

À propos de Citrix Receiver pour Chrome 2.2

Oct 20, 2016

Citrix Receiver pour Chrome est une application packagée Chrome native qui permet aux utilisateurs d'accéder à des bureaux virtuels et des applications hébergées depuis des appareils Chrome. Les ressources fournies par XenDesktop et XenApp sont agrégées dans un magasin StoreFront et mises à disposition au travers d'un site Citrix Receiver pour Web.

Lorsque l'application Citrix Receiver pour Chrome est installée, les utilisateurs peuvent accéder aux applications et bureaux depuis leurs navigateurs Web ; aucune configuration supplémentaire ni option de déploiement n'est requise sur StoreFront.

Nouveautés dans cette version

Configuration de la fiabilité de session

Citrix Receiver pour Chrome permet maintenant aux administrateurs de configurer les stratégies suivantes à l'aide de Citrix Studio :

1. Délai d'expiration de la fiabilité de session
2. Niveau de transparence de l'interface durant la reconnexion

Pour de plus amples informations, consultez la section [Configuration de la fiabilité de session](#).

Améliorations apportées au fuseau horaire

Dans cette version, Citrix Receiver pour Chrome a étendu la prise en charge de l'anglais et de langues natives dans la redirection du fuseau horaire du client.

Problèmes connus

Problèmes connus dans Citrix Receiver pour Chrome 2.2

- La session se bloque lors du lancement d'applications publiées sur un VDA Linux
Solution : désactivez la barre d'outils lors de l'utilisation d'applications publiées sur un VDA Linux.
[#662083]

Problèmes connus avec Citrix Receiver pour Chrome 2.1

- ENH ID 0652697 : Dans certains cas, le connecteur de carte à puce Google peut se bloquer. Pour résoudre ce problème, déconnectez et reconnectez la session pour réactiver la redirection de carte à puce.

Problèmes connus dans Citrix Receiver pour Chrome 2.1 :

- La touche F5 n'affiche pas de vue miniature des applications ; au lieu de cela, une vignette des VDA affiche toutes les applications au sein d'une session.
[#615795]
- La zone de travail d'une session active n'est pas mise à jour lorsque vous déplacez ou masquez l'étagère Chromebook.
[#623585]
- Vous devrez peut-être utiliser Alt+Tab une seconde fois pour basculer entre applications de VDA différents.
- Une session peut se bloquer lors de la copie et du collage d'un volume important de données dans une session. Citrix recommande de copier des volumes de données inférieurs à 10 Mo lors de l'utilisation du Presse-papiers.
[#586671]
- Citrix recommande d'utiliser un chemin d'accès absolu plutôt qu'un chemin d'accès relatif dans les paramètres de registre Transfert de fichiers.
[#607455]
- Citrix Receiver pour Chrome ne prend pas en charge les claviers multilingues.

[ENH0602652]

- Lorsque du contenu est copié d'un document sur Google Drive (Gdrive) dans une session, le format du contenu copié peut ne pas être conservé. Pour résoudre le problème, ouvrez le document contenant le contenu copié à l'aide de l'application respective (par exemple, Google Docs, Microsoft Word ou Excel) et effectuez des opérations de presse-papiers. Cela devrait conserver le format dans la session.

[#606135]

- La combinaison ALT+F4 ne fonctionne pas comme prévu dans une session. Cliquez sur la touche **Rechercher/Windows** ainsi que sur les touches de la rangée supérieure pour simuler des touches de fonction sur un Chromebook. Vous pouvez également utiliser l'option **Paramètres du clavier** sur le Chromebook pour cocher la case « Considérer les touches de la rangée supérieure comme des touches de fonction ». Cela active l'utilisation directe des touches de la rangée supérieure et permet de simuler des touches de fonction.

[#607326]

Problèmes résolus

Problèmes résolus dans Citrix Receiver pour Chrome 2.1.0.33

Comparaison avec : Citrix Receiver pour Chrome 2.0

Citrix Receiver pour Chrome 2.2 contient toutes les corrections qui ont été introduites dans les versions 2.1, 1.9, 1.8, 1.7, 1.6, 1.5 et 1.4 ainsi que les corrections suivantes :

- Impossible de se connecter aux anciennes versions de StoreFront ou NetScaler Gateway ; une session s'ouvrait dans un navigateur au lieu de Citrix Receiver.

[#653981]

- Il était impossible de lancer une session depuis RDP ou des scénarios double hop Citrix ICA.

[#653980]

- Les touches CTRL et MAJ ne fonctionnaient pas lors de la sélection de fichiers ou de texte.

[#654185]

Configuration système requise

Oct 20, 2016

Configuration requise pour la machine utilisateur

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 (version 50 ou ultérieure) pour accéder aux bureaux et applications à l'aide de Citrix Receiver pour Chrome. Citrix vous recommande d'utiliser Citrix Receiver pour Chrome avec les versions Stable Channel de Google Chrome. Citrix Receiver pour Chrome est uniquement pris en charge sur Chrome OS.

Configuration requise sur les serveurs Citrix

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 Citrix Receiver pour Web pour accéder aux magasins. Citrix 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 3.6
- StoreFront 3.5
- StoreFront 3.0
- StoreFront 2.5
- Interface Web 5.4

Receiver pour Chrome peut être utilisé pour accéder aux bureaux et applications mis à disposition par les versions des produits suivants :

- LTSR (XenApp) CU1, LTSR (XenDesktop) CU1 - 7.6.1000
- XenDesktop 7.6 et versions ultérieures
- XenApp 7.9
- XenApp 6.5

Remarque

Citrix Receiver pour Chrome prend en charge toutes les versions de XenApp et XenDesktop prises en charge comme indiqué dans le cycle de vie des produits Citrix. Consultez le [tableau des produits](#) pour plus d'informations.

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 Citrix Receiver pour Chrome est déployé. Citrix 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 11.1

- NetScaler Gateway 11.0
- NetScaler Gateway 10.5

Citrix 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 7.4 et version supérieure

Déploiement de Citrix Receiver

Oct 20, 2016

Il existe un certain nombre d'options permettant de déployer Citrix 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 de plus amples informations sur la configuration de Chrome, consultez l'article [CTX141844](#) du centre de connaissances.
- Vous pouvez reconditionner Citrix 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 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 Citrix Receiver pour Chrome. Comme l'application est préconfigurée, les utilisateurs peuvent commencer à travailler avec Citrix Receiver pour Chrome dès qu'ils l'ont installé sans avoir à effectuer d'étapes de configuration supplémentaires. Vous pouvez distribuer votre application Citrix 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 Citrix Receiver pour Chrome depuis le Chrome Web Store en recherchant Citrix Receiver et en cliquant sur Ajouter à Chrome.
Une fois l'installation terminée, Citrix Receiver pour Chrome doit être configuré avec les détails de connexion de NetScaler 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 Citrix 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](#).
 - Donnez aux utilisateurs l'adresse URL qu'ils doivent entrer manuellement lorsqu'ils démarrent Citrix Receiver pour Chrome pour la première fois.

Pour reconditionner Citrix Receiver pour Chrome

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

1. Téléchargez la version décompressée de Citrix 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 Citrix Receiver pour Chrome.
Les fichiers de configuration avec des noms différents ou dans d'autres emplacements ne sont pas inclus lorsque Citrix 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 Citrix 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 Citrix Receiver pour Web.
5. Par défaut, Citrix Receiver pour Chrome peut ouvrir toute extension de fichier dans l'application Fichiers dans un Chromebook destiné à ouvrir des fichiers dans Google Drive à l'aide du composant FileAccess dans le VDA. Si un administrateur souhaite désactiver cette option pour télécharger la version décompressée de Citrix Receiver pour Chrome, la section « file handlers » du fichier manifest.ison doit être modifiée comme suit :

```
"file handlers" : {  
  "text" :  
    "extensions" : [  
      "ica",  
      "cr"  
    ]  
}
```

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 Citrix Receiver pour Chrome. Vous devez placer votre application reconditionnée sur liste blanche 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 en général dans le répertoire `c:\inetpub\wwwroot\Citrix\nomdumagasin\`, où *nomdumagasin* désigne le nom attribué au magasin au moment de sa création.
8. Recherchez l'élément suivant dans le fichier.
`<html5 ... chromeAppOrigins="chrome-extension://haiffjcadagjljoggckpgfnoeiflnem" ... />`
9. **Modifiez la valeur de l'attribut** `chromeAppOrigins` **sur** `chrome-extension://haiffjcadagjljoggckpgfnoeiflnem|chrome-extension://packageid`, où **packageid** est l'ID généré pour votre application reconditionnée.

Configuration de votre environnement

Oct 20, 2016

Pour permettre aux utilisateurs de Citrix 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.

Également dans cet article :

[Configuration de Receiver pour Chrome](#)

[Activation de l'authentification par carte à puce](#)

[Configuration de la redirection de port COM série](#)

[Configuration du Single Sign-On \(SSO\) avec Google et Citrix à l'aide de l'authentification SAML](#)

[Activation de l'impression Google Cloud et du pilote d'impression universelle Citrix](#)

[Activation et désactivation de l'accès à Google Drive](#)

[Activation et configuration du mode Kiosque](#)

[Configuration de la fiabilité de session](#)

Configuration de Receiver pour Chrome

Cette section contient des informations sur :

- Stratégie d'administrateur Google
- Web.config dans Storefront
- default.ica
- configuration.js

Configuration de Receiver à l'aide d'une stratégie d'administrateur Google

Dans les versions antérieures, seule la configuration liée au magasin/à la balise pouvait être transmise via une stratégie d'administrateur Google. Pour de plus amples informations sur cette stratégie, reportez-vous à la section [Configuration de Receiver pour Chrome](#) dans le centre de connaissances.

Avec la version 2.1 de Citrix Receiver pour Chrome, d'autres configurations Chrome peuvent également être transmises via la stratégie d'administrateur Google.

Remarque

Citrix recommande d'utiliser cette méthode uniquement lorsque Citrix Receiver pour Chrome est reconditionné pour les utilisateurs.

Pour de plus amples informations, reportez-vous à l'exemple de texte de stratégie ci-dessous :

```
{

  "settings": {

    "Value": {

      "settings_version": "1.0",

      "store_settings": {

        "name": "RTST",

        "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"
    }
},
"engine_settings":{
    "ui":{
        "sessionsize": {
            "windowstate": "fullscreen",
            "available" : {
                "default" : "Fit_To_Window",
                "values" : ["Fit_To_Window", "Use_Device_Pixel_Ratio", "
            }
        },

```

```
"toolbar": {  
  
    "menubar":true,  
  
    "usb": true,  
  
    "fileTransfer":true,  
  
    "about":true,  
  
    "lock":true,  
  
    "disconnect":true,  
  
    "logoff":true,  
  
    "fullscreen":true,  
  
    "multitouch":true,  
  
    "preferences":true,  
  
    "gestureGuide":true  
  
}
```

```
},
```

```
"features":{
```

```
"com":{
```

```
    "portname" : "COM5"
```

```
},
```

```

    "graphics" : {

      "features" : {

        "graphics" : {

          "jpegSupport" : true,

          "h264Support" : {

            "enabled" : true,

            "losslessOverlays" : true,

            "dirtyRegions" : true,

            "yuv444Support" : false

          }

        },

        "filetransfer" : {

          "allowupload" : true,

          "allowdownload" : true,

          "maxuploadsize"      : 2147483647,

          "maxdownloadsize" : 2147483647

        }

      },

      "nacl" : {

        "supportNacl" : true,

```

```
        "graphics": {  
            "enable": true  
        },  
        "video": {  
            "enable": true  
        },  
        "audio": {  
            "enable": true  
        }  
    }  
}  
}  
}
```

Configuration de Receiver pour Chrome à l'aide du fichier Web.config dans StoreFront

Pour changer la configuration à l'aide du fichier Web.config :

1. Ouvrez le fichier **web.config** du site Citrix Receiver pour Web. Le fichier est généralement situé dans **C:\inetpub\wwwroot\Citrix\storenameWeb**, 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 = '{"ui":{"toolbar":{"menubar": false}}}'
```


Remarque

Citrix vous recommande d'utiliser le fichier **web.config** à des fins de configuration uniquement lorsqu'une version de Receiver pour Chrome provenant du magasin d'applications est utilisée.

Configuration de Receiver pour Chrome à l'aide du fichier default.ica

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

1. 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 **nom du site** 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.
2. Ajoutez une nouvelle clé à la fin du fichier, **chromeAppPreferences** en définissant sa valeur en tant qu'objet JSON.

Par exemple :

```
chromeAppPreferences={"ui":{"toolbar":{"menubar": false}}}
```

Remarque

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

Exemple de fichier **default.ica** :

```
;  
;  
; Fichier .ica de substitution  
;  
;  
; Ajoutez les paramètres du fichier ICA que vous voulez envoyer aux appareils clients  
; à ce fichier. Les paramètres contenus dans ce fichier écrasent les  
; paramètres générés par Delivery Services.  
;
```

```
[WFClient]
```

```
Version=2
```

```
RemoveICAFile=yes
```

```
ProxyTimeout=30000
```

ProxyFavorIEConnectionSetting=Yes

ProxyUseFQDN=Off

[ApplicationServers]

Application=

[Application]

TransportDriver=TCP/IP

DoNotUseDefaultCSL=On

BrowserProtocol=HTTPonTCP

LocHttpBrowserAddress=!

WinStationDriver=ICA 3.0

ProxyTimeout=30000

AutologonAllowed=ON

;EncryptionLevelSession=RC5 (128 bit)

[EncRC5-0]

DriverNameWin16=pd0w.dll

DriverNameWin32=pd0n.dll

[EncRC5-40]

DriverNameWin16=pd40w.dll

DriverNameWin32=pd40n.dll

[EncRC5-56]

DriverNameWin16=pd56w.dll

DriverNameWin32=pd56n.dll

[EncRC5-128]

DriverNameWin16=pdc128w.dll

DriverNameWin32=pdc128n.dll

[Compress]

DriverNameWin16=pdcompw.dll

DriverNameWin32=pdcompn.dll

chromeAppPreferences={"ui": {"toolbar": { "menubar": false}}}

Configuration de Citrix Receiver pour Chrome à l'aide du fichier configuration.js

Le fichier **configuration.js** se trouve dans le dossier racine Applications Chrome. Accédez à ce fichier directement pour apporter des modifications à Citrix Receiver pour Chrome.

Conseil

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.

Remarque

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.

Activation de l'authentification par carte à puce

Receiver pour Chrome prend en charge les lecteurs de carte à puce USB avec StoreFront. Vous pouvez utiliser des cartes à puce aux fins suivantes :

- Authentification d'ouverture de session par carte à puce à Receiver pour Chrome.
- Applications publiées prenant en charge les cartes à puce pour accéder aux lecteurs de carte à puce locaux.
- Les applications telles que Microsoft Word et Outlook qui sont lancées dans des sessions ICA peuvent accéder à des cartes à puce pour signer des documents et des e-mails.

Cartes à puce prises en charge :

- Cartes PIV
- Cartes CAC

Les cartes à puce pour votre appareil Chrome exigent ce qui suit :

- Authentification par carte à puce à StoreFront versions 3.6 et supérieures

Important

Pour l'authentification par carte à puce à StoreFront 3.5 ou version antérieure, les utilisateurs ont besoin d'un script personnalisé pour activer l'authentification par carte à puce. Contactez l'assistance technique Citrix pour plus de détails.

- XenDesktop 7.6 et version supérieure
- XenApp 6.5 et version supérieure

Pour configurer la prise en charge de carte à puce sur votre appareil Chrome :

1. Installez l'application de connecteur de carte à puce. Veuillez noter que l'application de carte à puce est requise pour la prise en charge de PCSC sur l'appareil Chrome. 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. Veuillez noter qu'une application middleware (par exemple, Charismathics ou CACKey) est requise car elle agit en tant qu'interface de communication avec la carte à puce et d'autres certificats clients.
 - Pour installer l'extension de carte à puce Charismathics, reportez-vous aux instructions du [site Web de Chrome](#).
 - Pour installer CACKey, reportez-vous aux instructions du [site Web de Chrome](#).

Remarque

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. Configurez l'authentification par carte à puce à l'aide de NetScaler Gateway. Reportez-vous aux instructions figurant dans le [site de documentation sur les produits](#).

Important

L'authentification obligatoire du client est requise lorsqu'une session est lancée. Pour empêcher cela, reportez-vous aux instructions contenues dans la section **Third reduction (one PIN prompt)** de la [documentation NetScaler](#).

La prise en charge de l'authentification par carte à puce présente les limitations suivantes :

- Le certificat de carte à puce est mis en cache même après que la carte à puce soit retirée de l'appareil Chrome. Il s'agit d'un problème connu qui existe dans Google Chrome. Redémarrez l'appareil Chrome pour effacer le cache.
- Lorsque Receiver pour Chrome est reconditionné, les administrateurs doivent obtenir l'appID mis sur liste blanche par Google pour s'assurer que l'application de connecteur de carte à puce est acceptée.
- Seul un lecteur de carte à puce est pris en charge à la fois.

Configuration de la redirection de port COM série

Pour configurer la redirection de port COM série, activez la fonctionnalité en appliquant les paramètres de la stratégie de redirection des ports de XenApp/XenDesktop. Pour de plus amples informations, reportez-vous à [l'article sur les paramètres de stratégie](#).

Remarque

Par défaut, Receiver pour Chrome 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 dans XenApp/XenDesktop, configurez Receiver pour Chrome à l'aide de l'une des méthodes suivantes :

- Stratégie d'administrateur Google
- En utilisant le fichier configuration.js
- En changeant le mappage par défaut en émettant une commande dans une session ICA active.

En utilisant une stratégie d'administrateur 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 Receiver pour Chrome est reconditionné.

Modifiez la stratégie d'administrateur Google en incluant ce qui suit :

commande

COPIER

```
{

  "settings": {

    "Value": {

      "settings_version": "1.0",

      "store_settings": {

        "rf_web": {

          "url": "<http://YourStoreWebURL>"

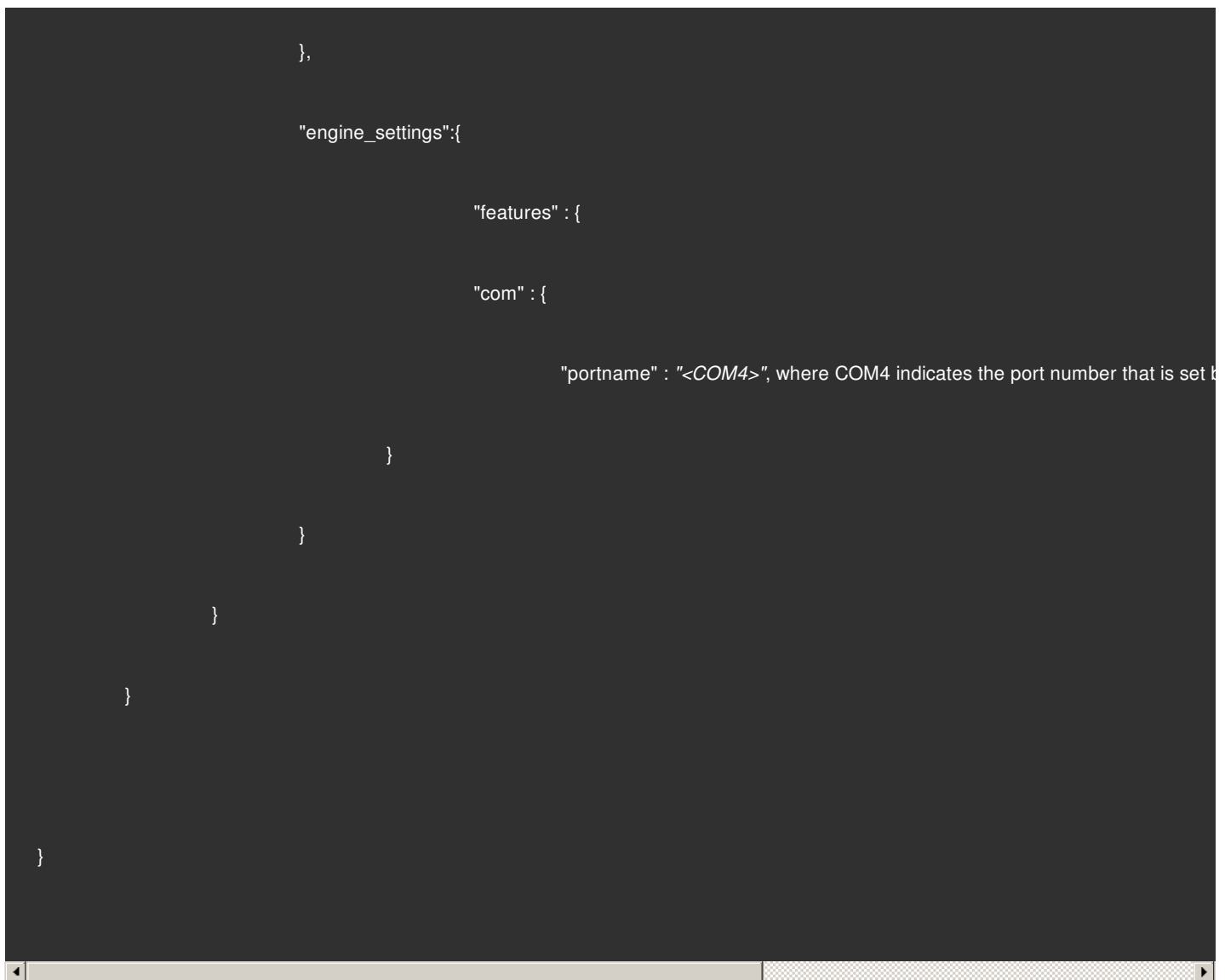
        }

      }

    }

  }

}
```



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 :

```
"com" : {
  "portname" : "COM4"
}
```

Remarque

Citrix vous recommande d'utiliser le fichier **configuration.js** pour configurer la redirection de port série uniquement lorsque Receiver pour Chrome est reconditionné et republié 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 en exécutant la commande suivante dans une session ICA active :

commande

COPIER

```
net use COM4 : \\Client\COM5
```

Conseil

Dans l'exemple ci-dessus, COM4 est le port série préféré utilisé pour la redirection.

Configuration du Single Sign-On (SSO) avec Google et Citrix à l'aide de l'authentification SAML

Pour configurer SSO :

1. Configurez le fournisseur d'identité (IdP) tiers pour l'authentification SAML si cela n'est pas déjà configuré (par exemple, ADFS 2.0). Pour de plus amples informations, reportez-vous à l'article [How to Configure NetScaler SAML to Work with Microsoft AD FS 2.0 IDP](#).
2. Configurez SSO avec Google Apps à l'aide du IdP SAML ; cela permet aux utilisateurs d'usurper l'identité d'un tiers afin d'utiliser Google Apps au lieu du compte Google Entreprise. Pour de plus amples informations, reportez-vous à l'article [Set up Single Sign-On \(SSO\) for Google Apps accounts using third party identity providers](#).
3. Configurez les appareils Chrome de manière à vous connecter via l'IdP SAML ; cela permet aux utilisateurs de se connecter aux appareils Chrome à l'aide d'un [fournisseur d'identité tiers](#).
4. Configurez NetScaler Gateway de manière à vous connecter via l'IdP SAML ; cela permet aux utilisateurs de se connecter à NetScaler Gateway à l'aide d'un fournisseur d'identité tiers. Reportez-vous à l'article [décrivant comment configurer l'authentification SAML](#).
5. Configurez XenApp et XenDesktop pour l'authentification fédérée pour autoriser la connexion aux sessions XenApp/XenDesktop à l'aide de certificats générés dynamiquement après le processus d'ouverture de session SAML au lieu de taper un nom d'utilisateur et un mot de passe. Pour de plus amples informations, reportez-vous à l'article [décrivant l'authentification fédérée](#).
6. Installez et configurez le SSO SAML pour l'extension d'application Chrome sur les appareils Chrome. Pour de plus amples informations, reportez-vous au [site Web de Google](#). Cette extension récupère les cookies SAML depuis le navigateur et les communique à Citrix Receiver. Cette extension doit être configurée avec la stratégie suivante pour permettre à Receiver d'obtenir les cookies SAML :

commande

COPIER

```
{  
  
  "whitelist" : {  
  
    "Value" : [  
  
      {  
  
        "appld" : "haiffjcadagjljoggckpgfnoeiflnem",  
  
        "domain" : "saml.yourcompany.com"  
  
      }  
  
    ]  
  
  }  
  
}
```

Conseil

Si vous reconditionnez Receiver pour Chrome, changez l'**appld** en conséquence. Changez également le domaine au profit du domaine IdP SAML de votre entreprise.

7. Configurez Receiver de manière à utiliser NetScaler Gateway configuré pour l'ouverture de session SAML. Cela permet aux utilisateurs d'utiliser le NetScaler Gateway configuré pour l'ouverture de session SAML. Reportez-vous au [centre de connaissances](#) pour de plus amples informations.

Activation de l'impression Google Cloud et du pilote d'impression universelle Citrix

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.

Important

Configuration requise

Vous avez besoin d'un compte MyCitrix pour accéder à la page de téléchargement de Citrix Receiver pour Chrome.

Téléchargez l'imprimante PDF Citrix depuis la [page de téléchargement de Citrix Receiver pour Chrome](#).

Pour autoriser les utilisateurs à imprimer des documents ouverts avec des applications ou des applications hébergées

1. Téléchargez l'imprimante PDF Citrix 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 Créer automatiquement l'imprimante universelle PDF sur Activé.

Activation et désactivation de l'accès à Google Drive

Grâce à la prise en charge de Google Drive, vos utilisateurs peuvent maintenant ouvrir des fichiers Windows, les modifier et les enregistrer à partir d'un appareil Chrome exécutant Citrix Receiver. 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.

À titre d'exemple, si l'un de vos utilisateurs 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 par XenApp. Le fichier peut être consulté, modifié et enregistré sur Google Drive.

Configuration requise

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

Pour activer l'accès à Google Drive depuis 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.

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 le fichier et ouvrez-le avec Citrix Receiver.

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

Pour désactiver l'accès à Google Drive depuis Citrix Receiver

Dans le fichier manifest.json, remplacez :

```
"file_handlers" : {  
  "all-file-types" : {  
    "extensions" : [  
      "*" ]  
    }  
  },  
}
```

par :

Code COPIER

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

Activation et configuration du mode Kiosque

Le mode Kiosque de Citrix Receiver pour Chrome permet d'exécuter toutes les applications dans la même fenêtre. Grâce à cette fonctionnalité, vous pouvez exécuter des applications Citrix Receiver 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 URL persistante.

Vous pouvez contrôler ces fonctionnalités en ajustant les paramètres Kiosque dans le panneau d'administration Chrome pour les appareils Chrome gérés.

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. [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 via Google Policy Management à l'aide de la console d'administration Google.

Exemple de fichier .cr

COPIER

```
<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>
```

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.

exemple

COPIER

```
{  
  
  "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 "  
  
  }  
  
  }  
  
  }  
  
  }  
  
}
```

Fiabilité de session

Grâce à la fiabilité de session, la session reste active sur le serveur. Pour indiquer que la connectivité est interrompue, l'affichage de l'utilisateur reste figé jusqu'à ce que la connectivité soit rétablie de l'autre côté du tunnel. L'utilisateur a toujours accès à l'affichage de l'application durant l'interruption et peut reprendre l'interaction avec l'application lorsque la connexion réseau est rétablie. La fonction de fiabilité de session permet aux utilisateurs de se reconnecter sans avoir à s'authentifier de nouveau.

Important

Les utilisateurs de Citrix Receiver pour Chrome ne peuvent pas changer le paramètre de serveur.

Vous pouvez utiliser la fonction de fiabilité de session avec le protocole TLS (Transport Layer Security).

Remarque

Vous pouvez utiliser la fonction de fiabilité de session avec le protocole TLS (Transport Layer Security).

Utilisation des stratégies de fiabilité de session

Le paramètre de stratégie Connexions de fiabilité de session autorise ou interdit la fiabilité de session.

Le paramètre de stratégie Expiration de délai de la fiabilité de session est réglé par défaut sur 180 secondes, ou trois minutes. La durée de maintien d'une session dans l'état actif peut être prolongée. Toutefois, cette fonctionnalité étant conçue à des fins de convivialité, elle ne déconnecte pas la session.

Conseil

Si vous augmentez la durée pour laquelle une session est gardée ouverte, les risques d'accès non autorisé sont accrus : un utilisateur distrait peut s'éloigner de sa machine cliente et il est alors possible que des utilisateurs non autorisés accèdent à sa session.

Les connexions entrantes de fiabilité de session utilisent le port 2598, à moins que vous ne changiez le numéro de port défini dans le paramètre de stratégie Numéro de port de la fiabilité de session.

Remarque

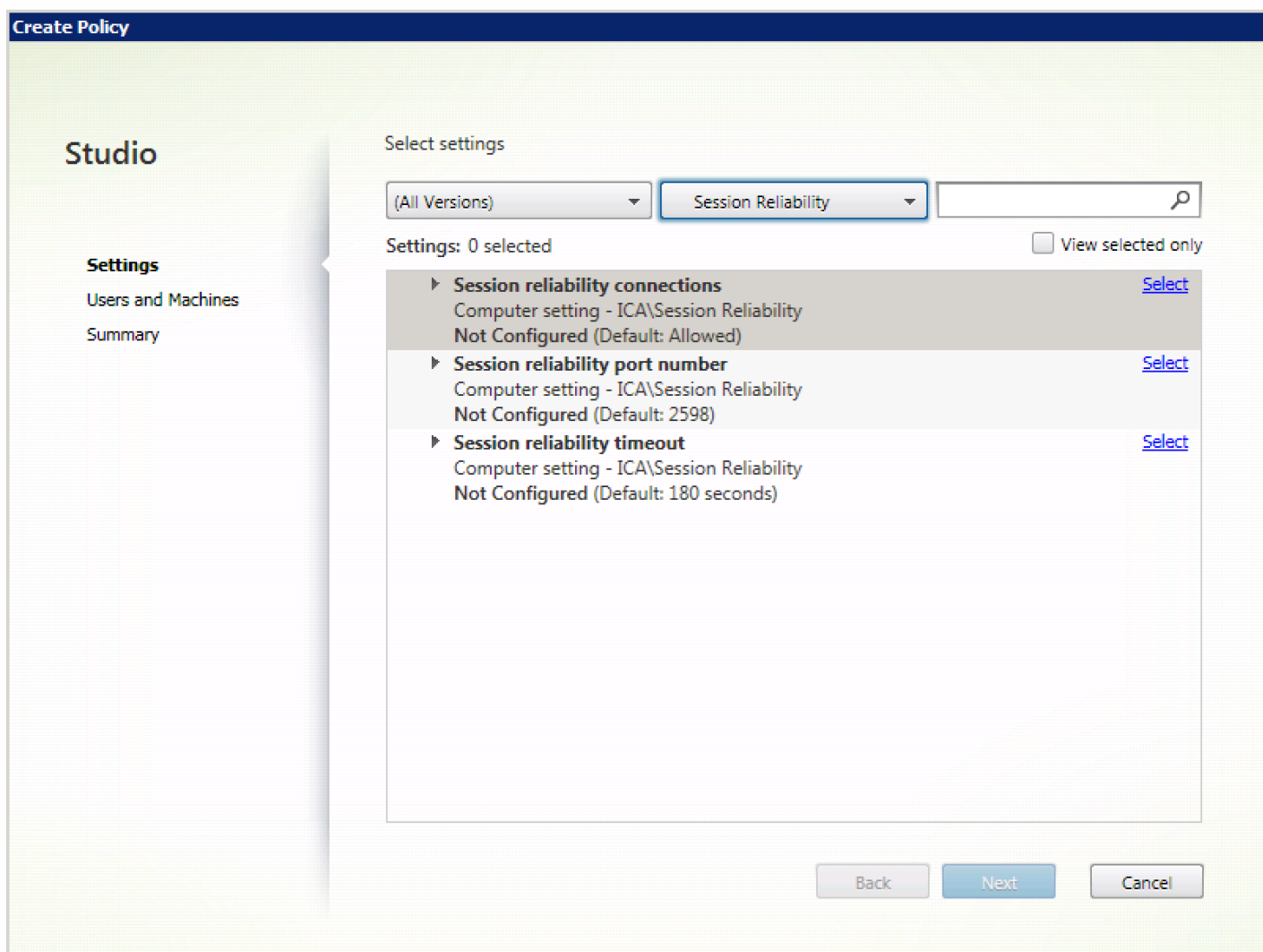
La fiabilité de session est activée par défaut au niveau du serveur. Pour désactiver cette fonctionnalité, configurez la stratégie gérée par le serveur.

Configuration de la fiabilité de session

Par défaut, la fiabilité de session est activée.

Pour désactiver la fiabilité de session :

1. Lancez Citrix Studio.
2. Ouvrez la stratégie **Connexions de fiabilité de session**.
3. Définissez la stratégie sur **Interdit**.



Configuration de l'expiration du délai de la fiabilité de session

Remarque

La stratégie Expiration de délai de la fiabilité de session peut uniquement être configurée avec XenApp/XenDesktop 7.11 et plus.

Pour modifier l'expiration du délai de la fiabilité de session :

Par défaut, l'expiration du délai de la fiabilité de session est réglée sur 180 secondes.

1. Lancez Citrix Studio.

2. Ouvrez la stratégie **Expiration de délai de la fiabilité de session**.
3. Modifiez la valeur d'expiration.
4. Cliquez sur **OK**.

Configuration du niveau de transparence de l'interface durant la reconnexion

L'interface utilisateur de la session est affichée durant les tentatives de reconnexion de la fiabilité de session. Le niveau de transparence de l'interface utilisateur peut être modifié à l'aide d'une stratégie Studio.

Par défaut, la transparence de l'interface durant la reconnexion est définie sur 80 %.

Pour modifier le niveau de transparence de l'interface durant la reconnexion :

1. Lancez Citrix Studio.
2. Ouvrez la stratégie **Niveau de transparence de l'interface durant la reconnexion**.
3. Modifiez la valeur.
4. Cliquez sur **OK**.

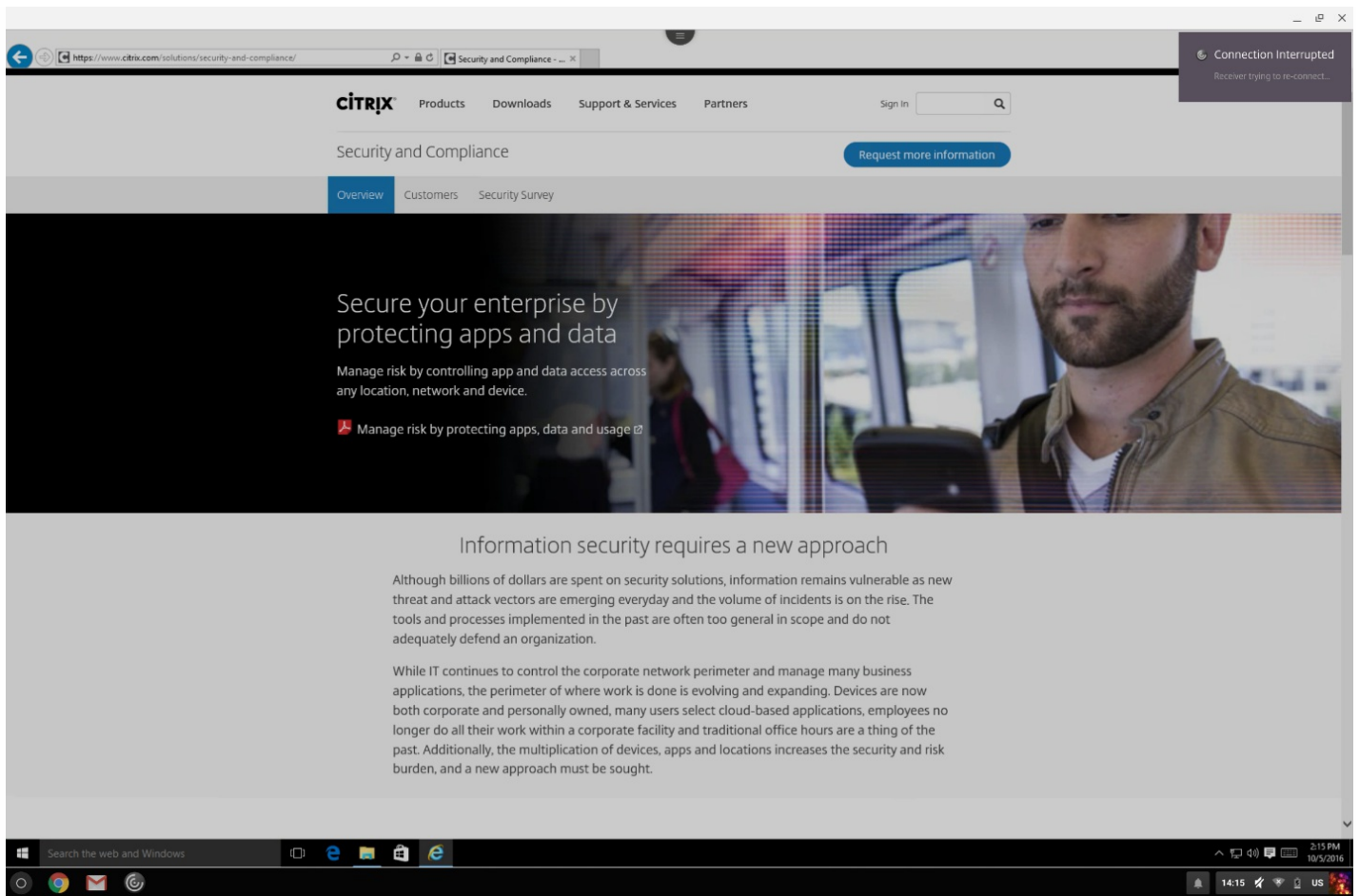
Pour XenDesktop version 7.11 ou antérieure, utilisez le fichier default.ica dans StoreFront pour modifier le délai d'expiration de la connexion d'une session.

Paramètre	Exemple	Compte
SessionReliabilityTTL	SessionReliabilityTTL=120	180

Fonctionnement de la fiabilité de session

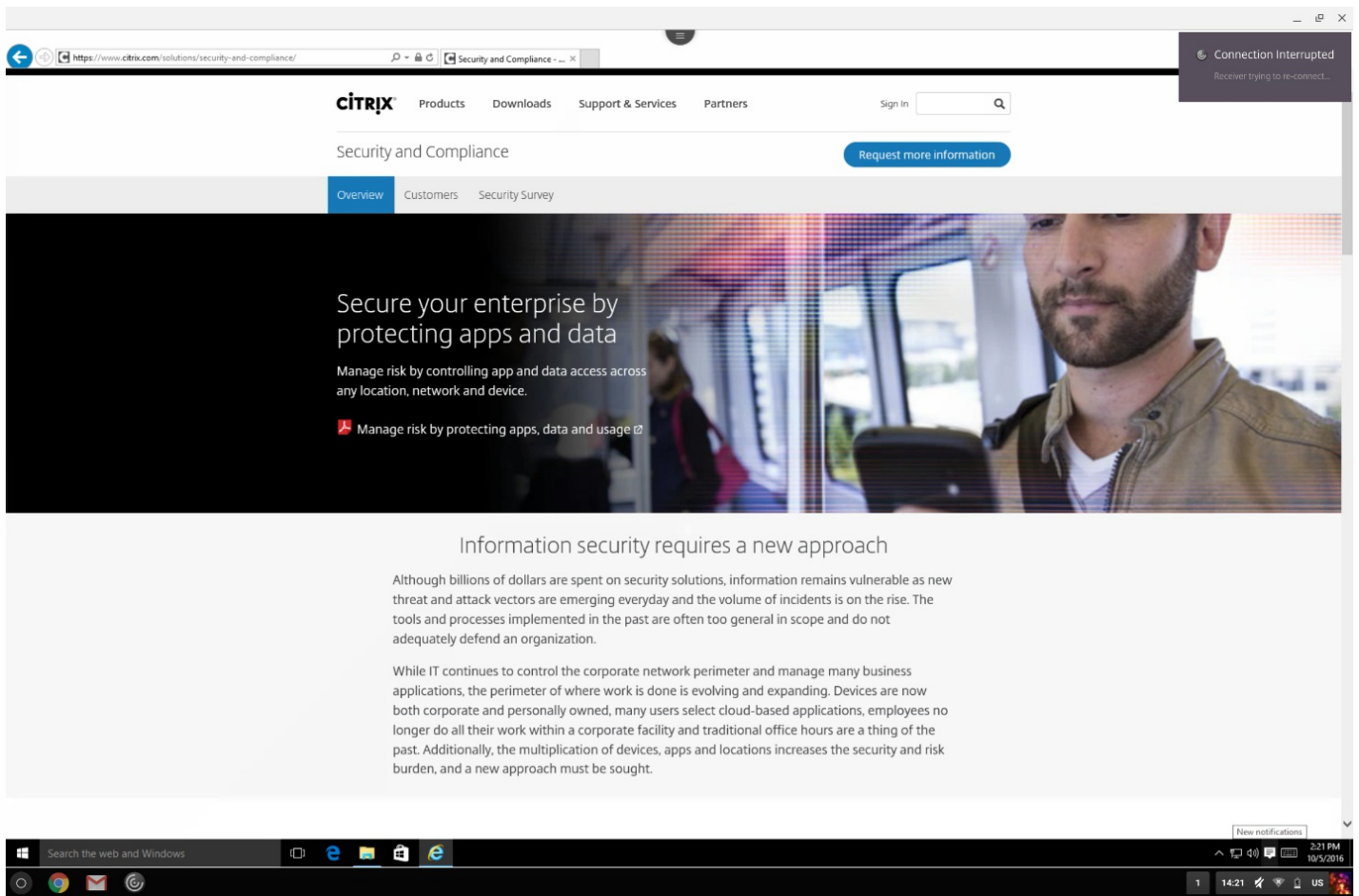
Tenez compte de ce qui suit lorsque la fiabilité de session est activée :

- Une fenêtre de session est grisée lorsqu'une reconnexion est en cours. Une fois que la session a expiré, elle est déconnectée.



Remarque

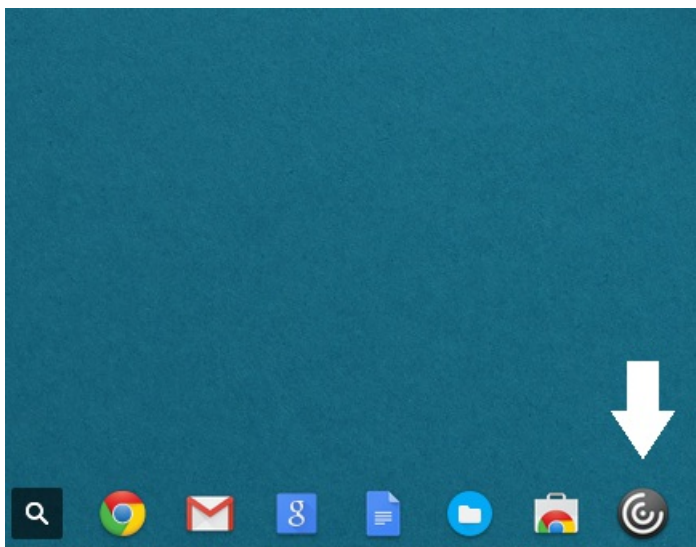
Vous pouvez modifier les niveaux de gris utilisés pour une session inactive à l'aide de Desktop Studio. Par défaut, cette valeur est définie sur 80. La valeur maximale ne peut pas dépasser 100 (indique une fenêtre transparente) et la valeur minimale peut être réglée sur 0 (écran entièrement noir).



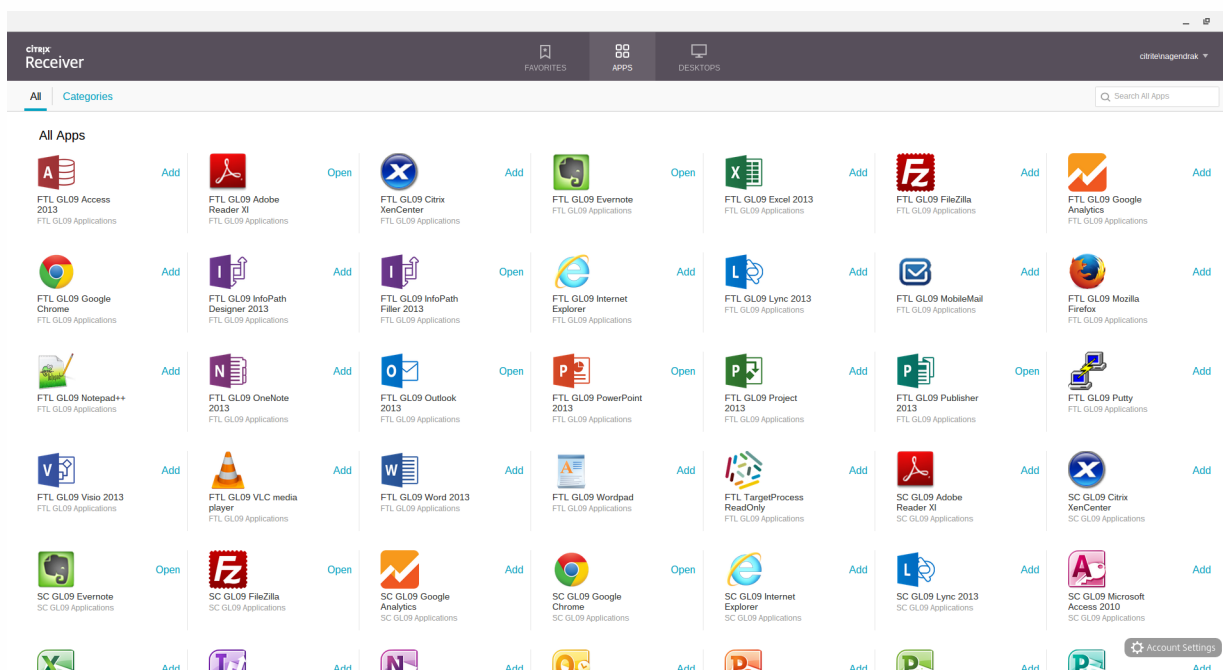
Expérience utilisateur

Oct 20, 2016

Après installation et configuration de Citrix 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 Uninstall.



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.



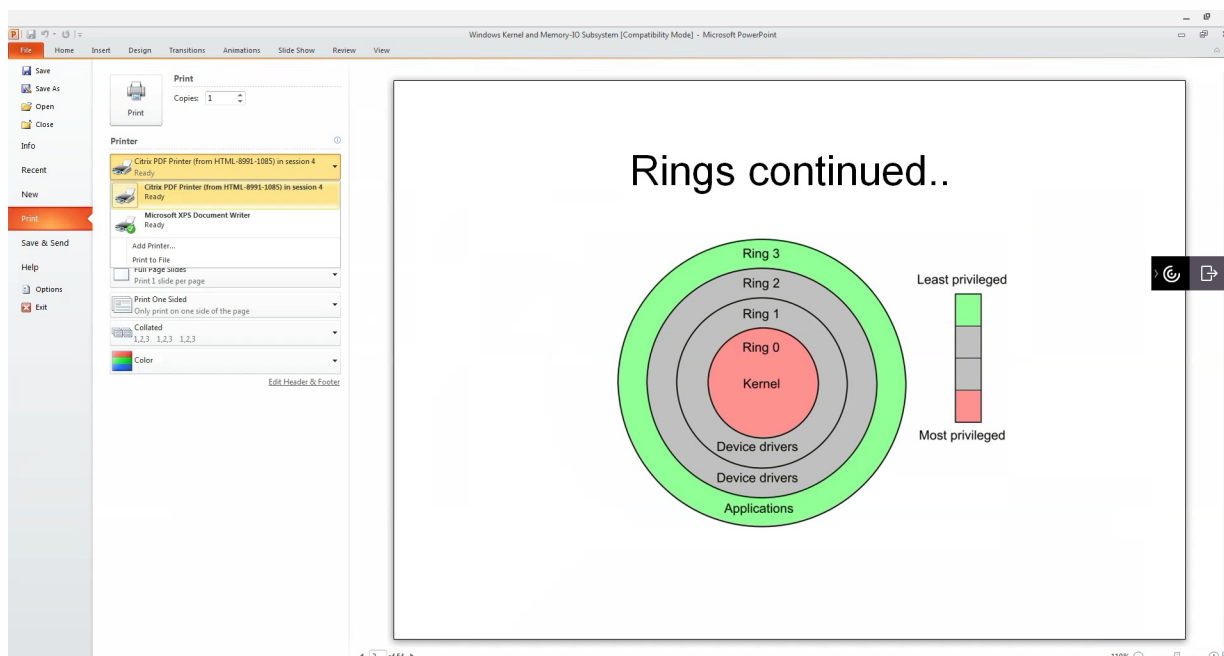
Lorsqu'un utilisateur démarre une application supplémentaire, Citrix Receiver pour Chrome permet de vérifier si l'application peut être lancée au sein d'une session existante avant de créer une nouvelle session. Cela permet aux utilisateurs d'accéder à plusieurs applications via une seule connexion afin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



Pour activer la journalisation pour Citrix 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.

Activer la journalisation sur les appareils utilisateur

Pour capturer les journaux sur un appareil utilisateur :

1. Sur l'appareil utilisateur, cliquez sur le bouton avec une image de paramètres dans la partie inférieure droite de la page d'ouverture de session de Citrix 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.

Configuration du fuseau horaire du client

Pour activer le fuseau horaire sur le client :

1. Lancez Citrix Studio.
2. Ouvrez la stratégie **Utilisation de l'heure locale du client**.
3. Définissez la stratégie sur **Utiliser le fuseau horaire du client**.

