Citrix Secure Private Access - Legacy

Contents

Configure Secure Private Access for on-premises deployments - Legacy

November 22, 2023

The Secure Private Access for on-premises solution configuration is a four-step process.

1. Publish the apps
2. Publish the policies for the apps
3. Enable routing of traffic through NetScaler Gateway
4. Configure authorization policies

Important:

A config tool is available to quickly onboard apps and policies for the apps and also configure the NetScaler Gateway and StoreFront settings. However, note the following before using the tool.

- Read the Publish the apps and Publish policies for the apps sections to ensure that you have the complete understanding of the configuration requirements for the on-premises solution configuration.

- This tool can only be used as a complement to the existing procedures documented in this topic and does not replace the configuration that must be performed manually.

For complete details about the tool, see Configure apps and policies using the Secure Private Access config tool.

Step 1: Publish the apps
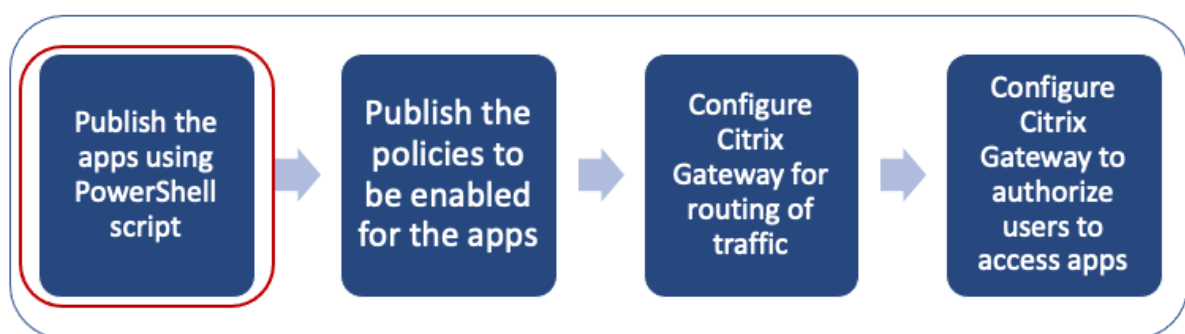
You must use the PowerShell script to publish the URLs. Once the app is published, it can then be managed using the Citrix Studio console.

You can download the PowerShell script from https://www.citrix.com/downloads/workspace-app/powershell-module-for-configuring-secure-private-access-for-storefront/configure-secure-private-access-for-storefront.html.

---

1. On the machine containing the PowerShell SDK, open PowerShell.

2. Run the following command:

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

3. Define the variables for the Web app.

```
1  $citrixUrl: " <URL of the app> "
2  $appName: <app name as it must appear on Workspace>
3  $DesktopGroupId: 1
4  $desktopgroupname: <your desktop group name>
5  $AppIconFilePath:  <path of the image file>
6  <!--NeedCopy-->
```

> **Note:**
>
> Ensure to update the placeholders marked with angular brackets (< >) before running the command.

After assigning the location and application name, run the following command to publish the application.

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

The published app appears under the **Applications** section in **Citrix Studio**. You can now modify the app details from the Citrix Studio console itself.

For more info on publishing the app and changing the default icon of the published app, see Publish content.

Step 2: Publish policies for the apps
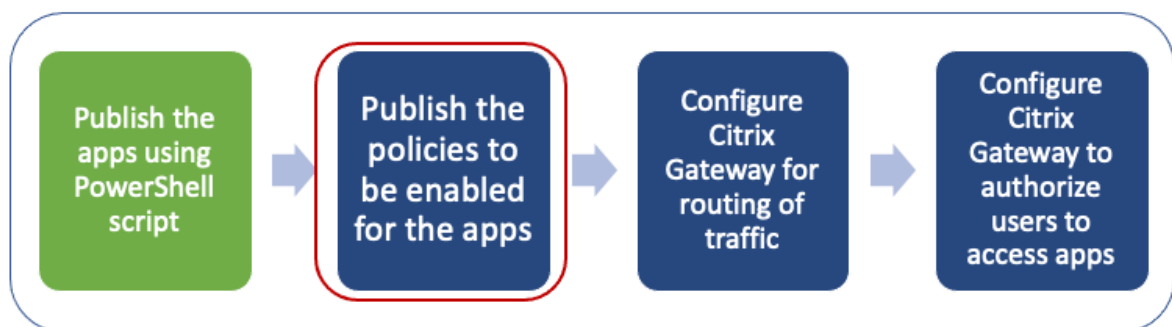
The policy file defines each published app's routing and security controls. You must update the policy file on how a Web or a SaaS app is routed (via gateway or without gateway).

To enforce access policies on the apps, you must publish the policies for each of the Web or SaaS app. To do this, you must update the policy JSON file and the Web.config file.

- **Policy JSON file:** Update the policy JSON file with the app details and the security policies for the apps. The policy JSON file must then be placed in the StoreFront server at `C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser`.

  > **Note:**
  >
  > You must create the folders named **Resources** and **SecureBrowser** and then add the policy JSON file in the SecureBrowser folder.
  > For more details on the various policy actions and their values, see Application access policy details.

- **Web.config file:** To make the new policy details available for the Citrix Workspace app and Citrix Enterprise Browser, you must modify the web.config file in the StoreFront store directory. You must edit the file to add a new XML tag with the name route. The Web.config file must then be placed in the location C:\inetpub\wwwroot\Citrix\Store1.

  See Sample end-to-end configuration for an example XML file.

  > **Note:**
  >
  > In the path, "store1" refers to the name specified for the store when it was created. If a different store name is used, then an appropriate folder must be created.

  It is recommended that you add a new route at the end of existing routes. In case you add a route in the middle, you must manually update the order number for all the subsequent routes.

Step 3: Enable routing of traffic through NetScaler Gateway
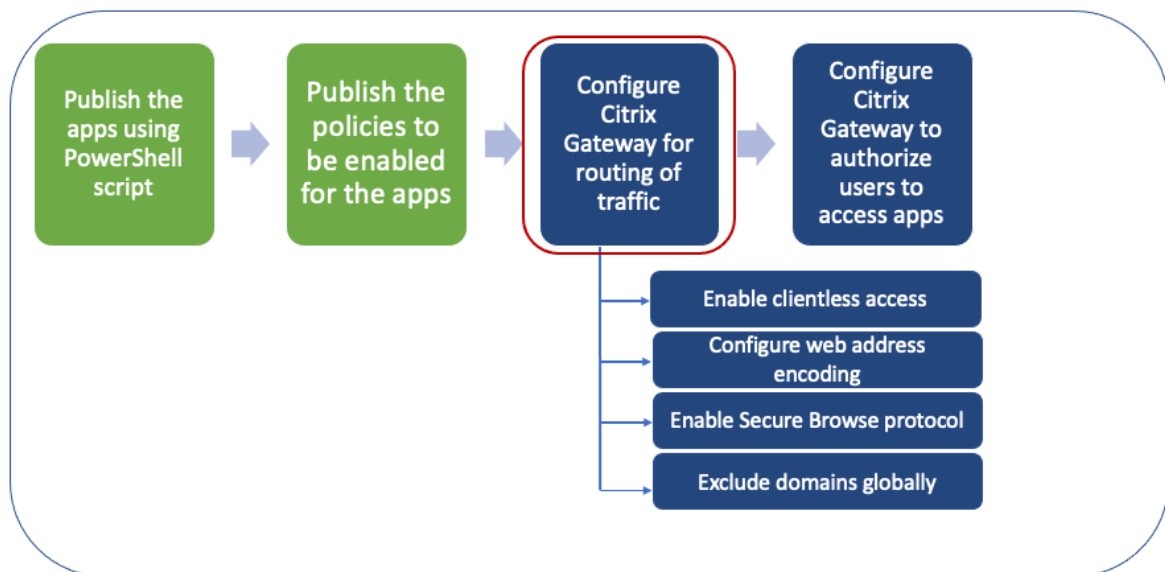
Enabling routing of traffic through NetScaler Gateway involves the following steps:

- Enable clientless access
- Enable URL encoding
- Enable Secure Browse
- Exclude domains from being rewritten in clientless access mode

Clientless access, URL encoding, and secure browse can be enabled globally or per session policy.

- The globally enabled setting applies to all configured NetScaler Gateway virtual servers.
- Per session policy setting applies for users, groups, or Gateway virtual servers.

Enable clientless access

To enable clientless access globally by using the NetScaler Gateway GUI:

On the **Configuration** tab, expand **Citrix Gateway** and then click **Global Settings**.
In the Global Settings page, click **Change global** settings.
On the **Client Experience** tab, in Clientless Access, select **ON**, and then click **OK**.

To enable clientless access by using a session policy by using the NetScaler Gateway GUI:

If you want only a select group of users, groups, or virtual servers to use clientless access, disable or clear clientless access globally. Then, using a session policy, enable clientless access and bind it to users, groups, or virtual servers.

1. On the **Configuration** tab, expand **Citrix Gateway** and then click **Policies > Session**.

2. Click the **Session Policy** tab, and then click **Add**.

3. In **Name**, type a name for the policy.

4. Next to **Profile**, click **New**.

5. In **Name**, type a name for the profile.

6. On the **Client Experience** tab, next to Clientless Access, click **Override Global**, select **On**, and then click **Create**.

7. In **Expression**, enter `true`. When you enter the value `true`, the policy is always applied to the level to which it is bound.

8. Click **Create**, and then click **Close**.

← Configure Citrix Gateway Session Profile

Name

sess_act

Unchecked Override Global check box indicates that the value is inherited from Global Citrix Gateway Parameters.

| Network Configuration | Client Experience | Security | Published Applications | Remote Desktop | PCoIP |

Accounting Policy

⌄

Override Global

☐ Display Home Page
Home Page

☐ Override Global

URL for Web-Based Email

https://exch2013.cgwsanity.net/ow ☐ Override Global

Split Tunnel*

ON ☐ Override Global

Session Time-out (mins)

30 ☐ Override Global

Client Idle Time-out (mins)

☐ Override Global

Clientless Access*

On ⌄ ☑ Override Global ⓘ

To enable clientless access globally by using the NetScaler Gateway CLI:

At the command prompt, run the following command:

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

To enable clientless access per session policy by using the NetScaler Gateway CLI:

At the command prompt, run the following command:

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

Enable URL encoding

When you enable clientless access, you can choose to encode the addresses of internal Web applications or to leave the address as clear text. It is recommended that you leave the web address as clear text for clientless access.

To enable URL encoding globally by using the NetScaler Gateway GUI:

1. On the **Configuration** tab, expand **Citrix Gateway** and then click **Global Settings**.
2. In the **Global Settings** page, click **Change global settings**.
3. On the **Client Experience** tab, in **Clientless Access URL Encoding**, select the setting for encoding your web URL, and then click **OK**.

To enable URL encoding at the session policy level by using the NetScaler Gateway GUI:

1. On the **Configuration** tab, expand **Citrix Gateway** and then click **Policies > Session**.
2. Click the **Session Policy**, tab and then click **Add**.
3. In **Name**, type a name for the policy.
4. Next to **Profile**, click **New**.
5. In **Name**, type a name for the profile.
6. On the **Client Experience** tab, next to **Clientless Access URL Encoding**, click **Override Global**, select the encoding level, and then click **OK**.
7. In **Expression**, enter **true**. When you enter the value **true**, the policy is always applied to the level to which it is bound.

To enable URL encoding globally by using the NetScaler Gateway CLI:

At the command prompt, run the following command:

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

To enable URL encoding per session policy by using the NetScaler Gateway CLI:

At the command prompt, run the following command:

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

Enable Secure Browse

Secure browse and clientless access work together to allow connections using the clientless VPN mode. You must enable the secure browse mode so that Citrix Enterprise Browser can use the secure browse mode to access apps without the legacy VPN.

> **Note:**
>
> When the end user doesn't have Citrix Enterprise Browser installed, the published URLs with the **SPAEnabled** tag open through the device's default browser instead of Citrix Enterprise Browser. In such a case, the security policies don't apply. The issue occurs on the StoreFront deployments only.

To enable secure browse mode globally by using the NetScaler Gateway GUI:

1. On the **Configuration** tab, expand **Citrix Gateway** and then click **Global Settings**.
2. In the Global Settings page, click **Change global settings**.
3. On the **Security** tab, in Secure Browse, select **ENABLED**, and then click **OK**.

To enable secure browse mode at the session policy level by using the NetScaler Gateway GUI:

1. On the **Configuration** tab, expand **Citrix Gateway** and then click **Policies > Session**.
2. Click the **Session Policy** tab, and then click **Add**.
3. In **Name**, type a name for the policy.
4. Next to **Profile**, click **New**.
5. In **Name**, type a name for the profile.
6. On the **Security** tab, click **Override global**, and set **Secure Browse** to **ENABLED**.

To enable secure browse globally by using the NetScaler Gateway CLI:

At the command prompt, run the following command:

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

To enable secure browse per session policy by using the NetScaler Gateway CLI:

At the command prompt, run the following command:

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

Exclude domains from being rewritten in clientless access mode

You must specify the domains to prevent StoreFront from rewriting the URLs in clientless access mode. Exclude StoreFront server FQDNs, or StoreFront load balancer FQDNs, and citrix.com. This setting can be applied only globally.

1. Navigate to **Citrix Gateway > Global Settings**.
2. In **Clientless Access**, click **Configure Domains** for Clientless Access.
3. Select **Exclude Domain**.

---

4. In **Domain Names**, and enter the domain names (StoreFront server FQDNs, or StoreFront load balancer FQDNs).

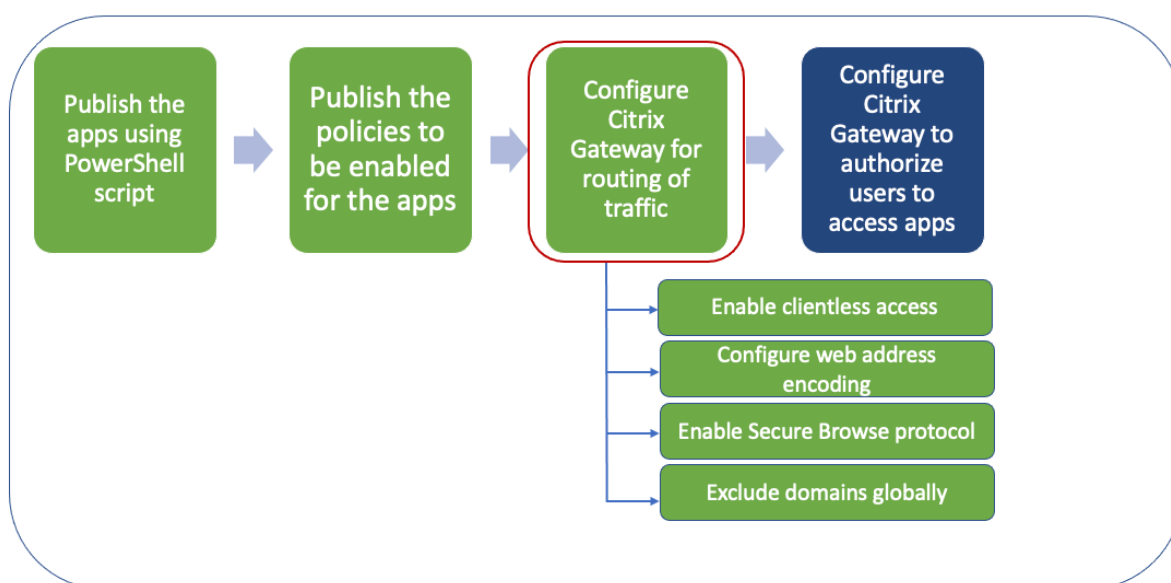5. Click the **+** sign and enter `citrix.com`.

6. Click **OK**.

To exclude domains by using the NetScaler Gateway CLI:

At the command prompt, run the following command:

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

Step 4: Configure authorization policies

Authorization specifies the network resources to which users have access when they log on to NetScaler Gateway. The default setting for authorization is to deny access to all network resources. Citrix recommends using the default global setting and then creating authorization policies to define the network resources users can access.

You configure authorization on NetScaler Gateway by using an authorization policy and expressions. After you create an authorization policy, you can bind it to the users or groups that you configured on the appliance. User policies have a higher priority than group-bound policies.

Default authorization policies: Two authorization policies must be created to allow access to the StoreFront server and deny access to all published web apps.

- Allow_StoreFront
- Deny_ALL

Web app authorization policies: After creating the default authorization policies, you must create authorization policies for each published web app.

- Allow_<app1>
- Allow_<app2>

To configure an authorization policy by using the NetScaler Gateway GUI:

1. Navigate to **Citrix Gateway > Policies > Authorization**.
2. In the details pane, click **Add**.
3. In Name, type a name for the policy.
4. In Action, select **Allow or Deny**.
5. In Expression, click **Expression Editor**.
6. To configure an expression, click **Select** and choose the necessary elements.
7. Click **Done**.
8. Click **Create**.

To configure an authorization policy by using the NetScaler Gateway CLI:

At the command prompt, run the following command:

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

To bind an authorization policy to a user/group by using the NetScaler Gateway GUI:

1. Navigate to **Citrix Gateway > User Administration**.
2. Click **AAA Users** or **AAA Groups**.
3. In the details pane, select a user/group and then click **Edit**.
4. In **Advanced Settings**, click **Authorization Policies**.

5. In the Policy Binding page, select a policy or create a policy.

6. In **Priority**, set the priority number.

7. In **Type**, select the request type and then click **OK**.

To bind an authorization policy by using the NetScaler Gateway CLI:

At the command prompt, run the following command:

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

Sample end-to-end configuration

In this example, an app named "Docs"with the URL https://docs.citrix.com is published to Citrix Workspace.

1. On the machine containing the PowerShell SDK, open PowerShell.

2. Run the following command.

```
1  Add-PsSnapin Citrix\*
2  $dg = Get-BrokerDesktopGroup – Name PublishedContentApps
3  <!--NeedCopy-->
```
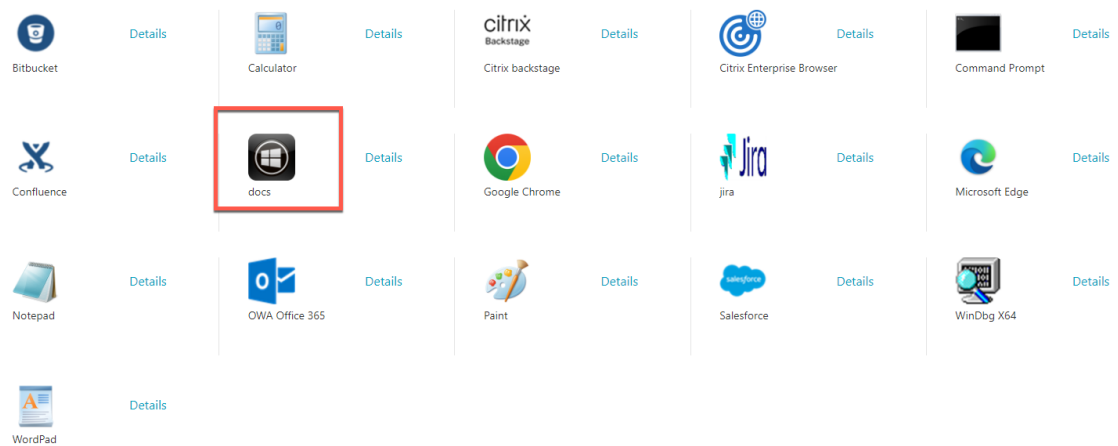
3. Add the following details to the cmdlet.

```
1  $citrixUrl: " https://docs.citrix.com "
2  $appName: docs
3  $DesktopGroupId: 1
4  $desktopgroupname: <mydesktop23>
5  <!--NeedCopy-->
```

4. Run the following command.

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

The app is now published on Citrix Workspace.

5. Update the policy JSON file with the app ("docs") details. Ensure the following:

- `proxytraffic_v1` value is always set to `secureBrowse`. This setting ensures that the Citrix Enterprise Browser tunnels the traffic to the webpage via NetScaler Gateway using the secure browse protocol.
- `browser_v1` value is always set to `embeddedBrowser`. This setting is only applicable when Citrix Enterprise Browser (CEB) is configured as a work browser. When set to `embeddedBrowser`, links related to configured Secure Private Access domains open in CEB.
- `secureBrowseAddress` value is your NetScaler Gateway URL.

```json
{
  "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. Place the policy JSON file at C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser.

7. Modify the Web.config file to point to the policy file that you updated.

```xml
<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. On your NetScaler Gateway on-premises appliance, do the following:

   - Enable clientless access to the apps. You can enable clientless access globally or at a session level.
   - Enable web address encoding
   - Enable Secure Browse mode
   - Exclude domains from being rewritten in clientless access mode

For details, see Step 3: Enable authentication and authorization using the on-premises NetScaler Gateway.

End-user flow

- Log on to StoreFront as a user who can access applications in the PublishedContentApps delivery group.

- Once you log on, you must see the new application with the default icon. You can customize the icon as required. For details, see https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/.

- When you click the app, the app opens in Citrix Enterprise Browser.

Application access policy details

The following table lists the available access policy options and their values.

Key name	Policy description	Value
screencapture_v1	Enable or disable the anti-screen capture feature for the webpage	enabled or disabled
keylogging_v1	Enable or disable anti-keylogging for the webpage	enabled or disabled
watermark_v1	Display or not display the watermark on the webpage	enabled or disabled
upload_v1	Enable or disable uploads the webpage	enabled or disabled
printing_v1	Enable or disable printing from the webpage	enabled or disabled
download_v1	Enable or disable downloads from the webpage	enabled or disabled

Key name	Policy description	Value
clipboard_v1	Enable or disable the clipboard on the webpage	enabled or disabled
proxytraffic_v1	Determines whether the Citrix Enterprise Browser tunnels the traffic to the webpage via NetScaler Gateway using secure browse or enables direct access	direct or secureBrowse
browser_v1	Applicable only when Citrix Enterprise Browser is configured as the Work Browser. When set to embeddedBrowser, links related to configured Secure Private Access domains open in Citrix Enterprise Browser	systemBrowser or embedded-Browser

Key name	Policy description	Value		
name	Name of the Web or the SaaS app published	It is recommended that you use the same name that you have entered while publishing the app patterns	Comma-separated list of domain names related to this app. You can also use wildcards. These domain names are used to apply policies on the apps by the Citrix Enterprise Browser.	Examples: ".*office.com/*", ".*office.net/*", ".*microsoft.com/* ".share-point.com/*"

Note:

Anti-keylogging and anti-screen capturing require the installation of the App protection feature that comes with the Citrix Workspace app.

Configure apps and policies using the Secure Private Access config tool - Legacy

November 22, 2023

You can use the Secure Private Access config tool on a Citrix Virtual Apps and Desktops delivery controller to quickly create a SaaS or Web application. In addition, you can use this tool to set application restrictions, traffic routing, and create a NetScaler Gateway. The tool generates script files as output that can be run on the respective machines to deploy the configuration.

Supported product versions

Ensure that your product meets the minimal version requirements.

- Citrix Workspace app

    - Windows –2303 and later

– macOS –2304 and later

- Citrix Virtual Apps and Desktops –Supported LTSR and current versions
- StoreFront –LTSR 2203 or non-LTSR 2212 and later
- NetScaler –12.1 and later

Prerequisites to use the config tool

- Access to download the config tool from the Downloads page.
- Admin permissions on the Citrix Virtual Apps and Desktops controller to run the config tool.
- At least one delivery group exists on the delivery controller.

## Get started with the config tool

You can perform the following tasks using the config tool.
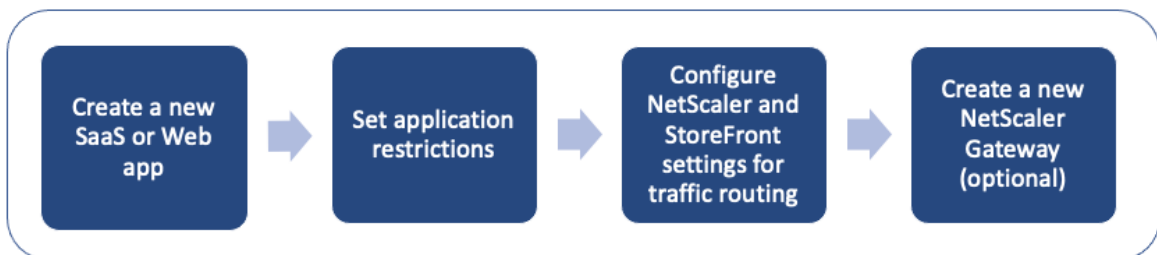
- Publish a new application
- Set application restrictions
- Configure StoreFront and NetScaler Gateway settings
- Configure a new NetScaler Gateway

Publish a new application

1. Run the config tool.

2. In the **Select an App** section, select **New App** in the drop-down list, and then click **Add**.
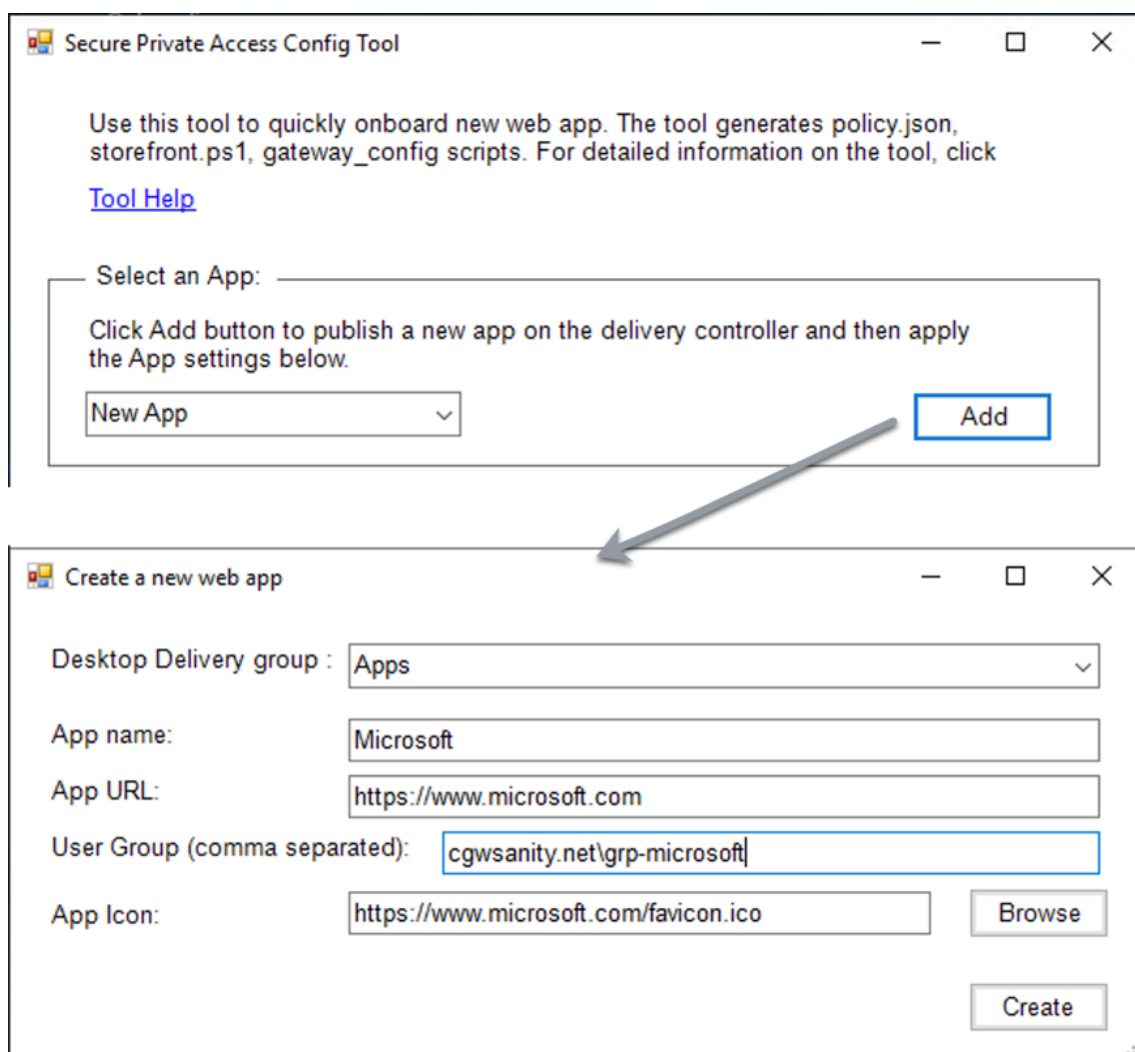
3. Complete the app configuration.

- **Desktop Delivery group**: Select the delivery group for which this app must be made accessible.
  All existing delivery groups are enumerated in the Desktop delivery group.

- **App name**: Enter the app name.

- **App URL**: Specify the URL for the app.

- **User group**: Enter both the domain name and group name in the format "Domain\Group". User groups can contain spaces. For example, "cgwsanity.net\grp-microsoft", "cgwsanity.net\grp microsoft".
  These groups must already exist in the 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.

- **App icon**: The tool uses favicon.ico of the URL if detected. Admin can also customize the icons if necessary. If no icon is provided by the admin, the default icon is assigned to the app.

4. Click **Create**.

The application is published on the delivery controller and is available to the users in the User groups in StoreFront.

Set application restrictions

After you have published a new application, you can enable or disable restrictions for that app.

1. In the **Select an App** section, select the app from the drop-down list for which you want to enforce the settings.

2. Configure the app settings in the **App Settings** section.

- **Related Domains Patterns**: The related domain URL is auto-populated based on the app URL. Admins can add additional domains separated by a comma.
- **Active Directory Group**: Enter the groups for which this application must be accessible. This is a mandatory field.
  You can enter multiple groups separated by a comma. These groups must match the groups available in the Active Directory. There is no validation done on the group names that you enter here. So, it is important that you take care to enter the group names to match with what is there in the Active Directory.
- **App settings**: All app settings are restricted (selected) by default. You can select or clear the appropriate settings that you want for the user groups.
- **Proxy traffic**: Select secureBrowse. This setting enables the Citrix Enterprise Browser to tunnel the traffic to the webpage via NetScaler Gateway.

3. Click **Apply**.

Configure StoreFront and NetScaler Gateway settings

You can configure settings for routing traffic through NetScaler Gateway. You can configure an existing NetScaler Gateway or create a new NetScaler Gateway in the **Gateway and StoreFront settings** section.
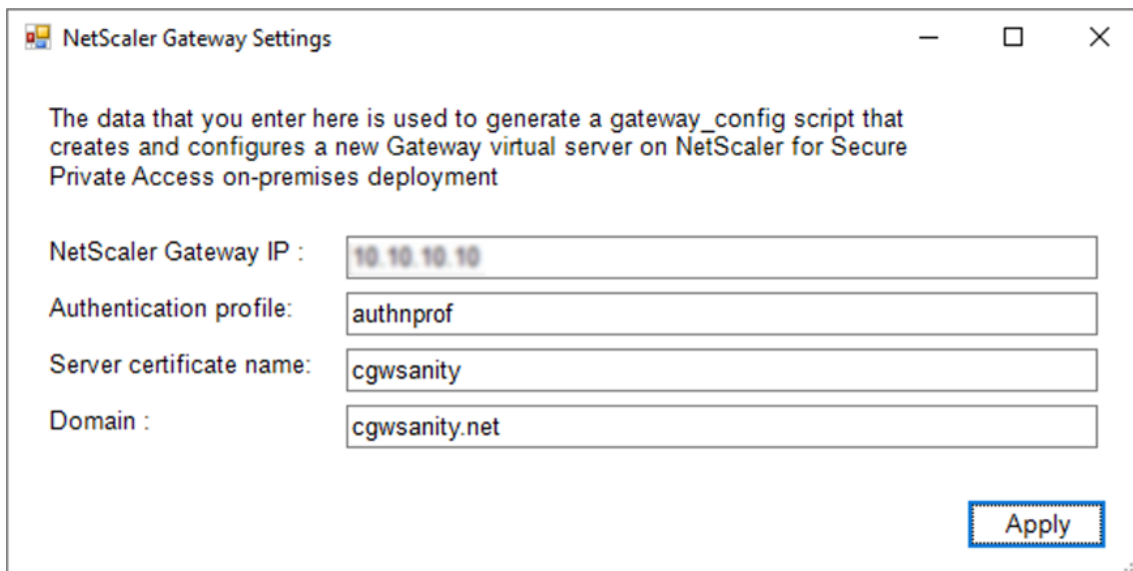

- **Default route**: If a policy is not defined for the app, the default route is applied for the apps.

  - **secureBrowse**: The Citrix Enterprise Browser tunnels the traffic to the webpage via NetScaler Gateway.
  - **Direct**: The Citrix Enterprise Browser enables direct access to the apps.

- **NetScaler Gateway**: Enter the NetScaler Gateway URL.

- **StoreFront Store URL**: Enter the complete StoreFront store URL. For example, `http://< directory path>/Citrix/<StoreName>`. You can get the URL from the StoreFront console.

- (Optional) **Create New Gateway**: Select the checkbox to create a new NetScaler Gateway and click **Create**.

Create a new NetScaler Gateway (optional)

You can create a new NetScaler Gateway if you do not want to change the existing gateway settings.

If you already have a NetScaler Gateway, you can configure the authorization policies and bindings for the apps by using the config tool.

1. You must enter the following details for the new NetScaler Gateway. No validation is done by the tool on the values that you enter when creating a new gateway. So, it is important that you take care to enter accurate values.

- **Gateway IP**: IP address of the NetScaler Gateway.

- **Authentication profile**: Enter the authentication profile name that is already configured on NetScaler. For details, see Authentication profiles.

- **Server certificate name**: Enter the SSL certificate name that is already configured on NetScaler. For details, see SSL certificates.

- **Domain**: Used for SSO to apps in the internal network. For details, see VPN session action.

2. Click **Apply**.

3. Click **Generate policy and scripts**.

   The policy.json, storefront.ps1, and gateway_config files are generated and stored in the location from where you have run the config tool.
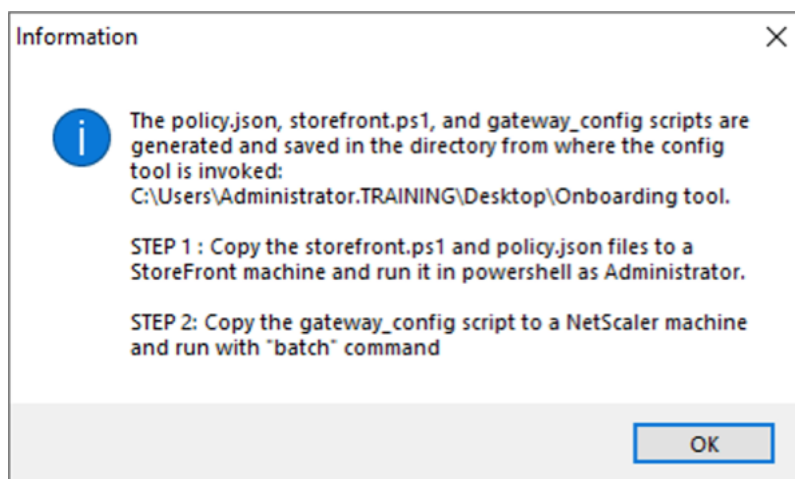
When you open the gateway_config file in a supported application, you can view two sections in the output file.

- Sections related to NetScaler Gateway configuration (applicable only when a new gateway is created)
- Sections related to the authorization policies, user groups, and binding policies to the user groups.

The following image displays the gateway_config file of a new NetScaler Gateway configuration.

```
################################################################################################
#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 ██.██.███.███ ███ –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
```

The following image displays the gateway_config file of an updated NetScaler Gateway configuration.

```
################################################################################
#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 with the new NetScaler Gateway

- For configuring StoreFront and NetScaler Gateway settings in the tool, you need the following:

  - NetScaler Gateway FQDN
  - StoreFront store URL

- StoreFront configuration requirements:

  - NetScaler Gateway: Remote access is enabled.
  - Pass-through authentication from NetScaler Gateway is enabled.
  - Active directory: Admin access to add or update users or groups, and to configure authentication profile or policies on NetScaler.

For more details, see Integrate NetScaler Gateway with StoreFront.

Use the config tool output files to deploy apps and policies configuration

The config tool generates the following files. These files are saved in the location/directory where the tool is uploaded and run.

- policy.json
- storefront.ps1
- gateway_config

1. Copy storefront.ps1 files to StoreFront.

2. Run the storefront.ps1 script on PowerShell, as an administrator.

   The script creates a Resources\SecureBrowser folder if it is not already available in the path under store.

   The script also updates the web.config file for the route for the policy.json file.

3. Copy the policy.json file to the Resources\SecureBrowser folder that the storefront.ps1 creates under the store.

4. Copy the gateway_config to a NetScaler and run the script using the following batch command on the NetScaler CLI.

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

> **Note:**
>
> - When any configuration change is done in the tool, the scripts and policies have to be regenerated. You must copy the policy.json file again to the Resources\SecureBrowser folder on the StoreFront machine and the gateway_config script has to be run again on the NetScaler.
> - You don't have to run the storefront.ps1 again if the store name/URL is not changed.

Additional references

Refer to the following documentation for more details.

- Secure Private Access for on-premises
- Deployment Guide: Secure Private Access On-Premises