

À propos de cette version

Nov 18, 2015

Receiver pour Chrome est hébergé sur des serveurs StoreFront et permet aux utilisateurs d'accéder à des bureaux virtuels et des applications hébergées depuis un navigateur Web. Les ressources fournies par XenDesktop et XenApp sont agrégées dans un magasin StoreFront et mises à disposition au travers d'un site Receiver pour Web. Lorsque Receiver pour Chrome est activé sur le site, les utilisateurs peuvent accéder aux bureaux et applications depuis leurs navigateurs Web sans avoir à installer Receiver localement sur leurs machines.

Lorsqu'elle est utilisée en conjonction avec les capacités de personnalisation et de valorisation de la marque centralisées de StoreFront 3.0, cette version de Receiver pour Chrome permet aux utilisateurs de bénéficier d'une expérience de sélection d'applications et de bureaux gérée de manière centralisée depuis StoreFront.

Nouveautés dans cette version

Ouverture de fichiers depuis Google Drive

La prise en charge de Google Drive dans XenApp est maintenant incluse dans cette version de Receiver pour Chrome. Grâce à cette fonctionnalité, les utilisateurs peuvent maintenant ouvrir des fichiers Windows, les modifier et les enregistrer à partir d'un appareil Chrome exécutant Receiver. Lorsque vous utilisez un appareil Google Chrome, vous pouvez utiliser des applications Windows (par exemple, Microsoft Word) et accéder aux fichiers résidant sur Google Drive sans aucun problème.

À titre d'exemple, si un utilisateur ouvre un fichier dans Google Drive (un fichier .DOC joint téléchargé depuis Gmail par exemple), qu'il le modifie puis qu'il l'enregistre sur Google Drive, il est possible d'accéder au fichier dans une application hébergée XenApp ; le fichier peut être consulté, modifié et enregistré sur Google Drive.

Pour activer cette fonctionnalité, ouvrez les fichiers Google Drive à l'aide de Citrix Receiver.

1. Installez FileAccess.exe sur chaque VDA XenApp/XenDesktop.
2. Configurez les associations de type de fichiers (FTA) appropriées pour les applications publiées dans Citrix AppCenter/Desktop studio.
3. Sur le VDA XenApp/XenDesktop, les sites <https://accounts.google.com> et <https://ssl.gstatic.com> doivent être approuvés et les cookies de ces sites doivent être activés.
4. Seuls les fichiers provenant de Google Drive (uniquement le dossier « Mon Drive ») peuvent être ouverts à l'aide de Citrix Receiver. Pour ouvrir un fichier provenant de Google Drive, cliquez avec le bouton droit sur un fichier et ouvrez-le avec Citrix Receiver.

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

Pour désactiver la fonctionnalité :

Dans le fichier manifest.json, remplacez

```
"file_handlers" : {  
  "all-file-types" : {  
    "extensions" : [  
      ""
```

```
    ]  
  }  
},  
par  
"file_handlers" : {  
  "cr-file-type" : {  
    "extensions" : [  
      "cr",  
      "ica"  
    ]  
  }  
},  
},
```

Mode Kiosque

Dans les versions précédentes, le mode Kiosque sur Chromebook pouvait uniquement exécuter une seule application et fenêtre à la fois. À compter de cette version de Receiver pour Chrome, le mode Kiosque permet d'exécuter toutes les applications dans la même fenêtre.

Grâce à cette fonctionnalité, vous pouvez exécuter des applications Receiver en mode Kiosque, puis lancer des applications ou bureaux Windows à l'aide du même mode. En outre, cette nouvelle fonctionnalité vous permet de publier des applications ou bureaux distants en tant que package Chrome dédié à l'aide de l'URL persistante. Vous pouvez contrôler ces fonctionnalités en ajustant les paramètres Kiosque dans le panneau d'administration Chrome pour les appareils Chrome gérés.

Tenez compte de ce qui suit lors de l'utilisation de cette nouvelle fonctionnalité :

- Référez-vous aux instructions du [site de support de Google](#) pour savoir comment autoriser l'application Receiver à s'exécuter en mode Kiosque sur les appareils Chrome gérés et non gérés.
- Si vous déployez une application Receiver, vous devez la [publier](#) en définissant les options de visibilité sur Public/non répertorié pour garantir l'interopérabilité avec le mode Kiosque.
- 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 via Google Policy Management à l'aide de la console d'administration Google. Exemple de fichier .cr :

http://votre_URLWebRf_ou_urlpersistante>

Mystore

<https://votreentreprise.gateway.com>>

<http://votreentreprise.sitewebinterne.net>>

<http://www.votreentreprise.sitewebexterne.com>>

Remarque : si vous utilisez la console d'administration Google, modifiez le fichier policy.txt contenant la configuration Receiver. Remplacez la valeur « url » sous « rf_web » avec une URL persistante.

Par exemple :

```
{
"settings":{
"Value":{
"settings_version": "1.0",
"store_settings":{
"beacons":{
"external": [
{
"url": "http://www.votreentreprise.sitewebexterne.com"
}
],
"internal": [
{
"url": "http://votreentreprise.sitewebinterne.net"
}
]
},
"gateways": [
{
"is_default": true,
"url": "https://votreentreprise.gateway.com"
}
],
"name": "mystore",
"rf_web": {
```

```
"url": "http://votre_URLWebRf_ou_urlpersistante"
```

```
}  
}  
}  
}  
}
```

Fiabilité de session

Receiver pour Chrome inclut désormais une fiabilité de session améliorée afin d'offrir aux utilisateurs mobiles un accès sans interruption aux applications et bureaux virtuels lorsqu'ils changent de points d'accès réseau. Cette fonctionnalité améliore l'expérience utilisateur en garantissant une connectivité sans interruption, même lorsque l'appareil de l'utilisateur est mis hors puis sous tension lors du passage en mode veille.

Remarque : les sessions reprendront uniquement après le rétablissement de la connectivité réseau après 180 secondes.

Les corrections suivantes sont nécessaires pour utiliser cette fonctionnalité :

- ICATS760WX64022
- ICAWS760WX64022
- ICAWS760WX86022

Transfert de fichiers

Receiver pour Chrome permet de transférer des fichiers de manière sécurisée entre un appareil virtuel et des sessions XenDesktop virtuelles. Cette fonctionnalité utilise un canal virtuel de transfert de fichiers au lieu d'un mappage de lecteur client.

Les utilisateurs peuvent pas défaut :

- Charger des fichiers à partir d'un dossier de téléchargement local ou d'un périphérique connecté et accéder aux données à partir de leurs sessions XenDesktop.
- Télécharger des fichiers depuis leurs sessions XenDesktop sur un dossier ou un périphérique sur leur appareil.

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

Configuration requise

- XenDesktop 7.6 ou XenApp 7.6 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

- 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)

Stratégies de transfert de fichiers

Par défaut, le transfert de fichiers est activé. Utilisez Citrix Studio pour modifier ces stratégies. Elles se trouvent sous Paramètres utilisateur < ICA\Redirection de dossiers. Tenez compte de ce qui suit lors de l'utilisation des stratégies de transfert de fichiers :

- Autoriser le transfert de fichiers entre le bureau et le client. Autorise ou empêche les utilisateurs de transférer des fichiers entre une session XenDesktop virtuelle et leurs appareils.
- Charger des fichiers sur le bureau. Autorise ou empêche les utilisateurs de charger des fichiers depuis leurs appareils sur une session XenDesktop virtuelle.
- Télécharger des fichiers depuis le bureau. Autorise ou empêche les utilisateurs de télécharger des fichiers depuis une session XenDesktop virtuelle vers leurs appareils.

Problèmes connus

- La modification d'un nom de fichier sur un hôte (point de terminaison) n'est pas reflétée dans Google drive. [#0563810]
- La modification des noms de fichiers de fichiers volumineux prend beaucoup de temps lors du chargement sur Google Drive. Pour résoudre ce problème, modifiez le délai d'expiration de persistance de session sur 1 minute dans la propriété de groupe de mise à disposition de Studio. [#0568884]
- En mode Kiosque, Chromebook n'est mappé sur aucun profil utilisateur. Les certificats peuvent uniquement être distribués auprès d'utilisateurs et non auprès d'appareils dans le panneau Google Drive ; les certificats doivent être ajoutés manuellement pour chaque appareil à l'aide du Gestionnaire de certificats. [#0568114]
- L'impression PDF échoue dans la version v.42 et supérieure de Chrome lors de l'exécution en mode Kiosque. [#0557600]
- La configuration du clavier ne peut pas être modifiée pour les appareils Chromebook en mode Kiosque. [#0572307]
- Lorsque vous êtes connecté directement à StoreFront, la fiabilité de session peut échouer lorsque vous passez d'un réseau câblé à un réseau sans fil. [#0572310]
- Lors de l'utilisation du transfert de fichiers, utilisez le bouton de la barre d'outils. [#0565725, #0564879, #0564920]
- Lorsque les fonctionnalités de chargement/téléchargement sont désactivées à l'aide d'une stratégie Studio, la barre d'outils continue à afficher les options de bouton pour ces fonctionnalités. [#0564555]
- CloudBridge ne parvient pas à analyser les connexions. [#0566330]

Configuration système requise

Nov 18, 2015

Cette rubrique dresse la liste des versions des produits Citrix pris en charge pour Receiver pour Chrome et des conditions requises pour que les utilisateurs puissent accéder aux bureaux virtuels et applications hébergées. Elle suppose que tous les ordinateurs répondent à la configuration matérielle minimale requise pour le système d'exploitation installé.

Configuration requise pour la machine utilisateur

Les utilisateurs requièrent des machines exécutant le système d'exploitation Google Chrome (version 37 ou ultérieure) pour accéder aux bureaux et applications à l'aide de Receiver pour Chrome. Citrix vous recommande d'utiliser Receiver pour Chrome avec les versions Stable Channel de Google Chrome. Receiver pour Chrome est uniquement prise en charge sur Chrome OS.

Configuration requise sur les serveurs Citrix

Receiver pour Chrome prend en charge l'accès aux bureaux et applications via les versions suivantes de StoreFront. Les utilisateurs doivent utiliser des sites Receiver pour Web pour accéder aux magasins. Receiver pour Chrome 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 3.0
- Interface Web 5.4

Lorsque les utilisateurs se connectent via NetScaler Gateway, Receiver pour Chrome peut être utilisé pour accéder aux bureaux et applications mis à disposition par toutes les versions de XenDesktop et XenApp qui sont prises en charge par StoreFront.

Pour les connexions directes via StoreFront sans NetScaler Gateway, Receiver pour Chrome peut être utilisé pour accéder aux bureaux et applications mis à disposition par les versions des produits suivants.

- XenDesktop
 - XenDesktop 7.6
- XenApp
 - XenApp 7.6
 - XenApp 6,5

Le Hotfix Rollup Pack 3 ou version ultérieure et la mise à jour Group Policy Management 1.7 doivent également être installés sur le serveur XenApp 6.5.

Sécurisation des connexions utilisateur

Dans un environnement de production, Citrix vous recommande de sécuriser les communications entre les sites Receiver pour Web et les machines des utilisateurs à l'aide de NetScaler 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 Receiver pour Chrome est déployé. Receiver pour Chrome permet aux utilisateurs d'accéder à des bureaux et applications à partir de réseaux publics à l'aide des versions suivantes de NetScaler Gateway.

- NetScaler Gateway 10.5
- NetScaler Gateway 10.1

Receiver pour Chrome prend désormais 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 7.3.1

Configurer votre environnement

Aug 23, 2016

Pour permettre aux utilisateurs de Receiver pour Chrome d'accéder aux ressources hébergées sur XenDesktop et XenApp, vous devez créer un magasin StoreFront. Vous devez également activer les connexions WebSocket sur NetScaler Gateway, XenApp et XenDesktop, si nécessaire. En outre, vous pouvez améliorer l'expérience de l'utilisateur en installant les composants facultatifs sur les machines qui mettent à disposition les bureaux et applications.

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Pour activer les connexions directes à XenDesktop et XenApp

Receiver pour Chrome utilise le protocole WebSocket pour accéder aux bureaux virtuels et aux applications hébergées. Par défaut, les connexions WebSocket sont interdites sur XenDesktop et XenApp. Si vous souhaitez autoriser les utilisateurs à accéder aux bureaux et applications depuis le réseau local sans se connecter via NetScaler Gateway, les connexions WebSocket doivent être autorisées sur XenDesktop et XenApp.

Les connexions WebSocket sont également désactivées par défaut sur NetScaler Gateway. Pour les utilisateurs distants qui accèdent à leurs bureaux et applications via NetScaler Gateway, vous devez créer un profil HTTP avec les connexions WebSocket activées et lier ces dernières au serveur virtuel NetScaler Gateway ou appliquer le profil de manière globale. Pour de plus amples informations sur la création de profils HTTP, consultez la section [Configurations HTTP](#).

Important : si vous utilisez SecureICA pour crypter les communications entre les machines des utilisateurs et vos serveurs XenDesktop ou XenApp, veuillez noter que Receiver pour Chrome prend uniquement en charge le cryptage de base.

1. Dans Citrix Studio, sélectionnez le nœud Stratégie dans le panneau gauche et créez une nouvelle stratégie ou modifiez une stratégie existante.

Pour de plus amples informations sur la configuration des stratégies XenDesktop et XenApp, consultez la section [Stratégies Citrix](#).

2. Définissez le paramètre de stratégie Connexions WebSockets sur Autorisé.
3. Si vous voulez modifier le port utilisé pour les connexions WebSocket, modifiez le paramètre de stratégie Numéro de port WebSockets.

Par défaut, XenDesktop et XenApp utilisent le port 8008 pour les connexions WebSocket. Si vous choisissez d'utiliser un port différent, en raison d'un pare-feu ou d'autres restrictions de réseau, par exemple, vous devez également configurer le site Receiver pour Web afin qu'il utilise le nouveau port.

4. Pour restreindre l'accès à XenDesktop ou XenApp à des sites Receiver pour Web approuvés, spécifiez une liste séparée par des virgules des adresses URL des sites de confiance pour le paramètre de stratégie Liste des serveurs d'origine approuvés WebSockets.

Par défaut, les connexions provenant de tous les sites Receiver pour Web sont acceptées.

5. Sur chaque ordinateur fournissant des bureaux et applications aux utilisateurs de Receiver pour Chrome, vérifiez que les connexions TCP entrantes sur le port que vous avez configuré pour les connexions WebSocket ne sont pas bloquées par des pare-feux, qu'aucune autre application n'utilise le port, et que le trafic sur le port n'est pas redirigé vers d'autres ports.
6. Si vous utilisez XenDesktop, vérifiez que vous avez mis à jour chaque machine fournissant des bureaux aux utilisateurs de Receiver pour Chrome avec les dernières mises à jour disponibles de Virtual Delivery Agent et les derniers correctifs.

7. Si vous prévoyez de créer des machines à l'aide de Machine Creation Services (MCS), sur l'image principale, créez une entrée de registre sur HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies si elle n'est pas déjà présente, puis ajoutez les clés de registre suivantes.
- Créez une clé de Registre avec une valeur de type REG_DWORD dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies\AcceptWebSocketsConnections. Définissez la valeur de la nouvelle clé sur 1.
 - Créez une clé de Registre avec une valeur de type REG_DWORD dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies\WebSocketsPort. Définissez la valeur de la nouvelle clé sur le port que vous avez choisi pour les connexions WebSocket dans la stratégie XenDesktop ou XenApp. La valeur par défaut est 8008.
 - Créez une clé de Registre avec une valeur de type REG_SZ dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies\WSTrustedOriginServerList. Pour la valeur de la nouvelle clé, spécifiez une liste séparée par des virgules des adresses URL des sites Receiver pour Web approuvés ou définissez la valeur sur * pour accepter des connexions à partir de tous les sites Receiver pour Web.
- N'appliquez pas les stratégies WebSocket XenDesktop ou XenApp aux machines provisionnées à l'aide de cette image principale. Vous pouvez vérifier si les stratégies WebSocket sont appliquées sur l'image principale à l'aide de l'outil rsop.msc ou en exécutant la commande gpresult à partir d'une invite de commande.

Cette solution ne peut pas être utilisée avec des déploiements mis à disposition et gérés par App Orchestration.

8. Si vous prévoyez de déployer des machines provisionnées (non persistantes) à l'aide de Provisioning Services, créez le catalogue de machines et le groupe de mise à disposition pour lesquels vous souhaitez activer les connexions à Receiver pour Chrome. Assurez-vous que les stratégies WebSocket que vous configurez s'appliquent à votre catalogue de machines.

Les machines doivent être redémarrées pour appliquer les stratégies WebSocket. Pour les machines Provisioning Services configurées pour utiliser les fichiers de cache en écriture permanents et les machines déployées à l'aide de MCS (qui ont des disques d'identité séparés), les stratégies sont conservées lorsque les machines redémarrent. Toutefois, pour les catalogues de machines Provisioning Services configurés pour utiliser les fichiers de cache en écriture temporaires, ces stratégies doivent être appliquées au vDisk ou elles ne seront pas implémentées correctement sur les machines cibles.

Effectuez les étapes suivantes pour vous assurer que les stratégies sont correctement appliquées au vDisk.

1. À l'aide de la console Provisioning Services, arrêtez une machine cible qui fait partie du catalogue de machines et du groupe de mise à disposition. Modifiez le type d'accès de la machine cible de Production à Maintenance. Pour de plus amples informations, consultez la section [Gestion des machines cibles](#). Vous devez utiliser une machine cible qui fait partie du catalogue de machines et du groupe de mise à disposition ou les stratégies ne seront pas appliquées.
2. Créez une nouvelle version de votre vDisk et laissez Access défini sur Maintenance. Pour de plus amples informations, consultez la section [Mise à jour manuelle d'une image vDisk](#).
3. Démarrez la machine cible de maintenance, sélectionnez la version du vDisk de maintenance depuis le menu de démarrage. Vérifiez que les clés suivantes sont ajoutées au Registre.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICAPolicies\AcceptWebSocketsConnections

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICAPolicies\WebSocketsPort

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICAPolicies\WSTrustedOriginServerList
4. Arrêtez la machine cible, modifiez le type d'accès de la machine cible sur Production, et promouvez la nouvelle version

du vDisk au rang de production. Ensuite, redémarrez la machine cible et redémarrez toute autre machine cible exécutées depuis le vDisk existant.

Si vous n'utilisez pas le contrôle des versions de vDisk, vous pouvez appliquer les stratégies à votre image vDisk de base en arrêtant toutes les machines cibles qui utilisent le vDisk, en plaçant le vDisk en mode Private Image, puis en démarrant la machine cible pour mettre à jour l'image.

Pour configurer des composants facultatifs

Il existe deux composants facultatifs qui permettent d'améliorer l'expérience des utilisateurs de Receiver pour Chrome en optimisant l'intégration avec XenDesktop, XenApp et Chrome OS.

- App Switcher permet aux utilisateurs de basculer entre plusieurs applications exécutées dans la même session. Lorsque le partage de session est activé (valeur par défaut) sur XenApp, les applications ouvertes dans la même session apparaissent dans la même fenêtre. App Switcher fournit une barre des tâches dans la session qui affiche toutes les applications en cours d'exécution dans la session, ce qui permet aux utilisateurs de basculer entre elles.
 - Le pilote d'imprimante universelle 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. Lorsqu'un utilisateur sélectionne l'option Citrix PDF Printer, le pilote convertit le fichier au format PDF et transfère le fichier PDF sur la machine locale. Le fichier PDF est alors ouvert dans une nouvelle fenêtre pour visualisation et impression au travers de Google Cloud Print.
1. Si vous prévoyez d'activer le partage de session sur votre déploiement XenApp, téléchargez le programme d'installation d'App Switcher. Assurez-vous que .NET Framework 4.5 est installé et activé, puis installez App Switcher sur chaque machine qui met à disposition des applications auprès des utilisateurs de Receiver pour Chrome. App Switcher est configuré pour s'exécuter automatiquement en arrière-plan lorsque les utilisateurs établissent une session.
 2. Si vous souhaitez autoriser les utilisateurs à imprimer des 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, effectuez les étapes suivantes.
 1. Téléchargez le Citrix PDF Printing Feature Pack et installez le pilote d'imprimante universelle PDF Citrix sur chaque machine mettant à disposition des bureaux ou applications pour les utilisateurs de Receiver pour Chrome. 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 nouvelle stratégie ou modifiez une stratégie existante.
Pour de plus amples informations sur la configuration des stratégies XenDesktop et XenApp, consultez la section [Stratégies Citrix](#).
 3. Définissez le paramètre de stratégie Auto-create PDF Universal Printer sur Activé.

Déployer Receiver

Nov 18, 2015

Il existe un certain nombre d'options permettant de déployer Receiver pour Chrome.

- Vous pouvez utiliser la console de gestion des applications Google pour configurer Citrix Receiver à l'aide de la stratégie Google. Pour obtenir davantage d'informations, veuillez consulter l'article [CTX141844](#).
- Vous pouvez reconditionner Receiver pour Chrome afin d'inclure un fichier de configuration Citrix Receiver (.cr) que vous avez généré. Le fichier .cr contient les détails de connexion pour NetScaler Gateway et le site 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 Receiver pour Chrome. Comme l'application est préconfigurée, les utilisateurs peuvent commencer à travailler avec Receiver pour Chrome dès qu'ils l'ont installé sans avoir à effectuer d'étapes de configuration supplémentaires.

Vous pouvez distribuer votre application Receiver pour Chrome personnalisée aux utilisateurs 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 installent Receiver pour Chrome depuis le Chrome Web Store en recherchant Citrix Receiver et en cliquant sur Ajouter à Chrome.

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

- Vous générez un fichier .cr contenant les détails de connexion appropriés et distribuez ce fichier aux utilisateurs. Pour configurer Receiver pour Chrome, 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](#).
- Vous donnez aux utilisateurs l'adresse URL qu'ils doivent entrer manuellement lorsqu'ils démarrent Receiver pour Chrome pour la première fois.

Pour reconditionner Receiver pour Chrome

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

1. Téléchargez la version décompressée de Receiver pour Chrome sur un emplacement approprié.
2. Téléchargez le fichier de configuration exemple et modifiez-le pour votre environnement.
3. Renommez le fichier de configuration modifié sur default.cr et copiez-le sur le répertoire racine de Receiver pour Chrome. Les fichiers de configuration avec des noms différents ou dans d'autres emplacements ne sont pas inclus lorsque Receiver pour Chrome est reconditionné.
4. Si vous souhaitez activer la barre d'outils dans les sessions qui permet aux utilisateurs d'envoyer la combinaison CTRL+ALT+SUPPR sur leurs bureaux et applications, suivez les étapes suivantes.
 1. Utilisez un éditeur de texte pour ouvrir le fichier configuration.js dans le répertoire racine de Receiver pour Chrome.
 2. Recherchez la section suivante dans le fichier.

```
'appPrefs':{ 'chromeApp':{ 'ui' : { 'toolbar' : { 'menubar':false, 'clipboard': false
```

3. Modifiez le paramètre de l'attribut menubar sur true.

Lorsque vous activez la barre d'outils dans les sessions de cette manière, il n'est pas nécessaire d'activer la barre d'outils dans le fichier de configuration du site Receiver pour Web.

5. 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 Receiver pour Chrome. Vous devez placer votre application reconditionnée sur liste blanche pour autoriser les utilisateurs à se connecter à un site Receiver pour Web.

6. Sur le serveur StoreFront, utilisez un éditeur de texte pour ouvrir le fichier `web.config` du site Receiver pour Web, qui se trouve en général dans le répertoire `c:\inetpub\wwwroot\Citrix\nomdumagasin\`, où `nomdumagasin` désigne le nom attribué au magasin au moment de sa création.

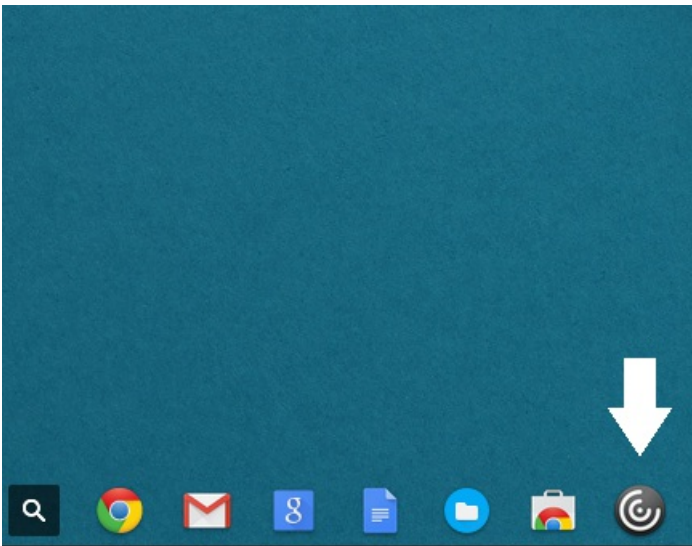
7. Recherchez l'élément suivant dans le fichier.

8. Modifiez la valeur de l'attribut `chromeAppOrigins` sur **`chrome-extension://haiffjcadaglljoggckpgfnoeiflnem|chrome-extension://idpackage`**, où `idpackage` est l'ID généré pour votre application reconditionnée.

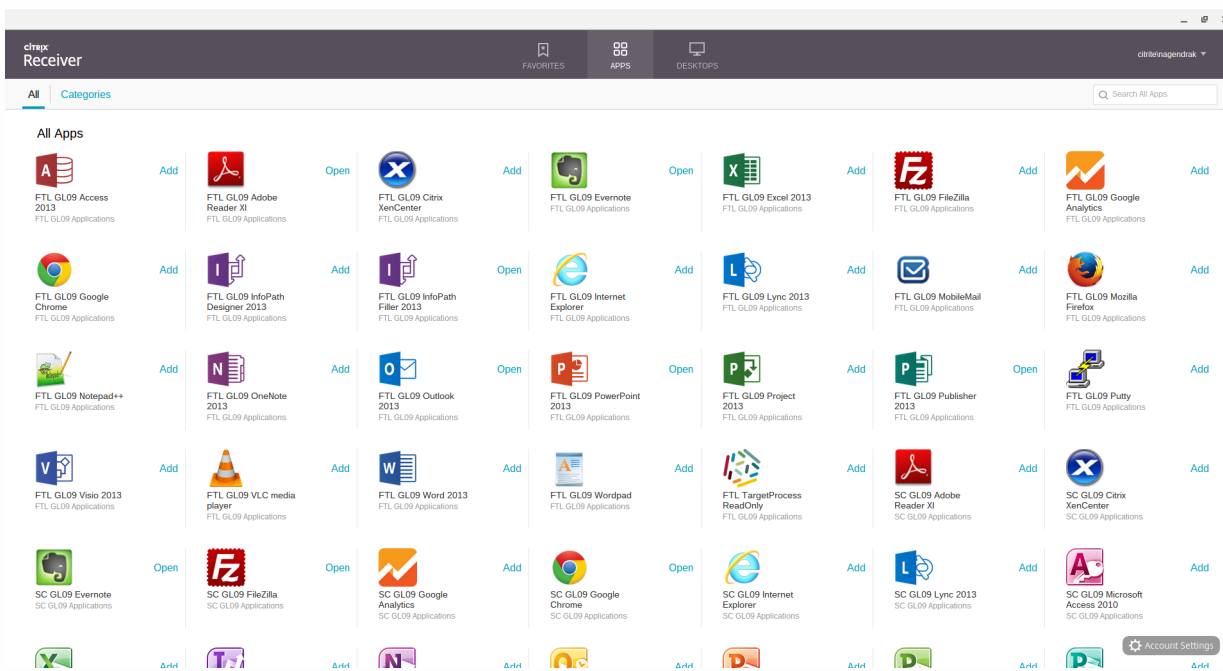
Expérience utilisateur

Nov 18, 2015

Après installation et configuration de Receiver pour Chrome, les utilisateurs cliquent sur l'icône Citrix Receiver dans la liste des applications Chrome pour démarrer Receiver pour Chrome, comme indiqué dans la figure suivante. Pour supprimer Receiver pour Chrome de leurs appareils, vos utilisateurs doivent cliquer avec le bouton droit sur l'icône de Citrix Receiver dans la liste des applications Chrome et sélectionner Désinstaller.



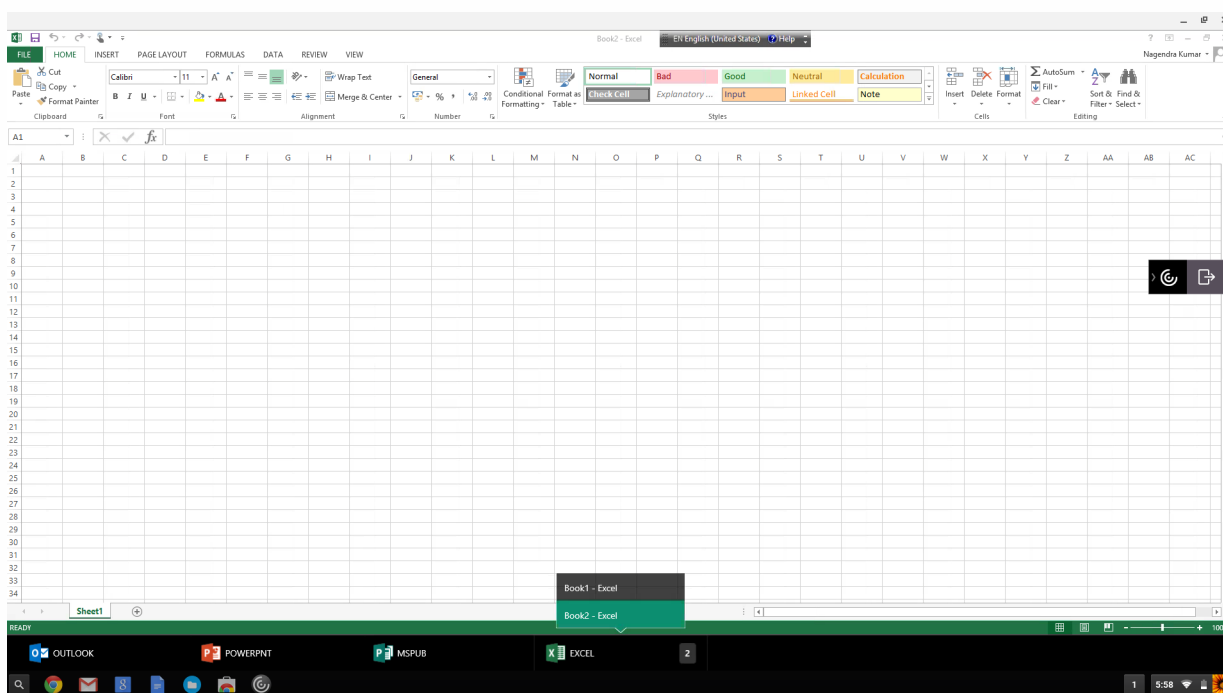
Après qu'ils aient ouvert une session, les bureaux et les applications des utilisateurs s'affichent, comme indiqué dans la figure suivante. Les utilisateurs peuvent rechercher des ressources et cliquer sur une icône pour démarrer un bureau ou une application dans une nouvelle fenêtre.



Lorsqu'un utilisateur démarre une application supplémentaire, Receiver pour Chrome permet de vérifier si l'application peut être lancée au sein d'une session existante avant de créer une nouvelle session. Cela permet aux utilisateurs d'accéder à plusieurs applications via une seule connexion afin que les ressources disponibles soient utilisées plus efficacement.

Pour que le partage de session soit possible, les applications doivent être hébergées sur la même machine et doivent être configurées en mode de fenêtre transparente avec les mêmes paramètres en matière 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.

Les applications exécutées dans la même session s'affichent dans la même fenêtre. Si App Switcher est installé sur la machine mettant les applications à disposition, une barre des tâches s'affiche au bas de la fenêtre, comme indiqué dans la figure suivante. La barre des tâches affiche toutes les applications en cours d'exécution dans la session, ce qui permet aux utilisateurs de basculer entre les applications. Les utilisateurs peuvent configurer la barre des tâches afin qu'elle soit masquée automatiquement et utiliser des petites icônes pour réduire la quantité d'espace utilisée par la barre des tâches.

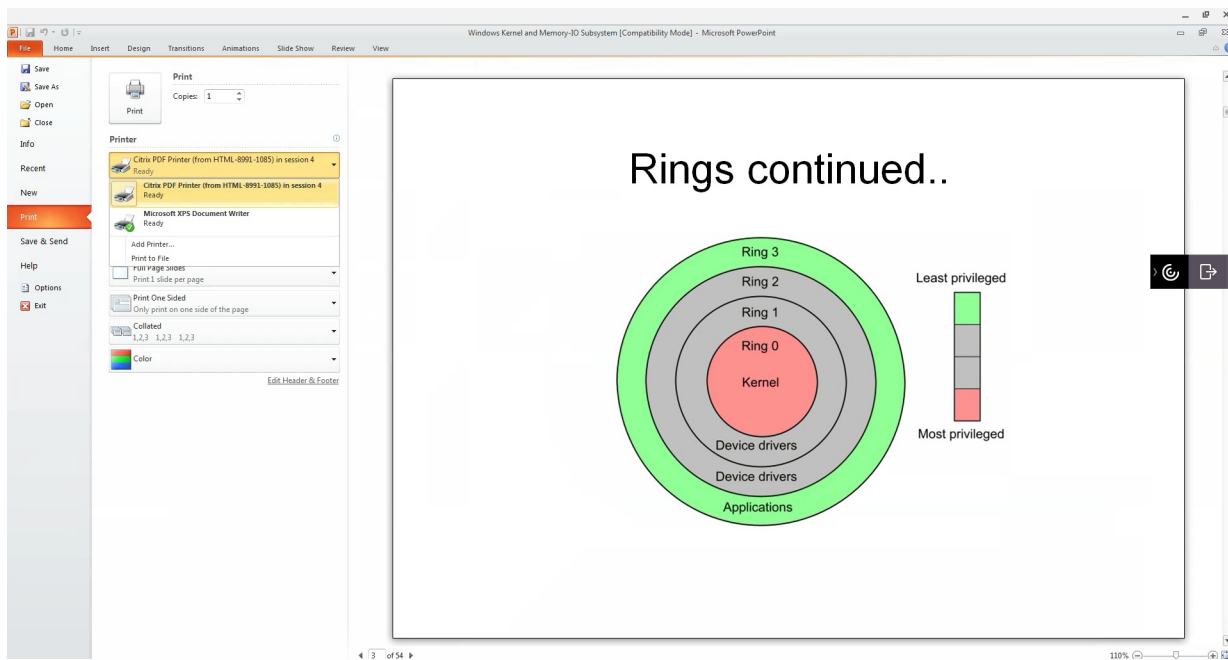


Les utilisateurs peuvent utiliser des raccourcis standard Windows pour copier des données, y compris du texte, des tableaux et des images, entre les applications hébergées, aussi bien au sein de la même session qu'entre des sessions différentes. Seul du texte brut Unicode peut être copié et collé entre des applications hébergées et le Presse-papiers local de la machine.

Les utilisateurs peuvent utiliser les raccourcis clavier Windows standard avec Receiver pour Chrome, car ces raccourcis sont transmis depuis les applications hébergées de Chrome OS. 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 Chrome OS. Veuillez noter cependant qu'il faut également appuyer sur la touche Windows pour que les touches de fonction soient reconnues, un clavier externe est donc requis. Pour de plus amples informations sur l'utilisation de claviers Windows avec le système d'exploitation Chrome OS, veuillez consulter <https://support.google.com/chromebook/answer/1047364>. Les raccourcis spécifiques à Citrix, tels que ceux permettant de basculer entre les sessions et les fenêtres, ne peuvent pas être utilisés avec Receiver pour Chrome.

Lorsque vous imprimez un document ouvert avec une application hébergée ou une application exécutée sur un bureau virtuel, l'utilisateur a la possibilité d'imprimer le document au format PDF, comme indiqué dans la figure suivante. Le PDF est

ensuite transféré sur la machine locale à des fins d'affichage et d'impression à partir d'une imprimante connectée localement ou de Google Cloud Print. Le fichier n'est pas stocké par Receiver pour Chrome.



Pour activer la journalisation pour Receiver pour Chrome

Pour faciliter la résolution des problèmes de connexion, des journaux peuvent être générés sur l'appareil utilisateur et les machines fournissant des bureaux et des applications aux utilisateurs.

1. Pour capturer des journaux sur un appareil utilisateur, effectuez les étapes suivantes.
 1. Sur l'appareil utilisateur, cliquez sur Account Settings dans la partie inférieure droite de la page d'ouverture de session de Receiver pour Chrome.
 2. Dans la boîte de dialogue Settings, cliquez sur Start Logging.
Les détails des fichiers journaux collectés sont répertoriés dans la boîte de dialogue Settings.
 3. Cliquez sur Stop Logging pour mettre fin à la collecte des journaux sur l'appareil utilisateur.
2. Pour activer la journalisation pour App Switcher sur les machines qui fournissent des applications pour les utilisateurs, suivez les étapes suivantes.
 1. Utilisez un éditeur de texte pour ouvrir le fichier AppSwitcher.exe.config, qui se trouve généralement dans le répertoire C:\Program Files (x86)\Citrix\App Switcher.
 2. Recherchez la section suivante dans le fichier.
False
 3. Modifiez le contenu de l'élément sur True pour activer la journalisation de App Switcher.
Les fichiers journaux de App Switcher sont enregistrés dans le répertoire \AppData\Citrix\AppSwitcher\Logs. Le répertoire\AppData est masqué par défaut.