



Application Citrix Workspace 2402 LTSR pour Windows

Contents

À propos de l'application Citrix Workspace 2402 LTSR pour Windows	4
Application Citrix Workspace 2402 LTSR pour Windows	7
Problèmes résolus	71
Problèmes connus	73
Configuration système requise et compatibilité	74
Installer et désinstaller	80
Déployer	103
Configuration du magasin	112
Gestion des mises à jour et des plugins	125
Mise à jour	125
Gestion des plugins	138
Expérience de l'application	148
Mise à disposition d'applications	148
Amélioration de l'expérience de lancement de Virtual Apps and Desktops	161
Préférences de l'application	162
Applications SaaS	169
Collecte et surveillance des données	170
Sécurité et authentification	173
Sécurité	173
Sécuriser les communications	177
Authentification	194
Matrice d'authentification pass-through au domaine	220

Authentification pass-through au domaine pour Citrix Workspace en utilisant un Citrix Gateway local en tant que fournisseur d'identité	229
Authentification pass-through au domaine pour Citrix Workspace en utilisant Azure Active Directory en tant que fournisseur d'identité	246
Authentification pass-through au domaine pour Citrix Workspace en utilisant Okta en tant que fournisseur d'identité	250
HDX	252
Graphisme et affichage	252
Microsoft Teams optimisé	264
Transport HDX	267
Redirection du contenu du navigateur	268
Redirection bidirectionnelle du contenu	271
Référence des paramètres ICA	277
Appareils	278
Souris	278
Clavier	280
Impression	298
USB	301
Mappage des lecteurs clients	322
Microphone	325
Stratégie de groupe	325
Expérience de session	328
Citrix Workspace Desktop Lock	337
SDK (Software Development Kit) et API	344
Storebrowse	346

Storebrowse pour Workspace	357
Dépannage	359
Fin de prise en charge	365

À propos de l'application Citrix Workspace 2402 LTSR pour Windows

April 22, 2024

Cette documentation décrit les fonctionnalités et les configurations de l'application Citrix Workspace 2402 LTSR pour Windows. Cette version est la dernière version LTSR (Long Term Service Release) de l'application Citrix Workspace pour Windows et ne concerne que les clients LTSR.

La documentation de la version actuelle de l'application Citrix Workspace pour Windows est disponible à partir de [Application Citrix Workspace pour Windows](#). Pour de plus amples informations sur les cycles de vie des versions LTSR et CR, consultez la section [Étapes clés du cycle de vie de l'application Citrix Workspace](#).

Remarque :

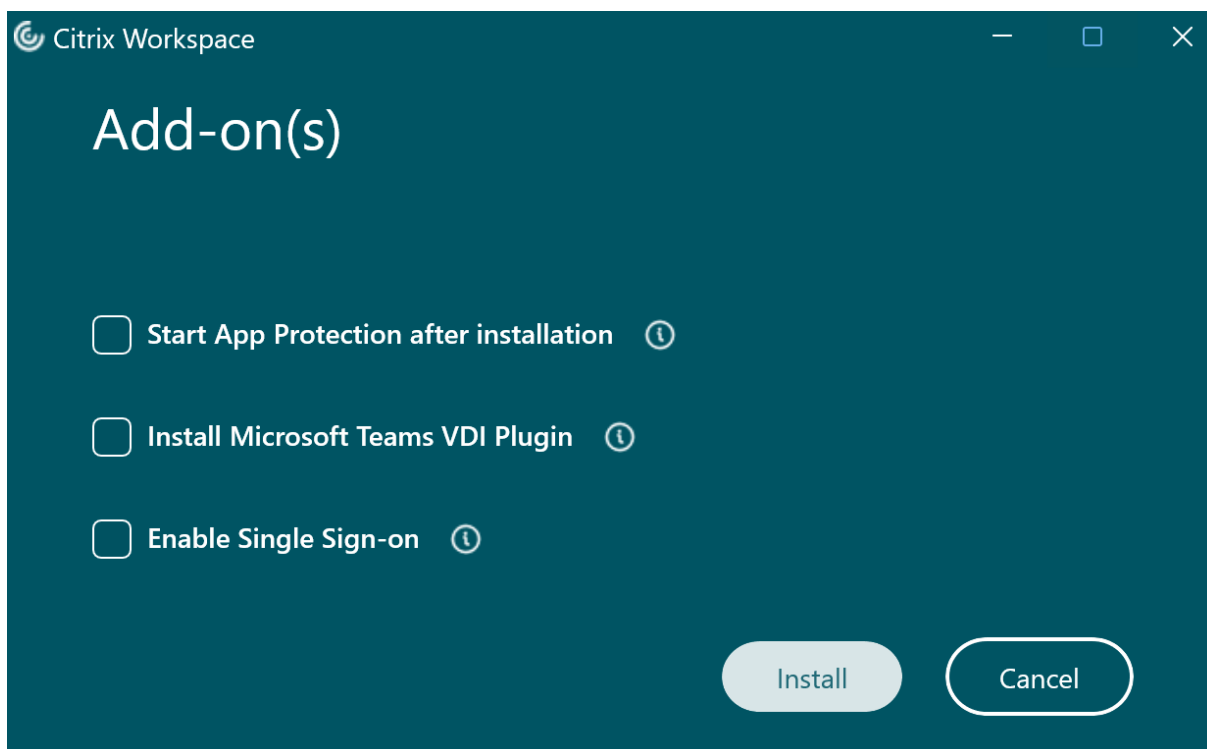
- Si vous avez activé la mise à jour automatique sur votre application Citrix Workspace et que vous avez opté pour le programme LTSR, l'application Citrix Workspace 2203.1 LTSR pour Windows se met automatiquement à jour vers l'application Citrix Workspace 2402 LTSR pour Windows.
- Si vous avez activé la mise à jour automatique sur votre application Citrix Workspace et que vous avez opté pour le programme CR, la version CR de l'application Citrix Workspace est automatiquement mise à jour vers l'application Citrix Workspace 2311.1 pour Windows.

Téléchargements

[Application Citrix Workspace 2402 LTSR pour Windows](#)

Nouveaux modules complémentaires et nouveau packaging

Pour l'application Citrix Workspace pour 2402 LTSR, vous pouvez installer le plug-in d'optimisation Microsoft Teams, Citrix Enterprise Browser et App Protection depuis la page Modules complémentaires lors de l'installation de l'application Citrix Workspace. Vous pouvez gérer ces modules complémentaires indépendamment de l'application Citrix Workspace. Par exemple, vous pouvez les mettre à jour ou les désinstaller indépendamment de l'application Citrix Workspace.



Pré-requis pour .NET 6.0.25

La dernière version de l'application Citrix Workspace 2402 LTSR nécessite .NET 6.0.25 et est également compatible avec les versions supérieures de .NET.

Modification du comportement d'optimisation de Microsoft Teams

Avec la version 2402 LTSR de l'application Citrix Workspace, les utilisateurs ont désormais la possibilité d'installer le nouveau plug-in VDI Microsoft Teams lors de l'installation de l'application Citrix Workspace, directement depuis l'écran des modules complémentaires.

Pour de plus amples informations, consultez la section [Nouveautés](#).

Vous pouvez également consulter [Prise en charge Microsoft Teams 2.1 pour VDI/DaaS](#).

Nouvelles fonctionnalités et améliorations

Pour plus d'informations sur les nouvelles fonctionnalités, les problèmes résolus et les problèmes connus de cette version, consultez les sections suivantes.

- [Nouveautés de la version 2402 LTSR](#)
- [Problèmes résolus dans la version 2402 LTSR](#)
- [Problèmes connus dans la version 2402 LTSR](#)

Liens utiles

- [Tableau des fonctionnalités de l'application Citrix Workspace](#)
- [Étapes clés du cycle de vie de l'application Citrix Workspace](#)
- [Informations supplémentaires sur le cycle de vie pour Citrix Receiver pour Windows](#)

Modifications apportées aux noms et aux numéros de version des produits Citrix

Pour plus d'informations sur les modifications apportées aux noms du produit et aux numéros de version en 2018, reportez-vous à la section [Nouveaux noms et numéros](#).

Composants de base

Composants LTSR 2402 de base	Version
Citrix Virtual Apps and Desktops 7 LTSR avec mises à jour cumulatives	1912 LTSR
Citrix Virtual Apps and Desktops 7 LTSR avec mises à jour cumulatives	2203.1 LTSR
Citrix Virtual Apps and Desktops 7 CR	2402 CR

Composants compatibles

Les composants suivants sont compatibles avec les environnements LTSR. Ils ne bénéficient pas des avantages du programme LTSR (cycle de vie prolongé et mises à jour cumulatives contenant uniquement des corrections).

Composants et fonctionnalités compatibles

Citrix Endpoint Analysis

Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)

Redirection du contenu du navigateur

Citrix Enterprise Browser

Application Citrix Workspace 2402 LTSR pour Windows

April 23, 2024

Découvrez les nouvelles fonctionnalités et améliorations disponibles pour l'application Citrix Workspace 2402 LTSR pour Windows.

Important :

Citrix Enterprise Browser peut être utilisé comme composant compatible avec l'application Citrix Workspace LTSR. Cependant, il n'est pas installé par défaut.

Pour installer Citrix Enterprise Browser, ajoutez le paramètre du commutateur d'installation `InstallEmbeddedBrowser=Y` ou `Addlocal CitrixEnterpriseBrowser` dans le cadre d'une installation avec ligne de commande.

Nouveautés de la version 2402 LTSR

La liste suivante répertorie les fonctionnalités disponibles dans l'application Citrix Workspace 2402 LTSR pour Windows.

Remarque :

Pour plus d'informations sur les nouveaux modules complémentaires et les modifications apportées au packaging, consultez la section [Nouveaux modules complémentaires et packaging](#).

- 2402
 - Initiative de développement durable pour le lancement d'un cloud hybride
 - Authentification pass-through au domaine amélioré pour l'authentification unique (authentification unique améliorée)
 - Prise en charge des stratégies NetScaler avancées pour Storebrowse sous Windows
 - Mise à niveau de la version pour Chromium Embedded Framework
 - Installer le plug-in VDI Microsoft Teams pour Citrix
 - Partage du son du système lors de réunions (Technical Preview)
 - Masquer l'option de dépannage pour les utilisateurs
 - App Protection
 - * Liste verte des captures d'écran
 - * Liste d'exclusion des processus
 - * Liste d'exclusion des pilotes de filtre USB

- Citrix Endpoint Analysis
- Citrix Enterprise Browser
 - * Indicateur de sécurité lors de la consultation de sites Web
 - * Citrix Enterprise Browser introduit des paramètres supplémentaires dans Global App Configuration Service
- 2311.1
 - Présentation du nouveau programme d'installation de l'application Citrix Workspace
 - Prise en charge du Gestionnaire d'activités dans les magasins cloud
 - Sélection automatique du codec vidéo
 - Mode de tolérance de pertes pour l'audio
 - Synchronisation de plusieurs claviers en début de session
 - Amélioration des performances de la redirection du contenu du navigateur
 - Mise à niveau de la version pour Chromium Embedded Framework
 - Mise à jour importante concernant les noms de pilotes et de fichiers d'App Protection
 - Flou et effets d'arrière-plan pour optimiser Microsoft Teams avec HDX
 - Citrix Enterprise Browser
 - * [Amélioration de l'expérience utilisateur et du temps de rechargement des sessions](#)
 - * [Amélioration du design des filigranes](#)
 - * [Prise en charge de l'extension de navigateur personnalisée](#)
 - * Simplification de la SSO aux applications Web et SaaS grâce à Global App Configuration Service
 - * [Gestion de l'authentification directe dans Citrix Enterprise Browser](#)
 - * [Amélioration des fonctionnalités de surveillance des activités des utilisateurs finaux](#)
- 2309
 - Conditions préalables supplémentaires pour .NET
 - Amélioration de l'expérience de lancement de Virtual Apps and Desktops
 - Ajout de l'option Dépannage dans la barre d'état système de l'application Citrix Workspace
 - Initiative de développement durable pour l'application Citrix Workspace
 - Commandes pour configurer la synchronisation de la disposition du clavier à l'aide de l'interface de ligne de commande
 - Commande pour nettoyer et installer l'application Citrix Workspace
 - Mises à jour de Microsoft Teams optimisé
 - App Protection
 - * Mise à jour importante concernant les noms de fichiers
 - * Détection d'altération des stratégies
 - * App Protection avec scénario double saut

- Citrix Enterprise Browser
 - * [Authentification via Citrix Enterprise Browser](#)
- 2307
 - Ajout de la prise en charge de tonalités courtes dans Microsoft Teams optimisé
 - Citrix Enterprise Browser
 - * [Raccourci Citrix Enterprise Browser](#)
- 2305.1
 - Amélioration de l'expérience de lancement de Virtual Apps and Desktops
 - Suivi de l'état de la commande Storebrowse
 - Prise en charge des méthodes d'authentification modernes pour les magasins StoreFront
 - Prise en charge de plus de 200 groupes dans Azure AD
 - App Protection
 - * Amélioration de la protection contre l'enregistrement de frappe
 - Citrix Enterprise Browser
 - * Prise en charge des extensions de navigateur
 - * Modification de la mise en œuvre de la stratégie Authentification par mot de passe sécurisé (SPA) sur les applications Web et SaaS internes
 - * Utiliser Global App Config Service pour gérer Citrix Enterprise Browser
- 2303
 - Configurer le chemin du stockage des données temporaires du navigateur pour la superposition de redirection du contenu du navigateur
 - Prise en charge des méthodes d'authentification modernes pour les magasins StoreFront
 - Expérience améliorée pour des visioconférences dans Microsoft Teams optimisé
 - Amélioration de la App Protection : injection anti-DLL
 - Citrix Enterprise Browser
 - * Prise en charge de Secure Private Access pour StoreFront
- 2302
 - Amélioration de l'expérience de reconnexion d'applications et de bureaux virtuels
 - Gestion des applications clientes pour le plug-in Zoom
 - Modification du comportement de sélection des périphériques audio pour la version optimisée de Microsoft Teams
 - Amélioration de App Protection
 - Citrix Enterprise Browser
 - * Ouvrir toutes les applications Web et SaaS via Citrix Enterprise Browser

- * Option permettant de démarrer Citrix Enterprise Browser depuis l'application Citrix Workspace
- 2212
 - Gestion des applications clientes
 - Contrôle de la version à mise à jour automatique
 - Forcer l'invite de connexion pour le fournisseur d'identité fédéré
 - Expérience de reconnexion améliorée après expiration du fichier de location de connexion
 - Prise en charge de l'installation par défaut de la App Protection
 - Amélioration de la App Protection : détection et notification de capture d'écran
 - Optimisation de Desktop Viewer
 - Citrix Enterprise Browser
 - * Définir Citrix Enterprise Browser comme navigateur de travail
- 2210.5
 - Amélioration de la mise à jour automatique
- 2210
 - Flou d'arrière-plan pour la redirection de la webcam
 - Améliorations d'App Protection pour les applications Web et SaaS sur Windows 11
 - Limiter les résolutions vidéo
 - Changement de nom pour Citrix Workspace Browser
 - Ouvrir toutes les applications Web et SaaS via Citrix Enterprise Browser
 - Prise en charge de la mise à jour automatique de l'application Citrix Workspace sur le VDA
 - Citrix Enterprise Browser (anciennement Citrix Workspace Browser)
- 2207
 - Flou et effets d'arrière-plan pour l'optimisation de Microsoft Teams avec HDX
 - Amélioration apportées à la mise à jour automatique
 - Remarque sur la mise à jour de l'application Citrix Workspace
- 2206
 - Performances graphiques améliorées
 - Activer la correspondance DPI
- 2205
 - Modifications apportées à Citrix Casting
 - Accès rapide aux ressources
 - Déconnexion du magasin Web personnalisé en quittant l'application Citrix Workspace

- Prise en charge de l'ouverture de l'application Citrix Workspace en mode agrandi
- Prise en charge de Storebrowse pour Workspace
- 2204.1
 - Amélioration de la redirection audio
 - Optimisation pour Microsoft Teams

2402 LTSR (version initiale)

Initiative de développement durable pour le lancement d'un cloud hybride

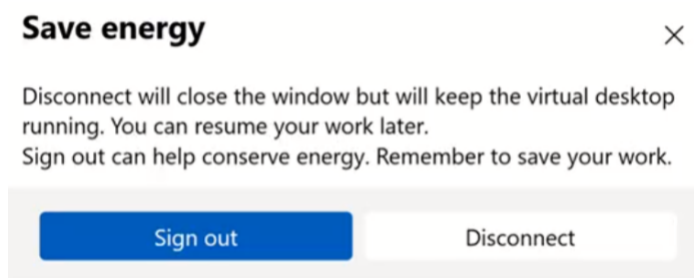
Remarque :

Cette fonctionnalité était auparavant disponible pour les lancements natifs (dans le cloud et locaux) à partir de la version 2309 de l'application Citrix Workspace.

À partir de la version 2402 de l'application Citrix Workspace, cette fonctionnalité est disponible pour les lancements hybrides sur le cloud. Après activation de cette fonctionnalité et lorsqu'un utilisateur ferme un bureau virtuel, une invite apparaît pour que l'utilisateur se déconnecte de la session de bureau. Cette fonctionnalité permet d'économiser de l'énergie si des stratégies du système d'exploitation Windows sont utilisées pour arrêter les machines virtuelles lorsqu'aucun utilisateur n'est connecté.

Pour activer cette fonctionnalité, procédez comme suit :

1. Accédez à Citrix Studio.
2. Cliquez sur **Groupes de mise à disposition** dans le volet de navigation de gauche.
3. Sélectionnez le VDA requis dans la section **Groupe de mise à disposition**.
4. Cliquez sur l'icône **Modifier**. La page **Modifier le groupe de mise à disposition** s'affiche.
5. Cliquez sur **Bureaux** dans le volet de navigation de gauche.
6. Sélectionnez le VDA requis auquel vous devez ajouter les mots clés.
7. Cliquez sur **Modifier**. La page **Modifier le bureau** s'affiche.
8. Définissez le mot clé `ICA-LogOffOnClose` sur **true** dans le champ **Description**.
9. Cliquez sur **OK**. La boîte de dialogue suivante s'affiche lorsque vous fermez le bureau virtuel :



Personnaliser le texte sur l'écran Économiser l'énergie Vous pouvez également personnaliser le texte sur l'écran **Économiser l'énergie**.

1. Suivez les étapes 1 à 8 de la section précédente.
2. Définissez le mot clé `ICA-PromptMessage` avec le texte requis dans le champ **Description**.

Remarque :

Le nombre maximum de caractères autorisés dans le champ Description est de 200.

Exemple :

```
1 KEYWORDS:ICA-LogOffOnClose=true ICA-PromptMessage="Do you want to  
Log off?"  
2 <!--NeedCopy-->
```

Edit Desktop

Display name:

Description:

The name and description are shown in Citrix Workspace app.

Restrict launches to machines with tag:

Allow everyone with access to this delivery group to use a desktop

Restrict desktop use:

Allow list ? ↓
CWAWINAD\Domain Users
TestVeda(CWAWINAD\TestVeda)

Enable desktop
Clear this check box to disable delivery of this desktop.

Session roaming
When enabled, if the user launches this desktop and then moves to another device, the same session is used, and applications are available on both devices. When disabled, the session no longer roams between devices.

Les mots clés sont attribués par défaut aux nouveaux ordinateurs de bureau affectés au groupe. Pour les ordinateurs de bureau existants, exécutez les commandes PowerShell suivantes pour appliquer les modifications :

```
1 $dg = Get-BrokerDesktopGroup -Name '<group name>' -Property 'Name'  
    , 'UId'  
2  
3 $apr = @( Get-BrokerAssignmentPolicyRule -DesktopGroupUId $dg.UId  
    -Property 'Description' )  
4  
5 Get-BrokerMachine -DesktopGroupUId $dg.UId -IsAssigned $true | Set  
    -BrokerMachine -Description $apr[0].Description  
6 <!--NeedCopy-->
```

Avec ce script PowerShell, il est possible d'avoir plusieurs règles de stratégie d'attribution pour un seul groupe de mise à disposition. Avec Citrix Studio, vous pouvez également configurer plusieurs règles de stratégie d'attribution, chacune avec une valeur de description unique et un éventuel ensemble de mots clés différents.

3. Cliquez sur **OK**. La boîte de dialogue suivante s'affiche lorsque vous fermez le bureau virtuel.



Authentification pass-through au domaine amélioré pour l'authentification unique (authentification unique améliorée)

Auparavant, l'application Citrix Workspace pour Windows ne prenait en charge que l'authentification SSON ou l'authentification pass-through au domaine pour l'authentification unique (Single Sign-On) auprès des environnements Citrix Virtual Apps and Desktops à l'aide des informations d'identification utilisateur. Cette authentification permet à l'utilisateur de s'authentifier auprès du domaine sur son appareil et d'utiliser ses applications et bureaux virtuels sans avoir à se réauthentifier.

Cette approche d'authentification pass-through au domaine à l'aide des informations d'identification de l'utilisateur présente les limites suivantes :

- Ne prend pas en charge l'authentification sans mot de passe avec les méthodes d'authentification modernes telles que Windows Hello ou FIDO2. Un composant supplémentaire, le Service d'authentification fédérée ou FAS, est requis pour l'authentification unique (SSO).
- L'installation ou la mise à niveau de l'application Citrix Workspace avec l'authentification SSON activée requiert le redémarrage de l'appareil.
- Requiert l'activation des notifications MPR (Multi Provider Router) sur les machines Windows 11.R

- Doit figurer en haut de la liste des fournisseurs de réseaux.

Remarque :

Cette fonctionnalité n'est pas prise en charge sur Windows 10 32 bits et Windows Server 2016.

Configuration système requise :

- Application Citrix Workspace 2309 ou version ultérieure
- Citrix Virtual Apps and Desktops 2308 ou version ultérieure

Versions du système d'exploitation VDA prises en charge :

- Pour les OS multi-session :
 - Windows Server 2019
 - Windows Server 2022
- Pour les OS mono-session :
 - Windows 10 version 22H2
 - Windows 11 version 22H2

Pré-requis :

- Le client ou le point de terminaison doit être connecté au domaine.
- Requier une visibilité directe sur Active Directory.

Paramètres StoreFront et DDC Configurez un environnement d'authentification pass-through au domaine à l'aide des paramètres suivants :

Remarque :

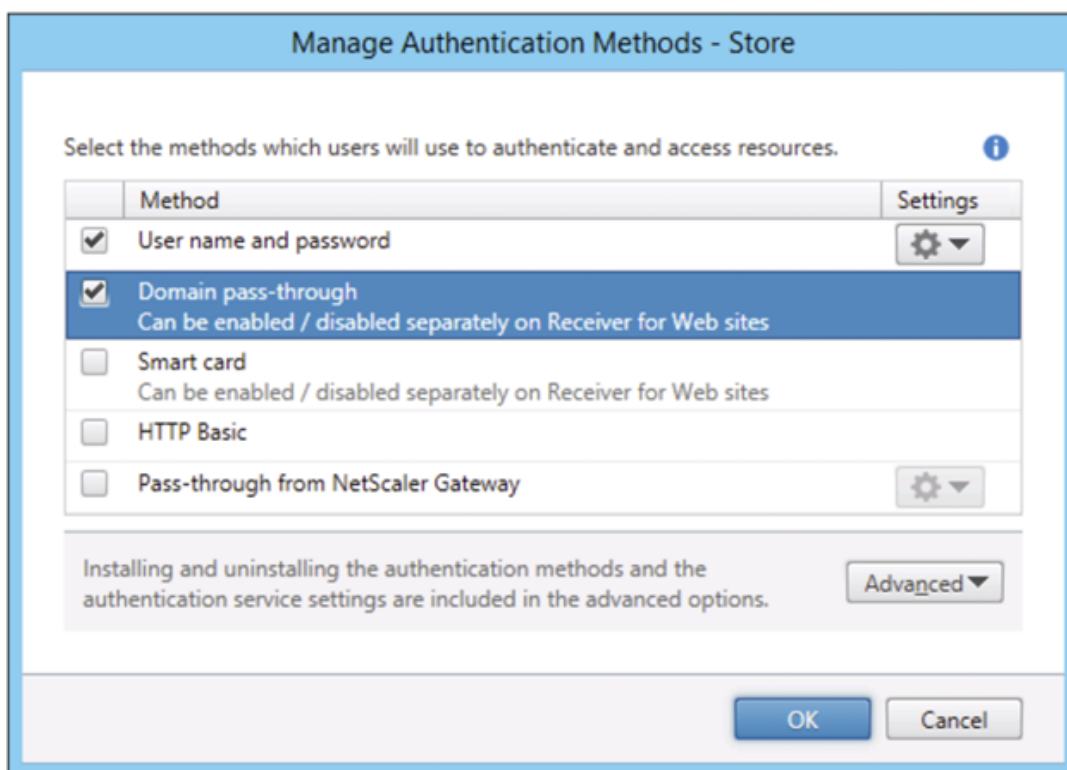
Vous pouvez ignorer cette étape si vous avez déjà configuré l'authentification pass-through au domaine dans votre environnement.

1. Lorsque l'application Citrix Workspace est configurée sur StoreFront :
 - a) Ouvrez **StoreFront Studio**.
 - b) Accédez à **Magasin > Gérer les méthodes d'authentification**.
 - c) Activez **Authentification pass-through au domaine**.

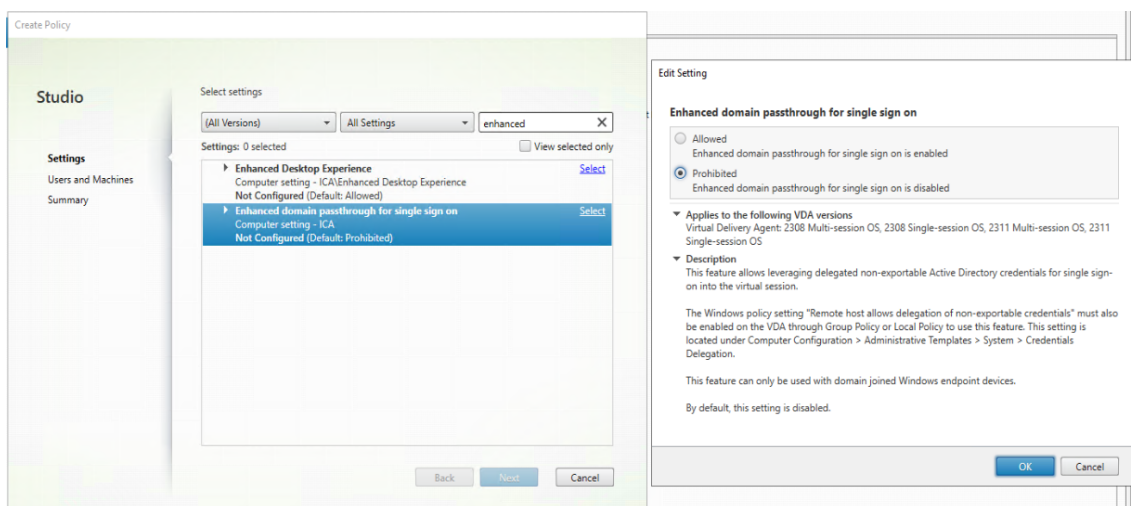
Ou

1. Lorsque vous utilisez l'application Citrix Workspace via le navigateur :
 - a) Ouvrez StoreFront.

- b) Ouvrez **Magasins > Sites Receiver pour Web > Gérer les méthodes d'authentification**.
- c) Activez **Authentification pass-through au domaine**.



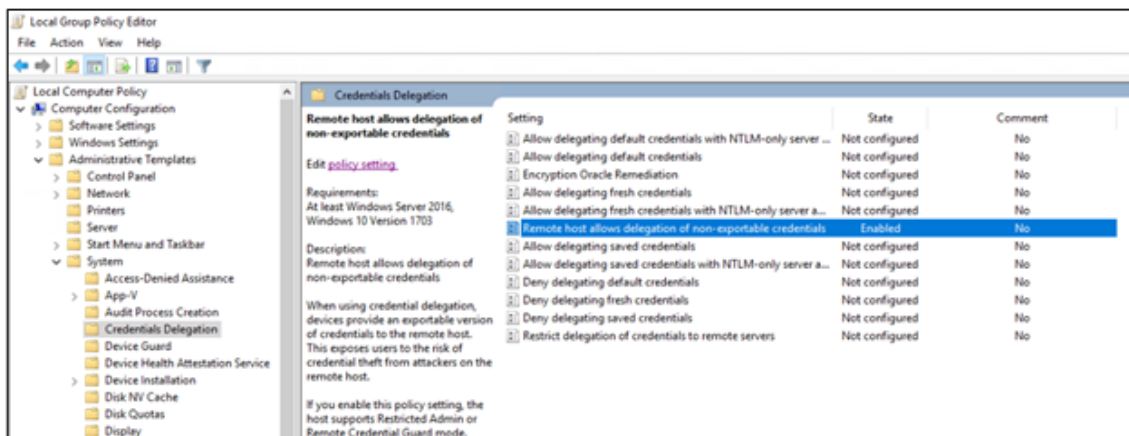
2. Activez la stratégie **Amélioration de l'authentification pass-through au domaine pour l'authentification unique** sur Desktop Delivery Controller.



3. Cliquez sur **OK**.

Paramètres du VDA

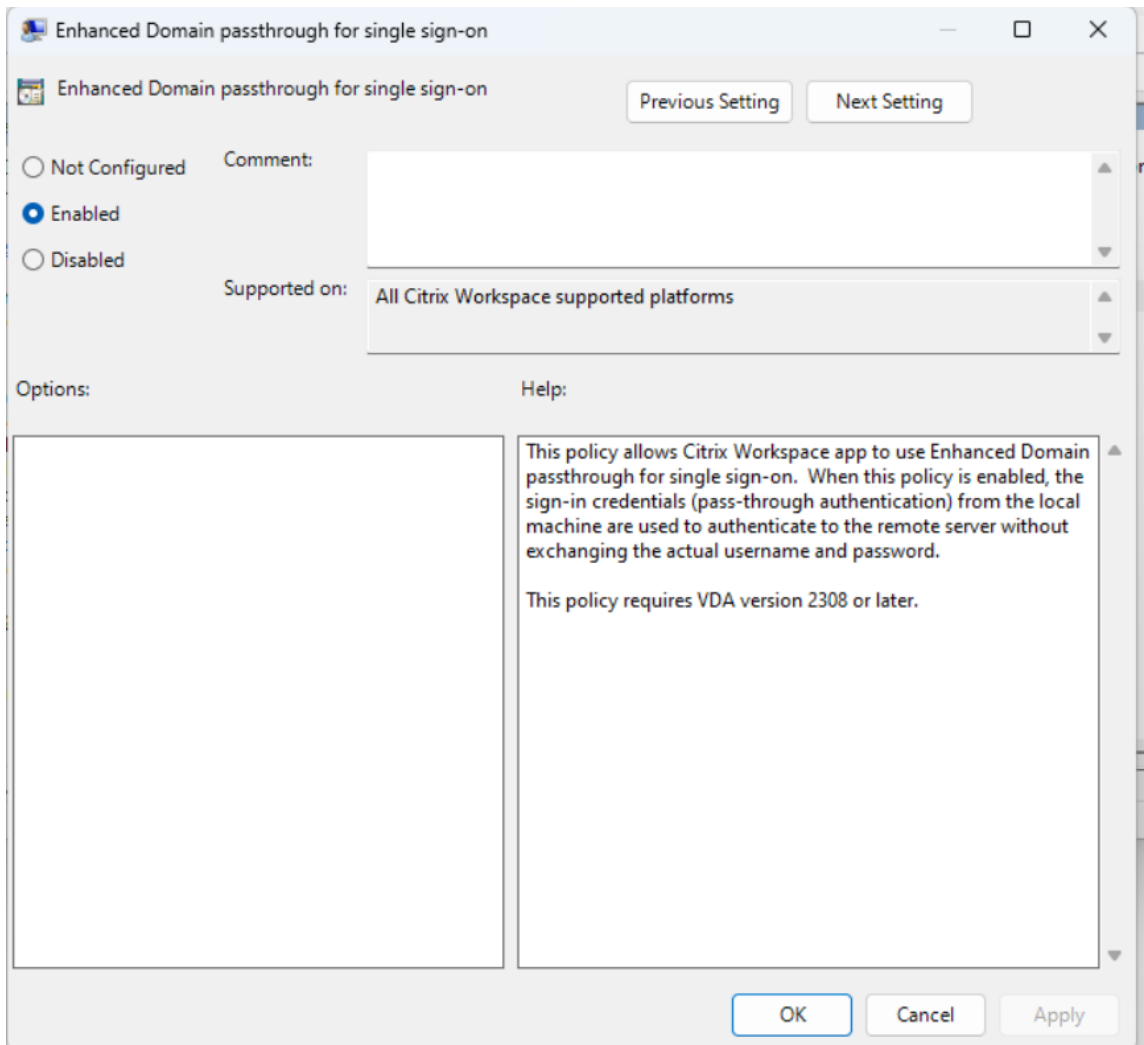
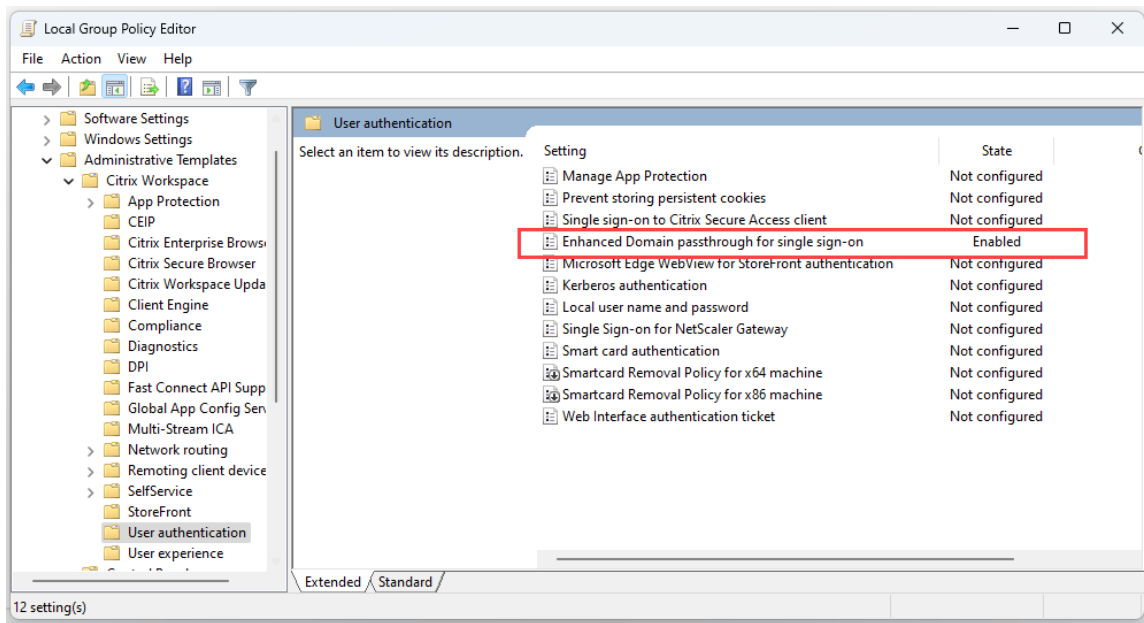
1. Accédez à **Configuration ordinateur\ Modèles d'administration\Systeme\Délégation des informations d'identification** sur le VDA.
2. Activez le paramètre de stratégie Windows **L'hôte distant autorise la délégation des informations d'identification non exportables** sur le VDA.



3. Redémarrez la machine.

Paramètres du client

1. Assurez-vous que la machine cliente est jointe au domaine.
2. Assurez-vous d'utiliser une machine cliente 64 bits.
3. Ouvrez l'**éditeur de stratégie de groupe**.
4. Accédez à **Configuration ordinateur\Modèles d'administration\Composants Citrix\Citrix Workspace\Authentification utilisateur**.
5. Configurez la stratégie de groupe **Amélioration de l'authentification pass-through au domaine pour l'authentification unique**.

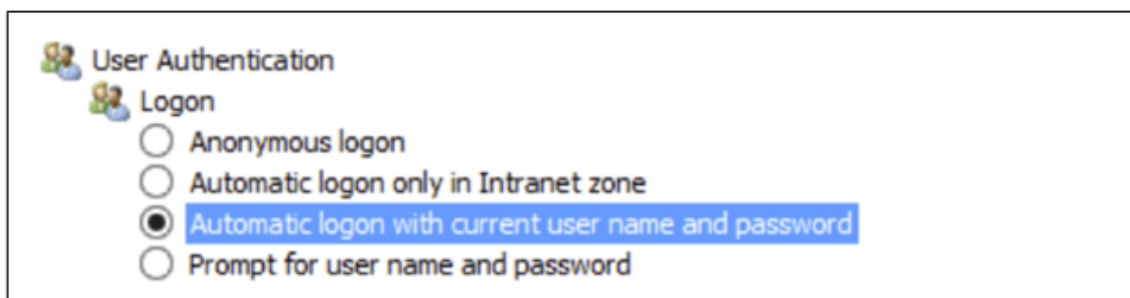


6. Modifiez les paramètres **Options Internet** sur le client.

Remarque :

Vous pouvez ignorer cette étape si vous avez déjà configuré l'authentification pass-through au domaine dans votre environnement.

1. Ajoutez le serveur StoreFront à la liste de sites de confiance à l'aide des **Options Internet**. Pour ajouter :
 - a) Ouvrez **Options Internet** depuis **Panneau de configuration > Réseau et Internet**.
 - b) Cliquez sur **Sécurité > Intranet local**, puis sur **Sites**. La fenêtre **Intranet Local** s'affiche.
 - c) Cliquez sur l'onglet **Avancé**.
 - d) Ajoutez l'adresse URL ou le nom de domaine complet de StoreFront avec les protocoles HTTP ou HTTPS appropriés.
 - e) Cliquez sur **Fermer**, puis sur **OK**.
2. Modifiez les paramètres Authentification utilisateur dans Internet Explorer. Pour modifier :
 - a) Ouvrez **Options Internet** depuis **Panneau de configuration > Réseau et Internet**.
 - b) Cliquez sur l'onglet **Sécurité > Intranet local**.
 - c) Cliquez sur **Personnaliser le niveau**. La fenêtre **Paramètres de sécurité—Zone Intranet local** s'affiche.
 - d) Dans le panneau **Authentification utilisateur**, sélectionnez **Ouverture de session automatique avec le nom d'utilisateur et le mot de passe actuel**.



3. Cliquez sur **OK**.

Prise en charge des stratégies NetScaler avancées pour Storebrowse sous Windows

L'application Citrix Workspace pour Windows prend désormais en charge les stratégies avancées sur NetScaler Gateway avec Storebrowse. Le protocole d'authentification pris en charge est l'authentification LDAP. Storebrowse est un utilitaire de ligne de commande 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 de plus amples informations, consultez la page de [Storebrowse](#).

Remarque :

Le protocole d'authentification nFactor n'est pas pris en charge par Storebrowse sous Windows.

Installer le plug-in VDI Microsoft Teams pour Citrix

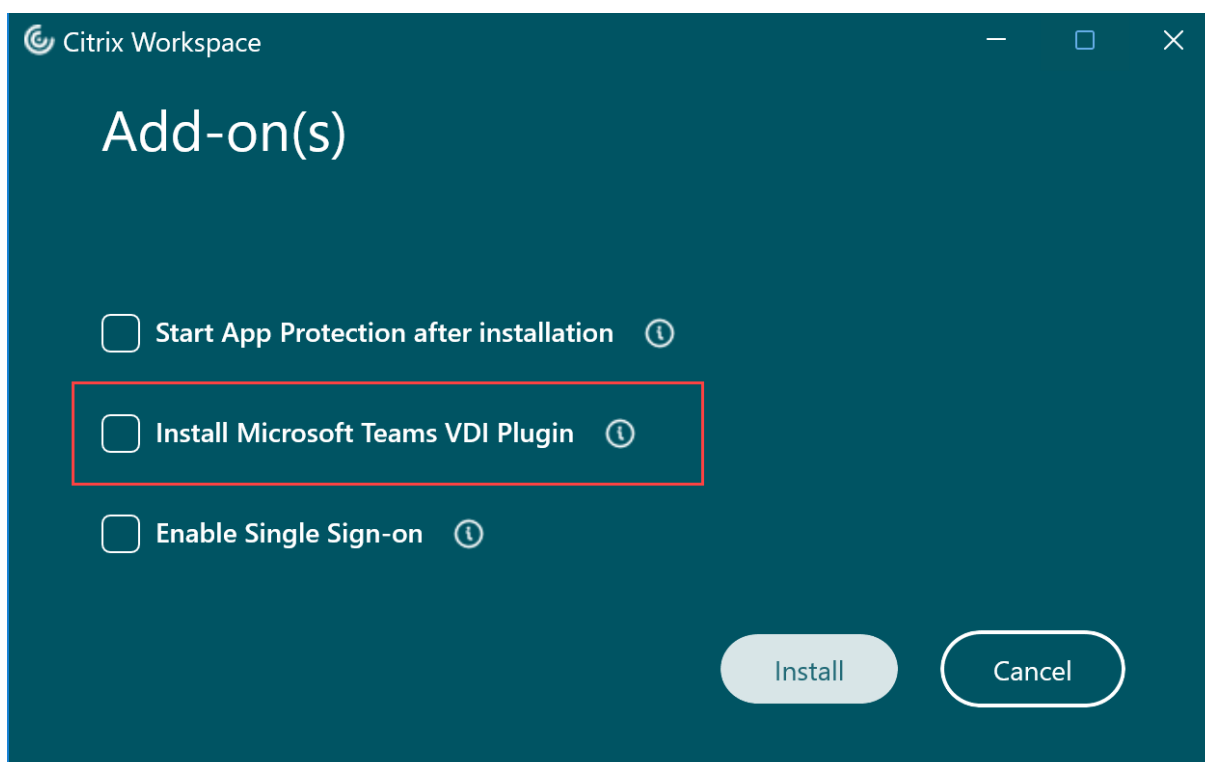
Vous pouvez désormais installer le plug-in VDI Microsoft Teams lors de l'installation de l'application Citrix Workspace à l'aide de l'une des options suivantes.

Remarque :

Pour la compatibilité des versions avec le VDI et les détails de configuration, consultez les exigences relatives à la prise en charge Microsoft Teams 2.1 pour VDI/DaaS et au nouveau plug-in VDI Microsoft Teams.

Utilisation de l'interface utilisateur

1. Sur la page des **modules complémentaires**, cochez la case **Installer le plug-in VDI Microsoft Teams**, puis cliquez sur **Installer**.
2. Acceptez le contrat d'utilisation qui s'affiche et poursuivez l'installation de l'application Citrix Workspace.



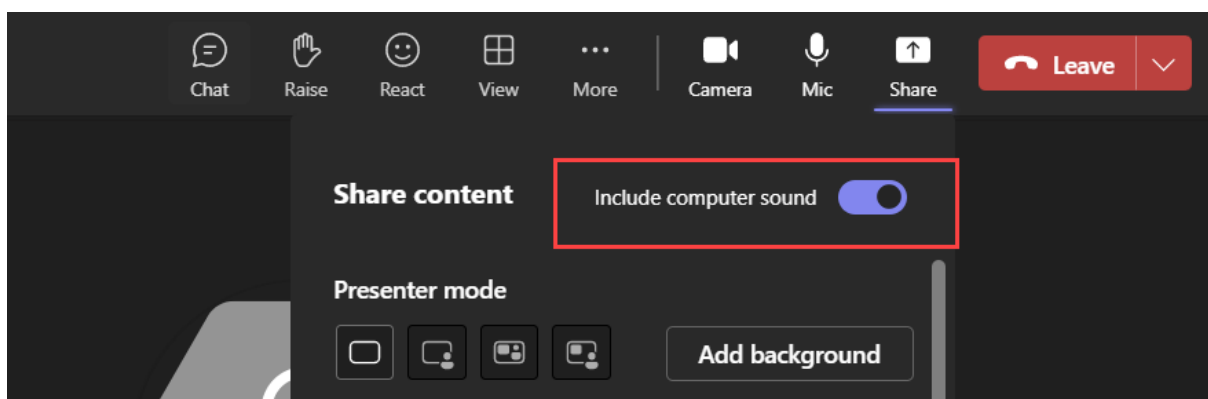
Utilisation de la ligne de commande Utilisez le commutateur de ligne de commande / `installMSTeamsPlugin`.

Par exemple : `CitrixWorkspaceApp.exe /installMSTeamsPlugin`

Partager le son du système [Technical Preview]

Vous pouvez désormais partager le son diffusé sur votre VDA avec les participants à une réunion. Sélectionnez l'option **Inclure le son de l'ordinateur** pour rendre vos réunions plus intéressantes. Vous devez activer cette fonctionnalité via le registre en réglant `HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\EnableSystemAudio` (DWORD) sur 1.

Pour les utilisateurs, cette option n'est pas activée par défaut. Ils doivent l'activer avant de partager leur écran.



Limitations

- Le son ne peut pas être partagé à l'aide de cette fonctionnalité lorsque vous partagez l'écran avec des applications ou des onglets redirigés vers RAVE et BCR.
- L'annulation de l'écho est désactivée si la fonctionnalité Partager le son du système est activée.
- Cette fonctionnalité n'est prise en charge que sur les bureaux publiés.

Remarque :

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

Masquer l'option de dépannage pour les utilisateurs

Les administrateurs peuvent désormais masquer les options de dépannage pour leurs utilisateurs à l'aide de l'éditeur de stratégie de groupe. Une fois ce paramètre activé, l'option de dépannage qui était auparavant visible pour les utilisateurs dans la barre d'état système sera masquée.

1. Dans l'éditeur de stratégie de groupe, accédez à **Modèles d'administration > Composants Citrix > Citrix Workspace > Self Service**.

2. Sélectionnez le dossier **Options de dépannage**.

The screenshot shows the Group Policy Editor interface. The left pane shows the hierarchy: SelfService > Troubleshooting Options. The right pane displays a list of settings with columns for Setting, State, and Comment. The 'Troubleshooting Options' folder is highlighted with a red box.

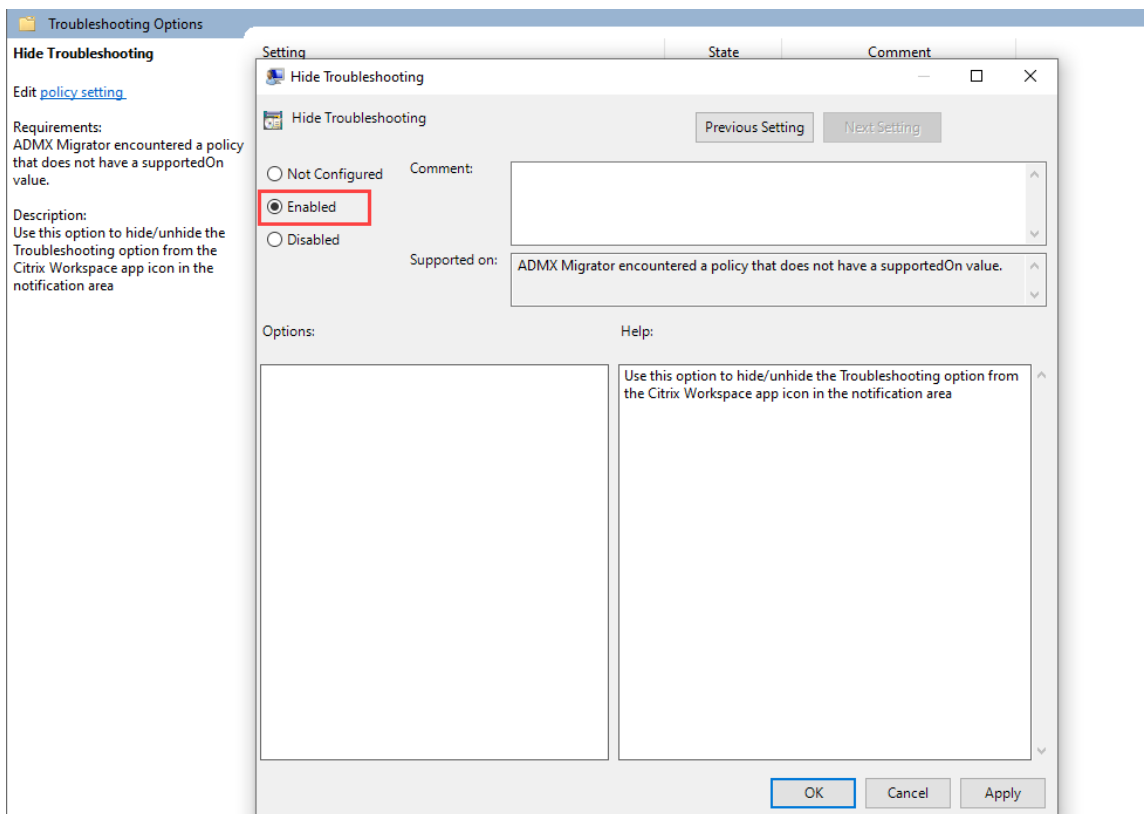
Setting	State	Comment
Advance Preferences Options		
Troubleshooting Options		
Allow users to Add/Remove Account	Not configured	No
Manage App Protection	Not configured	No
Manage App shortcut	Disabled	No
Enable Default FTA	Not configured	No
Enable FTA	Not configured	No
EnableFTU	Not configured	No
Enable application PreLaunch	Not configured	No
Quick Desktop Launch Support	Not configured	No
Silent authentication for Citrix Workspace	Not configured	No
Local app discovery	Not configured	No
Local Application Protection	Not configured	No
Allow/Prevent users to publish safe content	Not configured	No
Allow/Prevent users to publish unsafe content	Not configured	No
Control when Citrix Workspace attempts to reconnect to exi...	Not configured	No
Manage SelfServiceMode	Not configured	No
Store authentication tokens	Not configured	No
vPrefer	Not configured	No

3. Sélectionnez le paramètre **Masquer le dépannage**.

The screenshot shows the Group Policy Editor interface with the 'Troubleshooting Options' folder selected in the left pane. The right pane shows two settings: 'Hide Send Feedback' and 'Hide Troubleshooting'. The 'Hide Troubleshooting' setting is highlighted with a red box.

Setting	State	Comment
Hide Send Feedback	Not configured	No
Hide Troubleshooting	Not configured	No

4. Dans la boîte de dialogue Masquer le dépannage, cochez la case **Activé**. Si vous cochez cette case, l'option de dépannage est masquée pour les utilisateurs.



5. Cliquez sur **OK** pour enregistrer les paramètres.

Mise à niveau de la version pour Chromium Embedded Framework

Chromium Embedded Framework (CEF) est mis à niveau vers la version 120. Cette mise à niveau de version permet de résoudre les failles de sécurité.

App Protection

Liste verte des captures d'écran Si l'application Citrix Workspace, Citrix Virtual Apps and Desktops ou les applications SaaS sont activés avec la stratégie de prévention des captures d'écran App Protection, vous ne pouvez pas capturer leurs écrans à l'aide d'un outil de capture d'écran.

Toutefois, à partir de la version 2402 de l'application Citrix Workspace pour Windows, la fonctionnalité Liste verte des captures d'écran vous permet d'ajouter une application à la liste verte des captures d'écran. Cette fonctionnalité vous permet d'utiliser l'application inscrite sur la liste verte et de capturer l'écran de la ressource activée avec la stratégie de prévention des captures d'écran App Protection. Pour plus d'informations, consultez la section [Liste verte des captures d'écran](#).

Liste d'exclusion des processus Lorsque vous lancez un processus ou une application sur votre appareil, des DLL App Protection sont injectées dans chaque processus si l'App Protection est activée. Parfois, cela peut empêcher le processus ou l'application de fonctionner en raison de problèmes de compatibilité avec la DLL.

À partir de la version 2402 de l'application Citrix Workspace pour Windows, vous pouvez ajouter n'importe quel processus à la liste d'exclusion des processus afin d'éviter l'injection de la DLL App Protection dans ce processus particulier et de résoudre les problèmes de compatibilité causés par la présence de DLL App Protection. Pour plus d'informations, consultez la section [Liste d'exclusion des processus](#).

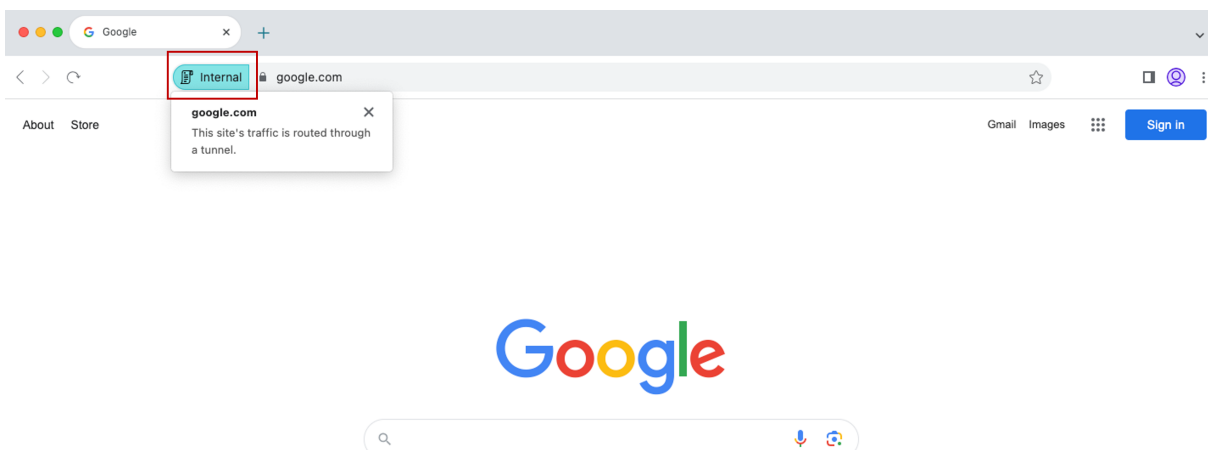
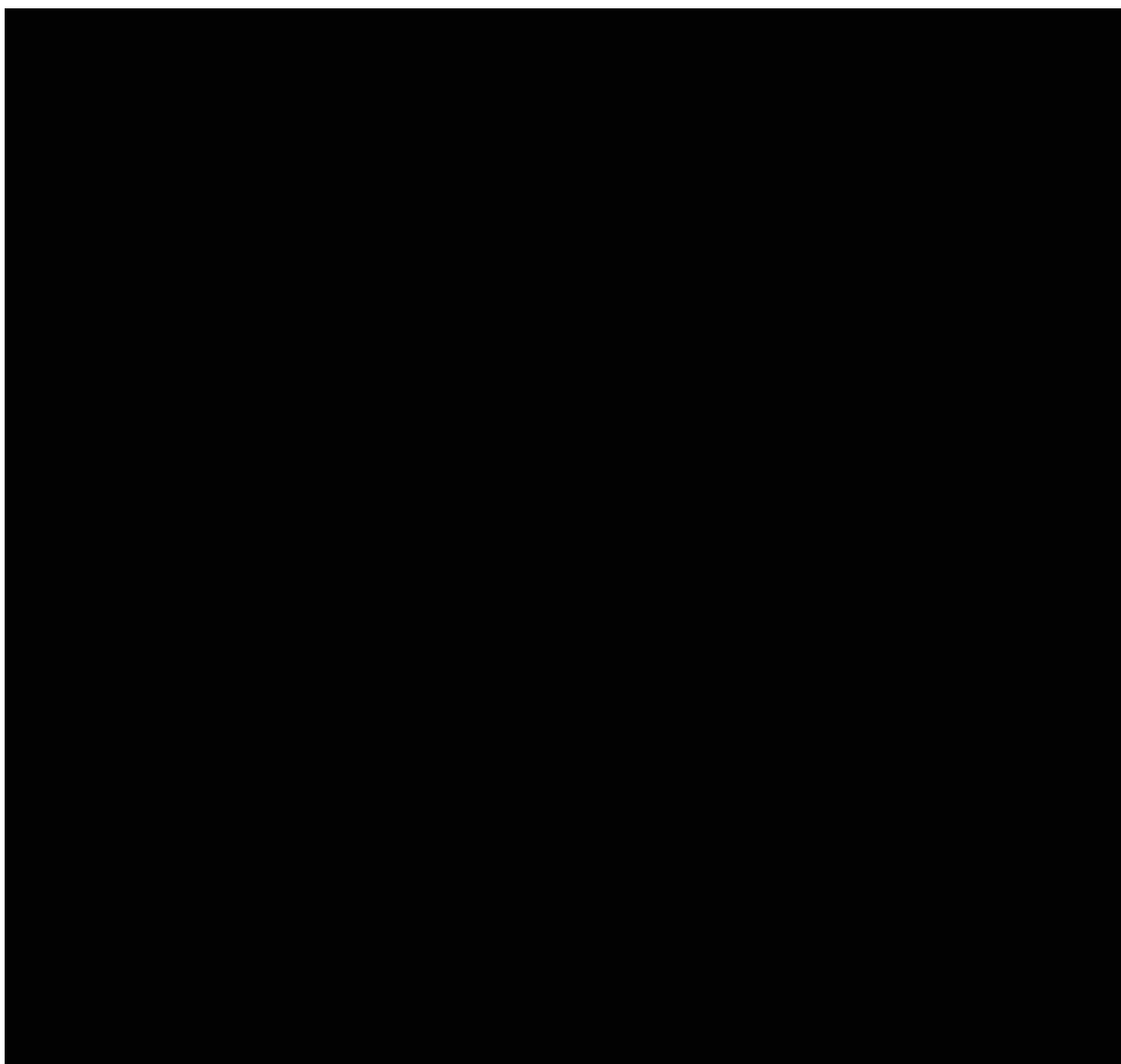
Liste d'exclusion des pilotes de filtre USB Parfois, lorsque vous utilisez des claviers externes spécialisés tels que des claviers de gaming avec l'application Citrix Workspace, le pilote de filtre USB App Protection peut entraîner des problèmes de compatibilité et vous empêcher d'utiliser le clavier.

À partir de la version 2402 de l'application Citrix Workspace pour Windows, la fonctionnalité Liste d'exclusion des pilotes de filtre USB vous permet d'exclure tout périphérique USB présentant des problèmes de compatibilité avec l'application Citrix Workspace à l'aide de l'ID fournisseur et de l'ID produit de l'appareil. Pour plus d'informations, consultez la section [Liste d'exclusion des pilotes de filtre USB](#).

Citrix Enterprise Browser

Cette version de Citrix Enterprise Browser est installée avec l'application Citrix Workspace pour Windows 2402 et repose sur la version 122 de Chromium.

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



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

- Activer le remplissage automatique des adresses - Permet aux administrateurs d'activer ou de désactiver les suggestions de remplissage automatique pour les adresses.
- Activer le remplissage automatique des cartes de crédit - Permet aux administrateurs d'activer ou de désactiver les suggestions de remplissage automatique pour les informations de carte de crédit.
- Protocoles de lancement automatique à partir des origines - Permet aux administrateurs de spécifier une liste de protocoles qui peuvent lancer une application externe à partir des origines répertoriées sans en informer l'utilisateur.
- Activer les avertissements de sécurité des indicateurs de ligne de commande - Permet aux administrateurs d'afficher ou de masquer les avertissements de sécurité, qui apparaissent lorsque des indicateurs de ligne de commande potentiellement dangereux tentent de lancer Enterprise Browser.
- Paramètre de gestion des cookies par défaut - Permet aux administrateurs de gérer les cookies d'un site Web.
- Paramètre de gestion des fenêtres contextuelles par défaut - Permet aux administrateurs de gérer les fenêtres contextuelles d'un site Web.
- Sources d'installation des extensions - Permet aux administrateurs de spécifier des sources valides pour que les utilisateurs puissent installer des extensions, des applications et des thèmes.
- Désactiver les pages d'avertissement similaires - Permet aux administrateurs d'indiquer des domaines préférés dans lesquels les pages d'avertissement similaires ne s'afficheront pas lorsque l'utilisateur en consulteront les pages.
- Activer la requête de mode de paiement - Permet aux administrateurs d'autoriser les sites Web à vérifier si les utilisateurs ont enregistré des modes de paiement.
- Gérer l'enregistrement de l'historique du navigateur - Permet aux administrateurs de gérer l'enregistrement de l'historique de Citrix Enterprise Browser.
- Gérer les suggestions de recherche - Permet aux administrateurs d'activer ou de désactiver les suggestions de recherche dans la barre d'adresses d'Enterprise Browser.
- Activer l'exportation des signets - Permet aux administrateurs d'activer une option permettant d'exporter les signets dans Enterprise Browser.
- Forcer les profils éphémères - Permet aux administrateurs d'effacer ou de conserver les données du profil utilisateur lorsque les utilisateurs ferment Enterprise Browser.

Pour plus d'informations, consultez la page [Gérer Citrix Enterprise Browser via Global App Configuration Service](#) dans la documentation de Citrix Enterprise Browser.

Pour plus d'informations sur les exemples de données JSON, consultez [Exemples de données](#)

JSON.

Citrix Endpoint Analysis

Dans cette version, le client EPA est fourni avec le programme d'installation de l'application Citrix Workspace. Pour installer le client, l'application Citrix Workspace doit être installée à l'aide de l'option de ligne de commande `InstalleEPAclient`.

Exemple : `./CitrixworkspaceApp.exe InstalleEPAclient`

Remarque :

L'analyse de point de terminaison n'est pas installée par défaut.

Dans cette version, la version du package EPA est 23.11.1.20.

Fonctionnalité incluse dans les versions précédentes

Cette version prend en charge les fonctionnalités incluses dans les versions 2204.1 à 2311.1 de l'application Citrix Workspace pour Windows, comme indiqué ci-dessous.

2311.1

Les fonctionnalités suivantes ont été ajoutées dans cette version :

- [Présentation du nouveau programme d'installation de l'application Citrix Workspace](#)
- [Prise en charge du Gestionnaire d'activités sur les magasins cloud](#)
- [Sélection automatique du codec vidéo](#)
- [Mode de tolérance de pertes pour l'audio](#)
- [Synchronisation de plusieurs claviers en début de session](#)
- [Amélioration des performances de la redirection du contenu du navigateur](#)
- [Mise à niveau de la version pour Chromium Embedded Framework](#)
- [Mise à jour importante concernant les noms de fichiers d'App Protection](#)
- [Citrix Enterprise Browser](#)
 - [Amélioration de l'expérience utilisateur et du temps de rechargement des sessions](#)
 - [Amélioration du design des filigranes](#)
 - [Prise en charge de l'extension de navigateur personnalisée](#)
 - [Simplification de la SSO aux applications Web et SaaS grâce à Global App Configuration Service](#)
 - [Gestion de l'authentification directe dans Citrix Enterprise Browser](#)
 - [Amélioration des fonctionnalités de surveillance des activités des utilisateurs finaux](#)

Remarque :

La redirection du contenu du navigateur basée sur Internet Explorer est obsolète à compter de la version 2311.1 de l'application Citrix Workspace pour Windows. Vous pouvez également utiliser la redirection du contenu du navigateur basée sur Google Chrome.

Présentation du nouveau programme d'installation de l'application Citrix Workspace

L'interface utilisateur du programme d'installation de l'application Citrix Workspace a été remaniée pour offrir une apparence moderne et simple, ainsi qu'une meilleure expérience utilisateur. Par défaut, le nouveau programme d'installation est activé.

Pré-requis :

Le nouveau programme d'installation requiert également que .Net Desktop Runtime 6.0.20 ou version ultérieure soit installé au préalable. Pour en savoir plus sur les autres exigences, consultez la section [Configuration requise](#).

Le nouveau programme d'installation est activé par défaut. Pour en savoir plus, consultez la section [Installation basée sur l'interface utilisateur](#).

Remarque :

À partir de la version 2311.1 de l'application Citrix Workspace pour Windows, le `TrolleyExpress` est remplacé par `CWAInstaller-<date and timestamp>`. Par exemple, le journal est enregistré sous `C:\Program Files (x86)\Citrix\Logs\CTXWorkspaceInstallLogs-20231225-093441`.

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

L'application Citrix Workspace pour Mac prend en charge la fonctionnalité Gestionnaire d'activités. Cette fonctionnalité permet aux utilisateurs d'afficher toutes leurs sessions d'application et de bureau actives et d'interagir avec celles-ci en un seul endroit. Pour afficher les sessions actives dans le **Gestionnaire d'activités**, cliquez sur l'icône **Gestionnaire d'activités**. Vous pouvez effectuer les actions suivantes sur une application ou un ordinateur de bureau en cliquant sur le bouton représentant des points de suspension (...) dans le Gestionnaire d'activités :

- **Fermer la session** : ferme la session en cours. Toutes les applications de la session sont fermées et tous les fichiers non enregistrés sont perdus.
- **Déconnecter** : la session à distance est déconnectée, mais les applications et les bureaux sont actifs en arrière-plan.
- **Redémarrer** : arrête le bureau et le redémarre.
- **Arrêter** : ferme les bureaux déconnectés.

- **Arrêt forcé** : force la mise hors tension de votre bureau en cas de problème technique.
- Cliquez sur le bouton **X** pour mettre fin à la session active de l'application depuis le Gestionnaire d'activités.

Pour plus d'informations, consultez [Gestionnaire d'activités](#).

Remarque :

Cette fonctionnalité est disponible dans l'application Citrix Workspace pour Windows uniquement si la [nouvelle expérience Workspace](#) est activée.

Sélection automatique du codec vidéo

Avec cette version, l'application Citrix Workspace pour Windows détecte désormais automatiquement le meilleur codec vidéo à appliquer. Lors de l'installation de l'application Citrix Workspace pour Windows, les capacités de décodage du terminal sont évaluées. Ces informations permettent à l'application Citrix Workspace pour Windows de sélectionner le meilleur codec à utiliser avec le VDA au démarrage de la session. Les codecs vidéo sont évalués dans l'ordre suivant :

1. AV1
2. H.265
3. H.264

Cette fonctionnalité est disponible lorsque la politique d'**utilisation d'un codec vidéo pour la compression** est définie sur l'une des valeurs suivantes :

- **Utiliser au choix**
- **Pour l'écran entier**
- **Pour les zones changeant constamment**

Pour plus d'informations sur la politique d'**utilisation d'un codec vidéo pour la compression**, consultez la section [Utiliser un codec vidéo pour la compression](#).

La sélection automatique s'applique uniquement aux variantes YUV 4:2:0 de ces codecs. Le format YUV 4:2:0 utilisant moins de bande passante, la qualité est réduite. Si le paramètre de la politique **Qualité visuelle** est défini sur **Sans perte si possible** ou **Toujours sans perte** et si la politique **Autoriser l'absence de perte visuelle** est définie sur **Activée**, la sélection automatique du codec vidéo est désactivée et le format YUV 4:4:4 H.264 ou H.265 est utilisé à la place.

Pour plus d'informations sur ces politiques, consultez les sections suivantes :

- [Qualité visuelle](#)
- [Autoriser la compression visuelle sans perte](#)

Cette fonctionnalité est activée par défaut.

Pour plus d'informations, consultez la section [Sélection automatique du codec 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. Le codec vidéo H.265 doit être pris en charge et activé sur le VDA et dans l'application Citrix Workspace.

À partir de l'application Citrix Workspace 2311.1, cette fonctionnalité est automatiquement activée avec l'introduction de la fonctionnalité **Sélection automatique du codec vidéo**.

Pour plus d'informations, consultez la documentation sur le codec vidéo [H.265](#).

AV1 L'application Citrix Workspace prend en charge l'utilisation du codec vidéo AV1 pour l'accélération matérielle des graphiques et vidéos distants. Le codec vidéo AV1 doit être pris en charge et activé sur le VDA et dans l'application Citrix Workspace.

À partir de l'application Citrix Workspace 2311.1, cette fonctionnalité est automatiquement activée avec l'introduction de la fonctionnalité **Sélection automatique du codec vidéo**.

Pour de plus amples informations, consultez la documentation sur le codec vidéo [AV1](#).

Mode de tolérance de pertes pour l'audio

Dans cette version, l'application Citrix Workspace prend en charge le mode de tolérance de pertes (EDT compression avec perte) pour la redirection audio. Cette fonctionnalité améliore l'expérience utilisateur pour le streaming en temps réel lorsque les utilisateurs se connectent via des réseaux à latence élevée et à perte de paquets.

Vous devez utiliser la version 2311 ou ultérieure du VDA. Par défaut, cette fonctionnalité est activée sur l'application Citrix Workspace pour Windows. Par contre, elle est désactivée sur le VDA.

Pour plus d'informations, consultez la documentation sur le [Mode de tolérance de pertes pour l'audio](#).

Synchronisation de plusieurs claviers en début de session

Auparavant, seul le clavier actif du client était synchronisé avec le VDA après le démarrage de la session en mode plein écran. Dans ce scénario, si vous n'avez configuré **Synchroniser une seule fois lorsque la session est lancée** sur votre application Citrix Workspace et que vous avez dû changer de clavier, vous devez installer manuellement le clavier sur votre poste de travail distant. De même, si vous avez configuré **Autoriser la synchronisation dynamique** sur votre application Citrix Workspace, vous devez basculer en mode fenêtré, modifier le clavier de votre client, puis revenir en mode plein écran.

Dans cette version, tous les claviers disponibles sur le client sont synchronisés avec le VDA après le démarrage de la session en mode plein écran. Vous pouvez sélectionner le clavier requis dans la liste des claviers installés ou disponibles sur le client après le démarrage de la session en mode plein écran.

Pour plus d'informations, consultez la documentation [Synchroniser plusieurs claviers au début de la session](#).

Amélioration des performances de la redirection du contenu du navigateur

Auparavant, la redirection du contenu du navigateur utilisait le cache d'espace disque côté client et les informations mises en cache n'étaient pas supprimées lors d'une mise à niveau. Cette configuration s'est traduite par une augmentation de l'utilisation de l'espace disque au fil du temps et un comportement incohérent lors de la redirection d'une page avec la redirection du contenu du navigateur.

Dans cette version, la redirection du contenu du navigateur utilise un cache en mémoire pour résoudre ce problème. Cette amélioration contribue à améliorer les performances de la redirection du contenu du navigateur.

Cette fonction est désactivée par défaut.

Pour plus d'informations, consultez la section [Amélioration des performances de la redirection du contenu du navigateur](#).

Mise à niveau de la version pour Chromium Embedded Framework

Chromium Embedded Framework (CEF) est mis à niveau vers la version 117. Cette mise à niveau de version permet de résoudre les failles de sécurité.

Mise à jour importante concernant les noms de pilotes et de fichiers d'App Protection

À partir de l'application Citrix Workspace pour Windows 2311.1, les noms de fichiers et de pilotes suivants sont mis à jour comme suit :

Nom existant	Nouveau nom
<code>EntryProtect.dll</code>	<code>ctxapdotnet.dll</code>
<code>entryprotect.sys</code>	<code>ctxapdriver.sys</code>
<code>epclient32.dll</code>	<code>ctxapclient32.dll</code>
<code>epclient64.dll</code>	<code>ctxapclient64.dll</code>
<code>epinject.sys</code>	<code>ctxapinject.sys</code>
<code>epusbfilter.sys</code>	<code>ctxapusbfilter.sys</code>
<code>entryprotectdrv</code>	<code>ctxapdriver</code>

Nom existant	Nouveau nom
<code>epinject6</code>	<code>ctxapinject</code>

Ces fichiers sont installés dans `%ProgramFiles(x86)%\Citrix\ICA Client` par défaut.

Si vous avez ajouté l'un des noms de fichier ou de pilote précédents à la liste verte de votre environnement, mettez la liste à jour.

Flou et effets d'arrière-plan pour optimiser Microsoft Teams avec HDX

À partir de la version 2311.1 de l'application Citrix Workspace, vous pouvez sélectionner les options de flou et d'effets d'arrière-plan suivantes :

- Aucun effet d'arrière-plan
- Sélectionner le flou d'arrière-plan
- Sélectionner l'image d'arrière-plan

Citrix Enterprise Browser

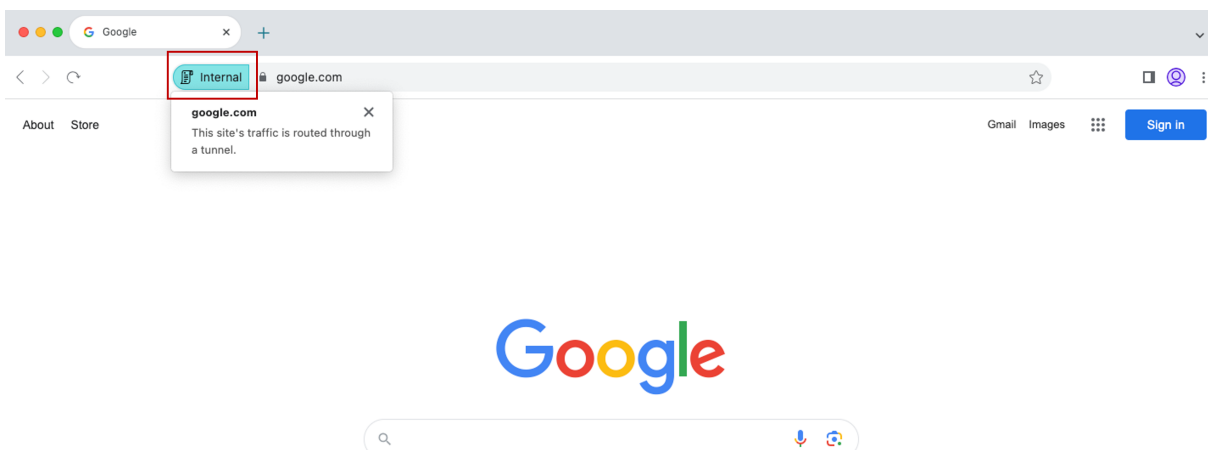
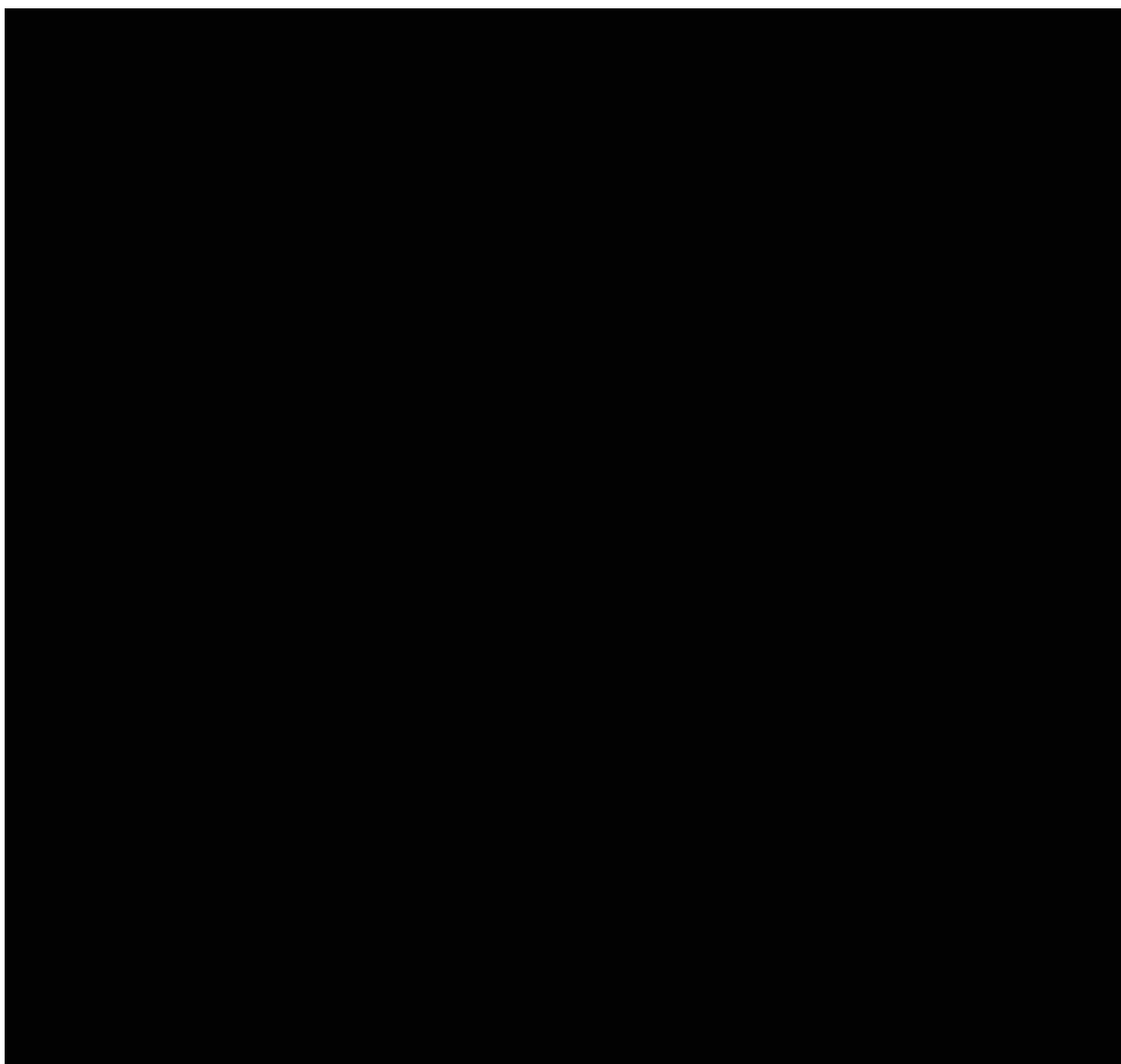
Cette version inclut Citrix Enterprise Browser version 119.1.1.60, basé sur Chromium version 115. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#)

.

Citrix Enterprise Browser introduit des paramètres supplémentaires dans Global App Configuration Service Des paramètres supplémentaires ont été ajoutés à Global App Configuration Service (GACS) pour configurer Citrix Enterprise Browser. Pour plus d'informations, consultez [Gérer Citrix Enterprise Browser via GACS](#).

Indicateur de sécurité lors de la consultation de sites Web

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



Amélioration de l'expérience utilisateur Auparavant, Citrix Enterprise Browser affichait une fenêtre modale de reconnexion lorsque vous tentiez d'effectuer une action après l'expiration de votre session. À partir de la version 2311.1 de l'application Citrix Workspace pour Windows (qui correspond à la version 119.1.1.60 de Chromium), il n'existe plus de fenêtre modale de reconnexion. À la place, une icône de chargement apparaît désormais dans l'onglet du navigateur lorsque vous tentez d'effectuer une action après l'expiration de votre session.

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

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

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

Remarque :

Nous vous recommandons de redémarrer l'application Citrix Workspace lorsque vous modifiez les paramètres de Citrix Enterprise Browser dans GACS. Cependant, vous pouvez également attendre la fin de l'actualisation automatique. Pour plus d'informations sur la durée de synchronisation des stratégies extraites de GACS, reportez-vous à la section [Fréquence de mise à jour des paramètres](#).

Extension de la fonctionnalité d'authentification unique simplifiée à StoreFront La fonctionnalité d'authentification unique (SSO) est désormais disponible pour StoreFront. Elle garantit une

expérience SSO unifiée. Grâce à cette nouvelle fonctionnalité, les utilisateurs n'ont plus besoin de s'authentifier séparément lorsqu'ils accèdent à des applications via StoreFront. Pour simplifier l'utilisation de cette fonctionnalité SSO, utilisez le même fournisseur d'identité (IdP) pour les applications Web et SaaS, ainsi que pour StoreFront. Pour plus d'informations sur la gestion de l'authentification unique via GACS, consultez la section [Gestion de l'authentification unique pour les applications Web et SaaS via Global App Configuration Service](#).

Gestion de l'authentification directe dans Citrix Enterprise Browser L'authentification pass-through (PTA) est une fonctionnalité d'Azure AD Connect. Avec la PTA, les informations d'identification de l'utilisateur sont transmises de la machine cliente au serveur. Vous ne voyez rien, car tout se passe en arrière-plan. Dans cette méthode d'authentification, la machine cliente communique directement avec le serveur d'authentification pour valider les informations d'identification de l'utilisateur. La PTA est généralement utilisée lorsque votre machine cliente et le serveur d'authentification se font mutuellement confiance et que votre machine cliente est considérée comme sécurisée. Pour plus d'informations sur l'authentification directe Microsoft Azure AD, consultez la section [Authentification unique transparente Microsoft Entra](#).

Pour faciliter l'authentification pass-through, l'extension Windows Accounts est requise pour interagir avec les applications nécessitant un accès basé sur Azure AD dans Enterprise Browser. L'administrateur doit configurer cette extension de [comptes Windows](#) dans la liste obligatoire sous **Extension-InstallForcelist**. Pour plus d'informations sur la configuration des extensions obligatoires, consultez la section [Extension obligatoire](#).

Amélioration des fonctionnalités de surveillance des activités des utilisateurs finaux Auparavant, les administrateurs ne pouvaient pas surveiller les activités des utilisateurs finaux, telles que les applications consultées et le type de trafic. À partir de l'application Citrix Workspace pour Windows 2311.1 (correspondant à la version 119.1.1.60 de Chromium), il est désormais également possible de surveiller ces détails.

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

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

2309.1

Nouveautés

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

Citrix Enterprise Browser

Cette version inclut Citrix Enterprise Browser version 117.1.1.13, basé sur Chromium version 117. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

2309

Nouveautés

Remarque :

À partir de cette version, assurez-vous que la version de Microsoft Edge WebView2 Runtime est 117 ou une version ultérieure. Nous vous recommandons d'installer la dernière version pour bénéficier des nouvelles fonctionnalités et des correctifs liés à la sécurité.

Les fonctionnalités suivantes ont été ajoutées dans cette version :

- [Conditions préalables supplémentaires pour .NET](#)
- [Amélioration de l'expérience de lancement de Virtual Apps and Desktops](#)
- [Ajout de l'option Dépannage dans la barre d'état système de l'application Citrix Workspace](#)
 - [Envoi de commentaires sur l'application Citrix Workspace](#)
- [Initiative de développement durable pour l'application Citrix Workspace](#)
- [Configuration de la synchronisation de la disposition du clavier à l'aide de l'interface de ligne de commande](#)
- [Commande pour nettoyer et installer l'application Citrix Workspace](#)
- [App Protection](#)
 - [Mise à jour importante concernant les noms de fichiers](#)
 - [Détection d'altération des stratégies](#)
 - [App Protection avec le scénario double saut \(DoubleHop\)](#)
- [Citrix Enterprise Browser](#)
 - [Authentification via Citrix Enterprise Browser](#)

Conditions préalables supplémentaires pour .NET Outre .NET Framework 4.8, l'application Citrix Workspace requiert la version x86 de .NET Desktop Runtime 6.0 pour les systèmes x86 et x64 dotés de privilèges d'administrateur. Pour plus d'informations, consultez la section [Configuration requise pour .NET](#).

Amélioration de l'expérience de lancement de Virtual Apps and Desktops

Remarque :

À partir de la version 2305.1 de l'application Citrix Workspace, cette fonctionnalité est généralement disponible pour les magasins cloud, et à partir de la version 2309 pour les magasins locaux.

Auparavant, la boîte de dialogue de progression du lancement n'était pas intuitive. Les utilisateurs pensaient que le lancement ne répondait pas et ils fermaient la boîte de dialogue, car les messages de notification restaient affichés.

Avec cette amélioration, l'expérience de lancement d'applications et de bureaux est plus informatif, moderne et convivial sur l'application Citrix Workspace pour Windows. Cette fonctionnalité permet d'améliorer l'engagement auprès des utilisateurs grâce à des informations pertinentes et opportunes sur l'état du lancement.

Pour plus d'informations, consultez [Amélioration de l'expérience de lancement d'applications et de bureaux virtuels](#).

Ajout de l'option Dépannage dans la barre d'état système de l'application Citrix Workspace

L'option **Dépannage** a été ajoutée pour améliorer l'expérience utilisateur et faciliter le dépannage. Vous pouvez cliquer avec le bouton droit sur l'icône de l'application Citrix Workspace dans la barre d'état système située dans le coin inférieur droit de votre écran, puis sélectionner **Dépannage** pour y accéder.

Les options disponibles dans la section Dépannage sont les suivantes :

- Envoyer des commentaires
- Collecter les journaux
- Vérifier la configuration
- Réinitialiser les données d'application
- Aide

Envoi de commentaires sur l'application Citrix Workspace

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

Pour plus d'informations, consultez [Ajout de l'option Dépannage dans la barre d'état système de l'application Citrix Workspace](#).

Initiative de développement durable pour l'application Citrix Workspace Lorsque cette fonctionnalité est activée et qu'un utilisateur ferme un bureau virtuel, une invite apparaît pour que l'utilisateur se déconnecte de la session de bureau. Cette fonctionnalité peut contribuer à économiser de l'énergie si des stratégies du système d'exploitation Windows sont utilisées pour arrêter les machines virtuelles lorsqu'aucun utilisateur n'est connecté.

Pour plus d'informations, consultez [Initiative de développement durable pour l'application Citrix Workspace](#).

Commandes pour configurer la synchronisation de la disposition du clavier à l'aide de l'interface de ligne de commande Auparavant, vous pouviez configurer la synchronisation de la disposition du clavier uniquement à l'aide de l'interface graphique ou en mettant à jour le fichier de configuration. Dans cette version, de nouvelles commandes ont été ajoutées pour configurer la synchronisation de la disposition du clavier à l'aide de l'interface de ligne de commande.

Pour plus d'informations, consultez [Configurer la synchronisation de la disposition du clavier à l'aide de l'interface de ligne de commande](#).

Commande pour nettoyer et installer l'application Citrix Workspace Utilisez la commande `/CleanInstall` pour nettoyer les traces restantes, telles que les fichiers et les valeurs de registre d'une désinstallation précédente, puis installez la nouvelle version de l'application Citrix Workspace.

Par exemple :

```
1 CitrixWorkspaceApp.exe /CleanInstall
2 <!--NeedCopy-->
```

Mises à jour de Microsoft Teams optimisé

Fin de vie prochaine pour l'interface utilisateur à fenêtre unique de Microsoft Teams À partir du 31 janvier 2024, Microsoft ne prendra plus en charge l'interface utilisateur à fenêtre unique de Microsoft Teams lors de l'utilisation de l'optimisation VDI Microsoft Teams et ne prendra en charge que l'expérience en mode multi-fenêtres. Vous devez utiliser une version de Citrix Virtual Apps and Desktops et de l'application Citrix Workspace prenant en charge la fonctionnalité multi-fenêtres pour continuer à utiliser certaines fonctionnalités de Microsoft Teams optimisé. Pour en savoir plus, consultez la section [Fin de vie prochaine pour l'interface utilisateur à fenêtre unique de Microsoft Teams](#).

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

App Protection

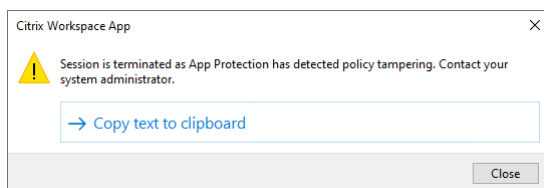
Mise à jour importante concernant les noms de fichiers Dans une prochaine version de l'application Citrix Workspace pour Windows, les noms de fichiers suivants seront mis à jour :

Nom de fichier existant	Nouveau nom de fichier
EntryProtect.dll	ctxapdotnet.dll
entryprotect.sys	ctxapdriver.sys
epclient32.dll	ctxapclient32.dll
epclient64.dll	ctxapclient64.dll
epinject.sys	ctxapinject.sys
epusbfilter.sys	ctxapusbfilter.sys
entryprotectdrv	ctxapdriver
epinject6	ctxapinject

Ces fichiers sont installés dans %ProgramFiles(x86)%\Citrix\ICA Client par défaut.

Si vous avez ajouté l'un des noms de fichiers précédents à la liste des autorisations de votre environnement, mettez à jour la liste.

Détection d'altération des stratégies La fonction de détection d'altération des stratégies empêche l'utilisateur d'accéder à la session d'application ou de bureau virtuel si les stratégies de prévention de capture d'écran et de protection contre l'enregistrement de frappe du composant App Protection sont altérées. Si une altération des stratégies est détectée, la session d'application ou de bureau virtuel sera interrompue en affichant le message d'erreur suivant :



Remarque :

Cette fonctionnalité ne sera disponible qu'après la publication de la prochaine version de Citrix Virtual Apps and Desktops.

Pour plus d'informations sur la fonctionnalité de détection d'altération des stratégies, consultez la section [Détection d'altération des stratégies](#).

Fonctionnalité complète de partage de bureau depuis le VDA avec l'application Citrix Workspace Auparavant, lorsque la App Protection était activée, le partage de bureau était désactivé pour Microsoft Teams optimisé, car la App Protection n'autorise pas la capture d'écran.

À partir de la version 2309 de l'application Citrix Workspace pour Windows, le partage de bureau est activé pour Optimized Microsoft Teams, même si l'App Protection est activée.

Pour plus d'informations, consultez la section [Compatibilité avec l'optimisation HDX pour Microsoft Teams](#).

App Protection avec le scénario double saut (DoubleHop) Les fonctionnalités App Protection ne sont pas prises en charge dans un scénario double saut (DoubleHop). Le double saut (ou « Double-Hop ») désigne une session Citrix Virtual Apps ou Virtual Desktops exécutée dans le cadre d'une session Citrix Virtual Desktops. Auparavant, vous étiez autorisé à lancer des applications et des bureaux virtuels dotés de stratégies de protection des applications dans un scénario à double saut. Cependant, les fonctionnalités App Protection n'étaient pas appliquées.

À présent, une stratégie de groupe Windows a été ajoutée et vous permet de bloquer l'ouverture d'applications et de bureaux virtuels dotés de stratégies de protection des applications dans un scénario à double saut. Pour en savoir plus sur l'activation du paramètre **Bloquer le lancement de DoubleHop**, consultez la section [Activer le paramètre Bloquer le lancement de DoubleHop](#).

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 117.1.1.9, basé sur Chromium version 117. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

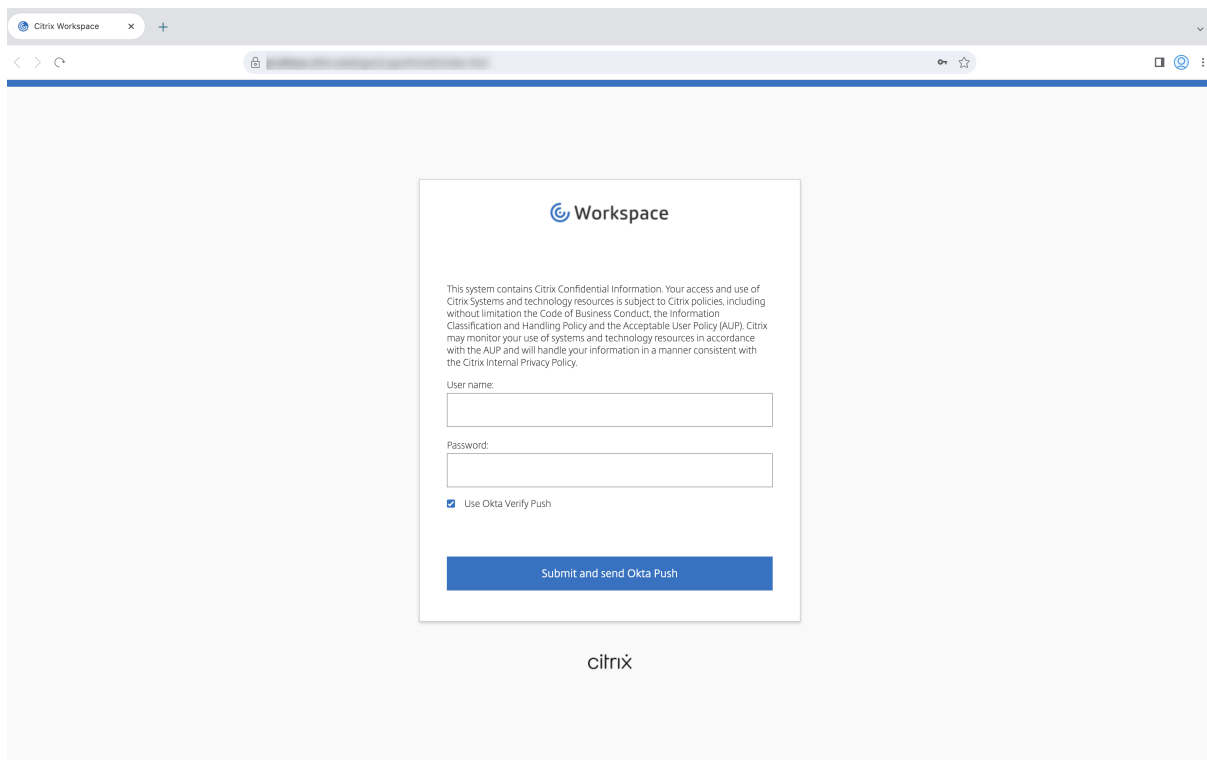
Authentification via Citrix Enterprise Browser Auparavant, si le jeton d'authentification de l'application Citrix Workspace expirait, vous ne pouviez pas utiliser Enterprise Browser. Vous deviez passer à l'application Citrix Workspace et vous réauthentifier pour continuer à utiliser Enterprise Browser.

À partir de la version 2309 de l'application Citrix Workspace pour Windows (qui correspond à la version 117.1.1.9 de Chromium), vous ne pouvez vous authentifier dans Enterprise Browser que lorsque

le magasin reste le même. Cela garantit également l'authentification auprès de l'application Citrix Workspace. De plus, cette fonctionnalité offre une expérience de connexion fluide.

Remarque :

- Cette fonctionnalité s'applique aux magasins Workspace.



2307.1

Nouveautés

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

2307

Nouveautés

Ajout de la prise en charge de tonalités courtes dans Microsoft Teams optimisé Auparavant, lorsque la fonction de sonnerie secondaire était activée, les tonalités courtes, telles que les bips ou les notifications, étaient émises à plusieurs reprises. Par exemple, la tonalité émise lorsqu'un invité rejoignait la réunion Microsoft Teams était répétée. La seule solution était de quitter et de redémarrer Microsoft Teams. Ce problème entraînait une expérience utilisateur médiocre.

Dans cette version, l'application Citrix Workspace prend en charge la lecture des tonalités courtes selon vos besoins. Cette prise en charge active également la fonction de sonnerie secondaire.

Pré-requis :

Effectuez une mise à jour vers la dernière version de Microsoft Teams.

Remarque :

La fonctionnalité précédente n'est disponible qu'après le déploiement d'une mise à jour correspondante de Microsoft Teams. Consultez la mise à jour de la documentation et l'annonce dans [CTX253754](#).

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 112.1.1.24, basé sur Chromium version 112. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

Raccourci Citrix Enterprise Browser À partir de l'application Citrix Workspace pour Windows 2307, un administrateur peut configurer et contrôler la présence du raccourci Citrix Enterprise Browser dans le menu **Démarrer**.

Remarque :

Par défaut, ce paramètre est activé pour les magasins Workspace.

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

- Objet de stratégie de groupe (GPO)
- Global App Configuration Service (GACS)
- web.config.file.

Remarques :

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

- set the **CEBShortcutEnabled** attribute to **false** in the `web.config` file.
- disable the **Enable Citrix Enterprise Browser shortcut** property in GPO and GACS.

Utilisation de l'objet de stratégie de groupe

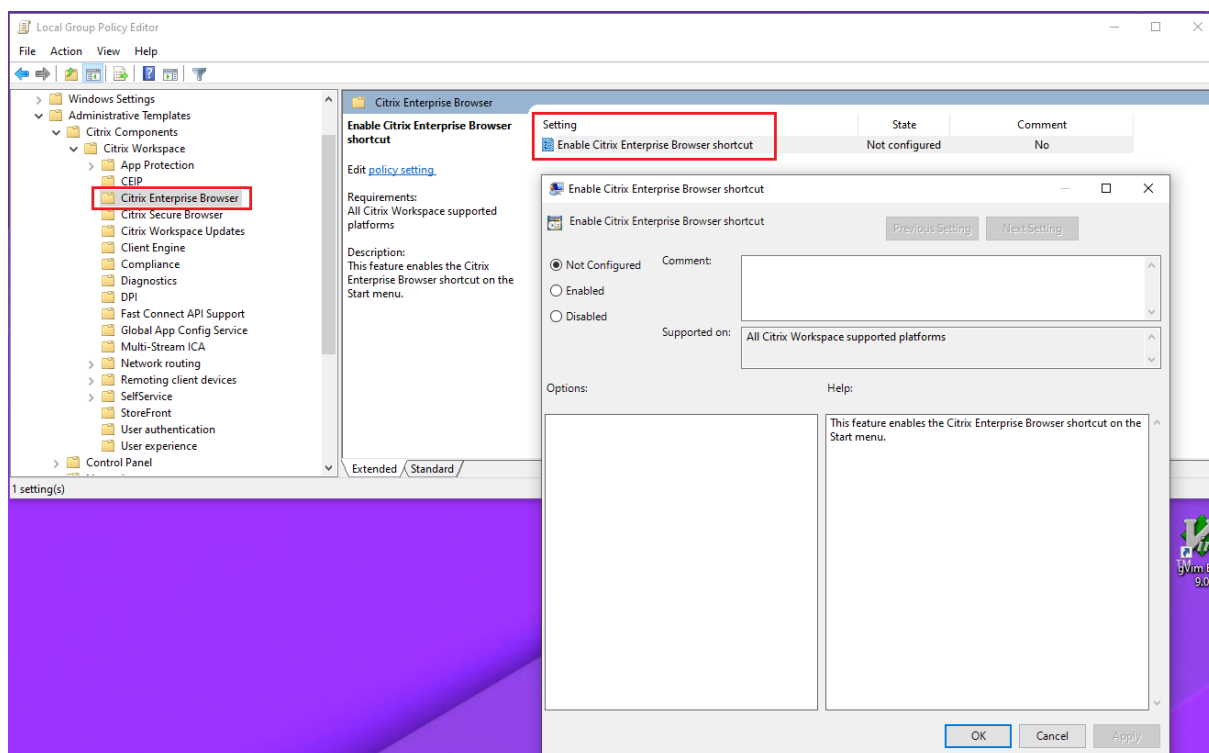
Les administrateurs peuvent utiliser la propriété **Activer le raccourci Citrix Enterprise Browser** pour contrôler l'affichage du raccourci Citrix Enterprise Browser dans le menu Démarrer.

Remarque :

La configuration via GPO est applicable sur Workspace et StoreFront.

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

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 > Citrix Enterprise Browser**.
3. Sélectionnez l'option de raccourci **Activer Citrix Enterprise Browser**.



Pour plus d'informations sur l'utilisation de l'objet de stratégie de groupe, consultez la page [Modèle d'administration d'objet de stratégie de groupe](#).

Global App Configuration Service (GACS)

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

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

Remarque :

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

Fichier web.config :

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

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

Remarque :

La configuration via `web.config` est applicable sur StoreFront.

Utilisation du fichier web.config :

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

1. Utilisez un éditeur de texte pour ouvrir le fichier `web.config`, qui se trouve généralement dans `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Recherchez l'élément de compte d'utilisateur dans le fichier (Store est le nom du compte de votre déploiement)
Par exemple: `<account id=... name="Store">`
3. Avant la balise `</account>`, accédez aux propriétés de ce compte utilisateur et ajoutez ce qui suit :

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

Voici un exemple de fichier `web.config` :

```
1 <account>
2
3     <clear />
4
5     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
        F84Store"
```

```
6
7     description="" published="true" updaterType="Citrix"
8         remoteAccessType="None">
9     <annotatedServices>
10    <clear />
11    <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
12        <metadata>
13            <plugins>
14                <clear />
15            </plugins>
16            <trustSettings>
17                <clear />
18            </trustSettings>
19            <properties>
20                <property name="CEBShortcutEnabled" value="True
21                    " />
22            </properties>
23        </metadata>
24    </annotatedServiceRecord>
25 </annotatedServices>
26 <metadata>
27     <plugins>
28         <clear />
29     </plugins>
30     <trustSettings>
31         <clear />
32     </trustSettings>
33     <properties>
34         <clear />
35     </properties>
36 </metadata>
37 </account>
38 <!--NeedCopy-->
```

2305.1

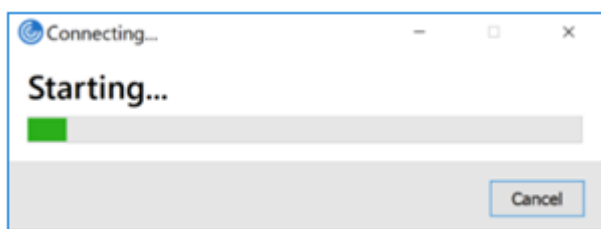
Nouveautés

Amélioration de l'expérience de lancement de Virtual Apps and Desktops

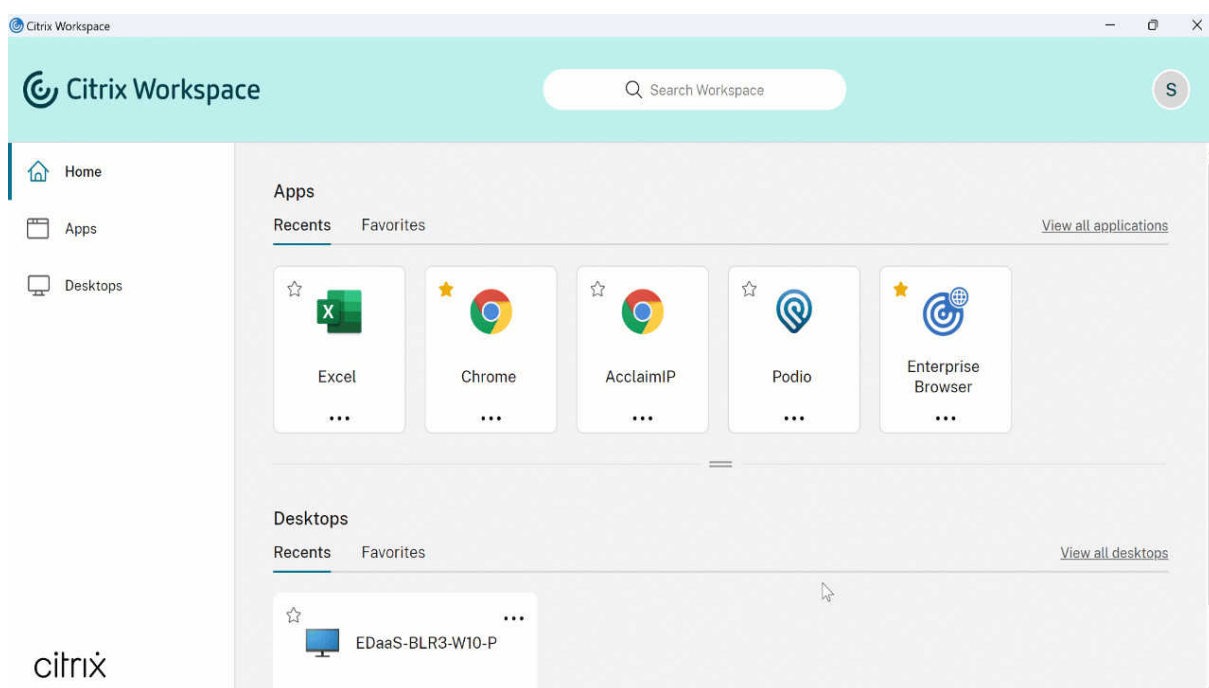
Remarque :

Cette fonctionnalité est en disponibilité générale pour les magasins cloud et disponible en version Technical Preview pour les magasins locaux.

Auparavant, la boîte de dialogue de progression du lancement n'était pas intuitive. Les utilisateurs pensaient que le lancement ne répondait pas et ils fermaient la boîte de dialogue, car les messages de notification restaient affichés.



Avec cette amélioration, l'expérience de lancement d'applications et de bureaux est plus informatif, moderne et convivial sur l'application Citrix Workspace pour Windows. Cette fonctionnalité permet d'améliorer l'engagement auprès des utilisateurs grâce à des informations pertinentes et opportunes sur l'état du lancement. La notification apparaît dans le coin inférieur droit de l'écran.



Au lieu d'une icône de chargement, les utilisateurs peuvent consulter des notifications pertinentes concernant la progression du lancement. Si un lancement est en cours et que l'utilisateur tente de fermer le navigateur, un message d'avertissement s'affiche.

À partir de l'application Citrix Workspace pour Windows 2305.1, cette fonctionnalité est activée par défaut dans les sessions cloud.

Vous pouvez activer cette fonctionnalité à l'aide de la clé de registre de la session StoreFront (locale). Pour plus d'informations, consultez [Amélioration de l'expérience de lancement d'applications et de bureaux virtuels](#).

Suivi de l'état de la commande Storebrowse Vous pouvez suivre l'état d'exécution d'une commande Storebrowse dans un fichier. Pour suivre l'état de réussite, saisissez un nom de fichier unique

avec la commande `-f launch`. Cette commande génère un fichier portant le nom que vous avez indiqué. L'état d'échec est présent dans le fichier `ica.error` qui est créé automatiquement.

Remarque :

Assurez-vous d'ajouter une extension `.ica` au nom du fichier à l'aide de la commande `-f launch`. Dans le cas contraire, le fichier n'est pas généré.

Les fichiers permettant de suivre à la fois les réussites et les échecs sont disponibles dans `%LOCALAPPDATA%\citrix\selfservice\cache` ; vous pouvez ainsi les surveiller selon vos besoins.

Cette amélioration est activée par défaut.

Voici un exemple d'utilisation de la commande de lancement avec l'option `-f` :

```
1 -launch -f <uniqueFileName.ica> "launchcommandline"
2 For example:
3 SelfService.exe storebrowse -launch -f uniqueFileName.ica -s store0-5
   c3ec017 -CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-
   e33d0695df39.Notepad -ica "https://cwawiniwstest.cloudburrito.com/
   Citrix/Store/resources/v2/
   YTLh0GUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkJm5Lk5vdGVwYWQ-/launch/
   ica" -cmdline
4
5 <!--NeedCopy-->
```

Prise en charge des méthodes d'authentification modernes pour les magasins StoreFront L'application Citrix Workspace 2305.1 pour Windows prend en charge les méthodes d'authentification modernes pour les magasins StoreFront. Vous pouvez vous authentifier auprès des magasins Citrix StoreFront de l'une des manières suivantes :

- Utilisation des clés de sécurité Windows Hello et FIDO2. Pour plus d'informations, consultez la section [Autres méthodes d'authentification](#).
- Authentification unique auprès des magasins Citrix StoreFront à partir de machines Azure Active Directory (AAD) jointes avec AAD en tant que fournisseur d'identité. Pour plus d'informations, consultez la section [Autres méthodes d'authentification](#).
- Les administrateurs Workspace peuvent configurer et appliquer les stratégies d'accès conditionnel Azure Active Directory pour les utilisateurs qui s'authentifient sur les magasins Citrix StoreFront. Pour plus d'informations, consultez la section [Prise en charge de l'accès conditionnel avec Azure AD](#).

Pour activer cette fonctionnalité, vous devez utiliser Microsoft Edge WebView2 comme navigateur sous-jacent pour l'authentification directe de StoreFront et de la passerelle.

Remarque :

Assurez-vous que la version de Microsoft Edge WebView2 Runtime est 102 ou ultérieure.

Vous pouvez activer des méthodes d'authentification modernes pour les magasins StoreFront à l'aide de Global App Config Service et du modèle d'objet de stratégie de groupe (GPO). Pour plus d'informations, consultez la section [Prise en charge des méthodes d'authentification modernes pour les magasins StoreFront](#).

Prise en charge de plus de 200 groupes dans Azure AD Avec cette version, un utilisateur d'Azure AD faisant partie de plus de 200 groupes peut voir les applications et les bureaux qui lui sont attribués. Auparavant, le même utilisateur ne pouvait pas voir ces applications et ces bureaux.

Remarque :

Les utilisateurs doivent se déconnecter de l'application Citrix Workspace et se reconnecter pour activer cette fonctionnalité.

App Protection

Amélioration de la protection contre l'enregistrement de frappe Grâce à cette amélioration, la protection contre l'enregistrement de frappe est activée sur les écrans d'authentification et du Self-Service Plug-in (SSP) si l'un des critères suivants est rempli :

- Vous avez activé la App Protection à l'aide de l'une des méthodes suivantes :
 - En sélectionnant la case **Démarrer la App Protection** lors de l'installation.
 - Démarrez le composant App Protection à l'aide du paramètre de ligne de commande `startappprotection`.
- Si vous n'avez pas sélectionné la case **Démarrer App Protection** ou si vous n'avez pas utilisé le paramètre de ligne de commande `startappprotection` lors de l'installation, la protection contre l'enregistrement de frappe est activée après le lancement de la première ressource protégée.

Remarque :

Les paramètres Global App Configuration Service (GACS) et des objets de stratégie de groupe (GPO) remplacent le comportement précédent. Par exemple, si vous avez désactivé la stratégie GACS ou GPO pour ces écrans, la protection contre l'enregistrement de frappe n'est pas activée sur les écrans d'authentification et du SSP.

Mise à jour importante concernant les noms de fichiers Dans une prochaine version de l'application Citrix Workspace pour Windows, les noms de fichiers suivants seront mis à jour :

- EntryProtect.dll
- entryprotect.sys
- epclient32.dll
- epclient64.dll
- epinject.sys
- epusbfilter.sys
- entryprotectdrv
- epinject6

Ces fichiers sont installés sous %ProgramFiles(x86)%\Citrix\ICA Client\.

Si vous avez ajouté l'un de ces noms de fichiers à la liste d'autorisation de votre environnement, mettez à jour la liste d'autorisation lorsque les nouveaux noms de fichiers sont annoncés.

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 105.1.1.27, basé sur Chromium version 105. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

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

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

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

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

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

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

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

Remarques :

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

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

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

Interface utilisateur

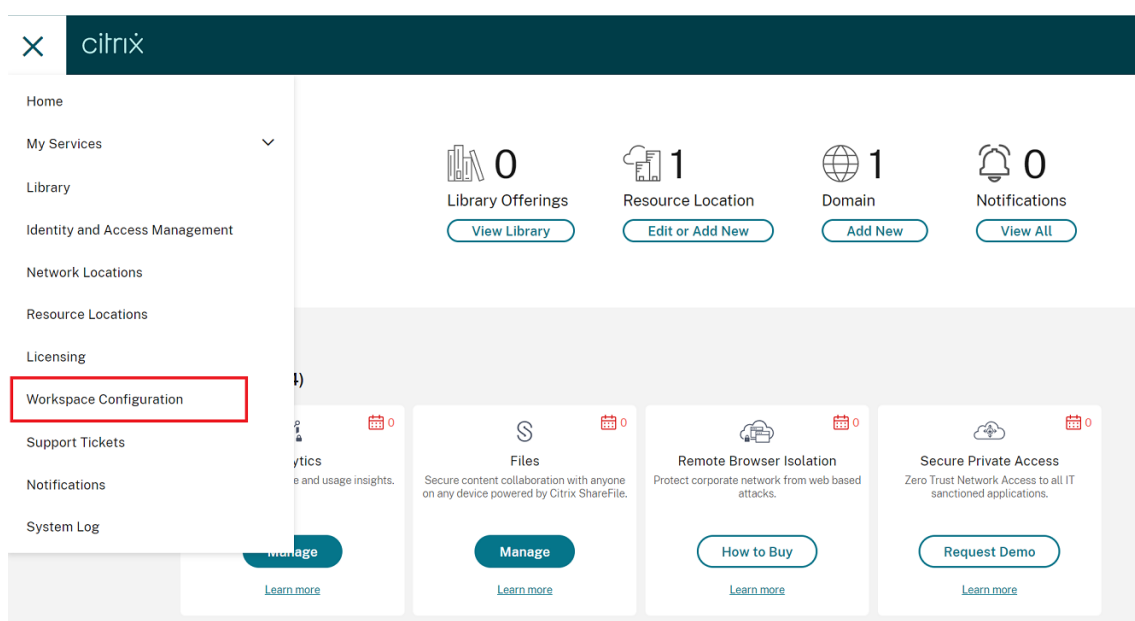
Pour configurer Citrix Enterprise Browser via l'interface utilisateur d'administration GACS, procédez comme suit :

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

Remarque :

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

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



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

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

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

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

2303

Nouveautés

Configurer le chemin du stockage des données temporaires du navigateur pour la superposition de redirection du contenu du navigateur À partir de la version 2303 de l'application Citrix Workspace, vous êtes invité à configurer le chemin du stockage des données temporaires pour un navigateur basé sur Chromium Embedded Framework (CEF).

Pour plus d'informations, consultez la section [Configurer le chemin du stockage des données temporaires du navigateur pour la superposition de redirection du contenu du navigateur](#).

Prise en charge des méthodes d'authentification modernes pour les magasins StoreFront L'application Citrix Workspace 2303 pour Windows prend en charge les méthodes d'authentification modernes pour les magasins StoreFront. Vous pouvez vous authentifier auprès des magasins Citrix StoreFront de l'une des manières suivantes :

- Utilisation des clés de sécurité Windows Hello et FIDO2. Pour plus d'informations, consultez la section [Autres méthodes d'authentification](#).
- Authentification unique auprès des magasins Citrix StoreFront à partir de machines Azure Active Directory (AAD) jointes avec AAD en tant que fournisseur d'identité. Pour plus d'informations, consultez la section [Autres méthodes d'authentification](#).
- Les administrateurs Workspace peuvent configurer et appliquer les stratégies d'accès conditionnel Azure Active Directory pour les utilisateurs qui s'authentifient sur les magasins Citrix StoreFront. Pour plus d'informations, consultez la section [Prise en charge de l'accès conditionnel avec Azure AD](#).

Pour activer cette fonctionnalité, vous devez utiliser Microsoft Edge WebView2 comme navigateur sous-jacent pour l'authentification directe de StoreFront et de la passerelle.

Remarque :

Assurez-vous que la version de Microsoft Edge WebView2 Runtime est 102 ou ultérieure.

Vous pouvez activer des méthodes d'authentification modernes pour les magasins StoreFront à l'aide du modèle de GPO. Pour plus d'informations, consultez la section [Prise en charge des méthodes d'authentification modernes pour les magasins StoreFront](#).

Expérience améliorée pour des visioconférences dans Microsoft Teams optimisé À compter de cette version, la prise en charge de la diffusion simultanée est activée par défaut pour des visioconférences dans Microsoft Teams optimisé. La qualité et l'expérience des visioconférences sur différents

terminaux sont améliorées en s'adaptant à la résolution appropriée pour offrir la meilleure expérience d'appel à tous les appelants.

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

Remarque :

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

Amélioration de la protection des applications : injection anti-DLL Dans le cadre de la protection des applications, nous avons apporté une amélioration de la sécurité qui permet de protéger l'application Citrix Workspace contre certaines bibliothèques DLL non autorisées ou certains modules non fiables. Si de tels modules non fiables sont injectés, l'application Citrix Workspace détecte ces interventions et arrête le chargement des modules.

La protection contre les injections de DLL peut être activée pour les composants suivants :

- Citrix Auth Manager
- Interface utilisateur de l'application Citrix Workspace
- Citrix Virtual Apps and Desktops

Pour plus d'informations, consultez la documentation [App Protection](#).

Clause d'exclusion de responsabilité :

cette fonctionnalité opère en filtrant l'accès aux fonctions requises du système d'exploitation sous-jacent (appels d'API spécifiques requis pour charger les DLL). Cela signifie qu'elle peut fournir une protection même contre certains outils de piratage personnalisés et spécifiques. Cependant, à mesure que les systèmes d'exploitation évoluent, de nouvelles méthodes de chargement des DLL peuvent apparaître. 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.

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 109.1.1.29, basé sur Chromium version 109. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

Prise en charge de Secure Private Access pour StoreFront En tant qu'administrateur, vous pouvez désormais configurer des applications Web et SaaS dans StoreFront à l'aide d'une solution Secure Private Access. Une fois que l'administrateur a configuré l'application, les utilisateurs finaux peuvent ouvrir les applications Web et SaaS à l'aide de Citrix Enterprise Browser et bénéficier d'une sécurité renforcée.

Pour plus d'informations, consultez la section [Déploiement local de Citrix Enterprise Browser](#) dans la documentation de Citrix Secure Private Access.

2302

Nouveautés

Amélioration de l'expérience de reconnexion d'applications et de bureaux virtuels Cette version offre une expérience utilisateur améliorée lors de la reconnexion aux applications et aux bureaux virtuels dont vous étiez déconnecté.

Lorsque l'application Citrix Workspace tente d'actualiser l'application Citrix Workspace déconnectée ou de démarrer de nouvelles applications ou nouveaux bureaux virtuels dans le cadre de la fonctionnalité Contrôle de l'espace de travail, l'invite suivante s'affiche :

Restore session?

You have one or more apps/desktops running from the previous session in Citrix Workspace app. Would you like to restore them?

Remember my preference



Cette invite s'affiche uniquement lorsque l'option **show reconnection prompt to reconnect sessions** est définie sur true dans Global App Configuration Service.

Cliquez sur **Restaurer** pour vous reconnecter afin d'ouvrir des applications et des bureaux virtuels nouveaux et déconnectés. Si vous souhaitez démarrer uniquement les applications et les bureaux récemment sélectionnés, cliquez sur **Annuler**.

Vous pouvez également sélectionner **Mémoriser ma préférence** pour appliquer la préférence sélectionnée lors de la prochaine connexion.

La nouvelle invite **Restaurer la session ?** apparaît uniquement si :

- l'utilisateur essaie de démarrer une application appartenant à un magasin d'espace de travail,
- les stratégies administratives ou les paramètres de configuration de l'application ne sont pas configurés pour la fonctionnalité Contrôle de l'espace de travail,
- les options de reconnexion de Contrôle de l'espace de travail sont définies par défaut sur le client.

Remarque :

Les paramètres de reconnexion dans les **options de reconnexion** ont priorité sur les préférences définies dans la boîte de dialogue. Pour plus d'informations, consultez la section [Configurer les options de reconnexion à l'aide de la boîte de dialogue Préférences avancées](#).

Gestion des applications clientes pour le plug-in Zoom Vous pouvez désormais gérer le plug-in Zoom à l'aide de la fonctionnalité Gestion des applications clientes.

Pour plus d'informations, consultez la section [Gestion des applications clientes pour le plug-in Zoom](#).

Modification du comportement de sélection des périphériques audio pour la version optimisée de Microsoft Teams À compter de cette version, lorsque vous modifiez les périphériques audio par défaut dans les paramètres audio du terminal, Microsoft Teams optimisé dans Citrix VDI modifie la sélection actuelle de périphériques audio pour qu'elle corresponde aux valeurs par défaut du terminal.

Toutefois, si vous sélectionnez un périphérique de manière explicite dans Microsoft Teams, votre sélection est prioritaire et ne correspond pas aux valeurs par défaut du terminal. Votre sélection est persistante jusqu'à ce que vous effaciez le cache Microsoft Teams.

Amélioration de App Protection À compter de cette version, l'application Citrix Workspace pour Windows vous permet de configurer la protection des applications pour Authentication et Self-Service Plug-in à l'aide de Global App Configuration. Auparavant, vous pouviez configurer ces composants uniquement à l'aide de l'objet de stratégie de groupe.

Si vous activez les fonctionnalités de protection contre l'enregistrement de frappe et contre la capture d'écran à l'aide du service Global App Configuration, elles s'appliquent à la fois à Authentication et à Self-Service Plug-in.

Remarque :

Les configurations de Global App Configuration Service ne s'appliquent pas aux applications virtuelles, aux bureaux virtuels, aux applications Web et aux applications SaaS. Ces ressources continuent d'être contrôlées à l'aide du Delivery Controller et de Citrix Secure Private Access. Pour plus d'informations, consultez la section [Configuration](#) de la documentation Protection des applications.

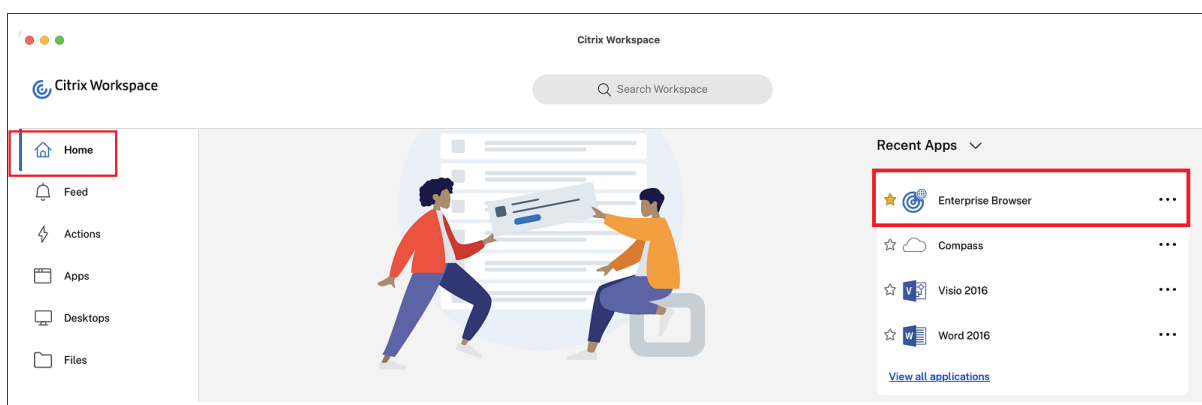
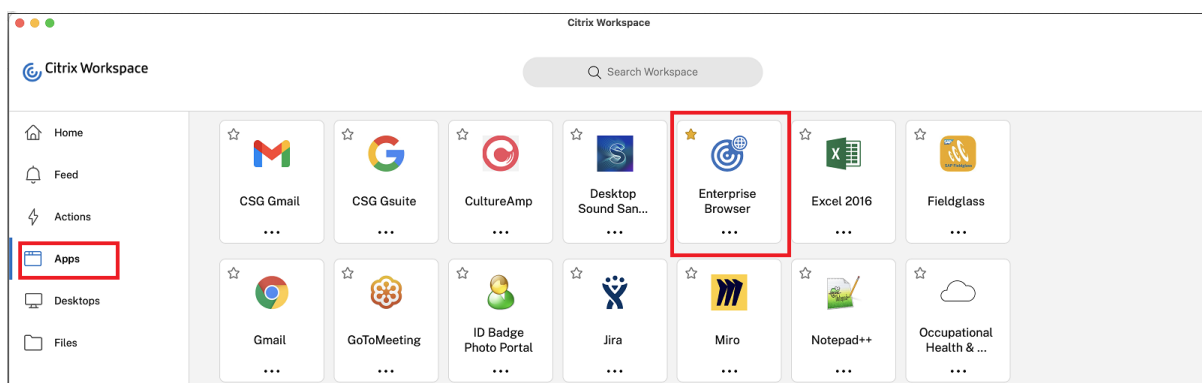
Pour plus d'informations, consultez la section [Amélioration de la protection des applications](#).

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 108.1.1.97, basé sur Chromium version 108. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

Ouvrir toutes les applications Web et SaaS via Citrix Enterprise Browser Dans cette version d'Enterprise Browser (dans l'application Citrix Workspace pour Windows), toutes les applications Web internes et les applications SaaS externes disponibles dans l'application Citrix Workspace s'ouvrent dans Citrix Enterprise Browser.

Option permettant de démarrer Citrix Enterprise Browser depuis l'application Citrix Workspace Auparavant, vous pouviez ouvrir Citrix Enterprise Browser à partir de l'application Citrix Workspace après avoir ouvert une application Web ou SaaS.

À partir de cette version, vous pouvez ouvrir Citrix Enterprise Browser directement à partir de l'application Citrix Workspace sans avoir à ouvrir une application Web ou SaaS. Cette fonctionnalité permet d'accéder facilement à Citrix Enterprise Browser et ne nécessite aucune configuration de la part des administrateurs. Cette fonctionnalité est disponible par défaut.



Remarque :

L'utilisateur final doit avoir accès à au moins une application Web ou SaaS via Secure Private Access.

2212

Nouveautés

Remarque :

À partir de cette version, assurez-vous que la version de Microsoft Edge WebView2 Runtime est 102 ou une version ultérieure. Pour plus d'informations, consultez la section [Configuration système requise et compatibilité](#).

Gestion des applications clientes L'application Citrix Workspace 2212 pour Windows offre désormais une fonctionnalité de gestion des applications clientes qui fait de l'application Citrix Workspace une application cliente unique requise sur le terminal pour installer et gérer des agents tels que Secure Access Agent et le plug-in Endpoint Analysis (EPA).

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

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

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

Les administrateurs peuvent contrôler la version en définissant la version dans la propriété `maximumAllowedVersion` dans Global App Config Service.

Exemple de fichier JSON dans Global App Config Service :

```
1 {
2
3   "category": "AutoUpdate",
4   "userOverride": false,
5   "assignedTo": [
6     "AllUsersNoAuthentication"
7   ],
8   "settings": [
9     {
10
11       "name": "Auto Update plugins settings",
12       "value": [
13         {
14
15           "pluginSettings": {
16
17             "upgradeToLatest": false,
18             "deploymentMode": "InstallAndUpdate",
19             "stream": "Current",
20             "maximumAllowedVersion": "23.03.0.49",
21             "minimumAllowedVersion": "0.0.0.0",
22             "delayGroup": "Fast"
23           }
24         },
25         {
26           "pluginName": "WorkspaceApp",
27           "pluginId": "1CDF566D-B2C7-47CA-802F-6283C862E1D6"
28         }
29       ]
30     }
31   ]
32 }
33
34
35
36 <!--NeedCopy-->
```

Lorsque la version est définie, l'application Citrix Workspace sur l'appareil de l'utilisateur est automatiquement mise à jour vers la version spécifiée dans la propriété `maximumAllowedVersion`.

Remarques :

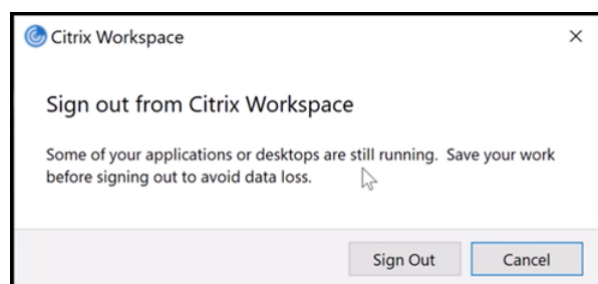
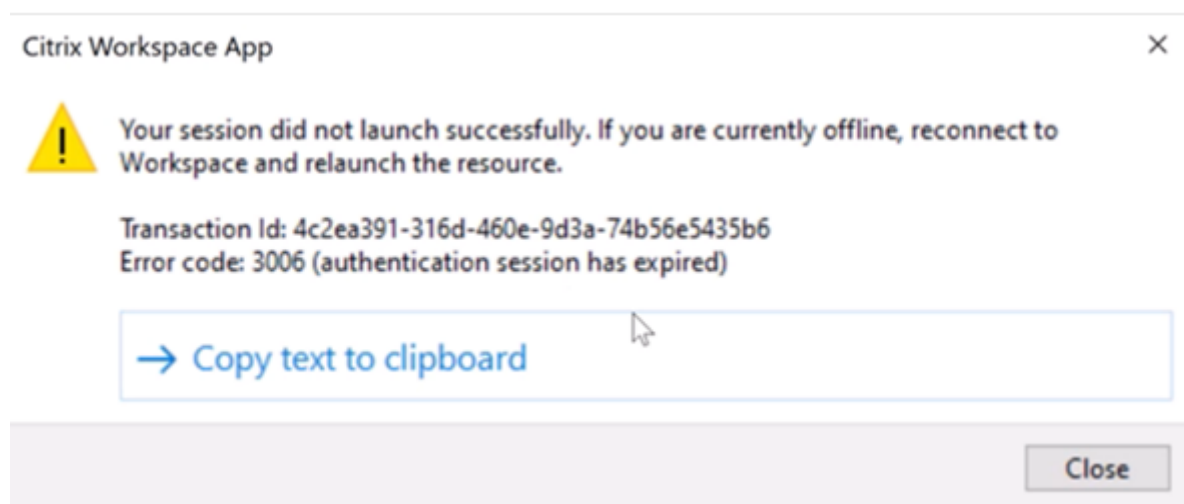
- Actuellement, tous les paramètres mentionnés dans le fichier JSON précédent sont obligatoires. Vous devez fournir des valeurs pour les paramètres `upgradeToLatest` et `maximumAllowedVersion` en fonction des besoins de votre organisation. Toutefois, pour les autres paramètres, vous pouvez utiliser des valeurs similaires à celles du fichier JSON d'exemple.
- Pour avoir accès au contrôle de la version de mise à jour automatique, le paramètre `upgradeToLatest` de Global App Config Service doit être défini sur « false ». Si ce paramètre est défini sur true, `maximumAllowedVersion` est ignoré.
- Ne modifiez pas la valeur de `pluginId` car cet ID est mappé à l'application Citrix Workspace.
- Si l'administrateur n'a pas configuré la version dans Global App Config Service, l'application Citrix Workspace est mise à jour vers la dernière version disponible par défaut.

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

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

Expérience de reconnexion améliorée après expiration du fichier de location de connexion Au-paravant, aucune notification n'était envoyée à l'utilisateur final lorsque le fichier de location de connexion et le jeton d'authentification expiraient.

À partir de cette version, un message d'erreur et une boîte de dialogue de consentement s'affichent. La boîte de dialogue de consentement s'affiche uniquement lorsque des ressources sont en cours d'exécution dans la session. Si aucune ressource n'est en cours d'exécution, seule la boîte de dialogue d'erreur s'affiche. Vous êtes déconnecté sans que la boîte de dialogue de consentement ne vous y invite.



Vous pouvez cliquer sur **Déconnexion** pour vous déconnecter de la session d'application Citrix Workspace en cours ou sur **Annuler** pour poursuivre la session.

Remarque :

Enregistrez vos données avant de cliquer sur **Déconnexion**.

Prise en charge de l'installation par défaut de la App Protection Le composant App Protection est désormais installé par défaut lors de l'installation de l'application Citrix Workspace.

La case à cocher **Activer App Protection** qui apparaît lors de l'installation est remplacée par Démarrer App Protection après l'installation.



Lorsque vous cochez cette case, la fonctionnalité App Protection démarre immédiatement après l'installation.

Remarque :

Si vous n'activez pas cette case à cocher, App Protection démarre automatiquement dès le premier démarrage d'une ressource ou d'un composant protégé pour les clients pouvant bénéficier d'App Protection.

Vous pouvez également démarrer le composant App Protection à l'aide du paramètre de ligne de commande `/startappprotection`. Cependant, l'ancien commutateur `/includeappprotection` est obsolète.

Remarque :

Auparavant, les fonctionnalités anti-capture d'écran et de protection contre l'enregistrement de frappe étaient appliquées par défaut pour l'authentification Citrix et les écrans de l'application Citrix Workspace. Toutefois, à partir de la version 2212, ces fonctionnalités sont désactivées par défaut et doivent être configurées à l'aide de l'objet de stratégie de groupe. Pour plus d'informations sur la configuration de l'objet de stratégie de groupe, consultez la section [Amélioration de la configuration d'App Protection](#).

Amélioration de la protection des applications : détection et notification de capture d'écran À partir de cette version, vous pouvez afficher une notification lorsqu'une éventuelle tentative de capture d'écran est effectuée sur des ressources protégées. Pour plus d'informations sur les ressources protégées par App Protection, consultez la section [Éléments inclus dans App Protection](#).

La notification apparaît lorsqu'il y a une :

- tentative de capture d'écran ou d'enregistrement de vidéo à l'aide d'un outil de capture d'écran
- tentative de capture d'écran à l'aide de la touche Impression écran

Remarque :

La notification n'apparaît qu'une seule fois par instance en cours d'exécution de l'outil de capture d'écran. La notification réapparaît si vous relancez l'outil et effectuez une tentative de capture d'écran.

Optimisation de Desktop Viewer Cette version optimise l'expérience de Desktop Viewer en réduisant le temps de lancement de 5 secondes. La barre d'outils de **Desktop Viewer** s'ouvre rapidement et peut afficher l'écran de connexion à une session Windows par défaut. Les administrateurs peuvent masquer cette expérience en configurant le registre suivant pour introduire un délai en millisecondes :

- Emplacement : HKEY_CURRENT_USER\SOFTWARE\Citrix\XenDesktop\DesktopViewer
- Nom : ExtendConnectScreenMS
- Type : DWORD
- Valeur : 00000000 (délai en millisecondes)

Remarque :

La configuration du registre est facultative.

Citrix Enterprise Browser

Remarque :

À partir de l'application Citrix Workspace pour Windows version 2210, la fonctionnalité **Ouvrir toutes les applications Web et SaaS via Citrix Enterprise Browser** est désactivée.

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

- **Définir Citrix Enterprise Browser comme navigateur de travail**

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

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

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

2210.5

Nouveautés

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

Amélioration de la mise à jour automatique L'application Citrix Workspace prend désormais en charge la mise à jour automatique lorsque la configuration automatique du proxy (PAC) et la détection WPAD (Web Proxy Auto-Discovery Protocol) sont activées.

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

2210

Nouveautés

Flou d'arrière-plan pour la redirection de la webcam L'application Citrix Workspace pour Windows prend désormais en charge le flou d'arrière-plan pour la redirection de la webcam. Vous pouvez activer cette fonctionnalité en sélectionnant **Préférences > Connexions > Activer flou d'arrière-plan**.

Améliorations d'App Protection pour les applications Web et SaaS sur Windows 11 Cette amélioration de la protection des applications optimise l'expérience et les fonctionnalités de sécurité pour les utilisateurs d'applications Web et SaaS sous Windows 11. Cette amélioration est disponible via le navigateur Citrix Enterprise Browser pour les clients Secure Private Access.

Limiter les résolutions vidéo Les administrateurs dont les utilisateurs utilisent des points de terminaison client moins performants peuvent choisir de limiter les résolutions vidéo entrantes ou sortantes afin de réduire l'impact du codage et du décodage vidéo sur ces points de terminaison. À partir de l'application Citrix Workspace 2010 pour Windows, vous pouvez limiter ces résolutions à l'aide des options de configuration du client.

Remarque :

Les utilisateurs utilisant des résolutions restreintes affecteront la qualité vidéo globale de la conférence, car le serveur Microsoft Teams sera obligé d'utiliser la résolution du plus petit dénominateur commun pour tous les participants à la conférence.

Les contraintes d'appel sont désactivées par défaut sur le client avec l'application Citrix Workspace 2210. Pour l'activer, les administrateurs doivent définir les configurations côté client suivantes dans le fichier HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream :

Nom	Type	Mandatory	Valeurs acceptées
EnableSimulcast	Entier	OUI	1-3 (Définir sur 1)
MaxOutgoingResolution	Entier	OUI	180, 240, 360, 540, 720, 1080 (résolutions prises en charge par Microsoft Teams)
MaxIncomingResolution	Entier	OUI	180, 240, 360, 540, 720, 1080 (résolutions prises en charge par Microsoft Teams)
MaxIncomingStreams	Entier	OUI	1-8
MaxSimulcastLayers	Entier	OUI	1-3 (Définir sur 1)
MaxVideoFrameRate	Entier	NON	1-30
MaxScreenShareFrameRate	Entier	NON	1-15

Toutes les clés sont des valeurs DWORD.

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 105.1.1.27, basé sur Chromium version 105. Pour plus d'informations sur Citrix Enterprise Browser, consultez la documentation de [Citrix Enterprise Browser](#).

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

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

- L'interface utilisateur du produit, le contenu intégré au produit, ainsi que les images et les instructions de la documentation produit seront mis à jour au cours des prochaines semaines.
- Il est possible que certains éléments (tels que les commandes et les MSI) continuent à conserver leurs anciens noms pour éviter de casser les scripts clients existants.
- La documentation produit associée et les autres ressources (telles que les vidéos et les billets de blog) auxquelles la documentation de ce produit renvoie peuvent toujours contenir des noms anciens.

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

Remarque :

À partir de l'application Citrix Workspace pour Windows version 2210, la fonctionnalité **Ouvrir toutes les applications Web et SaaS via Citrix Enterprise Browser** est désactivée.

Prise en charge de la mise à jour automatique de l'application Citrix Workspace sur le VDA Vous pouvez désormais activer la fonctionnalité de mise à jour automatique sur le VDA en créant la valeur de registre suivante :

Sur une machine 32 bits :

- Clé de registre : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\AutoUpdate
- Valeur de registre : AllowAutoUpdateOnVDA
- Type de registre : REG_SZ
- Données du registre : True

Sur une machine 64 bits :

- Clé de registre : HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\AutoUpdate
- Valeur de registre : AllowAutoUpdateOnVDA
- Type de registre : REG_SZ
- Données du registre : True

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

- **Profils de Citrix Enterprise Browser**

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

Remarque :

Après la mise à niveau vers la version 103.2.1.10 et la première connexion à l'appareil, seuls les mots de passe précédemment enregistrés sont supprimés. Lorsque vous vous connectez à l'appareil en utilisant un autre magasin pour la première fois, toutes vos données précédemment enregistrées sont perdues.

2207

Nouveautés

Flou et effets d'arrière-plan pour l'optimisation de Microsoft Teams avec HDX L'application Citrix Workspace pour Windows prend désormais en charge le flou et les effets d'arrière-plan dans l'optimisation Microsoft Teams avec HDX.

Vous pouvez flouter ou remplacer l'arrière-plan par une image personnalisée et éviter les distractions inattendues en aidant la conversation à rester centrée sur la silhouette (corps et visage). La fonctionnalité peut être utilisée avec les appels P2P ou les conférences téléphoniques.

Remarque :

Cette fonctionnalité est désormais intégrée à l'interface utilisateur/aux boutons de Microsoft Teams. La prise en charge de fenêtres multiples est une condition préalable qui nécessite une mise à jour du VDA vers 2112 ou une version ultérieure. Pour plus d'informations, consultez [Réunions et chat en mode multi-fenêtres](#).

Limitations :

- Le remplacement de l'arrière-plan défini par l'administrateur et l'utilisateur n'est pas pris en charge.
- L'effet d'arrière-plan ne persiste pas entre les sessions. Lorsque vous fermez et relancez Microsoft Teams ou que le VDA est reconnecté, l'effet d'arrière-plan est réinitialisé sur Désactivé.

- Une fois la session ICA reconnectée, l'effet est désactivé. Toutefois, une coche sur l'interface utilisateur de Microsoft Teams indique que l'effet précédent est toujours activé. Citrix et Microsoft travaillent ensemble pour résoudre ce problème.
- L'appareil doit être connecté à Internet lors du remplacement de l'image d'arrière-plan.

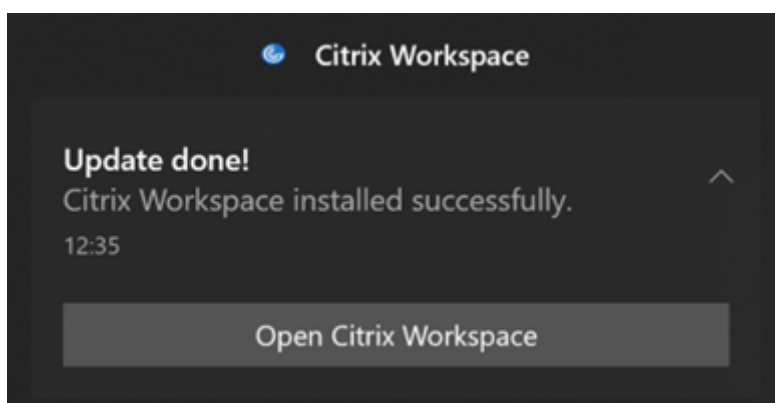
Remarque :

Cette fonctionnalité est disponible uniquement après le déploiement d'une future mise à jour de Microsoft Teams. Une fois la mise à jour déployée par Microsoft, vous pourrez consulter l'article du centre de connaissances [CTX253754](#) et la page [Roadmap Microsoft 365](#) pour obtenir plus d'informations sur la mise à jour de la documentation et l'annonce.

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

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

Lorsque l'installation est terminée, la notification suivante s'affiche :



Si l'application Citrix Workspace ne trouve pas le bon moment pour installer les mises à jour en arrière-plan, une notification s'affiche.

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 102.1.1.14, basé sur Chromium version 102.

Remarque sur la mise à jour de l'application Citrix Workspace Lors de la mise à jour de l'application Citrix Workspace pour Windows depuis la version précédente vers 2207, l'utilisateur est invité à se connecter. La connexion est requise uniquement pour le magasin Workspace.

2206

Nouveautés

Performances graphiques améliorées L'application Citrix Workspace 2206 apporte des améliorations importantes aux performances des GPU intégrés Intel :

- La consommation du GPU graphique a été réduite, améliorant ainsi les performances globales.

Les problèmes suivants ont été résolus :

- Nombre d'images par seconde faible après la lecture d'une vidéo sur un processeur graphique Intel 10e génération ou supérieur.
- Différence de luminosité en mode Build-To-Lossless ou pour les zones changeant constamment sur les GPU Intel et AMD.

Activer la correspondance DPI À partir de l'application Citrix Workspace 2206 pour Windows, la correspondance DPI est activée par défaut. Cela signifie que l'application Citrix Workspace tente de faire correspondre automatiquement la résolution d'affichage et les paramètres de mise à l'échelle DPI du client Windows local à la session Citrix. Dans le cadre de cette modification, l'option DPI élevé disponible sous Préférences avancées dans l'application Citrix Workspace n'est plus disponible. Pour obtenir davantage d'informations, veuillez consulter l'article [CTX460068](#) du centre de connaissances.

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 101.1.1.12, basé sur Chromium version 101. Pour connaître les fonctionnalités ou les corrections de bogues dans Citrix Enterprise Browser, consultez [Nouveautés](#) dans la documentation de Citrix Enterprise Browser.

2205

Nouveautés

Remarque :

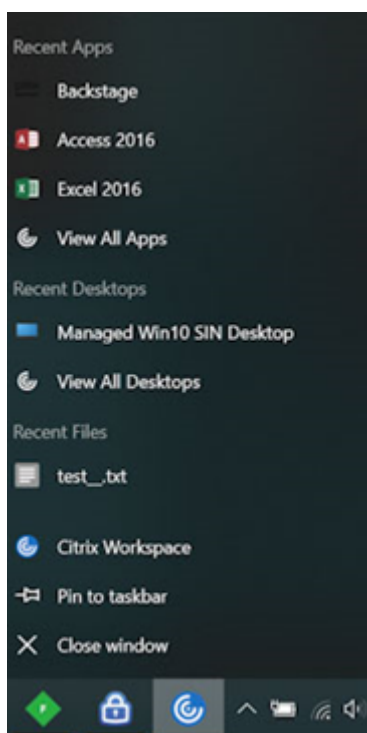
À partir de cette version, assurez-vous que la version de Microsoft Edge WebView2 Runtime est 99 ou une version ultérieure. Pour plus d'informations, consultez la section [Configuration système requise et compatibilité](#).

Modifications apportées à Citrix Casting Auparavant, Citrix Casting était activé par défaut lors de l'installation de l'application Citrix Workspace. À partir de cette version, Citrix Casting est activé uniquement si vous exécutez le programme d'installation de l'application Citrix Workspace avec la

commande `/IncludeCitrixCasting` pendant l'installation.

Lorsque vous mettez à jour l'application Citrix Workspace, Citrix Casting est automatiquement mis à jour. Pour plus d'informations sur Citrix Casting, consultez [Citrix Casting](#).

Accès rapide aux ressources À partir de cette version, vous pouvez accéder rapidement à vos applications et bureaux récemment utilisés. Cliquez avec le bouton droit de la souris sur l'icône de l'application Citrix Workspace dans la barre des tâches pour afficher et ouvrir les ressources récemment utilisées à partir du menu contextuel.



Déconnexion du magasin Web personnalisé en quittant l'application Citrix Workspace Lorsque l'attribut `signoutCustomWebstoreOnExit` est défini sur True, la fermeture de l'application Citrix Workspace vous déconnecte des magasins Web personnalisés. Vous pouvez configurer l'attribut `signoutCustomWebstoreOnExit` dans **Global App Configuration Service**.

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

Prise en charge de l'ouverture de l'application Citrix Workspace en mode agrandi À partir de cette version, vous pouvez choisir d'ouvrir l'application Citrix Workspace en mode agrandi. Au lieu de maximiser l'application Citrix Workspace manuellement à chaque fois, vous pouvez définir la propriété `maximise workspace window` dans Global App Configuration Service pour permettre à l'application Citrix Workspace de s'ouvrir en mode agrandi par défaut.

Pour plus d'informations sur Global App Configuration Service, consultez la section [Mise en route](#).

Prise en charge de Storebrowse pour Workspace L'application Citrix Workspace pour Windows prend en charge Storebrowse sur Self Service et permet aux utilisateurs de Storebrowse d'accéder aux fonctionnalités Cloud et de Workspace.

Remarque :

- Cette fonctionnalité prend en charge Storebrowse uniquement avec l'authentification unique.
- Les prérequis mentionnés dans [Configuration système requise et compatibilité](#) doivent être disponibles pour utiliser cette fonctionnalité.

Pour plus d'informations, consultez [Storebrowse pour Workspace](#).

Citrix Enterprise Browser

- Cette version inclut Citrix Enterprise Browser version 99.1.1.8, basé sur Chromium version 99. Pour connaître les fonctionnalités ou les corrections de bogues dans Citrix Enterprise Browser, consultez [Nouveautés](#) dans la documentation de Citrix Enterprise Browser.
- L'application Citrix Workspace vous avertit désormais de la fermeture des fenêtres de navigateur actives lorsque vous effectuez l'une des opérations suivantes dans l'application Citrix Workspace :
 - Se déconnecter d'un magasin
 - Passer à un autre magasin
 - Ajouter un nouveau magasin
 - Supprimer le magasin actuel

2204.1

Nouveautés

Amélioration de la redirection audio Prise en charge améliorée de l'annulation de l'écho audio pour tous les codecs audio, y compris l'audio adaptatif et tous les anciens codecs audio

Citrix Enterprise Browser Cette version inclut Citrix Enterprise Browser version 98.1.2.20, basé sur Chromium version 98. Pour connaître les fonctionnalités ou les corrections de bogues dans Citrix Enterprise Browser, consultez [Nouveautés](#) dans la documentation de Citrix Enterprise Browser.

Optimisation pour Microsoft Teams

- **Protection des applications et amélioration de Microsoft Teams** : Microsoft Teams prend en charge les vidéos entrantes et le partage d'écran lorsque l'application Citrix Workspace pour Windows sur laquelle la fonctionnalité de protection des applications est activée est en mode Desktop Viewer uniquement. Les applications publiées en mode transparent ne rendent pas les vidéos entrantes ni le partage d'écran.

Ancienne documentation

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

Avis de tiers

L'application Citrix Workspace 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)

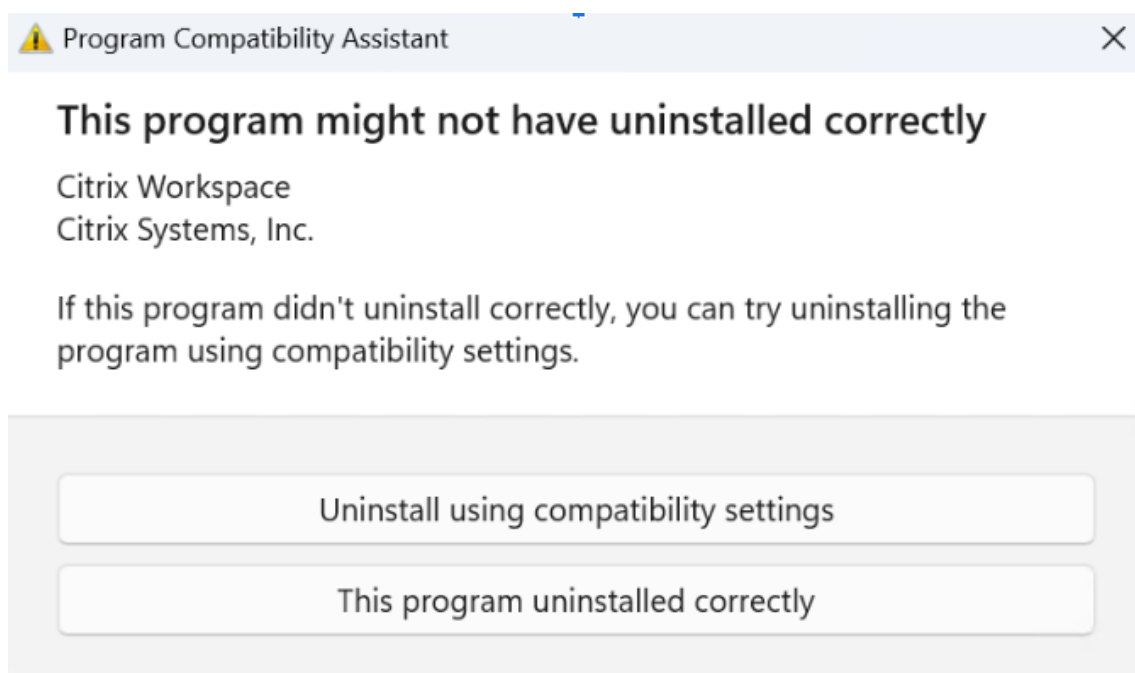
Problèmes résolus

April 22, 2024

Problèmes résolus dans la version 2402 LTSR

- Vous remarquerez peut-être l'absence de focus automatique dans le bureau virtuel ouvert en mode plein écran. Vous devez cliquer à l'intérieur de la session pour vous réactiver le focus. [RFWIN-32051]
- Lors de la reconnexion d'applications publiées, une instance supplémentaire d'une application publiée s'ouvre. [CVADHELP-24485]
- Il se peut que le pavé tactile et le clavier logiciel Windows Surface ne soient pas pris en charge sur l'écran de connexion de l'application Citrix Workspace. Ce problème se produit lorsque vous vous connectez à une session publiée depuis le VDA Windows en mode plein écran. Pour le contourner, ouvrez la session en mode fenêtré, puis connectez-vous à l'application Citrix Workspace. [RFWIN-32050]
- Deux instances d'une application publiée, par exemple app1, sont observées après la déconnexion d'app1 et le lancement d'une autre application à partir du même VDA. [RFWIN-32517]

- Pour la version **Windows 10 32bits x86**, la case **Activer le flou d'arrière-plan** est supprimée car l'effet de flou d'arrière-plan n'est pas pris en charge dans cette version. [HDX-60308]
- Il se peut que le pavé tactile et le clavier logiciel Windows Surface ne soient pas pris en charge sur l'écran de connexion de l'application Citrix Workspace. Ce problème se produit lorsque vous vous connectez à une session publiée depuis le VDA Windows en mode plein écran. [RFWIN-32050]
- Le son peut être endommagé si plusieurs flux sont diffusés en même temps sur la même page. [HDX-50486]
- Vous remarquerez peut-être des artefacts visuels lorsque vous tentez de diviser l'écran ou de régler le moniteur principal dans l'onglet **Disposition du moniteur** de l'écran **Préférences**. [HDX-59798]
- Windows Media Player (WMP) affiche un écran noir avec Rave activé sur un moniteur lorsque le moniteur principal n'est pas le moniteur le plus à gauche (lorsque plusieurs unités de traitement graphique sont impliquées). Pour résoudre ce problème, le moteur de rendu par défaut **VMR9** a été redéfini sur **EVR**.
Si vous souhaitez désactiver **EVR**, créez `DWORD AllowEvrH264 = 0` sous `Computer\HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream`. [HDX-60494]
- Lorsque vous partagez un écran et incluez le son d'un ordinateur, si plusieurs périphériques de sortie audio diffusent du son, un ou plusieurs récepteurs peuvent remarquer des artefacts sonores. [HDX-48213]
- Le BCR peut lire plusieurs flux audio en même temps plutôt qu'un flux actif. [HDX-61600]
- Si vous utilisez des moniteurs externes, puis passez à un moniteur unique (par exemple, un ordinateur portable), la taille des options du menu de l'application Citrix Workspace, du texte de l'interface utilisateur et des boîtes de dialogue peut apparaître inférieure à la taille d'affichage normale. [HDX-47575]
- Lorsque vous effectuez une mise à niveau vers la version 2402 de l'application Citrix Workspace, la commande `InstallEmbeddedBrowser=N` n'est pas exécutée si le navigateur Citrix Enterprise est déjà installé. [RFWIN-33169]
- Si vous utilisez un son mono pour des flux audio stéréo, il se peut que vous n'entendiez qu'un seul canal audio dans un écouteur au lieu de recevoir les deux canaux dans les deux oreilles. [HDX-56344]
- Lors de la désinstallation de l'application Citrix Workspace 2402 LTSR pour Windows - Technical Preview depuis **Panneau de configuration > Programmes > Programmes et fonctionnalités**, la fenêtre contextuelle suivante s'affiche :



Le problème se produit par intermittence sur les machines Windows 11. De plus, ce problème ne se produit dans le cadre d'aucune autre méthode de désinstallation, y compris la désinstallation depuis **Démarrer > Applications > Applications et fonctionnalités**. La désinstallation s'est terminée avec succès même si le message d'erreur précédent s'affiche. [RFWIN-32669]

- Le processus de démarrage de l'application Citrix Workspace peut s'exécuter par défaut dans le cadre de sessions d'application publiées. Si vous souhaitez exécuter le processus de démarrage dans une session d'application publiée, configurez la clé de registre `RunCWAInPublishedAppSession` de type `DWORD` dans `HKLM/Software/Wow6432Node/Citrix/ICA Client`. [CVADHELP-24070]

Problèmes connus

April 22, 2024

Problèmes connus dans la version 2402 LTSR

- Dans un scénario à double saut, il est possible que la touche `ALT + TAB` ne fonctionne pas sur les clients macOS. [CVADHELP-23085]

Configuration système requise et compatibilité

April 23, 2024

Exigences

Configuration matérielle requise

- 2 Go de RAM minimum
- Le tableau suivant fournit des informations sur l'espace disque requis pour installer l'application Citrix Workspace.

Type d'installation	Espace disque requis
Nouvelle installation	1 Go
Mettre à niveau	1 Go

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 `Citrix\Logs\CTXWorkspaceInstallLogs-*`.

Configuration logicielle requise

- Microsoft Edge WebView2 Runtime version 119 ou ultérieure
- .NET Framework 4.8 et .NET Desktop Runtime 6.0.25 ou version ultérieure
- Dernière version de Microsoft Visual C++ Redistributable

Remarque :

Pour gérer les correctifs de sécurité de Microsoft ou d'autres composants dépendants de tiers (par exemple : .NET Core, .NET Framework, VC redistributable, Edge Webview), vous pouvez utiliser l'une des méthodes suivantes :

- Activer la mise à jour automatique de Windows sur les machines clientes
- Les administrateurs informatiques géreront le déploiement des correctifs à l'aide d'outils

tels que SCCM

Configuration requise pour Microsoft Edge WebView2

- L'application Citrix Workspace est fournie avec la version [Evergreen Bootstrapper](#) de Microsoft Edge WebView2 Runtime.
- Le programme d'installation de l'application Citrix Workspace peut installer Microsoft Edge WebView2 Runtime lors de l'installation de l'application Citrix Workspace. Toutefois, pour cette installation, vous devez être connecté à Internet. Vous pouvez également installer le package [Microsoft Edge WebView2 Runtime Evergreen Standalone Installer](#) hors ligne approprié avant d'installer l'application Citrix Workspace.
- L'appareil doit avoir accès aux URL suivantes :
 - https://*.dl.delivery.mp.microsoft.com pour télécharger Microsoft Edge WebView2 Runtime lors de l'installation de l'application Citrix Workspace. Pour plus d'informations, consultez [Liste verte pour les points de terminaison de Microsoft Edge](#).
 - <https://msedge.api.cdp.microsoft.com> pour vérifier la mise à jour de Microsoft Edge WebView2 Runtime.
 - Connexion Internet
 - L'appareil doit avoir accès aux URL suivantes :

Remarque :

Lorsque vous essayez d'installer ou de mettre à niveau l'application Citrix Workspace avec des privilèges de non administrateur et que Microsoft Edge WebView2 Runtime n'est pas présent, l'installation s'arrête avec le message suivant : « Vous devez être connecté en tant qu'administrateur pour installer les packages requis suivants : Edge Webview2 Runtime ».

Configuration requise pour .NET

Pré-requis

- Versions .NET Framework 4.8 et x86 de .NET Desktop Runtime 6.0.25 ou version ultérieure. Vous devez installer la version x86 même sur un système x64.
- En cas d'installation de .NET dans le cadre de l'installation de l'application Citrix Workspace, assurez-vous d'être connecté à Internet.
- Privilèges d'administrateur

Remarque :

Si vous essayez d'installer ou de mettre à niveau l'application Citrix Workspace avec des privilèges non administrateur et que .NET Framework 4.8 ou .NET Desktop Runtime 6.0.25 ou version ultérieure n'est pas présent sur le système, l'installation échoue.

Méthode d'installation

Version .NET

Méthode de déploiement

L'application Citrix Workspace 1904 ou version ultérieure requiert .NET Framework 4.8. Outre .NET Framework 4.8, l'application Citrix Workspace 2309 ou version ultérieure requiert la version x86 de .NET Desktop Runtime 6.0.25 ou version ultérieure pour les systèmes x86 et x64.

Méthode 1 : l'application Citrix Workspace installe .NET Framework 4.8 et la dernière version de .NET Desktop Runtime 6.0 en même temps que l'installation de l'application. Cette installation est en ligne et requiert une connexion Internet. L'appareil doit avoir accès à l'URL de domaine

downloadplugins.citrix.com.

Méthode 2 : pour les appareils non connectés à Internet, les administrateurs ont la possibilité de télécharger un programme d'installation hors ligne pour l'application Citrix Workspace disponible sur la page [Téléchargements](#). L'administrateur peut également installer les composants requis à l'aide d'une méthode de déploiement, SCCM par exemple.

Méthode 3 : les administrateurs peuvent installer [.NET Framework 4.8](#) et [.NET Desktop Runtime 6.0.25](#) séparément depuis le site Microsoft avant d'installer l'application Citrix Workspace. Il est recommandé de télécharger la dernière version de .NET Desktop Runtime 6.0 (6.0.25 ou version ultérieure).

Configuration requise pour Microsoft Visual C++ Redistributable L'application Citrix Workspace nécessite la 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 partir de la version 1904, le programme d'installation de Microsoft Visual C++ Redistributable ne sont pas emballés avec le programme d'installation de l'application Citrix Workspace. Lors de l'installation de l'application Citrix Workspace, le programme d'installation vérifie si le package Microsoft Visual C++ Redistributable est présent sur le système et l'installe si nécessaire.

Remarque :

Si le package Microsoft Visual C++ Redistributable n'existe pas sur votre système, l'installation de l'application Citrix Workspace avec des privilèges non administrateur peut 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 Citrix [CTX250044](#).

Exigences en matière de connectivité

Gestion des feature flag Si un problème survient avec l'application Citrix Workspace en production, utilisez des commutateurs de fonctionnalité (feature flag) et un service tiers appelé LaunchDarkly pour désactiver dynamiquement une fonctionnalité affectée dans l'application Citrix Workspace, même après sa livraison.

Vous n'avez pas besoin d'effectuer des configurations pour activer le trafic vers LaunchDarkly, sauf si un pare-feu ou un proxy bloque le trafic sortant. Dans ce cas, vous activez le trafic vers LaunchDarkly via des URL ou adresses IP spécifiques, en fonction des exigences de votre stratégie.

Vous pouvez activer le trafic vers les URL suivantes :

- [events.launchdarkly.com](#)
- [stream.launchdarkly.com](#)
- [clientstream.launchdarkly.com](#)
- [Firehose.launchdarkly.com](#)
- [mobile.launchdarkly.com](#)

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

Configuration système requise pour LaunchDarkly Vérifiez si les applications peuvent communiquer avec les services suivants si le split tunneling sur Citrix ADC est **désactivé** :

- Service LaunchDarkly
- Service d'écoute APNs

Désactivation du service LaunchDarkly Vous pouvez désactiver le service LaunchDarkly à l'aide d'une stratégie GPO (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 > Conformité**.
3. Sélectionnez la stratégie **Désactiver l'envoi de données à des tiers** et définissez-la sur **Activé**.
4. Cliquez sur **Appliquer** et **OK**.

Ports

Pour plus d'informations sur les ports requis, consultez la section [Ports de communication Citrix communs](#).

Matrice de compatibilité

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

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.
- L'installation de l'application Citrix Workspace sur Windows n'est prise en charge que si les clients bénéficient d'un support standard ou étendu de Microsoft.
- L'application Citrix Workspace pour Windows est prise en charge uniquement en mode émulateur sur le système d'exploitation Windows ARM64.
- 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 logi-

ciel 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](#).

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

Système d'exploitation

Windows 11

Windows 10 Enterprise (Éditions 32 bits et 64 bits). Pour plus d'informations sur les versions Windows 10 compatibles, consultez [Compatibilité de Windows 10 avec l'application Citrix Workspace pour Windows](#).

Windows 10 Enterprise (2016 LTSB 1607, LTSC 2019)

Windows 10 (Édition familiale*, Pro)

Windows Server 2022

Windows Server 2019

Windows Server 2016

*Aucune prise en charge de l'authentification pass-through au domaine, de Desktop Lock, de l'API FastConnect et des configurations qui nécessitent un ordinateur Windows joint au domaine.

Compatibilité de Windows 10 ou 11 avec l'application Citrix Workspace pour Windows

Le tableau suivant répertorie le numéro de version de Windows 10 et l'application Citrix Workspace compatible correspondante pour les versions de Windows.

Numéro de version de Windows 10	Numéro de compilation	Version de l'application Citrix Workspace
22H2	19045	2206 et versions ultérieures
21H2	19044	2112.1 et versions ultérieures
21H1	19043.928	2106 et versions ultérieures
20H2	19042.508	2012 et versions ultérieures
2004	19041.113	2006.1 et versions ultérieures
1909	18363.418	1911 et versions ultérieures

Numéro de version de Windows 10	Numéro de compilation	Version de l'application Citrix Workspace
1903	18362.116	1909 et versions ultérieures
1809	17763.107	1812 et versions ultérieures
1803	17134.376	1808 et versions ultérieures

Remarque :

Les versions de Windows 10 sont uniquement compatibles avec les versions de l'application Citrix Workspace mentionnées. Par exemple, Windows 10 version 21H1 n'est pas compatible avec les versions antérieures à 2106.

Le tableau suivant répertorie le numéro de version de Windows 11 et l'application Citrix Workspace compatible correspondante pour les versions de Windows.

Numéro de version de Windows 11	Numéro de compilation	Version de l'application Citrix Workspace
23H2	22631	2311 et versions ultérieures
22H2	22621	2209 et versions ultérieures
21H2	22000	2109.1 et versions ultérieures

Installer et désinstaller

April 22, 2024

Vous pouvez télécharger l'application Citrix Workspace à partir de la [page de téléchargement](#) de Citrix ou de 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](#).

Remarque :

Vérifiez que vous avez installé toutes les exigences requises par le système, comme indiqué dans la section [Configuration système requise](#).

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](#), l'authentification unique [Single Sign-On](#), la [protection des applications](#) 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	Pour 64 bits : C:\Program Files (x86)\Citrix\ICA Client ; pour 32 bits : C:\Program Files\Citrix\ICA Client	Installation par système
Utilisateur	%USERPROFILE%\AppData\Local\Citrix\ICA Client	Installation par utilisateur

Remarque :

Les administrateurs peuvent remplacer l'instance de l'application Citrix Workspace installée par l'utilisateur et poursuivre l'installation.

Commande pour nettoyer et installer l'application Citrix Workspace

Utilisez la commande `/CleanInstall` pour nettoyer les traces restantes, telles que les fichiers et les valeurs de registre d'une désinstallation précédente, puis installez la nouvelle version de l'application Citrix Workspace.

Par exemple :

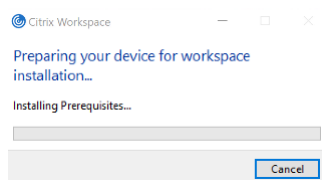
```
1 CitrixWorkspaceApp.exe /CleanInstall
2 <!--NeedCopy-->
```

Installation basée sur l'interface utilisateur

Vous pouvez installer l'application Citrix Workspace pour Windows en exécutant manuellement le package d'installation **CitrixWorkspaceApp.exe**.

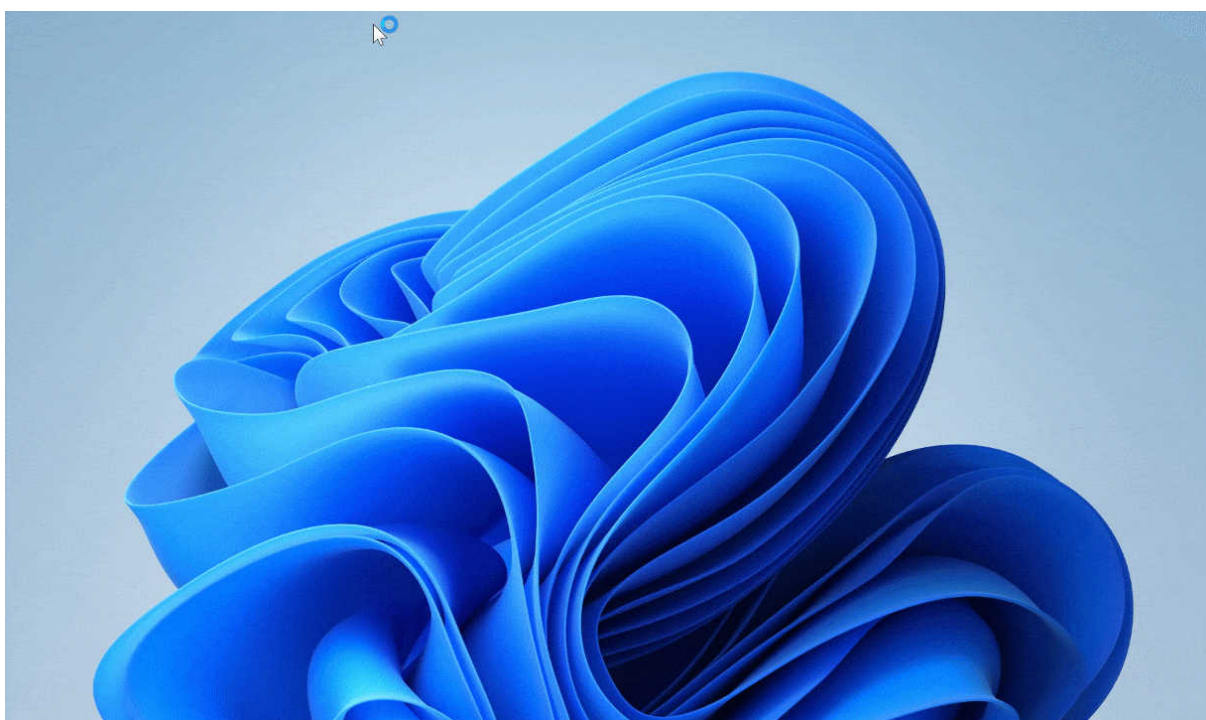
1. Lancez le fichier `CitrixWorkspaceApp.exe`.

Le système vérifie les conditions requises pour l'application Citrix Workspace et, le cas échéant, l'installe automatiquement.



Après avoir installé les composants prérequis, l'écran **Bienvenue dans le programme d'installation de Citrix Workspace** s'affiche.

2. Cliquez sur **Continuer**. La page **Contrat de licence Citrix** s'affiche.
3. Lisez et acceptez le contrat de licence Citrix et poursuivez l'installation. L'installation de l'application Citrix Workspace se poursuit et se termine avec succès.
4. Lors de l'installation avec des privilèges d'administrateur, si nécessaire pour activer la fonctionnalité App Protection, cochez la case **Démarrer App Protection après l'installation**. L'installation de l'application Citrix Workspace se poursuit et se termine avec succès.

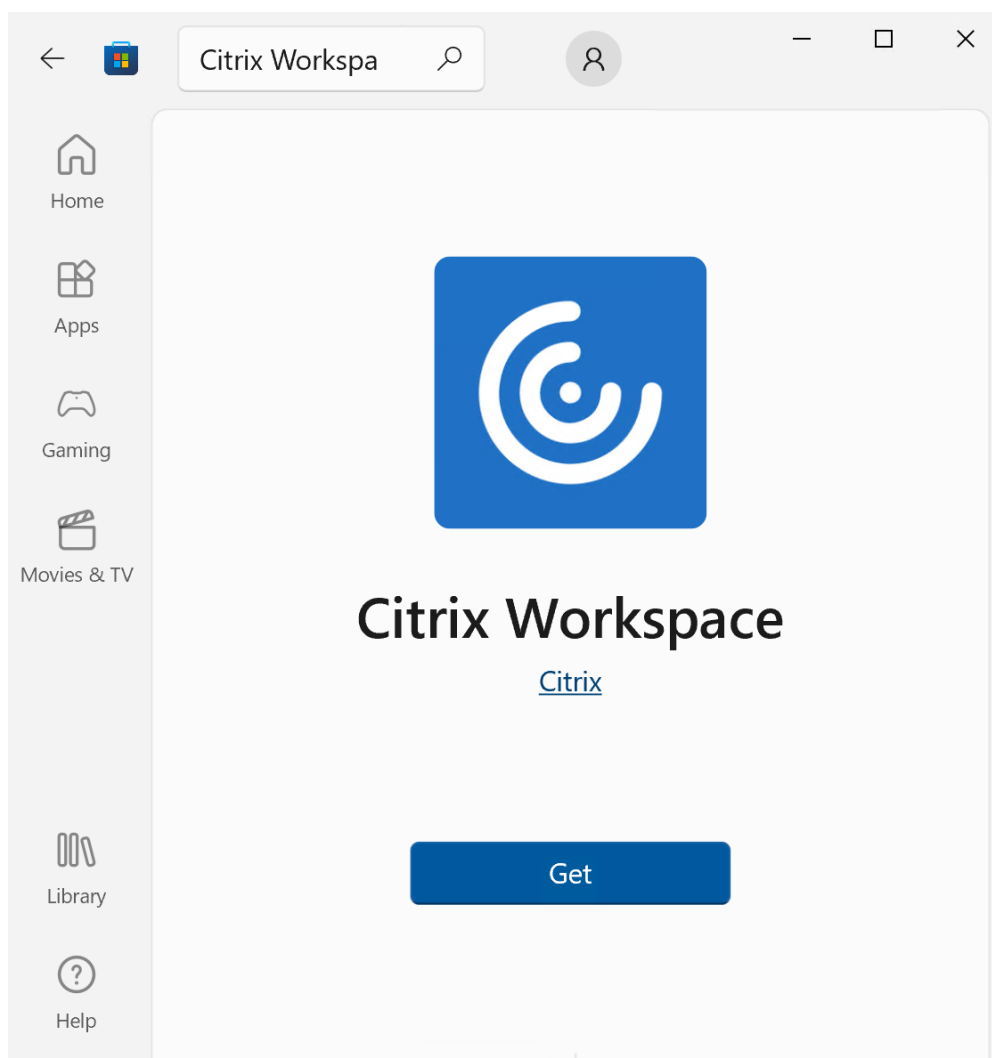


Important :

TrolleyExpress est remplacé par `CWAInstaller-<date and timestamp>`. Par exemple, le journal est enregistré sous `C:\Program Files (x86)\Citrix\Logs\CTXWorkspaceInstallLogs-20231225-093441`.

Utilisation de Windows Store

1. Accédez à Microsoft Store.
2. Recherchez Citrix Workspace.



1. Cliquez sur **Obtenir**. L'application Citrix Workspace est installée.

Installation avec ligne de commande

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

Pour installer l'application Citrix Workspace à l'aide de la ligne de commande Windows, lancez l'invite de commande et tapez ce qui suit sur une seule ligne :

- Nom de fichier du programme d'installation
- Commandes d'installation
- Propriétés d'installation

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 de mise à jour](#)
- [Paramètres d'installation](#)
- [Paramètres des fonctionnalités HDX](#)
- [Préférences et paramètres de l'interface utilisateur](#)
- [Paramètres d'authentification](#)

Paramètres courants

Commande	Description
<code>? Ou help</code>	Répertorie toutes les commandes et propriétés d'installation.
<code>/silent</code>	Désactive les boîtes de dialogue et les invites d'installation pendant l'installation.
<code>noreboot</code>	Supprime les invites 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. Les périphériques USB sont activés uniquement après le redémarrage de l'appareil.

Commande	Description
<code>/forceinstall</code>	Ce commutateur est efficace lors du nettoyage de toute configuration ou entrée existante de l'application Citrix Workspace sur le système. Utilisez ce commutateur lors de la mise à niveau à partir d'une version non prise en charge de l'application Citrix Workspace et lorsque l'installation ou la mise à niveau échoue.

Remarque :

Le commutateur `forceinstall` remplace le commutateur `rcu`. 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](#).

Paramètres de mise à jour automatique

Détecter la mise à jour disponible

- Commande : `AutoUpdateCheck`
- Description : cette commande indique que l'application Citrix Workspace détecte lorsqu'une mise à jour est disponible.

Les valeurs possibles sont les suivantes :

Valeurs de la commande		
AutoUpdateCheck	Description	Exemple
Auto (valeur par défaut)	Vous êtes informé lorsqu'une mise à jour est disponible.	<code>CitrixWorkspaceApp.exe AutoUpdateCheck=auto.</code>
Manual	Vous n'êtes informé pas lorsqu'une mise à jour est disponible. Recherchez les mises à jour manuellement.	<code>CitrixWorkspaceApp.exe AutoUpdateCheck>manual</code>
Désactivé	Les mises à jour automatiques sont désactivées.	<code>CitrixWorkspaceApp.exe AutoUpdateCheck=disabled.</code>

Remarque :

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

Sélectionner la version à mettre à jour

- Commande `AutoUpdateStream`
- Description : si vous avez activé la mise à jour automatique, vous pouvez choisir la version que vous souhaitez mettre à jour. Pour plus d'informations, consultez la section [Étapes du cycle de vie](#).

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
AutoUpdateStream		
LTSR	Mise à jour automatique uniquement vers des mises à jour cumulatives Long Term Service Release.	<code>CitrixWorkspaceApp.exe AutoUpdateStream=LTSR.</code>
Current	Mise à jour vers la dernière version de l'application Citrix Workspace.	<code>CitrixWorkspaceApp.exe AutoUpdateStream=Current</code>

Différer les notifications de mise à jour

- Commande : `DeferUpdateCount`
- Description : indique le nombre de fois où vous pouvez différer les notifications lorsqu'une mise à jour est disponible. Pour plus d'informations, consultez la section [Mises à jour de Citrix Workspace](#).

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
DeferUpdateCount		
-1 (valeur par défaut)	Permet de différer les notifications n'importe quel nombre de fois.	<code>CitrixWorkspaceApp.exe DeferUpdateCount=-1</code>

Valeur de la commande	Description	Exemple
DeferUpdateCount		
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.	<code>CitrixWorkspaceApp.exe DeferUpdateCount =0</code>
Tout autre nombre 'n'	Permet de différer la notification n'importe quel nombre de fois. L'option Me rappeler plus tard s'affiche le nombre « n » de fois défini.	<code>CitrixWorkspaceApp.exe DeferUpdateCount =<n></code>

Remarque :

à partir de la version 2207 de l'application Citrix Workspace pour Windows, la fonctionnalité de mise à jour automatique est améliorée et le paramètre `DeferUpdateCount` n'est pas applicable.

Définir la priorité de déploiement

- Commande : `AURolloutPriority`
- Description : lorsqu'une nouvelle version de l'application est disponible, 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.

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
AURolloutPriority		
Auto (valeur par défaut)	Vous recevez les mises à jour pendant la période de mise à disposition configurée par Citrix.	<code>CitrixWorkspaceApp.exe AURolloutPriority =Auto</code>
Fast (Rapide)	Vous recevez les mises à jour au début de la période de mise à disposition.	<code>CitrixWorkspaceApp.exe AURolloutPriority =Fast</code>

Valeur de la commande	Description	Exemple
AURolloutPriority		
Moyen	Vous recevez les mises à jour au milieu de la période de mise à disposition.	<code>CitrixWorkspaceApp.exe AURolloutPriority=Medium</code>
Slow (Lent)	Vous recevez les mises à jour à la fin de la période de mise à disposition.	<code>CitrixWorkspaceApp.exe AURolloutPriority=Slow</code>

Paramètres de configuration du magasin

Configurer le magasin

- Commande : [ALLOWADDSTORE](#)
- Description : permet de configurer les magasins (http ou https) en fonction du paramètre spécifié.

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
ALLOWADDSTORE		
S (valeur par défaut)	Permet d'ajouter ou de supprimer uniquement des magasins sécurisés (configuré avec HTTPS).	<code>CitrixWorkspaceApp.exe ALLOWADDSTORE=S</code>
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.	<code>CitrixWorkspaceApp.exe ALLOWADDSTORE=A</code>
N	N'autorise pas les utilisateurs à ajouter ou à supprimer leur propre magasin.	<code>CitrixWorkspaceApp.exe ALLOWADDSTORE=N</code>

Enregistrer les informations d'identification du magasin localement

- Commande : [ALLWSAVEPWD](#)

- Description : permet d'enregistrer les informations d'identification du magasin localement. Ce paramètre s'applique uniquement aux magasins utilisant le protocole de l'application Citrix Workspace.

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
ALLOWSAVEPWD		
• S (valeur par défaut)	Autorise l'enregistrement du mot de passe uniquement pour les magasins sécurisés (configurés avec HTTPS).	<code>CitrixWorkspaceApp.exe ALLOWSAVEPWD=S</code>
N	N'autorise pas l'enregistrement du mot de passe.	<code>CitrixWorkspaceApp.exe ALLOWSAVEPWD=N</code>
A	Autorise l'enregistrement du mot de passe pour les magasins sécurisés (HTTPS) et les magasins non sécurisés (HTTP).	<code>CitrixWorkspaceApp.exe ALLOWSAVEPWD=A</code>

Exemples de configuration du magasin à l'aide de l'installation par ligne de commande

Pour spécifier l'URL du magasin StoreFront :

```
1 CitrixWorkspaceApp.exe /silent
2 STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;HR
  App Store
3
4 <!--NeedCopy-->
```

Pour spécifier l'adresse URL du magasin Citrix Gateway :

```
1 CitrixWorkspaceApp.exe STORE0= HRStore;https://ag.mycompany.com#
  Storename;On;Store
2 <!--NeedCopy-->
```

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

Remarque :

- Dans une configuration multi-magasins, une seule configuration de l'URL du magasin Citrix Gateway est autorisée et doit figurer en premier de la liste (paramètre STORE0).

- 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.
- Le paramètre « Discovery » n'est pas requis lors de la spécification d'une URL de magasin Citrix Gateway.

Pour configurer plusieurs magasins :

```
1 CitrixWorkspaceApp.exe STORE0= NetScaler Store;https://ag.mycompany.com#Storename;On;NetScaler Store
2 STORE1="StoreFront Store;https://testserver.net/Citrix/MyBackupStore/discovery;on; StoreFrontStore
3 <!--NeedCopy-->
```

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.

Paramètres d'installation

Démarrer la protection des applications

- Commande : `startAppProtection`
- Description : démarre la protection des applications et offre une sécurité renforcée en protégeant les clients contre les programmes malveillants d'enregistrement de frappe et de capture d'écran.
- Exemple : `CitrixWorkspaceApp.exe startAppProtection`

Pour plus d'informations, consultez [Protection des applications](#).

Remarque :

Le commutateur `startAppProtection` remplace le commutateur `includeAppProtection`. Le commutateur `includeAppProtection` est obsolète. Pour plus d'informations, consultez [Fin de prise en charge](#).

Exclure les fichiers binaires de Citrix Enterprise Browser

- Commande : `InstallEmbeddedBrowser`
- Description : exclut les fichiers binaires de Citrix Enterprise Browser.
- Exemple : exécutez le commutateur `InstallEmbeddedBrowser=N` pour exclure la fonctionnalité de navigateur intégré.

Vous pouvez exclure les fichiers binaires de Citrix Enterprise Browser uniquement dans les cas suivants :

- Nouvelle installation
- Mise à niveau à partir d'une version qui n'inclut pas les fichiers binaires de Citrix Enterprise Browser.

Si votre version de l'application Citrix Workspace inclut les fichiers binaires de Citrix Enterprise Browser et que vous effectuez une mise à niveau vers la version 2002, les fichiers binaires de Citrix Enterprise Browser sont automatiquement mis à jour pendant la mise à niveau.

Spécifier un répertoire d'installation personnalisé

- Commande : `INSTALLDIR`
- Description : 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`.
- Exemple : `CitrixWorkspaceApp.exe INSTALLDIR=C:\custom path\Citrix`.

Remarque :

Le dossier **Program Files** est protégé par le système d'exploitation. Si vous souhaitez utiliser un dossier personnalisé autre que Program Files, assurez-vous que le dossier dispose des autorisations appropriées et qu'il est protégé.

Installer un ou plusieurs composants spécifiques

- Commande : `ADDLOCAL`
- Description : utilisez la clé `ADDLOCAL` pour installer un ou plusieurs composants spécifiques de l'application Citrix Workspace. À l'aide de cette clé, si vous installez des composants spécifiques, l'application Citrix Workspace installe tous les composants obligatoires par défaut.

Remarque :

Nous vous recommandons d'utiliser la clé `ADDLOCAL` uniquement si vous souhaitez installer des composants spécifiques de l'application Citrix Workspace. Par défaut, si aucun paramètre `ADDLOCAL` n'est spécifié, tous les composants pris en charge sont installés lors de l'installation de l'application Citrix Workspace.

Le tableau suivant répertorie les composants pris en charge par la clé `ADDLOCAL` :

Clé ADDLOCAL	Nom du composant	Description
<code>ReceiverInside</code>	Receiver	Fournit des services SDK d'espace de travail à Self-Service Plug-in.
<code>ICA_Client</code>	Moteur HDX	Ce composant gère le processus de lancement du fichier ou de la session ICA.
<code>BCR_Client</code>	Client BCR	Plug-in permettant de gérer la redirection du contenu de navigation.
<code>USB</code>	Client USB	Plug-in permettant de prendre en charge la redirection USB.
<code>DesktopViewer</code>	Client Desktop Viewer	Framework d'interface utilisateur pour bureau virtuel.
<code>AM</code>	AuthManager	Gestionnaire d'authentification : autorise l'utilisateur à accéder à l'application Citrix Workspace.
<code>SSON</code>	SSON	Composant Single Sign-on : prend en charge l'authentification unique.
<code>SELSERVICE</code>	Self-Service	Plug-in pour Citrix Workspace pour un lancement natif.
<code>WebHelper</code>	WebHelper	Assistance permettant de connecter le navigateur à l'application d'espace de travail native.
<code>CitrixEnterpriseBrowser</code>	Navigateur	Navigateur natif qui permet aux utilisateurs d'ouvrir des applications Web et SaaS depuis l'application Citrix Workspace de manière sécurisée.

Par exemple, à l'aide de la commande suivante, vous pouvez installer les composants mentionnés dans la commande :

```
1 CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,BCR_Client,USB,DesktopViewer,AM,SSON,SelfService,WebHelper,
```

```
CitrixEnterpriseBrowser
2 <!--NeedCopy-->
```

Remarque :

La fonction App Protection est installée par défaut. Par conséquent, `AppProtection` n'est plus une option valide pour ADDLOCAL.

Installer Citrix Casting

Important :

Pour l'application Citrix Workspace LTSR version 2402 et versions ultérieures, Citrix Casting ne peut pas être installé même avec la commande `IncludeCitrixCasting`. Pour utiliser cette fonctionnalité, vous devez utiliser une ancienne version de l'application Citrix Workspace. Pour plus d'informations, consultez la page [Fin de prise en charge](#).

- Commande : `IncludeCitrixCasting`
- Description : installe Citrix Casting pendant l'installation.

Pour plus d'informations sur Citrix Casting, consultez [Citrix Casting](#).

Paramètres des fonctionnalités HDX

Définir la redirection bidirectionnelle du contenu

- Commande : `ALLOW_BIDIRCONTENTREDIRECTION`
- Description : indique si la redirection bidirectionnelle du contenu du client vers l'hôte est activée. Pour plus d'informations, consultez la section [Paramètres de stratégie Redirection bidirectionnelle du contenu](#) de la documentation Citrix Virtual Apps and Desktops.

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
0 (valeur par défaut)	Indique que la redirection bidirectionnelle du contenu est désactivée.	<code>CitrixWorkspaceApp.exe</code> <code>ALLOW_BIDIRCONTENTREDIRECTION=0</code>
1	Indique que la redirection bidirectionnelle du contenu est activée.	<code>CitrixWorkspaceApp.exe</code> <code>ALLOW_BIDIRCONTENTREDIRECTION=1</code>

Définir Local App Access

- Commande : [FORCE_LAA](#)
- Description : indique que l'application Citrix Workspace est installée avec le composant Local App Access côté client. Installez l'application 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.

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
FORCE_LAA		
0 (valeur par défaut)	Indique que le composant Local App Access n'est pas installé.	<code>CitrixWorkspaceApp.exe FORCE_LAA =0</code>
1	Indique que le composant Local App Access côté client est installé.	<code>CitrixWorkspaceApp.exe FORCE_LAA =1</code>

Définir la fonctionnalité de redirection des adresses URL sur les machines utilisateur

- Commande : [ALLOW_CLIENTHOSTEDAPPSURL](#)
- Description : 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.

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
ALLOW_CLIENTHOSTEDAPPSURL		
0 (valeur par défaut)	Désactive la fonctionnalité de redirection des adresses URL sur les machines utilisateur.	<code>CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL =0</code>
1	Active la fonctionnalité de redirection des adresses URL sur les machines utilisateur.	<code>CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL =1</code>

Afficher des icônes pour des documents ou des fichiers

- Commande : `LEGACYFTAICONS`
- Description : spécifie si les icônes 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.

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
LEGACYFTAICONS		
False (valeur par défaut)	Affiche les icônes 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.	<code>CitrixWorkspaceApp.exe LEGACYFTAICONS=False</code>
True	N'affiche pas les icônes pour les documents ou les fichiers qui disposent d'associations de type de fichier avec des applications faisant l'objet d'une souscription.	<code>CitrixWorkspaceApp.exe LEGACYFTAICONS=True</code>

Préférences et paramètres de l'interface utilisateur

Spécifier le répertoire des raccourcis dans le menu Démarrer et sur le bureau

Valeur de la commande	Description	Nom du répertoire	Exemple
<code>CitrixWorkspaceApp.exe STARTMENUDIR</code>	Spécifie le répertoire des raccourcis dans le menu Démarrer.	Par défaut, toutes les applications apparaissent sous Démarrer > Tous les programmes . Vous pouvez spécifier le chemin d'accès relatif des raccourcis dans le dossier <code>Programs</code> .	Pour placer les raccourcis sous Démarrer > Tous les programmes > Workspace , spécifiez <code>STARTMENUDIR=Workspace</code> .
<code>CitrixWorkspaceApp.exe DESKTOPDIR</code>	Spécifie le répertoire des raccourcis sur le Bureau.	Vous pouvez spécifier le chemin d'accès relatif des raccourcis.	Pour placer les raccourcis sous Démarrer > Tous les programmes > Workspace , spécifiez <code>DESKTOPDIR=Workspace</code> .

Remarque :

Lorsque vous utilisez l'option `DESKTOPDIR`, définissez la clé `PutShortcutsOnDesktop` sur `True`.

Contrôler l'accès à l'interface en libre-service

- Commande : `SELFSEVICEMODE`
- Description : contrôle l'accès à l'interface utilisateur en libre-service de l'application Citrix Workspace.

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
<code>SELFSEVICEMODE</code>		
<code>True</code>	Indique que l'utilisateur a accès à l'interface utilisateur en libre-service.	<code>CitrixWorkspaceApp.exe SELFSEVICEMODE=True</code>

Valeur de la commande	Description	Exemple
SELFSEVICEMODE		
False	Indique que l'utilisateur n'a pas accès à l'interface utilisateur en libre-service.	<code>CitrixWorkspaceApp.exe SELFSEVICEMODE=False</code>

Contrôler le pré-lancement de session

- Commande : [ENABLEPRELAUNCH](#)
- Description : contrôle le pré-lancement de session. Pour plus d'informations, consultez la section [Temps de lancement des applications](#).

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
ENABLEPRELAUNCH		
True	Indique que le pré-lancement de session est activé.	<code>CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True</code>
False	Indique que le pré-lancement de session est désactivé.	<code>CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False</code>

Masquer l'option Raccourcis et reconnexion

- Commande : [DisableSetting](#)
- Description : 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](#).

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
DisableSetting		
0 (valeur par défaut)	Affiche les options Raccourcis et Reconnexion sur la page Préférences avancées.	<code>CitrixWorkspaceApp.exe DisableSetting=0</code>

Valeur de la commande		
DisableSetting	Description	Exemple
1	Affiche uniquement l'option Reconnexion sur la page Préférences avancées.	<code>CitrixWorkspaceApp.exe DisableSetting=1</code>
2	Affiche uniquement l'option Raccourcis sur la page Préférences avancées.	<code>CitrixWorkspaceApp.exe DisableSetting=2</code>
3	Les options Raccourcis et Reconnexion sont masquées sur la page Préférences avancées.	<code>CitrixWorkspaceApp.exe DisableSetting=3</code>

Activer le programme d'amélioration de l'expérience utilisateur (CEIP)

- Commande : [EnableCEIP](#)
- Description : indique votre participation au programme d'amélioration de l'expérience utilisateur (CEIP). Pour plus d'informations, veuillez consulter la section [CEIP \(programme d'amélioration de l'expérience du client\)](#).

Les valeurs possibles sont les suivantes :

Valeur EnableCEIPcommand	Description	Exemple
True (valeur par défaut)	Permet de participer au programme d'amélioration de l'expérience utilisateur (CEIP) de Citrix.	<code>CitrixWorkspaceApp.exe EnableCEIP=True</code>
False	Permet de désactiver le programme d'amélioration de l'expérience utilisateur (CEIP) de Citrix.	<code>CitrixWorkspaceApp.exe EnableCEIP=False</code>

Activer le suivi permanent

- Commande : [EnableTracing](#)
- Description : contrôle la fonction de **suivi permanent**.

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
EnableTracing		
True (valeur par défaut)	Active la fonction de suivi permanent .	<code>CitrixWorkspaceApp.exe EnableTracing=true</code>
False	Désactive la fonction de suivi permanent .	<code>CitrixWorkspaceApp.exe EnableTracing=false</code>

Spécifier le nom pour identifier la machine utilisateur

- Commande : `CLIENT_NAME`
- Description : spécifie le nom utilisé pour identifier la machine utilisateur sur le serveur.
- `<ClientName>` : spécifie le nom utilisé pour identifier la machine utilisateur sur le serveur. Le nom par défaut est `%COMPUTERNAME%`.
- Exemple : `CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%`.

Définir le nom du client comme nom de la machine

- Commande : `ENABLE_DYNAMIC_CLIENT_NAME`
- Description : autorise l'utilisation d'un nom de client identique au nom de machine. Lorsque vous modifiez le nom de machine, le nom de client change en conséquence.

Les valeurs possibles sont les suivantes :

Valeur de la commande EN- ABLE_DYNAMIC_CLIENT_NAME	Description	Exemple
Oui (valeur par défaut)	Autorise l'utilisation d'un nom de client identique au nom de machine.	<code>CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=Yes</code>
Non	N'autorise pas l'utilisation d'un nom de client identique au nom de machine. Spécifiez une valeur pour la propriété <code>CLIENT_NAME</code> .	<code>CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No</code>

Paramètres d'authentification

Inclure l'authentification unique (Single Sign-On)

- Commande : `/includeSSON`
- Description : requiert une installation en tant qu'administrateur. Indique que l'application Citrix Workspace est installée avec le composant d'authentification unique (Single Sign-On). Consultez la section [Authentification pass-through au domaine](#) pour plus d'informations.
- Exemple : `CitrixWorkspaceApp.exe /includeSSON`

Remarque :

La commande `includeSSON` prend uniquement en charge la nouvelle installation de l'application Citrix Workspace.

Activer l'authentification unique (Single Sign-On)

- Commande : `ENABLE_SSON`
- Description : active l'authentification Single Sign-On lorsque l'application Citrix Workspace est installée avec la commande `/includeSSON`. Pour plus d'informations, consultez la section [Authentification pass-through au domaine](#).

Les valeurs possibles sont les suivantes :

Valeur de la commande	Description	Exemple
ENABLE_SSON		
Oui (valeur par défaut)	Indique que l'authentification unique est activée.	<code>CitrixWorkspaceApp.exe ENABLE_SSON=Yes</code>
Non	Indique que l'authentification unique est désactivée.	<code>CitrixWorkspaceApp.exe ENABLE_SSON=No</code>

Désinstaller l'application Citrix Workspace

Désinstaller à l'aide du programme de désinstallation Windows

Vous pouvez désinstaller l'application Citrix Workspace pour Windows à partir du **Panneau de configuration**. Pour plus d'informations, consultez la section [Désinstaller l'application Citrix Workspace pour Windows](#).

Remarque :

Lors de l'installation de l'application Citrix Workspace, vous recevez une invite pour désinstaller

le package Citrix HDX RTME. Cliquez sur **OK** pour poursuivre la désinstallation.

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

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

```
1 CitrixWorkspaceApp.exe /uninstall
2 <!--NeedCopy-->
```

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

```
1 CitrixWorkspaceApp.exe /silent /uninstall
2 <!--NeedCopy-->
```

Remarque :

Le programme d'installation de l'application Citrix Workspace ne contrôle pas les clés de registre liées à l'objet de stratégie de groupe. Elles sont donc conservées après la désinstallation. Si vous trouvez des entrées, mettez-les à jour à l'aide de [gpedit](#) ou supprimez-les manuellement.

Dépannage

Error codes

- Pour les codes d'erreur liés au programme d'installation, consultez les [messages d'erreur MsiExec.exe et InstMsi.exe](#).
- Pour les codes d'erreur liés au système, consultez [Codes d'erreur système](#).

Emplacement du journal du programme d'installation

Par défaut, les journaux du programme d'installation se trouvent dans l'emplacement suivant :

	Dossier du journal d'installation	Type d'installation
Administrateur	Pour 64 bits : C:\Program Files (x86)\Citrix\Logs ; 32 bits : C:\Program Files\Citrix\ICA Client	Installation par système
Utilisateur	%USERPROFILE%\AppData\Local\Citrix\Logs	Installation par utilisateur

Remarque :

TrolleyExpress est remplacé par CWAInstaller-`<date and timestamp>`. Par exemple, le journal est enregistré sous `C:\Program Files (x86)\Citrix\Logs\CTXWorkspaceInstallLogs-20231225-093441`.

Dépannage

Error codes

- Pour les codes d'erreur liés au programme d'installation, consultez les [messages d'erreur MsiExec.exe et InstMsi.exe](#).
- Pour les codes d'erreur liés au système, consultez [Codes d'erreur système](#).

Emplacement du journal du programme d'installation

Par défaut, les journaux du programme d'installation se trouvent dans l'emplacement suivant :

	Dossier du journal d'installation	Type d'installation
Administrateur	Pour 64 bits : C:\Program Files (x86)\Citrix\Logs ; 32 bits : C:\Program Files\Citrix\ICA Client	Installation par système
Utilisateur	%USERPROFILE%\AppData\Local\Citrix\Logs	Installation par utilisateur

Réinitialiser l'application Citrix Workspace

La réinitialisation de l'application Citrix Workspace restaure les paramètres par défaut.

Les éléments suivants sont réinitialisés lorsque vous réinitialisez l'application Citrix Workspace :

- Tous les comptes et magasins configurés.
- Applications fournies par le Self-Service Plug-in, leurs icônes et leurs clés de registre.
- Associations de types de fichiers créées par le Self-Service Plug-in.
- Fichiers mis en cache et mots de passe enregistrés.
- Paramètres de registre par utilisateur.
- Installations par machine et leurs paramètres de registre.
- Paramètres de registre de Citrix Gateway pour l'application Citrix Workspace.

Exécutez la commande suivante à partir de l'interface de ligne de commande pour réinitialiser l'application Citrix Workspace :

```
1 "C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe  
  " -cleanUser  
2 <!--NeedCopy-->
```

Pour effectuer une réinitialisation silencieuse, utilisez la commande suivante :

```
1 "C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe  
  " /silent -cleanUser  
2 <!--NeedCopy-->
```

Remarque :

Utilisez le U majuscule dans le paramètre.

La réinitialisation de l'application Citrix Workspace n'a aucune incidence sur ce qui suit :

- Installation d'une application Citrix Workspace ou d'un plug-in.
- Paramètres de verrouillage ICA par machine.
- Configurations de modèles d'administration d'objets de stratégie de groupe (GPO) pour l'application Citrix Workspace.

Déployer

April 22, 2024

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](#).
- Avant de lancer Workspace Web, installez l'application Citrix Workspace pour Windows. 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](#).
- Utilisez Microsoft Endpoint Manager (Intune). Pour plus d'informations, consultez [Déployer l'application Citrix Workspace dans Microsoft Endpoint Manager \(Intune\)](#).

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 en fonction de votre structure organisationnelle. 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.

Pour plus d'informations sur la création d'une unité d'organisation dans Azure Active Directory, consultez [Créer une unité d'organisation \(OU\) dans un domaine géré Azure Active Directory Domain Services](#).

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** : spécifie le partage réseau contenant les packs du programme d'installation de l'application Citrix Workspace. 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** : 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](#).

Type de déploiement	Pour déployer	Pour supprimer
Par ordinateur	CheckAndDeployWorkspacePerMachineStoreWorkScript.bat	CheckAndRemoveWorkspacePerMachineStoreWorkScript.bat
Par utilisateur	CheckAndDeployWorkspacePerUserStoreWorkScript.bat	CheckAndRemoveWorkspacePerUserStoreWorkScript.bat

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**, copiez le script approprié dans le dossier affiché et fermez la boîte de dialogue.
5. 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 attribuées 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

Workspace pour Web vous permet d'accéder aux magasins StoreFront via un navigateur depuis une page Web.

Avant de vous connecter à une application à partir d'un navigateur, procédez comme suit :

1. Installez l'application Citrix Workspace pour Windows.
2. Déployer l'application Citrix Workspace à partir de Workspace pour Web

Si Workspace pour Web détecte qu'aucune version compatible de l'application Citrix Workspace n'est présente, une invite s'affiche. L'invite vous demande de télécharger et d'installer l'application Citrix Workspace pour Windows.

Remarque :

L'espace de travail pour le Web ne prend pas en charge la découverte de compte basée sur une adresse e-mail.

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 [Configurer StoreFront 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.

Vous pouvez déployer l'application Citrix Workspace à l'aide du SCCM à l'aide des quatre parties suivantes :

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 /silent /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** : saisissez le numéro de version de l'application Citrix Workspace actuelle

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 configuré. Vous pouvez également programmer ou installer à la demande. L'état de l'installation s'affiche dans le **Centre logiciel** après le démarrage de l'installation.

Création de regroupements de périphériques

1. Démarrez la console **Configuration Manager**, cliquez sur **Ressources et Conformité > Présentation > Périphériques**.
2. Cliquez avec le bouton droit de la souris sur **Regroupements de périphériques** et sélectionnez **Créer un regroupement de périphériques**.
L'Assistant **Création d'un regroupement de périphériques** s'affiche.
3. Dans le panneau **Général**, tapez le **nom** du périphérique et cliquez sur **Parcourir** pour 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 :

La configuration de l'application Citrix Workspace à l'aide du SCCM peuvent échouer lorsque l'attribut **MSIRESTARTMANAGERCONTROL** est défini sur **False**.

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.

Déployer l'application Citrix Workspace dans Microsoft Endpoint Manager (Intune)

Pour déployer l'application Citrix Workspace (application Win 32 native) dans Microsoft Endpoint Manager (Intune), procédez comme suit :

1. Créez les dossiers suivants :
 - Un dossier pour stocker tous les fichiers sources nécessaires à l'installation, par exemple, `C:\CitrixWorkspace_Executable`.
 - Un dossier pour le fichier de sortie. Les fichiers de sortie se trouvent dans un fichier `.intunewin`, par exemple, `C:\Intune_CitrixWorkspaceApp`.
 - Un dossier pour l'outil Microsoft Win32 Content Prep Tool, par exemple, `C:\Intune_WinAppTool`. Cet outil permet de convertir les fichiers d'installation au

format `.intunewin`. Vous pouvez télécharger l'outil de packaging à partir de [Microsoft-Win32-Content-Prep-Tool](#).

2. Convertissez tous les fichiers sources nécessaires à l'installation en un fichier `.intunewin` :

- a) Lancez l'invite de commande et accédez au dossier où se trouve Microsoft Win32 Content Prep Tool, par exemple, `C:\Intune_WinAppTool`.
- b) Exécutez la commande `IntuneWinAppUtil.exe`.
- c) À l'invite, saisissez les informations suivantes :

- **Dossier source** : `C:\CitrixWorkspace_Executable`
 - **Fichier d'installation** : `CitrixWorkspaceApp.exe`
 - **Dossier de sortie** : `C:\Intune_CitrixWorkspaceApp`
- Le fichier `.intunewin` est créé.

3. Ajoutez le package à Microsoft Endpoint Manager (Intune) :

- a) Ouvrez la console Microsoft Endpoint Manager (Intune) : <https://endpoint.microsoft.com/#home>.

Remarque :

Les instructions suivantes ne peuvent être exécutées que sur <https://endpoint.microsoft.com/#home>. Vous pouvez également ajouter le package via <https://portal.azure.com>.

- b) Cliquez sur **Applications > Application Windows**, puis sur **+Ajouter**.
- c) Sélectionnez **Application Windows (Win 32)** dans la liste déroulante **Type d'application**.
- d) Cliquez sur **Fichier de package d'application**, recherchez le fichier `CitrixWorkspaceApp.intunewin`, puis cliquez sur **OK**.
- e) Cliquez sur **Informations sur l'application** et renseignez les informations obligatoires, Nom, Description et Éditeur, puis cliquez sur **OK**.
- f) Cliquez sur **Programme**, saisissez les informations suivantes, puis cliquez sur **OK** :

- Commande d'installation : `CitrixWorkspaceApp.exe /silent`
- Commande de désinstallation : `CitrixWorkspaceApp.exe /uninstall`
- Comportement d'installation : Système

- g) Cliquez sur **Exigence**, saisissez les informations requises, puis cliquez sur **OK**.

Remarque :

Sélectionnez x64 et x32 dans la liste Architecture du système d'exploitation. La ver-

sion du système d'exploitation peut être toute version prenant en charge Win 1607 et versions ultérieures.

- h) Cliquez sur **Règles de détection**, sélectionnez **Configuration manuelle des règles de détection** sous **Format des règles**, puis cliquez sur **OK**.
- i) Cliquez sur **Ajouter**, sélectionnez le **Type de règle** requis, puis cliquez sur **OK**.
 - Si le **Type de règle** est défini sur **Fichier**, le chemin peut être, par exemple, `C:\Program Files (x86)\Citrix\ICA Client\wfica32.exe`.
 - Si le **Type de règle** est défini sur **Registre**, entrez `HKEY_CURRENT_USER\Software\Citrix` sous **Chemin** et sélectionnez **La clé existe** sous **Méthode de détection**.
- j) Cliquez sur **Codes de retour**, vérifiez si les codes de retour par défaut sont valides, puis cliquez sur **OK**.
- k) Cliquez sur **Ajouter** pour ajouter l'application à Intune.

4. Vérifiez si le déploiement a réussi :

- a) Cliquez sur **Accueil > Applications > Windows**.
- b) Cliquez sur **État d'installation de l'appareil**.

L'état de l'appareil indique le nombre d'appareils sur lesquels l'application Citrix Workspace est installée.

Configuration du magasin

April 22, 2024

Magasin

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

Un **magasin** regroupe les applications et les bureaux disponibles pour un utilisateur en un seul endroit. Un utilisateur peut avoir plusieurs magasins et passer d'un magasin à l'autre selon ses besoins. Un administrateur fournit l'URL du magasin contenant des ressources et des paramètres préconfigurés. Vous pouvez accéder à ces magasins via l'application Citrix Workspace.

Types de magasins

Vous pouvez ajouter les types de magasins suivants dans l'application Citrix Workspace : Workspace, StoreFront, Citrix Gateway Store et Magasin Web personnalisé.

Workspace

Citrix Workspace est un magasin d'applications d'entreprise basé sur le cloud qui fournit un accès sécurisé et unifié aux applications, aux bureaux et au contenu (ressources) depuis n'importe où et sur n'importe quel appareil. Ces ressources peuvent être des instances Citrix DaaS, des applications de contenu, des applications locales et mobiles, des applications SaaS et Web, ainsi que des applications de navigateur. Pour plus d'informations, consultez la section [Vue d'ensemble de Citrix Workspace](#).

StoreFront

StoreFront est un magasin d'applications d'entreprise sur site qui regroupe les applications et les bureaux des sites Citrix Virtual Apps and Desktops en un seul magasin facile à utiliser pour les utilisateurs.

Pour plus d'informations, consultez la documentation de [StoreFront](#).

Citrix Gateway Store

Configurez Citrix Gateway pour permettre aux utilisateurs de se connecter depuis l'extérieur du réseau interne. Par exemple, les utilisateurs qui se connectent à partir d'Internet ou à partir d'emplacements distants.

Magasins Web personnalisés

Cette fonctionnalité permet d'accéder au magasin Web personnalisé de votre organisation à partir de l'application Citrix Workspace pour Windows. Pour utiliser cette fonctionnalité, l'administrateur doit ajouter le domaine ou le magasin Web personnalisé à la liste des URL autorisées dans Global App Configuration Service.

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

Vous pouvez fournir l'URL du magasin Web personnalisé sur l'écran **Ajouter un compte** dans l'application Citrix Workspace. Le magasin Web personnalisé s'ouvre dans la fenêtre de l'application Citrix Workspace native.

Pour supprimer le magasin Web personnalisé, accédez à **Comptes > Ajouter ou supprimer des comptes**, sélectionnez l'URL du magasin Web personnalisé, puis cliquez sur **Supprimer**.

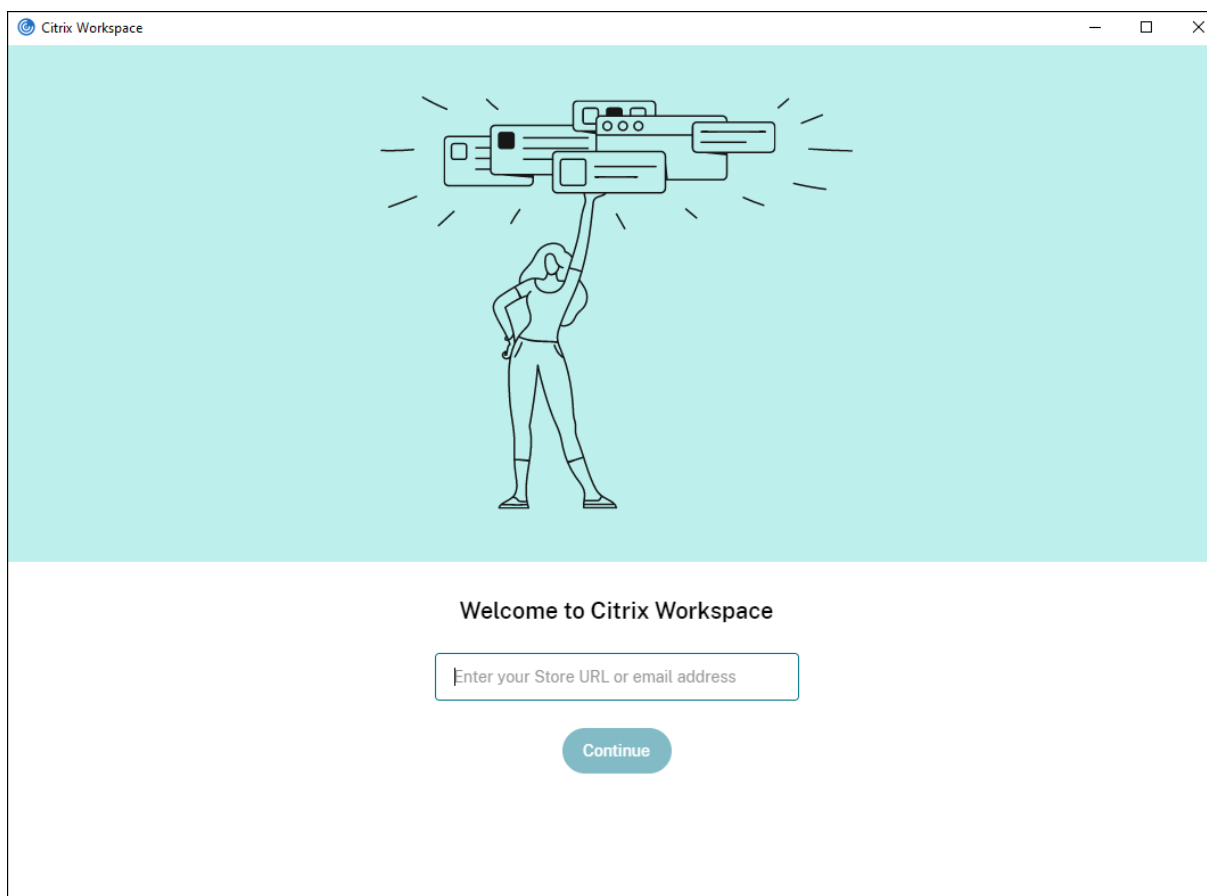
Ajouter l'URL du magasin à l'application Citrix Workspace

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 fournissant aux utilisateurs des informations de compte à entrer manuellement
- En configurant la découverte de compte basée sur une adresse e-mail
- Ajouter un magasin via l'interface de ligne de commande
- Fichier de provisioning
- En utilisant le modèle d'administration d'objet de stratégie de groupe

Fournir aux utilisateurs des informations de compte à entrer manuellement

Une fois l'installation de l'application Citrix Workspace réussie, l'écran suivant s'affiche. Les utilisateurs doivent saisir une adresse e-mail ou une adresse de serveur pour accéder aux applications et aux bureaux. 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 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 vous connecter à un magasin Workspace, fournissez l'URL de Workspace.
- Pour les connexions à un magasin StoreFront, indiquez l'adresse URL de ce serveur. Par exemple : <https://servername.company.com>.
- Pour les connexions établies via Citrix Gateway, déterminez d'abord si l'utilisateur a accès à tous les magasins configurés ou uniquement au magasin avec accès distant 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 :

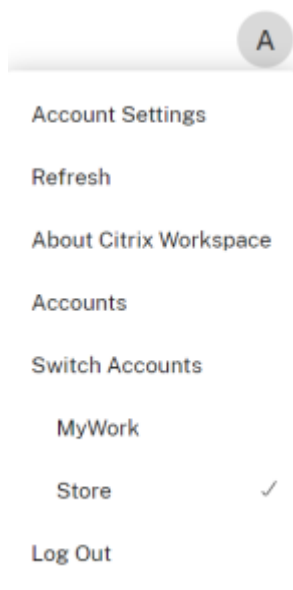
CitrixGatewayFQDN?MyStoreName :

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
- * server2.com?HRApps pour accéder **HRApps**

La fonctionnalité **CitrixGatewayFQDN?MyStoreName** 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.

Une fois l'application Citrix Workspace configurée avec l'URL du magasin, le compte peut être géré à partir de l'option **Comptes** du menu de profil.



Sur les machines clientes configurées pour l'authentification par proxy, si les informations d'identification de proxy ne sont pas stockées dans le **Gestionnaire d'informations d'identification Windows**, une invite d'authentification s'affiche, vous demandant d'entrer les informations d'identification de proxy. L'application Citrix Workspace enregistre ensuite les informations d'identification du serveur proxy dans le **Gestionnaire d'informations d'identification Windows**. Cela se traduit par une expérience de connexion transparente car vous n'avez pas besoin d'enregistrer manuellement vos informations d'identification dans le **Gestionnaire d'informations d'identification Windows** avant d'accéder à l'application Citrix Workspace.

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 SRV de DNS. L'application invite ensuite l'utilisateur à se connecter pour accéder aux applications et bureaux virtuels.

Pour configurer la découverte de compte basée sur une adresse e-mail pour les magasins Citrix Workspace, reportez-vous à la section de [mise en route](#) dans la documentation Global App Configuration Service.

Pour configurer la découverte de compte basée sur une adresse e-mail pour les magasins Citrix StoreFront ou Citrix Gateway, consultez la section [Configuration de la découverte de compte basée sur une adresse e-mail](#).

Ajouter un magasin via l'interface de ligne de commande

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

Pour plus d'informations, consultez la section [Liste des paramètres de ligne de commande](#).

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 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.

Utiliser le modèle d'administration d'objet de stratégie de groupe Pour ajouter ou spécifier un Citrix StoreFront ou 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. Sélectionnez l'option **Activé** et cliquez sur **Afficher**. Si vous activez ce paramètre de stratégie, vous pouvez entrer une liste de comptes StoreFront et l'adresse URL de NetScaler Gateway.
5. Saisissez l'URL dans le champ **Valeur**.

6. Spécifiez l'URL du magasin utilisée avec l'application Citrix Workspace :

```
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'URL du magasin est au format suivant /Citrix/Store/Discovery. Pour obtenir l'URL, exportez un fichier de provisioning de StoreFront, ouvrez-le dans Bloc-notes et copiez l'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.
- descriptionmagasin : description du magasin, telle que Magasin des applications RH.

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

```
Exemple : STORE0= HRStore;https://ag.mycompany.com#Storename;On;  
Store
```

où #Store name est le nom du magasin derrière Citrix Gateway.

Remarque :

- L'URL du magasin Citrix Gateway doit figurer en premier dans la liste (paramètre STORE0).
- Dans une configuration comportant plusieurs magasins, une seule configuration d'URL de magasin Citrix Gateway est autorisée.
- 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.
- Le paramètre /Discovery n'est pas requis lors de la spécification d'une URL de magasin Citrix Gateway.

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 après le redémarrage de l'application. Aucune réinitialisation n'est nécessaire.

Remarque :

L'application Citrix Workspace version 1808 ou ultérieure ne nécessite pas de réinitialisation lors d'une nouvelle installation. Dans le cas d'une mise à niveau vers la version 1808 ou une version ultérieure, vous devez réinitialiser l'application Citrix Workspace pour que les modifications prennent effet.

Limitations :

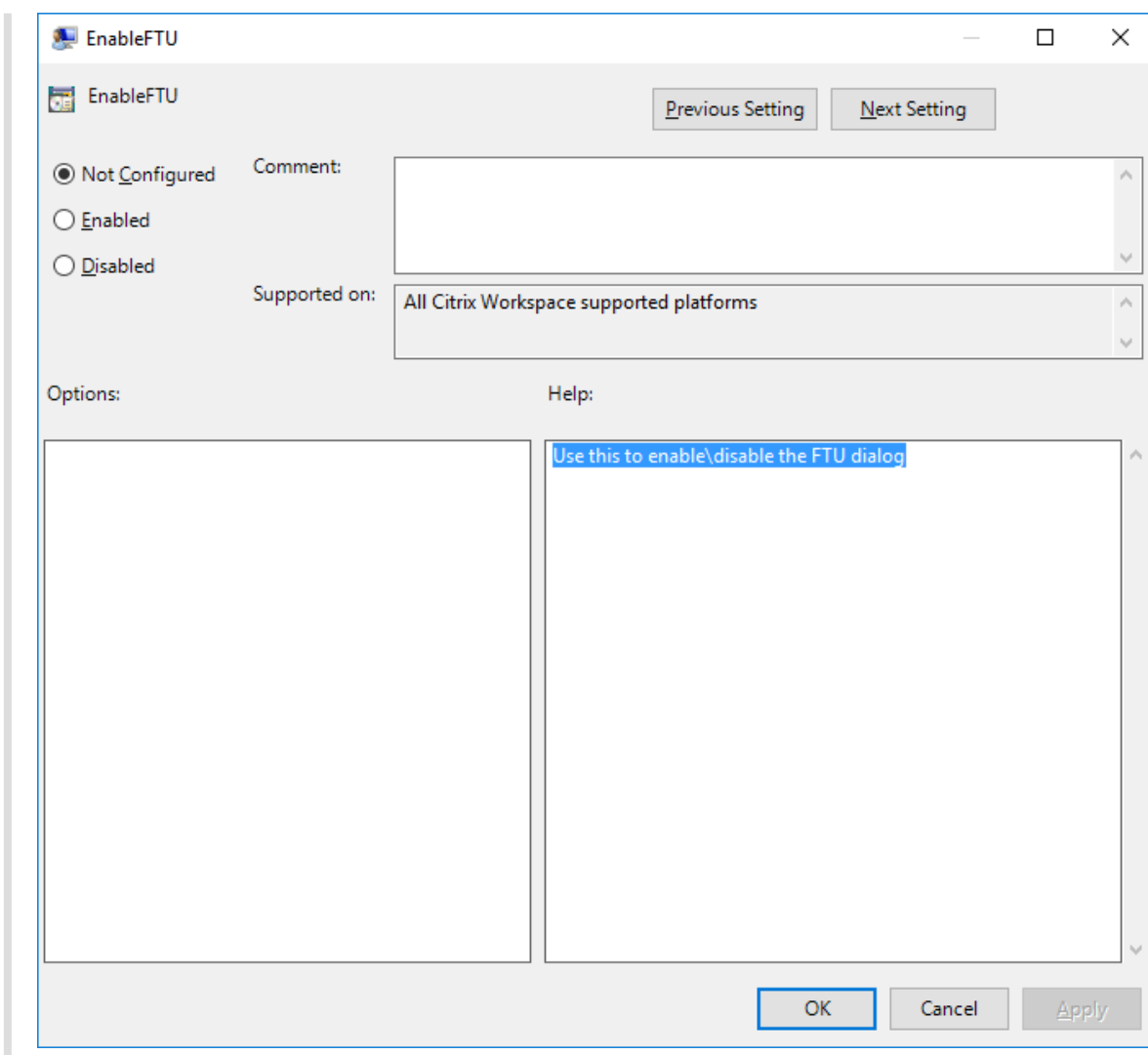
- L'URL de Citrix Gateway doit être indiquée en premier, suivie de l'adresse ou des adresses URL de StoreFront.
- Il n'est pas possible de spécifier plusieurs adresses URL de Citrix Gateway.

Remarque :

Les utilisateurs peuvent également accéder au magasin via un navigateur Web. Les utilisateurs peuvent se connecter au magasin Citrix à partir d'un navigateur Web et lancer une application ou un bureau virtuel à partir du Web. Le lancement de l'application ou du bureau virtuel utilise les fonctionnalités de l'application Citrix Workspace installée en mode natif.

Dans ce cas, il peut être souhaitable de masquer l'invite **Ajouter un compte** pour les utilisateurs. Pour cela, vous pouvez utiliser le paramètre suivant :

- **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.



Résolution des noms 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 sur le serveur.

Par défaut, la résolution de nom DNS est désactivée sur le serveur et activée 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 générer des problèmes sérieux nécessitant la réinstallation du système d'exploitation. Nous ne pouvons 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. Effectuez une copie de sauvegarde de votre 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.

Connecter

L'application Citrix Workspace permet aux utilisateurs d'accéder en libre-service et en toute sécurité à des applications et bureaux virtuels, et d'accéder à la demande à des applications Windows, Web et SaaS (Logiciel en tant que service). L'accès utilisateur est géré par Citrix StoreFront ou les pages Web créées avec l'Interface Web.

Pour se connecter à des ressources à l'aide de l'interface utilisateur Citrix Workspace

La page d'accueil de l'application Citrix Workspace affiche les applications et les bureaux virtuels mis à la disposition des utilisateurs en fonction de leurs paramètres de compte (c'est-à-dire, le serveur auquel ils se connectent) et les paramètres configurés par les administrateurs Citrix Virtual Apps and Desktops ou Citrix DaaS. À l'aide de la page **Préférences > Comptes**, vous pouvez configurer l'URL d'un serveur StoreFront ou, si la découverte de compte par e-mail est configurée, en entrant votre adresse e-mail.

Après la connexion à un magasin, le mode libre-service affiche les onglets **Favoris**, **Bureaux** et **Applications**. Pour lancer une session, cliquez sur l'icône appropriée. Pour ajouter une icône aux **Favoris**, cliquez sur l'icône ... et sélectionnez **Ajouter aux Favoris**.

Migration de l'URL de StoreFront vers Workspace

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

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

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

Pour activer cette fonctionnalité, effectuez les opérations suivantes :

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

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://storefront.acme.com:443",
6     "migrationUrl": [
7       {
8
9         "url": "https://sampleworkspace.cloud.com:443",
10        "storeFrontValidUntil": "2023-05-01"
11      }
12    ]
13  ]
14 }
15 ,
16 "settings": {
17
18   "name": "Productivity Apps",
19   "description": "Provides access StoreFront to Workspace Migration"
20 ,
```

```
20 "useForAppConfig": true,  
21 "appSettings": {  
22  
23   "windows": [  
24     {  
25  
26       "category": "root",  
27       "userOverride": false,  
28       "assignmentPriority": 0,  
29       "assignedTo": [  
30         "AllUsersNoAuthentication"  
31       ],  
32       "settings": [  
33         {  
34  
35           "name": "Hide advanced preferences",  
36           "value": false  
37         }  
38  
39       ]  
40     }  
41  
42   ]  
43 }  
44  
45 }  
46  
47 }  
48  
49  
50 <!--NeedCopy-->
```

Remarque :

Si vous configurez la charge utile pour la première fois, utilisez **POST**.

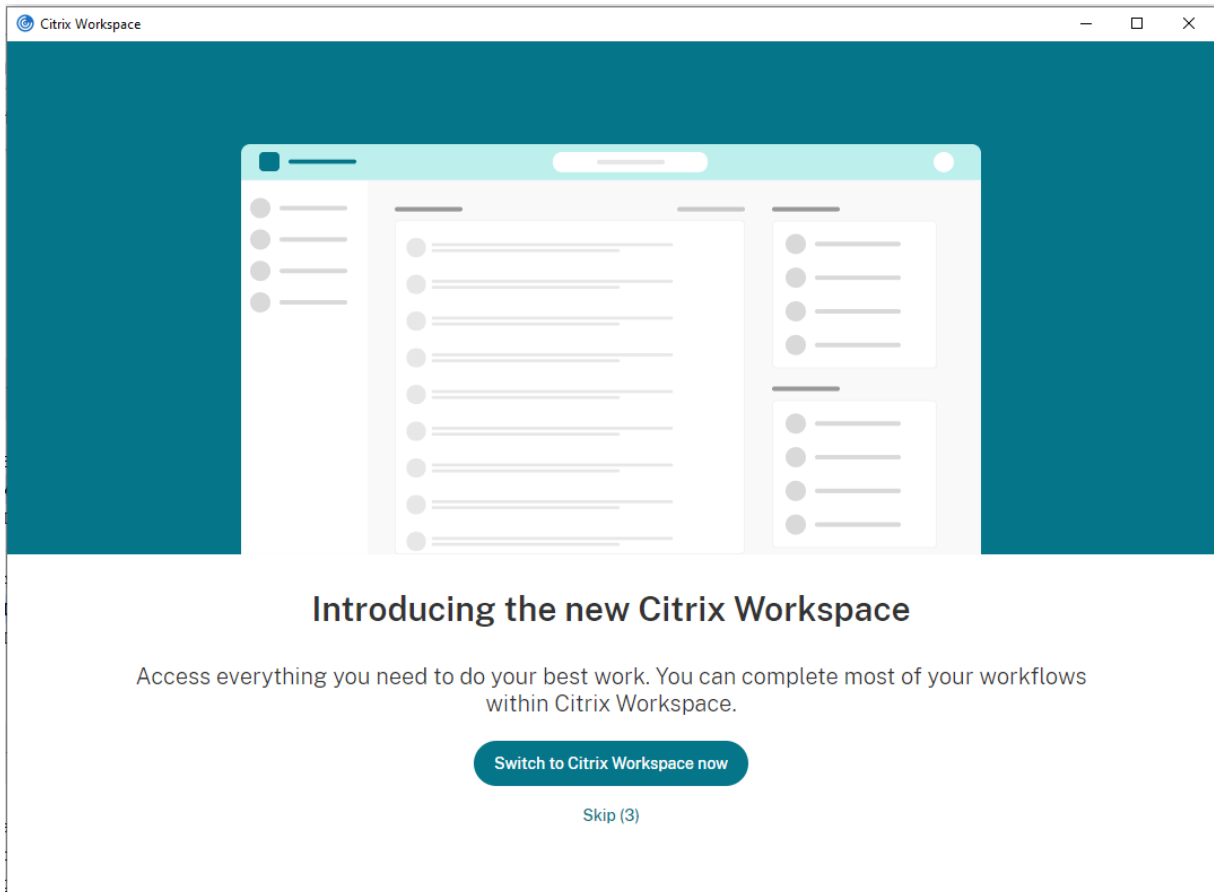
Si vous modifiez la configuration de la charge utile existante, utilisez **PUT** et assurez-vous que vous disposez de la charge utile comprenant tous les paramètres pris en charge.

3. Spécifiez l'URL StoreFront `storefront.com` comme valeur du champ **URL** dans la section **serviceURL**.
4. Configurez l'URL Workspace `xyz.cloud.com` dans la section **migrationUrl**.
5. Utilisez **storeFrontValidUntil** pour définir la chronologie de la suppression du magasin Store-Front de l'application Citrix Workspace. Ce champ est facultatif. Vous pouvez définir la valeur suivante en fonction de vos besoins :
 - Date de validité au format (AAAA-MM-JJ)

Remarque :

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

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



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

Prise en charge de la détection des applications locales dans l'application Citrix Workspace

À partir de la version 2112.1, les administrateurs peuvent configurer la détection et l'énumération des applications installées localement dans l'application Citrix Workspace. Vous pouvez configurer cette fonctionnalité avec Global App Configuration Service. Pour plus d'informations sur la configuration de cette fonctionnalité, consultez [Global App Configuration Service](#).

Cette fonctionnalité est idéale pour les appareils exécutés en mode kiosque et pour les applications qui ne peuvent pas être virtualisées dans Citrix Workspace.

Gestion des mises à jour et des plugins

April 22, 2024

Cette section décrit les éléments suivants :

- [Mises à jour](#)
- [Gestion des plugins](#)

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](#). Pour plus d'informations sur l'installation, reportez-vous à la section [Installation et désinstallation](#).

Mise à jour automatique

Lorsqu'une nouvelle version de l'application Citrix Workspace est disponible, 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.
- 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. Une notification s'affiche lorsque des mises à jour HDX RTME sont disponibles sur la version LTSR et la version actuelle de l'application Citrix Workspace.
- À partir de la version 2105, les chemins d'accès du 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 plus d'informations sur la journalisation, consultez la section [Collecte de journaux](#).
- 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**. L'option **Rechercher les mises à jour** est disponible sur les instances de l'application Citrix Workspace installées par l'utilisateur et celles installées par l'administrateur.
- Vous pouvez également effectuer une mise à jour automatique lorsque la configuration automatique du proxy (PAC) et la détection WPAD (Web Proxy Auto-Discovery Protocol) sont activées. Cela n'est pas pris en charge lorsque le proxy exige des informations d'identification pour l'authentification.
- Si une suite de chiffrement non EDCHE est ajoutée, Citrix Workspace ne peut pas accéder au serveur de mise à jour automatique Citrix et l'erreur suivante apparaît lors de la mise à jour automatique :

Impossible de se connecter au serveur

Redémarrez l'application Citrix Workspace pour Windows après une mise à jour manuelle ou automatique.

Vous pouvez vérifier la version actuelle de l'application Citrix Workspace installée sur votre appareil via les **préférences avancées** ou consulter le registre **DisplayVersion** depuis `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\CitrixOnlinePluginPackWeb`.

Pour consulter la version dans les **préférences avancées** :

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

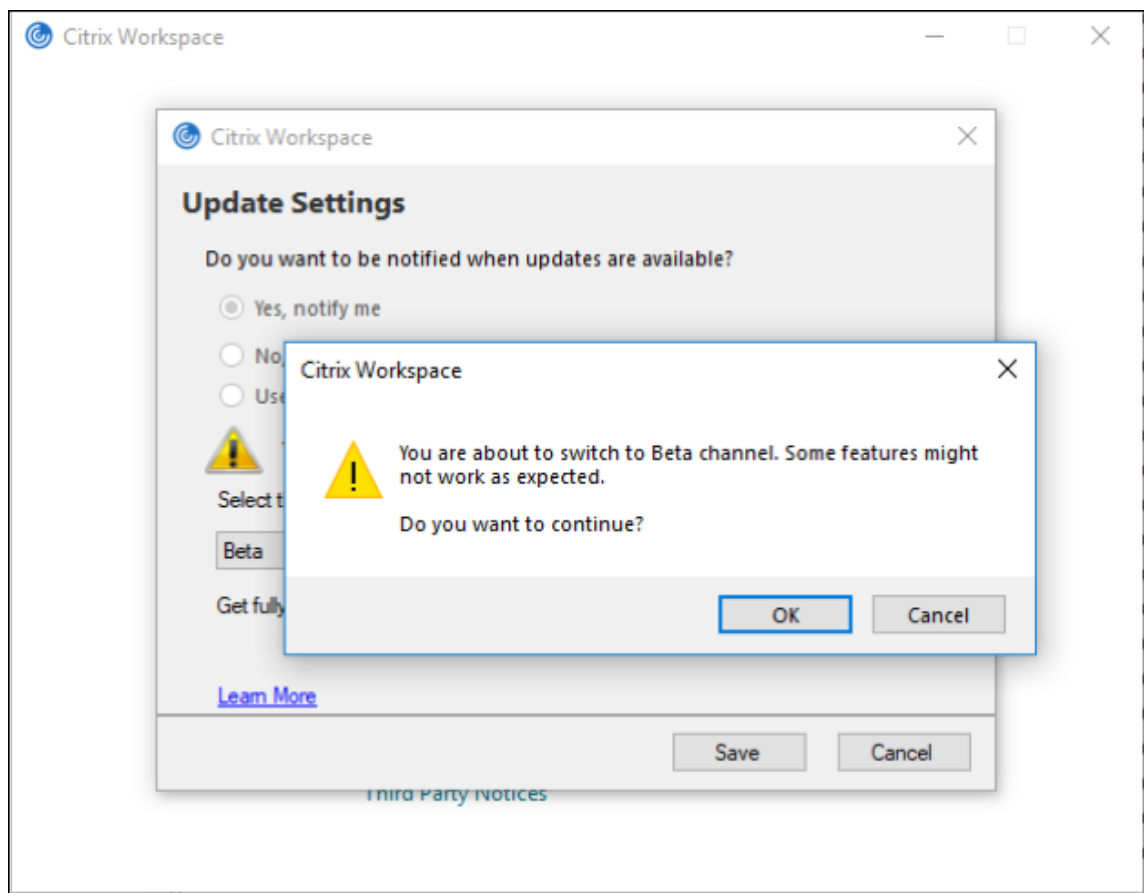
La version de l'application Citrix Workspace s'affiche dans la section **À propos de**.

Installation du programme Bêta de l'application Citrix Workspace

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

1. Ouvrez l'application Citrix Workspace à partir de la barre d'état système.
2. Accédez à **Préférences avancées > Mises à jour Citrix Workspace**.
3. Sélectionnez **Bêta** dans la liste déroulante, lorsque la version Bêta est disponible, puis cliquez sur **Enregistrer**.

Une fenêtre de notification apparaît.



4. Cliquez sur **OK** pour effectuer la mise à jour vers la version Bêta.

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

1. Ouvrez l'application Citrix Workspace à partir de la barre d'état système.
2. Accédez à **Préférences avancées > Mises à jour Citrix Workspace**.
3. Sur l'écran **Paramètres de mise à jour**, sélectionnez **Version** dans la liste déroulante du canal de mise à jour, puis cliquez sur **Enregistrer**.

Remarque :

- Si de nouvelles mises à jour sont disponibles, une notification de mise à jour automatique s'affiche.
- Les versions Bêta sont disponibles pour que les clients puissent effectuer leurs tests dans leurs environnements hors production ou de production limitée, et partager leurs commentaires. Citrix n'offre pas de support pour les versions Bêta, mais accepte les [commentaires](#) pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance. Il est conseillé de ne pas déployer de versions bêta dans les environnements de production.

Prise en charge de la mise à jour automatique de l'application Citrix Workspace sur le VDA

À partir de l'application Citrix Workspace pour Windows version 2209, vous pouvez activer la fonctionnalité de mise à jour automatique sur le VDA. Pour activer cette fonctionnalité, vous devez créer la valeur de registre suivante :

Sur une machine 32 bits :

- Clé de registre : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\AutoUpdate
- Valeur de registre : AllowAutoUpdateOnVDA
- Type de registre : REG_SZ
- Données du registre : True

Sur une machine 64 bits :

- Clé de registre : HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\AutoUpdate
- Valeur de registre : AllowAutoUpdateOnVDA
- Type de registre : REG_SZ
- Données du registre : True

Contrôle de la version à mise à jour automatique

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

Les administrateurs peuvent contrôler la version en définissant la version dans la propriété `maximumAllowedVersion` dans Global App Config Service.

Exemple de fichier JSON dans Global App Config Service :

```
1 {
2
3   "category": "AutoUpdate",
4   "userOverride": false,
5   "assignedTo": [
6     "AllUsersNoAuthentication"
7   ],
8   "settings": [
9     {
10
11       "name": "Auto Update plugins settings",
12       "value": [
13         {
14
15           "pluginSettings": {
16
17             "upgradeToLatest": false,
18             "deploymentMode": "InstallAndUpdate",
19             "stream": "Current",
20             "maximumAllowedVersion": "23.03.0.49",
21             "minimumAllowedVersion": "0.0.0.0",
22             "delayGroup": "Fast"
23           }
24         },
25         {
26           "pluginName": "WorkspaceApp",
27           "pluginId": "1CDF566D-B2C7-47CA-802F-6283C862E1D6"
28         }
29       ]
30     }
31   ]
32 }
33
34
35
36 <!--NeedCopy-->
```

Lorsque la version est définie, l'application Citrix Workspace sur l'appareil de l'utilisateur est automatiquement mise à jour vers la version spécifiée dans la propriété `maximumAllowedVersion`.

Remarques :

- Actuellement, tous les paramètres mentionnés dans le fichier JSON précédent sont obligatoires. Vous devez fournir des valeurs pour le paramètre `upgradeToLatest` et le paramètre `maximumAllowedVersion` en fonction des besoins de votre organisation. Toutefois, pour les autres paramètres, vous pouvez utiliser des valeurs similaires à celles

du fichier JSON d'exemple.

- Pour avoir accès au contrôle de la version de mise à jour automatique, le paramètre `upgradeToLatest` de Global App Config Service doit être défini sur « false ». Si le paramètre est défini sur « true », `maximumAllowedVersion` sera ignoré.
- Ne modifiez pas la valeur de `pluginId` car elle est mappée à l'application Citrix Workspace.
- Si l'administrateur n'a pas configuré la version dans Global App Config Service, l'application Citrix Workspace est mise à jour vers la dernière version disponible par défaut.

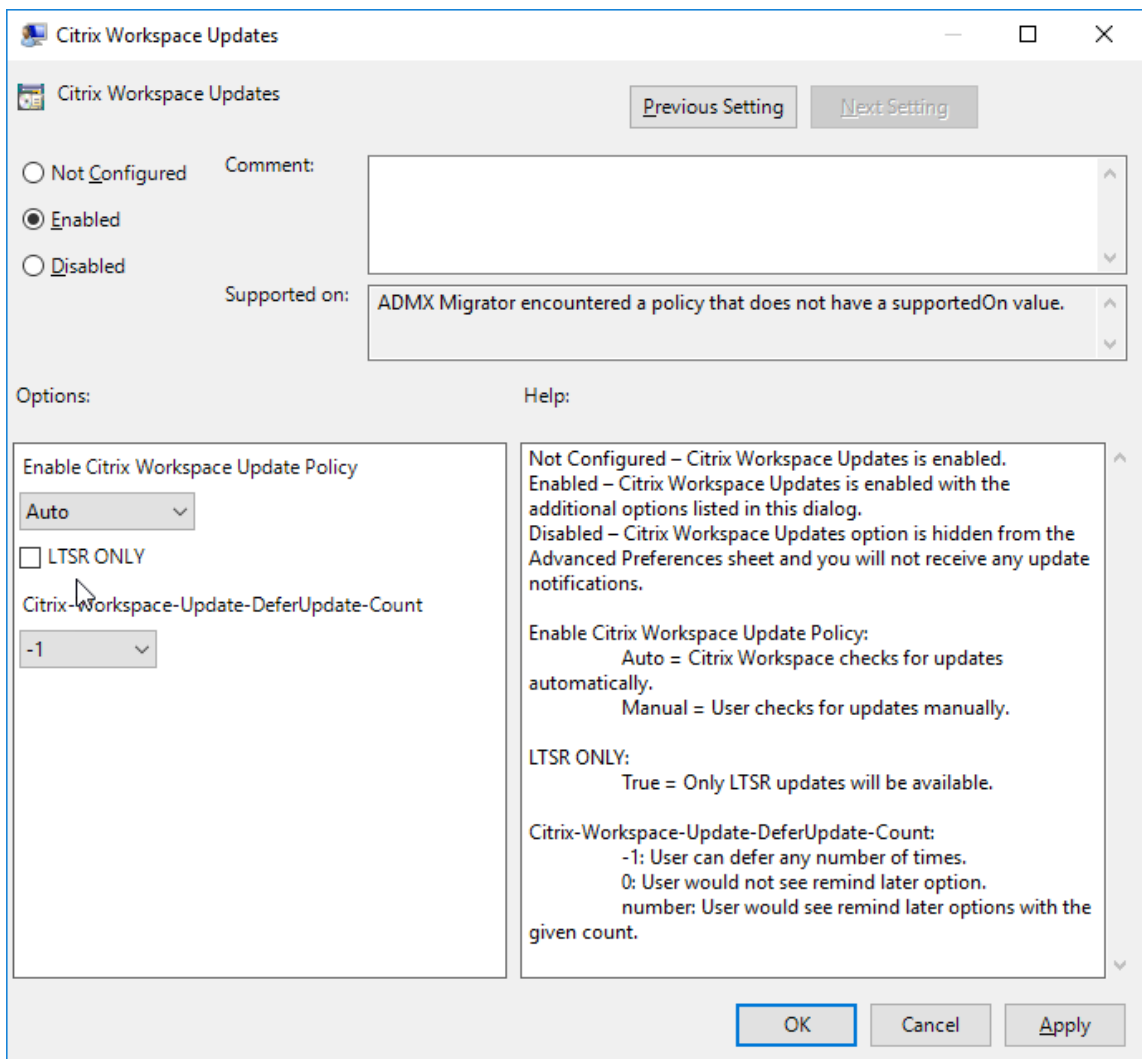
Configuration avancée des mises à jour automatiques (mises à jour de Citrix Workspace)

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. Global App Configuration Service (GACS)
3. Interface de ligne de commande
4. GUI
5. StoreFront

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

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



3. **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. L’option **Désactivé** masque également l’option Mises à jour de Workspace sur la page Préférences avancées.

4. **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 la liste déroulante **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). Ce paramètre s’applique uniquement aux versions antérieures à l’application Citrix Workspace 2207. Dans les versions 2207 ou ultérieures, la mise à jour de l’application Citrix

Workspace est automatique et vous n'êtes pas averti lorsqu'une mise à jour est disponible.

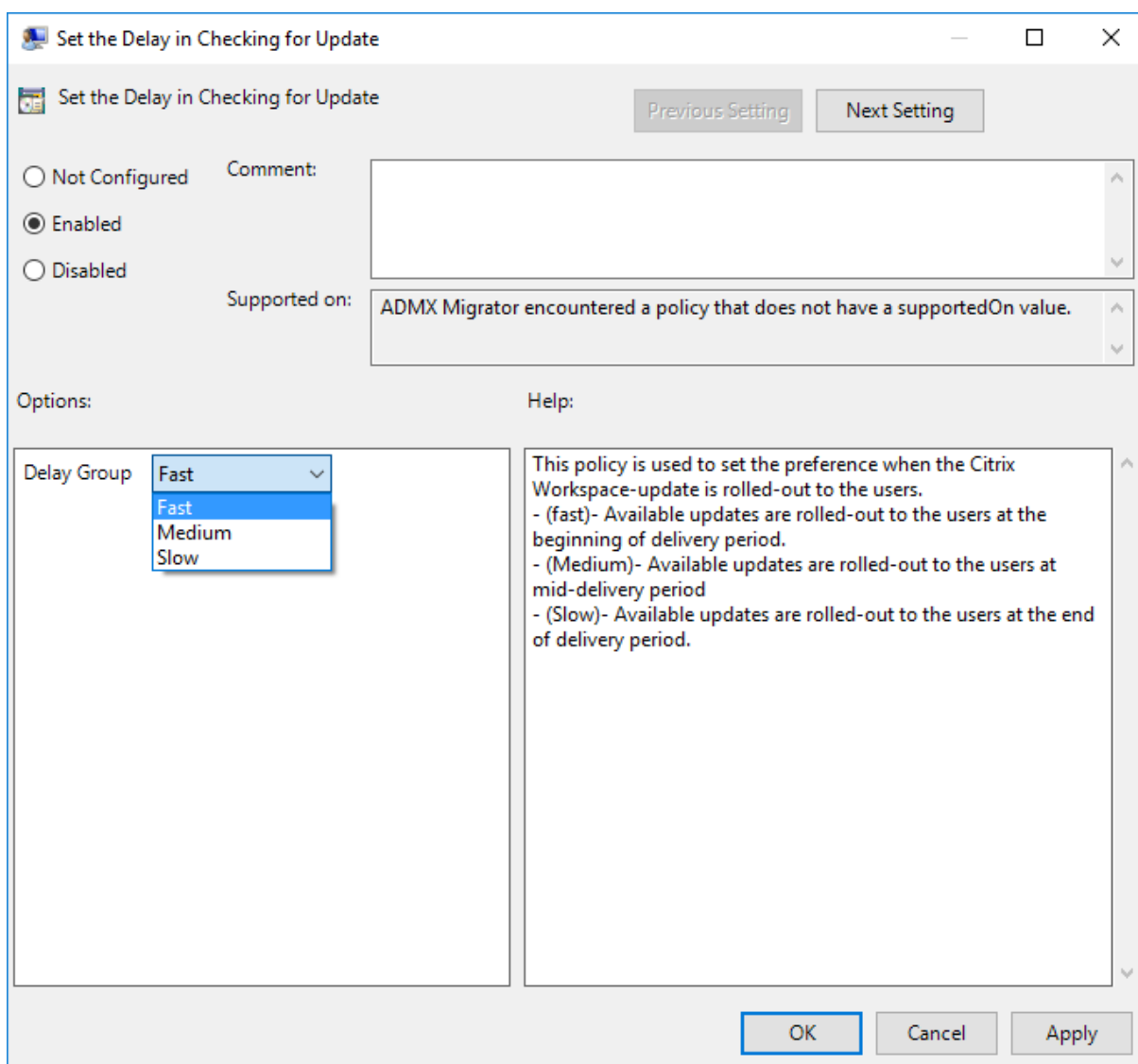
- Manuel : vous n'êtes pas informé lorsqu'une mise à jour est disponible. Recherchez les mises à jour manuellement.
5. Sélectionnez **LTSR UNIQUEMENT** pour obtenir les mises à jour de LTSR uniquement.
 6. Dans la liste déroulante **Citrix-Workspace-Update-DeferUpdate-Count**, sélectionnez une valeur comprise entre -1 et 30 :
 - Si la valeur est 0, l'option **Me rappeler plus tard** n'apparaît pas. L'invite **Mise à jour disponible** s'affiche à chaque vérification automatique périodique de mise à jour.
 - Si la valeur est -1, l'option **Me rappeler plus tard** s'affiche avec l'invite **Mise à jour disponible**. Vous pouvez différer la notification de mise à jour autant de fois que nécessaire.
 - Une valeur comprise entre 1 et 30 définit le nombre de fois que l'option **Me rappeler ultérieurement** avec l'invite **Mise à jour disponible** doit apparaître. Vous pouvez différer la notification de mise à jour en fonction de la valeur définie dans ce champ. Cependant, vous verrez toujours l'invite **Mise à jour disponible**, mais sans l'option **Me rappeler ultérieurement**.

Remarque :

À partir de l'application Citrix Workspace pour Windows version 2207, la fonctionnalité de mise à jour automatique est améliorée et le champ **Citrix-Workspace-Update-DeferUpdate-Count** n'est pas obligatoire.

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 de la liste déroulante **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. L'option **Désactivé** 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.

`CitrixReceiverUpdater.exe` se trouve généralement dans `CitrixWorkspaceInstallLocation\Citrix\Ica Client\Receiver`. Vous pouvez exécuter le binaire `CitrixReceiverUpdater.exe` 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 :

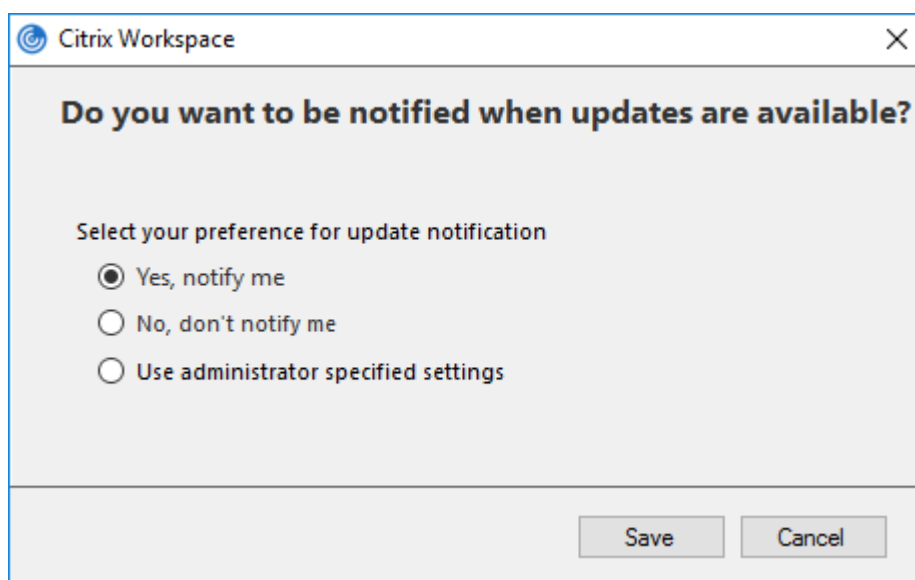
`/AutoUpdateCheck` est un paramètre obligatoire que vous devez définir pour configurer d'autres paramètres comme `/AutoUpdateStream`, `/DeferUpdateCount`, `/AURolloutPriority`.

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

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

1. Cliquez avec le bouton droit de la souris sur l'icône de l'application Citrix Workspace dans la zone de notification.
2. Sélectionnez **Préférences avancées > Mises à jour de Citrix Workspace**.
3. Sélectionnez l'une des options de préférence de notification suivantes :

- **Oui, me notifier** : vous êtes averti lorsqu'une mise à jour est disponible pour l'application Citrix Workspace.
- **Non, ne pas me notifier** : vous n'êtes pas averti lorsqu'une mise à jour est disponible pour l'application Citrix Workspace. Vérifiez les mises à jour manuellement.
- **Utiliser les paramètres spécifiés par l'administrateur** : utilise les paramètres configurés sur le serveur StoreFront.



4. Cliquez sur **Enregistrer**.

Remarque :

- Les options **Oui, me notifier** et **Non, ne pas me notifier** s'appliquent uniquement aux versions antérieures à l'application Citrix Workspace 2207. Dans les versions 2207 ou ultérieures, la mise à jour de l'application Citrix Workspace est automatique et vous n'êtes pas averti lorsqu'une mise à jour est disponible. Si vous sélectionnez l'option **Non, ne pas me notifier**, vous devez vérifier manuellement les mises à jour.
- Vous pouvez masquer la totalité ou une partie de la page Préférences avancées disponible à partir de l'icône de l'application Citrix Workspace. 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)

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

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

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

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

```
1 <account>
2
3   <clear />
4
5   <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
6     F84Store"
7     description="" published="true" updaterType="Citrix"
8     remoteAccessType="None">
9
10    <annotatedServices>
11
12      <clear />
13
14      <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
15
16        <metadata>
17
18          <plugins>
19
20            <clear />
21
22          </plugins>
23
24          <trustSettings>
25
26            <clear />
27
28          </trustSettings>
29
30          <properties>
31
32            <property name="Auto-Update-Check" value="auto" />
33
34            <property name="Auto-Update-DeferUpdate-Count" value=
35              ="1" />
36
37            <property name="Auto-Update-LTSR-Only" value=
38              ="FALSE" />
39
40            <property name="Auto-Update-Rollout-Priority" value=
41              ="fast" />
42
43          </properties>
44
45        </annotatedServiceRecord>
46
47      </annotatedServices>
48
49    </account>
50
```

```
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 (défaut) : recherche et effectue les mises à jour automatiquement.
 - Manuel : les mises à jour ne sont récupérées que lorsque l'utilisateur effectue une demande de vérification depuis le menu de la barre d'état système de l'application Citrix Workspace.
 - Désactivé : aucune recherche de mises à jour n'est effectuée.
- **Auto-Update-LTSR-Only** : indique que la mise à jour de la version est pour LTSR uniquement.
 - True : le programme de mise à jour ignore toutes les mises à jour qui ne sont pas marquées comme LTSR. Seules les mises à jour LTSR sont considérées.

- False (défaut) : le programme de mise à jour ne considère que les mises à jour du flux actuel.
- **Auto-update-Rollout-Priority** : indique la période de mise à disposition pendant laquelle vous pouvez recevoir la mise à jour.
 - Rapide : les mises à jour sont déployées au début de la période de mise à disposition.
 - Moyen : les mises à jour sont déployées vers le milieu de la période de mise à disposition.
 - Lent : les mises à jour sont déployées à la fin de la période de mise à disposition.
- **Auto-update-DeferUpdate-Count** : indique le nombre de fois que vous pouvez reporter les notifications de mises à jour de la version.

Remarque :

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

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

Gestion des plugins

April 22, 2024

L'application Citrix Workspace pour Windows offre une fonctionnalité de gestion des plug-ins qui fait de l'application Citrix Workspace une application cliente unique requise sur le terminal pour installer et gérer des agents tels que Secure Access Agent et le plug-in Endpoint Analysis (EPA).

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

La gestion des plug-ins inclut les étapes suivantes :

- Les administrateurs doivent spécifier les agents requis sur les appareils des utilisateurs finaux dans Global App Configuration Service. Les administrateurs peuvent spécifier Secure Access Agent et l'agent Endpoint Analysis (EPA).
- L'application Citrix Workspace extrait la liste des agents à partir de Global App Configuration Service.
- Sur la base de la liste extraite de Global App Configuration Service, l'application Citrix Workspace télécharge les packages d'agents via le service de mise à jour automatique. Si l'agent n'

est pas déjà installé sur le terminal, l'application Citrix Workspace déclenche l'installation de l'agent. Si l'agent est déjà installé, l'application Citrix Workspace déclenche une mise à jour de l'agent (si la version de l'agent téléchargé est supérieure à la version installée).

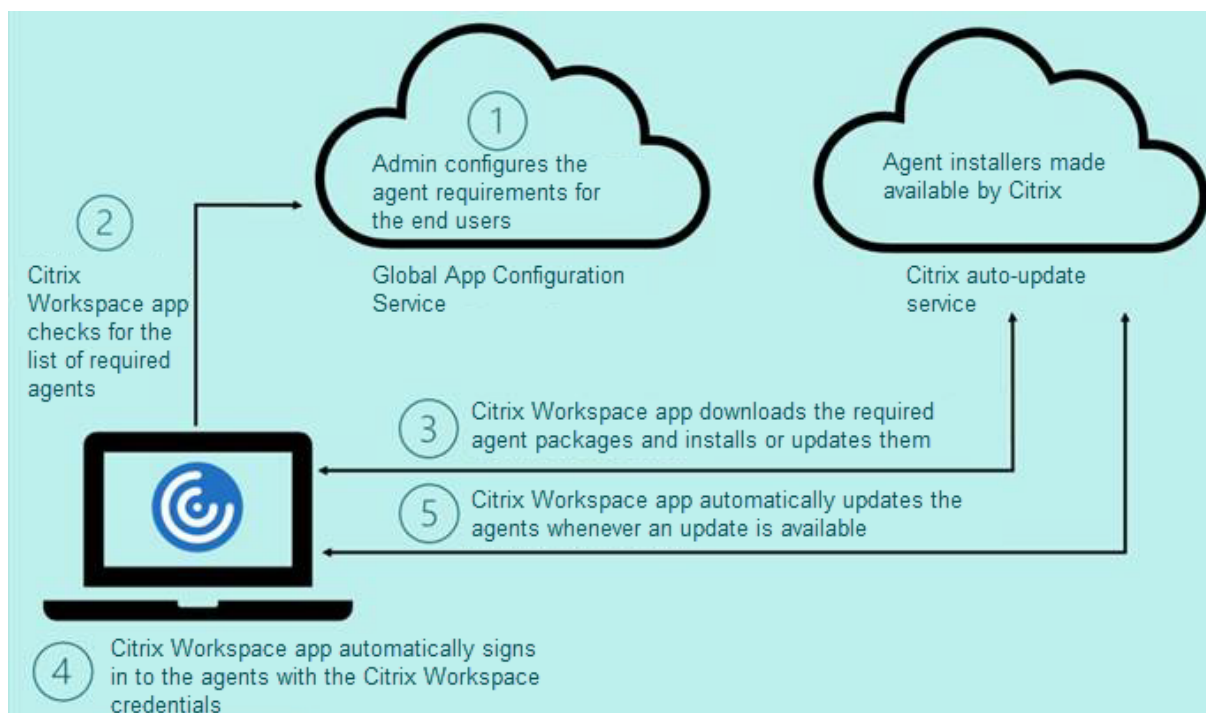
L'application Citrix Workspace garantit la mise à jour automatique des agents chaque fois qu'une mise à jour est disponible à l'avenir.

L'application Citrix Workspace se connecte automatiquement aux agents à l'aide des informations d'identification de Citrix Workspace.

Remarques :

- Si les plug-ins EPA et ZTNA n'existent pas, ils sont téléchargés et installés lors de l'ajout du magasin ou du compte pour la première fois.
- Si le magasin ou le compte et les plug-ins existent déjà et que le programme d'installation contient une version supérieure, les plug-ins sont mis à jour pendant le cycle de mise à jour automatique.

Le schéma suivant illustre le workflow :



Important :

Global App Configuration Service est requis pour activer la fonctionnalité de gestion des plug-ins.

- Pour les magasins cloud, l'interface utilisateur de Global App Configuration Service est accessible dans la section **Configuration de l'espace de travail** du portail d'administration

- Citrix Cloud. Pour plus d'informations, consultez [Configurer l'application Citrix Workspace](#).
- Pour intégrer des magasins sur site ou pour les clients qui souhaitent configurer la détection basée sur les e-mails pour les magasins cloud, consultez la documentation de [Global App Configuration Service](#).

Vous pouvez activer la fonctionnalité de gestion des plug-ins à l'aide des méthodes suivantes :

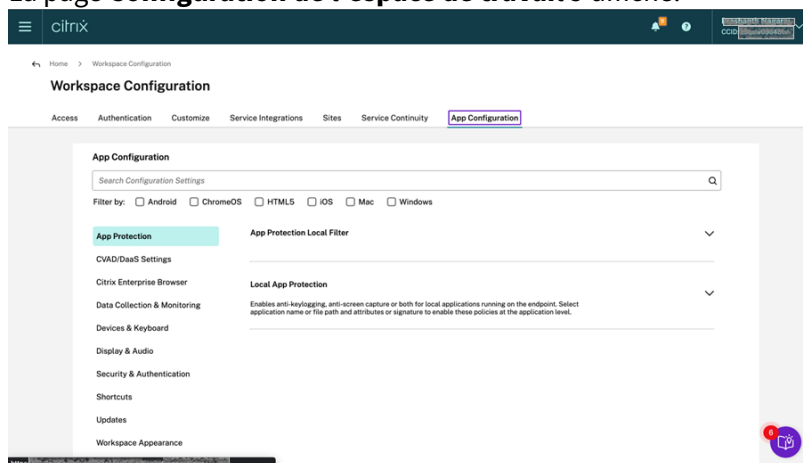
- Utilisation de l'interface utilisateur de Global App Configuration Service : utilisez cette méthode pour déployer la dernière version du client.
- Utilisation de l'API Global App Configuration Service : utilisez cette méthode pour personnaliser l'installation avec des paramètres permettant de contrôler la version, les modes de déploiement, les intervalles de mise à jour automatique, etc.

Activer la gestion des plug-ins à l'aide de l'interface utilisateur de Global App Configuration Service

Cette méthode s'applique uniquement aux magasins cloud. Les agents (EPA/Secure Access, plug-in Zoom ou plug-in WebEx) peuvent être déployés par les administrateurs à l'aide de l'interface utilisateur.

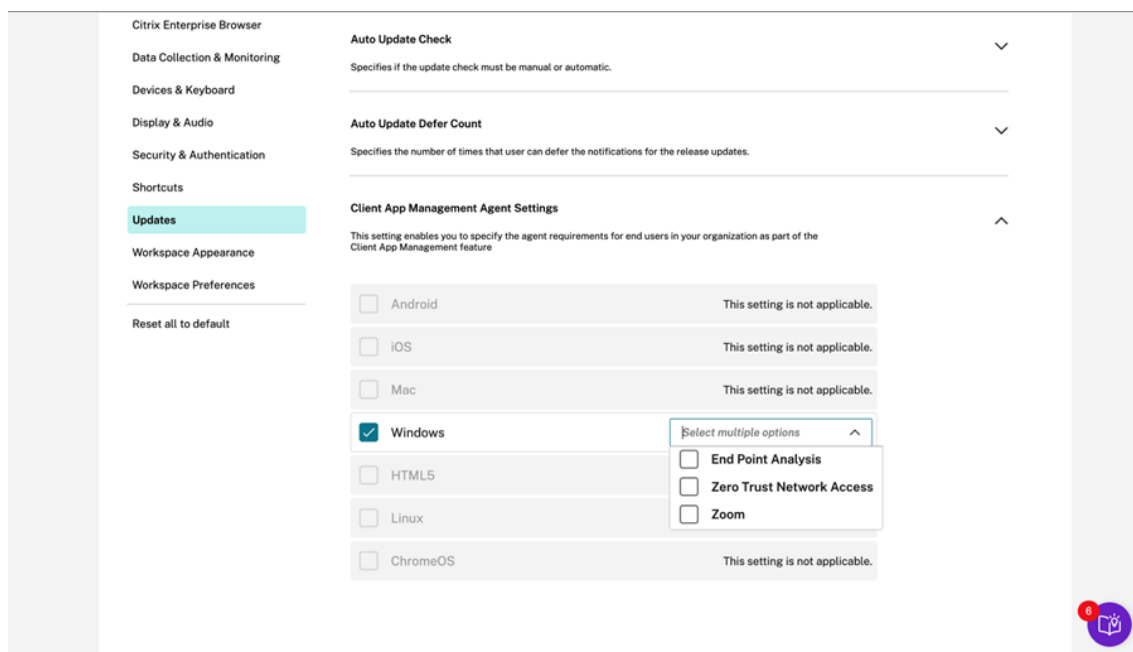
1. Connectez-vous à [Citrix Cloud](#).
2. Dans le menu en haut à gauche de l'écran, sélectionnez **Configuration de l'espace de travail**.

La page **Configuration de l'espace de travail** s'affiche.



3. Cliquez sur l'onglet **Configuration de l'application**.
4. Cliquez sur **Mises à jour**.
5. Assurez-vous que la case **Windows** est cochée.

- Sélectionnez les agents requis à côté de **Windows** dans la liste déroulante **Paramètres de l'agent de gestion des applications clientes**.



Activer la gestion des plug-ins à l'aide de l'API Global App Configuration Service

- Configurez et intégrez les paramètres dans Global App Configuration Service à l'aide de l'API. Pour plus d'informations, consultez [Mapper les URL de service et configurer les paramètres](#).
- La configuration Global App Configuration suivante doit être intégrée pour que le magasin/compte puisse intégrer l'analyse de point de terminaison et ZTNA/Secure Access Client :

```

1  {
2
3    "serviceURL":
4    {
5
6      "url": "https://storefront.acme.com:443"
7    }
8  ,
9    "settings":
10   {
11
12     "description": "Install and update plugins",
13     "name": "Install and update plugins",
14     "useForAppConfig": true,
15     "appSettings":
16     {
17
18       "windows":
19       [

```

```
20     {
21
22         "assignedTo":
23         [
24             "AllUsersNoAuthentication"
25         ],
26         "category": "AutoUpdate",
27         "settings":
28         [
29             {
30
31                 "name": "Auto Update plugins settings",
32                 "value":
33                 [
34                     {
35
36                         "pluginId": "8A8AF6C0-11F6-4343-
37                             BA2D-A85A766170D4",
38                         "pluginName": "Citrix EPA Client",
39                         "pluginSettings":
40                         {
41
42                             "delayGroup": "Fast",
43                             "deploymentMode": "
44                                 InstallAndUpdate",
45                             "detectRule": "UpgradeCode:{
46                                 37A181F7-870E-4BDF-B0EA-E3B4766119FE }
47                                 ",
48                             "isBlocking": true,
49                             "isFTU": true,
50                             "maximumAllowedVersion": "
51                                 23.8.1.24",
52                             "minimumAllowedVersion": "
53                                 0.0.0.0",
54                             "stream": "Current",
55                             "upgradeToLatest": true
56                         }
57                     }
58                 ],
59                 "pluginId": "9A8AF6C0-11F6-4343-
60                             BA2D-A85A766170D5",
61                 "pluginName": "Citrix Secure Access
62                             Client",
63                 "pluginSettings":
64                 {
65
66                     "delayGroup": "Fast",
67                     "deploymentMode": "
68                         InstallAndUpdate",
69                     "detectRule": "UpgradeCode:{
```

```
66 F0ED53AB-11BE-4E9C-87E5-CD4A81DA2A4D }
67 ",
68         "isBlocking": false,
69         "isFTU": true,
70         "maximumAllowedVersion": "
71             21.8.0.0",
72         "minimumAllowedVersion": "
73             0.0.0.0",
74         "stream": "Current",
75         "upgradeToLatest": true
76     }
77 },
78     {
79
80         "pluginId": "C03BAE37-F3AC-4D63-8
81             BC1-3C9CD2BC9E8D",
82         "pluginName": "WebEx VDI
83             AutoUpgrade Plugin",
84         "pluginSettings":
85         {
86             "delayGroup": "Fast",
87             "deploymentMode": "
88                 InstallAndUpdate",
89             "detectRule": "UpgradeCode:{
90                 AA2AACDC-D30B-433F-A602-3E25975010A6 }
91                 ",
92             "isBlocking": false,
93             "isFTU": false,
94             "maximumAllowedVersion": "
95                 3.1.0.24263",
96             "minimumAllowedVersion": "0.0.0
97                 ",
98             "stream": "Current",
99             "upgradeToLatest": true
100         }
101     }
102 ]
103 ],
104 "userOverride": false
105 }
106 ]
107 }
108 }
109 }
110 }
111 }
```



```

112 }
113
114
115 <!--NeedCopy-->

```

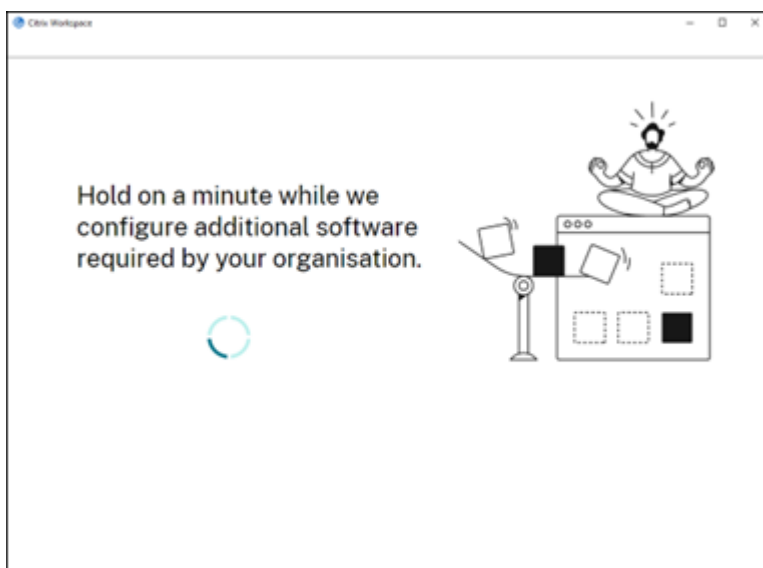
Le tableau suivant répertorie le schéma, les valeurs et la description des paramètres de gestion des plug-ins.

Paramètre du schéma	Valeur	Description
<code>isBlocking</code>	True ou False	Lorsque le paramètre <code>isBlocking</code> est défini sur <code>true</code> , le plug-in est considéré comme obligatoire et la page de connexion n'apparaît que lorsque le plug-in requis est installé. Citrix vous recommande de définir EPA comme plug-in obligatoire.
<code>pluginName</code>	Nom convivial pour le plug-in.	Le nom du plug-in peut être modifié.
<code>pluginId</code>	Identifiant du plug-in.	ne doit pas être modifié.
<code>delayGroup</code>	Fast, Medium, Slow	Intervalle de mise à jour automatique auquel les plug-ins doivent être mis à jour.
<code>deploymentMode</code>	InstallAndUpdate/Update	InstallAndUpdate : le plug-in peut être nouvellement installé et mis à jour avec la nouvelle version. Update : seule une mise à jour est autorisée, aucune nouvelle installation.
<code>None</code>	Aucune action n'est requise pour ce plug-in.	
<code>detectRule</code>	La valeur ne peut pas être modifiée.	Vérifie si le plug-in est déjà installé ou non.
<code>maximumAllowedVersion</code>	Version maximale autorisée du plug-in.	
<code>minimumAllowedVersion</code>	Version minimale autorisée du plug-in.	
<code>upgradeToLatest</code>	True ou False	Doit être défini sur <code>False</code> pour prendre en charge <code>maximumAllowedVersion</code> et <code>minimumAllowedVersion</code> . <code>True</code> : la dernière version du plug-in est prise en compte lors de la mise à jour.
<code>Stream</code>	Current	Doit être réglé sur <code>Current</code> pour recevoir l'installation ou la mise à jour automatique des plug-ins.

Flux de travail utilisateur

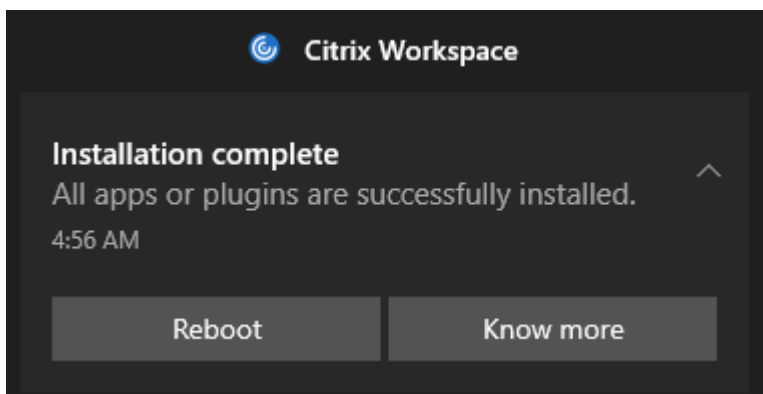
1. Téléchargez et installez l'application Citrix Workspace pour Windows.
2. Cliquez sur **Ajouter un compte** à la fin de l'installation.
3. Ajoutez le magasin/compte dans lequel les paramètres de configuration de l'application sont intégrés.

Le message suivant s'affiche lors de l'installation des plug-ins obligatoires :

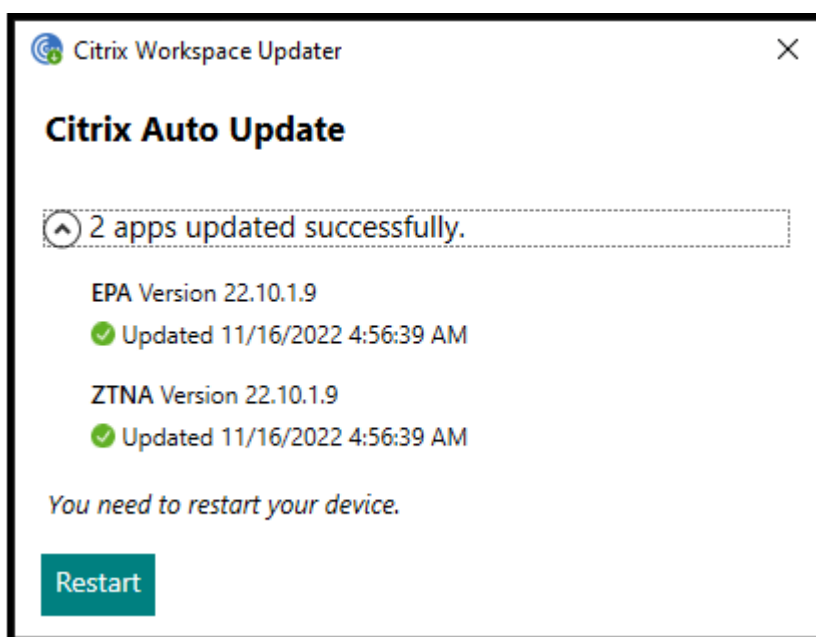


(Installation en attente)

4. Lorsque l'installation est terminée, la notification toast suivante s'affiche :



5. Cliquez sur **Know More** (En savoir plus) pour connaître les plug-ins installés.



Gestion des plug-ins pour le plug-in Zoom

Le téléchargement, l'installation et la mise à jour automatique du plug-in Zoom sont également pris en charge et gérés de la même manière que les plug-ins EPA et ZTNA.

Le paramètre Global App Configuration suivant doit être intégré pour que le magasin/compte puisse tirer parti de cette fonctionnalité :

```
1 {
2
3   "serviceURL":
4   {
5
6     "url": "https://storefront.acme.com:443"
7   }
8   ,
9   "settings":
10  {
11
12    "description": "Install and update plugins",
13    "name": "Install and update plugins",
14    "useForAppConfig": true,
15    "appSettings":
16    {
17
18      "windows":
19      [
20        {
21
22          "assignedTo":
23          [
```

```
24         "AllUsersNoAuthentication"
25     ],
26     "category": "AutoUpdate",
27     "settings":
28     [
29         {
30
31             "name": "Auto Update plugins settings",
32             "value":
33             [
34                 {
35
36                     "pluginId": "1A4BB471-022C-4C87-
37                         BDCD-0B64FB42869C",
38                     "pluginName": "Zoom VDI AutoUpgrade
39                         Plugin",
40                     "pluginSettings":
41                     {
42
43                         "delayGroup": "Fast",
44                         "deploymentMode": "
45                         InstallAndUpdate",
46                         "detectRule": "UpgradeCode:{
47                         34225638-14F3-4059-BE34-175AC9B35435 }
48                         ",
49                         "isBlocking": false,
50                         "isFTU": false,
51                         "maximumAllowedVersion": "
52                         5.11.2872",
53                         "minimumAllowedVersion": "0.0.0
54                         ",
55                         "stream": "Current",
56                         "upgradeToLatest": true
57                     }
58                 }
59             ]
60         },
61     ],
62     "userOverride": false
63 }
64 }
65 }
66 }
67 }
68 }
69 }
70 }
71 <!--NeedCopy-->
```

Expérience de l'application

April 22, 2024

Cette section décrit les éléments suivants :

- [Mise à disposition d'applications](#)
- [Amélioration de l'expérience de lancement de Virtual Apps and Desktops](#)
- [Préférences de l'application](#)
- [Applications SaaS](#)
- [Collecte et surveillance des données](#)

Mise à disposition d'applications

April 22, 2024

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

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

vous permet de localiser toutes les applications publiées là où vous vous attendez à les trouver à l'aide du schéma de navigation Windows habituel.

Pour 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

Il vous suffit d'ajouter un compte StoreFront à l'application Citrix Workspace ou de configurer l'application Citrix Workspace pour qu'elle pointe vers un site StoreFront pour pouvoir configurer le mode libre-service. La configuration permet aux utilisateurs de s'abonner à des applications à partir de l'interface utilisateur de Citrix Workspace. L'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. Au lieu de cela, les applications sont affichées individuellement ou sous le dossier racine. Les applications ne se trouvent pas dans les sous-dossiers de catégorie définis avec Citrix Virtual Apps and Desktops et Citrix DaaS.

- 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 les 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 changer 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

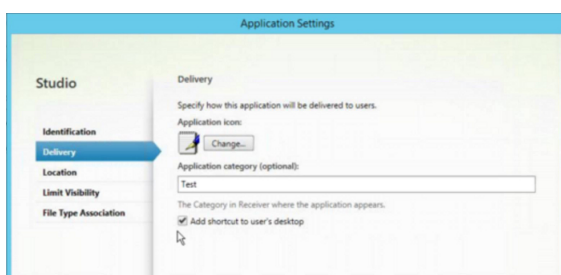
L'application Citrix Workspace peut être configurée pour placer automatiquement des raccourcis d'applications et de bureaux directement dans le menu Démarrer ou sur le bureau. Toutefois,

cette configuration est similaire aux versions précédentes de Workspace pour Windows. Toutefois, la version 4.2.100 a introduit la possibilité 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.

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 requise.
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

L'application Citrix Workspace fournit des fonctionnalités permettant de copier les stubs .EXE à partir d'un partage réseau, si :

- il y a un retard dans l'énumération des applications à chaque connexion, ou
- il est nécessaire de signer numériquement les stubs d'application.

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

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.

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 que les modifications prennent effet.

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 vous avez des dizaines, voire des centaines d'applications, autorisez les utilisateurs à sélectionner les applications à ajouter aux **Favoris** et 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 accédez à Workspace pour 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 place 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, placez-les toutes 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 souhaitez 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 souhaitez 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 voient les applications pendant qu'un autre utilisateur partage le point de terminaison, vous pouvez supprimer les applications lorsque l'utilisateur ferme sa session et quitte l'application.

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 à la fin de session	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 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 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'ap-

application Citrix Workspace, l'application Citrix Workspace annule l'abonnement à l'application mais ne la désinstalle pas.

Remarque :

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

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

- `prefer="Nomapplication"`

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

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

- `prefer="\\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 et Citrix DaaS.

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.

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 qui héberge 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) ou
- 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 du VDA. Si elle est présente, lance l'instance locale de l'application. Sinon, une instance hébergée de l'application est lancée.

Si vous lancez une application qui ne se trouve pas sur le VDA, l'application Citrix Workspace lance l'application hébergée. 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](#). Lorsque vous procédez à une 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**.

5. Dans la liste déroulante **Autoriser les 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, Word-Pad ou l'invite de commandes). Elle lance ensuite 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.
6. Cliquez sur **Appliquer** et **OK**.
7. Redémarrez la session pour que les modifications prennent effet.

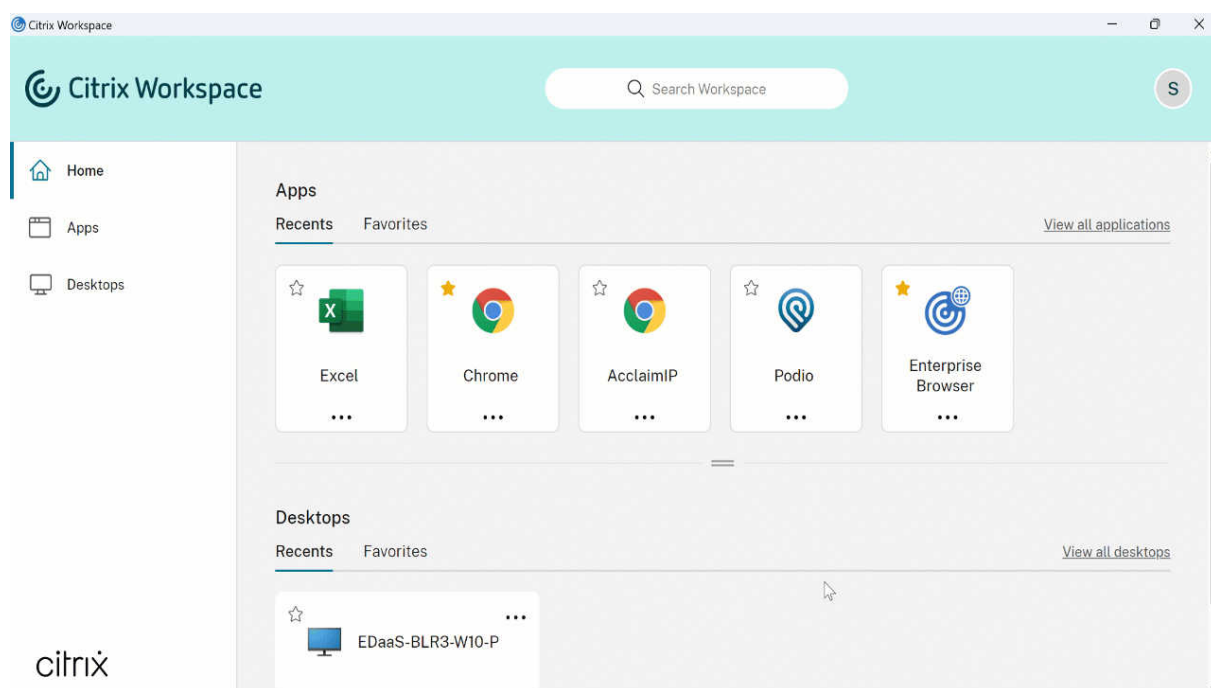
Limitation :

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

Amélioration de l'expérience de lancement de Virtual Apps and Desktops

April 22, 2024

Cette fonctionnalité est activée par défaut pour les magasins sur site et dans le cloud. Avec cette amélioration, l'expérience de lancement d'applications et de bureaux est plus informatif, moderne et convivial sur l'application Citrix Workspace pour Windows. Cela permet d'améliorer l'engagement auprès des utilisateurs grâce à des informations pertinentes et opportunes sur l'état du lancement. La notification apparaît dans le coin inférieur droit de l'écran.



Au lieu d'une icône de chargement, les utilisateurs peuvent consulter des notifications pertinentes concernant la progression du lancement. Si un lancement est en cours et que l'utilisateur tente de fermer le navigateur, un message d'avertissement s'affiche.

Préférences de l'application

April 22, 2024

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, vous pouvez :

- 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 Paramètres avancés

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

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 suivant 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. Lancez 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**.

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.

La fonctionnalité Citrix Casting vous permet d'accéder instantanément et en toute sécurité à n'importe quelle application à partir d'un appareil mobile et de l'afficher sur un 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).

Pré-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 est autorisé 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.
- Exécutez la commande `/IncludeCitrixCasting` pendant l'installation pour activer Citrix Casting.

Configurer le lancement de Citrix Casting

Remarque :

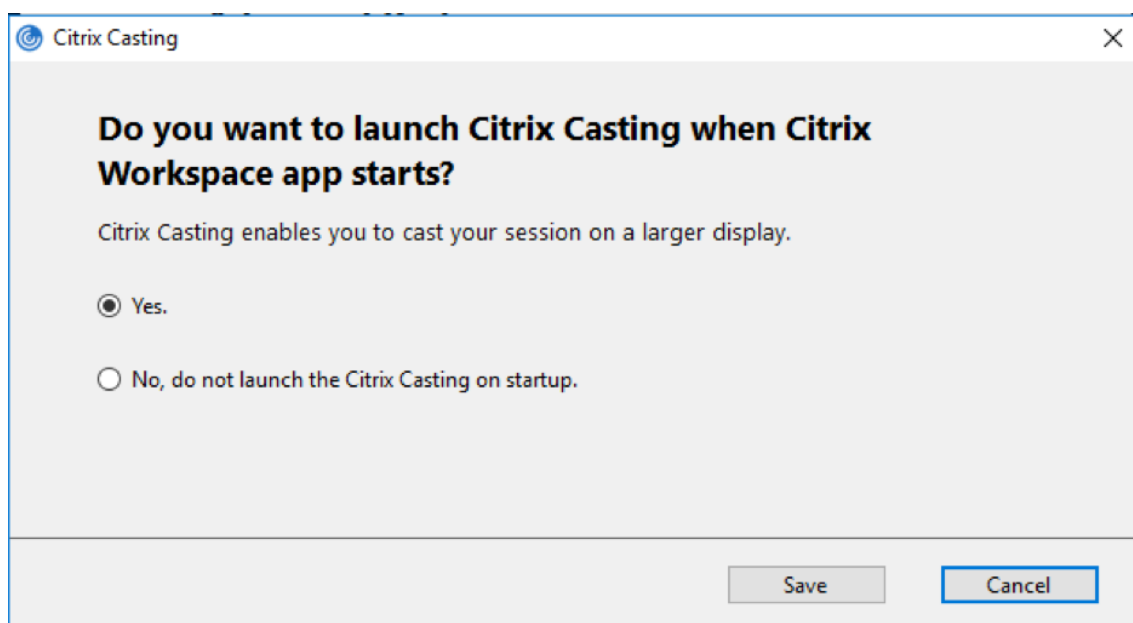
Vous pouvez masquer tout ou partie de la feuille Préférences avancées. Pour plus d'informations, consultez la section [Page Préférences avancées](#).

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.

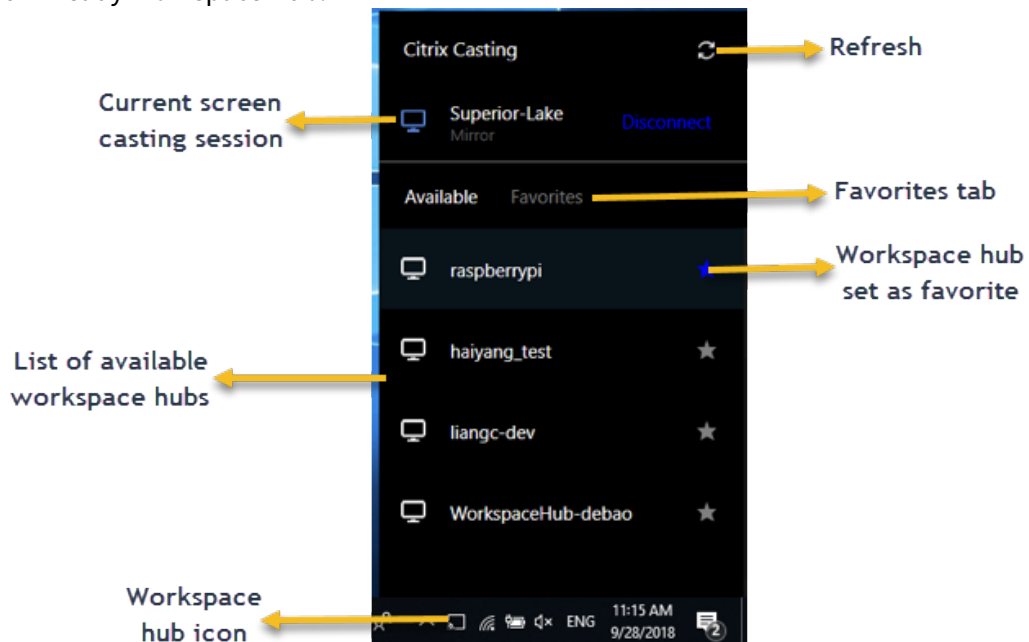
2. Sélectionnez le Workspace Hub pour la diffusion de votre écran et choisissez l'une des options suivantes :
- **Mettre en miroir** pour dupliquer l'écran principal et diffuser l'affichage sur l'appareil Workspace Hub connecté.
 - **Étendre** pour utiliser l'écran de l'appareil Workspace Hub en tant 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, veuillez 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 s'il affiche les détails de l'appareil du hub d'espace de travail.
5. Cliquez sur **Actualiser** dans Citrix Ready Workspace Hub et essayez de vous reconnecter à Workspace Hub.

Problèmes connus et limitations

- Citrix Casting ne fonctionne que si l'appareil est connecté au même réseau que Citrix Ready Workspace Hub.
- En cas de problèmes de réseau, il peut y avoir un décalage d'affichage sur Workspace Hub Device.
- Lorsque vous sélectionnez **Étendre**, l'écran principal sur lequel l'application Citrix Ready Workspace Hub est lancé clignote plusieurs fois.
- Dans le mode **Étendre**, vous ne pouvez pas définir l'affichage secondaire comme affichage principal.
- 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.
- 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.
- Plusieurs sessions de diffusion d'écran ne sont pas prises en charge.
- La résolution d'écran maximale prise en charge par Citrix Casting est de 1920 x 1440.
- 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.
- Cette fonctionnalité n'est pas prise en charge sur l'application Citrix Workspace pour Windows (Store).

- Sous Windows 10, Build 1607, Citrix Casting en mode **Étendre** peut ne pas être correctement positionné.

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

Applications SaaS

April 22, 2024

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. Les administrateurs peuvent y parvenir en filtrant l'accès à des sites Web et à des catégories de sites Web spécifiques.

L'application Citrix Workspace pour Windows prend en charge l'utilisation des applications SaaS à l'aide de Citrix Secure Private Access. 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.

L'application Citrix Workspace lance les applications SaaS sur Citrix Enterprise Browser (anciennement Citrix Workspace Browser). Pour plus d'informations, consultez la documentation du [Citrix Enterprise Browser](#).

Limitations :

- 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, vous pouvez encore enregistrer le PDF. Pour remédier à ce problème, vous pouvez désactiver l'option d'impression afin de désactiver la fonctionnalité de téléchargement.
- Il est possible que les vidéos intégrées à une application ne fonctionnent pas.
- Vous ne pouvez pas ouvrir d'applications SaaS à l'aide des commandes Storebrowse.

Pour plus d'informations sur la configuration de l'espace de travail, consultez la section [Configuration de l'espace de travail](#) dans Citrix Cloud.

Collecte et surveillance des données

April 22, 2024

Citrix Analytics

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

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 le service Citrix Analytics 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 :

- La transmission d'adresses IP se produit dans le meilleur des cas. Bien que l'application Citrix Workspace transmette toutes les adresses IP sur lesquelles elle est lancée, 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.

L'application Citrix Workspace est conçue pour transmettre en toute sécurité des données à Citrix Analytics Service à partir de sessions ICA que vous lancez depuis un navigateur.

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

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 aident Citrix à améliorer la qualité, les fonctionnalités et les performances de l'application Citrix Workspace, à allouer correctement les ressources à des fins de développement de produits, à maintenir les niveaux de service et à gérer les investissements en personnel et en infrastructure.

Données collectées

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

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

Version du système d'exploitation*	Version de l'application 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	Raison de la bannière hors ligne

Modèle/propriétés de l'appareil	État du lancement de sessions Citrix Virtual Apps and Desktops	Nom de l'application/du bureau virtuel	État de la mise à jour automatique
Détails de la location de connexion	Utilisation de la fonctionnalité de migration de l'URL de StoreFront vers Workspace	Utilisation de Citrix Enterprise Browser	Canal de mise à jour automatique
Détails du délai d'inactivité	Version de Citrix Enterprise Browser		

Préférences de collecte de données

À compter de la version 2205, les utilisateurs et les administrateurs peuvent arrêter d'envoyer des données CEIP (à l'exception des deux éléments de données qui peuvent être bloqués comme indiqué dans la remarque ci-dessous) en suivant les étapes ci-dessous.

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 en tant qu'administrateur 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** ou que vous avez défini la clé `Enable_CEIP` sur `False`, vous pouvez également arrêter d'envoyer les deux derniers éléments de données du programme CEIP, c'est-à-dire la version du système d'exploitation et de l'application Citrix Workspace, en accédant à l'entrée de Registre suivante et en définissant la valeur :

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

Clé : DisableHeartbeat

Valeur : True

Informations supplémentaires

Citrix traite vos données conformément aux termes de votre contrat avec Citrix et les protège comme indiqué dans l'[Annexe sur la sécurité des Services Citrix](#). L'Annexe est disponible sur [Citrix Trust Center](#).

Sécurité et authentification

April 22, 2024

Cette section décrit les éléments suivants :

- [Sécurité](#)
- [Sécuriser les communications](#)
- [Authentification](#)
 - [Matrice d'authentification pass-through au domaine](#)
 - [Authentification pass-through au domaine pour Citrix Workspace en utilisant un Citrix Gateway local en tant que fournisseur d'identité](#)
 - [Authentification pass-through au domaine pour Citrix Workspace en utilisant Azure Active Directory en tant que fournisseur d'identité](#)
 - [Authentification pass-through au domaine pour Citrix Workspace en utilisant Okta en tant que fournisseur d'identité](#)

Sécurité

April 22, 2024

App Protection

App Protection est une fonctionnalité complémentaire qui offre une sécurité renforcée lors de l'utilisation de Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Cette fonctionnalité limite le risque d'infection par des programmes malveillants d'enregistrement de frappe et de capture d'écran. App Protection empêche l'exfiltration d'informations confidentielles telles que les informations d'identification de l'utilisateur et les informations sensibles affichées à l'écran. Cette fonctionnalité empêche les utilisateurs et les attaquants de prendre des captures d'écran et d'utiliser des enregistreurs de frappe pour récupérer et exploiter des informations sensibles. Pour plus d'informations, consultez [Protection des applications](#).

Clause d'exclusion de responsabilité

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

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

Remarque :

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

Amélioration de la sécurité des fichiers ICA

Cette fonctionnalité fournit une sécurité renforcée lors du traitement des fichiers ICA lors du lancement d'une session d'applications et de bureaux virtuels.

L'application Citrix Workspace vous permet de stocker le fichier ICA dans la mémoire système au lieu du disque local lorsque vous lancez une session d'applications et de bureaux virtuels.

Cette fonctionnalité vise à éliminer les attaques de surface et tout malware susceptible d'utiliser à mauvais escient le fichier ICA lorsqu'il est stocké localement. Cette fonctionnalité s'applique également aux sessions d'applications et de bureaux virtuels lancées sur Workspace for Web.

Configuration

La sécurité des fichiers ICA est également prise en charge lorsque Citrix Workspace ou StoreFront est accessible via le Web. La détection des clients est une condition préalable pour que cette fonctionnalité soit opérationnelle si elle est accessible via le Web. Si vous accédez à StoreFront à l'aide d'un navigateur, activez les attributs suivants dans le fichier web.config sur les déploiements StoreFront :

Version de StoreFront	Attribut
2.x	pluginassistant
3.x	protocolHandler

Lorsque vous vous connectez au magasin via le navigateur, cliquez sur **Détecter l'application Workspace**. Si l'invite n'apparaît pas, effacez les cookies du navigateur et réessayez.

S'il s'agit d'un déploiement Workspace, vous pouvez trouver les paramètres de détection du client en accédant à **Paramètres du compte > Avancé > Préférences de lancement des applications et des postes de travail**.

Vous pouvez prendre des mesures supplémentaires pour que les sessions soient lancées uniquement à l'aide d'un fichier ICA stocké sur la mémoire système. Utilisez l'une des méthodes suivantes :

- Modèle d'administration d'objet de stratégie de groupe (GPO) sur le client
- Global App Config Service
- Workspace pour Web

Utilisation de l'objet de stratégie de groupe :

Pour bloquer les lancements de session à partir de fichiers ICA stockés sur le disque local, procédez comme suit :

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 > Moteur client**.
3. Sélectionnez la stratégie **Lancement sécurisé de session de fichier ICA** et définissez-la sur **Activé**.
4. Cliquez sur **Appliquer** et **OK**.

Utilisation du Global App Config Service :

Vous pouvez utiliser Global App Config Service à partir de l'application Citrix Workspace 2106.

Pour bloquer les lancements de session à partir de fichiers ICA stockés sur le disque local, procédez comme suit :

Définissez l'attribut **Block Direct ICA File Launches** sur **True**.

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

Utilisation de Workspace pour Web :

Pour interdire le téléchargement de fichiers ICA sur le disque local lors de l'utilisation de Workspace pour Web, procédez comme suit :

Exécutez le module PowerShell. Consultez [Configurer DisallowICADownload](#).

Remarque :

La stratégie **DisallowICADownload** n'est pas disponible pour les déploiements StoreFront.

Délai d'inactivité pour les sessions Citrix Workspace

Les administrateurs peuvent configurer la valeur de délai d'inactivité pour spécifier la durée d'inactivité autorisée avant que les utilisateurs ne soient déconnectés automatiquement de la session Citrix Workspace. Vous êtes automatiquement déconnecté de Workspace si la souris, le clavier ou la fonction tactile sont inactifs pendant l'intervalle de temps spécifié. Le délai d'inactivité n'affecte pas les sessions d'applications et de bureaux virtuels actives ni les magasins Citrix StoreFront.

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

L'expérience utilisateur est la suivante :

- Une notification apparaît dans la fenêtre de votre session trois minutes avant votre déconnexion, avec la possibilité de rester connecté ou de vous déconnecter.
- La notification n'apparaît que si la valeur de délai d'inactivité configurée est supérieure ou égale à cinq minutes.
- Les utilisateurs peuvent cliquer sur **Rester connecté** pour ignorer la notification et continuer à utiliser l'application, auquel cas le minuteur d'inactivité est réinitialisé à sa valeur configurée. Vous pouvez également cliquer sur **Déconnexion** pour mettre fin à la session du magasin actuel.

Remarque :

Les administrateurs peuvent configurer le délai d'inactivité uniquement pour les sessions Workspace (cloud).

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 diverses technologies sécurisées, dont :

- Citrix Gateway : pour plus d'informations, reportez-vous aux rubriques de cette section et à la documentation Citrix Gateway et StoreFront.
- 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.
- Les versions 1.0 à 1.3 de Transport Layer Security (TLS) sont prises en charge.
- Serveur de confiance pour établir des relations d'approbation avec les connexions à l'application Citrix Workspace.
- Signature de fichier ICA
- Protection de l'autorité de sécurité locale (LSA)
- Serveur proxy pour déploiements de Citrix Virtual Apps uniquement : un serveur proxy SOCKS ou serveur proxy sécurisé. Les serveurs proxy permettent de limiter l'accès au réseau et depuis le réseau. Ils gèrent également 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.
- Proxy sortant

Citrix Gateway

Citrix Gateway (anciennement Access Gateway) sécurise les connexions aux magasins StoreFront. Ce service permet également aux administrateurs de contrôler l'accès des utilisateurs aux bureaux et aux applications de manière détaillée.

Pour se connecter à des bureaux et des applications via Citrix Gateway :

1. Spécifiez l'URL de Citrix Gateway qui vous a été fournie par votre administrateur de l'une des manières suivantes :
 - La première fois que vous utilisez l'interface utilisateur en libre-service, vous êtes invité à entrer l'adresse URL dans la boîte de dialogue **Ajouter compte**.
 - Lorsque vous utilisez l'interface utilisateur en libre-service ultérieurement, entrez l'URL en cliquant sur **Préférences > Comptes > Ajouter**.
 - Si vous établissez une connexion avec la commande storebrowse, entrez l'adresse URL sur la ligne de commande.

L'URL spécifie la passerelle et, éventuellement, un magasin spécifique :

- Pour vous connecter au premier magasin trouvé par l'application Citrix Workspace, utilisez une URL au format suivant :
 - <https://passerelle.société.com>
 - Pour vous connecter à un magasin spécifique, utilisez une URL au format <https://gateway.company.com?storename>. Le format de cette URL dynamique n'est pas un format standard ; n'incluez pas le signe égal (=) dans l'URL. Si vous établissez une connexion à un magasin spécifique avec storebrowse, vous devrez peut-être utiliser des guillemets autour de l'URL dans la commande storebrowse.
1. Lorsque vous y êtes invité, connectez-vous au magasin (via la passerelle) à l'aide de votre nom d'utilisateur, mot de passe et de jeton de sécurité. Pour de plus amples informations sur cette étape, consultez la documentation de Citrix Gateway.

Lorsque l'authentification est terminée, vos bureaux et applications sont affichés.

Connexion via un pare-feu

Les pare-feu de réseau peuvent autoriser ou empêcher le passage des paquets de données en fonction de l'adresse et du port de destination. Si vous utilisez un pare-feu, l'application Citrix Workspace pour Windows peut 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 ou HDX	TCP/UDP	1494	Accès aux applications et bureaux virtuels
ICA ou HDX avec fiabilité de session	TCP/UDP	2598	Accès aux applications et bureaux virtuels
ICA ou HDX sur TLS	TCP/UDP	443	Accès aux applications et bureaux virtuels

Pour plus d'informations sur les ports, consultez l'article [CTX101810](#) du centre de connaissances.

Transport Layer Security (TLS)

Le protocole Transport Layer Security (TLS) remplace le protocole SSL (Secure Sockets Layer). Le groupe de travail Internet Engineering Taskforce (IETF) l'a rebaptisé TLS lorsqu'il est devenu responsable du développement de TLS sous la forme d'une norme ouverte.

TLS garantit la sécurité des communications de données grâce à l'authentification des serveurs, au chiffrement du flux de données et aux contrôles d'intégrité des messages. Certaines organisations, notamment des organisations gouvernementales américaines, requièrent l'utilisation du protocole TLS pour la sécurisation de leurs communications de données. Ces organisations peuvent également exiger l'utilisation d'une cryptographie éprouvée, telle que FIPS 140. La norme FIPS 140 est une norme de cryptographie.

Pour utiliser le chiffrement TLS comme moyen de communication, vous devez configurer la machine utilisateur et l'application Citrix Workspace. Pour plus d'informations sur la sécurisation des communications StoreFront, consultez la section [Sécuriser](#) dans la documentation de StoreFront. Pour plus d'informations sur la sécurisation du VDA, consultez la section [Transport Layer Security \(TLS\)](#) dans la documentation de Citrix Virtual Apps and Desktops.

Vous pouvez utiliser les stratégies suivantes pour :

- Imposer l'utilisation de TLS : nous vous recommandons d'utiliser TLS pour les connexions utilisant des réseaux non approuvés, y compris Internet.
- Imposer l'utilisation de la cryptographie approuvée FIPS (Federal Information Processing Standards) : la cryptographie approuvée suit 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.
- 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.

L'application Citrix Workspace pour Windows prend en charge les suites de chiffrement suivantes pour le protocole TLS 1.2 :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Pour plus d'informations sur les suites de chiffrement prises en charge, consultez l'article [CTX250104](#) du centre de connaissances.

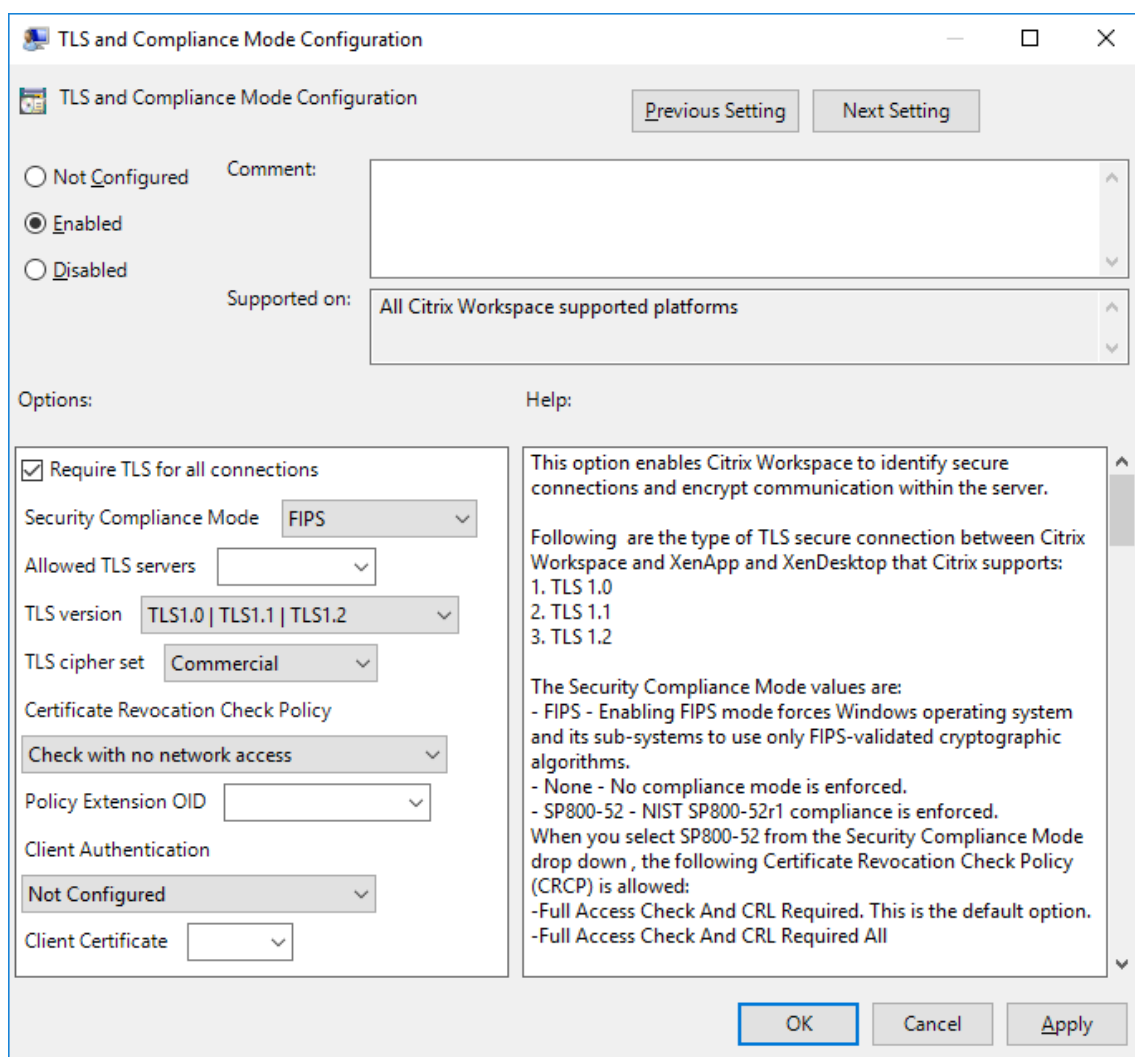
Important :

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

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

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 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 suivent les 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**, définissez le paramètre **Stratégie de vérification de la liste de révocation de certificats** sur **Exiger vérification avec accès complet et liste de révocation de certificats**.

Lorsque vous sélectionnez **SP800-52**, l'application Citrix Workspace vérifie que le certificat de serveur suit les 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. Utilisez une liste séparée par des virgules pour vous assurer que l'application Citrix Workspace se connecte uniquement à un serveur spécifié. 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 ou n'approuve pas l'émetteur, la connexion est refusée.
- d) Dans le menu **Versión 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 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 d'une suite de chiffrement TLS spécifique, sélectionnez Gouvernement (GOV), Commercial (COM) ou Quelconque (ALL). Pour plus d'informations, consultez l'article [CTX250104](#) du centre de connaissances.

- b) 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. Une liste de révocation de certificats pour vérifier le certificat serveur disponible auprès du serveur Relais SSL/Citrix Secure Web Gateway cible n'est pas obligatoire.
 - **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. Une liste de révocation de certificats pour vérifier le certificat de serveur disponible auprès du serveur cible n'est pas critique.
 - **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 vous sélectionnez l'option **OID de l'extension de stratégie**, 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.

Pour plus d'informations sur la matrice des connexions réseau internes et externes, consultez l'article [CTX250104](#) du centre de connaissances.

Serveur approuvé

Imposer des connexions aux serveurs fiables

La stratégie de configuration d'un serveur approuvé identifie et applique les relations d'approbation aux connexions de l'application Citrix Workspace.

À l'aide de cette stratégie, les administrateurs peuvent contrôler la manière dont le client identifie l'application ou le bureau publié auquel il se connecte. Le client détermine un niveau de confiance, appelé région de confiance à chaque connexion. La région de confiance déterminera comment configurer le client pour la connexion.

L'activation de cette stratégie empêche les connexions aux serveurs qui ne se trouvent pas dans les régions de confiance.

Par défaut, l'identification de la région est basée sur l'adresse du serveur auquel le client se connecte. Pour être membre d'une région de confiance, le serveur doit être membre de la zone **Sites de confiance** de Windows. Vous pouvez configurer cela à l'aide du paramètre **Zone Internet Windows**.

L'adresse du serveur peut également être spécifiquement approuvée à l'aide du paramètre **Adresse**. L'adresse du serveur doit être une liste de serveurs séparés par des virgules prenant en charge l'utilisation de caractères génériques, par exemple `cps*.citrix.com`.

Pour activer la configuration des serveurs approuvés avec le modèle d'administration d'objet de stratégie de groupe

Conditions préalables :

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 > 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**. Cette option force le client à effectuer l'identification à l'aide d'un serveur de confiance.
5. Dans le menu déroulant **Zone Internet Windows**, sélectionnez l'adresse client-serveur. Ce paramètre s'applique uniquement à la zone Sites de confiance Windows.
6. Dans le champ **Adresse**, définissez l'adresse client-serveur 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**.

Lorsque cette stratégie est activée et que le serveur ne se trouve pas dans la région de confiance, la connexion est empêchée et un message d'erreur s'affiche.

Le serveur identifié doit être ajouté à la **zone Sites de confiance** Windows pour que la connexion réussisse. Par exemple, ajoutez le serveur en tant que « http:// » ou « https:// » pour les connexions SSL.

Remarque :

Pour les connexions SSL, le nom commun du certificat doit être approuvé. Pour les connexions non SSL, tous les serveurs qui sont contactés doivent être approuvés individuellement.

Assurez-vous également que le nom de domaine complet interne de StoreFront est ajouté à la zone Intranet local ou aux zones Sites de confiance. Pour plus d'informations, consultez **Modifier les paramètres d'Internet Explorer** dans la section [Authentifier](#).

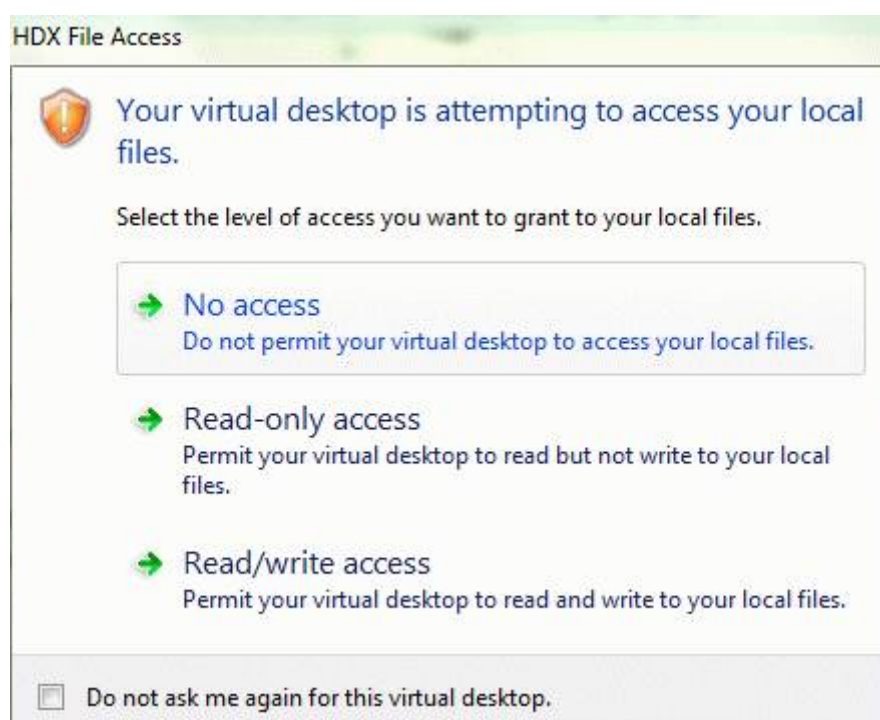
Client Selective Trust

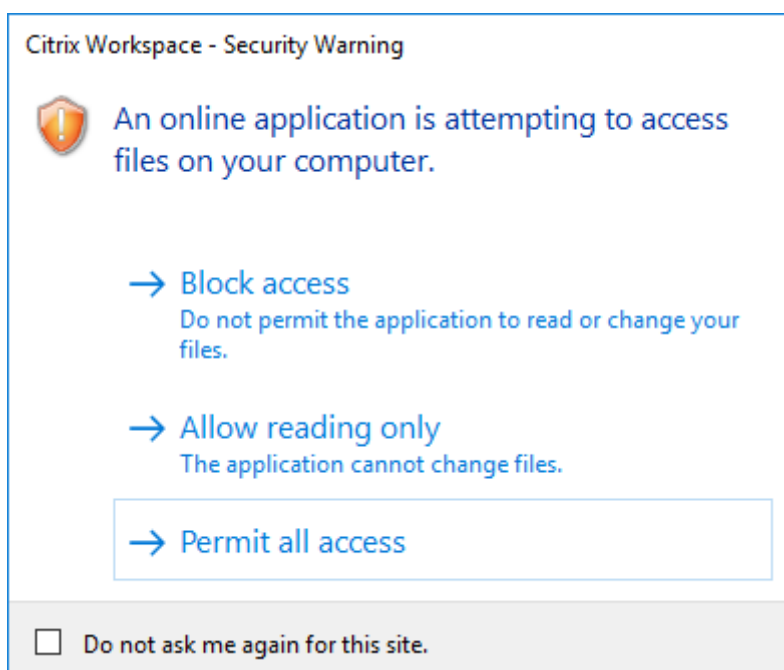
En plus d'autoriser ou d'empêcher les connexions aux serveurs, le client utilise également les régions pour identifier un accès SSO aux fichiers, au microphone ou à la webcam.

Régions	Ressources	Niveau d'accès
Internet	Fichier, microphone, Web	Demande d'accès à l'utilisateur, l'authentification unique SSO n'est pas autorisée
Intranet	Microphone, Web	Demande d'accès à l'utilisateur, l'authentification unique SSO est autorisée

Régions	Ressources	Niveau d'accès
Sites restreints	Tous	Aucun accès et aucune connexion ne peuvent être empêchés
Approuvé	Microphone, Web	Lecture ou écriture, l'authentification unique SSO est autorisée

Lorsque l'utilisateur a sélectionné la valeur par défaut pour une région, la boîte de dialogue suivante peut apparaître :





Les administrateurs peuvent modifier ce comportement par défaut en créant et en configurant les clés de registre **Client Selective Trust** à l'aide de la stratégie de groupe ou dans le registre. Pour plus d'informations sur la configuration des clés de registre Client Selective Trust, consultez l'article [CTX133565](#) du centre de connaissances.

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 fonctionnalité de 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.

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 verte 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 verte. 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 non valide. Le lancement de la session échoue 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, nous vous recommandons 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.
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.

Protection de l'autorité de sécurité locale (LSA)

L'application Citrix Workspace prend en charge la protection de l'autorité de sécurité locale (LSA) de Windows, qui conserve des informations sur tous les aspects de la sécurité locale sur un système. Cette prise en charge fournit le niveau LSA de protection du système pour les bureaux hébergés.

Connexion via un serveur proxy

Les serveurs proxy permettent de limiter l'accès vers et depuis votre réseau et de gérer les connexions entre l'application Citrix Workspace pour 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.

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. Configurez les paramètres **Internet** du navigateur Web par défaut de la machine utilisateur en conséquence.

Pour appliquer les paramètres de proxy via le fichier ICA sur StoreFront, consultez l'article [CTX136516](#) du centre de connaissances.

Prise en charge du proxy ICA sortant

SmartControl permet aux administrateurs de configurer et d'appliquer des stratégies qui affectent l'environnement. Par exemple, vous pouvez interdire aux utilisateurs de mapper des lecteurs sur leurs bureaux distants. Vous pouvez obtenir la granularité nécessaire à l'aide de la fonctionnalité SmartControl sur Citrix Gateway.

Le scénario change lorsque l'application Citrix Workspace et Citrix Gateway appartiennent à des comptes d'entreprise distincts. Dans de tels cas, le domaine client ne peut pas appliquer la fonctionnalité SmartControl car la passerelle n'existe pas sur le domaine. Vous pouvez ensuite utiliser le proxy ICA sortant. La fonctionnalité de proxy ICA sortant vous permet d'utiliser la fonctionnalité SmartControl 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. Utilisez le plug-in proxy sortant pour configurer un seul proxy statique ou sélectionnez un serveur proxy lors de l'exécution.

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 ou 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"
```

Connexions et certificats

Connexions

- Magasin HTTP
- Magasin HTTPS
- Citrix Gateway 10.5 et versions ultérieures

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 :

Un avertissement de certificat non approuvé s'affiche si le certificat de la passerelle distante ne peut pas être vérifié lors de la connexion. Cet avertissement s'affiche lorsque le certificat racine est manquant dans le keystore local. 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 un 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. Utilisez des certificats génériques conformément à la stratégie de sécurité de votre organisation. 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](#).

Liste de révocation de certificats

La liste de révocation de certificats (CRL) permet à l'application Citrix Workspace de vérifier si le certificat du serveur est révoqué. La vérification des certificats 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. Vous pouvez également configurer la vérification des certificats pour permettre aux utilisateurs de n'ouvrir leurs sessions que si toutes les listes de révocation de certificats ont été vérifiées.

Si vous configurez la vérification du certificat sur votre ordinateur local, quittez l'application Citrix Workspace. Vérifiez que tous les composants Citrix Workspace, y compris le **centre de connexion**, sont fermés.

Pour plus d'informations, consultez la section [Transport Layer Security](#).

Prise en charge pour atténuer les attaques de type « man-in-the-middle »

L'application Citrix Workspace pour Windows vous aide à réduire le risque d'une attaque de type « man-in-the-middle » à l'aide de la fonctionnalité d'**épinglage de certificat d'entreprise** de Microsoft Windows. Une attaque « man-in-the-middle » désigne un type de cyberattaque dans le cadre duquel l'attaquant intercepte et relaie secrètement des messages entre deux parties qui pensent communiquer directement entre elles.

Auparavant, lorsque vous contactiez le serveur du magasin, il n'était pas possible de vérifier si la réponse reçue provenait du serveur que vous souhaitiez contacter ou non. À l'aide de la fonctionnalité d'**épinglage de certificat d'entreprise** de Microsoft Windows, vous pouvez vérifier la validité et l'intégrité du serveur en épinglant son certificat.

L'application Citrix Workspace pour Windows est préconfigurée pour savoir quel certificat de serveur elle doit recevoir pour un domaine ou un site particulier à l'aide des règles d'épinglage de certificat. Si le certificat de serveur ne correspond pas au certificat de serveur préconfiguré, l'application Citrix Workspace pour Windows empêche la session d'avoir lieu.

Pour plus d'informations sur le déploiement de la fonctionnalité d'**épinglage de certificat d'entreprise**, consultez la [documentation Microsoft](#).

Remarque :

Vous devez prendre en compte l'expiration du certificat et mettre à jour correctement les stratégies de groupe et les listes de certificats de confiance. Sinon, la session risque de ne pas démarrer, même si aucune attaque n'est présente.

Authentification

April 22, 2024

Vous pouvez configurer plusieurs types d'authentification pour votre application Citrix Workspace, y compris l'authentification pass-through (authentification unique, Single Sign-on ou SSON) au domaine, par carte à puce et pass-through Kerberos.

Authentification par Domain pass-through (Single Sign-On)

L'authentification pass-through au domaine (authentification unique, Single Sign-on ou SSON) vous permet de vous authentifier auprès d'un domaine et d'utiliser Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) sans avoir à vous réauthentifier.

Remarque :

Si vous désactivez la stratégie **Activer les notifications MPR pour le système** dans le modèle d'objet de stratégie de groupe, la fonctionnalité d'authentification pass-through au domaine (Single Sign-On) n'est pas prise en charge sous Windows 11.

Cette fonctionnalité est disponible dans l'application Citrix Workspace pour Windows versions 2012 et ultérieures.

Lorsque cette option est activée, le pass-through au domaine (authentification unique) met en cache vos informations d'identification, afin que vous puissiez vous connecter à d'autres applications Citrix sans avoir à vous connecter à chaque fois. Assurez-vous que seuls les logiciels conformes aux politiques de votre entreprise s'exécutent sur votre appareil afin de limiter le risque de compromission des informations d'identification.

Lorsque vous ouvrez une session sur l'application Citrix Workspace, vos informations d'identification sont transmises à StoreFront avec les applications, les bureaux et les paramètres du menu Démarrer. Après avoir configuré Single Sign-On, vous pouvez ouvrir une session sur l'application Citrix Workspace et lancer des sessions d'applications et de bureaux virtuels sans ressaisir vos informations d'identification.

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 (GPO). Pour plus d'informations sur la configuration de l'authentification unique à l'aide du modèle d'administration d'objet de stratégie de groupe (GPO), 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

- GUI

Remarque :

Les termes authentification pass-through au domaine (ou unique), single sign-on et SSON peuvent être utilisés de manière interchangeable dans ce document.

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

Pour configurer l'authentification Single Sign-On lors d'une nouvelle installation, suivez les étapes suivantes :

1. Configuration sur StoreFront.
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 l'authentification unique sur StoreFront

Single Sign-on vous permet de vous authentifier auprès d'un domaine et d'utiliser Citrix Virtual Apps and Desktops et Citrix DaaS depuis le même domaine sans procéder à une nouvelle authentification pour chaque application ou bureau.

Lorsque vous ajoutez un magasin à l'aide de l'utilitaire **Storebrowse**, vos informations d'identification sont transmises au serveur Citrix Gateway avec les applications et les bureaux énumérés pour vous, y compris les paramètres du menu Démarrer. Après avoir configuré Single Sign-on, vous pouvez ajouter le magasin, énumérer vos applications et bureaux et lancer les ressources nécessaires sans saisir à plusieurs reprises vos informations d'identification.

Selon le déploiement Citrix Virtual Apps and Desktops, l'authentification Single Sign-On peut être configurée sur StoreFront 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	Lancez Citrix Studio, accédez à Magasin > Gérer les méthodes d'authentification - Magasin > activez Authentification pass-through au domaine .	Lorsque l'application Citrix Workspace n'est pas configurée avec Single Sign-On, elle change automatiquement la méthode d'authentification de Par le domaine à Par nom d'utilisateur et mot de passe , le cas échéant.
Lorsque Workspace pour Web est requis	Lancez Magasins > Workspace pour Web > Gérer les méthodes d'authentification - Magasin > activez Authentification pass-through au domaine .	Lorsque l'application Citrix Workspace n'est pas configurée avec Single Sign-On, elle change automatiquement la méthode d'authentification de Par le domaine à Par nom d'utilisateur et mot de passe , 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. Cependant, vous devez vous assurer que vous avez activé l'authentification de base et l'authentification à facteur unique (nFactor avec 1 facteur) sur Citrix Gateway.

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. Sélectionnez **Activé**.
4. Cliquez sur **Appliquer** et **OK**.
5. Redémarrez l'application Citrix Workspace pour que les modifications prennent effet.

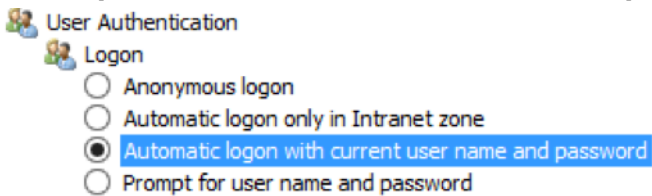
Configurer les services d'approbation XML sur le Delivery Controller

Sur Citrix Virtual Apps and Desktops et Citrix DaaS, 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 ajouter :
 - a) Lancez **Options Internet** à partir du panneau de configuration.
 - b) Cliquez sur **Sécurité > Intranet local**, puis sur **Sites**.
La fenêtre **Intranet Local** s'affiche.
 - c) Sélectionnez **Avancé**.
 - d) Ajoutez l'adresse URL ou le nom de domaine complet de StoreFront avec les protocoles HTTP ou HTTPS appropriés.
 - e) Cliquez sur **Appliquer** et **OK**.

2. Modifiez les paramètres **Authentification utilisateur** dans **Internet Explorer**. Pour modifier :
 - a) Lancez **Options Internet** à partir du panneau de configuration.
 - b) Cliquez sur l'onglet **Sécurité > Intranet local**.
 - c) Cliquez sur **Personnaliser le niveau**. La fenêtre **Paramètres de sécurité—Zone Intranet local** s'affiche.
 - d) Dans le panneau **Authentification utilisateur**, sélectionnez **Ouverture de session automatique avec le nom d'utilisateur et le mot de passe actuel**.
 - e) Cliquez sur **Appliquer** et **OK**.

Configurer Single Sign-On à l'aide de l'interface de ligne de commande

Installez l'application Citrix Workspace avec le commutateur `/includeSSON` et redémarrez-la pour que les modifications prennent effet.

Configurer le Single Sign-On à l'aide de l'interface 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 un magasin existant (ou configurer un nouveau magasin) à l'aide de l'application Citrix Workspace sans fournir d'informations d'identification utilisateur.

Configurer Single Sign-on sur Citrix Workspace pour Web

Vous pouvez configurer Single Sign-on sur Workspace pour Web à l'aide du modèle d'administration d'objet de stratégie de groupe.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de Workspace pour Web en exécutant `gpedit.msc`.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration > Composants Citrix > 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 Single Sign-on est activé. Pour cela, démarrez le **gestionnaire des tâches** et vérifiez si le processus `ssonsvr.exe` est en cours d'exécution.

Configurer Single Sign-on à l'aide d'Active Directory

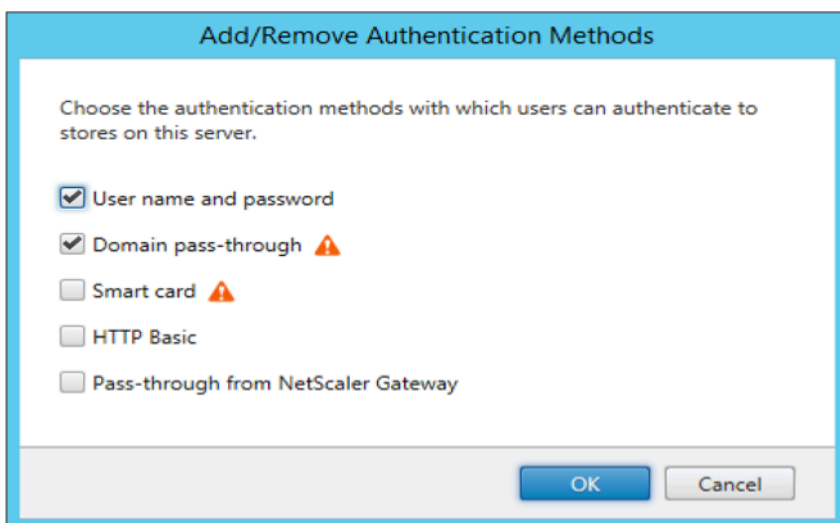
Procédez comme suit pour configurer l'application Citrix Workspace pour l'authentification pass-through à l'aide de la stratégie de groupe Active Directory. Dans ce scénario, vous pouvez obtenir l'authentification Single Sign-on sans utiliser les outils de déploiement de logiciels d'entreprise, tels que Microsoft System Center Configuration Manager.

1. Téléchargez et placez le fichier d'installation de l'application Citrix Workspace ([CitrixWorkspaceApp.exe](#)) sur un partage réseau approprié. Il doit être accessible par les machines cibles sur lesquelles vous installez l'application Citrix Workspace.
2. Obtenez le `CheckAndDeployWorkspacePerMachineStartupScript.bat` modèle à partir de la page [Téléchargement de l'application Citrix Workspace pour Windows](#).
3. Modifiez le contenu pour refléter l'emplacement et la version de `CitrixWorkspaceApp.exe`.
4. Dans la console **Gestion des stratégies de groupe Active Directory**, entrez `CheckAndDeployWorkspacePerMachineStartupScript.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 `receiver.adml`.
6. Après avoir ajouté le modèle `receiver.adml`, accédez à **Configuration ordinateur > Modèles d'administration > Composants Citrix > Citrix Workspace > Authentification utilisateur**. Pour plus d'informations sur l'ajout de fichiers de modèle, consultez la section [Modèle d'administration d'objet de stratégie de groupe](#).
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 l'authentification unique sur StoreFront

Configuration du StoreFront

1. Lancez **Citrix Studio** sur le serveur StoreFront et sélectionnez **Magasins > Gérer les méthodes d'authentification - Magasin**.
2. Sélectionnez **Authentification pass-through au domaine**.



Jetons d'authentification

Les jetons d'authentification sont chiffrés et stockés sur le disque local, de sorte que vous n'avez pas besoin de saisir à nouveau vos informations d'identification lorsque votre système ou votre session redémarre. L'application Citrix Workspace offre une option permettant de désactiver le stockage des jetons d'authentification sur le disque local.

Pour une sécurité renforcée, nous fournissons maintenant une stratégie Objet de stratégie de groupe (GPO) pour configurer le stockage de jetons d'authentification.

Remarque :

Cette configuration ne s'applique qu'aux déploiements dans le cloud.

Pour désactiver le stockage des jetons d'authentification à l'aide de la stratégie Objet de stratégie de groupe (GPO) :

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 > Self-Service**.
3. Dans la stratégie **Stocker les jetons d'authentification**, sélectionnez l'une des options suivantes :
 - **Activé** : indique que les jetons d'authentification sont stockés sur le disque. Par défaut, cette option est définie sur **Activé**.
 - **Désactivé** : indique que les jetons d'authentification ne sont pas stockés sur le disque. Saisissez à nouveau vos informations d'identification lorsque votre système ou votre session redémarre.

4. Cliquez sur **Appliquer** et **OK**.

À compter de la version 2106, l'application Citrix Workspace offre une option supplémentaire permettant de désactiver le stockage des jetons d'authentification sur le disque local. En plus de la configuration d'objet de stratégie de groupe existante, vous pouvez également désactiver le stockage de jetons d'authentification sur le disque local à l'aide du Global App Configuration Service.

Dans Global App Configuration Service, définissez l'attribut **Store Authentication Tokens** sur **False**.

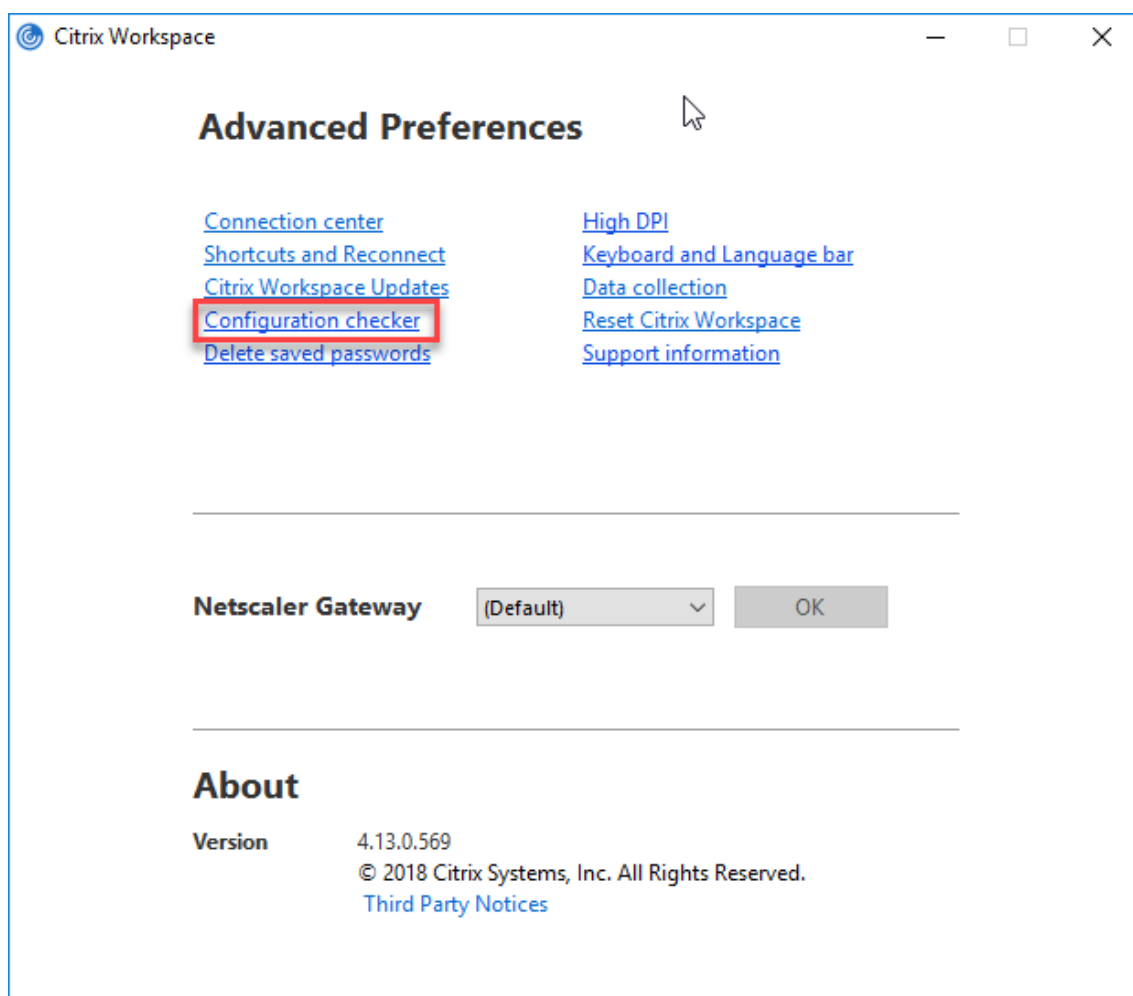
Vous pouvez configurer ce paramètre à l'aide de Global App Configuration Service selon l'une des méthodes suivantes :

- Interface utilisateur (UI) de Global App Configuration service : pour configurer à l'aide de l'interface utilisateur, voir [Configurer l'application Citrix Workspace](#)
- API : pour configurer les paramètres à l'aide d'API, consultez le document [Citrix Developer](#).

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 de 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, pour la réussite et l'échec.

L'utilisateur dispose de plus d'informations sur chaque point de contrôle et les résultats correspondants.

Les tests suivants sont effectués :

1. Installé avec Single Sign-on.
2. Capture des informations d'identification d'ouverture de session.
3. Enregistrement du fournisseur réseau : le résultat du test pour l'enregistrement du fournisseur de réseau affiche une coche verte uniquement si « Citrix Single Sign-On » est défini en tant que premier élément dans la liste des fournisseurs de réseau. Si Citrix Single Sign-On s'affiche ailleurs dans la liste, le résultat de test pour l'inscription du fournisseur réseau s'affiche avec un I bleu et des informations supplémentaires.
4. Processus de Single Sign-On en cours d'exécution.
5. Stratégie de groupe : par défaut, cette stratégie est configurée sur le client.
6. Paramètres Internet pour les zones de sécurité : assurez-vous que vous ajoutez le magasin/l'adresse URL du service XenApp à la liste des zones de sécurité dans les Options Internet. Si les zones de sécurité sont configurées via une stratégie de groupe, toute modification de la stratégie requiert que la fenêtre **Préférences avancées** soit rouverte pour que les modifications soient prises en compte et pour afficher l'état correct du test.
7. Méthode d'authentification pour StoreFront.

Remarque :

- Si vous accédez à Workspace pour Web, les résultats du test ne sont pas applicables.
- Si l'application Citrix Workspace est configurée avec plusieurs magasins, le test de la méthode d'authentification est exécuté sur tous les magasins configurés.
- Vous pouvez enregistrer les résultats du test sous forme de rapports. Le format par défaut du rapport est .txt.

Masquer l'outil d'analyse de la configuration dans la fenêtre Préférences avancées

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant `gpedit.msc`.
2. Accédez à **Composants Citrix > 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`.

Limitation :

L'outil d'analyse de la configuration ne comprend pas le point de contrôle pour la configuration de l'

option Faire confiance aux requêtes envoyées au service XML sur les serveurs Citrix Virtual Apps and Desktops.

Test de balise L'application Citrix Workspace vous permet d'effectuer un test de balise à l'aide du contrôleur de balises disponible dans l'**outil d'analyse de la configuration**. Un test de balise permet de vérifier si la balise (ping.citrix.com) est accessible. Ce test de diagnostic permet d'écartier 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 l'option **Contrôleur de balises** dans la liste de tests et cliquez sur **Exécuter**.

Les résultats du test peuvent être les suivants :

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

Remarque :

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

Authentification pass-through au domaine (Single Sign-On) 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 (Single Sign-on ou SSON) Kerberos pour les déploiements qui utilisent des cartes à puce. Kerberos est l'une des méthodes d'authentification incluses à l'**authentification Windows intégrée (IWA)**.

Lorsque l'authentification Kerberos est activée, Kerberos gère l'authentification sans mots de passe pour l'application Citrix Workspace, ce qui évite les attaques de type cheval de Troie destinées à obtenir les mots de passe sur la machine utilisateur. Les utilisateurs peuvent se connecter à l'aide de n'importe quelle méthode d'authentification et accéder aux ressources publiées, par exemple, un identificateur biométrique tel qu'un lecteur d'empreintes digitales.

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 (anciennement appelé client ICA) transmet le code PIN de la carte à puce au VDA afin de connecter l'utilisateur à la session de l'application Citrix Workspace. Citrix Virtual Apps and Desktops 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 sont 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 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 effectuer une copie de sauvegarde avant de modifier le registre.

Authentification pass-through au domaine (Single Sign-on) avec Kerberos en vue de l'utilisation avec des cartes à puce

Avant de continuer, consultez 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 :

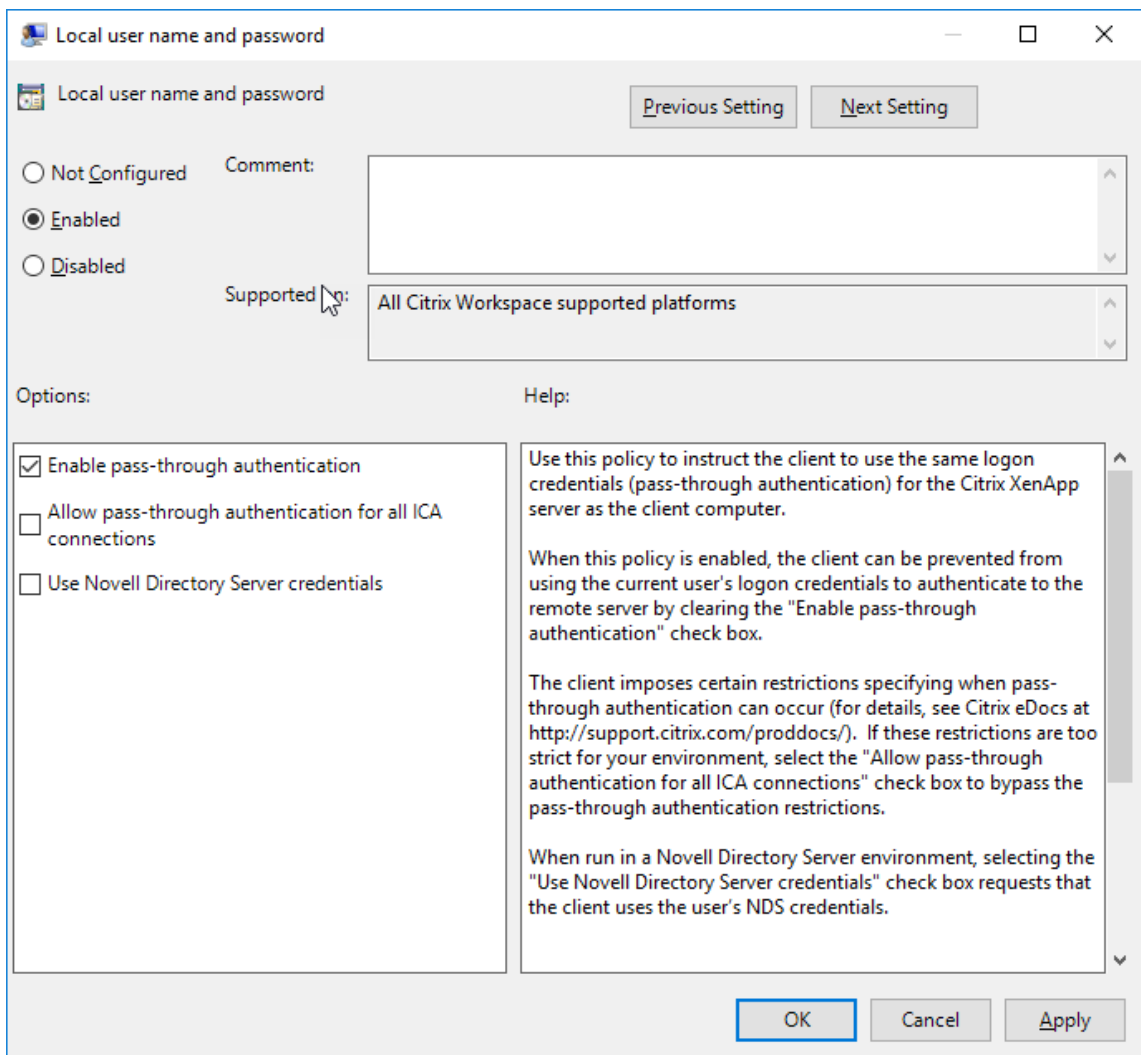
- `/includeSSON`

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.

Prise en charge de l'accès conditionnel avec Azure Active Directory

L'accès conditionnel est un outil utilisé par Azure Active Directory pour appliquer les stratégies d'organisation. Les administrateurs de Workspace peuvent configurer et appliquer les stratégies d'accès conditionnel Azure Active Directory pour les utilisateurs qui s'authentifient auprès de l'application

Citrix Workspace. Microsoft Edge WebView2 Runtime version 99 ou ultérieure doit être installé sur la machine Windows exécutant l'application Citrix Workspace.

Pour obtenir plus de détails et des instructions sur la configuration des stratégies d'accès conditionnel avec Azure Active Directory, consultez la **documentation Azure AD relative à l'accès conditionnel** sur docs.microsoft.com/fr-fr/azure/active-directory/conditional-access/.

Remarque :

Cette fonctionnalité est prise en charge uniquement sur les déploiements Workspace (Cloud).

Prise en charge des méthodes d'authentification modernes pour les magasins StoreFront

Vous pouvez activer la prise en charge des méthodes d'authentification modernes pour les magasins StoreFront à l'aide du modèle d'objet de stratégie de groupe (GPO). Vous pouvez activer cette fonctionnalité à l'aide du service Global App Configuration.

Vous pouvez vous authentifier auprès des magasins Citrix StoreFront de l'une des manières suivantes :

- Utilisation des clés de sécurité Windows Hello et FIDO2. Pour plus d'informations, consultez la section [Autres méthodes d'authentification](#).
- Authentification unique auprès des magasins Citrix StoreFront à partir de machines Azure Active Directory (AAD) jointes avec AAD en tant que fournisseur d'identité. Pour plus d'informations, consultez la section [Autres méthodes d'authentification](#).
- Les administrateurs Workspace peuvent configurer et appliquer les stratégies d'accès conditionnel Azure Active Directory pour les utilisateurs qui s'authentifient sur les magasins Citrix StoreFront. Pour plus d'informations, consultez la section [Prise en charge de l'accès conditionnel avec Azure AD](#).

Pour activer cette fonctionnalité, vous devez utiliser Microsoft Edge WebView2 comme navigateur sous-jacent pour l'authentification directe de StoreFront et de la passerelle.

Remarque :

Assurez-vous que la version de Microsoft Edge WebView2 Runtime est 102 ou ultérieure.

Vous pouvez activer des méthodes d'authentification modernes pour les magasins StoreFront à l'aide de Global App Config Service et du modèle d'objet de stratégie de groupe (GPO).

Utilisation de Global App Config Service

Pour activer cette fonctionnalité :

1. Dans le menu **Citrix Cloud**, sélectionnez **Configuration de l'espace de travail**, puis sélectionnez **Configuration d'applications**.
2. Cliquez sur **Sécurité et authentification**.
3. Assurez-vous que la case **Windows** est cochée.
4. Sélectionnez **Activé** en regard de **Windows** dans la liste déroulante **Microsoft Edge WebView pour l'authentification StoreFront**.

Microsoft Edge WebView For StoreFront Authentication

This policy allows to control the WebView where the StoreFront authentication related web content is loaded. Microsoft Edge WebView2 provides support for modern authentication methods for StoreFront authentication.

<input type="checkbox"/>	Android	This setting is not applicable.
<input type="checkbox"/>	iOS	This setting is not applicable.
<input type="checkbox"/>	Mac	This setting is not applicable.
<input checked="" type="checkbox"/>	Windows	Enabled
<input type="checkbox"/>	HTML5	This setting is not applicable.
<input type="checkbox"/>	Linux	This setting is not applicable.

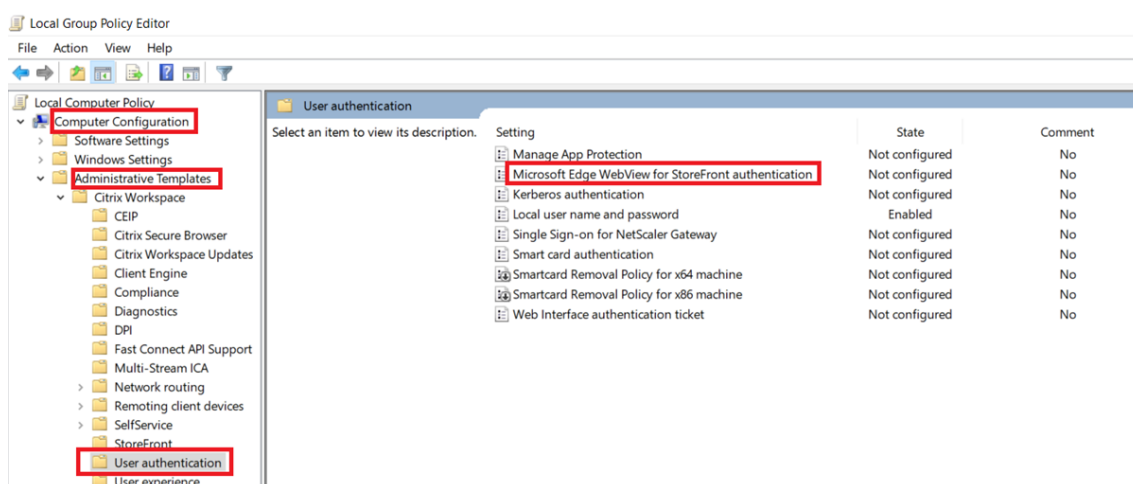
Remarque :

Si vous sélectionnez **Désactivé** en regard de **Windows** dans la liste déroulante **Microsoft Edge WebView pour l'authentification StoreFront**, Internet Explorer WebView est utilisé dans l'application Citrix Workspace. Par conséquent, les méthodes d'authentification modernes pour les magasins Citrix StoreFront ne sont pas prises en charge.

Utilisation de GPO

Pour activer cette fonctionnalité :

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 > Authentification utilisateur**.
3. Cliquez sur la stratégie **Microsoft Edge WebView pour l'authentification StoreFront** et définissez-la sur **Activé**.



4. Cliquez sur **Appliquer**, puis sur **OK**.

Lorsque cette stratégie est désactivée, l'application Citrix Workspace utilise Internet Explorer Web-View. Par conséquent, les méthodes d'authentification modernes pour les magasins Citrix StoreFront ne sont pas prises en charge.

Autres méthodes d'authentification

Vous pouvez configurer les mécanismes d'authentification suivants avec l'application Citrix Workspace. Pour que les mécanismes d'authentification suivants fonctionnent comme prévu, Microsoft Edge WebView2 Runtime version 99 ou version ultérieure doit être installé sur la machine Windows exécutant l'application Citrix Workspace.

1. Authentification basée sur Windows Hello : pour obtenir des instructions sur la configuration de l'authentification basée sur Windows Hello, consultez la section **Configurer les paramètres de Windows Hello Entreprise - Certificat d'autorisation** (docs.microsoft.com/fr-fr/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings).

Remarque :

L'authentification basée sur Windows Hello avec pass-through au domaine (Single Sign-on ou SSON) n'est pas prise en charge.

2. Authentification basée sur les clés de sécurité FIDO2 : les clés de sécurité FIDO2 permettent aux employés de l'entreprise de s'authentifier sans entrer de nom d'utilisateur ou de mot de passe. Vous pouvez configurer l'authentification basée sur les clés de sécurité FIDO2 sur Citrix Workspace. Si vous souhaitez que vos utilisateurs s'authentifient auprès de Citrix Workspace avec leur compte Azure AD à l'aide d'une clé de sécurité FIDO2, consultez la section **Activer la connexion par clé de sécurité sans mot de passe** (docs.microsoft.com/fr-fr/azure/active-directory/authentication/howto-authentication-passwordless-security-key).

3. Vous pouvez également configurer l'authentification unique (SSO) auprès de l'application Citrix Workspace à partir de machines Azure Active Directory (AAD) jointes avec AAD en tant que fournisseur d'identité. Pour de plus amples informations sur la configuration d'Azure Active Directory Domain Services, consultez **Présentation d'Azure Active Directory Domain Services** sur docs.microsoft.com/fr-fr/azure/active-directory-domain-services/overview. Pour plus d'informations sur la façon de connecter Azure Active Directory à Citrix Cloud, consultez la section [Connecter Azure Active Directory à Citrix Cloud](#).

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 à l'aide de la carte à puce peuvent démarrer des applications et des bureaux virtuels sans avoir à se réauthentifier.
 - L'application Citrix Workspace qui s'exécute sur des machines n'appartenant pas au domaine avec des informations d'identification de carte à puce doivent de nouveau entrer leurs informations d'identification pour démarrer une application ou un bureau virtuel.

L'authentification pass-through requiert une configuration sur StoreFront et l'application Citrix Workspace.

- **Authentification bimodale** : avec l'authentification bimodale, les utilisateurs peuvent choisir d'utiliser une carte à puce ou d'entrer leurs nom d'utilisateur et mot de passe. Cette fonctionnalité est utile lorsque vous ne pouvez pas utiliser de carte à puce. Par exemple, le certificat d'ouverture de session a expiré. Des magasins dédiés doivent être configurés pour chaque site pour permettre l'authentification bimodale et la méthode **DisableCtrlAltDel** doit être définie sur **False** pour autoriser les cartes à puce. L'authentification bimodale requiert la configuration de StoreFront.

L'authentification bimodale permet à l'administrateur StoreFront de proposer à 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 utilisés pour une seule carte à puce et si plusieurs cartes à puce sont utilisées. Lorsque vous insérez une carte à puce dans un lecteur

de cartes, les certificats s'appliquent à toutes les applications qui s'exécutent sur la machine utilisateur, y compris l'application Citrix Workspace.

- **Authentification du certificat client** : l'authentification du certificat client requiert la configuration de Citrix Gateway et de StoreFront.
 - Pour accéder à StoreFront via Citrix Gateway, vous devez vous ré-authentifier après le retrait de la 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.
- **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 pendant la session utilisateur et n'est pas stocké sur le disque.
- L'application Citrix Workspace ne reconnecte pas une session lorsqu'une carte à puce est insérée.
- Lorsqu'elle est configurée pour utiliser l'authentification par carte à puce, l'application Citrix Workspace ne prend pas en charge l'authentification unique avec réseau privé virtuel (VPN) ou le pré-lancement de session. Pour utiliser un VPN avec une authentification par carte à puce, installez le plug-in Citrix Gateway. Ouvrez une session via une page Web à l'aide de cartes à puce et de 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 possibilité de résoudre les problèmes

provenant d'une mauvaise utilisation de l'Éditeur du Registre. Veillez à effectuer une copie de sauvegarde avant de modifier le registre.

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.

- Dans l'Éditeur du Registre, accédez au chemin suivant et définissez la chaîne `SSONCheckEnabled` sur `False` si le composant d'authentification unique n'est pas installé.

```
HKEY_CURRENT_USER\Software{ Wow6432 } \Citrix\AuthManager\protocols  
\integratedwindows\
```

```
HKEY_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\  
protocols\integratedwindows\
```

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.

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 d'authentification différente, par exemple, un nom d'utilisateur et un mot de passe, la ligne de commande est la suivante :

```
/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
```

Ce type d'authentification empêche la capture des informations d'identification au moment de l'ouverture de session et permet à l'application Citrix Workspace de stocker 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 `SmartCardDefault` ou `LatestExpiry` suivante à la clé de registre `HKEY_CURRENT_USER OR HKEY_LOCAL_MACHINE\Software\[Wow6432Node\Citrix\AuthManager:CertificateSelectionMode={Prompt`

•

Les valeurs définies dans la `HKEY_CURRENT_USER` ont priorité sur les valeurs définies dans la `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 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\AuthManager : SmartCardPINEntry=CSP`.

Modifications de la prise en charge et du retrait des cartes à puce

Une session Citrix Virtual Apps se déconnecte lorsque vous retirez la carte à puce. Si l'application Citrix Workspace est configuré avec l'authentification par carte à puce, configurez la stratégie correspondante sur l'application Citrix Workspace pour Windows pour appliquer la fermeture de session de Citrix Virtual Apps. L'utilisateur reste connecté à la session de l'application Citrix Workspace.

Limitation :

Lorsque vous ouvrez une session sur l'application Citrix Workspace à l'aide de l'authentification par carte à puce, le nom d'utilisateur est affiché comme **Session ouverte**.

Carte à puce rapide La carte à puce rapide constitue une amélioration par rapport à la redirection de carte à puce PC/SC HDX existante. Elle améliore les performances lorsque les cartes à puce sont utilisées dans des environnements WAN à latence élevée.

Les cartes à puce rapides sont uniquement prises en charge sur Windows VDA.

Pour activer une connexion par carte à puce rapide sur l'application Citrix Workspace :

La connexion par carte à puce rapide est activée par défaut sur le VDA et désactivée par défaut sur l'application Citrix Workspace. Pour activer une connexion par carte à puce rapide, incluez le paramètre suivant dans le fichier **default.ica** du site StoreFront associé :

```
1 copy[WFClient]
2 SmartCardCryptographicRedirection=On
3 <!--NeedCopy-->
```

Pour désactiver la connexion par carte à puce rapide sur l'application Citrix Workspace :

Pour désactiver la connexion par carte à puce rapide sur l'application Citrix Workspace, supprimez le paramètre **SmartCardCryptographicRedirection** du fichier **default.ica** du site StoreFront associé.

Pour de plus amples informations, consultez la section [Cartes à puce](#).

Authentification silencieuse pour Citrix Workspace

L'application Citrix Workspace introduit une stratégie d'objet de stratégie de groupe (GPO) pour activer l'authentification silencieuse pour Citrix Workspace. Cette stratégie permet à l'application Citrix Workspace de se connecter automatiquement à Citrix Workspace au démarrage du système. Utilisez cette stratégie uniquement lorsque le pass-through au domaine (authentification unique, Single Sign-on ou SSON) est configuré pour Citrix Workspace sur des appareils joints à un domaine. Cette fonctionnalité est disponible dans l'application Citrix Workspace pour Windows versions 2012 et ultérieures.

Pour que cette stratégie fonctionne, les critères suivants doivent être respectés :

- L'authentification unique doit être activée.
- La clé **SelfServiceMode** doit être définie sur **Off** dans l'éditeur du Registre.

Activation de l'authentification silencieuse :

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**.
3. Cliquez sur la stratégie **Authentification silencieuse pour Citrix Workspace** et définissez la valeur sur **Activé**.
4. Cliquez sur **Appliquer** et **OK**.

Empêcher l'application Citrix Workspace pour Windows de mettre les mots de passe et les noms d'utilisateur en cache

Par défaut, l'application Citrix Workspace pour Windows remplit automatiquement le dernier nom d'utilisateur saisi. Pour effacer le remplissage automatique du champ du nom d'utilisateur, modifiez le registre sur la machine utilisateur :

1. Créez une valeur REG_SZ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\RememberUsername.
2. Définissez sa valeur sur false.

Pour désactiver la case à cocher **Mémoriser mon mot de passe** et empêcher une connexion automatique, créez la clé de registre suivante sur la machine cliente sur laquelle l'application Citrix Workspace pour Windows est installée :

- Chemin : HKEY_LOCAL_MACHINE\Software\wow6432node\Citrix\AuthManager
- Type : REG_SZ
- Nom : SavePasswordMode
- Valeur : Never

Remarque :

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 effectuer une copie de sauvegarde avant de modifier le registre.

Pour empêcher la mise en cache des informations d'identification pour les magasins StoreFront, consultez [Empêcher l'application Citrix Workspace pour Windows de mettre les mots de passe et les noms d'utilisateur en cache](#) dans la documentation StoreFront.

Prise en charge de plus de 200 groupes dans Azure AD

Avec cette version, un utilisateur d'Azure AD faisant partie de plus de 200 groupes peut voir les applications et les bureaux qui lui sont attribués. Auparavant, le même utilisateur ne pouvait pas voir ces

applications et ces bureaux.

Remarque :

Les utilisateurs doivent se déconnecter de l'application Citrix Workspace et se reconnecter pour activer cette fonctionnalité.

Prise en charge de l'authentification par proxy

Auparavant, sur les machines clientes configurées pour l'authentification par proxy, si les informations d'identification de proxy n'étaient pas stockées dans le **Gestionnaire d'informations d'identification Windows**, vous ne pouviez pas vous authentifier auprès de l'application Citrix Workspace.

À partir de l'application Citrix Workspace version 2102, sur les machines clientes configurées pour l'authentification proxy, si les informations d'identification de proxy ne sont pas stockées dans le **Gestionnaire d'informations d'identification de Windows**, une invite d'authentification s'affiche et vous demande d'entrer les informations d'identification de proxy. L'application Citrix Workspace enregistre ensuite les informations d'identification du serveur proxy dans le **Gestionnaire d'informations d'identification Windows**. Cela se traduit par une expérience de connexion transparente car vous n'avez pas besoin d'enregistrer manuellement vos informations d'identification dans le Gestionnaire d'informations d'identification Windows avant d'accéder à l'application Citrix Workspace.

User-Agent

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

Remarque :

Les numéros de version mentionnés dans le cadre des éléments User-Agent dans le tableau suivant sont des exemples et sont automatiquement mis à jour en fonction des versions que vous utilisez.

Le tableau suivant répertorie le scénario, la description et l'élément User-Agent correspondant pour chaque scénario :

Scénario	Description	User-Agent
Requêtes HTTP classiques	En général, une requête réseau émise par l'application Citrix Workspace contient un élément user-agent. Par exemple, des requêtes réseau telles que <code>GET /Citrix/Roaming/Accounts</code> et <code>GET /AGServices/discover</code> .	<code>CitrixReceiver/23.5.0.63 Windows/10.0 (22H2 Build 19045.2965) SelfService/23.5.0.63 (Release)X1Class CWACapable</code>
Magasins cloud	Lorsqu'un utilisateur s'authentifie auprès d'un magasin cloud dans l'application Citrix Workspace, les requêtes réseau sont effectuées avec un élément user-agent spécifique. Par exemple, des requêtes réseau avec le chemin <code>/core/connect/authorize</code> .	<code>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50 CWA/23.5.0.63 Windows/10.0 (22H2 Build 19045.2965)</code>
Magasin local avec Gateway Advanced Auth à l'aide d'Edge WebView	Lorsqu'un utilisateur s'authentifie auprès de Gateway avec la configuration Advanced Auth sur l'application Citrix Workspace à l'aide d'Edge WebView, les requêtes réseau sont effectuées avec un élément user-agent spécifique. Par exemple, des requêtes réseau telles que <code>GET /nf/auth/doWebview.do</code> et <code>GET /logon/LogonPoint/tmindex.html</code> .	<code>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.54 CWAWEBVIEW/23.2.0.2111 Windows/10.0 (22H2 Build 19045.2364)</code>

Scénario	Description	User-Agent
Magasin local avec Gateway Advanced Auth à l'aide d'IE WebView	Lorsqu'un utilisateur s'authentifie auprès de Gateway avec la configuration Advanced Auth sur l'application Citrix Workspace à l'aide d'Internet Explorer WebView, les requêtes réseau sont effectuées avec un élément user-agent spécifique. Par exemple, des requêtes réseau telles que <code>GET /nf/auth/doWebview.do</code> et <code>GET /logon/LogonPoint/tmindex.html</code> .	<code>Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko, CWAWEVIEW/23.5.0.43</code>
Magasin Web personnalisé	Lorsqu'un utilisateur ajoute un magasin Web personnalisé à l'application Citrix Workspace, l'application envoie un élément user-agent.	<code>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50 CWA/23.5.0.63 Windows/10.0 (22H2 Build 19045.2965)</code>

Matrice d'authentification pass-through au domaine

April 22, 2024

Si vous utilisez Citrix Workspace et que vous souhaitez obtenir une authentification pass-through au domaine, les tableaux des sous-sections décrivent les différents scénarios et indiquent si vous pouvez réaliser l'authentification pass-through au domaine pour chaque scénario.

Voici les différents éléments d'en-tête des tableaux, ainsi que des informations supplémentaires sur ces éléments :

- Point de terminaison joint à : spécifie le répertoire auquel le point de terminaison est joint. Le

répertoire fournit un contrôle d'accès aux ressources locales. Il peut s'agir du répertoire Active Directory (AD) local, du répertoire Azure Active Directory (AAD) ou d'un système hybride.

- Fournisseur d'identité (IdP) : entité utilisée pour fournir des services d'authentification à Citrix Workspace. Elle vous permet de vous connecter aux ressources.
- Federated Authentication Service (FAS) : pour plus d'informations, consultez [Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix](#).
- Virtual Delivery Agent (VDA) : pour plus d'informations, consultez [Installer les VDA](#).
- VDA joint à : spécifie le répertoire auquel l'appareil VDA est joint. Pour de plus amples informations, consultez la section [Gestion des identités et des accès](#).
- SSO (Single Sign-On) vers Citrix Workspace/VDA : la valeur Oui ou Non indique si l'authentification pass-through au domaine vers Citrix Workspace ou le VDA est pris en charge.
- Application Citrix Workspace : pour obtenir Single Sign-On ou l'authentification unique, consultez la section [Configurer l'authentification Single Sign-On lors d'une nouvelle installation dans Authentification pass-through au domaine](#).

Remarque :

Vous pouvez avoir besoin de la dernière version de l'application Citrix Workspace pour bénéficier de la prise en charge de l'authentification pass-through au domaine dans certains des scénarios suivants.

Prise en charge de l'authentification pass-through au domaine pour Citrix Workspace

Point de terminaison joint à	Fournisseur d'identité	VDA joint à	SSO vers Citrix Workspace	SSO vers VDA	Documentation
AD	Passerelle Citrix Gateway locale	AD	Oui	Application Citrix Workspace/FAS	Authentification pass-through au domaine pour Citrix Workspace à l'aide d'une instance Citrix Gateway locale en tant que fournisseur d'identité

Point de terminaison joint à	Fournisseur d'identité	VDA joint à	SSO vers Citrix Workspace	SSO vers VDA	Documentation
AD	Authentification AD adaptative		Oui	Application Citrix Workspace/FAS	Pour configurer l'authentification adaptative, consultez la section Service d'authentification adaptative et suivez les instructions de la section Authentification pass-through au domaine pour Citrix Workspace en utilisant un Citrix Gateway local en tant que fournisseur d'identité.

Point de terminaison joint à	Fournisseur d'identité	VDA joint à	SSO vers Citrix Workspace	SSO vers VDA	Documentation
AD	Citrix Gateway fédéré vers un autre fournisseur d'identité (AAD/Okta)	AD	Oui	Application Citrix Workspace/FAS	Configurez le fournisseur d'identité à l'aide de la section Configurer l'authentification unique SAML et reportez-vous à la documentation du fournisseur d'identité utilisé pour configurer l'authentification pass-through au domaine. Authentification pass-through au domaine pour Citrix Workspace en utilisant Okta en tant que fournisseur d'identité
AD	Okta	AD	Oui	Application Citrix Workspace/FAS	

Point de terminaison joint à	Fournisseur d'identité	VDA joint à	SSO vers Citrix Workspace	SSO vers VDA	Documentation
Joint à AD/Hybride	AAD (AD avec AAD Connect)	AD	Oui	Application Citrix Workspace/FAS **	Authentification pass-through au domaine pour Citrix Workspace en utilisant Azure Active Directory en tant que fournisseur d'identité
AD	Tout fournisseur d'identité basé sur SAML (par exemple, ADFS)	AD	Oui	Application Citrix Workspace/FAS	Consultez Connecter SAML en tant que fournisseur d'identité à Citrix Cloud et reportez-vous à la documentation relative au fournisseur d'identité utilisé pour configurer l'authentification pass-through au domaine.
AD	AD	AD	Non	Non pris en charge	SO
AD	AD + OTP	AD	Non	Non pris en charge	SO
AD	AAD	AAD	Non	Non pris en charge	SO

Point de terminaison joint à	Fournisseur d'identité	VDA joint à	SSO vers Citrix Workspace	SSO vers VDA	Documentation
AAD	AAD sans domaine AD local	AD	Oui	FAS	Citrix Workspace utilise Microsoft Edge WebView qui permet l'authentification unique (SSO) sur Workspace. L'authentification unique (SSO) vers VDA est prise en charge via FAS. Pour plus d'informations, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

Point de terminaison joint à	Fournisseur d'identité	VDA joint à	SSO vers Citrix Workspace	SSO vers VDA	Documentation
AAD	AAD	AAD	Oui	L'utilisateur doit saisir ses informations d'identification	Citrix Workspace utilise Microsoft Edge WebView qui permet l'authentification unique (SSO) sur Workspace. L'authentification unique (SSO) au VDA n'est pas prise en charge.

Point de terminaison joint à	Fournisseur d'identité	VDA joint à	SSO vers Citrix Workspace	SSO vers VDA	Documentation
Non-joint à un domaine	Fournisseur d'identité prenant en charge l'authentification sans mot de passe - lien	AD	Non	FAS	Citrix Workspace utilise Microsoft Edge WebView qui permet l'authentification unique (SSO) sur Workspace. L'authentification unique (SSO) vers VDA est prise en charge via FAS. Pour plus d'informations, consultez la section Autres méthodes d'authentification auprès de Citrix Workspace .

Remarques :

- Le domaine AD doit pouvoir accéder au client pour que Kerberos fonctionne.
- **Citrix Single Sign-On (SSONSVR.exe) fonctionne uniquement avec le nom d'utilisateur ou le mot de passe du client. Si l'utilisateur utilise Windows Hello pour se connecter, le Service d'authentification fédérée (FAS) est requis.
- L'authentification peut ne pas être totalement silencieuse dans le cloud si LLT est activé ou si la stratégie d'acceptation de l'utilisateur final est configurée.

- Il est recommandé de configurer FAS tel qu'il s'applique aux plates-formes autres que Windows.

Prise en charge de l'authentification pass-through au domaine pour StoreFront

Point de terminaison joint à	Fournisseur d'identité	VDA joint à	SSO vers Citrix Workspace	SSO vers VDA	Documentation
AD	StoreFront	AD	Oui	Application Citrix Workspace	Authentification pass-through au domaine
Joint à AD/Hybrid/Windows Hello Entreprise	StoreFront	AD	Oui(1)	Application Citrix Workspace /FAS (2)	Authentification pass-through au domaine et Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix
AD	Citrix Gateway - Authentification avancée	AD	Oui	Application Citrix Workspace(3)	
AD	Citrix Gateway - Authentification de base	AD	Oui	Application Citrix Workspace(4)	Authentification pass-through au domaine

Remarques :

1. Dans l'Éditeur du Registre, accédez au chemin suivant et définissez la chaîne `SSONCheckEnabled` sur `False` si le composant d'authentification unique n'est pas installé.

`HKEY_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\protocols\integratedwindows\`

The key prevents the Citrix Workspace app authentication manager from checking for the

- single sign-on component and allows Citrix Workspace app to authenticate to StoreFront.
2. Si vous utilisez Windows Hello pour vous connecter, le Service d'authentification fédérée (FAS) est requis et la configuration du registre est requise pour activer l'authentification unique (SSO).
 3. Le domaine AD doit pouvoir accéder au client car il utilise Kerberos.
 4. Fonctionne même si le domaine AD ne peut pas accéder au client. N'utilise pas Kerberos.

Authentification pass-through au domaine pour Citrix Workspace en utilisant un Citrix Gateway local en tant que fournisseur d'identité

April 22, 2024

Important :

Cet article vous aide à configurer l'authentification pass-through au domaine. Si vous avez déjà configuré un Gateway local en tant que fournisseur d'identité, passez à la section [Configurer l'authentification pass-through en tant que méthode d'authentification dans Citrix Gateway](#).

Citrix Cloud prend en charge l'utilisation d'un Citrix Gateway local en tant que fournisseur d'identité pour authentifier les abonnés qui se connectent à leurs espaces de travail.

En utilisant l'authentification Citrix Gateway, vous pouvez :

- Continuer à authentifier les utilisateurs via votre Citrix Gateway existant afin qu'ils puissent accéder aux ressources de votre déploiement local d'applications et de bureaux virtuels via Citrix Workspace.
- Utilisez les fonctions d'authentification, d'autorisation et d'audit de Citrix Gateway avec Citrix Workspace.
- Fournissez à vos utilisateurs l'accès aux ressources dont ils ont besoin via Citrix Workspace en utilisant des fonctions telles que l'authentification unique, les cartes à puce, les jetons sécurisés, les stratégies d'accès conditionnel, la fédération.

L'authentification Citrix Gateway est prise en charge pour une utilisation avec les versions de produit suivantes :

- Citrix Gateway 13.1.4.43 Édition Advanced ou ultérieure

Pré-requis :

- Cloud Connector - Vous devez disposer d'au moins deux serveurs sur lesquels installer le logiciel Citrix Cloud Connector.

- Active Directory et assurez-vous que le domaine est enregistré.
- Configuration requise pour Citrix Gateway
 - Utilisez des stratégies avancées sur le Gateway local en raison de la dépréciation des stratégies classiques.
 - Lors de la configuration de Gateway pour l'authentification des abonnés à Citrix Workspace, Gateway agit en tant que fournisseur OpenID Connect. Les messages entre Citrix Cloud et Gateway sont conformes au protocole OIDC, qui inclut la signature numérique de jetons. Par conséquent, vous devez configurer un certificat pour signer ces jetons.
 - Synchronisation de l'horloge : Citrix Gateway doit être synchronisé avec l'heure NTP.

Pour plus de détails, consultez la section [Pré-requis](#) dans la documentation Citrix Cloud.

Avant de créer la stratégie d'authentification de fournisseur d'identité, vous devez d'abord configurer Citrix Workspace ou Cloud pour utiliser Gateway comme option d'authentification dans le fournisseur d'identité. Pour plus d'informations sur la configuration, consultez [Connecter un Citrix Gateway local à Citrix Cloud](#). Lorsque vous avez terminé la configuration, l'ID client, le code secret et l'URL de redirection nécessaires à la création de la stratégie d'authentification de fournisseur d'identité sont générés.

L'authentification pass-through au domaine pour Workspace pour Web est activée si vous utilisez Internet Explorer, Microsoft Edge, Mozilla Firefox et Google Chrome. L'authentification pass-through au domaine n'est activée que lorsque le client est détecté avec succès.

Remarque :

Si le client HTML5 est préféré par un utilisateur ou est appliqué par l'administrateur, la méthode d'authentification pass-through du domaine n'est pas activée.

Lorsque vous lancez l'URL StoreFront dans un navigateur, l'invite **Detect Receiver** s'affiche.

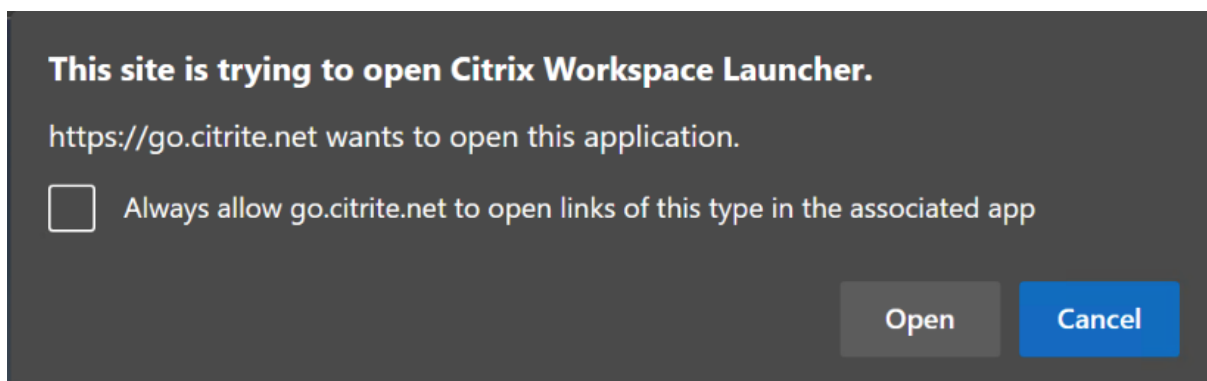
Si les appareils sont gérés, configurez la stratégie de groupe pour désactiver cette invite au lieu de désactiver la détection des clients. Pour plus d'informations, consultez :

- [URLAllowList](#) dans la documentation Microsoft.
- [URLAllowList](#) dans la documentation de Google Chrome.

Remarque :

Le gestionnaire de protocole utilisé par l'application Citrix Workspace est **receiver:**. Configurez-le en tant qu'URL autorisée.

Les utilisateurs peuvent également cocher la case comme indiqué dans l'exemple suivant d'invite d'URL StoreFront dans l'invite de détection de client. L'activation de cette case à cocher permet également de contourner l'invite pour les lancements suivants.



Les étapes suivantes expliquent comment Citrix Gateway peut être configuré en tant que fournisseur d'identité.

Créer une stratégie d'authentification de fournisseur d'identité sur le Citrix Gateway local

La création d'une stratégie d'authentification de fournisseur d'identité implique les tâches suivantes :

1. Créer un profil d'authentification de fournisseur d'identité
2. Ajouter une stratégie d'authentification de fournisseur d'identité
3. Lier la stratégie d'authentification de fournisseur d'identité à un serveur virtuel
4. Lier le certificat globalement

Créer un profil d'authentification de fournisseur d'identité

1. Pour créer un profil d'authentification de fournisseur d'identité à l'aide de l'interface de ligne de commande, tapez ce qui suit dans l'invite de commande :

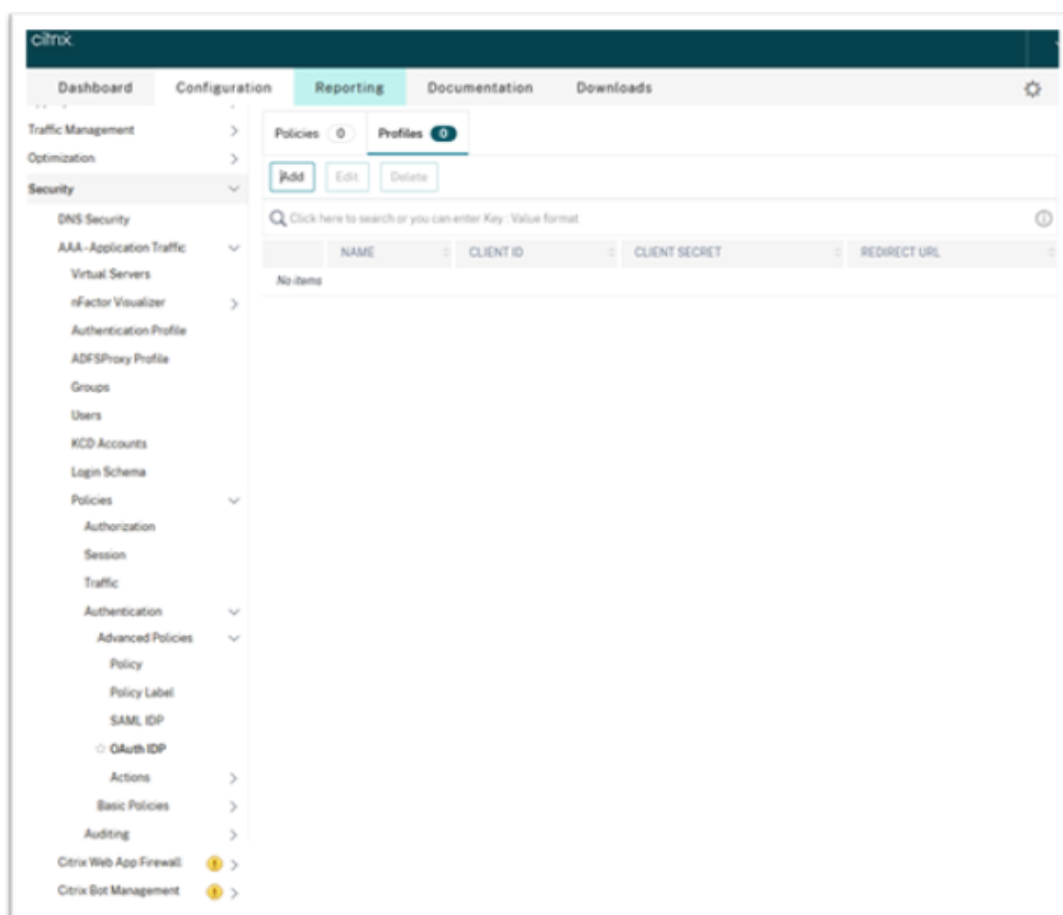
```
1 add authentication OAuthIdPProfile <name> [-clientID <string>] [-  
  clientSecret ] [-redirectURL <URL>] [-issuer <string>] [-audience  
  <string>] [-skewTime <mins>] [-defaultAuthenticationGroup <  
  string>]  
2  
3 add authentication OAuthIdPPolicy <name> -rule <expression> [-  
  action <string> [-undefAction <string>] [-comment <string>] [-  
  logAction <string>]  
4  
5 add authentication ldapAction <name> -serverIP <IP> -ldapBase "dc=  
  aaa,dc=local"  
6  
7 ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password  
  > -ldapLoginName sAMAccountName  
8
```



```
9 add authentication policy <name> -rule <expression> -action <
  string>
10
11 bind authentication vserver auth_vs -policy <ldap_policy_name> -
  priority <integer> -gotoPriorityExpression NEXT
12
13 bind authentication vserver auth_vs -policy <OAuthIdPPolicyName> -
  priority <integer> -gotoPriorityExpression END
14
15 bind vpn global -certkey <>
16
17 <!--NeedCopy-->
```

2. Pour créer un profil d'authentification de fournisseur d'identité à l'aide de l'interface graphique :

a) Connectez-vous à votre portail de gestion Citrix Gateway local et accédez à **Security > AAA –Application Traffic > Policies > Authentication > Advanced Policies > OAuth IDP**.



b) Dans la page **OAuth IdP**, cliquez sur l'onglet **Profiles**, puis sur **Add**.

c) Configurez le profil OAuth IdP.

Remarque :

- Copiez et collez les valeurs d’ID client, de secret et d’URL de redirection depuis **Citrix Cloud > Gestion des identités et des accès > Authentification** pour établir la connexion à Citrix Cloud.
- Entrez correctement l’URL de la passerelle dans le champ **Nom de l’émetteur**. Par exemple, <https://GatewayFQDN.com>.
- Copiez et collez également l’identifiant du client dans le champ **Audience**.
- **Send Password** : activez cette option pour la prise en charge de l’authentification unique. Par défaut, cette option est désactivée.

d) Dans l’écran **Create Authentication OAuth IdP Profile**, définissez des valeurs pour les paramètres suivants et cliquez sur **Create**.

- **Name** : nom du profil d’authentification. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_). Le nom ne doit contenir que des lettres, des chiffres et le tiret (-), le point (.) la livre (#), l’espace (), l’arobase (@), le signe égal à (=), deux-points (:) et des caractères de soulignement. Vous ne pouvez pas modifier le nom une fois le profil créé.
- **Client ID** : chaîne unique qui identifie le fournisseur de services. Le serveur d’autorisation déduit la configuration du client en utilisant cet ID. Longueur maximale : 127.
- **Client Secret** : chaîne secrète établie par l’utilisateur et le serveur d’autorisation. Longueur maximale : 239.
- **Redirect URL** : point de terminaison sur le fournisseur de services sur lequel le code/jeton doit être publié.
- **Issuer Name** : identité du serveur dont les jetons doivent être acceptés. Longueur maximale : 127. Exemple : <https://GatewayFQDN.com>.
- **Audience** : destinataire cible du jeton envoyé par l’IdP. Le destinataire vérifie ce jeton.
- **Skew Time** : cette option spécifie le décalage d’horloge autorisé (en minutes) que Citrix ADC autorise sur un jeton entrant. Par exemple, si SkewTime est 10, le jeton est valide de (heure actuelle - 10) minutes à (heure actuelle + 10) minutes, soit 20 minutes en tout. Valeur par défaut : 5
- **Default Authentication Group** : groupe ajouté à la liste des groupes internes de la session lorsque ce profil est choisi par le fournisseur d’identité et peut être utilisé dans le flux nFactor. Il peut être utilisé dans l’expression (AAA.USER.IS_MEMBER_OF(“xxx”)) pour les stratégies d’authentification afin d’identifier le flux nFactor lié à la partie de confiance. Longueur maximale : 63

Un groupe est ajouté à la session pour ce profil afin de simplifier l’évaluation des stratégies et de faciliter la personnalisation des stratégies. Ce groupe est le groupe par défaut qui est choisi lorsque l’authentification réussit, en plus des groupes extraits. Longueur maximale : 63.

The screenshot shows the Citrix console interface for creating an OAuth IDP profile. The form includes the following fields and options:

- Name***: gatewayIDP
- Client ID***: cclientid
- Client Secret***: cclientsecret
- Redirect URL***: https://redirecturl
- Issuer Name**: (empty)
- Audience**: cclientid
- Skew Time (mins)**: 5
- Default Authentication Group**: testGroup
- Relaying Party Metadata URL**: (empty)
- Refresh Interval**: 50
- Encrypt Token**:
- Signature Service**: (empty)
- Attributes**: (empty)
- Send Password**:

At the bottom, there are two buttons: **Create** (highlighted in blue) and **Close**.

Ajouter une stratégie d'authentification de fournisseur d'identité

1. Sur la page OAuth IdP, cliquez sur **Policies**, puis sur **Add**.
2. Dans l'écran **Create Authentication OAuth IdP Policy**, définissez des valeurs pour les paramètres suivants et cliquez sur **Create**.
 - **Name** : nom de la stratégie d'authentification.
 - **Action** : nom du profil créé précédemment.
 - **Log Action** : nom de l'action du journal des messages à utiliser lorsqu'une demande correspond à cette stratégie. Ce champ n'est pas obligatoire.
 - **Undefined-Result Action** : action à effectuer si le résultat de l'évaluation des stratégies n'est pas défini (UNDEF). Ce champ n'est pas obligatoire.
 - **Expression** : expression syntaxique par défaut utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, true.
 - **Comments** : tout commentaire concernant la stratégie.

The screenshot shows the Citrix Gateway configuration interface for creating an OAuth IDP Policy. The page title is "Create Authentication OAuth IDP Policy". The interface includes the following fields and controls:

- Name***: A text input field containing "gatewayIDP_pol".
- Action***: A dropdown menu with "gatewayIDP" selected, accompanied by "Add" and "Edit" buttons.
- Log Action**: A dropdown menu with an empty selection, accompanied by "Add" and "Edit" buttons.
- Undefined Result Action**: A dropdown menu with an empty selection.
- Expression***: A text area containing "true". Above the text area are three "Select" dropdown menus and an "Expression Editor" link. Below the text area is an "Evaluate" button.
- Comments**: A text input field.
- Buttons**: "Create" and "Close" buttons at the bottom.

Remarque :

Lorsque SendPassword est défini sur ON (OFF par défaut), les informations d'identification de l'utilisateur sont cryptées et transmises via un canal sécurisé à Citrix Cloud. La transmission des informations d'identification utilisateur via un canal sécurisé vous permet d'activer l'authentification unique pour Citrix Virtual Apps and Desktops lors du lancement.

Lier la stratégie d'authentification de fournisseur d'identité et la stratégie LDAP au serveur d'authentification virtuel

Vous devez maintenant lier la stratégie d'authentification de fournisseur d'identité au serveur d'authentification virtuel sur le Citrix Gateway local.

1. Connectez-vous à votre portail de gestion Citrix Gateway local et accédez à **Configuration > Security > AAA-Application Traffic > Policies > Authentication > Advanced Policies > Actions > LDAP**.
2. Sur l'écran **Actions DAP**, cliquez sur **Ajouter**.
3. Dans l'écran Create Authentication LDAP Server, définissez des valeurs pour les paramètres suivants et cliquez sur **Create**.
 - **Name** : nom de l'action LDAP.

- **ServerName/ServerIP** : indiquez le nom de domaine complet ou l'adresse IP du serveur LDAP.
 - Choisissez les valeurs appropriées pour le **type de sécurité**, le **port**, le **type de serveur** et le **délai d'expiration**.
 - Assurez-vous que l'option **Authentication** est cochée.
 - **Base DN** : base à partir de laquelle démarrer la recherche LDAP. Par exemple `dc=aaa,dc=local`.
 - **Administrator Bind DN** : nom d'utilisateur de la liaison au serveur LDAP. Par exemple, `admin@aaa.local`.
 - **Administrator Password/Confirm Password** : mot de passe pour lier LDAP.
 - Cliquez sur **Test Connection** pour tester vos paramètres.
 - **Server Logon Name Attribute** : choisissez "sAMAccountName"
 - Les autres champs ne sont pas obligatoires et peuvent donc être configurés selon les besoins.
4. Accédez à **Configuration > Security > AAA-Application Traffic > Politiques > Authentication > Advanced Policies > Policy**.
 5. Dans l'écran **Test Connection**, cliquez sur **Add**.
 6. Sur la page **Create Authentication Policy**, définissez des valeurs pour les paramètres suivants et cliquez sur **Create**.
 - **Name** : nom de la stratégie d'authentification LDAP.
 - **Action Type** : choisissez LDAP.
 - **Action** : choisissez l'action LDAP.
 - **Expression** : expression syntaxique par défaut utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, `true**`.

Lier le certificat globalement au VPN

La liaison globale du certificat au VPN nécessite un accès CLI au Citrix Gateway local. À l'aide de Putty (ou similaire), connectez-vous au Citrix Gateway local à l'aide de SSH.

1. Lancez un utilitaire de ligne de commande, tel que Putty.
2. Connectez-vous au Citrix Gateway local à l'aide de SSH.
3. Entrez la commande suivante :

```
show vpn global
```

Remarque :

Aucun certificat ne doit être lié.

```
Done
> show vpn global

1) VPN Clientless Access Policy Name: ns_cvpa_owa_policy Priority: 95000
   Bindpoint: REQ_DEFAULT
2) VPN Clientless Access Policy Name: ns_cvpa_sp_policy Priority: 96000
   Bindpoint: REQ_DEFAULT
3) VPN Clientless Access Policy Name: ns_cvpa_sp2013_policy Priority: 97000
   Bindpoint: REQ_DEFAULT
4) VPN Clientless Access Policy Name: ns_cvpa_default_policy Priority: 100000
   Bindpoint: REQ_DEFAULT

Done
>
```

4. Pour répertorier les certificats sur le Citrix Gateway local, tapez la commande suivante :

```
show ssl certkey
```

5. Sélectionnez le certificat approprié et tapez la commande suivante pour lier le certificat globalement au VPN :

```
bind vpn global -certkey cert_key_name
```

où cert_key_name est le nom du certificat.

6. Tapez la commande suivante pour vérifier si le certificat est lié globalement au VPN :

```
show vpn global
```

```
Done
> show vpn global
Certificate: Gateway_ ██████████

1) VPN Clientless Access Policy Name: ns_cvpa_owa_policy Priority: 95000
   Bindpoint: REQ_DEFAULT
2) VPN Clientless Access Policy Name: ns_cvpa_sp_policy Priority: 96000
   Bindpoint: REQ_DEFAULT
3) VPN Clientless Access Policy Name: ns_cvpa_sp2013_policy Priority: 97000
   Bindpoint: REQ_DEFAULT
4) VPN Clientless Access Policy Name: ns_cvpa_default_policy Priority: 100000
   Bindpoint: REQ_DEFAULT

Done
>
```

Configurer l'authentification pass-through au domaine en tant que méthode d'authentification dans Citrix Gateway

Lorsque vous avez terminé la configuration de Citrix Gateway en tant que fournisseur d'identité, effectuez les étapes suivantes pour configurer l'authentification pass-through au domaine en tant que méthode d'authentification dans Citrix Gateway.

Lorsque l'authentification pass-through au domaine est définie comme méthode d'authentification, le client utilise des tickets Kerberos pour s'authentifier au lieu des informations d'identification. Citrix Gateway prend en charge l'emprunt d'identité et la délégation Kerberos contrainte (KCD). Toutefois, cet article décrit l'authentification KCD. Pour obtenir davantage d'informations, veuillez consulter l'article [CTX236593](#) du centre de connaissances.

La configuration de l'authentification pass-through inclut les étapes suivantes :

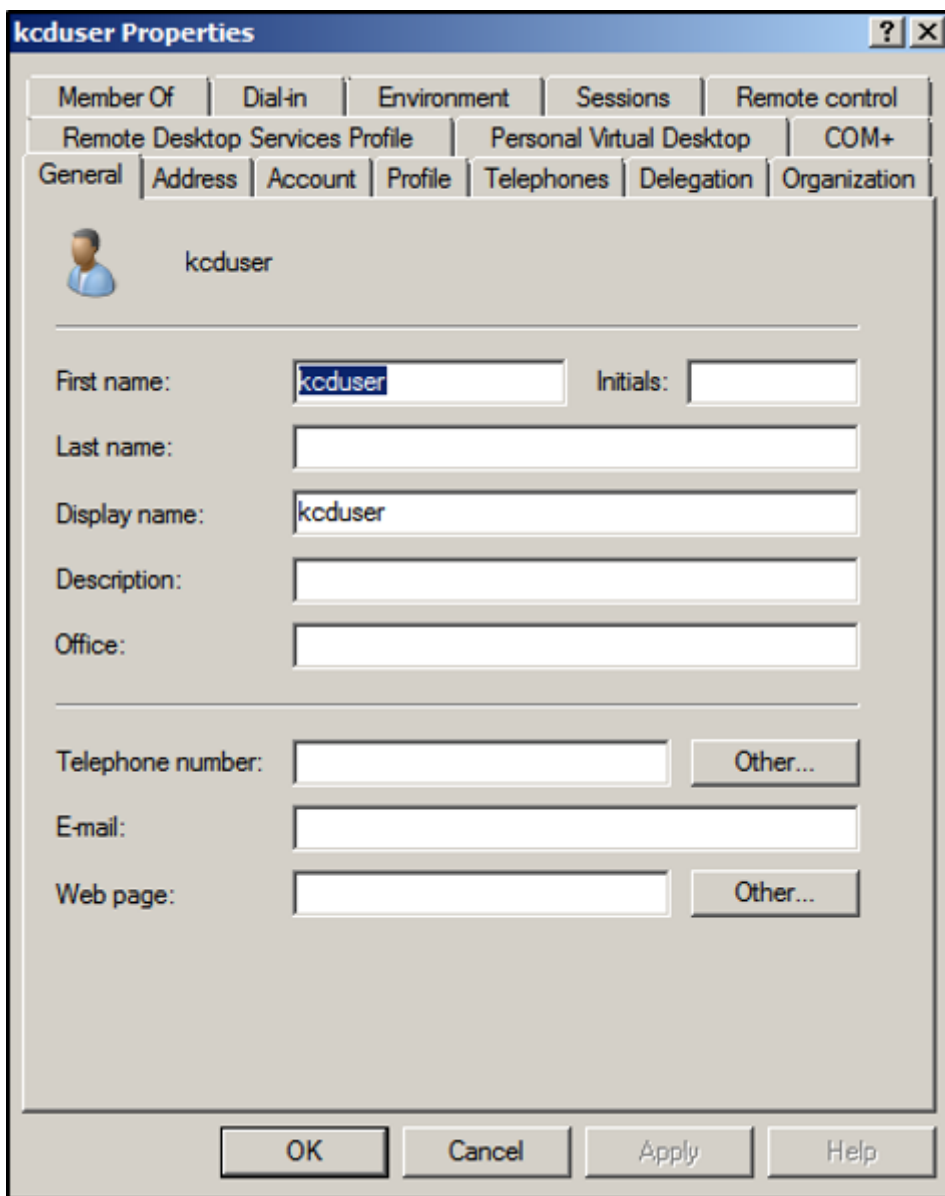
1. Configuration de la délégation Kerberos contrainte
2. Configuration du client

Configuration de la délégation Kerberos contrainte

1. Créer un utilisateur KCD dans Active Directory

Kerberos fonctionne sur un système d’octroi de tickets pour authentifier les utilisateurs auprès des ressources et implique un client, un serveur et un centre de distribution de clés (KDC).

Pour que Kerberos fonctionne, le client doit demander un ticket au KDC. Le client doit d’abord s’authentifier auprès du KDC à l’aide de son nom d’utilisateur, de son mot de passe et de son domaine avant de demander un ticket, appelé demande AS.



2. Associez le nouvel utilisateur au nom principal de service (SPN).

Le nom principal de service de la passerelle est utilisé par le client pour s'authentifier.

- Service Principal Name (SPN) : un nom principal de service (SPN) est un identifiant unique d'une instance de service. L'authentification Kerberos utilise le nom principal de service pour associer une instance de service à un compte de connexion au service. Cette fonction permet à une application cliente de demander l'authentification de service d'un compte même si le client ne possède pas le nom du compte.

SetSPN est l'application permettant de gérer les SPN sur un appareil Windows. Avec SetSPN, vous pouvez afficher, modifier et supprimer des enregistrements SPN.

- a) Sur le serveur Active Directory, ouvrez une invite de commande.
- b) Dans l'invite de commandes, saisissez la commande suivante :

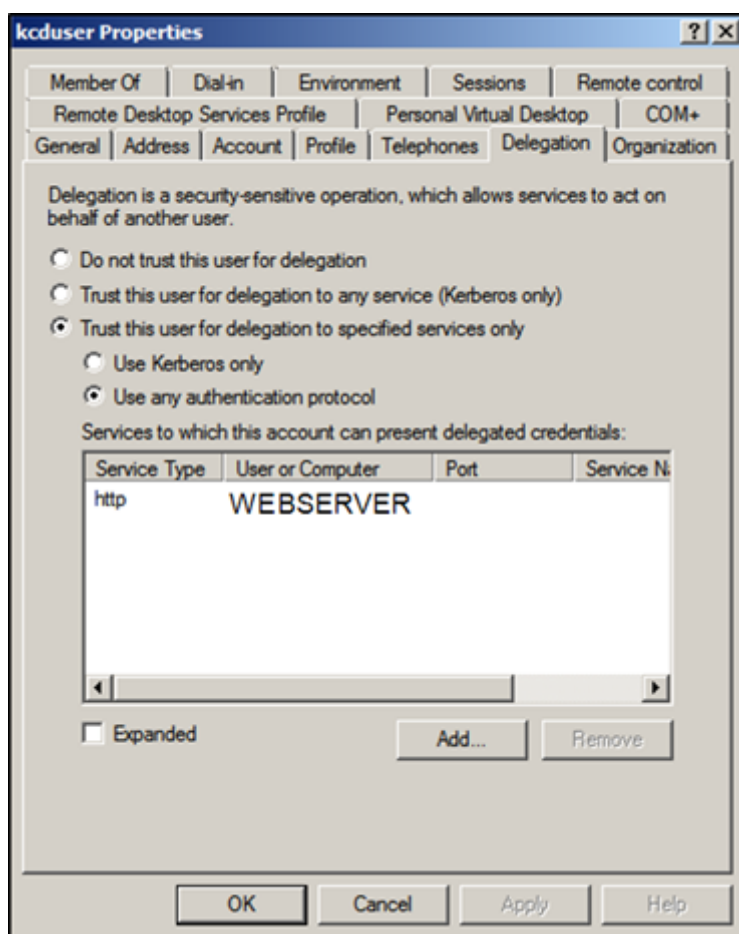
```
setspn -A http/<LB fqdn> <domain\Kerberos user>
```

- c) Pour confirmer les SPN de l'utilisateur Kerberos, exécutez la commande suivante :

```
setspn -l <Kerberos user>
```

L'onglet Délégation s'affiche après l'exécution de la commande `setspn`.

- d) Sélectionnez l'option **Trust this user for delegation to specified services only** et l'option **Use any authentication protocol**. Ajoutez le serveur Web et sélectionnez le service HTTP.

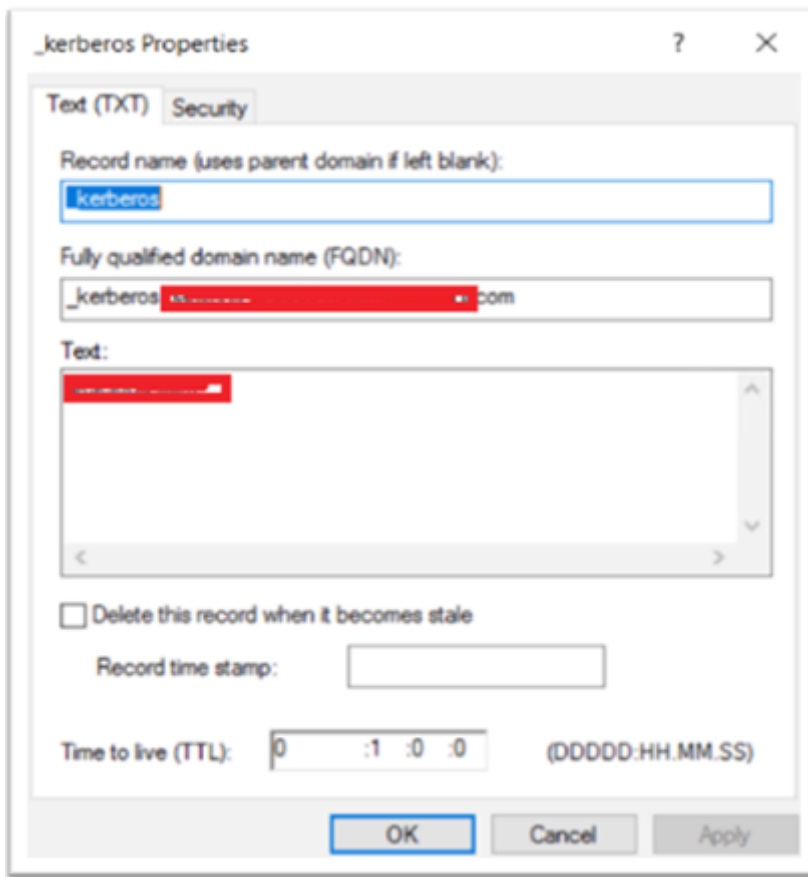


3. Créez un enregistrement DNS pour que le client trouve le SPN de la passerelle :

Ajoutez un enregistrement DNS TXT dans Active Directory.

Remarque :

Name doit commencer par _Kerberos, Data doit être le nom de domaine. Le FQDN doit afficher Kerberos..



Le client joint au domaine utilise `_kerberos.fqdn` pour demander des tickets. Par exemple, si le client est joint à `citrite.net`, le système d'exploitation peut obtenir des tickets pour tous les sites Web avec `*.citrite.net`. Toutefois, si le domaine Gateway est externe, comme `gateway.citrix.com`, le système d'exploitation client ne peut pas obtenir le ticket Kerberos.

Par conséquent, vous devez créer un enregistrement DNS TXT qui aide le client à rechercher `_kerberos.gateway.citrix.com` et à obtenir le ticket Kerberos pour l'authentification.

4. Configurez Kerberos en tant que facteur d'authentification.

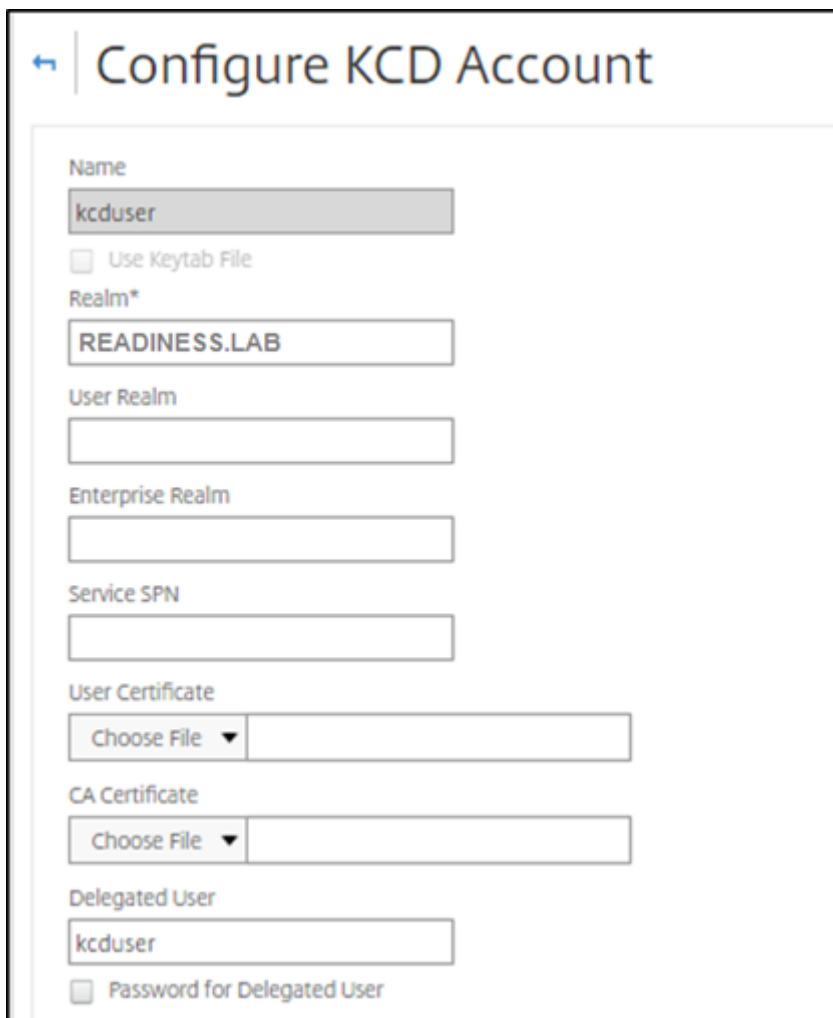
- a) Créez un compte KCD pour l'utilisateur NetScaler. Ici, nous avons choisi de le faire manuellement, mais vous pouvez créer un fichier keytab.

Remarque :

Si vous utilisez d'autres domaines (domaine interne et domaine externe), vous devez définir le SPN du service sur `HTTP/PublicFQDN.com@InternalDomain.ext`.

- **Realm** : royaume Kerberos. En général, le suffixe de votre domaine interne.
- **User Realm** : il s'agit du suffixe de domaine interne de votre utilisateur.
- **Enterprise Realm** : cette option ne doit être fournie que dans certains déploiements KDC pour lesquels le KDC attend un nom d'utilisateur d'entreprise au lieu du SPN.

- **Delegated User** : il s'agit du compte d'utilisateur NetScaler pour KCD que vous avez créé dans AD au cours des étapes précédentes. Assurez-vous que le mot de passe est correct.



The screenshot shows a web interface titled "Configure KCD Account". The form includes the following fields and options:

- Name**: Text input field containing "kcduser".
- Use Keytab File
- Realm***: Text input field containing "READINESS.LAB".
- User Realm**: Text input field (empty).
- Enterprise Realm**: Text input field (empty).
- Service SPN**: Text input field (empty).
- User Certificate**: Text input field with a "Choose File" dropdown menu.
- CA Certificate**: Text input field with a "Choose File" dropdown menu.
- Delegated User**: Text input field containing "kcduser".
- Password for Delegated User

- b) Assurez-vous que le profil de session utilise le bon compte KCD. Liez la stratégie de session au serveur virtuel d'authentification, d'autorisation et d'audit.

	Override Global
Session Time-out (mins)	<input checked="" type="checkbox"/>
Default Authorization Action*	<input checked="" type="checkbox"/>
Single Sign-on to Web Applications*	<input checked="" type="checkbox"/>
Credential Index*	<input checked="" type="checkbox"/>
Single Sign-on Domain	<input checked="" type="checkbox"/>
HTTPOnly Cookie*	<input type="checkbox"/>
Enable Persistent Cookie*	<input type="checkbox"/>
Persistent Cookie Validity	<input type="checkbox"/>
KCD Account	<input checked="" type="checkbox"/>

- c) Liez la stratégie d'authentification au serveur virtuel d'authentification, d'autorisation et d'audit. Ces stratégies utilisent des méthodes d'authentification, d'autorisation et d'audit qui n'obtiennent pas de mot de passe auprès du client, d'où la nécessité d'utiliser KCD. Cependant, ils doivent toujours obtenir le nom d'utilisateur et les informations de domaine, au format UPN.

Remarque :

Vous pouvez utiliser l'adresse IP ou l'analyse de point de terminaison pour différencier les appareils joints à un domaine et ceux n'appartenant pas à un domaine et utiliser Kerberos ou LDAP standard comme facteur d'authentification.

Configurer le client

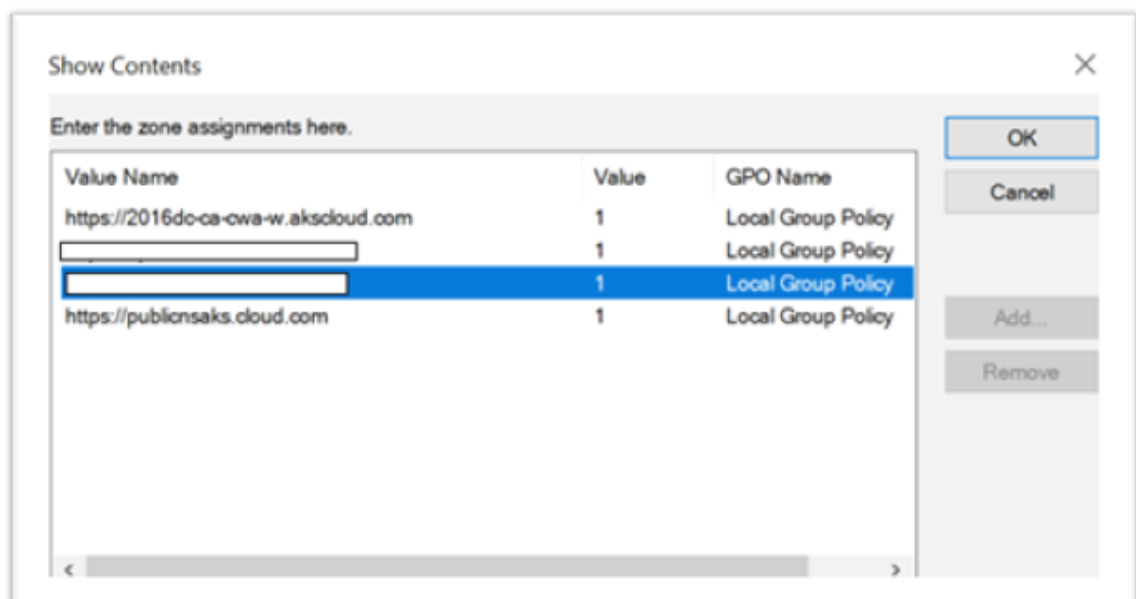
Pour assurer la réussite de l'authentification unique au VDA, effectuez les opérations suivantes.

Pré-requis :

- Machine jointe au domaine
- Citrix Workspace 2112.1 ou version ultérieure avec le paramètre d'authentification unique activé
- Faire confiance aux URL qui vérifient si les connexions sont sécurisées
- Valider Kerberos à partir du client et d'AD. Le système d'exploitation client doit être connecté à AD pour obtenir des tickets Kerberos.

Voici quelques-unes des URL auxquelles le navigateur doit faire confiance :

- URL ou nom de domaine complet de la passerelle
 - NOM DE DOMAINE COMPLET AD
 - URL de l'espace de travail pour l'authentification unique à partir de lancements par navigateur
1. Si vous utilisez Internet Explorer, Microsoft Edge ou Google Chrome, procédez comme suit :
 - a) Lancez le navigateur.
 - b) Ouvrez l'éditeur de stratégie de groupe local sur le client.



- a) Accédez à la page **Configuration ordinateur > Composant Windows > Internet Explorer > Panneau de configuration Internet > Sécurité**.
 - b) Ouvrez la liste des attributions de sites aux zones et ajoutez toutes les URL répertoriées avec la valeur un (1).
 - c) (Facultatif) Exécutez [Gpupdate](#) pour appliquer les stratégies.
2. Si vous utilisez le navigateur Mozilla Firefox, procédez comme suit :
- a) Ouvrez le navigateur.
 - b) Saisissez `about:config` dans la barre de recherche.
 - c) Acceptez le risque et continuez.
 - d) Dans le champ de recherche, saisissez **negotiate**.
 - e) Dans la liste des données renseignées, vérifiez si **network.negotiate-auth.trusted-uris** est défini sur la valeur du domaine.



La configuration côté client est terminée.

3. Connectez-vous à Citrix Workspace en utilisant l'application ou le navigateur.

Aucune invite ne doit s'afficher pour demander un nom d'utilisateur ou mot de passe sur un appareil joint à un domaine.

Résolution des problèmes de Kerberos

Remarque :

Vous devez être administrateur de domaine pour exécuter cette étape de vérification.

Dans l'invite de commande ou dans Windows PowerShell, exécutez la commande suivante pour vérifier la validation du ticket Kerberos pour l'utilisateur SPN :

```
KLIST get host/FQDN of AD
```

Authentification pass-through au domaine pour Citrix Workspace en utilisant Azure Active Directory en tant que fournisseur d'identité

April 22, 2024

Vous pouvez implémenter l'authentification unique (SSO ou Single Sign-On) à Citrix Workspace à l'aide d'Azure Active Directory (AAD) en tant que fournisseur d'identité avec des points de terminaison/machines virtuelles joints au domaine, hybrides et inscrits auprès de Azure AD.

Avec cette configuration, vous pouvez également utiliser Windows Hello pour l'authentification unique à Citrix Workspace à l'aide de points de terminaison inscrits auprès de AAD.

- Vous pouvez vous authentifier auprès de l'application Citrix Workspace via Windows Hello.
- Authentification basée sur FIDO2 avec l'application Citrix Workspace.
- Authentification unique (SSO) à l'application Citrix Workspace à partir de machines jointes à Microsoft AAD (AAD en tant que fournisseur d'identité). Accès conditionnel avec AAD.

Pour utiliser l'authentification unique sur les applications et les bureaux virtuels, vous pouvez déployer FAS ou configurer l'application Citrix Workspace comme suit.

Remarque :

Vous pouvez utiliser l'authentification unique pour les ressources Citrix Workspace uniquement avec Windows Hello. Toutefois, vous êtes invité à saisir un nom d'utilisateur et un mot de passe lorsque vous accédez à vos applications et bureaux virtuels publiés. Pour résoudre ce problème, vous pouvez déployer FAS et SSO sur des applications et des bureaux virtuels.

Pré-requis :

1. Connectez Azure Active Directory à Citrix Cloud. Pour plus d'informations, consultez [Connecter Azure Active Directory à Citrix Cloud](#) dans la documentation Citrix Cloud.
2. Activez l'authentification Azure AD pour l'accès aux espaces de travail. Pour plus d'informations, consultez [Activer l'authentification Azure AD pour les espaces de travail](#) dans la documentation Citrix Cloud.

Pour utiliser l'authentification unique avec Citrix Workspace, procédez comme suit :

1. Configurez l'application Citrix Workspace avec includeSSON
2. Désactivez l'attribut `prompt=login` dans Citrix Cloud.
3. Configurez l'authentification unique Azure Active Directory avec Azure Active Directory Connect.

Configurer l'application Citrix Workspace pour prendre en charge l'authentification unique

Pré-requis :

- Citrix Workspace version 2109 ou supérieure.

Remarque :

Si vous utilisez FAS pour l'authentification unique, la configuration de Citrix Workspace n'est pas nécessaire.

1. Installez l'application Citrix Workspace depuis la ligne de commande administrative avec l'option `includeSSON` :

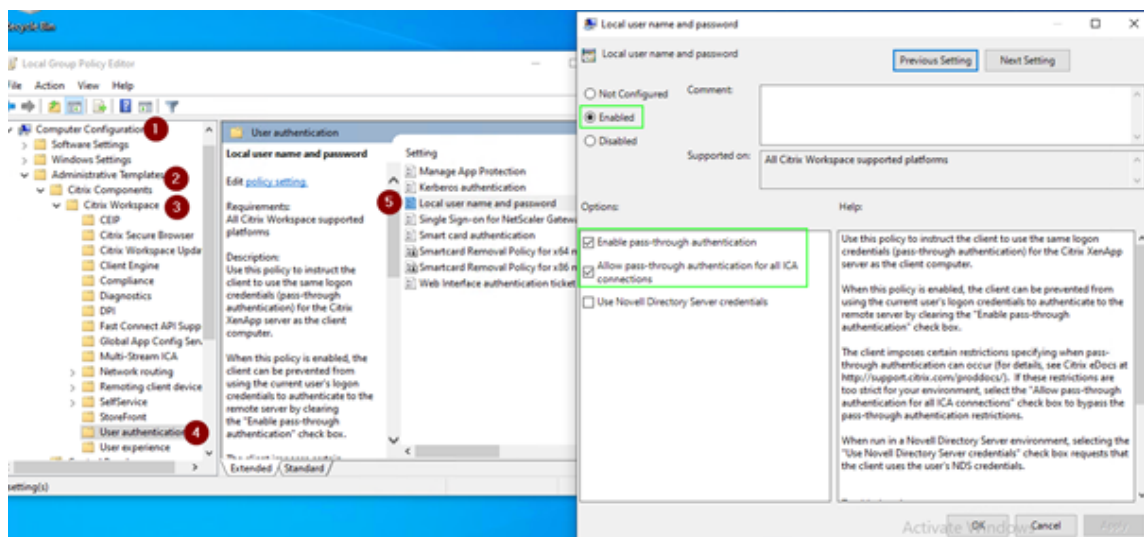
```
CitrixWorkspaceApp.exe /includeSSON
```

2. Déconnectez-vous du client Windows et connectez-vous pour démarrer le serveur SSON.
3. Cliquez sur **Configuration ordinateur > Modèles d'administration > Composants Citrix > Citrix Workspace > Authentification utilisateur** pour modifier l'objet de stratégie de groupe Citrix Workspace et autoriser **Nom d'utilisateur et mot de passe locaux**.

Remarque :

Ces stratégies peuvent être transmises à l'appareil client via Active Directory. Cette étape est requise uniquement lors de l'accès à Citrix Workspace depuis le navigateur Web.

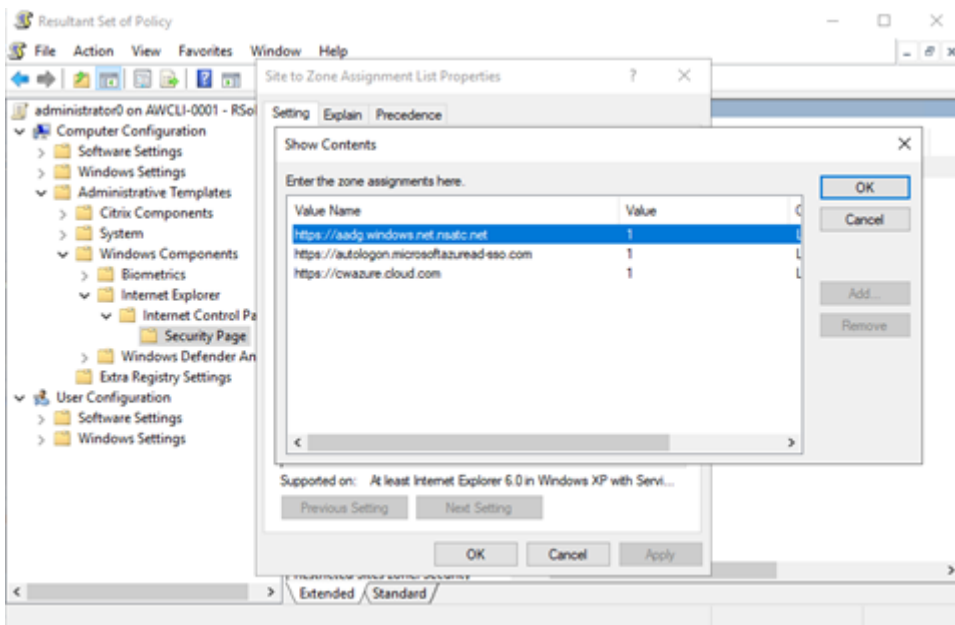
4. Activez le paramètre comme indiqué sur la capture d'écran.



5. Ajoutez les sites de confiance suivants via l'objet de stratégie de groupe :

- <https://aadg.windows.net.nsatc.net>

- <https://autologon.microsoftazuread-sso.com>
- <https://xxxtenantxxx.cloud.com>: URL de l'espace de travail



Remarque :

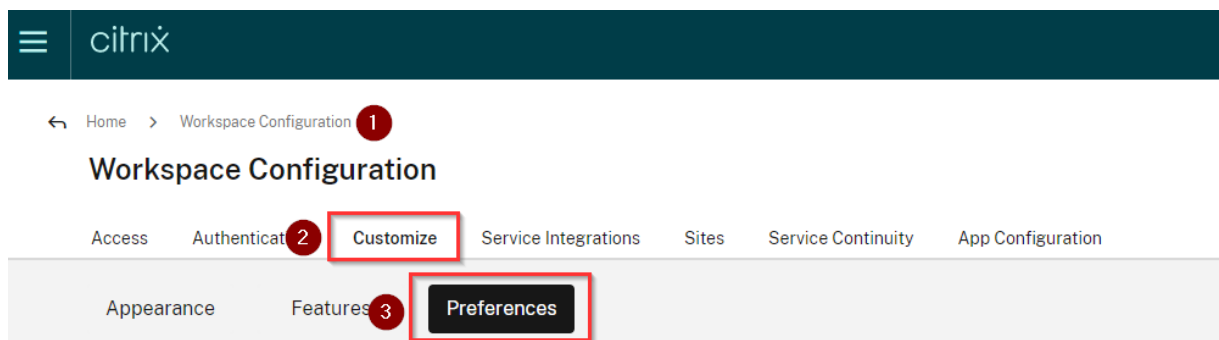
L'authentification unique pour AAD est désactivée lorsque le registre **AllowSSOForEdgeWebView** dans `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` est défini sur `false`.

Désactiver le paramètre `prompt=login` dans Citrix Cloud

Par défaut, `prompt=login` est activé pour Citrix Workspace, ce qui force l'authentification même si l'utilisateur a choisi de **rester connecté** ou si l'appareil est joint à Azure AD.

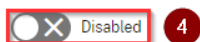
Vous pouvez désactiver `prompt=login` dans votre compte Citrix Cloud. Accédez à `Workspace Configuration\Customize\Preferences-Federated Identity Provider Sessions` et désactivez le paramètre.

Pour obtenir davantage d'informations, consultez l'article [CTX253779](#) du Centre de connaissances.



Workspace Sessions

Federated Identity Provider Sessions



When Workspace is configured to use a federated identity provider, the authentication session and its lifetime are controlled by the identity provider. When enabled, Workspace forces a login prompt with the identity provider when a new Workspace session is needed. When disabled, a subscriber will not be prompted to authenticate with the identity provider if accessing Workspace with a valid session, achieving single sign-on.

Remarque :

Sur les appareils AAD ou AAD hybrides joints, si AAD est utilisé comme IdP pour Workspace, l'application Citrix Workspace ne demande pas d'informations d'identification. Les utilisateurs peuvent se connecter automatiquement à l'aide d'un compte professionnel ou scolaire.

Pour permettre aux utilisateurs de se connecter à l'aide d'un autre compte, définissez le registre suivant sur false.

Créez et ajoutez une chaîne de registre REG_SZ appelée **AllowSSOForEdgeWebview** sous `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` ou `Computer\HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle` et définissez sa valeur sur False. Si les utilisateurs se déconnectent de l'application Citrix Workspace, ils peuvent également se connecter avec un compte différent lors de la prochaine connexion.

Configurer l'authentification unique Azure Active Directory avec Azure Active Directory Connect

- Si vous installez Azure Active Directory Connect pour la première fois, sur la page **Connexion utilisateur**, sélectionnez **Authentification directe** comme méthode de connexion. Pour plus d'informations, consultez [Authentification directe Azure Active Directory : Démarrage rapide](#) dans la documentation Microsoft.
- Si Microsoft Azure Active Directory Connect existe :
 1. Sélectionnez la tâche **Modifier la connexion utilisateur** et cliquez sur **Suivant**.
 2. Sélectionnez **Authentification unique** comme méthode de connexion.

Remarque :

Vous pouvez ignorer cette étape si l'appareil client est joint à Azure AD ou hybride. Si l'appareil est joint à AD, l'authentification unique au domaine fonctionne avec l'authentification Kerberos.

Authentification pass-through au domaine pour Citrix Workspace en utilisant Okta en tant que fournisseur d'identité

April 22, 2024

Vous pouvez utiliser l'authentification unique avec Citrix Workspace en utilisant Okta en tant que fournisseur d'identité (IdP).

Pré-requis :

- Citrix Cloud
 - Cloud Connector

Remarque ::

Si vous utilisez Citrix Cloud pour la première fois, définissez un emplacement de ressources et configurez les connecteurs. Il est recommandé de déployer au moins deux connecteurs cloud dans les environnements de production. Pour plus d'informations sur l'installation de Citrix Cloud Connector, consultez [Installation de Cloud Connector](#).

- Citrix Workspace
- Service d'authentification fédérée (facultatif). Pour plus d'informations, consultez [Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix](#).
- Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)
- VDA joint au domaine AD ou appareils physiques joints à AD
- Locataire Okta
 - Agent Okta IWA (Integrated Windows Authentication)
 - Okta Verify (Okta Verify peut être téléchargé depuis le magasin d'applications) (facultatif)
- Active Directory

1. Déployez l'agent Okta AD :

- a) Dans le portail d'administration Okta, cliquez sur **Directory > Directory Integrations**.
- b) Cliquez sur **Add Directory > Add Active Directory**.
- c) Passez en revue les exigences d'installation en suivant le flux de travail, qui couvre l'architecture de l'agent et les exigences d'installation.
- d) Cliquez sur le bouton **Set Up Active Directory**, puis sur **Download Agent**.

- e) Installez l'agent Okta AD sur un serveur Windows en suivant les instructions fournies dans [Install the Okta Active Directory agent](#).

Remarque :

Assurez-vous que les conditions préalables mentionnées dans [Active Directory integration prerequisites](#) sont remplies avant d'installer l'agent.

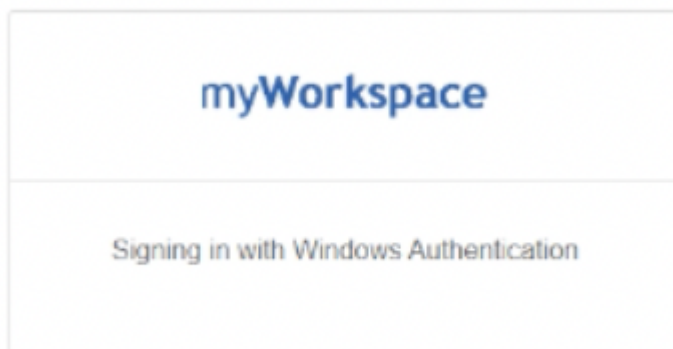
2. Configurez Integrated Windows Authentication (IWA) :

- Sur le portail d'administration Okta, cliquez sur **Security**, puis sur **Delegated Authentication**.
- Faites défiler vers le bas jusqu'à la partie **On-prem Desktop SSO** sur la page qui se charge et cliquez sur **Download Agent**.
- Configurez les **règles de routage** (Routing Rules) pour IWA. Pour plus d'informations, voir [Configure Identity Provider routing rules](#).

3. Lancez le portail client Okta.

Remarque :

- Lorsque vous installez Okta IWA Agent et que l'état est activé, vous pouvez vous connecter à partir d'un appareil joint au domaine Windows. Cette configuration passe également la connexion et vous dirige vers la page de connexion IWA, puis transmet les informations d'identification de l'utilisateur.



- Pour plus d'informations sur la résolution des problèmes, consultez l'article [Install and configure the Okta IWA Web agent for Desktop single sign-on](#).

4. Connectez-vous à Citrix Cloud sur <https://citrix.cloud.com> et activez Okta en tant que fournisseur d'identité. Pour plus d'informations, consultez [Tech Insight: Authentication - Okta](#) dans la documentation de Citrix Tech Zone.

Remarque :

Vous pouvez vous connecter à partir de l'application Citrix Workspace ou du navigateur,

les deux fournissant l'expérience d'authentification pass-through conformément à la documentation Tech Zone.

5. Pour utiliser l'authentification unique sur les applications et les bureaux virtuels, vous pouvez déployer FAS ou configurer l'application Citrix Workspace.

Remarque :

Sans FAS, vous êtes invité à saisir le nom d'utilisateur et le mot de passe AD. Pour plus d'informations, consultez [Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix](#).

Si vous n'utilisez pas FAS, [configurez l'application Citrix Workspace pour qu'elle prenne en charge l'authentification unique](#).

HDX

April 22, 2024

Cette section décrit les éléments suivants :

- [Graphisme et affichage](#)
- [Microsoft Teams optimisé](#)
- [Transport HDX](#)
- [Redirection du contenu du navigateur](#)
- [Redirection bidirectionnelle du contenu](#)
- [Référence des paramètres ICA](#)

Graphisme et affichage

April 23, 2024

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 peut détecter chacun des moniteurs. 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**.
 - * Dans la console de gestion Citrix pour le serveur Citrix Virtual Apps, sélectionnez la batterie de serveurs et dans le panneau des tâches, sélectionnez :
 - **Modifier les propriétés du serveur > Modifier toutes les propriétés > Valeur par défaut du serveur > HDX Broadcast > Affichage** ou
 - **Modifier les propriétés du 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.

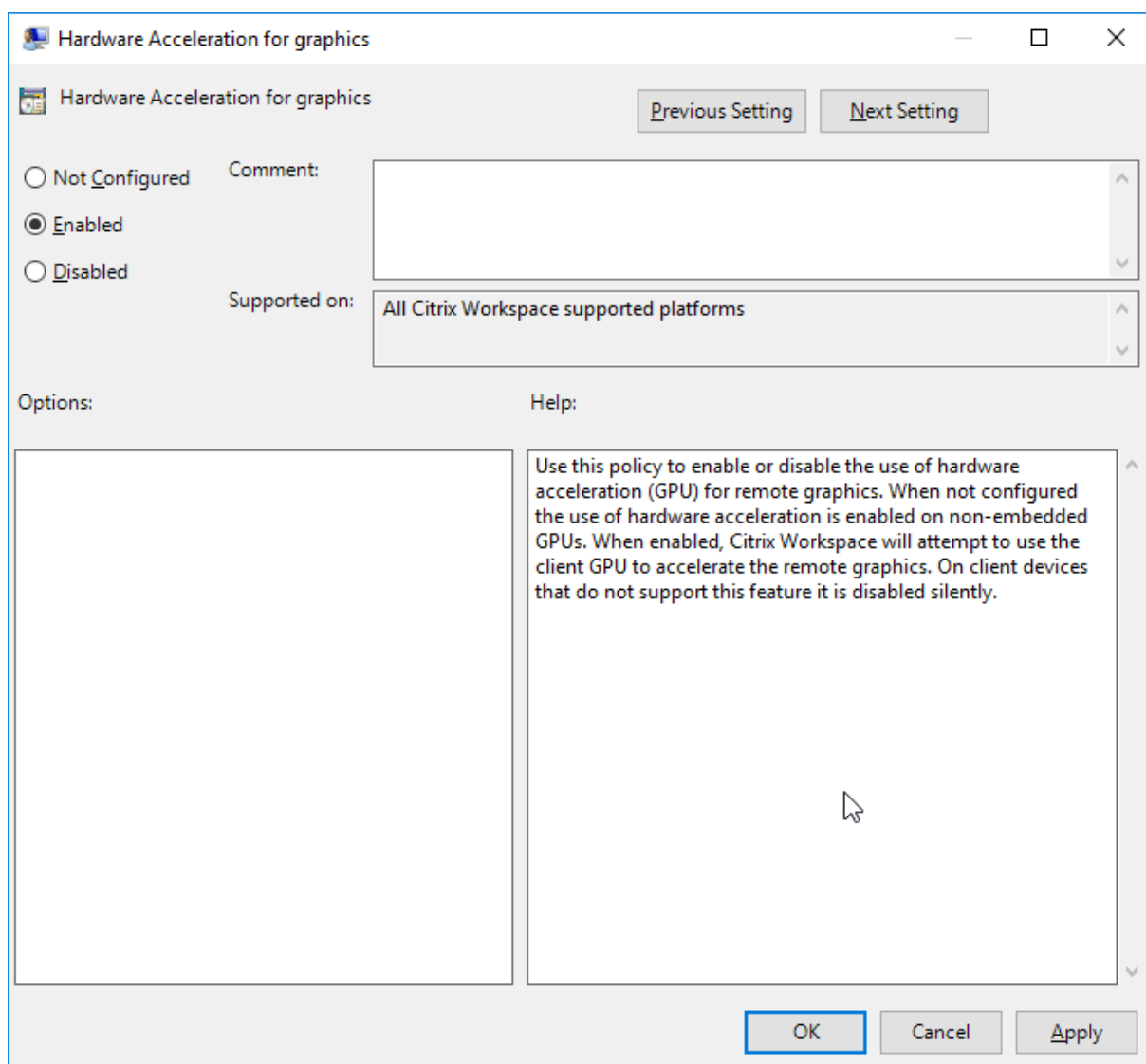
Pour calculer les exigences de mémoire graphique de la session pour Citrix Virtual Apps and Desktops et Citrix DaaS, consultez l'article [CTX115637](#) du centre de connaissances.

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 vérifier si la stratégie est définie et si l'accélération matérielle est utilisée pour une session ICA active, vérifiez 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 est effectué sur le processeur.

- Lors de la connexion à un serveur Citrix Virtual Apps exécuté sur Windows Server 2008 R2, n'utilisez pas 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.

Disposition d'affichage virtuel

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

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

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

À partir de l'application Citrix Workspace pour Windows 2106, la disposition de l'affichage virtuel est également prise en charge pour les sessions de bureau en mode multi-moniteur et en mode plein écran. La disposition d'affichage virtuel est activée par défaut. Dans un scénario multi-moniteur, la même disposition d'affichage virtuel est appliquée à tous les moniteurs de session si le nombre total d'écrans virtuels ne dépasse pas huit écrans virtuels. Si cette limite est dépassée, la disposition de l'affichage virtuel est ignorée et n'est appliquée à aucun moniteur de session.

L'amélioration multi-moniteur peut être désactivée en définissant la clé de registre suivante :

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

Nom : **SplitAllMonitors**

; Type : DWORD

Valeurs :

1 - Activé

0 - Désactivé

Mise à l'échelle DPI

L'application Citrix Workspace prend en charge les résolutions élevées de même que la correspondance de la résolution d'affichage et des paramètres d'échelle DPI entre le client Windows et la session d'applications et de bureaux virtuels.

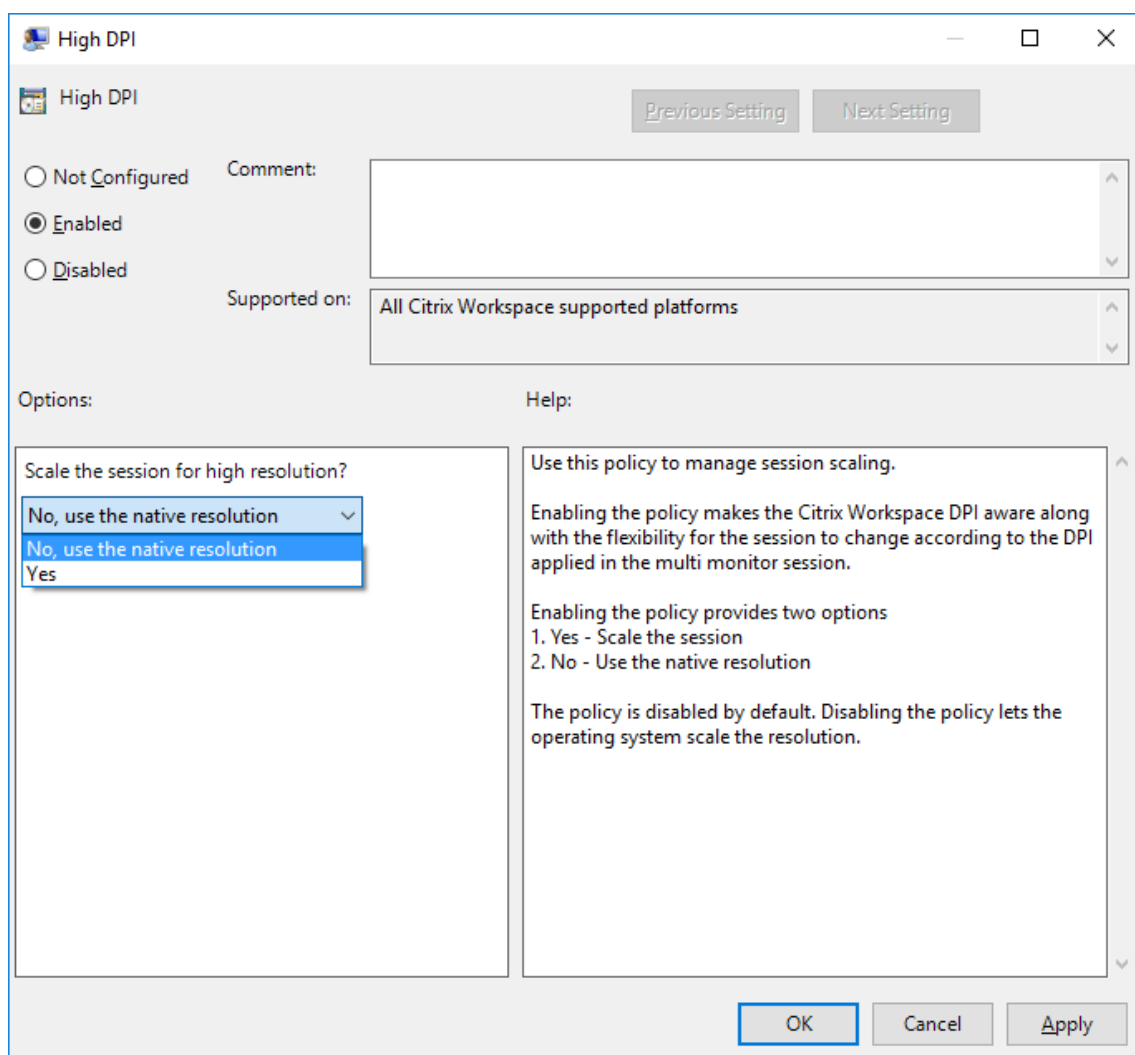
La mise à l'échelle DPI est principalement utilisée avec des moniteurs de grande taille et de haute résolution pour afficher des applications, du texte, des images et d'autres éléments graphiques dans une taille permettant de les visualiser aisément.

Cette fonctionnalité est activée par défaut ; il s'agit du paramètre recommandé pour tous les cas d'utilisation. Toutefois, les administrateurs peuvent toujours configurer la mise à l'échelle DPI à l'aide du modèle d'administration d'objet de stratégie de groupe (configuration par machine) si nécessaire.

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

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 :

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 **DPI élevé**.
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.

REMARQUE :

Considérations supplémentaires :

- La correspondance DPI nécessite Citrix Virtual Apps and Desktops version 1912 LTSR ou versions ultérieures.
- Le paramètre **Non, utiliser la résolution native** (correspondance DPI) est recommandé dans la plupart des cas.
- Le paramètre par défaut **Laisser le système d'exploitation régler la résolution** désactive la prise en charge de DPI sur l'application Citrix Workspace. Ce mode peut générer des graphiques flous lorsque la résolution du client Windows est définie sur une valeur autre que 100%. Ce mode ne prend pas en charge plusieurs moniteurs avec différentes échelles de résolution.
- Si vous sélectionnez l'option **Oui**, l'application Citrix Workspace augmente la résolution de la fenêtre de session pour qu'elle corresponde à la résolution configurée sur le client Windows. Il s'agit d'une fonction héritée recommandée uniquement pour les connexions à d'anciens environnements XenApp et XenDesktop lorsque des résolutions supérieures à 100% sont requises sur le client. Ce mode peut entraîner des images floues.

Pour plus d'informations sur la résolution des problèmes liés à la mise à l'échelle DPI, consultez l'article [CTX230017](#) du centre de connaissances.

Sélection automatique du codec vidéo

L'application Citrix Workspace pour Windows détecte désormais automatiquement le meilleur codec vidéo à utiliser. Lors de l'installation de l'application Citrix Workspace pour Windows, les capacités de décodage du terminal sont évaluées. Ces informations permettent à l'application Citrix Workspace pour Windows de sélectionner le meilleur codec à utiliser avec le VDA au démarrage de la session. Les codecs vidéo sont évalués dans l'ordre suivant :

1. AV1

2. H.265
3. H.264

Cette fonctionnalité est disponible lorsque la politique d'**utilisation d'un codec vidéo pour la compression** est définie sur l'une des valeurs suivantes :

- **Utiliser au choix**
- **Pour l'écran entier**
- **Pour les zones changeant constamment**

Pour plus d'informations sur la politique d'**utilisation d'un codec vidéo pour la compression**, consultez la section [Utiliser un codec vidéo pour la compression](#).

La sélection automatique s'applique uniquement aux variantes YUV 4:2:0 de ces codecs. Le format YUV 4:2:0 utilisant moins de bande passante, la qualité est réduite. Si le paramètre de la politique **Qualité visuelle** est défini sur **Sans perte si possible** ou **Toujours sans perte** et si la politique **Autoriser l'absence de perte visuelle** est définie sur **Activée**, la sélection automatique du codec vidéo est désactivée et le format YUV 4:4:4 H.264 ou H.265 est utilisé à la place.

Pour plus d'informations sur ces politiques, consultez les sections suivantes :

- [Qualité visuelle](#)
- [Autoriser la compression visuelle sans perte](#)

Remarque :

Le format YUV 4:2:0 est un sous-échantillonnage chromatique et une technique de compression des couleurs qui réduit la consommation globale de bande passante.

Lors de la connexion à une ressource, l'application Citrix Workspace teste la capacité du point de terminaison à decoder les codecs vidéo H.265 et AV1 et à enregistrer ces fonctionnalités dans le registre. L'application Citrix Workspace sélectionne ensuite automatiquement le meilleur codec vidéo à utiliser et négocie ce codec avec le VDA. Si le VDA et le client peuvent utiliser les codecs H.265 et AV1, AV1 est sélectionné comme codec vidéo. Si AV1 n'est disponible ni sur le VDA ni sur le client, H.265 est sélectionné. Si H.265 n'est pas non plus disponible sur l'un et l'autre, la session utilise H.264 comme codec vidéo.

Cette fonctionnalité est activée par défaut.

Pour désactiver la sélection automatique du codec vidéo, définissez **DisableDecoderCaps** comme suit :

1. Ouvrez 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`.

Ou

Accéder à `HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Graphics Engine`

3. Créez une clé DWORD nommée **DisableDecoderCaps** et définissez la valeur de la clé sur 1.

Si la valeur de **DisableDecoderCaps** est définie sur 1 dans HKEY_LOCAL_MACHINE ou HKEY_CURRENT_USER, la sélection automatique du codec vidéo n'est pas utilisée.

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. Le codec vidéo H.265 doit être pris en charge et activé à la fois sur le VDA et sur l'application Citrix Workspace. Si 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.

Pré-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.

GPU client prenant en charge le décodage H.265 :

- GPU NVIDIA de génération Pascal ou version ultérieure
- GPU Intel de 6e génération ou version ultérieure
- AMD de génération GCN3 ou version ultérieure

Remarque :

cette fonctionnalité doit satisfaire à d'autres exigences en matière de VDA, telles que les suivantes :

- GPU NVIDIA de génération Maxwell ou version ultérieure
- GPU Intel de 6e génération ou version ultérieure
- GPU AMD de génération Raven ou version ultérieure

Cette fonctionnalité est automatiquement activée avec l'introduction de la fonctionnalité **Sélection automatique du codec vidéo**.

Ce comportement est modifiable en contrôlant explicitement le décodage H.265 à l'aide de la clé de registre **EnableH265** côté client.

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

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

1. Ouvrez l'Éditeur du Registre en tapant `regedit` dans la commande Exécuter.
2. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine`.
3. Créez une clé DWORD nommée **EnableH265** et définissez la valeur de la clé sur 1.
4. Redémarrez la session pour que les modifications prennent effet.

La présence de la clé **EnableH265** désactive la détection automatique. La définition de la clé **EnableH265** sur 0 désactive le décodage H.265. Par conséquent, la session n'utilise pas le codec vidéo H.265, même s'il est configuré sur le VDA.

En définissant la clé **EnableH265** sur 1, l'application Citrix Workspace pour Windows essaie d'utiliser le décodage H.265. Si le décodage H.265 échoue, le client et le serveur reviennent au codage H.264.

Il est également possible d'activer l'utilisation du codec H.265 en configurant 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 (GPO) :

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 >> Expérience utilisateur**.
3. Sélectionnez la stratégie Décodage H265 pour graphiques.
4. Sélectionnez **Activé**.
5. Cliquez sur **Appliquer**, puis sur **OK**.
6. 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, les paramètres de la stratégie Décodage H265 pour graphiques sont ignorés. La fonctionnalité n'est donc pas appliquée et le codec vidéo H.264 est utilisé.
- Vous pouvez utiliser l'indicateur d'état des graphiques et Citrix HDX Monitor pour valider l'

utilisation du codec vidéo.

AV1

L'application Citrix Workspace prend en charge l'utilisation du codec vidéo AV1 pour l'accélération matérielle des graphiques et vidéos distants. Le codec vidéo AV1 doit être pris en charge et activé sur le VDA et dans l'application Citrix Workspace.

Les prérequis du codec AV1 sont les suivants :

- VDA 2308 ou version ultérieure.
- Application Citrix Workspace 2305 pour Windows ou version ultérieure
- Activez la stratégie **Utiliser le codage matériel pour le codec vidéo** sur le VDA (par défaut).
- L'application Citrix Workspace pour Windows est conforme à la configuration matérielle client suivante pour AV1 :
 - NVIDIA Ampere ou version ultérieure
 - Intel 11e génération/Arc ou version ultérieure
 - AMD Radeon RX 6000/Radeon Pro W6000 series (RDNA2) ou version ultérieure

Remarque :

AV1 requiert de satisfaire à d'autres exigences en matière de VDA, telles que les suivantes :

- GPU de génération NVIDIA Lovelace ou version ultérieure (par exemple, L4/L40)
- GPU Intel de génération Arc ou version ultérieure

Cette fonctionnalité est automatiquement activée avec l'introduction de la fonctionnalité **Sélection automatique du codec vidéo**.

Ce comportement est modifiable en contrôlant explicitement le décodage AV1 à l'aide de la clé de registre **EnableAV1** côté client.

Configuration du codage vidéo AV1 à l'aide de l'Éditeur du Registre :

Activation du codage vidéo AV1 sur un réseau n'appartenant pas au domaine sur un système d'exploitation 32 bits :

1. Ouvrez 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 **EnableAV1** et définissez la valeur de la clé sur 1.
4. Redémarrez la session pour que les modifications prennent effet.

Activation du codage vidéo AV1 sur un réseau n'appartenant pas au domaine sur un système d'exploitation 64 bits :

1. Ouvrez 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 **EnableAV1** et définissez la valeur de la clé sur 1.
4. Redémarrez la session pour que les modifications prennent effet.

La présence de la clé **EnableAV1** désactive la détection automatique. La définition de **EnableAV1** sur 0 désactive le décodage AV1 de sorte que la session n'utilise pas le codec vidéo AV1.

En définissant la clé **EnableAV1** sur 1, l'application Citrix Workspace pour Windows essaie d'utiliser le décodage AV1. Si le décodage AV1 échoue, le client et le serveur reviennent au codage H.264.

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 AV1 pour graphiques sont ignorés et la fonctionnalité ne fonctionne pas. La fonctionnalité n'est donc pas appliquée et le codec vidéo H.264 est utilisé.

Vous pouvez utiliser l'indicateur d'état des graphiques et Citrix HDX Monitor pour valider l'utilisation du codec vidéo.

Microsoft Teams optimisé

April 22, 2024

Ajout de la prise en charge de tonalités courtes dans Microsoft Teams optimisé

Auparavant, lorsque la fonction de sonnerie secondaire était activée, les tonalités courtes, telles que les bips ou les notifications, étaient émises à plusieurs reprises. Par exemple, la tonalité émise lorsqu'un invité rejoignait la réunion Microsoft Teams était répétée. La seule solution était de quitter et de redémarrer Microsoft Teams. Ce problème entraînait une expérience utilisateur médiocre.

L'application Citrix Workspace prend en charge la lecture des tonalités courtes selon vos besoins. Cette prise en charge active également la fonction de sonnerie secondaire.

Pré-requis :

Effectuez une mise à jour vers la dernière version de Microsoft Teams.

Expérience améliorée pour des visioconférences dans Microsoft Teams optimisé

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

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

Flou et effets d'arrière-plan pour l'optimisation de Microsoft Teams avec HDX

L'application Citrix Workspace pour Windows prend désormais en charge le flou et les effets d'arrière-plan dans l'optimisation Microsoft Teams avec HDX.

Vous pouvez flouter ou remplacer l'arrière-plan par une image personnalisée et éviter les distractions inattendues en aidant la conversation à rester centrée sur la silhouette (corps et visage). La fonctionnalité peut être utilisée avec les appels P2P ou les conférences téléphoniques.

Vous pouvez sélectionner les options de flou et d'effets d'arrière-plan suivantes :

- Aucun effet d'arrière-plan
- Sélectionner le flou d'arrière-plan
- Sélectionner l'image d'arrière-plan

Remarque :

Cette fonctionnalité est désormais intégrée à l'interface utilisateur/aux boutons de Microsoft Teams. La prise en charge de fenêtres multiples est une condition préalable qui nécessite une mise à jour du VDA vers 2112 ou une version ultérieure. Pour plus d'informations, consultez Réunions et chat en mode multi-fenêtres.

Limitations :

- Le remplacement de l'arrière-plan défini par l'utilisateur n'est pas pris en charge.
- L'effet d'arrière-plan ne persiste pas entre les sessions. Lorsque vous fermez et relancez Microsoft Teams ou que le VDA est reconnecté, l'effet d'arrière-plan est réinitialisé sur Désactivé.
- Une fois la session ICA reconnectée, l'effet est désactivé. Toutefois, une coche sur l'interface utilisateur de Microsoft Teams indique que l'effet précédent est toujours activé. Citrix et Microsoft travaillent ensemble pour résoudre ce problème.
- L'appareil doit être connecté à Internet lors du remplacement de l'image d'arrière-plan.

Remarque :

Cette fonctionnalité est disponible uniquement après le déploiement d'une future mise à jour de Microsoft Teams. Une fois la mise à jour déployée par Microsoft, vous pourrez consulter les articles [CTX253754](#) et [Microsoft 365 Public roadmap](#) pour la mise à jour de la documentation et l'annonce.

Annulation d'écho acoustique

L'annulation d'écho dans `HdxRtcEngine.exe` peut être désactivée pour résoudre les problèmes de performances audio ou de compatibilité avec les périphériques dotés de fonctionnalités AEC intégrées.

Accédez au chemin du registre `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` et créez la clé suivante :

Nom : EnableAEC

Type : REG_DWORD

Données : 0

(0 désactive AEC ; 1 active AEC. Si `Regkey` n'est pas présent, le comportement par défaut dans `HdxRtcEngine` est d'activer AEC, quelles que soient les capacités matérielles du périphérique.)

Amélioration apportées à l'optimisation de Microsoft Teams

- La version de WebRTC utilisée pour Microsoft Teams optimisé a été mise à niveau vers la version M98.
- **Modification du comportement de sélection des périphériques audio pour la version optimisée de Microsoft Teams** - Lorsque vous modifiez les périphériques audio par défaut dans les paramètres audio du terminal, Microsoft Teams optimisé dans Citrix VDI modifie la sélection actuelle de périphériques audio pour qu'elle corresponde aux valeurs par défaut du terminal.

```
1 However, if you make an explicit device selection in Microsoft Teams, your selection takes precedence and does not follow the endpoint defaults. Your selection is persistent until you clear the Microsoft Teams cache.
```

Pour plus d'informations sur les fonctionnalités incluses dans les versions qui ont atteint la fin de vie (EOL), consultez l'[ancienne documentation](#).

Transport HDX

April 22, 2024

Débit adaptatif HDX

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

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

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

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

Important :

Le débit adaptatif HDX modifie les tampons de sortie en déplaçant ce mécanisme du client vers le VDA. Par conséquent, l'ajustement du nombre de mémoires tampons de sortie sur le client, tel que décrit dans l'article du centre de connaissances [CTX125027](#), n'a aucun effet.

Transport adaptatif

Le transport adaptatif est un mécanisme de Citrix Virtual Apps and Desktops et Citrix DaaS qui permet d'utiliser Enlightened Data Transport (EDT) comme protocole de transport pour les connexions ICA. Pour de plus amples informations, consultez la section [Transport adaptatif](#) dans la documentation Citrix Virtual Apps and Desktops.

Mode de tolérance de pertes pour l'audio

L'application Citrix Workspace utilise le mode de tolérance aux pertes pour la redirection audio. Cette fonctionnalité améliore l'expérience utilisateur pour le streaming en temps réel lorsque les utilisateurs se connectent via des réseaux à latence élevée et à perte de paquets.

Vous devez utiliser la version 2311 ou ultérieure du VDA. Par défaut, cette fonctionnalité est activée sur l'application Citrix Workspace pour Windows. Par contre, elle est désactivée sur le VDA.

Pour activer le mode de tolérance de pertes pour l'audio, configurez la valeur de registre suivante et redémarrez la machine.

Pour un VDA multi-session :

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio
- Nom de la valeur : EdtUnreliableAllowed
- Type de valeur : DWORD
- Données de valeur : 1

Pour un poste de travail VDA :

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio
- Nom de la valeur : EdtUnreliableAllowed
- Type de valeur : DWORD
- Données de valeur : 1

Redirection du contenu du navigateur

April 22, 2024

La redirection du contenu du navigateur empêche le rendu des pages Web sur liste d'autorisation du côté VDA. Cette fonctionnalité utilise l'application Citrix Workspace pour instancier un moteur de rendu correspondant côté client, qui récupère le contenu HTTP et HTTPS de l'URL.

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

- Les cookies persistent d'une session à l'autre : lorsque vous quittez et relancez un navigateur, vous n'êtes pas invité à saisir à nouveau vos informations d'identification.
- Les navigateurs respectent désormais la langue définie sur le système local.

Pour plus d'informations, consultez la section [Redirection du contenu du navigateur](#).

Important :

- La redirection du contenu du navigateur peut être activée pour 2402 LTSR à l'aide de la ligne de commande
- Elle est activée par défaut pour toutes les versions actuelles de l'application Citrix Workspace pour Windows.
- La redirection du contenu du navigateur n'est pas prise en charge pour les versions 1912 et 2203.1 LTSR de l'application Citrix Workspace.

Pour activer la redirection du contenu du navigateur sur le VDA, assurez-vous que les stratégies suivantes sont activées sur Citrix Web Studio :

- [Redirection du contenu du navigateur](#)
- [Configuration de l'ACL de redirection du contenu de navigateur](#)
- [Sites d'authentification de redirection du contenu du navigateur](#)

Configurer le chemin du stockage des données temporaires du navigateur pour la superposition de redirection du contenu du navigateur

Vous pouvez configurer le chemin de stockage des données temporaires pour un navigateur basé sur Chromium Embedded Framework (CEF). Vous pouvez configurer le chemin sur le VDA ou le client comme suit :

Sur le VDA :

1. Ouvrez l'Éditeur du Registre en tapant `regedit` dans la commande Exécuter.
2. Accédez au chemin du registre `HKEY_LOCAL_MACHINE\Software\Citrix\DXMediaStream\ClientConfigurations\WindowsCef`.
3. Créez l'entrée de chaîne **BCRProfilePath** et définissez sa valeur sur folder pour les fichiers BCRtmp basés sur CEF. Par exemple :

```
"BCRProfilePath"="C:\\tmp\\AlternateBcrProfilePath"
```

4. Redémarrez la session pour que les modifications prennent effet.

Sur le client :

1. Ouvrez l'Éditeur du Registre en tapant `regedit` dans la commande Exécuter.
2. Accédez au chemin du registre `HKEY_CURRENT_USER\Software\Citrix\HdxMediaStream`.
3. Créez une valeur de registre avec les attributs suivants :
 - Nom de la clé de registre : `BCRProfilePath`

- Valeur de registre : chaîne <folder for CEF based BCRtmp files>

4. Redémarrez l'application Citrix Workspace pour que les modifications prennent effet.

Remarque :

Chromium Embedded Framework (CEF) est mis à niveau vers la version 117. Cette mise à niveau de version permet de résoudre les failles de sécurité.

Limitations :

La redirection du contenu du navigateur présente les limites suivantes :

- Ne prend pas en charge les applications Web qui nécessitent des fenêtres contextuelles ou la persistance des cookies de session.
- Microsoft Internet Explorer n'est pas pris en charge.
- Les applications qui dépendent du service d'authentification de Google (comme Google Meet) sont actuellement bloquées.
- Actuellement, le plug-in d'extension n'est pas officiellement publié sur Microsoft Edge. Il existe toutefois une solution.
- La stratégie de redirection vidéo HTML5 doit être désactivée lorsque la redirection du contenu du navigateur est utilisée.
- Les utilisateurs finaux peuvent parfois être déconnectés de leurs sessions en raison d'un manque de fiabilité réseau, de temps d'attente réseau très variables ou de limites des terminaux sans fil. La redirection du contenu du navigateur ne dispose pas d'un mécanisme de repli ou de reporting suffisant pour prendre en charge de tels scénarios.
- Les fichiers téléchargés via la superposition sont stockés localement (sur la machine cliente de l'utilisateur final).

Amélioration des performances de la redirection du contenu du navigateur

Auparavant, la redirection du contenu du navigateur utilisait le cache d'espace disque côté client et les informations mises en cache n'étaient pas supprimées lors d'une mise à niveau. Cette configuration s'est traduite par une augmentation de l'utilisation de l'espace disque au fil du temps et un comportement incohérent lors de la redirection d'une page avec la redirection du contenu du navigateur.

Pour résoudre ce problème, la redirection du contenu du navigateur utilise un cache en mémoire. Cette amélioration contribue à améliorer les performances de la redirection du contenu du navigateur.

Cette fonction est désactivée par défaut. Vous pouvez activer cette fonctionnalité sur un VDA ou un client comme suit :

Sur le VDA :

1. Ouvrez l'Éditeur du Registre en tapant `regedit` dans la commande Exécuter.
2. Accédez au chemin du registre `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXMediaStream\ClientConfigurations\WindowsCef`.
3. Créez une clé `DWORD` nommée `BCRStoreCEFCacheInMemory` et définissez la valeur de la clé sur 1.

Si la valeur de `BCRStoreCEFCacheInMemory` est définie sur 0, la redirection du contenu du navigateur utilise l'espace disque du client.

Sur le client :

1. Ouvrez l'Éditeur du Registre en tapant `regedit` dans la commande Exécuter.
2. Accédez au chemin du registre `HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream`.
3. Créez une clé `DWORD` nommée `BCRStoreCEFCacheInMemory` et définissez la valeur de la clé sur 1.

Si la valeur de `BCRStoreCEFCacheInMemory` est définie sur 0, la redirection du contenu du navigateur utilise l'espace disque du client.

Remarque :

- Si `BCRStoreCEFCacheInMemory` est défini à la fois sur le client et sur le VDA, le paramètre sur le client est prioritaire.
- Si `BCRProfilePath` et `BCRStoreCEFCacheInMemory` sont tous les deux définis, la configuration de `BCRProfilePath` est prioritaire et la configuration de `BCRStoreCEFCacheInMemory` n'est pas prise en compte.

Limitation :

La limite de taille du cache en mémoire est fixée à 10 Mo.

Redirection bidirectionnelle du contenu

April 22, 2024

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.

Citrix propose la redirection hôte vers client et Local App Access pour la redirection client vers URL. Toutefois, 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**.

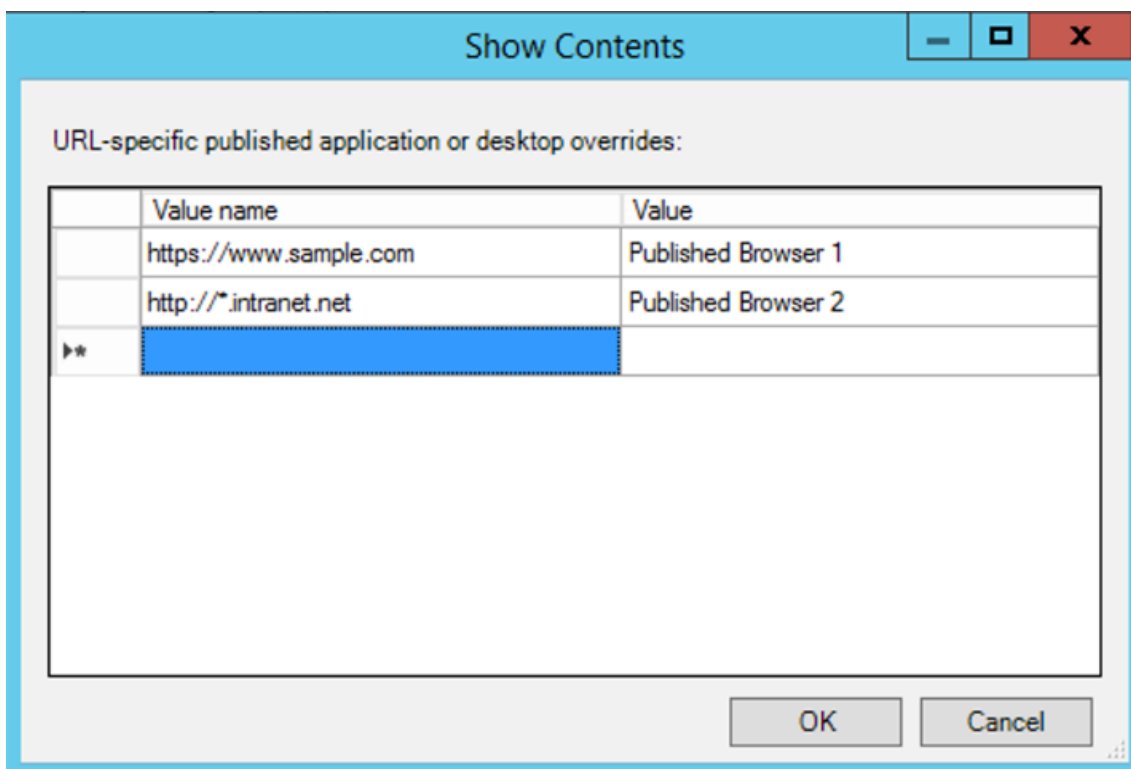
1. Dans le champ **Nom de l'application/du bureau publié**, indiquez le nom de la ressource utilisée pour lancer l'URL redirigée.

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** et **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 sur le client de l'application Citrix Workspace et 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 utilisent 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 lorsqu'une adresse URL est redirigée sur le client. Lorsqu'une 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 existe et que les stratégies de redirection de contenu hôte sont définies sur Activé sur la même machine. Citrix vous recommande de désactiver soit la fonctionnalité d'association de type de fichier serveur ou de redirection de contenu hôte (URL) pour vous assurer que la redirection d'URL fonctionne correctement.
- Dans Internet Explorer, cliquez sur **Paramètres > Options Internet > Avancé**, puis cochez la case **Activer les extensions tierce partie du navigateur** dans la section **Navigation**.

Limitation :

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

Prise en charge des URL bidirectionnelles avec les navigateurs Chromium

La redirection bidirectionnelle de contenu vous permet de configurer les URL pour qu'elles soient redirigées du client vers le serveur et du serveur vers le client à l'aide de stratégies sur le serveur et le client.

Les stratégies de serveur sont définies sur le Delivery Controller et les stratégies client sont définies sur l'application Citrix Workspace à l'aide du modèle d'administration de l'objet de stratégie de groupe (GPO).

À partir de la version 2106, la prise en charge de la redirection bidirectionnelle d'URL a été ajoutée pour Google Chrome et Microsoft Edge.

Pré-requis :

- Citrix Virtual Apps and Desktops 2106 ou versions ultérieures
- Extension de redirection du navigateur version 5.0.

Pour enregistrer le navigateur Google Chrome avec la redirection bidirectionnelle d'URL, exécutez la commande suivante à partir du dossier d'installation de l'application Citrix Workspace :

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome / verbose
```

Remarque :

Lorsque vous utilisez ces commandes sur les navigateurs Chrome, l'[extension de redirection bidirectionnelle du contenu](#) est installée automatiquement à partir du Chrome Web Store.

Pour annuler l'enregistrement du navigateur Google Chrome de la redirection bidirectionnelle d'URL, exécutez la commande suivante à partir du dossier d'installation de l'application Citrix Workspace :

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome / verbose
```

Remarque :

Si l'erreur suivante s'affiche lorsque vous accédez à la page Extensions du navigateur, ignorez le message :

```
Websocket connection to wss://... failed.
```

Pour plus d'informations sur la configuration de la redirection des URL sur l'application Citrix Workspace, consultez [.Redirection bidirectionnelle du contenu](#).

Pour plus d'informations sur la redirection de contenu du navigateur, consultez [Redirection du contenu de navigateur](#) dans la documentation Citrix Virtual Apps and Desktops.

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 les utilisateurs souhaitent afficher plusieurs bureaux simultanément, les informations peuvent être 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 possi-

bilité 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 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 de 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\...

Référence des paramètres ICA

April 22, 2024

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 \(PDF\)](#)

Appareils

April 22, 2024

Cette section décrit les éléments suivants :

- [Souris](#)
- [Clavier](#)
- [Impression](#)
- [USB](#)
- [Mappage des lecteurs clients](#)
- [Microphone](#)

Souris

April 22, 2024

Souris relative

La fonctionnalité de la souris relative détermine la distance de déplacement de la souris depuis la dernière image dans une fenêtre ou un écran.

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

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. L'interprétation est requise pour les applications qui exigent des entrées de souris relatives plutôt qu'absolues.

Vous pouvez configurer la fonctionnalité par utilisateur et par session, ce qui donne un contrôle plus granulaire sur la disponibilité des fonctionnalités.

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.

Configurer la souris relative à l'aide de l'Éditeur du Registre

Pour configurer la fonctionnalité, définissez les clés de registre suivantes le cas échéant, puis redémarrez la session pour que les modifications prennent effet :

Pour que la fonctionnalité soit disponible par session :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse

Pour que la fonctionnalité soit disponible par utilisateur :

HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse

- Nom : RelativeMouse
- Type : REG_SZ
- Valeur : True

Remarque :

- Les valeurs définies dans l'Éditeur du Registre ont priorité sur les paramètres du fichier ICA.
- Les valeurs définies dans HKEY_LOCAL_MACHINE et HKEY_CURRENT_USER doivent être les mêmes. Différentes valeurs peuvent provoquer des conflits.

Configurer la souris relative à l'aide du fichier default.ica

1. Ouvrez le fichier default.ica qui se trouve généralement sur `C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica` où « site name » est le nom spécifié pour le site lors de sa création. Pour les clients StoreFront, le fichier default.ica se trouve 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 clé avec le nom RelativeMouse dans la section WFClient. Définissez sa valeur 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.

Clavier

April 22, 2024

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

Prise en charge des icônes de couleurs 32 bits dans l'application Citrix Workspace :

L'application Citrix Workspace prend en charge les icônes de couleur élevée 32 bits. Pour fournir des applications transparentes, elle sélectionne automatiquement la profondeur de couleur pour :

- les applications visibles dans la boîte de dialogue **Centre de connexion**,
- le menu Démarrer, et
- la barre des tâches.

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.

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.

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

L'intégration du menu Démarrer et la fonction 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, et pour les utilisateurs qui ont besoin d'accéder à un ensemble d'applications de base de manière cohérente.

L'indicateur, nommé appelé **SelfServiceMode**, est défini sur `True` par défaut. Lorsque l'administrateur définit l'indicateur **SelfServiceMode** sur `False`, vous ne pouvez pas accéder à l'interface utilisateur en libre-service. Au lieu de cela, vous pouvez accéder aux applications faisant l'objet d'une souscription depuis le menu Démarrer ou à l'aide de raccourcis bureau, connu sous le nom de mode Raccourci uniquement.

Les utilisateurs et les administrateurs peuvent utiliser plusieurs 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 vous supprimez une icône de raccourci du bureau, l'icône est rétablie lorsque l'utilisateur sélectionne **Actualiser** depuis l'icône de l'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 pour 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. Les administrateurs peuvent également fournir des privilèges spéciaux en ajoutant manuellement une clé de registre (HideEditStores-Dialog) sur l'ordinateur client. 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. Après avoir modifié 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 10 n'autorise pas la création de dossiers imbriqués dans le menu Démarrer. Les applications peuvent apparaître dans 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.
- La fonctionnalité Auto Re-install Modified Apps peut être activée à l'aide de la clé de Registre [AutoReInstallModifiedApps](#). Lorsque [AutoReInstallModifiedApps](#) est activé, les modifications apportées aux attributs d'applications et de bureaux publiés sur le serveur sont affichées sur la machine cliente. Lorsque la clé [AutoReInstallModifiedApps](#) est désactivée, les attributs d'applications et de bureaux ne sont pas mis à jour. De plus, les raccourcis ne sont pas restaurés lors de l'actualisation s'ils sont supprimés sur le client. Par défaut, [AutoReInstallModifiedApps](#) est activée.

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**.
- Modifiez les clés de registre avant de configurer un magasin. Si, à tout moment, vous ou un utilisateur souhaitez personnaliser les clés de registre, vous ou l'utilisateur devez :
 1. réinitialiser l'application Citrix Workspace
 2. configurer les clés de registre, puis
 3. reconfigurer le magasin.

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. Par exemple, le contrôle de l'espace de travail permet 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, le contrôle de l'espace de travail 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 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 la 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 la valeur : 0

Remarque :

Vous pouvez également définir la clé **WSCReconnectAll** sur false si vous ne souhaitez pas créer de clé.

Clés de registre pour machines 32 bits

Clé de registre : WSCSupported Valeur : True

Chemin d'accès à la clé :

- 1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
- 2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
- 4 - HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

Clé de registre : WSCReconnectAll Valeur : True

Chemin d'accès à la clé :

- 1 - `HKEY_CURRENT_USER\Software\Citrix\Dazzle`
- 2 - `HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties`
- 3 - `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle`
- 4 - `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle`

Clé de Registre : WSCReconnectMode Valeur : 3

Chemin d'accès à la clé :

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
  primaryStoreID +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

Clé de Registre : WSCReconnectModeUser Valeur : le registre n'est pas créé lors de l'installation.

Chemin d'accès à la clé :

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
  +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

Clés de registre pour machines 64 bits :

Clé de registre : WSCSupported Valeur : True

Chemin d'accès à la clé :

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
  +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

Clé de registre : WSCReconnectAll Valeur : True

Chemin d'accès à la clé :

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
  primaryStoreID + \Properties
3 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

Clé de Registre : WSCReconnectMode Valeur : 3

Chemin d'accès à la clé :

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
  primaryStoreID +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

Clé de Registre : WSCReconnectModeUser **Valeur :** le registre n'est pas créé lors de l'installation.

Chemin d'accès à la clé :

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
  +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

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 vous permet de basculer entre leurs dispositions de clavier préférées sur la machine cliente. Cette fonction est désactivée par défaut. La synchronisation de la disposition du clavier permet à la disposition du clavier client de se synchroniser automatiquement avec la session d'applications et de bureaux virtuels.

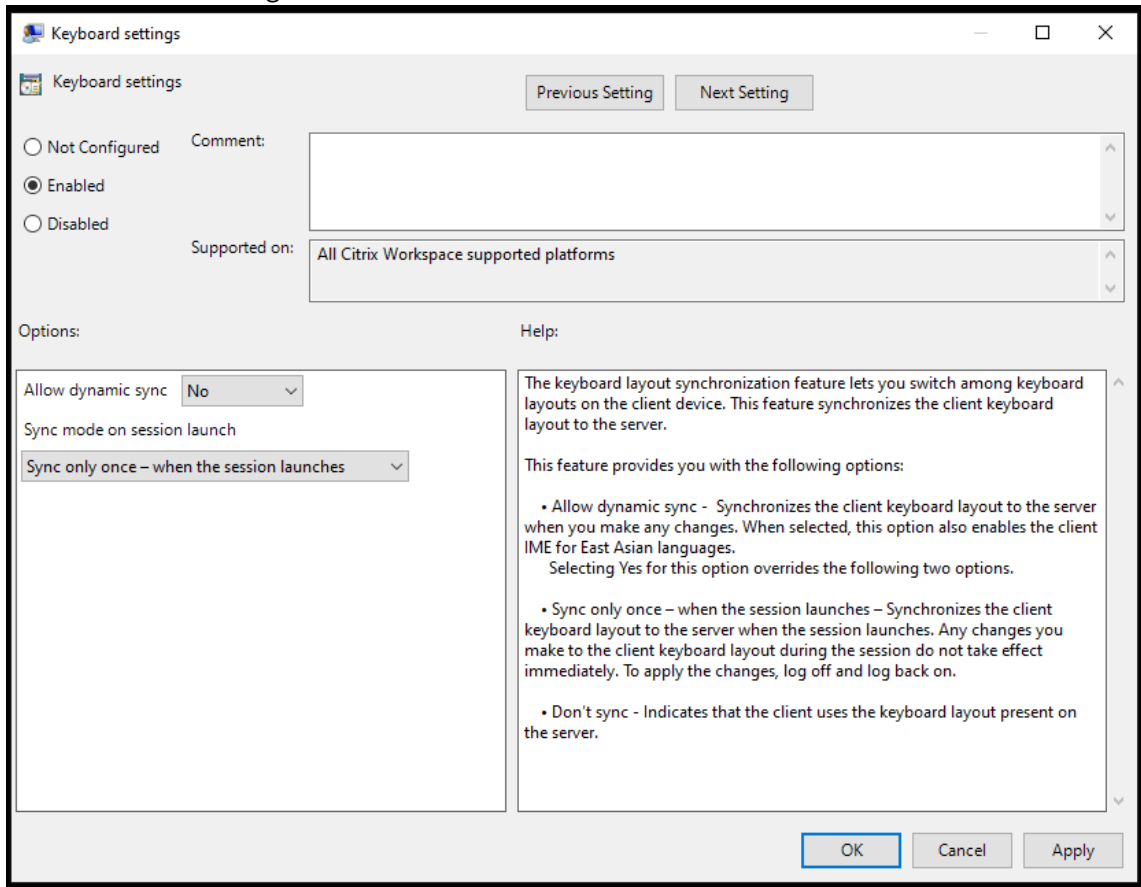
Pour configurer la synchronisation de la disposition du clavier à l'aide du modèle d'administration GPO :

Remarque :

La configuration de l'objet de stratégie de groupe a priorité sur les configurations de StoreFront et l'interface graphique.

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** ou **Configuration utilisateur**, accédez à **Modèles d'administration > Modèles d'administration (ADM) > Composants Citrix > Citrix Workspace > Expérience utilisateur**.

3. Sélectionnez la stratégie **Paramètres du clavier**.



4. Sélectionnez **Activé** et sélectionnez l'une des options suivantes :

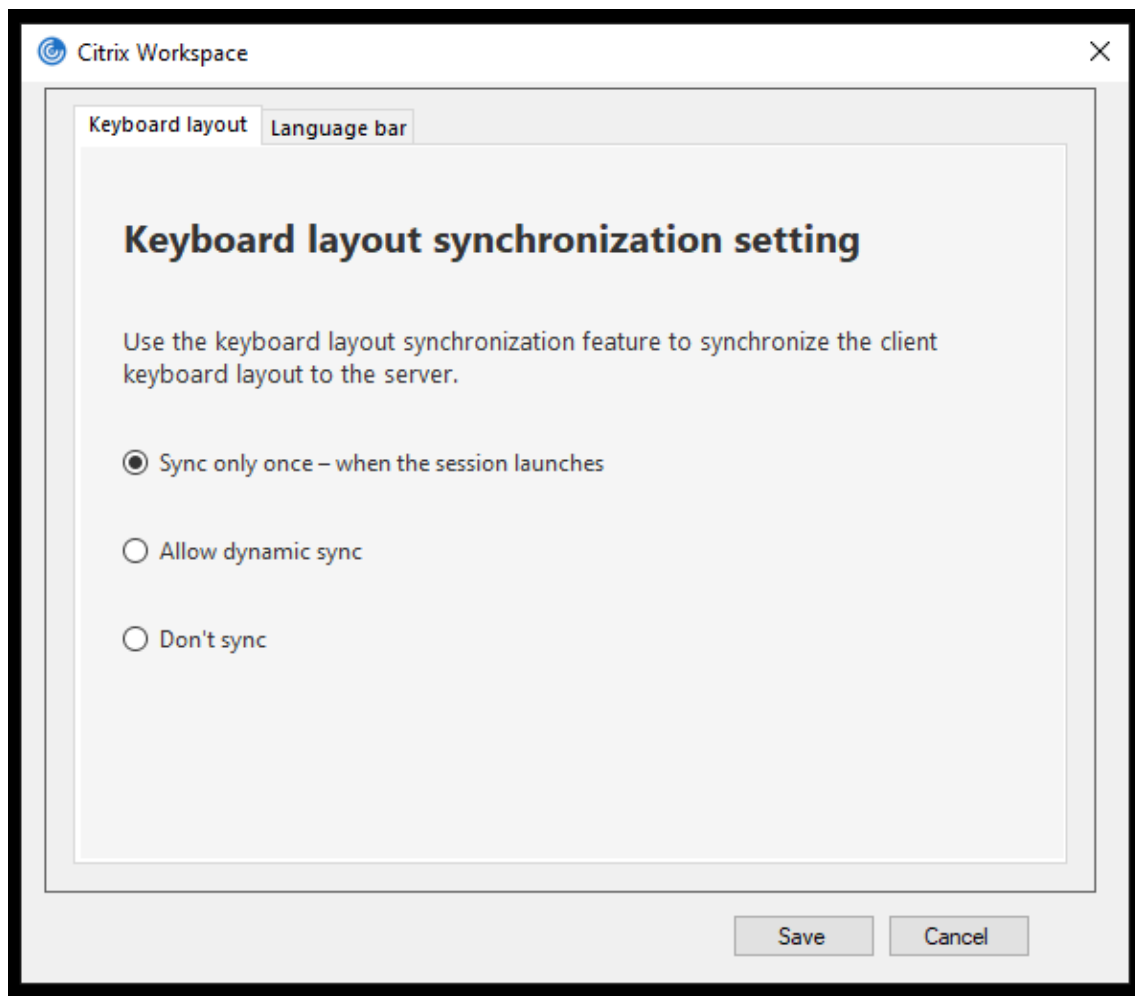
- **Autoriser la synchronisation dynamique** - Dans le menu déroulant, sélectionnez **Oui** ou **Non**. Cette option synchronise la disposition du clavier client sur le serveur lorsque vous modifiez la disposition du clavier client. Lorsqu'elle est sélectionnée, cette option active également l'éditeur IME du client pour les langues d'Asie de l'Est. Si vous sélectionnez **Oui** pour cette option, vous remplacez les deux options suivantes.
- **Mode de synchronisation lors du lancement de la session** - Dans le menu déroulant, sélectionnez l'une des options suivantes :
 - **Synchroniser une seule fois –lorsque la session est lancée** - Synchronise la disposition du clavier du client avec le serveur lorsque la session est lancée. Les modifications que vous apportez à la disposition du clavier du client pendant la session ne prennent pas effet immédiatement. Pour appliquer les modifications, déconnectez-vous et reconnectez-vous.
 - **Ne pas synchroniser** - Indique que le client utilise la disposition du clavier présente sur le serveur.

5. Sélectionnez **Appliquer** et **OK**.

Pour configurer la synchronisation de la disposition du clavier à l'aide de l'interface utilisateur graphique :

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 :
 - **Synchroniser une seule fois - lorsque la session est lancée** : indique que la disposition du clavier n'est synchronisée à partir du VDA qu'une seule fois au lancement de la session.
 - **Autoriser la synchronisation dynamique** : indique que la disposition du clavier est synchronisée dynamiquement avec le VDA lorsque le clavier client est modifié dans une session.
 - **Ne pas synchroniser** : indique que le client utilise la disposition du clavier présente sur le serveur.
3. Cliquez sur **Enregistrer**.

Pour configurer la synchronisation de la disposition du clavier à l'aide de la CLI :

Exécutez la commande suivante à partir du dossier d'installation de l'application Citrix Workspace pour Windows.

En général, le dossier d'installation de l'application Citrix Workspace se trouve sous `C:\Program files (x86)\Citrix\ICA Client`.

- Pour activer : `wfica32.exe /localime:on`
- Pour désactiver : `wfica32.exe /localime:off`

L'utilisation de l'option de disposition du clavier client 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 client 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.

Configuration de la synchronisation de la disposition du clavier à l'aide de l'interface de ligne de commande Les commandes suivantes ont été ajoutées pour configurer la synchronisation de la disposition du clavier à l'aide de l'interface de ligne de commande :

Commandes	Description
<code>wfica32.exe /kbdsyncmode:once</code>	Définit le mode de synchronisation du clavier sur « Synchroniser une seule fois ».
<code>wfica32.exe /kbdsyncmode:dynamic</code>	Définit le mode de synchronisation du clavier sur « Synchronisation dynamique ».
<code>wfica32.exe /kbdsyncmode:no</code>	Définit le mode de synchronisation du clavier sur « Ne pas synchroniser ».

Exécutez les commandes précédentes à partir du dossier d'installation de l'application Citrix Workspace pour Windows.

Généralement, le dossier d'installation de l'application Citrix Workspace se trouve sous `C:\Program files (x86)\Citrix\ICA Client`.

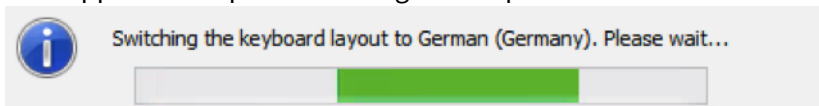
Configuration de la synchronisation du clavier sur un VDA Windows

Remarque :

La procédure suivante s'applique uniquement sur Windows Server 2016 et versions ultérieures. Sur Windows Server 2012 R2 et versions antérieures, la fonctionnalité de synchronisation du clavier est activée par défaut.

1. Lancez l'Éditeur du Registre et naviguez jusqu'à `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Créez l'entrée `DWORD DisableKeyboardSync` et définissez sa valeur sur 0.
 - 1 désactive la fonctionnalité de synchronisation de la disposition du clavier.
3. Redémarrez la session pour que les modifications prennent effet.

Après avoir activé la disposition du clavier sur le VDA et l'application Citrix Workspace, la fenêtre suivante apparaît lorsque vous changez la disposition de clavier.



Cette fenêtre indique que la disposition du clavier session est en cours de basculement vers la disposition du clavier client.

Configuration de la synchronisation du clavier sur un VDA Linux

Lancez l'invite de commande et exécutez la commande suivante :

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar"-v "SyncKeyboardLayout"-d "0x00000001"
```

Redémarrez le VDA pour que les modifications prennent effet.

Pour plus d'informations sur la fonctionnalité de synchronisation de la disposition du clavier sur les VDA Linux, consultez [Synchronisation dynamique de la disposition du clavier](#).

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 que les prob-

lèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre peuvent être résolus. Vous utilisez l'Éditeur du Registre à vos propres risques. 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 la disposition du clavier sur le client est modifiée 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 + Shift`. Pour résoudre ce problème, utilisez la barre de langue dans la session RDP pour changer la disposition du clavier.

Barre de langue

La barre de langue affiche la langue d'entrée préférée dans une session. 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 la barre de langue à l'aide du modèle d'administration GPO :

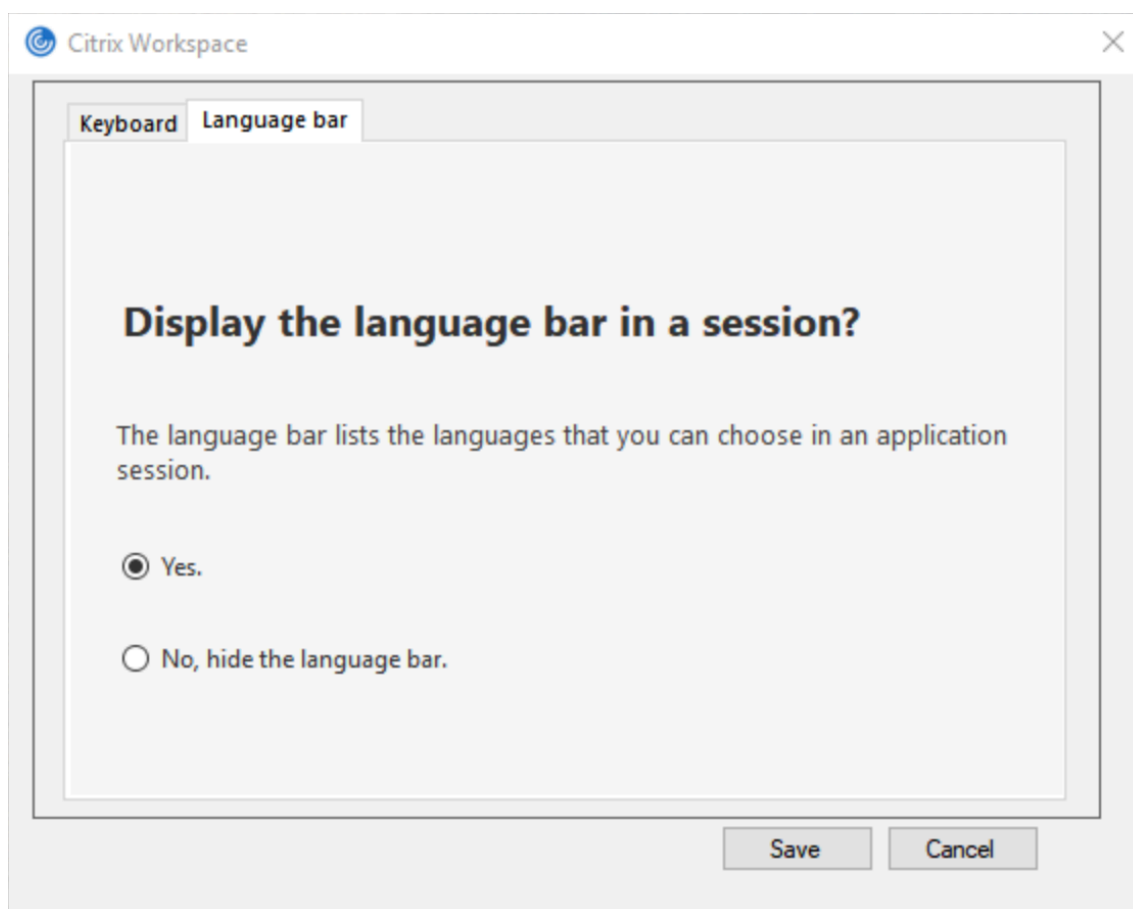
La barre de langue affiche la langue de saisie préférée dans une session.

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** ou **Configuration utilisateur**, accédez à **Modèles d'administration** > **Modèles d'administration (ADM)** > **Composants Citrix** > **Citrix Workspace** > **Expérience utilisateur**.
3. Sélectionnez la stratégie **Barre de langue**.
4. Sélectionnez **Activé** et sélectionnez l'une des options suivantes :
 - Oui : indique que la barre de langue apparaît dans une session d'application.
 - Non, masquer la barre de langue - Indique que la barre de langue est masquée dans une session d'application.
5. Cliquez sur **Appliquer** et **OK**.

Configurer la barre de langue à l'aide de l'interface utilisateur graphique :

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 apparaît 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.

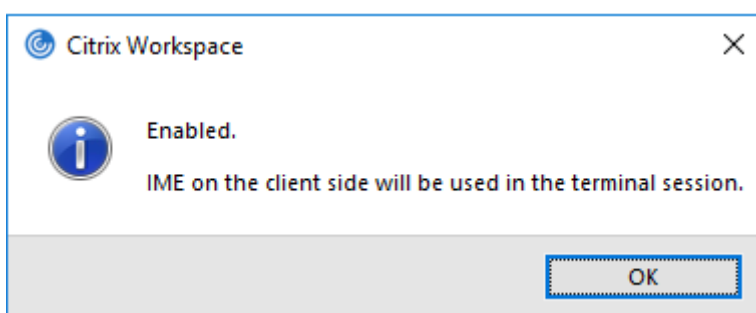
Éditeurs IME clients génériques

Remarque :

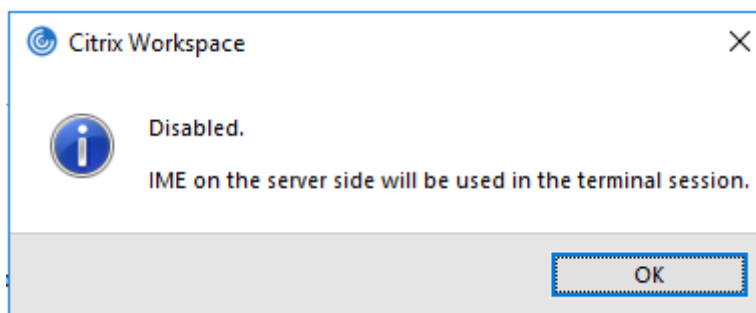
Si vous utilisez un système d'exploitation Windows 10 version 2004, vous pouvez rencontrer certains problèmes techniques lors de l'utilisation de la fonctionnalité IME dans une session. Ces problèmes sont dus à une limitation par un tiers. Pour plus d'informations, veuillez consulter l'[article Microsoft](#).

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`.



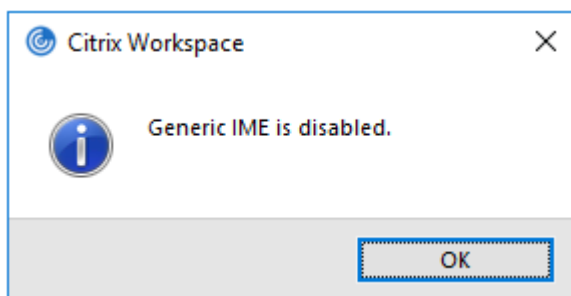
- Pour désactiver l'éditeur IME client générique, exécutez la commande `wfica32.exe /localime:off` à partir du dossier d'installation de l'application Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`.



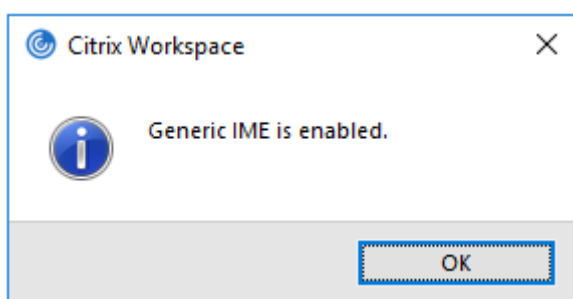
Remarque :

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 le paramètre de synchronisation de la mise en page est défini sur **Désactivé**, le basculement n'active pas l'éditeur IME client générique.

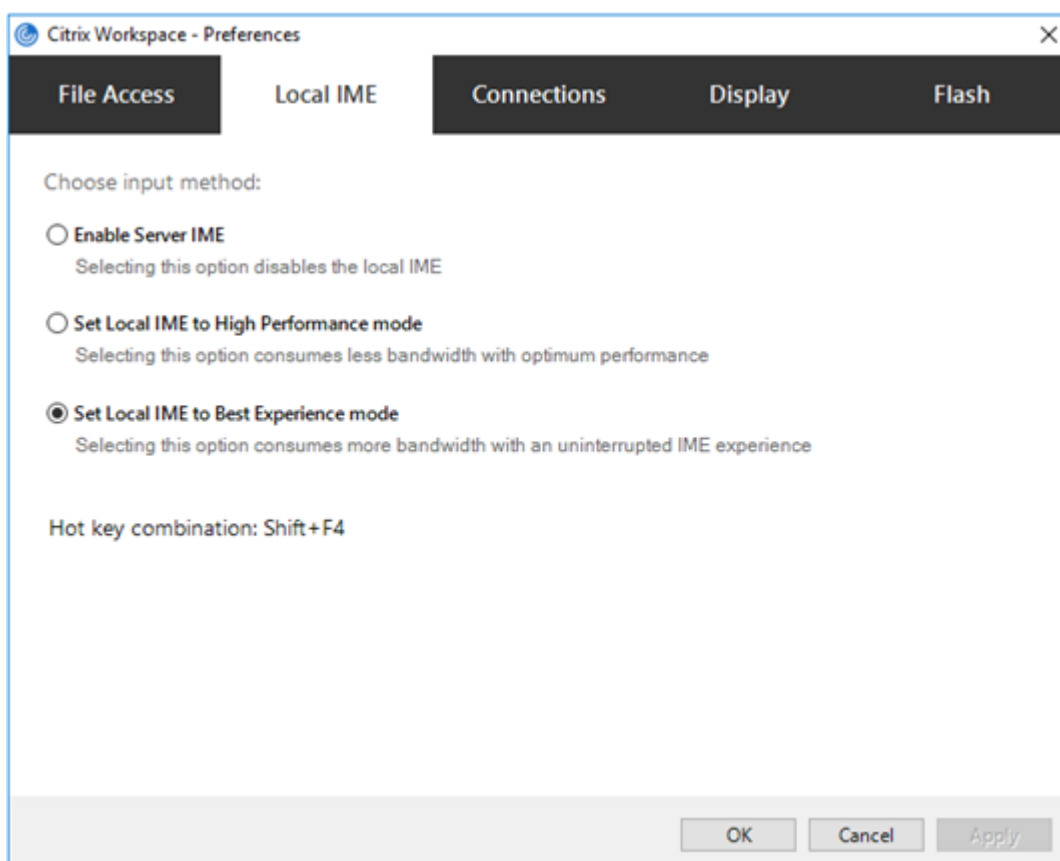
Configuration d'éditeurs IME clients génériques à l'aide de l'interface utilisateur graphique :

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. 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 suivantes 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 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_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Key`

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

Vous pouvez utiliser le raccourci clavier **Maj+F4** pour sélectionner différents modes IME dans une session

Les différentes options des modes IME apparaissent dans le coin supérieur droit de la session lorsque vous basculez à l'aide de ce raccourci clavier.



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 désactiver, cliquez sur **Sécurité** et décochez **Activer le mode protégé**.

Synchronisation de plusieurs claviers en début de session

Auparavant, seul le clavier actif du client était synchronisé avec le VDA après le démarrage de la session en mode plein écran. Dans ce scénario, si vous n'avez configuré **Synchroniser une seule fois lorsque la session est lancée** sur votre application Citrix Workspace et que vous avez dû changer de clavier, vous devez installer manuellement le clavier sur votre poste de travail distant. De même, si vous avez configuré **Autoriser la synchronisation dynamique** sur votre application Citrix Workspace, vous devez basculer en mode fenêtré, modifier le clavier de votre client, puis revenir en mode plein écran.

Tous les claviers disponibles sur le client sont synchronisés avec le VDA après le démarrage de la session en mode plein écran. Vous pouvez sélectionner le clavier requis dans la liste des claviers installés ou disponibles sur le client après le démarrage de la session en mode plein écran.

La fonctionnalité **Synchroniser plusieurs claviers au début de la session** est activée par défaut sur VDA et désactivée par défaut sur l'application Citrix Workspace.

Pré-requis

Dans l'application Citrix Workspace pour Windows :

Activez le paramètre du clavier local **Synchroniser une seule fois lorsque la session est lancée**. Pour plus d'informations, consultez la section [Disposition du clavier](#).

Sur le VDA :

Activez les stratégies VDA suivantes :

- Mappage du clavier Unicode. Pour plus d'informations, consultez la section [Activer le mappage du clavier Unicode](#) ou [Éditeur de méthode de clavier et d'entrée \(IME\)](#).
- Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME. Pour plus d'informations, consultez la section [Éditeur de méthode de clavier et d'entrée \(IME\)](#)

Configuration de l'application Citrix Workspace :

Cette fonctionnalité n'est applicable qu'aux bureaux virtuels. Cette fonction est désactivée par défaut. Pour activer cette fonctionnalité, procédez comme suit :

1. Accédez à la section [Virtual Channels\Keyboard] du fichier **All_Regions.ini**.
2. Ajoutez une clé de registre booléenne `SyncKbdLayoutList to HKEY_CURRENT_USER\SOFTWARE\Citrix\Ica Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard`.
3. Définissez la valeur sur 1.

Configuration du VDA :

La fonctionnalité **Synchroniser plusieurs claviers au début de la session** est activée par défaut sur VDA.

Pour désactiver cette fonctionnalité, mettez à jour le registre VDA comme suit :

1. Ouvrez l'Éditeur du Registre et accédez à `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Créez l'entrée DWORD `DisableKbdLayoutList` et définissez sa valeur sur 0. La définition de la valeur sur 1 désactive la fonction **Synchroniser plusieurs claviers au début de la session**.
3. Redémarrez la session pour que les modifications prennent effet.

Impression

April 22, 2024

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 modifiez les options Compression d'image et Cache d'image et de police.

Commande du clavier à l'écran

Pour permettre 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
- l'appareil est en mode tente ou tablette.

Sur certains appareils et dans certaines circonstances, l'application Citrix Workspace ne peut pas détecter avec précision le mode de l'appareil. Le clavier à l'écran peut également apparaître lorsque vous ne le souhaitez pas.

Pour supprimer l'affichage du clavier à l'écran lors de l'utilisation d'un appareil convertible :

- créez une valeur REG_DWORD DisableKeyboardPopup dans `HKEY\LOCAL_MACHINE\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 suivants 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

Impression PDF

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

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

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

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

Pré-requis :

- 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 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 comprend 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.

USB

April 22, 2024

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. Un tel environnement permet à ces appareils d'interagir avec des packages, 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
- Carte réseau intégrée
- 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 d'applications virtuelles :

- Dongles Bluetooth
- Carte réseau intégrée
- 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 un 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 sélectionner les périphériques USB qui doivent être connectés à distance au bureau virtuel 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.

Classes de périphériques USB autorisées par défaut

Les règles de stratégie USB par défaut autorisent différentes classes de périphériques USB.

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. Ces classes de périphériques USB sont les suivantes.

- **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 les applications virtuelles car ces périphériques ne sont pas disponibles pour l'accès à distance dans les applications virtuelles 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 en tant que périphériques de stockage de masse. Il est également 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 les applications virtuelles car ces périphériques ne sont pas disponibles pour l'accès à distance dans les applications virtuelles 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 qui sont utilisés pour manipuler du matériel vidéo ou lié à la vidéo. Ces périphériques, tels que les webcams, les caméscopes numériques, les convertisseurs vidéo analogique, certains tuner TV et certains appareils photo numériques 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 règles de stratégie USB par défaut n'autorisent pas les différentes classes de périphériques USB suivantes :

- 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). En effet, la majorité des claviers et des souris sont correctement gérés sans prise en charge USB. 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

Modifiez le fichier de modèle Citrix Workspace pour Windows pour mettre à jour la liste des périphériques USB disponibles pour l'envoi vers des bureaux. La mise à jour 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

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.

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.

Redirection de périphérique USB composite

USB 2.1 et versions ultérieures prennent en charge la notion de périphériques USB composites selon laquelle plusieurs périphériques enfants partagent une seule connexion avec le même bus USB. Ces périphériques utilisent un espace de configuration unique et une connexion de bus partagée où un numéro d'interface unique 00-ff est utilisé pour identifier chaque machine enfant. Ces périphériques sont aussi différents du concentrateur USB qui fournit une nouvelle origine de bus USB pour d'autres périphériques USB pris en charge indépendamment pour la connexion.

Les périphériques composites détectés sur le point de terminaison client peuvent être transférés à l'hôte virtuel en tant que :

- un seul périphérique USB composite ou
- un ensemble de périphériques enfants indépendants (périphériques partitionnés)

Lorsqu'un périphérique USB composite est transféré, l'ensemble du périphérique devient indisponible pour le point de terminaison. Le transfert bloque aussi l'utilisation locale du périphérique pour toutes les applications sur le point de terminaison, y compris le client Citrix Workspace requis pour une expérience HDX optimisée à distance.

Envisagez l'utilisation d'un casque USB avec périphérique audio et bouton HID pour le contrôle du son et du volume. Si l'ensemble du périphérique est transféré à l'aide d'un canal USB générique, le périphérique devient indisponible pour la redirection sur le canal audio HDX optimisé. Toutefois, vous pouvez obtenir la meilleure expérience possible lorsque l'audio est envoyé via le canal audio HDX optimisé, contrairement à l'audio envoyé à l'aide de pilotes audio du côté hôte via la communication USB générique à distance. Ce comportement est dû à la nature bruyante des protocoles audio USB.

Vous remarquerez également des problèmes lorsque le clavier système ou le périphérique de pointage fait partie d'un périphérique composite avec d'autres fonctionnalités intégrées requises pour la prise en charge de sessions à distance. Lorsqu'un périphérique composite complet est transféré, le clavier ou la souris du système devient inutilisable sur le point de terminaison, sauf dans l'application ou la session de bureau à distance.

Pour résoudre ces problèmes, Citrix vous recommande de partitionner le périphérique composite et de transférer uniquement les interfaces enfants qui utilisent un canal USB générique. Un tel mécanisme garantit que les autres périphériques enfants peuvent être utilisés par les applications sur le point de terminaison client, y compris l'application Citrix Workspace qui fournit des expériences HDX optimisées, tout en autorisant uniquement les périphériques requis à être transférés et disponibles vers la session à distance.

Règles de périphériques :

Comme pour les périphériques USB standard, les règles de périphériques définies dans la stratégie ou la configuration de l'application Citrix Workspace client sur le point de terminaison sélectionnent les périphériques composites à transférer. L'application Citrix Workspace utilise ces règles pour décider sur quels périphériques USB la redirection vers la session à distance doit être autorisée ou bloquée.

Chaque règle se compose d'un mot clé d'action (Allow, Connect ou Deny), de deux-points (:) et de zéro ou plusieurs paramètres de filtre correspondant aux périphériques réels du sous-système USB des points de terminaison. Ces paramètres de filtre correspondent aux métadonnées du descripteur de périphérique USB utilisées par chaque périphérique USB pour s'identifier.

Chaque règle de périphériques est constituée d'un texte en clair qui s'affiche sur une seule ligne et d'un commentaire facultatif après le caractère #. Les règles sont mises en correspondance de haut en bas (ordre de priorité décroissant). La première règle qui correspond au périphérique ou à l'interface enfant est appliquée. Les règles suivantes qui sélectionnent le même périphérique ou la même interface sont ignorées.

Exemples de règle de périphérique :

- ALLOW: vid=046D pid=0102 # Autoriser un périphérique spécifique par VID/PID
- ALLOW: vid=0505 class=03 subclass=01 # Autoriser n'importe quel PID pour le fournisseur 0505 lorsque subclass=01
- DENY: vid=0850 pid=040C # Refuser un périphérique spécifique (y compris tous les périphériques enfants)
- DENY: class=03 subclass=01 prot=01 # Refuser tout périphérique correspondant à tous les filtres
- CONNECT: vid=0911 pid=0C1C # Autoriser et connecter automatiquement un périphérique spécifique
- ALLOW: vid=0286 pid=0101 split=01 # Diviser ce périphérique et autoriser toutes les interfaces
- ALLOW: vid=1050 pid=0407 split=01 intf=00,01 # Diviser et autoriser seulement 2 interfaces
- CONNECT: vid=1050 pid=0407 split=01 intf=02 # Diviser et connecter automatiquement l'interface 2
- DENY: vid=1050 pid=0407 split=1 intf=03 # Empêcher la communication à distance de l'interface 03

Vous pouvez utiliser l'un des paramètres de filtre suivants pour appliquer des règles aux périphériques rencontrés :

Paramètre de filtre	Description
vid=xxxx	ID de fournisseur du périphérique USB (code hexadécimal à quatre chiffres)
pid=xxxx	ID de produit du périphérique USB (code hexadécimal à quatre chiffres)
rel=xxxx	ID de version du périphérique USB (code hexadécimal à quatre chiffres)
class=xx	Code de classe du périphérique USB (code hexadécimal à deux chiffres)
subclass=xx	Code de sous-classe du périphérique USB (code hexadécimal à deux chiffres)
prot=xx	Code de protocole du périphérique USB (code hexadécimal à deux chiffres)
split=1 (ou split=0)	Permet de sélectionner un périphérique composite à partitionner (ou à ne pas partitionner)
intf=xx[,xx,xx,...]	Permet de sélectionner un ensemble spécifique d'interfaces enfants d'un périphérique composite (liste de codes hexadécimaux à deux chiffres séparée par des virgules)

Les six premiers paramètres permettent de sélectionner les périphériques USB pour lesquels la règle doit être appliquée. Si aucun paramètre n'est spécifié, la règle fait correspondre un périphérique à n'importe quelle valeur pour ce paramètre.

Le forum USB Implementors conserve une liste des valeurs de classe, de sous-classe et de protocole définies sur la page [Defined Class Codes](#). USB-IF conserve également une liste des ID de fournisseur enregistrés. Vous pouvez vérifier le fournisseur, le produit, la version et les ID d'interface d'un périphérique spécifique directement dans le Gestionnaire de périphériques Windows ou à l'aide d'un outil gratuit tel que UsbTreeView.

Lorsqu'ils sont présents, les deux derniers paramètres s'appliquent uniquement aux périphériques composites USB. Le paramètre « split » détermine si un périphérique composite doit être transféré en tant que périphérique partitionné ou en tant que périphérique composite unique.

- *Split=1* indique que les interfaces enfants sélectionnées d'un périphérique composite doivent être transférées en tant que périphériques partitionnés.
- *Split=0* indique que le périphérique composite ne doit pas être partitionné.

Remarque :

Si le paramètre *split* est omis, *Split=0* est la valeur par défaut.

Le paramètre *intf* sélectionne les interfaces enfants spécifiques du périphérique composite auquel l'action doit être appliquée. S'il est omis, l'action s'applique à toutes les interfaces du périphérique composite.

Considérez l'utilisation d'un périphérique casque USB composite avec trois interfaces :

- Interface 0 : points de terminaison de périphérique de classe audio
- Interface 3 : points de terminaison de périphérique de classe HID (bouton de volume et bouton de désactivation du son)
- Interface 5 : interface de gestion/mise à jour

Les règles suggérées pour ce type de périphérique sont les suivantes :

- CONNECT: vid=047F pid=C039 split=1 intf=03 # Autoriser et connecter automatiquement le périphérique HID
- DENY: vid=047F pid=C039 split=1 intf=00 # Refuser les points de terminaison audio
- ALLOW: vid=047F pid=C039 split=1 intf=05 # Autoriser mgmt intf mais ne pas connecter automatiquement

Activer la stratégie Règles de périphériques :

L'application Citrix Workspace pour Windows comprend un ensemble de règles de périphériques par défaut qui filtre certaines classes indésirables et autorise une catégorie que les clients rencontrent souvent.

Vous pouvez vérifier ces règles de périphériques par défaut dans le registre système en accédant à :

- `HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\GenericUSB` (32 bits Windows) ou
- `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Citrix\ICA Client\GenericUSB` (64 bits Windows), dans la valeur de chaînes multiples appelée **DeviceRules**.

Toutefois, dans l'application Citrix Workspace pour Windows, vous pouvez appliquer une stratégie **Règles de périphériques USB** pour remplacer ces règles par défaut.

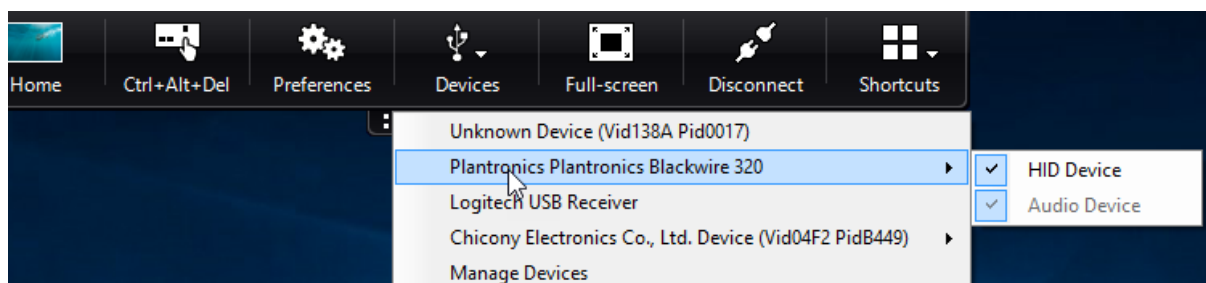
Pour activer la stratégie Règles de périphériques pour l'application Citrix Workspace pour Windows :

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 > 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**, collez (ou modifiez directement) les règles de périphériques USB à déployer.
6. Cliquez sur **Appliquer** et **OK**.

Citrix recommande de conserver les règles par défaut livrées avec le client lors de la création de cette stratégie en copiant les règles d'origine et en insérant de nouvelles règles pour modifier le comportement selon vos besoins

Connexion des périphériques USB :

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**.

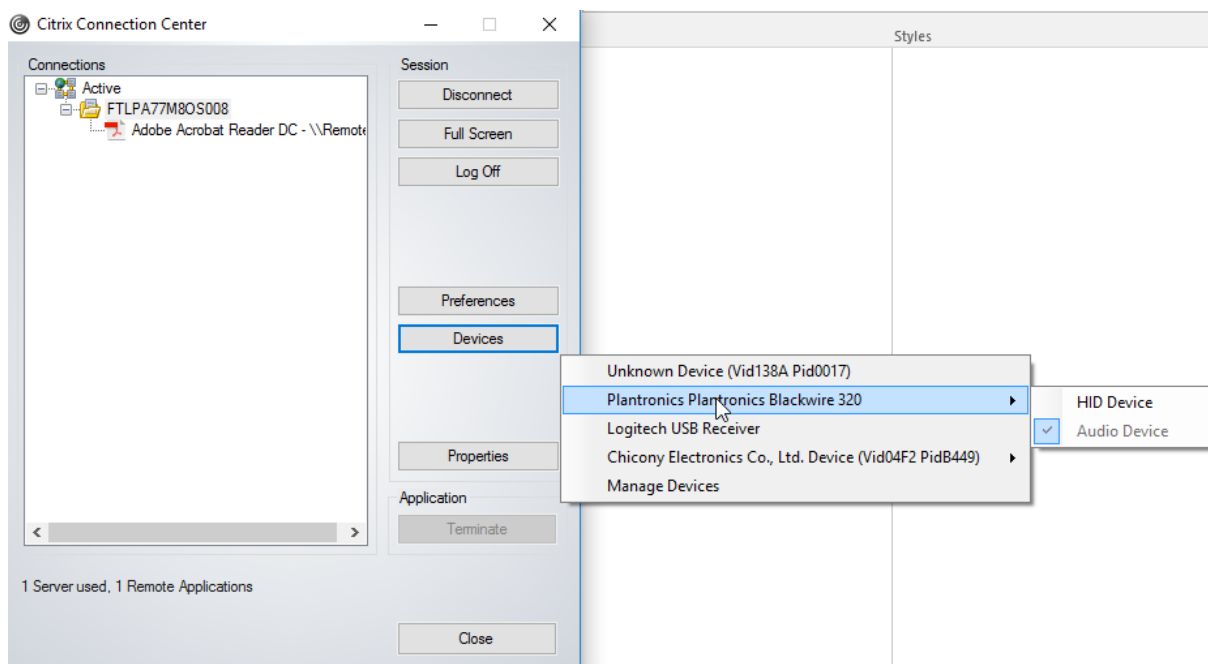


Remarque :

Le mot clé `CONNECT` active la connexion automatique d'un périphérique USB. Toutefois, si le

mot clé CONNECT n'est pas utilisé 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 connecter un périphérique autorisé.

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



Pour connecter automatiquement une interface :

Le mot clé CONNECT introduit dans l'application Citrix Workspace pour Windows 2109 permet la redirection automatique des périphériques USB. La règle CONNECT peut remplacer la règle ALLOW si l'administrateur autorise le périphérique ou les interfaces sélectionnées à se connecter automatiquement dans la session.

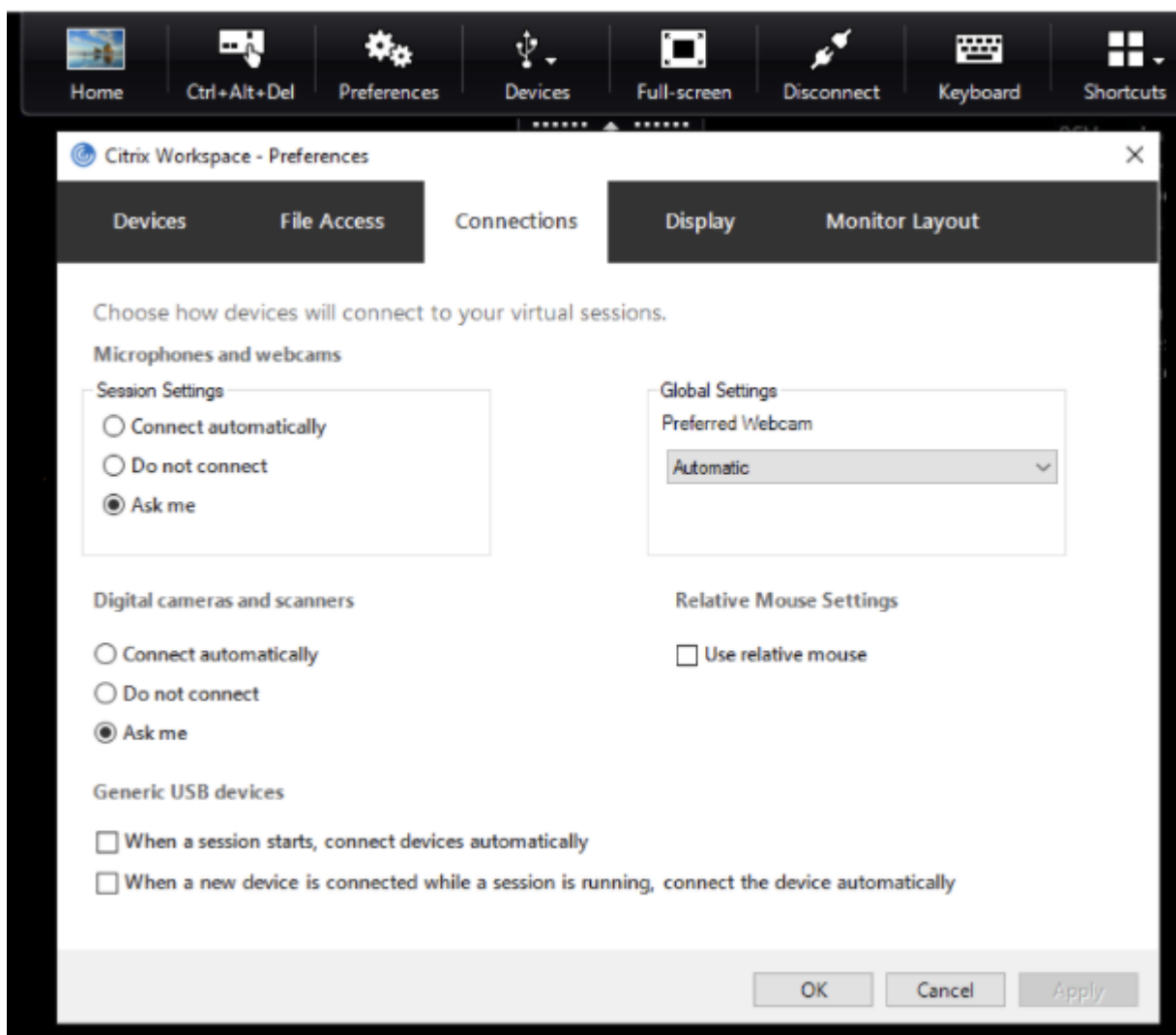
1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant gpedit.msc.
2. Sous le nœud **Configuration utilisateur**, accédez à **Modèles d'administration > Composants Citrix > Citrix Workspace > Accès à distance des périphériques clients > Utilisation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

Par exemple, `CONNECT: vid=047F pid=C039 split=01 intf=00,03` : permet de partitionner un périphérique composite, d'établir la connexion automatique des interfaces 00 et 03, et de restreindre les autres interfaces de ce périphérique.

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

Modification des préférences de connexion automatique du périphérique USB :

L'application Citrix Workspace se connecte automatiquement aux périphériques USB marqués avec une action `CONNECT` en fonction des préférences définies pour la ressource de bureau actuelle. Vous pouvez modifier les préférences dans la barre d'outils de **Desktop Viewer** comme illustré dans l'image suivante.



Les deux cases à cocher en bas du panneau contrôlent si les périphériques doivent se connecter automatiquement ou attendre une connexion manuelle dans la session. Ces paramètres ne sont pas activés par défaut. Vous pouvez modifier les préférences si des périphériques USB génériques doivent être connectés automatiquement.

Un administrateur peut également remplacer les préférences de l'utilisateur en déployant les stratégies correspondantes à partir du modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace. Les stratégies périphérique et utilisateur se trouvent sous **Modèles d'administration > Composants Citrix > Citrix Workspace > Accès à distance des périphériques clients > Utilisation à distance de dispositifs USB génériques**. Les stratégies correspondantes sont nommées Périphériques USB existants et Nouveaux périphériques USB respectivement.

Modifier le paramètre par défaut du périphérique partitionné :

Par défaut, l'application Citrix Workspace pour Windows partitionne uniquement les périphériques composites qui sont explicitement marqués avec *Split=1* dans les règles de périphériques. Toutefois, il est possible de modifier la disposition par défaut pour partitionner tous les périphériques composites qui ne sont pas marqués avec *Split=0* dans une règle de périphérique correspondante.

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant `gpedit.msc`.
2. Sous le nœud **Configuration utilisateur**, accédez à **Modèles d'administration > Composants Citrix > Citrix Workspace > Accès à distance des périphériques clients > Utilisation à distance de dispositifs USB génériques**.
3. Sélectionnez la stratégie **SplitDevices**.
4. Sélectionnez **Activé**.
5. Cliquez sur **Appliquer** et **OK** pour enregistrer la stratégie.

Remarque :

Citrix recommande d'utiliser des règles de périphériques explicites pour identifier des périphériques ou des interfaces spécifiques qui doivent être partitionnés au lieu de modifier la valeur par défaut. Ce paramètre sera obsolète dans une version ultérieure.

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.
- Parfois, les périphériques USB composites peuvent ne pas être automatiquement fractionnés même si une règle de redirection de périphérique correcte est définie pour les fractionner. Le problème se produit car le périphérique est en mode faible consommation. Dans pareils cas, le périphérique enfant qui passe en mode faible consommation peut ne pas figurer dans la liste des périphériques. Pour résoudre ce problème, vous pouvez utiliser l'une des solutions suivantes :
 - Déconnectez la session, insérez le périphérique USB et reconnectez-vous à la session.
 - Débranchez le périphérique USB et rebranchez-le. Cette action fait sortir le périphérique du mode faible consommation. [HDX-34143]

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.

Les claviers Bloomberg offrent d'autres fonctionnalités par rapport aux claviers standard, ce qui permet à l'utilisateur d'accéder aux données du marché financier et d'effectuer des transactions.

Le clavier Bloomberg se compose de plusieurs périphériques USB intégrés à une même coque physique :

- Clavier
- Lecteur d'empreintes digitales
- Périphérique audio
- Concentrateur USB pour connecter tous ces périphériques au système
- Boutons HID, par exemple, Muet, Augmenter le volume et Baisser le volume pour le périphérique audio

Outre les fonctionnalités normales de ces périphériques, le périphérique audio prend en charge certaines touches, le contrôle du clavier et des voyants de clavier.

Pour utiliser la fonctionnalité spécialisée dans une session, vous devez rediriger le périphérique audio en tant que périphérique USB. Cette redirection met le périphérique audio à la disposition de la session, mais empêche le périphérique audio d'être utilisé localement. En outre, les fonctionnalités spécialisées peuvent uniquement être utilisées au cours d'une session et ne peuvent pas être partagées entre plusieurs sessions.

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 5 :

À partir de l'application Citrix Workspace pour Windows version 2109, un nouveau mot clé CONNECT est introduit pour autoriser la connexion automatique des périphériques USB au démarrage de la session et lors de l'insertion de périphériques. Le mot clé CONNECT peut être utilisé pour remplacer le mot clé ALLOW lorsque l'utilisateur souhaite qu'un périphérique USB ou une interface se connecte automatiquement.

Remarque :

Avec l'introduction de la version 2 des règles de redirection de périphériques dans Studio de Citrix Virtual Apps and Desktops, il n'est pas nécessaire de configurer le clavier Bloomberg 5 via des stratégies de groupe côté client dans l'application Citrix Workspace pour Windows. Pour

plus de détails, consultez la section [Règles de redirection de périphérique USB client \(version 2\)](#) dans la documentation de Citrix Virtual Apps and Desktops.

Pour les versions antérieures à la version 2212 de l'application Citrix Workspace pour Windows, l'exemple suivant montre comment utiliser le mot clé CONNECT :

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. Dans la zone de texte **Règles de périphériques USB**, ajoutez les règles suivantes si elles n'existent pas.
 - CONNECT: vid=1188 pid=A101 # Module biométrique Bloomberg 5
 - DENY: vid=1188 pid=A001 split=01 intf=00 # Clavier principal Bloomberg 5
 - CONNECT: vid=1188 pid=A001 split=01 intf=01 # HID du clavier Bloomberg 5
 - DENY: vid=1188 pid=A301 split=01 intf=02 # Canal audio du clavier Bloomberg 5
 - CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # HID du canal audio du clavier Bloomberg 5

Remarque :

Les sauts de lignes ou les points-virgules peuvent être utilisés pour séparer les règles, ce qui permet de lire des valeurs de registre sur une ou plusieurs lignes.

6. Cliquez sur **Appliquer** et **OK** pour enregistrer la stratégie.
7. Dans la fenêtre **Préférences**, sélectionnez l'onglet **Connexions** et sélectionnez automatiquement une ou les deux cases à cocher pour les périphériques connectés. La fenêtre **Préférences** est accessible depuis la barre d'outils du bureau ou le Gestionnaire de connexions.

Une fois cette procédure effectuée, le clavier Bloomberg 5 est prêt à être utilisé. Les règles DENY mentionnées dans les étapes ci-dessus forcent la redirection du clavier principal et du canal audio via le canal optimisé, et non via la redirection USB générique. Les règles CONNECT activent la redirection automatique du module d'empreinte digitale, les touches spéciales sur le clavier et les touches liées au contrôle audio.

Configurer le clavier Bloomberg 4 ou 3 :

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.

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.

La prise en charge du clavier Bloomberg 3 est disponible dans le composant Online Plug-in 11.2 pour Windows et les versions ultérieures.

La prise en charge du clavier Bloomberg 4 est disponible pour Windows Receiver 4.8 et versions ultérieures.

Déterminer si la prise en charge des claviers Bloomberg est activée :

- Pour vérifier si la prise en charge du clavier Bloomberg est activée dans le composant Online Plug-in, vérifiez comment Desktop Viewer signale les périphériques du clavier Bloomberg. Si Desktop Viewer n'est pas utilisé, vous pouvez vérifier le registre sur la machine sur laquelle le composant Online Plug-in est en cours d'exécution.
- Si la prise en charge du clavier Bloomberg est activée, l'application Desktop Viewer affiche :
 - Deux périphériques pour le clavier Bloomberg 3 qui apparaissent en tant que **Bloomberg Fingerprint Scanner** et **Bloomberg Keyboard Audio**.
 - Un périphérique redirigé pour le clavier Bloomberg 4. Ce périphérique apparaît sous le nom de **Bloomberg LP Keyboard 2013**.
- Si la prise en charge des claviers Bloomberg est activée, deux périphériques sont affichés dans l'application Desktop Viewer. L'un apparaît en tant que **Bloomberg Fingerprint Scanner** comme auparavant, et l'autre en tant que **Bloomberg Keyboard Features**.
- Si le pilote du périphérique Bloomberg Fingerprint Scanner n'est pas installé, l'entrée Bloomberg Fingerprint Scanner peut ne pas s'afficher dans Desktop Viewer. Si l'entrée est manquante, le périphérique Bloomberg Fingerprint Scanner peut ne pas être disponible pour la redirection. Vous pouvez toujours vérifier le nom de l'autre périphérique Bloomberg sur lequel la prise en charge des claviers Bloomberg est activée.

- Vous pouvez également vérifier la valeur dans le registre pour savoir si la prise en charge est activée :

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB\EnableBloombergHID`

Si la valeur n'existe pas ou est égale à 0 (zéro), la prise en charge des claviers Bloomberg n'est pas activée. Si la valeur est égale à 1, la prise en charge est activée.

Activer la prise en charge du clavier Bloomberg :

Remarque :

Citrix Receiver pour Windows 4.8 a introduit la prise en charge des périphériques composites via la stratégie **SplitDevices**. Toutefois, vous devez utiliser la fonction du clavier Bloomberg au lieu de cette stratégie pour le clavier Bloomberg 4.

La prise en charge du clavier Bloomberg modifie la manière dont certains périphériques USB sont redirigés vers une session. Cette prise en charge n'est pas activée par défaut.

- Pour activer la prise en charge pendant l'installation, spécifiez la valeur de la propriété **ENABLE_HID_REDIRECTION** sur TRUE sur la ligne de commande d'installation. Par exemple :

```
CitrixOnlinePluginFull.exe /silent
ADDLOCAL="ICA_CLIENT,PN_AGENT,SSON,USB"
ENABLE_SSON="no"INSTALLDIR="c:\test"
ENABLE_DYNAMIC_CLIENT_NAME="Yes"
DEFAULT_NDSCONTEXT="Context1,Context2"
SERVER_LOCATION="http://testserver.net"ENABLE_HID_REDIRECTION="
TRUE"
```

- Pour activer la prise en charge après l'installation du composant Online Plug-in, modifiez le registre Windows sur le système sur lequel Online Plug-in est en cours d'exécution :

1. Ouvrez l'Éditeur du Registre.
2. Accédez à la clé suivante :

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`

3. Si la valeur **EnableBloombergHID** existe, définissez les données de valeur sur 1.
4. Si la valeur **EnableBloombergHID** n'existe pas, créez une valeur DWORD avec le nom `EnableBloombergHID` et définissez les données de valeur sur 1.

Désactiver la prise en charge du clavier Bloomberg :

Vous pouvez désactiver la prise en charge du clavier Bloomberg dans le composant Online Plug-in comme suit :

1. Ouvrez l'Éditeur du Registre sur le système exécutant le logiciel Online Plug-in.

2. Accédez à la clé suivante :

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`

3. Si la valeur **EnableBloombergHID** existe, définissez les données de valeur sur 0 (zéro).

Si la valeur **EnableBloombergHID** n'existe pas, cela indique que la prise en charge du clavier Bloomberg n'est pas activée. Dans ce cas, vous n'avez pas besoin de modifier les valeurs de registre.

Utiliser les claviers Bloomberg sans activer la prise en charge :

- Vous pouvez utiliser le clavier sans activer la prise en charge du clavier Bloomberg dans le composant Online Plug-in. Toutefois, vous ne pouvez pas bénéficier du partage des fonctionnalités spécialisées entre plusieurs sessions et vous pouvez rencontrer une bande passante réseau accrue provenant de l'audio.
- Les touches normales du clavier Bloomberg sont disponibles de la même manière que tout autre clavier. Vous n'avez aucune action spéciale à effectuer.
- Pour utiliser les touches Bloomberg spécialisées, vous devez rediriger le périphérique audio du clavier Bloomberg dans la session. Si vous utilisez l'application Desktop Viewer, le nom du fabricant et le nom des périphériques USB s'affichent et **Bloomberg Keyboard Audio** s'affiche pour le périphérique audio du clavier Bloomberg.
- Pour utiliser le lecteur d'empreintes digitales, vous devez rediriger le périphérique vers Bloomberg Fingerprint Scanner. Si les pilotes du lecteur d'empreintes digitales ne sont pas installés localement, le périphérique est uniquement affiché :
 - si le composant Online Plug-in est défini pour connecter les périphériques automatiquement ou
 - pour permettre à l'utilisateur de choisir de connecter les périphériques.

En outre, si le clavier Bloomberg est connecté avant d'établir la session et que les pilotes du lecteur d'empreintes digitales n'existent pas localement, le lecteur d'empreintes digitales n'apparaît pas et ne peut pas être utilisé dans la session.

Remarque :

Pour Bloomberg 3, le lecteur d'empreintes digitales peut être utilisé soit dans une session unique, soit par le système local, mais ne peut pas être partagé. La redirection est interdite avec Bloomberg 4.

Utiliser les claviers Bloomberg après l'activation de la prise en charge :

- Si vous activez la prise en charge des claviers Bloomberg dans le composant Online Plug-in, vous bénéficiez du partage de la fonctionnalité de clavier spécialisé entre plusieurs sessions. Vous bénéficiez également d'une bande passante réseau inférieure provenant de l'audio.

- L'activation de la prise en charge du clavier Bloomberg empêche la redirection du périphérique audio du clavier Bloomberg. Au lieu de cela, un nouveau périphérique est disponible. Si vous utilisez l'application Desktop Viewer, ce périphérique est appelé Bloomberg Keyboard Features. La redirection de ce périphérique fournit les clés Bloomberg spécialisées à la session.

L'activation de la prise en charge du clavier Bloomberg n'affecte que les touches Bloomberg spécialisées et le périphérique audio. En effet, les touches ordinaires et le lecteur d'empreintes digitales sont utilisés de la même manière que lorsque la prise en charge n'est pas activée.

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 vers le serveur. L'appareil multimédia comprend les appareils photo, les scanners, les lecteurs multimédia et les terminaux de point de vente. 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 ou notifier 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 est le numéro du port COM sur le serveur (les ports 1 à 9 sont disponibles pour le mappage) et
- z est le numéro du port COM client que vous voulez mapper

4. Pour confirmer l'opération, entrez la commande suivante :

```
net use
```

L'invite affiche les lecteurs mappés, les ports LPT et les 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.

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](#). Lorsque vous procédez à la 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** et **OK**.
5. Ouvrez l'invite de commande en mode administrateur.
6. Exécutez la commande suivante
`gpupdate /force`.

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. Vous pouvez le configurer via la stratégie de l'application Citrix Workspace pour Windows **Accès à distance des appareils clients > Mappage des lecteurs clients**. Lorsque vous appliquez cette stratégie, les lecteurs de la machine utilisateur sont automatiquement mappés vers les lettres de lecteur sur le bureau virtuel lorsque les utilisateurs ouvrent une session. Les lecteurs sont affichés sous la forme de dossiers partagés associés à des lettres de lecteur mappé.

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

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

Si vous activez les stratégies USB générique et Mappage des lecteurs clients et insérez un périphérique de stockage de masse 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.

Mappage des lecteurs clients

April 22, 2024

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

Cette fonctionnalité est activée par défaut.

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

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

Nom : `DisableFullStreamWrite`

Type : REG_DWORD

Valeur :

`0x01` - désactive,

`0` ou supprime - active

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.

Désactiver les mappages de 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.

Dans l'exemple suivant, 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.

Microphone

April 22, 2024

L'application Citrix Workspace prend en charge plusieurs entrées microphone côté client. Vous pouvez utiliser des microphones installés localement 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 l'observateur Citrix Virtual Apps and Desktops et Citrix DaaS pour désactiver leurs micros et webcams.

Stratégie de groupe

April 22, 2024

Modèle d'administration d'objet de stratégie de groupe

Nous vous recommandons d'utiliser le modèle d'administration d'objet de stratégie de groupe pour configurer des règles pour :

- Routage réseau
- Serveurs proxy
- Configuration de serveur de confiance
- Routage utilisateur
- Machines utilisateur distantes
- Expérience 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. L'importation est utile pour appliquer les paramètres de l'application Citrix Workspace à différentes machines utilisateur réparties dans l'entreprise. Pour appliquer les modifications sur 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.

Le répertoire d'installation inclut `CitrixBase.admx` et `CitrixBase.adml`, ainsi que les fichiers de modèles d'administration (`receiver.adml` ou `receiver.admx`'`receiver.adml`').

Remarque :

Les fichiers `.admx` et `.adml` sont destinés à être utilisés avec la version de Windows mentionnée dans le [tableau de compatibilité](#).

Si l'application Citrix Workspace a été installée avec le VDA, les fichiers ADMX/ADML se trouvent généralement dans le répertoire `\<installation directory>\Online Plugin\Configuration`.

Si l'application Citrix Workspace a été installée sans le VDA, les fichiers ADMX/ADML se trouvent généralement dans le répertoire suivant.

- Pour 64 bits : `C:\Program Files (x86)\Citrix\ICA Client\Configuration directory`
- Pour 32 bits : `C:\Program Files\Citrix\ICA Client\Configuration directory`

Reportez-vous au tableau suivant 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
<code>receiver.adm</code>	<code>\ICA Client\Configuration</code>
<code>receiver.admx</code>	<code>\ICA Client\Configuration</code>
<code>receiver.adml</code>	<code>\ICA Client\Configuration\[MUIculture]</code>
<code>CitrixBase.admx</code>	<code>\ICA Client\Configuration</code>
<code>CitrixBase.adml</code>	<code>\ICA Client\Configuration\[MUIculture]</code>

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. Les paramètres antérieurs sont conservés après l'importation. Pour plus d'informations, consultez la procédure suivante :

Pour ajouter des fichiers de modèle receiver.admx/adml à l'objet de stratégie de groupe local :

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

Après avoir installé l'application Citrix Workspace, copiez les fichiers modèles suivants :

Type de fichier	Copier à partir de	Copier sur
receiver.admx	Installation Directory\ICA Client\ Configuration\ receiver.admx	%systemroot%\ policyDefinitions
CitrixBase.admx	Installation Directory\ICA Client\ Configuration\ CitrixBase.admx	%systemroot%\ policyDefinitions
receiver.adml	Installation Directory\ICA Client\ Configuration\ [MUICulture]receiver. adml	%systemroot%\ policyDefinitions\ [MUICulture]
CitrixBase.adml	Installation Directory\ICA Client\ Configuration\ [MUICulture] CitrixBase.adml	%systemroot%\ policyDefinitions\ [MUICulture]

Remarque :

Ajoutez CitrixBase.admx/CitrixBase.adml au dossier `\PolicyDefinitions` pour afficher les fichiers de modèle dans **Modèles d'administration > Composants Citrix > Citrix Workspace**.

Expérience de session

April 22, 2024

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 fonction de pré-lancement permet de créer une session de pré-lancement. La session de pré-lancement est créée lorsqu'un utilisateur ouvre une session sur l'application Citrix Workspace, ou à une heure planifiée si l'utilisateur s'est connecté.

La 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.

Pour plus d'informations, consultez les instructions de pré-lancement de session et de persistance de session dans l'article de Citrix Virtual Apps and Desktops [Gérer les groupes de mise à disposition](#).

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 partager 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 pour les périodes de trafic élevé.

La configuration du pré-lancement sur un serveur Citrix Virtual Apps comprend les étapes suivantes :

- la création, la modification ou la suppression d'applications de pré-lancement, et
- la mise à jour des 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. Les valeurs de registre peuvent être modifiées 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 les valeurs.

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**

Type : REG_DWORD

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 REG_DWORD

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**

Type : REG_DWORD

Valeur :

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

HH: MM	M:T:W:TH:F:S:SU où HH et MM correspondent aux heures et minutes. M:T:W:TH:F:S:SU correspondent aux jours de la semaine. Par exemple, pour activer le pré-lancement planifié le lundi, mercredi et vendredi à 13:45, définissez Schedule de la sorte : Schedule=13:45	1:0:1:0:1:0:0. La session démarre en fait entre 13h15 et 13h45.
--------	---	---

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.

Desktop Viewer

Différentes entreprises peuvent avoir différents besoins. La configuration requise pour la manière dont les utilisateurs accèdent aux bureaux virtuels peut varier d'un utilisateur à un autre et à mesure que vos besoins évoluent. 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 configuration de 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 sur 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 certaines fonctionnalités d'accessibilité Microsoft, telles que les touches rémanentes, les touches filtres et les touches bascules 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. Les séquences de raccourcis sont par exemple la séquence Ctrl+F1 qui reproduit Ctrl+Alt+Suppr, et Maj+F2 qui permet de basculer les applications du mode plein écran au mode fenêtre, et vice versa.

Remarque :

Vous ne pouvez pas utiliser de séquences de raccourcis clavier avec des bureaux virtuels affichés dans Desktop Viewer, c'est-à-dire avec des sessions d'applications et de bureaux virtuels. Toutefois, vous pouvez les utiliser avec des applications publiées, c'est-à-dire avec des sessions d'applications virtuelles.

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 le délai d'expiration, procédez comme suit :

1. Lancez l'Éditeur du Registre.
2. Accédez au chemin d'accès suivant :
 - Sur un système 64 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\Engine`
 - Sur un système 32 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\`
3. Créez une clé de Registre comme suit :
 - Type : REG_DWORD
 - Nom : `SI_INACTIVE_MS`
 - Valeur : 4, si vous voulez que l'indicateur d'état disparaisse plus tôt.

Lorsque vous configurez cette clé, l'indicateur d'état peut apparaître et disparaître fréquemment. Ce comportement est normal. Pour supprimer l'indicateur d'état, procédez comme suit :

1. Lancez l'Éditeur du Registre.
2. Accédez au chemin d'accès suivant :
 - Sur un système 64 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\`
 - Sur un système 32 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\`
3. Créez une clé de Registre comme suit :
 - Type : REG_DWORD
 - Nom : `NotificationDelay`
 - Valeur : toute valeur en milliseconde (par exemple, 120000)

Amélioration de l'expérience de reconnexion d'applications et de bureaux virtuels

La version 2302 de Citrix Workspace offre une expérience utilisateur améliorée lors de la reconnexion aux applications et aux bureaux virtuels dont vous étiez déconnecté.

Lorsque l'application Citrix Workspace tente d'actualiser l'application Citrix Workspace déconnectée ou de démarrer de nouvelles applications ou nouveaux bureaux virtuels dans le cadre de la fonctionnalité Contrôle de l'espace de travail, l'invite suivante s'affiche :

Restore session?

You have one or more apps/desktops running from the previous session in Citrix Workspace app. Would you like to restore them?

Remember my preference



Cette invite s'affiche uniquement lorsque l'option **show reconnection prompt to reconnect sessions** est définie sur true dans Global App Configuration Service.

Cliquez sur **Restaurer** pour vous reconnecter afin d'ouvrir des applications et des bureaux virtuels nouveaux et déconnectés. Si vous souhaitez démarrer uniquement les applications et les bureaux récemment sélectionnés, cliquez sur **Annuler**.

Vous pouvez également sélectionner **Mémoriser ma préférence** pour appliquer la préférence sélectionnée lors de la prochaine connexion.

La nouvelle invite **Restaurer la session ?** apparaît uniquement si :

- l'utilisateur essaie de démarrer une application appartenant à un magasin d'espace de travail,
- les stratégies administratives ou les paramètres de configuration de l'application ne sont pas configurés pour la fonctionnalité Contrôle de l'espace de travail,
- les options de reconnexion de Contrôle de l'espace de travail sont définies par défaut sur le client.

Remarque :

Les paramètres de reconnexion dans les **options de reconnexion** ont priorité sur les préférences définies dans la boîte de dialogue. Pour plus d'informations, voir [Configurer les options de reconnexion à l'aide de la boîte de dialogue Préférences avancées](#).

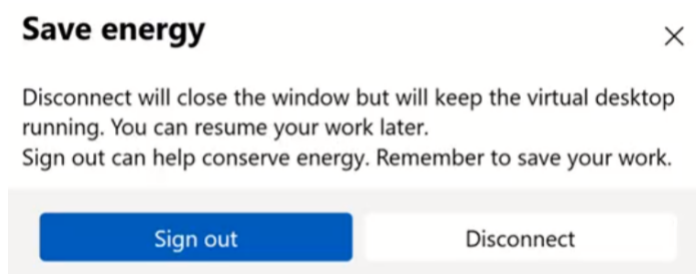
Initiative de développement durable pour l'application Citrix Workspace

Pour un lancement natif

Lorsque cette fonctionnalité est activée et qu'un utilisateur ferme un bureau virtuel, une invite s'affiche pour se déconnecter de la session de bureau. Cette fonctionnalité permet d'économiser de l'énergie si des stratégies du système d'exploitation Windows sont utilisées pour arrêter les machines virtuelles lorsqu'aucun utilisateur n'est connecté.

Pour activer cette fonctionnalité, procédez comme suit :

1. Accédez à Citrix Studio.
2. Cliquez sur **Groupes de mise à disposition** dans le volet de navigation de gauche.
3. Sélectionnez le VDA requis dans la section **Groupe de mise à disposition**.
4. Cliquez sur l'icône **Modifier**. La page **Modifier le groupe de mise à disposition** s'affiche.
5. Cliquez sur **Bureaux** dans le volet de navigation de gauche.
6. Sélectionnez le VDA requis auquel vous devez ajouter les mots clés.
7. Cliquez sur **Modifier**. La page **Modifier le bureau** s'affiche.
8. Définissez le mot clé `LogoffOnClose` sur **true** dans le champ **Description**.
9. Cliquez sur **OK**. La boîte de dialogue suivante s'affiche lorsque vous fermez le bureau virtuel :



Personnalisation du texte dans l'écran Économiser l'énergie Vous pouvez également personnaliser le texte dans l'écran **Économiser l'énergie**.

1. Suivez les étapes 1 à 8 de la section précédente.
2. Définissez le mot clé `PromptMessage` avec le texte requis dans le champ **Description**.

Exemple :

```
1 KEYWORDS:LogoffOnClose=true PromptMessage="Do you want to Log off?"  
2 <!--NeedCopy-->
```

Edit Desktop

Display name:

TSVDA-2019

Description:

KEYWORDS:LogoffOnClose=true PromptMessage="Do you want to Log off?"

The name and description are shown in Citrix Workspace app.

Restrict launches to machines with tag:

Select...

Allow everyone with access to this delivery group to use a desktop

Restrict desktop use:

Allow list ?

You have not yet added any users or groups.

Add

Enable desktop

Clear this check box to disable delivery of this desktop.

Session roaming

When enabled, if the user launches this desktop and then moves to another device, the same session is used, and applications are available on both devices. When disabled, the session no longer roams between devices.

OK

Cancel

Les mots clés sont attribués par défaut aux nouveaux ordinateurs de bureau affectés au groupe. Pour les ordinateurs de bureau existants, exécutez les commandes PowerShell suivantes pour appliquer les modifications :

```
1 $dg = Get-BrokerDesktopGroup -Name '<group name>' -Property 'Name', 'Uid'
2
3 $apr = @( Get-BrokerAssignmentPolicyRule -DesktopGroupUid $dg.Uid
4           -Property 'Description' )
5 Get-BrokerMachine -DesktopGroupUid $dg.Uid -IsAssigned $true | Set
6   -BrokerMachine -Description $apr[0].Description
7 <!--NeedCopy-->
```


Avec ce script PowerShell, il est possible d'avoir plusieurs règles de stratégie d'attribution pour un seul groupe de mise à disposition. Avec Citrix Studio, vous pouvez également configurer plusieurs règles de stratégie d'attribution, chacune avec une valeur de description unique et un éventuel ensemble de mots clés différents.

3. Cliquez sur **OK**. La boîte de dialogue suivante s'affiche lorsque vous fermez le bureau virtuel.

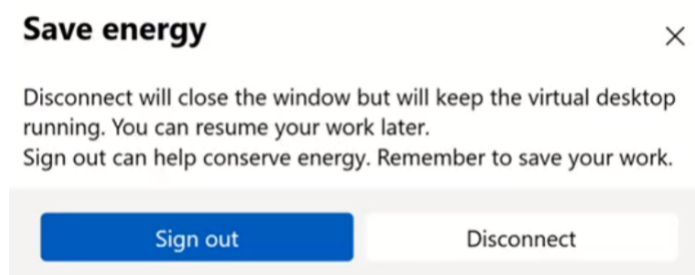


Pour un lancement hybride sur le cloud

À partir de la version 2402 de l'application Citrix Workspace, cette fonctionnalité est disponible pour les lancements hybrides sur le cloud. Une fois que cette fonctionnalité est activée et qu'un utilisateur ferme un bureau virtuel, une invite s'affiche pour se déconnecter de la session de bureau. Cette fonctionnalité permet d'économiser de l'énergie si des stratégies du système d'exploitation Windows sont utilisées pour arrêter les machines virtuelles lorsqu'aucun utilisateur n'est connecté.

Pour activer cette fonctionnalité, procédez comme suit :

1. Accédez à Citrix Studio.
2. Cliquez sur **Groupes de mise à disposition** dans le volet de navigation de gauche.
3. Sélectionnez le VDA requis dans la section **Groupe de mise à disposition**.
4. Cliquez sur l'icône **Modifier**. La page **Modifier le groupe de mise à disposition** s'affiche.
5. Cliquez sur **Bureaux** dans le volet de navigation de gauche.
6. Sélectionnez le VDA requis auquel vous devez ajouter les mots clés.
7. Cliquez sur **Modifier**. La page **Modifier le bureau** s'affiche.
8. Définissez le mot clé `ICA-LogOffOnClose` sur **true** dans le champ **Description**.
9. Cliquez sur **OK**. La boîte de dialogue suivante s'affiche lorsque vous fermez le bureau virtuel :



Personnalisation du texte dans l'écran Économiser l'énergie

Vous pouvez également personnaliser le texte dans l'écran **Économiser l'énergie**.

1. Suivez les étapes 1 à 8 de la section précédente.
2. Définissez le mot clé `ICA-PromptMessage` avec le texte requis dans le champ **Description**.

Remarque :

Le nombre maximum de caractères autorisés dans le champ Description est de 200.

Exemple :

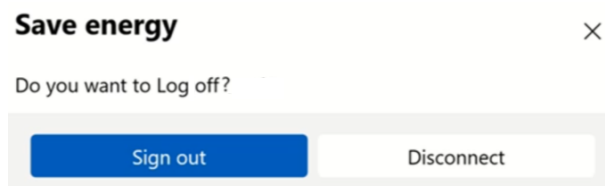
```
1 KEYWORDS:ICA-LogOffOnClose=true ="Do you want to Log off?"
2 <!--NeedCopy-->
```

Les mots clés sont attribués par défaut aux nouveaux ordinateurs de bureau affectés au groupe. Pour les ordinateurs de bureau existants, exécutez les commandes PowerShell suivantes pour appliquer les modifications :

```
1 $dgc = Get-BrokerDesktopGroup -Name '<group name>' -Property 'Name'
   , 'Uid'
2
3 $apr = @( Get-BrokerAssignmentPolicyRule -DesktopGroupUid $dgc.Uid
   -Property 'Description' )
4
5 Get-BrokerMachine -DesktopGroupUid $dgc.Uid -IsAssigned $true | Set
   -BrokerMachine -Description $apr[0].Description
6 <!--NeedCopy-->
```

Avec ce script PowerShell, il est possible d'avoir plusieurs règles de stratégie d'attribution pour un seul groupe de mise à disposition. Avec Citrix Studio, vous pouvez également configurer plusieurs règles de stratégie d'attribution, chacune avec une valeur de description unique et un éventuel ensemble de mots clés différents.

3. Cliquez sur **OK**. La boîte de dialogue suivante s'affiche lorsque vous fermez le bureau virtuel.



Citrix Workspace Desktop Lock

April 22, 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. Elle 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.

Remarque :

Lorsque vous utilisez l'application Citrix Workspace pour Windows avec Desktop Lock, un utilisateur est connecté au premier bureau dans l'ordre alphabétique des noms de tous les bureaux disponibles pour l'utilisateur. À l'heure actuelle, il n'existe aucune option permettant de choisir de manière sélective le bureau auquel l'utilisateur doit se connecter. De plus, cette fonctionnalité ne prend en charge que les ordinateurs de bureau et ne prend pas en charge les applications.

Installez l'application Citrix Workspace pour Windows avec l'indicateur `/includeSSON`. Configurez le magasin et le Single Sign-On, au choix avec le fichier adm/admx ou l'option de ligne de commande. Pour de plus amples informations, consultez la section [Installer](#).

Installez ensuite Citrix Workspace Desktop Lock en tant qu'administrateur à l'aide du fichier `CitrixWorkspaceDesktopLock.msi` disponible sur la page des [téléchargements de Citrix](#).

Configuration système requise

- Microsoft Visual C++ 2005 avec Service Pack 1 Redistributable Package Pour plus d'informations, consultez la page de [téléchargement de Microsoft](#).
- Pris en charge sous Windows 10 (Anniversary Update incluse) et Windows 11.
- Se connecte à StoreFront via des protocoles natifs uniquement.
- Points de terminaison appartenant à des domaines.
- Les machines utilisateur doivent être connectées à un réseau local (LAN) ou 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.
- Un profil utilisateur local est créé sur le terminal lorsque l'utilisateur se connecte au système. Le profil est conservé sur le terminal même lorsque l'utilisateur se déconnecte et en fonction des configurations de gestion des profils.

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 partir d'une invite de commande, exécutez la commande suivante :

Par exemple :

```
1 CitrixWorkspaceApp.exe
2 /includeSSON
3 STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/
  discovery;on;Desktop Store"
4 <!--NeedCopy-->
```

La commande est disponible dans l'application Citrix Workspace et dans le dossier **Plug-ins > Windows > Application Citrix Workspace** sur le support d'installation. Pour plus d'informations sur les commandes, consultez la documentation d'installation de l'application Citrix Workspace de la section [Installer](#).

3. Dans le même dossier du support d'installation, cliquez deux fois sur `CitrixWorkspaceDesktopLock.msi`. L'assistant Desktop Lock apparaît. Suivez les invites.
4. Une fois l'installation terminée, redémarrez la machine utilisateur. Si vous avez l'autorisation d'accéder à un bureau et que vous ouvrez une session en tant qu'utilisateur de domaine, la machine s'affiche à l'aide de Citrix Workspace Desktop Lock.

Pour vous permettre d'administrer la machine utilisateur après l'installation, le compte utilisé pour installer `CitrixWorkspaceDesktopLock.msi` est exclu du shell de remplacement. Si ce compte est supprimé ultérieurement, vous ne pourrez pas ouvrir de session pour administrer la machine.

Pour exécuter une **installation silencieuse** de Citrix Workspace Desktop Lock, utilisez la ligne de commande suivante :

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

Configurer l'application Citrix Workspace pour Desktop Lock

Lorsque vous vous êtes connecté en tant que non-administrateur, Desktop Lock lance automatiquement une session de bureau attribué.

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'administra-**

tion classiques (ADM) > Composants Citrix). Les fichiers .admx se trouvent dans %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 contrôle le périphérique USB et l'affiche dans l'interface utilisateur.
 - Activez la règle de stratégie USB.
 - Dans **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 **Application Citrix Workspace > Accès à distance des périphériques clients**, activez et configurez la stratégie de mappage du lecteur client.
- Microphone : dans **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. Ajoutez l'URL au format bureau ://delivery-group-name.
 - 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. Desktop Lock garantit que la machine utilisateur n'est pas laissée 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 comme suit :

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+Supprimer : 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 (Software Development Kit) et API

April 22, 2024

SDK de déclaration d'identité du certificat

Le SDK de déclaration d'identité de certificat permet aux développeurs de créer un plug-in. Le plug-in 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.

La dernière version de la [déclaration d'identité de certificat pour Citrix Workspace pour Windows](#) est la version **2212**.

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 (VD-API) est utilisée avec les fonctions de canal virtuel dans le SDK de l'API Citrix Server (WF-API SDK) pour créer de nouveaux canaux virtuels. La prise en charge de canal virtuel fournie par VD-API 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 WF-API pour écrire sur le côté serveur du canal virtuel.

La dernière version du [SDK du canal virtuel pour Windows](#) est la version **2302**.

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 à la fonctionnalité Single Sign-On (SSO). 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 pour connecter les utilisateurs à des applications ou bureaux virtuels, puis les déconnecter de ces sessions.

La dernière version de l'[API Fast Connect pour Citrix Workspace pour Windows](#) est la version **2212**.

Pour plus d'informations, veuillez consulter la page [Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows](#).

Scripts pour le déploiement de Citrix Workspace pour Windows

Il s'agit d'exemples de scripts permettant de déployer et de configurer l'application Citrix Workspace.

La dernière version des [Scripts de déploiement de Citrix Workspace pour Windows](#) est la version **2212**.

Storebrowse

April 22, 2024

Remarque :

Cet article s'applique uniquement aux déploiements locaux de Citrix Workspace. Pour les déploiements dans le cloud, consultez la documentation de [Storebrowse pour Workspace](#).

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

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

- Ajouter un magasin.
- Répertorier les applications et les bureaux publiés à partir d'un magasin configuré.
- Générer manuellement un fichier ICA en sélectionnant un bureau virtuel ou une application virtuelle 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](#). Une fois l'installation de l'application Citrix Workspace terminée, l'utilitaire **Storebrowse** se trouve dans le dossier d'installation de [AuthManager](#).

Pour confirmer que l'utilitaire **Storebrowse** est installé avec le composant **Authmanager**, vérifiez le chemin d'accès du Registre suivant :

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\Inst
Sur une machine 64 bits	[HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\A

Exigences

- Application Citrix Workspace version 1808 pour Windows ou version ultérieure
- Minimum de 530 Mo d'espace disque libre.
- 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 Server 2022

Windows Server 2016

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 :

Sur un magasin HTTP, l'utilitaire **Storebrowse** n'accepte pas les informations d'identification à l'aide de la ligne de commande.

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** : entrez les informations d'identification pour l'authentification aux magasins. L'authentification explicite est activée par défaut lorsque vous créez votre premier magasin.
- **Authentification pass-through au domaine** : une l'authentification aux ordinateurs appartenant au domaine effectuée, vous êtes automatiquement connectés aux magasins. Pour utiliser cette option, activez l'authentification pass-through lors de l'installation de l'application Citrix Workspace. Pour plus d'informations sur le pass-through au domaine, consultez [Configuration de l'authentification pass-through](#).
- **HTTP de base** : cette méthode est utilisée par les intégrations de clients tiers et les portails Web, où une interface utilisateur externe a été utilisée pour capturer un nom d'utilisateur et un mot de passe de domaine qualifié. StoreFront utilise la fonctionnalité d'authentification de base d'IIS pour transférer les informations d'identification au serveur StoreFront. StoreFront utilise ensuite soit les [services de domaine](#), soit l'[authentification du service XML Broker](#) pour valider les informations d'identification et obtenir les informations de groupe. Pour plus d'informations sur l'activation de l'authentification HTTP de base, consultez [HTTP de base](#) dans la documentation sur la [gestion des méthodes d'authentification](#).

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 : activez la méthode d'authentification HTTP basique sur StoreFront lorsque vous utilisez l'util-

itaire **Storebrowse**. Cette méthode s'applique lorsque l'utilisateur fournit les informations d'identification à l'aide des commandes **Storebrowse**.

- Utilisez le [Authmanager](#) qui est inclus dans l'application Citrix Workspace pour Windows. Vous pouvez utiliser cette méthode lorsque vous utilisez l'authentification pass-through au domaine. Pour plus d'informations, consultez la documentation [Authentification pass-through au domaine](#).

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.

Remarque :

Vous ne pouvez pas ouvrir d'applications SaaS ou de [contenu publié](#) à l'aide des commandes Storebrowse.

Utilisation des commandes

La section suivante fournit des informations détaillées sur les commandes que vous pouvez utiliser depuis l'utilitaire **Storebrowse**.

Ajouter un magasin

`-a, --addstore`

Description :

Ajoute un nouveau magasin. Renvoie l'URL complète du magasin. Si le renvoi échoue, une erreur est signalée.

Remarque :

La configuration multi-magasins est prise en charge sur 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>
```

Aide

/?

Description :

Fournit des détails sur l'utilisation de l'utilitaire **Storebrowse**.

Répertoire des magasins

(-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
```

Énumération

(-M 0x2000 -E)

Description :

Énumère les ressources.

Exemple de commande sur StoreFront :

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Exemple de commande sur Citrix Gateway :

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E <https://my.secondexample.net>
```

Quick launch

```
-q, --quicklaunch
```

Description :

Génère le fichier ICA 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. L'URL de lancement 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 typique se présente comme suit :

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/Stress/resources/v2/Q29udHJvbGxlcisi5DYWxjdWxhdG9y/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/Q2hJk0lmNoPQrSTV9y/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.secondexamplestore.com>
```

Lancement

```
-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. Le nom peut

être le serveur StoreFront ou l'URL de Citrix Gateway. Le fichier ICA est généré dans le répertoire %LocalAppData%\Citrix\Storebrowse\cache.

Exécutez la commande suivante pour obtenir le nom d'affichage des applications et des bureaux publiés :

```
.\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/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

Le nom en gras dans la sortie précédente 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>
```

Lancement de session

-S, --sessionlaunch

Description :

Avec cette commande, vous pouvez ajouter un magasin, vérifier et lancer les ressources publiées. Cette option accepte les paramètres suivants :

- Nom d'utilisateur
- Mot de passe
- Domaine
- Nom de la ressource à lancer
- URL du magasin

Toutefois, si l'utilisateur ne fournit pas les informations d'identification, [AuthManager](#) invite l'utilisateur à entrer les informations d'identification, puis la ressource est lancée.

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/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

Le nom en gras dans la sortie précédente 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>
```

Dossier de fichiers

-f, --filefolder

Description :

Génère le fichier ICA dans le chemin d'accès personnalisé pour une application et des bureaux publiés.

L'option launch nécessite un nom de dossier et le nom de la ressource comme entrée avec l'URL du magasin. L'URL du magasin 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 }
```

Authentification des traces

-t, --traceauthentication

Description :

Génère des journaux pour le composant **AuthManager**. 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 doit 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 }
```

Supprimer un magasin

`-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.secondexamplestore.com
```

Suivi de l'état de la commande Storebrowse

Vous pouvez suivre l'état d'exécution d'une commande Storebrowse dans un fichier. Pour suivre l'état de réussite, saisissez un nom de fichier unique avec la commande `-f launch`. Cette commande génère un fichier portant le nom que vous avez indiqué. L'état d'échec est présent dans le fichier `ica.error` qui est créé automatiquement.

Remarque :

Assurez-vous d'ajouter une extension `.ica` au nom du fichier à l'aide de la commande `-f`

launch. Dans le cas contraire, le fichier n'est pas généré.

Les fichiers permettant de suivre à la fois les réussites et les échecs sont disponibles dans %LOCALAPPDATA%\citrix\selfservice\cache ; vous pouvez ainsi les surveiller selon vos besoins.

Cette amélioration est activée par défaut.

Voici un exemple d'utilisation de la commande de lancement avec l'option -f :

```
1 -launch -f <uniqueFileName.ica> "launchcommandline"  
2 For example:  
3 SelfService.exe storebrowse -launch -f uniqueFileName.ica -s store0-5  
   c3ec017 -CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-  
   e33d0695df39.Notepad -ica "https://cwawiniwstest.cloudburrito.com/  
   Citrix/Store/resources/v2/  
   YTLh0GUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkJm5Lk5vdGVwYWQ-/launch/  
   ica" -cmdline  
4  
5 <!--NeedCopy-->
```

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 (anciennement Citrix Virtual Apps and Desktops Service) fourni par le domaine. Vous pouvez vous connecter sans procéder à une nouvelle authentification pour chaque application ou bureau. Lorsque vous ajoutez un magasin, vos informations d'identification sont transmises au serveur Citrix Gateway, ainsi que les instances Citrix Virtual Apps and Desktops et Citrix DaaS et les paramètres du menu Démarrer.

Cette fonctionnalité est prise en charge sur Citrix Gateway version 11 et ultérieure.

Pré-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.

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.

Limitations :

- Activez la méthode d'**authentification HTTP de base** 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 vérifier ou lancer les applications et les bureaux virtuels publiés, l'injection des informations d'identification à l'aide de l'option de ligne de commande n'est pas prise en charge. Pour résoudre ce problème, utilisez le module externe **AuthManager** si 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.

Pour activer la fonctionnalité SSON pour les applications tierces qui utilisent ICOSDK, créez le registre suivant :

- Clé de registre : `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Valeur du registre : chemin complet des applications tierces
- Type de registre : `reg_multi_sz`

Exemple :

- Clé de registre : `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Valeur de registre : `C:\temp1\abc.exe;C:\temp2\xyz.exe`
- Type de registre : `reg_multi_sz`

Remarque :

- Vous pouvez fournir plusieurs applications tierces séparées par des points-virgules.
- Cette fonctionnalité est prise en charge à partir de la version 2107.

Storebrowse pour Workspace

April 23, 2024

L'application Citrix Workspace pour Windows prend en charge **Storebrowse** lors du déploiement en libre-service et sur site de l'application Citrix Workspace. Cela permet également aux utilisateurs de **Storebrowse** d'accéder aux fonctionnalités de Cloud et Workspace.

Remarque :

- Cet article s'applique uniquement aux déploiements cloud de Citrix Workspace. Pour les déploiements locaux, consultez la documentation de [Storebrowse](#).
- Cette fonctionnalité prend en charge **Storebrowse** uniquement avec l'authentification unique.
- Les prérequis mentionnés dans [Configuration système requise et compatibilité](#) doivent être disponibles pour utiliser cette fonctionnalité.
- Vous ne pouvez pas ouvrir d'applications SaaS ou de [contenu publié](#) à l'aide des commandes Storebrowse.

Utilisation des commandes

La section suivante fournit des informations détaillées sur les commandes que vous pouvez utiliser depuis l'utilitaire **Storebrowse**.

Remarque :

- Cette fonctionnalité prend également en charge d'autres commandes du Self-Service Plug-in, comme indiqué dans l'article [CTX200337](#).
- Vous pouvez exécuter les commandes suivantes dans l'invite de commandes.
 - -a "[discoveryurl](#)" : ajoute un magasin via la ligne de commande. Cette commande n'affiche pas l'invite d'authentification lorsque l'authentification unique (SSO) est activée. Par exemple, des domaines AAD joignent des appareils sur lesquels l'authentification s'effectue via WebView. Sur les autres appareils, l'invite d'authentification s'affiche.
 - Exemple : `SelfService.exe storebrowse -a "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`
 - -d "[discoveryurl](#)" : supprime le magasin.
 - Exemple : `SelfService.exe storebrowse -d "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`

- `-e "discoveryurl"` : exporte les détails de la ressource au format JSON. Cette commande stocke le fichier `resource.json` dans l'emplacement par défaut `%LOCALAPPDATA%\citrix\selfservice`. L'application Citrix Workspace doit être active pour exécuter cette commande et l'utilisateur doit être connecté.

- Exemple : `SelfService.exe storebrowse -e "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`

Vous pouvez également spécifier votre propre chemin si vous ne souhaitez pas stocker le fichier `resource.json` dans l'emplacement par défaut.

- Exemple : `.\SelfService.exe storebrowse -e "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"C:\Users\. Cela stocke le fichier resource.json dans le fichier C:\Users\.`

- `-q "FriendlyName" "discoveryurl"` : utilisez cette commande pour lancer rapidement la ressource spécifiée.

- Exemple : `SelfService.exe storebrowse -q "Excel 2016" "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`

- `-launch "launchcommandline"` : lancement de ressources à l'aide de « `launchcommandline` » depuis `resource.json`.

Remarque :

- Copiez « `launchcommandline` » depuis le fichier `resource.json`.
 - Supprimez / de « `launchcommandline` » spécifié dans le fichier `resource.json` avant d'exécuter la commande.

- Exemple : `SelfService.exe storebrowse -launch -s store0-5c3ec017-CitrixID store0-5c3ec017@a9a8e3ac-099d-4577-b84e-e33d0695df39 .Notepad -ica "https://cwawiniwstest.cloudburrito.com/Citrix/Store/resources/v2/YTlh0GUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkJm5Lk5-/launch/ica"-cmdline`

Après avoir exécuté `-launch "launchcommandline"`, le fichier `ica` sera stocké dans le répertoire `%LOCALAPPDATA%\citrix\selfservice\cache`. Double-cliquez sur le fichier `ica` pour lancer la ressource.

- `-liststore` : répertorie les magasins qui sont ajoutés dans le Self-Service Plug-in (SSP). La liste des magasins doit inclure l'ID de magasin et l'URL de détection pour chaque magasin.

- Exemple : `SelfService.exe storebrowse -liststore`

Remarque :

L'application Citrix Workspace doit être active pour exécuter la commande `-liststore`.

La commande `Selfservice.exe storebrowse -liststore` stocke le fichier `store-details.json` dans `AppData\Local\Citrix\SelfService`.

Dépannage

April 22, 2024

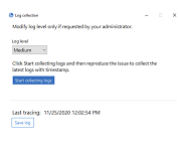
Collecte de journaux

La collecte des journaux simplifie le processus de collecte des journaux pour l'application Citrix Workspace. Les journaux aident Citrix à résoudre les problèmes et, en cas de problèmes complexes, facilitent le support. Cette fonctionnalité est disponible dans l'application Citrix Workspace pour Windows versions 2012 et ultérieures.

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

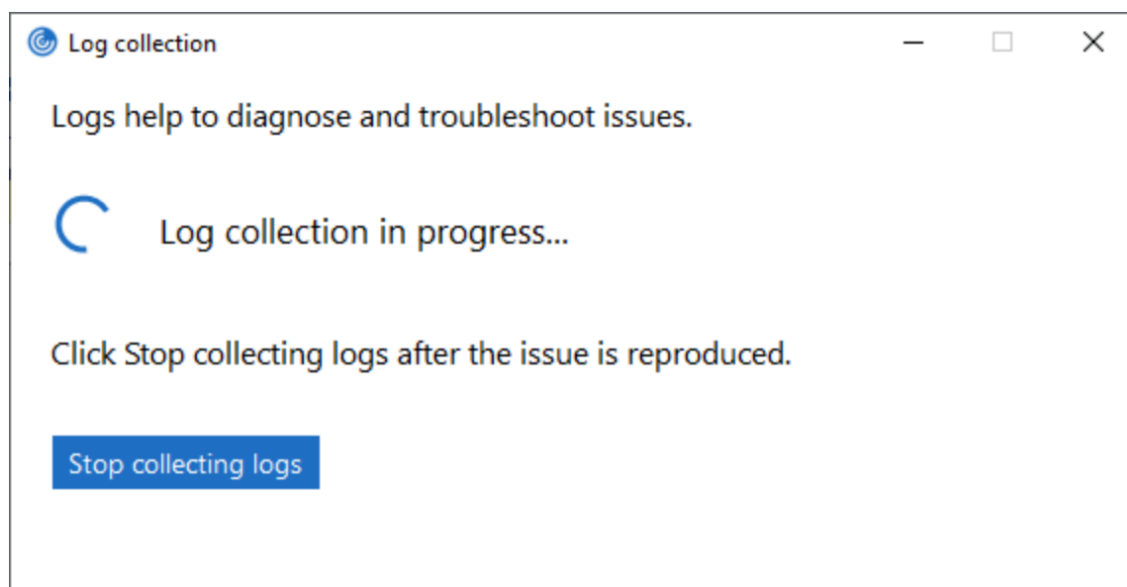
Collecte de journaux :

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 **Collecte de journaux**.
La boîte de dialogue de collecte de journaux s'affiche.



3. Sélectionnez l'un des niveaux de journalisation suivants :
 - Faible
 - Moyen
 - Verbose
4. Cliquez sur **Démarrer la collecte des journaux** pour reproduire le problème et collecter les derniers journaux.

Le processus de collecte des journaux démarre.



5. Cliquez sur **Arrêter la collecte des journaux** une fois le problème reproduit.
6. Cliquez sur **Enregistrer le journal** pour enregistrer les journaux dans l'emplacement souhaité.

Données collectées par le biais de journaux

Matériel

- Informations sur les moniteurs connectés
- Informations sur la mémoire
- Cartes réseau
- Processeur
- Informations de diagnostic DirectX

Logiciel

- Version de l'application Citrix Workspace
- Informations sur le système d'exploitation (version, Service Pack et architecture)
- Version d'Internet Explorer
- Navigateur par défaut
- Version d'ActiveX Flash
- Version Flash NPAPI

Registre

- HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager
- HKEY_LOCAL_MACHINE\Software\Citrix\CitrixCAB

- HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
- HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client
- HKEY_LOCAL_MACHINE\Software\Citrix\Install
- HKEY_LOCAL_MACHINE\Software\Citrix\InstallDetect
- HKEY_LOCAL_MACHINE\Software\Citrix\PluginPackages
- HKEY_LOCAL_MACHINE\Software\Citrix\Receiver
- HKEY_LOCAL_MACHINE\Software\Citrix\ReceiverInside
- HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop
- HKEY_LOCAL_MACHINE\Software\Policies\Citrix
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider\Order
- HKEY_CURRENT_USER\Software\Citrix\AuthManager
- HKEY_CURRENT_USER\Software\Citrix\CitrixCAB
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\ICA Client
- HKEY_CURRENT_USER\Software\Citrix\Install
- HKEY_CURRENT_USER\Software\Citrix\InstallDetect
- HKEY_CURRENT_USER\Software\Citrix\PluginPackages
- HKEY_CURRENT_USER\Software\Citrix\Receiver
- HKEY_CURRENT_USER\Software\Citrix\ReceiverInside
- HKEY_CURRENT_USER\Software\Citrix\XenDesktop
- HKEY_CURRENT_USER\Software\Policies\Citrix
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\VisualEffects
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains

Journaux d'événements

- Journaux d'événements des applications
- Journal d'événements système

Traçage

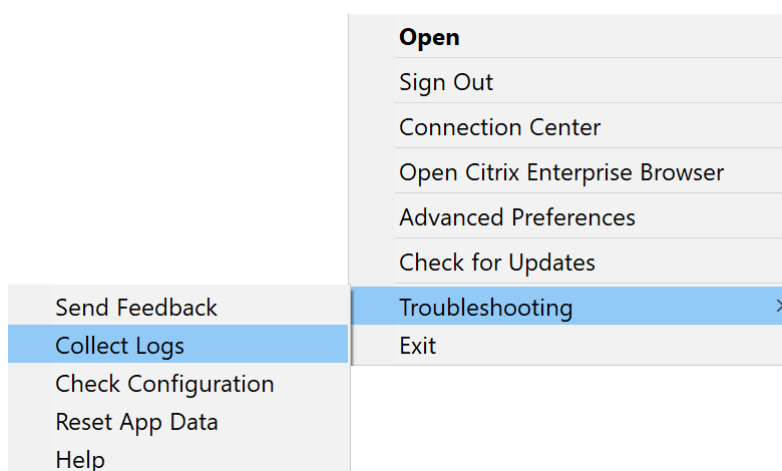
- HDX
- Shell, Auth Manager et Self Service Plug-in pour Receiver
- Journaux d'installation
- Journaux permanents

Ajout de l'option **Dépannage** dans la barre d'état système de l'application Citrix Workspace

L'option **Dépannage** a été ajoutée pour améliorer l'expérience utilisateur et faciliter le dépannage. Vous pouvez cliquer avec le bouton droit sur l'icône de l'application Citrix Workspace dans la barre d'état système située dans le coin inférieur droit de votre écran, puis sélectionner **Dépannage** pour y accéder.

Les options disponibles dans la section Dépannage sont les suivantes :

- Envoyer des commentaires
- Collecter les journaux
- Vérifier la configuration
- Réinitialiser les données d'application
- Aide

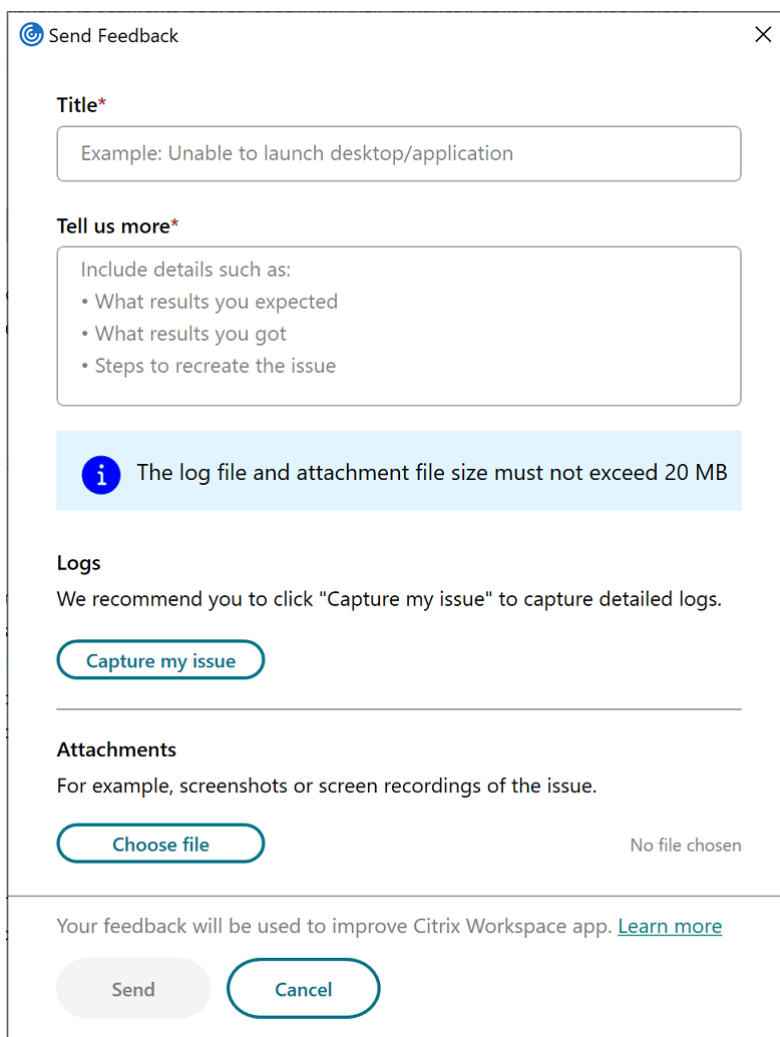


Envoi de commentaires sur l'application Citrix Workspace

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

Vous pouvez envoyer des commentaires en suivant les étapes suivantes :

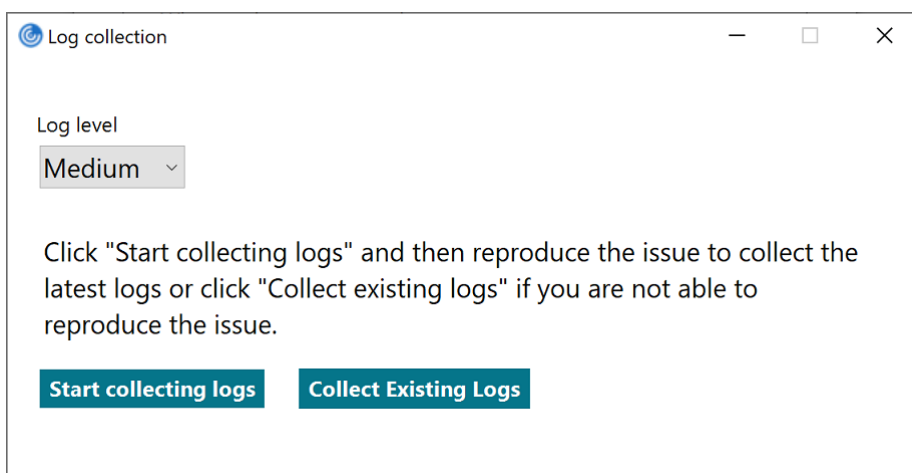
1. Cliquez avec le bouton droit sur l'icône de l'application Citrix Workspace dans la zone de notification et sélectionnez **Dépannage > Envoyer des commentaires**. L'écran **Envoyer des commentaires** s'affiche.



The image shows a 'Send Feedback' dialog box with the following sections:

- Title***: A text input field containing the example text 'Example: Unable to launch desktop/application'.
- Tell us more***: A text area containing the instruction 'Include details such as:' followed by a bulleted list: 'What results you expected', 'What results you got', and 'Steps to recreate the issue'.
- Information banner**: A light blue banner with an information icon and the text 'The log file and attachment file size must not exceed 20 MB'.
- Logs**: A section with the text 'We recommend you to click "Capture my issue" to capture detailed logs.' and a 'Capture my issue' button.
- Attachments**: A section with the text 'For example, screenshots or screen recordings of the issue.' and a 'Choose file' button. To the right of the button, it says 'No file chosen'.
- Footer**: A line of text stating 'Your feedback will be used to improve Citrix Workspace app. [Learn more](#)'.
- Buttons**: 'Send' and 'Cancel' buttons at the bottom.

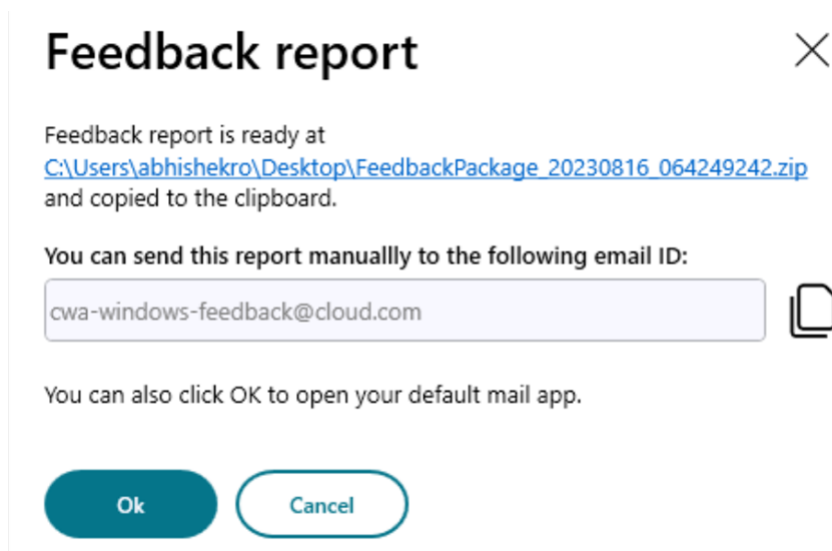
2. Sous **Titre**, spécifiez le type de problème.
3. Ajoutez les détails du problème dans le champ **Dites-nous en plus**.
4. Cliquez sur **Capturer mon problème**. L'écran **Collecte de journaux** s'affiche.



The image shows a 'Log collection' dialog box with the following elements:

- Log level**: A dropdown menu currently set to 'Medium'.
- Instructions**: Text stating 'Click "Start collecting logs" and then reproduce the issue to collect the latest logs or click "Collect existing logs" if you are not able to reproduce the issue.'
- Buttons**: Two buttons at the bottom: 'Start collecting logs' and 'Collect Existing Logs'.

- a) Cliquez sur **Démarrer la collecte des journaux** pour reproduire le problème et collecter les derniers journaux.
 - b) Cliquez sur **Arrêter la collecte des journaux** une fois le problème reproduit.
Ou
Cliquez sur **Collecter les journaux existants** si vous ne parvenez pas à reproduire le problème.
 - c) Cliquez sur **Arrêter la collecte des journaux** une fois le problème reproduit.
5. Assurez-vous que les fichiers journaux sont affichés à côté de **Capturer mon problème**.
 6. Cliquez sur **Choisir un fichier** et ajoutez les pièces jointes décrivant vos problèmes, telles que des captures d'écran ou des enregistrements d'écran. La taille de fichier maximale autorisée pour toutes les pièces jointes, y compris le fichier journal, est de 20 Mo.
 7. Cliquez sur **Envoyer**. L'écran **Rapport de commentaires** s'affiche.



Le fichier .zip contient les fichiers journaux, la description du problème sous forme de fichiers de test et les pièces jointes.

8. Vous pouvez envoyer le rapport de commentaires à Citrix à l'aide des options suivantes :
 - Cliquez sur **OK** pour utiliser l'application de messagerie par défaut de votre système.

Ou

- Envoyez le rapport manuellement à l'adresse e-mail fournie.

Remarque :

Assurez-vous que le fichier .zip est joint à l'e-mail.

Fin de prise en charge

April 22, 2024

Les annonces de cet article visent à vous avertir à l'avance des plates-formes, des produits Citrix et des fonctionnalités qui vont disparaître. Grâce à ces annonces, vous pouvez prendre les décisions appropriées en temps opportun.

Citrix surveille l'utilisation des clients et leurs commentaires pour déterminer quand les retirer. Les annonces peuvent être modifiées dans les versions ultérieures et peuvent ne pas contenir chaque fonctionnalité amenée à disparaître.

Les éléments obsolètes ne sont pas retirés immédiatement. Citrix continue de les prendre en charge dans cette version, mais ils seront retirés à l'avenir.

Tableau de fin de prise en charge

Élément	Abandon annoncé	Supprimé dans	Solution alternative
Redirection du contenu du navigateur basée sur Internet Explorer	2311.1	2311.1	Redirection du contenu du navigateur basée sur Google Chrome
Prise en charge du format WebRTC SDP (Plan B)	2309		Mettez à niveau l'application Citrix Workspace vers une version prise en charge.
Prise en charge du mode fenêtre unique dans Optimisation Microsoft Teams	2309		Mettez à niveau l'application Citrix Workspace vers une version prenant en charge le mode multi-fenêtres. Pour plus d'informations, consultez Tableau des fonctionnalités et versions prises en charge .

Élément	Abandon annoncé	Supprimé dans	Solution alternative
Commutateur / includeappprotection	2212	2212	Utiliser / startappprotection pour démarrer le composant Protection des applications
Prise en charge des URL personnalisées grâce aux redirections 301	2210		Migration de l'URL de StoreFront vers Workspace
Prise en charge de Windows 8.1 et Windows Server 2012 R2	2204.1	2204.1	Utilisez le système d'exploitation pris en charge comme indiqué dans la section Configuration système requise .
Citrix Casting est installé par défaut avec l'application Citrix Workspace.	2112.1	2205	Citrix Casting peut être installé à la demande avec l'application Citrix Workspace. Remarque : Citrix Casting n'est pas installé par défaut avec l'application Citrix Workspace.
L'option Tous les comptes du menu pour les magasins Workspace (cloud) uniquement.	2112.1	2202	
L'option Mémoriser le mot de passe de l'écran d'ouverture de session dans les magasins (cloud) de l'application Workspace.	2008	2008	

Élément	Abandon annoncé	Supprimé dans	Solution alternative
Citrix Receiver pour la plateforme Windows universelle (UWP)	2006	2102	
L'option permettant d'ajouter ou de supprimer les descriptions de magasins dans la boîte de dialogue Ajouter ou supprimer des comptes . La colonne Description n'est plus disponible.	2006.1		Vous pouvez ajouter ou supprimer les détails du compte de magasin sans y ajouter de description.
L'option permettant d'activer ou de désactiver les magasins dans la boîte de dialogue Ajouter ou supprimer des comptes	2006.1		
Prise en charge pour Windows 7	2002	2006.1	Utilisez le système d'exploitation pris en charge comme indiqué dans la section Configuration système requise . REMARQUE : Windows 7 est pris en charge dans la version 2002.
Commutateur d'installation <code>/rcu</code>	1909		Utilisez le commutateur <code>/forceinstall</code> au lieu de <code>/rcu</code> .

Élément	Abandon annoncé	Supprimé dans	Solution alternative
Installation à la demande de Citrix Casting avec l'application Citrix Workspace	2112.1	2402	Utiliser une ancienne version de l'application Citrix Workspace



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).