Application Citrix Workspace 1912 LTSR pour Windows

Contents

À propos de cette version

September 25, 2023

Nouveautés dans la version 1912

La mise à jour cumulative 7 (CU7) est la mise à jour la plus récente de la version LTSR 1912.

Améliorations apportées à Microsoft Teams

L'amélioration suivante de Microsoft Teams est prise en charge pour CU6 et les versions ultérieures :

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

Les améliorations suivantes de Microsoft Teams sont prises en charge pour CU5 et les versions ultérieures :

- Améliorations apportées au partage d'écran - Lorsque vous partagez votre écran, seul l'écran Desktop Viewer est capturé au format bitmap natif.
- Les interlocuteurs peuvent désormais voir le pointeur de la souris du présentateur dans une session de partage d'écran.
- Amélioration de la lecture vidéo.
- Amélioration apportées aux performances et à la fiabilité.
- Le moteur de média WebRTC respecte désormais le serveur proxy configuré sur la machine cliente.
- Amélioration des configurations de l'annulation de l'écho, du contrôle automatique du gain, de la suppression du bruit : si Microsoft Teams configure ces options, Microsoft Teams redirigé par Citrix respecte les valeurs configurées. Sinon, ces options sont définies sur True par défaut.
- Vous pouvez désormais configurer une interface réseau préférée pour le trafic multimédia.

  Accédez à `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` et créez une clé appelée `NetworkPreference`(REG_DWORD).

  Sélectionnez l'une des valeurs suivantes selon les besoins :

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

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

- Vous pouvez désormais désactiver le module de périphérique audio 2 (ADM2) afin que l'ancien module de périphérique audio (ADM) soit utilisé pour les microphones à quatre canaux. Cela permet de résoudre les problèmes liés aux microphones dans un appel.

  Pour désactiver ADM2, accédez à `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`, créez une clé appelée `DisableADM2` (REG_DWORD) et définissez la valeur sur 1.

- `DirectWShow` est maintenant le moteur de rendu par défaut.

  Pour modifier le moteur de rendu par défaut, procédez comme suit :

  - Lancez l'Éditeur du Registre.
  - Accédez à l'emplacement de clé suivant : `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`.
  - Mettez à jour la valeur suivante : `"UseDirectShowRendererAsPrimary"=dword:00000000`.

    Autres valeurs possibles :

    * 0: Media Foundation
    * 1: DirectShow (par défaut)

  - Relancez l'application Citrix Workspace.

> **Remarque :**
>
> - Les améliorations sont prises en charge uniquement sur les points de terminaison du système d'exploitation Desktop Microsoft Windows 10.
> - Les améliorations ne sont pas prises en charge sur les points de terminaison des systèmes d'exploitation Microsoft Windows 7 et 8.
> - La prise en charge de l'amélioration est déterminée lors de l'installation du package de l'application Citrix Workspace. Nous vous recommandons de désinstaller l'application Citrix Workspace lorsque vous mettez à niveau le système d'exploitation Microsoft Windows de la version 7 vers la version 10.

Protection des applications

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

La protection des applications est une fonctionnalité complémentaire qui offre une sécurité renforcée lors de l'utilisation de Citrix Virtual Apps and Desktops. Elle limite le risque d'être infecté par des programmes malveillants d'enregistrement de frappe et de capture d'écran. La protection des applications empêche l'exfiltration d'informations confidentielles telles que les informations d'identification de l'utilisateur et les informations sensibles affichées à l'écran. Cette fonctionnalité empêche les utilisateurs et les attaquants de prendre des captures d'écran et d'utiliser des enregistreurs de frappe pour récupérer et exploiter des informations sensibles.

> **Remarque :**
>
> Citrix recommande d'utiliser uniquement l'application Citrix Workspace native pour lancer une session protégée.

La protection des applications est configurée entre StoreFront et le Controller à l'aide du Controller. Pour plus d'informations sur la configuration de la protection des applications sur le Controller, consultez la documentation Protection des applications. Cette configuration est ensuite appliquée à l'application Citrix Workspace en incluant le composant de protection des applications à l'aide de l'une des méthodes suivantes :

- Interface utilisateur graphique
- Interface de ligne de commande

Vous pouvez inclure le composant de protection des applications à la fois lors de l'installation de l'application Citrix Workspace ou de l'installation à la demande.

> **Remarque :**
>
> - Cette fonctionnalité est prise en charge uniquement sur les systèmes d'exploitation Microsoft Windows Desktop tels que Windows 10, Windows 8.1 et Windows 7.

> - Cette fonctionnalité n'est pas prise en charge par le protocole de bureau distant (RDP ou Remote Desktop Protocol).

Pour plus d'informations sur la configuration de la protection des applications dans l'application Citrix Workspace, consultez la section Protection des applications.

Amélioration de la protection des applications Précédemment, lorsque vous essayiez de prendre une capture d'écran d'une fenêtre protégée, l'écran entier, y compris les applications non protégées en arrière-plan, était occulté.

Maintenant, lorsque vous prenez une copie d'écran à l'aide d'un outil de capture d'écran, seule la fenêtre protégée est occultée ou masquée. Vous pouvez prendre une copie d'écran de la zone située en dehors de la fenêtre protégée, sauf en mode non-Aero où l'écran entier est occulté.

Toutefois, si vous utilisez la touche **Impr écran** pour capturer une copie d'écran, vous devez quitter l'application Citrix Workspace.

En outre, cette version résout certains problèmes pour améliorer la fonctionnalité de protection des applications.

Amélioration apportée au programme d'installation

Dans les versions antérieures, si un administrateur tentait d'installer l'application Citrix Workspace sur un système sur lequel une instance de l'application était installée par l'utilisateur, l'installation était bloquée.

Avec cette version, les administrateurs peuvent désormais remplacer l'instance de l'application Citrix Workspace installée par l'utilisateur et poursuivre l'installation.

Amélioration des mises à jour Citrix Workspace

Dans les versions antérieures, si l'application Citrix Workspace était installée par un administrateur, un non-administrateur ne pouvait pas la mettre à jour.

Avec cette version, un non-administrateur peut mettre à jour l'application Citrix Workspace sur une instance installée par un administrateur. Pour ce faire, cliquez avec le bouton droit de la souris sur l'icône de l'application Citrix Workspace dans la zone de notification et sélectionnez Rechercher les mises à jour.

> **Remarque :**

> L'option **Rechercher les mises à jour** est désormais disponible sur les instances de l'application Citrix Workspace installées par l'utilisateur et celles installées par l'administrateur.

Prise en charge du proxy sortant

Smart Control permet aux administrateurs de définir des stratégies avancées pour configurer et appliquer les attributs d'environnement utilisateur pour les applications et les bureaux virtuels à l'aide de Citrix Gateway. Par exemple, vous pouvez interdire aux utilisateurs de mapper des lecteurs sur leurs bureaux distants. Cela peut être réalisé à l'aide de la fonctionnalité Smart Control de Citrix Gateway.

Toutefois, le scénario change lorsque l'application Citrix Workspace et Citrix Gateway appartiennent à des comptes d'entreprise distincts. Dans de tels scénarios, le domaine client ne peut pas appliquer la fonctionnalité Smart Control car la passerelle n'existe pas sur le domaine client. Au lieu de cela, vous pouvez utiliser le proxy ICA sortant. Le proxy ICA sortant vous permet d'utiliser la fonctionnalité Smart Control même lorsque l'application Citrix Workspace et Citrix Gateway sont déployées dans différentes organisations.

L'application Citrix Workspace prend en charge les lancements de session à l'aide du proxy LAN Citrix ADC. Un seul proxy statique peut être configuré ou le serveur proxy peut être sélectionné lors de l'exécution à l'aide du plug-in de proxy sortant.

Vous pouvez configurer les proxys sortants à l'aide des méthodes suivantes :

- Proxy statique : le serveur proxy est configuré en fournissant un nom d'hôte proxy et un numéro de port.
- Proxy dynamique : un serveur proxy unique peut être sélectionné parmi un ou plusieurs serveurs proxy à l'aide de la DLL du plug-in de proxy.

Vous pouvez configurer le proxy sortant à l'aide du modèle d'administration de l'objet de stratégie de groupe et de l'Éditeur du Registre.

Pour plus d'informations sur le proxy sortant, consultez la section Prise en charge du proxy ICA sortant dans la documentation Citrix Gateway.

Pour plus d'informations sur la configuration du proxy sortant dans l'application Citrix Workspace, consultez la section Proxy sortant.

Fichiers binaires du navigateur Citrix intégré

Cette version n'installe plus le navigateur Citrix intégré. Dans les cas où vous effectuez une mise à niveau vers la version 1912, le navigateur Citrix intégré est supprimé.

En l'absence du navigateur Citrix intégré, les fonctionnalités suivantes changent :

- La redirection du contenu du navigateur ne fonctionne pas.
- Les applications SaaS et Web ne sont pas lancées à l'aide du navigateur Citrix intégré. Au lieu de cela, elles sont lancées dans Citrix Secure Browser Service.

Amélioration apportée au partage de bureau avec Microsoft Teams

Lorsque vous partagez votre espace de travail à l'aide de Microsoft Teams, l'application Citrix Workspace affiche une bordure rouge qui entoure la zone du moniteur en cours de partage. Vous pouvez partager uniquement la fenêtre Desktop Viewer ou n'importe quelle fenêtre locale superposée au-dessus de celle-ci. Lorsque vous réduisez la fenêtre Desktop Viewer, le partage d'écran est suspendu.

Estimation des performances au niveau du codage du point de terminaison sur Microsoft Teams

Lorsque le processus HdxTeams.exe (le moteur multimédia WebRTC intégré dans l'application Citrix Workspace qui gère la redirection Microsoft Teams) est lancé, la meilleure résolution de codage que le processeur du point de terminaison peut gérer sans surcharge est estimée. Les valeurs possibles sont 240p, 360p, 720p et 1080p.

Le processus d'estimation des performances (également appelé `webrtcapi.EndpointPerformance`) s'exécute lorsque HdxTeams.exe est démarré. Le code macroblock détermine la meilleure résolution possible avec le point de terminaison particulier. La résolution la plus élevée possible est ensuite incluse lors de la négociation du codec entre les homologues, ou entre l'homologue et le serveur de conférence.

Pour plus d'informations sur la configuration du codage du point de terminaison, consultez la section Estimation des performances au niveau du codage du point de terminaison sur Microsoft Teams.

Pour de plus amples informations, consultez Optimisation Microsoft Teams dans la documentation de Citrix Virtual Apps and Desktops.

Améliorations apportées à Citrix Analytics Service

Avec cette version, l'application Citrix Workspace transmet en toute sécurité l'adresse IP publique du dernier saut réseau à Citrix Analytics Service. Ces données sont collectées à chaque lancement de session. Cela aide Citrix Analytics Service à analyser si les problèmes de performances sont liés à des zones géographiques spécifiques. Par défaut, les journaux d'adresses IP sont envoyés à Citrix Analytics Service. Toutefois, vous pouvez désactiver cette option sur l'application Citrix Workspace à l'aide de l'éditeur du Registre.

Pour désactiver la transmission du journal d'adresses IP, accédez au chemin d'accès du Registre suivant et définissez la clé `SendPublicIPAddress` sur **Désactivé**.

- Sur les machines Windows 64 bits, accédez à : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`.
- Sur les machines Windows 32 bits, accédez à : `HKEY_LOCAL_MACHINE\SOFTWARE \Citrix\Dazzle`.

> **Remarque :**
>
> - Bien que l'application Citrix Workspace transmette toutes les adresses IP sur lesquelles elle est lancée, la transmission d'adresses IP se produit dans le meilleur des cas. Certaines adresses peuvent ne pas être exactes.
> - Dans les environnements clients fermés, où les points de terminaison fonctionnent dans un intranet, assurez-vous que l'URL `https://locus.analytics.cloud.com/api/locateip` est placée sur liste blanche sur le point de terminaison.

Pour plus d'informations sur la façon dont Performance Analytics utilise ces informations, consultez Recherche en libre-service des performances.

Problèmes résolus

November 2, 2023

Application Citrix Workspace 1912 LTSR CU7 pour Windows

Comparé à : application Citrix Workspace 1912 LTSR CU6

Redirection de contenu

- Lorsque Desktop Viewer est défini sur le mode plein écran et que le navigateur par défaut est agrandi sur le terminal, la fonctionnalité de redirection bidirectionnelle du contenu peut ne pas mettre la fenêtre du navigateur Web par défaut local au premier plan. Le problème se produit avec les navigateurs Web par défaut locaux autres qu'Internet Explorer. [CVADHELP-19041]

Ouverture de session/Authentification

- Les tentatives d'ajout d'URL Citrix Gateway peuvent échouer par intermittence avec ce message d'erreur :

Impossible de contacter le service d'authentification.

[CVADHELP-19415]

Session/Connexion

- L'utilisation de l'utilitaire Storebrowse pour énumérer les ressources pour l'URL Citrix Gateway peut échouer lorsqu'au moins l'un des Delivery Controller configurés n'est pas accessible. [CVADHELP-15416]
- Lorsque Citrix IME est activé, certaines applications tierces peuvent ne pas répondre et le lancement d'applications dans une session utilisateur peut échouer. Le problème se produit en raison de la défaillance du module CtxIme. [CVADHELP-18511]
- Toute tentative d'actualisation ou de lancement d'une application entraîne le message d'erreur **Impossible de contacter le magasin**. Ce problème se produit lorsque la récupération de la description du raccourci pour des applications spécifiques auxquelles vous êtes abonné échoue.

  Vos applications ne sont pas disponibles pour l'instant. Réessayez dans quelques minutes ou contactez votre service d'assistance avec cette information : impossible de contacter le magasin.

  [CVADHELP-18736]
- Les tentatives de lancement d'une session utilisateur peuvent échouer après l'utilisation de la commande **selfservice.exe —init —ipoll —exit**. [CVADHELP-19095]
- Avec ce correctif, vous pouvez définir **TWITaskbarGroupingMode** sur **GroupNone** dans `HKEY_CURRENT_USER` ou `HKEY_LOCAL_MACHINE`. La clé **TWITaskbarGroupingMode** est disponible sous, par exemple, HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows. [CVADHELP-19106]

Expérience utilisateur

- Lorsque la stratégie Sans perte si possible est activée dans un environnement comportant plusieurs moniteurs, le fait d'étendre l'écran sur un ordinateur portable et un moniteur externe peut entraîner une distorsion de l'image. [CVADHELP-19065]

Application Citrix Workspace 1912 LTSR CU6 pour Windows

Comparé à : application Citrix Workspace 1912 LTSR CU5

Problèmes liés aux machines clientes

- Dans une session de l'application Citrix Workspace, lorsque vous démarrez une vidéo YouTube ou un appel Microsoft Teams, puis déconnectez le casque, la session peut cesser de répondre. [CVADHELP-17629]

Installation, désinstallation, mise à niveau

- Lorsque vous mettez à niveau l'application Citrix Workspace pour Windows de la version CU4 vers la version CU5 sans installer l'outil self-service, l'invite suivante peut s'afficher :

  Tentative de mise à niveau à partir d'une version non prise en charge

  Citrix Workspace désinstalle automatiquement votre ancienne version et supprime tous vos paramètres ; vous pourrez restaurer ceux-ci ultérieurement. Sinon, vous devrez tout supprimer manuellement. Cliquez sur OK pour continuer.

  [CVADHELP-18790]

Ouverture de session/Authentification

- L'ouverture de session sur Citrix Gateway à l'aide d'un mot de passe incorrect permet à Storebrowse d'effectuer plusieurs tentatives d'authentification susceptibles de verrouiller le compte d'utilisateur. [CVADHELP-17467]
- L'authentification de l'application Citrix Workspace peut échouer après l'initialisation lorsque vous tentez d'utiliser une carte à puce via Citrix Gateway. Si vous actualisez le processus d'authentification après 15 minutes, un message d'erreur 404 peut apparaître dans le navigateur intégré de Citrix Workspace. Cela entraîne le blocage de l'application dans la boucle d'authentification jusqu'à ce que vous la fermiez et la rouvriez. [CVADHELP-18305]

Session/Connexion

- L'ouverture d'une application publiée à l'aide de la redirection de dossiers lorsque le partage de redirection de dossiers est hors connexion peut échouer avec le message d'erreur suivant :

  Impossible de lancer votre application

  [CVADHELP-16387]

- Lorsque vous tentez d'ouvrir une application à l'aide du raccourci avec les options **Limiter à une instance par utilisateur** et **vPrefer** activées, une erreur d'échec de connexion peut apparaître sur Citrix Director. [CVADHELP-17372]

- Lors d'une conférence téléphonique, lorsque vous utilisez Microsoft Teams en mode optimisé HDX, la partie vidéo des appels entrants peut clignoter. [CVADHELP-17398]
- L'application Citrix Workspace peut interroger des balises externes pour les magasins internes. Avec ce correctif, les balises externes ne sont pas interrogées lorsque le magasin est utilisé sans la passerelle. [CVADHELP-18275]
- Les raccourcis pour les applications publiées via l'application Citrix Workspace ne peuvent pas être créés sans les autorisations appropriées. Par conséquent, les icônes peuvent être téléchargées dans le profil utilisateur à chaque actualisation, ce qui augmente la taille du cache sur les points de terminaison et la consommation du processeur du côté StoreFront. [CVADHELP-18609]
- Un appel pair à pair Microsoft Teams optimisé entre l'application Citrix Workspace pour Mac et l'application Citrix Workspace pour Windows peut se déconnecter. [CVADHELP-18696]
- Le lancement de sessions à partir de groupes de mise à disposition avec une règle de stratégie d'accès spécifiant l'adresse IP du client peut échouer si le client possède plusieurs cartes réseau.

  ```
  Rule: Set-BrokerAccessPolicyRule -Name <rulename> -includedClientIPs
   <Client ip address>
  ```

  [CVADHELP-18783]

Exceptions système

- Citrix Authentication Manager (AuthManSvr.exe) peut se fermer de manière inattendue lors de l'ouverture de session. [CVADHELP-17233]

Expérience utilisateur

- Lorsque vous ouvrez une fenêtre de bureau en mode fenêtré dans un environnement multi-moniteur, le comportement suivant peut être observé.

  La fenêtre ouverte sur le moniteur 1 et déplacée vers le moniteur 2 peut apparaître agrandie sur le moniteur 1 au lieu du moniteur 2.

  [CVADHELP-17373]

Interface utilisateur

- Avec ce correctif, vous pouvez basculer vers le compte requis lorsque plusieurs comptes et le registre du compte actuel sont configurés. [CVADHELP-17718]

- La configuration simultanée d'un magasin activé et d'un magasin désactivé à l'aide d'un objet de stratégie de groupe peut entraîner une interface utilisateur non X1 ou une interface utilisateur avec « bulles vertes » au lieu d'une interface utilisateur X1 pour la première fois sur le magasin activé. [CVADHELP-17942]
- La désactivation du compte de magasin dans l'application Citrix Workspace peut ne pas supprimer les raccourcis d'application du menu **Démarrer** ou du bureau. [CVADHELP-18260]

Application Citrix Workspace 1912 LTSR CU5 pour Windows

Comparé à : application Citrix Workspace 1912 LTSR CU4

Problèmes liés aux machines clientes

- Lorsque vous utilisez l'application Citrix Workspace 1912 LTSR CU4, les machines connectées avec des ports COM supérieurs à 9 peuvent ne pas être mappées au sein de la session. [CVADHELP-17734]

Installation, désinstallation, mise à niveau

- Les tentatives de mise à niveau de l'application Citrix Workspace pour Windows à l'aide du paramètre **/forceinstall** peuvent échouer. Le problème se produit lorsque l'utilitaire de nettoyage Receiver ne parvient pas à démarrer le processus de nettoyage. [CVADHELP-17656]

Ouverture de session/Authentification

- Si une session Citrix Gateway expire, Citrix Workspace peut ne pas demander d'authentification lors du lancement d'une application. [CVADHELP-17187]

Fenêtres transparentes

- Certaines applications tierces peuvent rester au premier plan en gardant d'autres applications lancées en arrière-plan. [CVADHELP-16897]

Problèmes de sécurité

- Les tentatives d'installation de l'application Citrix Workspace 1912 LTSR pour Windows peuvent échouer lorsque les fichiers .cat USB sont signés avec un certificat SHA-1. [CVADHELP-17679]

Session/Connexion

- Lorsque vous parcourez des pages Web sur certains navigateurs utilisant le langage HTML ou des animations sur un client fin GPU, l'application Citrix Workspace pour Windows peut ne plus répondre. Le problème se produit lorsque le processus wfica32 utilise une quantité importante de mémoire. [CVADHELP-16172]
- Après la mise à niveau de l'application Citrix Workspace pour Windows vers la version 1912 LTSR CU1 ou CU2, la fiabilité de session peut échouer. Le problème se produit lorsque le protocole EDT (Enlightened Data Transport) est activé et que la connexion se fait via Citrix Gateway. [CVADHELP-16694]
- Les tentatives de lancement d'une session via l'application Citrix Workspace pour Windows peuvent échouer lorsque le port CGP (2598) est bloqué sur le point de terminaison. [CVADHELP-17632]

Expérience utilisateur

- Ce correctif supprime la fenêtre contextuelle du compte approuvé en utilisant un nouveau paramètre d'objet de stratégie de groupe : **Liste des comptes de magasin approuvés**. [CVADHELP-16597]
- Lorsque vous utilisez certaines applications tierces sur un VDA, les mouvements de la souris peuvent être retardés. [CVADHELP-16737]

Interface utilisateur

- Lorsque vous utilisez l'application Citrix Workspace 1912 LTSR CU2 pour Windows, les raccourcis du menu Démarrer peuvent ne pas être actualisés automatiquement. Le problème se produit lorsqu'une nouvelle application est ajoutée ou qu'une modification est effectuée sur le serveur principal. [CVADHELP-17122]
- La définition de la valeur **CurrentAccount** sur **AllAccount** sous le registre HKEY_LOCAL_MACHINE\Software\C peut ne pas prendre effet. Le problème se produit lorsqu'au moins un compte de magasin est présent. [CVADHELP-17229]
- Lorsque vous tentez de vous connecter à des machines clientes légères Wyse à l'aide de l'application Citrix Workspace pour Windows, l'invite d'autorisation peut apparaître derrière l'écran **Desktop Lock** . Par conséquent, vous ne pouvez pas ouvrir de session avant d'avoir mis la fenêtre d'invite d'autorisation au premier plan. [CVADHELP-17880]

Application Citrix Workspace 1912 LTSR CU4 pour Windows

Comparé à : application Citrix Workspace 1912 LTSR CU3

Problèmes liés aux machines clientes

- Lorsque la stratégie **Redirection de port COM client** est activée, les tentatives d'accès au port COM du périphérique Bluetooth peuvent échouer. [CVADHELP-14939]

Ouverture de session/Authentification

- Les tentatives de connexion à l'application Citrix Workspace version 1912 LTSR CU3 pour Windows peuvent échouer lorsque le nom d'utilisateur contient des caractères umlaut. [CVADHELP-17267]

Problèmes de sécurité

- La protection binaire Control Flow Guard peut être manquante dans les binaires. [CVADHELP-16531]

Session/Connexion

- Lors de l'utilisation de la fonctionnalité de partage d'écran dans Microsoft Teams pour un appel pair à pair, un écran noir peut apparaître. [CVADHELP-15605]
- Si la stratégie **HDX Adaptive Transport** est définie sur **Préféré** et que l'option **Découverte MTU EDT** est activée, un écran gris ou noir peut apparaître avec un message d'avertissement lorsque vous tentez de lancer des applications ou des bureaux. [CVADHELP-15805]
- Le raccourci créé pour une application peut ne pas être supprimé même après la désactivation de l'application ou la modification du chemin d'accès du raccourci. [[CVADHELP-16448]
- Les tentatives de lancement d'applications via l'application Citrix Workspace pour Windows peuvent échouer lors de la connexion ou de la déconnexion d'une connexion VPN via Citrix Gateway. [CVADHELP-16714]
- Dans un scénario de double-hop, les noms de client de point de terminaison peuvent ne pas être transférés vers un Delivery Controller ou Director. Le problème se produit avec VDA Version 2003 et ultérieure. [CVADHELP-16783]

- Après la mise à niveau de l'application Citrix Workspace pour Windows vers la version 1912 LTSR CU1 ou CU2, la fiabilité de session peut échouer. Le problème se produit lorsque le protocole EDT (Enlightened Data Transport) est activé et que la connexion se fait via Citrix Gateway. [CVADHELP-16694]

Expérience utilisateur

- Lors de l'utilisation de l'application Citrix Workspace version 1912 LTSR CU2 pour Windows, une session peut afficher des artefacts graphiques qui masquent le contenu à l'écran. [CVADHELP-16451]
- Après la mise à niveau de Citrix Receiver version 4.9.6 pour Windows vers l'application Citrix Workspace version 1912 LTSR CU2 ou CU3, avec la tentative de lancement d'un raccourci d'application, les icônes de raccourci peuvent clignoter sur certains bureaux. [CVADHELP-16967]

Interface utilisateur

- Si vous sélectionnez **Déconnexion** lorsqu'une session est en cours d'exécution, l'invite de **déconnexion** s'affiche pour confirmer l'action. Appuyez sur **Annuler** provoquera une erreur. [CVADHELP-15516]
- Lorsque vous mettez à niveau Citrix Receiver version 4.9 LTSR CU7 pour Windows vers l'application Citrix Workspace version CU2 ou CU3 pour Windows et que vous tentez de définir le compte de magasin par défaut, un comportement incohérent peut se produire. Par exemple, le compte de magasin par défaut se règle toujours sur Tous les comptes. Avec cette modification, la définition du compte de magasin principal sur un nom de magasin différent persiste même après la fermeture et le redémarrage de l'application Citrix Workspace. [CVADHELP-16903]

Application Citrix Workspace 1912 LTSR CU3 pour Windows

Comparé à : application Citrix Workspace 1912 LTSR CU2

Installation, désinstallation, mise à niveau

- Lorsque vous tentez d'actualiser l'application Citrix Workspace à l'aide de son raccourci créé manuellement, le raccourci peut être supprimé puis recréé. [CVADHELP-15397]

Clavier

- Lorsque vous utilisez un clavier de langue japonaise, le mode de saisie Pleine-chasse peut ne pas fonctionner avec Microsoft Excel lancé via Local App Access. Le problème se produit avec l'application Citrix Workspace pour Windows sur laquelle la fonctionnalité de protection des applications est activée. [CVADHELP-15410]

Ouverture de session/Authentification

- Même après avoir activé les stratégies **Rester connecté** et **Ne plus me demander pendant 60 jours**, Microsoft Azure Multi-Factor Authentication peut toujours demander l'authentification.

  > **Remarque :**
  >
  > Nous recommandons aux utilisateurs de quitter leurs magasins plutôt que de se déconnecter de leurs magasins. Si les utilisateurs se déconnectent des magasins à l'aide de l'authentification webview, ils peuvent être invités à s'authentifier à nouveau car les cookies Internet Explorer sont effacés dans de tels scénarios. Par défaut, le correctif est activé (les cookies sont stockés). Vous pouvez désactiver le correctif en activant la stratégie GPO **Empêcher le stockage des cookies persistants** sous **Composants Citrix > Citrix Workspace > Authentification utilisateur**. Si vous désactivez le correctif, les cookies ne sont pas stockés et sont effacés lors de la déconnexion. Si vous désactivez le correctif, les cookies ne sont pas stockés et sont effacés lors de la déconnexion.

  [CVADHELP-14814]

- Sur les appareils connectés à Azure Active Directory (AD), lorsque l'application Citrix Workspace tente d'accéder à un magasin, puis transmet les informations d'identification d'ouverture de session de point de terminaison, les utilisateurs peuvent ne pas être autorisés à ouvrir une session. En outre, il n'y a pas d'option pour ouvrir une session avec un autre compte utilisateur. [CVADHELP-14844]

Impression

- Lorsque vous envoyez un document sous forme de données brutes vers la file d'attente d'impression, il se peut que le document ne soit pas imprimé. Le problème se produit lorsque vous utilisez le pilote d'imprimante XPS. [CVADHELP-14497]

Session/Connexion

- Dans certains scénarios, l'utilisation des licences de produit Citrix affichée dans Citrix Studio ne correspond pas à l'utilisation des licences affichée dans Citrix License Manager. [CVADHELP-

14950]

- Lorsque l'option **vPrefer** est activée, les applications App-V peuvent démarrer sur un serveur distant plutôt que sur un serveur local. [CVADHELP-15356]
- Lorsque vous lancez un bureau publié via une application Citrix Workspace native pour Windows, l'application Citrix Workspace native s'exécute automatiquement au premier plan du bureau. Le problème se produit lorsque la fonctionnalité **Local App Access** est activée. [CVADHELP-15654]
- Le processus Selfservice.exe peut ne plus répondre et une invite **.NET-BroadcastEventWindow.4.0.0.0.1** peut apparaître. Le problème se produit lorsque vous tentez de fermer la session d'un système exécutant Windows 10 version 1909. [CVADHELP-15700]
- Vous pouvez configurer l'application Citrix Workspace pour Windows pour qu'elle se connecte à tous les comptes lors de l'établissement d'une session. Si vous vous déconnectez de l'application Citrix Workspace et que vous vous reconnectez, le paramètre du compte de magasin change pour un seul compte de magasin plutôt que tous les comptes par défaut. [CVADHELP-15728]
- Lorsque la stratégie de redirection bidirectionnelle du contenu est activée, les tentatives de redirection d'une URL d'un client vers un VDA peuvent échouer. [CVADHELP-15739]
- Dans les scénarios dans lesquels les serveurs proxy n'utilisent pas le port 8080, l'application Citrix Workspace peut ne pas se connecter aux applications et aux bureaux publiés. Le problème se produit car l'application Citrix Workspace pour Windows peut ne pas utiliser le port proxy et utiliser le port par défaut 8080 à la place. [CVADHELP-15977]
- L'application Citrix Workspace pour Windows peut ignorer les paramètres de type proxy. Le problème se produit sur les versions non anglaises du système d'exploitation Microsoft Windows. [CVADHELP-16017]
- Lorsque le paramètre de Registre **EnableFactoryReset** est défini sur **False**, les tentatives de désinstallation de l'application Citrix Workspace peuvent échouer avec le message d'erreur suivant :

  Cette fonctionnalité a été désactivée.

  [CVADHELP-16114]
- Avec Microsoft Teams en mode optimisé, lorsque vous participez à une conférence téléphonique, le son peut être déformé. [CVADHELP-16232]

Exceptions système

- Lorsque la stratégie **EchoCancellation** est activée et que la qualité audio est définie sur moyenne, le processus wfica32.exe peut se fermer par intermittence, ce qui entraîne éventuellement la déconnexion des sessions. [CVADHELP-14568]

- Le processus Receiver.exe peut se fermer de manière inattendue. [CVADHELP-15669]

Application Citrix Workspace 1912 LTSR CU2 pour Windows

Comparé à : application Citrix Workspace 1912 LTSR CU1

Installation, désinstallation, mise à niveau

- Les tentatives de mise à niveau de l'application Citrix Workspace pour Windows de la version 190*x* vers la version 1912 peuvent échouer. Le problème se produit lorsqu'un fichier contrevenant est présent dans le chemin d'accès du dossier exécutable. [CVADHELP-15277]
- Lorsque vous tentez de mettre à jour l'application Citrix Workspace de la version 1912 vers la version 1912 CU1 ou 2006, la fonctionnalité de mise à jour de l'application Citrix Workspace peut ne pas fonctionner sur les systèmes d'exploitation en langue autre que l'anglais. [CVADHELP-15357]

Clavier

- Lorsque vous utilisez l'éditeur de méthode d'entrée Chinois (IME) Wuxiami, la touche Maj peut rester bloquée en position enfoncée. Le problème se produit si l'heure locale générique est définie sur **ON**. [CVADHELP-15243]

Problèmes de sécurité

- Ce correctif résout un problème de sécurité. Pour plus d'informations, consultez l'article CTX277662 du centre de connaissances. [CVADHELP-15613]

Session/Connexion

- Lorsque l'outil de modification du Registre est désactivé, les clés de Registre provenant de l'installation précédente peuvent ne pas être conservées après une mise à niveau. Par conséquent, les tentatives de lancement d'un bureau échouent. [CVADHELP-15104]
- L'application Citrix Workspace peut afficher une erreur de script sur les versions antérieures à 1911 et une page blanche sur les versions 1911 et ultérieures. Le problème se produit avec les magasins utilisant le contrôle du navigateur Internet Explorer pour afficher les pages de connexion lorsque des stratégies d'objet de stratégie de groupe de base de sécurité Microsoft sont appliquées. [CVADHELP-15475]

- Dans un scénario double-hop, les tentatives de lancement d'une application à l'aide du raccourci du menu **Démarrer** peuvent échouer. Le problème se produit si vous activez la limite d'application d'une instance par utilisateur. [CVADHELP-15576]
- Lorsque vous vous connectez à un magasin via l'application Citrix Workspace version 1912 ou ultérieure, les applications peuvent ne pas être énumérées. [CVADHELP-15597]

Expérience utilisateur

- Si vous vous connectez au Self-Service Plug-in (SSP) via un VPN, les tentatives d'actualisation du SSP peuvent échouer. [CVADHELP-14418]
- Les tentatives d'utilisation de la commande **SelfService.exe -init -ipoll -exit** pour fermer le processus SelfService.exe peuvent échouer. [CVADHELP-15126]
- Lorsque vous utilisez un stylet HP Active pour écrire sur une application publiée, la fonctionnalité d'écriture peut présenter un délai de trois à quatre secondes. [CVADHELP-15203]
- Les tentatives de lancement d'une session peuvent échouer après une nouvelle installation de l'application Citrix Workspace pour Windows ou la mise à niveau d'une installation existante vers la dernière version. Le lancement de la session est bloqué sur l'écran **Préparation de votre bureau**. Le problème se produit lorsque vous configurez Desktop Lock à l'aide d'une URL Citrix Gateway.

  > **Remarque :**
  >
  > Un écran noir apparaît pendant un certain temps avant que Desktop Lock ne s'affiche la première fois que vous configurez l'application Citrix Workspace pour Windows à l'aide d'une URL Citrix Gateway et de Desktop Lock. Si l'écran noir persiste pendant une longue période, déconnectez-vous en utilisant **Ctrl+Alt+Suppr** pour les machines physiques et **Ctrl+Alt+Fin** pour les machines virtuelles.

  [CVADHELP-15334]
- Après la mise à niveau de l'application Citrix Workspace vers la version 1912 CU1 à partir de la version 1912, l'énumération des applications peut être lente et prendre jusqu'à 10 minutes. [CVADHELP-15766]

Correctif 1 pour l'application Citrix Workspace 1912 LTSR CU1 pour Windows (19.12.1001)

Comparaison avec : application Citrix Workspace 1912 LTSR CU1 pour Windows

Problèmes de sécurité

- Ce correctif résout un problème de sécurité. Pour plus d'informations, consultez l'article CTX277662 du centre de connaissances. [CVADHELP-15613]

Application Citrix Workspace 1912 LTSR CU1 pour Windows

Comparé à : application Citrix Workspace 1912 LTSR

Redirection de contenu

- Lorsque vous tentez de rediriger une URL longue, l'URL peut ne pas être redirigée vers un VDA et le processus Redirector.exe se ferme de façon inattendue avec l'exception suivante :

  INVALID_CRUNTIME_PARAMETER

  [CVADHELP-13197]

Installation, désinstallation, mise à niveau

- Les tentatives d'installation ou de mise à niveau de l'application Citrix Workspace sur un VDA qui exécute Windows 10 peuvent échouer. Le problème se produit lorsque vous effectuez les étapes suivantes :

  1. Installez l'application Citrix Workspace.
  2. Installez un VDA.
  3. Mettez à niveau l'application Citrix Workspace vers une version ultérieure.

  Le problème se produit car la mise à niveau ou l'installation entraîne la suppression des cartes vidéo Citrix. [CVADHELP-13764]

- Les tentatives d'utilisation de la fonctionnalité de mise à jour automatique pour mettre à jour automatiquement HDX RealTime Media Engine (RTME) avec l'application Citrix Workspace peuvent échouer. La mise à niveau de RTME vers la dernière version échoue. [CVADHELP-15047]

Ouverture de session/Authentification

- Si vous ajoutez deux magasins à l'application Citrix Workspace pour Windows à l'aide de deux comptes différents, le bouton Connexion peut ne pas fonctionner pour le magasin secondaire après suppression du magasin principal. [CVADHELP-13805]

- Lorsque l'authentification multifacteur est activée et que la boîte de dialogue Sécurité Windows est utilisée pour se connecter, la boîte de dialogue ADFS (Active Directory Federation Services) n'apparaît pas lors de l'authentification pour les magasins. [CVADHELP-14316]
- Lorsque vous configurez Citrix Gateway pour prendre en charge l'authentification unique via l'application Citrix Workspace, l'authentification unique peut échouer. Le problème se produit lorsqu'un nom d'utilisateur ou un mot de passe contient des caractères spéciaux tels que **%**, **=** et **&**. [CVADHELP-14564]

SDK

- Ce correctif améliore la prise en charge des handles de clés privées héritées. [CVADHELP-14530]

Session/Connexion

- Lorsque les fonctionnalités Local App Access et Desktop Lock sont activées, lorsque vous exécutez la fonction Changer d'utilisateur après avoir appuyé sur la touche Ctrl+Alt+Suppr, la session utilisateur locale peut se reconnecter. Toutefois, lorsque la session du serveur tente de se reconnecter, le VDA est bloqué sur un écran blanc qui affiche le message connecté au bureau. Le bureau ne s'affiche jamais. [CVADHELP-13046]
- Dans un environnement multi-moniteur, les tentatives d'agrandissement d'une session utilisateur peuvent échouer. Le problème se produit lorsque vous reconnectez votre ordinateur portable à la station d'accueil. [CVADHELP-13614]
- Dans un scénario double-hop, Citrix HDX Engine peut se fermer de manière inattendue lorsque vous tentez de lancer une session. [CVADHELP-13915]
- Lorsque l'option **vPrefer** est activée dans l'application Citrix Workspace, les tentatives de lancement d'une application App-V peuvent échouer avec le message d'erreur suivant :

  Impossible de démarrer

  [CVADHELP-14039]
- Après avoir ajouté des applications publiées à vos **favoris**, vous ne pouvez ouvrir qu'une seule application. Le problème se produit lorsque ces applications publiées utilisent le même nom d'exécutable, comme indiqué par **KEYWORDS:prefer="<`application_name`>**. [CVADHELP-14098]
- Les valeurs de Registre liées à la fonctionnalité obsolète, **HDX MediaStream pour Flash** (par exemple, Flash et Flash2) peuvent ne pas être supprimées du paramètre de Registre, HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Mod 3.0\VirtualDriver après la mise à niveau l'application Citrix Workspace. Ce problème peut entraîner un échec de connexion. [CVADHELP-14850]

Exceptions système

- Le processus wfica32.exe peut se fermer de manière inattendue lorsque vous tentez de vous reconnecter à une session. Le problème se produit avec la version 1904.1 de l'application Citrix Workspace pour Windows. [CVADHELP-12807]
- Lorsque Local App Access est activé, une session peut cesser de répondre et afficher le message d'erreur suivant :

  Citrix HDX Engine is not responding

  [CVADHELP-14058]
- Si vous tentez d'installer l'application Citrix Workspace sans configurer le mode libre-service, une exception peut se produire. Le problème se produit lorsque vous ouvrez le menu **Raccourcis et reconnexion** à partir de **Préférences avancées**. Le problème se produit avec les versions 1907 à 2002 de l'application Citrix Workspace. [CVADHELP-14940]

TWAIN

- Les tentatives de scan à l'aide d'un périphérique TWAIN peuvent échouer. La colonne **État** de l'onglet **Applications** du Gestionnaire des tâches Windows affiche « Ne répond pas » pour Citrix HDX Engine. [CVADHELP-14782]

Expérience utilisateur

- Dans les scénarios à double saut où les VDA pour système d'exploitation multi-session s'exécutent dans le premier saut et les applications publiées s'exécutent dans le second saut, l'option Actualiser les applications du menu du compte de l'application Citrix Workspace peut ne pas fonctionner. [CVADHELP-13230]
- Lorsque vous ajoutez un compte à l'aide d'une URL de magasin sur l'application Citrix Workspace pour Windows, cela peut prendre beaucoup de temps. Le problème se produit lorsque l'URL contient un numéro de port. [CVADHELP-14051]
- Vous pouvez voir deux icônes d'application Citrix Workspace dans la barre d'état système. Le problème se produit avec l'application Citrix Workspace version 1912. [CVADHELP-14577]
- Lorsque vous utilisez l'authentification unique dans un environnement VDA, un écran de démarrage peut apparaître. Le problème se produit lorsque vous mettez à niveau l'application Citrix Workspace pour Windows vers la version 1911 ou une version ultérieure. [CVADHELP-14590]

Interface utilisateur

- Une application peut tenter de se placer au premier plan par intermittence, déplaçant l'application en cours. Son icône dans la barre des tâches peut clignoter, informant l'utilisateur que l'application tente de s'afficher au premier plan. [CVADHELP-13071]

Application Citrix Workspace 1912 LTSR pour Windows

> **Remarque :**
>
> Si vous êtes un client disposant de la version actuelle de l'application Citrix Workspace 1911 et que vous souhaitez passer à la version LTSR :
>
> Cette version contient les correctifs suivants par rapport à l'application Citrix Workspace 1911.
>
> Si vous êtes un client disposant de Citrix Receiver 4.9 pour Windows et que vous souhaitez rester sur la version LTSR :
>
> Cette version contient tous les correctifs inclus dans Citrix Receiver pour Windows 4.9, y compris les mises à jour cumulatives jusqu'à la version 4.12, et tous les correctifs inclus dans l'application Citrix Workspace 1808 à 1911, ainsi que la liste suivante de correctifs inclus dans l'application Citrix Workspace 2002 (par rapport à l'application Citrix Workspace 1911) : la version 1912 contient tous les correctifs entre Citrix Receiver pour Windows 4.9 LTSR CU9 et l'application Citrix Workspace 1911 ainsi que les correctifs suivants :

Redirection HDX MediaStream Windows Media

- Dans un environnement multi-moniteur, lorsque vous lisez une vidéo MP4 à l'aide du Windows Media Player dans une session utilisateur, la vidéo peut être correctement lue sur le moniteur principal. Toutefois, lorsque vous déplacez le lecteur sur un autre écran, un écran noir peut apparaître sur le moniteur secondaire ou un moniteur étendu connecté via DisplayLink à l'aide d'une station d'accueil. [CVADHELP-11848]

Session/Connexion

- Lorsque vous tentez de vous reconnecter à une session à partir de HDX RealTime Media Engine à l'aide d'une carte à puce rapide, HDX RealTime Media peut se fermer de façon inattendue. [CVADHELP-12605]
- Lorsque les applications publiées reçoivent de nombreuses demandes de lecture de sons courts pendant une courte période de temps, le processus wfica32.exe peut se fermer de façon inattendue. [CVADHELP-12855]

- Une fois qu'un délai d'expiration de session s'est écoulé, il se peut que la session se déconnecte automatiquement. Lorsque vous tentez de relancer la session, le lancement de la session prend plus de temps que d'habitude. Le problème se produit en cas d'interruption du réseau. [CVADHELP-13017]
- Une fenêtre d'application transparente peut être partiellement tronquée et rester tronquée jusqu'à ce que vous redimensionniez manuellement la fenêtre. [CVADHELP-13108]
- L'application Citrix Workspace effectue désormais une vérification de la présence d'icônes de raccourci chaque fois qu'elle est actualisée ou démarrée. Si aucune icône n'est disponible, l'application Citrix Workspace récupère à nouveau l'icône. Cela garantit que les raccourcis apparaissent correctement. [RFWIN-15501]
- Lorsque vous tentez d'activer la stratégie de redirection de contenu bidirectionnel (sous **Configuration ordinateur > Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Workspace > Expérience utilisateur**), vous êtes invité à saisir une entrée spécifique d'URL même si vous n'activez pas les remplacements d'application ou de bureau spécifiques d'URL. [RFWIN-15867]

Exceptions système

- Le processus Receiver.exe peut se fermer de manière inattendue lors de la capture des traces CDF. [CVADHELP-13077]

Problèmes connus

June 13, 2023

Problèmes connus dans l'application Citrix Workspace 1912 LTSR CU7 pour Windows

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

Problèmes connus dans l'application Citrix Workspace 1912 LTSR CU6 pour Windows

- Lorsque vous partagez votre écran dans Microsoft Teams, en tant qu'application publiée, la bordure rouge en bas de l'écran partagé n'apparaît pas. [LCMRFWIN-4194]

Problèmes connus dans l'application Citrix Workspace 1912 LTSR CU5 pour Windows

- Lorsque vous connectez certaines applications distantes tierces telles que mRemoteNG à un point de terminaison et que vous ancrez la barre d'outils de l'application publiée sur les côtés, le système peut ne plus répondre avec une utilisation de l'UC de 100 %. [LCMRFWIN-4164]
- Lorsque vous tentez d'arrêter le partage d'écran pendant des appels optimisés Microsoft Teams, la session peut ne plus répondre par intermittence. [LCMRFWIN-4184]

Problèmes connus dans l'application Citrix Workspace 1912 LTSR CU4 pour Windows

- Au cours d'une session, lorsque vous cliquez sur **Rechercher les mises à jour** et que les mises à jour sont téléchargées correctement, la session en cours n'est pas répertoriée dans la boîte de dialogue **Téléchargement réussi**. [RFWIN-23152]

Problèmes connus dans l'application Citrix Workspace 1912 LTSR CU3 pour Windows

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

Problèmes connus dans l'application Citrix Workspace 1912 LTSR CU2 pour Windows

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

Problèmes connus dans l'application Citrix Workspace 1912 LTSR CU1 pour Windows

- Les tentatives d'utilisation de la webcam dans une réunion WebEx peuvent provoquer l'échec de l'application Citrix Workspace. Le problème se produit lorsque vous définissez l'audio UDP sur **Medium**.

  Pour contourner le problème, accédez au chemin d'accès suivant dans l'Éditeur du Registre et effectuez la configuration suivante :

  Chemin : HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Adva

  Nom : EchoCancellation

  Type : REG_SZ

  Valeur : FALSE

  [DOCFB-3805]

Problèmes connus dans l'application Citrix Workspace 1912 LTSR pour Windows

- Les tentatives de capture d'écran à l'aide de la touche **Imprimer écran** peuvent échouer. Ce problème se produit lorsque vous réduisez une session d'application Citrix Workspace protégée. [RFWIN-15155]
- Lorsque vous lancez Microsoft Word à la fois dans une session publiée et sur votre machine locale et que vous supprimez le magasin dans **Comptes**, le message d'erreur suivant s'affiche lorsque vous lancez l'application sur la machine locale :

  Voulez-vous rechercher une application dans Citrix Workspace afin d'ouvrir ce fichier ?

  [RFWIN-15884]
- Les tentatives de lancement d'une session sur un VDA compatible SSL peuvent échouer. [RFWIN-16129]
- Dans une session de bureau protégée, les tentatives de capture d'écran d'une session non protégée peuvent échouer. [RFWIN-16704]
- Il se peut que vous ne puissiez pas supprimer les détails du magasin qui ont été ajoutés à l'aide du modèle d'administration d'objet de stratégie de groupe via l'interface utilisateur graphique. [RFWIN-16754]
- Les tentatives de modification de l'affichage dans une session protégée entraînent la fermeture de la session. [RFWIN-16784]

Avis de tiers

June 13, 2023

L'application Citrix Workspace 1912 LTSR pour Windows 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 (Téléchargement PDF)

Configuration système requise et compatibilité

April 22, 2024

Exigences

- 1 Go de RAM.
- Configuration requise pour .NET Framework
  - Self-Service Plug-in requiert NET 4.6.2. 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 l'application Citrix Workspace pour Windows. Pour plus d'informations, consultez la section Utilisation des paramètres de ligne de commande.
- Dernière version de Microsoft Visual C++ Redistributable.

  > **Remarque :**
  >
  > Citrix vous recommande d'utiliser la dernière version de Microsoft Visual C++ Redistributable. Sinon, une invite de redémarrage peut s'afficher pendant une mise à niveau.

  À compter de la version 1904, le package d'installation de l'application Citrix Workspace ne contient pas les fichiers binaires individuels de Microsoft Visual C++ Redistributable, mais inclut le programme d'installation de Microsoft Visual C++ Redistributable. Le programme d'installation de l'application Citrix Workspace vérifie si le package Microsoft Visual C++ Redistributable est présent sur le système durant l'installation et l'installe si nécessaire. L'application Citrix Workspace version 1912 et ultérieure requiert Microsoft Visual C++ Redistributable version 14.24.28127.4 ou ultérieure.

  > **Remarque :**
  >
  > Les tentatives d'installation de l'application Citrix Workspace avec des privilèges non administrateur sur un système sans le package Microsoft Visual C++ Redistributable peuvent échouer.

  Seul un administrateur peut installer le package Microsoft Visual C++ Redistributable.

  Pour résoudre les problèmes liés à .NET Framework ou à l'installation de Microsoft Visual C++ Redistributable, consultez l'article du centre de connaissances CTX250044.

Matrice de compatibilité

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

L'application Citrix Workspace est compatible avec les systèmes d'exploitation Windows suivants :

> **Remarque :**
>
> Le plug-in EPA (End-Point Analysis) de Citrix Gateway est pris en charge sur Citrix Workspace. Sur l'application Citrix Workspace native, il est pris en charge uniquement lors de l'utilisation de l'authentification nFactor. Pour plus d'informations, consultez Configurer l'analyse EPA pré-authentification et post-authentification en tant que facteur dans l'authentification nFactor dans la documentation Citrix ADC.

Système d'exploitation

Windows 10, éditions Entreprise 32 bits et 64 bits. Pour plus d'informations sur le système d'exploitation Windows 10 compatible, consultez Compatibilité de Windows 10 avec l'application Citrix Workspace pour Windows.
Windows 10 éditions Pro 32 bits et 64 bits (prises en charge à partir de l'application Citrix Workspace 1912 LTSR CU5 pour Windows et versions ultérieures)
Windows 8.1, éditions 32 bits et 64 bits (y compris l'édition Embedded)

Windows 7, 32 bits et 64 bits (ESU, Extended Security Update ou mise à jour de sécurité étendue)

Windows 7 Embedded Standard (ESU, Extended Security Update ou mise à jour de sécurité étendue)

Windows Thin PC

Windows Server 2016

Windows Server 2012 R2, édition Standard et Datacenter

Windows Server 2019

Windows Server 2008 R2

Windows 10 Entreprise LTSC 2019

Windows 10 Entreprise 2016 LTSB 1607

Compatibilité de Windows 10 avec l'application Citrix Workspace pour Windows

> **Remarque :**
>
> - Il n'est pas recommandé d'installer des versions du logiciel Citrix qui ont été publiées avant la version du canal semestriel. Les clients qui choisissent de le faire devront vérifier, avant de contacter l'assistance, si le problème rencontré n'est pas déjà résolu avec une version de logiciel Citrix plus récente, si disponible. Ils devront peut-être procéder à une mise à niveau vers une version de logiciel Citrix plus récente.
> - Une fois qu'une version de Windows 10 atteint la fin de service, cette version n'est plus

> desservie ou prise en charge par Microsoft. Citrix prend en charge l'exécution de son logiciel uniquement sur un système d'exploitation qui est pris en charge par son fabricant. Pour plus d'informations sur la fin du service de Windows 10, consultez la page Infos-clés sur le cycle de vie Windows.

Version de l'application Citrix Workspace	Numéro de version de Windows 10 édition Entreprise	Numéro de compilation
1912 CU7 et versions ultérieures	LTSC 2021	19044
1912 CU6 et versions ultérieures	21H2	19044
1912 CU6 et versions ultérieures	21H2	19044
1912 CU5 et versions ultérieures	21H1	19043.1165
1912 CU2 et versions ultérieures	20H2	19042.685
1912 CU1 et versions ultérieures	2004	19041.329
1911 et versions ultérieures	1909	18363.418
1909 et versions ultérieures	1903	18362.116
1812 et versions ultérieures	1809	17763.107
1808 et versions ultérieures	10 1803	17134.376

Navigateurs pris en charge

Pour obtenir une liste des navigateurs pris en charge, consultez la section Accéder aux magasins via les sites Citrix Receiver pour Web.

Matrice des systèmes d'exploitation

Système d'exploitation pris en charge sur les appareils tactiles
Windows 10
Windows 8
Windows 7

Système d'exploitation pris en charge sur les appareils tactiles

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

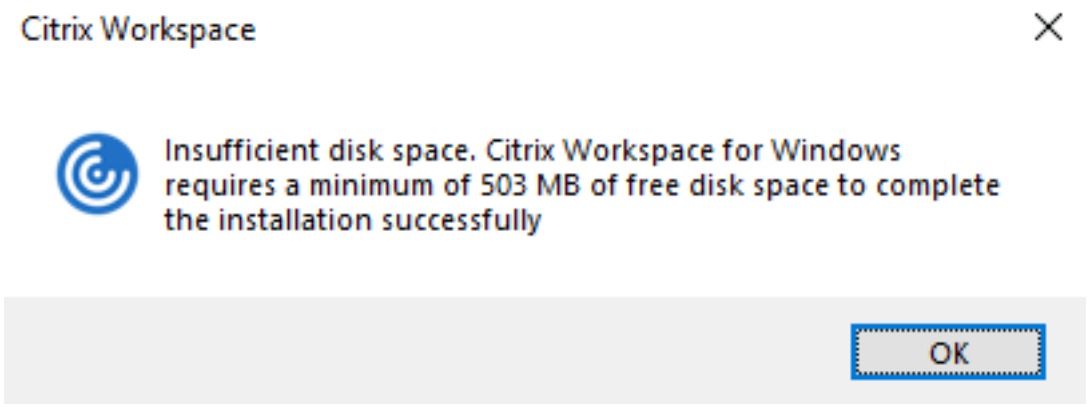
Validation de l'espace disque disponible

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

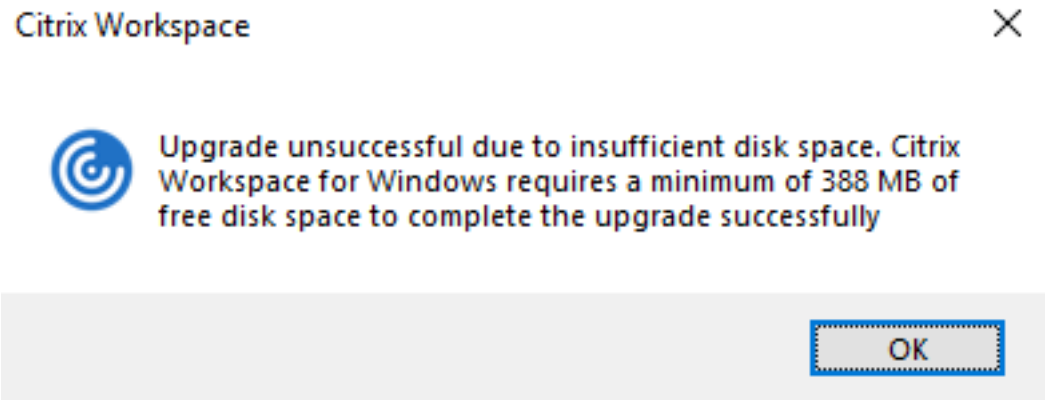
Type d'installation	Espace disque requis
Nouvelle installation	572 Mo
Mettre à niveau	350 Mo

L'application Citrix Workspace vérifie l'espace disque requis pour compléter 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 d'une mise à niveau, l'installation se termine lorsque l'espace disque est insuffisant et que 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

Remarque :

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

- 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.

Certificats racines

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, consultez la section Configuration de certificats intermédiaires.

Authentification

Authentification à StoreFront

	Workspace pour Web utilisant des navigateurs	Site StoreFront Services (natif)	StoreFront, Citrix Virtual Apps and Desktops (natif), Citrix DaaS	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*
Authentification pass-through au domaine	Oui	Oui	Oui		
Jeton de sécurité				Oui*	Oui*
Authentification à 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 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*	
Authentification à 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 plus d'informations sur l'authentification, consultez

- Configuration de l'authentification et de l'autorisation dans la documentation Citrix Gateway.
- Configurer l'authentification et la délégation dans la documentation 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. Cette vérification permet d'améliorer 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 CRL pour permettre aux utilisateurs de n'ouvrir leurs sessions que si toutes les listes de révocation de certificats ont été vérifiées.

Quittez l'application Citrix Workspace et fermez tous les composants Citrix Workspace, y compris le **Centre de connexion**.

Pour plus d'informations, consultez la section TLS.

Installer et désinstaller

May 23, 2024

Remarques à l'intention des administrateurs avant l'installation de l'application Citrix Workspace 1912 LTSR pour Windows

- L'application Citrix Workspace 1912 LTSR pour Windows nécessite la version 4.6.2 ou ultérieure de .NET Framework. Le programme d'installation de l'application Citrix Workspace télécharge et installe .NET Framework si la version n'est pas présente dans le système. Toutefois, nous vous recommandons d'installer manuellement le composant .NET Framework requis avant d'installer ou de mettre à jour l'application Citrix Workspace.
- Si vous tentez une installation sans assistance, consultez l'article du centre de connaissances CTX257546.
- Pour connaître les dernières informations sur les suites de chiffrement prises en charge et non prises en charge, consultez l'article du centre de connaissances CTX250104.

Vous pouvez installer l'application Citrix Workspace en téléchargeant le package d'installation `CitrixWorkspaceApp.exe` à partir de la page de téléchargement ou depuis la page de téléchargement de votre entreprise (si disponible). Vous pouvez installer le package à l'aide des méthodes suivantes :

- 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.

Installation avec des privilèges d'administrateur et non administrateur :

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 et Citrix Ready Workspace Hub avec l'application Citrix Workspace pour Windows.

Le tableau suivant décrit les différences lorsque l'application Citrix Workspace est installée par un administrateur ou par un utilisateur :

	Dossier d'installation	Type d'installation
Administrateur	C:\Program Files (x86)\Citrix\ICA Client	Installation par système
Utilisateur	%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.

Utilisation d'un programme d'installation Windows

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`.

Par défaut, les journaux du programme d'installation se trouvent sur `%temp%\CTXReceiverInstallLogs*.logs`.

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 la section Authentification pass-through au domaine pour plus d'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 partir 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 dossier temporaire du système avant le lancement de l'installation. Cet espace disponible comprend les fichiers programmes, les données utilisateur et les dossiers temporaires après le lancement de plusieurs applications.

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 :

- Paramètres courants
- Paramètres d'installation
- Paramètres des fonctionnalités HDX
- Préférences et paramètres de l'interface utilisateur
- 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 Citrix 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 Single Sign-On. Consultez la section Authentification pass-through au domaine pour plus d'informations.
- /`rcu` - Ce commutateur n'est efficace que lors de la mise à niveau d'une version non prise en charge du logiciel. Indique que l'application Citrix Workspace sera installée ou mise à niveau en désinstallant la version existante du logiciel. Cela permet également de nettoyer les paramètres existants.

  > Remarque :
  >
  > Le commutateur /`rcu` n'est plus pris en charge à compter de la version 1909. Pour plus d'informations, consultez Fin de prise en charge.

- /`forceinstall` : ce commutateur est efficace lors du nettoyage de toute configuration ou entrée existante de l'application Citrix Workspace sur le système dans les scénarios suivants :

- Vous effectuez une mise à niveau à partir d'une version non prise en charge de la version de l'application Citrix Workspace.
- L'installation ou la mise à niveau échoue.

Paramètres d'installation

/AutoUpdateCheck

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`.
- Manuel : vous n'êtes pas informé lorsqu'une mise à jour est disponible. 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

Si vous avez activé la mise à jour automatique, vous pouvez choisir le canal de publication vers lequel vous souhaitez mettre à jour. Pour plus d'informations, consultez la section Étapes du cycle de vie.

- LTSR : mise à jour automatique uniquement vers des mises à jour cumulatives Long Term Service Release. Par exemple, `CitrixWorkspaceApp.exe /AutoUpdateStream=LTSR`.
- Current (Actuel) : mise à jour vers la dernière version de l'application Citrix Workspace. Par exemple, `CitrixWorkspaceApp.exe /AutoUpdateStream=Current`.

/DeferUpdateCount

Indique le nombre de fois où vous pouvez différer les notifications de mise à jour lorsqu'une mise à jour est disponible. Pour plus d'informations, consultez la section Mises à jour de Citrix Workspace.

- -1 (valeur par défaut) : permet de différer les notifications 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. Vous ne recevrez plus de rappel à propos de la mise à jour. Par exemple, `CitrixWorkspaceApp.exe /DeferUpdateCount=0`.

- Tout autre numéro « n » : permet de différer les notifications de mise à jour un nombre « n » de fois. L'option **Me rappeler plus tard** s'affiche le nombre « n » de fois défini. Par exemple, `CitrixWorkspaceApp.exe /DeferUpdateCount=<n>`.

/AURolloutPriority

Lorsqu'une nouvelle version de l'application est publiée, Citrix déploie la mise à jour pendant une période de mise à disposition spécifique. Avec ce paramètre, vous pouvez contrôler à quel moment de cette période vous pouvez recevoir la mise à jour.

- Auto (par défaut) : vous recevez les mises à jour pendant la période de mise à disposition configurée par Citrix. Par exemple, `CitrixWorkspaceApp.exe /AURolloutPriority=Auto`.
- Fast (Rapide) : vous recevez les mises à jour au début de la période de mise à disposition. Par exemple, `CitrixWorkspaceApp.exe /AURolloutPriority=Fast`.
- Medium (Moyen) : vous recevez les mises à jour au milieu de la période de mise à disposition. Par exemple, `CitrixWorkspaceApp.exe /AURolloutPriority=Medium`.
- Slow (Lent) : vous recevez les mises à jour à la fin de la période de mise à disposition. Par exemple, `CitrixWorkspaceApp.exe /AURolloutPriority=Slow`.

/includeappprotection

Fournit une sécurité renforcée lors de l'utilisation de Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) en protégeant les clients contre les programmes malveillants d'enregistrement de frappe et de capture d'écran.

- `CitrixWorkspaceApp.exe /includeappprotection`

Pour plus d'informations, consultez la section App Protection.

INSTALLDIR

Spécifie le répertoire d'installation personnalisé pour l'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

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

Paramètres des fonctionnalités HDX

ALLOW_BIDIRCONTENTREDIRECTION

Indique que la redirection bidirectionnelle du contenu du client vers l'hôte et de l'hôte vers le client est activée. Pour plus d'informations, consultez la section Paramètres de stratégie Redirection bidirectionnelle du contenu de la documentation 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

Indique que l'application Citrix Workspace est installée avec le composant Local App Access côté client. Vous devez installer l'application Citrix Workspace avec des privilèges d'administrateur pour que ce composant fonctionne. Pour plus d'informations, consultez la section Local App Access de la documentation Citrix Virtual Apps and Desktops.

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

LEGACYFTAICONS

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

Active la fonctionnalité de redirection des adresses URL sur les machines utilisateur. Pour plus d'informations, consultez la section Local App Access de la documentation 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

ALLOWADDSTORE

Permet de configurer les magasins (http ou https) en fonction du paramètre spécifié.

- S (valeur par défaut) : permet d'ajouter ou de supprimer des magasins sécurisés uniquement (configuré avec HTTPS). Par exemple, `CitrixWorkspaceApp.exe ALLOWADDSTORE=S`.
- A : permet d'ajouter ou de supprimer des magasins sécurisés (HTTPS) et des magasins non sécurisés (HTTP). Non applicable si l'application Citrix Workspace est installée par utilisateur. Par exemple, `CitrixWorkspaceApp.exe ALLOWADDSTORE=A`.
- N : permet de ne jamais autoriser les utilisateurs à ajouter ou supprimer leur propre magasin. Par exemple, `CitrixWorkspaceApp.exe ALLOWADDSTORE=N`.

ALLOWSAVEPWD

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

STARTMENUDIR

Spécifie le dossier 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.

DESKTOPDIR

Spécifie le dossier des raccourcis sur le Bureau.

> **Remarque :**
>
> Lorsque vous utilisez l'option DESKTOPDIR, définissez la clé PutShortcutsOnDesktop sur True.

- <Directory Name> : vous pouvez spécifier le chemin d'accès relatif des raccourcis. Par exemple, pour placer les raccourcis sous Démarrer > Tous les programmes > Workspace, spécifiez DESKTOPDIR=\Workspace.

SELFSERVICEMODE

Contrôle l'accès à l'interface utilisateur en libre-service de l'application Citrix Workspace.

- 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

Contrôle le pré-lancement de session. Consultez la section Temps de lancement des applications pour plus d'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

Masque l'affichage de l'option **Raccourcis et reconnexion** sur la page **Préférences avancées**. Pour plus d'informations, consultez la section Masquer des paramètres spécifiques sur la page Paramètres avancés.

- 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

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

- True (valeur par défaut) : choisir de participer au programme CEIP. Par exemple, `CitrixWorkspaceApp.exe EnableCEIP=True`.
- False : choisir de ne pas participer au programme CEIP. Par exemple, `CitrixWorkspaceApp.exe EnableCEIP=False`.

EnableTracing

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

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%`. Par exemple, `CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%`.

ENABLE_DYNAMIC_CLIENT_NAME

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

Active l'authentification Single Sign-On lorsque l'application Citrix Workspace est installée avec la commande `/includeSSON`. Consultez la section Authentification pass-through au domaine pour plus d'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

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, consultez la section 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 Citrix 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 mettre à disposition 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 du magasin, par exemple `HR App Store`.

Exemples d'installation par ligne de commande

Pour spécifier l'adresse URL du magasin Citrix Gateway :

```
CitrixWorkspaceApp.exe STORE0=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.
> - Si vous configurez plusieurs magasins, placez l'URL du magasin Citrix Gateway en premier dans la liste. Seule une configuration d'URL de magasin Citrix Gateway est autorisée.

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

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

Désinstaller

Utilisation du programme de désinstallation Windows :

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.

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
```

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

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

> **Remarque :**
>
> - Les clés de registre créées par receiver.adm/receiver.adml ou receiver.admx sont conservées après la désinstallation.
> - Si vous trouvez des entrées dans l'Éditeur du Registre après la désinstallation, supprimez-les manuellement.

Déploiement

November 2, 2023

Vous pouvez déployer l'application Citrix Workspace à l'aide des méthodes suivantes :

- 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, consultez la section Utilisation d'Active Directory et d'exemples de scripts.

- Utilisation de Workspace pour Web pour vous assurer que les utilisateurs ont installé l'application Citrix Workspace pour Windows avant de lancer une application à partir d'un navigateur. Pour plus d'informations, consultez la section 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, consultez la section Utilisation de System Center Configuration Manager 2012 R2.

Utilisation d'Active Directory et d'exemples de scripts

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 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 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 connaître la syntaxe de la ligne de commande, consultez la section Utilisation des paramètres de ligne de commande.

Scripts

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

Type de déploiement	Pour déployer	Pour supprimer
Par ordinateur	CheckAndDeployWorkspacePerMachineStartupScript.bat	CheckAndRemoveWorkspacePerMachineSta
Par utilisateur	CheckAndDeployWorkspacePerUserLogonScript.bat	CheckAndRemoveWorkspacePerUserLogonS

Pour ajouter des scripts de démarrage :

1. Ouvrez la Console de gestion des stratégies de groupe.
2. Sélectionnez **Configuration ordinateur** OU **Configuration utilisateur** > **Stratégies** > **Paramètres Windows** > **Scripts**.
3. Dans le panneau droit de la console Gestion des stratégies de groupe, sélectionnez **Ouverture de session**.
4. Sélectionnez **Afficher les fichiers** et copiez le script approprié dans le dossier affiché.
5. Fermez la boîte de dialogue.
6. Dans le menu **Propriétés**, 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 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.

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` : `CitrixWorkspaceAppWeb.exe`.
3. Déployez le fichier exécutable renommé à l'aide de votre méthode de déploiement habituelle. Si vous utilisez StoreFront, consultez la section Configuration de sites Workspace pour Web à l'aide des fichiers de configuration dans la documentation 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 le numéro de version de l'application Citrix Workspace que vous allez déployer.

    > **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 **Suivant**.

    Un message de réussite s'affiche.

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

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 maintenance (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, sous **Nom**, entrez le nom du périphérique et cliquez sur **Parcourir** pour sélectionner la 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 **Suivant**. 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.

Mise à jour

April 22, 2024

Mise à jour manuelle

Si vous avez déjà installé l'application Citrix Workspace pour Windows, téléchargez et installez la dernière version de l'application à partir de la page Téléchargements de Citrix.

Mise à jour automatique

À partir de la version 1912 Cumulative Update 4 (CU4), les chemins d'accès au journal des mises à jour Citrix Workspace sont modifiés. Les journaux des mises à jour de Workspace se trouvent dans C:\Program Files (x86)\Citrix\Logs pour la mise à jour à l'échelle de la machine. Les journaux se trouvent dans le dossier temporaire de l'utilisateur pour la mise à jour à l'échelle de l'utilisateur.

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

> **Remarque :**
>
> - Si vous avez configuré un proxy de sortie d'interception SSL, vous devez ajouter une exception pour le serveur de mise à jour automatique Workspace `https://downloadplugins.citrix.com/` afin de recevoir les mises à jour de Citrix.
> - La mise à jour automatique n'est pas disponible pour les versions antérieures à l'application Citrix Workspace 2104 et à l'application Citrix Workspace 1912 LTSR CU4.
> - Si vous avez configuré un proxy de sortie d'interception SSL, vous devez ajouter une exception pour le service Receiver auto-update Signature `https://citrixupdates.cloud.com/` et l'emplacement de téléchargement `https://downloadplugins.citrix.com/` afin de recevoir les mises à jour de Citrix.
> - Votre système doit disposer d'une connexion Internet pour recevoir les mises à jour.
> - 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 Access.
> - Les mises à jour de l'application Citrix Workspace sont désactivées sur les machines sur lesquelles Desktop Lock est installé.
> - Les utilisateurs de Workspace pour Web ne peuvent pas télécharger automatiquement la stratégie de StoreFront.
> - Les mises à jour Citrix Workspace peuvent être limitées aux mises à jour LTSR uniquement.
> - Citrix 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.

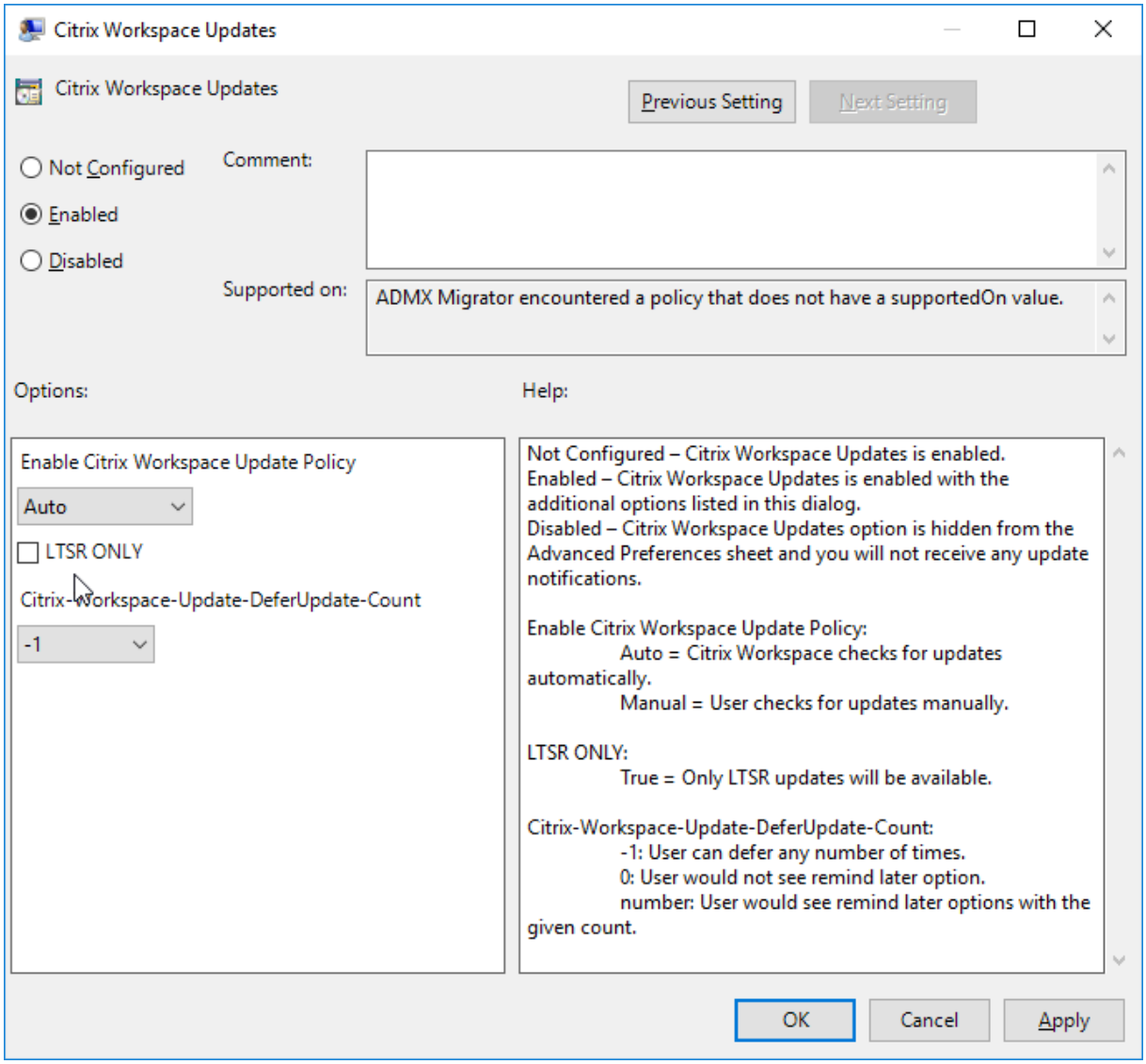
Configuration avancée des mises à jour automatiques (mises à jour de Citrix Workspace)

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

1. Modèle d'administration d'objet de stratégie de groupe
2. Interface de ligne de commande
3. Interface utilisateur graphique
4. StoreFront

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

Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc et accédez au nœud Configuration de l'ordinateur, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Mises à jour de Workspace**.



1. **Activer ou désactiver les mises à jour** : sélectionnez **Activé** ou **Désactivé** pour activer ou désactiver les mises à jour de Workspace.

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

2. **Notification de mise à jour** : lorsqu'une mise à jour est disponible, vous pouvez en être automatiquement notifié ou choisir de rechercher les mises à jour manuellement. Après avoir activé les mises à jour de Workspace, sélectionnez l'une des options suivantes dans le menu déroulant **Stratégie d'activation de la mise à jour de Citrix Workspace** :

   - Auto : vous êtes informé lorsqu'une mise à jour est disponible (valeur par défaut).

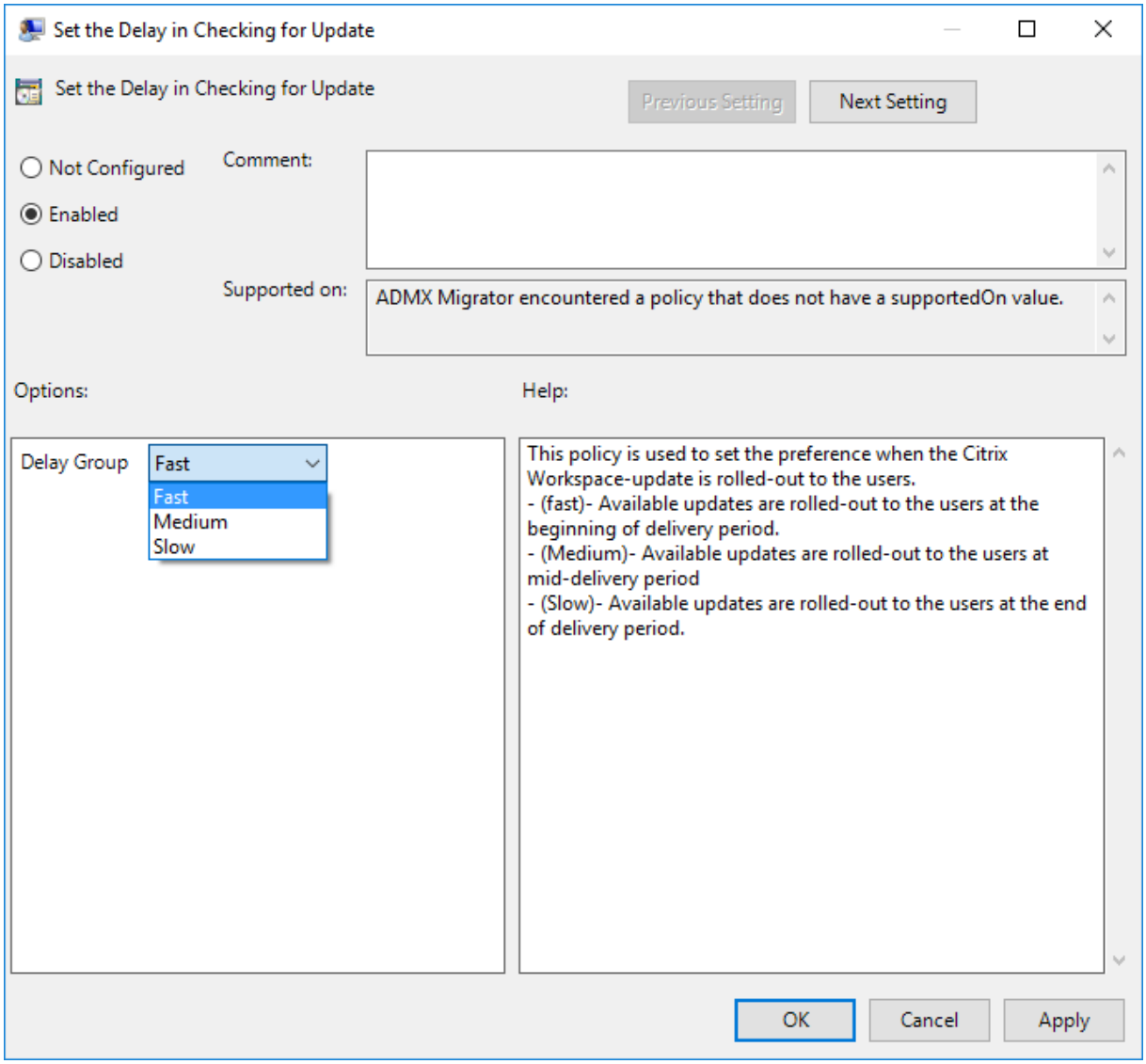
- Manuel : vous n'êtes pas informé lorsqu'une mise à jour est disponible. Recherchez les mises à jour manuellement.

3. Sélectionnez **LTSR UNIQUEMENT** pour obtenir les mises à jour de LTSR uniquement.
4. Dans la liste déroulante **Citrix-Workspace-Update-DeferUpdate-Count**, sélectionnez une valeur comprise entre -1 et 30 :

   - -1 : permet de différer les notifications un nombre indéfini de fois (valeur par défaut).
   - 0 - Vous ne recevrez qu'une seule notification pour la mise à jour.

Configurer le délai de recherche de mises à jour Lorsqu'une nouvelle version de l'application Citrix Workspace est disponible, Citrix déploie la mise à jour pendant une période de mise à disposition spécifique. Avec cette propriété, vous pouvez contrôler à quel moment de cette période vous pouvez recevoir la mise à jour.

Pour configurer la période de mise à disposition, exécutez `gpedit.msc` pour lancer le modèle d'administration d'objet de stratégie de groupe. Sous le nœud Configuration ordinateur, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Définir le délai de recherche de mises à jour**.



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.

> **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.

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

En spécifiant des paramètres de ligne de commande lors de l'installation de l'application Citrix Workspace :

Vous pouvez configurer les mises à jour de Workspace en spécifiant des paramètres de ligne de commande lors de l'installation de l'application Citrix Workspace. Pour plus d'informations, consultez la section Paramètres d'installation.

En utilisant des paramètres de ligne de commande après l'installation de l'application Citrix Workspace :

Les mises à jour de Citrix Workspace peuvent également être configurées après l'installation de l'application Citrix Workspace pour Windows. Accédez à l'emplacement de CitrixReceiverUpdater.exe à l'aide de la ligne de commande Windows.

CitrixWorkspaceUpdater.exe est généralement accessible depuis `CitrixWorkspaceInstallLocation\Citrix\Ica Client\Receiver`. Vous pouvez exécuter ce binaire avec les paramètres de ligne de commande répertoriés dans la section Paramètres d'installation.

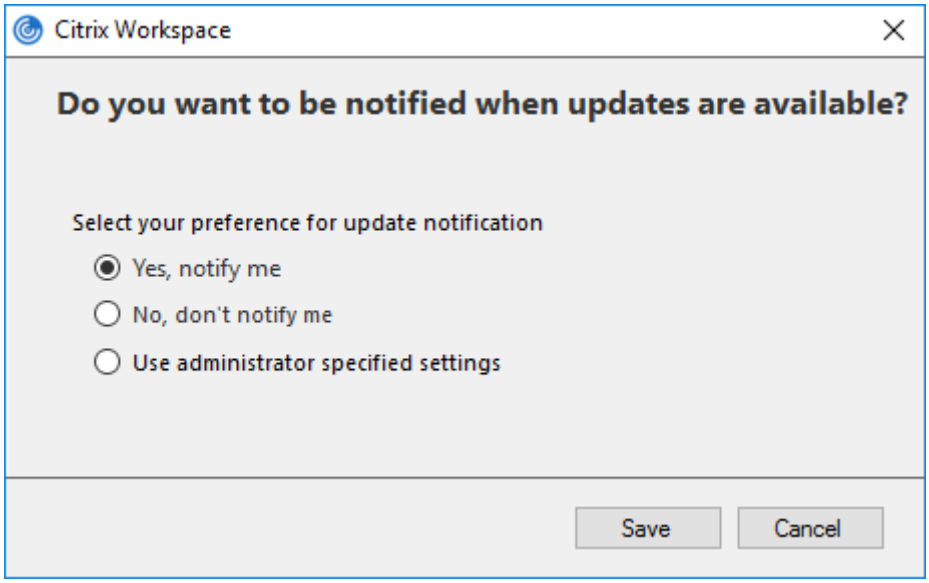
Par exemple,

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

> **Remarque** :
>
> `/AutoUpdateCheck` est un paramètre obligatoire que vous devez définir pour configurer d'autres paramètres comme `/AutoUpdateStream`, `/DeferUpdateCount`, `/AURolloutPriority`.

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

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



> **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, consultez la section Page Préférences avancées.

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

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

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

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

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

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

   ```
   <account>

       <clear />

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

   ```



```
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>
70
71  <!--NeedCopy-->
```

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

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

Mise en route

April 22, 2024

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
- Citrix Gateway Store

- Ajouter l'URL du magasin à l'application Citrix Workspace
- Mappage des lecteurs clients
- Résolution des noms 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	\ICA Client\Configuration
receiver.admx	\ICA Client\Configuration
receiver.adml	\ICA Client\Configuration\[MUIculture]
CitrixBase.admx	\ICA Client\Configuration
CitrixBase.adml	\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 `\<Installation Directory>\ICA Client\Configuration\receiver.adm`.
5. Sélectionnez **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 ont été ajoutés à l'objet de stratégie de groupe 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.admx	%systemroot%\policyDefinitions
CitrixBase.admx	Répertoire d'installation\ICA Client\Configuration\CitrixBase.admx	%systemroot%\policyDefinitions
receiver.adml	Répertoire d'installation\ICA Client\Configuration[MUIculture]receiver.adml	%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 authentifie une connexion à Citrix Virtual Apps and Desktops, Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) et VDI-in-a-Box, en énumérant et en regroupant les

bureaux et applications disponibles dans des magasins auxquels vous pouvez accéder via l'application Citrix Workspace.

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 Utilisation des paramètres de ligne de commande 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 : `CitrixWorkspaceApp.exe STORE0= HRStore;https://ag.mycompany.com#Storename;On;Store`
où #Store name est le nom du magasin derrière 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.
- 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_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle` (64 bits)

`HKEY_LOCAL_MACHINE\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_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\\Dazzle` (64 bits)

`HKEY_LOCAL_MACHINE\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.

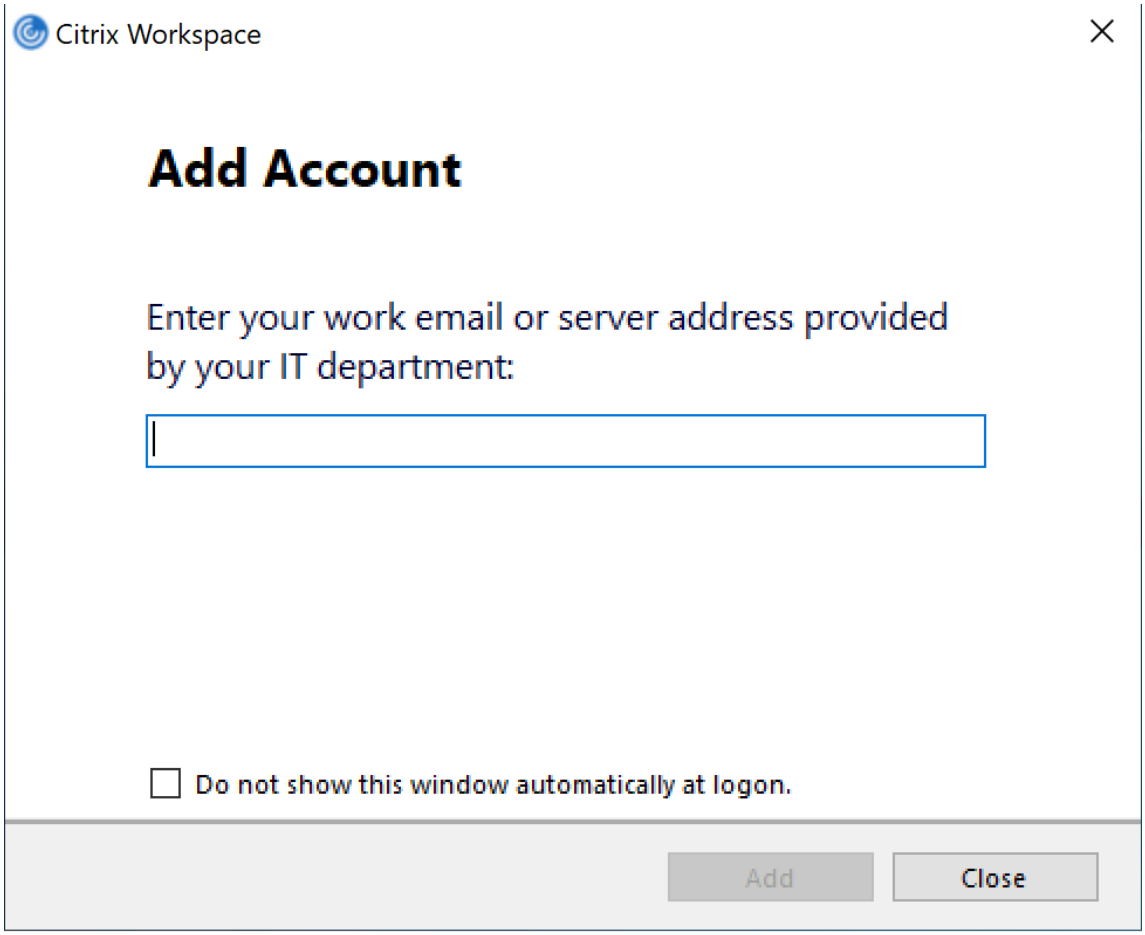
Suppression de la boîte de dialogue Ajouter un compte

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.

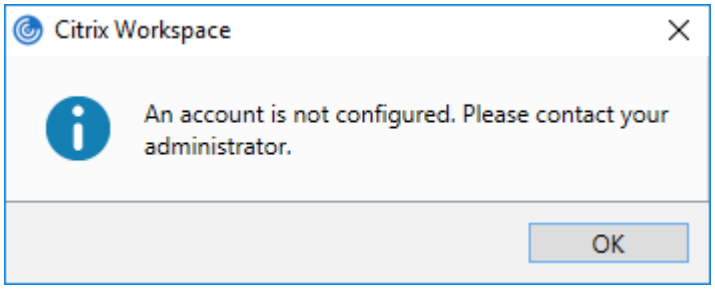
2. **Installation par ligne de commande**

   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
   ```

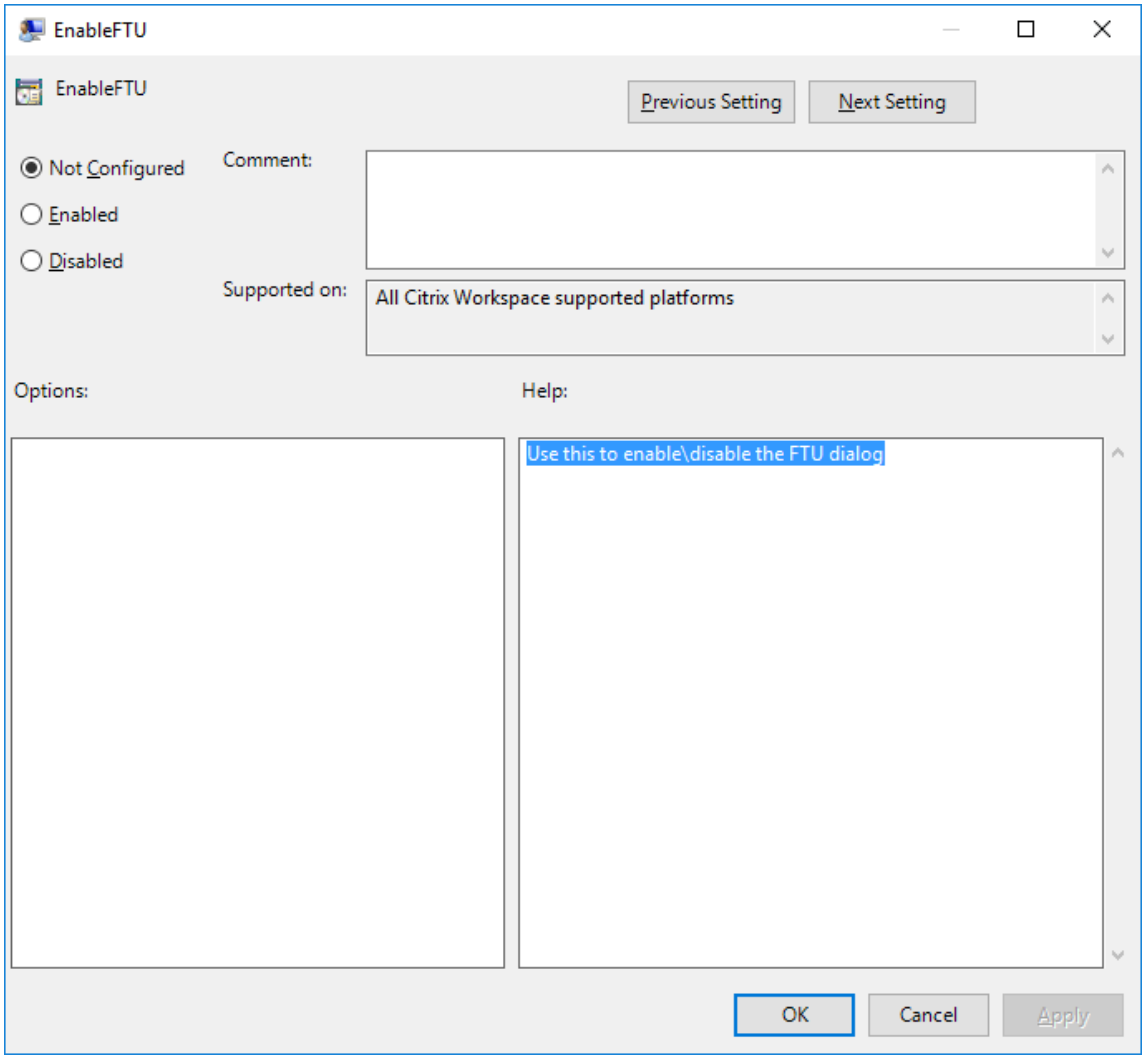
   Ce paramètre étant spécifique à la machine, il s'applique à tous les utilisateurs.

   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** vers **CitrixWorkspaceAppWeb.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 l'option **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 sur la configuration de la découverte de compte basée sur une adresse e-

mail, consultez la section Global App Configuration Service.

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://servername.company.com`.

  Pour les déploiements Interface Web, indiquez l'URL du site Citrix DaaS.

- 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 l'Éditeur du Registre. 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 de 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
A	A
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
A	A
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 l'Éditeur du Registre. 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

May 23, 2024

App Protection

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

La protection des applications est une fonctionnalité complémentaire qui offre une sécurité renforcée lors de l'utilisation de Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Elle limite le risque d'être infecté par des programmes malveillants d'enregistrement de frappe et de capture d'écran. App Protection empêche l'exfiltration d'informations

confidentielles telles que les informations d'identification de l'utilisateur et les informations sensibles affichées à l'écran. Cette fonctionnalité empêche les utilisateurs et les attaquants de prendre des captures d'écran et d'utiliser des enregistreurs de frappe pour récupérer et exploiter des informations sensibles.

La fonction App Protection nécessite l'installation d'une licence complémentaire sur votre serveur de licences. Une licence Citrix Virtual Desktops doit être également présente. Pour plus d'informations sur les licences, consultez la section Configurer de la documentation Protection des applications.

Exigences :

- Citrix Virtual Apps and Desktops 1912 ou versions ultérieures
- StoreFront 1912
- Application Citrix Workspace Version 1912 ou ultérieure.

Logiciels requis :

- La fonctionnalité de protection des applications doit être activée sur le Controller. Pour plus d'informations, consultez la documentation App Protection.

Vous pouvez inclure le composant de protection des applications avec l'application Citrix Workspace à l'aide des méthodes suivantes :

- Lors de l'installation de l'application Citrix Workspace à l'aide d'une interface de ligne de commande ou d'une interface utilisateur graphique OU
- Lors du lancement d'une application (installation à la demande)

> **Remarque :**
>
> - Cette fonctionnalité est prise en charge uniquement sur les systèmes d'exploitation Microsoft Windows Desktop tels que Windows 10, Windows 8.1 et Windows 7.
> - Cette fonctionnalité n'est pas prise en charge par le protocole de bureau distant (RDP ou Remote Desktop Protocol).

Protection de session HDX locale :

Deux stratégies offrent des fonctionnalités de protection contre les programmes d'enregistrement de frappe et de capture d'écran dans une session. Ces stratégies doivent être configurées via PowerShell. Aucune interface utilisateur graphique n'est disponible à cet effet.

> **Remarque :**
>
> Citrix DaaS ne prend pas en charge la fonctionnalité de protection des applications.

Pour plus d'informations sur la configuration de la protection des applications sur Citrix Virtual Apps and Desktops, consultez la documentation Protection des applications.

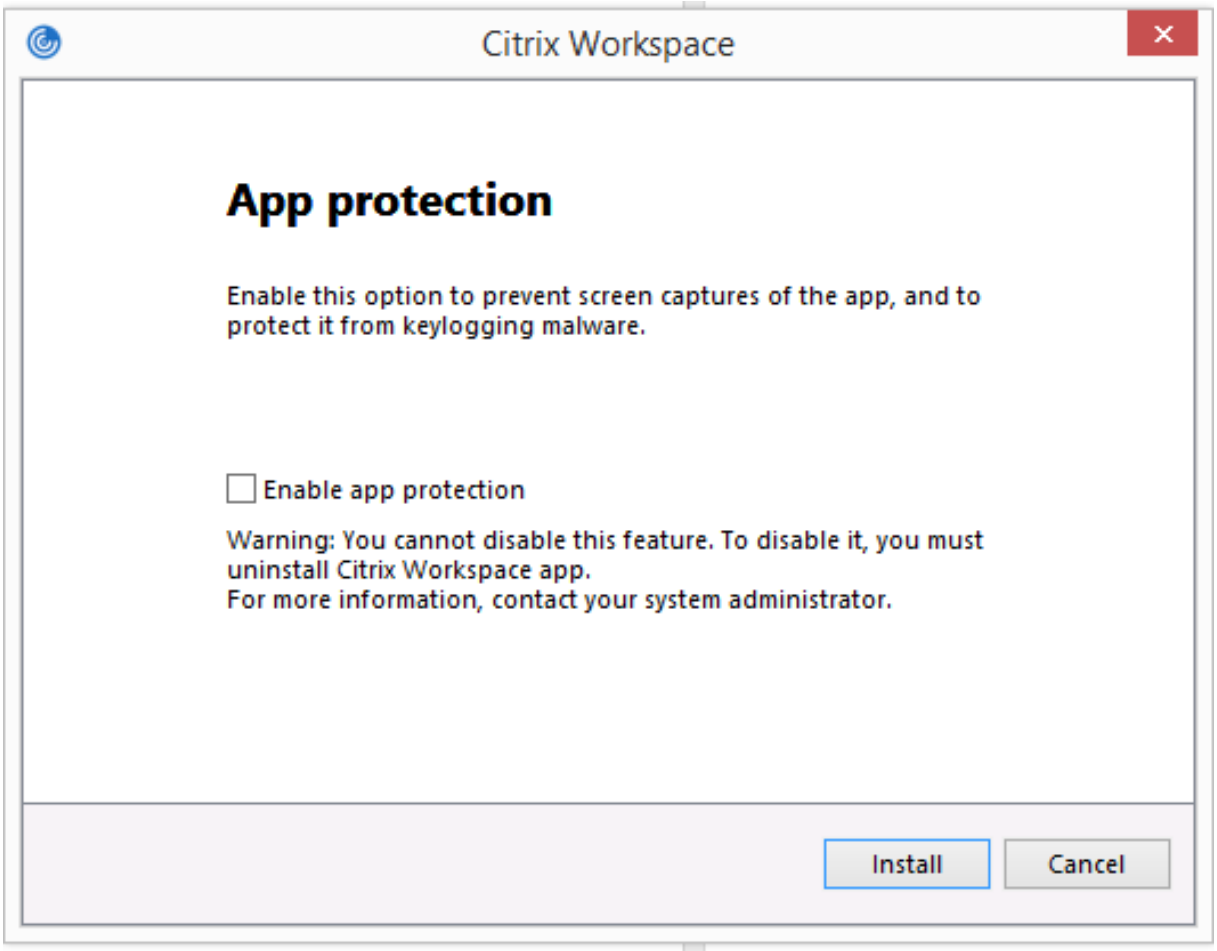
Protection des applications –Configuration dans l'application Citrix Workspace

> **Remarque :**
>
> - Incluez le composant de protection des applications avec l'application Citrix Workspace uniquement si votre administrateur vous a demandé de le faire.
> - Le composant de protection des applications peut avoir un impact sur les capacités de capture d'écran de votre appareil.

Lors de l'installation de l'application Citrix Workspace, vous pouvez inclure la protection des applications à l'aide de l'une des méthodes suivantes :

- Interface utilisateur graphique
- Interface de ligne de commande

Interface utilisateur graphique Lors de l'installation de l'application Citrix Workspace, utilisez la boîte de dialogue suivante pour inclure le composant de protection des applications. Sélectionnez **Activer protection des applications**, puis cliquez sur **Installer** pour poursuivre l'installation.



> **Remarque :**
>
> Si vous n'activez pas la protection des applications pendant l'installation, une invite s'affiche lorsque vous lancez une application protégée. Suivez l'invite pour installer le composant de protection des applications.

Interface de ligne de commande Utilisez l'option de ligne de commande /`includeappprotection` pendant l'installation de l'application Citrix Workspace pour ajouter le composant de protection des applications.

Le tableau suivant fournit des informations sur les écrans protégés en fonction du déploiement :

Déploiement d'App Protection	Écrans protégés	Écrans non protégés
Inclus dans l'application Citrix Workspace	Boîte de dialogue Self-Service Plug-in et Authentication Manager/Informations d'identification utilisateur	Centre de connexion, Appareils, messages d'erreur liés à l'application Citrix Workspace, Reconnexion automatique des clients, Ajouter un compte
Configuré sur le Controller	Écran de session ICA (applications et bureaux)	Centre de connexion, Appareils, messages d'erreur liés à l'application Citrix Workspace, Reconnexion automatique des clients, Ajouter un compte

Comportement attendu :

Le comportement attendu dépend de la façon dont les utilisateurs accèdent au magasin StoreFront qui contient des ressources protégées.

> **Remarque :**
>
> - Citrix recommande d'utiliser uniquement l'application Citrix Workspace native pour lancer une session protégée.

- **Comportement sur Workspace pour Web :**

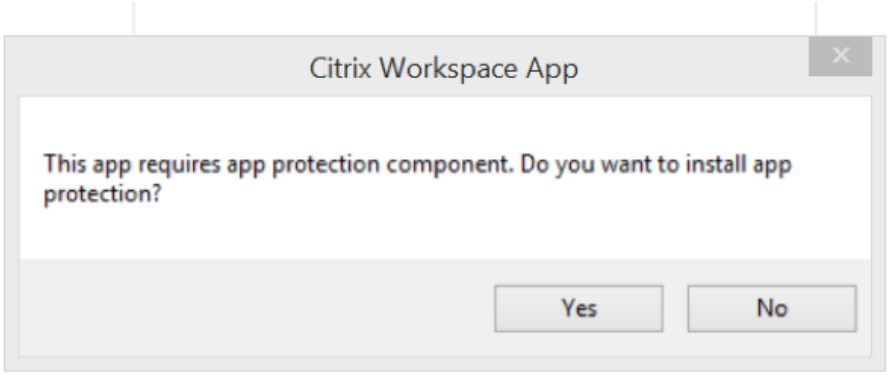
  Le composant de protection des applications n'est pas pris en charge dans les configurations Workspace pour Web. Les applications protégées par des stratégies de protection des applications ne sont pas énumérées. Pour plus d'informations sur les ressources attribuées, contactez votre administrateur système.

- **Comportement sur les versions de l'application Citrix Workspace ne prenant pas en charge la protection des applications :**

Sur l'application Citrix Workspace 1911 et versions antérieures, les applications protégées par des stratégies de protection des applications ne sont pas énumérées dans StoreFront.

- **Comportement des applications dont la fonctionnalité de protection des applications est configurée sur le Controller :**

  Si la protection des applications est configurée sur le Controller et que vous essayez de lancer une application protégée, la protection des applications est installée à la demande. La boîte de dialogue suivante s'affiche :



  Après avoir cliqué sur **Oui**, le composant de protection des applications est installé et l'utilisateur peut lancer l'application protégée.

- **Comportement de la session protégée sur le protocole de bureau distant (RDP ou Remote Desktop Protocol)**

  - Votre session protégée active se déconnecte si vous lancez une session RDP (Remote Desktop Protocol).
  - Vous ne pouvez pas lancer une session protégée dans une session RDP (Remote Desktop Protocol).

Journaux des erreurs liés à la protection des applications :

Les journaux liés au composant de protection des applications sont enregistrés dans la sortie de débogage. Pour collecter ces journaux, procédez comme suit :

1. Téléchargez et installez l'application DebugView à partir du site Web de Microsoft.
2. Lancez l'invite de commande et exécutez la commande suivante :

   ```
   Dbgview.exe /t /k /v /l C:\logs.txt
   ```

   Dans l'exemple ci-dessus, vous pouvez afficher les journaux dans le fichier log.txt.

La commande indique ce qui suit :

- /t : l'application DebugView démarre avec un affichage réduit dans la zone de notification.
- /k : active la capture du noyau.
- /v : active la capture détaillée du noyau.
- /l : journalise la sortie dans un fichier spécifique.

Désinstaller le composant de protection des applications :

Pour désinstaller le composant de protection des applications, vous devez désinstaller l'application Citrix Workspace de votre système. Redémarrez le système pour que les modifications prennent effet.

> **Remarque :**
>
> La protection des applications est prise en charge uniquement lors de la mise à niveau à partir de la version 1912.

Problèmes connus et limitations :

- Cette fonctionnalité n'est pas prise en charge sur les systèmes d'exploitation Microsoft Server tels que Windows Server 2012 R2 et Windows Server 2016.
- Pour effectuer une capture d'écran de l'appareil local, les fenêtres associées à l'application Citrix Workspace doivent être réduites. Sinon, vous ne pouvez pas effectuer de capture d'écran de votre appareil local.
- Aucune fonctionnalité ne prend en charge les scénarios double-hop.
- Pour que cette fonctionnalité fonctionne correctement, désactivez la stratégie **Redirection du Presse-papiers client** sur le VDA.

Estimation des performances au niveau du codage du point de terminaison sur Microsoft Teams

Lorsque vous lancez le processus HdxTeams.exe (le moteur multimédia WebRTC intégré dans l'application Citrix Workspace qui gère la redirection Microsoft Teams), la meilleure résolution de codage que le processeur du point de terminaison peut gérer sans surcharge est estimée. Les valeurs possibles sont 240p, 360p, 720p et 1080p.

Le processus d'estimation des performances (également appelé `webrtcapi.EndpointPerformance`) s'exécute lorsque HdxTeams.exe est démarré. Le code macroblock détermine la meilleure résolution possible avec le point de terminaison particulier. La résolution la plus élevée possible est ensuite incluse lors de la négociation du codec entre les homologues, ou entre l'homologue et le serveur de conférence.

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

Performances des points de terminaison	Résolution maximale	Valeur de clé de registre
fast	1080p	3
medium	720p	2
slow	360p	1
very slow	240p	0

Il existe des indicateurs de configuration pour désactiver le codec VP9 ou H264.
H264 utilise une charge processeur plus basse mais consomme plus de bande passante. Au contraire, VP9 utilise une charge processeur plus élevée mais consomme moins de bande passante.

Chemin du registre dans l'application Citrix Workspace :

Accédez au chemin du registre HKEY_CURRENT_USER HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream et créez les clés suivantes :\

Nom	Type	Valeurs	Description
DisableVP9	DWORD	1 ; 0	1 : désactiver le codec VP9 ; 0 : activer
DisableH264	DWORD	1 ; 0	1 : désactiver le codec H.264 ; 0 : activer
OverridePerformance	DWORD	0 ; 1 ; 2 ; 3	Force les performances souhaitées. La valeur doit être comprise entre 0 et 3, où 0 indique un traitement très lent et 3 un traitement très rapide.

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

Transport adaptatif

Le transport adaptatif est un mécanisme de transport de données pour Citrix Virtual Apps and Desktops et Citrix DaaS. Plus rapide et évolutif, il améliore l'interactivité avec les applications et il 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 tentent de connecter en parallèle la reconnexion de la fiabilité de session et 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
- 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 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**.

L'application Citrix Workspace facilite le transport adaptatif par défaut. En outre, et ceci également par défaut, le client tente d'utiliser le transport adaptatif uniquement si le VDA est configuré sur **Préféré** sur le Delivery Controller 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.

Utilisez le modèle d'administration d'objet de stratégie de groupe (GPO) pour désactiver le transport adaptatif sur le client.

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 désactivé (Off) 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 Citrix Workspace** 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 le client essaie de se connecter au serveur en utilisant UDP en premier. Si UDP n'est pas disponible, la connexion bascule sur TCP en tant que solution de secours.
    - **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.

Pour utiliser le transport adaptatif, ajoutez les fichiers de modèle de l'application Citrix Workspace au dossier **Définitions de stratégie** . Pour plus d'informations sur l'ajout de 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 la section Transport adaptatif dans la documentation Citrix Virtual Apps and Desktops.

Page Préférences avancées

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
  - Haute résolution
  - Informations de support
  - Raccourcis et reconnexion
  - 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 Préférences avancées 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** > **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
Activé	Masque le paramètre
Désactivé	Affiche le paramètre

Masquer les paramètres spécifiques suivants sur la page :

- Outil d'analyse de la configuration
- Centre de connexion
- Haute résolution
- Collecte des données
- Supprimer les mots de passe enregistrés
- Clavier et barre de langue
- Raccourcis et reconnexion
- Informations de support
- 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 :
    - True : affiche l'option Réinitialiser Workspace sur la page Préférences avancées.
    - 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 et Citrix DaaS, 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 utiliser un site Workspace pour Web ou un site Interface Web 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 : vous pouvez configurer l'application Citrix Workspace de manière à placer automatiquement des raccourcis d'applications et de bureaux directement dans le menu Démarrer ou sur le bureau. Le nouveau mode *raccourci uniquement* vous permet de localiser les applications publiées à l'aide du schéma de navigation Windows habituel.

Pour de plus amples informations, consultez la section Créer des groupes de mise à disposition dans la documentation de Citrix Virtual Apps and Desktops.

Configurer le mode libre-service

Ajoutez un compte StoreFront à l'application Citrix Workspace ou configurez l'application Citrix Workspace pour qu'elle pointe vers un site StoreFront pour utiliser le mode libre-serivce. Le mode libre-service permet aux utilisateurs de s'abonner à des applications à partir de l'interface utilisateur 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** > **Self 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 et 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 and Desktops.

- 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 plus d'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 :

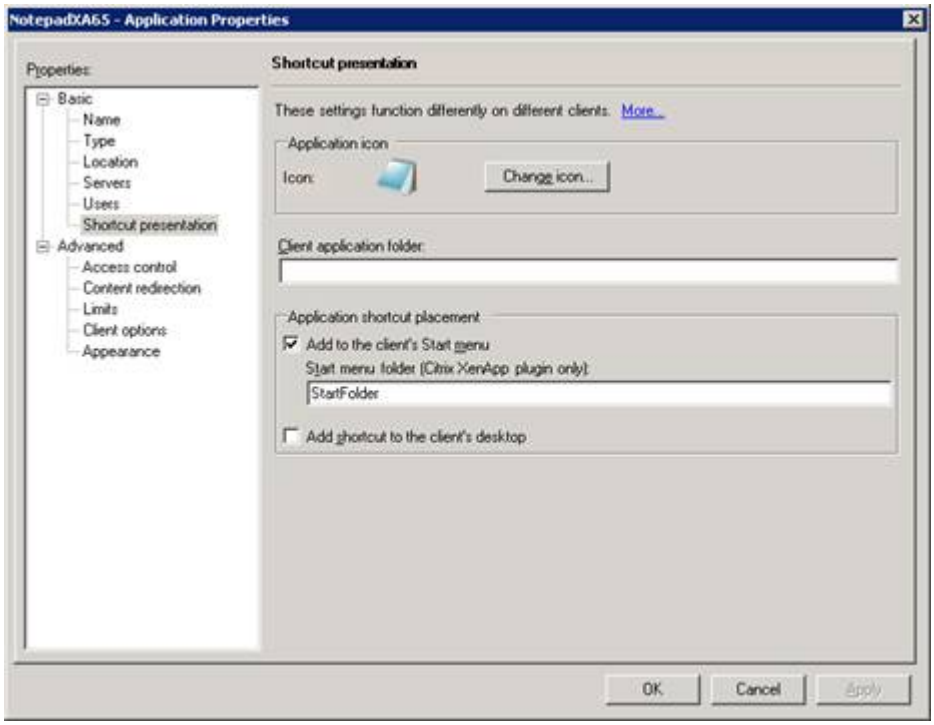
Si vous souhaitez que les paramètres par application déterminent où les applications sont placées indépendamment du mode utilisé (libre-service ou mode du menu Démarrer).	Configurez l'application Citrix Workspace pour Windows avec **PutShortcutsInStartMenu**=**false** et activez les paramètres par application.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

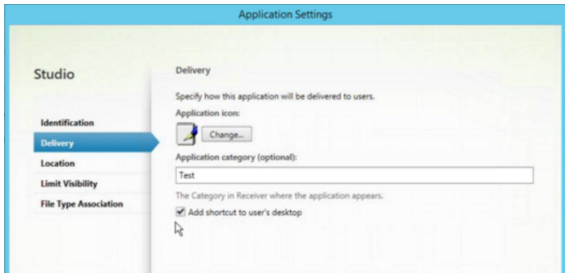
1. Dans l'écran des **propriétés d'application XenApp**, développez les propriétés **de base**.
2. Sélectionnez l'option Présentation du raccourci.
3. Dans la section Emplacement(s) du ou des raccourci(s) de l'écran **Présentation du raccourci**, sélectionnez la case **Ajouter** un raccourci dans le 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 plusieurs 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 l'Éditeur du Registre. 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.

À partir de la version 1912, vous pouvez configurer le comportement d'actualisation automatique dans l'application Citrix Workspace à l'aide de l'Éditeur du Registre.

Avec les versions antérieures, lorsque vous redémarrez l'application Citrix Workspace, une actualisation automatique se produit même lorsque les données du cache sont disponibles.

> **Remarque :**
>
> Vous ne pouvez pas configurer cette option sur les comptes non X1 Store.

Pour configurer l'actualisation automatique à l'aide de l'Éditeur de Registre :

1. Lancez l'Éditeur du Registre et accédez au chemin HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix
2. Créez les clés de valeur de chaîne suivantes :

Clé de registre	Valeur
InitialRefreshMinMs	10000 (10 secondes)
InitialRefreshMaxMs	15000 (15 secondes)
SuppressRefreshMs	1000 (1 seconde)

3. Enregistrez et fermez l'éditeur.

> **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="\\Folder1\Folder2\…\ApplicationName"

  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="\Folder1\Folder2\…\ApplicationName"

  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 si le chemin d'accès au fichier de raccourci se termine par 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, consultez la section « Recommandations supplémentaires » de la rubrique Optimiser l'expérience utilisateur dans la documentation 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.

Pour plus d'informations, consultez Pré-lancement et persistance de session dans un groupe de mise à disposition dans la documentation 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 aux minutes ; M:T:W:TH:F:S:SU correspond au jour 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 :

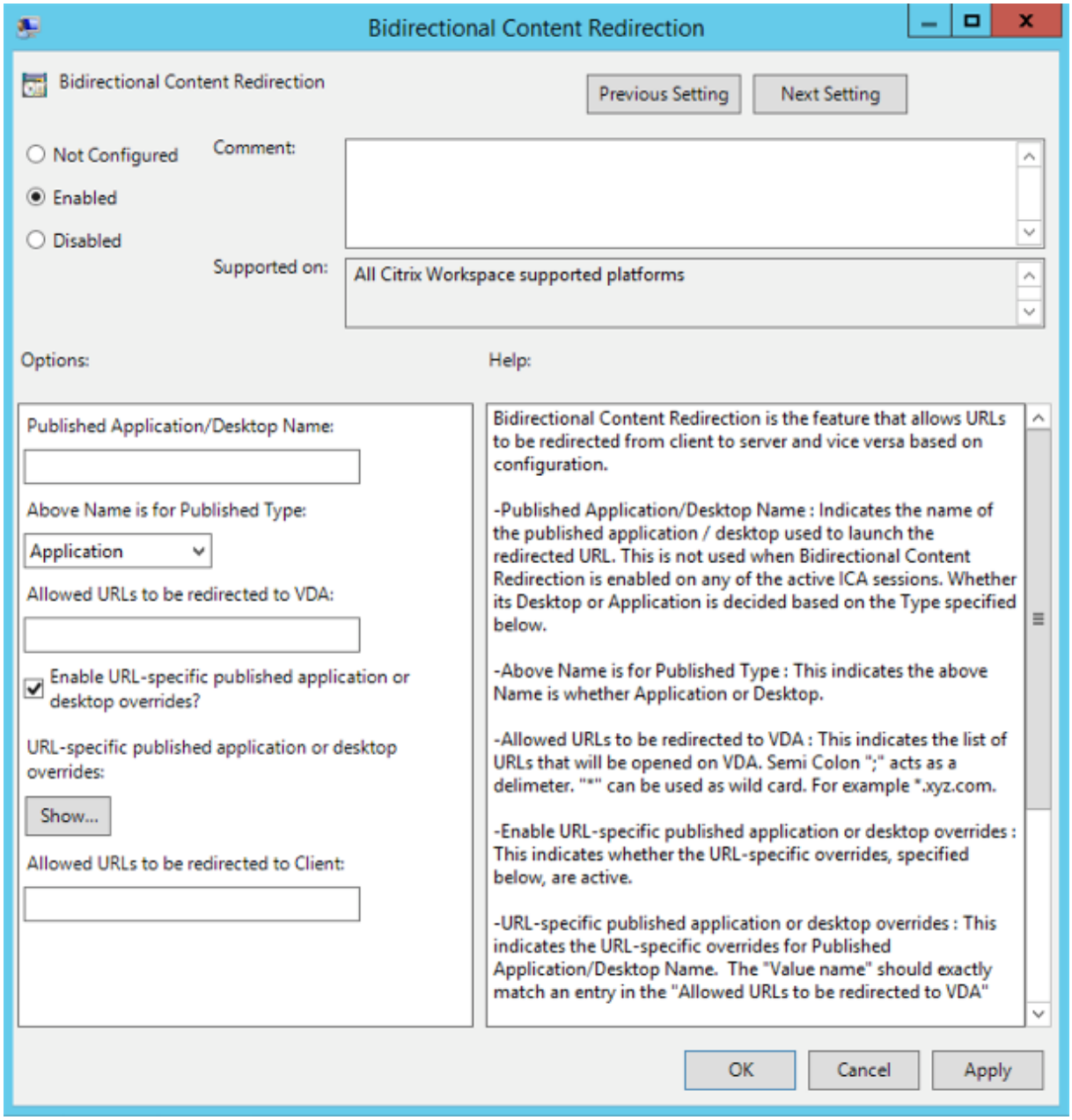
1. Modèle d'administration d'objet de stratégie de groupe
2. Éditeur du Registre

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

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**.

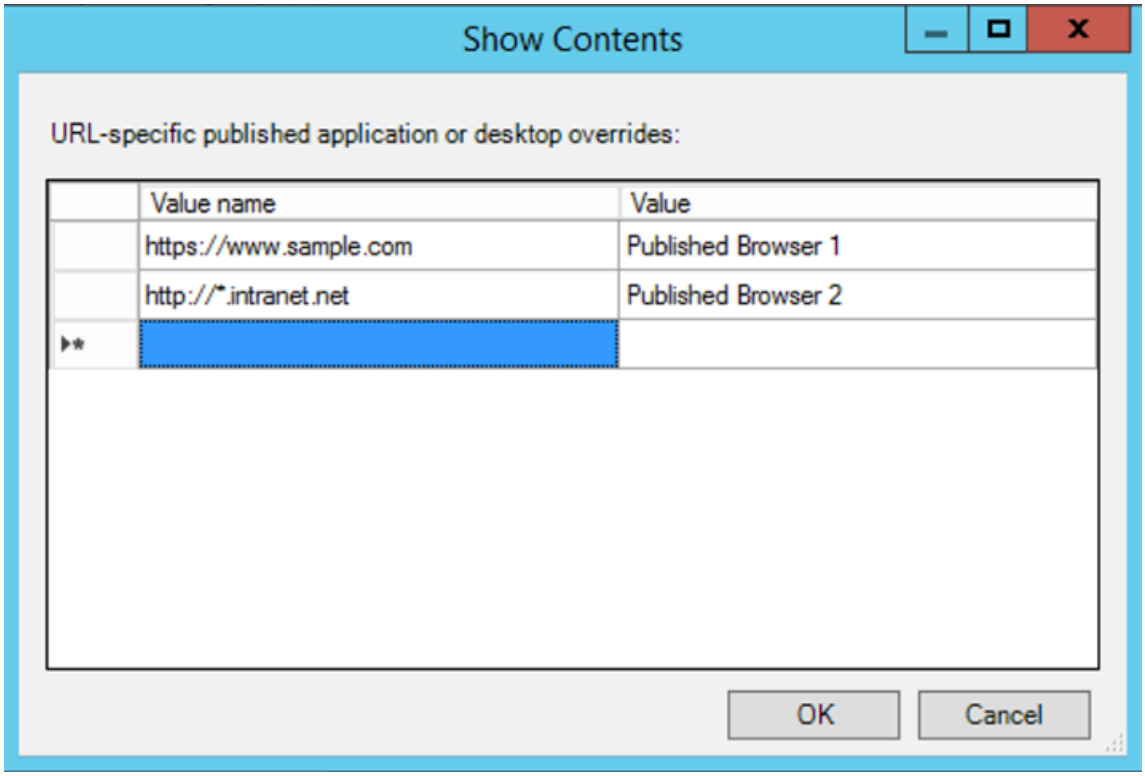


1. Dans le champ **Nom de l'application/du bureau publié**, indiquez le nom de la ressource utilisée pour lancer l'URL redirigée.

   > **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.

2. Dans le **Type de ressource utilisée pour la publication**, sélectionnez **Application** ou **Bureau** pour la ressource selon le cas.

3. Dans le champ **URL autorisées à être redirigées sur le VDA**, entrez l'URL à rediriger. Séparez la liste par des points-virgules.
4. Sélectionnez **Activer le remplacement des applications ou des postes publiés avec des URL spécifiques ?** pour remplacer une URL.
5. Cliquez sur **Afficher** pour afficher une liste dans laquelle le nom de la valeur doit correspondre à l'une des URL répertoriées dans le champ **URL autorisées à être redirigées sur le VDA**. La valeur doit correspondre au nom d'une application publiée.



6. Dans le champ **URL autorisées à être redirigées sur le client**, entrez l'URL à rediriger du serveur vers le client. Séparez la liste par des points-virgules.

> **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.

7. Cliquez sur **Appliquer**, puis sur **OK**.
8. 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.
> - Assurez-vous qu'une seule des stratégies d'association de type de fichier serveur et de redirection de contenu hôte est définie sur Activé sur la même machine. Citrix vous recommande de désactiver soit la fonctionnalité d'association de type de fichier serveur soit la fonctionnalité de redirection de contenu hôte (URL) pour vous assurer que la redirection d'URL fonctionne correctement.

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 d'applications et de bureaux virtuels. 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 l'Éditeur du Registre. 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 et Citrix DaaS 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).

Logiciels requis :

- 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

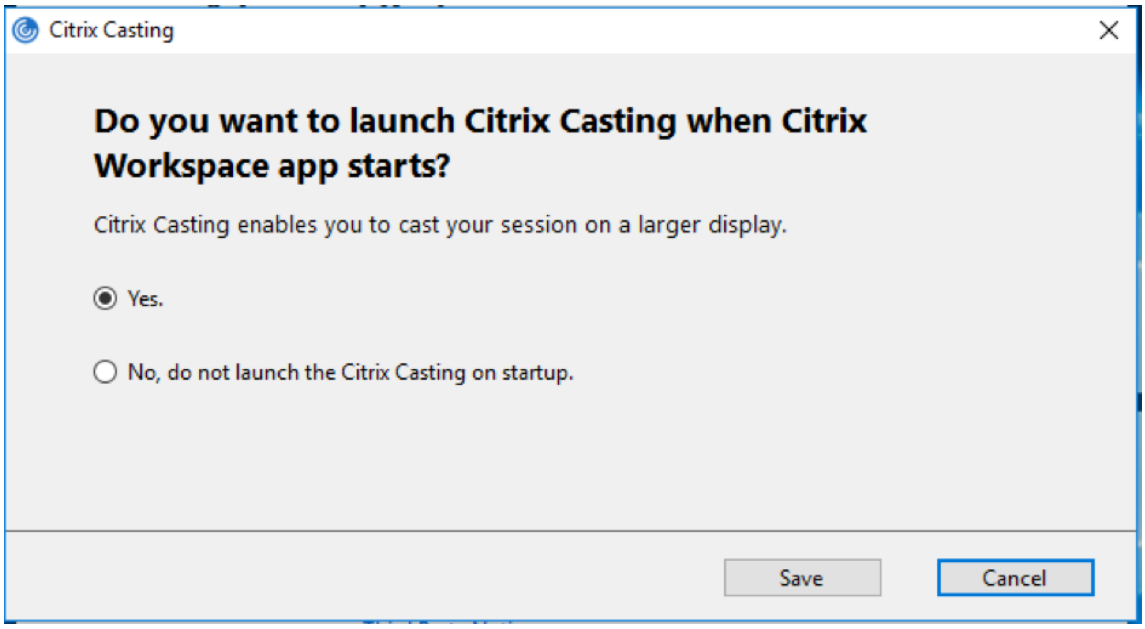
> **Remarque :**
>
> Vous pouvez masquer partiellement ou totalement la page Préférences avancées disponible à partir de l'icône de l'application Citrix Workspace dans la zone de notification. Pour plus d'informations, consultez la section Page Préférences avancées.

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 se lance au démarrage de l'application Citrix Workspace.
    - Non, ne pas lancer Citrix Casting au démarrage : indique que Citrix Casting ne se lance pas 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 hubs disponibles s'affiche. La liste est triée en fonction de la valeur RSSI du package de balises de Workspace Hub.

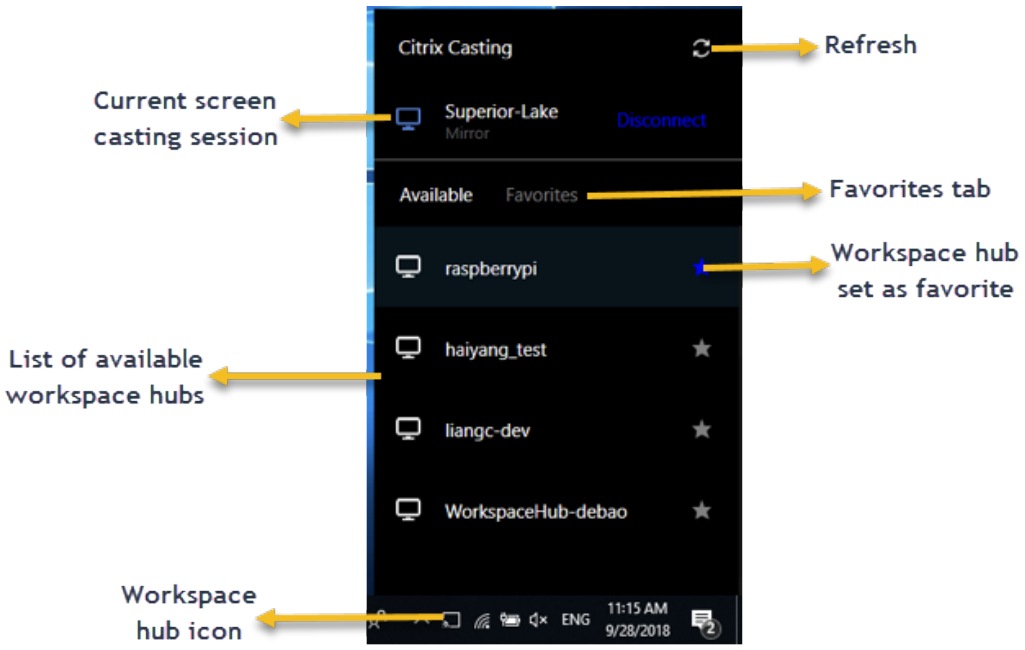
2. Sélectionnez le Workspace Hub pour la diffusion de votre écran et choisissez l'une des options suivantes :

    - **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 **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 Workspace Hub 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 :

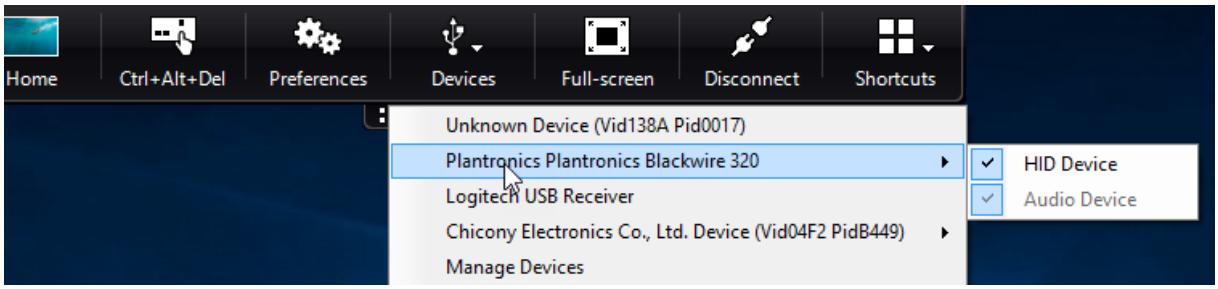
1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **Accès à distance des périphériques clients** > **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**.

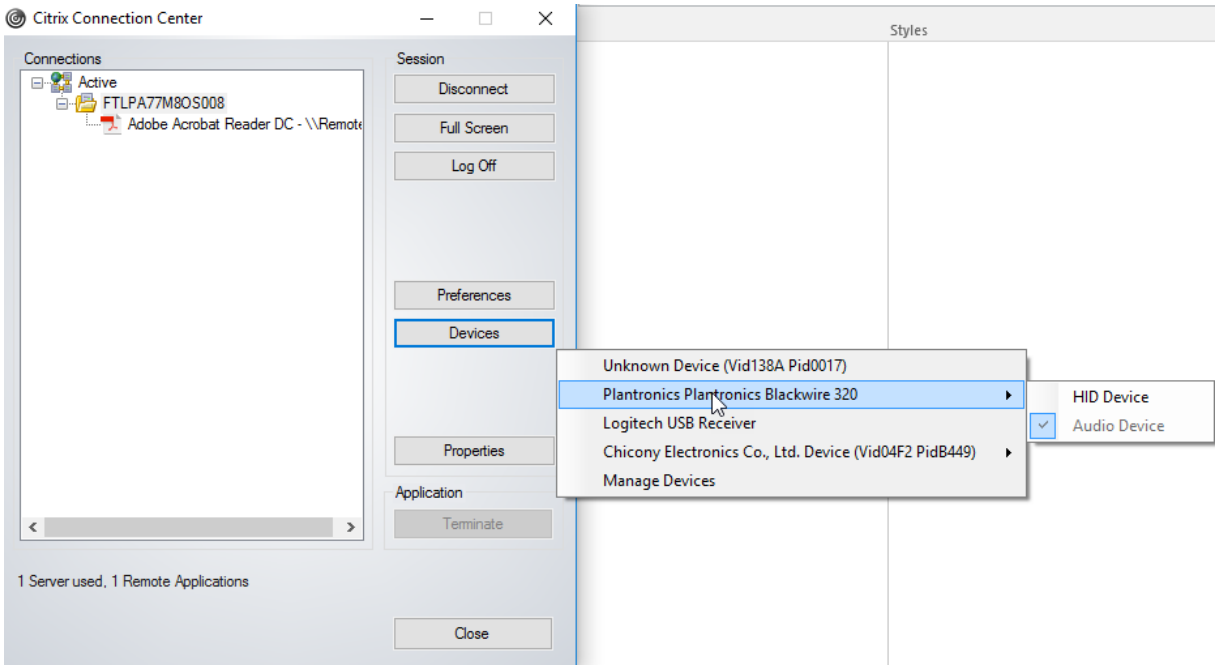
5. Dans la zone de texte **Règles de périphériques USB**, ajoutez le périphérique USB que vous souhaitez autoriser ou interdire.
   Par exemple, `ALLOW: vid=047F pid= C039 split=01 intf=00,03` autorise l'interface 00 et 03 et interdit les autres.
6. Cliquez sur **Appliquer**, puis sur **OK**.

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



> **Remarque :**
>
> Lorsque vous partitionnez un périphérique USB composite pour la redirection USB générique, vous devez sélectionner le périphérique à partir de Desktop Viewer ou du Centre de connexion pour rediriger le périphérique.

Dans une session d'application, les périphériques USB partitionnés 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
TRUE	Numéro valide 0 -n	Autorise l'interface spécifiée
TRUE	Numéro non valide	Autorise toutes les interfaces
FAUX	Toute valeur	Autorise USB générique du périphérique parent
Aucun 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
TRUE	Numéro valide 0 -n	Interdit l'interface spécifiée
TRUE	Numéro non valide	Interdit toutes les interfaces
FAUX	Toute valeur	Interdit USB générique du périphérique parent
Aucun 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 :

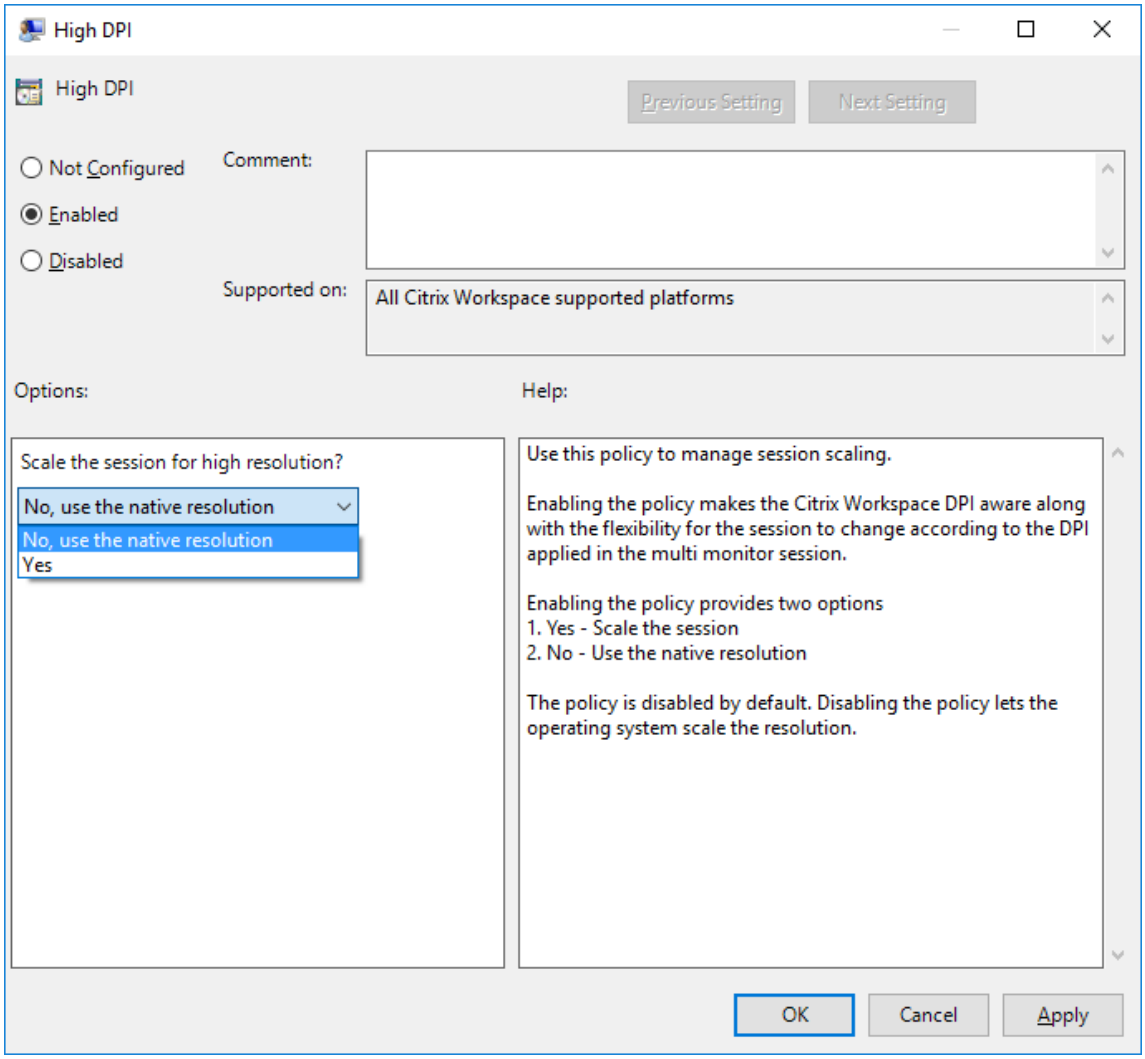
1. Modèle d'administration d'objet de stratégie de groupe (configuration par machine)
2. Préférences avancées (configuration par utilisateur)

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

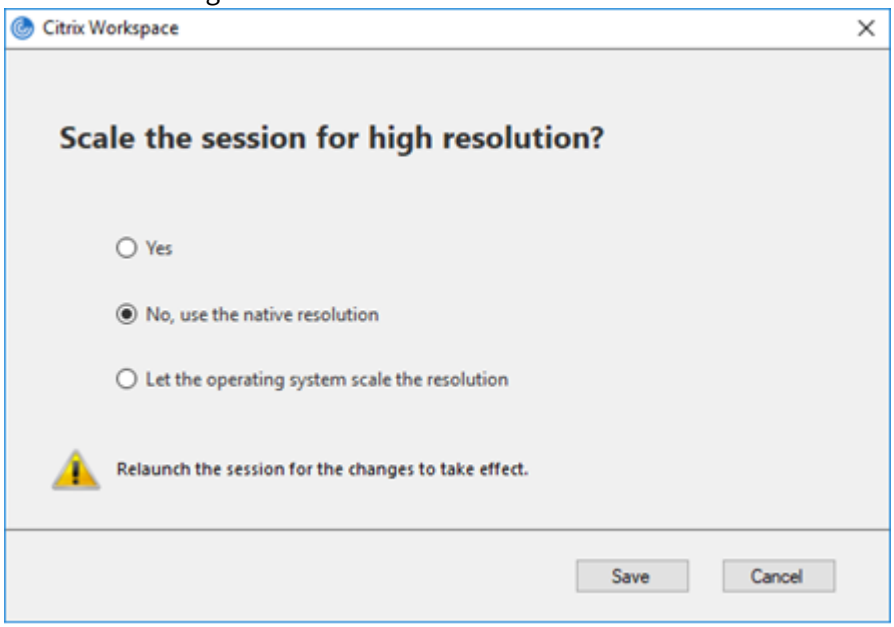
Configurer la mise à l'échelle DPI à l'aide de l'interface utilisateur graphique :

> **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, consultez la section 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 Paramètres 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 Citrix 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 con-

nectant 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.

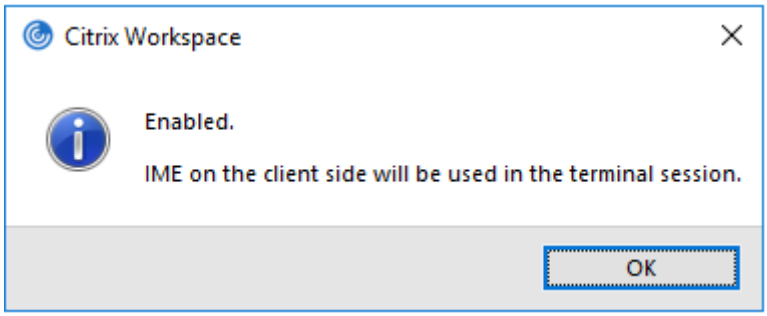
Vous pouvez définir un DPI pour les moniteurs virtuels qui sont utilisés pour la mise à l'échelle ou la correspondance DPI. Après avoir appliqué une disposition de moniteur virtuel, redimensionnez ou reconnectez la session.

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

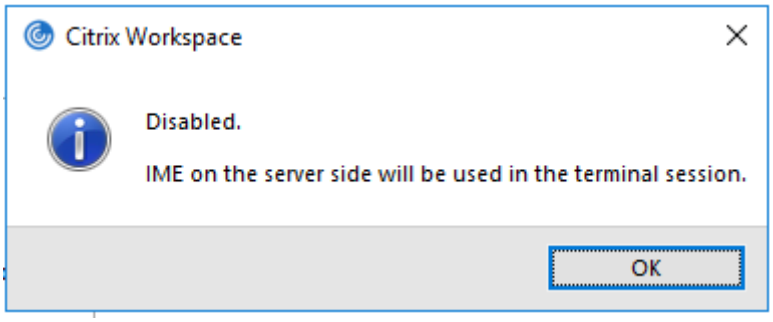
Éditeurs IME clients génériques

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`.

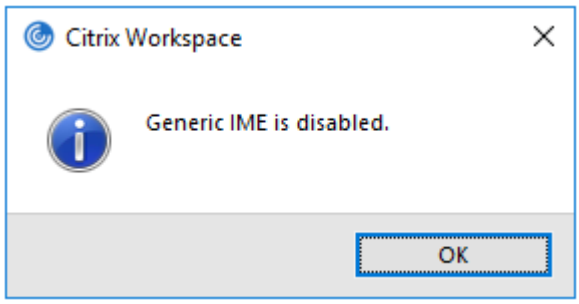


- Pour désactiver l'éditeur IME client générique, exécutez la commande `wfica32.exe /localime:off`à partir du dossier d'installation de l'application Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`.

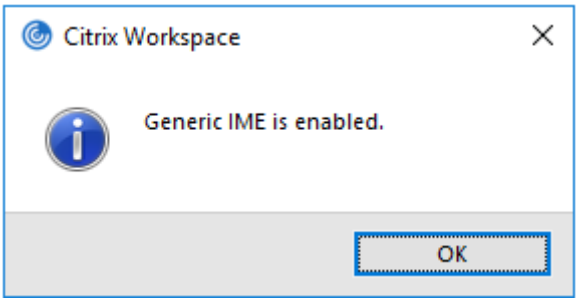


> **Remarque :**
>
> Vous pouvez utiliser le commutateur de ligne de commande `wfica32.exe /localime:on` pour activer l'éditeur IME client générique et la synchronisation de la disposition du clavier.

- 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.

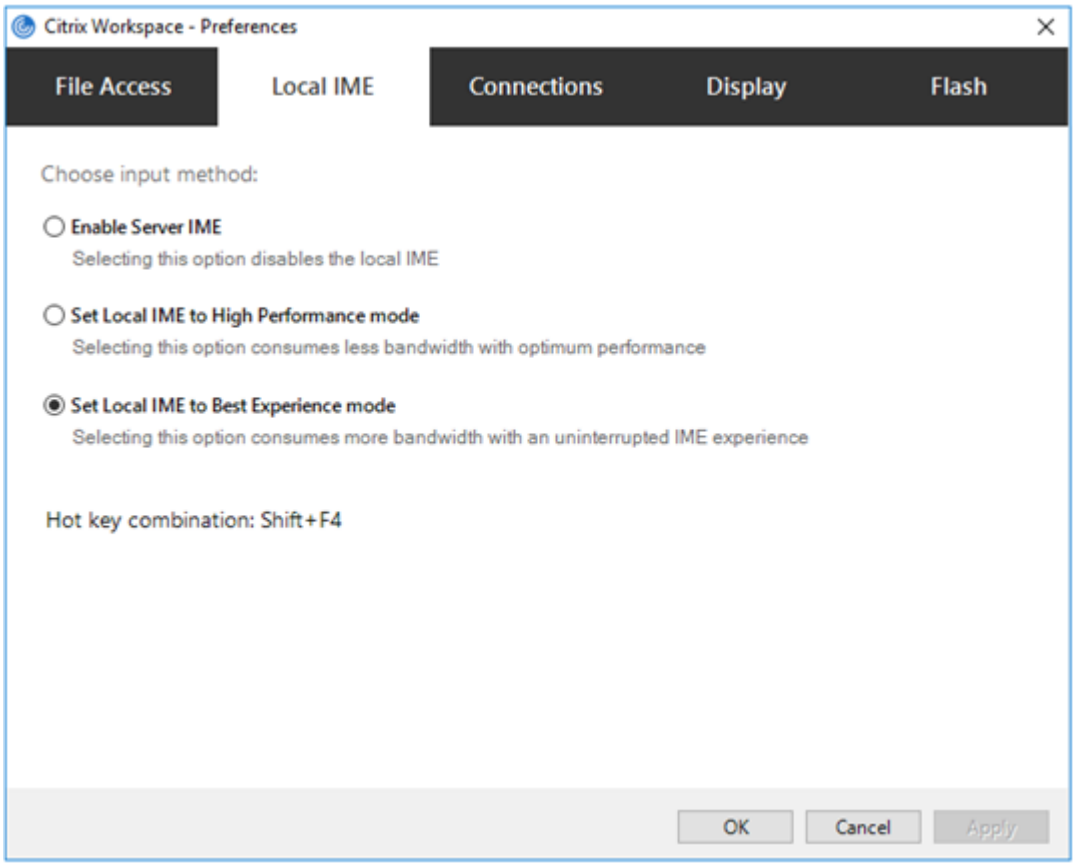
Configuration d'éditeurs IME clients génériques à l'aide de l'interface utilisateur graphique :

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, consultez la section 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 la case **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.

Logiciels requis :

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 du 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**, puis 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, puis 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

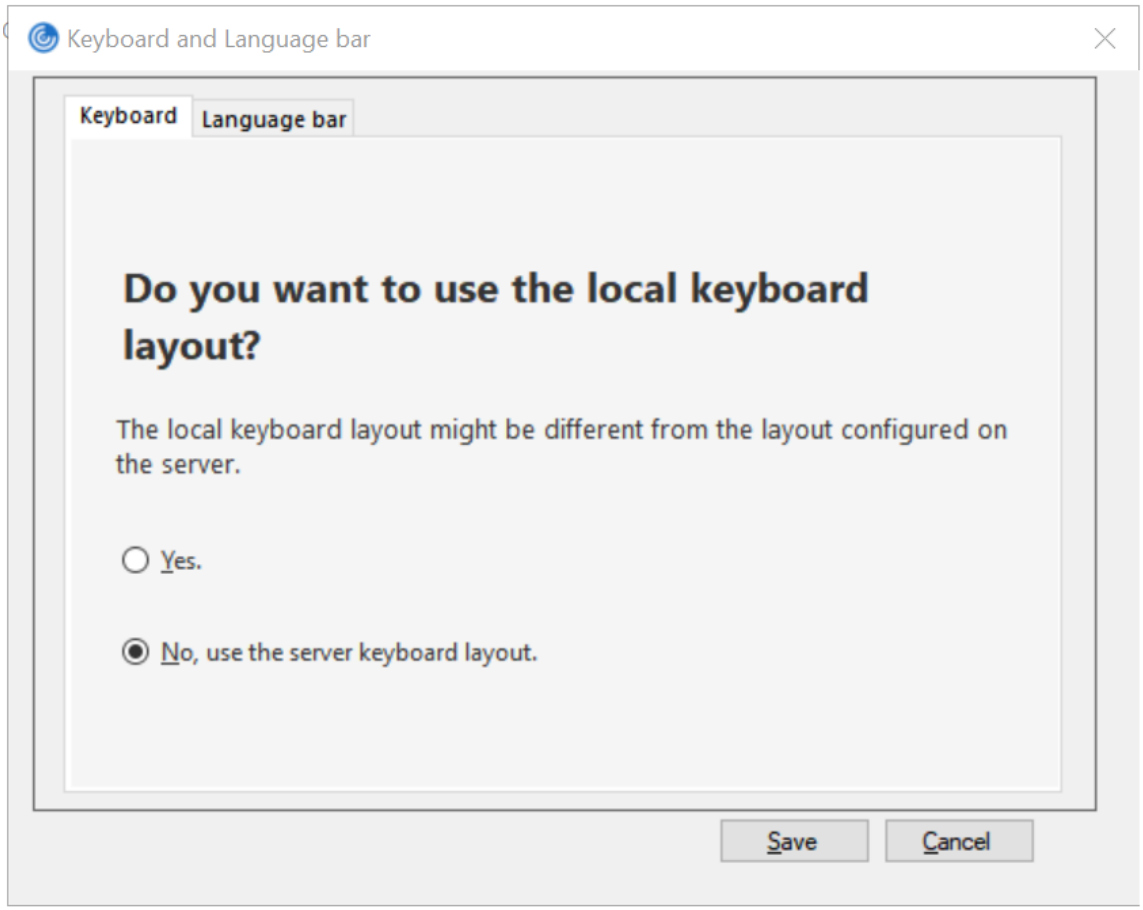
> **Remarque :**
>
> Vous pouvez masquer partiellement ou totalement la page Préférences avancées disponible à partir de l'icône de l'application Citrix Workspace dans la zone de notification. Pour plus d'informations, consultez la section Page Préférences avancées.

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 l'Éditeur du Registre. 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 avec un paramètre de registre sur le VDA : dans `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme`, ajoutez une nouvelle clé appelée **DisableKeyboardSync** et définissez la valeur sur 0.

Barre de langue

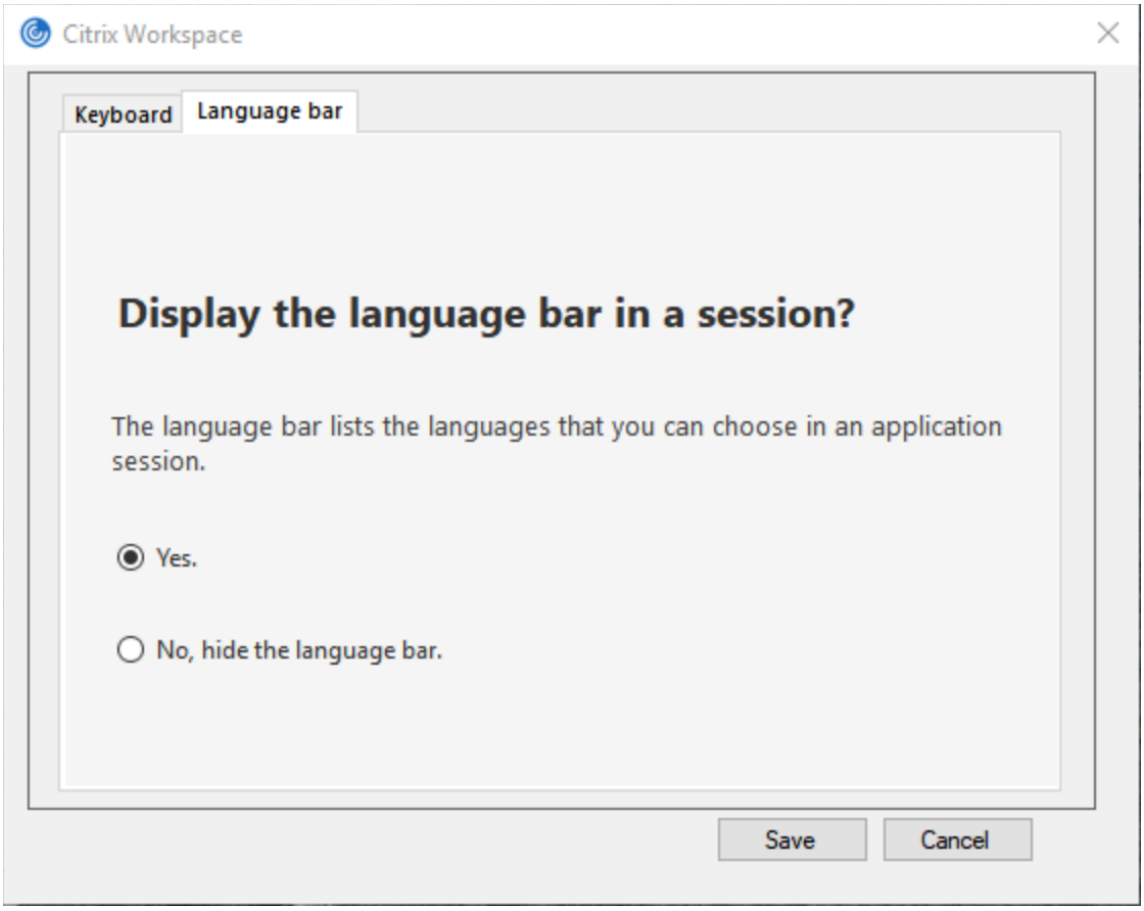
La barre de langue affiche la langue d'entrée préférée dans une session. Dans les versions antérieures, vous pouviez modifier ce paramètre en utilisant uniquement les clés de registre du VDA. À partir de Citrix Receiver pour Windows version 4.11, vous pouvez modifier les paramètres à l'aide de la boîte 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. Accédez 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 et Citrix DaaS. Vous pouvez brancher des périphériques USB à vos ordinateurs ; 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 et Citrix DaaS 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 d'applications et de bureaux virtuels ; 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 et Citrix DaaS. 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 d'applications et de bureaux virtuels :

- 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

Fonctionnalité	Mappage des lecteurs clients	Prise en charge USB
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 d'applications et de bureaux virtuels 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 configuration 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 l'Éditeur du Registre. 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, veuillez consulter la section Paramètres de stratégie Périphériques USB, voir 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 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.
> - 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 de l'application locale sur des bureaux publiés dans la documentation Citrix Virtual Apps and Desktops.

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

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 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** > **Self 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 :

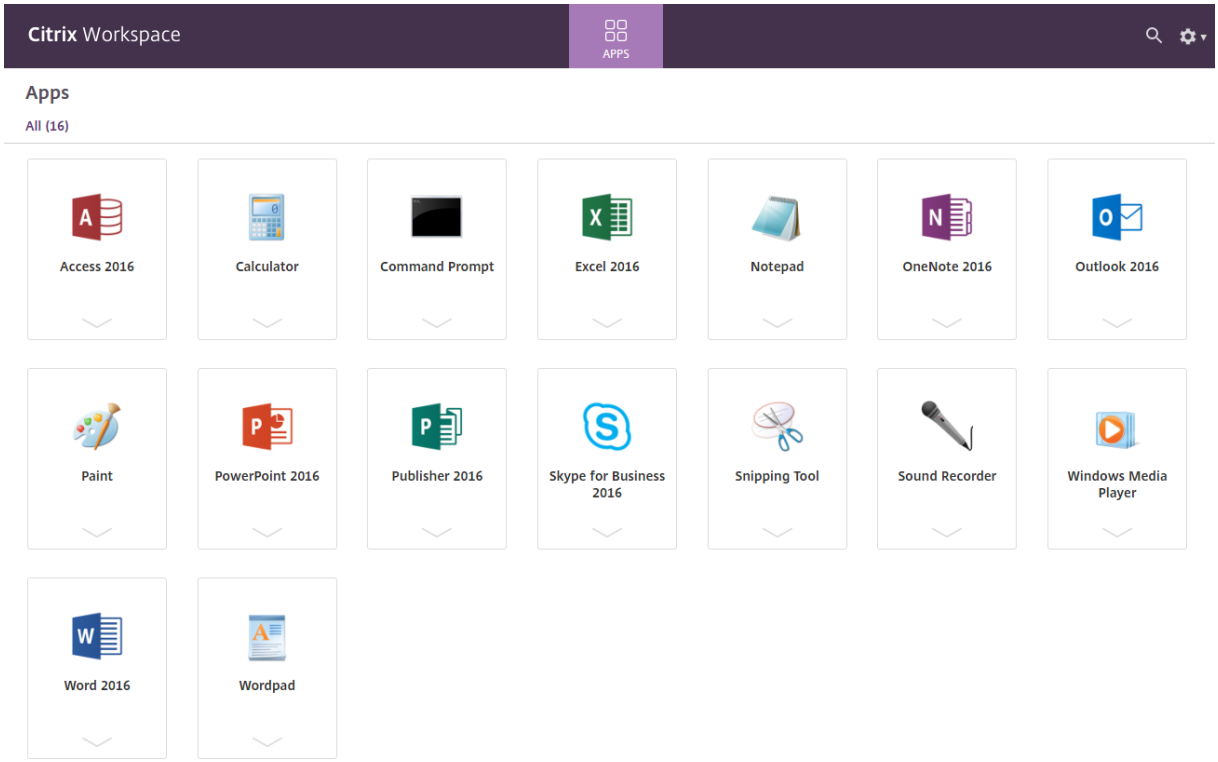
- Workspace pour Web ne prend pas en charge cette fonctionnalité.

Configuration de Workspace

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 ».



Applications SaaS

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.

Logiciels requis :

- 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 Citrix Enterprise Browser (anciennement Citrix Workspace Browser) 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 et les bureaux 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.

Configuration du cache à l'aide de l'objet de stratégie de groupe :

Lorsque plusieurs utilisateurs utilisent le même périphérique pour se connecter et accéder aux applications Secure SaaS, le cache est transféré à l'utilisateur suivant, partageant ainsi les informations de navigation entre les utilisateurs.

Pour résoudre ce problème, l'application Citrix Workspace propose une nouvelle stratégie d'administration d'objet de stratégie de groupe (GPO). Cette stratégie ne permet pas le stockage du cache du navigateur sur le périphérique local.

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 de l'ordinateur**, accédez à **Modèles d'administration** > **Citrix Workspace** > **Citrix Secure Browser**.
3. Sélectionnez la stratégie **Cache**.
   Remarque : cette stratégie est définie par défaut sur **Activé**.
4. Pour la désactiver, sélectionnez **Désactivé**, puis cliquez sur **Appliquer** et **OK**.
5. Redémarrez l'application Citrix Workspace pour que les modifications prennent effet.

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.

Impression PDF

Logiciels requis :

- 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 la 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 plus d'informations, veuillez consulter la section Mode tablette pour appareils à écran tactile dans la documentation 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.

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
```

```
1 - Name: Mouse
2 - Type: REG_SZ
3 - Value: 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 les paramètres **Souris relative**, activez l'option **Utiliser la souris relative**.
6. Cliquez sur **Appliquer** et **OK**.

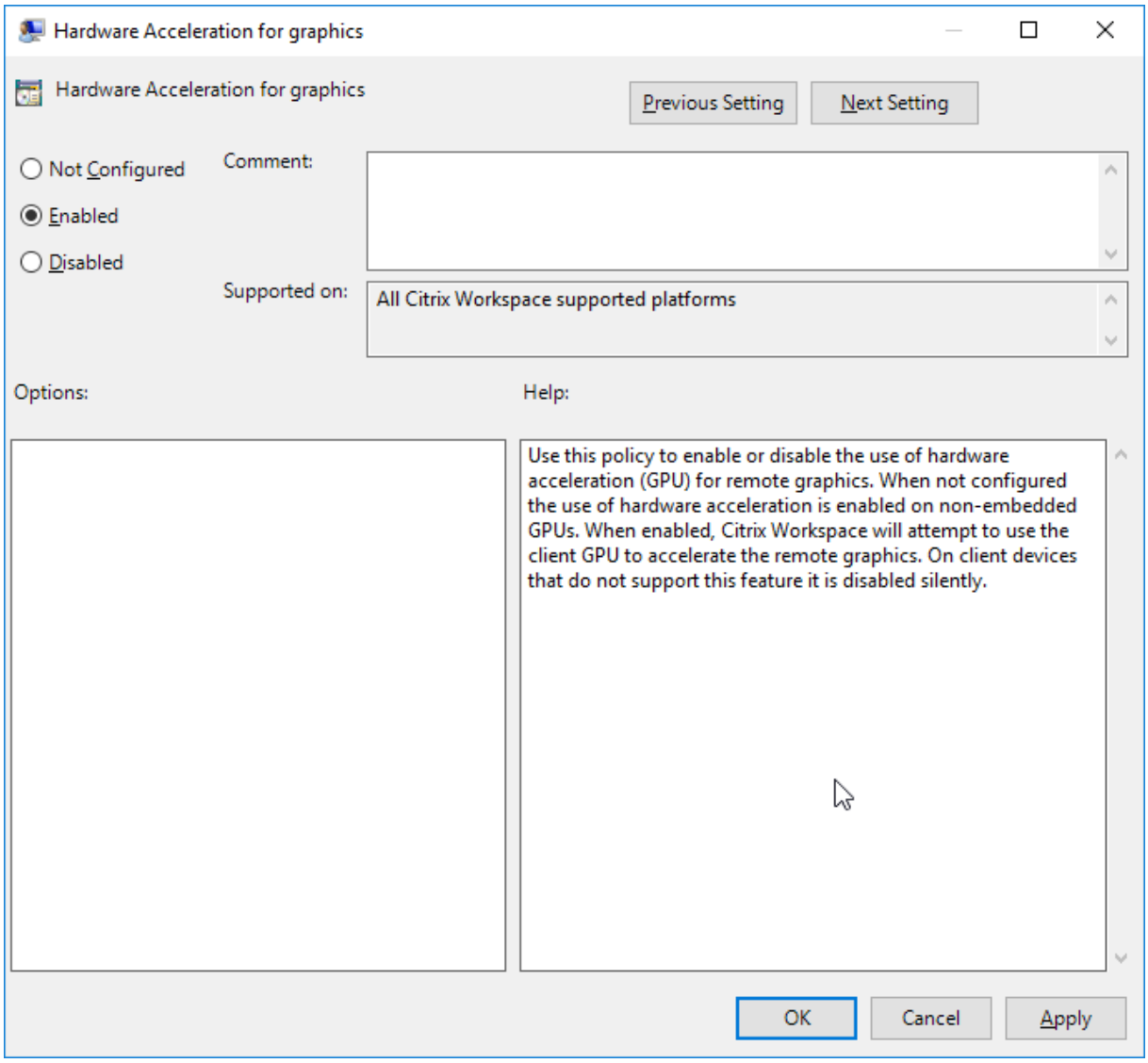
> **Remarque :**
>
> La configuration de la souris relative à partir de Desktop Viewer applique la fonctionnalité à chaque session uniquement.

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 et Citrix DaaS peuvent également utiliser les Préférences de Citrix Virtual Apps and Desktops Viewer pour désactiver leurs micros et webcams.

Prise en charge multi-moniteurs

L'application Citrix Workspace pour Windows permet d'utiliser jusqu'à huit moniteurs.

Chaque écran faisant partie d'une configuration multi-moniteur 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 et Citrix DaaS : pour afficher la fenêtre Desktop Viewer sur n'importe quel sous-ensemble de moniteurs, 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 et Citrix DaaS : 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 d'applications et de bureaux virtuels, 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-moniteur, 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 doit être en mesure de détecter chaque écran. Sur les plates-formes Windows, pour vérifier que cette détection se produit, accédez à **Paramètres** > **Système**, puis cliquez sur **Afficher** et confirmez que chaque écran apparaît 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 Desktop Viewer 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 et Citrix DaaS, 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 l'affichage du clavier à l'écran 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 valeur 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 couleur 32 bits :

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 l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Pour définir une profondeur préférée, vous pouvez ajouter une clé de registre de chaîne nommée `TWIDesiredIconColor` à `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences` et la définir sur 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 et Citrix DaaS 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 d'applications

et de bureaux virtuels), 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 la connexion 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, Citrix 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)

Données collectées	Description	Comment elles sont utilisées
Données de configuration et d'utilisation	Le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) rassemble des données de configuration et d'utilisation à partir de l'application Citrix Workspace pour Windows et les envoie automatiquement à Citrix et Google Analytics.	Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de l'application Citrix Workspace.

Informations supplémentaires

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

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

Vous pouvez désactiver l'envoi de données via le programme CEIP à Citrix et Google Analytics (à l'exception des deux éléments de données collectés pour Google Analytics indiqués par un * dans le deuxième tableau ci-dessous) comme suit :

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 boîte de dialogue **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**.

Vous pouvez également accéder à l'entrée de Registre suivante et définir la valeur comme suit :

Chemin : `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

Clé : `Enable_CEIP`

Valeur : `False`

> **Remarque :**
>
> Une fois que vous avez sélectionné **Non merci** dans la boîte de dialogue de collecte de données

> ou défini la clé `Enable_CEIP` sur `False`, si vous souhaitez désactiver l'envoi des deux derniers éléments de données CEIP collectés par Google Analytics (c'est-à-dire la version du système d'exploitation et la version de l'application Citrix Workspace), accédez à l'entrée de registre suivante et définissez la valeur comme suggéré :

Chemin : `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

Clé : `DisableHeartbeat`

Valeur : `True`

Les données spécifiques à CEIP collectées par Citrix sont les suivantes :

Version du système d'exploitation	Version de l'application Citrix Workspace	Périphériques externes connectés	Résolution de l'écran
Version de Flash	Configuration de Desktop Lock	Tactile	Configuration de l'authentification
Méthode de lancement de session	Configuration des graphiques	Configuration de Desktop Viewer	Impression
Erreur de connexion	Temps de lancement	Langue de l'application Citrix Workspace	Informations sur le VDA
État SSON	État d'installation	Temps d'installation	Protocole de connexion
Version d'Internet Explorer			

Les données spécifiques à CEIP collectées par Google Analytics sont les suivantes :

Version du système d'exploitation*	Version de l'application Citrix Workspace*	Configuration de l'authentification	Langue de l'application Citrix Workspace
Méthode de lancement de session	Erreur de connexion	Protocole de connexion	Informations sur le VDA
Configuration de l'installation	État d'installation	Disposition du clavier client	Configuration du magasin

Préférence de mise à jour automatique	Utilisation du Centre de connexion	Configuration de la fonction App Protection

Authentification

November 2, 2023

Sécurisez les connexions entre l'application Citrix Workspace et les ressources publiées pour optimiser la sécurité. Vous pouvez configurer les types d'authentification suivants :

- Authentification pass-through au domaine
- Carte à puce
- Authentification pass-through Kerberos

Authentification pass-through au domaine

Single Sign-On vous permet de vous authentifier et d'utiliser les applications et les bureaux virtuels sans procéder à une nouvelle authentification.

La connexion à l'application Citrix Workspace permet de transmettre vos informations d'identification et vos ressources énumérées à StoreFront.

Dans les versions antérieures, lorsqu'ils utilisaient Google Chrome, Microsoft Edge ou Mozilla FireFox, les utilisateurs pouvaient lancer des sessions d'authentification unique même si la fonctionnalité n'était pas activée.

À compter de la version 1905, tous les navigateurs Web requièrent la configuration de l'authentification unique à l'aide du modèle d'administration de l'objet de stratégie de groupe. Pour plus d'informations sur la configuration de l'authentification unique à l'aide du modèle d'administration d'objet de stratégie de groupe, reportez-vous à la section Configurer Single Sign-on avec 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 (GUI)

Configurer l'authentification Single Sign-On lors d'une nouvelle installation

Configuration de l'authentification Single Sign-On lors d'une nouvelle installation :

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 type de 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'authentification Single Sign-On n'est pas configurée, l'application Citrix Workspace 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 Workspace pour Web est requis	Lancez **Magasin** > **Workspace pour Web** > **Gérer les méthodes d'authentification** > activez **Authentification pass-through au domaine**.	Lorsque l'authentification Single Sign-On n'est pas configurée, l'application Citrix Workspace change automatiquement la méthode d'authentification de l'**authentification pass-through au domaine** vers **Nom d'utilisateur et mot de passe**, le cas échéant.

Cas d'utilisation	Détails de la configuration	Informations supplémentaires
Lorsque StoreFront n'est pas configuré	Si l'interface Web est configurée sur le VDA, lancez le site XenApp Services > **Méthodes d'authentification** > **Activer l'authentification pass-through**.	Lorsque l'authentification Single Sign-On n'est pas configurée, l'application Citrix Workspace 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** et **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 et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), 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

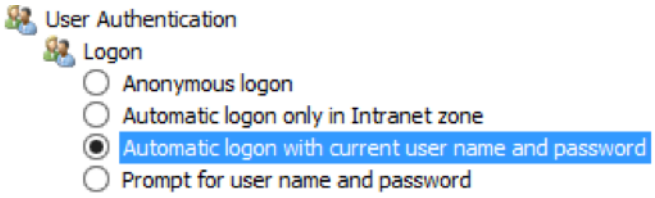
1. Ajoutez le serveur StoreFront à la liste de sites de confiance à l'aide d'Internet Explorer. Pour ce faire :

    a) Lancez **Options Internet** à partir du panneau de configuration.

b) Cliquez sur **Sécurité** > **Internet local**, puis 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** et **OK**.

2. Modifiez les paramètres **Authentification utilisateur** dans **Internet Explorer**. Pour ce faire :

a) Lancez **Options Internet** à partir du panneau de configuration.
b) Cliquez sur l'onglet **Sécurité** > **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**.



a) Cliquez sur **Appliquer** et **OK**.

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** et suivez les invites pour terminer l'installation.

Vous pouvez maintenant vous connecter 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** > **Citrix Workspace** > **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** et **OK**.
7. Redémarrez Workspace pour Web pour que les modifications prennent effet.

Vérifiez que l'authentification Single Sign-On est activée. 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

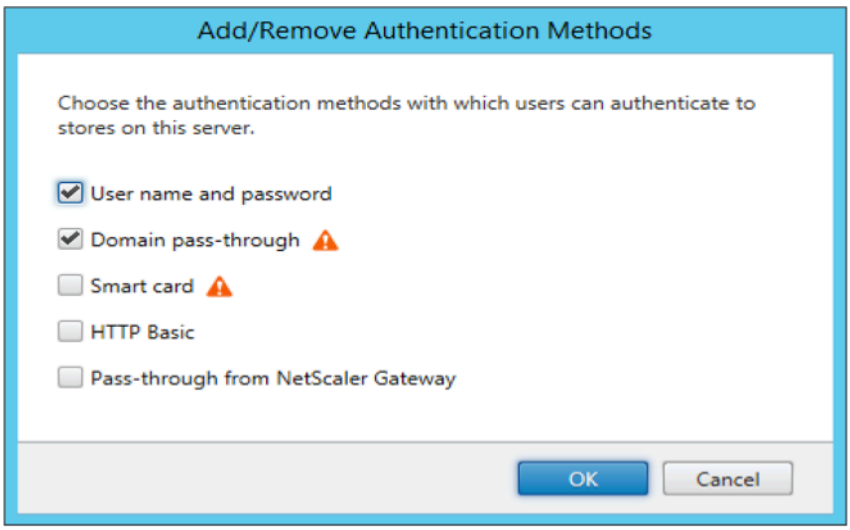
Vous pouvez configurer l'authentification Single Sign-On à l'aide d'Active Directory. Vous n'avez pas besoin d'utiliser des outils de déploiement, tels que Microsoft System Center Configuration Manager dans ce cas.

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 l'emplacement et la version de `CitrixWorkspaceApp.exe`.

4. Dans la console **Gestion des stratégies de groupe Active Directory**, entrez `CheckAndDeployWorkspace.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

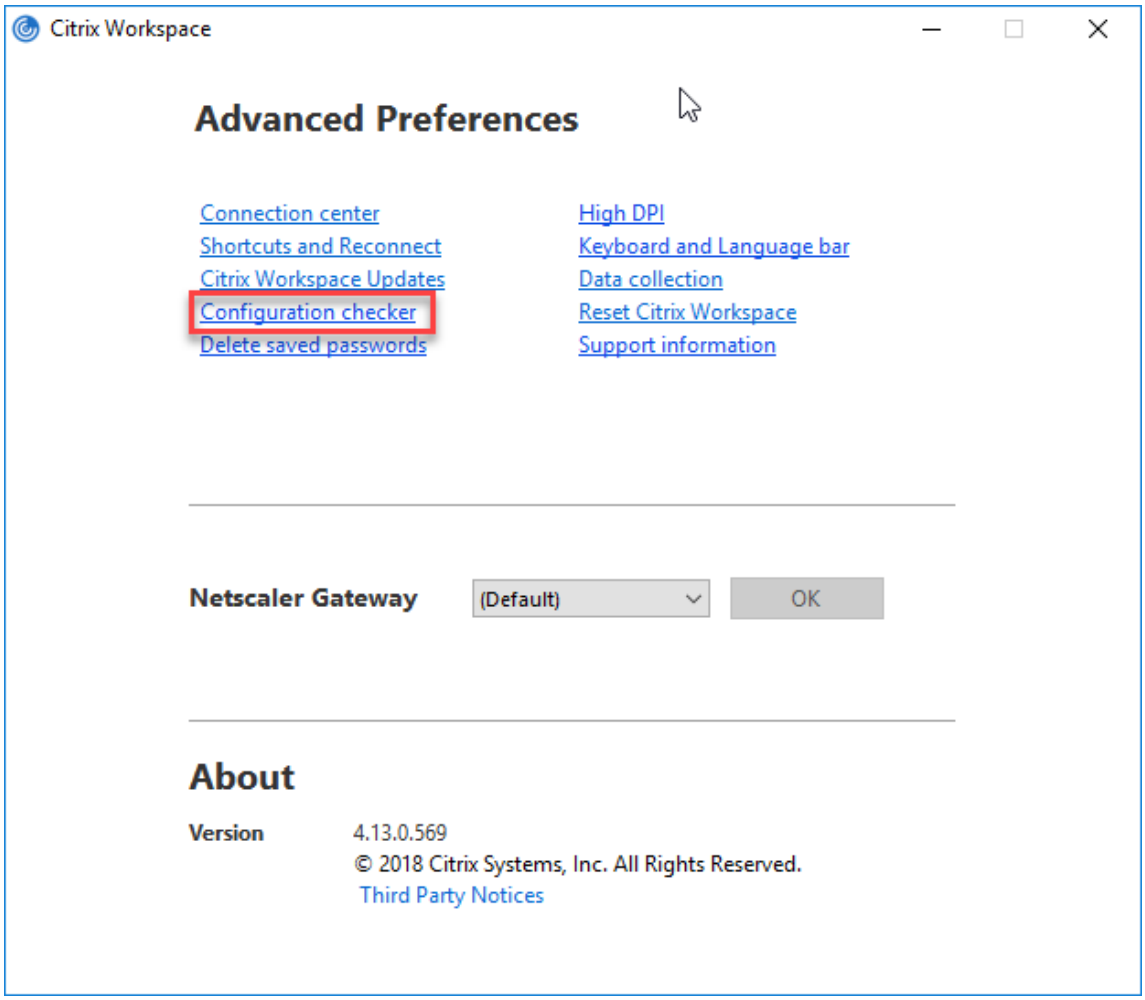
Configuration du StoreFront Ouvrez **Citrix Studio** sur le serveur StoreFront et sélectionnez **Authentification -> Ajouter/supprimer des méthodes d'authentification**. Sélectionnez **Authentification pass-through au domaine**.



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 Single Sign-On 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 Citrix** 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.

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 :**
>
> - Les résultats du test ne s'appliquent pas aux configurations Workspace pour Web.
> - Dans une configuration multi-magasins, le test de méthode d'authentification s'exécute 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** > **Citrix Workspace** > **Libre-service** > **DisableConfigChecker**.
3. Cliquez sur **Activé** pour masquer l'Outil d'analyse de la configuration dans la fenêtre **Préférences avancées**.

4. Cliquez sur **Appliquer** et **OK**.
5. Exécutez la commande `gpupdate /force`.

Limite :

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 le VDA.

Test de balise Le contrôleur de balises fait partie de l'utilitaire **Outil d'analyse de la configuration**. Il vous permet d'effectuer un test de balise pour confirmer si la balise (ping.citrix.com) est accessible. Ce test 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.

Authentification pass-through au domaine avec Kerberos

Cette rubrique s'applique uniquement aux connexions entre l'application Citrix Workspace pour Windows, StoreFront, Citrix Virtual Apps and Desktops et Citrix DaaS.

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).

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, Citrix Virtual Apps and Desktops et Citrix DaaS 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 Citrix Workspace les informations relatives à la disponibilité de Citrix Virtual Apps and Desktops et Citrix DaaS.

   > **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 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 et Citrix DaaS fournissent 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 et Citrix DaaS. 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 l'Éditeur du Registre. 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 :

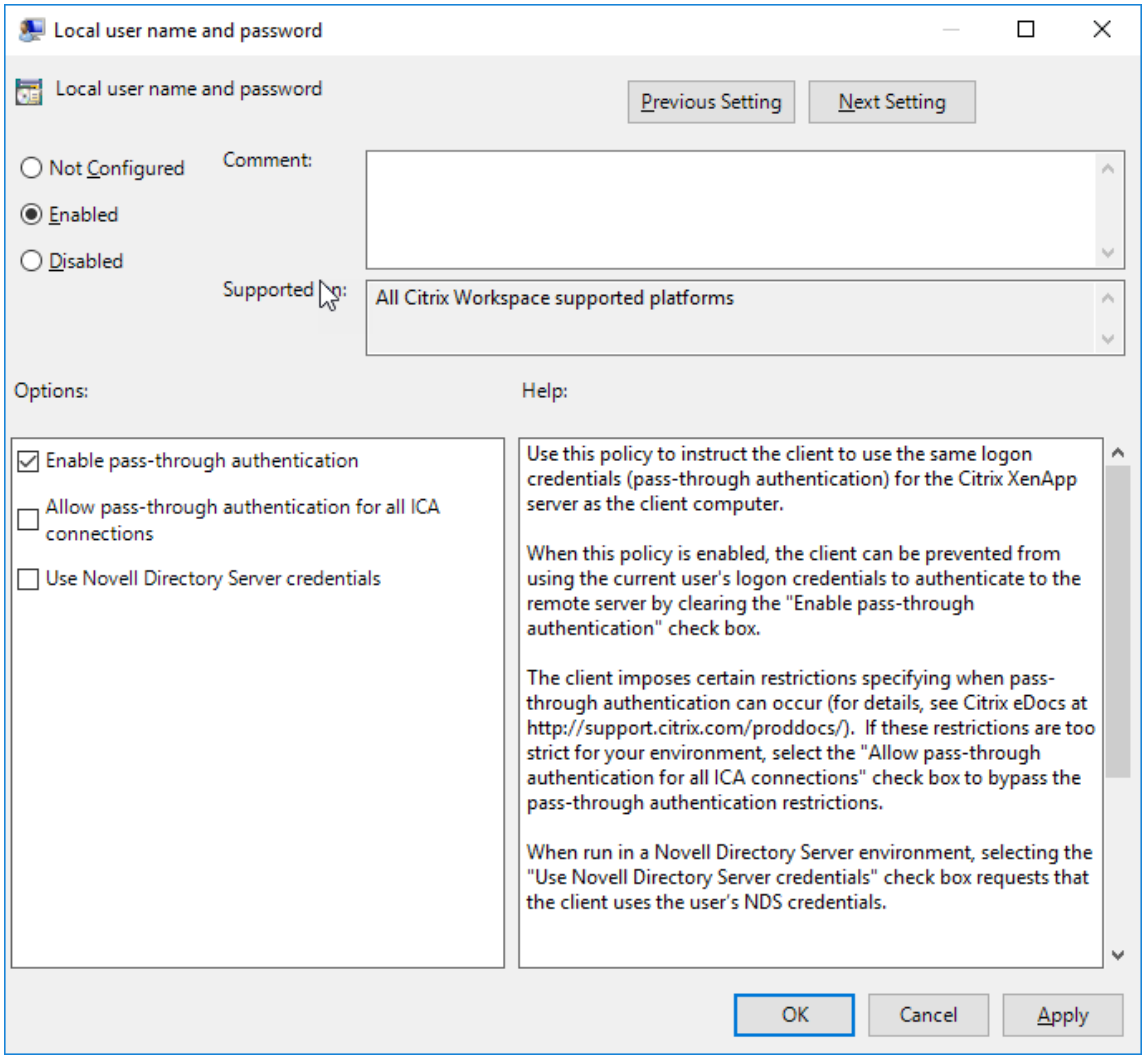
- `/includeSSON`

  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 et Citrix DaaS. Citrix Virtual Apps and Desktops et Citrix DaaS 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.

Carte 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 un bureau ou une application.

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.

- **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 d'applications et de bureaux virtuels.

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 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 ou HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\AuthManager:
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.

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.

Limite :

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

April 22, 2024

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.

Prise en charge du proxy ICA sortant

Smart Control permet aux administrateurs de définir des stratégies avancées pour configurer et appliquer les attributs d'environnement utilisateur pour Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktop Service) à l'aide de Citrix Gateway. Par exemple, vous pouvez interdire aux utilisateurs de mapper des lecteurs sur leurs bureaux distants. Cela peut être réalisé à l'aide de la fonctionnalité Smart Control de Citrix Gateway.

Toutefois, le scénario change lorsque l'application Citrix Workspace et Citrix Gateway appartiennent à des comptes d'entreprise distincts. Dans de tels scénarios, le domaine client ne peut pas appliquer la fonctionnalité Smart Control car la passerelle n'existe pas sur le domaine client. Au lieu de cela, vous pouvez utiliser le proxy ICA sortant. Le proxy ICA sortant vous permet d'utiliser la fonctionnalité Smart Control même lorsque l'application Citrix Workspace et Citrix Gateway sont déployées dans différentes organisations.

L'application Citrix Workspace prend en charge les lancements de session à l'aide du proxy LAN NetScaler. Un seul proxy statique peut être configuré ou le serveur proxy peut être sélectionné lors de l'exécution à l'aide du plug-in de proxy sortant.

Vous pouvez configurer les proxys sortants à l'aide des méthodes suivantes :

- Proxy statique : le serveur proxy est configuré en fournissant un nom d'hôte proxy et un numéro de port.
- Proxy dynamique : un serveur proxy unique peut être sélectionné parmi un ou plusieurs serveurs proxy à l'aide de la DLL du plug-in de proxy.

Vous pouvez configurer le proxy sortant à l'aide du modèle d'administration de l'objet de stratégie de groupe et de l'Éditeur du Registre.

Pour plus d'informations sur le proxy sortant, consultez la section Prise en charge du proxy ICA sortant dans la documentation Citrix Gateway.

Prise en charge du proxy sortant –Configuration

> **Remarque :**
>
> Si le proxy statique et le proxy dynamique sont tous deux configurés, la configuration du proxy dynamique a priorité.

Configuration du proxy sortant à l'aide du modèle d'administration de l'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** > **Citrix Workspace** > **Routage réseau**.
3. Sélectionnez l'une des options suivantes :
    - Pour le proxy statique : sélectionnez la stratégie **Configurer le proxy LAN NetScaler manuellement**. Sélectionnez **Activé**, puis indiquez le nom d'hôte et le numéro de port.
    - Pour le proxy dynamique : sélectionnez la stratégie **Configurer le proxy LAN NetScaler à l'aide de DLL**. Sélectionnez **Activé**, puis indiquez le chemin d'accès complet au fichier DLL. Par exemple, `C:\Workspace\Proxy\ProxyChooser.dll`.
4. Cliquez sur **Appliquer** et **OK**.

Configuration du proxy sortant à l'aide de l'Éditeur du Registre :

- **Pour le proxy statique :**

  - Lancez l'Éditeur du Registre et naviguez jusqu'à `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler`.
  - Créez des clés de valeur DWORD comme suit :

```
"StaticProxyEnabled"=dword:00000001
"ProxyHost"="testproxy1.testdomain.com
"ProxyPort"=dword:000001bb
```

- **Pour le proxy dynamique :**

  - Lancez l'Éditeur du Registre et naviguez jusqu'à `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler LAN Proxy`.
  - Créez des clés de valeur DWORD comme suit :

```
"DynamicProxyEnabled"=dword:00000001
"ProxyChooserDLL"="c:\\Workspace\\Proxy\\ProxyChooser.dll"
```

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.

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.

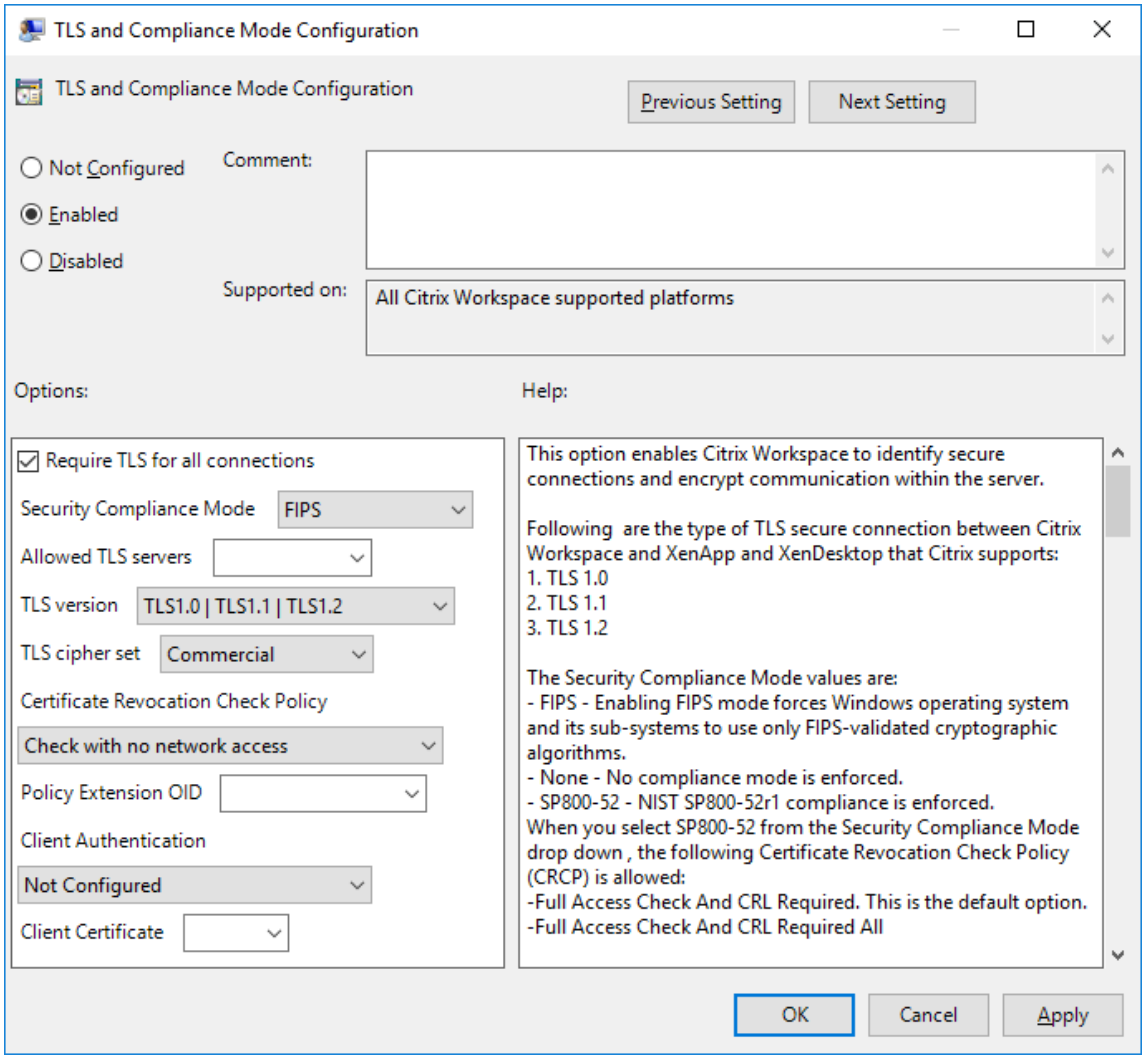
Vous pouvez utiliser les options suivantes pour :

- 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 et Citrix DaaS.
- 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.

   a) 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.

   b) Dans le menu **Mode de conformité aux normes de sécurité**, sélectionnez l'option appropriée :

      i. **Aucun** : aucun mode de conformité n'est appliqué.
      ii. **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.

i. **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.

c) 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.

d) 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.

a) **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

a) 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.

a) **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.

b) 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.

a) Utilisez le paramètre **Certificat client** pour spécifier l'empreinte numérique du certificat d'identification et éviter une intervention inutile de l'utilisateur.

b) 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

Pour plus d'informations sur les ports, consultez l'article CTX101810 du centre de connaissances.

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.

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.

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 Objets de stratégie de groupe ou de StoreFront. 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.

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.

Storebrowse

April 22, 2024

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 ou applications Citrix Virtual Apps and Desktops et Citrix DaaS publié(e)s (anciennement Citrix Virtual Apps and Desktops Service) à partir d'un magasin configuré
- Générer manuellement un fichier ICA en sélectionnant un bureau ou une application Citrix Virtual Apps and Desktops et Citrix DaaS 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 Configurer l'authentification pass-through au domaine.
- **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 prise en charge 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'

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 0
x2000 –E <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Exemple de commande sur Citrix Gateway :

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –M 0
x2000 –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_published_ 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_published_ 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_Name } <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 et Citrix DaaS 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 virtuels 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 virtuels 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.

Logiciels requis :

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 de 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** et **OK**.
5. Redémarrez la session de l'application Citrix Workspace pour que les modifications prennent effet.

Limites :

- 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 virtuels 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

January 17, 2024

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 suivant est disponible dans la barre d'outils :

- Ctrl+Alt+Suppr
- Préférences
- Appareils
- Déconnecter.

L'application Citrix Workspace pour Windows avec Desktop Lock fonctionne sur les machines appartenant à un domaine sur lesquelles SSON est activé et qui sont configurées avec un magasin. 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.

Installation de Desktop Lock à l'aide de l'interface de ligne de commande

Logiciels requis :

- Vous devez être l'administrateur sur une machine jointe au domaine.
- L'authentification unique doit être activée.
- Le magasin doit être configuré.

1. Installez l'application Citrix Workspace en exécutant la commande suivante :

```
`CitrixWorkspaceApp.exe /includeSSON /Silent STORE0= " AppStore;
    https://testserver.net/Citrix/MyStore/discover;on;Desktop App
    Store" `
```

2. Téléchargez le fichier `CitrixWorkspaceDesktopLock.msi` disponible sur la page Téléchargements Citrix.
3. Installez Desktop Lock en exécutant la commande suivante :

```
installationSilent : msiexec /i CitrixWorkspaceDesktopLock.msi /
qn
```

Le bureau publié est lancé automatiquement après la connexion en tant qu'utilisateur.

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.
- 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. Pour plus d'informations, consultez la section Configurer Local App Access et la redirection d'adresse URL dans la documentation Citrix Virtual Apps and Desktops.

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 Desktop Viewer.
- La plupart des touches de raccourci des fenêtres sont transmises à la session à distance, à l'exception de Windows+L.
- Ctrl+F1 déclenche Ctrl+Alt+Suppr lorsque vous désactivez la connexion ou Desktop Viewer pour les connexions de bureau.

> **Remarque :**
>
> Lorsque Desktop Lock est installé et que `LiveInDesktopDisconnectOnLock` est défini sur **False** dans le chemin du Registre `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` ou `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`, la session active est déconnectée lorsque le point final se réveille du mode veille prolongée ou du mode veille.

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 utilisant des cartes à puce, consultez la section Carte à puce.

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 les commandes, consultez la section Installer.

1. Dans le même dossier du support d'installation, cliquez deux fois sur `CitrixWorkspaceDesktopLock.msi`. L'assistant Desktop Lock apparaît. Suivez les invites.
2. 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 l'application Citrix Workspace pour 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 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 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

November 2, 2023

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 d'applications et de bureaux virtuels.

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

June 13, 2023

Le fichier de référence des paramètres 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.

Référence des paramètres ICA (PDF)