    c) Cliquez sur **Personnaliser le niveau**. La fenêtre **Paramètres de sécurité – Zone Sites de confiance** s'affiche.
    d) Dans le panneau **Authentification utilisateur**, sélectionnez **Ouverture de session automatique avec le nom d'utilisateur et le mot de passe actuel**.



Configurer Single Sign-on à l'aide de l'interface de ligne de commande

Installez l'application Citrix Workspace pour Windows avec le commutateur `/includeSSON` et redémarrez-la pour que les modifications prennent effet.

> **Remarque :**
>
> Si l'application Citrix Workspace pour Windows a été installée sans le composant Single Sign-on, la mise à niveau vers la dernière version de l'application Citrix Workspace avec le commutateur `/includeSSON` n'est pas prise en charge.

Configurer Single Sign-on à l'aide de l'interface utilisateur graphique

1. Accédez au fichier d'installation de l'application Citrix Workspace (CitrixWorkspaceApp.exe).
2. Cliquez deux fois sur `CitrixWorkspaceApp.exe` pour lancer le programme d'installation.
3. Dans l'assistant d'installation **Activer l'authentification unique**, sélectionnez l'option **Activer l'authentification unique**.
4. Cliquez sur **Suivant** pour terminer l'installation.

Vous pouvez maintenant vous connecter à un magasin existant (ou configurer un nouveau magasin) à l'aide de l'application Citrix Workspace sans fournir d'informations d'identification utilisateur.

Configurer Single Sign-on sur Citrix Workspace pour Web

Vous pouvez configurer Single Sign-on sur Workspace pour Web à l'aide du modèle d'administration d'objet de stratégie de groupe.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de Workspace pour Web en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Workspace pour Windows** > **Authentification utilisateur**.
3. Sélectionnez la stratégie **Nom d'utilisateur et mot de passe locaux** et définissez-la sur **Activé**.
4. Cliquez sur **Activer l'authentification pass-through**. Cette option permet à Workspace pour Web d'utiliser vos informations d'identification d'ouverture de session pour l'authentification sur le serveur distant.

5. Cliquez sur **Autoriser l'authentification pass-through pour toutes les connexions ICA**. Cette option ignore toute restriction d'authentification et autorise le transfert des informations d'identification sur toutes les connexions.
6. Cliquez sur **Appliquer**, puis sur **OK**.
7. Redémarrez Workspace pour Web pour que les modifications prennent effet.

Vérifiez que Single Sign-on est activé. Pour cela, démarrez le **gestionnaire des tâches** et vérifiez si le processus `ssonsvr.exe` est en cours d'exécution.

Configurer Single Sign-on à l'aide d'Active Directory

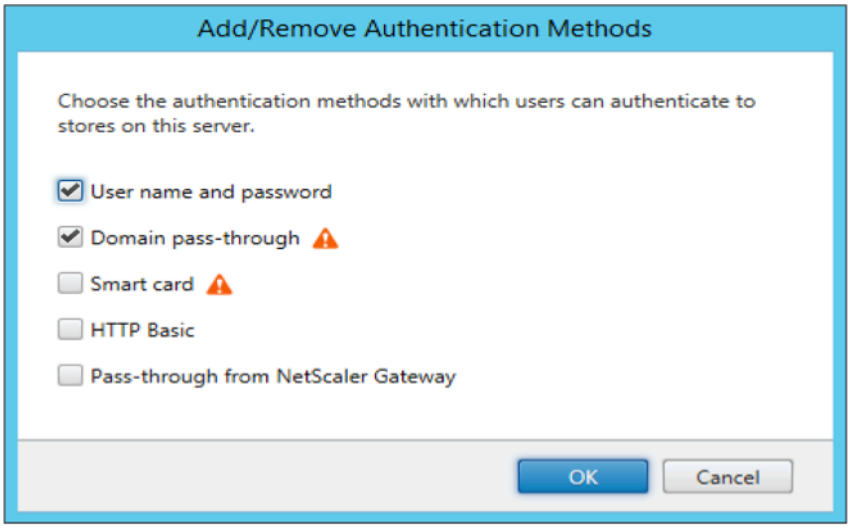
Procédez comme suit pour configurer l'application Citrix Workspace pour l'authentification pass-through à l'aide de la stratégie de groupe Active Directory. Dans ce scénario, vous pouvez obtenir l'authentification Single Sign-on sans utiliser les outils de déploiement de logiciels d'entreprise, tels que Microsoft System Center Configuration Manager.

1. Téléchargez et placez le fichier d'installation de l'application Citrix Workspace (CitrixWorkspaceApp.exe) sur un partage réseau approprié. Il doit être accessible par les machines cibles sur lesquelles vous installez l'application Citrix Workspace.
2. Obtenez le `CheckAndDeployWorkspacePerMachineStartupScript.bat`modèle à partir de la page Téléchargement de l'application Citrix Workspace pour Windows.
3. Modifiez le contenu pour refléter l'emplacement et la version de `CitrixWorkspaceApp.exe`.
4. Dans la console **Gestion des stratégies de groupe Active Directory**, entrez `CheckAndDeployWorkspacePe.bat` comme script de démarrage. Pour plus d'informations sur le déploiement des scripts de démarrage, consultez la section Active Directory.
5. Dans le nœud **Configuration ordinateur**, accédez à **Modèles d'administration > Ajout/Suppression de modèles** pour ajouter le fichier `icaclient.adm`.
6. Après avoir ajouté le modèle `icaclient.adm`, accédez à **Configuration ordinateur** > **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Authentification utilisateur**.
7. Sélectionnez la stratégie **Nom d'utilisateur et mot de passe locaux** et définissez-la sur **Activé**.
8. Sélectionnez **Activer l'authentification pass-through** et cliquez sur **Appliquer**.
9. Redémarrez la machine pour que les modifications prennent effet.

Configurer Single Sign-On sur StoreFront et l'interface Web

Configuration du StoreFront

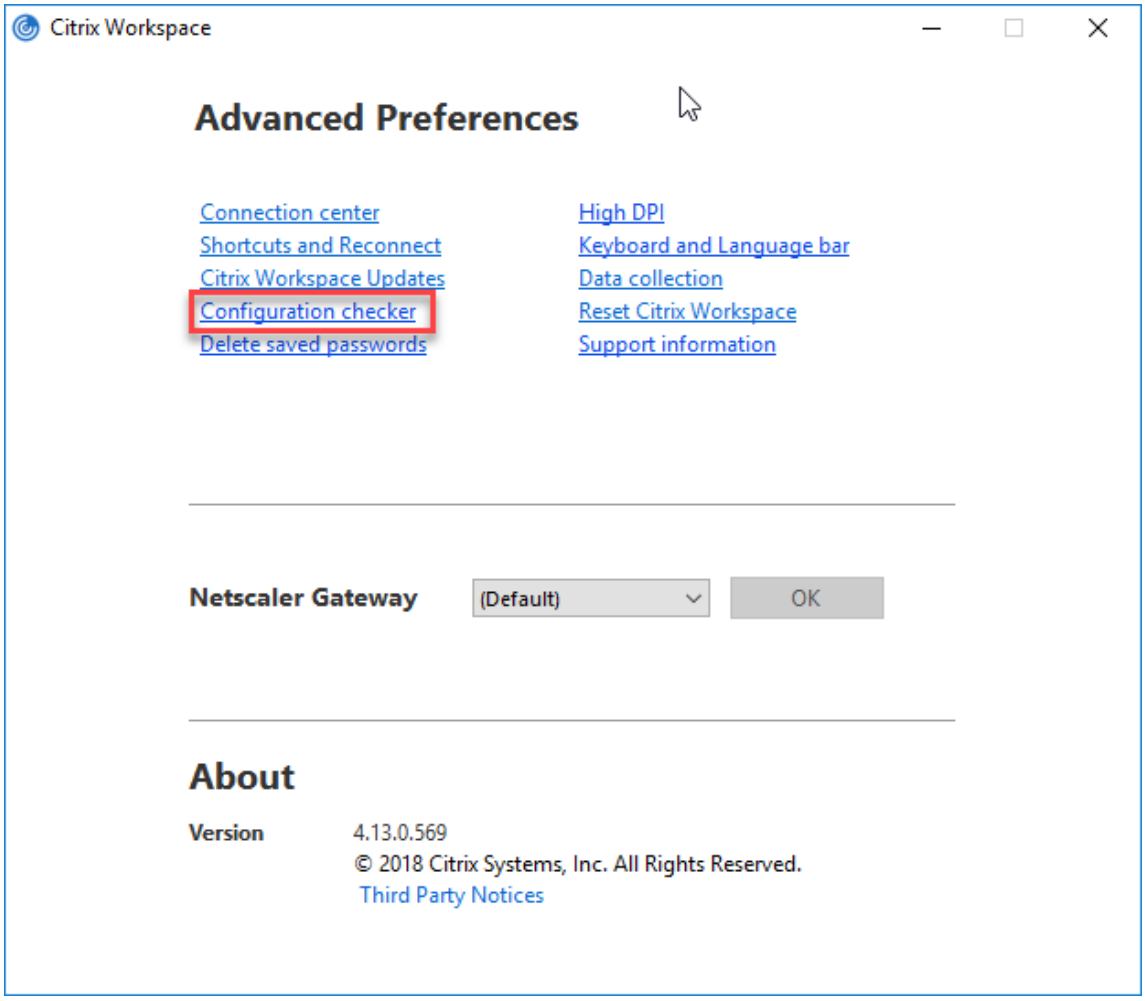
Ouvrez **Citrix Studio** sur le serveur StoreFront et sélectionnez **Authentification -> Ajouter/-supprimer des méthodes d'authentification**. Sélectionnez **Authentification pass-through au domaine**.



Outil d'analyse de la configuration

L'Outil d'analyse de la configuration vous permet d'exécuter un test pour vous assurer que Single Sign-On est correctement configuré. Le test est exécuté sur les différents points de contrôle de la configuration de l'authentification unique et affiche les résultats de la configuration.

1. Cliquez avec le bouton droit de la souris sur l'icône de l'application Citrix Workspace dans la zone de notification et cliquez sur **Préférences avancées**.
   La boîte de dialogue **Préférences avancées** s'affiche.
2. Cliquez sur **Outil d'analyse de la configuration**.
   La fenêtre **Outil d'analyse de la configuration** s'affiche.



3. Sélectionnez **SSONChecker** dans le volet **Sélectionner**.
4. Cliquez sur **Exécuter**. Une barre de progression apparaît, affichant l'état du test.

La fenêtre **Outil d'analyse de la configuration** comporte les colonnes suivantes :

1. **État :** affiche le résultat d'un test sur un point de contrôle.
   - Une coche verte indique que le point de contrôle est correctement configuré.
   - Un I bleu indique des informations sur le point de contrôle.
   - Un X rouge indique que le point de contrôle n'est pas configuré correctement.
2. **Fournisseur :** affiche le nom du module sur lequel le test est exécuté. Dans ce cas, Single Sign-on.
3. **Suite :** indique la catégorie du test. Par exemple, Installation.
4. **Test :** indique le nom du test qui est exécuté.
5. **Détails :** fournit des informations supplémentaires sur le test, indépendamment de la réussite ou de l'échec.

L'utilisateur dispose de plus d'informations sur chaque point de contrôle et les résultats correspondants.

Les tests suivants sont effectués :

1. Installé avec Single Sign-on
2. Capture des informations d'identification d'ouverture de session
3. Enregistrement du fournisseur réseau : le résultat du test pour l'enregistrement du fournisseur de réseau affiche une coche verte uniquement si « Citrix Single Sign-On » est défini en tant que premier élément dans la liste des fournisseurs de réseau. Si Citrix Single Sign-On s'affiche ailleurs dans la liste, le résultat de test pour l'inscription du fournisseur réseau s'affiche avec un I bleu et des informations supplémentaires.
4. Processus de Single Sign-On en cours d'exécution
5. Stratégie de groupe : par défaut, cette stratégie est configurée sur le client.
6. Paramètres Internet pour les zones de sécurité : assurez-vous que vous ajoutez le magasin/l'adresse URL du service XenApp à la liste des zones de sécurité dans les Options Internet.
   Si les zones de sécurité sont configurées via une stratégie de groupe, toute modification de la stratégie requiert que la fenêtre **Préférences avancées** soit rouverte pour que les modifications soient prises en compte et pour afficher l'état correct du test.
7. Méthode d'authentification pour l'Interface Web ou StoreFront.

> **Remarque :**
>
> - Si vous accédez à Workspace pour Web, les résultats du test ne sont pas applicables.
> - Si l'application Citrix Workspace est configurée avec plusieurs magasins, le test de la méthode d'authentification est exécuté sur tous les magasins configurés.
> - Vous pouvez enregistrer les résultats du test sous forme de rapports. Le format par défaut du rapport est .txt.

Masquer l'outil d'analyse de la configuration dans la fenêtre Préférences avancées

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Accédez à **Composants Citrix** > **Workspace pour Windows** > **Libre-service** > **DisableConfigChecker**.
3. Cliquez sur **Activé** pour masquer l'option Outil d'analyse de la configuration dans la fenêtre **Préférences avancées**.
4. Cliquez sur **Appliquer**, puis sur **OK**.
5. Exécutez la commande `gpupdate /force`.

Limitation :

L'outil d'analyse de la configuration ne comprend pas le point de contrôle pour la configuration de

l'option Faire confiance aux requêtes envoyées au service XML sur les serveurs Citrix Virtual Apps and Desktops.

Test de balise

L'application Citrix Workspace vous permet d'effectuer un test de balise à l'aide du contrôleur de balises disponible dans l'**outil d'analyse de la configuration**. Un test de balise permet de vérifier si la balise (ping.citrix.com) est accessible. Ce test de diagnostic permet d'écarter l'une des nombreuses causes possibles d'une énumération lente des données, à savoir l'indisponibilité de la balise. Pour exécuter le test, cliquez avec le bouton droit de la souris sur l'application Citrix Workspace dans la zone de notification et sélectionnez **Préférences avancées** > **Outil d'analyse de la configuration**. Sélectionnez **Contrôleur de balises** dans la liste de tests et cliquez sur **Exécuter**.

Les résultats du test peuvent être les suivants :

- Accessible : la balise peut contacter l'application Citrix Workspace.
- Inaccessible : l'application Citrix Workspace ne peut pas contacter la balise.
- Partiellement accessible : l'application Citrix Workspace peut contacter la balise par intermittence.

> **Remarque :**
>
> - Les résultats du test ne s'appliquent pas à Workspace pour Web.
> - Vous pouvez enregistrer les résultats du test sous forme de rapports. Le format par défaut du rapport est .txt.

Authentification pass-through au domaine avec Kerberos

Cette rubrique s'applique uniquement aux connexions entre l'application Citrix Workspace pour Windows, StoreFront et Citrix Virtual Apps and Desktops.

L'application Citrix Workspace prend en charge l'authentification pass-through au domaine Kerberos pour les déploiements qui utilisent des cartes à puce. Kerberos est l'une des méthodes d'authentification incluses à l'authentification Windows intégrée (IWA).

Lorsque l'authentification Kerberos est activée, Kerberos gère l'authentification sans mots de passe pour l'application Citrix Workspace, ce qui évite les attaques de type cheval de Troie destinées à obtenir les mots de passe sur la machine utilisateur. Les utilisateurs peuvent ouvrir une session avec la méthode d'authentification de leur choix et accéder aux ressources publiées. Par exemple, un système d'authentification biométrique tel qu'un lecteur d'empreinte digitale peut être utilisé.

Lorsque vous vous connectez à l'aide d'une carte à puce à l'application Citrix Workspace, StoreFront et Citrix Virtual Apps and Desktops configurés pour l'authentification par carte à puce, l'application Citrix Workspace effectue les opérations suivantes :

1. capture le code PIN de la carte à puce pendant le processus Single Sign-on ;
2. utilise IWA (Kerberos) pour authentifier l'utilisateur auprès de StoreFront. StoreFront fournit ensuite à l'application Workspace les informations relatives à la disponibilité de Citrix Virtual Apps and Desktops.

   > **Remarque**
   >
   > Activez Kerberos pour éviter l'affichage d'invites de saisie de code PIN supplémentaires. Si vous n'utilisez pas l'authentification Kerberos, l'application Citrix Workspace s'authentifie auprès de StoreFront à l'aide des informations d'identification de la carte à puce.

3. Le moteur HDX (anciennement appelé client ICA) transmet le code PIN de la carte à puce au VDA afin de connecter l'utilisateur à la session de l'application Citrix Workspace. Citrix Virtual Apps and Desktops fournit ensuite les ressources demandées.

Pour utiliser l'authentification Kerberos avec l'application Citrix Workspace, assurez-vous que la configuration de Kerberos respecte les critères suivants.

- Kerberos fonctionne uniquement entre l'application Citrix Workspace et les serveurs appartenant aux mêmes domaines Windows Server ou à des domaines approuvés. Les serveurs doivent également être approuvés pour délégation, une option configurée via l'outil de gestion des utilisateurs et machines Active Directory.
- Kerberos doit être activé sur le domaine et dans Citrix Virtual Apps and Desktops. Pour renforcer la sécurité et vous assurer que Kerberos est utilisé, désactivez toutes les options IWA non Kerberos sur le domaine.
- L'ouverture de session Kerberos n'est pas disponible pour les connexions Services Bureau à distance configurées pour utiliser l'authentification de base, pour toujours utiliser les informations d'ouverture de session spécifiées, ou pour toujours inviter les utilisateurs à entrer un mot de passe.

> **Avertissement**
>
> Une utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux pouvant nécessiter la réinstallation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à sauvegarder le registre avant de le modifier.

Authentification pass-through au domaine avec Kerberos en vue de l'utilisation avec des cartes à puce

Avant de poursuivre, consultez les informations relatives aux cartes à puce dans la section Sécuriser votre déploiement de la documentation Citrix Virtual Apps and Desktops.

Lorsque vous installez l'application Citrix Workspace pour Windows, incluez l'option de ligne de commande suivante :

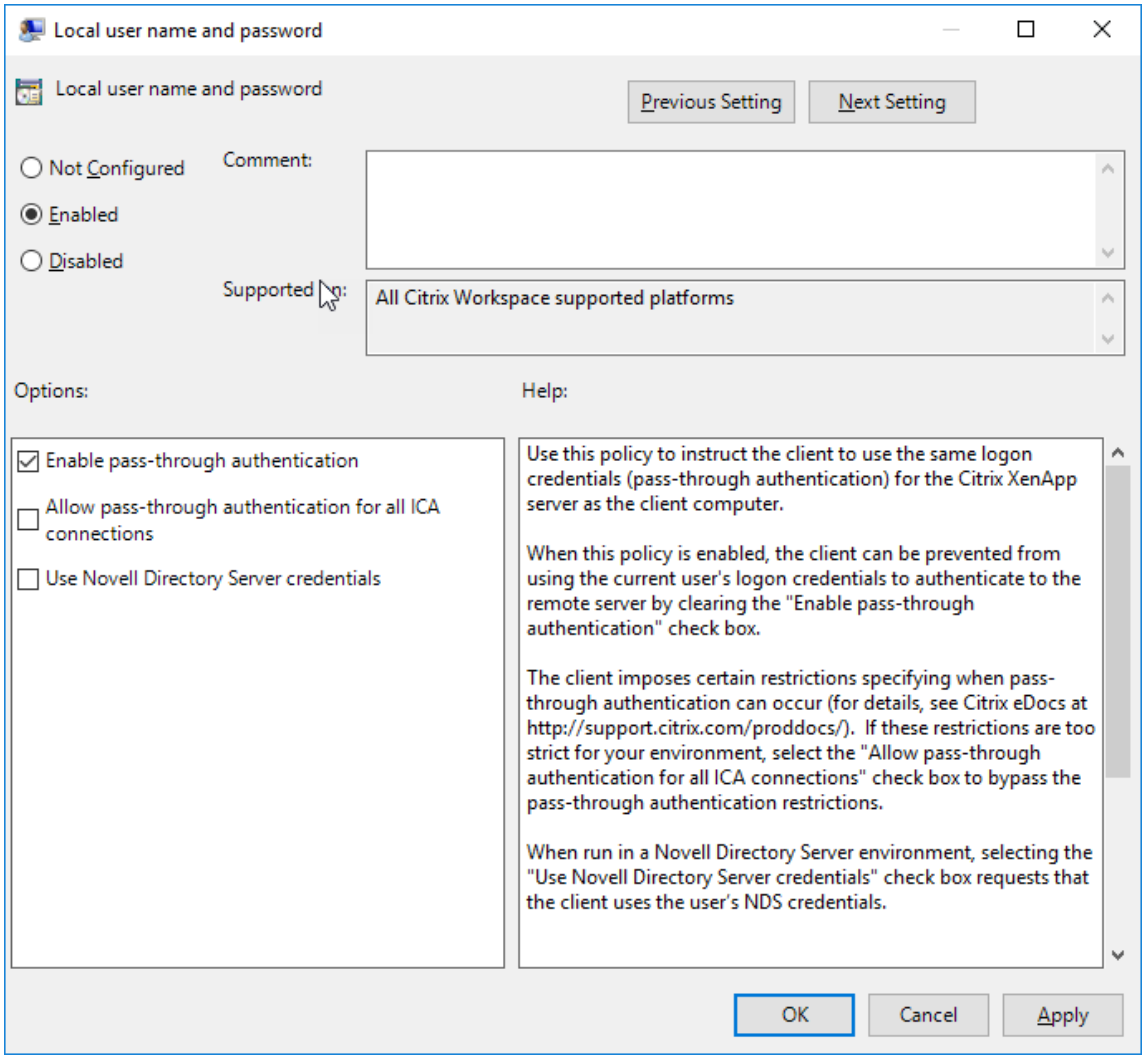
- `/includeSSON`

  Cette option installe le composant Single Sign-on sur l'ordinateur appartenant au domaine, ce qui permet à votre espace de travail de s'authentifier auprès de StoreFront à l'aide de IWA (Kerberos). Le composant Single Sign-on mémorise le code PIN de la carte à puce, qui est ensuite utilisé par le moteur HDX pour transmettre à distance le matériel et les informations d'identification de la carte à puce à Citrix Virtual Apps and Desktops. Citrix Virtual Apps and Desktops sélectionne automatiquement un certificat à partir de la carte à puce et obtient le code PIN à partir du moteur HDX.

  L'option associée `ENABLE\\_SSON` est activée par défaut.

Si une stratégie de sécurité vous empêche d'activer Single Sign-on sur une machine, configurez l'application Citrix Workspace à l'aide du modèle d'administration d'objet de stratégie de groupe.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sélectionnez **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Authentification utilisateur** > **Nom d'utilisateur et mot de passe locaux**.
3. Sélectionnez **Activer l'authentification pass-through**.
4. Redémarrez l'application Citrix Workspace pour que les modifications prennent effet.



Pour configurer StoreFront :

Lorsque vous configurez le service d'authentification sur le serveur StoreFront, sélectionnez l'option Authentification pass-through au domaine. Ce paramètre active l'authentification Windows intégrée. Vous n'avez pas besoin de sélectionner l'option Carte à puce, sauf si vous disposez également de clients n'appartenant pas au domaine qui se connectent à StoreFront à l'aide de cartes à puce.

Pour plus d'informations sur l'utilisation de cartes à puce avec StoreFront, consultez la section Configurer le service d'authentification dans la documentation de StoreFront.

Cartes à puce

L'application Citrix Workspace pour Windows prend en charge l'authentification par carte à puce suivante :

- **Authentification pass-through (Single Sign-On)** : l'authentification pass-through capture les informations d'identification de la carte à puce lorsque les utilisateurs ouvrent une session sur

l'application Citrix Workspace. Citrix Workspace utilise les informations d'identification capturées comme suit :

- Les utilisateurs dont les machines appartiennent au domaine qui ouvrent une session sur l'application Citrix Workspace avec des informations d'identification de carte à puce peuvent démarrer des applications et des bureaux virtuels sans procéder à une nouvelle authentification.
- L'application Citrix Workspace qui s'exécute sur des machines n'appartenant pas au domaine avec des informations d'identification de carte à puce doivent de nouveau entrer leurs informations d'identification pour démarrer une application ou un bureau virtuel.

L'authentification pass-through requiert une configuration sur StoreFront et l'application Citrix Workspace.

- **Authentification bimodale** : avec l'authentification bimodale, les utilisateurs peuvent choisir d'utiliser une carte à puce ou d'entrer leurs nom d'utilisateur et mot de passe. Cette fonctionnalité est utile lorsque vous ne pouvez pas utiliser de carte à puce. Par exemple, le certificat d'ouverture de session a expiré. Des magasins dédiés doivent être configurés pour chaque site pour permettre l'authentification bimodale et la méthode **DisableCtrlAltDel** doit être définie sur **False** pour autoriser les cartes à puce. L'authentification bimodale requiert la configuration de StoreFront.

  L'authentification bimodale permet à l'administrateur StoreFront de proposer à l'utilisateur à la fois l'authentification par nom d'utilisateur et mot de passe et par carte à puce pour le même magasin en les sélectionnant dans la console StoreFront. Consultez la documentation StoreFront.

- **Certificats multiples** : de multiples certificats peuvent être disponibles pour une seule carte à puce et si plusieurs cartes à puce sont utilisées. Lorsque vous insérez une carte à puce dans un lecteur de cartes, les certificats s'appliquent à toutes les applications qui s'exécutent sur la machine utilisateur, y compris l'application Citrix Workspace.

- **Authentification du certificat client** : l'authentification du certificat client requiert la configuration de Citrix Gateway et de StoreFront.

  - Pour accéder à StoreFront via Citrix Gateway, vous devrez peut-être vous ré-authentifier après le retrait d'une carte à puce.
  - Lorsque la configuration SSL de Citrix Gateway est définie sur authentification du certificat client obligatoire, la sécurité des opérations est garantie. Toutefois, l'authentification du certificat client obligatoire n'est pas compatible avec l'authentification bimodale.

- **Sessions double hop** : si une session double hop est nécessaire, une connexion est établie entre l'application Citrix Workspace et le bureau virtuel de l'utilisateur. Les déploiements qui prennent en charge le double-hop sont décrits dans la documentation Citrix Virtual Apps and Desktops.

- **Applications activées pour carte à puce** : 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 Citrix Virtual Apps and Desktops.

Limitations :

- Les certificats doivent être stockés sur une carte à puce et non sur la machine utilisateur.
- L'application Citrix Workspace n'enregistre pas le choix de certificat de l'utilisateur, mais mémorise le code PIN lors de la configuration. Le code PIN est mis en cache dans la mémoire non paginée uniquement pendant la session utilisateur et n'est pas stocké sur le disque.
- L'application Citrix Workspace ne reconnecte pas une session lorsqu'une carte à puce est insérée.
- Lorsqu'elle est configurée pour utiliser l'authentification par carte à puce, l'application Citrix Workspace ne prend pas en charge l'authentification unique avec réseau privé virtuel (VPN) ou le pré-lancement de session. Pour utiliser un VPN avec l'authentification par carte à puce, installez Citrix Gateway Plug-in, ouvrez une session via une page Web et utilisez vos cartes à puce et 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.
- Les communications du programme de mise à jour de l'application Citrix Workspace avec citrix.com et Merchandising Server ne sont pas compatibles avec l'authentification par carte à puce sur Citrix Gateway.

> **Avertissement**
>
> Certaines configurations nécessitent des modifications du registre. Une utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux pouvant nécessiter la réinstallation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Veillez à sauvegarder le registre avant de le modifier.

Pour activer le Single Sign-On (SSO) pour l'authentification par carte à puce :

Pour configurer l'application Citrix Workspace pour Windows, incluez l'option de ligne de commande suivante lors de l'installation :

- `ENABLE\\_SSON=Yes`

  L'authentification pass-through est également appelée Single Sign-On (SSO). L'activation de ce paramètre empêche l'application Citrix Workspace d'afficher une seconde invite de saisie du code PIN.

- Définissez **SSONCheckEnabled** sur false si le composant Single Sign-on n'est pas installé. La clé empêche le gestionnaire d'authentification de l'application Citrix Workspace de rechercher le composant Single Sign-on, ce qui permet à Citrix Workspace de s'authentifier auprès de StoreFront.


```
HKEY\\_CURRENT\\_USER\Software\Citrix\AuthManager\protocols\integratedwindows
\

HKEY\\_LOCAL\\_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows
\
```

Pour activer l'authentification par carte à puce sur StoreFront au lieu de Kerberos, installez l'application Citrix Workspace pour Windows à l'aide des options de ligne de commande suivantes.

- `/includeSSON` installe l'authentification Single Sign-On (authentification pass-through). Permet la mise en cache des informations d'identification et l'utilisation de l'authentification pass-through au domaine.
- Si l'utilisateur ouvre une session sur le point de terminaison avec une méthode autre que la carte à puce pour l'authentification de l'application Citrix Workspace pour Windows (par exemple, le nom d'utilisateur et le mot de passe), la ligne de commande est la suivante :

  ```
  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
  ```

Aucune information d'identification n'est capturée lors de l'ouverture de session et l'application Citrix Workspace peut mémoriser le code PIN lors de l'ouverture de session sur l'application Citrix Workspace.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Rendez-vous sur **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Authentification utilisateur** > **Nom d'utilisateur et mot de passe locaux**.
3. Sélectionnez **Activer l'authentification pass-through**. En fonction de la configuration et des paramètres de sécurité, sélectionnez l'option **Autoriser l'authentification pass-through pour toutes les connexions ICA** pour que l'authentification pass-through fonctionne.

Pour configurer StoreFront :

- Lorsque vous configurez le service d'authentification, sélectionnez la case à cocher **Carte à puce**.

Pour plus d'informations sur l'utilisation de cartes à puce avec StoreFront, consultez la section Configurer le service d'authentification dans la documentation de StoreFront.

Pour activer l'utilisation de cartes à puce sur les machines utilisateur :

1. Importez le certificat racine d'autorité de certification dans le keystore de la machine.
2. Installez les logiciels intermédiaires de chiffrement du fournisseur de services.
3. Installez et configurez l'application Citrix Workspace.

Pour modifier la façon dont les certificats sont sélectionnés :

Par défaut, si plusieurs certificats sont valides, l'application Citrix Workspace invite l'utilisateur à en choisir un dans la liste. Vous pouvez également configurer l'application Citrix Workspace pour qu'elle

utilise le certificat par défaut (celui du fournisseur de carte à puce) ou le certificat présentant la date d'expiration la plus éloignée. S'il n'existe aucun certificat valide, l'utilisateur en est notifié et il a la possibilité d'utiliser une autre méthode d'ouverture de session, le cas échéant.

Un certificat valide doit présenter ces caractéristiques :

- L'heure actuelle de l'horloge sur l'ordinateur doit se situer dans la période de validité du certificat.
- La **clé publique du sujet** doit utiliser l'algorithme RSA et présenter une longueur de 1 024, 2 048 ou 4 096 bits.
- L'utilisation de la clé doit contenir une signature numérique.
- L'autre nom du sujet doit contenir le nom d'utilisateur principal (UPN).
- L'utilisation améliorée de la clé doit contenir l'ouverture de session par carte à puce et l'authentification client, ou toute utilisation de clé.
- L'une des autorités de certification sur la chaîne de l'émetteur du certificat doit correspondre à l'un des noms uniques autorisés (DN) envoyé par le serveur dans la négociation TLS.

Modifiez la manière dont les certificats sont sélectionnés en utilisant l'une des méthodes suivantes :

- Spécifiez l'option `AM\\_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }` sur la ligne de commande de l'application Citrix Workspace.

  Prompt est la valeur par défaut. Pour SmartCardDefault ou LatestExpiry, si plusieurs certificats répondent aux critères, l'application Citrix Workspace invite l'utilisateur à choisir un certificat.

- Ajoutez la valeur de clé suivante à la clé de registre HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE\Softwa : CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }.

Les valeurs définies dans HKEY_CURRENT_USER sont prioritaires sur les valeurs définies dans HKEY_LOCAL_MACHINE afin d'aider l'utilisateur à sélectionner un certificat.

Pour utiliser des invites de code PIN CSP :

Par défaut, les invites de saisie du code PIN sont fournies par l'application Citrix Workspace pour Windows plutôt que par le fournisseur de service cryptographique (CSP) de la carte à puce. L'application Citrix Workspace invite les utilisateurs à entrer un code PIN lorsque cela est requis et transmet le code PIN au CSP de la carte à puce. Si votre site ou votre carte à puce impose des mesures de sécurité plus strictes, telles que la désactivation de la mise en cache du code PIN par processus ou par session, vous pouvez configurer l'application Citrix Workspace pour qu'elle utilise à la place les composants du CSP pour gérer la saisie du code PIN, y compris l'invite de saisie du code PIN.

Modifiez la manière dont la saisie du code PIN est traitée en utilisant l'une des méthodes suivantes :

- Spécifiez l'option `AM\\_SMARTCARDPINENTRY=CSP` sur la ligne de commande de l'application Citrix Workspace.
- Ajoutez la valeur de clé suivante à la clé de registre HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix SmartCardPINEntry=CSP.

Authentification par carte à puce pour l'interface Web

Si l'application Citrix Workspace pour Windows a été installée avec un composant SSON, l'authentification pass-through est activée par défaut, même si l'authentification pass-through par code PIN pour carte à puce n'est pas activée sur le site PNAgent XenApp, le paramètre pass-through comme méthode d'authentification ne sera plus valide. L'écran ci-dessous montre comment activer la carte à puce comme méthode d'authentification lorsque l'application Citrix Workspace est configurée correctement avec SSON.

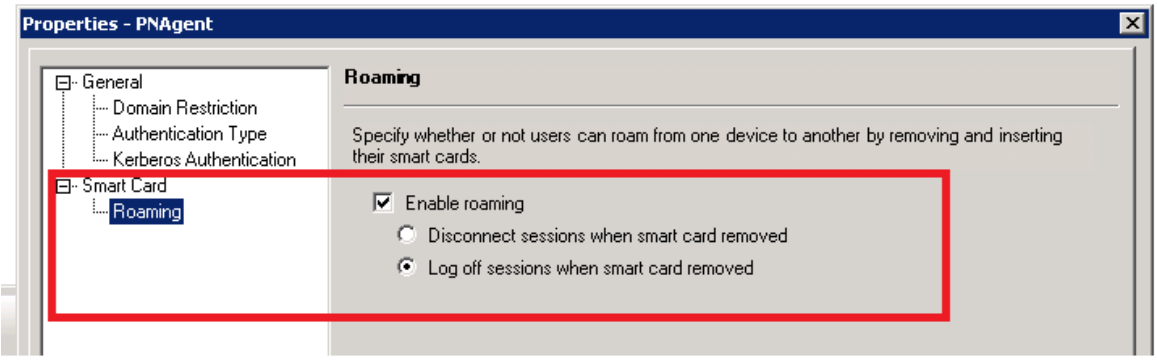
Utilisez la stratégie de retrait de carte à puce pour contrôler le comportement de retrait de la carte à puce lorsqu'un utilisateur s'authentifie auprès du site PNAgent de l'Interface Web Citrix 5.4.

Lorsque cette stratégie est activée, l'utilisateur est déconnecté de la session Citrix Virtual Apps si la carte à puce a été retirée de la machine cliente. Toutefois, l'utilisateur est toujours connecté à l'application Citrix Workspace.

Pour que cette stratégie soit appliquée, la stratégie de retrait de carte à puce doit être définie dans le site XenApp Services de l'Interface Web. Les paramètres se trouvent sur l'Interface Web 5.4, **Site XenApp Services > Authentification unique avec carte à puce > Activer l'itinérance > Fermer les sessions lors du retrait d'une carte à puce**.

Lorsque la stratégie de retrait de carte à puce est désactivée, la session Citrix Virtual Apps de l'utilisateur est déconnectée si la carte à puce est retirée de la machine cliente. Le retrait de la carte à puce sur le site XenApp Services de l'interface Web n'a aucun effet.

> **Remarque :**
>
> Il existe des stratégies distinctes pour les clients 32 bits et 64 bits. Pour les machines 32 bits, le nom de la stratégie est **Stratégie de retrait de carte à puce (machine 32 bits)** et pour les machines 64 bits, le nom de la stratégie est **Stratégie de retrait de carte à puce (machine 64 bits)**.



Modifications de la prise en charge et du retrait des cartes à puce

Tenez compte de ce qui suit lors de l'ouverture de session sur un site PNAgent XenApp 6.5 :

- L'ouverture de session par carte à puce est prise en charge pour les connexions au site PNAgent.
- La stratégie de retrait de carte à puce a été modifiée sur le site PNAgent :

Une session Citrix Virtual Apps est fermée lorsque la carte à puce est retirée : si le site PNAgent est configuré avec l'authentification par carte à puce, la stratégie correspondante doit être configurée sur l'application Citrix Workspace pour Windows pour appliquer la fermeture de session de Citrix Virtual Apps. Activez l'itinérance pour l'authentification par carte à puce sur le site PNAgent XenApp et activez la stratégie de retrait de carte à puce, qui déconnecte Citrix Virtual Apps de la session de l'application Citrix Workspace. L'utilisateur reste connecté à la session de l'application Citrix Workspace.

Limitation :

Lorsque vous ouvrez une session sur le site PNAgent à l'aide de l'authentification par carte à puce, le nom d'utilisateur est affiché comme **Session ouverte**.

Sécuriser les communications

March 18, 2019

Pour sécuriser les communications entre le serveur Citrix Virtual Apps and Desktops et l'application Citrix Workspace, vous pouvez intégrer vos connexions de l'application Citrix Workspace à l'aide de technologies sécurisées, dont :

- Citrix Gateway : pour plus d'informations, reportez-vous aux rubriques de cette section et à la documentation Citrix Gateway et StoreFront.

  > **Remarque :**
  >
  > Citrix recommande d'utiliser Citrix Gateway entre les serveurs StoreFront et les machines utilisateur.

- Un pare-feu : les pare-feu de réseau peuvent autoriser ou empêcher le passage des paquets de données en fonction de l'adresse et du port de destination. Si vous utilisez l'application Citrix Workspace avec un pare-feu de réseau qui mappe l'adresse IP interne du serveur sur une adresse Internet externe (c'est-à-dire, la traduction d'adresse de réseau, ou NAT), configurez l'adresse externe.
- Serveur approuvé.
- Pour les déploiements de Citrix Virtual Apps ou de l'Interface Web uniquement (non applicable à XenDesktop 7) : un serveur proxy SOCKS ou serveur proxy sécurisé (également appelé serveur proxy de sécurité, serveur proxy HTTPS). Vous pouvez utiliser des serveurs proxy pour

limiter l'accès à l'intérieur et à l'extérieur de votre réseau, et pour gérer les connexions entre l'application Citrix Workspace et le serveur. L'application Citrix Workspace prend en charge les protocoles de proxy SOCKS et de proxy sécurisé.

- S'applique uniquement aux déploiements de Citrix Virtual Apps ou de l'Interface Web ; ne s'applique pas aux solutions XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5, ou XenApp 7.5 : Relais SSL utilisant les protocoles TLS.
- Pour Citrix Virtual Apps and Desktops 7.6, vous pouvez activer une connexion SSL directement entre des utilisateurs et des VDA.

L'application Citrix Workspace est compatible avec les environnements utilisant les modèles de sécurité de bureau Microsoft Specialized Security - Limited Functionality (SSLF). Ces modèles sont pris en charge sur plusieurs plates-formes Windows.

Suites de chiffrement obsolètes

La version 4.12 contient deux modifications importantes pour les protocoles de communications sécurisées TLS/DTLS : la prise en charge de **DTLS 1.2** et la fin de prise en charge des suites de chiffrement TLS/DTLS.

DTLS 1.2 prend en charge le protocole de transport UDP, l'équivalent de TLS 1.2 pour le protocole de transport TCP. Des versions antérieures de l'application Citrix Workspace pour Windows prenaient déjà en charge TLS 1.2.

Les suites de chiffrement avec le préfixe **TLS_RSA_** ne proposent pas la fonctionnalité Forward Secrecy. De manière générale, ces suites de chiffrement sont maintenant obsolètes dans le secteur. Toutefois, pour prendre en charge la rétrocompatibilité avec les anciennes versions de Citrix Virtual Apps and Desktops, l'application Citrix Workspace pour Windows peut utiliser ces suites de chiffrement.

Un nouveau modèle d'administration d'objet de stratégie de groupe a été créé pour autoriser l'utilisation des suites de chiffrement obsolètes. Dans Citrix Receiver pour Windows 4.12, cette stratégie est activée par défaut, mais n'applique pas la fin de prise en charge de ces suites de chiffrement à l'aide des algorithmes de chiffrement AES ou 3DES par défaut. Toutefois, vous pouvez modifier et utiliser cette stratégie pour appliquer la fin de prise en charge de manière plus stricte.

Voici une liste des suites de chiffrement obsolètes :

- TLS_RSA_AES256_GCM_SHA384
- TLS_RSA_AES128_GCM_SHA256
- TLS_RSA_AES256_CBC_SHA256
- TLS_RSA_AES256_CBC_SHA
- TLS_RSA_AES128_CBC_SHA

- TLS_RSA_3DES_CBC_EDE_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

> **Remarque :**
>
> Les deux dernières suites de chiffrement utilisent l'algorithme RC4 qui est obsolète car ces suites de chiffrement ne sont pas sécurisées. Vous pouvez également considérer la suite de chiffrement **TLS_RSA_3DES_CBC_EDE_SHA** comme étant obsolète. Vous pouvez utiliser cette stratégie pour appliquer toutes ces suites obsolètes.

Pour plus d'informations sur la configuration DTLS v1.2, consultez la section Transport adaptatif dans la documentation Citrix Virtual Apps and Desktops.

> **Remarque :**
>
> Lorsque vous mettez à niveau ou installez l'application Citrix Workspace pour Windows pour la première fois, ajoutez les derniers fichiers de modèle à l'objet de stratégie de groupe local. Pour plus d'informations sur l'ajout de fichiers de modèle à l'objet de stratégie de groupe local, consultez la section Modèle d'administration d'objet de stratégie de groupe. En cas de mise à niveau, les paramètres existants sont conservés lors de l'importation des derniers fichiers.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Routage réseau**.
3. Sélectionnez la stratégie **Suites de chiffrement obsolètes**.
4. Sélectionnez **Activé** et choisissez l'une des options suivantes :
   a) **TLS_RSA_**: *By default, TLS_RSA_* is selected. Cette option doit être sélectionnée pour vous permettre d'utiliser les deux autres suites de chiffrement. Les suites de chiffrement suivantes sont incluses lorsque vous sélectionnez cette option :
      i. TLS_RSA_AES256_GCM_SHA384
      ii. TLS_RSA_AES128_GCM_SHA256
      iii. TLS_RSA_AES256_CBC_SHA256
      iv. TLS_RSA_AES256_CBC_SHA
      v. TLS_RSA_AES128_CBC_SHA
      vi. TLS_RSA_3DES_CBC_EDE_SHA
   b) **TLS_RSA_WITH_RC4_128_MD5** : sélectionnez cette option pour utiliser la suite de chiffrement RC4-MD5.
   c) **TLS_RSA_WITH_RC4_128_SHA** : sélectionnez cette option pour utiliser la suite de chiffrement RC4_128_SHA.
5. Cliquez sur **Appliquer**, puis sur **OK**.
6. Exécutez `gpupdate /force` pour que les modifications prennent effet.

Le tableau suivant répertorie les suites de chiffrement compris dans chaque ensemble :

Ciphersuite	Native Cyrpto Kit mode and cipher set								
	Open		FIPS				SP800-52		
	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y		Y	Y		Y	Y	
TLS_RSA_WITH_AES_256_GCM_SHA384 (1) (2)	X								
TLS_RSA_WITH_AES_128_GCM_SHA256 (1) (2)	X	X							
TLS_RSA_WITH_AES_256_CBC_SHA256 (1) (2)	X								
TLS_RSA_WITH_AES_256_CBC_SHA (2)	X								
TLS_RSA_WITH_AES_128_CBC_SHA (2)	X	X							
TLS_RSA_WITH_RC4_128_SHA (2) (3)	X	X							
TLS_RSA_WITH_RC4_128_MD5 (2) (3)	X	X							
TLS_RSA_WITH_3DES_EDE_CBC_SHA (2)	X								
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	Y	Y	Y	Y	Y	Y	Y	Y	Y
Notes									
(1) Ciphersuites that require TLS1.2/DTLS 1.2									
(2) Ciphersuites disabled by default									
(3) Ciphersuites not available for DTLS protocol									
Y - Supported ciphersuites									
X-Deprecated ciphersuites									

TLS

Cette rubrique s'applique à Citrix Virtual Apps and Desktops version 7.6 et versions ultérieures.

Pour utiliser le cryptage TLS pour toutes les communications de l'application Citrix Workspace avec le serveur, configurez la machine utilisateur, l'application Citrix Workspace et, si vous utilisez l'Interface Web, le serveur qui exécute cette interface. Pour obtenir des informations sur la sécurisation des communications StoreFront, consultez la section Sécuriser dans la documentation StoreFront. Pour obtenir des informations sur la sécurisation de l'Interface Web, consultez la section Sécuriser dans la documentation de l'Interface Web.

Conditions préalables :

Les machines utilisateur doivent présenter la configuration spécifiée dans la section Configuration système requise.

Utilisez cette stratégie pour configurer les options TLS qui permettent à l'application Citrix Workspace d'identifier de manière sécurisée le serveur auquel il se connecte et de crypter toutes les communications avec le serveur.

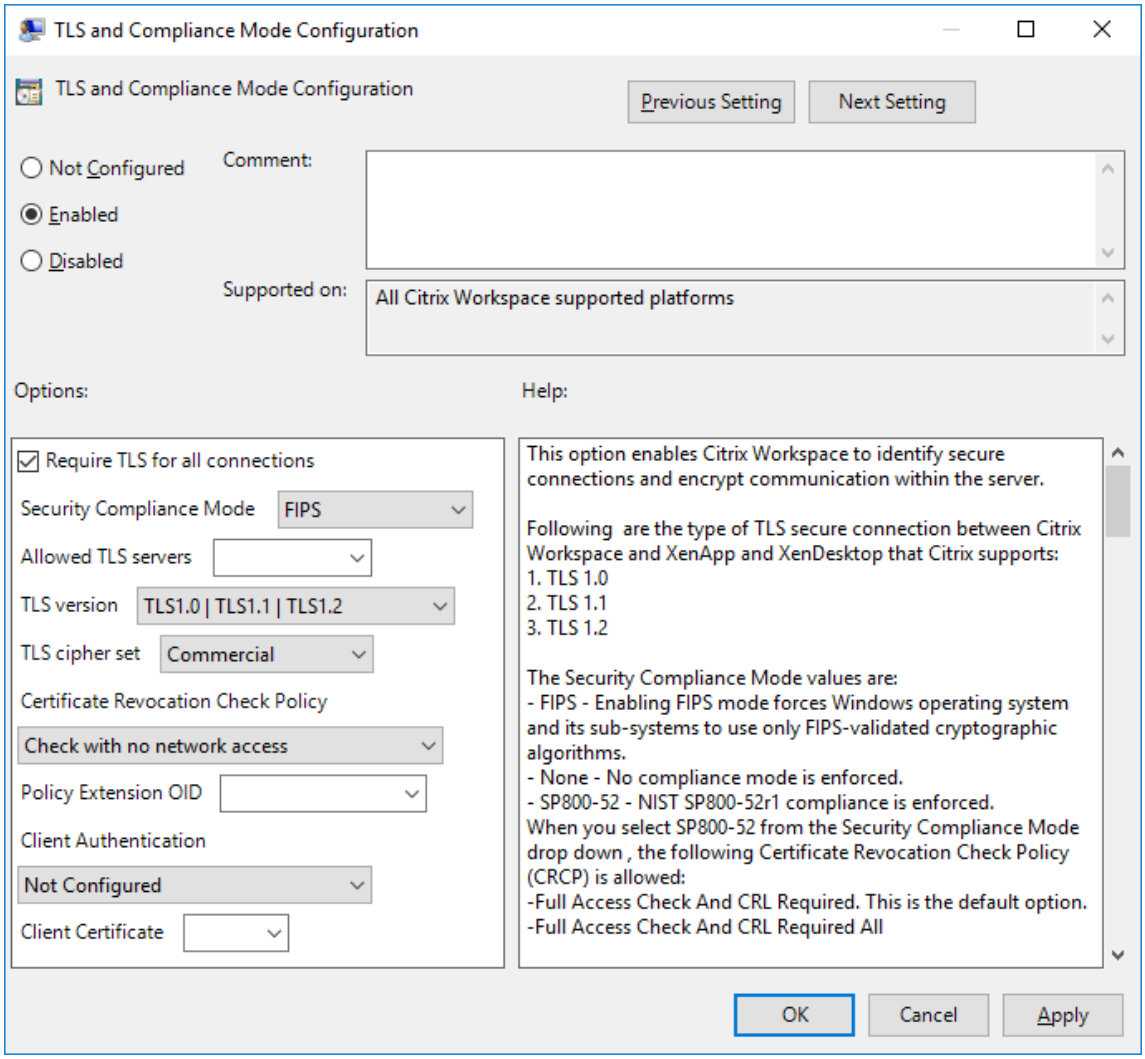
Vous pouvez utiliser les options suivantes pour :

- Imposer l'utilisation de TLS : Citrix recommande d'utiliser le protocole TLS pour toutes les connexions sur des réseaux non approuvés, y compris Internet.
- Imposer l'utilisation de la cryptographie approuvée FIPS (Federal Information Processing Standards) : la cryptographie approuvée et l'aide suivent les recommandations de la norme NIST SP 800-52. Ces options sont désactivées par défaut.

- Imposer l'utilisation d'une version spécifique du protocole TLS et de suites de chiffrement TLS spécifiques : Citrix prend en charge les protocoles TLS 1.0, TLS 1.1 et TLS 1.2 entre l'application Citrix Workspace pour Windows et Citrix Virtual Apps and Desktops.
- Vous connecter uniquement à des serveurs spécifiques.
- Vérifier si le certificat de serveur est révoqué.
- Rechercher une stratégie d'émission de certificats de serveur spécifique.
- Sélectionner un certificat client particulier, si le serveur est configuré pour en demander un.

Prise en charge du protocole TLS

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Citrix Workspace** > **Routage réseau** et sélectionnez la stratégie **Configuration de TLS et du mode de conformité**.



3. Sélectionnez **Activé** pour activer les connexions sécurisées et crypter les communications sur le serveur. Définissez les options suivantes :

   > **Remarque :**
   >
   > Citrix recommande d'utiliser TLS pour sécuriser les connexions.

4. Sélectionnez **Exiger TLS pour toutes les connexions** pour obliger l'application Citrix Workspace à utiliser TLS pour toutes les connexions aux applications et bureaux publiés.
5. Dans le menu **Mode de conformité aux normes de sécurité**, sélectionnez l'option appropriée :

   a) **Aucun** : aucun mode de conformité n'est appliqué.

   b) **SP800-52** : sélectionnez **SP800-52** pour la conformité avec la norme NIST SP 800-52. Sélectionnez cette option uniquement si les serveurs ou la passerelle sont conformes aux recommandations de la norme NIST SP 800-52.

> **Remarque :**
>
> Si vous sélectionnez **SP800-52**, la cryptographie approuvée FIPS est automatiquement utilisée, même si l'option **Activer FIPS** n'est pas sélectionnée. Vous devez également activer l'option de sécurité Windows **Chiffrement système : utilisez des algorithmes compatibles FIPS pour le chiffrement, le hachage et la signature**. Sinon, la connexion de l'application Citrix Workspace aux applications et bureaux publiés risque d'échouer.

Si vous sélectionnez **SP800-52**, vous devez sélectionner le paramètre **Stratégie de vérification de la liste de révocation de certificats** avec **Vérifier avec accès complet** ou **Exiger vérification avec accès complet et toutes les listes de révocation de certificats**.

Lorsque vous sélectionnez **SP800-52**, l'application Citrix Workspace vérifie que le certificat de serveur est conforme aux recommandations de la norme NIST SP 800-52. Si le certificat de serveur n'est pas conforme, la connexion de l'application Citrix Workspace risque d'échouer.

c) **Activer FIPS** : sélectionnez cette option pour imposer l'utilisation de la cryptographie approuvée FIPS. Vous devez également activer l'option de sécurité Windows de la stratégie de groupe de système d'exploitation **Chiffrement système : utilisez des algorithmes compatibles FIPS pour le chiffrement, le hachage et la signature**. Sinon, la connexion de l'application Citrix Workspace aux applications et bureaux publiés risque d'échouer.

6. Dans le menu déroulant **Serveurs TLS autorisés**, sélectionnez le numéro de port. Vous pouvez vous assurer que l'application Citrix Workspace pour Windows se connecte uniquement à un serveur spécifié dans une liste séparée par des virgules. Vous pouvez spécifier des numéros de port et des caractères génériques. Par exemple, *.citrix.com: 4433 autorise les connexions à tout serveur dont le nom commun se termine par .citrix.com sur le port 4433. L'émetteur du certificat certifie l'exactitude des informations contenues dans un certificat de sécurité. Si Citrix Workspace ne reconnaît pas et n'approuve pas l'émetteur, la connexion est refusée.
7. Dans le menu **Version TLS**, sélectionnez une des options suivantes :
   - **TLS 1.0, TLS 1.1 ou TLS 1.2** : il s'agit du paramètre par défaut. Cette option est recommandée uniquement si TLS 1.0 est requis pour des raisons de compatibilité.
   - **TLS 1.1 ou TLS 1.2** : utilisez cette option pour vous assurer que les connexions ICA utilisent TLS 1.1 ou TLS 1.2.
   - **TLS 1.2** : cette option est recommandée si TLS 1.2 est exigé par une entreprise.
8. **Suite de chiffrement TLS** : pour forcer l'utilisation des suites de chiffrement TLS, sélectionnez Gouvernement (GOV), Commercial (COM) ou Quelconque (ALL). Dans certaines configurations de Citrix Gateway, vous devrez peut-être sélectionner **COM**. L'application Citrix Workspace

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 :**
>
> Citrix ne recommande pas l'utilisation de clés RSA de longueur de 1 024 bits.

- **Quelconque** : lorsque l'option « Quelconque » est sélectionnée, la stratégie n'est pas configurée et les suites de chiffrement suivantes sont autorisées :
  a) TLS_RSA_WITH_RC4_128_MD5
  b) TLS_RSA_WITH_RC4_128_SHA
  c) TLS_RSA_WITH_3DES_EDE_CBC_SHA
  d) TLS_RSA_WITH_AES_128_CBC_SHA
  e) TLS_RSA_WITH_AES_256_CBC_SHA
  f) TLS_RSA_WITH_AES_128_GCM_SHA256
  g) TLS_RSA_WITH_AES_256_GCM_SHA384
- **Commerciale** : lorsque l'option « Commerciale » est sélectionnée, seules les suites de chiffrement suivantes sont autorisées :
  a) TLS_RSA_WITH_RC4_128_MD5
  b) TLS_RSA_WITH_RC4_128_SHA
  c) TLS_RSA_WITH_AES_128_CBC_SHA
  d) TLS_RSA_WITH_AES_128_GCM_SHA256
- **Gouvernementale** : lorsque l'option « Gouvernementale » est sélectionnée, seules les suites de chiffrement suivantes sont autorisées :
  a) TLS_RSA_WITH_AES_256_CBC_SHA
  b) TLS_RSA_WITH_3DES_EDE_CBC_SHA
  c) TLS_RSA_WITH_AES_128_GCM_SHA256
  d) TLS_RSA_WITH_AES_256_GCM_SHA384

9. Dans le menu **Stratégie de vérification de la liste de révocation de certificats**, sélectionnez une des options suivantes :
   - **Vérifier sans accès au réseau** : la liste de révocation des 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 de la liste de révocation de certificats n'est pas obligatoire à la vérification du certificat serveur présenté par le serveur Relais SSL/Citrix Secure Web Gateway cible.
   - **Vérifier avec accès complet** : 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. Si des informations de révocation sont trouvées pour un certificat, la connexion

est refusée. L'utilisation d'une liste de révocation de certificats n'est pas indispensable à la vérification du certificat serveur présenté par le serveur cible.

- **Exiger vérification avec accès complet et liste de révocation de certificats** : 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 est refusée. Si des informations de révocation sont trouvées pour un certificat, la connexion sera refusée.
- **Exiger vérification avec accès complet et toutes les listes de révocation de certificats** : la liste de révocation de certificats est vérifiée, y compris l'autorité de certification racine. Les magasins locaux de la liste de révocation de certificats et tous les points de distribution sont utilisés. Si des informations de révocation sont trouvées pour un certificat, la connexion est refusée. Si des informations de révocation sont trouvées pour un certificat, la connexion sera refusée.
- **Aucune vérification** : la liste de révocation des certificats n'est pas vérifiée.

10. **OID de l'extension de stratégie** vous permet de limiter la connexion de l'application Citrix Workspace aux serveurs ayant une stratégie d'émission de certificats spécifique. Si l'option **OID de l'extension de stratégie** est sélectionnée, l'application Citrix Workspace n'accepte que les certificats de serveur contenant cet OID d'extension de stratégie.
11. Dans le menu **Authentification client**, sélectionnez une des options suivantes :
    - **Désactivé** : l'authentification client est désactivée
    - **Afficher sélecteur de certificats** : toujours demander à l'utilisateur de sélectionner un certificat
    - **Sélectionner automatiquement si possible** : demander à l'utilisateur uniquement lorsque plusieurs certificats sont disponibles
    - **Non configuré** : indique que l'authentification du client n'est pas configurée.
    - **Utiliser certificat spécifié** : utiliser le certificat client défini dans l'option Certificat client.
12. Utilisez le paramètre **Certificat client** pour spécifier l'empreinte numérique du certificat d'identification et éviter une intervention inutile de l'utilisateur.
13. Cliquez sur **Appliquer** et **OK** pour enregistrer la stratégie.

Le tableau suivant répertorie les suites de chiffrement compris dans chaque ensemble :

Ciphersuite	Native Cyrpto Kit mode and cipher set								
	Open			FIPS			SP800-52		
	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y		Y	Y		Y	Y	
TLS_RSA_WITH_AES_256_GCM_SHA384 (1) (2)	X								
TLS_RSA_WITH_AES_128_GCM_SHA256 (1) (2)	X	X							
TLS_RSA_WITH_AES_256_CBC_SHA256 (1) (2)	X								
TLS_RSA_WITH_AES_256_CBC_SHA (2)	X								
TLS_RSA_WITH_AES_128_CBC_SHA (2)	X	X							
TLS_RSA_WITH_RC4_128_SHA (2) (3)	X	X							
TLS_RSA_WITH_RC4_128_MD5 (2) (3)	X	X							
TLS_RSA_WITH_3DES_EDE_CBC_SHA (2)	X								
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	Y	Y	Y	Y	Y	Y	Y	Y	Y
Notes									
(1) Ciphersuites that require TLS1.2/DTLS 1.2									
(2) Ciphersuites disabled by default									
(3) Ciphersuites not available for DTLS protocol									
Y - Supported ciphersuites									
X-Deprecated ciphersuites									

Pare-feu

Les pare-feu de réseau peuvent autoriser ou empêcher le passage des paquets de données en fonction de l'adresse et du port de destination. Si vous utilisez un pare-feu dans votre déploiement, l'application Citrix Workspace pour Windows doit pouvoir communiquer via le pare-feu avec le serveur Web et le serveur Citrix.

Ports de communication Citrix communs

Source	Type	Port	Détails
Application Citrix Workspace	TCP	80/443	Communication avec StoreFront
ICA/HDX	TCP	1494	Accès aux applications et bureaux virtuels
ICA/HDX avec fiabilité de session	TCP	2598	Accès aux applications et bureaux virtuels
ICA/HDX sur SSL	TCP	443	Accès aux applications et bureaux virtuels

Source	Type	Port	Détails
ICA/HDX depuis Workspace HTML5	TCP	8008	Accès aux applications et bureaux virtuels
Audio ICA/HDX sur UDP	TCP	16500 - 16509	Plage pour les ports audio ICA/HDX
IMA	TCP	2512	Independent Management Architecture (IMA)
Console de gestion	TCP	2513	Consoles de gestion Citrix et *Services WCF Remarque : pour les plates-formes 7.5 et ultérieures basées sur FMA, le port 2513 n'est PAS utilisé.
Demande application/bureau	TCP	80/8080/443	Service XML
STA	TCP	80/8080/443	Secure Ticketing Authority (intégré au service XML)

> **Remarque :**
>
> Dans XenApp 6.5, le port 2513 est utilisé par les Services XenApp Commands Reporting via WCF.

Si le pare-feu est configuré pour la traduction d'adresses réseau (NAT), vous pouvez utiliser l'Interface Web pour définir les mappages depuis les adresses internes vers les adresses externes et les ports. Par exemple, si votre serveur Citrix Virtual Apps and Desktops n'est pas configuré avec une adresse secondaire, vous pouvez configurer l'Interface Web pour qu'elle fournisse une adresse secondaire à l'application Citrix Workspace. L'application utilisera l'adresse externe et le numéro de port pour se connecter au serveur. Pour plus d'informations, veuillez consulter la documentation relative à l'Interface Web.

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 Windows et les serveurs. L'application Citrix Workspace

prend en charge les protocoles de proxy SOCKS et de proxy sécurisé.

Lorsqu'elle communique avec le serveur, l'application Citrix Workspace utilise les paramètres de serveur proxy configurés à distance sur le serveur qui exécute Workspace pour Web ou l'Interface Web. Pour de plus amples informations sur la configuration du serveur proxy, reportez-vous à la documentation relative à StoreFront ou à l'Interface Web.

Lors la communication avec le serveur Web, l'application Citrix Workspace utilise les paramètres de serveur proxy configurés via les paramètres **Internet** du navigateur Web par défaut sur la machine utilisateur. Vous devez configurer les paramètres **Internet** du navigateur Web par défaut de la machine utilisateur en conséquence.

Configurez les paramètres de proxy à l'aide de l'Éditeur du Registre pour forcer l'application Citrix Workspace à utiliser ou à ignorer le serveur proxy lors des connexions.

> **Avertissement**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre.

1. Accéder à `\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\AuthManager`
2. Définissez le paramètre **ProxyEnabled** (REG_SZ).
   - True : indique que l'application Citrix Workspace utilise le serveur proxy lors des connexions.
   - False : indique que l'application Citrix Workspace ignore le serveur proxy lors des connexions.
3. Redémarrez l'application Citrix Workspace pour que les modifications prennent effet.

Citrix Secure Web Gateway

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

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

L'application Citrix Workspace utilise des paramètres configurés à distance sur le serveur exécutant l'Interface Web pour se connecter aux serveurs exécutant Citrix Secure Web Gateway. Consultez les rubriques de l'Interface Web pour obtenir des informations sur la configuration des paramètres d'un serveur proxy pour l'application Citrix Workspace.

Pour plus d'informations sur la configuration des paramètres de serveur proxy, veuillez consulter la documentation de l'Interface Web.

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

- le nom de domaine complet du serveur Citrix Secure Web Gateway ;
- le numéro de port du serveur Citrix Secure Web Gateway.

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.mon_entreprise.com est un nom de domaine complet car il liste dans l'ordre un nom d'hôte (mon_ordinateur), un domaine intermédiaire (mon_entreprise) et un domaine de tête (com). La combinaison du domaine intermédiaire et du domaine de tête (mon_entreprise.com) est appelée nom de domaine.

Serveur approuvé

La configuration d'un serveur approuvé identifie et applique les relations d'approbation aux connexions de l'application Citrix Workspace.

Lorsque vous activez la fonction Serveurs approuvés, l'application Citrix Workspace spécifie les exigences et détermine si la connexion au serveur peut être approuvée ou non. Par exemple, une application Citrix Workspace se connectant à une certaine adresse (comme `https://\*.citrix.com`) avec un type de connexion donné (comme TLS) est dirigée vers une zone de confiance sur le serveur.

Lorsque vous activez cette fonctionnalité, le serveur connecté se trouve dans la zone **Sites de confiance Windows**. Pour obtenir des instructions étape par étape sur l'ajout des serveurs à la zone **Sites de confiance Windows**, veuillez consultez l'aide en ligne d'Internet Explorer.

Pour activer la configuration des serveurs approuvés avec le modèle d'administration d'objet de stratégie de groupe

Configuration requise :

Fermez les composants de l'application Citrix Workspace pour Windows, y compris le centre de connexion.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Dans le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Modèles d'administration classiques (ADM)** > **Composants Citrix** > **Citrix Workspace** > **Routage réseau** > **Paramétrer la configuration d'un serveur approuvé**.
3. Sélectionnez **Activé** pour forcer l'application Citrix Workspace pour Windows à identifier la région.

4. Sélectionnez **Appliquer configuration d'un serveur approuvé**. Cela force le client à effectuer l'identification à l'aide d'un serveur de confiance.
5. Dans la liste déroulante **Zone Internet Windows**, sélectionnez l'adresse du serveur client. Ce paramètre s'applique uniquement à la zone Sites de confiance Windows.
6. Dans le champ **Adresse**, définissez l'adresse du serveur de client pour une zone de site de confiance autre que Windows. Vous pouvez utiliser une liste séparée par des virgules.
7. Cliquez sur **OK** et sur **Appliquer**.

Signature de fichier ICA

La signature de fichier ICA permet de vous protéger contre le lancement non autorisé d'applications ou de bureaux. L'application Citrix Workspace vérifie, à l'aide d'une stratégie administrative, qu'une source approuvée est à l'origine du lancement de l'application ou du bureau, et empêche le lancement provenant de serveurs non approuvés. Vous pouvez configurer la signature de fichier ICA à l'aide du modèle d'administration des objets de stratégie de groupe, StoreFront ou Citrix Merchandising Server. Par défaut, la signature de fichier ICA n'est pas activée par défaut.

Pour plus d'informations sur l'activation de la signature de fichier ICA pour StoreFront, reportez-vous à la section Activer la signature de fichier ICA dans la documentation StoreFront.

Pour le déploiement de l'Interface Web, cette dernière active et configure le lancement d'applications ou de bureaux de manière à y inclure une signature durant le processus de lancement à l'aide du service Signature de fichier ICA. Le service peut signer le fichier ICA à l'aide d'un certificat provenant du magasin de certificats personnel de l'ordinateur.

Citrix Merchandising Server, en association avec l'application Citrix Workspace, active et configure la vérification de la signature de lancement à l'aide de l'assistant Citrix Merchandising Server Administrator Console > Deliveries afin d'ajouter des empreintes numériques de certificats de confiance.

Configurer la signature de fichier ICA

> **Remarque :**
>
> Si CitrixBase.admx\adml n'est pas ajouté à l'objet de stratégie de groupe local, la stratégie **Activer la signature de fichier ICA** peut être absente.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix**.
3. Sélectionnez la stratégie **Activer la signature de fichier ICA**, puis sélectionnez une option selon les besoins :

a) Activé - Indique que vous pouvez ajouter l'empreinte numérique du certificat de signature à la liste blanche des empreintes de certificats de confiance.
b) Certificats de confiance - Cliquez sur **Afficher** pour supprimer l'empreinte de certificat de signature existante de la liste blanche. Vous pouvez copier et coller les empreintes numériques de certificat de signature à partir des propriétés du certificat de signature.
c) Stratégie de sécurité - Sélectionnez l'une des options suivantes dans le menu.
    i. Autoriser uniquement les lancements signés (plus sécurisé) - Autorise uniquement le lancement d'applications ou de bureaux signés à partir d'un serveur approuvé. Un avertissement de sécurité apparaît en cas de signature invalide. Vous ne pouvez pas lancer la session en raison d'une non-autorisation.
    ii. Demander à l'utilisateur lors de lancements non signés (moins sécurisé) - Une invite de message s'affiche lorsqu'une session non signée ou non valide est lancée. Vous pouvez choisir de continuer le lancement ou d'annuler le lancement (option par défaut).

4. Cliquez sur **Appliquer** et **OK** pour enregistrer la stratégie.
5. Redémarrez la session de l'application Citrix Workspace pour que les modifications prennent effet.

Pour sélectionner et distribuer un certificat de signature numérique :

Lors de la sélection d'un certificat de signature numérique, Citrix vous recommande de choisir l'une des solutions suivantes (elles apparaissent par ordre de priorité) :

1. Achetez un certificat de signature de code ou certificat de signature SSL émanant d'une autorité de certification publique (CA).
2. Si votre entreprise dispose d'une autorité de certification privée, créez un certificat de signature de code ou certificat de signature SSL à l'aide de l'autorité de certification privée.
3. Utilisez un certificat SSL existant, tel que le certificat du serveur de l'Interface Web.
4. Créez un certificat d'autorité de certification racine et distribuez-le sur les machines utilisateur à l'aide d'un objet de stratégie de groupe ou dans le cadre d'une installation manuelle.

Niveau d'élévation

Lorsque le contrôle d'accès utilisateur (UAC) est activé sur des machines exécutant Windows 10, Windows 8 ou Windows 7, seuls les processus au même niveau d'élévation/d'intégrité que `wfcrun32.exe` peuvent lancer les applications virtuelles.

Exemple 1 :

Lorsque `wfcrun32.exe` est exécuté en mode d'utilisateur normal (pas d'élévation), les autres processus, tels que l'application Citrix Workspace, doivent être exécutés en mode d'utilisateur normal pour lancer des applications via `wfcrun32.exe`.

Exemple 2 :

Lorsque `wfcrun32.exe` est exécuté en mode élevé, les autres processus, tels que l'application Citrix Workspace, le Centre de connexion et les applications tierces utilisant l'objet de client ICA qui sont exécutés en mode non élevé ne peuvent pas communiquer avec `wfcrun32.exe`.

Storebrowse

March 26, 2019

Storebrowse est un utilitaire de ligne de commande léger qui permet l'interaction entre le client et le serveur. Il est utilisé pour authentifier toutes les opérations dans StoreFront et avec Citrix Gateway.

Pour plus d'informations sur l'ancienne version de l'utilitaire Storebrowse pour Citrix Receiver pour Windows, consultez la documentation relative à Storebrowse pour Citrix Receiver pour Windows.

Grâce à l'utilitaire Storebrowse, les administrateurs peuvent automatiser les opérations quotidiennes suivantes :

- Ajouter un magasin
- Énumérer les bureaux et applications Citrix Virtual Apps and Desktops publiés à partir d'un magasin configuré
- Générer manuellement un fichier ICA en sélectionnant un bureau ou une application Citrix Virtual Apps and Desktops publié(e)
- Générer un fichier ICA à l'aide de la ligne de commande Storebrowse
- Lancer l'application publiée

L'utilitaire Storebrowse fait partie du composant Authmanager. Après l'installation de l'application Citrix Workspace, l'utilitaire Storebrowse se trouve dans le dossier d'installation de `AuthManager`.

Vous pouvez vérifier si l'utilitaire Storebrowse est installé avec le composant `Authmanager` en vérifiant le chemin du registre de la manière suivante :

Lorsque l'application Citrix Workspace est installée par les administrateurs :

Sur une machine 32 bits	[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\Inst
Sur une machine 64 bits	[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\A

Lorsque l'application Citrix Workspace est installée par les utilisateurs (et non les administrateurs) :

Sur une machine 32 bits	[HKEY_CURRENT_USER\SOFTWARE\Citrix\AuthManager\Insta
Sur une machine 64 bits	[HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\Au

Exigences

Installez l'application Citrix Workspace version 1808 pour Windows ou version ultérieure pour que l'utilitaire Storebrowse fonctionne de manière transparente entre StoreFront et Citrix Gateway. L'application Citrix Workspace version 1809 requiert une capacité minimale de 530 Mo d'espace disque disponible et 2 Go de RAM.

Compatibility Matrix

L'utilitaire Storebrowse est compatible avec les systèmes d'exploitation suivants :

Système d'exploitation
Windows 10, éditions 32 bits et 64 bits
Windows 8.1, éditions 32 bits et 64 bits
Windows 7 SP1, éditions 32 bits et 64 bits
Windows Thin PC
Windows Server 2016
Windows Server 2012 R2, édition Standard et Datacenter
Windows Server 2012, édition Standard et Datacenter
Windows Server 2008 R2, édition 64 bits
Windows Server 2008 R2, édition 64 bits

Connexions

L'utilitaire Storebrowse prend en charge les types de connexions suivants :

- Magasin HTTP
- Magasin HTTPS
- Citrix Gateway 11.0 et versions ultérieures

> **Remarque :**
>
> L'utilitaire Storebrowse n'accepte pas les informations d'identification à l'aide de la ligne de commande sur un magasin HTTP.

Méthodes d'authentification

Serveurs StoreFront

StoreFront prend en charge différentes méthodes d'authentification pour accéder aux magasins, mais toutes ces méthodes ne sont pas recommandées. Pour des raisons de sécurité, certaines méthodes d'authentification sont désactivées par défaut lors de la création d'un magasin.

- **Nom d'utilisateur et mot de passe** : les utilisateurs peuvent saisir leurs informations d'identification et sont authentifiés lorsqu'ils accèdent à leurs magasins. L'authentification explicite est activée par défaut lorsque vous créez votre premier magasin. Toutes les méthodes d'accès utilisateur prennent en charge l'authentification explicite.
- **Authentification pass-through au domaine** : les utilisateurs doivent s'authentifier sur leur ordinateur Windows membre d'un domaine et leur session est automatiquement ouverte lorsqu'ils accèdent à leurs magasins. Pour pouvoir utiliser cette option, l'authentification pass-through doit être activée lorsque l'application Citrix Workspace est installée sur les machines utilisateur. Pour plus d'informations sur la configuration de l'authentification pass-through au domaine, consultez la section Configuration de l'authentification pass-through.
- **HTTP basique** : l'utilitaire Storebrowse requiert que l'authentification HTTP basique soit activée pour communiquer avec les serveurs StoreFront. Par défaut, cette option est désactivée sur le serveur StoreFront. Vous devez activer la méthode d'authentification HTTP basique.

L'utilitaire Storebrowse prend en charge les méthodes d'authentification via l'une des méthodes suivantes :

- En utilisant le composant `AuthManager` qui est intégré à l'utilitaire Storebrowse. Remarque : vous devez activer la méthode d'authentification HTTP basique sur StoreFront lorsque vous utilisez l'utilitaire Storebrowse. Cela s'applique lorsque l'utilisateur fournit les informations d'identification à l'aide des commandes Storebrowse.
- En utilisant le composant `Authmanager` externe qui peut être inclus avec l'application Citrix Workspace pour Windows.

Prise en charge de Citrix Gateway

Avec la dernière version de l'utilitaire Storebrowse, vous pouvez désormais ajouter une URL Citrix Gateway. Aucune configuration supplémentaire n'est requise dans l'utilitaire Storebrowse pour communiquer avec Citrix Gateway.

Authentification unique (Single Sign-On) avec Citrix Gateway

Outre la prise en charge de Citrix Gateway nouvellement ajoutée, vous pouvez désormais utiliser Single Sign-On. Vous pouvez ajouter un nouveau magasin et énumérer les ressources publiées sans avoir à fournir vos informations d'identification d'utilisateur.

Pour plus d'informations sur la configuration de Single Sign-on avec Citrix Gateway, consultez la section Prise en charge de l'authentification unique (Single Sign-On) avec Citrix Gateway.

> **Remarque :**
>
> Cette fonctionnalité est prise en charge uniquement sur les machines appartenant à un domaine sur lesquelles Citrix Gateway est configurée avec l'authentification unique Single Sign-On.

Lancer une application ou un bureau publié

Vous pouvez maintenant lancer une ressource directement à partir du magasin sans avoir à utiliser un fichier ICA.

Utilisation des commandes

La section suivante fournit des informations détaillées sur les commandes que vous pouvez utiliser depuis l'utilitaire Storebrowse.

-a –addstore

Description :

Ajoute un nouveau magasin. Renvoie l'URL complète du magasin. Si cela échoue, une erreur est signalée.

> **Remarque :**
>
> Vous pouvez ajouter plusieurs magasins à l'aide de l'utilitaire Storebrowse.

Exemple de commande sur StoreFront :

Commande :

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of Storefront
*
```

Exemple :

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -a [https://
my.firstexamplestore.net](https://my.firstexamplestore.net)
```


Exemple de commande sur Citrix Gateway :

Commande :

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of CitrixGateway
*
```

Exemple :

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -a <https://
mysecondexample.com>
```

/?

Description :

Fournit des détails sur l'utilisation de l'utilitaire Storebrowse.

(-l), –liststore

Description :

Répertorie les magasins ajoutés par l'utilisateur.

Exemple de commande sur StoreFront :

```
.\storebrowse.exe -l
```

Exemple de commande sur Citrix Gateway :

```
.\storebrowse.exe -l
```

(-M 0x2000 -E)

Description :

Énumère les ressources disponibles.

Exemple de commande sur StoreFront :

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E
<https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Exemple de commande sur Citrix Gateway :

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E
<https://my.secondexample.net>
```


-q, –quicklaunch

Description :

Génère le fichier ICA requis pour les applications et les bureaux publiés à l'aide de l'utilitaire Storebrowse. L'option quicklaunch nécessite une URL de lancement en tant qu'entrée avec l'URL du magasin, qui peut être le serveur StoreFront ou l'URL de Citrix Gateway. Le fichier ICA est généré dans le répertoire `%LocalAppData%\Citrix\Storebrowse\cache`.

Vous pouvez obtenir l'URL de lancement de toutes les applications et bureaux publiés en exécutant la commande suivante :

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/
discovery
```

Une URL de lancement ressemble généralement à celle-ci :

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix/
Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

Exemple de commande sur StoreFront :

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q { Launch_URL_of_publ
 apps and desktops } <https://my.firstexamplestore.net/Citrix/Store/resources
/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix
/Store/discovery>
```

Exemple de commande sur Citrix Gateway :

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q { Launch_URL_of_publ
 apps and desktops } <https://my.secondexmaplestore.com>
```

-L, –launch

Description :

Génère le fichier ICA requis pour les applications et les bureaux publiés à l'aide de l'utilitaire Storebrowse. L'option launch nécessite le nom de la ressource ainsi que l'URL du magasin, qui peut être le serveur StoreFront ou l'URL de Citrix Gateway. Le fichier ICA est généré dans le répertoire `%LocalAppData%\Citrix\Storebrowse\cache`.

Vous pouvez obtenir le nom d'affichage des applications et bureaux publiés en exécutant la commande suivante :

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/
discovery
```

Cette commande entraîne la sortie suivante :


```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix/
Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

Le nom en gras dans la sortie ci-dessus est utilisé comme paramètre d'entrée pour l'option launch.

Exemple de commande sur StoreFront :

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L  "{
Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Exemple de commande sur Citrix Gateway :

```
<.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L { Resource_Name
 } https://my.secondexamplestore.com>
```

-S, –sessionlaunch

Description :

Vous pouvez ajouter le magasin, énumérer les ressources publiées (applications et bureaux) et lancer la ressource avec cette commande unique. Cette option prend en compte les paramètres suivants : Nom d'utilisateur, Mot de passe, Domaine, Nom convivial de la ressource à lancer et URL du magasin. Toutefois, si l'utilisateur ne fournit pas les informations d'identification, une invite `AuthManager` est envoyée pour entrer ces informations, puis le lancement de la ressource se produit.

Vous pouvez obtenir le nom de la ressource des applications et bureaux publiés en exécutant la commande suivante :

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/
discovery
```

Cette commande entraîne la sortie suivante :

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix/
Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

Le nom en gras dans la sortie ci-dessus est utilisé comme paramètre d'entrée pour l'option `-S`.

Exemple de commande sur StoreFront :

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S  "{
Friendly_Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/
discovery >
```

Exemple de commande sur Citrix Gateway :

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S { Friendly_Resource_
 } <https://my.secondexamplestore.com>
```


-f, –filefolder

Description :

Génère le fichier ICA requis dans le chemin personnalisé tel qu'il est défini dans l'option –f pour les applications et les bureaux publiés à l'aide de l'utilitaire Storebrowse.

L'option launch nécessite un nom de dossier avec le nom de la ressource comme paramètre d'entrée, ainsi que l'URL du magasin, qui peut être le serveur StoreFront ou l'URL de Citrix Gateway.

Exemple de commande sur StoreFront :

```
.\storebrowse.exe -f "C:\Temp\Launch.ica" -L "Resource_Name" { Store }
```

Exemple de commande sur Citrix Gateway :

```
.\storebrowse.exe -f "C:\Temp\Launch.ica" -L "Resource_Name" { NSG_URL }
```

-t, –traceauthentication

Description :

Génère des journaux pour le composant `AuthManager` intégré à l'utilitaire Storebrowse. Les journaux sont générés uniquement si l'utilitaire Storebrowse utilise un composant `AuthManager` intégré. Les journaux sont générés dans le répertoire `localappdata%\Citrix\Storebrowse\logs`.

Remarque : cette option ne peut pas être le dernier paramètre répertorié dans la ligne de commande de l'utilisateur.

Exemple de commande sur StoreFront :

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a {
StoreURL }
```

Exemple de commande sur Citrix Gateway :

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a {
NSG_URL }
```

-d, –deletestore

Description :

Supprime le magasin StoreFront ou Citrix Gateway existant.

Exemple de commande sur StoreFront :

```
.\storebrowse.exe -d https://my.firstexamplestore.net/Citrix/Store/discovery
```

Exemple de commande sur Citrix Gateway :


```
.\storebrowse.exe -d https://my.secondexmaplestore.com
```

Prise en charge de l'authentification unique (Single Sign-On) avec Citrix Gateway

Single Sign-on vous permet de vous authentifier auprès d'un domaine et d'utiliser Citrix Virtual Apps and Desktops mis à disposition par ce domaine sans procéder à une nouvelle authentification pour chaque application ou bureau. Lorsque vous ajoutez un magasin à l'aide de l'utilitaire Storebrowse, vos informations d'identification sont transmises au serveur Citrix Gateway avec les applications et bureaux Citrix Virtual Apps and Desktops énumérés pour vous, y compris les paramètres du menu Démarrer. Après avoir configuré Single Sign-on, vous pouvez ajouter le magasin, énumérer les applications et bureaux Citrix Virtual Apps and Desktops et lancer les ressources nécessaires sans saisir à plusieurs reprises vos informations d'identification.

Cette fonctionnalité est prise en charge sur Citrix Gateway version 11 et ultérieure.

Conditions préalables :

Pour plus d'informations sur les conditions préalables à la configuration de Single Sign-On pour Citrix Gateway, consultez la section Configurer l'authentification pass-through au domaine.

La fonctionnalité Single Sign-On peut être activée avec Citrix Gateway via le modèle d'administration d'objet de stratégie de groupe.

> **Remarque :**
>
> Lorsque vous mettez à niveau Citrix Receiver vers l'application Citrix Workspace ou installez l'application Citrix Workspace pour la première fois, vous devez ajouter les derniers fichiers de modèle à l'objet de stratégie de groupe local. Pour plus d'informations sur l'ajout des fichiers de modèle à l'objet de stratégie de groupe local, consultez la section Configuration du modèle d'administration d'objet de stratégie de groupe. En cas de mise à niveau, les paramètres existants sont conservés lors de l'importation des derniers fichiers.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Authentification utilisateur** > **Single Sign-on pour Citrix Gateway**.
3. Utilisez les options Activer/Désactiver pour activer ou désactiver l'option Single Sign-On.
4. Cliquez sur **Appliquer**, puis sur **OK**.
5. Redémarrez la session de l'application Citrix Workspace pour que les modifications prennent effet.

Limitations :

- La méthode d'authentification HTTP de base doit être activée sur le serveur StoreFront pour les opérations d'injection d'informations d'identification avec l'utilitaire Storebrowse.
- Si vous avez un magasin HTTP et que vous essayez de vous connecter au magasin à l'aide de l'utilitaire pour énumérer ou lancer les applications et les bureaux Citrix Virtual Apps and Desktops publiés, l'injection des informations d'identification à l'aide de la ligne de commande n'est pas prise en charge. Pour résoudre ce problème, utilisez le module externe `AuthManager` qui est déclenché lorsque vous ne fournissez pas d'informations d'identification à l'aide de la ligne de commande.
- L'utilitaire Storebrowse prend actuellement en charge uniquement la passerelle Citrix Gateway configurée pour un seul magasin sur le serveur StoreFront.
- L'injection d'informations d'identification dans l'utilitaire Storebrowse ne fonctionne que si Citrix Gateway est configuré avec l'authentification à facteur unique.
- Les options de ligne de commande `Username (-U)`, `Password (-P)` et `Domain (-D)` de l'utilitaire Storebrowse sont sensibles à la casse et doivent être uniquement entrées en majuscules.

Citrix Workspace Desktop Lock

February 20, 2019

Vous pouvez utiliser Citrix Workspace Desktop Lock lorsque vous n'avez pas besoin d'interagir avec le bureau local. Vous pouvez utiliser Desktop Viewer (si cette option est activée), mais seul le jeu d'options requis est disponible dans la barre d'outils : Ctrl+Alt+Suppr, Préférences, Périphériques et Déconnecter.

L'application Citrix Workspace pour Windows avec Desktop Lock fonctionne sur des machines appartenant à un domaine et sur lesquelles SSON est activé et le magasin est configuré. Il peut également être utilisé sur des machines n'appartenant pas à un domaine sur lesquelles le SSON n'est pas activé. Il ne prend pas en charge les sites PNA. Les versions antérieures de Desktop Lock ne sont pas prises en charge lors de la mise à niveau vers Citrix Receiver pour Windows 4.2 ou versions ultérieures.

Vous devez installer l'application Citrix Workspace pour Windows avec l'indicateur `/includeSSON`. Vous devez configurer le magasin et le Single Sign-On, au choix avec le fichier adm/admx ou l'option cmdline. Pour plus d'informations, consultez la section Installer et configurer Citrix Receiver à l'aide de la ligne de commande.

Installez ensuite Citrix Workspace Desktop Lock en tant qu'administrateur à l'aide du fichier `CitrixWorkspaceDesktopLock.msi` disponible sur la page des téléchargements de Citrix.

Configuration système requise

- Microsoft Visual C++ 2005 avec Service Pack 1 Redistributable Package Pour plus d'informations, consultez la page de téléchargement de Microsoft.
- Pris en charge sous Windows 7 (y compris Embedded Edition), Windows 7 Thin PC, Windows 8, Windows 8.1 et Windows 10 (Anniversary Update incluse).
- Se connecte à StoreFront via des protocoles natifs uniquement.
- Postes de travail appartenant et n'appartenant pas à un domaine
- Les machines utilisateur doivent être connectées à un réseau local (LAN) ou un réseau étendu (WAN).

Local App Access

> **Important**
>
> L'activation de Local App Access peut permettre l'accès au bureau local, sauf si un verrouillage a été appliqué avec le modèle d'objet de stratégie de groupe ou une stratégie similaire. Consultez Configurer Local App Access et la redirection d'adresse URL dans Citrix Virtual Apps and Desktops pour plus d'informations.

Utilisation de Citrix Workspace Desktop Lock

- Vous pouvez utiliser Citrix Workspace Desktop Lock avec les fonctionnalités suivantes de l'application Citrix Workspace :
  - 3Dpro, Flash, USB, HDX Insight, plug-in Microsoft Lync 2013 et Local App Access
  - Authentification de domaine, à deux facteurs ou par carte à puce uniquement
- Fermeture de la session Citrix Workspace Desktop Lock sur le périphérique d'extrémité
- La redirection Flash est désactivée sur Windows 8 et versions supérieures. La redirection Flash est activée sur Windows 7.
- Desktop Viewer est optimisé pour Citrix Workspace Desktop Lock sans les propriétés Home, Restore, Maximize et Display.
- Ctrl+Alt+Suppr est disponible sur la barre d'outils Viewer.
- La plupart des touches de raccourci des fenêtres sont transmises à la session à distance, à l'exception de Windows+L. Pour plus d'informations, consultez la section Transmission des touches de raccourci Windows à la session distante.
- Ctrl+F1 déclenche Ctrl+Alt+Suppr lorsque vous désactivez la connexion ou Desktop Viewer pour les connexions de bureau.

Installer Citrix Workspace Desktop Lock

Cette procédure installe l'application Citrix Workspace pour Windows de telle sorte que les bureaux virtuels soient affichés via Citrix Workspace Desktop Lock. Pour les déploiements qui utilisent des cartes à puce, consultez la section
Pour configurer des cartes à puce à utiliser avec les machines exécutant Receiver Desktop Lock.

1. Citrix vous recommande d'utiliser un compte d'administrateur local.
2. À l'invite de commandes, exécutez la commande suivante (dans l'application Citrix Workspace et Plug-ins > Windows > dossier de l'application Citrix Workspace pour Windows sur le support d'installation).

   Par exemple :

   ```
   CitrixWorkspaceApp.exe
         /includeSSON
   STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/
      discovery;on;Desktop Store"
   ```

   Pour plus d'informations sur la commande, consultez la documentation relative à l'installation de l'application Citrix Workspace dans la section Configure and install Citrix Worksapce for Windows using command-line parameters.
3. Dans le même dossier du support d'installation, cliquez deux fois sur `CitrixReceiverDesktopLock.MSI`. L'assistant Desktop Lock apparaît. Suivez les invites.
4. Une fois l'installation terminée, redémarrez la machine utilisateur. Si vous avez l'autorisation d'accéder à un bureau et que vous ouvrez une session en tant qu'utilisateur de domaine, la machine s'affiche à l'aide de Citrix Workspace Desktop Lock.

Pour vous permettre d'administrer la machine utilisateur après l'installation, le compte utilisé pour installer `CitrixWorkspaceDesktopLock.msi` est exclu du shell de remplacement. Si ce compte est supprimé ultérieurement, vous ne pourrez pas ouvrir de session pour administrer la machine.

Pour exécuter une **installation silencieuse** de Citrix Workspace Desktop Lock, utilisez la ligne de commande suivante :

```
msiexec /i CitrixWorkspaceDesktopLock.msi /qn
```

Configurer Citrix Workspace pour Windows Desktop Lock

N'accordez l'accès qu'à un bureau virtuel exécutant Citrix Workspace Desktop Lock à chaque utilisateur.

À l'aide des stratégies Active Directory, empêchez les utilisateurs de mettre les bureaux virtuels en veille prolongée.

Utilisez le même compte d'administrateur pour la configuration de Citrix Workspace Desktop Lock que pour son installation.

- Assurez-vous que les fichiers receiver.admx (ou receiver.adml) et receiver_usb.admx (.adml) sont chargés dans la stratégie de groupe (où les stratégies apparaissent dans Configuration ordinateur ou Configuration utilisateur > Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix). Les fichiers .admx sont situés à l'adresse %Program Files%\Citrix\ICA Client\Configuration\.
- Préférences USB : lorsqu'un utilisateur connecte un périphérique USB, ce périphérique est automatiquement envoyé sur le bureau virtuel ; aucune intervention de l'utilisateur n'est requise. Le bureau virtuel est responsable du contrôle du périphérique USB et de son affichage dans l'interface utilisateur.
  - Activez la règle de stratégie USB.
  - Dans l'application Citrix Workspace > Accès à distance des périphériques clients > Utilisation à distance de dispositifs USB génériques, activez et configurez les stratégies Périphériques USB existants et Nouveaux périphériques USB.
- Mappage de lecteur : dans l'application Citrix Workspace > Accès à distance des périphériques clients, activez et configurez la stratégie de mappage du lecteur client.
- Microphone : dans l'application Citrix Workspace > Accès à distance des périphériques clients, activez et configurez la stratégie du microphone client.

Configurer des cartes à puce à utiliser avec les machines exécutant Citrix Workspace pour Windows Desktop Lock

1. Configurer StoreFront.
   a) Configurez le service XML pour utiliser la résolution d'adresse DNS pour la prise en charge Kerberos.
   b) Configurez des sites StoreFront pour l'accès HTTPS, créez un certificat de serveur signé par votre autorité de certification de domaine et ajoutez la liaison HTTPS au site Web par défaut.
   c) Assurez-vous que l'authentification pass-through avec carte à puce est activée (activée par défaut).
   d) Activez Kerberos.
   e) Activez Kerberos et Authentification pass-through avec carte à puce.
   f) Activez Accès anonyme sur le site Web IIS par défaut et utilisez Authentification Windows intégrée.
   g) Assurez-vous que le site Web IIS par défaut ne nécessite pas SSL et ignore les certificats clients.
2. Utilisez la console de gestion des stratégies de groupe pour configurer les stratégies d'ordinateur local sur la machine utilisateur.

a) Importez le modèle Receiver.admx depuis %Program Files%\Citrix\ICA Client\Configuration\.
b) Développez Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Workspace > Authentification de l'utilisateur.
c) Activez Authentification par carte à puce.
d) Activez Nom de l'utilisateur et mot de passe locaux.

3. Configurez la machine utilisateur avant d'installer Citrix Workspace Desktop Lock.
   a) Ajoutez l'adresse URL du Delivery Controller à la liste Sites de confiance de Windows Internet Explorer.
   b) Ajoutez l'adresse URL pour le premier groupe de mise à disposition à la liste Sites de confiance d'Internet Explorer dans le formulaire de bureau://nom-groupe-mise-à-disposition.
   c) Configurez Internet Explorer afin d'utiliser la connexion automatique aux sites de confiance.

Lorsque Citrix Workspace Desktop Lock est installé sur la machine utilisateur, une stratégie de retrait de carte à puce cohérente est appliquée. Par exemple, si la stratégie Windows de retrait de carte à puce est définie sur Forcer la fermeture de session pour le bureau, l'utilisateur doit également fermer sa session sur la machine utilisateur, quelle que soit la stratégie Windows définie pour le retrait de la carte à puce. Cela évite de laisser la machine utilisateur dans un état incohérent. Cela s'applique uniquement aux machines utilisateur avec Citrix Workspace Desktop Lock.

Supprimer Citrix Workspace Desktop Lock

Veillez à supprimer les deux composants répertoriés ci-dessous.

1. Ouvrez une session avec le compte d'administrateur local qui a été utilisé pour installer et configurer Citrix Workspace Desktop Lock.
2. À partir de la fonctionnalité Windows pour la suppression ou la modification de programmes :
   - Supprimez Citrix Workspace Desktop Lock.
   - Supprimez l'application Citrix Workspace pour Windows.

Transmission des touches de raccourci Windows à la session distante

La plupart des touches de raccourci Windows sont transmises à la session distante. Cette section présente certains des raccourcis les plus courants.

Windows

- Win+D : réduit toutes les fenêtres sur le bureau.
- Alt+Tab : change la fenêtre active.
- Ctrl+Alt+Suppr : via Ctrl+F1 et la barre d'outils Desktop Viewer.

- Alt+Maj+Tab
- Windows+Tab
- Windows+Maj+Tab
- Windows+toutes les touches de caractères

Windows 8

- Win+C : ouvre la barre de charme.
- Win+Q : ouvre la section Recherche de la barre de charme.
- Win+H : affiche la section Partager la barre de charme.
- Win+K : affiche la section Périphériques de la barre de charme.
- Win+I : affiche la section Paramètres de la barre de charme.
- Win+Q : permet de rechercher des applications.
- Win+W : permet de rechercher des paramètres.
- Win+F : permet de rechercher des fichiers.

Applications Windows 8

- Win+Z : affiche les options d'applications
- Win+. : ancre une application sur la gauche.
- Win + MAJ +. : ancre une application sur la droite.
- Ctrl+Tab : permet de parcourir l'historique des applications.
- Alt+F4 : ferme une application.

Bureau

- Win+D : ouvre le bureau.
- Win+, : passage furtif sur le bureau.
- Win+B : retour au bureau.

Autre

- Win+U : ouvre les options d'ergonomie.
- Ctrl+Échap : ouvre le menu Démarrer.
- Win+Entrée : ouvre le narrateur Windows.
- Win+X : permet d'accéder aux outils de menu du système.
- Win+Imprécran : permet de faire une copie d'écran et d'enregistrer les images.
- Win+Tab : permet de basculer entre les applications.
- Win+T : affiche un aperçu des fenêtres dans la barre des tâches.

SDK et API

March 18, 2019

SDK de déclaration d'identité du certificat

Grâce au SDK de déclaration d'identité de certificat, les développeurs peuvent créer un plug-in qui permet à l'application Citrix Workspace de s'authentifier auprès du serveur StoreFront à l'aide du certificat installé sur la machine cliente. La déclaration d'identité du certificat permet de déclarer l'identité de la carte à puce de l'utilisateur à un serveur StoreFront sans effectuer d'authentification basée sur une carte à puce.

Pour plus d'informations, consultez la page Certificate Identity Declaration SDK for Citrix Workspace app for Windows.

SDK Citrix Common Connection Manager

Le SDK Common Connection Manager (CCM) fournit un ensemble d'API natives qui vous permettent d'interagir et d'effectuer des opérations de base à l'aide de scripts. Ce SDK ne nécessite pas de téléchargement distinct, car il fait partie du package d'installation de l'application Citrix Workspace pour Windows.

> **Remarque :**
>
> Certaines des API liées au lancement nécessitent le fichier ICA pour initier le processus de lancement sur les sessions Citrix Virtual Apps and Desktops.

Les capacités du SDK CCM incluent :

- Lancement de session
  - Permet de lancer des applications et des postes de travail à l'aide du fichier ICA généré.
- Déconnexion de session
  - Similaire à l'opération de déconnexion à l'aide du Centre de connexion. La déconnexion peut s'appliquer à toutes les sessions ou à un utilisateur spécifique.
- Fermeture de session
  - Similaire à l'opération de fermeture de session à l'aide du Centre de connexion. La fermeture peut s'appliquer à toutes les sessions ou à un utilisateur spécifique.
- Informations de session
  - Fournit différentes méthodes pour obtenir des informations liées à la connexion des sessions lancées. Cela inclut les sessions de bureau, d'application et d'application transparente inverse

Pour plus d'informations sur la documentation du SDK, veuillez consulter Programmers guide to Citrix CCM SDK.

SDK du canal virtuel Citrix

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

Le SDK du canal virtuel offre ce qui suit :

- L'interface Citrix Virtual Driver Application Programming Interface (VDAPI) est utilisée avec les fonctions de canal virtuel dans le SDK de l'API Citrix Server (WFAPI SDK) pour créer de nouveaux canaux virtuels. La prise en charge de canal virtuel fournie par VDAPI est conçue pour faciliter l'écriture de vos propres canaux virtuels.
- L'API de contrôle de Windows, qui améliore l'expérience visuelle et la prise en charge des applications tierces intégrées avec ICA.
- Un code source opérationnel pour exemples de programmes de canal virtuel qui illustrent les techniques de programmation.
- Le SDK de canal virtuel requiert le SDK WFAPI pour écrire sur le côté serveur du canal virtuel.

Pour plus d'informations, veuillez consulter la page Citrix Virtual Channel SDK for Citrix Workspace app for Windows.

API Fast Connect 3 Credential Insertion

L'API Fast Connect 3 Credential Insertion offre une interface qui fournit des informations d'identification d'utilisateur à la fonctionnalité Single Sign-On (SSON). Cette fonctionnalité est disponible dans l'application Citrix Workspace pour Windows versions 4.2 et ultérieures. À l'aide de cette API, les partenaires Citrix peuvent fournir des produits d'authentification et SSO utilisant StoreFront ou l'Interface Web pour connecter les utilisateurs à des applications ou bureaux virtuels, puis les déconnecter de ces sessions.

Pour plus d'informations, veuillez consulter la page Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows.

Référence des paramètres ICA

October 8, 2018

Référence des paramètres ICA

La référence des paramètres de fichier ICA inclut des paramètres de registre et des listes de paramètres de fichiers ICA, permettant aux administrateurs de personnaliser le comportement de l'application Citrix Workspace. Vous pouvez également l'utiliser pour corriger des comportements inattendus de l'application.

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