Citrix Secure Private Access - Legacy

Machine translated content

Disclaimer

La version officielle de ce document est en anglais. Certains contenus de la documentation Cloud Software Group ont été traduits de façon automatique à des fins pratiques uniquement. Cloud Software Group n'exerce aucun contrôle sur le contenu traduit de façon automatique, qui peut contenir des erreurs, des imprécisions ou un langage inapproprié. Aucune garantie, explicite ou implicite, n'est fournie quant à l'exactitude, la fiabilité, la pertinence ou la justesse de toute traduction effectuée depuis l'anglais d'origine vers une autre langue, ou quant à la conformité de votre produit ou service Cloud Software Group à tout contenu traduit de façon automatique, et toute garantie fournie en vertu du contrat de licence de l'utilisateur final ou des conditions d'utilisation des services applicables, ou de tout autre accord avec Cloud Software Group, quant à la conformité du produit ou service à toute documentation ne s'applique pas dans la mesure où cette documentation a été traduite de façon automatique. Cloud Software Group ne pourra être tenu responsable de tout dommage ou problème dû à l'utilisation de contenu traduit de façon automatique.

Contents

Configuration de Secure Private Access pour les déploiements sur site - Legacy

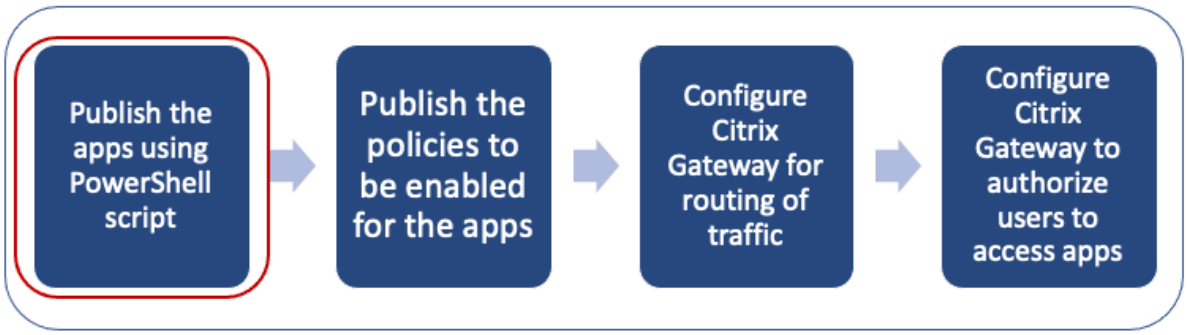
December 27, 2023

La configuration de la solution Secure Private Access for on-premises est un processus en quatre étapes.

1. Publier les applications
2. Publier les stratégies relatives aux applications
3. Activer le routage du trafic via NetScaler Gateway
4. Configuration des stratégies d'autorisation

> **Important :**
>
> un outil de configuration est disponible pour intégrer rapidement les applications et les stratégies relatives aux applications, ainsi que pour configurer les paramètres NetScaler Gateway et StoreFront. Toutefois, prenez note des points suivants avant d'utiliser l'outil.
>
> - Lisez les sections Publier les applications et Stratégies de publication pour les applications pour vous assurer de bien comprendre les exigences de configuration pour la configuration de la solution sur site.
> - Cet outil ne peut être utilisé qu'en complément des procédures existantes documentées dans cette rubrique et ne remplace pas la configuration qui doit être effectuée manuellement.
>
> Pour plus de détails sur l'outil, voir Configurer des applications et des stratégies à l'aide de l'outil de configuration Secure Private Access.

Étape 1 : Publier les applications



Vous devez utiliser le script PowerShell pour publier les URL. Une fois l'application publiée, elle peut être gérée à l'aide de la console Citrix Studio.

Vous pouvez télécharger le script PowerShell à partir de https://www.citrix.com/downloads/workspace-app/powershell-module-for-configuring-secure-private-access-for-storefront/configure-secure-private-access-for-storefront.html.

1. Sur la machine contenant le SDK PowerShell, ouvrez PowerShell.
2. Exécutez la commande suivante :

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup -Name PublishedContentApps
```

3. Définissez les variables de l'application Web.

```
$citrixUrl: " <URL of the app> "
$appName: <app name as it must appear on Workspace>
$DesktopGroupId: 1
$desktopgroupname: <your desktop group name>
$AppIconFilePath:  <path of the image file>
```

> **Remarque :**
>
> Assurez-vous de mettre à jour les espaces réservés marqués par des crochets angulaires (< >) avant d'exécuter la commande.

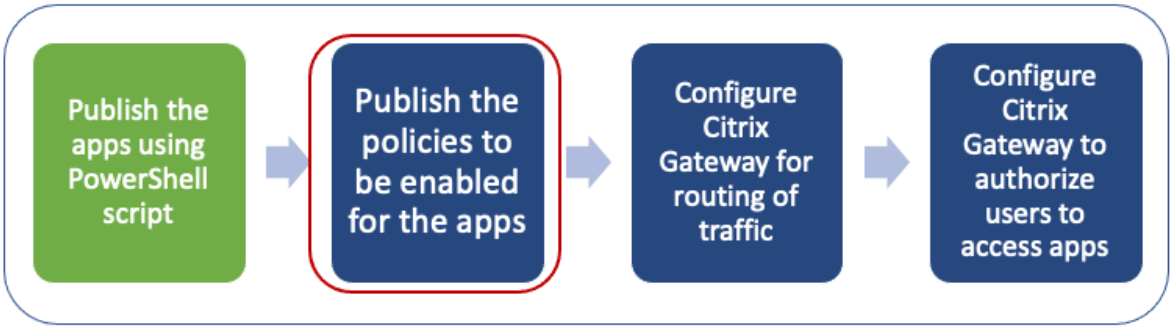
Après avoir attribué l'emplacement et le nom de l'application, exécutez la commande suivante pour publier l'application.

```
New-BrokerApplication -ApplicationType PublishedContent -
    CommandLineExecutable $citrixURL -Name $appName -DesktopGroup $dg.
    Uid
```

L'application publiée apparaît dans la section **Applications** de **Citrix Studio**. Vous pouvez désormais modifier les détails de l'application depuis la console Citrix Studio elle-même.

Pour plus d'informations sur la publication de l'application et la modification de l'icône par défaut de l'application publiée, voir Publier du contenu.

Étape 2 : publier des stratégies pour les applications



Le fichier de stratégie définit le routage et les contrôles de sécurité de chaque application publiée. Vous devez mettre à jour le fichier de stratégie sur la façon dont une application Web ou SaaS est routée (via une passerelle ou sans passerelle).

Pour appliquer des stratégies d'accès aux applications, vous devez publier les stratégies pour chaque application Web ou SaaS. Pour ce faire, vous devez mettre à jour le fichier JSON de stratégie et le fichier Web.config.

- **Fichier JSON de stratégie :** mettez à jour le fichier JSON de stratégie avec les détails de l'application et les stratégies de sécurité des applications. Le fichier JSON de stratégie doit ensuite être placé sur le serveur StoreFront à l'adresse `C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser`.

  > **Remarque :**
  >
  > Vous devez créer les dossiers nommés **Resources** et **SecureBrowser**, puis ajouter le fichier JSON de stratégie dans le dossier SecureBrowser.
  > Pour plus de détails sur les différentes actions stratégiques et leurs valeurs, consultez la section Détails de la stratégie d'accès aux applications.

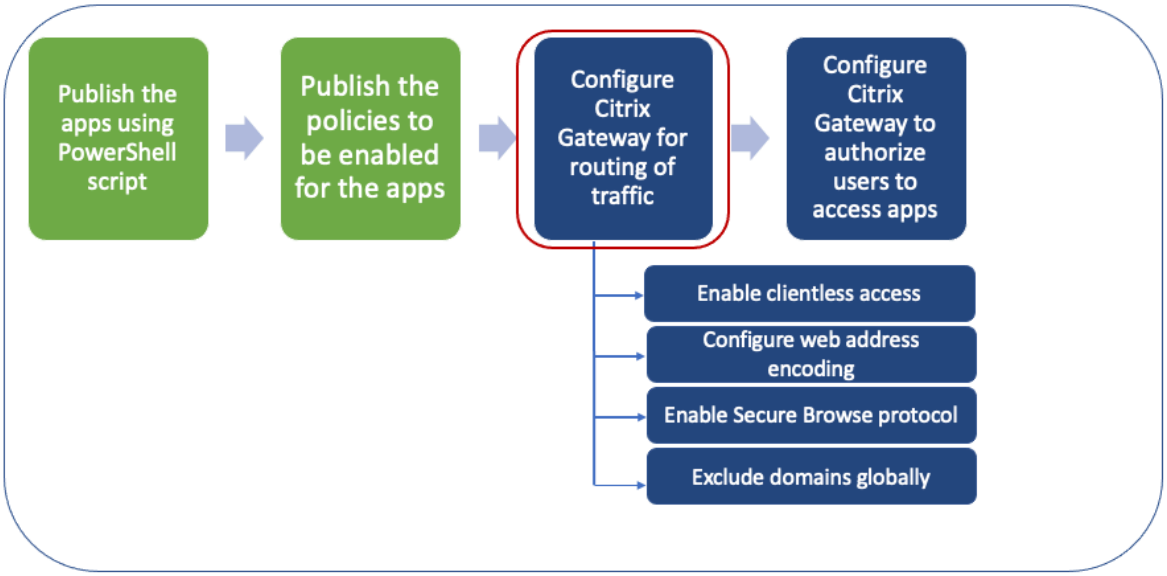
- **Fichier Web.config :** pour que les détails de la nouvelle stratégie soient disponibles pour l'application Citrix Workspace et le navigateur Citrix Enterprise, vous devez modifier le fichier web.config dans le répertoire StoreFront. Vous devez modifier le fichier pour ajouter une nouvelle balise XML portant le nom route. Le fichier Web.config doit ensuite être placé à l'emplacement C:\inetpub\wwwroot\Citrix\Store1.

  Reportez-vous à la section Exemple de configuration de bout en bout pour un exemple de fichier XML.

  > **Remarque :**
  >
  > Dans le chemin, « store1 » fait référence au nom spécifié pour le magasin lors de sa création. Si un nom de magasin différent est utilisé, un dossier approprié doit être créé.

Il est recommandé d'ajouter un nouvel itinéraire à la fin des itinéraires existants. Si vous ajoutez un itinéraire au milieu, vous devez mettre à jour manuellement le numéro de commande pour tous les itinéraires suivants.

Étape 3 : activer le routage du trafic via NetScaler Gateway



L'activation du routage du trafic via NetScaler Gateway implique les étapes suivantes :

- Activer l'accès sans client
- Activer le codage des URL
- Activer la Secure Browse
- Exclure les domaines de la réécriture en mode d'accès sans client

L'accès sans client, le codage des URL et la navigation sécurisée peuvent être activés globalement ou selon une stratégie de session.

- Le paramètre activé globalement s'applique à tous les serveurs virtuels NetScaler Gateway configurés.
- Le paramètre de stratégie par session s'applique aux utilisateurs, aux groupes ou aux serveurs virtuels Gateway.

Activer l'accès sans client

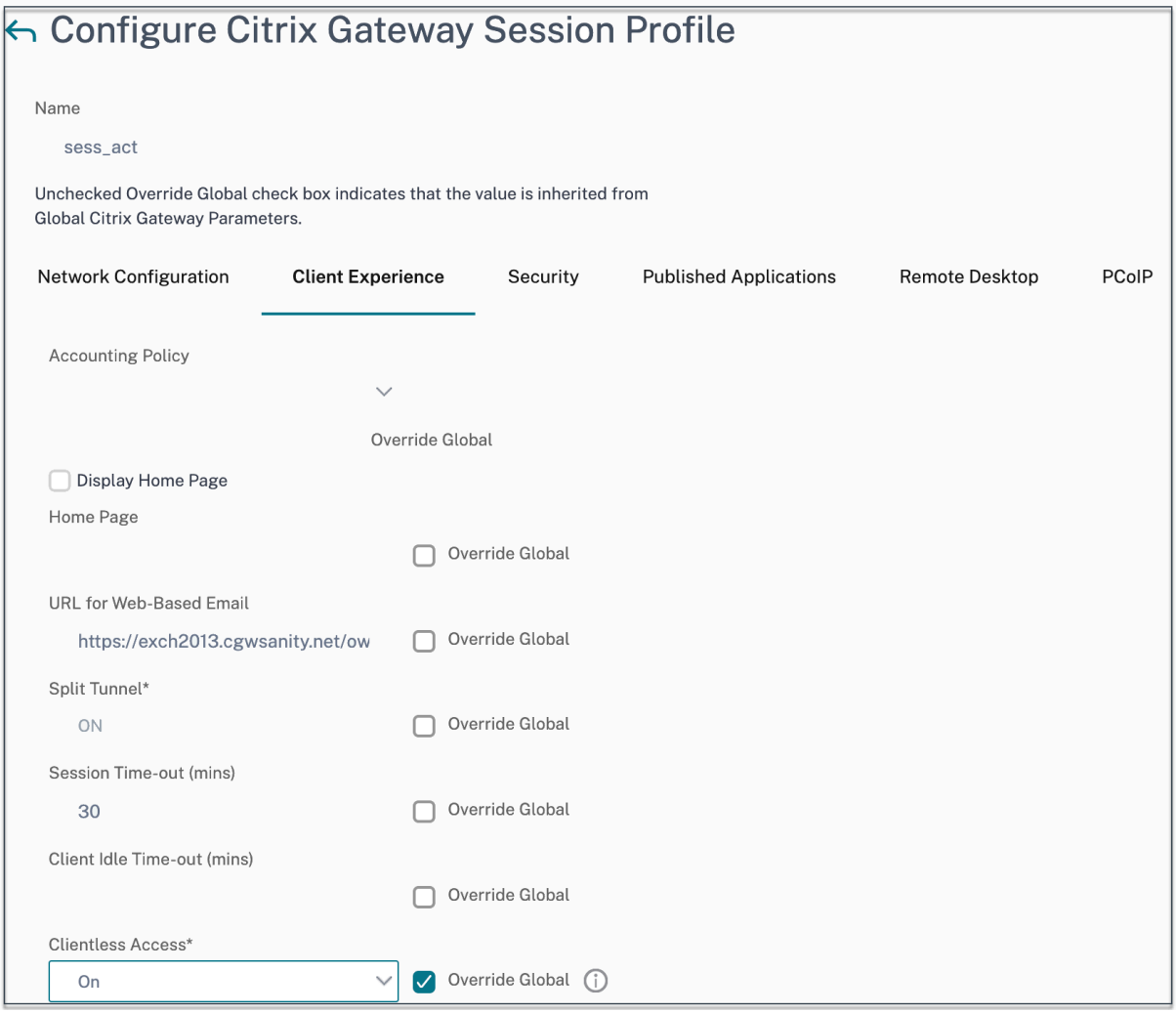
Pour activer l'accès sans client à l'échelle mondiale à l'aide de l'interface graphique de NetScaler Gateway, procédez comme suit :

Dans l'onglet **Configuration**, développez **Citrix Gateway**, puis cliquez sur **Paramètres généraux**.
Sur la page Paramètres généraux, cliquez sur **Modifier** les paramètres généraux .
Dans l'onglet **Expérience client**, dans Accès sans client, sélectionnez **Activé**, puis cliquez sur **OK**.

Pour activer l'accès sans client à l'aide d'une stratégie de session à l'aide de l'interface graphique de NetScaler Gateway :

Si vous souhaitez qu'un groupe restreint d'utilisateurs, de groupes ou de serveurs virtuels utilise l'accès sans client, désactivez ou effacez l'accès sans client à l'échelle mondiale. Ensuite, à l'aide d'une stratégie de session, activez l'accès sans client et liez-le à des utilisateurs, des groupes ou des serveurs virtuels.

1. Dans l'onglet **Configuration**, développez **Citrix Gateway**, puis cliquez sur **Stratégies > Session**.
2. Cliquez sur l'onglet **Stratégie de session**, puis sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la stratégie.
4. À côté de **Profil**, cliquez sur **Nouveau**.
5. Dans **Nom** , saisissez le nom du profil.
6. Dans l'onglet **Expérience client**, à côté de Clientless Access, cliquez **sur**Override Global**, sélectionnez Activé**, puis cliquez sur **Créer**.
7. Dans **Expression**, entrez `true`. Lorsque vous entrez la valeur `true`, la stratégie est toujours appliquée au niveau auquel elle est liée.
8. Cliquez sur **Créer** , puis sur **Fermer** .



Pour activer l'accès sans client à l'échelle mondiale à l'aide de l'interface de ligne de commande NetScaler Gateway :

À l'invite de commandes, exécutez la commande suivante :

```
set vpn parameter -clientlessVpnMode On -icaProxy OFF
```

Pour activer la stratégie d'accès sans client par session à l'aide de l'interface de ligne de commande NetScaler Gateway :

À l'invite de commandes, exécutez la commande suivante :

```
set vpn sessionAction <session-profile-name> -clientlessVpnMode On -
    icaProxy OFF
```


Activer le codage des URL

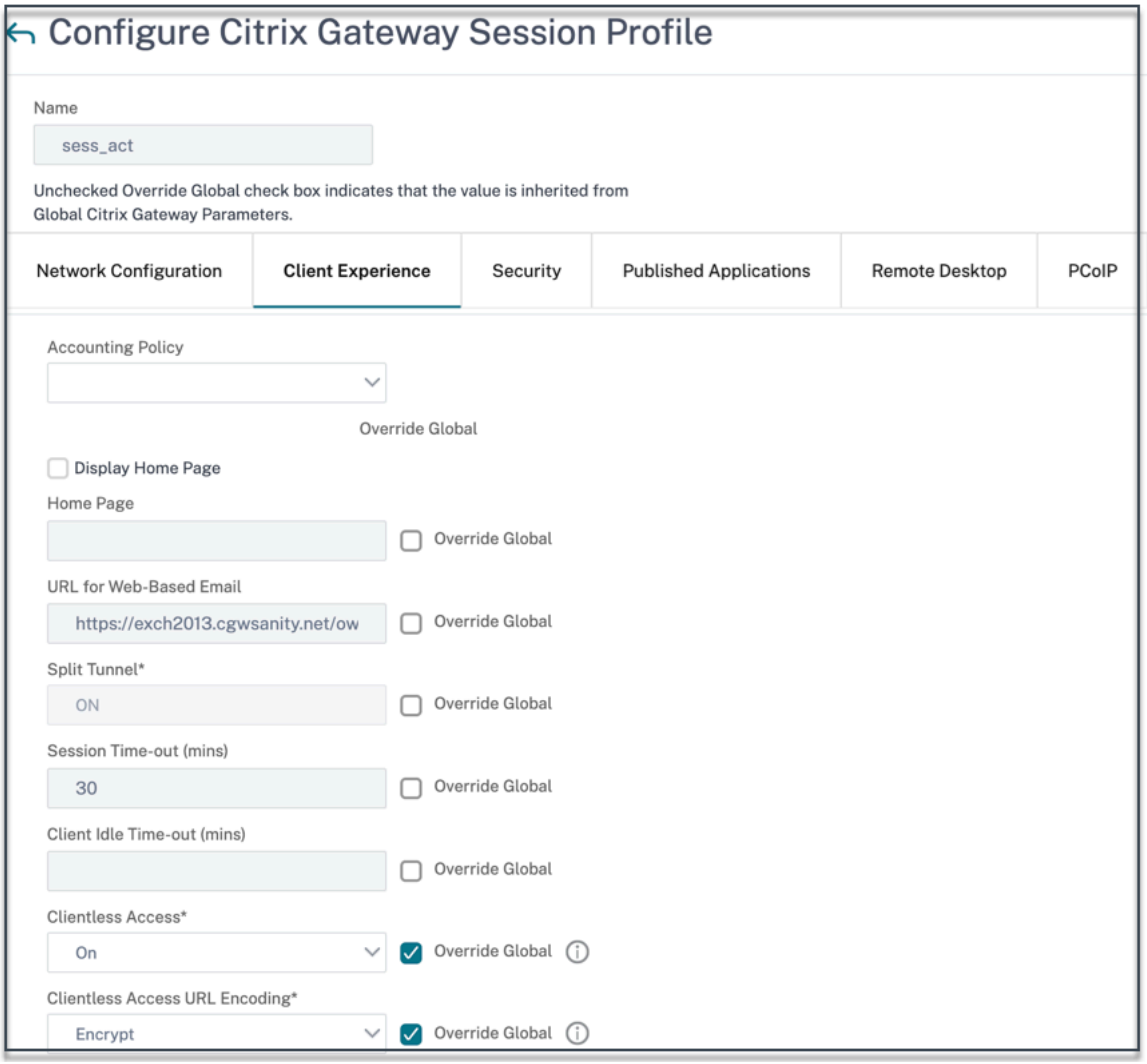
Lorsque vous activez l'accès sans client, vous pouvez choisir de coder les adresses des applications Web internes ou de conserver l'adresse en texte clair. Il est recommandé de laisser l'adresse Web sous forme de texte clair pour un accès sans client.

Pour activer le codage des URL à l'échelle mondiale à l'aide de l'interface graphique de NetScaler Gateway, procédez comme suit :

1. Dans l'onglet **Configuration**, développez **Citrix Gateway**, puis cliquez sur **Paramètres généraux**.
2. Sur la page **Paramètres généraux**, cliquez sur **Modifier les paramètres généraux**.
3. Dans l'onglet **Expérience client**, dans **Encodage d'URL d'accès sans**client, sélectionnez le paramètre de codage de votre URL Web, puis cliquez sur **OK**.

Pour activer le codage des URL au niveau de la stratégie de session à l'aide de l'interface graphique de NetScaler Gateway, procédez comme suit :

1. Dans l'onglet **Configuration**, développez **Citrix Gateway**, puis cliquez sur **Stratégies > Session**.
2. Cliquez sur l'onglet **Stratégie de session**, puis cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la stratégie.
4. À côté de **Profil**, cliquez sur **Nouveau**.
5. Dans **Nom** , saisissez le nom du profil.
6. Dans l'onglet **Expérience client**, à côté de **Codage de l'URL d'accès sans client**, cliquez sur **Override Global**, sélectionnez le niveau de codage, puis cliquez sur **OK**.
7. Dans **Expression**, entrez `true`. Lorsque vous entrez la valeur `true`, la stratégie est toujours appliquée au niveau auquel elle est liée.



Pour activer le codage des URL à l'échelle mondiale à l'aide de l'interface de ligne de commande NetScaler Gateway, procédez comme suit :

À l'invite de commandes, exécutez la commande suivante :

```
set vpn parameter -clientlessModeUrlEncoding TRANSPARENT
```

Pour activer la stratégie d'encodage des URL par session à l'aide de l'interface de ligne de commande NetScaler Gateway, procédez comme suit :

À l'invite de commandes, exécutez la commande suivante :

```
set vpn sessionAction <session-profile-name> -clientlessModeUrlEncoding
    TRANSPARENT
```


Activer la Secure Browse

La navigation sécurisée et l'accès sans client fonctionnent ensemble pour permettre les connexions à l'aide du mode VPN sans client. Vous devez activer le mode navigation sécurisée afin que Citrix Enterprise Browser puisse utiliser le mode navigation sécurisée pour accéder aux applications sans l' ancien VPN.

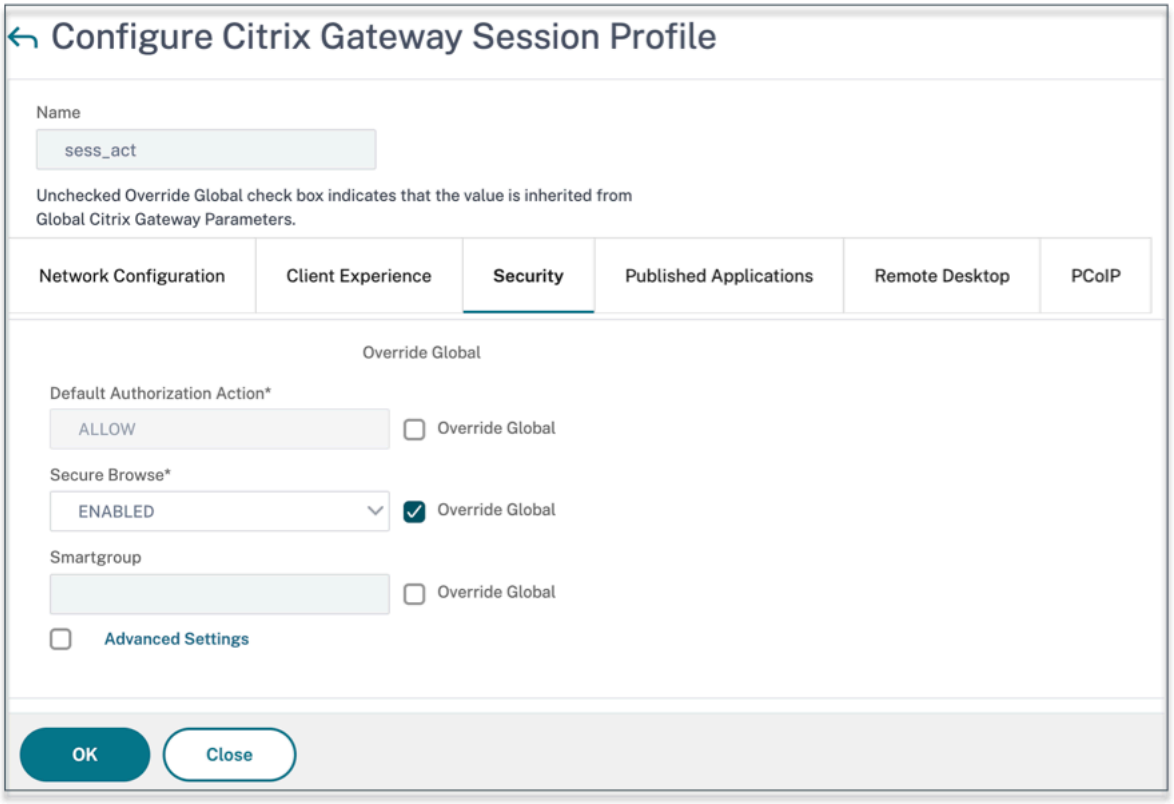
> **Remarque :**
>
> lorsque le navigateur Citrix Enterprise n'est pas installé sur l'utilisateur final, les URL publiées avec la balise **SPAEnabled** s'ouvrent via le navigateur par défaut de l'appareil au lieu du navigateur Citrix Enterprise. Dans ce cas, les stratégies de sécurité ne s'appliquent pas. Le problème se produit uniquement sur les déploiements de StoreFront.

Pour activer le mode navigation sécurisée à l'échelle mondiale à l'aide de l'interface graphique de NetScaler Gateway, procédez comme suit :

1. Dans l'onglet **Configuration**, développez **Citrix Gateway**, puis cliquez sur **Paramètres généraux**.
2. Sur la page Paramètres généraux, cliquez sur **Modifier les paramètres** généraux .
3. Dans l'onglet **Sécurité**, dans Secure Browse, sélectionnez **ACTIVÉ**, puis cliquez sur **OK**.

Pour activer le mode navigation sécurisée au niveau de la stratégie de session à l'aide de l'interface graphique de NetScaler Gateway :

1. Dans l'onglet **Configuration**, développez **Citrix Gateway**, puis cliquez sur **Stratégies > Session**.
2. Cliquez sur l'onglet **Stratégie de session**, puis sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la stratégie.
4. À côté de **Profil**, cliquez sur **Nouveau**.
5. Dans **Nom** , saisissez le nom du profil.
6. Dans l'onglet **Sécurité**, cliquez sur **Ignorer les paramètres globaux**et définissez **Secure Browse surACTIVÉ**.



Pour activer la navigation sécurisée à l'échelle mondiale à l'aide de l'interface de ligne de commande NetScaler Gateway :

À l'invite de commandes, exécutez la commande suivante :

```
set vpn parameter -secureBrowse ENABLED
```

Pour activer la stratégie de navigation sécurisée par session à l'aide de l'interface de ligne de commande NetScaler Gateway :

À l'invite de commandes, exécutez la commande suivante :

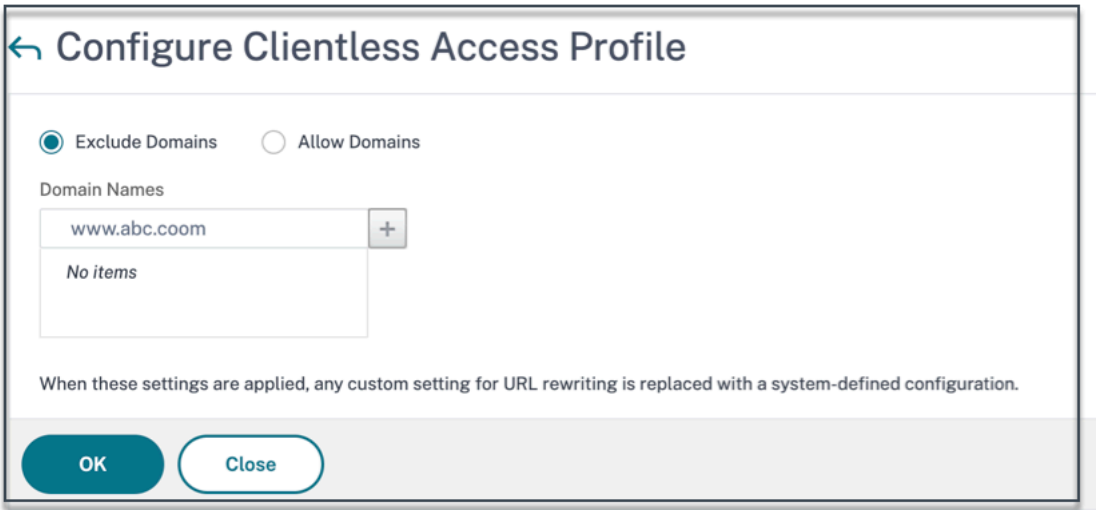
```
set vpn sessionAction <session-profile-name> -secureBrowse ENABLED
```

Exclure les domaines de la réécriture en mode d'accès sans client

Vous devez spécifier les domaines pour empêcher StoreFront de réécrire les URL en mode d'accès sans client. Excluez les noms de domaine complets du serveur StoreFront, les noms de domaine complets de l'équilibreur de charge StoreFront et citrix.com. Ce paramètre ne peut être appliqué que globalement.

1. Accédez à **Citrix Gateway > Paramètres globaux**.
2. Dans **Accès sans client**, cliquez sur **Configurer les domaines** pour l'accès sans client.

3. Sélectionnez **Exclure le domaine**.
4. Dans **Noms de domaine**, entrez les noms de domaine (noms de domaine complets du serveur StoreFront ou noms de domaine complets de l'équilibreur de charge StoreFront).
5. Cliquez sur le signe **+** et entrez `citrix.com`.
6. Cliquez sur **OK**.

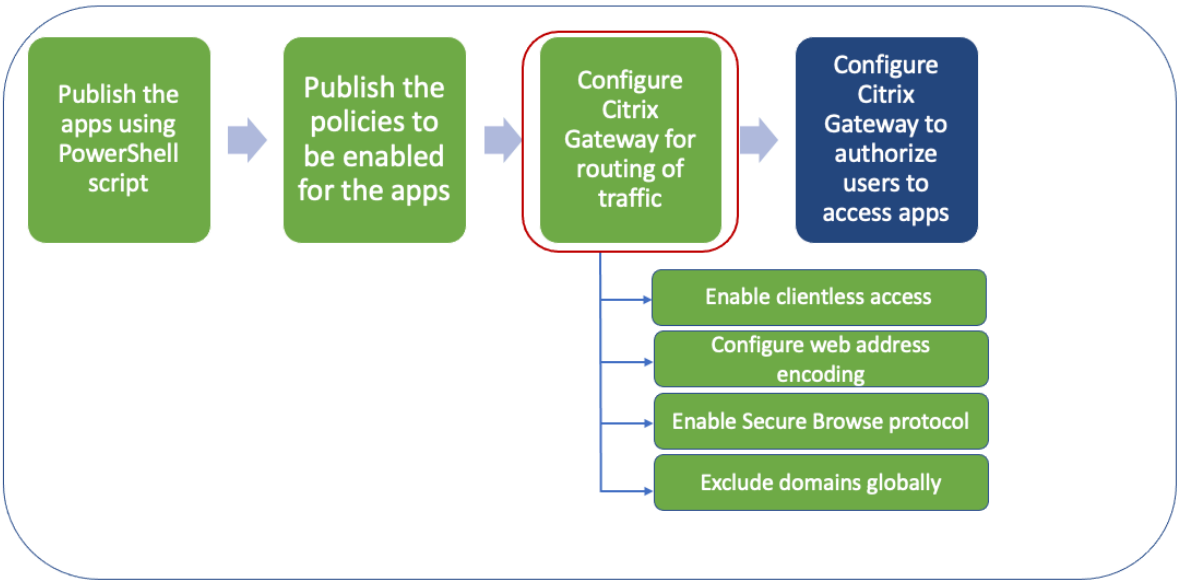


Pour exclure des domaines à l'aide de l'interface de ligne de commande NetScaler Gateway :

À l'invite de commandes, exécutez la commande suivante :

```
bind policy patset ns_cvpn_default_bypass_domains <StoreFront-FQDN>
bind policy patset ns_cvpn_default_bypass_domains citrix.com
```

Étape 4 : Configuration des stratégies d'autorisation



L'autorisation spécifie les ressources réseau auxquelles les utilisateurs ont accès lorsqu'ils se connectent à NetScaler Gateway. Le paramètre par défaut de l'autorisation consiste à refuser l'accès à toutes les ressources réseau. Citrix recommande d'utiliser le paramètre global par défaut, puis de créer des stratégies d'autorisation pour définir les ressources réseau auxquelles les utilisateurs peuvent accéder.

Vous configurez l'autorisation sur NetScaler Gateway à l'aide d'une stratégie et d'expressions d'autorisation. Après avoir créé une stratégie d'autorisation, vous pouvez la lier aux utilisateurs ou aux groupes que vous avez configurés sur l'appliance. Les stratégies utilisateur ont une priorité plus élevée que les stratégies liées aux groupes.

Stratégies d'autorisation par défaut : deux stratégies d'autorisation doivent être créées pour autoriser l'accès au serveur StoreFront et refuser l'accès à toutes les applications Web publiées.

- Allow_StoreFront
- Deny_ALL

Stratégies d'autorisation des applications Web : après avoir créé les stratégies d'autorisation par défaut, vous devez créer des stratégies d'autorisation pour chaque application Web publiée.

- `Allow_<app1>`
- `Allow_<app2>`

Pour configurer une stratégie d'autorisation à l'aide de l'interface graphique de NetScaler Gateway, procédez comme suit :

1. Accédez à **Citrix Gateway > Stratégies > Autorisation**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans Nom, tapez le nom de la stratégie.
4. Dans Action, sélectionnez **Autoriser ou Refuser**.
5. Dans Expression, cliquez sur **Expression Editor**.
6. Pour configurer une expression, cliquez sur **Sélectionner** et choisissez les éléments nécessaires.
7. Cliquez sur **Terminé**.
8. Cliquez sur **Créer**.

Pour configurer une stratégie d'autorisation à l'aide de l'interface de ligne de commande NetScaler Gateway :

À l'invite de commandes, exécutez la commande suivante :

```
add authorization policy <policy-name> "HTTP.REQ.HOSTNAME.CONTAINS("<
    StoreFront-FQDN>")" ALLOW
```

Pour lier une stratégie d'autorisation à un utilisateur/groupe à l'aide de l'interface graphique de NetScaler Gateway :

1. Accédez à **Citrix Gateway > Administration des utilisateurs**.
2. Cliquez sur **Utilisateurs AAA** ou **Groupes AAA**.
3. Dans le volet d'informations, sélectionnez un utilisateur/un groupe, puis cliquez sur **Modifier**.
4. Dans les **paramètres avancés**, cliquez sur **Stratégies d'autorisation**.
5. Sur la page Policy Binding, sélectionnez une stratégie ou créez-en une.
6. Dans **Priorité**, définissez le numéro de priorité.
7. Dans **Type**, sélectionnez le type de demande, puis cliquez sur **OK**.

Pour lier une stratégie d'autorisation à l'aide de l'interface de ligne de commande NetScaler Gateway :

À l'invite de commandes, exécutez la commande suivante :

```
bind aaa group <group-name> -policy <policy-name> -priority <priority>
    -gotoPriorityExpression END
```

Exemple de configuration de bout en bout

Dans cet exemple, une application nommée « Docs » avec l'URL https://docs.citrix.com est publiée sur Citrix Workspace.

1. Sur la machine contenant le SDK PowerShell, ouvrez PowerShell.
2. Exécutez la commande suivante.

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

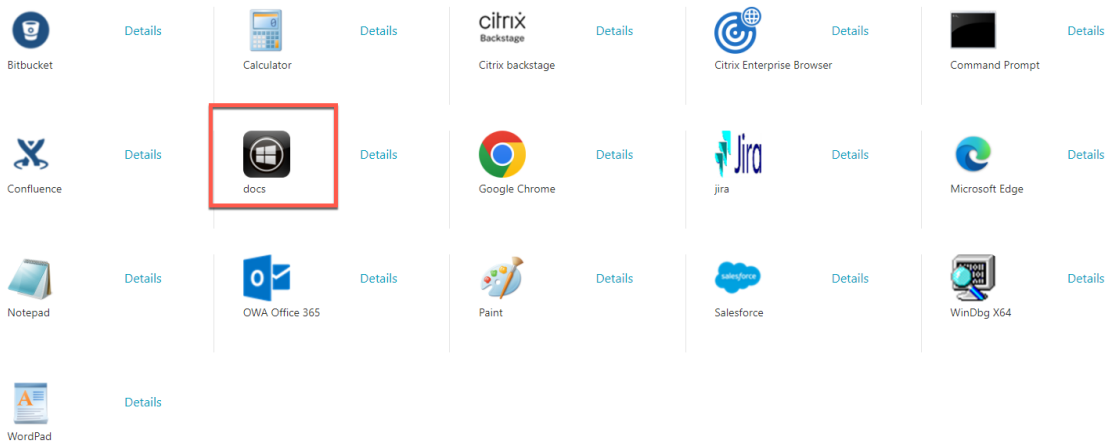
3. Ajoutez les informations suivantes à l'applet de commande.

```
$citrixUrl: "https://docs.citrix.com"
$appName: docs
$DesktopGroupId: 1
$desktopgroupname: <mydesktop23>
```

4. Exécutez la commande suivante.

```
New-BrokerApplication –ApplicationType PublishedContent –
    CommandLineExecutable $citrixURL –Name $appName –DesktopGroup
     $dg.Uid
```

L'application est désormais publiée sur Citrix Workspace.



5. Mettez à jour le fichier JSON de stratégie avec les détails de l'application (« docs »). Vérifiez les points suivants.

    - `proxytraffic_v1` la valeur est toujours définie sur `secureBrowse`. Ce paramètre garantit que le navigateur Citrix Enterprise achemine le trafic vers la page Web via NetScaler Gateway à l'aide du protocole de navigation sécurisée.
    - `browser_v1` la valeur est toujours définie sur `embeddedBrowser`. Ce paramètre n'est applicable que lorsque le navigateur Citrix Enterprise (CEB) est configuré en tant que navigateur professionnel. Lorsque cette option est définie sur `embeddedBrowser`, les liens relatifs aux domaines Secure Private Access configurés s'ouvrent dans CEB.
    - La valeur `secureBrowseAddress` est l'URL de votre NetScaler Gateway.


```
{
  "policies": [
    {
      "name": "Docs",
      "patterns": ["*.docs.netscaler.com/*"],
      "policy": {
        "watermark_v1": "enabled",
        "clipboard_v1": "disabled",
        "printing_v1": "disabled",
        "download_v1": "disabled",
        "upload_v1": "disabled",
        "keylogging_v1": "disabled",
        "screencapture_v1": "enabled",
        "proxytraffic_v1": "secureBrowse",
        "browser_v1" : "embeddedBrowser"
      }

    }],
  "system": {
    "secureBrowseAddress": "https://yournetscalergateway.com"
  }
}
```

6. Placez le fichier JSON de stratégie dans C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser.
7. Modifiez le fichier Web.config pour qu'il pointe vers le fichier de régulation que vous avez mis à jour.

```
<route name="webSecurePolicy" order="22" url="Resources/SecureBrowser/policy.json">
        <defaults>
          <add param="controller" value="BrowserPolicy" />
          <add param="action" value="BrowserResources" />
        </defaults>
        <data>
          <add name="endpointId" value="WebSecurePolicy" />
          <add name="endpointCapabilities" value="webSecurePolicy" />
          <add name="CommonData" factory="Citrix.DeliveryServices.Configuration.ObjectCollectionFactory, Citrix.DeliveryServices.Configuration, Version=3.23.0.0, Culture=neutral,
PublicKeyToken=e8b77d454fa2a856" path="citrix.deliveryservices/dazzleResources" property="commonData" />
        </data>
      </route>
```

8. Sur votre appliance NetScaler Gateway sur site, procédez comme suit :
   - Activez l'accès sans client aux applications. Vous pouvez activer l'accès sans client au niveau mondial ou au niveau de la session.
   - Activer le codage des adresses Web
   - Activer le mode de Secure Browse
   - Exclure les domaines de la réécriture en mode d'accès sans client

Pour plus de détails, consultez Étape 3 : Activation de l'authentification et de l'autorisation à l'aide de NetScaler Gateway sur site.

Flux d'utilisateurs finaux

- Connectez-vous à StoreFront en tant qu'utilisateur autorisé à accéder aux applications du groupe de mise à disposition PublishedContentApps.
- Une fois connecté, vous devez voir la nouvelle application avec l'icône par défaut. Vous pouvez personnaliser l'icône selon vos besoins. Pour plus de détails, consultez https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/.
- Lorsque vous cliquez sur l'application, celle-ci s'ouvre dans Citrix Enterprise Browser.

Détails de la stratégie d'accès aux applications

Le tableau suivant répertorie les options de stratégie d'accès disponibles et leurs valeurs.

Nom de la clé	Description de la stratégie	Valeur
—	—	—
screencapture_v1	Activer ou désactiver la fonction anti-capture d'écran pour la page Web	activé ou désactivé
keylogging_v1	Activer ou désactiver l'anti-keylogging pour la page Web	activé ou désactivé
watermark_v1	Afficher ou ne pas afficher le filigrane sur la page Web	activé ou désactivé
upload_v1	Activer ou désactiver le téléchargement de la page Web	activé ou désactivé
printing_v1	Activer ou désactiver l'impression à partir de la page Web	activé ou désactivé
download_v1	Activer ou désactiver les téléchargements depuis la page Web	activé ou désactivé
clipboard_v1	Activer ou désactiver le presse-papiers sur la page Web	activé ou désactivé
proxytraffic_v1	Détermine si le navigateur Citrix Enterprise canalise le trafic vers la page Web via NetScaler Gateway à l'aide d'une navigation sécurisée ou permet un accès direct.	direct ou SecureBrowse
browser_v1	Applicable uniquement lorsque Citrix Enterprise Browser est configuré comme navigateur professionnel. Lorsque cette option est définie sur EmbeddedBrowser, les liens relatifs aux domaines Secure Private Access configurés s'ouvrent dans le navigateur Citrix Enterprise	SystemBrowser ou EmbeddedBrowser
Nom	Nom du Web ou de l'application SaaS publiée	Il est recommandé d'utiliser le même nom que celui que vous avez saisi lors de la publication des modèles d'application	Liste séparée par des virgules des noms de domaine liés à cette application. Vous pouvez également utiliser des caractères génériques. Ces noms de domaine sont utilisés pour appliquer des stratégies aux applications par le Citrix Enterprise Browser.	*Exemples : "*.office.com/*", "*.office.net/*", "*.microsoft.com/*" .sharepoint.com/**"

> **Remarque :**
>
> les fonctions anti-keylogging et anti-capture d'écran nécessitent l'installation de la fonctionnalité de protection des applications fournie avec l'application Citrix Workspace.

Configurer les applications et les stratégies à l'aide de l'outil de configuration Secure Private Access - Legacy

August 26, 2024

Vous pouvez utiliser l'outil de configuration Secure Private Access sur un contrôleur de mise à disposition Citrix Virtual Apps and Desktops pour créer rapidement une application SaaS ou Web. En outre, vous pouvez utiliser cet outil pour définir les restrictions des applications, le routage du trafic et créer un NetScaler Gateway. L'outil génère des fichiers de script en sortie qui peuvent être exécutés sur les machines respectives pour déployer la configuration.

Versions de produits prises en charge

Assurez-vous que votre produit répond aux exigences minimales de la version.

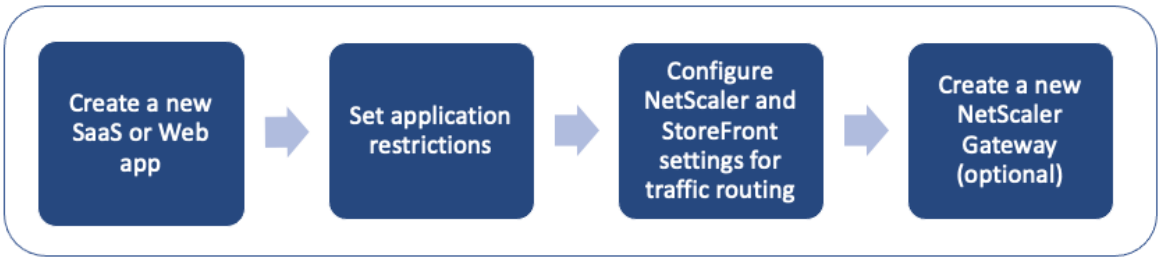
- Application Citrix Workspace
  - Windows —2303 et versions ultérieures
  - macOS —2304 et versions ultérieures
- Citrix Virtual Apps and Desktops : versions LTSR et actuelles prises en charge
- StoreFront : LTSR 2203 ou version non LTSR 2212 et versions ultérieures
- NetScaler —12.1 et versions ultérieures

Prérequis pour utiliser l'outil de configuration

- Accédez au téléchargement de l'outil de configuration depuis la page Téléchargements.
- Autorisations d'administrateur sur le contrôleur Citrix Virtual Apps and Desktops pour exécuter l'outil de configuration.
- Au moins un groupe de mise à disposition existe sur le contrôleur de mise à disposition.

Commencez à utiliser l'outil de configuration

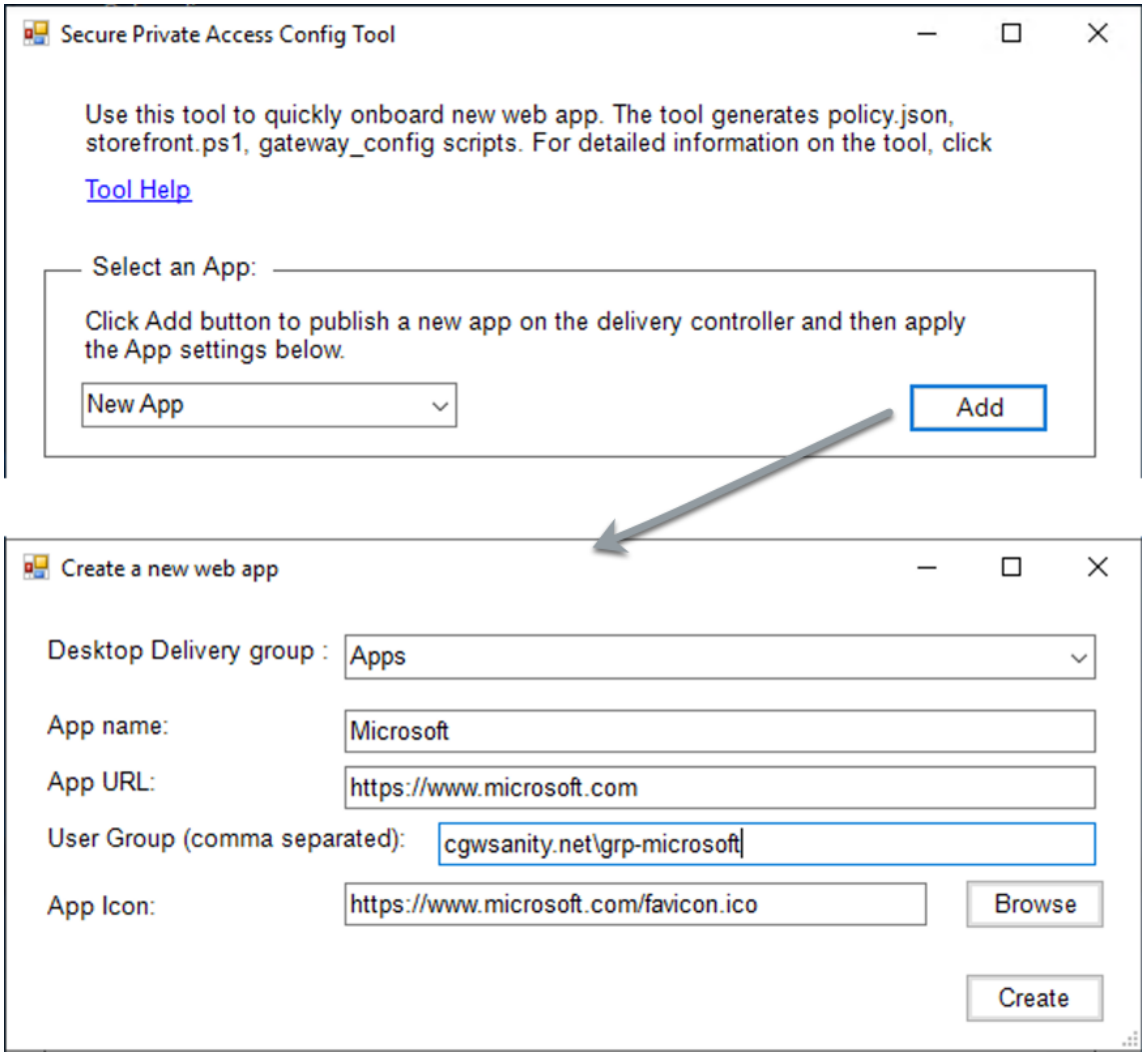
Vous pouvez effectuer les tâches suivantes à l'aide de l'outil de configuration.



- Publier une nouvelle application
- Définir les restrictions d'application
- Configurer les paramètres de StoreFront et NetScaler Gateway
- Configurer un nouveau NetScaler Gateway

Publier une nouvelle application

1. Exécutez l'outil de configuration.
2. Dans la section **Sélectionner une application**, sélectionnez **Nouvelle application** dans la liste déroulante, puis cliquez sur **Ajouter**.



3. Terminez la configuration de l'application.

   - **Groupe de mise à disposition pour ordinateur de bureau** : sélectionnez le groupe de mise à disposition pour lequel cette application doit être rendue accessible.
     Tous les groupes de mise à disposition existants sont énumérés dans le groupe de mise à disposition Desktop.
   - **Nom de l'application** : entrez le nom de l'application.
   - **URL de l'application** : Spécifiez l'URL de l'application.
   - **Groupe d'utilisateurs** : Entrez à la fois le nom de domaine et le nom du groupe au format « Domaine \ Groupe ». Les groupes d'utilisateurs peuvent contenir des espaces. Par exemple, « cgwsanity.net \ grp-microsoft », « cgwsanity.net \ grp microsoft ».
     Ces groupes doivent déjà exister dans Active Directory.

> **Note:**
>
> – Built-in domain security groups such as "Domain Users"or "Domain Admins"are not supported. Only the manually created user groups must be used.
> – The user group is only used in NetScaler Gateway authorization policies and not for app assignments in Citrix Virtual Apps and Desktops. Hence, the user group that you enter here is not visible in Studio.

- **Icône de l'application** : l'outil utilise le fichier favicon.ico de l'URL s'il est détecté. L'administrateur peut également personnaliser les icônes si nécessaire. Si aucune icône n'est fournie par l'administrateur, l'icône par défaut est attribuée à l'application.

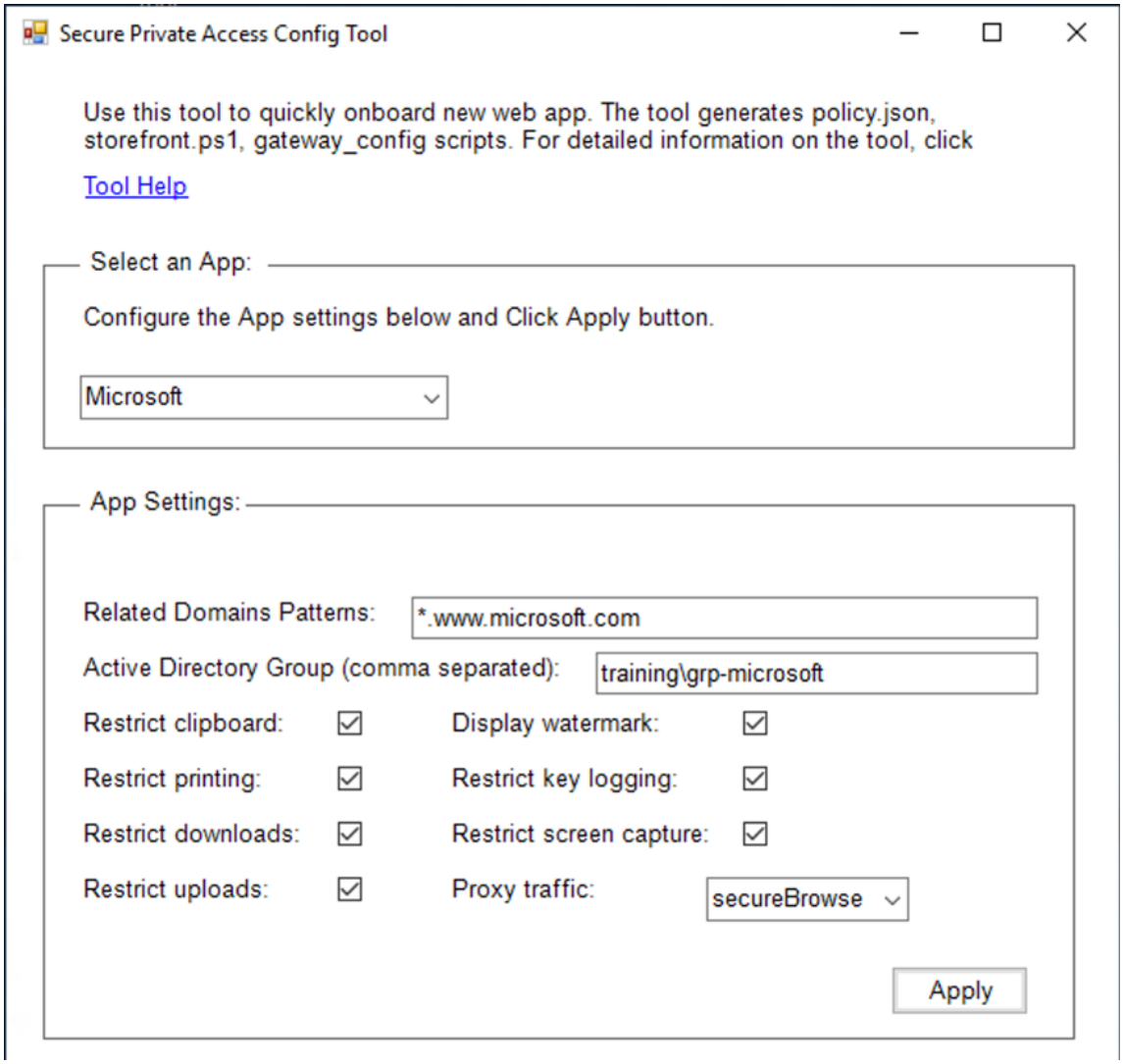
4. Cliquez sur **Créer**.

L'application est publiée sur le Delivery Controller et est disponible pour les utilisateurs des groupes d'utilisateurs de StoreFront.

Définir les restrictions d'application

Après avoir publié une nouvelle application, vous pouvez activer ou désactiver les restrictions pour cette application.

1. Dans la section **Sélectionner une application**, sélectionnez l'application dans la liste déroulante pour laquelle vous souhaitez appliquer les paramètres.



2. Configurez les paramètres de l'**application dans la section Paramètres** de l'application.

   - **Modèles de domaines associés** : L'URL du domaine associé est renseignée automatiquement en fonction de l'URL de l'application. Les administrateurs peuvent ajouter des domaines supplémentaires séparés par une virgule.
   - **Groupe Active Directory** : entrez les groupes pour lesquels cette application doit être accessible. Ce champ est obligatoire.

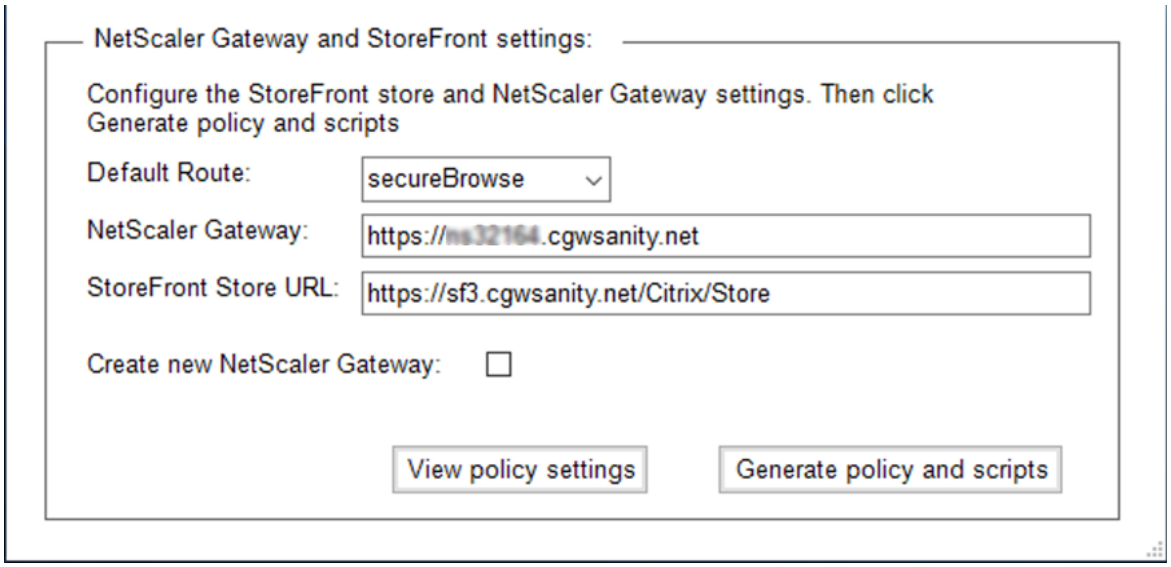
     Vous pouvez saisir plusieurs groupes séparés par une virgule. Ces groupes doivent correspondre aux groupes disponibles dans Active Directory. Aucune validation n'est effectuée sur les noms de groupe que vous saisissez ici. Il est donc important que vous preniez soin de saisir les noms des groupes pour qu'ils correspondent à ceux qui figurent dans Active Directory.
   - **Paramètres de l'application** : tous les paramètres de l'application sont restreints (sélectionnés) par défaut. Vous pouvez sélectionner ou effacer les paramètres appropriés que vous souhaitez pour les groupes d'utilisateurs.

- **Trafic proxy** : sélectionnez SecureBrowse. Ce paramètre permet au navigateur d'entreprise Citrix de canaliser le trafic vers la page Web via NetScaler Gateway.

3. Cliquez sur **Appliquer**.

Configurer les paramètres de StoreFront et NetScaler Gateway

Vous pouvez configurer les paramètres de routage du trafic via NetScaler Gateway. Vous pouvez configurer un NetScaler Gateway existant ou créer un nouveau NetScaler Gateway dans la section **Paramètres de Gateway et StoreFront**.



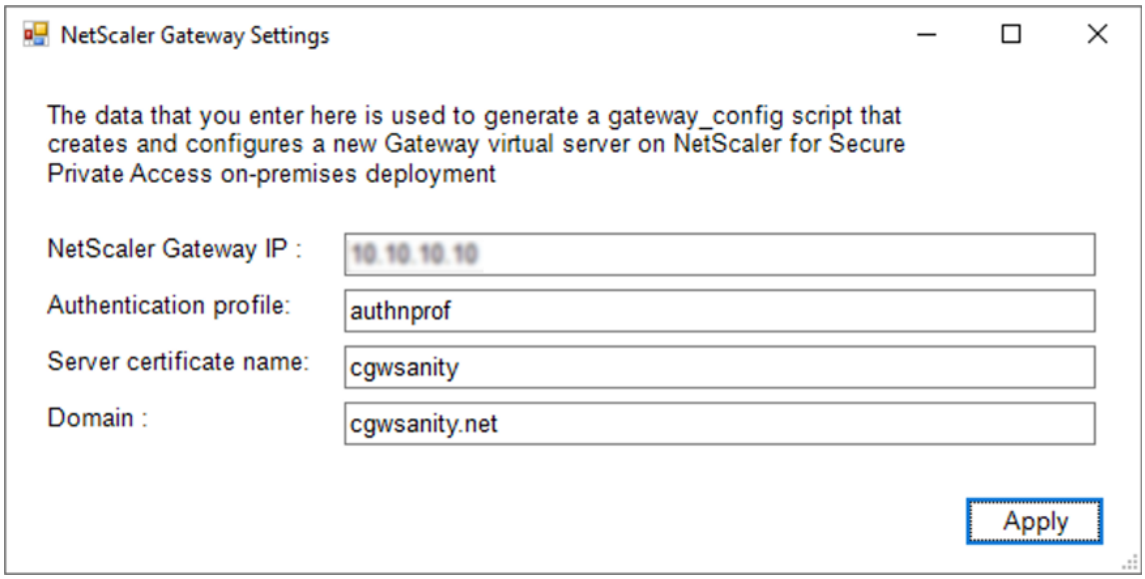
- **Itinéraire par défaut** : si aucune stratégie n'est définie pour l'application, l'itinéraire par défaut est appliqué pour les applications.
  - **SecureBrowse** : le navigateur d'entreprise Citrix tunnelise le trafic vers la page Web via NetScaler Gateway.
  - **Direct** : le navigateur d'entreprise Citrix permet un accès direct aux applications.
- **NetScaler Gateway** : entrez l'URL de NetScaler Gateway.
- **URL du magasin StoreFront : entrez l'URL**complète du magasin StoreFront. Par exemple, `http://<directory path>/Citrix/<StoreName>`. Vous pouvez obtenir l'URL à partir de la console StoreFront.
- (Facultatif) **Créer une nouvelle passerelle** : cochez la case pour créer un nouveau NetScaler Gateway et cliquez sur **Créer**.

Créez un nouveau NetScaler Gateway (facultatif)

Vous pouvez créer un nouveau NetScaler Gateway si vous ne souhaitez pas modifier les paramètres de passerelle existants.

Si vous possédez déjà NetScaler Gateway, vous pouvez configurer les stratégies d'autorisation et les liaisons pour les applications à l'aide de l'outil de configuration.

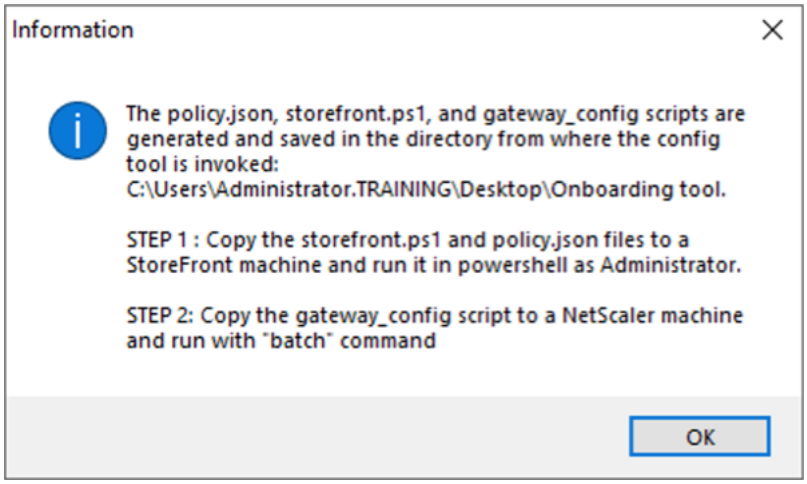
1. Vous devez saisir les informations suivantes pour le nouveau NetScaler Gateway. Aucune validation n'est effectuée par l'outil sur les valeurs que vous saisissez lors de la création d'une nouvelle passerelle. Il est donc important que vous preniez soin de saisir des valeurs précises.



   - **IP de la passerelle** : adresse IP de NetScaler Gateway.
   - **Profil d'authentification** : entrez le nom du profil d'authentification déjà configuré sur NetScaler. Pour plus de détails, voir Profils d'authentification.
   - **Nom du certificat du serveur** : entrez le nom du certificat SSL déjà configuré sur NetScaler. Pour plus de détails, consultez la section Certificats SSL.
   - **Domaine** : utilisé pour l'authentification unique (SSO) pour les applications du réseau interne. Pour plus de détails, consultez la section Action de la session VPN.

2. Cliquez sur **Appliquer**.
3. Cliquez sur **Générer une stratégie et des scripts**.

   Les fichiers policy.json, storefront.ps1 et gateway_config sont générés et stockés à l'emplacement à partir duquel vous avez exécuté l'outil de configuration.



Lorsque vous ouvrez le fichier gateway_config dans une application compatible, vous pouvez afficher deux sections du fichier de sortie.

- Sections relatives à la configuration de NetScaler Gateway (applicables uniquement lorsqu'une nouvelle passerelle est créée)
- Sections relatives aux stratégies d'autorisation, aux groupes d'utilisateurs et aux stratégies de liaison aux groupes d'utilisateurs.

L'image suivante montre le fichier gateway_config d'une nouvelle configuration de NetScaler Gateway.


```
############################################################################################################
#1. Upload file to NetScaler (e.g. to /var/tmp)
#2. Run batch command (e.g. batch -fileName /var/tmp/gateway_config -outfile /var/tmp/gateway_config_output)
#3. Analyze output (e.g. cat /var/tmp/gateway_config_output)
############################################################################################################

# Enable NS features
enable ns feature SSL SSLVPN AAA

# Add Gateway
add vpn vserver _XD_SPAGateway_443 SSL [redacted] -Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile
-deploymentType ICA_STOREFRONT -vserverFqdn gwalextest.spaopdev.local -authnProfile spaopdev_auth_prof -icaOnly OFF

# Add excluded domains
bind policy patset ns_cvpn_default_bypass_domains corealextest.spaopdev.local
bind policy patset ns_cvpn_default_bypass_domains citrix.com

# Add session actions
add vpn sessionAction AC_OS_SPAGateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF
-wihome "http://corealextest.spaopdev.local/Citrix/StoreWeb" -ClientChoices OFF -ntDomain spaopdev.local -clientlessVpnMode ON
-clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "http://corealextest.spaopdev.local" -sfGatewayAuthType domain

add vpn sessionAction AC_WB_SPAGateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF
-wihome "http://corealextest.spaopdev.local/Citrix/StoreWeb" -ClientChoices OFF -ntDomain spaopdev.local -clientlessVpnMode ON
-clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "http://corealextest.spaopdev.local" -sfGatewayAuthType domain

# Add session policies
add vpn sessionPolicy PL_OS_SPAGateway "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")" AC_OS_SPAGateway
add vpn sessionPolicy PL_WB_SPAGateway "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT" AC_WB_SPAGateway

# Bind policies to vserver
bind vpn vserver _XD_SPAGateway_443 -policy PL_OS_SPAGateway -priority 100 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver _XD_SPAGateway_443 -policy PL_WB_SPAGateway -priority 110 -gotoPriorityExpression NEXT -type REQUEST

# Bind SSL cert to GW
bind ssl vserver _XD_SPAGateway_443 -certkeyName spaopdev

# Add default authorization policies
add authorization policy ALLOW_STOREFRONT "HTTP.REQ.HOSTNAME.CONTAINS(\"corealextest.spaopdev.local\")" ALLOW
add authorization policy DENY_ALL true DENY

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "SPAOP users"
bind aaa group "SPAOP users" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "SPAOP users" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.google.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.google.com\")" ALLOW

unbind aaa group "SPAOP users" -policy www.google.com
bind aaa group "SPAOP users" -policy www.google.com -priority 100 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupab"
bind aaa group "groupab" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupab" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

unbind aaa group "groupab" -policy www.google.com
bind aaa group "groupab" -policy www.google.com -priority 110 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupxy"
bind aaa group "groupxy" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupxy" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.microsoft.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.microsoft.com\")" ALLOW

unbind aaa group "groupxy" -policy www.microsoft.com
bind aaa group "groupxy" -policy www.microsoft.com -priority 120 -gotoPriorityExpression END

# Save
save ns config
```

L'image suivante montre le fichier gateway_config d'une configuration NetScaler Gateway mise à jour.


```
#############################################################################################################
#1. Upload file to NetScaler (e.g. to /tmp)
#2. Run batch command (e.g. batch -fileName /tmp/Gateway_config -outfile /tmp/Gateway_config_output)
#3. Analyze output (e.g. cat /tmp/Gateway_config_output)
#############################################################################################################

# Add default authorization policies
add  policy ALLOW_STOREFRONT "HTTP.REQ.HOSTNAME.CONTAINS(\"corealextest.spaopdev.local\")" ALLOW
add  policy DENY_ALL true DENY

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "SPAOP users"
bind aaa group "SPAOP users" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "SPAOP users" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.google.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.google.com\")" ALLOW

unbind aaa group "SPAOP users" -policy www.google.com
bind aaa group "SPAOP users" -policy www.google.com -priority 100 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupab"
bind aaa group "groupab" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupab" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

unbind aaa group "groupab" -policy www.google.com
bind aaa group "groupab" -policy www.google.com -priority 110 -gotoPriorityExpression END

# Add group and bind default policies: ALLOW_STOREFRONT, DENY_ALL
add aaa group "groupxy"
bind aaa group "groupxy" -policy ALLOW_STOREFRONT -priority 10 -gotoPriorityExpression END
bind aaa group "groupxy" -policy DENY_ALL -priority 65000 -gotoPriorityExpression END

add authorization policy www.microsoft.com "HTTP.REQ.HOSTNAME.CONTAINS(\"www.microsoft.com\")" ALLOW

unbind aaa group "groupxy" -policy www.microsoft.com
bind aaa group "groupxy" -policy www.microsoft.com -priority 120 -gotoPriorityExpression END

# Save
save ns config
```

Configurer StoreFront avec le nouveau NetScaler Gateway

- Pour configurer les paramètres de StoreFront et NetScaler Gateway dans l'outil, vous avez besoin des éléments suivants :
  - Nom de domaine complet de NetScaler Gateway
  - URL du magasin StoreFront
- Exigences de configuration de StoreFront :
  - NetScaler Gateway : l'accès à distance est activé.
  - L'authentification directe depuis NetScaler Gateway est activée.
  - Active Directory : accès administrateur pour ajouter ou mettre à jour des utilisateurs ou des groupes, et pour configurer le profil ou les stratégies d'authentification sur NetScaler.

Pour plus de détails, voir Intégrer NetScaler Gateway à StoreFront.

Utiliser les fichiers de sortie de l'outil de configuration pour déployer des applications et configurer des stratégies

L'outil de configuration génère les fichiers suivants. Ces fichiers sont enregistrés à l'emplacement/-dans le répertoire où l'outil est chargé et exécuté.

- policy.json
- storefront.ps1
- gateway_config

1. Copiez les fichiers storefront.ps1 dans StoreFront.
2. Exécutez le script storefront.ps1 sur PowerShell, en tant qu'administrateur.

   Le script crée un dossier Resources \ SecureBrowser s'il n'est pas déjà disponible dans le chemin du magasin.

   Le script met également à jour le fichier web.config correspondant à l'itinéraire du fichier policy.json.
3. Copiez le fichier policy.json dans le dossier Resources \ SecureBrowser créé par storefront.ps1 sous le magasin.
4. Copiez le gateway_config sur un NetScaler et exécutez le script à l'aide de la commande batch suivante sur l'interface de ligne de commande NetScaler.

   ```
   batch -fileName /var/tmp/gateway_config -outfile /var/tmp/gateway_config_o
   ```

> **Remarque :**
>
> - Lorsqu'une modification de configuration est effectuée dans l'outil, les scripts et les stratégies doivent être régénérés. Vous devez copier à nouveau le fichier policy.json dans le dossier Resources \ SecureBrowser de la machine StoreFront et le script gateway_config doit être réexécuté sur NetScaler.
> - Il n'est pas nécessaire de réexécuter le fichier storefront.ps1 si le nom/l'URL du magasin n'est pas modifié.

Références supplémentaires

Reportez-vous à la documentation suivante pour plus de détails.

- Secure Private Access for on-premises
- Guide de déploiement : Secure Private Access sur site