Citrix Secure Private Access - Legado

Machine translated content

Disclaimer

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Cloud Software Group solo tiene traducción automática. Cloud Software Group no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Cloud Software Group se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Cloud Software Group, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Cloud Software Group no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

Contents

Configurar Secure Private Access para implementaciones locales - Legacy

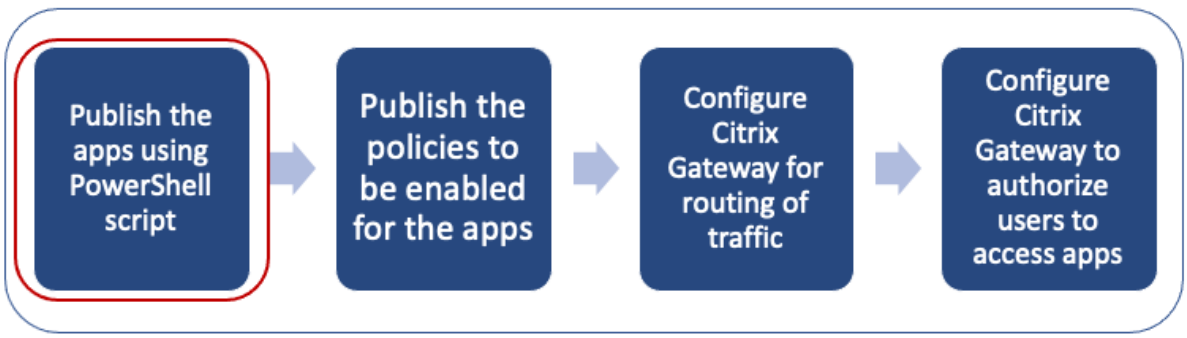
December 27, 2023

La configuración de la solución de Secure Private Access para instalaciones locales es un proceso de cuatro pasos.

1. Publica las aplicaciones
2. Publica las directivas de las aplicaciones
3. Habilite el enrutamiento del tráfico a través de NetScaler Gateway
4. Configurar directivas de autorización

> **Importante:**
>
> Hay una herramienta de configuración disponible para incorporar rápidamente aplicaciones y directivas para las aplicaciones y también para configurar los ajustes de NetScaler Gateway y StoreFront. Sin embargo, tenga en cuenta lo siguiente antes de utilizar la herramienta.
>
> - Lea las secciones Publicar las aplicaciones y Publicar directivas para las aplicaciones para asegurarse de que comprende completamente los requisitos de configuración para la configuración de la solución local.
> - Esta herramienta solo se puede utilizar como complemento de los procedimientos existentes documentados en este tema y no reemplaza la configuración que debe realizarse manualmente.
>
> Para obtener información completa sobre la herramienta, consulte Configurar aplicaciones y directivas mediante la herramienta de configuración de Secure Private Access.

Paso 1: Publica las aplicaciones



Debe usar el script de PowerShell para publicar las URL. Una vez publicada la aplicación, se puede administrar mediante la consola de Citrix Studio.

Puede descargar el script de PowerShell desde https://www.citrix.com/downloads/workspace-app/powershell-module-for-configuring-secure-private-access-for-storefront/configure-secure-private-access-for-storefront.html.

1. En la máquina que contiene el SDK de PowerShell, abra PowerShell.
2. Ejecute este comando:

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup -Name PublishedContentApps
<!--NeedCopy-->
```

3. Defina las variables de la aplicación 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>
<!--NeedCopy-->
```

> **Nota:**
>
> Asegúrese de actualizar los marcadores marcados con corchetes angulares (< >) antes de ejecutar el comando.

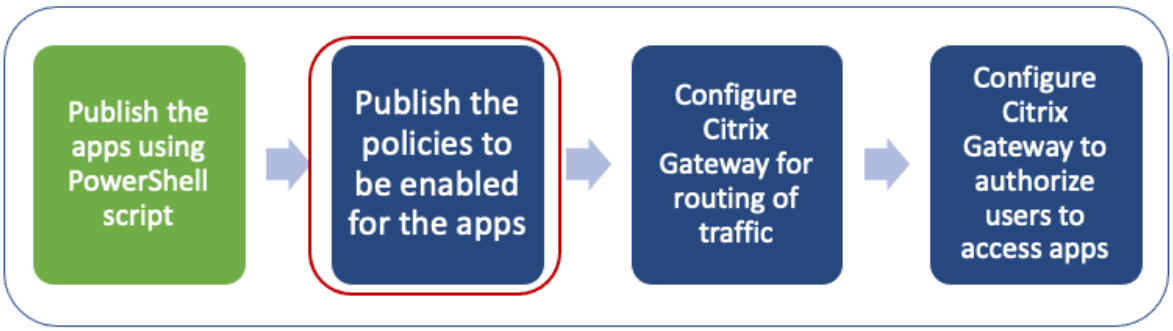
Tras asignar la ubicación y el nombre de la aplicación, ejecute el siguiente comando para publicar la aplicación.

```
New-BrokerApplication -ApplicationType PublishedContent -
    CommandLineExecutable $citrixURL -Name $appName -DesktopGroup $dg.
    Uid
<!--NeedCopy-->
```

La aplicación publicada aparece en la sección **Aplicaciones** de **Citrix Studio**. Ahora puede modificar los detalles de la aplicación desde la propia consola de Citrix Studio.

Para obtener más información sobre cómo publicar la aplicación y cambiar el icono predeterminado de la aplicación publicada, consulte Publicar contenido.

Paso 2: Publicar directivas para las aplicaciones



El archivo de directivas define los controles de enrutamiento y seguridad de cada aplicación publicada. Debe actualizar el archivo de directivas sobre cómo se enruta una aplicación web o SaaS (a través de una puerta de enlace o sin una puerta de enlace).

Para hacer cumplir las directivas de acceso a las aplicaciones, debe publicar las directivas de cada una de las aplicaciones web o SaaS. Para ello, debe actualizar el archivo JSON de la directiva y el archivo Web.config.

- **Archivo JSON de directivas:** actualice el archivo JSON de directivas con los detalles de la aplicación y las directivas de seguridad de las aplicaciones. A continuación, el archivo JSON de la directiva debe colocarse en el servidor de StoreFront en `C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser`.

  > **Nota:**
  >
  > Debe crear las carpetas denominadas **Resources** y **SecureBrowser** y, a continuación, agregar el archivo JSON de la directiva a la carpeta SecureBrowser.
  > Para obtener más información sobre las distintas acciones directivas y sus valores, consulte los detalles de la directiva de acceso a la aplicación.

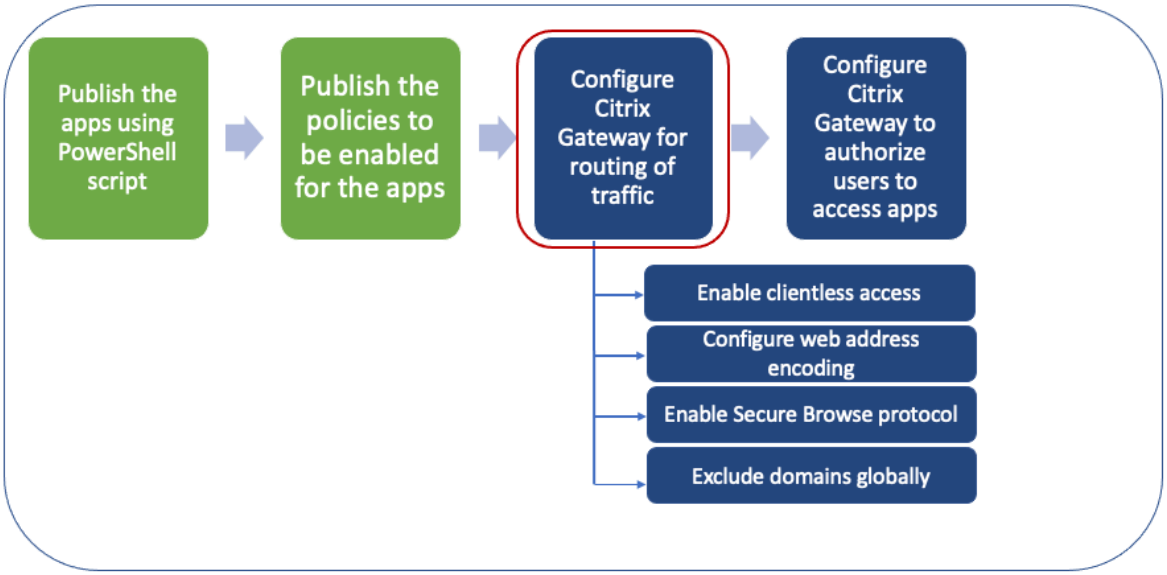
- **Archivo web.config:** Para que los detalles de la nueva directiva estén disponibles para la aplicación Citrix Workspace y Citrix Enterprise Browser, debe modificar el archivo web.config en el directorio de almacenes de StoreFront. Debe modificar el archivo para agregar una nueva etiqueta XML con el nombre route. A continuación, el archivo Web.config debe colocarse en la ubicación C:\inetpub\wwwroot\Citrix\Store1.

  Consulte Ejemplo de configuración de extremo a extremo para ver un archivo XML de ejemplo.

  > **Nota:**
  >
  > En la ruta, "store1"hace referencia al nombre especificado para el almacén cuando se creó. Si se utiliza un nombre de almacén diferente, se debe crear una carpeta adecuada.

Se recomienda agregar una nueva ruta al final de las rutas existentes. En caso de agregar una ruta en el medio, debe actualizar manualmente el número de pedido para todas las rutas siguientes.

Paso 3: Habilitar el enrutamiento del tráfico a través de NetScaler Gateway



Habilitar el enrutamiento del tráfico a través de NetScaler Gateway implica los siguientes pasos:

- Habilitar el acceso sin cliente
- Habilitar la codificación URL
- Habilitar Secure Browse
- Excluir dominios para que no se reescriban en modo de acceso sin cliente

El acceso sin cliente, la codificación de URL y la navegación segura se pueden habilitar globalmente o mediante una directiva por sesión.

- La configuración habilitada globalmente se aplica a todos los servidores virtuales NetScaler Gateway configurados.
- La configuración de la directiva por sesión se aplica a los usuarios, grupos o servidores virtuales de Gateway.

Habilitar el acceso sin cliente

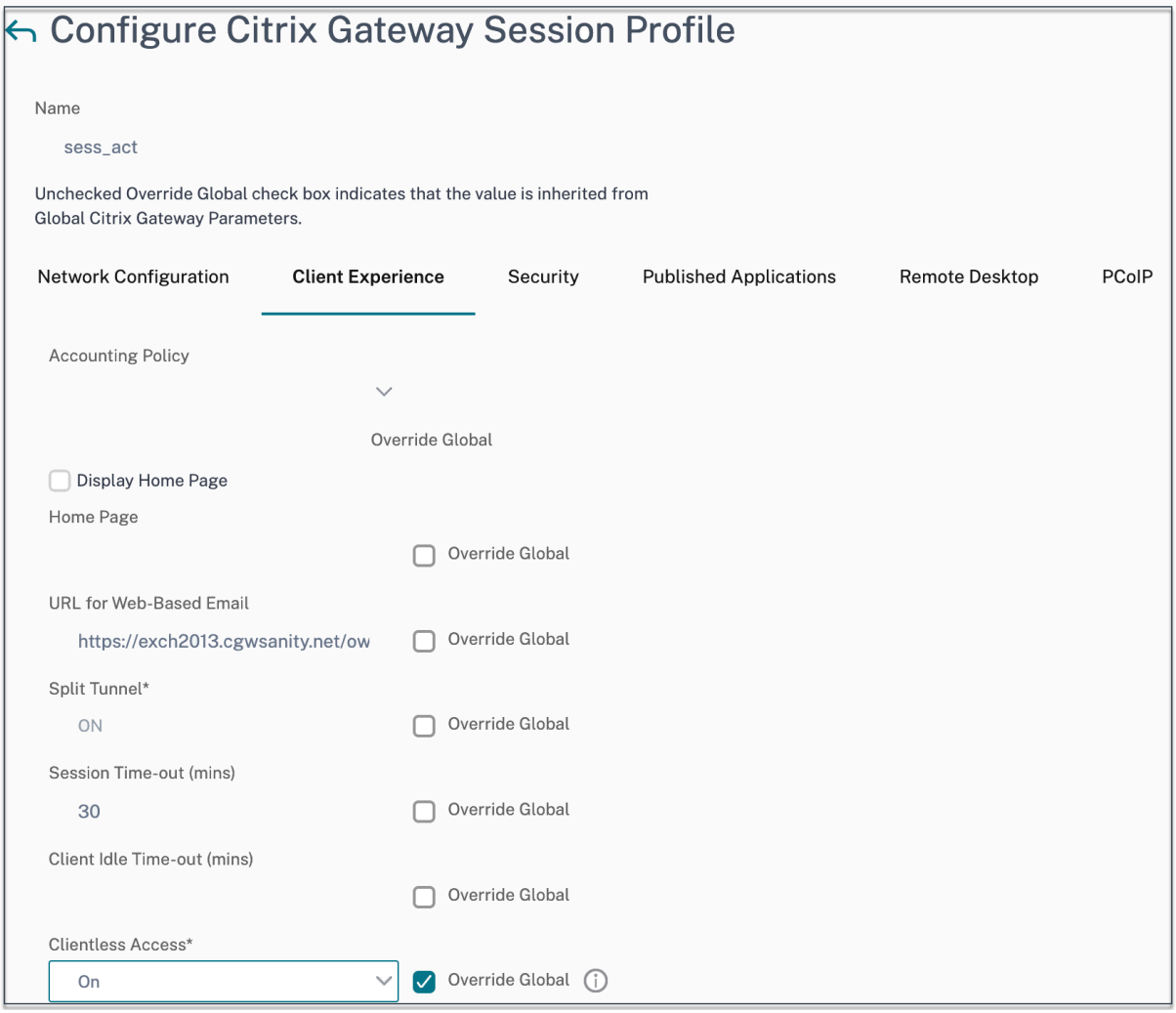
Para habilitar el acceso sin cliente a nivel mundial mediante la interfaz gráfica de usuario de NetScaler Gateway:

En la ficha **Configuración**, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global**.
En la página Configuración global, haz clic en **Cambiar la configuración global** .
En la ficha Experiencia del cliente**, en Acceso sin cliente, seleccione ACTIVADO y, a continuación, haga clic en**Aceptar**.**

Para habilitar el acceso sin cliente mediante una directiva de sesión mediante la GUI de NetScaler Gateway:

Si quiere que solo un grupo selecto de usuarios, grupos o servidores virtuales utilice el acceso sin cliente, desactive o borre el acceso sin cliente de forma global. A continuación, mediante una directiva de sesión, habilite el acceso sin cliente y vincúlelo a usuarios, grupos o servidores virtuales.

1. En la ficha **Configuración**, expanda **Citrix Gateway** y, a continuación, haga clic en **Directivas > Sesión**.
2. Haga clic en la ficha **Directiva de sesión** y, a continuación, en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Perfil**, haga clic en **Nuevo**.
5. En **Nombre** , escriba un nombre para el perfil.
6. En la ficha **Experiencia del cliente**, junto a Clientless Access, haga clic en **Anular global**, seleccione **Activar** y, a continuación, haga clic en **Crear**.
7. En **Expresión**, escriba `true`. Al introducir el valor `true`, la directiva siempre se aplica al nivel al que está vinculada.
8. Haga clic en **Crear** y, a continuación, en **Cerrar** .



Para habilitar el acceso sin cliente a nivel mundial mediante la CLI de NetScaler Gateway:

En el símbolo del sistema, ejecute el siguiente comando:

```
set vpn parameter -clientlessVpnMode On -icaProxy OFF
<!--NeedCopy-->
```

Para habilitar la directiva de acceso sin cliente por sesión mediante la CLI de NetScaler Gateway:

En el símbolo del sistema, ejecute el siguiente comando:

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


Habilitar la codificación URL

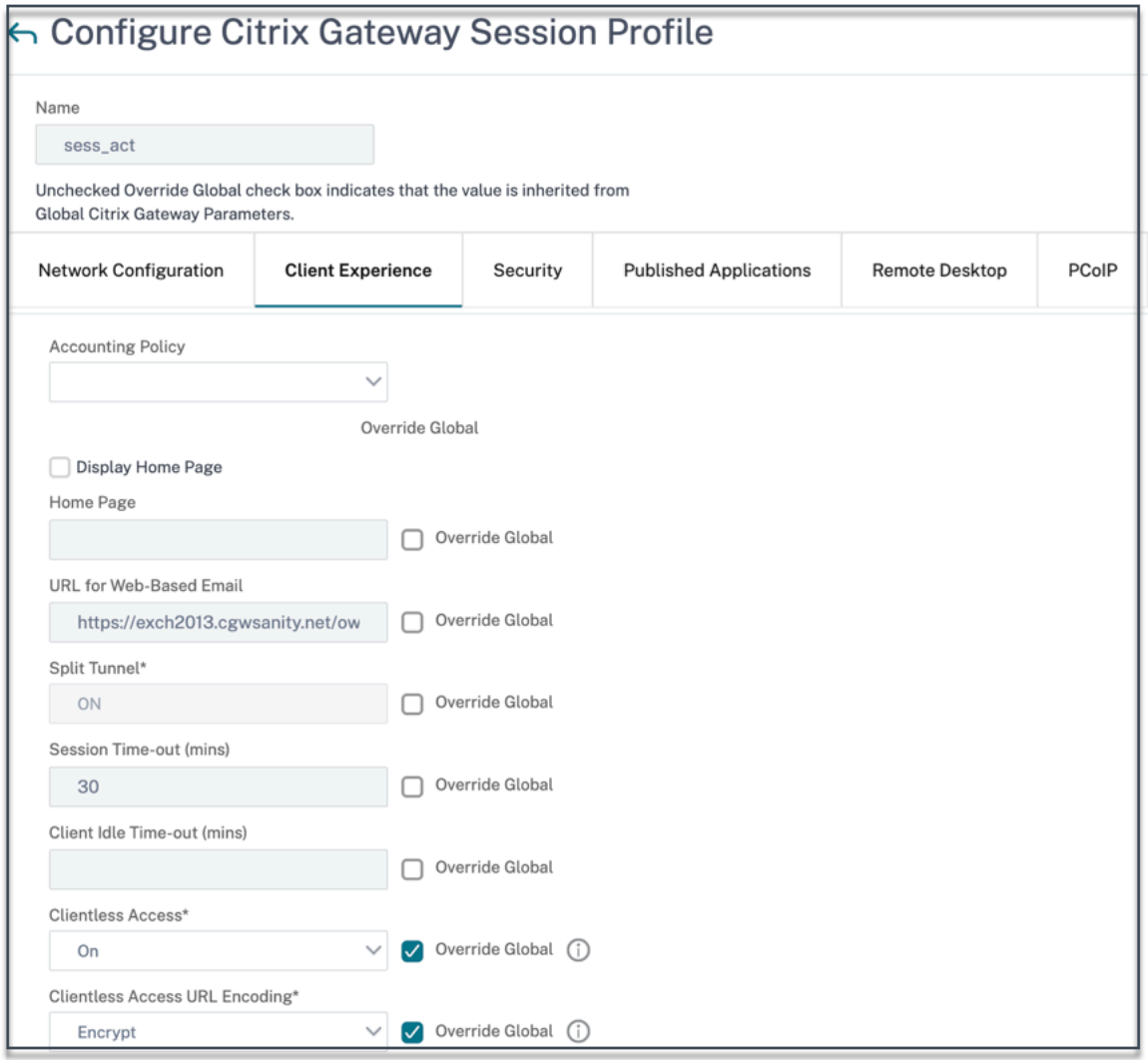
Al habilitar el acceso sin cliente, puede optar por codificar las direcciones de las aplicaciones web internas o dejar la dirección como texto sin cifrar. Se recomienda dejar la dirección web como texto sin cifrar para un acceso sin clientes.

Para habilitar la codificación URL de forma global mediante la interfaz gráfica de usuario de NetScaler Gateway:

1. En la ficha **Configuración**, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global**.
2. En la página **Configuración global** , haz clic en **Cambiar la configuración global** .
3. En la ficha **Experiencia del cliente**, en **Codificación de URL de acceso sin cliente**, seleccione la configuración para codificar la URL web y, a continuación, haga clic en **Aceptar**.

Para habilitar la codificación de URL a nivel de directiva de sesión mediante la GUI de NetScaler Gateway:

1. En la ficha **Configuración**, expanda **Citrix Gateway** y, a continuación, haga clic en **Directivas > Sesión**.
2. Haga clic en la ficha **Directiva de sesión**y, a continuación, en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Perfil**, haga clic en **Nuevo**.
5. En **Nombre** , escriba un nombre para el perfil.
6. En la ficha **Experiencia del cliente**, junto a **Codificación URL de acceso sin cliente**, haga clic en **Anular global**, seleccione el nivel de codificación y, a continuación, haga clic en **Aceptar**.
7. En **Expresión**, escriba `true`. Al introducir el valor `true`, la directiva siempre se aplica al nivel al que está vinculada.



Para habilitar la codificación URL de forma global mediante la CLI de NetScaler Gateway:

En el símbolo del sistema, ejecute el siguiente comando:

```
set vpn parameter -clientlessModeUrlEncoding TRANSPARENT
<!--NeedCopy-->
```

Para habilitar la directiva de codificación de URL por sesión mediante la CLI de NetScaler Gateway:

En el símbolo del sistema, ejecute el siguiente comando:

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


Habilitar Secure Browse

La navegación segura y el acceso sin cliente funcionan en conjunto para permitir las conexiones mediante el modo VPN sin cliente. Debe habilitar el modo de navegación segura para que Citrix Enterprise Browser pueda usar el modo de navegación segura para acceder a las aplicaciones sin la VPN antigua.

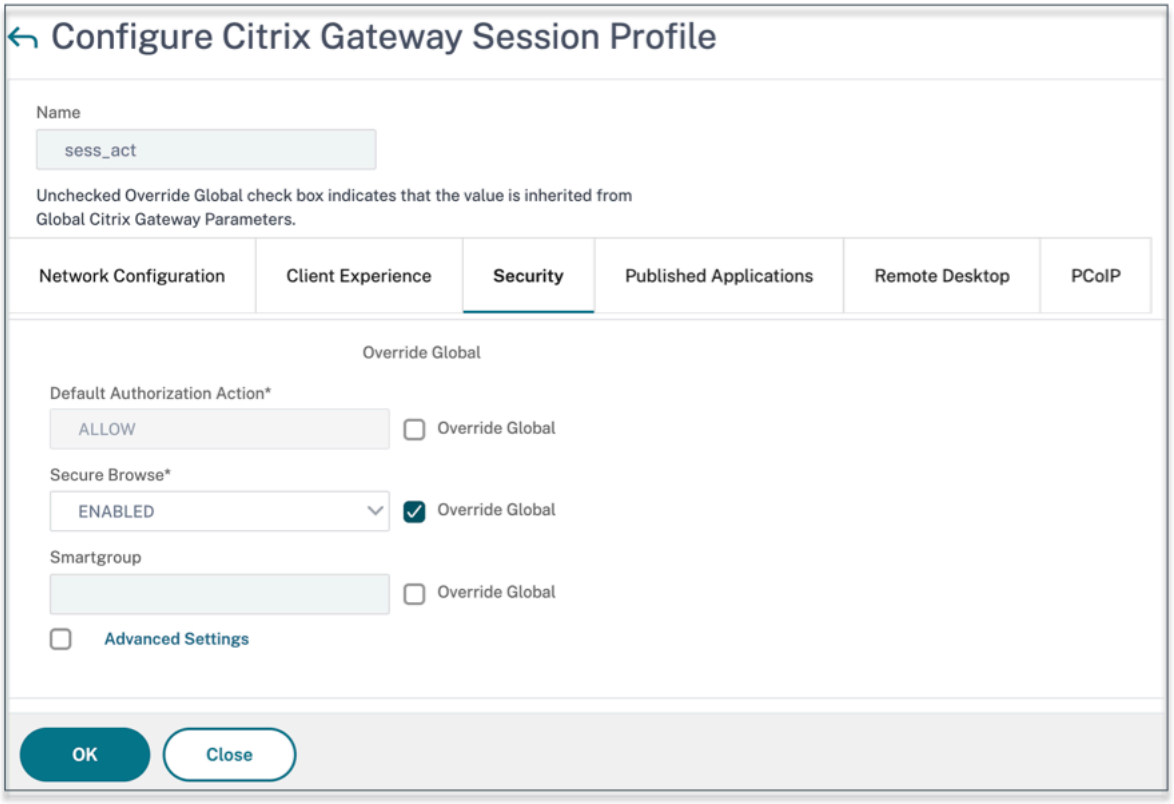
> **Nota:**
>
> Cuando el usuario final no tiene instalado Citrix Enterprise Browser, las URL publicadas con la etiqueta **SPAEnabled** se abren a través del explorador web predeterminado del dispositivo en lugar de hacerlo en Citrix Enterprise Browser. En tal caso, las directivas de seguridad no se aplican. El problema se produce únicamente en las implementaciones de StoreFront.

Para habilitar el modo de navegación segura a nivel mundial mediante la interfaz gráfica de usuario de NetScaler Gateway:

1. En la ficha **Configuración**, expanda **Citrix Gateway** y, a continuación, haga clic en **Configuración global**.
2. En la página Configuración global, haga clic en **Cambiar la configuración global**.
3. En la ficha **Seguridad**, en Secure Browse, seleccione **ACTIVADO** y, a continuación, haga clic en **Aceptar**.

Para habilitar el modo de navegación segura a nivel de directiva de sesión mediante la GUI de NetScaler Gateway:

1. En la ficha **Configuración**, expanda **Citrix Gateway** y, a continuación, haga clic en **Directivas > Sesión**.
2. Haga clic en la ficha **Directiva de sesión** y, a continuación, en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Perfil**, haga clic en **Nuevo**.
5. En **Nombre** , escriba un nombre para el perfil.
6. En la ficha **Seguridad**, haga clic en **Anular de forma global** y defina **Secure Browse** como **ACTIVADA**.



Para habilitar una navegación segura a nivel mundial mediante la CLI de NetScaler Gateway:

En el símbolo del sistema, ejecute el siguiente comando:

```
set vpn parameter -secureBrowse ENABLED
<!--NeedCopy-->
```

Para habilitar la directiva de navegación segura por sesión mediante la CLI de NetScaler Gateway:

En el símbolo del sistema, ejecute el siguiente comando:

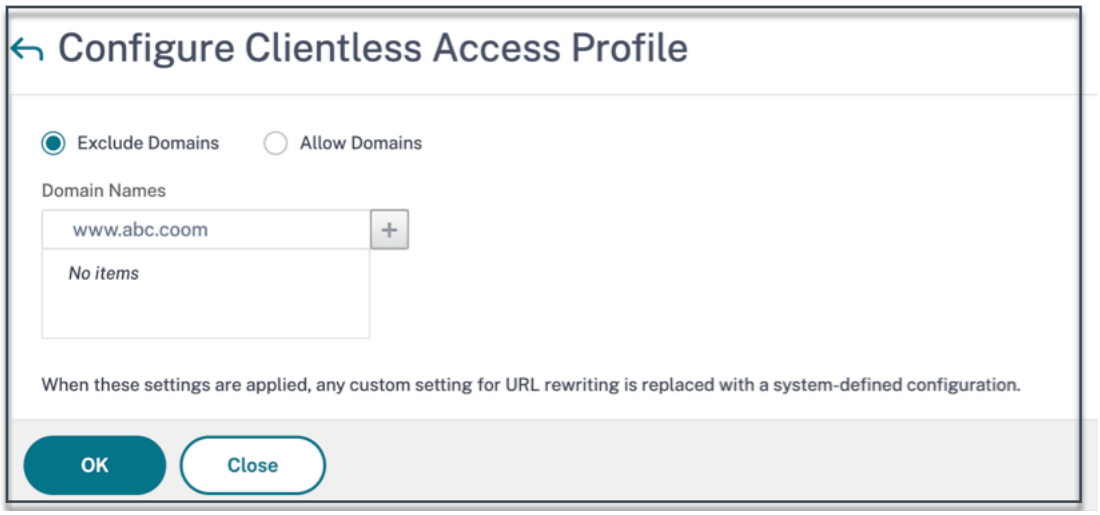
```
set vpn sessionAction <session-profile-name> -secureBrowse ENABLED
<!--NeedCopy-->
```

Excluir dominios para que no se reescriban en modo de acceso sin cliente

Debe especificar los dominios para evitar que StoreFront reescriba las URL en el modo de acceso sin cliente. Excluya los FQDN del servidor StoreFront o los FQDN del equilibrador de carga de StoreFront y citrix.com. Esta configuración solo se puede aplicar de forma global.

1. Vaya a **Citrix Gateway > Configuración global**.
2. En **Acceso sin cliente**, haga clic en **Configurar dominios** para acceso sin cliente.
3. Seleccione **Excluir dominio**.

4. En **Nombres de dominio**, introduzca los nombres de dominio (FQDN del servidor StoreFront o FQDN del equilibrador de carga de StoreFront).
5. Haga clic en el signo **+** y escriba `citrix.com`.
6. Haga clic en **Aceptar**.

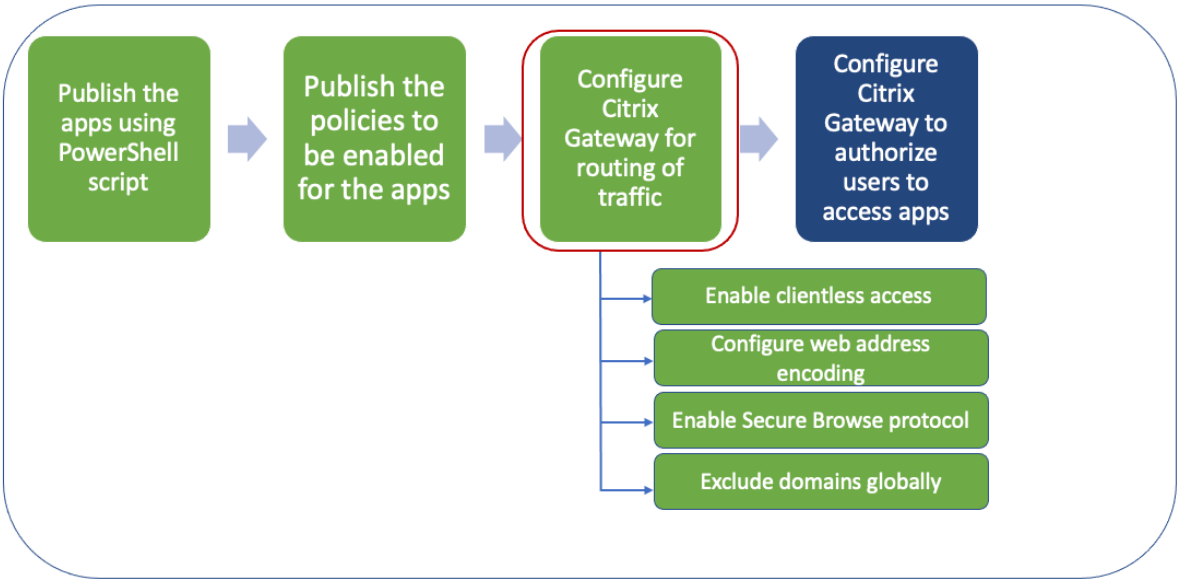


Para excluir dominios mediante la CLI de NetScaler Gateway:

En el símbolo del sistema, ejecute el siguiente comando:

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

Paso 4: Configurar las directivas de autorización



La autorización especifica los recursos de red a los que tienen acceso los usuarios cuando inician sesión en NetScaler Gateway. La configuración predeterminada de la autorización es denegar el acceso a todos los recursos de red. Citrix recomienda utilizar la configuración global predeterminada y, a continuación, crear directivas de autorización para definir los recursos de red a los que pueden acceder los usuarios.

La autorización se configura en NetScaler Gateway mediante una directiva de autorización y expresiones. Después de crear una directiva de autorización, puede vincularla a los usuarios o grupos que haya configurado en el dispositivo. Las directivas de usuario tienen una prioridad más alta que las directivas vinculadas a grupos.

Directivas de autorización predeterminadas: se deben crear dos directivas de autorización para permitir el acceso al servidor StoreFront y denegar el acceso a todas las aplicaciones web publicadas.

- Allow_StoreFront
- Deny_ALL

Directivas de autorización de aplicaciones web: después de crear las directivas de autorización predeterminadas, debe crear directivas de autorización para cada aplicación web publicada.

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

Para configurar una directiva de autorización mediante la GUI de NetScaler Gateway:

1. Vaya a **Citrix Gateway > Directivas > Autorización**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En Nombre, escriba un nombre para la directiva.
4. En Acción, selecciona **Permitir o Denegar**.
5. En Expresión, haga clic en **Editor de expresiones**.
6. Para configurar una expresión, haga clic en **Seleccionar** y elija los elementos necesarios.
7. Haga clic en **Listo**.
8. Haga clic en **Crear**.

Para configurar una directiva de autorización mediante la CLI de NetScaler Gateway:

En el símbolo del sistema, ejecute el siguiente comando:

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

Para vincular una directiva de autorización a un usuario o grupo mediante la GUI de NetScaler Gateway:

1. Vaya a **Citrix Gateway > Administración de usuarios**.

2. Haga clic en **Usuarios AAAo Grupos AAA**.
3. En el panel de detalles, seleccione un usuario o grupo y, a continuación, haga clic en **Modificar**.
4. En **Configuración avanzada**, haga clic en **Directivas de autorización**.
5. En la página Vinculación de directivas, seleccione una directiva o cree una directiva.
6. En **Prioridad**, defina el número de prioridad.
7. En **Tipo**, seleccione el tipo de solicitud y, a continuación, haga clic en **Aceptar**.

Para vincular una directiva de autorización mediante la CLI de NetScaler Gateway:

En el símbolo del sistema, ejecute el siguiente comando:

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

Ejemplo de configuración de extremo a extremo

En este ejemplo, se publica en Citrix Workspace una aplicación denominada “Docs”con la URL https://docs.citrix.com.

1. En la máquina que contiene el SDK de PowerShell, abra PowerShell.
2. Ejecute el comando siguiente.

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup –Name PublishedContentApps
<!--NeedCopy-->
```

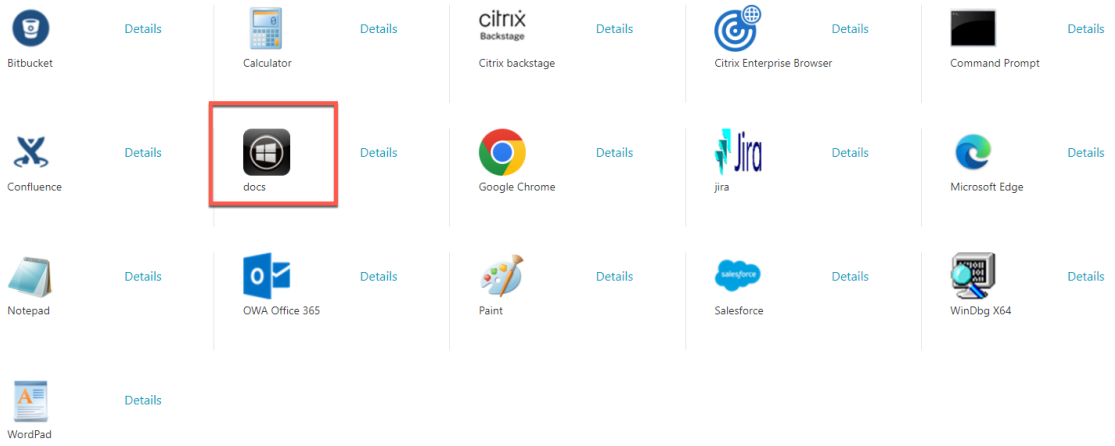
3. Agregue los siguientes detalles al cmdlet.

```
$citrixUrl: “https://docs.citrix.com”
$appName: docs
$DesktopGroupId: 1
$desktopgroupname: <mydesktop23>
<!--NeedCopy-->
```

4. Ejecute el comando siguiente.

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

La aplicación ahora está publicada en Citrix Workspace.



5. Actualice el archivo JSON de la directiva con los detalles de la aplicación (“documentos”). Asegúrese de lo siguiente:

   - El valor `proxytraffic_v1` siempre se establece en `secureBrowse`. Esta configuración garantiza que Citrix Enterprise Browser dirija el tráfico a la página web a través de NetScaler Gateway mediante el protocolo de navegación segura.
   - El valor `browser_v1` siempre se establece en `embeddedBrowser`. Esta configuración solo se aplica cuando Citrix Enterprise Browser (CEB) está configurado como explorador web de trabajo. Si se establece en `embeddedBrowser`, los enlaces relacionados con los dominios de Secure Private Access configurados se abren en CEB.
   - `secureBrowseAddress` el valor es la URL de 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. Coloque el archivo JSON de la directiva en C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser.
7. Modifique el archivo Web.config para que apunte al archivo de directivas que ha actualizado.

```
<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. En su dispositivo local de NetScaler Gateway, haga lo siguiente:
   - Habilite el acceso sin cliente a las aplicaciones. Puede habilitar el acceso sin cliente de forma global o a nivel de sesión.
   - Habilitar la codificación de direcciones web
   - Habilitar el modo Secure Browse
   - Excluir dominios para que no se reescriban en modo de acceso sin cliente

Para obtener más información, consulte el paso 3: Habilitar la autenticación y la autorización mediante el NetScaler Gateway local.

Flujo del usuario final

- Inicie sesión en StoreFront como usuario que puede acceder a las aplicaciones del grupo de entrega PublishedContentApps.
- Al iniciar sesión, debe ver la nueva aplicación con el icono predeterminado. Puede personalizar el icono según sea necesario. Para obtener información detallada, consulte.https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/
- Al hacer clic en la aplicación, la aplicación se abre en Citrix Enterprise Browser.

Detalles de la directiva de acceso a la aplicación

La siguiente tabla muestra las opciones de directiva de acceso disponibles y sus valores.

Nombre de la clave	Descripción de la directiva	Valor
—	—	—
screencapture_v1	Habilitar o inhabilitar la función de protección contra capturas de pantalla de la página web	enabled o disabled
keylogging_v1	Habilitar o inhabilitar la protección contra el registro de tecleo en la página web	enabled o disabled
watermark_v1	Mostrar o no mostrar la marca de agua en la página web	enabled o disabled
upload_v1	Habilitar o inhabilitar las cargas en la página web	enabled o disabled
printing_v1	Habilitar o inhabilitar la impresión desde la página web	enabled o disabled
download_v1	Habilitar o inhabilitar las descargas desde la página web	enabled o disabled
clipboard_v1	Habilitar o inhabilitar el portapapeles en la página web	enabled o disabled
proxytraffic_v1	Determina si Citrix Enterprise Browser canaliza el tráfico a la página web a través de NetScaler Gateway mediante una navegación segura o permite el acceso directo.	direct o secureBrowse
browser_v1	Aplicable solo cuando Citrix Enterprise Browser está configurado como explorador web de trabajo. Cuando se establece en embeddedBrowser, los enlaces relacionados con los dominios de Secure Private Access configurados se abren en Citrix Enterprise Browser	systemBrowser o embeddedBrowser
Nombre	Nombre de la Web o de la aplicación SaaS publicada	Se recomienda que utilice el mismo nombre que introdujo al publicar los patrones de la aplicación	Lista de nombres de dominio relacionados con esta aplicación separados por comas. También puede utilizar caracteres comodín. El explorador web Citrix Enterprise Browser utiliza estos nombres de dominio para aplicar directivas a las aplicaciones.	Ejemplos: “*.office.com/*”, “*.office.net/*”, “*.microsoft.com/*“.sharepoint.com/*”

> **Nota:**
>
> La protección contra el registro de tecleo y las capturas de pantalla, es necesario instalar la función de protección de aplicaciones que viene con la aplicación Citrix Workspace.

Configure aplicaciones y directivas con la herramienta de configuración de Secure Private Access - Legacy

February 16, 2024

Puede utilizar la herramienta de configuración de Secure Private Access en un controlador de entrega de Citrix Virtual Apps and Desktops para crear rápidamente una aplicación web o SaaS. Además, puede utilizar esta herramienta para establecer las restricciones de las aplicaciones, el enrutamiento del tráfico y crear un NetScaler Gateway. La herramienta genera archivos de script como salida que se pueden ejecutar en las máquinas respectivas para implementar la configuración.

Versiones de productos compatibles

Asegúrese de que su producto cumpla con los requisitos mínimos de versión.

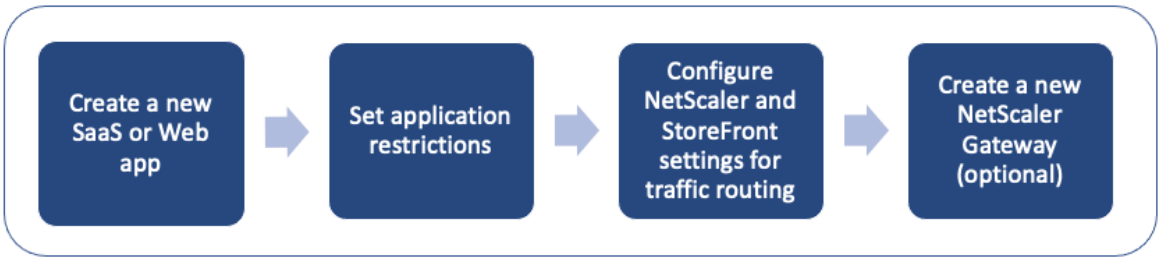
- Aplicación Citrix Workspace
  - Windows: 2303 y versiones posteriores
  - macOS —2304 y versiones posteriores
- Citrix Virtual Apps and Desktops: versiones LTSR compatibles y actuales
- StoreFront: LTSR 2203 o no LTSR 2212 y versiones posteriores
- NetScaler: 12.1 y versiones posteriores

Requisitos previos para utilizar la herramienta de configuración

- Acceda para descargar la herramienta de configuración desde la página de descargas.
- Permisos de administrador en el controlador Citrix Virtual Apps and Desktops para ejecutar la herramienta de configuración.
- Existe al menos un grupo de entrega en el controlador de entrega.

Comience con la herramienta de configuración

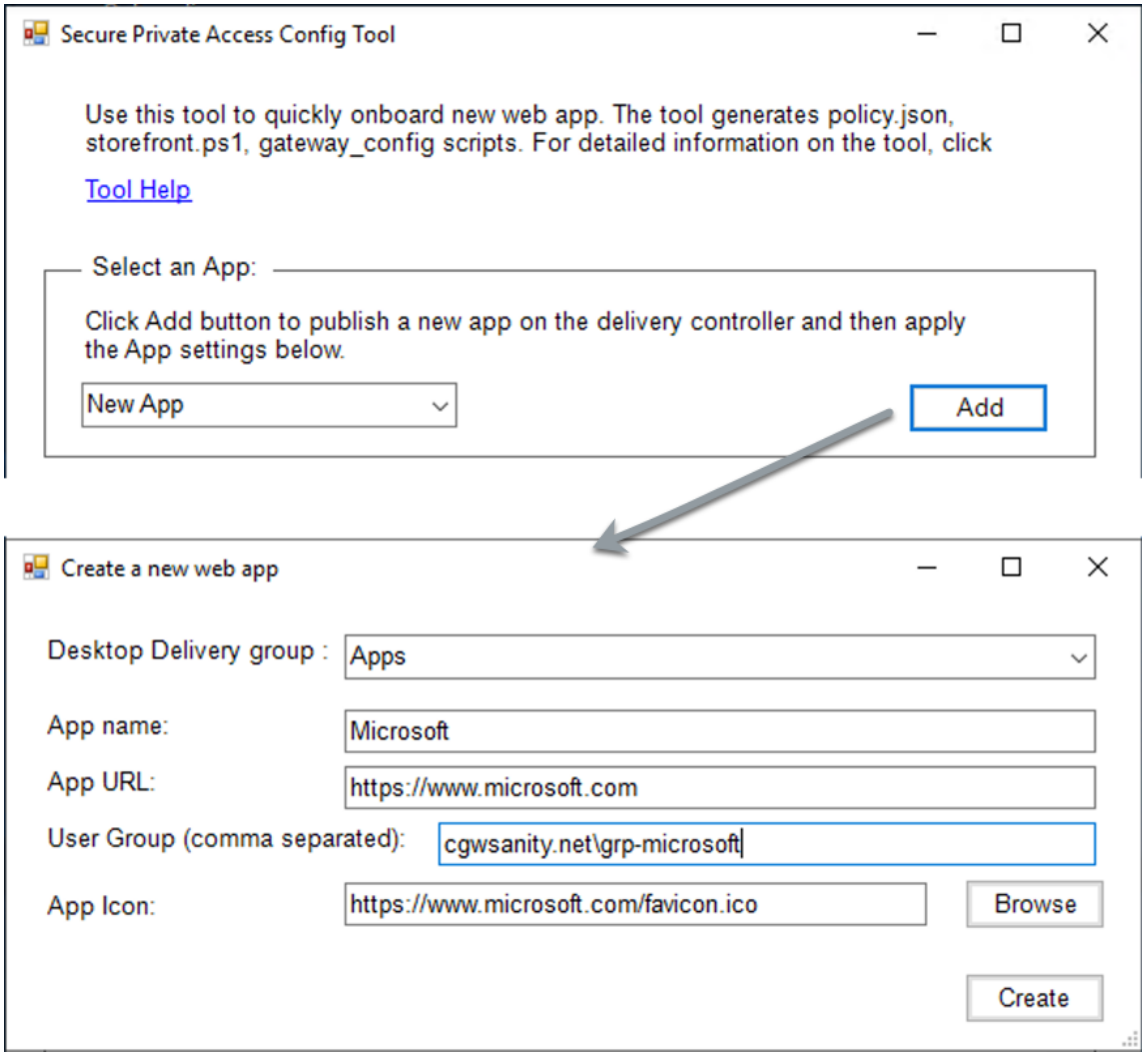
Puede realizar las siguientes tareas con la herramienta de configuración.



- Publicar una nueva aplicación
- Establecer restricciones de aplicación
- Configurar los ajustes de StoreFront y NetScaler Gateway
- Configurar un nuevo NetScaler Gateway

Publicar una nueva aplicación

1. Ejecute la herramienta de configuración.
2. En la sección **Seleccione una aplicación**, seleccione **Nueva aplicación** en la lista desplegable y, a continuación, haga clic en **Agregar**.



3. Complete la configuración de la aplicación.

   - **Grupo de entrega de escritorio**: seleccione el grupo de entrega para el que se debe hacer accesible esta aplicación.
     Todos los grupos de entrega existentes se enumeran en el grupo de entrega de escritorio.
   - **Nombre de la aplicación**: introduzca el nombre de la aplicación.
   - **URL de la aplicación**: especifique la URL de la aplicación.
   - **Grupo de usuarios**: introduzca el nombre de dominio y el nombre del grupo en el formato “Dominio\ Grupo”. Los grupos de usuarios pueden contener espacios. Por ejemplo, “cgwsanity.net\grp-microsoft”, “cgwsanity.net\grp microsoft”.
     Estos grupos ya deben existir en 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.

- **Icono de la aplicación**: la herramienta usa el archivo favicon.ico de la URL si se detecta. El administrador también puede personalizar los iconos si es necesario. Si el administrador no proporciona ningún icono, se asigna el icono predeterminado a la aplicación.

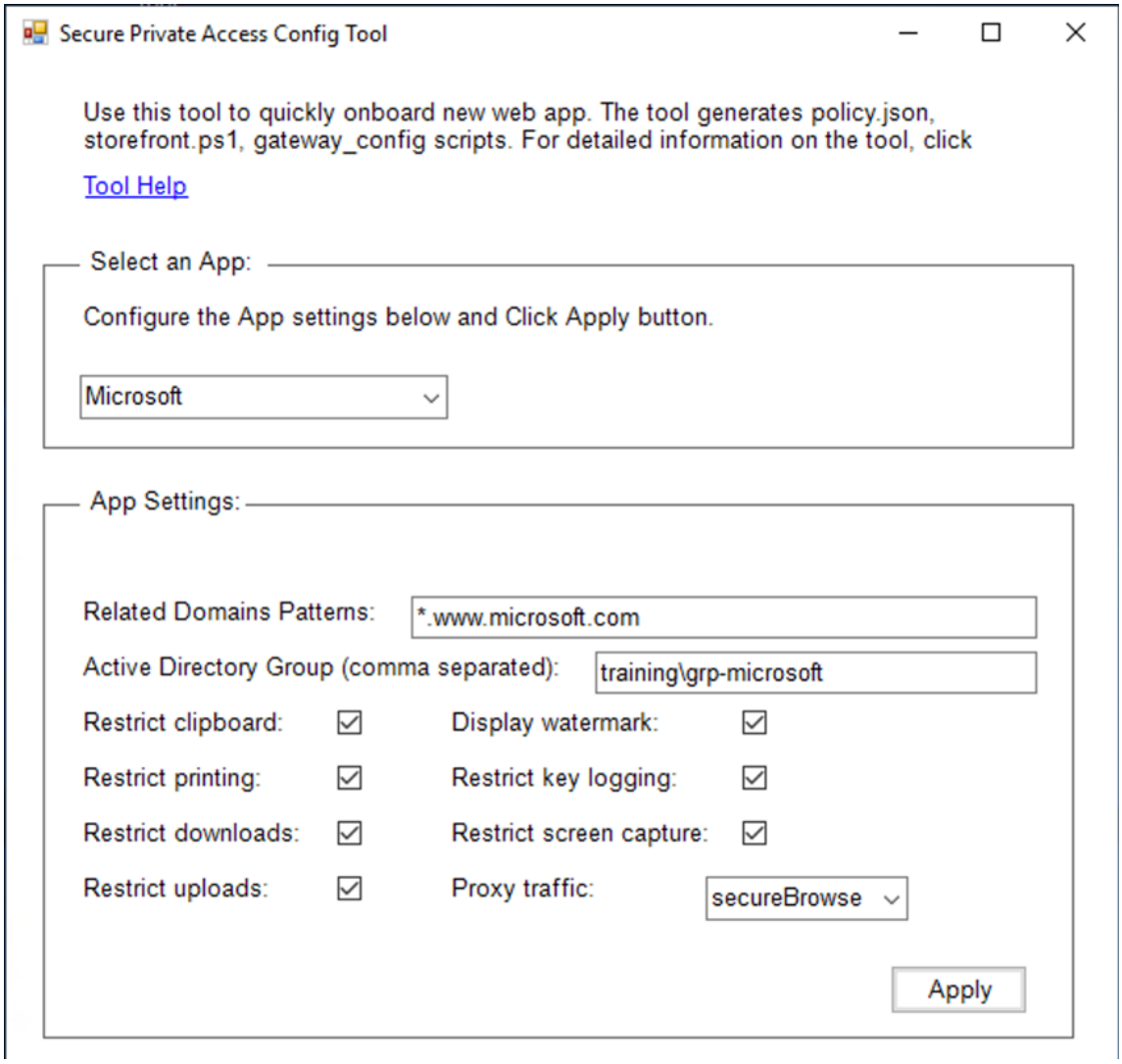
4. Haga clic en **Crear**.

La aplicación se publica en el controlador de entrega y está disponible para los usuarios de los grupos de usuarios de StoreFront.

Establecer restricciones de aplicación

Después de publicar una nueva aplicación, puede habilitar o inhabilitar las restricciones para esa aplicación.

1. En la sección **Seleccione una aplicación**, seleccione la aplicación de la lista desplegable para la que desee aplicar la configuración.



2. Configure los ajustes de la aplicación en la sección **Configuración de la aplicación**.

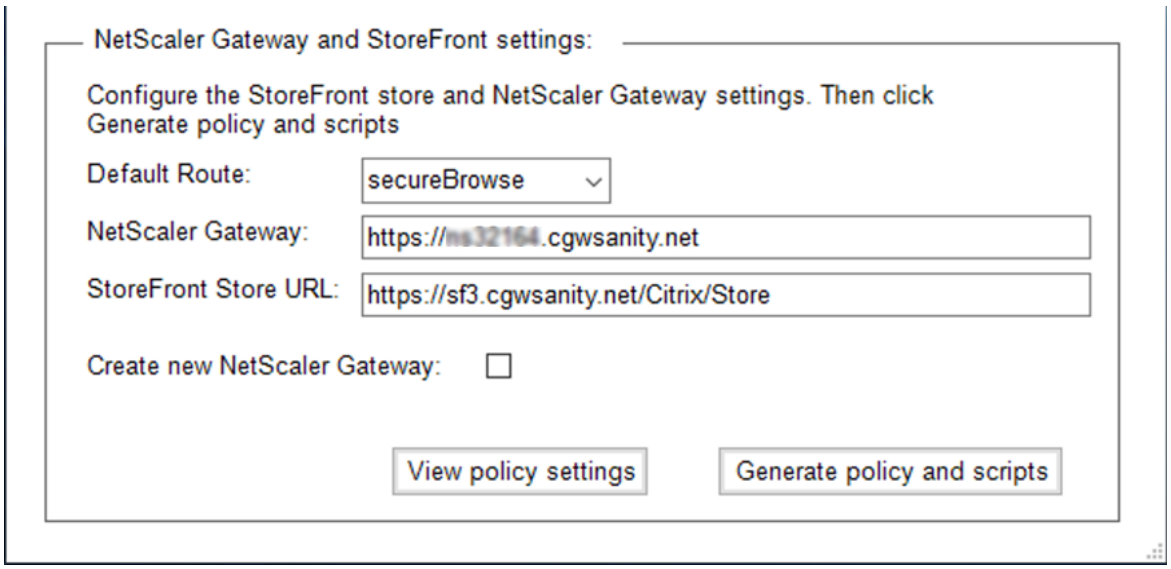
   - **Patrones de dominios relacionados**: la URL del dominio relacionado se rellena automáticamente en función de la URL de la aplicación. Los administradores pueden agregar dominios adicionales separados por una coma.
   - **Grupo de Active Directory**: introduzca los grupos para los que debe estar accesible esta aplicación. Este campo es obligatorio.
     Puede introducir varios grupos separados por una coma. Estos grupos deben coincidir con los grupos disponibles en Active Directory. Los nombres de los grupos que introduzca aquí no se validan. Por lo tanto, es importante que introduzca los nombres de los grupos para que coincidan con los que hay en Active Directory.
   - **Configuración de la aplicación**: todos los ajustes de la aplicación están restringidos (seleccionados) de forma predeterminada. Puede seleccionar o borrar la configuración adecuada que desee para los grupos de usuarios.
   - **Tráfico de proxy**: Seleccione secureBrowse. Esta configuración permite que el explorador

web empresarial de Citrix canalice el tráfico a la página web a través de NetScaler Gateway.

3. Haga clic en **Aplicar**.

Configurar los ajustes de StoreFront y NetScaler Gateway

Puede configurar los ajustes para enrutar el tráfico a través de NetScaler Gateway. Puede configurar un NetScaler Gateway existente o crear un NetScaler Gateway nuevo en la sección **Parámetros de Gateway y StoreFront**.



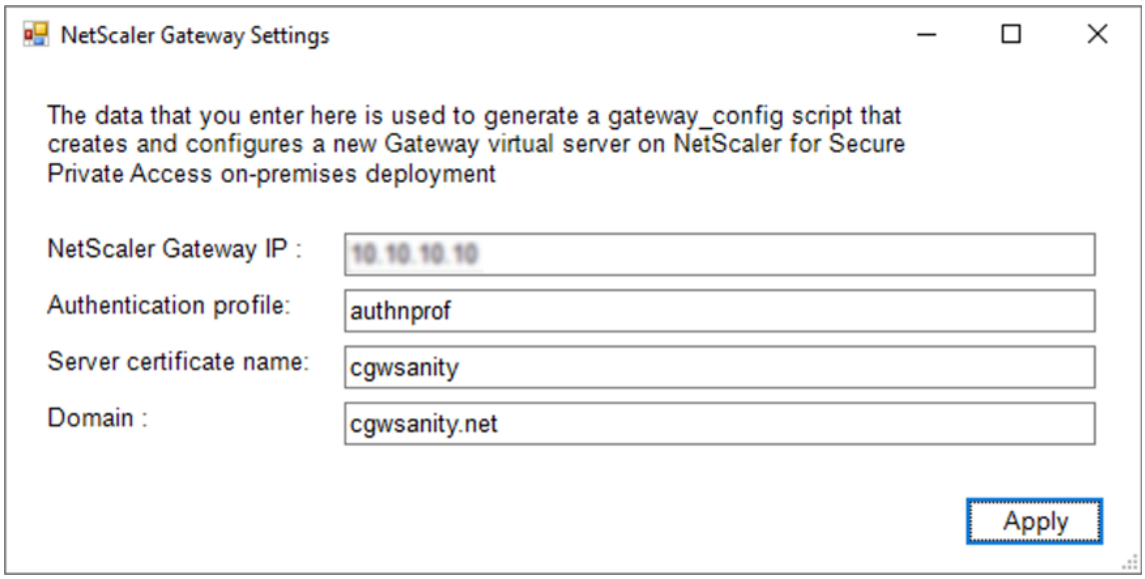
- **Ruta predeterminada**: si no se define una directiva para la aplicación, se aplica la ruta predeterminada a las aplicaciones.
  - **secureBrowse**: el explorador web empresarial de Citrix canaliza el tráfico a la página web a través de NetScaler Gateway.
  - **Directo**: el explorador web empresarial de Citrix permite el acceso directo a las aplicaciones.
- **NetScaler Gateway**: introduzca la URL de NetScaler Gateway.
- **URL del almacén de StoreFront**: Introduzca la URL completa del almacén de StoreFront. Por ejemplo:.`http://<directory path>/Citrix/<StoreName>` Puede obtener la URL desde la consola de StoreFront.
- (Opcional) **Crear nueva puerta de enlace**: Seleccione la casilla de verificación para crear un NetScaler Gateway nuevo y haga clic en **Crear**.

Crear un nuevo NetScaler Gateway (opcional)

Puede crear un nuevo NetScaler Gateway si no desea cambiar la configuración de la puerta de enlace existente.

Si ya tiene un NetScaler Gateway, puede configurar las directivas de autorización y los enlaces de las aplicaciones mediante la herramienta de configuración.

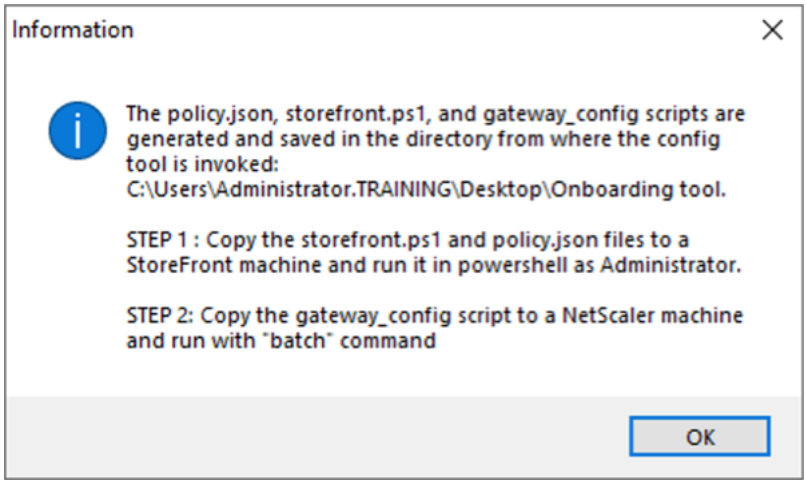
1. Debe introducir los siguientes detalles para el nuevo NetScaler Gateway. La herramienta no valida los valores que se introducen al crear una nueva puerta de enlace. Por lo tanto, es importante que tenga cuidado de introducir valores precisos.



   - **IP de puerta**de enlace: dirección IP de NetScaler Gateway.
   - **Perfil de autenticación**: introduzca el nombre del perfil de autenticación que ya está configurado en NetScaler. Para obtener más información, consulte Perfiles de autenticación.
   - **Nombre del certificado de servidor**: introduzca el nombre del certificado SSL que ya está configurado en NetScaler. Para obtener más información, consulte Certificados SSL.
   - **Dominio**: se utiliza para el inicio de sesión único de las aplicaciones de la red interna. Para obtener más información, consulte Acción de sesión de VPN.

2. Haga clic en **Aplicar**.
3. Haga clic en **Generar directivas y scripts**.

   Los archivos policy.json, storefront.ps1 y gateway_config se generan y almacenan en la ubicación desde la que se ha ejecutado la herramienta de configuración.



Al abrir el archivo gateway_config en una aplicación compatible, puede ver dos secciones en el archivo de salida.

- Secciones relacionadas con la configuración de NetScaler Gateway (aplicable solo cuando se crea una nueva puerta de enlace)
- Secciones relacionadas con las directivas de autorización, los grupos de usuarios y las directivas vinculantes a los grupos de usuarios.

La siguiente imagen muestra el archivo gateway_config de una nueva configuración 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
```

La siguiente imagen muestra el archivo gateway_config de una configuración de NetScaler Gateway actualizada.


```
#############################################################################################################
#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
```

Configure StoreFront con el nuevo NetScaler Gateway

- Para configurar los ajustes de StoreFront y NetScaler Gateway en la herramienta, necesita lo siguiente:
  - FQDN de NetScaler Gateway
  - URL de almacén de StoreFront
- Requisitos de configuración de StoreFront:
  - NetScaler Gateway: el acceso remoto está habilitado.
  - La autenticación de transferencia de NetScaler Gateway está habilitada.
  - Active Directory: acceso de administrador para agregar o actualizar usuarios o grupos y configurar el perfil o las directivas de autenticación en NetScaler.

Para obtener más información, consulte Integrar NetScaler Gateway conStoreFront.

Utilice los archivos de salida de la herramienta de configuración para implementar la configuración de aplicaciones y directivas

La herramienta de configuración genera los siguientes archivos. Estos archivos se guardan en la ubicación/directorio donde se carga y ejecuta la herramienta.

- policy.json
- storefront.ps1
- gateway_config

1. Copie los archivos de storefront.ps1 a StoreFront.
2. Ejecute el script storefront.ps1 en PowerShell, como administrador.

   El script crea una carpeta Resources\ SecureBrowser si aún no está disponible en la ruta almacenada.

   El script también actualiza el archivo web.config de la ruta del archivo policy.json.
3. Copia el archivo policy.json a la carpeta Resources\ SecureBrowser que storefront.ps1 crea en el almacén.
4. Copie el gateway_config en un NetScaler y ejecute el script mediante el siguiente comando por lotes en la CLI de NetScaler.

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

> **Nota:**
>
> - Cuando se realiza algún cambio de configuración en la herramienta, se deben volver a generar los scripts y las directivas. Debe volver a copiar el archivo policy.json a la carpeta Resources\ SecureBrowser del equipo StoreFront y el script gateway_config debe volver a ejecutarse en NetScaler.
> - No es necesario volver a ejecutar storefront.ps1 si no se cambia el nombre o la URL del almacén.

Referencias adicionales

Consulte la siguiente documentación para obtener más información.

- Secure Private Access para instalaciones locales
- Guía de implementación: Secure Private Access en las instalaciones