Application Citrix Workspace pour ChromeOS

Contents

Application Citrix Workspace pour ChromeOS

June 18, 2024

L'application Citrix Workspace pour ChromeOS est une application packagée Chrome native qui vous permet d'accéder aux applications et aux bureaux virtuels hébergés par Citrix sur Workspace à partir d'appareils Chrome. Elle est disponible sur le Chrome Web Store.

Pour obtenir des informations détaillées concernant les fonctionnalités, les problèmes résolus et les problèmes connus, consultez la page À propos de cette version.

Une fois l'application Citrix Workspace pour ChromeOS installée, vous pouvez accéder aux postes de travail et aux applications depuis vos navigateurs Web. Aucune configuration ou option de déploiement supplémentaire n'est requise sur StoreFront.

Pour plus d'informations sur les fonctionnalités disponibles dans l'application Citrix Workspace pour ChromeOS, consultez le Tableau des fonctionnalités de l'application Citrix Workspace.

Pour plus d'informations sur les éléments obsolètes, consultez la page Fin de prise en charge.

Langues prises en charge

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

Compatibilité avec ChromeOS LTS

Google offre une version LTS (Support à long terme) de ChromeOS si vous préférez moins de mises à jour. À tout moment, une ou plusieurs versions de l'application Citrix Workspace sont compatibles avec la dernière version de ChromeOS LTS.

Si vous recherchez une version de l'application Citrix Workspace dotée des dernières corrections de bogues et des nouvelles fonctionnalités, nous vous recommandons :

- Utiliser la dernière version de l'application Citrix Workspace
- Utiliser la dernière version de Google ChromeOS sur le canal stable.

Pour plus d'informations sur la rétrocompatibilité, les exclusions et les questions courantes, consultez la section Compatibilité avec ChromeOS LTS sur la page d'installation.

Articles de référence

- Global App Configuration Service
- Optimisation pour Microsoft Teams
- Optimisation de Microsoft Teams dans les environnements Citrix Virtual Apps and Desktops
- Fiche technique : Authentification unique pour Workspace
- Document technique : guide de démarrage rapide de l'application Citrix Workspace
- Fiche technique : Citrix Workspace
- Documentation destinée aux développeurs - Application Citrix Workspace pour Chrome HDX SDK
- Documentation destinée aux développeurs - Citrix Virtual Channel SDK
- Calendrier de publication de l'application Citrix Workspace

Nouveautés dans les produits associés

- Citrix DaaS
- Citrix Workspace
- StoreFront
- Application Citrix Workspace pour Windows
- Application Citrix Workspace pour HTML5
- Interface utilisateur de Workspace

Ancienne documentation

Pour les versions de produits qui ont atteint leur fin de vie, consultez la section Ancienne documentation.

À propos de cette version

June 19, 2024

Découvrez les nouvelles fonctionnalités, les améliorations, les problèmes résolus et les problèmes connus.

> **Remarque :**
>
> Vous recherchez des fonctionnalités en version Technical Preview ? Nous avons rassemblé ces fonctionnalités dans une liste afin que vous puissiez les trouver en un seul endroit. Découvrez notre page Fonctionnalités de la version Technical Preview et partagez vos commentaires en util-

> isant le lien vers le formulaire Podio ci-joint.

Nouveautés de la version 2405

Cette version est compatible avec ChromeOS version 125. Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Technical Preview

- Barre d'outils dans la session améliorée.

Pour obtenir la liste complète des fonctionnalités Technical Preview, consultez la page Fonctionnalités de la version Technical Preview.

Problèmes résolus dans la version 2405

- Dans une configuration multi-écrans, lorsque vous ouvrez une application publiée, un écran vide apparaît à la place de l'écran de l'application. Le problème se produit lorsque vous utilisez le mode H.264 en plein écran. Pour en savoir plus, consultez Limitations. [CVADHELP-24883]
- Sur les appareils non gérés, lorsque vous démarrez une application ou une session de bureau, le nom du client envoyé depuis l'application Citrix Workspace pour ChromeOS est HTML5-X-X. Après le correctif, le nom du client apparaît désormais sous la forme CrOS-X-X. [RFHTMCRM-12155]
- Lorsque vous activez la fonctionnalité de continuité du service et que vous démarrez une session hors ligne, le téléchargement des fichiers de location échoue par intermittence, une fois que vous vous déconnectez de Citrix Workspace et que vous vous reconnectez. [RFHTMCRM-12492]
- Lorsque vous démarrez une session de bureau et que vous ouvrez une application pour saisir du texte, le texte entré disparaît, puis réapparaît. Vous pouvez remarquer que le texte scintille. Le problème se produit lorsque vous utilisez le mode H.264 en plein écran. Pour en savoir plus, consultez Limitations. [CVADHELP-24883]

Problèmes connus dans la version 2405

Il n'y a aucun nouveau problème connu.

> **Remarque :**
>
> - Pour obtenir la liste complète des problèmes des versions précédentes, consultez la section Problèmes connus.

Versions précédentes

Cette section fournit des informations sur les nouvelles fonctionnalités et les problèmes résolus dans les versions précédentes que nous prenons en charge conformément aux étapes du cycle de vie de l'application Citrix Workspace.

2402.1

Nouveautés

Cette version est compatible avec ChromeOS version 121. Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Prise en charge de l'optimisation de Zoom À partir de la version 2402.1, l'application Citrix Workspace pour ChromeOS prend en charge l'intégration à la solution d'infrastructure de bureau virtuel (VDI, Virtual Desktop Infrastructure) Zoom pour une expérience de conférence audio et vidéo optimisée dans les sessions .

Après avoir résolu les dépendances tierces liées à cette fonctionnalité, celle-ci peut désormais être configurée et utilisée immédiatement. Les utilisateurs peuvent profiter d'un son et d'une vidéo optimisés, et constater une diminution de la consommation des ressources VDA lors des réunions Zoom dans la session Citrix.

Pour plus d'informations sur cette fonctionnalité, consultez la section Prise en charge de l'optimisation de Zoom.

Continuité du service À partir de la version 2402.1, la fonctionnalité de continuité de service est désactivée.

> **Remarque :**
>
> Si vous avez précédemment activé la fonctionnalité de continuité de service et que vous utilisez une ancienne version de l'application Citrix Workspace pour ChromeOS, il est possible que vous ne puissiez pas utiliser la fonctionnalité de continuité de service. Pour activer cette fonctionnalité, il est recommandé de mettre à jour l'application Citrix Workspace vers la dernière version, 2402.1 ou ultérieure, et de suivre les instructions de l'article CTX632723 du Centre de connais-

> sances.
>
> Pour plus d'informations sur la configuration, consultez la documentation Continuité du service.

Outil Configuration Utility Cette version aborde les domaines qui améliorent la stabilité globale de l'outil Configuration Utility. Le paramètre de configuration **allowEditStoreName** est inclus dans l'outil.

Comment accéder à l'outil Auparavant, l'outil Configuration Utility était disponible sur la page Centre de connaissances.

À partir de la version 2402, vous pouvez télécharger l'outil Configuration Utility depuis la page Téléchargements de Citrix.

SDK du canal virtuel À compter de la version 2402, le SDK du canal virtuel Citrix (VCSDK) pour ChromeOS possède des capacités et des fonctionnalités qui facilitent la compatibilité de l'application Citrix Workspace pour ChromeOS avec les plug-ins tiers. Les plug-ins tiers doivent être intégrés au VCSDK. Cette gestion des fonctionnalités garantit une compatibilité ascendante et descendante fluide entre toutes les versions et combinaisons. Pour plus d'informations sur ces fonctionnalités, consultez la page de documentation destinée aux développeurs.

De plus, des API permettant de prendre en charge les scénarios multi-écrans ont été ajoutées.

Paramètre de proxy HTTP sur Chromebook Si vous avez configuré le paramètre de proxy HTTP sur votre Chromebook, il est possible que vos sessions ne démarrent pas.

Pour plus d'informations sur la résolution de ce problème, consultez l'article Paramètre de proxy HTTP sur Chromebook.

Nom abrégé de l'URL du magasin Auparavant, vous pouviez voir les URL des magasins, mais aucune disposition ne permettait d'ajouter ou de modifier un nom abrégé pour les URL des magasins. Cette disposition a rendu difficile pour les administrateurs et les utilisateurs de se souvenir des URL des magasins.

À partir de la version 2402, pour les utilisateurs gérés, les administrateurs peuvent envoyer un nom de magasin personnalisé ainsi que l'URL du magasin depuis la console d'administration Google. Cette fonctionnalité permet aux utilisateurs d'identifier plus facilement les différents magasins.

Pour plus d'informations sur cette fonctionnalité, consultez Nom abrégé de l'URL du magasin.

Problèmes résolus

- Si vous disposez de bureaux virtuels dont le nom de groupe de mise à disposition contient des caractères multioctets, vous ne pouvez pas démarrer de session de bureau virtuel. [CVADHELP-24846]
- Si vous participez à un appel Microsoft Teams optimisé et que vous décidez de ne plus partager votre écran, il est possible que vous observiez un rectangle vide à la place de la section vidéo. [RFHTMCRM-11689]
- En mode kiosque, les sessions peuvent ne pas démarrer automatiquement même lorsque le paramètre de **lancement automatique du bureau** est activé dans StoreFront. [CVADHELP-23698] [RFHTMCRM-11815]
- Lorsque vous activez la fonctionnalité de continuité de service et que vous cliquez sur **Reconnecter à Workspace**, la bannière **Utiliser l'espace de travail hors ligne** ne s'affiche pas sur l'écran de connexion. [RFHTMCRM-11720]
- L'icône de l'application Citrix Workspace apparaît sur l'étagère Chrome à la place des icônes de la session de bureau proprement dite. Le problème se produit lorsque vous activez la fonctionnalité de continuité de service et que le déploiement dans le cloud est interrompu. [RFHTMCRM-11647]
- Lorsque vous copiez et collez des fichiers de plus de 4 Ko à l'aide de la fonctionnalité de mappage des lecteurs clients depuis votre appareil local vers le VDA, les données peuvent être corrompues. [RFHTMCRM-12156]
- Au cours d'une session, les clics de souris peuvent ne plus répondre. [RFHTMCRM-11841] [CVADHELP-24210]
- Lorsqu'un utilisateur se déconnecte de la page d'un magasin (intentionnellement ou suite à une inactivité) et se reconnecte à la même page de magasin, la page du magasin peut être vide ou un compteur infini peut apparaître. Le problème se produit sur les déploiements cloud activés pour la continuité de service. [RFHTMCRM -12212]

2312

Nouveautés

Cette version est compatible avec ChromeOS version 119. Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Prise en charge de la sonnerie secondaire Vous pouvez utiliser la fonction de sonnerie secondaire pour sélectionner un appareil secondaire sur lequel vous souhaitez recevoir la notification d'appel

entrant dans une version de Microsoft Teams optimisée.

Par exemple, imaginez que vous avez défini un haut-parleur comme sonnerie secondaire et que votre point de terminaison est connecté à un casque. Dans ce cas, Microsoft Teams envoie la sonnerie d'appel entrant au casque et au haut-parleur. Vous ne pouvez pas définir de sonnerie secondaire dans les cas suivants :

- Lorsque vous n'êtes pas connecté à plusieurs périphériques audio
- Lorsque le périphérique n'est pas disponible (par exemple, un casque Bluetooth)

> **Remarque**
>
> Cette fonctionnalité est désactivée par défaut.

Limites connues de cette fonctionnalité

- Lorsque vous activez cette fonctionnalité, vous pouvez entendre la sonnerie secondaire deux fois avec un léger décalage. Ce problème est un bogue dans Microsoft Teams qui devrait être corrigé dans la prochaine version de Microsoft Teams.

Pour plus d'informations sur la configuration, consultez Prise en charge de la sonnerie secondaire.

Implémentation de la diffusion simultanée pour des visioconférences dans Microsoft Teams optimisé À compter de la version 2312, la prise en charge de la diffusion simultanée est activée par défaut pour des visioconférences dans Microsoft Teams optimisé. Avec cette version, la qualité et l'expérience des visioconférences sur différents terminaux sont améliorées. L'adaptation à la résolution appropriée permet ainsi d'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 en fonction de plusieurs facteurs, tels que la capacité du point de terminaison, les conditions du réseau, et ainsi de suite. Par exemple, 720p, 360p, 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.

URL du magasin sans HTTPS À partir de la version 2312, vous pouvez saisir l'URL du magasin directement sans mentionner `https://` explicitement dans l'URL.

> **Remarque :**
>
> Si vous utilisez toujours un magasin `http`, nous vous recommandons vivement de migrer vers le magasin `https`. En attendant, vous pouvez accéder à votre magasin `http` en ajoutant `http` explicitement au début de l'URL du magasin.

Problèmes résolus

- Il se peut qu'une session ne démarre pas en cas d'interruption du déploiement dans le cloud. Pour plus d'informations sur la configuration de la continuité de service, consultez Continuité de service. [RFHTMCRM-11539]
- Au cours d'une session, lorsque vous ouvrez l'application Microsoft Excel et que vous utilisez la combinaison de touches **Ctrl + barre d'espace**, la combinaison de touches peut ne pas fonctionner comme prévu. [RFHTMCRM-11718]

2311

Nouveautés de la version 2311

Cette version est compatible avec ChromeOS version 119. Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Technical Preview

- Transport adaptatif

Pour obtenir la liste complète des fonctionnalités Technical Preview, consultez la page Fonctionnalités de la version Technical Preview.

Problèmes résolus dans la version 2311

- La redirection USB peut échouer si la stratégie DDC V1 définie sur Citrix Studio de la machine DDC ne prend pas effet. Le problème se produit lorsque la stratégie DDC V1 n'est pas définie comme une priorité supérieure à celle du paramètre de registre VDA avec la clé `\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\GenericUSB`. [RFHTMCRM-11072]
- Lorsque vous démarrez une session de bureau et que vous consultez la console Citrix Director, la valeur ICARTT peut apparaître nulle. La valeur ICARTT peut avoir une valeur positive lorsque vous la vérifiez immédiatement après le début de la session. Cependant, après un certain temps, elle peut apparaître à nouveau nulle. [CVADHELP-23905]

2310

Nouveautés

Cette version est compatible avec ChromeOS version 118. Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes résolus dans la version 2310

- Lorsque vous ouvrez l'application Citrix Workspace pour lancer une session ChromeOS sur un Chromebook, il est possible que les fichiers Google Drive ne s'ouvrent pas. [RFHTMCRM-10540]
- Lorsque vous ouvrez l'application Citrix Workspace pour ChromeOS et que vous accédez à **Paramètres** > **Général** > puis sélectionnez l'option **Mise à l'échelle DPI haute résolution**, il se peut que le curseur s'affiche en double lorsque vous lancez la session de bureau. [RFHTMCRM-10839]
- Lorsque vous utilisez Microsoft Teams dans une session de bureau, la vidéo du participant peut ne pas s'afficher correctement lorsque vous définissez la résolution d'affichage sur l'option **Mise à l'échelle du ratio de pixels de l'appareil**. [RFHTMCRM-5271]
- Au cours d'une session, les périphériques audio, tels que les haut-parleurs et les microphones, peuvent ne pas apparaître. Le problème se produit si la machine locale ne possède aucun microphone ou si l'utilisateur désactive tous les microphones. [RFHTMCRM-10900]

2309.5

Nouveautés

Cette version est compatible avec ChromeOS version 117. Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Problèmes résolus

Cette version résout les problèmes liés à l'API de gestion des fenêtres avec le SDK du canal virtuel.

2309

Nouveautés

Cette version est compatible avec ChromeOS version 117. Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

Mode de saisie Scancode L'application Citrix Workspace vous permet d'utiliser des claviers physiques externes pour interagir avec la disposition du clavier côté serveur sur le VDA. Lorsque les administrateurs activent le mode Scancode, l'utilisateur peut être amené à utiliser la disposition du clavier du serveur plutôt que celle du client.

Cette fonctionnalité améliore l'expérience utilisateur, en particulier lors de l'utilisation d'un clavier physique pour les langues d'Asie de l'Est

> **Remarques :**
>
> - Cette fonctionnalité est désactivée par défaut.
> - Sur les appareils tactiles, lorsque le mode Scancode est activé, le clavier logiciel affiché à l'écran ne fonctionne pas depuis l'application Citrix Workspace.

Pour plus d'informations sur la configuration, consultez Mode de saisie Scancode.

Mappage de clavier personnalisé À partir de la version 2309, les utilisateurs peuvent utiliser des raccourcis et des combinaisons de touches spécifiques à Windows lorsque le VDA est une machine Windows et que le périphérique d'entrée natif est un clavier ChromeOS. Vous pouvez désormais mapper les touches **Ctrl** et **Alt** à l'aide d'un mappage personnalisé. L'utilisateur peut sélectionner la touche Ctrl droite ou gauche pour faire office de touche Alt.

> **Remarques :**
>
> - Le mappage n'est possible qu'en mode plein écran.
> - Une fois le paramètre enregistré, le mappage affecte toutes les sessions.
> - Par défaut, cette fonction est activée.

Pour plus d'informations sur la configuration, consultez la section Mappage de clavier personnalisé.

Pour plus d'informations sur l'utilisation de cette fonctionnalité, consultez la documentation d'aide.

Raccourcis système vers le VDA en mode plein écran À partir de la version 2309, l'application Citrix Workspace sur les appareils ChromeOS prend en charge le transfert de raccourcis système vers le VDA (session de bureau à distance) en mode plein écran. Cependant, cette configuration ne prend pas effet sur le système d'exploitation client.

Auparavant, l'utilisation de ces combinaisons fonctionnait localement. Désormais, lorsque la fonctionnalité est activée et en mode plein écran, ces combinaisons sont envoyées au VDA mais ne prennent pas effet localement. Par exemple, la touche **Actualiser** est une touche système sur Chromebook, et la combinaison **Ctrl+Maj+R** représente un raccourci système sur ChromeOS permettant de

faire pivoter l'écran. Cependant, le VDA Windows n'entreprend aucune action car il n'existe aucun raccourci de ce type dans le système d'exploitation Windows.

Comme autre exemple, `Alt`+ [est utilisé pour épingler une fenêtre ChromeOS sur la gauche, mais le même raccourci n'a aucun effet sur le Windows VDA. Certaines applications peuvent utiliser de tels raccourcis pour une fonction spécifique. Par exemple, certains scanneurs de codes-barres utilisent `Alt`+ [comme préfixe.

> **Remarque :**
>
> - Cette fonctionnalité est activée par défaut.

Pour plus d'informations sur la configuration, consultez la section Raccourcis système vers le VDA en mode plein écran.

Problèmes résolus dans la version 2309

- En mode kiosque avec une configuration multi-moniteurs, les deux écrans peuvent devenir noirs lorsque vous connectez votre deuxième moniteur et que vous démarrez la session [RFHTMCRM-10905].

  Si vous utilisez la version 2308, nous vous recommandons de passer à la version 2309.

  Toutefois, si vous souhaitez continuer à travailler avec la version 2308, ajoutez les données JSON suivantes depuis la console d'administration Google :

```
{

"settings": {

        "Value": {

                "settings_version": "1.0",
                "engine_settings": {

                        "features": {

                                    "graphics": {

                                    "graphicsWebWorker": {

                                                "enabled":
                                                   false
                                        }
,
                                "graphicsWasmRender": false
                                        }

                                 }
```



```
23
24                                  }
25
26                              }
27
28                          }
29
30                   }
31
32                <!--NeedCopy-->
```

2308

Nouveautés dans la version 2308

Cette version est compatible avec ChromeOS version 115. Cette version améliore les performances liées aux graphismes.

Problèmes résolus dans la version 2308

- Lorsque vous démarrez une session en mode Session Invité gérée, la redirection USB automatique peut ne pas fonctionner comme prévu. [RFHTMCRM-10625]
- La fonctionnalité de continuité de service ne fonctionne pas. En d'autres termes, vous ne pouvez pas vous connecter aux applications et aux bureaux DaaS en cas de panne. [RFHTMCRM-9261]

2307

Nouveautés

Cette version est compatible avec ChromeOS version 114. En outre, elle résout certains problèmes afin d'améliorer la stabilité et les performances générales.

Améliorations apportées à Microsoft Teams L'optimisation de Microsoft Teams prend en charge la transcription en temps réel de la source audio du haut-parleur lorsque la fonction Sous-titres en direct est activée dans Microsoft Teams.

Redirection automatique des périphériques USB Pour rediriger automatiquement les périphériques USB, vous devez suivre les règles relatives aux périphériques USB.
Vous pouvez configurer les règles relatives aux périphériques USB par les moyens suivants :

- Stratégie d'administration Google
- Règles des périphériques
- Règles de redirection de périphérique USB client (version 2)

Amélioration de l'expérience de session HDX Grâce à une technique de compression améliorée, l'application Citrix Workspace pour ChromeOS consomme peu de ressources réseau et améliore la réactivité des sessions.

Améliorations apportées à la redirection USB composite via des stratégies DDC À partir de la version 2307, vous pouvez déterminer si une interface ou une classe USB composite particulière peut être redirigée vers un VDA (Virtual Delivery Agent) par défaut ou non. Si un port USB composite est connecté à l'appareil ChromeOS, la configuration **EnableDefaultAllowPolicy** vous permet de décider d'autoriser par défaut la redirection USB via des stratégies DDC. Les versions 2212 et ultérieures du VDA prennent en charge cette fonctionnalité.

Pour plus d'informations, consultez la section Améliorations apportées à la redirection USB composite via des stratégies DDC dans la documentation.

Mappage des lecteurs clients À partir de la version 2307, la fonctionnalité de mappage des lecteurs clients (CDM) prend en charge le mappage de dossiers sur l'appareil ChromeOS pour les rendre accessibles dans une session. Vous pouvez mapper n'importe quel dossier depuis l'appareil ChromeOS. Il peut s'agir, par exemple, des dossiers provenant de Téléchargements, de Google Drive et de clés USB, si le dossier ne contient pas de fichiers système.

L'utilisateur peut effectuer les opérations suivantes :

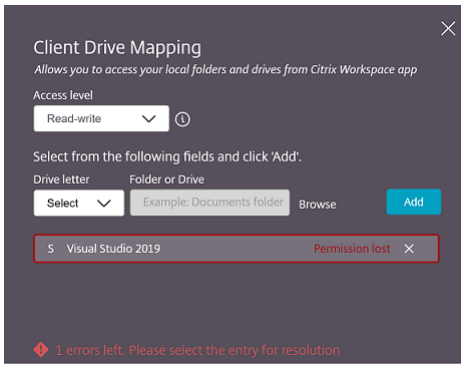
- Copiez les fichiers et les dossiers sur le lecteur mappé à partir de la session et inversement.
- Afficher la liste des fichiers et des dossiers du lecteur mappé.
- Ouvrez, lisez et modifiez le contenu des fichiers sur le lecteur mappé.
- Afficher les propriétés du fichier (heure de modification et taille de fichier uniquement) sur le lecteur mappé.

Cette fonctionnalité offre l'avantage d'accéder à la fois aux lecteurs de bureaux virtuels et aux lecteurs de machines locales dans l'explorateur de fichiers au sein de la session HDX.

Limitations connues

- Vous ne pouvez pas renommer les fichiers et dossiers à l'intérieur du lecteur mappé.
- Les mappages portent uniquement le nom du dossier (non le chemin complet).

- Si votre dossier local contient des fichiers cachés et que vous avez mappé le même dossier, les fichiers cachés sont visibles dans la session sur le lecteur mappé.
- Vous ne pouvez pas modifier la propriété du fichier pour qu'elle soit accessible en lecture seule sur le lecteur mappé.
- CDM n'est pas pris en charge si les sessions sont ouvertes en mode intégré à l'aide du SDK HDX.
- Lorsque vous mappez un dossier à partir d'un périphérique amovible et que vous le supprimez pendant une session active, vous ne pouvez pas utiliser le lecteur mappé dans cette session. Cliquez sur le **X** près des mappages que vous voulez supprimer manuellement.



Pour plus d'informations, consultez la section Mappage des lecteurs clients dans la documentation.

Technical Preview

- Accessibilité et TalkBack

Pour obtenir la liste complète des fonctionnalités Technical Preview, consultez la page Fonctionnalités de la version Technical Preview.

Problèmes résolus

- Lorsque l'utilisateur ouvre une application publiée et actualise l'application Citrix Workspace, une instance dupliquée de l'application publiée apparaît. Pour appliquer les paramètres de configuration, consultez la section Actualisation du magasin. [CVADHELP-22229]
- En mode multi-moniteurs, lorsque vous ouvrez une application publiée sur le deuxième moniteur, les clics de souris peuvent ne pas se comporter comme prévu. [CVADHELP-21916]
- Il est possible que la fenêtre de notification de progression du lancement de session (qui apparaît en bas à droite de l'écran) ne se ferme pas même après le démarrage de la session. Ce problème survient avec la version 7.15 du VDA. [RFHTMCRM-10161]

2306

Cette version est compatible avec la version 114 de ChromeOS, désignée par Google comme version de support à long terme (LTS). À ce titre, Citrix continue de prendre en charge cette version jusqu'à la fin du cycle de vie de la version LTS. Consultez la déclaration de compatibilité Citrix pour plus d'informations sur les exclusions.

Nouveautés

Configurer la redirection des périphériques USB composites via des stratégies DDC Auparavant, les administrateurs utilisaient les stratégies d'administration Google pour configurer la redirection USB côté client.

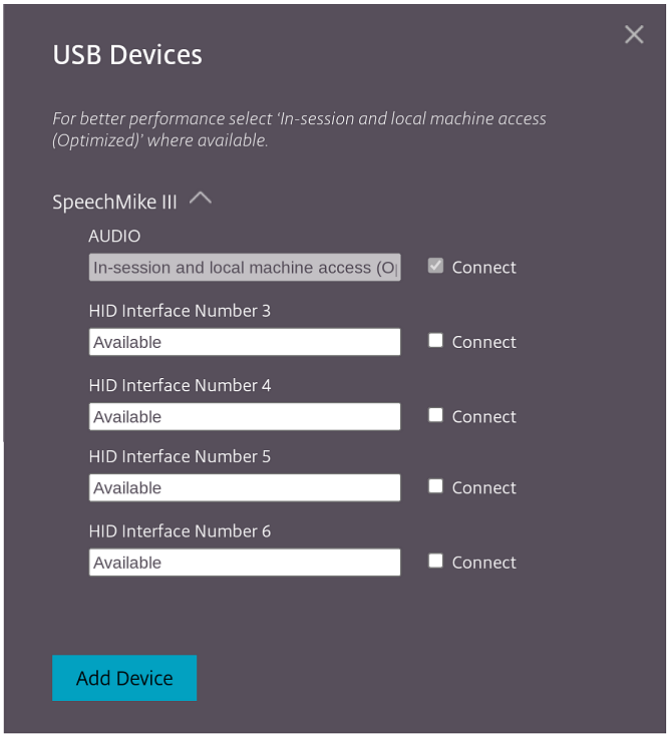
À partir de la version 2306, vous pouvez également configurer la redirection USB via les stratégies DDC. Les configurations via des stratégies DDC permettent aux administrateurs de définir les stratégies et les comportements de manière unifiée et centralisée. Ces stratégies s'appliquent aux déploiements sur site et dans le cloud sur les appareils et les utilisateurs gérés. Cette fonctionnalité est prise en charge sur les versions 2212 et ultérieures du VDA.

Pour plus d'informations sur la procédure de configuration, consultez la section Configurer la redirection des périphériques USB composites via des stratégies DDC.

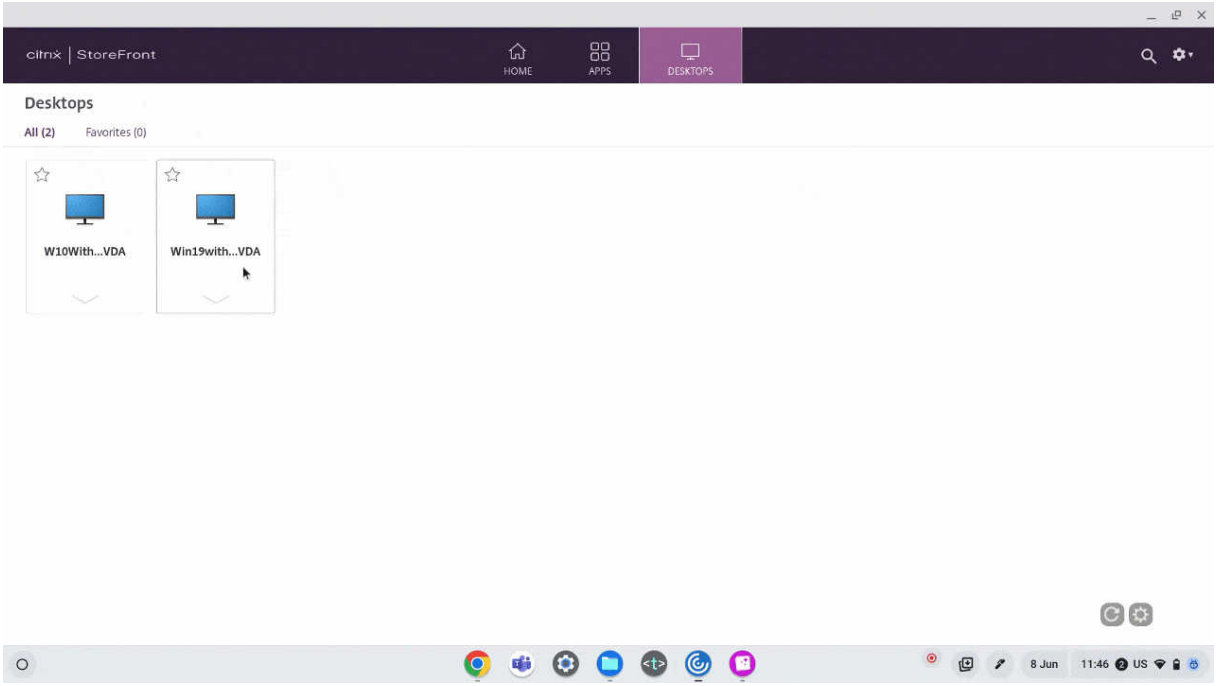
Améliorations apportées à l'interface utilisateur des périphériques USB composites À partir de la version 2306, lorsque la configuration d'un périphérique USB composite est définie sur « split: true », l'interface utilisateur **Périphériques USB** affiche les composants en fonction des numéros d'interface plutôt que des classes d'interface.

Pour plus d'informations, consultez l'article Redirection USB composite.

Interface utilisateur Voici un exemple :



Amélioration de l'expérience de lancement de Virtual Apps and Desktops À partir de la version 2306, l'expérience améliorée de lancement d'applications et de bureaux fournit des informations pertinentes et actualisées sur l'état du lancement.



Problèmes résolus

- Lorsque vous débranchez et rebranchez le périphérique USB qui est déjà en session, la redirection du périphérique échoue à nouveau. Un compteur de progression du chargement apparaît jusqu'à ce que vous redémarriez l'application Citrix Workspace. [FRHTMCRM-9715]
- Lorsque vous participez à une réunion Microsoft Teams optimisée, le streaming de la caméra échoue. La vidéo est floue et peut parfois ne plus répondre. Le problème se produit lorsque la fonctionnalité de partage d'écran est désactivée et que l'utilisateur active la caméra lors d'une réunion Microsoft Teams. [RFHTMCRM-9968]
- Sur un Chromebook, lorsque la session est en mode tablette, vous devrez peut-être appuyer plusieurs fois sur l'icône de l'application depuis l'étagère Chrome, par exemple l'icône du Bloc-notes, pour ramener l'application transparente au premier plan. [RFHTMCRM-9803]
- Lorsque les sessions sont en mode tablette, le stylet d'un Chromebook peut ne pas fonctionner. [RFHTMCRM-9951]
- Au cours d'une session, l'utilisateur peut observer des problèmes audio intermittents. Le problème se produit après la mise à niveau vers l'application Citrix Workspace pour ChromeOS 2304 et versions ultérieures. [CVADHELP-22784]

2305

Nouveautés

Prise en charge des imprimantes réseau Auparavant, l'option Imprimante PDF Citrix était utilisée pour imprimer à partir de la session de bureau virtuel. Le pilote d'imprimante convertissait le fichier au format PDF et le transférait sur l'appareil local. Le fichier PDF s'ouvrait alors dans une nouvelle fenêtre pour visualisation et impression.

À compter de la version 2305, l'application Citrix Workspace pour ChromeOS prend en charge l'impression réseau. Les utilisateurs peuvent consulter la liste des imprimantes connectées à leur Chromebook au cours de la session. Les utilisateurs peuvent sélectionner une imprimante directement sans générer de fichiers PDF intermédiaires sur l'appareil local. Cette fonctionnalité est prise en charge sur les :

- VDA version 2112 et versions ultérieures
- ChromeOS version 112 et versions ultérieures

> **Remarque :**
>
> - Par défaut, cette fonctionnalité est activée et seul le format PDF pour l'impression de métafichiers est pris en charge.

Pour plus d'informations sur la configuration, consultez Prise en charge des imprimantes réseau.

Prise en charge de magasins multiples À partir de la version 2305, les administrateurs informatiques peuvent attribuer plusieurs magasins aux utilisateurs. Désormais, les utilisateurs peuvent facilement passer d'un magasin à l'autre sans avoir à se souvenir de l'URL exacte du magasin. Cette fonctionnalité améliore l'expérience utilisateur lors de l'accès à plusieurs magasins.

Pour plus d'informations sur la configuration, consultez Prise en charge de magasins multiples.

Améliorations apportées à la redirection des URL Auparavant, lorsque la redirection hôte vers client était activée, les URL étaient interceptées sur le VDA du serveur et envoyées à l'appareil de l'utilisateur. L'application Citrix Workspace pour ChromeOS affichait une boîte de dialogue invitant l'utilisateur à ouvrir l'URL dans la session ou sur l'appareil local. La boîte de dialogue s'affichait pour chaque URL.

À partir de la version 2305, les administrateurs peuvent configurer la redirection des URL. Ainsi, les liens peuvent être ouverts sur l'appareil local sans boîte de dialogue supplémentaire. Cette amélioration améliore l'expérience utilisateur.

> **Remarque :**
>
> - Cette fonctionnalité est désactivée par défaut.

Pour plus d'informations sur la configuration, consultez Améliorations apportées à la redirection des URL.

Prise en charge du fichier manifeste V3 pour les scénarios du SDK À compter de la version 2305, l'application Citrix Workspace pour ChromeOS prend en charge le SDK HDX avec les extensions Chrome dotées de la version 3 du fichier manifeste.

Pour plus d'informations, accédez à la page Citrix Workspace app for ChromeOS HDX SDK dans la documentation du développeur.

Améliorations apportées au SDK du canal virtuel À compter de la version 2305, l'application Citrix Workspace pour ChromeOS prend en charge les API de gestion des fenêtres dans le SDK du canal virtuel. Les API Web permettent aux administrateurs informatiques de créer des applications interactives et de les personnaliser pour leurs utilisateurs finaux.

Problèmes résolus

- Lorsque vous essayez de déconnecter une session d'application virtuelle ou de bureau via le SDK HDX pour ChromeOS, la session reste active dans DDC. Toutefois, l'état de la session passe à inactif au bout de quelques minutes. [RFHTMCRM-9181]

- Lors d'une session, lorsque deux participants se trouvent dans la réunion Microsoft Teams optimisée, le partage d'écran et le son peuvent échouer. Le problème se produit lorsque vous activez et désactivez la caméra plusieurs fois au cours de l'appel. [CVADHELP-22251]
- Lorsque vous effectuez la mise à niveau de votre appareil vers la version 108 de ChromeOS, le texte affiché sur le bureau publié peut apparaître flou. Le problème se produit sur les appareils sur lesquels l'unité de traitement graphique (GPU) ne prend pas en charge la précision moyenne. [CVADHELP-22362]

  > **Remarque :**
  >
  > – Les paramètres d'affichage de certains appareils ne prennent pas en charge la haute précision, mais le texte sur le bureau publié peut s'afficher correctement. Cependant, l'affichage peut sembler anormal à cause de ce correctif. Pour corriger ce problème, les administrateurs peuvent définir l'attribut **webglHighPrecision** sur **false** via la stratégie d'administration Google.
  > Voici un exemple de données JSON :

```
1 ```
2          "hardware" : {
3
4              "webglHighPrecision" : false
5           }
6 ,
7 <!--NeedCopy--> ```
```

2304

Nouveautés

Amélioration des gestes sur les appareils tactiles À partir de la version 2304, l'application Citrix Workspace améliore l'expérience liée aux gestes, au multipoint et au clavier logiciel (mode tablette). Dans vos sessions de l'application Citrix Workspace, vous pouvez utiliser tous les gestes multipoint habituels, notamment toucher, balayer et faire glisser.

Voici le guide des gestes :

Pour ce faire :	Sur l'application Citrix Workspace, procédez comme suit :
Clic simple	Toucher à un doigt
Clic droit	Toucher-Maintenir-Relâcher

Pour ce faire :	Sur l'application Citrix Workspace, procédez comme suit :
Ouvrir le clavier à l'écran	Toucher à trois doigts (ou à partir de la barre d'outils, toucher l'icône **Clavier**)
Déplacer	Toucher-Maintenir-Faire glisser
Activer le curseur	Toucher à deux doigts

Problèmes résolus dans la version 2304

- Il n'y a aucun problème résolu dans cette version.

2303

Nouveautés

Cette version est compatible avec ChromeOS version 111. En outre, elle résout certains problèmes afin d'améliorer la stabilité et les performances générales.

Prise en charge des périphériques audio Plug and Play Auparavant, un seul périphérique de lecture et d'enregistrement audio était pris en charge et était affiché en tant que **Citrix HDX Audio**, quel que soit le nom réel du périphérique.

À partir de la version 2303, vous pouvez connecter plusieurs périphériques audio et les rediriger vers le VDA. Lorsque vous redirigez des périphériques audio USB, vous pouvez afficher le nom réel du périphérique audio sous les paramètres **Son** > **Lecture** et **Son** > **Enregistrement** sur le VDA. La liste des périphériques du VDA est mise à jour dynamiquement chaque fois qu'un périphérique audio est branché ou retiré.

> **Remarque :**
>
> Cette fonctionnalité est activée par défaut.

Pour plus d'informations, consultez Prise en charge des périphériques audio Plug and Play.

Flou d'arrière-plan et effets dans l'optimisation de Microsoft Teams À compter de la version 2303, l'application Citrix Workspace pour ChromeOS prend en charge le flou et les effets d'arrière-plan dans l'optimisation de Microsoft Teams pour les appels vidéo. Vous pouvez flouter ou remplacer les effets d'arrière-plan fournis par Microsoft Teams pour éviter les distractions inattendues en aidant la

conversation à rester centrée sur la silhouette (corps et visage). Cette fonctionnalité peut être utilisée avec les appels P2P et les conférences téléphoniques.

> **Remarques :**
>
> - Cette fonctionnalité est désactivée par défaut.
> - Cette fonctionnalité est désormais intégrée à l'interface utilisateur 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.

Pour plus d'informations, consultez Flou d'arrière-plan et effets dans l'optimisation de Microsoft Teams.

Problèmes résolus dans la version 2303

- Au cours d'une session, lorsque deux participants rejoignent une réunion Microsoft Teams optimisée, l'écran devient noir lorsque la caméra est désactivée. En outre, les icônes telles que Partage d'écran, Conversation ou Contacts sont disponibles et cliquables. Cependant, lorsque vous cliquez sur ces icônes, les options correspondantes sont masquées sous l'écran noir et n'apparaissent pas comme prévu. [CVADHELP-22173]

2301.1

Nouveautés

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

Problèmes résolus

- Lorsque vous copiez ou collez du texte dans la session, celle-ci ne répond plus. Le problème se produit lorsque vous utilisez l'application Citrix Workspace pour ChromeOS version 2301. [CVADHELP-21951]
- La redirection du périphérique audio vers la session Citrix Virtual Apps and Desktops ne fonctionne pas. Un « X » rouge apparaît sur l'icône de réglage du volume dans la barre d'état système. Le problème se produit après la mise à jour de l'application Citrix Workspace pour ChromeOS vers la version 2301. [RFHTMCRM-8799]

2301

Nouveautés

Cette version est compatible avec ChromeOS version 109. En outre, elle résout certains problèmes afin d'améliorer la stabilité et les performances générales.

Continuité du service La fonction Continuité du service supprime ou réduit la dépendance à l'égard de la disponibilité des composants impliqués dans le processus de connexion. Vous pouvez lancer des sessions Citrix Virtual Apps and Desktops et Citrix DaaS quel que soit l'état d'intégrité des services cloud. En d'autres termes, la continuité du service vous permet de vous connecter aux applications et aux bureaux DaaS en cas de panne. Pour ce faire, votre appareil doit maintenir une connexion réseau à un emplacement de ressources.

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

Prise en charge des périphériques audio Plug and Play Auparavant, un seul périphérique de lecture et d'enregistrement audio était pris en charge et était affiché en tant que **Citrix HDX Audio**, quel que soit le nom réel du périphérique.

À partir de la version 2301, nous prenons en charge plusieurs périphériques audio et les redirigeons vers le VDA. Désormais, lorsque vous redirigez des périphériques audio, vous pouvez afficher le nom réel du périphérique audio sous les paramètres **Son** > **Lecture** et **Son** > **Enregistrement** sur le VDA. La liste des périphériques du VDA est mise à jour dynamiquement chaque fois qu'un périphérique audio est branché ou retiré.

Limitations connues

- Sur le VDA, le nom du périphérique audio intégré est affiché uniquement en anglais. Le problème se produit lorsque vous utilisez des appareils basés sur ChromeOS. [RFHTMCRM-8667]

Pour plus d'informations, consultez la documentation Prise en charge des périphériques audio Plug and Play.

Conversations et réunions à fenêtres multiples pour Microsoft Teams À partir de la version 2301, vous pouvez utiliser plusieurs fenêtres pour les conversations et les réunions dans Microsoft Teams. Vous pouvez ouvrir plusieurs fenêtres pour les conversations ou les réunions de différentes manières.

Pour plus d'informations sur cette fonctionnalité, consultez Afficher une conversation dans Teams.

Pour plus d'informations sur le dépannage, consultez CTX253754.

Microsoft va mettre fin à la prise en charge de la fonctionnalité de fenêtre unique. Si vous utilisez une ancienne version de l'application Citrix Workspace ou de Virtual Delivery Agent (VDA), vous pouvez effectuer une mise à niveau vers :

- Application Citrix Workspace 2301 ou version ultérieure
  et
- VDA 2203 ou version ultérieure

Redirection du contenu du navigateur La redirection du contenu du navigateur redirige le contenu du navigateur distant vers le bureau de l'ordinateur de l'utilisateur. La redirection du contenu du navigateur est un navigateur Web sans cadre et sans bordure qui s'exécute dans la fenêtre du bureau distant et couvre (superpose) la zone de contenu du navigateur distant (VDA).

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 HTML5 ou WebRTC. Seule la fenêtre d'affichage (zone visible de l'utilisateur d'une page Web) est redirigée vers le point de terminaison. La redirection du contenu du navigateur ne redirige pas l'interface utilisateur (barre d'adresse, barre d'outils, etc.) du navigateur sur le VDA.

En d'autres mots, la redirection du contenu du navigateur permet d'afficher les pages Web dans la liste verte du côté client. 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.

> **Remarque :**
>
> - La redirection du contenu du navigateur est compatible avec les versions 2212 et ultérieures de Citrix Virtual Apps and Desktops.

Pour plus d'informations sur la configuration de la liste d'autorisation, voir :

- Extension Chrome de redirection du contenu du navigateur.
- Paramètres de stratégie Redirection du contenu du navigateur.

Problèmes connus liés à cette fonctionnalité

- Pendant la redirection du contenu du navigateur, lorsque vous ouvrez un lien vers un site Web dans un nouvel onglet, celui-ci s'ouvre dans le navigateur client au lieu du navigateur de session. [HDX-43206]

Limites connues de cette fonctionnalité

- Cette fonctionnalité ne prend pas en charge les éléments suivants :
  - Scénario de récupération du serveur et de restitution du client.
  - Serveur Integrated Windows Authentication (IWA).
  - Fonctionnalité multi-moniteurs.
- Lorsque vous chargez ou téléchargez un fichier sur certains sites Web redirigés par la redirection du contenu du navigateur, le sélecteur de fichiers ChromeOS apparaît à la place d'un sélecteur de fichiers de session VDA. [HDX-43207]
- L'impression n'est pas prise en charge à partir de pages redirigées par la redirection du contenu du navigateur.

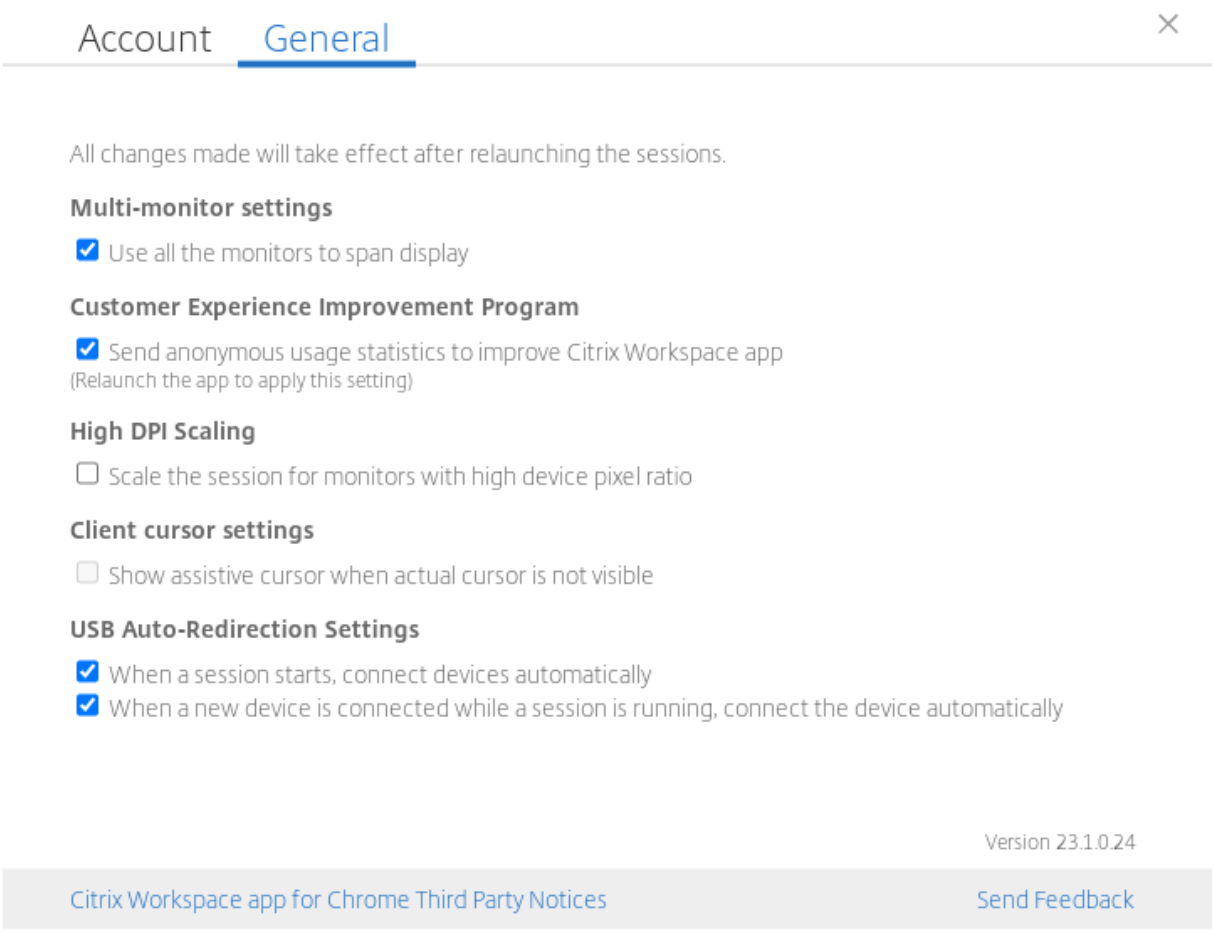
Double saut À partir de la version 2301, l'application Citrix Workspace prend en charge les scénarios à double saut. Cette fonctionnalité constitue une amélioration de la redirection USB.

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

Paramètres de redirection automatique USB Auparavant, aucune option liée aux paramètres de redirection automatique USB ne permettait de définir les préférences de l'utilisateur. Les administrateurs contrôlant ces stratégies, l'utilisateur devait rediriger manuellement les périphériques USB requis à chaque lancement de session.

À partir de la version 2301, l'utilisateur peut sélectionner une préférence pour la redirection automatique pour n'importe quel périphérique USB au sein d'une session Virtual Desktop. L'application Citrix Workspace fournit désormais des paramètres au niveau de l'application grâce auxquels l'utilisateur peut contrôler la redirection automatique USB. L'utilisateur peut définir des préférences et enregistrer les paramètres pour tous les lancements de session.

Il existe deux options : l'une au lancement de la session et l'autre pendant que la session est en cours.



Remarque :

- Cette fonctionnalité prend en charge les déploiements sur site et dans le cloud, et n'est disponible que pour les utilisateurs d'appareils Chrome gérés.

Problèmes résolus dans la version 2301

- Dans les déploiements dans le cloud, la fonctionnalité d'impression PDF améliorée ne fonctionne pas comme prévu. L'aperçu d'impression s'ouvre dans une nouvelle fenêtre au lieu de s'ouvrir dans la même fenêtre. [RFHTMCRM-8672]
- La redirection de webcam ne fonctionne pas lorsque vous utilisez Citrix Virtual Apps and Desktops version 2206 et versions ultérieures. Avec le dernier correctif, la redirection de la webcam est réussie depuis l'application Citrix Workspace pour ChromeOS version 2301 et versions ultérieures. [RFHTMCRM-8580]
- Lorsque vous utilisez Citrix Virtual Apps and Desktops version 2203 et versions ultérieures, vous pouvez constater que la session VDA semble déformée. [RFHTMCRM-8657]

- Lorsque vous utilisez un Chromebook et que vous essayez de lancer un appel depuis Microsoft Teams optimisé, l'appel ne fonctionne pas comme prévu. Le message d'erreur suivant s'affiche :

  « Connexion impossible ». [CVADHELP-21670] [CVADHELP-21500]

Problèmes connus

Problèmes connus dans la version 2402.1

- La fonctionnalité de continuité de service peut ne pas fonctionner pour les URL de domaine personnalisées. [RFHTMCRM-12363]
- Si vous tentez de télécharger ou de modifier des fichiers dans le lecteur mappé à partir d'un VDA à l'aide d'applications utilisant des fichiers temporaires, les données peuvent être corrompues. Par exemple, les navigateurs et les applications Microsoft Office telles qu'Excel. [RFHTMCRM-12156] [RFHTMCRM-11474]
- Au cours d'une session, il est possible que vous observiez une mauvaise qualité audio. La hauteur du flux audio peut changer automatiquement.

  Pour contourner le problème, définissez l'attribut **AudioRedirectionV4** sur **false**. Pour obtenir la procédure de désactivation de **AudioRedirectionV4**, consultez la section Prise en charge des périphériques audio Plug and Play. [CVADHELP-24722]

Problèmes connus dans la version 2402

- Si vous tentez de télécharger ou de modifier des fichiers dans le lecteur mappé à partir d'un VDA à l'aide d'applications utilisant des fichiers temporaires, les données peuvent être corrompues. Par exemple, les navigateurs et les applications Microsoft Office telles qu'Excel. [RFHTMCRM-12156] [RFHTMCRM-11474]
- Lorsqu'un utilisateur se déconnecte de la page d'un magasin (intentionnellement ou suite à une inactivité) et se reconnecte à la même page de magasin, la page du magasin peut être vide ou un compteur infini peut apparaître. Le problème se produit sur les déploiements cloud activés pour la continuité de service.

  Pour contourner le problème, cliquez sur l'icône **Recharger** sur la page du magasin. [RFHTMCRM-12212]
- Au cours d'une session, il est possible que vous observiez une mauvaise qualité audio. La hauteur du flux audio peut changer automatiquement.

Pour contourner le problème, définissez l'attribut **AudioRedirectionV4** sur **false**. Pour obtenir la procédure de désactivation de **AudioRedirectionV4**, consultez la section Prise en charge des périphériques audio Plug and Play. [CVADHELP-24722]

Problèmes connus dans la version 2312

- Lorsque vous activez la fonctionnalité de continuité de service et lorsqu'une interruption du déploiement dans le cloud survient, l'icône de l'application Citrix Workspace apparaît sur l'étagère Chrome au lieu des icônes de la session de bureau ou d'application. [RFHTMCRM-11647]

Problèmes connus dans la version 2310

- Lorsque vous lancez une session de bureau à l'aide de l'application Citrix Workspace, des blocs verts apparaissent sur l'écran d'affichage et bloquent l'interface utilisateur. Le problème peut se produire lorsque vous déplacez une fenêtre d'application à l'intérieur du bureau lancé. [CVADHELP-23377]
- En mode kiosque, les sessions peuvent ne pas démarrer automatiquement. [CVADHELP-23698]

Problèmes connus dans la version 2309

- Sur les appareils Chromebook, l'application Citrix Workspace ne passe pas de IPv6 à IPv4 sur un réseau Wi-Fi à double pile. [CVADHELP-22537]

Problèmes connus dans la version 2203

- La redirection de la webcam peut ne pas fonctionner dans certaines instances de Citrix Virtual Apps and Desktops ou XenDesktop. [HDX-39396]

Limitations

- L'application Citrix Workspace pour ChromeOS ne prend pas en charge le mode graphique H.264 plein écran avec plusieurs moniteurs.
- Lors du partage d'écran à l'aide de l'optimisation Microsoft Teams, la bordure rouge autour de la fenêtre partagée n'apparaît pas.
- Lorsque l'option **Utiliser le codage matériel pour le codec vidéo** est définie sur **Activé** dans Citrix Studio, votre écran peut apparaître en vert pendant une session utilisant un VDA Intel vGPU. [RFHTMCRM-5521]

- Dans les sessions multi-moniteurs utilisant un VDA Microsoft Windows 7, les moniteurs étendus peuvent apparaître en noir. De plus, le curseur de la souris peut ne pas s'afficher correctement. Nous vous recommandons de sélectionner une résolution d'affichage combinée de moins de 4800 pixels en largeur et en hauteur. [RFHTMCRM-5539]
- Le serveur revient sur YUV420 même lorsqu'il est configuré sur le paramètre Graphics-Thinwire YUV444. Les applications riches en graphiques sont limitées à la gamme YUV420. [RFHTMCRM-5520]
- L'authentification unique (SSO) avec Google IdP (fournisseur d'identité) n'est pas prise en charge.
- Lorsque vous essayez de vous connecter à l'application Citrix Workspace, vous pouvez observer des problèmes lors du processus de connexion. Le message d'erreur suivant s'affiche : ERR_TOO_MANY_REDIRECTS.

  Le problème se produit lorsque vous utilisez Google IdP. [CVADHELP-19362]
- Dans l'appel vidéo Microsoft Teams optimisé, lorsque vous ajoutez le troisième participant, la vidéo devient vide pour l'un des deux premiers participants. Le problème se produit lorsque les deux premiers participants utilisent ChromeOS et que le troisième utilise un système d'exploitation différent. [RFHTMCRM-7408]
- Lorsque vous connectez plusieurs périphériques audio au cours d'une session, vous pouvez entendre le son provenant d'un seul périphérique. Il se peut que vous ne puissiez pas passer à l'autre périphérique audio. [HDX-49312]
- Au cours d'une session, il se peut que vous n'entendiez pas le son provenant de certaines applications lorsque vous vous déconnectez et que vous vous reconnectez à votre session précédente via la barre d'outils. [HDX-49313]
- Lorsque les utilisateurs finaux se connectent au magasin configuré via Imprivata en tant que fournisseur d'identité, l'écran de détection des clients apparaît. Toutefois, lorsque les utilisateurs cliquent sur **Détecter l'application Citrix Workspace**, l'erreur suivante s'affiche :

  receiver links are blocked (« Les liens Receiver sont bloqués. »)

  Pour contourner ce problème, rechargez l'application Citrix Workspace pour ChromeOS. [CVADHELP-22026]
- Lorsque vous changez de réseau et que l'une des connexions Wi-Fi n'est pas connectée à Internet, la fonctionnalité de fiabilité de session ne fonctionne pas correctement. [RFHTMCRM-12349]
- Le minuteur de synchronisation des fichiers de location est réinitialisé chaque fois que vous cliquez sur le bouton de rechargement de l'application Citrix Workspace. Cette action a un impact sur la mise à disposition de la fonctionnalité de continuité de service à l'utilisateur final. [RFHTMCRM-12499]

- Le téléchargement des fichiers de location échoue après la déconnexion et la reconnexion à l'application Citrix Workspace pour ChromeOS. [RFHTMCRM-12492]
- La fonctionnalité de continuité de service n'est pas prise en charge en mode kiosque. [RFHTMCRM-12518]

Fin de prise en charge

Pour plus d'informations sur les éléments obsolètes, consultez la page Fin de prise en charge.

Ancienne documentation

Pour les versions de produits qui ont atteint leur fin de vie, consultez la section Ancienne documentation.

Technical Preview

Les fonctionnalités présentées dans les versions Technical Preview sont disponibles à des fins d'utilisation dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités présentées dans les versions Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut prendre en considération les commentaires en fonction de leur gravité, criticité et importance.

Fonctionnalités de la version Technical Preview

June 18, 2024

Les fonctionnalités présentées dans les versions Technical Preview sont disponibles à des fins d'utilisation dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités présentées dans les versions Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut prendre en considération les commentaires en fonction de leur gravité, criticité et importance.

Liste des fonctionnalités de la version Technical Preview

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

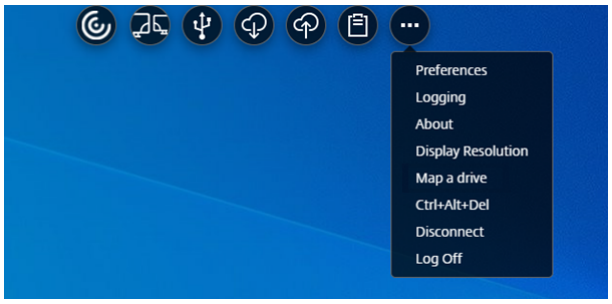
Titre	Disponible à partir de la version	Formulaire d'activation (cliquez sur l'icône)	Formulaire de commentaires (cliquez sur l'icône)
Barre d'outils dans la session améliorée	2405	Vous pouvez configurer la fonctionnalité	
Transport adaptatif	2311		
Accessibilité et TalkBack	2307	Activation non requise	

Barre d'outils dans la session améliorée

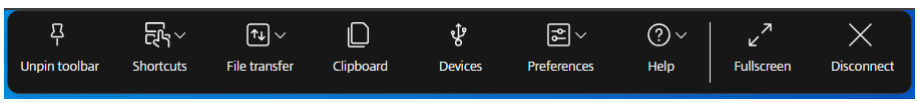
Cette fonctionnalité est disponible en version Technical Preview depuis la publication de la version 2405.

À partir de la version 2405, une interface utilisateur améliorée de la barre d'outils apparaît lorsque vous démarrez une session de bureau. L'apparence de l'interface utilisateur de la barre d'outils dans la session a changé. L'interface utilisateur de la barre d'outils est spécialement conçue pour améliorer l'expérience de l'utilisateur final en organisant les options de manière conviviale.

Ancienne interface utilisateur de la barre d'outils



Nouvelle interface utilisateur de la barre d'outils



> **Remarque :**
>
> Cette fonction est désactivée par défaut. Pour activer cette fonctionnalité, suivez les étapes de configuration. Pour nous faire part de vos commentaires sur cette fonctionnalité, cliquez sur le formulaire Podio.

Configuration

Vous pouvez activer la nouvelle interface utilisateur de la barre d'outils à l'aide de la stratégie d'administration Google.

Stratégie d'administration Google Pour les appareils et les utilisateurs gérés, les administrateurs peuvent activer la fonctionnalité à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé **engine_settings**.

   > **Remarque :**
   >
   > Vous pouvez également appliquer cette configuration aux éléments suivants :
   >
   > - **Appareil** > **Chrome** > **Applications et extensions** > **Utilisateurs et navigateurs** > Rechercher l'extension > Règles relatives aux extensions
   > - **Appareil** > **Chrome** > **Applications et extensions** > **Kiosques** > Rechercher l'extension > Règles relatives aux extensions
   > - **Appareil** > **Chrome** > **Applications et extensions** > **Sessions Invité gérées** > Rechercher l'extension > Règles relatives aux extensions

   Voici un exemple de données JSON :

```
{

    "engine_settings": {

        "ui": {

            "toolbar":
                {
  "switchToNewToolbar": true
                }

             }

        }
```



```
15
16    }
17
18  <!--NeedCopy-->
```

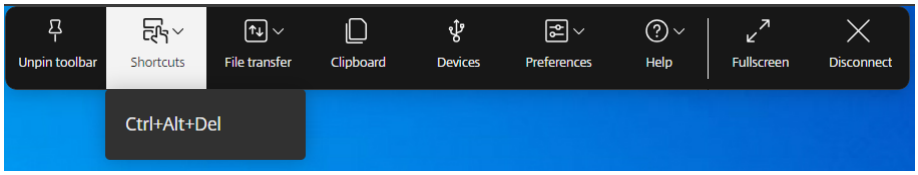
4. Enregistrez les modifications.

Icônes et actions

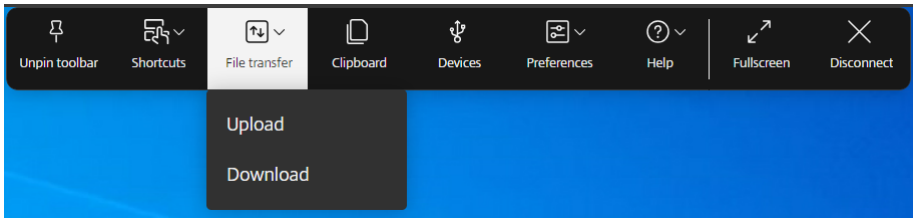
Les utilisateurs finaux peuvent effectuer les actions suivantes :

> **Remarque :**
>
> Les icônes ne sont visibles pour les utilisateurs finaux que si l'administrateur de leur organisation a activé la fonctionnalité spécifique.

- **Encoche de la barre d'outils** : lorsque vous démarrez une application ou une session de bureau, l'encoche de la barre d'outils apparaît en haut de l'écran. Lorsque vous cliquez sur l'encoche, la barre d'outils apparaît à l'état non épinglé. Faites glisser et repositionnez l'encoche de la barre d'outils sur n'importe quel côté de l'écran. Après avoir relâché la souris, l'encoche s'aligne automatiquement sur le bord le plus proche.
- **Épingler** : lorsque vous l'épinglez, vous pouvez faire glisser la barre d'outils et la repositionner sur n'importe quel côté de l'écran. Après avoir relâché la souris, l'encoche s'aligne automatiquement sur le bord le plus proche. L'avantage d'épingler la barre d'outils est qu'elle ne se réduit en une encoche une fois que vous avez effectué une action impliquant des icônes de barre d'outils.
- **Désépingler** : lorsque vous désépinglez la barre d'outils, elle se réduit en une encoche une fois que vous avez effectué une action impliquant des icônes de barre d'outils.
- **Touches de raccourci** : vous pouvez exécuter la fonction **Ctrl + Alt + Suppr** en cliquant sur un bouton. Cette option permet aux utilisateurs de se déconnecter, de changer d'utilisateur, de verrouiller le système ou d'accéder au Gestionnaire des tâches.



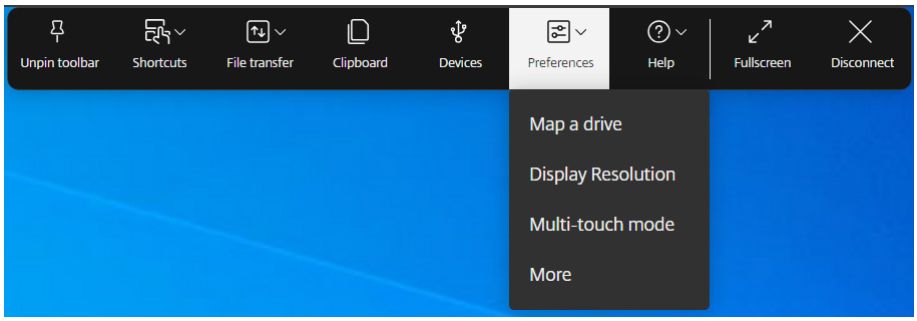
- **Transfert de fichiers** : vous pouvez charger ou télécharger un fichier entre une machine utilisateur et une session. Pour plus d'informations, consultez la section Gestion des fichiers.



- **Presse-papiers** : vous pouvez utiliser l'option Presse-papiers pour copier et coller du texte brut et des données HTML du VDA vers le périphérique local et inversement. Pour plus d'informations, consultez la section Presse-papiers.
- **Périphériques** : cliquez pour ouvrir la boîte de dialogue **Périphériques USB**. Cliquez sur **Ajouter** pour afficher les périphériques USB connectés au périphérique local. La boîte de dialogue répertorie les appareils qui peuvent être redirigés vers la session. Pour rediriger les périphériques USB, sélectionnez un périphérique approprié, puis cliquez sur **Connecter**. Pour plus d'informations, reportez-vous à la section Redirection de périphérique USB.

  > **Remarque :**
  >
  > Vous pouvez afficher l'icône **Périphériques** uniquement si votre administrateur informatique fournit un accès aux périphériques USB connectés via les paramètres de stratégie.

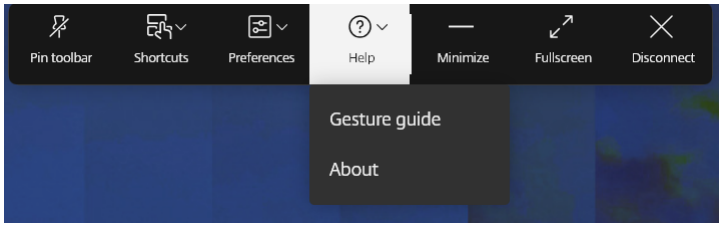
- **Préférence** : vous pouvez définir vos préférences comme suit. Les quatre options suivantes apparaissent :



  - **Mapper un lecteur** : la fonctionnalité de mappage des lecteurs clients (CDM, Client Drive Mapping) vous permet d'accéder à vos dossiers et lecteurs locaux depuis l'application Citrix Workspace. Pour plus d'informations, consultez la section Gestion des fichiers.
  - **Résolution d'affichage** : sélectionnez la taille de la résolution pour l'affichage de la session. Par défaut, la résolution de l'écran est définie sur Ajuster à l'écran.
  - **Mode tactile multipoint** : cliquez pour utiliser le mode tactile multipoint. Vous pouvez basculer entre le mode panoramique et le mode tactile multipoint. Cette option est applicable aux appareils à écran tactile. Pour de plus amples informations, consultez la section Prise en charge des appareils mobiles et à écran tactile.

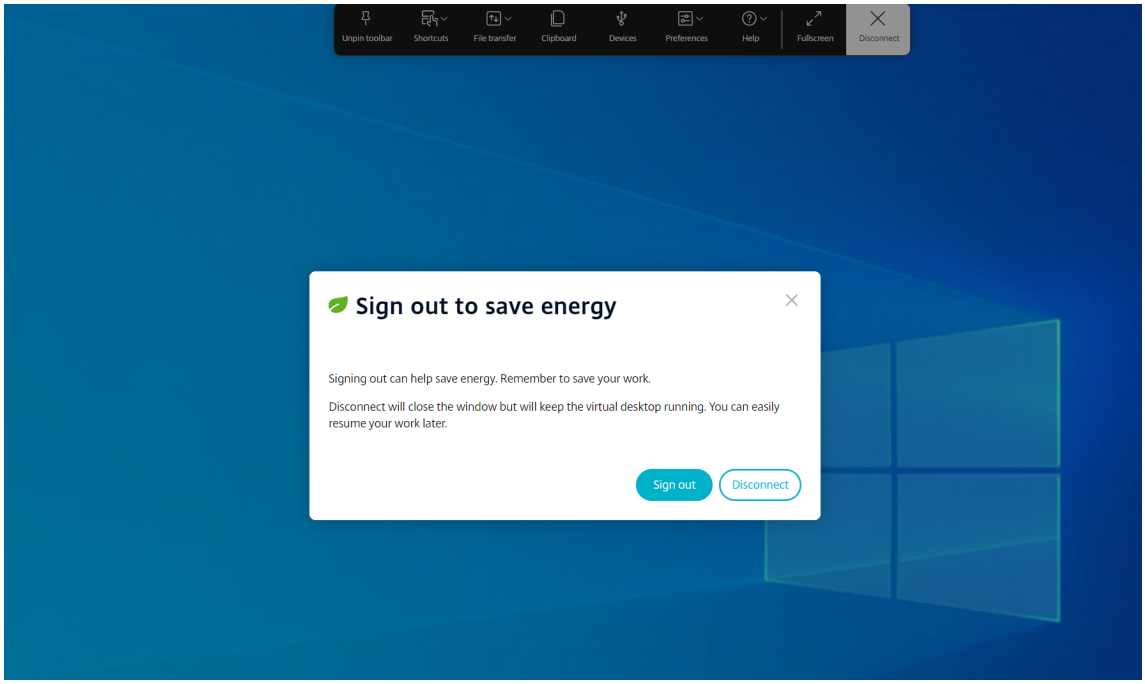
  - **Plus** : affiche les préférences relatives au bouton du clavier logiciel et au Programme d'amélioration de l'expérience utilisateur Citrix (CEIP).

- **Aide** : les trois options suivantes s'affichent :



  - **Guide de gestuelle** : un guide de gestuelle s'affiche avec des détails sur la façon d'utiliser les gestes tactiles. Cette option est applicable aux appareils à écran tactile.
  - **À propos** : affiche la version actuelle de l'application Citrix Workspace que vous utilisez.

- **Réduire** : vous pouvez réduire la fenêtre de session.
- **Plein écran** : vous pouvez passer de l'écran en mode fenêtré au mode plein écran. Si vous avez une configuration multi-écrans, le bouton plein écran étend l'écran sur l'ensemble de la configuration et fonctionne également comme un bouton multi-écrans.
- **Déconnecter** : l'action de déconnexion permet au bureau virtuel de continuer à fonctionner. Déconnexion pour économiser de l'énergie. Pour plus d'informations, consultez Initiative de développement durable pour l'application Citrix Workspace.



Transport adaptatif

Cette fonctionnalité est disponible en version Technical Preview depuis la publication de la version 2311.

À partir de la version 2311, l'application Citrix Workspace pour ChromeOS prend en charge la fonctionnalité Transport adaptatif.

Le transport adaptatif offre une expérience utilisateur supérieure sur les connexions longue distance difficiles tout en maintenant la capacité à monter en charge du serveur. Cette fonctionnalité offre une expérience HDX de haute qualité sur les plates-formes Web.

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

> **Remarques :**
>
> - Cette fonction est désactivée par défaut.
> - Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le formulaire Podio.

Configuration système requise

Les exigences suivantes sont requises pour utiliser le transport adaptatif et EDT :

- Plan de contrôle
  - Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)
  - Citrix Virtual Apps and Desktops 1912 ou versions ultérieures
- Virtual Delivery Agent
  - Version 1912 ou ultérieure (2203 ou ultérieure recommandée)
  - 2012 est la version minimale requise pour utiliser EDT avec Citrix Gateway Service
- StoreFront
  - Version 3.12.x
  - Version 1912.0.x
- Citrix Gateway (ADC)
  - 13.1.17.42 ou version ultérieure (recommandé)
  - 13.0.52.24 ou version ultérieure
  - 12.1.56.22 ou version ultérieure

- Pare-feu (du côté VDA)

  UDP 1494 entrant : si la fiabilité de session est désactivée

  UDP 2598 entrant : si la fiabilité de session est activée

  UDP 443 entrant : si vous activez le VDA SSL pour le chiffrement ICA (DTLS)

  UDP 443 sortant : si vous utilisez Citrix Gateway Service Pour plus d'informations, consultez la documentation Citrix Gateway Service.

Configurations d'administrateur

- Pour configurer le paramètre **Transport adaptatif HDX** dans la stratégie Citrix, consultez la section Configuration de la documentation Citrix Virtual Apps and Desktops.
- Vous pouvez configurer la fonctionnalité de transport adaptatif de la manière suivante :

  Stratégie d'administration Google

  Pour les appareils et les utilisateurs gérés, les administrateurs peuvent activer la fonctionnalité à l'aide de la stratégie d'administration Google comme suit :

  1. Connectez-vous à la stratégie d'administration Google.
  2. Vous pouvez appliquer cette configuration aux éléments suivants :
     - **Appareil** > **Chrome** > **Applications et extensions** > **Utilisateurs et navigateurs** > Rechercher l'extension > Règles relatives aux extensions
     - **Appareil** > **Chrome** > **Applications et extensions** > **Kiosques** > Rechercher l'extension > Règles relatives aux extensions
     - **Appareil** > **Chrome** > **Applications et extensions** > **Sessions Invité gérées** > Rechercher l'extension > Règles relatives aux extensions

  Voici un exemple de données JSON :

```
{

"settings": {

"Value": {

    "settings_version": "1.0",
            "engine_settings": {

                "features": {

                    "edt": {

                        "enabled": true
```

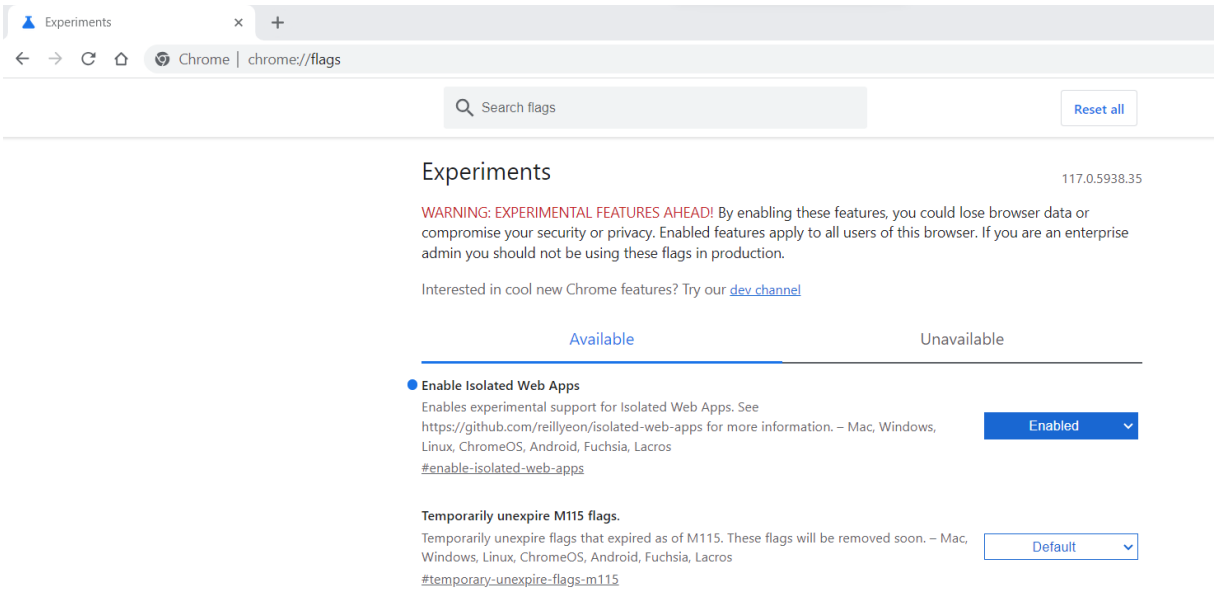


```
                                    }

                                }

                            }

                        }

                    }

    }

<!--NeedCopy-->
```

3. Enregistrez les modifications.

Configuration de l'utilisateur

Pour activer la fonctionnalité de transport adaptatif, entrez `chrome://flags` dans la barre d'adresse du navigateur Google Chrome. Activez l'option **Activer les applications Web isolées** comme indiqué dans la capture d'écran suivante :



Accessibilité et TalkBack

Cette fonctionnalité est disponible en version Technical Preview depuis la publication de la version 2307.

L'application Citrix Workspace offre une expérience utilisateur améliorée grâce à la fonctionnalité TalkBack. La fonctionnalité TalkBack aide les utilisateurs finaux qui ont des difficultés à voir l'écran.

Le narrateur lit à haute voix les éléments figurant à l'écran lors de l'utilisation de l'interface utilisateur.

Pour utiliser le narrateur ChromeOS (ChromeVox), les utilisateurs finaux doivent l'activer à l'aide du raccourci clavier Ctrl+Alt+Z. Pour désactiver le narrateur, utilisez la même combinaison de touches.

> **Remarque :**
>
> - Cette fonctionnalité est désactivée par défaut.

Configuration

Vous pouvez configurer la fonctionnalité d'accessibilité de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

Configuration.js Pour activer la fonctionnalité d'accessibilité à l'aide du fichier**configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le **dossier racine ChromeApp**.

   > **Remarques :**
   >
   > - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
   > - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
   > - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

2. Modifiez le fichier **configuration.js** et ajoutez l'attribut **accessibility**. Définissez l'attribut **enable** sur **true**.

   Voici un exemple de données JSON :

```
'features' :
{

    'accessibility': {

          'enable': true
         }
 ,
 }


```



```
<!--NeedCopy-->
```

3. Enregistrez les modifications.

Stratégie d'administration Google Pour les appareils et les utilisateurs gérés, les administrateurs peuvent activer la fonctionnalité à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils > Gestion de Chrome > Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier policy.txt sous la clé engine_settings.
   Voici un exemple de données JSON :

```
'features' :
{

    'accessibility': {

          'enable': true
         }
 ,
 }


<!--NeedCopy-->
```

4. Enregistrez les modifications.

Conditions préalables à l'installation

May 16, 2024

Configuration système requise et compatibilité

Exigences

Tous les périphériques doivent répondre à la configuration matérielle minimale requise pour le système d'exploitation installé.

Les périphériques des utilisateurs requièrent le système d'exploitation Google Chrome OS pour accéder aux bureaux et applications à l'aide de l'application Citrix Workspace. Citrix vous recommande d'utiliser la dernière application Citrix Workspace du canal Stable de Google ChromeOS.

L'application Citrix Workspace pour ChromeOS est uniquement prise en charge sur ChromeOS. L'application Citrix Workspace prend également en charge le système d'exploitation ChromeOS Flex.

Ajouter et ouvrir des applications Chrome L'application Citrix Workspace pour ChromeOS est uniquement prise en charge sur ChromeOS. Sur votre Chromebook, vous pouvez ajouter et ouvrir des applications depuis le Chrome Web Store. Pour de plus amples informations, consultez l'article de support Google.

> **Remarques :**
>
> - Les applications Chrome du Chrome Web Store ne sont prises en charge que sur les Chromebooks et ne fonctionneront pas sous Windows, Mac ou Linux après décembre 2022.
> - Les appareils Chromebook en fin de vie (EOL) ne sont pas mis à jour vers les versions plus récentes de Google ChromeOS. Les appareils EOL ne prennent pas en charge toutes les mises à jour de l'application Citrix Workspace pour ChromeOS. Nous recommandons et prenons en charge les dernières versions du système d'exploitation de Google Chrome.

Prise en charge

L'application Citrix Workspace pour ChromeOS prend en charge l'accès aux bureaux et applications via les versions suivantes de StoreFront. Les utilisateurs doivent utiliser des sites Citrix Receiver pour Web pour accéder aux magasins. L'application Citrix Workspace pour ChromeOS ne prend pas en charge l'accès direct aux magasins StoreFront, que vous utilisiez l'adresse URL du magasin ou l'adresse URL d'un site XenApp Services.

- StoreFront 2.5 et versions ultérieures

L'application Citrix Workspace pour ChromeOS peut être utilisée pour accéder aux bureaux et applications mis à disposition par les versions des produits suivants :

- XenApp et XenDesktop 7.6 et versions ultérieures

Sécurisation des connexions utilisateur

Dans un environnement de production, Citrix vous recommande de sécuriser les communications entre les sites Citrix Workspace pour Web et les machines des utilisateurs à l'aide de Citrix Gateway et du protocole HTTPS. Citrix recommande d'utiliser des certificats SSL avec une taille de clé d'au moins 1024 bits dans l'environnement dans lequel l'application Citrix Workspace pour ChromeOS est déployée. L'application Citrix Workspace pour ChromeOS permet aux utilisateurs d'accéder à des bureaux et applications à partir de réseaux publics à l'aide des versions suivantes de Citrix Gateway.

- NetScaler Gateway 10.5 et versions ultérieures

L'application Citrix Workspace pour ChromeOS prend en charge CloudBridge, ce qui permet de désactiver la compression et la compression d'imprimante, ainsi que d'utiliser les capacités d'analyse HDX Insight et les afficher dans CloudBridge Insight Center.

- CloudBridge 7.4 et versions ultérieures

> **Remarque :**
>
> Si vous ne parvenez pas à vous connecter au VDA compatible SSL avec l'application Citrix Workspace pour ChromeOS, consultez Paramètres TLS sur les VDA. Configurez la suite de chiffrement qui vous convient.

Configuration requise pour l'optimisation pour Microsoft Teams

Version minimale :

- L'optimisation de Microsoft Teams pour les appels audio, les appels vidéo et le partage d'écran est généralement disponible à partir de la version 2105.5.

  Nous vous recommandons d'utiliser la dernière version de l'application Citrix Workspace pour ChromeOS. Par défaut, le partage d'écran est désactivé. Pour activer le partage d'écran, consultez la section relative aux paramètres.

- VDA version 1906 ou ultérieure.

Matériel :

Pour une visioconférence peer-to-peer ou un partage d'écran, les exigences minimales sont les suivantes :

- un processeur Intel® Core™ i3 avec processeur quatre cœurs 2,4 GHz prenant en charge la résolution HD 720p.

Installer

May 16, 2024

Les utilisateurs et les administrateurs informatiques peuvent installer l'application Citrix Workspace pour ChromeOS.

Installation depuis le Chrome Web Store

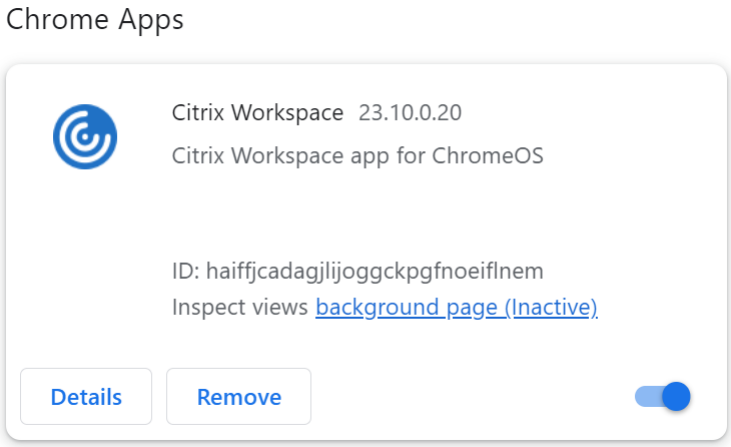
Les utilisateurs peuvent installer l'application Citrix Workspace pour ChromeOS depuis le Chrome Web Store comme suit :

1. Cliquez sur le lien https://chromewebstore.google.com/detail/citrix-workspace/haiffjcadagjlijoggckpgfnoeiflnem.

   La page du magasin en ligne de l'application Citrix Workspace pour ChromeOS s'affiche.

2. Cliquez sur **Ajouter à Chrome**.

   L'application est installée. Accédez à `chrome://extensions` dans votre navigateur Chrome pour afficher les applications Chrome.

3. Recherchez l'*application Citrix Workspace* dans le lanceur ChromeOS pour l'utiliser.

> **Remarque**
>
> Pour commencer à utiliser l'application, les utilisateurs peuvent saisir une URL de magasin valide ou une adresse e-mail. En général, un administrateur informatique vous donne l'adresse URL du magasin ou configure votre adresse e-mail avec les URL de magasin associées. Respectez les directives de votre organisation.

Installer manuellement

Il existe un certain nombre d'options permettant de déployer l'application Citrix Workspace pour ChromeOS.

- Vous pouvez utiliser la console de gestion des applications Google pour configurer Citrix Workspace à l'aide de la stratégie Google. Pour de plus amples informations sur la configuration de ChromeOS, consultez l'article CTX141844 du centre de connaissances.

- Vous pouvez reconditionner l'application Citrix Workspace pour ChromeOS afin d'inclure un fichier de configuration Citrix Workspace (.cr) que vous avez généré. Le fichier **.cr** contient les détails de connexion pour Citrix Gateway et le site Citrix Receiver pour Web qui fournit les bureaux et applications des utilisateurs. Les utilisateurs accèdent à chrome://extensions puis ils font glisser le fichier de l'application reconditionnée (.crx) sur la fenêtre Chrome pour installer l'application Citrix Workspace pour ChromeOS. L'application étant préconfigurée, les utilisateurs peuvent commencer à travailler avec l'application Citrix Workspace lorsqu'ils l'installent, sans avoir à effectuer d'étapes de configuration supplémentaires.

Les administrateurs peuvent distribuer votre application Citrix Workspace pour ChromeOS personnalisée aux utilisateurs finaux des manières suivantes :

- Publiez l'application reconditionnée auprès des utilisateurs via Google Apps for Business à l'aide de la console Google Admin Console.
- Fournissez le fichier .crx aux utilisateurs par d'autres moyens, par exemple par courrier électronique.
- Les utilisateurs peuvent installer l'application Citrix Workspace pour ChromeOS depuis le Chrome Web Store. Pour plus d'informations, consultez la section Installation depuis le Chrome Web Store.

Une fois l'installation terminée, l'application Citrix Workspace doit être configurée avec les détails de connexion de Citrix Gateway et du site Citrix Receiver pour Web qui fournit les bureaux et applications des utilisateurs. Ceci peut être réalisé de deux façons :

- Générez un fichier **.cr** contenant les détails de connexion appropriés et distribuez ce fichier aux utilisateurs. Pour configurer l'application Citrix Workspace pour ChromeOS, les utilisateurs double-cliquent sur le fichier **.cr** et cliquent sur Ajouter lorsqu'ils y sont invités. Pour plus d'informations sur la génération de fichiers .cr à partir de StoreFront, consultez la section Exporter les fichiers de provisioning de magasin auprès d'utilisateurs.
- Donnez aux utilisateurs l'adresse URL qu'ils doivent entrer manuellement lorsqu'ils démarrent l'application Citrix Workspace pour ChromeOS pour la première fois.

Reconditionner

Pour simplifier le processus de déploiement auprès des utilisateurs, vous pouvez reconditionner l'application Citrix Workspace pour ChromeOS avec un nouveau fichier **.cr** pour préconfigurer l'application Citrix Workspace pour ChromeOS avec les détails de connexion pour votre environnement. Les utilisateurs peuvent commencer à travailler avec l'application Citrix Workspace pour ChromeOS dès qu'ils l'ont installée sans avoir à effectuer d'étapes de configuration supplémentaires.

1. Téléchargez la version décompressée de l'application Citrix Workspace pour ChromeOS sur un emplacement approprié.

2. Téléchargez le fichier de configuration exemple et modifiez-le pour l'adapter à votre environnement.
3. Renommez le fichier de configuration modifié sur default.cr et copiez-le sur le répertoire racine de l'application Citrix Workspace pour ChromeOS.

   Les fichiers de configuration avec des noms différents ou dans d'autres emplacements ne sont pas inclus lorsque l'application Citrix Workspace pour ChromeOS est reconditionnée.
4. Par défaut, la barre d'outils de la session est activée. Si vous souhaitez désactiver la barre d'outils de la session, suivez les étapes suivantes.

   Remarque : nous vous recommandons de sauvegarder le fichier configuration.js avant de le modifier.

   a) Utilisez un éditeur de texte pour ouvrir le fichier configuration.js dans le répertoire racine de l'application Citrix Workspace pour Chrome.

   b) Recherchez la section suivante dans le fichier.

   ```
   pre codeblock 'appPrefs':{ 'chromeApp':{ 'ui': { 'toolbar': {
    'menubar':true, 'clipboard': false <!--NeedCopy-->
   ```

   c) Modifiez le paramètre de l'attribut menubar sur **true**.

   Remarque : pour remplacer toute configuration précédente, nous vous recommandons d'utiliser la console d'administration Google pour distribuer la stratégie.
5. Par défaut, l'application Citrix Workspace pour ChromeOS peut ouvrir n'importe quelle extension de fichier à l'aide de l'application Fichiers d'un Chromebook. Vous pouvez utiliser le Chromebook destiné à ouvrir des fichiers dans Google Drive à l'aide du composant FileAccess du VDA.

   Si un administrateur souhaite désactiver cette option pour télécharger la version décompressée de l'application Citrix Workspace, la section « file handlers » du fichier manifest.json doit être modifiée comme suit :

```
"file handlers" : {

        "text" :
            "extensions" :  [
                 "ica",
                  "cr"
              ]
           }

    }

<!--NeedCopy-->
```


6. Dans Chrome, accédez à chrome://extensions, sélectionnez la case à cocher **Mode Développeur** située dans la partie supérieure droite de la page et cliquez sur le bouton **Empaqueter l'extension**.

   Pour des raisons de sécurité, StoreFront n'accepte que les connexions provenant d'instances de l'application Citrix Workspace pour ChromeOS. Vous devez placer votre application reconditionnée sur liste verte pour autoriser les utilisateurs à se connecter à un site Citrix Receiver pour Web.

7. Sur le serveur StoreFront, utilisez un éditeur de texte pour ouvrir le fichier web.config du site Citrix Receiver pour Web, qui se trouve dans le répertoire **C:\inetpub\wwwroot\Citrix\storename**. Le *nom du magasin* est le nom qui est spécifié pour le magasin lors de sa création.

8. Recherchez les éléments suivants dans le fichier.

   ```
   pre codeblock <html5 ... chromeAppOrigins="chrome-extension://
   haiffjcadagjlijoggckpgfnoeiflnem"... /> <!--NeedCopy-->
   ```

9. Modifiez la valeur de l'attribut **chromeAppOrigins** sur chrome-extension:*//packageid* où **packageid** est l'ID généré pour votre application reconditionnée.

Versions de sauvegarde et d'accès anticipé (EAR)

Une option permet aux utilisateurs d'utiliser les versions de sauvegarde et d'accès anticipé de l'application Citrix Workspace pour ChromeOS. L'option de sauvegarde assure la continuité de l'activité en cas de problèmes dans la version de production. Avant de poursuivre, familiarisez-vous avec les ID de version suivants :

- `haiffjcadagjlijoggckpgfnoeiflnem` : ID de la version publiée de l'application Citrix Workspace pour ChromeOS sur le Chrome Web Store.
- `lbfgjakkeeccemhonnolnmglmfmccaag` : ID de la version Early Access Release (EAR) de l'application Citrix Workspace pour ChromeOS.
- `anjihnbmjbbpofafpmklejenkgnjfcdi` : ID de la version de sauvegarde de l'application Citrix Workspace pour ChromeOS. La version de sauvegarde contient le contenu de la version antérieure à la version de production actuelle avec un ID de version différent.

Pour accéder à la version de sauvegarde

Pour accéder à la version de sauvegarde, procédez comme suit :

1. Cliquez sur le lien https://chrome.google.com/webstore/detail/citrix-workspace-backup/anjihnbmjbbpofafpmklejenkgnjfcdi.

   La page de l'extension de la sauvegarde de l'application Citrix Workspace s'affiche.

2. Cliquez sur **Ajouter à Chrome**.

   L'application est installée. Accédez à `chrome://extensions` dans votre navigateur Chrome pour afficher l'extension.

3. Recherchez l'application Citrix Workspace dans le lanceur ChromeOS pour l'utiliser.

Pour accéder à la version EAR

Pour accéder à la version EAR, procédez comme suit :

1. Cliquez sur le lien https://chrome.google.com/webstore/detail/citrix-workspace-backup/lbfgjakkeeccemhonnolnmglmfmccaag.

   La page de l'extension de l'application Citrix Workspace pour ChromeOS s'affiche.

2. Cliquez sur **Ajouter à Chrome**.

   L'application est installée. Accédez à `chrome://extensions` dans votre navigateur Chrome pour afficher l'extension.

3. Recherchez l'application Citrix Workspace dans le lanceur ChromeOS pour l'utiliser.

Compatibilité avec ChromeOS LTS

Google offre une version LTS (Support à long terme) de ChromeOS si vous préférez moins de mises à jour. À tout moment, une ou plusieurs versions de l'application Citrix Workspace sont compatibles avec la dernière version de ChromeOS LTS.

Si vous recherchez une version de l'application Citrix Workspace dotée des dernières corrections de bogues et des nouvelles fonctionnalités, nous vous invitons à suivre les recommandations ci-dessous :

- Utiliser la dernière version de l'application Citrix Workspace
- Utiliser la dernière version de Google ChromeOS sur le canal stable

Rétrocompatibilité

Les corrections de bogues sur ChromeOS ou l'application Citrix Workspace peuvent ne pas être rétrocompatibles avec la version ChromeOS LTS. Pour bénéficier de la rétrocompatibilité, vous devrez peut-être passer au canal stable de ChromeOS.

Les nouvelles fonctionnalités proposées par Citrix ou Google peuvent dépendre des versions logicielles les plus récentes. Pour accéder aux nouvelles fonctionnalités, utilisez le canal stable pour ChromeOS et la dernière version de l'application Citrix Workspace.

Exclusions

Les fonctionnalités suivantes ne sont pas compatibles avec ChromeOS LTS :

- Optimisation pour Microsoft Teams
- Redirection du contenu du navigateur

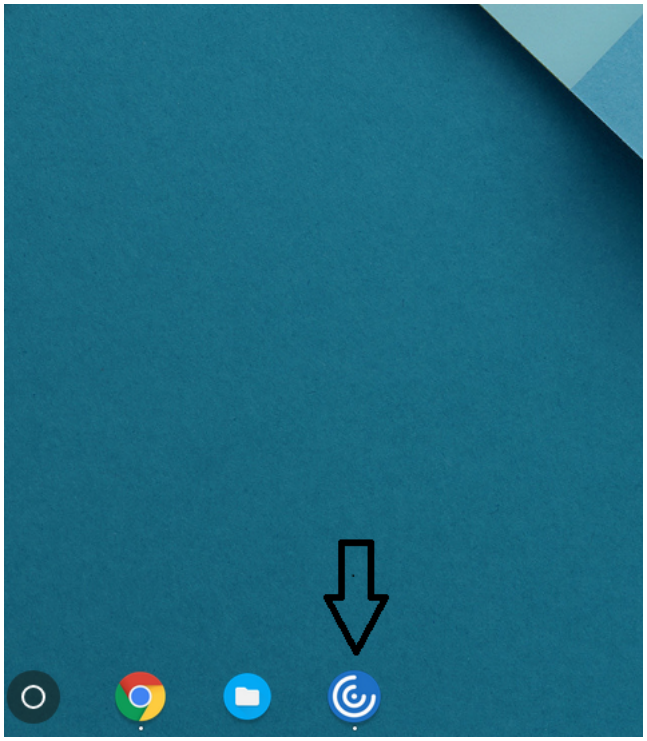
Les mises à jour des fonctionnalités exclues sont disponibles sur la dernière version de ChromeOS sur le canal stable, ainsi que sur la dernière version de l'application Citrix Workspace.

Questions courantes

- Comment savoir quelle version de l'application Citrix Workspace est compatible avec la dernière version de ChromeOS LTS ?
  - Vous trouverez la dernière version sur la page À propos de cette version.
  - Le fichier installable de la dernière version est disponible sur la page Citrix Downloads.
- En tant qu'administrateur, comment puis-je effectuer des tests sur le canal ChromeOS LTS ?
  - Pour plus d'informations, consultez les versions Support à long terme (LTS) sur la page Education de Google ChromeOS.
- En tant qu'administrateur, que dois-je faire si je rencontre un problème sur ChromeOS LTS avec l'application Citrix Workspace ?
  - Vérifiez si vous observez le même problème avec la dernière version de ChromeOS sur le canal stable et la dernière version de l'application Citrix Workspace. Si c'est le cas, signalez le problème via vos canaux de support habituels. Si ce n'est pas le cas, mettez à jour vers la version dans laquelle vous n'avez pas rencontré le problème.

Désinstaller

Après avoir installé et configuré l'application Citrix Workspace, sélectionnez l'icône Citrix Workspace dans la liste des applications Chrome. L'application Citrix Workspace pour ChromeOS démarre comme indiqué dans l'image suivante. Pour supprimer l'application Citrix Workspace pour ChromeOS de vos appareils, cliquez avec le bouton droit sur l'icône de Citrix Workspace dans la liste des applications Chrome et sélectionnez **Désinstaller**.



Mettre à niveau

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

- Téléchargez l'application Citrix Workspace à partir de la page des téléchargements de Citrix et installez l'application pour mettre à niveau Citrix Receiver vers l'application Citrix Workspace.
- Mettez à niveau votre application Citrix Workspace à l'aide du App Store de votre OS.
- Sous Windows et macOS, mettez automatiquement à jour l'application Citrix Workspace à partir de Citrix Receiver à l'aide des mises à jour de Citrix Receiver.

Pour accéder à la documentation de Citrix Receiver pour Chrome, consultez Citrix Receiver.

Prise en main

May 16, 2024

Configurer

Les applications et bureaux s'affichent après l'ouverture de session. Vous pouvez rechercher des ressources et cliquer sur une icône pour démarrer un bureau ou une application dans une nouvelle fenêtre.

Lorsque vous démarrez une application supplémentaire, l'application Citrix Workspace pour ChromeOS vérifie si l'application peut être lancée dans une session existante avant de créer une session. Cela vous permet d'accéder à plusieurs applications dans une seule session.

Vous pouvez configurer les fonctionnalités de l'application Citrix Workspace pour ChromeOS à l'aide de l'une des méthodes suivantes :

- Stratégie d'administration Google
- web.config dans StoreFront
- default.ica
- configuration.js

> **Remarque :**
>
> À partir de la version 1901, l'écran de démarrage n'est plus visible pour les utilisateurs. Le schéma **"splashScreen": false** ne sera plus pris en charge dans les futures versions. Vous devez supprimer le schéma, s'il est présent, de la stratégie d'administration Google ou du fichier configuration.js.

Utilisation de la stratégie d'administration Google

> **Remarque :**
>
> Citrix recommande d'utiliser cette méthode uniquement lorsque l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.

Préalablement à la version 2.1, seules les configurations liées au magasin ou à la balise peuvent être transmises via la stratégie d'administration Google. Pour de plus amples informations sur cette stratégie, consultez les articles CTX141844 et CTX229141 du centre de connaissances.

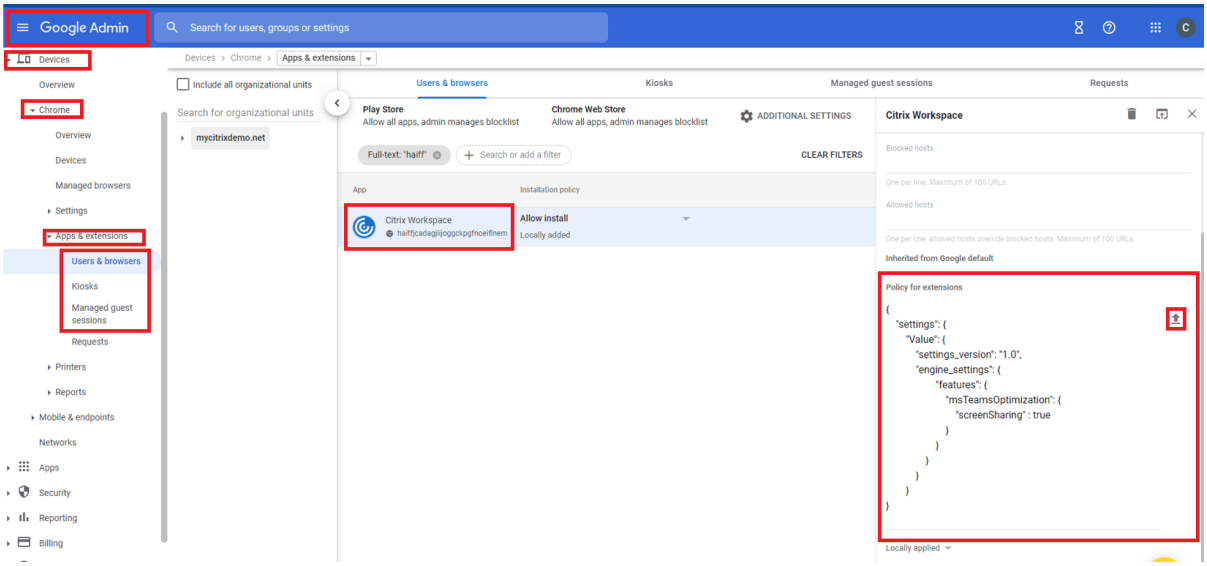
Avec la version 2.1 de l'application Citrix Workspace pour ChromeOS, d'autres configurations Chrome peuvent également être transmises via la stratégie d'administration Google.

Comment distribuer des stratégies via la console d'administration Google

Pour transmettre une stratégie via la console d'administration Google, procédez comme suit :

1. Dans la console **d'administration Google**, sélectionnez **Appareils > Chrome > Applications et extensions > Utilisateurs et navigateurs**.

2. Recherchez l'application Citrix Workspace (entrez l'ID de l'application du magasin Web, par exemple `haiffjcadagjlijoggckpgfnoeiflnem`).
3. Cliquez sur l'icône de l'application Citrix Workspace.
4. La page Règles relatives aux extensions s'affiche. Copiez et collez la stratégie ou chargez le fichier policy.txt avec le fichier JSON correspondant.
5. Cliquez sur **Enregistrer**.
6. Répétez les étapes pour **Kiosque** et **Sessions Invité gérées** selon vos besoins.



Pour plus d'informations, consultez le support de Google.

Vérification de la configuration des stratégies

Pour vérifier que les stratégies sont correctement transmises, procédez comme suit :

1. Accédez à `chrome://policy/`.
2. Cliquez sur `Reload policies`.
3. Recherchez l'ID du magasin Web de l'application Citrix Workspace pour ChromeOS, qui est `haiffjcadagjlijoggckpgfnoeiflnem`.
    - Si les stratégies sont transmises avec succès à partir de la console d'administration Google, elles apparaissent sous l'ID du magasin en ligne : `haiffjcadagjlijoggckpgfnoeiflnem` . Si ce n'est pas le cas, vérifiez que les stratégies sont correctement configurées. Pour créer ou modifier la stratégie, assurez-vous d'utiliser le `Configuration Utility Tool`.
    - Si les stratégies apparaissent sous l'ID du magasin Web mais ne prennent pas effet dans la session, contactez le support technique Citrix.

Utilisation du fichier web.config

> **Remarque :**
>
> Citrix vous recommande d'utiliser le fichier **web.config** à des fins de configuration uniquement lorsqu'une version de l'application Citrix Workspace pour ChromeOS provenant du magasin d'applications est utilisée.

Pour modifier la configuration à l'aide de la méthode du fichier web.config (uniquement pour ceux utilisant des instances StoreFront locales) :

1. Ouvrez le fichier **web.config** du site Citrix Receiver pour Web. Ce fichier figure dans **C:\inetpub\wwwroot\Citrix\<nomdumagasinWeb>**, où *nomdumagasin* est le nom spécifié pour le magasin lors de sa création.
2. Localisez le champ **chromeAppPreferences** et définissez sa valeur en tant que chaîne JSON.

Par exemple :

```
chromeAppPreferences = {

    "ui": {

        "toolbar": {

            "menubar": false
             }

             }

             }

<!--NeedCopy-->
```

Un autre exemple est le suivant :

Utilisation du fichier default.ica

> **Remarque :**
>
> Citrix vous recommande d'utiliser le fichier **default.ica** à des fins de configuration uniquement pour les utilisateurs de l'Interface Web.

L'application Citrix Workspace pour ChromeOS autorise les fichiers Custom.ica sans aucune valeur de programme initial.

Pour changer la configuration à l'aide du fichier **default.ica** :

1. Ouvrez le fichier default.ica qui se trouve sur **C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica**po les clients Interface Web, où **site name** est le nom spécifié pour le site lors de sa création.
   Pour les clients StoreFront, le fichier **default.ica** figure dans **C:\inetpub\wwwroot\Citrix\\\<nom du magasin\>\App_Data\default.ica**, où **nom du magasin** est le nom spécifié pour le magasin lors de sa création.
2. Ajoutez une clé à la fin du fichier, **chromeAppPreferences** en définissant sa valeur en tant qu'objet JSON.

Par exemple :

```
chromeAppPreferences={

    "ui":{

        "toolbar": {

```



```
            "menubar": false
             }

             }

             }

<!--NeedCopy-->
```

Exemple de fichier **default.ica** :

web.config default.ica

```
[Application]
TransportDriver=TCP/IP
DoNotUseDefaultCSL=On
BrowserProtocol=HTTPonTCP
LocHttpBrowserAddress=!
WinStationDriver=ICA 3.0
ProxyTimeout=30000
AutologonAllowed=ON
TWIMode=Off
FontSmoothingType=0

[EncRC5-0]
DriverNameWin16=pdc0w.dll
DriverNameWin32=pdc0n.dll

[EncRC5-40]
DriverNameWin16=pdc40w.dll
DriverNameWin32=pdc40n.dll

[EncRC5-56]
DriverNameWin16=pdc56w.dll
DriverNameWin32=pdc56n.dll

[EncRC5-128]
DriverNameWin16=pdc128w.dll
DriverNameWin32=pdc128n.dll

[Compress]
DriverNameWin16=pdcompw.dll
DriverNameWin32=pdcompn.dll

chromeAppPreferences = '{"ui":{"toolbar":{"menubar":false,"displayResolution":false}}}'
```

En utilisant le fichier configuration.js

Le fichier **configuration.js** se trouve dans le dossier racine **ChromeApp**. Accédez directement à ce fichier pour modifier l'application Citrix Workspace pour ChromeOS.

> **Remarque :**
>
> - Citrix vous recommande de sauvegarder le fichier configuration.js avant de le modifier.
> - Des informations d'identification de niveau administrateur sont nécessaires pour modifier le fichier configuration.js ; après la modification du fichier, reconditionnez l'application

> pour apporter des modifications supplémentaires aux éléments de la barre d'outils.
> - En mode Kiosque, la barre d'outils est masquée par défaut. Lors de la modification du fichier configuration.js pour activer la barre d'outils, assurez-vous que le mode Kiosque est désactivé. Citrix vous recommande d'utiliser l'une des méthodes alternatives (par exemple, le fichier default.ica) pour activer la barre d'outils.

Branding personnalisé du logo et des icônes

Vous pouvez personnaliser le logo de l'application Citrix Workspace et les icônes des applications et des bureaux comme vous le souhaitez. Vous pouvez les personnaliser comme suit :

1. Installez l'application Citrix Workspace pour ChromeOS depuis le Chrome Web Store.
2. Accédez au dossier **/chromeAppUI/resources/images**.
3. Remplacez les images suivantes par les images de votre choix, mais avec les mêmes dimensions :
   - icon_16x16.png
   - icon_32x32.png
   - icon_48x48.png
   - icon_128x128.png
   - icon_256x256.png
4. Accédez au dossier **racine Applications Chrome** et ouvrez le fichier **manifest.json**.
5. Remplacez la valeur du nom et de la description par le texte requis.
6. Enregistrez les modifications.
7. Rechargez l'application depuis la page des extensions.

Configurer

May 16, 2024

Gestion des feature flag

Si un problème survient avec l'application Citrix Workspace en production, nous pouvons désactiver dynamiquement une fonctionnalité affectée dans l'application Citrix Workspace même après la livraison de la fonctionnalité. Pour ce faire, nous utilisons des commutateurs de fonctionnalité et un service tiers appelé LaunchDarkly.

Comment configurer

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

Vous pouvez activer le trafic et la communication vers LaunchDarkly des manières suivantes :

Activer le trafic vers les URL suivantes

- events.launchdarkly.com
- app.launchdarkly.com

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

Disposition pour désactiver le service LaunchDarkly Vous pouvez désactiver le service LaunchDarkly sur les magasins sur site et dans le cloud.

Dans la configuration cloud, les administrateurs peuvent désactiver le service LaunchDarkly en définissant l'attribut **enableLaunchDarkly** sur **False** dans Global App Configuration Service.

Pour plus d'informations, consultez la documentation Global App Configuration Service.

Avec le déploiement sur site, les administrateurs peuvent désactiver le service LaunchDarkly à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la console d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé **engine_settings**.

```
"thirdPartyServices": {


  "enableLaunchDarkly": false

 }
 ,

<!--NeedCopy-->
```


4. Cliquez sur **Enregistrer**.

> **Remarque :**
>
> - Par défaut, le service LaunchDarkly est activé si l'attribut **enableLaunchDarkly** n'est pas présent.

Avec le déploiement sur site, les administrateurs peuvent désactiver le service LaunchDarkly à l'aide du fichier configuration.js comme suit :

> **Remarque :**
>
> - Des informations d'identification de niveau administrateur sont nécessaires pour modifier le fichier configuration.js ; après la modification du fichier, reconditionnez l'application pour que les modifications prennent effet.

1. Ouvrez le fichier **configuration.js**.
2. Ajoutez l'attribut **enableLaunchDarkly** et définissez-le sur **false**.

```
"thirdPartyServices": {


    "enableLaunchDarkly": false

      }
 ,
<!--NeedCopy-->
```

3. Cliquez sur **Enregistrer**.

> **Remarque :**
>
> - Par défaut, le service LaunchDarkly est activé si l'attribut **enableLaunchDarkly** n'est pas présent.

Remarque sur le fichier JSON de configuration

Avec la version 2202.1 (22.2.1.8), l'application Citrix Workspace utilise uniquement le fichier JSON valide pour transmettre la configuration. Procédez comme suit pour valider le fichier JSON :

1. Vérifiez les données JSON. Cliquez sur le lien https://jsonlint.com/ pour vérifier.
2. Suivez les étapes mentionnées dans la page Get started pour effectuer la mise à jour :
   - Stratégie Google
   - web.config
   - default.ica

- configuration.js

Nous vous recommandons d'utiliser l'utilitaire de configuration pour générer des paramètres JSON valides afin de personnaliser l'application Citrix Workspace pour ChromeOS à l'aide de ce qui suit :

- configuration.js
- web.config
- default.ica
- Stratégie Google

> **Remarque** :
>
> Vous pouvez rencontrer des problèmes de lancement de session lorsque le fichier JSON de configuration n'est pas valide.

Paramètre de proxy HTTP sur Chromebook

Si vous avez configuré le paramètre de proxy HTTP sur votre Chromebook, il est possible que vos sessions ne démarrent pas.

Pour résoudre le problème, vous pouvez désactiver le paramètre **nativeSocket** sur la console d'administration Google et vous assurer que vous avez activé la stratégie **connexions WebSockets** dans DDC. Pour plus d'informations, veuillez consulter l'article WebSocket.

Voici un exemple de données JSON :

```
{

        "settings": {

        "Value": {

              "settings_version": "1.0",
              "engine_settings": {

                          "transport":
                                 {
  "nativeSocket": false
                                     }

                               }

                        }

           }

 }

```



```
<!--NeedCopy-->
```

> **Avertissement :**
>
> La désactivation de l'attribut **nativeSocket** active la connexion WebSocket, ce qui peut affecter les performances par rapport à l'utilisation d'un socket natif.

Mode kiosque

Le mode kiosque de l'application Citrix Workspace pour ChromeOS vous permet d'exécuter toutes les applications dans la même fenêtre. Grâce à cette fonctionnalité, vous pouvez exécuter des applications Citrix Workspace en mode Kiosque, puis lancer des applications ou bureaux Windows à l'aide du même mode. En outre, le mode Kiosque vous permet de publier des applications ou bureaux distants en tant que package Chrome dédié à l'aide d'une l'URL persistante.

Comment configurer

Vous pouvez contrôler cette fonctionnalité en ajustant les paramètres du kiosque dans le panneau d'administration de Chrome. Ce paramètre s'applique uniquement aux appareils Chrome gérés.

Référez-vous aux instructions du site de support de Google pour savoir comment autoriser l'application Citrix Workspace à s'exécuter en mode Kiosque sur les appareils Chrome gérés et non gérés.

Si vous déployez une application Citrix Workspace, vous devez la publier en définissant les options de visibilité sur `Public`/`unlisted` pour vérifier l'interopérabilité avec le mode Kiosque. Accédez au Tableau de bord du développeur Chrome Web Store.

L'URL du magasin est en lecture seule lorsque le mode Kiosque est actif, et elle ne peut pas être modifiée à l'aide de l'écran des paramètres du **compte**. Vous pouvez toutefois modifier ce paramètre :

- en reconditionnant l'application avec le fichier `.cr`, ou
- en utilisant la console d'administration Google. Utilisez la gestion des stratégies Google pour accéder à la console d'administration Google.

```
    <Services version="1.0">
    <Service>
    <rfWeb>http://your_RfWebURL_or_persistenturl</rfWeb>
    <Name>Mystore</Name>
    <Gateways>
    <Gateway>
    <Location>https://yourcompany.gateway.com</Location>
    </Gateway>
    </Gateways>
    <Beacons>
    <Internal>
    <Beacon>http://yourcompany.internalwebsite.net</Beacon>
```



```
    </Internal>
    <External>
    <Beacon>http://www.yourcompany.externalwebsite.com</Beacon>
    </External>
    </Beacons>
    </Service>
    </Services>

<!--NeedCopy-->
```

Si vous utilisez la console d'administration Google, modifiez le fichier **policy.txt** contenant la configuration de Citrix Workspace. Remplacez la valeur « url » sous « rf_web » avec une URL persistante.

```
    {

    "settings": {

    "Value": {

    "settings_version": "1.0",
    "store_settings": {

    "beacons": {

    "external": [
    {

    "url": "http://www.yourcompany.externalwebsite.com"
     }

    ],
    "internal": [
    {

    "url": "http://yourcompany.internalwebsite.net"
     }

    ]
     }
 ,
    "gateways": [
    {

    "is_default": true,
    "url": "https://yourcompany.gateway.com"
     }

    ],
    "name": "mystore",
    "rf_web": {

    "url": " http://your_RfWebURL_or_persistenturl "
     }
```



```
41
42          }
43
44          }
45
46          }
47
48          }
49
50  <!--NeedCopy-->
```

Global App Configuration Service

À partir de cette version, en tant qu'administrateur, vous pouvez utiliser Global App Configuration Service pour :

- gérer et configurer de manière centralisée les paramètres des applications et définir les valeurs par défaut ;
- appliquer les paramètres pour les appareils gérés et non gérés (BYOD) ;
- appliquer les paramètres à la fois pour les utilisateurs cloud (domaine revendiqué) et pour les utilisateurs locaux (URL revendiquée).

Pour plus d'informations, consultez la documentation Global App Configuration Service.

> **Remarques :**
>
> Cette fonctionnalité est uniquement disponible pour Workspace et les magasins HTTPS.
> Pour que Global App Configuration Service fonctionne, assurez-vous que vos utilisateurs peuvent accéder aux URL `https://discovery.cem.cloud.us`, `https://gacs-discovery.cloud.com` et `https://gacs-config.cloud.com`.

CEIP (programme d'amélioration de l'expérience du client)

May 16, 2024

Comment configurer

Données collectées	Description	Quel usage faisons-nous de ces données
Données de configuration et d'utilisation	Le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) rassemble des données de configuration et d'utilisation à partir de l'application Citrix Workspace et les envoie automatiquement à Citrix et Google Analytics.	Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de l'application Citrix Workspace.

Informations supplémentaires

Citrix traite vos données conformément aux termes de votre contrat. Citrix protège vos données comme indiqué dans l'Annexe sur la sécurité des Services Citrix sur Citrix Trust Center.

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

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

Données CEIP pour Citrix et Google Analytics

À partir de la version 2203, les utilisateurs peuvent :

- décider d'envoyer ou non les données d'utilisation à Citrix et Google Analytics ;
- bloquer le programme CEIP via l'interface graphique.

Désactivation du programme CEIP

Vous pouvez désactiver l'envoi de données via le programme CEIP à Citrix et Google Analytics. Pour ce faire, utilisez l'une des méthodes suivantes :

- Désactiver le programme CEIP à l'aide d'une stratégie d'administration Google
- Désactiver le programme CEIP à l'aide du fichier configuration.js

> **Remarque :**
>
> Lorsque vous désactivez le programme CEIP pour la version 2203 et versions ultérieures, des informations minimales contenant la version installée de l'application Citrix Workspace sont chargées. Ces informations aussi succinctes qu'elles soient sont utiles à Citrix car elles permettent de connaître la répartition des différentes versions utilisées par les clients.

Pour désactiver le programme CEIP à l'aide d'une stratégie d'administration Google

> **Remarque :**
>
> Des informations d'identification de niveau administrateur sont nécessaires pour effectuer cette procédure.

1. Connectez-vous à la console d'administration Google.
2. Accédez à **Gestion des appareils > Gestion de Chrome > Paramètres utilisateur**.
3. Ajoutez les chaînes affichées après l'étape 4 au fichier policy.txt sous la clé **engine_settings**.
4. Cliquez sur **Enregistrer**.

Pour obtenir davantage d'informations sur la stratégie Google, veuillez consulter l'article CTX141844 du centre de connaissances.

Pour les versions 1907 et antérieures, définissez l'attribut enabled sous **ceip** sur **false**.

```
"ceip":{

    "enabled":false,
 }

<!--NeedCopy-->
```

Pour les versions 1908 et ultérieures, définissez l'attribut enabled sous **analytics** sur **false**. Cependant, la clé **analytics** est rétrocompatible avec la clé **ceip**.

```
"analytics":{

    "enabled":false,
 }

<!--NeedCopy-->
```

Pour désactiver le programme CEIP à l'aide du fichier configuration.js

Le fichier **configuration.js** se trouve dans le dossier racine **ChromeApp**. Modifiez ce fichier pour configurer l'application Citrix Workspace pour ChromeOS.


```
> **Notes:**
>
> -  Citrix recommends that you back up the **configuration.js** file before making changes.
> -  Citrix recommends editing the **configuration.js** file, only if the Citrix Workspace app for ChromeOS is repackaged for users.
> -  Administrator-level credentials are required to edit the **configuration.js** file.
```

Pour les versions 1907 et antérieures, définissez l'attribut enabled sous **ceip** sur **false** dans le fichier **configuration.js**.

```
"ceip":{

    "enabled":false,
 }

<!--NeedCopy-->
```

Pour les versions 1908 et ultérieures, définissez l'attribut enabled sous **analytics** sur **false** dans le fichier **configuration.js**.

```
"analytics":{

    "enabled":false,
 }


<!--NeedCopy-->
```

Blocage de CEIP

Pour les versions 2007 et ultérieures, les administrateurs sont autorisés à bloquer CEIP via le fichier configuration.js et la stratégie d'administration Google.

Pour les versions 2203 et ultérieures, les utilisateurs sont autorisés à bloquer le programme CEIP via l'interface graphique.

Cette configuration a priorité sur la configuration effectuée via l'interface utilisateur graphique et la stratégie d'administration Google, et les données CEIP ne sont pas envoyées à Citrix.

Pour bloquer le programme CEIP à l'aide d'une stratégie d'administration Google

> **Remarque :**

> Des informations d'identification de niveau administrateur sont nécessaires pour effectuer cette procédure.

1. Connectez-vous à la console d'administration Google.
2. Accédez à **Gestion des appareils > Gestion de Chrome > Paramètres utilisateur**.
3. Ajoutez les chaînes affichées après l'étape 4 au fichier policy.txt sous la clé **engine_settings**.
4. Cliquez sur **Enregistrer**.

```
"analytics":{

    "connectionEnabled":false,
                  }

<!--NeedCopy-->
```

Pour bloquer le programme CEIP à l'aide du fichier configuration.js

1. Ouvrez le fichier configuration.js.
2. Ajoutez l'attribut **connectionEnabled** et définissez l'attribut sur **false** :

```
"analytics":{

"connectionEnabled":false,
              }


<!--NeedCopy-->
```

Pour bloquer le programme CEIP à l'aide de l'interface graphique

> **Remarque :**
>
> Seul l'utilisateur peut modifier les paramètres du programme CEIP à l'aide de l'interface graphique.

1. Lancez l'application Citrix Workspace pour ChromeOS.
2. Sélectionnez **Paramètres > Généraux**.
3. Décochez la case **Aidez-nous à améliorer Citrix Workspace en envoyant des statistiques d'utilisation anonymes**.

Redémarrez l'application Citrix Workspace pour que les modifications prennent effet.

Données CEIP spécifiques

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

Version de l'application Citrix Workspace	Mode de session (kiosque, public/général)	Type de session (bureau/application)	Informations sur XenDesktop (versions du Delivery Controller et du VDA)
Type de lancement (SDK/ICAFile/FTA/Store, etc.)	Fuseau horaire de la session	Langue de la session	Disposition du clavier client
Type de socket réseau (HTTPS/HTTP)	Utilisation des fonctionnalités (presse-papiers, transfert de fichiers, commutateur d'applications, impression, USB, carte à puce, etc.)	Ratio de pixels de l'appareil	Secure ICA (utilisé/non utilisé)
ID d'actif des Chromebooks d'entreprise inscrits	Délai d'expiration de la reconnexion (si ! = 180)	Multimoniteur	Global App Configuration Service

Presse-papiers

May 16, 2024

Prise en charge de la copie de clips d'image

À l'aide des raccourcis clavier standard, vous pouvez copier et coller des clips d'image entre votre appareil local et vos sessions d'applications et de bureaux virtuels. Vous pouvez utiliser les raccourcis clavier standard pour copier et coller. Par exemple, vous pouvez utiliser des applications telles que Microsoft Word, Microsoft Paint et Adobe Photoshop. Auparavant, cette fonctionnalité n'était disponible que pour le texte.

> **Remarque :**
>
> - En raison de contraintes de bande passante réseau, les sessions peuvent ne plus répondre lorsque vous tentez de copier et de coller un clip d'image de plus de 2 Mo.

- Vous pouvez sélectionner et appuyer sur Ctrl + C et Ctrl + V pour copier et coller. La fonctionnalité de clic droit pour copier ou coller est également prise en charge.
- Nous avons testé cette fonctionnalité avec les formats BMP, PNG, JPEG et GIF.

Configuration du Presse-papiers

Vous pouvez copier du contenu HTML et préserver le formatage lors de la copie d'un lien dans Chrome. Une balise <img> est ajoutée au format HTML, ce qui vous permet de copier des images et du texte. Cette fonctionnalité est plus riche que le texte brut.

Pour activer cette fonctionnalité, ajoutez l'entrée de registre suivante au VDA :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\Virtual Clipboard\Additional Formats\HTML Format
"**Nom"="HTML Format**"

> **Avertissement**
>
> Une utilisation incorrecte de l'Éditeur du Registre peut occasionner de sérieux problèmes qui pourraient nécessiter l'installation du système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à effectuer une copie de sauvegarde avant de modifier le registre.

La fonction Presse-papiers a résolu de nombreux problèmes. Pour plus d'informations, consultez l'article CTX086028 du centre de connaissances.

Prise en charge du format de données HTML

À compter de la version 2207, vous pouvez utiliser le format HTML pour les opérations sur le presse-papiers entre le bureau virtuel et le terminal. Lorsque vous copiez et collez les données HTML, le format du contenu source est copié. Lorsque vous collez les données, le contenu de destination est également mis en forme. Le format HTML offre également une meilleure apparence.

Pour plus d'informations sur la façon de définir les stratégies, consultez Formats d'écriture autorisés dans le Presse-papiers client dans la documentation de Citrix Virtual Apps and Desktops.

Le presse-papiers prend en charge le format HTML

Vous pouvez utiliser le format HTML pour les opérations sur le presse-papiers entre le bureau virtuel et le terminal. Lorsque vous copiez les données HTML, le format du contenu source est copié, et lorsque

vous collez les données, le contenu de destination prend en charge la mise en forme. Le format HTML offre également une meilleure apparence.

Pour plus d'informations sur la façon de définir les stratégies, consultez Formats d'écriture autorisés dans le Presse-papiers client dans la documentation de Citrix Virtual Apps and Desktops.

Gestion des fichiers

May 16, 2024

Transfert de fichiers

L'application Citrix Workspace pour ChromeOS permet de transférer des fichiers en toute sécurité entre un appareil utilisateur et une session. La session peut être du type Citrix Virtual Apps and Desktops ou une session Citrix DaaS. Cette fonctionnalité utilise un canal virtuel de transfert de fichiers au lieu d'un mappage de lecteur client.

Les utilisateurs peuvent par défaut :

- Charger des fichiers depuis un dossier de téléchargement local ou un périphérique connecté.
- Accéder en toute facilité aux données depuis leurs sessions Citrix Virtual Apps and Desktops et Citrix DaaS.
- Télécharger des fichiers depuis leurs sessions Citrix Virtual Apps and Desktops et Citrix DaaS.
- Vous pouvez télécharger des fichiers dans un dossier local ou un périphérique sur leur appareil utilisateur.

Les administrateurs peuvent configurer le transfert de fichiers, les chargements et téléchargements dans Citrix Studio à l'aide de stratégies.

> **Logiciels requis**

- XenApp ou XenDesktop 7.6 ou version supérieure, avec :
  - Correction ICATS760WX64022.msp sur des VDA avec OS serveur (Windows 2008 R2 ou Windows 2012 R2)
  - Correction ICAWS760WX86022.msp ou ICAWS760WX64022.msp sur des VDA avec OS client (Windows 7 ou Windows 8.1)
- Pour modifier les stratégies de transfert de fichier : correction de gestion des stratégies de groupe GPMx240WX64002.msi ou GPMx240WX86002.msi sur les machines exécutant Citrix Studio.

Limitations des fonctionnalités :

- Un utilisateur peut charger ou télécharger un maximum de 10 fichiers simultanément.
- Taille de fichier maximale :
  - Pour les chargements : 2147483647 octets (2 Go)
  - Pour les téléchargements : 262144000 octets (250 Mo)
- Si l'une des stratégies **Charger des fichiers sur le bureau** ou **Télécharger des fichiers depuis le bureau** est définie sur **Désactivé**, la barre d'outils affiche toujours les icônes de chargement et de téléchargement. Toutefois, la fonctionnalité est basée sur le paramètre de stratégie. Si les deux stratégies sont définies sur **Désactivé**, les icônes de chargement et de téléchargement ne sont pas affichées dans la barre d'outils.

Configurer des stratégies de transfert de fichiers

Pour configurer le transfert de fichiers à l'aide d'une stratégie Citrix Studio

Par défaut, le transfert de fichiers est activé.

Utilisez Citrix Studio pour modifier les stratégies suivantes. Elles se trouvent sous **Paramètres** utilisateur > **ICA** > **Redirection de fichier**.

Stratégie Citrix Studio	Description
Autoriser le transfert de fichiers entre le bureau et le client	Pour activer ou désactiver la fonction de transfert de fichiers
Charger des fichiers sur le bureau	Pour activer ou désactiver le chargement de fichiers dans la session. Requiert que la stratégie « Autoriser le transfert de fichiers entre le bureau et le client » soit définie sur true.
Télécharger des fichiers depuis le bureau	Pour activer ou désactiver le téléchargement de fichiers depuis la session. Requiert que la stratégie « Autoriser le transfert de fichiers entre le bureau et le client » soit définie sur true.

Pour configurer le transfert de fichiers à l'aide du fichier configuration.js

Le fichier **configuration.js** se trouve dans le dossier racine **ChromeApp**. Modifiez ce fichier directement pour modifier l'application Citrix Workspace en fonction de vos besoins.

Remarques :

- Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
- Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
- Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**. Après avoir modifié le fichier, reconditionnez l'application pour apporter d'autres modifications aux éléments de la barre d'outils.

Pour masquer la configuration du transfert de fichiers à l'aide du fichier configuration.js

Ouvrez le fichier **configuration.js** et configurez les paramètres comme ci-dessous :

Paramètres de transfert de fichiers sur le client	Description
AllowUpload	Pour activer ou désactiver le chargement du côté client. Paramètre défini par défaut sur true (activé).
AllowDownload	Pour activer ou désactiver le téléchargement du côté client. Paramètre défini par défaut sur true (activé).
MaxUploadSize	Pour définir la taille maximale en octets du fichier qui peut être chargé. La valeur par défaut est 2 147 483 648 octets (2 Go).
MaxDownloadSize	Pour définir la taille maximale en octets du fichier qui peut être téléchargé. La valeur par défaut est 2147483648 octets (2 Go).

Voici les cas comportements disponibles lorsque les stratégies définies dans Citrix Studio et le client sont différentes.

Stratégie Citrix Studio Chargement/téléchargement	Paramètre côté client Chargement/téléchargement	Comportement
DÉSACTIVÉ	ACTIVÉ	DÉSACTIVÉ
DÉSACTIVÉ	DÉSACTIVÉ	DÉSACTIVÉ
ACTIVÉ	DÉSACTIVÉ	DÉSACTIVÉ
ACTIVÉ	ACTIVÉ	ACTIVÉ

> **Remarque :**
>
> Lorsqu'une valeur de **taille maximale de chargement ou téléchargement** différente est définie dans le Registre et les paramètres côté client, la valeur de taille minimum est appliquée aux deux emplacements.

Pour configurer le transfert de fichiers à l'aide de la stratégie d'administration Google

Par défaut, la fonctionnalité de transfert de fichiers est activée.

Pour la désactiver, définissez l'attribut « enabled » sur « false ».

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "ui": {

                        "features": {

                           "filetransfer" : {

                                   "allowupload": true,
                                   "allowdownload": true,
                                   "maxuploadsize": 2147483647,
                                   "maxdownloadsize": 2147483647
                            }

                        }

                    }

                }

         }

     }

 }


<!--NeedCopy-->
```

Liste des paramètres de transfert de fichiers ainsi que leurs descriptions :

- `allowupload` : vous permet de charger des fichiers depuis l'appareil vers une session à dis-

tance.

- `allowdownload` : vous permet de télécharger des fichiers depuis un appareil vers une session à distance.
- `maxuploadsize` : taille maximale du fichier, en octets, qui peut être chargé. La valeur par défaut est 2 147 483 648 octets (2 Go).
- `maxdownloadsize` : taille maximale du fichier, en octets, qui peut être téléchargé. La valeur par défaut est 2 147 483 648 octets (2 Go).

Mappage des lecteurs clients

À partir de la version 2307, la fonctionnalité de mappage des lecteurs clients (CDM) prend en charge le mappage de dossiers sur l'appareil ChromeOS pour les rendre accessibles dans une session. Vous pouvez mapper un dossier de l'appareil ChromeOS (par ex. des dossiers Téléchargements, Google Drive, ou de lecteurs USB) s'il ne contient aucun fichier système.

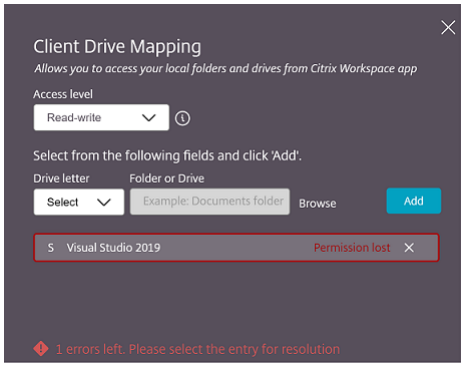
L'utilisateur peut effectuer les opérations suivantes :

- Copiez les fichiers et les dossiers sur le lecteur mappé à partir de la session et inversement.
- Afficher la liste des fichiers et des dossiers du lecteur mappé.
- Ouvrez, lisez et modifiez le contenu des fichiers sur le lecteur mappé.
- Afficher les propriétés du fichier (heure de modification et taille de fichier uniquement) sur le lecteur mappé.

Cette fonctionnalité offre l'avantage d'accéder à la fois aux lecteurs de bureaux virtuels et aux lecteurs de machines locales dans l'explorateur de fichiers au sein de la session HDX.

Limitations connues

- Vous ne pouvez pas renommer les fichiers et dossiers à l'intérieur du lecteur mappé.
- Les mappages portent uniquement le nom du dossier (non le chemin complet).
- Si votre dossier local contient des fichiers cachés et que vous avez mappé le même dossier, les fichiers cachés sont visibles dans la session sur le lecteur mappé.
- Vous ne pouvez pas modifier la propriété du fichier pour qu'elle soit accessible en lecture seule sur le lecteur mappé.
- CDM n'est pas pris en charge si les sessions sont ouvertes en mode intégré à l'aide du SDK HDX.
- Lorsque vous mappez un dossier à partir d'un périphérique amovible et que vous le supprimez pendant une session active, vous ne pouvez pas utiliser ce lecteur mappé dans cette session. Cliquez sur le **X** près des mappages que vous voulez supprimer manuellement.



Configurer le CDM

Vous pouvez configurer cette fonctionnalité CDM de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

> **Remarque :**
>
> - Comme condition préalable, un administrateur doit activer la stratégie **Redirection de lecteur client** sur le Delivery Controller (DDC). Pour de plus amples informations, consultez Redirection de lecteur client dans la documentation de Citrix Virtual Apps and Desktops.

Configuration.js

Pour désactiver la prise en charge CDM à l'aide du fichier **configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le **dossier racine ChromeApp**.
2. Modifiez ce fichier pour configurer la fonctionnalité CDM.

   > **Remarques :**
   >
   > - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
   > - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
   > - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

3. Définissez la valeur **clientDriveMapping** sur **false**.

   Voici un exemple de données JSON :


```
'features': {

    'clientDriveMapping': {

       'enabled': false,
       'availableAccessLevels': ["Read-write","Read-only,No-access
          "],
       'accessLevel': "Read-write"
     }

 }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Stratégie d'administration Google

Pour les appareils et les utilisateurs gérés, les administrateurs peuvent désactiver la fonctionnalité CDM à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous **engine_settings**.

   > **Remarque :**
   >
   > Vous pouvez également appliquer cette configuration aux éléments suivants :
   >
   > - **Appareil** > **Chrome** > **Applications et extensions** > **Kiosques** > Rechercher l'extension > Règles relatives aux extensions
   > - **Appareil** > **Chrome** > **Applications et extensions** > **Sessions Invité gérées** > Rechercher l'extension > Règles relatives aux extensions

   Voici un exemple de données JSON :

```
{

"settings": {

    "Value": {

        "settings_version": "2.0",
        "engine_settings": {

            "features": {

```



```
                "clientDriveMapping": {

                "availableAccessLevels": ["Read-write", "Read-only
                   ","No-access"],
                "accessLevel": "Read-write"
                                }

                          }

                     }

                 }

            }

 }

<!--NeedCopy-->
```

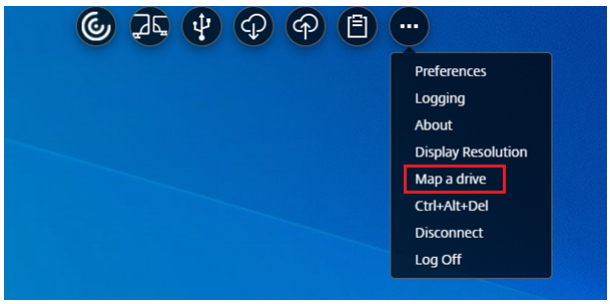
4. Enregistrez les modifications.

Niveau d'accès Si la fonctionnalité est activée, vous pouvez définir les niveaux d'accès aux dossiers ou aux lecteurs. Par exemple, si un administrateur définit **availableAccessLevels** sur [**« Aucun accès », « Lecture seule »**], les options **Accès en lecture seule** et **Aucun accès** peuvent s'afficher dans la liste déroulante pour l'utilisateur final.

Comment utiliser la fonctionnalité CDM

Sessions de bureau :

1. Accédez à la **barre d'outils** > **(...)** > **Mapper un lecteur**.

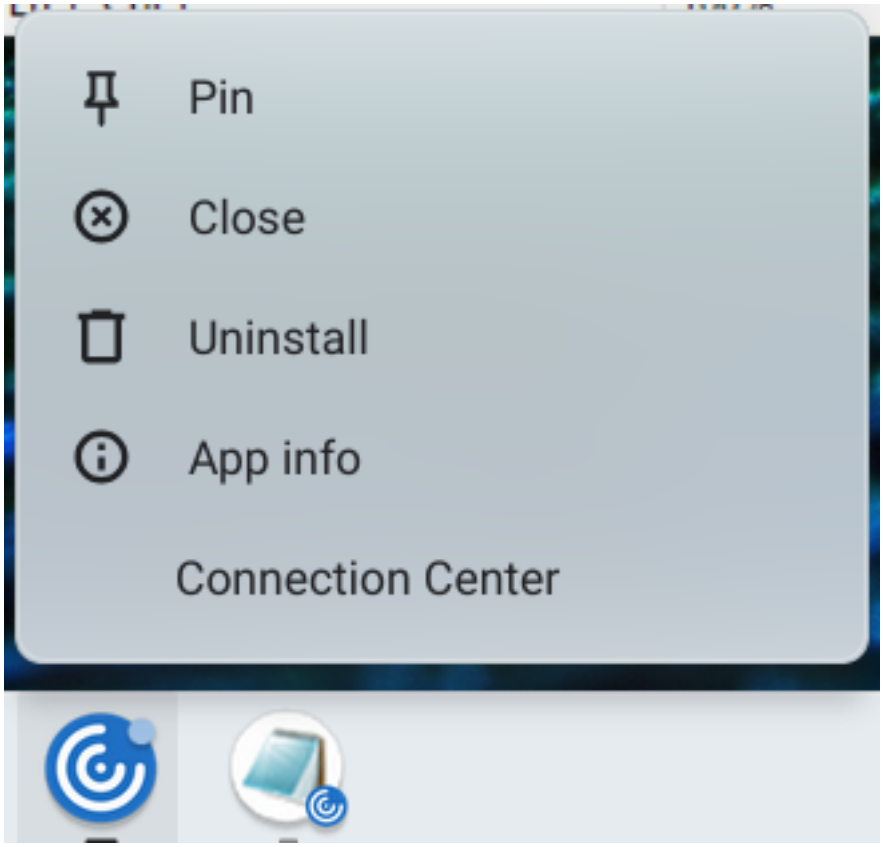


   La boîte de dialogue CDM s'affiche.

2. Pour connaître les étapes suivantes, consultez la section Utilisation de l'interface utilisateur CDM.

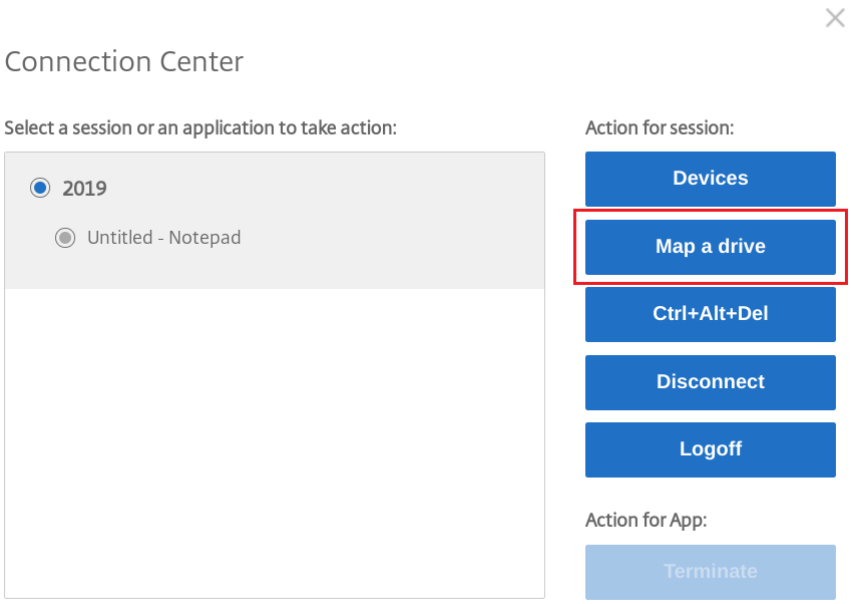
Sessions d'application et de bureau :

1. Dans l'étagère Chrome, cliquez avec le bouton droit sur l'icône de l'application Citrix Workspace et sélectionnez **Centre de connexion**



L'écran **Centre de connexion** s'affiche.

2. Sélectionnez la session et l'application, puis cliquez sur **Mapper un lecteur**.

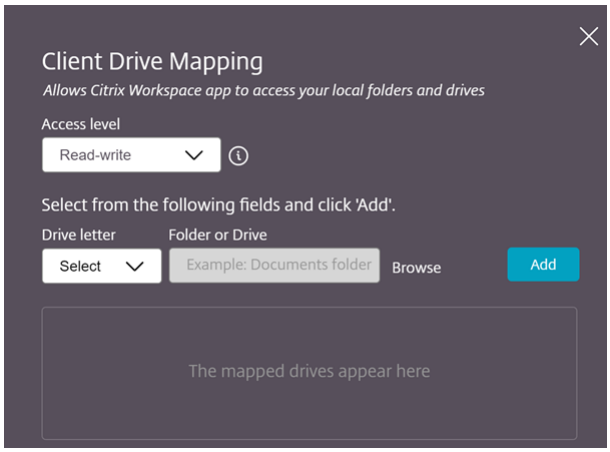


La boîte de dialogue CDM s'affiche.

3. Pour connaître les étapes suivantes, consultez la section Utilisation de l'interface utilisateur CDM.

Utilisation de l'interface utilisateur CDM

1. Sélectionnez le **niveau d'accès** pour le dossier ou le lecteur. L'option de la liste déroulante qui s'affiche dépend du niveau d'accès défini par l'administrateur informatique de votre organisation pour votre profil.



2. Sélectionnez une **lettre de lecteur** et cliquez sur **Parcourir** pour accéder à votre dossier ou lecteur sur votre Chromebook.
3. Cliquez sur **Ajouter**.
4. Déconnectez et reconnectez la session.

   La session affiche la lettre du lecteur mappée au sein de la session.

Association de type de fichier

May 16, 2024

Accès à Google Drive

Grâce à la prise en charge de Google Drive, les utilisateurs peuvent ouvrir des types de fichiers Windows, les modifier et les enregistrer à partir d'un appareil Chrome exécutant Citrix Workspace. Lorsque vous utilisez un appareil Google Chrome, vos utilisateurs peuvent utiliser des applications

Windows (par exemple, Microsoft Word) et accéder aux fichiers résidant sur Google Drive sans aucun problème.

Si un utilisateur ouvre un fichier dans Google Drive, le modifie et l'enregistre dans Drive, le même fichier est accessible via l'application hébergée Citrix Virtual Apps. Il peut s'agir, par exemple, d'une pièce jointe `.docx` téléchargée depuis Gmail. Le fichier peut être consulté, modifié et enregistré sur Google Drive.

Comment configurer

Logiciels requis

Pour autoriser l'accès à Google Drive, vous devez installer le composant Citrix File Access (FileAccess.exe) sur votre VDA et activer les associations de type de fichier dans Citrix Studio. Vous pouvez télécharger Citrix File Access depuis la page de téléchargement de Citrix.

Pour activer l'accès à Google Drive depuis l'application Citrix Workspace

1. Installez `FileAccess.exe` sur chaque VDA Citrix Virtual Apps, Citrix Virtual Apps and Desktops ou Citrix DaaS.
2. Configurez les associations de type de fichiers (FTA) appropriées pour les applications publiées dans Citrix Studio.
3. Activez les cookies et approuvez les sites `https://accounts.google.com` et <`https://ssl.gstatic.com`>. Vous pouvez le faire sur un VDA Citrix Virtual Apps, Citrix Virtual Apps and Desktops ou Citrix DaaS.

Seuls les fichiers provenant de Google Drive peuvent être ouverts à l'aide de l'application Citrix Workspace. Pour ouvrir un fichier provenant de Google Drive, cliquez avec le bouton droit sur le fichier et ouvrez-le avec Citrix Workspace.

Citrix recommande de n'associer qu'un seul type de fichier à une application publiée.

Prise en charge des connexions proxy

L'application Citrix Workspace pour ChromeOS prend en charge l'ouverture de documents à partir de Google Drive à l'aide d'applications publiées via les serveurs proxy non authentifiés.

Pour configurer :

Pour activer la connexion par proxy, configurez le paramètre proxy dans les options Internet.

Pour désactiver l'accès à Google Drive depuis Citrix Workspace

Dans le fichier manifest.json, remplacez :

```
"file_handlers" : {

      "all-file-types" : {

         "extensions" : [
            "*"
         ]
       }

    }
 ,
<!--NeedCopy-->
```

par :

```
    "file_handlers" : {

          "cr-file-type" : {

             "extensions" : [
                "cr",
               "ica"
             ]
           }

        }
 ,
<!--NeedCopy-->
```

Graphiques

June 18, 2024

Graphiques et H.264

Comment configurer

Pour configurer les graphiques et la prise en charge du protocole H.264, utilisez la stratégie d'administration Google en incluant les éléments suivants. Par défaut, la prise en charge du protocole H.264 est activée. Pour la désactiver, définissez l'attribut « enabled » sur « false ».


```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "ui": {

                       "features": {

                           "graphics": {

                               "jpegSupport": true,
                               "h264Support" : {

                                    "enabled": true,
                                    "losslessOverlays": true,
                                    "dirtyRegions": true,
                                    "yuv444Support": false
                                }

                            }

                        }

                    }

                }

        }

    }


<!--NeedCopy-->
```

Liste des options graphiques ainsi que leurs descriptions :

- « jpegSupport » : fonctionnalité JPEG dans les graphiques Thinwire.
- « h264Support » : prise en charge du protocole H.264.
- « enabled » : capacité de prise en charge H.264 dans Thinwire.
- « losslessOverlays » : capacité de superposition sans perte dans Thinwire.
- « dirtyRegions » : capacité de « régions sales » dans Thinwire.
- « yuv444Support » : capacité de prise en charge Yuv444 dans Thinwire.

> **Remarque :**
>
> Nous recommandons de définir le **Mode graphique d'ancienne génération** sur **Désactivé**.

Limitations de la fonctionnalité

- L'application Citrix Workspace pour ChromeOS ne prend pas en charge le mode graphique H.264 plein écran avec plusieurs moniteurs.
- Lorsque vous démarrez une session de bureau et que vous ouvrez une application pour saisir du texte, le texte entré disparaît, puis réapparaît. Vous pouvez remarquer que le texte scintille. Le problème se produit lorsque vous utilisez le mode H.264 en plein écran.
- Dans une configuration multi-écrans, lorsque vous ouvrez une application publiée, un écran vide apparaît à la place de l'écran de l'application. Le problème se produit lorsque vous utilisez le mode H.264 en plein écran.

Selective H.264

Comment configurer

Configuration de l'utilisation sélective de H.264 dans StoreFront à l'aide du fichier web.config
Pour modifier la configuration de l'utilisation sélective de H.264 à l'aide du fichier web.config :

1. Ouvrez le fichier web.config du site Web Citrix Receiver.
   Ce fichier figure dans le dossier C:\inetpub\wwwroot\Citrix\<Nom du magasin>Web, où *Nom du magasin* est le nom spécifié pour le magasin lors de sa création.
2. Localisez le champ **chromeAppPreferences** et définissez sa valeur en tant que chaîne JSON ; par exemple :
   chromeAppPreferences='{"graphics":{"selectiveH264":false}}

Configuration de l'utilisation sélective de H.264 à l'aide du fichier configuration.js Le fichier **configuration.js** se trouve dans le dossier racine **ChromeApp**. Modifiez ce fichier pour modifier l'application Citrix Workspace en fonction de vos besoins.

L'utilisation sélective de H.264 est définie sur true par défaut.

Pour désactiver la configuration de l'utilisation sélective de H.264 à l'aide du fichier configuration.js :

1. Ouvrez le fichier configuration.js et définissez l'attribut selectiveH264 sur **false**.


```
'graphics': {
        'selectiveH264': false
}
```

> **Remarques :**
>
> - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
> - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
> - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

Autre (H.264)

Comment configurer

Pour configurer H.264, utilisez la stratégie d'administration Google en incluant les éléments suivants : Par défaut, l'option sous l'**autre** section est désactivée. Pour l'activer, définissez l'attribut « disabled » sous « h264nonworker » sur « true ».

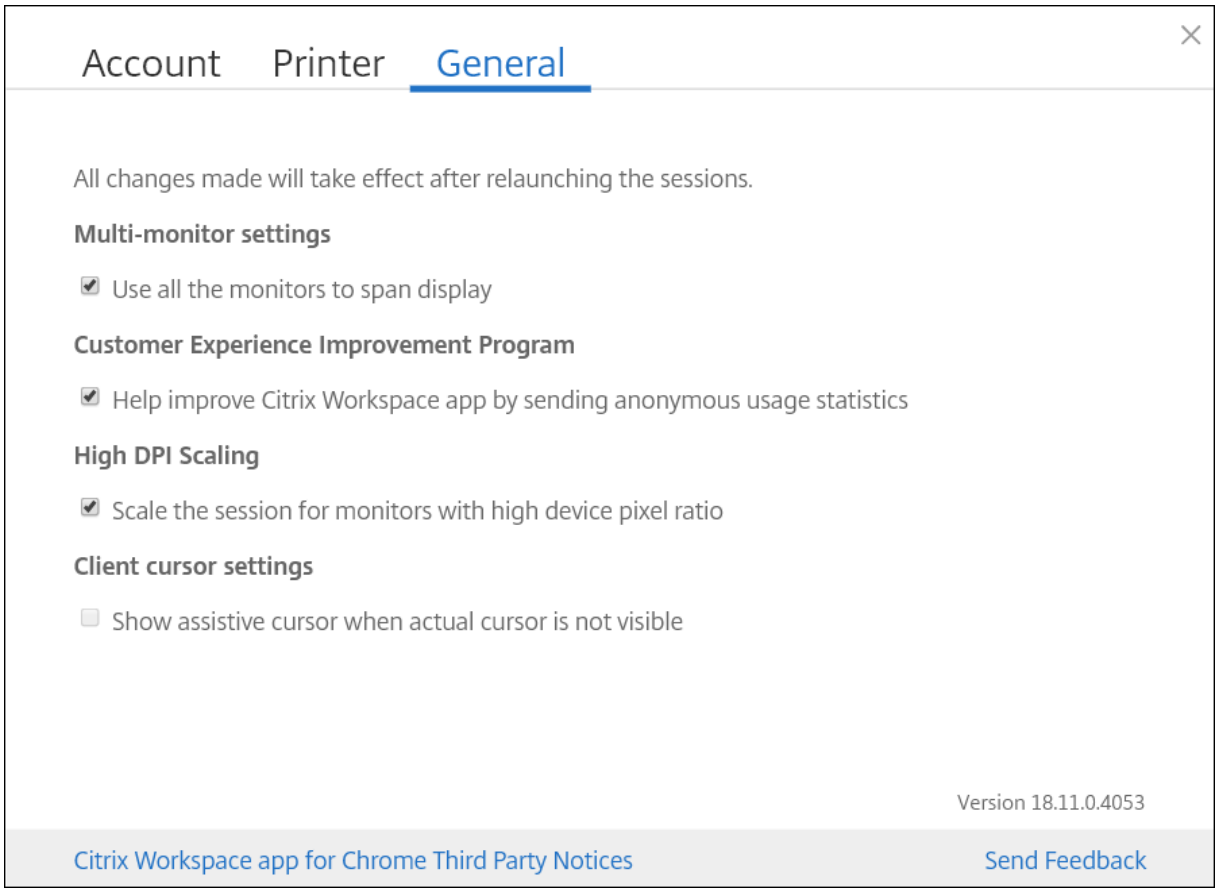
```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "other": {

                        "h264nonworker" : false
                         }

                 }

          }

     }

 }


<!--NeedCopy-->
```


Liste des options ainsi que leurs descriptions :

- « h264nonworker » : activez l'option pour décoder la trame H.264 dans le thread principal.

Curseur d'assistance

Lorsqu'aucun curseur n'est visible dans une session de bureau, vous pouvez activer un curseur d'assistance. Nécessite un redémarrage de session.



Comment configurer

La fonctionnalité de curseur d'assistance est désactivée par défaut. Pour activer la fonction de curseur d'assistance, utilisez la stratégie d'administration Google en incluant les éléments suivants.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
```



```
8               "engine_settings": {
9
10                  "ui": {
11
12                      "assistiveCursor": true
13                       }
14
15                   }
16
17                }
18
19            }
20
21    }
22
23
24  <!--NeedCopy-->
```

Remarque :

- Si un administrateur active le curseur d'assistance comme décrit ci-dessus, la case à cocher correspondante est sélectionnée par défaut dans les paramètres côté client. Pour désactiver la fonctionnalité, décochez la case.
- Si un administrateur désactive le curseur d'assistance comme décrit ci-dessus, la case à cocher est désélectionnée et la fonctionnalité désactivée.

Mise à l'échelle DPI

À propos de cette fonctionnalité

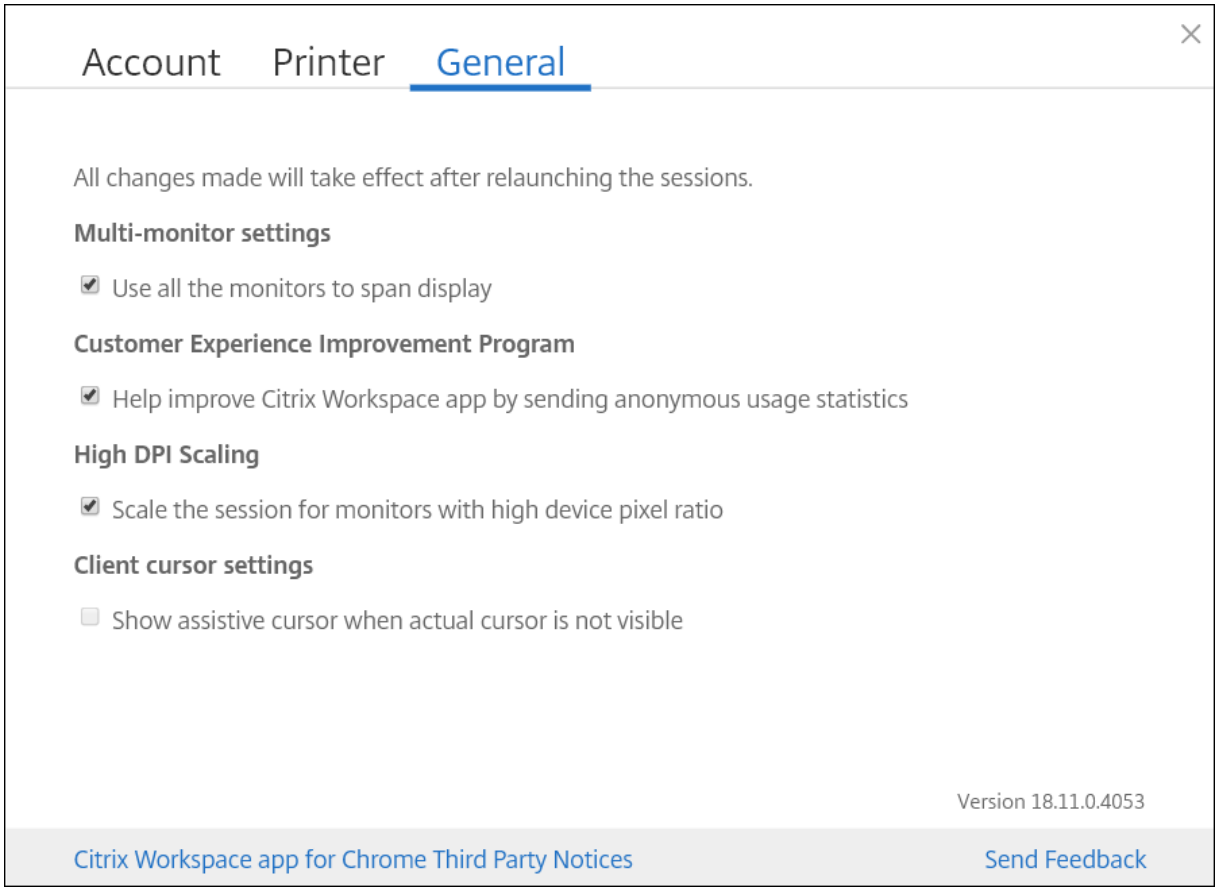
L'application Citrix Workspace pour ChromeOS permet au système d'exploitation de contrôler la résolution des sessions d'application et de bureau et prend en charge la mise à l'échelle DPI du client pour les sessions d'application sur un seul moniteur.

L'application Citrix Workspace pour ChromeOS prend en charge la mise à l'échelle DPI en vous permettant de définir la résolution du VDA sur les moniteurs présentant un ratio de pixels élevé.

La fonctionnalité **Mise à l'échelle DPI haute résolution** est désactivée par défaut pour les sessions d'application et de bureau. Pour une meilleure résolution sur les appareils à haute résolution, accédez à **Paramètres** et activez la case à cocher **Mise à l'échelle DPI haute résolution**.

Comment configurer

Vous pouvez configurer le paramètre **Mise à l'échelle DPI haute résolution** uniquement à l'aide de la stratégie d'administration Google.



La fonction de mise à l'échelle DPI **Mettre à l'échelle la session des moniteurs dont le ratio de pixels est élevé** est activée par défaut.

Pour définir la résolution des sessions de bureau, accédez à la barre d'outils de session. Sélectionnez **Préférences** > **Résolution d'affichage** > **Utiliser le ratio de pixels de l'appareil** pour définir la résolution correcte sur le VDA. Lorsque la résolution est correctement définie sur le VDA, le texte flou devient plus net.

Pour activer ou désactiver la fonctionnalité, modifiez la stratégie **Console d'administration Google** et définissez la valeur de **scaleToDPI** sur **true** ou **false**.

Par exemple, pour désactiver la fonction, définissez la propriété **scaleToDPI** sur **false**.

```
{

    "settings": {

                "Value": {

                        "settings_version": "1.0",
                              "engine_settings": {

       "features" : {

```



```
        "graphics" : {

                "dpiSetting": {

                                    "scaleToDPI": false
                                     }

                                }

                            }

                        }

                    }

                }

            }


<!--NeedCopy-->
```

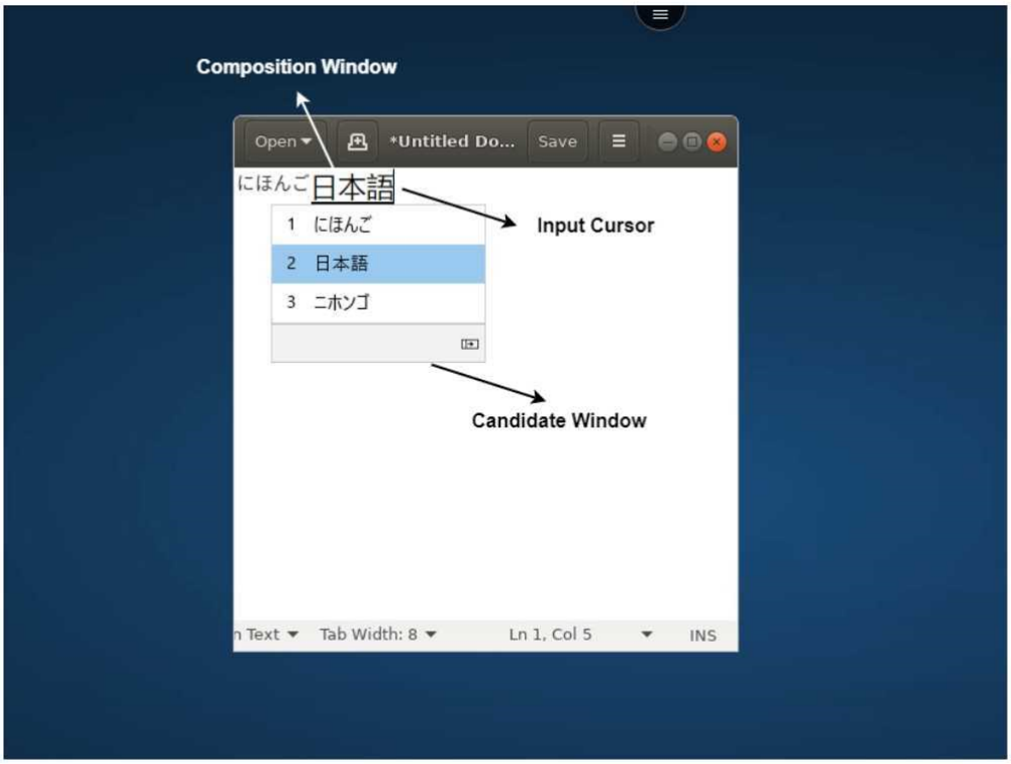
Clavier

May 16, 2024

Éditeur IME client générique pour les langues d'Asie orientale

La fonctionnalité d'éditeur IME client générique (IME) améliore l'expérience de saisie et d'affichage des caractères chinois, japonais et coréen (CJK). Cette fonctionnalité vous permet de composer des caractères CJK à la position du curseur lorsque vous êtes dans une session. La fonctionnalité est disponible pour les environnements VDA Windows et VDA Linux.

En général, l'éditeur IME affiche des composants d'interface utilisateur tels que la fenêtre candidate et la fenêtre de composition. La fenêtre de composition contient les caractères de composition et les éléments d'interface utilisateur de composition. Par exemple, soulignement et couleur d'arrière-plan. La fenêtre candidate affiche la liste des candidats.



La fenêtre de composition permet de choisir entre les caractères confirmés et les caractères de composition. La fenêtre de composition et la fenêtre candidate se déplacent avec le curseur de saisie. Par conséquent, la fonction fournit une saisie améliorée des caractères à l'emplacement du curseur dans la fenêtre de composition. De plus, elle améliore l'affichage dans la fenêtre de composition et la fenêtre candidate.

Pré-requis :

- Pour Linux VDA, activez la stratégie **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME**.
- Pour les VDA Windows, activez les stratégies **Mappage de disposition du clavier Unicode**, **Synchronisation de la disposition du clavier client** et **Améliorations apportées à l'éditeur IME**.
- Utilisez Citrix Linux VDA version 2012 et ultérieure. Pour les VDA Citrix Windows, toutes les versions de VDA Windows actuellement disponibles prennent en charge la fonctionnalité d'éditeur IME client générique (IME).
- La langue du navigateur doit être en japonais, chinois (simplifié), chinois (traditionnel) ou coréen.
- Utilisez Google Chrome ou Mozilla Firefox.

Limitations des fonctionnalités :

- La composition des caractères échoue dans la cellule Microsoft Excel. Le problème se produit lorsque la cellule est sélectionnée à l'aide d'un clic de souris. [RFHTMCRM-6086]

- L'IME client générique est désormais pris en charge lorsque vous utilisez un écran étendu. Toutefois, pour les sessions multi-écrans qui ne sont pas encore prises en charge, vous pouvez utiliser l'**éditeur IME du serveur** à la place.

  Pour activer l'**éditeur IME du serveur** :

  1. Changez la langue du VDA ou du clavier du serveur en chinois, japonais ou coréen (CJK) selon vos besoins.
  2. Redéfinissez la langue du clavier Chromebook sur Anglais.

Problème connu dans cette fonctionnalité :

- Lorsque Citrix IME n'est pas ajouté à la session de bureau d'un VDA, vous ne pourrez peut-être pas saisir les caractères IME. Le problème se produit par intermittence sur les versions 2202 et antérieures du VDA. [HDX-36748]

Configuration :

À partir de la version 2209, la fonctionnalité IME client générique est activée par défaut.

En tant qu'administrateur, vous pouvez désactiver la fonctionnalité à l'aide du fichier **configuration.js** sur le serveur StoreFront (ProgramFiles%\Citrix\Receiver StoreFront\HTML5Client). Pour désactiver la fonctionnalité, accédez à **appPrefs** > **chromeApp** > **feature** > **ime** > définissez **genericIME** sur **false**.

Par exemple,

```
    "appPrefs":{

        "chromeApp":{

            "features" : {

                    "ime" : {

                    "genericIME": false
                }

       }

     }

     }

<!--NeedCopy-->
```

- En tant qu'administrateur, vous pouvez désactiver cette fonctionnalité à l'aide de la console Google Admin Policy en définissant **genericIME** sur **false**.
  Par exemple,


```
    {

    "settings": {

    "Value": {

      "settings_version": "1.0",
      "engine_settings": {

        "features": {

          "ime": {

            "genericIME": false
           }

         }

       }

      }

 }

<!--NeedCopy-->
```

Raccourcis

Vous pouvez utiliser les raccourcis Windows standard pour copier des données, notamment du texte, des tableaux et des images, entre applications hébergées. Les applications hébergées peuvent être :

- dans la même session
- au sein de différentes sessions

Seul du texte brut Unicode peut être copié et collé entre des applications hébergées et le Presse-papiers local de la machine.

Les utilisateurs peuvent utiliser les raccourcis clavier Windows standard avec l'application Citrix Workspace pour ChromeOS, car ces raccourcis sont transmis depuis les applications hébergées de ChromeOS. De même, les raccourcis spécifiques à certaines applications peuvent également être utilisés, à condition qu'ils n'entrent pas en conflit avec des raccourcis de ChromeOS.

Toutefois, vous devez également appuyer sur la touche **Windows** pour que les touches de fonction soient reconnues. Un clavier externe est donc nécessaire. Pour de plus amples informations sur l'utilisation de claviers Windows avec le système d'exploitation ChromeOS, veuillez consulter https:

//support.google.com/chromebook/answer/1047364. Les raccourcis propres à Citrix, tels que ceux permettant de basculer entre les sessions et les fenêtres, ne peuvent pas être utilisés avec l'application Citrix Workspace pour ChromeOS.

Raccourcis Excel

Comment configurer

Les raccourcis clavier sont configurés avec l'attribut **sendAllKeys**.

Pour que tous les raccourcis Excel fonctionnent, configurez ce qui suit : **HTML5_CONFIG > features > sendAllKeys**

L'attribut **sendAllKeys** est réglé par défaut sur **true.** Pour modifier la valeur par défaut, ouvrez le fichier **configuration.js**, ajoutez l'attribut **sendAllKeys** et définissez l'attribut sur **false.**

Pour plus d'informations, consultez la section Comment distribuer des stratégies via la console d'administration Google.

Prise en charge de la touche de logo Microsoft Windows et des touches de raccourci

> **Remarque :**
>
> - Sur les appareils Chromebook, utilisez la touche Rechercher pour mapper la clé du logo Microsoft Windows.

À compter de la version 2108, nous prenons en charge la touche du logo Microsoft Windows et les touches de raccourci dans vos sessions de l'application Citrix Workspace pour ChromeOS.

Nous avons ajouté la prise en charge des combinaisons de touches suivantes :

- Windows + R
- Windows + D
- Windows + E
- Windows + M
- Windows + S
- Windows + CTRL + S
- Windows + T
- Windows + U
- Windows + numéro
- Windows + X
- Windows + K

Affichage automatique du clavier virtuel

À partir de la version 2211, un clavier virtuel apparaît automatiquement lorsque vous placez le curseur sur un champ modifiable. Cette fonctionnalité améliore l'expérience utilisateur sur les appareils à écran tactile, contrairement au comportement précédent où vous deviez cliquer sur l'icône du clavier pour afficher le clavier virtuel.

Mode de saisie Scancode

L'application Citrix Workspace vous permet d'utiliser des claviers physiques externes pour interagir avec la disposition du clavier côté serveur sur le VDA. Lorsque les administrateurs activent le mode Scancode, l'utilisateur peut être amené à utiliser la disposition du clavier du serveur plutôt que celle du client.

Cette fonctionnalité améliore l'expérience utilisateur, en particulier lors de l'utilisation d'un clavier physique pour les langues d'Asie de l'Est

> **Remarques :**
>
> - Cette fonctionnalité est désactivée par défaut.
> - Sur les appareils tactiles, lorsque le mode Scancode est activé, le clavier logiciel affiché à l'écran ne fonctionne pas depuis l'application Citrix Workspace.

Configuration

Vous pouvez configurer la méthode de saisie Scancode de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

Configuration.js

> **Remarques :**
>
> - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
> - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
> - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

Pour activer la fonctionnalité de prise en charge du mode Scancode à l'aide du fichier**configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le dossier racine ChromeApp.
2. Modifiez le fichier et définissez la valeur **scancode** sur **true**.

   Voici un exemple de données JSON :

```
"features" : {

        "ime": {

           "scancode": true,
         }

 }

<!--NeedCopy-->
```

3. Enregistrez les modifications.

Stratégie d'administration Google Pour les appareils et les utilisateurs gérés, les administrateurs peuvent activer la fonctionnalité de prise en charge du mode Scancode à l'aide de la stratégie d'administrateur Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé engine_settings.

   > **Remarque :**
   >
   > Vous pouvez également appliquer cette configuration aux éléments suivants :
   >
   > - **Appareil** > **Chrome** > **Applications et extensions** > **Kiosques** > Rechercher l'extension > Règles relatives aux extensions
   > - **Appareil** > **Chrome** > **Applications et extensions** > **Sessions Invité gérées** > Rechercher l'extension > Règles relatives aux extensions

   Voici un exemple de données JSON :

```
"features" :
{

    "ime": {

                "scancode": true
             }

 }

<!--NeedCopy-->
```


4. Enregistrez les modifications.

Mappage de clavier personnalisé

À partir de la version 2309, les utilisateurs peuvent utiliser des raccourcis et des combinaisons de touches spécifiques à Windows lorsque le VDA est une machine Windows et que le périphérique d'entrée natif est un clavier ChromeOS. Vous pouvez désormais mapper les touches **Ctrl** et **Alt** à l'aide d'un mappage personnalisé. L'utilisateur peut sélectionner la touche Ctrl droite ou gauche pour faire office de touche Alt.

> **Remarques :**
>
> - Le mappage n'est possible qu'en mode plein écran.
> - Une fois le paramètre enregistré, le mappage affecte toutes les sessions.
> - Par défaut, cette fonction est activée.

Configuration

Vous pouvez configurer le mappage de clavier personnalisé de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

Configuration.js

> **Remarques :**
>
> - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
> - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
> - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

Pour désactiver cette fonctionnalité à l'aide du fichier **configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le dossier racine ChromeApp.
2. Modifiez le fichier et définissez la valeur **CustomKeyboardMapping** sur **false**.

   Voici un exemple de données JSON :

```
"features" : {

        "ime": {
```



```
4
5             "CustomKeyboardMapping": false,
6           }
7
8   }
9
10  <!--NeedCopy-->
```

3. Enregistrez les modifications.

Stratégie d'administration Google Pour les appareils et les utilisateurs gérés, les administrateurs peuvent activer la fonctionnalité à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé engine_settings.

   > **Remarques :**
   >
   > Vous pouvez également appliquer cette configuration aux éléments suivants :
   >
   > - **Appareil** > **Chrome** > **Applications et extensions** > **Kiosques** > Rechercher l'extension > Règles relatives aux extensions
   > - **Appareil** > **Chrome** > **Applications et extensions** > **Sessions Invité gérées** > Rechercher l'extension > Règles relatives aux extensions

   Voici un exemple de données JSON :

```
1   "features" :
2   {
3
4       "ime": {
5
6                   "CustomKeyboardMapping": false
7                 }
8
9   }
10
11  <!--NeedCopy-->
```

4. Enregistrez les modifications.

Pour plus d'informations sur l'utilisation de cette fonctionnalité, consultez l'article de la documentation d'aide.

Raccourcis système vers le VDA en mode plein écran

À partir de la version 2309, l'application Citrix Workspace sur les appareils ChromeOS prend en charge le transfert de raccourcis système vers le VDA (session de bureau à distance) en mode plein écran. Cependant, cette configuration ne prend pas effet sur le système d'exploitation client.

Auparavant, l'utilisation de ces combinaisons fonctionnait localement. Désormais, lorsque la fonctionnalité est activée et en mode plein écran, ces combinaisons sont envoyées au VDA mais ne prennent pas effet localement. Par exemple, la touche **Actualiser** est une touche système sur Chromebook, et la combinaison **Ctrl+Maj+Actualiser** représente un raccourci système sur ChromeOS permettant de faire pivoter l'écran. Cependant, le VDA Windows n'entreprend aucune action car il n'existe aucun raccourci de ce type dans le système d'exploitation Windows.

Comme autre exemple, `Alt`+ [est utilisé pour épingler une fenêtre ChromeOS sur la gauche, mais le même raccourci n'a aucun effet sur le Windows VDA. Certaines applications peuvent utiliser de tels raccourcis pour une fonction spécifique. Par exemple, certains scanneurs de codes-barres utilisent `Alt`+ [comme préfixe.

> **Remarque :**
>
> - Cette fonctionnalité est activée par défaut.

Les combinaisons de touches sont les suivantes :

Combinaison de touches de raccourci	Action sur ChromeOS
Action sur ChromeOS	Se déconnecter
Ctrl+Maj+Actualiser	Faire pivoter l'écran de 90 degrés
Ctrl+Maj+L	Verrouiller le Chromebook
Alt+ [	Épingler une fenêtre sur la gauche
Alt+]	Épingler une fenêtre sur la droite, touches pour accéder à la barre latérale, ancrer et restaurer les fenêtres.
Alt+« - »	Réduire la fenêtre
Alt+« + »	Agrandir la fenêtre

> **Remarque :**
>
> - Ces raccourcis système peuvent ne pas avoir les mêmes actions dans le VDA, car il s'agit de raccourcis système ChromeOS.

Configuration

Vous pouvez configurer cette fonctionnalité de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

Configuration.js

> **Remarques :**
>
> - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
> - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
> - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

Pour désactiver cette fonctionnalité à l'aide du fichier **configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le dossier racine ChromeApp.
2. Modifiez le fichier et définissez la valeur **sendSysShortcutForFullscreen** sur **false**.

   Voici un exemple de données JSON :

```
"features" : {

        "ime": {

           "sendSysShortcutForFullscreen": false,
         }

 }

<!--NeedCopy-->
```

3. Enregistrez les modifications.

Stratégie d'administration Google Pour les appareils et les utilisateurs gérés, les administrateurs peuvent désactiver la fonctionnalité à l'aide de la stratégie d'administrateur Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé engine_settings.

> **Remarques :**
>
> Vous pouvez également appliquer cette configuration aux éléments suivants :
>
> - **Appareil** > **Chrome** > **Applications et extensions** > **Kiosques** > Rechercher l'extension > Règles relatives aux extensions
> - **Appareil** > **Chrome** > **Applications et extensions** > **Sessions Invité gérées** > Rechercher l'extension > Règles relatives aux extensions

Voici un exemple de données JSON :

```
"features" :
{

    "ime": {

                "sendSysShortcutForFullscreen": false
            }

 }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Gestion des licences

May 16, 2024

ID d'actif

À propos de cette fonctionnalité

L'application Citrix Workspace utilise un ID d'actif défini par les administrateurs via la console d'administration Google comme nom de client pour les sessions lancées à partir de Chromebooks inscrits.

Comment configurer

Par défaut, l'application Citrix Workspace continue de générer un ID client unique pour les Chromebooks inscrits, ce qui est similaire aux versions antérieures. Pour utiliser cette fonctionnalité, vous devez définir une stratégie pour l'application Citrix Workspace.

La valeur de données que vous entrez ne peut pas comporter plus de 15 caractères. Les valeurs de plus de 15 caractères sont tronquées à 15 caractères.

Configuration de l'ID d'actif

1. Connectez-vous à la console d'administration Google.
2. Accédez à `Device Management` > `Chrome` > `Devices Console` et ajoutez `Asset ID` de l'appareil.
3. Modifiez la stratégie `Google Admin Console` et définissez la valeur `useAssetID` sur **`true`**. Par défaut, `useAssetID` est défini sur **`false`**.

```
{

"settings": {

"Value": {

  "settings_version": "1.0",
  "engine_settings": {

    "uniqueID": {

      "useAssetID": true
                  }

              }

          }

      }

 }


<!--NeedCopy-->
```

Limitations des fonctionnalités :

- Vous devez disposer d'une stratégie d'administration Google qui peut être distribuée. Sinon, la méthode actuelle de génération d'un ID client unique pour les Chromebooks gérés est utilisée.
- N'entrez pas de valeur contenant plus de 15 caractères. Les valeurs de plus de 15 caractères sont tronquées à 15 caractères.

ID unique et ID d'actif

Un ID unique est appliqué en tant que préfixe au nom du client.

L'application Citrix Workspace utilise un ID d'actif défini par les administrateurs via la **console d'administration Google** comme nom de client pour les sessions lancées à partir de Chromebooks inscrits.

Comment configurer

Pour configurer un ID d'actif à l'aide de l'interface graphique, accédez à **Gestion des appareils** > **Chrome** > **Console**, puis ajoutez l'**ID d'actif** de l'appareil.

Pour configurer manuellement un ID d'actif et un ID unique, utilisez la stratégie d'administration Google en incluant les éléments suivants :

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                        "uniqueID" : {

                                "prefixKey" : "CR-",
                                "restrictNameLength" : true,
                                "useAssetID": false
                                     }

                                  }

          }

      }

 }


<!--NeedCopy-->
```

Liste des paramètres d'ID unique ainsi que leurs descriptions :

- «prefixKey » : préfixe à utiliser avant le nom du client. La valeur par défaut est CR.
- « restrictNameLength » : active ou désactive la longueur du nom prefixKey.
- « useAssetID » : ID d'actif défini comme nom de client pour les sessions lancées à partir de Chromebooks inscrits.

Limitations des fonctionnalités :

- Vous devez disposer d'une stratégie d'administration Google qui peut être distribuée. Sinon, la méthode actuelle de génération d'un ID client unique pour les Chromebooks gérés est utilisée.
- N'entrez pas de valeur contenant plus de 15 caractères. Les valeurs de plus de 15 caractères sont tronquées à 15 caractères.

Multimédia

May 16, 2024

Audio

Vous pouvez utiliser un casque USB au sein d'une session pour parler et écouter. Vous pouvez également utiliser les boutons sur le casque USB (comme tels que désactiver le son et sauter). L'expérience utilisateur est enrichie en fournissant une sortie audio fluide.

Audio adaptatif

Avec l'audio adaptatif, vous n'avez pas besoin de configurer les stratégies de qualité audio sur le VDA. L'audio adaptatif optimise les paramètres de votre environnement. Il remplace les formats de compression audio obsolètes pour offrir une excellente expérience utilisateur.

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

Attributs de la fonctionnalité

Il existe deux attributs pour la fonctionnalité :

- **EnableAdaptiveAudio :** définissez la valeur sur true pour activer la fonction d'audio adaptatif. Définissez la valeur sur false pour désactiver la fonctionnalité.
- **EnableStereoRecording :** l'enregistrement stéréo est une fonctionnalité facultative. Cette fonctionnalité est désactivée par défaut. Définissez la valeur de l'attribut **EnableStereoRecording** sur **true** pour activer l'enregistrement stéréo ou définissez la valeur sur **false** pour désactiver la fonctionnalité. Cette fonctionnalité ne peut être prise en charge que lorsque la fonction d'audio adaptative est activée. Lorsque l'attribut **EnableStereoRecording** est défini sur true, l'enregistrement stéréo est pris en charge avec l'annulation de l'écho désactivée.

Comment configurer

Vous pouvez configurer la fonctionnalité d'audio adaptatif des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

Configuration.js Pour configurer l'audio adaptatif à l'aide du fichier **configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le **dossier racine ChromeApp**.
2. Modifiez ce fichier pour configurer la fonctionnalité d'audio adaptatif.

   > **Remarques :**
   >
   > - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
   > - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
   > - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

3. Définissez la valeur par défaut de **EnableAdaptiveAudio** sur **true**. Définissez la valeur par défaut de **EnableStereoRecording** sur **false**.

   Voici un exemple de données JSON :

```
"features" : {

    "audio" : {

    "EnableAdaptiveAudio": true
             }

 }


"features" : {

    "audio" : {

        "EnableStereoRecording": false
             }

 }

<!--NeedCopy-->
```


4. Enregistrez les modifications.

> **Remarque :**
>
> - Pour désactiver la fonctionnalité, définissez l'attribut **EnableAdaptiveAudio** sur **false**.

Stratégie d'administration Google Lors du déploiement sur site, les administrateurs peuvent activer la fonctionnalité d'audio adaptatif à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé **engine_settings**.

   Voici un exemple de données JSON :

```
"features" : {

    "audio" : {

        "EnableAdaptiveAudio": {

            "type": "boolean" }

                    }

                }


"features" : {

    "audio" : {

        "EnableStereoRecording": {

            "type": "boolean" }

                }

             }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Prise en charge des périphériques audio Plug and Play

Auparavant, un seul périphérique de lecture et d'enregistrement audio était pris en charge et était affiché en tant que **Citrix HDX Audio**, quel que soit le nom réel du périphérique.

À partir de la version 2301, nous prenons en charge plusieurs périphériques audio et les redirigeons vers le VDA. Désormais, lorsque vous redirigez des périphériques audio, vous pouvez afficher le nom réel du périphérique audio sous les paramètres **Son** > **Lecture** et **Son** > **Enregistrement** sur le VDA. La liste des périphériques du VDA est mise à jour dynamiquement chaque fois qu'un périphérique audio est branché ou retiré.

> **Remarque :**
>
> Cette fonctionnalité est activée par défaut.

Configuration

Vous pouvez configurer cette fonctionnalité de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

Configuration.js Pour désactiver la prise en charge des périphériques audio Plug and Play à l'aide du fichier **configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le **dossier racine ChromeApp**.
2. Modifiez le fichier pour configurer la fonctionnalité de prise en charge des périphériques audio Plug and Play.

   > **Remarques :**
   >
   > - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
   > - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
   > - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

3. Définissez la valeur de **AudioRedirectionV4** sur **false**. Voici un exemple de données JSON :

```
1     "features" : {
2
3         "audio" : {
4
```



```
            "AudioRedirectionV4": false
                    }

          }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Stratégie d'administration Google Lors du déploiement sur site, les administrateurs peuvent désactiver la fonctionnalité de prise en charge des périphériques audio Plug and Play à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **.txt** sous la clé **engine_settings**.

   Voici un exemple de données JSON :

```
    "features" : {

        "audio" : {

          "AudioRedirectionV4": false
                  }

         }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Limitations connues

- Sur le VDA, le nom du périphérique audio intégré est affiché uniquement en anglais. Le problème se produit lorsque vous utilisez des appareils basés sur ChromeOS. [RFHTMCRM-8667]

Webcam

L'application Citrix Workspace pour ChromeOS améliore la fonctionnalité de redirection de webcam. L'encodage matériel H.264 pour webcam permet de réduire la charge du processeur et d'augmenter l'autonomie de la batterie pour les appareils Chromebook. Ces appareils sont équipés d'encodeurs basés sur la norme H.264, qui tire parti de la fonctionnalité Intel via l'API PPB_VideoEncoder.

L'application Citrix Workspace pour ChromeOS prend en charge la redirection de webcam pour les applications 32 bits et 64 bits.

Redirection de webcam

La redirection de webcam est disponible pour les applications 32 bits et 64 bits. La prise en charge de la redirection de webcam avec les applications 32 bits et 64 bits est limitée aux webcams intégrées.

Vous pouvez désormais utiliser des webcams externes dans les sessions d'applications et de bureaux virtuels de l'application Citrix Workspace pour ChromeOS. L'application Citrix Workspace détecte les webcams externes récemment connectées et les rend disponibles à l'utilisation.

Comment configurer

Configurez la redirection de webcam pour applications 64 bits comme suit :

Configuration de la webcam à l'aide du fichier configuration.js et de la console d'administration Google Pour les versions 2101 et ultérieures :

Configurez la redirection de webcam en utilisant le chemin suivant : **HTML5_CONFIG > features > video**

> **Remarque :**
>
> Nous vous recommandons d'utiliser le chemin **HTML5_CONFIG > features > video** pour configurer la redirection de webcam. L'autre chemin continuera de fonctionner pendant un certain temps et sera supprimé dans une version ultérieure.

Recommandations pour la redirection de webcam

- Définissez la stratégie Qualité audio de Citrix Delivery Controller sur Faible ou Moyen. Lorsque vous utilisez des Chromebooks de faible puissance, des décalages audio peuvent se produire si vous ne définissez pas la stratégie Qualité audio.
- Pour des performances optimales, nous vous recommandons d'utiliser des Chromebooks haut de gamme et des réseaux à faible latence avec des connexions à bande passante élevée.
- Définissez la clé de Registre suivante sur un VDA :

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime

  Nom : OfferH264ToApp

  Type : REG_DWORD

  Valeur : 1

> **Remarque :**
>
> ce paramètre s'applique au paramètre utilisateur actuel. Pour les nouveaux utilisateurs, définissez la clé de Registre via l'éditeur d'objets de stratégie de groupe (GPO) de Windows.

AVERTISSEMENT : 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.

Optimisation pour Microsoft Teams

May 16, 2024

Vous pouvez utiliser les fonctionnalités suivantes de Microsoft Teams pour les sessions de bureau virtuel et d'application virtuelle :

- Appels audio optimisés
- Appels vidéo optimisés
- Partage d'écran optimisé

Uniquement pris en charge sur les VDA versions 1906 et ultérieures.

> **Remarques :**
>
> - Par défaut, le partage d'écran permet de partager la totalité de l'écran. Toutefois, vous pouvez limiter le partage d'écran uniquement au contenu de l'application Citrix Workspace. Pour plus d'informations, consultez Limiter le partage d'écran du contenu de l'application Citrix Workspace. Pour activer la fonctionnalité de partage d'écran via la stratégie d'administration Google, consultez la section Paramètres d'optimisation de Microsoft Teams.
> - Pour résoudre les problèmes et basculer Microsoft Teams du mode optimisé au mode non optimisé au sein de votre session client, consultez Dépannage de l'optimisation de Microsoft Teams.
> - Lors du partage d'écran à l'aide de l'optimisation Microsoft Teams, la bordure rouge autour de la fenêtre partagée n'apparaît pas.
> - Le partage d'applications n'est pas pris en charge.
> - L'optimisation de Microsoft Teams pour les appels audio, les appels vidéo et le partage d'

> écran est généralement disponible à partir de la version 2105.5. Nous vous recommandons de mettre à jour vers la dernière version de l'application Citrix Workspace pour ChromeOS.

Appels vidéo et partage d'écran sur des moniteurs externes

Sur votre moniteur externe, vous pouvez désormais utiliser les fonctionnalités suivantes de Microsoft Teams lors des appels.

- Vidéo optimisée
- Partage d'écran optimisé

Ces fonctionnalités sont disponibles pour les appels Microsoft Teams dans les bureaux virtuels. Elles sont également disponibles pour les appels effectués via l'application virtuelle Microsoft Teams, lorsque vous placez les fenêtres Microsoft Teams sur un moniteur externe.

Remarques (mise à jour de ChromeOS version 96)

- Pour éviter tout impact de la mise à jour de ChromeOS version 96 sur le fonctionnement de Microsoft Teams, procédez comme suit avant de mettre à jour ChromeOS :
- Pour les utilisateurs disposant d'une version reconditionnée de l'application Citrix Workspace, consultez l'article CTX331648 du centre de connaissances et suivez les étapes.
- Pour tous les autres utilisateurs de l'application Citrix Workspace pour ChromeOS, version 2110 et antérieure, consultez l'article CTX331653du centre de connaissances.

Paramètres d'optimisation de Microsoft Teams

Pour activer le partage d'écran

Pour activer le partage d'écran à l'aide de la stratégie d'administration Google, définissez la valeur de partage d'écran sur **true** pour **msTeamsOptimization**, comme suit.

Pour plus d'informations, consultez l'article Comment distribuer des stratégies via la console d'administration Google.

```
{

  "settings": {

     "Value": {

       "settings_version": "1.0",
          "engine_settings": {

```



```
                "features":{

                    "msTeamsOptimization":{

                    "screenSharing" : true
                        }

                    }

                }

            }

        }

<!--NeedCopy-->
```

Pour activer le partage d'écran pour les utilisateurs BYOD (Apportez votre propre appareil) (uniquement pour ceux utilisant des instances StoreFront locales) :

Suivez les étapes décrites dans l'article Utiliser webconfig et ajoutez la valeur **chromeAppPreferences** comme suit :

Par exemple :

```
chromeAppPreferences = {

    "features":{

        "msTeamsOptimization":{

            "screenSharing":true
             }

             }

             }

<!--NeedCopy-->
```

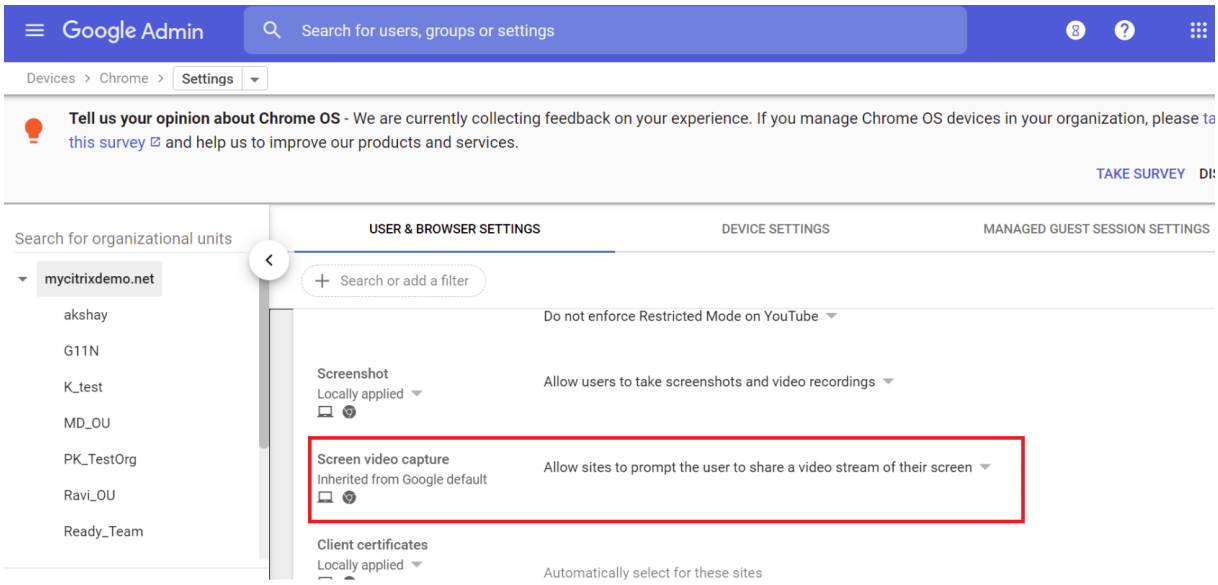
Paramètres de la console d'administration Google

Assurez-vous que les paramètres suivants sont autorisés dans la **console d'administration Google** pour que l'optimisation du partage d'écran fonctionne.

Dans la **console d'administration Google**, sous **Appareils** > **Chrome** > **Paramètres**, sélectionnez > **Autoriser les sites à inviter l'utilisateur à partager un flux vidéo de son écran**sous **Capture vidéo**

d'écran pour les trois catégories :

- **Paramètres utilisateurs et navigateurs**
- **Paramètres de l'appareil**
- **Paramètres des sessions Invité gérées** (ou une catégorie appropriée).



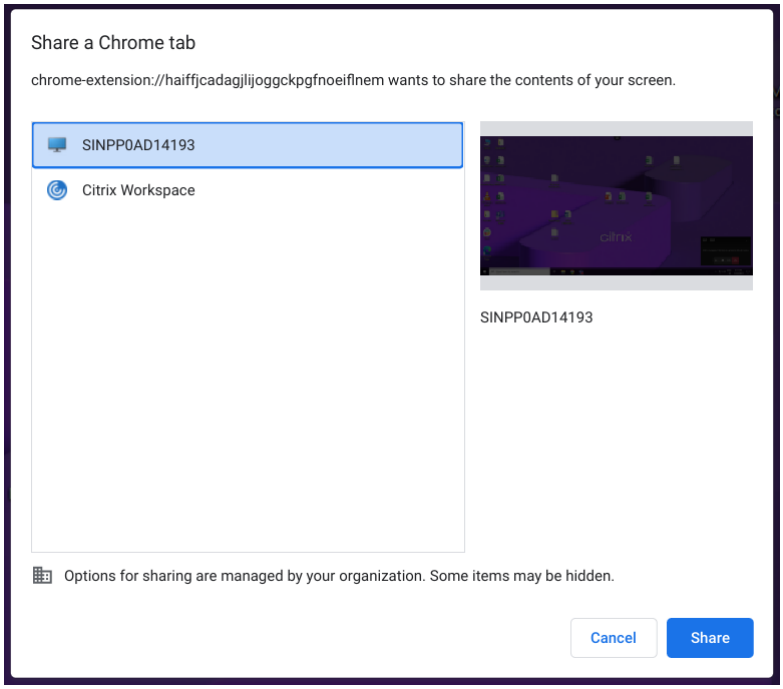
Limiter le partage d'écran du contenu de l'application Citrix Workspace

Pour optimiser Microsoft Teams, les administrateurs peuvent limiter le partage d'écran des applications et des bureaux uniquement via l'application Citrix Workspace sur les appareils Chrome gérés. Lorsque les administrateurs activent cette fonctionnalité, les utilisateurs ne peuvent partager que les ressources qui sont ouvertes à partir de l'application Citrix Workspace.

Cette fonctionnalité est applicable à Chrome version M98 et ultérieure.

Pour configurer les paramètres, utilisez les stratégies de Google comme suit :

1. Accédez à la console d'**administration Google** > **Paramètres** > **Paramètres utilisateurs et navigateurs**.
2. Accédez à **Capture vidéo de l'écran autorisée par les sites** > **Autoriser la capture vidéo de l'onglet (même site uniquement) par ces sites** et entrez l'ID de l'application Citrix Workspace pour ChromeOS -haiffjcadagjlijoggckpgfnoeiflnem.

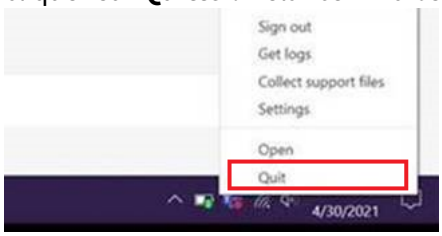


Désormais, les utilisateurs finaux peuvent sélectionner l'onglet et partager du contenu ouvert via l'application Citrix Workspace uniquement.

Dépannage de l'optimisation de Microsoft Teams

Pour basculer Microsoft Teams du mode optimisé au mode non optimisé au sein de vos sessions clientes, procédez comme suit :

- Quittez Microsoft Teams en cliquant avec le bouton droit sur l'icône Microsoft Teams, puis cliquez sur **Quitter.** Relancez Microsoft Teams.



- Si quitter ne fonctionne pas, déconnectez-vous de la session et reconnectez-vous.
- Si la déconnexion et la reconnexion ne fonctionnent pas, effacez le cache dans le répertoire **C:\Users\Administrator\AppData\Roaming\Microsoft\Teams** sur le VDA, puis redémarrez Microsoft Teams.

Pour plus d'informations, consultez Dépannage.

Pour dépanner la version de la bibliothèque shim, consultez la section Journaux d'optimisation de Microsoft Teams.

Prise en charge des appels d'urgence dynamiques

L'application Citrix Workspace prend en charge les appels d'urgence dynamiques. Lorsque cette fonction est utilisée avec les forfaits d'appel Microsoft, Operator Connect et Direct Routing, elle permet de :

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

La notification est fournie en fonction de l'emplacement actuel de l'application Citrix Workspace exécutée sur le point de terminaison, au lieu du client Microsoft Teams sur le VDA.

La loi Ray Baum exige que l'emplacement de la personne effectuant l'appel d'urgence soit transmis au centre de réception des appels d'urgence approprié. À partir de l'application Citrix Workspace 2112 pour ChromeOS, l'optimisation Microsoft Teams avec HDX est conforme à la loi Ray Baum.

Flou d'arrière-plan et effets dans l'optimisation de Microsoft Teams

À compter de la version 2303, l'application Citrix Workspace pour ChromeOS prend en charge le flou et les effets d'arrière-plan dans l'optimisation de Microsoft Teams pour les appels vidéo. Vous pouvez flouter ou remplacer les effets d'arrière-plan fournis par Microsoft Teams. Cette fonctionnalité vous permet d'éviter les distractions inattendues en permettant à la conversation de rester centrée sur la silhouette (corps et visage). Cette fonctionnalité peut être utilisée avec les appels P2P et les conférences téléphoniques.

> **Remarques :**
>
> - Cette fonctionnalité est désactivée par défaut.
> - Cette fonctionnalité est désormais intégrée à l'interface utilisateur 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.
- Lorsque vous activez cette fonctionnalité, vous pouvez rencontrer des problèmes de performances.
- 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.

Comment configurer Vous pouvez activer la fonction d'effet d'arrière-plan de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google
- Global App Configuration Service

Configuration.js Pour configurer le flou et les effets d'arrière-plan à l'aide du fichier **configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le dossier racine **ChromeApp**.

   > **Remarques :**
   >
   > - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
   > - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
   > - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

2. Modifiez le fichier **configuration.js** et définissez la valeur par défaut de backgroundEffects sur true.

   Voici un exemple de données JSON :

   ```
   "features" :
   {

       "msTeamsOptimization" : {

           "backgroundEffects" : true
        }

    }

   <!--NeedCopy-->
   ```

3. Enregistrez les modifications.

Stratégie d'administration Google Lors du déploiement sur site, les administrateurs peuvent activer la fonctionnalité d'effet d'arrière-plan à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.

2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé **engine_settings**.
   Voici un exemple de données JSON :

```
"features" :
{

    "msTeamsOptimization" : {

        "backgroundEffects" : true
     }

 }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Global App Configuration Service Lors de la configuration cloud, les administrateurs peuvent activer la fonctionnalité d'effet d'arrière-plan en définissant l'attribut **backgroundEffects** sur **true** dans Global App Configuration Service.

Pour plus d'informations, consultez la documentation Global App Configuration Service.

Prise en charge de DTMF (Dual Tone Multi Frequency) avec Microsoft Teams

L'application Citrix Workspace prend désormais en charge l'interaction de signalisation DTMF avec les systèmes de téléphonie (par exemple, RTPC) et les téléconférences dans Microsoft Teams. Cette fonctionnalité est activée par défaut.

Sous-titres instantanés dans Microsoft Teams

L'optimisation de Microsoft Teams prend en charge la transcription en temps réel de la source audio du haut-parleur lorsque la fonction Sous-titres en direct est activée dans Microsoft Teams.

Prise en charge de la sonnerie secondaire

À partir de la version 2312, vous pouvez utiliser la fonction de sonnerie secondaire pour sélectionner un appareil secondaire sur lequel vous souhaitez recevoir la notification d'appel entrant. Cette fonctionnalité n'est applicable que lorsque Microsoft Teams est optimisé.

Par exemple, imaginez que vous avez défini un haut-parleur comme sonnerie secondaire et que votre point de terminaison est connecté à un casque. Dans ce cas, Microsoft Teams envoie la sonnerie d'

appel entrant au casque et au haut-parleur. Vous ne pouvez pas définir de sonnerie secondaire dans les cas suivants :

- Lorsque vous n'êtes pas connecté à plusieurs périphériques audio
- Lorsque le périphérique n'est pas disponible (par exemple, un casque Bluetooth)

> **Remarque**
>
> Cette fonctionnalité est désactivée par défaut.

Limites connues de cette fonctionnalité

- Lorsque vous activez cette fonctionnalité, vous pouvez entendre la sonnerie secondaire deux fois avec un léger décalage. Ce problème est un bogue dans Microsoft Teams qui devrait être corrigé dans la prochaine version de Microsoft Teams.

Configuration

Vous pouvez configurer la fonctionnalité de sonnerie secondaire de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

Configuration.js

> **Remarques :**
>
> Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
> Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
> Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

Pour activer cette fonctionnalité à l'aide du fichier**configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le dossier racine ChromeApp.
2. Modifiez le fichier et définissez la valeur **secondaryRingtone** sur **true**.

   Voici un exemple de données JSON :

```
{

    "features":{

```



```
        "msTeamsOptimization":{

            "secondaryRingtone" : true
             }

         }

 }

<!--NeedCopy-->
```

3. Enregistrez les modifications.

Stratégie d'administration Google Pour les appareils et les utilisateurs gérés, les administrateurs peuvent activer la fonctionnalité à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Vous pouvez également appliquer cette configuration aux éléments suivants :
   - **Appareil** > **Chrome** > **Applications et extensions** > **Utilisateurs et navigateurs** > Rechercher l'extension > Règles relatives aux extensions
   - **Appareil** > **Chrome** > **Applications et extensions** > **Kiosques** > Rechercher l'extension > Règles relatives aux extensions
   - **Appareil** > **Chrome** > **Applications et extensions** > **Sessions Invité gérées** > Rechercher l'extension > Règles relatives aux extensions

   Voici un exemple de données JSON :

```
      {

          "settings": {

                "Value": {

                   "settings_version": "1.0",
                     "engine_settings": {

                          "features":{

                                  "msTeamsOptimization":{

                                         "secondaryRingtone" :
                                            true  }

                                              }

                                       }

                                    }
```



```
21
22                                          }
23
24                  }
25
26  <!--NeedCopy-->
```

3. Enregistrez les modifications.

Implémentation de la diffusion simultanée pour des visioconférences dans Microsoft Teams optimisé

À compter de la version 2312, la prise en charge de la diffusion simultanée est activée par défaut pour des visioconférences dans Microsoft Teams optimisé. Avec cette version, la qualité et l'expérience des visioconférences sur différents terminaux sont améliorées. L'adaptation à la résolution appropriée permet ainsi d'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). Les résolutions dépendent de plusieurs facteurs, notamment la capacité du point de terminaison, les conditions du réseau, etc. Le point de terminaison récepteur demande ensuite la résolution de qualité maximale qu'il peut gérer, offrant ainsi à tous les utilisateurs une expérience vidéo optimale.

Prise en charge de l'optimisation de Zoom

May 16, 2024

À partir de la version 2402.1, l'application Citrix Workspace pour ChromeOS prend en charge l'intégration à la solution d'infrastructure de bureau virtuel (VDI, Virtual Desktop Infrastructure) Zoom pour une expérience de conférence audio et vidéo optimisée dans les sessions .

> **Remarque :**
>
> Cette fonctionnalité est activée par défaut, mais les administrateurs doivent la configurer. Uniquement pris en charge sur les VDA versions 1906 et ultérieures.

Logiciels requis

Les administrateurs doivent configurer :

- La stratégie DDC **VirtualChannelWhiteList** pour utiliser les canaux virtuels Zoom. Pour plus d'informations, consultez la section Paramètres de stratégie de liste d'autorisation des canaux virtuels dans la documentation .
- Les prérequis pour configurer Zoom VDI pour ChromeOS.

Limitations de la fonctionnalité

- La fenêtre d'affichage des conférences Zoom est limitée au moniteur principal uniquement.
- Les périphériques HID ne sont pas pris en charge
- Pour d'autres limitations, consultez la section Limitations liées à l'utilisation de Zoom VDI pour ChromeOS.

Comment configurer

Vous pouvez configurer cette fonctionnalité de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

Configuration.js

> **Remarques :**
>
> - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
> - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
> - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

Pour activer cette fonctionnalité à l'aide du fichier **configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le dossier racine ChromeApp.
2. Modifiez le fichier **configuration.js** et ajoutez les URL Zoom selon les besoins.

   Voici un exemple de données JSON :

```
"features" :
{

    "customVC": [
    {
```



```
6
7           "streamName": "ZOOMHDX",
8           "appId": "html=https://zoom.us/vdi/plugin"
9       }
10   ,
11      {
12
13          "streamName": "ZOOMHDC",
14          "appId": "html=https://zoom.us/vdi/plugin"
15       }
16   ,
17      {
18
19          "streamName": "ZOOMPHX",
20          "appId": "html=https://zoom.us/vdi/plugin"
21       }
22
23  ],
24  "customVCWhitelistURL": [
25      {
26
27          "url": "https://zoom.us/vdi/plugin",
28          "permissions": [
29              "media"
30          ]
31       }
32   ,
33      {
34
35          "url": "https://zoom.us/vdi/webview",
36          "permissions": [
37              "media"
38          ]
39       }
40
41  ]
42
43   }
44
45  <!--NeedCopy-->
```

3. Enregistrez les modifications.

Stratégie d'administration Google

Pour les appareils et les utilisateurs gérés, les administrateurs peuvent activer la fonctionnalité à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.

3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé engine_settings.

> **Remarque :**
>
> Vous pouvez également appliquer cette configuration aux éléments suivants :
>
> - **Appareil** > **Chrome** > **Applications et extensions** > **Utilisateurs et navigateurs** > Rechercher l'extension > Règles relatives aux extensions.
> - **Appareil** > **Chrome** > **Applications et extensions** > **Kiosques** > Rechercher l'extension > Règles relatives aux extensions.
> - **Appareil** > **Chrome** > **Applications et extensions** > **Sessions Invité gérées** > Rechercher l'extension > Règles relatives aux extensions.

Voici un exemple de données JSON :

```
{

"settings": {

"Value": {

    "settings_version": "1.0",

"customVC": [
   {

       "streamName": "ZOOMHDX",
       "appId": "html=https://zoom.us/vdi/plugin"
    }
 ,
   {

       "streamName": "ZOOMHDC",
       "appId": "html=https://zoom.us/vdi/plugin"
    }
 ,
   {

       "streamName": "ZOOMPHX",
       "appId": "html=https://zoom.us/vdi/plugin"
    }

],
"customVCWhitelistURL": [
   {

       "url": "https://zoom.us/vdi/plugin",
       "permissions": [
           "media"
       ]
    }
 ,
```



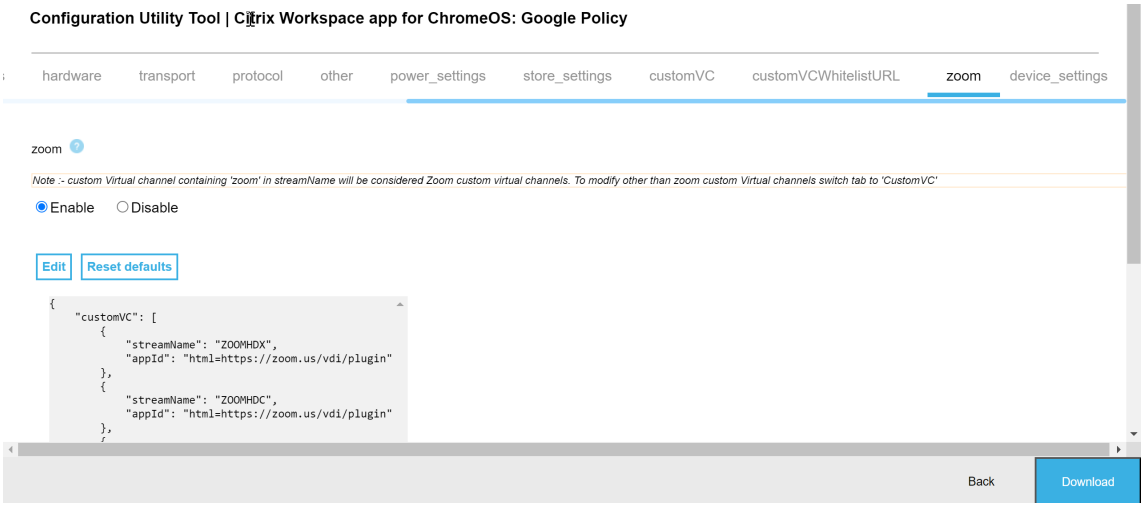
```
    {

        "url": "https://zoom.us/vdi/webview",
        "permissions": [
            "media"
        ]
     }

]
 }

 }

 }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Outil Configuration Utility

Pour personnaliser la fonctionnalité :

1. Cliquez sur Téléchargements.
2. Accédez à la section **Outil Configuration Utility** et développez l'élément.
3. Téléchargez et décompressez le fichier.
4. Cliquez sur le lien de documentation de l'outil Configuration Utility pour comprendre comment utiliser l'outil.
5. Créez une configuration de stratégie Google.
6. Faites défiler l'écran horizontalement et sélectionnez l'onglet **Zoom**. Activez la fonctionnalité pour continuer.



7. Cliquez sur **Télécharger** pour générer et enregistrer le fichier **policy.txt**.
8. Personnalisez cette fonctionnalité selon les besoins en fournissant les URL appropriées.
9. Ouvrez l'application Citrix Workspace dans la console d'administration Google.
10. Téléchargez le fichier **policy.txt** généré ou copiez-collez le contenu.

Configuration de Zoom VDI pour ChromeOS

Pour plus d'informations, consultez l'article du support Zoom sur la configuration de Zoom VDI pour ChromeOS.

Multimoniteur

May 16, 2024

Affichage multi-moniteurs

La fonction d'affichage multi-écrans prend en charge jusqu'à deux moniteurs externes (1 moniteur de périphérique intégré + 2 moniteurs externes). La fonctionnalité multi-moniteurs est activée par défaut.

Les boîtes de dialogue d'interface et les barres d'outils s'affichent uniquement sur l'écran principal. Toutefois, les boîtes de dialogue d'authentification par carte à puce et USB s'affichent sur plusieurs écrans.

Comment configurer

La fonctionnalité multi-moniteurs est activée par défaut.

> **Remarque :**
>
> - Si vous utilisez l'application Citrix Workspace sur XenApp 6.5, définissez la stratégie d'**observation** sur **Désactivé** pour utiliser la fonctionnalité multi-moniteurs.
> - Dans une session de bureau sur laquelle la fenêtre est en plein écran, l'option **Résolution d'affichage** dans les paramètres **Préférences** est désactivée.
> - Les boîtes de dialogue d'interface et les barres d'outils s'affichent uniquement sur l'écran

> principal. Toutefois, les boîtes de dialogue d'authentification par carte à puce et USB s'affichent sur plusieurs écrans.

Pour désactiver l'affichage multi-moniteurs amélioré en mode kiosque

L'affichage multi-moniteurs amélioré en mode kiosque est activé par défaut.

Pour désactiver la fonctionnalité dans le mode kiosque, modifiez le fichier **configuration.js** ou la stratégie **Console d'administration Google** et définissez la valeur de **kioskMultimonitor** sur **false**.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
            "engine_settings": {

                "features": {

                    "graphics": {

                        "multiMonitor": true,
                        "kioskMultimonitor": true
                    }

                }

            }

        }

    }

}


<!--NeedCopy-->
```

> **Remarque :**
>
> Pour lancer une session en mode kiosque, vous devez activer le mode **bureau unifié**.

1. Lancez un navigateur Web et entrez la commande suivante : chrome://flags
2. Dans la liste qui s'affiche, recherchez UnifiedDesktopMode et définissez-le sur **Activé**.

Pour configurer le mode Bureau unifié

1. Connectez-vous à la console d'administration Google.

2. Accédez à **Gestion des appareils > Gestion de Chrome > Paramètres utilisateur**.
3. Définissez la stratégie Bureau unifié sur **Rendre le mode Bureau unifié accessible à l'utilisateur**.
4. Cliquez sur **Enregistrer**.

Performances multi-moniteurs

L'application Citrix Workspace pour ChromeOS améliore les performances globales et la stabilité des sessions dans les scénarios multi-moniteurs. Dans les versions antérieures, lorsqu'une session était en cours d'exécution sur plusieurs écrans, cela entraînait une dégradation des performances.

Comment configurer

Affichage multi-moniteurs en mode kiosque L'affichage multi-moniteurs amélioré en mode kiosque est activé par défaut.

Pour désactiver le mode kiosque, modifiez le fichier **configuration.js** ou la stratégie **Console d'administration Google** et définissez la valeur de **kioskMultimonitor** sur **false**.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
            "engine_settings": {

                "features": {

                    "graphics": {

                        "kioskMultimonitor": false
                    }

                }

            }

        }

    }


<!--NeedCopy-->
```


> **Remarque :**
>
> Pour lancer une session en mode kiosque, vous devez activer le mode **bureau unifié**.

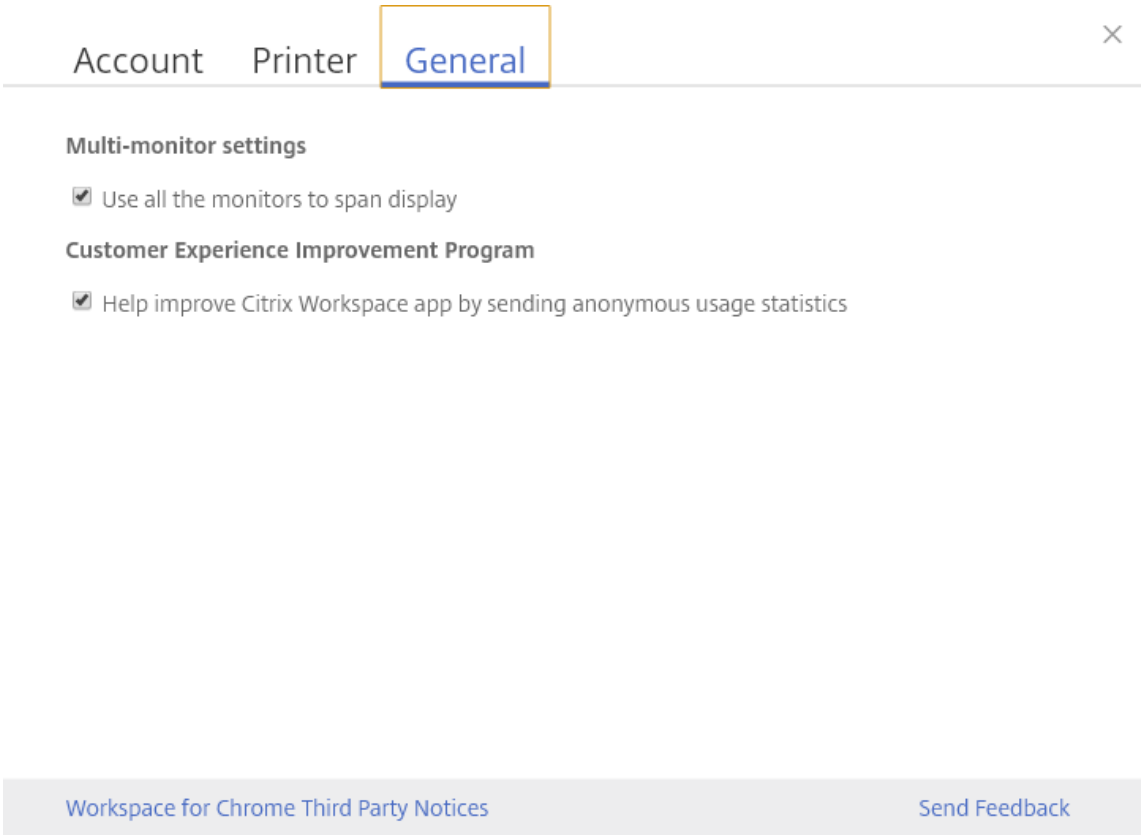
1. Lancez un navigateur Web et entrez la commande suivante : chrome://flags
2. Dans la liste qui s'affiche, recherchez UnifiedDesktopMode et définissez-le sur **Activé**.

Pour configurer le mode bureau unifié à l'aide d'une stratégie d'administration Google

1. Connectez-vous à la console d'administration Google.
2. Accédez à **Gestion des appareils > Gestion de Chrome > Paramètres utilisateur**.
3. Définissez la stratégie Bureau unifié sur **Rendre le mode Bureau unifié accessible à l'utilisateur**.
4. Cliquez sur **Enregistrer**.

Pour désactiver la fonctionnalité multi-moniteurs La fonctionnalité multi-moniteurs est activée par défaut.

1. Lancez l'application Citrix Workspace pour ChromeOS.
2. Sélectionnez **Paramètres > Généraux**.
3. Décochez **Utiliser tous les moniteurs pour couvrir l'affichage**.



L'affichage multi-moniteurs est disponible aussi bien pour les bureaux que pour les applications.

Lors de l'utilisation d'un affichage multi-moniteurs, la session de bureau peut s'étendre sur plusieurs écrans de deux façons :

4. Mode fenêtré : la session de bureau s'affiche sur un seul écran.
5. Mode plein écran : lorsqu'une session de bureau bascule en mode plein écran, elle s'affiche en mode multi-moniteurs uniquement lorsque l'option **Utiliser tous les moniteurs pour couvrir l'affichage** est sélectionnée.

   Pour que l'affichage s'étende aux écrans dans une session de bureau, sélectionnez l'option **Utiliser tous les moniteurs pour couvrir l'affichage** et cliquez sur le mode plein écran lorsque les deux écrans sont connectés.

   Dans une session d'application, lorsque deux écrans sont connectés et que l'option **Utiliser tous les moniteurs pour couvrir l'affichage est sélectionnée**, la session s'affiche automatiquement en mode multi-moniteurs.

Utilisation de Citrix Virtual Desktops sur deux moniteurs :

1. Cliquez sur **Mode multi-moniteurs** dans la barre d'outils.

   L'écran est maintenant étendu aux deux moniteurs.

Limitations des fonctionnalités :

- L'application Citrix Workspace pour ChromeOS ne prend pas en charge le mode graphique H.264 plein écran avec plusieurs moniteurs.
- La limite du nombre de moniteurs n'est pas codée en dur. La résolution totale à gérer et à afficher affecte la limitation.
  - Cette fonction prend en charge jusqu'à deux moniteurs externes (1 moniteur de périphérique intégré + 2 moniteurs externes). Si vous lancez une session avec une résolution d'écran supérieure à [2 x (1920x1080)] pixels, vous risquez de rencontrer des retards d'écran. Les limites de résolution du moniteur peuvent provoquer des retards d'écran.
  - L'écran intégré des derniers Chromebooks prend en charge une résolution supérieure à 1920x1080 pixels. La fonctionnalité n'a pas été testée sur de tels appareils.
- En mode multi-moniteurs, le mode H264 plein écran est désactivé en raison de problèmes détectés lors de tests.
  - Lorsque vous utilisez un moniteur unique externe de grande taille, le problème ne se produit pas et H264 reste en cours d'exécution. Le mode H264 sélectif s'exécute également dans ce scénario.

- Lorsque vous utilisez des écrans avec des résolutions différentes, vous pouvez rencontrer des problèmes de performances.
- Lorsque vous utilisez des moniteurs intégrés avec une résolution plus élevée et des moniteurs externes dont la résolution est faible, des problèmes de performances peuvent se produire.

Prise en charge des bureaux virtuels dans des configurations à plusieurs moniteurs

Vous pouvez désormais utiliser votre bureau virtuel en mode plein écran sur un sous-ensemble de moniteurs disponibles. Auparavant, lorsque vous aviez sélectionné le mode multi-moniteurs dans la barre d'outils, le bureau virtuel s'étendait sur tous les moniteurs disponibles. Vous pouvez maintenant faire glisser votre bureau virtuel pour couvrir deux moniteurs (sur plus de deux), puis sélectionner le mode multi-moniteurs. Un cas d'utilisation typique de ce scénario est celui où vous avez choisi d'exécuter une application de visioconférence sur le moniteur de votre appareil natif et que vous souhaitez afficher le contenu de votre bureau virtuel en plein écran sur vos deux autres moniteurs pendant l'appel.

> **Remarque :**
>
> - Pour utiliser cette fonctionnalité, sous **Paramètres généraux** > **Paramètres multi-écrans** > sélectionnez l'option **Utiliser tous les moniteurs pour couvrir l'affichage**.

Périphériques

May 20, 2024

Redirection de périphérique USB

L'application Citrix Workspace pour ChromeOS prend en charge un large éventail de périphériques USB. Grâce à cette fonctionnalité, vous pouvez créer une stratégie Google permettant d'identifier l'identificateur PID/VID du périphérique de manière à autoriser son utilisation dans Citrix Workspace. Cette prise en charge s'étend également aux nouveaux périphériques USB.

Comment configurer

Pour de plus amples informations sur la configuration des périphériques USB, consultez l'article CTX200825 du centre de connaissances.

Redirection automatique des périphériques USB en mode kiosque

En mode kiosque, les périphériques USB sont redirigés automatiquement au sein d'une session sans aucune intervention manuelle. Dans les modes utilisateur et public, lors de la première utilisation, vous devez rediriger manuellement le périphérique USB dans la session à partir de la barre d'outils ou du Centre de connexion. Cette redirection USB manuelle est effectuée pour accorder au système d'exploitation Chrome l'autorisation d'accéder au périphérique USB. Lorsqu'un périphérique USB est inséré, il est automatiquement redirigé dans la session.

> **Important :**
>
> - Si vous insérez un périphérique USB lorsque de nombreuses sessions sont en cours d'exécution, il est redirigé dans la session qui est active.
> - Si aucune session n'est active, le périphérique USB n'est redirigé dans aucune session.
> - Si une seule session est en cours d'exécution et qu'elle n'est pas active lorsque vous insérez le périphérique USB, sa redirection peut échouer.

Pour rediriger le périphérique USB vers une nouvelle session

> **Remarque :**
>
> Pour rediriger le périphérique USB vers une nouvelle session, vous devez supprimer le périphérique USB de la session précédente.

1. Cliquez avec le bouton droit de la souris sur l'icône Citrix Workspace et sélectionnez **Centre de connexion**. La fenêtre Centre de connexion s'affiche.
2. Sélectionnez une session ou une application.
3. Cliquez sur **Périphériques**.
4. Accédez à la section **USB**.
5. Cliquez sur **Libérer tous les périphériques**.

Double saut

À partir de la version 2301, l'application Citrix Workspace prend en charge les scénarios à double saut. Cette fonctionnalité constitue une amélioration de la redirection USB.

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

Redirection USB composite

Auparavant, lorsqu'un périphérique USB composite était connecté à l'appareil local, il pouvait être uniquement utilisé en tant que périphérique unique via la redirection USB. L'inconvénient était que

les interfaces telles que l'audio et la vidéo étaient également redirigées via USB, malgré les canaux optimisés. Les interfaces n'étaient pas séparées et, en raison de cette incapacité, les administrateurs ne pouvaient pas décider quels composants rediriger via USB et quels composants rediriger via le canal virtuel optimisé (comme l'interface audio) pour obtenir de meilleures performances.

À compter de la version 2211, les administrateurs peuvent configurer si certaines interfaces sont redirigées vers la session via la redirection USB ou non. L'utilisateur final peut maintenant sélectionner et rediriger une interface constitutive spécifique d'un périphérique USB composite vers la session de l'application Citrix Workspace via la redirection USB.

À propos de la redirection USB composite

USB 2.1 et versions ultérieures prennent en charge la notion de périphériques USB composites selon laquelle de nombreux 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 l'appareil local. Le transfert bloque également l'utilisation locale du périphérique pour toutes les applications de l'appareil local, y compris l'application Citrix Workspace.

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 de meilleures performances lorsque l'audio est envoyé via un canal audio HDX optimisé comparé à un canal générique.

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 l'appareil local, y compris l'application Citrix Workspace qui fournit des expériences HDX optimisées. Cette méthode permet de transférer les périphériques requis et de les mettre à disposition de la session distante.

Comment activer cette fonctionnalité

Vous pouvez activer cette fonctionnalité de différentes manières :

- Configuration.js
- Global App Configuration Service
- Stratégie d'administration Google

Configuration.js Pour configurer la redirection USB composite à l'aide du fichier **configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le dossier racine **ChromeApp**.
2. Modifiez le fichier **configuration.js** pour configurer la fonctionnalité de redirection USB composite.

   > **Remarques :**
   >
   > - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
   > - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
   > - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

3. Définissez **enableCompositeDeviceSplit** sur **true**.

Voici un exemple de données JSON :

```
```
{

    "features": {

        "usb": {

            "enableCompositeDeviceSplit": true
         }

     }

 }

<!--NeedCopy--> ```
```

1. Enregistrez les modifications.

 
```

> **Remarque :**
>
> - Pour désactiver la fonctionnalité, définissez l'attribut **enableCompositeDeviceSplit** sur **false**.

Global App Configuration Service Dans la configuration cloud, les administrateurs peuvent activer la fonctionnalité de redirection USB composite en définissant l'attribut **enableCompositeDeviceSplit** sur true dans le Global App Configuration Service.

Pour plus d'informations, consultez la documentation Global App Configuration Service.

Stratégie d'administration Google Lors du déploiement sur site, les administrateurs peuvent activer la fonctionnalité de redirection USB composite à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé engine_settings. Voici un exemple de données JSON :

```
{

    "features": {

        "usb": {

            "enableCompositeDeviceSplit": true
         }

     }

 }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Configuration

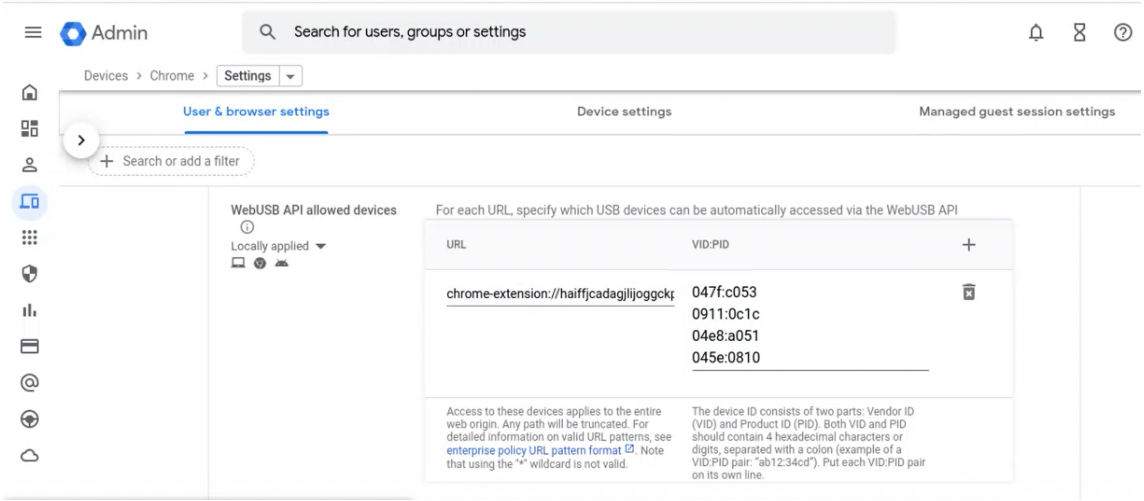
Pré-requis :

- Mettez sur liste verte les périphériques USB avec des valeurs VID:PID et activez la stratégie de redirection des périphériques USB sur Delivery Controller. Pour plus d'informations, consultez l'article CTX200825 du centre de connaissances.

- Cette fonctionnalité fonctionne sur les appareils gérés et non sur les appareils BYOD.

Pour activer la détection automatique des périphériques USB :

1. Accédez aux paramètres de la stratégie d'administration Google.
2. Sélectionnez l'option **Appareils autorisés pour l'API WebUSB**.
3. Entrez l'ID d'extension de l'application Citrix Workspace pour ChromeOS. Par exemple, chrome-extension : `//haiffjcadagjlijoggckpgfnoeiflnem`.
4. Ajoutez le VID et le PID de l'appareil comme suit :



   Après avoir ajouté les valeurs VID et PID, l'application Citrix Workspace peut désormais détecter automatiquement les périphériques dans la session.

5. Appliquez la stratégie d'administration Google. Pour en savoir plus sur les règles relatives aux appareils et obtenir des exemples de données JSON, consultez la section suivante.
6. Enregistrez les modifications.

Règles des périphériques

L'application Citrix Workspace utilise les règles des périphériques pour décider sur quels périphériques USB la redirection vers la session à distance doit être autorisée ou bloquée.

Voici l'explication des mots clés :

- **allow :** cette section inclut la liste des périphériques et de leurs interfaces enfants qui peuvent être redirigés vers la session.
- **deny :** cette section inclut la liste des périphériques et de leurs interfaces enfants qui ne peuvent pas être redirigés vers la session.

- **autoRedirect :** cette section inclut la liste des périphériques et de leurs interfaces enfants qui peuvent être redirigés automatiquement vers la session via la redirection USB.

  > **Remarque :**
  >
  > - Chaque objet représente un périphérique avec les valeurs `vid` et `pid` obligatoires du périphérique USB. Les valeurs « split » et « interfaceClass » sont facultatives.

- **vid, pid (obligatoire) :** représente l'identifiant du fournisseur (VID) et l'identifiant de produit (PID) du périphérique USB. Entrez les valeurs au format hexadécimal.
- **split (facultatif) :** attend une valeur booléenne qui indique si le périphérique doit être divisé en interfaces enfants ou non.
- **interfaceClass (facultatif) :** représente la classe d'interface USB. Les valeurs autorisées sont audio, video, hid, imprimante, storage, etc.

Voici un exemple de données JSON :

```
{

"settings": {

"value": {

"settings_version": "1.0",
"device_settings": {

"deviceRules": {


    "allow": [
        {
 "vid": "11","pid": "22",  "split":true, "interfaceClass":["audio","
    video"] }
  //split device and allow redirection of 'audio' & 'video' interfaces.
    ],

    "deny": [
        {
 "vid": "33","pid": "44" }
 ,  //deny redirection of this whole device with vid= 33 & pid = 44,
    including all of its interfaces.
        {
 "vid": "77","pid": "88","split":true,"interfaceClass":["audio"] }
     //split device and deny the redirection of 'audio' interface only;
          remaining interfaces(if any) are redirected through USB.
    ],

    "autoRedirect": [
    {
 "vid": "55","pid": "66" }
```



```
31   , //auto redirect the device when it's connected.
32      {
33   "vid": "55","pid": "66","split":true,"interfaceClass":["hid"] }
34    //split device and auto redirect only the 'hid' interface when the
         device is connected.
35      ]
36                      }
37
38                  }
39
40              }
41
42          }
43
44    }
45
46  <!--NeedCopy-->
```

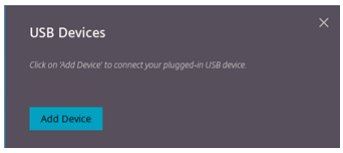
Comment utiliser cette fonctionnalité

Pour utiliser la fonctionnalité de redirection USB composite, procédez comme suit :

1. Cliquez sur l'icône USB dans la barre d'outils.

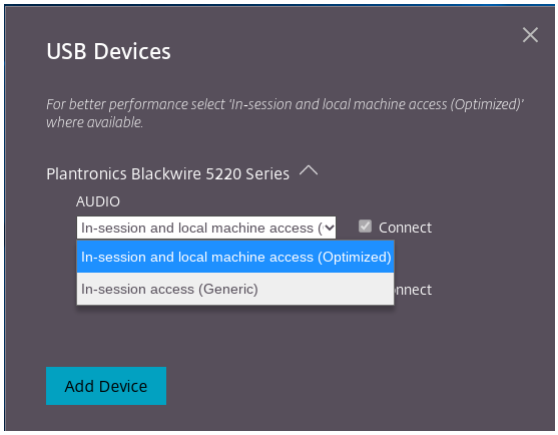
   Si aucun périphérique USB n'est connecté, la fenêtre contextuelle suivante s'affiche :

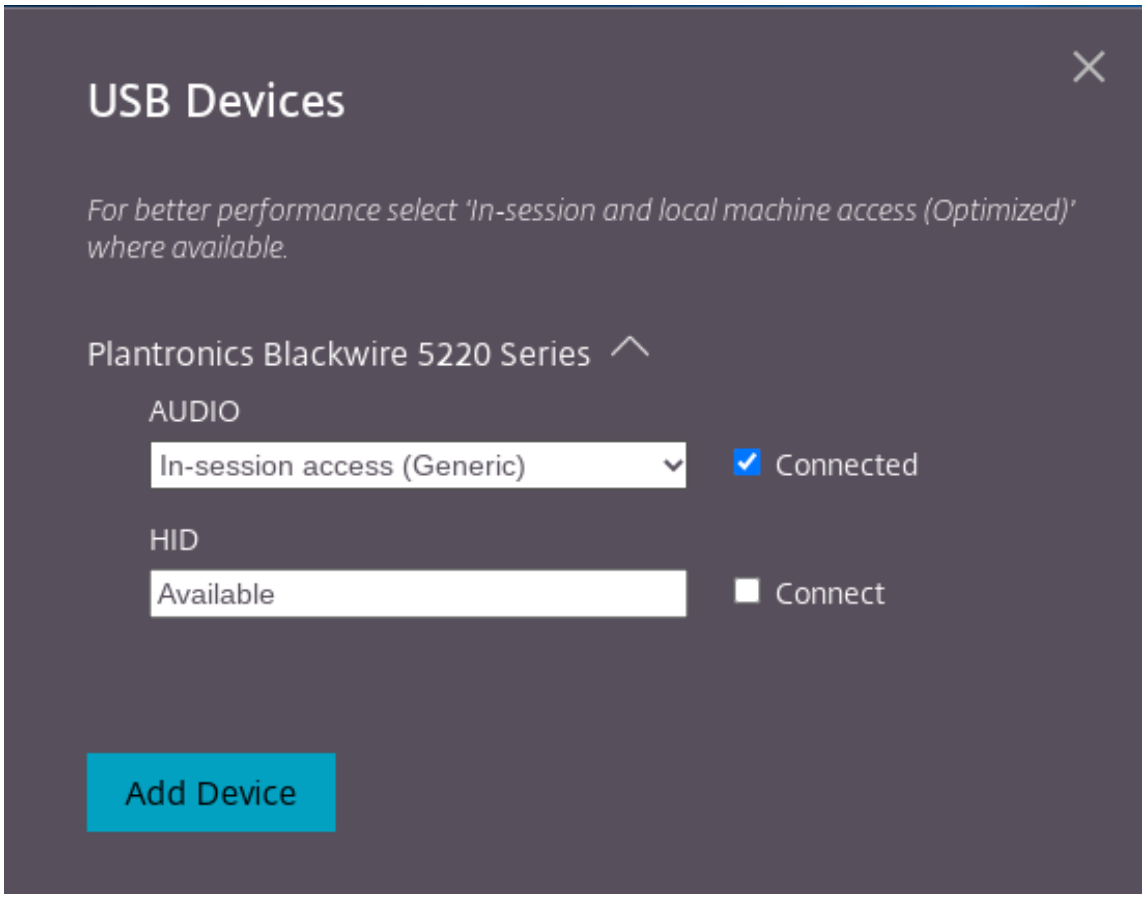
2. Connectez un périphérique USB à votre machine locale.
   La fenêtre contextuelle suivante peut apparaître :

3. Cliquez sur **Périphériques USB** pour afficher et rediriger le composant USB. Une fois la connexion établie, l'application Citrix Workspace détecte le périphérique USB. Pour chaque interface constitutive USB, vous voyez un menu déroulant. Les deux options sont les suivantes :

   - **Accès aux machines locales et dans la session (optimisé) :** sélectionnez cette option si vous souhaitez accéder au périphérique USB sur votre appareil et au cours d'une session.
   - **Accès dans la session (générique) :** sélectionnez cette option si vous souhaitez accéder au périphérique USB uniquement pendant la session.
     Pour de meilleures performances, sélectionnez l'option **Accès aux machines locales et dans la session (optimisé)**.



4. Sélectionnez **Connecter** pour rediriger l'interface.



Une fois la redirection réussie, le statut passe à **Connecté**.

Remarques :

- Pour ajouter un périphérique USB manuellement, cliquez sur **Ajouter un appareil**. La boîte de dialogue du sélecteur de Chrome s'affiche et répertorie les périphériques USB. Vous pouvez sélectionner le périphérique dans la liste.

> - Si la connexion à un périphérique USB est refusée, le message d'erreur suivant s'affiche :
>
>   Votre administrateur a bloqué le périphérique nouvellement inséré.
>   Contactez l'administrateur de votre organisation pour obtenir de l'aide.

Comment transférer l'interface USB entre les sessions

Lorsque vous cliquez sur l'icône USB dans la barre d'outils, la liste des périphériques USB connectés à vos sessions s'affiche. Si le périphérique USB est déjà utilisé dans une autre session, vous pouvez constater que le composant USB affiche l'état **Connecté à une autre session**.

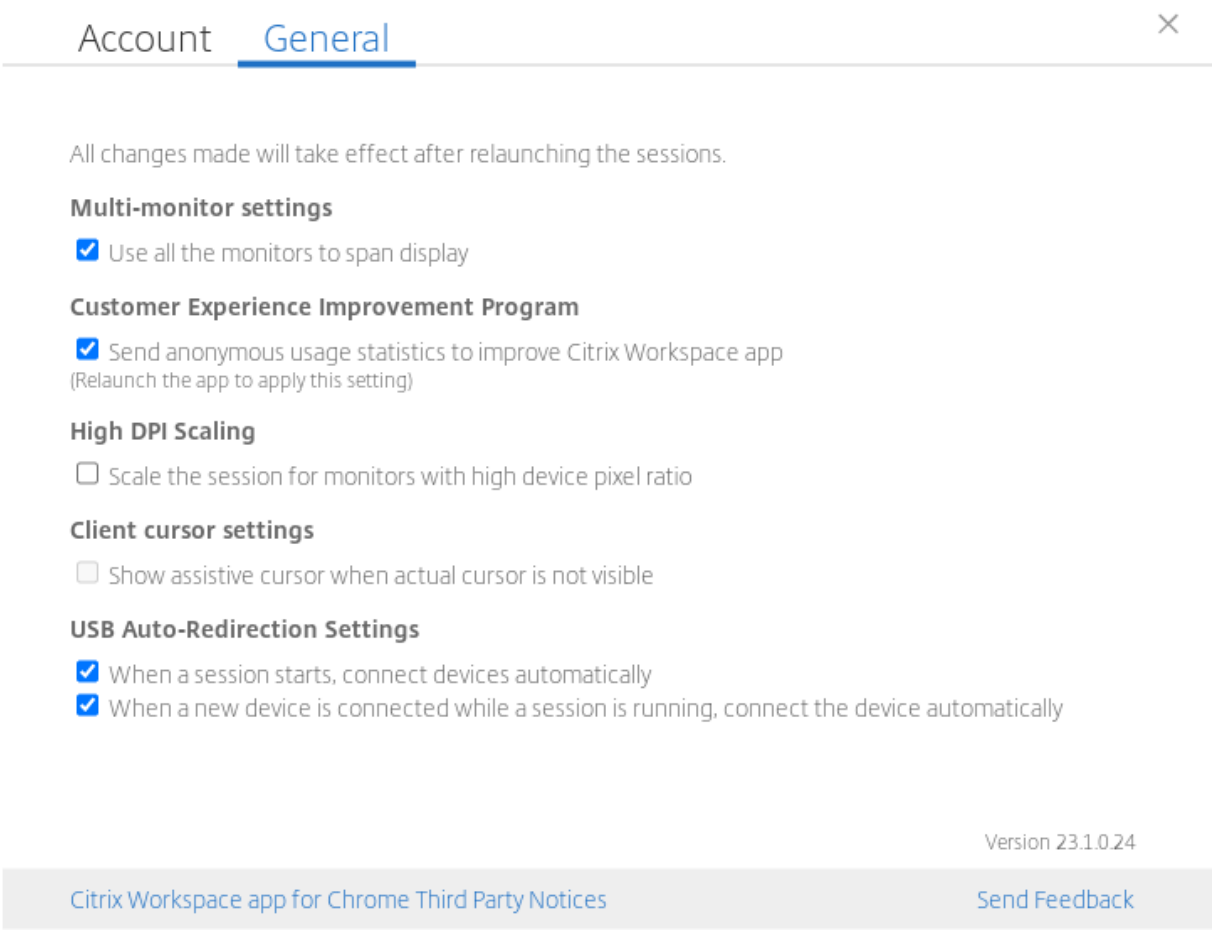
Pour rediriger vers la session en cours, sélectionnez **Connecter** en face du composant USB. Le statut change en conséquence.

Paramètres de redirection automatique USB composite

Auparavant, aucune option liée aux paramètres de redirection automatique USB ne permettait de définir les préférences de l'utilisateur. Les administrateurs contrôlant ces stratégies, l'utilisateur devait rediriger manuellement les périphériques USB requis à chaque lancement de session.

À partir de la version 2301, l'utilisateur peut sélectionner une préférence pour la redirection automatique pour n'importe quel périphérique USB au sein d'une session Virtual Desktop. L'application Citrix Workspace fournit désormais des paramètres au niveau de l'application grâce auxquels l'utilisateur peut contrôler la redirection automatique USB. L'utilisateur peut définir des préférences et enregistrer les paramètres pour tous les lancements de session.

Il existe deux options : l'une au lancement de la session et l'autre pendant que la session est en cours.



> **Remarque :**
>
> - Cette fonctionnalité prend en charge les déploiements sur site et dans le cloud, et n'est disponible que pour les utilisateurs d'appareils Chrome gérés.

Configurer la redirection des périphériques USB composites via des stratégies DDC

Auparavant, les administrateurs utilisaient les stratégies d'administration Google pour configurer la redirection USB côté client.

À partir de la version 2306, vous pouvez également configurer la redirection USB via les stratégies DDC. Les configurations via des stratégies DDC permettent aux administrateurs de définir les stratégies et les comportements de manière unifiée et centralisée. Ces stratégies s'appliquent aux déploiements sur site et dans le cloud sur les appareils et les utilisateurs gérés. Cette fonctionnalité est prise en charge sur les versions 2212 et ultérieures du VDA.

Configuration

Vous pouvez configurer cette fonctionnalité de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

> **Remarque :**
>
> - La stratégie **enableDDCUSBPolicy** est définie sur **true** par défaut.

Configuration.js Pour désactiver cette fonctionnalité à l'aide du fichier **configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le **dossier racine ChromeApp**.
2. Modifiez le fichier.

   > **Remarques :**
   >
   > - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
   > - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
   > - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

3. Définissez la valeur de **enableDDCUSBPolicy** sur **false**. Voici un exemple de données JSON :

```
"features" : {

"usb" : {

   "enableDDCUSBPolicy": false
     }

 }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Stratégie d'administration Google Pour les appareils et les utilisateurs gérés, les administrateurs peuvent désactiver cette fonctionnalité en utilisant la stratégie d'administration Google comme suit :

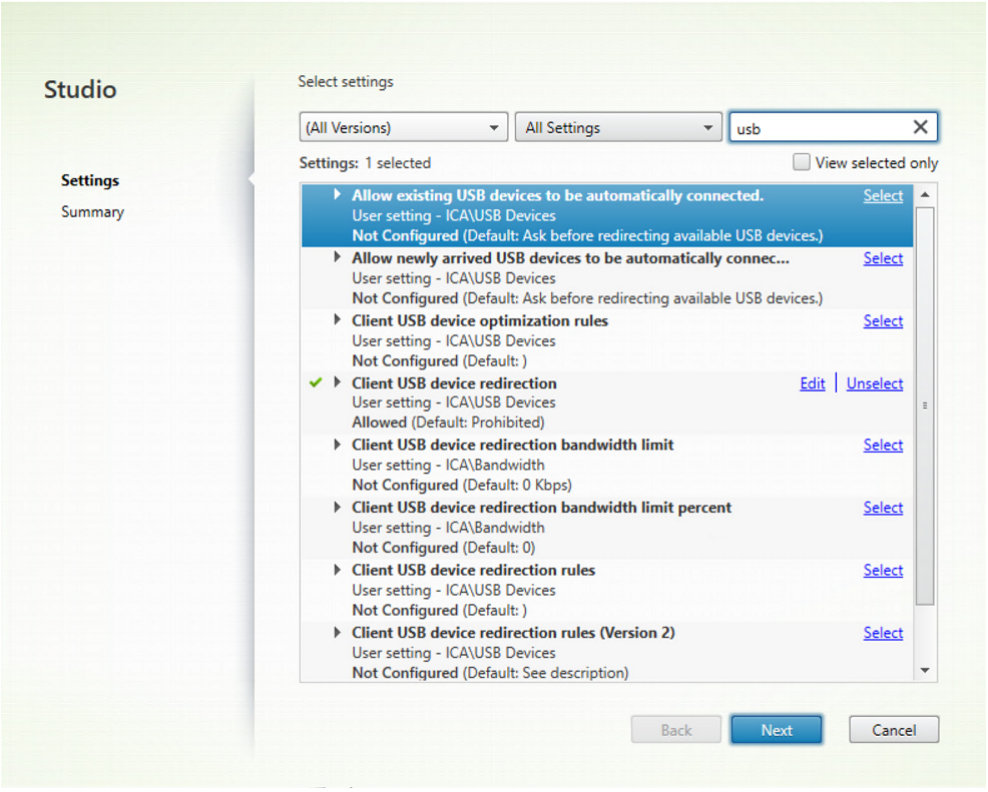
1. Connectez-vous à la stratégie d'administration Google.

2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé engine_settings.
   Voici un exemple de données JSON :

```
    "features" : {

    "usb" : {

       "enableDDCUSBPolicy": false
     }

 }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Stratégie DDC La capture d'écran suivante montre les stratégies DDC liées à la redirection USB. Cette fonctionnalité est prise en charge sur les versions 2212 et ultérieures du VDA.



Pour plus d'informations sur les stratégies DDC liées à la redirection USB, consultez les articles suivants dans la documentation de Citrix Virtual Apps and Desktops :

- Règles de redirection de périphérique USB client

- Autoriser la connexion automatique des périphériques USB existants
- Autoriser la connexion automatique des nouveaux périphériques USB
- Règles de redirection de périphérique USB client (version 2)

Redirection automatique des périphériques USB

Pour rediriger automatiquement les périphériques USB, vous devez suivre les règles relatives aux périphériques USB.
Vous pouvez configurer les règles relatives aux périphériques USB par les moyens suivants :

- Stratégie d'administration Google
- Règles de redirection de périphérique USB client (version 2)

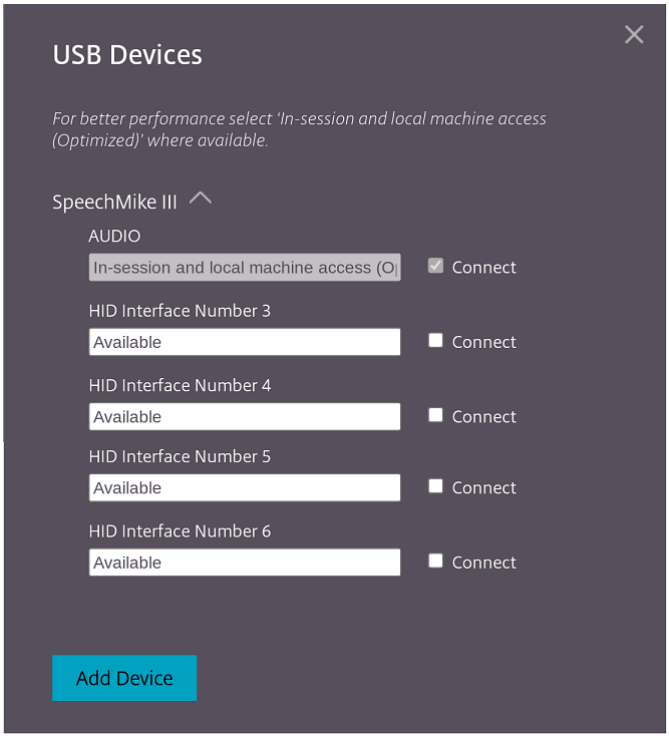
Améliorations apportées à l'interface utilisateur des périphériques USB composites

À partir de la version 2306, lorsque la configuration d'un périphérique USB composite est définie sur « split: true », l'interface utilisateur **Périphériques USB** affiche les composants en fonction des numéros d'interface plutôt que des classes d'interface.

Pour plus d'informations, consultez l'article Redirection USB composite.

Interface utilisateur

Voici un exemple :



Améliorations apportées à la redirection USB composite via des stratégies DDC

À partir de la version 2307, vous pouvez déterminer si une interface ou une classe USB composite particulière peut être redirigée vers un VDA (Virtual Delivery Agent) par défaut ou non. Si un port USB composite est connecté à l'appareil ChromeOS, la configuration **EnableDefaultAllowPolicy** vous permet de décider d'autoriser par défaut la redirection USB via des stratégies DDC. Les versions 2212 et ultérieures du VDA prennent en charge cette fonctionnalité.

Utilisation

Lorsque vous définissez l'attribut **EnableDefaultAllowPolicy** sur **true**et que vous redirigez une classe d'interface ou un numéro d'interface spécifique vers le VDA, ajoutez une règle de stratégie pour empêcher la redirection des autres classes ou numéros d'interface. Vous pouvez configurer cette fonctionnalité via la stratégie DDC (**Règles de redirection de périphérique USB client) (version 2)**.

Pour plus d'informations, consultez la section Règles de redirection de périphérique USB (version 2). De plus, vous pouvez configurer la partie de refus via la stratégie d'administration Google, mais uniquement au niveau de la classe d'interface.

Pour plus d'informations, consultez la section Améliorations apportées à l'interface utilisateur des périphériques USB composites.

Voici un exemple de configuration via la stratégie DDC **(Règles de redirection de périphérique USB client) (version 2)**, dans laquelle vous autorisez la redirection à l'interface numéro 03.

```
```
"DENY: vid=1188 pid=A301 split=01 intf=00,01,02"
<!--NeedCopy--> ```
```

Voici un exemple de configuration via la règle de stratégie d'administration Google, dans laquelle vous autorisez l'interface HID à rediriger la classe d'interface audio et à la refuser.

```
```
"deny": [
    {
 "vid":"05e9", "pid":"0428", "split":true, "interfaceClass":["audio"]
     }

]
<!--NeedCopy--> ```
```

Configuration Vous pouvez configurer cette fonctionnalité de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

> **Remarque :**
>
> - Par défaut, la stratégie **enableDefaultAllowPolicy** est définie sur **true**.

Configuration.js Pour désactiver cette fonctionnalité à l'aide du fichier **configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le **dossier racine ChromeApp**.
2. Modifiez le fichier.

   > **Remarques :**
   >
   > - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
   > - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
   > - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

3. Définissez la valeur **EnableDefaultAllowPolicy** sur **false**.

   Voici un exemple de données JSON :


```
"features" : {

   "usb" : {

   "enableDefaultAllowPolicy": false
     }

 }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Stratégie d'administration Google Pour les appareils et les utilisateurs gérés, les administrateurs peuvent désactiver cette fonctionnalité en utilisant la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils**> **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé **engine_settings**.

   Voici un exemple de données JSON :

```
'features' : {

    'usb' : {

    'enableDefaultAllowPolicy': {
 "type": "false" }

     }

   }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Redirection de port COM série

Par défaut, l'application Citrix Workspace pour ChromeOS mappe COM5 en tant que port COM série préféré pour la redirection.

Comment configurer

Pour configurer la redirection de port COM série, activez la fonctionnalité en appliquant les paramètres de la stratégie de redirection des ports de Citrix Virtual Apps and Desktops et Citrix DaaS. Pour de plus amples informations sur la redirection des ports, consultez la section Paramètres de stratégie de redirection des ports.

> **Remarque :**
>
> Par défaut, l'application Citrix Workspace pour ChromeOS mappe COM5 en tant que port COM série préféré pour la redirection.

Après avoir activé les paramètres de la stratégie de redirection du port COM série sur le VDA, configurez l'application Citrix Workspace pour ChromeOS à l'aide de l'une des méthodes suivantes :

- Stratégie d'administration Google
- Fichier configuration.js
- En changeant le mappage par défaut en émettant une commande dans une session ICA active.

En utilisant une stratégie d'administration Google pour configurer la redirection de port COM
Utilisez cette méthode pour rediriger le port COM série en modifiant le fichier de stratégie.

> **Conseil :**
>
> Citrix vous recommande de configurer le port COM à l'aide du fichier de stratégie uniquement lorsque l'application Citrix Workspace pour ChromeOS est reconditionnée.

Modifiez la stratégie d'administration Google en incluant ce qui suit :

```
    {

      "settings": {

                "Value": {

                 "settings_version": "1.0",
                 "store_settings": {

                 "rf_web": {

                 "url": "<http://YourStoreWebURL>"
                   }

                   }
,
                  "engine_settings":{

                  "features" : {
```



```
20
21                  "com" : {
22
23        "portname" : "<COM4>", where COM4 indicates the port number that
           is set by the administrator.
                                                }
24
25                                            }
26
27                                            }
28
29                                            }
30
31                                            }
32
33                                           }
34
35
36   <!--NeedCopy-->
```

Liste des paramètres de nom de port COM série ainsi que leurs descriptions :

- « portname » : numéro de port pour le canal virtuel COM (série). Par défaut, la valeur est COM5.

En utilisant le fichier configuration.js pour configurer la redirection de port COM Utilisez cette méthode pour rediriger le port COM série en modifiant le fichier **configuration.js**. Localisez le champ portname dans le fichier configuration.js et modifiez la valeur en changeant le numéro de port.

Par exemple :

```
1  "com" :{
2
3
4  "portname" : "COM4"
5
6   }
7
8  <!--NeedCopy-->
```

> **Remarque :**
>
> Citrix vous recommande d'utiliser le fichier configuration.js pour configurer la redirection de port série uniquement lorsque l'application Citrix Workspace pour ChromeOS est reconditionnée et republiée depuis StoreFront.

En émettant une commande dans une session ICA pour configurer la redirection de port COM Utilisez cette méthode pour rediriger le port COM série. Exécutez la commande suivante dans une session ICA active :


```
    net use COM4 : \Client\COM5
<!--NeedCopy-->
```

> **Conseil :**
>
> Dans l'exemple ci-dessus, COM4 est le port série préféré utilisé pour la redirection.

Paramètres d'alimentation

May 16, 2024

Paramètre d'éveil

L'application Citrix Workspace pour ChromeOS maintient les appareils Chromebook gérés éveillés même lorsque les utilisateurs ne sont pas actifs.

Le paramètre d'éveil est désactivé par défaut.

Comment configurer

Pour l'activer, modifiez la stratégie **Google Admin Console** et définissez la valeur de la propriété **keep_awake_level** sous **power_settings** sur **"system"** ou **"display"** et redémarrez la session.

Le niveau **system** maintient le système éveillé, mais permet à l'écran d'être assombri ou éteint. Le niveau **display** maintient le système éveillé et actif.

```
{

 "settings": {

     "Value": {

         "settings_version": "1.0",
         "power_settings": {

             "keep_awake_level":  ” system ”  or  “ display ”
              }

            }

         }

     }

```



```
<!--NeedCopy-->
```

Liste des paramètres d'alimentation ainsi que leurs descriptions :

- « keep_awake_level » : maintient les appareils éveillés même lorsque les utilisateurs ne sont pas actifs. Vous pouvez choisir l'une des deux valeurs suivantes :
  - « system » : maintient le système éveillé, mais permet à l'écran d'être assombri ou éteint.
  - « display » : maintient le système éveillé et actif.

> **Remarque :**
>
> Pour le mode Kiosque, assurez-vous que le paramètre **Autoriser l'application à gérer l'alimentation** dans la **console d'administration Google** est désactivé.

Impression

May 16, 2024

Impression PDF

Le pilote d'imprimante universel PDF Citrix permet aux utilisateurs d'imprimer les documents ouverts avec des applications hébergées ou des applications exécutées sur des bureaux virtuels mis à disposition par XenDesktop 7.6 et XenApp 7.6 ou version supérieure. Lorsqu'un utilisateur sélectionne l'option Imprimante PDF Citrix, le pilote convertit le fichier au format PDF et transfère le PDF sur l'appareil local. Le fichier PDF s'ouvre alors dans une nouvelle fenêtre pour visualisation et impression.

Lorsque vous imprimez un document ouvert avec une application hébergée ou une application exécutée sur un bureau virtuel, vous pouvez imprimer le document au format PDF. Vous pouvez transférer le PDF sur l'appareil local pour l'afficher et l'imprimer à partir d'une imprimante connectée localement. Le fichier n'est pas stocké dans l'application Citrix Workspace pour ChromeOS.

> **Important**
>
> L'impression PDF locale est uniquement prise en charge sur XenApp et XenDesktop 7.6 ou versions ultérieures.

Comment configurer

Exigences Vous avez besoin d'un compte MyCitrix pour accéder à la page de téléchargement de l'application Citrix Workspace pour ChromeOS.

Pour autoriser les utilisateurs à imprimer des documents ouverts avec des applications ou des bureaux hébergés :

1. Téléchargez l'imprimante PDF Citrix et installez le pilote d'imprimante universelle PDF Citrix sur chaque machine VDA mettant à disposition des bureaux ou applications pour les utilisateurs de l'application Citrix Workspace. Après l'installation du pilote d'imprimante, redémarrez la machine.
2. Dans Citrix Studio, sélectionnez le **nœud Stratégie** dans le panneau gauche et créez une stratégie ou modifiez une stratégie existante.

   Pour de plus amples informations sur la configuration des stratégies Citrix Virtual Apps and Desktops, consultez la section Stratégies.
3. Définissez le paramètre de stratégie Créer automatiquement l'imprimante universelle PDF sur **Activé**.

Prise en charge des imprimantes réseau

Auparavant, l'option Imprimante PDF Citrix était utilisée pour imprimer à partir de la session de bureau virtuel. Le pilote d'imprimante convertissait le fichier au format PDF et le transférait sur l'appareil local. Le fichier PDF s'ouvrait alors dans une nouvelle fenêtre pour visualisation et impression.

À compter de la version 2305, l'application Citrix Workspace pour ChromeOS prend en charge l'impression réseau. Les utilisateurs peuvent consulter la liste des imprimantes connectées à leur Chromebook au cours de la session. Les utilisateurs peuvent sélectionner une imprimante directement sans générer de fichiers PDF intermédiaires sur l'appareil local. Cette fonctionnalité est prise en charge sur les :

- VDA version 2112 et versions ultérieures
- ChromeOS version 112 et versions ultérieures

> **Remarque :**
>
> - Par défaut, cette fonctionnalité est activée et seul le format PDF pour l'impression de métafichiers est pris en charge.

Pour plus d'informations, consultez les articles suivants :

- Gérer les imprimantes et les pilotes d'impression de votre environnement dans la documentation Citrix Virtual Apps and Desktops
- Article du centre de connaissances How to use Citrix Policy to Set a Default Session Printer - CTX232031

- Article du centre de connaissances Citrix Printing Quick Start Guide and Default configuration - CTX227534

Configuration

Vous pouvez désactiver cette fonctionnalité de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

> **Remarque :**
>
> - Au préalable, l'administrateur informatique doit activer la stratégie **Créer automatiquement l'imprimante universelle générique** sur le Delivery Controller (DDC). Pour plus d'informations, consultez Paramètres de stratégie d'imprimantes clientes dans la documentation de Citrix Virtual Apps and Desktops.

Configuration.js Pour désactiver cette fonctionnalité à l'aide du fichier **configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le dossier racine ChromeApp.

   > **Remarques :**
   >
   > - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
   > - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
   > - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

2. Modifiez le fichier **configuration.js** et définissez la valeur par défaut de **networkPrinting** sur false. Voici un exemple de données JSON :

```
{

  "features": {

     " networkPrinting ": {

          "enable": false
                      }

     }

```



```
 }

<!--NeedCopy-->
```

3. Enregistrez les modifications.

Stratégie d'administration Google Les administrateurs informatiques peuvent désactiver cette fonctionnalité en utilisant la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé **engine_settings**. Voici un exemple de données JSON :

```
{

   "features": {

        " networkPrinting ": {

            "enable": false
                 }

         }

 }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

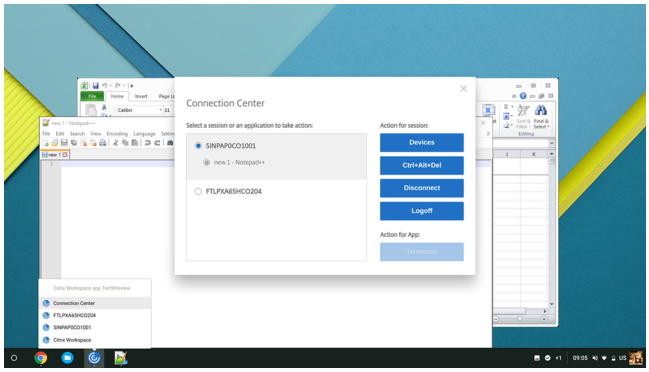
Expérience fluide

May 16, 2024

Centre de connexion

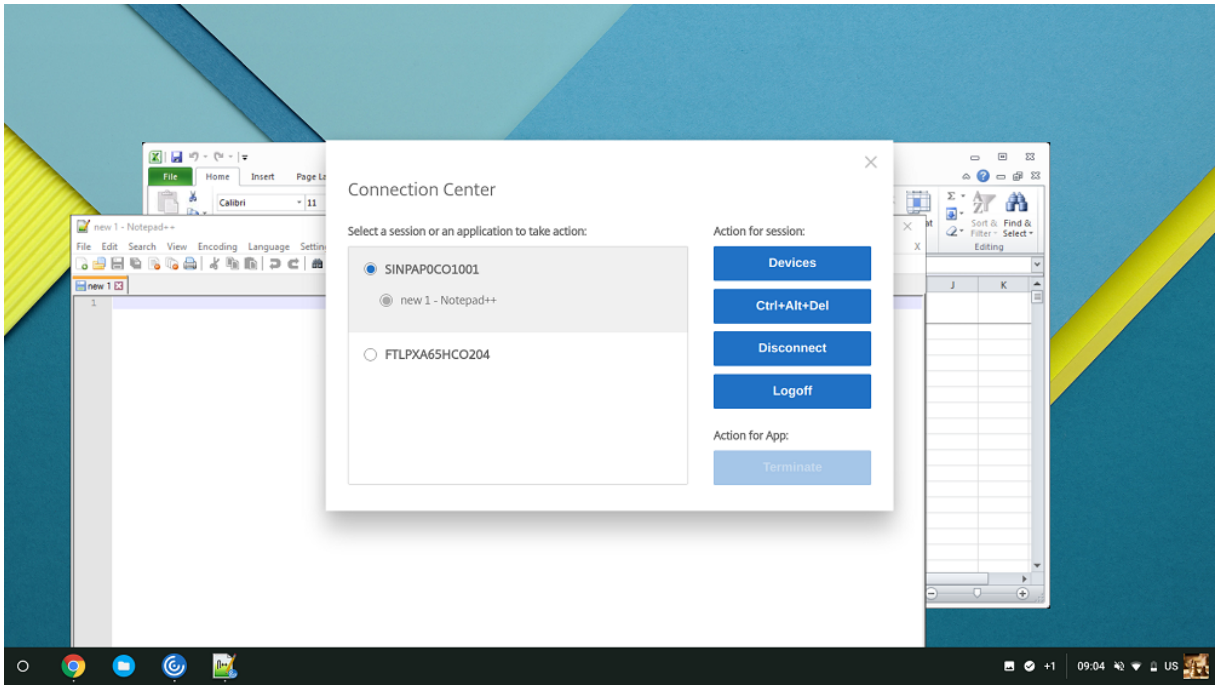
Le Centre de connexion facilite la gestion des applications lors de sessions fluides en fournissant une barre des tâches qui répertorie toutes les applications ouvertes.

Pour lancer le Centre de connexion, cliquez avec le bouton droit sur l'icône de l'application Citrix Workspace et sélectionnez **Centre de connexion**.



Dans le Centre de connexion, vous pouvez sélectionner une application et :

1. Afficher les périphériques.
2. Envoyer la commande Ctrl+Alt+Suppr.
3. Déconnecter une session.
4. Fermer une session.



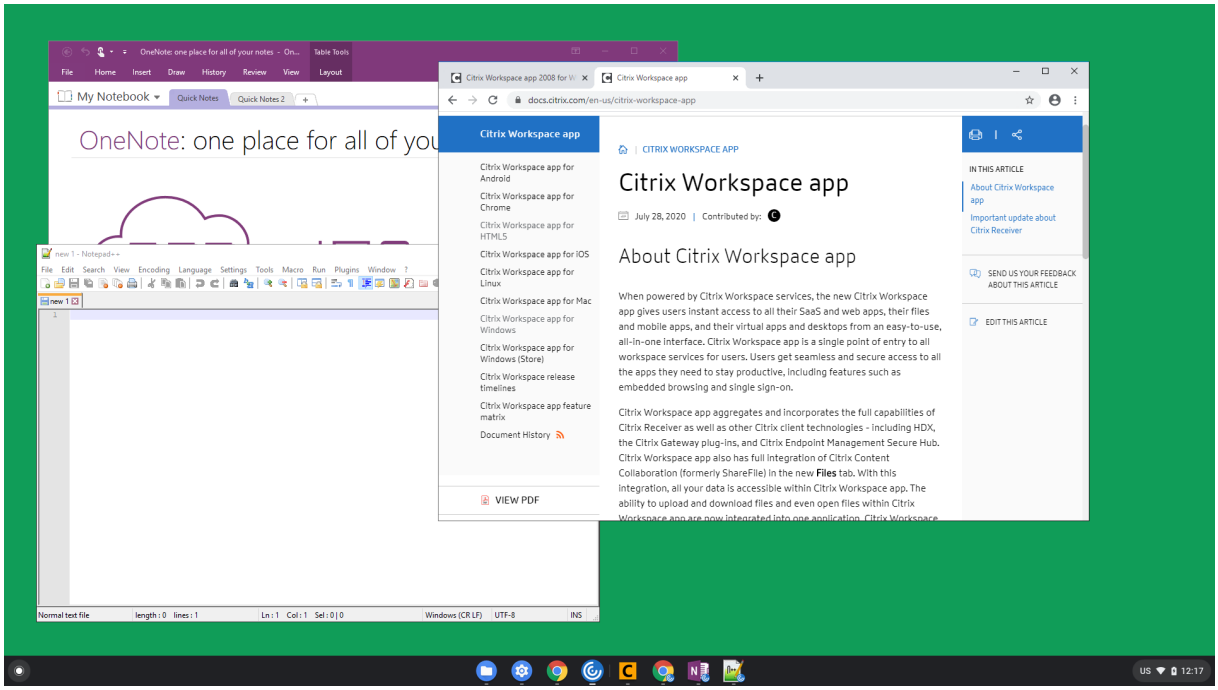
Vous pouvez également utiliser le Centre de connexion pour fermer une application en sélectionnant le bouton radio en regard d'une application et en sélectionnant **Terminer**.

Intégration de fenêtres transparentes

En permettant l'intégration, au sein d'une session active, de multiples applications hébergées dans des fenêtres séparées, l'application Citrix Workspace pour ChromeOS améliore l'expérience utilisateur. Grâce à cette fonctionnalité, l'application Citrix Workspace pour ChromeOS vous permet de dé-

marrer des applications dans une interface utilisateur indépendante plutôt que de démarrer toutes les applications d'une session dans une seule fenêtre.

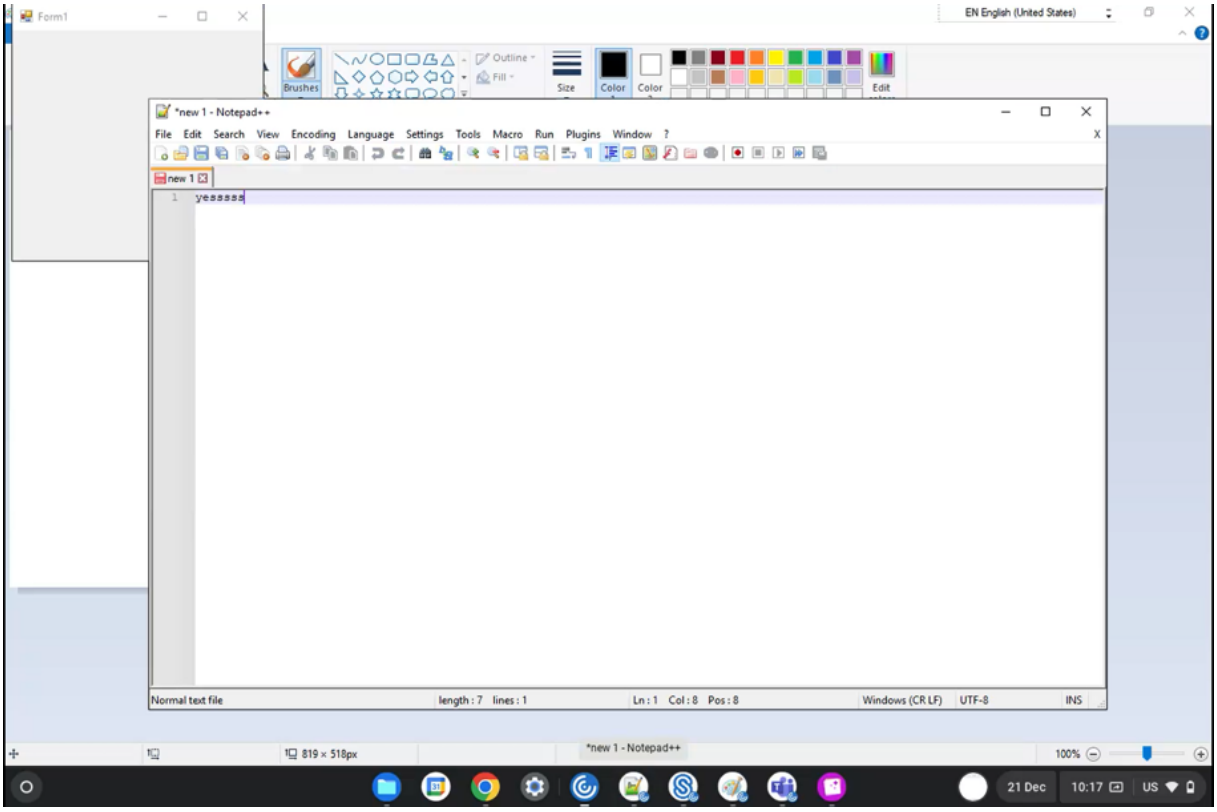
Les applications transparentes peuvent être hébergées dans des fenêtres séparées. Grâce à cette fonctionnalité, les applications distantes sont exécutées en natif sur la machine cliente.



Limitations des fonctionnalités :

- Des entrées supplémentaires apparaissent dans la barre des tâches de Chrome. Cliquez sur l'une de ces entrées pour mettre la session sélectionnée au premier plan.
- Toutes les applications ouvertes dans une session active s'exécutent dans une seule fenêtre. La sélection d'une application dans une session active ramène cette fenêtre au premier plan ainsi que toutes les autres applications appartenant à cette session.

Utilisez l'icône d'application transparente dans la barre des tâches pour passer rapidement d'une application à l'autre :



> **Conseil :**
>
> Toutes les applications d'une session sont exécutées dans une seule fenêtre. Lorsque vous déplacez une application sur un second moniteur, toutes les applications qui font partie de cette session sont déplacées vers le second moniteur.

Changement d'applications

Affiche les applications ouvertes dans une session.

> **Remarque :**
>
> Cette option est uniquement disponible pour le mode kiosque.

App Switcher permet aux utilisateurs de basculer entre plusieurs applications exécutées dans la même session. L'application prioritaire est mise en surbrillance.

Comment configurer

Pour procéder à la configuration, utilisez la stratégie d'administration Google en incluant les éléments suivants :


```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "ui": {

                        "appSwitcher": {

                            "showTaskbar": true,
                            "showIconsOnly": false,
                            "autoHide": false
                                        }

                           }

                    }

         }

     }

 }


<!--NeedCopy-->
```

Liste des options de basculement entre applications ainsi que leurs descriptions :

- **showTaskbar** : si ce paramètre est défini sur « true », la barre des tâches apparaît en bas de la session. Pour masquer la barre des tâches, définissez cette option sur « false ».
- **showIconsOnly** : si le paramètre est défini sur « true », les icônes de la barre des tâches apparaissent. Par défaut, le paramètre est défini sur « false ».
- **autoHide** : si le paramètre est défini sur « true », la barre des tâches est automatiquement masquée. Par défaut, le paramètre est défini sur « false ».

Icônes de la barre des tâches

Les applications et les bureaux configurés à l'aide de Citrix Virtual Apps and Desktops et Citrix DaaS dans une session active sont affichés en tant qu'applications distinctes. Vous pouvez voir ces applications dans la barre des tâches (étagère) de l'appareil ChromeOS. Cette fonctionnalité s'applique aux applications et bureaux publiés. Le comportement de cette fonctionnalité est similaire à l'expérience de la barre des tâches qui est fournie par le système d'exploitation Windows.

Cette fonctionnalité est activée par défaut.

Comment configurer

Configuration des icônes de barre des tâches à l'aide d'une stratégie d'administration Google

> **Remarque :**
>
> Citrix recommande d'utiliser cette méthode uniquement lorsque l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.

1. Connectez-vous à la console d'administration Google.
2. Accédez à **Gestion des appareils > Gestion de Chrome > Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier `policy.txt`.

```
//Preferences for chrome app
'appPrefs':{
    'chromeApp':{
        'seamless' : {
            'showInShelf' : false
        },
```

4. Cliquez sur **Enregistrer** et fermez le fichier.

Configuration des icônes de barre des tâches à l'aide du fichier `web.config` de StoreFront

> **Remarque :**
>
> Citrix recommande d'utiliser la méthode du fichier `web.config` uniquement à des fins de configuration. Vous pouvez utiliser cette méthode lorsque la version de magasin de l'application Citrix Workspace pour ChromeOS est utilisée.

1. Ouvrez le fichier `web.config` du site Citrix Receiver pour Web. Ce fichier se trouve dans `C:\inetpub\wwwroot\Citrix\\\\<Storename>Web`, où `Storename` est le nom spécifié pour le magasin lors de sa création.
2. Localisez le champ **chromeAppPreferences** et définissez sa valeur en tant que chaîne JSON.

Par exemple :

```
chromeAppPreferences='{

    "seamless":{

        "showInShelf":false
         }

         }

<!--NeedCopy-->
```


Configuration des icônes de barre des tâches à l'aide du fichier configuration.js Le fichier **configuration.js** se trouve dans le dossier racine **ChromeApp**. Accédez directement à ce fichier pour modifier l'application Citrix Workspace.

> **Remarque :**
>
> Des informations d'identification de niveau administrateur sont nécessaires pour modifier le fichier configuration.js ; après la modification du fichier, reconditionnez l'application pour que les modifications prennent effet.

Pour modifier la barre des tâches de ChromeOS à l'aide du fichier configuration.js :

1. Ouvrez le fichier configuration.js et définissez l'attribut **showInShelf** sur true.

Par exemple :

```
//Preferences for chrome app
'appPrefs':{
    'chromeApp':{
        'seamless' : {
            'showInShelf' : false
        },
```

Limitations des fonctionnalités :

1. Lorsque plusieurs instances de la même application sont lancées, l'icône de l'application n'est pas superposée et s'affiche en tant que deux icônes distinctes. Par exemple, deux instances de Bloc-notes affichent deux icônes Bloc-notes dans la barre des tâches.
2. L'épinglage d'applications n'est pas pris en charge.

Expérience de session

June 18, 2024

Mode plein écran

Comment configurer

Pour configurer votre session de bureau pour toujours l'ouvrir en mode plein écran, modifiez la stratégie d'administration Google en incluant ce qui suit :

> **Remarque :**
>
> - Par défaut, les sessions de bureau s'ouvrent dans des fenêtres maximisées où la valeur « window state » est définie sur « maximized ».

```
{


      "settings": {


                      "Value": {

                      "settings_version": "1.0",
                      "engine_settings": {

                      "ui": {

                      "sessionsize": {

                      "windowstate": "fullscreen"
                                }

                                        }

                                                }

                              }

                  }

 }

<!--NeedCopy-->
```

Taille de session

Comment configurer

Le paramètre de taille de session vous permet de personnaliser les résolutions d'une session. Modifiez la stratégie d'administration Google en incluant ce qui suit :

```
{

    "settings": {

      "Value": {

            "settings_version": "1.0",
```



```
            "engine_settings": {

            "ui": {

                "sessionsize" : {

                    "minwidth" : 240,
                    "minheigh" : 120,
                    "available" : {

                            "default" : "Fit_To_Window",
                            "values" : [
                                        "Fit_To_Window",
                                        "Use_Device_Pixel_Ratio",
                                        "1280x800",
                                        "1440x900",
                                        "1600x1200"
                                    ]
                        }

                    }

                }

            }

    }

}


<!--NeedCopy-->
```

Liste des différents paramètres de résolution ainsi que leurs descriptions :

- **minwidth** = 240 : largeur minimale pour les sessions.
- **minheight** = 120 : hauteur minimale pour les sessions.
- **available** : options permettant de définir des préférences de résolution pour les sessions.
  - **default** : la valeur que vous définissez s'applique à la résolution par défaut. Par défaut, la valeur est définie sur « Fit_To_Window ». Vous pouvez modifier la valeur par défaut comme suit :
    - **values** : les autres valeurs de résolution sont :
      - **Fit_To_Window** : valeur de résolution par défaut disponible. Elle correspond à la taille de la fenêtre pour émuler différentes résolutions d'écran.
      - **Use_Device_Pixel_Ratio** : met à l'échelle les sessions en fonction du DPI de l'appareil.
      - **1280x800** : définit la taille de la session sur 1 280*800 pixels.

- **1440x900** : définit la taille de la session sur 1 440*900 pixels.
- **1600x1200** : définit la taille de la session sur 1 600*1 200 pixels.

Net Promoter Score

L'application Citrix Workspace pour ChromeOS vous invite à répondre périodiquement à des enquêtes Net Promoter Score (NPS). L'invite vous demande d'évaluer votre expérience avec l'application Citrix Workspace pour ChromeOS. Nous utilisons les scores NPS pour mesurer la satisfaction de la clientèle et pour améliorer davantage l'application.

Vous pouvez évaluer votre expérience sur une échelle de 1 à 5, 5 indiquant que vous êtes satisfait.

Comment configurer

Pour configurer NPS, utilisez la stratégie d'administration Google en incluant les éléments suivants. Si l'option est définie sur « true », l'utilisateur peut fournir une évaluation.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "ui": {

                        "netPromoters": true
                           }

                 }

          }

     }

 }


<!--NeedCopy-->
```

Lancement automatique des sessions ICA

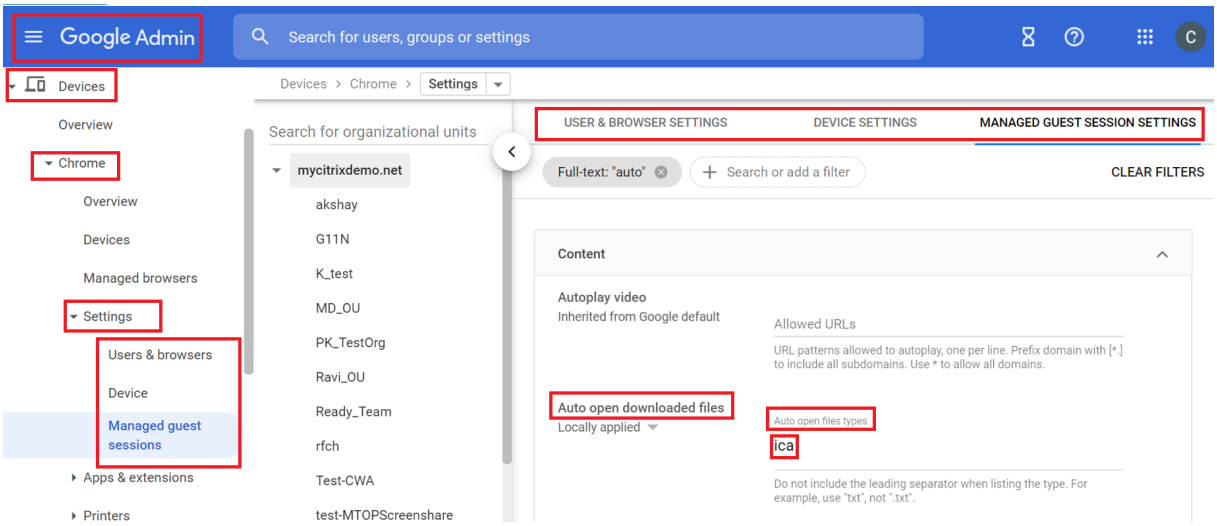
L'application Citrix Workspace pour ChromeOS prend en charge le lancement automatique des sessions ICA (Independent Computing Architecture) sur les appareils ou utilisateurs gérés par Google.

Avec cette fonctionnalité, vous pouvez accéder à des ressources à distance depuis Citrix Workspace pour Web. Le fichier ICA téléchargé démarre automatiquement avec l'application Citrix Workspace pour ChromeOS, s'il a été installé sur l'appareil. Auparavant, vous pouviez télécharger uniquement des fichiers ICA et ouvrir les fichiers manuellement afin de démarrer les ressources. De plus, le fichier ICA n'était pas supprimé lors de l'ouverture et restait sur l'appareil. Maintenant, le fichier ICA est automatiquement supprimé de l'appareil, une fois qu'il a été utilisé pour lancer automatiquement la session.

Comment configurer

Pour configurer le lancement automatique des sessions ICA, connectez-vous en tant qu'administrateur et effectuez les opérations suivantes :

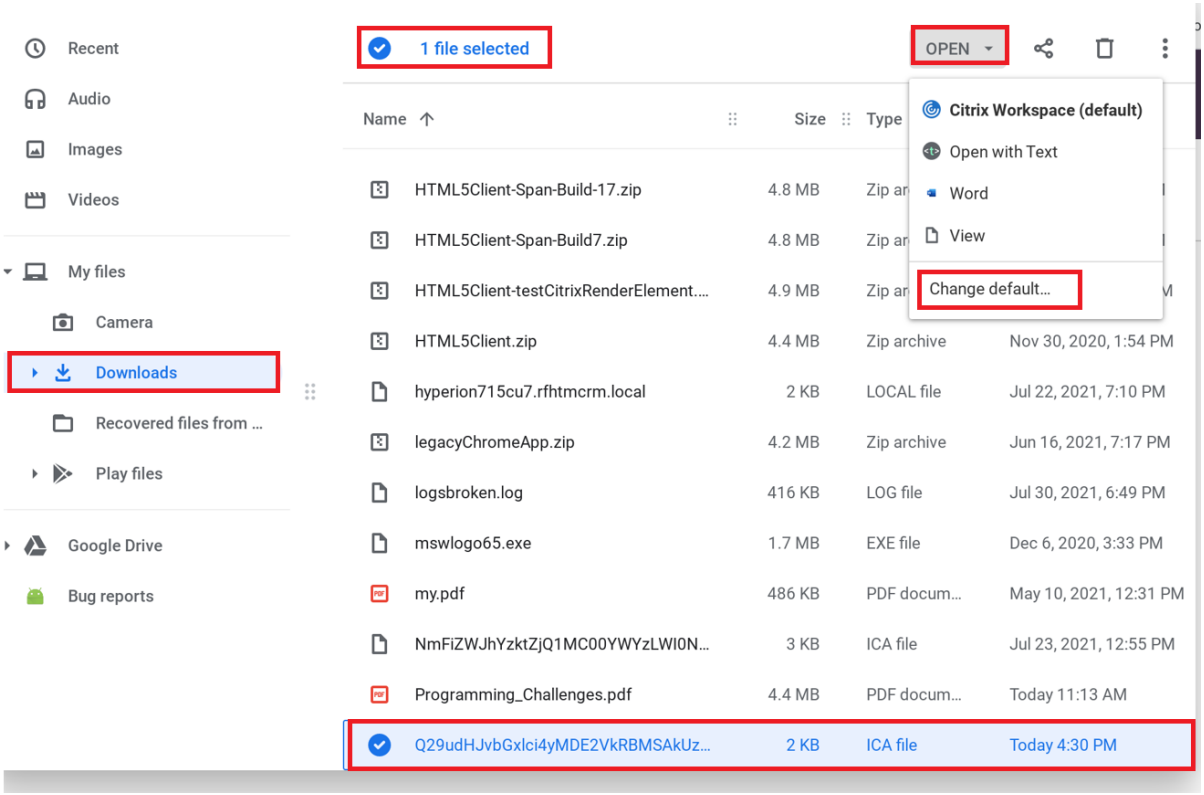
1. Connectez-vous à la console d'**administration Google**.
2. Dans la **console d'administration Google**, sélectionnez **Appareils > Chrome > Paramètres**.
3. Ensuite, sous **Paramètres**, sélectionnez **Utilisateurs et navigateurs**, **Appareil** et **Paramètres des sessions Invité gérées** (le cas échéant). Définissez l'option **Ouvrir automatiquement les fichiers téléchargés** et ajoutez **ica** sous **Ouvrir automatiquement les types de fichiers** pour **Paramètres des utilisateurs et du navigateur**, **Paramètres de l'appareil** et **Paramètres des sessions Invité gérées**, le cas échéant (pour les utilisateurs et les appareils gérés).



Ensuite, demandez à vos utilisateurs d'associer le fichier ICA à l'application Citrix Workspace pour ChromeOS sur leurs appareils ChromeOS, comme suit :

1. Ouvrez le **gestionnaire de fichiers** et accédez au fichier ICA précédemment téléchargé.
2. Cliquez sur le fichier ICA.
3. Sur le côté droit de la barre de navigation, cliquez sur **Ouvrir** et sélectionnez la flèche en regard de l'option.

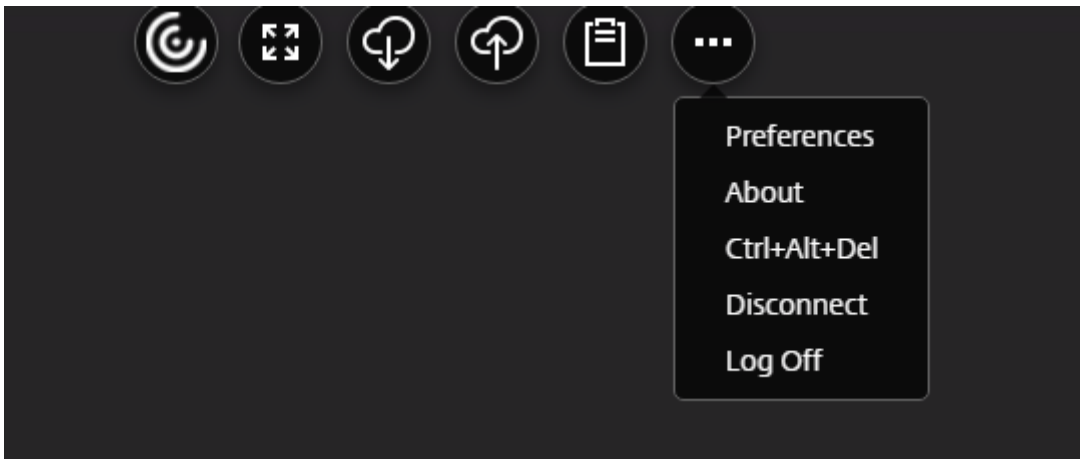
4. Ensuite, sélectionnez **Modifier la valeur par défaut**.
5. La liste des applications disponibles s'affiche.
6. Sélectionnez **Citrix Workspace**.



Barre d'outils et boîtes de dialogue en session

La barre d'outils en session est une barre d'outils flottante qui peut être déplacée n'importe où sur l'écran. L'icône de l'application Citrix Workspace est intégrée à la barre d'outils. Une barre d'outils personnalisée améliore l'expérience utilisateur. Cette amélioration fournit de nouvelles options accessibles depuis la barre d'outils qui sont destinées à faciliter les tâches courantes telles que :

- le basculement en mode plein écran ;
- le chargement ou le téléchargement de fichiers ;
- la copie de contenu depuis une session active sur le presse-papiers afin de faciliter le partage entre sessions ;
- l'accès à plus d'options.



> **Remarque :**
>
> Sur les appareils tactiles, l'icône de l'application Citrix Workspace apparaît en haut au centre pour indiquer la barre d'outils flottante lors des sessions de bureau. Un bouton de menu représentant la barre d'outils flottante se convertit en icône Citrix Workspace lorsque vous déplacez votre curseur vers celui-ci.

Comment configurer

La barre d'outils est activée par défaut.

Pour masquer ou personnaliser des éléments de barre d'outils individuels, modifiez la stratégie d'administration Google en incluant les éléments suivants :

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                "ui" : {

                    "toolbar" : {

                            "menubar" :true,
                            "usb": true,
                            "fileTransfer":true,
                            "about":true,
                            "lock":true,
                            "disconnect":true,
                            "logoff":true,
                            "fullscreen":true,
                            "multitouch":true,
```



```
                                "preferences":true,
                                "gestureGuide":true
                                      }

                           }

                     }

           }

      }

 }


<!--NeedCopy-->
```

Liste des paramètres de la barre d'outils en session ainsi que leurs descriptions :

- **menubar** : la barre d'outils apparaît lorsqu'elle est définie sur **true** et est masquée lorsqu'elle est définie sur **false**.
- **usb** : ouvre la boîte de dialogue Périphériques USB. Contient la liste des périphériques pouvant être redirigés vers la session. Pour rediriger un périphérique USB, sélectionnez un périphérique approprié et cliquez sur **Connexion**.
- **fileTransfer** : fonctionnalité de transfert de fichiers sécurisée entre une machine utilisateur et une session Citrix Virtual Apps and Desktops et Citrix DaaS. Vous pouvez charger et télécharger des fichiers vers et depuis une session et accéder facilement aux données.
- **about** : affiche la page des licences tierces et fournit le numéro de version.
- **lock** : envoie la commande « Ctrl+Alt+Suppr » à la session.
- **disconnect** : déconnecte la session.
- **logoff** : ferme la session.
- **fullscreen** : règle la session en mode plein écran. Si la session est connectée en mode multi-moniteurs, l'icône multi-moniteurs apparaît dans la barre de menus plutôt qu'une icône plein écran. Une icône **Restaurer** apparaît dans la barre de menus en mode plein écran. Pour restaurer le mode optimisé, cliquez sur **Restaurer** dans l'interface utilisateur de la barre d'outils.
- **multitouch** : ce mode configure un accès distant à tous les gestes de la session virtuelle ; l'application fonctionne selon les gestes qu'elle prend en charge.
- **preferences** : fournit des options pour personnaliser le programme CEIP et les paramètres de résolution d'affichage.
- **gestureGuide** : fournit le guide des gestes en mode tactile.

Pour masquer la configuration de la barre d'outils à l'aide du fichier configuration.js :

Le fichier `configuration.js` se trouve dans le dossier **racine de ChromeApp**. Modifiez ce fichier directement pour apporter des modifications à l'application Citrix Workspace pour ChromeOS.

1. Ouvrez le fichier configuration.js et définissez l'attribut menubar sur false.

Vous pouvez également masquer une icône individuelle pour éviter qu'elle ne s'affiche dans la barre d'outils. À titre d'exemple, pour masquer le bouton Ctrl+Alt+Suppr dans la barre d'outils :

1. Ouvrez le fichier configuration.js et définissez l'attribut lock sur false.

> **Remarques :**
>
> - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
> - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
> - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

Partage de session

Pour le partage de session, les applications doivent être hébergées sur la même machine et doivent être configurées en mode de fenêtre transparente avec les mêmes paramètres de taille de fenêtre, nombre de couleurs et cryptage. Le partage de session est activé par défaut lorsqu'une application hébergée est mise à disposition.

Indicateur d'état de la batterie

L'état de la batterie de l'appareil s'affiche dans la zone de notification d'une session de bureau virtuel. Auparavant, l'indicateur d'état de la batterie n'était pas visible pendant la session, ce qui entraînait parfois une perte de productivité lorsque l'ordinateur portable s'éteignait après que la batterie soit épuisée.

Cette fonctionnalité est prise en charge uniquement sur les versions 7.18 et ultérieures du VDA.

> **Remarque :**
>
> - Avec le VDA exécuté sur Microsoft Windows 10, l'indicateur d'état de la batterie peut prendre environ 1 ou 2 minutes avant d'apparaître.

Continuité du service

La fonction Continuité du service supprime ou réduit la dépendance à l'égard de la disponibilité des composants impliqués dans le processus de connexion. Vous pouvez lancer des sessions Citrix Virtual Apps and Desktops et Citrix DaaS quel que soit l'état d'intégrité des services cloud. En d'autres termes, la continuité du service vous permet de vous connecter aux applications et aux bureaux DaaS en

cas de panne. Pour ce faire, votre appareil doit maintenir une connexion réseau à un emplacement de ressources.

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

> **Remarques :**
>
> - La fonctionnalité de continuité de service est désactivée.
> - Si vous avez précédemment activé la fonctionnalité de continuité de service et que vous utilisez une ancienne version de l'application Citrix Workspace pour ChromeOS, il est possible que vous ne puissiez pas utiliser la fonctionnalité de continuité de service. Pour activer cette fonctionnalité, il est recommandé de mettre à jour l'application Citrix Workspace vers la dernière version, 2402.1 ou ultérieure, et de suivre les instructions de l'article CTX632723 du Centre de connaissances.

Configuration

Vous pouvez activer la fonctionnalité de continuité de service de la manière suivante :

- Stratégie d'administration Google

Stratégie d'administration Google Pour les appareils et les utilisateurs gérés, les administrateurs peuvent activer la fonctionnalité de continuité de service à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Vous pouvez appliquer cette configuration aux éléments suivants :
   - **Appareil** > **Chrome** > **Applications et extensions** > **Utilisateurs et navigateurs** > Rechercher l'extension > Règles relatives aux extensions
   - **Appareil** > **Chrome** > **Applications et extensions** > **Kiosques** > Rechercher l'extension > Règles relatives aux extensions
   - **Appareil** > **Chrome** > **Applications et extensions** > **Sessions Invité gérées** > Rechercher l'extension > Règles relatives aux extensions

   Voici un exemple de données JSON :

```
{

"settings": {

    "Value": {

```



```
        "settings_version": "1.0",
        "engine_settings": {

            "features": {

                "serviceContinuity":{

                    "enable": true
                     }

                 }

              }

          }

      }

 }


<!--NeedCopy-->
```

Redirection de contenu du navigateur

La redirection du contenu du navigateur (BCR) redirige le contenu du navigateur distant vers l'appareil du client. La redirection du contenu du navigateur est un navigateur Web sans cadre et sans bordure qui s'exécute dans la fenêtre du bureau distant et couvre (superpose) la zone de contenu du navigateur distant (VDA).

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 HTML5 ou WebRTC. Seule la fenêtre d'affichage (zone visible de l'utilisateur d'une page Web) est redirigée vers le point de terminaison. La redirection du contenu du navigateur ne redirige pas l'interface utilisateur (barre d'adresse, barre d'outils, etc.) du navigateur sur le VDA.

En d'autres mots, la redirection du contenu du navigateur permet d'afficher les pages Web dans la liste verte du côté client. 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.

Pour plus d'informations sur la configuration de la liste d'autorisation, voir :

- Extension Chrome de redirection du contenu du navigateur
- Paramètres de stratégie Redirection du contenu du navigateur

Problèmes connus liés à cette fonctionnalité

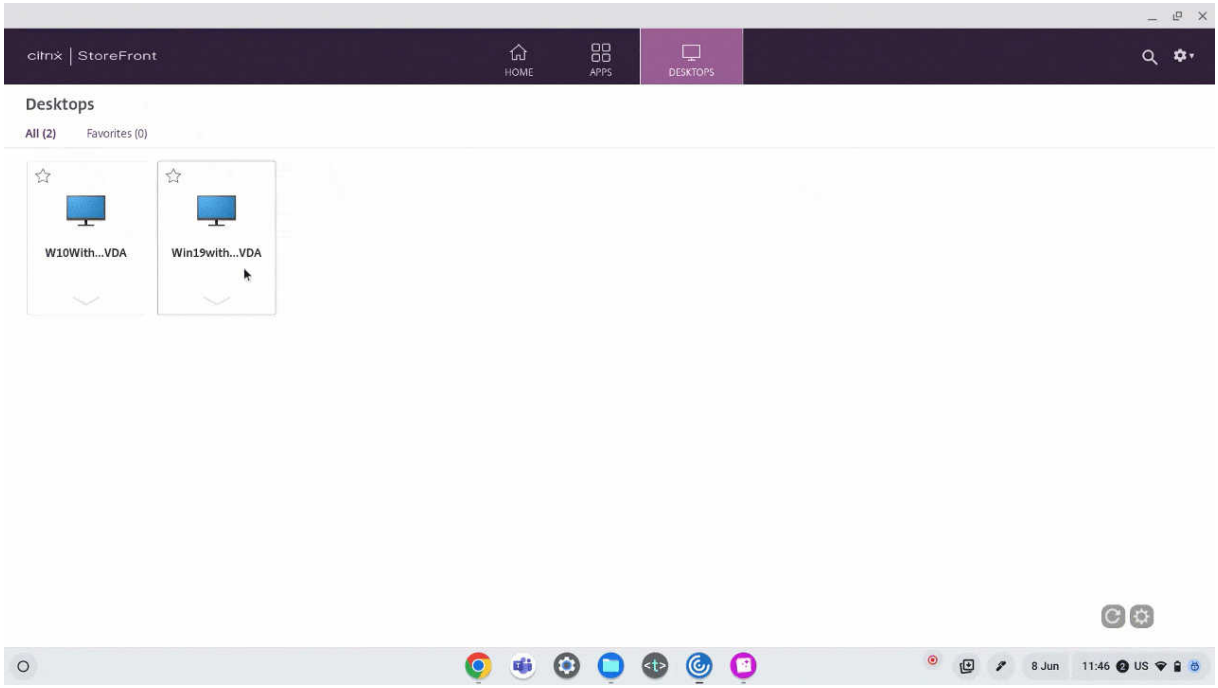
- Lors de la superposition de la redirection du contenu du navigateur, lorsque vous ouvrez un lien vers un site Web dans un nouvel onglet, celui-ci s'ouvre dans le navigateur client au lieu du navigateur de session. [HDX-43206]

Limites connues de cette fonctionnalité

- Cette fonctionnalité ne prend pas en charge ce qui suit :
  - Scénario de récupération du serveur et de restitution du client.
  - Serveur Integrated Windows Authentication (IWA).
  - Fonctionnalité multi-moniteurs.
- Lorsque vous chargez ou téléchargez un fichier sur certains sites Web redirigés par la redirection du contenu du navigateur, le sélecteur de fichiers ChromeOS apparaît à la place d'un sélecteur de fichiers de session VDA. [HDX-43207]
- L'impression n'est pas prise en charge à partir de pages redirigées par la redirection du contenu du navigateur.

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

À partir de la version 2306, l'expérience améliorée de lancement d'applications et de bureaux fournit des informations pertinentes et actualisées sur l'état du lancement.



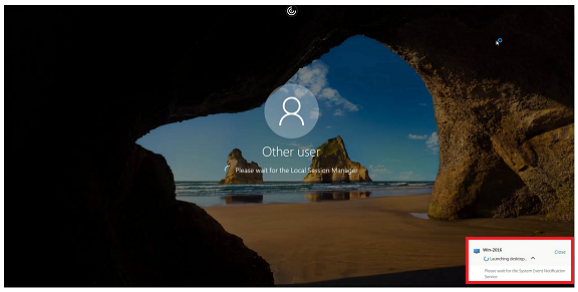
Configurer l'affichage des notifications de lancement de session

À partir de la version 2307, les administrateurs peuvent activer ou désactiver l'affichage des notifications de progression de lancement à l'aide de la configuration suivante.

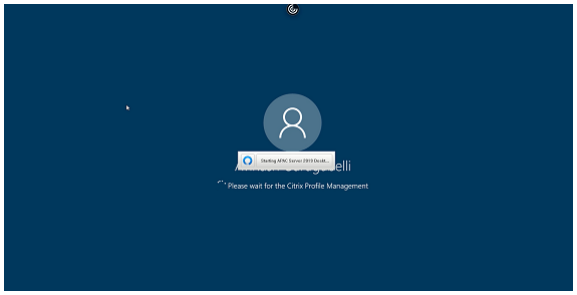
Si cette configuration est activée, vous pourrez afficher les notifications de progression de lancement des sessions en bas à droite de l'écran. Si cette configuration est désactivée, vous ne pourrez pas afficher les notifications de progression de lancement des sessions.

> **Remarque :**
>
> - Par défaut, cette configuration est activée.

Si les notifications sont désactivées, aucune information actualisée et pertinente sur l'état du lancement ne s'affiche pour les utilisateurs finaux.



Si les notifications sont activées, la progression du lancement s'affiche dans le coin inférieur droit de l'écran des utilisateurs finaux.



Configurations Vous pouvez configurer cette fonctionnalité de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

Configuration.js Pour désactiver cette fonctionnalité à l'aide du fichier **configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le **dossier racine ChromeApp**.

2. Modifiez le fichier.

   > **Remarques :**
   >
   > - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
   > - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
   > - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

3. Pour désactiver l'affichage des notifications de progression de lancement, définissez la valeur **CTXTUI** sur **false**.
   Voici un exemple de données JSON :

```
{

"vc_channel":{

    "CTXTUI": false
     }

 }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Stratégie d'administration Google Pour les appareils et les utilisateurs gérés, les administrateurs peuvent désactiver cette fonctionnalité en utilisant la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé **engine_settings**.

   Voici un exemple de données JSON :

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
            "engine_settings": {

```



```
                "vc_channel":

{
                    "CTXTUI": false                }


            }

        }

    }

<!--NeedCopy-->
```

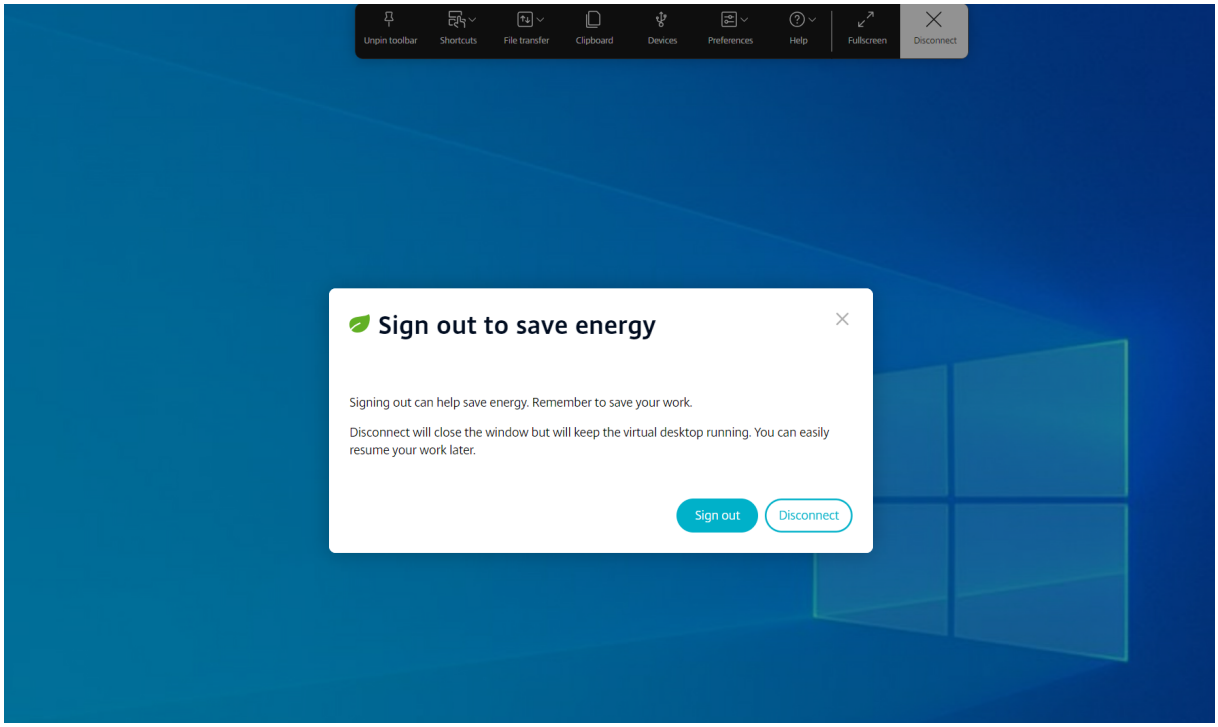
4. Enregistrez les modifications.

Initiative de développement durable pour l'application Citrix Workspace

Auparavant, les bureaux virtuels étaient déconnectés lorsque les utilisateurs les fermaient en appuyant sur le bouton « X ». Cela consommait de l'énergie inutilement.

À partir de la version 2405, nous avons introduit une initiative de développement durable qui encourage les utilisateurs à économiser l'énergie qui pourrait être consommée par l'exécution de bureaux virtuels inutilisés.

Lorsque cette fonctionnalité est activée et que les utilisateurs appuient sur l'icône **X** pour déconnecter la session, une invite s'affiche pour se déconnecter de la session de bureau. Cette fonctionnalité peut être utile dans les entreprises qui utilisent des stratégies de système d'exploitation Windows pour arrêter les machines virtuelles lorsqu'aucun utilisateur n'est connecté.



Les utilisateurs finaux peuvent quitter la session de deux manières :

Déconnecter pour économiser l'énergie : cette action durable arrête la machine virtuelle et permet d'économiser de l'énergie. Les utilisateurs finaux doivent s'assurer de sauvegarder leur travail avant de se déconnecter.

Déconnecter pour fermer la fenêtre de session de bureau virtuel. Cependant, la session virtuelle reste active jusqu'à la prochaine connexion. Les utilisateurs finaux peuvent facilement reprendre leur travail.

Expérience de magasin

May 16, 2024

Paramètres du magasin (« Store settings »)

Comment configurer

Pour créer un magasin, vous identifiez et configurez les communications avec les serveurs. Vous pouvez fournir les ressources que vous souhaitez mettre à disposition dans le magasin. Si vous le souhaitez, vous pouvez également configurer l'accès distant au magasin via Citrix Gateway. Pour

configurer les paramètres du magasin, modifiez la stratégie d'administration Google en incluant les éléments suivants :

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
            "store_settings": {

                "name": "SampleStore",
                "gateways": [{

                    "url": "https: //yourcompany.gateway.com",
                    "is_default": true
                 }
 ],
                "beacons": {

                    "internal": [{

                        "url": "http: //yourcompany.internalwebsite.net
                            "
                     }
 ],
                    "external": [{

                        "url": "http: //www.yourcompany.externalwebsite
                            .com"
                     }
 ]
                 }
 ,
                "rf_web": {

                    "url": "http: //yourcompany.storefrontstoreweb.net"
                 }

             }

          }

     }

 }


<!--NeedCopy-->
```

Liste des paramètres du magasin ainsi que leurs descriptions :

- « name » : entrez le nom du magasin.
- « gateways » : URL de passerelle.

  Ajoutez des URL de passerelle au format `https://gateway.domain.com` ou `https://yourcompany.gateway.com` cliquez sur **Add** sur la page de l'outil.

  Vous pouvez définir une passerelle par défaut si deux URL de passerelle ou plus sont ajoutées.

  Pour utiliser une passerelle comme valeur par défaut, définissez l'indicateur « is_default » sur true. Sinon, définissez l'indicateur sur false.

  Par exemple :

```
    {

        "settings": {

            "Value": {

            "settings_version": "1.0",
            "store_settings": {

                "name": "RTST",
                    "gateways": [{

                        "url": "https: //yourcompany.gateway.com"
                            ,
                        "is_default": true
                     }
,
                    {

                        "url": "https://gateway2.domain.com",
                        "is_default": false
                     }
]
                }

        }

    }


<!--NeedCopy-->
```

- « internal » : détermine si l'application Citrix Workspace se connecte directement à StoreFront ou si elle se connecte via une passerelle. Par exemple, `https://storefront.domain.com`.
- « external » : détermine si l'interface réseau spécifiée est disponible et autorise le trafic. Par

exemple, `https://citrix.com`.

- « rf_web » : URL du magasin.

Prise en charge de magasins multiples

À partir de la version 2305, les administrateurs informatiques peuvent attribuer plusieurs magasins aux utilisateurs. Désormais, les utilisateurs peuvent facilement passer d'un magasin à l'autre sans avoir à se souvenir de l'URL exacte du magasin. Cette fonctionnalité améliore l'expérience utilisateur lors de l'accès à plusieurs magasins.

Comment configurer

Pour configurer plusieurs magasins, les administrateurs informatiques peuvent modifier la stratégie d'administration Google. Voici un exemple de données JSON :

```
{

      "settings_version": "1.0",
      "store_settings": {

            "name": "SampleStore",
            "gateways": [{

                  "url": " https: //yourcompany.gateway.com",
                  "is_default": true
             }
 ],
            "beacons": {

                  "internal": [{

                        "url": " http: //yourcompany.internalwebsite.
   net"
                   }
 ],
                  "external": [{

                  "url": " http: //www.yourcompany.externalwebsite.com"
                   }
 ]
             }
 ,
            "rf_web": {

                  "url": " http: //yourcompany.storefrontstoreweb.net"
             }
 ,
            "secondary_stores": [{
```



```
33
34                    "name": " SampleStore",
35                    "gateways": [{
36
37                          "url": " https: //yourcompany.gateway.com ",
38                          "is_default": true
39                     }
40    ],
41                    "beacons": {
42
43                         "internal": [{
44
45                          "url": " http: //yourcompany.internalwebsite.
        net "
46                           }
47    ],
48                          "external": [{
49
50                      "url": " http: //www.yourcompany.externalwebsite.
        com "
51                           }
52    ]
53                     }
54    ,
55                    "rf_web": {
56
57                    "url": " http: //yourcompany.storefrontstoreweb.net "
58                     }
59
60                }
61    , {
62
63                    "rf_web": {
64
65                    "url": " http: //yourcompany.storefrontstoreweb.net "
66                     }
67
68                }
69    ]
70          }
71
72    }
73
74  <!--NeedCopy-->
```

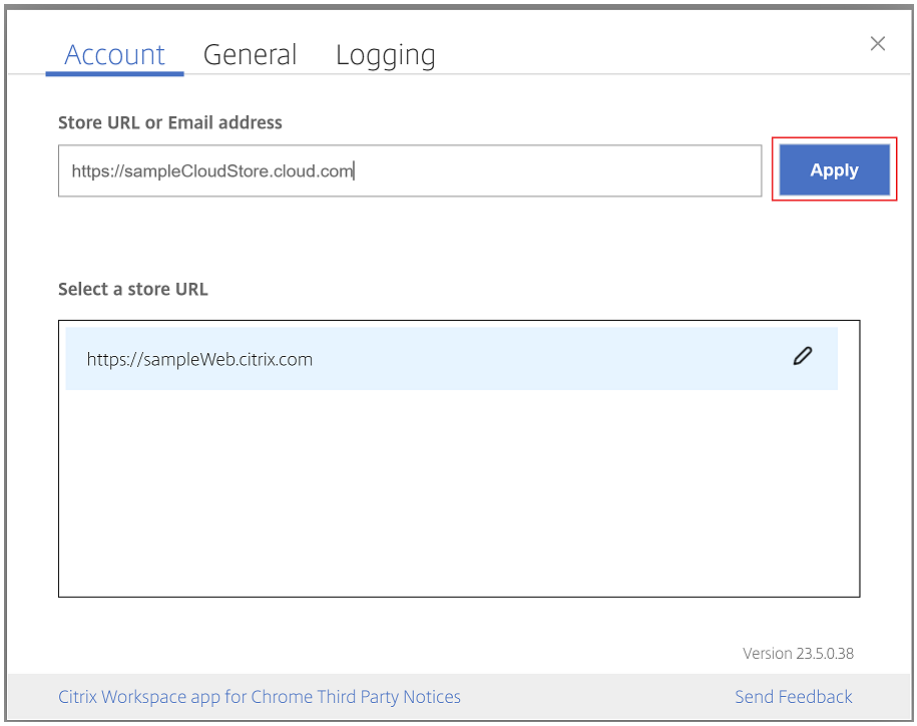
L'attribut **secondary_stores** vous permet de configurer plusieurs magasins. Un administrateur peut utiliser la structure JSON plusieurs fois. Pour plus d'informations sur la personnalisation de l'application Citrix Workspace pour ChromeOS, consultez Outil Configuration Utility.

Magasins StoreFront multiples

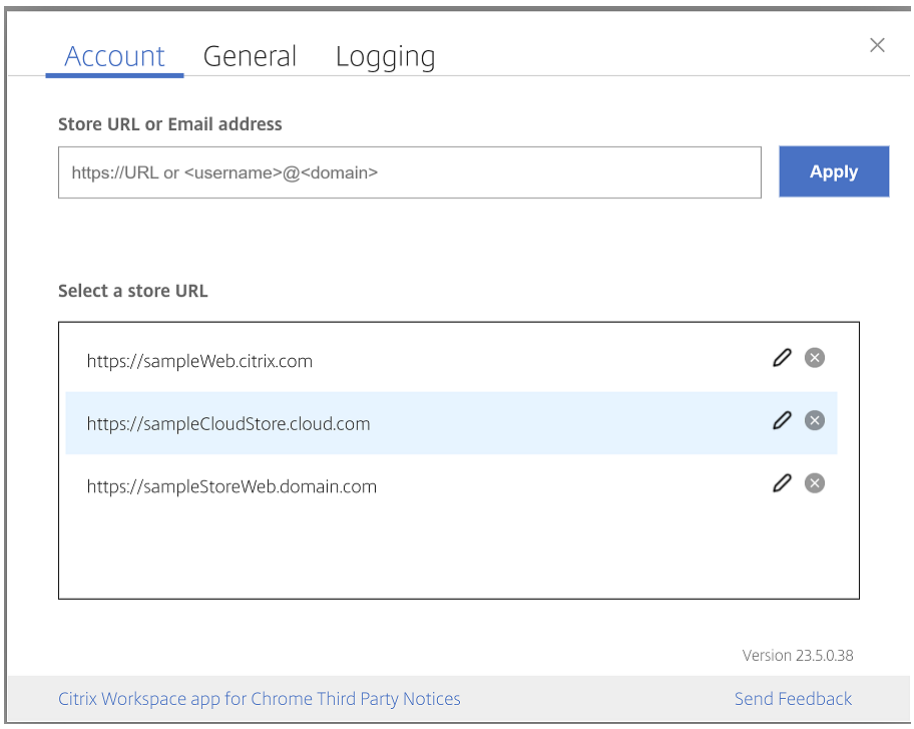
Vous pouvez modifier l'adresse du magasin sans avoir à redémarrer Citrix Workspace. Les sessions Citrix Workspace existantes (le cas échéant) continuent à s'exécuter sans interruption.

Pour ajouter des magasins :

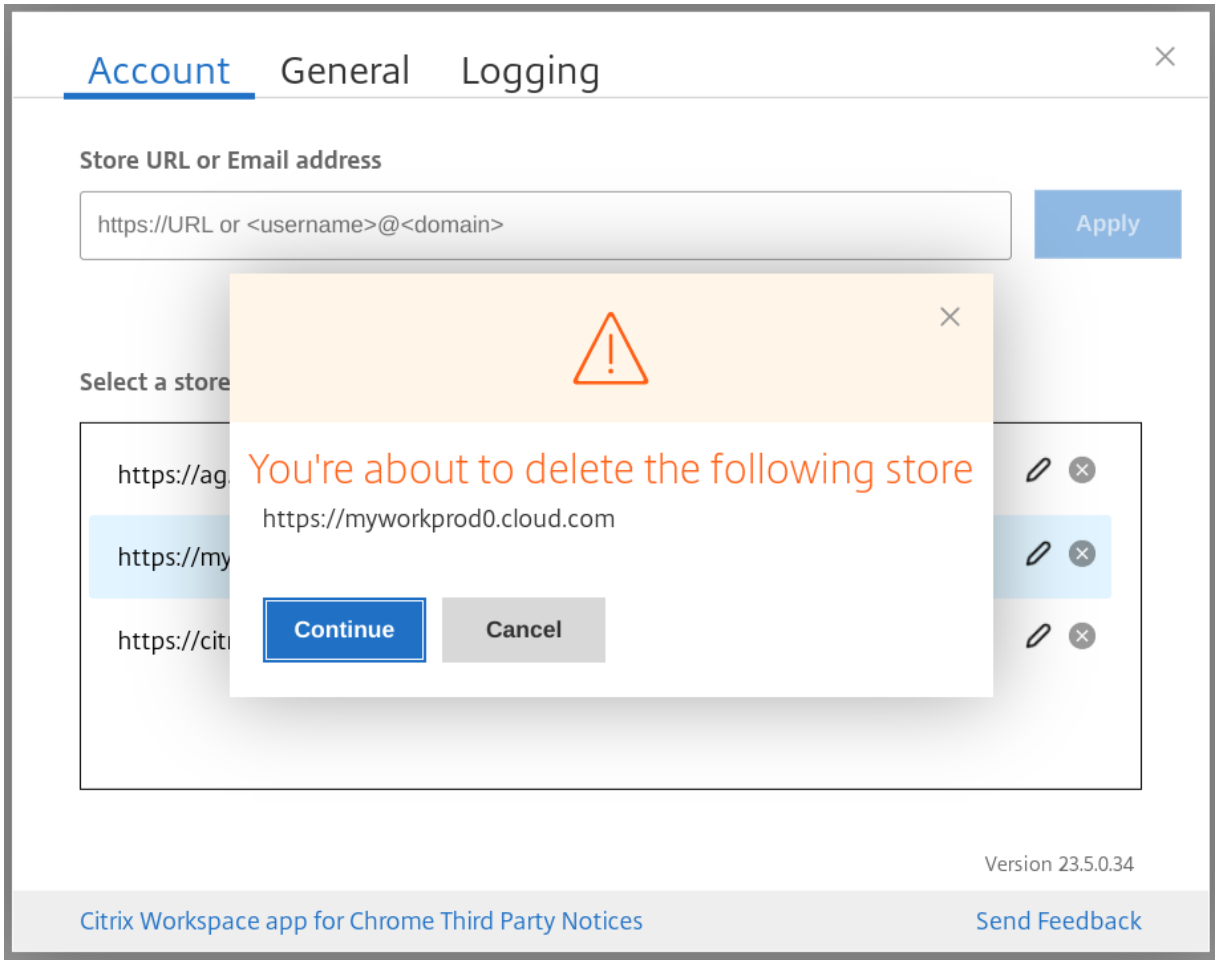
1. Cliquez sur **Paramètres** dans l'application Citrix Workspace pour ChromeOS, puis sélectionnez l'onglet **Compte**.
2. Entrez l'URL ou l'adresse e-mail de StoreFront dans le champ **URL de magasin ou adresse e-mail**.
3. Cliquez sur **Appliquer** pour enregistrer le nouveau magasin.



Pour changer de magasin, sélectionnez-le dans la liste **Sélectionnez une URL de magasin**.



Pour supprimer un magasin de la liste, cliquez sur l'icône **Supprimer** en regard de l'adresse du magasin que vous souhaitez supprimer et confirmez la suppression.



Recharger le magasin

Dans la fenêtre de l'application Citrix Workspace pour ChromeOS, un bouton a été ajouté pour les opérations de rechargement. Lorsque vous cliquez sur le bouton, les cookies du magasin sont effacés et la page du magasin est rechargée.

Actualiser le magasin

À partir de la version 2307, vous pouvez appliquer les configurations suivantes pour éviter de dupliquer les instances des applications publiées.

> **Remarque :**
>
> - Par défaut, la configuration est désactivée. Lorsque vous activez cette configuration, les instances dupliquées de l'application publiée ne s'affichent pas. Cliquez sur l'⟳ pour actualiser le magasin.

Vous pouvez configurer cette fonctionnalité de l'une des manières suivantes :

• Configuration.js
• Stratégie d'administration Google

Configuration.js

Pour activer cette fonctionnalité à l'aide du fichier**configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le **dossier racine ChromeApp**.

   > **Remarques :**
   >
   > - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
   > - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
   > - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

2. Modifiez le fichier et définissez **Actualiser le magasin** sur **Vrai**.

   Voici un exemple de données JSON :

   ```
   'ui' :{

     'refreshStore': true
    }

   <!--NeedCopy-->
   ```

3. Enregistrez les modifications.

Stratégie d'administration Google

Pour les appareils et les utilisateurs gérés, les administrateurs peuvent activer la fonctionnalité à l'aide de la stratégie d'administrateur Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous **engine_settings**.

   > **Remarque :**
   >
   > Vous pouvez également appliquer cette configuration aux éléments suivants :

> - **Appareil** > **Chrome** > **Applications et extensions** > **Kiosques** > Rechercher l'extension > Règles relatives aux extensions
> - **Appareil** > **Chrome** > **Applications et extensions** > **Sessions Invité gérées** > Rechercher l'extension > Règles relatives aux extensions

Voici un exemple de données JSON :

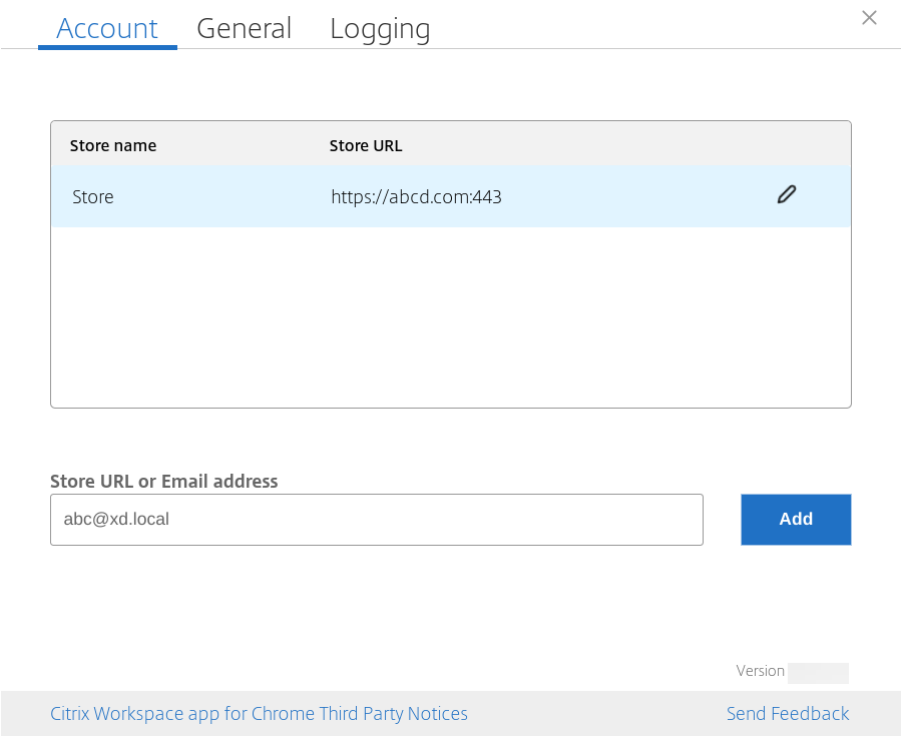
```
{

"settings": {

"Value": {

  "settings_version": "1.0",
  "engine_settings": {

    "ui": {

      "refreshStore": true
         }

       }

     }

   }

 }

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Détection de magasin basée sur l'adresse e-mail

Vous pouvez désormais utiliser votre adresse e-mail pour accéder à l'application Citrix Workspace sans avoir à mémoriser l'URL du magasin. Les magasins attribués à votre compte sont automatiquement renseignés. Accédez au menu déroulant **Comptes** > **URL de magasin ou adresse e-mail** pour afficher la liste des magasins associés à votre adresse e-mail.

> **Remarque :**
>
> Vous pouvez toujours utiliser l'URL du magasin pour vous connecter.



En tant qu'administrateur, pour gérer et renseigner automatiquement les comptes de magasin, consultez préalablement la section Présentation de l'API Citrix Cloud.

Pour plus d'informations, consultez Global App Configuration Service.

Nom abrégé de l'URL du magasin

Auparavant, vous pouviez voir les URL des magasins, mais aucune disposition ne permettait d'ajouter ou de modifier un nom abrégé pour les URL des magasins. Cette disposition a rendu difficile pour les administrateurs et les utilisateurs de se souvenir des URL des magasins.

À partir de la version 2402, pour les utilisateurs gérés, les administrateurs peuvent envoyer un nom de magasin personnalisé ainsi que l'URL du magasin depuis la console d'administration Google. Cette fonctionnalité permet aux utilisateurs d'identifier plus facilement les différents magasins. L'administrateur peut également décider si l'utilisateur peut modifier le nom du magasin ou non en définissant l'attribut **allowEditStoreName** sur **true** ou **false**. Pour plus d'informations, consultez la section suivante.

Pour les utilisateurs du BYOD, le nom du magasin est généré automatiquement. Par exemple, Magasin, Magasin 1, Magasin 2, etc. Les magasins sont renseignés à l'aide de la fonction de découverte de magasins par e-mail. Les utilisateurs peuvent modifier le nom du magasin selon leurs besoins.

Configuration

Par défaut, les utilisateurs du BYOD peuvent modifier le nom du magasin.

Pour les appareils et les utilisateurs gérés, les administrateurs peuvent définir l'attribut **allowEditStoreName** sur **true** pour activer la fonctionnalité à l'aide de la console d'administration Google, comme suit.

> **Remarque :**
>
> - Par défaut, l'attribut **allowEditStoreName** est défini sur **false**.

Stratégie d'administration Google Pour activer la stratégie, procédez comme suit :

1. Connectez-vous à la console d'administration Google.
2. Vous pouvez également appliquer cette configuration aux éléments suivants :
   - **Appareil** > **Chrome** > **Applications et extensions** > **Utilisateurs et navigateurs** > Rechercher l'extension > Règles relatives aux extensions
   - **Appareil** > **Chrome** > **Applications et extensions** > **Kiosques** > Rechercher l'extension > Règles relatives aux extensions
   - **Appareil** > **Chrome** > **Applications et extensions** > **Sessions Invité gérées** > Rechercher l'extension > Règles relatives aux extensions

   Voici un exemple de données JSON :

```
{

"settings": {

    "Value": {

        "settings_version": "1.0",
        "store_settings": {

            "name": "Citrix store",
            "allowEditStoreName": true,
            "rf_web":
               {

                "url": "https://xyz.cloud.com"
                                                    }

                }
 ,
         }

     }

```



```
23   }
24
25 <!--NeedCopy-->
```

3. Enregistrez les modifications.

> **Remarque** :
>
> Dans l'extrait de code, le **nom** de l'attribut fait référence au nom abrégé du magasin.

Comment utiliser cette fonctionnalité Par défaut, les utilisateurs du BYOD peuvent modifier le nom du magasin. Pour les utilisateurs gérés, si l'administrateur de votre organisation autorise la modification du nom du magasin, vous pouvez le faire. Pour plus d'informations, consultez Nom abrégé de l'URL du magasin.

Prise en charge des appareils mobiles et à écran tactile

May 16, 2024

Mode tactile multipoint

L'application Citrix Workspace pour ChromeOS vous permet de définir le mode **Multipoint** comme mode par défaut via la console d'administration Google. Le mode multipoint permet d'activer les gestes multipoint.

Vous pouvez basculer entre le mode Panoramique et le mode Multipoint. Auparavant, le mode panoramique était défini comme mode par défaut.

Lorsque vous lancez une session sur un périphérique tactile, les gestes par défaut sont gérés en mode panoramique. Vous pouvez passer en mode multipoint à l'aide de la barre d'outils. Cette fonctionnalité offre une meilleure expérience utilisateur.

Comment configurer

Pour définir la fonctionnalité comme valeur par défaut, modifiez la stratégie **Google Admin Console** et définissez la valeur **defaultMode** sur **Multitouch**.

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



```
        "Value": {

            "settings_version": "1.0",
                        "engine_settings": {

                            "ui": {

                                "touch" : {

                                    "defaultMode" : "multitouch"
                                     }

                                }

                            }

                        }

                    }


<!--NeedCopy-->
```

Prise en charge du mode tactile

L'application Citrix Workspace pour ChromeOS améliore désormais la prise en charge tactile en vous permettant d'exécuter des sessions sur des appareils Chrome tactiles en mode tablette. Cette fonctionnalité inclut la prise en charge des gestes, du multipoint et du clavier logiciel.

L'icône **Ouvrir le clavier** apparaît désormais dans la barre d'outils de session lorsqu'un appareil Chrome est en mode tablette. Lorsque vous utilisez cette fonctionnalité ou que vous touchez l'écran avec trois doigts, le clavier logiciel s'affiche.

Amélioration des gestes sur les appareils tactiles

À partir de la version 23.4.0, l'application Citrix Workspace améliore l'expérience liée aux gestes, au multipoint et au clavier logiciel (mode tablette). Dans vos sessions de l'application Citrix Workspace, vous pouvez utiliser tous les gestes multipoint habituels, notamment toucher, balayer et faire glisser.

Voici le guide des gestes :

Pour ce faire :	Sur l'application Citrix Workspace, procédez comme suit :
Clic simple	Toucher à un doigt
Clic droit	Toucher-Maintenir-Relâcher
Ouvrir le clavier à l'écran	Toucher à trois doigts (ou à partir de la barre d'outils, toucher l'icône **Clavier**)
Déplacer	Toucher-Maintenir-Faire glisser
Activer le curseur	Toucher à deux doigts

Affichage automatique du clavier

Vous pouvez activer l'affichage automatique du clavier sur un serveur à l'aide du bouton de clavier flottant qui apparaît dans un champ de saisie. Pour que la fonction d'affichage automatique du clavier soit disponible, vérifiez que le paramètre côté serveur est activé.

Limitations des fonctionnalités :

- Toucher avec trois doigts pour récupérer le clavier logiciel ne fonctionne pas en mode tactile multipoint. Cette méthode fonctionne uniquement en mode panoramique.
- Pour que le clavier logiciel fonctionne correctement, fermez-le toujours à l'aide de l'icône Ouvrir le clavier de la barre d'outils de la session plutôt qu'à l'aide du clavier logiciel du système. Si vous fermez le clavier logiciel à l'aide du clavier logiciel du système, le clavier logiciel peut se comporter de manière inattendue.

Comment configurer

Pour activer le paramètre côté serveur, procédez comme suit :

1. Sur le Delivery Controller, ouvrez Citrix Studio.
2. Sélectionnez **Stratégies**.
3. Cliquez sur **Créer une stratégie**.
4. Recherchez **Affichage automatique du clavier** et sélectionnez **Autorisé**.

Redirection des URL

May 16, 2024

Redirection hôte vers client

La redirection de contenu vous permet de contrôler si les utilisateurs accèdent aux informations :

- en utilisant des applications publiées sur des serveurs ou
- en exécutant des applications localement sur les appareils des utilisateurs.

« Redirection hôte vers client » est un type de redirection de contenu. Elle est prise en charge uniquement sur les VDA avec OS de serveur (et non sur les VDA avec OS de bureau) avec Citrix XenApp et XenDesktop versions 7.15 LTSR et ultérieures.

Pour de plus amples informations, consultez Redirection hôte vers client - XenApp et XenDesktop dans la documentation XenApp et XenDesktop.

Lorsque la redirection hôte vers client est activée, les adresses URL sont interceptées sur le VDA de serveur puis envoyées vers la machine utilisateur. L'application Citrix Workspace pour ChromeOS affiche une boîte de dialogue invitant l'utilisateur à ouvrir l'URL dans la session ou sur l'appareil local. La boîte de dialogue s'affiche pour chaque URL.

Lorsque la redirection hôte vers client est désactivée, les utilisateurs ouvrent les adresses URL à l'aide de navigateurs Web ou de lecteurs multimédias sur le VDA de serveur. Lorsque la redirection hôte vers client est activée, les utilisateurs ne peuvent pas la désactiver.

La redirection hôte vers client était auparavant appelée redirection serveur vers client.

Pour plus d'informations, consultez Redirection de contenu générale dans la documentation de Citrix Virtual Apps and Desktops.

Améliorations apportées à la redirection des URL

Auparavant, lorsque la redirection hôte vers client était activée, les URL étaient interceptées sur le VDA du serveur et envoyées à l'appareil de l'utilisateur. L'application Citrix Workspace pour ChromeOS affichait une boîte de dialogue invitant l'utilisateur à ouvrir l'URL dans la session ou sur l'appareil local. La boîte de dialogue s'affichait pour chaque URL.

À partir de la version 2305, les administrateurs peuvent configurer la redirection des URL. Ainsi, les liens peuvent être ouverts sur l'appareil local sans boîte de dialogue supplémentaire. Cette amélioration améliore l'expérience utilisateur.

> **Remarque :**
>
> - Cette fonctionnalité est désactivée par défaut.

Comment configurer

Vous pouvez activer cette fonctionnalité de l'une des manières suivantes :

- Configuration.js
- Stratégie d'administration Google

Configuration.js Pour activer cette fonctionnalité à l'aide du fichier**configuration.js**, procédez comme suit :

1. Recherchez le fichier **configuration.js** dans le dossier racine **ChromeApp**.

   > **Remarques :**
   >
   > - Citrix recommande de sauvegarder le fichier **configuration.js** avant d'y apporter des modifications.
   > - Citrix recommande de modifier le fichier **configuration.js** uniquement si l'application Citrix Workspace pour ChromeOS est reconditionnée pour les utilisateurs.
   > - Les informations d'identification de niveau administrateur sont requises pour modifier le fichier **configuration.js**.

2. Modifiez le fichier **configuration.js** et définissez la valeur par défaut de **forceOpenInClient** sur **true**. Voici un exemple de données JSON :

```
{

"features": {

        "UrlRedirection": {

        "forceOpenInClient": true
             }

    }

 }

<!--NeedCopy-->
```

3. Enregistrez les modifications.

Stratégie d'administration Google Lors du déploiement sur site, les administrateurs peuvent activer cette fonctionnalité à l'aide de la stratégie d'administration Google comme suit :

1. Connectez-vous à la stratégie d'administration Google.
2. Accédez à **Gestion des appareils** > **Gestion de Chrome** > **Paramètres utilisateur**.
3. Ajoutez les chaînes suivantes au fichier **policy.txt** sous la clé **engine_settings**. Voici un exemple de données JSON :


```
{

  "features": {

    "UrlRedirection": {

        "forceOpenInClient": true
                    }

          }

}

<!--NeedCopy-->
```

4. Enregistrez les modifications.

Canaux virtuels

May 16, 2024

À propos des canaux virtuels

Un canal virtuel consiste en un pilote virtuel côté client qui communique avec une application côté serveur. Les canaux virtuels font partie intégrante de l'expérience à distance avec les serveurs Citrix Virtual Apps and Desktops.

Les canaux virtuels sont utilisés pour les éléments suivants :

- Impression
- Mappage de port série
- Presse-papiers
- Audio
- Multimédia
- Canal de contrôle
- EUEM
- USB
- Transfert de fichiers
- Mobilité
- Multipoint
- Carte à puce
- Mobile Receiver

- Microsoft Teams
- Éditeur de méthode d'entrée
- Redirection du contenu du navigateur
- Mappage des lecteurs clients
- Interface utilisateur transparente

Comment configurer

Tous les canaux virtuels sont activés par défaut. Pour désactiver un canal virtuel particulier, utilisez la stratégie d'administration Google en incluant les éléments suivants. Sélectionnez le nom de la fonction sous « vc_channel » et cliquez sur **Add** sur la page de l'outil. Par exemple :

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                        "vc_channel": {

                            "<vc_name1>": false,
                            "<vc_name2>": false,
                            "<vc_name3>": false,
                            "<vc_namen>": false
                                        }

                                }

          }

     }

 }


<!--NeedCopy-->
```

Pour activer un canal virtuel particulier (« vc_channel »), sélectionnez la fonction et cliquez sur **Remove** sur la page de l'outil.

> **Remarque :**
>
> Les noms peuvent être compris entre 1 et n. Le dernier nom « n » ne peut pas avoir de virgule après la valeur définie sur true ou false.


```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "vc_channel": {

                        "CTXCPM ": false,
                        "CTXCAM ": false,
                        "CTXGUSB": false
                                    }

                                   }

         }

     }

 }


<!--NeedCopy-->
```

Liste des paramètres de canaux virtuels ainsi que leurs descriptions :

- « CTXCPM » : impression PDF.
- « CTXCCM » : mappage des ports série client.
- « CTXCLIP » : opérations du Presse-papiers de la session au VDA et du VDA à la session.
- « CTXCAM » : mappage audio client.
- « CTXMM » : redirection multimédia Citrix.
- « CTXCTL » : canal virtuel de contrôle Citrix.
- « CTXEUEM » : surveillance de l'expérience utilisateur final.
- « CTXGUSB » : rediriger les périphériques USB vers la session.
- « CTXFILE » : le transfert de fichiers s'effectue de manière sécurisée entre une machine utilisateur et une session Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Vous pouvez charger et télécharger des fichiers vers et depuis une session et accéder facilement aux données.
- « CTXMTCH » : le mode tactile multipoint configure un accès distant à tous les gestes de la session virtuelle. L'application fonctionne selon les gestes qu'elle prend en charge.
- « CTXSCRD » : prise en charge de la carte à puce.
- « CTXMOB » : canal virtuel Mobile Receiver.
- « CTXMTOP » : canal virtuel Microsoft Teams.
- « CTXIME » : éditeur de méthode d'entrée.

- « CTXCSB » : redirection du contenu du navigateur.
- « CTXCDM » : mappage des lecteurs clients.
- « CTXTUI » : interface utilisateur transparente.

Canaux virtuels personnalisés

Le SDK du canal virtuel pour Chrome permet aux applications Chrome tierces d'écrire des canaux virtuels personnalisés. Ces canaux sont initialisés avec les sessions d'application et de bureau lancées à l'aide de l'application Citrix Workspace ou du SDK HDX pour Chrome.

En outre, le SDK du canal virtuel offre un moyen facile d'écrire et de recevoir des données à partir de l'application Chrome tierce, ainsi que de l'application et du bureau.

Comment configurer

Pour configurer des canaux virtuels personnalisés, utilisez la stratégie d'administration Google en incluant les éléments suivants.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "customVC": [
                        {

                    "appId": "xyz",
                    "streamName": "abc"
                         }

                    ]
                 }

          }

      }

 }


<!--NeedCopy-->
```

Liste des options de canaux virtuels personnalisés ainsi que leurs descriptions :

- « appId » : ID de l'application Chrome qui met en œuvre des canaux virtuels personnalisés.
- « streamName » : nom du canal virtuel.

Dépannage

May 16, 2024

Comment collecter des journaux

L'application Citrix Workspace pour ChromeOS fournit des horodatages dans les journaux générés par l'appareil utilisateur. L'application Citrix Workspace prend en charge la collecte des journaux pour les sessions d'applications et de bureaux virtuels en cours.

En tant qu'utilisateur final, vous pouvez collecter des journaux pour faciliter le dépannage. Les journaux peuvent être générés à la fois sur la machine utilisateur et sur les machines. Les journaux peuvent être destinés aux ordinateurs de bureau et aux applications.

Auparavant, vous ne pouviez collecter des journaux que pour les sessions lancées après avoir sélectionné **Démarrer la journalisation** pendant une session en cours. Désormais, les journaux sont collectés pour les sessions en cours et suivantes jusqu'à ce que vous sélectionniez **Arrêter la journalisation**.

Pour activer la journalisation sur les appareils utilisateur

1. Sur la machine utilisateur, lancez l'application Citrix Workspace et accédez à la page de connexion.
2. Sélectionnez le bouton avec une image de paramètres dans le coin inférieur droit.
3. Dans la boîte de dialogue **Paramètres**, cliquez sur **Démarrer la journalisation**.

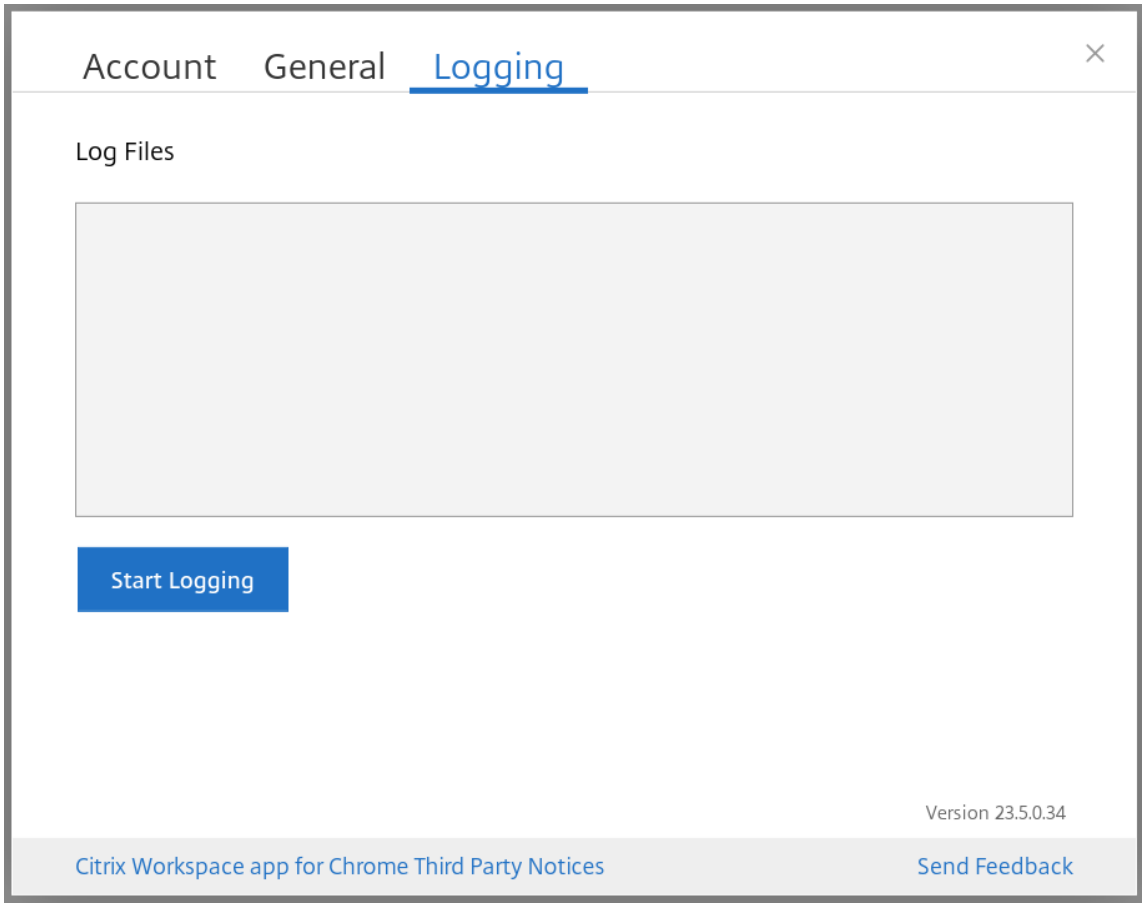
   Les détails des fichiers journaux collectés sont répertoriés dans la boîte de dialogue **Paramètres**.
4. Sélectionnez sur **Arrêter la journalisation** pour mettre fin à la collecte des journaux sur l'appareil utilisateur.

Journaux du client

> **Remarque :**
>
> - À partir de la version 2207, les journaux de la console font partie des journaux du client.

1. Cliquez sur le bouton **Paramètres** en bas à droite de l'écran **Connexion** de l'application Citrix Workspace.

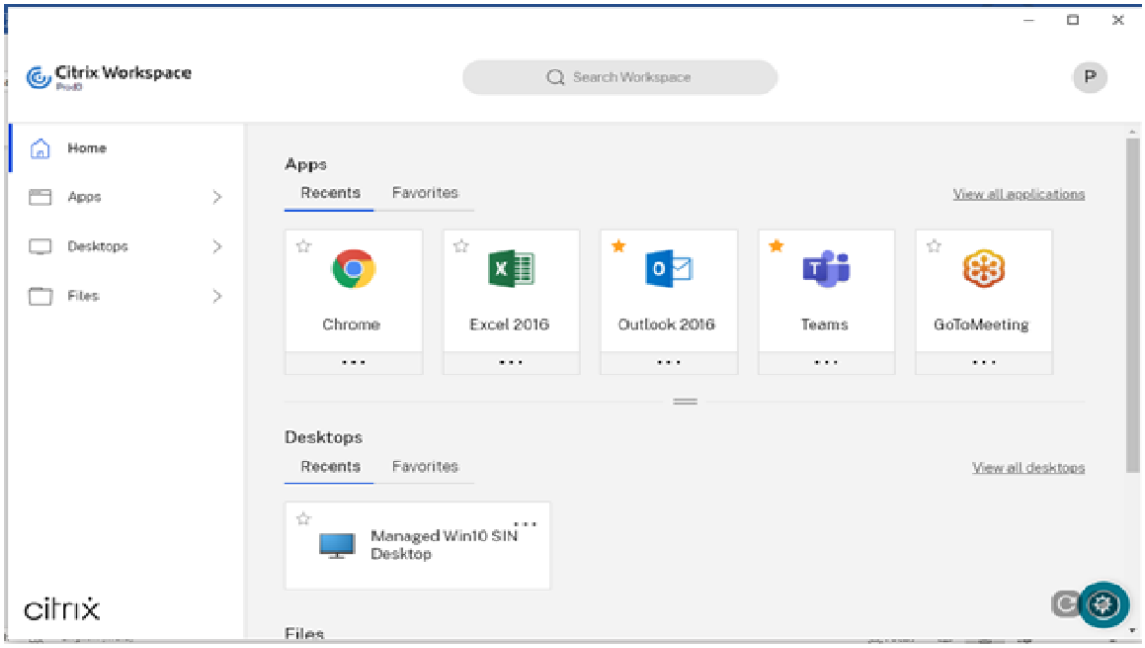
2. Cliquez sur le bouton **Démarrer la journalisation** sous **Journalisation** pour activer la collecte des journaux.



3. Le bouton **Démarrer la journalisation** devient **Arrêter la journalisation**. Ce changement indique que la collecte de journaux est activée.

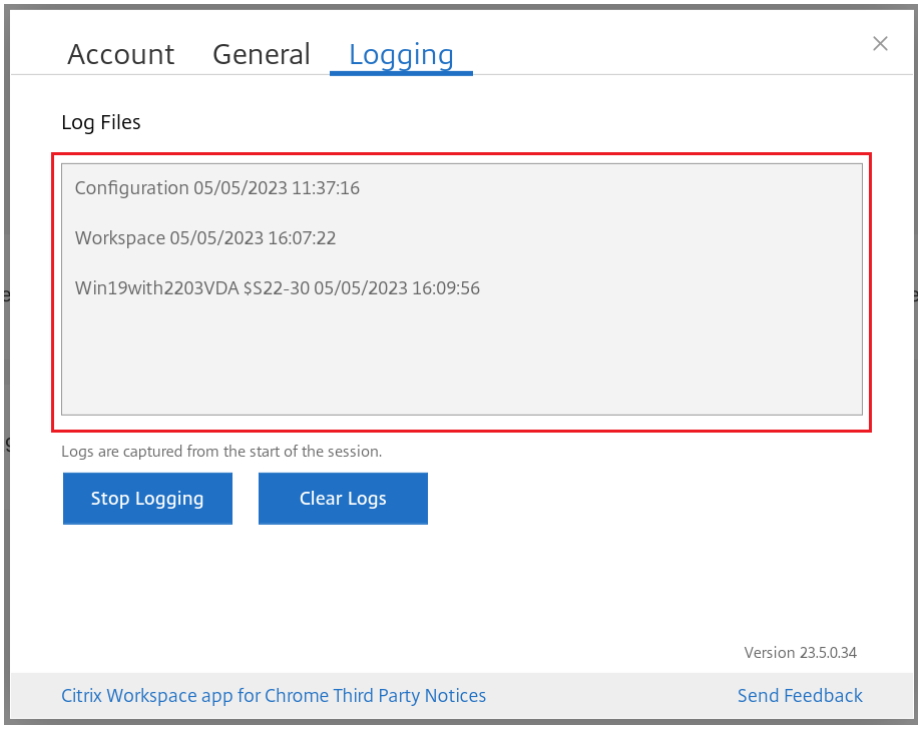
   Fermez la boîte de dialogue **Compte**.

4. Connectez-vous au bureau virtuel de l'application Citrix Workspace et lancez votre session d'application virtuelle et reproduisez le problème pour collecter des journaux.



Continuez à travailler sur la session pour reproduire le problème.

5. Une fois le problème reproduit, fermez la session.
6. Cliquez à nouveau sur le bouton **Paramètres** pour ouvrir la boîte de dialogue **Compte**.
7. Sélectionnez l'onglet **Journalisation**.
8. La boîte de dialogue **Journalisation** affiche la liste des **fichiers journaux** capturés.



9. Une petite flèche apparaît à droite des fichiers journaux que vous survolez avec la souris.

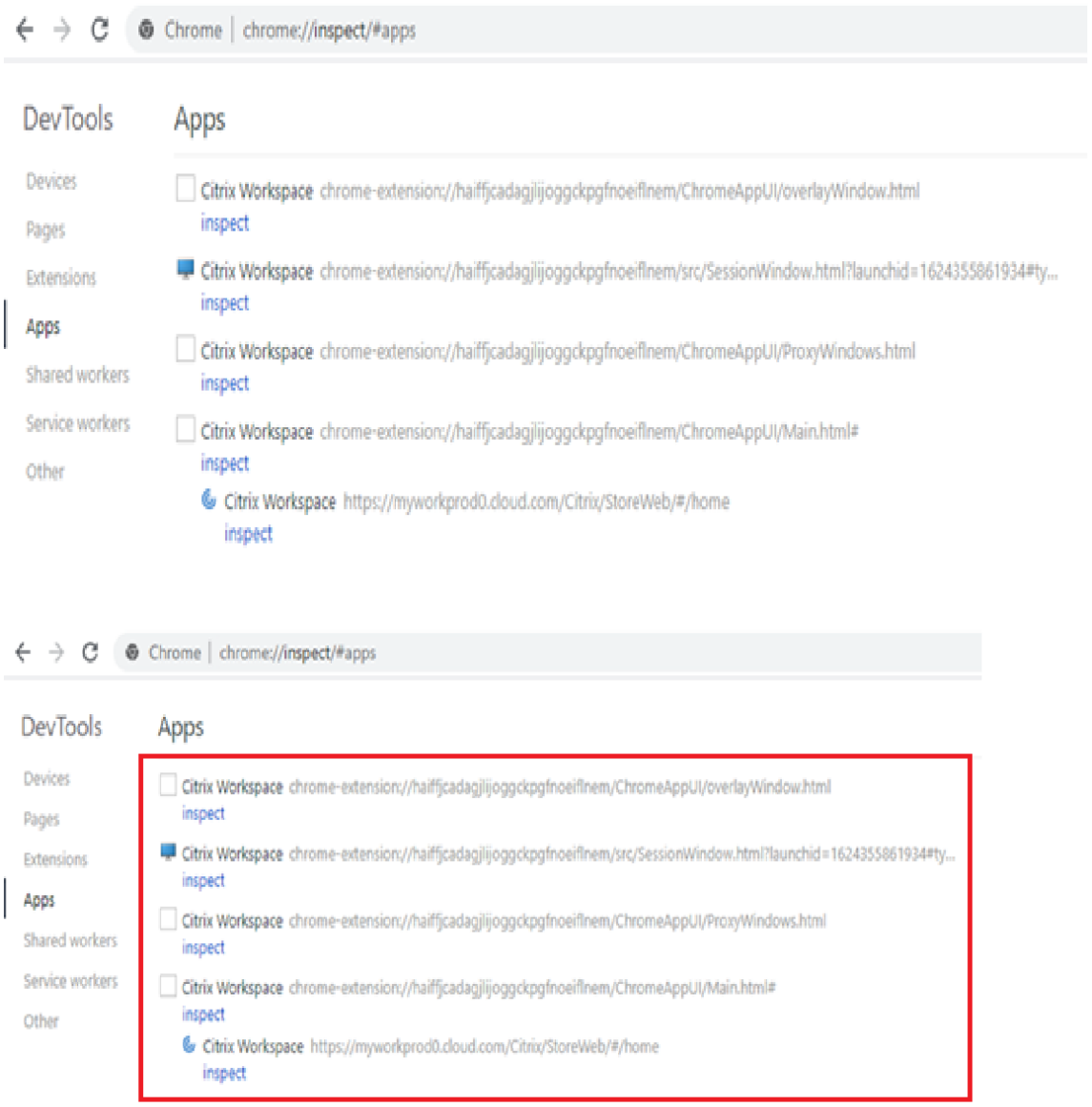
10. Cliquez sur le bouton de la flèche pour télécharger et enregistrer le fichier journal.
11. Enregistrez tous les fichiers journaux répertoriés sous **Fichiers journaux** et partagez-les avec l'administrateur ou l'ingénieur de support Citrix.
12. Cliquez sur **Arrêter la journalisation**.

> **Remarque :**
>
> En mode Kiosque, les fichiers peuvent être enregistrés sur un périphérique USB amovible.

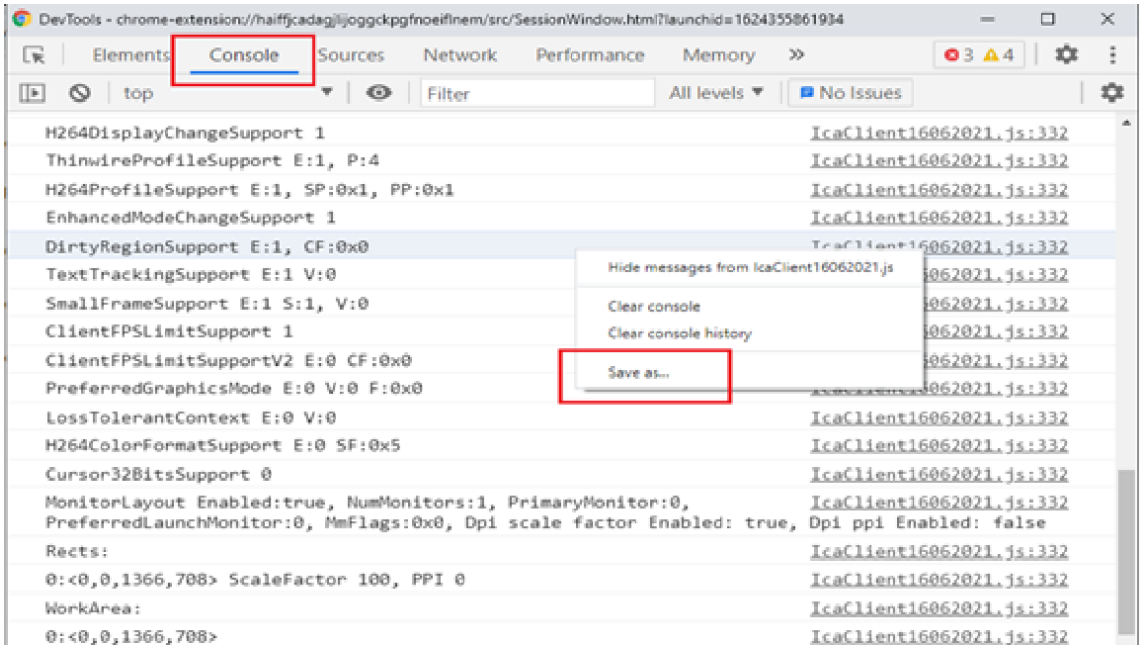
Journaux de la console

> **Remarque :**
>
> - À partir de la version 2207 et des versions ultérieures, les journaux de la console font partie des journaux du client. Par conséquent, la seule collecte des journaux du client peut suffire.

1. Ouvrez la page **chrome://inspect/#apps** dans le navigateur Google Chrome de votre application Citrix Workspace.
2. Dans l'onglet **Applications**, cliquez sur **inspect** pour toutes les fenêtres associées à Citrix Workspace : SessionWindow.html, Main.html (et ses nœuds enfants).



3. Pour chaque fenêtre d'outil de développement ouverte, cliquez sur **Console**. Ensuite, enregistrez le journal entier en cliquant avec le bouton droit de la souris et en sélectionnant l'option **Save as**.



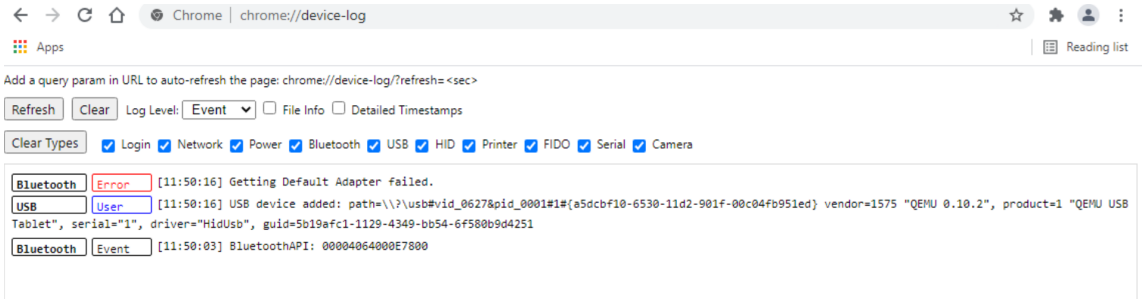
Journaux de redirection USB

1. Suivez les étapes décrites dans la section Utilisation de Web.config pour ChromeOS et activez moreLogs pour USB en :

   Ajoutant la valeur de configuration de moreLogs à chromeAppPreferences dans le fichier web.config sur StoreFront :

   ```
   chromeAppPreferences ='{ "moreLogs":{ "usb":true } } '
   ```

2. Ensuite, ouvrez un nouvel onglet dans le navigateur Google Chrome, entrez **chrome://device-log** et partagez les journaux.



Journaux de transfert de fichiers

Les journaux de transfert de fichiers peuvent être récupérées depuis le client et le serveur.

Pour récupérer les journaux de transfert de fichiers depuis le client :

1. Lancez un navigateur.
2. Accédez à l'adresse URL suivante pour démarrer la journalisation :
   <urlstorefront>/clients/html5client/src/viewlog.html
   où *<urlstorefront>* est le nom de domaine complet ou l'adresse IP du serveur StoreFront sur lequel le magasin est configuré.

Pour plus d'informations sur le transfert de fichiers, consultez le blog HTML5 and Chrome File Transfer Explained.

Journaux d'optimisation de Microsoft Teams

L'optimisation de Microsoft Teams prend en charge la dernière version 1.8.0.12 de la bibliothèque shim.

Pour connaître la version actuelle de shim que vous utilisez :

1. Lancez l'application Microsoft Teams et lancez un appel avec l'un des utilisateurs.
2. Agrandissez la fenêtre Microsoft Teams une fois l'appel établi.
3. Ouvrez le **clavier virtuel** à l'intérieur de la session et cliquez sur les touches **Ctrl + Alt + Maj + 1**.
   Vous pouvez désormais afficher les fichiers journaux dans le dossier des téléchargements.
4. Ouvrez le fichier `MSTeams Diagnostics Log <date><time>_vdi partner.txt` et recherchez la version de la cale sous **type_script**.
   Comparez la version de shim avec la version 1.8.0.12.
5. (Facultatif) Si la version de shim n'est pas 1.8.0.12, contactez votre administrateur pour effectuer la mise à niveau vers la dernière version.

Journaux clients en mode kiosque

Pour collecter les journaux en mode kiosque :

1. Connectez un périphérique USB amovible à votre Chromebook.
2. Téléchargez le fichier journal.
3. Enregistrez le fichier journal sur le périphérique USB connecté.

   Le fichier journal est transféré sur le périphérique USB.

Raccourcis

- Le raccourci clavier Ctrl+Alt+Maj+1 peut ne pas fonctionner dans Microsoft Teams optimisé au sein d'un poste de travail virtuel. Pour contourner le problème, ouvrez le **clavier à l'écran** et utilisez le raccourci. [RFHTMCRM-5441]

Outil Configuration Utility

May 16, 2024

Il existe quatre options pour personnaliser l'application Citrix Workspace pour ChromeOS :

- configuration.js
- web.config
- default.ica
- Stratégie Google

Les quatre options sont disponibles sur l'outil Configuration Utility, une page Web de configuration basée sur l'interface utilisateur.

Téléchargez l'outil Configuration Utility depuis la page Téléchargements.

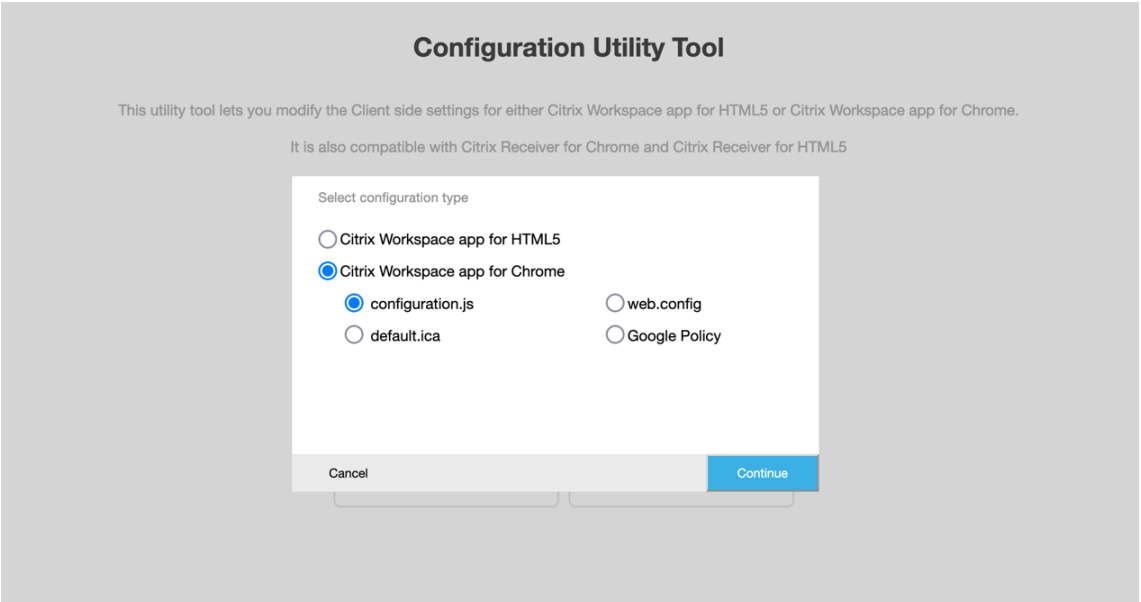
Comment utiliser l'outil Configuration Utility

1. Cliquez sur **Create New**.
2. Sélectionnez **Citrix Workspace app for Chrome** et choisissez l'une des quatre options de configuration. Cliquez ensuite sur **Continue** pour continuer ou cliquez sur **Cancel** pour revenir à la page d'accueil.

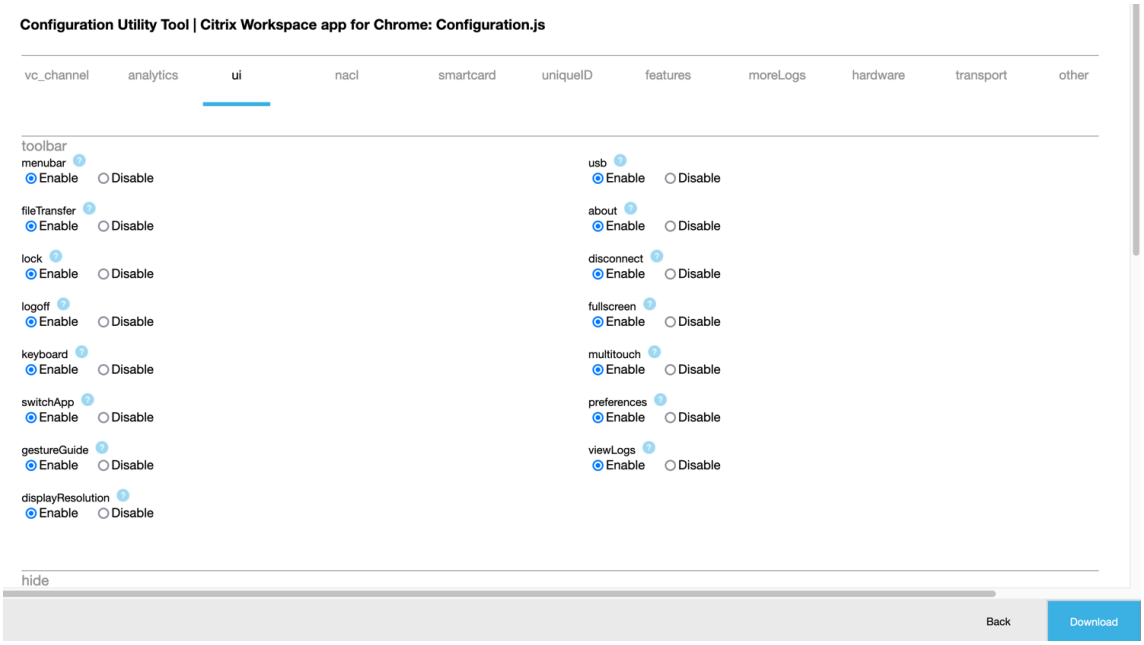
Pour configuration.js

Pour créer une configuration

1. Après avoir sélectionné **configuration.js**, cliquez sur **Continue** pour configurer ou cliquez sur **Cancel** pour revenir à la page d'accueil.



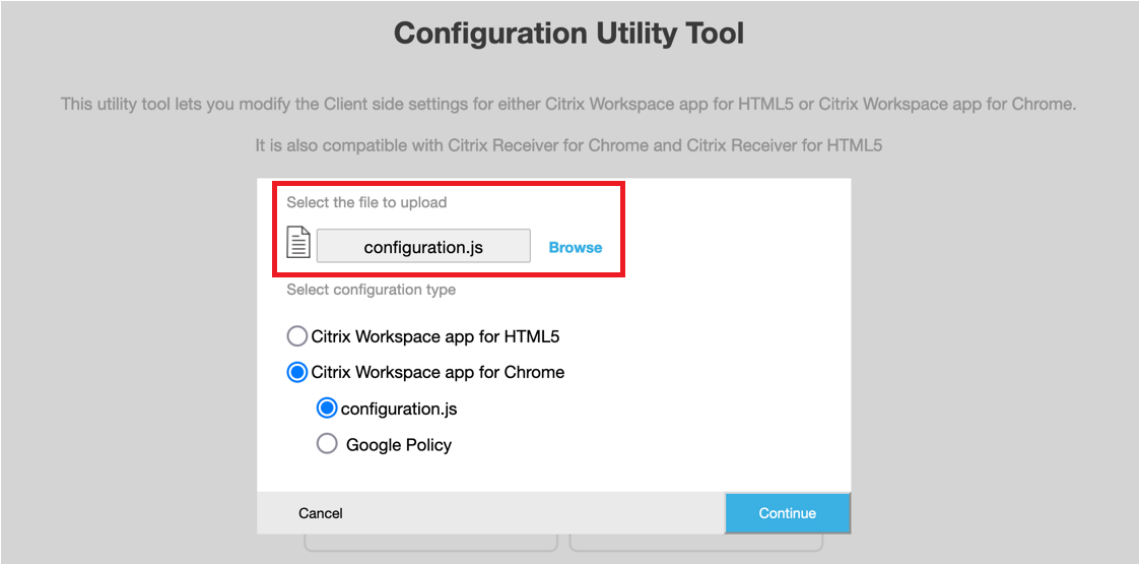
2. Dans l'outil **Configuration Utility Tool**, sélectionnez la fonctionnalité souhaitée et choisissez les valeurs appropriées.



3. Cliquez sur **Download** pour télécharger le fichier configuration.js.

Pour modifier une configuration

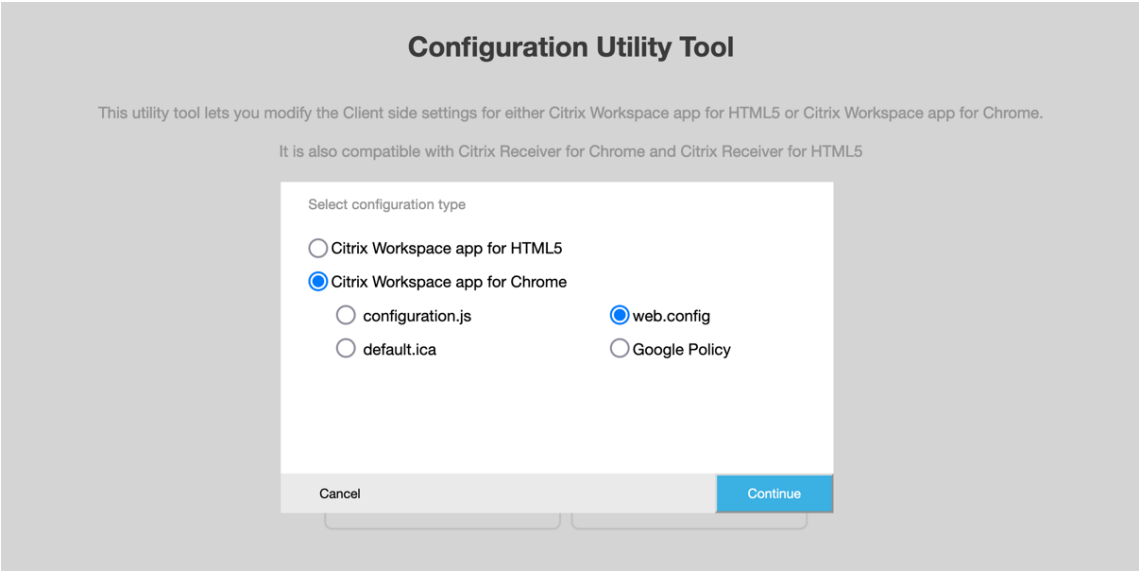
1. Cliquez sur **Upload existing file**.
2. Sélectionnez **Citrix Workspace app for Chrome** et sélectionnez **configuration.js**.
3. Cliquez sur **Browse** et accédez à l'emplacement du fichier configuration.js pour sélectionner et charger le fichier.



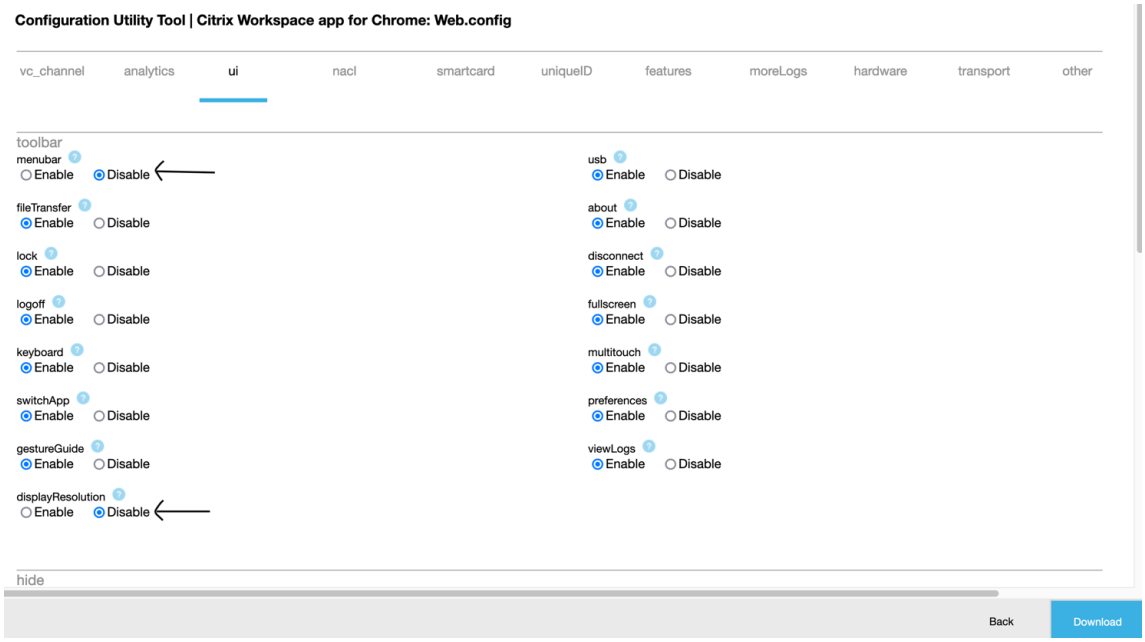
4. Cliquez sur **Continue** pour configurer ou sur **Cancel** pour revenir à la page d'accueil.
5. Sélectionnez les fonctions souhaitées et choisissez les valeurs appropriées.
6. Cliquez sur **Download** pour télécharger le fichier configuration.js.

Pour web.config (dans StoreFront)

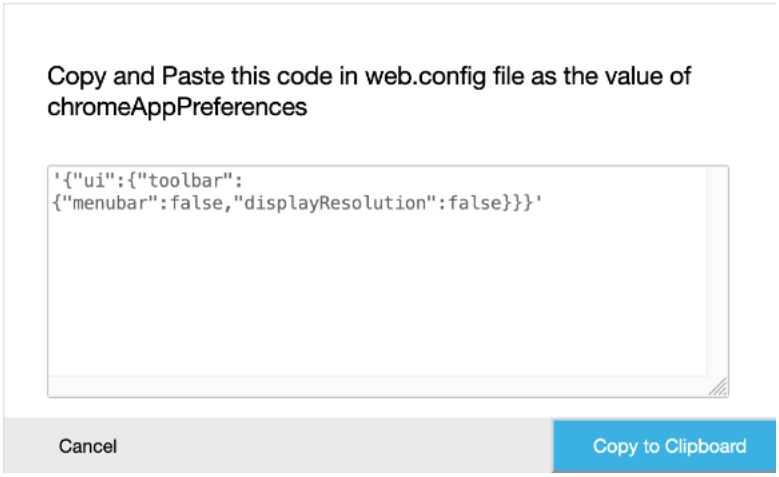
1. Après avoir sélectionné **web.config**, cliquez sur **Continue** pour configurer ou cliquez sur **Cancel** pour revenir à la page d'accueil.



2. Sélectionnez les paramètres souhaités et leurs valeurs appropriées et cliquez sur **Télécharger**(par exemple, sélectionnez menubar : désactiver ; displayResolution : désactiver)



3. Copiez le contenu dans la boîte de dialogue.



4. Ouvrez le fichier web.config du site Citrix Receiver pour Web. Le fichier est situé dans **C:\inetpub\wwwroot\Citrix\nomdumagasinWeb**, où nomdumagasin est le nom spécifié pour le magasin lors de sa création.
5. Localisez le champ chromeAppPreferences dans le fichier et définissez sa valeur avec la chaîne JSON copiée dans la boîte de dialogue.

```
chromeAppPreferences = '{

    "ui":{

        "toolbar":{

            "menubar":false,"displayResolution":false
             }
```

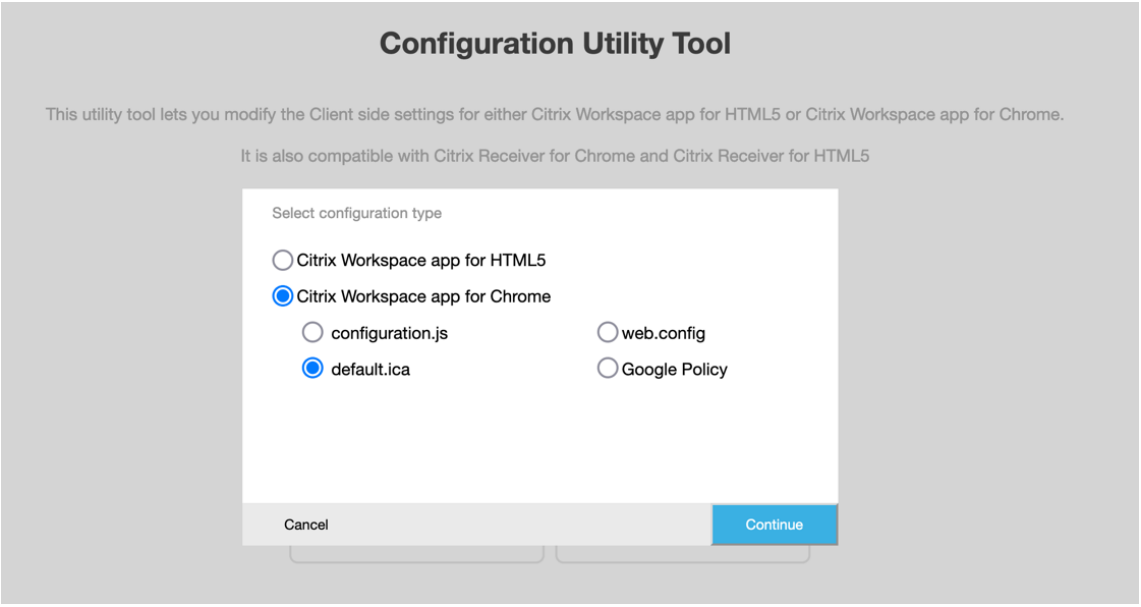


```
                        }

                        }
 '
<!--NeedCopy-->
```

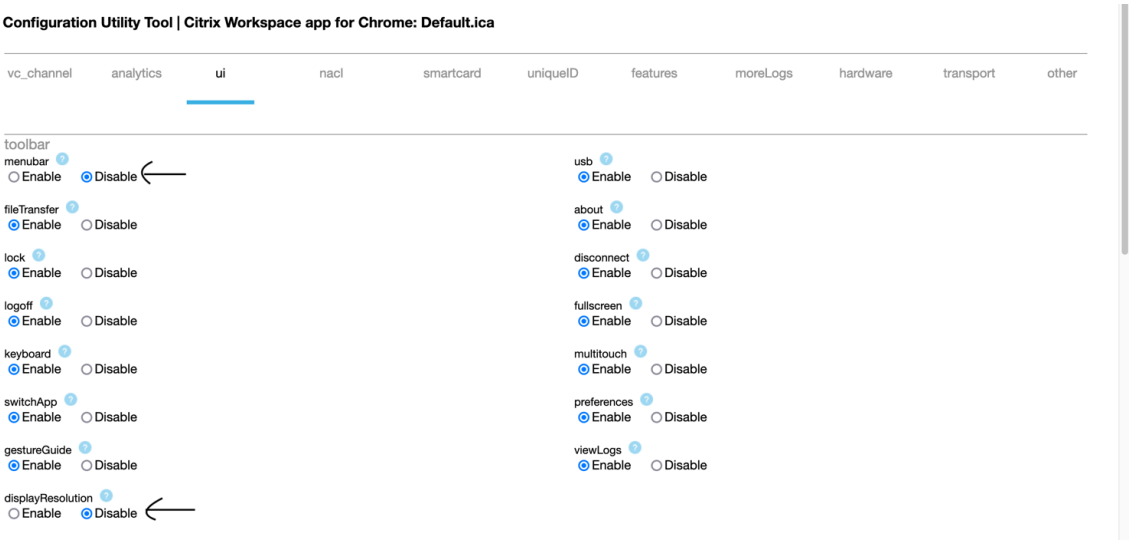
```
web.config  default.ica
    <csrfProtection excludedUserAgents="CitrixReceiver;CitrixWebAPI-NoCSRFToken" />
  </serverSettings>
  <clientSettings>
    <authManager getUsernameURL="Authentication/GetUserName" logoffURL="Authentication/Logoff"
      changeCredentialsURL="ExplicitAuth/GetChangeCredentialForm"
      loginFormTimeout="5" webviewReturnURL="ExplicitAuth/Bounce"
      webviewResumeURL="ExplicitAuth/ResumeForms" allowSelfServiceAccountManagementURL="ExplicitAuth
    <storeProxy keepAliveURL="Home/KeepAlive">
      <resourcesProxy listURL="Resources/List" resourceDetails="default" />
      <sessionsProxy listAvailableURL="Sessions/ListAvailable" disconnectURL="Sessions/Disconnect"
        logoffURL="Sessions/Logoff" />
      <clientAssistantProxy getDetectionTicketURL="ClientAssistant/GetDetectionTicket"
        getDetectionStatusURL="ClientAssistant/GetDetectionStatus" />
    </storeProxy>
    <pluginAssistant enabled="true" upgradeAtLogin="false" showAfterLogin="false">
      <win32 path="http://downloadplugins.citrix.com/Windows/CitrixReceiverWeb.exe" />
      <macOS path="http://downloadplugins.citrix.com/Mac/CitrixReceiverWeb.dmg"
        minimumSupportedOSVersion="10.6" />
      <html5 enabled="Fallback" platforms="Firefox;Chrome;Version/([6-9]|\d\d).*Safari;MSIE \d\d;Tri
        launchURL="clients/HTML5Client/src/SessionWindow.html" preferences=""
        singleTabLaunch="false" chromeAppOrigins="chrome-extension://haiffjcadagjlijoggckpgfnoeiflne
        chromeAppPreferences = '{"ui":{"toolbar":{"menubar":false,"displayResolution":false}}}' />
      <protocolHandler enabled="true" platforms="(Macintosh|Windows NT).*((Firefox/((5[2-9]|[6789][0
        skipDoubleHopCheckWhenDisabled="false" />
    </pluginAssistant>
```

Pour default.ica

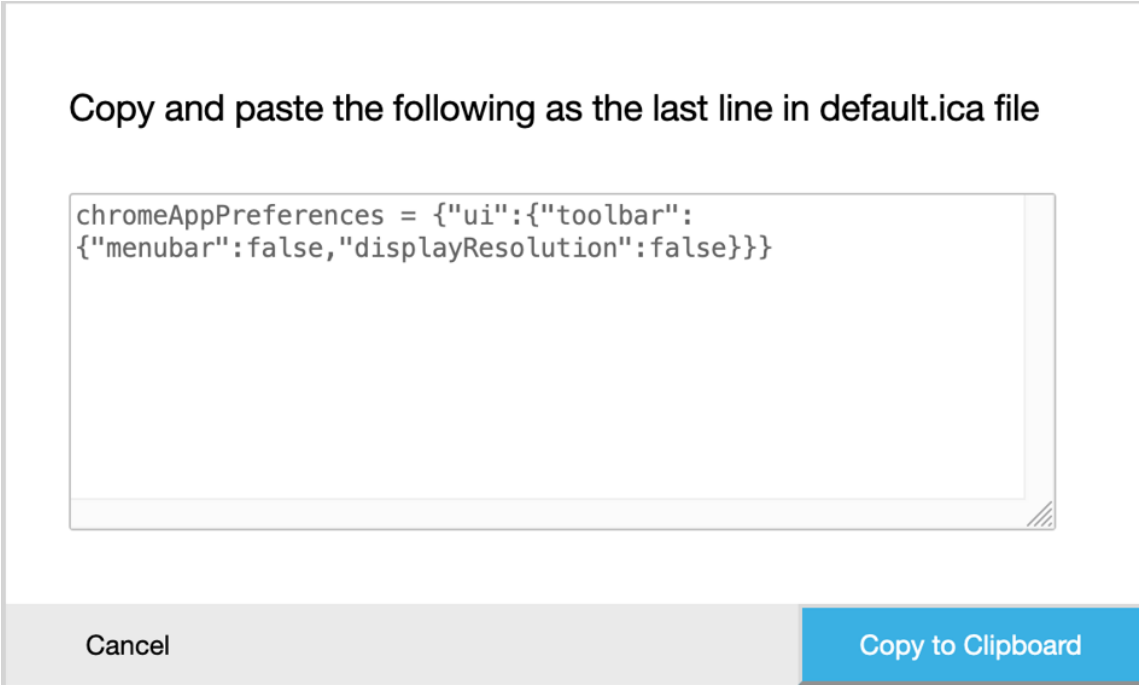
1. Après avoir sélectionné **default.ica**, cliquez sur **Continue** pour configurer ou cliquez sur **Cancel** pour revenir à la page d'accueil.



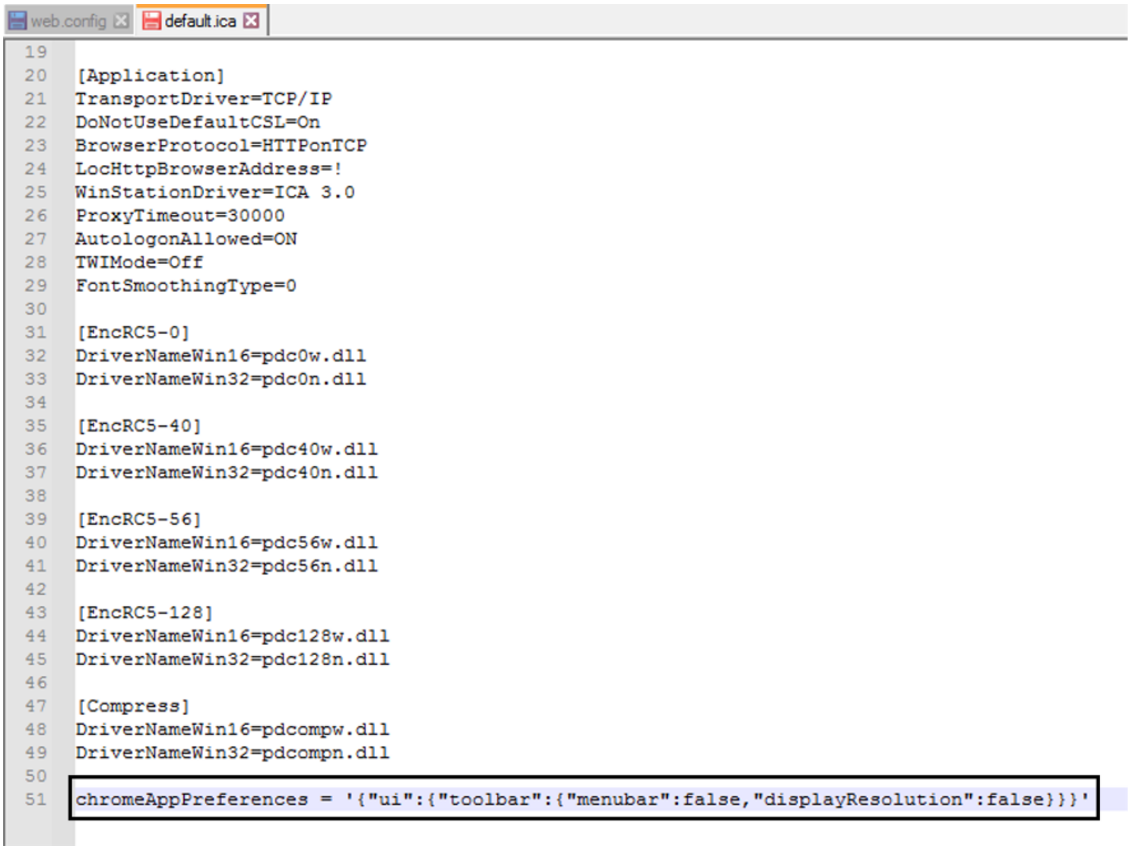
2. Sélectionnez les paramètres souhaités et leurs valeurs appropriées et cliquez sur **Télécharger**(par exemple, sélectionnez **menubar** > **désactiver** et **displayResolution** > **désactiver**).



3. Copiez le contenu dans la boîte de dialogue.



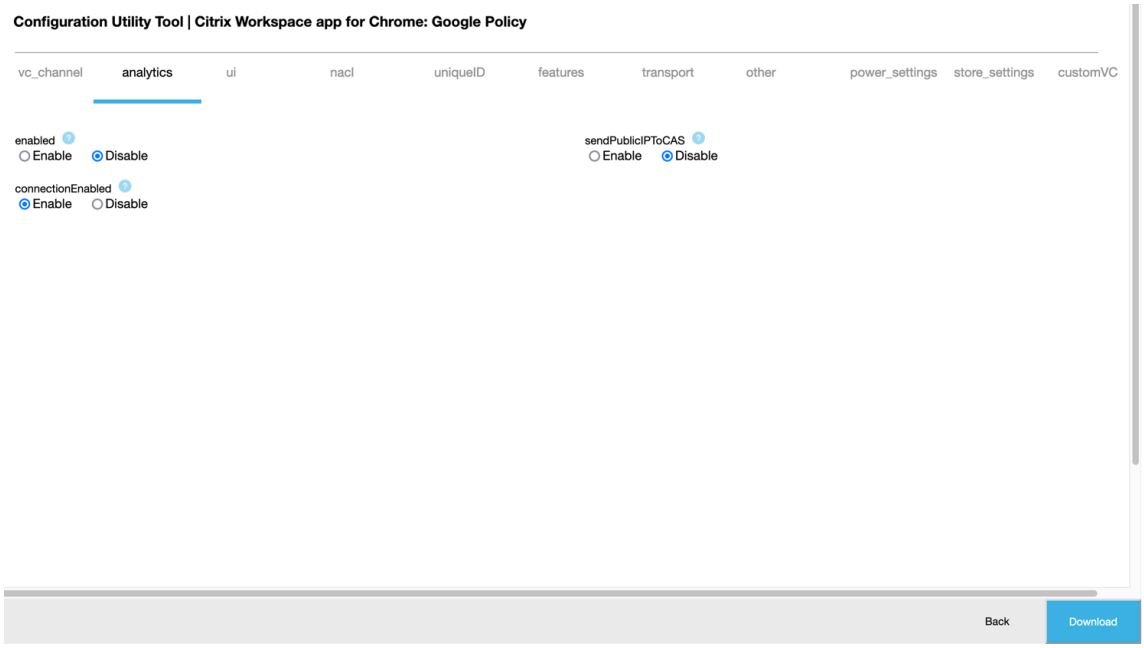
4. Ouvrez le fichier default.ica qui se trouve généralement sur **C:\inetpub\wwwroot\Citrix\<nom du site>\conf\default.ica** pour les clients Interface Web, où site name est le nom spécifié pour le site lors de sa création. Pour les clients StoreFront, le fichier default.ica figure généralement dans **C:\inetpub\wwwroot\Citrix\<nom du magasin>\App_Data\default.ica**, où nom du magasin est le nom spécifié pour le magasin lors de sa création.
5. Ajoutez le contenu dans la dernière ligne du fichier default.ica comme indiqué.



Pour la stratégie Google

Comment créer une configuration

1. Après avoir sélectionné **Google Policy**, cliquez sur **Continue** pour configurer ou cliquez sur **Cancel** pour revenir à la page d'accueil.
2. Sélectionnez les paramètres souhaités et leurs valeurs appropriées et cliquez sur **Télécharger** (par exemple, sélectionnez sendPublicIPToCas : disabled)



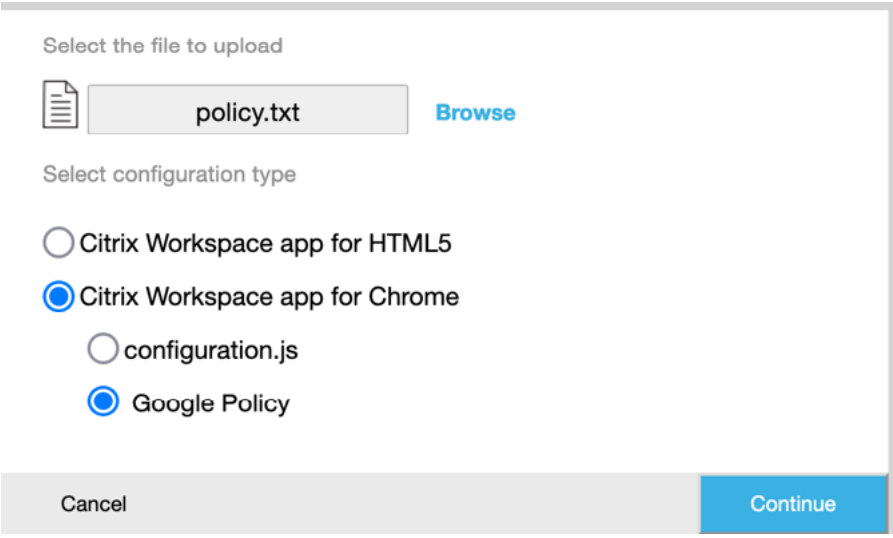
3. Lorsque vous cliquez sur **Télécharger**, le fichier **policy.txt** est créé.

Comment modifier une configuration

> **Limitation des fonctionnalités :**
>
> Vous ne pouvez modifier que les valeurs et les paramètres présents dans le fichier de chargement (**policy.txt**). Si vous devez modifier d'autres stratégies, créez un fichier de stratégie pour inclure les paramètres. Pour plus d'informations, consultez Comment créer une configuration.

1. Cliquez sur **Upload existing file**.

2. Sélectionnez **Application Citrix Workspace pour Chrome**, puis sélectionnez le fichier **policy.txt**.



3. Cliquez sur **Parcourir** et accédez à l'emplacement du fichier **policy.txt** pour sélectionner et charger le fichier.
4. Cliquez sur **Continue** pour modifier ou cliquez sur **Cancel** pour revenir à la page d'accueil.
5. Modifiez les paramètres en choisissant les valeurs appropriées.
6. Cliquez sur **Télécharger** pour télécharger le fichier **policy.txt** mis à jour.

Authentification

June 18, 2024

Carte à puce

L'application Citrix Workspace pour ChromeOS prend en charge les lecteurs de carte à puce USB avec StoreFront. Vous pouvez utiliser des cartes à puce aux fins suivantes :

- Authentification par carte à puce à l'application Citrix Workspace.
- Applications publiées prenant en charge les cartes à puce pour accéder aux lecteurs de carte à puce locaux.
- Cartes à puce pour la signature de documents et d'e-mails. Par exemple, Microsoft Word et Outlook lancés dans les sessions ICA.

Cartes à puce prises en charge (avec lecteurs de cartes à puce USB) :

- PIV (Personal Identity Verification)
- CAC (Common Access Cards)

Logiciels requis

- StoreFront versions 3.6 ou supérieures
- XenDesktop 7.6 ou version ultérieure
- XenApp 6.5 ou version ultérieure
- Citrix Virtual Apps and Desktops 1808 ou version ultérieure
- Application Citrix Workspace 1808 ou version ultérieure

> **Important :**
>
> - Pour l'authentification par carte à puce à StoreFront 3.5 ou version antérieure, vous avez besoin d'un script personnalisé pour activer l'authentification par carte à puce. Contactez l'assistance Citrix pour obtenir de l'aide.
> - Pour accéder aux dernières informations sur les versions prises en charge, consultez les étapes du cycle de vie pour l'application Citrix Workspace et Citrix Virtual Apps and Desktops.

Prérequis pour la configuration de l'appareil

- Google Smart Card Connector est une application qui interagit avec les lecteurs de cartes à puce USB de l'appareil. L'application de connecteur divulgue les API Personal Computer Smart Card (PCSC) Lite à d'autres applications, y compris l'application Citrix Workspace.
- Les fournisseurs de certificats sont les applications intermédiaires écrites par les fournisseurs qui interagissent avec le connecteur de carte à puce. Les applications intermédiaires accèdent au lecteur de carte à puce, lisent les certificats et fournissent des certificats de carte à puce à ChromeOS.

  Les applications intermédiaires implémentent également la fonctionnalité de signature à l'aide d'invites de saisie du code PIN.
  Par exemple, CACKey.

  Pour plus d'informations, consultez Déployer des cartes à puce sur ChromeOS.
- Lorsque vous configurez l'authentification par carte à puce sur StoreFront, l'application Citrix Workspace demande à ChromeOS de fournir des certificats clients sur la carte à puce. ChromeOS présente les certificats qu'il a reçus des fournisseurs. Les invites de saisie du code PIN indiquent l'authentification.

L'application Citrix Workspace possède une liste approuvée de systèmes d'exploitation autorisés pour l'authentification par carte à puce. StoreFront 3.6 et versions ultérieures approuvent également ChromeOS. Pour les versions antérieures de StoreFront, vous pouvez utiliser un script personnalisé pour autoriser l'authentification par carte à puce sur ChromeOS. Contactez le support technique Citrix pour obtenir un script personnalisé.

- L'application Citrix Workspace ne contrôle pas le flux d'authentification par carte à puce avec StoreFront. Toutefois, dans certains cas, StoreFront peut vous demander de fermer le navigateur pour effacer les cookies.

  Pour effacer tous les cookies et recharger l'URL du magasin, cliquez sur le bouton de rechargement dans l'application Citrix Workspace pour ChromeOS.

  Parfois, pour effacer tous les cookies, vous pouvez vous déconnecter de l'appareil ChromeOS.

- Lorsque vous tentez de lancer une session de bureau ou d'application, l'application Citrix Workspace n'utilise pas la redirection de carte à puce. Au lieu de cela, elle interagit avec l'application de connecteur de carte à puce pour les API PC/SC lite.

  Les invites de saisie du code PIN requises pour la connexion à Windows apparaissent au cours de la session. Ici, les fournisseurs de certificats n'ont aucun rôle. L'application Citrix Workspace gère les activités dans la session telles que le double saut ou la signature d'e-mails.

Limites relatives aux cartes à puce

- Lorsque vous retirez la carte à puce de l'appareil ChromeOS, le certificat de carte à puce est mis en cache. Ce comportement est un problème connu qui existe dans Google Chrome. Redémarrez l'appareil ChromeOS pour effacer le cache.
- Lorsque l'application Citrix Workspace pour ChromeOS est reconditionnée, en tant qu'administrateur, obtenez l'approbation AppID auprès de Google. Cela confirme que l'application du connecteur de carte à puce est approuvée.
- Seul un lecteur de carte à puce est pris en charge à la fois.
- Les cartes à puce virtuelles et les cartes à puce rapides ne sont pas prises en charge.
- Les cartes à puce ne sont pas prises en charge sur Citrix Workspace (cloud).

Pour configurer la prise en charge de carte à puce sur votre appareil ChromeOS

1. Installez l'application de connecteur de carte à puce. L'application de carte à puce est requise pour la prise en charge de la carte PCSC (Personal Computer Smart Card) sur l'appareil ChromeOS. Cette application lit la carte à puce à l'aide de l'interface USB. Vous pouvez installer cette application depuis le site Web de Chrome.

2. Installez l'application middleware. Une application intermédiaire est requise en tant qu'interface de communication avec la carte à puce et les autres certificats clients. Par exemple, Charismathics ou CACkey :

    - Pour installer l'extension de carte à puce Charismathics ou CACKey, reportez-vous aux instructions du site Web de Chrome.
    - Pour de plus amples informations sur les applications middleware et l'authentification par carte à puce, reportez-vous au site de support de Google.

3. Configuration de l'authentification par carte à puce avec :

    - Citrix Gateway
    - Console de gestion StoreFront

    Pour plus d'informations, consultez Configuration de l'authentification par carte à puce et Configuration du service d'authentification dans la documentation de Citrix Gateway.

Authentification SAML

Pour configurer le Single Sign-On :

1. Configurez le fournisseur d'identité (IdP) tiers pour l'authentification SAML s'il n'est pas déjà configuré. Par exemple, ADFS 2.0.

    Pour obtenir davantage d'informations, veuillez consulter l'article CTX133919 du centre de connaissances.

2. Configurez le Single Sign-On avec Google Apps à l'aide du fournisseur d'identité SAML. La configuration permet aux utilisateurs d'appliquer une identité tierce afin d'utiliser les applications Google au lieu du compte Google Enterprise.

    Pour de plus amples informations, consultez l'article Configurer l'authentification unique pour les comptes Google gérés faisant appel à des fournisseurs d'identité tiers sur le Centre d'aide de Google.

3. Configurez les appareils Chrome pour qu'ils se connectent via le fournisseur d'identité SAML. La configuration permet aux utilisateurs de se connecter à des appareils Chrome à l'aide d'un fournisseur d'identité tiers.

    Pour de plus amples informations, consultez l'article Configurer l'authentification unique SAML sur les appareils Chrome sur le Centre d'aide Google.

4. Configurez Citrix Gateway pour vous connecter via le fournisseur d'identité SAML. La configuration permet aux utilisateurs de se connecter à Citrix Gateway à l'aide d'un fournisseur d'identité tiers.

Pour plus d'informations, consultez la section Configuring SAML Authentication.

5. Configurez Citrix Virtual Apps and Desktops pour l'authentification fédérée afin d'autoriser la connexion aux sessions Citrix Virtual Apps and Desktops à l'aide de certificats générés dynamiquement. Vous pouvez effectuer cette action après la connexion SAML au lieu de saisir un nom d'utilisateur et un mot de passe.

   Pour plus d'informations, consultez la section Service d'authentification fédérée.

   Pour obtenir l'authentification unique pour les Virtual Apps and Desktops, vous devez déployer un service d'authentification fédérée (FAS).

   > **Remarque :**
   >
   > Sans FAS, vous êtes invité à saisir le nom d'utilisateur et le mot de passe Active Directory. Pour plus d'informations, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

6. Installez et configurez le SSO SAML pour l'extension d'application Chrome sur les appareils Chrome. Pour de plus amples informations, consultez le site Web de Google. Cette extension récupère les cookies SAML depuis le navigateur et les communique à l'application Citrix Workspace. Cette extension doit être configurée avec la stratégie suivante pour permettre à Citrix Workspace d'obtenir les cookies SAML.

   Si vous reconditionnez l'application Citrix Workspace pour ChromeOS, changez l'appId correctement. Changez également le domaine au profit du domaine IdP SAML de votre entreprise.

```
{

    "whitelist" : {

        "Value" : [
            {

            "appId" : "haiffjcadagjlijoggckpgfnoeiflnem",
            "domain" : "saml.yourcompany.com"
             }

        ]
      }

 }

<!--NeedCopy-->
```

7. Configurez Citrix Workspace de manière à utiliser Citrix Gateway configuré pour la connexion SAML. La configuration permet aux utilisateurs d'utiliser Citrix Gateway configuré pour la connexion SAML. Pour de plus amples informations sur la configuration de ChromeOS, consultez l'article CTX141844 du centre de connaissances.

Authentification unique pour l'application Citrix Workspace utilisant Okta comme fournisseur d'identité

May 16, 2024

Vous pouvez configurer l'authentification unique (SSO) pour l'application Citrix Workspace en utilisant Okta comme fournisseur d'identité.

Logiciels requis

Les prérequis suivants nécessitent des privilèges d'administrateur :

- 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.

- Application 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 (AD)

Comment configurer l'authentification unique (SSO)

Voici les étapes à suivre pour configurer l'authentification unique pour l'application Citrix Workspace en utilisant Okta en tant que fournisseur d'identité :

1. Installer l'agent Okta AD
2. Créer une intégration d'application Web Okta OIDC
3. Configurer l'application Web Okta OIDC
4. Créer un jeton API Okta
5. Connecter Citrix Cloud à votre organisation Okta
6. Activer l'authentification Okta pour les espaces de travail
7. Configurer le contournement de l'authentification multifacteur (MFA) Okta
8. Configurer l'agent Integrated Windows Authentication (IWA) Okta
9. Configurer la règle de routage du fournisseur d'identité
10. Configurer le fournisseur d'identité Okta avec Google Admin Console
11. Configurer l'authentification unique pour l'application Citrix Workspace pour ChromeOS à l'aide de l'extension d'authentification unique SAML pour Chrome

Installer l'agent Okta AD

Pré-requis :

Avant d'installer l'agent, assurez-vous de satisfaire aux conditions requises indiquées dans le lien des conditions préalables à l'intégration d'Active Directory.

Pour installer l'agent Okta AD :

1. Dans le portail d'administration Okta, cliquez sur **Directory** > **Directory Integrations**.
2. Cliquez sur **Add Directory** > **Add Active Directory**.
3. 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.
4. Cliquez sur le bouton **Set Up Active Directory**, puis sur **Download Agent**.
5. Installez l'agent Okta AD sur un serveur Windows en suivant les instructions fournies dans Install the Okta AD agent.

Créer une intégration d'application Web Okta OIDC

Pour utiliser Okta en tant que fournisseur d'identité, une application Web Okta **OIDC (OpenID Connect)** doit être créée afin que les informations d'identification de l'utilisateur puissent être utilisées avec Citrix Cloud. Cette application lance la séquence de connexion et gère également la redirection vers l'URL Citrix Workspace en cas de déconnexion.

Pour en savoir plus, voir Créer une intégration d'application Web Okta OIDC.

Configurer l'application Web Okta OIDC

Une fois l'application Okta OIDC créée, configurez-la avec les paramètres requis pour Citrix Cloud. Ces paramètres sont requis à des fins d'authentification lorsque les abonnés se connectent à Citrix Workspace avec Okta.

Pour en savoir plus, consultez le lien Configurer l'application Web Okta OIDC.

Créer un jeton API Okta

Pour en savoir plus sur la création d'un jeton API Okta, voir Créer un jeton API Okta.

Connecter Citrix Cloud à votre organisation Okta

Pour en savoir plus sur la manière de connecter Citrix Cloud, voir Connecter Citrix Cloud à votre entreprise Okta.

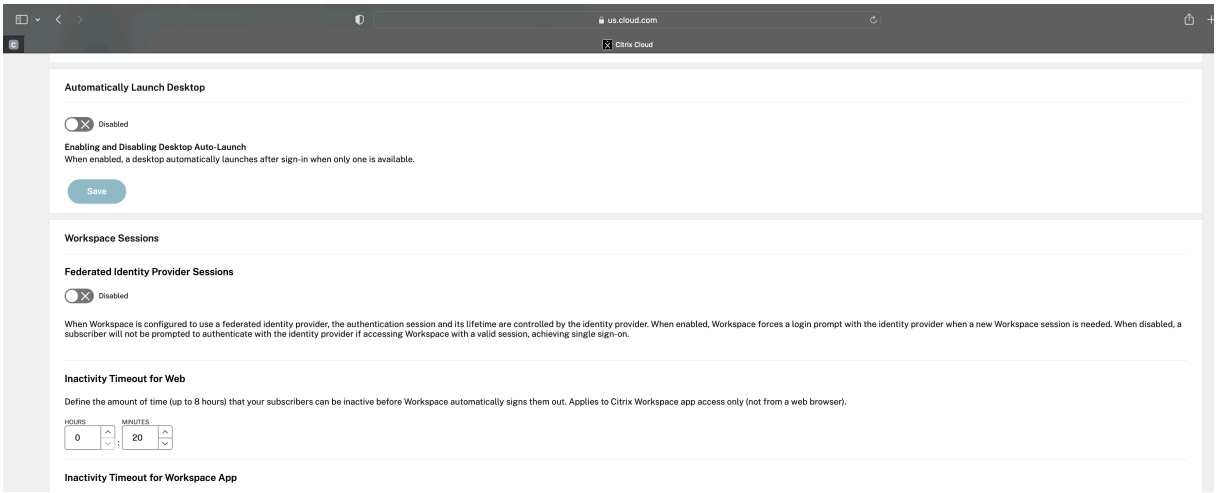
Activer l'authentification Okta pour les espaces de travail

Pour en savoir plus sur l'activation de l'authentification Okta, voir Activer l'authentification Oktapour les espaces de travail.

Configurer le contournement de l'authentification multifacteur (MFA) Okta

Créez une zone réseau définissant un ensemble d'adresses IP à faire figurer sur une liste blanche pour accéder à la configuration. Pour en savoir plus, voir Créer des zones pour les adresses IP.

Assurez-vous de désactiver l'option **Sessions de fournisseurs d'identité fédérés**. Accédez à la console cloud sous **Configuration de l'espace de travail** > **Personnaliser** > **Préférences** et désactivez les **sessions de fournisseurs d'identité fédérés**.



Configurer l'agent Integrated Windows Authentication (IWA) Okta

L'agent IWA Okta est un agent Web léger des Internet Information Services (IIS) qui active l'authentification unique pour ordinateur de bureau (DSSO) sur le service Okta.

La DSSO est utilisée si un ordinateur appartenant à un domaine accède à Citrix Cloud. Cet ordinateur appartenant à un domaine n'a pas besoin d'être invité à s'authentifier.

1. Assurez-vous que la liste de conditions préalables suivante est remplie.

   Pour obtenir la liste des conditions préalables pour installer l'agent Web IWA Okta, voir Conditions préalables à l'installation de l'agent Web IWA Okta.

2. Installer l'agent IWA Okta.

   Pour installer l'agent Web IWA Okta, voir Installer l'agent Web IWA Okta.

3. Configurez un navigateur Windows pour l'authentification unique.

   Pour configurer le navigateur Windows pour l'authentification unique, voir Configurer des navigateurs Windows pour l'authentification unique.

4. Tester l'agent Web IWA Okta.

   Après avoir téléchargé et installé l'agent Web IWA Okta, vérifiez si le serveur IWA fonctionne depuis une machine cliente.

   Si l'agent Okta est correctement configuré, des informations relatives à **UserPrincipalName** et **SecurityIdentifier** apparaissent.

   Pour en savoir plus sur la procédure de vérification, voir Tester l'agent Web IWA Okta.

Configurer la règle de routage du fournisseur d'identité

Pour configurer la **règle de routage du fournisseur d'identité**, voir Configurer la règle de routage du fournisseur d'identité.

> **Remarque :**
>
> Dans le champ **fournisseur(s) d'identité**, assurez-vous de sélectionner **OnPremDSSO**.

Configurer le fournisseur d'identité Okta avec Google Admin Console

1. Pour créer une application SAML (Security Assertion Markup Language), voir Créer des intégrations d'applications SAML.

   Assurez-vous de saisir une URL dans les champs **URL d'authentification unique** et **URI d'audience (ID d'entité SP)**. Par exemple, `https://admin.google.com`.

   > **Remarque :**
   >
   > Il se peut que vous deviez modifier l'exemple d'URL après avoir créé le profil SAML dans Google Admin Console. Pour plus de détails, consultez les étapes suivantes.

2. Configurer SAML avec un fournisseur d'identité tiers dans Google Admin Console.

   Pour créer un profil d'authentification unique (SSO) pour votre entreprise et attribuer les utilisateurs, suivez les étapes décrites dans le lien Créer un profil d'authentification unique SAML.

   Pour obtenir les informations de connexion, de déconnexion, d'émetteur et d'autres informations de fournisseur d'identité sur Okta pour le profil SAML, suivez les étapes décrites dans le lien Ajouter un fournisseur d'identité SAML.

3. Pour configurer un profil SAML, consultez le lien Comment configurer SAML 2.0 pour Google Workspace.

4. Configurer un profil SAML dans OKTA à l'aide des détails du profil SAML de Google pour synchroniser les profils :

   a) Cliquez sur **Sécurité** > **Authentification** > **Authentification unique avec un fournisseur d'identité tiers** > **Profils d'authentification unique tiers** > ouvrez votre profil SAML.

   b) Sur la page du tableau de bord Okta (fournisseur d'identité), ajoutez les détails du profil SAML de Google (fournisseur de services).

   - Cliquez sur **URL d'authentification unique > URL ACS**, puis sélectionnez l'option **Utiliser ceci pour l'URL du destinataire** et **l'URL de destination**.
   - Cliquez sur **URI d'audience (ID d'entité SP)** > **ID d'entité**.

Une fois les profils SAML de fournisseur d'identité et de fournisseur de services synchronisés, la page de connexion pour les utilisateurs gérés apparaît sur la page de connexion Okta du Chromebook.

5. Attribuez des utilisateurs à votre application OKTA SAML.

   Pour en savoir plus sur la manière d'attribuer des utilisateurs, consultez le lien Attribuer une intégration d'application à un utilisateur.

Points de contrôle de validation

- Lorsque les utilisateurs ajoutent le compte Google d'entreprise dans le Chromebook, ils peuvent se connecter à l'aide d'informations d'identification Okta.
- Une fois connecté au Chromebook, l'utilisateur doit pouvoir ouvrir le navigateur Google Chrome et saisir l'URL Citrix Workspace.
- L'utilisateur doit être en mesure de voir l'interface utilisateur de l'application Citrix Workspace. L'utilisateur doit pouvoir accéder aux applications et aux bureaux virtuels sans avoir à fournir ses informations d'identification.

> **Remarque :**
>
> Si l'authentification unique échoue, recommencez l'étape Configurer le fournisseur d'identité Okta avec Google Admin Console.

Configurer l'authentification unique pour l'application Citrix Workspace pour ChromeOS à l'aide de l'extension d'authentification unique SAML pour Chrome

Pour configurer l'authentification unique à l'aide de l'extension SAML, procédez comme suit :

1. Installez et configurez le SSO SAML pour l'extension d'application Chrome sur les appareils Chrome.

   Pour installer l'extension, cliquez sur Authentification unique SAML pour applications Chrome.

2. Cette extension récupère les cookies SAML depuis le navigateur et les communique à l'application Citrix Workspace pour ChromeOS.

3. Configurez l'extension avec la stratégie suivante pour permettre à Citrix Workspace d'obtenir les cookies SAML. Remplacez le domaine par le domaine du fournisseur d'identité Okta de votre entreprise.

```
{

    "whitelist" : {
```



```
4
5          "Value" : [
6              {
7
8                  "appId" : "haiffjcadagjlijoggckpgfnoeiflnem",
9                  "domain" : "<domain.okta.com>"
10                  }
11
12             ]
13          }
14
15  }
16
17 <!--NeedCopy-->
```

> **Remarque :**
>
> Si vous reconditionnez l'application Citrix Workspace pour ChromeOS, remplacez `haiffjcadagjlijoggckpgfnoeiflnem` par l'AppID reconditionné.

4. Déployer un service d'authentification fédérée (FAS) pour obtenir l'authentification unique sur les Virtual Apps and Desktops.

   Pour obtenir l'authentification unique pour les Virtual Apps and Desktops, vous pouvez déployer un service d'authentification fédérée (FAS) ou configurer l'application Citrix Workspace.

   > **Remarque :**
   >
   > - Sans FAS, vous êtes invité à saisir le nom d'utilisateur et le mot de passe Active Directory. Pour plus d'informations, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

Authentification unique pour l'application Citrix Workspace utilisant Microsoft Azure comme fournisseur d'identité

May 16, 2024

Vous pouvez configurer l'authentification unique (SSO) SAML (Security Assertion Markup Language) pour les appareils ChromeOS. Utilisez Microsoft Entra ID (anciennement Azure Active Directory) comme fournisseur d'identité SAML et Google Admin comme fournisseur de services.

Vous ne pouvez configurer cette fonctionnalité que pour les utilisateurs gérés. Nous avons ajouté à l'annuaire Active Directory (AD) local des machines virtuelles Citrix créées sur Azure, comme cas d'utilisation. Si vous possédez des machines virtuelles locales basées sur AD sur Azure et que les utilisateurs utilisent Microsoft Entra ID, suivez cet article.

Logiciels requis

Les prérequis suivants nécessitent des privilèges d'administrateur :

- Active Directory (AD)

  Installez et configurez un contrôleur de domaine actif dans votre configuration. Pour plus d'informations, consultez la section Installation d'AD DS à l'aide du Gestionnaire de serveur. Pour installer Active Directory Domain Services à l'aide du Gestionnaire de serveur, suivez les étapes 1 à 19.

- Autorité de certification (CA)

  Installez la CA. Pour plus d'informations, consultez la section Installer l'autorité de certification.

  Une autorité de certification peut être installée et configurée sur l'une des machines suivantes :

  - une nouvelle machine dédiée
  - une machine CA existante
  - une installation de ce composant d'autorité de certification sur Citrix Cloud Connector
  - la machine Active Directory

- Citrix Cloud et Citrix Cloud Connector

  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 Cloud Connector dans les environnements de production. Pour plus d'informations sur l'installation de Citrix Cloud Connector, consultez Installation de Cloud Connector.

- Compte administrateur global sur le portail Azure

  Vous devez être un administrateur global de Microsoft Entra ID. Ce privilège vous permet de configurer Citrix Cloud pour utiliser Entra ID en tant que fournisseur d'identité. Pour plus d'informations sur les autorisations demandées par Citrix Cloud lors de la connexion et de l'utilisation d'Entra ID, consultez la section Autorisations Azure Active Directory pour Citrix Cloud.

- 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.

- Compte administrateur global sur la console d'administration Google
- Application Citrix Workspace

Prise en main

Pour commencer, procédez comme suit :

- Joignez toutes les machines au domaine avant de configurer les logiciels installés ou les rôles qui s'y trouvent.
- Installez le logiciel Citrix Cloud Connector sur la machine correspondante, mais ne configurez rien pour l'instant.
- Installez le FAS Citrix sur la machine correspondante, mais ne configurez rien pour l'instant.

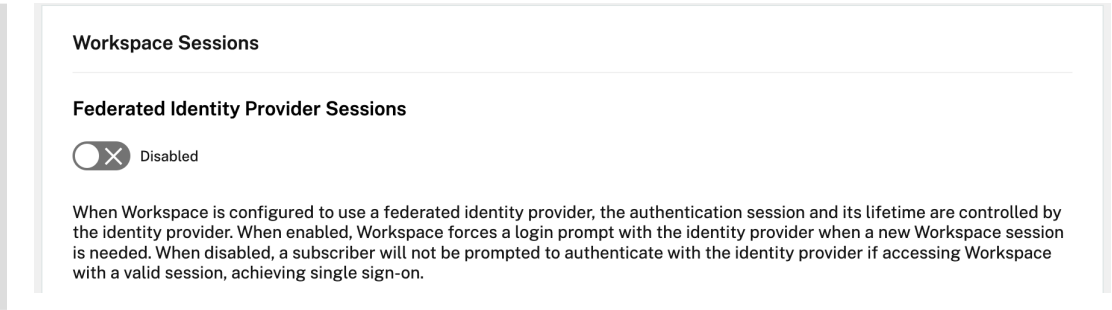
Comment configurer Citrix Cloud pour utiliser Azure AD en tant que fournisseur d'identité

> **Remarque :**
>
> Assurez-vous que vous remplissez tous les prérequis.

1. Pour connecter Entra ID à Citrix Cloud, consultez la section Connecter Azure Active Directory à Citrix Cloud.
2. Pour ajouter des administrateurs à Citrix Cloud à partir d'Entra ID, consultez la section Ajouter des administrateurs à Citrix Cloud depuis Azure AD.
3. Pour vous connecter à Citrix Cloud à l'aide d'Entra ID, consultez la section Se connecter à Citrix Cloud à l'aide d'Azure AD.
4. Pour activer les fonctionnalités avancées d'Entra ID, consultez la section Activer les fonctionnalités avancées d'Azure AD.
5. Pour vous reconnecter à Entra ID pour l'application mise à jour, consultez la section Se reconnecter à Azure AD pour l'application mise à jour.
6. Pour vous reconnecter à Entra ID, consultez la section Se reconnecter à Azure AD pour l'application mise à jour.
7. Pour synchroniser des comptes avec Entra ID Connect, consultez la section Synchroniser des comptes.

   Il est recommandé de synchroniser vos comptes AD locaux avec Entra ID.

   > **Remarque :**
   >
   > Désactivez l'invite de connexion pour les sessions de fournisseur d'identité fédéré dans la configuration Citrix Workspace.



Configurer l'authentification unique et le provisioning utilisateur entre Microsoft Azure et ChromeOS sur le portail Azure

Après avoir configuré le provisioning de l'authentification unique (SSO) entre un locataire Microsoft Entra ID et Google pour ChromeOS, les utilisateurs peuvent se connecter à une page d'authentification Azure plutôt qu'à l'écran de connexion Google sur leurs appareils ChromeOS.

Pour plus d'informations, consultez :

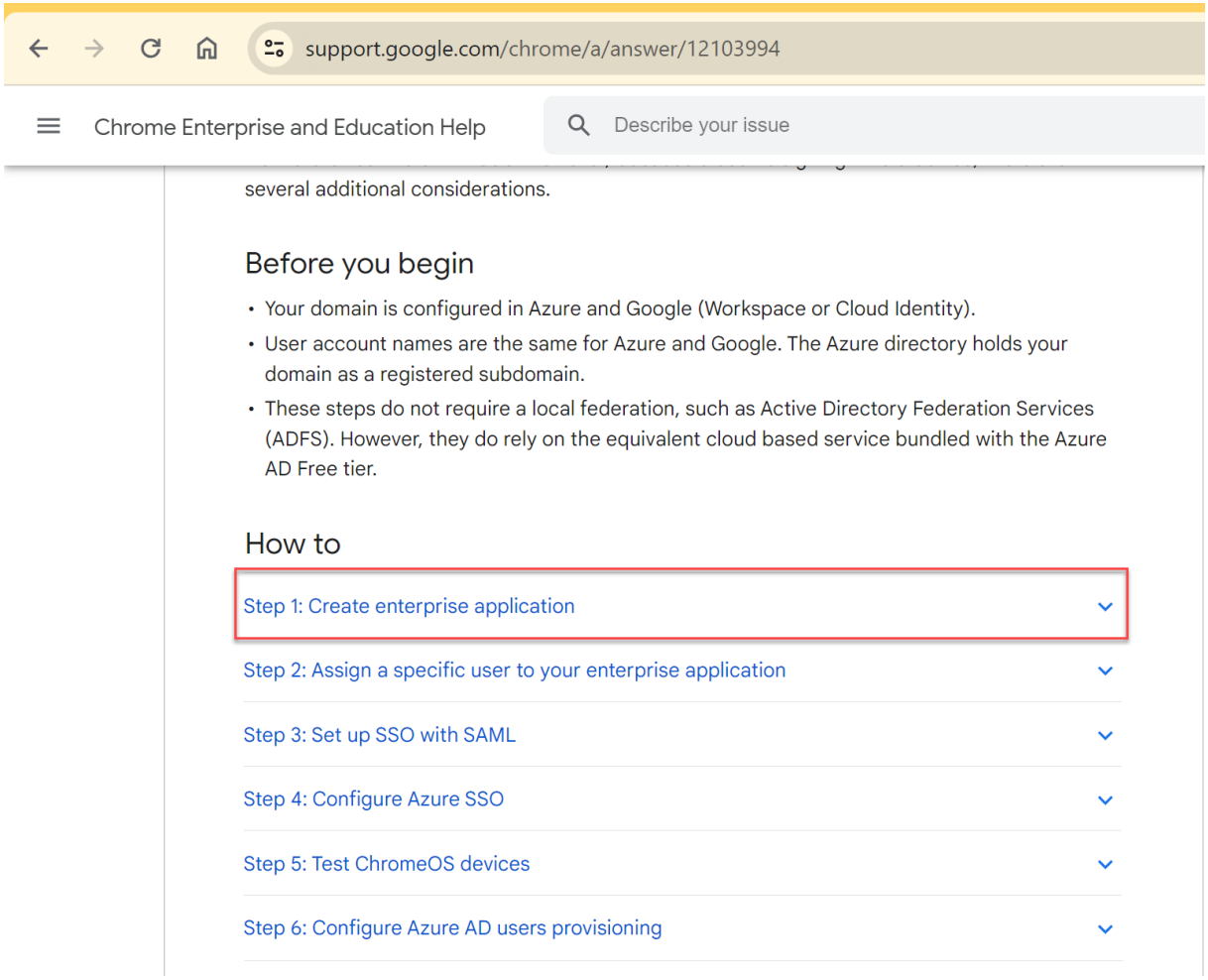
- L'article de Google Configurer l'authentification unique et le provisioning utilisateur entre Microsoft Azure et ChromeOS.

et

- Le didacticiel Microsoft Intégration de l'authentification unique Microsoft Entra avec Google Cloud/le connecteur G Suite par Microsoft.

Pour configurer l'authentification unique sur le portail Azure :

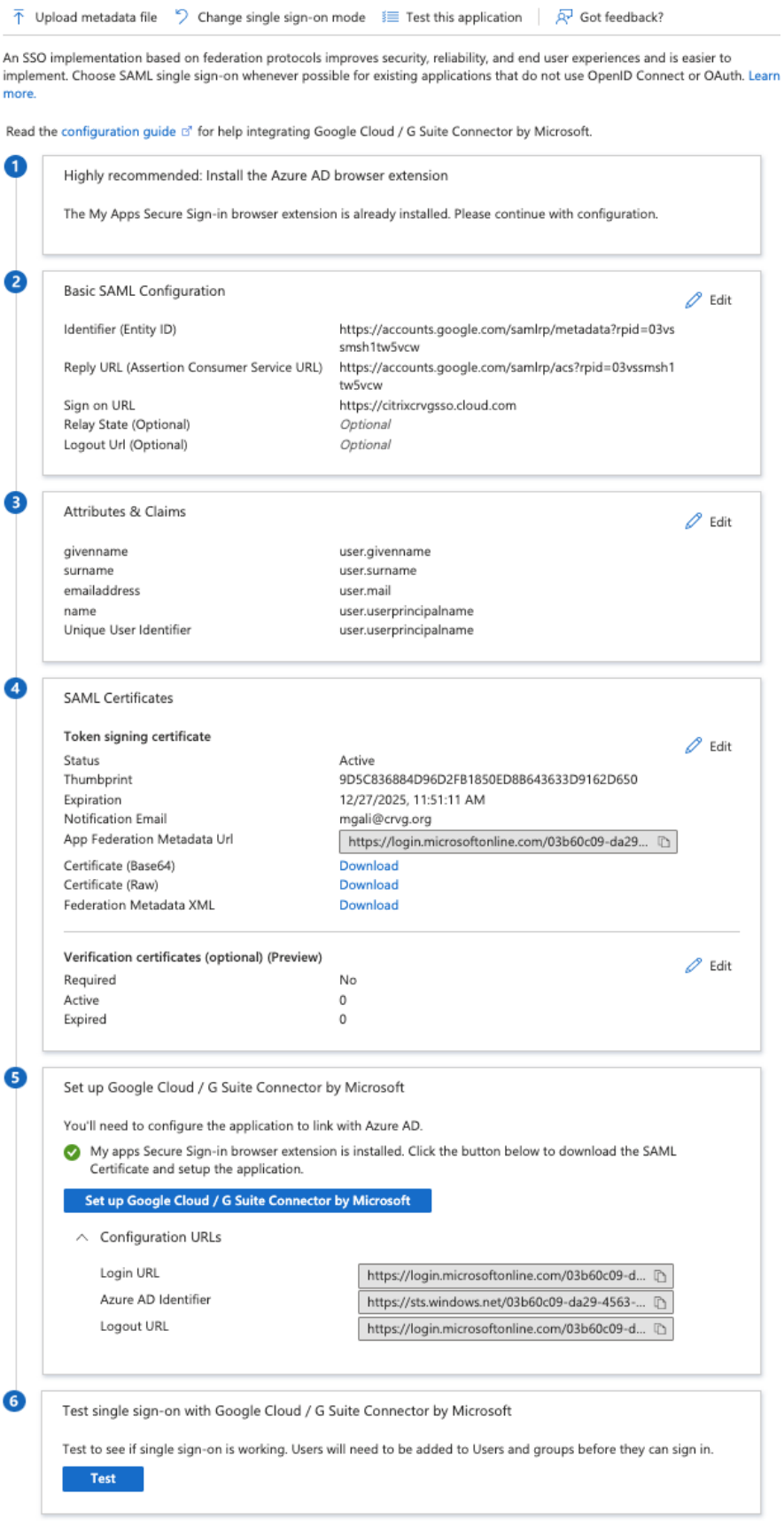
1. Créez une application d'entreprise sur le portail Microsoft Entra ID. Pour plus d'informations, consultez l'étape 1 de l'article de Google Configurer l'authentification unique et le provisioning utilisateur entre Microsoft Azure et ChromeOS.



1. Attribuez un ou plusieurs utilisateurs à l'application d'entreprise que vous avez créée à l'étape 1. Pour plus d'informations, consultez l'étape 2 de l'article de Google Configurer l'authentification unique et le provisioning utilisateur entre Microsoft Azure et ChromeOS.
2. Configurez l'authentification unique avec SAML. Pour plus d'informations, consultez l'étape 3 de l'article de Google Configurer l'authentification unique et le provisioning utilisateur entre Microsoft Azure et ChromeOS.

   > **Remarque :**
   >
   > Il est recommandé de modifier la configuration SAML de base après avoir créé la stratégie SAML dans la stratégie d'administration Google.

   Une fois que vous avez configuré des URL sur le portail Azure pour l'authentification unique basée sur SAML, l'application s'affiche comme suit.



> **Point de contrôle de validation**
>
> Lorsque vous saisissez l'URL du magasin, la page de connexion du fournisseur d'identité Azure doit apparaître. En cas d'échec, consultez à nouveau les étapes Configurer l'authentification unique et le provisioning utilisateur entre Microsoft Azure et ChromeOS sur le portail Azure.

Configurer le profil d'authentification unique SAML avec la console d'administration Google

- Ajoutez le domaine et les utilisateurs et créez une unité d'organisation. Pour plus d'informations, consultez le guide complet des unités d'organisation de Google.
- Créez le profil d'authentification unique SAML avec Microsoft Entra ID comme fournisseur d'identité. Pour plus d'informations, consultez la section Configurer l'authentification unique SAML pour les utilisateurs d'Azure AD.

> **Point de contrôle de validation**
>
> À l'aide du Chromebook, vous devez pouvoir vous connecter à l'application Citrix Workspace en utilisant les informations d'identification Azure. Lorsque vous saisissez l'URL du magasin dans le navigateur, vous devez pouvoir vous connecter.

Configurer l'authentification unique pour l'application Citrix Workspace pour ChromeOS à l'aide de l'extension d'authentification unique SAML pour Chrome

Pour configurer l'authentification unique à l'aide de l'extension SAML, procédez comme suit :

1. Installez et configurez le SSO SAML pour l'extension d'application Chrome sur les appareils Chrome.

   Pour installer l'extension, cliquez sur Authentification unique SAML pour applications Chrome.

2. Cette extension récupère les cookies SAML depuis le navigateur et les communique à l'application Citrix Workspace pour ChromeOS.

3. Configurez l'extension avec la stratégie suivante pour permettre à l'application Citrix Workspace d'obtenir les cookies SAML. Les données JSON sont les suivantes :

```
{

"allowlist": {

    "Value": [
        {

            "appId": "haiffjcadagjlijoggckpgfnoeiflnem",
```



```
            "domain": "login.microsoftonline.com"
        }

    ]
}

}

<!--NeedCopy-->
```

> **Point de contrôle de validation**
>
> Lorsque vous démarrez l'application Citrix Workspace avec le magasin du fournisseur d'identité Azure et l'extension de l'authentification unique, votre connexion à l'application Citrix Workspace doit aboutir.

Déployer un service d'authentification fédérée (FAS) pour obtenir l'authentification unique sur les Virtual Apps and Desktops

Pour obtenir l'authentification unique pour les Virtual Apps and Desktops, vous pouvez déployer un service d'authentification fédérée (FAS).

> **Remarque :**
>
> Sans FAS, vous êtes invité à saisir le nom d'utilisateur et le mot de passe Active Directory. Pour plus d'informations, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

SDK et API

May 16, 2024

SDK HDX

L'application Citrix Workspace pour ChromeOS introduit une API (API expérimentale) qui permet aux applications Chrome tierces de verrouiller, déverrouiller et se déconnecter :

- Citrix Virtual Apps and Desktops
- d'une session Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)

En utilisant cette API, vous pouvez lancer l'application Citrix Workspace pour ChromeOS à la fois en mode intégré et en mode Kiosque. Les sessions lancées en mode intégré fonctionnent de la même façon que les sessions lancées en mode kiosque.

Pour accéder à la documentation relative au SDK, consultez HDX SDK for Citrix Workspace app for ChromeOS.

Pour obtenir des exemples de SDK HDX, consultez la page de téléchargement de Citrix.

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 ou Citrix Virtual Apps and Desktops. Cette version du SDK prend en charge l'écriture de nouveaux canaux virtuels pour l'application Citrix Workspace pour ChromeOS. Si vous souhaitez écrire des pilotes virtuels pour d'autres plates-formes clientes, contactez Citrix.

Le SDK du canal virtuel offre ce qui suit :

- Une interface conviviale qui peut être utilisée avec les canaux virtuels du SDK de l'API Citrix Server (WFAPI SDK) pour créer de nouveaux canaux virtuels.
- Un code source opérationnel pour plusieurs exemples de programmes de canal virtuel qui illustrent les techniques de programmation.
- Le SDK de canal virtuel requiert le SDK WFAPI pour écrire sur le côté serveur du canal virtuel.

Pour accéder à la documentation relative au SDK de canal virtuel, consultez Citrix Virtual Channel SDK for Citrix Workspace app for ChromeOS.

Améliorations apportées au SDK du canal virtuel

À compter de la version 2305, l'application Citrix Workspace pour ChromeOS prend en charge les API de gestion des fenêtres dans le SDK du canal virtuel. Les API Web permettent aux administrateurs informatiques de créer des applications interactives et de les personnaliser pour leurs utilisateurs finaux.

Procédure à suivre pour consommer l'API dans l'application Chrome tierce

1. Installez la dernière version de l'application Citrix Workspace pour ChromeOS. Consultez la page des téléchargements Citrix pour de plus amples informations.

2. Ajoutez l'application Chrome tierce sur la liste verte en ajoutant le fichier de stratégie de l'application Citrix Workspace pour ChromeOS. Utilisez les paramètres de gestion de Chrome pour ajouter la stratégie.

   Pour de plus amples informations, consultez Gérer les applications Chrome par unité organisationnelle sur le Centre d'aide Google.

   Pour ajouter l'application Chrome tierce à la liste verte, voici un exemple de données `policy.txt` JSON :

```
{

      "settings": {

              "Value": {

              "settings_version": "1.0",
              "store_settings": {

              "externalApps": [“ <3rdParty_App1_ExtnID>” ,“ <3rdParty_App2_ExtnID>” ]
                                    }

                          }

                 }

 }

<!--NeedCopy-->
```

   > **Remarque :**
   >
   > `<3rdParty_App1_ExtnID>` est utilisé à titre d'exemple pour le nom de externalApps et peut envoyer des messages à l'application Citrix Workspace pour ChromeOS. Obtenez votre **ID d'application** (appid) sur le site chrome://extensions.

3. Lancez la session d'application ou de bureau dans Citrix Workspace pour ChromeOS comme suit :

- Obtenir le workspaceappID

  ```
  var workspaceappID = "haiffjcadagjlijoggckpgfnoeiflnem ";
  ```

  > **Remarque :**
  >
  > Dans cet exemple, **workspaceappID** indique la version du magasin de l'application Citrix Workspace pour ChromeOS. Si vous utilisez une version reconditionnée de l'application Citrix Workspace pour ChromeOS, utilisez le workspaceappID approprié.

- Convertissez les données ICA du format INI au format JSON.

> **Remarque :**
>
> Le fichier ICA est généralement récupéré depuis StoreFront en tant que fichier INI. Utilisez la fonction d'assistance suivante pour convertir un fichier ICA du format INI au format JSON.

```
//Helper function to convert ica in INI format to JSON
function convertICA_INI_TO_JSON(data){

var keyVals = {
 }
;
if (data) {

var dataArr;
if(data.indexOf('\r')==-1){

dataArr = data.split('\n');
 }
else{

dataArr = data.split('\r\n');
 }

for (var i = 0; i < dataArr.length; i++) {

var nameValue = dataArr[i].split('=', 2);
if (nameValue.length === 2) {

keyVals[nameValue[0]] = nameValue[1];
 }

// This is required as LaunchReference contains '=' as well. The above split('=',2) will not provide
// the complete LaunchReference. Ideally, something like the following should be used generically as well
// because there can be other variables that use the '=' character as part of the value.
if (nameValue[0] === "LaunchReference") {

var index = dataArr[i].indexOf('=');
var value = dataArr[i].substr(index + 1);
keyVals[nameValue[0]] = value;
 }

 }

console.log(keyVals);//to remove
return keyVals;
 }

return null;
```



```
 }


<!--NeedCopy-->
```

- Envoyez un message ICA depuis l'application Chrome tierce à l'application Citrix Workspace pour ChromeOS.

```
var icaFileJson = {
... }
; // ICA file passed as JSON key value pairs.
var message = {

"method" : "launchSession",
"icaData" : icaJSON
 }
;
chrome.runtime.sendMessage(workspaceappID, message,
function(launchStatus) {

if (launchStatus.success) {

// handle success.
console.log("Session launch was attempted successfully");
 }
 else {

// handle errors.
console.log("error during session launch: ", launchStatus.message
    );
 }

 }
);

<!--NeedCopy-->
```

Pour de plus amples informations sur les commandes API **sendMessage**, consultez les liens suivants :

https://developer.chrome.com/extensions/runtime#event-onMessageExternal

https://developer.chrome.com/extensions/runtime#method-sendMessage

Prise en charge du fichier manifeste V3 pour les scénarios du SDK

À compter de la version 2305, l'application Citrix Workspace pour ChromeOS prend en charge le SDK HDX avec les extensions Chrome dotées de la version 3 du fichier manifeste.

Pour plus d'informations, accédez à la page Citrix Workspace app for ChromeOS HDX SDK dans la documentation du développeur.

Fin de prise en charge

May 16, 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.

Élément	Abandon annoncé	Supprimé dans	Solution alternative
Aucun pour l'instant	-	-	-